Sustainable Communication Networks
Prof. Dr. Anna Förster

# A Framework for Sensor Monitoring and Suspicious activities Detection

| | |
|---|---|
| **Prerequisites:** | - Good knowledge of Python and embedded programming<br>- Have experience working with database<br>- Machine learning and deep learning algorithms |
| **Level:** | - This topic is appropriate for Master Students |
| **Language:** | - English |

## Introduction

There is a smart camera that tries to capture images in outside environments. So, it is important to ensure that the camera has a clear view of the proposed area, and if anyone tries to change its angle or breaks it, we have to be informed. This proposal aims to present a project centered around finding an approach to detect suspicious actions against the camera using statistical and machine learning techniques and then triggering alerts.

## Project description

The following tasks need to be executed:

- Step 1: Listing possible suspicious actions that can happen to the camera node and cause the problem in delivering intended pictures :
  - In this step, list several suspicious behaviors, such as changing the camera direction, covering the lens and causing Blurred and unclear images, removing the camera, etc., which cause the camera to operate unreliably or stop working.
- Step 2: Design the complete system with all hardware and software components required:
  - Make a list of the required hardware and design your architecture
- Step 3: Implement the basic system for recording and storing data for several days:
  - In this step, you must gather a dataset from normal behavior and suspicion attempts (based on the list you created in Step 1). Record the ground truth of these events. You need to gather data from different conditions, such as different times of day and crowded/empty places.
- Step 4: Analyse the data with multiple ML algorithms and statistical models to recognize a malicious event to find how you can recognize the malicious event
  - In this step, you have to analyze your images with a statistical modeling approach and ML models to find the normal and abnormal images. The intent of having both statistical and ML models is to see their performance in analysing the images

- Step 5: Implement the detection approach on the sensor nodes and the alarms.
  - In this step, by implementing the model that you find to recognize the suspicious actions on your node and test the implementation in the outside environment, record the malicious test events and how the system reacted. Make a video of some of these events.

- Step 6: Using deep learning approaches to produce synthetic images based on the images that you collected in previous steps :
  - It is important to have more comprehensive datasets from your normal operation of the camera node. So, in this step, you have to augment your data set with synthetic images produced by deep learning approaches like Generative Adversarial Networks (GANs) and then test your model with these synthetic images.

- Step :7 • Document all steps and their results.

## Contact

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

## References