Towards the detection of mobile DDoS attacks in 5G multi-tenant networks

Serrano Mamolar, Ana; Pervez, Zeeshan; Wang, Qi; Alcaraz Calero, Jose M.

Published in:
European Conference on Network and Communication

Accepted/In press: 15/04/2019

Document Version
Peer reviewed version

Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks

Ana Serrano Mamolar
Univ. of the West of Scotland

Zeeshan Pervez
Univ. of the West of Scotland

Qi Wang
Univ. of the West of Scotland

Jose M. Alcaraz-Calero
Univ. of the West of Scotland

***Abstract*—The fifth-generation (5G) mobile networks target a variety of new use cases that involve a massive amount of heterogeneous devices connected to the same infrastructure. This trend also brings new security threats, and one of the most critical ones for the availability of network services is a Distributed Denial of Service (DDoS) attack. A small portion of the billions of connected devices can be employed as a botnet to trigger a massive DDoS flooding attack that can bring down important services or affect the complete infrastructure. Traditional security systems against DDoS attacks are generally designed to work in infrastructures with a particular topology. However, the mobility of many devices subscribed to the network should be taken into account when designing defence systems. Otherwise, both the detection and the trace back of the attacker will be limited to non-mobile devices as the source of the attack. This is specially relevant when security needs to be part of the definition of the network slices associated to the 5G networks. This paper presents a novel approach to overcome the limitation of traditional detection systems. A novel sensor provides the required information to trace back an attacker even if it is moving among different locations. The proposed approach is suitable to be deployed in almost all 5G network segments including the Edge. Architectural design is described and empirical experiments have validated the proposed approach.**

***Index Terms*—5G Network, DDoS Attack, Mobile botnet, Attacker traceback**

I. Introduction

The next generation of telecommunication networks (5G) is already hitting the market in 2019 and will continue expanding worldwide. Many benefits are expected such as speed and latency improvements, which will increase the number of user equipment (UE) subscribers. It is predicted to reach 1.5 billion of 5G subscriptions for enhanced mobile broadband by the end of 2024 according to Ericsson mobility report [1]. In fact, 5G is the first mobile technology designed to meet the unique requirements of connected devices for health, industrial applications, transportation and many IoT devices. However, that increase of mobile and non-mobile devices connected to a 5G infrastructure will also increase the potential cyber threats. Distributed Denial of Service (DDoS) attack is an important threat for these networks, and detection and mitigation strategies need to be adapted to protect 5G infrastructures against them.

DDoS attack detection and mitigation has been an important topic in the literature. They are considered particularly difficult to detect or trace back due to their distributed nature [2]. Moreover, many times attackers use fake IP addresses to hide their identities, which makes it more complicated to trace back. Furthermore, a critical issue to take into consideration is the possible mobility of the devices used as a botnet. Any UE can move around different locations. Thus, the network topology can change unpredictably, being more complicated to trace back the origin of an attack and let alone to mitigate it. Therefore, traditional detection and mitigation systems, which are not aware of these random changes in topology, will not be able to protect 5G mobile networks. Trace back mechanisms, such as packet marking or link testing[3], are not viable in case of a DDoS attack because of their high computational, network or management overheads. One crucial objective declared by the 5G-PPP Architecture Working Group is to create a cognitive and autonomic network management system that can self-adapt to the changing conditions of the network, which includes changes in the topology of the network [4]. To achieve this goal it is essential to start gathering enough meta-data to be aware of user mobility. The approach presented in this paper is based on a cooperative work between a traditional Intrusion Detection System (IDS), and a novel alert enhancer that provides needed metadata to allow the trace back of mobile users.

Fig. 1 shows a brief scheme of the segments of a 5G architecture. In this figure, there are different UE devices connected to the 5G network and they can be for instance mobile phones, cars, ambulances or computers. They are connected to the network through the 5G Radio Access Network (RAN), which is typically associated with the deployment of the antennas and Remote Radio Heads (RRHs) or Distributed Units (DUs) on top of the buildings. The Edge Segment is typically associated with the last mile of the network, where machines are allocated to run different needed processes close to the user and where BaseBand Units (BBUs) or Centralised Units (CUs) are allocated. In Fig. 1, the Edge and Core Segments have been represented as a multi-tenant network, where different virtual operators share the infrastructure. Thus, two edges have been depicted and in each edge two different tenants are being served for illustration purposes. In fact, the two virtual machines in each of the edges belong to two different virtual network operators. This multi-tenancy property, where a different operator can share the cost of the physical infrastructure, is a key characteristic of 5G networks, and a new challenge to be overcome for defence mechanisms. In the Core Segment, there are various control plane and data plane components for mobility and session management, among others. Finally, network operators are interconnected

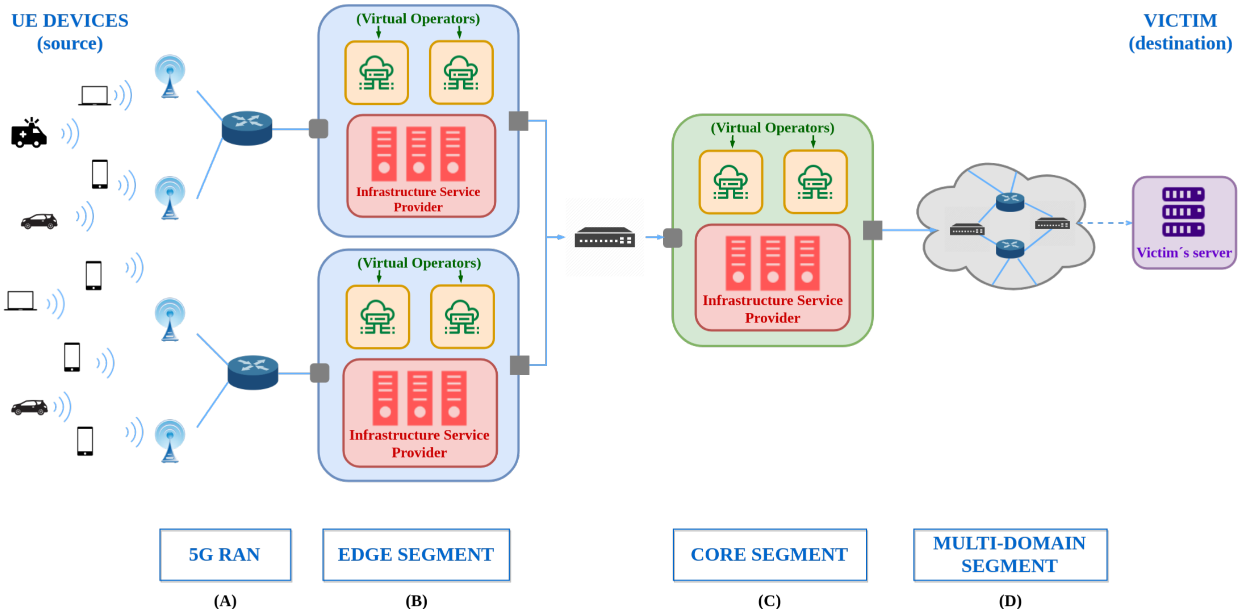

Fig. 1. Overview Architecture of a 5G multi-tenant infrastructure.

to each other through the Multi-Domain Segment. A more detailed description of the 5G architecture can be found at [5].

There are many discussions about the best location to deploy a defence system [6] [7]. The three main possible locations are inside the Edge Segment, inside the Core Segment and outside the Multi-Domain Segment. In addition, a hybrid approach of them has been discussed. To allocate it in the Edge Segment will provide as an advantage a quick detection and mitigation of the attack from a UE botnet due to the short distance. Moreover, it avoids affecting the rest of the infrastructure. However, in case of a massive distributed attack, there is a lack of aggregated information in such a close point, and the accuracy of the detection can be affected. Locating the defence system inside the Core Segment, close to the victim, has the advantage of having all the needed aggregated information of all the malicious traffic from the distributed attack. However, at this point, the detection of the attack can be late since the attack has already affected the infrastructure. Deployment in the Multi-Domain Segment is an excellent point to have extensive knowledge of the source of the attack, but probably not to know the victim. This work is focused on a hybrid alternative, where a Network Intrusion Detection System (NIDS) can be deployed in the Edge, the Core or the Multi-Domain Segment. This novel NIDS can be deployed flexibly as mentioned, and more importantly, it is capable of detecting the attack coming from mobile users and providing the needed information for proper mitigation in the next step.

A. State of the art

Different works such as [8] and [9] have demonstrated the ability of mobile botnets to carry out coordinated attacks against a common victim. Among the current available NIDS tools, there is no NIDS that supports a complete defence for mobile edge 5G multi-tenant networks. This is mainly because that conventional NIDSs are not ready to provide the needed information to be able to apply fine-grained countermeasures for attackers acting from mobile users. The design of novel defence mechanisms within a 5G network environment should consider the technological advancement of 5G's new paradigm. Existing work have contributed to overcoming some of the different challenges in the traceback of an DDoS attacker. In [10], OpenFlow switches are used to present a tracing back anomaly approach. Potential paths of the attack identified through a graph-based model, but the exact point of the attack is not provided. In [11], Software Defined Networking (SDN) traffic is classified using Support Vector Machines. The features extracted from the traffic for the classification process are described in this work. However, none on the features are related to the identification of the 5G user, needed to manage mobility. In case of a DDoS from mobile UEs, this approach does not allow tracing back the origin of the attack and consequently proper mitigation is not possible. In [12], mitigation is proposed through a two hierarchies of filtering process. A first filter is placed at the mobile edge computing servers to prevent spoofing attacks close to the source. A second filter located in cloud servers classifies the traffic of the complete network. Nevertheless, tracing back the mobile attacker is not supported.

B. Contributions of this work

The following contributions and innovations towards the protection of future generation mobile networks are provided in this work:

- To allow the detection of DDoS attacks towards fine-grained mitigation when the source of the attack is a UE

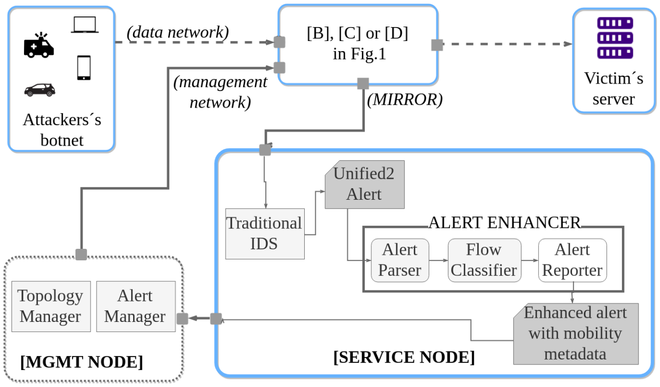

Fig. 2. System design.

moving across different locations.

- To allow flexible allocation of the detection system. The novel NIDS can be deployed in almost all the 5G network segments including the Edge, the Core and Multi-Domain Segments.
- To allow the mitigation of the attack at any point of the malicious flow path, either close to the source of the attack or close to the victim because of the extended knowledge of the source of the attack.
- To allow the integration with different conventional NIDSs because of the plugin-based design of this approach.

II. System Design

In order to overcome the current limitations of traditional NIDSs for mobile edge 5G infrastructures, a novel approach is proposed. When a DDoS attack is triggered by a mobile botnet, the main limitation of traditional NIDSs is the lack of information to trace back the origin of the attack for proper mitigation. This approach solves the problem by combining traditional NIDSs with an advanced classifier to obtain the missing needed information. This approach leads to the first step towards a complete self-managed defence of mobile network infrastructures due to the extended information provided within the detection of the attack.

A. Architecture overview

The proposed system can be deployed in three different locations of a 5G infrastructure. Specifically, in the Edge Segment (Fig. 1 [B]), the Core Segment (Fig. 1 [C]), or the Multi-Domain Segment (Fig. 1 [D]). Fig. 2 shows how the traffic coming from the data network is mirrored to a service node of the management network. In this service node, the traditional NIDS is deployed, and its alerts are then extended by our novel component, which reports a new alert with the extended metadata aware of mobility. This novel component is referred to as Alert Enhancer (AE). Fig. 2 depicts the architectural elements of this new AE component:

- **Alert Parser**: This module consumes the traditional NIDS alerts. It has a plugin-based design, and thus the AE is extensible to any alert format coming from any traditional NIDS. The current implemented version in this work supports Unified2 [13] format, a widespread format used by many traditional NIDS such as Snort, Suricata and Bro, as well as some alert managing software such as Barnyard and Pigsty. It is a binary format that allows fast processing and minimises packet loss. However, any other alert format could be processed by the AE if the plugin with the parser is added.
- **Flow Classifier**: This module extracts the needed metadata from the malicious flow. The complete packet with the flow headers is included in the Unified2 alert previously parsed by the Alert Parser. The role of the flow classifier is to extract the values stored in network byte order and classify them through Deep Packet Inspection (DPI). The definition of different patterns has been added to this module, so different network protocols at any level of the OSI model can be matched. Current NIDSs only provides information regarding the outer header, while the minimum information needed for a proper traceback of the attacker in a multi-tenant mobile infrastructure is the Unique Virtual ID that identifies a Virtual Operator (VNI) and the Tunnel Endpoint Identification (TEID) that identifies the UE. Those two values, included in inner headers, are extracted by the flow classifier. A more detailed list of the extended information extracted by the classifier is depicted in the next section.
- **Alert Reporter**: This module reports the enhanced alert including the information of the alert provided by the traditional NIDS (such as type of attack, alert time, and priority) and the metadata extracted by the flow classifier to allow the traceback of the source of the attack and thus a fine-grained mitigation. This enhanced alert is sent through the management interface to the Management Node through a RabbitMQ message bus. With this information the Management Node, would be able to take decisions of how and where to mitigate the attack (out of the scope of this work).

III. Empirical results

This research is focused on attacks launched by botnets formed by a high volume of mobile devices sending malicious traffic against the network. To assure the scalability of the proposed solution, several scalability tests have been run. The solution has been prototyped and validated in a real scenario for the use case of a large-scale DDoS UDP flooding attack within a 5G multi-tenant network. A UDP flooding attack is a DDoS attack that floods a target with UDP packets [2]. The primary purpose of this attack is to overwhelm random ports on the targeted host. Due to the unknown application associated with the received datagram, the victim sends back an ICMP Destination Unreachable packet per UDP packet received. Thus, the victim resources become overwhelmed for a significant amount of UDP packets received, and consequently, its services become unavailable. The attack has been emulated running Bonesi [14] in each UE. This tool has been configured to send traffic from one IP address per UE. The experiments

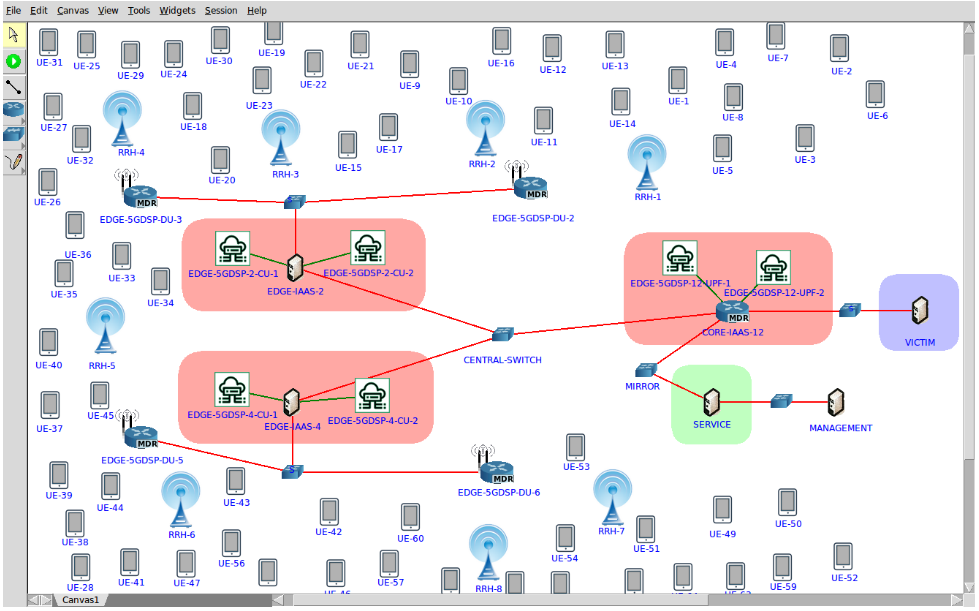

Fig. 3. Example of an experiment scenario in CORE emulator

generate UDP flooding traffic of 25 Mbps and 50 Mbps from each UE, which is a realistic scenario considering today's speed in the UE subscriptions. The Common Open Research Emulator (CORE) [15] has been employed to validate the solution in terms of scalability. Developed by Boeing Research and Technology and US Navy Research Laboratory, CORE is a proven large-scale container-based deployment tool with a realistic emulator of network conditions. The CORE provides an Infrastructure-as-a-service (IaaS) stack, which makes use of Linux network namespaces as the hypervisor to allow the creation of a set of lightweight virtual machines that acts as a real node, creating a complete functional infrastructure. Different scenarios such as the one shown in Fig. 3 have been generated and executed, to test the scalability and flexibility of the proposed solution. In the scenario of Fig. 3 64 UE devices are represented as mobile phones and connected to several antennas (RRH), and they represent botnets that will trigger the attack. The Edge Segment is represented by different Infrastructure Providers (IAAS, eg. EDGE-IAAS-2) and Virtual Operators (eg. EDGE-5GDSP-2-CU-1), similarly with the Core Segment. In this case, our solution is deployed in the Core Segment, where the traffic is mirrored and received by the Service Node. The management node depicted in this scenario is out of the scope of the presented work and thus not considered for the experiments. The attack triggered by the botnets target to the victim node tagged as VICTIM in Fig. 3. The experiments have measured the detection time of the attack for different CORE scenarios that follow the same scheme of the one in Fig. 3 but changing the number of UE devices that compose the botnet. The detection time is measured from the starting time of the malicious flow to the time when the enhanced alert is reported. Two different sets of experiments have been run using two different traditional NIDSs, Snort and Suricata. Fig. 4 shows the results for the two sets of experiments, ranging the size of the botnet from 2 to 512 UE devices. Each experiment has been repeated for the two different attack bandwidths, 25 Mb and 50 Mb respectively.

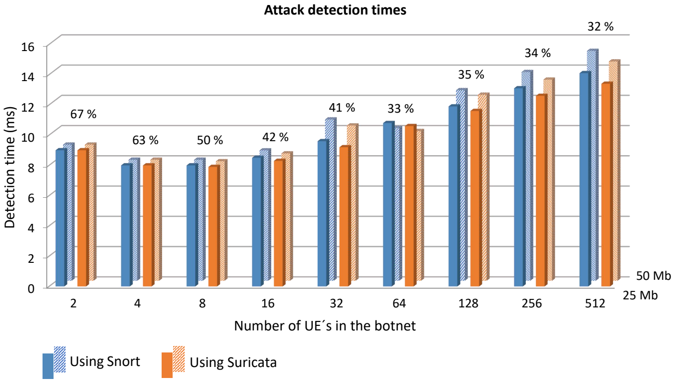

Fig. 4. Detection times of attack of 25 Mb and 50 Mb launched from a botnet composed by different number of UE devices

In terms of the traditional NIDS used it can be concluded that both have a very similar behaviour not affecting the overall performance. Furthermore, the results show a detection time of less than 16 milliseconds for the worst scenario, a botnet with 512 UE devices and a 50Mb attack bandwidth. The overhead added by the Alert Enhancer is showed as a percentage of the total time, being 32% for the larger botnet, equivalent to 6 milliseconds of the total detection time, which is an acceptable overhead for a detection system taking into account the benefits of the improved accuracy for a future efficient mitigation system. A very important aspect to highlight from the results is that the behaviour of the system is similar

TABLE I
METADATA INCLUDED IN ALERTS

Feature	Traditional NIDS	Alert Enhancer
sensor id	✓	✓*
event id	✓	✓*
event second	✓	✓*
event microsecond	✓	✓*
signature id	✓	✓*
generator id	✓	✓*
signature revision	✓	✓*
classification id	✓	✓*
priority id	✓	✓*
Outer Source IP	✓	✓
Outer Destination IP	✓	✓
Outer Source port	✓	✓
Outer Destination port	✓	✓
protocol	✓	✓
impact flag	✓	✓*
impact	✓	✓*
blocked	✓	✓*
flowId	✗	✓
parentFlowId	✗	✓
Outer MAC Src	✗	✓
Outer MAC Dst	✗	✓
Inner MAC Src	✗	✓
Inner MAC Dst	✗	✓
l3Proto	✗	✓
Inner Source IP	✗	✓
Inner Destination IP	✗	✓
l4Proto	✗	✓
flowLabel	✗	✓
Inner Source Port	✗	✓
l7Proto	✗	✓
l7Key1-5	✗	✓
encapsulationLayer (e.g. 0,1,2)	✗	✓
encapsulationId (e.g. VNID, TEID)	✗	✓
encapsulationType1-5 (e.g. vxlan, gtp)	✗	✓
packetStructure	✗	✓
completePacketStructure	✗	✓
firstPacketSeen	✗	✓

** means that this feature is inherited from the Traditional NIDS.*

regardless the number of UE devices in the botnet and the bandwidth of the attack.

Beyond the detection times, a very important validated contribution is the advanced information provided in the enhanced alert that assures a crucial improvement in the accuracy of the mitigation of the attack. Table I details a comparison of the features provided by both the traditional NIDSs and the proposed Alert Enhancer. The key features for an accurate mitigation at any point of the network are highlighted in bold. Most of them are provided only by the Alert Enhancer, especially those related to the inner layers of the packet, crucial information for the traceback of the attacker.

IV. Conclusion

In this paper, a novel approach is proposed to achieve advanced trace back of the source of a DDoS attack with a mobile botnet. The implementation of the proposed solution uses a realistic 5G infrastructure, overcoming the current limitations of the traditional NIDSs. This approach is the first step towards proper mitigation of DDoS attacks with mobile UEs employed as attackers. The proposed approach has been empirically tested in a real 5G infrastructure and validated to fill the gaps of the state of the art without adding significant overheads. The overhead added to the detection time of two traditional NIDSs tested is less than 6 milliseconds for an attack triggered by a botnet of 512 mobile UEs with each UE sending a 50Mb flooding attack. The architecture presented is modular and plugin-based, which allows the user to integrate it easily with any other NIDS not explicitly considered in this work.

Acknowledgment

This work was funded by the European Commission Horizon 20205G-PPP Programme under Grant Agreement Number H2020-ICT-2016-2/761913 (SliceNet: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks). This work was additionally funded by the UWS 5G Video Lab project.

References

[1] Ericsson, "Ericsson Mobility Report November 2018," Tech. Rep., 2018. [Online]. Available: www.ericsson.com/mobility-report

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6489876/

[3] Y. C. Wu, H. R. Tseng, W. Yang, and R. H. Jan, "DDoS detection and traceback with decision tree and grey relational analysis," in *3rd International Conference on Multimedia and Ubiquitous Engineering, MUE 2009*. IEEE, jun 2009, pp. 306–314. [Online]. Available: http://ieeexplore.ieee.org/document/5318904/

[4] P. P. P. Architecture and W. Group, "5G PPP Architecture Working Group - View on 5G Architecture (Version 2.0)," 5G PPP Architecture Working Group, Tech. Rep., 2017. [Online]. Available: https://5g-ppp.eu/white-papers/

[5] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S240595951730019X

[6] "LNICST 115 - A Comparative Analysis of Various Deployment Based DDoS Defense Schemes," Tech. Rep., 2013. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-642-37949-9_53.pdf

[7] A. S. Pimpalkar and A. R. B. Patil, "Detection and defense mechanisms against DDoS attacks: A review," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, mar 2015, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7193118/

[8] P. Farina, E. Cambiaso, G. Papaleo, and M. Aiello, "Are mobile botnets a possible threat? The case of SlowBot Net," *Comput. Secur.*, vol. 58, pp. 268–283, may 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816300086

[9] M. Anagnostopoulos, G. Kambourakis, and S. Gritzalis, "New facets of mobile botnet: architecture and evaluation," *Int. J. Inf. Secur.*, vol. 15, no. 5, pp. 455–473, oct 2016. [Online]. Available: http://link.springer.com/10.1007/s10207-015-0310-0

[10] J. Francois and O. Festor, "Anomaly traceback using software defined networking," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, dec 2014, pp. 203–208. [Online]. Available: http://ieeexplore.ieee.org/document/7084328/

[11] Z. Fan and R. Liu, "Investigation of machine learning based network traffic classification," in *2017 International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, aug 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/8108090/

[12] V. L. Nguyen, P. C. Lin, and R. H. Hwang, "MECPASS: Distributed Denial of Service Defense Architecture for Mobile Networks," *IEEE Netw.*, vol. 32, no. 1, pp. 118–124, jan 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8270642/

[13] "README.unified2," 2018. [Online]. Available: https://www.snort.org/faq/readme-unified2

[14] M. Goldstein, "BoNeSi, the DDoS Botnet Simulator." 2006. [Online]. Available: https://github.com/markus-Go/bonesi

[15] "Common Open Research Emulator (CORE) — Networks and Communication Systems Branch." [Online]. Available: http://www.nrl.navy.mil/itd/ncs/products/core