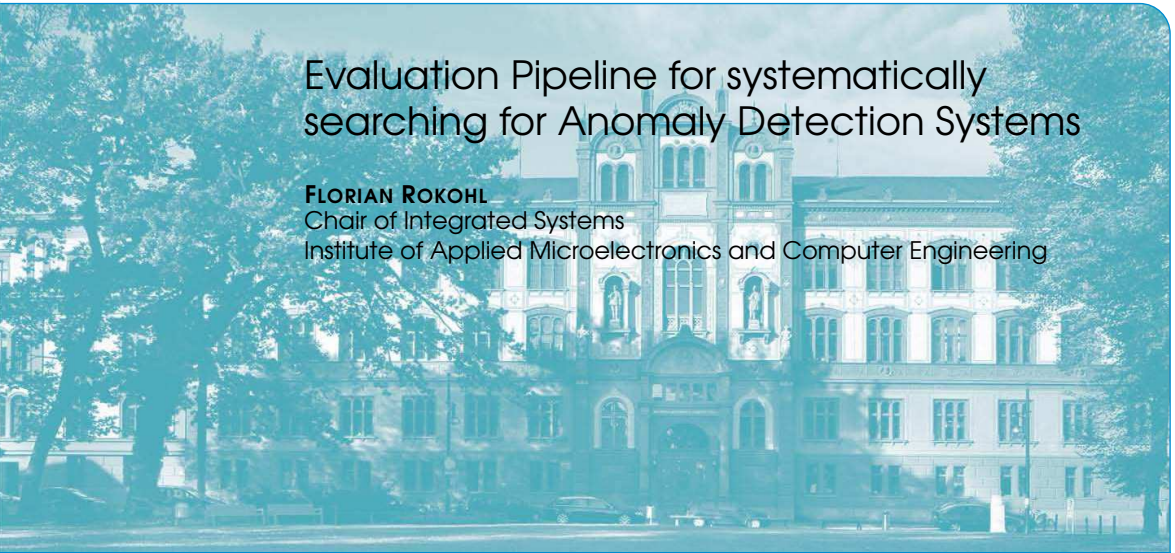

Evaluation Pipeline for systematically searching for Anomaly Detection Systems

Florian Rokohl
Chair of Integrated Systems
Institute of Applied Microelectronics and Computer Engineering

Motivation

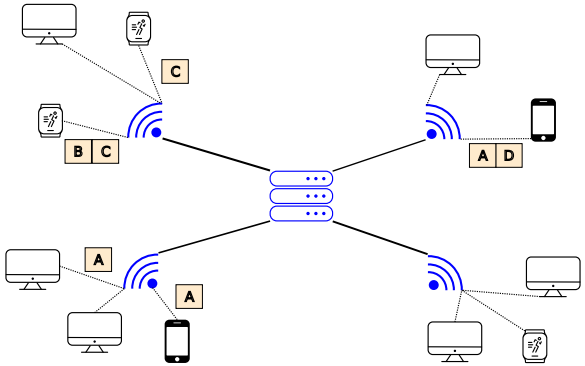

Figure: Example Network

Motivation

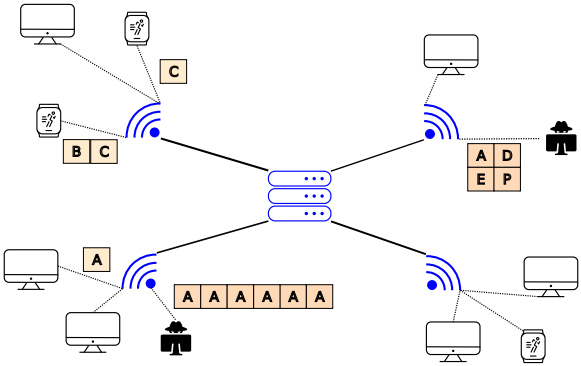

Figure: Example Network

Motivated Questions

1. Which kind of anomalies do we want to detect?
2. How to extract information from the raw network packets?
3. How to evaluate the extracted information?
4. Which hardware technologies and which optimizations should we use?

Problem comparing different approaches

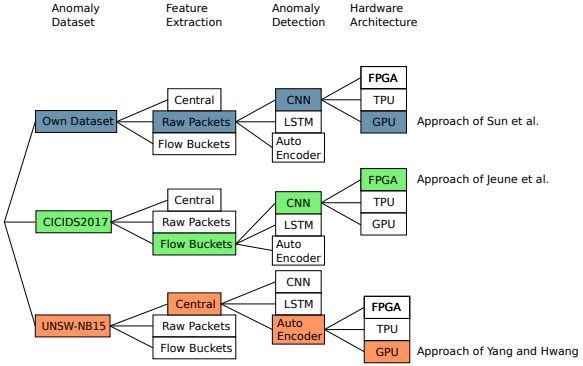

Figure: Design Space Tree

Solution

Hardware Architecture

Figure: Proposed Solution

Solution

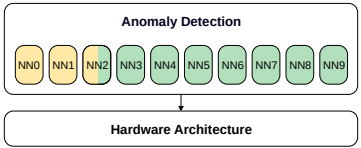

Figure: Proposed Solution

Solution

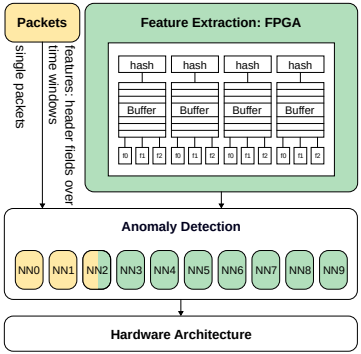

Figure: Proposed Solution

Solution

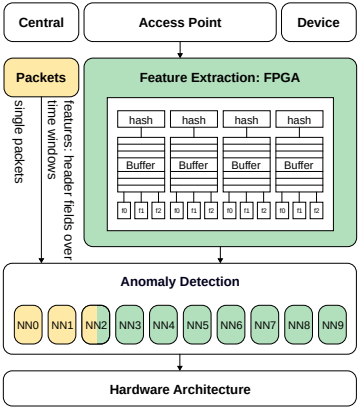

Figure: Proposed Solution

Thank you for your attention and I am open to answering questions!

This research is part of the MedCS.5 project, funded by the BSI.