Teaching network security in mobile 5G using ONOS SDN controller

Christos Bouras*†, Anastasia Kollia†, Andreas Papazois†
*Computer Technology Institute & Press "Diophantus", Patras, Greece
†Computer Engineering & Informatics Dept., University of Patras, Greece
bouras@cti.gr, akollia@ceid.upatras.gr, papazois@ceid.upatras.gr

***Abstract*—Software Defined Networking (SDN) constitutes a fundamental technological solution which responds to the most essential challenges in 5G and beyond networks. Security still remains one of its most controversial issues. Security should be ensured in order to create reliable and consistent networks and on line applications and satisfy the demands of Service Level Agreements (SLAs). Therefore, teaching security of SDN and NFV is fundamental for academia these days. In this paper, we are going to summarize the most fundamental issues related to SDN security challenges and problems appearing alongside with the key back-doors in future SDN mobile networks. Several solutions utilizing SDN capabilities are suggested to avoid SDN security issues. We are also presenting experiments of network topologies using well-known network attack scenarios performed to showcase how networks' security could be taught using SDN controllers. Experiments are conducted using the Open Network Operating System (ONOS) controller indicating that security teaching using ONOS controller is easy and offers many benefits. Future research activity in the field is proposed.**

***Keywords*—SDN, NFV, 5G, security, ONOS, IPRAN, MCORD, mobile networks, teaching, experimentation**

I. Introduction

Cloud computing has become very promising regarding 5G network development. Software Defined Networking (SDN) is prototyped by the OpenFlow protocol and results into flexible, scalable, highly efficient and centralized architectures. Despite these advantages, SDN appears to face several security issues, without special provision of which, the adoption of SDN will be reluctantly faced by enterprises and large organizations. Teaching 5G security is of primary importance for academia, research and development, as SDN will raise a new approach for developing 5G networks.

The centralized network control, which is introduced in SDN among many fundamental benefits, has also many drawbacks. For example, security is doubted, because if an attacker/bot/application takes over the controller, namely the intelligence part of the network, it would take over the whole network without letting it function properly. As a result, this would lead to Denial Of Service (DOS) or Distributed Denial Of Service (DDOS) attacks if the controller or a cluster of controllers are attacked respectively. There are also some other minor attacks that cause additional trouble and should be solved (Eavesdropping, Data Modification, Identity Spoofing, Password based, Man In the Middle (MITM), Compromised Key, Sniffer, Application layer).

Although many efficient solutions have already been presented regarding the conventional systems' security, SDN's security has not adequately been investigated. SDN has been thoroughly analyzed concerning its architectural framework [1], [10], its abstraction levels (application, infrastructure, controller), its protocols for mobile, wireless and wired cases [1], [3], [11]. Academic students should be taught that classic security solutions may not apply to SDN networks.

The most fundamental ideas about security in SDN networks, that should be presented in security tutorials are summarized below. The security system presented in [15] and [17] differs from conventional SDN security systems. It is a possible response to DDOS attacks and is called DaMask-D. New trends and characteristics alongside with the main challenges of DDOS attacks are summarized in [16]. The principles and practices for securing SDN are presented by the Open Networking Foundation (ONF) [12]. The most fundamental challenges regarding the SDN are summarized by the ONF in [12], including: architecture, centralized control, programmability, challenges of integrating special legacy protocols and the cross domain connections.

Hybrid Cloud remains the ideal solution for cloud networking, because it allows hiding the crucial infrastructure while it enables public commercial applications [8]. When a botnet or another type of attack occurs, measures solve the problems [18]. DDOS flooding attack is presented and several measures to combat it are summarized.

Controllers are able to update and delete flow entries, to react responding to packets and pro-act with pre-defined rules [9]. Real-time rules help improving security throughout the operational phase of the network. Nowadays, the augmenting rate of network attacks is dealt with [7]. MITM attacks are possible in switches and connected hosts since network intelligence is nested into the controller [13].

Several techniques, such as flooding, Network Time Protocol (NTP) amplification, malformed packets are utilized by DDOS flooding in order to attack centralized frameworks [4]. Most time elapses until attacking packets in traffic are detected.

Different abstraction levels in SDN are important sources of attacking problems in SDN based architectures [14]. Although several flow based techniques are used for detecting DDOS attacks, filtering rules are fundamental for the maximization of the dropped malicious traffic. Mobile network security is enabled through the SDN technology and its most fundamental benefits [6].

Potential back-doors existing in SDN networks are: switches, base stations and access points, controller and cluster of controllers, applications in the application layers and malicious hosts (Internet of Things (IoT) devices, mobile phones, personal computers (PCs) etc).

SDN network teaching has been presented in [5], but has not adequately been investigated. We have already published a comparative research activity of SDN and NFV in 5G [2]. In this research activity, we gather the most important background studies concerning the security in SDN, we notice the basic controversial issues raised, we propose several solutions in relation to the referred problems. We explain the most fundamental principles of training academic students in security concerning 5G networks. We perform several experiments of network attacking in mobile networks recording the reactions of the ONOS controller. These experiments could be used for educational purposes in network laboratories.

The remaining part of this paper is structured as follows: In Section II SDN security challenges, that should be discussed in networking tutorials are presented. In Section III authors propose important ideas and solutions to enhance security in networking infrastructure. In Section IV authors perform

several experiments concerning attacks in SDN systems using the ONOS controller, that could be introduced in network security laboratories. In Section V the conclusions about the usage of ONOS in network security tutorials are summed up and future research in the field is proposed.

II. SDN SECURITY CHALLENGES

In this section the main security unsolved challenges, that easily confuse students and should be explained, are presented. 5G mobile networks will consist of extremely different devices and technologies, such as IoT, mobile devices, hosts, adhoc networks, etc. Fig. 1 depicts all the possible types of attacks that happen in mobile SDN systems. The network is split in three different layers. In the infrastructure layer attack one or several switches or access points may bring extra traffic in the network. In the application layer an application drains all network resources by sending continuous requests for packet routing into the controller(s). In the controllers' layer attack, if one or more controllers are victimized, traffic is not normally forwarded and the network could become non functional.

SDN security is intercepted by some of the SDN's properties. Firstly, the OpenFlow protocol contains weaknesses into communication between devices, regarding the centralize nature of the network and the low intelligence of switches. Interception probably leads to information disclosure. The OpenFlow switches are easily impersonated by malicious hosts.

Although DDOS attack is the most perilous one as it puts a large part or the whole network out of order, there are also other network attacks that may cause less crucial problems, but are also dangerous for the operation of the network. Network intelligence is included only inside the controller and as a result, all other network parts, such as white-box switches included in the infrastructure layer and all kinds of applications have to communicate with the controller. Therefore, the controller becomes the main attack target. All communication mechanisms between all SDN layers are possibly attacked. The simplification of the switches and network devices, which are replaced by NFVs rend them tempting attacking points.

Attackers (individuals or botnets) do not want to be stopped, want to preserve gained access and share their attacking information into underground communities. Most attackers perform attacks to be amused, to damage systems, out of competitiveness, as a way to be distinguished among other users. Some malicious attacks happen by accidental incidents as well. The most common SDN network attacks, that should be analytically explained, are summarized below:

- **Eavesdropping:** is the type of attack, that communication between devices is monitored secretly by some other part except for the devices communicating and is performed in the following sides of SDN mobile networks: communication between base stations, access points & base stations, access points & controller, switches & controllers, controller & applications, all switches and applications.
- **Identity spoofing:** is the type of the attack, in which the user is using an IP, that is not authorized to use. For example, in SDN an attacker could take control of the IP of a mobile host into a private network or even take over the controller itself.
- **Password-related attacks:** Most controllers include an authorization system for their manager.
- **MITM attack:** in this type of attack the attacker may intervene or even alter the communication between two parties, that consider their communication is unimpeded.
- **Sniffer attack:** is the application that is able to capture several network packets.
- **Applications:** The application layer itself contains both public and private applications. If an application is attacked it could resolve to send requests to servers or to the controller for routing of packets wasting CPU and bandwidth resources.
- **DOS:** is the type of network attack and the network does not respond properly. Such attacks possibly happen when:
  - A fast mobile connection sends packets for routing continuously, while other packets of more slow connections remain inactive.
  - Controller is vacuumed of its routing table or it is filled with IPs that not correspond to actual destinations (access points, base stations).
  - Poses the controller out-of order.
- **Sensitive Data Protection:** Most mobile devices do not have passwords enabled. Communication channels are unsafe for data. If a mobile phone is into a Bluetooth open connection could be traceable by devices and become target. Wireless transactions are not always encrypted and it becomes easier to intercept bank accounts, passwords, personal data etc.
- **Security into software:** Devices' software could be out-of-date or untrusted, may include unauthorized configurations.

Fig. 2 considering the weak points of the mobile networks in 5G, which are based on SDN controllers and NFVs, presents the main steps an attacker follows in order to find a back-door and perform attacks. Access points, base stations, mobile network services, such as Mobile Office Re-architected as a Data Center (MCORD) services, Address Resolution Protocol (ARP) tables, Dynamic Host Configuration Protocol (DHCP), password checking access are possible unsafe components.

III. PROPOSED SOLUTIONS FOR SECURITY ISSUES

It should also be explained that security is not only fundamental for systems' viability, but also because network providers are bounded by strict Service Level Agreements (SLA), which impose stipulations and in case several requirements are not provided, may lead to large fines and penalties. Standard security solutions may not apply to SDN networks because of their nature that is centralized and includes several abstraction layers.

According to [12], a designing scheme should:

- Define the security dependencies and the trust boundaries of the mobile networks
- Assure robust identity of access points/base stations
- Build security policies based on open standards
- Protect all SDN layers (application, infrastructure, controller) and their interconnections
- Protect operational data between controllers and access points
- Initialize system design with security standards
- Provide accountability and traceability of unknown devices and hosts
- Analyze the exact properties of manageable security controls

Several solutions that ensure network security using the SDN systems and could be explained to students, are discussed below:

- **General security guidelines:** Pro-activeness is a good idea. Security should be taken into consideration a priori. All network components' information should be frequently backed up.
- **Firewalls:** are built using NFV including well-known network functionality and induce all the software advantages. In SDN networks, firewalls should be active and

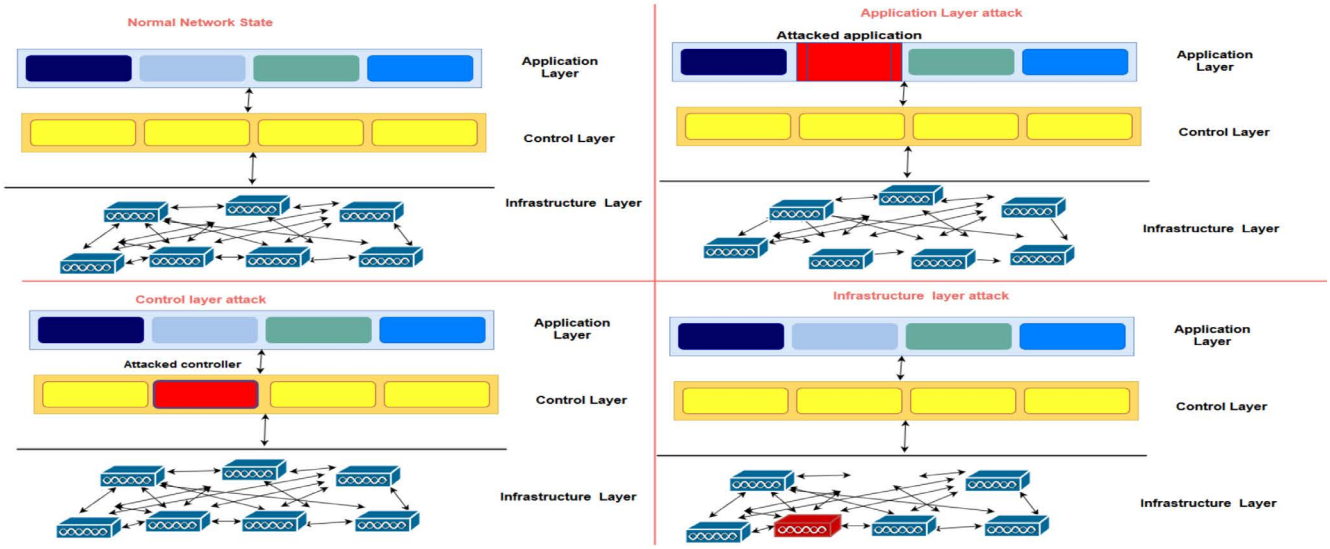

Fig. 1: The possible type of network attacks in an architecture based on SDN.

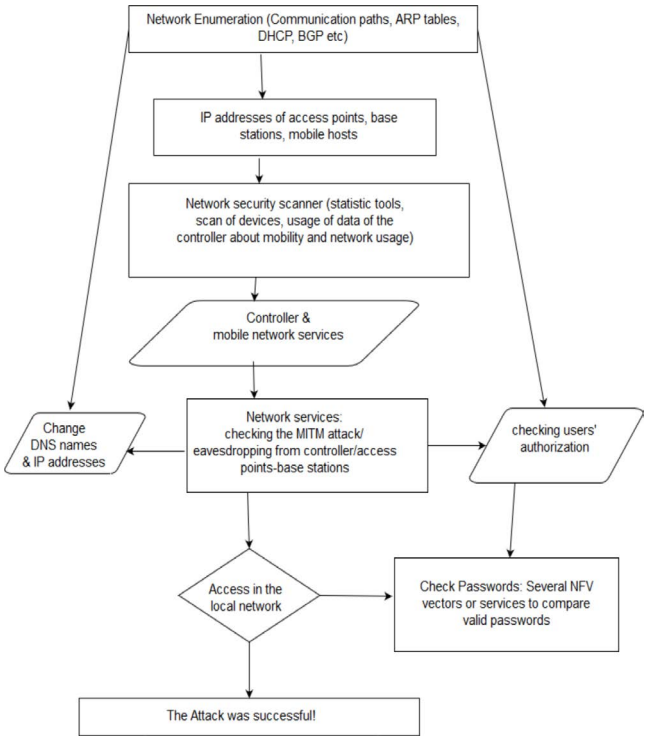

Fig. 2: Description of the methodology of attacking networks in 5G.

well-designed. As NFVs are software sources, so it is important that special check is implemented and quality assurance mechanisms are followed.

- **Option of administrative passwords:** should be complex and not easily guessed by some possible intruder. A probable solution would be to introduce several layers of a user to get into the interface of the controller. Alongside, only particular IPs should have access to the controller interface.
- **All systems should be updated:** All networking software, functionalities, NFVs, interfacing etc. should be regularly updated so as to keep up with the latest versions. Operating system packages should be regularly upgraded.
- **Protected Media Access Control (MAC) addresses:** should not be open and visible by other users or they could change dynamically so as not to be traceable.
- **Monitor Packets to save controllers:** SDN technology allows several controller instances to exist in the whole system. As a result, one or a cluster of controllers in the control layer could not forward packets but crosscheck packets received to save main functional controllers and avoid DDOS attacks.
- **Security plan creation:** It is fundamental that a special security plan is created and that everyone respects it. A ”Plan B” should be applied if the whole network is attacked.
- **Strengthen authentication strategies:** Strict strategies should be applied so that networks are not susceptible to attacks. Several encryption policies could be adopted to avoid eavesdropping.
- **Remote disabling of lost devices:** As a lost mobile device is a back door to many private data of its owner, it would be fundamental if the devices could be disabled remotely.
- **Testing Techniques:** is an effective way of crosschecking if a different party is implicated in the communication.
- **Last network level:** Special care should be taken among the switches, the base stations, the access points and the connected hosts. Mobile hosts are the last part of the network so an influx of the attacker is possible by white-box switches or IoT devices/hosts.
- **Authentication of Applications:** In several SDN controllers e.g the ONOS controller there is an option of securing the control layer from the application layer. There could be application authentication to limit unknown or untrusted apps to drain all network’s resources. Role-based or permission based access control so that only specific applications gain access into the control layer.
- **White-listing:** could be a solution not only for applications, network managers, routes, hosts, mobile devices. Several white-lists could be made in order to avoid such problems.
- **Encryption:** is essential not only for the two factor communication and authentication of communication between users, but could also be a tool for data stored into the device or the external media.

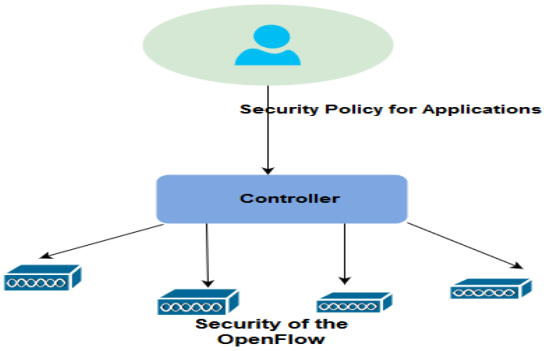

Fig. 3: The general concept of the security mode in SDN.

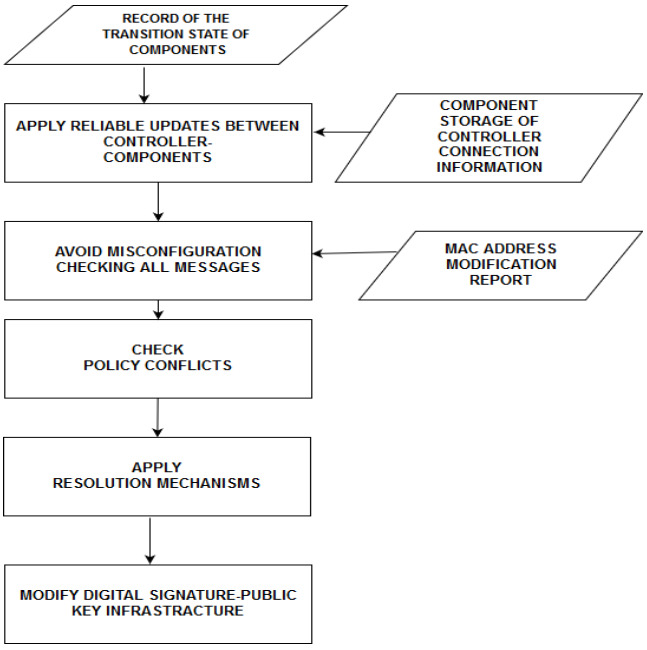

Fig. 4: Description of the methodology of securing networks in 5G.

Fig. 3 presents the graph of the security standards of the security mode of SDN. The controller is the network orchestrator and manages the whole network. Stricter policy is implemented and could present the control layer the southbound and the northbound APIs as a whole, which makes it hard for an application to attack them. Fig. 4 describes a possible model, that should be respected regarding security in 5G. Log transition state of all the components, components-controllers connection information and MAC address modification report are input regularly. Several processes should be created so as to check all updates' reliability, validate messages to avoid unintended consequences of misconfiguration. Controller should keep up with policy conflict resolution mechanisms. A Public Key Infrastructure (PKI) should ensure security in the controller.

IV. Experimentation

In this section, there are several tests concerning the security of a mobile SDN architecture using the ONOS controller, that could be used for teaching mobile network security in 5G. The ONOS controller is used for experimentation as it is simple, contains a unix-like interface and many use cases that could be used for network tutorials for wired, wireless and mobile SDN.

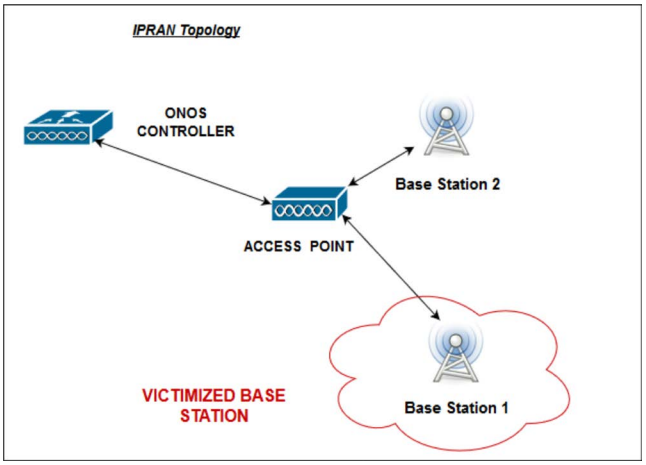

Fig. 5: Experimental topology of mobile network with a victimized Base Station.

There are two modes enabling ONOS security mode enabled and not enabled.

Before enabling the ONOS security-mode:

- Starting the ONOS and executing "summary" before introducing each topology, the only device existing in the controller interface is the controller.
- After introducing each topology and executing "summary", inside the network there are the devices that communicate with the controller interface.
- After ping tests for the connectivity, the "flows" command shows nothing into the ONOS controller.
- Executing the command "devices" the controller and the access point are not visible in the ONOS interface.

After enabling the ONOS security-mode: The ONOS security-mode enhances the robustness of the network. A starting version is available for experimenting although, this is a project that is on progress. To enable the security-mode of the ONOS environment on, the following actions should happen:

- Firstly, it is needed to enable the karaf secure version **onos-setup-karaf secure**
- and then it is important to enable the "ONOS tarball" using the **onos-package -s -t**.

A. Radio Access Network (RAN)

In Fig. 5 the tested topology is presented. It is based on the IPRAN use case of ONOS. In this topology, there are 2 base stations and 1 access point. The base stations are connected to the access point. The access point communicates with the ONOS controller. The whole topology is controlled by ONOS. The base station (sta2) is flooded by large traffic, which is produced by the other base station (sta1), which is victimized. A malicious user takes over the base station sta1 and sends packets into the other base station incessantly.

The two following commands should run to make the one station victimized and send a large number of packets (10.000.000.000) into the other one:

- For the base station 1: **sta1 ping -s &**
- For the packets exchanged: **sta1 ping -c 10.000.000.000 sta2**

The experiments are conducted enabling the security-mode of ONOS on and off. This security configuration is able to ensure that the ONOS controller is protected when it comes to malicious attacks. Most malicious attacks could be prevented. The security mode of ONOS is actually an ongoing project.

This fact means that several fundamental configurations and functionalities could be added to novel version of the ONOS controller, which could lead to clever architectures protecting the network infrastructure.

Initially, when security-mode is off whatever experiment is conducted no results are visible in the interface of the controller. After starting the topology, the experiments **devices**, **flows** and **summary** on the ONOS controller are not showing the devices or the data flows into the controller interface.

After the security-mode of the ONOS controller is enabled, the following experiments are conduced:

- Starting the ONOS and executing ”summary” before introducing the topology, the only device existing in the controller interface is the controller.
- After introducing the topology and executing ”summary”, inside the network there is another device in the controller interface that is the access point.
- After the ping test for the connectivity, the ”flows” command shows the necessary components that are integrated in the ONOS controller.
- Executing the command ”devices” the controller and the access point are visible in the ONOS interface.
- Executing the ”net” there are the sta1, the sta2 and the ap, namely the two base stations and the access point.

Packets are exchanged infinitely. At any time the controller could kill this flow. For example, checking the transmission time could be a criterion that a device or node, in this case the base station, is victimized by a malicious user. As a result, after a predefined time, a malicious flow could be killed. What is more, when security-mode is on all conducted experiments are obvious and results are recorded into the side of the controller and become visible in the controller interfacing. After starting the topology, the experiments **devices**, **flows** and **summary** on the ONOS controller show the devices, the data flows existing in the controller interface.

B. Heterogeneous Network

In Fig. 6 the tested topology is presented. In this topology, there are 2 base stations, 1 access point, 4 switches connected with 4 hosts connected to each one of them. The base stations are connected to the access point. The access point communicates with the ONOS controller. All switches communicate with the controller. The whole topology is controlled by ONOS. The simple white-box switches are used as virtual routers, because programmable logic is integrated to them and except simple switching they have routing capabilities. A switch is victimized by an attacker as a result it is possible for the attacker to control the packet routing, change the ARP table or even stop the routing of the packets.

The switch functions as a virtual router. A malicious user takes over the switch s3 and sends packets into the other base station incessantly. The two following commands should run to make the switch victimized:

- For the switch s3: **xterm s3**
- For the packets exchanged: **tcpdump -i any**

Initially, when security-mode is off whatever experiment is conducted there are not any results from the side of the controller. After starting the topology, the experiments **devices**, **flows** and **summary** on the ONOS controller are not showing the devices or the data flows into the controller interface.

After the security-mode of the ONOS controller is enabled, the following experiments are conduced:

- Starting the ONOS and executing ”summary” before introducing the topology, the only device existing in the controller interface is the controller.
- After introducing the topology and executing ”summary”, inside the network there is another device in the controller interface that is the access point.

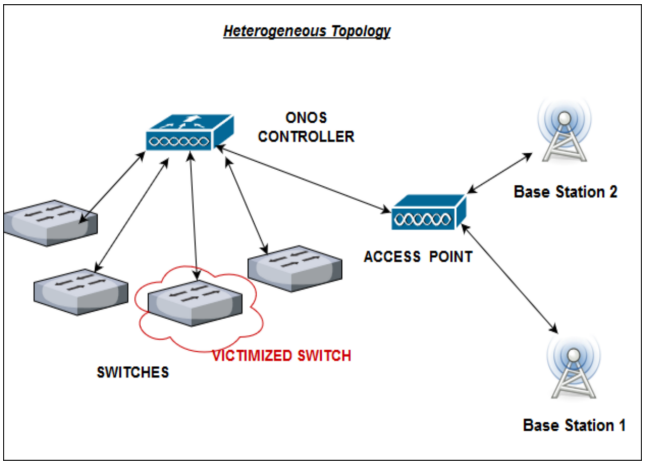

Fig. 6: Experimental topology of an heterogeneous network with a victimized virtual router (switch).

- After the ping test for the connectivity, the ”flows” command shows the necessary components that are integrated in the ONOS controller.
- Executing the command ”devices” the controller and the access point are visible in the ONOS interface.
- Executing the ”net” there are the sta1, the sta2, the ap, the switches and the hosts.

Packets are externally monitored. This is a case of eavesdropping. The controller could not stop this flow, because it may be a flow of the normal network. For example, if the ARP table is modified it is possible that the controller considers it a normal behavior and confronts these packets as normal ones that just change the routing tables, because they add new routes in the network. After starting the topology, the experiments **devices**, **flows** and **summary** on the ONOS controller show the devices, the data flows existing in the controller interface.

C. Results

Security is one of the most fundamental issues concerning the next generation of mobile networks. 5G raising demands require significant properties for the next generation of mobile networks. The combination of SDN and NFV is fundamental and provides highly efficient, high performance and high coverage networks. So it could be a viable solution for 5G if its most common security problems are faced. Teaching 5G security could be easy using the ONOS controller and is also indispensable for modern network tutorials, as 5G networks will be based on SDN and virtualization techniques.

Most security challenges of SDN networks should be thoroughly explained to students, such as eavesdropping, identity spoofing, password-related attacking, MITM, sniffer, DDOS & DOS, software & application security. In this direction, experimental examples in ONOS could help.

Solutions are different than in conventional network systems, such as: creating security guidelines, firewall protection, strong administrative passwords, system updating, protection of MAC addresses, packet monitoring, security plan, several authentication strategies, disabling the lost devices, last network level, authentication of applications, white & blacklisting, novel encryption mechanisms should be analyzed.

Creating and reviewing a methodology of attacking could lead to find and show system’s vulnerabilities. Therefore, teaching weak points, proposing solutions, enhancing and strengthening of network security is vital for academic students.

SDN controllers should be more carefully designed so that security difficulties are avoided. ONOS offers a security mode. It is an ongoing project, which means that several issues concerning the security could also be considered. Several types of attacks could be avoided if the controller monitors the network traffic and several rules should be implemented and deployed to cut down on the security issues. The security mode of ONOS is actually an ongoing project. This fact means that several fundamental configurations and functionalities could be added to newer versions of the ONOS controller, which could lead to clever architectures protecting the network infrastructure.

The experiments conducted could be used to explain problems of security in mobile, adhoc and heterogeneous networks and introduce students to a new approach of understanding such essential problems. Analytically, students understand IPRAN use cases, mobile networks, mobile network configurations, introducing mobile network components, security protocols, cryptographic mechanisms, SDN controllers security modes in securing networks, virtualizing testings.

The ONOS controller offers fundamental benefits. Students could:

- Create and introduce mobile and heterogeneous topologies
- Deeply understand of network security issues, controller and abstraction layers
- Create mobile network topologies
- Teach 5G security requirements & challenges
- Analyze SDN and virtualization differences of conventional security
- Deepen in different types of network attacking by experiments and examples
- Outline security requirements of virtualized components
- Explain security protocols (Transport Layer Security (TLS), Secure Sockets Layer (SSL))

Finally, ONOS controller is easy as it is a unix-like controller, it also has a big active community. Students and tutors could profit from its flexibility in order to help them understand and teach novel technologies respectively. SDN and NFV will be fundamental in the teaching process as it consists integral solution for 5G and future networks in general, so students should be introduced in this kind of networks.

V. Conclusions & Future Research Activity

In this paper, the background literature regarding the security was overviewed. Several fundamental challenges of the security were analyzed. We summarized the methodology for attacking mobile networks. We modified the existing methodology of securing wired networks and proposed several ways of protecting mobile networks and devices. Experiments were conducted concerning attacks in mobile networks, that showed that teaching could be easy and efficient using ONOS. Conclusions, related to the security of networks in 5G were summarized.

Future research activity in the field could provide security mechanisms and modified editions of communication protocols of most layers, such as the Border Gateway Protocol (BGP), the User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Internet Protocol (IP) version 4 and 6, the Address Resolution Protocol (ARP), Secure Sockets Layer (SSL) and Transport Layer Security (TLS). What is more, several actions could be taken into consideration so that OpenFlow protocol is modified in accordance with security principles and prototypes. Several more efficient cryptographic mechanisms could be investigated and implemented in order to enhance security in SDN systems. It is fundamental to find all possible back-doors of the mobile networks using Quality Assurance & Testing mechanisms which will indicate the weaknesses of the SDN framework. The solutions of the 5G security problems will integrate many fundamental measures.

References

[1] C. Bernardos, A. De La Oliva, P. Serrano, A. Banchs, L. Contreras, H. Jin, and J. Zuniga. An architecture for software defined wireless networking. *Wireless Communications, IEEE*, 21(3):52–61, June 2014.

[2] C. Bouras, A. Kollia, and A. Papazois. Sdn & nfv in 5g: Advancements and challenges (icin2017, paris, france, 7-9 march 2017). In *Proc. 20 th ICIN Conference Innovations in Clouds, Internet and Networks (ICIN2017, Paris, France, 7-9 March 2017)*, Paris, France, 2017.

[3] A. Bradai, K. Singh, T. Ahmed, and T. Rasheed. Cellular software defined networking: A framework. *Communications Magazine, IEEE*, 53(6):36–43, 2015.

[4] T. Chin, X. Mountrouidou, X. Li, and K. Xiong. Selective packet inspection to detect dos flooding using software defined networking (sdn). In *2015 IEEE 35th International Conference on Distributed Computing Systems Workshops*, pages 95–99. IEEE, 2015.

[5] S. Cosgrove. Teaching software defined networking: It's not just coding. In *2016 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pages 139–144, Dec 2016.

[6] X. Duan and X. Wang. Authentication handover and privacy protection in 5g hetnets using software-defined networking. *Communications Magazine, IEEE*, 53(4):28–35, April 2015.

[7] J. François, L. Dolberg, O. Festor, and T. Engel. Network security through software defined networking: A survey. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications*, IPTComm '14, pages 6:1–6:8, New York, NY, USA, 2014. ACM.

[8] B. JAMES. Security and privacy challenges in cloud computing environments.

[9] R. Jin and B. Wang. Malware detection for mobile devices using software-defined networking. In *Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop*, GREE '13, pages 81–88, Washington, DC, USA, 2013. IEEE Computer Society.

[10] I. Ku, Y. Lu, and M. Gerla. Software-defined mobile cloud: Architecture, services and use cases. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International*, pages 1–6. IEEE, 2014.

[11] X. J. L. E. Li, L. Vanbever, and J. Rexford. Cellsdn: Software-defined cellular core networks. 2013.

[12] OPEN NETWORKING FOUNDATION. Principles and practices for securing software-defined networks. Technical report, OPEN NETWORKING FOUNDATION (ONF), January 2015.

[13] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran. Security in software-defined networking: Threats and countermeasures. *Mobile Networks and Applications*, pages 1–13.

[14] M. Vizváry and J. Vykopal. Future of ddos attacks mitigation in software defined networks. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pages 123–127. Springer, 2014.

[15] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou. Ddos attack protection in the era of cloud computing and software-defined networking. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 624–629, Oct 2014.

[16] Q. Yan and F. R. Yu. Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine*, 53(4):52–59, April 2015.

[17] Q. Yan, F. R. Yu, Q. Gong, and J. Li. Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys Tutorials*, 18(1):602–622, Firstquarter 2016.

[18] 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*, 15(4):2046–2069, Fourth 2013.