Protokolle für privatsphärengerechtes Smart Metering

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

von der Fakultät für Informatik
des Karlsruher Instituts für Technologie (KIT)

genehmigte

Dissertation

von

Dipl.-Inform. Sören Finster

aus Pforzheim

Tag der mündlichen Prüfung:	16. Juli 2014
Erste Gutachterin:	Professorin Dr. Martina Zitterbart
	Karlsruher Institut für Technologie (KIT)
Zweiter Gutachter:	Professor Dr. Christoph Sorge
	Universität des Saarlandes

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Stromnetze galten für lange Zeit als die größten, von Menschen geschaffenen Maschinen[1]. Eines der weltweit größten Stromnetze, das „europäische Verbundsystem“ (auch *UCTE-Verbundnetz* genannt), hat eine geographische Ausdehnung von mehreren tausend Kilometern und deckt damit große Teile Europas ab. Es versorgt über 450 Millionen Menschen mit Strom und erreicht dabei Spitzenlasten von 390 Gigawatt [30]. Erzeugt wird diese Leistung von einer Vielzahl von Stromerzeugern innerhalb des gesamten Netzes. Die Koordination dieser Stromerzeuger stellt eine Herausforderung dar, die mit wachsender Zahl an Stromerzeugern zunehmend komplexer wird.

Aktuelle Stromnetze wurden nicht für die Größe und Komplexität entworfen, mit der sie heute betrieben werden. Stattdessen liegt ein langer Prozess von Anpassungen und schrittweisen Verbesserungen hinter ihnen. Deshalb spricht man auch von der *Evolution* der Stromnetze. Doch dieser erprobte Prozess der langsamen Weiterentwicklung wird durch neue Rahmenbedingungen auf die Probe gestellt. Das zunehmende Maß an regenerativer und dezentraler Energieerzeugung führt zu einem wesentlich höheren Bedarf an Information und Kommunikation. Wo vorher wenige Großkraftwerke koordiniert werden mussten, wird nun die gleiche Leistung von einer Vielzahl von Klein- und Kleinstkraftwerken erzeugt. Dazu zählen Photovoltaikanlagen, Kraft-Wärme-Kopplungen und Biogasanlagen. Diese Kleinstkraftwerke befinden sich teilweise in Privathaushalten, die über das gesamte Stromnetz verteilt sind. Die Koordination dieser Vielzahl an dezentralen

[1] Um diesen Titel konkurriert heutzutage das Internet mit ihnen.

Stromerzeugern stellt eine der größten Herausforderungen bei der Evolution des klassischen Stromnetzes zum *Smart Grid* dar.

Ein wichtiges Werkzeug, um dieser Herausforderung zu begegnen, ist das Smart Metering (auch *Advanced Metering Infrastructure*). Hierbei wird der klassische Stromzähler im Haushalt durch einen *intelligenten Stromzähler* ersetzt. Intelligente Stromzähler zeichnen sich im Besonderen dadurch aus, dass sie an ein Kommunikationsnetz, wie beispielsweise das Internet, angebunden sind. Durch diese Anbindung kann der Zähler automatisiert aus der Ferne von einem sogenannten *Messdienstleister* ausgelesen werden. Somit wird ein detaillierter und zeitnaher Einblick in die aktuelle Energieerzeugungs- und Energieverbrauchssituation im Stromnetz erreicht. Dies birgt Vorteile, insbesondere für Planung und Koordination der Energieerzeugung. Aber auch für die Kalkulation von zeit- oder lastvariablen Tarifen oder zur Information im Haushalt eignen sich die zeitlich hochaktuellen Verbrauchsdaten. Für das Jahr 2020 wird mit weltweit 800 Millionen installierten intelligenten Stromzählern gerechnet [130].

Jedoch wird durch Smart Metering auch ein Einblick in die privaten Geschehnisse innerhalb des Haushalts gegeben. Das regelmäßige Auslesen des intelligenten Stromzählers führt zu einer detaillierten Übersicht über den Energieverbrauch eines Haushalts. Diese kann Rückschlüsse auf höchst private Informationen gewähren. Naheliegend sind dabei Rückschlüsse auf die Anwesenheit und damit auf Arbeits- und Urlaubszeiten. Aber auch intimere Details sind über den Energieverbrauch zugänglich: Anzahl der Bewohner, Besitz bestimmter Geräte wie beispielsweise einer Klimaanlage oder persönliche Gewohnheiten und Rituale. In den falschen Händen sind Smart Metering Daten ein gefährliches Werkzeug. In Österreich äußerte sich die Furcht vor Datenmissbrauch in einer Gesetzesänderung, die Bürgern die Möglichkeit zum Ausstieg aus dem bisher vorgeschriebenen Smart Metering ermöglicht [110].

1.1 Problemstellung

Damit Smart Metering als Werkzeug für die Realisierung des Smart Grids bedenkenlos eingesetzt werden kann, ist der Schutz der Privatsphäre unabdingbar. Dies beinhaltet vor allem den Schutz vor unbefugtem Zugriff auf Messdaten. Dieser Aspekt ist auch für die Daten erhebenden Parteien von größter Wichtigkeit. Ein Datenleck könnte schwerwiegende Folgen haben und gegebenenfalls hohe Schadenersatzforderungen nach sich ziehen. Somit haben selbst die Empfänger der

Daten ein großes Interesse möglichst nur die Daten zu erfassen und zu speichern, die auch wirklich für die Erbringung ihrer Dienste nötig sind. Dies wäre auch im Interesse der Kunden, die schon das Sammeln und Speichern der Messdaten als Verletzung der Privatsphäre wahrnehmen.

Das Forschungsfeld des „privatsphärengerechten Smart Meterings“ widmet sich der Frage, wie ohne Verletzung der Privatsphäre Smart Metering durchgeführt werden kann. Dabei bestimmt die Anwendung, die mittels Smart Metering realisiert werden soll, welche Freiheitsgrade zum Privatsphärenschutz genutzt werden können. Beim Smart Metering zur Rechnungslegung können Messwerte beispielsweise über die Zeit hinweg aggregiert werden, um monatliche oder jährliche Rechnungen zu erstellen. Ein Smart Metering zur Stromnetzüberwachung oder Produktionsplanung benötigt jedoch zeitlich sehr aktuelle Daten und kann daher keine Aggregation über die Zeit verwenden. Ein häufig verfolgter Lösungsansatz ist daher die *Aggregation von Messwerten* über mehrere Haushalte. Diesem Prinzip liegt die Beobachtung zu Grunde, dass für viele Anwendungen im Smart Grid die Einzelbetrachtung eines Haushalts nicht nötig ist. Stattdessen genügt die Betrachtung einer Menge von Haushalten als Ganzes, also das Aggregat der einzelnen Messwerte, die von intelligenten Stromzählern in den Haushalten gemessen wurden.

Die privatsphärengerechte Aggregation von Messwerten stellt insbesondere dann eine Herausforderung dar, wenn diese ohne Unterstützung durch eine vertrauenswürdige dritte Partei geschieht. In der Literatur wird dieser Herausforderung häufig mittels rechenintensiver, kryptologischer Methoden begegnet. Dabei wird außer Acht gelassen, dass intelligente Stromzähler nur in sehr beschränktem Umfang über Rechen- und Speicherkapazität verfügen.

Der von den vorgeschlagenen Verfahren gewährte Privatsphärenschutz wird in vielen Fällen nur in der Präsenz eines sehr schwach modellierten, passiven Angreifers betrachtet. Auch wird nicht betrachtet, dass der Messdienstleister der Angreifer sein könnte oder von diesem korrumpiert sein könnte. Da die Privatsphäre auch vor dem Messdienstleister geschützt werden soll, ist ein Ausschluss eines Angriffs durch den Messdienstleister realitätsfern.

Ein Aspekt, der bisher keine Beachtung fand, ist die Unzuverlässigkeit der Kommunikationsanbindung der intelligenten Stromzähler und die Unzuverlässigkeit der intelligenten Stromzähler selbst. Um im Smart Grid eingesetzt werden zu können, sollte ein Smart Metering Verfahren auch bei Störungen noch weitestgehend seine Funktionalität beibehalten. Daher sollten, bereits beim Entwurf eines Smart

Metering Verfahrens, solche Störungen berücksichtigt und ihre Auswirkungen auf das Verfahren untersucht werden.

Es stellen sich daher folgende Anforderungen an ein Verfahren zum privatsphärengerechten Smart Metering:

- Durchführbarkeit auf ressourcenbeschränkter Hardware.
- Schutz der Privatsphäre auch bei Angriffen durch Außenstehende und durch den Messdienstleister.
- Weitestgehende Funktion auch bei Störungen.

1.2 Zielsetzung und Beiträge

Ziel dieser Arbeit ist die Entwicklung und Evaluation von Verfahren zum privatsphärengerechten Smart Metering zur Stromnetzüberwachung und Produktionsplanung. Im Fokus steht hierbei der Privatsphärenschutz. Das Übermitteln gefälschter Messdaten, beispielsweise zum Stromdiebstahl, wird in dieser Arbeit nicht betrachtet. Die realistische Einsetzbarkeit der Verfahren auf ressourcenbeschränkter Hardware stellt ein wichtiges Ziel für die Entwicklung der Verfahren dar.

Es werden Rahmenbedingungen angenommen, die einen Ausfall von intelligenten Stromzählern oder Kommunikationsanbindungen jederzeit vorsehen. Bei der Entwicklung der Verfahren muss daher berücksichtigt werden, dass auch bei solchen Störungen die Funktion des Smart Meterings weitestgehend erhalten bleibt. Insbesondere ist eine Evaluation dieser Eigenschaft ein wichtiges Ziel dieser Arbeit.

Der Schutz der Privatsphäre soll nicht auf dem Vertrauen in eine dritte Partei aufgebaut und auch bei Anwesenheit von starken, aktiven Angreifern betrachtet werden. Diese Betrachtung muss den Messdienstleister als Angreifer berücksichtigen.

Die Arbeit umfasst die folgenden Beiträge:

- **Entwurf und Evaluation eines Verfahrens zur privatsphärengerechten Datenaggregation:** Das in dieser Arbeit vorgestellte SMART-ER Verfahren baut auf den Grundprinzipien des Slice-Mix-Aggregate (SMART) Verfahrens auf. Es bietet, bei sehr geringem Ressourcenverbrauch, einen hervorragenden Privatsphärenschutz.

Es wird gezeigt, dass bereits mit wenigen Kilobyte an übertragenen Daten und einigen trivialen Rechenoperationen ein Privatsphärenschutz erreicht wird, der Angriffen von dritten, also ohne Kooperation mit dem Messdienstleister, widersteht. Auch bei einer Kooperation des Messdienstleisters mit dem Angreifer bietet SMART-ER einen guten Privatsphärenschutz. Dieser besteht bereits dann für einen Haushalt, wenn dessen intelligenter Stromzähler mit mindestens einem anderen intelligenten Stromzähler kooperieren kann, der ebenfalls nicht mit dem Angreifer kooperiert.

Mittels einer simulativen Untersuchung wird das Verhalten von SMART-ER bei Störungen evaluiert. Im Vergleich mit einem nicht privatsphärengerechten Verfahren schneidet SMART-ER nur unwesentlich schlechter ab. Dies erreicht SMART-ER durch eine Partitionierung der intelligenten Stromzähler in Gruppen einer konfigurierbaren Gruppengröße. Je größer die Gruppengröße dabei konfiguriert wird, desto stärker wirken sich Störungen auf das Ergebnis aus.

- **Entwurf und Evaluation eines Verfahrens zur dezentralen Gruppenorganisation:** Da die zentrale Partitionierung der intelligenten Stromzähler in SMART-ER eine Möglichkeit für einen Angriff bietet, wird mit dem Smart Meter Speeddating Verfahren eine dezentrale Gruppenbildung von kleinen SMART-ER Gruppen vorgestellt.

  In diesem Verfahren organisieren sich intelligente Stromzähler selbständig und ohne Einfluss durch den Messdienstleister in kleine Gruppen. Mit dieser Gruppeneinteilung wird dann das SMART-ER Verfahren durchgeführt. Die Gruppenbildung wird dabei von Messintervall zu Messintervall neu vorgenommen.

  Es wird gezeigt, dass ein Angriff auf das Smart Meter Speeddating Verfahren die Kooperation des Messdienstleisters und einen großen Anteil an kooperierenden intelligenten Stromzählern benötigt um mit hoher Wahrscheinlichkeit erfolgreich sein zu können. Ein solcher Angriff kann aufgrund von statistischen Anomalien von den intelligenten Stromzählern erkannt werden.

  Die Einsetzbarkeit des Verfahrens auf ressourcenbeschränkter Hardware wird auch durch eine Evaluierung auf Knoten eines Sensornetzes nachgewiesen.

Mittels einer simulativen Untersuchung wird das Verhalten von Smart Meter Speeddating bei Störungen evaluiert und gezeigt, dass es auch dann die Funktionalität des Smart Meterings weitestgehend erhält.

- **Entwurf und Evaluation eines Verfahrens zur dezentralen Aggregation:** Das in dieser Arbeit vorgestellte Elderberry Verfahren stellt einen Ansatz zur dezentralen Aggregation dar. Im Gegensatz zum Smart Meter Speeddating Verfahren findet eine Vorverarbeitung von Messdaten ohne Mitwirken des Messdienstleisters, also dezentral, statt. Dies ermöglicht eine Aggregation über eine größere Gruppengröße während deren Nachteile für die Leistung bei Störungen abgeschwächt werden.

  Elderberry nutzt ein peer-to-peer Overlaynetz um eine dezentrale Organisation der intelligenten Stromzähler in sogenannte Abschnitte zu realisieren. Innerhalb dieser Abschnitte führen intelligente Stromzähler selbständig das SMART-ER Verfahren untereinander durch, indem einige intelligente Stromzähler Funktionalität des Messdienstleisters übernehmen. Durch einen sogenannten Ende-zu-Ende-Fragmentaustausch wird gewährleistet, dass auch in Elderberry ein Angriff auf die Privatsphäre eines Haushalts nur dann durchgeführt werden kann, wenn der Messdienstleister mit dem Angreifer kooperiert. Auch dann ist ein Angriff mit hoher Erfolgswahrscheinlichkeit nur mit einer sehr großen Anzahl an korrumpierten intelligenten Stromzählern möglich.

  Die Evaluation der Funktion bei Störungen zeigt, dass das Elderberry Verfahren mittels der dezentralen Aggregation ein vergleichbares oder besseres Ergebnis als das SMART-ER Verfahren bei gleicher Anzahl Messwerte pro Aggregat erreicht.

- **Simulationswerkzeug OverGrid:** Ein weiterer Beitrag ist die Erweiterung des Simulationswerkzeugs OverSim zur Simulation von Stromnetzen. Das resultierende Simulationswerkzeug wird OverGrid genannt und durch eine modulare Architektur realisiert. So kann ein Haushalt aus vielen einzelnen Verbrauchs- und Produktionsmodulen bestehen, die jeweils einzeln implementiert werden können. Die realitätsnahe Implementierung dieser Module führt zu Lastgängen, die auch in realen Stromnetzen auftreten können.

1.3 Zugrunde liegende Veröffentlichungen

Diese Arbeit baut auf einer Reihe von Veröffentlichungen auf. Die hier präsentierten Ergebnisse entstanden durch wesentlich umfangreichere Evaluationen und werden ausführlicher diskutiert als es im Rahmen der jeweiligen Veröffentlichung möglich gewesen wäre.

- Das in Kapitel 5 behandelte Verfahren SMART-ER wurde in der Grundidee auf dem VDE Kongress 2010 [55] vorgestellt. Eine deutliche Weiterentwicklung mit wesentlich besseren Garantien konnte dann im Workshop *Communications and Control for Smart Energy Systems* auf der INFOCOM 2014 präsentiert werden [54].

- Das in Kapitel 6 vorgestellte Smart Meter Speeddating wurde auf der *International Conference on Smart Grid Communications (SmartGridComm 2013)* präsentiert [51].

- Das in Kapitel 7 behandelte Elderberry Verfahren ist eine Weiterentwicklung des auf dem INFOCOM 2013 Workshop *Communications and Control for Smart Energy Systems* vorgestellten Verfahrens [52].

- Die Übersicht über den Stand der Forschung basiert auf Erkenntnissen aus einem Survey, das im Journal *IEEE Communications Surveys & Tutorials* im dritten Quartal 2014 veröffentlicht werden wird [53].

1.4 Gliederung

In Kapitel 2 werden die für das Verständnis dieser Arbeit notwendigen Grundlagen vermittelt. Insbesondere werden Grundlagen zu Stromnetzen, Smart Metering und Angreifermodellen für Smart Metering gelegt. Auch die Funktionsweise strukturierter peer-to-peer Systeme und die in dieser Arbeite verwendeten kryptographischen Verfahren werden erläutert.

Eine Übersicht über den aktuellen Stand der Forschung zum Thema Privatsphärenschutz im Smart Metering wird in Kapitel 3 dargelegt. Hierzu findet eine Kategorisierung der Arbeiten in Smart Metering zur Rechnungslegung und Smart Metering zur Stromnetzüberwachung und Produktionsplanung statt. In

Abschnitt 3.5.3 werden mit der vorliegenden Arbeit enger verwandte Arbeiten vorgestellt und anhand von definierten Kriterien ein Vergleich und eine Abgrenzung vorgenommen.

In Kapitel 4 wir das, im Rahmen dieser Arbeit entworfene, Simulationswerkzeug OverGrid vorgestellt. Es dient zur effizienten Simulation von Stromnetzen in einem für das Smart Metering Szenario ausreichenden Detailgrad.

In Kapitel 5 wird das Verfahren SMART-ER vorgestellt. Es realisiert durch eine Kooperation von intelligenten Stromzähler untereinander einen peer-to-peer Privatsphärenschutz, der detailliert betrachtet und evaluiert wird. Insbesondere wird der Privatsphärenschutz von SMART-ER in Anwesenheit von starken Angreifern nachgewiesen. Anschließend wird eine Evaluation der mittels SMART-ER erzielbaren Smart Metering Leistung auch bei Störungen evaluiert.

SMART-ER wird in Kapitel 6 als Baustein im Smart Meter Speeddating Verfahren verwendet, welches eine dezentrale Gruppenorganisation der intelligenten Stromzähler vornimmt. Es wird zunächst eine Parameterstudie durchgeführt um geeignete Parameterkonfigurationen zu identifizieren. Deren Privatsphärenschutz und Smart Metering Leistung wird dann evaluiert. Ebenfalls wird eine Implementierung des Verfahrens für extrem ressourcenbeschränkte Hardware vorgestellt.

Kapitel 7 stellt das Elderberry Verfahren zum dezentralen Smart Metering vor. Elderberry ist eine Alternative zum Smart Meter Speeddating und setzt ebenfalls das SMART-ER Verfahren als Baustein ein. Auch Elderberry wird auf Privatsphärenschutz und Smart Metering Leistung evaluiert.

Abschließend werden in Kapitel 8 die Ergebnisse dieser Arbeit zusammengefasst und ein Ausblick auf zukünftige Arbeiten gegeben.

Anhang A ist ein Glossar der in dieser Arbeit verwendeten Begriffe. In Anhang B werden weitere Ergebnisse zu Evaluationen aus Kapitel 6 dargestellt.

Kapitel 2

Grundlagen

Im folgenden Kapitel werden Grundlagen erläutert, die zum Verständnis der Arbeit notwendig sind. Die behandelten Bereiche sind:

- Smart Grid und Smart Metering (Abschnitt 2.1)
- Privatsphäre und Privatsphärenschutz (Abschnitt 2.2)
- Privatsphärengerechte Datenaggregation – SMART (Abschnitt 2.3)
- Peer-to-peer Systeme (Abschnitt 2.4)
- Kryptologische Verfahren (Abschnitt 2.5)

2.1 Smart Grid und Smart Metering

In diesem Abschnitt werden die Grundlagen zum Thema Smart Grid und Smart Metering behandelt. Zunächst wird in Abschnitt 2.1.1 der Begriff Smart Grid erläutert. In Abschnitt 2.1.2 wird das Thema Smart Metering diskutiert. Die Standardisierung von Smart Metering wird in Abschnitt 2.1.3 behandelt. In Abschnitt 2.1.4 werden Angreifermodelle im Smart Metering diskutiert und das in dieser Arbeit verwendete Angreifermodell erläutert.

2.1.1 Smart Grid

Klassische Stromnetze stellen ein hierarchisches Netz der Stromversorgung dar. Energie wird an wenigen Orten zentral erzeugt, durch Übertragungsnetze nahe

zu den Verbrauchern geleitet und dort von Verteilnetzen letztlich ausgeliefert. Der Bezug von Energie wird durch *Energieversorger* abgewickelt, deren Kunden die Haushalte und Endverbraucher sind.

Das Smart Grid als Vision sieht eine Vielzahl von kleinen, autonomen aber miteinander verbundenen Teilnetzen, sogenannten *Microgrids* vor. Das Ziel eines Ausgleichs von Energieerzeugung und Energieverbrauch wird dann sowohl innerhalb eines Microgrids als auch zwischen Microgrids verfolgt. Das Stromnetz selbst wird vom reinen Transportmedium zur dynamisch und eigenständig agierenden Technologie. Die hierfür benötigten Daten können, unter anderem, vom Smart Metering bereitgestellt werden. Es stellt bei der evolutionären Entwicklung vom klassischen Stromnetz zum Smart Grid eine wichtige Schlüsselfunktion dar [63]. Eine Übersicht über das Smart Grid und den Weg dahin bietet beispielsweise Farhangi [49].

2.1.2 Smart Metering

In seiner einfachsten Form beschreibt *Smart Metering* den Einsatz von kommunikationsfähigen Messeinrichtungen in den Haushalten der Kunden. Diese Messeinrichtungen, sogenannte *intelligente Stromzähler*, erlauben eine bidirektionale Kommunikation mit einer Gegenstelle, dem sogenannten *Messdienstleister*. Als *Kommunikationsanbindung* kann beispielsweise der Internetanschluss des Haushalts genutzt werden. Oft wird Smart Metering auch unter dem Begriff *Advanced Metering Infrastructure (AMI)* geführt.

Die bidirektionale Kommunikation der intelligenten Stromzähler ermöglicht Dienste, die früher schwierig oder nicht realisierbar waren. Zur Erkennung von Stromausfällen, beispielsweise, verließ man sich vor dem Smart Metering auf die zeitnahen Beschwerden der Kunden. Mittels Smart Metering können Störungen schneller und ohne Interaktion mit dem Kunden entdeckt werden. Durch Beobachtung der Qualität der Stromversorgung im Smart Metering kann der Ursache für die Störung möglicherweise sogar entgegengewirkt werden, bevor diese Auswirkungen auf den Kunden hat.

Smart Metering ermöglicht auch das zeitnahe Verfolgen von Stromflüssen in einem Stromnetz und damit die zeitnahe Ermittlung des Strombedarfs der Haushalte. Dies spielt insbesondere dann eine Rolle, wenn die Stromproduktion nicht oder nur teilweise steuerbar ist. Bei erneuerbaren Energien, wie Windkraft oder Sonnenenergie, ist dies der Fall. Diese Energie steht zur Verfügung wenn Wind weht oder die Sonne scheint, was im Allgemeinen unabhängig vom Strombedarf der

Kunden eintritt. Mittels Smart Metering kann auf eine Energieknappheit zeitnah reagiert werden. Beispielsweise können weitere Stromerzeuger hinzugeschaltet werden oder eine Anpassung des Strompreises bei *variablen Tarifen* stattfinden. Das direkte Steuern von Energieerzeugern und Energieverbrauchern im Haushalt, wie beispielsweise einer Kraft-Wärme-Kopplung, ist eine Möglichkeit die unter dem Begriff *Demand Side Management (DSM)* geführt wird.

Einige dieser Anwendungen können auch ohne Smart Metering mittels Messeinrichtungen im Stromnetz realisiert werden. Sogenannte *Phasor Measurement Units (PMU)* können detaillierte Daten über Stromflüsse und Stromqualität ermitteln. Wird eine PMU beispielsweise in einer Ortsnetzstation eingerichtet, so können mit ihr detaillierte Daten über das an die Ortsnetzstation angeschlossene Stromnetz ermittelt werden. Eine PMU in der Ortsnetzstation kann jedoch nicht zwischen den angeschlossenen Haushalten unterscheiden und kann daher lediglich Daten über das gesamte angeschlossene Stromnetz liefern. Smart Metering bietet hier mehr Flexibilität und kann Teilmengen der Haushalte des Ortsnetzes betrachten. Dies ist beispielsweise nötig, wenn die Haushalte eines Ortsnetzes verschiedenen Energieversorgungsunternehmen zugehörig sind und diese ein Smart Metering ihrer Kunden durchführen.

Der Begriff „Smart Metering“ beschreibt das Konzept des Messens mittels intelligenter Stromzähler. Die konkrete Durchführung von Smart Metering, also die Anwendung des Konzepts, wird in dieser Arbeit als *Instanz eines Smart Meterings* bezeichnet. Eine Instanz eines Smart Meterings wird durch folgende Parameter charakterisiert:

Zielgruppe: Sie enthält die intelligenten Stromzähler, die von der Instanz des Smart Meterings erfasst werden sollen. Um eine realistische Größenordnung der Anzahl an intelligenten Stromzählern abzuschätzen, werden Zahlen aus dem Monitoringbericht 2013 der Bundesnetzagentur [17] verwendet. Dieser listet für Deutschland circa 48,7 Millionen Zählpunkte, die von 806 Verteilnetzbetreibern und 906 Energieversorgern versorgt werden. Dabei versorgt circa ein Drittel der Energieversorger zwischen 1 000 und 10 000 und ein weiteres Drittel zwischen 10 000 und 30 000 Zählpunkte. Die Anteile für Verteilnetzbetreiber unterscheiden sich nur geringfügig. Nimmt man an, dass ein Verteilnetzbetreiber oder Energieversorger alle zugeordneten Haushalte in einer Instanz eines Smart Meterings aufnehmen möchte, so ist eine Größenordnung von mehreren tausend bis mehreren zehntausend intelligenten Stromzählern realistisch.

Messgröße: Die physikalische Größe, die das Ziel der Messung ist. Dies kann beispielsweise die Leistungsaufnahme des zugehörigen Haushalts in Watt sein. Auch der aufsummierte Energieverbrauch seit der letzten Messung (in Wattstunden) könnte eine Messgröße darstellen. Das Ergebnis einer Messung wird *Messwert* genannt.

Messintervall: Der zeitliche Abstand zwischen zwei durchgeführten Messungen. In aktuellen Pilotprojekten zum Smart Metering, aber auch in der Literatur, hat sich ein Messintervall von 15 Minuten etabliert (siehe beispielsweise [13, 44, 48, 136]).

Betrachtet man eine Verfahren zum Smart Metering aus Sicht des Messdienstleisters, so können für dessen Einsatz folgende Leistungsmerkmale festgestellt werden:

Smart Metering Reichweite (SM-Reichweite): Der Anteil der Zielgruppe, für den der Messdienstleister nach einer Messung (und der SM-Latenz) Messwerte erhält. Die SM-Reichweite wird anteilig zur Zielgruppe in Prozent gemessen.

Smart Metering Latenz (SM-Latenz): Die Zeit, die zwischen Messung der Messgröße und Eintreffen des Messwertes beim Messdienstleister vergeht. Die SM-Latenz wird in Sekunden gemessen.

Kürzestes Smart Metering Intervall (SM-Intervall): Das kürzeste Messintervall, das mittels der eingesetzten Technik realisierbar ist. Das kürzeste SM-Intervall wird in Sekunden gemessen.

Betrachtet man ein gewöhnliches, also nicht privatsphärengerechtes Verfahren zum Smart Metering, bei dem Messwerte vom Messdienstleister direkt bei den intelligenten Stromzählern der Zielgruppe abgerufen oder von diesen an den Messdienstleister gesendet werden, so sind die Leistungsmerkmale dieses Smart Meterings einfach zu bestimmen. Der Messdienstleister erhält Messwerte von den intelligenten Stromzählern innerhalb kürzester Zeit nach der Messung. Wieviel Zeit dazwischen liegt, ist hauptsächlich von der Kommunikationslatenz zwischen intelligentem Stromzähler und Messdienstleister abhängig.

Der Messdienstleister erhält Messwerte von allen intelligenten Stromzähler, die für ihn erreichbar sind. Von intelligenten Stromzählern mit gestörter Kommunikationsanbindung oder defekten intelligenten Stromzählern erhält er keine Messwerte.

Seine SM-Reichweite entspricht also gerade dem Anteil, der zum Zeitpunkt der Messung verfügbar ist.

Der Messdienstleister kann Messungen in sehr kurzen Zeitabständen, also mit kurzem Messintervall, durchführen. Limitiert ist er hier nur durch seine eigene Infrastruktur, die Fähigkeiten des intelligenten Stromzählers und die Datenraten der Kommunikationsanbindungen. Die Leistungsmerkmale eines Verfahrens zum nicht privatsphärengerechten Smart Metering sind also hauptsächlich beeinflusst durch technische Einschränkungen.

Bei Verfahren zum privatsphärengerechten Smart Metering steht der Privatsphärenschutz im Vordergrund und Leistungsmerkmale des erzielten Smart Meterings spielen eher eine untergeordnete Rolle. Für einen realen Einsatz eines privatsphärengerechten Smart Meterings ist dennoch interessant, inwiefern der zusätzliche Privatsphärenschutz Auswirkungen auf die Leistungsmerkmale hat.

2.1.3 Smart Metering Standardisierung

Der Standardisierungsprozess ist für eine Realisierung der Vision des Smart Grids von immenser Bedeutung. Interoperabilität und Stabilität spielen in Stromnetzen eine wichtige Rolle. Die Standardisierung zum Smart Grid wird seit Jahren vorangetrieben. Daher herrscht auch kein Mangel an Standards, die eine technische Realisierung eines Smart Meterings ermöglichen. Beispielsweise gibt es eine Fülle von standardisierten Protokollen zur Fernauslese von intelligenten Stromzählern, wie DLMS/COSEM oder SML. Eine Übersicht über diese Vielzahl bietet beispielsweise Feuerhahn et al. [50]. Eine Übersicht die zusätzlich das Feld der Hausautomation mit einbezieht wird von Craemer et al. [28] gegeben.

Der Fokus der Standardisierungsbemühungen liegt jedoch auf der technischen Realisierbarkeit. Privatsphärenschutz findet, zumindest zunächst, keine Beachtung. Mit dem kürzlich veröffentlichten „Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“ [15] macht das Bundesamt für Sicherheit in der Informationstechnik einen ersten Schritt in Richtung Standardisierung von Smart Metering und dessen Sicherheit. Das Schutzprofil definiert Mindestsicherheitsanforderungen an intelligente Stromzähler. Beispielsweise wird die Unterstützung von Verschlüsselungsverfahren und der Einsatz einer Firewall gefordert. Der Privatsphärenschutz wird hier auf der Ebene der Sicherheitsanforderungen diskutiert. So wird angenommen, dass ein autorisierter und authentifizierter Zugriff auf sensible Daten die Privatsphäre nicht verletzt. Letztlich wird einer autorisierten und authentifizierten Partei, beispielsweise dem

Messdienstleister, vertraut. Eine Pseudonymisierung durch den intelligenten Stromzähler ist im Schutzprofil zwar vorgesehen, eine konkrete Standardisierung von privatsphärengerechtem Smart Metering, beispielsweise mittels Aggregation, wird jedoch nicht durchgeführt.

2.1.4 Angreifermodelle im privatsphärengerechten Smart Metering

Ein Angriff auf ein privatsphärengerechtes Smart Metering hat das Ziel detaillierte Informationen über einzelne Haushalte zu gewinnen. Mittels genauer Informationen über Geschehnisse und Gewohnheiten innerhalb eines Haushalts kann beispielsweise zielgerichtete Werbung mit hoher Präzision geschaltet werden. An charakteristischen Lastgängen einer Klimaanlage lässt sich erkennen, ob ein Haushalt über eine solche verfügt oder nicht. Ein Haushalt ohne Klimaanlage könnte im Hochsommer verstärkt mit Werbung für Klimaanlagen beliefert werden. Doch auch die Verwendung der Informationen für illegale Tätigkeiten liefert Motivation zum Angriff. Wissen über Arbeits-, Urlaubszeiten und Gewohnheiten erlaubt beispielsweise weitestgehend gefahrlose Wohnungseinbrüche. Auch Erpressung mittels gewonnener privater Informationen ist denkbar. Privatsphärengerechtes Smart Metering muss also auch in Anwesenheit eines Angreifers privatsphärengerecht sein. Der Privatsphärenschutz stellt somit ein wichtiges Schutzziel dar.

Um bewerten zu können inwiefern dieses Schutzziel erreicht wurde, ist es nötig eine genaue Vorstellung der Fähigkeiten eines potentiellen Angreifers zu haben. Diese Fähigkeiten werden mittels eines *Angreifermodells* spezifiziert. Der Großteil der in Kapitel 3 behandelten verwandten Arbeiten zum privatsphärengerechten Smart Metering erwähnt gar kein Angreifermodell oder wählt ein schwaches Angreifermodell, wie den sogenannten *honest-but-curious*-Angreifer (vgl. semi-honest in [59]). Dabei handelt es sich um einen Angreifer, der sich absolut protokollkonform verhält und lediglich aus den dabei erzielbaren Daten seine Schlüsse zieht. Im Falle eines Smart Meterings würde dies für einen Angreifer folgendes bedeuten:

- Der Angreifer muss am Smart Metering als ordentlicher Teilnehmer partizipieren. Er muss also entweder die Rolle eines intelligenter Stromzählers oder die Rolle des Messdienstleisters einnehmen.

- Der Angreifer kann das Smart Metering nicht außerhalb der vorgesehenen Freiräume beeinflussen. Dies beinhaltet auch das Einhalten von Vorschriften zur *zufälligen Wahl* von Werten oder Kommunikationspartnern, beispiels-

weise anderen intelligenten Stromzählern. Eine gezielte Wahl, auch wenn sie unerkannt stattfinden könnte, wird dadurch ausgeschlossen.

- Der Angreifer kann lediglich mittels der ohnehin empfangenen und selbst generierten Daten versuchen sein Angriffsziel zu erreichen.

Zusätzlich zum schwachen Angreifermodell wird teilweise die Rolle des Messdienstleisters mit Aufgaben betraut, die für die Garantie der Privatsphäre höchst sensibel sind. Ein Beispiel hierfür ist die Auswahl eines intelligenten Stromzählers aus einer Menge von intelligenten Stromzählern. Schreibt das Protokoll vor, dass diese Wahl durch den Messdienstleister *zufällig* durchgeführt wird, so wird im honest-but-curious-Angreifermodell davon ausgegangen, dass der Messdienstleister keinen Einfluss auf diese Wahl hat. Selbst wenn eine gezielte Wahl wertvolle Informationen für den Messdienstleister offen legen würde und nicht bemerkt werden würde, wird erwartet dass der Messdienstleister diese Möglichkeit nicht nutzt. Dies impliziert eine gewisse Vertrauensbeziehung zu der Partei, vor der die Privatsphäre eigentlich geschützt werden soll. Wäre der Messdienstleister vertrauenswürdig, so könnten intelligente Stromzähler ihre Daten direkt und lediglich verschlüsselt übertragen.

Der Grund für die Wahl des eher schwachen honest-but-curious Modells liegt sicherlich an den speziellen Gegebenheiten des Smart Meterings. So wird häufig angenommen, dass es sich bei intelligenten Stromzählern um Geräte mit erhöhten Sicherheitsanforderungen handelt, die durch ihre Konstruktion folgende Eigenschaften aufweisen:

Identitätsnachweis: Ein intelligenter Stromzähler ist mit einer eindeutigen Identität ausgestattet, die eine Identifikation durch den Messdienstleister und andere intelligente Stromzähler zulässt. Dies kann beispielsweise eine Seriennummer des Herstellers sein.

Zertifikatsnachweis: Ein intelligenter Stromzähler ist vom Hersteller als solcher zertifiziert und kann dies auch gegenüber dem Messdienstleister und anderen intelligenten Stromzählern über die Kommunikationsschnittstelle nachweisen. Dieser Nachweis zertifiziert die Konstruktion des intelligenten Stromzählers nach gültigen technischen Richtlinien und erstreckt sich auch auf den Identitätsnachweis. Damit konstituiert der Zertifikatsnachweis eine *Authentifizierung* der Identität und der Echtheit des intelligenten Stromzählers.

Manipulationssicherheit: Ein intelligenter Stromzähler lässt sich nicht in seinen grundlegenden Eigenschaften manipulieren. Der Hersteller hat entsprechende Vorkehrungen getroffen, so dass ein Versuch der Manipulation – beispielsweise das Öffnen des Gehäuses – zur Unbrauchbarkeit des Zählers selbst und auch aller enthaltenen Daten führt. Im Speziellen lässt sich also die enthaltene Software nicht ändern und auch enthaltenes kryptographisches Material ist weder manipulierbar noch auslesbar. Die Manipulationssicherheit wird auch dadurch unterstützt, dass intelligente Stromzähler üblicherweise nicht öffentlich zugänglich angebracht sind sondern sich in abgeschlossenen Kellerräumen befinden.

Diese Eigenschaften können als Motivation für das honest-but-curious Angreifermodell gesehen werden. Aus ihnen folgt direkt die Möglichkeit mittels der Authentifizierung eine verschlüsselte Verbindung zwischen beliebigen intelligenten Stromzählern und dem Messdienstleister herzustellen. Dies verhindert das aktive Abhören von Informationen, die nicht für den eigenen Zähler bestimmt sind. Gleichermaßen verhindert die Manipulationssicherheit einen Eingriff in die Software der intelligenten Stromzähler und damit auch weitgehend einen Eingriff in die Abläufe des Smart Meterings.

Bei einer näheren Betrachtung des Smart Metering Szenarios bleiben einem Angreifer jedoch selbst mit diesen Annahmen Angriffsmöglichkeiten, die über die des honest-but-curious Angreifers hinausgehen:

Identitätserzeugung: Ein Angreifer hat die Möglichkeit einen intelligenten Stromzähler auf dem freien Markt selbst zu beschaffen. Sofern keine Maßnahmen zur Zugangskontrolle ergriffen werden, eröffnet dies die Möglichkeit, dass ein Angreifer an einem Smart Metering teilnimmt, obwohl er nicht ordentlicher Teilnehmer ist (vgl. Sybil-Attacke in Abschnitt 2.4.2). Durch die Beschaffung der intelligenten Stromzähler ist dies jedoch mit finanziellem Aufwand verbunden.

Kommunikationsselektion: Steht ein intelligenter Stromzähler unter Kontrolle eines Angreifers, so kann der Angreifer den Datenverkehr zu und vom Zähler selektiv verhindern. Beispielsweise könnte eine Firewall-Regel im Router dafür sorgen, dass ein intelligenter Stromzähler lediglich mit einer ausgewählten Menge an anderen intelligenten Stromzählern kommunizieren kann.

Organisationsmanipulation: Der Messdienstleister ist in diesem Angreifermodell nicht den Eigenschaften eines intelligenten Stromzählers unterbunden und dementsprechend frei in seiner Angriffstechnik. Er kann insbesondere bei der

Organisation des Smart Meterings frei Entscheidungen treffen und sich dabei auch nicht protokollkonform verhalten.

Es zeigt sich also, dass allein durch die Kommunikationsselektion ein größerer Einfluss des Angreifers auf den Datenverkehr gegeben ist, als es das honest-but-curious Modell vorsieht. Bezieht man noch Organisationsmanipulation und Identitätserzeugung mit ein, so muss man zu dem Schluss kommen, dass das honest-but-curious Modell die Realität nicht ausreichend abbildet.

Zusätzlich ist auch die Annahme der Manipulationssicherheit nur sicher in Relation zur vom Angreifer aufgebrachten Zeit und zum Aufwand. Es existieren zahlreiche Berichte über Sicherheitslücken in aktuell ausgebrachten intelligenten Stromzählern (beispielsweise in [18, 32]). Diese legen den Schluss nahe, dass die Annahme der Manipulationssicherheit nicht der Realität entspricht.

Aus diesen Gründen wird in dieser Arbeit nicht das honest-but-curious Angreifermodell verwendet. Auch wird der Messdienstleister explizit als potentieller Angreifer betrachtet. Als Angreifermodell wird ein Modell nach Dolev-Yao [36] verwendet.

Der Angreifer verfügt über einen beschränkten Vorrat an Ressourcen wie Rechenzeit, Kommunikationsrate, IP-Adressen und finanzielle Mittel. Aus der Beschränkung der verfügbaren Rechenzeit resultiert auch die Sicherheit aktueller kryptographischer Verfahren. Es wird angenommen, dass Verschlüsselungsverfahren wie AES, Verfahren zur digitalen Signatur wie ECDSA, sowie auch kryptographische Hashfunktionen wie die SHA-Gruppe bei korrektem Einsatz nicht angreifbar sind. In diesem Angreifermodell kann ein Angreifer beliebige Nachrichten abfangen, lesen und verändern. Korrekt eingesetzte kryptographische Verfahren können dies verhindern.

Als Besonderheit des Smart Metering Szenarios wird angenommen, dass für intelligente Stromzähler der Identitätsnachweis und der Zertifikatsnachweis verfügbar sind. Da diese Nachweise mittels kryptographischer Verfahren erbracht werden können, wird angenommen, dass sie durch die Beschränkung der verfügbaren Rechenzeit geschützt sind. Sie können vom Angreifer nicht manipuliert werden. Dies führt zum Schluss, dass eine gültige Identität nur durch den Besitz oder die Korrumpierung eines intelligenten Zählers für den Angreifer verfügbar ist.

Mittels Identitätsnachweis und Zertifikatsnachweis kann jederzeit eine kryptographisch gesicherte Verbindung zwischen intelligenten Stromzählern aufgebaut und damit Integrität, Vertraulichkeit und Authentizität gewährleistet werden. Auch

wird angenommen, dass eine entsprechend gesicherte Verbindung mit dem Messdienstleister aufgebaut werden kann (beispielsweise mittels einer PKI). Daher wird in dieser Arbeit davon ausgegangen, dass der Angreifer lediglich Nachrichten erkennen und abfangen kann. Der Inhalt bleibt geheim und vor Manipulation geschützt. Wird jedoch der Angreifer durch eine an der Kommunikation teilnehmende Partei repräsentiert, so liegt der Inhalt dieser Kommunikation für den Angreifer offen.

Durch den Wegfall der Manipulationssicherheit kann der Angreifer auch regulär teilnehmende intelligente Stromzähler korrumpieren. Ebenso kann die Software dieser Zähler manipuliert werden. Es wird aber angenommen, dass eine Korrumpierung nur mit physikalischem Zugriff durchgeführt werden kann. Damit verfügt ein Angreifer, der im Besitz eines regulär teilnehmenden intelligenten Stromzählers ist, über vollständige Kontrolle.

Zusammengefasst hat ein Angreifer des in dieser Arbeit verwendeten Angreifermodells folgende Fähigkeiten:

- Er kann mehrere intelligente Stromzähler besitzen. Dies ist jedoch mit finanziellem Aufwand verbunden. Durch die Annahme beschränkter finanzieller Mittel, ist die Anzahl der intelligenten Stromzähler limitiert.
- Er kann intelligente Stromzähler bestimmter Haushalte korrumpieren und damit vollständige Kontrolle über diese übernehmen. Dies ist jedoch mit erheblichem Aufwand verbunden, da angenommen wird, dass hierfür Zugang zu verschlossenen Räumen, technische Kenntnis und Zeit nötig sind.
- Das Verhalten eines korrumpierten oder im Besitz des Angreifers befindlichen intelligenten Stromzählers ist vom Angreifer in allen Aspekten beeinflussbar.
- Ein Angreifer kann einzelne Nachrichten abfangen. Dies ist mit erheblichem Aufwand verbunden, da hierfür entweder Zugriff auf die Kommunikationsinfrastruktur des Haushalts, des Internet Service Providers oder des Messdienstleisters benötigt wird.
- Ist der Angreifer Messdienstleister oder hat er diesen korrumpiert, so kann er zusätzlich den Verlauf des Smart Meterings beeinflussen. Dies erlaubt dem Messdienstleister explizit gegen Vorschriften, wie zufällige Wahl von Variablen, zu verstoßen.

Wann ein Angriff erfolgreich durchgeführt wurde hängt von der Verwertung der dabei gewonnenen Daten ab. Ist das Ziel des Angreifers beispielsweise Wissen

über die Anwesenheit einer beliebigen Person im Haushalt zu einem bestimmten Zeitpunkt, so genügt möglicherweise ein einzelner Messwert um dieses Ziel zu erreichen. Soll jedoch das Vorhandensein der im Beispiel genannten Klimaanlage ermittelt werden, so benötigt der Angreifer einen zeitlichen Verlauf des Energieverbrauchs. Für einen erfolgreichen Angriff wären dann mehrere, aufeinanderfolgende Messwerte notwendig.

2.2 Privatsphäre und Privatsphärenschutz

Die Privatsphäre im Sinne moderner Demokratien stellt einen Raum dar, in dem ein Mensch sein Recht auf freie Entfaltung der Persönlichkeit ohne Beeinflussung von außen wahrnehmen kann. Dies erfordert insbesondere, dass der Raum der Privatsphäre nicht durch andere Menschen einsehbar ist. In Deutschland ist das Recht auf Privatsphäre aus dem Grundgesetz abgeleitet. Die maßgeblichen Artikel sind die allgemeinen Persönlichkeitsrechte (Artikel 1 und 2), sowie die Unverletzlichkeit der Wohnung (Artikel 13). Mit Artikel 10 des Grundgesetzes ist das Brief-, Post- und Fernmeldegeheimnis ebenfalls als unverletzlich garantiert. Die Privatsphäre wird dadurch auch auf die Kommunikation ausgedehnt. Mit dem Recht auf informationelle Selbstbestimmung, einer Ausprägung des allgemeinen Persönlichkeitsrechts, wird die Privatsphäre ebenfalls gestärkt. Das Recht auf informationelle Selbstbestimmung wurde 1983 vom Bundesverfassungsgericht als Grundrecht anerkannt und räumt dem Einzelnen die Befugnis ein, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ [95].

Im Rahmen dieser Arbeit wird privatsphärengerechtes Smart Metering betrachtet. Hierfür ist es nötig unterscheiden zu können, ob ein Smart Metering privatsphärengerecht durchgeführt wird oder nicht. Der Begriff der Privatsphäre ist durch die Gesetzgebung nicht scharf definiert. Da der Umfang der Privatsphäre vom einzelnen Individuum abhängt, ist dies auch nicht möglich. Ob ein Smart Metering privatsphärengerecht durchgeführt wird oder nicht, hängt letztlich vom Individuum ab, dessen Privatsphären betroffen ist. Im Kontext dieser Arbeit wird dennoch eine einheitliche Definition vorgenommen, um eine Bewertung eines Verfahrens zum Smart Metering vornehmen zu können. Da Smart Metering auf der Basis von Haushalten durchgeführt wird, wird in dieser Arbeit von der Privatsphäre der Menschen abstrahiert und die Privatsphäre von Haushalten betrachtet.

Privatsphärengerechtes Smart Metering wird in dieser Arbeit mittels Mechanismen realisiert, die auf der Datenaggregation über mehrere Haushalte hinweg

basieren. Dieser Ansatz ist in der Literatur weit verbreitet (siehe Abschnitte 3.5.2 und 3.5.3 oder Erkin et al. [47] für eine weitere Übersicht). Der Ansatz basiert auf der Idee, dass ein Aggregat der Daten einzelner Haushalte, wie beispielsweise die Summe der einzelnen Energieverbräuche, das eigentliche Ziel des Smart Meterings darstellt und daher die Erhebung dieses Aggregats ausreicht. Eine Erhebung einzelner Messwerte von Haushalten und damit von personenbezogenen Daten, wird nicht durchgeführt. Durch diesen Verzicht entspricht der Ansatz dem Konzept der Datensparsamkeit und Datenvermeidung.

Die Definition, wann ein Smart Metering privatsphärengerecht durchgeführt wird, wird in zwei Kategorien aufgeteilt. Der *Privatsphärenschutz des Einzelnen* betrachtet einen einzelnen Haushalt. Der *Privatsphärenschutz einer Gruppe* behandelt eine Gruppe von Haushalten, über die in ein Aggregat gebildet wurde.

In dieser Arbeit wird ein Smart Metering bezüglich des Privatsphärenschutzes des Einzelnen genau dann als privatsphärengerecht betrachtet, wenn folgende Kriterien erfüllt sind:

- Die Messwerte eines Haushaltes können nur in einer aggregierten Form ermittelt werden. Das bedeutet, dass niemand (außer dem Haushalt selbst) einen Messwert des Haushaltes kennt. Lediglich Aggregate, die Messwerte des Haushaltes enthalten, dürfen anderen bekannt sein. Es folgt, dass Aggregate über Messwerte von mindestens zwei Haushalten gebildet werden müssen.

- Ein Aggregat darf (mit technischen Mitteln) keine Rückschlüsse auf Verhältnisse zwischen den eingeflossenen Messwerten erlauben. Als Beispiel sei angenommen, dass durch Aufsummieren zweier Messwerte ein Aggregat mit dem Wert 200 entstanden ist. Es muss gewährleistet sein, dass alle Messwerte a, b mit $a + b = 200$ aus technischer Sicht gleich wahrscheinlich sind. Ob nun $a = 0$ und $b = 200$ oder $a = 100$ und $b = 100$ in das Aggregat eingeflossen ist, darf nicht am Aggregat selbst erkannt werden können.

Diese Kriterien gewährleisten insbesondere, dass kein Zeitpunkt existiert, für den der Messwert eines Haushalts ermittelt werden kann. Dies schließt die Berechnung eines Profils des Haushalts, also den zeitlichen Verlauf von Messwerten, aus.

Betrachtet man lediglich den Privatsphärenschutz des Einzelnen, so würde beispielsweise eine Datenaggregation über zwei Haushalte hinweg ausreichen um ein privatsphärengerechtes Smart Metering zu erhalten. Davon kann jedoch im Allgemeinen nicht ausgegangen werden. Obwohl, nach der Datenaggregation, die

Messwerte der einzelnen Haushalte nicht bestimmt werden können, liegt mittels deren Aggregat möglicherweise eine Verletzung der Privatsphäre vor. Dies ist insbesondere dann der Fall, wenn die Datenaggregation immer über dieselben Haushalte hinweg stattfindet und somit ein Profil der Gruppe erstellt werden kann. Daher ist der Privatsphärenschutz einer Gruppe separat zu betrachten.

Die Frage nach dem Privatsphärenschutz einer Gruppe ist nicht spezifisch für diese Arbeit sondern stellt sich in allen Arbeiten, die mittels Aggregation Privatsphäre schützen. Eine allgemeingültige Definition, wann ein Aggregat von Messwerten den Privatsphärenschutz einer Gruppe gewährleistet oder nicht, ist aufgrund der individuellen Auffassung von Privatsphäre auch nicht möglich. Bei einer Einschätzung spielen, neben den technischen Variablen wie Gruppengröße und Varianz der Messwerte, auch externe Informationsquellen und gesellschaftliche Aspekte eine Rolle (siehe hierfür beispielsweise Jawurek et al. [70]). Die Beantwortung dieser Fragestellung steht nicht im Fokus dieser technischen Arbeit. Um dennoch eine Einschätzung des Privatsphärenschutzes einer Gruppe vornehmen zu können, werden zwei Kriterien betrachtet:

Gruppengröße: Mit der Anzahl der Haushalte, die in einer Gruppe enthalten sind, steigt auch der Privatsphärenschutz. Dies folgt einerseits aus der Tatsache, dass Informationen die aus dem Aggregat geschlossen werden können, wie beispielsweise der Besitz einer Klimaanlage, nicht auf einen einzelnen Haushalt zurückführbar sind. Andererseits wird die Erkennung dieser Informationen aus dem Aggregat deutlich erschwert. In Arbeiten zur Erkennung von Haushaltsgeräte am Profil eines einzelnen Haushalts (siehe beispielsweise Kolter et al. [79] oder Weiss et al. [137]) wird diese Aufgabe bereits durch die Verwendung mehrerer Haushaltsgeräte gleichzeitig deutlich erschwert. Durch eine Aggregation über mehrere Haushalte wird die Komplexität der Erkennung also weiter erhöht.

Länge des Messintervalls: Mit einem längeren Messintervall, also selteneren Messungen, steigt der Privatsphärenschutz. Je seltener eine Messung durchgeführt wird, desto weniger detailliert kann ein Profil der Gruppe ausfallen. In einer Arbeit von Molina-Markham et al. [96] wird gezeigt, dass eine Verlängerung des Messintervalls signifikante Einbußen in der Genauigkeit des dort beschriebenen Verfahrens zur Erkennung von Haushaltsgeräten verursacht.

In den Verfahren, die in dieser Arbeit vorgestellt werden, wird der Privatsphärenschutz des Einzelnen, wie er in diesem Abschnitt definiert ist, jederzeit gewährt. Der Privatsphärenschutz einer Gruppe wird entweder über eine konfigurierbare

Gruppengröße (Kapitel 5 und 7) oder ein seltenes Auftreten der gleichen Gruppenkonfiguration (Kapitel 6) adressiert.

2.3 Privatsphärengerechte Datenaggregation – SMART

Das in dieser Arbeit vorgestellte SMART-ER Verfahren basiert in seinen Grundkonzepten auf den Ideen des SMART Verfahrens [66, 67]. Diese werden im Folgenden vorgestellt. Eine Analyse von SMART wird in Abschnitt 5.3.1 durchgeführt.

SMART (Slice-Mix-Aggregate) ist ein Verfahren zur privatsphärengerechten Datenaggregation in drahtlosen Sensornetzen. Ziel des Verfahrens ist eine korrekte Erfassung von aggregierten Daten an einer Datensenke, ohne dass ein einzelnes Datum seinem Ursprung zugeordnet werden kann. Es stellt damit eine Form der sicheren Mehrparteienberechnung dar (siehe beispielsweise [25, 138]. Dabei fallen diese Daten verteilt auf Sensorknoten im Netz an. Im Folgenden werden diese Daten *Messwerte* genannt, da sie von den Sensorknoten mittels der Sensorik gemessen werden. Auch die Datensenke ist Teilnehmer dieses drahtlosen Sensornetzes.

2.3.1 Konzept

In diesem Abschnitt wird das Konzept von SMART vorgestellt. Das Verfahren besteht aus drei Schritten, die in Abbildung 2.1 grafisch veranschaulicht sind:

- **S**lice: Aufspalten von Messwerten in sogenannte *Fragmente*
- **M**ix: Mischen von Fragmenten zwischen Knoten
- **A**gg**r**ega**t**e: Aggregieren von Fragmenten

In ❶ ist zu sehen wie der Messwert auf jedem Knoten in Fragmente aufgeteilt wird. Beispielsweise wird der Messwert von Knoten A (roter Kasten) in die Fragmente $\{A1, A2, A3\}$ aufgespalten. Diese werden anschließend über zufällig ausgewählte, andere teilnehmende Knoten verteilt[1]. Eines dieser Fragmente ($A1$) wird jedoch auf Knoten A zurückbehalten, also nicht an einen anderen Knoten weitergegeben. In ❷ werden die auf den Knoten vorhandenen und empfangenen

[1] In Sensornetzen fließt in die Wahl der Empfänger der Standort der Knoten mit ein. So könnte beispielsweise nur aus den Knoten zufällig ausgewählt werden, die sich in Funkreichweite des Senders befinden.

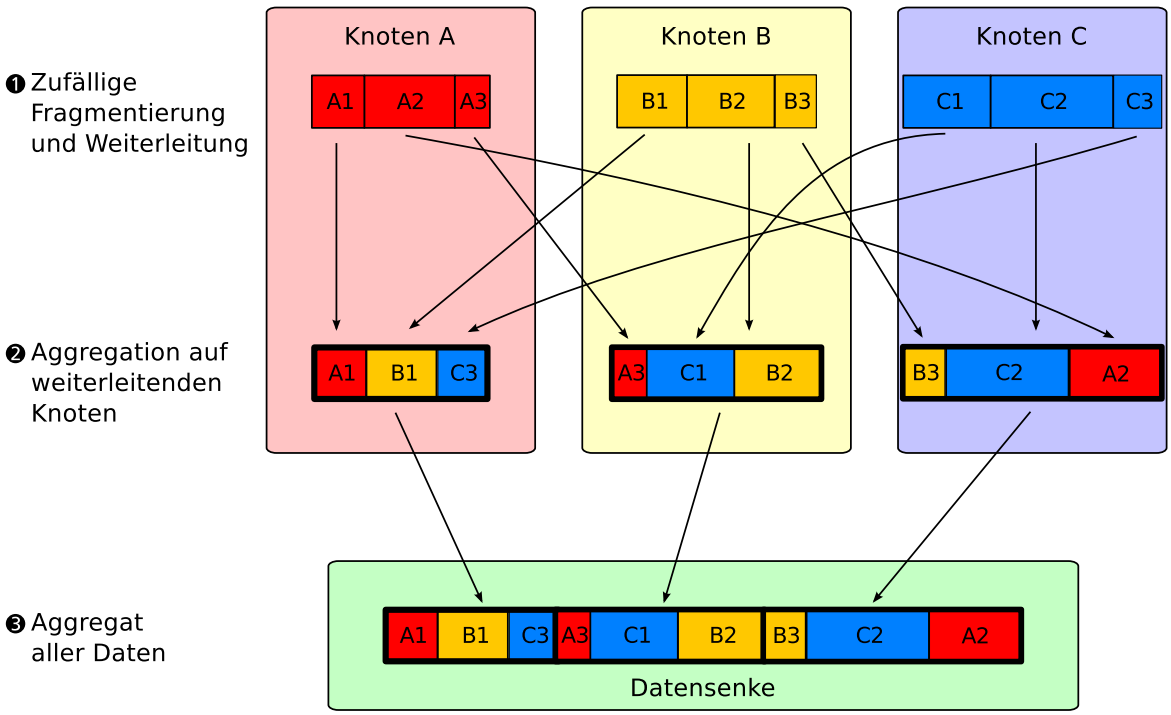


Abbildung 2.1: *Grundkonzept des SMART Verfahrens.*

Fragmente zu neuen Fragmenten aggregiert (dargestellt durch den dick gezeichneten schwarzen Rahmen). Die Zusammensetzung innerhalb dieser Rahmen ist nur dem aggregierenden Knoten bekannt. Eine Umkehrung dieses Schritts darf ohne dieses Wissen nicht möglich sein. Diese Aggregate aus Einzelfragmenten werden an die Datensenke gesendet. Abschließend werden in ❸ die von der Datensenke empfangenen Fragmente abermals aggregiert, um einen Gesamtwert zu erhalten.

Wie in der Grafik deutlich zu erkennen ist, besteht das abschließende Aggregat in ❸ aus allen Teilfragmenten, die in ❶ gebildet wurden. Das Aggregat entspricht also dem Aggregat der Messwerte aller drei Knoten. Aus den bereits teilweise aggregierten Fragmenten, die im Übergang von ❷ nach ❸ übertragen wurden, können jedoch die ursprünglichen Messwerte nicht wiederhergestellt werden.

Der Ablauf des Verfahrens aus der Sicht eines einzelnen Knotens gliedert sich dabei in folgende Phasen. Diese sind in Abbildung 2.2 grafisch dargestellt.

(1) *Messen* des Messwertes und Fragmentierung

(2) *Austausch* von Fragmenten mit anderen Knoten

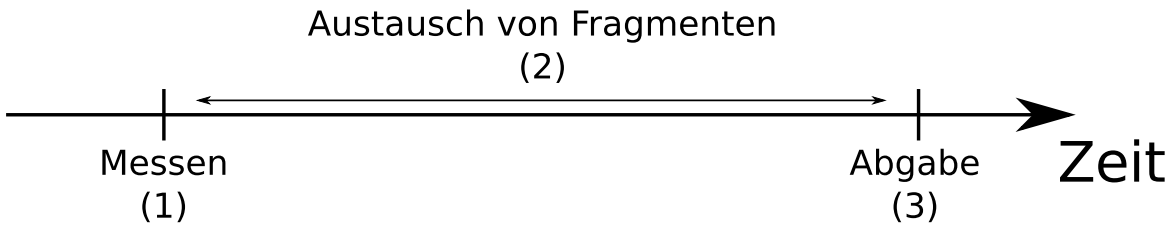


Abbildung 2.2: *Zeitlicher Ablauf des SMART Verfahrens.*

(3) *Abgabe* der aggregierten Daten bei der Datensenke

Für die Fragmentierung wird in der Veröffentlichung zum SMART Verfahren [66] zwischen zwei Fällen unterschieden: Fragmente mit ausschließlich positiven Werten oder zusätzlich auch negative Werte. Im Falle von ausschließlich positiven Werten wird in [66] folgender Algorithmus zum Fragmentieren vorgeschlagen: Sei p_i der zu aggregierende Messwert von Knoten i und J die Gesamtzahl der Knoten. Dann muss gelten $p_i = \sum_{j=1}^{J} p_{ij}$ wobei jedes p_{ij} ein Fragment darstellt, das Knoten i an Knoten j übermittelt. Um die verschiedenen p_{ij} zu ermitteln wird in [66] die in Gleichung (2.1) gelistete Berechnungsvorschrift empfohlen. Die Funktion rand() zieht hierbei gleichverteilt eine Zufallszahl aus dem Intervall $[0,1]$.

$$\begin{aligned} p_{i1} &= \text{rand}() \times p_i \\ p_{ij} &= \text{rand}() \times (p_i - \sum_{k=1}^{j-1} p_{ik}) \\ p_{iJ} &= p_i - \sum_{k=1}^{J-1} p_{ik} \end{aligned} \tag{2.1}$$

Anschaulich bedeutet dies, dass das erste Fragment einen zufälligen Teil von p_i darstellt. Jedes weitere Fragment stellt einen zufälligen Teil von p_i abzüglich der bereits erzeugten Fragmente dar. Das letzte Fragment entspricht dem Rest von p_i abzüglich der bereits erzeugten Fragmente.

Um auch negative Fragmente zu realisieren, wird zuerst eine vorher bestimmte Anzahl von Fragmenten nach selbem Muster generiert. Deren Summe sei X. Dann werden diese Fragmente negiert und der Wert p_i um deren Summe erhöht, also $p_i = p_i + X$. Die restlichen, positiven Fragmente werden dann nach schon bekanntem Muster und mit dem neuen p_i erzeugt.

2.4 Peer-to-peer Systeme

Ein *peer-to-peer System* ist ein selbstorganisierendes Netz aus einer Menge von gleichberechtigten Teilnehmern. Diese werden *Peers* genannt. Die Funktionalität des peer-to-peer Systems wird dabei von allen Peers gemeinsam erbracht. Jeder Peer nutzt die Dienste, die andere Peers anbieten und bietet auch selbst diese Dienste an. Im Zuge dessen werden die Ressourcen der Peers, wie beispielsweise Rechen- und Speicherkapazitäten, gleichermaßen genutzt. Eine Übersicht über peer-to-peer Systeme bieten beispielsweise Steinmetz und Wehrle [125].

Zur Organisation von peer-to-peer Systemen wird in der Regel ein *Overlaynetz* verwendet. Ein Overlaynetz stellt eine Abstraktion über dem eigentlichen, verwendeten Kommunikationsnetz dar und hat eine eigene Topologie. Ein Beispiel für eine solche Topologie ist ein Ring. Diese logische Topologie ist unabhängig von der Struktur des eigentlichen Kommunikationsnetzes. Peers sind in dieser logischen Topologie angeordnet und haben, im Fall eines Rings, einen Vorgänger und Nachfolger. Diese Einordnung ist in der Regel unabhängig vom eigentlichen Kommunikationsnetz.

Bei peer-to-peer Systemen kann zwischen strukturierten und unstrukturierten peer-to-peer Systemen unterschieden werden.

Unstrukturierte peer-to-peer Systeme, wie beispielsweise Gnutella [114], verwenden eine lose, gewachsene Topologie. Wird nach einem Datum im peer-to-peer System gesucht, so wird eine Anfrage an alle Nachbarn gesendet. Diese wiederholen den Vorgang und fluten so die Anfrage durch das peer-to-peer System. Der Aufwand für eine Suchanfrage ist daher sehr groß.

Strukturierte peer-to-peer Systeme, wie beispielsweise Kademlia [90], verwenden eine strenge Ordnung der Topologie um Anfragen effizient zum richtigen Empfänger zu leiten. Jeder Peer hat eine sogenannte Overlay-ID, die einen Standort in der Topologie darstellt. Diese Struktur ermöglicht eine gezielte und effiziente Suche nach anderen Peers, die dann zur effizienten Realisierung von Anfragen genutzt werden kann.

2.4.1 Key-based Routing

Ein wichtiger Dienst eines strukturierten peer-to-peer Systems stellt das *Key-based Routing (KBR)* [31] dar. Jedem Peer wird neben seiner Overlay-ID noch ein Bereich der Overlay-IDs zugewiesen, für den er zuständig ist. Bei einer Ringtopologie könnte dies beispielsweise der Bereich bis zum nachfolgenden Peer sein. Zusätzlich

verwaltet jeder Peer eine sogenannte Routingtabelle, in der er Routinginformationen zu seinen Overlay-Nachbarn speichert. Ein Datum oder ein Dienst wird im peer-to-peer System mittels einer Overlay-ID adressiert. Soll nun ein Datum abgerufen oder ein Dienst in Anspruch genommen werden, so kann die Nachricht immer an einen Peer weitergesendet werden, dessen Overlay-ID in der Overlay-Topologie näher an der Ziel-Overlay-ID liegt. So erreicht die Nachricht sukzessive ihr Ziel.

2.4.2 Der Sybil-Angriff

In peer-to-peer Systemen basieren viele Mechanismen auf der Tatsache, dass eine große Anzahl an Teilnehmern zur Verfügung steht. Beispielsweise kann in einem peer-to-peer System das Speichern von Daten so ausgestaltet werden, dass immer mehrere Kopien der Daten im Netz, also bei unterschiedlichen Teilnehmern gespeichert sind. Fällt nun einer der Teilnehmer, die ein bestimmtes Datum gespeichert haben, aus, so existieren weiterhin Kopien im peer-to-peer Netz. Auch können absichtliche Veränderungen des gespeicherten Datums durch einen Angreifer entdeckt werden, wenn die Kopien der Teilnehmer nicht mehr identisch sind.

Mit dem Sybil-Angriff [37] wird ein Möglichkeit zur Umgehung solcher Sicherheitsmechanismen beschrieben. Existiert im peer-to-peer Netz keine Möglichkeit zur Überprüfung der Identität der anderen Teilnehmer, so kann ein Angreifer gefälschte Identitäten erzeugen. Mit Hilfe dieser gefälschten Identitäten kann dann dem peer-to-peer Netz die Wirksamkeit von Sicherheitsmechanismen vorgetäuscht werden, obwohl diese nicht gegeben ist. Im obigen Beispiel der Datenspeicherung könnte ein Angreifer die falschen Identitäten so in Position bringen, dass sie alle der Teilnehmer darstellen, die ein bestimmtes Datum speichern. Der Angreifer hat nun Kontrolle über dieses Datum und kann es verändern, ohne dass dies von anderen Teilnehmern entdeckt werden kann.

In [37] wurde gezeigt, dass ein Sybil-Angriff nur durch eine Überprüfung der Identitäten vermeidbar ist. Um aber eine Identität überprüfen zu können, muss diese durch eine vertrauenswürdige Zertifizierungsstelle bestätigt werden.

2.5 Kryptologische Verfahren

In dieser Arbeit werden kryptologische Verfahren verwendet um vertrauliche Kommunikation oder unbeeinflussbare Bestimmungen von Overlay-IDs durchzuführen. Daher wird hier ein kurzer Überblick über kryptologische Verfahren gegeben. Eine ausführliche Übersicht bietet beispielsweise Schneier et al. [120].

2.5.1 Kryptologische Hashfunktionen

Hashfunktionen werden in der Kryptologie zu vielen Zwecken verwendet. Ein Beispiel ist die Integritätsprüfung. Eine Hashfunktion bildet ein Datum beliebiger Länge auf einen Hashwert ab. Damit sich die Hashfunktion für kryptologische Anwendungen eignet muss sie gewährleisten, dass sie nicht mit vertretbarem Aufwand umgekehrt werden kann. Ausgehend von einem Hashwert darf das ursprüngliche Datum nicht mit vertretbarem Aufwand bestimmt werden können. Eine Hashfunktion stellt also eine Einwegfunktion dar. Es darf auch nicht mit vertretbarem Aufwand möglich sein zu einem Hashwert y ein beliebiges Datum x zu finden, so dass $h(x) = y$ gilt. Des Weiteren muss es praktisch unmöglich sein zu einem gegebenen Datum x ein zweites Datum x' zu finden, so dass $h(x) = h(x')$ gilt. Auch muss es praktisch unmöglich sein zwei Daten x, y mit identischen Hashwerten $h(x) = h(y)$ zu finden.

Eine häufig verwendete Hashfunktion ist SHA-1 [39], die für Daten beliebiger Länge Hashwerte der Länge 160 Bit generiert. Mit SHA-3 [102] wurde kürzlich die neueste Generation der SHA Familie von Hashfunktionen standardisiert.

2.5.2 Symmetrische und asymmetrische Verschlüsselungsverfahren

Verschlüsselungsverfahren überführen einen Klartext mittels eines Schlüssels in ein sogenanntes *Chiffrat*. Sie verschlüsseln den Klartext. Das Chiffrat kann nicht ohne Kenntnis eines passenden Schlüssels wieder in den Klartext überführt werden (entschlüsseln).

Man unterscheidet zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Bei symmetrischen Verschlüsselungsverfahren wird derselbe Schlüssel zum Ver- und Entschlüsseln verwendet. Beispiele für symmetrische Verschlüsselungsverfahren sind AES und DES. Asymmetrische Verschlüsselungsverfahren verwenden unterschiedliche Schlüssel zum Ver- und Entschlüsseln. Der Schlüssel zum Verschlüsseln wird *öffentlicher Schlüssel* oder *public Key* genannt.

Er wird für gewöhnlich öffentlich zugänglich gemacht. Der Schlüssel zum Entschlüsseln wird dementsprechend *privater Schlüssel* oder *private Key* genannt und vom Eigentümer geheim gehalten.

2.5.3 Homomorphe Verschlüsselungsverfahren

Homomorphe Verschlüsselungsverfahren verschlüsseln Daten auf eine Weise, die Berechnungen auf den verschlüsselten Daten zulässt, ohne sie vorher zu entschlüsseln. Werden beispielsweise zwei Zahlen verschlüsselt, so können die beiden Chiffrate von einem Dritten, ohne Kenntnis der Schlüssel, addiert werden. Das Resultat kann danach entschlüsselt werden und entspricht der Addition der Klartexte.

Homomorphe Verschlüsselungsverfahren werden in zwei Kategorien eingeteilt: partiell homomorphe Verschlüsselungsverfahren und vollhomomorphe Verschlüsselungsverfahren. Ein partiell homomorphes Verschlüsselungsverfahren erlaubt Berechnungen auf den verschlüsselten Daten mittels einer Operation, beispielsweise der Addition oder der Multiplikation. Ein Beispiel hierfür ist das ElGamal-Verschlüsselungssystem [43], das eine Multiplikation erlaubt. Ein vollhomomorphes Verschlüsselungsverfahren erlaubt sowohl Addition als auch Multiplikation. Ein Beispiel ist das von Gentry [58] vorgestellte Verfahren.

Es existieren auch Verschlüsselungsverfahren, die nicht nur homomorph in den Chiffraten, sondern auch in den Schlüsseln sind. Wenn ein Wert v mit dem Schlüssel a verschlüsselt wurde, dann resultiert das Chiffrat v_a. Wenn ein anderer Wert w mit dem Schlüssel b verschlüsselt wurde (w_b), so kann die Summe $v_a + w_b = x_{a+b}$ mit dem Schlüssel $a + b$ entschlüsselt werden.

2.5.4 Commitment Verfahren

Commitment Verfahren [14] sind ein kryptologisches Werkzeug, das die unwiderrufliche Wahl eines Wertes ermöglicht, ohne diesen zu verraten. Einigen sich zwei Parteien, A und B, auf ein Commitment Verfahren, so kann Partei A ein Commitment $c = Commit(x, r)$ erstellen, das für Partei B zunächst keinen Informationsgehalt hat. Das Commitment c kann durch A geöffnet werden, indem A die Werte x und r offenlegt. Führt B die Operation Open(c, x, r) durch, so ist diese erfolgreich.

Durch die Berechnung von c ist außerdem gewährleistet, dass für die gegebenen Werte c, x und r die Berechnung eines $x' \neq x$ und r', so dass Open(c, x', r')

erfolgreich ist, mit sehr großem Rechenaufwand verbunden ist. Hat sich A auf ein Commitment c gegenüber B festgelegt, indem A dieses beispielsweise an B übertragen hat, so hat sich A auch auf die Werte x und r festgelegt, allerdings ohne diese gegenüber B zu offenbaren.

Kapitel 3

Stand der Forschung

Das folgende Kapitel widmet sich dem Stand de Forschung zum privatsphärengerechten Smart Metering. Zunächst wird in Abschnitt 3.1 der Bedarf für eine privatsphärengerechte Variante von Smart Metering mittels Beispielen zum Stand der Forschung zur Analyse von Energieverbrauchsdaten begründet.

Es folgt in Abschnitt 3.2 eine Kategorisierung von Arbeiten zum privatsphärengerechten Smart Metering. Die Kategorisierung wird anhand der Zielsetzung des Smart Meterings vorgenommen. Dieser Kategorisierung folgend werden Arbeiten zur privatsphärengerechten Rechnungslegung mittels Smart Metering (Abschnitt 3.4) und Arbeiten zur privatsphärengerechten Stromnetzüberwachung und Produktionsplanung (Abschnitt 3.5) behandelt. Arbeiten, die ein Entstehen schützenswerter Daten gänzlich vermeiden bilden eine Ausnahme zu dieser Kategorisierung und werden in Abschnitt 3.3 behandelt.

In Abschnitt 3.5.3 werden die Arbeiten behandelt, deren Ziel ein privatsphärengerechtes Smart Metering zur Stromnetzüberwachung und Produktionsplanung mittels Aggregation ohne vertrauenswürdige dritte Partei ist. Da dies dem Ansatz der Verfahren in der vorliegenden Arbeit entspricht, wird anhand von definierten Kriterien eine genauere Betrachtung sowie ein Vergleich und eine Abgrenzung mit der vorliegenden Arbeit vorgenommen.

Abschließend wird in Abschnitt 3.6 eine Bewertung des Stands der Forschung vorgenommen.

3.1 Smart Metering und Privatsphäre

Das Sammeln der Daten im Smart Metering durch einen Dritten birgt das Risiko einer Verletzung der Privatsphäre. Unter dem Begriff *Nonintrusive load monitoring (NILM)* versteht man die Interpretation der durch intelligente Stromzähler ermittelten Daten um Erkenntnisse über die verursachenden Verbraucher und Erzeuger zu gewinnen. Erste Geräte hierfür wurden bereits 1985 von Hart [64] gebaut und konnten bestimmte Charakteristika einzelnen Energieverbrauchern zuordnen. Beispielsweise der konstante Verbrauch von 60 Watt dem Betrieb einer Glühbirne oder die einzelnen Phasen des Waschvorgangs der Waschmaschine. Mit Hilfe des NILM konnte dann festgestellt werden, ob jemand zu Hause war und in Einzelfällen was diese Person tat. Eine, 1991 veröffentlichte, Studie von Sultanem [128] zeigte, dass einzelne Geräte auch noch im *Gesamtverbrauch* des Haushalts identifizierbar sind. Ein früher Kommentar von Hart zum Thema NILM war, „dass der Verbrauch elektrischer Energie als genauso privat erachtet werden muss, wie jedes Telefongespräch“ [65].

Erste Arbeiten zu NILM konzentrierten sich auf Daten, die durch kurze Messintervalle von 5 Sekunden entstanden. Spätere Arbeiten widmeten sich der Verbesserung der Erkennung von Geräten bei gleichbleibendem Messintervall oder kürzeren Messintervallen (beispielsweise [2, 81, 82, 85, 96]). Ein Beispiel neueren Datums ist eine Veröffentlichung von Weiss et al. [137], in der mittels eines intelligenten Stromzählers und einem Messintervall von 1 Sekunde Haushaltsgeräte identifiziert werden. Selbst im Mischbetrieb konnten die Ein- und Ausschaltvorgänge der betrachteten Geräte mit einer Trefferquote von 90% bestimmt werden. Auch längere Messintervalle von bis zu einer Stunde bieten Möglichkeiten zur Identifizierung einzelner Geräte (beispielsweise [79, 86, 109]).

Schon 2009 waren Millionen von intelligenten Stromzählern mit der Fähigkeit für Messintervalle im Sekundenbereich installiert [22]. Häufig ohne ein wirksames Sicherheitskonzept, wie beispielsweise von Rouf et al. [117] gezeigt. Viele sammeln bereits Daten, die jedem, der Zugriff darauf hat, ein detailliertes Bild der Haushaltsbewohner liefern können. Der Eingriff in die Privatsphäre ist kaum zu unterschätzen wenn detaillierte Tagesabläufe der Haushaltsbewohner ermittelt werden können [86]. Die Verwendung dieser Informationen kann, im besten Fall, zu zielgerichteter Werbung führen. Gezielte Wohnungseinbrüche in besonders lohnenswerte Ziele gehören zu den schwerwiegenderen Folgen dieses Eingriffs in die Privatsphäre.

Die Vorteile und die Notwendigkeit des Smart Meterings für das Smart Grid sind immens. Doch der Eingriff in die Privatsphäre durch den intelligenten Stromzähler stellt einen hohen Preis dar. Im Folgenden werden Arbeiten vorgestellt, die Smart Metering ohne, oder nur mit geringen Einschränkungen der Privatsphäre ermöglichen.

3.2 Kategorisierung Smart Metering

In der Literatur gibt es zahlreiche Ansätze zu privatsphärengerechtem Smart Metering. Viele dieser Ansätze unterscheiden sich jedoch grundlegend bereits bei der eigentlichen Zielsetzung: der Anwendung des Smart Meterings. Diese bestimmt letztlich, welche Möglichkeiten zum Privatsphärenschutz offen stehen. Eine Kategorisierung nach Zielsetzung bietet sich daher an, und wird deshalb in dieser Arbeit durchgeführt. In der Literatur lassen sich im Wesentlichen zwei grundlegende Anwendungen des Smart Meterings identifizieren:

- Smart Metering zur Rechnungslegung
- Smart Metering zur Stromnetzüberwachung und Produktionsplanung

Dabei stellt das Smart Metering zur Rechnungslegung einen Sonderfall der klassischen Abrechnung dar. Diese wird in Deutschland traditionell jährlich durchgeführt und benötigt ein Ablesen des Stromzählers um den Jahresverbrauch zu ermitteln. Das Smart Metering zur Rechnungslegung verkürzt nun diesen Zeitraum (*Messintervall*), und kann eine Abrechnung wesentlich öfter, beispielsweise jeden Monat, durchführen. Dies ermöglicht den Verzicht auf Abschlagszahlungen und bietet dem Kunden eine zeitnahe Rückmeldung über seinen Verbrauch. Da hierbei eine genau Abbildung von Verbrauch zu Kunden durchgeführt wird, ist die Privatsphäre maßgeblich durch ein kurzes Messintervall gefährdet.

Das Smart Metering zur Stromnetzüberwachung und Produktionsplanung betrachtet die Leistungsaufnahme über eine Menge von teilnehmenden Haushalten hinweg. Ein Zweck ist die Überwachung des Stromnetzes zur Früherkennung von Stromausfällen und Überlastsituationen. Interessiert an diesen Daten sind vor allem Netzbetreiber und Energiehändler. Netzbetreiber können mittels Smart Metering beispielsweise alle Haushalte, die an eine bestimmte Ortsnetzstation angeschlossen sind, und damit einen Teil ihres Stromnetzes überwachen. Energiehändler können durch die Beobachtung ihrer eigenen Kunden frühzeitig und präzise Entscheidungen über Stromproduktion oder über ihren Handel an Strombörsen treffen. In

beiden Fällen ist es nötig die Messungen in kurzen Messintervallen durchzuführen und die Ergebnisse zeitnah zu erhalten. In aktuellen Pilotprojekten zum Smart Metering, aber auch in der Literatur, hat sich ein Messintervall von 15 Minuten etabliert (siehe beispielsweise [13, 44, 136]). Im Gegensatz zum Smart Metering zur Rechnungslegung kann hier auf eine direkte Abbildung von einzelnen Messwerten auf einzelne Kunden weitestgehend verzichtet werden. Von Interesse ist die Gesamtsicht auf die Menge der beobachteten intelligenten Stromzähler und damit, beispielsweise, die Summe der aktuellen Leistungsaufnahmen.

Aus Sicht des Privatsphärenschutzes gibt es drei Unterscheidungsmerkmale für diese beiden Smart Meterings: das *Messintervall*, die Möglichkeit Messwerte einem speziellen Haushalt zuordnen zu können (*Zuordnung*) und die *Genauigkeit*. Während das Smart Metering zur Rechnungslegung eine perfekte Zuordnung (wer die Rechnung bekommt) und hohe Genauigkeit (welcher Betrag eingefordert wird) erfordert, ist das Messintervall von geringerer Bedeutung. Das Smart Metering zur Stromnetzüberwachung und Produktionsplanung benötigt kurze Messintervalle und ebenfalls eine hohe Genauigkeit. Da Stromnetzsegmente oder Kundenkreise im Mittelpunkt stehen ist die Zuordnung weniger wichtig.

Die meisten veröffentlichten Arbeiten zum privatsphärengerechten Smart Metering widmen sich einer der beiden Smart Metering Anwendungen. Nur wenige Arbeiten betrachten beide Anwendungen gleichzeitig. Daher werden im Folgenden die Arbeiten zu privatsphärengerechtem Smart Metering aufgeteilt in Arbeiten zu privatsphärengerechtem Smart Metering zur Rechnungslegung (Abschnitt 3.4 und in Arbeiten zu privatsphärengerechtem Smart Metering zur Stromnetzüberwachung und Produktionsplanung (Abschnitt 3.5). Arbeiten die beide Anwendungen betrachten werden in beiden Abschnitten behandelt. Eine Ausnahme hiervon sind Arbeiten, die nicht das Smart Metering privatsphärengerecht gestalten sondern das Entstehen von schützenswerten Daten verhindern. Diese sind nicht im Fokus dieser Arbeit und werden daher nur kurz in Abschnitt 3.3 behandelt.

3.3 Arbeiten zur Vermeidung der Entstehung schützenswerter Daten

In diesem Abschnitt werden Arbeiten behandelt, die durch zusätzlichen Verbrauch oder zusätzliche Erzeugung den resultierenden Energieverbrauch eines Haushalts dergestalt beeinflussen, dass er auch bei genauer Untersuchung keine Gefahr mehr für die Privatsphäre darstellt. Dies wird in den Arbeiten dann als erreicht angesehen,

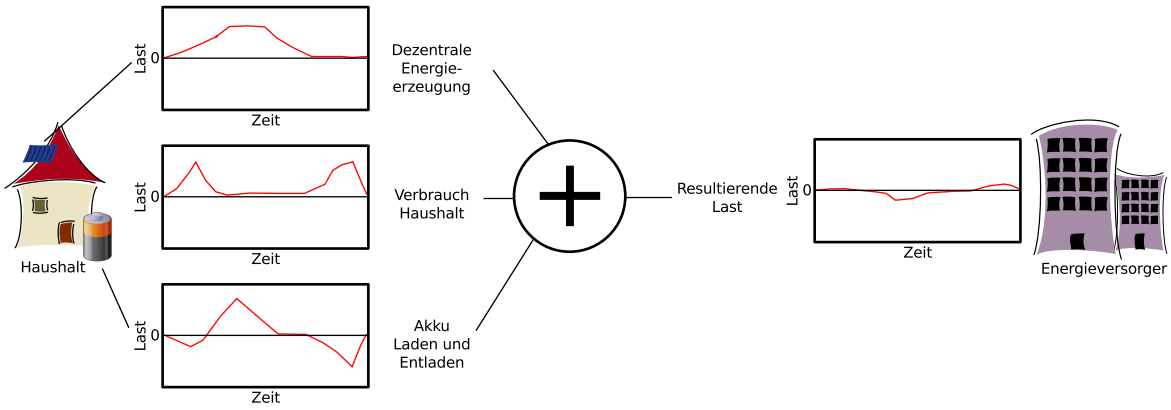


Abbildung 3.1: *Vermeidung der Entstehung schützenswerter Daten mittels Akkumulatoren.*

wenn der resultierende Energieverbrauch oder die resultierende Energieproduktion eines Haushalts für eine möglichst lange Zeit konstant ist.

Um dies zu erreichen wird in den Arbeiten von Kalogridis et al. [73, 74] und McLaughlin et al. [92] ein Energiespeicher mit hoher Kapazität im Haushalt installiert (siehe Abbildung 3.1). Aufgrund von historischen Daten wird eine durchschnittlicher Energiebedarf berechnet, den ein Steuergerät dann versucht zu halten. Benötigt der Haushalt weniger Energie, so wird mit der überschüssigen Energie der Energiespeicher geladen. Benötigt der Haushalt mehr Energie, so wird diese vom Energiespeicher gestellt, sofern er über genügend Energiereserven verfügt. Das Resultat ist, bei perfekter Bestimmung des durchschnittlichen Energiebedarfs und ausreichend großem Energiespeicher, ein konstanter Energiebedarf gegenüber dem Stromnetz.

Ein wesentliches Problem, das in diesen Arbeiten behandelt wird, ist die begrenzte Kapazität des Energiespeichers, dessen Ineffizienz und dessen Abnutzung durch regelmäßige Laden und Entladen. Die begrenzte Kapazität schränkt ein, wie flexibel der Energiebedarf eines Haushalts im Vergleich zum errechneten Durchschnittsbedarf sein darf. Die Ineffizienz, also die Differenz zwischen Energie die geladen wurde und Energie die der Energiespeicher dann leisten kann, sorgt für einen konstanten Energiebedarf, der nur zum Schutz der Privatsphäre genutzt wird. Dieser, sowie auch die Abnutzung des Energiespeichers, verursacht letztlich Kosten.

Da diese Arbeiten einen deutlich unterschiedlichen Ansatz zum Privatsphärenschutz verfolgen als die vorliegende Arbeit, wird nicht näher auf die Details der Arbeiten eingegangen.

3.4 Arbeiten zum Smart Metering zur Rechnungslegung

Smart Metering zur Rechnungslegung wird häufig nicht als Gefahr für die Privatsphäre angesehen, da zur Rechnungslegung bereits aggregierte Daten verwendet werden können. Das Ablesen eines normalen, also nicht intelligenten, Stromzählers ist bereits eine Aggregation des Energieverbrauchs über die Zeit, die seit der letzten Ablesung vergangen ist. Für einen einfachen Tarif, beispielsweise ein Preis pro Kilowattstunde für die gesamte Abrechnungsperiode, kann dieses Verfahren auch mittels eines intelligenten Stromzählers durchgeführt werden und stellt somit keine Gefahr für die Privatsphäre dar.[1] Eines der Ziele des Smart Grids ist jedoch die Möglichkeit für komplexere Tarife. Der Preis für den konsumierten Strom könnte beispielsweise von der Tageszeit, der verursachten Last oder dem Überschreiten eines Kontingents abhängen. Eine Protokoll zum privatsphärengerechten Smart Metering zur Rechnungslegung ermöglicht solch komplexe Tarife ohne die Privatsphäre des Kunden zu gefährden.

In der Literatur gibt es hierfür drei grundlegende Ansätze:

- Rechnungslegung durch eine dritte, vertrauenswürdige Partei.
- Rechnungslegung durch den intelligenten Stromzähler mittels Trusted Computing.
- Rechnungslegung durch den intelligenten Stromzähler und Überprüfung der Ergebnisse mittels kryptologischen Methoden.

Da der Fokus dieser Arbeit auf dem Smart Metering zur Stromnetzüberwachung und Produktionsplanung liegt, wird im Folgenden nur kurz auf die Arbeiten zum Smart Metering zur Rechnungslegung eingegangen.

3.4.1 Vertrauenswürdige, dritte Partei

Führt man eine dritte, vertrauenswürdige Partei ein, so kann diese genau jene Aufgaben übernehmen, die eine Gefahr für die Privatsphäre bedeuten würden. In

[1] Dieser Schluss gilt nur bei hinreichend langen Abrechnungsperiode. Wird beispielsweise wochenweise eine Rechnung erstellt, wäre eine mehrwöchige Urlaubsreise leicht zu entdecken. Sind die Abrechnungsperioden so kurz, dass sie die Privatsphäre bedrohen, kann dies nicht mit technischen Mitteln gelöst werden.

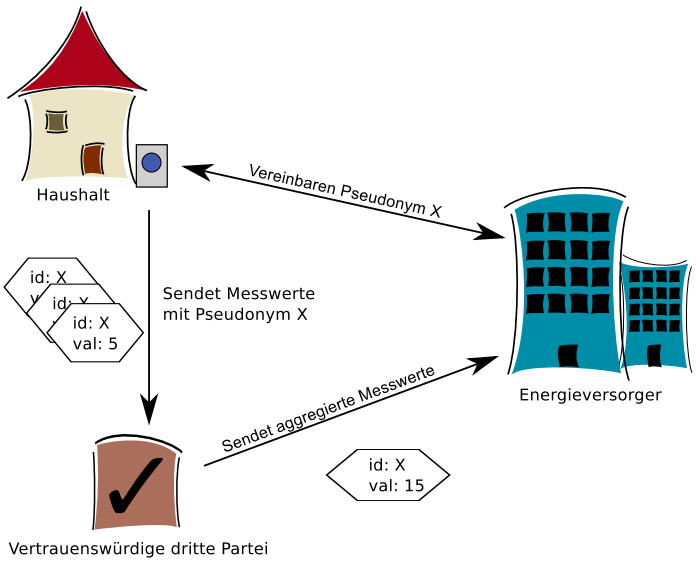


Abbildung 3.2: *Rechnungslegung mittels einer vertrauenswürdigen, dritten Partei.*

einer Veröffentlichung von Bohli et al. [13] wird ein Verfahren skizziert, bei dem die intelligenten Stromzähler periodisch ihre Messwerte an eine dritte Partei senden. Diese aggregiert Messwerte einzelner intelligenter Stromzähler über den Zeitraum der Abrechnungsperiode und leitet das Aggregat dann an den Energieversorger weiter. Um zu verhindern, dass die dritte Partei die Privatsphäre eines Haushalts verletzt, einigt sich der intelligente Stromzähler mit dem Energieversorger auf ein Pseudonym, das beide gegenüber der dritten Partei verwenden. Dieses Vorgehen ist in Abbildung 3.2 dargestellt.

Die Verwendung von Pseudonymen zum Schutz der Privatsphäre ist jedoch problematisch. Besonders wenn sekundäre Informationsquellen hinzugezogen werden können, ist eine effektive Pseudonymisierung schwierig. Wie Jawurek et al in [70] zeigen, kann mittels Anomalieerkennung und Verhaltensmustern eine Pseudonymisierung aufgehoben werden, wenn hinreichend genaue sekundäre Informationen vorliegen. Hierzu gehören beispielsweise Arbeits- oder Urlaubszeiten.

Ein generelles Problem einer Lösung mit vertrauenswürdiger Partei ist das hohe Vertrauen, das der Haushalt und der Energieversorger in die dritte Partei investieren muss. Wem ein solches Vertrauen entgegengebracht werden kann bleibt eine offene Frage.

3.4.2 Trusted Computing

Ein Ansatz, der zum Beispiel in den Arbeiten von Challener et al. [24] und Petrlic [106] verfolgt wird, ist die Verwendung eines *Trusted Platform Module (TPM)* im intelligenten Stromzähler. Das TPM realisiert *Trusted Computing* indem es Integrität und Vertraulichkeit der Berechnungen innerhalb des intelligenten Stromzählers garantiert und gegenüber dem Energieversorger nachweisen kann. Dadurch kann ein intelligenter Stromzähler selbst die Rechnungslegung durchführen. Dem Energieversorger muss nur noch der Endbetrag der Rechnung und der Nachweis des TPM über dessen korrekte Ermittlung übermittelt werden.

Dieser Ansatz ist einfach zu realisieren. Die Widerstandskraft eines TPMs gegen ernsthafte Angriffe wird allerdings in Zweifel gezogen [135].

3.4.3 Kryptologische Methoden

Einige Arbeiten verwenden kryptologische Commitments (siehe Abschnitt 2.5.4) um ebenfalls eine Berechnung auf dem intelligenten Stromzähler durchführen zu können. Im Gegensatz zum Trusted Computing findet der Nachweis über eine korrekte Kalkulation mittels kryptologischer Methoden statt.

Das am häufigsten verwendete Commitment Verfahren in Protokollen zum privatsphärengerechten Smart Metering sind Pedersen-Commitments [105]. Sie haben homomorphe Eigenschaften, die Berechnungen mit Commitments erlauben, die dann auch auf dem Inhalt der Commitments operieren. So führt die Multiplikation zweier Pedersen-Commitments zur Addition der Inhalte. Mittels Exponenzieren von Pedersen-Commitments können diese dann auch um ganzzahlige Faktoren multipliziert werden (siehe Formel 3.1).

$$\begin{aligned} Commit(x,r) \cdot Commit(y,s) &= Commit(x+y, r+s) \\ Commit(x,r)^k &= Commit(x \cdot k,\ r \cdot k) \end{aligned} \tag{3.1}$$

Diese Eigenschaft wird in den Arbeiten von Jawurek et al. [69] und Molina-Markham et al. [96] ausgenutzt um folgendermaßen ein privatsphärengerechtes Smart Metering zur Rechnungslegung zu realisieren (siehe auch Abbildung 3.3):

Ein intelligenter Stromzähler generiert Commitmentes $c_i = Commit(x_i, r_i)$ für jeden Messwert x_i einer Reihe von Messwerten mit jeweils einer Zufallszahl r_i. Diese Commitments werden vom intelligenten Stromzähler signiert und an den Energieversorger übertragen. Der Energieversorger stellt dem intelligenten Strom-

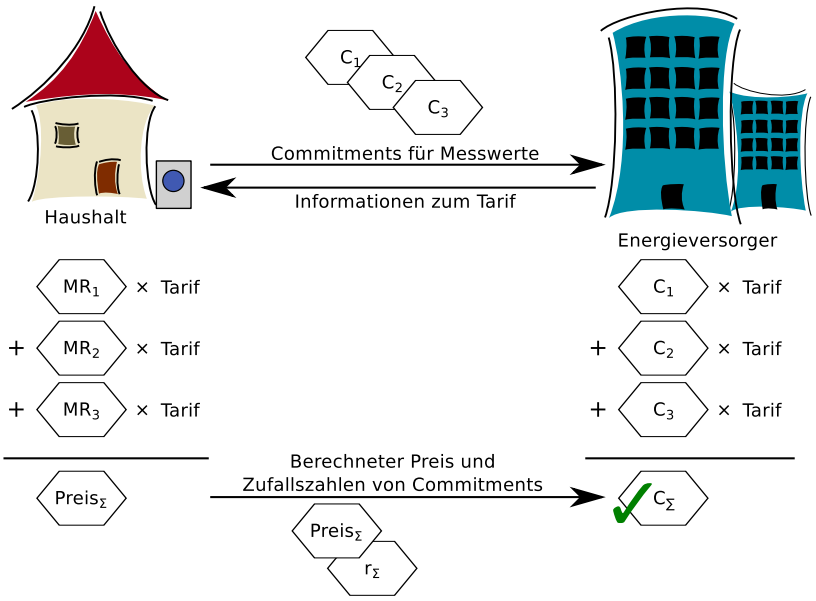


Abbildung 3.3: *Rechnungslegung mittels eines Commitment Verfahrens.*

zähler Tarifinformationen zur Verfügung. Mittels dieser Informationen berechnet der intelligente Stromzähler den Rechnungsbetrag, indem er jedes x_i mit dem korrespondierenden Preis multipliziert. Anschließend summiert er die Ergebnisse auf um den Endbetrag der Rechnung zu ermitteln. Gleichermaßen verfährt er mit den Zufallszahlen r_i. Das Ergebnis der Kalkulationen mittels der x_i und r_i wird anschließend an den Energieversorger übertragen.

Der Energieversorger überprüft die Korrektheit der Berechnung indem er dieselben Kalkulationen auf den empfangenen Commitments c_i durchführt. Das Ergebnis ist ein neues Commitment, das sich mittels dem vom intelligenten Stromzähler übertragenen Rechnungsbetrag und Zufallswert öffnen lassen muss.

Das hier beschriebene, grundlegende Verfahren hat zwei Nachteile: es kann nur relativ einfache, zeitbasierte Tarifsysteme abbilden und es benötigt manipulationssichere intelligente Stromzähler. Letzteres ist ein sinnvolle Grundannahme, da ein Smart Metering zur Rechnungslegung nur dann funktionieren kann, wenn die eigentliche Zähleinrichtung nicht manipuliert werden kann. Für komplexere Tarifsysteme existiert von Danezis et al. [113] ein Ansatz, der ebenfalls auf Commitments basiert, aber wesentlich komplexer ist.

3.4.4 Zusammenfassung

Die verschiedenen Ansätze zum Smart Metering zur Rechnungslegung unterscheiden sich hauptsächlich in der Frage, wem Vertrauen entgegengebracht wird. Ansätze aus Abschnitt 3.4.1 führen eine dritte Partei in, die per Definition vertrauenswürdig ist. In Abschnitt 3.4.2 wird der intelligente Stromzähler selbst zum vertrauenswürdigen Gerät. In Abschnitt 3.4.3 muss nur ein kleiner Teil des intelligenten Stromzählers vertrauenswürdig sein: die Zähleinheit, die gleichzeitig Commitments generiert. Die Berechnung selbst ist mittels kryptologischer Methoden durch den Energieversorger verifizierbar ohne die Einzelwerte zu kennen.

3.5 Arbeiten zum Smart Metering zur Stromnetzüberwachung und Produktionsplanung

Das Smart Metering zur Stromnetzüberwachung und Produktionsplanung beschäftigt sich, im Gegensatz zum Smart Metering zur Rechnungslegung, nicht mit einzelnen Haushalten. Stattdessen sind Haushalte in bestimmten Abschnitten des Stromnetzes oder Kunden eines bestimmten Energieversorgers Gegenstand des Smart Meterings. Eine naheliegende Möglichkeit des Privatsphärenschutzes besteht darin, die Haushalte der jeweiligen Smart Metering Instanz aggregiert zu betrachten. Dies ist auch der Ansatz, den die meisten Arbeiten zum privatsphärengerechten Smart Metering zur Stromnetzüberwachung und Produktionsplanung verfolgen.

Die Arbeiten zur privatsphärengerechten Bestimmung dieser Gesamtsicht auf die betrachteten Haushalte können aufgrund ihres grundlegenden Ansatzes in folgende Kategorien eingeteilt werden:

- Anonymisierung / Pseudonymisierung.
- Aggregation mittels einer dritten, vertrauenswürdigen Partei.
- Aggregation ohne eine dritte Partei.

Jede dieser Kategorien wird im Folgenden einzeln behandelt. Zunächst wird jeweils der grundlegende Ansatz erläutert um dann auf spezifische Arbeiten einzugehen.

3.5.1 Anonymisierung / Pseudonymisierung

Einen naheliegenden Ansatz zum Privatsphärenschutz stellt die Entfernung identifizierender Informationen aus den Messdaten dar. Dabei können die Identitäten der intelligenten Stromzähler und Haushalte entfernt werden. Auch ein Ersetzen mit nicht zurückführbaren Pseudonymen ist möglich. Ein Problem das bei der Entfernung identifizierender Informationen auftritt ist, dass den resultierenden Daten zunächst nicht vertraut werden kann. Im Speziellen kann nicht ausgeschlossen werden, dass die Messdaten falsch oder gar aus einer unberechtigten Quelle sind.

Um diesen Ansatz dennoch durchführen zu können, greifen einige Arbeiten auf eine vertrauenswürdige, dritte Partei zurück. Diese fungiert als Vermittler und garantiert dem Haushalt die Anonymität oder Pseudonymität während sie dem Auftraggeber des Smart Meterings die Korrektheit der erfassten Daten garantiert. Intelligente Stromzähler übersenden ihre Daten der vertrauenswürdigen dritten Partei, die dann identifizierende Informationen entfernt und die resultierenden Daten an den Auftraggeber des Smart Meterings weiterleitet. Das Vertrauen, das die Haushalte in die dritte Partei haben müssen, ist hier sehr groß. Da die dritte Partei über alle sensiblen Informationen verfügt, muss nicht nur darauf vertraut werden, dass sie diese nicht an den Auftraggeber weitergibt, sondern auch, dass sie die sensiblen Daten wirksam schützt und nicht missbraucht.

In den Arbeiten von Petrlic [106] und Molina-Markham et al. [96] wird dieses Vorgehen verwendet. Es wird eine Public-Key Infrastruktur verwendet, so dass ein intelligente Stromzähler seine Messwerte für die dritte Datei verschlüsseln und signieren kann. Diese überprüft die Signatur, entfernt oder ersetzt die Identität und sendet die modifizierten Daten, verschlüsselt und signiert, an den Auftraggeber des Smart Meterings. Geht man von der Vertrauenswürdigkeit der dritten Partei aus, so erzielt dieses Vorgehen das gewünschte Ergebnis. Abhängig von den Fähigkeiten eines Angreifers existieren jedoch Informationsquellen durch Seitenkanäle. Kann ein Angreifer sowohl die Kommunikationsanbindung des intelligenten Stromzählers, als auch die der dritten Partei abhören, so kann er den Versand von Messwerten miteinander korrelieren. Auch ohne die Daten entschlüsseln zu können, kann der Angreifer den (verschlüsselten) Messwert *nach* der Anonymisierung weiterhin einem Haushalt zuordnen. Eine detailliertere Diskussion des Problems der *Verkehrsanalyse* wurde von Chaum [26] durchgeführt.

Efthymiou und Kalogridis [42] stellen einen Ansatz vor, der dieses Problem umgeht. Ein intelligenter Stromzähler verfügt dabei über zwei, von der vertrauenswürdigen dritten Partei zertifizierten, Identitäten. Eine Identität identifiziert den

Haushalt und dient der Übermittlung von Daten in langen Messintervallen, also Daten, die keine Bedrohung für die Privatsphäre darstellen. Die andere Identität identifiziert lediglich ein Pseudonym. In beiden Fällen werden die Daten direkt an den Auftraggeber des Smart Meterings gesendet und mit dem Zertifikat der entsprechenden Identität signiert. Die Vergabe der Pseudonyme stellt dabei ein Problem dar. Fügt der Auftraggeber des Smart Meterings einen weiteren Haushalt zu einem bestehenden Smart Metering hinzu, so muss auch ein neues Pseudonym entstehen. Korreliert er diese beiden Ereignisse, so kann er die Pseudonymisierung aufheben. Zur Vermeidung wird in der Arbeit eine ausführliche und langwierige Routine zur Vergabe der Pseudonyme verwendet. Sie beinhaltet mehrere zufällige Wartezeiten zwischen einzelnen Schritten um eine Korrelation zu verhindern. Dies resultiert allerdings in Vergabezeiten für Pseudonyme, die in Tagen gemessen werden müssen.

3.5.2 Aggregation mittels einer vertrauenswürdigen, dritten Partei

Eine Entkopplung von den Daten einzelner Haushalte bieten Ansätze, die eine Aggregation über mehrere Haushalte hinweg durchführen. In diesem Abschnitt werden Ansätze behandelt, die eine Aggregation mit Hilfe einer vertrauenswürdigen dritten Partei durchführen. Das grundlegende Prinzip ist in Abbildung 3.4 dargestellt. In der abgebildeten, einfachen Variante wäre von Seiten der Haushalte, wie im vorhergehenden Abschnitt, ein sehr großes Vertrauen nötig.

Eine Variation dieses Grundprinzips wird von Kim et al. [76] vorgestellt. In dieser Arbeit wird als Messgröße der Phasenverschiebungswinkel verwendet um durch die dritte Partei eine Abschätzung des Stromnetzzustandes durchführen zu lassen. Da der Auftraggeber nur das Ergebnis dieser Abschätzung erfährt, ist die Privatsphäre der Haushalte vor ihm geschützt. Um die Privatsphäre der Haushalte auch vor der dritten Partei zu schützen wird ausgenutzt, dass die Abschätzung auch bei Variation der Eingangsdaten innerhalb gewisser Freiheitsgrad zum gleichen Ergebnis führt. Diese Freiheitsgrade teilt der Auftraggeber den intelligenten Stromzählern mit. Diese verändern ihre Messdaten entsprechend, bevor sie an die dritte Partei gesendet werden. Das vertrauen in die dritte Partei reduziert sich damit aus Sicht der Haushalte dahingehend, dass diese nicht mit dem Auftraggeber kooperiert. Der Auftraggeber muss darauf vertrauen, dass die dritte Partei die Abschätzung des Stromnetzzustandes korrekt vornimmt.

Vetter et al. [136] schildern einen hybriden Ansatz, der auf der Verwendung von homomorpher Verschlüsselung (siehe Abschnitt 2.5.3) basiert. Neben der

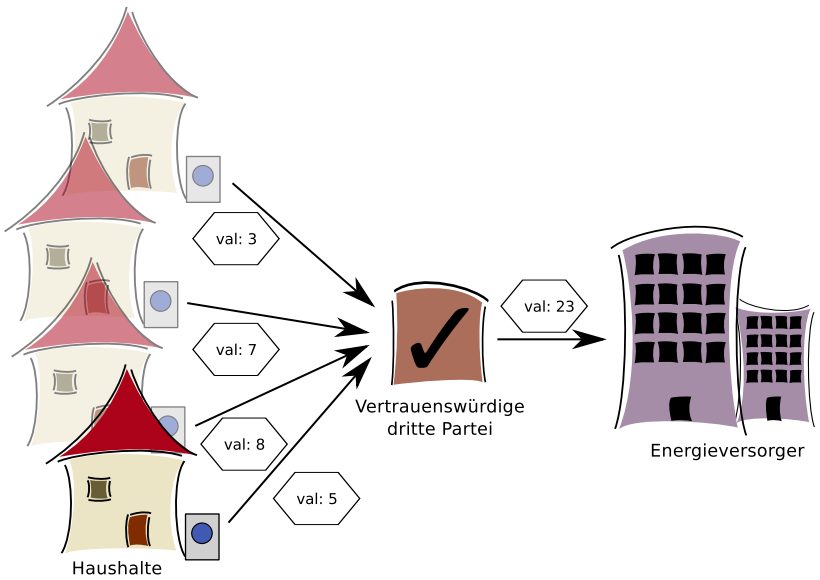


Abbildung 3.4: *Aggregation von Messdaten über Haushalte mittels einer vertrauenswürdigen dritten Partei.*

vertrauenswürdigen dritten Partei (hier *Key Authority* genannt) wird eine vierte Partei eingeführt, der die eigentliche Datenhaltung obliegt (Datenbank). Diese muss nicht vertrauenswürdig sein. Das Prinzip ist in Abbildung 3.5 dargestellt.

Jeder intelligente Stromzähler verschlüsselt seine Messwerte mittels eines homomorphen Verschlüsselungsverfahrens und einem privaten Schlüssel, den er von der Key Authority bezieht. Das Verschlüsselungsverfahren muss dabei sowohl in den Chiffraten, als auch in den Schlüsseln homomorph sein. Die so verschlüsselten Messwerte überträgt er dann an eine Datenbank. Da die Datenbank nicht im Besitz von Schlüsselmaterial ist, kann sie die verschlüsselten Daten nicht entschlüsseln. Sie kann aber von anderen Parteien, beispielsweise dem Auftraggeber des Smart Meterings, abgefragt werden. Um die abgefragten Daten jedoch entschlüsseln zu können, wird Schlüsselmaterial benötigt. Dieses kann von der Key Authority erfragt werden. Um die Privatsphäre der Haushalte zu schützen, liefert diese aber nur aggregiertes (also homomorph aufsummiertes) Schlüsselmaterial über eine ausreichende Anzahl an Haushalte. Die abfragende Partei bekommt also nur einen Schlüssel, der das Aggregat über mehrere Haushalte entschlüsselt. Dieses kann sie mittels der aus der Datenbank erfragten, einzelnen Messwerte selbst bilden und dann entschlüsseln.

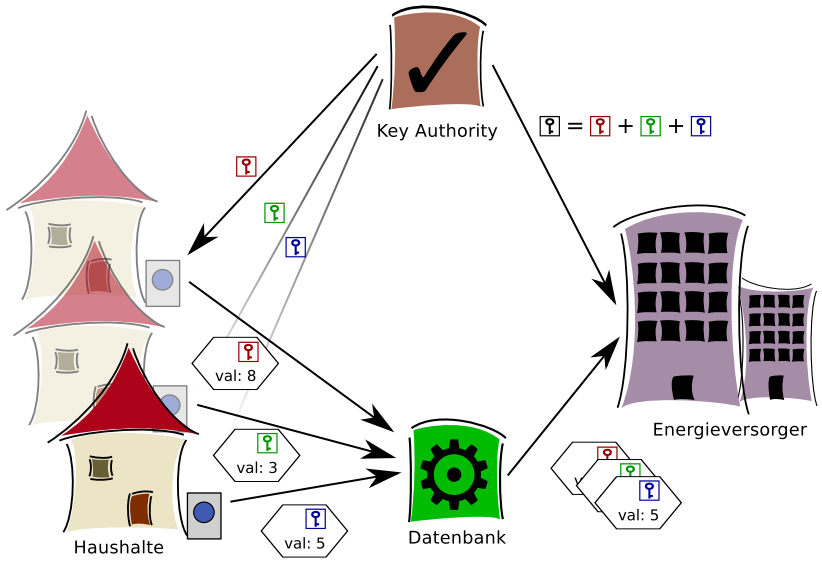


Abbildung 3.5: *Trennung von Datenhaltung und Rechtevergabe in [136].*

Dieser Ansatz separiert die beiden Aufgaben Datenhaltung und Rechtevergabe effektiv und ermöglicht somit eine schlankere, und damit möglicherweise günstigere, vertrauenswürdige Partei. Die Haushalte müssen der Key Authority jedoch großes Vertrauen entgegenbringen, da diese über Schlüsselmaterial verfügt, das vollen Zugriff auf die sensiblen Daten ermöglicht. Selbst wenn die Datenbank keinen Zugriff auf einzelne Messwerte erlaubt, kann die Key Authority aus entsprechend konstruierten Aggregaten diese berechnen.

Eine Arbeit von Rottondi et al. [116] beschreibt zwei Aggregationsverfahren. Eines, das mittels Shamir's Secret Sharing [122] als unterliegendes Kryptosystem funktioniert und eines, das auf dem Cramer-Shoup-Kryptosystem [29] aufbaut. Beide Varianten tauschen verschlüsselte Messwerte zwischen intelligenten Stromzählern aus und aggregieren diese bevor sie zum Auftraggeber gesendet werden. Zur Aggregation werden Zwischensysteme, genannt *Gateways*, verwendet. Die Organisation der Aggregation wird von einer zentralen Partei, genannt *Konfigurator*, durchgeführt. Diese entscheidet insbesondere, ob eine Aggregation den konfigurierten Richtlinien zum Privatsphärenschutz entspricht und erteilt nur dann eine entsprechende Autorisierung der Aggregation.

3.5.3 Aggregation ohne dritte Partei

In diesem Abschnitt werden Ansätze vorgestellt, die eine Aggregation von Messdaten über intelligente Stromzähler hinweg durchführen, ohne eine vertrauenswürdige dritte Partei zu benötigen. Als einzige involvierte Parteien verbleiben die intelligenten Stromzähler der Haushalte und der Auftraggeber des Smart Meterings. Eine der großen Herausforderungen dieser Ansätze besteht darin, dass eine Aggregation durchgeführt werden muss *ohne*, dass der Auftraggeber des Smart Meterings oder ein anderer intelligenter Stromzähler in den Besitz des Klartexts der Messdaten kommt.

Da die in der vorliegenden Arbeit vorgestellten Verfahren ebenfalls das Ziel einer Aggregation ohne vertrauenswürdige dritte Partei verfolgen, werden die Arbeiten in diesem Abschnitt detaillierter diskutiert, als die Arbeiten in den vorhergehenden Abschnitten. Es werden zunächst Kriterien eines privatsphärengerechten Smart Meterings definiert. Anhand dieser Kriterien werden die Verfahren bewertet. Die in dieser Arbeit eingeführten Verfahren werden ebenfalls eingeordnet. Eine tabellarische Übersicht über die Erfüllung der Kriterien ist in Tabelle 3.1 auf Seite 53 gegeben.

K1 Privatsphärenschutz bei korrumpiertem Auftraggeber

Ein Verfahren zum privatsphärengerechten Smart Metering sollte die Privatsphäre der einzelnen Haushalte schützen. Wie in Abschnitt 2.1.4 motiviert, sollte dies auch dann der Fall sein, wenn der Auftraggeber aktiv in das Geschehen eingreift.

K2 Hohe SM-Reichweite auch bei Störungen

Auch bei privatsphärengerechtem Smart Metering sollte gewährleistet sein, dass selbst bei Störungen der intelligenten Stromzähler oder der Kommunikationsinfrastruktur eine hohe SM-Reichweite (siehe Abschnitt 2.1.2) erreicht wird. Insbesondere sollten Störungen einzelner intelligenter Stromzähler oder einzelner Kommunikationsanbindungen keinen Einfluss auf große Teile oder gar das gesamte Smart Metering haben.

K3 Realisierbarkeit auf ressourcenbeschränkter Hardware

Da intelligente Stromzähler über beschränkte Ressourcen verfügen, ist eine mögliche Realisierung des Verfahrens mit limitierten Rechen- und Speicherkapazitäten und mit geringem Kommunikationsaufwand wünschenswert.

K4 SM-Latenz

Primär steht beim privatsphärengerechten Smart Metering der Privatsphärenschutz im Vordergrund. Mit diesem Kriterium wird beurteilt ob dennoch eine niedrige SM-Latenz (siehe Abschnitt 2.1.2) erzielt werden kann.

K5 Kurzes SM-Intervall

Analog zur SM-Latenz ist ein kurzes SM-Intervall zwar wünschenswert, jedoch neben dem Privatsphärenschutz nur zweitrangig.

Li et al. [83, 84] organisieren die intelligenten Stromzähler in einem Aggregationsbaum. Das heißt, jedem intelligenten Stromzähler wird ein anderer intelligenter Stromzähler als Vaterknoten und mehrere andere intelligente Stromzähler als Kindknoten zugewiesen. Diese Zuweisung findet durch den Auftraggeber des Smart Meterings statt. Im Zuge der Zuweisung teilt der Auftraggeber auch seinen öffentlichen Schlüssel für ein asymmetrisches, homomorphes Verschlüsselungsverfahren mit (Paillier und Pointcheval [104]). Somit ist jeder intelligente Stromzähler in der Lage, seinen Messwert mittels des öffentlichen Schlüssels des Auftraggebers zu verschlüsseln. Ein so verschlüsselter Messwert ist für die anderen intelligenten Stromzähler nicht mehr lesbar. Durch die homomorphe Eigenschaft des Verschlüsselungsverfahrens können diese allerdings mit den verschlüsselten Werten rechnen, konkret: sie aufsummieren.

Innerhalb eines Messintervalls misst jeder intelligente Stromzähler seinen aktuellen Messwert und verschlüsselt diesen mittels des öffentlichen Schlüssels des Auftraggebers. Danach beginnen die intelligenten Stromzähler ohne Kindknoten, also die Blätter im Aggregationsbaum, ihre verschlüsselten Messwerte an ihre Vaterknoten zu senden. Hat ein intelligenter Stromzähler die verschlüsselten Messwerte seiner Kindknoten erhalten, summiert er sie mit seinem eigenen, verschlüsselten Messwert auf. Das Ergebnis wird dann wieder an den Vaterknoten gesendet. Dieses Vorgehen wiederholt sich so lange, bis die Daten bei der Wurzel des Aggregationsbaumes ankommen. Diese sendet ihr Ergebnis dann an den

Auftraggeber des Smart Meterings. Da der Auftraggeber des Smart Meterings im Besitz des passenden geheimen Schlüssels ist, kann er den erhaltenen Wert, also die Summe aller Messwerte der intelligenten Stromzähler im Aggregationsbaum, entschlüsseln.

Das in der Arbeit verwendete Angreifermodell entspricht dem honest-but-curious-Angreifer (siehe Abschnitt 2.1.4) und schließt damit ein aktives Eingreifen des Auftraggebers des Smart Meterings aus. Wäre dies nicht der Fall, könnte der Auftraggeber durch die von ihm durchgeführte Zuweisung von Vater- und Kindknoten korrumpierte Stromzähler in sensible Positionen des Aggregationsbaums einfügen. So würde zum Angriff auf die Privatsphäre eines einzelnen Haushalts ein einzelner korrumpierter Stromzähler genügen, wenn der Auftraggeber das Angriffsziel als Blattknoten und den korrumpierten Stromzähler als direkten Vaterknoten des Angriffsziels einsetzt. Das Kriterium K1 wird daher negativ bewertet.

Störungen der Kommunikationsanbindung der intelligenten Stromzähler (Churn) werden in dieser Arbeit nicht behandelt. Aufgrund des Aggregationsbaums ist damit zu rechnen, dass eine Störung eines einzelnen intelligenten Stromzählers den Verlust der Daten aller direkten und indirekten Kindknoten bedeutet. Eine Störung der Wurzel des Aggregationsbaums würde den Verlust des gesamten Smart Metering Ergebnisses bedeuten. Daher wird auch Kriterium K2 negativ bewertet.

Der Rechen-, Speicher- und Kommunikationsaufwand ist sehr gering und das verwendete homomorphe Verschlüsselungsverfahren realisiert die homomorphe Addition mittels Multiplikation. Das Kriterium K3 ist daher positiv zu bewerten.

Durch den Einsatz eines Aggregationsbaumes, der bis zur Wurzel durchlaufen werden muss, steigt die SM-Latenz des Verfahrens mit der Anzahl an teilnehmenden intelligenten Stromzählern. Auch wenn diese nur logarithmisch steigt, sind für große Anzahlen an intelligenten Stromzählern sehr lange SM-Latenzen möglich. Das Kriterium K4 ist daher negativ zu bewerten.

Auch wenn durch die hohe SM-Latenz Ergebnisse noch nicht beim Auftraggeber angekommen sind, kann schon das nächste Messintervall gestartet werden. Für das Kriterium K5 ist also eine positive Bewertung gerechtfertigt.

Garcia und Jacobs [57] verwenden zur Aggregation die Grundprinzipien des SMART Verfahrens (siehe Abschnitt 2.3) und Infrastruktur (genannt *Datenkonzentrator*) auf Ebene der Ortsnetzstation des Stromnetzes. Der Datenkonzentrator stellt einen zentralen Austausch- und Aggregationspunkt für die verschlüsselten Messwerte der intelligenten Zähler dar. Zwischen den intelligenten Stromzählern selbst findet keine direkte Kommunikation statt. Als Verschlüsselungsverfahren kommt wie in [83] das Verfahren nach Paillier und Pointcheval zum Einsatz. An-

ders als in [83] verfügt jedoch *jeder* intelligente Stromzähler über ein eigenes Schlüsselpaar. Der öffentliche Teil des Schlüsselpaares muss allen anderen intelligenten Stromzählern bekannt sein oder über den Datenkonzentrator zur Verfügung gestellt werden.

Das SMART-Verfahren wird in der Arbeit über den Datenkonzentrator realisiert. Jeder intelligente Stromzähler teilt seinen eigenen Messwert in so viele Teile auf, wie intelligente Stromzähler am Datenkonzentrator angeschlossen sind. Ein Teil wird zurückbehalten, die restlichen Teile sind jeweils für einen anderen intelligenten Stromzähler bestimmt. Sie werden mit dem öffentlichen Schlüssel des Ziels verschlüsselt und an den Datenkonzentrator gesendet. Dieser sammelt für jeden intelligenten Stromzähler die eintreffenden, verschlüsselten Teile und aggregiert sie mittels der homomorphen Eigenschaften des Verschlüsselungsverfahrens. Das Aggregat sendet er dann an den jeweiligen intelligenten Stromzähler. Dieser kann das Aggregat entschlüsseln, seinen zurückbehaltenen Teil des Messwertes aufaddieren und letztlich den so maskierten Messwert wieder an den Datenkonzentrator senden.

In der Arbeit wird kein Angreifermodell genannt. Die Sicherheitsanalyse behandelt lediglich das grundlegende Verfahren und ignoriert weitere Faktoren, beispielsweise den Datenkonzentrator. Obwohl dieser nur mit verschlüsselten Daten operiert, kann er eine Selektion der Daten durchführen, die er tatsächlich weitergibt. Kooperiert er mit dem Auftraggeber des Smart Meterings kann er beeinflussen, welche Daten tatsächlich aggregiert werden, ohne dass diese Modifikation den einzelnen intelligenten Stromzähler auffallen könnte. Das Kriterium K1 wird daher neutral bewertet.

Auch in dieser Arbeit werden Störungen nicht betrachtet. Durch die Verwendung der SMART Prinzipien kann ein Ausfall eines einzelnen intelligenten Stromzählers, und damit der Verlust des zurückbehaltenen Fragments, das Smart Metering Ergebnis um einen zufälligen Wert verfälschen. Dieser Fehlerzustand kann nicht behoben werden und führt zu einem Ausfall des Smart Meterings. Das Kriterium K2 wird daher negativ bewertet.

Der Rechenaufwand bei diesem Verfahren ist hoch, da viele Operationen im homomorphen Verschlüsselungsverfahren durchgeführt werden müssen. Den Großteil der Operationen übernimmt jedoch der eingesetzte Datenkonzentrator, was die intelligenten Stromzähler entlastet. Kriterium K3 wird daher neutral bewertet.

Da die Grundprinzipien des SMART-Verfahrens verwendet werden, wird der Messwert zuerst ermittelt bevor der Austausch der intelligenten Stromzähler untereinander stattfinden kann. Dies verzögert das Eintreffen der Daten beim

Auftraggeber um die Zeit, die der Austausch untereinander benötigt. Da dies zwar eine Verzögerung darstellt, diese aber nicht von der Anzahl intelligenter Stromzähler abhängt, wird das Kriterium K4 mit neutral bewertet.

Auch wenn die Ergebnisse noch nicht beim Auftraggeber angekommen sind, kann schon das nächste Messintervall gestartet werden. Für das Kriterium K5 ist also eine positive Bewertung gerechtfertigt.

Erkin und Tsudik [46] stützen ihren Ansatz zum privatsphärengerechten Smart Metering auf eine angepasste Variante des asymmetrischen, homomorphen Verschlüsselungsverfahrens von Paillier und Pointcheval. Allerdings verfügen alle intelligenten Stromzähler in diesem Ansatz über den gleichen öffentlichen und privaten Schlüssel des Verschlüsselungsverfahrens. Das Verschlüsselungsverfahren wird hauptsächlich wegen seiner homomorphen Eigenschaften genutzt. Zwischen intelligente Stromzählern werden Informationen so ausgetauscht, dass jeder intelligente Stromzähler seinen Messwert im modifizierten Verschlüsselungsverfahren so verschlüsseln kann, dass eine Entschlüsselung des Messwerts alleine keine Informationen über den Messwert enthält. Die Entschlüsselung der (homomorph berechneten) Summe der verschlüsselten Messwerte führt jedoch zum korrekten Ergebnis. Die Berechnung dieser Summe wird auf einem zufällig gewählten intelligenten Stromzähler durchgeführt.

Durch die Verwendung des angepassten Verschlüsselungsverfahrens ist es dem Auftraggeber nur dann möglich einen Messwert eines bestimmten intelligenten Stromzählers zu erhalten, wenn er alle anderen intelligenten Stromzähler korrumpiert. Der Privatsphärenschutz bei korrumpiertem Auftraggeber (K1) ist daher positiv bewertet. Der Nachteil bei diesem Vorgehen ist, dass eine Störung eines einzelnen intelligenten Stromzählers bereits zum Verlust des gesamten Aggregats führen muss. Kriterium K2 ist daher negativ bewertet. Diese Bewertung ist insbesondere in Kombination zu betrachten. Werden eine Vielzahl intelligenter Stromzähler verwendet (also der Angriff mittels korrumpierter intelligenter Stromzähler erschwert), so steigt die Wahrscheinlichkeit für Störungen und damit auch die Wahrscheinlichkeit für einen Ausfall des Smart Meterings.

Das angepasste Verschlüsselungsverfahren nutzt stark das Exponenzieren und führt ausführliche Berechnungen, die linear mit der Anzahl an teilnehmenden intelligenten Stromzählern steigen, auf einem einzelnen intelligenten Stromzähler aus. Die Realisierung auf ressourcenbeschränkter Hardware (K3) ist daher negativ bewertet. Dies wirkt sich auch auf die SM-Latenz aus. Die Zeit, die der zentral berechnende intelligente Stromzähler mit der Berechnung des Ergebnisses verbringt, erhöht die SM-Latenz. Zusätzlich muss zuerst jeder intelligente Stromzähler

an den zentral berechnenden intelligenten Stromzähler senden. Kriterium K4 ist daher neutral bewertet. Ebenfalls ist das kürzeste Messintervall limitiert durch die Rechenkapazität des zentral berechnenden intelligenten Stromzählers. Auch Kriterium K5 ist daher neutral bewertet.

In einer Arbeit von Goméz Mármol et al. [60, 61] übertragen die intelligenten Stromzähler ihre Messwerte direkt an den Auftraggeber des Smart Meterings. Jeder Messwert wird vorher allerdings mit einem zufälligen Schlüssel eines homomorphen Verschlüsselungsverfahrens ([1, 20]) verschlüsselt. Dieses ist nicht nur homomorph in den Chiffraten, sondern auch in den Schlüsseln. Diese Eigenschaft wird in der Arbeit verwendet. Die wesentliche Herausforderung besteht darin, den Auftraggeber des Smart Meterings mit einem Schlüssel für das Aggregat der Messwerte auszustatten.

Die intelligenten Stromzähler werden hierzu in einer Gruppe organisiert, aus der ein intelligenter Stromzähler (der sogenannte *Key Aggregator*) ausgewählt wird. Wie diese Auswahl stattfindet wird nicht genauer spezifiziert, mit [123] jedoch eine Lösung von einigen der Autoren vorgeschlagen. Auch soll diese Auswahl regelmäßig erneuert werden. Für das erste durchgeführte Messintervall übetragen alle intelligenten Stromzähler einer Gruppe anonym ihren verwendeten Schlüssel an den Key Aggregator. Hierfür wird eine anonyme Kommunikationsmöglichkeit (vorgeschlagen wird beispielsweise Tor [34]) benötigt. Der Key Aggregator bildet das Aggregat dieser Schlüssel und leitet das Ergebnis an den Auftraggeber des Smart Meterings weiter. Nun verfügt dieser über den benötigten Schlüssel und kann, nachdem er die verschlüsselten Messwerte aufaggregiert hat, das Aggregat entschlüsseln.

In den weiteren Messintervallen wird eine Veränderung der Schlüssel der einzelnen intelligenten Stromzähler erzwungen. Das Ziel dabei ist, dass jeder intelligente Stromzähler einen neuen, zufälligen Schlüssel generiert, der vom Auftraggeber des Smart Meterings benötigte Schlüssel aber identisch bleibt. Zu diesem Zweck werden die intelligenten Stromzähler der Gruppe in einer ringförmigen Struktur arrangiert. Wie diese ringförmige Struktur etabliert, geändert und gewartet wird, ist nicht Bestandteil der Arbeit. Nach Etablierung der ringförmigen Struktur hat jeder intelligente Stromzähler einen Vorgänger und einen Nachfolger. Jeder intelligente Stromzähler koordiniert nun mit seinem Vorgänger und Nachfolger die Variation der Schlüssel so, dass sich das Aggregat der Schlüssel nicht verändert. Danach verfügt jeder intelligente Stromzähler im Ring über einen neuen, zufälligen Schlüssel, der nur ihm bekannt ist. Das Aggregat dieser neuen Schlüssel ist

jedoch gleich dem Aggregat der vorherigen Schlüssel. Dieses Verfahren wird für jedes Messintervall wiederholt.

Das Angreifermodell in dieser Arbeit berücksichtigt (als einzige in dieser Auflistung) einen starken Angreifer, der in Kooperation mit dem Auftraggeber des Smart Meterings korrumpierte intelligente Stromzähler einbringen kann. Der Einsatz eines Anonymisierungsnetzwerks verhindert, dass ein korrumpierter Key Aggregator die Privatsphäre der Haushalte verletzen kann. Kann ein Angreifer jedoch korrumpierte intelligente Stromzähler in der Ring-Struktur an beliebigen Stellen platzieren, so kann er auch einen erfolgreichen Angriff durchführen. Wie diese Ring-Struktur aufgebaut wird ist in der Arbeit nicht beschreiben. Die Sicherheitsanalyse geht von einer zufälligen, also nicht durch den Angreifer beeinflussbaren, Anordnung aus. Für einen verlässlichen Angriff würde ein Angreifer genügend korrumpierte intelligente Stromzähler benötigen, um die Gruppe des Angriffsziels aufzufüllen. Insgesamt ist das Kriterium K1 hier positiv zu bewerten.

In der Arbeit wird auch Churn betrachtet. Der Ausfall eines intelligenten Stromzähler kann zu einem Ausfall des Smart Metering führen, da das gebildete Aggregat nutzlos wird. Die vorgeschlagene Handhabung von Churn stellt einen alternativen Protokollablauf vor, der eine Angriff durch einen korrumpierten Key Aggregator ermöglicht. Daher wird vorgeschlagen, dieses nur dann einzusetzen, wenn Churn beobachtet wurde und seinen Einsatz zur protokollieren. Ein Ausfall eines Key Aggregators wird nicht explizit behandelt, muss aber im Verlust des Smart Metering Ergebnisses für die gesamte Gruppe resultieren, falls er zum Zeitpunkt der Berechnung des aggregierten Keys auftritt. Insgesamt ist das Kriterium K2 neutral zu bewerten.

Das verwendete Verschlüsselungsverfahren ist trotz homomorpher Eigenschaften sehr effizient auch auf ressourcenbeschränkter Hardware durchführbar. Die potentiell schwierig auf ressourcenbeschränkter Hardware durchführbare Kommunikation über ein Anonymisierungsnetzwerk findet (bei hoher Verfügbarkeit der intelligenten Stromzähler) nur selten statt. Daher ist Kriterium K3 positiv bewertet.

Die SM-Latenz des Verfahrens ist nur durch den Versand des verschlüsselten Messwerts durch den intelligenten Stromzähler limitiert. Kriterium K4 ist also positiv bewertet.

Das kleinstmögliche SM-Intervall ist abhängig von der Zeit, die ein intelligenter Stromzähler benötigt um seinen Schlüssel mittels der Ringstruktur zu verändern. Dies involviert pro intelligentem Stromzähler einen Empfang von Daten des Vorgängers und ein Versand von Daten an den Nachfolger. Unter der Voraussetzung, dass die Ring-Struktur etabliert und stabil ist, kann dieser Vorgang parallel für alle

intelligenten Stromzähler in sehr kurzer Zeit durchgeführt werden. Daher wird das Kriterium K5 positiv bewertet.

Der grundlegende Ansatz der Arbeit ist ähnlich zum in der vorliegenden Arbeit vorgestellten SMART-ER-Verfahren: intelligente Stromzähler tauschen untereinander Werte aus, um ihren Messwert zu maskieren und senden den maskierten Messwert dann direkt an den Auftraggeber. In SMART-ER muss allerdings keine Struktur innerhalb der Gruppe aufgebaut und gepflegt werden. Auch benötigt SMART-ER weder ein Anonymisierungsnetzwerk, noch wird ein intelligenter Stromzähler mit einer besonderen Rolle betraut. Ein intelligenter Stromzähler kooperiert mit zufällig gewählten oder allen intelligenten Stromzählern seiner Gruppe. Störungen von einzelnen intelligenten Stromzählern führen in SMART-ER zu einer verringerten SM-Reichweite, aber weder zum Totalausfall des Smart Meterings noch zu einem eingeschränkten Privatsphärenschutz.

Auch SMART-ER im direkten Einsatz, sowie SMART-ER in Kombination mit SMSD oder Elderberry sind in Tabelle 3.1 eingetragen. Für eine detaillierte Betrachtung der Verfahren sei hier auf die jeweiligen Kapitel dieser Arbeit verwiesen. Erwähnenswert ist jedoch, dass sowohl SMSD als auch Elderberry auch dann den Privatsphärenschutz gewährleisten, wenn der Auftraggeber über eine große Anzahl von korrumpierten intelligenten Stromzählern verfügt.

Eine tabellarische Aufstellung der besprochenen Arbeiten ist in Tabelle 3.2 gegeben.

3.5.4 Zusammenfassung

Die grundlegenden Ansätze zum Smart Metering zur Stromnetzüberwachung und Produktionsplanung können nicht wie im Smart Metering zur Rechnungslegung auf eine zeitliche Aggregation zurückgreifen. Verwendete Strategien umfassen das Entfernen identifizierender Daten (Abschnitt 3.5.1), die Aggregation über Haushalte hinweg mittels einer vertrauenswürdigen dritten Partei (Abschnitt 3.5.2) und die Aggregation über Haushalte hinweg *ohne* eine vertrauenswürdige dritte Partei. Die Ansätze zur Entfernung von identifizierenden Daten, also Anonymisierung oder Pseudonymisierung, haben einen schwerwiegenden Nachteil: der Detailgrad der resultierenden Daten kann so groß sein, dass eine nachträgliche Zuweisung mittels Sekundärinformationen einfach ist. Das Ausschließen einer nachträglichen Zuweisung, also die Unverknüpfbarkeit der Daten, ist jedoch bei heutigen Möglichkeiten der Informationsbeschaffung schwierig zu realisieren (siehe beispielsweise Jawurek et al. [70]). Die Aggregation über Haushalte hinweg umgeht dieses Pro-

Arbeiten	Kriterien				
	K1[1]	K2[1]	K3[1]	K4[1]	K5[1]
Li et al. [83, 84]	⊖	⊖	⊕	⊖	⊕
Garcia und Jacobs [57]	⊙	⊖	⊙	⊖	⊕
Erkin und Tsudik [46]	⊕	⊖	⊖	⊙	⊙
Gomez Mármol et al. [60, 61]	⊕	⊙	⊕	⊕	⊕
SMART-ER direkt (Kapitel 5)	⊕	⊕	⊕	⊕	⊕
SMART-ER + SMSD[2] (Kapitel 6)	⊕	⊕	⊕	⊕	⊙
SMART-ER + Elderberry[2] (Kapitel 7)	⊕	⊕	⊕	⊙	⊕

[1] ⊕ = Erfüllt (positiv), ⊙ = Teilweise erfüllt (neutral), ⊖ = Nicht erfüllt (negativ)
[2] Privatsphärenschutz auch bei großer Anzahl korrumpierter intelligenter Stromzähler

Tabelle 3.1: *Bewertung der betrachteten Arbeiten.*

blem. Verwendet ein Ansatz jedoch eine vertrauenswürdige dritte Partei, so stellt sich die Frage woraus dieses Vertrauen resultiert. Ansätze ohne vertrauenswürdige Partei stellen daher den vielversprechendsten Weg zum privatsphärengerechten Smart Metering zur Stromnetzüberwachung und Produktionsplanung dar.

3.6 Bewertung des Stands der Forschung

Das Forschungsfeld des privatsphärengerechten Smart Meterings enthält zahlreiche Arbeiten, die *grundlegende Lösungsansätze* vorstellen. Einige zentrale Fragen des Themengebiets werden jedoch nur vereinzelt aufgegriffen und in ihrer Gesamtheit daher nicht beantwortet:

- **Realisierbarkeit der Verfahren** Die meisten Arbeiten lassen eine Evaluation der Durchführbarkeit der vorgeschlagenen Verfahren gänzlich vermissen oder evaluieren nur einen Teilaspekt des vorgestellten Verfahrens. Ressourcenbeschränkte Hardware und niedrige Datenraten der Kommunikationsanbindung sind jedoch wichtiger und häufig angeführter Bestandteil des Smart Metering Szenarios.

Tabelle 3.2: *Vergleich von Ansätzen zur Aggregation über Haushalte ohne vertrauenswürdige dritte Partei.*

Paper	Kryptosystem (Aggregat)	Aggregation durch	Schlüsselverwaltung	Angreifer-modell	Churn behandelt?
Li et al. [83, 84]	Homomorph (Messwerte)	Mehrere intelligente Stromzähler (Aggregationsbaum)	Öffentlicher Schlüssel des Auftraggebers	honest-but-curious	nein
Garcia und Jacobs [57]	Homomorph (Messwerte)	Jeden Stromzähler	Zufällige Schlüssel, PKI	-	nein
Erkin und Tsudik [46]	Homomorph (Messwerte)	Designierten Stromzähler	keine	honest-but-curious	nein
Gomez Mármol et al. [60, 61]	Homomorph (Schlüssel)	Designierten Stromzähler	Zufällige Schlüssel, Aggregation durch designierten Stromzähler	Abhören, korrumpierte Stromzähler	ja
SMART-ER	verbesserte SMART Variante (Messwerte)	Auftraggeber	keine	korrumpierte Stromzähler und Auftraggeber	ja
SMSD	SMART-ER (Messwerte)	Auftraggeber	keine	s.o.	ja
Elderberry	SMART-ER (Messwerte)	Auftraggeber und Stromzähler	keine	s.o.	ja

- **Privatsphärenschutz auch bei Angriffen** Die verwendeten Angreifermodelle beinhalten oft einen schwachen Angreifer, der nicht aktiv in die Geschehnisse eingreift. Teilweise werden sogar der Partei, vor der die Privatsphäre geschützt werden soll, privatsphärentechnisch sensible Aufgaben übertragen. Ob ein vorgeschlagenes Verfahren einem starken Angreifer, möglicherweise mit Kooperation des Auftraggebers des Smart Meterings, standhalten kann, bleibt meist offen.

- **Betrachtung von Churn** Nur sehr selten wird die Zuverlässigkeit der Kommunikationsanbindung der intelligenten Stromzähler betrachtet. Ein Smart Metering Verfahren sollte jedoch auch unter Störungen einzelner intelligenter Stromzähler verwertbare Daten liefern. Ein privatsphärengerechtes Smart Metering sollte dies dann auch weiterhin privatsphärengerecht erreichen.

Kapitel 4

OverGrid

Bei der Erforschung von Smart Metering Protokollen stellt die Evaluation der neuen Protokolle eine Herausforderung dar. Zur Simulation von Stromnetzen existieren zahlreiche Simulationswerkzeuge (beispielsweise NEPLAN [129]). Auch zur Simulation von Kommunikationsprotokollen existieren Simulationswerkzeuge (beispielsweise NS-2 [91] oder OMNeT++ [133] in Kombination mit dem INET Framework [134]). Die Kombination der Simulation von Kommunikationsprotokollen und Stromnetzen ist jedoch ein Forschungsfeld, das erst mit dem Aufkommen der Vision des Smart Grids an Aufmerksamkeit der Forschungsgemeinschaft gewonnen hat. Mit Hilfe der Co-Simulation, also der Kombination von bestehenden Simulationswerkzeugen, wurden Simulationswerkzeuge vorgeschlagen, die eine umfassende Simulation eines Smart Grids und zugehöriger Kommunikationsinfrastruktur ermöglichen (beispielsweise [119]). Durch die Kombination von komplexer Stromnetzsimulation und komplexer Simulation von Kommunikationsinfrastruktur entstehen jedoch Simulationswerkzeuge von immenser Komplexität. Dies wirkt sich negativ auf Skalierbarkeit und Laufzeitverhalten aus.

Zur Evaluation von Protokollen zum Smart Metering ist eine detaillierte Simulation des Stromnetzes nicht nötig. Die elektrotechnisch korrekte Simulation von beispielsweise Spannungsfluktuationen und Frequenzschwankungen übersteigt den nötigen Realismus bei Weitem, wenn das Smart Metering letztlich nur die gemessene Last der intelligenten Stromzähler betrachtet. Aus diesem Grund wurde für diese Arbeit das Simulationswerkzeug *OverGrid* entwickelt. Hierfür wurde ein bestehendes Simulationswerkzeug zur Simulation von Kommunikationsprotokollen um eine abstrakte Stromnetzsimulation erweitert. Als Basis wurde das, am Institut für Telematik entwickelte, Simulationswerkzeug OverSim [4, 5]

und dessen Weiterentwicklung OverArch [7] ausgewählt. Es bietet eine hervorragende Skalierbarkeit und Flexibilität die eine effiziente Simulation und einfache Erweiterbarkeit ermöglichen.

Die wesentlichen neuen Komponenten von Overgrid sind angepasste Churngeneratoren und ein Subsystem zur Stromnetzsimulation. Diese werden im Folgenden beschrieben.

4.1 Angepasste Churngeneratoren

Da OverSim zur Simulation von peer-to-peer Overlayprotokollen entworfen wurde, verfügt es bereits über eine Vielzahl an Möglichkeiten zur Simulation des ständigen Wechsels der am Overlay beteiligten Knoten. Unter dem Begriff *Churn* wird diese Knotenfluktuation zusammengefasst. OverSim bietet Churngeneratoren, die eine flexible Modellierung des gewünschten Churns erlauben. Jedoch sind diese Churngeneratoren für die Evaluation von Overlay-Protokollen entworfen und haben daher nur ein sehr beschränktes Verständnis von Knoten die gerade von Churn betroffen, also vom Kommunikationsnetz getrennt, sind. OverSim simuliert lediglich Knoten, die *nicht* von Churn betroffen sind. Somit profitiert die Skalierbarkeit von OverSim, da eine Simulation mit einer großen Anzahl an Knoten bei hohem Churn deutlich weniger Aufwand verursacht.

Wird durch einen Churngenerator bestimmt, dass ein Knoten von Churn betroffen ist, so wird er vollständig aus der Simulation entfernt. Endet der Einfluss von Churn, so erzeugt der Churngenerator einen gänzlich neuen Knoten. Zwar kann der Zustand des Knotens vor dem Einfluss von Churn persistiert und bei der neuen Initialisierung wieder eingepflegt werden, der Knoten selbst hat aber während seiner Abwesenheit keinen Einfluss mehr auf die Simulation. Auch wird zu Beginn der Simulation der Anteil, der zu diesem Zeitpunkt nicht von Churn betroffenen Knoten, berechnet und nur diese Anzahl an Knoten erzeugt.

Für OverGrid ist dieses Verhalten der Churngeneratoren nachteilig, da ein Knoten auch im Falle einer gestörten Kommunikationsverbindung weiterhin Strom verbrauchen sollte. Wäre dies nicht der Fall, so hätte Churn keine Auswirkung auf die Leistung des Smart Meterings. Da gerade dies Untersuchungsgegenstand ist, muss ein Knoten auch im Falle einer gestörten Kommunikationsverbindung weiterhin Strom verbrauchen.

Daher wurden in OverGrid die Churngeneratoren von OverSim in den folgenden Punkten angepasst:

- Bei einem Churnereignis wird ein Knoten nicht gelöscht oder erzeugt sondern nur dessen Kommunikationsfähigkeit deaktiviert.
- Zu Beginn einer Simulation werden *alle* konfigurierten Knoten erzeugt. Die Kommunikationsfähigkeit der Knoten, für die berechnet wurde, dass sie von Churn betroffen sind, wird deaktiviert.

4.2 Simulation des Stromnetzes

Um für das Smart Metering eine realitätsnahe Datenquelle zu schaffen, wurde eine Erweiterung zur Simulation von Stromnetzen entwickelt. Das Hauptaugenmerk lag dabei auf der Gewinnung von realistischen Verbrauchs- und Produktionswerten für Haushalte und nicht auf der elektrotechnisch exakten Simulation von Stromnetzen. Daher wurde von technischen Details des Stromnetzes abstrahiert und lediglich der Energieverbrauch und die Energieerzeugung einzelner Haushalte betrachtet. Verbraucht ein Haushalt mehr Energie als er erzeugt, so bezieht er den Fehlbetrag aus einem Stromnetz mit (in der Simulation) unendlichem Vorrat. Erzeugt er mehr Energie als er verbraucht, so wird diese in das Stromnetz eingespeist. Der Gesamtbetrag an Energie, der aus oder in das Stromnetz fließt entspricht dabei der Summe der Energieerzeugung und des Energieverbrauchs der einzelnen Haushalte.

Folgende Anforderungen wurden an die Simulation des Stromnetzes gestellt:

- **Realitätsnähe:** Die Simulationen des Stromnetzes sollen Daten erzeugen, die in den Grenzen der gewählten Abstraktionsebene realitätsnah sind.
- **Konfigurierbarkeit:** Der Energieverbrauch und die Energieerzeugung einzelner Haushalte soll konfigurierbar sein.
- **Erweiterbarkeit:** Der Simulator soll modular aufgebaut sein um zukünftige Erweiterungen zu ermöglichen.
- **Komplexität:** Der Rechenaufwand für die Stromnetzsimulation soll so niedrig wie möglich sein.
- **Skalierbarkeit:** Die Simulation soll gut skalierbar sein und eine realistische Anzahl von Haushalten für eine Instanz eines Smart Meterings simulieren können. Wie in Abschnitt 2.1.2 erläutert sind dies bis zu mehrere zehntausend Haushalte.

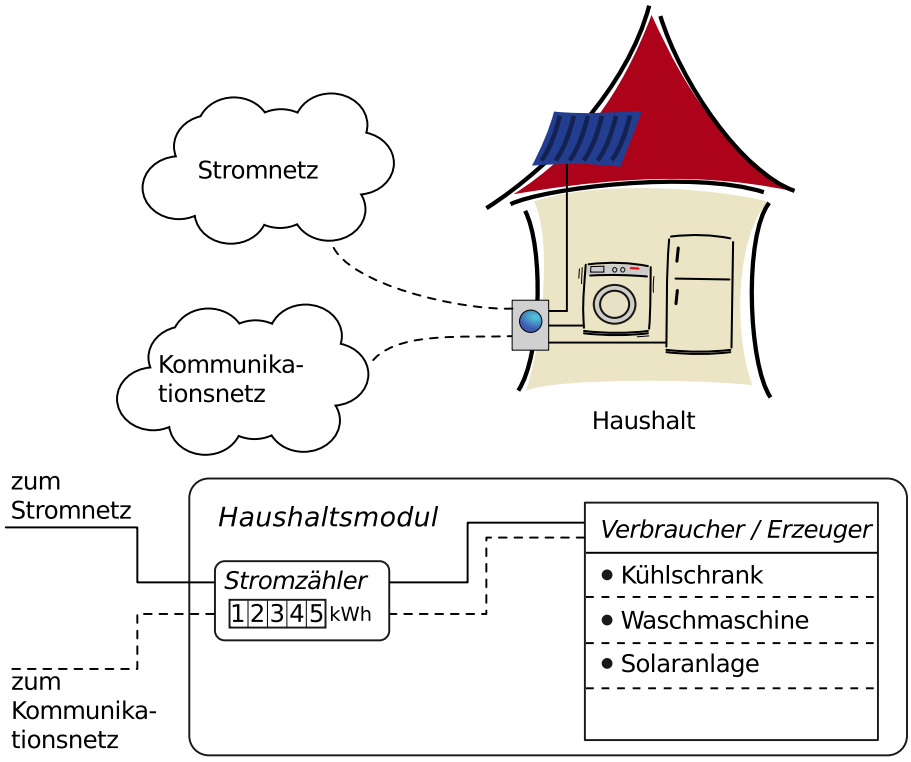


Abbildung 4.1: *Modell eines Haushalts mit Verbrauchern und Erzeugern.*

Die Beschreibung der Stromnetzsimulation gliedert sich in zwei Teile. Zunächst wird die Simulation eines einzelnen Haushalts beschrieben. Danach wird erläutert, wie das Zusammenspiel der Haushalte im Stromnetz funktioniert.

4.3 Simulation eines Haushalts

Im Simulationswerkzeug OverSim verfügt jeder simulierte Knoten über eine Anzahl an Modulen. Die Simulation eines Haushalts ist in solch einem Modul gekapselt, also Bestandteil eines Knotens. Das Haushalts-Modul selbst enthält weitere Module (siehe Abbildung 4.1). Diese sind

- genau einen intelligenten Stromzähler *(erforderlich)*
- und eine beliebige Anzahl an Verbrauchern / Erzeugern *(optional)*

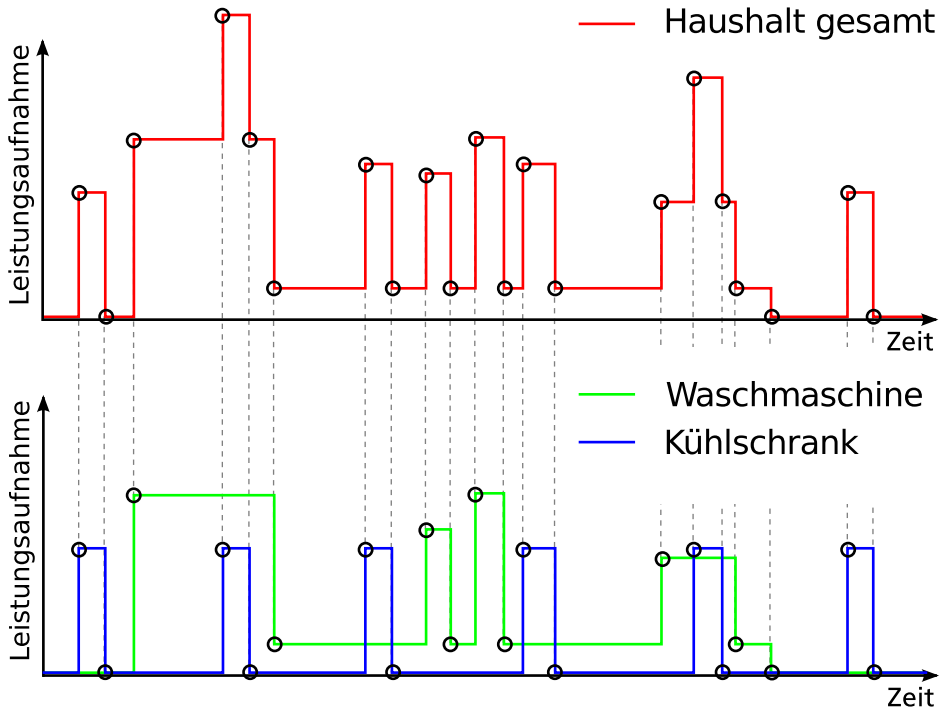


Abbildung 4.2: *Resultierende Leistungsaufnahme und Events.*

Das Stromzähler-Modul stellt die zentrale Schnittstelle des Haushalts dar. Es bietet eine Schnittstelle an, über die Benachrichtigungen über ein Ereignis zur Energieerzeugung oder zum Energieverbrauch gesendet werden. Ein Ereignis ist in diesem Sinne eine Veränderung im Verbrauch oder der Erzeugung. Eine Schreibtischlampe, beispielsweise, könnte beim Einschalten ein $60W$-Ereignis und beim Ausschalten ein $0W$-Ereignis senden. Dieser Mechanismus wird *Power Indication* genannt und erlaubt jedem angeschlossenen Modul die Übermittlung von Power Indication Ereignissen. Der intelligente Stromzähler registriert diese Ereignisse und berechnet den Gesamtverbrauch oder die Gesamterzeugung des Haushalts. Dieser Vorgang ist beispielhaft mit einem Kühlschrank und einer Waschmaschine als Verbraucher in Abbildung 4.2 dargestellt. Auf der x-Achse ist der zeitliche Verlauf und auf der y-Achse die Leistungsaufnahme aufgetragen. Im unteren Schaubild sind die Leistungsaufnahmen des Kühlschranks (blau) und der Waschmaschine (grün) dargestellt. Das obere Schaubild zeigt die Gesamtleistungsaufnahme des Haushalts. Jedesmal wenn einer der Verbraucher eine Veränderung seiner Leistungsaufnahme signalisieren möchte, löst er ein Power Indication Ereignis aus. Diese sind im Schaubild als Kreise dargestellt.

Durch den Power Indication Mechanismus kann OverGrid die Komplexität der Stromnetzsimulation sehr niedrig halten. Nur bei Änderungen im Energieverbrauch fällt Rechenaufwand an, der sich auf einfache arithmetische Operationen beschränkt.

Durch die Ausgestaltung der Verbraucher und Erzeuger als eigenständige OverSim-Module können in OverGrid beliebige Verbraucher und Erzeuger simuliert werden. Diese Funktionalität wurde bereits erfolgreich genutzt um mobile Verbraucher im Rahmen eines Projekts zur Elektromobilität [75] zu untersuchen. Unter der Verwendung von OverSim-Funktionen zur Emulation wäre auch die Anbindung von realen Verbrauchern möglich. OverGrid selbst bietet mit der *BaseConsumer* eine abstrakte Klasse zur einfachen Implementierung von Verbrauchern und Erzeugern. Zusätzlich stellt OverGrid folgende Verbraucher und Erzeuger bereit.

4.3.1 Statischer Verbraucher

Der statische Verbraucher ist eine einfaches Beispiels für einen Verbraucher. Seine einzige Funktion besteht darin, nach der Initialisierung des Simulationswerkzeugs einen konfigurierbaren, konstanten Verbrauch per Power Indication Ereignis anzuzeigen.

4.3.2 Zufälliger Verbraucher

Eine Form des zufälligen Verbrauchers ist in OverGrid mittels des *RandomWalkConsumers* gegeben. Als Eingabeparameter akzeptiert er einen Maximalverbrauch m, eine maximale Schrittweite s und eine maximale Wartezeit t. Nach der Initialisierung signalisiert er einen zufälligen Verbrauch zwischen 0 und m. In gleichverteilt zufälligen Intervallen aus $[0, t]$ führt er danach jeweils einen Schritt einer Zufallsbewegung (Random Walk) zwischen 0 und m aus, wobei die Länge jedes Schritts zufällig zwischen 0 und s liegt.

Der so ausgestaltete Verbraucher erzeugt einen zufälligen Energieverbrauch, der keinem festen Muster entspricht. Er kann vor allem dazu genutzt werden andere Verbraucher zu ergänzen. Ein Beispiel für seine Anwendung wäre die Modellierung eines Fernsehgeräts. Dessen Energieverbrauch besteht einerseits aus einem Grundbedarf, der in eingeschaltetem Zustand immer verbraucht wird, und andererseits aus einem Energiebedarf der von der aktuellen Bildschirmhelligkeit und damit vom eingeschalteten Fernsehprogramm abhängig ist. Liegt nur der

durchschnittliche Energiebedarf des Fernsehgeräts vor, so kann es mittels einer Kombination aus statischem Verbraucher (für den Grundbedarf) und zufälligem Verbraucher (für den variablen Bedarf) modelliert werden.

4.3.3 Profilbasierte Verbraucher und Erzeuger

Um eine genaue Steuerung eines Verbrauchers oder Erzeugers ohne die Entwicklung von OverSim-Modulen zu ermöglichen, wurde in OverGrid eine profilbasierte Variante, der *ProfileConsumer* eingeführt. Dieser Implementierung kann eine XML-Datei übergeben werden, die ein zeitbasiertes Profil enthält. Das Profil enthält Dauer und Wert einer Reihe von Power Indication Ereignissen. Trotz des Namens des Moduls (Profile*Consumer*) können diese Ereignisse auch Energieerzeugung signalisieren. Nachdem diese Ereignisse abgearbeitet wurden, wird wieder mit dem ersten Ereignis angefangen. Zusätzlich zum Profil unterstützt der ProfileConsumer auch eine konfigurierbare Skalierung der Power Indication Ereignisse.

OverGrid liegen bereits mehrere solcher Profile bei:

- Die *VDEW-Profile* enthalten mehrere Profile und entsprechen den gängigen Standardlastprofilen [93]. So ist beispielsweise das Profil für einen Haushalt in der Übergangszeit (März-Mai) verfügbar. Alle Profile sind normiert auf einen Jahresverbrauch von einer Megawattstunde und können mittels der Skalierungsfunktion des ProfileConsumers auf den gewünschten Jahresverbrauch skaliert werden. Somit können Haushalte mit einer unterschiedlichen Anzahl an Bewohnern simuliert werden.

- Das *Solar-Profile* entspricht der normierten Einspeisung einer Photovoltaikanlage im April entsprechend den Daten vom Bundesverband der Energie- und Wasserwirtschaft (BDEW). Es ist ebenfalls auf eine Megawattstunde pro Jahr normiert und kann mit der Skalierungsfunktion angepasst werden.

4.4 Simulation hierarchischer Stromnetze

Die Simulation hierarchischer Stromnetze stellt eine Weiterführung der Konzepte zur Simulation eines Haushalts dar. Jeder intelligente Stromzähler eines Haushalts ist neben seiner eigenen Implementierung der Power Indication Schnittstelle auch Konsument einer Power Indication Schnittstelle. Er agiert also als Verbraucher oder

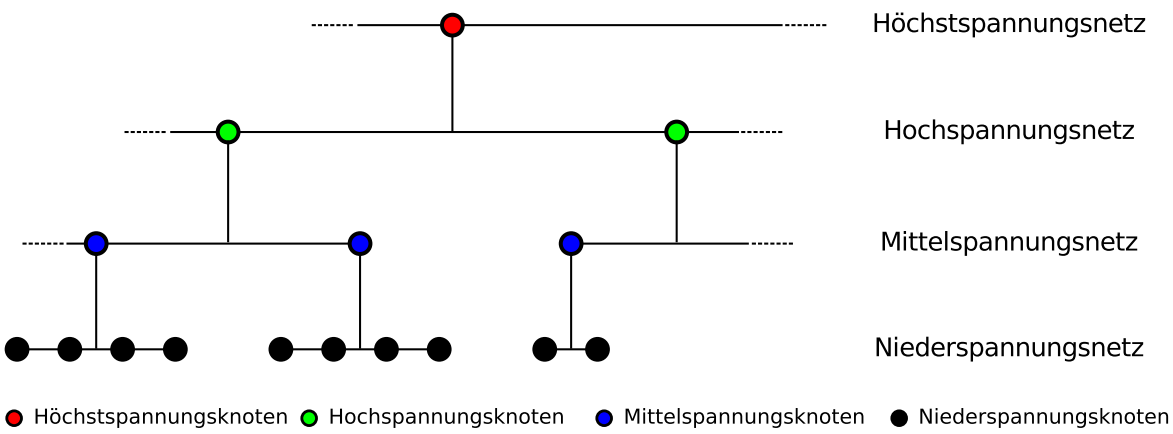


Abbildung 4.3: *Hierarchische Simulation eines Stromnetzes.*

Erzeuger, der an einen übergeordneten intelligenten Stromzähler angeschlossen ist.

Dieser Mechanismus erlaubt die hierarchische Anordnung von intelligenten Stromzählern um verschiedene Segmente und Hierarchien eines Stromnetzes zu simulieren. So kann beispielsweise die Stromnetzhierarchie vom Niederspannungsnetz bis zum Höchstspannungsnetz abgebildet werden (siehe Abbildung 4.3). Auf den Hierarchiestufen kann durch den modularisierten Ansatz Funktionalität implementiert werden, die beispielsweise einen Lastausgleich zwischen den angeschlossenen Teilnetzen durchführt. An der Wurzel der Hierarchie muss immer ein einziger, abschließender intelligenter Stromzähler, das sogenannte *Root Meter* stehen. An diesem Stromzähler kann dann der globale Energieüberschuss oder Energiemangel abgelesen werden.

4.5 Zusammenfassung

In diesem Kapitel wurde das Simulationswerkzeug OverGrid vorgestellt. Es basiert auf dem Open-Source Overlay-Framework OverSim, das international in Forschung und Lehre erfolgreich eingesetzt wird.

Um Protokolle für Smart Metering evaluieren zu können, waren Anpassungen an den Churngeneratoren des Oversim-Frameworks nötig. Diese Anpassungen wurden in das OverSim-Framework aufgenommen und werden bereits in laufenden Arbeiten verwendet und weiterentwickelt.

Die Stromnetzsimulation basiert in OverGrid auf dem Power Indication Mechanismus, der nur dann Rechenaufwand verursacht, wenn Änderungen des Energieverbrauchs auftreten. Die Simulation des Stromnetzes ist mittels eigenständiger Module gelöst, was eine große Flexibilität bei der Entwicklung von Stromnetzszenarien erlaubt.

Mittels, bereits in OverGrid integrierten, Verbrauchs- und Erzeugungsprofilen können realistische Stromverbrauchszenarien einfach implementiert werden. Die Profile stützen sich auf Standardlastprofile von Energieverbänden und können, beispielsweise auf die gewünschte Haushaltsgröße, skaliert werden. Mit OverGrid steht damit ein Simulationswerkzeug zur Verfügung, das die Möglichkeiten zur Kommunikationsnetzsimulation von OverSim bietet und gleichzeitig eine realistische, effiziente Simulation eines Stromnetzes durchführt.

Kapitel 5

Peer-to-peer Privatsphärenschutz

Ein im privatsphärengerechten Smart Metering häufig verwendeter Ansatz zum Privatsphärenschutz ist die Aggregation. Sie kann entweder über die Zeit oder über Haushalte hinweg durchgeführt werden. Eine Aggregation über Zeit hinweg wird beim Smart Metering zur Rechnungslegung durchgeführt und erfordert in der Regel keine Kooperation zwischen einzelnen Haushalten (siehe Abschnitt 3.4). Eine Aggregation über Haushalte hinweg wird im Smart Metering zur Stromnetzüberwachung und Produktionsplanung verwendet und nutzt meistens eine Kooperation zwischen einzelnen Haushalten oder eine vertrauenswürdige dritte Partei (siehe Abschnitt 3.5). Beide Varianten des Smart Metering können unabhängig voneinander eingesetzt werden.

In diesem Kapitel wird SMART-ER, ein Verfahren für privatsphärengerechtes Smart Metering zur Stromnetzüberwachung und Produktionsplanung, vorgestellt. Ziel des Verfahrens ist die Durchführung eines privatsphärengerechten Smart Meterings *ohne* eine vertrauenswürdige dritte Partei. Es basiert auf den Grundlagen des SMART-Verfahrens (siehe Abschnitt 2.3), das in drahtlosen Sensornetzen eingesetzt wird. SMART-ER weist eine geringe Softwarekomplexität auf und benötigt keine komplexen kryptographischen Operationen. Auch wurde im Entwurf des SMART-ER-Verfahrens das Problem unzuverlässiger intelligenter Stromzähler und Kommunikationsverbindungen berücksichtigt. SMART-ER enthält Mechanismen, die auch bei Störungen von Stromzählern oder Kommunikationsinfrastruktur für eine weitestgehende Funktionalität des Smart Meterings sorgen.

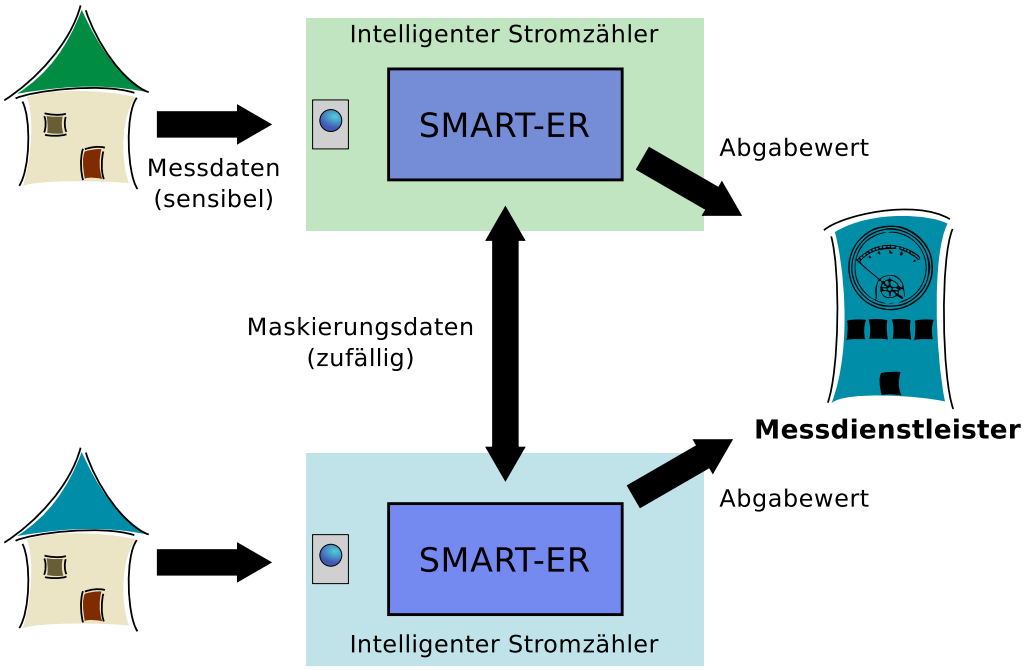


Abbildung 5.1: *Informationsfluss im SMART-ER-Verfahren.*

In SMART-ER kooperieren intelligente Stromzähler um ihre *Messwerte* zu maskieren. Ein Messwert ist beispielsweise die vom Stromzähler gemessene Last, mit der ein Haushalt gerade Energie aus dem Stromnetz bezieht. Dieses Vorgehen ist in Abbildung 5.1 illustriert. Die intelligenten Stromzähler tauschen untereinander *Maskierungsdaten* in Form von sogenannten *Fragmenten* aus. Diese Maskierungsdaten werden zufällig generiert und enthalten dabei keine Informationen über den Messwert. Sie werden aber dazu genutzt, die Messwerte in maskierte Messwerte, sogenannte *Abgabewerte* umzuwandeln. Mittels dieser Abgabewerte können dann die Daten privatsphärengerecht an den Messdienstleister übertragen werden. Dieser kann aus den einzeln übertragenen Abgabewerten nicht mehr auf die ursprünglichen Messwerte schließen. Dennoch ist sichergestellt, dass die Summe der übertragenen Abgabewerte, das sogenannte Aggregat, der Summe der ursprünglichen Messwerte entspricht.

Der Zusatz ER in SMART-ER steht für die wesentlichen Entwurfsziele:

- **E**xakte Smart Metering Ergebnisse. Das von SMART-ER ermittelte Aggregat über die Messwerte der intelligenten Stromzähler muss sich für eine weitere Verwendung, beispielsweise zur Extrapolation, eignen. Ein Aggregat, das von SMART-ER ermittelt wurde, darf keinen Fehler enthalten.

- **R**obuste Smart Metering Ergebnisse. Das Smart Metering soll auch bei Störungen der intelligenten Stromzähler oder deren Kommunikationsanbindung weitestgehend funktionsfähig bleiben.

Beide Ziele stehen dabei in einer Abhängigkeit voneinander. Beim real eingesetzten Smart Metering ist von sporadischen Störungen der Kommunikationsverbindung oder der intelligenten Stromzähler auszugehen. Zu einem beliebigen Zeitpunkt ist also nur eine Teilmenge der intelligenten Stromzähler funktions- oder kommunikationsfähig. Die nicht funktions- oder kommunikationsfähigen intelligenten Stromzähler können nicht im Rahmen des Smart Metering gemessen werden. Das kombinierte Entwurfsziel ist also ein robustes und exaktes Smart Metering Ergebnis, das über eine größtmögliche Zahl an intelligenten Stromzählern eine fehlerfreie Aussage triff. Mittels Extrapolation kann dann auch eine Aussage über die Gesamtmenge an intelligenten Stromzählern getroffen werden [108].

Um diese Ziele zu erreichen wurde der SMART Algorithmus erweitert. Die neu eingeführten Konzepte sind:

Fragmentierungsmechanismus Es wurde ein neuer Fragmentierungsmechanismus auf Basis des Restklassenrings $\mathbb{Z}/q\mathbb{Z}$ entworfen. Er gewährleistet den Schutz der Privatsphäre gegenüber anderen intelligenten Stromzählern und dem Messdienstleister. Auch eine Kooperation zwischen anderen intelligenten Stromzählern und dem Messdienstleister stellt keine Gefahr für die Privatsphäre dar, sofern mindestens ein intelligenter Stromzähler der Gruppe nicht mit dem Messdienstleister kooperiert.

Vorgezogener Fragmentaustausch Der neue Fragmentierungsmechanismus ermöglicht einen geänderten zeitlichen Ablauf des Verfahrens. Das Austauschen von Fragmenten ist nun nicht mehr vom Messwert abhängig und kann deshalb schon durchgeführt werden, bevor dieser überhaupt gemessen wurde. Hierdurch kann früher als bei SMART, nämlich bereits kurz nach dem Messzeitpunkt, mit der Übermittlung der Ergebnisse begonnen werden.

Abhängigkeitsverfolgung: Sendet ein intelligenter Stromzähler Fragmente an einen anderen Stromzähler, so entsteht eine Abhängigkeit von diesem Stromzähler. Kann dieser seinen Abgabewert nicht an den Messdienstleister senden, so ist auch das Fragment verloren. Diese Abhängigkeit wird vom sendenden Stromzähler vermerkt und bei der Abgabe des Abgabewerts dem Messdienstleister mitgeteilt.

Abhängigkeitsauflösung: Der Messdienstleister nutzt die Ergebnisse der Abhängigkeitsverfolgung um eine Überprüfung der abgegebenen Abgabewerte durchzuführen. Können die Abhängigkeiten eines Abgabewerts nicht erfüllt werden, so entfernt er den Abgabewert.

Gruppenbildung: Mittels einer Einteilung der intelligenten Stromzähler in Gruppen wird ein Ausbreiten der Abhängigkeiten eingedämmt. Ein fehlender Abgabewert hat so nur Auswirkungen auf die Gruppe und niemals auf die Gesamtheit der intelligenten Stromzähler.

Der weitere Verlauf des Kapitels ist folgendermaßen strukturiert. Zunächst werden in Abschnitt 5.1 die getroffenen Annahmen und benutzten Variablen vorgestellt. In Abschnitt 5.2 werden die Schwächen des SMART-Verfahrens bezüglich des Einsatzes im Smart Metering analysiert und eine Generalisierung der zu Grunde liegenden mathematischen Zusammenhänge vorgenommen. Diese bilden die Basis für Teile des Entwurfs des SMART-ER-Verfahrens, das in Abschnitt 5.3 vorgestellt wird. Insbesondere werden die Änderungen im Vergleich zu SMART diskutiert. Anschließend folgt in Abschnitt 5.4 eine Evaluierung des durch SMART-ER garantierten Privatsphärenschutzes. Es wird gezeigt, dass der Privatsphärenschutz von SMART-ER auch dann gewährleistet ist, wenn der Messdienstleister, andere intelligente Stromzähler oder der Messdienstleister und andere intelligente Stromzähler korrumpiert sind. In Abschnitt 5.5 wird eine Evaluation der Smart Metering Leistung durchgeführt und gezeigt, dass die eingeführten Mechanismen, bei vernachlässigbarem Mehraufwand für Kommunikation, stets zu fehlerfreien Smart Metering Ergebnissen führen. Abschließend wird in Abschnitt 5.6 das Kapitel zusammengefasst.

5.1 Annahmen und Variablen

Zur näheren Betrachtung wird im Folgenden eine Instanz eines Smart Meterings zur Stromnetzüberwachung und Produktionsplanung angenommen. Diese Instanz eines Smart Meterings könnte beispielsweise von einem Energielieferanten mittels eines Messdienstleisters durchgeführt werden, um den Energieverbrauch der eigenen Kunden zeitnah verfolgen zu können. Ziel des Smart Meterings ist die Überwachung einer Menge von intelligenten Stromzählern Z in regelmäßigen Intervallen von 15 Minuten. Diese werden *Messintervalle* $M = \{m_1, \ldots\}$ genannt. Es wird angenommen, dass die intelligenten Stromzähler zur Einhaltung dieser

Tabelle 5.1: *Verwendete Variablen.*

Eigenschaft	Ausprägung / Variable
Menge der Zähler	$Z = \{z_1, \ldots, z_n\}$
Messintervalle	$M = \{m_1, \ldots\}$ der Länge 15 Minuten
Überwachte Eigenschaft	Leistungsaufnahme $P(z_i, m_j)$
Ergebnisse	Menge der Zähler mit Abgabewerten $Z_{m_j}^{(A)} \subseteq Z$
	Leistungsaufnahme $P(Z_{m_j}^{(A)}, m_j) = \sum P(z_i, m_j)$
	mit $z_i \in Z_{m_j}^{(A)}, m_j \in M$

Messintervalle über grob (±1 Sekunde) synchronisierte Echtzeituhren verfügen. Innerhalb eines Messintervalls existiert ein fester *Messzeitpunkt*, zu dem die intelligenten Stromzähler ihren Messwert für diesen Messzeitpunkt bestimmen. In dieser Arbeit wird angenommen, dass dieser zu Beginn des Messintervalls eintritt. Startet das Messintervall m_1 beispielsweise um 0 Uhr, so ist auch der Messzeitpunkt um 0 Uhr. Der nächste Messzeitpunkt wäre dann ein Messintervall, also 15 Minuten, später. Die Messgröße ist die von den intelligenten Stromzählern gemessene Leistungsaufnahme zum Messzeitpunkt eines zugehörigen Haushaltes: $P(z, m)$ mit $z \in Z$ und $m \in M$. Durch äußere Umstände ist es möglich, dass ein intelligenter Stromzähler aus der Menge Z für ein Messintervall m_j keine Daten liefert. Dies kann beispielsweise durch eine Störung der Kommunikationsinfrastruktur oder durch einen Hardwaredefekt verursacht werden. Daher umfasst die Teilmenge $Z_{m_j}^{(A)} \subseteq Z$ alle intelligenten Stromzähler in Z, die für das Messintervall m_j einen Abgabewert abgeben konnten. Der beobachtete Wert des Smart Meterings ist somit für jedes Messintervall die gesamte Leistungsaufnahme der intelligenten Stromzähler, die in der Lage waren Daten beim Messdienstleister abzuliefern: $P(Z_{m_j}^{(A)}, m_j)$. Dies entspricht der Summe $\sum P(z, m_j)$ mit $z \in Z_{m_j}^{(A)}$. Zusätzlich zur beobachteten Messgröße wird ebenfalls die Beteiligung der intelligenten Stromzähler ermittelt. So stellt neben $P(Z, m_j)$ auch die Menge $Z_{m_j}^{(A)} \subseteq Z$ ein Ergebnis des Smart Meterings dar. Die Variablen des Smart Meterings sind nochmals in Tabelle 5.1 aufgeführt.

Es wird davon ausgegangen, dass sowohl die Kommunikation zwischen intelligenten Stromzählern als auch zwischen Stromzählern und Messdienstleister mittels eines zuverlässigen Transportprotokolls (beispielsweise TCP [107] oder SCTP [126]) erfolgt und entsprechende Verbindungen nach Bedarf auf- und abge-

baut werden. Wie in Abschnitt 2.1.4 motiviert, wird angenommen, dass Integrität, Authentizität und Vertraulichkeit dieser Kommunikation durch den Einsatz entsprechender Verfahren (beispielsweise TLS [111] oder QUIC [115]) sichergestellt wird.

5.2 Analyse und Generalisierung des SMART-Verfahrens

Um im Kontext von privatsphärengerechten Smart Metering Anwendungen, wie beispielsweise Produktionsplanung, eingesetzt werden zu können, müssen die Ergebnisse des Smart Meterings

- privatsphärengerecht ermittelt werden,
- hinreichend exakt sein und
- zeitnah eintreffen.

Mittels der erhobenen Daten werden Entscheidungen getroffen, die weitreichende Auswirkungen technischer und wirtschaftlicher Natur haben können. Fehlerhafte Produktionsplanung kann nicht nur die Netzstabilität negativ beeinflussen, sondern auch zu finanziellen Verlusten führen.

Das SMART-Verfahren stellt mit seiner geringen Softwarekomplexität ein vielversprechendes Verfahren zur privatsphärengerechten Datenaggregation dar. Es hat jedoch zwei wesentliche Nachteile, die einen Einsatz im Smart Metering verhindern:

- Der vorgeschlagene Fragmentierungsmechanismus schützt die Privatsphäre nur ungenügend
- Ein Verlust von Fragmenten sorgt für ein verfälschtes Ergebnis

Der Mechanismus zur Fragmentierung aus der Veröffentlichung von He et al. [66] nutzt für die Berechnung der Fragmente den Messwert. Dies ist aus informationstheoretischer Sicht bedenklich. Ein Einfluss der Messwerte auf die Fragmente kann Rückschlüsse auf die Messwerte durch Beobachten der Fragmente erlauben. Der vorgeschlagene Mechanismus erlaubt in der Tat diese Rückschlüsse. Bei der Berechnung der Fragmente gilt für alle Fragmente $p_{ij} \leq p_i$. Jedes Fragment ist kleiner oder gleich dem Messwert. Anhand eines Fragments kann also ein Minimum für den Messwert p_i bestimmt werden. Beim vorgeschlagenen Mechanismus zur Berechnung von negativen Fragmenten gilt dann auch $|p_{ij}| \leq 2p_i$.

Dies ist allerdings kein Problem des grundsätzlichen Algorithmus. Im Folgenden wird gezeigt, dass die mathematischen Grundlagen des Verfahrens große Freiheiten für das Vorgehen zur Fragmentierung und Aggregation erlauben. Anschließend wird anhand eines Beispiels die Generalisierung angewandt.

Um die Operationen zur Aggregation und Fragmentierung zu ermöglichen wird eine abelsche Gruppe, wie beispielsweise $(\mathbb{Z}, +)$, benötigt. Dabei gewährleistet die Gruppeneigenschaft „Existenz von inversen Elementen“, dass eine Fragmentierung möglich ist. Um die Aggregation unabhängig von der Reihenfolge durchzuführen, wird die Gruppeneigenschaft „Assoziativität“ und die Kommutativität der abelschen Gruppe benötigt. Im Folgenden sei W die Gruppe und $\oplus$ die kommutative Verknüpfung.

Die Aggregation dient dazu eine beliebige Menge an Datenfragmenten zu einem Datum zusammenzufassen. Ihre Definitionsmenge ist also

$$\mathscr{P}_{\text{fin}}(W) := \{M \subseteq W\} \text{ mit endlichem } \quad |M|$$

die Potenzmenge der endlichen Teilmengen von W. Die Aggregation ist dann als Abbildung $\mathscr{A} : \mathscr{P}_{\text{fin}}(W) \to W$ definiert mit:

$$\begin{aligned} \mathscr{A}(\{w\}) &= w & w &\in W \\ \mathscr{A}(\{w_1, w_2, \ldots, w_n\}) &= w_1 \oplus w_2 \oplus \ldots \oplus w_n & \forall n > 1, w_1 \ldots w_n &\in W \end{aligned}$$

Durch die Kommutativität und Assoziativität von $\oplus$ kann $\mathscr{A}$ in beliebiger Reihenfolge und auch auf Teilmengen von $\{w_1, ..., w_n\}$ angewendet werden.

Damit die Funktion $\mathscr{A}$ zur privatsphärengerechten Aggregation verwendet werden kann, darf sie nicht invertierbar sein. Aus einem Aggregat darf also nicht hervorgehen, welche Einzelwerte zum Endergebnis beigetragen haben. Auch dürfen mittels einem Aggregat keine Rückschlüsse auf die eingegangenen Einzelwerte, wie beispielsweise Anzahl oder Verteilung, gezogen werden können. Es muss also gelten, dass für ein vorliegendes Aggregat $x \in W$ alle endlichen Teilmengen von W, deren Aggregat ebenfalls x ergibt, gleich wahrscheinlich sind.

Passend zur Aggregation $\mathscr{A}$ muss eine Abbildung zur Fragmentierung $\mathscr{F}$ existieren mit $\mathscr{F} : W \to \mathscr{P}_{\text{fin}}(W)$.

Es muss gelten:

$$\mathscr{A}(\mathscr{F}(w)) = \mathscr{A}(\{w_1, \ldots, w_n\} = w \quad \forall w \in W.$$

Wenn alle Werte, die aus einer Fragmentierung des Wertes w mittels der Fragmentierungsfunktion $\mathscr{F}$ hervorgegangen sind, mittels der Aggregationsfunktion $\mathscr{A}$ wieder zusammengefasst werden, so ist das Ergebnis wieder der ursprüngliche Wert w.

Wie bereits erwähnt ist die Fragmentierbarkeit eines Elements $w \in W$ durch die Gruppeneigenschaft „Existenz von inversen Elementen“ gegeben. Mittels der inversen Elemente lässt sich für beliebige abelsche Gruppen ein Element w folgendermaßen in n Elemente $w_1, \ldots, w_n$ zerlegen:

- Wähle $n-1$ zufällige Elemente $r_1, \ldots, r_{n-1} \in W$.
- Bestimme die Inversen der zufälligen Elemente $r_1, \ldots, r_{n-1}$ bezüglich der Gruppe $(W, \oplus)$. Diese seien $inv_\oplus(r_1), \ldots, inv_\oplus(r_{n-1}) \in W$. Die Funktion $inv_\oplus(x)$ bestimmt dabei das Inverse von x bezüglich der Operation $\oplus$. Somit ist $inv_\oplus(x) \oplus x$ das neutrale Element der Gruppe.
- Die ersten $n-1$ Werte entsprechen dann $r_1, \ldots, r_{n-1}$. Der letzte Wert berechnet sich wie folgt: $w \oplus inv_\oplus(r_1) \oplus \ldots \oplus inv_\oplus(r_{n-1})$

Beispiel: Die aktuelle Leistungsaufnahme eines Haushaltes kann durch eine ganze Zahl in Watt angegeben werden. Damit kann die kommutative Gruppe $(\mathbb{Z}, +)$ mit gewöhnlicher Addition verwendet werden. Sei 800 die aktuelle Leistungsaufnahme eines Haushaltes in Watt. Dieser Wert soll in 5 Fragmente aufgeteilt werden. Hierzu werden die 4 Zufallszahlen $(195, -206, 1990, -798)$ bestimmt. Die Inversen bezüglich Addition dieser Zufallszahlen sind $(-195, 206, -1990, 798)$. Die 5 Fragmente bestehen nun aus den vier Zufallszahlen und zusätzlich aus dem Aggregat des Messwertes und der Inversen aller Zufallszahlen: $800+(-195)+206+(-1990)+798 = -381$. Zur Rekonstruktion des Messwerts wird Kenntnis aller 5 Fragmente und der Aggregationsfunktion benötigt. Das Aggregat dieser Fragmente ergibt genau die Leistungsaufnahme: $\mathscr{A}(195, -206, 1990, -798, -381) = 800$

Falls alle Fragmente im endgültigen Aggregat enthalten sind, ist sichergestellt, dass der Messwert im endgültigen Aggregat enthalten ist. Dabei ist die Reihenfolge und die Anzahl an Zwischenschritten der Aggregation irrelevant. Auch das Aggregieren von zusätzlichen Fragmenten anderer Herkunft in etwaigen Zwischenschritten stellt kein Problem dar. Es muss allerdings gewährleistet werden, dass auch die Fragmente anderer Herkunft vollzählig in das endgültige Aggregat aggregiert werden.

Der Austausch von Fragmenten dient dazu die Werte des einzelnen Knotens während der Übertragung zu maskieren. Der Austausch von Fragmenten findet über eine Menge von anderen Knoten statt. Jeder Knoten teilt sein gemessenes Datum w in $n+1$ Fragmente $\mathscr{F}(w) = \{w_1, \ldots, w_{n+1}\}$ auf. Dabei entspricht n der Anzahl der vorgesehenen Empfänger. Das Aggregat $\mathscr{A}(\mathscr{F}(\{w_1, \ldots, w_{n+1}\}))$ entspricht, gemäß den Vorschriften der Fragmentierung, dem gemessenen Datum w. Die einzelnen Fragmente werden an n verschiedene Empfänger versendet, wobei jeder Empfänger genau ein Fragment erhält. Das letzte Fragment behält der Knoten selbst. Maskieren heißt hier insbesondere, dass die Kenntnis von weniger als $n+1$ Fragmenten nicht ausreicht um auf den ursprünglichen Messwert zu schließen. Der Messwert kann erst durch Kenntnis *aller* Fragmente wiederhergestellt werden.

Im zweiten Schritt aggregiert jeder Knoten das zurückbehaltene, eigene und fremde, empfangene Fragmente mittels der Aggregationsfunktion $\mathscr{A}$ zu einem einzigen Wert. Allein aus diesem Wert können die aggregierten Werte nicht mehr ermittelt werden, da die Aggregationsfunktion $\mathscr{A}$ nicht invertierbar ist und auch keine Rückschlüsse auf die eingegangenen Teilwerte erlaubt. Dieser Abgabewert wird von jedem Knotens im dritten Schritt an die Datensenke geschickt, welche wiederum mittels $\mathscr{A}$ eine Aggregation aller empfangenen Aggregate vornimmt. Das Ergebnis ist dann die Summe der eingeflossenen Ursprungswerte.

Die hier durchgeführte Generalisierung der mathematischen Grundlagen ermöglicht nun große Freiheiten bei der Wahl der abelschen Gruppe und dem zugehörigen Fragmentierungsmechanismus. Diese werden im Entwurf des SMART-ER-Verfahrens genutzt.

Unabhängig vom Privatsphärenschutz betrachtet das SMART-Verfahren nicht den sporadischen Ausfall von Kommunikationsinfrastruktur oder den Ausfall der Knoten selbst. Kann ein Knoten das Aggregat der zurückbehaltenen und empfangenen Fragmente nicht zur Datensenke senden, so ist das Endergebnis verfälscht. Besonders schwer wiegt, dass der Grad der Verfälschung nicht verlässlich abschätzbar ist. Insbesondere kann nicht davon ausgegangen werden, dass der Verlust der Daten eines oder mehrerer Knoten durch eine Abschätzung kompensiert werden kann. Dies stellt einen Widerspruch zu den Anforderungen des Smart Meterings dar.

5.3 SMART-ER

In diesem Abschnitt werden die Aspekte von SMART-ER detailliert behandelt. Zuerst wird in Abschnitt 5.3.1 die abelsche Gruppe $\mathbb{Z}/q\mathbb{Z}$ und der zugehörige Fragmentierungsmechanismus von SMART-ER geschildert. Es folgt der geänderte zeitliche Ablauf des Verfahrens in Abschnitt 5.3.2. Die Auswahl der Fragmentempfänger durch jeden intelligenten Stromzähler wird in Abschnitt 5.3.3 behandelt. Die Abhängigkeitsverfolgung und -auflösung wird in Abschnitt 5.3.4 betrachtet. Abschließend wird die Gruppenbildung in Abschnitt 5.3.5 erläutert. Die Implementierung von SMART-ER wird abschließend in Abschnitt 5.3.6 behandelt.

5.3.1 Abelsche Gruppen und Fragmentierung

Motivation für einen neuen Fragmentierungsmechanismus in SMART-ER ist der Schutz der Privatsphäre. Im Speziellen soll ein unbeabsichtigter Informationsfluss durch die Fragmente selbst ausgeschlossen werden. Dies impliziert, dass die Berechnung der Fragmente nicht vom Messwert abhängen darf. Wie bereits in Abschnitt 5.2 eingeführt, ist ein Fragmentieren mittels zufällig gewählten Elementen der abelschen Gruppe möglich. Da ein Informationsfluss durch die Fragmente ausgeschlossen werden soll, muss jedes mögliche Fragment mit der gleichen Wahrscheinlichkeit auftreten. Die Beobachtung eines bestimmten Fragments hätte somit keinen Informationsgehalt, da die Beobachtung jedes anderen Fragment mit der gleichen Wahrscheinlichkeit möglich wäre. Der Ausschluss eines Informationsflusses ist daher dann gewährleistet, wenn Fragmente mit gleicherverteilter Wahrscheinlichkeit aus den Elementen der zu Grunde liegenden abelschen Gruppe gezogen werden. In einer realistischen Implementierung ist dies nicht für eine Gruppe mit unendlich vielen Elementen durchführbar. So ist es beispielsweise nicht möglich zufällig und gleichverteilt ein Element der ganzen Zahlen zu wählen.

Die naheliegende Lösung wäre ein Intervall festzulegen, innerhalb dessen die Zufallszahlen gleichverteilt gezogen werden können. Beispielsweise wäre ein Intervall $[0, 2000]$ denkbar. Doch die zufällige Wahl mittels eines Intervalls verursacht zwei Probleme:

(1) Ist der geheim zu haltende Wert im Vergleich zum Intervall sehr groß, so kann der Abgabewert Restinformation enthalten. So würde im obigen Beispiel ein Wert von 100 000 kaum von einer kleinen Zahl aus- und eingehenden

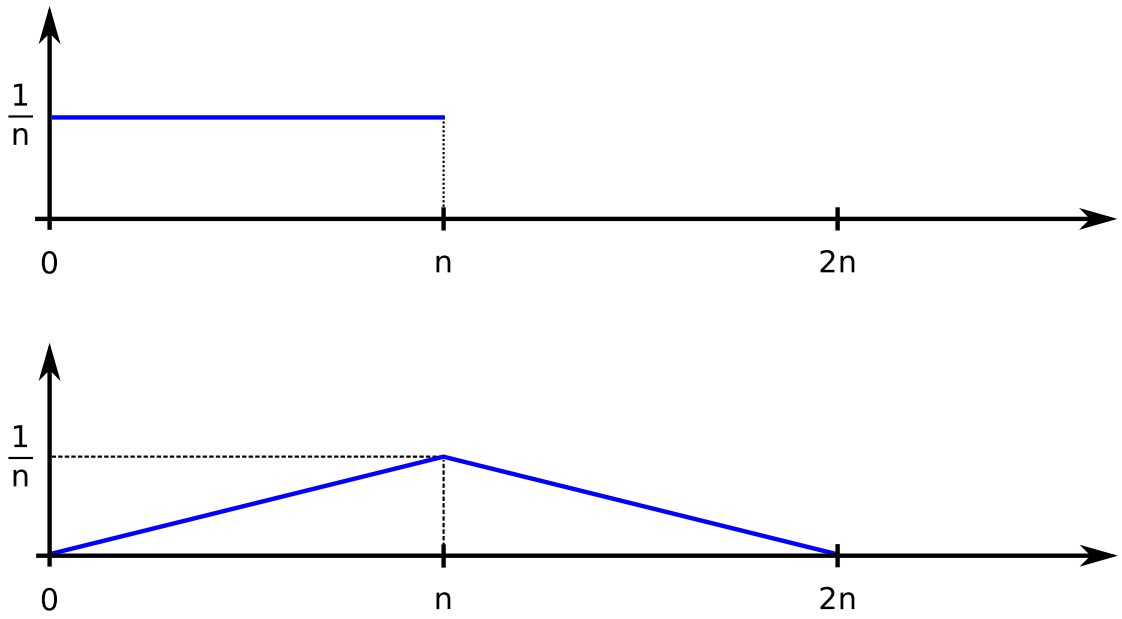


Abbildung 5.2: *Dichtefunktion einer gleichverteilten Zufallsvariable im Intervall* $[0, n]$ *(oben) und Dichtefunktion einer Zufallsvariable die aus der Summer zweier solcher entsteht (unten).*

Fragmenten beeinflusst werden. Der Abgabewert würde auf einen exzessiv hohen Wert hindeuten.

(2) Eine Summenbildung der Fragmente würde die Verteilung der gleichverteilt gezogenen Zufallszahlen verändern. So ist bereits die Verteilung der Summe zweier solcher Zufallszahlen nicht mehr gleichverteilt. Zur Illustration sei auf die Darstellung als Dichtefunktion in Abbildung 5.2 verwiesen. Für ein Fragment gilt die Gleichverteilung. Jeder Wert im Intervall $[0, n]$ ist gleich wahrscheinlich. Für die Summe zweier Fragmente gilt dies bereits nicht mehr. Beispielsweise ist der Wert $2n$ nur dann möglich, wenn zwei mal n gezogen wurde. Für den Wert n gibt es jedoch eine Vielzahl an Möglichkeiten. Eine Summe an den Rändern des neu entstandenen Intervalls $[0, 2n]$ ist somit wesentlich weniger wahrscheinlich als in der Mitte.

Um diese Probleme zu vermeiden, verwendet SMART-ER als Grundmodell die endliche abelsche Gruppe des Restklassenrings $\mathbb{Z}/q\mathbb{Z}$, also die ganzen Zahlen modulo q mit gewöhnlicher Addition. Durch die endliche Anzahl an Elementen ermöglicht diese Gruppe eine gleichverteilte, zufällige Wahl eines Elements. Durch die Summenbildung modulo q wird sichergestellt, dass auch bei Aufsummierung

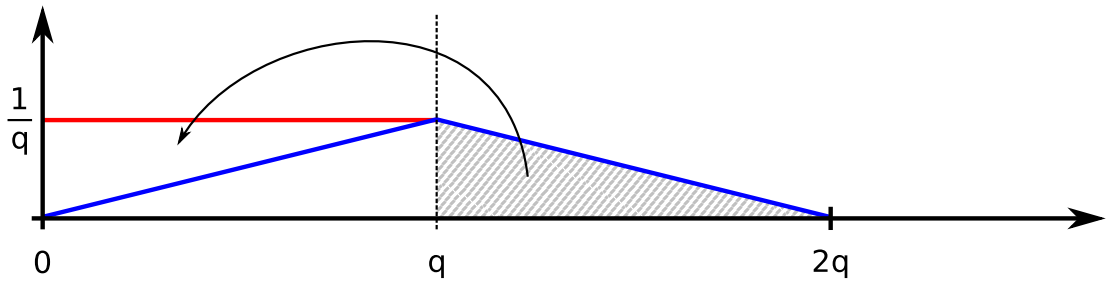


Abbildung 5.3: *Resultierende Dichtefunktion (rot) einer Addition bei gleichverteilten Zufallsvariablen aus $\mathbb{Z}/q\mathbb{Z}$ und entsprechender Summenbildung.*

die Gleichverteilung bestehen bleibt. Anschaulich ist dies mittels der resultierenden Dichtefunktion in Abbildung 5.3 dargestellt. Werte, die über das Intervall hinausgehen, werden durch das Modulo-Rechnen wieder in denselben Wertebereich abgebildet. Die resultierende Dichtefunktion (rot eingezeichnet) ist damit wieder die einer Gleichverteilung. Denn sind X, Y zwei unabhängig, identisch gleichverteilte Zufallsvariablen, also $P(X = a) = P(Y = a) = \frac{1}{q}$ für alle $a \in \mathbb{Z}/q\mathbb{Z}$, so gilt

$$P(X + Y = a) = \sum_{b \in \mathbb{Z}/q\mathbb{Z}} P(X = b) \cdot P(Y = a - b) = q \cdot \frac{1}{q} \cdot \frac{1}{q} = \frac{1}{q}.$$

Dies liegt daran, dass in $\mathbb{Z}/q\mathbb{Z}$ für jedes $a \in \mathbb{Z}/q\mathbb{Z}$ genau ein $l \in \mathbb{Z}/q\mathbb{Z}$ existiert mit $l = a - b$. Wären X und Y gleichverteilt auf einem Intervall $[0, n] \subseteq \mathbb{Z}$, so wäre dies nicht der Fall.

Der neue Fragmentierungsmechanismus wird realisiert, wie bereits in 5.2 für beliebige abelsche Gruppen eingeführt. Um ein Fragment zu erzeugen, wird ein zufälliges $r \in \mathbb{Z}/q\mathbb{Z}$ bestimmt. Bei der Berechnung des Abgabewerts muss das Inverse von r auf den Messwert addiert werden. Dies entspricht in $\mathbb{Z}/q\mathbb{Z}$ einer einfachen Subtraktion mit r. Empfangene Fragmente müssen aufaddiert werden. In Abbildung 5.4 ist der Vorgang des Empfangs und des Versands von Fragmenten nochmals anschaulich mit $q = 2^{32}$ dargestellt. Jeder Pfeil in der Abbildung entspricht einem Fragment und die jeweilige Länge des Pfeils entspricht dem Wert aus $\mathbb{Z}/q\mathbb{Z}$ des Fragments. Die Pfeile auf dem äußeren Rand des Zahlenraums entsprechen den empfangenen Fragmenten. Die Pfeile im Inneren des Zahlenraums entsprechen den versendeten. Die Farbe des jeweiligen Pfeils stellt dabei einen anderen intelligenten Stromzähler da. Der betrachtete intelligente Stromzähler hat

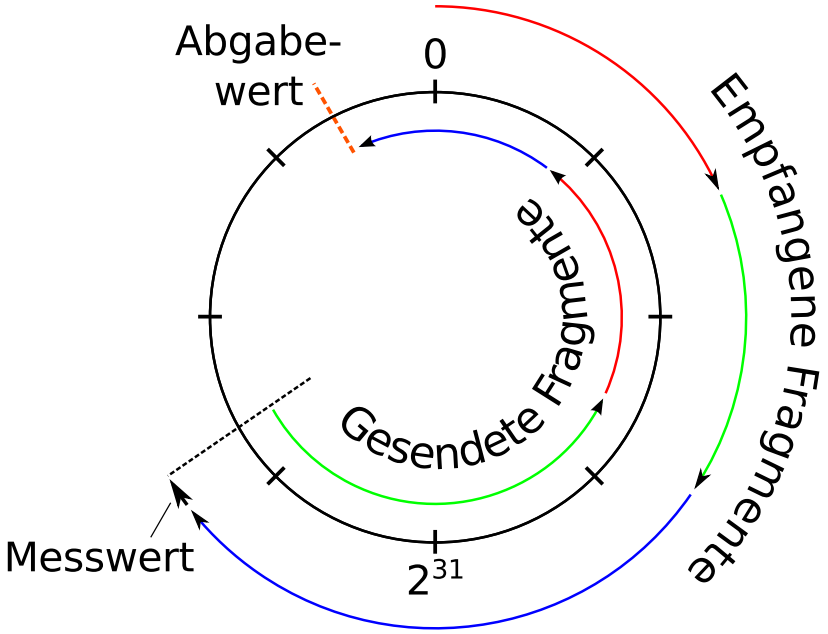


Abbildung 5.4: *Empfang (außen) und Versand (innen) von Fragmenten im Restklassenring $\mathbb{Z}/2^{32}\mathbb{Z}$.*

mit den Stromzählern rot, grün und blau Fragmente getauscht. Er addiert die empfangenen Fragmente und seinen Messwert auf. Dann subtrahiert er die von ihm versendeten Fragmente. Dass es dabei zu einem Ganzzahlunterlauf kommt ist ohne Relevanz. Er wird bei der späteren Aggregation durch die anderen intelligenten Stromzähler ausgeglichen.

Bei der Wahl von q, also der Größe des Restklassenrings, ist zu beachten, dass keine Werte größer oder gleich q dargestellt werden können. Da sich Fragmente im finalen Aggregat der Abgabewerte gegenseitig auslöschen, ist die Wahl von q für deren Berechnung irrelevant. Da aber die Summe der Messwerte darstellbar sein sollte, muss q nicht nur größer als jeder Messwert, sondern auch größer als die maximale Summe ausfallen. Ebenfalls muss in Betracht gezogen werden, ob negative Summen möglich sind. In Regionen mit starker Verbreitung von dezentraler Energieerzeugung, beispielsweise Photovoltaikanlagen auf Häuserdächern, wäre dies vorstellbar. Daher sollte ein entsprechend großer Bereich am Ende des darstellbaren Zahlenraums als negative Zahlen interpretiert werden.

Für die Wahl von q bietet sich eine Zweierpotenz an, da die Berechnungen dann von Prozessoren effizient durchgeführt werden können. Dies gilt besonders dann, wenn q der Berechnungsbreite der arithmetischen Einheit des verwendeten Pro-

zessors entspricht. Der entstehende Ganzzahlüberlauf realisiert dann automatisch die nötige Modulo-Berechnung ohne negative Einflüsse auf die Leistung.

Für die in dieser Arbeit durchgeführte Evaluation wurde für q der Wert 2^{32} verwendet. Daraus resultiert ein maximaler Wert von ungefähr vier Milliarden. Dabei wird das letzte Viertel des Zahlenraums als negativ interpretiert. Wird Watt als Einheit verwendet, so umfasst der darstellbare Zahlenraum die Werte von ungefähr -1 Gigawatt bis ungefähr 3 Gigawatt. Damit reicht der negative Zahlenraum aus um ungefähr die Einspeisung eines kleinen Kernkraftwerks zu erfassen [16]. Besonders im Hinblick auf die im späteren Abschnitt 5.3.5 erläuterte Gruppenbildung ist dieser Zahlenraum mehr als ausreichend.

5.3.2 Zeitlicher Ablauf

Durch den geänderten Fragmentierungsmechanismus können alle Fragmente erzeugt werden ohne den Messwert zu kennen. Auch muss dieser nicht bekannt sein, um den Austausch von Fragmenten vorzunehmen. Ebenfalls ist es nicht nötig die Anzahl der benötigten Fragmente im Voraus zu bestimmen. Ein neues Fragment lässt sich bei Bedarf jederzeit erzeugen und hängt von keinen weiteren Parametern ab. Hieraus resultiert ein geänderter zeitlicher Ablauf, der eine frühere Abgabe des Messwertes ermöglicht.

Der neue Ablauf des Verfahrens aus der Sicht eines einzelnen intelligenten Stromzählers gliedert sich dabei in folgende Phasen. Diese sind in Abbildung 5.5 grafisch dargestellt.

(1) Start des Verfahrens

(2) Austausch von Fragmenten mit anderen intelligenten Stromzählern

(3) Bestimmen des Messwertes und Berechnen des Abgabewertes

(4) Senden des Abgabewerts an die Datensenke

Es ergibt sich ein zeitlicher Vorteil gegenüber SMART. Die zeitintensive Kommunikation zwischen den einzelnen intelligenten Stromzählern kann nun zeitlich *vor* dem Messzeitpunkt durchgeführt werden. Nachdem der Messwert bestimmt wurde, kann sofort ein Abgabewert berechnet und an die Datensenke übermittelt werden. Im Gegensatz zum SMART-Verfahren erreicht das SMART-ER-Verfahren die gleiche Smart Metering Latenz (siehe Abschnitt 2.1.2), die ein nicht privatsphärengerechtes Verfahren auch erreicht. Bezüglich der Latenz entsteht also *kein Nachteil*

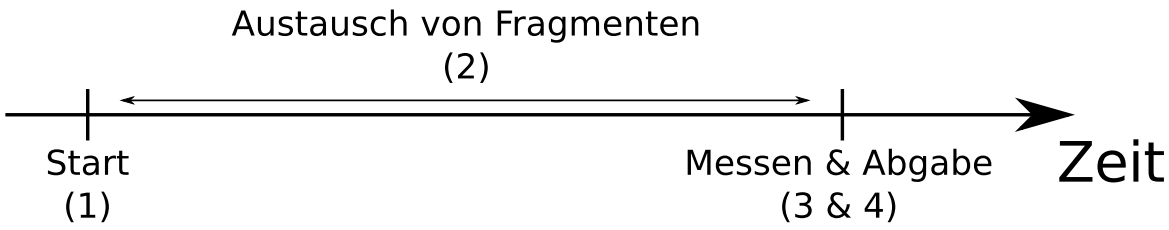


Abbildung 5.5: *Zeitlicher Ablauf des SMART-ER-Verfahrens.*

durch den Einsatz von SMART-ER gegenüber einem nicht privatsphärengerechten Verfahren.

Auf das kürzeste mögliche Messintervall hat der geänderte zeitliche Ablauf jedoch keine Auswirkung. Sowohl in SMART als auch in SMART-ER muss der Fragmentaustausch vorgenommen werden, bevor eine Abgabe an den Messdienstleister durchgeführt werden kann. Die Dauer des Fragmentaustauschs stellt also die Untergrenze für ein Messintervall dar.

5.3.3 Auswahl der Fragmentempfänger

Im SMART-Verfahren wählt ein Knoten die Empfänger der Fragmente anhand ihrer Erreichbarkeit über die Funkschnittstelle aus. Dies ist in dem hier betrachteten Smart Metering Szenario nicht möglich, da alle intelligenten Stromzähler über das Internet gleichermaßen erreichbar sind. Es wäre möglich eine Auswahl der Empfänger aufgrund der Kommunikationslatenz durchzuführen, jedoch müsste diese dann vor einer Auswahl bestimmt werden. In dieser Arbeit wird daher davon abgesehen. Alle intelligenten Stromzähler kommen gleichermaßen als mögliche Empfänger von Fragmenten in Frage.

Konkret bedeutet dies, dass der Messdienstleister jeden intelligenten Stromzähler mit einer Liste der potentiellen Fragmentempfänger inklusive IP-Adresse ausstattet[1]. Jeder intelligente Stromzähler wählt dann in jedem Messintervall zufällig eine konfigurierbare Anzahl J an anderen intelligenten Stromzählern aus dieser Liste aus, an die er Fragmente versendet.

[1] Wie in Abschnitt 5.3.5 erläutert wird, umfasst diese Liste *nicht* alle intelligenten Stromzähler des Smart Meterings

5.3.4 Abhängigkeitsverfolgung und -auflösung

Um das Entwurfsziel der fehlerfreien Smart Metering Ergebnisse zu erfüllen ist eine nähere Betrachtung der entstehenden Abhängigkeiten nötig. Im Folgenden wird ein Messintervall m_j einzeln betrachtet. Zur besseren Lesbarkeit wird daher auf den Index m_j in beispielsweise $Z^{(A)}_{m_j}$ verzichtet und lediglich $Z^{(A)}$ geschrieben. Das Folgende gilt für alle $m_j \in M$.

Zur Betrachtung der Abhängigkeiten wird die Relation $\rightsquigarrow$ als „sendet Fragment an“ definiert: Falls für die intelligenten Stromzähler $z_i, z_j \in Z$ gilt $z_i \rightsquigarrow z_j$, dann sendet z_i ein Fragment an z_j. Hierdurch entstehen zwei Abhängigkeiten zwischen z_i und z_j. Bedingt durch die Berechnung des Abgabewertes a_i von z_i, ist dieser nur gültig, wenn auch der Abgabewert a_j von z_j, in das Aggregat der Abgabewerte eingeht. Fehlt a_j, so fehlt auch das von z_i gesendete Fragment. Das selbe gilt auch für die Gültigkeit von a_j. Dieses enthält das empfangene Fragment, das von z_i gesendet wurde. Ohne a_i führt a_j zu fehlerhaften Ergebnissen im Aggregat der Abgabewerte, da das Fragment nicht ausgeglichen wird. Um ein korrektes Aggregat der Abgabewerte zu garantieren, muss also gewährleistet werden, dass entweder a_i und a_j, oder keines von beiden in die Berechnung eingeht. Um dies zu ermöglichen enthält der Abgabewert jedes intelligenten Stromzählers in SMART-ER neben dem Wert auch eine Liste an intelligenten Stromzählern. Sie enthält jeden Stromzähler, an den ein Fragment gesendet wurde oder von dem ein Fragment empfangen wurde.

Die Abhängigkeit zweier intelligenter Stromzähler voneinander sei mit der Relation „hängt ab von“ ($\leftrightsquigarrow$) definiert. Sie ist die symmetrische, reflexive, transitive Hülle der Relation $\rightsquigarrow$ auf der Menge der intelligenten Stromzähler Z. ($\leftrightsquigarrow$) ist also die von ($\rightsquigarrow$) erzeugte Äquivalenzrelation.

Es ist zu erwarten, dass ein Großteil der beteiligten intelligenten Stromzähler erfolgreich am Smart Metering teilnimmt. Dennoch kann es vorkommen, dass beispielsweise durch Probleme in der Kommunikationsinfrastruktur einzelne intelligente Stromzähler vom senden eines Abgabewerts abgehalten werden. Daher sei $Z^{(A)} \subseteq Z$ die Teilmenge der teilnehmenden intelligenten Stromzähler, die ihren Abgabewert an die Datensenke übermitteln konnten. Die Aufgabe der Datensenke ist nun, aus den übermittelten Abgabewerten der intelligenten Stromzähler $Z^{(A)}$ ein fehlerfreies Ergebnis für eine möglichst große Teilmenge von $Z^{(A)}$ zu berechnen. Im Speziellen bedeutet dies, dass ungültige Abgabewerte entfernt werden müssen. Hierzu sucht die Datensenke die größte Teilmenge von intelligenten Stromzählern

$Z^{(V)} \subseteq Z^{(A)}$, so dass keine Abhängigkeit von einem $z_i \in Z^{(V)}$ zu einem $z_j \notin Z^{(V)}$ existiert. Daher sei $Z^{(V)}$ definiert als:

$$Z^{(V)} = \{z_i \in Z^{(A)} \mid \forall z_j \in Z : z_i \nleftrightarrow z_j \Rightarrow z_j \in Z^{(A)}\}$$

Es ist zu zeigen, dass für alle $z_i \in Z^{(V)}$ und $z_j \in Z$ gilt, dass $z_i \nleftrightarrow z_j \Rightarrow z_j \in Z^{(V)}$. Dies wird im Folgenden durch einen Widerspruchsbeweis gezeigt:

Angenommen es existiert ein $z_i \in Z^{(V)}$ und ein $z_j \in Z \setminus Z^{(V)}$ mit $z_i \nleftrightarrow z_j$.

Durch die Konstruktion von $Z^{(V)}$ folgt aus der Annahme, dass $z_j \in Z^{(A)}$. Da aber $z_j \notin Z^{(V)}$ muss ein z_k existieren mit $z_k \in Z \setminus Z^{(A)}$ und $z_j \nleftrightarrow z_k$. Da $z_i \nleftrightarrow z_j$ und $z_j \nleftrightarrow z_k$ folgt durch die Transitivität von ($\nleftrightarrow$), dass $z_i \nleftrightarrow z_k$. Da aber $z_k \notin Z^{(A)}$ folgt, dass $z_i \notin Z^{(V)}$. Dies stellt einen Widerspruch zur Annahme dar.

Es bleibt lediglich zu zeigen, dass $Z^{(V)}$ die größtmögliche Teilmenge ist, die das gewünschte Kriterium erfüllt. Diese Eigenschaft folgt jedoch direkt, denn jeder $z_i \in Z^{(A)} \setminus Z^{(V)}$ hängt von einem anderen intelligenten Stromzähler ab, der nicht in $Z^{(A)}$ ist. □

Um also zum bestmöglichen, fehlerfreien Smart Metering Ergebnis zu kommen, muss die Datensenke die symmetrische, reflexive, transitive Hülle der übermittelten Abhängigkeiten berechnen. Diese kann beispielsweise mittels des Floyd-Warshall-Algorithmus in $\Theta\left(n^3\right)$ ermittelt werden (siehe beispielsweise Cormen et al. [27], Kapitel 25). Danach entfernt die Datensenke alle Abgabewerte, deren daraus folgende Abhängigkeiten nicht erfüllt werden konnten. Die verbleibenden werden dann aggregiert und bilden das Ergebnis.

Zur Illustration des Effekts der Abhängigkeitsverfolgung und -auflösung wurde die Gruppenbildung, die im Folgenden erläutert wird, in SMART-ER deaktiviert und ein Tagesablauf des Smart Meterings der Leistungsaufnahme von 500 Haushalten aufgezeichnet. Churn wurde entsprechend Abschnitt 5.5.3 konfiguriert und jeder intelligente Stromzähler versendete vier Fragmente ($J = 4$). Bei jedem Versand wurde der Empfänger zufällig aus den 499 anderen intelligenten Stromzählern ausgewählt. Das Ergebnis dieser Simulation ist in Abbildung 5.6 zu sehen. Die x-Achse stellt die Tageszeit dar, beginnend mit 0 Uhr. Auf der y-Achse ist in Kilowatt einmal das Aggregat des Messdienstleisters nach der Abhängigkeitsauflösung, also das Smart Metering Ergebnis (rot), die tatsächliche Leistungsaufnahme (grün) und die Differenz, der Messfehler (blau) aufgetragen. Das Smart Metering Ergebnis der Anschaulichkeit wegen als Kurve eingezeichnet. Tatsächlich existieren Messwerte

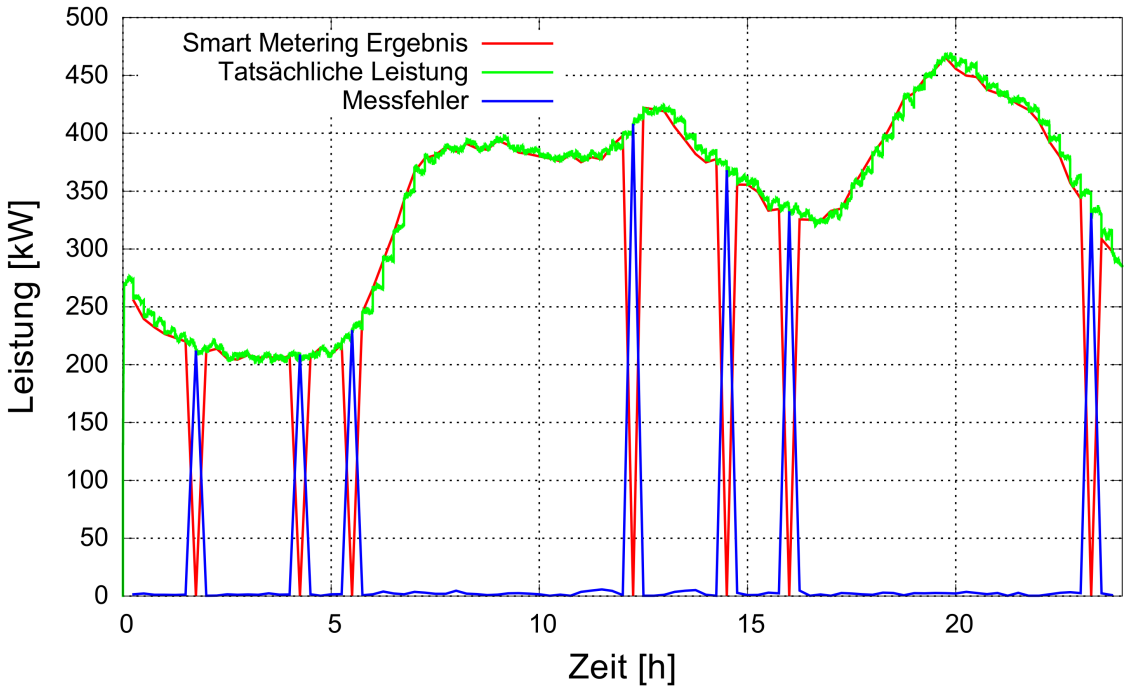


Abbildung 5.6: *Tagesverlauf eines Smart Meterings von 500 Haushalten mittels SMART-ER bei deaktivierter Gruppenbildung.*

immer nur für das jeweilige Messintervall, also als Punkte in 15 Minuten Abständen. Auch der Messfehler wurde nur in diesen Intervallen berechnet.

Ein positiver Messfehler bedeutet, dass das Smart Metering Ergebnis geringer als die tatsächliche Leistungsaufnahme war. Ein negativer Messfehler würde ein zu hohes Smart Metering Ergebnis bedeuten. Die Abhängigkeitsverfolgung und -auflösung resultiert in einem fehlerfreien Ergebnis, das aber nur eine Teilmenge der intelligenten Stromzähler beinhalten. Der Messfehler in der Abbildung ist daher stets positiv. Wenn ein Messfehler entsteht, so ist er auf nicht gesendete oder entfernte Abgabewerte zurückzuführen. Im Graph ist auch ein Problem zu erkennen, das alleine durch die Abhängigkeitsverfolgung und -auflösung nicht lösbar ist. An mehreren Zeitpunkten im Tagesverlauf kam es zu einem Smart Metering Ergebnis von 0 Kilowatt. Damit entspricht der Messfehler exakt der tatsächlichen Leistung. Die Ursache und Lösung zu diesem Problem wird im nächsten Abschnitt behandelt.

5.3.5 Gruppenbildung

Durch die Abhängigkeitsverfolgung kann nun sichergestellt werden, dass für eine Teilmenge der intelligenten Stromzähler ein fehlerfreies Ergebnis vorliegt und der Messfehler genau den Messwerten der Stromzähler entspricht, die nicht in dieser Teilmenge enthalten sind. Betrachtet man einen einzelnen intelligenten Stromzähler z_i, so ist die durch die Äquivalenzrelation ($\leftrightsquigarrow$) definierte Äquivalenzklasse von z_i gegeben durch:

$$[z_i] = \{z_j \in Z \mid z_i \leftrightsquigarrow z_j\}$$

Gilt für einen intelligenten Stromzähler $z_j \in [z_i]$, dass er keinen Abgabewert abgeben konnte, so ist auch der Abgabewert von allen anderen Stromzählern in $[z_i]$ ungültig.

Durch Transitivität und zufällige Wahl von anderen intelligenten Stromzählern kann $[z_i]$ sehr groß werden. Besonders durch die Transitivität kann durch den Versand eines Fragments eine Abhängigkeit zwischen zwei bisher unabhängigen Mengen an intelligenten Stromzählern hergestellt werden. Dadurch ist es durchaus möglich, dass eine Äquivalenzklasse fast alle oder alle Stromzähler umfasst. In Simulationen war dies bereits beim Versand von zwei Fragmenten ($J = 2$) sehr häufig der Fall ($> 99\%$ der Messintervalle). In den durchgeführten Simulationen für $J > 2$ umfassten alle Äquivalenzklassen stets alle intelligenten Stromzähler.

Geht ein Abgabewert verloren, so führt die Abhängigkeitsauflösung eine Bereinigung der Abgabewerte durch. Dabei werden die Abgabewerte der intelligenten Stromzähler entfernt, die in der Äquivalenzklasse des Stromzählers sind dessen Abgabewert verloren ging. Bei einer sehr großen Äquivalenzklasse ist die verbleibende Menge an intelligenten Stromzählern, über die eine fehlerfreie Aussage getroffen werden kann, dann sehr klein oder gar leer. Dieses Phänomen trat in Abbildung 5.6 mehrmals im Tagesverlauf auf.

Um dieses Problem zu vermeiden verwendet SMART-ER eine Gruppenbildung. Die Menge der intelligenten Stromzähler wird in disjunkte Teilmengen (Gruppen) $\{G_1, \ldots, G_n\}$ mit der gleichen Anzahl g an intelligenten Stromzählern pro Gruppe aufgeteilt. Jeder intelligente Stromzähler wird dabei einer Gruppe $G_i \subseteq Z$ zugewiesen. Die Anzahl der intelligenten Stromzähler pro Gruppe g wird als *Gruppengröße* bezeichnet. Lässt sich $|Z|$ nicht ohne Rest in Gruppen der Größe g einteilen, so wird der Rest über alle Gruppen gleichmäßig verteilt. Eine Gruppe hat also mindestens Größe g und höchstens Größe $2g - 1$. Ist $|Z|$ im Vergleich zu g sehr groß,

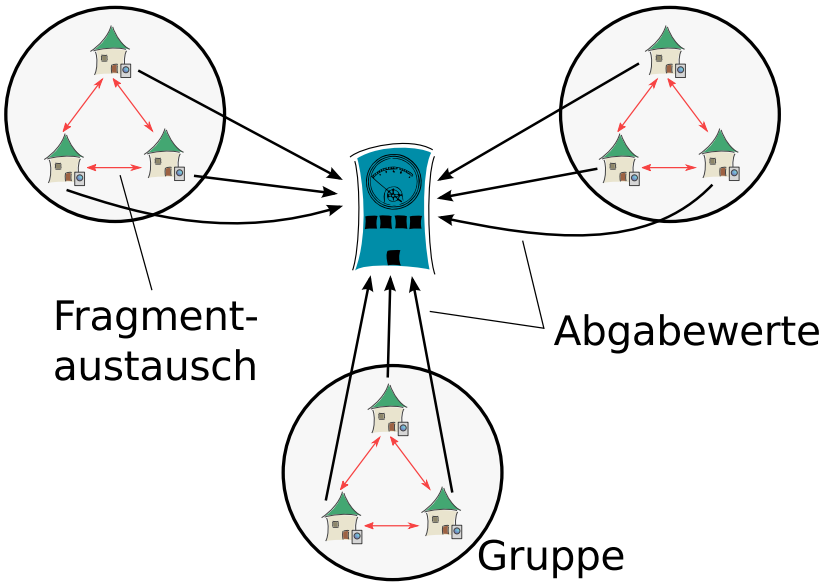


Abbildung 5.7: *Gruppenbildung in SMART-ER. Fragmentierung (rot) innerhalb der Gruppe und einzelne Abgabe (schwarz).*

haben fast alle Gruppen Größe g und wenige Gruppen Größe $g+1$. Die zufällige Wahl von J Fragmentempfängern findet dann nicht mehr unter der Menge aller Stromzähler, sondern nur noch unter den anderen Gruppenmitgliedern statt.

Dieses Vorgehen ist in Abbildung 5.7 dargestellt. Die Einteilung der intelligenten Stromzähler in Gruppen ist hier durch die Kreise symbolisiert. Innerhalb der Gruppe werden Fragmente ausgetauscht. Dies wird durch rote Pfeile dargestellt. Die Abgabe der aggregierten Werte findet für jeden intelligenten Stromzähler einzeln statt (schwarze Pfeile).

Durch die Gruppenbildung wird sichergestellt, dass $\forall z \in G_i : [z] \subseteq G_i$. Es wird also verhindert, dass die Äquivalenzklasse ungehindert anwachsen kann. Die Äquivalenzklasse eines intelligenten Stromzählers kann mit Gruppenbildung maximal die gesamte Gruppe umfassen. Wie bereits erwähnt ist dies schon für kleine J der Fall. Der Verlust eines Abgabewertes beeinflusst also in der Regel die gesamte Gruppe des betroffenen intelligenten Stromzählers. Stromzähler in anderen Gruppen werden von dem Verlust nicht beeinflusst.

Die Anzahl der intelligenten Stromzähler in einer Gruppe hängt von der Einteilung in Gruppen ab. Da ein Privatsphärenschutz in einer Gruppe mit lediglich einem einzelnen intelligenten Stromzähler nicht vorhanden wäre, muss für jede Gruppe gelten, dass sie mindestens zwei intelligente Stromzähler enthält. Für

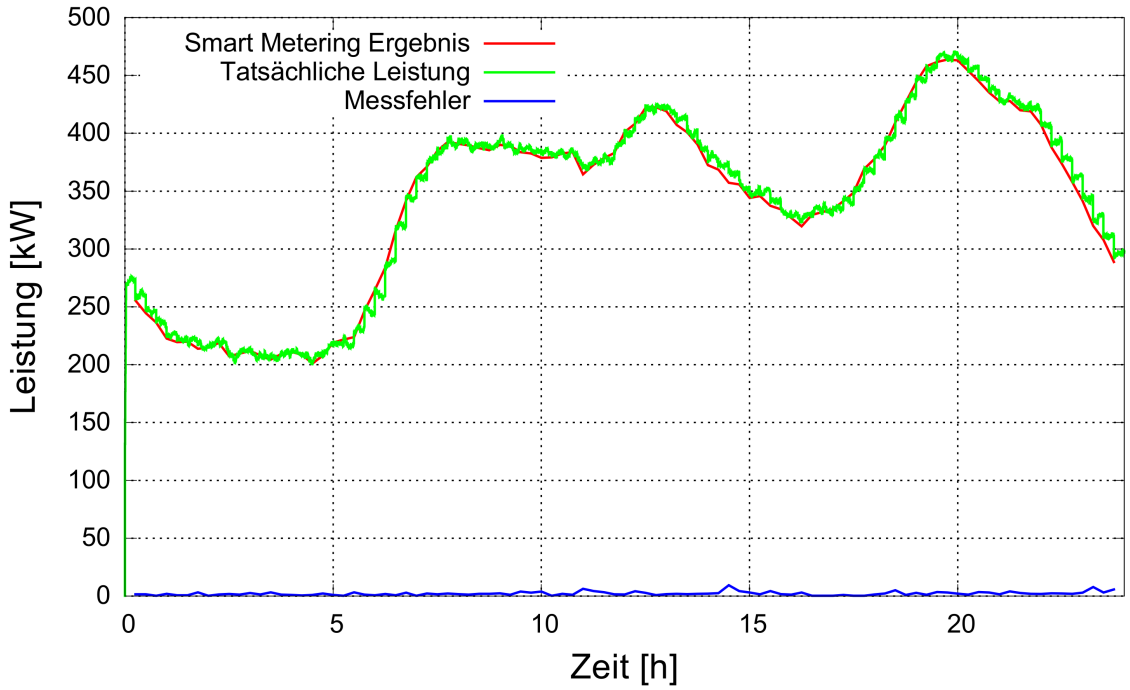


Abbildung 5.8: *Tagesverlauf eines Smart Meterings von 500 Haushalten mit aktivierter Gruppenbildung sowie aktivierter Abhängigkeitsverfolgung und -auflösung.*

einen realen Einsatz ist durchaus denkbar, dass diese Mindestgruppengröße zum besseren Privatsphärenschutz höher gesetzt wird und ein intelligenter Stromzähler die Teilnahme verweigert, wenn ihm kleinere Gruppen zugewiesen werden.

Mit einer größeren Anzahl an intelligenten Stromzählern in einer Gruppe wächst auch die Äquivalenzklasse. Kleinere Gruppengrößen sind daher weniger empfindlich bei Churn, können jedoch bedenklich für den Privatsphärenschutz sein. Dieser Sachverhalt wird in Abschnitt 5.4 näher betrachtet.

Zur Illustration sei nochmals ein Tagesverlauf wie in Abbildung 5.6 gezeigt. Die Parametrisierung ist dieselbe, also mit $J = 4$. Jedoch wurde zusätzlich eine Gruppenbildung von jeweils fünf intelligenten Stromzählern pro Gruppe durchgeführt. Ein intelligenter Stromzähler versendete also an alle anderen intelligenten Stromzähler seine Gruppe Fragmente. Wie in Abbildung 5.8 gut zu sehen ist, tritt das Phänomen der 0-Kilowatt-Ergebnisse nicht mehr auf. Ausfälle von intelligenten Stromzählern sind in ihrem Einfluss auf die einzelnen Gruppen beschränkt. Die Äquivalenzklasse eines intelligenten Stromzählers kann die Gruppengrenzen nicht überschreiten. Das Smart Metering Ergebnis trifft nun zuverlässig eine

Tabelle 5.2: *SMART-ER Protokollparameter.*

Parameter	Variable
Gruppenmitglieder	$G \subseteq Z$
Anzahl zu versendender Fragmente	$J \in \mathbb{N}^+$
Maximaler Fragmentwert	$I \in \mathbb{N}^+$

fehlerfreie Aussage über eine sehr große Teilmenge der teilnehmenden intelligenten Stromzähler. Der Messfehler besteht nur noch aus den Messwerten der intelligenten Stromzähler, die nicht in der Teilmenge enthalten sind. Das Smart Metering Ergebnis eignet sich damit für eine Extrapolation auf die Gesamtmenge der teilnehmenden intelligenten Stromzähler.

5.3.6 Implementierung

Wie in Abschnitt 5.3.2 beschrieben kann in SMART-ER das Austauschen von Fragmenten schon vor der Bestimmung des Messwertes erfolgen. Daher ist es nötig den Start des Verfahrens festzulegen. Da nach dem Messzeitpunkt eine sofortige Abgabe stattfindet, bestimmt der Start des Verfahrens auch automatisch die Dauer des Verfahrens. In dieser Implementierung wird die Dauer auf 10 Sekunden gesetzt um der benötigten Dauer für den Verbindungsaufbau und etwaigen Sendewiederholungen Rechnung zu tragen.

Jedem intelligenten Stromzähler steht eine Liste der Gruppenmitglieder G zur Verfügung. Sie wird vom Messdienstleister mittels Partitionierung von Z errechnet. Der Parameter J bestimmt die Anzahl an zu versendenden Fragmenten. Dabei muss $J \leq |G| - 1$ gelten. Zur besseren Vergleichbarkeit in der späteren Evaluation wurde für diese SMART-ER Implementierung die Möglichkeit einer Beschränkung des Fragmentwerts mittels des Parameters I implementiert. Wird er nicht explizit gesetzt, so gilt $I = 2^{32}$. Die Protokollparameter von SMART-ER sind nochmal in Tabelle 5.2 zusammengefasst.

Der Ablauf auf einem intelligenten Stromzähler ist wie folgt (siehe Algorithmus 1). Zu Beginn wird die Menge der Abhängigkeiten auf die leere Menge und der zu übertragende Wert p auf 0 initialisiert. Beim Beginn des Verfahrens, also zum Messzeitpunkt minus Schutzzeit, wählt der intelligente Stromzähler aus seiner Gruppe G eine Teilmenge der Größe J aus. Für jeden gewählten intelligenten Stromzähler n wird ein neues Fragment aus der Menge $\{0, \ldots, I\}$ gezogen

Algorithmus 1 SMART-ER Client.

```
G ← Set of group members
J ← number of Fragments to send out
loop
    D ← ∅
    p ← 0
    repeat
        sleep 1
    until currentTime() == submitTime() −10
    M ← selectRandomNodes(G, J)
    for all n ∈ M do
        f ← genRandomFrag()
        sendFrag(n,f)
        D ← D ∪ {n}
        p ← p − f
    end for
    repeat
        (f, n) ← receiveSlice()          ▷ f = fragment, n = sending node
        p ← p + f
        D ← D ∪ {n}
    until currentTime() == submitTime()
    p ← p+ measurePower()
    submitToSink(p, D)
end loop
```

und diesem zugeschickt. Zusätzlich wird n in die Menge der Abhängigkeiten D aufgenommen. Das gesendete Fragment wird von p abgezogen. Jedes empfangene Fragment wird auf p aufaddiert und der Sender in D aufgenommen. Ist der Zeitpunkt des Messintervalls erreicht, so wird die Leistungsaufnahme gemessen und auf p aufaddiert. Danach wird p zusammen mit D an den Messdienstleister gesendet.

Der Messdienstleister empfängt Abgabewerte samt Abhängigkeiten von intelligenten Stromzählern. Dabei werden die empfangenen Abgabewerte nicht sofort aufaddiert, sondern zwischengespeichert. Er wartet, vom Messzeitpunkt an, eine Schutzzeit von 10 Sekunden auf eintreffende Daten. Diese Schutzzeit existiert um bei kurzfristigen Kommunikationsproblemen, beispielsweise Paketverlusten, genügend Zeit für Sendewiederholungen zu haben. Nachdem die Schutzzeit abgelaufen

ist, überprüft der Messdienstleister anhand der Abhängigkeiten die Gültigkeit der Abgabewerte (siehe Abschnitt 5.3.4) und verwirft ungültige Abgabewerte. Die verbleibenden Abgabewerte werden aggregiert. Dem Auftraggeber der Smart Metering Instanz übermittelt der Messdienstleister dann

- die Menge der intelligenten Stromzähler die zum aggregierten Wert beigetragen haben ($= Z^{(V)}$)
- den aggregierten Wert $P(Z^{(V)})$
- die Menge der intelligenten Stromzähler, die zwar Abgabewerte übermitteln konnten, aber durch die Abhängigkeitsauflösung nicht im Aggregat berücksichtigt werden konnten ($= Z^{(A)} \setminus Z^{(V)}$)

Mittels der Mengen $Z^{(V)}$ und $Z^{(A)} \setminus Z^{(V)}$ kann die Menge $Z^{(A)}$ berechnet werden.

5.4 Evaluation des Privatsphärenschutzes

In diesem Abschnitt wird der Privatsphärenschutz des Einzelnen des SMART-ER-Verfahrens analysiert. Es wird ein einzelner intelligenter Stromzähler in einer SMART-ER Gruppe G betrachtet. Die Privatsphäre eines einzelnen Haushaltes wird in dieser Arbeit, wie in Abschnitt 2.2 eingeführt, genau dann als geschützt betrachtet, wenn Messwerte des Haushalts nur in ihrer aggregierten Form anderen Parteien als dem Haushalt selbst bekannt werden können und wenn ein vorliegendes Aggregat keine Rückschlüsse über die eingeflossenen Messwerte erlaubt außer, dass deren Aggregat dem vorliegenden Aggregat entspricht.

Zunächst wird angenommen, dass $J = |G| - 1$ gilt. Ein intelligenter Stromzähler sendet also Fragmente an alle anderen Gruppenmitglieder. Der Fall von $J < |G| - 1$ wird in Abschnitt 5.4.6 wieder aufgegriffen. Da angenommen wird, dass Integrität und Vertraulichkeit der Kommunikationsverbindungen zwischen intelligenten Stromzählern und auch zum Messdienstleister gesichert sind, kann ein Abhören oder Verändern der Daten ausgeschlossen werden (siehe Abschnitt 2.1.4). Es bleibt zu untersuchen, welche Folgen die Korrumpierung einzelner Teilnehmer, also intelligenter Stromzähler oder Messdienstleister, auf die Privatsphäre hat.

Die in diesem Kapitel durchgeführten Analysen zeigen, dass SMART-ER auch dann Privatsphärenschutz leistet, wenn ein Angreifer

- ein oder mehrere intelligente Stromzähler der Gruppe korrumpiert (Abschnitt 5.4.1).

Tabelle 5.3: *Übersicht der Variablen zur Evaluation des Privatsphärenschutzes von SMART-ER.*

Variable	Bedeutung
p_X	Messwert des Zählers X
$p_X^{(1)}$, $p_X^{(2)}$	Messwerte für Zähler X, die im Rahmen der Abläufe (1 und 2) von Spieler 1 festgelegt werden.
p_{XY}	Fragment, das Zähler X an Zähler Y sendet
δ_{XY}	Die Differenz zweier Fragmente, $\delta_{XY} = p_{YX} - p_{XY}$
V_X	Abgabewert des Zählers X

- den Messdienstleister korrumpiert (Abschnitt 5.4.2).
- den Messdienstleister und ein oder bis zu $|G| - 2$ intelligente Stromzähler der Gruppe korrumpiert (Abschnitt 5.4.3).

Sind der Messdienstleister und $|G| - 1$ intelligente Stromzähler der Gruppe korrumpiert, so bleibt außer dem betrachteten intelligenten Stromzähler kein Teilnehmer übrig, der nicht korrumpiert wäre. Dann kann keine Privatsphäre garantiert werden. Jede dieser Konfigurationen wird in einem Teilabschnitt im Folgenden behandelt.

Danach folgt eine Betrachtung des Privatsphärenschutzes, falls ein intelligenter Stromzähler Fragmente nur an eine Teilmenge seiner Gruppe sendet, in Abschnitt 5.4.6.

In Abschnitt 5.4.7 wird gezeigt, dass eine statistische Analyse von Seiten des Messdienstleisters keine Gefahr für die Privatsphäre darstellt.

Schließlich wird der Privatsphärenschutz in SMART-ER bei kleinen Gruppengrößen betrachtet und diskutiert inwiefern die Gruppenzuordnung durch den Messdienstleister eine Gefahr für die Privatsphäre darstellt.

Zur Evaluation des Privatsphärenschutzes werden eine Reihe von Variablen verwendet. Diese sind in Tabelle 5.3 zusammengefasst.

5.4.1 Korrumpierte intelligente Stromzähler

Zur Evaluierung der Privatsphäre in SMART-ER mit korrumpierten Stromzählern wird das Minimalszenario in Abbildung 5.9 betrachtet. Zähler B sei in dieser

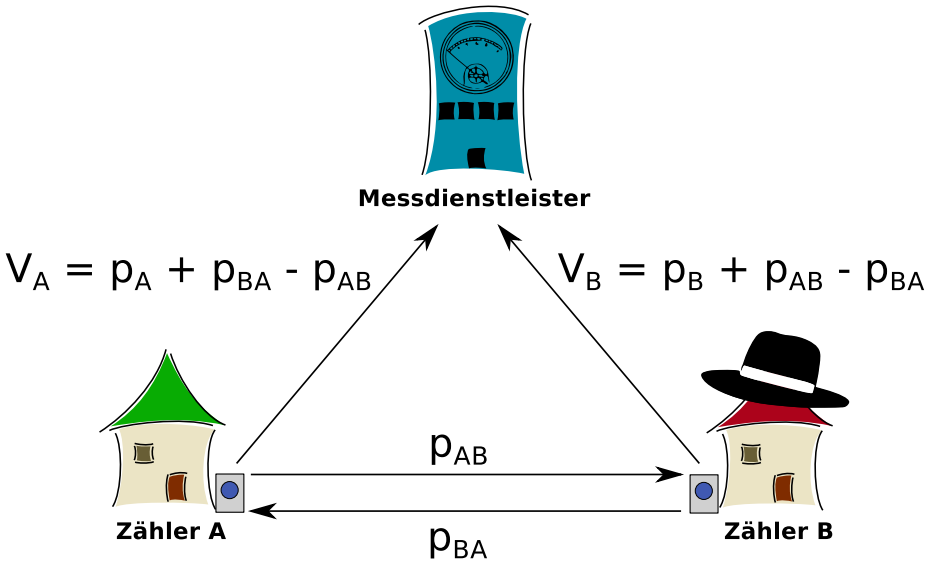


Abbildung 5.9: *Minimalszenario zur Untersuchung der erzielten Privatsphäre bei korrumpierten intelligenten Stromzählern.*

Konfiguration der korrumpierte intelligente Stromzähler (symbolisiert durch einen schwarzen Hut). Zähler *A* sei der betrachtete intelligente Stromzähler dessen Privatsphäre geschützt werden soll.

Der Angreifer erlangt dann lediglich Kenntnis des Werts p_{AB}. Die Daten, die Zähler *A* an den Messdienstleister schickt sind dem Angreifer nicht bekannt. Die Zahl p_{AB} ist zufällig und gleichverteilt aus einem endlichen Wertebereich gezogen und daher ohne Informationsgehalt. Die Privatsphäre von Zähler *A* wird hierdurch nicht berührt. Der Fall korrumpierter intelligenter Stromzähler lässt sich leicht auf mehr als einen korrumpierten Stromzähler erweitern. Auch wenn der Angreifer mehr intelligente Stromzähler korrumpiert, so verfügt er weiterhin lediglich über zufällig gezogene Zahlen. Auch mit Kenntnis von mehr zufällig gezogenen Zahlen entsteht dem Angreifer kein Erkenntnisgewinn. Die Privatsphäre bleibt also auch bei beliebiger Anzahl an korrumpierten intelligenten Stromzählern gewahrt.

5.4.2 Korrumpierter Messdienstleister

Um das Maß an erreichtem Privatsphärenschutz durch SMART-ER bei korrumpiertem Messdienstleister zu evaluieren wird der spieltheoretische Ansatz von Bohli et al. [13] verwendet: das Smart Meter Privacy Break Game (SMPBG). In

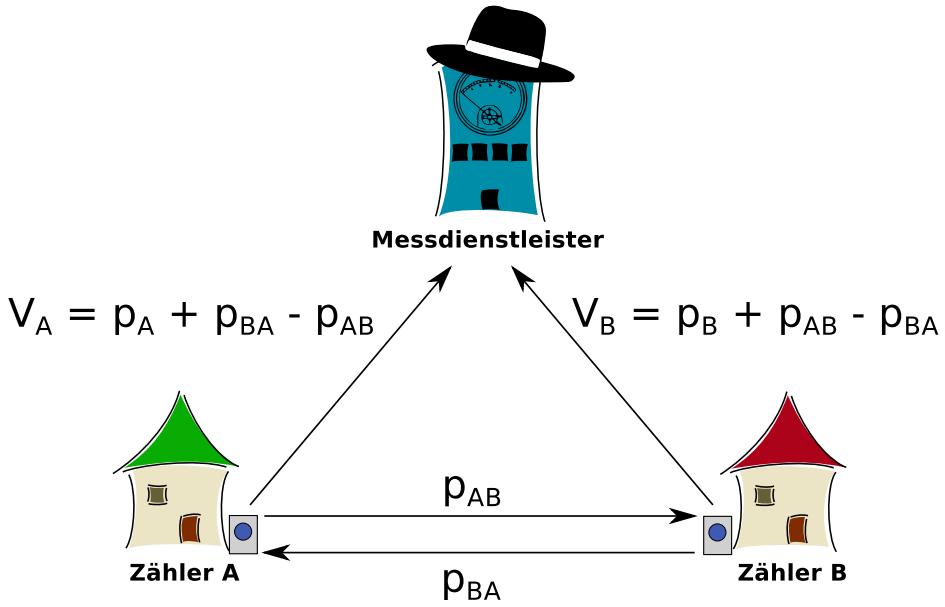


Abbildung 5.10: *Minimalszenario zur Untersuchung der erzielten Privatsphäre bei korrumpiertem Messdienstleister.*

diesem Ansatz existieren zwei Spieler. Spieler 1, der den Angreifer symbolisiert, und Spieler 2, der den Verteidiger symbolisiert. Spieler 1 wählt zwei Smart Metering Abläufe, die bei korrekter Funktion des Smart Meterings nicht unterscheidbar sein sollten. Er schreibt also für jeden Ablauf genau vor, welche relevanten Daten anfallen. Im Szenario dieser Arbeit ist dies die Leistungsaufnahme der beteiligten Haushalte. Diese beiden Abläufe müssen aber der Einschränkung genügen, dass sie bei korrekter Durchführung des Smart Meterings für den Messdienstleister nicht unterscheidbar sein dürfen. Im Szenario dieser Arbeit bedeutet dies, dass beide Abläufe die gleiche Gesamtleistungsaufnahme über alle Haushalte aufweisen. Spieler 2 wählt geheim eines dieser Szenarien aus und führt das Smart Metering entsprechend durch. Spieler 1 bekommt nun einen Mitschnitt des Smart Meterings der seinen Angriffsfähigkeiten entspricht. Dies sind alle Daten, die der Messdienstleister empfangen hat. Er gewinnt das Spiel, falls er erraten kann welches Szenario von Spieler 2 gewählt wurde. Falls Spieler 1 mit einer höheren Wahrscheinlichkeit gewinnen kann, als es eine zufällige Wahl ermöglicht, ist das Smart Metering Verfahren nicht effektiv im Schutz der Privatsphäre.

Um SMART-ER mit Hilfe dieser Methodik zu untersuchen wird wieder ein minimales Szenario untersucht. Es enthält lediglich zwei intelligente Stromzähler und den Messdienstleister (siehe Abbildung 5.10).

Hat der Angreifer Kontrolle über den Messdienstleister, so besteht sein Mitschnitt aus den Abgabewerten der beiden intelligenten Stromzähler. Diese seien $V_A = p_A + p_{BA} - p_{AB}$ für Stromzähler A und $V_B = p_B + p_{AB} - p_{BA}$ für Stromzähler B. Damit verfügt Spieler 1 über die Werte V_A und V_B.

Durch die Wahl des mathematischen Grundmodells (siehe Abschnitt 5.2) gelten für die Summen (und damit auch Differenzen) von Fragmenten besondere Bedingungen. Die Summenbildung $(+a) : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ stellt eine Bijektion dar. Ist der zweite Summand in einer Summe eine gleichverteilte Zufallsvariable und der erste Summand fest, so ist auch die Summe eine gleichverteilte Zufallsvariable. Insbesondere sind also die Summen von unabhängigen Fragmenten ebenso gleichverteilt, wie die einzelnen Fragmente selbst. V_A lässt sich daher vereinfachen zu $V_A = p_A + \delta_{AB}$, wobei δ_{AB} die Differenz $p_{BA} - p_{AB}$ darstellt. Diese Differenz ist nur den beiden Zählern A und B bekannt. Entsprechend ist $V_B = p_B + (-\delta_{AB})$. Da es sich bei δ_{AB} um eine gleichverteilte Zufallsvariable aus dem gesamten Zahlenraum handelt, ist die Wahrscheinlichkeit, dass V_A einen bestimmten Wert y annimmt $P(V_A = y) = 1/q$, wobei q die Größe des Zahlenraums darstellt ($q = 2^{32}$ in SMART-ER). Es ist also jeder mögliche Wert von V_A gleich wahrscheinlich. Die Betrachtung eines einzelnen Wertes gibt dem Angreifer also keinen Aufschluss, aber er kann Berechnungen anstellen. Ein Aufsummieren von V_A und V_B würde gerade das gewünschte Smart Metering Ergebnis erzeugen und daher keinen Mehrwert bilden. Die einzige Information, die Spieler 1 aus V_A und V_B ziehen kann, ist dementsprechend die Differenz:

$$d = V_A - V_B = p_A + \delta_{AB} - p_B + \delta_{AB} = p_A - p_B + 2\delta_{AB}$$

Betrachtet werden nun zwei von Spieler 1 gelieferte Abläufe $\{p_A^{(1)}, p_B^{(1)}\}$ und $\{p_A^{(2)}, p_B^{(2)}\}$. Diese erfüllen die Voraussetzung des SMPBG: $p_A^{(1)} + p_B^{(1)} = p_A^{(2)} + p_B^{(2)}$, resultieren also in der gleichen Summe. Es resultieren die Differenzen $d^{(1)}$ und $d^{(2)}$:

$$d^{(1)} = V_A^{(1)} - V_B^{(1)} = p_A^{(1)} - p_B^{(1)} + 2\delta_{AB}^{(1)}$$
$$d^{(2)} = V_A^{(2)} - V_B^{(2)} = p_A^{(2)} - p_B^{(2)} + 2\delta_{AB}^{(2)}$$

Da q in SMART-ER von der Berechnungsbreite des Prozessors abhängt, ist q eine Zweierpotenz und damit gerade. Damit sind die $2\delta_{AB}$ nicht mehr gleichverteilt in $\mathbb{Z}/q\mathbb{Z}$, sondern nur noch gleichverteilt in $2\mathbb{Z}/q\mathbb{Z}$, den geraden Zahlen.

Dies wäre problematisch, wenn Spieler 1 die Abläufe so gestalten könnte, dass diese Differenzen einmal gerade und einmal ungerade ausfallen. Da aber $p_A^{(1)} + p_B^{(1)} = p_A^{(2)} + p_B^{(2)}$ gefordert wird, ist die Differenz $d^{(1)}$ gerade, genau dann wenn $d^{(2)}$ gerade ist. Das heißt, dass für eine beliebige Zahl $y \in \mathbb{Z}/q\mathbb{Z}$ gilt: Wenn $d^{(1)}$ und y beide gerade oder beide ungerade sind, dann sind die Wahrscheinlichkeiten

$$\begin{aligned} P(d^{(1)} = y) &= P\left(p_A^{(1)} - p_B^{(1)} + 2\delta_{AB}^{(1)} = y\right) \\ &= P\left(2\delta_{AB}^{(1)} = y - p_A^{(1)} + p_B^{(1)}\right) = \frac{2}{q} \\ P(d^{(2)} = y) &= P\left(p_A^{(2)} - p_B^{(2)} + 2\delta_{AB}^{(2)} = y\right) \\ &= P\left(2\delta_{AB}^{(2)} = y - p_A^{(2)} + p_B^{(2)}\right) = \frac{2}{q} \end{aligned}$$

Ansonsten ist $P(d^{(1)} = y) = P(d^{(2)} = y) = 0$. Insbesondere heißt das, dass

$$\forall y \in \mathbb{Z}/q\mathbb{Z}: \quad P\left(d^{(1)} = y\right) = P\left(d^{(2)} = y\right)$$

Die Beobachtung einer bestimmten Differenz ist also für beide Szenarien gleich wahrscheinlich. Damit ist auch aus der Differenz kein Erkenntnisgewinn möglich. Die Privatsphäre bleibt also auch dann gewahrt, wenn der Angreifer Kontrolle über den Messdienstleister hat.

5.4.3 Korrumpierter Messdienstleister und Stromzähler

Im Folgenden wird eine Untersuchung der Privatsphäre durchgeführt, wenn sowohl der Messdienstleister, als auch eine Zahl von intelligenten Stromzählern korrumpiert wurde. Dabei wird der Fall betrachtet, dass außer dem betrachteten Zähler A noch mindestens ein weiterer intelligenter Stromzähler nicht korrumpiert ist (siehe Abbildung 5.11).

Um in diesem Fall, also bei korrumpierten intelligenten Stromzählern *und* korrumpiertem Messdienstleister, eine Untersuchung der Privatsphäre durchführen zu können, ist es notwendig das Smart Meter Privacy Break Game zu erweitern.

Sei $Z_h \subset Z$ die Menge der nicht korrumpierten Stromzähler mit $|Z_h| \geq 2$ und $Z_d \subset Z$ die Menge der korrumpierten Stromzähler. Spieler 1 kann nun zusätzlich während des Smart Meterings für alle $z \in Z_d$ die gesendeten Daten frei wählen. Somit kennt Spieler 1 alle p_X für $X \in Z_d$. Außerdem kennt er

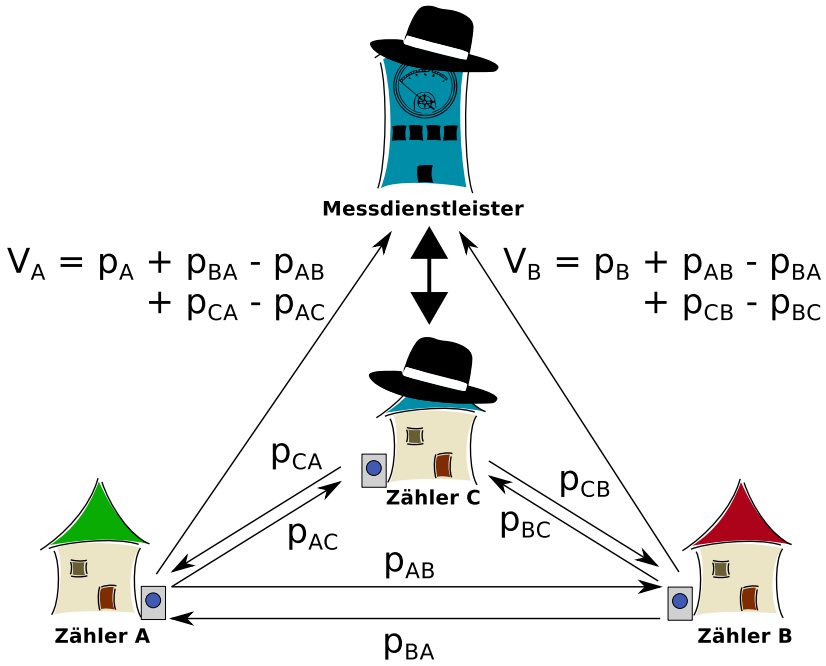


Abbildung 5.11: *Minimalszenario zur Untersuchung der erzielten Privatsphäre bei korrumpiertem Messdienstleister und einer Teilmenge von korrumpierten intelligenten Stromzählern.*

$$\sum_{X \in Z_h} p_X = \sum_{X \in Z} p_X - \sum_{X \in Z_d} p_X$$

also die Summe der Messwerte aller nicht korrumpierten intelligenten Stromzähler. Unter vorherigen Regeln wäre ihm der Sieg also sicher.

Entsprechend müssen seine Fähigkeiten zur Wahl der Szenarien so eingeschränkt werden, dass ein Sieg aufgrund dieser Kenntnisse nicht möglich ist. Daraus folgt, dass für die zwei von ihm gewählten Szenarien

$$\sum_{X \in Z_h} p_X^{(1)} = \sum_{X \in Z_h} p_X^{(2)}$$

gelten muss. Die Summe der Messwerte der nicht korrumpierten intelligenten Stromzähler muss gleich sein.

Spieler 1 kann nun mittels den Abgabewerten V_X mit $X \in Z$ beliebige Berechnungen anstellen. Da V_X mit $X \in Z_d$ dem Spieler bekannt ist und von ihm beliebig gesetzt werden kann, ist es für Berechnungen ohne Nutzen. Es bleiben also die Abgabewerte der nicht korrumpierten intelligenten Stromzähler. Im Folgenden

wird untersucht, welchen Erkenntnisgewinn Spieler 1 mittels Berechnungen auf den Abgabewerten erreichen kann. In jede mögliche Berechnung kann ein Abgabewert eines intelligenten Stromzählers entweder positiv oder negativ einfließen. Daher sei $M = M_1 \cup M_2 \subseteq Z_h$ eine Teilmenge der nicht korrumpierten intelligenten Stromzähler. Dabei enthält M_1 die Stromzähler, deren Abgabewerte positiv in die Berechnung eingehen. M_2 enthält entsprechend die Stromzähler, deren Abgabewerte negativ in die Berechnung eingehen. Um die folgende Umformung zu vereinfachen wird $\delta_{AA} = 0$ gesetzt. Die durchführbaren Berechnungen werden nach Summen von Messwerten und Summen von Fragmenten aufgeschlüsselt:

$$\begin{aligned}\sum_{A\in M_1} V_A - \sum_{A\in M_2} V_A &= \sum_{A\in M_1}\left(p_A + \sum_{X\in Z}\delta_{AX}\right) - \sum_{A\in M_2}\left(p_A + \sum_{X\in Z}\delta_{AX}\right)\\ &= \sum_{A\in M_1} p_A - \sum_{A\in M_2} p_A + \sum_{A\in M_1, B\in M_2} 2\delta_{AB}\\ &\quad + \sum_{A\in M_1}\sum_{X\in Z\setminus M}\delta_{AX} - \sum_{A\in M_2}\sum_{X\in Z\setminus M}\delta_{AX}\end{aligned}$$

Nun können zwei Fälle unterschieden werden:

- $M \setminus Z_h \neq \emptyset$, es gibt also einen nicht korrumpierten Stromzähler, dessen Abgabewert nicht in die Berechnung eingeflossen ist.
- $M = Z_h$, es sind also alle Abgabewerte der nicht korrumpierten Stromzähler in die Berechnung eingeflossen.

Im ersten Fall beinhaltet die Summe ein einzelnes δ_{AX}, wobei sowohl A, als auch X nicht korrumpiert sind. Es handelt sich also um ein zufälliges, gleichverteiltes Fragment. Die Summe liefert Spieler 1 also keine Informationen.

Im zweiten Fall ist es nötig die resultierende Formel in ihren Einzelbestandteilen zu betrachten:

$$\underbrace{\sum_{A\in M_1} p_A - \sum_{A\in M_2} p_A}_{(1)} + \underbrace{2\cdot\sum_{A\in M_1, B\in M_2}\delta_{AB}}_{(2)} + \underbrace{\sum_{A\in M_1}\sum_{X\in Z\setminus M}\delta_{AX} - \sum_{A\in M_2}\sum_{X\in Z\setminus M}\delta_{AX}}_{(3)}$$

Teil (3) kann von Spieler 1 frei gewählt werden, weil er an jedem δ_{AX} mit mindestens einem korrumpierten Stromzähler beteiligt ist. Diese Teilsumme ist

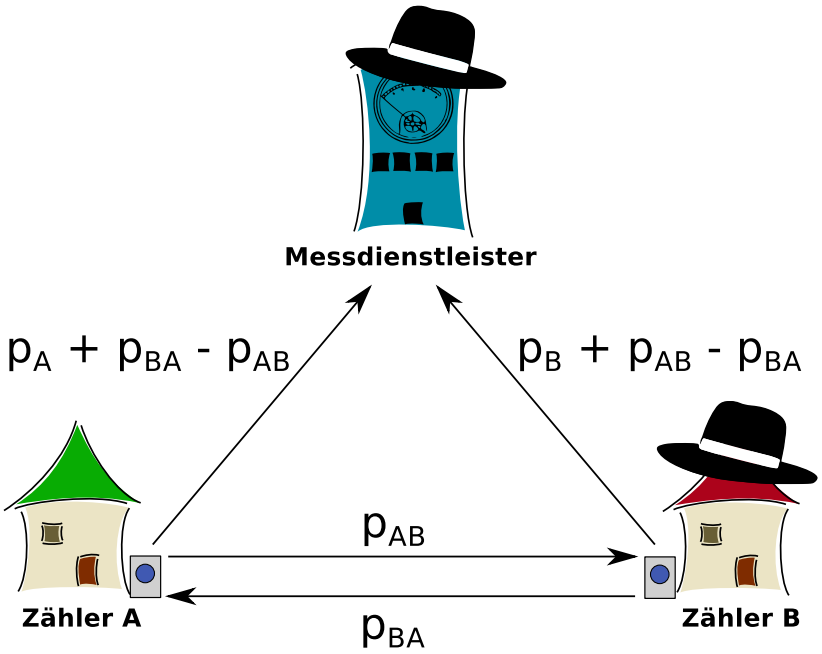


Abbildung 5.12: *Minimalszenario zur Untersuchung der erzielten Privatsphäre bei korrumpiertem Messdienstleister und korrumpierten intelligenten Stromzählern.*

Spieler 1 also bekannt. Da die Summe $\sum_{X \in Z_h} p_X$ in beiden, vom Spieler gewählten, Szenarien gleich ist, ist die Teilsumme (1) entweder in beiden Szenarien gerade oder in beiden ungerade. Genau wie im Fall eines (einzeln) korrumpierten Messdienstleisters maskiert die Teilsumme (2), die eine zufällige, gleichverteilte, gerade Zahl ist, die Teilsumme (1) vollständig. Spieler 1 hat also auch falls er Messdienstleister *und* eine Menge von intelligenten Stromzählern korrumpiert hat nur die Möglichkeit zu raten.

5.4.4 Alle anderen Parteien korrumpiert

Bleibt abschließend der Fall zu untersuchen, in dem der Angreifer den Messdienstleister *und* alle bis auf einen Zähler kontrolliert (siehe Abbildung 5.12). Hier kann das SMART-ER-Verfahren dann keine Privatsphäre mehr garantieren. Durch das Wissen der korrumpierten Zähler lässt sich jedes Fragment wieder aus V_A herausrechnen und die Privatsphäre von Zähler A ist verloren.

5.4.5 Zusammenfassung korrumpierter Teilnehmer

Alle Fälle zusammengefasst bedeutet dies, dass die Privatsphäre eines einzelnen Haushalts genau dann geschützt bleibt, wenn mindestens eine andere Partei seiner Gruppe nicht korrumpiert ist. Unabhängig davon, ob diese Partei der Messdienstleister oder ein anderer intelligenter Stromzähler ist. Dies stellt einen sehr starken Schutz der Privatsphäre dar. Das SMART-ER-Verfahren kann jeden intelligenten Stromzähler zur Verbesserung des Privatsphärenschutzes hinzuziehen. Werden dabei auch korrumpierte intelligente Stromzähler genutzt, so leidet die Privatsphäre *nicht* darunter. Gleichzeitig bietet die Kooperation mit einem nicht korrumpierten intelligenten Stromzähler einen sofortigen Privatsphärenschutz.

5.4.6 SMART-ER mit $J < |G| - 1$

In der vorhergehenden Betrachtung wurde angenommen, dass ein intelligenter Stromzähler Fragmente an alle anderen intelligenten Stromzähler seiner Gruppe sendet. In Abschnitt 5.5 wird gezeigt, dass der Kommunikations- und Rechenaufwand hierfür vernachlässigbar gering ist. Selbst für große Gruppen kann ein intelligenter Stromzähler Fragmente an alle anderen intelligenten Stromzähler versenden. Wie in den vorhergehenden Abschnitten gezeigt wurde, erzielt er mit dieser Strategie den bestmöglichen Privatsphärenschutz. Dennoch wird hier kurz darauf eingegangen, welche Auswirkungen ein $J < |G| - 1$ auf den Privatsphärenschutz hat. Dieses Szenario wäre beispielsweise vorstellbar, wenn ein intelligenter Stromzähler über eine außergewöhnlich geringe Sendedatenrate verfügt und daher eine Reduktion der versendeten Fragmente vornimmt.

Wie bereits in den vorhergehenden Abschnitten gezeigt, ist die Privatsphäre eines intelligenten Stromzählers nur dann in Gefahr, wenn er ausschließlich mit korrumpierten intelligenten Stromzählern Fragmente ausgetauscht hat und der Messdienstleister ebenfalls korrumpiert ist. Um dies zu betrachten, sei eine Gruppe G angenommen, die aus dem hier betrachteten Zähler z_1, einer Menge von korrumpierten Stromzählern Z_d und einer Menge von nicht korrumpierten Stromzählern Z_h besteht. Es gilt also $G = \{z_1\} \cup Z_d \cup Z_h$. Die Privatsphäre von z_1 ist genau dann nicht mehr geschützt wenn folgende Bedingungen erfüllt sind:

(1) Bei der Auswahl seiner J Fragmentempfänger hat z_1 keinen intelligenten Stromzähler $z \in Z_h$ ausgewählt.

(2) Für jeden intelligenten Stromzähler $z \in Z_h$ gilt, dass z nicht z_1 als Fragmentempfänger ausgewählt hat.

Da jeder intelligente Stromzähler seine Fragmentempfänger unabhängig von den anderen intelligenten Stromzähler wählt, ist auch das Eintreten dieser beiden Bedingungen unabhängig voneinander. Die Wahl der Fragmentempfänger erfolgt mittels zufälligem Ziehen aus G und kann daher mittels des Urnenmodells und „Ziehen ohne Zurücklegen“ betrachtet werden. Sei die Menge der ausgewählten Fragmentempfänger des intelligenten Stromzählers z mit F_z bezeichnet. Die Wahrscheinlichkeit, dass F_{z_1} keinen intelligenten Stromzähler aus Z_h enthält, entspricht genau der Wahrscheinlichkeit, dass F_{z_1} nur intelligente Stromzähler aus Z_d enthält. Für (1) muss also gelten, dass nach J-fachem Ziehen aus einer Menge mit $|G|-1$ Elementen, von denen $|Z_d|$ Elemente als Treffer betrachtet werden, J Treffer zu verzeichnen sind. Die entsprechende Wahrscheinlichkeitsverteilung entspricht der hypergeometrischen Verteilung:

$$P(F_{z_1} \cap Z_h = \emptyset) = \frac{\binom{J}{J}\binom{(|G|-1)-J}{|Z_d|-J}}{\binom{(|G|-1)}{|Z_d|}} = \frac{\binom{(|G|-1)-J}{|Z_d|-J}}{\binom{(|G|-1)}{|Z_d|}} \tag{5.1}$$

$$= \frac{|Z_d| \cdot (|Z_d|-1) \cdot \ldots \cdot (|Z_d|-J+1)}{\underbrace{(|G|-1) \cdot (|G|-2) \cdot \ldots \cdot (|G|-J)}_{J \text{ Terme}}} \tag{5.2}$$

$$\leq \frac{|Z_d|^J}{(|G|-J)^J} \tag{5.3}$$

Als Beispiel sei angenommen, dass der Rest der Gruppe von Stromzähler z_1 zur Hälfte aus korrumpierten und zur anderen Hälfte aus nicht korrumpierten intelligenten Stromzählern besteht. Insgesamt (inklusive z_1) umfasse die Gruppe $2|Z_d|+1$ Stromzähler. Für $|Z_d| = 5$ entspräche dies einer Gruppe von 11 intelligenten Stromzählern. Für diese Gruppe kann mittels Gleichung 5.2 die Wahrscheinlichkeit für Bedingung (1) ausgerechnet werden. Sie beträgt $\approx 22\%$. Mit $J = 3$ reduziert sich die Wahrscheinlichkeit auf $\approx 8\%$. Mittels der Abschätzung 5.3 folgt

$$P(F_z \cap Z_h = \emptyset) \leq \frac{|Z_d|^J}{(2|Z_d|+1-J)^J} \overset{|Z_d| \to \infty}{\longrightarrow} \left(\frac{1}{2}\right)^J \tag{5.4}$$

und damit eine Abschätzung der Wahrscheinlichkeit für Bedingung (1) für große Gruppengrößen mit einem Anteil von 50% der korrumpierten intelligenten Stromzähler an der Gesamtzahl. Für $J = 2$ ergibt sich eine asymptotische obere Schranke von 25%. Für $J = 3$ ergibt sich eine asymptotische obere Schranke von $12,5\%$.

Damit die Privatsphäre von z_1 verletzt ist, muss jedoch auch Bedingung (2) erfüllt sein. Die Wahrscheinlichkeit, dass $z_1 \in F_z$ für ein $z \in Z_h$, entspricht gerade dem J-fachen ziehen aus $|G|-1$ Elementen, von denen lediglich eines als Treffer gewertet wird:

$$P(z_1 \in F_z) = \frac{\binom{J}{1}\binom{(|G|-1)-J}{1-1}}{\binom{(|G|-1)}{1}} = \frac{J}{|G|-1} \tag{5.5}$$

Die Wahrscheinlichkeit, dass kein $z \in Z_h$ den intelligenten Stromzähler z_1 als Fragmentempfänger wählt ist also:

$$P\left(\nexists z \in Z_h : z_1 \in F_z\right) = \left(1 - P\left(z_1 \in F_z\right)\right)^{|Z_h|} \tag{5.6}$$

Für das obige Beispiel mit $J = 2$ ergibt sich $(1-0,2)^5 \approx 0,33$. Mit circa 33%-iger Wahrscheinlichkeit hat keiner der fünf nicht korrumpierten Stromzähler z_1 ausgewählt. Für $J = 3$ ergeben sich nur noch $\approx 16,8\%$.

Die Wahrscheinlichkeit, dass die beiden voneinander unabhängigen Bedingungen (1) und (2) gleichzeitig im Beispiel von 11 intelligenten Stromzählern bei $J = 2$ auftreten beläuft sich auf $7,2\%$. Für $J = 3$ ergeben sich nur noch $1,4\%$. Behält man den Anteil korrumpierter intelligenter Stromzähler bei 50% bei, so steigen diese Wahrscheinlichkeiten mit der Gruppengröße an. Wie jedoch gezeigt wurde existieren asymptotische obere Schranken mit 25% bei $J = 2$ und $12,5\%$ bei $J = 3$. Doch selbst bei einer Gruppengröße von 1 001 intelligenten Stromzählern erreichen die Wahrscheinlichkeiten nicht die 10%-Marke (bei $J = 2$), respektive die 3%-Marke (bei $J = 3$).

Es kann also geschlossen werden, dass eine Verwendung von SMART-ER mit $J < |G|-1$ einen Angriff mit weniger als $|G|-1$ korrumpierten Stromzählern ermöglicht. Dessen Erfolgswahrscheinlichkeit hängt hauptsächlich vom Anteil korrumpierter Stromzähler in der jeweiligen Gruppe ab und ist selbst bei 50% sehr gering.

5.4.7 Statistische Analyse der Abgabewerte

In den vorhergehenden Abschnitten wurde ein einzelnes Messintervall betrachtet. Geht man von kryptographisch korrekt gezogenen Zufallszahlen aus, kann eine statistische Analyse auf dieser relativ kleinen Anzahl an Zufallszahlen keinen Erfolg haben. Im Folgenden wird betrachtet, inwiefern eine statistische Analyse der abgegebenen Werte über einen längeren Zeitraum Aufschluss über Messwerte geben kann. Da der Messdienstleister die ihm übermittelten Werte frei verwenden kann, steht ihm die Möglichkeit offen Berechnungen außerhalb von $\mathbb{Z}/q\mathbb{Z}$ durchzuführen. Betrachtet er jede Abgabe einzeln, so stellt sie die Summe eines Messwertes und eines Maskierungswertes dar. Also $V = p + m$, wobei m eine gleichverteilte Zufallsvariable aus $\mathbb{Z}/q\mathbb{Z}$ ist. Betrachtet der Messdienstleister nun eine Reihe von Abgabewerten $\{V_1, V_2, \ldots, V_n\}$ und bildet das arithmetische Mittel ohne modulo q zu rechnen, so erhält er

$$\frac{1}{n}\sum_{i=1}^{n} V_i = \frac{1}{n}\sum_{i=1}^{n}(p_i + m_i) = \frac{1}{n}\sum_{i=1}^{n} p_i + \frac{1}{n}\sum_{i=1}^{n} m_i \tag{5.7}$$

die Summe aus dem arithmetischen Mittel der Messwerte und dem arithmetischen Mittel der Maskierungswerte. Dies ist für den Messdienstleister von besonderem Interesse. Da sich Maskierungswerte aus unabhängigen, identisch verteilten Zufallszahlen zusammensetzen trifft das Gesetz der großen Zahlen [78] eine Aussage über das arithmetische Mittel der Maskierungswerte: Das arithmetische Mittel der Zufallsvariablen konvergiert stochastisch gegen μ, dem Erwartungswert, für $n \to \infty$. Um in SMART-ER auch negative Werte zu erlauben wurde das letzte Viertel von $\mathbb{Z}/q\mathbb{Z}$ als negativ interpretiert. Betrachtet man diese in $\mathbb{Z}$, so werden die Zufallsvariablen aus dem Intervall $[-\frac{q}{4}, \ldots, 0, \ldots, \frac{3}{4}q - 1]$ gezogen. Der Erwartungswert ist daher

$$\frac{1}{q}\sum_{i=-\frac{q}{4}}^{\frac{3}{4}q-1} i = \frac{1}{4}(q-2) \tag{5.8}$$

Das arithmetische Mittel der Maskierungswerte konvergiert also stochastisch gegen $\frac{1}{4}(q-2)$ für $n \to \infty$. Gemäß Gleichung (5.7) kann mit diesem Wissen ein Rückschluss auf das arithmetische Mittel der Messwerte p_i möglich sein.

Um auszuschließen, dass dieser statistische Zusammenhang eine Gefahr für die Privatsphäre darstellt, wird im Folgenden der zentrale Grenzwertsatz der Statistik [78] zur Analyse herangezogen. Hierzu wird die Wahrscheinlichkeit

berechnet, mit der ein entsprechend berechnetes arithmetisches Mittel innerhalb einer gegebenen Genauigkeit liegt.

Zunächst wird die Varianz der aufsummierten Zufallszahlen benötigt. Seien $X_1, X_2, \ldots$ die zufällig, unabhängig, gleichverteilt gezogenen Zufallszahlen. Wie in Gleichung (5.8) berechnet ist der Erwartungswert $\mu = \frac{1}{4}(q-2)$. Weiter ergibt sich die Varianz

$$Var(X) = \sigma^2 = \frac{1}{q} \sum_{i=-\frac{q}{4}}^{\frac{3}{4}q-1} (i-\mu)^2 = \frac{1}{q} \sum_{i=-\frac{q}{4}}^{\frac{3}{4}q-1} \left(i - \left(\frac{1}{4}(q-2) \right) \right)^2 = \frac{q^2+26}{12} \tag{5.9}$$

Sei nun Y_n mit $n \in \mathbb{N}$ die partielle Summe der ersten n Zufallszahlen. Weiter sei

$$M_n = \frac{Y_n}{n} = \frac{1}{n} \sum_{i=1}^{n} X_i$$

das arithmetische Mittel einer Stichprobe $X_1, \ldots, X_n$. Dem zentralen Grenzwertsatz folgend liegt die Verteilungsfunktion von M_n für große n nahe der Normalverteilung mit Erwartungswert μ und Varianz $\frac{\sigma^2}{n}$. Eine Faustregel der Statistik besagt, dass ab $n > 30$ die Abweichung dieser Abschätzung so gering ist, dass sie vernachlässigt werden kann [97]. Für SMART-ER bedeutet dies, dass sich die Verteilung des arithmetischen Mittels der Maskierungswerte schon nach einem Beobachtungszeitraum von einem Tag ($n = 96$) sehr gut durch die Normalverteilung approximieren lässt. Dies wird im Folgenden verwendet.

Beobachtet ein Messdienstleister nun eine Reihe von Messwerten und schätzt das Mittel der Maskierungswerte mittels des Erwartungswerts, so kann sein voraussichtlicher Fehler mittels der Normalverteilung approximiert werden. Je größer dabei die Stichprobe, also der Beobachtungszeitraum, desto genauer wird die Schätzung. Ist eine hinreichend genaue Schätzung des arithmetischen Mittels möglich, so ist die Privatsphäre in Gefahr. Im Folgenden wird daher die Genauigkeit einer solchen Schätzung in Abhängigkeit des Beobachtungszeitraums untersucht. Es wird die Wahrscheinlichkeit $P(t, G) = P(|M_{96t} - \mu| \geq G)$ berechnet.

- t bezeichnet den Beobachtungszeitraum in Tagen. Hieraus berechnet sich die Anzahl an eingeflossenen Zufallszahlen auf der Basis eines Messintervalls von 15 Minuten.

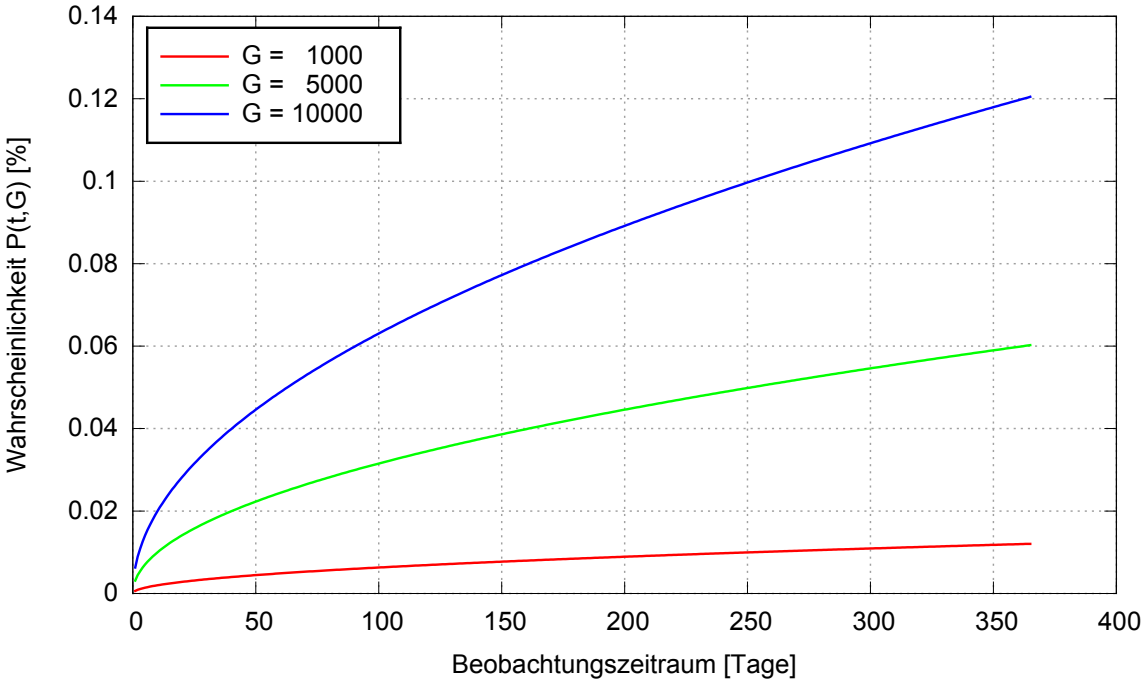


Abbildung 5.13: *Wahrscheinlichkeit nach n Tagen den Durchschnitt der Maskierungswerte bis auf Genauigkeit ±G bestimmen zu können.*

- G Die gewünschte Genauigkeit. Mit Wahrscheinlichkeit P hat die Schätzung des Messdienstleisters höchstens Abstand G von dem tatsächlichen arithmetischen Mittel der Maskierungswerte.

Für $G \in \{1\,000, 5\,000, 10\,000\}$ ist $P(t, G)$ in Abhängigkeit von t als Graph in Abbildung 5.13 aufgetragen.

Für $t = 365$ und $G = 10\,000$ ist $P(t, G) \approx 0,12\%$. Dies entspricht der Wahrscheinlichkeit nach einer einjährigen Sammlung der Abgabewerte den durchschnittlichen Messwert bis auf eine Genauigkeit von ±10 000 bestimmen zu können. In dieser Arbeit wird die Leistungsaufnahme ermittelt und Watt als Einheit benutzt. Ein durchschnittlicher 2-Personen Haushalt hat eine durchschnittliche Leistungsaufnahme von ungefähr 400 Watt. Die sehr unwahrscheinlich erreichbare Genauigkeit von ±10 000 Watt wäre also nicht einmal ausreichend für einen Erkenntnisgewinn.

Zusammenfassend kann also gesagt werden, dass das Gesetz der großen Zahlen Aussagen über den Durchschnitt von Messwerten zulässt. Diese können aber erst nach sehr langer Zeit mit verwendbarer Sicherheit getroffen werden. Die Privatsphäre der Haushalte wird also eher durch eine jährlichen Abrechnung, die

dann auch genaue und verlässliche Aussagen über den Durchschnittsverbrauch trifft, verletzt, als dass sie durch SMART-ER verletzt wird.

5.4.8 Privatsphäre einer Gruppe

Die in SMART-ER eingeführte Gruppenbildung stellt einen Mechanismus zur Verbesserung der Robustheit dar. Mittels der Gruppenbildung wird auch bei Störungen ein Totalausfall des Smart Meterings verhindert. Allerdings wirft die Gruppenbildung auch die Frage nach der Privatsphäre der Gruppe (siehe Abschnitt 2.2) auf. Es entsteht ein Spannungsfeld zwischen einer besseren Robustheit bei Störungen (kleine Gruppengrößen) und einem besseren Schutz der Privatsphäre der Gruppe (große Gruppengrößen). Um eine Kosten-Nutzen-Analyse vornehmen zu können müsste eine Bewertung der Privatsphäre einer Gruppe in Abhängigkeit der Gruppengröße verfügbar sein.

Die Fragestellung nach einer solchen Bewertung ist nicht durch SMART-ER aufgeworfen, sondern allen Verfahren, die mittels Aggregatbildung Privatsphäre schützen, gemein. Eine solche Bewertung ist in der Literatur nicht verfügbar und abhängig von vielen externen und teilweise nicht technischen Variablen, wie beispielsweise der Verteilung der Messwerte. Auch spielen externe Informationsquellen, wie beispielsweise Arbeitszeiten, eine große Rolle (siehe hierfür Jawurek et al. [70]). Eine solche Bewertung steht nicht im Fokus dieser Arbeit und wird daher auch nicht vorgenommen.

Mittels der konfigurierbaren Gruppengröße des SMART-ER-Verfahrens kann die Gruppengröße flexibel angepasst werden. Tritt der Fall ein, dass eine entsprechende Bewertung der Privatsphäre einer Gruppe möglich wird, so kann nach einer Kosten-Nutzen-Analyse der optimale Wert für die Gruppengröße in SMART-ER konfiguriert werden.

5.4.9 Gruppenbildung durch den Messdienstleister

In diesem Abschnitt wurde gezeigt, dass SMART-ER genau dann die Privatsphäre eines intelligenten Stromzählers schützt, wenn sich mindestens eine andere Partei korrekt verhält. Dabei ist es irrelevant, ob diese Partei der Messdienstleister oder ein anderer intelligenter Stromzähler in derselben Gruppe ist.

Dadurch sind Angriffe auf die Privatsphäre ohne Kooperation mit dem Messdienstleister ausgeschlossen. Die Privatsphäre eines Haushalts ist selbst dann

geschützt, wenn alle anderen beteiligten intelligenten Stromzähler von einem Angreifer korrumpiert wurden.

Betrachtet wird nun ein korrumpierter Messdienstleister. Alleine gelingt es ihm nicht den Privatsphärenschutz eines Haushalts zu brechen. Verfügt er allerdings über eine Anzahl an korrumpierten intelligenten Stromzählern, so lässt SMART-ER einen Angriffsvektor offen. Angenommen der Messdienstleister versucht die Privatsphäre eines bestimmten Haushalts zu verletzen. Dies gelingt ihm, wenn er die Gruppe des zugehörigen intelligenten Stromzählers mit korrumpierten intelligenten Stromzählern füllen kann. Da in der hier vorgestellten Grundvariante von SMART-ER der Messdienstleister die Gruppeneinteilung vornimmt, stellt lediglich die Beschaffung der korrumpierten intelligenten Stromzähler eine Hürde dar. Deren Anzahl ist durch die konfigurierte Gruppengröße $|G|$ beschränkt. Auch ist eine gleichzeitige Verwendung korrumpierter intelligenter Stromzähler in mehreren Gruppen denkbar. Die daraus resultierende, nicht disjunkte Einteilung in Gruppen führt dann zu einer, für den Angreifer, besseren Nutzung der korrumpierten intelligenten Stromzähler.

Das Brechen des Privatsphärenschutzes eines Haushalts für einen Messintervall ist mit diesem Angriffsvektor also mit den Kosten der Beschaffung von $|G|-1$ korrumpierten intelligenten Stromzählern verbunden. Wird die Gruppenzusammensetzung beibehalten, so ist die Privatsphäre auch in jedem folgenden Messintervall gebrochen.

Zur Lösung dieses Problem liegt nahe, dass sich die Gruppenzusammensetzung von Messintervall zu Messintervall ändern muss. Dabei können zwei Strategien verfolgt werden:

- Jeder intelligente Stromzähler fordert pro Messintervall eine völlig neue Gruppe ohne Überschneidungen mit den vorherigen Gruppen.

- Jeder intelligente Stromzähler fordert, dass pro Messintervall ein Gruppenmitglied durch einen bisher noch nicht verwendeten intelligenten Stromzähler ersetzt wird.

Beide Strategien können nur eine gewisse Zeit durchgeführt werden, bevor ein Erfüllen der Forderung mangels weiterer intelligenter Stromzähler unmöglich wird. Wird für jedes Messintervall eine völlig neue Gruppe gefordert, so erhöht sich der Angriffsaufwand für den Messdienstleister stark. Das Brechen des Privatsphärenschutzes eines Haushalts in n Messintervallen würde nun $n \times (|G|-1)$ korrumpierte

intelligente Stromzähler benötigen. Das Fordern lediglich eines neuen Gruppenmitglieds pro Messintervall vereinfacht den Angriff. Hier sind für n Messintervalle nur $|G|-1+n-1=|G|+n-2$ korrumpierte intelligente Stromzähler nötig. Als Vorteil hätte diese Strategie, dass eine Wiederholung der Gruppenkonfiguration erst später eintritt.

Trotz der geschilderten Möglichkeiten diesen Angriffsvektor abzumildern, ist eine Lösung des Gruppenbildungsproblems ohne Beeinflussungsmöglichkeit durch den Messdienstleister wünschenswert. In Kapitel 6 und Kapitel 7 werden mit den Verfahren *Speeddating* und *Elderberry* Lösungen vorgestellt.

5.5 Evaluation der Smart Metering Leistung

In diesem Abschnitt wird eine Evaluation von SMART-ER bezüglich der Smart Metering Leistung durchgeführt. Hierzu werden mehrere Aspekte des Verfahrens analysiert und simulativ untersucht:

- Die Leistung von SMART-ER bezüglich des Smart Meterings wird in Abschnitt 5.5.4 betrachtet. Als Metrik wird hier vor allem der Anteil an intelligenten Stromzählern, über die eine fehlerfreie Aussage getroffen werden konnte, betrachtet ($= Z^{(V)}$).

- In Abschnitt 5.5.5 wird der Rechenaufwand von SMART-ER für einzelne intelligente Stromzähler und den Messdienstleister betrachtet.

- In Abschnitt 5.5.6 wird der Kommunikationsaufwand von SMART-ER für einzelne intelligente Stromzähler und den Messdienstleister betrachtet.

Im Rahmen dieser Evaluation wird SMART-ER auch mit anderen Verfahren verglichen. Da der Fragmentierungsmechanismus von SMART ungeeignet für das Smart Metering Szenario ist, wurde eine Variante von SMART, genannt SMART+, implementiert, die sich lediglich durch einen verbesserten Fragmentierungsmechanismus von SMART unterscheidet. Um die Effektivität der Änderungen zu SMART zu evaluieren wird SMART-ER in den Punkten Kommunikationsaufwand und Performanz mit SMART+ verglichen. Um allgemeine Vergleichswerte zu erreichen wird SMART-ER auch mit Baseline verglichen. Dieses Verfahren verzichtet gänzlich auf den Privatsphärenschutz. Jeder intelligente Stromzähler in Baseline misst zum festgelegten Zeitpunkt seinen Messwert und sendet ihn an den Messdienstleister.

Algorithmus 2 Baseline Client.

```
loop
    repeat
        sleep 1
    until currentTime() == submitTime()
    p ← measurePower()
    submitToSink(p)
end loop
```

Insbesondere findet also keine Kommunikation mit anderen intelligenten Stromzählern statt. Der Vergleich mit Baseline stellt dar, welche Einbußen für das Smart Metering durch den Schutz der Privatsphäre mittels SMART-ER zu erwarten sind. Die beiden Vergleichsverfahren werden im Folgenden kurz erläutert.

Alle Verfahren wurden in C++ im Simulator OverGrid (siehe Abschnitt 4) implementiert. Die Kommunikation zwischen intelligenten Stromzählern untereinander und zwischen intelligenten Stromzählern und dem Messdienstleister verwendet die von OverSim bereitgestellte Funktionalitäten *BaseRPC* und *Simple-Underlay*. Das Simple-Underlay verwendet Daten aus dem CAIDA/Skitter-Projekt [68, 87] um eine effiziente Simulation von realistischem Internet-Datenverkehr zu realisieren. BaseRPC ermöglicht einen zuverlässigen Nachrichtenaustausch, der mittels Sequenznummern, Quittungen und Sendewiederholungen realisiert wird. Der mittels BaseRPC simulierte Overhead berücksichtigt nicht Schicht 1 bis 3 des ISO/OSI-Referenzmodells. Auf die Simulation von kryptographisch gesicherten Verbindungen wurde aus Effizienzgründen verzichtet.

5.5.1 Baseline

Das Baseline Verfahren stellt eine möglichst einfach gehaltene Implementierung eines Smart Metering ohne jeglichen Privatsphärenschutz dar. Jeder intelligente Stromzähler wartet auf den Abgabezeitpunkt, misst seine aktuelle Leistungsaufnahme und sendet diese mittels eines zuverlässigen Transportprotokolls an den Messdienstleister (siehe Algorithmus 2).

Der Messdienstleister empfängt die übermittelten Messwerte und speichert sie. Sind Messwerte von allen intelligenten Stromzählern des Smart Meterings eingetroffen, so übermittelt er sie an den Auftraggeber. Sollten die Messwerte nicht vollzählig eintreffen, also einzelne intelligente Stromzähler keine Daten übertragen,

werden nach Ablauf von 10 Sekunden die bis dahin eingetroffenen Daten an den Auftraggeber übertragen. Die Zeitspanne ist ausreichend groß gewählt um etwaige Sendewiederholungen durch das zuverlässige Transportprotokoll, beispielsweise aufgrund von Paketverlusten, erfolgreich durchführen zu können.

5.5.2 SMART+

Da sich der in [66] vorgeschlagene Fragmentierungsmechanismus als untauglich für das Smart Metering Szenario erwiesen hat, wurde mit SMART+ ein Vergleichsverfahren implementiert, das sich lediglich im Punkt Fragmentierungsmechanismus von SMART unterscheidet. Anstatt Fragmente abhängig vom Messwert zu wählen, werden Zufallszahlen aus einer festgelegten Menge $\{0,\ldots,I\}$ gezogen. Dabei stellt I den Protokollparameter des maximalen Fragmentwerts dar.

Jedem intelligenten Stromzähler steht eine Liste der anderen teilnehmenden intelligenten Stromzähler Z zur Verfügung. Diese wird vom Messdienstleister einmalig zu Beginn zur Verfügung gestellt und enthält beispielsweise Identitäten und IP-Adressen der intelligenten Stromzähler.

Als weiteren Protokollparameter führt das SMART-Verfahren J ein, die konfigurierte Anzahl an zu verschickenden Fragmenten pro intelligentem Stromzähler.

Der Ablauf auf den intelligenten Stromzählern ist dann wie folgt (siehe auch Algorithmus 3). Wie in Baseline wird auf den Messzeitpunkt gewartet und dann der aktuelle Messwert gemessen. Dann wird aus der Menge der intelligenten Stromzähler Z eine Teilmenge Y der Größe J ausgewählt. Für jeden gewählten intelligenten Stromzähler z wird ein neues Fragment f aus $\{0,\ldots,I\}$ gezogen und diesem zugeschickt. Jedes versendete Fragment wird dann vom gemessenen Wert p abgezogen. Gleichzeitig werden die eintreffenden Fragmente von anderen intelligenten Stromzählern auf p aufaddiert. Nach Ablauf einer Schutzzeit von 10 Sekunden wird p an den Messdienstleister übermittelt. Diese Schutzzeit ist nötig, da ein intelligenter Stromzähler nicht wissen kann, welche anderen Stromzählern beschlossen haben ihm ein Fragment zu senden. Auch ist eine Wartezeit nötig um bei kurzfristigen Kommunikationsproblemen, wie Paketverlusten, Sendewiederholungen zu ermöglichen. Die gewählte Dauer ermöglicht dies. Nach Ablauf dieser Schutzzeit wird davon ausgegangen, dass alle funktionsfähigen Stromzähler in der Lage waren ihren Wert zu übertragen.

Die ersten Abgabewerte treffen somit erst nach Ablauf dieser Schutzzeit beim Messdienstleister ein. Er aggregiert alle eintreffenden Abgabewerte auf einen einzelnen Wert und vermerkt zusätzlich, von welchen intelligenten Stromzählern

Algorithmus 3 SMART+ Client.

```
Z ← Set of all nodes
J ← number of Fragments to send out
loop
    repeat
        sleep 1
    until currentTime() == submitTime()
    Y ← selectRandomNodes(Z,J)
    p ← measurePower()
    for all z ∈ Y do
        f ← genRandomFrag()
        sendFrag(z,f)
        p ← p − f
    end for
    repeat
        f ← receiveFrag()
        p ← p + f
    until currentTime() == submitTime() +10
    submitToSink(p)
end loop
```

er Abgabewerte empfangen hat ($= Z^{(A)}$). Nach Ablauf einer weiteren Schutzzeit von 10 Sekunden sendet er den aggregierten Wert und $Z^{(A)}$ an den Auftraggeber.

5.5.3 Annahmen

Für die Evaluation der Verfahren im Simulator OverGrid wurden Annahmen bezüglich Datenraten, der Zuverlässigkeit der Kommunikationsverbindung und dem Stromverbrauch der Haushalte getroffen. Diese werden im Folgenden kurz erläutert.

Datenraten

Im Smart Metering können große Mengen an Daten anfallen. Dennoch ist der eigentliche Kommunikationsaufwand pro intelligentem Stromzähler eher als gering einzuschätzen. Bei einer direkten Übertragung eines Messwertes zum Messdienstleister fallen pro intelligentem Stromzähler nur wenige hundert Byte Daten an. Da

in diesem Szenario der intelligente Stromzähler über einen DSL-Anschluss an das Internet angebunden ist, gelten für ihn auch entsprechende Beschränkungen. Laut dem Bericht zum Breitbandatlas Mitte 2013 [132] ist eine Empfangsdatenrate von 6 Megabit pro Sekunde für 91,7% der Haushalte in Deutschland verfügbar. Daher wird in dieser Arbeit eine maximal erreichbare Empfangsdatenrate von 6 Megabit pro Sekunde für DSL-Anschlüsse angenommen. Entsprechend der Asymmetrie von DSL-Anschlüssen wird die maximale Senderate mit 512 Kilobit pro Sekunde angenommen.

Da ein Messdienstleister eine Vielzahl an intelligenten Stromzählern betreut, muss dieser mit wesentlich größeren Datenmengen rechnen. Als maximal erreichbare Datenrate für den Messdienstleister wird daher eine in Rechenzentren übliche Datenrate von 1 Gigabit pro Sekunde angenommen.

Zuverlässigkeit der Kommunikationsanbindung

Mit der Zuverlässigkeit eines technischen Systems wird angegeben, wie verlässlich ein Dienst innerhalb eines Zeitintervalls erbracht wird. Für das Smart Metering spielt die Zuverlässigkeit der Kommunikationsanbindung eine wichtige Rolle. Ein Ausfall verhindert die Teilnahme am Smart Metering. Durch die große Anzahl an Teilnehmern kann somit selbst bei einer hohen Zuverlässigkeit pro Teilnehmer nicht von einer permanenten Verfügbarkeit des Dienstes ausgegangen werden. Um dies untersuchen zu können, wird in diesem Abschnitt eine Annahme über die Zuverlässigkeit der Kommunikationsanbindung getroffen.

Für die Zuverlässigkeit des Messdienstleisters werden in diesem Szenario keine Einschränkungen angenommen. Es kann davon ausgegangen werden, dass der Messdienstleister Maßnahmen zur Erhöhung der Zuverlässigkeit ergreift. Beispielsweise kann eine mehrfach redundante Anbindung des Rechenzentrums und eine unterbrechungsfreie Stromversorgung verwendet werden. Natürlich können auch diese Maßnahmen keine vollständige Verfügbarkeit garantieren. Für die Untersuchungen, die im Rahmen dieser Arbeit durchgeführt werden wird jedoch angenommen, dass die Internetanbindung und der Dienst des Messdienstleisters störungsfrei verfügbar sind.

Um die Zuverlässigkeit der DSL-Verbindungen einschätzen zu können sind ausführliche Feldstudien nötig. Die hierfür benötigten Daten fallen zwar bei Internetprovidern direkt an, sind jedoch nicht öffentlich verfügbar. Auch in der Literatur sind keine ausführlichen Studien verfügbar.

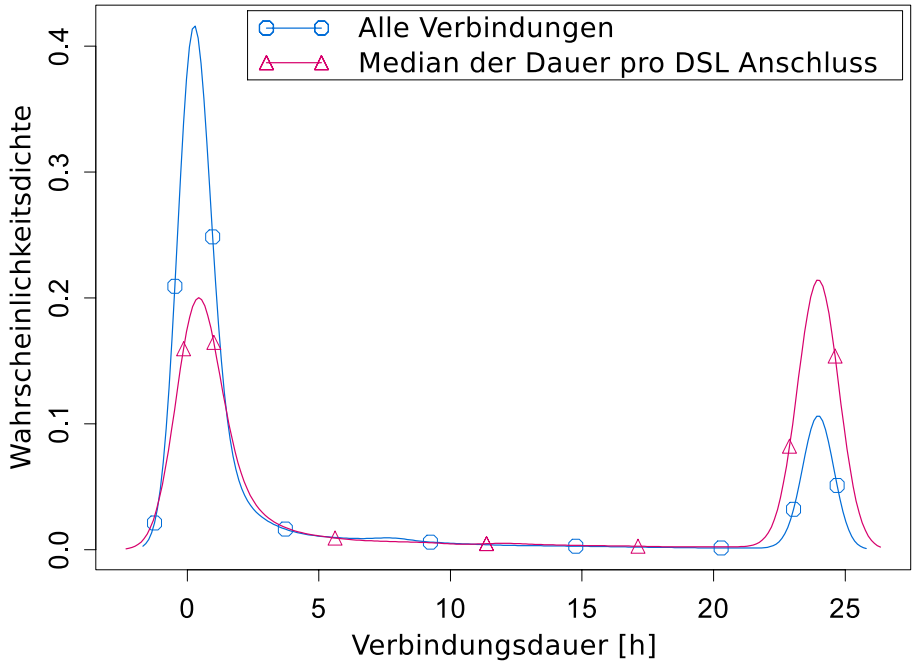


Abbildung 5.14: *Wahrscheinlichkeitsdichte für die Dauer einer DSL-Verbindung. Quelle: [88]*

Um dennoch die Zuverlässigkeit einer DSL-Verbindung realistisch einschätzen zu können, wird eine Abschätzung der Zuverlässigkeit einer DSL-Leitung aufgrund verfügbarer Daten vorgenommen. Von Maier et al. [88] wurde die Dauer von DSL-Sessions für 20 000 DSL-Anschlüsse evaluiert. Die Autoren kommen dabei zum Ergebnis, dass es im Wesentlichen zwei Klassen von DSL-Verbindungen gibt: sehr kurzlebige und solche, die ungefähr 24 Stunden lang bestehen. Die erste Klasse erklären die Autoren mit automatischen Verbindungstrennungen bei Inaktivität von DSL-Routern oder händischen Trennungen durch den Kunden. Die zweite Klasse wird einer vom Internetprovider eingerichteten Zwangstrennung zugeschrieben, die eine Verbindung nach ungefähr 24 Stunden unterbricht.

Für das Smart Metering Szenario kann davon ausgegangen werden, dass keine händische Trennung durch den Kunden erfolgt. Auch eine automatische Trennung durch den DSL-Router wird ausgeschlossen. Dadurch entfällt die Klasse der kurzlebigen Verbindungen und es verbleibt lediglich die Klasse der ungefähr 24-stündigen Verbindungen. Daher wird in diesem Szenario angenommen, dass eine DSL-Verbindung im Durchschnitt 24 Stunden besteht.

Tabelle 5.4: *Angenommene Eigenschaften der Kommunikationsanbindung intelligenter Stromzähler.*

Eigenschaft	Annahme
Maximale Sendedatenrate	512 kbit/e
Maximale Empfangsdatenrate	6 000 kbit/s
Zuverlässigkeit	99,5%

Zusätzlich zur durchschnittlichen Verbindungsdauer muss auch die durchschnittliche Dauer bis zur Wiederverbindung abgeschätzt werden. Da hierzu auch in [88] keine Angaben gemacht werden, wird die errechnete Verfügbarkeit aus durschnittlicher Verbindungsdauer und durchschnittlicher Nichtverfügbarkeit herangezogen. Um einen realistischen Vergleichswert für die Verfügbarkeit zu ermitteln wurde die garantierte Verfügbarkeit einer Standleitung der Deutschen Telekom herangezogen [33]. Für diese garantiert der Anbieter eine Verfügbarkeit von 98,5%. Bei einer doppelten Ausfertigung der Anbindung (Zweitanbindung) erhöht sich die Garantie auf 99,5%. Unter dem Gesichtspunkt, dass die abgegebenen Garantien sicherlich Reserven des Anbieters enthalten, wird für eine DSL-Anbindung die höhere Verfügbarkeit betrachtet.

Die Fluktuation der intelligenten Stromzähler (im Folgenden *Churn* genannt) wird mittels des LifetimeChurn-Generators aus OverSim erzeugt. Dessen Weibull-Verteilung wurde mit dem Form-Parameter $k = 1$ parametrisiert, welcher zufällige, externe Ereignisse modelliert. Diese Verteilung wird häufig zur Modellierung zufälliger Zeitintervalle benutzt und kommt beispielsweise bei der Modellierung von Geräteausfällen während der Betriebsphase zum Einsatz.

Im Folgenden wird der hier motivierte Churn als *normaler Churn* bezeichnet. Gesteigerter Churn wird durch eine Variation der durchschnittlichen Verbindungsdauer und damit einer Variation der Verfügbarkeit erzeugt.

Die angenommenen Eigenschaften der Kommunikationsanbindung der intelligenten Stromzähler ist in Tabelle 5.4 zusammengefasst.

Stromverbrauch der Haushalte

Der Stromverbrauch der Haushalte wurde in OverGrid mittels profilbasierten Verbrauchern modelliert (siehe Abschnitt 4.3.3). Hierfür wurden aktualisierte, gängige VDEW-Standardlastprofile auf der Basis von [93] für die Übergangszeit

(März-Mai) verwendet. Diese wurden auf den durchschnittlichen Verbrauch von Ein- bis Sechs-Personen-Haushalten gemäß Informationen einer Erhebung der EnergieAgentur NRW [45] skaliert. Aus der gleichen Quelle wurde die Verteilung der Haushaltsgrößen verwendet.

Der profilbasierte Verbrauch der Haushalte wurde durch einen zufälligen Verbraucher mit einer geringen Maximallast (siehe Abschnitt 4.3.2) von 200 Watt ergänzt.

5.5.4 Leistung

Um die Effizienz der eingeführten Konzepte zu untersuchen, wurde SMART-ER mit SMART+ verglichen. Da der maximale Fragmentwert in SMART+ starken Einfluss auf die Smart Metering Ergebnisse hat, ist der Maximalwert der Fragmente in beiden Implementierungen konfigurierbar.

Im Folgenden werden zur Untersuchung der Leistung von SMART-ER folgende Untersuchungen durchgeführt:

- Untersuchung von SMART+ und SMART-ER bezüglich der Abhängigkeit des Messfehlers vom maximalen Fragmentwert
- Vergleich von SMART+ und SMART-ER bezüglich Skalierbarkeit der Verfahren
- Vergleich von SMART+ und SMART-ER bezüglich der Leistung unter Churn
- Untersuchung von SMART-ER bei variierender Gruppengröße
- Vergleich von SMART-ER und Baseline bezüglich Skalierbarkeit
- Vergleich von SMART-ER und Baseline bezüglich der Leistung unter Churn

Da SMART+, auch für Teilmengen, keine fehlerfreien Ergebnisse liefert, ist ein Vergleich mittels des Messfehlers als Metrik angebracht. Dieser sei pro Messintervall f_m für $m \in M$ definiert als Differenz vom Smart Metering Ergebnis zum tatsächlich gemessenen Wert. Zur Bewertung der erzielten Messergebnisse wurde das quadratische Mittel (siehe Gleichung 5.10) der Messfehler über den Versuchszeitraum verwendet. Das quadratische Mittel wird in der Statistik häufig als Maß für die Qualität eines Schätzers verwendet. Dabei fließt die Abweichung zwischen Schätzung und Beobachtung quadratisch ein. Hierdurch werden stärkere Abweichungen „härter“ bestraft als weniger starke Abweichungen.

$$QMW = \sqrt{\frac{1}{|M|} \sum_{m \in M} f_m^2} \tag{5.10}$$

Im Folgenden wird auch die Extrapolation der Smart Metering Ergebnisse betrachtet. Die Aussage der Ergebnisse über eine Teilmenge von Z wird also auf die Gesamtmenge Z hochgerechnet. Für SMART+ wird das Smart Metering Ergebnis durch $|Z^{(A)}|$ geteilt und mit $|Z|$ multipliziert. Für SMART-ER wird das Ergebnis entsprechend durch $|Z^{(V)}|$ geteilt und mit $|Z|$ multipliziert.

Zunächst wird ein Vergleich der SMART+ Implementierung mit SMART-ER bezüglich des maximalen Fragmentwerts vorgenommen. Ziel dieses Vergleichs ist die Abhängigkeit, respektive Unabhängigkeit, der Smart Metering Ergebnisse vom maximalen Wert der Fragmente zu zeigen. Da der Fragmentierungsmechanismus von SMART-ER Fragmente aus ganz $\mathbb{Z}/q\mathbb{Z}$, also im Speziellen Fragmente mit sehr hohem Wert, erzeugt, stellt diese Unabhängigkeit eine wichtige Protokolleigenschaft dar. Die Abhängigkeitsverfolgung und -auflösung von SMART-ER garantiert, dass Fragmente nur dann in das Smart Metering Ergebnis eingehen, wenn alle Abhängigkeiten erfüllt sind. Der entstehende Messfehler entspricht also den Messwerten der intelligenten Stromzähler, die entweder keinen Abgabewert abgeben konnten oder deren Abgabewert aufgrund nicht erfüllter Abhängigkeiten nicht in das Ergebnis eingegangen ist. Das bedeutet, dass für SMART-ER erwartet wird, dass das Smart Metering Ergebnis unabhängig vom maximalen Fragmentwert ist. Da ein Verlust eines Abgabewerts in SMART+ nicht weiter behandelt wird, zieht er eine Verfälschung des Smart Metering Ergebnisses nach sich. Wie stark diese Verfälschung ist, hängt vom Wert der dadurch verlorenen Fragmente ab. Für SMART+ wird also eine Abhängigkeit der Smart Metering Ergebnisse vom maximalen Fragmentwert erwartet.

Als Vergleichszenario wurde in OverGrid ein Tagesverlauf des Smart Meterings durchgeführt und das quadratische Mittel über die einzelnen Messintervalle des Tages gebildet. Das quadratische Mittel wird dann als Vergleichsmetrik verwendet. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.5 zusammengefasst.

In Abbildung 5.15 ist das quadratische Mittel der Messfehler (y-Achse) in Abhängigkeit vom maximalen Fragmentwert (x-Achse) samt 98%-Konfidenzintervall aufgetragen. SMART+ (Symbol: Quadrat) und SMART-ER (Symbol: Kreis) wurden je zweimal eingezeichnet. Einmal das unmittelbare Smart Metering Ergebnis (nicht ausgefülltes Symbol) und einmal das extrapolierte Ergebnis (ausgefülltes Symbol). Wie in der Abbildung zu sehen ist, hängt das direkte und das extrapolierte

Tabelle 5.5: *Parameterkonfigurationen zur Untersuchung des Einflusses des maximalen Fragmentwerts auf den Messfehler von SMART+ und SMART-ER.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	1 000
Churn	normal
Simuliertes Messintervall	15 Minuten
Simulations-Wiederholungen	je Parametrisierung 50
Simulierter Zeitraum	1 Tag (96 Messintervalle)
Maximaler Fragmentwert	$\{1\,000, 2\,000, \ldots, 20\,000\}$
Anzahl versendeter Fragmente J	2
Gruppengröße (nur SMART-ER)	$J+1$

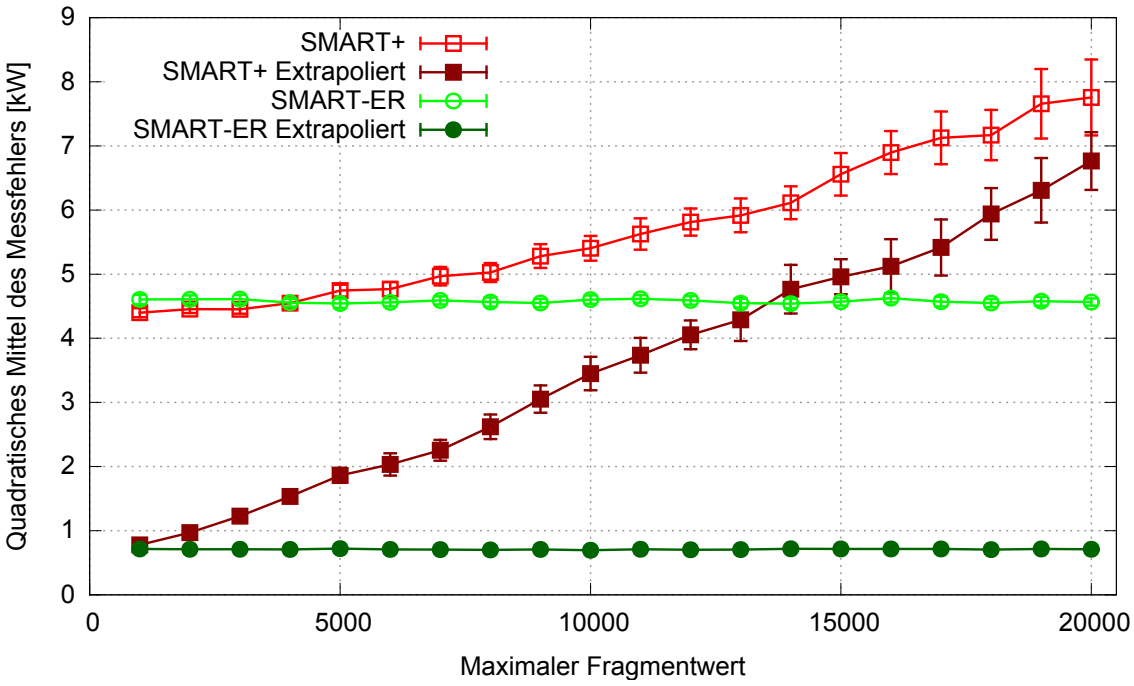


Abbildung 5.15: *Quadratisches Mittel des Messfehlers in Abhängigkeit des maximalen Fragmentwerts.*

Smart Metering Ergebnis von SMART-ER nicht vom maximalen Fragmentwert ab. Das Smart Metering Ergebnis zwischen dem kleinsten betrachteten maximalen Fragmentwert (1 000) und dem größten betrachteten maximalen Fragmentwert (20 000) unterscheidet sich lediglich um 0,03 kW – also 30 W (direkt), respektive 4 W (extrapoliert). Im Verlauf zeigt sich eine sehr geringe Varianz und die Konfidenzintervalle des Messfehlers von SMART-ER sind so klein, dass sie größtenteils durch das Symbol verdeckt werden. Das Ergebnis von SMART+ hingegen hängt stark vom maximalen Fragmentwert ab. Das Smart Metering Ergebnis zwischen dem kleinsten betrachteten maximalen Fragmentwert und dem größten betrachteten maximalen Fragmentwert unterscheidet sich um 3,35 kW (direkt), respektive 5,98 kW (extrapoliert). Wie man an den großen Konfidenzintervallen erkennen kann, streut der Messfehler von SMART+ stärker.

Für besonders kleine maximale Fragmentwerte ist zu beobachten, dass SMART+ sogar geringfügig genauere Werte als SMART-ER liefert. Die Ursache hierfür liegt in der geringen Auswirkung der Fragmente. Fällt in SMART+ ein intelligenter Stromzähler durch Churn aus, so ist der verursachte Fehler durch die Fragmente nur klein. Zusätzlich führt der Ausfall eines intelligenten Stromzählers in SMART+ nicht automatisch zu weiteren Ausfällen. In SMART-ER führt der Ausfall eines intelligenten Stromzählers unweigerlich auch zum Ausfall seiner Gruppenmitglieder. Mit einem sehr kleinen maximalen Fragmentwert können jedoch auch nur Fragmente mit kleinem Wert aus einer kleinen Menge von möglichen Fragmenten zufällig gezogen werden. Dies beeinträchtigt den Privatsphärenschutz, da große Messwerte möglicherweise nur noch unzureichend maskiert werden können.

Steigert sich der maximale Fragmentwert, so steigert sich auch der Messfehler in SMART+. Das Gleiche gilt für die Streuung des Messfehlers. Die Konfidenzintervalle werden größer. Auch der Messfehler der extrapolierten Ergebnisse von SMART+ wächst mit steigendem maximalem Fragmentwert an. Vergleicht man den Verlauf von SMART+ mit dem Verlauf des extrapolierten SMART+, so ist zu erkennen, dass das extrapolierte SMART+ schneller ansteigt als SMART+. Für den größten, betrachteten maximalen Fragmentwert von 20 000 berühren sich die Konfidenzintervalle von SMART+ und dem extrapolierten SMART+. Die Grundlage, die SMART+ für die Extrapolation darstellt, ist hier also so ungenau, dass mittels Extrapolation nur noch eine geringfügige Verbesserung der Ergebnisse erreicht werden kann.

Im weiteren Verlauf des Vergleichs von SMART+ mit SMART-ER werden zwei maximale Fragmentwerte betrachtet: 3 000 und 10 000. Da SMART+ mit größeren maximalen Fragmentwerten wesentlich ungenauere Ergebnisse liefert wurde der

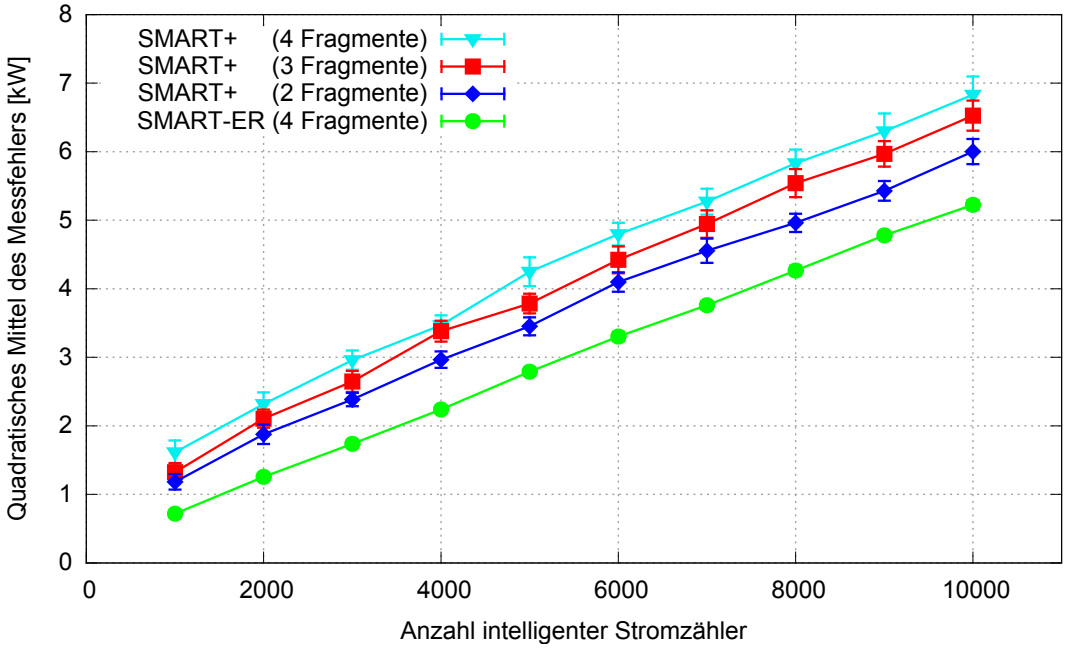
Tabelle 5.6: *Parameterkonfigurationen zur Untersuchung der Skalierbarkeit von SMART+ und SMART-ER.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{1\,000, 2\,000, \ldots, 10\,000\}$
Churn	normal
Simuliertes Messintervall	15 Minuten
Simulations-Wiederholungen	je Parametrisierung 50
Simulierter Zeitraum	1 Tag (96 Messintervalle)
Maximaler Fragmentwert	$\{3\,000, 10\,000\}$
Anzahl versendeter Fragmente J	$\{2, 3, 4\}$
Gruppengröße (nur SMART-ER)	$J + 1$

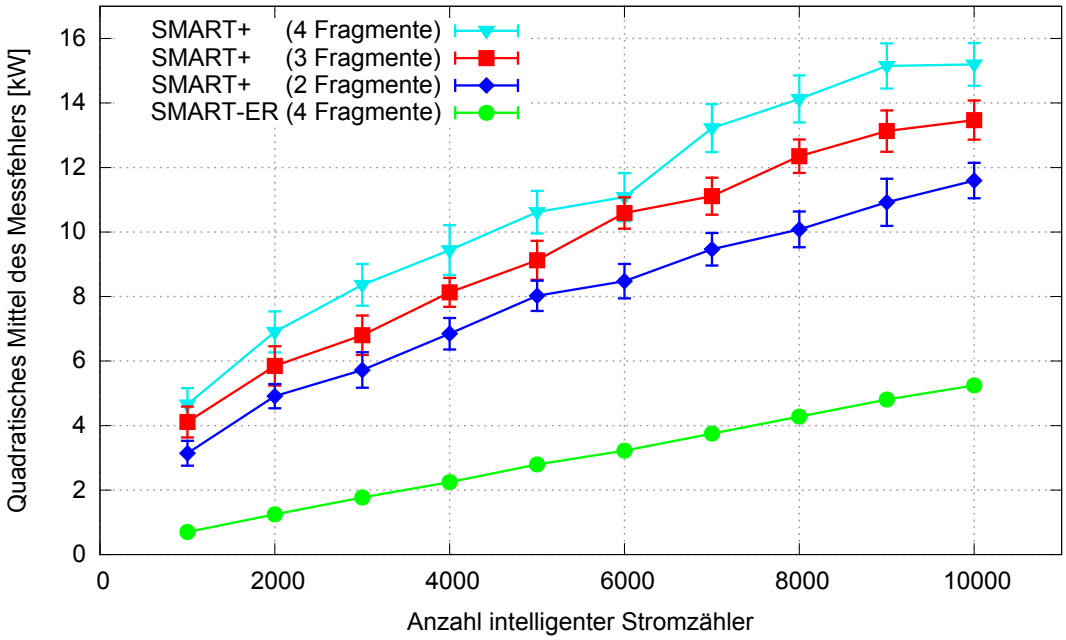
niedrige Wert von 3 000 zur besseren Vergleichbarkeit gewählt. Da der Schutz der Privatsphäre in dieser Konfiguration bestenfalls rudimentär einzuschätzen ist, wurde auch der etwas besser zu bewertende Wert von 10 000 betrachtet.

Um die Skalierbarkeit der Verfahren zu betrachten, wurden Simulationen mit wechselnder Anzahl von intelligenten Stromzählern durchgeführt. Es wurde wieder ein Tagesverlauf des Smart Meterings durchgeführt und das quadratische Mittel über die einzelnen Messintervalle des Tages gebildet. Zusätzlich wurde die Anzahl der versendeten Fragmente für SMART+, respektive Anzahl an versendeten Fragmenten und Gruppengröße für SMART-ER variiert. Die für SMART-ER gewählte Gruppengröße entspricht der kleinstmöglichen Konfiguration der Gruppengröße für ein gegebenes J. Eine detaillierte Untersuchung der Auswirkungen der konfigurierten Gruppengröße wird im weiteren Verlauf dieses Abschnitts behandelt. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.6 zusammengefasst.

In Abbildung 5.16a ist der quadratische Messfehler der Verfahren mit maximalem Fragmentwert von 3 000 aufgetragen. In Abbildung 5.16b ist dieselbe Untersuchung mit einem maximalen Fragmentwert von 10 000 zu sehen. Wie in Abschnitt 5.3.5 erläutert, führt eine Erhöhung von J bei SMART-ER nicht zu einer Erhöhung des Messfehlers, da bereits bei $J = 2$ die Äquivalenzklasse fast immer die gesamte Gruppe umfasst. In dieser Untersuchung konnte dieses Verhalten belegt werden: für alle Belegungen von J erreichte SMART-ER qualitativ den gleichen Messfehler. Bei der Darstellung in Abbildung 5.16 wären die Ergebnisse



(a) *Für einen maximalen Fragmentwert von 3 000.*



(b) *Für einen maximalen Fragmentwert von 10 000.*

Abbildung 5.16: *Quadratisches Mittel des Messfehlers in Abhängigkeit der Anzahl an simulierten intelligenten Stromzählern.*

Tabelle 5.7: *Parameterkonfigurationen zur Untersuchung der Robustheit unter stärkerem Churn von SMART+ und SMART-ER.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	1 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simuliertes Messintervall	15 Minuten
Simulations-Wiederholungen	je Parametrisierung 50
Simulierter Zeitraum	1 Tag (96 Messintervalle)
Maximaler Fragmentwert	$\{3\,000, 10\,000\}$
Anzahl versendeter Fragmente J	2
Gruppengröße (nur SMART-ER)	$J+1$

für SMART-ER mit variierendem J deckungsgleich. Zur besseren Übersichtlichkeit ist daher nur eine Parametrisierung eingezeichnet ($J = 4$).

Erwartungsgemäß steigt der Messfehler bei allen Verfahren linear mit der Anzahl der teilnehmenden intelligenten Stromzähler. Je mehr intelligente Stromzähler beteiligt sind, desto mehr intelligente Stromzähler werden von Churn betroffen. Es ist aber zu beobachten, dass SMART+ mit mehr intelligenten Stromzählern auch stärker variierende Messfehler produziert (größere Konfidenzintervalle). Die Konfidenzintervalle von SMART-ER werden in dieser Skalierung durch das Symbol selbst verdeckt. Auch führen mehr Fragmente zu höheren Messfehlern. Bei der Betrachtung von Abbildung 5.16b ist zu beachten, dass eine andere Skalierung als in Abbildung 5.16a vorliegt. Die y-Achse hat hier einen doppelt so hohen Maximalwert. Es ist zu erkennen, dass die Ergebnisse mit einem maximalen Fragmentwert von 10 000 für SMART+ deutlich schlechter ausfallen (mehr als doppelt so hoher Messfehler verglichen mit den Ergebnissen für einen maximalen Fragmentwert von 3 000), während sie für SMART-ER identisch sind.

Da unterschiedliche Gruppengrößen in SMART-ER in diesen Skalierungen nicht erkennbar sind, wird eine Betrachtung der Auswirkung unterschiedlicher Gruppengrößen getrennt von SMART+ im weiteren Verlauf der Arbeit durchgeführt.

Um den Vergleich zwischen SMART+ und SMART-ER abzuschließen wurde auch die Auswirkung von höherem Churn untersucht. Hierzu wurde der Churn vom als

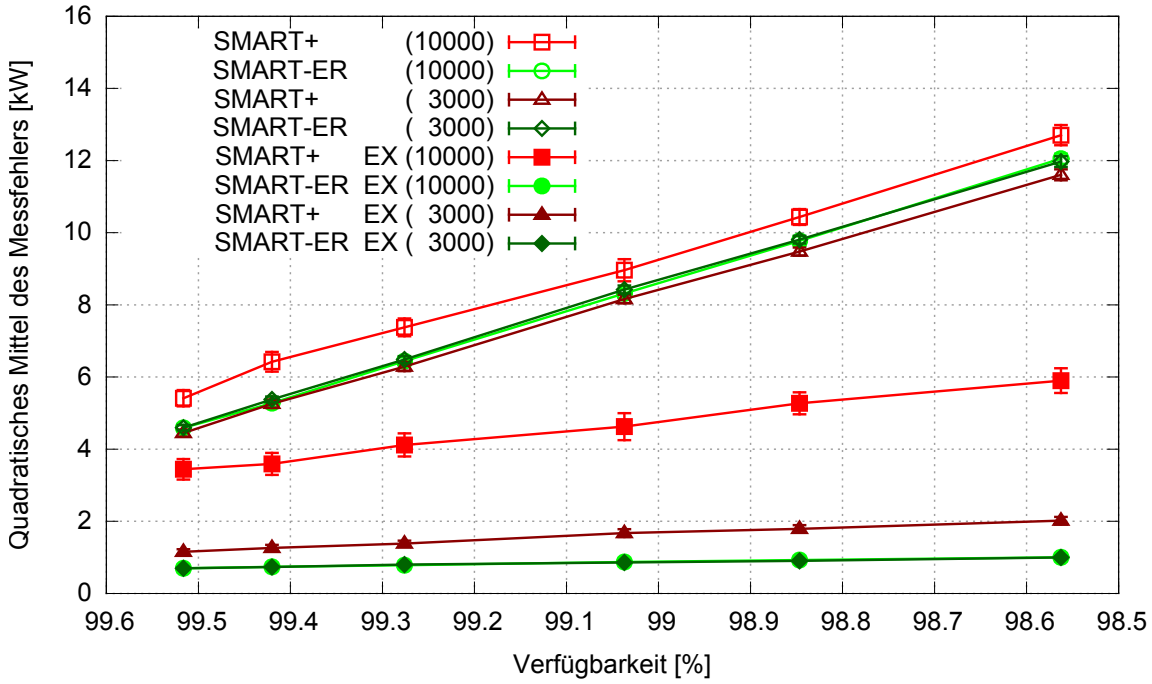


Abbildung 5.17: *Quadratisches Mittel des Messfehlers in Abhängigkeit des Churns. Simuliert für 1 000 intelligente Stromzähler über einen Tag.*

normal bezeichneten Churn, der einer Verfügbarkeit von $\approx 99,5\%$ entspricht, bis zu starkem Churn ($\approx 98,55\%$) variiert. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.7 zusammengefasst.

In Abbildung 5.17 ist der quadratische Messfehler in Abhängigkeit von der durchschnittlichen Verfügbarkeit (also des Churns) mit 98%-Konfidenzintervallen (meist verdeckt durch das Symbol) aufgetragen. Wieder wird unterschieden zwischen extrapolierten Ergebnissen (ausgefüllte Symbole, Zusatz „EX“) und direkten Smart Metering Ergebnissen (nicht ausgefüllte Symbole). Für jeden konfigurierten maximalen Fragmentwert ist eine separate Kurve eingezeichnet. Erwartungsgemäß steigt der quadratische Messfehler mit sinkender Verfügbarkeit an.

Betrachtet man zunächst die nicht extrapolierten Ergebnisse (nicht ausgefüllte Symbole), so ist zu erkennen, dass die Ergebnisse für beide maximalen Fragmentwerte (3 000 und 10 000) von SMART-ER (Symbol: Kreis und Raute) deckungsgleich sind. Sie liegen ungefähr gleichauf mit den Ergebnissen für SMART+ und einem maximalen Fragmentwert von 3 000 (Symbol: Dreieck). Bei höherem Churn ist ein geringfügig schlechteres Ergebnis für SMART-ER zu beobachten. Dies liegt an der Abhängigkeit innerhalb der Gruppe. Fällt ein intelligenter Stromzähler der

Gruppe aus, so fehlt das gesamte Aggregat der Gruppe im endgültigen Ergebnis. Der Messfehler von SMART-ER steigt hier also etwas stärker als der von SMART+. Betrachtet man aber die, privatsphärentechnisch weniger bedenkliche, Konfiguration mit einem maximalen Fragmentwert von 10 000, so liefert SMART+ hier ungenauere Ergebnisse als SMART-ER.

Vergleicht man jedoch die extrapolierten Ergebnisse für maximale Fragmentwerte von 3 000 (Symbol: Dreieck und Raute), so zeigt sich, dass SMART-ER auch bei stärkerem Churn eine bessere Grundlage zur Extrapolation bietet als SMART+. Die Ursache hierfür liegt in der Genauigkeit der Ausgangswerte für die Extrapolation. SMART-ER liefert einen aggregierten Wert, der dem Aggregat der Messwerte der erfassten intelligenten Stromzähler ($Z^{(V)}$) entspricht. Dieses Aggregat bildet eine gute Ausgangsbasis für eine Extrapolation. SMART+ liefert einen aggregierten Wert, der *nicht* dem Aggregat der Messwerte der erfassten intelligenten Stromzähler ($Z^{(A)}$) entspricht. Das Aggregat von SMART+ ist mit einem Fehler behaftet und bildet daher keine gute Ausgangsbasis für eine Extrapolation. Insbesondere verschlechtert sich die Qualität der extrapolierten Smart Metering Ergebnisse von SMART+ mit stärkerem Churn.

Betrachtet man die extrapolierten Ergebnisse für maximale Fragmentwerte von 10 000 (Symbol: Quadrat und Kreis), so sind die Ergebnisse für SMART-ER deckungsgleich mit denen mit maximalem Fragmentwert von 3 000 (Symbol Raute). Für SMART+ jedoch ist das extrapolierte Ergebnis mit einem wesentlich höheren Messfehler behaftet als mit einem maximalen Fragmentwert von 3 000.

Der Vergleich zwischen SMART+ und SMART-ER zeigt, dass die eingeführten Mechanismen zu besseren Ergebnissen führen. Selbst mit für SMART+ günstiger, und damit privatsphärentechnisch bedenklicher, Parametrisierung sind die Ergebnisse von SMART-ER robuster. Zusätzlich sind die fehlerfreien Aussagen von SMART-ER eine bessere Basis für eine genaue Extrapolation.

Im weiteren Verlauf werden zunächst die Auswirkungen der konfigurierbaren Gruppengröße in SMART-ER untersucht und dann ein Vergleich zwischen SMART-ER und Baseline durchgeführt. Dieser Vergleich erlaubt eine Abschätzung, inwieweit Nachteile durch den Einsatz von privatsphärengerechtem Smart Metering mittels SMART-ER im Vergleich zu nicht privatsphärengerechtem Smart Metering zu erwarten sind. Da die beiden, im Folgenden betrachteten, Verfahren keine fehlerbehafteten Ergebnisse liefern, kann als Metrik der Anteil der validen Abgabewerte an der Gesamtmenge der intelligenten Stromzähler Z betrachtet werden. Für SMART-ER entspricht dies $|Z^{(V)}/|Z||$. Für Baseline kann $|Z^{(A)}/|Z||$ verwendet werden, da jeder abgegebene Wert valide ist. Diese Vergleichsmetrik

Tabelle 5.8: *Parameterkonfigurationen zur Untersuchung der Gruppengröße von SMART-ER.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	1 000
Churn	$\approx 99,5\%$ und $\approx 99,0\%$ Verfügbarkeit
Simuliertes Messintervall	15 Minuten
Simulations-Wiederholungen	je Parametrisierung 150
Maximaler Fragmentwert	2^{32}
Gruppengröße	$G \in \{3, 4, \ldots, 20\}$
Anzahl versendeter Fragmente	Gruppengröße -1

bietet den Vorteil, dass vom tatsächlichen Energieverbrauch abstrahiert werden kann und entspricht der Smart Metering Reichweite.

Zunächst wird die Gruppengröße von SMART-ER näher betrachtet. Hierfür wurde untersucht, inwiefern sich der Anteil valider Abgabewerte pro Messintervall mit steigender Gruppengröße verhält. Auch wurde zum Vergleich ein erhöhter Churn betrachtet. SMART-ER wurde so konfiguriert, dass ein intelligenter Stromzähler Fragmente immer an alle anderen intelligenten Stromzähler der Gruppe versendet. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.8 zusammengefasst.

In Abbildung 5.18 ist das Ergebnis der Untersuchung der SMART-ER Gruppengröße zu sehen. Dargestellt ist der durchschnittliche Anteil der validen Abgabewerte pro Messintervall (y-Achse) in Abhängigkeit von der konfigurierten Gruppengröße (x-Achse) mit 98%-Konfidenzintervallen. Es ist zu sehen, wie sich größere Gruppen negativ auf den Anteil valider Abgabewerte auswirken. Größere Gruppen führen zu größeren Äquivalenzklassen bezüglich der Abhängigkeit von intelligenten Stromzählern untereinander. Fällt ein intelligenter Stromzähler aus, so sind die Abgabewerte der gesamten Äquivalenzklasse, nicht valide. Da die Äquivalenzklasse sich in den meisten Fällen auf die gesamte Gruppe ausdehnt, fällt damit die gesamte Gruppe aus. Der Simulationslauf mit höherem Churn (Symbol: Quadrate) zeigt dabei, dass sich der Effekt noch verstärkt. Große Gruppen und hoher Churn stellen damit eine ungünstige Kombination dar.

Abschließend wird noch ein direkter Vergleich zwischen Baseline und SMART-ER vorgenommen. Zunächst wird dieser in Abhängigkeit der Anzahl der intelligenten Stromzähler durchgeführt. Hierfür wurden bei normalem Churn Baseline und

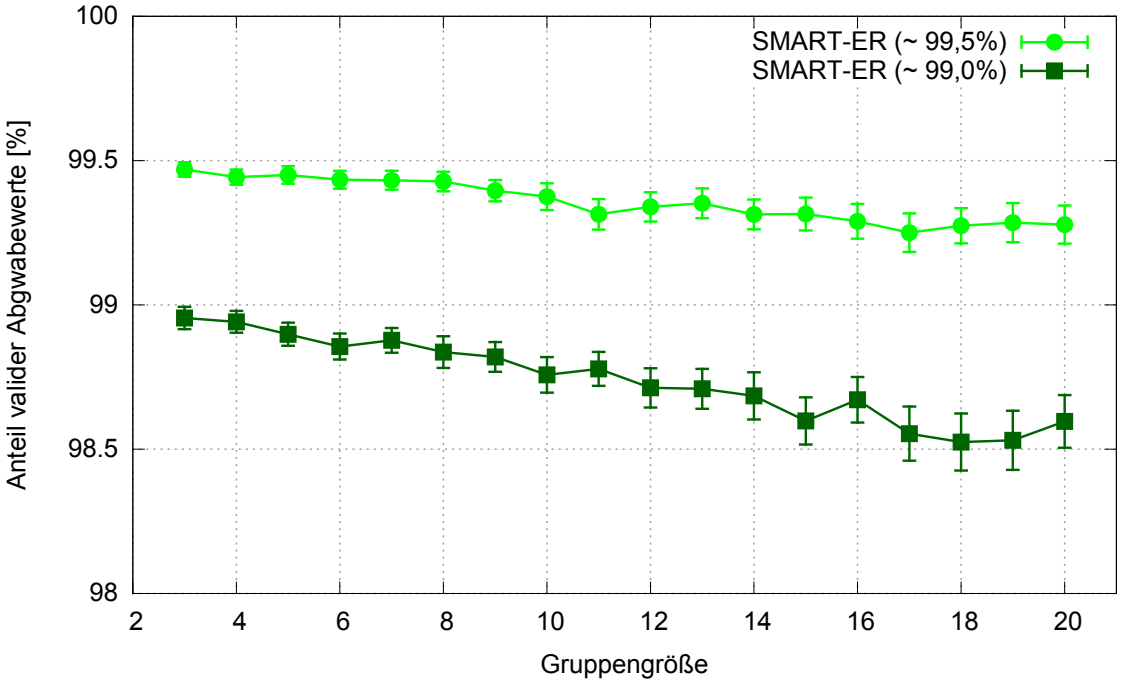


Abbildung 5.18: *Anteil valider Abgabewerte in Abhängigkeit der konfigurierten Gruppengröße und des Churns.*

SMART-ER mit variierender Gruppengröße betrachtet. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.9 zusammengefasst.

In Abbildung 5.19 wird der durchschnittliche Anteil valider Abgabewerte pro Messintervall (y-Achse) in Abhängigkeit von der Anzahl teilnehmender intelligenter Stromzähler (x-Achse) mit 98%-Konfidenzintervallen dargestellt. Jeder Konfiguration der Gruppengröße von SMART-ER ist als eigene Kurve eingezeichnet. In der Abbildung ist zu erkennen, dass SMART-ER (Symbol: Kreis, Quadrat, Raute) konsistent weniger valide Abgabewerte liefert als Baseline (Symbol: Kreuz). Dieses Ergebnis ist zu erwarten, da Baseline keinerlei Abhängigkeiten unter den intelligenten Stromzählern hat. Daher fehlen hier lediglich die intelligenten Stromzähler, die durch den Churn von einer Abgabe abgehalten wurden. Bei SMART-ER kommen zu diesen fehlenden Stromzählern noch die Abhängigkeiten hinzu. Diese Abhängigkeiten korrelieren mit der Gruppengröße und führen daher, bei einer größeren Gruppengröße, auch zu einem schlechteren Ergebnis. Für die kleinste betrachtete Gruppengröße (Symbol: Kreis) ist nur ein geringfügiger Nachteil von SMART-ER im Vergleich zu Baseline erkennbar. Mit durchschnittlich $0,04$ Prozentpunkten unter Baseline stellt SMART-ER nur eine geringfügige Verschlechterung gegenüber

Tabelle 5.9: *Parameterkonfigurationen zum Vergleich von Baseline und SMART-ER in Abhängigkeit der Anzahl teilnehmender intelligenter Stromzähler.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{1\,000, 2\,000, \ldots, 10\,000\}$
Churn	normal
Simulations-Wiederholungen	je Parametrisierung 150
Simuliertes Messintervall	15 Minuten
Maximaler Fragmentwert	2^{32}
Gruppengröße	$G \in \{3, 10, 20\}$
Anzahl versendeter Fragmente	Gruppengröße -1

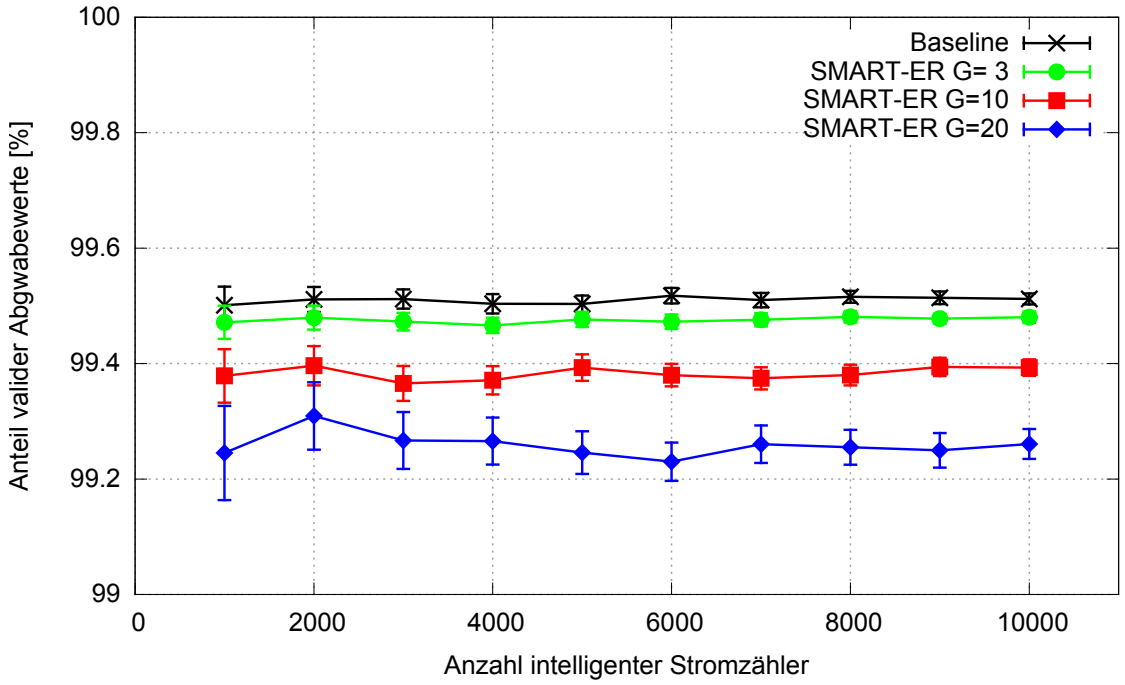


Abbildung 5.19: *Vergleich SMART-ER und Baseline bezüglich Anteil valider Abgabewerte in Abhängigkeit der Anzahl an intelligenten Stromzählern.*

Tabelle 5.10: *Parameterkonfigurationen zum Vergleich von Baseline und SMART-ER unter verschieden starkem Churn.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	1 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 150
Simuliertes Messintervall	15 Minuten
Maximaler Fragmentwert	2^{32}
Gruppengröße	$G \in \{3, 10, 20\}$
Anzahl versendeter Fragmente	Gruppengröße -1

Baseline dar. Insbesondere, wenn dies in Relation zu den 0,5 Prozentpunkten betrachtet wird, die Baseline durch Churn von 100% trennen. Bei der größten betrachtete Gruppengröße (Symbol: Raute) beträgt der Nachteil gegenüber Baseline durchschnittlich 0,16 Prozentpunkte. Ebenfalls zu erkennen ist die gute Skalierbarkeit des Verfahrens. Die Anzahl der simulierten intelligenten Stromzähler hat keinen negativen Einfluss auf die Qualität der Smart Metering Ergebnisse. Mit mehr intelligenten Stromzählern reduzieren sich die Konfidenzintervalle.

Letztlich wird noch ein Vergleich von SMART-ER und Baseline bei unterschiedlichem Churn durchgeführt. Auch hier wurde SMART-ER mit variierender Gruppengröße betrachtet. Die Parameterkonfiguration der Untersuchung ist in Tabelle 5.10 zusammengefasst.

In Abbildung 5.20 ist der durchschnittliche Anteil der validen Abgabewerte pro Messintervall (y-Achse) in Abhängigkeit des Churns mit 98%-Konfidenzintervallen aufgetragen. Jede simulierte Gruppengröße von SMART-ER wurde als eigene Kurve eingezeichnet. Die Ergebnisse zeigen, dass beide Verfahren vom stärkeren Churn betroffen sind. Dabei wird SMART-ER (Symbol: Kreis, Quadrat, Raute) mit steigendem Churn auch stärker betroffen. Der Abstand zu Baseline (Symbol: Kreuz) steigt mit zunehmendem Churn, respektive geringerer Verfügbarkeit. Während bei normalem Churn SMART-ER in der kleinsten simulierten Gruppengröße (Symbol:Kreis) durchschnittlich nur 0,04 Prozentpunkte Abstand zu Baseline hat, sind dies beim stärksten simulierten Churn durchschnittlich 0,09 Prozentpunkte. Dieser

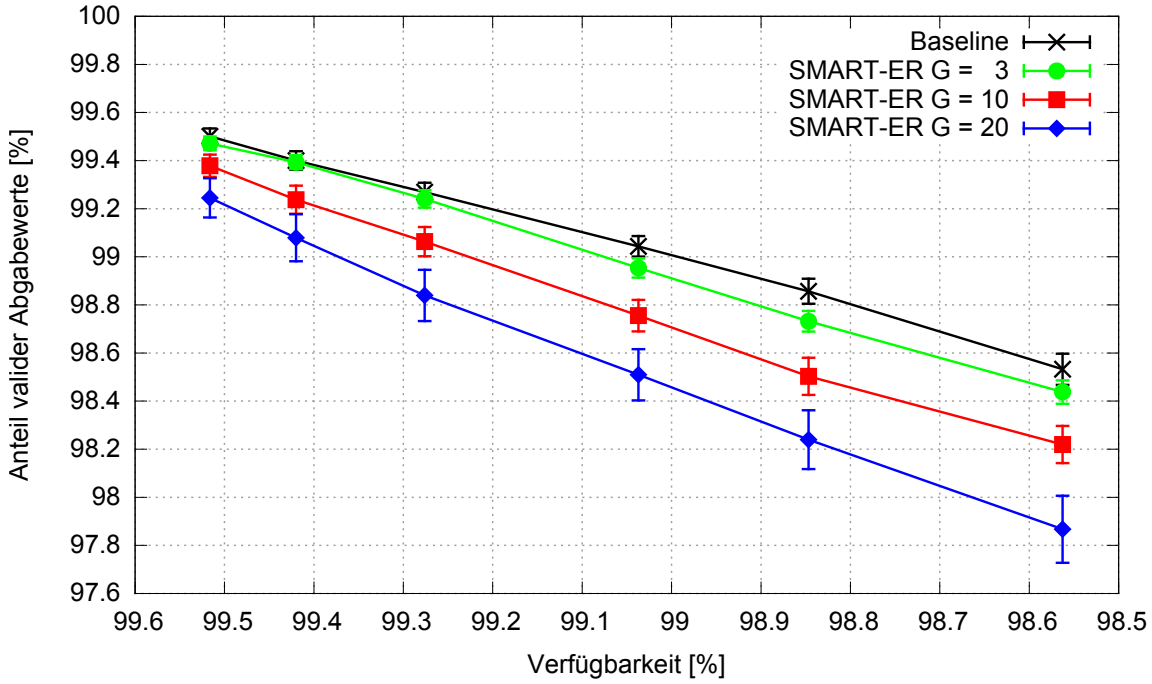


Abbildung 5.20: *Vergleich SMART-ER und Baseline bezüglich Anteil valider Abgabewerte in Abhängigkeit des Churns.*

Nachteil bei Churn intensiviert sich mit steigender Gruppengröße. Ursächlich hierfür ist die stärkere Abhängigkeiten zwischen einzelnen intelligenten Stromzählern bei größeren Gruppen.

Die hier durchgeführten Untersuchungen zeigen, dass ein Smart Metering mittels SMART-ER durchschnittlich einen geringeren Anteil an validen Abgabewerten liefert als Baseline. Der Unterschied fällt jedoch, relativ zum Anteil den Baseline insgesamt erreicht, nur geringfügig aus. Bei größeren Gruppen und höherem Churn fällt dieser Unterschied stärker aus. Die konkreten Auswirkungen dieser Unterschiede sind abhängig von der Verteilung der Messwerte über die Haushalte hinweg und von der weiteren Verwendung der durch das Smart Metering ermittelten Daten. Sie können daher im Rahmen dieser Arbeit nicht abgeschätzt werden. Da aber der Anteil valider Abgabewerte von Baseline durch Churn bereits reduziert ist, muss eine Anwendung, die durch Smart Metering ermittelte Daten verwendet, ohnehin mit diesem verringerten Anteil umgehen können.

5.5.5 Rechenaufwand

Im Folgenden werden die drei Verfahren, Baseline, SMART+ und SMART-ER bezüglich des verursachten Rechenaufwands verglichen. Da die Annahme gilt, dass es sich bei intelligenten Stromzählern um Geräte mit beschränkter Rechenkapazität handelt, ist der verursachte Rechenaufwand besonders interessant. Der Fokus dieser Betrachtung liegt auf dem Rechenaufwand, den die Verfahren selbst verursachen. Die Sicherung der Kommunikation zwischen intelligenten Stromzählern und zwischen intelligenten Stromzählern und Messdienstleister verursacht ebenfalls Rechenaufwand, der hier aber nicht betrachtet wird. Er ist implementierungsspezifisch und wird im realistischen Einsatz von der zur Verfügung stehenden Hardware abhängen und auch mittels Hardwareunterstützung realisiert werden.

Bei Baseline wird durch das Verfahren kein Rechenaufwand verursacht. Die intelligenten Stromzähler messen lediglich die Leistungsaufnahme und übermitteln diesen. Auch der Messdienstleister führt keine Berechnungen durch sondern reicht die Messwerte direkt an den Auftraggeber weiter.

Bei SMART+ wird durch Fragmentbildung und Austausch ein höherer Rechenaufwand verursacht. So müssen, dem Protokollparameter der zu versendenden Fragmente entsprechend, J Zufallszahlen gezogen werden. Jede davon verursacht eine Subtraktion. Für jedes Eintreffen eines Fragments wird eine Addition benötigt. Der Messdienstleister führt ebenfalls lediglich Additionen durch. Für jeden übermittelten Messwert eine. Der Rechenaufwand von SMART+ ist also auf wenige arithmetische Operationen und das Ziehen von Zufallszahlen beschränkt. Auch für Geräte mit beschränkter Rechenkapazität ist dieser Rechenaufwand vernachlässigbar.

SMART-ER benötigt den selben Rechenaufwand wie SMART+ und zusätzlich etwas Rechenaufwand für die Pflege der Abhängigkeitsliste eines jeden intelligenten Stromzählers. Da die Abhängigkeitsliste durch den Protokollparameter der Gruppengröße nach oben beschränkt ist, kann auch dieser Aufwand vernachlässigt werden. Der Rechenaufwand für den Messdienstleister steigt in SMART-ER jedoch signifikant durch die Abhängigkeitsauflösung. Wie bereits in Abschnitt 5.3.4 erwähnt weist der entsprechende Algorithmus eine asymptotische Laufzeit von $\Theta(n^3)$ auf. Um den Rechenaufwand abschätzen zu können, wurde der Algorithmus implementiert und auf einem Intel Core 2 Duo P8700 Prozessor mit 2,53GHz getestet. Es wurden für eine bestimmte Anzahl intelligenter Stromzähler zufällige Abhängigkeiten bestimmt und dann eine Abhängigkeitsauflösung durchgeführt. Die Anzahl an intelligenten Stromzählern würde somit der Gruppengröße entsprechen. Da-

bei konnten Abhängigkeitsauflösungen von 1 000 intelligenten Stromzählern in 1 Millisekunde durchgeführt werden. Auch bis zu 10 000 intelligente Stromzähler konnten, auch im schlechtesten Fall, in unter 20 Millisekunden abgearbeitet werden.

Zusammenfassend kann gesagt werden, dass der zusätzliche Rechenaufwand für die intelligenten Stromzähler durch das SMART-ER-Verfahren vernachlässigbar ist. Der zusätzliche Rechenaufwand für den Messdienstleister fällt durch die Abhängigkeitsauflösung höher aus. Aber auch er ist, selbst für ein Smart Metering mit einer Gruppengröße von zehntausend intelligenten Stromzählern, unkritisch.

5.5.6 Kommunikationsaufwand

In diesem Abschnitt wird der Kommunikationsaufwand von SMART-ER im Vergleich zu SMART und Baseline analysiert. Hierzu werden die zu übertragenen Nutzdaten für ein Smart Metering Intervall abgeschätzt. Hierfür spielt das verwendete Kryptosystem eine Rolle. Da die Wahl der kryptographischen Primitiven und des verwendeten Kryptosystems im realistischen Einsatz hauptsächlich von der zur Verfügung stehenden Hardware abhängt, kann hier keine Festlegung erfolgen. Der Speicherbedarf für kryptographische Primitiven wird deshalb beispielhaft dem Kryptosystem NaCl [11] entnommen. Das Kryptosystem NaCl ist im Rahmen der EU Projekte „Computer Aided Cryptography Engineering“ (CACE) [19] und „European Network of Excellence in Cryptology II“ (ECRYPT II) [41] entstanden. Es verwendet die elliptische Kurve Curve25519 [8], die Stromchiffre Salsa20 [10] und den Message-Authentication Code Poly1305 [9] um ein authentifiziertes, publickey basiertes Verschlüsselungsverfahren zu implementieren. Hierfür verwendet es pro verschlüsselter Nachricht einen sogenannten *public key authenticator*, der einerseits zur Authentifizierung der Nachricht dient und andererseits, durch das Einfließen von aufsteigenden Zahlen, Replay-Attacken verhindert. Das Signaturverfahren von NaCl basiert auf Curve25519 und der kryptologischen Hashfunktion SHA-512 [38]. Das NaCl Kryptosystem wurde ausgewählt weil es ein modernes Kryptosystem mit hohem Sicherheitsniveau darstellt und seine kryptographischen Primitiven eine einfache Berechnung des Kommunikationsaufwands ermöglichen. Im realen Einsatz wäre eine Verwendung von TLS [111], unter Verwendung der in Hardware verfügbaren Verschlüsselungsverfahren (beispielsweise AES [101]), aufgrund der starken Verbreitung wahrscheinlich. Der Speicherbedarf für die kryptographische Primitiven ist in Tabelle 5.11 zusammengefasst. Des Weiteren werden

für die Übertragung des Messwertes 4 Byte, für einen Zeitstempel 8 Byte und für den Identifikator eines intelligenten Stromzählers 8 Byte veranschlagt.

Der Kommunikationsaufwand von Baseline besteht lediglich aus einer Nachricht pro intelligentem Stromzähler pro Messintervall. Die Nachricht enthält einen Messwert samt Zeitstempel und Identifikator. Sie wird verschlüsselt übertragen. Da davon auszugehen ist, dass der Messdienstleister bereits über die öffentlichen Schlüssel der zugehörigen intelligenten Stromzähler verfügt, müssen diese nicht übertragen werden. Lediglich der public-key authenticator muss noch zur Authentifizierung angehängt werden. Pro intelligentem Stromzähler und Messintervall fallen also $4+8+24+8=44$ Byte Nutzdaten an.

Für SMART+ fällt derselbe Kommunikationsaufwand zur Abgabe der Werte beim Messdienstleister an. Zusätzlich müssen noch Fragmente zwischen den intelligenten Stromzählern ausgetauscht werden. Eine solche Nachricht besteht aus Fragment (4 Byte), Identifikator (8 Byte) und public-key authenticator (24 Byte). Also $4+8+24=36$ Byte. Die Anzahl verschickter Fragmente pro intelligentem Stromzähler ist durch den Protokollparamenter J bestimmt. Ein intelligenter Stromzähler verschickt also $J \times 36+44$ Byte innerhalb eines Messzyklus.

SMART-ER unterscheidet sich, den Kommunikationsaufwand betreffend, zu SMART+ lediglich in der Abgabe beim Messdienstleister. Sie enthält, neben den schon bei Baseline benötigten Daten, noch eine Liste der Abhängigkeiten, also Identifikatoren. Die Länge dieser Liste ist nach oben durch die Gruppengröße $|G|$ begrenzt. Bei Abhängigkeit von allen anderen Gruppenmitgliedern ist der Kommunikationsaufwand von SMART-ER zur Abgabe beim Messdienstleister maximal $(|G|-1) \times 8+44$ Bytes. Diese Werte sind in Tabelle 5.12 zusammengefasst.

Um SMART+ und SMART-ER direkt zu vergleichen kann die Gruppengröße $|G|$ anhand der Fragmentzahl J mit $|G|=J+1$ bestimmt werden. Dadurch werden Fragmente an dieselbe Zahl von anderen intelligenten Stromzählern versendet. Der Mehraufwand von SMART-ER zu SMART+ resultiert dann lediglich in der Abhängigkeitsliste, die mit $(|G|-1) \times 8$ Byte veranschlagt ist. Daher ist selbst bei sehr großen Gruppengrößen der Mehraufwand durch SMART-ER im Vergleich zu SMART+ vernachlässigbar.

Im direkten Vergleich zwischen SMART-ER und Baseline fällt vor allem die zusätzliche Kommunikation zwischen intelligenten Stromzählern auf. Doch auch dies umfasst bei moderater Gruppengröße $|G|$ oder limitiertem Fragmentversand J mit wenigen hundert Byte ein sehr kleines Datenvolumen pro intelligentem Stromzähler. Selbst mit stark limitierter Kommunikationsinfrastruktur ist dieser Kommunikationsaufwand vernachlässigbar. Auch durch die Zunahme der an den

Tabelle 5.11: *Speicherbedarf für kryptographische Primitiven in Nachrichten.*

Kryptographische Primitive	Speicherbedarf [Byte]
Authenticated Public-Key Encryption (Curve25519XSalsa20Poly1305)	
Public key	32 Byte
Private key	32 Byte
Public-key authenticator	24 Byte
Public-Key Signatures (Ed25519)	
Public key	32 Byte
Private key	64 Byte
Signatur	64 Byte

Tabelle 5.12: *Kommunikationsaufwand der Verfahren im Vergleich.*

Vorgang	Kommunikationsaufwand [Byte]
Baseline	
Fragmentierung	—
Abgabe beim Messdienstleister	44 Byte
SMART+	
Fragmentierung (J Fragmente)	$J \times 36$ Byte
Abgabe beim Messdienstleister	44 Byte
SMART-ER	
Fragmentierung ($\|G\|-1$ Fragmente)	$(\|G\|-1) \times 36$ Byte
Abgabe beim Messdienstleister	$(\|G\|-1) \times 8 + 44$ Byte

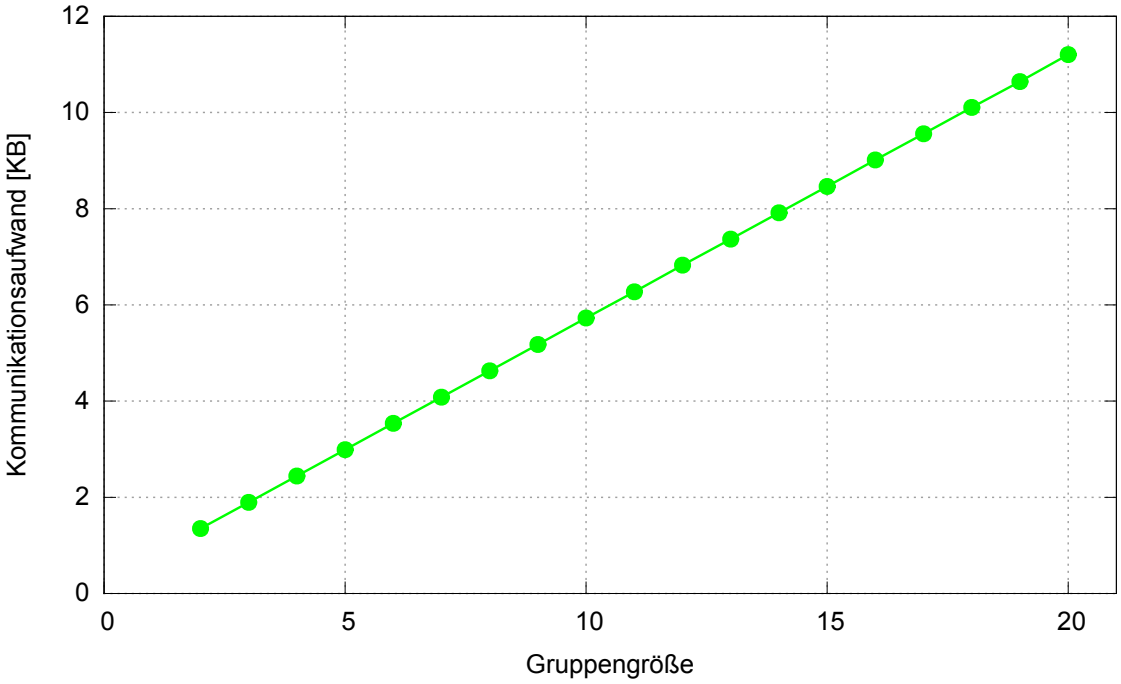


Abbildung 5.21: *Kommunikationsaufwand von SMART-ER für ein Messintervall in Abhängigkeit von der Gruppengröße.*

Messdienstleister übermittelten Daten durch die Abhängigkeitslisten entsteht nur ein geringes Datenvolumen von wenigen hundert Byte.

Der Zusammenhang zwischen Gruppengröße und Kommunikationsaufwand ist auch in den Ergebnissen der Simulation gut ersichtlich. In Abbildung 5.21 ist der Kommunikationsaufwand, also die übertragenen Bytes pro intelligentem Stromzähler pro Messintervall, in Abhängigkeit von der Gruppengröße aufgetragen. Diese beinhalten nicht nur die reinen Nutzdaten, sondern auch die für den Transport benötigten Daten (Header). Für kleine Gruppengrößen liegt der Kommunikationsaufwand bei wenigen Kilobyte pro Messintervall. Und selbst bei Gruppengrößen bis zu 20 intelligenten Stromzählern sind unter 12 Kilobyte nötig.

Bei der Betrachtung des Kommunikationsaufwands ist zu beachten, wie dieser im zeitlichen Verlauf des Messintervalls auftritt. Im Fall von SMART-ER sind die wesentlichen Ereignisse der Start des Versands der Fragmente und die Abgabe beim Messdienstleister direkt im Anschluss an den Messzeitpunkt. Durch den sehr geringen Kommunikationsaufwand stellt dies bei der angenommenen Sendedatenrate kein Problem dar. Beispielsweise können 12 Kilobyte mit der angenommenen Datenrate innerhalb von circa 180 Millisekunden übertragen werden. Auch das

beinahe gleichzeitige Eintreffen der Abgabewerte beim Messdienstleister stellt selbst bei großen Anzahlen von intelligenten Stromzählern kein Problem dar. Der Zeitraum des Eintreffens wird durch unterschiedliche Latenzen und nicht perfekt synchrone Uhren im realen Einsatz leicht variieren. Auch kann von einem Messdienstleister erwartet werden, dass er über dem Smart Metering entsprechende Ressourcen verfügt.

Zusammenfassend kann geschlossen werden, dass das SMART-ER-Verfahren im Vergleich zu SMART+ nur unwesentlich mehr Kommunikationsaufwand verursacht. Im Vergleich zu Baseline fällt dieser höher aus, ist bei moderner Kommunikationsinfrastruktur jedoch ebenfalls vernachlässigbar.

5.6 Zusammenfassung

In diesem Kapitel wurde das SMART-ER-Verfahren zum peer-to-peer Privatsphärenschutz im Smart Metering vorgestellt. Es basiert auf den Grundkonzepten des SMART-Verfahrens zur privatsphärengerechten Datenaggregation in drahtlosen Sensornetzen.

Mit SMART-ER wurde ein neuer Fragmentierungsmechanismus eingeführt, der jeglichen ungewollten Informationsfluss verhindert. Des Weiteren garantiert SMART-ER durch Abhängigkeitsverfolgung und Abhängigkeitsauflösung fehlerfreie Ergebnisse für eine möglichst große Teilmenge der intelligenten Stromzähler. Mittels Gruppenbildung werden diese auch bei Störungen der Kommunikationsinfrastruktur erreicht.

Es wurde gezeigt, dass SMART-ER genau dann die Privatsphäre eines Haushalts effektiv schützt, wenn mit mindestens einer weitere teilnehmenden Partei kooperiert wird, die nicht vom Angreifer korrumpiert ist. Dabei ist ohne Relevanz, ob diese Partei ein anderer intelligenter Stromzähler oder der Messdienstleister ist. Der erreichte Privatsphärenschutz ist damit maximal für den peer-to-peer Privatsphärenschutz. Eine einzelne, nicht korrumpierte Partei garantiert bereits die Privatsphäre, die auch durch korrumpierte Parteien nicht mehr eingeschränkt werden kann. Auch wurde gezeigt, dass SMART-ER robust gegen statistische Analysen der Abgabewerte ist. Auch wurde die Gruppenorganisation durch den Messdienstleister als möglicher Angriffsvektor identifiziert. Dieses Problem wird im folgenden Kapitel diskutiert und gelöst.

SMART-ER wurde zur Evaluation der Smart Metering Leistung im Vergleich zu einem Verfahren ohne Privatsphärenschutz und zu einer SMART Variante evalu-

iert. Die Ergebnisse zeigen die Effektivität der eingeführten Mechanismen. Auch unter Störungen der Kommunikationsinfrastruktur liefert SMART-ER fehlerfreie Aussagen über eine Teilmenge der theoretisch teilnehmenden intelligenten Stromzähler. Dabei ist der Anteil der intelligenten Stromzähler über die SMART-ER eine Aussage liefert nur geringfügig kleiner als bei einem Verfahren ohne Privatsphärenschutz. Der durch SMART-ER verursachte Mehraufwand für Kommunikation und Berechnungen ist dabei vernachlässigbar.

Kapitel 6

Dezentrale Gruppenbildung

Das im vorherigen Kapitel vorgestellte SMART-ER Verfahren ermöglicht intelligenten Stromzählern eine robuste, privatsphärengerechte Datenaggregation, die auch im Fall von Kommunikationsstörungen fehlerfreie Messergebnisse liefert. Um die Robustheit zu gewährleisten, verwendet es Gruppenbildung. Dabei wird die Gesamtmenge der intelligenten Stromzähler in disjunkte Teilmengen, die Gruppen, partitioniert. Im vorherigen Kapitel wurde angenommen, dass diese Gruppenbildung durch den Messdienstleister durchgeführt wird (siehe Abbildung 6.1). Dass dies aus privatsphärentechnischer Sicht bedenklich ist, wurde in der Evaluation der Privatsphäre diskutiert. Möglichst große Gruppen waren hier aus privatsphärentechnischer Sicht wünschenswert, während die Evaluation der Smart Metering Leistung zeigte, dass möglichst kleine Gruppen vorteilhaft sind. Dabei war die Forderung einer großen Gruppengröße maßgeblich durch den Einfluss des Messdienstleisters motiviert. Wie die Analyse gezeigt hat, ist ein Privatsphärenschutz des Einzelnen mittels SMART-ER bereits dann gewährleistet, wenn eine Partei aus der Gruppe oder der Messdienstleister nicht korrumpiert ist. Wenn der Messdienstleister keinen Einfluss auf die Gruppenzusammensetzung nimmt, so sind, betreffend des Privatsphärenschutzes des Einzelnen, auch kleine Gruppen vertretbar.

Auch ohne Einfluss des Messdienstleisters haben kleine Gruppen einen Nachteil. Der Privatsphärenschutz der Gruppe ist in besonders kleinen Gruppen weniger ausgeprägt. Das Profil einer Gruppe mit wenigen Teilnehmern offenbart mehr Informationen über einzelne Teilnehmer als das Gruppenprofil einer Gruppe mit vielen Teilnehmern. In Arbeiten zum Angriff auf die Privatsphäre von Haushalten spielt

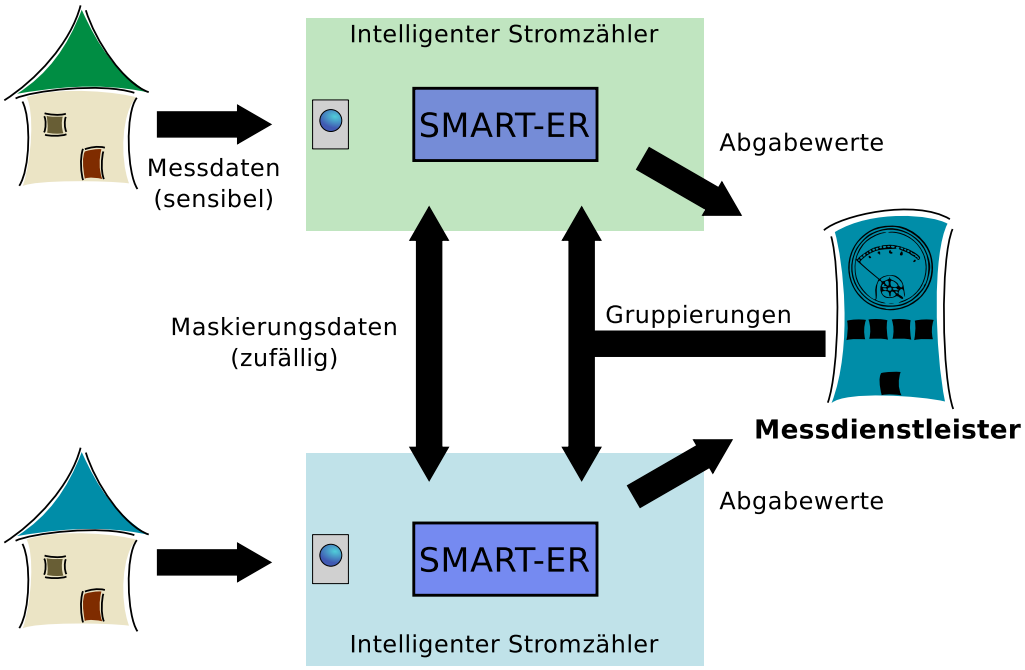


Abbildung 6.1: *Informationsfluss in SMART-ER.*

zur Informationsgewinnung insbesondere die zeitliche Abfolge von Messwerten eine Rolle (siehe beispielsweise [79, 86, 96]). Das Auftreten von Veränderungen der Messwerte im zeitlichen Verlauf, genannt *Power-Events*, gibt Aufschluss über Gewohnheiten und Besitz von bestimmten Haushaltsgeräteklassen (beispielsweise einer Klimaanlage). Ein Power-Event ist beispielsweise das manuelle Ein- und Ausschalten eines Fernsehers oder das automatische Ein- und Ausschalten einer Klimaanlage. Die Aggregation von Messwerten sorgt einerseits dafür, dass Power-Events nicht einzelnen Haushalten zugeordnet werden können und andererseits dafür, dass eine stärkere Überlappung von Power-Events ihre Erkennung erschwert. Bei einer Aggregation über eine sehr kleine Gruppe sind diese schützenden Effekte jedoch weniger ausgeprägt. Um dennoch kleine Gruppen einsetzen zu können, kann die Zusammensetzung der Gruppen über die Zeit hinweg variiert werden. Power-Events werden dann im zeitlichen Verlauf über Aggregate verteilt, zu denen unterschiedliche Haushalte beigetragen haben.

Ausgehend von der Annahme, dass insbesondere die Beobachtung von Power-Events über einen zeitlichen Verlauf eine Gefahr für den Privatsphärenschutz

darstellt und dass diese Power-Events von Messintervall zu Messintervall bei einer Vielzahl von Haushalten auftreten, lassen sich folgende Ziele formulieren:

- Bilden kleiner Gruppen zur Erhöhung der Smart Metering Leistung
- Bilden dieser Gruppen ohne Einflussnahme des Messdienstleisters
- Regelmäßiger Wechsel der Gruppenzusammensetzung zur Vermeidung der Gruppenprofilbildung

In diesem Kapitel wird *Smart Meter Speeddating (SMSD)* [51] vorgestellt. Es ist ein Verfahren zur dezentralen Gruppenbildung dessen Entwurf von diesen Zielen geprägt ist. Das Verfahren bildet Gruppen mit zufälligen, kleinen Gruppengrößen für SMART-ER. Die maximal gebildete Gruppengröße lässt sich mittels eines Parameters bestimmen. Dabei sollte dieser Parameter mindestens drei sein, um auch Smart Metering Instanzen mit ungerader Anzahl an teilnehmenden intelligenten Stromzählern zu ermöglichen. Wären nur Gruppen der Größe zwei möglich, so wäre in diesem Fall ausgeschlossen, dass alle teilnehmenden intelligenten Stromzähler Mitglied einer Gruppe sind. Intelligente Stromzähler, die nicht Mitglied einer Gruppe sind, nehmen nicht am Smart Metering teil, da dieses für sie dann nicht privatsphärengerecht wäre. Die Gruppenbildung findet in SMSD ohne Einflussnahme durch den Messdienstleister statt. Die aus einer Gruppenbildung resultierende Gruppenzusammensetzung ist zufällig. Der regelmäßige Wechsel der Gruppenzusammensetzung wird durch eine Gruppenbildung in jedem Messintervall ermöglicht. Das Zusammenspiel zwischen SMSD und SMART-ER ist in Abbildung 6.2 dargestellt.

Die Gruppenbildung in SMSD findet zufällig statt und wird für jedes Messintervall wiederholt. Das hat zur Folge, dass die Zusammensetzung der Gruppen in aufeinanderfolgenden Messintervallen mit sehr hoher Wahrscheinlichkeit unterschiedlich ausfällt. Dies verhindert die Bildung von Gruppenprofilen beim Messdienstleister und erschwert gleichzeitig einen Angriff mittels korrumpierter intelligenter Stromzähler. Bedingt durch die kleine Gruppengröße ist der Privatsphärenschutz der Gruppe (siehe Abschnitt 2.2), der sich durch die Gruppengröße ergibt, nur schwach ausgeprägt. Der häufige Wechsel der Gruppenzusammensetzung führt jedoch zu einem seltenen Auftreten der gleichen Gruppenkonfiguration. Daher kann ein Gruppenprofil auch nur wenige Einträge haben. Der Privatsphärenschutz der Gruppe ist dadurch vergleichbar mit dem Privatsphärenschutz der durch ein langes Messintervall gewährleistet wird.

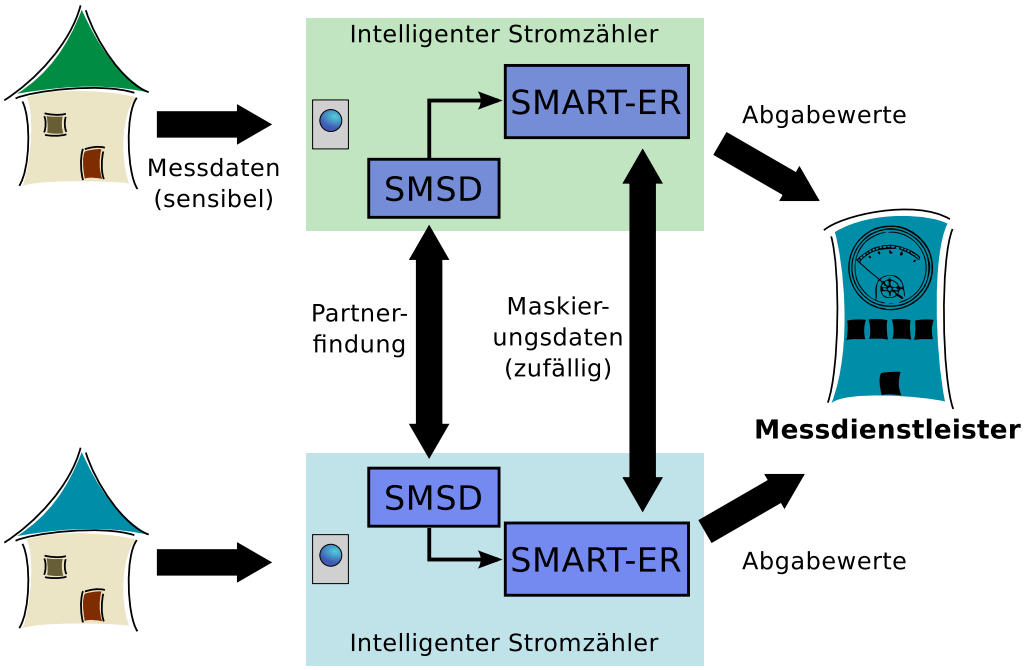


Abbildung 6.2: *Informationsfluss mit Smart Meter Speeddating.*

Wie im vorherigen Kapitel gezeigt, stellen korrumpierte Stromzähler nur dann eine Gefahr für die Privatsphäre eines Einzelnen dar, wenn sie mit dem Messdienstleister kooperieren und in derselben Gruppe sind. Ziel von Smart Meter Speeddating ist es einen Angriff auf einen ausgewählten intelligenten Stromzähler zu erschweren. Die hier vorgestellte Gruppenbildung erschwert es korrumpierten Stromzählern in die Gruppe eines ausgewählten intelligenten Stromzählers zu gelangen.

Das Kapitel ist wie folgt strukturiert. Zunächst werden in Abschnitt 6.1 Strategien zur dezentralen Gruppenbildung und die für SMSD ausgewählte Strategie vorgestellt. In Abschnitt 6.2 wird das Smart Meter Speeddating Verfahren eingeführt. Da das Verfahren mittels zahlreicher Protokollparameter konfigurierbar ist, werden in Abschnitt 6.3 die Protokollparameter untersucht und geeignete Kombinationen identifiziert. In Abschnitt 6.4 wird der durch SMSD erzielte Privatsphärenschutz diskutiert. Abschnitt 6.5 widmet sich der Untersuchung der erzielten Smart Metering Leistung bevor dann in Abschnitt 6.7 das Kapitel zusammengefasst wird.

6.1 Strategien zur dezentralen Gruppenbildung

Das Grundproblem einer dezentralen Gruppenbildung besteht darin, dass keine zentralen Entscheidungen getroffen werden können. Ob ein intelligenter Stromzähler z_1 mit einem anderen intelligenten Stromzähler z_2 kooperiert, also Mitglied seiner Gruppe wird, muss von z_1 eigenständig und lokal entschieden werden. Fällt diese Entscheidung positiv aus, kann er eine Anfrage an z_2 stellen. Dann muss auch z_2 darüber entscheiden, ob eine Kooperation mit z_1 gewollt ist. Dies birgt das Problem, dass eine Gruppe nur dann zustande kommt, wenn beide Stromzähler sich zur gemeinsamen Kooperation entscheiden. Insbesondere muss jeder der beiden Stromzähler zum Schluss kommen, dass das potentielle Gruppenmitglied eine gute Wahl darstellt.

Das Problem lässt sich in zwei grundlegende Probleme zerlegen:

- Die Auswahl eines potentiellen Partners aus der Menge der teilnehmenden intelligenten Stromzähler Z.
- Die Entscheidung über die Annahme eines anfragenden intelligenten Stromzählers.

Sei z_1 ein intelligenter Stromzähler, der durch Lösen des ersten Problems zu dem Schluss kommt, dass er mit dem intelligenten Stromzähler z_2 in einer Gruppe sein möchte. Weiter sei angenommen, dass z_2 durch Lösen des zweiten Problems zum Schluss kommt, dass auch z_1 ein geeigneter Partner ist. Somit entsteht eine Gruppe der Größe zwei mit den Mitgliedern z_1 und z_2. Um größere Gruppen als Zweiergruppen zu ermöglichen, kann diese Gruppe erweitert werden. Hierfür müssen die Rollen der intelligenten Stromzähler bei der Partnersuche genauer betrachtet werden. Dem intelligenten Stromzähler z_1 wird die Rolle *A* (**a**nfragender Stromzähler) und dem intelligenten Stromzähler z_2 die Rolle *B* (**b**ejahender Stromzähler) zugewiesen. Es existieren nun mehrere Möglichkeiten:

(1) Nur *A* darf weitere Stromzähler annehmen

(2) Nur *B* darf weitere Stromzähler annehmen

(3) *A* und *B* dürfen weitere Stromzähler annehmen

Möglichkeit (1) stellt ein Problem für die Rollenklassifizierung und für die Kontrolle der Gruppengröße dar. Falls *A* eine Anfrage eines weiteren intelligenten

Stromzählers z_3 annehmen würde, so wäre A gleichzeitig auch in der Rolle B (aus Sicht von z_3) und z_3 in der Rolle A. Da Stromzähler der Rolle A weitere Stromzähler annehmen dürfen, kann z_3 wiederum einen weiteren intelligenten Stromzähler in die Gruppe aufnehmen. Dadurch wären der Gruppengröße keine Grenzen gesetzt, was dem Entwurfsziel der kleinen Gruppen widerspricht und eine Gefahr für die Smart Metering Leistung darstellt.

Möglichkeit (2) bietet die bessere Alternative. Die Rollenverteilung bleibt hier konsistent, da z_2 weiterhin die Rolle B behält und der neu hinzukommende z_3 die Rolle A einnimmt. Die Gruppengröße wird durch B effektiv kontrolliert und kann im Rahmen der Vorgaben gehalten werden um eine hohe Smart Metering Leistung zu erzielen.

Möglichkeit (3) hat das selbe Problem wie Möglichkeit (1) und führt zu unbeschränkten Gruppengrößen. Aus diesem Grund wurde für das im Folgenden behandelte SMSD die Möglichkeit (2) gewählt. Ein intelligenter Stromzähler der Rolle A nimmt keine Anfragen an. Ein Stromzähler der Rolle B nimmt weitere Anfragen an.

6.2 Smart Meter Speeddating (SMSD)

Smart Meter Speeddating ist ein Verfahren zur dezentralen Gruppenbildung für SMART-ER. Die intelligenten Stromzähler eines Smart Meterings werden in SMSD im Rahmen der Initialisierung vom Messdienstleister lediglich mit einer Gesamtliste der an der Instanz teilnehmenden intelligenten Stromzähler versorgt. Die Gruppenbildung und der SMART-ER Fragmentaustausch werden dann *ohne* Einfluss durch den Messdienstleister ausgeführt. Dieser Vorgang wird für jedes Messintervall erneut durchgeführt, was zu ständig wechselnden Gruppenzusammensetzungen führt.

Wie in Abschnitt 2.1.4 motiviert wird auch bei SMSD davon ausgegangen, dass zwischen intelligenten Stromzählern untereinander und zwischen intelligenten Stromzählern und dem Messdienstleister kryptographisch gesicherte Verbindungen aufgebaut werden können. Die Integrität und Vertraulichkeit der Kommunikation ist damit gewährleistet. Durch den Identitätsnachweis und Zertifikatsnachweis ist ein Sybil-Angriff (siehe Abschnitt 2.4.2) nur mittels zertifizierter intelligenter Stromzähler möglich und gleichzeitig die Authentizität gewährleistet.

Das SMSD-Verfahren bildet zunächst Gruppen der Größe zwei, die dann erweitert werden. Deshalb wird, wenn eine Situation aus der Sicht eines intelligenten

Stromzählers betrachtet wird, das andere Gruppenmitglied auch als *Partner* bezeichnet. Bilden zwei intelligente Stromzähler eine gemeinsame Gruppe, so wird von einer *Paarung* von intelligenten Stromzählern gesprochen. Da auch ein Smart Metering mit einer ungeraden Anzahl von intelligenten Stromzählern von Smart Meter Speeddating unterstützt werden soll, muss mindestens eine Paarung zu einer Dreiergruppe erweitert werden. Eine Gruppenbildung mit lediglich Paarungen und nur einer erweiterten Paarung würde jedoch eine Koordination erfordern, die in einem dezentralen Verfahren nicht möglich ist[1]. Da Smart Meter Speeddating eine dezentrale Gruppenbildung durchführt, kann nicht gewährleistet werden, dass nur eine erweiterte Paarung gebildet wird.

Smart Meter Speeddating lässt sich in zwei Routinen zerlegen, die gemeinsam eine Gruppenbildung ermöglichen. Jeder intelligente Stromzähler führt diese beiden Routinen nebenläufig aus:

Suchroutine: Um einen Partner zu finden, wartet die Suchroutine einen zufälligen Zeitraum, der gleichverteilt aus dem Intervall $[0, \ldots, t_{max}]$ gezogen wird. Der Wert t_{max} ist ein Protokollparameter und entspricht der maximalen Wartezeit. Danach wählt der intelligente Stromzähler zufällig aus der Liste aller intelligenten Stromzähler einen potentiellen Partner aus und stellt eine Anfrage auf Partnerschaft an diesen. Wird diese Anfrage positiv beantwortet, so wurde ein Partner gefunden und die Suchroutine ist beendet. Ansonsten beginnt die Suchroutine von vorne.

Annahmeroutine: Damit Gruppen entstehen können, muss jeder intelligente Stromzähler auch bereit sein Anfragen auf Partnerschaft zu akzeptieren. Um aber zu vermeiden, dass ein intelligenter Stromzähler sich seinen Partner gezielt wählen kann, selektiert die Annahmeroutine zufällig aus den eintreffenden Anfragen. Dies wird dadurch erreicht, dass zu Beginn bestimmt wird, dass die ersten m eingetroffenen Anfragen abgelehnt werden. Die Zufallszahl m wird dabei aus der Menge $\{1, \ldots, m_{max}\}$ gleichverteilt gezogen. Der Wert m_{max} ist ein Protokollparameter und sorgt dafür, dass spätestens nach m_{max} eingetroffenen Anfragen eine Anfrage angenommen wird. Nach der Annahme einer Anfrage wird die Suchroutine gestoppt. Die Annahmeroutine wird jedoch wiederholt, um weitere intelligente Stromzähler in die Gruppe aufzunehmen. Das Vorgehen ist das selbe, verwendet jedoch für jeden weiteren Durchlauf eine Zufallszahl a, die aus der Menge $\{1, \ldots, a_{max}\}$ gezogen wird. Der Wert a_{max} ist ebenfalls ein Protokollparameter

[1] Zu dem Zeitpunkt, zu dem die erweiterte Paarung gebildet wird, ist globales Wissen nötig: sind alle anderen intelligenten Stromzähler bereits Mitglied einer Paarung?

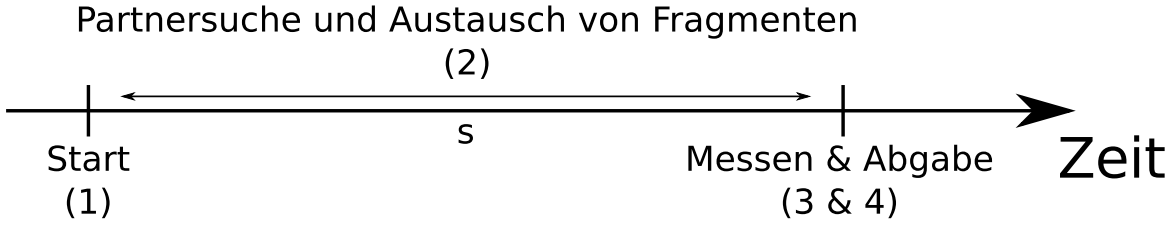


Abbildung 6.3: *Zeitlicher Ablauf von Smart Meter Speeddating.*

und sorgt dafür, dass spätestens nach a_{max} weiteren Anfragen, *nach* Annahme der letzten Anfrage, eine Anfrage angenommen wird. Die Annahmeroutine wird so oft wiederholt, bis die maximale Gruppengröße g_{max} erreicht ist.

Diese beiden Routinen werden nebenläufig auf jedem intelligenten Stromzähler durchgeführt. Lediglich während auf die Antwort einer, von der Suchroutine gesendeten, Anfrage gewartet wird, kann die Annahmeroutine eintreffende Anfragen weder positiv noch negativ beantworten. Dies hat den Hintergrund, dass in diesem Zeitraum nicht bekannt ist, ob der, von der Suchroutine, angefragte intelligente Stromzähler die Anfrage akzeptiert oder nicht. In diesem Fall beantwortet die Annahmeroutine eintreffende Anfragen mit einer neutralen Antwort. Dies hat den Vorteil, dass sofort eine Antwort gesendet werden kann. Würde zunächst auf die Antwort der ausstehenden Suchanfrage gewartet werden, so könnte die eigene Antwort stark verzögert werden. Da aber ein anderer intelligenter Stromzähler auf genau diese Antwort warten würde, wäre ein kaskadierender Effekt die Folge.

Beide Routinen werden für die konfigurierbare Suchdauer s durchgeführt. Diese wird zeitlich *vor* dem Messzeitpunkt angesiedelt (siehe Abbildung 6.3). Zum Start des Verfahrens (1) beginnen alle intelligenten Stromzähler mit Smart Meter Speeddating. Hierzu werden die beiden beschriebenen Routinen gestartet und die Suchroutine sorgt für das Versenden von Anfragen. Diese enthalten bereits ein zufälliges SMART-ER Fragment, für den Fall einer erfolgreichen Annahme. Nimmt die Annahmeroutine eine Anfrage an, so wird in der Antwort ebenfalls ein zufälliges SMART-ER Fragment mitgesendet. Dadurch mischt sich in (2) die Partnersuche und der Austausch von Fragmenten. Nach Ablauf der Suchdauer s, tritt der Messzeitpunkt (3) ein. Die intelligenten Stromzähler beenden Such- und Annahmeroutine, messen ihre Leistungsaufnahme, führen eine Maskierung mittels der SMART-ER Fragmente durch und senden den resultierenden Abgabewert an den Messdienstleister.

Tabelle 6.1: *Protokollparameter des Smart Meter Speeddating Verfahrens.*

Parameter	Variable
Menge der Zähler	$Z = \{z_1, \ldots, z_n\}$
Suchdauer	s
Maximale Gruppengröße	g_{max}
Maximale Wartezeit zwischen Anfragen	t_{max}
Maximale Anzahl abgelehnter Anfragen (initiale Gruppenbildung)	m_{max}
Maximale Anzahl abgelehnter Anfragen (erweiterte Gruppenbildung)	a_{max}

Wie zu erkennen ist, erreicht Smart Meter Speeddating die gleiche Smart Metering Latenz (siehe Abschnitt 2.1.2), die ein nicht privatsphärengerechtes Verfahren auch erreicht. Direkt nach Messen des Messwertes kann ein Abgabewert an den Messdienstleister gesendet werden. Bezüglich der Latenz entsteht also auch bei Smart Meter Speeddating *kein Nachteil* gegenüber einem nicht privatsphärengerechten Verfahren. Das kürzeste mögliche Messintervall ist in Smart Meter Speeddating jedoch limitiert durch die konfigurierbare Dauer s. Wie in Abschnitt 6.3.4 gezeigt wird, muss diese im Bereich weniger Minuten konfiguriert werden.

Die Protokollparameter des Smart Meter Speeddatings sind also die Suchdauer (s), die maximale Gruppengröße g_{max}, die Obergrenze des Intervalls für Wartezeiten der Suchroutine (t_{max}) und die jeweils späteste Erst- und Zweitannahme (m_{max}, a_{max}). Diese sind in Tabelle 6.1 zusammengefasst.

6.2.1 Suchroutine

Jeder intelligente Stromzähler wird vom Messdienstleister mit einer Liste Z, der am Smart Metering teilnehmenden intelligenten Stromzähler versorgt. Diese Liste entspricht der Zielgruppe der Smart Metering Instanz. Zusätzlich zu den Eingabeparametern pflegt jeder Stromzähler eine Liste von Stromzählern Z_T, die zu Beginn jedes Messintervalls als leere Liste initialisiert wird. Sie wird genutzt um über die bereits kontaktierten intelligenten Stromzähler Buch zu führen.

Um einen SMART-ER Partner zu finden führt ein intelligenter Stromzähler folgende Schritte durch:

(1) Warte eine zufällige Zeit t aus dem Intervall $[0, t_{max}]$

(2) Wähle einen zufälligen intelligenten Stromzähler $z_k \in Z \setminus Z_T$ aus

(3) Sende einen *pair-request* an z_k. Diese Nachricht enthält bereits ein zufälliges Fragment für eine etwaige SMART-ER Kooperation. Bis zum Eintreffen einer Antwort wird die Annahmeroutine über eine ausstehende Antwort in Kenntnis gesetzt.

Für einen versendeten *pair-request* sind drei Antworten möglich:

- *busy-deny:* Mit z_k konnte *zum gegenwärtigen Zeitpunkt* keine Gruppe gebildet werden. Die Suchroutine wird erneut gestartet.
- *pair-deny:* Mit z_k kann jetzt und auch für den Rest des Messintervalls keine Gruppe gebildet werden. Die Liste Z_T wird um z_k ergänzt und die Suchroutine erneut gestartet.
- *pair-accept:* Mit z_k konnte eine Gruppe gebildet werden. Das *pair-accept* enthält bereits ein SMART-ER Fragment zur späteren Maskierung des Messwerts. Die Suchroutine ist beendet.

Sollte der unwahrscheinliche Fall eintreten, dass $Z \setminus Z_T$ die leere Menge ist, so ist der Vorgang ebenfalls beendet. Der betreffende intelligente Stromzähler hat dann in diesem Messintervall durch die Suchroutine keinen Partner gefunden.

Der Ablauf der Suchroutine ist in Algorithmus 4 dargestellt. Durch die Suchroutine wird gewährleistet, dass ein intelligenter Stromzähler seinen Partner zufällig wählt. Wenn aber alle intelligenten Stromzähler einen Partner auswählen, so verbleibt niemand um ausgewählt zu werden. Dieses Problem wird im nächsten Abschnitt mit der Annahmeroutine gelöst.

6.2.2 Annahmeroutine

Nachdem jeder intelligente Stromzähler die Möglichkeit hat einen zufälligen Partner zu finden, muss nun auch gewährleistet werden, dass sich intelligente Stromzähler als Partner zur Verfügung stellen. Eine der wesentlichen Herausforderungen für Smart Meter Speeddating besteht darin, diese *Annahmeroutine* ebenfalls möglichst zufällig zu gestalten. Konkret muss verhindert werden, dass ein intelligenter Stromzähler direkt von einem anderen intelligenten Stromzähler zu

Algorithmus 4 Speeddating Suchroutine (searchRoutine).

$Z_T \leftarrow \emptyset$
Global Variable: *busy*
repeat
  sleep randomTime $\in [0, t_{max}]$
  $z_k \leftarrow$ selectRandomNode($Z \setminus Z_T$)
  $f_{out} \leftarrow$ genRandomFrag()
  busy $\leftarrow$ true
  $(answer, f_{in}) \leftarrow$ send-pair-request(z_k, f_{out})
  if *answer* == pair-deny **then**
    $Z_T \leftarrow Z_T \cup \{z_k\}$
  else if *answer* == pair-accept **then**
    paired $\leftarrow$ true
    $p \leftarrow p + f_{in} - f_{out}$
    $D \leftarrow D \cup \{z_k\}$ ▷ Add z_k to SMART-ER dependencies
  end if
  busy $\leftarrow$ false
until *paired* **or** $Z_T = Z$

einer Partnerschaft „gezwungen“ werden kann. Um dies zu verhindern selektiert die Annahmeroutine aus den eintreffenden *pair-request* Nachrichten eine zufällige. Der Absender wird der erste Partner. Aus den danach eintreffenden werden weitere zufällig selektiert bis die maximale Gruppengröße erreicht ist oder die Annahmeroutine aufgrund des Endes der Suchdauer beendet wird. Außerdem wird durch das Führen einer Liste bereits abgelehnter intelligenter Stromzähler (Z_B) verhindert, dass vom selben intelligenten Stromzähler mehrere *pair-request* Nachrichten berücksichtigt werden. Der Ablauf ist wie folgt:

Zu Beginn des Messintervalls wird die Liste Z_B mit der leeren Liste initialisiert. Zur zufälligen Selektion wird die ganzen Zahl m aus der Menge $\{1, \ldots, m_{max}\}$ gezogen. Mittels m wird entschieden, nach wievielen Anfragen von unterschiedlichen intelligenten Stromzählern eine Anfrage akzeptiert wird. Gleichermaßen wird mit der ganzen Zahl a verfahren, die jeweils bestimmt nach wievielen Anfragen der nächste intelligente Stromzähler angenommen wird. Sie wird, nach der Annahme eines weiteren intelligenten Stromzählers, aus der Menge $\{1, \ldots, a_{max}\}$ gezogen.

Die Mengen, aus denen m und a gezogen werden, enthalten *nicht* die 0. Durch den Ausschluss der 0 wird die erste eintreffende Anfrage immer abgelehnt. Diese Entwurfsentscheidung wurde getroffen um die Komplexität einer gezielten Paa-

rung zu erhöhen. Wäre es möglich, dass die erste Anfrage angenommen wird, so hätte der erste anfragende intelligente Stromzähler einen Vorteil: seine Anfrage würde mit Wahrscheinlichkeit $P(m = 0) = \frac{1}{m_{max}+1}$, respektive $P(a = 0) = \frac{1}{a_{max}+1}$, angenommen werden. Und zwar unabhängig davon, wie sich alle anderen intelligenten Stromzähler des Smart Meterings verhalten. Ein angreifender intelligenter Stromzähler könnte sich durch besonders schnelles Anfragen diese Wahrscheinlichkeit sichern. Durch Ausschluss der 0 ist es kein Vorteil mehr die erste Anfrage senden zu können. Um überhaupt in einer Gruppe mit dem angefragten intelligenten Stromzähler sein zu können, muss ein intelligenter Stromzähler seine Anfrage frühestens als zweiter und spätestens an Stelle l mit

$$\begin{aligned} l &= m_{max} + 1 + (g_{max} - 2) \cdot (a_{max} + 1) \\ &= m_{max} + g_{max} \cdot a_{max} + g_{max} - 2a_{max} - 1 \end{aligned}$$

an das Ziel senden. Ist beispielsweise $g_{max} = 4$, $m_{max} = 10$ und $a_{max} = 5$, so können nur die zweite bis $l = 23$-te Anfrage überhaupt in Frage kommen. Diesen Bereich zu treffen wird dadurch erschwert, dass andere intelligente Stromzähler des Smart Meterings zu zufälligen Zeitpunkten ebenfalls Anfragen an das Ziel senden. Zusätzlich ist dies lediglich der maximale Bereich. Da m und jeweils a zufällig gewählt werden, kann der Bereich auch wesentlich kleiner sein. Mit beispielsweise $m = 1$ und jeweils $a = 1$ wäre der zu treffende Bereich im obigen Beispiel lediglich bis zur sechsten Anfrage.

Das Vorgehen der Annahmeroutine wird im Folgenden beschrieben. Die verwendete Variable w wird zu Beginn der Annahmeroutine mit m initialisiert, das zufällig gezogen wird. Wenn nun eine *pair-request* Nachricht von einem intelligenten Stromzähler z_k bei z eintrifft gibt es folgende Möglichkeiten:

- Falls $z_k \in Z_B$ wird mit *pair-deny* geantwortet.
- Falls z bereits Mitglied einer Gruppe mit g_{max} Mitgliedern ist, so wird mit *pair-deny* geantwortet.
- Wartet die Suchroutine gerade auf eine Antwort, so kann keine Anfrage akzeptiert werden. Die Suchroutine könnte (bei der später eintreffenden Antwort) erfolgreich sein und dadurch könnte ein inkonsistenter Zustand entstehen. Daher wird auf eintreffende Anfragen mit *busy-deny* geantwortet.

- Falls $z_k \notin Z_B$ und $w > 0$ wird mit *pair-deny* geantwortet. Der anfragende intelligente Stromzähler ist zu früh und wird daher abgelehnt. Zusätzlich wird er zu Z_B hinzugefügt, da sein einziger Versuch verbraucht ist. Außerdem wird w um eins dekrementiert.

- Falls $z_k \notin Z_B$ und $w = 0$ wird mit *pair-accept* geantwortet. Der intelligente Stromzähler z_k wurde in der Gruppe aufgenommen. An die *pair-accept* Nachricht wird ein zufälliges SMART-ER Fragment angehängt. Falls die Gruppengröße noch nicht g_{max} erreicht hat, wird w auf ein zufällig gezogenes a gesetzt und die Annahmeroutine wiederholt. Ist eine Gruppengröße von g_{max} erreicht, so werden (bereits beim zweiten Aufzählungspunkt) alle eintreffenden Anfragen mit *pair-deny* beantwortet.

Der Ablauf der Annahmeroutine ist in Algorithmus 5 dargestellt. Die Annahmeroutine gewährleistet, dass ein intelligenter Stromzähler aus den anfragenden intelligenten Stromzählern zufällig Kandidaten auswählt. Zusätzlich wird sichergestellt, dass jeder intelligente Stromzähler maximal eine Anfrage an jeden anderen intelligenten Stromzähler senden kann. Sollte ein intelligenter Stromzähler dennoch mehrere Anfragen an denselben anderen intelligenten Stromzähler senden, so werden diese ignoriert.

6.2.3 Gesamtverfahren

Der Ablauf des Gesamtverfahrens kann nun mittels der beschriebenen Routinen geschildert werden (siehe Algorithmus 6). Vor jedem Messintervall setzt ein intelligenter Stromzähler seine Variablen auf den Initialzustand zurück: eine leere Abhängigkeitsliste D, einen mit 0 initialisierten Messwert p und die beiden Variablen paired und busy auf jeweils false. Zum Startzeitpunkt werden die Such- und Annahmeroutine parallel gestartet. Wenn der Abgabezeitpunkt eintritt, muss lediglich geprüft werden, ob eine der Routinen erfolgreich war. Ist dies der Fall, wird der Messwert mit den Maskierungsdaten maskiert und an den Messdienstleister geschickt. Andernfalls wird eine Fehlernachricht an den Messdienstleister geschickt, um zu signalisieren, dass der intelligente Stromzähler zwar verfügbar war, aber kein privatsphärengerechtes Smart Metering durchführen konnte. Dies ist nötig um eine Störungserkennung, die beispielsweise Stromausfälle erkennt, nicht unnötig auszulösen.

Algorithmus 5 Speeddating Annahmeroutine (getFoundRoutine).

$Z_B \leftarrow \emptyset$
$g \leftarrow 1$
$w \leftarrow \text{rand}(\{1, \ldots, m_{max}\})$
loop
  $(z_k, f_{in}) \leftarrow$ receiveRequest() ▷ Incoming request from node z_k
  if $z_k \in Z_B$ **or** $g = g_{max}$ **then**
    reply(z_k, pair-deny)
  else if *busy* **then**
    reply(z_k, busy-deny)
  else if $w > 0$ **then** ▷ Deny request (too early)
    $w \leftarrow w - 1$
    $Z_B \leftarrow Z_B \cup \{z_k\}$ ▷ Add z_k to blocklist
    reply(z_k, pair-deny)
  else if $w == 0$ **then** ▷ Accept request
    $f_{out} \leftarrow$ genRandomFrag()
    reply(z_k, pair-accept, f_{out})
    $p \leftarrow p + f_{in} - f_{out}$
    $D \leftarrow D \cup \{z_k\}$ ▷ Add z_k to SMART-ER dependencies
    paired $\leftarrow$ true
    $g \leftarrow g + 1$
    if $g < g_{max}$ **then**
      $w \leftarrow \text{rand}(\{1, \ldots, a_{max}\})$ ▷ Restart for more members
    end if
  end if
end loop

Algorithmus 6 Smart Meter Speeddating.

```
Z ← Set of Smart Meters
loop
    D ← ∅, p ← 0, paired ← false, busy ← false
    repeat
        sleep 1                                          ▷ Wait for start
    until currentTime() == submitTime() − s
    run searchRoutine
    run getFoundRoutine
    repeat
        sleep 1                                  ▷ Wait while running routines
    until currentTime() == submitTime()
    stop searchRoutine
    stop getFoundRoutine
    if paired then
        p ← p + measurePower()
        submitToSink(p, D)
    else
        submitToSink(not_paired)
    end if
end loop
```

6.3 Parameterstudie

Das SMSD-Verfahren lässt sich mit einer Vielzahl an Protokollparametern (g_{max}, m_{max}, a_{max}, s und t_{max}) konfigurieren. Deshalb wird hier eine Parameterstudie durchgeführt. Sie identifiziert einzelne Parameterkonfigurationen für Smart Meter Speeddating die im Folgenden dann näher analysiert werden. Die Parameterstudie bewertet Parameterkonfigurationen anhand ihrer Smart Metering Leistung. Wie zu Beginn des Kapitels motiviert, ist eines der Ziele das Bilden möglichst kleiner Gruppen zur Erhöhung der Smart Metering Leistung. Es ist daher naheliegend, den Parameter zur maximalen Gruppengröße (g_{max}) auf den (wie zu Beginn des Kapitels erläutert) kleinsten Wert von 3 zu setzen. Entsprechend den Untersuchungen in Abschnitt 5.5.4 ist hier die höchste Smart Metering Leistung zu erwarten. Dies wurde auch in Voruntersuchungen bestätigt. Die Ergebnisse der Voruntersuchungen sind im Anhang in Abschnitt B.1 dargestellt. Im Folgenden werden

daher ausschließlich Parameterkonfigurationen mit $g_{max} = 3$, also Zweier- und Dreiergruppen, untersucht.

Für die Parameterstudie wurde zunächst der Zusammenhang zwischen m_{max} und a_{max} näher betrachtet (Abschnitt 6.3.1). Es wurde festgestellt, dass sich Kombinationen mit a_{max} deutlich kleiner als m_{max} nachteilig auf die Smart Metering Leistung auswirken. Anschließend wurde untersucht, wie sich unterschiedliche Werte für a_{max} bei festem m_{max} auf die Smart Metering Leistung auswirken (Abschnitt 6.3.2). Als günstige Parameterkonfigurationen stellten sich Varianten mit a_{max} etwas kleiner als m_{max} heraus. In Abschnitt 6.3.3 wird der Einfluss der maximalen Wartezeit t_{max} und in Abschnitt 6.3.4 der Einfluss der Suchdauer untersucht. Mittels dieser Erkenntnisse werden dann in Abschnitt 6.3.5 die für die Evaluation ermittelten Parameterkonfigurationen zusammengefasst.

6.3.1 m_{max} in Kombination mit a_{max}

Intuitiv kann der Parameter m_{max} als Schwierigkeitsstufe für die Aufnahme in eine Zweierpaarung gesehen werden. Je höher m_{max} dabei ist, desto größer ist der Auswahlbereich, aus dem die intelligenten Stromzähler einen potentiellen Partner wählen. Analog kann a_{max} als Schwierigkeitsstufe für die Aufnahme in eine bereits bestehende Paarung gesehen werden. Betrachtet man jeden Parameter einzeln, so liegt die Annahme nahe, dass mit a_{max}, unabhängig von m_{max}, die Bildung von Dreiergruppen beeinflusst werden kann.

Ein hohes m_{max} lässt den intelligenten Stromzählern einen großen Spielraum zur Auswahl eines Partners. Da im Durchschnitt, bedingt durch das gleichverteilte ziehen von m aus $\{1, \ldots, m_{max}\}$, eine höhere Anzahl an Anfragen abgelehnt wird bevor eine Anfrage angenommen wird, erhöht sich die benötigte Suchdauer. Dies kann letztlich dazu führen, dass eine größere Anzahl an intelligenten Stromzählern keinen Partner finden kann und keinen Abgabewert übermittelt. Ein niedriges a_{max} begünstigt die Dreiergruppenbildung. Intuitiv könnte die Smart Metering Leistung eines hohen m_{max} durch ein niedriges a_{max} verbessert werden. Die Suchdauer könnte kürzer ausfallen, da intelligente Stromzähler schneller Anschluss an eine bestehende Zweiergruppe finden.

Dies ist jedoch im Allgemeinen *nicht* der Fall. Wie in diesem Abschnitt gezeigt wird, sind nicht alle Kombinationen von m_{max} und a_{max} tauglich. Im Speziellen sind sehr kleine a_{max} bei großen m_{max} sogar von Nachteil.

Zur Untersuchung wurden Kombinationen von m_{max} und a_{max} simuliert. Die betrachteten Parameterkonfigurationen sind in Tabelle 6.2 zusammengefasst. Die

Tabelle 6.2: *Parameterkonfigurationen für Simulationen zu m_{max} in Kombination mit a_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	10 Minuten
t_{max}	1 Sekunde
m_{max}	$\{3, 5, 10, 15, \ldots, 35\}$
a_{max}	$\{3, 5, 10, 15, \ldots, 35\}$

Suchdauer wurde sehr lang parametrisiert um den intelligenten Stromzählern genug Zeit für Anfragen an andere intelligente Stromzähler einzuräumen. Die Suchdauer stellt in dieser Untersuchung also keinen limitierenden Faktor dar[2]. Das arithmetische Mittel sowie 98%-Konfidenzintervalle der Ergebnisse sind in Abbildung 6.4 aufgezeichnet. Entlang der x-Achse ist die Konfiguration für m_{max} aufgetragen. Auf der y-Achse der Anteil valider Abgabewerte aufgezeichnet. Die Konfigurationen für den Parameter a_{max} sind als einzelne Kurven dargestellt. Die betrachteten Werte für $a_{max} > 20$ zeigen bei dieser Skalierung keine sichtbare Abweichung von der 100% Marke und sind der Übersichtlichkeit wegen nicht eingezeichnet.

In der Abbildung ist zu erkennen, dass Kombinationen von großem m_{max} und kleinem a_{max} problematisch sind. Am Beispiel von $a_{max} = 3$ (Symbol: Dreieck), ist zu beobachten, dass für kleine m_{max} der Anteil valider Abgabewerte nicht negativ beeinflusst wird und praktisch bei 100% liegt. Wird nun m_{max} erhöht, also die Paarbildung erschwert, so sinkt der Anteil der validen Abgabewerte ab $m_{max} = 10$ stetig. Die erleichterte Dreiergruppenbildung sorgt hier also für ein *schlechteres Gesamtergebnis*. Betrachtet man die anderen Werte für a_{max} so zeigt sich ein Muster. Für $a_{max} = 5$ verschlechtern sich die Gesamtergebnisse ab $m_{max} = 15$. Für $a_{max} = 10$ ist dies ab $m_{max} = 25$ der Fall. Generell kann geschlossen werden, dass für a_{max} kleiner als m_{max} eine Beeinträchtigung des Gesamtergebnisses auftreten kann.

[2]Dies wird durch Ergebnisse der Untersuchung des Einflusses der Suchdauer (Abschnitt 6.3.4) bestätigt.

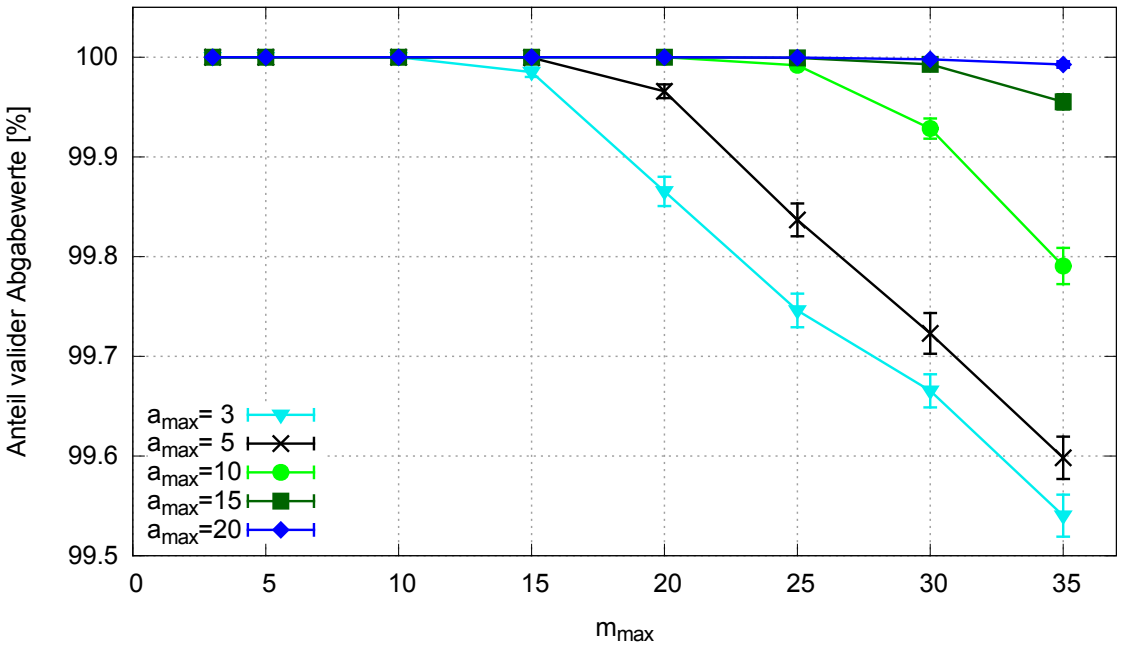


Abbildung 6.4: *Parameterstudie m_{max} und a_{max}.*

Für $a_{max} \geq m_{max}$ ist für die betrachteten Konfigurationen keine Beeinträchtigung beobachtbar.

Um diesen Zusammenhang zu erläutern, ist eine nähere Betrachtung von großen m_{max} notwendig. Mit einem hohen m_{max} steht einem intelligenten Stromzähler ein großer Bereich zur Wahl der anzunehmenden Anfrage zur Verfügung. Da m gleichverteilt aus $\{0, \ldots, m_{max}\}$ gezogen wird, herrscht zwischen den einzelnen intelligenten Stromzählern eine größere Varianz von m, als dies bei kleinem m_{max} der Fall wäre. Während einige intelligente Stromzähler einen sehr kleinen Wert für m ziehen, haben andere einen sehr großen Wert für m. Beispielhaft sei ein intelligenter Stromzähler z_1 mit $m = 3$ und ein anderer Stromzähler z_2 mit $m = 23$ angenommen. z_1 kann frühzeitig, also schon nach 3 Anfragen, einen Partner annehmen und die Annahme eines dritten Stromzählers in Angriff nehmen. Bereits durch die erste Annahme wird die Zahl der potentiell bei z_2 anfragenden Knoten um eins verringert. Ist nun a_{max} relativ zu m_{max} klein, so wird z_1 mit hoher Wahrscheinlichkeit noch eine zweite Anfrage annehmen, bevor z_2 überhaupt eine erste annehmen konnte. Damit wird die Zahl der potentiell bei z_2 anfragenden

Stromzähler weiter reduziert. Dieses Ungleichgewicht kann letztlich für z_2 zur Folge haben, dass er keinen Partner findet.

Mit Hilfe dieser Betrachtung kann eine grobe Regel formuliert werden: Sinkt der Erwartungswert $E(m+a)$ unter m_{max}, so steigt die Wahrscheinlichkeit für ein Auftreten eines Ungleichgewichts schnell an. Ist $E(m+a)$ nur geringfügig kleiner als m_{max}, so ist die Wahrscheinlichkeit für das Auftreten des Ungleichgewichts so gering, dass andere Effekte diese kompensieren. Die Suchroutinen der intelligenten Stromzähler mit hohem m (z_2 im obigen Beispiel) könnten beispielsweise zum Erfolg führen. Das Gesamtergebnis wird dann nicht oder nur unwesentlich beeinträchtigt. Ist $E(m+a)$ deutlich kleiner als m_{max} ist auch die Wahrscheinlichkeit für das Auftreten eines Ungleichgewichts groß. Hierdurch wird das Gesamtergebnis negativ beeinflusst.

Für eine Parameterkonfiguration von SMSD ist also eine Wahl von $a_{max} \geq m_{max}$ problemlos. Ist a_{max} geringfügig kleiner als m_{max} muss in Einzelfällen mit Beeinträchtigungen gerechnet werden. Von Parameterkonfigurationen mit a_{max} deutlich kleiner als m_{max} ist generell abzuraten.

6.3.2 Einfluss von a_{max} bei festem m_{max}

Um den Einfluss von a_{max} auf das Gesamtergebnis und die Dreiergruppenbildung abschätzen zu können, wurde dieser exemplarisch für $m_{max} = 20$ untersucht. Weitere Simulationen zeigten, dass die Aussagen von $m_{max} = 20$ auch qualitativ für andere m_{max} zutreffen. Die Ergebnisse dieser weiteren Simulationen sind in Anhang B.2 dargestellt. Da ein hohes a_{max} die Dreiergruppenbildung behindert, ist davon auszugehen, dass auch eine längere Suchdauer benötigt wird. Um diesen Zusammenhang zu untersuchen wurden die im Folgenden behandelten Simulationen mit variierender Suchdauer durchgeführt. Die Ergebnisse können dadurch wie ein zeitlicher Verlauf eines durchschnittlichen Messintervalls interpretiert werden. Die Parameterkonfigurationen der Untersuchung sind in Tabelle 6.3 zusammengefasst. Für jede Parameterkonfiguration wurde das arithmetische Mittel sowie das 98%-Konfidenzintervall berechnet. Mit $a_{max} = 5$ und $a_{max} = 10$ wurden exemplarisch auch Parameterkonfigurationen untersucht, die entsprechend der Regel aus dem vorherigen Abschnitt problematisch sind. Zur besseren Übersichtlichkeit ist in einigen der folgenden Abbildungen nur $a_{max} = 5$ eingezeichnet. Die jeweiligen Abbildungen mit $a_{max} = 10$ sind in Anhang B.2 aufgeführt.

Die Simulationsergebnisse sind in Abbildung 6.5 dargestellt. Der Anteil valider Abgabewerte (y-Achse) ist in Abhängigkeit von der Suchdauer (x-Achse)

Tabelle 6.3: *Parameterkonfigurationen für Simulationen zum Einfluss von a_{max} bei festem m_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{5, 10, 20, 30, \ldots, 60, 80, 100, \ldots, 300\}$
t_{max}	1 Sekunde
m_{max}	20
a_{max}	$\{5, 10, 15, 20, 30\}$

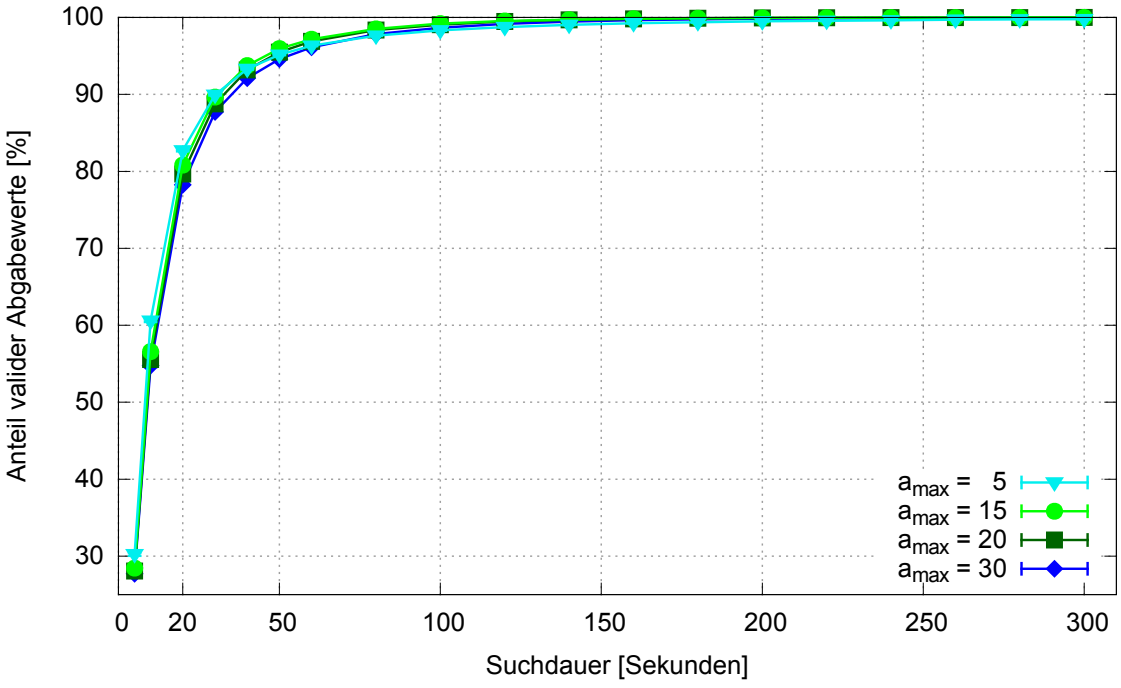
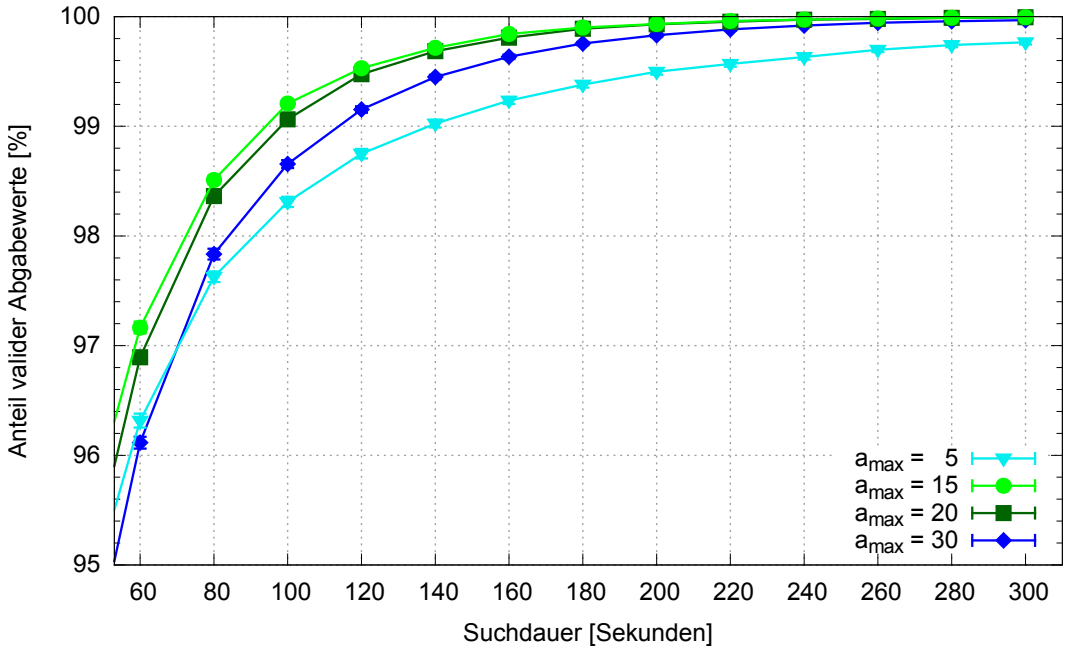


Abbildung 6.5: *Anteil valider Abgabewerte bei $m_{max} = 20$ und variierendem a_{max}.*

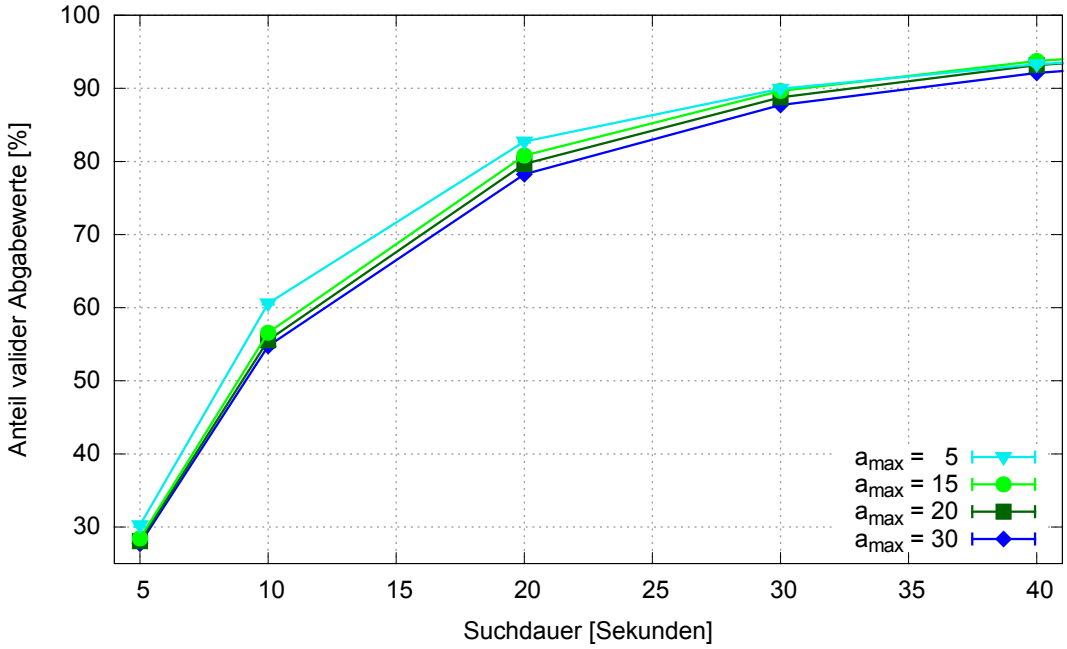
aufgezeichnet. Jede Konfiguration von a_{max} ist als Kurve aufgetragen. Durch die Variation der Suchdauer können die eingezeichneten Kurven als zeitlicher Verlauf interpretiert werden. So kann abgelesen werden, dass nach 20 Sekunden bei allen Konfigurationen von a_{max} ungefähr 80% der intelligenten Stromzähler eine Gruppe finden konnten. Nach 50 Sekunden ist dieser Anteil bereits auf ungefähr 95% angestiegen. Generell ist ersichtlich, dass zu Beginn der Suchdauer ein sehr schneller Anstieg der validen Abgabewerte und damit auch der erfolgreich gebildeten Gruppen erfolgt. Bereits nach 5 Sekunden sind circa 30% der intelligenten Stromzähler in einer Gruppe. Nach 20 Sekunden sind dies bereits circa 80%. Im weiteren Verlauf der Suchdauer geht die Rate der Gruppenbildung und -findung dann deutlich zurück und der Anteil valider Abgabewerte nähert sich langsam der 100% Marke an. Bei der dargestellten Skalierung sind zwischen den einzelnen Konfigurationen für a_{max} nur schwer Unterschiede erkennbar. Daher wird im Folgenden eine Detailbetrachtung dieser Abbildung durchgeführt.

In Abbildung 6.6a sind die Ergebnisse für die Suchdauern von 60 bis 300 Sekunden aufgezeichnet. Durch die Konzentration auf diesen Abschnitt der Suchdauer ist eine wesentlich detailliertere Darstellung möglich. Vergleicht man verschiedene Konfigurationen für a_{max} miteinander, so zeigt sich, dass bei gleichbleibender Suchdauer ein kleineres a_{max} einen höheren Anteil an validen Abgabewerten erreicht. Beispielsweise erreicht $a_{max} = 15$ (Symbol: Kreis) nach 100 Sekunden Suchdauer bereits $99,2\%$ während $a_{max} = 30$ (Symbol: Raute) nach 100 Sekunden lediglich $98,6\%$ erreicht. Erst nach 120 Sekunden kann $a_{max} = 30$ mit $99,1\%$ annähernd ein vergleichbares Ergebnis wie $a_{max} = 15$ nach 100 Sekunden erzielen. Es kann also geschlossen werden, dass eine Verringerung von a_{max} bei gleichbleibender Suchdauer ein besseres Ergebnis erzielt. Analog kann auch geschlossen werden, dass eine Erhöhung von a_{max} eine Verlängerung der Suchdauer erfordert um das gleiche Ergebnis zu erzielen. Hervorzuheben ist, dass die Parameterkonfiguration mit $a_{max} = 15$ (Symbol: Kreis) konsistent für alle simulierten Suchdauern bessere Ergebnisse liefert, als die Parameterkonfiguration mit $a_{max} = m_{max} = 20$. Besonders für kurze Suchdauern stellt diese Parameterkonfiguration damit die bessere Wahl dar.

Die Schlussfolgerung, dass kleine a_{max} von Vorteil sind, gilt allerdings nur, wenn die im vorherigen Abschnitt formulierte Regel erfüllt ist. Dies ist an der exemplarisch ausgewählten, ungünstigen Parameterkonfiguration $a_{max} = 5$ (Symbol: Dreieck) gut zu erkennen. Ihr Ergebnis fällt ab einer Suchdauer von 80 Sekunden durchgängig schlechter aus, als das der Parameterkonfiguration, die der Regel entsprechen. Betrachtet man jedoch die Ergebnisse für eine Suchdauer von



(a) *Detailbetrachtung von* 40 *bis* 300 *Sekunden.*



(b) *Detailbetrachtung von* 5 *bis* 40 *Sekunden.*

Abbildung 6.6: *Detailbetrachtungen der Anteile valider Abgabewerte bei* $m_{max} = 20$ *und variierendem* a_{max}.

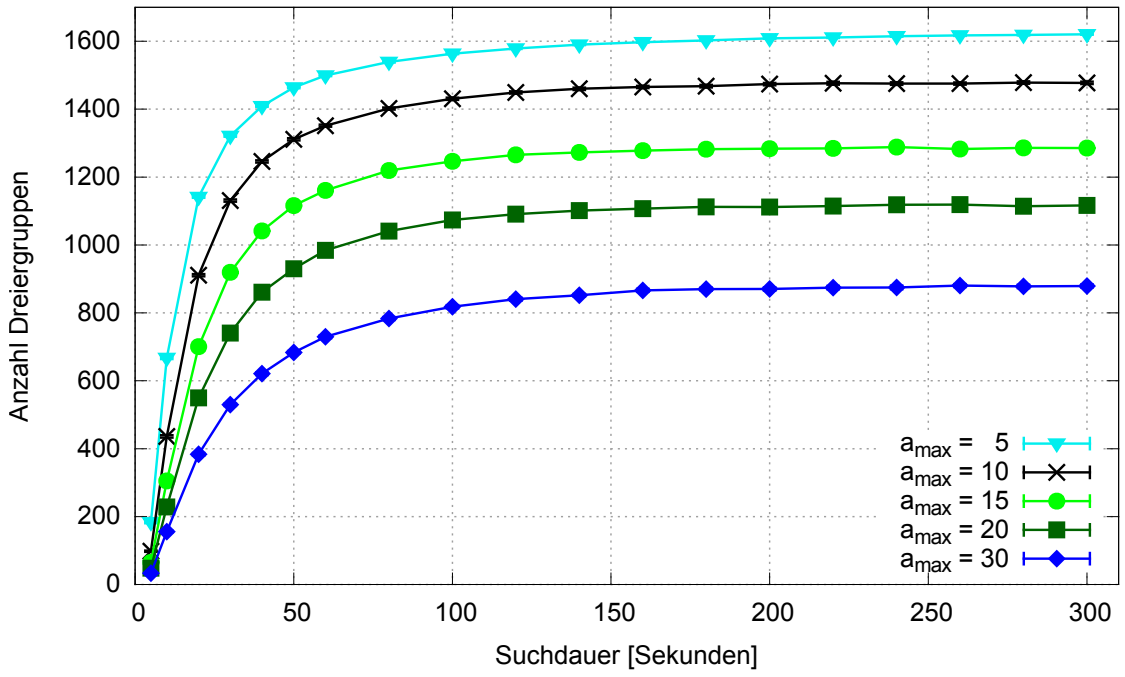


Abbildung 6.7: *Anzahl Dreiergruppen bei* $m_{max} = 20$ *und variierendem* a_{max}.

60 Sekunden, so erzielt $a_{max} = 5$ einen höheren Anteil valider Abgabewerte als $a_{max} = 30$. Es liegt der Schluss nahe, dass das zu niedrige a_{max} eine beschleunigte Partnerfindung zu Beginn der Suchdauer verursacht, die sich dann im späteren Verlauf negativ auswirkt. Die negativen Auswirkungen im Verlauf der Suchdauer sind gut zu erkennen. Selbst nach 300 Sekunden erreicht $a_{max} = 5$ nur ein Anteil von $99,8\%$.

Zur Untersuchung der beschleunigten Partnerfindung ist eine Detailbetrachtung der ersten 60 Sekunden der Suchdauer in Abbildung 6.6b aufgezeichnet. Im Vergleich zu Abbildung 6.6a wird hier ein deutlich kürzerer Zeitraum abgebildet. Die, entsprechend der formulierten Regel, ungünstige Parameterkonfiguration $a_{max} = 5$ führt zunächst zu einem schnelleren Anstieg des Anteils der validen Abgabewerte, als die Parametrisierungen die mit der Regel konform sind. Dieser initiale Vorteil wird jedoch im zeitlichen Verlauf geringer und führt schließlich zu einem durchgehend schlechteren Ergebnis. Für $a_{max} = 10$ tritt das gleiche Verhalten, allerdings weniger ausgeprägt, ein. Die entsprechenden Abbildungen sind Abbildung B.9 und Abbildung B.10 in Anhang B.2. Diese Ergebnisse bestätigen die Regel aus dem vorherigen Abschnitt.

Dass der Parameter a_{max} die Anzahl an entstehenden Dreiergruppen beeinflusst ist in Abbildung 6.7 zu erkennen. Auf der x-Achse ist hier wieder die Suchdauer in Sekunden aufgetragen, während auf der y-Achse diesmal das arithmetische Mittel der Anzahl der gebildeten Dreiergruppen samt 98%-Konfidenzintervalle aufgezeichnet wird. Durch die Skalierung und die geringe Größe der Konfidenzintervalle sind diese in der Abbildung nicht zu erkennen. Die verschiedenen Werte für a_{max} sind als einzelne Kurven dargestellt. Sie zeigen deutlich den Einfluss von a_{max} auf die Anzahl Dreiergruppen. Erwartungsgemäß sorgt ein niedriger Wert für a_{max} für eine hohe Zahl an Dreiergruppen. Beispielsweise werden für $a_{max} = 5$ circa 1 600 Dreiergruppen gebildet. Damit sind 96% der teilnehmenden intelligenten Stromzähler in Dreiergruppen organisiert. Bei $a_{max} = 30$ sind dies mit circa 900 Dreiergruppen nur 54% der teilnehmenden Stromzähler. Betrachtet man den zeitlichen Verlauf, so ist zu erkennen, dass die Bildung der Dreiergruppen schnell abflacht und dass sich bereits nach durchschnittlich 100 Sekunden die Anzahl der Dreiergruppen nur noch geringfügig verändert.

Der Parameter a_{max} stellt also eine gute Möglichkeit zur Beeinflussung der Anzahl an Dreiergruppen dar. Wird er geringfügig kleiner als m_{max} gewählt, so sorgt er für eine schnelle Gruppenbildung. Wird er höher gewählt, so sorgt er für eine geringere Anzahl an Dreiergruppen, benötigt aber auch eine längere Suchdauer.

6.3.3 Einfluss von t_{max}

Der Parameter t_{max}, die maximale Wartezeit zwischen zwei Anfragen der Suchroutine, beeinflusst die benötigte Suchdauer. Da ein intelligenter Stromzähler seine Wartezeit vor jeder Anfrage zufällig aus dem Intervall $[0, t_{max}]$ zieht, ist seine durchschnittliche Wartezeit $\frac{t_{max}}{2}$. Durch die Beschränkung der Suchdauer kann die Anzahl der durchschnittlich versendeten Anfragen für den Fall, dass ein intelligenter Stromzähler keinen Partner findet, abgeschätzt werden. Diese ist $\frac{2s}{t_{max}}$ und wird nur dann erreicht, wenn sowohl die Suchroutine als auch die Annahmeroutine bis zum Ende der Suchdauer erfolglos war.

Um die Wahrscheinlichkeit einer erfolgreichen Suchroutine zu erhöhen, ist eine möglichst hohe Anzahl an Anfragen und damit eine möglichst kurze Wartezeit erforderlich. Eine zu kurze Wartezeit zwischen zwei Anfragen kann aber die Annahmeroutine negativ beeinflussen. Wäre die Wartezeit 0, so würden alle intelligenten Stromzähler konstant Anfragen senden und damit die Annahmeroutine blockieren. Um den optimalen Wert für t_{max} zu finden wurde dieser näher untersucht.

Tabelle 6.4: *Parameterkonfigurationen für Simulationen zum Einfluss von t_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{120, 160, 200, 240\}$
t_{max}	$\{100, 200, \ldots, 2\,000\}$ Millisekunden
m_{max}	20
a_{max}	15

Die Parameterkonfigurationen der Untersuchung sind in Tabelle 6.4 aufgelistet. Es wurde die maximale Wartezeit variiert. Als Konfiguration für m_{max} und a_{max} wurde exemplarisch die bereits im vorigen Abschnitt verwendete Kombination $m_{max} = 20, a_{max} = 15$ verwendet. Weitere Simulationen zeigten, dass die Aussagen qualitativ auch für andere Kombinationen zutreffen. Die Ergebnisse dieser weiteren Simulationen sind in Anhang B.3 dargestellt. Basierend auf den Ergebnissen aus Abbildung 6.6a wurden für die Suchdauer die vier aufgelisteten Werte ausgewählt. Mit 120 Sekunden als ersten Wert wurde für diese Parameterkonfiguration eine so kurze Suchdauer gewählt, dass nicht alle intelligenten Stromzähler einen Partner finden. Die steigenden Suchdauern nähern sich dann der benötigten Suchdauer für diese Parameterkonfiguration an.

In Abbildung 6.8 ist der Anteil valider Abgabewerte (y-Achse) in Abhängigkeit von der maximalen Wartezeit t_{max} (x-Achse) aufgetragen. Es ist das arithmetische Mittel und 98%-Konfidenzintervalle zu sehen. Jede Suchdauer ist als eigene Kurve eingezeichnet. Es ist zu erkennen, wie ein kleines t_{max} durch Beeinträchtigung der Annahmeroutine zu schlechteren Ergebnissen führt. Dies ist unabhängig von der Suchdauer zu beobachten. Ebenso gilt dies für eine zu lange Wartezeit. Ab einem gewissen Wert für t_{max} sinkt für jede Suchdauer der Anteil valider Abgabewerte mit steigendem t_{max}.

Besonders deutlich lässt sich die Auswirkung von t_{max} bei einer sehr kurzen Suchdauer beobachten. Die Parameterkonfiguration mit $s = 120$ (Symbol: Dreieck) zeigt deutlich die Wichtigkeit der Balance zwischen Suchroutine und Annahmeroutine. Ist t_{max} zu klein, funktioniert die Annahmeroutine nur eingeschränkt.

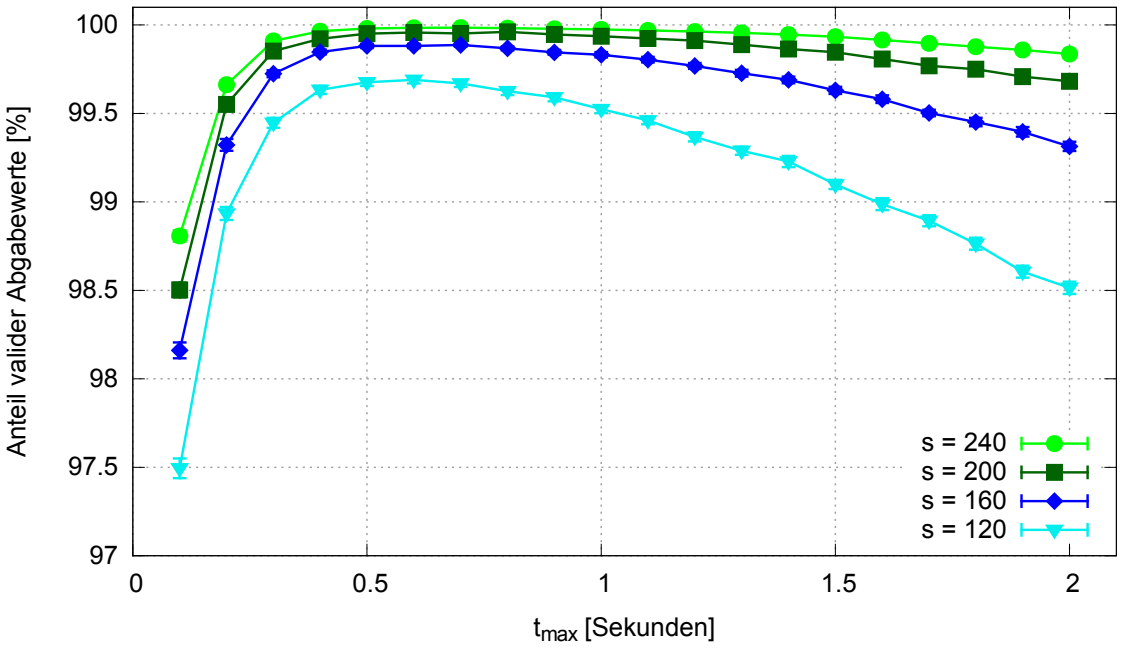


Abbildung 6.8: *Anteil valider Abgabewerte in Abhängigkeit von* t_{max}.

Ist t_{max} zu groß, kann die Suchroutine nicht genügend Anfragen versenden. Der optimale Wert für t_{max} ist bei (zu) kurzer Suchdauer bei 600 Millisekunden.

Wird die Suchdauer ausreichend lange gewählt (hier $s = 240$), so sind für t_{max} mehrere Werte optimal. Ab 600 Millisekunden erreichen die validen Abgabewerte ihr Maximum und sinken erst ab circa 1,2 Sekunden wieder ab.

Aufgrund dieser Ergebnisse wird im Folgenden t_{max} mit 600 Millisekunden konfiguriert.

6.3.4 Einfluss der Suchdauer

Wie bereits in den vorhergehenden Untersuchungen ersichtlich war, existiert für eine bestimmte Parameterkonfiguration von m_{max}, a_{max} und t_{max} eine benötigte Suchdauer s. Diese wird in diesem Abschnitt für eine Anzahl an Parameterkonfigurationen ermittelt. Die betrachteten Parameterkonfigurationen sind in Tabelle 6.5 zusammengefasst. Es wurde die in Abschnitt 6.3.3 ermittelte maximale Wartezeit und eine variierende Suchdauer verwendet. Die verwendeten *Kombinationen* von a_{max} und m_{max} resultieren aus der Untersuchung in Abschnitt 6.3.1.

Tabelle 6.5: *Parameterkonfigurationen für Simulationen zum Einfluss der Suchdauer.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{60, 80, 100, \ldots, 400\}$
t_{max}	600 Millisekunden
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$ in Kombination
a_{max}	$\overbrace{\{3,\ 5,\ 10,\ 15, 20\}}$

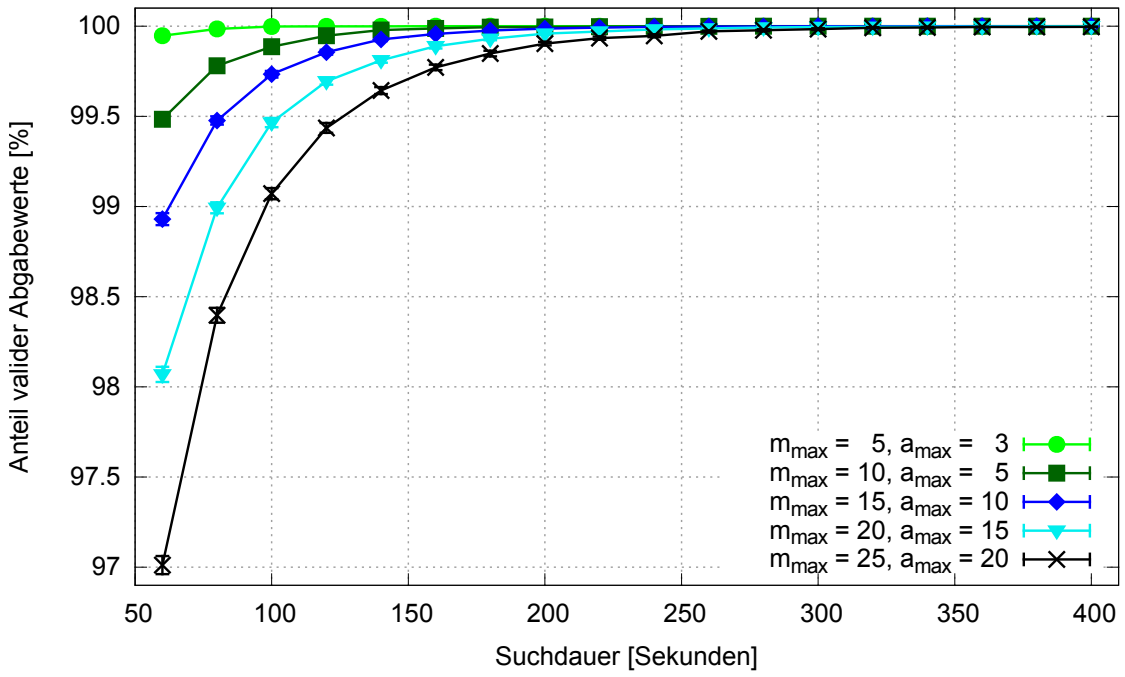


Abbildung 6.9: *Anteil valider Abgabewerte in Abhängigkeit von der Suchdauer s.*

Tabelle 6.6: *Benötigte Suchdauern für SMSD Parameterkonfigurationen.*

m_{max}	a_{max}	Suchdauer [Sekunden]
5	3	100
10	5	180
15	10	220
20	15	280
25	20	320

In Abbildung 6.9 ist der Anteil valider Abgabewerte (y-Achse) in Abhängigkeit von der Suchdauer s (x-Achse) aufgetragen. Jede Parameterkonfiguration von m_{max} und a_{max} ist als eigene Kurve aufgetragen und zeigt arithmetisches Mittel und 98%-Konfidenzintervalle. Zu erkennen ist, wie höhere Werte für m_{max} auch längere Suchdauern benötigen. Die benötigte Suchdauer wurde für jede Parameterkonfiguration so bestimmt, dass nach ihrem Ablauf konsistent ein Anteil von $99,99\%$ valider Abgabewerte vorliegt. Sie liegt beispielsweise für $m_{max} = 5$ bei 100 Sekunden und für $m_{max} = 25$ bei 320 Sekunden. Die Ergebnisse für die ausgewählten Parameterkonfigurationen sind in Tabelle 6.6 zusammengefasst. Auf eine Auflistung der maximalen Wartezeit t_{max} wurde verzichtet, da sie für alle Einträge gleich ist. Die benötigte Suchdauer pro Parameterkonfiguration stellt gleichzeitig das kleinste mögliche Messintervall dar. Da alle benötigten Suchdauern deutlich unter dem anvisierten Messintervall von 15 Minuten liegen, können auch alle Parameterkonfigurationen eingesetzt werden. Soll jedoch ein kürzeres Messintervall realisiert werden, muss entweder eine Parameterkonfiguration mit niedrigerer Suchdauer verwendet oder eine reduzierte Leistung aufgrund zu kurzer Suchdauer akzeptiert werden.

6.3.5 Zusammenfassung

Durch die Studie der Parameter konnten in Abschnitt 6.3.1 Parameterkonfigurationen mit a_{max} deutlich kleiner als m_{max} als untauglich identifiziert werden. Eine nähere Betrachtung zeigte in Abschnitt 6.3.2, dass eine Parameterkonfiguration von a_{max}, die nur wenig kleiner als m_{max} ist, einen positiven Effekt auf die benötigte Suchdauer hat. In Abschnitt 6.3.3 konnte eine optimale maximale Wartezeit t_{max} von 600 Millisekunden bestimmt werden. Mittels dieser Erkenntnisse konn-

ten in Abschnitt 6.3.4 für ausgewählte Parameterkonfigurationen die benötigten Suchdauern bestimmt werden. Diese benötigten Suchdauern stellen gleichzeitig das kleinste Smart Metering Intervall der Parameterkonfiguration dar.

Mittels dieser Erkenntnisse können die Parameterkonfigurationen aus Tabelle 6.6 nun in Hinsicht auf Privatsphärenschutz und Smart Metering Leistung untersucht werden. Im Folgenden werden die Parameterkonfigurationen anhand des Wertes für m_{max} referenziert. So ist mit der Parameterkonfiguration $m_{max} = 10$ immer die Parameterkonfiguration $m_{max} = 10, a_{max} = 5, s = 180$ und $t_{max} = 600$ ms gemeint. Andernfalls wird explizit darauf hingewiesen.

6.4 Evaluation des Privatsphärenschutzes

Da Smart Meter Speeddating das in Kapitel 5 beschriebene SMART-ER Verfahren verwendet, gilt dessen Privatsphärenschutz auch für SMSD. Im Speziellen bedeutet dies, dass in SMSD die Privatsphäre eines einzelnen Haushalts gewahrt bleibt, solange mindestens eine beteiligte Partei nicht korrumpiert ist. Für einen intelligenten Stromzähler in SMSD sind diese Parteien ein oder zwei weitere intelligente Stromzähler und der Messdienstleister. Ist der Messdienstleister nicht korrumpiert, so geht von dem oder den anderen intelligenten Stromzählern keine Gefahr für die Privatsphäre aus, selbst wenn diese miteinander kooperieren. Falls der Messdienstleister korrumpiert ist, genügt ein nicht korrumpierter intelligenter Stromzähler in der Gruppe um die Privatsphäre des Einzelnen zu wahren. Eine Gefahr für die Privatsphäre eines einzelnen intelligenten Stromzählers besteht also nur dann, wenn sowohl der Messdienstleister, als auch der oder die anderen intelligenten Stromzähler korrumpiert sind.

Im Folgenden wird daher davon ausgegangen, dass ein Angriff durch den Messdienstleister organisiert wird und dieser über eine Anzahl korrumpierter intelligenter Stromzähler verfügt. Das Ziel seines Angriffs ist die Ermittlung eines Lastprofils des intelligenten Stromzähler z_T, des Angriffsziels.

Dabei werden folgende Angriffskategorien unterschieden, die in den folgenden Abschnitten betrachtet werden:

Passive Angriffe Sowohl der Messdienstleister, als auch die korrumpierten intelligenten Stromzähler verhalten sich protokollkonform.

Angriffe auf die Annahmeroutine Korrumpierte Stromzähler versuchen aktiv vom Angriffsziel als Partner angenommen zu werden.

Angriffe auf die Suchroutine Korrumpierte Stromzähler versuchen aktiv möglichst häufig vom Angriffsziel gewählt zu werden.

Statistische Analyse Der Messdienstleister wertet erhaltene Informationen aus und zieht hierzu möglicherweise Sekundärinformationen hinzu.

Zusätzlich zur Privatsphäre des einzelnen muss in SMSD auch die Privatsphäre der Gruppe betrachtet werden. Durch die geringe Gruppengröße wäre eine mögliche Profilbildung pro Gruppe ebenfalls eine Gefahrenquelle für die Privatsphäre des einzelnen. Aus einem Gruppenprofil kann zwar weniger Information gewonnen werden als aus Einzelprofilen, aber dennoch besteht die Möglichkeit sensible Informationen preis zu geben. Daher werden im folgenden Abschnitt zuerst die durch SMSD resultierenden Gruppenkonfigurationen untersucht. Danach folgt eine Untersuchung der möglichen Angriffe durch den Messdienstleister.

6.4.1 Gruppenbildung in SMSD

Um eine einfache Gruppenprofilbildung zu verhindern, verwendet SMSD zufällige Gruppenbildung und ständig wechselnde Gruppenzusammensetzung. Das bedeutet, dass in jedem Messintervall eine neue, zufällige Gruppenbildung stattfindet. Falls also durch einfache Beobachtung der abgegebenen Werte ein Gruppenprofil einer bestimmten Gruppe erstellt werden soll, kann dies nur über die Messintervalle geschehen, in denen diese Gruppe in exakt derselben Gruppenzusammensetzung auftritt.

Um die Qualität eines auf diesem Wege entstandenen Gruppenprofils abschätzen zu können, wurde eine Simulation von SMSD mit 1 000 intelligenten Stromzählern und $m_{max} = 5$ über einen (simulierten) Zeitraum von einem Monat durchgeführt. In diesem Zeitraum wurden 2 880 Messintervalle durchgeführt. Während der Simulation wurde in einer Matrix M aufgezeichnet, welche intelligenten Stromzähler in einem Messintervall gemeinsam in einer Gruppe waren. Das heißt, dass in einem Messintervall in dem eine Gruppierung $\{z_1, z_2\}$ aufgetreten ist, die Matrix M an der Stelle $M_{1,2}$ und $M_{2,1}$ um eins erhöht wurde. Wenn eine Gruppierung $\{z_1, z_2, z_3\}$ aufgetreten ist, dann wurde sowohl $M_{1,2}$ und $M_{2,1}$ als auch $M_{2,3}$ und $M_{3,2}$, sowie $M_{1,3}$ und $M_{3,1}$ jeweils um eins erhöht.

In Abbildung 6.10 ist M als Heatmap dargestellt. Dabei repräsentiert jeder Bildpunkt ein Paar von intelligenten Stromzählern. Die Farbe des Bildpunkts wird entsprechend der Anzahl an gemeinsamen Messintervallen ausgewählt. Dabei entspricht Schwarz dem beobachteten Maximalwert über alle Paarungen und Weiß

der 0. Hat beispielsweise der intelligente Stromzähler z_1 während des Beobachtungszeitraums nie mit Stromzähler z_2 in einem Messintervall kooperiert, so ist der Bildpunkt an der Koordinate (z_1, z_2) weiß. Entspricht die Anzahl an Kooperationen der Maximalzahl über die Heatmap, so ist der Bildpunkt schwarz. Liegt die Anzahl der Paarungen dazwischen, so ist der Bildpunkt im entsprechenden Grauton gehalten.

Wie deutlich zu erkennen ist, existiert in der Heatmap kein Muster, außer der Diagonalen und die Spiegelung an der Diagonalen. Die Diagonale ist weiß, da die Gruppenmitgliedschaft eines intelligenter Stromzähler mit sich selbst nicht gezählt wurde. Da eine Gruppenmitgliedschaft bijektiv ist, ist die Matrix an der Diagonalen gespiegelt. Der höchste Eintrag in der Matrix M hatte den Wert 16. In der Heatmap existieren also neben Schwarz (16) und Weiß (0) noch weitere 15 Grauwerte. Der Eintrag mit der Höchstzahl 16 trat in der Matrix genau einmal auf. Das bedeutet, dass es genau *ein* Paar von intelligenten Stromzählern gab, das in 16 Messintervallen in der gleichen Gruppe war. Über etwaige dritte Mitglieder dieser Gruppen liefert die Matrix M keine Aussage. Drei Paare waren in 15 Messintervallen und vier Paare in 14 Messintervallen in einer Gruppe.

Um die Verteilung der Werte zu veranschaulichen wurde ein Histogramm angefertigt. Ebenfalls wurde der Versuch mit $a_{max} = 10$ wiederholt um den Einfluss einer Parameterkonfiguration mit geringerer Dreiergruppenbildung zu untersuchen. Die Histogramme sind in Abbildung 6.11 abgebildet. Auf der x-Achse ist die Anzahl der gemeinsamen Messintervalle aufgetragen. Auf der y-Achse ist die Anzahl an intelligente Stromzähler Paaren aufgetragen, die so viele gemeinsame Messintervalle hatten. Es sind sowohl die Werte für $a_{max} = 3$ (grün), als auch die Werte für $a_{max} = 10$ (rot) eingezeichnet. Beispielsweise gab es bei $a_{max} = 10$ ungefähr 60 000 Paare von intelligenten Stromzählern, die genau ein mal zusammen in derselben Gruppe waren.

Sowohl für $a_{max} = 3$, als auch für $a_{max} = 10$ ist die am häufigsten auftretende Anzahl gemeinsamer Messintervalle die 3 und reduziert sich schnell bis auf wenige zweistellige Einzelfälle. Dies bedeutet, dass der Großteil der intelligenten Stromzähler während des gesamten beobachteten Monats nur wenige Male mit dem gleichen anderen Stromzähler in einer Gruppe war. Selbst für die Einzelfälle, die häufiger mit demselben anderen Stromzähler in einer Gruppe waren, sind 16 Kooperationen im Monat noch keine Gefahr für die Privatsphäre. Zumal ein Teil dieser Kooperationen mit einem zusätzlichen, dritten intelligenten Stromzähler, im Rahmen einer Dreiergruppe stattfindet. Betrachtet man $a_{max} = 3$ und $a_{max} = 10$ im Vergleich, so ist zu beobachten, dass das Histogramm von $a_{max} = 10$

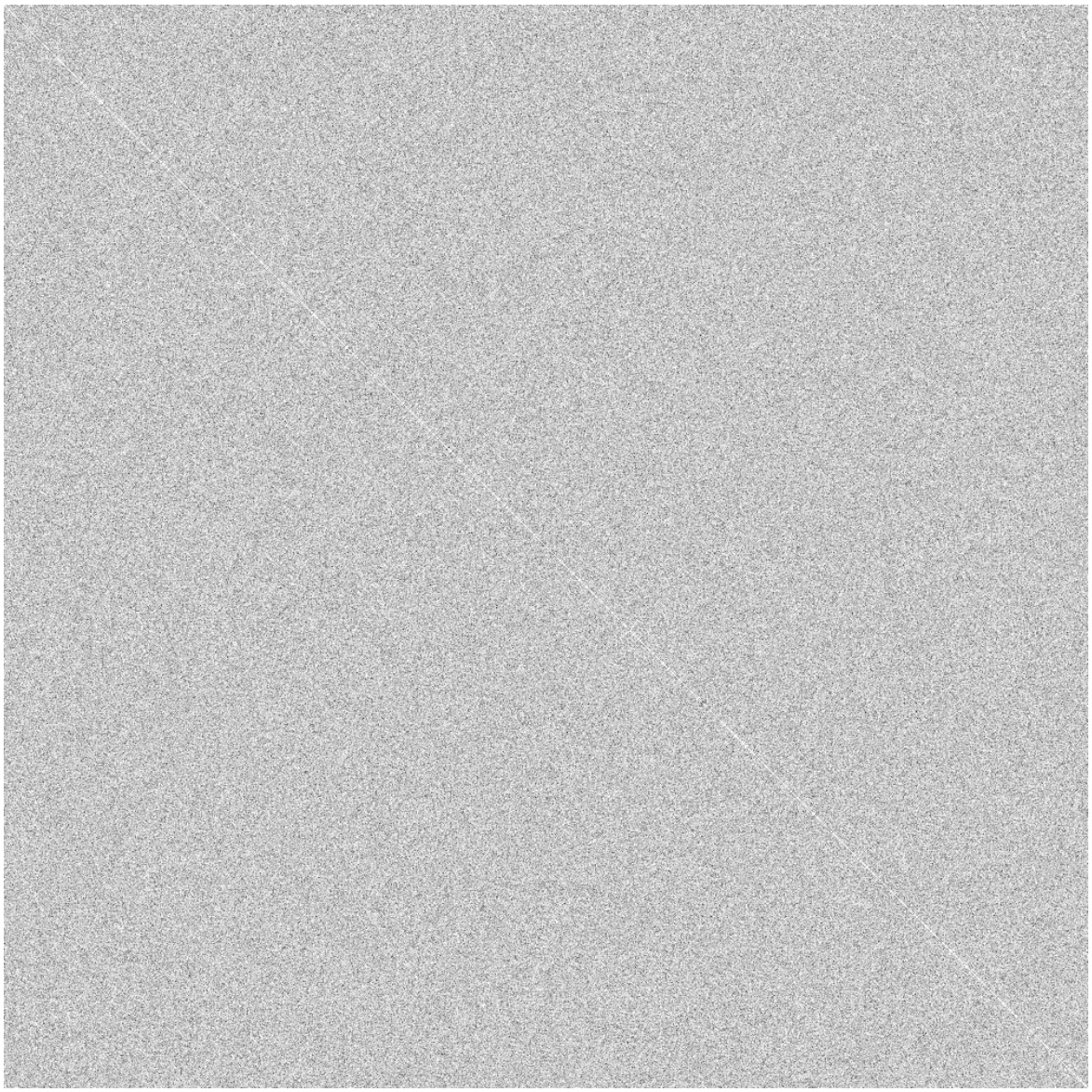


Abbildung 6.10: *Speeddating Heatmap: Simulation von 1 000 intelligenten Stromzählern mit $m_{max} = 5$ über einen Zeitraum von einem Monat.*

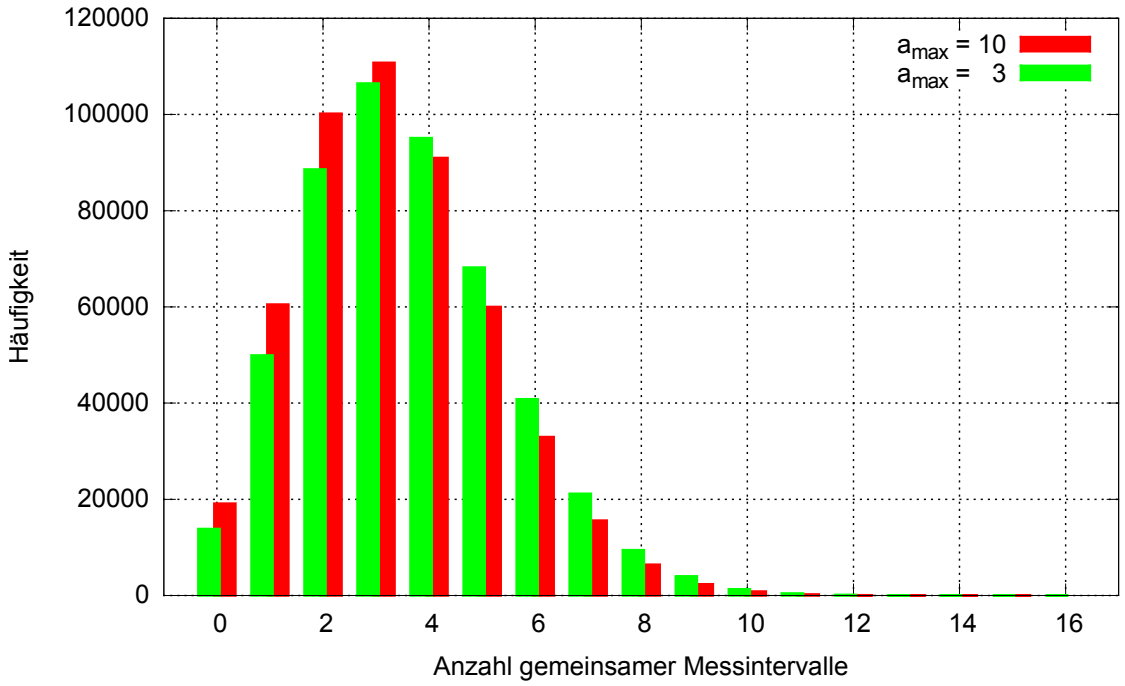


Abbildung 6.11: *Histogramm der Heatmap (Abbildung 6.10).*

komprimierter im unteren Bereich der gemeinsamen Messintervalle ist. Das arithmetische Mittel liegt für $a_{max} = 3$ bei $3,58$ Kooperationen, für $a_{max} = 10$ bei $3,29$ Kooperationen. Die schwächere Dreiergruppenbildung sorgt hier für eine stärkere Durchmischung der intelligenten Stromzähler. Auch ist die Maximalzahl an gemeinsamen Messintervallen bei $a_{max} = 10$ eins weniger, also nur 15.

Um ein konkretes Beispiel zur Veranschaulichung der zufälligen Gruppenbildung zu geben, wurden die genauen Gruppenzusammensetzungen der Simulation mit $a_{max} = 3$ betrachtet. Hierfür wurden aus jedem Messintervall die gebildeten Gruppen extrahiert. Insgesamt konnten so, über den gesamten Betrachtungszeitraum, 971 567 verschiedene Gruppen beobachtet werden. Für jede Gruppe wurde ermittelt, in wievielen Messintervallen sie auftrat. Von den insgesamt gebildeten Gruppen traten $91,72\%$ genau einmal auf. Ein geringer Anteil von $0,05\%$ der Gruppen trat in mehr als vier Messintervallen auf. Der schlechteste Fall trat für genau eine Gruppe von zwei intelligenten Stromzählern ein, die im gesamten beobachteten Zeitraum sieben Messintervalle in genau dieser Gruppenzusammensetzung hatten. Ein Gruppenprofil, das der Messdienstleister für die zugehörigen beiden Haushalte anfertigen könnte, hätte für den beobachteten Monat lediglich

sieben Einträge. Selbst in diesem schlechtesten Einzelfall ist die Gefahr für die Privatsphäre der beiden Haushalte sehr gering.

Zusammenfassend kann geschlossen werden, dass selbst bei einer relativ geringen Teilnehmerzahl von 1 000 intelligenten Stromzählern die erreichte Durchmischung nur sehr grobe Gruppenprofile zulassen würde. Die Dreiergruppenbildung erschwert die Profilbildung zusätzlich. Selbst bei einer so geringen Teilnehmerzahl würde ein Gruppenprofil im Schnitt pro Monat nur eine sehr kleine, einstellige Zahl an Einträgen enthalten. Das betrachtete Maximum lag in der Simulation bei sieben Einträgen. Für größere Teilnehmerzahlen wären dies noch deutlich weniger Einträge. Eine Gefahr für die Privatsphäre der Gruppe kann mit einer einfachen Gruppenprofilbildung durch den Messdienstleister nicht entstehen.

6.4.2 Passiver Angriff

Ein passiver Angriff durch den Messdienstleister besteht aus einer Anzahl an korrumpierten intelligenten Stromzählern, die sich aber protokollkonform verhalten. Der Messdienstleister bekommt genau dann Aufschluss über einen Messwert vom Angriffsziel z_T, wenn z_T im zugehörigen Messintervall ausschließlich mit korrumpierten Stromzählern kooperiert hat. Um ein Lastprofil von z_T mit zeitlicher Auflösung der Instanz des Smart Meterings berechnen zu können, muss dieser Messwert für eine Anzahl direkt aufeinanderfolgender Messintervalle, beispielsweise $\{m_1, m_2, m_3, \ldots\}$, ermittelt werden. Wie aber bereits im vorigen Abschnitt gezeigt, sorgt die zufällige Gruppenbildung in Smart Meter Speeddating für eine starke Durchmischung. Zur Abschätzung der Erfolgswahrscheinlichkeit für einen passiven Angriff wird die Betrachtung aus Abschnitt 6.4.1 aufgegriffen. Da dort auch Dreiergruppen gezählt wurden, stellt die Anzahl an Kooperationen eine Abschätzung nach oben dar. Dabei lag die durchschnittliche Anzahl Kooperationen bereits nahe am Minimum. Würde für die 1 000 intelligenten Stromzähler ein perfekte Reihenfolge, die in möglichst wenigen Kooperationen resultiert, aufgestellt werden, so wären dies im Schnitt $\frac{30 \cdot 24 \cdot 4}{1000} = 2,88$ Kooperationen. Es kann also geschlossen werden, dass sich Kooperationen eines intelligenten Stromzähler annähernd gleichverteilt über die intelligenten Stromzähler erstrecken. Das bedeutet, dass selbst mit einer großen Anzahl an korrumpierten intelligenten Stromzählern, beispielsweise 10% der beteiligten Stromzähler, eine Profilbildung nur mit einer geringen zeitlichen Auflösung durchführbar wäre. Im Beispiel wäre dies mit einem Zehntel der zeitlichen Auflösung der Messintervalle möglich. Ein Angriff durch

den Messdienstleister muss also aktiv durchgeführt werden um gute Aussichten auf Erfolg zu haben.

6.4.3 Angriff auf die Annahmeroutine

Ein erfolgreicher Angriff auf die Annahmeroutine von z_T innerhalb eines einzelnen Messintervalls bedeutet, dass z_T ausschließlich korrumpierte intelligente Stromzähler annimmt. Sei zunächst der Fall betrachtet, dass z_T nur eine Zweiergruppe bildet.

In diesem Fall hat z_T die Zahl m zufällig aus der Menge $\{1, \ldots, m_{max}\}$ gezogen und die Zahl a ist ohne Relevanz. Mit m wird bestimmt, wieviele Anfragen z_T ablehnt, bevor eine Anfrage angenommen wird. Betrachtet man die bei z_T eingehenden Anfragen als zeitlich geordnete Liste, so stellen die zweite bis $m_{max}+1$-te eintreffende Anfrage einen potentiellen Kandidaten dar. Der Angreifer muss nun sicherstellen, dass ein korrumpierter intelligenter Stromzähler an Position $m+1$ steht. Angenommen der Angreifer verfügt lediglich über einen korrumpierten Stromzähler. Da der Angreifer keine Kenntnis von m hat, kann er lediglich versuchen den korrumpierten intelligenten Stromzähler in den Kreis der möglichen Kandidaten einzuordnen. Gelingt ihm dies, so kann er mit einer Erfolgswahrscheinlichkeit von $\frac{1}{m_{max}}$ rechnen. Um aber dieses Ziel zu erreichen, darf die Anfrage des korrumpierten intelligenten Stromzählers weder als erste bei z_T eintreffen (die erste Anfrage wird immer abgelehnt), noch darf sie später als die $m_{max}+1$-te eintreffen. Die Erfolgswahrscheinlichkeit $\frac{1}{m_{max}}$ stellt also eine obere Grenze dar.

Verfügt der Angreifer über zwei korrumpierte intelligente Stromzähler, so kann er beide so früh wie möglich eine Anfrage an z_T senden lassen. Unter der Voraussetzung, dass kein anderer intelligenter Stromzähler frühzeitig eine Anfrage gesendet hat, würde dieses Vorgehen die Erfolgswahrscheinlichkeit von $\frac{1}{m_{max}}$ sichern. Generalisiert man dieses Vorgehen auf n korrumpierte intelligente Stromzähler, so kann eine Erfolgswahrscheinlichkeit von $\frac{n-1}{m_{max}}$ (oder 1 falls $n-1 \geq m_{max}$) erreicht werden. Dies gilt aber nur unter der Voraussetzung, dass kein anderer, nicht korrumpierter, intelligenter Stromzähler eine Anfrage gesendet hat. Da der Angreifer auf andere, nicht korrumpierte intelligente Stromzähler keinen Einfluss hat, kann er seine Erfolgswahrscheinlichkeit nur durch sehr schnelles Senden der Anfragen zu Beginn der Suchdauer maximieren. Das Eintreffen einer sehr großen Anzahl an Anfragen zu Beginn der Suchdauer stellt jedoch ein extrem anormales Verhalten dar und könnte von einer einfachen Anomalieerkennung entdeckt werden. Bevor

auf die mögliche Realisierung einer solchen eingegangen wird, muss jedoch noch der Fall einer Dreiergruppe mit z_T betrachtet werden.

Der Angreifer kann z_T nicht dazu zwingen lediglich eine Zweiergruppe zu bilden. Selbst wenn ein korrumpierter intelligenter Stromzähler erfolgreich eine Paarung mit z_T eingegangen ist, können weitere Anfragen von anderen, nicht korrumpierten intelligenten Stromzählern dazu führen, dass z_T eine Dreiergruppe eingeht. In diesem Fall wäre der Angriff erfolglos.

Um seine Erfolgschancen zu maximieren, muss ein Angreifer also sicherstellen, dass korrumpierte intelligente Stromzähler an zwei Positionen der Liste der bei z_T anfragenden intelligenten Stromzähler stehen: an der Stelle, die durch das von z_T zufällig gewählte m bestimmt wird *und* an der Stelle, die durch das von z_T zufällig gewählte a bestimmt wird. Da der Angreifer weder genaue Informationen über m, noch über a hat, muss er also sicherstellen, dass die gesamte Liste bis zur Länge $L = m_{max} + 1 + a_{max} + 1$ durch korrumpierte Stromzähler repräsentiert wird. Verfügt er über weniger als L korrumpierte intelligente Stromzähler, so ist die Erfolgswahrscheinlichkeit pro Messintervall entsprechend reduziert. Höhere Werte für m_{max} und a_{max} sorgen also für einen höheren Bedarf an korrumpierten Stromzählern für diesen Angriff.

Doch selbst wenn eine hohe Anzahl korrumpierter intelligenter Stromzähler vom Messdienstleister eingesetzt wird, so kann jederzeit ein anderer, nicht korrumpierter Stromzähler eine Anfrage an z_T senden. Sind nicht korrumpierte Stromzähler in der Liste der Anfragen vorhanden, so kann der Angriff fehlschlagen, wenn z_T solch einen Stromzähler mittels m oder a auswählt. Folglich ist der Angriff nur probabilistisch möglich. Dabei wird ein Erfolg um so wahrscheinlicher, je weniger nicht korrumpierte Stromzähler in der Anfrageliste stehen. Das Optimum könnte der Angreifer erreichen, wenn er alle korrumpierten intelligenten Stromzähler so früh wie möglich Anfragen schicken lässt. Wie bereits erwähnt, führt dieses Verhalten jedoch zu einer starken Anomalie der eintreffenden Anfragen bei z_T, die sehr einfach zu entdecken wäre.

Als Beispiel, wie diese Anomalieerkennung durchgeführt werden könnte, sei die Liste der eintreffenden Anfragen als Warteschlange interpretiert. Da zu Beginn der Suchdauer alle intelligenten Stromzähler Suchanfragen an einen zufälligen anderen intelligenten Stromzähler versenden, kann davon ausgegangen werden, dass das Eintreffen jeder Anfrage zufällig und voneinander unabhängig ist. Das Verhalten der eintreffenden Anfragen kann daher mit der Poisson-Verteilung (siehe beispielsweise Zimmermann und Stache [139]) beschrieben werden. Verwendet man t_{max} als Zeiteinheit, so kann die mittlere Ankunftsrate λ entweder stochastisch

oder mittels Beobachtung eines nicht angegriffenen Smart Meterings bestimmt werden.

Mittels der Wahrscheinlichkeit

$$P(t,n) = \frac{(\lambda t)^n}{n!} e^{-\lambda t}$$

innerhalb von t Zeiteinheiten n Anfragen zu erhalten, lässt sich dann eine beobachtete Situation durch den intelligenten Stromzähler bewerten. Wird ein Angriff erkannt, so könnte sich der betroffene Stromzähler für dieses Messintervall zurückziehen und keinen Abgabewert senden. Der Angriff wäre dann erfolglos. Tritt dies für viele Messintervalle auf, kann beispielsweise ein Aufsichtsorgan oder der Haushalt über die Angriffe informiert werden.

Ein Angriff auf die Annahmeroutine mit maximierter Erfolgschance benötigt also mindestens $m_{max} + 1 + a_{max} + 1$ korrumpierte Stromzähler. Er kann aber nur dann unentdeckt durchgeführt werden, wenn er kein signifikant anormales Aufkommen von Anfragen bei z_T verursacht. Ein annähernd normales Aufkommen von Anfragen bedeutet jedoch, dass auch nicht korrumpierte Stromzähler in der Anfrageliste auftauchen und damit die Erfolgswahrscheinlichkeit der Attacke signifikant reduziert wird. Wird die Attacke so durchgeführt, dass sie gar kein anormales Aufkommen verursacht, so resultiert dies in der Situation eines passiven Angriffs.

6.4.4 Angriff auf die Suchroutine

Die Suchroutine in Smart Meter Speeddating wählt aus der Gesamtliste der teilnehmenden intelligenten Stromzähler zufällig einen aus. Da die Annahmeroutine aber viele Anfragen ablehnt, wählt die Suchroutine mehrmals potentielle Partner aus und sendet eine Anfrage an diesen. So lange, bis die Suchroutine oder die Annahmeroutine erfolgreich war. Dieses Verhalten der Suchroutine kann zu einem Angriff genutzt werden:

Angenommen in einem Smart Metering ist ein Anteil von x% der intelligenten Stromzähler korrumpiert. Daraus folgt, dass jede zufällige Wahl der Suchroutine von Stromzähler z_T mit der Wahrscheinlichkeit x% einen korrumpierten intelligenten Stromzähler auswählt. Erhält ein korrumpierter Stromzähler eine Anfrage von z_T, so nimmt er diese an. Das Angriffsziel ist dann für dieses Messintervall erfüllt, da z_T gemäß seiner Rolle als anfragender intelligenter Stromzähler selbst

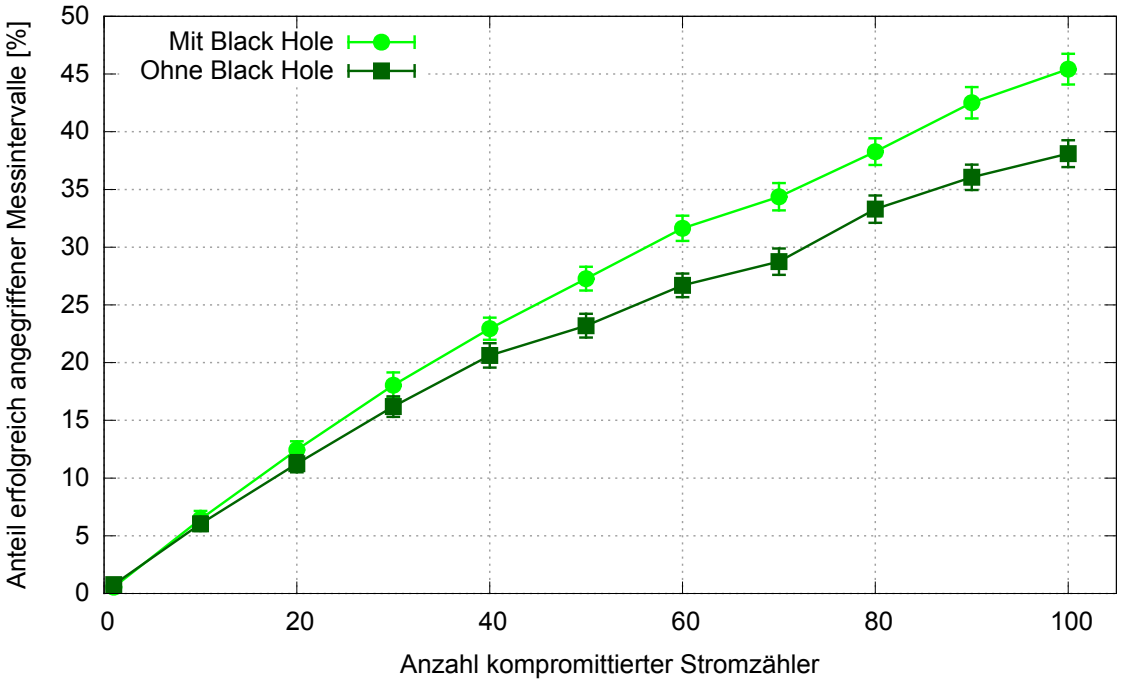


Abbildung 6.12: *Wirksamkeit der Promiscuous Sybil Attacke bei 1 000 intelligenten Stromzählern ($m_{max} = 5$).*

keine Anfragen annehmen darf. Das häufige Ablehnen von Anfragen durch nicht korrumpierte Stromzähler begünstigt die Attacke deutlich, so dass die Erfolgswahrscheinlichkeit wesentlich höher als x% liegt.

Das Ausbringen von korrumpierten intelligenten Stromzählern, die eine Anfrage von z_T sofort annehmen, wird im Folgenden als *Promiscuous Sybil* Angriff bezeichnet. Dabei führen die korrumpierten Stromzähler selbst keine Suchroutine durch und lehnen Anfragen von anderen intelligenten Stromzählern $z_i \neq z_T$ ab. Eine Intensivierung der Promiscuous Sybil Attacke ist mittels eines kombinierten *Black Hole (BH)* Angriffs möglich. Hier nehmen die korrumpierten Stromzähler *alle* eintreffenden Anfragen an und reduzieren damit die Anzahl der nicht korrumpierten Stromzähler, die mit z_T noch kooperieren könnten.

Um die Erfolgswahrscheinlichkeit dieser Angriffe zu untersuchen wurden beide in OverGrid implementiert und mit 1 000 intelligenten Stromzählern für die Dauer eines Monats evaluiert. Als Parameterkonfiguration für Smart Meter Speeddating wurde die, aus Abschnitt 6.3.5 bekannte, Parameterkonfiguration mit $m_{max} = 5$ verwendet. Die Anzahl der korrumpierten Stromzähler wurde von 1 bis 100, also

von einem Promille bis 10% der Gesamtzahl, variiert. Der Anteil der Messintervalle, in denen z_T in einer Gruppe mit ausschließlich korrumpierten intelligenten Stromzählern war, ist in Abhängigkeit von der Anzahl korrumpierter intelligenter Stromzähler in Abbildung 6.12 aufgezeichnet. Auf der x-Achse ist dabei die Anzahl der eingesetzten korrumpierten Stromzähler und auf der y-Achse der Anteil der Messintervalle mit erfolgreicher Attacke auf z_T eingezeichnet.

Es ist zu erkennen, dass die Erfolgswahrscheinlichkeit beider Attacken mit der Anzahl der korrumpierten Stromzähler wächst. Dabei steigt die Erfolgswahrscheinlichkeit der Black Hole Attacke im Vergleich zur normalen Promiscuous Sybil Attacke stärker mit der Anzahl korrumpierter Stromzähler. Dies entspricht den Erwartungen, da eine größere Anzahl an korrumpierten Stromzählern den Black Hole Effekt verstärkt. Jeder nicht korrumpierte Stromzähler der eine Anfrage an einen der korrumpierten Stromzähler sendet, wird effektiv für das Angriffsziel z_T aus dem Smart Metering entfernt. Dies verringert die Wahrscheinlichkeit für z_T bei einer versendeten Anfrage von einem nicht korrumpierten Stromzähler angenommen zu werden.

Doch genau wie der Angriff auf die Annahmeroutine sorgt auch der Angriff auf die Suchroutine für eine statistische Anomalie. Sehr deutlich lässt sich dies anhand der Heatmap des simulierten Black Hole Angriffs nachvollziehen (Abbildung 6.13). Jeder Bildpunkt beschreibt wieder die Häufigkeit der Kooperationen zwischen zwei intelligenten Stromzählern. Die sehr dunklen Balken in der Heatmap stellen die intelligenten Stromzähler, die eine Promiscuous Sybil (BH) Attacke durchführen dar. Sie haben außerordentlich viele Kooperationen mit anderen intelligenten Stromzählern. Der Rest der Heatmap ist im Vergleich zu der normalen, also nicht während eines Angriffs aufgezeichneten, Heatmap (Abbildung 6.10) deutlich: die sehr hellen Regionen zeigen extrem seltene Kooperationen mit den anderen, nicht korrumpierten Stromzählern.

Den einzelnen Stromzählern fehlt natürlich die von der Heatmap gestellte Gesamtsicht auf die Geschehnisse. Jedoch verfügt jeder intelligente Stromzähler über eine einzelne Zeile der Heatmap, sofern er für jedes Messintervall die mit ihm kooperierenden intelligenten Stromzähler protokolliert. Dies lässt sich selbst für einen längeren Zeitraum mit geringem Speicheraufwand realisieren. Anhand dieses Protokolls ist es für einen intelligenten Stromzähler einfach eine Promiscuous Sybil Attacke mit oder ohne Black Hole zu identifizieren und zu bekämpfen: ist die Anzahl an Kooperationen mit einem intelligenten Stromzähler deutlich höher als im Mittel mit den anderen intelligenten Stromzählern, so liegt vermutlich eine Attacke vor. Als Gegenmaßnahme kann der betreffende Stromzähler temporär oder

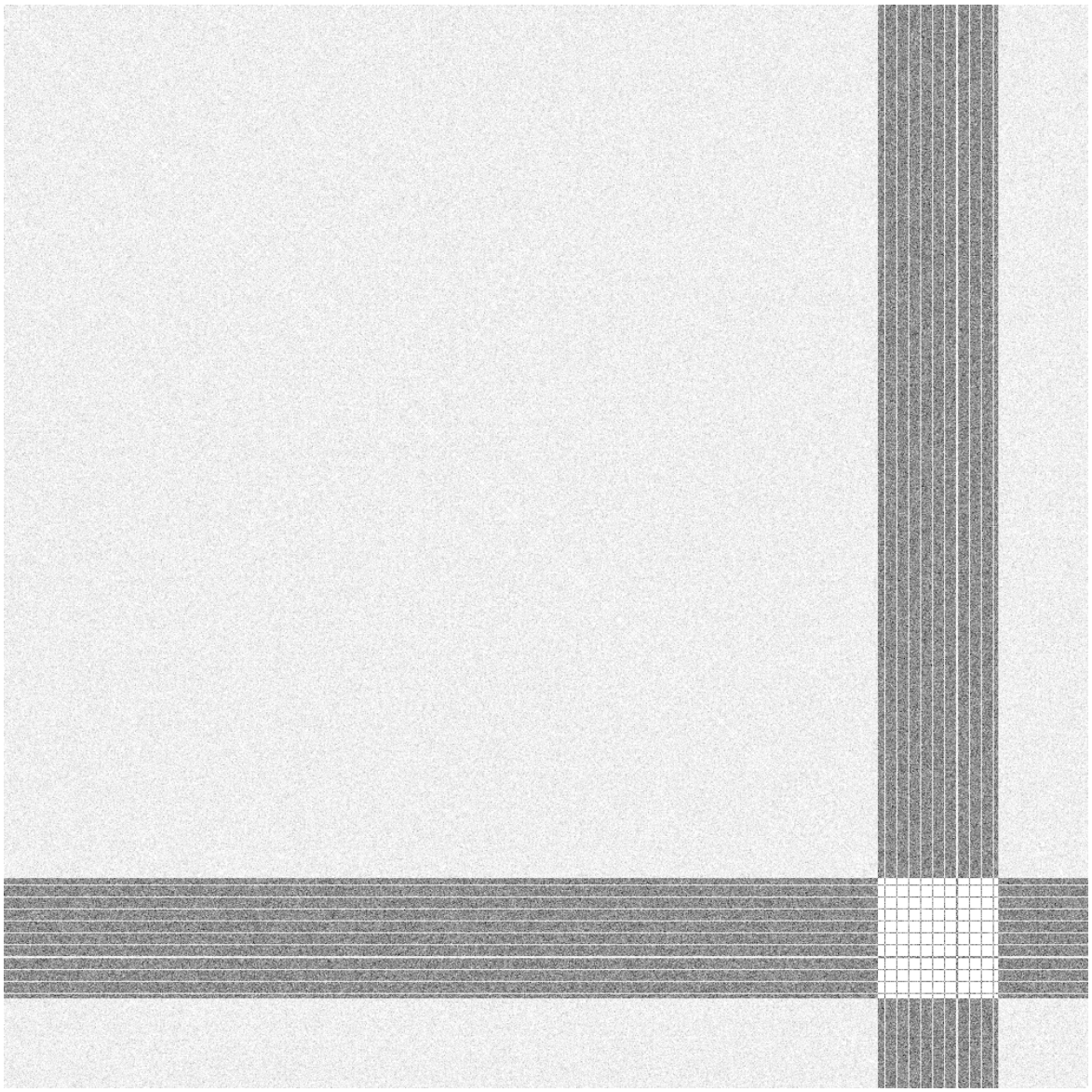


Abbildung 6.13: *Speeddating Heatmap: Angriff mittels* 10% *Promiscuous-Sybil (BH) mit* $m_{max} = 5$ *über einen Zeitraum von einem Monat.*

dauerhaft ignoriert werden. Dadurch könnte mit der Promiscuous Sybil Attacke (mit und ohne Black Hole) lediglich ein Ungleichgewicht der Kooperationen und damit eine leichte Bevorzugung der korrumpierten intelligenten Stromzähler erreicht werden. Wie stark dieses Ungleichgewicht ausfällt ist letztlich von der Toleranz der Abweichung zum Mittelwert der Anzahl an Kooperationen abhängig.

Es kann zusammengefasst werden, dass die Promiscuous Sybil Attacke bei einem Einsatz einer ausreichenden Anzahl von korrumpierten intelligenten Stromzählern sehr effektiv ist. Trotzdem ist sie nur probabilistisch erfolgreich, also nicht planbar in einem Messintervall. Besonders aber mit der Black Hole Erweiterung sorgt sie schon ab einem geringen Anteil von korrumpierten Stromzählern für eine so hohe Erfolgswahrscheinlichkeit, dass eine Gefahr für die Privatsphäre besteht. Jedoch sind beide Angriffsvarianten nicht unerkannt durchführbar. Beim angegriffenen intelligenten Stromzähler sorgt die Promiscuous Sybil Attacke für ein starkes Ungleichgewicht bezüglich der Kooperationen mit anderen intelligenten Stromzählern. Wird die Attacke mit einer Black Hole Attacke kombiniert, so tritt dieses Ungleichgewicht bei *allen* intelligenten Stromzählern auf.

6.4.5 Statistische Analyse

Das SMSD-Verfahren hat als eines der Entwurfsziele die Bildung möglichst kleiner Gruppen zur Erhöhung der Smart Metering Leistung. Wie bereits diskutiert führen kleine Gruppen zu einem schwächeren Schutz der Privatsphäre der Gruppe. Auch wenn der häufige Wechsel der Gruppenkonfiguration das Zuordnen des zeitlichen Verlaufs von Power-Events verhindert, kann bereits die Einzelbetrachtung einer kleinen Gruppe, also insbesondere nicht im zeitlichen Verlauf, eine Gefahr für die Privatsphäre darstellen.

Seien beispielsweise die intelligenten Stromzähler z_1 und z_2 zweier Haushalte angenommen. Diese seien in einem Messintervall in einer Zweiergruppe. Erhält der Messdienstleister im Rahmen von SMSD nun die Abgabewerte von z_1 und z_2, so kann er das Aggregat der beiden Haushalte für dieses Messintervall bestimmen. Wird als Messgröße die aktuelle Last verwendet, so erhält der Messdienstleister die aktuelle Last der beiden Haushalte zusammen. Auch ohne einen zeitlichen Verlauf kann diese Information bereits die Privatsphäre der Haushalte verletzen. Schließlich ist an der aktuellen Last mit hoher Wahrscheinlichkeit die Anwesenheit von Personen im Haushalt erkennbar.

Verfügt der Messdienstleister neben den Informationen aus dem SMSD-Verfahren über Sekundärinformationen, so kann er möglicherweise noch weitere Informa-

tionen aus den Smart Metering Daten ermitteln. Weiß der Messdienstleister beispielsweise mit Sicherheit, dass keiner der beiden Haushalte über Energieerzeugungsanlagen (wie beispielsweise Photovoltaik) verfügt, so kann er ausschließen, dass einer der Haushalte negativ zur aktuellen Last beigetragen, also den anderen Haushalt teilweise kompensiert hat.

Auch kann der Messdienstleister die Aggregate der verschiedenen Gruppen über mehrere Messintervalle hinweg speichern und gegeneinander aufrechnen oder korrelieren. Insbesondere mit Sekundärinformationen könnte hier ein Erkenntnisgewinn möglich sein. Da dies aber über mehrere Messintervalle hinweg mit sich verändernden Daten geschehen müsste, ist anzunehmen, dass die ermittelten Daten bestenfalls fehlerbehaftete Durchschnittswerte der Messintervalle ergeben.

Die Bewertung von Privatsphäre und Privatsphärenschutz ist eine offene Forschungsfrage. Deshalb kann hier nicht abschließend beurteilt werden, ob beispielsweise die zeitlich isolierte Betrachtung des Aggregats von zwei Haushalten bereits eine Verletzung der Privatsphäre darstellt oder nicht. Sollten größere Gruppenkonfigurationen wünschenswert sein, so kann mit dem, in dieser Arbeit nicht näher betrachteten, Parameter g_{max} eine Variante von SMSD realisiert werden, die auch größere Gruppenkonfigurationen erzeugen kann. Auch wird mit dem Elderberry-Verfahren in Kapitel 7 ein Verfahren mit einer Aggregation über deutlich größere Gruppen vorgestellt.

6.4.6 Zusammenfassung

Wie in den vorhergehenden Abschnitten gezeigt wurden, existieren mehrere Möglichkeiten das Smart Meter Speeddating Verfahren anzugreifen. Durch die stark zufällige Durchmischung der Gruppierungen ist ein rein passiver und damit nicht erkennbarer Angriff jedoch wenig erfolgversprechend. Die Angriffe auf Suchroutine und Annahmeroutine ermöglichen es Einfluss auf die Gruppenbildung zu nehmen. Damit ist, wenn auch nicht unentdeckt, ein Angriff auf die Privatsphäre einzelner Haushalte möglich. Wie aber gezeigt wurde, muss dieser Angriff vom Messdienstleister erfolgen. Ein Angriff, der lediglich durch korrumpierte Stromzähler durchgeführt wird, kann keinen Erfolg haben (siehe Abschnitt 5.4).

Zwar wird in dieser Arbeit der Messdienstleister als potentieller Angreifer gewertet, aber dennoch muss berücksichtigt werden, dass die Folgen eines vom Messdienstleister durchgeführten und entdeckten Angriffs schwerwiegend für den Messdienstleister wären. Wird der Messdienstleister bei einem Angriff ertappt, so

ist dies mindestens rufschädigend. Seine Motivation für einen Angriff sinkt also mit der Gefahr der Entdeckung.

Durch die gute Durchmischung der Gruppenbildung gewährleistet SMSD eine gleichmäßige Verteilung der Gruppenzugehörigkeit. Sind in einem Smart Metering beispielsweise 1 000 intelligente Stromzähler beteiligt, so kann ein einzelner intelligenter Stromzähler davon ausgehen, dass er mit jedem anderen intelligenten Stromzähler im Schnitt circa vier mal im Monat kooperiert. Dabei findet ein Teil dieser Kooperationen im Rahmen von erweiterten Paarungen, also unter Mitwirken eines weiteren intelligenten Stromzählers, statt. Dank dieser starken Durchmischung benötigt ein erfolgreicher, schwer zu entdeckender Angriff einen sehr großen Anteil an korrumpierten Stromzählern. Eine Sybil Attacke größeren Ausmaßes ist für den Messdienstleister mit großen Kosten für die Anschaffung der intelligenten Stromzähler verbunden.

Damit stellt sowohl die hohe Gefahr einer mögliche Entdeckung und der damit verbundenen Folgen als auch der hohe Bedarf an korrumpierten intelligenten Stromzählern eine hohe Hürde für Angriffe durch den Messdienstleisters dar.

6.5 Evaluation der Smart Metering Leistung

In diesem Abschnitt wird eine Evaluation von Smart Meter Speeddating bezüglich der Smart Metering Leistung durchgeführt. Wie auch schon bei der Evaluation des Smart Metering Leistung von SMART-ER in Abschnitt 5.5 werden folgende Aspekte betrachtet:

- Der Anteil an validen Abgabewerten unter Churn (Abschnitt 6.5.1). Hier wird Smart Meter Speeddating auch mit dem aus Abschnitt 5.5 bekannten Baseline verglichen.

- Der Rechenaufwand von Smart Meter Speeddating für einzelne intelligente Stromzähler (Abschnitt 6.5.2).

- Der Speicheraufwand von Smart Meter Speeddating auf einzelnen intelligenten Stromzählern (Abschnitt 6.5.3).

- Der für Smart Meter Speeddating verursachte Kommunikationsaufwand (Abschnitt 6.5.4).

Tabelle 6.7: *Parameterkonfigurationen zum Vergleich von Smart Meter Speeddating und Baseline unter verschieden starkem Churn.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
s	entsprechend Abschnitt 6.3.5
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$
	in Kombination
a_{max}	$\overbrace{\{3,\ 5,\ 10,\ 15, 20\}}$

6.5.1 Leistung

Zur Evaluation der Smart Metering Leistung wurde der Anteil valider Abgabewerte in Abhängigkeit vom Churn betrachtet. Zusätzlich zu den in Abschnitt 6.3.5 gewählten Parameterkonfigurationen von Smart Meter Speeddating wurde zum Vergleich Baseline aus Abschnitt 5.5 hinzugezogen. Die betrachteten Parameterkonfigurationen sind in Tabelle 6.7 zusammengefasst. Die Ergebnisse sind in Abbildung 6.14 zu sehen. Auf der x-Achse ist die durchschnittliche Verfügbarkeit der Kommunikationsverbindung aufgetragen. Auf der y-Achse ist der erzielte Anteil an validen Abgabewerten eingezeichnet. Für jede Parameterkonfiguration von Smart Meter Speeddating ist das arithmetischem Mittel mit 98%-Konfidenzintervall eingezeichnet.

Es ist zu erkennen, dass die Leistung jeder Parameterkonfiguration im Wesentlichen linear mit der Verfügbarkeit abnimmt. Dabei sorgt ein höherer Wert für m_{max} auch für eine etwas stärkere Empfindlichkeit für Churn. Dies ist gut an der Gruppe der $m_{max} \geq 10$ zu erkennen (Symbole: gefülltes Quadrat, Raute, Dreieck, leeres Quadrat). Diese Gruppe der Parameterkonfigurationen befinden sich bei der höchsten untersuchten Verfügbarkeit noch in einem Bereich von circa $0,25$ Prozentpunkten. Dies ist der Abstand zwischen $m_{max} = 10$ (Symbol: gefülltes Quadrat) und $m_{max} = 25$ (Symbol: leeres Quadrat). Bei der geringsten simulier-

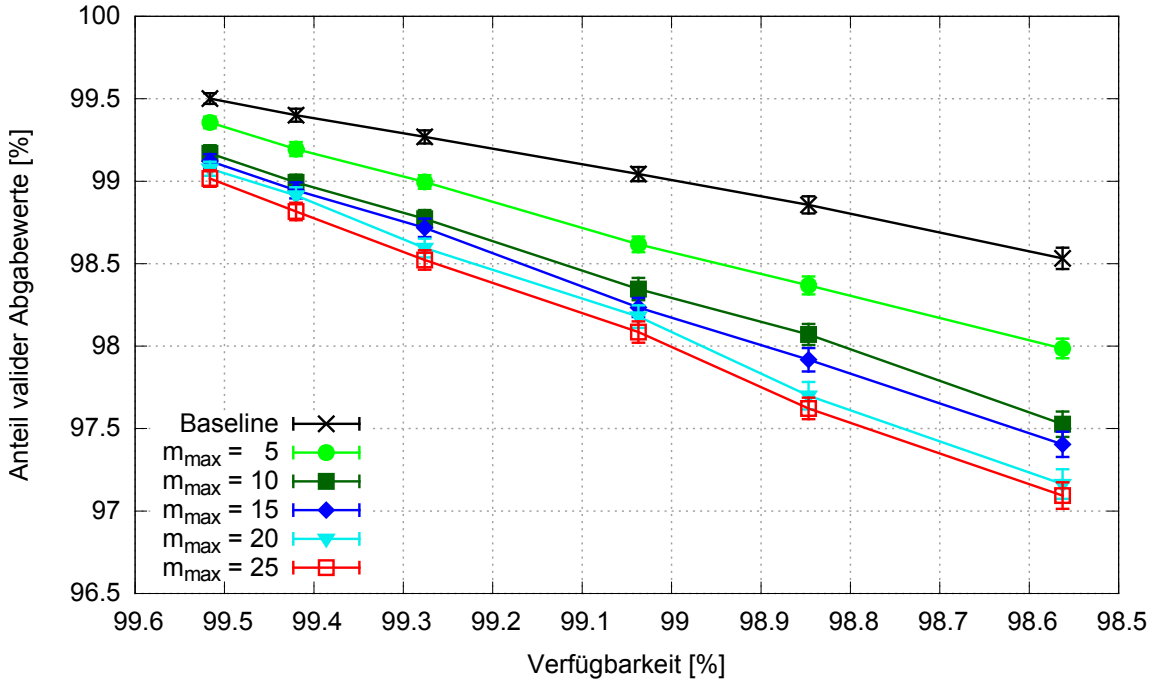


Abbildung 6.14: *Vergleich von Smart Meter Speeddating Parameterkonfigurationen mit Baseline in Abhängigkeit des Churns.*

ten Verfügbarkeit umfasst dieser Bereich circa 0,5 Prozentpunkte. Der Abstand zwischen der besten und der schlechtesten Parameterkonfiguration hat sich also vergrößert. Bemerkenswert ist jedoch, dass bei der als normal angenommenen Verfügbarkeit ($\approx 99,5\%$) selbst für hohe m_{max} der Anteil valider Abgabewerte über 99% liegt. Das theoretische Maximum, also Baseline, liegt hier bei 99,5%. Und auch bei starkem Churn sind für die Parameterkonfiguration mit der schlechtesten Smart Metering Leistung ($m_{max} = 25$, rot) im Mittel immer noch über 97% der intelligenten Stromzähler im Smart Metering Ergebnis enthalten. Für Baseline liegt der Wert bei 98,5%.

Um die Smart Metering Leistung von Smart Meter Speeddating im Vergleich zu der erreichbaren Leistung bei einem alleinigen Einsatz von SMART-ER einschätzen zu können, wurde ein direkter Vergleich zwischen den beiden Verfahren durchgeführt. Für SMART-ER wurden hierfür Parameterkonfigurationen mit einer Gruppengröße G ausgewählt, so dass $G-1 = m_{max} + a_{max} + 2$ der verglichenen Smart Meter Speeddating Konfiguration entspricht. Diese Gruppengröße ist aus Abschnitt 6.4.3 abgeleitet. Dort wurde $m_{max} + a_{max} + 2$ als benötigte Anzahl von

Tabelle 6.8: *Parameterkonfigurationen zum Vergleich von Smart Meter Speeddating und SMART-ER unter verschieden starkem Churn.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
s	entsprechend Abschnitt 6.3.5
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$
	in Kombination
a_{max}	$\overbrace{\{3,\ 5,\ 10,\ 15, 20\}}$
SMART-ER Gruppengröße	$G \in \{11, 28, 48\}$
Anzahl versendeter Fragmente	Gruppengröße -1

korrumpierten intelligenten Stromzählern ermittelt, um einen Angriff auf die Annahmeroutine durchzuführen, der eine hohe Erfolgswahrscheinlichkeit hat[3]. Bei einem alleinigen Einsatz von SMART-ER mit einer Gruppengröße von G würde ein Messdienstleister mit $G-1$ korrumpierten intelligenten Stromzählern die Privatsphäre eines einzelnen Haushaltes erfolgreich angreifen können. Bei den verglichenen Parameterkonfigurationen von Smart Meter Speeddating und SMART-ER ist also mit einem besseren Schutz gegen Angriffe des Messdienstleister bei Smart Meter Speeddating zu rechnen. Die betrachteten Parameterkonfigurationen sind in Tabelle 6.8 zusammengefasst. Es wurde für beide Verfahren der Anteil valider Abgabewerte in Abhängigkeit vom Churn betrachtet. Die Ergebnisse sind in Abbildung 6.15 zu sehen. Auf der x-Achse ist die durchschnittliche Verfügbarkeit der Kommunikationsverbindung aufgetragen. Auf der y-Achse ist der erzielte Anteil an validen Abgabewerten eingezeichnet. Für jede Parameterkonfiguration ist das arithmetischem Mittel mit 98%-Konfidenzintervall eingezeichnet. Die Parameterkonfigurationen von Smart Meter Speeddating wurden mit verschiedenen leeren Symbolen (Quadrat, Raute, Kreis) in rot eingezeichnet. Die entsprechenden

[3]Dies gilt allerdings nur ohne die dort erläuterte Anomalieerkennung.

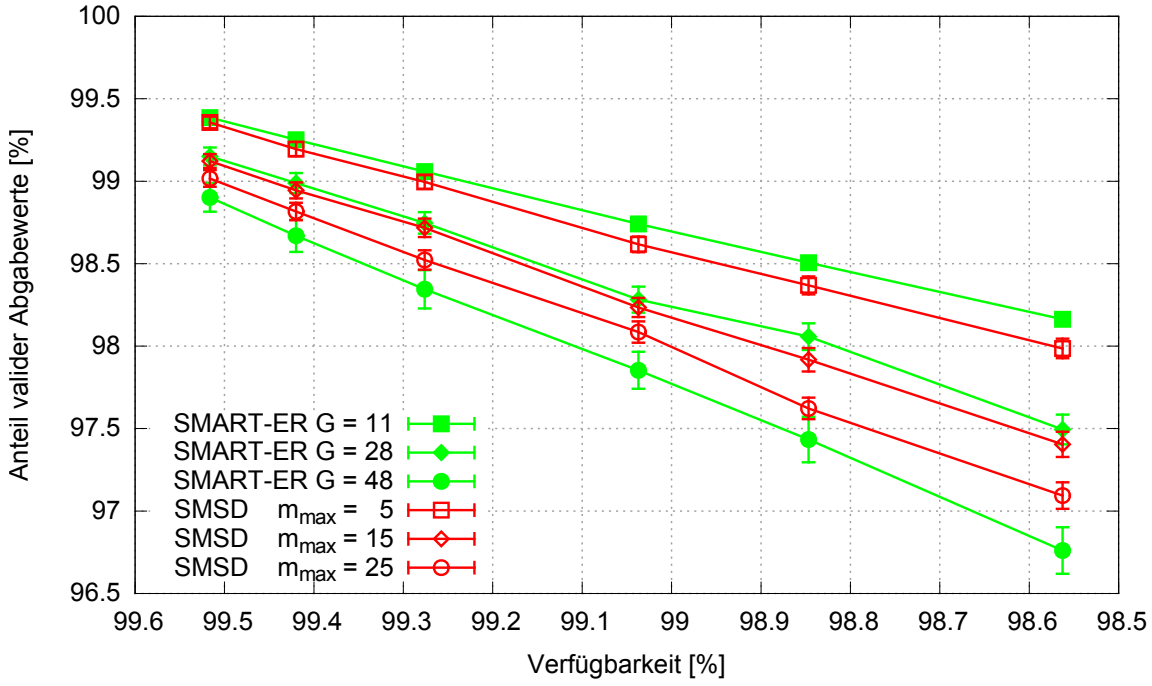


Abbildung 6.15: *Vergleich von Smart Meter Speeddating Parameterkonfigurationen mit SMART-ER in Abhängigkeit des Churns.*

SMART-ER Parameterkonfigurationen wurden mit dem gleichen, aber gefüllten Symbol in grün eingezeichnet.

Betrachtet man zunächst die Parameterkonfigurationen mit $G = 11$ (Symbol: Quadrat), respektive $m_{max} = 5$, so ist zu erkennen, dass Smart Meter Speeddating bereits bei normalem Churn geringfügig schlechtere Ergebnisse liefert als ein direkter Einsatz von SMART-ER. Dieser Nachteil intensiviert sich bei stärkerem Churn etwas. Da Smart Meter Speeddating eine dezentrale Gruppenbildung durchführt, kann es trotz der kleinen Gruppengröße nicht die Leistung von SMART-ER, das mittels zentral gebildeter Gruppen funktioniert, erreichen. Vergleicht man jedoch die Parameterkonfiguration mit $G = 28$ (Symbol: Raute), respektive $m_{max} = 15$, so fällt der Unterschied weniger deutlich aus. Im Durchschnitt ist Smart Meter Speeddating auch hier etwas schlechter als SMART-ER. Aufgrund der sich teilweise überschneidenden Konfidenzintervalle kann hier aber keine definitive Aussage getroffen werden. Die Parameterkonfiguration mit $G = 48$ (Symbol: Kreis), respektive $m_{max} = 25$, zeigt einen deutlichen Vorteil von Smart Meter Speeddating gegenüber SMART-ER. Hier wird der Nachteil, der durch die dezentrale Gruppen-

Tabelle 6.9: *Parameterkonfigurationen zur Untersuchung der Skalierbarkeit von Smart Meter Speeddating.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{1\,000, 2\,000, \ldots, 10\,000\}$
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
s	entsprechend Abschnitt 6.3.5
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$ in Kombination
a_{max}	$\overbrace{\{3,\ 5,\ 10,\ 15, 20\}}$

bildung entsteht, durch die kleinen Gruppengröße von Smart Meter Speeddating kompensiert, so dass insgesamt eine bessere Leistung als die der verglichenen Parameterkonfiguration von SMART-ER erzielt werden kann.

Zieht man in Betracht, dass Smart Meter Speeddating bei den hier verglichenen Parameterkonfigurationen einen besseren Schutz gegen einen Angriff des Messdienstleisters bietet, so kann dies als sehr gutes Ergebnis für Smart Meter Speeddating gewertet werden. Während bei SMART-ER ein Angriff mit einer ausreichenden Anzahl an korrumpierten intelligenten Stromzählern ($G-1$) immer und unerkannt Erfolg hat, ist ein Angriff bei Smart Meter Speeddating nur mit einer Wahrscheinlichkeit und mit hohem Erkennungsrisiko durchführbar.

Zur Evaluation der Skalierbarkeit von Smart Meter Speeddating wurden die in Abschnitt 6.3.5 vorgestellten Parameterkonfigurationen mit variierender Anzahl an intelligenten Stromzählern und mit normalem Churn simuliert. Die betrachteten Parameterkonfigurationen sind in Tabelle 6.9 zusammengefasst. Es wurde je Parameterkonfiguration das arithmetische Mittel samt 98%-Konfidenzintervall berechnet und in Abbildung 6.16 eingezeichnet. Auf der x-Achse ist die Anzahl simulierter intelligenter Stromzähler aufgetragen. Auf der y-Achse ist der Anteil valider Abgabewerte aufgetragen. Jede Parameterkonfiguration von Smart Meter Speeddating ist als eigene Kurve eingezeichnet.

Es lässt sich erkennen, dass Smart Meter Speeddating hervorragend skaliert. Der Anteil valider Abgabewerte bleibt für jede Parameterkonfiguration durchgehend

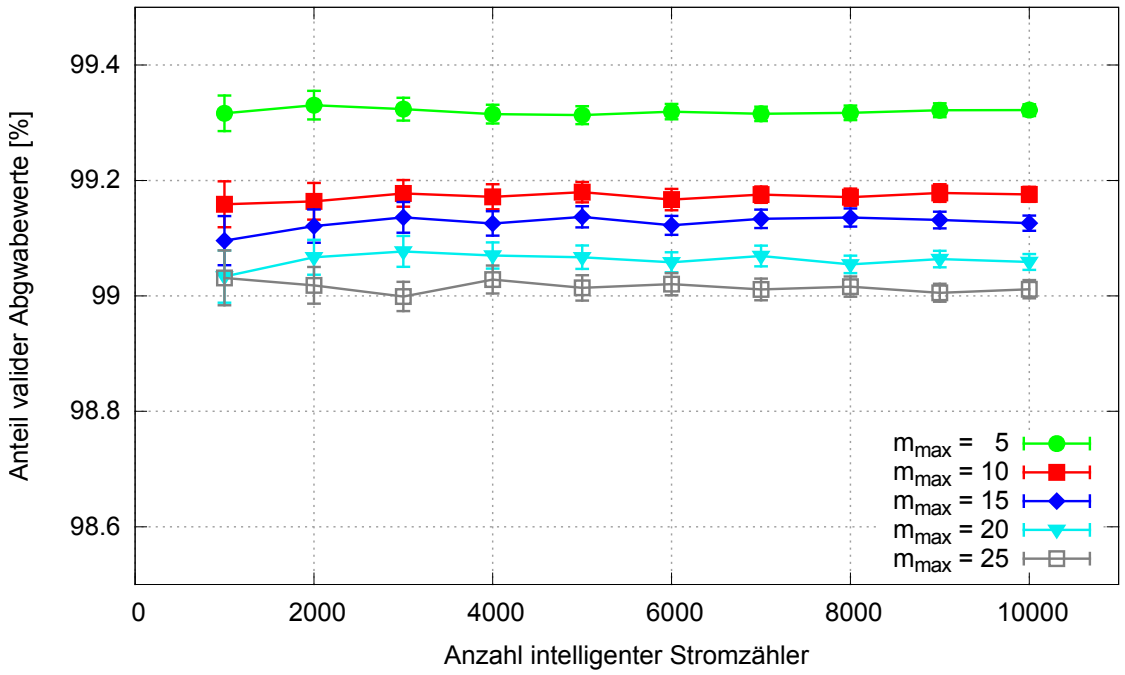


Abbildung 6.16: *Skalierbarkeit von Smart Meter Speeddating Parameterkonfigurationen.*

stabil. Dies ist zu erwarten, da eine größere Anzahl ein teilnehmenden intelligenten Stromzählern zu mehr Möglichkeiten der Gruppenbildung führt und damit das Verfahren eher begünstigt als verschlechtert. Dies ist auch an den Konfidenzintervallen der verschiedenen Parameterkonfigurationen zu erkennen. Mit steigender Anzahl simulierter intelligenter Stromzähler werden die Konfidenzintervalle kleiner. Dies spricht nicht nur für eine sehr gute Skalierbarkeit des Verfahrens, sondern auch für stabilere Ergebnisse mit wachsender Anzahl an intelligenten Stromzählern.

6.5.2 Rechenaufwand

Das Smart Meter Speeddating verwendet SMART-ER als Baustein. Daher fällt auch der SMART-ER Rechenaufwand aus Abschnitt 5.5.5 in Smart Meter Speeddating an. Der zusätzliche Rechenaufwand für Smart Meter Speeddating fällt sehr gering aus. Er beschränkt sich auf das zufällige Ziehen von SMART-ER Fragmenten, die für eine potentielle Annahme in den Anfragen bereits mitgeschickt werden und die Verwaltung der Variablen a, m. Für a und m muss ebenfalls für jedes Messintervall

eine Zufallszahl gezogen werden. Neben dem Ziehen von Zufallszahlen sind nur sehr wenige $(a + m)$ arithmetische Operationen nötig.

Durch die geringe Gruppengröße von 2 oder 3 in Smart Meter Speeddating wird der Aufwand für das Verwalten der SMART-ER Abhängigkeitsliste vereinfacht. Sie kann in Smart Meter Speeddating auf jedem intelligenten Stromzähler maximal zwei Einträge lang sein.

Der Rechenaufwand für Smart Meter Speeddating wird also dominiert durch das verwendete SMART-ER Verfahren, welches ebenfalls schon einen sehr geringen Rechenaufwand aufwies. Durch die geringe Gruppengröße wird dieser sogar noch reduziert. Insgesamt ist dadurch der Rechenaufwand für Smart Meter Speeddating bei heutigen Geräten mit beschränkter Rechenkapazität vernachlässigbar.

6.5.3 Speicheraufwand

Smart Meter Speeddating benötigt die Gesamtliste der teilnehmenden intelligenten Stromzähler Z auf jedem intelligenten Stromzähler. Pro Eintrag in Z ist die IP-Adresse des intelligenten Stromzählers (16 Byte bei IPv6), ein Identifikator (8 Byte) und Schlüsselmaterial (32 Byte) nötig. In der Summe hat ein Eintrag in Z also 56 Byte.

Zusätzlich zu der Gesamtliste sind die Listen Z_T (Liste bereits kontaktierter intelligenter Stromzähler) und Z_B (Liste blockierter intelligenter Stromzähler) notwendig. Bei speichereffizienter Implementierung können diese als Listen von Zeigern auf Einträge in Z realisiert werden. Sie benötigen pro Eintrag also nur die Größe eines Zeigers (4 Byte bei 32-bit Architektur). Der Speicherbedarf für beide Listen ist stark vom Zufall und der Parameterkonfiguration abhängig. Die Länge von Z_T, beispielsweise, ist durch die Parameter s und t_{max} beeinflusst. Im Mittel sendet ein intelligenter Stromzähler alle $\frac{t_{max}}{2}$ ein *pair-request*, was zu einem Eintrag in Z_T führen kann. Tut er dies während der gesamten Suchdauer s, so hat Z_T für die Länge den Erwartungswert $\frac{2s}{t_{max}}$. Je nach Parameterkonfiguration sind also wenige hundert Einträge zu erwarten. Da diese Werte jedoch nur im Mittel gelten, wird für die Berechnung der schlechteste Fall angenommen. Beide Listen enthalten alle teilnehmenden intelligenten Stromzähler.

Der Gesamtspeicheraufwand ist also nach oben begrenzt durch $|Z| \times (56+4+4) = |Z| \times 64$ Bytes. Der maximale Speicheraufwand für 10 000 intelligente Stromzähler liegt damit bei 625 Kilobyte. Mit 16 Megabyte Speicher könnte ein intelligenter Stromzähler somit an einem Smart Metering mit über 250 000 intelligenten Stromzählern teilnehmen.

Durch das lineare Wachstum des Speicheraufwands in der Anzahl der teilnehmenden intelligenten Stromzähler muss dieser bei der Planung berücksichtigt werden. Doch, wie hier gezeigt, kann auch mit, nach aktuellem Stand, spärlicher Speicherausstattung eine sehr große Zahl an intelligenten Stromzählern in einem Smart Metering mit Smart Meter Speeddating verwendet werden.

6.5.4 Kommunikationsaufwand

Im Folgenden wird der Kommunikationsaufwand von Smart Meter Speeddating betrachtet. Da das Verhalten des Verfahrens stark vom Zufall abhängt, ist auch sein verursachter Kommunikationsaufwand stark vom Zufall abhängig und kann nur schwer genau abgeschätzt werden. Daher wird im Folgenden zunächst eine pessimistische Abschätzung vorgenommen um eine wahrscheinliche Obergrenze für den Kommunikationsaufwand zu bestimmen. Danach wird der im Simulator beobachtete Kommunikationsaufwand betrachtet.

Der Kommunikationsaufwand in Smart Meter Speeddating wird maßgeblich durch den Versand von Anfragen verursacht. Analog zu Abschnitt 5.5.6 enthalten diese ein SMART-ER Fragment (4 Byte), einen Identifikator (8 Byte) und einen public key authenticator (24 Byte). Also insgesamt 36 Byte. Die versendeten Antworten auf Anfragen enthalten im negativen Fall lediglich den public key authenticator (24 Byte) und ein Flag (1 Byte). Im positiven Fall enthält die Antwort zusätzlich ein Fragment.

Als absolute Obergrenze für den Versand von Anfragen kann angenommen werden, dass ein intelligenter Stromzähler für die gesamte Suchdauer (erfolglose) Anfragen verschickt. Für die daraus resultierende Anzahl an versendeten Anfragen kann aber keine sinnvolle Obergrenze angegeben werden, da die Zeit zwischen zwei Anfragen die Dauer bis zur Antwort und eine zufällige Wartezeit aus dem Intervall $[0, \ldots, t_{max}]$ umfasst. Theoretisch könnte ein intelligenter Stromzähler immer sehr kleine Werte ziehen und damit nur die Dauer bis zur eintreffenden Antwort zwischen zwei Anfragen warten. Dieses Verhalten ist allerdings extrem unwahrscheinlich und damit, selbst für eine pessimistische Abschätzung, ungeeignet. Auch kann die Dauer bis zu einer Antwort nur schlecht eingeschätzt werden. Um dennoch eine Abschätzung durchzuführen, wird die Dauer bis zur Antwort vernachlässigt, also mit 0 Sekunden abgeschätzt, und die durchschnittliche Wartezeit $\frac{t_{max}}{2}$ angenommen. Da in dieser Abschätzung für die gesamte Suchdauer s Anfragen versendet werden, sind die im Durchschnitt $\frac{2s}{t_{max}}$ Anfragen.

Als harte Obergrenze für die verschickten Antworten kann angenommen werden, dass ein intelligenter Stromzähler von allen anderen teilnehmenden Stromzähler eine Anfrage bekommen hat. Also $|Z|-1$ Anfragen, die bis auf eine alle negativ ausfallen. Dies ergibt $|Z|-2$ mal 25 Byte und ein mal 29 Byte.

Zusätzlich kommt der Versand eines maskierten Messwerts an den Messdienstleister hinzu. Dieser enthält den maskierten Messwert (4 Byte), den Identifikator (8 Byte), die Liste der Abhängigkeiten (maximal 2×8 Byte) und den public key authenticator (24 Byte). Also maximal 52 Byte.

Eine pessimistische Abschätzung für den Kommunikationsaufwand der Nutzdaten einer Smart Meter Speeddating Parameterkonfiguration lässt sich also mittels

$$\frac{2s}{t_{max}} \times 36 + 25 \times (|Z|-2) + 29 + 52 \tag{6.1}$$

berechnen. Beispielhaft sind Abschätzungen für die behandelten Parameterkonfigurationen in Tabelle 6.10 für ein Smart Metering mit $|Z| = 1\,000$ intelligenten Stromzählern aufgelistet. Da dieser Kommunikationsaufwand gleichmäßig über die gesamte Suchdauer anfallen würde, wird auch die durchschnittliche Senderate während der Suchdauer in der Tabelle aufgelistet. Bei Parameterkonfigurationen mit größerem m_{max} fällt dieser trotz höherem absoluten Kommunikationsaufwand kleiner aus. Ursache hierfür ist, dass der Aufwand über einen längeren Zeitraum, nämlich die Suchdauer s anfällt. Wie an den Werten zu erkennen ist, sind selbst die Obergrenzen für den Kommunikationsaufwand problemlos für einen handelsüblichen DSL-Anschluss machbar. Selbst das gesamte Kommunikationsaufkommen für $m_{max} = 25$ könnte mit der angenommenen Sendedatenrate innerhalb einer Sekunde versendet werden. Tatsächlich wird es nur im Verlauf von fünf Minuten versendet.

Der verursachte Kommunikationsaufwand wurde im Simulator für ein Smart Metering mit 5 000 intelligenten Stromzählern ohne Churn betrachtet. Hierfür wurden für die Simulationsläufe aus Abschnitt 6.5.1, also die Parameterkonfigurationen $m_{max} = \{5, 10, 15, 20, 25\}$, der Kommunikationsaufwand pro Messintervall als arithmetisches Mittel in Abbildung 6.17 eingezeichnet. Auch die jeweiligen 98%-Konfidenzintervalle wurden berechnet. Aufgrund der Skalierung werden sie in der Abbildung jedoch vom Symbol verdeckt. Auf der x-Achse ist die Parameterkonfiguration für m_{max} eingezeichnet, auf der y-Achse der Kommunikationsaufwand in Kilobyte. Es ist zu erkennen, dass der Kommunikationsaufwand mit größerem m_{max} auch deutlich ansteigt. Mit einem Maximalwert von ca. 14 Kilobyte ist er allerdings vernachlässigbar gering.

Tabelle 6.10: *Obergrenzen für den Kommunikationsaufwand für Smart Meter Speeddating für ein Messintervall.*

Parameter-konfiguration	Kommunikationsaufwand gesamt	Durchschnittliche Sendedatenrate während der Suchdauer
$m_{max} = 5$	37 031 Byte	2,96 kbit/s
$m_{max} = 10$	46 631 Byte	2,07 kbit/s
$m_{max} = 15$	51 431 Byte	1,87 kbit/s
$m_{max} = 20$	58 631 Byte	1,68 kbit/s
$m_{max} = 25$	63 431 Byte	1,59 kbit/s

Zusammenfassend kann geschlossen werden, dass Smart Meter Speeddating einen höheren Kommunikationsaufwand als SMART-ER für einen einzelnen intelligenten Stromzähler verursacht. Der resultierende Kommunikationsaufwand ist jedoch immer noch sehr gering und selbst für Anschlüsse mit geringen Datenraten problemlos handhabbar.

6.6 Exkurs: SMSD für Sensornetze

Im Rahmen einer Diplomarbeit von Stephan Munz [100] wurde untersucht, ob das Smart Meter Speeddating Verfahren auch für Sensornetze eingesetzt werden kann. Anlass hierfür war die Existenz eines Referenzdesigns für einen spartanisch ausgerüsteten, auf Energiesparen ausgelegten, intelligenten Stromzähler von Texas Instruments [131]. In diesem Referenzdesign wurde eine sehr ähnliche Hardwarebasis wie in Sensornetzen eingesetzt. Im Speziellen waren die zur Verfügung gestellten Speicher- und Rechenkapazitäten vergleichbar mit denen der MICAz Sensorknoten [94]. Diese stellen im Forschungsgebiet der Sensornetze eine sehr verbreitete Plattform dar. Die Eigenschaften dieser Experimentierplattform sind in Tabelle 6.11 dargestellt. Ein Sensorknoten stellt damit eine extrem ressourcenbeschränkte Hardwarebasis dar.

Als Szenario wurde in der Arbeit ein großes Mehrfamilienhaus oder Hochhaus mit entsprechend vielen Haushalten angenommen. Im Keller dieses Hauses befindet sich eine Menge von intelligenten Stromzählern, die aus einem MICAz Sensorknoten mit entsprechender Sensorik bestehen. Die intelligenten Stromzäh-

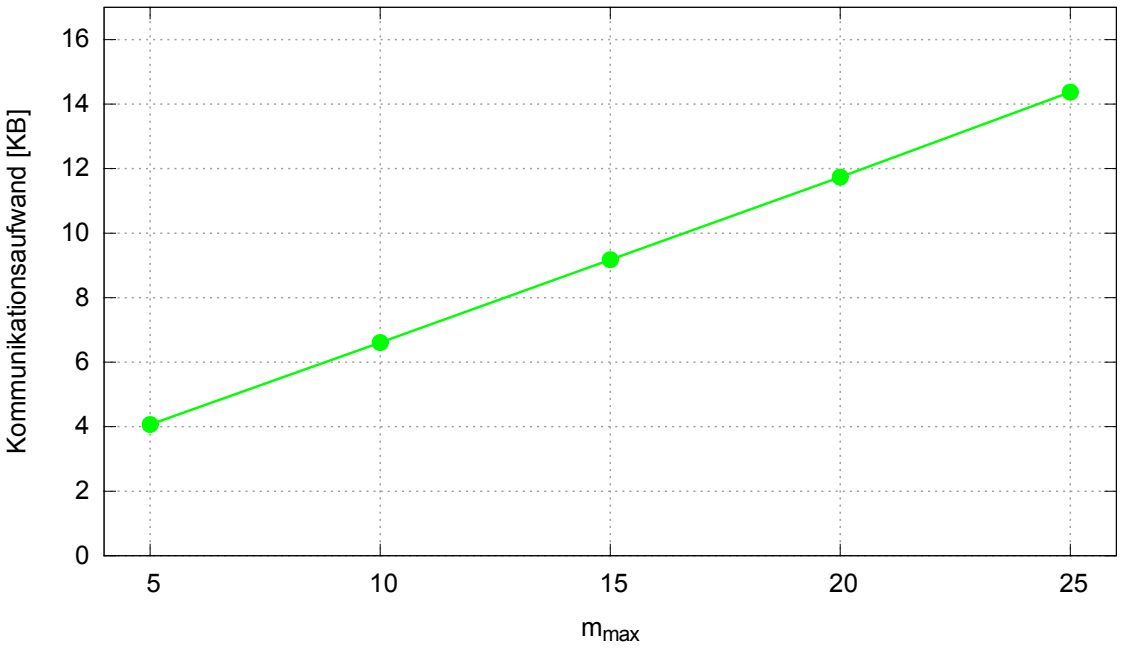


Abbildung 6.17: *Kommunikationsaufwand von Smart Meter Speeddating in Abhängigkeit von m_{max}.*

ler befinden sich alle in Funkreichweite und sollen über die Funkschnittstelle das Smart Meter Speeddating Verfahren durchführen, um einen privatsphärengerechten Abgabewert zu erhalten. Das Szenario unterscheidet sich damit deutlich vom Szenario der vorliegenden Arbeit. Die wesentlichen Punkte sind:

- **Anzahl an intelligenten Stromzählern:** Die Anzahl an intelligenten Stromzählern im Szenario für Sensornetze ist beschränkt durch die Anzahl Haushalte, die sich denselben Keller teilen. In der Arbeit wurden 32 intelligente Stromzähler und 128 intelligente Stromzähler betrachtet.
- **Drahtlose Kommunikation:** Die intelligenten Stromzähler im Szenario für Sensornetze kommunizieren über die Funkschnittstelle. Sie teilen sich damit alle ein gemeinsames Medium mit sehr geringer Bandbreite. Als Funkstandard kommt IEEE802.15.4 (ZigBee) mit einer maximalen Datentransferrate von 250 Kilobit pro Sekunde zum Einsatz.
- **Kein Churn:** Das Szenario enthielt keinen Churn. Es wurde weder ein Ausfall eines Sensorknotens noch dessen Kommunikationsfähigkeit betrachtet.

Tabelle 6.11: *Technische Daten des MICAz-Sensorknoten.*

Komponente	Technische Daten
Mikrocontroller	ATmega128L
Flashspeicher	128 KB
Ext. Flashspeicher für Messdaten	512 KB
Arbeitsspeicher	4 KB
Funkchip	CC2420
Frequenzband	2,4 GHz ISM
Taktfrequenz	7,37 MHz
Betriebsspannung	2,7V - 3,6V

Durch die Verwendung einer Funkschnittstelle sind jedoch Kollisionen beim Medienzugriff eine Quelle von Kommunikationsstörungen.

- **Keine Hardware-Kryptographie:** Auf den eingesetzten Sensorknoten war keine Unterstützung der Kryptographieoperationen durch Hardware vorhanden.

Da komplexe Kryptographieoperationen auf dem 8 Mhz Microcontroller praktisch nicht durchführbar sind, ist das SMSD Verfahren ein hervorragender Kandidat für dieses Szenario. Dennoch wird aber eine vertrauliche Kommunikation zwischen den Sensorknoten benötigt. Insbesondere, da diese sich im geänderten Szenario den gleichen Kommunikationskanal teilen. Daher wurde auf symmetrische Kryptographie zurückgegriffen und entsprechendes Schlüsselmaterial auf den Sensorknoten vorverteilt. Das Verfahren wurde im Simulator AVRORA+ [62] implementiert und evaluiert. Die wesentlichen Erkenntnisse werden hier kurz zusammengefasst:

- **Zu wenige intelligente Stromzähler:** Bei der Evaluation des Verfahrens konnte festgestellt werden, dass selbst mit einer Parametrisierung mit kleinen m_{max} und a_{max}, in Szenarien mit 32 intelligenten Stromzählern nicht alle Stromzähler einen Abgabewert erzeugen konnten. Da das SMSD Verfahren im Entwurf von einer großen Anzahl an intelligenten Stromzählern ausgeht, ist es für einen einzelnen intelligenten Stromzähler praktisch unmöglich eine Anfrage an alle anderen intelligenten Stromzähler zu senden.

Im kleineren Sensornetzszenario kann dieses jedoch auftreten. In Simulationen mit 32 intelligenten Stromzählern konnte beobachtet werden, dass einzelne intelligente Stromzähler keinen Partner finden konnten. Dies trat ein, wenn alle anderen bereits in einer Paarung waren und der betreffende intelligente Stromzähler bereits alle anderen einmal kontaktiert hatte. Entsprechend des SMSD Verfahrens durfte er daher nicht mehr angenommen werden. In der Arbeit konnte das Auftreten dieses Phänomens mittels einer Protokollanpassung um 37% reduziert werden.

- **Größeres t_{max} bei geteiltem Medium:** Der Parameter t_{max} bestimmt die maximale Wartezeit zwischen dem Versenden von zwei Suchanfragen. Senden im Sensornetzszenario sehr viele Sensorknoten zum annähernd gleichen Zeitpunkt, so kommt es zu Kollisionen beim Medienzugriff auf den Funkkanal. Diese beeinträchtigen den Verlauf des Verfahrens und können zu schlechteren Gesamtergebnissen führen. Für das Sensornetzszenario wurde daher ein t_{max} von 6 Sekunden verwendet.

Für die vorliegende Arbeit von besonderem Interesse ist die Durchführbarkeit des Verfahrens auf beschränkter Hardware. Mit nur geringfügigen Anpassungen konnten das SMSD Verfahren auf einer extrem ressourcenbeschränkten Plattform erfolgreich eingesetzt werden. Auch führte die Evaluation des Smart Meter Speeddating Verfahrens für Sensornetze zu qualitativ vergleichbaren Ergebnissen bezüglich Gruppenbildung (Abschnitt 6.4.1) und Empfindlichkeit für einen Angriff auf die Suchroutine (Abschnitt 6.4.4).

6.7 Zusammenfassung

In diesem Kapitel wurde das Smart Meter Speeddating Verfahren zur dezentralen Gruppenbildung für SMART-ER vorgestellt. Ausgehend von einer Gesamtliste der teilnehmenden intelligenten Stromzähler ermöglicht es kleine Gruppen von intelligenten Stromzählern zu bilden, ohne dass der Messdienstleister darauf Einfluss nehmen kann. Die entstehenden Gruppen werden für jedes Messintervall neu bestimmt, was eine sehr hohe Durchmischung der Gruppenzusammensetzung mit sich bringt.

Da das Smart Meter Speeddating Verfahren SMART-ER verwendet, hat es auch die gleichen Garantien bezüglich der Privatsphäre. Ein Angriff auf die Privatsphäre eines Haushalts ist nur durch den Messdienstleister möglich. Die Eigenschaften

von Smart Meter Speeddating erschweren einen Angriff jedoch deutlich. Er lässt sich, unter Einsatz von einer Vielzahl von korrumpierten Stromzählern, nur mit probabilistischem Erfolg durchführen. Zusätzlich sorgt die gute Durchmischung der Gruppenzusammensetzung zu einer guten Erkennbarkeit von Angriffen. Dies senkt die Motivation des Messdienstleisters für einen Angriff. Einzelne intelligente Stromzähler können durch eine einfache Anomalieerkennung vermutete Angriffe melden und Gegenmaßnahmen einleiten. Ein Angriff auf das Smart Meter Speeddating Verfahren ist unbemerkt also nur unter Einsatz einer sehr hohen Anzahl an korrumpierten Stromzählern möglich. Eine offene Frage jedoch ist, wem das Erkennen eines Angriffs angezeigt werden sollte. Eine naheliegende Lösung wäre eine Anzeige im betroffenen Haushalt, aber auch eine zentrale Institution zum Melden von Verstößen wäre denkbar. Diese jedoch, könnte korrumpiert werden und ein Angriff damit unentdeckt durchgeführt werden.

Die Evaluation der Smart Metering Leistung zeigt, dass Smart Meter Speeddating sehr gut skaliert und auch unter stärkerem Churn ein gutes Smart Metering Ergebnis liefert. Ein direkter Vergleich mit einem alleinigen Einsatz von SMART-ER zeigte eine gute Smart Metering Leistung bei besserem Schutz gegen Angriffe durch den Messdienstleister. Diese Ergebnisse werden mit vernachlässigbarem Kommunikations- und Rechenaufwand erzielt. Smart Meter Speeddating benötigt zwischen Messintervallen Zeit zur Bildung neuer Gruppen. Die benötigte Zeit ist jedoch deutlich unter dem anvisierten Smart Metering Intervall von 15 Minuten. Lediglich der Speicheraufwand fällt durch das Vorhalten einer Liste mit allen am Smart Metering teilnehmenden intelligenten Stromzählern und der zugehörigen Daten höher aus. Doch auch für Smart Metering Instanzen mit sehr vielen intelligenten Stromzählern ($> 100\,000$) genügen hierfür wenige Megabyte an Speicher.

Kapitel 7

Dezentrale Aggregation

Das in Kapitel 5 vorgestellte SMART-ER-Verfahren ermöglicht eine robuste, privatsphärengerechte Aggregation der Messwerte. Robustheit auch bei Kommunikationsstörungen wird bei SMART-ER durch Einteilung der intelligenten Stromzähler in Gruppen realisiert. Der Privatsphärenschutz der Gruppe (siehe Abschnitt 2.2) in SMART-ER ist abhängig von der konfigurierbaren Anzahl intelligenter Stromzähler pro Gruppe. Eine höhere Anzahl verbessert den Privatsphärenschutz der Gruppe aber verschlechtert die Robustheit. Für SMART-ER ergibt sich somit ein Zielkonflikt. Gegen einen direkten Einsatz von SMART-ER spricht auch, dass ein korrumpierter Messdienstleister korrumpierte intelligente Stromzähler in Gruppen platzieren kann. Verfügt er über genügend korrumpierte intelligente Stromzähler (Gruppengröße -1), so kann er auch den Privatsphärenschutz des Einzelnen außer Kraft setzen.

In Kapitel 6 wurde mit SMSD insbesondere der letztgenannte Punkt durch eine dezentrale Gruppenorganisation adressiert. Da es dem Messdienstleister nicht mehr möglich ist gezielt korrumpierte intelligente Stromzähler in Gruppen zu platzieren, können kleine Gruppengrößen zur Verbesserung der Robustheit eingesetzt werden. Auch der Privatsphärenschutz der Gruppe wird in SMSD durch einen regelmäßigen Wechsel der Gruppenzusammensetzung adressiert. Die dezentrale Gruppenorganisation benötigt jedoch Zeit zwischen zwei Messintervallen und kann daher nur dann eingesetzt werden, wenn zwischen zwei Messintervallen genügend Zeit (wenige Minuten) zur Verfügung steht. Außerdem erlangt der Messdienstleister in SMSD, bedingt durch die kleine Gruppengröße, für einzelne Messintervalle die aggregierten Messwerte von wenigen Haushalten. Letztlich

wächst der Speicheraufwand von SMSD linear in der Anzahl der an der Smart Metering Instanz teilnehmenden intelligenten Stromzähler. Bei besonders spärlicher Speicherausstattung der intelligenten Stromzähler könnte dies den Einsatz von SMSD bei besonders großen Smart Metering Instanzen verhindern.

Beiden bereits vorgestellten Verfahren ist gemein, dass die eigentliche Aggregation der Messwerte zentral durch den Messdienstleister vorgenommen wird. In diesem Kapitel wird das Verfahren *Elderberry* [52] vorgestellt, das eine dezentrale Aggregation mittels eines peer-to-peer Overlaynetzes realisiert. Durch die Verwendung eines Overlaynetzes kann Elderberry für wesentlich größere Smart Metering Instanzen verwendet werden. Beispielsweise wächst der Speicheraufwand nur logarithmisch in der Anzahl der teilnehmenden intelligenten Stromzähler. Damit eignet sich Elderberry auch für sehr große Smart Metering Instanzen, in denen SMSD wegen des Speicherbedarfs nicht eingesetzt werden kann.

Aufbauend auf dem SMART-ER-Verfahren realisiert Elderberry eine privatsphärengerechte Aggregation mit deutlich größerer Gruppengröße als SMSD und kann auch bei sehr kurzen Smart Metering Intervallen eingesetzt werden. Die Aggregation in Elderberry findet in mehreren Schritten dezentral, also ohne Mitwirken des Messdienstleisters, statt. Zunächst wird die Gesamtmenge der intelligenten Stromzähler in disjunkte Teilmengen, sogenannte *Abschnitte*, aufgeteilt. Diese Aufteilung kann nicht durch den Messdienstleister beeinflusst werden. In einem ersten Schritt wird, mittels SMART-ER und kleiner Gruppengröße, dezentral ein Aggregat pro solchem Abschnitt gebildet. Die Rolle des Messdienstleisters wird dabei in jedem Abschnitt von einem intelligenten Stromzähler (genannt *Abschnittorganisator*) übernommen. Der Messdienstleister erhält keine Kenntnis von diesen Aggregaten, was eine kleine Gruppengröße und damit eine gute Robustheit auch bei Kommunikationsstörungen ermöglicht[1]. Da diese abschnittweise erstellten Aggregate bereits mehrere Gruppen umfassen, ist die Privatsphäre einer Gruppe durch die große Anzahl an eingeflossenen Messwerten sehr gut geschützt. Das Aggregat kann dann direkt an den Messdienstleister übertragen werden oder mit weiteren Aggregaten, mittels der sogenannten *Overlay-Aggregation*, weiter aggregiert werden um die Anzahl Haushalte pro an den Messdienstleister gesendetem Aggregat weiter zu erhöhen. Durch diesen Ansatz erreicht Elderberry eine vergleichbare oder bessere Robustheit bei Kommunikationsstörungen als SMART-ER bei vergleichbarem Privatsphärenschutz einer Gruppe. Gleichzeitig kann der Messdienstleister nur dann

[1] Auch der Abschnittorganisator erhält nur ein maskiertes Aggregat. Wie dies erreicht wird ist in Abschnitt 7.1 und im Detail in Abschnitt 7.1.5 erläutert.

korrumpierte intelligente Stromzähler in Gruppen platzieren, wenn er über eine extrem große Anzahl verfügt.

Elderberry erreicht eine privatsphärengerechte Aggregation über eine große Anzahl an Haushalte mit vergleichbarer oder besserer Leistung als ein vergleichbar konfiguriertes SMART-ER und erreicht dabei einen wesentlich besseren Schutz gegen eine Platzierung von korrumpierten Stromzählern durch den Messdienstleister. Es stellt eine Alternative zu SMSD dar, wenn eine Aggregation über eine größere Anzahl an intelligenten Stromzählern, ein kurzes Messintervall oder eine sehr große Anzahl an insgesamt teilnehmenden intelligenten Stromzählern erwünscht ist.

Das Kapitel ist folgendermaßen strukturiert. In Abschnitt 7.1 wird das Verfahren vorgestellt. Zunächst wird eine Übersicht über das Verfahren gegeben und dann auf die einzelnen Teilaspekte eingegangen. Dann wird in Abschnitt 7.2 der Privatsphärenschutz untersucht. Es wird gezeigt, dass ein Angriff auf die Privatsphäre eines Haushaltes nur in Kooperation mit dem Messdienstleister und unter Einsatz einer großen Anzahl an intelligenten Stromzählern eine hohe Erfolgswahrscheinlichkeit haben kann. In Abschnitt 7.3 wird die Smart Metering Leistung des Verfahrens evaluiert und gezeigt, dass Elderberry, im Vergleich zu einem vergleichbar konfigurierten SMART-ER, vergleichbare oder bessere Ergebnisse liefert. Auch wird die Skalierbarkeit von Elderberry für 1 000 bis 100 000 teilnehmende intelligente Stromzähler untersucht und bestätigt. Es wird auch Rechen-, Speicher- und Kommunikationsaufwand betrachtet und geschlossen, dass diese im Vergleich zu SMART-ER zwar höher, aber immernoch problemlos realisierbar sind. Schließlich wird in Abschnitt 7.4 das Kapitel noch einmal zusammengefasst. Die in diesem Kapitel verwendeten Begriffe und Notationen sind in Tabelle 7.1 zusammengefasst.

7.1 Elderberry

Elderberry verwendet das klassische *teile und herrsche* Paradigma um Smart Metering und dezentrale Aggregation zu realisieren. Das generelle Konzept von Elderberry ist in Abbildung 7.1 illustriert. Jeder intelligente Stromzähler ist in Elderberry Teilnehmer eines strukturierten Overlaynetzes. Die im Overlaynetz zugewiesene Overlay-ID entspricht einem Punkt im Overlay-ID-Raum, auf dem der intelligente Stromzähler liegt. Die Overlay-IDs der intelligenten Stromzähler werden in Elderberry regelmäßig gewechselt. Die Dauer der Gültigkeit der Overlay-IDs wird als *Epoche* bezeichnet. Der Overlay-ID-Raum (von 0 bis $2^{160}-1$) ist in der

Tabelle 7.1: *Begriffe und Notationen.*

Begriff / Notation	Bedeutung
Overlay-ID (OID)	Identifikator eines Stromzählers im Overlaynetz.
Overlay-ID-Raum	Raum der möglichen Overlay-IDs (hier: 0 bis $2^{160}-1$).
Epoche	Zeitraum, für den die Zuordnung der Overlay-IDs gültig ist (hier: 1 Tag).
Abschnitte	Partitionierung des Overlay-ID-Raums in disjunkte Teilmengen. Wird durch Parameter A ermittelt.
Abschnitt-organisator (AO)	Rolle eines Stromzählers. Der AO repräsentiert den Messdienstleister in der Durchführung von SMART-ER pro Abschnitt.
AO-Punkt	OID innerhalb eines Abschnitts, die den AO bestimmt.
Gruppen	Partitionierung eines Abschnitts in disjunkte Teilmengen zur Durchführung von SMART-ER. Wird vom Abschnittorganisator vorgenommen.
Ende-zu-Ende-Fragmentaustausch	Austausch von SMART-ER Fragmenten zwischen Messdienstleister und jedem Stromzähler zum Schutz der Aggregation vor den Abschnittorganisatoren.
Overlay-Aggregation	Weitere Aggregation, der schon bestehenden Aggregate *bevor* diese an den Messdienstleister gesendet werden.
Aggregator (AG)	Rolle eines Stromzählers, der im Rahmen der Overlay-Aggregation Aggregate aggregiert.
Parameter: A	Anzahl an Stromzählern, die im Smart Metering geplant sind.
Parameter: O	Anzahl an Overlay-Aggregationen, die in Elderberry durchgeführt werden.
Parameter: EK	Dauer einer Epoche und Zeitstempel des Beginns der ersten Epoche.
Parameter: MK	Dauer eines Messintervalls und Zeitstempel des Beginns des ersten Messintervalls.
b	Länge des Präfixes eines Abschnitts. Bestimmt Anzahl der Abschnitte (2^b). Wird aus Parameter A ermittelt.

Abbildung am unteren Rand dargestellt. Jeder schwarze Punkt verkörpert einen intelligenten Stromzähler. Der Overlay-ID-Raum wird in sogenannte *Abschnitte* partitioniert, die mittels eines Präfixes der beinhalteten Overlay-IDs identifiziert werden können. Diese Einteilung in Abschnitte ist unabhängig vom in Elderberry verwendeten SMART-ER-Verfahren. Insbesondere ist der Begriff „Abschnitt“ vom in Elderberry verwendeten Begriff „Gruppe“ zu unterscheiden.

In jedem der, von Elderberry bestimmten, Abschnitte wird unabhängig von den anderen Abschnitten ein Smart Metering mittels des SMART-ER-Verfahrens aus Kapitel 5 durchgeführt. Die Rolle des Messdienstleisters in SMART-ER wird in jedem Abschnitt von einem intelligenten Stromzähler des Abschnitts übernommen, der im Folgenden *Abschnittorganisator (AO)* genannt wird. Der Abschnittorganisator übernimmt in Elderberry alle Aufgaben des Messdienstleisters für den Abschnitt, für den er Organisator ist. Das bedeutet, dass er die intelligenten Stromzähler seines Abschnitts zur Durchführung von SMART-ER in Gruppen einteilt. In jedem Abschnitt existiert also ein Abschnittorganisator und eine, von ihm eingeteilte, Menge von SMART-ER Gruppen.

Mittels dieser eingeteilten Gruppen wird nun das SMART-ER-Verfahren durchgeführt. Jeder intelligente Stromzähler tauscht Fragmente mit den anderen intelligenten Stromzählern seiner Gruppe aus und sendet seinen so maskierten Abgabewert an den Abschnittorganisator. Dieser aggregiert die empfangenen maskierten Abgabewerte sowie seinen eigenen Abgabewert und ermittelt somit das Aggregat des gesamten Abschnitts.

Nachdem die Abschnittorganisatoren das Ergebnis für ihren jeweiligen Abschnitt erhoben haben, können sie dieses zur sogenannten *Overlay-Aggregation* an *Aggregatoren (AG)* senden. Diese führen eine weitere Aggregation der Ergebnisse durch und senden das Aggregat an den jeweilig übergeordneten Aggregator weiter. Dieses Vorgehen wird wiederholt, bis die Wurzel oder eine konfigurierbare maximale Anzahl O an Aggregationen erreicht wurde. Die verbleibenden Aggregate werden dann an den Messdienstleister gesendet.

Um zu verhindern, dass durch den dezentralen Ansatz ein Angriff auf die Privatsphäre eines Haushalts ohne Mitwirken des Messdienstleister möglich ist, wird für jeden intelligenten Stromzähler ein Ende-zu-Ende-Fragmentaustausch mit dem Messdienstleister durchgeführt. Jeder intelligente Stromzähler fügt, zusätzlich zum Fragmentaustausch in SMART-ER, ein weiteres Fragment zu seinem Messwert hinzu. Dieses wird mittels eines kryptographisch sicheren Pseudozufallszahlengenerators generiert. Der Anfangszustand des Pseudozufallszahlengenerators ist dem Messdienstleister bekannt. Er kann somit diese Fragmente wieder aus dem

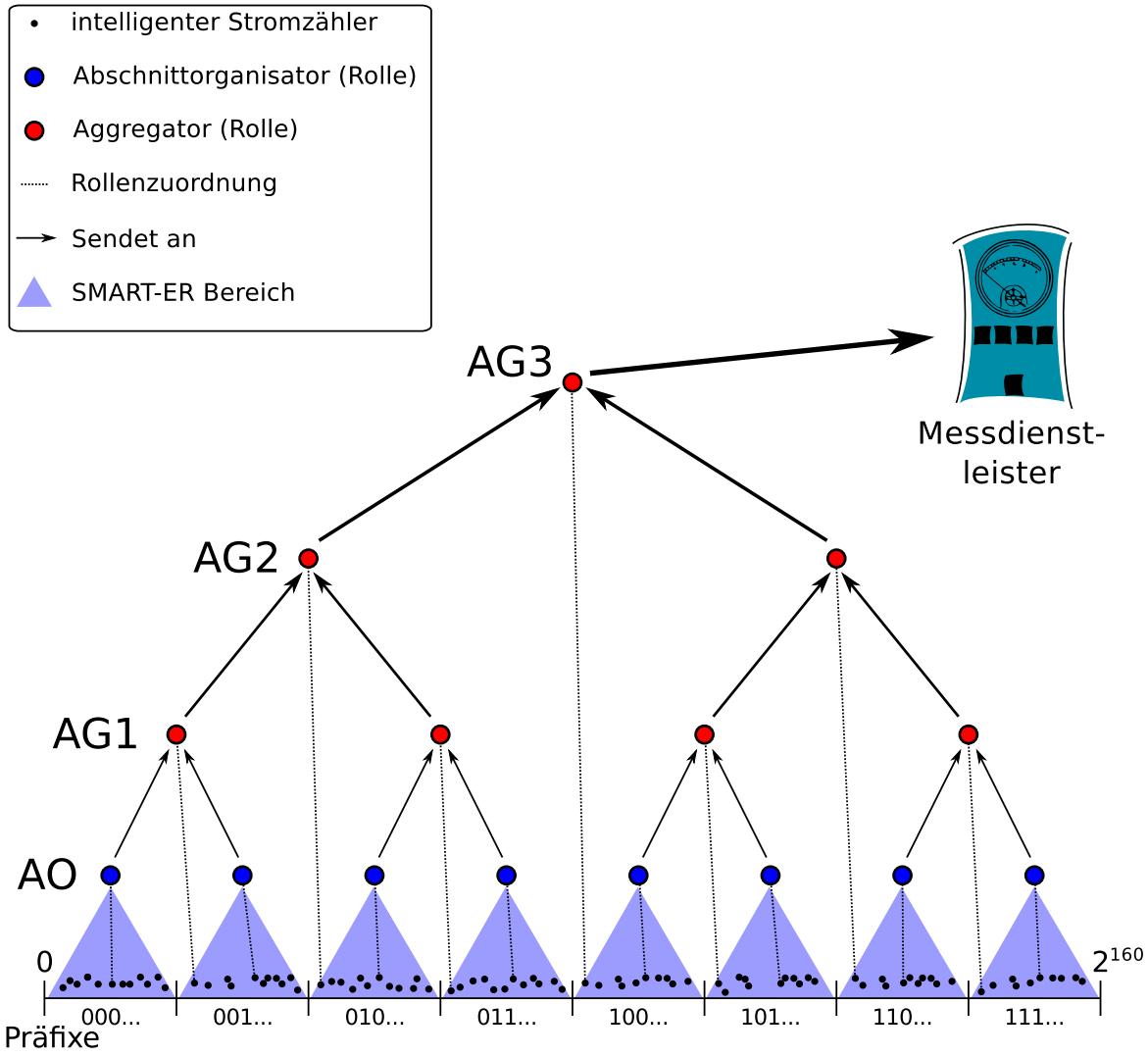


Abbildung 7.1: *Elderberry Konzept.*

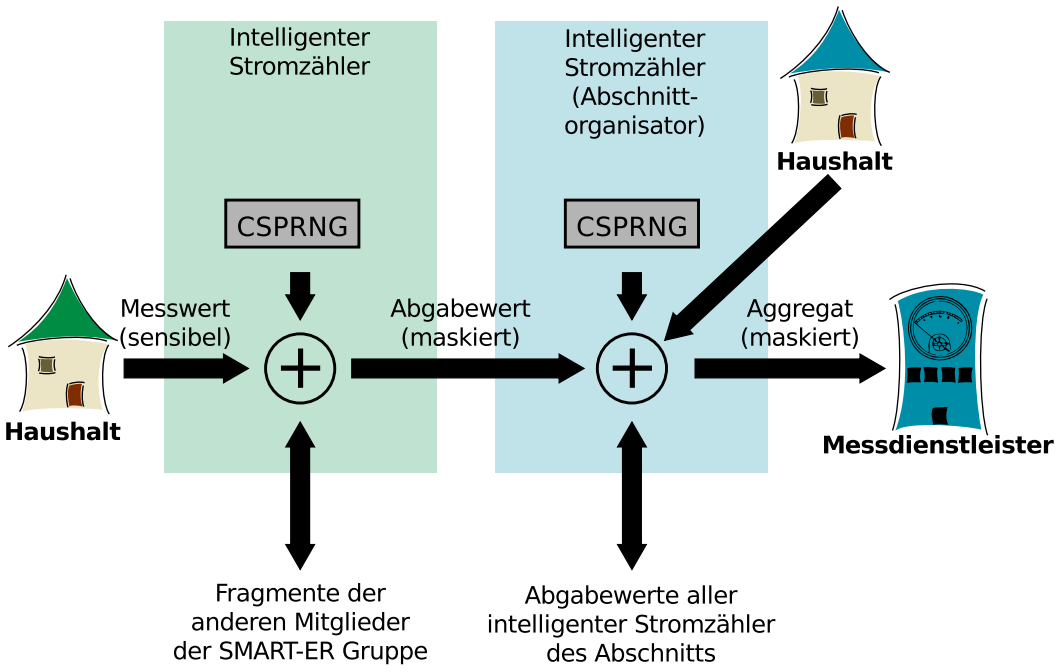


Abbildung 7.2: *Verlauf eines Messwertes während der Aggregation in Elderberry.*

Aggregat entfernen. Dies verhindert, dass der Abschnittorganisator oder ein Aggregator Informationen über die Aggregate von Messwerten oder die Messwerte selbst erlangt. Mit diesem Mechanismus wird sichergestellt, dass ein Angriff ohne Mitwirken des Messdienstleisters nicht möglich ist. Eine detaillierte Beschreibung des Mechanismus ist in Abschnitt 7.1.5 gegeben.

Die Bezeichnungen *Abschnittorganisator* und *Aggregator* sind lediglich Rollen in Elderberry. Jede dieser Rollen wird von einem intelligenten Stromzähler eingenommen. Ein regelmäßiger Wechsel der Overlay-ID im Rahmen der Epochen sorgt dafür, dass diese Rollen regelmäßig durch andere intelligente Stromzähler eingenommen werden. Auf lange Sicht wird eine ungleichmäßige Belastung einzelner intelligenter Stromzähler dadurch vermieden.

Der vereinfachte Verlauf eines Messwertes während der Aggregation in Elderberry ist schematisch in Abbildung 7.2 dargestellt. Es sind zwei intelligente Stromzähler (farbige Kästen) mit zugehörigen Haushalten zu sehen. Der grüne intelligente Stromzähler nimmt weder die Rolle eines Abschnittorganisators noch die eines Aggregators ein. Der blaue intelligente Stromzähler nimmt die Rolle eines Abschnittorganisators ein. Nachdem der grüne intelligente Stromzähler einen Messwert ermittelt hat, fügt er diesem ein Fragment hinzu, das durch einen kryp-

tographisch sicheren Pseudozufallszahlengenerator (CSPRNG) generiert wurde. Ebenfalls fließen die, mit den anderen intelligenten Stromzählern ausgetauschten, Fragmente in den Messwert ein. Der daraus entstehende Abgabewert wird an den blauen intelligenten Stromzähler, den Abschnittorganisator, gesendet. Dieser aggregiert den Abgabewert des grünen intelligenten Stromzählers mit den Abgabewerten der restlichen intelligenten Stromzähler des Abschnitts. Danach wird noch sein eigener Messwert sowie ein Fragment, das durch den CSPRNG generiert wurde, aggregiert. Das Endergebnis sendet der Abschnittorganisator dann an den Messdienstleister[2]. Da der Messdienstleister über die Anfangszustände der Pseudozufallszahlengeneratoren verfügt, kann er die eingeflossenen Fragmente aus dem Aggregat entfernen und erlangt somit ein korrektes Aggregat.

Im Folgenden werden die Details des Elderberry Verfahrens behandelt. Abschnitt 7.1.1 behandelt die Wahl des Overlaynetzes. Die Overlay-ID spielt in Elderberry eine wichtige Rolle. Wie sie für einen intelligenten Stromzähler ermittelt wird, wird in Abschnitt 7.1.2 erläutert. Die Overlay-ID wird in Elderberry in regelmäßigen Abständen, sogenannten Epochen, neu bestimmt. Das Vorgehen wird in Abschnitt 7.1.3 erläutert. In Abschnitt 7.1.4 wird behandelt, wie intelligente Stromzähler Zugang zum Overlaynetz erlangen und wie sie überprüfen können ob ein anderer intelligenter Stromzähler zugangsberechtigt ist. In Abschnitt 7.1.5 wird erläutert, wie der Ende-zu-Ende-Fragmentaustausch mit dem Messdienstleister initialisiert und verwendet wird. Wie der Overlay-ID-Raum in Abschnitte unterteilt wird, ist in Abschnitt 7.1.6 beschrieben. Die Wahl eines Abschnittorganisators innerhalb der Abschnitte wird in Abschnitt 7.1.7 behandelt. Wie abschnittsweise SMART-ER durchgeführt wird und welche Änderungen am SMART-ER Ablauf nötig sind wird in Abschnitt 7.1.8 erläutert. In Abschnitt 7.1.9 wird beschrieben, wie die Aggregation innerhalb des Overlaynetzes stattfindet bevor dann letztlich in Abschnitt 7.1.10 der zeitliche Gesamtverlauf des Verfahrens noch einmal zusammengefasst wird.

7.1.1 Overlaynetz

Das Overlaynetz wird im Entwurf von Elderberry als Dienst angesehen, der von einer unabhängigen Komponente erbracht werden kann. Da in Elderberry die Overlay-ID und der Overlay-ID-Raum als wichtiges Werkzeug dienen, muss eine effiziente Weiterleitung von Nachrichten an eine Overlay-ID gewährleistet werden.

[2]In diesem Beispiel wird keine Overlay-Aggregation durchgeführt.

Daher muss ein strukturiertes peer-to-peer Overlaynetz mit Key-based Routing verwendet werden. Dies kann beispielsweise mittels Chord [127], Kademlia [90] oder Pastry [118] realisiert werden. Insbesondere Overlaynetze, in deren Entwurf die Sicherheit der Overlay-ID-basierten Weiterleitung eine Rolle spielte, stellen gute Kandidaten dar. Als Beispiel sei hier S/Kademlia [6] genannt.

7.1.2 Bestimmung der Overlay-ID

In Elderberry wird der Overlay-ID-Raum in Abschnitte eingeteilt. Aufgrund der Overlay-ID eines intelligenten Stromzählers entscheidet sich, in welchem Abschnitt er im Overlaynetz angesiedelt wird. Die Wahl der Overlay-ID spielt damit insofern eine wichtige Rolle, dass aufgrund der gewählten Overlay-ID entschieden wird, mit welchen anderen intelligenten Stromzählern das SMART-ER Verfahren durchgeführt wird. Kann ein korrumpierter Messdienstleister korrumpierte intelligente Stromzähler im Abschnitt des Angriffsziels platzieren, so erhöht dies die Wahrscheinlichkeit eines erfolgreichen Angriffs. Daher ist die Bestimmung der Overlay-ID für die Resistenz gegen Angriffe relevant. An die Bestimmung der Overlay-ID werden folgende Anforderungen gestellt:

(1) Ein intelligenter Stromzähler kann seine eigene Overlay-ID nicht gezielt wählen. Dies verhindert, dass sich ein intelligenter Stromzähler gezielt einen Abschnitt wählen kann.

(2) Es muss jedem intelligenten Stromzähler möglich sein die Overlay-ID eines anderen intelligenten Stromzählers auf Gültigkeit zu überprüfen. Hält sich beispielsweise ein korrumpierter intelligenter Stromzähler nicht an die Vorschrift zur Bestimmung der Overlay-ID, so muss dies erkannt werden können.

(3) Overlay-IDs müssen regelmäßig gewechselt werden können. Der Zeitpunkt, für den eine Overlay-ID gültig ist wird als *Epoche* bezeichnet. Da die Anzahl intelligenter Stromzähler in einzelnen Abschnitten vom Zufall beeinflusst wird, können in Elderberry ungünstige Kombinationen auftreten. Beispielsweise können sehr weniger oder sehr viele intelligente Stromzähler in einem Abschnitt sein. Bei zu wenigen intelligenten Stromzählern kann das SMART-ER-Verfahren nicht mehr privatsphärengerecht durchgeführt werden. Bei zu vielen intelligenten Stromzählern wird der zuständige Abschnittorganisator

möglicherweise überlastet. Ein regelmäßiger Wechsel der Overlay-ID verhindert, dass ein intelligenter Stromzähler ständig von diesen ungünstigen Kombinationen betroffen ist.

(4) Die Overlay-IDs der intelligenten Stromzähler einer Epoche sollten möglichst gleichverteilt über den gesamten Zahlenraum der Overlay-IDs verteilt sein. Wie in Abschnitt 7.1.6 behandelt wird, beruht die Berechnung der Abschnittanzahl auf dieser Annahme.

Betrachtet man nur die Punkte (1) und (2), so könnte die Identität (siehe Abschnitt 2.1.4) des intelligenten Stromzählers als Overlay-ID genutzt werden. Auf diese hat ein intelligenter Stromzähler selbst keinen Einfluss, da sie bei der Produktion vom Hersteller vergeben wird. Auch kann sie im Rahmen des Identitätsnachweises einem anderen intelligenten Stromzähler bestätigt werden. Jedoch genügt sie allein nicht den Punkten (3) und (4).

Um auch den Punkten (3) und (4) zu genügen, wird die Overlay-ID *nicht allein* auf Basis der Identität eines intelligenten Stromzählers ermittelt. Stattdessen wird die Identität des Stromzähler um eine Variable v ergänzt, die für alle intelligenten Stromzähler gleichermaßen zugänglich sein muss. Das Ergebnis wird dann mittels einer kryptologischen Hashfunktion in eine Overlay-ID umgewandelt. Als Hashfunktion bietet sich beispielsweise RIPEMD-160 [35] oder SHA-1 [39] an, da die Längen der resultierenden Hashes mit 160 Bit der in Overlaynetzen häufig verwendeten Overlay-ID-Länge entsprechen. Hashfunktionen mit längeren Hashes, wie beispielsweise SHA-3 [102], können verwendet werden indem der resultierende Hash auf die Länge einer Overlay-ID gekürzt wird. Bei der Berechnung der Overlay-ID ist zu beachten, dass die Identität des Stromzählers und die Variable v gegebenenfalls um ein (der verwendeten Hashfunktion entsprechendes) Padding erweitert werden müssen bevor sie mittels der Hashfunktion in eine Overlay-ID umgewandelt werden können.

Alternativ kann dieses Vorgehen auch mit Hilfe eines HMACs [80] durchgeführt werden, wobei die Variable v als Schlüssel und die Identität des intelligenten Stromzählers als Nachricht interpretiert wird. Dies bietet sich an, da eine effiziente HMAC-Implementierung mit großer Wahrscheinlichkeit bereits in Hardware vorliegt. Der Vorteil gegenüber einem Vorgehen mittels einem einfachen Hash liegt lediglich in der möglicherweise effizienteren und fehlerfreien Implementierung in Hardware.

Um regelmäßige Wechsel zu ermöglichen, muss sich die Variable v mindestens so häufig ändern, wie regelmäßige Wechsel erwünscht sind. Dabei ist zu berück-

sichtigen, dass ein Wechsel der Overlay-IDs den Aufwand eines erneuten Beitritts zum Overlaynetz verursacht. Ein Wechsel der Overlay-ID für jedes Messintervall würde einen signifikanten Aufwand verursachen. In dieser Arbeit wird ein Wechsel der Overlay-ID einmal täglich durchgeführt. Daher genügt als Variable das aktuelle Datum.

Mit ID_z als Identität des Stromzählers z und v dem Tag, an dem das Smart Metering durchgeführt werden soll, wird die Overlay-ID (OID) mittels der kryptologischen Hashfunktion H entsprechend RFC2104 [80] bestimmt. Dabei stellt der Operator | die Konkatenation und der Operator ⊕ exklusives Oder dar. Die Konstanten opad und ipad werden zum Padding auf die Blockgröße der Hashfunktion genutzt.

$$\text{OID}_z = \text{HMAC}(v, ID_z) = H\left((v \oplus \text{opad}) | H\left((v \oplus \text{ipad}) | ID_z\right)\right) \tag{7.1}$$

Das Verfahren zur Ermittlung der Overlay-ID ist somit eng verwandt mit den Verfahren zur Erzeugung von Einmalpasswörtern (RFC4226 [98]) und zeitbasierten Einmalpasswörtern (RFC6238 [99]). Beide verwenden ebenfalls einen HMAC zur Herleitung. Bei zeitbasierten Einmalpasswörtern fließt in diesem HMAC ebenfalls ein Zeitstempel ein. Diese enthalten jeweils noch eine nachgestellte Reduzierung der Ausgabe auf wenige Byte durch eine zufällige Selektion eines Teilbereichs. Der RFC zur Erzeugung von Einmalpasswörtern enthält einen Nachweis, dass der Inhalt dieses Teilbereichs gleichverteilt ist.

Jeder intelligente Stromzähler kann somit seine OID für einen bestimmten Tag selbst bestimmen. Zusätzlich kann jeder intelligente Stromzähler die OID eines anderen intelligenten Stromzählers anhand dessen Identität bestimmen. Dies ermöglicht die Überprüfung von OIDs anderer intelligenter Stromzähler. Erbringt ein intelligenter Stromzähler im Rahmen der Kommunikation einen Identitätsnachweis (siehe Abschnitt 2.1.4), so kann seine OID vom Kommunikationspartner bestimmt und damit auch überprüft werden. Daraus folgt, dass auch ein korrumpierter intelligenter Stromzähler seine OID nicht frei wählen kann, da sie an die Identität gebunden ist.

Diese Ermittlung der Overlay-ID birgt ein sehr geringes Risiko einer Kollision von Overlay-IDs. Übliche Overlay-IDs von strukturierten Overlaynetzen haben eine Länge von 160 Bit [90]. Der dadurch entstehende Zahlenraum für Overlay-IDs ist extrem groß und Kollisionen damit extrem unwahrscheinlich. Sollte dennoch eine Kollision auftreten, also die OIDs der intelligenten Stromzähler z_1 und z_2 innerhalb einer Epoche gleich sein, so wird diese im Overlaynetz erkannt und die

beiden intelligenten Stromzähler können anhand ihrer Identität unterschieden werden. In diesem Fall muss eine Kollisionsauflösung durchgeführt werden. Die Ermittlung einer alternativen Overlay-ID im Fall einer Kollision wäre problematisch, da ein dritter intelligenter Stromzähler die Kollision nur schlecht oder gar nicht nachvollziehen kann. Zur Kollisionsauflösung wird daher vorgeschlagen, dass sich der intelligente Stromzähler mit der numerisch kleineren Identität vom Smart Metering für diese Epoche (hier ein Tag) zurückzieht.

7.1.3 Vorgehen bei Epochenwechsel

Wie im vorherigen Abschnitt motiviert, sind Overlay-IDs in Elderberry immer nur für eine gewisse Zeit, eine sogenannte *Epoche*, gültig. Zum Wechseln der Overlay-IDs am Ende einer Epoche wird parallel zum bestehenden Overlaynetz kurz vor Ende der Epoche ein zweites Overlaynetz aufgebaut. Die intelligenten Stromzähler sind dann für kurze Zeit in zwei Overlaynetzen mit unterschiedlichen Overlay-IDs vertreten. Das neue Overlaynetz wird erst mit Beginn des ersten Messintervalls der nächsten Epoche genutzt. Ab diesem Zeitpunkt wird die Verwendung des alten Overlaynetzes eingestellt.

Durch dieses Vorgehen wird ein nahtloser Übergang zwischen Epochen gewährleistet. Dabei können Informationen aus dem bestehenden Overlaynetz (beispielsweise die IP-Adressen und Identitäten bekannter intelligenter Stromzähler) zur effizienteren Etablierung des neuen Overlaynetzes genutzt werden.

7.1.4 Zugang zum Overlaynetz

Ein intelligenter Stromzähler z wird vom Messdienstleister für die Teilnahme an einem Smart Metering konfiguriert. Hierzu wird ihm eine Konfiguration K zum Smart Metering übermittelt, die folgende Daten enthält:

- Die Epochenkonfiguration EK: Dauer einer Epoche und Zeitstempel des Beginns der ersten Epoche.
- Die Konfiguration der Messintervalle MK: Dauer eines Messintervalls und Zeitstempel des Beginns des ersten Messintervalls.
- Die Anzahl der am Smart Metering teilnehmenden intelligenten Stromzähler A.
- Die Anzahl an durchzuführenden Overlay-Aggregationen O.

Zusätzlich erhält der intelligente Stromzähler eine Signatur des Messdienstleisters über die gesamte Konfiguration konkateniert mit seiner Identität ID_z. Diese Signatur $ZB_z = Sig_{MD}(K|ID_z)$ stellt die Zugangsberechtigung für den intelligenten Stromzähler z dar.

Mittels ZB_z kann sich ein intelligenter Stromzähler gegenüber anderen intelligenten Stromzählern als berechtigt ausweisen. Dafür wäre prinzipiell eine Signatur der Identität bereits ausreichend. Um aber zu verhindern, dass der Messdienstleister verschiedene Konfigurationen des Smart Meterings an verschiedene intelligente Stromzähler herausgeben kann, erstreckt sich die Signatur auch über die Konfiguration. Möchte sich nun ein intelligenter Stromzähler z_1 gegenüber einem anderen intelligenten Stromzähler z_2 ausweisen, so überträgt er lediglich seine Identität, deren Nachweis und ZB_{z_1}. Die Konfiguration K kennt z_2 bereits und kann daher ZB_{z_1} nur mittels ID_{z_1} überprüfen.

Die Anzahl der teilnehmenden intelligenten Stromzähler A in K stellt die Anzahl der *geplanten* teilnehmenden intelligenten Stromzähler dar und nicht die Anzahl, die gerade aktuell ist. Diese kann, beispielsweise durch Einfluss von Churn, variieren. Die Anzahl A ist also ein, durch den Messdienstleister, konfigurierter Parameter des Verfahrens. Mittels A wird die Berechnung der Abschnittanzahl (siehe Abschnitt 7.1.6) durchgeführt.

Um initial dem Overlaynetz beizutreten benötigt ein intelligenter Stromzähler die Möglichkeit Kontakt mit mindestens einem, bereits beigetretenen, intelligenten Stromzähler aufzunehmen. Dieser kann vom Messdienstleister hergestellt werden.

7.1.5 Initialisierung und Verwendung des Ende-zu-Ende-Fragmentaustauschs

Um zu verhindern, dass im Rahmen der dezentralen Aggregation Angriffe ohne Mitwirken des Messdienstleisters möglich sind, wird in Elderberry ein Ende-zu-Ende-Fragmentaustausch zwischen intelligenten Stromzählern und Messdienstleister vorgenommen.

Der Grundgedanke hinter dem Ende-zu-Ende-Fragmentaustausch ist, dass jeder intelligente Stromzähler pro Messintervall einen zusätzlichen Fragmentaustausch mit dem Messdienstleister vornimmt. Es wird pro Messintervall ein Fragment bestimmt, dass der intelligente Stromzähler seinem Messwert hinzufügt. Dadurch wird jeder Messwert zusätzlich maskiert. Die Funktionalität der dezentralen Aggregation wird nicht beeinflusst. Die Aggregate, die ein Abschnittorganisator bildet,

sind jedoch ohne Aussagekraft, da die eingeflossenen Messwerte zusätzlich maskiert wurden und diese Maskierung dem Abschnittorganisator nicht bekannt ist. Ohne Mitwirken des Messdienstleisters können also auch im Rahmen der dezentralen Aggregation keine Messwerte oder Aggregate von Messwerten ermittelt werden.

Der Messdienstleister erhält als Ergebnis des Smart Meterings ein oder mehrere so maskierte Aggregate und eine Liste der intelligenten Stromzähler, die zu dem jeweiligen Aggregat beigetragen haben. Um die Maskierung aufzuheben muss er lediglich für jeden intelligenten Stromzähler der Liste das passende Fragment aus dem Aggregat entfernen.

Um zu Vermeiden, dass in jedem Messintervall jeder intelligente Stromzähler mit dem Messdienstleister kommunizieren muss, wird kein tatsächlicher Fragmentaustausch vorgenommen. Stattdessen wird im Rahmen der Konfiguration eines intelligenten Stromzählers (siehe Abschnitt 7.1.4) ein kryptographisch sicherer Pseudozufallszahlengenerator mit einem Wert initialisiert. Hierfür kann beispielsweise AES im Counter-Mode [77] zum Einsatz kommen. Mit Hilfe des Pseudozufallszahlengenerators generiert der intelligente Stromzähler für jedes Messintervall ein Fragment und erhöht dann den Counter. Der Messdienstleister muss lediglich pro intelligentem Stromzähler den Initialisierungszeitpunkt und den initialen Wert vorhalten. Er kann dann für jedes Messintervall das Fragment unabhängig vom intelligenten Stromzähler berechnen und, sofern der intelligente Stromzähler zum Aggregat beigetragen hat, vom Aggregat abziehen.

7.1.6 Berechnung der Abschnittanzahl

Ein zentrales Element in Elderberry stellt die Einteilung des Overlay-ID-Raums in Abschnitte dar. Hierfür muss eine Berechnung der Abschnittanzahl durchgeführt werden. Sie wird von jedem intelligenten Stromzähler mittels der konfigurierten Anzahl der teilnehmenden intelligenten Stromzähler A berechnet. Die Anzahl an Abschnitten bleibt während des Smart Meterings, also insbesondere für mehrere Epochen, gleich. Die Abschnittanzahl muss so bestimmt werden, dass

(1) in jedem Abschnitt genügend intelligente Stromzähler für einen wirksamen Privatsphärenschutz vorhanden sind.

(2) in jedem Abschnitt nur so viele intelligente Stromzähler sind, dass der zuständige Abschnittorganisator nicht überlastet wird.

Falls (1) für einen Abschnitt nicht erfüllt ist, wird in diesem Abschnitt kein Smart Metering durchgeführt. Dementsprechend fehlen die intelligenten Stromzähler des Abschnitts im Gesamtergebnis. Wenn (2) nicht erfüllt ist, so kommt es ebenfalls zu einer verringerten Smart Metering Leistung. Wird eine der Anforderungen nicht erfüllt, so hat dies nur für die Dauer eine Epoche Auswirkungen. Danach werden die Overlay-IDs neu berechnet und damit ändert sich auch die Zusammensetzungen der Abschnitte. Durch den dezentralen Ansatz von Elderberry wirken sich Störungen in einzelnen Abschnitten nicht auf andere Abschnitte aus.

Zu (1) wurde in Kapitel 5 gezeigt, dass im SMART-ER Verfahren die Privatsphäre des Einzelnen bereits dann geschützt ist, wenn mindestens ein kooperierender intelligenter Stromzähler nicht korrumpiert ist. Der Abschnittorganisator ist in Elderberry in der Rolle des Messdienstleisters. Er nimmt nicht am Fragmentaustausch von SMART-ER teil, sondern organisiert diesen indem er die intelligenten Stromzähler für SMART-ER in Gruppen einteilt und das Aggregat aller intelligenter Stromzähler des Abschnitts mittels der Abgabewerte berechnet. Seinen eigenen (mittels Pseudozufallszahlengenerator maskierten) Messwert aggregiert der Abschnittorganisator mit dem Aggregat der intelligenten Stromzähler des Abschnitts. Um einen Schutz der Privatsphäre des Einzelnen zu ermöglichen müssen also mindestens drei intelligente Stromzähler pro Abschnitt vorhanden sein: ein Abschnittorganisator und ein zwei intelligente Stromzähler. Für (1) sind also Gruppen von mindestens drei intelligenten Stromzählern nötig. Sehr große Gruppen stellen allerdings ein Problem für (2) dar. Der Abschnittorganisator wird durch einen normalen intelligenten Stromzähler realisiert und muss daher auch mit dessen begrenzten Ressourcen arbeiten: geringe Rechenkapazität, geringe Speicherkapazität, niedrige Sendedatenraten der Kommunikationsanbindung und deren Unzuverlässigkeit (Churn).

Die niedrige Sendedatenrate stellt einen limitierenden Faktor für die maximale Anzahl intelligenter Stromzähler pro Abschnitt dar. Im Verlauf von Elderberry muss ein Abschnittorganisator eine Liste der jeweiligen Gruppenmitglieder an alle intelligenten Stromzähler in seinem Abschnitt senden. Dies verursacht beim Abschnittorganisator ein zu sendendes Datenvolumen, das von der Anzahl der Einträge in jeder Liste abhängt. Diese Anzahl hängt von der konfigurierten SMART-ER Gruppengröße ab. Sie ist mindestens so groß, wie die konfigurierte Gruppengröße[3].

[3] Die genaue Anzahl Einträge liegt geringfügig höher, da bei der Einteilung in Gruppen überzählige intelligente Stromzähler auf die Gruppen aufgeteilt werden. Siehe Abschnitt 7.1.8.

Daher sollte die Anzahl intelligenter Stromzähler pro Abschnitt nach oben limitiert sein.

Ebenfalls stellt die Unzuverlässigkeit der Kommunikationsanbindung des Abschnittorganisators einen limitierenden Faktor dar. Der Abschnittorganisator nimmt für die intelligenten Stromzähler des Abschnitts die Rolle des Messdienstleisters ein. Damit hat er, innerhalb seines Abschnitts, eine zentrale Rolle. Fällt er zu einem ungünstigen Zeitpunkt aus, so wird die Präzision des Smart Metering Ergebnis negativ beeinflusst. Fällt er beispielsweise nach Durchführung von SMART-ER, aber vor der Weitergabe des Aggregats an den Aggregationsmechanismus aus, so fehlt im Smart Metering Ergebnis der gesamte Abschnitt. Auch aus diesem Grund sollte die Anzahl intelligenter Stromzähler pro Abschnitt nach oben limitiert sein.

Um den Kommunikationsaufwand für Abschnittorganisatoren und die Konsequenzen einer Störung eines Abschnittorganisators in Grenzen zu halten, wurde im Folgenden eine durchschnittliche Gruppengröße von 50 intelligenten Stromzählern anvisiert. Dieser Wert wurde aus folgenden Gründen gewählt:

- In einem Abschnitt mit 50 intelligenten Stromzählern ist das Datenvolumen der Nutzdaten niedrig genug um die Kommunikationsanbindung des Abschnittorganisators nicht zu überlasten. Bei einer vollständigen Ausnutzung der theoretisch zur Verfügung stehenden Datenrate (siehe Abschnitt 5.1) ließe es sich in deutlich unter einer Sekunde übertragbar.

- Der Speicheraufwand des Abschnittorganisators für 50 intelligente Stromzähler ist vernachlässigbar gering.

- Der Abschnittorganisator muss die Abhängigkeitsauflösung von SMART-ER durchführen. Doch selbst auf sehr beschränkter Hardware können die Abhängigkeiten von 50 intelligenten Stromzählern in kürzester Zeit aufgelöst werden.

Ein Wert von 50 ist somit für alle Einschränkungen des Abschnittorganisators geeignet.

Die Abschnitte in Elderberry werden durch die Festlegung einer Präfixlänge b gebildet. Damit entspricht die Anzahl an Abschnitten 2^b. Ausgehend von der Annahme der Gleichverteilung der Overlay-IDs der intelligenten Stromzähler (siehe Abschnitt 7.1.2) und der anvisierten Anzahl von 50 Stromzählern pro Abschnitt, kann b in Abhängigkeit der konfigurierten Anzahl an teilnehmenden Stromzählern A wie folgt berechnet werden:

$$b = \left\lfloor log_2\left(\frac{A}{50}\right)\right\rfloor \tag{7.2}$$

Das Abrunden zum nächstniedrigeren Ganzzahlwert sorgt hier für ein kleineres b. Das bedeutet, dass eine geringere Anzahl an Abschnitten gebildet wird und damit eine höhere durchschnittliche Anzahl an intelligenten Stromzählern pro Abschnitt folgt.

Um die Wahl der Präfixlänge beurteilen zu können, wurden für eine gegebene Anzahl an teilnehmenden intelligenten Stromzählern zwei Wahrscheinlichkeiten unter Annahme der Gleichverteilung der Overlay-IDs berechnet:

- Die Wahrscheinlichkeit, dass kein Abschnitt mit weniger als drei intelligenten Stromzählern existiert. Da dies die Mindestanzahl für einen funktionsfähigen Privatsphärenschutz darstellt (zwei intelligente Stromzähler als SMART-ER Gruppe und ein intelligenter Stromzähler als Abschnittorganisator), ist dies die Wahrscheinlichkeit, dass in allen Abschnitten ein funktionsfähiger Privatsphärenschutz realisiert werden kann.

- Die Wahrscheinlichkeit, dass alle Abschnitte mindestens fünf, aber maximal 100 intelligente Stromzähler enthalten. Dies entspricht dem Wunschbereich: ein kleiner Sicherheitsabstand zum Minimum für den Privatsphärenschutz und dem doppelten der anvisierten durchschnittlichen Anzahl zur Schonung der Abschnittorganisatoren.

Die Wahrscheinlichkeiten sind in Abbildung 7.3 aufgezeichnet. Für die Anzahl intelligenter Stromzähler wurden Werte von 1 000 bis zu einer Million verwendet. Auf der x-Achse ist die Anzahl der teilnehmenden intelligenten Stromzähler und auf der y-Achse sind die Wahrscheinlichkeiten in Prozent aufgetragen. Die Wahrscheinlichkeit dafür, dass alle Abschnitte mindestens fünf und maximal 100 intelligente Stromzähler enthalten ist in rot eingezeichnet. Die Wahrscheinlichkeit dafür, dass kein Abschnitt weniger als drei intelligente Stromzähler enthält ist in grün eingezeichnet. Beide Wahrscheinlichkeiten sind für den Großteil des betrachteten Bereichs sehr nahe an 100%. Jedoch immer dann, wenn eine Verlängerung des Abschnittpräfixes durchgeführt wird, führt dies auch zu einer Reduktion der Wahrscheinlichkeiten. Dies ist besonders bei der Wahrscheinlichkeit für den Wunschbereich zu erkennen. Betrachtet man den Wechsel von Präfixlänge 13 zu Präfixlänge 14 bei 819 200 intelligenten Stromzählern, so reduziert sich die

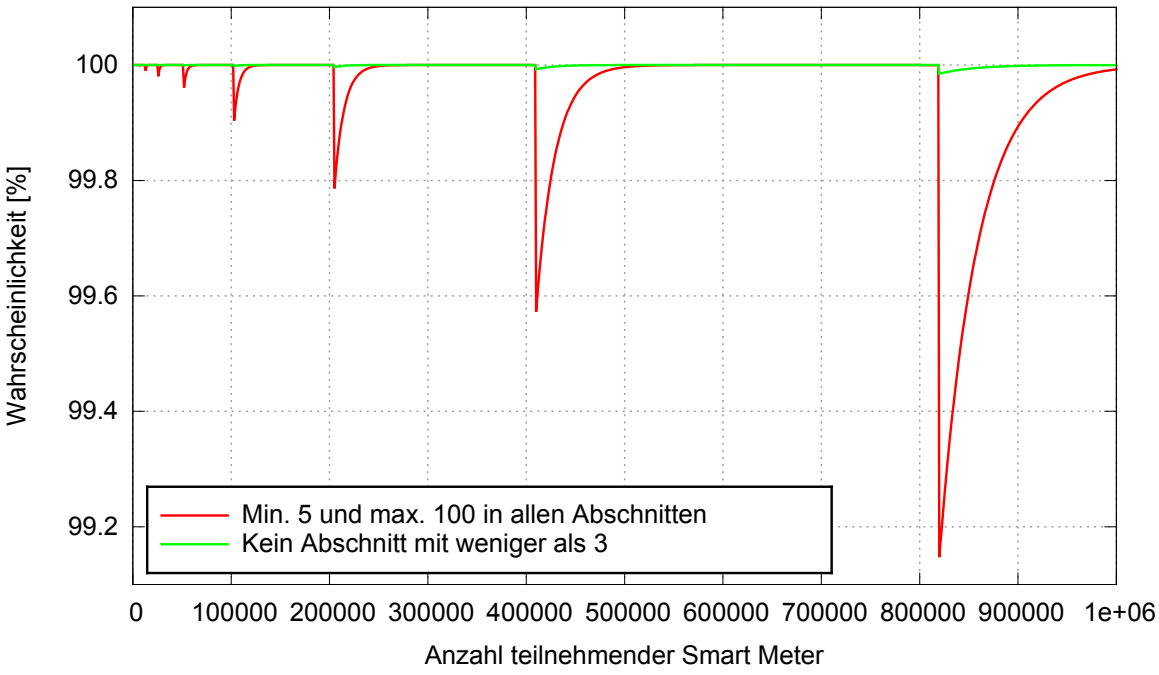


Abbildung 7.3: *Wahrscheinlichkeiten für Abschnittbelegungen.*

Wahrscheinlichkeit, dass alle Abschnitte mindestens fünf und maximal 100 intelligente Stromzähler enthalten auf circa 99, 13%. Die Wahrscheinlichkeit, dass kein Abschnitt mit weniger als drei intelligenten Stromzählern entsteht reduziert sich ebenfalls. Die Reduktion fällt mit gerundeten 99, 98% jedoch wesentlich weniger stark aus als die des Wunschbereichs.

Diese Wahrscheinlichkeiten sind im Kontext der Epochenlänge zu interpretieren, da zu Beginn der Epoche die Abschnitte eingeteilt werden und diese ihre Gültigkeit für die Dauer der Epoche behalten. Wird beispielsweise eine Epochenlänge von einem Tag gewählt, so besteht an jedem Tag die Wahrscheinlichkeit von 0, 87%, dass nicht alle Abschnitte dem Wunschbereich entsprechen. Innerhalb eines Jahres ist also an drei Tagen mit diesem Ereignis zu rechnen. Die Wahrscheinlichkeit, dass tatsächlich ein Abschnitt zu wenige intelligente Stromzähler enthält um privatsphärengerecht am Smart Metering teilzunehmen ist wesentlich geringer. Dieser Fall tritt im Durchschnitt alle 6 500 Tage ein. Dies entspricht ungefähr 17 Jahren und 9 Monaten. Da dies die Zahlen für den schlechtesten abgebildeten Fall sind, ist das Ausfallrisiko vernachlässigbar.

Dass die Wahrscheinlichkeit des Einhaltens des Wunschbereichs beim Wechsel der Präfixlänge einen Sprung nach unten macht deutet auf zu spärlich besetzte Abschnitte hin. Daher wurde eine alternative Berechnung der Präfixlänge untersucht. Hierzu wurde der Wechsel der Präfixlänge erst bei einer größeren Anzahl an intelligenten Stromzählern durchgeführt:

$$b = \left\lfloor log_2 \left(\frac{A - \frac{A}{10}}{50} \right) \right\rfloor \tag{7.3}$$

Die besprochenen Wahrscheinlichkeiten sind für die neue Präfixlängenberechnung in Abbildung 7.4 dargestellt. Die Wahrscheinlichkeit für einen Abschnitt mit zu wenigen intelligenten Stromzählern ist erwartungsgemäß geringer. Für den letzten in der Abbildung dargestellten Wechsel der Präfixlänge bei 910 222 intelligenten Stromzählern und bei einer Epochenlänge von einem Tag ist dieser Fall nun alle 85 280 Tage, also ungefähr alle 233 Jahre, zu erwarten. Betrachtet man die Wahrscheinlichkeit dafür, dass alle Abschnitte dem Wunschbereich entsprechen, so ist auch diese deutlich verbessert. Anhand der Abbildung ist zu erkennen, dass nun bereits beim Annähern der Grenze zur Verlängerung des Abschnittpräfixes eine Reduzierung der Wahrscheinlichkeit eintritt. Dies ist auf die größere Anzahl an intelligenten Stromzählern pro Abschnitt zurückzuführen. Betrachtet man wieder den letzten Wechsel des Präfixes in der Abbildung, so sinkt die Wahrscheinlichkeit nur noch auf circa 99, 92%. Selbst im schlechtesten Fall und bei sehr vielen teilnehmenden intelligenten Stromzählern sind Abschnitte, die nicht dem Wunschbereich entsprechen sehr selten. Abschnitte, die aufgrund ihrer geringen Zahl an intelligenten Stromzählern kein privatsphärengerechtes Smart Metering durchführen können sind extrem selten.

Für die weitere Evaluation wurde aufgrund der höheren Wahrscheinlichkeiten die Präfixlängenberechnung aus Formel 7.3 verwendet.

7.1.7 Bestimmung des Abschnittorganisators

Jeder Abschnitt enthält eine Anzahl von intelligenten Stromzählern von denen einer die Rolle des Messdienstleisters einnimmt. Der Abschnittorganisator wird in Elderberry bestimmt, indem innerhalb des Abschnitts eine Punkt im Overlay-ID-Raum berechnet wird, der sich in der Mitte des Abschnitts befindet. Der intelligente Zähler, der im Overlaynetz mittels des Key-based Routings für diesen Punkt verantwortlich ist, wird Abschnittorganisator.

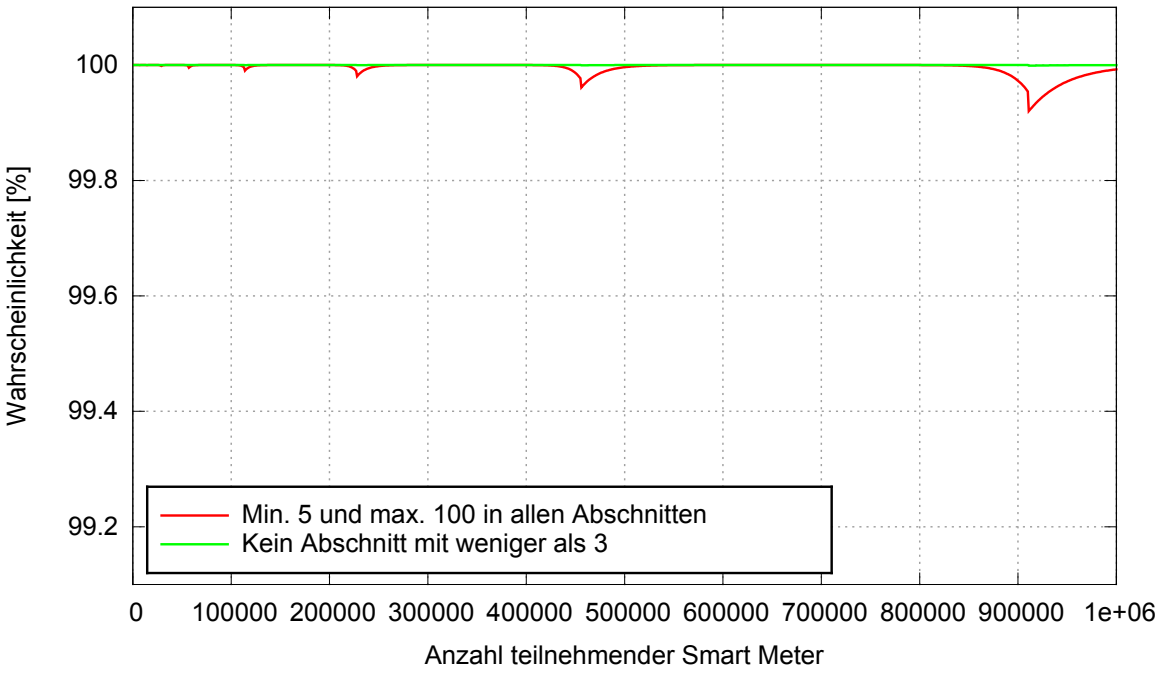


Abbildung 7.4: *Wahrscheinlichkeiten für Abschnittbelegungen bei neuer Präfixlängenberechnung.*

Dieser Punkt kann von jedem intelligenter Stromzähler z mittels seiner Overlay-ID OID_z und der Präfixlänge b berechnet werden. In der folgenden Formel stellt der Operator $\wedge$ die bitweise Und-Verknüpfung dar, $\vee$ die bitweise Oder-Verknüpfung. Die Länge der Overlay-IDs wird mit l abgekürzt. Im Exponenten steht jeweils, wie häufig das Bit wiederholt wird.

$$\text{AO-Punkt} = \left(\left(OID_z \wedge 1^b 0^{l-b}\right) \vee 0^b 10^{l-b-1}\right) \tag{7.4}$$

Das eigene Präfix wird mittels eines Filters, der Präfixlänge b Einsen und sonst Nullen enthält, aus der eigenen OID ermittelt. Daraufhin wird das $b+1$-te Bit auf 1 gesetzt.

Ist z für den AO-Punkt zuständig, so ist z der Abschnittorganisator. Andernfalls kann z den Abschnittorganisator kontaktieren, indem eine Nachricht an die Overlay-ID AO-Punkt durch das Overlaynetz geroutet wird.

7.1.8 Abschnittsweise Durchführung von SMART-ER

Innerhalb der Abschnitte wird SMART-ER, wie es in Kapitel 5 beschrieben ist, durchgeführt. Es muss jedoch geringfügig angepasst werden, da ein Abschnittorganisator initial nicht über dieselben Daten verfügt wie ein Messdienstleister.

Der Abschnittorganisator benötigt für die SMART-ER Gruppeneinteilung eine vollständige Liste der intelligenten Stromzähler in seinem Abschnitt. Daher meldet sich jeder intelligente Stromzähler *vor* Beginn des SMART-ER Verfahrens bei seinem zuständigen AO mittels einer Registrierungsnachricht an. Da zu diesem Zeitpunkt weder die Overlay-ID des AO noch die IP-Adresse des AO bekannt sind, wird diese Registrierungsnachricht durch das Overlaynetz an die Overlay-ID des AO-Punkts geroutet. Die Registrierungsnachricht enthält die IP-Adresse des sich registrierenden intelligenten Stromzählers. Somit kann die Antwort des AO direkt, anstatt über das Overlaynetz, versendet werden.

Nachdem alle intelligenten Stromzähler beim AO registriert sind, teilt dieser die Stromzähler zufällig in Gruppen ein. Die Anzahl der Gruppen richtet sich dabei nach der in SMART-ER konfigurierten Gruppengröße. Überzählige intelligente Stromzähler werden gleichmäßig auf die Gruppen verteilt. Der AO versendet dann an jeden intelligenten Stromzähler im Abschnitt die jeweilige Gruppe.

Danach kann SMART-ER wie in Kapitel 5 geschildert durchgeführt werden. Der AO übernimmt dabei alle Aufgaben des Messdienstleisters. Nachdem SMART-ER durchgeführt wurde, verfügt der AO über das Aggregat der intelligenten Stromzähler des Abschnitts. Er fügt noch seinen eigenen Messwert hinzu und reicht das Ergebnis dann an die Aggregationskomponente weiter.

7.1.9 Overlay-Aggregation

Wie beschrieben wird in Elderberry abschnittsweise SMART-ER durchgeführt. Das Ergebnis sind privatsphärengerecht aggregierte Messwerte der intelligenten Stromzähler eines jeden Abschnitts. Damit verfügen nach der Durchführung von SMART-ER 2^b AOs über aggregierte Messwerte die jeweils über circa 50 intelligente Stromzähler gebildet wurden (siehe Abschnitt 7.1.6). Diese bereits aggregierten Messwerte können in Elderberry mittels der Overlay-Aggregation weiter aggregiert werden. Wie häufig diese durchgeführt wird ist vom Messdienstleister mittels des Parameters O konfiguriert.

Durch die Overlay-Aggregation reduziert sich die Anzahl Nachrichten, die an den Messdienstleister gesendet werden. Das Volumen der Nutzdaten wird jedoch

nur geringfügig verringert, da es hauptsächlich aus der Liste der beteiligten intelligenten Stromzähler besteht. Werden beispielsweise zwei Ergebnisse aus SMART-ER aggregiert, so enthalten diese jeweils einen aggregierten Messwert und jeweils eine Liste von circa 50 Identitäten intelligenter Stromzähler. Das resultierende Aggregat enthält einen aggregierten Messwert (die Summe) und die Vereinigung der beiden Listen.

Die Overlay-Aggregation dient jedoch nicht nur der Reduktion der eintreffenden Nachrichten beim Messdienstleister, sondern erhöht zusätzlich den Privatsphärenschutz. Sendet jeder AO sofort und direkt an den Messdienstleister, so kann der Messdienstleister Profile pro Epoche pro Abschnitt erstellen. Die Anzahl intelligenter Stromzähler pro Abschnitt wurde in Abschnitt 7.1.6 so gewählt, dass bereits von einem wirksamen Privatsphärenschutz ausgegangen werden kann. Mittels der Aggregation im Overlaynetz kann noch eine weitere Verbesserung erreicht werden.

Zur Overlay-Aggregation nutzt Elderberry einen Aggregationsbaum, der auf der Struktur der Overlay-IDs aufgebaut ist. Jeder Knoten in diesem Binärbaum entspricht einer Overlay-ID. An der Wurzel steht die Mitte der Overlay-IDs. Die Kinder der Wurzel halbieren jeweils den Overlay-ID-Raum (siehe Abbildung 7.1). Dies setzt sich rekursiv fort, bis der Baum die Höhe b erreicht. Dadurch hat der Baum 2^{b-1} Blätter, also genau halb so viele Blätter wie es Abschnitte gibt. Jedes Blatt ist somit für genau zwei Abschnitte zuständig.

Jeder intelligente Stromzähler kann diesen Binärbaum selbständig mittels b herleiten. Das Ergebnis sind Punkte im Overlay-ID-Raum, an denen sich der jeweilige Baumknoten befindet. Mittels einer Nachricht an einen entsprechenden Punkt, kann der jeweils dafür zuständige intelligente Stromzähler aufgefunden werden.

Die Aggregation findet in Elderberry in Intervallen nach der Durchführung des SMART-ER Verfahrens statt. Ist der Protokollparameter $O = 0$, so wird keine Overlay-Aggregation durchgeführt. Jeder AO sendet die Ergebnisse des SMART-ER Verfahrens direkt an den Messdienstleister. Andernfalls schließt sich an das SMART-ER Verfahren eine Reihe von Overlay-Aggregationen $\{o_1, \ldots, o_O\}$ an. Zu Beginn jeder Overlay-Aggregation bestimmt *jeder* intelligente Stromzähler ob ihm Daten zur Aggregation vorliegen. Ist dies der Fall, so bestimmt er den für ihn zuständigen Aggregator dieser Overlay-Aggregation und sendet diesem die Messwerte zu. Das bedeutet, dass in o_1 jeder AO den für seinen Abschnitt zuständigen Aggregator ermittelt und seine Messwerte an diesen sendet. Diese entsprechen

den Blattknoten im Binärbaum. In der letzten Overlay-Aggregation werden die vorliegenden Messwerte dann direkt an den Messdienstleister gesendet.

Das generische Vorgehen ist hier nötig, da die Overlay-Aggregation Rücksicht auf sich ändernde Zuständigkeiten im Overlaynetz nehmen muss. Bei den Aggregatoren handelt es sich lediglich um Rollen, die von intelligenten Stromzählern eingenommen werden. Es ist möglich, dass ein intelligenter Stromzähler durch Churn seine Rolle als Aggregator zwischen verschiedenen Overlay-Aggregationen verliert oder neu einnimmt. Daher wird pro Overlay-Aggregation immer der gerade gültige Aggregator bestimmt. diese Zuständigkeit wandert in jeder Overlay-Aggregation eine Ebene des Binärbaumes höher. Durch dieses Vorgehen können auch kurzfristige Ausfälle der Kommunikationsinfrastruktur kompensiert werden. Kann ein intelligenter Stromzähler seine zur Overlay-Aggregation o_n vorliegenden Messwerte nicht rechtzeitig senden, so können diese auch in jeder späteren Overlay-Aggregation $o_{n+1}, o_{n+2}, \ldots$ noch an den für diese Overlay-Aggregation gültigen Aggregator gesendet werden. Auch ein Direktversand an den Messdienstleister in o_O ist möglich.

Die Anzahl durchzuführenden Overlay-Aggregationen sollte jedoch aus zwei Gründen limitiert werden:

- Das zu versendende Datenvolumen pro Aggregator steigt mit der Anzahl an Overlay-Aggregationen.
- Mit jeder Overlay-Aggregation übernehmen weniger intelligente Stromzähler die Verantwortung für mehr Daten.

Mit jeder Overlay-Aggregation müssen mehr Daten von den Aggregatoren an ihre Eltern-Aggregatoren gesendet werden. Zwar können die aggregierten Messwerte zusammengefasst werden, die Liste der beteiligten intelligenten Stromzähler jedoch verdoppelt sich (im Schnitt) mit jedem Aggregationsschritt. Da das Senden von Daten einen limitierenden Faktor für die intelligenten Stromzähler darstellt, muss die Anzahl der in einer Overlay-Aggregation beinhalteten intelligenten Stromzähler limitiert werden. Um die Aggregatoren nicht zu sehr zu belasten sollte die Anzahl an Overlay-Aggregationen auf maximal fünf limitiert werden. Ausgehend von einer pessimistischen Abschätzung von 100 intelligenten Stromzählern pro Abschnitt würde der letzte Aggregator (also die Aggregatoren aus o_O) über den aggregierten Messwert von 3 200 intelligenten Stromzählern verfügen. Ausgehend von der in Abschnitt 5.5.3 angenommenen Sendedatenrate von 512 kbit pro Sekunde würde die Übertragung dieser 3 200 Identitäten mit jeweils 8 Byte

an den Messdienstleister 400 Millisekunden beanspruchen. Dies kann noch als zumutbarer Aufwand angesehen werden.

Mit dem erhöhten Datenvolumen steigt aber auch die Konzentration der Daten auf wenige intelligente Stromzähler. Je mehr Overlay-Aggregationen durchgeführt werden, desto weniger intelligente Stromzähler sind mit der Datenhaltung betraut. Damit erhöht sich auch die Menge an verlorenen Daten, falls ein intelligenter Stromzähler ausfällt, während er im Besitz der Daten ist. Eine hohe Anzahl an Overlay-Aggregationen führt also auch zu einer Verschlechterung der Smart Metering Leistung unter Churn.

Inwieweit die Vorteile der Overlay-Aggregation deren Nachteile aufwiegen ist von zwei Kriterien abhängig:

- Die gewünschte Anzahl an Messwerten pro Aggregat, das der Messdienstleister erhält. Mit jeder Overlay-Aggregation wird dieser Wert verdoppelt und damit auch der Privatsphärenschutz verbessert.

- Die Größe der Smart Metering Instanz und der Leistungsfähigkeit des Messdienstleisters. Gerade für sehr große Smart Metering Instanzen kann die Leistungsfähigkeit des Messdienstleisters zum Engpass werden. Ohne Overlay-Aggregation muss er pro Messintervall mit $\frac{|Z|}{2^b}$ Kontaktaufnahmen durch intelligente Stromzähler rechnen. Ist $|Z|$ sehr groß könnten Kommunikationsanbindung oder Rechenkapazität ein Problem darstellen. In diesem Fall kann mittels O reguliert werden, wieviele Kontaktaufnahmen pro Messintervall eintreten. Generell muss der Messdienstleister dann mit $\frac{1}{2^O} \times \frac{|Z|}{2^b}$ Kontaktaufnahmen rechnen.

7.1.10 Gesamtverlauf

Abschließend wird der zeitliche Gesamtverlauf des Verfahrens noch einmal zusammengefasst. Er ist in Abbildung 7.5 illustriert.

(1) Jeder intelligente Stromzähler registriert sich bei seinem Abschnittorganisator. Falls er selbst Abschnittorganisator ist, entfällt dieser Schritt.

(2) Jeder intelligente Stromzähler erhält von seinem Abschnittorganisator die SMART-ER Gruppenkonfiguration. Dies stellt gleichzeitig den Start des SMART-ER Verfahrens dar.

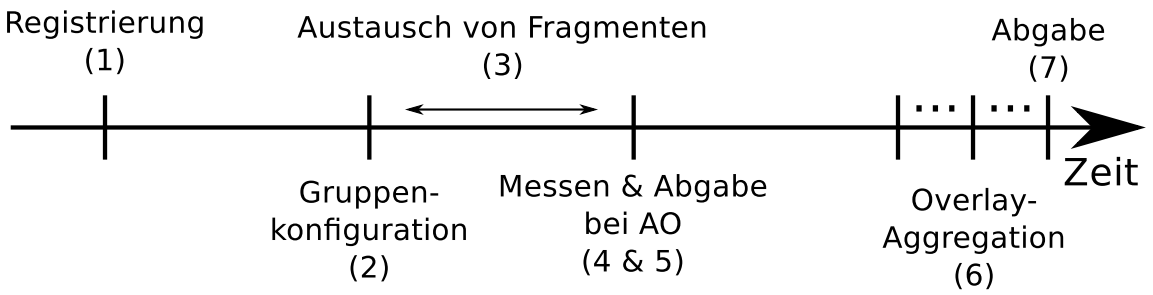


Abbildung 7.5: *Zeitlicher Ablauf des Elderberry Verfahrens.*

(3) Jeder intelligente Stromzähler tauscht SMART-ER Fragmente mit seinen Gruppenmitgliedern aus.

(4) Der Messzeitpunkt ist erreicht. Jeder intelligente Stromzähler misst seinen eigenen Messwert, generiert ein Fragment für den Ende-zu-Ende-Fragmentaustausch, und berechnet den Abgabewert.

(5) Der Abgabewert wird an den Abschnittorganisator versandt. Der Abschnittorganisator generiert ein Fragment für den Ende-zu-Ende-Fragmentaustausch und aggregiert dieses und alle eintreffenden Abgabewerte mit seinem eigenen Messwert.

(6) Es findet eine festgelegte Anzahl an Overlay-Aggregationen statt.

(7) Im Rahmen der letzten Overlay-Aggregation werden die aggregierten Messwerte zum Messdienstleister gesendet.

Zwischen den Schritten (1), (2), (5), (6) und (7) muss den intelligenten Stromzählern jeweils genügend Zeit eingeräumt werden um die vorliegenden Daten zu versenden und etwaige Sendewiederholungen durchzuführen.

Das Elderberry Verfahren hat damit, im Gegensatz zu SMART-ER und Smart Meter Speeddating, eine höhere Smart Metering Latenz (siehe Abschnitt 2.1.2) als ein nicht privatsphärengerechtes Verfahren. Nachdem die Messwerte ermittelt wurden, müssen diese zunächst durch den Abschnittorganisator aggregiert werden. Wird keine Overlay-Aggregation durchgeführt, so beträgt die zusätzliche Smart Metering Latenz gerade das Senden an den Abschnittorganisator und dessen Verarbeitung der Daten. Unter der Annahme, dass die Bearbeitungszeit durch den Abschnittorganisator vernachlässigbar ist, wird die Smart Metering Latenz

gegenüber einem nicht privatsphärengerechten Verfahren verdoppelt (zwei Sendevorgänge statt einem). Werden zusätzlich eine Anzahl von Overlay-Aggregationen vorgenommen, so tritt entsprechend dieser Anzahl eine weitere Erhöhung der Smart Metering Latenz auf.

Vergleicht man das kürzeste mögliche Messintervall von Elderberry und SMART-ER, so wird dieses in Elderberry lediglich durch die Registrierung und den Versand der Gruppenkonfiguration erhöht. Im Gegensatz zu Smart Meter Speeddating kann also in Elderberry auch ein sehr kurzes Messintervall von beispielsweise unter einer Minute realisiert werden.

7.1.11 Implementierung

Elderberry wurde zur Evaluation in OverGrid implementiert. Hierzu wurde die Implementierung von SMART-ER aus Kapitel 5 um die Elderberry-spezifischen Eigenschaften erweitert (siehe Abschnitt 7.1.8).

Da OverGrid eine Anpassung des Simulationswerkzeugs OverSim darstellt, sind die in OverSim verfügbaren Implementierungen von Overlaynetzwerken auch in OverGrid verfügbar. Als Kandidaten für das in Elderberry verwendete Overlaynetzwerk kamen Chord [127], Pastry [118], Bamboo [112], Koorde [72], Broose [56] und Kademlia [90] in Frage. Aufgrund des Vergleichs dieser Protokolle in [3] wurde in dieser Implementierung das Kademlia Overlaynetz verwendet. Es erwies sich bei den im Smart Metering zu erwartenden Churn-Raten als sehr effizient bezüglich Lookup-Zeiten und Kommunikationsaufwand. Zum Einsatz kam eine Overlay-ID-Länge von 160 Bit.

Zwischen den in Abschnitt 7.1.10 besprochenen Phasen, die eine direkte Kommunikation zwischen intelligenten Stromzählern beinhalten, wurde jeweils 5 Sekunden gewartet. Der Austausch von Fragmenten wird wie in Kapitel 5 über einen Zeitraum von 10 Sekunden durchgeführt. Da die Registrierung beim Abschnittorganisator und die Overlay-Aggregation jeweils einen Overlay-ID-Lookup beinhalten, wurde für diese eine längere Zeit von 15 Sekunden eingeplant. Diese Wartezeiten waren ausreichend um intelligenten Stromzählern den Versand der jeweilig anliegenden Daten und etwaige Sendewiederholungen zu ermöglichen.

7.2 Evaluation des Privatsphärenschutzes

Der Privatsphärenschutz des Elderberry Verfahrens setzt auf den sehr guten Eigenschaften des SMART-ER Verfahrens auf. Durch die abschnittweise Durchführung von SMART-ER werden alle Messwerte zuerst durch SMART-ER aggregiert, bevor sie dann durch Elderberry weiterverarbeitet werden. Der Ende-zu-Ende-Fragmentaustausch stellt eine weitere Maskierung der Messwerte sicher. Die in Elderberry durchgeführte Overlay-Aggregation ist daher privatsphärentechnisch unbedenklich. Ein Angriff auf die Privatsphäre eines einzelnen Haushalts muss bereits bei der Durchführung des abschnittweise durchgeführten SMART-ER Verfahrens ansetzen und benötigt zwingend die Kooperation des Messdienstleisters.

Im Unterschied zum regulären SMART-ER fungiert im abschnittweise SMART-ER ein intelligenter Stromzähler (der Abschnittorganisator) als Messdienstleister. Dieser ist für die privatsphärengerechte Aggregation der maskierten Messwerte verantwortlich. Wie in Kapitel 5 gezeigt wurde, ist ein Angriff nicht ohne die Kooperation der Partei mit dieser Rolle möglich. Im Unterschied zu den bisher vorgestellten Verfahren wird diese Rolle in Elderberry von einem intelligenten Stromzähler eingenommen. Der in Abschnitt 7.1.5 vorgestellte Ende-zu-Ende-Fragmentaustausch verhindert jedoch, dass in Elderberry ein Angriff auf die Privatsphäre eines Haushalts *ohne* Mitwirken des Messdienstleisters möglich ist. Im Falle eines nicht korrumpierten Messdienstleisters gewährt Elderberry also den gleichen, vollständigen Schutz der Privatsphäre wie SMART-ER (Kapitel 5) und Smart Meter Speeddating (Kapitel 6).

Wie in Kapitel 5 gezeigt wurde, ist ein Angriff auf die Privatsphäre eines Haushalts nur dann möglich, wenn sowohl der Abschnittorganisator, als auch alle intelligenten Stromzähler der SMART-ER Gruppe des Angriffsziels korrumpiert sind. Dieser Angriff enthält für den Angreifer zwei wesentliche Herausforderungen:

- Einbringung von ausreichend korrumpierten intelligenten Stromzählern um die SMART-ER Gruppe des Angriffsziels zu füllen.
- Korrumpieren des Abschnittorganisators des Angriffsziels.

Da der Angriff das Korrumpieren des Abschnittorganisators voraussetzt, kann dieser dann auch die Gruppeneinteilung vornehmen. Dadurch benötigt der Angreifer nur noch genügend korrumpierte intelligente Stromzähler in diesem Abschnitt um eine SMART-ER Gruppe aufzufüllen, die der Abschnittorganisator dann dem Angriffsziel zuweist.

Die Anzahl der intelligenten Stromzähler pro Abschnitt spielt bei einem Angriff eine wichtige Rolle. Daher wird diese zunächst untersucht. Danach werden die beiden genannten Herausforderungen einzeln untersucht. Es wird gezeigt, dass ein Angriff nur mit einer gewissen Wahrscheinlichkeit erfolgreich sein kann. Um konkrete Wahrscheinlichkeiten nennen zu können sei angenommen, dass ein Angreifer in jeder zweiten Epoche einen erfolgreichen Angriff auf sein Angriffsziel verüben möchte. Im Folgenden wird anhand eines Smart Meterings mit 10 000 intelligenten Stromzählern die Frage beantwortet, welchen Anteil der intelligenten Stromzähler er zum Erreichen des Ziels korrumpieren müsste.

7.2.1 Anzahl intelligenter Stromzähler pro Abschnitt

Die Anzahl der intelligenten Stromzähler pro Abschnitt stellt ein wichtiges Merkmal in Elderberry dar. Wie in Abschnitt 7.1.6 diskutiert, führt eine zu geringe Anzahl an intelligenten Stromzählern in einem Abschnitt zum Ausfall des Abschnitts. Eine zu hohe Anzahl an intelligenten Stromzählern in einem Abschnitt führt wiederum zu einer starken Beanspruchung oder gar Überlastung des Abschnittorganisators.

Im Rahmen der Evaluation wurde die durchschnittliche Anzahl an intelligenten Stromzählern pro Abschnitt untersucht. Es wurde bei normalem Churn eine variierende Anzahl an teilnehmenden intelligenten Stromzählern simuliert. Da die Overlay-Aggregation keinen Einfluss auf die Anzahl intelligenter Stromzählern pro Abschnitt hat, wurde sie für diese Untersuchung abgeschaltet. Die betrachteten Parameterkonfigurationen sind in Tabelle 7.2 zusammengefasst.

Die Ergebnisse sind in Abbildung 7.6 zu sehen. Auf der x-Achse ist die Anzahl intelligenter Stromzähler im Smart Metering aufgetragen. Auf der y-Achse das arithmetische Mittel der Anzahl an intelligenten Stromzählern pro Abschnitt. Zusätzlich ist jeweils das Maximum und das Minimum eingetragen. Da für diese Untersuchung die Gesamtzahl der intelligenten Stromzähler variiert wurde, ändert sich auch die Präfixlänge. Um dies zu verdeutlichen wurde die eingezeichnete Linie bei jedem Wechsel der Präfixlänge unterbrochen.

In der Abbildung ist zu erkennen, dass die durchschnittliche Anzahl an intelligenten Stromzählern pro Abschnitt mit der Gesamtzahl an intelligenten Stromzählern ansteigt, so lange sich die Präfixlänge nicht ändert. Betrachtet sei beispielsweise die Anzahl pro Abschnitt startend ab 4 000 teilnehmenden intelligenten Stromzählern. Ausgehend von einem Wert bei circa 30 steigt sie linear mit der Anzahl an intelligenten Stromzählern im Smart Metering. Der Anstieg dauert bis ein durchschnittlicher Wert von circa 55 erreicht ist. Durch die Erhöhung der Präfixlänge

Tabelle 7.2: *Parameterkonfigurationen zur Evaluation der Anzahl intelligenter Stromzähler pro Abschnitt.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{2\,000, 3\,000, \ldots, 20\,000\}$
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
Simuliertes Messintervall	15 Minuten
Maximaler Fragmentwert	2^{32}
Anzahl Overlay-Aggregationen	$O = 0$
SMART-ER (intern) Gruppengröße	$G = 5$
Anzahl versendeter Fragmente	Gruppengröße -1

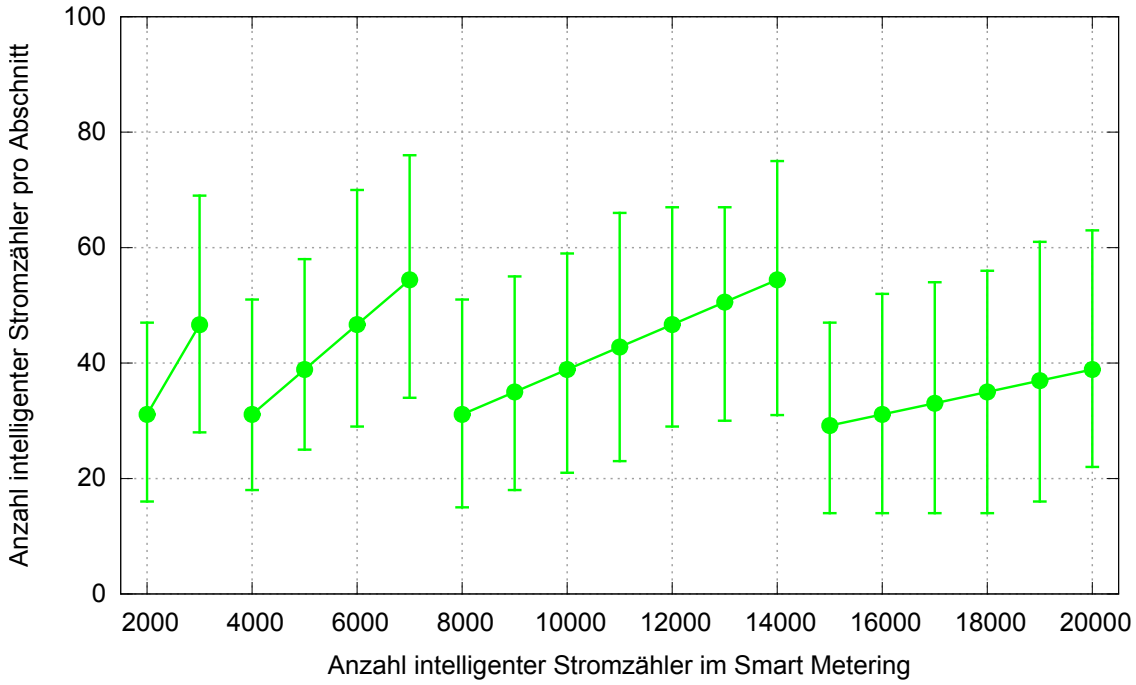


Abbildung 7.6: *Anzahl intelligenter Stromzähler pro Abschnitt.*

um eins (unterbrochene Linie) reduziert sich die durchschnittliche Anzahl an intelligenten Stromzählern pro Abschnitt wieder auf den Ausgangswert. Die flacher werdende Steigung des linearen Anstiegs ist der Verteilung der hinzukommenden intelligenten Stromzähler auf mehr Abschnitte geschuldet.

Neben der durchschnittlichen Anzahl ist bei dieser Betrachtung das Maximum und Minimum besonders wichtig. Wie in der Abbildung zu sehen, sind die Maxima und Minima nahe an den Durchschnittswerten. Der im gesamten Versuch kleinste beobachtete Abschnitt war mit 14 intelligenten Stromzählern noch immer mit genügend Stromzählern ausgestattet um SMART-ER durchzuführen. Der größte beobachtete Abschnitt hatte 76 intelligenten Stromzähler. Auch dieser Wert ist unbedenklich, da der Aufwand für den Abschnittorganisator bei 76 intelligenten Stromzählern noch problemlos ist (siehe Abschnitt 7.1.6).

7.2.2 Platzierung korrumpierter Stromzähler in Abschnitten

Um gezielt einen Angriff auf die Privatsphäre eines bestimmten Haushalts durchführen zu können, ist es für den Angreifer unumgänglich korrumpierte intelligente Stromzähler im Abschnitt des Angriffsziels zu platzieren. Dies ist jedoch durch das Prinzip der Overlay-ID-Bestimmung aus Abschnitt 7.1.2 erschwert. Ein intelligenter Stromzähler hat keinen Einfluss auf seine Overlay-ID. Sie hängt ausschließlich von der Identität des intelligenten Stromzählers und einer externen Zufallsquelle ab und wird mittels einer kryptologischen Hashfunktion ermittelt. Angriffe auf Overlaynetze, die eine freie Overlay-ID-Wahl benötigen (wie beispielsweise behandelt von Cerri et al. [23]) sind dadurch ausgeschlossen.

Zur Platzierung eines intelligenten Stromzählers innerhalb eines bestimmten Abschnitts kann ein Angreifer also nur eine Menge von korrumpierten intelligenten Stromzählern vorhalten und darauf warten, dass eine Teilmenge davon zufällig im selben Abschnitt wie das Angriffsziel ist. Geht man von einer Gleichverteilung der Overlay-IDs aus, so ist die Wahrscheinlichkeit für einen korrumpierten intelligenten Stromzähler im richtigen Abschnitt zu sein $\frac{1}{2^b}$. Um also durchschnittlich *einen* korrumpierten intelligenten Stromzähler im richtigen Abschnitt zu platzieren, werden 2^b korrumpierte intelligente Stromzähler benötigt. Sollen n korrumpierte intelligente Stromzähler mit großer Wahrscheinlichkeit im selben Abschnitt wie das Angriffsziel sein, so müssen circa $n \times 2^b$ korrumpierte intelligente Stromzähler vorgehalten werden.

Der Mechanismus zur Bestimmung der Overlay-ID aus Abschnitt 7.1.2 sorgt dafür, dass die Kosten (in Form von korrumpierten intelligenten Stromzählern) zur

probabilistischen Einbringung eines korrumpierten intelligenten Stromzählers in einen bestimmten Abschnitt mit der Anzahl der Abschnitte steigt. Diese wiederum steigt mit der Anzahl an intelligenten Stromzählern im Smart Metering. Schon bei 1 000 intelligenten Stromzählern (32 Abschnitte) werden pro korrumpiertem intelligenten Stromzähler im richtigen Abschnitt durchschnittlich 32 korrumpierte intelligente Stromzähler benötigt. Dies entspricht 3, 2% der Gesamtanzahl und stellt damit einen enormen Aufwand für den Angreifer dar.

Für die Fragestellung, welcher Anteil notwendig ist um bei einem Smart Metering mit 10 000 intelligenten Stromzählern in jeder zweiten Epoche erfolgreich zu sein (siehe Abschnitt 7.2), kann nun berechnet werden, wieviele korrumpierte intelligente Stromzähler zusätzlich benötigt werden, um einen korrumpierten intelligenten Stromzähler mit hoher Wahrscheinlichkeit im richtigen Abschnitt zu platzieren. Bei 10 000 intelligenten Stromzähler existieren 256 Abschnitte. Daher werden pro richtig platziertem korrumpierten intelligenten Stromzähler durchschnittlich 255 weitere korrumpierte intelligente Stromzähler benötigt.

7.2.3 Korrumpierter Abschnittorganisator

Durch den Einsatz des SMART-ER Verfahrens genügt es für einen erfolgreichen Angriff nicht eine große Zahl an korrumpierten intelligenten Stromzählern im Abschnitt des Angriffsziels zu haben. Um erfolgreich zu sein, muss auch der Abschnittorganisator durch einen korrumpierten intelligenten Stromzähler gestellt werden.

Um dieses Ziel zu erreichen muss ein korrumpierter intelligenter Stromzähler für den berechneten AO-Punkt im KBR verantwortlich sein. Welcher intelligente Stromzähler des Abschnitts für den AO-Punkt verantwortlich ist, hängt von der Verteilung der Overlay-IDs ab. Geht man von einer Gleichverteilung aus, so ist die Wahrscheinlichkeit Abschnittorganisator zu werden für einen beliebigen intelligenten Stromzähler $\frac{1}{n}$ (mit n als Anzahl intelligenter Stromzähler im Abschnitt). Um einen solchen Angriff also mit einer hohen Erfolgswahrscheinlichkeit durchzuführen ist eine großer Anteil an korrumpierten intelligenten Stromzählern pro Abschnitt notwendig.

Eine andere Möglichkeit für den Angreifer den Abschnittorganisator zu stellen ist die Zuständigkeit für den AO-Punkt vorzutäuschen. Dies kann nur dann funktionieren, wenn ein korrumpierter Stromzähler näher am AO-Punkt liegt, als das Angriffsziel. Je nach verwendetem Overlaynetz besteht dann die Möglichkeit, das Angriffsziel über die Zuständigkeit für den AO-Punkt gezielt zu belügen. Diese

Art Angriff wird beispielsweise von Castro et al. [21] und Srivatsa und Liu [124] behandelt. Eine Analyse der verschiedenen Overlaynetze übersteigt jedoch den Rahmen dieser Arbeit. Es sei jedoch auf S/Kademlia [6] verwiesen, das diesen Fall explizit behandelt und selbst bei einem hohen Anteil von korrumpierten Knoten ($\approx 30\%$) noch korrekte Werte liefert.

Wird das Smart Metering mit 10 000 intelligenten Stromzählern betrachtet, so kann aus Abbildung 7.6 geschlossen werden, dass durchschnittlich 38 intelligente Stromzähler in einem Abschnitt sind. Um in diesem Fall in jeder zweiten Epoche den Abschnittorganisator zu stellen, müssen $\frac{38}{2} = 19$ korrumpierte intelligente Stromzähler vorhanden sein. Wie in Abschnitt 7.2.2 gezeigt, werden für jeden dieser 19 korrumpierten intelligenten Stromzähler 255 weitere benötigt. Die Gesamtzahl der benötigten korrumpierten intelligenten Stromzähler, um in jeder zweiten Epoche einen erfolgreichen Angriff durchführen zu können, beträgt also $19 \times 256 = 4864$. Bei 10 000 intelligenten Stromzählern entspricht dies einem Anteil von $48,64\%$.

7.2.4 Mitwirken des Messdienstleisters

In der bisherigen Betrachtung wurde der Messdienstleister außen vor gelassen. Sein Einfluss ist bei dieser Form des dezentralen Smart Meterings auch nur gering. Ihm stehen lediglich zwei Möglichkeiten zur Beeinflussung offen:

- Übermittlung falscher Parameter in der Konfiguration
- Zuweisen eines eigens für das Angriffsziel geschaffenen Overlaynetzes

Bei der Übermittlung falscher Parameter in der Konfiguration ist jedoch durch die Konstruktion ausgeschlossen, dass nur dem Angriffsziel ein falscher Parameter mitgeteilt wird (siehe Abschnitt 7.1.4). Alle Parameter gelten somit für alle teilnehmenden intelligenten Stromzähler.

Der einzige Parameter, der einen Vorteil für den Angreifer ermöglichen könnte, ist die Anzahl der teilnehmenden intelligenten Stromzähler A. Er bestimmt wie viele Abschnitte gebildet werden. Wird er deutlich zu hoch gewählt, so würde dies in einer größeren Anzahl an Abschnitten und damit weniger intelligenten Stromzählern pro Abschnitt resultieren. Auf den ersten Blick schadet dies dem Angreifer, denn mit mehr Abschnitten muss er auch über mehr korrumpierte intelligente Stromzähler verfügen. Die zu hohe Abschnittanzahl führt jedoch auch zu dünner

besiedelten Abschnitten, was die Wahrscheinlichkeit erhöht den Abschnittorganisator zu stellen. Umgekehrt verhält es sich mit einer zu niedrig angesetzten Anzahl *A*. Sie reduziert die benötigte Anzahl an korrumpierten intelligenten Stromzählern um eine ausreichende Anzahl mit hoher Wahrscheinlichkeit in einen bestimmten Abschnitt einzubringen. Gleichzeitig verringert sich die Wahrscheinlichkeit, dass einer der korrumpierten intelligenten Stromzählern Abschnittorganisator wird.

Unabhängig davon ob der Messdienstleister ein zu großes oder zu kleines *A* wählt, ist eine starke Abweichung von der tatsächlichen Anzahl an intelligenten Stromzählern im Overlaynetz erkennbar. Zur effizienten Abschätzung der Größe von strukturierten Overlaynetzen durch jeden einzelnen Knoten existieren eine Vielzahl an Arbeiten (beispielsweise [89, 121]).

Wie in allen behandelten Verfahren muss der Messdienstleister das Smart Metering organisieren. Damit ergibt sich die Möglichkeit speziell für das Angriffsziel ein Smart Metering zu organisieren, das nur aus korrumpierten intelligenten Stromzählern besteht. Mittels einer einfachen Mindestgröße für das Smart Metering, beispielsweise 1 000 intelligente Stromzähler, kann der Aufwand für diesen Angriff beliebig hoch angesetzt werden.

7.2.5 Zusammenfassung

Zusammenfassend kann für Elderberry geschlossen werden, dass ein Angreifer kaum aktive Möglichkeiten zum Angriff auf die Privatsphäre hat. Die Einteilung in Abschnitte aufgrund der Identität der intelligenten Stromzähler verhindert die gezielte Platzierung von korrumpierten Stromzählern in den gewünschten Abschnitt. Der Angreifer muss eine große Zahl an korrumpierten intelligenten Stromzählern einsetzen um eine hohe Wahrscheinlichkeit für eine Platzierung im gewünschten Abschnitt zu erhalten.

Um überhaupt einen Angriff auf die Privatsphäre eines einzelnen Haushalts durchführen zu können, muss der Angreifer über mindesten zwei korrumpierte Stromzähler im Abschnitt des Angriffsziels verfügen. Ein korrumpierter Stromzähler muss als Abschnittorganisator fungieren. Der andere korrumpierte Stromzähler wird verwendet um die SMART-ER Gruppe des Angriffsziels aufzufüllen. Die Wahrscheinlichkeit, dass einer der beiden korrumpierten intelligenten Stromzähler zum Abschnittorganisator wird ist allerdings gering. Wie gezeigt wurde, ist ein Angriff mit hoher Erfolgswahrscheinlichkeit nur mit einem sehr großen Anteil an korrumpierten intelligenten Stromzählern möglich.

Zusätzlich können intelligente Stromzähler noch selbst Schutzmaßnahmen ergreifen. Beispielsweise könnte das Overlaynetz nach weiteren intelligenten Stromzählern im Abschnitt durchsucht werden, falls der Abschnittorganisator eine Gruppe mit weniger als der konfigurierten Gruppengröße übergibt. Liefert diese Suche weitere intelligente Stromzähler obwohl der Abschnittorganisator dauerhaft zu kleine Gruppen zuweist, liegt ein Angriff vor.

7.3 Evaluation der Smart Metering Leistung

Dieser Abschnitt beschäftigt sich mit der Evaluation des Elderberry Verfahrens bezüglich der Smart Metering Leistung. Analog zu den Evaluationen von SMART-ER ist er in vier Unterabschnitte eingeteilt:

- Abschnitt 7.3.1 betrachtet den Anteil an intelligenten Stromzählern, über die Elderberry unter Churn eine fehlerfreie Aussage trifft. Ebenfalls wir die Skalierbarkeit von Elderberry untersucht.
- Abschnitt 7.3.2 behandelt den Rechenaufwand, den Elderberry auf einem einzelnen intelligenten Stromzähler verursacht.
- Abschnitt 7.3.3 behandelt den Speicheraufwand, den ein einzelner intelligenter Stromzähler in Elderberry hat.
- Abschnitt 7.3.4 untersucht den Kommunikationsaufwand in Elderberry.

Das in Elderberry verwendete SMART-ER Verfahren wurde so konfiguriert, dass ein Abschnittorganisator Gruppen der Größe 5 bildet. Jeder intelligente Stromzähler eines Abschnitts versendet Fragmente an alle Mitglieder seiner Gruppe, also $|G| - 1$ Fragmente.

7.3.1 Leistung

Zur Untersuchung der Smart Metering Leistung von Elderberry wurden Untersuchungen mit variierendem Churn durchgeführt. Da Elderberry ein Overlaynetz verwendet, musste bei den Simulationen berücksichtigt werden, dass sich dieses in einem eingeschwungenen Zustand befindet. Für jede der in diesem Abschnitt durchgeführten Simulationen wurde daher eine initiale Aufbauphase durchgeführt,

Tabelle 7.3: *Parameterkonfigurationen zum Vergleich von Baseline, SMART-ER und Elderberry unter verschieden starkem Churn.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000 $\Rightarrow$ Präfixlänge[1] $b = 7$
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 150
Simuliertes Messintervall	15 Minuten
Maximaler Fragmentwert	2^{32}
SMART-ER Gruppengröße[2]	$G \in \{40, 80, 160\}$
Anzahl Overlay-Aggregationen[1]	$O \in \{0, 1, 2\}$
SMART-ER (intern) Gruppengröße[1]	$G = 5$
Anzahl versendeter Fragmente	Gruppengröße $- 1$

[1] nur Elderberry, [2] nur eigenständiges SMART-ER

in der im Abstand von jeweils 100 Millisekunden ein neuer intelligenter Stromzähler dem Overlaynetz beigetreten ist. Die Dauer dieser Phase ist damit abhängig von der Zahl an simulierten intelligenten Stromzählern. Nachdem die Aufbauphase beendet war, wurde eine Übergangszeit von 1 000 Sekunden gewartet, um zu gewährleisten, dass sich das Overlaynetz im eingeschwungenen Zustand befindet. Erst danach wurde mit der Aufzeichnung von Simulationsergebnissen begonnen.

Neben dem Churn wurde auch die Anzahl an Overlay-Aggregationen varriiert um deren Einfluss auf die Smart Metering Leistung aufzuzeigen. Auch wurde ein SMART Metering mit eigenständigem SMART-ER (also ohne Elderberry) simuliert. Die dabei verwendeten Gruppengrößen wurden so gewählt, dass sie der Gruppengrößen der verschiedenen Parameterkonfigurationen für die Overlay-Aggregation entsprechen. Bei 5 000 intelligenten Stromzählern und ohne Overlay-Aggregation erhielt der Messdienstleister Aggregate, die jeweils Messwerte von durchschnittlich 40 intelligenten Stromzählern beinhalteten. Entsprechend wurde für das eigenständige SMART-ER eine Gruppengröße von 40 konfiguriert um einen vergleichbaren Schutz der Privatsphäre der Gruppe zu erhalten. Die betrachteten Parameterkonfigurationen sind in Tabelle 7.3 zusammengefasst.

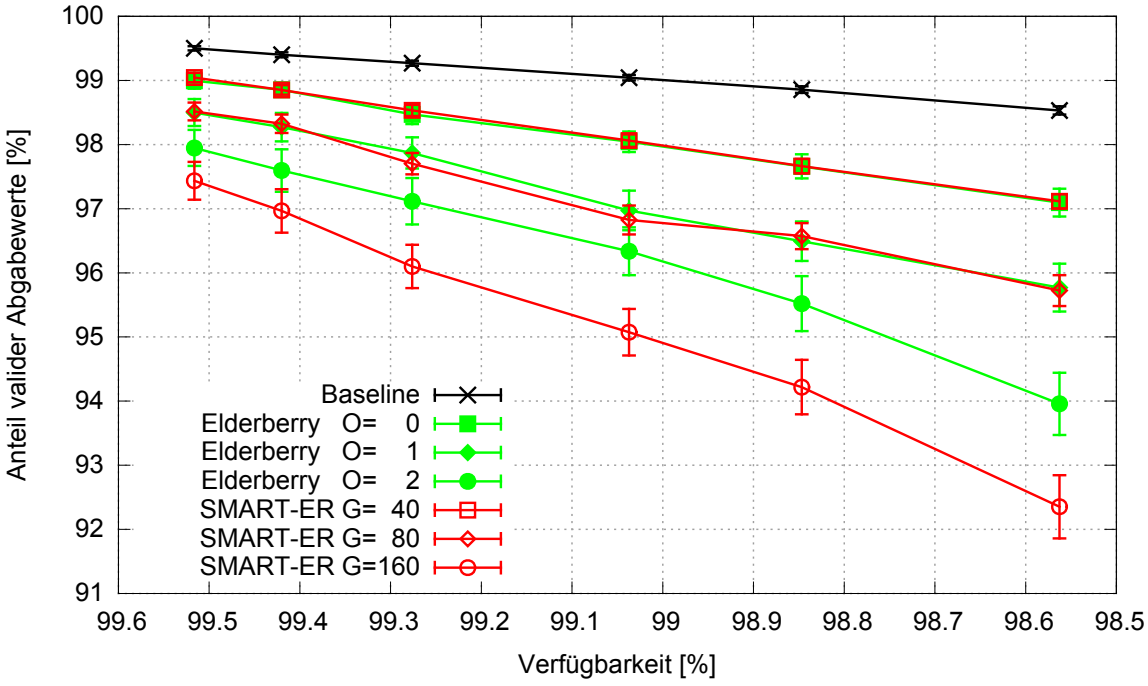


Abbildung 7.7: *Vergleich verschiedener Anzahlen an Overlay-Aggregationen unter Churn.*

Die Ergebnisse sind in Abbildung 7.7 zu sehen. Auf der x-Achse ist die durchschnittliche Verfügbarkeit der Kommunikationsanbindung der intelligenten Stromzähler aufgetragen. Auf der y-Achse ist der erzielte Anteil an validen Abgabewerten eingezeichnet. Elderberry (grün) wurde mit keiner Overlay-Aggregation (ausgefüllter Kreis), einer Overlay-Aggregation (ausgefüllter Diamant), und zwei Overlay-Aggregationen (ausgefülltes Dreieck) durchgeführt. Die entsprechenden SMART-ER Konfigurationen sind mit gleichem, aber nicht ausgefülltem, Symbol und in rot eingezeichnet. Eingezeichnet ist das arithmetische Mittel sowie 98% Konfidenzintervalle. Neben Elderberry und SMART-ER wurde auch das Verfahren Baseline aus Kapitel 5, das keinen Privatsphärenschutz bietet, eingezeichnet (Kreuz). Es dient zum Vergleich mit der maximal erreichbaren Leistung.

Die Abbildung zeigt, dass Elderberry ohne Overlay-Aggregation (Symbol: Quadrat) mit SMART-ER und Gruppengröße 40 vergleichbare Ergebnisse erzielt. Die Kurven verlaufen beinahe deckungsgleich. Für Elderberry sind jedoch geringfügig größere Konfidenzintervalle zu erkennen. Bei einer Overlay-Aggregation, respektive Gruppengröße 80, ist der durchschnittliche Anteil an validen Abgabewerten

von Elderberry für fast alle Parametrisierungen geringfügig höher. Aufgrund der Streuung und der daraus folgenden großen Konfidenzintervalle ist hier jedoch kein klarer Unterschied feststellbar. Für zwei Overlay-Aggregationen (Symbol: Kreis), respektive Gruppengröße 160, erreicht Elderberry konsistent einen deutlich höheren Anteil an validen Abgabewerten als SMART-ER. Es kann geschlossen werden, dass Elderberry bei vergleichbarem Schutz der Privatsphäre der Gruppe ein vergleichbares oder besseres Ergebnis liefert als SMART-ER.

Betrachtet man den Einfluss von Churn auf Elderberry, so ist bei normalem Churn und ohne Overlay-Aggregation der Anteil valider Abgabewerte bei 99% und sinkt beim stärksten betrachteten Churn bis auf 97% ab. Das Durchführen von Overlay-Aggregationen hat auf die Ergebnisse bei normalem Churn bereits negativen Einfluss. Dieser intensiviert sich mit stärker werdendem Churn. Während die Durchführung von zwei Overlay-Aggregationen bei normalem Churn zu Einbußen von circa einem Prozentpunkt gegenüber der Durchführung ohne Overlay-Aggregation führt, betragen die Einbußen beim stärksten simulierten Churn bereits drei Prozentpunkte. Eine höhere Anzahl von Overlay-Aggregationen verursacht schlechtere Ergebnisse. Dies ist naheliegend, da jede Overlay-Aggregation dazu führt, dass die bereits bestehenden Ergebnisse länger auf den intelligenten Stromzählern verbleiben. Zusätzlich halbiert jede Overlay-Aggregation die Anzahl an intelligenten Stromzählern, die im Besitz der Ergebnisse sind. Gleichzeitig verdoppelt jede Overlay-Aggregation die Anzahl an Messwerten, die ein aggregierender intelligenter Stromzähler vorhält. Bei zwei Overlay-Aggregationen und einer Präfixlänge von 7 sind vor der Abgabe an den Messdienstleister nur noch $2^{7-2} = 32$ intelligente Stromzähler im Besitz der Messdaten. Eine Störung der Kommunikationsanbindung eines einzelnen dieser Stromzähler kann zum Verlust der Messdaten von durchschnittlich $\frac{5\,000}{32} \approx 156$ intelligenten Stromzählern führen. Dies verursacht eine größere Varianz der Ergebnisse die sich in den größeren Konfidenzintervallen niederschlägt.

Neben der Leistung unter Churn wurde auch die Skalierbarkeit des Elderberry Verfahrens untersucht. Hierfür wurde bei normalem Churn und variierender Anzahl an Overlay-Aggregationen eine variierende Anzahl an intelligenten Stromzählern simuliert. Die betrachteten Parameterkonfigurationen sind in Tabelle 7.4 zusammengefasst. Wie am Anfang des Abschnitts beschrieben wurde mit Aufbauphase und Übergangszeit evaluiert. Die Ergebnisse sind in Abbildung 7.8 dargestellt. Auf der x-Achse ist die Anzahl simulierter intelligenter Stromzähler aufgetragen. Auf der y-Achse der Anteil an validen Abgabewerten. Dargestellt ist das arith-

Tabelle 7.4: *Parameterkonfigurationen zur Evaluation der Skalierbarkeit von Elderberry.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{1\,000, 2\,000, \ldots, 10\,000\}$
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 150
Simuliertes Messintervall	15 Minuten
Maximaler Fragmentwert	2^{32}
Anzahl Overlay-Aggregationen	$O \in \{0, 1, 2\}$
SMART-ER (intern) Gruppengröße	$G = 5$
Anzahl versendeter Fragmente	Gruppengröße -1

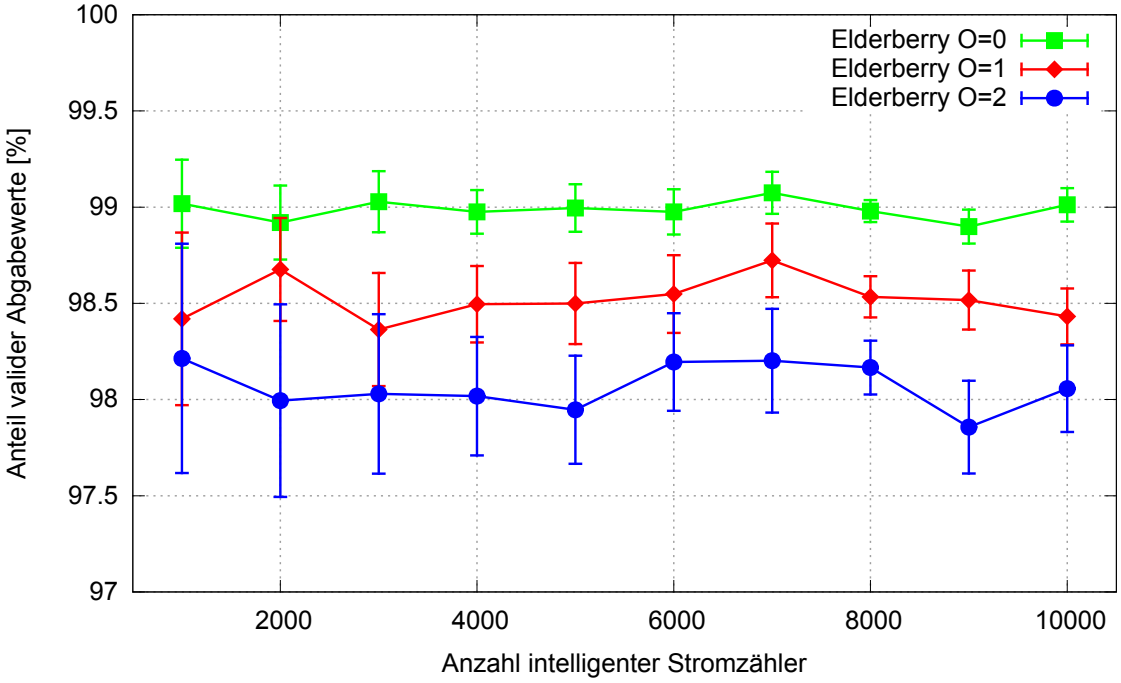


Abbildung 7.8: *Skalierbarkeit von Elderberry bis 10 000 Stromzähler.*

metische Mittel mit 98% Konfidenzintervallen für jede konfigurierte Anzahl an Overlay-Aggregationen.

Da Elderberry auf das Teile- und Herrsche-Paradigma aufbaut, ist seine Skalierbarkeit erwartungsgemäß hervorragend. Insbesondere ohne Overlay-Aggregation (Symbol: Quadrat) schwankt der Anteil valider Abgabewerte nur wenig über die verschiedenen Anzahlen an simulierten intelligenten Stromzählern. Auch ist zu sehen, dass die Konfidenzintervalle mit mehr intelligenten Stromzählern kleiner werden. Mit einer Overlay-Aggregation (Symbol: Raute) oder zwei Overlay-Aggregationen (Symbol: Kreis) ist insbesondere bei kleineren Anzahlen an intelligenten Stromzählern eine deutliche Schwankung der Ergebnisse anhand der großen Konfidenzintervalle erkennbar. Dies ist darauf zurückzuführen, dass bei gleichbleibender Anzahl Overlay-Aggregationen und einer kleineren Anzahl an teilnehmenden intelligenten Stromzählern weniger Aggregatoren im Besitz der Ergebnisse sind. Beispielhaft seien 1 000 teilnehmende intelligente Stromzähler und 5 000 teilnehmende intelligente Stromzähler vergleichen. Bei 1 000 teilnehmenden intelligenten Stromzählern ist $b = 5$. Also existieren $2^5 = 32$ Abschnitte. Nach zwei Overlay-Aggregationen werden dann lediglich acht Aggregate von ebensovielen Aggregatoren an den Messdienstleister gesendet. Fällt einer dieser acht Aggregatoren, nachdem er die Aggregate empfangen hat und bevor er sie weitersenden konnte, aus, so fehlt durchschnittlich auch ein achtel der Ergebnisse beim Messdienstleister. Vergleicht man dies mit 5 000 intelligenten Stromzählern, so wird klar warum die Varianz der Ergebnisse hier kleiner ausfallen muss. Bei 5 000 teilnehmenden intelligenten Stromzählern ist $b = 7$. Also existieren $2^7 = 128$ Abschnitte. Nach zwei Overlay-Aggregationen werden 32 Aggregate von ebensovielen Aggregatoren an den Messdienstleister gesendet. Fällt einer dieser 32 aus nachdem er die Aggregate empfangen hat und bevor er sie weitersenden konnte, so fehlt durchschnittlich auch ein 32-tel der Ergebnisse beim Messdienstleister. Anteilig an der Gesamtzahl wirkt sich der Ausfall eines Aggregators, während er im Besitz der jeweiligen Ergebnisse ist, bei einer größeren Anzahl an teilnehmenden intelligenten Stromzählern weniger stark aus.

Da Elderberry auch für den Einsatz in sehr großen Smart Meterings entworfen wurde, sind auch Simulationen mit einer wesentlich höheren Anzahl an intelligenten Stromzählern durchgeführt worden. Aufgrund des hohen Simulationsaufwands wurde allerdings eine andere Methodik verwendet. Es wurden 12 Stunden, also 48 aufeinanderfolgende Messintervalle des Smart Meterings, simuliert und der Durchschnitt über die Messintervalle gebildet. Dies ersparte die Durchführung von sehr vielen Aufbauphasen, die bei großer Anzahl an intelligenten Stromzählern

Tabelle 7.5: *Parameterkonfigurationen zur Evaluation der Skalierbarkeit von Elderberry für größere Smart Metering Instanzen.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	$\{10\,000, 20\,000, \ldots, 100\,000\}$
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 1
Simuliertes Messintervall	15 Minuten
Simulierter Zeitraum	12 Stunden (48 Messintervalle)
Maximaler Fragmentwert	2^{32}
Anzahl Overlay-Aggregationen	$O = 0$
SMART-ER (intern) Gruppengröße	$G = 5$
Anzahl versendeter Fragmente	Gruppengröße -1

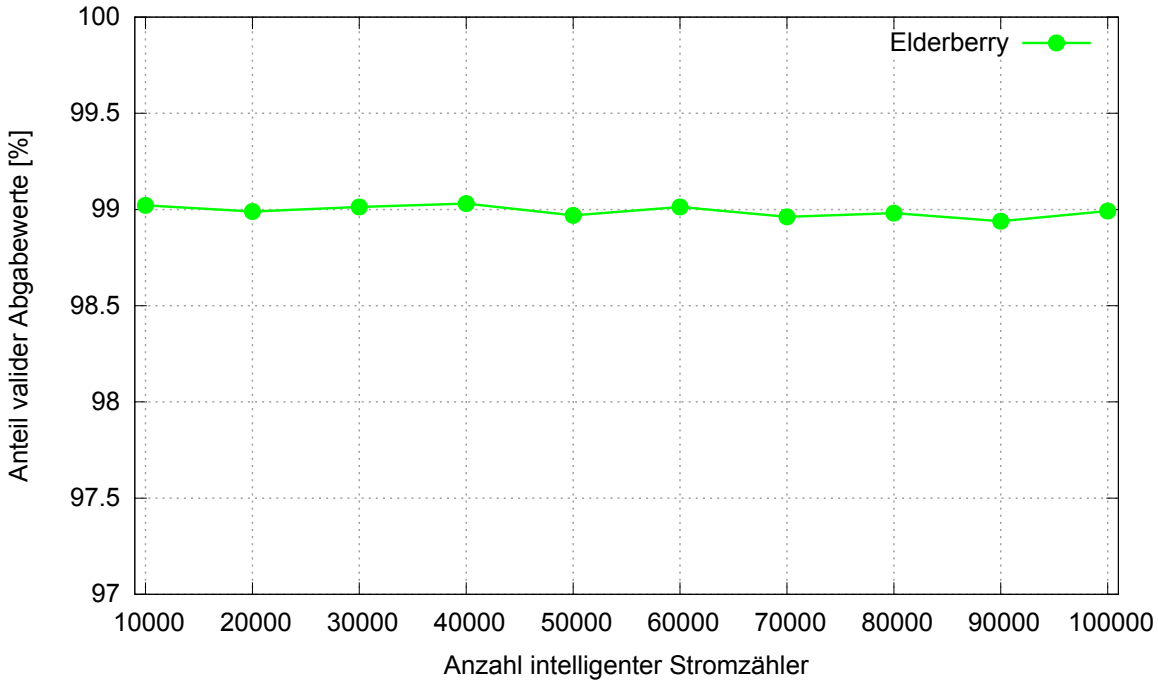


Abbildung 7.9: *Skalierbarkeit von Elderberry bis 100 000 Stromzähler.*

sehr lange dauern. Die betrachteten Parameterkonfigurationen sind in Tabelle 7.5 zusammengefasst. Die Ergebnisse sind in Abbildung 7.9 dargestellt. Auf der x-Achse ist die Anzahl simulierter intelligenter Stromzähler aufgetragen. Auf der y-Achse der Anteil an validen Abgabewerten. Eingezeichnet ist das arithmetische Mittel mit 98%-Konfidenzintervallen. Aufgrund der geringen Varianz der Ergebnisse werden diese vom Symbol verdeckt. Auch in dieser Simulationsreihe ist die gute Skalierbarkeit des Elderberry Verfahrens am waagerechten Verlauf der Kurve zu erkennen. Es konnte also gezeigt werden, dass sich Elderberry auch für sehr große Smart Metering Instanzen eignet.

Die Evaluation der Smart Metering Leistung von Elderberry hat ergeben, dass Elderberry vergleichbare oder bessere Ergebnisse liefert als eine SMART-ER Konfiguration bei vergleichbarem Schutz der Privatsphäre. Bei normalem Churn erreicht es ohne Overlay-Aggregation einen Anteil valider Abgabewerte von 99%. Auch nach zwei Overlay-Aggregationen sind bei normalem Churn noch durchschnittlich 98% der intelligenten Stromzähler im Smart Metering Ergebnis vertreten. Bedenkt man, dass selbst Baseline $0,5$ Prozentpunkte durch Churn verliert, so sind 2 Prozentpunkte für ein privatsphärengerechtes Smart Metering mit dezentraler, peer-to-peer Aggregation ein sehr gutes Ergebnis. In Simulationen bist zu 100 000 intelligenten Stromzählern konnte Elderberry eine sehr gute Skalierbarkeit nachgewiesen werden.

7.3.2 Rechenaufwand

Im Folgenden wird der Rechenaufwand des Elderberry Verfahrens untersucht. Elderberry verwendet ein Overlaynetz, weshalb auch für dessen Implementierung mit Rechenaufwand gerechnet werden muss. Da dieses Overlaynetz eine modulare Komponente ist und sich dessen Rechenaufwand je nach Implementierung ändern kann, wird dieser hier nicht näher untersucht. Evaluationen gängiger Overlaynetze für ihre Verwendung in mobilen Plattformen (siehe beispielsweise Ou et al. [103] für Kademlia) lassen jedoch darauf schließen, dass der verursachte Rechenaufwand mit modernen eingebetteten Systemen problemlos handhabbar ist.

Betrachtet man den Rechenaufwand des Elderberry Verfahrens selbst, so ist dieser in großen Teilen vergleichbar mit dem Rechenaufwand des SMART-ER Verfahrens aus Kapitel 5. Dies trifft insbesondere dann zu, wenn ein intelligenter Stromzähler in einer Epoche weder die Rolle Abschnittorganisator noch die Rolle Aggregator einnimmt. Der Mehraufwand im Vergleich zum SMART-ER Verfahren besteht in der Registrierung beim Abschnittorganisator und in der Überprüfung

von dessen Zugangsberechtigung. Auch muss ein intelligenter Stromzähler in Elderberry die Zugangsberechtigungen seiner Gruppenmitglieder überprüfen. Hier fällt also eine Überprüfung von insgesamt fünf Signaturen an. Diese Signaturen müssen nicht von den intelligenten Stromzählern geleistet werden, da die Zugangsberechtigung vom Messdienstleister signiert ist.

Mit einem deutlich größeren Rechenaufwand muss für den Abschnittorganisator gerechnet werden. Er muss die Zugangsberechtigungen der intelligenten Stromzähler prüfen, die sich bei ihm registrieren. Ebenfalls muss er für deren übermittelte, maskierte Messwerte eine Abhängigkeitsauflösung durchführen und die verbleibenden maskierten Messwerte aggregieren. Die Überprüfung der Zugangsberechtigungen verursacht mit großer Wahrscheinlichkeit unter 100 Überprüfungen von Signaturen (siehe Abschnitt 7.2.1). Welcher Rechenaufwand für die Überprüfungen der Signaturen anfällt ist abhängig vom verwendeten Signaturverfahren. Wird beispielsweise Ed25519 von Bernstein et al. [12] in einer Software-Implementierung verwendet, so genügt ein Prozessor mit circa 118 Megahertz Taktfrequenz eines aktuellen eingebetteten Systems (Statistiken zu ARM Cortex-A15 aus eBACS [40]) zur Überprüfung von 100 Signaturen innerhalb einer Sekunde. Steht eine hardwareunterstützte Implementierung zur Verfügung ist der Aufwand entsprechend geringer. Da diese Überprüfung nur einmal pro Epoche durchgeführt werden müssen, ist der Aufwand vernachlässigbar. Ebenfalls ist die Abhängigkeitsauflösung für so wenige intelligente Stromzähler auch mit beschränkten Ressourcen in kürzester Zeit durchführbar.

Erfüllt ein intelligenter Stromzähler die Rolle Aggregator, so muss er zusätzlich zu seinem Aufwand als normaler intelligenter Stromzähler, die Zugangsberechtigungen der intelligenten Stromzähler prüfen, die ihm Messdaten zur Aggregation zusenden. Im Normalfall handelt es sich hierbei um zwei intelligente Stromzähler. In Ausnahmesituationen können auch einzelne Aggregatoren übersprungen werden, weshalb auch mehr Sender möglich sind. Da aber nur wenige Overlay-Aggregationen sinnvoll sind (siehe Abschnitt 7.3.1), ist die Anzahl Sender auch im schlechtesten Fall sehr gering. Die empfangenen Daten müssen vom Aggregator noch aggregiert werden, was mittels einer einfachen Addition geschieht.

Unabhängig von der Rolle des intelligenten Stromzählers muss zur Realisierung des Ende-zu-Ende-Fragmentaustauschs (siehe Abschnitt 7.1.5) in jedem Messintervall ein zusätzliches Fragment mittels des kryptographisch sicheren Pseudozufallszahlengenerators erzeugt werden. Da ein solcher Pseudozufallszahlengenerator mittels einer Blockchiffre (beispielsweise AES [101]) realisiert werden kann, ist

der Rechenaufwand vernachlässigbar. Dies trifft insbesondere dann zu, wenn die Berechnung durch eine hardwareunterstützte Implementierung erfolgt.

Zusammenfassend kann geschlossen werden, dass der Rechenaufwand für das Elderberry Verfahren sehr gering ist. Im Vergleich zum SMART-ER Verfahren ist der hauptsächliche Mehraufwand der Überprüfung von wenigen Signaturen geschuldet. Werden diese mit Unterstützung von kryptographischer Hardware durchgeführt, ist der Mehraufwand gänzlich vernachlässigbar.

7.3.3 Speicheraufwand

Wie auch in Abschnitt 7.3.2 wird in diesem Abschnitt lediglich der Speicheraufwand des Elderberry Verfahrens selbst untersucht. Das verwendete Overlaynetz verursacht ebenfalls Speicheraufwand (beispielsweise für dessen Routingtabelle), der hier nicht näher betrachtet wird. Da peer-to-peer Overlaynetze auf eine Vielzahl von Teilnehmern ausgelegt sind (laut Jünemann et al. [71] erreichte die Kademlia-basierte Bittorrent DHT Anfang 2011 10 Millionen Teilnehmer) wächst der Aufwand nicht linear mit der Anzahl Teilnehmer sondern ist beschränkt oder wächst logarithmisch.

Durch das verwendete Teile- und Herrsche-Paradigma ist der Speicheraufwand in Elderberry sehr gering. Ein intelligenter Stromzähler, dem weder die Rolle Abschnittorganisator noch die Rolle Aggregator zufällt, muss nur den geringen Speicheraufwand des SMART-ER Verfahrens aufbringen.

Nimmt ein intelligenter Stromzähler die Rolle des Abschnittorganisators ein, so muss er die intelligenten Stromzähler seines Abschnitts verwalten. Er benötigt genügend Speicher um deren IP-Adressen vorzuhalten. Außerdem muss er die übermittelten maskierten Messwerte samt Abhängigkeitslisten zwischenspeichern bevor er die Abhängigkeitsauflösung und Aggregation durchführen kann. Da die Anzahl der intelligenten Stromzähler pro Abschnitt sehr gering ist, ist dieser Speicheraufwand mit nur wenigen Kilobyte, vernachlässigbar.

Nimmt ein intelligenter Stromzähler die Rolle eines Aggregators ein, so muss er nur wenig Speicher dafür vorhalten. Die eintreffenden Daten können auf denselben Wert aggregiert werden. Lediglich die Liste der beteiligten intelligenten Stromzähler wächst mit der Anzahl an Overlay-Aggregationen. Da nur wenige Overlay-Aggregationen sinnvoll sind, ist auch dieser Speicherbedarf mit wenigen Kilobyte realisierbar.

Unabhängig von der Rolle des intelligenten Stromzähler muss zur Realisierung des Ende-zu-Ende-Fragmentaustauschs der vom Messdienstleister gesetzte Initi-

alwert und ein Zähler gespeichert werden. Wird hierfür beispielsweise AES im Counter-Mode verwendet, so beträgt der Speicheraufwand einen AES-Schlüssel (16-32 Byte) und eine Zählvariable (4 Byte). Der resultierende Speicheraufwand ist vernachlässigbar.

Aus der Analyse des Speicheraufwandes folgt, dass durch die Dezentralität das Elderberry Verfahren mehr Zustand auf den intelligenten Stromzählern halten muss. Dies schlägt sich, verglichen mit SMART-ER, in einem höheren Speicheraufwand nieder. Dieser ist jedoch mit modernen eingebetteten Systemen problemlos.

7.3.4 Kommunikationsaufwand

Der Kommunikationsaufwand von Elderberry wird dominiert durch die Instandhaltung des Overlaynetzes. Das Kademlia Overlaynetz verursacht konstant einen geringen Kommunikationsaufwand zur Pflege der Routingtabellen. Dieser ist, insgesamt gerechnet, deutlich höher als der Kommunikationsaufwand der durch den Rest des Elderberry Verfahrens verursacht wird. In Abbildung 7.10 ist der beobachtete Kommunikationsaufwand während der Simulationen zur Skalierbarkeit des Verfahrens aus Abschnitt 7.3.1 abgebildet. Auf der x-Achse ist die Anzahl der simulierten intelligenten Stromzähler und auf der y-Achse der durchschnittliche Kommunikationsaufwand in Byte pro Sekunde eingezeichnet. Der verursachte Kommunikationsaufwand wurde in der Abbildung aufgeschlüsselt in den vom Overlaynetz verursachten Kommunikationsaufwand (unten) und den vom Rest des Elderberry Verfahrens verursachten Kommunikationsaufwand (oben).

Der Kommunikationsaufwand für das Overlaynetz wächst, wie bei strukturierten Overlaynetzen zu erwarten, logarithmisch in der Anzahl der intelligenten Stromzähler. Der durchschnittliche Kommunikationsaufwand für den Rest des Elderberry Verfahrens varriiert zwischen drei und fünf Byte pro Sekunde und wächst *nicht* mit der Anzahl intelligenter Stromzähler.

Der durchschnittliche Kommunikationsaufwand des Verfahrens ist für die angenommene Sendedatenrate der Kommunikationsanbindung der intelligenten Stromzähler problemlos. Jedoch verursacht Elderberry Schübe von Kommunikationsaufwand zu bestimmten Zeitpunkten des zeitlichen Ablaufs. Bei einer Betrachtung des durchschnittlichen Kommunikationsaufwands können diese nicht beurteilt werden. Diese wurden jedoch bereits beim Entwurf des Verfahrens berücksichtigt. So berücksichtigt die Berechnung der Abschnittanzahl (Abschnitt 7.1.6) bereits den Kommunikationsengpass des Abschnittorganisators. Bei der Diskussion der Overlay-Aggregation in Abschnitt 7.1.9 wurde bereits erläutert, dass diese

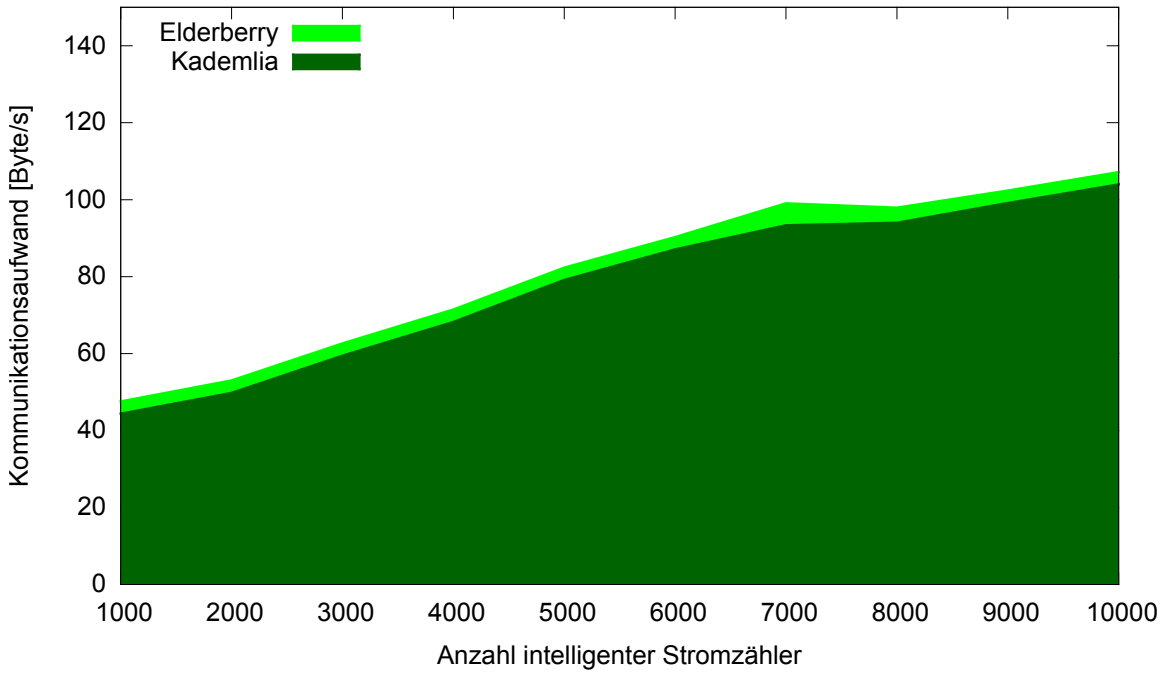


Abbildung 7.10: *Kommunikationsaufwand des Elderberry Verfahrens in Abhängigkeit der Anzahl intelligenter Stromzähler.*

nicht mehr als vier Schritte umfassen sollte um die Kommunikationsanbindung des intelligenten Stromzählers der die Rolle des Aggregators einnimmt zu schonen.

Es kann geschlossen werden, dass das Elderberry Verfahren einen höheren Kommunikationsaufwand verursacht als die in Kapitel 5 und Kapitel 6 vorgestellten Verfahren. Der Großteil dieses Kommunikationsaufwands entfällt dabei auf die Komponente des Overlaynetzwerks. Trotz des höheren Kommunikationsaufwands ist das Elderberry Verfahren mit der angenommenen Kommunikationsanbindung der intelligenten Stromzähler einsetzbar.

7.4 Zusammenfassung

In diesem Kapitel wurde das Elderberry Verfahren vorgestellt. Es realisiert ein privatsphärengerechtes Smart Metering mit dezentraler Aggregation. In diesem Verfahren stellt der Messdienstleister den einzelnen intelligenten Stromzählern nur Informationen über die Gesamtkonfiguration des durchzuführenden Smart

Meterings zur Verfügung. Die Organisation und Durchführung des Smart Meterings findet dann, ohne Einfluss durch den Messdienstleister, durch die intelligenten Stromzählern selbst statt. Hierzu wird ein strukturiertes Overlaynetzwerk mit Key-based Routing verwendet.

Das Verfahren verwendet das Teile- und Herrsche-Paradigma indem es die Menge der teilnehmenden intelligenten Stromzähler in Teilmengen, sogenannte Abschnitte, aufteilt. Diese Aufteilung geschieht dezentral unter Verwendung der Identitäten der intelligenten Stromzähler und einer externen Variablen, in dieser Arbeit dem Datum. Durch die Einbeziehung einer Variablen wird die Aufteilung in Teilmengen regelmäßig, in sogenannten Epochen, neu durchgeführt. Dies schließt aus, dass ein intelligenter Stromzähler dauerhaft von einer für ihn möglicherweise nachteiligen Einteilung in Teilmengen betroffen ist.

Innerhalb jedes Abschnitts nimmt ein intelligenter Stromzähler die Rolle des Abschnittorganisators ein und führt das aus Kapitel 5 bekannte SMART-ER Verfahren innerhalb des Abschnitts durch. Somit wird, pro Abschnitt, privatsphärengerechtes Smart Metering durchgeführt.

Nachdem abschnittweise Smart Metering Ergebnisse vorliegen, kann das Elderberry Verfahren diese Ergebnisse weiter aggregieren. Hierzu nehmen einzelne intelligente Stromzähler die Rolle eines sogenannten Aggregators ein. Aggregatoren sind in einer Baumstruktur organisiert und empfangen Daten von ihren Kindern. Diese können entweder Abschnittorganisatoren oder bereits andere Aggregatoren sein. Nach einer konfigurierbaren Anzahl an Aggregationen werden die Ergebnisse dann an den Messdienstleister weitergeleitet.

Die privatsphärenrelevanten Teile des Elderberry Verfahrens bauen auf dem SMART-ER Verfahren auf. Für den Privatsphärenschutz gelten daher dieselben Garantien. Ein wesentlicher Unterschied besteht jedoch darin, dass in Elderberry der Abschnittorganisator die Rolle des Messdienstleisters einnimmt. Mit Hilfe eines Ende-zu-Ende-Fragmentaustauschs wird gewährleistet, dass ein Abschnittorganisator keine Kenntnis der Aggregate einzelner Gruppen erhält und auch nicht, unabhängig vom Messdienstleister, einen Angriff mittels korrumpierter intelligenter Stromzähler durchführen kann. Elderberry gewährt also, genau wie SMART-ER und Smart Meter Speeddating, einen vollständigen Schutz der Privatsphäre bei nicht korrumpiertem Messdienstleister.

Für einen Angriff mit korrumpiertem Messdienstleister muss der Angreifer erreichen, dass die Rolle des Abschnittorganisators durch einen korrumpierten intelligenten Stromzähler eingenommen wird und dass weitere korrumpierte intelligenten Stromzähler im Abschnitt des Angriffsziels vorhanden sind. Der

Mechanismus zur Einteilung der intelligenten Stromzähler in Abschnitte verhindert aber eine aktive Platzierung von korrumpierten intelligenten Stromzählern. Die Voraussetzungen für einen Angriff können nur probabilistisch erreicht werden und es erfordert einen immensen Vorrat an korrumpierten intelligenten Stromzählern um eine hohe Erfolgschance zu haben.

Die Evaluation der Leistung des Elderberry Verfahrens zeigte eine sehr gute Skalierbarkeit in der Anzahl der intelligenten Stromzähler. Dabei konnte Elderberry eine Leistung erreichen, die mit einem vergleichbar konfigurierten SMART-ER-Verfahren vergleichbar oder besser ist. Im Gegensatz zu Smart Meter Speeddating kann Elderberry auch mit sehr kurzen Messintervallen eingesetzt werden und gewährt durch die große Anzahl ein einfließenden Messwerten pro (dem Messdienstleister gesendeten) Aggregat einen sehr guten Privatsphärenschutz der Gruppe. Diese Werte erreicht Elderberry bei geringem Rechen- und Speicheraufwand. Der Kommunikationsaufwand ist, bedingt durch die Instandhaltung des verwendeten Overlaynetzwerks, höher als bei den zuvor vorgestellten Verfahren. Mit durchschnittlich wenigen hundert Byte pro Sekunde ist er jedoch immernoch problemlos mit der angenommenen Datenrate realisierbar.

Kapitel 8

Zusammenfassung und Ausblick

Die Weiterentwicklung des klassischen Stromnetzes zum Smart Grid ist ein immenses Unterfangen, das durch den steigenden Einsatz regenerativer Energien an Dringlichkeit gewonnen hat. Langfristig nur schlecht einplanbare Energiequellen wie Windenergie und Solarenergie stellen hohe Ansprüche an ein Stromnetz, das dynamisch auf die sich ändernden Verhältnisse reagieren muss. Eine wichtige Schlüsselfunktion des Smart Grid ist das Smart Metering: intelligente Stromzähler, die den Energieverbrauch in kurzen Abständen messen und an einen Messdienstleister senden. Mittels dieser zeitlich aktuellen Informationen kann flexibel auf sich ändernden Energiebedarf reagiert werden.

Doch den Vorteilen des Smart Meterings steht eine Gefahr für die Privatsphäre gegenüber. Die vom Smart Metering erhobenen Daten können analysiert werden und eröffnen einen umfassenden Einblick in die Haushalte: Anzahl der Bewohner, Arbeitszeiten, Urlaube, Gewohnheiten, Haushaltsgeräte und selbst das abendliche Fernsehprogramm können daraus geschlossen werden. Das Forschungsgebiet des privatsphärengerechten Smart Meterings beschäftigt sich mit Lösungen, die weiterhin die Vorteile des Smart Meterings bieten, aber die Privatsphäre schützen. Ein genereller Ansatz ist die Aggregation von Messdaten über mehrere Haushalte hinweg. Die resultierenden, aggregierten Daten liefern weiterhin wertvolle Informationen über die aktuelle Verbrauchssituation, stellen aber keine Gefahr mehr für die Privatsphäre einzelner Haushalte dar.

Die privatsphärengerechte Aggregation der Messdaten stellt eine große Herausforderung dar. Insbesondere dann, wenn keine vertrauenswürdige dritte Partei hinzugezogen werden soll oder kann. Bestehende Arbeiten zu diesem Themenge-

biet verwenden häufig rechenintensive, kryptologische Methoden und lassen dabei außer Acht, dass ein intelligenter Stromzähler nur über sehr beschränkte Ressourcen verfügt. Untersuchungen, ob die vorgeschlagenen Verfahren mit beschränkten Ressourcen realisierbar sind, fehlen gänzlich. Auch ein realistisches Angreifermodell, das auch den Messdienstleister umfasst, lassen viele Arbeiten vermissen. Ebenfalls wurde bisher nicht betrachtet, inwiefern Störungen der Kommunikationsanbindung der intelligenten Stromzähler Auswirkungen auf die Leistungsfähigkeit des Smart Meterings haben. Möglichst geringe Auswirkungen der Störungen auf die Leistungsfähigkeit stellen aber eine wichtige Eigenschaft für den realen Einsatz dar.

Aus diesen Gründen wurden in dieser Arbeit Verfahren zum privatpshärengerechten Smart Metering ohne vertrauenswürdige dritte Partei entworfen und untersucht. Wichtige Punkte beim Entwurf waren:

- Realisierbarkeit auf ressourcenbeschränkter Hardware.
- Schutz der Privatsphäre auch bei Angriffen von Außenstehenden und bei Angriffen durch den Messdienstleister.
- Weitestgehender Funktionserhalt bei Störungen der Kommunikationsanbindung der intelligenten Stromzähler.

Zur Evaluation der entworfenen Verfahren wurde mit *OverGrid* ein Simulationswerkzeug auf Basis des Overlay-Frameworks *OverSim* entwickelt.

Die Schwerpunkte der Dissertation lassen sich in folgende Punkte gliedern:

- Entwurf eines Verfahrens zum peer-to-peer Privatsphärenschutz.
- Entwurf eines Verfahrens zur dezentralen Gruppenbildung.
- Entwurf eines Verfahrens zur dezentralen Aggregation.
- Evaluation von Rechen-, Speicher- und Kommunikationsaufwand der entworfenen Verfahren.
- Evaluation des Privatsphärenschutzes, der durch die entworfenen Verfahren erreicht wird.
- Evaluation der Leistungsfähigkeit der entworfenen Verfahren bei Störungen der Kommunikationsanbindung.

8.1 Ergebnisse der Arbeit

Das vorgestellte Verfahren zum peer-to-peer Privatsphärenschutz, *SMART-ER*, zeichnet sich durch einen sehr geringen Ressourcenverbrauch und hervorragenden Privatsphärenschutz aus. Wie in der Evaluation gezeigt wurde, genügen nur wenige Kilobyte an zu übertragenden Daten pro Messintervall zur Durchführung des Smart Meterings. Ein Angriff auf die Privatsphäre eines Haushalts ohne Kooperation des Messdienstleisters, also von Außen, ist ausgeschlossen. Auch wenn der Messdienstleister mit einem Angreifer kooperiert genügt die Kooperation mit einem einzelnen, nicht mit dem Angreifer kooperierenden, intelligenten Stromzähler um den Schutz der Privatsphäre eines Haushalts zu garantieren. Um eine hohe Leistungsfähigkeit bei Störungen der Kommunikationsanbindung der intelligenten Stromzähler zu erreichen, verwendet SMART-ER eine Partitionierung der beteiligten intelligenten Stromzähler in Gruppen. Hierdurch konnte mit SMART-ER eine Leistungsfähigkeit erreicht werden, die bei kleiner Gruppengröße und der angenommenen Zuverlässigkeit der Kommunikationsanbindung nur wenig unter der maximal erreichbaren Leistung liegt. Die Leistung wurde anhand der Smart Metering Reichweite bewertet. Sie bezeichnet den Anteil der am Smart Metering teilnehmenden intelligenten Stromzähler, der tatsächlich im Rahmen des Smart Metering einen Messwert liefern konnte. Ein Verfahren ohne Privatsphärenschutz erreichte eine Reichweite von 99,51% der intelligenten Stromzähler. SMART-ER erreichte mit 99,47% der intelligenten Stromzähler nur eine geringfügig kleinere Reichweite.

Erachtet man den Messdienstleister als vertrauenswürdig, so wurde mit SMART-ER ein Verfahren vorgestellt, das alle Ansprüche an ein privatsphärengerechtes Smart Metering Verfahren erfüllt und im Vergleich zu einem nicht privatsphärengerechten Verfahren nur sehr wenige Einbußen hat (0,04 Prozentpunkte). Da in dieser Arbeit jedoch das Angreifermodell einen Messdienstleister vorsieht, der mit dem Angreifer kooperiert, bildet die Gruppeneinteilung durch den Messdienstleister eine Schwachstelle. Der Messdienstleister kann durch gezielte Zuteilung von korrumpierten intelligenten Stromzählern die Privatsphäre eines Haushaltes angreifen. Mit einer größeren Gruppengröße kann der Bedarf an korrumpierten intelligenten Stromzählern zwar gesteigert werden, aber dies wirkt sich negativ auf die Smart Metering Leistung aus. Diese Schwachstelle wurde mit dem Verfahren zur dezentralen Gruppenbildung und mit dem Verfahren zur dezentralen Aggregation behandelt.

Das vorgestellte Verfahren zur dezentralen Gruppenbildung, *SMSD*, ermöglicht eine Einteilung der intelligenten Stromzähler in Kleingruppen ohne Einflussnahme durch den Messdienstleister. Die Gruppeneinteilung der intelligenten Stromzähler wird zufällig und für jedes Messintervall von Neuem organisiert. Zum Schutz der Privatsphäre verwendet es das SMART-ER Verfahren als Baustein und kann daher die gleichen Garantien liefern. Insbesondere ist auch bei SMSD ein Angriff ohne Mitwirken des Messdienstleisters ausgeschlossen. Mittels einer Kooperation mit dem Messdienstleister kann SMSD angegriffen werden. Die zufällige Gruppeneinteilung erfordert vom Angreifer jedoch den Besitz einer sehr großen Anzahl an korrumpierten intelligenten Stromzählern (beispielsweise 10% der Gesamtzahl) um pro Messintervall eine hohe Erfolgswahrscheinlichkeit zu haben (bei 10% korrumpierter Stromzähler beträgt diese 50%). Zusätzlich geht der Angreifer ein sehr hohes Risiko einer Entdeckung ein, da ein erfolgreicher Angriff ein statistisch stark anomales Verhalten erzeugt, das jeder intelligente Stromzähler eigenständig erkennen kann.

SMSD hat auch unter Störungen der Kommunikationsanbindung eine hohe Leistung, die etwas niedriger als SMART-ER ausfällt. Mit einer durchschnittlichen Reichweite von 99, 35% liegt SMSD 0, 16 Prozentpunkte unter einem Verfahren ohne Privatsphärenschutz. Die Realisierbarkeit von SMSD mit ressourcenbeschränkter Hardware wurde mittels einer Implementierung für Sensornetze nachgewiesen.

Die dezentrale Gruppenbildung von SMSD benötigt jedoch eine gewisse Zeit um die Gruppen zu bilden. Diese liegt im Bereich von wenigen Minuten. Da die Gruppenbildung in jedem Messintervall von neuem durchgeführt wird, muss mindestens diese Zeit zwischen zwei Messintervallen liegen. Für das häufig angenommene Messintervall von 15 Minuten ist SMSD problemlos einsetzbar. Für deutlich kürzere Messintervalle, beispielsweise unter einer Minute, ist SMSD nicht geeignet.

Die hohe Smart Metering Leistung wird in SMSD durch eine kleine Gruppengröße erreicht. Die dabei entstehenden Aggregate bieten für einzelne Messintervalle Einblicke in den aggregierten Energieverbrauch weniger Haushalte. Wird dies bereits als Eingriff in die Privatsphäre betrachtet, muss ein Verfahren mit einer größeren Gruppengröße verwendet werden.

Das Elderberry-Verfahren wurde daher als Alternative zu SMSD entworfen. Es verwendet das teile und herrsche Paradigma um die intelligenten Stromzähler mittels eines Overlaynetzes in Abschnitte zu organisieren. Die Einteilung der intelligenten Stromzähler in Abschnitte ist nicht vom Messdienstleister beeinflussbar und wird regelmäßig (in dieser Arbeit täglich) erneuert. Innerhalb jedes Abschnitts

führt Elderberry dann das SMART-ER Verfahren ausschließlich mittels teilnehmender intelligenter Stromzähler durch. Es bietet damit eine dezentrale Aggregation über eine große Anzahl an Haushalten. Trotz dezentraler Aggregation gewährleistet auch das Elderberry Verfahren, dass ein Angriff nur mit Kooperation des Messdienstleisters möglich ist. Auch mit Kooperation des Messdienstleister und einem sehr hohen Anteil von korrumpierten intelligenten Stromzählern ist nur eine geringe Erfolgswahrscheinlichkeit erzielbar.

Bedingt durch den dezentralen Ansatz erreicht das Elderberry Verfahren nicht die Leistung von SMSD. Mit einer durchschnittlichen Reichweite von 99,02% liegt Elderberry 0,49 Prozentpunkte unter einem Verfahren ohne Privatsphärenschutz. Vergleicht man die Smart Metering Leistung des Elderberry Verfahrens mit der Leistung von SMART-ER bei gleicher Anzahl Haushalte pro Aggregat, so erreicht Elderberry jedoch eine vergleichbare oder bessere Leistung.

Im Vergleich mit SMSD weist Elderberry einen höheren Kommunikationsaufwand auf. Mit ungefähr 100 Kilobyte pro Messintervall pro intelligentem Stromzähler bei 10 000 Stromzählern insgesamt ist dieser aber problemlos von der angenommenen Kommunikationsanbindung handhabbar. Vom Gesamtvolumen entfallen dabei 97% auf das verwendete Overlaynetz und lediglich ein kleiner Anteil auf den eigentlichen Teil des Smart Meterings.

Alle in dieser Arbeit vorgestellten Verfahren stellen bei vertrauenswürdigem Messdienstleister einen Schutz der Privatsphäre sicher. Für SMSD und Elderberry gilt, dass auch bei korrumpiertem Messdienstleister ein Angriff auf die Privatsphäre einzelner Haushalte nur unter Einsatz von zahlreichen korrumpierten intelligenten Stromzählern oder mit hohem Entdeckungsrisiko durchführbar ist.

Die erstmalige Untersuchung von Verfahren zum privatsphärengerechten Smart Metering auf Robustheit bei Störungen der Kommunikationsanbindung liefert wertvolle Informationen zur Beurteilung eines Einsatzes dieser Verfahren im realen Stromnetz.

Neben den Aussagen, die über die einzelnen vorgestellten Verfahren getroffen werden konnten, liefert diese Arbeit Antworten auf bisher offene, wichtige Fragen des privatsphärengerechten Smart Meterings:

- Privatsphärengerechtes Smart Metering kann auch mit ressourcenbeschränkter Hardware und mit niedrigen Datenraten durchgeführt werden.

- Auch bei Störungen der Kommunikationsanbindung der intelligenten Stromzähler kann mittels privatsphärengerechtem Smart Metering eine Leistung

erzielt werden, die nur geringfügig unter der eines nicht privatsphärengerechten Verfahrens liegt.

8.2 Weiterführende Arbeiten

Ein Aspekt, der in dieser Arbeit nicht betrachtet wurde, ist die rechtliche Situation dieser Form des Smart Meterings. Durch den Verzicht auf eine vertrauenswürdige dritte Partei wird ein Teil des Dienstes Smart Metering durch eine Kooperation der intelligenten Stromzähler untereinander erbracht. Im Falle von Elderberry sogar ein Großteil. Inwiefern diese Form der Diensterbringung vom Rechtsrahmen abgedeckt ist, war nicht Gegenstand dieser Arbeit. Die Beantwortung dieser Frage stellt jedoch ein wichtige Voraussetzung für den realen Einsatz von privatsphärengerechten Smart Metering Verfahren dar.

Auch wurden einzelne technische Probleme, die beim realen Einsatz der Verfahren auftreten können, nicht betrachtet. Die direkte Kommunikation zwischen intelligenten Stromzählern kann durch den verbreiteten Einsatz von Network Address Translation (NAT) bei Heimanschlüssen oder Firewalls behindert werden. Ebenfalls stellt die Versorgung von intelligenten Stromzählern mit Schlüsselmaterial zur Sicherung der Vertraulichkeit, Integrität und Authentizität einer Kommunikationsverbindung ein aktives Forschungsfeld dar.

Bei der Untersuchung des Elderberry Verfahrens zeigte sich, dass ein Großteil des Kommunikationsaufwands auf das verwendete, generische Overlaynetzwerk entfiel. Ein speziell auf die Anforderungen des Smart Meterings zugeschnittenes Overlaynetzwerk könnte den Kommunikationsaufwand möglicherweise reduzieren. Aufgrund der Komplexität des Themenfeldes wurde dieser Ansatz in dieser Arbeit nicht in Erwägung gezogen.

In dieser Arbeit wurde als Grundannahme von einer Kommunikationsanbindung der intelligenten Stromzähler per DSL des Haushalts ausgegangen. Die Evaluation der vorgestellten Verfahren zeigt, dass diese für den niedrigen Kommunikationsaufwand der Verfahren mehr als ausreichend ist. Ist kein DSL verfügbar, so wäre auch der Einsatz der Verfahren mit anderen Kommunikationstechnologien, beispielsweise mittels Mobilfunk, möglich. Ein Mischbetrieb von Kommunikationsanbindungen, bei denen sich einzelne Charakeristika (Datenrate, Latenz, Zuverlässigkeit) um Größenordnungen unterscheiden könnte jedoch, besonders für die Gruppenbildung des SMSD Verfahrens, eine Herausforderung darstellen. Auch könnte der Einsatz von Powerline-Kommunikation, der Kommunikation über das Stromnetz selbst, mit

ihrer Fähigkeit zum Broadcast und der Orientierung an der Stromnetzarchitektur interessante Herausforderungen und Möglichkeiten bieten.

Anhang A

Glossar

Abgabewert Privatsphärengerecht vorverarbeiteter Wert, der in SMART-ER an den Messdienstleister gesendet wird.

Abschnitt Partition des Overlay-ID-Raums in Elderberry.

Abschnittorganisator Rolle innerhalb von Elderberry, die innerhalb eines Abschnitts die Aufgaben des Messdienstleisters für SMART-ER erfüllt.

Advanced Metering Infrastructure (AMI) Häufig synonym benutzter Begriff für Smart Metering.

Churn Die Fluktuation der Verfügbarkeit von Teilnehmern einer Kommunikation bedingt durch Störungen der Teilnehmer oder deren Kommunikationsanbindung.

Annahmeroutine Subroutine von Smart Meter Speeddating, die eine zufällige Annahme eines anfragenden intelligenten Stromzählers ermöglicht.

AO-Punkt Overlay-ID in jedem Abschnitt bei Elderberry. Sie bestimmt den Abschnittorganisator.

Demand Side Management (DSM) Steuern von im Haushalt befindlichen Energieerzeugern und Energieverbrauchern von außen, beispielsweise durch den Energieversorger.

Energiehändler Kauft und verkauft Energie am Energiemarkt und an und von Endverbrauchern.

Energieversorger Wickelt den Bezug von Energie für seine Kunden (Haushalte und Endverbraucher) ab.

Epoche Dauer der Gültigkeit der Overlay-IDs in Elderberry. Overlay-IDs werden nach jeder Epoche gewechselt (hier: ein Tag).

Fragment Zufälliger Wert, mit dem ein Messwert maskiert werden kann. Mittels Fragmenten kann aus einem Messwert ein Abgabewert ermittelt werden.

Fragmentaustausch Das Sende und Empfangen von Fragmenten zwischen mehreren Parteien.

Gruppenbildung Mechanismus zur Bestimmung einer Partitionierung der Zielgruppe in disjunkte Teilmengen, sogenannte Gruppen.

Intelligenter Stromzähler Stromzähler mit Möglichkeit zur bidirektionalen Kommunikation mit dem Messdienstleister oder anderen intelligenten Stromzählern.

Kommunikationsaufwand Aufwand, der für die Kommunikation unter intelligenten Stromzählern oder mit dem Messdienstleister in einem Smart Metering Verfahren anfällt.

Maskierungsdaten Daten, die unter intelligenten Stromzählern ausgetauscht werden, um Messwerte zu maskieren. In SMART-ER werden diese Fragmente genannt.

Messintervall Der zeitliche Abstand zwischen zwei durchgeführten Messungen im Smart Metering.

Messdienstleister Liest intelligente Stromzähler aus oder bekommt von diesen Messwerte zugesandt. Vermittelt Ergebnisse an eigentliche Interessenten, beispielsweise Energieversorger.

Messgröße Die physikalische Größe, die das Ziel der Messung im Smart Metering ist. Beispielsweise der Stromverbrauch seit der letzten Messung.

Messwert Wert, der durch eine Messung der Messgröße entsteht.

Messzeitpunkt Der Zeitpunkt, zu dem ein Messwert gemessen wird.

Overlay-Aggregation Mechanismus in Elderberry zur weiteren Aggregatbildung nach der abschnittweisen Durchführung von SMART-ER.

Overlaynetz Abstraktion von dem eigentlichen Kommunikationsnetz in einem peer-to-peer System.

Overlay-ID Eindeutiger Identifikator eines Teilnehmers oder eines Datums in einem Overlaynetz.

Paarung Eine Zweiergruppe von intelligenten Stromzählern in Smart Meter Speeddating.

Phasor Measurement Unit (PMU) Messgerät zur Ermittlung detaillierter Daten über Stromflüsse und Stromqualität. Wird im Stromnetz und nicht im Haushalt eingesetzt.

Promiscuous Sybil Ein Angriff auf die Suchroutine des Smart Meter Speeddating Verfahrens.

Rechenaufwand Aufwand der für Berechnungen in einem Smart Metering Verfahren anfällt.

Smart Metering Instanz Eine konkrete Anwendung von Smart Metering. Bestimmt Zielgruppe, Messgröße und Messintervall.

Smart Metering Latenz (SM-Latenz) Die Zeit, die zwischen Messung der Messgröße und Eintreffen des Messwertes beim Messdienstleister vergeht.

Smart Metering Reichweite (SM-Reichweite) Der Anteil der Zielgruppe, für den der Messdienstleister nach einer Messung (und der SM-Latenz) Messwerte erhält.

Speicheraufwand Aufwand, der zur Speicherung von Daten auf intelligenten Stromzählern während eines Smart Metering Verfahrens aufgewendet werden muss.

Suchroutine Subroutine von Smart Meter Speeddating, die eine zufällige Wahl eines anderen intelligenten Stromzählers ermöglicht.

Kürzestes Smart Metering Intervall (SM-Intervall) Das kürzeste Messintervall, das mittels der eingesetzten Technik realisierbar ist.

Variable Tarife Abrechnungsmodelle für den Bezug von Energie, die keinen festen Preis pro bezogener Einheit enthalten.

Zielgruppe Die Menge der intelligenten Stromzähler, die in einer Instanz eines Smart Meterings betrachtet werden.

Anhang B

Weitere Ergebnisse zur Evaluation von Smart Meter Speeddating

B.1 SMSD mit $g_{max} > 3$

Im Folgenden werden die Simulationsergebnisse zur Voruntersuchung von Smart Meter Speeddating bezüglich des Parameters g_{max} dargestellt. Zunächst wurden für variierendes g_{max} verschiedene Parameterkonfigurationen von m_{max} und a_{max} auf ihren Anteil valider Abgabewerte unter Churn untersucht. Die verwendeten Parameterkonfigurationen sind in Tabelle B.1 aufgelistet.

Es wurden ebenfalls Parameterkonfigurationen mit, relativ zu m_{max}, kleinerem a_{max} betrachtet. Die verwendeten Parameterkonfigurationen sind in Tabelle B.2 aufgelistet. Zur Darstellung wurde hier eine Abhängigkeit von g_{max} verwendet.

Tabelle B.1: *Parameterkonfigurationen für Simulationen zum Einfluss von g_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$
	in Kombination
a_{max}	$\overbrace{\{3, 5, 10, 15, 20\}}$
s	entsprechend Tabelle 6.6
	$\{100, 180, 220, 280, 320\}$

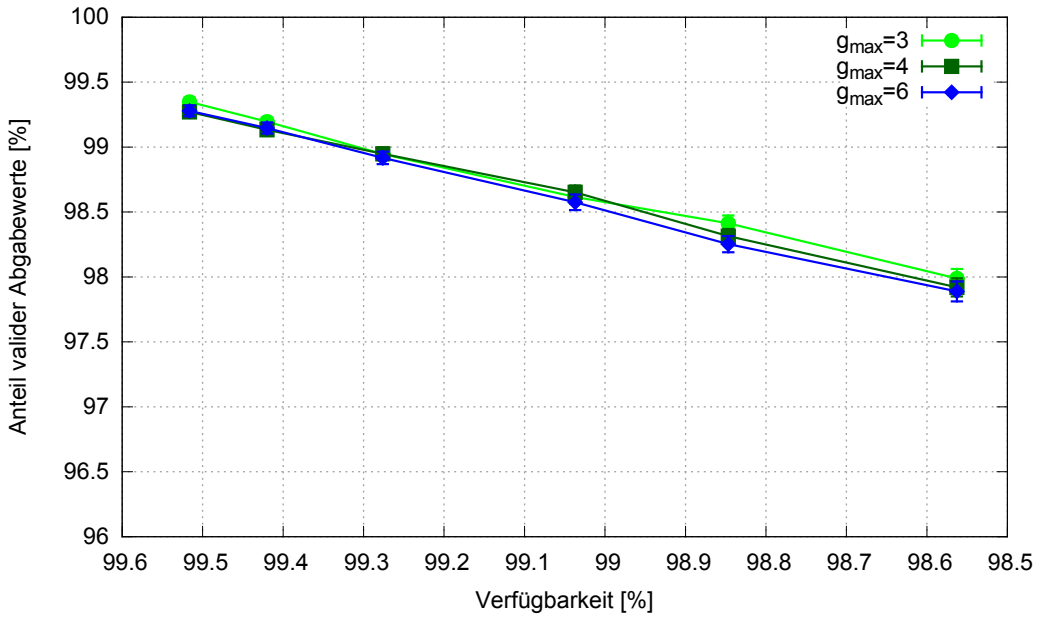


Abbildung B.1: *Anteil valider Abgabewerte in Abhängigkeit der Verfügbarkeit bei unterschiedlichem g_{max} und für $m_{max} = 5$.*

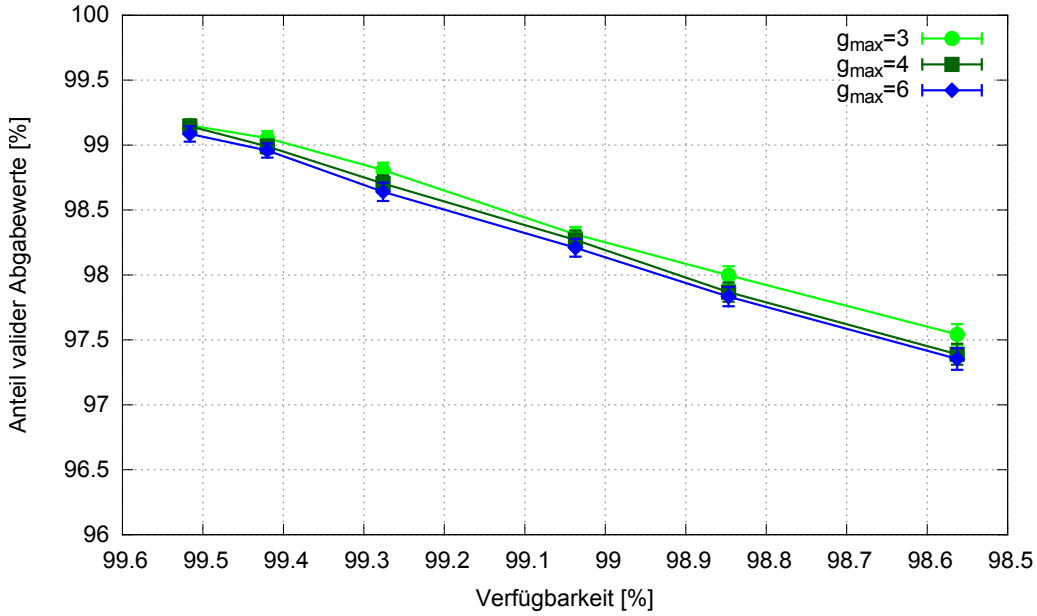


Abbildung B.2: *Anteil valider Abgabewerte in Abhängigkeit der Verfügbarkeit bei unterschiedlichem g_{max} und für $m_{max} = 10$.*

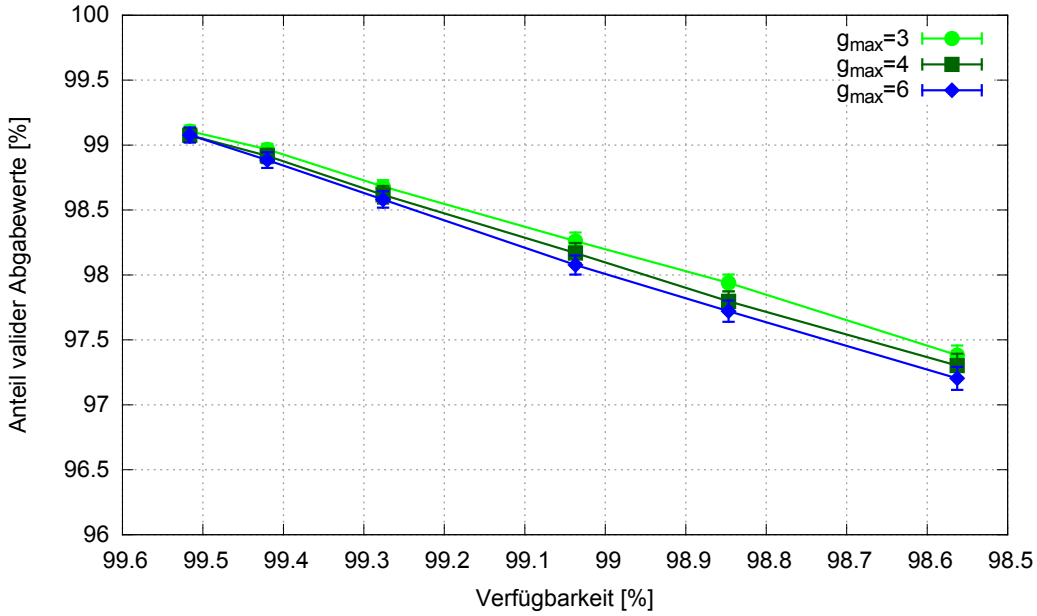


Abbildung B.3: *Anteil valider Abgabewerte in Abhängigkeit der Verfügbarkeit bei unterschiedlichem g_{max} und für $m_{max} = 15$.*

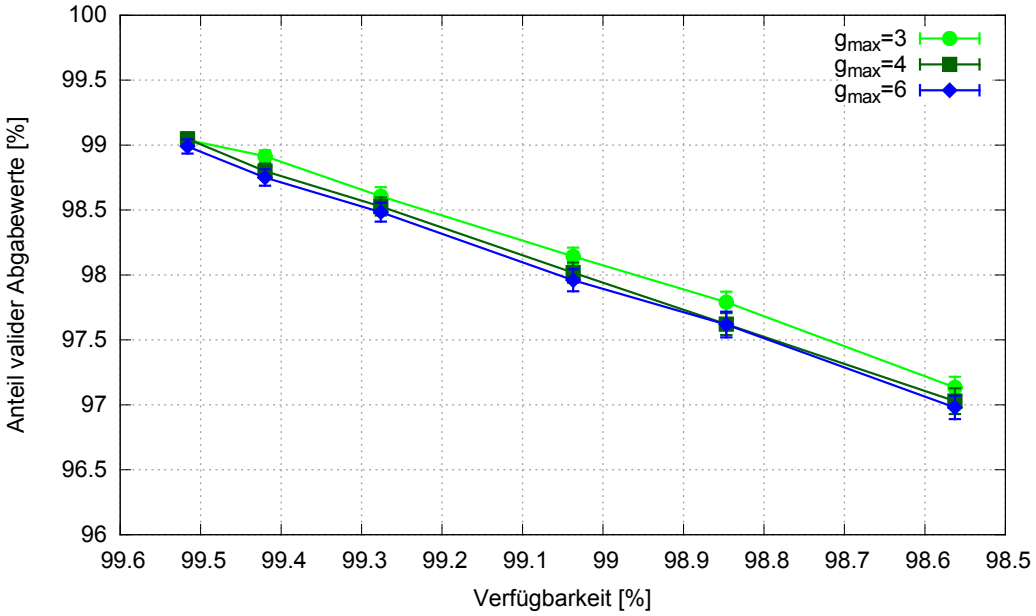


Abbildung B.4: *Anteil valider Abgabewerte in Abhängigkeit der Verfügbarkeit bei unterschiedlichem g_{max} und für $m_{max} = 20$.*

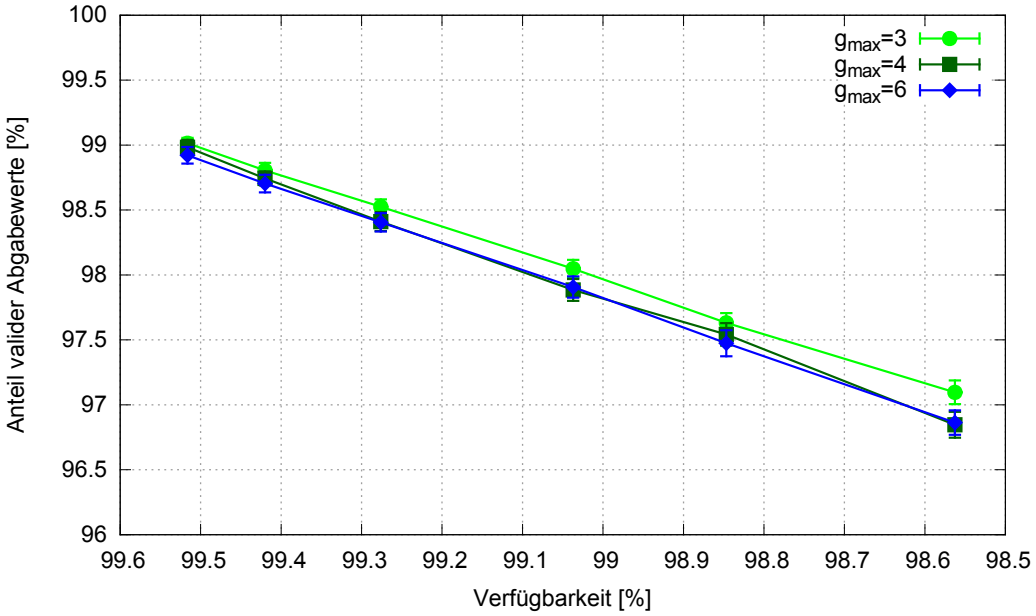


Abbildung B.5: *Anteil valider Abgabewerte in Abhängigkeit der Verfügbarkeit bei unterschiedlichem g_{max} und für $m_{max} = 20$.*

Tabelle B.2: *Parameterkonfigurationen für Simulationen zum Einfluss von g_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
m_{max}	$\underbrace{\{5, 10, 15, 20, 25\}}$
	in Kombination
a_{max}	$\overbrace{\{3, 3, 7, 13, 15\}}$
s	entsprechend Tabelle 6.6
	$\{100, 180, 220, 280, 320\}$

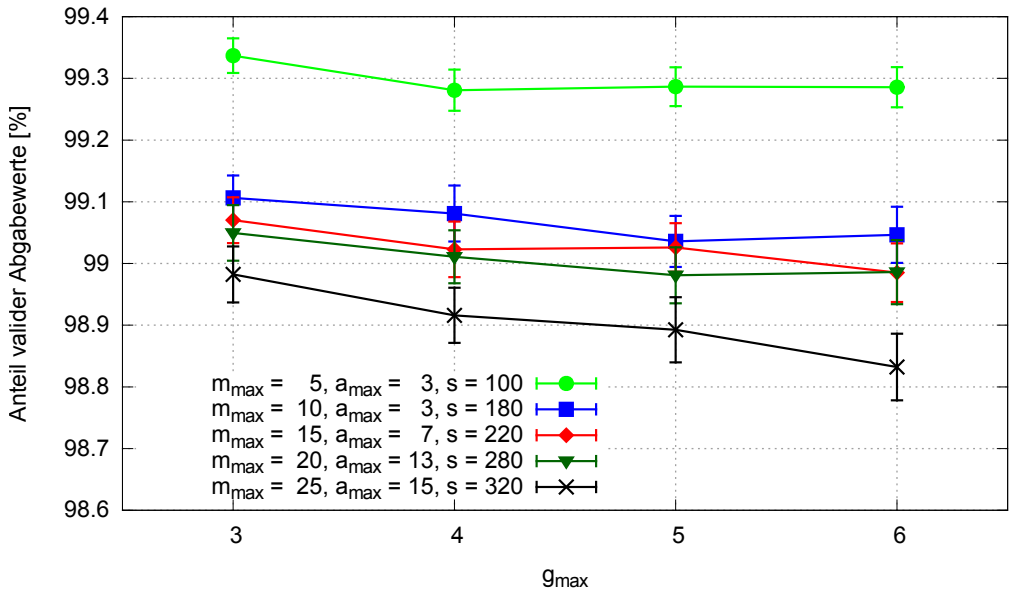


Abbildung B.6: *Anteil valider Abgabewerte in Abhängigkeit von g_{max} für Konfigurationen von m_{max} und a_{max}.*

B.2 Einfluss von a_{max} bei festem m_{max}

Im Folgenden sind weitere Ergebnisse zu Abschnitt 6.3.2 mit $m_{max} = 15$ und $m_{max} = 25$, sowie die Abbildungen von $m_{max} = 20$ mit eingezeichnetem $a_{max} = 10$ dargestellt.

Tabelle B.3: *Parameterkonfigurationen für Simulationen zum Einfluss von* $a_{max} = 15$ *bei festem* m_{max}.

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{5, 10, 20, 30, \ldots, 60, 80, 100, \ldots, 300\}$
t_{max}	1 Sekunde
m_{max}	15
a_{max}	$\{5, 10, 15, 20, 30\}$

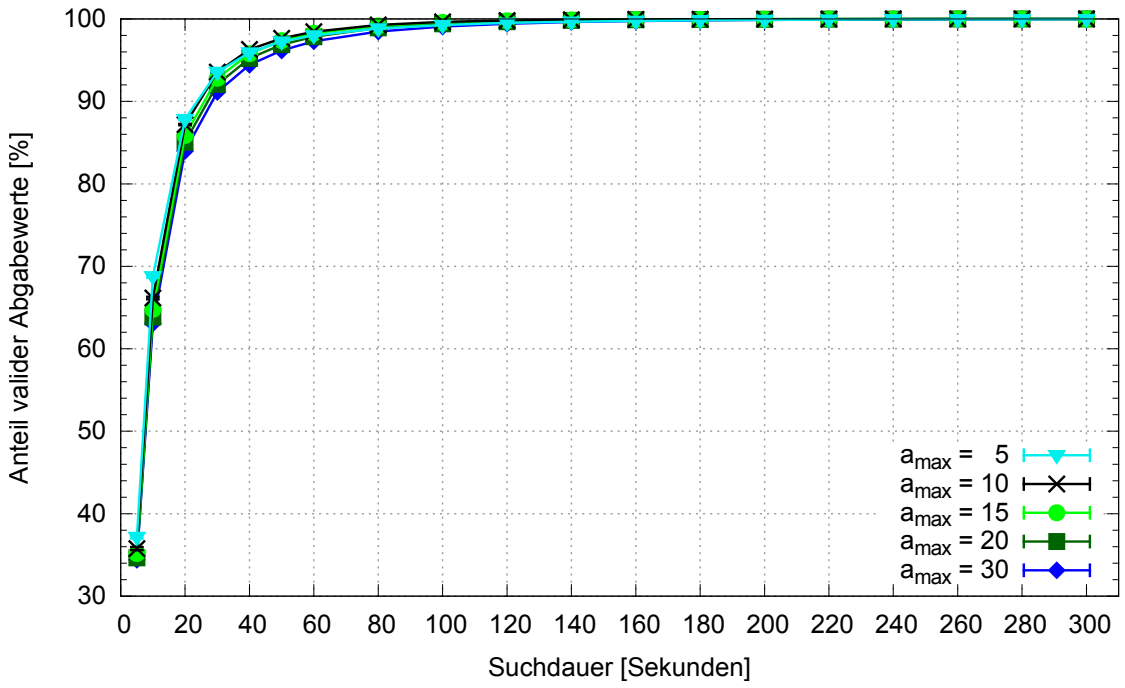
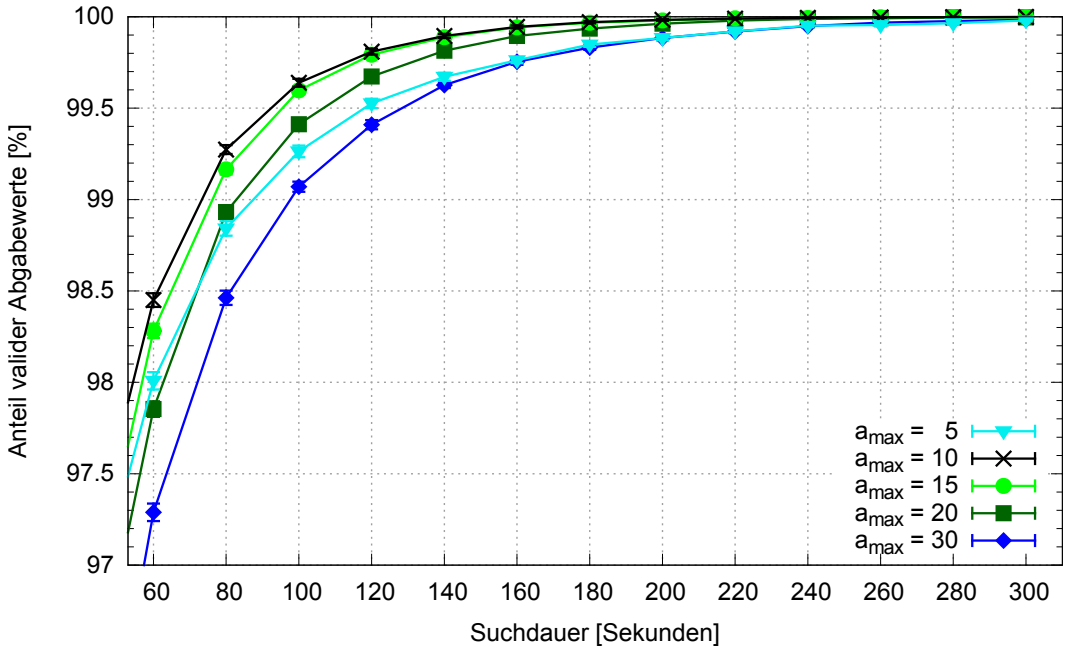
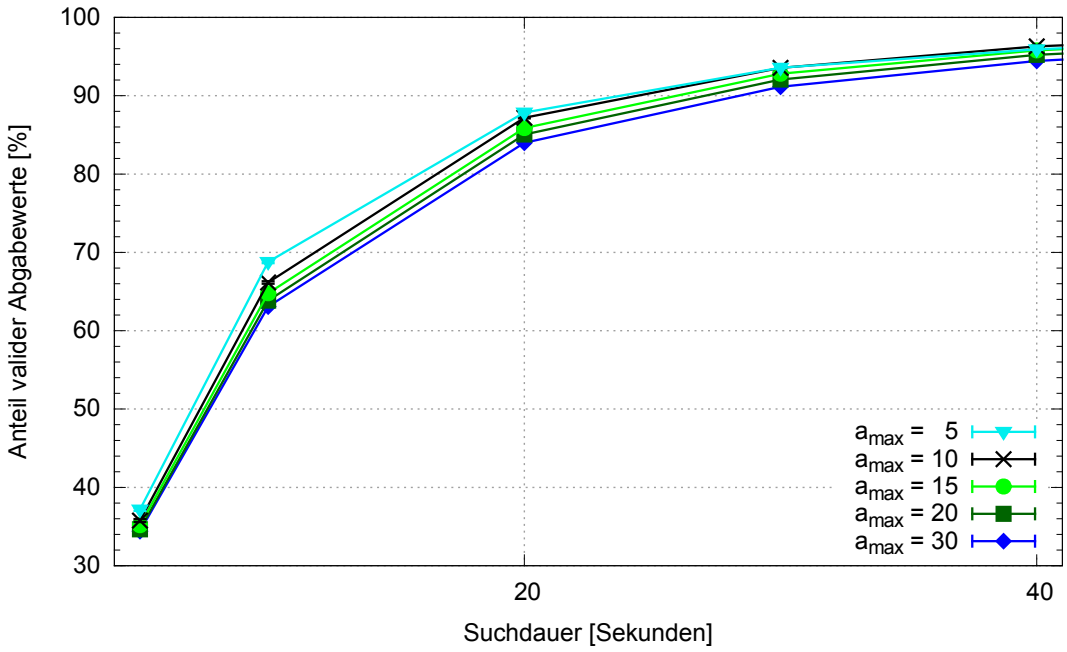


Abbildung B.7: *Anteil valider Abgabewerte bei* $m_{max} = 15$ *und variierendem* a_{max}.



(a) *Detailbetrachtung von* 40 *bis* 300 *Sekunden.*



(b) *Detailbetrachtung von* 5 *bis* 40 *Sekunden.*

Abbildung B.8: *Detailbetrachtungen der Anteile valider Abgabewerte bei* $m_{max} = 15$ *und variierendem* a_{max}.

Tabelle B.4: *Parameterkonfigurationen für Simulationen zum Einfluss von $a_{max} = 20$ bei festem m_{max}.*

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{5, 10, 20, 30, \ldots, 60, 80, 100, \ldots, 300\}$
t_{max}	1 Sekunde
m_{max}	20
a_{max}	$\{5, 10, 15, 20, 30\}$

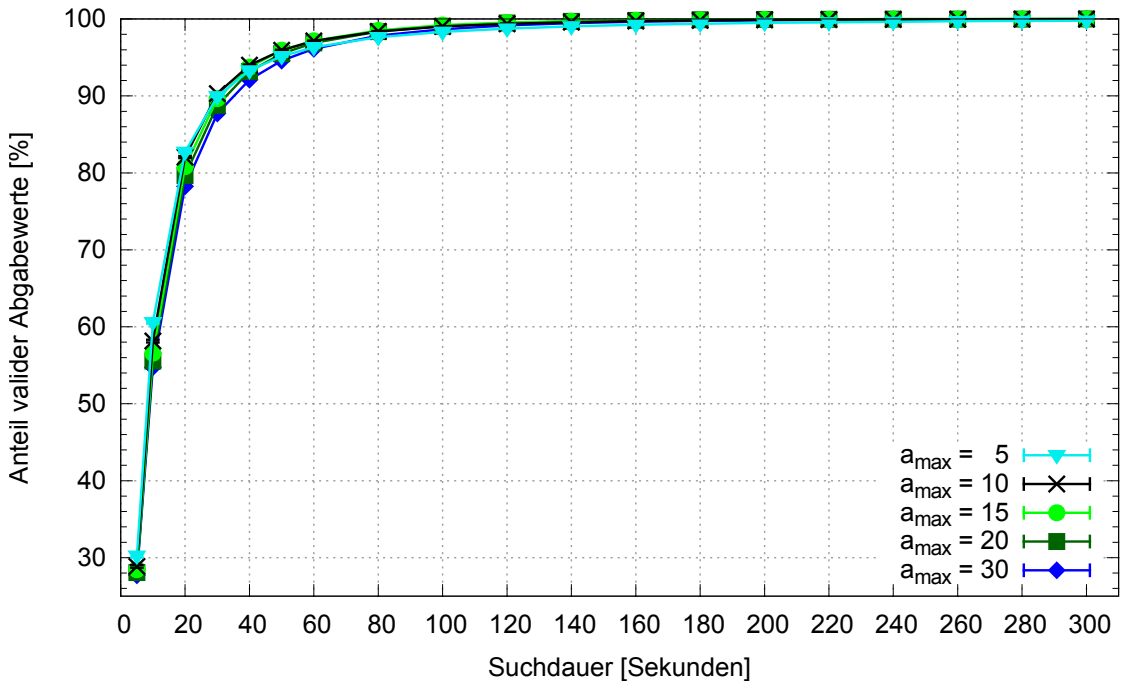
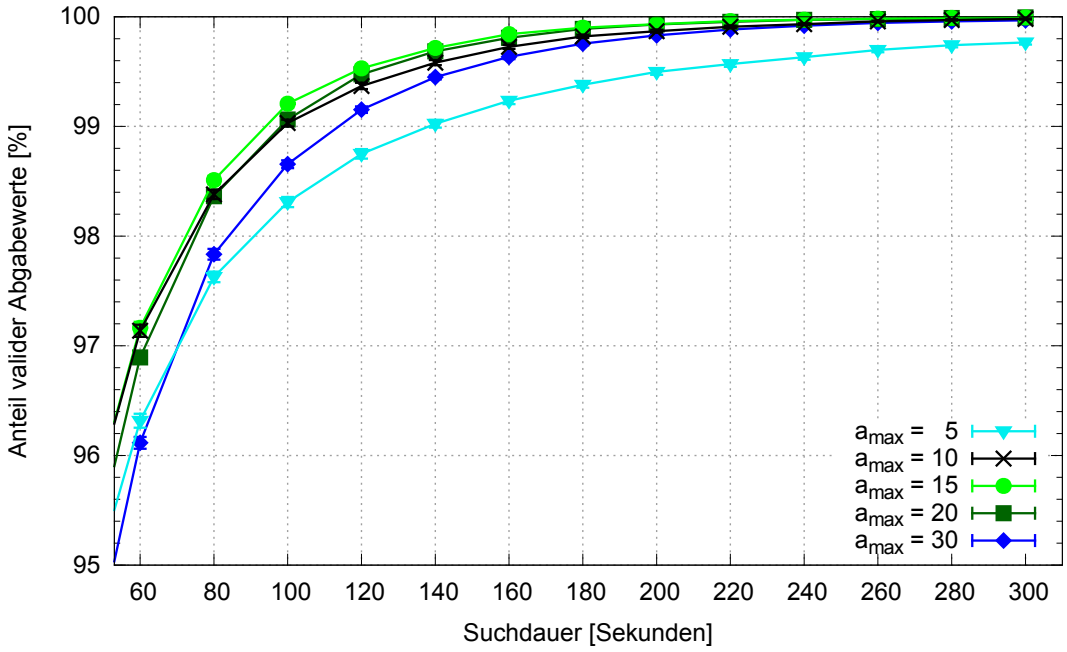
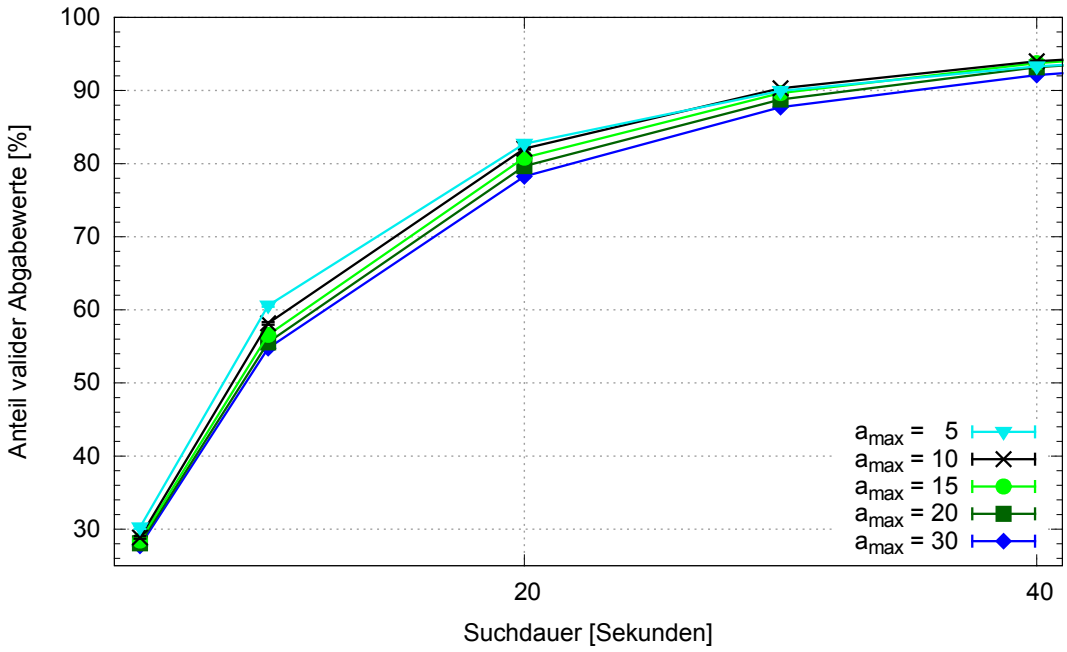


Abbildung B.9: *Anteil valider Abgabewerte bei $m_{max} = 20$ und variierendem a_{max}.*



(a) *Detailbetrachtung von* 40 *bis* 300 *Sekunden.*



(b) *Detailbetrachtung von* 5 *bis* 40 *Sekunden.*

Abbildung B.10: *Detailbetrachtungen der Anteile valider Abgabewerte bei* $m_{max} = 20$ *und variierendem* a_{max}.

Tabelle B.5: *Parameterkonfigurationen für Simulationen zum Einfluss von* $a_{max} = 25$ *bei festem* m_{max}.

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	keiner
Simulations-Wiederholungen	je Parametrisierung 100
s	$\{5, 10, 20, 30, \ldots, 60, 80, 100, \ldots, 300\}$
t_{max}	1 Sekunde
m_{max}	25
a_{max}	$\{5, 10, 15, 20, 30\}$

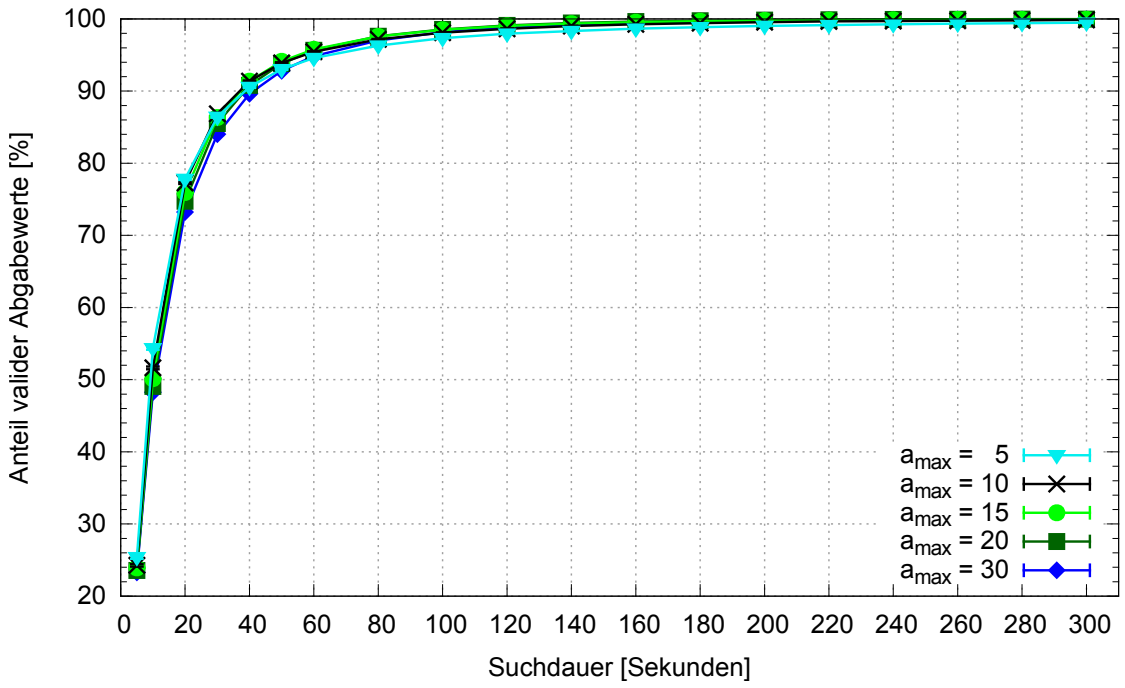
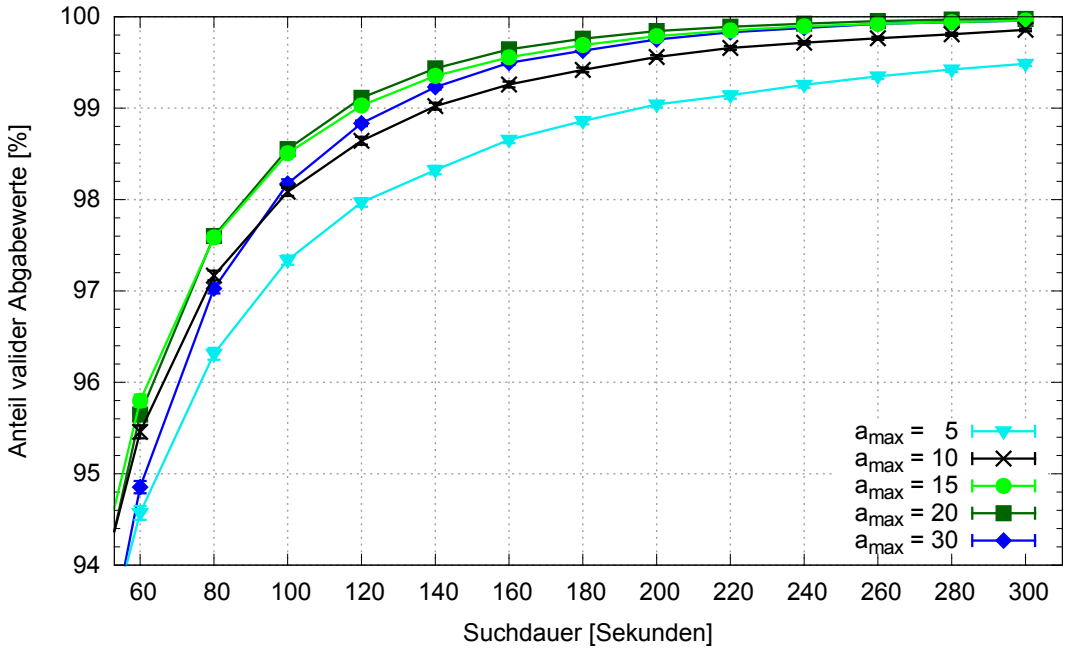
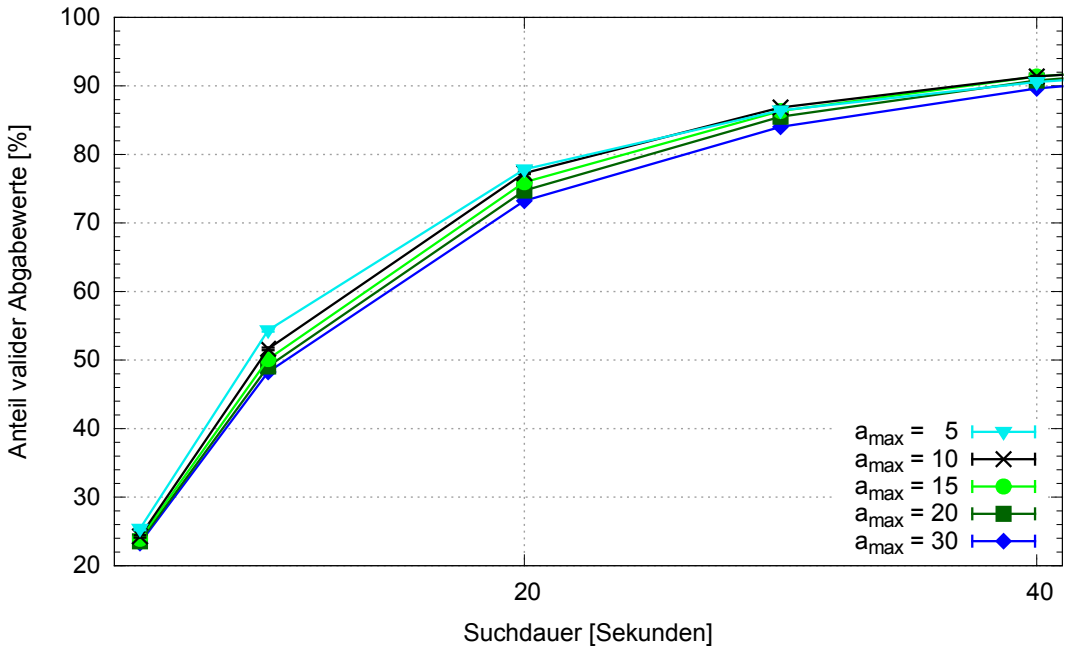


Abbildung B.11: *Anteil valider Abgabewerte bei* $m_{max} = 25$ *und variierendem* a_{max}.



(a) *Detailbetrachtung von* 40 *bis* 300 *Sekunden.*



(b) *Detailbetrachtung von* 5 *bis* 40 *Sekunden.*

Abbildung B.12: *Detailbetrachtungen der Anteile valider Abgabewerte bei* $m_{max} = 25$ *und variierendem* a_{max}.

B.3 Einfluss von t_{max}

Im Folgenden werden weitere Simulationsergebnisse zur Untersuchung aus Abschnitt 6.3.3 dargestellt. Die verwendeten Parameterkonfigurationen sind in Tabelle B.6 zusammengefasst.

Tabelle B.6: *Parameterkonfigurationen für weitere Simulationen zum Einfluss von* t_{max}.

Parameter	Belegung
Anzahl intelligenter Stromzähler	5 000
Churn	normal ($\approx 99,5\%$ Verfügbarkeit)
	bis stark ($\approx 98,55\%$ Verfügbarkeit)
Simulations-Wiederholungen	je Parametrisierung 100
t_{max}	600 Millisekunden
m_{max}	$\underbrace{\{10, 15, 25\}}$
	in Kombination
a_{max}	$\overbrace{\{5, 10, 20\}}$

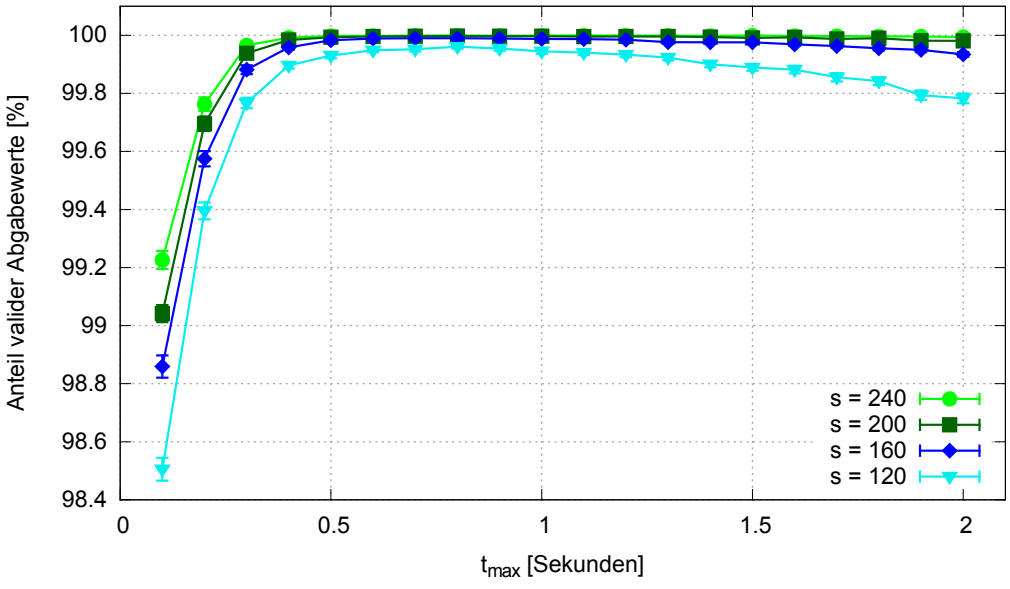


Abbildung B.13: *Anteil valider Abgabewerte in Abhängigkeit von der Suchdauer s für* $m_{max} = 10$.

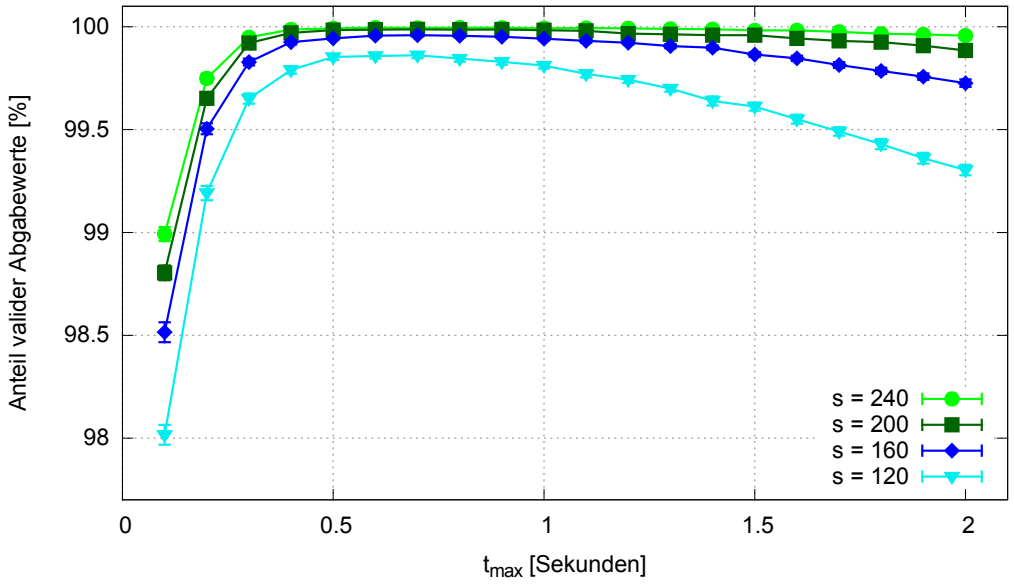


Abbildung B.14: *Anteil valider Abgabewerte in Abhängigkeit von der Suchdauer s für* $m_{max} = 15$.

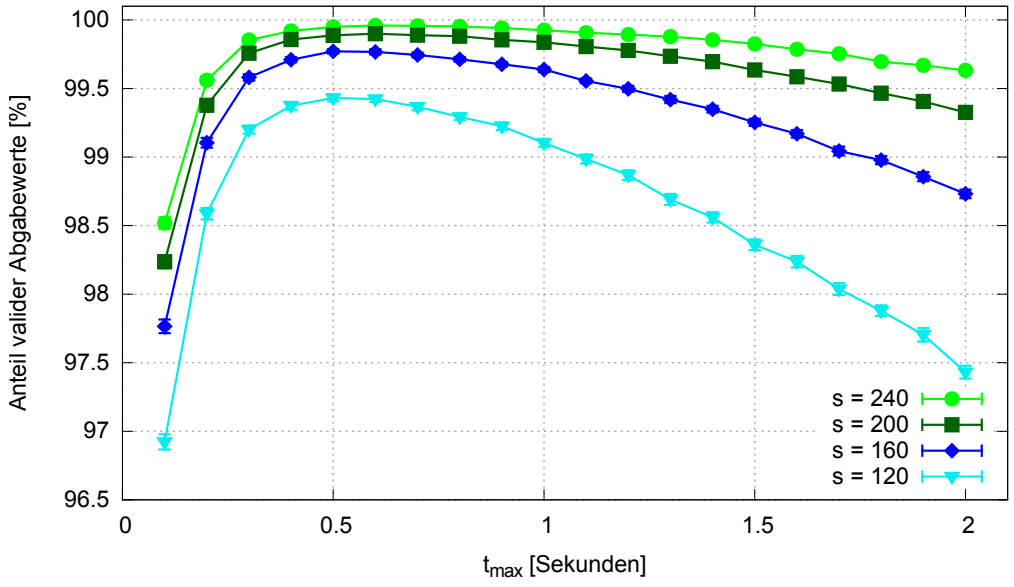


Abbildung B.15: *Anteil valider Abgabewerte in Abhängigkeit von der Suchdauer s für* $m_{max} = 25$.

Literatur

[1] F. Armknecht u. a. „A lifetime-optimized end-to-end encryption scheme for sensor networks allowing in-network processing“. In: *Computer Communications* 31.4 (März 2008), S. 734–749. ISSN: 01403664.

[2] M. Baranski und J. Voss. „Genetic algorithm for pattern detection in NIALM systems“. In: *IEEE International Conference on Systems, Man and Cybernetics*. The Hague, Okt. 2004, 3462–3468 vol. 4. ISBN: 0-7803-8567-5.

[3] I. Baumgart. *Verteilter Namensdienst für dezentrale IP-Telefonie*. KIT Scientific Publishing, 2011. ISBN: 978-3-86644-625-0.

[4] I. Baumgart, B. Heep und S. Krause. „OverSim: A Flexible Overlay Network Simulation Framework“. In: *Proceedings of 10th IEEE Global Internet Symposium (GI '07) in conjunction with IEEE INFOCOM 2007*. Anchorage: IEEE, Mai 2007, S. 79–84. ISBN: 978-1-4244-1697-4.

[5] I. Baumgart, B. Heep und S. Krause. „OverSim: A scalable and flexible overlay framework for simulation and real network applications“. In: *Proceedings of the Ninth International Conference on Peer-to-Peer Computing (IEEE P2P'09)*. Seattle: IEEE, Sep. 2009, S. 87–88. ISBN: 978-1-4244-5066-4.

[6] I. Baumgart und S. Mies. „S/Kademlia: A practicable approach towards secure key-based routing“. In: *2007 International Conference on Parallel and Distributed Systems*. Hsinchu: IEEE, Dez. 2007, S. 1–8. ISBN: 978-1-4244-1889-3.

[7] I. Baumgart u. a. „OverArch: A common architecture for structured and unstructured overlay networks“. In: *Proceedings of the 15th IEEE Global Internet Symposium in conjunction with IEEE INFOCOM 2012*. Orlando: IEEE, März 2012, S. 2534–2539. ISBN: 978-1-4673-1017-8.

[8] D. J. Bernstein. „Curve25519 : new Diffie-Hellman speed records“. In: *Public Key Cryptography - PKC 2006*. Bd. 25519. Springer Berlin Heidelberg, 2006, S. 207–228. ISBN: 978-3-540-33851-2.

[9] D. J. Bernstein. „The Poly1305-AES Message-Authentication Code“. In: *Fast Software Encryption*. Springer Berlin Heidelberg, 2005, S. 32–49. ISBN: 978-3-540-26541-2.

[10] D. J. Bernstein. „The Salsa20 Family of Stream Ciphers“. In: *New Stream Cipher Designs*. Springer Berlin Heidelberg, 2008, S. 84–97. ISBN: 978-3-540-68350-6.

[11] D. J. Bernstein, T. Lange und P. Schwabe. „The Security Impact of a New Cryptographic Library“. In: *Progress in Cryptology – LATINCRYPT 2012*. 2012, S. 159–176. ISBN: 978-3-642-33480-1.

[12] D. J. Bernstein u. a. „High-speed high-security signatures“. In: *Journal of Cryptographic Engineering* 2.2 (Aug. 2012), S. 77–89. ISSN: 2190-8508.

[13] J.-M. Bohli, C. Sorge und O. Ugus. „A Privacy Model for Smart Metering“. In: *IEEE International Conference on Communications Workshops (ICC)*. Capetown, Mai 2010, S. 1–5. ISBN: 978-1-4244-6824-9.

[14] G. Brassard, D. L. Chaum und C. Crépeau. „Minimum disclosure proofs of knowledge“. In: *Journal of Computer and System Sciences* 37 (1988), S. 156–189.

[15] Bundesamt für Sicherheit in der Informationstechnik. *Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen*. Techn. Ber. March. 2014.

[16] Bundesnetzagentur. *Kraftwerksliste der Bundestnetzagentur - Stand 19. Februar*. Techn. Ber. 2014.

[17] Bundesnetzagentur und Bundeskartellamt. *Monitoringbericht 2013*. Techn. Ber. 2013.

[18] C4 Security. *The Dark Side of the Smart Grid - Smart Meters (in)Security*. Techn. Ber. 2009.

[19] CACE. *Computer Aided Cryptography Engineering*. URL: `http://www.cace-project.eu/` (besucht am 03. 04. 2014).

[20] C. Castelluccia, E. Mykletun und G. Tsudik. „Efficient aggregation of encrypted data in wireless sensor networks“. In: *The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*. IEEE, 2005, S. 109–117. ISBN: 0-7695-2375-7.

[21] M. Castro u. a. „Secure routing for structured peer-to-peer overlay networks“. In: *ACM SIGOPS Operating Systems Review* 36.SI (Dez. 2002), S. 299–314. ISSN: 01635980.

[22] A. Cavoukian, J. Polonetsky und C. Wolf. „SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation“. In: *Identity in the Information Society* 3.2 (Apr. 2010), S. 275–294. ISSN: 1876-0678.

[23] D. Cerri u. a. „ID mapping attacks in P2P networks“. In: *GLOBECOM '05. IEEE Global Telecommunications Conference*. St. Louis: IEEE, Nov. 2005, S. 1785–1790. ISBN: 0-7803-9414-3.

[24] D. Challener u. a. *A practical guide to trusted computing*. First. IBM Press, 2007. ISBN: 9780132398428.

[25] D. Chaum. „The dining cryptographers problem: Unconditional sender and recipient untraceability“. In: *Journal of Cryptology* 1.1 (1988), S. 65–75. ISSN: 0933-2790.

[26] D. L. Chaum. „Untraceable electronic mail, return addresses, and digital pseudonyms“. In: *Communications of the ACM* 24.2 (Feb. 1981), S. 84–90. ISSN: 00010782.

[27] T. H. Cormen u. a. *Introduction to Algorithms*. 3rd Editio. Mit Press, 2009. ISBN: 978-0262033848.

[28] K. D. Craemer und G. Deconinck. „Analysis of State-of-the-art Smart Metering Communication Standards“. In: *Proceedings of the 5th Young Researchers Symposium*. Leuven, März 2010, S. 1–6.

[29] R. Cramer und V. Shoup. „Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption“. In: *Advances in Cryptology — EUROCRYPT 2002*. Springer Berlin Heidelberg, 2002, S. 45–64. ISBN: 978-3-540-43553-2.

[30] V. Crastan und D. Westermann. *Elektrische Energieversorgung 3*. Springer Berlin Heidelberg, 2011. ISBN: 3642200990.

[31] F. Dabek, B. Zhao und P. Druschel. „Towards a common API for structured peer-to-peer overlays“. In: *Peer-to-Peer Systems II*. Springer Berlin Heidelberg, 2003, S. 33–44. ISBN: 978-3-540-40724-9.

[32] M. Davis. „SmartGrid Device Security“. In: *Presentations at Black Hat USA*. 2009.

[33] Deutsche Telekom. *CompanyConnect Produktseite*. URL: `http://geschaeftskunden.telekom.de/festnetz/company-connect-internet-standleitung-bis-622-mbit-s-/40340` (besucht am 14. 01. 2014).

[34] R. Dingledine, N. Mathewson und P. Syverson. *Tor : The Second-Generation Onion Router*. Techn. Ber. DTIC Document, 2004.

[35] H. Dobbertin, A. Bosselaers und B. Preneel. „RIPEMD-160: A Strengthened Version of RIPEMD“. In: *Lecture Notes in Computer Science Vol. 1039*. Springer Berlin Heidelberg, 1996, S. 71–82. ISBN: 978-3-540-60865-3.

[36] D. Dolev und a. Yao. „On the security of public key protocols“. In: *IEEE Transactions on Information Theory* 29.2 (März 1983), S. 198–208. ISSN: 0018-9448.

[37] J. Douceur. „The sybil attack“. In: *Peer-To-Peer Systems*. Springer Berlin Heidelberg, 2002, S. 251–260. ISBN: 978-3-540-44179-3.

[38] D. Eastlake 3rd und T. Hansen. *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*. RFC 6234 (Informational). Internet Engineering Task Force, Mai 2011. URL: http://www.ietf.org/rfc/rfc6234.txt.

[39] D. Eastlake 3rd und P. Jones. *US Secure Hash Algorithm 1 (SHA1)*. RFC 3174 (Informational). Updated by RFCs 4634, 6234. Internet Engineering Task Force, Sep. 2001. URL: http://www.ietf.org/rfc/rfc3174.txt.

[40] ECRYPT NoE. *eBACS: ECRYPT Benchmarking of Cryptographic Systems*. URL: http://bench.cr.yp.to/results-sign.html (besucht am 20. 05. 2014).

[41] ECRYPT NoE. *European Network of Excellence in Cryptology II*. URL: http://www.ecrypt.eu.org/ (besucht am 03. 04. 2014).

[42] C. Efthymiou und G. Kalogridis. „Smart Grid Privacy via Anonymization of Smart Metering Data“. In: *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Gaithersburg, Okt. 2010, S. 238–243. ISBN: 978-1-4244-6510-1.

[43] T. Elgamal. „A public key cryptosystem and a signature scheme based on discrete logarithms“. In: *IEEE Transactions on Information Theory* 31.4 (Juli 1985), S. 469–472. ISSN: 0018-9448.

[44] EnBW Vertrieb GmbH. *MeRegio Internetauftritt*. URL: http://www.meregio.de (besucht am 31. 01. 2014).

[45] EnergieAgentur.NRW. *Erhebung: Wo im Haushalt bleibt der Strom?* URL: http://www.energieagentur.nrw.de/%5C_database/%5C_data/datainfopool/erhebung%5C_wo%5C_bleibt%5C_der%5C_strom.pdf (besucht am 15. 04. 2014).

[46] Z. Erkin und G. Tsudik. „Private Computation of Spatial and Temporal Power Consumption with Smart Meters“. In: *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2012, S. 561–577. ISBN: 978-3-642-31283-0.

[47] Z. Erkin u. a. „Privacy-preserving data aggregation in smart metering systems: an overview“. In: *IEEE Signal Processing Magazine* 30.2 (März 2013), S. 75–86. ISSN: 1053-5888.

[48] Ernst & Young. *Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler*. Techn. Ber. 2013.

[49] H. Farhangi. „The path of the smart grid“. In: *IEEE Power and Energy Magazine* 8.1 (Jan. 2010), S. 18–28. ISSN: 1540-7977.

[50] S. Feuerhahn u. a. „Comparison of the communication protocols DLMS/-COSEM, SML and IEC 61850 for smart metering applications“. In: *IEEE International Conference on Smart Grid Communications (SmartGrid-Comm)*. Brussels, Okt. 2011, S. 410–415. ISBN: 978-1-4577-1702-4.

[51] S. Finster. „Smart Meter Speed Dating, short-term relationships for improved privacy in Smart Metering“. In: *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Vancouver, Okt. 2013, S. 426–431. ISBN: 9781457717024.

[52] S. Finster und I. Baumgart. „Elderberry: A peer-to-peer, privacy-aware smart metering protocol“. In: *IEEE INFOCOM Workshop on Communications and Control for Smart Energy Systems*. Turin, Apr. 2013, S. 3411–3416. ISBN: 978-1-4673-5946-7.

[53] S. Finster und I. Baumgart. „Privacy-aware Smart Metering: A Survey“. In: *IEEE Communications Surveys & Tutorials* 16.3 (2014), noch nicht erschienen.

[54] S. Finster und I. Baumgart. „SMART-ER: peer-based privacy for smart metering“. In: *IEEE INFOCOM Workshop on Communications and Control for Smart Energy Systems*. Toronto, Apr. 2014, S. 642–647. ISBN: 978-1-4799-3088-3.

[55] S. Finster und M. Conrad. „Echtzeit-Smart-Metering ohne Verletzung der Privatsphäre“. In: *VDE Kongress 2010 - E-Mobility*. Leipzig: VDE Verlag, Nov. 2010.

[56] A. Gai und L. Viennot. „Broose: a practical distributed hashtable based on the de-Bruijn topology“. In: *Proceedings of the Fourth International Conference on Peer-to-Peer Computing*. Zurich: Ieee, Sep. 2004, S. 167–174. ISBN: 0-7695-2156-8.

[57] F. D. Garcia und B. Jacobs. „Privacy-Friendly Energy-Metering via Homomorphic Encryption“. In: *Proceedings of the 6th international conference on Security and trust management*. Surat, Mai 2011, S. 226–238.

[58] C. Gentry. „Computing arbitrary functions of encrypted data“. In: *Communications of the ACM* 53.3 (2010), S. 97–105. ISSN: 00010782.

[59] O. Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, 2004. ISBN: 978-0521830843.

[60] F. Gómez Mármol u. a. „Do not snoop my habits: preserving privacy in the smart grid“. In: *IEEE Communications Magazine* 50.5 (Mai 2012), S. 166–172. ISSN: 0163-6804.

[61] F. Gómez Mármol u. a. „Privacy-enhanced architecture for smart metering“. In: *International Journal of Information Security* 12.2 (2013), S. 67–82. ISSN: 1615-5262.

[62] C. Haas, J. Wilke und V. St. „Realistic Simulation of Energy Consumption in Wireless Sensor Networks“. In: *Proceedings of the 9th European Conference on Wireless Sensor Networks (EWSN)*. Springer Berlin Heidelberg, Feb. 2012, S. 82–97.

[63] D. Hart. „Using AMI to realize the Smart Grid“. In: *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century* (Juli 2008), S. 1–2.

[64] G. Hart. „Nonintrusive appliance load monitoring“. In: *Proceedings of the IEEE* 80.12 (1992), S. 1870–1891. ISSN: 00189219.

[65] G. Hart. „Residential energy monitoring and computerized surveillance via utility power flows“. In: *IEEE Technology and Society Magazine* 8.2 (Juni 1989), S. 12–16. ISSN: 0278-0097.

[66] W. He u. a. „PDA: Privacy-Preserving Data Aggregation for Information Collection“. In: *ACM Transactions on Sensor Networks* 8.1 (Aug. 2011), S. 1–22. ISSN: 15504859.

[67] W. He u. a. „PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks“. In: *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*. Anchorage, Mai 2007, S. 2045–2053. ISBN: 1-4244-1047-9.

[68] B. Huffaker u. a. „Topology discovery by active probing“. In: *Proceedings of the Symposium on Applications and the Internet (SAINT) Workshops*. Nara: IEEE Comput. Soc, Jan. 2002, S. 90–96. ISBN: 0-7695-1450-2.

[69] M. Jawurek, M. Johns und F. Kerschbaum. „Plug-In Privacy for Smart Metering Billing“. In: *Lecture Notes in Computer Science*. Lecture Notes in Computer Science 6794 (2011). Hrsg. von S. Fischer-Hübner und N. Hopper, S. 192–210.

[70] M. Jawurek, M. Johns und K. Rieck. „Smart metering de-pseudonymization“. In: *Proceedings of the 27th Annual Computer Security Applications Conference on - ACSAC '11*. Orlando, Dez. 2011, S. 227–236. ISBN: 9781450306720.

[71] K. Jünemann, P. Andelfinger und H. Hartenstein. „Towards a Basic DHT Service: Analyzing Network Characteristics of a Widely Deployed DHT“. In: *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*. Maui: IEEE, Juli 2011, S. 1–7. ISBN: 978-1-4577-0637-0.

[72] M. F. Kaashoek und D. R. Karger. „Koorde : A Simple Degree-Optimal Distributed Hash Table“. In: *Peer-to-Peer Systems II*. Springer Berlin Heidelberg, 2003, S. 98–107. ISBN: 978-3-540-40724-9.

[73] G. Kalogridis, Z. Fan und S. Basutkar. „Affordable Privacy for Home Smart Meters“. In: *IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*. Busan, Mai 2011, S. 77–84. ISBN: 978-1-4577-0524-3.

[74] G. Kalogridis u. a. „Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures“. In: *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Gaithersburg, Okt. 2010, S. 232–237. ISBN: 978-1-4244-6510-1.

[75] Karlsruher Institut für Technologie. *Forschungsprojekt MeRegioMobil - Elektromobilität im Energiesystem der Zukunft*. URL: `http://meregiomobil.forschung.kit.edu/` (besucht am 12. 05. 2014).

[76] Y. Kim, E. C.-H. Ngai und M. B. Srivastava. „Cooperative state estimation for preserving privacy of user behaviors in smart grid“. In: *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Gaithersburg, Okt. 2011, S. 178–183. ISBN: 978-1-4577-1702-4.

[77] D. Kleidermacher und M. Kleidermacher. *Embedded Systems Security*. Elsevier, 2012. ISBN: 978-0-12-386886-2.

[78] A. Klenke. *Wahrscheinlichkeitstheorie*. Springer, 2008. ISBN: 978-3540763178.

[79] J. Z. Kolter, S. Batra und A. Y. Ng. „Energy Disaggregation via Discriminative Sparse Coding“. In: *Advances in Neural Information Processing Systems*. 2010, S. 1153–1161.

[80] H. Krawczyk, M. Bellare und R. Canetti. *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104 (Informational). Updated by RFC 6151. Internet Engineering Task Force, Feb. 1997. URL: `http://www.ietf.org/rfc/rfc2104.txt`.

[81] H. Lam, G. Fung und W. Lee. „A Novel Method to Construct Taxonomy of Electrical Appliances Based on Load Signatures“. In: *IEEE Transactions on Consumer Electronics* 53.2 (2007), S. 653–660. ISSN: 0098-3063.

[82] C. Laughman u. a. „Power signature analysis“. In: *IEEE Power and Energy Magazine* 1.2 (März 2003), S. 56–63. ISSN: 1540-7977.

[83] F. Li, B. Luo und P. Liu. „Secure and privacy-preserving information aggregation for smart grids“. In: *International Journal of Security and Networks* 6.1 (2011), S. 28. ISSN: 1747-8405.

[84] F. Li, B. Luo und P. Liu. „Secure Information Aggregation for Smart Grids Using Homomorphic Encryption“. In: *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Gaithersburg, Okt. 2010, S. 327–332. ISBN: 978-1-4244-6510-1.

[85] M. A. Lisovich, D. K. Mulligan und S. B. Wicker. „Inferring Personal Information from Demand-Response Systems“. In: *IEEE Security & Privacy Magazine* 8.1 (Jan. 2010), S. 11–20. ISSN: 1540-7993.

[86] M. A. Lisovich und S. B. Wicker. „Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems“. In: *Clemson Power Systems Conference 2008*. Bd. 1. 1. März 2008, S. 1–10.

[87] P. Mahadevan u. a. *Lessons from Three Views of the Internet Topology*. Techn. Ber. University of California, San Diego, 2005. arXiv: 0508033v1 [arXiv:cs].

[88] G. Maier u. a. „On Dominant Characteristics of Residential Broadband Internet Traffic“. In: *IMC '09 Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. Chicago, Illinois: ACM, Nov. 2009, S. 90–102. ISBN: 9781605587707.

[89] L. Massoulié u. a. „Peer counting and sampling in overlay networks“. In: *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing - PODC '06*. Denver: ACM Press, Juli 2006, S. 123–132. ISBN: 1595933840.

[90] P. Maymounkov und D. Mazi. „Kademlia : A Peer-to-Peer Information System Based on the XOR Metric“. In: *Lecture Notes in Computer Science Vol. 2429*. Bd. 2429. Springer Berlin Heidelberg, 2002, S. 53–65. ISBN: 978-3-540-44179-3.

[91] S. McCanne und S. Floyd. *The Network Simulator ns-2*. URL: http://www.isi.edu/nsnam/ns/ (besucht am 12. 02. 2014).

[92] S. McLaughlin, P. McDaniel und W. Aiello. „Protecting consumer privacy from electric load monitoring“. In: *Proceedings of the 18th ACM conference on Computer and communications security - CCS '11*. Chicago, Okt. 2011, S. 87–98. ISBN: 9781450309486.

[93] H. Meier u. a. „Repräsentative VDEW Lastprofile“. In: *VDEW Materialien M32/99* (1999).

[94] MEMSIC Inc. *MICAz Wireless Measurement System*. URL: www.memsic.com/userfiles/files/Datasheets/WSN/micaz%5C_datasheet-t.pdf (besucht am 04. 03. 2014).

[95] Mitglieder des Bundesverfassungsgerichts. *Entscheidungen des Bundesverfassungsgerichts BVerfGE 65,1, Seite 44ff*. Tübingen: Mohr Siebeck, 1991.

[96] A. Molina-Markham u. a. „Private memoirs of a smart meter“. In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building - BuildSys '10* (2010), S. 61.

[97] D. C. Montgomery und G. C. Runger. *Applied Statistics and Probability for Engineers*. Fifth Edit. John Wiley & Sons, 2010. ISBN: 978-0470053041.

[98] D. M'Raihi u. a. *HOTP: An HMAC-Based One-Time Password Algorithm*. RFC 4226 (Informational). Internet Engineering Task Force, Dez. 2005. URL: http://www.ietf.org/rfc/rfc4226.txt.

[99] D. M'Raihi u. a. *TOTP: Time-Based One-Time Password Algorithm*. RFC 6238 (Informational). Internet Engineering Task Force, Mai 2011. URL: http://www.ietf.org/rfc/rfc6238.txt.

[100] S. Munz. „Privatheit, Smart-Metering und Sensornetze". Diplomarbeit. Karlsruher Institut für Technologie (KIT), 2014.

[101] National Institute of Standards and Technology. *Advanced encryption standard NIST FIPS PUB 197*. Techn. Ber. 2001.

[102] National Institute of Standards and Technology (NIST). *DRAFT FIPS PUB 202 SHA-3 Standard : Permutation-Based Hash and Extendable-Output Functions*. Gaithersburg, 2014.

[103] Z. Ou u. a. „Performance evaluation of a Kademlia-based communication-oriented P2P system under churn". In: *Computer Networks* 54.5 (Apr. 2010), S. 689–705. ISSN: 13891286.

[104] P. Paillier und D. Pointcheval. „Efficient Public-Key Cryptosystems Provably Secure against Active Adversaries". In: *Advances in Cryptology - ASIACRYPT'99*. Springer Berlin Heidelberg, 1999, S. 165–179. ISBN: 978-3-540-66666-0.

[105] T. P. Pedersen. „Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing". In: *Advances in Cryptology — CRYPTO '91, LNCS 576*. Springer Berlin Heidelberg, 1992. Kap. Session 3, S. 129–140. ISBN: 978-3-540-55188-1.

[106] R. Petrlic. „A privacy-preserving concept for smart grids". In: *Sicherheit in vernetzten Systemen* 18 (2010), B1–B14.

[107] J. Postel. *Transmission Control Protocol*. RFC 793 (Standard). Updated by RFCs 1122, 3168, 6093, 6528. Internet Engineering Task Force, Sep. 1981. URL: http://www.ietf.org/rfc/rfc793.txt.

[108] A. Probst, D. Baranek und S. Tenbohlen. „Optimierung der Lastprognose mittels Smart Meter Daten". In: *Proceedings of the 4th IEEE Power and Energy Student Summit (PESS)*. Bielefeld: IEEE, Jan. 2013.

[109] A. Prudenzi. „A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel“. In: *IEEE Power Engineering Society Winter Meeting*. Bd. 2. New York, 2002, 941–946 Vol. 2. ISBN: 0-7803-7322-7.

[110] Republik Österreich. *174. Bundesgesetz: Änderung des Elektrizitätswirtschafts- und –organisationsgesetzes 2010, des Gaswirtschaftsgesetzes 2011 und des Energie-Control-Gesetzes*. Aug. 2013.

[111] E. Rescorla. *SSL and TLS*. Addison-Wesley Longman, 2000, S. 304. ISBN: 0201615983.

[112] S. Rhea u. a. „Handling Churn in a DHT“. In: *Proceedings of the USENIX Annual Technical Conference*. Boston, 2004, S. 127–140.

[113] A. Rial und G. Danezis. „Privacy-preserving smart metering“. In: *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society - WPES '11*. Chicago, Okt. 2011, S. 49. ISBN: 9781450310024.

[114] M. Ripeanu. „Peer-to-peer architecture case study: Gnutella network“. In: *Proceedings of the First International Conference on Peer-to-Peer Computing*. Linkoping: IEEE, Aug. 2002, S. 99–100. ISBN: 0-7695-1503-7.

[115] J. Roskind. *QUIC: Quick UDP Internet Connections*. 2013. URL: `https://docs.google.com/document/d/1RNHkx%5C_VvKWyWg6Lr8SZ-saqsQx7rFV-ev2jRFUoVD34`.

[116] C. Rottondi, G. Verticale und C. Krauss. „Distributed Privacy-Preserving Aggregation of Metering Data in Smart Grids“. In: *IEEE Journal on Selected Areas in Communications* 31.7 (Juli 2013), S. 1342–1354. ISSN: 0733-8716.

[117] I. Rouf u. a. „Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems Categories and Subject Descriptors“. In: *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh, Okt. 2012, S. 462–473. ISBN: 9781450316514.

[118] A. Rowstron und P. Druschel. „Pastry : Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems“. In: *Middleware 2001*. 2001, S. 329–350. ISBN: 978-3-540-42800-8.

[119] S. Sambamoorthy u. a. „Power system and communication network co-simulation for smart grid applications“. In: *Innovative Smart Grid Technologies (ISGT), IEEE PES*. Anaheim: IEEE, Jan. 2011, S. 1–6. ISBN: 978-1-61284-218-9.

[120] B. Schneier und N. Ferguson. *Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography*. John Wiley & Sons, 2007. ISBN: 978-0470226261.

[121] T. M. Shafaat, A. Ghodsi und S. Haridi. „A Practical Approach to Network Size Estimation for Structured Overlays“. In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2008, S. 71–83. ISBN: 978-3-540-92156-1.

[122] A. Shamir. „How to share a secret“. In: *Communications of the ACM* 22.11 (Nov. 1979), S. 612–613. ISSN: 00010782.

[123] M. Sirivianos u. a. „Non-Manipulable Aggregator Node Election Protocols for Wireless Sensor Networks“. In: *2007 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops*. IEEE, Apr. 2007, S. 1–10. ISBN: 978-1-4244-0960-0.

[124] M. Srivatsa und L. Liu. „Vulnerabilities and Security Threats in Structured Overlay Networks: A Quantitative Analysis“. In: *20th Annual Computer Security Applications Conference*. Tucson: IEEE, Dez. 2004, S. 252–261. ISBN: 0-7695-2252-1.

[125] R. Steinmetz und K. Wehrle. *Peer-to-Peer Systems and Applications*. Springer, 2005. ISBN: 354029192X.

[126] R. Stewart. *Stream Control Transmission Protocol*. RFC 4960 (Proposed Standard). Updated by RFCs 6096, 6335. Internet Engineering Task Force, Sep. 2007. URL: `http://www.ietf.org/rfc/rfc4960.txt`.

[127] I. Stoica u. a. „Chord“. In: *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications - SIGCOMM '01*. San Diego, Aug. 2001, S. 149–160. ISBN: 1581134118.

[128] F. Sultanem. „Using appliance signatures for monitoring residential loads at meter panel level“. In: *IEEE Transactions on Power Delivery* 6.4 (Okt. 1991), S. 1380–1385. ISSN: 08858977.

[129] B. Switzerland. *NEPLAN*. URL: http://www.neplan.ch/ (besucht am 12. 02. 2014).

[130] Telefónica Digital. *The Smart Meter Revolution*. Techn. Ber. 2014.

[131] Texas Instruments. *Quick Start Guide to the Smart Meter Reference Design*. URL: http://www.ti.com/lit/an/slaa467/slaa467.pdf (besucht am 04. 03. 2014).

[132] TÜV Rheinland. *Bericht zum Breitbandatlas Mitte 2013*. Techn. Ber. 2013.

[133] A. Varga und R. Hornig. „An Overview of the OMNeT++ Simulation Environment“. In: *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*. ICST, 2008. ISBN: 978-963-9799-23-3.

[134] Various. *INET Framework*. URL: http://inet.omnetpp.org/ (besucht am 13. 02. 2014).

[135] S. Vaughan-Nichols. „How trustworthy is trusted computing?“ In: *Computer* 36.3 (März 2003), S. 18–20. ISSN: 0018-9162.

[136] B. Vetter u. a. „Homomorphic Primitives for a Privacy-Friendly Smart Metering Architecture“. In: *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2012)*. Rome, Juli 2012, S. 102–112.

[137] M. Weiss u. a. „Leveraging smart meter data to recognize home appliances“. In: *IEEE International Conference on Pervasive Computing and Communications*. März 2012, S. 190–197. ISBN: 978-1-4673-0258-6.

[138] A. C. Yao. „Protocols for secure computations“. In: *23rd Annual Symposium on Foundations of Computer Science*. Ieee, Nov. 1982, S. 160–164.

[139] W. Zimmermann und U. Stache. *Operations Research: Quantitative Methoden zur Entscheidungsvorbereitung*. Oldenbourg Wissenschaftsverlag, 2001. ISBN: 978-3486258165.