Sustainable Communication Networks
Prof. Dr. Anna Förster

Theft Protection of IoT Devices

Prerequisites:	- Good knowledge of LoRa, sensors and embedded programming (as from Internet of Things Module)
Level:	This topic is appropriate for Master Students
Language:	German or English

Introduction

Very often, IoT devices need to be deployed in publicly available spaces, e.g. to monitor forest fires. Very often, such devices draw the attention of people and sometimes get stolen. This is mostly due to the fact that people do not know what these devices do and believe they do not belong to anybody. If they were to understand better their purpose (fire protection), they will probably leave the devices where they are.
This project targets to implement such a sample system, consisting of several sensor nodes, equipped with temperature sensors to inform about possible fire in the forest. They are all connected via LoRaWAN to a cloud service to report their data. However, they also can recognise a possible theft with their accelerometer data and issue an alarm, such as a visual and/or voice alarm, or a pre-recorded voice message (e.g. "I am helping to protect this forest from fire - please leave me where I am"). Some resilience towards small shakes like from wind should be integrated too.

Project Description

The following steps are recommended:

- Design the complete system with all hardware and software components required. Make a list of required hardware, make sure it is compatible with each other and complete.
- Implement the basic system (fire monitoring), implement recording of accelerometer data on a local SD card with timestamps (real time).
- Deploy the system outdoors for several days, preferably on a tree (make sure you have permission!)
- Gather a dataset from nominal behaviour and from theft attempts (ranging from only small attempts to remove the node to successful removal). Record the ground truth of these events.
- Analyse the data with some simple statistical evaluation to find a threshold to recognise a malicious event.
- Implement the threshold on the sensor nodes (you can now remove the accelerometer data recording part) and the alarms.
- Test the implementation in the wild, make sure to record the malicious test events and how the system reacted. Make a video of some of these events).
- Document all steps and their results.

Contact

If you are interested in this work, please contact us via mail: projects@comnets.uni-bremen.de

February 23, 2022