Performance Analysis of Between Software Defined Wireless Network and Mobile Ad Hoc Network Under DoS Attack

Hüseyin POLAT
Department of Computer Engineering
Gazi University
Ankara, Turkey
polath@gazi.edu.tr

Onur POLAT
Department of Computer Engineering
Gazi University
Ankara, Turkey
onurpolat@gazi.edu.tr

Esra SÖĞÜT
Department of Computer Engineering
Gazi University
Ankara, Turkey
esrasogut@gazi.edu.tr

O. Ayhan ERDEM
Department of Computer Engineering
Gazi University
Ankara, Turkey
ayerdem@gazi.edu.tr

***Abstract*—The traditional network used today is unable to meet the increasing needs of technology in terms of management, scaling, and performance criteria. Major developments in information and communication technologies show that the traditional network structure is quite lacking in meeting the current requirements. In order to solve these problems, Software Defined Network (SDN) is capable of responding as it, is flexible, easier to manage and offers a new structure. Software Defined Networks have many advantages over traditional network structure. However, it also brings along many security threats due to its new architecture. For example, the DoS attack, which overloads the controller's processing and communication capacity in the SDN structure, is a significant threat. Mobile Ad Hoc Network (MANET), which is one of the wireless network technologies, is different from SDN technology. MANET is exposed to various attacks such as DoS due to its security vulnerabilities. The aim of the study is to reveal the security problems in SDN structure presented with a new understanding. This is based on the currently used network structures such as MANET. The study consists of two parts. First, DoS attacks against the SDN controller were performed. Different SDN controllers were used for more accurate results. Second, MANET was established and DoS attacks against this network were performed. Different MANET routing protocols were used for more accurate results. According to the scenario, attacks were performed and the performance values of the networks were tested. The reason for using two different networks in this study is to compare the performance values of these networks at the time of attack. According to the test results, both networks were adversely affected by the attacks. It was observed that network performance decreased in MANET structure but there was no network interruption. The SDN controller becomes dysfunctional and collapses as a result of the attack. While the innovations offered by the SDN structure are expected to provide solutions to many problems in traditional networks, there are still many vulnerabilities for network security.**

Keywords—SDN, Controller, MANET, Bandwidth, DoS

I. INTRODUCTION

The rapid growth and development of the IT world brings along many requirements. For example, traditional understanding is no longer sufficient for developing and growing data centers. The development of cloud computing and virtualization technologies also support this situation. With developing technologies, it is becoming increasingly difficult to meet the demands of accessibility, dynamic management, high bandwidth, and high connection speed by traditional networks. As the size, disorganization, complexity, and management problems of traditional networks increase, traditional approaches to configuration and optimization will not be sufficient in the near future [1].

The insufficiency of traditional approaches towards new needs leads to different solutions. One of these solutions is Software Defined Network (SDN) technology. The control and data plane, which coexist in the traditional network structure, are separated in SDN architecture. The control functionality of each device is removed so that each device becomes a simple element that transmits packets. With the SDN structure, the control mechanism is separated from the network devices and carried to an external device. This centralization simplifies the management and programming of the network structure. In addition, the network administrator is prevented from interfering the system incorrectly.

With the spread of SDN architecture, the issue of SDN security is gaining importance. Due to its features that are different from traditional networks, SDN architecture becomes more secure. In the SDN architecture, transmission devices regularly transmit network traffic information to the controller. Using this information, the controller can identify changes in the network, abnormal movements, and devices with malicious behavior. In addition, it applies security policies determined in accordance with these situations [2].

SDN architecture brings different security vulnerabilities with different structures. The most important security issue is attacks on the controller, which acts as the brain of the entire network. Attacks on the controller can prevent centralization of network information and may cause network configuration or routing problems. By hacking the controller by the attacker, the attacker can capture network information and interfere with the network. Such vulnerabilities make it attractive for attackers to focus on the controller [3]. One of the attacks on the SDN controller is DoS or DDoS attacks. With these attacks, it is aimed to consume the controller's resources such as bandwidth, processor, and memory. Thus, the communication between the devices in the entire network is broken and the network collapse is provided [4].

978-1-7281-3789-6/19/$31.00 ©2019 IEEE

Authorized licensed use limited to: ULAKBIM UASL - GAZI UNIV. Downloaded on October 02,2023 at 13:40:36 UTC from IEEE Xplore. Restrictions apply.

In this study, the effects of DDoS attack on controller in software defined wireless networks are analyzed. In addition, MANET network structure was used to show that SDN structure has security problems. DoS attacks were performed on these two networks and comparisons were made in terms of performance. The study consists of six chapters. The first section introduces the study and in the second section, the previous studies are given. In the third section SDN and in the fourth section MANET architectures are mentioned. In the following section, simulation design and results are given. In the last section, the result is given.

II. Related Works

In the field of cyber security, there are many studies dealing with the structure of SDN and the capabilities of SDN. For example, Demetriou et al. have provided a SDN-based solution for the cyber security of devices connected to the home network. They prepared a mobile application to prevent attacks from malicious applications. In order to control the communication between devices and applications, a structure consisting of stages such as device identification, access to the router, routing, monitoring and decision making has been established. This structure was tested and it was found to work effectively [5].

In another study, Karmakar et. al presented a security architecture for IoT networks using the capabilities of SDN. This architecture restricts network access to authenticated IoT devices. Policies were used to maintain network flow, and protocol was used to perform device authentication. The SDN controller acts as a decision maker for security policy. Network switches and gateways implement security policies. This policy and protocol oriented architecture ensures secure and dynamic management of network flows in the IoT infrastructure [6].

Kuerban et al. proposed a solution for DoS attacks on the SDN controller. This proposed structure collects the statistics of the switch and dynamically calculates the bandwidth of the controller. When a DoS attack occurs, this structure collects statistics and instructs the switch port to decelerate. This reduces the impact of the DoS attack on the network, but also affects other switches and normal traffic. It is stated that this structure may cause delays in real-time and dynamic studies [7].

Wang et al. proposed a new solution to protect the SDN structure from DoS attacks. This recommendation introduces new triggers to detect and prevent DoS attacks on both the control and data plane. Tests were performed to capture realistic hardware and software dynamics. Accordingly, DoS attacks were detected in SDN networks that maintained the performance of the data plane at a rate of 99.72% [8].

Yan and Yu reported that SDN is effective in detecting DDoS attacks. It has been emphasized that it is important to use many of the capabilities of SDN in providing this situation. These include software-based traffic analysis, dynamically updating routing rules, network programming, and the presence of a logical central controller [9].

Bawany et al. investigated SDN-based methods used in DDoS intrusion detection and mitigation. According to this study, there are methods such as machine learning, traffic pattern analysis, entropy, connection rate and the use of various detection tools together in intrusion detection. In order to reduce the attack effect, there are features such as deep packet inspection, traffic isolation, control bandwidth, block port, and drop packets [10].

Gkountis et al. conducted a study to prevent DDoS attacks against the SDN controller. To do this, they proposed a lightweight scheme based on a set of rules that can distinguish between packets sent to the network switch based on whether they are malicious or not. Experiments were performed with the Mininet emulator. Evaluations were made according to bandwidth consumption, number of entries in the flow table and CPU usage. The proposed scheme performed better than the older DDoS protection schemes and experiments [11].

Alsumayt et al. proposed a Monitoring, Detection and Improvement method to detect DoS attacks on MANET architecture. This method is based on calculating different values based on whether the nodes are reliable. This method was compared according to another available method with packet delivery rate and network overhead values. According to the results, the proposed method performed better than the present method [12].

III. Software Defined Network

The Software Defined Network architecture offers a flexible and easy-to-manage structure. As shown in Figure 1, the SDN architecture consists of control, data, and application planes.

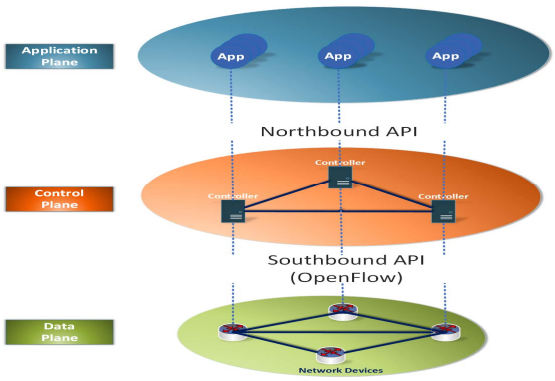


Fig. 1. Software defined network architecture

The data plane consists of transmission devices (such as routers, switches) that act and manage according to the rules set by the controller. These devices are simple and cannot perform complex operations. The other plane is the control plane that programs and manages the data plane. The controller is located in this plane. The controller communicates with the devices in the data plane via the Southbound interface and dominates the entire network with the traffic information it receives. The commonly used OpenFlow protocol provides the communication between the control and the data plane. The last plane is the application plane. In this plane, the controller is guided for policy determination. Communication between the application plane and the controller is carried out via the Northbound interface. With the network information provided by the controller, applications such as security, network monitoring, automation, and troubleshooting can be developed.

Authorized licensed use limited to: ULAKBIM UASL - GAZI UNIV. Downloaded on October 02,2023 at 13:40:36 UTC from IEEE Xplore. Restrictions apply.

IV. Mobile Ad Hoc Network

Mobile Ad Hoc Network is a wireless network that does not have any infrastructure and exchanges data between two nodes. This structure uses wireless media for communication, unlike wired networks. It can be placed in the network quickly and efficiently. Each node there serves as a router for the other nodes. This situation enables data to be routed through long-distance and multi-hop network paths without the need for wired infrastructure.

In the MANET structure, it is difficult to establish a safe path between the source and the target. By interfering with the network from outside, network traffic can be listened. The lack of central control authority and the lack of correct network entry points make it difficult to implement traditional security mechanisms. For these reasons, the MANET structure is vulnerable to noise, malfunction and attack.

Many protocols have been developed for routing on MANET. The most commonly used Dynamic Source Routing (DSR) and Dynamic Destination-Sequenced Distance-Vector (DSDV) prevention protocols were used in this study.

V. Design and Simulation Results

In this section, SDN and MANET structures are compared in terms of security. Topologies were established for both cases.

A. DoS Attack to Software Defined Wireless Network

Mininet-Wifi emulator was used in the study to create Software Defined Wireless Network topology. According to the topology shown in Figure 2, the SDN architecture consists of several elements. These are three Access Points connected to a remote controller (RYU or POX), four stations, and nine users connected to Access Points. Ubuntu 16.04 operating system was used on computers.

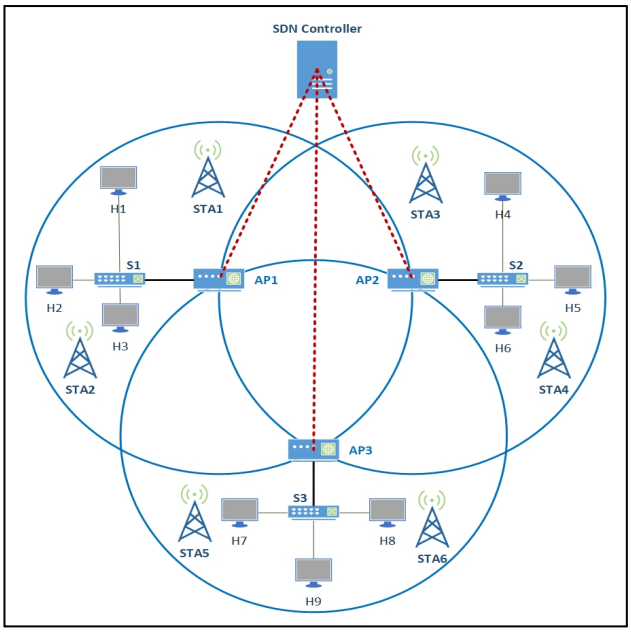


Fig. 2. The topology created within the scope of the study

Within the scenario created in the study, DoS attacks were carried out. These attacks were performed using the free Hping3 tool, which was used to generate TCP/IP packets. Iperf was used to test the bandwidth in the network. Iperf is a tool that can generate TCP and UDP data flows and measure network efficiency and bandwidth. The data from the Iperf tool were visualized with the Gnuplot drawing program. The malicious user in the scenario performed attacks. Three conditions were tested in this study:

- Firstly, only the ping packet was sent to the network. This situation represented the time of no attack.
- Secondly, DoS attacks were performed from random IP addresses from h1 user to h6 user.
- Finally, DoS attacks were performed from random IP addresses from h1 and h2 users to h6 user.

When these three conditions were met, the bandwidth of the network was measured. For this purpose, h3 user was set as client and h4 user was set as server. During the attack, an average of 1500 TCP packets were sent per second (1500 packets/sec). The main purpose of this attack was the depletion of the resources of the controller, which is the brain of the network in SDN architecture. As a result of this attack, access to the controller was prevented. If access to the controller is prevented, the SDN architecture collapses.

B. DoS Attack to Mobile Ad Hoc Network

The Network Simulator Version2 (NS2) simulator was used to create a traditional wireless network structure and the Iperf tool was used to test bandwidth. Data from the Iperf tool were visualized with the Gnuplot drawing program. In the scenario created in the study, a DoS attack was made against MANET just like it was done against SDN. Network performance was tested at the time of the attack. The simulation parameters are given in Table 1.

TABLE I. Simulation Parameters

Parameters	Values
Used Area (m2)	1000x1000
Simulation Time (seconds)	100
Link Layer	Application
Traffic Type	CBR
Number of Nodes	100, 120, 140, 160, 180
Data Type	UDP
Routing Protocol	DSDV, DSR

According to the simulation, two attackers carried out the DoS attack through the node. The speed of the nodes was kept constant by using a random transition point. DSDV and DSR protocols were used separately in simulation to test bandwidth during attack. The main purpose of using both routing protocols in simulation is to better test the attack effects.

C. Simulation Results

The results are discussed in three sections.

1) DoS Attack on POX Controller in SDN Architecture

Authorized licensed use limited to: ULAKBIM UASL - GAZI UNIV. Downloaded on October 02,2023 at 13:40:36 UTC from IEEE Xplore. Restrictions apply.

The DoS attack against the POX controller, one of the controllers in SDN architecture, is given in Figure 3.

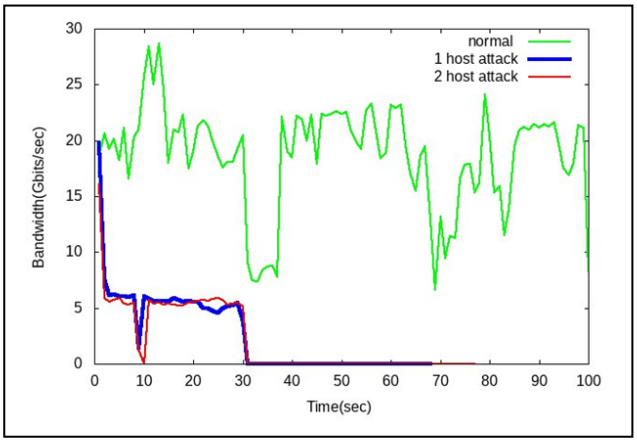


Fig. 3. Bandwidth values at the time of attack on POX controller

As shown in Figure 3, there was no significant change in bandwidth when only the ping packet was sent. This indicates that there is not much packet loss in the network. When the attack was made, the controller's resources were consumed. As the controller's resources are consumed, the controller cannot load a new flow into the switch. Controller flow inputs could not be created for new and normal packets to the network, and the SDN architecture was completely collapsed.

2) DoS Attack on RYU Controller in SDN Architecture

The DoS attack against the RYU controller, another controller in the SDN architecture, is presented in Figure 4.

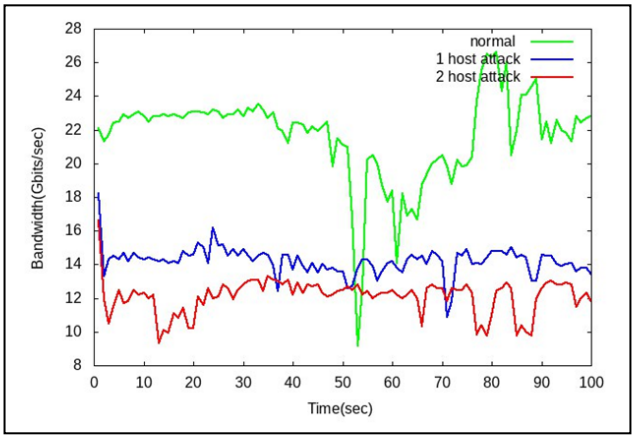


Fig. 4. Bandwidth values at the time of attack on RYU controller

As seen in Figure 4, sending only the ping packet to the network did not cause a large change in bandwidth. As a result of the attacks, the resources of the controller became exhausted and reached critical levels.

During the DoS attacks against RYU and POX controllers, the performance of the RYU controller was found to be better. This result showed that the selection of controllers in SDN architecture is important and affects the whole system.

3) DoS Attack on MANET Architecture

The DoS attack against MANET is shown in Figure 5.

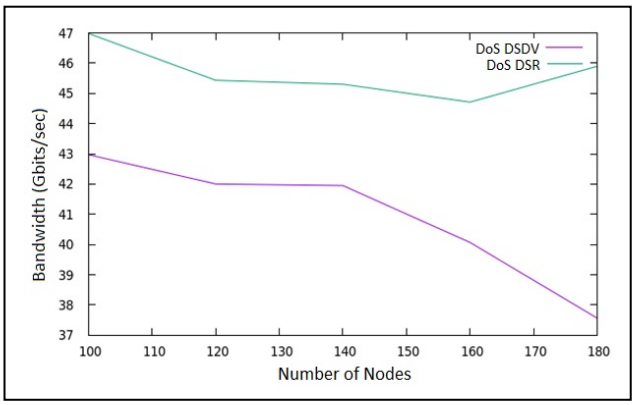


Fig. 5. Bandwidth values at the time of attack on MANET

In this section, two different MANET routing protocols were used as DSDV and DSR. For both protocols, the bandwidth of the network was measured at the time of the attack. Due to the increasing number of nodes in the network, bandwidth reduction was observed when both protocols were used.

When the two protocols were compared, the performance of the DSR protocol was found to be better than the DSDV protocol. The results showed that access to the network was never interrupted during attacks.

VI. Conclusion and Recommendations

SDN architecture, which is expected to be more efficient than traditional networks, has many security vulnerabilities. Traditional security solutions are insufficient for MANET, which is one of the wireless network architectures. When exposed to attacks, the system is affected and its functionality is impaired. Among the many types of attacks targeting SDN and MANET, DoS attacks are the most common.

In this study, DoS attacks against SDN and MANET are discussed. The results obtained from the analyses are vital for SDN and MANET security. When the SDN architecture was under DoS attack, the SDN controller lost its function and the whole system collapsed. The MANET architecture suffered from a loss of performance when it was under attack, but the system survived.

According to the previous studies, SDN architecture is expected to replace the existing traditional network in the near future. Therefore, it is thought that this study which focuses on the security problems of SDN architecture will contribute to the literature and will be a guide for the studies to be done. In order to ensure the security of SDN, further studies and an in-depth investigation of the issue are important for cyber security.

References

[1] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S., "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no 1, pp. 14-76, January 2015.

[2] Kuerban, M., Tian, Y., Yang, Q., Jia, Y., Huebert, B., and Poss, D., "FlowSec: DOS Attack Mitigation Strategy on SDN Controller," In Networking, Architecture and Storage (NAS) 2016 IEEE

Authorized licensed use limited to: ULAKBIM UASL - GAZI UNIV. Downloaded on October 02,2023 at 13:40:36 UTC from IEEE Xplore. Restrictions apply.

International Conference, pp. 1-2, Long Beach, CA, USA, August 2016.

[3] Polat, O., “Detection and mitigation of DoS attacks in software defined networks,” Master’s Thesis, Gazi University Graduate School of Natural and Applied Sciences, Ankara, 2017.

[4] Polat, H., and Polat, O., “The effect of DoS attack on ODL and POX SDN controllers,”In The 8th International Conference on Information Technology (ICIT), Amman, Jordan, May 2017.

[5] Demetriou, S., Zhang, N., Lee, Y., Wang, X., Gunter, C. A., Zhou, X., and Grace, M., “HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps,” In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 122-133, ACM, July 2017.

[6] Karmakar, K. K., Varadharajan, V., Nepal, S., and Tupakula, U., "SDN Enabled Secure IoT Architecture," In IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 581-585, Arlington, VA, USA, 2019.

[7] Kuerban, M., Tian, Y., Yang, Q., Jia, Y., Huebert, B., and Poss, D., "FlowSec: DOS Attack Mitigation Strategy on SDN Controller," In IEEE International Conference on Networking, Architecture and Storage (NAS), pp. 1-2, Long Beach, CA, 2016.

[8] Wang, S., Chandrasekharan, S., Gomez, K., Kandeepan, S., Al-Hourani, A., Asghar, M. R., Russello, G., and Zanna, P., "SECOD: SDN secure control and data plane algorithm for detecting and defending against DoS attacks," In IEEE/IFIP Network Operations and Management Symposium (NOMS), pp. 1-5, Taipei, 2018.

[9] Yan, Q., Yu, F.R., “Distributed denial of service attacks in software defined networking with cloud computing,” IEEE Commun. Mag., vol. 53, no. 4, pp. 52–59, 2015.

[10] Bawany, N. Z., Shamsi, J. A., and Salah, K., “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions,“ Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425-441, 2017.

[11] Gkountis, C, Taha, M., Lloret, J., and Kambourakis, G., "Lightweight algorithm for protecting SDN controller against DDoS attacks," In 10th IFIP Wireless and Mobile Networking Conference (WMNC), pp. 1-6, Valencia, 2017.

[12] Alsumayt, A., Haggerty, J., and Lotfi, A., "Evaluation of Detection Method to Mitigate DoS Attacks in MANETs," In 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5, Riyadh, 2018.

Authorized licensed use limited to: ULAKBIM UASL - GAZI UNIV. Downloaded on October 02,2023 at 13:40:36 UTC from IEEE Xplore. Restrictions apply.