Journal of Engineering Science and Technology
Vol. 17, No. 2 (2022) 1436 - 1446

DISTRIBUTED DENIAL OF SERVICE ATTACKS DETECTION USING STATISTICAL PROCESS CONTROL IN CENTRALIZED WIRELESS NETWORKS

HIND SOUNNI*, EL KAMOUN NAJIB, LAKRAMI FATIMA

[1]STIC laboratory, physics department, Chouaib Doukkali University,
Jabrane Khalil Jabrane Avenue, B.P: 299, El jadida, Morroco
*Corresponding Author: sounni.h@ucd.ac.ma

Abstract

The Wi-Fi network is exposed to several attacks such as Distributed Denial of Service. These attacks, in progressive expansion, can cause damages to the network by interrupting its services. In a Wi-Fi network, the attackers' primary purpose is to consume and overload the access point resources by establishing an excessive number of connections or requests until the network's saturation. This paper proposes a prevention system allowing the detection of Distributed Denial of Service attacks in a Wi-Fi network-based on the Software-Defined Network. The proposed approach is based on the fraction non-conforming control charts used in Statistical Process Control. A graphical representation of the Packet Drop Ratio is used to monitor the network in real-time. The proposed method does not require any modification of the 802.11 standard or the OpenFlow protocol. A performance evaluation of the Wi-Fi network is also done with the presence of a Distributed Denial of service attack to determine its impact on the network.

Keywords: DDoS, Software-defined network, Statistical process control, Wi-Fi.

1. Introduction

Denial of Service (DoS) or Distributed Denial of Service (DDoS) [1] attack is a continuous critical threat to the wireless network (Wi-Fi). It is designed to damage a device or network and make it unavailable to users; it consists of numerous traffic sources sending many false requests to a target. Exhausted by these requests, the target system can no longer provide an efficient service. Thus, the use of efficient tools is crucial to detect and specify these attacks. Some detectors operate at the host level, representing an ideal approach for detecting attacks with a limited impact on a single machine. However, some attacks, including DDoS attacks, can thoroughly saturate the targeted system. In some cases, saturation can occur at the network entry point; the reason why a detection at the network level is required, allowing to gather detection tools in a single point and share the resources. These tools must operate in real-time and be capable of processing high traffic, constant evolution, and not consuming large amounts of computing resources.

To meet the network equipment's capacity requirements in a Wi-Fi network [2], offer a centralized architecture and network automation, the Software-Defined Network (SDN) [3] is used. SDN is an emerging concept in network management; it enables networks to be built, operated, and secured. It is based on the centralized management of network flows offered by decoupling the controller plan from the data plan. The control plan is responsible for associating the routing decision to the packets; The data plan represents the physical or virtual infrastructure and deals with packets' routing, making networks flexible and programmable.

To ensure the SDN-based Wi-Fi network security against DDoS attacks. A new detection method based on statistical process control (SPC) is proposed, which manifested a high efficiency in the industrial field in quality management and supervision [4]. The experiment consists of executing a DDoS attack and implementing a module to detect these attacks on the SDN controller; This module allows detecting the DDoS attack in real-time using SPC-based quality control charts. The control chart uses predefined thresholds to supervise the quality criteria to be monitored. Thanks to the control chart, alerts are triggered when the thresholds drawn previously are exceeded. Besides, the adopted model against DDoS attacks does not require any change in the IEEE 802.11 [2] or Openflow [3] standards and allows real-time detection.

The rest of the paper is structured as follows: Section II presents related works. Section III describes the Dos and DDoS attacks. Section IV provides an overview of the Statistical Process Control. Section V introduces the proposed detection system. The experimental results and analysis are presented in Section VI, while section VII concludes the paper and offers suggestions for future researches.

2. Related works

Attacks detection remains a significant concern and challenging issue that has attracted both industrial organizations and the scientific community. Over the last few years, a variety of methods have been presented by researchers to detect DDoS attacks in SDN-based WLAN networks [5-9]. This section reviews the relevant solution proposed by the literature to prevent this type of attack in WLAN. A new detection algorithm is proposed by Elhigazi et al. [10] to detect and prevent the authentication request flood attacks; it uses MAC filter buffer to maintain and filter the MAC and buffer monitoring. Liu et al. [11]

developed and implemented an intelligent Platform named iWEP, which offers an advanced warning service for customers. Machine learning is used to provide the ability to defend against Dos' attacks. Agarwal et al. [12] proposed a novel intrusion detection mechanism based on machine learning to detect the flooding DoS attacks in Wi-Fi networks. Arshad and Hussain [13] presented a novel packet monitoring-based probabilistic DDOS attack defection and prevention model. Using trust mechanisms, Singh and Dhir [14] proposed a Distributed Agent-Based technique for detecting DDoS Attacks in WLAN; this mechanism is completely distributed and offers a warning when pre-attack events are identified. Most of these solutions require a modification of the IEEE standard, affecting the communication process. In this paper, the proposed solution is based on the Statistical Process Control and does not require changes of the IEEE 802.11 standard or OpenFlow protocol. Also, it allows network monitoring in real-time to identify variations due to attacks. Table 1 presents a comparative analysis of the studied detection and prevention solutions using a set of critical evaluation metrics. The table also shows the specifics of each adaptation solution when the DDoS attack is detected.

Table 1. Solutions against DoS & DDoS attacks.

Solutions against DoS & DDoS attacks	Centralized solutions	Detection	Prevention	Standard IEEE 802.11 modification	Real time	Statistical method
Authentication Flooding DOS Attack Detection and Prevention in 802.11 [10]	No	Yes	Yes	No	Yes	No
iWEP: An intelligent WLAN Early Warning Platform Using Edge Computing [11]	Yes	Yes	No	No	Yes	No
Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization [12]	No	Yes	No	No	No	No
A novel probabilistic based DDoS attack detection and prevention framework for dynamic LAN/WLAN networks [13]	No	Yes	Yes	No	Yes	No
Distributed agent-based technique for detecting distributed denial-of-service (DDoS) attacks in WLAN [14]	No	Yes	No	Yes	No	No

3. The Effect of the Dos/DDoS attack on the Wi-Fi network

Denial of service (DoS) is an attack designed to affect service availability; This can be accomplished in two ways: overflowing the destination with traffic or transmitting data that causes a failure. Common flooding attacks include; (1) Buffer overflow attacks, which send massive traffic to the target; (2) ICMP flood uses spoofed packets to ping all targeted network machines; (3) SYN flood is realized by sending a connection request to the target without intending to finish the negotiation; these requests allow the saturation of all ports; consequently, no port is available for legitimate users [15]. A distributed denial of service (DDoS) attack is an attack that occurs when two or more systems from several locations coordinate

a synchronized DoS attack to a common target at the same time. Because of these unique characteristics, DDoS is considered a high threat and of more significant concern to targeted networks [16].

In the Wi-Fi context, the DoS/DDoS attack targets the APs and make them unable to serve their users. The attacker intends to consume and overload the AP resources (Association table stored in memory) by establishing an excessive number of connections or sending authentication/association requests. As a result, the access point is associated with more and more fake stations until it causes a blockage due to buffer overflow and then experience failures.

To evaluate and analyse an SDN-based Wi-Fi network's performance during a DDoS attack, Mininet-Wifi [17] is used. The simulated network consists of 15 stations; the attackers are included. A comparison of the behavior of a normal network and a network under the DDoS attack is done. Figures 1-3 present the APs average value of the selected metrics, which are: the delay, the packet drop ratio (PDR) and the throughput.

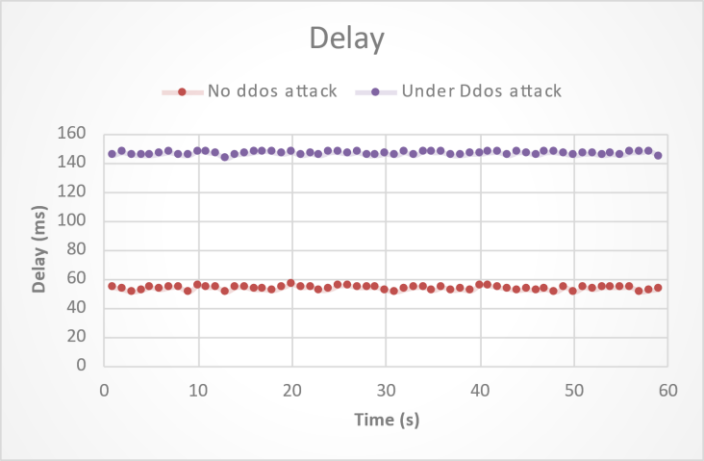

Fig. 1. Delay measurements with and without Dos attack.

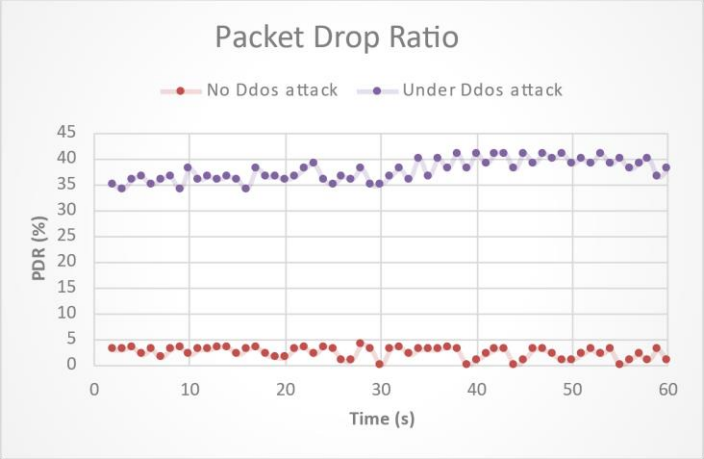

Fig. 2. Packet drop ratio measurements with and without Dos attack.

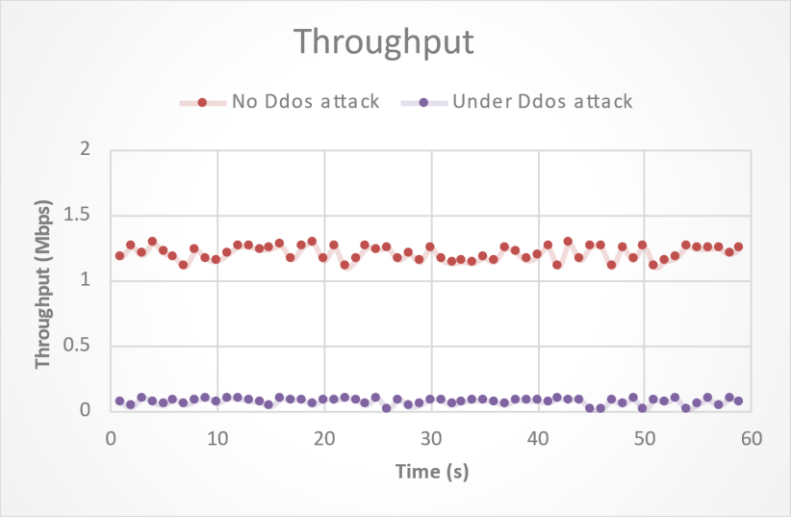

Fig. 3. Throughput measurements with and without Dos attack.

4. SPC (Statistical Process Control)

Statistical Process Control (SPC) is an objective decision-making mechanism allowing to determine whether a process is working correctly or not. The monitoring of the various processes is done via SPC-based quality control charts. The control charts are used to determine process capability and identify special causes of factors that inhibit maximum process performance. These control charts' basic idea is to present the quality characteristics numerically using a graph. A centerline (CL) represents the average value of the process control; this value is compared to the UCL (Upper Control Limit) and the LCL) and Lower Control Limit. If the average values are within the expected, specific, and normal variation levels, the process can be considered under control; otherwise, the process is considered out of control. Several types of control charts in SPC are presented in the literature; the two main types are attribute control charts and variable control charts [18].

In this paper, the non-conforming fraction chart to detect the DDoS attack is used. It is described as the number of non-conforming elements in a population compared to the overall number of elements. It is applied in cases of different sample sizes. The parameters used in this chart are presented in Table 2.

Table 2. Chart parameters

Parameters	Description
Di	Number of defectives units
$\widehat{P}$	Non-conforming fraction of the ith sample
$\overline{P}$	Average fraction non-conforming
n	Sample of size
m	Number of samples
UCL	Upper Control Limit
CL	Center Line
LCL	Lower Control Limit

The non-conforming fraction of the ith sample is represented in Eq.1, where D_i represents the ratio of defective items within a random sample size n. D_i is unknown, therefore, $\hat{P}$ should be estimated from the data collected by the selection of m preliminary sample. As specified in the charter and to ensure its effectiveness, the selected sample m must be a minimum of 20. $\hat{P}$ is given by Eq. (1).

$$\hat{P} = D_i/n \quad , i = 0, 1, 2, 3..., m. \tag{1}$$

The average fraction non-conforming is calculated by Eq. (2):

$$\bar{P} = \sum_{i=1}^{m} \hat{P}/m = \sum_{i=1}^{m} D_i/mn \tag{2}$$

The chart lines are presented by Eqs. (3), (4), and (5) [18]:

$$UCL = \bar{P} + 3\sqrt{\bar{P} + (1 - \bar{P})/n} \tag{3}$$

$$CL = \bar{P} \tag{4}$$

$$LCL = \bar{P} - 3\sqrt{\bar{P} + (1 - \bar{P})/n} \tag{5}$$

5. Proposed Detection System

The main idea is to observe the Wi-Fi network performances to detect the Dos/DDos attack. Several metrics can be used to monitor the network such as Delay, Throughput, Jitter. In this paper, the PDR (Packet Drop Ratio) is chosen since it is one of the key metrics that reflect the network's quality of service, and the most sensitive one especially in case of DDoS attack. Based on the evaluations performed, it can be observed that the PDR at the access point increases when the network is under attack. The PDR is defined as the ratio of lost packets to total sent packets and is expressed in %. As mentioned in the previous section, the DDoS attack allows the sending of a massive number of false connection requests to the access point, exhausted by these requests; a blockage is caused due to the overflow of its buffers. The access point can then no longer provide an efficient service, so the PDR increases during the attack. The PDR is considered as the fraction non-conforming. Accordingly, the idea is to monitor this packet drop by defining a pair of limits in the packet drop graph. The fractional non-conforming p-chart is used to detect the DDoS attacks. Figure 4 describes the SPC-based approach for DDoS Detection in SDN-based Wi-Fi networks.

The proposed algorithm starts by inspecting and observing the Packet Drop Ratio (PDR). Then, it simulates a typical environment, i.e., without any DDoS attack; this helps collect measurements. These measurements are used to calculate the chart parameters CL, UCL, and LCL. Once these parameters are calculated, they are reported on the same graph and the chosen metric measurements (PDR). When observing the graph's PDR flow, if some points exceed the control limits, they must be removed, and the chart parameters should be recalculated. If not, the process continues; The PDR flow is observed; if all the curve points are inside the limits, the network is considered as controlled, and no DDoS attack is detected. If a large deviation is detected and the points are beyond the limits, the network is under DDoS attack.

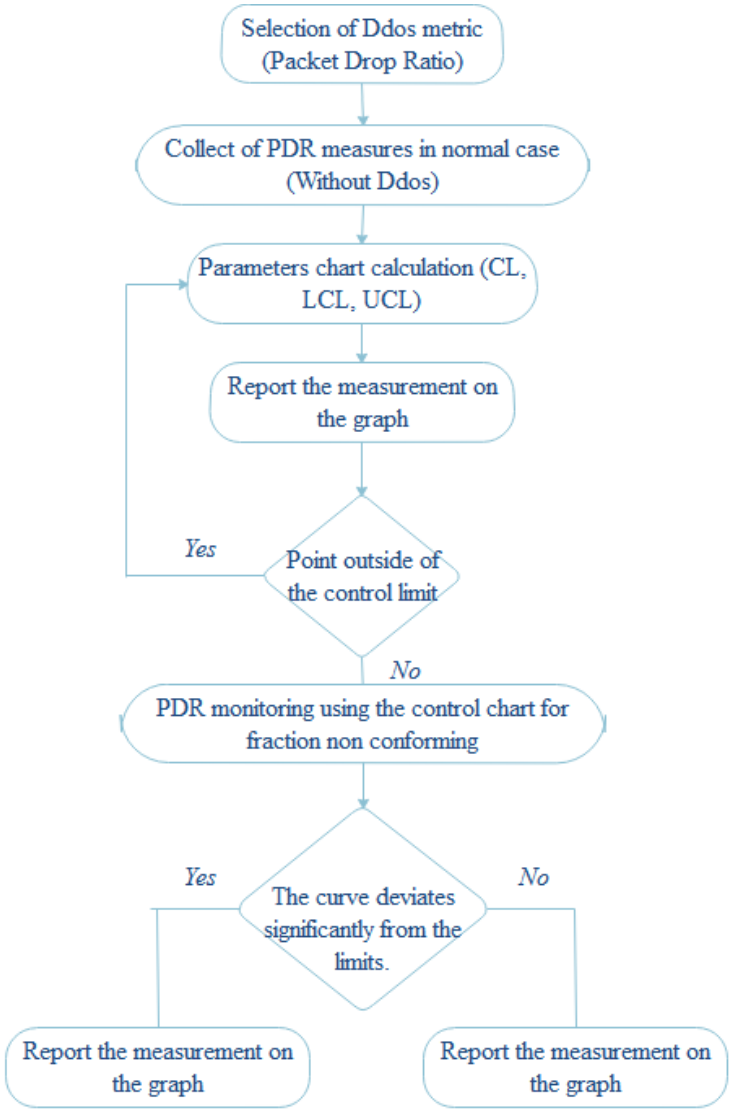

Fig. 4. SPC-based approach for DDoS Detection in SDN-based Wi-Fi networks.

6. Experimental Results and Analysis

To simulate the SDN-based Wi-Fi network and evaluate the proposed method, the mininet Wi-Fi version 2.2.2 running on Ubuntu 16.04 [19] is used. The whole topology is under the RYU controller [20] running on the Ubuntu server. To flood the APs buffer, the Aireplay-ng tool [21] is used on physical stations (Intel core i5, 16G RAM). To monitor and generate traffic in the network, Iperf is used. Figure 5 presents the topology used in the two scenarios (without and with DDoS attack); it consists of three access points, an SDN controller, and 15 stations. The access points' physical configuration is the same; the 802.11ac standard is used with a bandwidth of 500 Mbit/s.

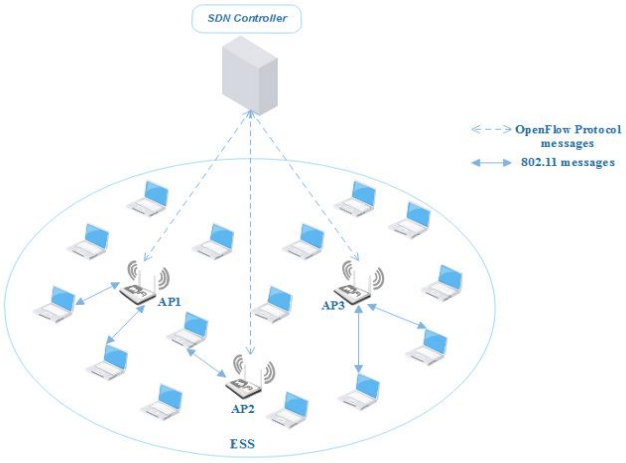

Fig. 5. Network topology.

The detection module is implemented in the SDN controller, giving it the ability to verify the received data. The steps order detailed in Fig. 4 must be respected to monitor the network. The analysis and supervision of the selected metric flow (PDR) is done using the non-conforming fraction control chart; the control limits LC, UCL, LCL are calculated and are respectively equal to 5.85, 7.877 and 3.825. In the first scenario (Fig. 6), no attack DDoS is triggered; the packet drop rate curve oscillates within limits; this means that the communication within the network is as usual. In the second scenario, the DDoS attack is performed; a significant deviation of the PDR curve is observed, which has exceeded the UCL limit. In this case, the network is considered as attacked (Fig. 7). The calculation of the centerline parameter consists of average PDR calculation, it depends mainly on the number of mobile stations in the Wi-Fi network. This method is considered as a powerful tool to analyse the data collected to determine the anomalies that may arise during the communication process.

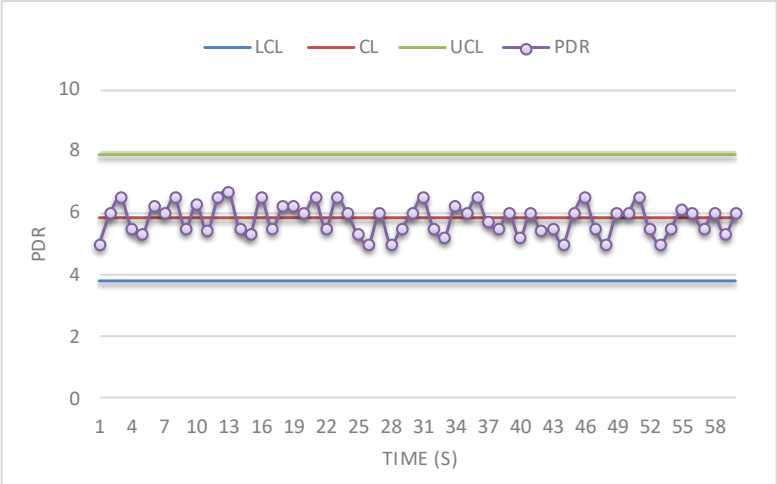

Fig. 6. Monitoring the PDR by the control chart for fraction non-conforming in the normal case (without DDoS attack).

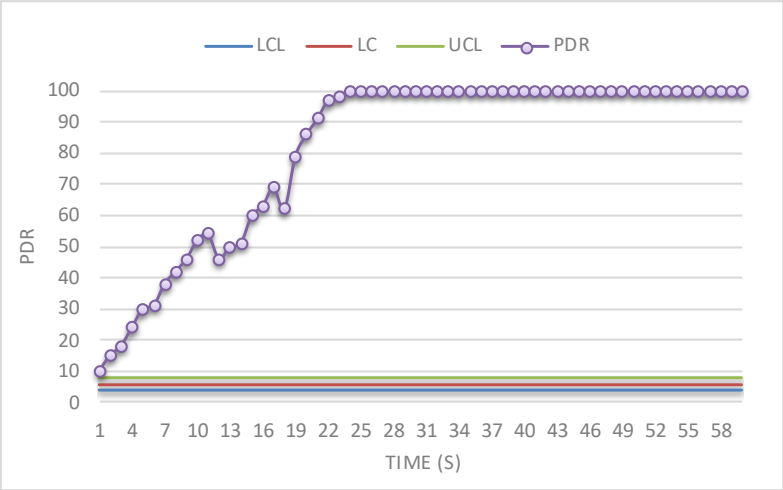

Fig. 7. Monitoring the PDR by the control chart for fraction non-conforming when a DDoS attack occurs.

7. Conclusion

Volumetric attacks like DDoS can reduce device throughput and cause packet drop in the whole network. To detect such an attack, the variation of these parameters must be monitored. This paper presents a DDoS detection scheme based on SPC using the fraction non-conforming control chart; This control chart is used to monitor the PDR variation; it collects data in a normal case, calculates graph parameters, and plots them in the same graph. The proposed method allows the detection of DDos attacks by monitoring the PDR metric graphs in real-time on one side, on the other side there is no change in the IEEE 802.11 and OpenFlow standard. In this article, no reaction mechanism against DDoS attacks has been proposed. In the future works, we will focus on this point and try to integrate reaction mechanism to the detection method. We will experiment with this method on other more complex scenarios using other attack types.

Nomenclatures

D_i	Number of defectives units
m	Number of samples
n	Sample of size
$\bar{P}$	Average fraction non-conforming
$\hat{P}$	Non-conforming fraction of the ith sample

Abbreviations

CL	Center Line
DoS	Denial of Service
DDoS	Distributed Denial of Service
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
LCL	Lower Control Limit

PDR	Packet Drop Ratio
SDN	Software-Defined Network
SPC	Statistical Process Control
UCL	Upper Control Limit
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

References

1. Silva, A. (2020). Distributed Denial of service attack in networks. Retrieved December 3, 2020. From http://eprints.rclis.org/40181/.
2. Costa, R.; Lau, J.; Portugal, P.; Vasques, F.; and Moraes, R. (2019). Handling real-time communication in infrastructured IEEE 802.11 wireless networks: The RT-WiFi approach. *Journal of Communications and Networks*, 21(3), 319-334.
3. Alsaeedi, M.; Mohamad, M.M.; and Al-Roubaiey, A.A. (2019). Toward adaptive and scalable OpenFlow-SDN flow control: A survey. IEEE Access, 7, 107346-107379.
4. Montgomery, D.C. (2008). *Introduction to statistical quality control*. John Wiley & Sons.
5. Li, S.; Cui, Y.; Ni, Y.; and Yan, L. (2019). An effective SDN controller scheduling method to defence DDoS attacks. *Chinese Journal of Electronics*, 28(2), 404-407.
6. Chen, J.; Tang, X.; Cheng, J.; Wang, F.; and Xu, R. (2020). DDoS attack detection method based on network abnormal behaviour in big data environment. *International Journal of Computational Science and Engineering*, 23(1), 22-30.
7. Saied, A.; Overill, R.E.; and Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*, 172, 385-393.
8. Yan, Q.; Yu, F. R.; Gong, Q.; and Li, J. (2016). 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 and Tutorials*, 18(1), 602-622.
9. Bawany, N.Z.; Shamsi, J.A.; and Salah, K. (2017). DDoS attack detection and mitigation using SDN: Methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42(2), 425-441.
10. Elhigazi, S.A.; Razak, M.A.; Hamdan, B.; Mohammed, I.; Abaker, A.; and Elsafi, A. (2020). Authentication flooding DOS attack detection and prevention in 802.11. 2020 *IEEE Student Conference on Research and Development* (*SCOReD*), Batu Pahat, Johor, Malaysia, 325-329.
11. Liu, R.; Wang, W.; Wang, J.; Ou, Z.; Qiu, H.; Wang, B.; and Liu, Q. (2019). iWEP: An intelligent WLAN early warning platform using edge computing. *Proceedings of the* 15*th International Conference on Mobile Ad-Hoc and Sensor Networks* (*MSN*), Shenzhen, China, 384-389.
12. Agarwal, M.; Pasumarthi, D.; Biswas, S.; and Nandi, S. (2016). Machine learning approach for detection of flooding DoS attacks in 802.11 networks

and attacker localization. *International Journal of Machine Learning and Cybernetics*, 7(6), 1035-1051.

13. Arshad, M.; and Hussain, M.A. (2017). A novel probabilistic based DDoS attack detection and prevention framework for dynamic LAN/WLAN networks. *Journal of Advanced Research in Dynamical and Control Systems*, 9(2), 272-286
14. Singh, H.; and Dhir, V. (2018). Distributed agent-based technique for detecting distributed denial-of-service (DDoS) attacks in WLAN. *International Journal of Advanced Research in Computer Science*, 9(1), 375-380.
15. Aung, M.A.C.; and Thant, K.P. (2019). IEEE 802.11 attacks and defenses. *Proceedings of the* 17*th International Conference on Computer Application* (*ICCA*), Yangon, Myanmar, 186-191.
16. Tushir, B.; Dalal, Y.; Dezfouli, B.; and Liu, Y.A. (2020). A quantitative study of DDoS and E-DDoS attacks on wi-fi smart home devices. IEEE Internet of Things Journal, 8(8), 6282 – 6292.
17. Fontes, R.D.R.; and Rothenberg, C.E. (2016). Mininet-wifi: a platform for hybrid physical-virtual software-defined wireless networking research. *Proceedings of the* 2016 *ACM SIGCOMM Conference*, 607-608.
18. Woodall, W.H. (1997). Control charts based on attribute data: bibliography and review. *Journal of quality Technology*, 29(2), 172-183.
19. Raggi, E.; Thomas, K.; and Van Vugt, S. (2011). *Beginning ubuntu linux*. Springer.
20. Asadollahi, S.; Goswami, B.; and Sameer, M. (2018). Ryu controller's scalability experiment on software defined networks. *Proceedings of* 2018 *IEEE International Conference on Current Trends in Advanced Computing* (*ICCTAC*), Bangalore, India, 1-5.
21. Visoottiviseth, V.; Akarasiriwong, P.; Chaiyasart, S.; and Chotivatunyu, S. (2017). PENTOS: Penetration testing tool for internet of thing devices. *Proceedings of TENCON* 2017 - 2017 *IEEE Region* 10 *Conference*; Penang, Malaysia, 2279-2284.