IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future

Project No. 863129

Deliverable D4.5

Laboratory demonstrator of reliable IoT discovery and classification

The IoT4CPS Consortium:

AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

For more information on this document or the IoT4CPS project, please contact:

Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Document Control

Title: Laboratory demonstrator of reliable IoT discovery and classification

Type: Public

Editor(s): Heribert Vallant (JR)

E-mail: heribert.vallant@joanneum.at

Author(s): Bernd Jandl-Scherf (JR), Harald Lernbeiß (JR), Kai Nahrgang (JR), Heribert Vallant (JR)

Doc ID: IoT4CPS-D4.5

Amendment History

Version	Date	Author	Description/Comments
V0.1	20.04.2020	Heribert Vallant	Initial document version prepared
V0.2	12.05.2020	Heribert Vallant	Showcase outlined
V0.3	08.06.2020	Heribert Vallant, Bernhard Jandl-Scherf, Harald Lernbeiß	LoRa setup description
V0.4	22.06.2020	Harald Lernbeiß	Raspberry Pi
V0.5	16.07.2020	Bernhard Jandl-Scherf, Harald Lernbeiß, Kai Nahrgang, Heribert Vallant	LoRa Scanner, initial laboratory set-up
V0.6	29.09.2020	Heribert Vallant, Frank Weber,	Final laboratory set-up, Experimental Results, Conclusion, Executive Summary
V0.7	29.09.2020	Harald Lernbeiß	Internal Review JR
V0.8	09.10.2020	Wolfgang Herzner	Review comments
V0.9	12.10.2020	Heinz Weiskirchner	Review comments
V1.0	16.10.2020	Heribert Vallant	Final Document, addressing review comments

Legal Notices

Content

Abbreviations

GUI	Graphical User Interface
CDPSnarf	Cisco Discovery Protocol Sniffer
HCI	Host Controller Interface
IIoT	Industrial Internet of Things
IoT	Internet of Things
LoRaWAN	Long Range Wide Area Network
MQTT	Message Queuing Telemetry Transport
Nmap	Network mapper
P0f	Passive OS fingerprinting

Executive Summary

This deliverable describes the IoT discovery experiments conducted with a laboratory demonstrator. The system to be analysed outlines a production site that comprises manufacturing machinery, carrier, sensors, and IT infrastructure where the various components communicate via LoRa, Bluetooth, and TCP/IP protocols. A prototypical implementation of the IoT discovery tool developed by JR is used for detection and classification of the assets and for identifying the system's network topology.

1 Introduction

The factories of the future have to cope with the emerging need of an increased uptime of machines, higher performance and flexibility rates, an improved level of productivity, and collective collaboration along the supply chain. To handle this, an efficient interconnection of physical assets and the cyber space is required. With the rapid growth of the Internet of Things (IoT), and its application in industrial areas, the so called Industrial Internet of Things (IIoT)/Industry 4.0 emerged. The benefit of pluggable IIoT components that support and monitor the production site with its machines and other assets comes with the risk of introducing structural security vulnerabilities, though. Each installed IIoT device might open security and safety issues to the whole production facility and must be registered with the asset management system and must be visible for the audit process. Therefore the network's structure as deployed on the spot must be uncovered first to reveal weak spots. As today's networks' complexity is steadily increasing it is crucial to automate this process as much as possible in order to achieve acceptable results with reasonable efforts.

A reliable IoT device classification and network discovery at runtime, that lists all active devices and interconnections in the manufacturing network, is most beneficial to discover vulnerabilities and very useful for an audit process.

This deliverable presents the laboratory setup for IoT discovery and summarizes the approach for a safe and reliable detection and classification of IoT devices and network topologies, which was one of the topics to investigate in IoT4CPS. Chapter 2 describes the automated tool-chain based scanning concept. In chapter 3 the set-up of the laboratory demonstrator is outlined while chapter 4 shows the results of the experiments. Finally chapter 5 summarizes the findings and gives an outlook on future activities.

2 IoT Discovery

Based on the cyber kill chain, which describes the steps an external attacker performs to penetrate a system, network reconnaissance – both external and internal – can be the basis for lateral movement within a network. There are different tools available, which support administrators in performing a network scan or network audit. With the introduction of IoT technology and its topological peculiarities, a concise and up-to-date overview of the network topology is increasingly difficult to achieve. Especially in cyber-physical environments, such as smart factories, obtaining a reliable picture of the network can be a tedious task due to intertwining of a vast amount of devices and different protocols.

In the context of IoT4CPS the IoT discovery is seen as a process to support the asset management and to maintain the identification of different components and therefore credentials or application keys needed for the different scanning modules are provided to obtain the full picture and to maximize the benefit.

2.1 Concept

The concept behind the network reconnaissance procedure is a step-by-step approach enabling a flexible use of different scanner modules and analyzer modules orchestrated according to a chosen policy. While scanner modules gather information about nodes in a network either by observing network traffic or by actively initiating communication, the purpose of analyzer modules is to correlate and to refine the gathered data. The majority of scanner modules delegates the actual work to well-known tools or libraries and implements a wrapper for harmonizing input and output. In that way a huge amount of existing functionality becomes ready for use in IoT discovery. Analyzer modules in contrast are typically tailored to examine a specific aspect of the data gathered by scanner modules or the data pre-processed by other analyzer modules. A policy determines the course of execution of a selection of modules and the arguments to feed to these modules. A typical policy puts so called passive scanner modules in the first phase to observe the network traffic and gather information about nodes in the network. The second phase consists of an analyzer module that processes the results of the passive scanners and determines network ranges that can serve as input for subsequent active scanners which could be used in the third phase. Finally an analytics step tries to assess the network's structure by determining interconnections of nodes, which can involve using traceroute information, gateways or data concentrators, operating system guessing information and looking for usual addresses. All information gathered or created by each module is normalized and stored in a database and can thus serve as a source of information for further analytic steps. Upon completion of a policy’s execution the application user is notified and the discovered network is ready for being visualized as a network graph with options for accessing and editing the data associated with each node, for rearranging the automatic layout of the graph, and for correcting the network structure based on knowledge that is beyond the reach of the automated discovery process.

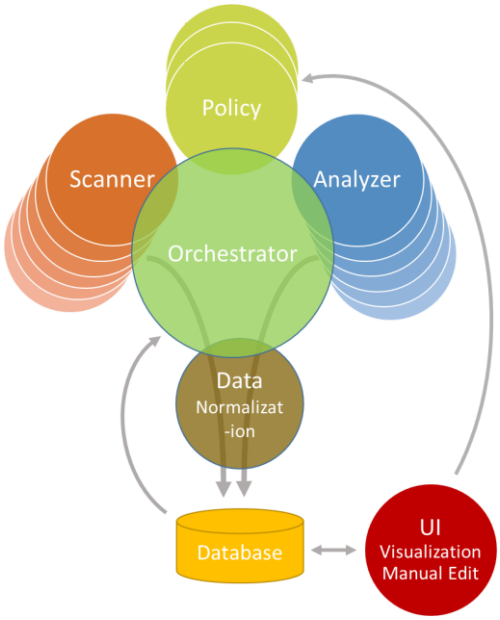

Figure 1: IoT discovery modules and interaction

For the IoT discovery setup a policy handling using LoRa, Bluetooth and Ethernet communication channels was specified and necessary parameters like timeouts but also credentials like LoRa application keys were provided. To ensure a reliable detection of all LoRa messages a packet forwarding of the LoRa base station to the IoT discovery tool was established.

From the architecture perspective the software has the capability to dynamically load scanner modules as plug-ins. As mentioned above most of the scanner plug-ins are implemented as a wrapper around a tool or a library that is developed by some third party completely independent from the IoT discovery tool. The plug-in's responsibility is to map the arguments as stated in the policy to the invocation of the tool / library and to normalize the output for storing results in the database. The following scanning tools have plug-in wrapper implementations and can therefore be used by the IoT discovery tool:

- Nmap - Network Mapper
- P0f Scanner - Passive OS fingerprinting tool
- Netdiscover
- CDPSnarf - Cisco Discovery Protocol Sniffer
- DMitry - Deepmagic Information Gathering Tool
- Snmpwalk
- ZMap

2.2 User interface

The IoT discovery tool comes with a user interface that allows for configuring policies, initiating IoT scans (that is, policy executions), viewing and editing IoT discovery results, and managing the information stored in the database.

Figure 2 shows the dialog that pops up when the user initiates an IoT scan. Some information must be provided by the user before the discovery process can start. The user needs to select a (previously configured) policy, the

network interfaces and the network address to be used, and needs to specify where in the database the results shall be put.

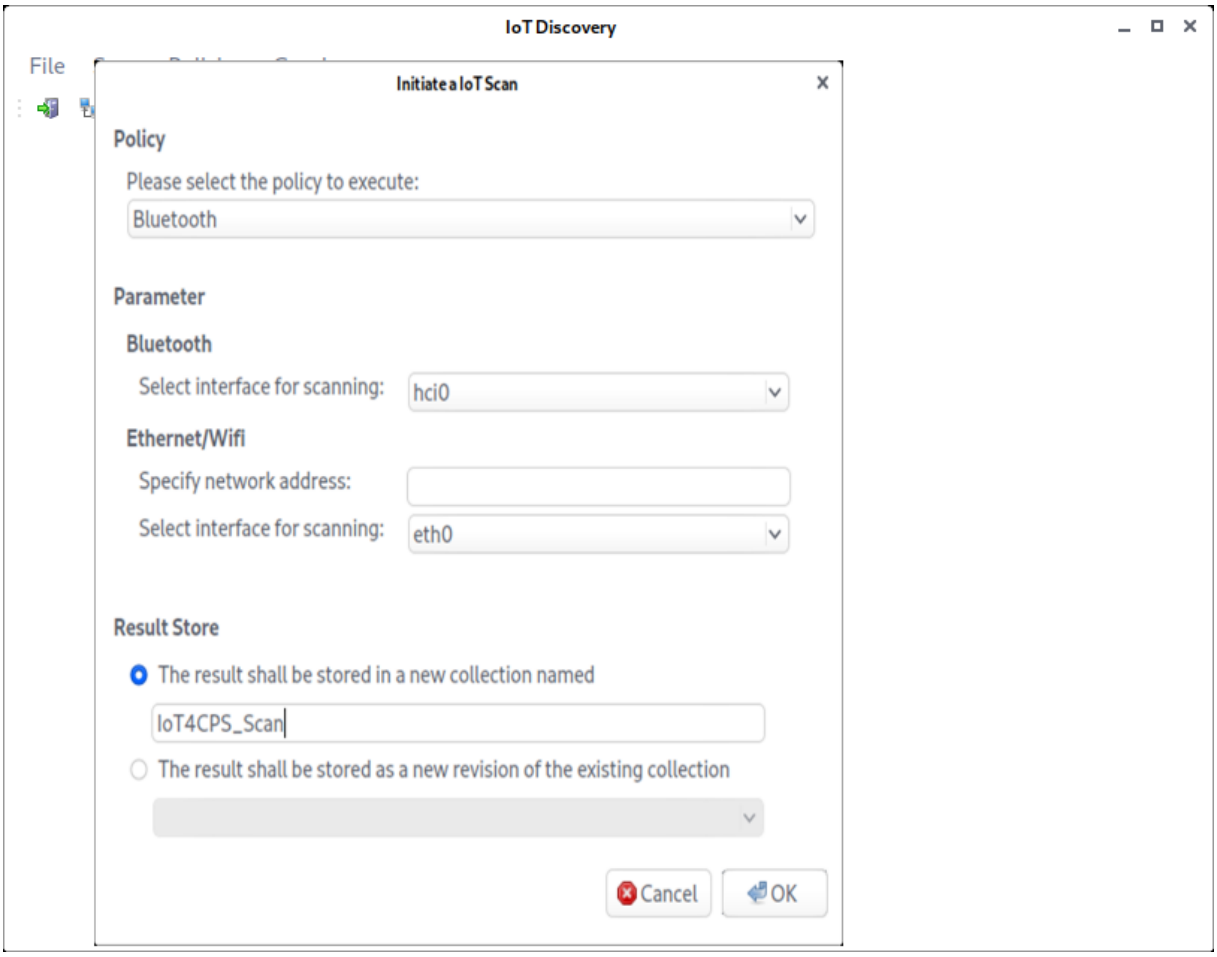

Figure 2 User Interface-IoT scan

3 Laboratory Demonstrator

The laboratory demonstrator reflects a scenario of a manufacturing hall with the production facilities, carriers, sensors for predictive maintenance, and environmental sensors, where all of these are interconnected with different communication modules, transmission channels and protocols.

3.1 Set-up

This section outlines the setup of the laboratory demonstrator and the components used to imitate an industrial environment setup. Figure 3 shows that setup with following components in place:

1. Manufacturing facility
2. Condition monitoring system
3. Carrier
4. Surveillance Camera
5. Environmental monitoring - Temperature
6. Environmental monitoring - Lighting
7. Environmental monitoring - Humidity

8. LoRa base station (data concentrator)
9. LoRaWAN network/application server
10. IPv6/Ipv4 Router/Switch
11. Cell phone
12. IoT Discovery tool

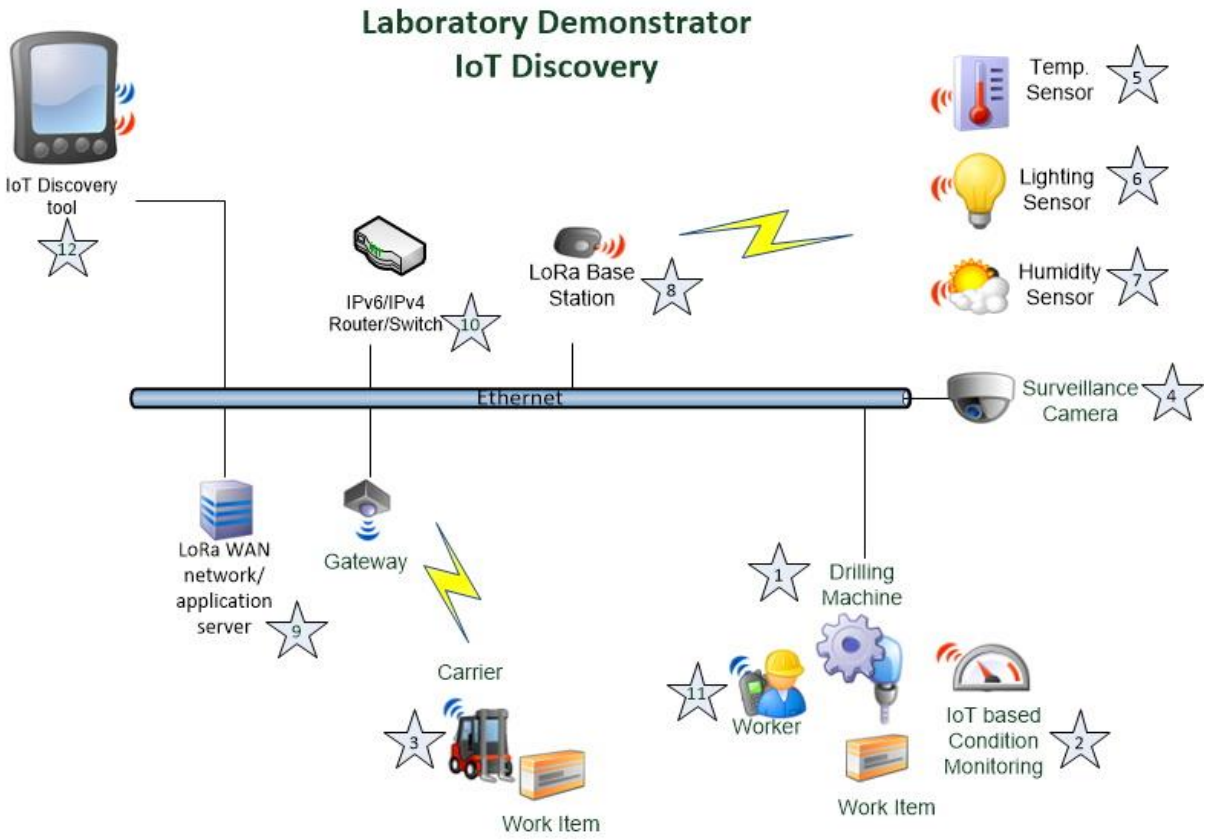

Figure 3 Setup of the laboratory demonstrator for IoT discovery

3.2 Details of the Hardware in use

1. Manufacturing facility:

   3 Axis CNC wood milling machine which executes the g-code, control software: Grbl Control; interface: USB, OS: Windows 10.
2. Condition monitoring system:

   HELTEC, Lexin ESP32 and Tensilica LX6 Dual Core APU Processor with 240 MHz;

   LoRa sx1276 chip with 868 MHz band; 2.4 cm blue OLED display, USB to UART Bridge CP2102;

   Vibration and noise sensor
3. Carrier

   Lego Mindstorms with Bluetooth communication
4. Surveillance Camera:

   IP Camera, resolution 2.5 MP

5. Environmental monitoring – Temperature/Humidity
   Dragino LHT65 LoRaWAN Temperature & Humidity Sensor with Temp. Probe
6. Environmental monitoring - Lighting
   HELTEC, Lexin ESP32 and Tensilica LX6 Dual Core APU Processor with 240 MHz; LoRa sx1276 chip with 868 MHz band; 2.4 cm blue OLED display, USB to UART Bridge CP2102
   Light sensor module, brightness sensor with digital output
7. Environmental monitoring - Humidity
   HELTEC, Lexin ESP32 and Tensilica LX6 Dual Core APU Processor with 240 MHz; LoRa sx1276 chip with 868 MHz band; 2.4 cm blue OLED display, USB to UART Bridge CP2102
   DHT22 Temperatur Humidity sensor with digital output
8. Lora base station (data concentrator)
   LG308 LoRaWAN Gateway with SX1301 LoRa concentrator providing 10 programmable parallel demodulation paths and two SX1257 LoRa transceivers
9. LoRaWAN network/application server
   Raspberry Pi 4 Model B; 4 GB, ARM-Cortex-A72 4 x, 1.50 GHz, 4 GB RAM
   Linux OS, Mosquitto MQTT broker, ChirpStack network / application server and dependencies (PostgreSQL database, Redis database)
10. IPv6/Ipv4 Router/Switch
    Cisco Catalyst
11. Cell phone
    Cell phone of the worker at the manufacturing environment
12. IoT Discovery tool
    Raspberry Pi 4 Model B; 4 GB, ARM-Cortex-A72 4 x, 1.50 GHz, 4 GB RAM
    Kali Linux OS, MongoDB database

3.3 Implementation

Figure 4 reflects the setup of the IoT Discovery demonstrator with the different components.

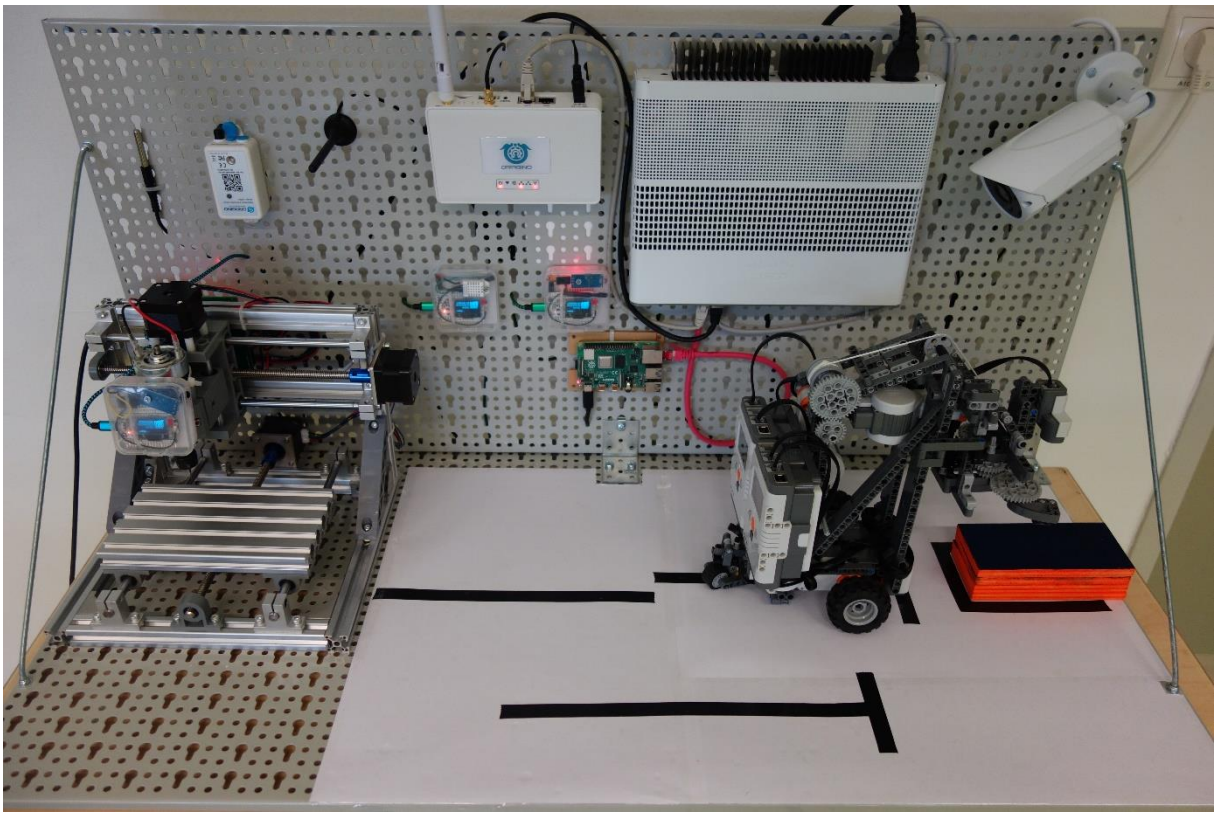

Figure 4 setup IoT Discovery demonstrator

4 Experimental Results

The output of the IoT discovery process is a network graph displaying the identified node and edge objects of the underlying network topology. As was to be expected from the specification of the laboratory demonstrator the following network topology was discovered

- LoRa:
  - Base station: fdcfcf27, 192.168.0.2
  - Sensor nodes: fdcfcd3c, fdcfcc65, fdcfcc2e, fdcfcc19
- Bluetooth
  - Carrier: 00:16:53:0B:1A:85, Fahrwerk; 00:16:53:0B:9F:55, Greifarm
  - Cell phone: 40:B0:76:13:E3:71, ASUS_X00TD, Smart phone
- LAN
  - IPv4
    - Manufacturing facility; 192.168.0.13
    - Camera: 192.168.0.10
    - LoraWAN network / application server: 192.168.0.4
    - Router: 192.168.0.1
    - LoRa Data Concentrator: 192.168.0.2

Figure 5 shows a screenshot of the network graph generated from the data collected by the IoT discovery tool. The numbers reflect the mappimg to the laboratory setup according to the numbering in Figure 3.

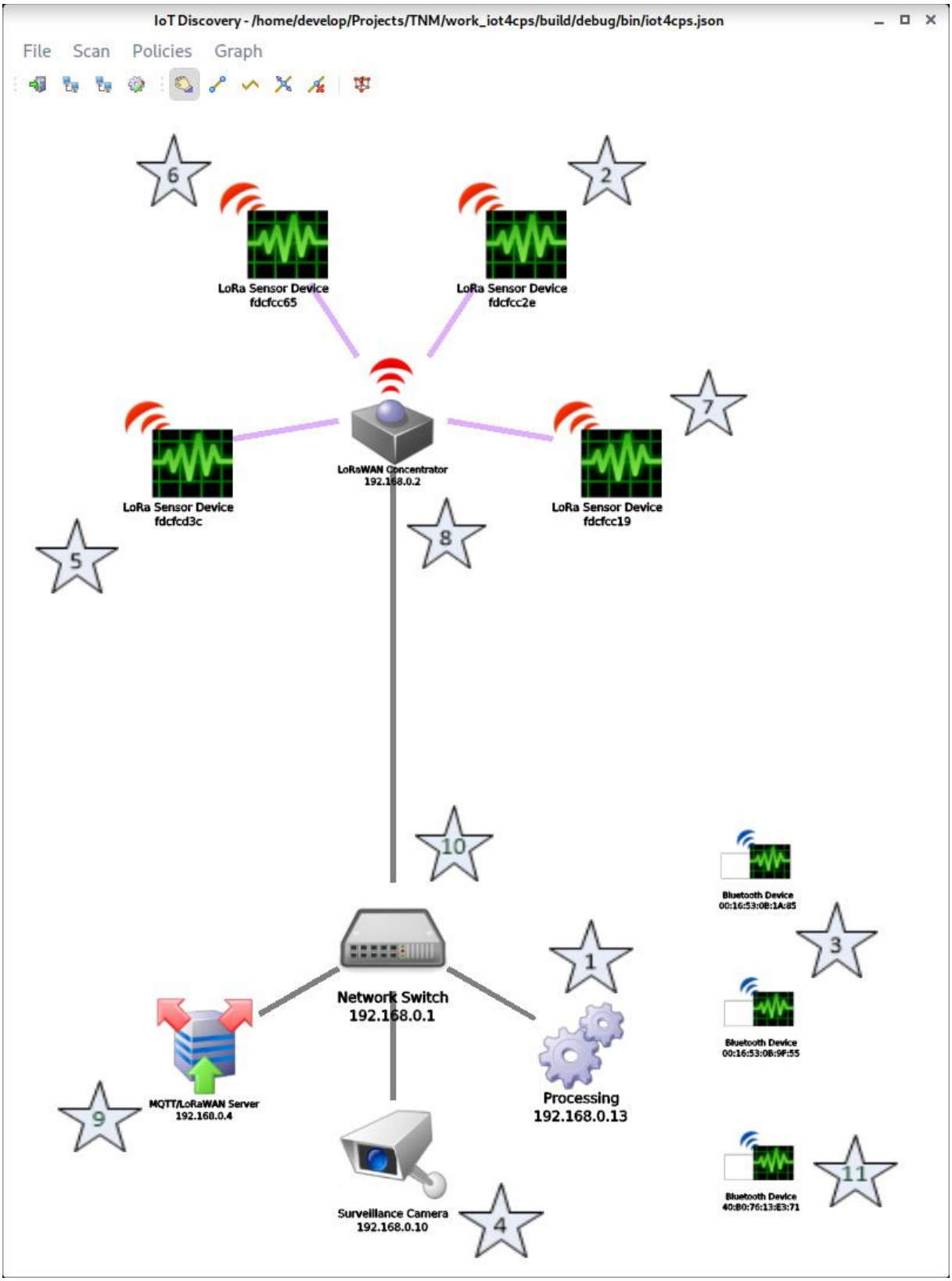

Figure 5 Resulting topology graph of the IoT scan

5 Conclusion

The work outlined in this deliverable shows that automated network mapping of a production site can contribute to obtain an authentic view of the actual network structure and connected equipment at any time. Up-to-date reports on the network topology help in administrating cyber-physical systems and provide the responsible CISO with the opportunity to easily check how the results align with the intended structure, which is very beneficial for an audit process.

At the moment the IoT Discovery tool supports setups with Ethernet (IPv4 and IPv6), LoRa, and Bluetooth based communication by default, but due to its flexible architecture additional scanner and analyzer modules can be added very easily. We expect that scanners with support for other IoT related communication protocols that are relevant in an industrial environment as well as more analyzers for investigating further security related aspects will be added in the near future.

6 References

1. Marksteiner, S., Lernbeiß, H. & Jandl-Scherf, B. (2016). An Iterative and Toolchain-Based Approach to Automate Scanning and Mapping Computer Networks. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'16) (S.37-43). ACM. ISBN: 978-1-4503-4566-8. DOI: 10.1145/2994475.2994479.
2. Marksteiner, S., Lernbeiß, H. & Jandl-Scherf, B. (2019) Automatically Determining a Network Reconnaissance Scope Using Passive Scanning Techniques. In Fourth International Congress on Information and Communication Technology, ICICT 2019, London, Volume 2 (S.117-127). Springer ISBN 978-981-32-9342-7. DOI 10.1007/978-981-32-9343-4