Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications

A Framework for IDS in Smart Cities

Krimmling, Jana

innovations
for high
performance
microelectronics

Member of
Leibniz Association

10/29/2014

http://www.smartie-project.eu/

Outline

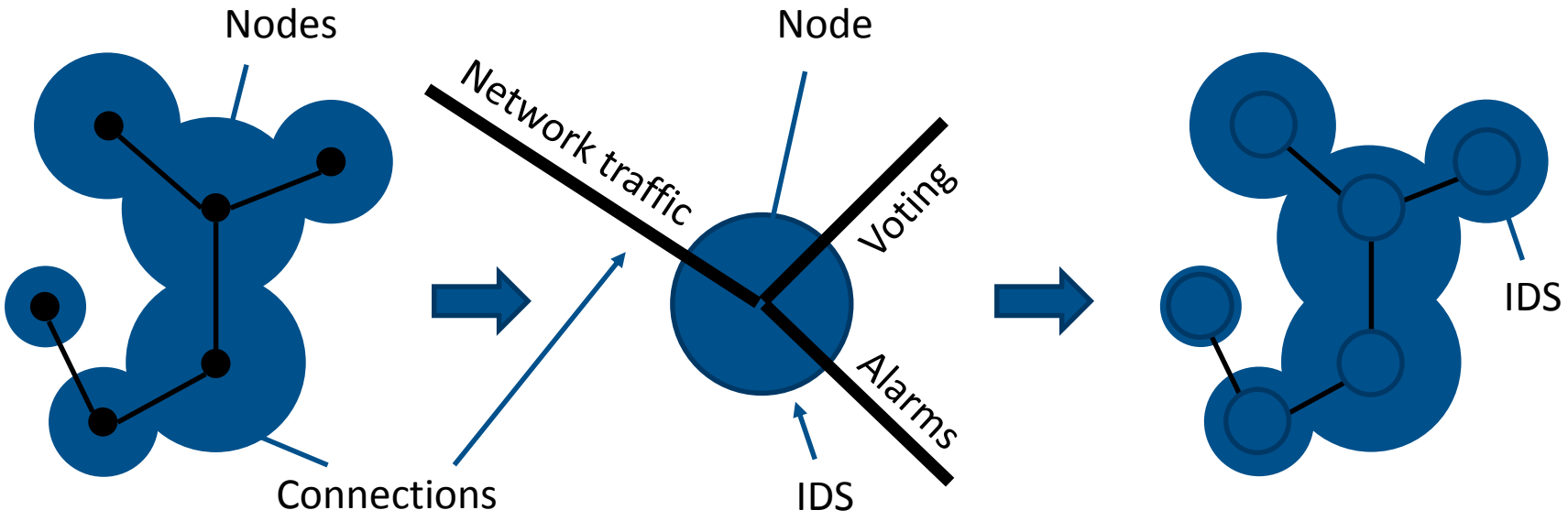
Introduction / Motivation

- We present a framework for IDS evaluation in Smart Cities using CoAP
  - Leightweight IDS can support and increase smart things network security
  - Hard to choose, compare and tune intrusion detection algorithms for a particular application
  - CoAP is expected to become one of the major smart things protocols
- Consists of a hybrid simulation and small testbed with real nodes
  - We give implementation details
  - Both have advantages and disadvantages for testing
- We show how to use it for a particular smart city scenario
  - Use case of the SMARTIE project
  - Public transport scenario using smart objects on buses
- We compare three IDS algorithms
  - Found a hybrid approach which is expected
  - Shows the feasiility of the approach

Outline

IDS Design and Evaluation

1. Analyse the scenario to protect
2. Design and implement IDS detection, voting, alarm distribution methods
3. Evaluate and optimize IDS for scenario



Smart city scenario or application

IDS design and implementation

Evaluation and tuning for smart city scenario

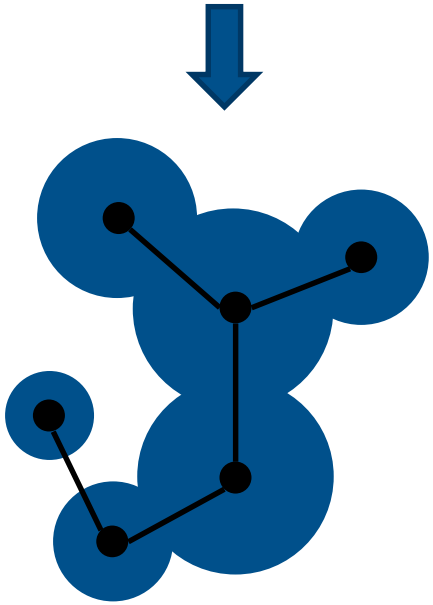
IDS Design and Evaluation

For that we ...

- Choose one of the available IDS algorithms ...
  - Rule based approaches
  - Anomaly or / and learning approaches
    - Statistical approaches, Support Vector Machines, Neural Networks, Baysian Network, Data mining, Clustering approaches, Nearest Neighbor Approaches, Spectral approaches, Information-theoretic approaches, ...
    - Hybrid models
- Define against which attacks we want to be protected ...
  - Jamming attacks, routing attacks, security related attacks
  - MitM and other complex attacks, ...
- Evaluate and optimize the IDS ...
  - Benchmark (streams), Comparison to other IDS
  - Tune the IDS for any specific application‘s needs

IDS Design and Evaluation

Network protocol



Smart city scenario

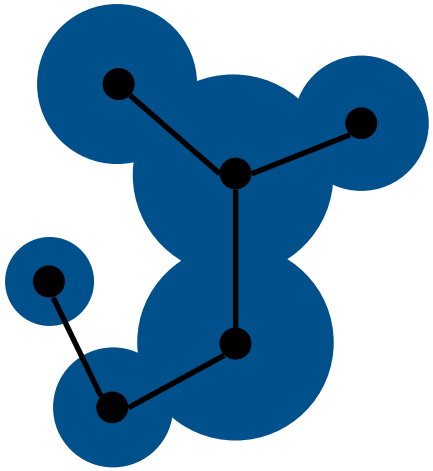
Application

IDS Implementation

IDS Design and Evaluation

Network protocol

Limited



Smart city scenario

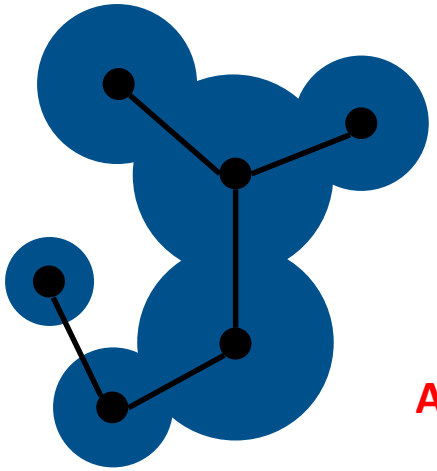
IDS Implementation

Application

IDS Design and Evaluation

Network protocol

Limited



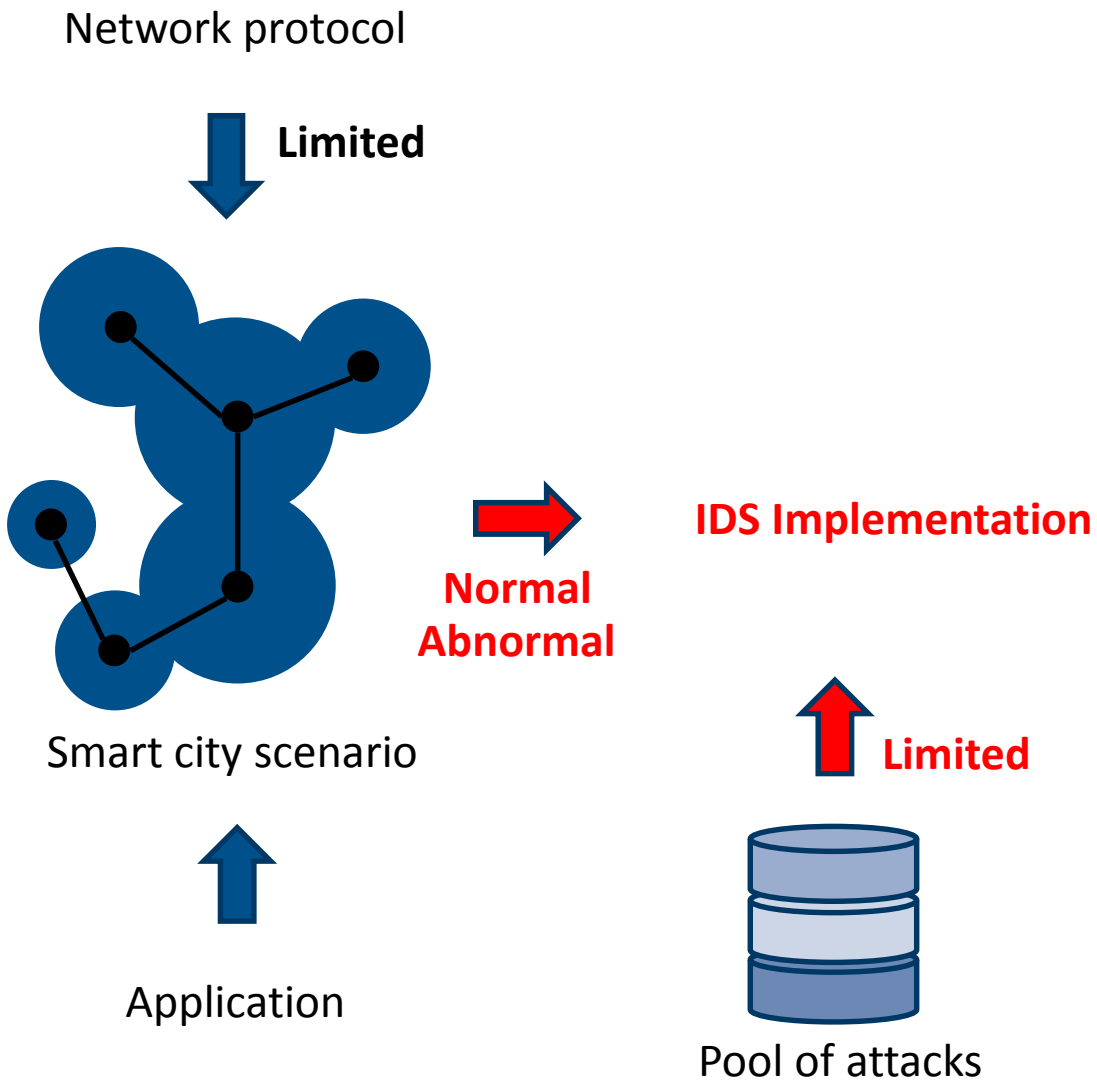
Smart city scenario

Normal
Abnormal

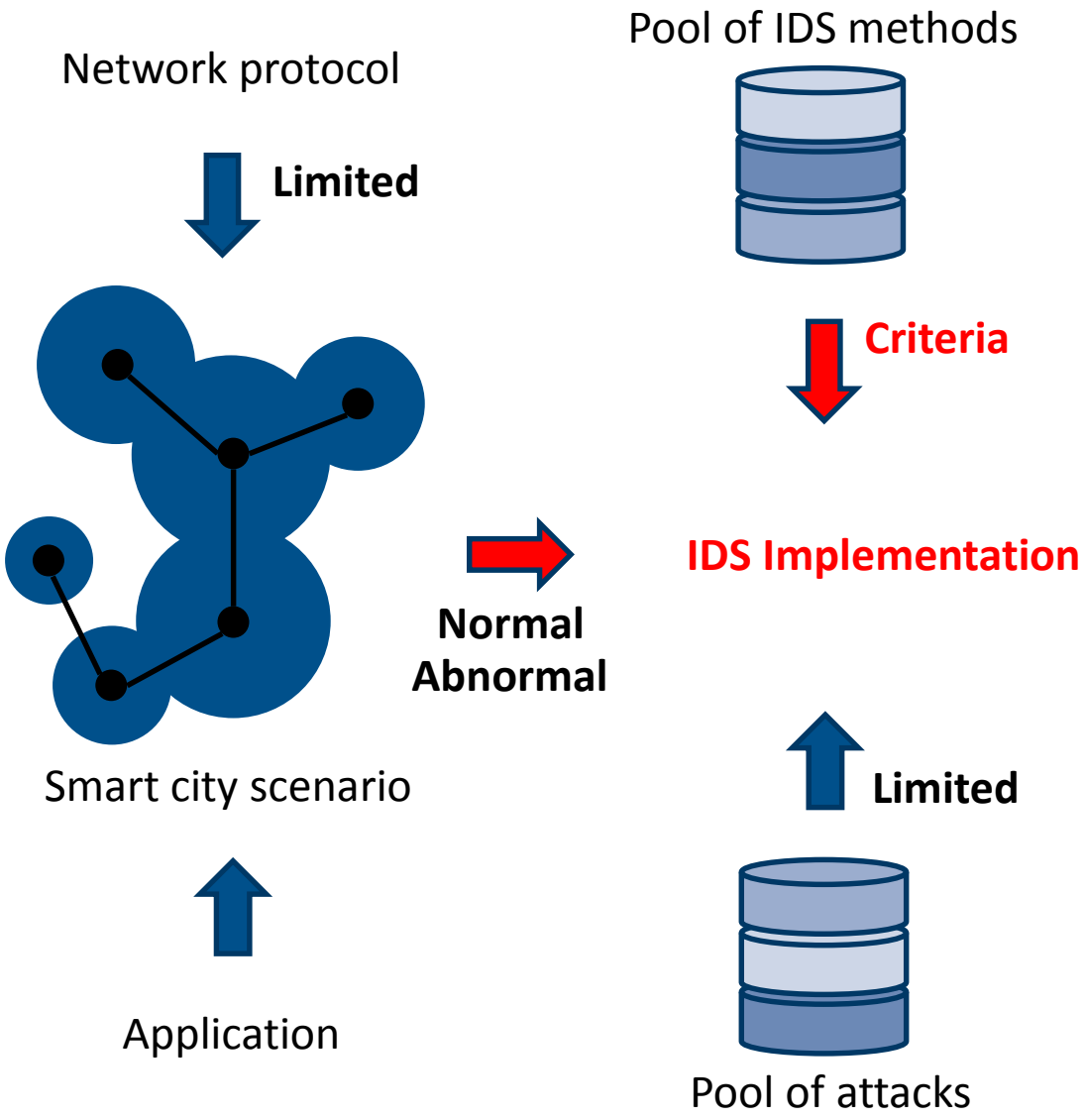
IDS Implementation

Application

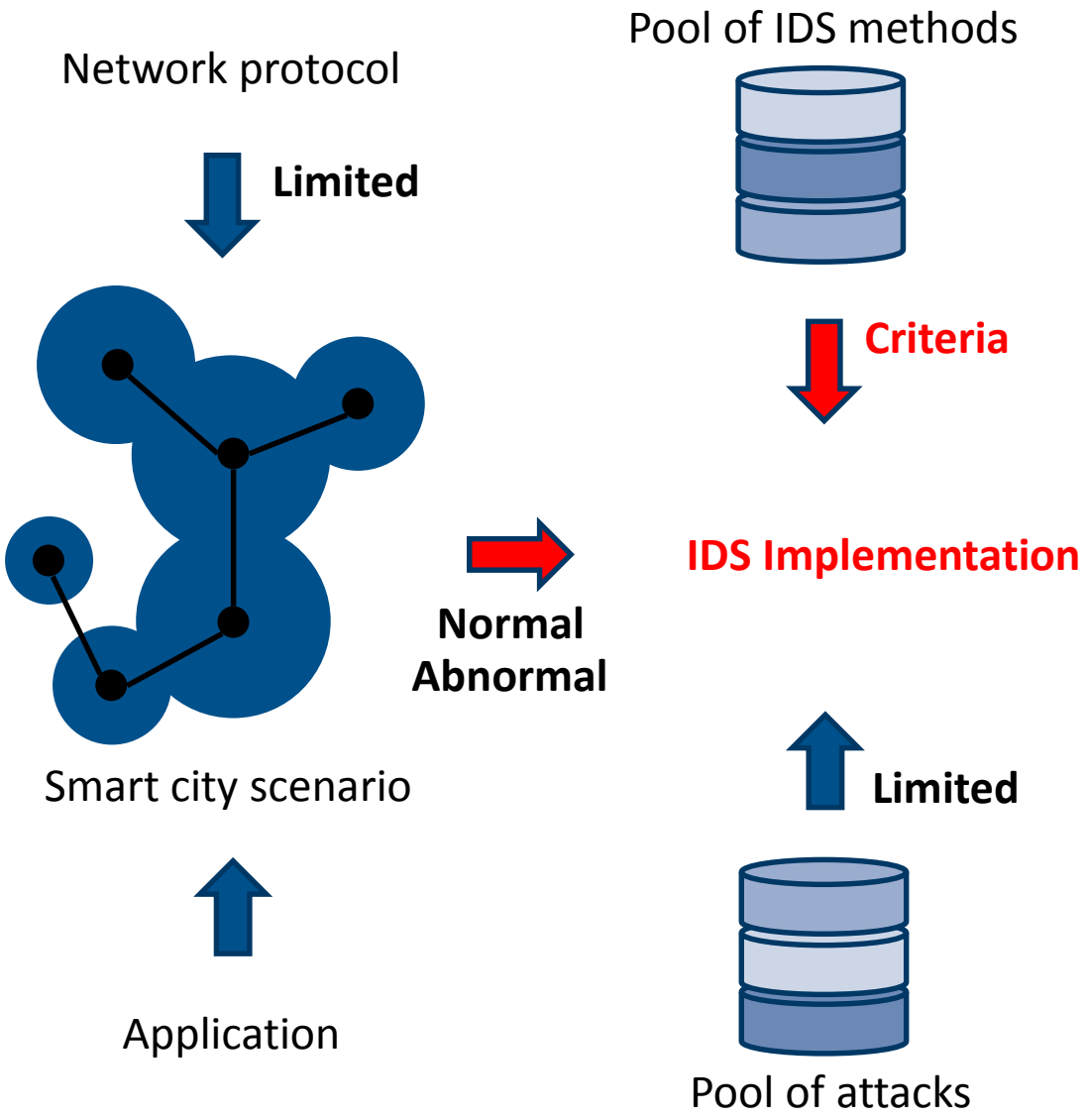
IDS Design and Evaluation



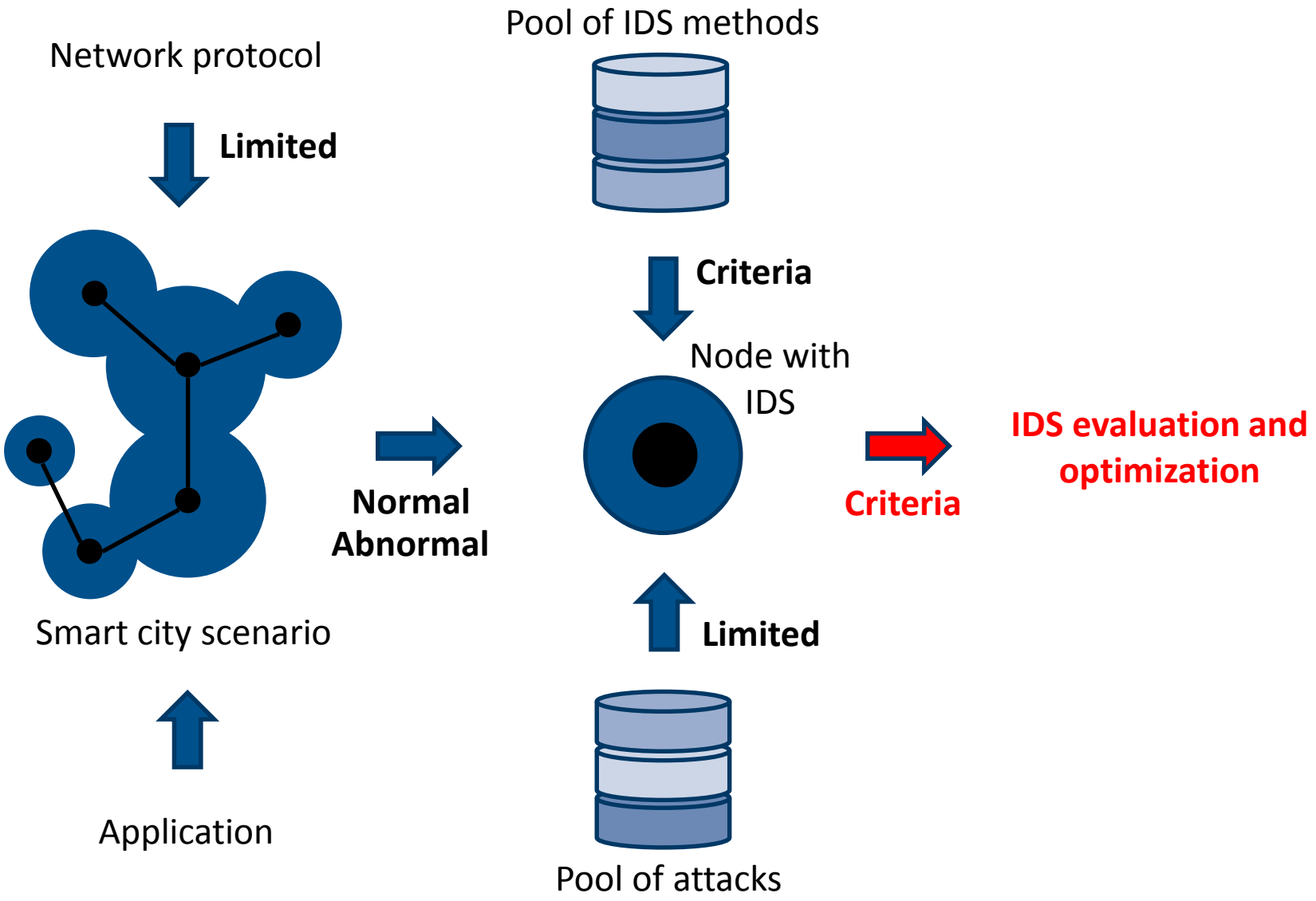
IDS Design and Evaluation



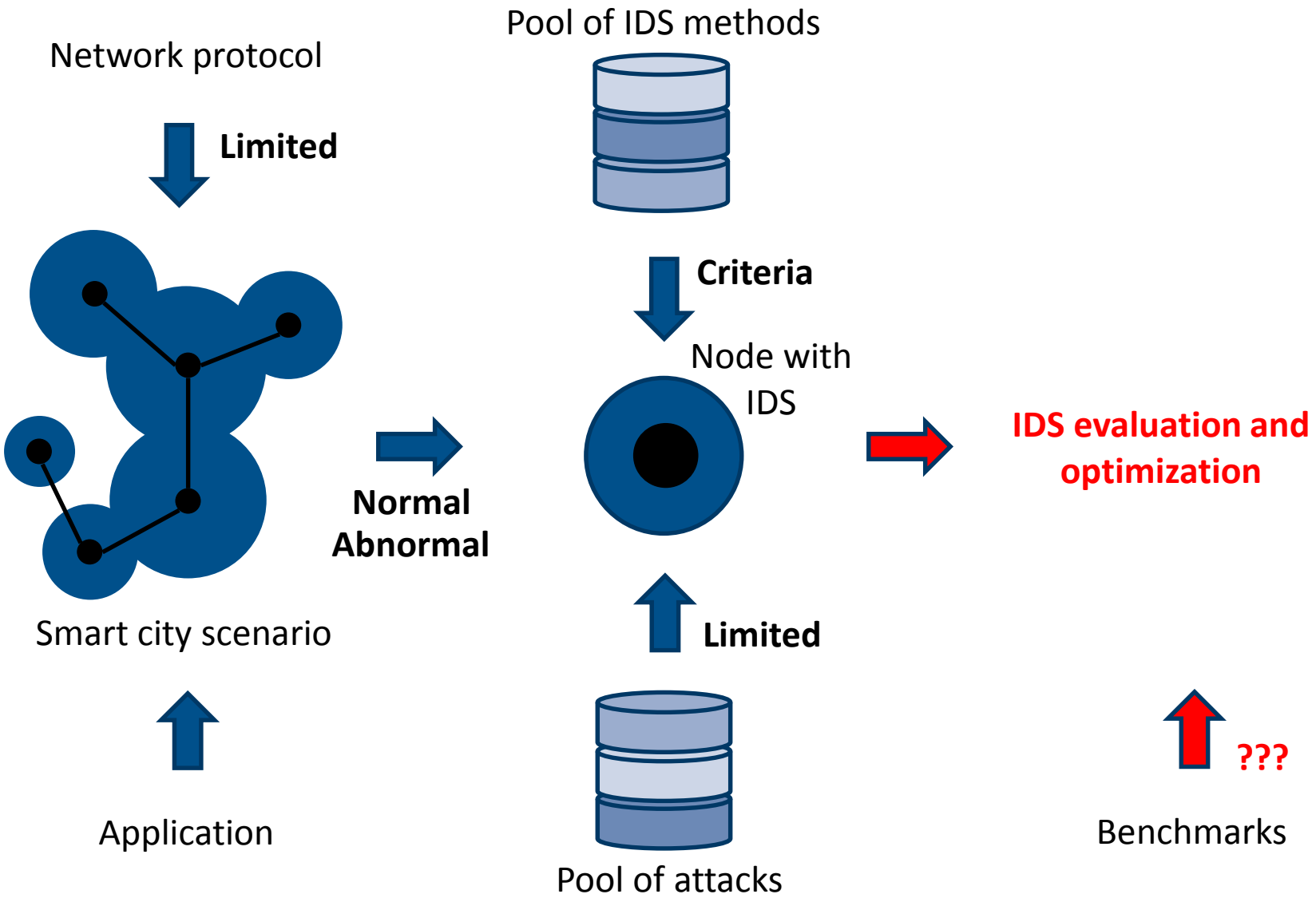
IDS Design and Evaluation



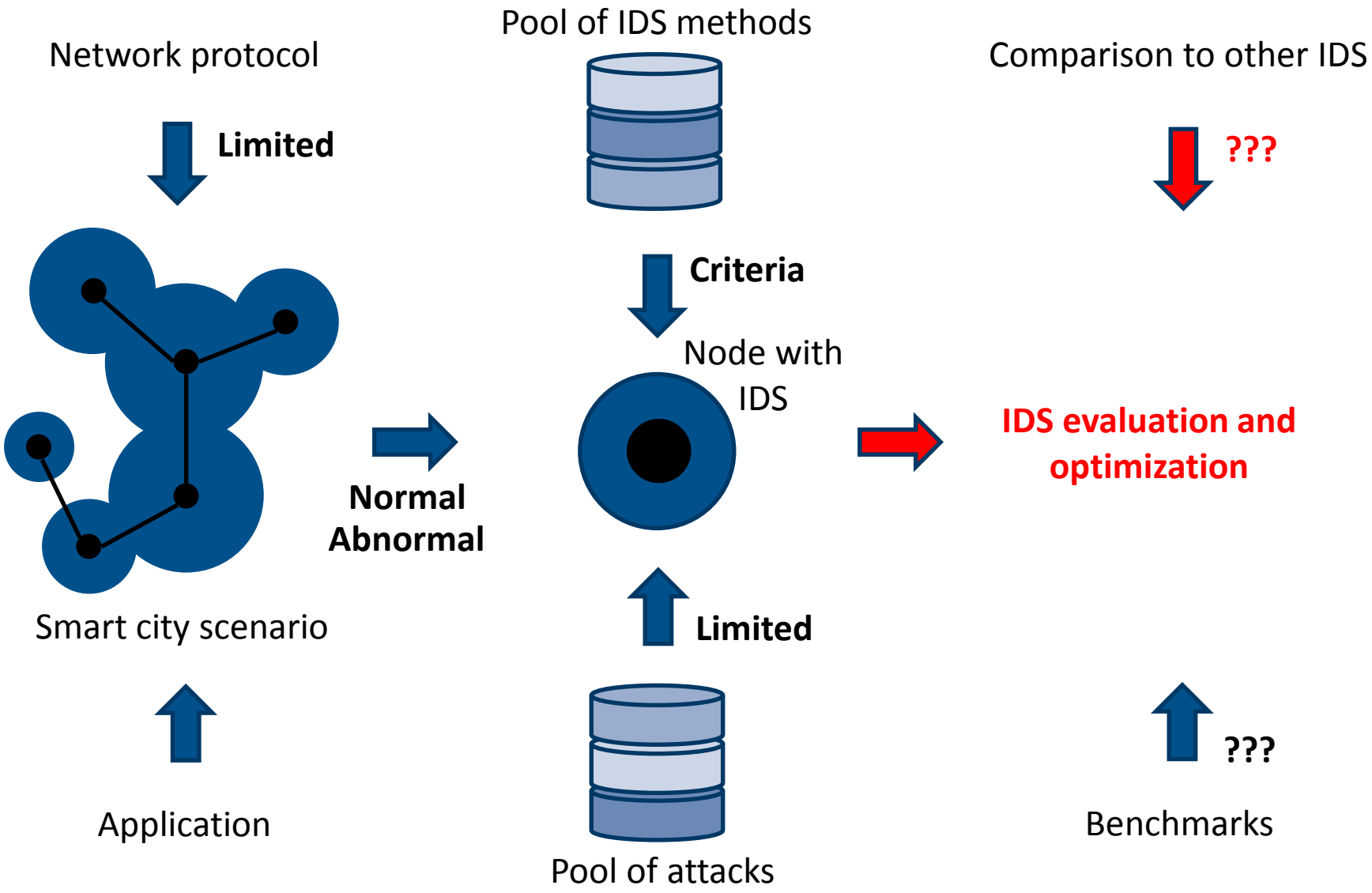
IDS Design and Evaluation



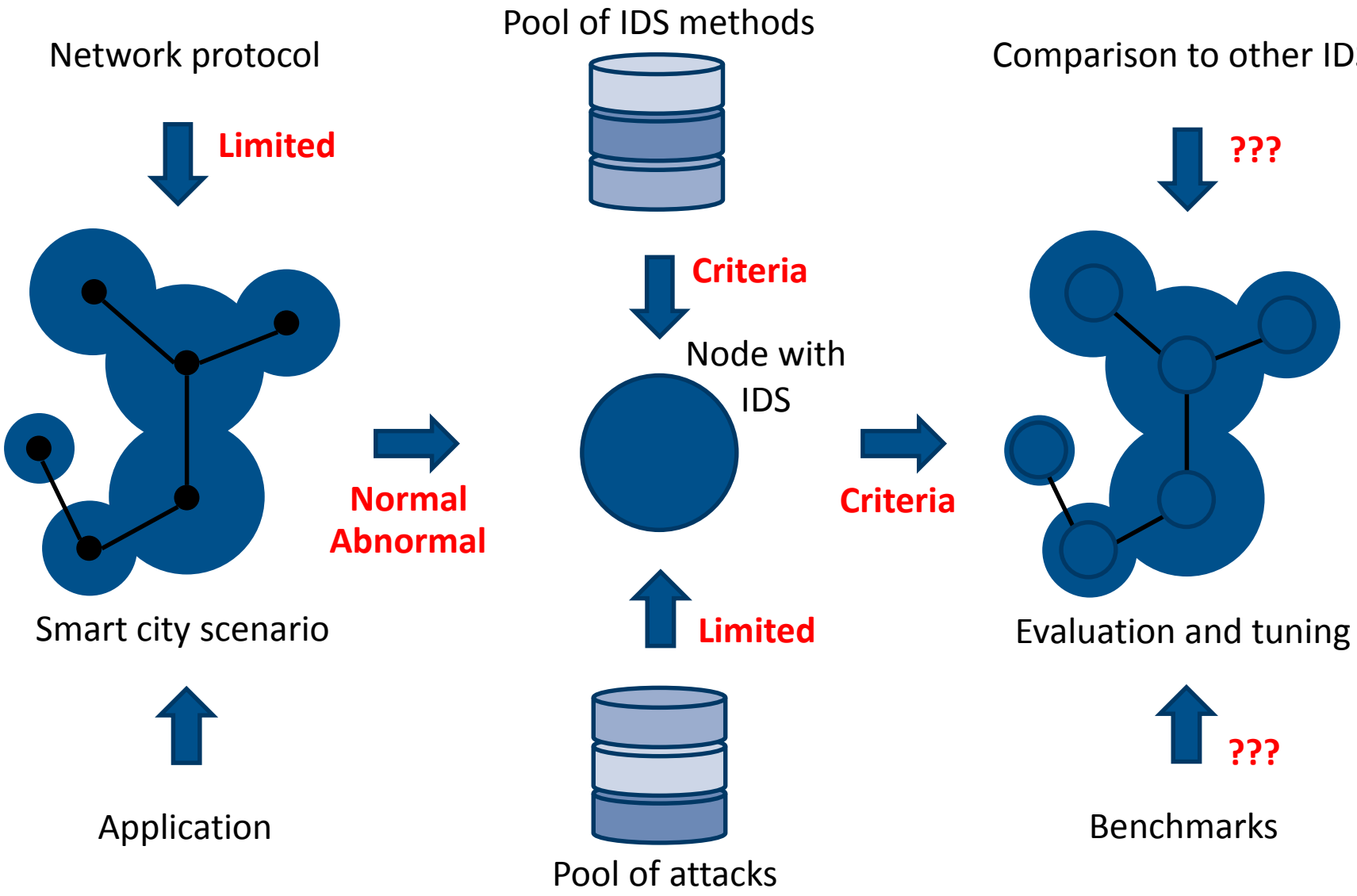
IDS Design and Evaluation



IDS Design and Evaluation

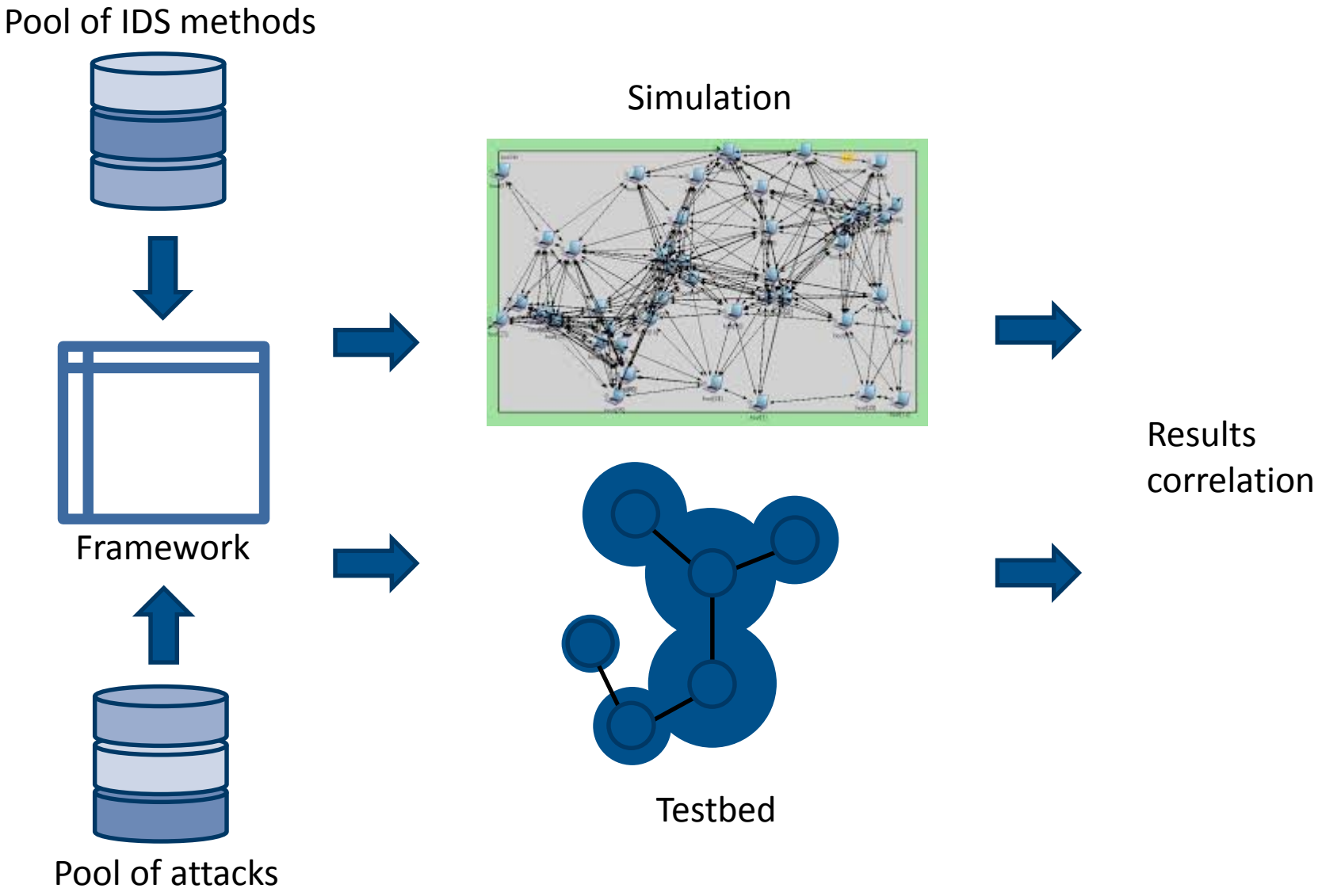


IDS Design and Evaluation

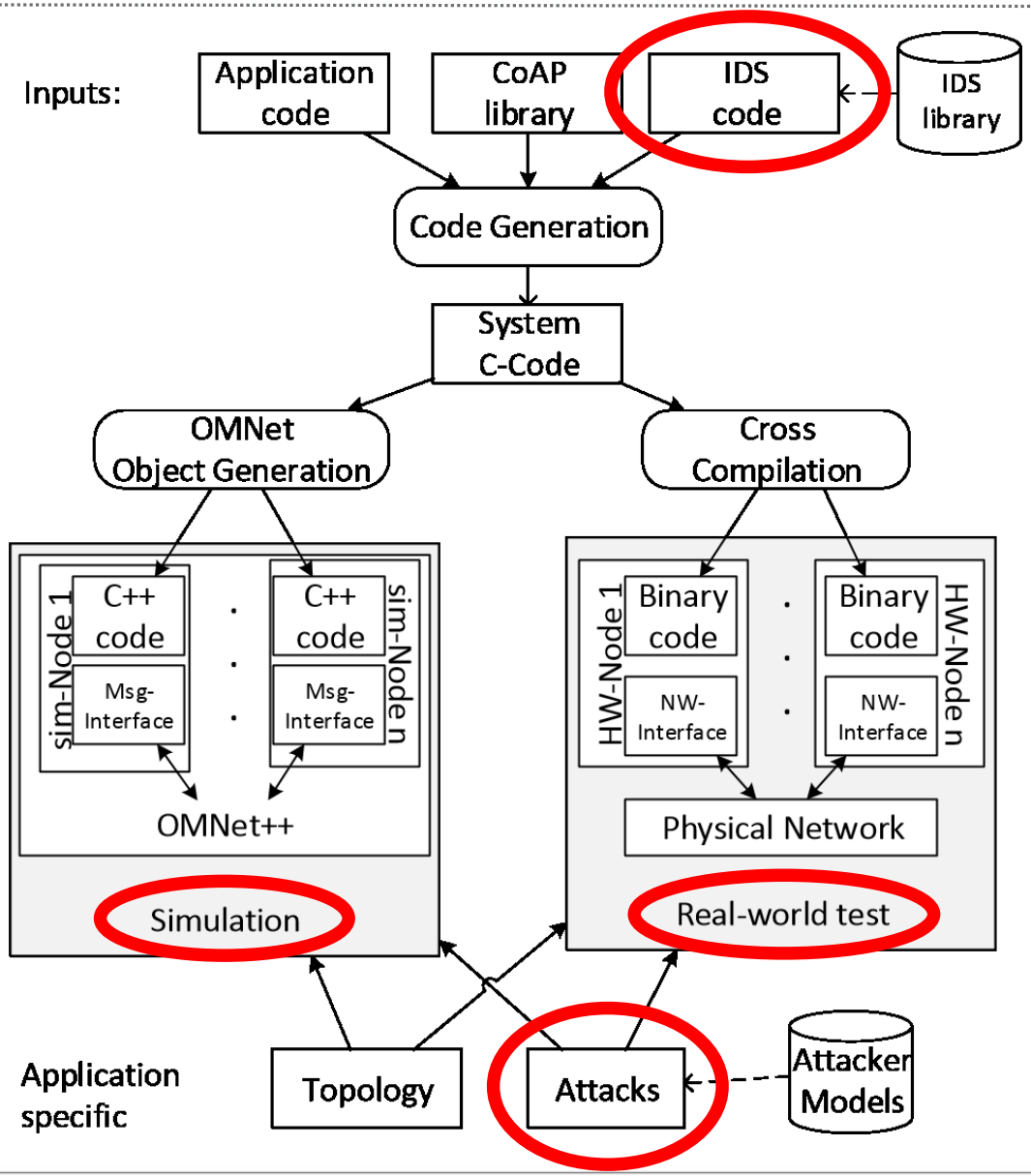


Outline

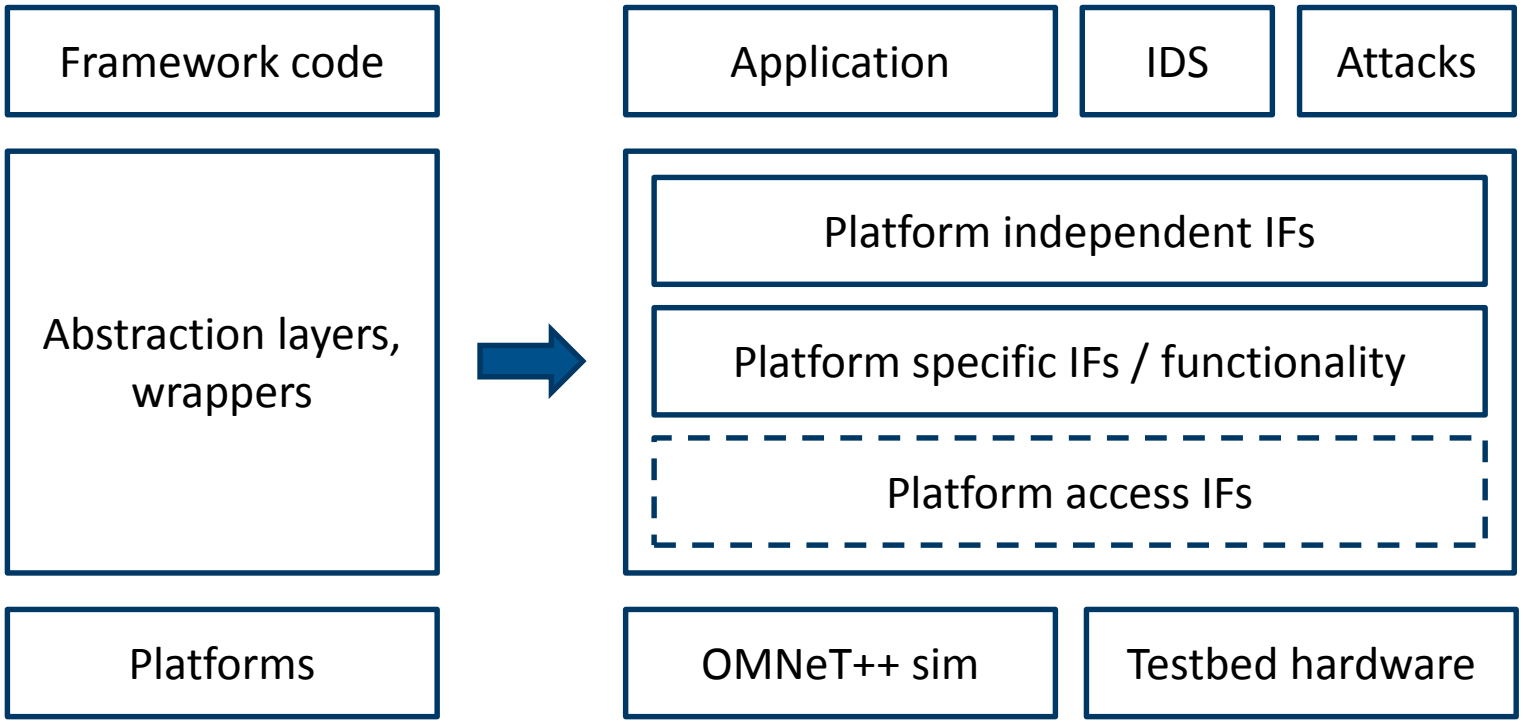
The IDS Evaluation Framework



The IDS Evaluation Framework



The IDS Evaluation Framework

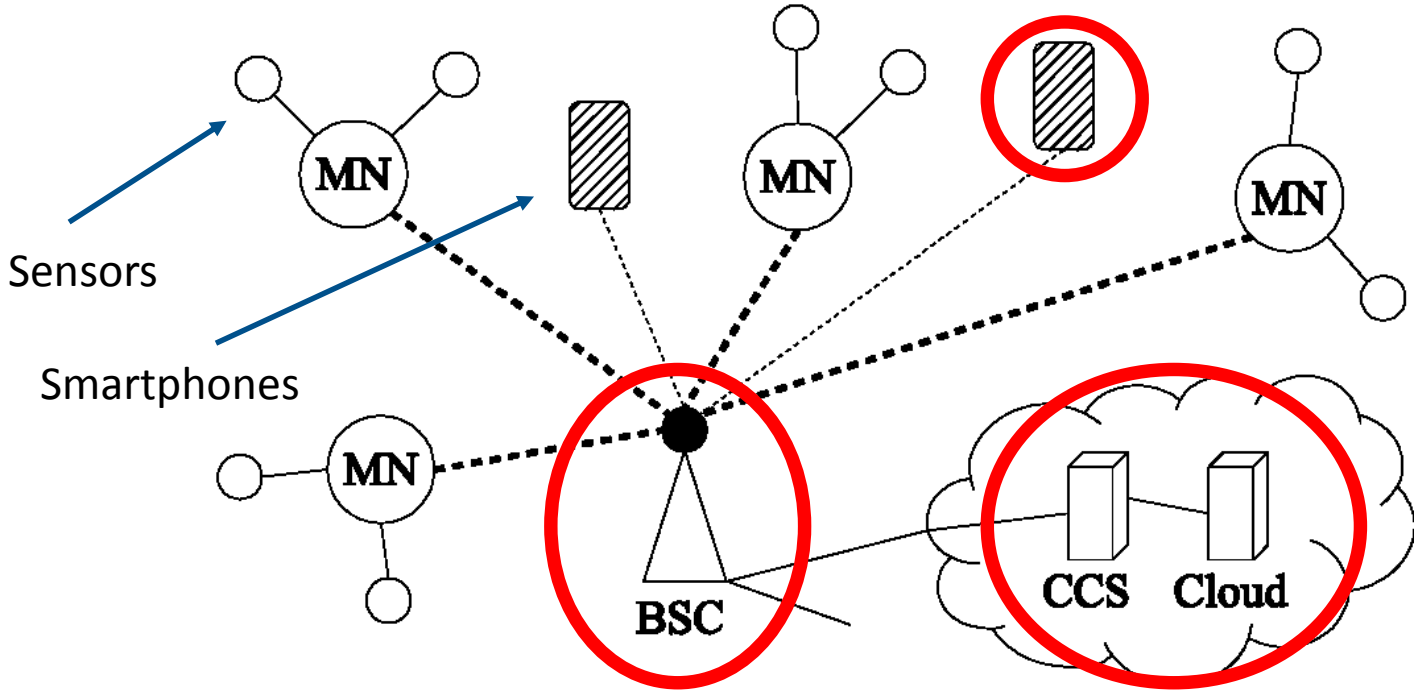


Outline

Public Transport Scenario

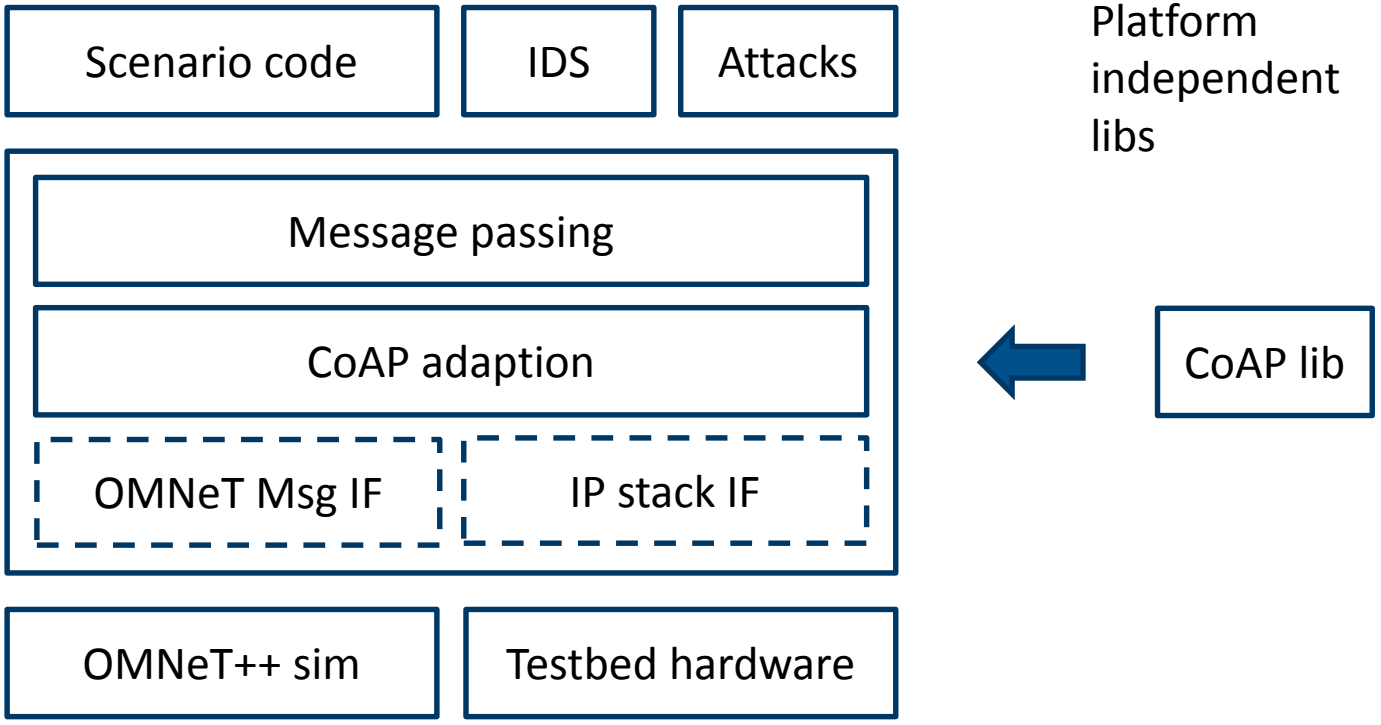
We introduce ...

- A smart application that needs an IDS (critical infrastructure)
- Smart objects on buses collect data for customer services → GPS positions, temperature, humidity, ….
- Customers access services using their smartphones



Outline

Application of the Framework



Application of the Framework

Involves ...

- Restful communication between smart devices and cloud
  - Client / server request / response
  - Use of external protocol lib useful
- Implementation of attacker models
  - Modified messages, malicious devices (sensors, nodes), disturbed communication
  - Jamming, routing attacks, attacks from Internet and customer devices
  - Dependent on protocol and application
- Implementation of intrusion detection methods
  - Rules based approach
  - Cluster algorithm
  - Neural Network

Outline

Results

We found...

- Some IDS methods are application and protocol dependent (i.e. rules)
- We used the presented framework to apply the three mentioned approaches
- We used attacks such as modified messages and malicious devices (sensors, nodes)
- First experiments show that a hybrid approach is a good starting point
  - Rules based / cluster based
  - Rules based / Neural Network

Outline

Conclusion

- Choosing IDS detection algorithm for particular problen is difficult
  - No tools
  - No easy way to compare existing solutions
- We presented a framework for IDS evaluation in Smart Cities using CoAP
  - Uses a hybrid testbed / sim approach
  - Combines simulation with small tested
- Applied our framework to a Smart City problem
  - Public Transport Scenario
  - Found a hybrid IDS approach
- Work to be done
  - Implement detection and attack algorithms further
  - Define IDS‘s more precisely

Thank you for your attention!

Krimmling, Jana

IHP – Innovations for High Performance Microelectronics
Im Technologiepark 25
15236 Frankfurt (Oder)
Germany
Phone: +49 (0) 335 5625 721
Fax: +49 (0) 335 5625 671
Email: krimmling@ihp-microelectronics.com

www.ihp-microelectronics.com

innovations
for high
performance
microelectronics

Member of
Leibniz Association