Topology-aware Cognitive Self-protection Framework for Automated Detection and Mitigation of Security and Privacy Incidents in 5G-IoT Networks

1st Pablo Benlloch-Caballero
University of the West of Scotland, UK
Pablo.Benlloch-Caballero@uws.ac.uk

2nd Ignacio Sanchez-Navarro
University of the West of Scotland, UK
ignacio.sanchez@uws.ac.uk

3rd Antonio Matencio-Escolar
University of the West of Scotland, UK
antonio.matencio@uws.ac.uk

4th Jose M. Alcaraz Calero
University of the West of Scotland, UK
Jose.Alcaraz-Calero@uws.ac.uk

5th Qi Wang
University of the West of Scotland,UK
qi.wang@uws.ac.uk

***Abstract*—Internet of Things (IoT) coupled with 5G networks enable unprecedented levels of scalability and performance in the computing industry. These enhanced performance features allow to offer and deploy a wide range of new use cases and services in scenarios such as Smart Cities, Smart Grid or Industry 5.0 just to mention a few. However, the inherent complexity of such networks is a serious concern in terms of security. Furthermore, the vulnerability and low-power constraints of IoT devices make such networks a targeted vector for cyber criminals. In this contribution, authors present an innovative topology-aware Cognitive Self-protection framework able to detect and mitigate attacks in an autonomous way with no human intervention in the wired segments of 5G-IoT multi-tenant networks. Preliminary tests carried out on a realistic emulated testbed show promising results in terms of time spent in stopping DDoS attacks (less than 47 seconds) and scalability for scenarios with different number of tenants and UEs (2 virtual tenants deployed in 4 Edge nodes and up to 64 IoT devices or sensors connected to the infrastructure).**

***Index Terms*—Network Security, IoT, 5G, Zero Touch Network Management.**

I. Introduction

The deployment of IoT systems is growing rapidly worldwide, fuelled by 5G technology [1]. 5G is a key technology able to provide mass connectivity for IoT devices whilst delivering high data rates, higher bandwidth, and low latency in IoT landscapes, allowing it to meet the challenging demands and Quality of Service (QoS) parameters of new use cases otherwise unforeseen in 4G/LTE networks. Similarly, the amount of security incidents is proliferating as IoT scenarios are rolled out, involving a huge number of unattended, resource-constrained, and hence vulnerable, IoT devices and sensors. Simultaneously, cyber-attacks are becoming more sophisticated, thus demanding strengthened cyber security capabilities, along with more effective mechanisms for attack detection and mitigation.

As defined by 5G PPP in [2], there are different stakeholders involved in the provisioning of network resources in 5G-IoT networks. A major role is played by Digital Service Providers (DSPs), supplying a range of digital services to different verticals, industries, or end-users. Virtualization Infrastructure Service Providers (VISP) provide and operates virtualized physical infrastructure comprising networking and computing resources, offering Infrastructure as a Service (IaaS) to DSPs. Hence, different DSPs can share a common physical multi-tenant infrastructure provided and managed by the same VISP, resulting in savings in Capital Expenditure (CAPEX) and Operational Expenditure (OPEX).

However, the deployment of 5G-IoT multi-tenant networks implies the use of overlay networks with different levels of nested encapsulation to support user mobility, e.g. GPRS Tunnelling protocol (GTP), and tenant isolation, using protocols such as Virtual eXtensive LAN (VXLAN), or Generic Routing Encapsulation (GRE). Therefore, an advanced security solution for this type of network must provide protection not only for traditional IP traffic but also for fine-grained security capabilities to handle the complex network traffic associated with multi-tenant network topologies.

The main contribution of this research work is the design, prototyping, and validation of a novel automated Cognitive Self-protection framework with topology awareness capabilities for the detection and mitigation of security and privacy incidents in the wired segments of 5G-IoT multi-tenant networks (i.e., Edge and Core). The following are the main innovations presented in this work:

- Novel dynamic IDS to detect security and privacy incidents suitable for dealing with the complexity of 5G-IoT

This research was funded by the European Commission under Grant Agreement H2020-SU-DS02-2020/101020259 ARCADIAN-IoT (Autonomous trust, security and privacy management framework for IoT)

979-8-3503-0322-3/23/$31.00 ©2023 IEEE

multi-tenant network traffic.

- Topology awareness system to analyze and identify the optimal mitigation point within the 5G-IoT network topology.
- Novel distributed mitigation security policy enforcer able to implement fine-grained security policies in 5G-IoT multi-tenant datapaths where different tunnelling and encapsulation protocols are used to guarantee user mobility and tenant isolation.
- Empirical validation and evaluation in a realistic emulated testbed.

The rest of the paper is organized as follows. Section II briefly overviews the current state of the art in 5G-IoT network security. Section III describes the design, architecture, and functionality of the proposed solution. Then, Section IV discusses the empirical results gathered to validate and evaluate the proposed framework. To conclude, in Section V we discuss the conclusions and outline our future research lines.

II. Related work

The significant number of research activities related to security in 5G-IoT networks is clear evidence of the interest and concern this topic arouses within the research community. A number of publications and surveys such as [3] and [4] highlight security and privacy aspects in 5G-IoT networks as one of the major challenges to be addressed in such architectures.

In [5], authors present a framework able to detect malicious traffic at the IoT-Edge layer and thus, to identify possible infected IoT devices in a botnet network. The analysis is carried out using Sparsity Representation and Reconstruction Error Threshold techniques. They used the NB-IoT data set to train the ML models and only benign traffic data is used to calculate the threshold error. This framework, however, is not able to protect all segments across the 5G architecture. Moreover, the authors have not considered the classification of 5G multi-tenant traffic.

In [6] and [7], both perform detection, analysis, and mitigation of the attack. [6] presents IoT Botnet Detection and Analysis (IoT-BDA), a framework based on honeypots for detecting, analyzing, identifying, and reporting botnets circulating on the Internet. On the other hand, [7] presents a framework running on the firmware of IoT devices. It tries to use Deep Learning (DL) techniques by using the Long Short-Term Memory (LSTM) algorithm to detect the attack. The mitigation technique is to disable infected IoT devices. Although the above contributions are of great interest, they do not present a solution that can perform fine-grained attack mitigation in overlay networks inherent to 5G multi-tenant deployments.

Authors in [8] propose a self-healing model to detect and mitigate Distributed Denial of Services (DDoS) attacks for Software Defined Networks (SDN) deployments with OpenFlow protocol, using POX and RYU as SDN controllers. They reach an accuracy of over 80% in filtering malicious traffic.

A novel SDN-based architecture to identify suspicious nodes in 4G/5G IoT networks and redirect their traffic to a secondary network slice is proposed in [9]. By following this approach, potential threats can be detected at an early stage and limit the damage by DDoS attacks originated in IoT devices.

Authors in [10] propose a self-healing protocol for automatic discovery and maintenance of the network topology in SDN deployments. It provides layer two topology discovery and autonomic fault recovery to enhance the control plane robustness. Preliminary results in a simulated testbed show the proposed protocol recovers the control topology efficiently in terms of time and message load. Similarly, in [11], authors implement a new topology discovery approach on the widely used POX controller platform, and evaluate it for a range of network topologies.

In [12], authors propose an agent-based approach called SHAPE to self-heal and self-protect the system from various kinds of security attacks including DDoS whilst dealing with hardware, software, and network faults.

To the best of the authors' knowledge, none of the existing state-of-the-art publications provides a self-healing mechanism for the detection and mitigation of cyber-attacks in 5G-IoT multi-tenant networks. In other words, detect and stop malicious traffic with no human intervention whilst enabling the enforcement of fine-grained security policies in the data-plane of complex overlay networks. This is the major contribution and innovation presented in this work.

III. Cognitive Self-protection framework

The Cognitive Self-protection framework presented in this work is composed of three main components whose responsibilities are divided into the accurate detection of the threat (Network Flow Monitoring), analysis, and decision of the action to be taken (Network Self-Healing), and enforcement of the mitigation strategy in the data-plane (Network Self-protection). The following subsections explain the functionality of each component, its responsibility, and its impact on the system as part of the Cognitive Self-protection framework. As depicted in Fig. 1, the communication and cooperation between the components are provided by means of a message bus tool. It grants communication between the different architectural components through a publishing/subscription paradigm. The proposed framework uses RabbitMQ [13] as message bus software since it is one of the most popular open-source message brokers. Fig. 1 shows the 4 message exchanges implemented for the interaction between the framework components: Network IDS Events, Topology, Network Healing Instructions and Network Self-protection Confirmations. This section also overviews a 5G-IoT Multi-tenant infrastructure that matches the case of study in this contribution and provides a realistic scenario to validate and empirically evaluate the proposed solution.

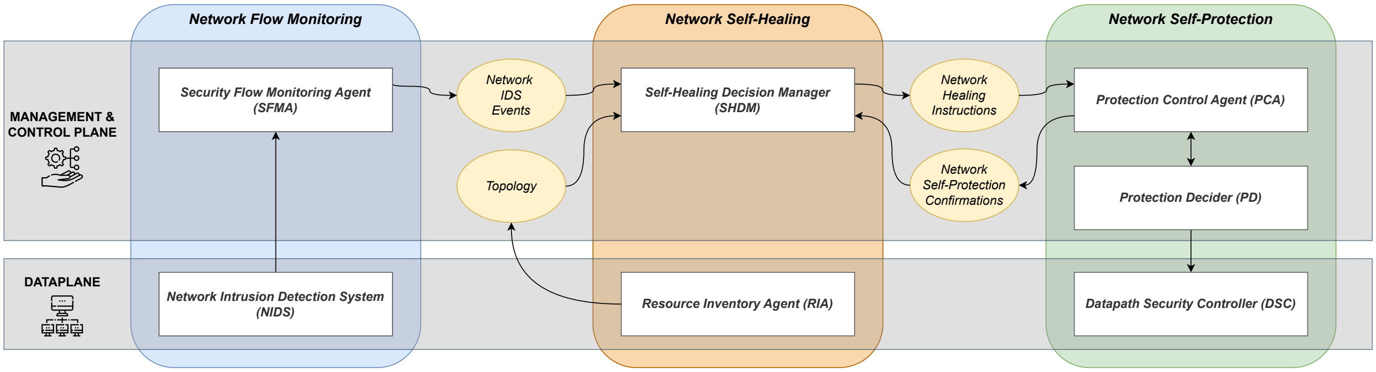
Network Flow Monitoring
Network Self-Healing
Network Self-Protection
MANAGEMENT & CONTROL PLANE
DATAPLANE
Security Flow Monitoring Agent (SFMA)
Network IDS Events
Topology
Self-Healing Decision Manager (SHDM)
Network Healing Instructions
Network Self-Protection Confirmations
Protection Control Agent (PCA)
Protection Decider (PD)
Network Intrusion Detection System (NIDS)
Resource Inventory Agent (RIA)
Datapath Security Controller (DSC)

Fig. 1. Topology-aware Cognitive Self-protection framework flow chart (architectural components and message exchanges).

A. 5G-IoT multi-Tenant network infrastructure

Fig. 2 depicts the 5G-IoT multi-Tenant network infrastructure proposed in this work. Six different network segments can be seen from a bottom-up perspective: *(i)* the Radio Access Network to connect the IoT devices to the 5G-IoT network through the gNBs and the Distributed Units (DUs), *(ii)* the Mobile/Multi-access Edge Computing (MEC) segment where the multi-tenancy feature is depicted by two different DSPs (notice the orange and green boxes) sharing the same physical infrastructure provided by one VISP (see the grey boxes), *(iii)* the transport network connecting the Edge and Core segments, *(iv)* the core segment with expanded service capabilities, scalability agility, and 5G core network functions such as the Session Management Function (SMF), the Access Management Function (AMF) and the User Plane Function (UPF), *(v)* the service and management layer where the centralized components of the proposed framework are deployed, and finally *(vi)* the Inter-Domain network segment to reach the internet and other domains.

B. Network Flow Monitoring

The Network Flow Monitoring (NFM) component (blue/left box in Fig. 1) is responsible for the detection of the attack. This component relies on the mirrored traffic from the transport network, as depicted in Fig. 2. The mirrored network traffic is sent to the Service layer, where this component is centralized and deployed to analyze the traffic introducing almost no additional latency in the primary data-plane.

The detection is carried out by the use of an enhanced Network Intrusion Detection System (NIDS), which will trigger an alert when a threat is registered in the system. The main contribution of this component is the extension of the traditional NIDS to provide detection in complex overlay networks and 5G-IoT network segments, information that traditional NIDS lacks. These extensions allow the accurate detection and classification of a malicious flow with specific, granular and effective alerts. The information provided by this component is separated into three categories differentiated by their purpose: first, metric information of the NIDS, such as the number of total packets of a specific technology that have been filtered or the dropped packets ratio, type of the attack, etc.; second, 5G network information relative to the malicious flow metadata such as information extracted from inner headers, number and types of overlay tunnelling and encapsulation protocols (e.g. VXLAN, GTP, GRE, etc.); and third, additional alert useful information such as alert type, alert impact, causes of the alert and if the flow is already stopped or not. The NFM extends Snort [14] as the base NIDS. The NFM publishes each alert to the RabbitMQ Network IDS Events exchange, where the following component of the framework is subscribed and will receive it.

C. Network Self-Healing

The Network Self-Healing (NSH) (orange/center box in Fig. 1) is the component in charge of analyzing the alert triggered by the NFM and deciding where should be stopped the attack. To do so, this component is divided into two different subcomponents:

- The Resource Inventory Agent (RIA) is a distributed software deployed in the data-plane (see deployment locations in Fig. 2) periodically reporting the information about the network topology (see Topology exchange in Fig. 1). This topological information is one of the main innovations of this work as it enables the NSH to determine the best optimal location to stop the attack following a logic predefined by the programmer, such as “near the source”, “near destination”, “n hops from the source”, etc. More details about RIAs’ architecture are presented in [15].
- The Self-Healing Decision Manager (SHDM) receives and aggregates the information about the topology to have a full view of the network. Then, when SHDM receives an alert from NFM, it uses the entire status of the topology to decide the optimal mitigation point where the attack can be stopped. Finally, the SHDM sends a Network Healing Instruction (see Network Healing Instructions exchange in Fig. 1) that will be received by the Network Self-Protection component. This instruction contains an action such as performing a drop, redirecting traffic, or mirroring the flow in a specific point of the datapath. These actions can be automated by the administrator through a policy

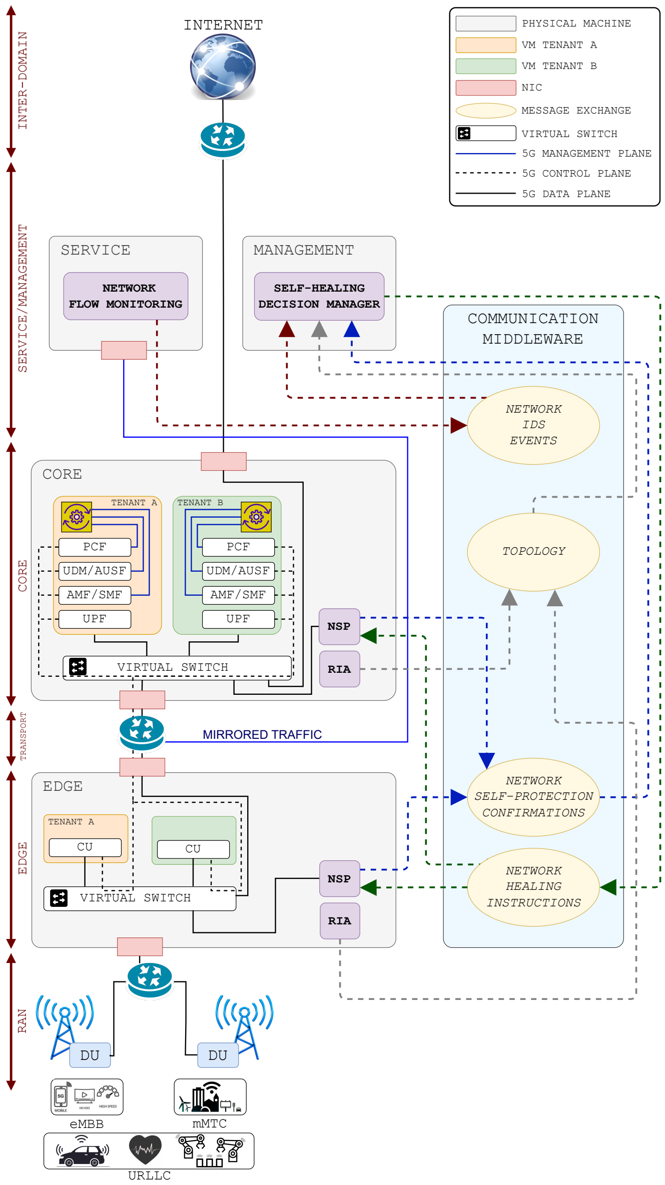

Fig. 2. 5G-IoT multi-Tenant network infrastructure with the topology-aware Cognitive Self-protection framework components deployed.

engine in order to define different strategies for each type of attack.

D. Network Self-Protection

The Network Self-Protection (NSP) component (green/right box in Fig. 1) is responsible for providing the self-protection capabilities in the wired segments of the data-plane, enforcing a set of protection policies. It is based on the well-known virtual switch OpenVSwitch (OVS) on which significant extensions have been undertaken to extend the data-plane programmability. The Network Self-protection architecture consists of three sub-components:

- Protection Decider (PD): Responsible for deciding on every instant what subset of rules from the complete set of protection rules located in the PD will be enforced in the following sub-component.
- Datapath Security Controller (DSC): It processes the network traffic and eventually enforces the protection rules into the data-plane. Every packet through the data-plane is deep inspected and classified, and an action is taken based on the subset of protection rules active at the moment.
- Protection Control Agent (PCA): It provides a North Bound Interface (NBI) for the communication with the NSH component (see Network Healing Instructions exchange in Fig. 1). The exposed NBI is an intend-based interface receiving technology-independent instructions that are translated into technology-dependent commands to be enforced in the data-plane. It also provides dynamic management of the life cycle of the set of protection rules (installation, modification, and deletion) to the NSH.

E. DDoS use case

In a User Datagram Protocol (UDP) DDoS attack, the attacker floods the target system with a high volume of UDP packets, overwhelming the system resources and causing it to become unresponsive. The attacker typically spoofs the source IP addresses to make it challenging to trace the origin of the attack. Since UDP does not verify the recipient's readiness or response, the flood of incoming UDP packets quickly saturates the target's network bandwidth, CPU, and memory resources. Consequently, legitimate traffic cannot reach the intended service, leading to a denial of service for legitimate users. Due to the huge impact of this attack on the overall system performance, this kind of attack has been chosen to demonstrate the suitability of the proposed solution in stressful scenarios. The design of the attack is as follows:

- The Maximum Transmission Unit (MTU) is set to 1500 Bytes.
- The Payload of the sent packets is nearly the maximum MTU, being 1250 Bytes.
- The expected maximum length of the network packet headers through the network is 132 Bytes, as depicted in Fig. 3.
- The emulated IoT devices collectively transmit at a fixed bandwidth of 1Gbps during each attack. The transmission rate for each IoT device varies based on the total number of devices connected. For instance, with 16 connected devices, each sends at 5600pps (Packets per Second), while with 32, it's 2800pps. This relationship is summarized in Table I for clarity.

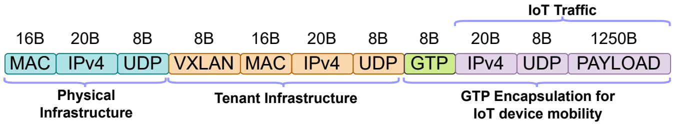

Fig. 3. 5G-IoT multi-tenant network traffic encapsulation pattern.

IV. Results and Empirical Validation

A. Testbed for empirical evaluation

To demonstrate the functionality and feasibility of the framework proposed in this research work, we have developed a testbed environment where a large number of experiments were executed to gather results for further analysis. The testbed was an emulated 5G network infrastructure matching the one depicted in Fig. 2. The infrastructure is compromised by a UDP DDoS attack launched from the infected IoT devices. In order to empirically validate the proposed framework, it has been tested in two different scenarios. The first scenario (A) was designed as depicted in Table I where the key element is the increase of the number of attackers, varying the number of UEs connected to each gNB. The rest of the network elements of the topology are fixed to 1 gNB connected to each DSP, 2 DSPs hosted on each ISP (multi-tenant isolation feature), and 2 Edge nodes connected to 1 Core node. The second scenario (B) was designed to evaluate a more complex network topology and increase the possible action points where the attack could be mitigated. For scenario B, the number of attackers is the same as in A, but the topology is built as follows: 2 gNB connected to each DSP, 2 DSPs hosted on each ISP, and 4 Edge nodes connected to 1 Core node.

TABLE I
Network topology for test bed in scenarios A and B.

Scenario	**A**				**B**			
No UE x gNB	4	8	12	16	1	2	3	4
No gNB x DSP	1	1	1	1	2	2	2	2
No DSP	2	2	2	2	2	2	2	2
No Edge	2	2	2	2	4	4	4	4
No Core	1	1	1	1	1	1	1	1
Total attacker	16	32	48	64	16	32	48	64
Packet rate (pps)	5600	2800	1875	1400	5600	2800	1875	1400
Consumed BW (Mbps)	64	32	22	16	64	32	22	16

The emulation tool used to deploy both scenarios is Common Open Research Emulator (CORE) [16]. It uses Linux Network Namespaces (netns) to emulate each of the different devices and networks on the infrastructure. The physical machine where the experiments were executed has an Ubuntu 20.04 LTS distribution with kernel version 5.15.0. As physical resources, it has a 56-core Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz and 128GB DDR4 2400 MHz of RAM.

The execution of the experiments consists of the creation of each scenario by running an automated script that performs the following sequence of steps for the creation of the environments leveraging CORE emulator functionalities:

1) Provide network topology information using configuration files.
2) Configure logs and outputs during experiment execution.
3) Set up network protocols and performance configurations for all the interfaces and connections between nodes.
4) Provision nodes with specific software based on their roles (Edge, Core, management, service, IoT device) in the experiment.
5) Create necessary tunnels (VXLAN, GTP, GRE, etc.) to provide multi-tenancy and user mobility features.
6) Launch the attack and activate the Cognitive Self-protection framework components.
7) Conclude the attack, gracefully shut down the topology, and retrieve logs, results, and outputs.

B. Results

For the set of experiments described in Table I, the results are shown in Fig. 4. This graph is divided into two different parts separated by a vertical red line: the left one related to scenario A and the right one to scenario B. Both parts show the same number of infected IoT devices on the X-axis, as mentioned above (16, 32, 48, and 64). The Y-axis represents the average consumed time for the Cognitive Self-protection framework from the detection to the mitigation of the attack. This time is represented in seconds and each colour represents the time consumed for each of the three components (blue for NFM, orange for NSH, and green for NSP).

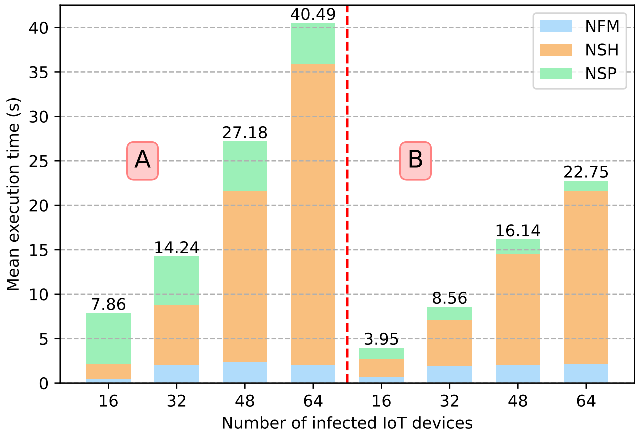

Fig. 4. Average time consumed by the Cognitive Self-protection framework, Scenario A (left) against Scenario B (Right).

The collected results can be analysed by considering the overall performance of the framework and by evaluating the individual overhead and behaviour for each component. Fig. 4 clearly indicates that, in both scenarios, the overall behaviour of the framework shows good scalability. In the worst case in scenario A, the attack is stopped in less than 41 seconds. In scenario B, with a more distributed network topology, the attack is mitigated in less than 23 seconds for the worst case with 64 infected IoT devices transmitting malicious traffic simultaneously. At first glance, the architectural component that introduces the most overhead is the NSH.

With respect to the individual impact of each component, the NFM outperforms in the overall framework. It shows a stable performance throughout every scenario (A and B) and also when the number of infected IoT devices is increased. For the worst-case setting (64 IoT devices), the time spent by the NFM is 2.06 seconds in scenario A and 2.20 seconds in scenario B. The NFM shows promising results regarding scalability.

As it can be observed by comparing the NSH behaviour in both scenarios, the execution time increases linearly when growing the number of IoT devices. However, the execution time in scenario A is higher for all the different settings when compared to scenario B. For the worst-case setting (64 IoT devices), the NSH required 33.8 seconds in scenario A and 19.4 seconds in scenario B. In scenario A, the topology consists of 2 Edge Compute nodes and 2 gNBs that are connected to each of the DSPs, thus the number of action points to enforce the mitigation of the attack is 4. As the SHDM is the centralized and cognitive component of the Cognitive Self-protection framework that will produce as an output the location to mitigate the threat with the promise of "close to source", all the workload for the study of the best location to mitigate the attack will be carried by itself. However, when switching to scenario B, not only the number of action points to mitigate the threat rise but also the number of distributed RIA components that are responsible for notifying the network topology information in real-time. This is why the NSH in Fig. 4 shows a better performance for scenario B. Distributing some workload when the number of attackers is the same is always improving the system.

Regarding the NSP, it shows a higher consumption time for scenario A than scenario B, but remains stable for all settings within each scenario. NSP required roughly 5 seconds in scenario A and approximately 1.5 seconds in scenario B to enforce the healing instructions in the data plane and eventually stop the attack. The NSP has a different response time due to its distributed deployment. This component is distributed over the different compute nodes on the topology, thus the workload is levelled by the number of NSP instances deployed across the infrastructure. Leveraging this distributed feature, Fig. 4 shows a better performance in the NSP when the topology grows whilst the number of IoT devices remains constant.

Therefore, the results of the experiments discussed above demonstrate the feasibility of the proposed solution to detect and mitigate cyber-attacks in 5G-IoT networks in an automated manner with no human intervention, showing promising preliminary results.

V. Conclusions

This work presents a novel topology-aware Cognitive Self-protection framework suitable for 5G-IoT multi-tenant networks able to detect and mitigate in an autonomous way cyber-attacks coming from compromised IoT devices and sensors. The proposed solution copes with complex network traffic with multiple levels of nested tunnelling and encapsulation protocols inherent to such infrastructures, such as GTP, VXLAN, or GRE, for example.

Empirical validation and evaluation have been conducted in an emulated testbed using CORE emulator to deploy the 5G-IoT topology. Preliminary results demonstrate the proposed solution stops a DDoS attack from 16 up to 64 infected UEs in less than 41 seconds in the worst-case scenario, showing better performance in more complex scenarios with 4 Edge nodes and 16 gNBs (23 seconds to mitigate the malicious traffic).

As a future line of work, authors will explore the scalability, efficiency, and performance of the proposed approach in terms of network size (number of UEs, Edge nodes, and CORE nodes) and volume of the attack (number of infected UEs and transmitted bandwidth of malicious traffic).

Acknowledgment

This research was funded by the European Commission under Grant Agreement H2020-SU-DS02-2020/101020259 ARCADIAN-IoT (Autonomous trust, security, and privacy management framework for IoT).

References

[1] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.

[2] C. M. Simone Redana, Ömer Bulakci, "View on 5G Architecture," tech. rep., 5G PPP, 2020.

[3] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, "On the security of the 5g-iot architecture," in *Proceedings of the international conference on smart cities and internet of things*, pp. 1–8, 2018.

[4] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5g in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, p. 107345, 2020.

[5] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the iot edge based on sparse representation," in *2019 Global IoT Summit (GIoTS)*, pp. 1–6, 2019.

[6] T. Trajanovski and N. Zhang, "An automated and comprehensive framework for iot botnet detection and analysis (iot-bda)," *IEEE Access*, vol. 9, pp. 124360–124383, 2021.

[7] M. M. Salim, S. K. Singh, and J. H. Park, "Securing smart cities using lstm algorithm and lightweight containers against botnet attacks," *Applied Soft Computing*, vol. 113, p. 107859, 2021.

[8] G. Sharma, H. Sharma, R. Pareek, N. Gour, R. S. Sharma, and A. Kumar, "Self-healing topology for ddos attack identification & discovery protocol in software-defined networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 8, pp. 2221–2232, 2021.

[9] D. Candal-Ventureira, P. Fondo-Ferreiro, F. Gil-Castiñeira, and F. J. González-Castaño, "Quarantining malicious iot devices in intelligent sliced mobile networks," *Sensors*, vol. 20, no. 18, p. 5054, 2020.

[10] L. Ochoa-Aday, C. Cervello-Pastor, and A. Fernandez-Fernandez, "Self-healing topology discovery protocol for software-defined networks," *IEEE communications letters*, vol. 22, no. 5, pp. 1070–1073, 2018.

[11] F. Pakzad, M. Portmann, W. L. Tan, and J. Indulska, "Efficient topology discovery in openflow-based software defined networks," *Computer Communications*, vol. 77, pp. 52–61, 2016.

[12] I. Chopra and M. Singh, "Shape, an approach for self-healing and self-protection in complex distributed networks," *The Journal of Supercomputing*, vol. 67, pp. 585–613, 2014.

[13] "RabbitMQ." Available at https://www.rabbitmq.com/documentation.html, 2023. Accessed on June 2023.

[14] "Snort Intrusion Detection System (IDS)." Available at https://www.snort.org, 2023. Accessed on June 2023.

[15] I. Sanchez-Navarro, A. S. Mamolar, Q. Wang, and J. M. Alcaraz Calero, "5gtoponet: Real-time topology discovery and management on 5g multi-tenant networks," *Future Generation Computer Systems*, vol. 114, pp. 435–447, 2021.

[16] "CORE: Common Open Research Emulator." Available at https://github.com/coreemu/core, 2023. Accessed on June 2023.