Framework zur Anomalie-basierten Angriffserkennung durch verteilte Instanzen

Endvortrag Diplomarbeit, 08.11.2007

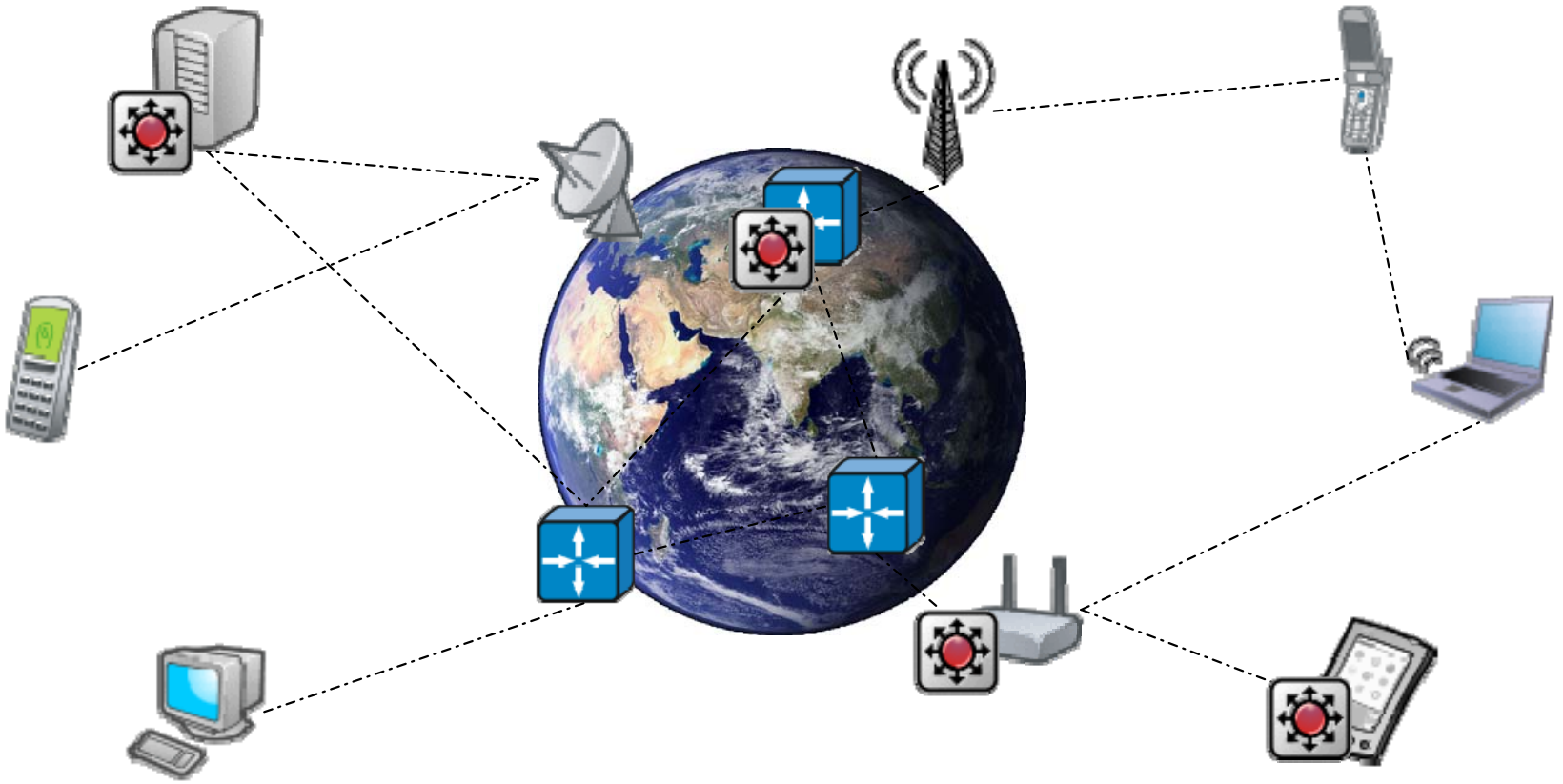
Christoph Mayer

Institut für Telematik

Motivation

DDoS- und Wurmangriffe sind die größten Gefahren, die zur Zeit das Internet bedrohen

(*Worldwide Infrastructure Security Report 2007, Arbor Networks)*

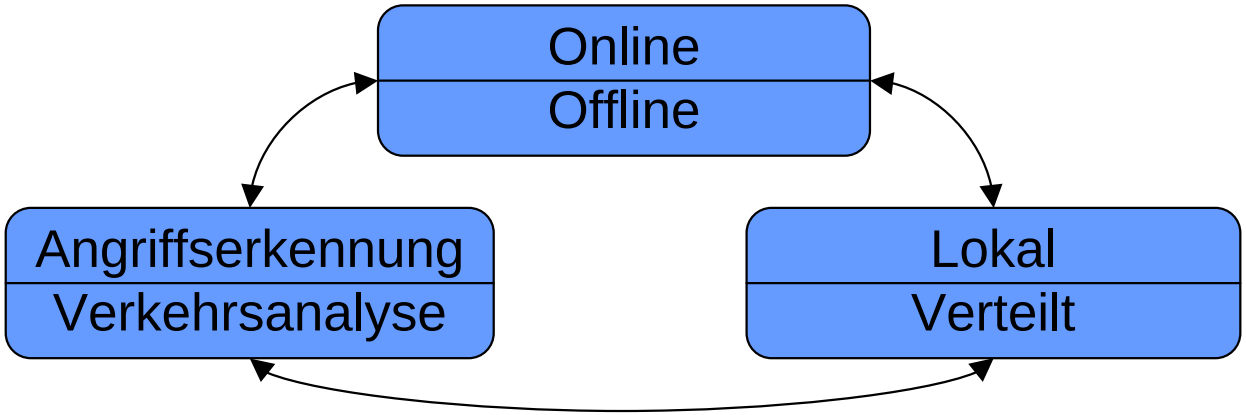


Anforderungen

- Skalierbarkeit
  - Betrieb im Netzinneren auf Vermittlungssystemen
  - Hohe Verkehrslast, geringe Ressourcen
- Erweiterbarkeit
  - Neue Protokolle
  - Neue Methoden zur Angriffserkennung
- Flexibilität
  - Verschiedene Laufzeitumgebungen
  - Baukastenprinzip
- Robustheit
  - Vermeidung von Überlast
  - Protokoll-Parser

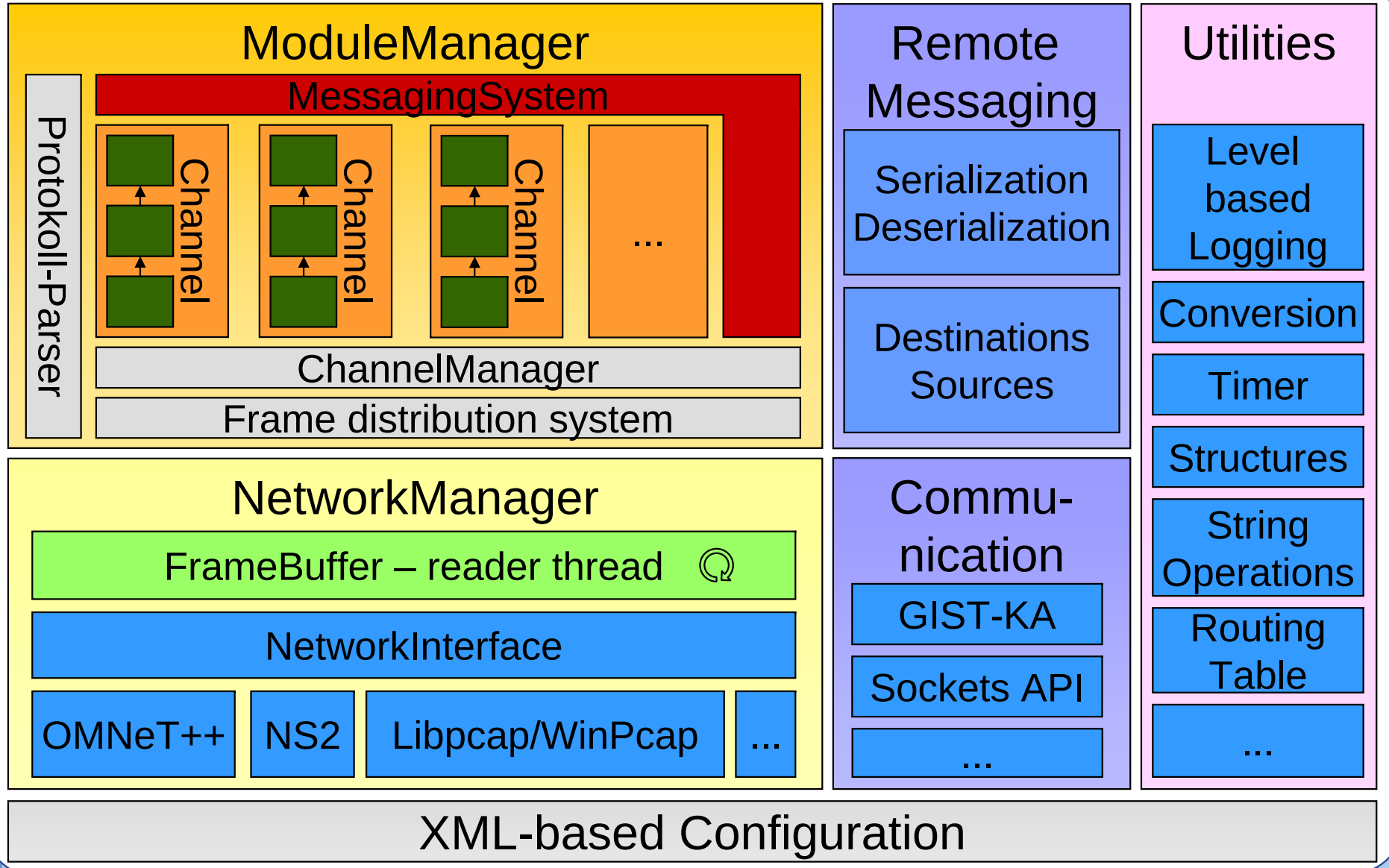
Ziel

- Flexibles Framework zur verteilten Angriffserkennung
  - Baustein-basiert (*Module*), flexibel konfigurierbar

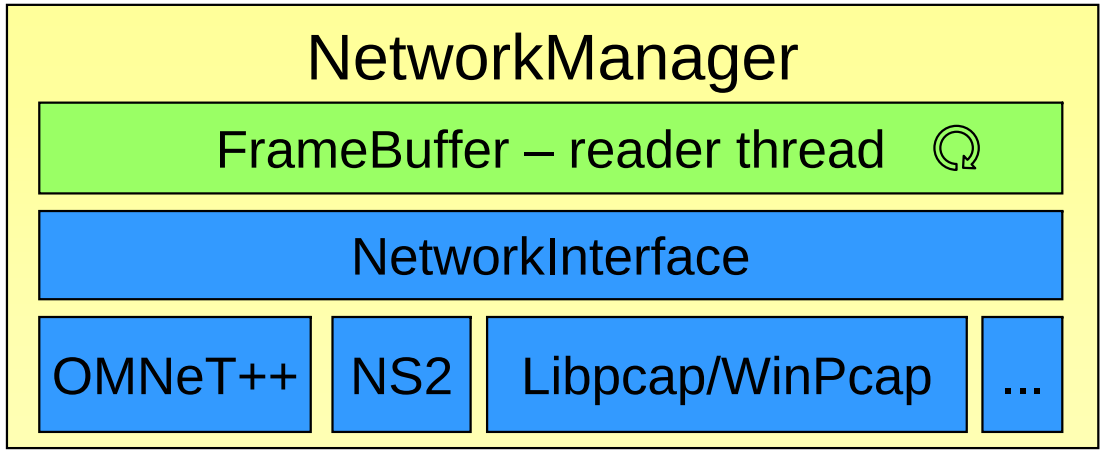


- Einfache Schnittstellen: Integration von Erweiterungen
  - Neue Protokolle, Methoden zur Angriffserkennung
  - Neue Komponenten (GUI, ...)
- Verschiedene Laufzeitumgebungen
  - Router, PC, Simulator, Sensorknoten, Netzwerkprozessor, ...
  - Laufzeitumgebung transparent für Module

Architektur

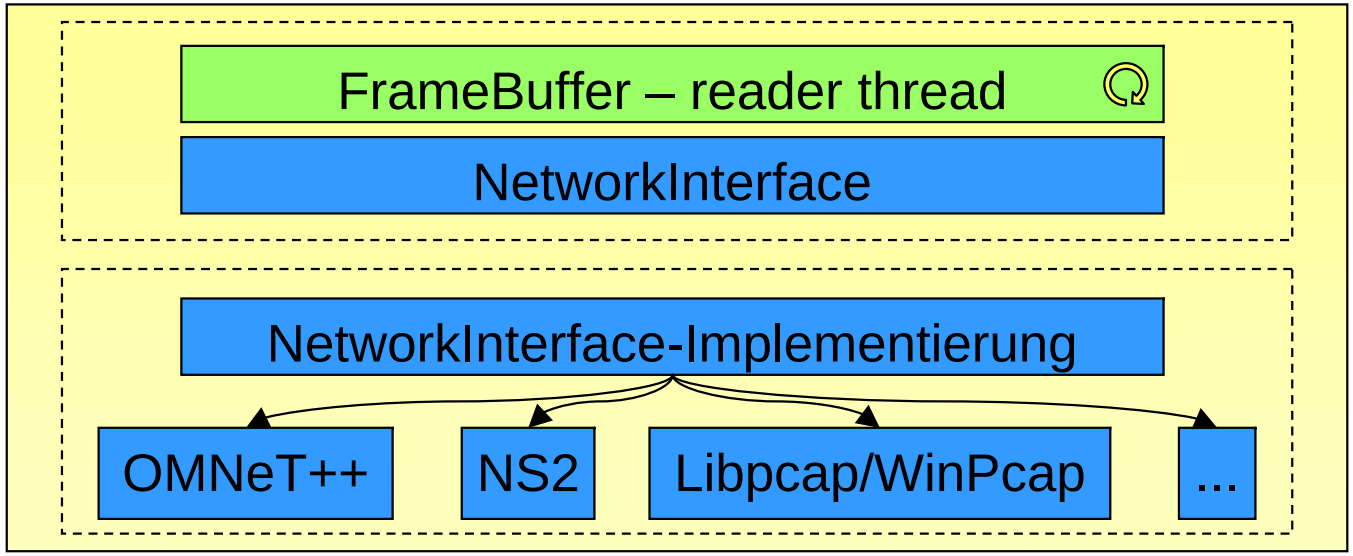


Architektur – Netzwerkabstraktion

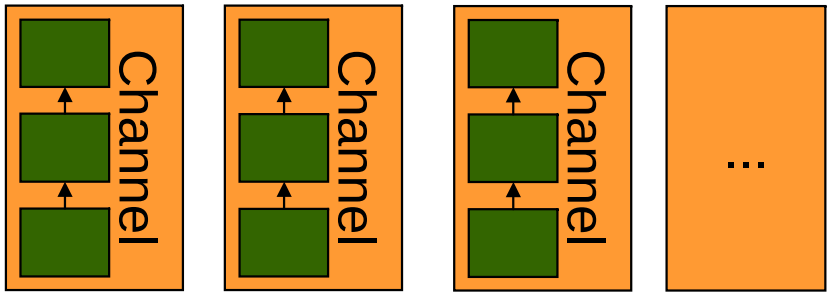


Netzwerkabstraktion

- Abstraktion des unterliegenden Netzes
  - Paketformate, notwendige Konvertierung
  - Abhängig von der Laufzeitumgebung
- Abfangen von Bursts
  - Zwischenspeicher für Frames
  - Begrenzungsmechanismen



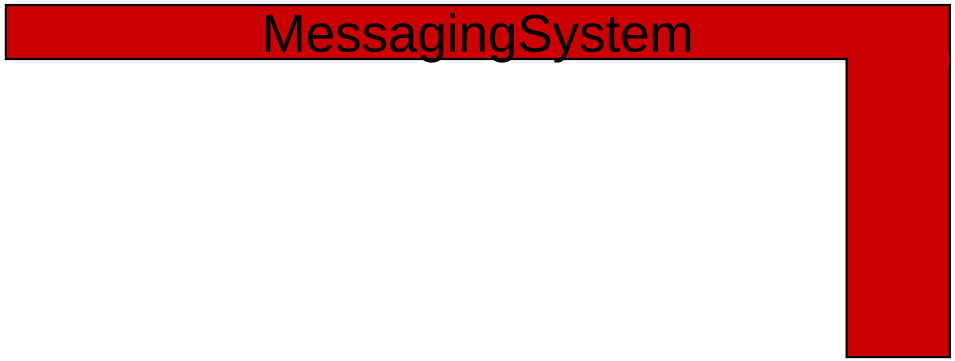
Architektur – Module



Module – funktionale Einheiten

- Modularisierung: Module als Bausteine
  - Klein und leichtgewichtig
  - In dynamische Bibliotheken ausgelagert
- Modul-Funktionalität
  - Sampling/Filtering/Überwachung von Frames
  - Sammeln von statistischen Daten, Analyse
- Channels
  - Funktionale Kette von Modulen
  - Verarbeitung von Netzwerkframes
  - Gruppierung von zusammengehörigen Modulen
  - Granularitätsstufen

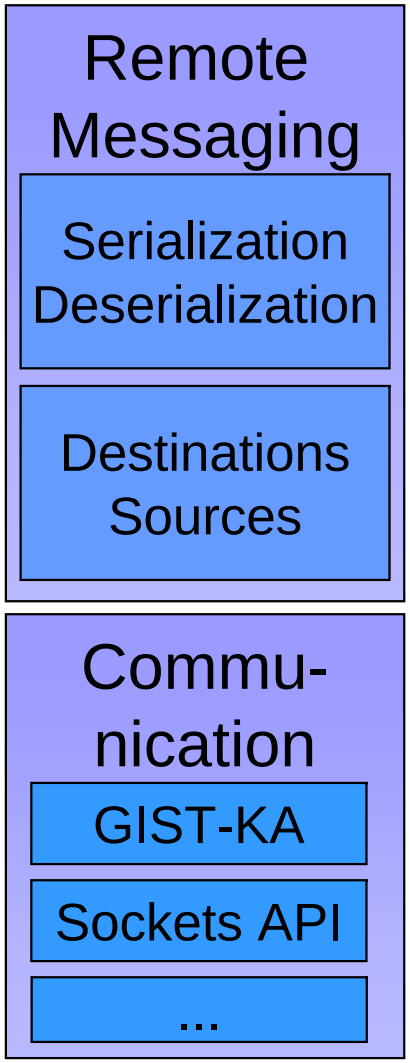
Architektur – Lokale Kommunikation



Lokale Kommunikation

- Datenzentrierte Kommunikation zwischen Modulen
  - Informationsquellen nicht bekannt
  - Daten werden in das System gesendet
  - Synchrone/asynchrone Nachrichtenzustellung
- Registrierungs-basiert
  - Modul registriert sich für interessante Nachrichten
- Beispiel: Statistische Verteilung
  - Analyse-Modul sammelt Daten zu einer statistischen Verteilung
  - Sendet diese Verteilung periodische aus
  - Interessierte Module registrieren sich und erhalten die Nachricht

Architektur – Verteilte Kommunikation



Verteilte Kommunikation

- Kommunikation zwischen entfernten Modulen
  - Transparenter Nachrichtenversand und Empfang
  - Beliebig komplexe Nachrichtenobjekte
- Serialisierung
  - Nachrichtenobjekte serialisieren und deserialisieren
  - Keine Paketformate notwendig
- Adressierung durch Versandoptionen
  - Lokal, entfernt, lokal + entfernt
  - Empfängerliste, Nachbarn
- Datenübertragung
  - Austauschbare Kommunikationsschicht
  - GIST, Sockets-API, ...

Architektur – Konfiguration

XML-based Configuration

XML-basierte Konfiguration

- Allgemein
  - Netzwerk, Tracedatei, Speedup, ...
- Baustein-Konfiguration
  - Instanziierung und Konfiguration von Modul-Bibliotheken
  - Mehrfache Instanziierung einer Bibliothek
- Baukastenprinzip
  - Verschaltung von Modulen zu Channels
  - Channel definiert zusammengehörige Funktionalität
  - Weitere Gruppierung von Channels
    - Granularirätsstufen

XML-basierte Konfiguration – Beispiel

Externe Bibliothek

Lokaler Name

```
<module name="Modules">
  <submodule lib  ="ModuleSamplingSystematicCountBased"
             name ="SamplingItemOne">
    <configitem name="SamplingCount">200</configitem>
    <configitem name="SelectionCount">1</configitem>
  </submodule>
  ...
</module>
```

Modul-Konfiguration

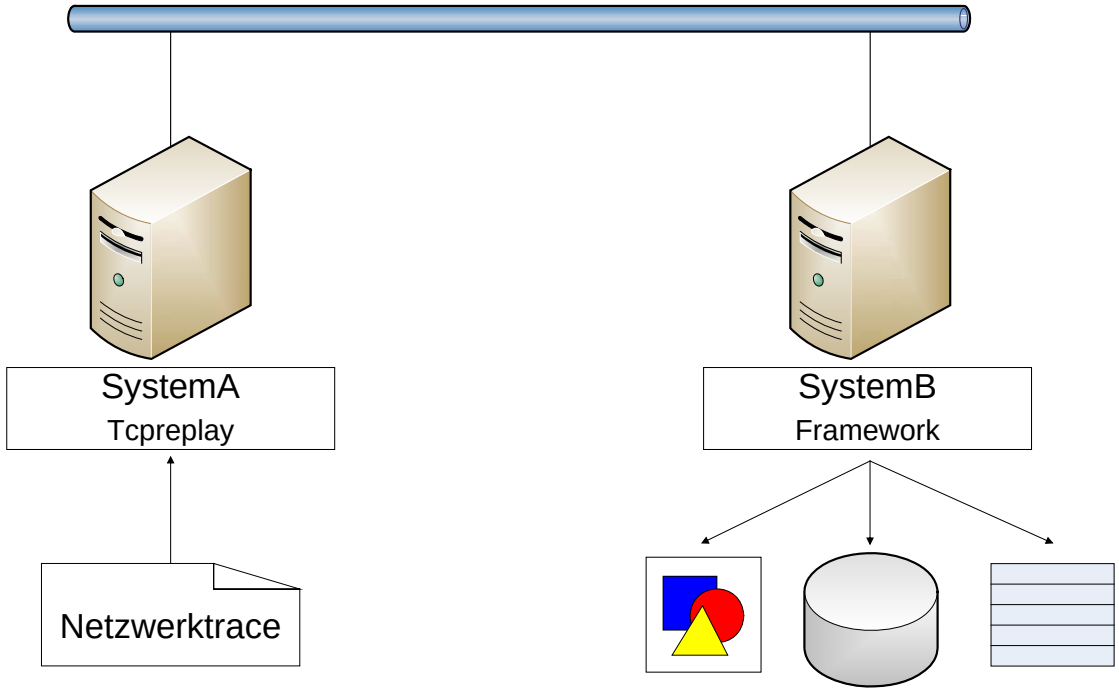
Channel Name

Channel Gruppe

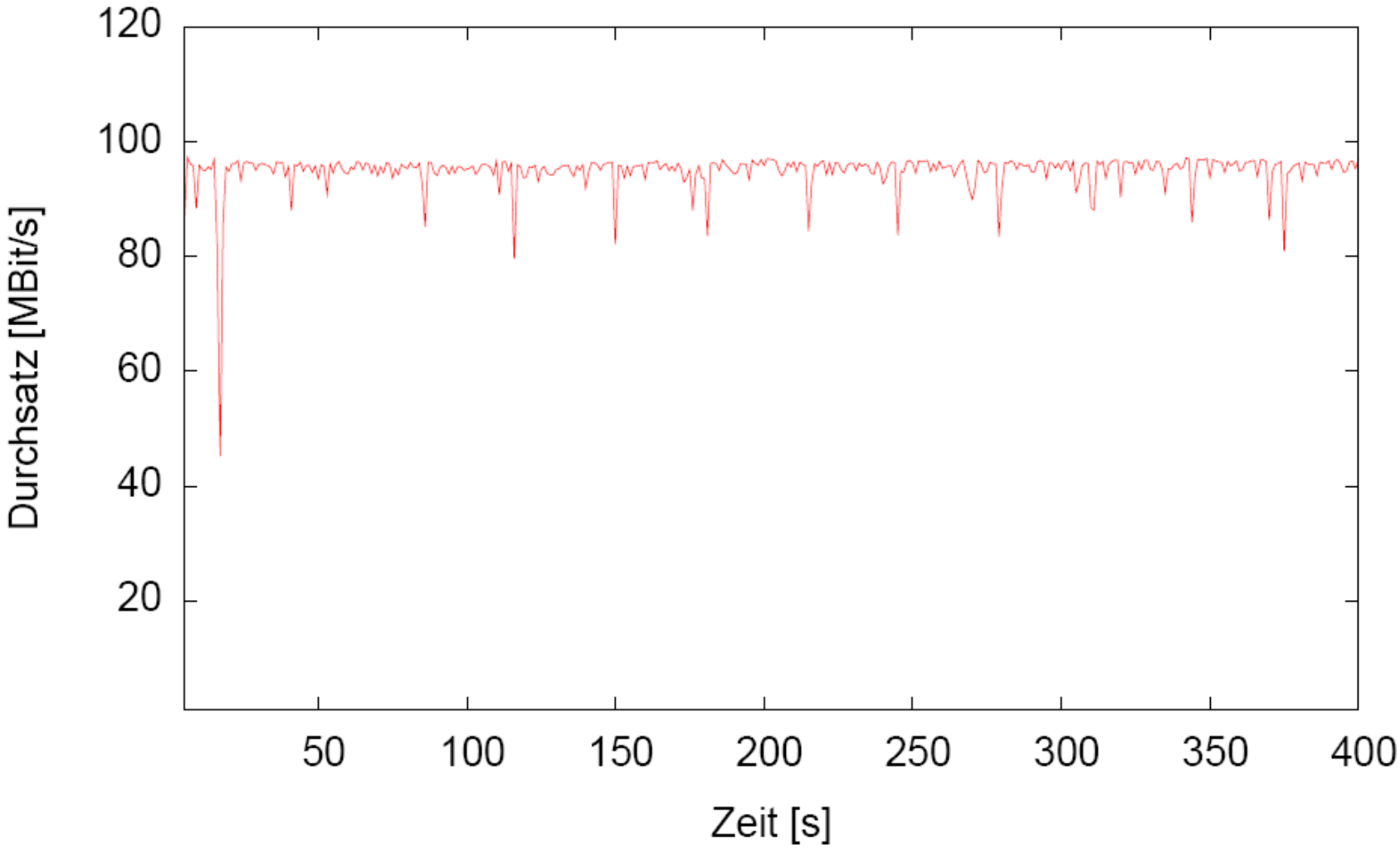
```
<module name="Channels">
  <submodule name="StageOne" stage="1">
    <configitem name="1">SamplingItemOne</configitem>
    <configitem name="2">...</configitem>
  </submodule>
  ...
</module>
```

Evaluation – Skalierbarkeit

- Systemaufbau
  - SystemA: Abspielen einer Netzwerktrace
  - SystemB: Betreibt Framework, Basisfunktionalität
  - Realistischer Verkehr, 100 MBit/s Ethernet

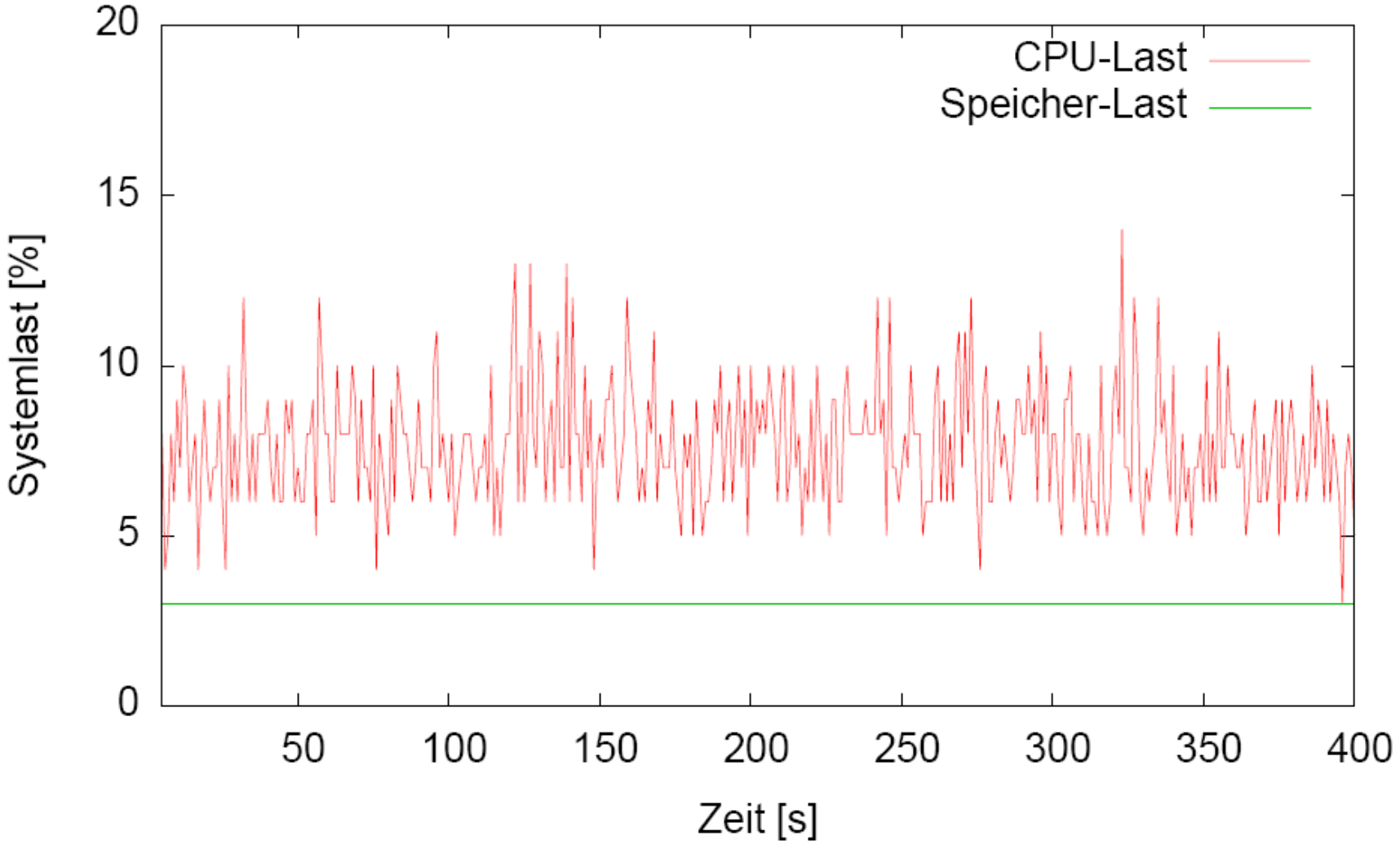


Evaluation – Skalierbarkeit



- Verarbeitung von 100 MBit/s kein Problem

Evaluation – Skalierbarkeit (2)



- CPU- und Speicherlast akzeptabel

Evaluation – Flexibilität

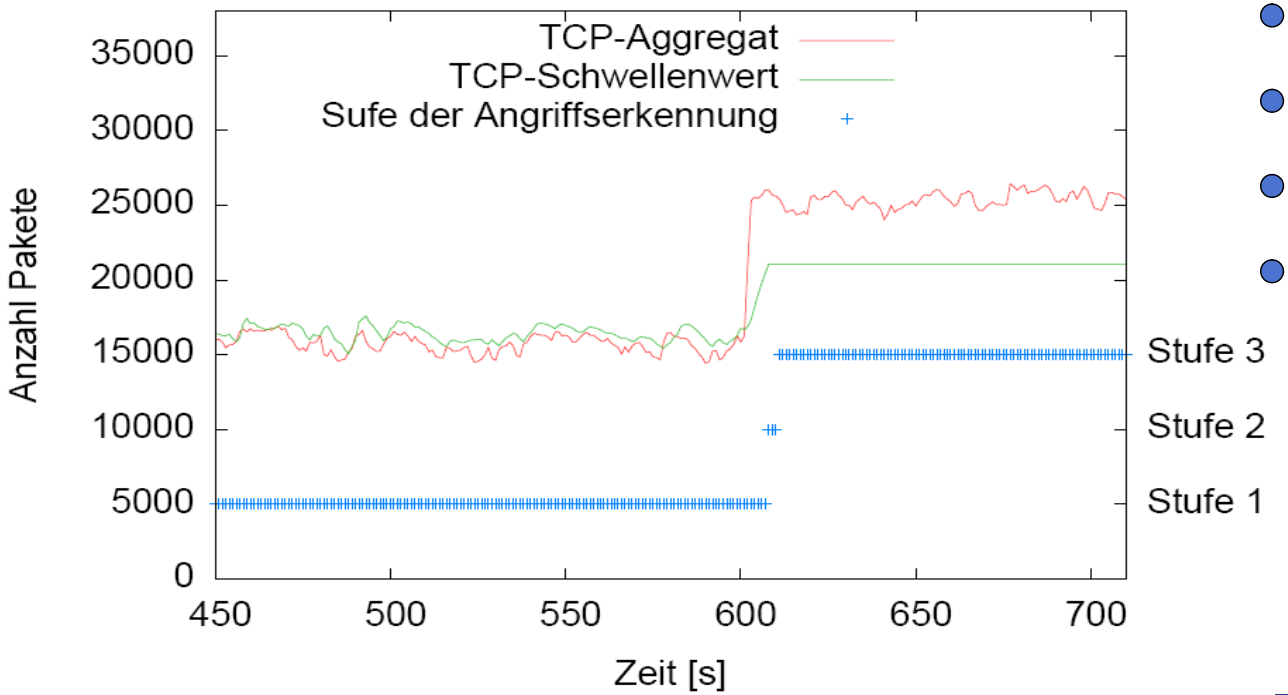
- OMNeT++ als Laufzeitumgebung
  - Kapselung der `main`-Funktion als `cSimpleModule`
  - Framework als Bibliothek von OMNeT++ geladen
  - Netwerkabstraktion für OMNeT++
- Stolpersteine
  - Threads: bekommen keine Prozessorzeit
  - Timer: Zeitdomäne der Simulationszeit
  - Pakete: andere Darstellung in OMNeT++
  - ...
- Resultat
  - Lokale und verteilte Angriffserkennung in großen Netzen
  - Simulation von DDoS- und Wurmangriffen

Evaluation – Erweiterbarkeit

- Integration einer Angriffserkennung
  - Extraktion der Aufgaben → Zerteilung in Module
  - Erstellung von Nachrichten für Kommunikation
  - Konfiguration gruppiert Module und definiert Granularitätsstufen
- Vorteile
  - Menge an Bausteinen → Wiederverwendbarkeit
  - Verschiedenen Laufzeitumgebungen
    - Z. B. Simulation in OMNeT++
  - Erweiterbarkeit
    - Verteilte Kommunikation leicht integrierbar
    - Module einfach austauschbar
    - Neue Funktionalität durch Module integrierbar

Simulation der Angriffserkennung

- Simulation verteilter Angriffe in OMNeT++
  - Realistische Topologie, selbstähnlicher Verkehr
  - Framework mit Angriffserkennung auf Core-Router
  - 150 DDoS-Zombies auf Endsystemen
  - Opfersystem auf Endsystem



- 3 Core-Router
- 9 Gateway-Router
- 113 Edge-Router
- 3257 Endsysteme

Zusammenfassung und Ausblick

- Framework zur verteilten Angriffserkennung
  - Einfache Integration von neuer Funktionalität
  - Lokale und verteilte Kommunikation
  - Flexibel konfigurierbar und einsetzbar
  - Verschiedene Laufzeitumgebungen
- Ausblick
  - Grafische Oberfläche
  - Weitere Laufzeitumgebungen, z. B. Sensorknoten
  - Methoden zur lokalen und verteilten Angriffserkennung
  - Simulation von verteilter Angriffserkennung in großen Netzen

Vielen Dank! Fragen?

Institut für Telematik