Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks

Serrano Mamolar, Ana; Pervez, Zeeshan; Alcaraz Calero, Jose M.; Masood Khattak, Asad

Published in:
Computers and Security

DOI:
10.1016/j.cose.2018.07.017

Published: 30/11/2018

Document Version
Peer reviewed version

Towards the Transversal Detection of DDoS Network Attacks in 5G Multi-Tenant Overlay Networks

Ana Serrano Mamolar, Zeeshan Pervez, *Senior Member, IEEE*, Jose M. Alcaraz Calero, *Senior Member, IEEE,* Asad Masood Khattak

***Abstract*—Currently, there is no any effective security solution which can detect cyber-attacks against 5G networks where multitenancy and user mobility are some unique characteristics that impose significant challenges over such security solutions. This paper focuses on addressing a transversal detection system to be able to protect at the same time, infrastructures, tenants and 5G users in both edge and core network segments of the 5G multi-tenant infrastructures. A novel approach which significantly extends the capabilities of a commonly used IDS, to accurately identify attacking nodes in a 5G network, regardless of multiple network traffic encapsulations, has been proposed in this paper. The proposed approach is suitable to be deployed in almost all 5G network segments including the Mobile Edge Computing. Both architectural design and data models are described in this contribution. Empirical experiments have been carried out a realistic 5G multi-tenant infrastructures to intensively validate the design of the proposed approach regarding scalability and flexibility.**

***Index Terms*— DDoS Attack, Multi-tenant, 5G Network, Security, Intrusion Detection System**

I. INTRODUCTION

Fifth-generation (5G) networks target a variety of new use cases, such as ultra-high definition video, self-driving cars, smart cities (internet-of-things), and remote telesurgery, all of them with a variety of specific requirements such as reliable communications, high data rates and low latency [1]. The novel 5G architecture should provide new capabilities not limited to voice and data but also for those new use cases mentioned and beyond. The natural movement towards the digitalisation of the society and the usage of 5G in critical applications like healthcare, transportation and industry has exacerbated the importance of the security of the underlying networks which empowers 5G. The Next Generation Mobile Network Alliance (*consortium of over 80 mobile operators, vendors, and research institutes*) explicitly highlighted the importance of security of 5G network "*enhanced performance is expected to be provided along with the capability to control a highly heterogeneous environment, and with the capability to, among others, ensure security and trust, identity, and privacy*" [2].

The protection of the network against any forms of cyber-attacks is of paramount importance [3], as they can cripple critical services – the recent attacks to UK's National Health Service [4] and telecommunication service provider [5] are clear evidence of this fact. During the last years, Distributed Denial-of-Service (DDoS) attacks have made their mark. In 2015, 50% of the companies surveyed by Kaspersky experienced some level of disruption due to a DDoS attack [6]. In 2016, the volume of DDoS attack traffic increased to around 600Gps, according to the worldwide infrastructure security report (WISR) [7]. With technological advancement, cyber attacks are becoming sophisticated and elusive. Recently, a DDoS attack called Mirai leveraged insecure IoT services to trigger a massive DNS DDoS attack that affected Dyn [8]. Such attack caused major Internet platforms and services in Europe and US to be unavailable. Since DDoS attacks are becoming subtle, it is getting more and more difficult to detect them, and even more difficult to be mitigated [9]. In this sense, when designing 5G networks, architectural considerations should go together with security considerations. Likewise, security considerations are expected to influence architectural decisions. 5G networks will increase both the capacity and speed, so it will increase the demand for traffic, consequently leading to more wide and intense security threats [10].

In this context, softwarisation is a key innovation coming with the 5G architecture where the different architectural elements of the 5G architectures can be running in software to enhance the flexibility of the 5G architecture. This new paradigm allows network operators the use of cloud infrastructures and mobile edge computing reducing both capital and operational costs by sharing resources between different network operators. Software-defined networking (SDN) and virtualisation technologies provide to network operators the capabilities to flexibly manage their hardware allowing them to create different isolated overlay networks with security boundaries between them for effective and secure sharing of physical resources. This capability of creating different isolated overlay networks which are sharing the same networking devices to implements multi-tenancy security in cloud infrastructures is mainly achieved by employing different encapsulation protocols. Currently, Virtual Extensible Local Area Network (VxLAN) and Generic Routing Encapsulation (GRE) protocols are two widely used alternatives. VxLAN [11] provides an overlays Layer 2 network according to the OSI reference model; whereas, GRE [11] provides an overlay Layer 3 network. Both make use of a tunnel identification which is used to identify the owner of the overlay network, allowing effective management and isolation of the traffic. Mobile

networks also make use of encapsulation protocols to allow fast user's mobility between antennas [12]. 5G networks are not an exception, and as is considered an evolution of 4G Long Term Evolution (LTE) networks, the tunnelling protocol used for this purpose is expected to be the General Packet Radio Service (GPRS) Tunnelling Protocol (GTP) [13].

Fig. 1 shows a simplified representation of different network segments of a 5G network. Radio Access Network (RAN) is typically associated with the deployment of Antennas and Remote Radio Heads (RRH) on top of buildings. Mobile Edge Computing Network is typically associated to the last mile where traditional Cost-of-the-Sell (COST) computers are allocated to process data close to the final user and where architectural elements such as Base Band Units (BBUs) are allocated, especially when a Cloud-RAN deployment is carried out. Core Network is where all the centralised parts of the 5G infrastructure are deployed to get access to users to other networks.

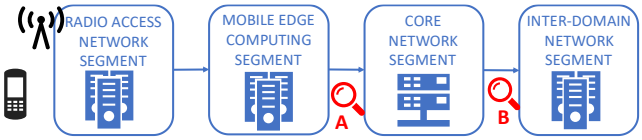


Fig. 1. 5G multi-tenant network segment

Fig. 2 represents a more detailed illustration of Fig. 1, where the reader can see the typically key architectural elements deployed in the core segment of the network. Authentication Server Function (AUSF) and User Data Management (UDM) are traditionally associated with Home Service Subscriber in 4G networks. Access and Mobility Function (AMF) and Session Mobile Function (SMF) are usually associated to Mobile Management Entity (MME) in 4G networks; whereas, User Plane Forwarding (UPF) is traditionally associated to Service Gateway (SGW) in 4G networks. All of these aforementioned architectural elements will be allocated in this 5G multi-tenant network segment. Also, the Multi-Domain Network segment is where the network operators are inter-connected to other network operators. In case, the reader is interested in a complete description of each of the roles of the different architectural elements envisioned in the 5G architecture, in [14] Kim et. Al. provides a very comprehensive description.

A typical 5G scenario is composed of tenants/operators sharing infrastructures where their traffic is completely isolated, and their respective 5G users are provided with mobility thanks to the encapsulation protocols. Fig. 2 presents such 5G scenario where there are physical resources that are shared by mean of the usage of a virtual layer and where the main architectural elements of the 5G architecture are depicted. When a User Equipment (UE) is connected to an antenna, which belongs to operator A, this user is identified in the 5G networks by their TEID (tunnel endpoint identification) of their associated GTP tunnels, being inserted by the BBU/UPF element in the data path. Also, some architectural elements of the 5G network are associated to a given tenant/operator, which is identified with its unique virtual ID (VNID) given by the VxLAN encapsulation, mainly being inserted/removed by the virtual switches as shown in the Fig. 2. It means that each packet sent from one user to another user allocated in a different antenna must be encapsulated at least twice in the network segment between the edge and the core of the network. In a first stage VxLAN isolates the tenant traffic, and in a second stage, GTP provides user mobility.

In this new 5G mobile edge infrastructure, there are several actors involved over the same infrastructure such as infrastructure owner/provider, different network operators /tenants sharing the usage of such infrastructure and different 5G users subscribed to each of the network operators.

A flow is defined as a set of packets or frames passing an observation point in the network during a certain time interval [15]. An example of this flow structure bypassing the 5G mobile edge network between edge and core is shown in Fig. 3

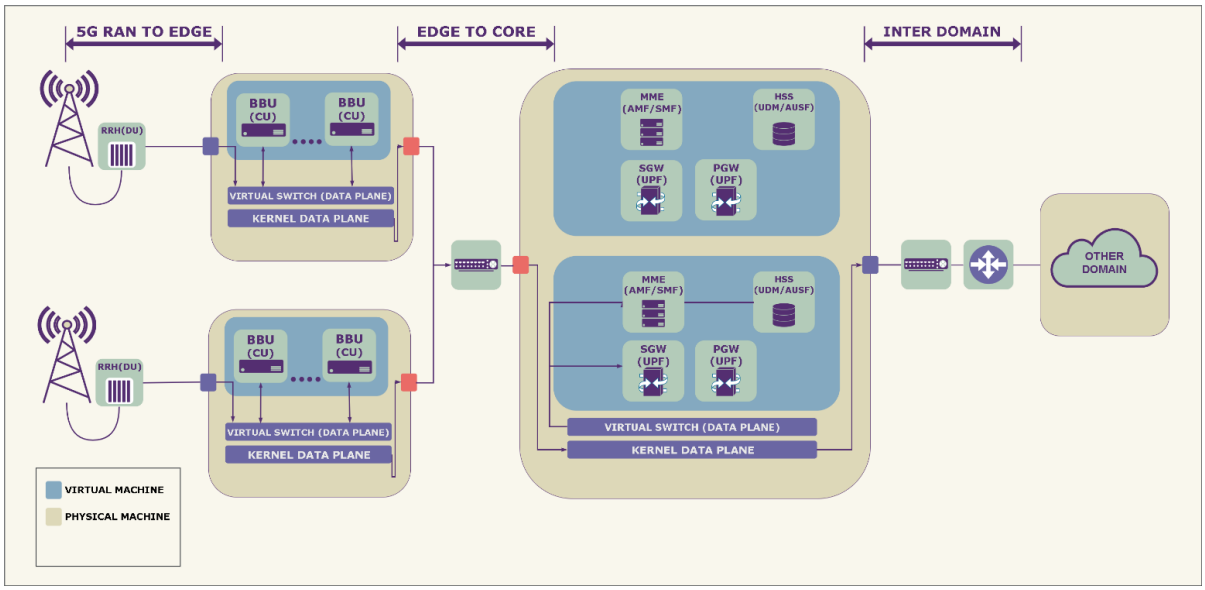


Fig. 2. Abstract architecture of a 5G multi-tenant infrastructure.

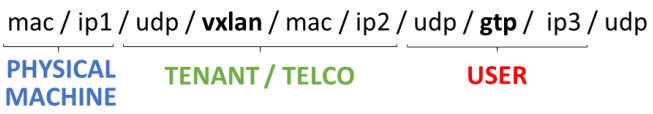


Fig. 3 Double-encapsulated 5G frame between edge and core.

A combination of Network Intrusion Detection Systems (NIDS) which could trigger alerts in case of an attack, together with other metrics related with the status of the network, such as packet loss and congestion, are traditionally used to detect DDoS attacks in 5G networks to provide efficient counter-measures. Traditionally, NIDS tools have been classified into two paradigms [16], namely anomaly-based and signature-based detection. The anomaly-based detection methods compare the network behaviour with a network behaviour model, already created. On the other hand, signature-based detection methods are based on matching of known attack signatures with the incoming patterns. Both have their advantages and disadvantages, but they share a clear limitation.

Traditional signature-based NIDS such as Snort [17] and anomaly-based NIDS such as Bro [18], to name a few, are mainly designed to provide detection capabilities to traditional IP networks. Thus, they do not provide support to detect transversal overlay networks being encapsulated over such IP networks. Snort provides essential support for both GRE and GTP overlay networks. However, GRE or GTP Snort's pre-processors must be considered to either detect attacks inside of such overlay networks or in the traditional IP traffic, but not both simultaneous. Thus, Snort lacks to provide transversal detection capabilities to protect both IP networks and encapsulated networks at same time. Also, only one of these encapsulations can be enabled at the same time, and to the best of our knowledge, no IDS support VxLAN encapsulation which is needed for the tenant-isolation of traffic allowing L2 overlay networks. Also, even the most advanced IDS published up to date does not provide any support for double encapsulated traffic (nested encapsulation) which is exactly the main requirement imposed by the 5G multi-tenant architectures.

This lack of support for transversal detection and nested encapsulation makes traditional IDS tools unsuitable for the new network traffic patterns imposed by 5G architecture, and it has been the main motivation of this research work. With this novel capability, the NIDS should be able to detect simultaneously attacks being addressed over a 5G user, a tenant or the entire infrastructure. The main contribution of this paper is the first NIDS with transversal protection capabilities and support for nested overlay networks to detect attacks against the mobile edge 5G multi-tenant network. The architecture presented in this contribution provides a significant set of innovations:

- The extension of the traditional alerts information that used to provide only information about the IP traffic to provide now more metadata information about the flow structure involved in the attack, including tenant and subscriber identification information. It allows the system to provide metadata about the network to accurately identify the origin of the attack to be able to react very selectively against such attack without affecting other traffic within the same network segment.
- The extension of a well-known NIDS, such as Snort, to be able to provide transversal detection capabilities to protect simultaneously, the 5G users, the tenant infrastructure, and the infrastructure provider.
- To allow the dynamic creation of overlays network while maintaining the detection over such newly created networks. The proposed system is not restrained by several encapsulations applied to 5G traffic and support any nested encapsulation.
- To allow a flexible allocation of the protection system. The proposed NIDS can be now deployed in almost all 5G network segments including the Mobile Edge Computing segment (see point A in Fig. 1), Core segment and Multi-domain segments (see point B in Fig. 1), against traditional NIDS where they will not work efficiently in almost any of these network segments. Thus, it is a significant advantage for Mobile Edge Security.

The proposed architecture has been empirically validated. Different experiments have been carried out to test the scalability of the architecture. The influence of different network conditions on the performance of the system has also been analysed to prove the flexibility over several types and levels of encapsulations. Also, different attacks conditions have been analysed regarding attack bandwidth and packet rate. The extensive validation has shown very good scalability results allowing to provide the transversal detection capabilities in a 5G multi-tenant network in less than 5 ms overhead of response time in average when compared against traditional NIDS solutions with no support for this type of detection.

The proposed architecture makes following significant contributions to Mobile Edge 5G Network security:

- Diverse types of traffic tagging and encapsulation protocols are supported such as VxLAN, GTP, GRE and tagging protocols such as MPLS and VLAN allowing the usage of the NIDS in the edge and other network segments, unlike traditional NIDS solutions.
- This approach accomplishes one of the most important requirements of 5G Network protection systems, which is being tenant-aware, but also 5G user-aware.

The rest of the paper is organised as: Section II presents the related work with different approaches to network security problem in a 5G network. Section III describes the design and architecture of the proposed system. Section IV shows the extended data model used to provide the underlying network information. Section V presents the performance evaluation of the proposed system. Section VI concludes the paper along with future work.

II. STATE OF THE ART

Despite the considerable number of available NIDS tools, there is no NIDS which supports a complete transversal defence for mobile edge 5G multi-tenant networks. Mainly, because

conventional NIDS does not provide support for the nested encapsulation demanded in such kind of architectures. For instance, Snort IDS incorporates a GTP pre-processor, so in the presence of a packet with just GTP encapsulation, it can match rules with the inner information of the packet. It enables matches of *gtp_version*, *gtp_type* and *gtp_info*. However, it does not work with a double encapsulated packet. Then, on the edge of a 5G network, Snort will not be able to provide any further information against attacks on 5G users. On the other hand, Snort also supports GRE encapsulation so that it can match its rules with the inner information of the packet. However, as occurred with GTP it does not work with double encapsulated packets. Finally, Snort does not support VxLAN encapsulation.

Novel defence mechanisms within a 5G network environment should consider the technological advancement of this new paradigm. There are three features mainly highlighted by the 5G PPP working group that would be included in those novel defence mechanisms [19]. First, multi-tenancy should be supported. Secondly, the novel mechanisms should be able to self-adapt to any change that could occur in the network topology. Moreover, lately, the overhead of the detection and mitigation system should not affect the overall performance of the network. A very small computation but also communication overhead should be added. Otherwise, the system would not be practical and scalable. Many works have been published addressing security threats in SDN, cloud computing and the more recent ones facing mobile edge 5G networks. Li and Wang [20] recently proposed a cooperative defence (CODE) framework against DDoS attacks for mobile edge computing by using NFV and SDN architectures. In this work, the approach is to provide an elastic and efficient resource defence usage to avoid that some nodes with an IPS get overwhelmed and lose their defence capacity, by requesting other IPS nodes their spare resources. Vidal et. Al. [21] proposed a new strategy for detection and mitigation of DDoS flooding attacks towards a self-managed 5G network. Inspired by biological defences mechanisms of human beings combined with strategies for DDoS detection based on the study of variations of the entropy of the network traffic. The traffic used for the validation process is created with hping3 tool, using different protocols and considering different network topologies. The traffic used in this work is pure IP, and the topology changes considered in the study are based on link distribution per node and number of nodes, but there is any reference to overlay networks and multitenancy. Maimó et al. [22] have recently presented a deep-learning based system to analyse network traffic by extracting features from network flows to identify cyber threats in 5G mobile networks. This solution is claimed to be self-adaptable to the volume of the network flows in real time. The validation of the solution is made with a well know dataset, the CTU dataset, which comprises scenarios with different numbers of infected computers and botnets families. Ros et al., [23] demonstrated an extensible IDS management architecture, where different IDS are installed in virtual machines, for different kinds of users and requirements in a cloud computing environment. It is claimed that the proposed management system could handle most of the VM-based IDSs. Pandeeswari and Kumar [24] proposed a novel IDS framework deployed at the VMM (Virtual Machine Monitor) in the cloud. It uses a fuzzy-cMean clustering mechanism with ANN (Artificial Neural Network) to learn attacks patterns to be detected in future. This framework is designed to be used in a network with a cloud topology that differs from a 5G network topology, where tenant isolation is not considered. Also, the dataset used for the experiments is a dataset of 1999 (DARPA's KDD cup dataset) which does not contain any mobile edge, cloud or 5G traffic.

Francois and Festor [25] proposed a tracebacking anomaly approach relying on OpenFlow switches. They defined a graph-based model to identify potential paths of the anomaly, locating the entry points of a DDoS attack in the network, but the exact origin of the attack is not provided. They tested their solution with two concrete topologies; however, no details were provided about the efficacy of the system beyond those two topologies, and no overlay networks were considered in their study.

Modi et al., [26] combined Snort and a decision tree classifier to detect known and unknown attacks. This solution is deployed behind virtual termination point to enable the detection of external and internal attacks. Although the system demonstrated good detection results, these results do not consider the possible encapsulation of the traffic – thus cannot be adopted for 5G networks to provide transversal security.

Wamg et al., [27] proposed a DDoS attack mitigation solution for SDN-based cloud computing, called DaMask. It is divided into two separated modules, DaMask-D for detection and DaMask-M for mitigation. In the detection module, they embed Snort along with Snort.AD, an anomaly-based detection plugin for Snort. This solution can adapt to frequent topological changes of the network regarding Virtual Machines allocations. However, their solution is dependent on cloud providers. Besides, it is not defined where the suspicious traffic is hosted after being detected. Although authors are considering multi-tenancy, their solution is not working with 5G traffic. Thus they are not considering every domain of a 5G network.

Liang et. at., [28] proposed a solution based on an architecture with four layers: data layer, control layer, security layer, and application layer. Also, a local control agent is introduced on the switch to enable performing localised actions ordered by the control layer. The work proposed by Giotis et al., [29] use OpenFlow middleboxes to stop malicious flows of a DDoS attack in legacy networks. This work handle traffic on a per-flow level within an NFV context. In this work, after a deep analysis of the challenges of the new SDN environment in the face of DDoS attack, a detection and mitigation system in the NFV context is proposed. A combination of anomaly-based detection and victim identification is used. However, this framework does not allow to identify the complete path of the attack within a 5G network.

Shamsolmoali et al., [30] used a statistically based filtering system, first removing the header field of every incoming packet and checking its Time to Live (TTL) value, and then comparing its header with a database based on Jensen-Shanon

divergence. Within this approach, just the headers of IP traffic are compared, so it would not be effective for a 5G network environment.

Liyanage et al., [31] proposed SIGMONA security architecture, a multi-tier security approach with four component: Secure Communication Component, Policy-Based Communication (PBC) Component, Security Management and Monitoring Component and Synchronized Network Security and Traffic Component. Within the PBC Component, there are included TCP-Splicing mechanisms with a bot detection scheme, for mitigating DDoS attacks targeted against the control plane. Although this work claims to secure 5G software defined mobile networks and both protect users and the network itself, it does not prove a complete transversal defence where both tenants and users are considered.

Ding et. at., [32] proposed an approach to attack detection by recognising flow patterns. In this work, the information coming from Snort IDS is correlated with network flows obtained by aggregated packets. If one flow is not correlated with any alert, then is labelled as a benign activity. Otherwise, it is labelled as an attack. Those labelled flows are then used to develop several learning classifiers to classify unlabelled traffic. A similar approach to this work is being used in our contribution regarding header analysis; however, this work only covers IP traffic, and our work has been significantly extended to detect attacks in mobile edge 5G multi-tenant networks.

Fan and Liu [33] use SVM (Support Vector Machines) and K-means to classify SDN traffic to address the new 5G networks paradigm. Ten types of traffic are considered, one of them is an attack. A self-collected dataset is used in this work due to the lack of publicly available 5G traffic datasets. They describe all the features used for the classification related to flows. Within the information of the flows used as features for the classification, there is no information related to encapsulation; either regarding the 5G user or the tenant information. It means that the traceback of a real 5G double encapsulated traffic in case of an attack will not be possible with this solution despite their claims.

A summary of all these previous works is shown in Table 1. In this table, the column IDS point out which type or types of IDS are used in the work if any. Column "F.A.", flow-aware, indicates whether the traffic analysis is handled per flow or not, i.e. only at global traffic patterns. Column "U.A.", indicates whether the system is user-aware or not, it means that if the detection system has any information regarding the user as an entry point of the attack. Likewise, the column "T.A." indicates whether the system is tenant-aware or not, which means if the detection system has gathered any information regarding the tenant as an entry point of the attack. From Table 1, none of the related works presented has managed to accomplish flow-aware, user-aware and tenant-aware, at the same time. None of them has considered nested encapsulation to be able to allocate their NIDS in the edge of the network. To the best of our knowledge, this contribution is the first one to be able to provide these capabilities simultaneously and to detect this kind of complex attacks in the edge of the 5G network due to the advanced transversal detection capabilities supported.

TABLE I. RELATED WORKS

Ref	Description	IDS	F.A.	U.A	T.A	N. E.
[20]	Cooperative defence framework against DDoS Attacks for 5G MEC leveraging NFV and SDN for effective use of the defence resource in each IPS.	-	-	-	-	-
[21]	Artificial Immune Systems to mitigate DDoS attacks	AI	NO	NO	NO	NO
[22]	Anomaly detection based on deep-learning for 5G networks	AI	YES	NO	NO	NO
[23]	IDS architecture for distributed cloud infrastructures	**	NO	NO	NO	NO
[24]	Anomaly detection system ate the hypervisor layer	AI	NO	NO	NO	NO
[25]	Traceback of DDoS attack in SDN carried out in each switch where the attack has been detected. Need to know the topology.	-	YES	NO	NO	NO
[26]	Detect anomalies between VMs	Snort	YES	NO	NO	NO
[27]	Virtualization of the network to mitigate DDoS over three strategies for making the scheme effective, inexpensive and with small overhead.	SB+AB	YES	NO	YES	NO
[28]	SDNM mechanism to protect the control layer against DoS attacks.	-	NO	NO	NO	NO
[29]	Control and filter of malicious traffic flows by deploying on-demand VNFs	AB	YES	NO	NO	NO
[30]	A statistical-based filtering system that compares packet header in a second stage of the filtering.	AB	NO	NO	NO	NO
[31]	Architecture that manages to mitigate DoS and DDoS attacks thanks to the security gateways proposed that hide controller from the outside.	-	NO	NO	NO	NO
[32]	Packet aggregation to obtain flows definition to be labelled based o Snort output and then being used in a classifier	Snort + ML	YES	NO	NO	NO
[33]	Two machine learning approaches for SDN traffic flow classifications	ML	YES	NO	NO	NO
	Our contribution - Snort Monitoring Agent (SMA)	Snort	YES	YES	YES	YES

A.I= Artificial Intelligence , AB. = Anomaly Based Detection, SB Signature Based Detection, ** several IDS's, - not indicated in the paper

F.A. = Flow Aware, U.A. = User Aware, T.A. = Tenant aware, N.E. = Nested Encapsulation

III. SYSTEM DESIGN

A novel approach is proposed to address the gap of defence mechanisms for mobile edge 5G multi-tenant infrastructure. Within this approach, a signature-based IDS is combined with a 5G traffic classifier to obtain the information to provide concrete and effective mitigation actions. This solution aims to be the first step towards a self-managed defence network system due to the extended metadata information provided as part of the detection of the attack. The architecture provided has

been coined as Snort Monitoring Agent (SMA) as it has been built as an agent extending Snort IDS capabilities.

A. Architecture overview and proposal description

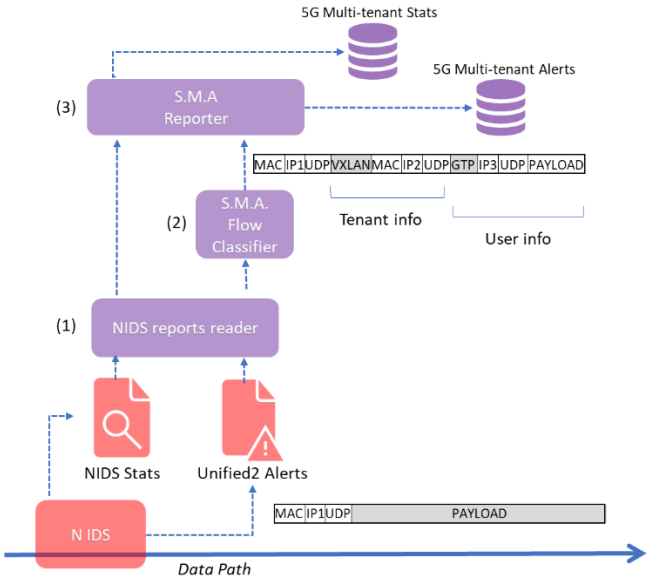


Fig. 4 System design.

The proposed system is composed of three main components, as shown in Fig. 4.

1) **NIDS Reports Reader** (see 1 in Fig. 4) its role is to retrieve events and statistics coming from the NIDS[1]. A plug-in based approach has been designed to enable our architecture to work with different NIDS. Each of the plugins oversees detecting the proper execution of the NIDS and parsing its log file where NIDS is dumping all the information on the events that are detected. NIDS Report Reader takes the log file tailing any new event logged by NIDS in Unified2 format. Unified2 [34] is a common output open format for network intrusion detection tools such as Snort, Suricata and Bro. Unified2 has been the chosen output format because it allows NIDS to operate faster and minimise the packet loss. Unified2 is also used by other tools such as Barnyard2 or Pigsty in production environments [35]. On the other side, the SMA reads the statistics report of NIDS with the same frequency that indicated in the NIDS configuration files.

Fig. 5 shows the capture of a packet with nested VxLAN and GTP encapsulations. An alert triggered by this packet is like the one shown in Fig. 6. For this example such alert has been converted from binary with the tool provided with Snort sources, u2spewfoo. It is important to emphasise that the information provided by the current alert does not allow to perform the identification of the malicious flow of the 5G user. Instead, only provides information about the first IP header which encapsulated all the traffic of all the users of all the tenants and thus it does not provide enough accuracy to be able to produce an alert associated to a specific 5G user.

[1] Although Snort was used in the validation process of the proposed solution, any IDS reporting in unified2 format could be used instead. The proposed system is independent of any specific IDS.

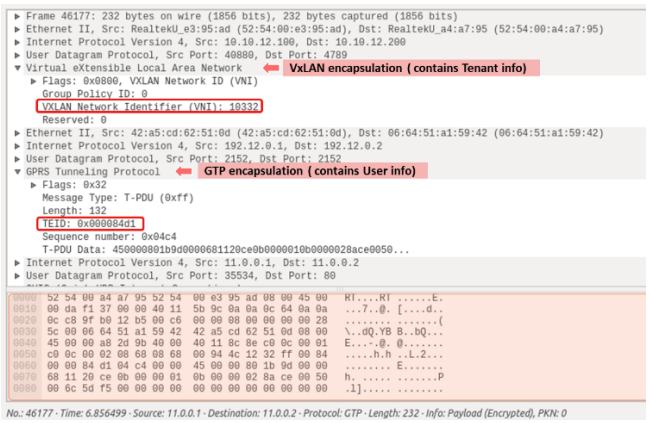


Fig. 5. Example of a capture of a packet with double encapsulation. The extended fields show the VNI and TEID identifiers corresponding to a tenant and a user.

```
(Event)
        sensor id: 0    event id: 46192 event second: 1530028986        event microsecond: 945672
        sig id: 10000003        gen id: 1       revision: 1      classification: 7
        priority: 2     ip source: 10.10.12.100 ip destination: 10.10.12.200
        src port: 40880 dest port: 4789 protocol: 17    impact_flag: 0  blocked: 0

Packet
        sensor id: 0    event id: 46192 event second: 1530028986
        packet second: 1530028986       packet microsecond: 945672
        linktype: 1     packet_length: 232
[    0] 52 54 00 A4 A7 95 52 54 00 E3 95 AD 08 00 45 00  RT....RT......E.
[   16] 00 DA F1 37 00 00 40 11 5B 9C 0A 0A 0C 64 0A 0A  ...7..@.[....d..
[   32] 0C C8 9F B0 12 B5 00 C6 00 00 08 00 00 00 00 28  ...............(
[   48] 5C 00 06 64 51 A1 59 42 42 A5 CD 62 51 0D 08 00  \..dQ.YBB..bQ...
[   64] 45 00 00 A8 2D 9B 40 00 40 11 8C 8E C0 0C 00 01  E...-.@.@.......
[   80] C0 0C 00 02 08 68 08 68 00 94 4C 12 32 FF 00 84  .....h.h..L.2...
[   96] 00 00 84 D1 04 C4 00 00 45 00 00 80 1B 9D 00 00  ........E.......
[  112] 68 11 20 CE 0B 00 00 01 0B 00 00 02 8A CE 00 50  h. ............P
[  128] 00 6C 5D F5 00 00 00 00 00 00 00 00 00 00 00 00  .l].............
[  144] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[  160] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[  176] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[  192] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[  208] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[  224] 00 00 00 00 00 00 00 00                          ........
```

Fig. 6. Example of a Snort alert triggered by the packet shown in Fig.5. This caption is an extract of a Snort log processed with the tool u2spewfoo.

2) **SMA Flow Classifier** (see 2 in Fig. 4) its role is to extract all the required information from the flow. The flow headers are included in the Unified2 format, and thus a custom parser for all the encapsulations previously described has been implemented. All values are stored in network byte order, so all the information is parsed into the SMA data model (described in Section IV). After being parsed, a Deep Packet Inspector (DPI) Flow classifier extracts all the information needed in the reaction/mitigation stage about the flow layers involved in each of the existing overlay networks. In Fig. 7 it is depicted a brief scheme of the sequencing process carried out by this DPI Flow classifier for a UDP packet similar to the one shown in Fig. 5 and for different levels of encapsulations. The IP Flow sequence (see 1 in Fig 7) shows the process followed for an IP flow with no encapsulation. The LTE Flow sequence corresponds with an LTE flow with GTP encapsulation (see 2 in Fig 7), the Multi-Tenant Flow sequence would match a multi-tenant flow with VxLAN encapsulation (see 3 in Fig 7) and the 5G Multi-Tenant Flow sequence corresponds to the one followed by the DPI Flow classifier with a packet like the one shown in Fig. 5 where there is multi-tenant isolation in 5G infrastructures (see 4 in Fig 7). The DPI flow classifier includes the definition of different patterns to match different network protocols, at any level of the OSI model.

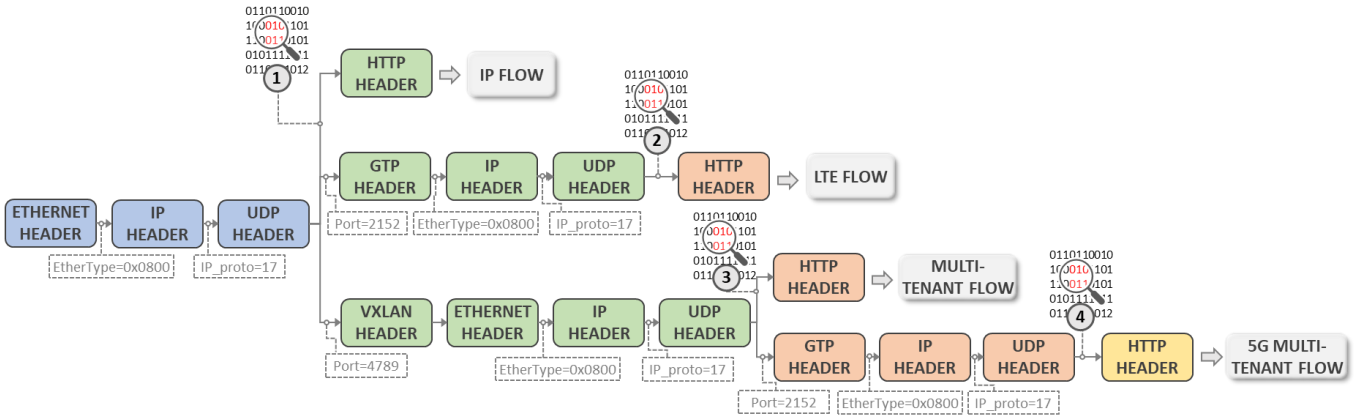


Fig. 7. Brief scheme of the parsing process of the DPI Flow Classifier for a UDP flow with different levels of encapsulations.

The last sequence is the more complex one since it corresponds with a 5G multi-tenant flow like the one depicted in Fig. 5 which has nested encapsulation. Thus, the parsing process match all the headers shown in the Wireshark capture: Ethernet/ IP/ UDP/ VxLAN/ Ethernet/ IP/ UDP/ GTP/IP/UDP/HTTP.

A sequence like this one is treated by Snort as traditional IP traffic (i.e. such us the first sequence) despite being a much complex flow. This fact is the reason why the information provided by the Snort alert depicted in Fig. 6 is only the one regarding the outer header. This lead to a lack of accuracy in the identification of the malicious 5G Flow and the enhancement of such accuracy is mainly provided by the novel classifier proposed.

The use of the DPI Flow classifier makes it possible to find and classify specific data contained in the packet, beyond the outer header and regarding the flow. Thus, it is possible to get transversal information from all the overlay layers of the packet, including user IDs, Tenant IDs, IP addresses involved and ports. This approach is a data-driven classification so that all the information provided in the output, is the complete information related to a flow. This architectural element of the system design allows the transversal detection of attacks since it dissects any overlay network extracting all the metadata along the parsing path to keep all the metadata associated. This component also allows the detection of attacks in all the network segments of the 5G mobile edge architecture mainly due to the support for nested encapsulation and of all the protocols being used in the traffic patterns between edge and core.

3) **SMA Reporter** (see 3 in Fig. 4) its role is to build JSON messages and report them. These messages are either new alerts or statistics. Within this JSON it is included information about the flows, about all the overlay networks, about the attack type detected, and other the place where the attack has been detected. The JSON of the alerts contains all the information related to the 5G multi-tenant traffic which generated the alert. The JSON of statistics is used as a set of metrics to extend the alert information and providing a further context in case of having to take a decision. When taking a flow as the basic unit, a typical countermeasure is to drop the malicious flow [36].


```
{"Alert": {
  "alertType": "7",
  "alertRuleId": "10000003",
  "alertImpact": 2,
  "alertTime": 1530028986945,
  "reportedTime": 1530037043509 },
 "Metadata": [{
      "flowId": "48A07435",
      "encapsulationLayer": 0,
      "macSrc": "52:54:00:E3:95:AD",
      "macDst": "52:54:00:A4:A7:95",
      "srcIP": "10.10.12.100",
      "dstIP": "10.10.12.200",
      "l4Proto": "17",
      "srcPort": "40880",
      "dstPort": "4789",
      "l7Proto": "vxlan" },
     {
      "flowId": "90D8AC34",
      "encapsulationLayer": 1,
      "encapsulationID1": "0000285C",
      "encapsulationType1": "vxlan",
      "firstPacketSeen": 1530037043509,
      "macSrc": "42:A5:CD:62:51:0D",
      "macDst": "06:64:51:A1:59:42",
      "l3Proto": "2048",
      "srcIP": "192.12.0.1",
      "dstIP": "192.12.0.2",
      "outSrcIP": "10.10.12.100",
      "outDstIP": "10.10.12.200",
      "l4Proto": "17",
      "srcPort": "2152",
      "dstPort": "2152",
      "l7Proto": "gtp-u"},
     {
      "flowId": "5BF5DE57",
      "encapsulationLayer": 2,
      "encapsulationID2": "000084D1",
      "encapsulationType2": "gtp",
      "srcIP": "11.0.0.1",
      "dstIP": "11.0.0.2",
      "outSrcIP": "10.10.12.100",
      "outDstIP": "10.10.12.200",
      "l4Proto": "17",
      "srcPort": "35534",
      "dstPort": "80",
      "l7Proto": "http" } ]}
```


Listing 1. Example of a report sent by the SMA

Within a 5G multi-tenant network in the context of the communication between edge and core, it is important to be able to choose the proper action to mitigate the attack. For instance, 1) to drop all the traffic from a user, 2) to drop all the traffic from a tenant, 3) to drop just the malicious flows coming from a user; 4) to drop all the traffic coming to that interface; 5) to drop all the traffic coming to the physical computer. The metadata provided in the JSON format allows performing any of these diverse types of fine-gain dropping actions.

An example of this JSON report is shown in Listing 1. In such report, it can be seen information that is already provided by Snort but also the extended information provided by the SMA metadata as a result of the new packet classification. Within this metadata, it can be found information about each of the encapsulation layers of the flow involved in the alert. In this example, an encapsulationLayer 0 provides information about the IP frame, an ecapsulationLayer 1 provides information about the VxLAN encapsulation, including the VNID identifier (Tenant identifier), and finally an encapsulationLayer 2 provides information regarding the GTP encapsulation, including the TEID identifier (5G User identifier). This information allows uniquely identifying the flows of each of the mobile users of the different mobile infrastructures that are deployed in the different tenants deployed in the infrastructure.

B. Design principles and limitations

To develop the proposed solution the following design principles have been followed:

- Modular design. A low coupling modular design has been approached to make the solution open future extensions. Thus, if a new alert format needs to be supported, a new extension of the NIDS Reports Reader module has to be added, without affecting the rest of the modules. The current version already supports different NIDS tools due to the use of unified2 as the first input format considered, used by Snort, Suricata and Bro. Likewise, new classifications could be added by just modifying the SMA Flow Classifier module. In the same way, if another reported method is required, just a new extension of the SMA Reporter has to be added.
- Extensible data model. A common data model has been designed to be used by the three modules that compose the SMA. This transversal module has been designed following the Data Access Object (DAO) pattern, providing an abstract interface to the modules. If a module needs to be extended it just have to satisfy the public interface of the DAO so that it can interact with the rest of the modules.

The limitations of the proposed solution are the following ones:

- A NIDS tool has to be installed, configured and run to make the SMA working. Also, the SMA has to be configured accordingly.
- Currently, the SMA only supports Unified2 alerts format. The NIDS Reports Reader module has to be extended to support another format.
- Since the SMA has been designed as an extension of a NIDS tool, it inherits the limitations of this NIDS regarding performance. For example, any limitation of the NIDS regarding bandwidth, delay or resource consumption is inherited by the SMA software.
- Some very specific communication protocols are not supported by the Flow Classifier yet. In this case, an extension of the Flow Classifier will be enough to satisfy the requirement of a new communication protocol, without having to modify the rest of the components or interfaces.

IV. DATA MODEL

Fig. 8 shows both Snort and the SMA data model regarding alerts. The output of Snort does not include any information about the encapsulation layers as pointed before and showed in Fig. 6. The data model defined in the SMA is using the same alert identifier and replicating some of the information provided by Snort and extending this information with the one obtained by the classifier about the packet. Among this information, it is worth to mention the "*encapsulationID*" for each overlay network. For instance, this field contains the TEID related to the GTP tunnel and the unique VNID of the VxLAN encapsulation protocol. The packet included in the alert will belong to a flow that identifies the origin of the attacker. This attacker is connected to an RRH that is connected to a BBU. In a scenario where all the UE users are infected by the Command & Control (CAC), we could get this same alert repeated for each user. The number of alerts per user will depend on the way rules have been configured, if these users are connected to different RRH and BBU's and belong to different tenants. All this information is needed to trace back the alert to its source, and this information is provided by the SMA. Therefore, in an alert scenario, the defence/mitigation system connected to the SMA could trace back the origin entry points and the origin of the attack, which makes it possible to mitigate the attack through proper location, without affecting other users, tenants or infrastructures.

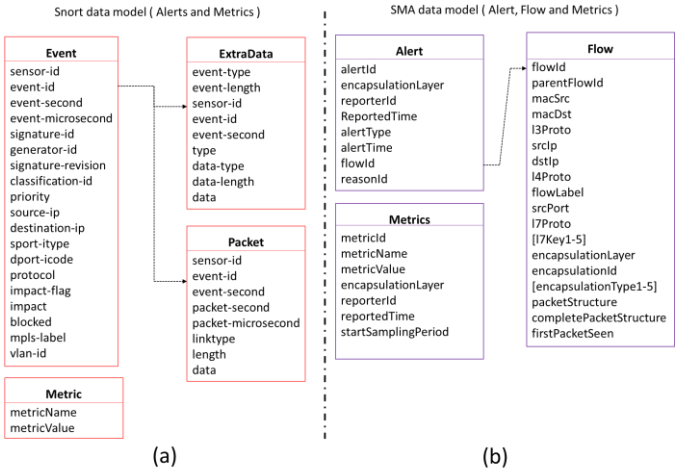


Fig. 8. a) Snort output data model ; b) SMA output data model

However, only with the output provided by NIDS (Snort), it will be impossible to extract the information related to users or tenants. Thus, it will not be possible to enforced actions by a defence/mitigation system related to the dropping of this kind

of overlay flows, being forced to drop all the traffic passing through the corresponding BBU from the same port of the alert. That means that every user connected to that BBU would lose connectivity and consequently its access to 5G services would be restrained. Thus, our system design provides a significant step forward by enabling the definition of very fine-grain mitigation rules for malicious traffic.

V. EMPIRICAL RESULTS

In this section, the use case prototyped for the empirical validation of the architecture is described in the next subsection. A well-known attack, UDP flooding attack, in a realistic scenario has been prototyped. Besides this, the testbed used in the validation process is also explained. Finally, the validation and scalability tests are presented with the obtained results.

A. Use Case Addressed

A User Datagram Protocol (UDP) flooding attack [37], by definition, is a DDoS attack that floods a target with UDP packets. The goal of the attack is to flood random ports on a remote host. This attack causes the host to check for the application listening on that port repeatedly and, when no application is found, reply with an ICMP 'Destination Unreachable' packet. This process weakens host resources, which can ultimately lead to inaccessibility of services. For empirical evaluation of the proposed system, UDP flooding attack within 5G multi-tenant networks has been chosen. For the simulation of a DDoS attack, Bonesi [38] has been used. Bonesi generates ICMP, UDP, and TCP flooding attacks from a given botnet size, by defining an IP range. In this case, the simulation has been made from just one IP address since the botnet is already represented by the number of UEs of our scenarios. Bonesi is configurable regarding rates and data volume. Therefore, Bonesi has been used to generate flooding traffic with different packet rates and payload size configurations. By combining both payload and packet rate, it is possible to obtain attacks of different bandwidth.

In order to measure the scalability of the SMA, UDP payload size between 0 and 1368 has been used, and bandwidth between 12.5 and 100 Mbps has been tested. Notice that this range of bandwidth is a very realistic one for a number of UE subscriptions in an LTE/5G network nowadays. Bonesi generates just IP traffic, so, to achieve 5G multi-tenant traffic, a real LTE/5G multi-tenant infrastructure deployed in our premises has been used to gather a PCAP file to be later used to scale up a DDoS attack. This infrastructure encapsulates the traffic from Bonesi using VxLAN for tenant isolation using OpenStack [39]. The tenant has inside a set of virtual machines using OpenAirInterface [40] that are used to allow the computer with Bonesi to connect to our LTE/5G antenna using an LTE/5G Dongle. Then, BBU encapsulated traffic in GTP to be sent to the SGW. Then, the traffic has been captured at the edge of the network to be able to intercept the communication between edge and core. Both encapsulations provide the infrastructure with tenant isolation and user mobility respectively, a key requirement for a 5G infrastructure. With the infrastructure available, different scripts of Bonesi has been executed to send traffic at different packet sizes and bandwidths. The sniffing of the PCAP has been performed at different physical and logical interfaces to be able to extract different encapsulation PCAPs.

Thus, depending on an experiment, a different PCAP has been used as base PCAP, regarding packet rate, bandwidth and number of encapsulations. For a specific experiment, as many as PCAPs are generated by rewriting the base PCAP, as it is the number of attackers. Therefore, the source and destination IPs had to correspond to the ones defined for each attacker and victim. Also, MAC addresses have been modified to have a correct routing adapted to the scenario. Also, destination ports have been changed to simulate a UDP flooding attack as well as the VNID to simulate a multitenancy environment.

B. Testbed

In order to emulate different real 5G scenarios, the Common Open Research Emulator (CORE) [41] has been used to emulate a DDoS attack. CORE is an open-source tool that is widely used for both research and military purposes. In contrast with network simulators, CORE as an Infrastructure-as-a-Service stack that allows the deployment of real x86-64 PC architectures using Linux containers and then creating virtual infrastructures by connected such containers within a network topology in real-time. CORE creates a Linux namespace for each of the emulated nodes to allow a complete container to act as a real node, creating a completely functional emulator. Different scenarios, like the one shown in Fig. 10 have been generated and executed, to test the scalability of the architecture presented herein. All the scenarios share a common deployment scheme which is a realistic 5G multi-tenant infrastructure. This deployment schema is shown in Fig. 9. The deployment scheme virtualises a 5G/LTE network; thus, it has considered mobility between antennas for users. From left to right in Fig. 9, the first nodes drawn are the mobile User Equipment (UE), which will act as the attacker(s).

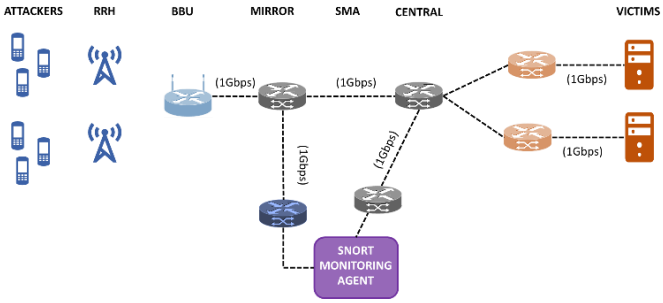


Fig. 9. A common scheme of the scenarios used for the experiments.

There are always at least two attackers, which are mobile users connected to an RRH. The BBU is shared by different RRHs. After that, it comes the core network whose links are configured to have a 1Gbps bandwidth in every link. On the other side of the network, there are the victims of the attacks, represented as servers. All the traffic that passes through the network is mirrored to the SMA node, in the centre of Fig. 9 , to intercept and analyse the traffic between edge and core network segments. Thus, Snort is configuring to trigger an alert in case of an attack and then processed by the SMA.

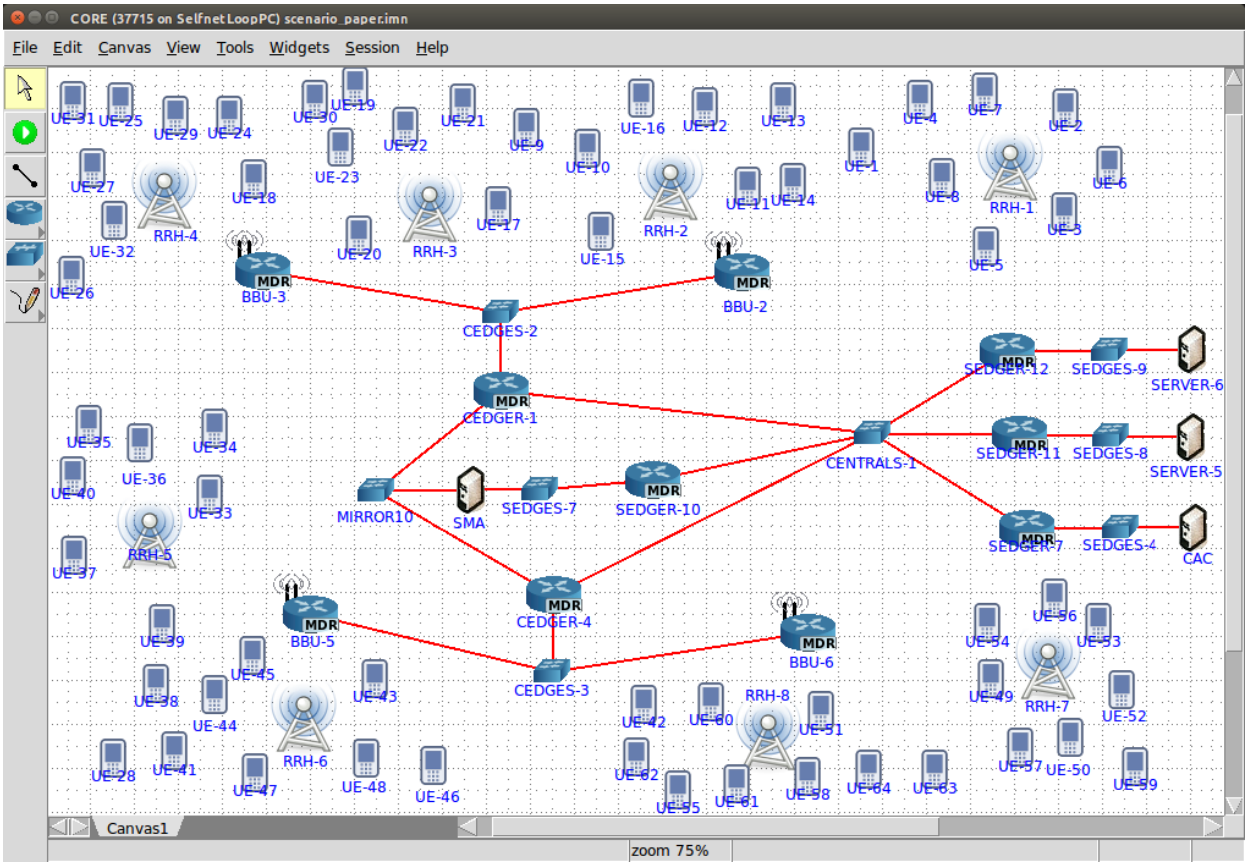


Fig. 10. Screenshot of the CORE Emulator for one of the scenarios executed.

This deployment scheme is replicated for different scenarios, varying the number of attackers, RRHs, BBUs, switches, and routers from the core network, the number of victims. Table II shows the ranges values for each of the scenarios executed.

TABLE II. Scenarios executed

VARIABLE	min	max	Step
Number of UEs per RRH	1	16	$Xn=Xn\text{-}_1*2$
Number RRHs per BBUs	1	4	$Xn=Xn\text{-}_1*2$
Number BBUs per switch	1	4	$Xn=Xn\text{-}_1*2$
Number of switches	1	16	$Xn=Xn\text{-}_1*2$
Number of victims	1	128	$Xn=Xn\text{-}_1*2$

Fig. 10 shows an example of a 5G multi-tenant scenario used for the experiments, created with the CORE. In this case, a DDoS attack with 64 attackers and one victim has been emulated. The nodes that work as an attacker are mobile subscribers labelled as UE. The nodes that work as a victim are labelled as SERVER. A key requirement for 5G networks is the connected mobility [42]. Thus, UE nodes have mobility, so that they change between antennas, and therefore end up connected to different BBUs. All the traffic passing through the named nodes CEDGER, is mirrored to the SMA node using iptables rules, so all the traffic passing form attackers to victims can be sniffed from there.

With all the different scenarios analysed, the aim is to test the flexibility of the SMA to topology changes as well as the scalability. At the same time, those different combinations allow testing different attacks regarding the number of victims, packet size, bandwidth, and packet rate. So, there could be attacks where every UE is attacking the same victim, or in the other extreme, each UE is attacking a different victim. The scenarios have been executed in an Intel Core i7 CPU 4.20 GHz, 32GB RAM hosting a Virtual machine with 16GB RAM and 4 cores. The overhead added has been measured in different scenarios in order to evaluate the system. For that purpose, the delay in milliseconds has been measured from the moment when Snort triggers the alert to the moment the SMA reports the extended alert. All the results have been executed with the same Snort configuration, which means, same rules and threshold configurations.

C. Validation Test

To validate the effectiveness of the usage of the SMA prototype in a 5G multi-tenant network, three key features have to be validated: first, to support multi-tenancy and 5G; second, self-adapt to any change which could occur in a network topology; and third to add an acceptable overhead, negligible for the whole system.

The first and the second features together, make possible to

protect at the same time, infrastructure, tenants and 5G users in both edge and core network segments of the 5G multi-tenant infrastructure. This capability is mainly possible thanks to the innovations presented in this contribution to be able to accurately identify the attacking nodes within the 5G network, in contrast to traditional NIDS's that only fit for traditional IP traffic. This capability has already been proved and discussed in this work, in Section III. An example of a 5G frame is depicted in the Wireshark capture shown in Fig. 5. That capture shows the headers of the encapsulation protocols, VxLAN and GTP. Also, the identifier of the tenant and the subscriber can be found in these headers respectively. Those identifiers are VNI=10332 and TEID=84D1. Both encapsulation layers and identifiers are crucial for accurate identification of the attacker node. Fig. 6 shows an extract of a Snort log with the alert triggered by the last packet where this information is clearly missing. In a later stage of this example, it has been depicted the output of the SMA for that same alert. This output, depicted in the SMA report of Listing 1, shows all the needed information to detect any flow of the 5G infrastructure thanks to the novel DPI Flow Classifier prototyped. This fact confirms the capability of the SMA to accurately identify the attacker node.

For the third feature to be validated, different experiments have been addressed to measure the overhead of the SMA.

The first group of experiments aimed to check the influence of various levels of encapsulations on the performance of the SMA. The more the levels of encapsulation, the greater is the size of the packet. The classifier module of the SMA extract information which is proportional to the number of layers of encapsulation applied to a flow. Fig. 11 shows the overhead introduced by the SMA when detecting attacks at various levels of encapsulations. In Fig. 11, presents attackers in a range of 2 to 256 UEs. The greater the number of attackers there are, the more flows must be processed by the SMA. The number of alerts received by the SMA and therefore the number of packets to process also depends on the configuration of the IDS, which is Snort in this validation process. Listing 2 shows an extract of a Snort rules definition file with the rule used for the validation experiments. This rule with signature id (sid) 10000003, defines the signature of a packet of the launched attack. It matches a UDP flooding attack where the IP source is equal to the variable $EXTERNAL_NET (defined as "any" in the Snort configuration file), any source port, a destination IP address equals the variable $HOME_NET (defined with the IP address of the victim in the Snort configuration file), destination port 4789 and a payload that contents "00000000".

```
alert udp $EXTERNAL_NET any -> $HOME_NET 4789
(msg:"Attempted DDOS UDP attack *00000000* message
detected"; content:"|00 00 00 00|";
classtype:attempted-dos; sid:10000003; rev:001;)
```

Listing 2. Example of the Snort rule defined to trigger alerts matching the launched attack of the experiments.

To reduce the noise related to the number of logged alerts rules, Snort includes a rule thresholding feature. It allows limiting the number of times a particular event is logged during a specific time interval. The definition of the thresholding used for the Snort rule of Listing 2 is shown in Listing 3. This thresholding definition means that the threshold will be tracked by IP destination (distributed attack) and that this rule with sid 10000003 logs every 500th event on this sid during one second. If less than 500 occur in 1 second, nothing gets logged. Once an event is logged, a new time period starts. That means that for an attack with a packet rate of 1000 packets per second, the NIDS logs approximately 2 events per second, which are then processed by the SMA. A higher or lower logging rate could be managed by varying the parameters of the threshold configuration file for this rule. However, the approach in these validation experiments has been to use different packet rate in the creation of the attack, as can be seen in the next section. Thus, in the previous example, to increase the periodicity of the events to approximately 4 events per second the packet rate should be of 2000 packets per second.

```
event_filter gen_id 1, sig_id 10000003, type
threshold, track by_dst, count 500, seconds 1
```

Listing 3. Extract of the threshold. conf file with the configuration of threshold for the rule used in the experiments.

In this experiment, all attackers are attacking the same victim. This experiment has been executed with four different PCAPs, each of them with a different encapsulation structure. The experiment has been executed for IP traffic, GTP over IP traffic, VXLAN over IP traffic and finally, VXLAN over GTP over IP traffic, which corresponds to the four parsing sequences depicted in Fig. 7 . The attack used for this experiment has 25 Mbps of bandwidth and a payload of 400 bytes, which is a packet rate of 5875 packets per second. In Fig. 11, it is shown how the system adds an overhead of just 3 ms of difference in the worst-case scenario between all the different encapsulation scenarios. These 3 ms are added to 10 ms delay taken by Snort to report the attack with a very tiny difference among the different numbers of encapsulations.

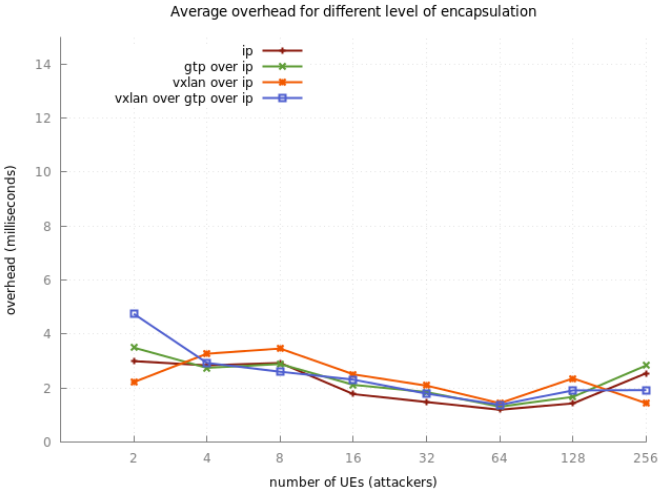


Fig. 11. Overhead introduced for a different number of attackers with different levels of encapsulations.

These results show a very little overhead to be able to have the

IDS detecting attacks in the edge of the network for 5G multi-tenant infrastructures. It validates the effectiveness of the proposed solution.

For a better understanding of all the subprocesses included in the entire use case, they are depicted in Fig. 12. The timeline shows every action point, and subprocess that happens since the attack is triggered until the SMA reports the event. The overhead measured in all the experiments presented in this section is the time invested by the SMA, which is the time lapsed from step 3 to step 6 shown in of Fig. 12.

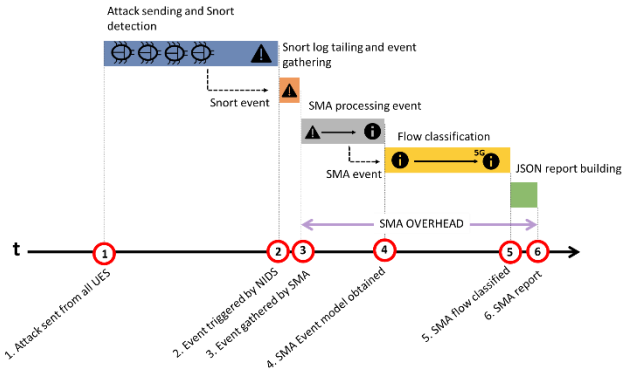


Fig. 12. Detached sub-processes of the use case.

Fig. 13 shows the absolute times of the entire process for the detection of a DDoS Attack using a Multi-Tenant 5G Flow. In this case, the experiment has been repeated 5 times on each of the two different NIDS´s supported in our prototype: Snort and Suricata. The same rule and threshold configuration have been used for both NIDS´s, obtaining the same alerts processed by the SMA in unified2 format. Snort version 2.9.9.0 and Suricata version 3.2 have been used in this testbed. The processing times gathered for both NIDS´s is insignificant as depicted in Fig. 13, being Snort 0.5 milliseconds slower than Suricata for the worst case. This little better behaviour of Suricata could be due to the multithreading supported by this tool, being this study out of the scope of this work. The processing times regarding the SMA are not affected by the NIDS replacements.

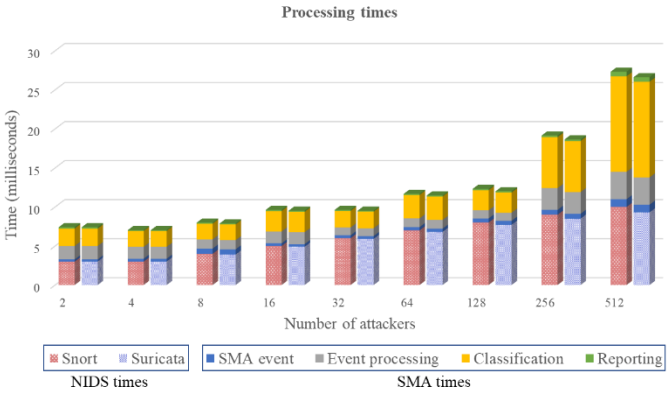


Fig. 13. Absolute times from attack sending time until SMA reporting time.

The first blocks of the stacked bar represent the time that passes since the attack is sent until the NIDS detects and reports the attack. The second block represents the time that passes from that Snort detection until the SMA start to process it. The third block corresponds to the time that the SMA spends in processing the event, that is interpreting the Unified2 and mapping into the objects of the SMA data model. The fourth block is the time spent in the classification of the flow, extracting all the overlays information. Moreover, the last block is the time spent in building the JSON to be reported. Notice that none of the results provided in this section has been compared with any other available research work, mainly because the functionality provided in this research work is, to the best of our knowledge, the first-of-its-kind to be published and thus there is not any other work to compare with.

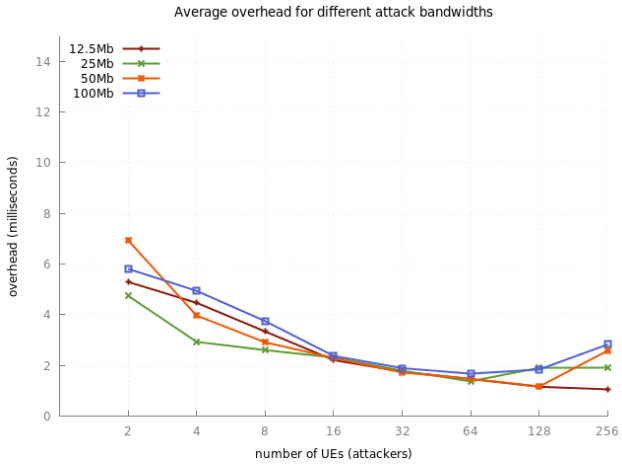


Fig. 14. Overhead introduced for a different number of attackers for different attack bandwidth.

E. Attack Behaviour Test

Fig. 15 shows the overhead introduced by the SMA for different packet rates. Two types of attacks shown in the figure: “one-to-one” which means that each UE attacks to a different victim; and “all-to-one” which means that every UE attacks to the same victim. These experiments have been executed for 128 attackers and a fixed bandwidth of 50Mb, which is a realistic scenario for a current mobile broadband user.

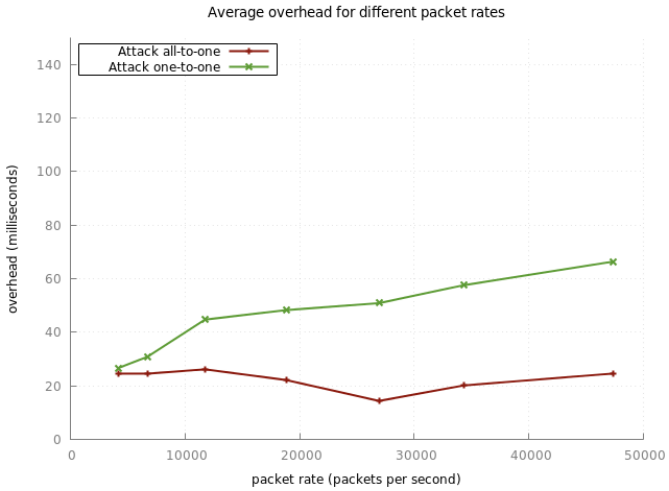


Fig. 15. Overhead introduced for different packet rates for the same number of attackers (128) and same bandwidth (50Mb). The results show two types of attack one-to-one (one UE attacks one victim) and all-to-one (every UE attacks to the same victim).

The payload size of the packets sent in the attacks has been ranged from the minimum possible (~0 bytes) to the maximum (1368 bytes). This payload range implies to have a packet rate ranged between 1466 packets per second (pps) and 47348pps for an attack of 50Mb of bandwidth. The higher is the packet rate, the more alerts will be triggered by the NIDS.

Fig. 15 shows a very stable behaviour of the system on average, although the standard deviation tends to increase with the packet rates. Fig. 15 also shows that the overhead is greater on average for the attack type "one-to-one" than it is for the attack "all-to-one". However, it is still below 70 ms for the worst case, where the attack is composed of packets with the minimum payload possible and a packet rate of 47348 pps.
These set of results indicates that the proposed SMA is suitable to protect both edge and core network segment of the novel 5G multi-tenant infrastructures.

Different experiments have been executed in order to test the scalability of the system and the performance against different levels of encapsulations. The scalability test has proved SMA can amicably handle the different scale of attacks regarding the number of attackers, the bandwidth of the attack and packet rates. For the overlying support pcaps with different encapsulations has been used. According to the results shown, it can be claimed that the SMA has successfully achieved the targets of tenant aware, topologically flexible and scalability with very acceptable overheads for detecting DDoS attacks in 5G networks. The control messages sent by the SMA could be received in the control plane by a manager to take a proper decision to mitigate the attack on time, having all the information required to enforce such decision.

VI. Conclusion

A novel system to efficiently protect against DDoS attacks in 5G multi-tenant networks has been proposed, implemented, and empirically validated. The proposed system efficiently protects tenants, infrastructure, the provider of the infrastructure and final-users in the 5G network simultaneously. This proposed system can be allocated to almost all the 5G network segments which is a significant advantage for Mobile Edge Security. The system has been validated against UDP flooding DDoS attack as realistic use case where more than 256 simultaneous attackers are injecting malicious traffic at 100Mb/s to a 5G network. The proposed system is based on the extension of a well-known IDS called Snort, but the system is extensible and thus valid for any other IDS that report events in Unified2 format. All the previous claims have been achieved without adding significant overhead to the system, which means that there are no significant delays in the reception of alerts comparing with the times provided by the IDS. It has been proved the scalability of the system, showing an almost constant behaviour even for the worst cases regarding the number of attackers or type of attack.

Future work will investigate the usage of this framework in a mitigation system, to mitigate the attack in the proper place. This combination of detection and mitigation will help in the closing of the cognitive management loop envisioned for the novel 5G infrastructures.

Acknowledgement

This work was funded in part by the European Commission Horizon 2020 5G PPP Programme under grant agreement number H2020-ICT-2014-2/671672 – SELFNET (Self-Organized Network Management in Virtualized and Software Defined Networks). This work is also supported by Zayed University Cluster Research Award #R18038. This work was additionally funded by the UWS 5G Video Lab project.

References

[1] 5G PPP, "5G PPP use cases and performance evaluation models," 2016.

[2] Next Generation Mobile Network Alliance, "NGMN 5G White Paper," *Ngmn*, pp. 1–125, 2015.

[3] G. Horn and P. Schneider, "Towards 5G security," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, pp. 1165–1170.

[4] "NHS cyber-attack causing disruption one week after breach | Society | The Guardian." [Online]. Available: https://www.theguardian.com/society/2017/may/19/nhs-cyber-attack-ransomware-disruption-breach. [Accessed: 22-Dec-2017].

[5] BBC, "TalkTalk cyber-attack: Website hit by 'significant' breach - BBC News," *BBC News*, 2015.

[6] K. Lab, "GLOBAL IT SECURITY RISKS SURVEY Global IT Security Risks Survey 2015: The current state of play."

[7] Arbor Network, "Worldwide Infrastructure Security Report," 2016. [Online]. Available: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf. [Accessed: 04-Dec-2017].

[8] "Major DDoS Attacks Involving IoT Devices," *European Union Agency for Network and Information*, 2016. [Online]. Available: https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices.

[9] F. Wang, H. Wang, X. Wang, and J. Su, "A new multistage approach to detect subtle DDoS attacks," *Math. Comput. Model.*, vol. 55, pp. 198–213, 2012.

[10] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017, pp. 193–199.

[11] Mahalingam M. et al., "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," Kenchiku Setsubi Iji Hozen Suishin Kyōkai, 2014.

[12] J. Gebert and D. Zeller, "Fat pipes for user plane tunnelling in 5G," in *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2016, pp. 1–6.

[13] 3rd Generation Partnership Project (3GPP), "TS 29060 V10.2.0 - Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface." 2011.

[14] J. Kim, D. Kim, and S. Choi, "3GPP SA2 architecture and functions for 5G mobile communication system," *ICT Express*, vol. 3, no. 1, pp. 1–8, Mar. 2017.

[15] B. Trammell, B. Claise, and P. Aitken, "Specification of the IP flow information export (IPFIX) protocol for the exchange of flow information," Internet Research Task Force, 2012.

[16] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Comput. Networks*, vol. 31, no. 8, pp. 805–822, Apr. 1999.

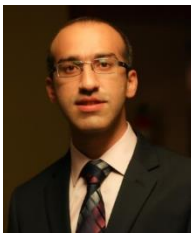
[17] Snort, "Snort - Network Intrusion Detection & Prevention System," 2016. [Online]. Available: https://www.snort.org/%5Cnhttps://snort.org/. [Accessed: 13-Apr-2018].

[18] M. Vallentin, "The Bro Network Security Monitor Tools of the Trade," *Bro.Org*, 2011. [Online]. Available: https://www.bro.org/.

[Accessed: 13-Apr-2018].
[19] "5G PPP Architecture Working Group View on 5G Architecture (Version 2.0)," 2017.
[20] H. Li and L. Wang, "Online orchestration of cooperative defense against DDoS attacks for 5G MEC," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.
[21] J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, "Adaptive artificial immune networks for mitigating DoS flooding attacks," *Swarm Evol. Comput.*, vol. 38, pp. 94–108, Feb. 2018.
[22] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.
[23] S. Ros, F. Cheng, and C. Meinel, "Intrusion Detection in the Cloud," in *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009, pp. 729–734.
[24] N. Pandeeswari and G. Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," *Mob. Networks Appl.*, vol. 21, no. 3, pp. 494–505, Jun. 2016.
[25] J. Francois and O. Festor, "Anomaly traceback using software defined networking," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 203–208.
[26] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, "A novel framework for intrusion detection in cloud," in *Proceedings of the Fifth International Conference on Security of Information and Networks - SIN '12*, 2012, pp. 67–74.
[27] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking," *Comput. Networks*, vol. 81, pp. 308–319, Oct. 2015.
[28] X. Liang and X. Qiu, "A software defined security architecture for SDN-based 5G network," in *2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, 2016, pp. 17–21.
[29] K. Giotis, G. Androulidakis, and V. Maglaris, "A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox," *Secur. Commun. Networks*, vol. 9, no. 13, p. n/a-n/a, Sep. 2015.
[30] P. Shamsolmoali and M. Zareapoor, "Statistical-based filtering system against DDOS attacks in cloud computing," in *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2014, pp. 1234–1239.
[31] M. Liyanage *et al.*, "Enhancing Security of Software Defined Mobile Networks," *IEEE Access*, vol. 5, pp. 9422–9438, 2017.
[32] T. Ding, A. AlEroud, and G. Karabatis, "Multi-granular aggregation of network flows for security analysis," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2015, pp. 173–175.
[33] Z. Fan and R. Liu, "Investigation of machine learning based network traffic classification," in *2017 International Symposium on Wireless Communication Systems (ISWCS)*, 2017, pp. 1–6.
[34] "README.unified2," 2018. [Online]. Available: https://www.snort.org/faq/readme-unified2. [Accessed: 11-Apr-2018].
[35] C. Sanders, J. Smith, C. Sanders, and J. Smith, "Signature-Based Detection with Snort and Suricata," in *Applied Network Security Monitoring*, Elsevier, 2014, pp. 203–254.
[36] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.
[37] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
[38] M. Goldstein, "BoNeSi, the DDoS Botnet Simulator.," 2016. [Online]. Available: https://github.com/markus-Go/bonesi. [Accessed: 04-Jun-2018].
[39] "OpenStack." [Online]. Available: https://www.openstack.org/. [Accessed: 18-Apr-2018].
[40] "OpenAirInterface." [Online]. Available: http://www.openairinterface.org/. [Accessed: 19-Dec-2017].
[41] "Common Open Research Emulator (CORE) | Networks and Communication Systems Branch." [Online]. Available: http://www.nrl.navy.mil/itd/ncs/products/core. [Accessed: 13-Apr-2018].
[42] M. Lauridsen, L. C. Gimenez, I. Rodriguez, T. B. Sorensen, and P. Mogensen, "From LTE to 5G for Connected Mobility," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 156–162, Mar. 2017.

Ana Serrano Mamolar is a PhD candidate at the University of the West of Scotland, United Kingdom, where she is involved in the H2020 5G-PPP Phase I SELFNET project. Her main interests include network management, cognitive control plane, cyber-security and self-protection in mobile edge computing and 5G networks.

Jose M. Alcaraz-Calero is a Full Professor in networks and security at the University of the West of Scotland. He is the technical co-coordinator of the EU H2020 5G-PPP Phase I SELFNET and the EU H2020 5G-PPP Phase II SliceNet projects. His professional interests include network cognition, network management, network security and control, service deployment, automation and orchestration in 5G mobile networks. Alcaraz Calero has a PhD in Computer Science, University of Murcia.



Zeeshan Pervez received his PhD in Computer Engineering from Kyung Hee University (KHU), South Korea. His research interests are security and privacy aspects of internet-of-things, cloud computing, cybersecurity and knowledge management. Since 2013, he has been with the University of the West of Scotland (UWS) as an Assistant Professor. He has published over 60 indexed journals, peer-reviewed conferences and book chapters. He has led and participated in several projects funded by the European Commission, UK and Korean Research Councils and industry. He is a Senior member of IEEE, Fellow of Higher Education Academy, and a Full member of EPSRC Review College.

Asad Masood Khattak received his PhD degree in Computer Engineering from Kyung Hee University, South Korea in 2012. He worked as Post-Doctoral Fellow at the Department of Computer Engineering, Kyung Hee University, South Korea and later joined the same department as Assistant Professor. In August 2014, he moved to Zayed University, UAE as Assistant Professor and is recently promoted to Associate Professor position. His current research focus is User Profiling, Ontology, Knowledge Management, and Context-aware Computing. He is currently leading three research projects and participating in five additional research projects in the same research fields. He has authored/coauthored more than 85 journal and conference articles in highly reputed venues.