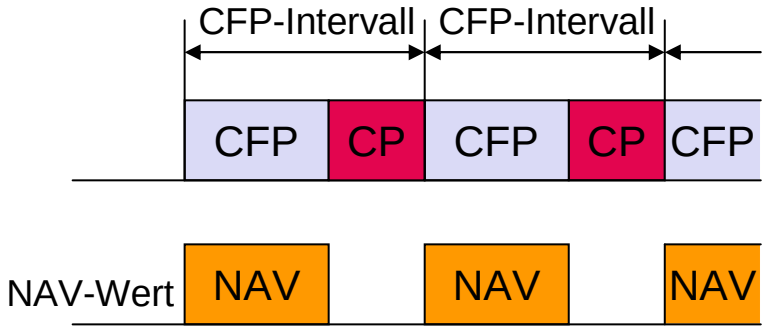
Point Coordination Function

- Zentrales MAC-Protokoll
  - Medienzugriff wird von Point Coordinator zentral gesteuert
- PCF ist optional, d.h. nicht jede Station muss PCF unterstützen, deshalb wird zwischen 2 Phasen unterschieden
  - Contention Period (CP) – Verwendung von DCF für den Medienzugriff
    - Auch Stationen die PCF nicht unterstützen können kommunizieren
  - Contention Free Period (CFP) – Verwendung von PCF für den Medienzugriff
    - Zentrale Steuerung ermöglicht Realisierung von zeitkritischen Diensten
- CFP-Intervall = CFP + CP
  - Vielfaches des Beacon-Intervalls
- Periodische Beacons des Access Points setzen NAV-Wert bei Stationen die kein PCF unterstützen



Point Coordination Function

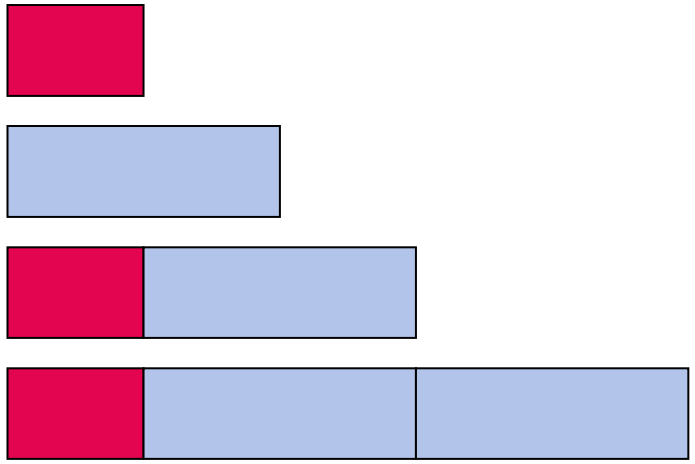
- Poll-Liste
  - Zugangspunkt führt eine Poll-Liste
    - Enthält alle PCF-fähigen Stationen
    - PCF-Fähigkeit wird bei Assoziierung mit dem WLAN von den Stationen bekannt gegeben
- Spezielle Wartezeit
  - Point (Coordination Function) Interframe Space (PIFS)
    - Mittlere Priorität
    - Berechnung:

SIFS (bei DSSS = 10 µs)

Slot Time (bei DSSS = 20 µs)

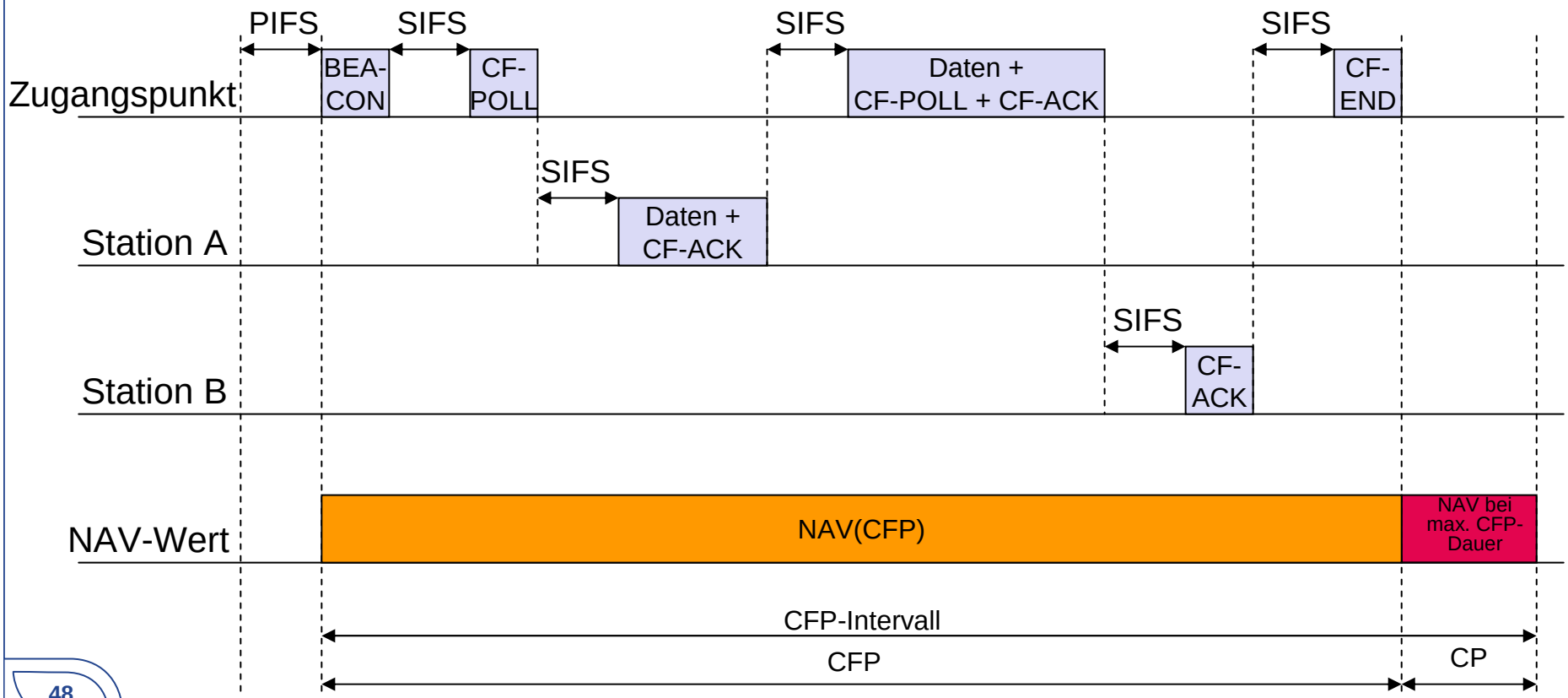
PIFS (bei DSSS = 30 µs)

DIFS (bei DSSS = 50 µs)



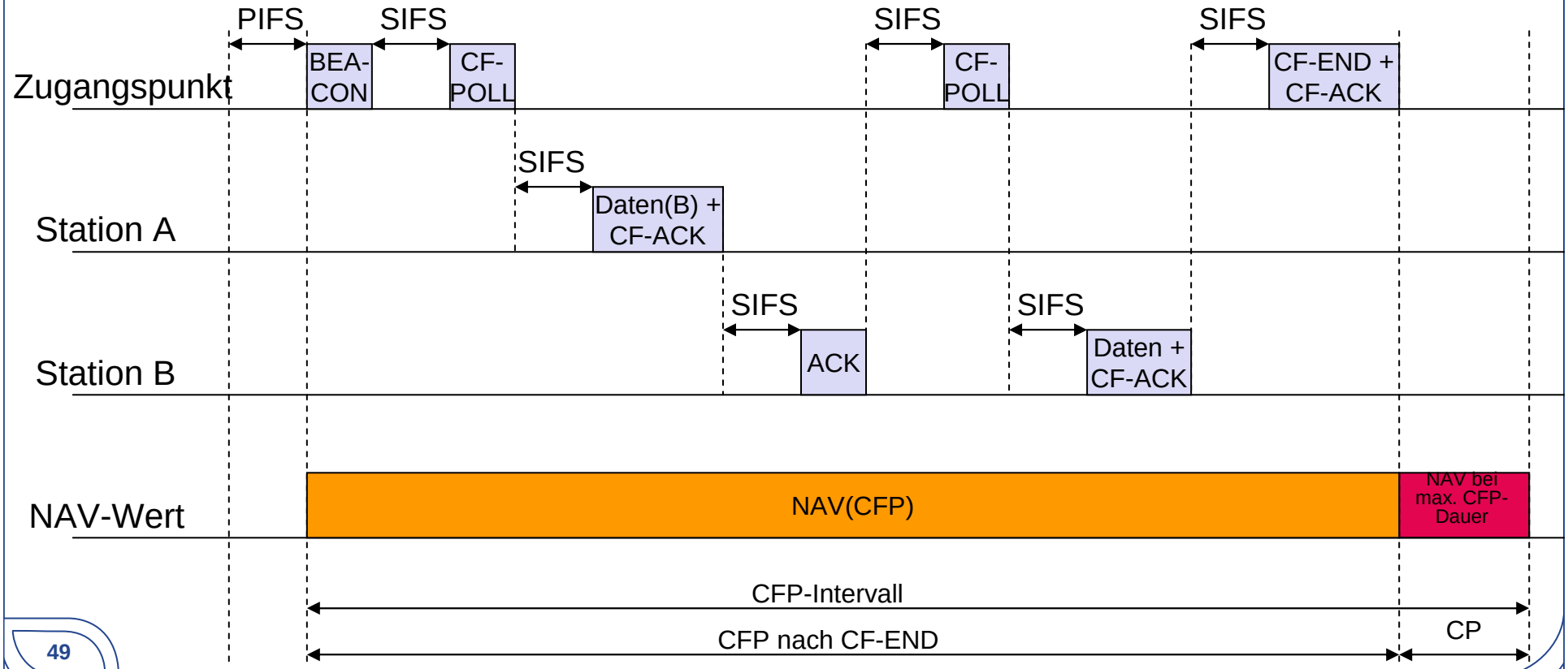
Kommunikation über Zugangspunkt

- Beispielablauf
  - Station A kommuniziert mit Station B über Zugangspunkt
    - Polling durch Zugangspunkt



Point Coordination Function

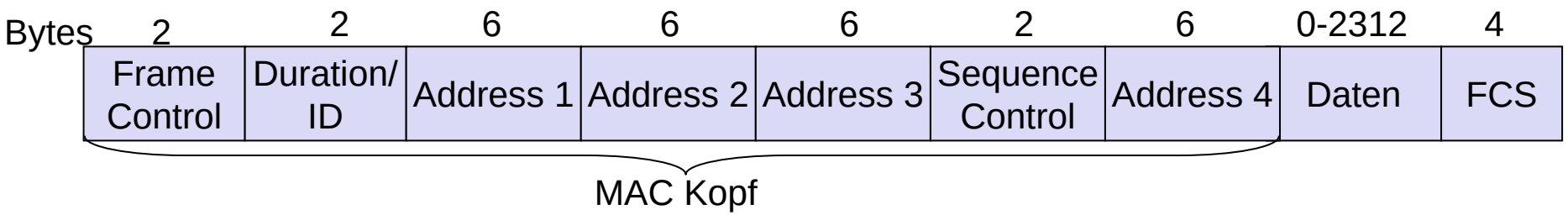
- Beispielablauf
  - Station A kommuniziert direkt mit Station B
- Vorteil
  - Geringere Belastung des Mediums



4.4.3 Format der MAC-Dateneinheiten

- Grundlegender Aufbau ähnlich dem bekannter MAC-Dateneinheiten
  - Kopf – Daten – Prüfsumme
- So in anderen MAC-Dateneinheiten nicht vorhanden
  - Bis zu vier Adressfelder
    - Länge des Kopfes variiert
  - Unterschiedliche Typen von MAC-Dateneinheiten
    - Daten-Dateneinheiten für den Transport von Nutzdaten
    - Kontroll-Dateneinheiten für die Steuerung des Medienzugriffs
    - Management-Dateneinheiten für das Management der Funkzelle
  - Duration/ID-Feld
    - Zeitangabe für die Datenübertragung
  - Sequenz-Kontroll-Feld
    - Fragmentnummer zur Kennzeichnung von Fragmenten
    - Sequenznummer zur Kennzeichnung von MSDUs

Generelles MAC-Format



- Felder
  - Duration/ID
    - Zeitangabe für Network Allocation Vector (NAV)
  - Sequence Control
    - Fragmentnummer (4 Bit) und Sequenznummer (12 Bit)
  - FCS: Frame Check Sequence
    - Prüfsumme
- Variable Länge des MAC-Headers
  - Felder Address 2, Address 3, Address 4, Sequence Control und Daten sind nur in bestimmten Dateneinheiten vorhanden

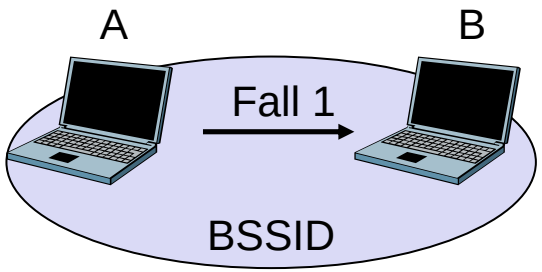
Frame-Control-Feld

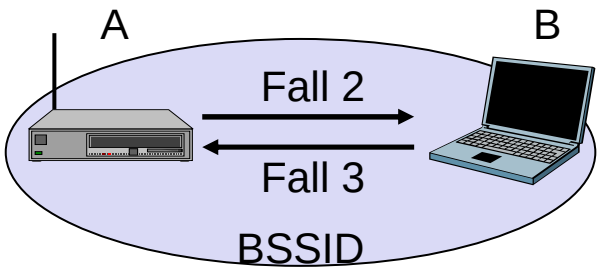
Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

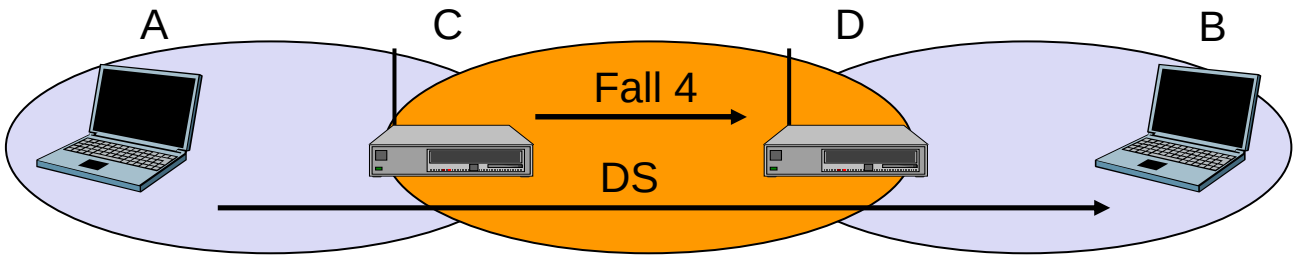
- Protocol-Version
  - Version des verwendeten Protokolls
- Type-Feld
  - Management-, Kontroll- oder Daten-Dateneinheit
- Subtype
  - Genauere Spezifikation der Dateneinheit
    - z.B. Type = Kontroll, Subtype = CTS
- ToDS/FromDS
  - Festlegung des Übertragungsweges
- More Fragment
  - Weitere Fragmente folgen
- Retry
  - Wiederholung einer Dateneinheit
- Power Management
  - Station wechselt in Passive Mode
- More Data
  - Weitere Daten stehen an
  - Station soll nicht in Passive Mode wechseln
- WEP
  - Dateneinheit ist verschlüsselt
- Order
  - Strikte Reihenfolgeerhaltung bei Fragmenten

Adressen in MAC-Dateneinheiten

Fall	Beschreibung	To DS	From DS	Adresse			
				1	2	3	4
1	Ad-hoc-Netzwerk	0	0	B	A	BSSID	-
2	Infrastruktur-Netzwerk, von AP	0	1	B	BSSID	A	-
3	Infrastruktur-Netzwerk, zu AP	1	0	BSSID	B	A	-
4	Infrastruktur-Netzwerk, im DS	1	1	D	C	B	A



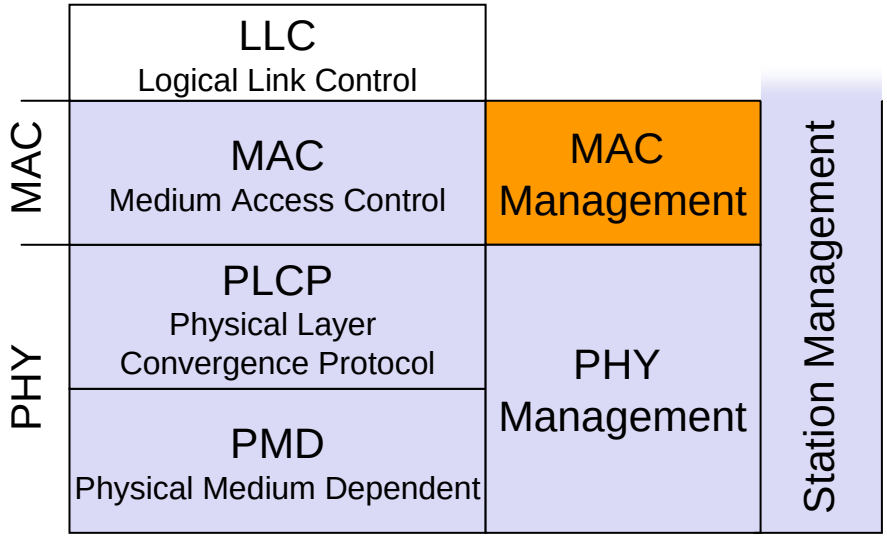




4.5 MAC Management

- Im Vergleich zu drahtgebundenen LANs wie IEEE 802.3 sind eine Reihe zusätzlicher Fragestellungen zu lösen. Zum Beispiel
  - Wie findet eine Station ein WLAN?
  - Wie wird eine Station Mitglied in einem WLAN?
  - Wie kann Energie durch „schlafen“ gespart werden?
  - Wie kann die drahtlose Kommunikation abgesichert werden?

→ Aufgaben des MAC Managements

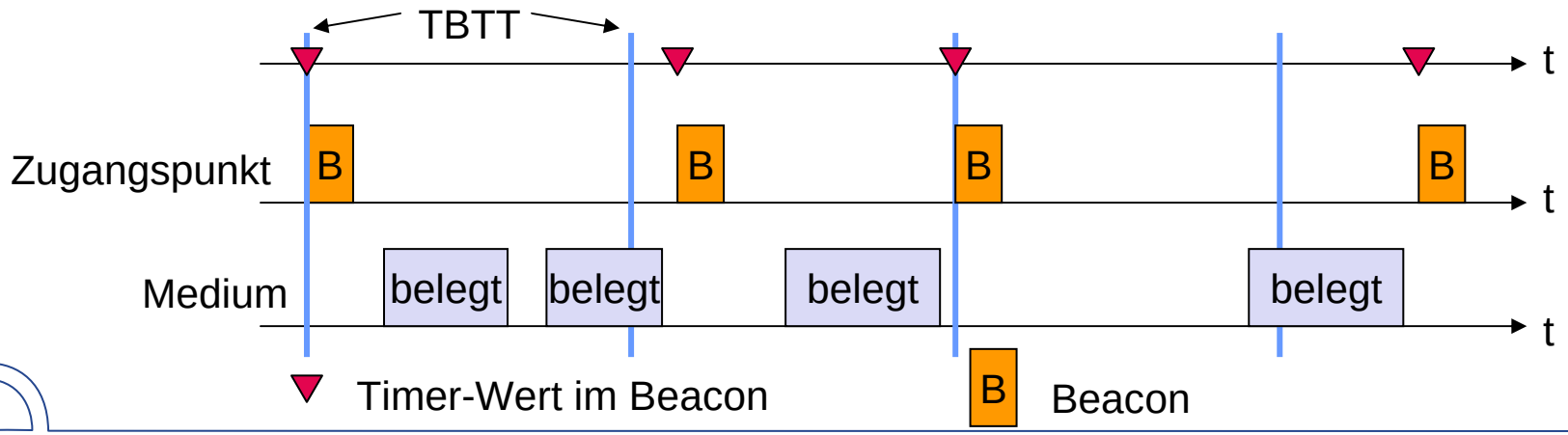


4.5.1 Synchronisation

- Problem
  - Für einige Aufgaben ist es erforderlich, dass die Stationen und Zugangspunkte über einen synchronisierten Timer verfügen, zum Beispiel:
    - Synchronisation der Sprungfolge bei FHSS
    - Power-Management
    - Koordination der PCF
- Timer Synchronisation Function (TSF)
  - Stationen und Zugangspunkte besitzen einen Timer
    - 64 Bit
    - 1 MHz
    - Genauigkeit: 25 ppm (Parts per million)
  - Synchronisation der Timer untereinander
    - Unterschiedliche Ansätze für Infrastruktur-Netz (BSS) und Ad-hoc Netz (IBSS)

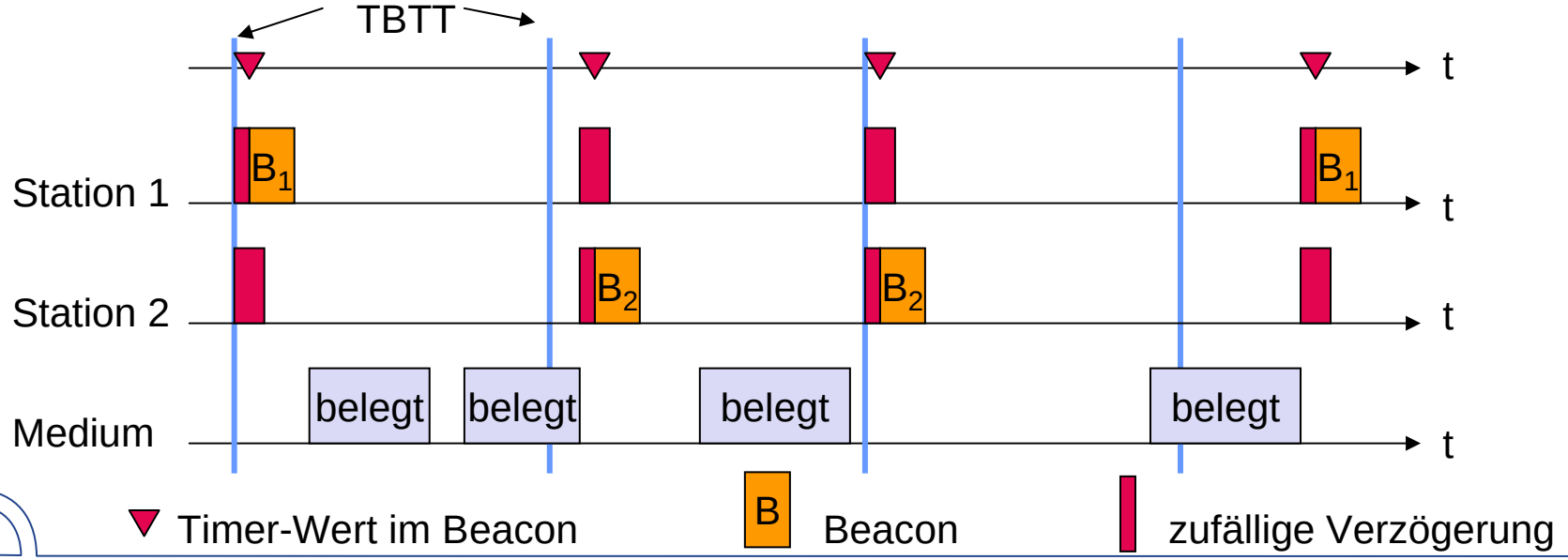
Timer-Synchronisation in einem BSS

- Zentraler Ansatz
  - Zugangspunkt sendet in regelmäßigen Abständen Beacons (Leuchtfeuer)
    - Broadcast-Dateneinheit
    - Enthält u.a. aktuellen Timer-Wert des Zugangspunkts
  - Target Beacon Transmission Time (TBTT)
    - Startzeitpunkt für das Aussenden eines Beacon
      - Zeit zwischen zwei Beacons typischerweise 102,4 ms
  - Wird beim Medienzugriff nicht anders behandelt als andere Dateneinheiten
    - Beacon kann verzögert werden
    - Timer-Wert im Beacon muss angepasst werden – repräsentiert echte Sendezeit
  - Stationen aktualisieren ihren Timer anhand der Informationen im Beacon

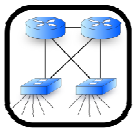


Timer-Synchronisation in einem IBSS

- Verteilter Ansatz
  - Nach Ablauf der TBTT bestimmt jede Station eine zufällige Verzögerung
  - Station sendet Beacon, wenn nach Ablauf der zufälligen Verzögerung noch kein Beacon empfangen wurde
  - Timer wird nur aktualisiert, falls Timer-Wert im Beacon größer war als eigener Wert
    - Synchronisation auf die am schnellsten laufende Uhr

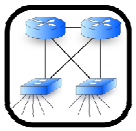


4.5.2 Scanning



- Problem
  - Wie können vorhandene WLANs gefunden werden?
    - Stationen besitzen meist keine Information über vorhandene WLANs
- Identifikation eines WLANs
  - Service Set Identifier (SSID)
    - Zwischen 0 und 32 Byte langer Netzwerkname
  - Zugangspunkte eines Infrastruktur-Netzwerkes haben alle die gleiche SSID
- Möglichkeit 1: Passives Scanning
  - Zugangspunkt sendet in regelmäßigen Abständen ein Beacon
  - Station hört nacheinander alle Kanäle ab
    - Typischer Zeitraum für Abhören eines Kanals: 204,8 ms – 256 ms
  - Empfang eines Beacons signalisiert Existenz eines Zugangspunkts
  - Bei Empfang mehrerer Beacons wird der Zugangspunkt mit dem besten Empfangssignal ausgewählt

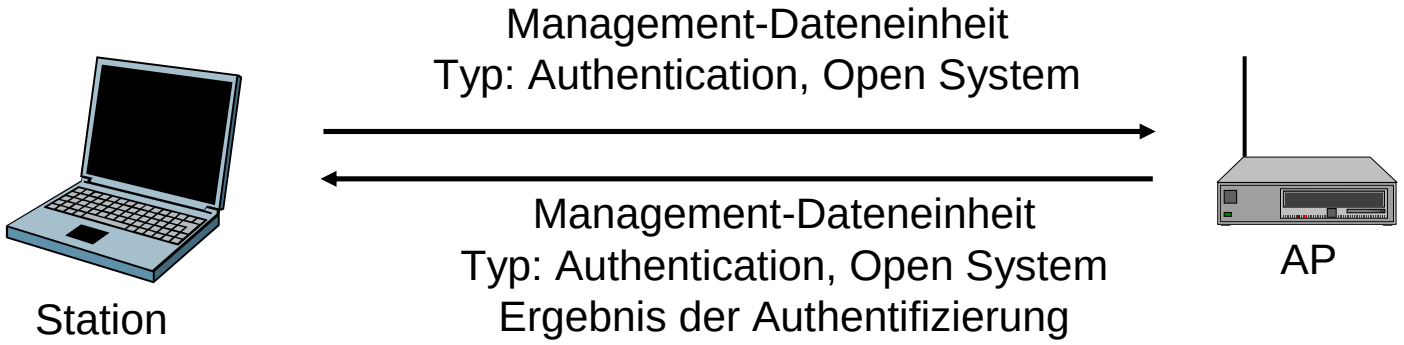
Scanning



- Möglichkeit 2: Aktives Scanning
  - Station sendet auf einem Kanal eine Probe-Request-Dateneinheit
    - SSID des gewünschten Netzwerkes oder Broadcast-SSID (ANY)
  - Zugangspunkte mit entsprechender SSID antworten mit Probe-Response-Dateneinheit
    - Empfang mehrerer Antworten
      - Auswahl des Zugangspunkts mit dem besten Empfangssignal
    - Kein Empfang einer Antwort nach Wartezeit (Probe-Delay)
      - Senden von Probe-Request-Dateneinheit auf anderem Kanal
- In Ad-hoc-Netzwerken wird nur aktives Scanning eingesetzt
  - Station die, letztes Beacon gesendet hat, übernimmt die Rolle des Zugangspunkts

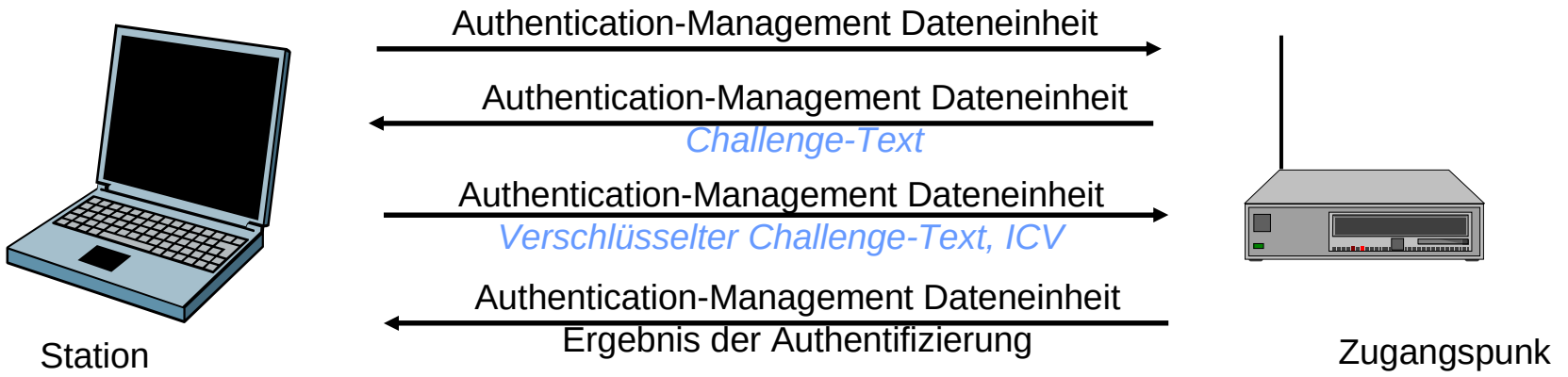
4.5.3 Authentifizierung

- Problem
  - Wer darf das WLAN nutzen?
    - Authentifizierung gegenüber dem Zugangspunkt
    - Authentifizierung zwischen zwei Stationen eines IBSS
- Möglichkeit 1: Open System Authentication
  - Keine tatsächliche Authentifizierung
  - WLAN von allen Stationen nutzbar die dies akzeptieren
  - Station sendet Dateneinheit zum Authentication-Management an AP
  - AP sendet Authentication-Management-Dateneinheit mit dem Ergebnis



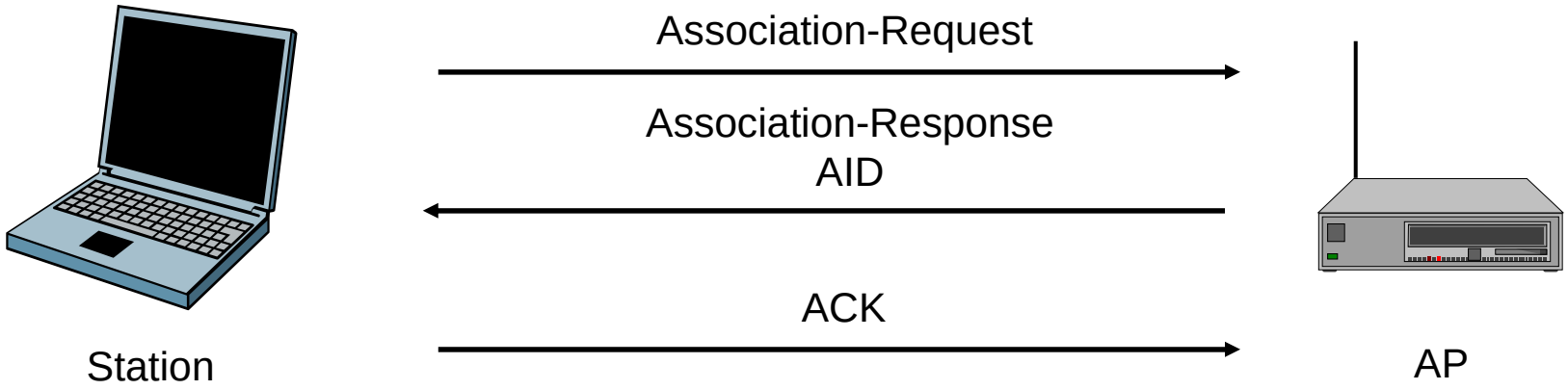
Authentifizierung

- Möglichkeit 2: Shared Key Authentication
  - Basiert auf Challenge-Response-Verfahren
    - Station sendet Authentication-Management Dateneinheit an Zugangspunkt
    - Zugangspunkt antwortet mit Authentication-Management Dateneinheit
      - enthält einen zufälligen, 128-Byte langen Challenge-Text
    - Station kopiert den erhaltenen Challenge-Text
      - Generiert Prüfsumme ICV und neuen IV
      - verschlüsselt Challenge-Text und ICV mit ihrem geheimen WEP-Schlüssel
      - sendet Ergebnis samt Initialisierungsvektor (IV) an den Zugangspunkt
    - Zugangspunkt empfängt verschlüsselten Text und ICV
      - Entschlüsselt Text mit seinem geheimen WEP-Schlüssel
      - Prüft Übereinstimmung mit ursprünglichem Challenge-Text
    - Zugangspunkt sendet Authentication-Management-Dateneinheit, die Ergebnis enthält

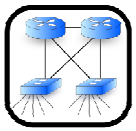


4.5.4 Assoziierung

- Herstellung einer eindeutigen Verbindung zwischen Station und AP
  - Erfolgt im direkten Anschluss an Authentifizierung
  - Station sendet Association-Request Dateneinheit
  - Bei Erfolg antwortet AP mit Association-Response
    - Enthält Assocoiation-ID (AID) über die eine Station eindeutig identifiziert werden kann
      - Wird u.a. für Power-Management benötigt
  - Bei Fehlschlagen der Assoziierung antwortet AP mit Disassociation
  - Station bestätigt mit ACK den Empfang des Association-Response

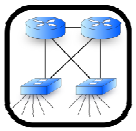


4.5.5 Reassoziierung



- Station führt Handover bei keiner oder schlechter Verbindung zum Zugangspunkt durch
  - Station führt Scanning nach neuem AP durch
  - Station sendet Reassociation-Request an neuen AP
    - Enthält die Adresse des alten Zugangspunkts
  - AP antwortet mit Reassociation-Response
    - Enthält neue AID, die für diesen Zugangspunkt gültig ist
  - Station bestätigt Empfang der Reassociation-Response mit ACK
  - AP informiert alle anderen Zugangspunkte des Distribution Systems über Reassoziierung
- Handoff auf Netzwerkschicht bei Subnetzwechsel notwendig
  - Siehe Teil IV: Mobiles Internet

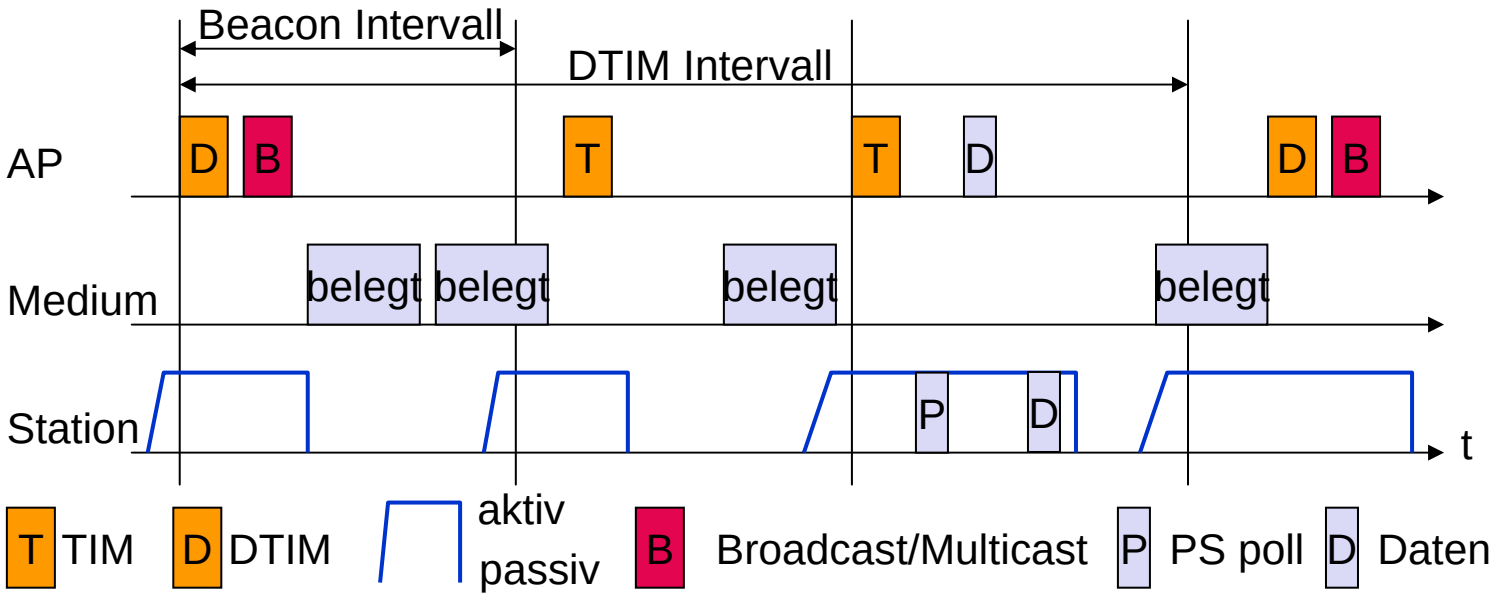
4.5.6 Power-Management



- Ziel
  - Die Stationen sollen möglichst wenig Energie verbrauchen.
- Betriebsmodi bei IEEE 802.11
  - Active Mode (AM)
    - Sende-/Empfangseinheit aktiv
      - Daten können gesendet und empfangen werden
  - Power Save (PS)
    - Sende-/Empfangseinheit ausgeschaltet
      - Kein Empfang oder Senden von Daten möglich
      - Dateneinheiten für diese Station müssen zwischengespeichert werden
        - Infrastruktur-Netz: Zugangspunkt
        - Ad-hoc Netz: alle Stationen müssen zwischenspeichern können
      - Sender signalisiert Übergang in PS-Modus über das Power-Management-Feld einer Dateneinheit
- Grundsätzlicher Ablauf
  - Stationen befinden sich die meiste Zeit im PS-Modus
  - Zwischenspeicherung von Dateneinheiten durch Zugangspunkte
  - Stationen wechseln zu festgelegten Zeitpunkten in den AM-Modus
  - Stationen rufen zwischengespeicherte Dateneinheiten ab
  - Station wechselt zurück in den PS-Modus

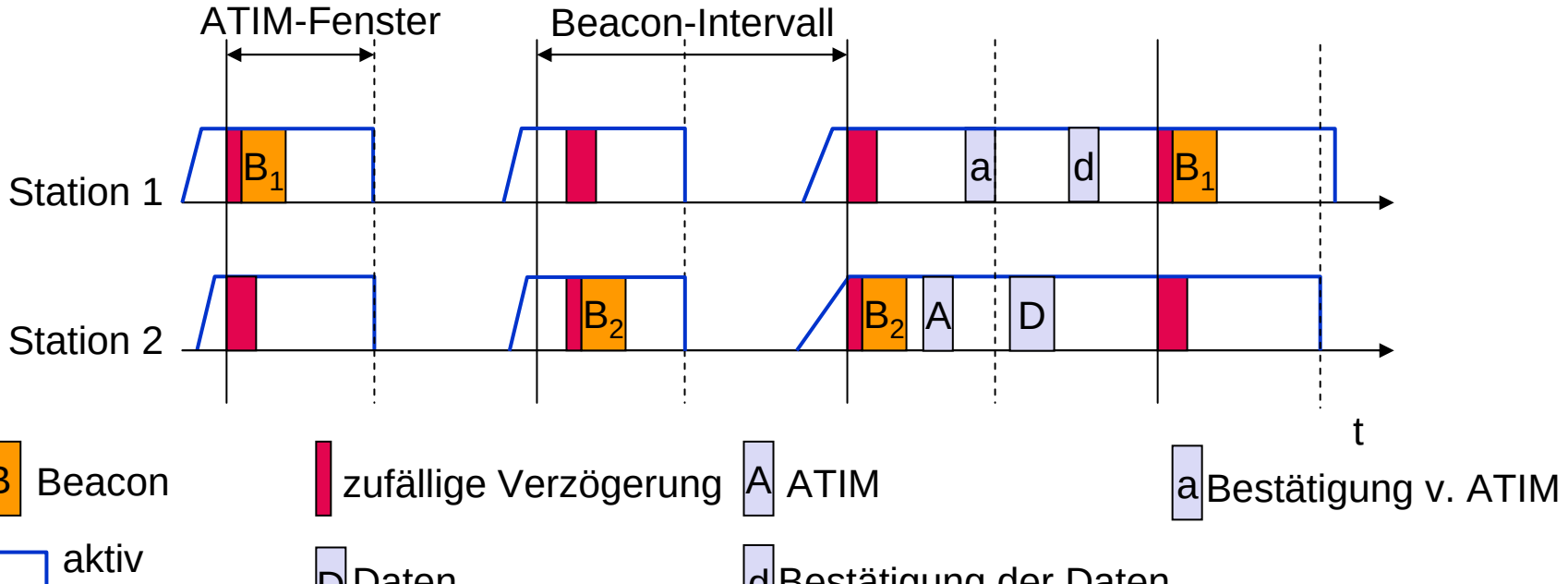
Power-Management in einem BSS

- Zugangspunkt für Zwischenspeicherung von Dateneinheiten verantwortlich
  - Annahme: verfügt über eine Stromversorgung und deshalb immer aktiv
- Traffic Indication Map (TIM)
  - Bekanntgabe von zwischengespeicherten Dateneinheiten (AIDs)
  - Kann in einem Beacon enthalten sein
- Delivery TIM Interval (DTIM-Intervall)
  - Intervall für zwischengespeicherte Broadcast/Multicast Dateneinheiten
    - Entspricht drei Beacon Intervallen
  - Werden nur einmalig an alle Stationen gesendet
- Abruf zwischengespeicherter Dateneinheiten mit Power Save Poll (PS-Poll)



Power-Management in einem IBSS

- Ad-hoc Traffic Indication Message (ATIM)
  - ATIM-Fenster
    - In diesem Zeitraum können alle Stationen Daten empfangen
    - Es können nur Beacons oder ATIMs gesendet werden
    - Kollisionen von ATIMs möglich (Skalierbarkeit?)
  - Bekanntgabe von Empfängern durch die sendende Station

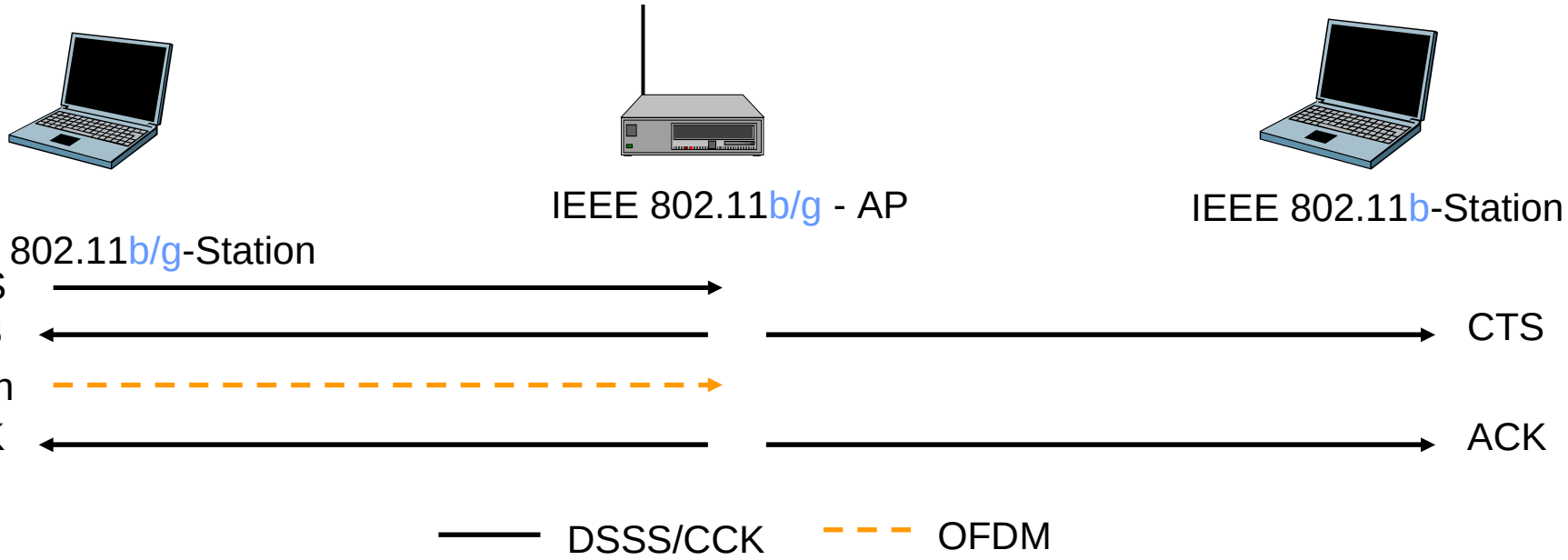


4.6 Erweiterungen der MAC-Schicht

- Protection-Mechanismus
  - Definiert in IEEE 802.11g
  - Koexistenz von 802.11, 802.11b und 802.11g im 2.4 GHz-Band
- Transmit Power Control
  - Definiert in IEEE 802.11h
  - Automatische Anpassung der Sendeleistung im 5 GHz-Band
- Dynamic Frequency Selection
  - Definiert in IEEE 802.11h
  - Automatischer Kanalwechsel im 5 GHz-Band
- Quality of Service (QoS)
  - Definiert in IEEE 802.11e
  - Bereitstellung von QoS-Fähigkeiten

Protection-Mechanismus

- Ziel
  - Koexistenz von 802.11, 802.11b und 802.11g im 2.4 GHz-Band
- Vorgehensweise
  - Beacons werden immer mit DSSS bzw. CCK gesendet
  - Anpassung des RTS/CTS-Mechanismus
    - Notwendig falls sich 802.11 oder 802.11b Stationen im BSS befinden



Protection-Mechanismus

- Maximaler Durchsatz einer TCP-Verbindung

Distance (Feet)	802.11b (Mbps)	802.11a (Mbps)	802.11g-only (Mbps)	802.11g Mixed Environment with CTS-to-self (Mbps)	802.11g Mixed Environment with RTS/CTS (Mbps)
10	5.8	24.7	24.7	14.7	11.8
50	5.8	19.8	24.7	14.7	11.8
100	5.8	12.4	19.8	12.7	10.6
150	5.8	4.9	12.4	9.1	8.0
200	3.7	0	4.9	4.2	4.1
250	1.6	0	1.6	1.6	1.6
300	0.9	0	0.9	0.9	0.9

© Dell Computer

Transmit Power Control - TPC

- Ziel
  - Automatische Anpassung der Sendeleistung
    - Festgelegte maximal zulässige Sendeleistung nicht überschreiten
    - Bestimmung der minimal notwendigen Sendeleistung
- Vorgehensweise
  - Während Assoziierung/Reassoziierung
    - Austausch über minimal und maximal zulässige Sendeleistung
    - Assoziierung/Reassoziierung einer Station wird ggf. verweigert
  - Beacons von Zugangspunkt (BSS) / Station (IBSS) enthalten maximal zulässige Sendeleistung eines Kanals
  - Dynamische Anpassung der Sendeleistung
    - Kommunizierende Stationen tauschen Verbindungsinformationen aus
      - TPC-Request/TPC-Response-Dateneinheiten
    - Algorithmus zur Anpassung der Sendeleistung ist nicht spezifiziert
      - Herstellerspezifische Lösungen

Dynamic Frequency Selection

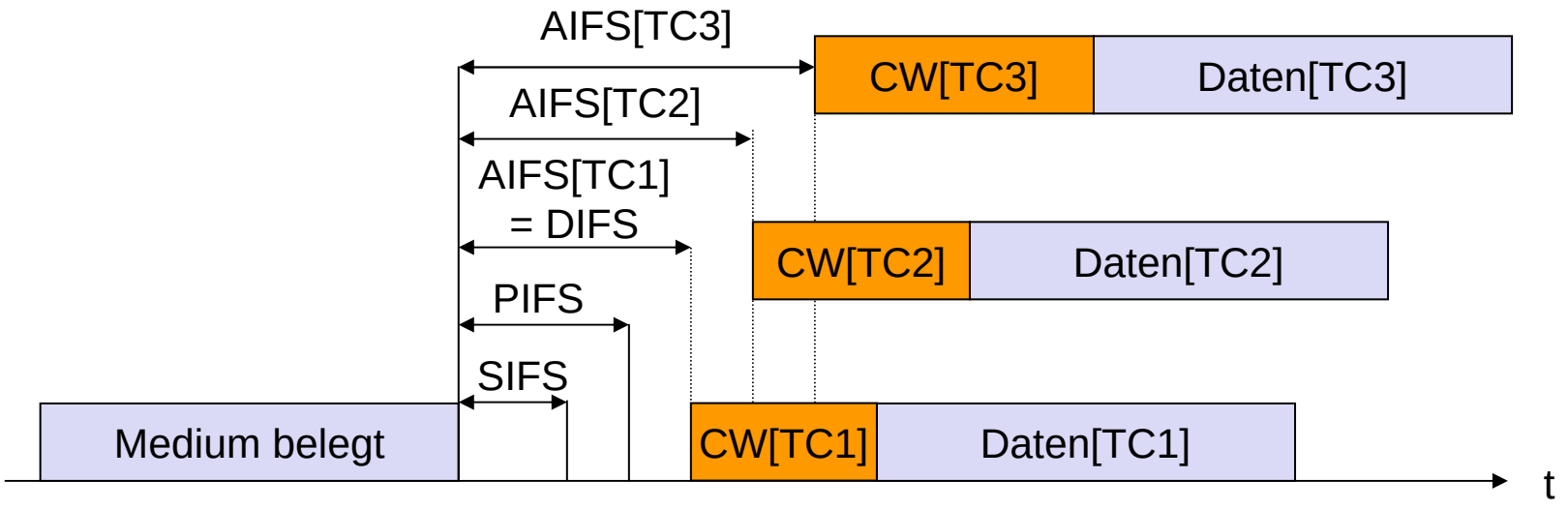
- Ziel
  - Automatischer Kanalwechsel im 5 GHz Band
    - Koexistenz mit Radar- und HIPERLAN/2 Systemen im gleichen Frequenzband
- Vorgehensweise
  - Kanal wird für eine gewisse Zeit (10 Sekunden) „ruhig gestellt“
    - Überprüfung des Kanals auf Verwendung durch andere Systeme
    - Über Beacons initiiert
    - Kriterien zur Erkennung eines anderen Systems nicht standardisiert
  - Medium wird in Sendepausen (SIFS/DIFS) nach anderen Systemen abgehört
  - Beauftragung anderer Stationen zur Überprüfung eines bestimmten Kanals
    - Senden von Measurement-Request-/Measurement-Response-Dateneinheiten
  - Fremdes System auf Kanal erkannt
    - Signalisierung eines Kanalwechsels
      - Beacons, Channel-Announcement-Dateneinheiten

Quality of Service

- Ziel
  - Bereitstellung von QoS-Fähigkeiten für zeitkritische Daten (z.B. VoIP)
    - QBSS = Funkzelle die QoS bereitstellt
- Vorgehensweise
  - Einführung von zwei neuen Medienzugriffsverfahren
    - Enhanced Distributed Coordination Function (EDCF)
      - Basiszugriffsverfahren in QBSS (ersetzt DCF)
      - Nur in CP (Contention Period) möglich
    - Hybrid Coordination Function (HCF)
      - Zentrale Verwaltung der QBSS
      - Hybrid Coordinator (HC) steuert Medienzugriff (ersetzt PCF)
      - Sowohl in CP als auch CFP möglich
  - Block-Acknowledgement-Mechanismus
    - Station kann bis zu 64 Dateneinheiten im Abstand von SIFS senden
    - Nach letzter Dateneinheit sendet die Station ein Block-ACK-Request
    - Empfänger antwortet mit Block-ACK-Response

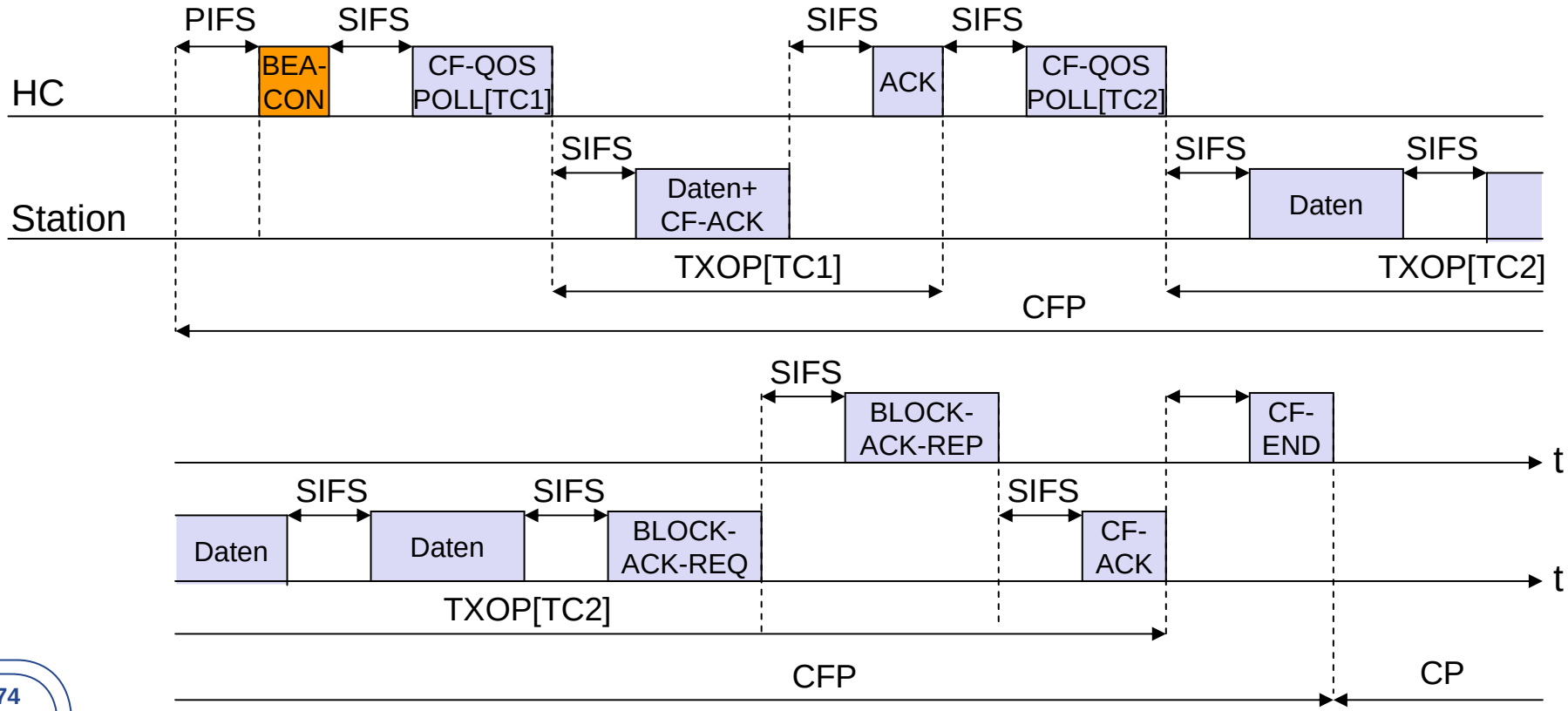
Enhanced Distributed Coordination Function

- Priorisierung von Daten durch 8 unterschiedliche Traffic Categories (TC)
- Höhere Priorität resultiert in geringerer Wartezeit beim Medienzugriff
  - Arbitration Interframe Space (AIFS)
    - Abhängig von verwendeter TC
  - Unabhängiger Backoff-Algorithmus für jede TC
    - Unterschiedliche Wertebereiche für das Wettbewerbsfenster (CW)
  - Interner Scheduler
    - Bei virtuellen Kollisionen werden Dateneinheiten mit höherer TC bevorzugt behandelt



Hybrid Coordination Function

- Transmission Opportunity (TXOP)
  - Zeitintervall für eine bestimmte Traffic Category
- Station teilen Hybrid Coordinator (HC) mit, für welche Stationen TXOPs benötigt werden
- HC leitet über QoS-Poll CFP für bestimmte TXOP ein



4.7 Zusammenfassung und Ausblick

- WLAN (802.11) hat sich als drahtloses lokales Netzwerk durchgesetzt
  - Betreibbar sowohl im Infrastruktur-Modus als auch Ad-hoc Modus
- Physikalische Schicht
  - Einsatz von DSSS im Basisstandard
  - Einsatz von OFDM in neueren Lösungen mit höherer Datenrate
  - Varianten sowohl für 2,4 GHz als auch für 5 GHz Band
  - Dateneinheiten beinhalten Information über die gewünschte Datenrate
    - Anfang wird immer mit langsamster Variante gesendet
    - Rückwärtskompatibilität
    - Längenangabe in Form einer Zeitangabe

Zusammenfassung und Ausblick

- Medienzugriff
  - CSMA/CA-Verfahren
    - CSMA/CD nicht anwendbar (versteckte Endgeräte, gleichzeitiges Senden und Empfangen …)
  - Zwei Zugriffsarten
    - Distribution Coordination Function (dezentral)
    - Point Coordination Function (zentral)
  - ARQ-Verfahren, Fragmentierung und Sicherheitsmechanismen in der MAC-Schicht
  - MAC-Dateneinheiten
    - Komplexer als z.B. bei Ethernet
    - Variable Kopflänge, Zeitangabe, mehrere Adressen
    - Frame-Controll Feld mit zusätzlicher Information
- MAC-Management
  - Synchronisation
  - Sicherheit
  - Scanning
  - Assoziierung/Reassoziierung
  - Power-Management

Erweiterungen in IEEE 802.11

- Inzwischen: zahlreiche Erweiterungen

IEEE Standard	Beschreibung
802.11	WLAN für 1-2 Mbit/s im 2,4 GHz-Band
802.11a	WLAN bis 54 Mbit/s im 5 GHz-Band
802.11b	Erweiterung von 802.11 bis 11 Mbit/s im 2,4 GHz Band
802.11d	Anpassung an nationale Regelungen
802.11e	MAC-Erweiterung zu 802.11a und b, um Quality of Service und verbessertes Power Management zu ermöglichen
802.11f	Kommunikation zwischen den Access Points (IAPP, Inter Access Point Protocol)
802.11g	Höhere Datenraten (bis 54 Mbit/s) im 2,4 GHz-Band
802.11h	Höhere Datenraten auf dem 5 GHz-Band mit automatischer Leistungsregelung und dynamischer Frequenzwahl
802.11i	MAC-Erweiterung, um verbessertes Sicherheits- und Authentifizierungsmechanismen zu ermöglichen

Aktuelle IEEE 802.11 Arbeitsgruppen

Arbeits-gruppe	Beschreibung
802.11j	Spezielles WLAN für Japan im 4,9 GHz und 5 GHz Band
802.11k	Interface für höhere Layer für Zugriff auf PHY- und MAC-Informationen
802.11n	„Next Generation WiFi“, Datenraten > 100 Mbit/s
802.11p	WiFi für Kommunikation zwischen Autos
802.11r	Minimierung der Verzögerung beim Wechsel der BSS
802.11s	Wireless Distribution System (WDS)
802.11t	Tests, Vergleiche und Einsatz von WLAN Geräten
802.11u	Spezifizierung der Informationen, die zwischen APs im DS ausgetauscht werden
802.11v	Interworking mit anderen Netzwerken

Mobilkommunikation

Teil III: Drahtlose lokale Netze

Kapitel 5

Mobile Ad Hoc Netze

Kapitelübersicht

I. Einleitung
1. Einführung und Grundlagen

II. Drahtlose Telekommunikationssysteme
2. GSM
3. UMTS

III. Drahtlose lokale Netze
4. IEEE 802.11 / WiFi
5. Mobile Ad Hoc Netze

IV. Drahtlose innerstätische Netze
6. IEEE 802.11s
7. IEEE 802.16 / WiMax

V. Drahtlose persönliche Netze
8. Bluetooth
9. IEEE 802.1.54 / ZigBee

VI. Positionsbestimmung
10. Positionsbestimmung

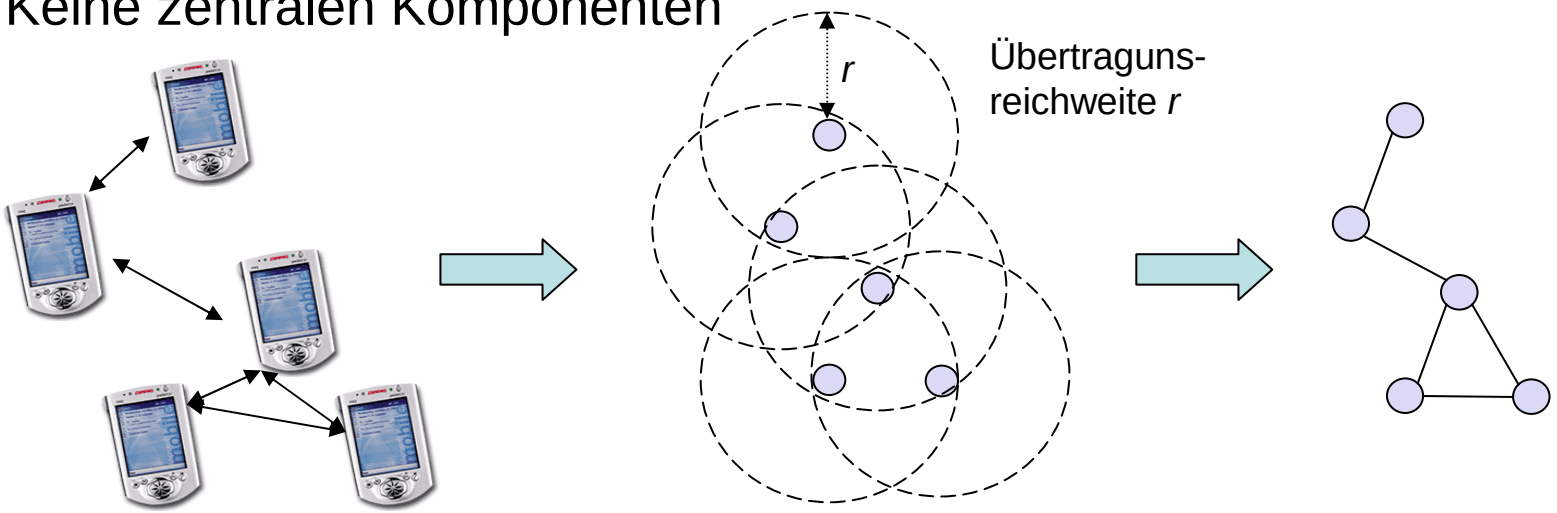
VII. Mobiles Internet
11. Mobile Vermittlungsschicht
12. Mobile Transportschicht

5 Mobile Ad-hoc Netze
- 5.1 Routing-Protokolle für MANETs
- 5.2 Aktuelle Forschungsgebiete
- 5.3 MANETs am ITM

Übungen
Referenzen

5 Mobile Ad-hoc-Netze (MANETs)

- Spontaner Zusammenschluss drahtloser Endgeräte
  - keine Infrastruktur (Basisstation/Access Points), kein Backbone
  - Verwendete Endgeräte können mobil sein
- Paketbasierte Vermittlung von Daten
  - Routen zwischen zwei Geräten können *mehrere Hops* lang sein
- Jedes Gerät ist Endgerät und gleichzeitig *Router*!
- Ad-hoc-Netze sind *selbst organisierend*
  - Keine zentralen Komponenten



Vorteile und Anwendungen

- Vorteile mobiler Ad-hoc-Netze
  - Netze können einfach, kostengünstig und schnell aufgebaut werden
    - Z.B. mit 802.11b im lizenzfreien Band (2.4 GHz)
  - Sendeleistung kann reduziert werden
    - Entfernung bis zu Nachbarn evtl. geringer als zur Basisstation
  - Robuster gegenüber dem Ausfall einzelner Komponenten
    - da vollständig dezentral
- Anwendung: Überall wo kein Zugriff auf Infrastruktur besteht
  - Militärischer Bereich
    - Verbände von Soldaten, Panzern, Flugzeugen,...
  - Ziviler Bereich
    - Konferenzen, Ausstellungen, Meetings, Vorlesungen, Gaming
    - Car-to-Car-Kommunikation, Netz für Taxifahrer, Polizeistreifen
    - Erweiterung zellularer Systeme (WLAN, UMTS)
  - Katastropheneinsätze
    - Nach Zusammenbruch der Infrastruktur (Telefonnetz bei Erdbeben)
    - Rettungsaktionen z.B. nach Lawinenunglücken

Eigenschaften von MANETs

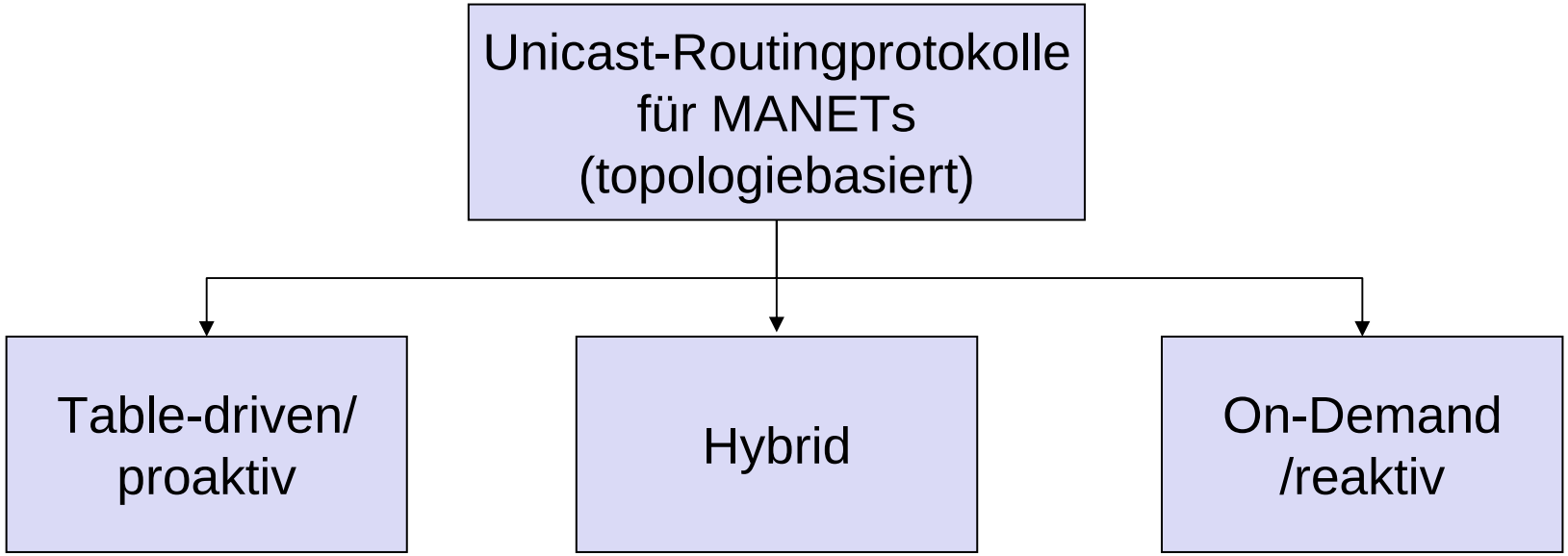
- Hoch dynamische Netztopologie
  - Mobilität der Geräte
  - Sich verändernde Eigenschaften des drahtlosen Kanals (Fading)
  - Partitionierung und Zusammenschlüsse von Ad-hoc-Netzen möglich
- Asymmetrische/Unidirektionale Verbindungen
  - Verbindungsqualität kann in beide Richtungen unterschiedlich sein
- Drahtloses Medium ist Semi-Broadcast-Medium
  - Versteckte und ausgelieferte Endgeräte
- Begrenzte Batterieleistung der mobilen Geräte
  - Verstärkt durch Signalisierungsverkehr z.B. des Routingprotokolls
- Begrenzte Bandbreite
  - Verstärkt durch Signalisierungsverkehr z.B. des Routingprotokolls und MAC-Protokoll (Kollisionen, versteckte Endgeräte etc.)
- Zeitliche Synchronisation der Geräte schwierig
  - Erschwert z.B. Energiesparmodi der Geräte (z.B. periodisches Schlafen)
- Sicherheitsmechanismen schwierig anzuwenden
  - Abhören des drahtlosen Kanals
  - Jedes Gerät muss Pakete an andere weiterleiten können

[III.10]

5.1 Routingprotokolle für MANETs

- Für Festnetz entwickelte Routingprotokolle (z.B. RIP, OSPF, ...) können nicht ohne weiteres in mobilen Ad-hoc-Netzen angewendet werden
  - Langsame Konvergenz
  - Zu hoher Overhead
- Routingprotokolle für MANETs müssen dagegen schnell konvergieren und möglichst wenig Bandbreite für den Kontrollverkehr verwenden
- Verschiedene Metriken in mobilen Ad-hoc-Netzen möglich
  - Minimale Anzahl Hops
  - Minimaler Delay
  - Minimale Paketverluste
  - Minimale Stausituationen (Load Balancing)
  - Minimale Interferenzen
  - Maximale Signalstabilität und zeitlich stabile Route
  - Maximale Batterielaufzeit eines mobilen Gerätes
  - Maximale Lebenszeit des gesamten Netzes
    - z.B. bis Partitionierung durch Batterielaufzeit-bedingten Ausfall von Knoten

Klassifikation von Routingprotokollen



- OLSR
- LANMAR
- TBRPF
- FSR
- STAR
- DSDV
- ...

- ZRP
- ...

- AODV
- DYMO
- DSR
- TORA
- ...

Hier nicht behandelt: positionsbasierte Routingprotokolle

Abkürzungen für Routingprotokolle

- OLSR — Optimized Link State Routing
- LANMAR — Landmark Ad Hoc Routing
- TBRPF — Topology Dissemination based on Reverse-Path Forwarding
- FSR — Fisheye State Routing
- STAR — Source Tree Adaptive Routing
- DSDV — Destination-Sequenced Distance Vector
- ZRP — Zone Routing Protocol
- DSR — Dynamic Source Routing
- AODV — Ad Hoc On Demand Distance Vector
- DYMO — Dynamic MANET On-demand
- TORA — Temporally-Ordered Routing Algorithm

Übersicht Ad-hoc-Routingprotokolle

- Fluten für den Datenversand
  - Einfachstes „Protokoll“: Jeder Knoten leitet jedes Paket genau einmal weiter
  - Sehr hoher Overhead
- Proaktives Routing (Table-driven)
  - Es werden fortlaufend Routen zu allen anderen Knoten unterhalten
  - Routen stehen ständig zur Verfügung
  - Konstant hoher Kontrolloverhead
- Reaktives Routing (On-demand)
  - Routen werden nur bei Bedarf bestimmt (Route Discovery)
  - Zeitverzögerung zu Beginn, da zunächst Route bestimmt werden muss
  - Kontrolloverhead abhängig von Anzahl der Verbindungen
- Hybrides Routing
  - Mischung aus proaktivem und reaktivem Routing
- Es gibt (bisher) nicht *das* Routingprotokoll für mobile Ad-hoc-Netze
  - Je nach Szenario ist das eine oder andere besser geeignet
  - Zahlreiche Publikationen auf diesem Gebiet
- Standardisierung von Ad-hoc-Routingprotokollen: IETF MANET WG  [III.9]

5.1.1 Proaktive Routingprotokolle

- Knoten bestimmt fortlaufend Routen zu allen anderen Knoten im Netz
  - Distance Vector Routing
    - Basiert auf Bellman-Ford Algorithmus
    - Danach ermittelt jeder Knoten jeweils für jeden anderen Knoten im Netz den Nachbarn (nächsten Hop), über den die kürzeste Route zu diesem Knoten besteht und die Länge dieser Route
    - Diese Information wird periodisch an alle Nachbarn versendet
    - Beispiele
      - Festnetz: Routing Information Protocol (RIP)
      - Ad-hoc-Netz: Destination-Sequenced Distance Vector Protocol (DSDV)
  - Link State Routing
    - Jeder Knoten versendet periodisch den Status seiner Links, zusammen mit den von Nachbarn empfangenen Link Status Informationen
    - Dadurch kennt jeder Knoten gesamte Netztopologie
    - Kürzeste Route zu jedem Knoten kann mit Dijkstra‘s Shortest Path First Algorithmus ermittelt werden
    - Beispiele
      - Festnetz: Open Shortest Path First (OSPF)
      - Ad-hoc-Netz: Optimized Link State Routing (OLSR) → Anhang

5.1.2 Reaktive Routingprotokolle

- Prinzip
  - Knoten kennt nur die Routen, die er auch benötigt
  - Keine periodischen Aktualisierungen
- Aufgaben eines reaktiven Routingprotokolls
  - Auffinden einer Route (Route Discovery)
    - Nur wenn ein Knoten Daten zu einem Zielknoten senden möchte, jedoch noch keine Route zu diesem Zielknoten besitzt
  - Aufrechterhaltung einer Route (Route Maintainance)
    - Nur wenn eine Route verwendet wird, dann wird auch dafür gesorgt werden, dass diese auch weiterhin funktioniert
- Vergleich mit proaktiven Routingprotokollen
  - Vorteil
    - Nur verwendete Routen werden bestimmt und aufrecht erhalten
    - Kein periodisches Versenden von Nachrichten nötig → Ressourceneinsparung
  - Nachteil
    - Zeitverzögerung zu Beginn einer Kommunikation, da Route erst noch bestimmt werden muss
    - Kontrolloverhead abhängig von Anzahl der Verbindungen und Mobilität

Ad-hoc On-Demand Distance Vector Routing Protokoll (AODV)

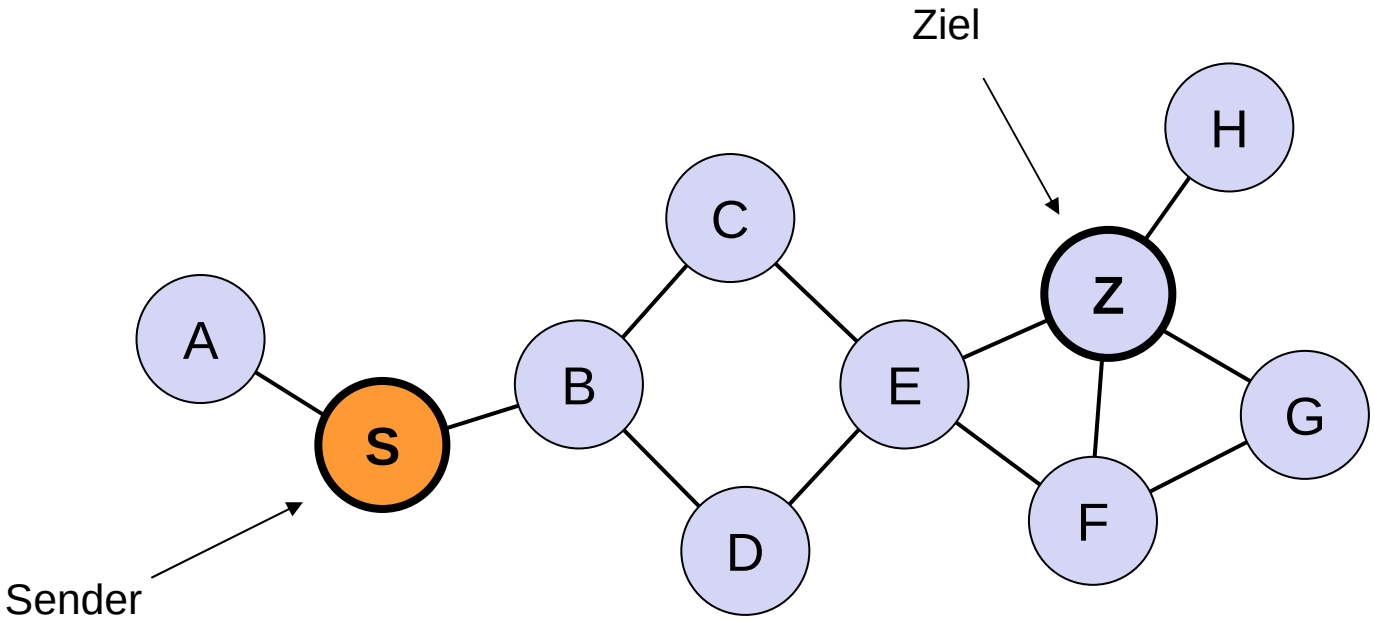
→ Auffinden einer Route

- Sender S flutet das Ad-hoc-Netz mit einem Route Request (RREQ)
  - RREQ enthält Zieladresse Z
- Knoten, die an der Weiterleitung des RREQs beteiligt sind, speichern die Adresse des Knotens, von welchem das RREQ empfangen wurde
- Es entsteht der so genannte „Reverse Path“ in Richtung des Senders S
  - Funktioniert nur bei bidirektionalen Links!
- Erhält Zielknoten Z den RREQ, beantwortet er dieses durch ein Route Reply (RREP)
  - RREP enthält Quelladresse S
- Weiterleitung des RREPs in Richtung von Knoten S ist direkt über den zuvor aufgebauten Reverse Path möglich
- Bei der Weiterleitung des RREPs wird der so genannte „Forward Path“ in Richtung des Zielknotens Z aufgebaut
- Der aufgebaute Forward Path wird für den Datenverkehr verwendet

→ Wird eine Route von S nach Z aufgebaut, so existiert automatisch auch eine Route von Z nach S!

AODV: Fluten des RREQs I

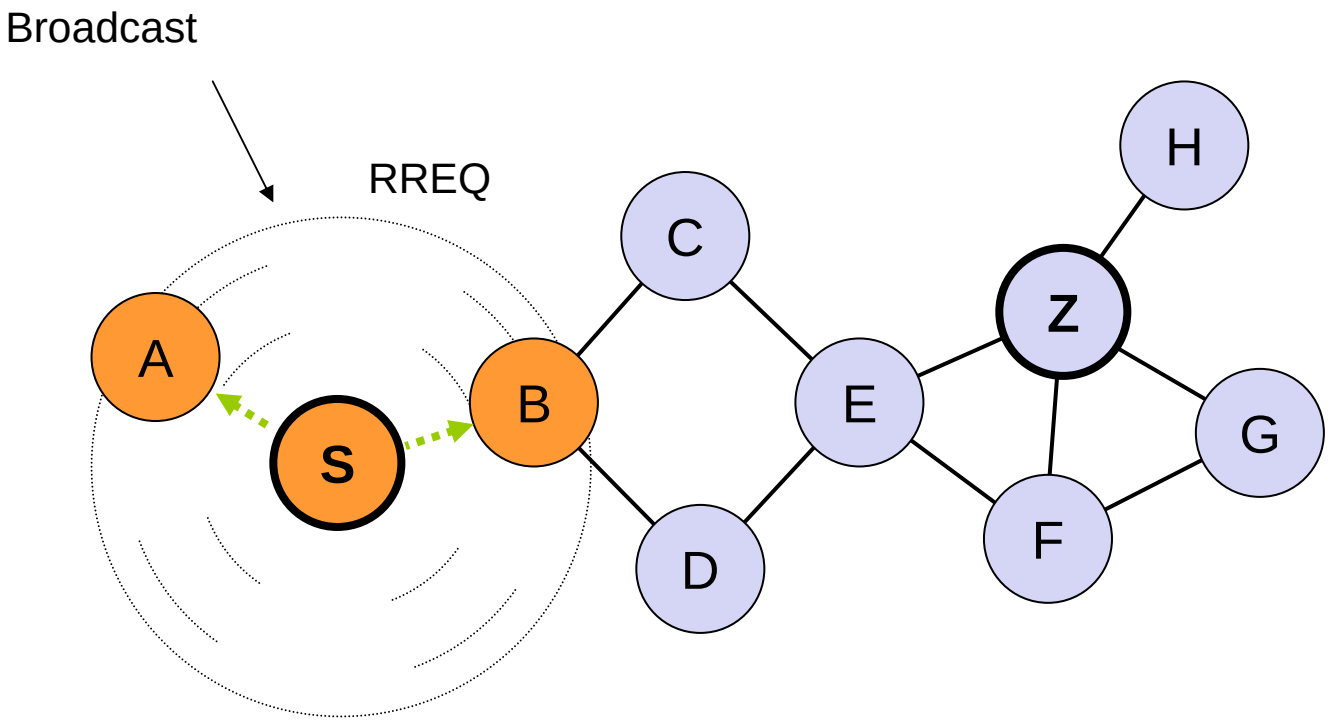
Suche eines Pfades von S nach Z:



Knoten, der RREQ empfangen hat

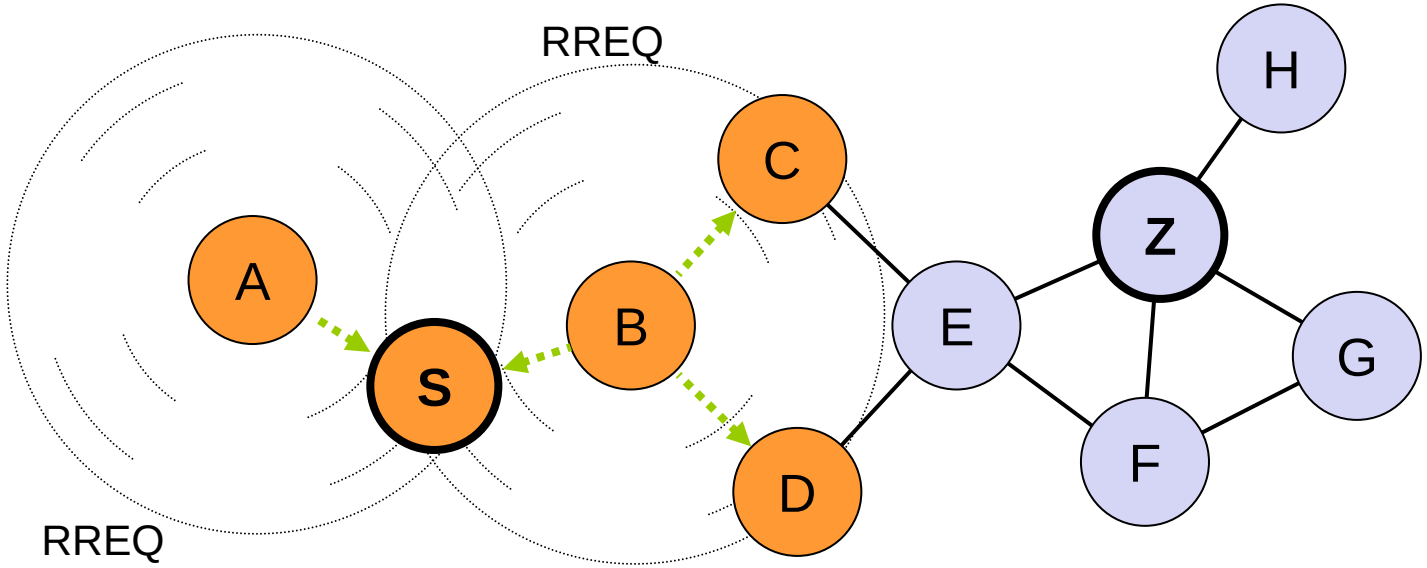
Knoten in Sende- und Empfangsreichweite (bidirektionale Links)

AODV: Fluten des RREQs II



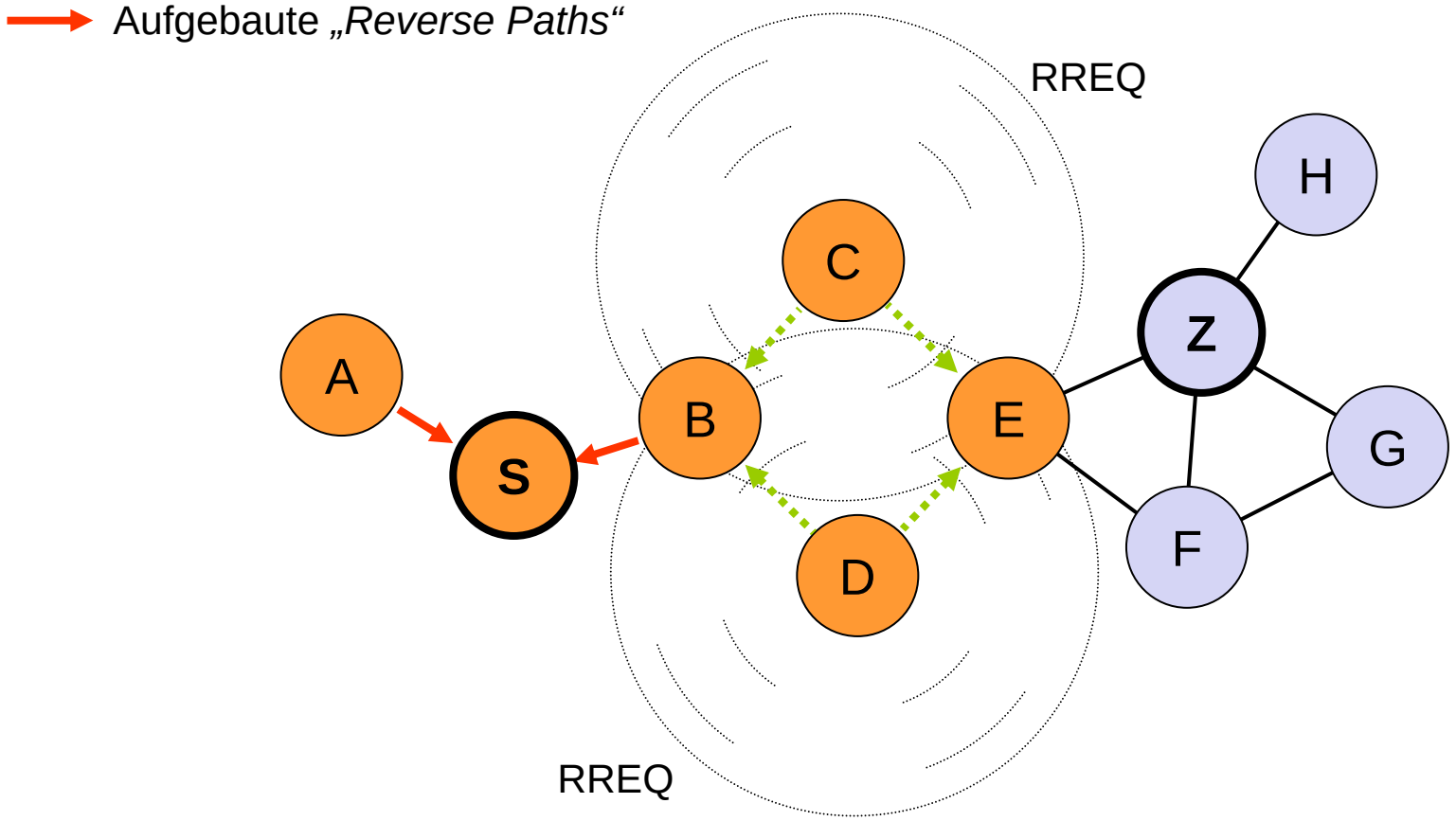
- Sender S verschickt RREQ per Broadcast
  - Alle Nachbarn in Reichweite empfangen das Paket

AODV: Fluten des RREQs III



- Jeder Knoten, der das RREQ empfängt leitet es per Broadcast weiter
- S leitet sein selbst versendetes RREQ nicht erneut weiter!

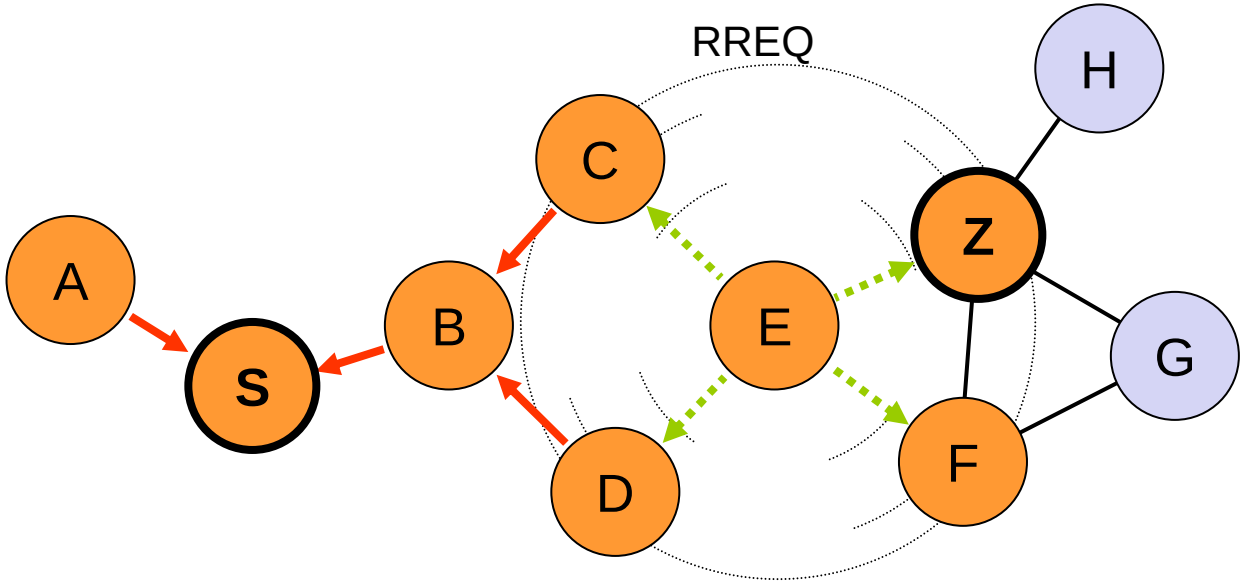
AODV: Fluten des RREQs IV



- Beim Weiterleiten merken sich Knoten woher das RREQ empfangen wurde
  - Es wird der Knoten mit dem geringen Hop-Count zu S gewählt
  - Es bildet sich der so genannte „*reverse path*“ zum Sender S

AODV: Fluten des RREQs V

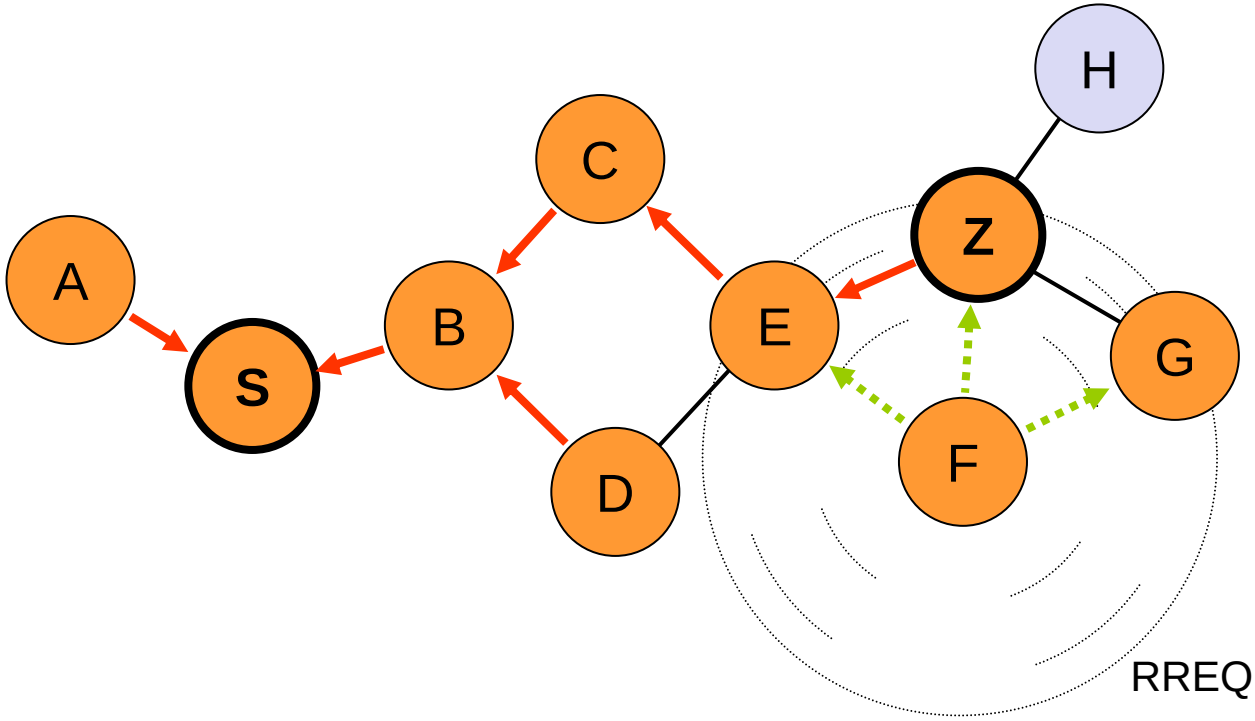
→ Aufgebaute „*Reverse Paths*“



- Duplikate werden durch Sequenznummern erkannt und nicht erneut weitergeleitet
  - Erfordert Zustandshaltung in den Knoten

AODV: Fluten des RREQs VI

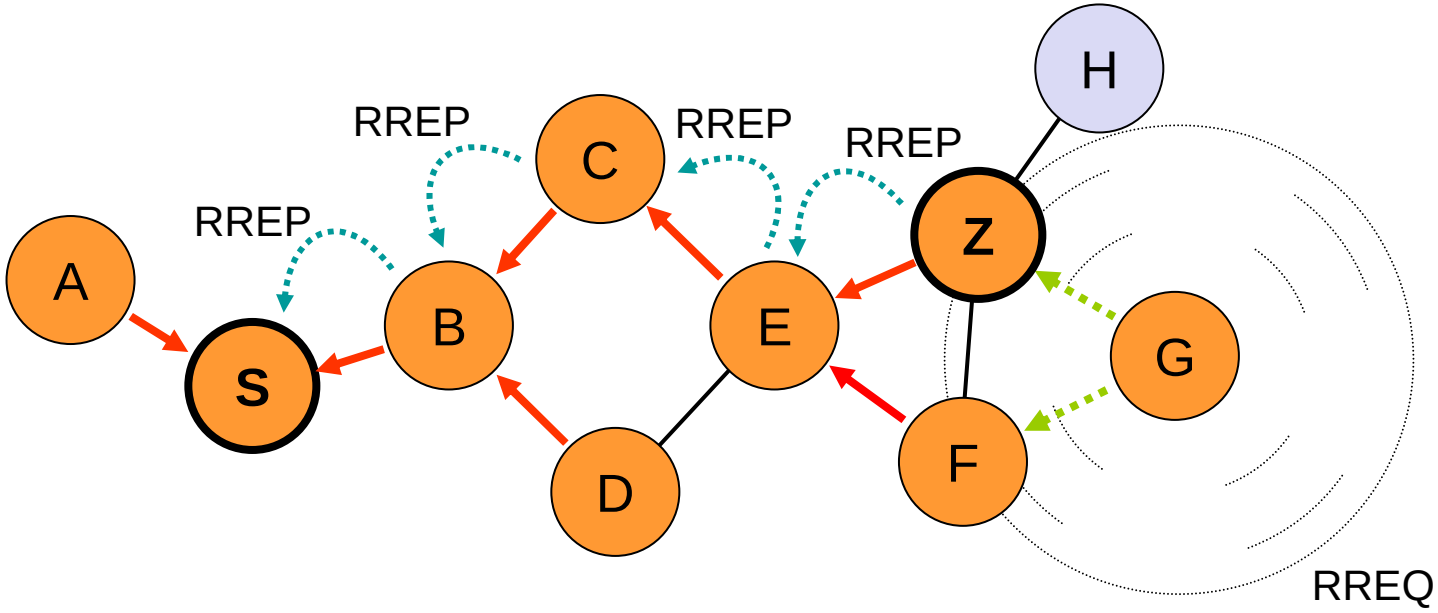
→ Aufgebaute „*Reverse Paths*“



- Das Ziel Z hat das von S ausgesendete RREQ empfangen
  - Es besteht jetzt ein vollständiger „*reverse path*“ von Z zu S

AODV: Fluten des RREQs VII

→ Aufgebaute „*Reverse Paths*“

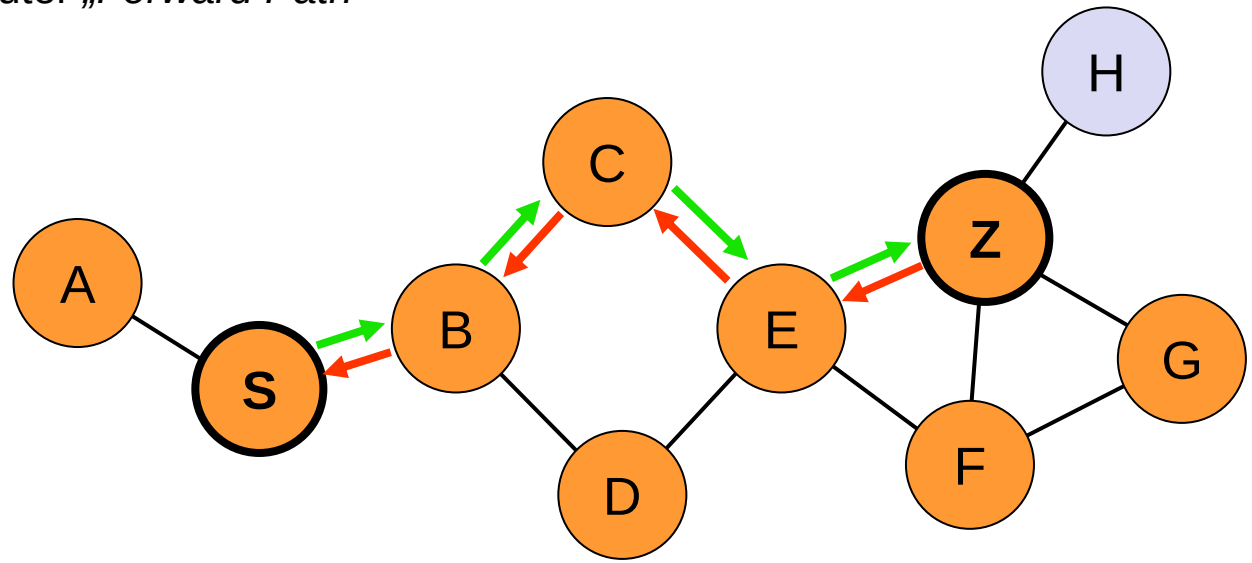


- Knoten Z sendet RREP über „*reverse path*“ zurück zu S
  - Next-Hop-Knoten auf „*reverse path*“ werden direkt adressiert (keine Broadcasts mehr)

AODV: Fluten des RREQs VII

Aufgebaute „*Reverse Paths*“

Aufgebauter „*Forward Path*“



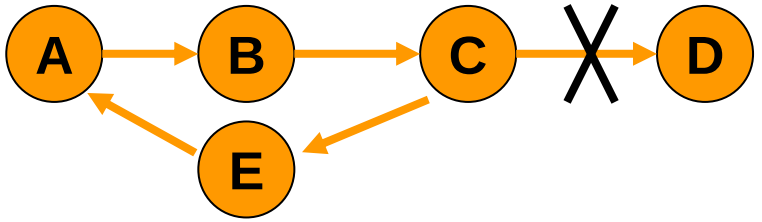
- Es entsteht der „*forward path*“ von S zu Z
  - Dieser wird für den Datentransport von S zu Z verwendet
- Nicht verwendete „*reverse path*“-Einträge werden nach Timeout gelöscht
- Wurde Route von S zu Z aufgebaut, besteht auch Route von Z zu S

AODV: Sequenznummern

- Jeder Knoten besitzt Zielsequenznummer (Destination Sequence Number)
  - Bestimmt die „Aktualität“ von Routinginformationen
  - Wird immer nur erhöht
    - Ausnahme: Überläufe
- RREQ enthält letzte bekannte Zielsequenznummer des Zielknotens
  - Zielknoten oder *Zwischenknoten*, die eine neuere Route (höhere Zielsequenznummer) kennen, antworten mit RREP
    - RREP enthält ebenfalls Zielsequenznummer
  - Kann Aufbau von Routen beschleunigen
  - Wenn mehrere RREP empfangen werden, dann wird der RREP mit der höchsten Zielsequenznummer verwendet
    - Bei gleicher Zielsequenznummer entscheidet geringerer Hop Count

AODV: Aufrechterhalten einer Route

- Reverse/Forwarding Path Einträge werden nach Timeout gelöscht
  - Soft-state Ansatz
- Das Übertragen von Daten entlang einer Route frischt diese auf
  - Timer werden zurückgesetzt
  - Optional werden auch HELLO-Nachrichten zur Auffrischung eingesetzt
- Erkennung von Link-Brüchen
  - Fehlende HELLO-Nachrichten
  - Fehlende Link-layer Acknowledgements (Quittungen auf MAC-Schicht)
- Reaktion auf Link-Brüche: Versenden eines RERR
  - Wird bis zu Quelle weitergeleitet
  - Quelle sucht neue Route mit einem RREQ
  - Enthält erhöhte Zielsequenznummer
- Zielsequenznummern verhindern Schleifen
  - A sendet an D, Link von C nach D bricht
  - RERR von C nach A geht verloren
  - Später sucht C nach D
    - RREQ enthält höhere Zielsequenznummer
  - A empfängt RREQ über C-E-A
  - A sieht höhere Zielsequenznummer und lässt RREP aus



AODV: Optimierungen

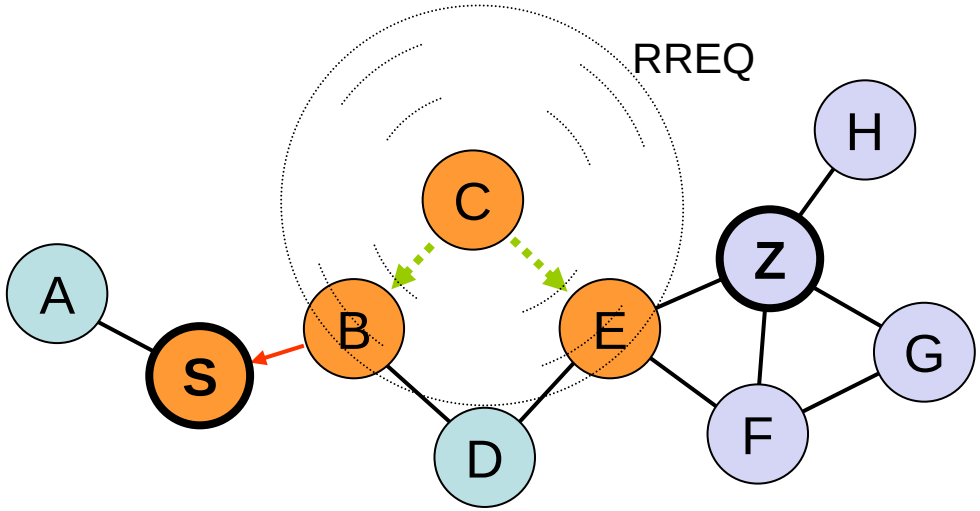
- Expanding Ring Search
  - RREQs werden nicht im kompletten Netz geflutet
    - RREQ zunächst mit kurzer Lebenszeit (TTL) versehen
    - Bleibt Suche erfolglos, wird RREQ mit höherer TTL versendet
  - Entlastet Netz bei Routenbestimmung zu nahe gelegenen Knoten
  - Bei entfernten Knoten
    - Verzögert Routenaufbau
    - Nahe gelegene Knoten müssen viele RREQs weiterleiten
- Local Route Repair
  - Bei Link-Abbruch wird nicht sofort RERR zur Quelle gesendet
    - Knoten, der Link-Abbruch feststellt, sucht neue Route zum Ziel mittels RREQ
  - Kann das Netz durchschnittlich entlasten
  - Kann zu schlechteren (längeren) Routen führen, da nur Teilstrecken neu bestimmt werden

→AODV ist „Standard-Protokoll“ (experimentell) in der IETF (RFC 3561)

Dynamic MANET On-demand (DYMO) Routing

- Weiterentwicklung von AODV
- Wichtigste Neuerung
  - RREQ beinhaltet Liste aller weiterleitenden Knoten
  - Knoten, die RREQ weiterleiten können zusätzliche Routen in Tabelle aufnehmen
  - Bsp: C leitet RREQ(von S über B) an E weiter

    E kennt jetzt Routen zu S, B und C

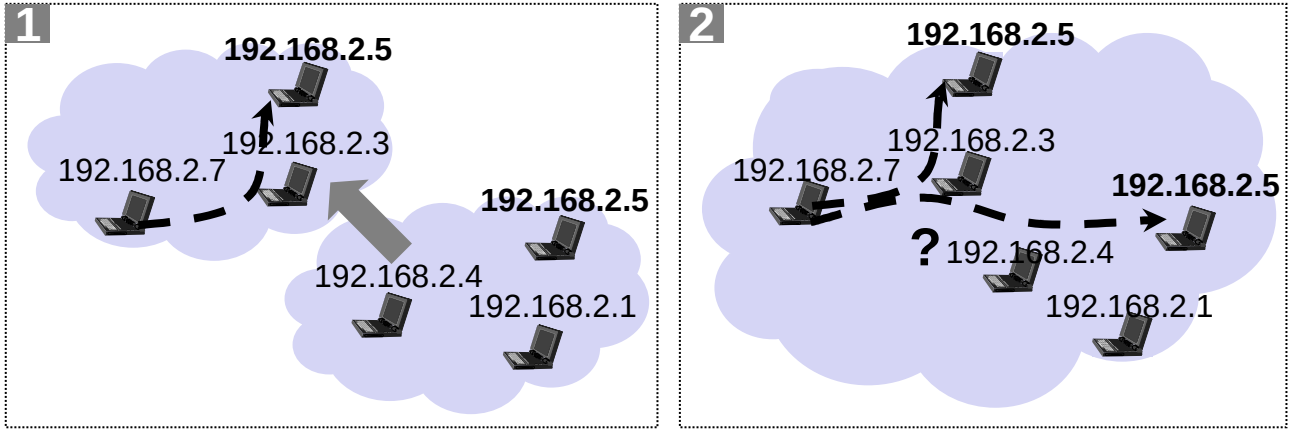


5.2 Aktuelle Forschungsgebiete

- In vielen Gebieten der mobilen Ad-hoc-Netze finden rege Forschungsaktivitäten statt (auch an unserem Institut)
  - Autokonfiguration
    - z.B. Zuweisung von eindeutigen IP Adressen nach verteiltem Mechanismus
  - Service Awareness
    - In mobilen Umgebungen ist das Auffinden mobiler Dienste entscheidend
  - Multicast-Routing
    - Gruppenanwendungen wie E-Learning basieren auf IP Multicast-Routing
  - Integration mit Festnetz
    - Wie kann die Integration von Mobilitätsprotokollen (Mobile IP) und Routing in mobilen Ad-hoc-Netzen realisiert werden?
  - Power Control
    - Kontrolle über die Topologie durch Variation der Sendeleistung der einzelnen Geräte und dadurch Minimierung der Interferenz zwischen den Knoten
  - Sicherheit
    - Wie bereits angesprochen ist die Integration von Sicherheitsmechanismen in mobile Ad-hoc-Netze sehr schwierig
  - Skalierbarkeit, ...

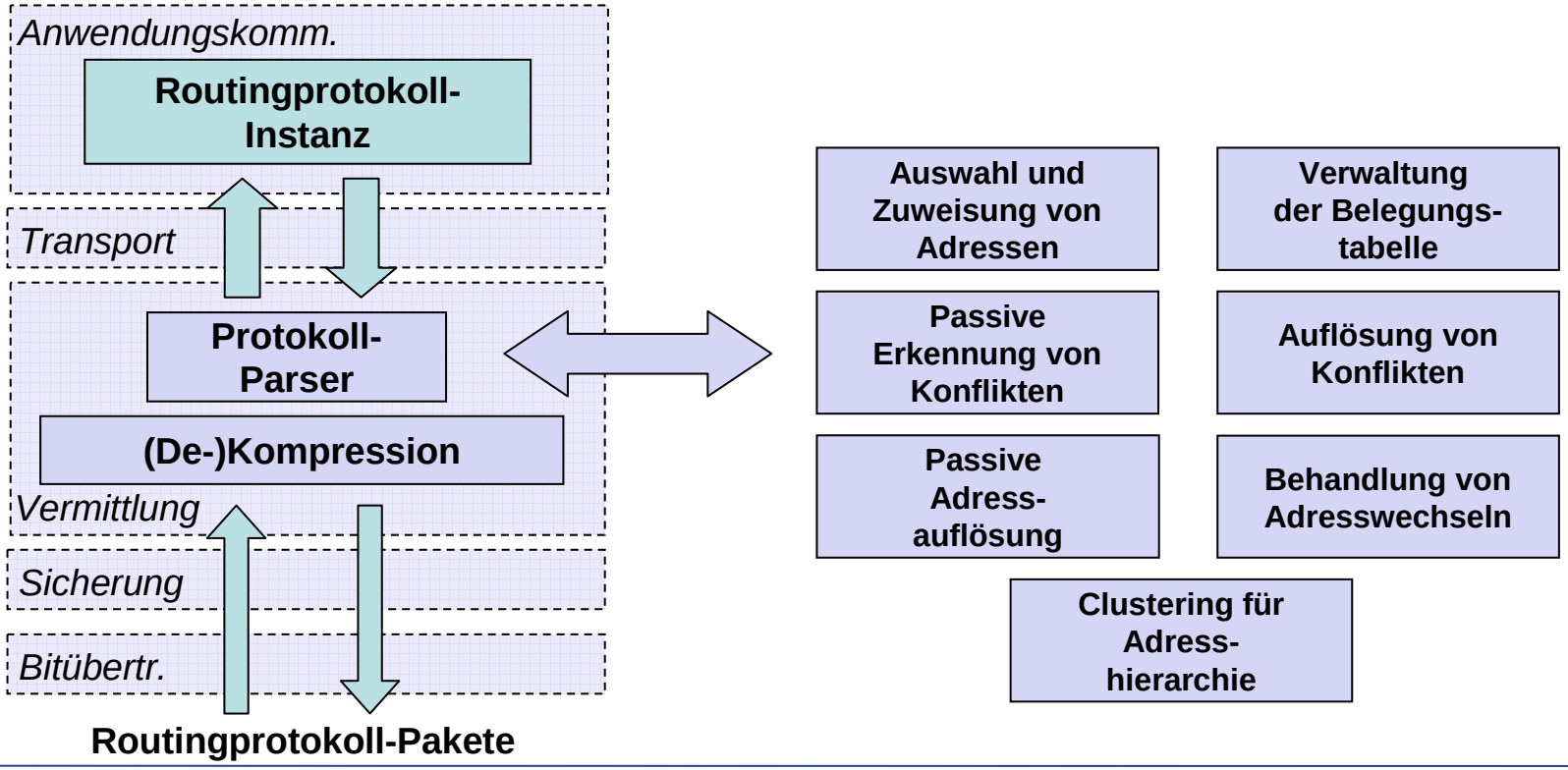
5.3 MANETs am ITM: Autokonfiguration

- IP Routingprotokolle setzen *eindeutige Adressen* voraus
  - Vordefinierte IP Adressen oft nicht möglich
  - Kein Administrator und keine Infrastruturkomponenten (z.B. DHCP-Server)
  - → *Autokonfiguration* erforderlich
- Anforderungen an die IP Autokonfiguration in MANETs
  - *Schnelle* und *effiziente* (bzgl. Ressourcenverbrauch) Zuweisung einer Adresse
  - *Robustheit* gegen Paketverluste
  - Unterstützung für *Netzverschmelzungen*
  - Minimierung der Anzahl der *Adresswechsel*
  - *Flexibilität* bzgl. Routingprotokoll

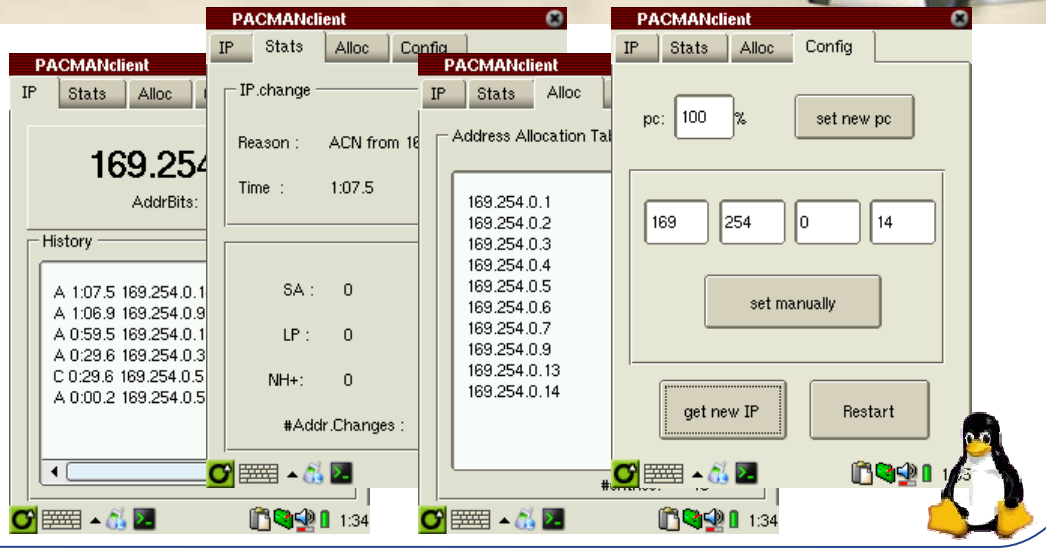


PACMAN: Passive Auto-Configuration of Mobile Ad-hoc Networks

- Robustheit durch hybriden Ansatz
  - Verteilte Belegungstabelle *und* Duplicate Address Detection (DAD)
- Effizienz durch Schichtenübergreifende/passive Mechanismen
  - Anomalieerkennung im Routingprotokollverkehr
  - Passive Synchronisation der Belegungstabelle



Evaluation im Testbett



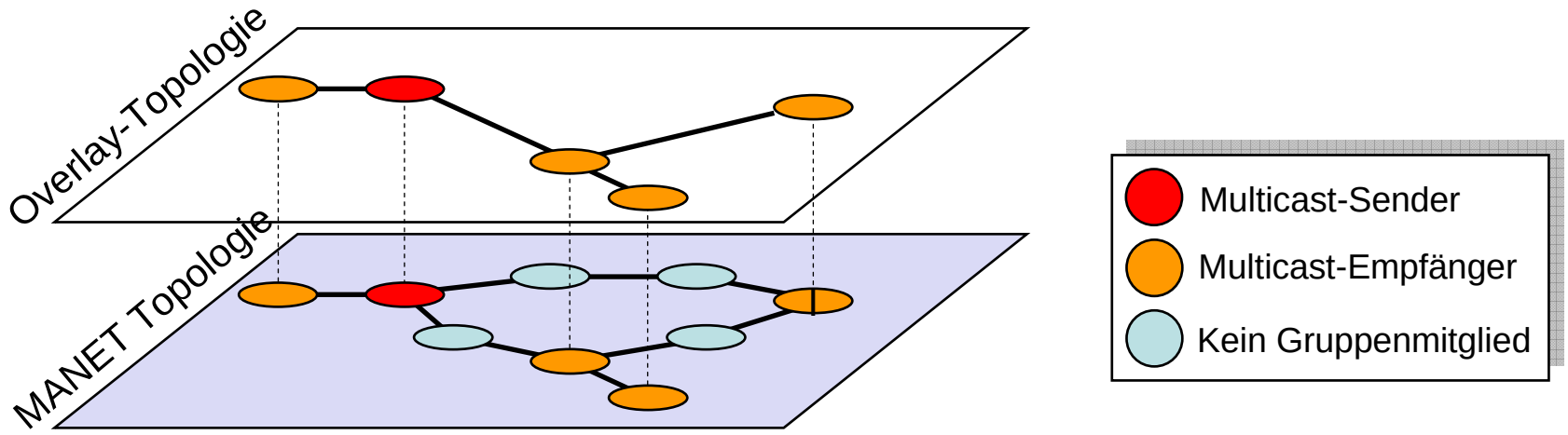
- → Lauffähige Implementierung für Handheld-PCs mit Linux-Betriebssystem
- → Modifikation der Routingprotokoll-Implementierungen nicht notwendig

MANETs am ITM: Multicast-Routing

- Hoher Bedarf an Gruppenkommunikation in MANETs
  - Knoten des MANETs arbeiten häufig an einer gemeinsame Aufgabe
    - z.B. Rettungsaktion, Sensornetzwerke, Verteilte Spiele
  - Koordination mit Hilfe von Gruppenkommunikation
- Multicast = 1:n Kommunikation
  - Ein Sender sendet ein Datenpaket an eine Gruppe von Empfängern
- Multicast-Routing /IP Multicast
  - Empfängergruppe wird über spezielle IP Multicast-Adressen adressiert
  - Anwendung des Senders sendet Datenpakete genau einmal an diese Adresse
  - Aufbau einer *Verteilstruktur* auf Vermittlungsschicht
    - Spezifiziert welche Knoten Datenpakete weiterleiten oder duplizieren müssen

ODOMP - On-Demand Overlay Multicast Protocol

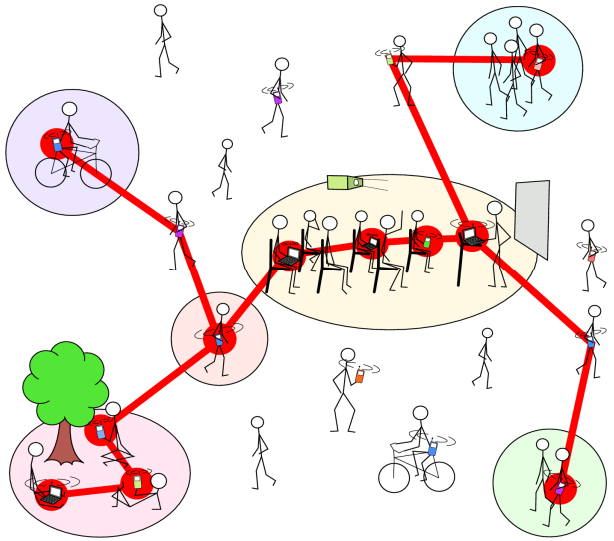
- Aufbau eines Overlays zwischen den Gruppenmitgliedern

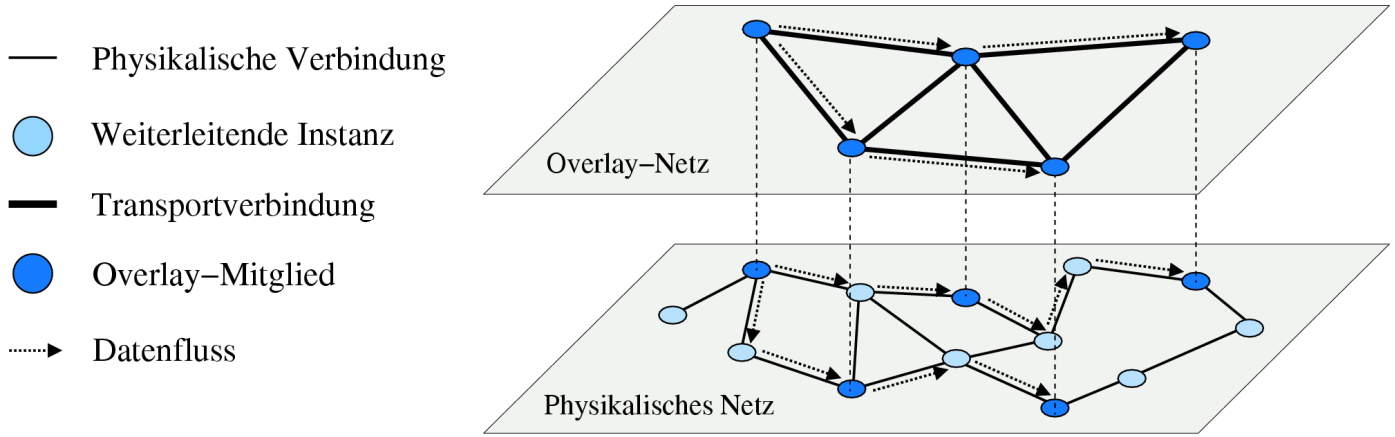


- Overlay wird zur Weiterleitung von Datenpaketen verwendet
  - Overlay hat die Form eines Baums (Sender = Wurzel)
  - Bestehlt aus IP Tunneln zwischen Gruppenmitgliedern
    - Unicast Routen werden durch bel. Unicast-Routingprotokoll bestimmt z.B. AODV/OLSR
- ODOMP Charakteristika
  - Reaktive – On-demand
  - Soft-state basiert

MANETs am ITM: Overlay-Multicast

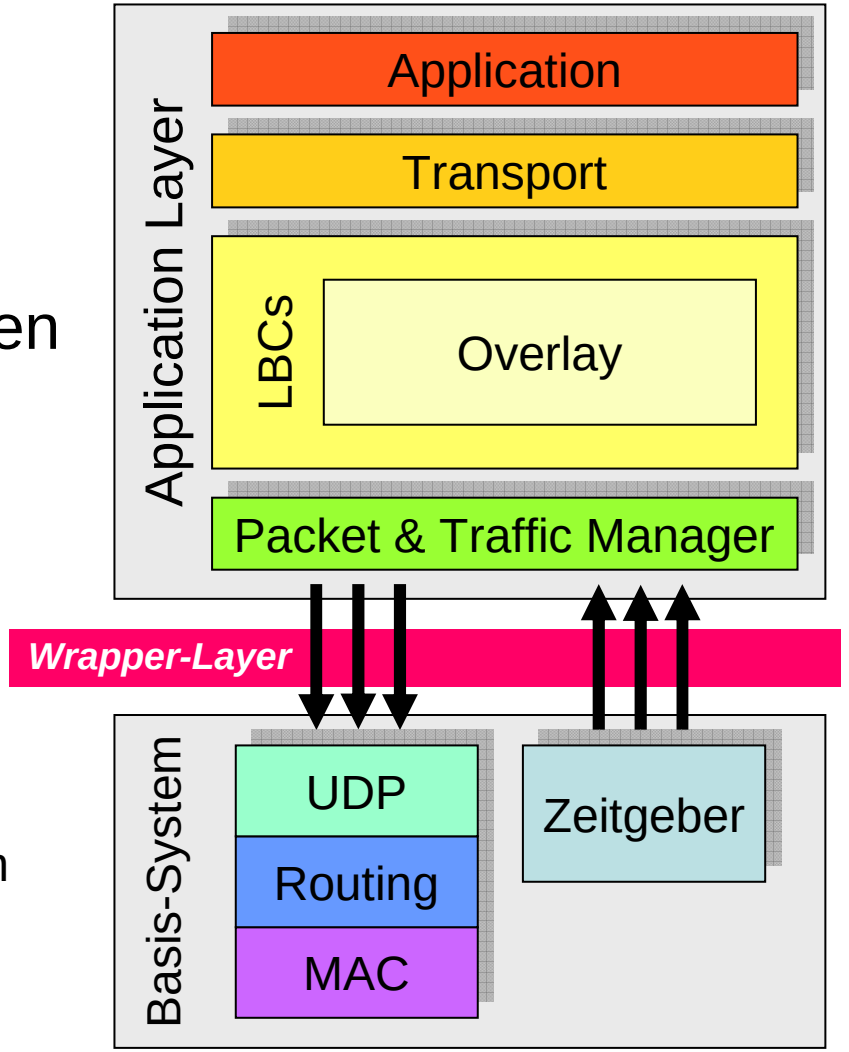
- Entwicklung eines P2P-Multicast-Dienstes
  - Kommunikation über Overlay-Netz
  - Dezentral, robust, einfach aufsetzbar, …
- Entwicklung von Anwendungen
  - VoIP, Echtzeit-Multiplayer-Spiele, Chat-Clients, Präsentations-Software, …
  - Unterscheiden sich in ihren Zuverlässigkeits-anforderungen





MAMAS – Modulares Baukastensystem für Multicast-Anwendungen

- Anwendung in Module aufspalten
  - Module haben spezielle Aufgabe
    - Transport, Overlay-Routing, …
  - Integriert in C++ Klassen
- Definition fester Modulschnittstellen
  - Module sind beliebig austauschbar
  - Module sind wieder verwendbar
  - Multicast-Dienst wird flexibel konfigurierbar
- Basis-System (≠ Betriebssystem)
  - Windows, Linux, …
  - Netzwerksimulationssoftware
    - Testen von Protokollen vor realem Betrieb!



III Übungen

- Warum kann das von Ethernet bekannte Medienzugriffsverfahren nicht im drahtlosen Bereich verwendet werden?
- Erklären Sie das bei 802.11 eingesetzte Medienzugriffsverfahren!
- Welche Vorteile bringt RTS/CTS?
- Wie können Kollissionen erkannt werden?
- Nennen Sie einige Vor- und Nachteile drahtloser LANs!
- Welche Ziele sind beim Entwurf drahtloser lokaler Netze zu beachten?
- Wie unterscheiden sich Infrastruktur- und Ad-hoc-Netzwerke? Nennen Sie Beispiele!
- Erläutern Sie die Funktionsweise der PCF.
- Welche Frequenzen werden für lokale Netze derzeit vorrangig eingesetzt? Vor-/Nachteile?
- Welche Schichten umfasst IEEE 802.11? Funktionen der standardisierten Schichten?

Übungen II

- Erläutern Sie den Ablauf des Power Managements in einem BSS!
- Was passiert, wenn eine Station in einem BSS den AP wechselt?
- Nennen Sie Schwachpunkte von WEP.
- Wie findet eine WLAN-Station ein WLAN?
- Nennen Sie Erweiterungen des Basisstandards und erläutern Sie deren Ziel und Realisierung.
- Was sind mobile Ad-hoc-Netze und was sind deren Eigenschaften?
- Warum können aus dem Festnetz bekannte Protokolle nicht in mobilen Ad-hoc-Netzen angewandt werden?
- Benennen und beschreiben Sie die besprochenen Kategorien von Routingprotokollen und nennen Sie je ein Beispielprotokoll!
- Was sind Vor- und Nachteile des Flutens für den Datentransfer?
- Wie funktioniert AODV?
- Was ist die Besonderheit bei OLSR?

III Referenzen und weiterführende Literatur

[III.1] J. Rech, Wireless LAN – 802.11-WLAN-Technologien und praktische Umsetzung im Detail, Verlag Heinz Heise, 2004

[III.2] B. O'Hara, A. Petrick, The IEEE 802.11 Handbook – A Designers Companion IEEE, 1999

[III.3] J. Schiller, Mobilkommunikation; Addison-Wesley, 2003 (Kapitel 7)

[III.4] A. Chandra, V. Gummalla, J. Limb, Wireless Medium Access Control Protocols, IEEE Communications Surveys & Tutorials, www.comsoc.org/livepubs/surveys/public/2q00issue/gummalla.html, 6/2000

[III.5] I. Stojmenovic, ed., Handbook of Wireless Networks and Mobile Computing – Kapitel 6: Wireless Media Access Control, John Wiley & Sons, February 2002

[III.6] http://www.rz.uni-karlsruhe.de/rd/dukath.php

[III.7] C.-K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, 2002

[III.8] C. Perkins, Ad-hoc Networking, Addison Wesley, 2000

[III.9] IETF MANET Working Group

http://www.ietf.org/html.charters/manet-charter.html

[III.10] The MANET Bibliography

http://www.antd.nist.gov/wctg/manet/manet_bibliog.html

Anhang: Optimized Link State Routing (OLSR)

- Ziel: Link Status Information *effizient* fluten!

1. Bestimmung der Nachbarschaft
   - Periodisches broadcasten von HELLO-Nachrichten. Diese enthalten:
     - Adresse der Knoten, von denen derzeit HELLO-Nachrichten empfangen werden
     - Status der Links zu diesen Knoten: symmetrisch (bi-) oder asymmetrisch (unidirektional)
   - Daraus errechenbare Nachbarschaftsbeziehungen
     - Y ist „1-hop Nachbar“ von X $\Leftrightarrow$ X empfängt HELLO-Nachricht von Y
     - Y ist „2-hop Nachbar“ von X $\Leftrightarrow$ Y $\neq$ X und X sieht Y in von Z empfangener HELLO-Nachricht
     - Y ist „strikter 2-hop Nachbar“ von X $\Leftrightarrow$ Y ist 2-hop aber nicht 1-hop Nachbar von X
     - Beziehungen sind jeweils symmetrisch und asymmetrisch definiert
     - Bsp.: X sieht sich in HELLO-Nachricht von Y $\Rightarrow$ Y ist symmetrischer 1-hop Nachbar von X
   - Nachbarschaftsinformation nach Timeout löschen zur Reaktion auf Link-Brüche

Multipoint Relays (MPR)

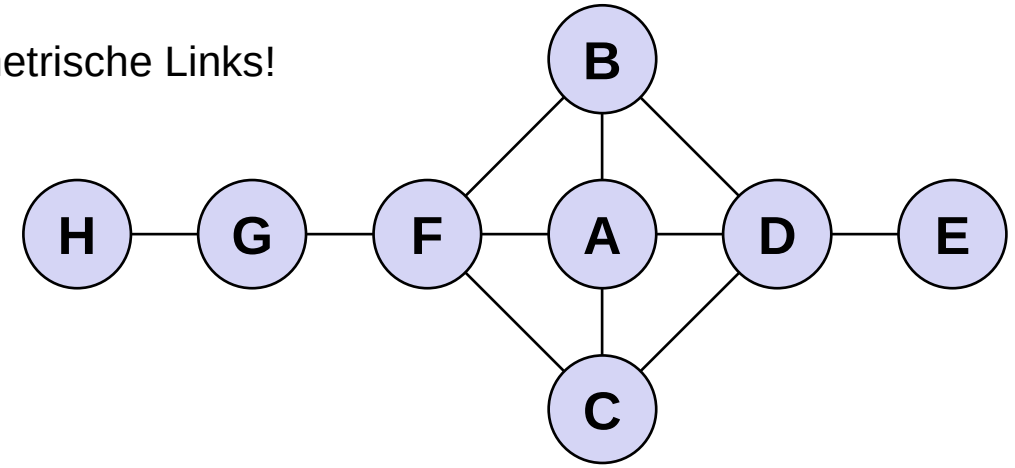
2. Bestimmung der „Multipoint Relays“ (MPR)
   - Die MPRs von X sind eine Teilmenge der symmetrischen 1-hop Nachbarn von X
   - Die Teilmenge wird so gewählt, dass jeder symmetrische 2-hop Nachbar von X über mindestens einen MPR erreichbar ist
   - Berechnung der Teilmenge anhand einer Heuristik bei jeder erkannten Änderung innerhalb der 2-hop Nachbarschaft
   - Gewählte MPRs werden in HELLO-Nachrichten bekannt gegeben

3. Bestimmung der „MPR Selectors“ (MS)
   - Die MS von X sind jene Knoten, welche X als MPR gewählt haben
   - X erfährt von diesen Knoten aufgrund empfangener HELLO-Nachrichten

Beispiel OLSR I

Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)

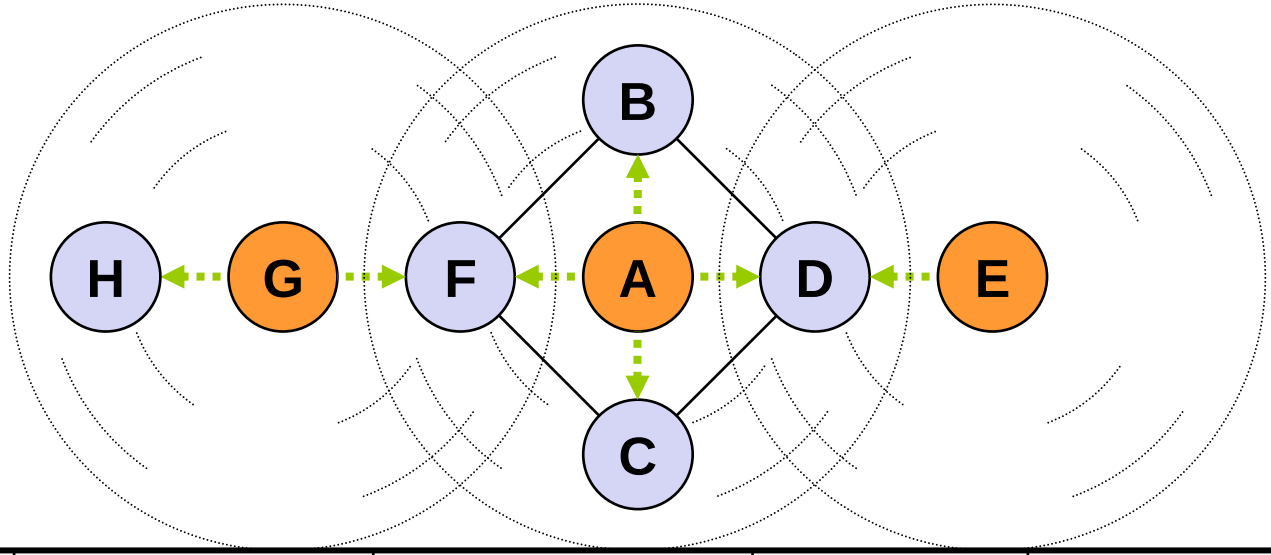
Hier nur symmetrische Links!



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A				
B				
C				
D				
E				
F				
G				
H				

Beispiel OLSR II

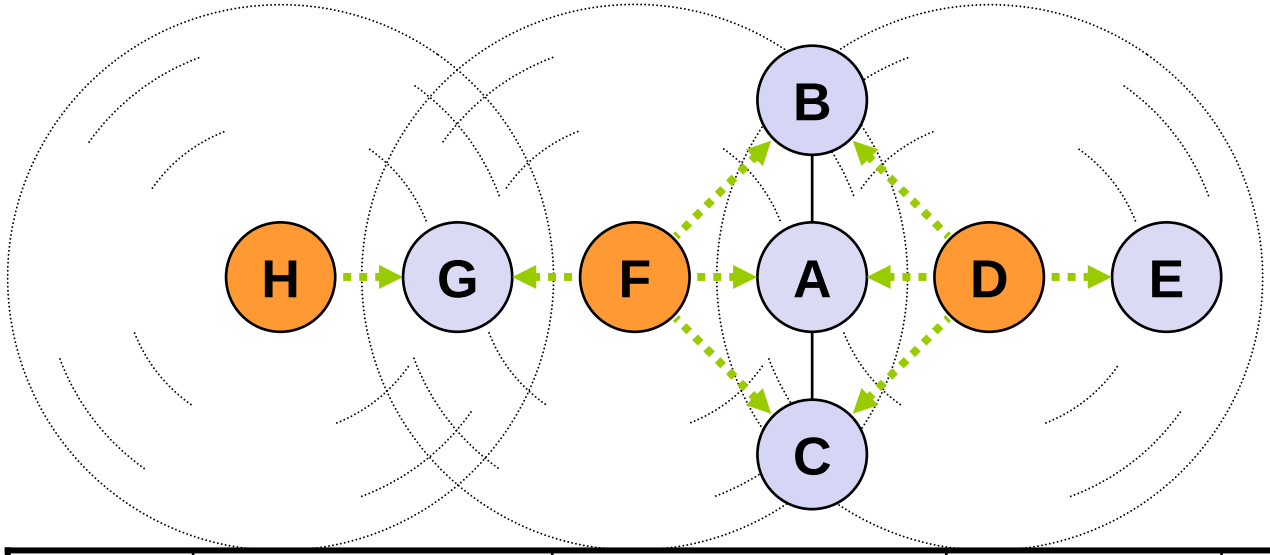
Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A				
B	A			
C	A			
D	A, E			
E				
F	A, G			
G				
H	G			

Beispiel OLSR III

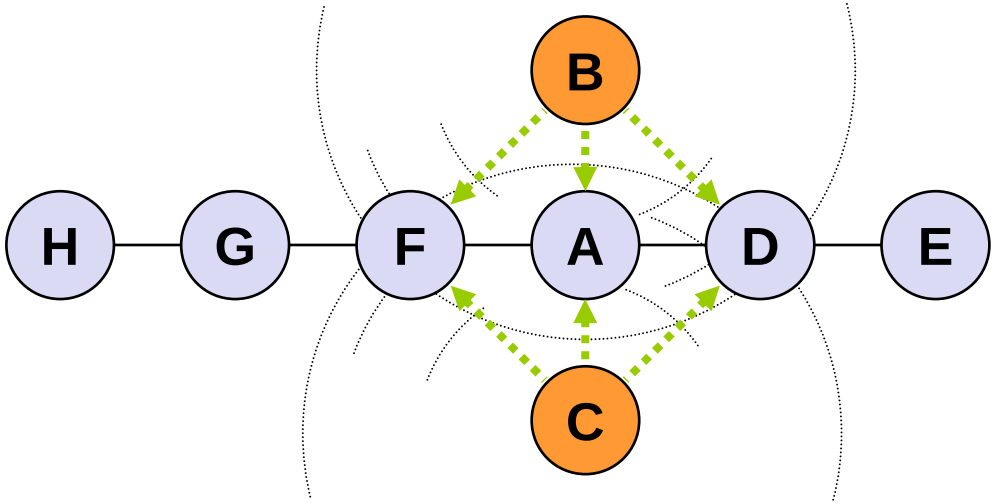
Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A	F, D	E, G	D, F	
B	A, D, F	E, G	D, F	
C	A, D, F	E, G	D, F	
D	A, E			
E	D	A	D	
F	A, G			
G	F, H	A	F	
H	G			

Beispiel OLSR IV

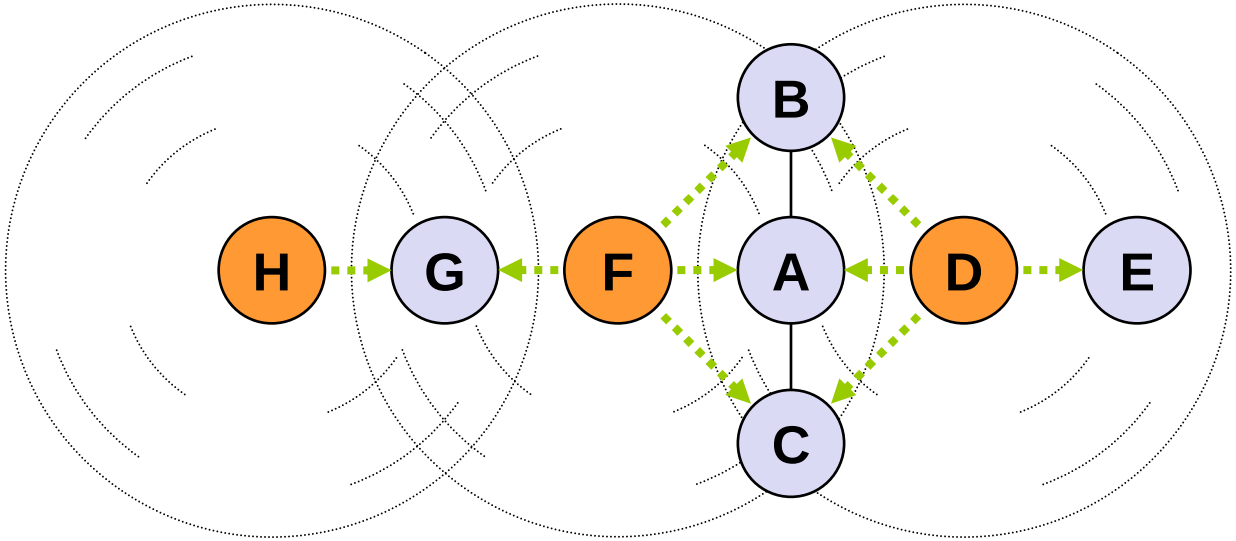
Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A	B, C, D, F	E, G	D, F	
B	A, D, F	E, G	D, F	
C	A, D, F	E, G	D, F	
D	A, B, C, E	F	B	B, C
E	D	A	D	
F	A, B, C, G	D	B	B, C
G	F, H	A	F	
H	G			

Beispiel OLSR V

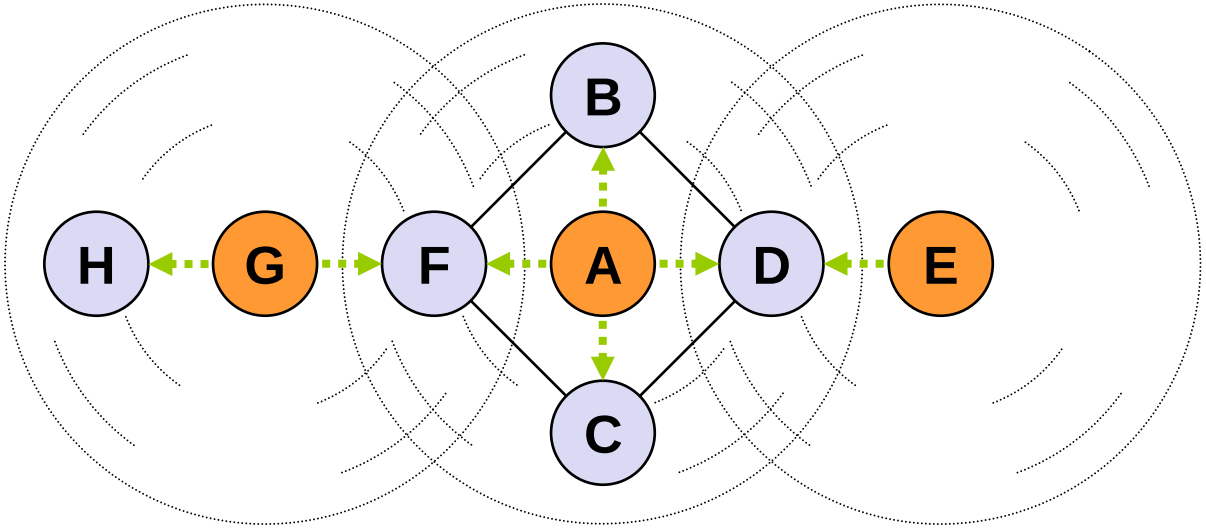
Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A	B, C, D, F	E, G	D, F	
B	A, D, F	C, E, G	D, F	D, F
C	A, D, F	B, E, G	D, F	
D	A, B, C, E	F	B	B, C
E	D	A, B, C	D	
F	A, B, C, G	D	B	B, C
G	F, H	A, B, C	F	
H	G			

Beispiel OLSR VI

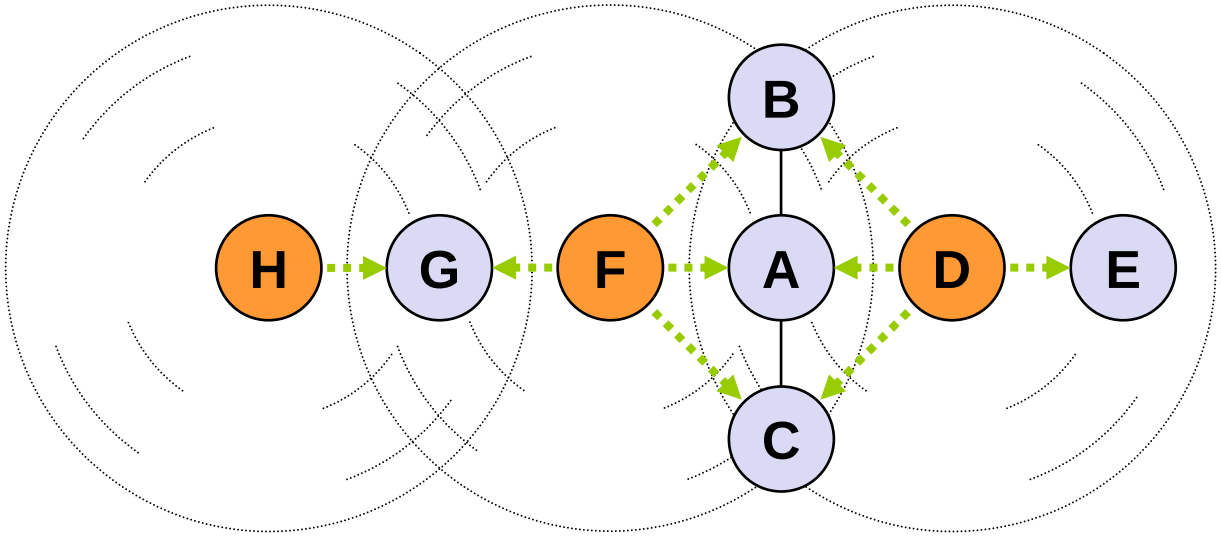
Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A	B, C, D, F	E, G	D, F	
B	A, D, F	C, E, G	D, F	D, F
C	A, D, F	B, E, G	D, F	
D	A, B, C, E	F	B	A, B, C, E
E	D	A, B, C	D	
F	A, B, C, G	D, H	B, G	A, B, C, G
G	F, H	A, B, C	F	
H	G	F	G	

Beispiel OLSR VII

Bestimmung der Nachbarn, MPR und MS (HELLO-Nachrichten)



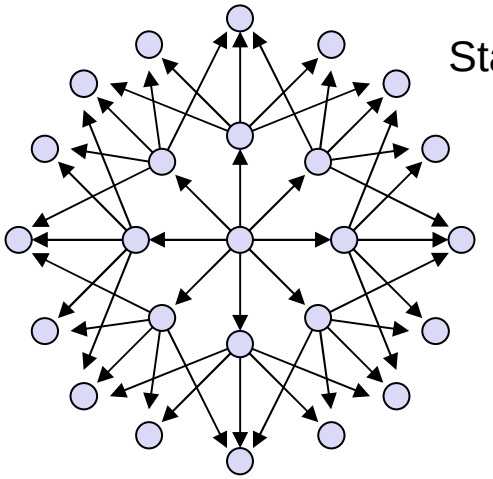
Knoten	1-hop Nachbarn	2-hop Nachbarn	MPR	MS
A	B, C, D, F	E, G	D, F	
B	A, D, F	C, E, G	D, F	D, F
C	A, D, F	B, E, G	D, F	
D	A, B, C, E	F	B	A, B, C, E
E	D	A, B, C	D	
F	A, B, C, G	D, H	B, G	A, B, C, G
G	F, H	A, B, C	F	F, H
H	G	F	G	

STABIL!

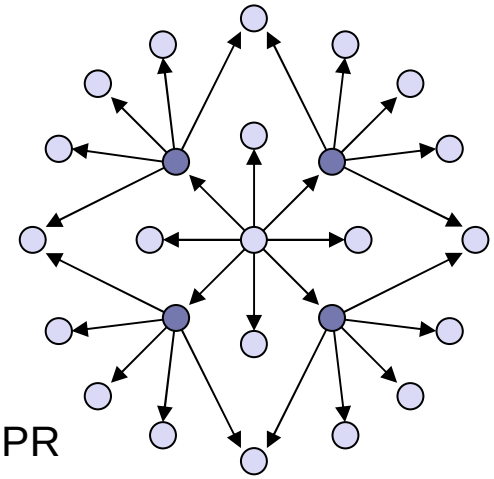
STABIL!

Optimized Link State Routing (OLSR)

- Hiermit möglich: Effizientes Fluten von Nachrichten
  - Quellknoten broadcastet Nachricht
  - Optimierung gegenüber dem Standard Fluten-Algorithmus:
    - Nicht *alle* Knoten leiten Nachricht weiter, sondern *nur* die MPR
      - Y leitet eine von X empfangene Nachricht wird weiter, falls X ein MS von Y ist
    - Weiterleitung ebenfalls als Broadcast
  - Vermeidung der Weiterleitung von Duplikaten durch Sequenznummern
  - Zahl der gewählten MPR wirkt sich direkt auf die Netzbelastung aus
    - Menge der MPR sollte möglichst optimal (minimal) sein, um Verkehr zu reduzieren



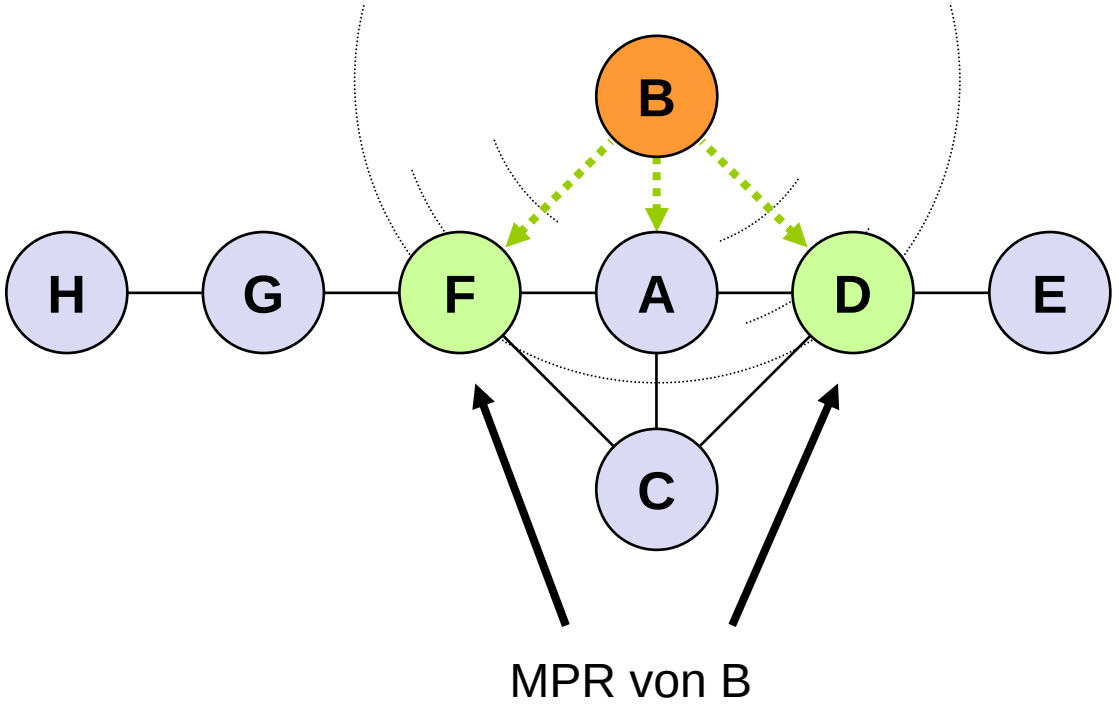
Standard Fluten



Effizientes Fluten mit MPR

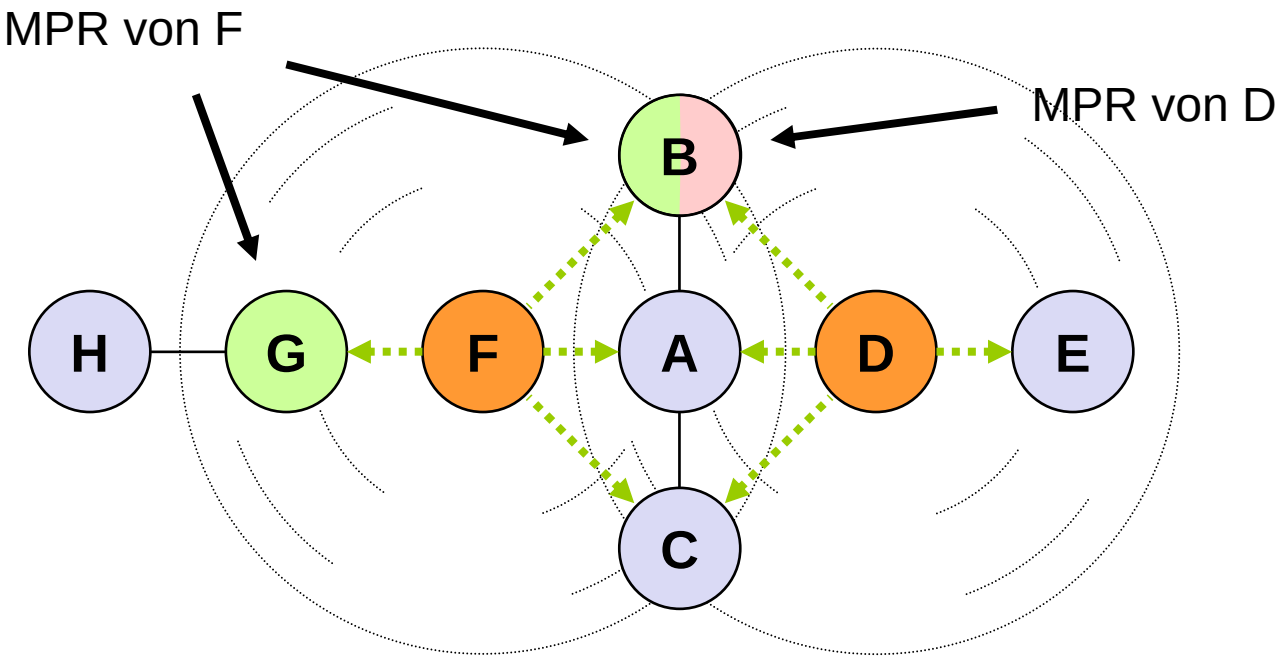
Beispiel OLSR VIII

Effizientes Fluten von Nachrichten, Beispiel: Quellknoten B



Beispiel OLSR IX

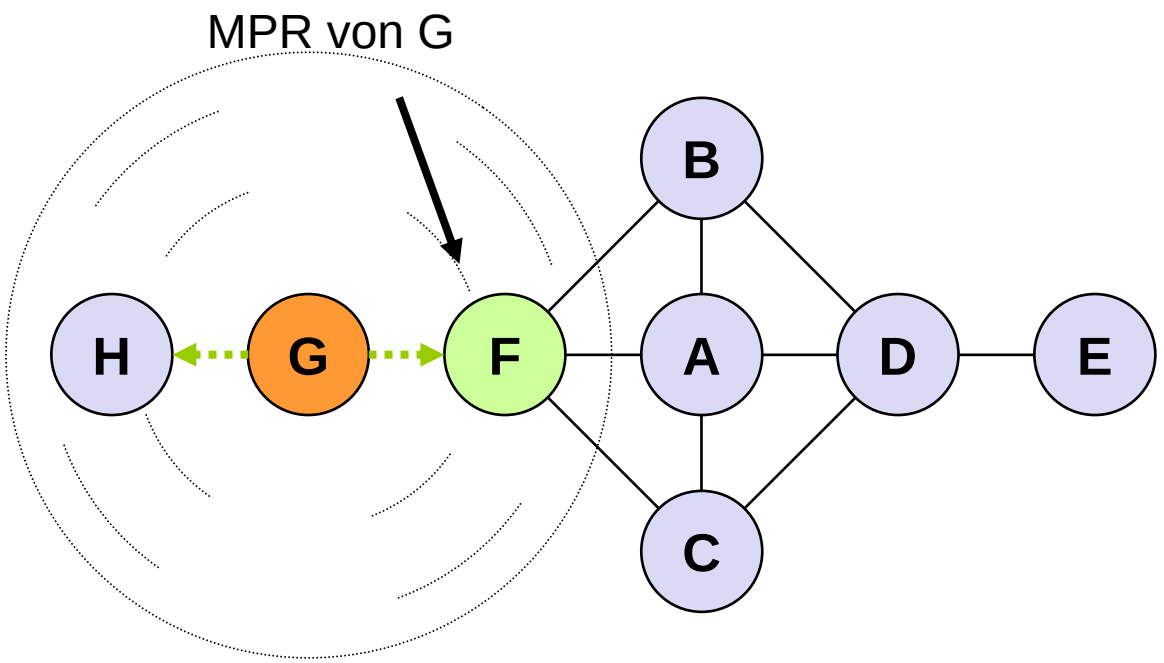
Effizientes Fluten von Nachrichten, Beispiel: Quellknoten B



- Knoten F und D sind MPR von B und leiten das empfangene Paket weiter

Beispiel OLSR X

Effizientes Fluten von Nachrichten, Beispiel: Quellknoten B



- Knoten B leitet das von F bzw. D empfangene Paket nicht erneut weiter (Sequenznummern)
- Knoten G ist MPR von F und leitet das von F empfangene Paket weiter
- Knoten F leitet das von G empfangene Paket nicht erneut weiter (Sequenznummern)

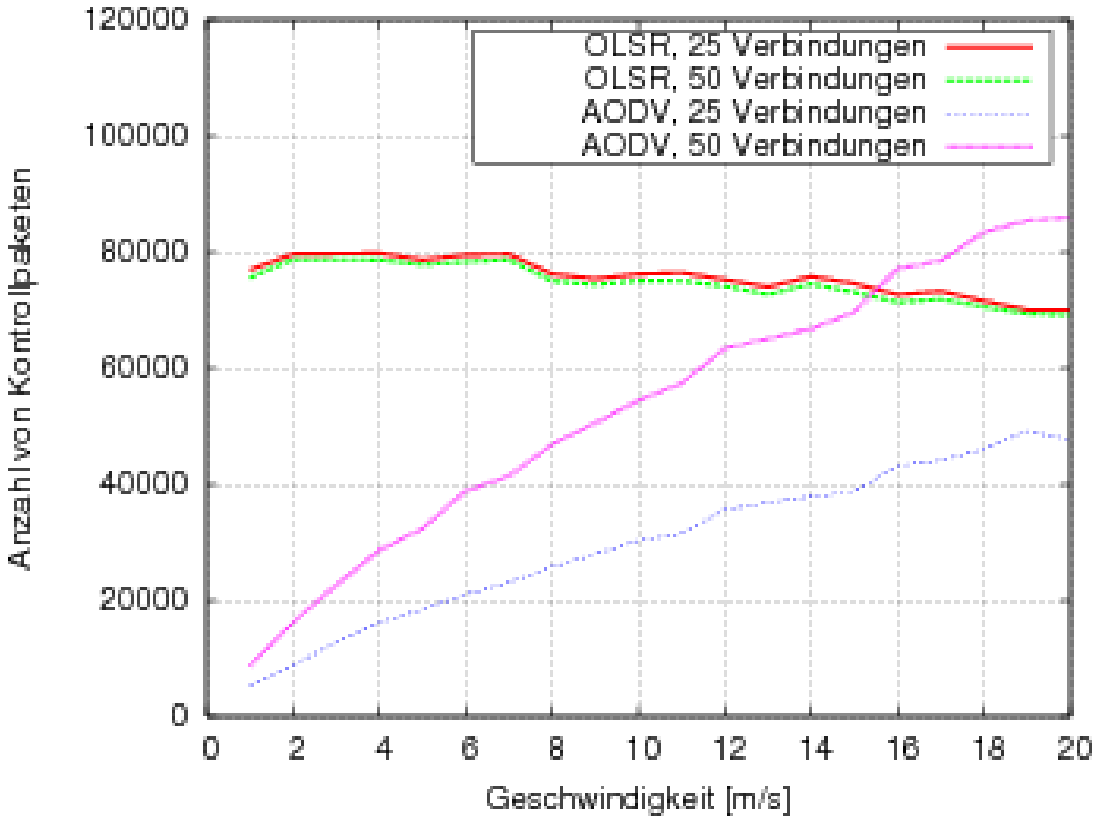
Optimized Link State Routing (OLSR)

- Effizientes Fluten von Link Status Informationen
  - Jeder Knoten X mit MS ≠ Ø versendet periodisch TC-Nachricht.
    - Enthält eigene Adresse
    - Komplette Liste der eigenen MS
  - Es werden also *nicht* die 1-hop Nachbarn propagiert! Grund:
    - Es sollen nur symmetrische Links propagiert werden
      - MS bilden *Teilmenge* der Knoten, zu denen symmetrische Links bestehen
    - Reduktion der Netzbelastung
      - Nicht alle Knoten senden TC-Nachrichten
  - Jeder Knoten im Netz sammelt MS aus TC-Nachrichten
    - Netztopologie ist in ausreichendem Maß rekonstruierbar
    - Kürzeste Routen können nach Dijkstra ermittelt werden
  - Optimierung: Piggyback von HELLO- und TC-Nachrichten
    - Weniger Medienzugriffe
- Besonders effektiv bei Netzen mit hoher Knotendichte
  - Nur wenige Knoten fungieren als MPR

→OLSR ist „Standard-Protokoll“ (experimentell) in der IETF (RFC 3626)

Vergleich AODV – OLSR

Anzahl Knoten	50
Simulationsfläche	1000m x 1000m
Simulationsdauer	600 Sekunden
Reichweite	250 m
Funktechnologie	IEEE 802.11
Mobilitätsmodell	Random Waypoint



→ Beobachtungen

- Kontrolloverhead von AODV steigt mit zunehmender Geschwindigkeit
- Kontrolloverhead von AODV steigt mit der Anzahl der Verbindungen
- Kontrolloverhead von OLSR ist unabhängig von der Anzahl der Verbindungen
- Kontrolloverhead von OLSR ist nahezu unabhängig von der Geschwindigkeit