Tesis Doctoral

Event-driven Principles and Complex Event Processing for Self-adaptive Network Analysis and Surveillance Systems

Defense

Rüdiger Gad

Universidad de Cádiz

2015-07-29

Outline

Outline

Motivation

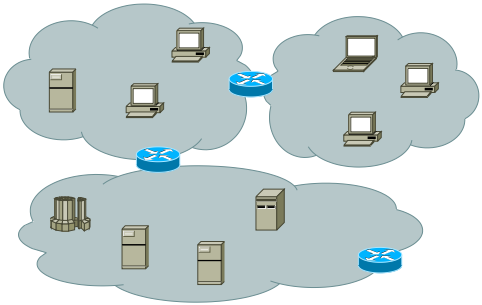
- IT is used ubiquitously.
  - Non-operational IT?
  - $\rightarrow$ **Severe Consequences!**
  - Importance of IT: **Critical**
- Computer Networks
  - Fundamental for IT Operation
  - Non-operational Networks? $\rightarrow$ Non-operational IT!
  - Importance of Networks: **Critical**

Assure Operational Computer Networks

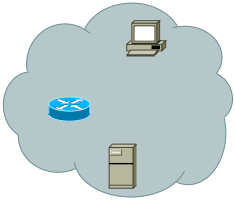
- Basis
  - Information
    - Detailed
    - Accurate
    - Up-to-date
    - ...
  - Network Analysis and Surveillance
    ("Network Reconnaissance" or "Network Monitoring")

Network Analysis and Surveillance (NAaS)

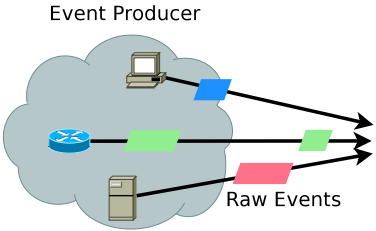
- Challenging
  - Distribution
  - Size
  - Change
  - Timeliness
  - Data Volume
  - ...



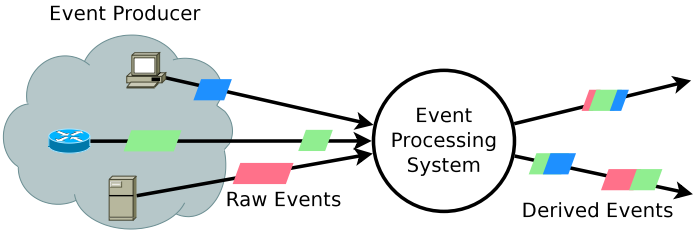
Event-driven Principles and Complex Event Processing (CEP) for NAaS



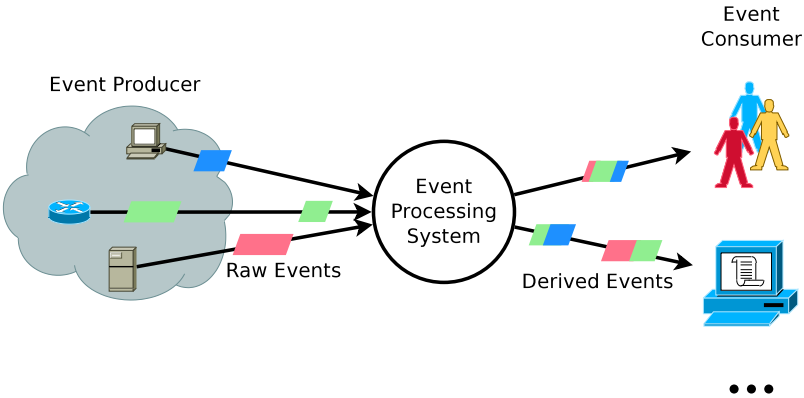
Event-driven Principles and Complex Event Processing (CEP) for NAaS



Event-driven Principles and Complex Event Processing (CEP) for NAaS



Event-driven Principles and Complex Event Processing (CEP) for NAaS



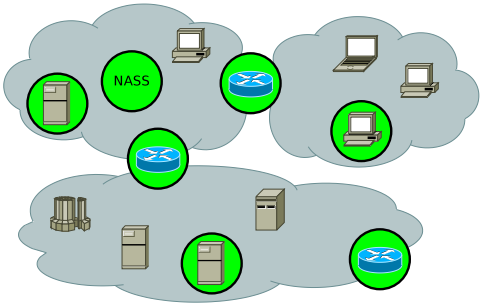
Event-driven Architecture (EDA) and CEP for NAaS

- Powerful Capabilities
- Existing Related Work
- Related Work, Limitations
  - Focused on Specific Use Cases
  - Conceptual/Architectural Focus
  - Real-world Applicability?

Outline

Aims

- Overarching Approach
- Convergence of Heterogeneous Data Sources
- Flexible
- Applicability
- Performance
- Complexity vs. Usability



Thesis Outline

- Analysis of Important Properties and Requirements
- Architecture for Overarching Event-driven NAaS
- Evaluation Prototype
  - Flexibility and Convergence of Data Sources
  - Performance
- Improvements in Distributed Contexts
- Coalescence Problems, Analysis and Solutions
- Improvements for Individual Components
- Threats to Validity

Thesis Outline

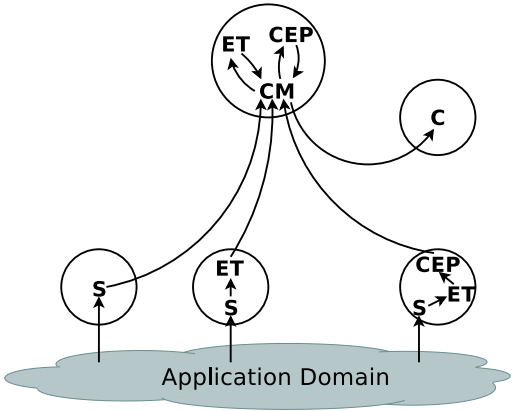
- Analysis of Important Properties and Requirements
- Architecture for Overarching Event-driven NAaS
- Evaluation Prototype
  - Flexibility and Convergence of Data Sources
  - Performance
- **Improvements in Distributed Contexts**
- Coalescence Problems, Analysis and Solutions
- **Improvements for Individual Components**
- Threats to Validity

General Architecture

- Important Properties and Requirements

General Architecture

- Important Properties and Requirements
- Event-driven Architecture
- Focus on the Essentials
- Unified Internal Event Representation
- Components
  - Sensors (S)
  - Event Transformer (ET)
  - ...



Prototype Implementation and Evaluation of Flexibility and Convergence

- Prototype Based on Architecture

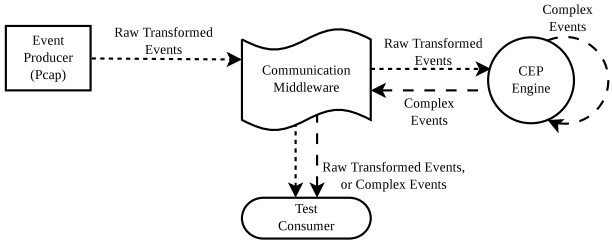


Figure: Evaluation Prototype

Prototype Implementation and Evaluation of Flexibility and Convergence

- Prototype Based on Architecture
- Evaluation of Flexibility and Convergence of Data Sources
- Step-wise Defined Goals
  - Basic System

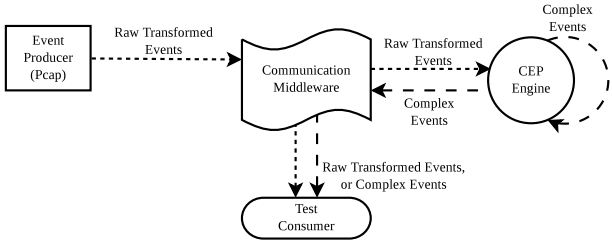


Figure: Evaluation Prototype

Prototype Implementation and Evaluation of Flexibility and Convergence

- Prototype Based on Architecture
- Evaluation of Flexibility and Convergence of Data Sources
- Step-wise Defined Goals
  - Basic System
  - Relocating Functionality

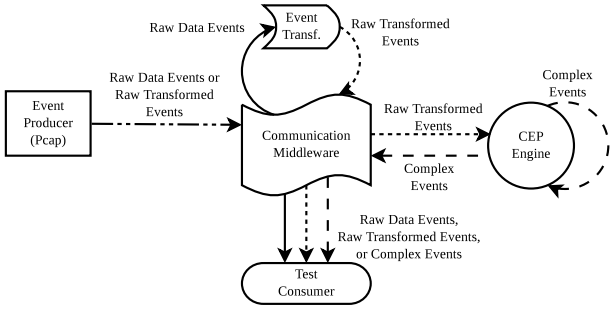


Figure: Evaluation Prototype

Prototype Implementation and Evaluation of Flexibility and Convergence

- Prototype Based on Architecture
- Evaluation of Flexibility and Convergence of Data Sources
- Step-wise Defined Goals
  - Basic System
  - Relocating Functionality
  - Convergence of Sensors

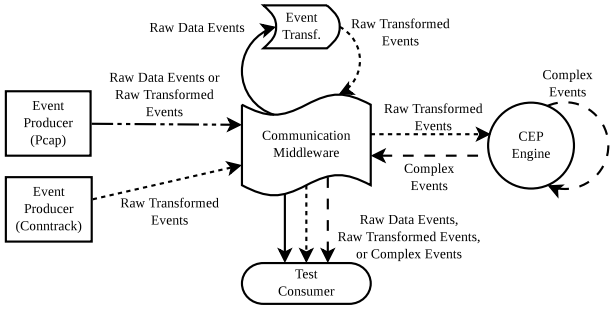


Figure: Evaluation Prototype

Prototype Implementation and Evaluation of Flexibility and Convergence

- Prototype Based on Architecture
- Evaluation of Flexibility and Convergence of Data Sources
- Step-wise Defined Goals
  - Basic System
  - Relocating Functionality
  - Convergence of Sensors
  - ...
- Results
  - **Flexible NAaS**
  - **Convergence of Sensors for NAaS**

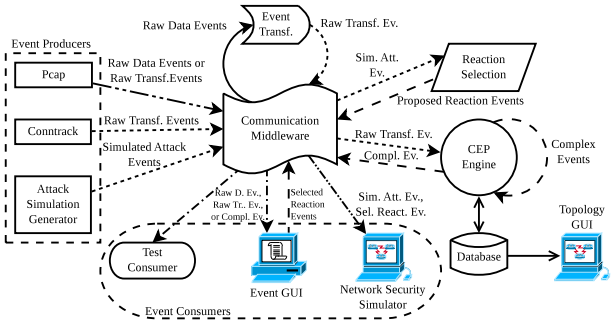
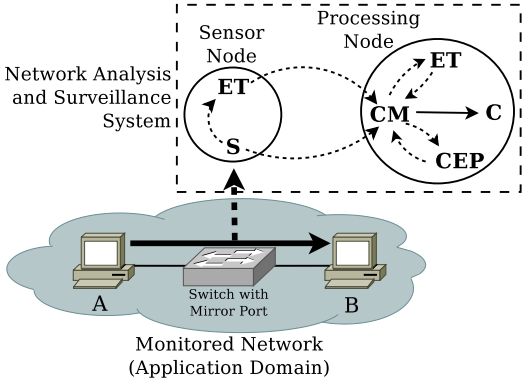


Figure: Evaluation Prototype

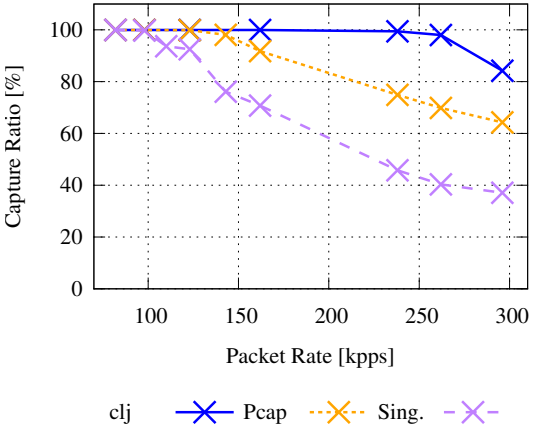
Performance Evaluation

- **Evaluation Setup**
- Packet Capturing as “Worst Case” Scenario



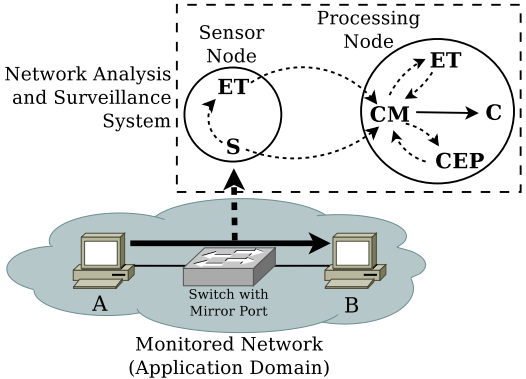
Performance Evaluation

- Evaluation Setup
- Packet Capturing as “Worst Case” Scenario
- Results
  - **Example Results**



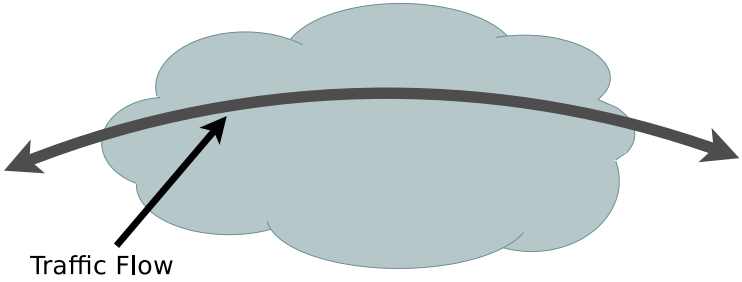
Performance Evaluation

- Evaluation Setup
- Packet Capturing as “Worst Case” Scenario
- Results
  - Example Results
  - **It works!**
  - **Most Critical: Sensor**



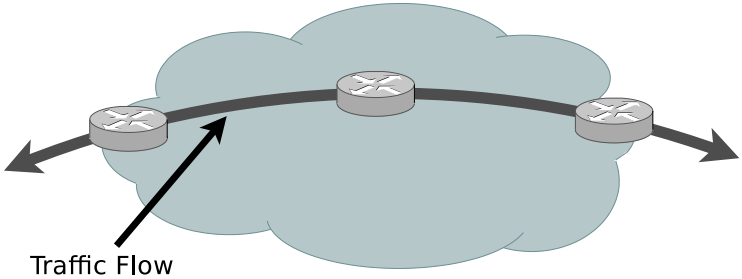
Outline

Sensors: Cooperation for Improving the Performance, Foundations



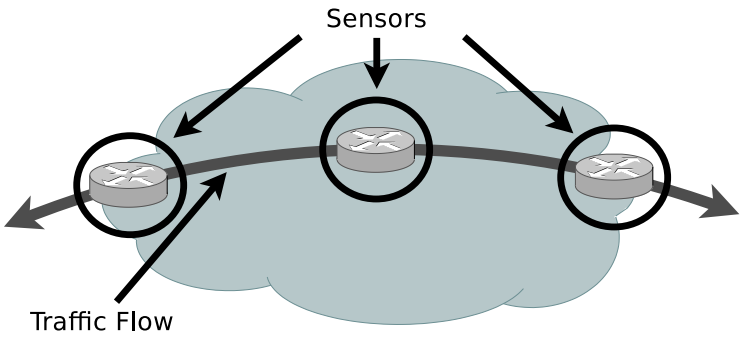
Paper: 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



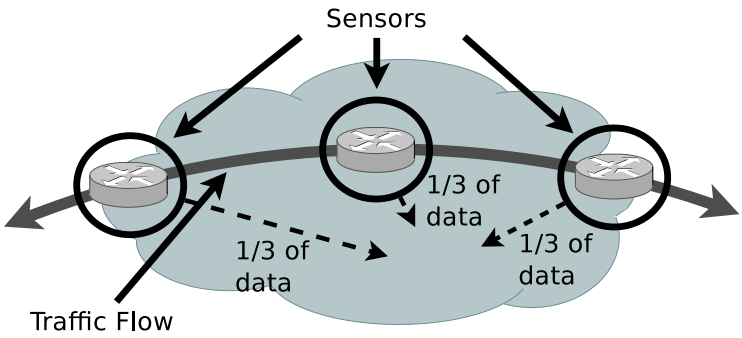
Paper: 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



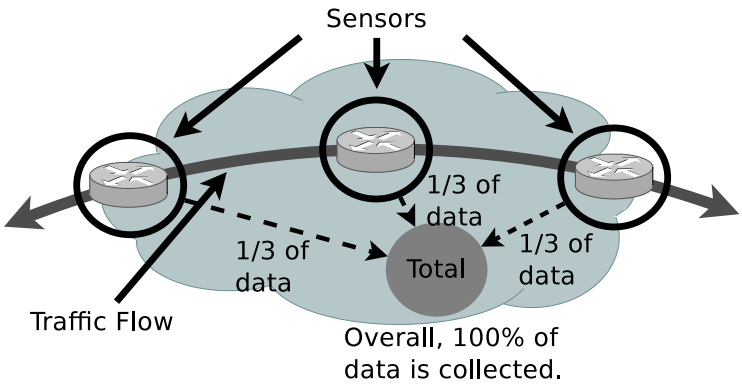
Paper: 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



Paper: 28th IEEE AINA 2014

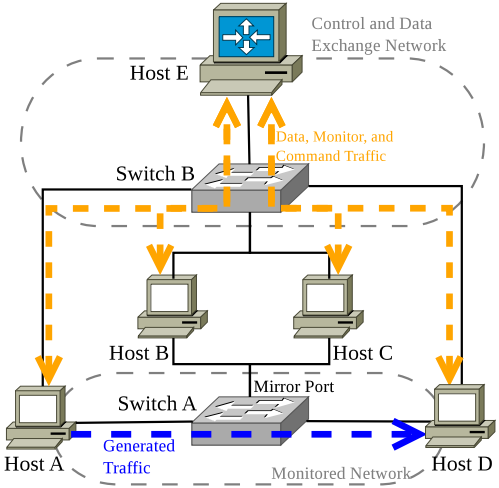
Sensors: Cooperation for Improving the Performance, Foundations



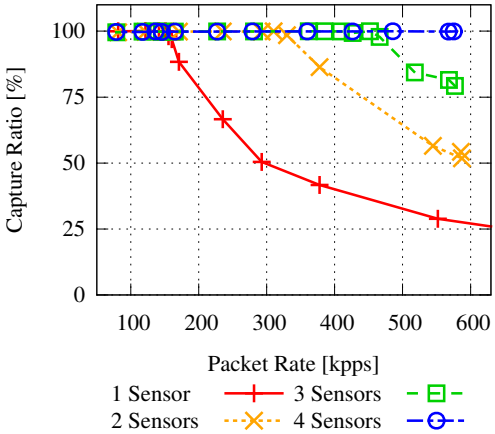
Paper: 28th IEEE AINA 2014

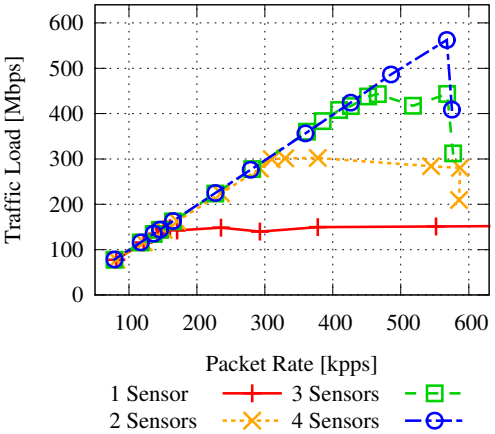
Cooperative Sensors, Architecture and Application

- Sensors: Hosts A to D
- Controller: Host E
  - Logic
  - Data Merging
  - Data Consumer
- Traffic Generation
  - Host A → Host D
- Paper: IEEE ICC 2015



Cooperative Sensors: Performance, Scalability, and Traffic Load





Cooperative Sensors: Improving Operation and Usability via Self-adaptivity

- Problem
  - Complexity of Operation & Usability
- Solution
  - Self-adaptation
- Example
  - On-demand Cooperation
- Aims
  - Capture as much as possible.
  - Avoid overload.
  - Reduce # of sensors.
- Apply cooperation as necessary.

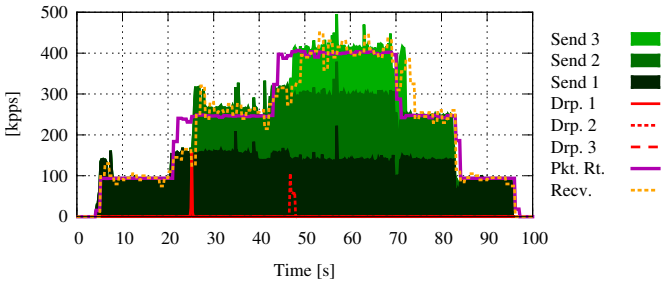
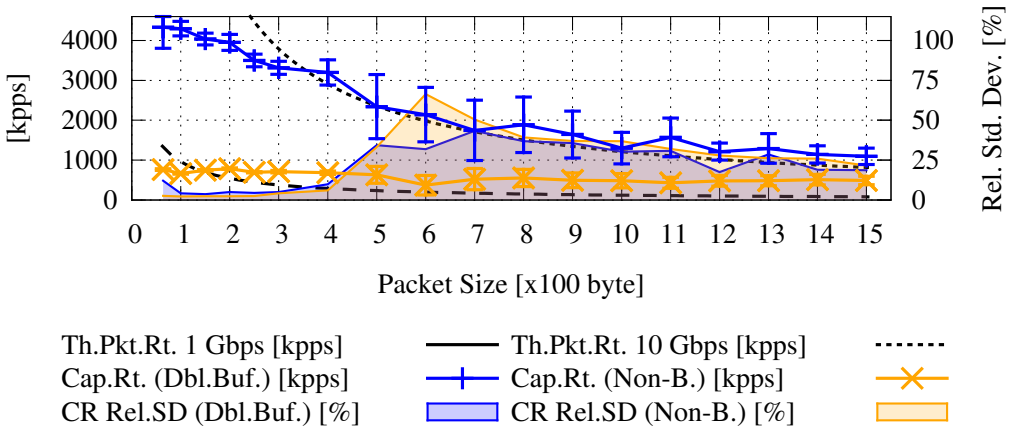


Figure: Detailed Results of an Example Experiment

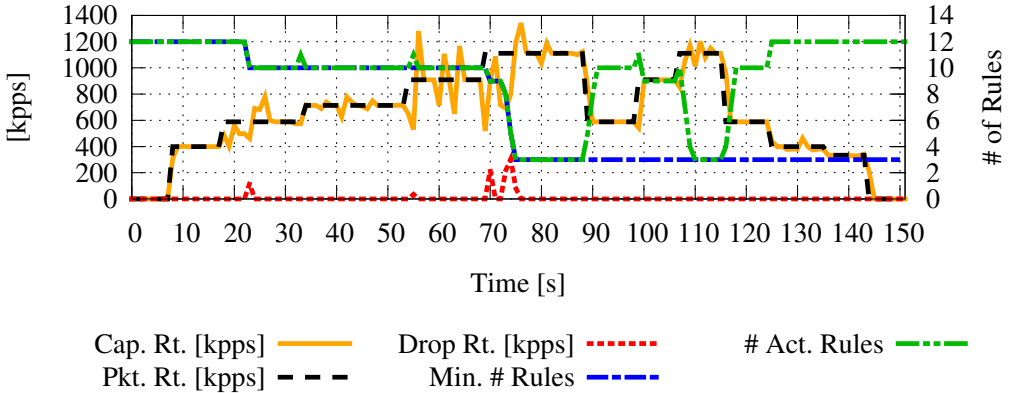
Improvements for Individual Components

- Example: Sensor
- Packet Capturing with Java & Clojure
- Analyze the optimization potential in various areas.
- Paper: 20th IEEE ISCC 2015

Raw Data Acquisition: Improved Method vs. Old Method



Example Results of Self-adaptive Performance-based Adjustment



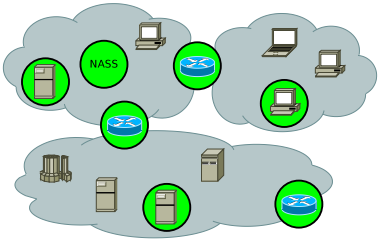
Outline

Summary

- Computer Networks: **Critical Importance**
- Assuring Operating Networks → **Information**
- **Network Analysis and Surveillance**
  (Network Reconnaissance, Network Monitoring)
- "Good" Information → **challenging**.
- (Contradicting) **Requirements** and **Properties**
- **EDA** and **CEP** to the Rescue
- **Related Work**: Too Focused, Real World Applicability?
- **Thesis Aims: Overarching and Applicable NAaS**

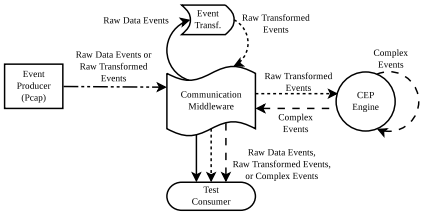
Answered Research Questions (I)

1. What are important properties and requirements for overarching and flexible NAaS?
   - → Enumeration and Discussion of Properties and Requirements
2. Does our NAaS approach offer convergence of data sources and is it flexible?
   - → Convergence works.
   - → The architecture is flexible.



Answered Research Questions (I)

1. What are important properties and requirements for overarching and flexible NAaS?
   → Enumeration and Discussion of Properties and Requirements
2. Does our NAaS approach offer convergence of data sources and is it flexible?
   → Convergence works.
   → The architecture is flexible.

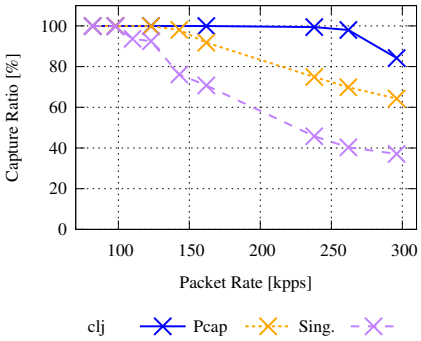


Answered Research Questions (II)

3 What are the performance limits and what is the most relevant bottleneck?
- → Detailed Performance Analysis
- → CEP and EDA for NAaS works.
- → Most Important Bottleneck: Sensors

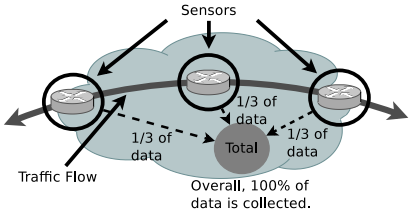
4 Can the most relevant performance bottleneck be addressed by leveraging distributed approaches?
- → Cooperative Sensors

5 Can the increased complexity of distributed approaches be addressed?
- → Self-adaptive On-demand Cooperation



Answered Research Questions (II)

3. What are the performance limits and what is the most relevant bottleneck?
   - → Detailed Performance Analysis
   - → CEP and EDA for NAaS works.
   - → Most Important Bottleneck: Sensors
4. Can the most relevant performance bottleneck be addressed by leveraging distributed approaches?
   - → Cooperative Sensors
5. Can the increased complexity of distributed approaches be addressed?
   - → Self-adaptive On-demand Cooperation

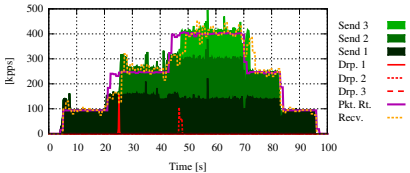


Answered Research Questions (II)

3 What are the performance limits and what is the most relevant bottleneck?
- → Detailed Performance Analysis
- → CEP and EDA for NAaS works.
- → Most Important Bottleneck: Sensors

4 Can the most relevant performance bottleneck be addressed by leveraging distributed approaches?
- → Cooperative Sensors

5 Can the increased complexity of distributed approaches be addressed?
- → Self-adaptive On-demand Cooperation



Answered Research Questions (III)

6 May the distributed nature of our approach cause additional performance issues and how can these be addressed?

→ Problem: Accumulating Data

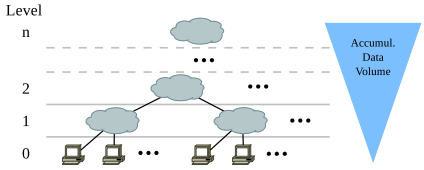
→ Hierarchical Event Patterns, Multi-tiered Setups

7 What is the most relevant performance limit of our approach in a non-distributed scenario and how can it be addressed?

→ Sensor

→ Example: Packet Capturing

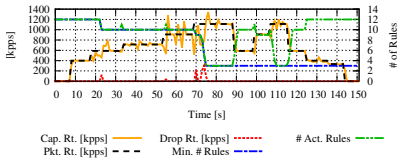
→ Various Improvements



Answered Research Questions (III)

6 May the distributed nature of our approach cause additional performance issues and how can these be addressed?
- → Problem: Accumulating Data
- → Hierarchical Event Patterns, Multi-tiered Setups

7 What is the most relevant performance limit of our approach in a non-distributed scenario and how can it be addressed?
- → Sensor
- → Example: Packet Capturing
- → Various Improvements



Publications

- Improving Network Traffic Acquisition and Processing with the Java Virtual Machine, R. Gad, M. Kappes, and I. Medina-Bulo, 20th IEEE ISCC 2015, in press
- Monitoring Traffic in Computer Networks with Dynamic Distributed Remote Packet Capturing, R. Gad, M. Kappes, and I. Medina-Bulo, IEEE ICC 2015, in press
- Analysis of the Feasibility to Combine CEP and EDA with Machine Learning using the Example of Network Analysis and Surveillance, R. Gad, M. Kappes, and I. Medina-Bulo, JCIS – SISTEDES 2014
- Bridging the Gap between Low-level Network Traffic Data Acquisition and Higher-level Frameworks, R. Gad, M. Kappes, and I. Medina-Bulo, IEEE COMPSACW 2014
- Header Field Based Partitioning of Network Traffic for Distributed Packet Capturing and Processing, R. Gad, R. Mueller-Bady, M. Kappes, and I. Medina-Bulo, 28th IEEE AINA 2014
- Employing the CEP Paradigm for Network Analysis and Surveillance, R. Gad, M. Kappes, J. Boubeta-Puig, and I. Medina-Bulo, AICT 2013
- Leveraging EDA and CEP for Integrating Low-level Network Analysis Methods into Modern, Distributed IT Architectures, R. Gad, M. Kappes, J. Boubeta-Puig, and I. Medina-Bulo, JCIS – SISTEDES 2012
- Hierarchical events for efficient distributed network analysis and surveillance, R. Gad, M. Kappes, J. Boubeta-Puig, and I. Medina-Bulo, WAS4FI 2012

Open Source Software Contributions

- Clojure and Java Packet Capturing Library
  `https://github.com/ruedigergad/clj-net-pcap`
- Distributed Remote Packet Capturing (DRePCap)
  `https://github.com/fg-netzwerksicherheit/drepcap`
  - clj-jms-activemq-toolkit
    `https://github.com/fg-netzwerksicherheit/clj-jms-activemq-toolkit`
  - drepcap-sensor
    `https://github.com/fg-netzwerksicherheit/drepcap-sensor`
  - drepcap-merger
    `https://github.com/fg-netzwerksicherheit/drepcap-merger`
  - drepcap-frontend
    `https://github.com/fg-netzwerksicherheit/drepcap-frontend`
- Patches for jNetPcap

Conclusion

- EDA and CEP for Overarching NAaS
- It works!
- Improved the state of the art.

End

Thank you for your attention!

Questions?

Rüdiger Gad

rgad@fb2.fra-uas.de

r.c.g@gmx.de