SPC-BASED APPROACH FOR DDOS ATTACK DETECTION USING X-MR CONTROL CHART

Hind Sounni, Najib Elkamoun, Fatima Lakrami, Faysal Bensalah*

Chouaib Doukkali University, Eljadida
Morocco

* Corresponding Author, e-mail: hind.sounni@gmail.com

Abstract: Distributed denial of service (DDoS) is an evolving critical threat for wireless (Wi-Fi) networks. The malicious nodes' primary purpose is to overload the access point resources by establishing an excessive number of connections or requests until saturation. In this paper, a new detection method based on the Statistical Process Control (SPC) is proposed using an X-MR chart. This method allows detecting DDoS attacks in real-time and does not require any modification of the 802.11 standard or the OpenFlow protocol. It also offers network real-time monitoring, which helps to identify variations due to attacks. A graphical representation of the delay and throughput is used to supervise the network.

Key words: Wi-Fi, Software-Defined Network, Distributed denial of Service, Statistical Process Control, X-MR chart.

1. INTRODUCTION

A Denial of Service (DoS) attack is designed to damage a device or network and make it unavailable to legitimate 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. In a wireless network (Wi-Fi), a denial of service attack can be accomplished through several ways: beacon flood [1], RTS/CTS attacks [2], Authentication request attacks [3] …

This paper introduces a new method to detect the DDoS attack in a Software-Defined Network-based Wi-Fi network. The SDN is an evolving technology in networking; it enables networks to be built, operated, and secured. It relies on centralized management of network flows offered by separating the control plane and the data plane [4]. 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. The proposed method is based on Statistical Process Control (SPC) [5].

The SPC is an objective decision-making mechanism for determining whether or not a process is working correctly. It consists of monitoring each process's variation; this allows identifying if this variation is natural or if it requires a correction. The SPC differentiates between two types of variations: "common cause" variations and "special cause" variations. The SPC uses control charts to monitor, verify and review a process to ensure that the controlled characters remain stable or within specifications, with some unavoidable variability. The control chart's basic idea is to represent a process's evolution over time using a graph. A centerline (CL) indicates the average value of the process control; this value is compared to the upper control limit (UCL) and the lower control limit (LCL). To calculate these lines (CL, UCL, and LCL), we use the data collected in the normal case (without attack). Comparing the current data with these lines allows concluding the conformity (control) or unpredictability (uncontrollable, affected by particular variation causes) of process variation. These charts present a flexible data collection and analysis tool used by various industries; they are considered among the seven essential quality tools. Several types of control charts in SPC are presented in the literature; the two main types are attribute control charts and variable control charts.

In this paper, we use a variable control chart called the X-MR control chart. In this case, a central measurement describes characteristic variation; usually, the X charts for the average and the MR chart for the mobile range. The control X-MR chart includes two graphs: the first one monitors the individual values to determine system failures. The second illustrates the moving range for quality control. This control chart is commonly used in the industrial field to control a given process's quality, especially when the system is changing rapidly. Additional control charts may be a good option for slow system variations (graph C for the weighted average).

The most popular security solutions against DDoS attacks do not require modifying the IEEE standard or the OpenFlow protocol in SDN architecture. Indeed, these changes can affect the communication process. This paper proposes a model based on a statistical method to analyze the Wi-Fi network and provide a real-time decision-making system. Statistical methods such as SPC (Statistical Process Control) are widely used and have proved their effectiveness in controlling industrial processes. Besides, it does not require any modification to the IEEE 802.11 standard or the OpenFlow protocol and offer real-time monitoring of the network to identify variations due to attacks.

The rest of the paper is structured as follows: Section II describes the Dos and DDoS attacks. Section III presents related works. Section IV provides an overview of the X-MR control chart. 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. DDOS ATTACK

A denial of service (DoS) attack is an attempt to disrupt the accessibility of network resources. Its objective is to damage or destroy system resources used by legitimate users. It generates high-speed malicious traffic, directs it to the targeted network, and consumes the victim's computing resources exhaustively. The attack is performed in different ways, such as flooding a network with unnecessary traffic, thus preventing legitimate client demands, manipulating connection information, for example, reinitializing a TCP session, and blocking access by interrupting the connection between communication systems. DoS attacks affect the entire world's organizations. The OSI model's seven layers are targeted, from Layer 1 (physical) to Layer 7 (application). The traffic generated during a DoS attack seems normal to the targeted systems; therefore, the challenge is to be able to detect whether it is a DoS attack or not.

Two types of denial of service attacks are presented: an undistributed denial of service attack and a distributed denial-of-service attack [6]. In an undistributed DoS attack, an attacker relies on a single host to flood other hosts. If the attacked machine is a high-performance one, this type of attack does not affect the targeted system. In a distributed DoS attack, the attack is launched from several hosts at the same time and focuses on one or more hosts, causing the victim's resources to be depleted [7]. DoS and DDoS attacks are presented in figure 1.

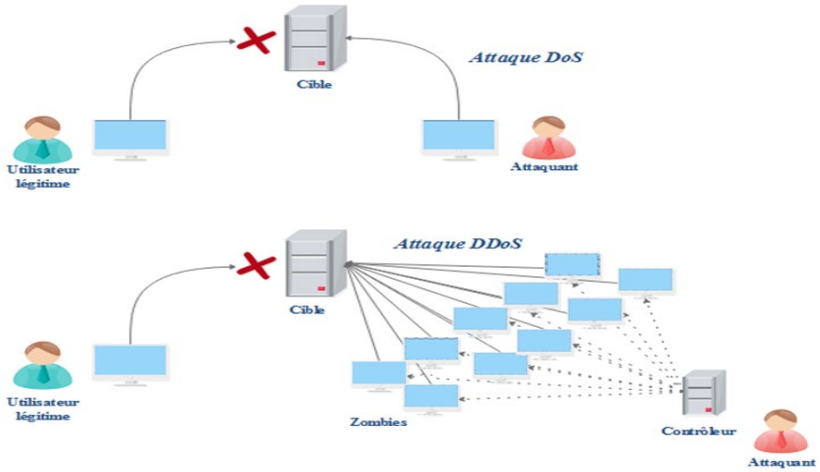

Fig. 1. Difference between DoS & DDoS attacks

3. RELATED WORKS

DDoS attack detection remains a significant concern for the scientific community. In recent years, researchers have presented various methods to detect and mitigate DDoS effects in wireless networks in general and in Wi-Fi networks in particular. A new detection algorithm is proposed by [3] to detect and prevent authentication request attacks; the MAC filter buffer is used to maintain MAC and

buffer monitoring. Authors [8] developed and implemented an intelligent platform called iWEP, which provides an early warning service to customers. Machine learning is used to defend against Dos saturation attacks. A new intrusion detection mechanism based on automatic learning to detect DoS saturation attacks in Wi-Fi networks is proposed in [9], and a new probabilistic model for detecting and preventing DDOS attacks based on packet monitoring is presented in [10].

Using trust mechanisms, the article [11] proposes a distributed agent-based technique to detect DDoS attacks in WLAN networks; this mechanism is fully distributed and offers an alert when pre-attack events are identified. The agents used in the architecture are autonomous, mobile, and cooperative entities. The agents used in this system are independent, mobile and collaborative elements. According to detection results, every agent performs a detecting algorithm and shares its report with the rest of the agents. A final warning is forwarded to the base station; the NS2 simulator simulates and tests the proposed approach. A real-time detection method for MAC layer DDoS attacks based on cumulative sum algorithms (CUSUM) is used in [12]. An Intrusion Detection System (IDS) based on the Discrete Event System (DES) to detect DoS de-authentication attacks is offered in [13].

The DES model includes both states and transitions. When one or more discrete events occur, a shift is done between two states. These events are modeled based on definitive changes in the network. Article [14] demonstrates that the use of IoT-specific network behaviors to notify feature selection can lead to high-precision DDoS detection in IoT network traffic.

4. X-MR CONTROL CHART

The X-MR control chart (moving range) is used when the measured characteristic is of the variable type (quantitative) and can be measured periodically; this tool detects anomalies quickly in a process. It allows process control by monitoring individual values' evolution and the variability between a given point and the next or previous one. It uses two distinct but complementary control charts. The first indicates the evolution of individual measurements (X), and the second shows the variability of these measurements (MR).

The mobile range is defined as follows [15]:

$$MR_i = |x_i - x_{i-1}| \quad (1)$$

where MRi is the moving range of the ith sample, and xi is the range number i. Control limit parameters for individual values are calculated by [15]:

$$UCL = \bar{x} + 3(\overline{MR})/d_2 \quad (2)$$

$$CL = \bar{x} \quad (3)$$

$$LCL = \bar{x} - 3(\overline{MR})/d_2 \quad (4)$$

where $\overline{MR}$: The average of the moving ranges from of two consecutive, x, and xi; *UCL*: The upper control limit; *LCL:* The lower control limit.

The variability of the process is monitored using the following equations [15]:

$$LCL = D_3 * \overline{MR} \quad (5)$$

$$UCL = D_4 * \overline{MR} \quad (6)$$

$$CL = \overline{MR} \quad (7)$$

d2, **D3** and **D4** are constants called control limit factors. These constants are well known and listed following sample size [16]. The mathematical sources of these equations are shown in [17].

5. PROPOSED METHOD

As mentioned previously, a DDoS attack causes significant deterioration of the Wi-Fi network performance. This paper proposes monitoring two metrics (delay and throughput) using our detection system based on the X-MR control chart. Delay and throughput are among the key metrics that reflect the network's quality of service; other metrics can be chosen, such as packet loss, jitter. The DDoS attack detection module is implemented on the SDN controller, which has a global network view and can automatically visualize the overall Wi-Fi network's status. The DDoS attack detection procedure is summarized in 3 steps:

Step 1: Determine the process metrics to be observed.

Step 2: Collect data in the normal case (without the DDoS) and calculate graph parameters (UCL, CL, LCL). For a correct and adequate calculation, the X-MR chart requests at least 20 values. In this paper, the number of values is set up to 150 values.

Step 3: Graphical representation of the calculated parameters and supervision of the collected metric values in real-time.

Visualizing the graphs, if the curves oscillate within limits defined by the chart, we consider that the network's communication is normal, i. e. no DDoS attack is carried out. However, if the curves oscillate out of the limits, we consider that the network's communication is abnormal, and the network undergoes a DDoS attack. Figure 2 illustrates the proposed method flowchart.

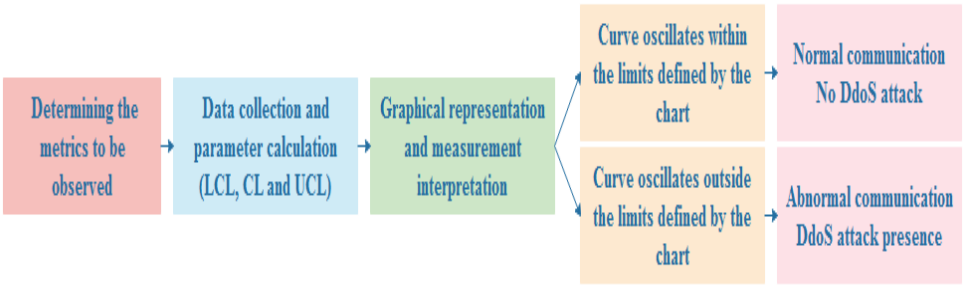

Fig. 2. DDoS Attack Detection Diagram using the X-MR Control Chart

5.1. X-MR control chart evaluation

5.1.1. Environment and simulation parameters

This section evaluates the proposed method's effectiveness in detecting the DDoS attack in a Wi-Fi network. The DDoS attack detection module is already implemented in the SDN controller. We have simulated a Wi-Fi network based on the SDN using mininet Wi-Fi [18]. Our topology consists of an RYU controller [19] installed on an Ubuntu server. The SDN controller controls OpenFlow access points; several fixed and mobile stations move from one AP to another. The Iperf tool is used to generate UDP traffic [20]. Table 1 presents the main simulation parameters.

Table 1. Simulation parameters

Parameters	***Value***
Stations number	*20*
Emulator	*Mininet Wi-Fi*
Controller	*RYU*
Trafic type	*UDP*
Number of attackers	*5*
Simulation time (s)	*60*
AP parameters	*802.11ac (500 Mbit/s)*
Other tools	*Airplay-ng, Iperf*
Mobility speed	*1 m/s*

5.1.2. Results and discussion

The X-MR control chart parameters are calculated using the equations presented in section 2.1. The X-MR control chart requires a minimum of 20 samples to ensure its efficiency and obtain flawless results. Measurements are collected and calculated using equations 2-7 without launching the DDoS attack. Table 2 summarizes the results:

Table 2. Simulation parameters

Parameters	***Value***	
Observation X	***Throughput***	***Delay***
Individual Observations Upper Control Limit (UCL)	*1,465*	*0,059*
Individual Observations Average (CL)	*1,24*	*0,0538*
Individual Observations Lower Control Limit (LCL)	*1,026*	*0,0488*
Moving range observation Upper control limit (UCL)	*0,65*	*0,023*
Moving range observations Average (CL)	*0,21*	*0,0067*
Moving range observation Lower control limit (LCL)	*0,0*	*0,0*

For real-time supervision, the values are taken instantaneously. The detection module is implemented in the SDN controller, giving it the ability to verify the received data. We supervised the network using the X-MR chart, for which the parameter values are presented in table 2. Figures 3-6 present the results of individual

measurements and mobile range of the two metrics (Throughput and Delay) in the normal case (without attack). The delay and throughput curves oscillate between the graph's limits; this means that no DDoS attack is launched and the communication is in a normal environment. The substantial variations observed in the mobile range of Delay and Throughput are normal variations due to common causes like the stations' mobility and topology changes. As explained previously, the X-MR control chart uses two distinct but complementary types of control charts. (The X chart) for averages and the R chart for moving ranges). These two charts detect different types of special causes. The first (X chart) indicates individual measurements' evolution, while the second (MR chart) indicates these measurements' variability.

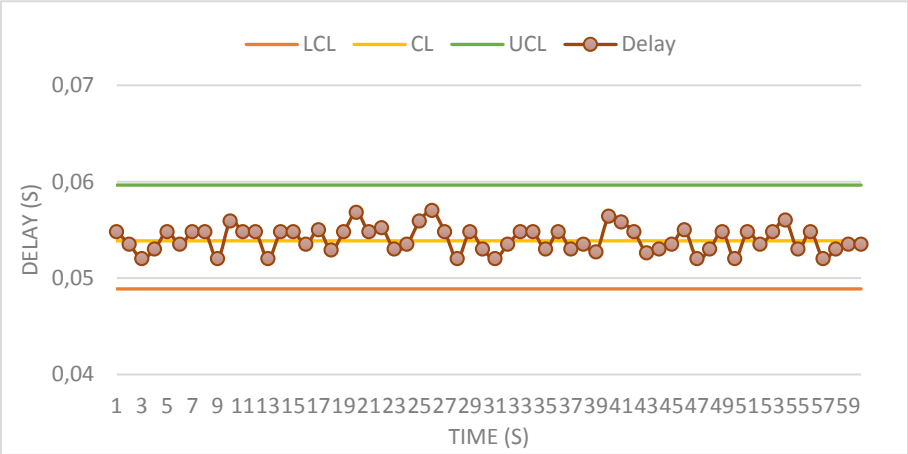

Fig. 3. Monitoring of individual delay measurements in the normal case (without DDoS attack)

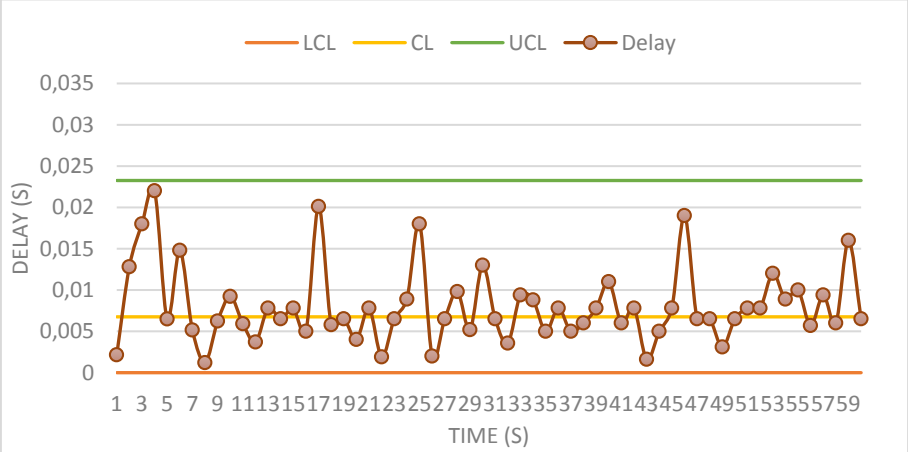

Fig. 4. Monitoring of delay mobile range in the normal case (without DDoS attack)

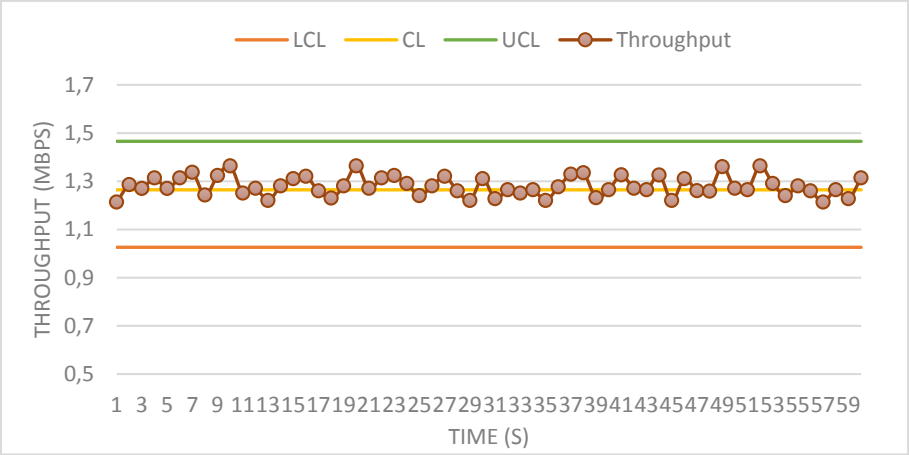

Fig. 5. Monitoring of individual throughput measurements in the normal case (without DDoS attack)

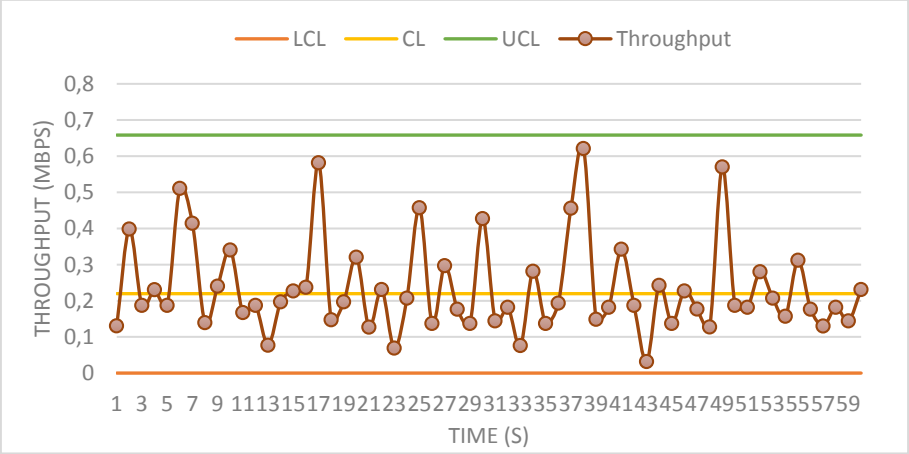

Fig. 6. Monitoring of throughput mobile range in the normal case (without DDoS attack)

Figures 7-10 show metrics graphs (delay and throughput) during a DDoS attack; we can observe that the curves' variations are outside the control limits for the graphs of the individual measurements as for those of the moving range. For the delay, the curves are oscillating over the upper limit (UCL) in the beginning and oscillate below the lower limit (LCL) for the throughput. These variations are caused by specific factors, which cause system disturbances; in our case, the DDoS attack is considered as the specific factor, and an intervention is required in the process.

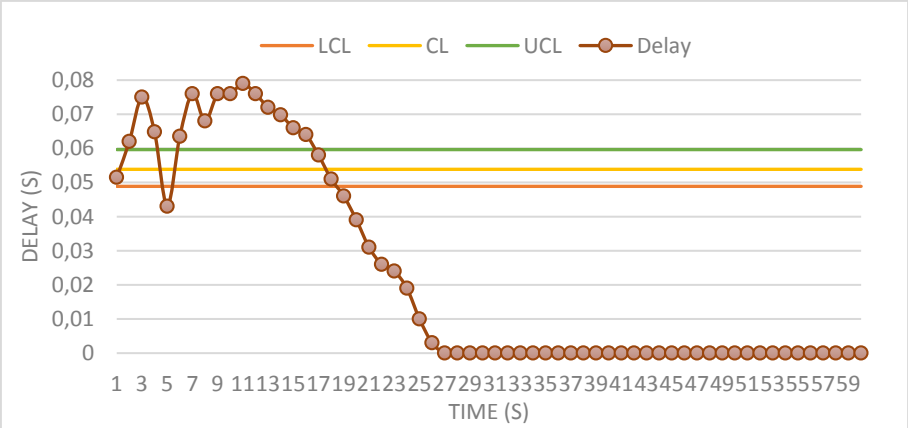

Fig. 7. Monitoring of individual delay measurements during the DDoS attack

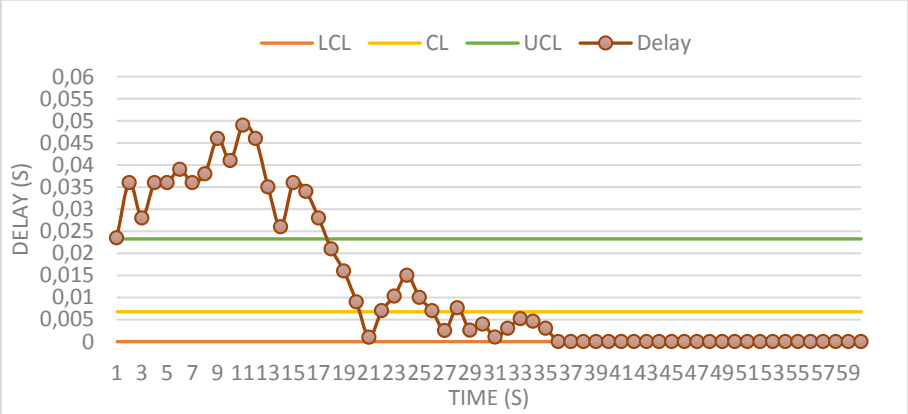

Fig. 8. Monitoring of delay mobile range during the DDoS attack

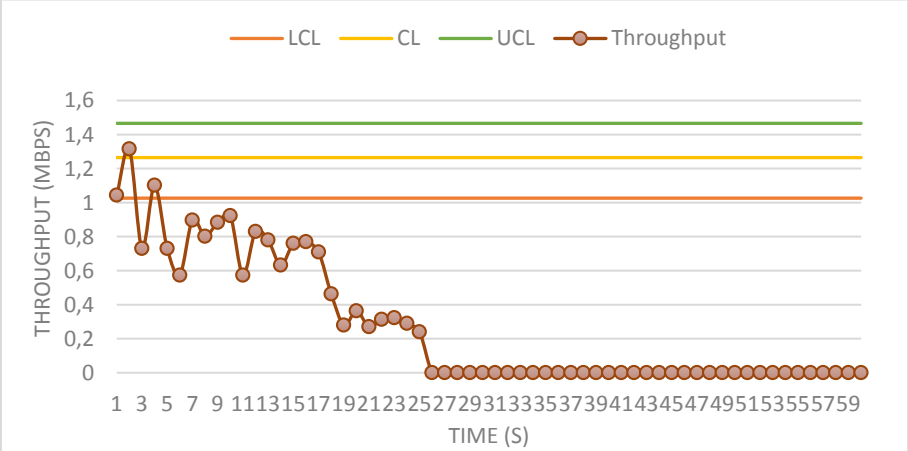

Fig. 9. Monitoring of individual throughput measurements during the DDoS attack

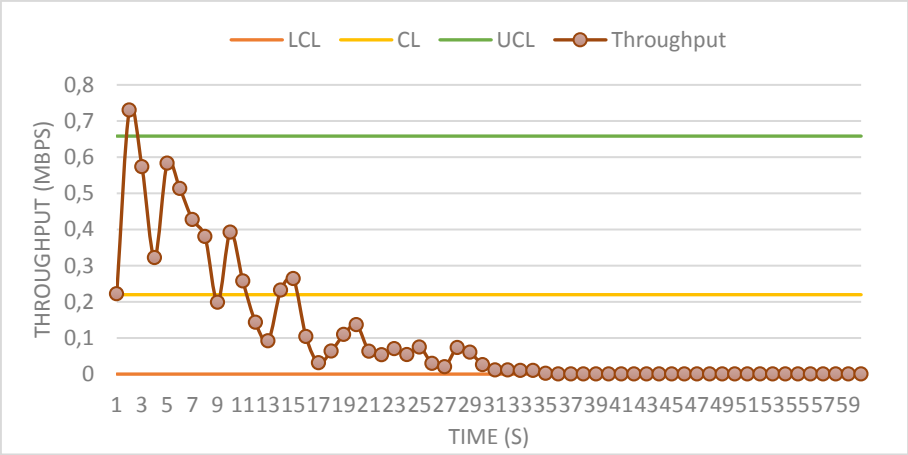

Fig. 10. Monitoring of throughput mobile range during the DDoS attack

6. CONCLUSION

Volumetric attacks such as DDoS can reduce device throughput and cause packet loss over the entire network. Therefore, early detection of this type of attack is required. In this paper, we introduced an SPC-based DDoS detection scheme using the X-MR control chart. The control charts are used to monitor the performance metrics variation; the metric used in this paper are delay and throughput; we can also use other metrics such as packet loss. The control chart is used to monitor these metrics' variation; it collects data in a normal case, calculates graph parameters, and plots them in the graph. The proposed attack identification system is promising and has many advantages, such as real-time attack detection. Besides, no modifications or changes in the IEEE 802.11 standard and OpenFlow are required.

REFERENCES

[1] S. Shaheen, A. Fahiem, A. Mayank at al. Detection of beacon transmission denial attack in ITS using temporal auto-correlation and random inspections, *Proceedings of the 20th International Conference on Distributed Computing and Networking*, January 2019, USA, pp. 317-326, Available at: https://dl.acm.org/doi/abs/10.1145/3288599.3288616.

[2] T. Jamal, M. Alam, M. M. Umair, Detection and prevention against RTS attacks in wireless LANs, in 2017 *International Conference on Communication, Computing and Digital Systems (C-CODE)*, 2017, p. 152-156.

[3] A. Elhigazi, S. A. Razak, M. Hamdan et.al. Authentication Flooding DOS Attack Detection and Prevention in 802.11, *2020 IEEE Student Conference on Research and Development (SCOReD)*, Sept. 2020, p. 325-329, doi: 10.1109/SCOReD50371.2020.9250990.

[4] Open Networking Foundation. *Software-Defined Networking: The New Norm for Networks*, 02 Mai 2013. https://opennetworking.org/sdn-resources/whitepapers/software-defined-networking-the-new-norm-for-networks/

[5] W. A. Shewhart, *Economic Control of Quality of Manufactured Product*. D. Van Nostrand Company, Incorporated, 1931.

[6] A. Aminu Ghali, R. Ahmad, H. S. A. Alhussian. Comparative Analysis of DoS and DDoS Attacks in Internet of Things Environment, *Artificial Intelligence and Bioinspired Computational Methods*, Cham, 2020, p. 183‑194, doi: 10.1007/978-3-030-51971-1_15.

[7] E. Džaferović, A. Sokol, A. Abd Almisreb, S. M. Norzeli. DoS and DDoS vulnerability of IoT: A review, *Sustainable Engineering and Innovation*, Vol. 1, No 1, 2019, pp. 43-48.

[8] R. Liu et al. iWEP: An Intelligent WLAN Early Warning Platform Using Edge Computing. *2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, Shenzhen, China, 2019, pp. 384-389, doi: 10.1109/MSN48538.2019.00079.

[9] M. Agarwal, D. Pasumarthi, S. Biswas, S. Nandi. Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization. *International Journal of Machine Learning and Cybernetics*, Vol. 7, No. 6, 2016, pp.1035-1051, doi: 10.1007/s13042-014-0309-2.

[10] M. Arshad, D. M. A. Hussain. A novel probabilistic based DDOS attacks detection and prevention framework for dynamic LAN/WLAN networks, *Journal of Advanced Research in Dynamical and Control Systems,* Vol. 9, No. 2, 2017, pp. 272-286.

[11] H. Singh, V. Dhir. Distributed agent based technique for detecting distributed denial-of-service (DDOS) attacks in WLAN, *International Journal of Advanced Research in Computer Science*, Vol. 9, No 1, 2018, pp. 375-380, doi: 10.26483/ijarcs.v9i1.5328.

[12] M. Dasari. Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks, *14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, January 2017, USA, pp. 939-944, doi: 10.1109/CCNC.2017.7983259.

[13] A. D. Seth, S. Biswas, A. K. Dhar. De-Authentication Attack Detection using Discrete Event Systems in 802.11 Wi-Fi Networks, *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec 2019, India, pp. 1-6, doi: 10.1109/ANTS47819.2019.9118100.

[14] R. Doshi, N. Apthorpe, N. Feamster. Machine Learning DDoS Detection for Consumer Internet of Things Devices, *2018 IEEE Security and Privacy Workshops (SPW)*, May 2018, USA, pp. 29-35, doi: 10.1109/SPW.2018.00013.

[15] J. Oakland, R. J. Oakland. *Statistical Process Control* (7th ed.), Abingdon, Oxon; New York, NY: Routledge, 2018.

[16] D. C. Montgomery. *Introduction to Statistical Quality Control*. John Wiley & Sons, Inc., 2009

[17] L. H. C. Tippett. On the Extreme Individuals and the Range of Samples Taken from a Normal Population, *Biometrika*, Vol. 17, No. 3/4, 2006, pp. 364-387, doi: 10.2307/2332087.

[18] R. Fontes, C. E. Rothenberg, Mininet-WiFi: Plataforma de Emulação para Redes sem Fio Definidas por Software , in *Anais Estendidos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC),* May 2019, p. 201-208, doi: 10.5753/sbrc_estendido.2019.7788.

[19] S. Asadollahi, B. Goswami, M. Sameer. Ryu controller's scalability experiment on software defined networks, *2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, Feb 2018, Bangalore, pp. 1-5, doi: 10.1109/ICCTAC.2018.8370397.

[20] C. H. Hsu, U. Kremer, IPERF: A framework for automatic construction of performance prediction models. In *Workshop on Profile and Feedback-Directed Compilation (PFDC)*, October, 1998, Paris, France.

Information about the authors:

Hind Sounni obtained the Master's degree in Networks and Telecommunications in 2016. She is a Ph. D Student in computer network at the STIC Laboratory at Chouaib Doukkali University. Her main research focuses on Wireless Local Area Network (WLAN), Networks Security, Software-defined network, and telecommunications.

Najib Elkamoun is a researcher and a professor at Chouaib Doukkali University, El Jadida, Morocco. He is a member of the STIC laboratory and team leader of the Networks and Telecommunications team. His main research focuses on WLAN, NGN, VPN, MPLS, Networks, QoS in mobile networks, SDN, Security.

Fatima Lakrami is a researcher and a professor at Chouaîb Doukkali University, El Jadida, Morocco. She got her Doctorate in Telecommunication and Networking in 2014 from Chouaîb Doukkali University, El Jadida, Morocco. Her main research focuses on wireless networks performance evaluation, Smart grid, SDN, VANETs, Security.

Manuscript received on 01 March 2021