

Scalable Cyber-Security Analysis for Smart Digital Communities through Multi-Resolution Network Simulation

Carmen Cheh*, Bennet Ng*, and David M. Nicol**

Illinois Advanced Research Center at Singapore Ltd.* , University of Illinois at Urbana-Champaign+

Problem Statement



Introducing security technologies to a system can result in **performance degradation** and **increased attack surfaces**.

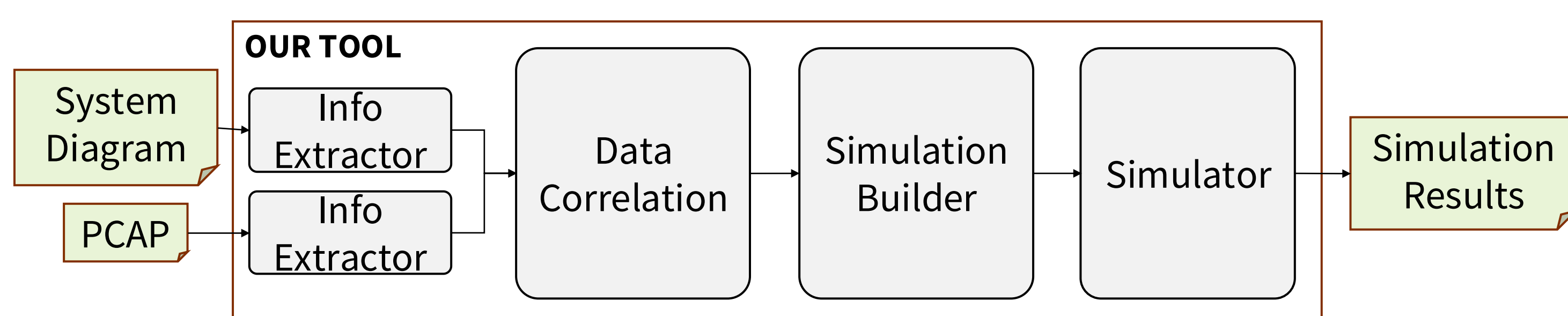


Analyzing the impact of such technologies on the system is **risky, costly, and unscalable**

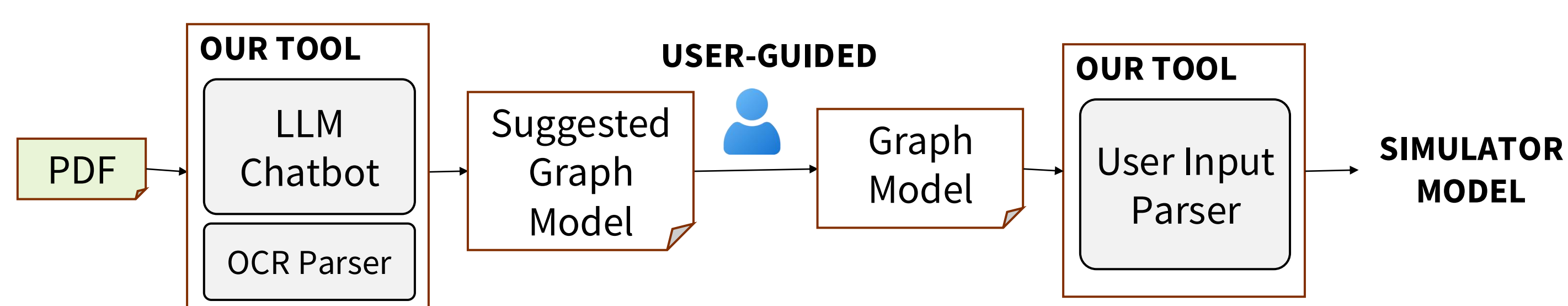
Our Solution

A framework that **automatically ingests system artifacts** to generate a simulation model which can then be **run at scale** to generate a set of **user-defined evaluation metrics** which addresses the following challenges:

- Ingesting system information at a level of granularity that is easy for the user to specify
- Modeling the system using a variety of information at different resolution levels
- Scalable analysis of large systems



Information Extraction – System Diagram



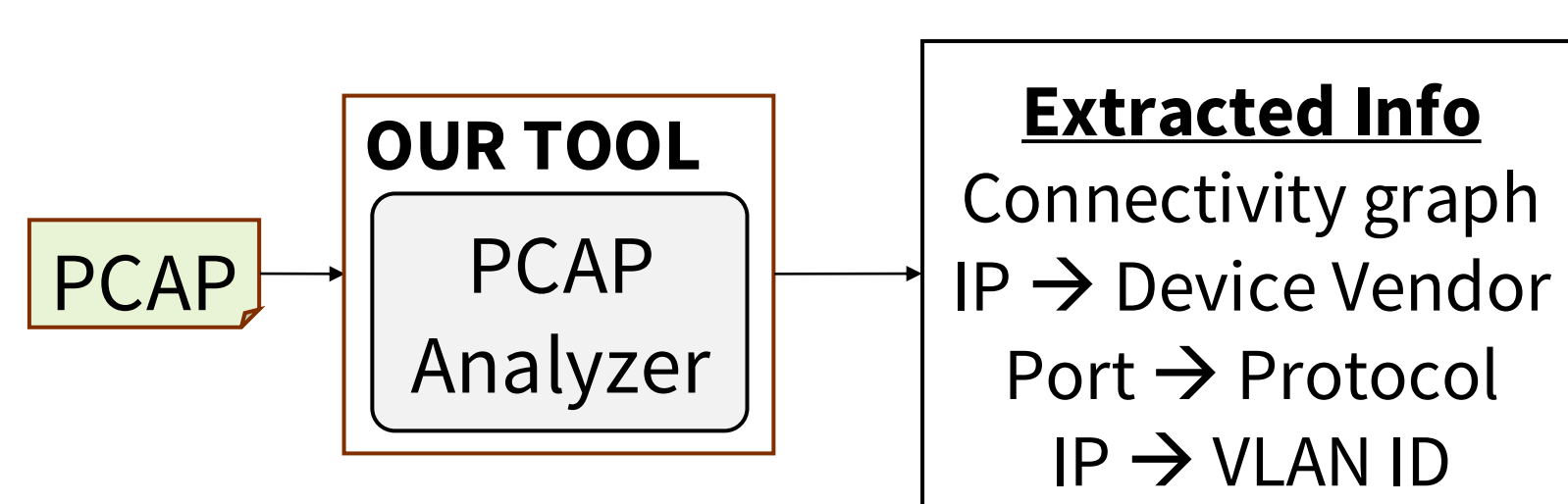
Challenges Faced

- LLMs are not well-versed in calculating layout
- LLM hallucination results in inaccurate parsing

Our Approach

- Combine the accuracy of programmatic solutions with the contextual interpretation of LLMs
- Introduce human-in-the-loop verification to prevent hallucinations

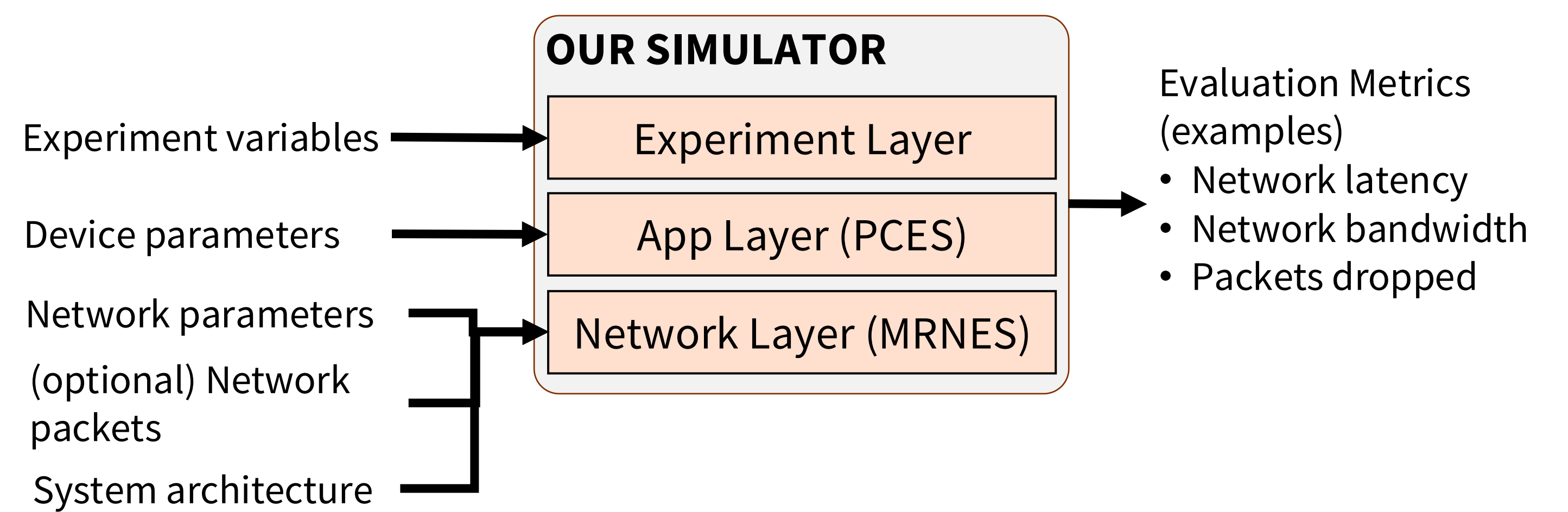
Information Extraction – Network Flows



Challenges Faced

- Network packets do not provide information on system topology
- System misconfigurations and device failures need to be accounted for

Network Emulator/Simulator – MRNES



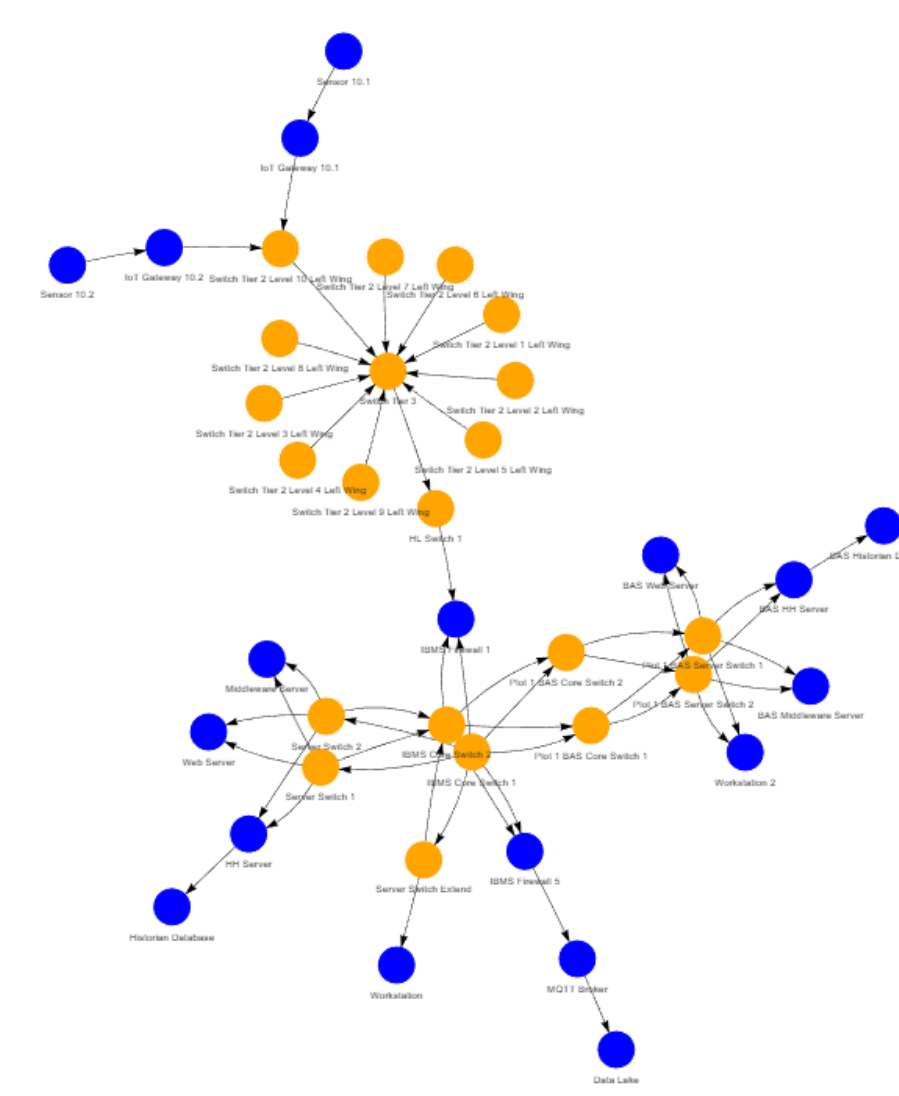
Challenges Faced

- Simulator needs to model a variety of different devices at scale
- Simulator must handle network inputs at different levels of granularity

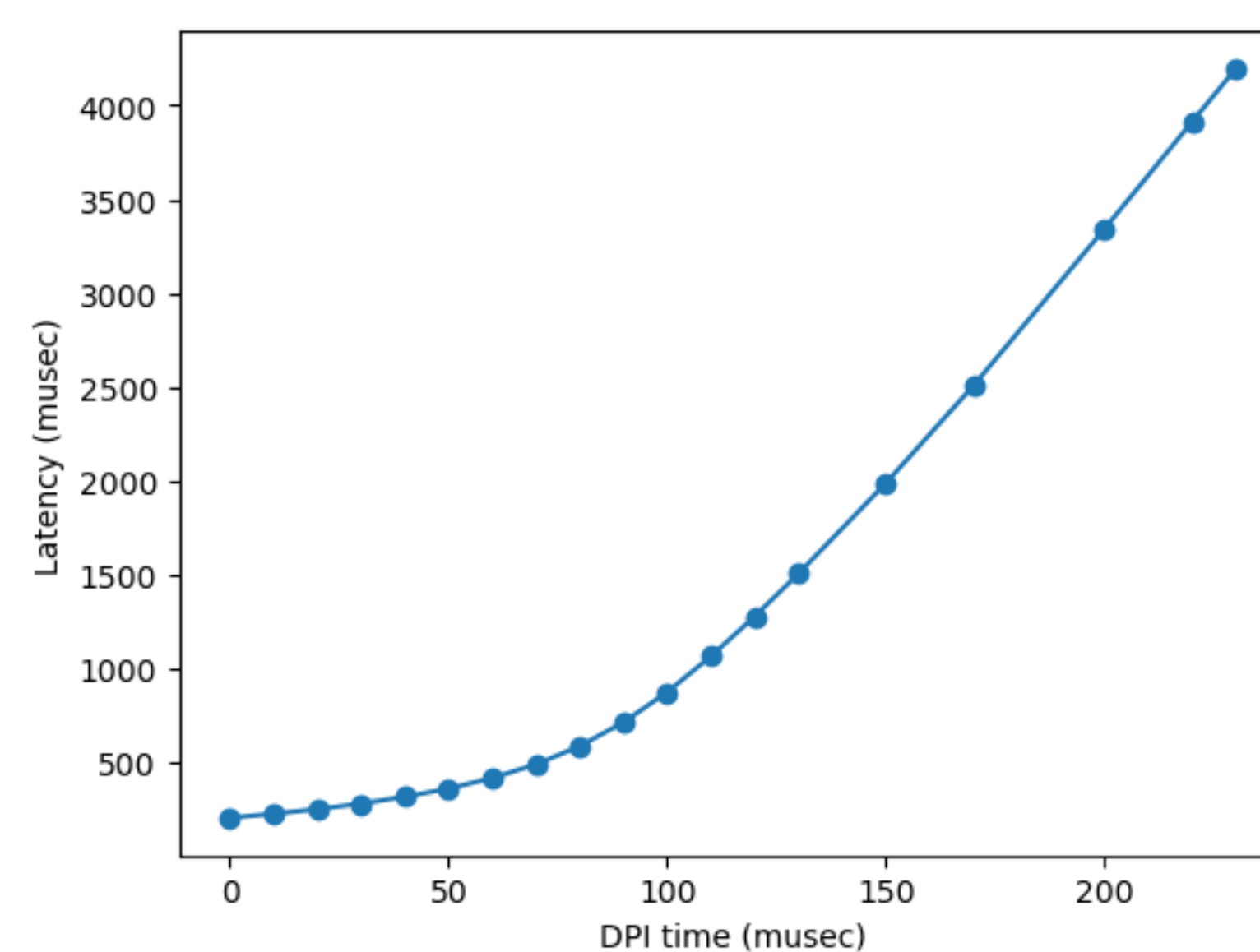
Our Approach

- Formalism that represents reference architectures
- Multi-resolution algorithms, prototypes demonstrating concepts, validation

Case Study – Building Management System



- Focused on IoT subsystem – sensors send data using MQTT protocol to MQTT broker
- Network flows analyses showed instances of
 - Misconfigured IoT gateway sending data to network device
 - Non-communicating IoT gateway
 - Additional port on broker for MQTT communication



Insights

- Processing time of security solution needs to be below 100 μ sec to support system performance
- Intelligent packet filtering needs to be conducted

Conclusion & Future Work

- Our approach to intelligent system modelling allows users to combine information at different levels of granularity for system analyses
- Results from case study show that our simulation approach provides critical insights to guide development of security technologies
- Currently addressing research problems on (1) interpreting diverse representations of system architecture with AI, (2) deriving system context using network packet traces, and (3) simulating diverse device types and attacks.