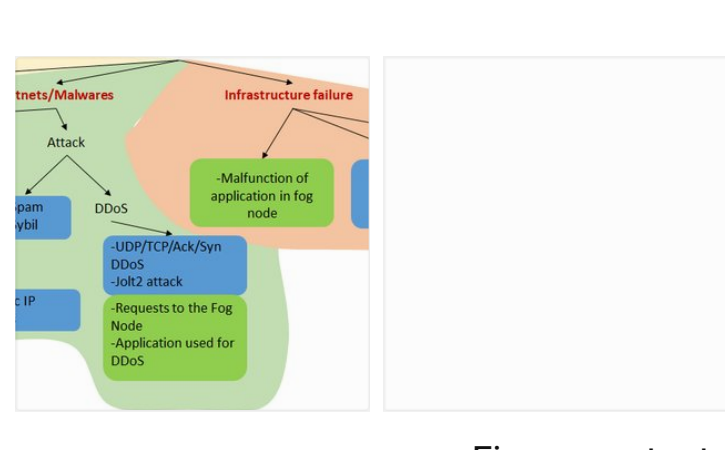
Improve cybersecurity of C ITS Road Side Infrastructure Installations: the SerIoT Secure and Safe IoT approach

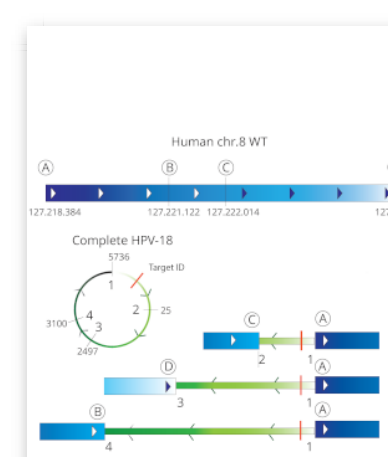
August 2019
DOI: 10.1109/ICCVE45908.2019.8965056
Conference: IEEE ICCVE 2019 · At: Graz, Austria
Project: SerIoT - Secure and Safe Internet of Things

Alexander Frötscher · Bernhard Monschiebl · Anastasios Drosou · Show all 5 authors · Martin J Reed

Abstract and figures

Cooperative Intelligent Transport Systems (C-ITS) need to be secured as it is deployed on roads in Europe. While some aspects of the communication security are secured others could still need improvement. SerIoT as a security project for the internet of things and offers various security mechanisms from the IoT domain which could be beneficial for C-ITS. Such security mechanisms contain a software defined network, the usage of honeypots and several mechanisms to analyze, monitor and mitigate threats on the system. Therefore C-ITS will benefit tremendously of the functionalities from these security mechanisms designed to cope with large attack surfaces and high network traffic found in IoT environments. To enable these technologies, modules developed within SerIoT are planned to be integrated into the Road Side ITS station. The station will also be connected to SerIoT SDN routers providing security for the station from malicious vehicles and the network





Improve cybersecurity of C-ITS Road Side Infrastructure Installations: the SerIoT – Secure and Safe IoT approach

Alexander Frötscher
Technologies and Services for Mobility
Austriatech GmbH.
Vienna, Austria
alexander.foetscher@austriatech.at

Bernhard Monschiebl
Technologies and Services for Mobility
Austriatech GmbH.
Vienna, Austria
bernhard.monschiebl@austriatech.at

Anastasios Drosou
Information Technologies Institute
Centre for Reasearch & Technology Hellas
Thessaloniki, Greece
drosou@iti.gr

Erol Gelenbe
Institute of Theoretical and Applied Informatics
Polish Academy of Sciences
Gliwice, Poland
e.gelenbe@imperial.ac.uk

Martin J.Reed
School of Computer Science and Electronic Engineering
University of Essex
Essex, United Kingdom
mjreed@essex.ac.uk

Mays Al-Naday
School of Computer Science and Electronic Engineering
University of Essex
Essex, United Kingdom
mfhaln@essex.ac.uk

***Abstract*— Cooperative Intelligent Transport Systems (C-ITS) need to be secured as it is deployed on roads in Europe. While some aspects of the communication security are secured others could still need improvement. SerIoT as a security project for the internet of things and offers various security mechanisms from the IoT domain which could be beneficial for C-ITS. Such security mechanisms contain a software defined network, the usage of honeypots and several mechanisms to analyze, monitor and mitigate threats on the system. Therefore C-ITS will benefit tremendously of the functionalities from these security mechanisms designed to cope with large attack surfaces and high network traffic found in IoT environments. To enable these technologies, modules developed within SerIoT are planned to be integrated into the Road Side ITS station. The station will also be connected to SerIoT SDN routers providing security for the station from malicious vehicles and the network**

Keywords— C-ITS, Cyber Security, IoT Technologies

I. Introduction (*Heading 1*)

Cooperative Intelligent Transport Systems (C-ITS) are currently deployed all over Europe. This development allows for the first time that V2I, and V2V communication is operational within Europe on large scale. Several countries (e.g. Austria, Germany, France, Slovenia or the Czech Republic) are in the process of rolling out ITS G5 capable roadside stations along major motorways with large deployment projects or public procurement tenders. This will allow road infrastructure operators to generate and send relevant traffic information with high accuracy and timely directly into vehicles, which will receive this information through their build in C-ITS stations. Since no communication technology is prone against security attacks and C-ITS is no exception, measures need to be taken to mitigate those attacks. Aspects of communication security between road side C-ITS stations and vehicles are defined for Europe in two documents called the Certificate policy for Cooperative Intelligent Transport Systems in Europe [1] and the Security Policy and Governance Framework for C-ITS in Europe [2].

II. SerIoT overview

Secure and Safe Internet of Things (SerIoT) is a Horizon 2020 Project within the EU aiming to develop a secure Internet of Things (IoT). To achieve this several partners from different fields have joined together to provide a combination of technologies which are software defined networks, fog computing, honeypots, monitoring and mitigation mechanisms and a policy based framework. This combination can secure existing and newly developed IoT Systems in the areas of Smart City, logistics, flexible manufacturing and surveillance. Within those areas several scenarios are worked on which were deemed to be the most important from the several end user partners. In the Smart Cities area for example especially 3 scenarios are important which are securing of sensors within public transport vehicles, mechanisms to secure automated driving communication and within C-ITS Security monitoring and mitigation of attacks on Road Side ITS stations. SerIoT aims to provide a scale able solution for all the different IoT systems.

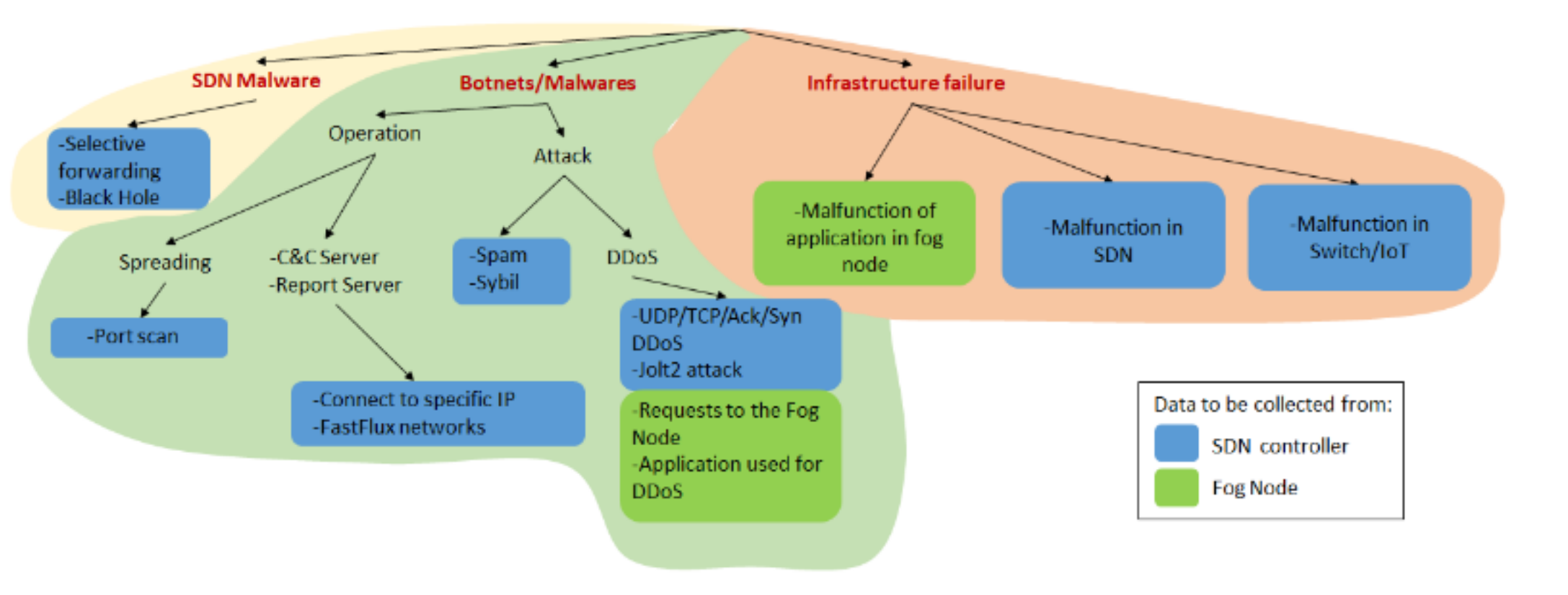


Fig. 1. Taxonomy of attacks endangering an IoT network

III. Analysis of cybersecurity threats, monitoring and mitigation

The SerIoT solution will implement a hybrid approach for ensuring adequate processing resources to support the functional needs of active IoT nodes & devices. Unavoidably, this can theoretically extend SerIoT's vulnerabilities and expose it to extra threats and as such, extra pre-cautions need to be taken. Based on a thorough investigation carried out on the state of the art of modern threats and attacks that are endangering IoT networks and infrastructures, a detailed taxonomy of has been formulated, as shown in Fig 1.

In the literature, the aforementioned threats are pursued by different threat-specific methodologies, that initially search for the exact characteristics of each threat and if detected in excess then an alarm is triggered. Not to mention that the threat detection mechanism is completely disconnected from the mitigation process. Within SerIoT, the threat detection problem will be addressed holistically for all possible threats, through the incorporation of Deep Neural Networks (DNNs). The innovation proposed, however, lies within the fact that the network itself will take advantage of its graph-based structure, in order to apply distributed intelligence along its whole corpus, as show in Fig 2. Specifically, two types of DNNs will be implemented, i.e. network node-specific ones and network edge-specific ones.

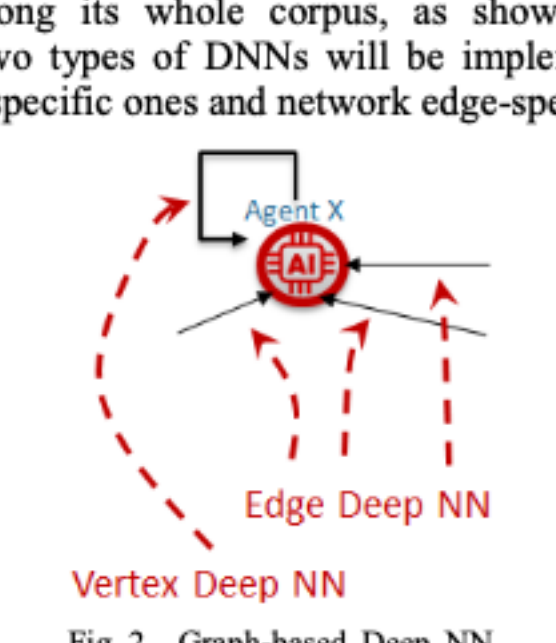


Fig. 2. Graph-based Deep NN approach.

It should also be mentioned that the proposed approach of smart network graph entities (i.e. nodes & edges) can also easily facilitate the mitigation execution mechanism of the network.

Finally, it should be highlighted that it is about the network's integrity and availability, including Quality of Service aspects. Yet, these cannot be always pertained with even the most accurate anomaly detection. Specifically, it takes some insight regarding the verification of the network's structural solidity and within SerIoT, this task is covered by a series of dedicated modules supporting static and runtime Formal Verification of the network's modules and architecture, as well as Penetration Testing approaches.

IV. Software Defined Network

The objective of the Software Defined Network (SDN) framework is to secure the IoT flows in the SerIoT test-bed so that they are not compromised by network based attacks. An additional concern is to carry out this primary function while also offering satisfactory Quality of Service (QoS), such as end-to-end delays and packet loss ratio, as well as minimum energy consumption as far as possible. To this effect, the SerIoT SDN uses an OpenFlow SDN-Controller that specifies and controls routing paths for the IoT applications [4][5]. In future versions of the system, the SDN-Controller may be generic software incarnated for different IoT sub-systems. The SDN-Controller in SerIoT uses cognitive packet routing [6] and Random Neural Network [7] based reinforcement learning, driven by a "Goal Function" that includes security and the detection of possible attacks [3]. In the absence of attacks the SDN-Controller follows paths that offer the best QoS, such as packet delay or de-sequencing which can adversely affect real-time applications, as well as minimum energy consumption.

CPN routing is distributed over selected network routers for measurement, observation, and threat detection to feed relevant data to the SDN routing engine. Visual analytics, and more generally analytics, will also be used for network wide decisions in a distributed manner.

V. Fog Nodes

Fog computing is a relatively new distributed computing model which enables computation and communication at the network edges [8]. Fog computing can be compared to cloud

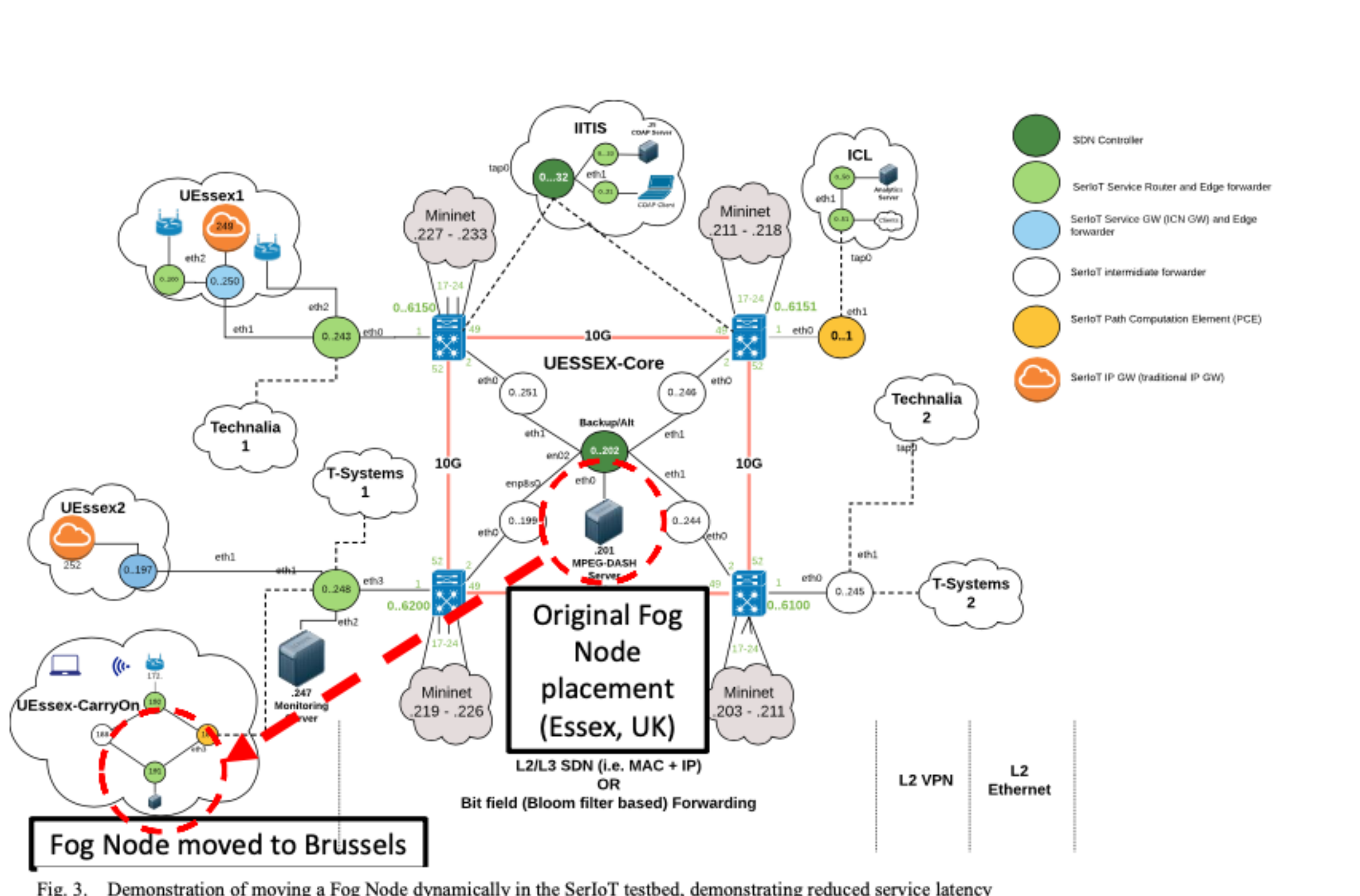


Fig. 3. Demonstration of moving a Fog Node dynamically in the SerIoT testbed, demonstrating reduced service latency

computing, but is designed to support latency-sensitive applications and local function off-loading for IoT devices. Within SerIoT, Fog computing can be used in two ways: firstly, it can be used by end-applications themselves for bringing application logic closer to the IoT devices and users; secondly, it can be used by SerIoT to move certain security functions closer to the edge systems. An example of the former, end-application use, is that in an autonomous (or AI aided) vehicular system it might prove advantageous to move certain application logic as close as possible to the C-ITS station, so that any decisions that need to be made can occur with minimum latency. In the case of the SerIoT components the security functions may benefit from dynamic movement, a good example being a honeypot device which might need to be moved to a particular location in reaction to threats as they are discovered by the SerIoT anomaly detection.

One of the challenges with the dynamic movement of Fog components is to ensure that network traffic goes to the correct node. This can be problematic if traditional IP addressing is used, as mobility is not native in IP and thus various techniques have to be used such as IP mobility anchoring [9]. Consequently, in SerIoT one of the techniques for communication between the Fog nodes is to use information-centric networking (ICN), in particular that enabled through the PURSUIT architecture as utilised by the POINT project [11]. This allows the traffic routing to be dynamically altered without resorting to anchoring of the traffic resulting in reduction of traffic in the network and the ability to reroute without the delays that DNS would incur [10]. Recent demonstrations of the Fog computing work in SerIoT involved dynamically moving a Fog Node from the South East of the UK to the location of the IoT device in Brussels using the SerIoT SDN/IoT testbed, as shown in Fig 3. This example demonstrated the change in IoT device to Fog Node latency from between 200-300 ms (when in Essex, UK) to less than 50 ms (when in Brussels); where the latter delay was predominately caused by local WiFi.

Fog computing has been demonstrated to improve service latency, but the ongoing challenge is to bring service dynamicity. This work has shown how this can be achieved using novel ICN routing, indeed in the example given above, the Fog Node was moved within 2 s without any change required in the IoT end-system which continued to use the same domain name (and even IP address) to access the Fog Node. Most of the movement delay was due to the mechanics of moving the application logic, the network can reroute in sub-second intervals. Continuing work will address the autonomous movement of Fog Nodes (e.g. due to security constraints) and reducing the latency of moving the application logic.

VI. Honeypots

Honeypots are software designed to detect novel and emerging patterns of botnets, DDoS attacks and malware. A honeypot is a trap set to detect or deflect attempts of unauthorized use of information systems. Generally, it is deployed to appear as a part of the network, although it is actually isolated and protected, moreover it should look like it contains information and functionalities that are valuable for attackers.

There are three main categories of honeypots available today classified via the level of interaction: Low Interaction, Medium Interaction and High Interaction. The level of interaction stands for how much the hacker will be able to interact with the system once infected.[12] The more amounts of data that the analysts would like to gather, the

higher level of interaction required; but a higher level of interaction brings more risks into the network security as well. SerIoT honeypots are chosen and adapted according to SerIoT requirements and use-cases. Among them Dionea, glastopf, honeytrap, kippo are mainly considered for testing and development purposes. A range of configurable options will be allocated and can be exercised according to the application usage.

These honeypots fall into two categories: Low and medium interaction honeypot. As per the IoT design constraints passive honeypots are suitable and effective in terms of cost and power. Active honeypots will be studied if time and resources permit.

We use a raspberry pi 3 device to deploy the honeypot. The rasp pi device will also deploy a typical IoT firmware such as IP cameras, routers and sensors. The honeypot will emulate various services such as HTTP, SSH, Telnet, FTP and SQL.

Most of the honeypots are either written in C or python languages and can be easily adapted to our requirements. A busybox will be chosen as the host operating system that runs the IoT applications and honeypot software.

A. *Lightweight anomaly detection engine:*

A virtualized honeypot device will host the anomaly detection algorithm. In specific this algorithm will be lightweight to fit IoT applications. The main focus of this detection engine is to operate in real-time with the honeypot in a virtualized environment. Different detection strategies and techniques are currently being studied and the best approaches will be integrated into the raspberry pi. Due to its lightweight nature, certain vendors can install this engine directly on their IoT device in case, needed.

Brute force detection, DoS attack, malware attacks and botnets will be the main focus of the SerIoT project. Detection based on source and destination IP address, ports, timing, protocols will be studied. Further, detection of malware such signature based and behavior based will be considered for study and if required machine learning techniques will be implemented. The algorithm will present various statistics regarding the attacks and anomalies.

B. *Integration with SDN*

A JSON based framework will be considered to deploy the interface between SDN and honeypot. The framework will carry necessary information such as IP addresses, ports, protocols, status and timing information required for the SDN controller to block/allow certain traffic.

VII. Extending C-ITS Security with SerIoT

Within C-ITS SerIoT will be used in different ways. First it will secure the Road Side ITS Station which is connected through the SDN to the Central ITS Station from the Service Providers Backend, which additionally secures the Service Provider from a malicious Road Side ITS Station. The Second way is monitoring of the Road Side ITS Station and the passing by vehicles to detect compromised stations and vehicles.

A. *Monitoring of R-ITS-S*

The Road Side ITS Stations Security architecture layer is planned to be extended with a SerIoT module called SerIoT Edge Forwarding Element which connects the station to SerIoT SDN. This allows SerIoT to monitor network traffic coming from and to the station and enable SerIoT SDN's primary function of Security Aware Routing. The outgoing information will therefore be routed via secure network paths in case the network itself gets compromised. The stations behavior will be monitored via SDN which can monitor network traffic coming from the station and find malicious packets and drop them on the way to its destination. Another way of monitoring the R-ITS-S is possible via a honeypot approach. The honeypot will be receiving messages send via the C-ITS network on the road side allowing monitoring of not only the messages send out by the R-ITS-S but also the messages send out by vehicles. Since all the communication in the C-ITS network is not encrypted since the broadcaster wants everyone who receives the message to be able to process it and no private data is transmitted such a check of messages is possible.

B. *Detection of malicious vehicles*

To detect malicious vehicles on the road and also protect the R-ITS-S from attacks a honeypot approach is considered which will deflect attacks onto a specific part of the R-ITS-S and could also monitor messages coming in over the ITS G5 interface. This monitoring could provide information about compromised vehicles, sending out malicious messages to disrupt C-ITS services. The honeypot will therefore function in two ways. In the first one it will protect critical modules of the R-ITS-S against attacks and second it will allow detection of vehicles attacking R-ITS-S. Due to the nature of the communication between Vehicle ITS stations and R-ITS-S it will not be possible to identify a specific sender and trace it as the privacy protection mechanism of C-ITS will not allow this. But the collected data will still help to develop further mechanisms to counter the detected attacks and will also provide data for C-ITS service providers and vehicle manufacturers about the vulnerabilities of their system, enabling them to close these detected vulnerabilties in the future.

VIII. Conclusions

SerIoT generates an overall and detailed security view on connected vehicles introduction scenarios in a public roads demonstration in Vienna, Austria, Europe. Additional to the PKI Infrastructure for securing data communication between C-ITS stations at the road infrastructure and in vehicles it proposes and validates a series of technologies from the IoT domain for the analysis and mitigation of security threats in the connected and automated vehicles environment.

The proposed security technologies are tested and validated in a living lab environment with real traffic information coded in C-ITS messages and available for end users. The combination of different security technologies in the demonstration enables the comparison of different security elements and strategies for detection, operation and mitigation of threats at C-ITS station level, and at network level. For the C-ITS stations technologies like honeypots and SerIoT forwarding element have high security improvement potential, at network level the SerIot SDN Router and the fog nodes can be effective. The demonstration results will give detailed data insights into the selected parameters and technology aspects of the single elements.

SerIoT adds several dimensions of analysis, testing and validation of single security technologies in the C-ITS