MONITORING IN THE INTERNET OF THINGS

Gabriela Morillo, Utz Roedig, Dirk Pesch
University College Cork

Abstract

IoT systems are used to monitor and control buildings, smart cities, factories, power plants and transport systems. Many IoT applications are considered critical systems, and their secure and reliable operation is essential. For this reason, it is desirable to monitor them.

(i) Generally, IoT monitoring is focused on a particular application such as IDS, performance, asset tracking, etc. This work describes different IoT monitoring applications, explains the underlying systems and discusses commonalities and differences in the variety of IoT monitoring applications.

(ii) Furthermore, we investigate how much information on NB-IoT devices a third party (an observer) can acquire. By observing signal and channel usage characteristics of devices, we want to show that it is possible to identify NB-IoT devices, determine how many devices are deployed in the vicinity of a base station, and perform an IDS attack. We will demonstrate that a third party can gather a detailed understanding of an IoT infrastructure without help from a provider or access to cryptographic keys.

(i) IoT Monitoring Systems

Objectives

- Several systems perform IoT Monitoring, our research aims to identify the common elements between each of these systems.
- Once commonalities are identified, we aim to determine if it is feasible to borrow components from one IoT monitoring system to use in another one in order to build one common IoT monitoring infrastructure.

The Need for Monitoring

- The need for monitoring arises with the real-world demands of people who are already using IoT devices in every aspect of their lives. IoT systems require more than many other IT systems in terms of continuous monitoring as they are very dynamic.
- Moreover, most of the IoT system parameters evolve significantly over the IoT deployment duration. To guarantee the intended system operation, it is necessary to monitor it continuously.
- Our research has described several elements and reasons why IoT systems exhibit such dynamic behaviour:

Lifespan
Coverage
Stakeholders
Mobility
Heterogeneity
RF Environment

IoT Monitoring Systems

IoT systems are very large-scale, and monitoring such installation cannot be human-driven, so automation is required. We categorize the IoT monitoring systems from the perspective of improving security and resilience. We identify the commonalities in five different IoT Monitoring systems:

Intrusion Detection
Asset Monitoring
Authentication
Localisation
Interference Monitoring
Traffic Monitoring

Outcomes

- To identify common elements in multiple systems that have been deployed for various application purposes. We have defined a new *high-level standard classification scheme*. It is based on four categories that can be applied for any of the IoT monitoring applications exposed in this research:
- Generic framework for these monitoring systems that use the same components.

Analysis Method
Performance Metric
Architecture Type
Measurements

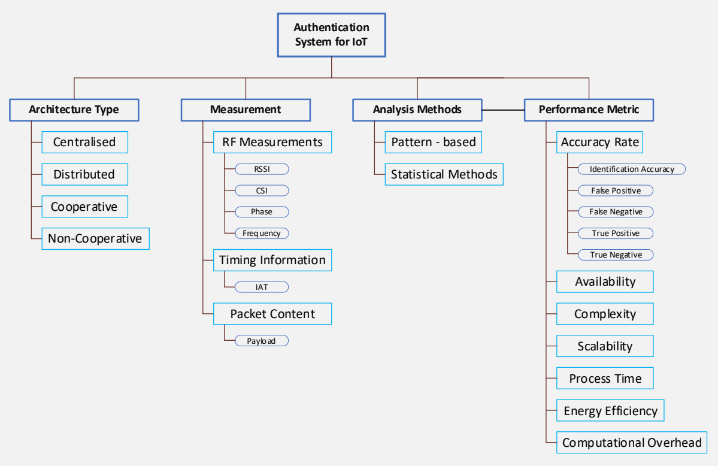


Fig 1. Schematic Overview of the proposed IDS Monitoring Model

(ii) Intrusion Detection in NB-IoT

Objectives

- Investigate signal and channel usage characteristics of UEs to identify NB-IoT devices and determine how many devices are deployed in a base station's vicinity.
- Identify which features can be collected/extracted for Intrusion Detection from an NB-IoT network.
- Design and implementation of an Intrusion Detection System for NB-IoT networks.

Core Research Questions:

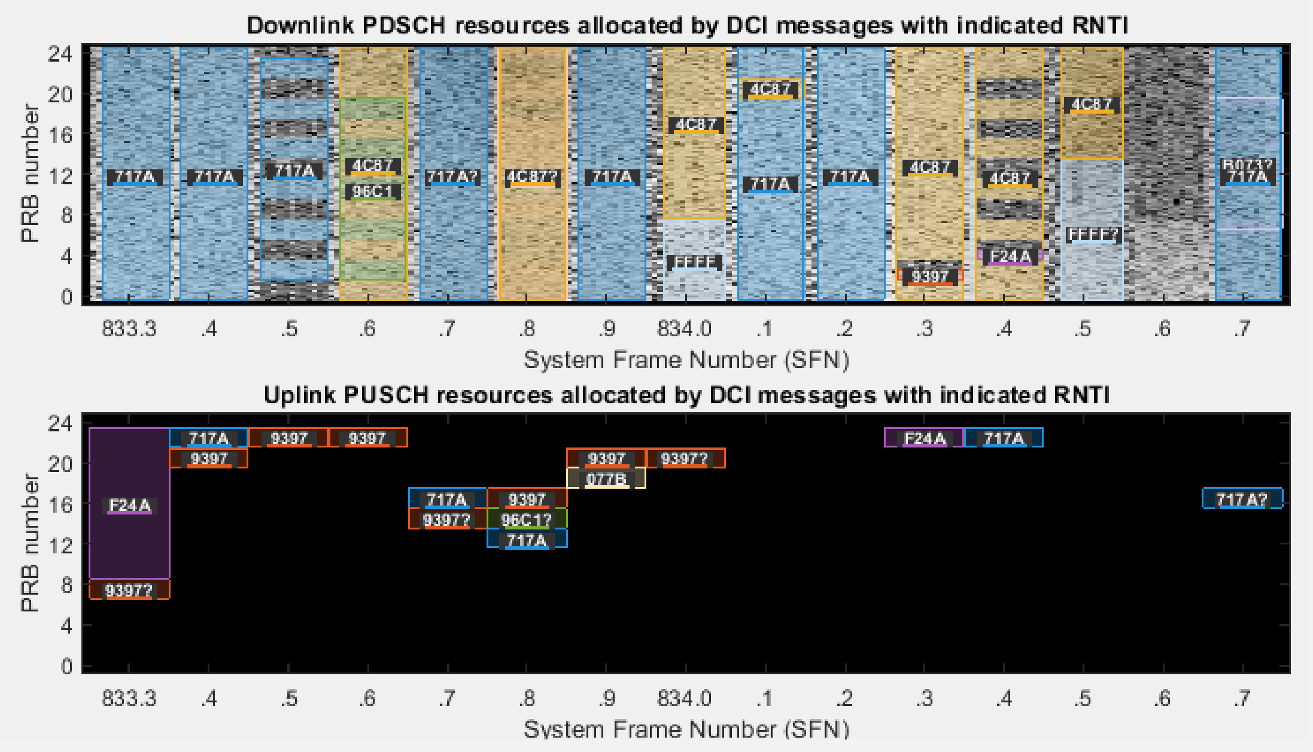
- Which features can we extract.
- Which algorithm should be employed to do IDS.
- What are the attacks that we want to detect with an IDS for NB-IoT.

NB-IoT IDS Structure

Following our previous work, for modelling an Intrusion Detection System for NB-IoT, now we need to define the following elements:

Architecture	• Centralised, overhearing of signals.
Features that can be extracted (Measurements)	The features used from the observation of the channel are: • NPDCCH – Narrowband IoT Physical Downlink Control Channel • DCI – Downlink Control Information • RNTI – Radio Network Temporary Identifier • PDSCH or PUSCH resource block allocations
Analysis Method	Also, it is needed to do some detections. The methods that we will be using are: • Statistical Methods • Pattern Learning
Potential Attacks	Some types of attacks that we want to detect are: • Impersonation attacks based on traffic
Performance Metrics	• Accuracy Detection, Energy Consumption

Experimental Environment

Simulation Environment	• MATLAB R2020b • Product: LTE-Toolbox / NB-IoT and LTE-M
Results Simulation in MATLAB	The simulation results might look like this: 

Expected Outcomes

The expected outcomes will be:

- Software and simulation model for detecting NB-IoT devices.
- Software and simulation model for an Intrusion Detection System in an NB-IoT network.

References

- B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things. Network Computer Appl., vol. 84, no. C, p. 25–37, Apr. 2017.
- O. Faraj, D. Megıas, A.-M. Ahmad, and J. Garcia-Alfaro, "Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things", New York, NY, USA, 2020.
- P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. Navarro-Ortiz, and J. M. Lopez-Soler, "An analytical performance evaluation framework for NB-IoT,"IEEE Internet of Things Journal, vol. 6, no. 4, pp. 7232–7240,2019.

Host Institution