SPRING 2016 Keynote

Event-driven Network Monitoring
&
Experiences during and after doing a PhD

Rüdiger Gad

Terma GmbH, Space, Ground Systems, Darmstadt, Germany

2016-06-02

Outline

Outline

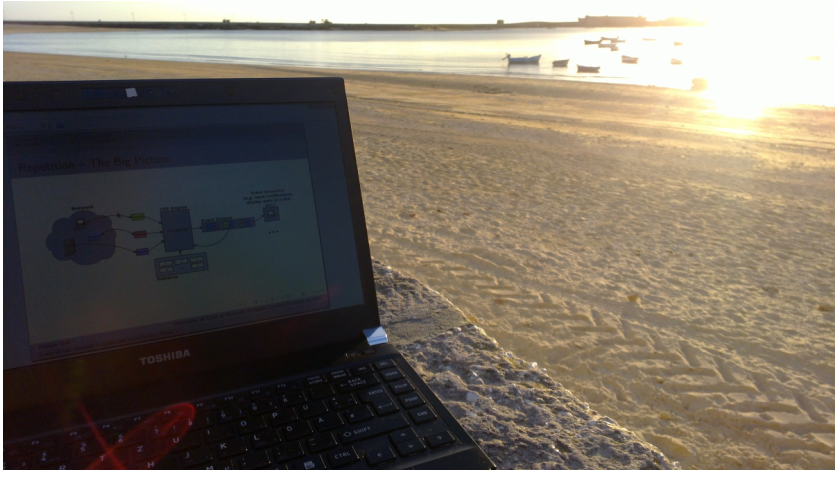
Some Context

- University of Cádiz (UCA)
- Spain, Andalusia
- Cooperation with the UCASE Research Group
- Employment at FRA-UAS as Research Assistant

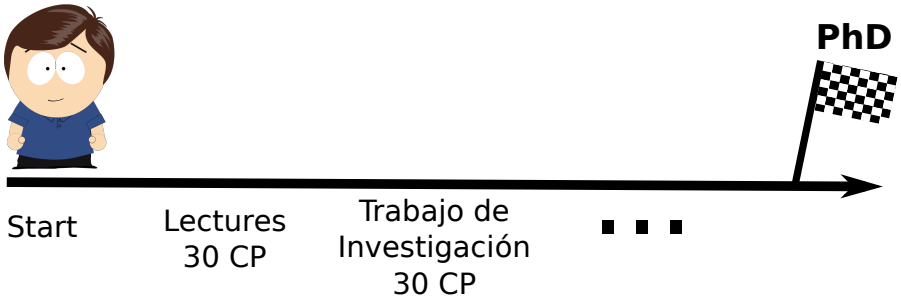
The PhD Program

- Regulated by Royal Decree
- Admission Requirements: 300 CP
- Study Fees: approximately 170 Euro/Year
- 2 Supervisors
- Other Aspects
  - Stay in Cádiz, about 5 Months
  - Regular Visits, about each 1/2 Year

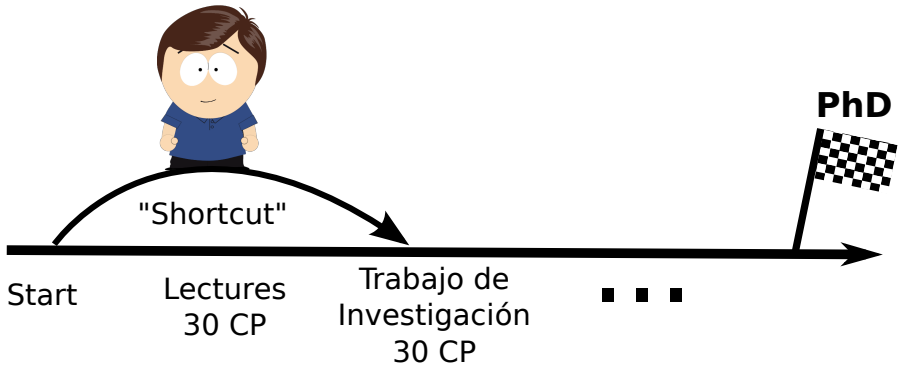
Being in Cádiz



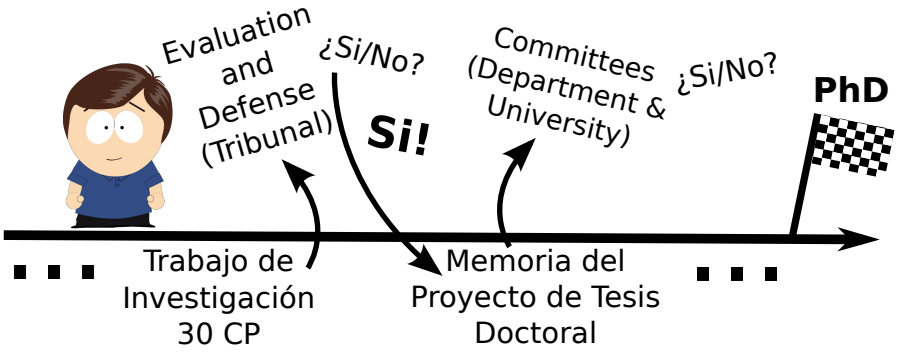
Progress of the PhD Studies



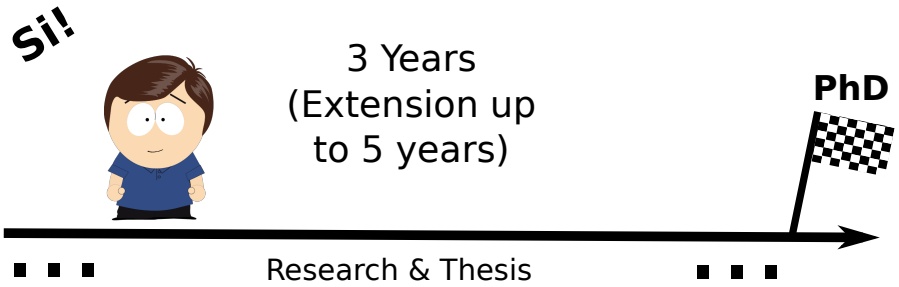
Progress of the PhD Studies



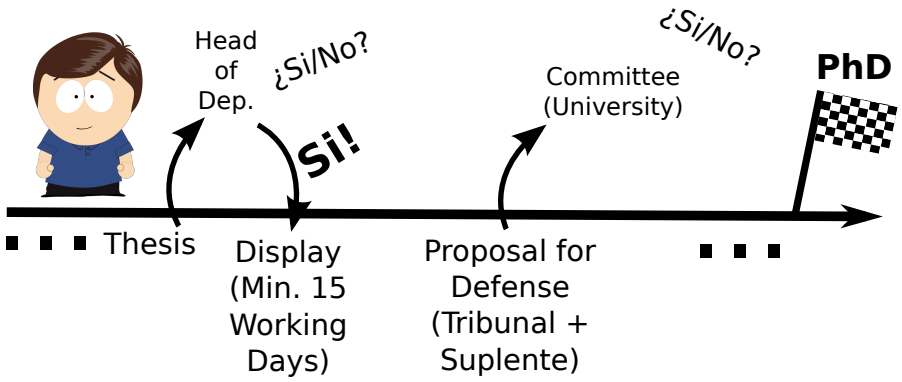
Progress of the PhD Studies



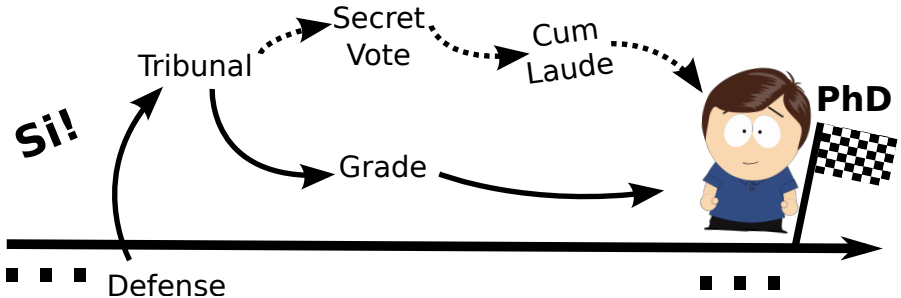
Progress of the PhD Studies



Progress of the PhD Studies



Progress of the PhD Studies



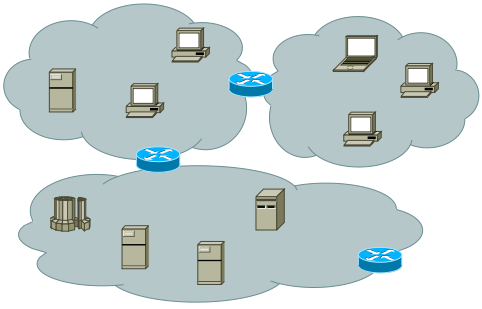
Outline

Assure Operational Computer Networks

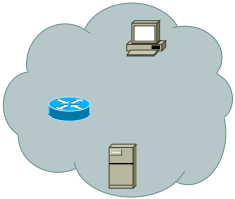
- Basis
  - Information
    - Detailed
    - Accurate
    - Up-to-date
    - ...
  - Network Monitoring
    ("Network Reconnaissance" or "Network Analysis and Surveillance")

Network Monitoring (NM)

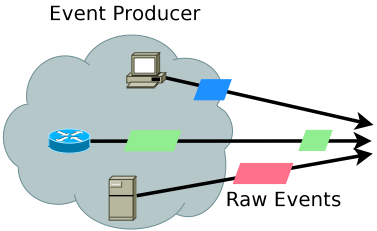
- Challenging
  - Distribution
  - Size
  - Change
  - Timeliness
  - Data Volume
  - ...



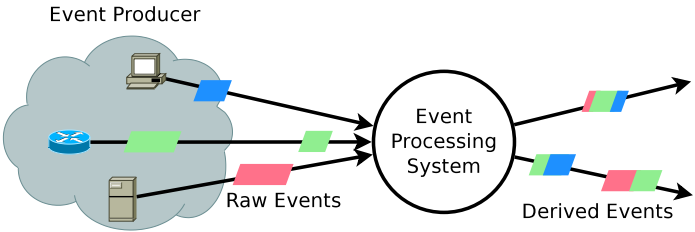
Event-driven Principles and Complex Event Processing (CEP) for NM



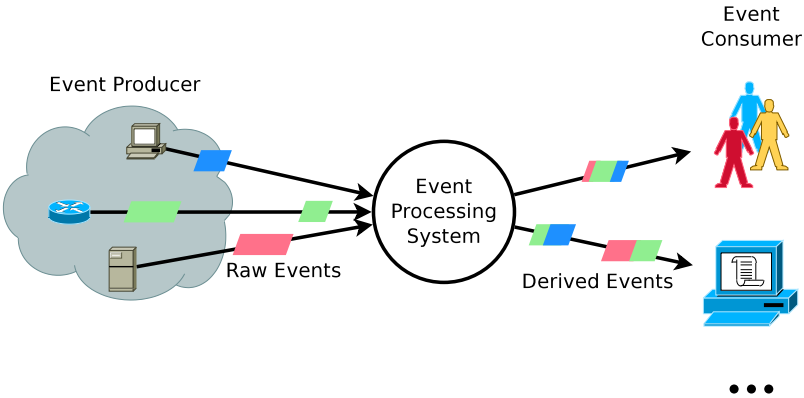
Event-driven Principles and Complex Event Processing (CEP) for NM



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



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

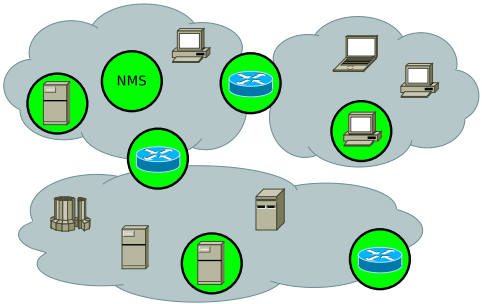


Event-driven Architecture (EDA) and CEP for NM

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

Aims

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

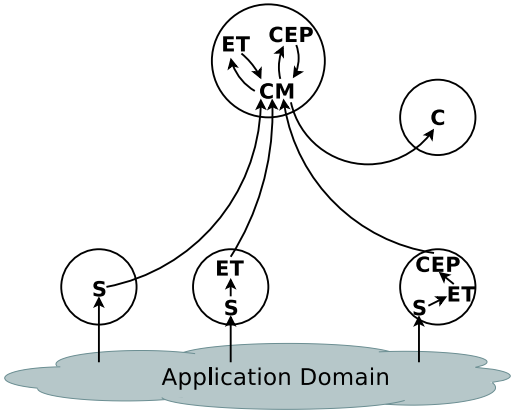


Generalized Event-driven Architecture

- Important Properties and Requirements

Generalized Event-driven 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

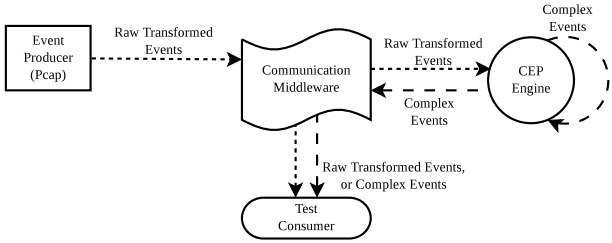


Figure: Evaluation Prototype

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

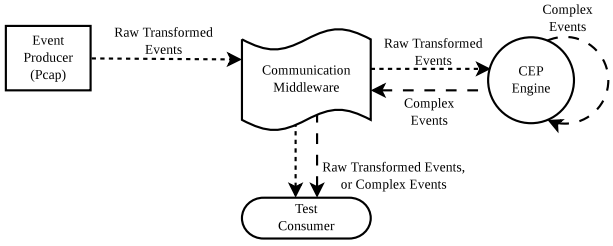


Figure: Evaluation Prototype

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

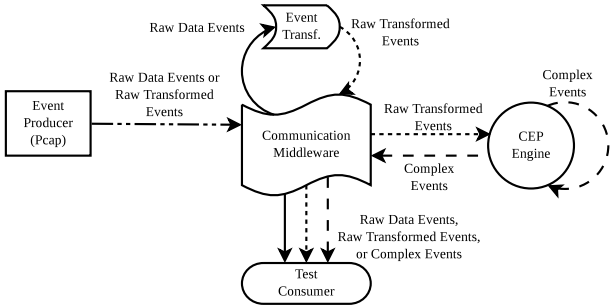


Figure: Evaluation Prototype

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

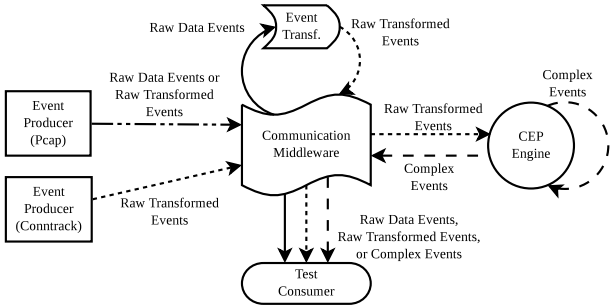


Figure: Evaluation Prototype

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**
  - **Convergence of Sensors**

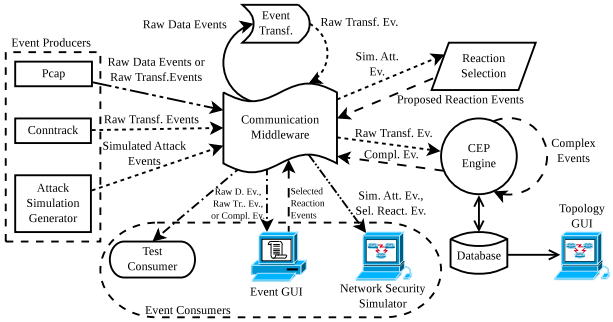
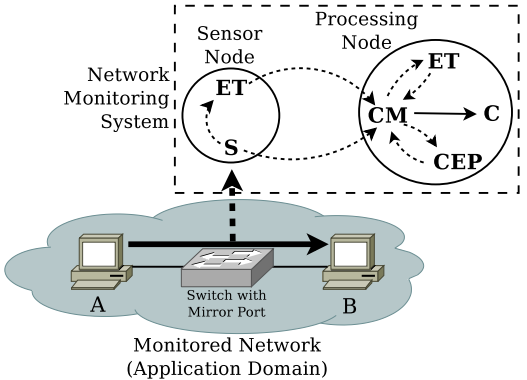


Figure: Evaluation Prototype

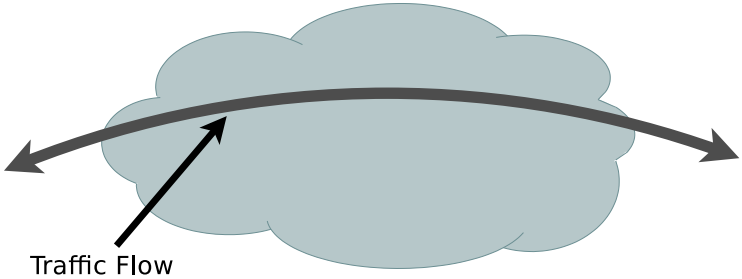
Performance Evaluation

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



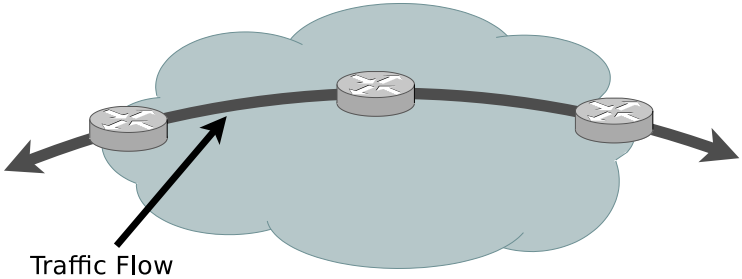
Outline

Sensors: Cooperation for Improving the Performance, Foundations



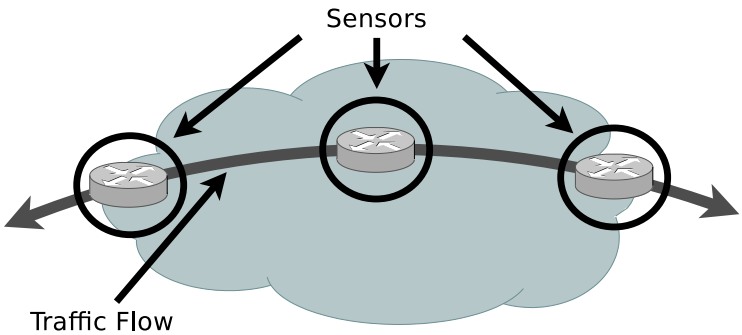
Paper: Gad et al., 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



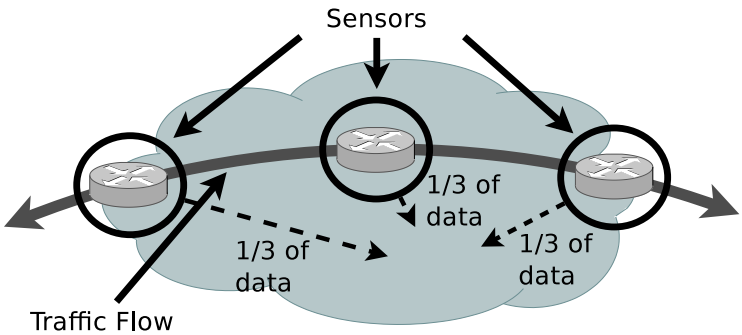
Paper: Gad et al., 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



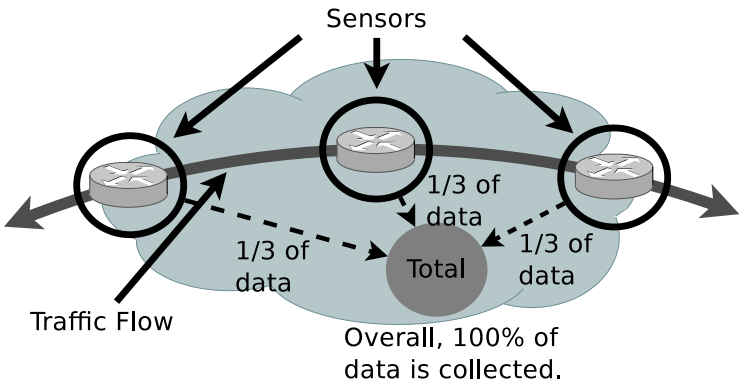
Paper: Gad et al., 28th IEEE AINA 2014

Sensors: Cooperation for Improving the Performance, Foundations



Paper: Gad et al., 28th IEEE AINA 2014

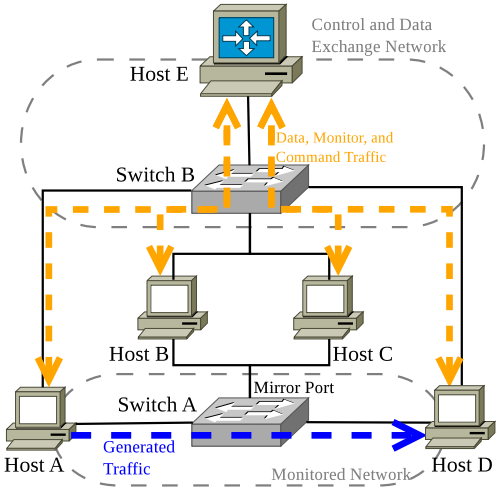
Sensors: Cooperation for Improving the Performance, Foundations



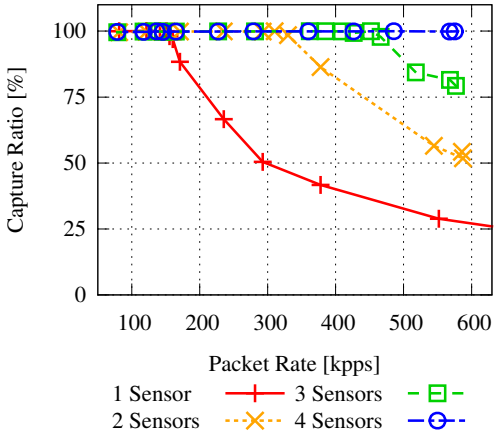
Paper: Gad et al., 28th IEEE AINA 2014

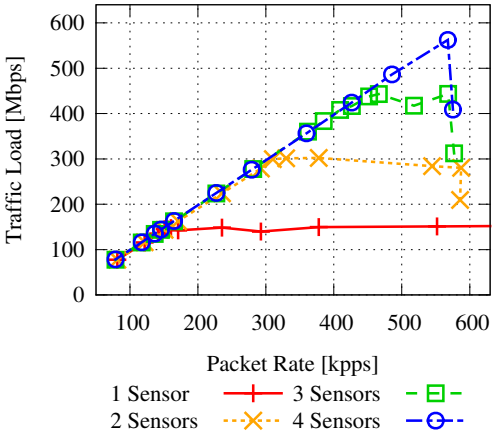
Cooperative Sensors, Architecture and Application

- Sensors: Hosts A to D
- Controller: Host E
  - Logic
  - Data Merging
  - Data Consumer
- Traffic Generation
  - Host A $\rightarrow$ Host D
- Paper: Gad et al., 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.

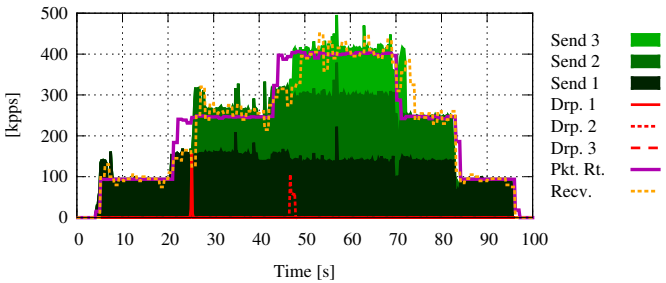
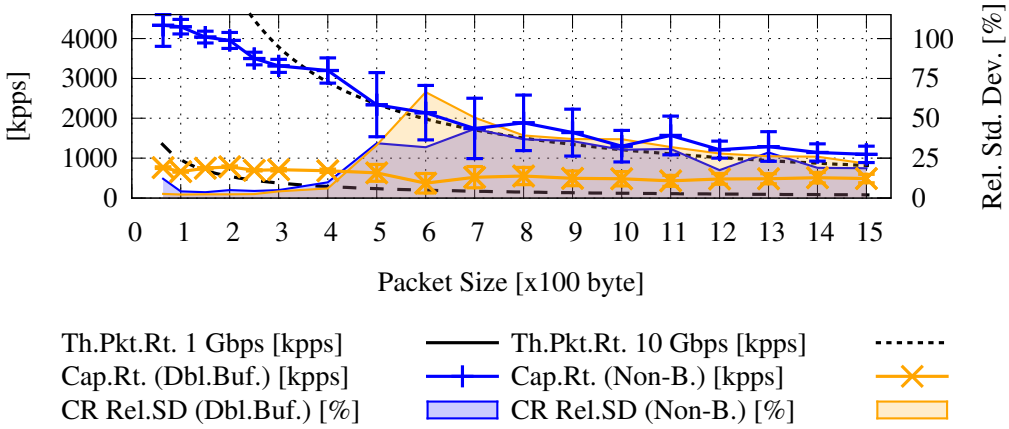


Figure: Detailed Results of an Example Experiment

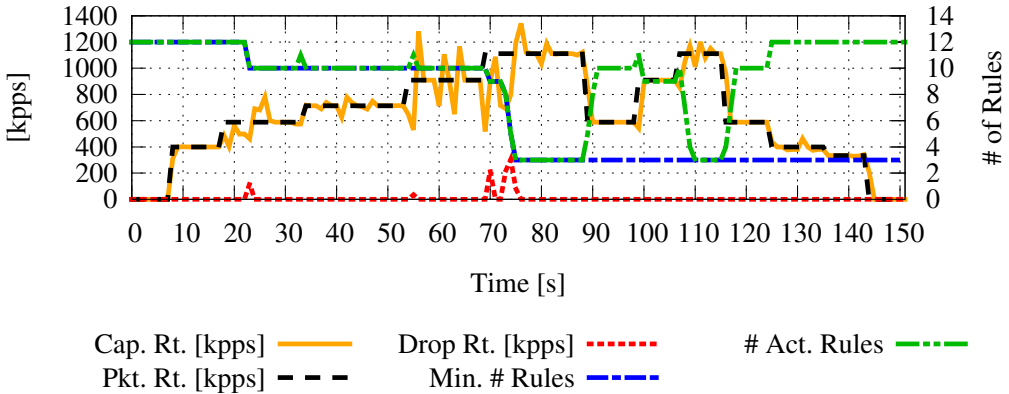
Improvements for Individual Components

- Example: Sensor
- Packet Capturing with Java & Clojure
- Analyze the optimization potential in various areas.
- Paper: Gad et al., 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 Monitoring**
  (Network Reconnaissance, Network Analysis and Surveillance)
- "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 NM**

Publications

- Local Programming Language Barriers in Stream-based Systems, R. Gad, M. Kappes, and I. Medina-Bulo, 21st IEEE ISCC 2016, in press
- Improving Network Traffic Acquisition and Processing with the Java Virtual Machine, R. Gad, M. Kappes, and I. Medina-Bulo, 20th IEEE ISCC 2015
- Monitoring Traffic in Computer Networks with Dynamic Distributed Remote Packet Capturing, R. Gad, M. Kappes, and I. Medina-Bulo, IEEE ICC 2015
- 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
- Distributed Event-driven Network Monitoring Evaluation Prototype (DENMEvaP)
  `https://github.com/ruedigergad/DENMEvaP`
- See also: `http://ruedigergad.com`

Conclusion

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

Outline

Considerations where to go?

- Industry vs. Academia?
- Family
  - Wife
  - Children
- Flexibility?
  - Relocating?
  - "Weekends at home"
  - "5 4 3 Model"
- Fun? (Exciting, Challenging, and Diverse Tasks)
- Longer Term Perspective?
- ...

My Choice

- Industry, Terma GmbH
- Senior Software Engineer, Space, Ground Systems
- Fun! (Exciting, Challenging, and Diverse Tasks)
  - Software Engineering
  - Work in Diverse Projects
  - Prototyping and Applied Research
  - Possibility to Shape and Influence the Progress
  - Preparation of Proposals
  - Responsibility for Team Members
  - Direct Customer Interaction
- Other aspects are also as wished.
  - Great Colleagues, Flexibility, Commuting, ...

Things I strengthened and learned while doing the PhD.

- Independent and Self-organized Work
- Ability to Handle Stress and Pressure
- Experience with
  - Research
  - Project Work and Administration
  - Creating Proposals
  - Supervision of Team Members
- "Applied Sciences"

Outline

End

Thank you for your attention!

Questions?

Rüdiger Gad

http://ruedigergad.com

ruga@terma.com

r.c.g@gmx.de