Postdoctoral position: Detection of weak signals attack in an IoT network

Global information

- Duration: 24 months
- Start: Fall 2023
- Location: The appointed Postdoc Research Fellow will be hired by ENSTA Bretagne, Brest, France, with shared time on Université Lyon 2, Lyon, France.
- Review of applications will start as soon as possible and continue until May 31, 2023, or until the post is filled, whichever is earlier.

Context

An Internet of Things (IoT) network is a set of interconnected devices that communicate without human interaction. They are one of the main pillars of intelligent technologies. The ubiquity of IoT systems, together with the sensitive information they handle give make them a critical component of our society. A security flaw may impact fields as diverse as defense, environment, health, industry, and even day-to-day management.

There are a large number of IoT protocols to meet all needs, whether it is the communication characteristics (range, consumption, frequency band, etc.) of the communication or the types of data (including the frequency transmission).

MQTT offers a messaging model based on publication/subscription in an extremely light way. A message broker then allows messages to be sent from a source to one or more recipients using specific routings.

In an IoT system, the complexity comes from is the multiplicity of data exchanges. It then requires monitoring and analysis systems – Network Intrusion Detection System – (as opposed to Host Intrusion Detection System). The implementation of such a system has already been studied by some of the project's partners (Laval, 2021).

Objective

This project aims at analysis IoT network exchanges to identify security problems visible in the meta-data of the messages (infractions, inconsistencies…). For this, we integrate three dimensions. The first one, naturally, comes from business domain. The second is linked to the analysis of the IoT network's properties. The third is the methodological aspects that allows to produce necessary software environment, considering constraints from the existing system and its possible evolutions.

Approach

The business domain (first dimension) will be comprised of attack scenarios on IoT networks (at the network level) that will be extracted from datasets.

The network property analysis (second dimension) relies on two complementary scientific works. The first is based on statistical and topological analyses of the IoT network, based on approaches such as graph signal processing (Ortega, 2018) or processing on other structures which can represent IoT networks (Ji, Kahn, & Tay, 2022). These approaches allow to evaluate the global properties of the network from the exchanges and properties of each of its nodes. The challenge remains to determine, thanks to these techniques, a classification of activities as normal or not.

The second work focuses on the recognition of patterns identified as potential security threats. The challenge is then to search for such patterns in the IoT network. Several approaches can be adopted depending on the network modeling choices: graph matching in a graph, or other approaches such as GraphFCA (Ferré & Cellier, 2020) in a knowledge graph or hypergraph. Although promising, these approaches are however thwarted by the nature of the attacks: local monitoring of exchanges does not allow the detection of weak signals, and thus the signature of the attacks. These two works are complementary: one allows a global monitoring of the network while the second seeks to identify potential threats following an alert raised by the first. Thus, the coupling of these two approaches allows an operational monitoring of the network for security purposes.

The agile generation of the software environment will be based on a model-driven software engineering approach. Models capture the domain. These models are then enriched (decorated, completed, associated) on demand, and transformed according to the targeted objectives. One of the main objectives here is to contribute to axis two, with axis one providing validation support. The Agile development logic allows us to guarantee the maintenance in operational condition of the tools, with an easy refactoring either in case of enlargement of the base of axis one, or in case of enrichment of the solutions of axis two. Any regressions generated by these evolutions are detected and removed as soon as possible thanks to the implementation of a test-driven software development policy.

Program

This project runs for 24 months. Its main steps are:

- First dimension: business domain
    - To define an attack dataset
    - To create of a signature for these problems with a focus on weak signals (dilution of requests over time, multiplication of paths, selective loss of packets, etc.);
- Second dimension: graph analysis
    - To study of the state of the art to choose an adequate modeling of the IoT network (graph, knowledge graph, hypergraph);
    - To create a normal activity profile type and search for methods to discover if the activity is compliant or not. In particular, IoT is characterized by intermittent

connectivity, parsimonious communications, etc. which distinguish it from an ordinary network;

- Third dimension: Software environment
    - To model network layers, their representations, and attacks, and to implement a framework for producing tools to identify a threat based on weak signals on the network. These tools could be based on automatic computational approaches.

Candidate profile

The key responsibilities of the Postdoctoral Research Fellow will be to deliver outcomes in a research project and ensure that milestones are met, to work with colleagues and postgraduates within the project covering many areas (graph theory, symbolic artificial intelligence, statistical artificial intelligence, security, software engineering), and to prepare materials for publications in journals and conferences.

The appointed Postdoc Research Fellow will be conjointly supervised by Prof. Loïc Lagadec (ENSTA Bretagne, Lab-STICC Lab) and Prof Jannik Laval (Univ. Lyon2, DISP Lab).

To apply, please send an email to loic.lagadec@ensta-bretagne.fr and jannik.laval@univ-lyon2.fr with a copy of your latest CV.

Bibliography

Ferré, S., & Cellier, P. (2020). Graph-FCA: An extension of formal concept analysis to knowledge graphs. *Discrete Applied Mathematics, Volume 273*, 81-102.

Ji, F., Kahn, G., & Tay, W. P. (2022). Signal Processing on Simplicial Complexes With Vertex Signals. *IEEE Access, Volume 10*, 41889-41901.

Laval, J., Amokrane, N., Thiam Niang, B., Derras, M., Moalla, N. (2023) Data interoperability assessment, case of messaging-based data exchanges. J Softw Evol Proc. 2023;e2538. doi:10.1002/smr.2538.

Ortega, A. a. (2018). Graph signal processing: Overview, challenges, and applications. *Proceedings of the IEEE*, 808-828.