Journal of Network and Computer Applications 145 (2019) 102416

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Autonomic protection of multi-tenant 5G mobile networks against UDP flooding DDoS attacks

Ana Serrano Mamolar, Pablo Salvá-García, Enrique Chirivella-Perez, Zeeshan Pervez, Jose M. Alcaraz Calero *, Qi Wang

University of the West of Scotland, UK

ARTICLE INFO

Keywords:
Self-managed networks
Autonomic control loop
5G network
DDoS attack
Multi-tenancy
Self-protection

ABSTRACT

There is a lack of effective security solutions that autonomously, without any human intervention, detect and mitigate DDoS cyber-attacks. The lack is exacerbated when the network to be protected is a 5G mobile network. 5G networks push multi-tenancy to the edge of the network. Both the 5G user mobility and multi-tenancy are challenges to be addressed by current security solutions. These challenges lead to an insufficient protection of 5G users, tenants and infrastructures. This research proposes a novel autonomic security system, including the design, implementation and empirical validation to demonstrate the efficient protection of the network against Distributed Denial of Service (DDoS) attacks by applying countermeasures decided on and taken by an autonomic system, instead of a human. The self-management architecture provides support for all the different phases involved in a DDoS attack, from the detection of an attack to its final mitigation, through making the appropriate autonomous decisions and enforcing actions. Empirical experiments have been performed to protect a 5G multi-tenant infrastructure against a User Datagram Protocol (UDP) flooding attack, as an example of an attack to validate the design and prototype of the proposed architecture. Scalability results show self-protection against DDoS attacks, without human intervention, in around one second for an attack of 256 simultaneous attackers with 100 Mbps bandwidth per attacker. Furthermore, results demonstrate the proposed approach is flow-, user- and tenant-aware, which allows applying different protection strategies within the infrastructure.

1. Introduction

The preparation of the network to battle against any forms of cyber-attacks is critical for our society, where the dependence on technologies is ever-increasing in almost all aspects of daily life. Distributed Denial of Service (DDoS) attacks have caused particular damage to network infrastructures during the last years (Cui et al., 2016). The Mirai attack took down major websites in 2016 using a massive number of compromised Internet-of-Things (IoT) devices.[1] The most recent and largest Memcached DDoS attack is the 1.35 terabits amplification attack, which compromised the Github platform in 2018.[2] Since DDoS attacks are becoming more complex and ingenious, it is becoming increasingly difficult to detect and mitigate them (Wang et al., 2012). This problem is exacerbated by the challenges imposed by the novel multi-tenant 5G networks.

For cost saving, most 5G infrastructures have been softwarised. It allows to instantiate multiple 5G infrastructures inside the same physical resources and, typically, network operators share such physical resources to minimise costs in a multi-tenant environment. Virtual tenant networks and tunnelling protocols keep the traffic of each tenant completely isolated, while their respective users are supported with mobility. Fig. 1 presents a 5G network where physical resources are shared through virtualisation and where the main architectural elements of the 5G architecture have been depicted. Both 5G and 4G components are illustrated to show their correspondence. It is worth mentioning the "v" prefix used in each of the architectural components refers to the virtualised version of the corresponding architectural component. Four different network segments are shown: Radio Access Network (RAN), Mobile Edge Computing Network, Core Network, and Inter-Domain Network. The RAN segment is associated with the deploy-

* Corresponding author.
E-mail address: jose.alcaraz-calero@uws.ac.uk (J.M. Alcaraz Calero).

[1] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices.

[2] https://www.wired.com/story/github-ddos-memcached/.

https://doi.org/10.1016/j.jnca.2019.102416
Received 28 November 2018; Received in revised form 18 July 2019; Accepted 28 July 2019
Available online 1 August 2019

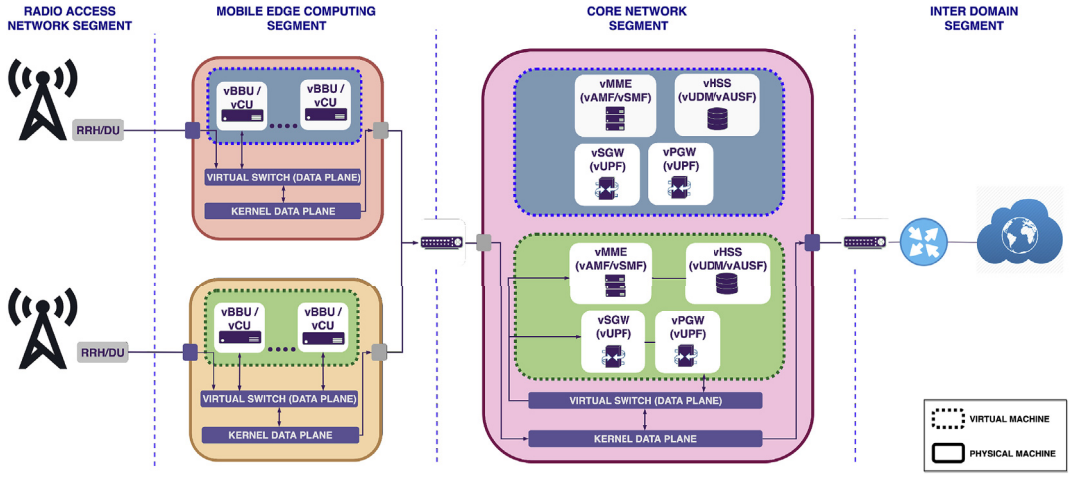


Fig. 1. Overview Architecture of a 5G multi-tenant infrastructure.

ment of Distributed Units (DUs) or Remote Radio Heads (RRHs) on top of buildings, towers, etc. The Mobile Edge Computing Network (MEC) segment is associated with the last mile where traditional Commercial-off-the-Shelf (COTS) computers are allocated to process data close to the final user and where architectural elements such as Central Units (CUs) or Base Band Units (BBU) are allocated, especially when a Cloud-RAN MEC deployment is employed. The Core Network segment is where the main parts of the 5G Core Network are deployed and where the access for the user to other networks is provided. Fig. 1 represents the 5G architectural elements deployed in the Core Network: Authentication Server Function (AUSF), Unified Data Management (UDM), Access and Mobility Management Function (AMF), Session Management Function (SMF) and User Plane Function (UPF). Kim et al. (2017) provide a comprehensive description of the different architectural elements envisioned in the 5G architecture. Moreover, different tenants/operators are depicted with different background colours and isolated through independent overlay networks to ensure multi-tenant traffic isolation.

This multi-tenant 5G infrastructures makes the structure of network flows dynamic across the different network segments, specially when the multi-tenancy capabilities have been extended to the edge of the network. This imposes a significant challenge for human administrators when they endeavour to detect DDoS attacks, since these may be hidden inside overlay networks. This challenge has already been suggested by Neves et al. (2017), indicating that it is vital to develop novel sensors and actuators to achieve an autonomic self-protection system in a 5G network, which are able to work in a multi-tenancy and mobility environment and which is far beyond the state of the art, where current sensors and actuators are designed for traditional IP networks. Additionally, once DDoS attacks are detected, tracking the flows across different network segments until the best place to mitigate such attack is found and understanding what type of rules should be applied to mitigate such attack according to the encapsulation protocols associated with such network segment are not trivial tasks, owed to the dynamic nature of the encapsulation protocols available within these networks. Current Intrusion Prevention Systems (IPS) are designed to work in a centralised way with defined static countermeasures, without providing support for such encapsulation protocol. Furthermore, countermeasures should be implemented by different actuators, which are placed in different network locations to enable a distributed mitigation of attacks, as an approach to dealing with the foreseen scalability of the attack, owed to the increase of the network speed and number of devices connected to the 5G network. These countermeasures should be enforced on real-time and based on an up-to-date state of the network and the foreseen impact of the attack dealing with such continuous changes to the packet structure, therefore imposing significant challenges in the automation of the mitigation strategy. The automation of this self-protection system would reduce human interventions and the response times of the system, which are the primary causes of service disruption in network environments, in favour of a cognitive and self-managed network.

The main contribution of this research is the design, prototyping, and validation of a self-management control loop to self-protect a multi-tenant 5G infrastructure against DDoS attacks without human intervention to overcome the challenges imposed by the 5G network previously described. To achieve such a system, several architectural components have been designed and prototypes and several innovations have been implemented on such components until a fully operational system is possibly achieved. The following contributions and innovations towards the protection of future generation computer networks are achieved in this work. First, current intrusion detection sensors (IDS) have been extended with detection capabilities over malicious flows contained in the 5G overlays networks for multi-tenancy and user mobility. Second, a novel network flow controller has been provided to act at any point across the data path, regardless of the dynamic structure of the flow structure and which is particularly suitable for MEC infrastructure where the network segment between Edge and Core expose a nested overlay network. Third, DDoS mitigation without collateral damages has been achieved as a result of the development of the autonomous system in charge of making decisions regarding the events and metrics gathered from IDS sensors. Without these three contributions, it would not be possible to act over this kind of fine-grained overlay flows, ending in situations where all the traffic within the same network segment is dropped during the attack and that affects other legitimate 5G users. Fourth, the proposed architecture separates the locations, where both detection and migration are carried out, allowing us to provide a distributed mitigation approach where the attacks are stopped in multiple places, allowing our cognitive autonomous system to take decisions on where to mitigate such attacks. Finally, the novel algorithm used in the autonomous system to determine where to perform the mitigation is a contribution to the state-of-the-art systems where the cognitive framework can determine the locations where the attacks should be stopped and the approach for the same to minimise the potential impact for the users. The proposed approach can take fine-grained decisions at the user-level, tenant-level, and flow-level. Based on the listed contributions, this work represents, to the best of our knowledge, the first autonomic network management framework capable to auto-protect large-scale 5G telecommunication infrastructures against massive DDoS attacks.

The rest of the paper is organised as follows. Section 2 presents the related work with different approaches to the detection and mit-

Table 1
Summary of related work.

	Topology Aware	Multitenancy support	Mobility support	Fine-grained mitigation	Distributed mitigation
Yan et al. (2018)	X	X	X	X	X
Hyun et al. (2017)	X	X	X	X	X
Hu et al. (2017)	X	X	X	X	X
Sahay et al. (2017)	X	X	X	X	✓
Ayoubi et al. (2018)	✓	X	X	X	X
Adat and Gupta (2017)	X	X	X	X	X
Bhunia and Gurusamy (2017)	X	X	X	X	X
Ozcelik et al. (2017)	X	X	X	X	✓
Giotis et al. (2014)	X	X	X	X	✓
Buragohain and Medhi (2016)	X	X	X	X	✓
Morales et al. (2015)	X	X	X	X	✓
Wang et al. (2015)	✓	X	X	X	✓
This contribution	✓	✓	✓	✓	✓

igation of DDoS attacks and cognitive networks. Section 3 describes the approach of this work by presenting the design and architecture towards a self-protected multi-tenant 5G network. Section 4 presents the performance evaluation of the proposed framework. Section 5 concludes the paper along with the future work.

2. Related work

The Architecture working group of the 5G Infrastructure Public Private Partnership (5G PPP) has highlighted three features for a defence mechanism to be included within a 5G network (5G PPP Architecture Working Group, 2016). First, multi-tenancy should be supported. Second, the novel mechanisms should be able to self-adapt to any changes that may occur in the network topology. Third, a short reaction time against events is required. Thus, the overhead added by the detection and mitigation system should not affect the overall performance of the network.

In recent years, some mechanisms have been proposed to defend against DDoS attacks. Despite the considerable number of published works related to the detection and mitigation of DDoS attacks, no defence system supports the aforementioned features. Therefore, those defence systems cannot achieve an effective defence for protecting users, tenants, and infrastructure in 5G multi-tenant networks with points of presence in the edges of the network. Some studies cover the complete detection and mitigation loop, while others are focus on either detection or mitigation. This related work is focused on those research works that provide a complete closed autonomous control loop.

Table 1 compares the key features addressed in this contribution with respect to the relevant existing works to clearly identify how our contribution goes a step forward. The analysis presented in Table 1 has led to the identification of some gaps in the literature. First, most existing works are not self-managed control loop solutions and still need human support to make decisions on the countermeasures to mitigate attacks (Hyun et al., 2017). Thus, long reaction times might end in dramatic high impact consequences such as substantial service disruption. Second, most solutions simply protect end hosts and do not provide protection at all the levels of users, tenants, and infrastructures. This is due to the lack of flow monitoring and control capabilities along the whole data path, to be able to act at different levels of granularity. Third, most proposed solutions are centralised defence mechanisms with an interface to the mitigation system (Hu et al., 2017; Sahay et al., 2017). However, a superior approach for DDoS attacks, mitigation would be a distributed defence system (Zargar et al., 2013), with multiple mitigation point locations differentiated. Fourth, most solutions are validated for a very particular topology and infrastructure (usually, a traditional IP network (Hu et al., 2017)). However, a cognitive management control loop should be aware of the network topology to understand where alerts are raised and where actions should be applied. Finally, the state-of-the-art regarding sensors and actuators is not ready to support 5G networks, since they do not consider multi-tenancy isolation and mobile users, which are key features in 5G (Yan et al., 2018; Hyun et al., 2017; Ayoubi et al., 2018).

As highlighted in Table 1, the self-managed protection approach for 5G networks presented herein expose a significant number of innovations. First, it is aware of the topology of the network and thus allows both distributed mitigation and spatial decisions. Second, supports user mobility and multi-tenant traffic isolation in both detection and mitigation even in the edge-to-core network segments which impose a nested encapsulation of network protocols. Moreover, it also allows to conduct different levels of mitigation by stopping the traffic at flow level, user level, and tenant level.

3. Towards a self-managed protection architecture for 5G multi-tenant networks

The proposed architecture is explained in detail in the subsequent sections. First, the characteristics of 5G network traffic are introduced. Second, an overview of the integrated self-managed control loop architecture is presented. Finally, all the components and their main innovations are explained in different subsections: Security Monitoring Agent (SMA), Decision Maker, Action Enforcer, and Flow Control Agent.

3.1. Dynamic 5G traffic

Any flow transmitted end to end in a 5G infrastructure changes its structure across its data path. Fig. 2 shows the packet structure across the data path. A first encapsulation such as Virtual Extensible Local Area Network (VxLAN) or Generic Routing Encapsulation (GRE) allows isolating multi-tenant traffic and is especially relevant in MEC architecture where multi-tenancy is pushed to the end of the network. A second encapsulation such as GPRS Tunnel Protocol (GTP) is used to allow end users' mobility. Most current solutions (Hyun et al., 2017; Sahay et al., 2017; Wang et al., 2015; Giotis et al., 2014) are focused on a pure IP network, instead of a real 5G multi-tenant network as used in this work. To the best of our knowledge, this work presents a first substantial effort to protect large network infrastructures using real 5G multi-tenant network traffic. The proposed architecture is validated against this 5G network traffic to overcome associated challenges, such as multi-tenancy, mobility, and self-adaptation to topology changes. The impact of the change of the flow structure regarding overhead on performance is investigated through empirical experiments in Section 4.

3.2. Self-protection autonomous control loop

The architecture of the self-managed control loop proposed is shown in Fig. 3. It depicts mobile users performing a DDoS attack. There are

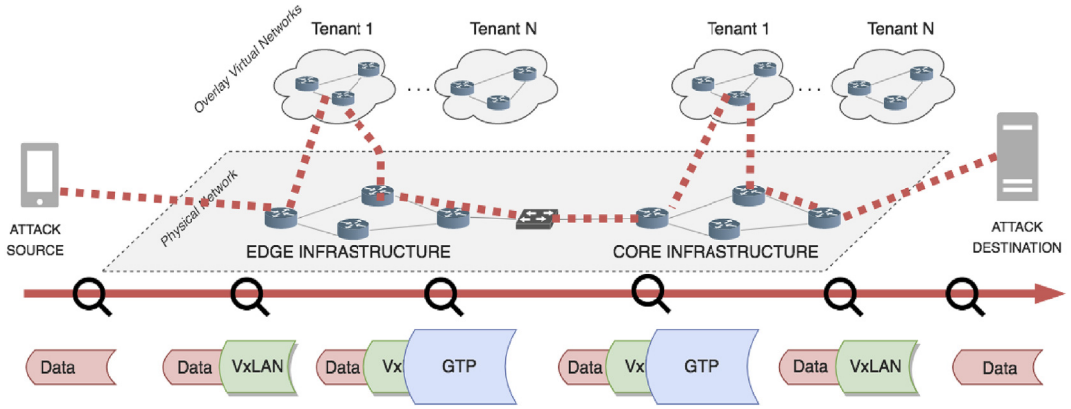


Fig. 2. Flow shape changes across the path.

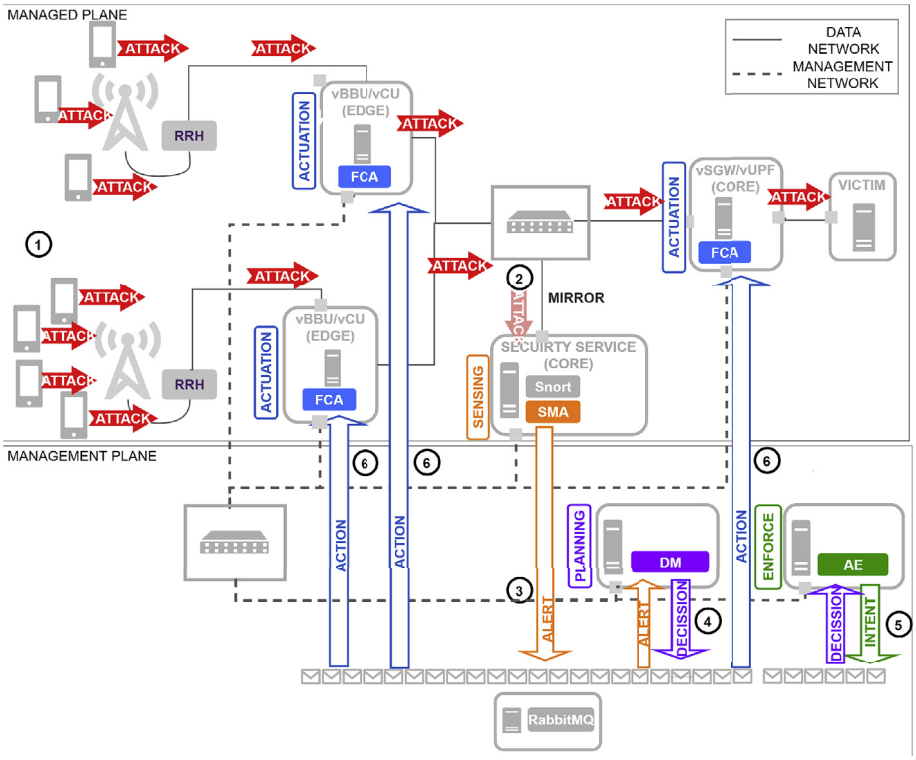


Fig. 3. Functional flow of the proposed architecture.

two networks drawn in this figure: data and management networks. The data network is used for user communications. Management network interconnects all components of the self-managed control loop for management purposes. These are as follows: 1) Security Monitoring Agent (SMA), Decision Maker (DM), Action Enforcer (AE), and several 5G flow control agents (FCAs) deployed in different parts of the network. They are interconnected using the RabbitMQ [3] message bus. Each step of the self-managed loop is labelled with a number in the figure, from 1 to 6, and will be detailed below.

The users of Fig. 3 belong to different tenants, and some of them have been infected to launch an uplink attack, which is represented in step (1). Traffic sent by them passes through both vBBUs/vCUs in the edge of the network and virtual Serving Gateway (vSGW)/vUPF in the core of the network on its way to the victim. Each of those physical locations where virtual machines are location has an FCA installed, used as a 5G actuator to mitigate attacks. The next step (2) mirrors all the traffic passing through the internal switch that interconnects the edge and core network segments to the security service machine.

Both Snort and a Security Monitoring Agent (SMA) have been deployed in this security service machine. Snort performs signature-based detection of malicious traffic and send such alerts to the SMA, which extends Snort capabilities by adding the required 5G and multi-tenant metadata to the alert allowing fine-grained mitigation of the attack. To achieve this purpose, SMA performs the packet classification of the multi-tenant 5G malicious flows. Step (3) takes place when the SMA raises the enhanced alert message to the Decision Maker, which takes a decision. The decision depends on the type of attack, the number of alerts received, and the strategy defined by the administrator of the infrastructure. The decision taken includes what to do (drop, forward or redirect) and where to do it (close to the source, close to the

[3] RabbitMQ is available at https://www.rabbitmq.com/.

destination, at *n* hops of the source, or at *n* hops of the destination). Such decision is sent to Action Enforcer (AE) (see step (4)). AE has the current topology of the network in real time, extracted from the SDN controller deployed to control traffic. Thus, AE converts the decision it into an implementable plan enforceable in concrete locations of the network. The plan is composed by a set of Intents (see step (5)). These are sent to the specific FCA component that will perform the action in step (6). To send the intent to a specific location, the architecture employs a topic-based message bus where the routing key is used to determine the specific receiver of the request.

Close to the source of the attack and close to the destination/victim are key locations to perform the attack mitigation. If the decision is to act close to the source of the attack, the action is carried out by the concrete FCA deployed in the BBU where the attack to be blocked is coming from. If the decision is to act close to the destination of the attack the action would be conducted by an FCA deployed in the server represented as SGW/UPF in Fig. 3. Each deployed FCA is able to stop the flows related to the attack that passes through the data path under their control with minimised impact on the infrastructure, as a result of the fine-grained network control prototyped of this component, able to deal with both multi-tenant traffic and 5g user traffic. It is noted that the actuators as a whole can deal with the distributed nature of the attack and then share the responsibility of mitigating the attacks among them. The splitting of such responsibility is performed by the AE component. Each of the components in the self-managed control loop is explained in details in the following subsections.

3.3. Security Monitoring Agent (SMA)

This SMA sensor has been built as an agent that extends current IDS capabilities. An Intrusion Detection System (IDS) is combined with a 5G traffic classifier to obtain the information about tenants and 5G subscribers needed to provide concrete and effective fine-grained mitigation actions. The capabilities and performance of this sensor are detailed in (Serrano et al., 2018).

For the empirical validation of the proposed work, Snort is selected as the IDS to be extended with SMA agent to provide the new detection capabilities in overlay networks. However, the SMA has been integrated with the Unified2 defacto standard format ,[4] which is a common and open output format for IDS, supported for example in Snort, Suricata, and Zeek/Bro .[5] Thus, Snort can be replaced by any other IDS that provides United2 as output format. Relying on an existing IDS, this architecture will provide support for any adversary model that is current supported by such IDS in terms of attack detection.

The main goal of this module is not to enhance the accuracy of the IDS in terms of false positives and false negatives. In fact, it fully relies on the detection accuracy provided by the IDS being utilised. Depending on the use case or attack type being signature-based or anomaly-based, the IDS could suits better than others; this was the main motivation to make the IDS implementation pluggable. SMA module, instead, enhances the accuracy of the detection in terms of the fine-grain identification of the source of the attack with a multi-tenant 5G network, providing more accurate knowledge of the source of the attack adding information about both the 5G user and tenant.

SMA has been designed and prototypes with three main software components:

IDS Reports Reader: It retrieves events and statistics coming from the IDS. A plug-in approach has been designed to allow working with different IDS.

SMA Flow Classifier: It extracts both tenant and user mobility metadata related to the malicious payload. All such information come from the Unified2 alert. Such an alert includes the packet itself in binary format. That binary representation is parsed and mapped into the SMA data model. Afterwards, a 5G multi-tenant flow classifier extracts the metadata existing about overlay networks, which is needed in the decision-making and mitigation stages. This 5G classifier enables finding and classifying specific data contained in the packet, beyond the traditional header. With this data-driven approach, it is possible to provide a transversal detection of attacks, since it dissects any overlay network and can thus identifying who is being attacked. Thanks to the support provided for nested encapsulation and for all the protocols used in the communications between edge and core networks, this component also allows the detection of attacks in all the network segments of the infrastructure (see Fig. 1).

SMA Alert: It builds and sends the alert messages in JSON (JavaScript Object Notation) format including information about the flows, overlay networks, attack type detected by the IDS, and the exact point (network segment, network equipment, interface, flow direction, etc.) where the attack has been detected.

3.4. Decision maker

The Decision Maker produces a decision indicating what to do (e.g., drop, redirect or mirror the flow) and where to do it, (e.g., close to the source (of attack), close to the destination (of attack), at *n* hops of the source, or at *n* hops of the destination). Such selection is currently implemented employing a policy-based engine that allows administrators to automate the decision-making task. A different strategy can be defined by administrators for each type of attack. In the case of a DDoS attack, the action to perform is DROP the malicious flows, and the place to act is as close to the source as possible.

Fig. 4 depicts the traffic of a regular mobile user that has been infected in a DDoS attack. It shows several traffic types that have been simultaneously sent: video streaming, radio streaming, and a VoIP call. At the same time, an attack is generated from the same user and is shown in the figure as the flow with the highest packet ratio. The figure illustrates how the decision taken (see label A) has ended with only the flow related to the attack being dropped in the BBU (close to the source). Therefore, the other streaming services have not been affected. Consequently, the user would not even notice the attack or the reaction of the system.

3.5. Action enforcer

When the strategic decision has been taken, it is necessary to refine such a decision into a concrete set of actions that are implementable in the managed 5G system to mitigate the attack. For this purpose, the AE component receives the decision and translates it into specific actions to be performed over the infrastructure. The actions (what to do) indicated in this control loop are elementary actions so that they can be directly implemented within the system. However, the location needs to be refined according to the strategy indicated in the decision (e.g., close to the source (the attacker) or close to the destination). The AE maintains the topology of the network in real time achieved by performing a periodic inventory of the network ports and on the forwarding tables of all the L2-capable devices of the data path. Both topology and L2 forwarding tables allow the AE to correlate the information related to the malicious flow reported in the decision with such forward tables to understand where (in which network ports) the attack is happening in the network and from this information identify the closest to the attacker based on ageing of the forwarding entries. Thus, the location strategy (e.g., close to the source, close to the destination) is converted into a specific location (e.g., PC1-E345/eth0) referring to an exact point of the physical infrastructure. The algorithm for the calculation of the

[4] Unified2 specification is available at https://www.snort.org/faq/readme-unified2.

[5] The Zeek Network Security Monitor is available at https://www.zeek.org/.

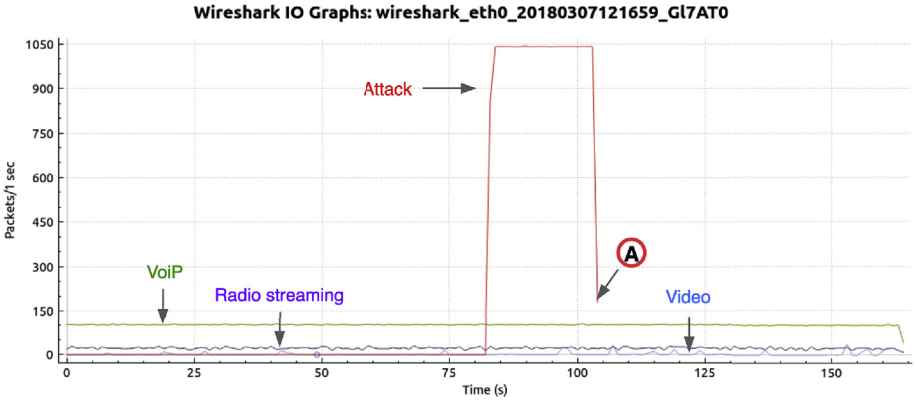


Fig. 4. Stopping an attack whilst protecting legitimate traffic from a user (traffic captured in a BBU).

location is explained in this subsection. The role of the action enforcer is the following:

First, to discover that the actuator has the capability to conduct such action (DROP) over such FLOW.

Second, to discover the location of the actuator that should enforce the action to accomplish the countermeasure to the cause of the alert, in this case, a DDoS attack. The AE has to discover which BBU is receiving this flow and choose where the action should be conducted by a suitable FCA. The AE has access to the inventory of the flows along the data path (reported by SMA) so that it has an instance of this flow for every reference point and the exact structure of the malicious flow at each point of its path. This information is used to change the original structure of the flow reported by the decision into a concrete one that may have (or not) been changed due to the overlay nature of the network. Furthermore, the AE can calculate the exact location of the action because it has access to the forwarding database (FDB) table that is used by Layer 2 devices to store the MAC addresses that have been learned in each port. The exact location of the action is decided in accordance with the metrics associated to the resources of such network port. In case of a DDoS attack, the strategy defined is acting as close to the source of the attack as possible. The metric used in this case is the number of rules already applied in each network port. From empirical results published in (Salva-Garcia et al., 2018) a maximum of 4096 rules is allowed in a software switch. If this limit has already been reached, the next closest location will be calculated, and so on. An explanation of the algorithm follows to calculate where to enforce the action is depicted in pseudocode in Algorithm 1.

3.6. Flow control agent

The FCA is an agent to expose network traffic control functionality. Every computer part of the infrastructure should have an FCA agent installed to control network traffic between physical and virtual machines. It is noted that there are already exist defacto agents for resource monitoring and inventory (such as SNMP agents), flow monitoring (such as NetFlow agents), and network control (such as OpenFlow agents). Such agents exist for years. However, some other parts of the computer do not yet have an agent to expose their functionality to the management plane (e.g., iptables and traffic control for the software data path). In this work, an FCA exposes such capabilities with two different aims: 1) to allow distributed mitigation and 2) to allow a protocol-agnostic API compatible with all these different implementations of the data path. OpenFlow will not work for 5G networks as it is; this has been the main reason for using the FCA in this approach until the standard provides this functionality. The northbound interface of the FCA provides a technology-independent interface and provides an alternative southbound implementation. As one of the southbound implementations, the FCA has been designed to provide modular filtering options implementing Netfilter ,[6] which allows using a set of hooks inside the Linux kernel to provide callback functions for every packet that traverses the respective hook within the network stack. The complexity of the rules enforced depends on the enforcing point, whether it belongs to an overlay network or not, as well as on the protection strategy defined, as will be shown in section 4.

Fig. 5 shows an example of the iptables rule defined by an FCA that has received the Intent produced by the AE to drop a flow that is part of a DDoS attack. The figure shows how the rule includes information about the tenant and user so that only a specific flow will be dropped in the compute where the FCA is deployed. This fine-grained approach means a significant advance for protecting users, tenants, and infrastructures simultaneously.

The distributed nature of the FCAs listening for Intents is a natural way to deal with the distributed nature of the DDoS by performing distributed mitigation of the flows in key location points in the network (e.g., close to the source), to protect the infrastructure against unnecessary flooding along any of the network segments.

4. Validation

The purpose of the experiments is to validate the effectiveness of the proposed autonomous control loop for 5G multi-tenant networks. Three key features must be validated: First, the support for multi-tenancy and 5G mobile; Second, the self-adaptation to any changes that could occur in the network topology; Third, acceptable reaction time of the autonomous control loop in case of a DDOS attack.

4.1. Attack description

For an empirical validation of the presented architecture, it has been decided to use a UDP flooding attacks (Zargar et al., 2013), coming from 5G users and passing by the 5G multi-tenant network, as an example to showcase the capabilities of the architecture. However, the authors are confident that this architecture will work for any attack that can be detected by the IDS deployed (e.g., Suricata or Snort). The main purpose of this attack is to overwhelm random ports on the targeted host. The targeted host checks for applications associated with these datagrams and when no application is found, it sends back an ICMP Destination Unreachable packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients. Thus, for a vast amount of UDP packets, the

[6] Netfilter project is available at http://www.netfilter.org.

Algorithm 1 Algorithm to find location.

```
input  : affected flow sample
output: location to act over affected flow
while locationFound ≠ true do
    /* iterate over all flow samples                                   */
    for each f ∈ flowInventory do
        /* iterate over all ifaces for f                               */
        for each i ∈ ifacesInventory do
            /* iterate over all fdb entries                            */
            for each fdb ∈ fdbInventory do
                if ( ft.flowId = affectedFlowSample.flowId and
                  ft.referencePointId =
                  affectedFlowSample.referencePointId and
                  ft.referencepointId = iface.id and
                  i.getId = fdb.devicePortId and ( fdb.mac = ft.srcMac
                  or fdb.mac = ft.srcOutMac or i.mac = ft.srcMac or
                  i.mac = ft.srcOutMac ) ) then
                    device ⟵ iface.device;
                    if CurrentRulesInstalled < MAX_RULES then
                        targetFlow ⟵ flow;
                        targetiface ⟵ iface;
                        return location;
                    else
                        if Intent was close to source then
                            get a sample of this flow in a further location;
                        else
                            get a sample of the flow in a closer location;
```

```
Chain FCA_74AB33D8_2 (1 references)
 pkts   bytes target  protopt  in  out   source   destination
    2     464 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x6e&0xffff=0x50&&0x6e&0xffff0000>>0x10=0x8ace" /* {Udp} */
   11    5698 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x60&0xff=0x11&&0x66=0xa010002&&0x6a=0xa080002" /* {Ip4} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x52=0x1" /* {Gtp} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x46&0xffff=0x868&&0x46&0xffff0000>>0x10=0x868" /* {Udp} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x38&0xff=0x11&&0x3e=0xc00c0001&&0x42=0xc00c0002" /* {Ip4} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x1f=0x285c" /* {Vxlan} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x14&0xffff=0x12b5&&0x14&0xffff0000>>0x10=0x9fb0" /* {Udp} */
    0       0 RETURN     all  --  *   *  0.0.0.0/0   0.0.0.0/0   u32 ! "0x6&0xff=0x11&&0xc=0xa010002&&0x10=0xa080002" /* {Ip4} */
    3    1554 LOG        all  --  *   *  0.0.0.0/0   0.0.0.0/0   limit: avg 2/day burst 5 LOG flags 0 level 7 prefix "BBU-2=74AB33D8 "
  390  202020 DROP       all  --  *   *  0.0.0.0/0   0.0.0.0/0
```

Fig. 5. Example of an iptables rule executed in one BBU to DROP every packet of a flow that belongs to double encapsulated traffic.

host resources become fully exploited, which could lead to the inaccessibility of services. The behaviour of the attacker has been considered constant over time in some aspects and variable in others. The variable features considered are the bandwidth of the attack and the number of bots that compose the botnet. These features are essential when defining the DDoS adversary model since they indicate the magnitude of damages. Since the UEs are distributed among different edges of the network, this attack is a distributed one. The maximum number of bots in these experiments has been marked by the limitation of running the experiments in the same machine. Bonesi [7] has been used for the emulation of the UDP flooding attack (i.e., attacker tool). For the experiments in this work, the attacker tool is installed in each UE. Experiments generate UDP flooding traffic with different packet rates and payload sizes to obtain attacks with different bandwidth (12.5, 25, 50, and 100 Mbps per users).

4.2. Validation testbed

To validate the proposed architecture and prototypes, Common Open Research Emulator (CORE) [8] is employed as a Kubernetes-like large-scale container-based deployment tool. CORE provides an Infrastructure-as-a-service (IaaS) stack to allow the deployment of a large number of UE nodes to generate UDP Flooding Attacks in different 5G topologies using containers. Once the scenario of the infrastructure is created, our multi-tenant network control configures the Open-VSwitch 2.9 with VXLAN for tenant isolation and deploys SGSNEmu to create LTE/5G User Equpment (UE) connections to the 5G network using GTP allowing the emulation of user mobility. To clarify, this architecture has been validated against a fully operational 5G multi-tenant infrastructure where eight real UEs are connected to the 5G infrastructure using OpenAirInterface [9] stack. To scale up to 256 UEs, we have decided to emulate the rest of devices.

Different scenarios such as the one shown in Fig. 6 have been generated and executed, to test the scalability and flexibility of the proposed autonomous control loop. All scenarios share a common base topology composed of two networks: one data path network, and one management network. In Fig. 6, the data network is represented in red and the management network is represented in green. The management network connects the nodes that contain the modules that compose the self-managed control loop, specifically SMA, Decision Maker, AE, and FCA actuators. The FCA is deployed in all the BBUs of each scenario as well as in each SEDGER-n where the SGW/UPF is deployed to enable

[7] BoNeSi: DDoS Botnet Emulator is available at https://github.com/markus-Go/bonesi.

[8] Common Open Research Emulator (CORE) is available at http://www.nrl.navy.mil/itd/ncs/products/core.

[9] OpenAirInterface is available at http://www.openairinterface.org/.

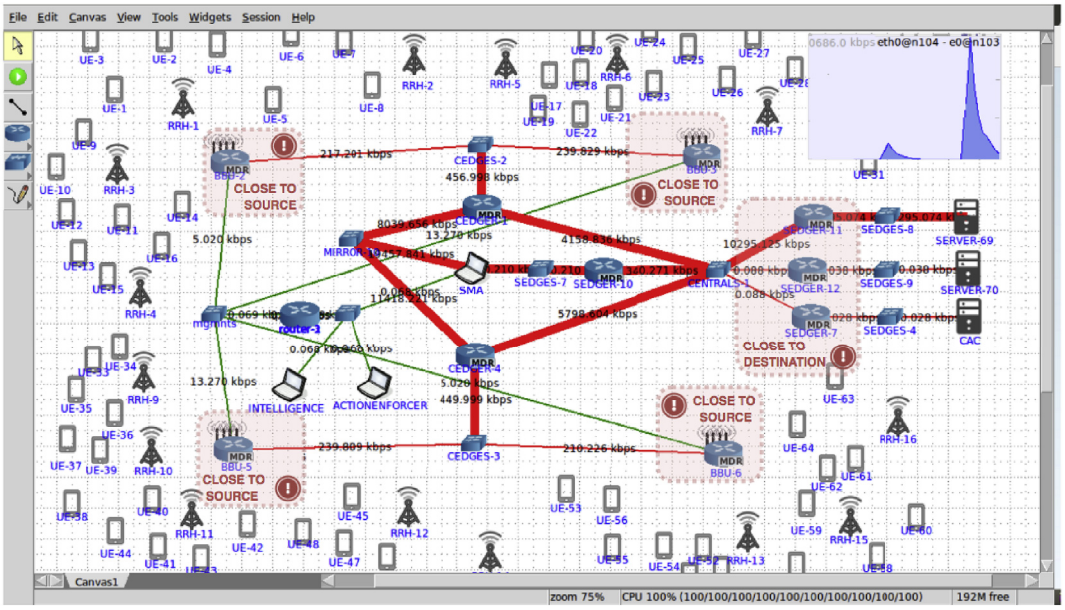


Fig. 6. 64 mobile users (UE-*n*) are attacking the same victim "SERVER-69" and the attack is being stopped by the self-managed loop presented in this paper.

to conduct actions close to the source and the destination of the attack respectively. Fig. 6 shows an example of a scenario with 64 UE nodes, represented by mobile devices which act as attackers. Those UE nodes are connected to an RRH and mobility between antennas is emulated to achieve a realistic 5G/LTE network without the need to purchase all the UEs for the experiment. A BBU can be shared by different RRHs, as shown in Fig. 6 where there are 16 RRHs for four BBUs. The BBUs are connected to the core network through a 1 Gbps bandwidth link. On the right centre of the figure are the victims of the attacks, represented as servers. In the case shown in Fig. 6, the attack involves all the UE nodes attacking the same victim at the same time, labelled as SERVER-69. All the traffic that passes through the data network is mirrored to the security service node that contains the SMA, labelled as SNORT node, to intercept and analyse the traffic between the edge and the core network segments. Therefore, all the traffic passing through the nodes named as CEDGER- (Cui et al., 2016; Neves et al., 2017) in Fig. 6, is mirrored to the node named as SNORT using predefined static iptables rules. Thus, Snort is configured to trigger an alert in the case of an attack and then processed by the SMA. CEDGER-n nodes that represent the edge segment are connected through a CENTRAL node to the core segment, which is represented by the nodes named as SEDGER- (Hu et al., 2017; Bhunia and Gurusamy, 2017; Ozcelik et al., 2017). Then, the victims are located in a different server named as SERVER-[69,70].

The scenarios have been executed on an Intel Core i7 CPU 4.20 GHz, 32 GB RAM hosting a Virtual machine with 16 GB RAM and 4 cores, and Linux 4.12 Kernel. To evaluate the system, the reaction time has been measured in different scenarios. For that purpose, the overhead in milliseconds has been measured from the moment where Snort has triggered the alert to the moment when the attack is stopped. All the results have been executed with the same Snort configuration, which imply, the same rules and threshold configurations for consideration. Different packet rates, bandwidths and number of encapsulations have been executed. For a specific experiment, every UE node has a different source and destination IPs have to correspond to the ones defined for each attacker and victim.

4.3. Functional validation results

It is necessary to protect the network against attacks in all the network segments of the 5G multi-tenant network. This work considers a tenant/operator as each of the Communication Service Providers that share the same physical infrastructure that belongs to an Infrastructure Service Provider. Acting at flow level has less impact on the quality of service of the shared infrastructure since this strategy avoids any collateral damage to the infrastructure. The user that was sending the flow is not even affected by the decision taken and only the malicious flows are dropped. At the same time, this fine-grained approach is less scalable. However, acting at the user level has a higher impact, since it affects all the traffic of a specific user, although, at the same time, it avoids collateral damages for the rest of the users connected to a BBU or that belong to a specific service provider. Finally, acting over a complete tenant is a very drastic decision and has a very high impact since it would affect all the traffic on that tenant.

The scenario shown in Fig. 6 has been used in this experiment. An attack is sent from different UE nodes belonging to different tenants to the same victim. The traffic passing through the BBU-2 node shown in Fig. 6 is shown in Fig. 7. To be concrete, the traffic from UEs 1–4 are passing through this BBU-2. UE-1 and UE-2 belong to tenant A (TA), while UE-3 and UE-4 belong to tenant B (TB). Only UE-1 is sending malicious traffic as the purpose is to validate the different ways to protect the network. Both TCP and UDP traffic is generated from all UEs. UE-1 traffic also contains the malicious UDO flooding attack.

Fig. 7 shows the results of the experiments to test the capability of the system to detect and mitigate a UDP Flooding Attack at three different levels of granularity. The three columns available in Fig. 7 (Fig. 7(a)–7(c)) represent a different levels of granularity in the mitigation decision and each row represents each of the four UE nodes analysed in the experiment.

In Fig. 7(a), the system decides to stop the attack close to the source by dropping just the malicious flow. By using the hash of the Flow Id associated with the malicious flow, TEID_1, and VNID_A, the system is capable to stop the exact malicious flow seamlessly. The only malicious flow shown in U1_TA is indicated in the plot by an arrow and shows the highest packet rate. Label A indicates the moment the decision is enforced into the FCA. It is noted that on time A, the malicious flow is stopped in UE1. The rest of the flows of UE1 are not stopped. The same happens to all the traffic of the rest of the users. (see in Fig. 7 how the attack affects the rest of the traffic), although when the attack is stopped the user would not have realised that an attack was sent from

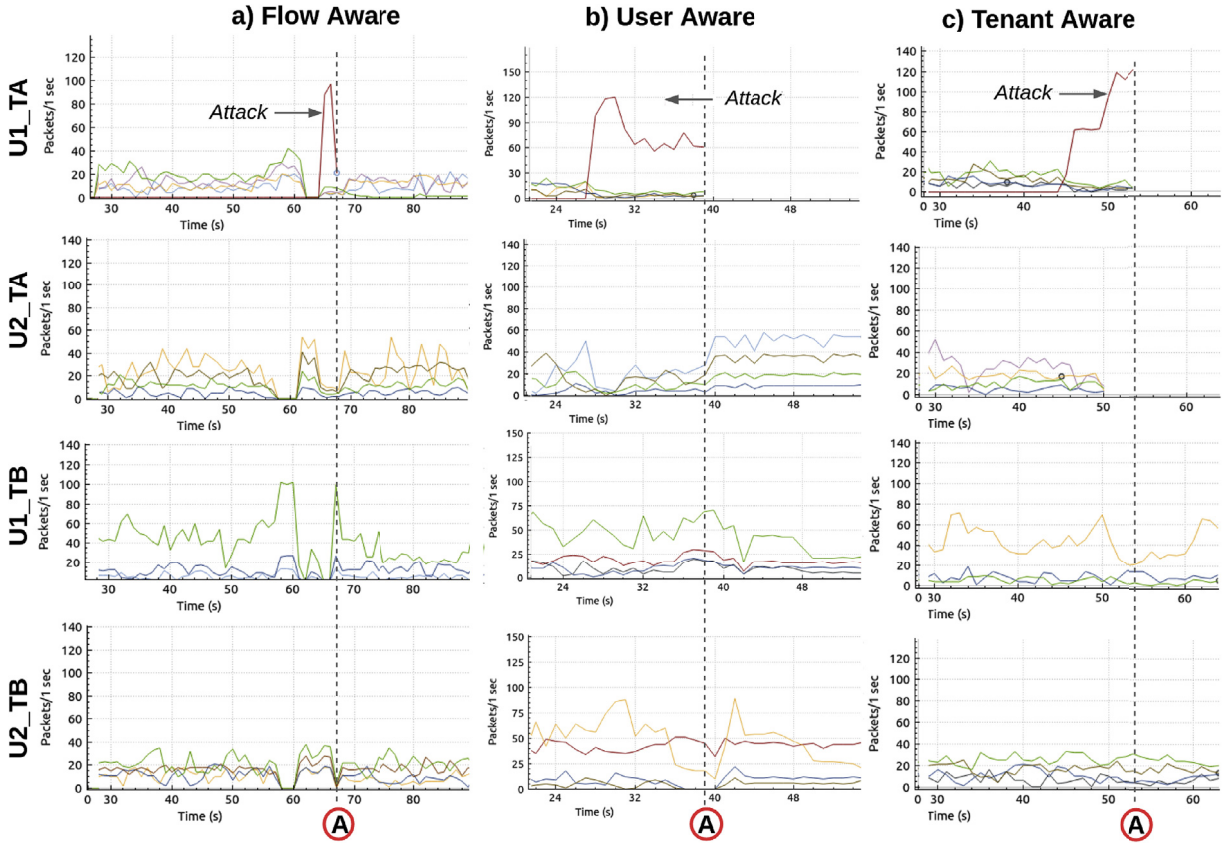


Fig. 7. Traffic Captures of 4 users passing through the same BBU. Two users belong to tenant A and twp to tenant B. Rows named as Un_Tx, which means user *n* of tenant *x*. The first user is always the one who sends the attack. a) stopping the malicious flow (Flow Aware); b) stopping every flow of the user that is sending the attack (User Aware); c) stopping all the flows from all the users of a tenant (Tenant Aware).

his/her device and that any flow has been dropped.

In Fig. 7(b), the system decides to drop close to source all the traffic from the user that is sending the attack. By using the TEID_1 and VNID_A, the system can stop all the traffic from that user, without affecting the rest of the users of that tenant. The figure shows how all the flows coming from UE1 have been dropped at time A onwards, but not the ones from UE2 that belongs to the same tenant A the ones from UE3 and UE4 that belong to tenant B. Thus, in a real scenario where the attacker has infected UE-1 and persists in the attack by changing its signature, the Decision Maker will conclude to drop all the traffic of this user to avoid collateral damage to the infrastructure. With this mitigation of the attack, this user, and only this one, would be affected cutting its own traffic, but the rest of the legitimate users would not notice any notable change in the behaviour of the network.

In Fig. 7(c), the system decides to stop all the traffic coming from a tenant. By using the VNID_A, all the traffic coming from the tenant can be dropped. The figure shows how all the flows of the users of tenant A, which are UE1 and UE2 that have been dropped at time A onwards. However, the traffic of the users of tenant B, UE3 and UE4, is not affected by the countermeasures carried out by the system.

The previous experiments demonstrate how the solution presented is able to provide a self-managed defence supporting 5G multi-tenancy and overlay networks.

4.4. Scalability and flexibility results

To demonstrate the scalability and flexibility of the architecture proposed, the first set of experiments analyse the influence of the number of attackers in the reaction time of the autonomic control loop with no human intervention as well as the bandwidth of the attack. The second set analyses the influence of the complexity of the flow structure and the number of attackers in the reaction time. The third sets analyse the influence of the complexity in the topology of the network by fixing the number of attackers and complexity of the flow structure to the highest values of the last two experiments (256 attackers and double encapsulation).

The network scenarios used for the experiments are represented in Table 2. It shows the number of nodes for each type (UE, RRH, BBU, CEDGE, SEDGE, and SERVER), following the same connections scheme as the one depicted in Fig. 6. The two columns in the left show the number of attackers and actuators for each scenario. The first eight rows of this table correspond to the scenarios used for the first and second sets of experiments, while the five remaining ones correspond to scenarios used in the third sets of experiments. At the same time, different input traffic variants have been used as the source of the attack. The variants are the complexity of the structure of the packet sent and the bandwidth of the attack.

For a better understanding, the time sequence has been divided into the sub-tasks involved in the autonomous control loop and measured in the experiments. Thus, the SMA time reflects the time from receiving the Snort event until the Alert is sent through the management network; the Decision Maker time is the time from receiving the Alert until the Decision is sent; the AE time is the time from receiving the Decision until the Intent is sent; finally, the FCA time is the time from receiving the Intent until the rule is first matched so the attack is mitigated and the Action from the FCA is sent to inform such Intent has been already enforced. All results are represented in stacked bars where each colour represents the time invested by one module of the self-managed loop: SMA, Decision Maker (DM), Action Enforcer (AE), and FCA.

Table 2
Topologies definition by node types per scenario.

nAttackers	nFCA	nCEDGE	nBBU/CEDGE	nRRH/BBU	nUE/RRH	nSEDGE	mSERVER
2	2	1	1	1	2	1	1
4	2	1	1	2	2	1	1
8	2	1	2	2	2	1	1
16	5	2	2	2	2	1	1
32	5	2	2	4	2	1	1
64	9	2	4	4	2	1	1
128	17	4	4	4	2	1	1
256	33	8	4	4	2	1	1
256	17	4	4	4	4	1	1
256	33	8	4	4	2	1	1
256	65	16	4	2	2	1	1
256	129	32	4	2	1	1	1
256	257	64	4	1	1	1	1

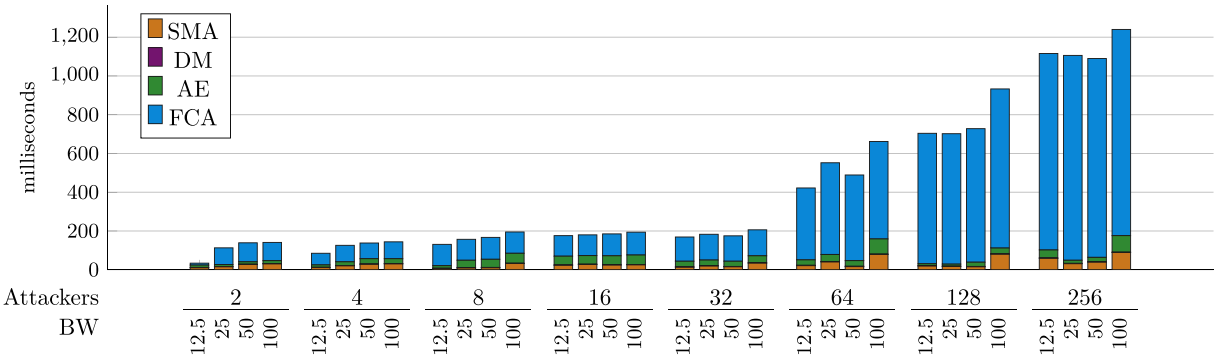


Fig. 8. Results of the reaction times of the proposed solution for the different number of simultaneous attackers and different bandwidths.

4.4.1. Results by attack intensity and number of attackers

Fig. 8 shows the reaction time of the self-managed loop ranging different attack bandwidths to compare the results under different stress conditions directly related to the intensity of the attack to measure the scalability of the system. The stacked bars show the time invested by each component to conduct its function. From bottom to top, the fragments correspond to the SMA, the Decision Maker, the AE, and the FCAs. It is noted that the time invested by the decision maker is inappreciable in the figure for all the scenarios analysed, being always a maximum of two milliseconds.

Bandwidth ranging from 12.5 to 100 Mb have been used for the experiments with GTP over VxLAN to use the real traffic passing between BBU and UPF in a multi-tenant 5G architectures. Fig. 8 shows that the system gets more and more saturated when the number of attackers is increased. The more attackers there are, the more flows the system have to manage. However, the execution time to detect, respond and mitigate the attack is directly proportional to the increase in the bandwidth of the attacks. These results prove the scalability of the system regarding bandwidth. It is noted that in the most stressed scenario 256 attackers at 100 Mbs are generating an attack of 25.6 Gb/s running on an environment with 256 containers allocated only in one physical machine, which is a very reasonable validation of scalability results and even under such stress levels the response time of the complete self-managed loop is less than 1.2 s.

4.4.2. Results by flow complexity and number of attackers

The same experiment has been run to investigate the influence of the complexity of the flow in the performance of the whole system. The flow changes across its path, with different encapsulations added or removed. The more levels of encapsulation, and the greater the size of the packet is, the more information extracted by the classifier module of the SMA and enforced by the FCA is. To stress the proposed control loop, traffic with different complexities is tested: pure IP traffic, GTP over IP traffic (5G traffic), VxLAN over IP traffic (Multi-tenant traffic), and VxLAN over GTP over IP traffic (5G Multi-tenant traffic). For this purpose, four different network traffic kinds have been used for each of the experiment tested in this section; all of them were created with a bandwidth of 25 Mbps. The number of attackers has been ranging exponentially between two and 256. Fig. 10 shows the reaction time of the system for different levels of encapsulation and a different number of attackers. This figure shows how the number of attackers influences the saturation of the system. However, the complexity of the flow barely affects the reaction time of the system. In the worst case, which is an attack originated from all 256 UE nodes with double encapsulation, the reaction time of the system is still below 1.2 s.

4.4.3. Results by topology complexity

These experiments investigate the influence of the complexity in the network topology by scaling up the number of CEDGE nodes, which are the nodes that connect the BBUs with infrastructure. Hence, increasing the number of CEDGE nodes will increase the number of BBUS, and consequently, more FCAs will be running. This increases in FCA to make the decision to act close to the source, that is more difficult a decision to be taken. The number of UE nodes in the botnet has been fixed to 256 (see bottom rows of Table 2). The bandwidth of the attack sent from each UE is 25 Mb. Moreover, it can be assured that the more CEDGE nodes there are, the fewer malicious flows related to the generated attack will be received by each CEDGE node. It results in a lower load for each FCA deployed in the infrastructure, having fewer rules to be added to control the attack. Fig. 9 shows the reaction time when the numbers of CEDGE node is ranged. One can observe an almost constant behaviour of the loop response time. The time consumed by the SMA and Decision Maker is almost the same for the five scenarios. This is the expected behaviour. Although more mirror rules have been introduced to mirror the traffic from each CEDGE, the number of malicious flows is the same, due to the fixed number

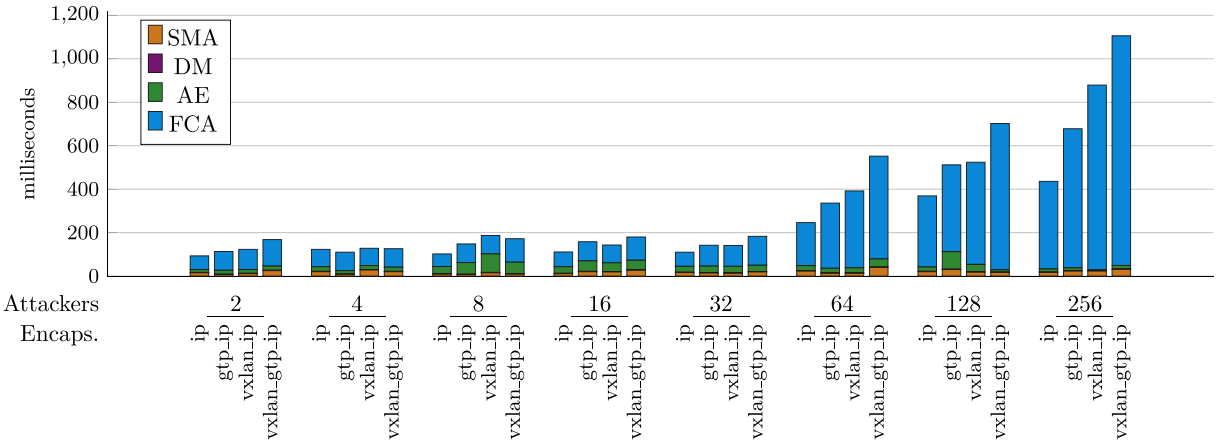


Fig. 9. Results of reaction time of the proposed solution for different number of simultaneous attackers and different levels of encapsulations.

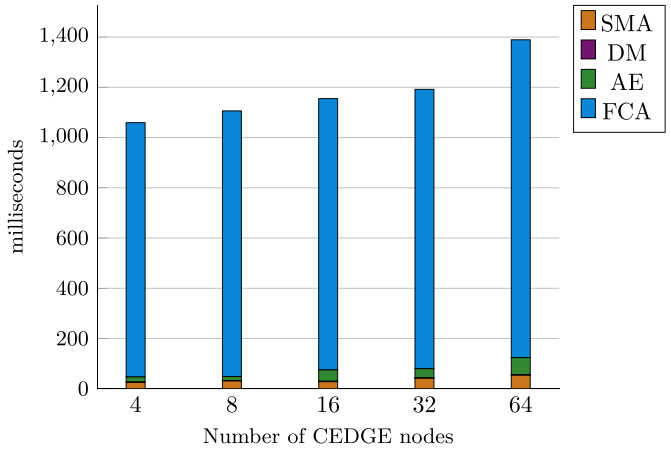


Fig. 10. Results of reaction time of the proposed solution for different number of CEDGE nodes and an attack launched from a botnet of 256 attackers sending a 25 Mb attack.

of UE nodes in the botnet. Thus, Snort is generating the same number of alerts and the same number of decisions are being produced. A slight time variation can be noted for the AE, which takes more time to build the intent when the number of possible locations increases. Analogously, it can be noted a time increase in the FCA. Overall, it shows that an exponential scaling up in the complexity of the topology only provides some hundreds of milliseconds of overhead in the response time of the autonomous loop, which validates the scalability of our approach.

All the previously described experiments have successfully validated the key features defined at the beginning of this paper: to achieve an autonomic network management control loop that self-protects multi-tenant 5G infrastructure against DDoS attacks without human intervention; to provide selective protection against DDoS attack providing user-aware, tenant-aware and flow-aware mitigation strategies; to be able to deal with the dynamic creation of overlays network whilst maintaining the detection and mitigation of the attack over such newly created networks; and finally, to be able to determine automatically not only the *how* but also the *where* to mitigate the attack.

Within the 5G verticals industries such as manufacturing, transport, logistics, self-driving, energy, massive IoT, and entertainment as well as public services such as smart cities, public health and education, those achievements would have a different impact. There are some services where security is a critical concern, and where the achievements of this work would imply a high impact. For instance, in health, transport or industrial automation the possibility of manual intervention to detect and mitigate a DDoS attack in a timely manner is not viable. Thus, the development of an autonomic management of the network, like the one presented in this paper, becomes indispensable. Short reaction time is crucial to guarantee the availability of the service.

5. Conclusion

A novel architecture to self-protect 5G multi-tenant networks against DDoS attacks has been proposed with support for edge computing that is able to simultaneously protect infrastructures, tenants, and users. It is composed by a 5G Security Monitoring Agent, a Decision Maker, an AE and a 5G Flow Control Agent actuator. The framework has been tested against a real DDoS attack in a 5G infrastructure. The results have proved that the autonomic self-managed loop fills the gaps of state-of-the-art. It has been proved that the autonomic loop is able to apply fine-grained countermeasures to mitigate the attack acting just over the malicious flows, avoiding affecting other users or tenants.

The proposed architecture enables awareness of topology for actuation, which makes it possible to work with logical locations, such as being close to the source of the attack or close to the destination, abstracting the physical topology of the infrastructure. The cognitive layer decides how and where to mitigate the attack based on awareness of the dynamic network topology.

Scalability experiments have proved that the self-managed loop handles effectively the bandwidth of the attack and the complexity of packet structures as well as the topology complexity by reacting and mitigating the attack in around one second for double encapsulated traffic with an attack launched from a botnet of 256 devices simultaneously sending malicious traffic of 100 Mbps of bandwidth. The results have demonstrated that the proposed solution can protect the forthcoming 5G networks.

The architecture proposed in this work is entirely modular, being adaptable to any new modules to be added. Moreover, this research could be applied to new use cases for the optimisation of the network functioning. New sensors and actuators can be added for a new use case, and new rules and policies could be applied to define a different strategy.

Declaration of interests

None.

Acknowledgment

This work was funded by the European Commission under Grant Agreement H2020-ICT-2016-2/761913 SLICENET (End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks) and by the UWS 5G Video Lab project.

References

5G PPP Architecture Working Group, 2016. View on 5G Architecture. White paper, no. .

Adat, V., Gupta, B.B., 2017. A DDoS attack mitigation framework for internet of things. In: 2017 International Conference on Communication and Signal Processing (ICCSP), vol. 4. IEEE, pp. 2036–2041.

Ayoubi, S., Limam, N., Salahuddin, M.A., Shahriar, N., Boutaba, R., Estrada-Solano, F., Caicedo, O.M., 2018. Machine learning for cognitive network management. IEEE Commun. Mag. 56 (1), 158–165.

Bhunia, S.S., Gurusamy, M., 2017. Dynamic attack detection and mitigation in IoT using SDN. In: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), vol. 11. IEEE, pp. 1–6.

Buragohain, C., Medhi, N., 2016. FlowTrApp: an SDN based architecture for DDoS attack detection and mitigation in data centers. In: 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), vol. 2. IEEE, pp. 519–524.

Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., Zheng, X., 2016. SD-Anti-DDoS: fast and efficient DDoS defense in software-defined networks. J. Netw. Comput. Appl. 68, 65–79.

Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., Maglaris, V., 2014. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput. Network. 62, 122–136.

Hu, D., Hong, P., Chen, Y., 2017. FADM: DDoS flooding attack detection and mitigation system in software-defined networking. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, vol. 12. IEEE, pp. 1–7.

Hyun, D., Kim, J., Hong, D., Jeong, J.P., 2017. SDN-based network security functions for effective DDoS attack mitigation. In: 2017 International Conference on Information and Communication Technology Convergence (ICTC), vol. 10. IEEE, pp. 834–839.

Kim, J., Kim, D., Choi, S., 2017. 3GPP SA2 architecture and functions for 5G mobile communication system. ICT Exp. 3 (1), 1–8.

Morales, L.V., Murillo, A.F., Rueda, S.J., 2015. Extending the floodlight controller. In: 2015 IEEE 14th International Symposium on Network Computing and Applications, vol. 9. IEEE, pp. 126–133.

Neves, P., Cal, R., Costa, M., Gaspar, G., Alcaraz-Calero, J., Wang, Q., Nightingale, J., Bernini, G., Carrozzo, G., Valdivieso, ., Villalba, L. J. Garca, Barros, M., Gravas, A., Santos, J., Maia, R., Preto, R., 11 2017. Future mode of operations for 5G. The SELFNET approach enabled by SDN/NFV. Comput. Stand. Interfac. 54, 229–246.

Ozcelik, M., Chalabianloo, N., Gur, G., 2017. Software-defined edge defense against IoT-based DDoS. In: 2017 IEEE International Conference on Computer and Information Technology (CIT), vol. 8. IEEE, pp. 308–313.

Sahay, R., Blanc, G., Zhang, Z., Debar, H., 9 2017. ArOMA: an SDN based autonomic DDoS mitigation framework. Comput. Secur. 70, 482–499.

Salva-Garcia, P., Alcaraz-Calero, J.M., Wang, Q., Bernabe, J.B., Skarmeta, A., 2018. 5G NB-IoT: efficient network traffic filtering for multitenant IoT cellular networks. Secur. Commun. Netw. 2018, 1–21.

Serrano, A., Pervez, Z., Alcaraz, J., Khattak, A., 2018. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. Comput. Secur. 79, 132–147.

Wang, F., Wang, H., Wang, X., Su, J., 2012. A new multistage approach to detect subtle DDoS attacks. Math. Comput. Model. 55, 198–213.

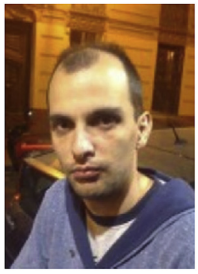
Wang, B., Zheng, Y., Lou, W., Hou, Y.T., 10 2015. DDoS attack protection in the era of cloud computing and Software-Defined Networking. Comput. Network. 81, 308–319.

Yan, Q., Huang, W., Luo, X., Gong, Q., Yu, F.R., 2018. A multi-level DDoS mitigation framework for the industrial internet of things. IEEE Commun. Mag. 56 (2), 30–36.

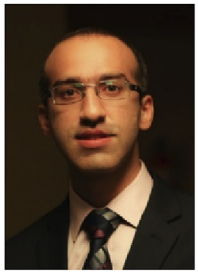
Zargar, S.T., Joshi, J., Tipper, D., 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutorials 15 (4), 2046–2069.

Ana Serrano Mamolar is a PhD candidate at the University of the West of Scotland (UWS), where she is involved in the H2020 5G-PPP Phase I SELFNET project. Her main interests include network management, cognitive control plane and cyber-security in MEC and 5G networks.

Pablo Salvá García is a PostDoctoral Researcher at UWS, where he is involved in the H2020 5G-PPP Phase II SLICENET project. His main interests include network management, cognitive control plane, software data paths and network video delivery in MEC and 5G networks.



Enrique Chirivella-Perez is a PostDoctoral Researcher at UWS. He is currently involved in the H2020 5G-PPP Phase 2 SLICENET project. His main interest includes network management, service automatic deployment and SDN in MEC and 5G networks.



Zeeshan Pervez is a Reader (Assistant Professor) at UWS. He is involved in the H2020 5G-PPP Phase 2 SLICENET project. His research interests include cyber-security and cyber-privacy in IoT, Cloud Computing, MEC and 5G networks.

Jose M. Alcaraz-Calero is a Professor at the UWS. He is the technical co-coordinator of the EU H2020 5G-PPP Phase I SELFNET and Phase II SliceNet projects. His current research interests focus on 5G mobile networks. Corresponding Author (jose.alcaraz-calero@uws.ac.uk)

Qi Wang is a Professor at the UWS. He is the technical co-coordinator of the EU H2020 5G-PPP Phase I SELFNET and Phase II SliceNet projects. His current research interests focus on 5G mobile networks.