Reverse Engineering Zigbee Protocol via Machine (Automata) Learning

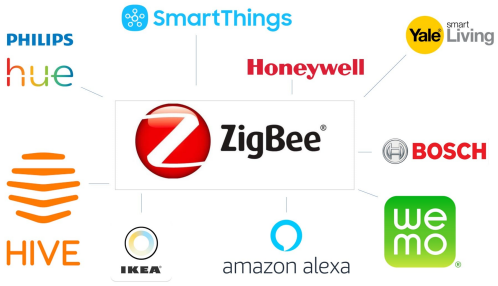
Advisor: **Masoud Ebrahimi**

Motivation

zigbee

Are you interested in IoT attacks?
Together we can do better than attacks!
Let's reverse engineer some IoT devices!

The goal is to reverse engineer zigbee protocol implemented in IoT device(s) and find bugs and flaws.



We have already implemented the Machine Learning algorithms you'll need to reverse engineer zigbee protocol. We also have successfully reverse engineered many systems; e.g. SD-Card Controllers, Intel's TPM, MQTT Brokers, NXP SPI Controllers, and WIFI access points.

SD intel NXP MQTT.ORG Wi Fi

You might ask yourself, if we have the framework and we have already reversed engineer many devices then what is left to do? First, to share the knowledge with you. Next, to implement an interface for zigbee devices in our framework. And finally, to benchmark more devices.

Goals and Tasks

- Learn basics of Automata Learning
- Get used to the existing framework (IAIK brewed)
- Implement an interface to zigbee devices
- Learn different zigbee implementations

Literature

- F. Vaandrager
  Model Learning
  Commun. ACM 2017
- Gutierrez, Jose A. and Callaway, Edgar H. and Barrett, Raymond
  IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks
  IEEE Standards Office, 2003

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Interest in Testing
- Interest in Machine Learning
- Know Mealy Machines
- Fair level of Python and Java

Advisor / Contact

masoud.ebrahimi@iaik.tugraz.at