Similarity Search for Network Traffic Fingerprinting in the Internet of Things (IoT) (Bachelor/Master)

Background

Machine-to-machine communication and the number of Internet-connected devices are growing rapidly. Billions of inexpensive Internet of Things (IoT) devices communicate independently with each other and with servers on the Internet. All kinds of everyday objects in public and private environments, such as street lamps, cameras, sensors, door locks, energy switches and household appliances, are being equipped with modern, mostly wireless communication technologies, providing numerous benefits but also security risks for their consumers. The behavior of these smart objects according to their network communication can provide unique indications of a specific device, security vulnerabilities or abnormal behavior.

Objectives

This thesis focusses on the analysis of similarity search methods for the identification of IoT devices from network traffic. The most popular approaches are based on in-depth packet analysis or feature based ML techniques (e.g. extraction of protocol header characteristics, statistical analysis or service usage and network flows). Nevertheless, ML methods often require huge amount of computational resources and effort for feature engineering. Applying similarity search and pattern recognition algorithms, for example Locality-Sensitive Hashing (LSH), Dynamic Time Warping (DTW) or Principal Component Analysis (PCA), to identify similarities in network traffic flows may be sufficient to identify IoT devices. The main tasks of this thesis are the following:

- Literature review and theoretical evaluation of similarity search methods for network traffic fingerprinting
- Analysis, theoretical investigation and comparison of current solutions
- Practical evaluation of feasible solutions or approaches in consultation with the supervisor
- Documentation and Reporting: Document the research process, experimental setups, findings, and challenges encountered during the work.

Requirements

Candidates should possess basic programming skills (e.g. Python) and have an interest in networking protocols and communication technologies. Familiarity with protocols, network communication architectures, Internet protocols, network security, data science, and machine learning models is advantageous.

Application Process

All applications must be submitted through the application website INTERAMT:
https://www.interamt.de/koop/app/trefferliste?partner=339
(Abschlussarbeiten Bachelor / Master; Pflichtpraktika)
Carefully note the information provided on the site to avoid any issues with your application.
Your application should include

- a short CV
- a current transcript of records
- the keyword "T3-SC-IOT" as a comment

For any questions or further details regarding this thesis and the application process, please feel free to contact ZITiS T3 (t3@zitis.bund.de) or PD Dr. Corinna Schmitt.