An Effective Network Intrusion Detection Using Hellinger Distance-Based Monitoring Mechanism

Benamar Bouyeddou[a] , Fouzi Harrou[b]
[a]STIC Lab., Department of Telecommunications,
Abou Bekr Belkaid University, Tlemcen, Algeria
e-mail: bouben81@yahoo.fr,

Ying Sun[b] and Benamar Kadri[a]
[b]King Abdullah University of Science and Technology,
CEMSE Division, Thuwal, 23955-6900, Saudi Arabia
e-mail: fouzi.harrou@kaust.edu.sa

***Abstract*— This paper proposes an intrusion detection scheme for Denial Of Service (DOS) and Distributed DOS (DDOS) attacks detection. We used Hellinger distance (HD), which is an effective measure to quantify the similarity between two distributions, to detect the presence of potential malicious attackers. Specifically, we applied HD-based anomaly detection mechanism to detect SYN and ICMPv6-based DOS/DDOS attacks. Here, Shewhart chart is applied to HD to set up a detection threshold. The proposed mechanism is evaluated using DARPA99 and ICMPv6 traffic datasets. Results indicate that our mechanism accomplished reliable detection of DOS/DDOS flooding attacks.**

Keywords—DOS/DDOS, SYN flooding, ICMPv6 attacks, Hellinger distance, DARPA99 dataset, ICMPv6 dataset.

I. Introduction

In today's fully connected world, intrusions and cyber-attacks are becoming a real fact to deal with it. Undoubtedly, Denial of Service and Distributed Denial of service (DOS/DDOS) attacks are still a challenging issue threatening modern information and communication technologies. As shown in Figure 1, hundreds to thousands of those attacks are arising every day and their consequences are more than being covered [1]. They are targeting to crash servers and systems as long as possible. To do this, attackers continue to exploit the well-known vulnerabilities and uncover a plethora of weaknesses existing in most of the new technologies (i.e., smart devices, Internet of things, clouds and virtualization). Various techniques off DOS/DDOS have been designed including individual and distributed inundation of victims with a large amount of traffic and sending invalid data structure (i.e., faked messages). The TCP-based SYN and ICMP-based DOS/DDOS are extensively used due to the significant importance of both protocols in the majority of new networking technologies [1-3].

Thereby, several methods have been designed to detect SYN flooding attacks. Hussain et .al [4] proposed a firewall-based forwarding of TCP connection using source's address and the number of their established connections. Al-hawarwreh [5] constructed a set of attributes to track SYN flooding attacks in clouds. Sun et al. [6] addressed the problem of IP address spoofing using a method called SACK^2. Ramadhan et al. [7] inspired by the Artificial Immune System and the Dendritic Cell Algorithm proposed a detection scheme for TCP-based DOS and DDOS flooding attacks. Fichera et al. [8] implemented the OPERTTA technique to establish TCP connections in software-defined networks. Other researchers focused on developing detection systems to deal with attacks against the protocol ICMP. Indeed, stopping the propagation of specific messages and services (e.g., ping and broadcast) was mainly used in IPv4 based networks. The Internet Engineering Task Force (IETF) released a secured version of the Neighbor Discovery Protocol for IPv6 environment [9]. In [10], the new ICMP traceback message is proposed to allow the traceability of the DDOS sources attacks. In [11] the Neighbor Discovery Protocol Monitoring (NDPMon) adapted the IPv4 ARPwatch protocol to detect NDP-based attacks related to the ICMPV6 protocol in the IPv6 environment. Zulkiflee et al. [12] distinguished the attacks using most pertinent traffic's attributes which are chosen with the SVM algorithm. The Source Address Validation Improvement (SAVI) [13] attached MAC and IPv6 addresses to construct traffic's rule filtering.

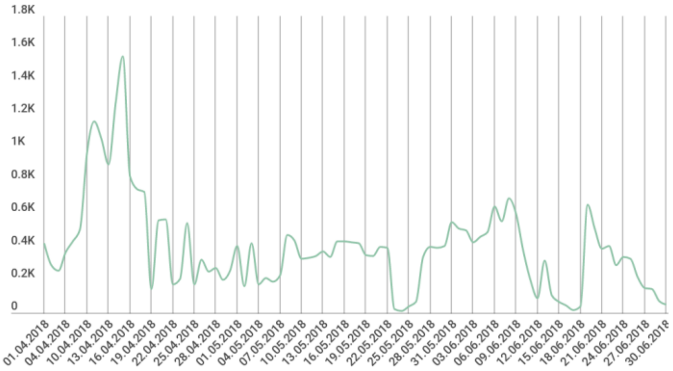


Fig. 1. DOS/DDOS attacks launched from April to June 2018 [1].

To detect SYN flooding and ICMPv6-based attacks, we introduce in this work an efficient scheme based on the Hellinger Distance (HD) [14]. The HD metric is widely used to evaluate the similarity between two probability distributions [15]. Here, we suggest using the HD measures as traffic anomaly detector. The HD distance between the distribution of the test traffic and the distribution of the attack-free traffic is much larger than the distance between the distribution of normal traffic and the reference distribution of the training data. HD values tend to zero under the attack-free traffic and increase significantly with the presence of attacks. Hence, the SYN and ICMPv6- based flooding attacks can be revealed by checking the HD measurements. To this end, we develop the HD-Shewhart chart by exploiting this attractive property of HD and the three-sigma rule to set the detection threshold. To assess the performance of HD-Shewhart, we have used two different traces of IP networks traffic, the first is the DARPA99 dataset and the second is an ICMPv6 traffic dataset. The remainder of this paper is organized as follows. Section II describes the SYN and the ICMPv6-based flooding DOS/DDOS attacks. In section III, we present the HD-Shewhart detection mechanism. Section IV evaluates the detection capacity of the HD-Shewhart approach. Finally, we conclude the paper in Section V.

II. TCP SYN AND ICMPV6-BASED FLOODING ATTACKS

A. TCP SYN flood attacks:

Till now, SYN flooding attacks still arise continuously although the efforts made in developing accurate detection mechanisms. The client can initiate a new TCP connection (Figure 2) with an SYN message sent to the TCP server. When the request is accepted, the server responds with the Synchronization/Acknowledgement (SYN/ACK) message and save the related information in the backlog queue. Finally, the client validates this connection by ACK the received SYN/ACK. Now, the client is connected, and the server deletes the saved information from the backlog queue. If the client does not validate his request, the connection stills half opened and its related information remains saved in the server's backlog. Unfortunately, this limitation was perfectly exploited by attackers to generate SYN flooding attacks.

SYN flooding attacks can be performed by creating several half-opened connections for exceeding the backlog queue capacity (Figure 3). As a result, the server will not be able to provide more connections even those requested by legitimate clients (i.e., the server is now under a denial of service attack). Generally speaking, there are different forms of SYN flooding DOS attacks: (i) Attacker generates the SYN messages using its own IP address. (ii) It can Spoof many IP addresses to bypass the security mechanisms. (iii) In SYN DDOS flooding attack (Figure 4), the attacker compromises several botnets machines and then orders them to simultaneously attack the victim [16].

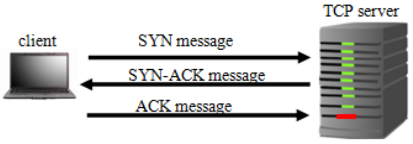


Fig. 2. Establishment process of a new TCP connection.

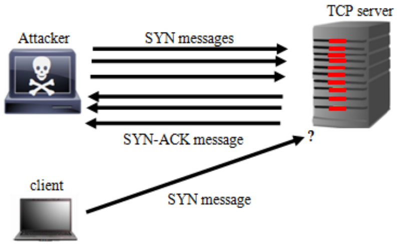


Fig. 3. SYN flooding DOS attack.

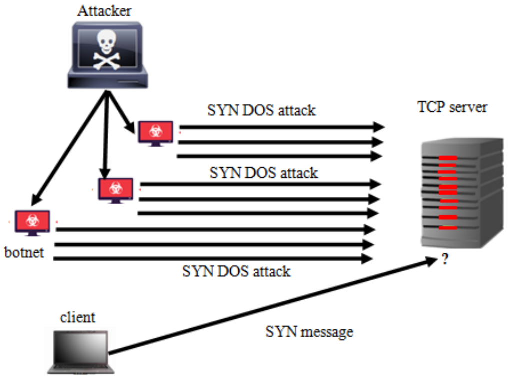


Fig. 4. SYN flooding DDOS attack.

B. DOS/DDOS using ICMPv6 :

The deployment of new technologies has significantly accelerated the migration to the Internet Protocol v6 (IPv6), which replaces more and more the Internet Protocol v4 (IPv4). However, this transition is not totally safe, the old IPv4 and the new class of attacks specific to IPv6 still possible. As shown in Figure 5, the dominant types of these attacks are the Denial of service ones [17].

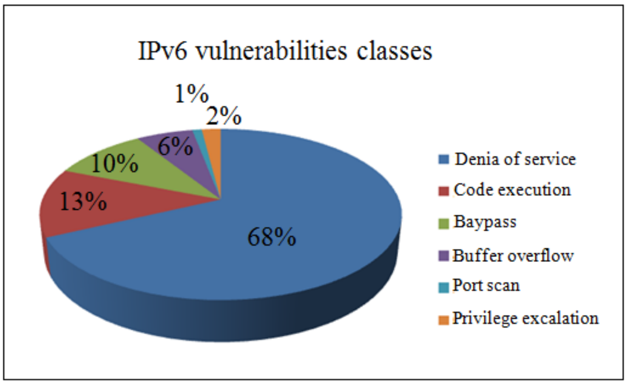


Fig. 5. IPv6 vulnerabilities classes [15].

As a fundamental element of IPv6 protocol stack, several functions depending on the Internet Control Message Protocol version 6 (ICMPv6), such as diagnostic operations, errors report, neighborhood discovering, address resolution and allocation, and duplicate address detection. Unfortunately, numerous attacks, and particularly, DOS/DDOS attacks against IPv6 (Figure 7) are directly related to this protocol. Figure 6 illustrates some examples of those attacks. In this work, we consider the flooding attacks that are related to the Neighbor Discovery Protocol (NDP) and exploits, precisely, three ICMPv6's messages which are Router Advertisement (RA), Neighbor Solicitation (NS) and Neighbor Advertisement (NA).

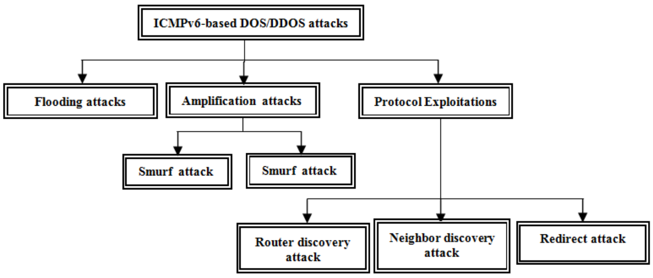


Fig. 6. Different classes of ICMPv6-based DOS/DDOS.

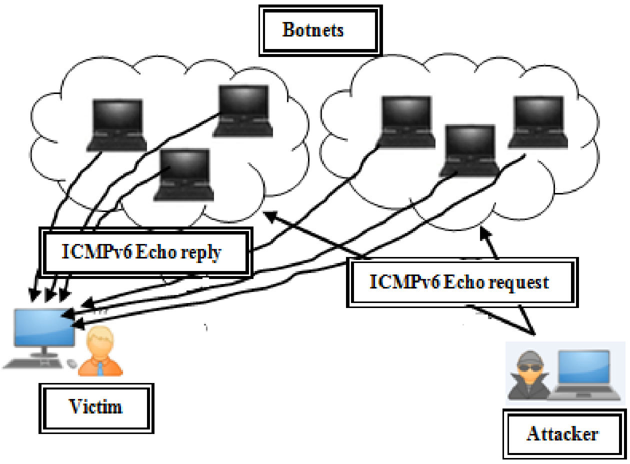
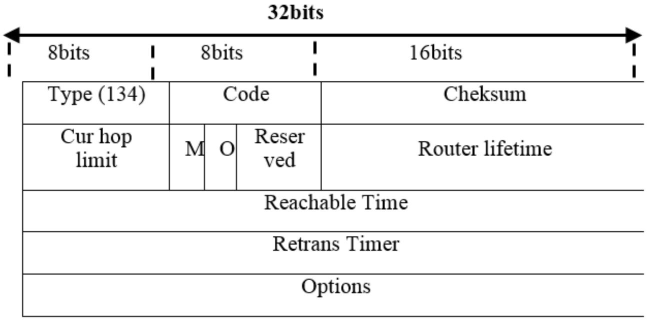


Fig. 7. Example of an ICMPv6-based DDOS attack.

- Router Advertisement Flooding attack:

The router advertisement flooding attack uses the RA ICMPv6 messages which are characterized by a type field equal to 134 and their structure is illustrated in Figure 8. Such messages are generally broadcasted repeatedly by routers to proclaim their presence or to providing routing information to the users who look for valid links to forward their data [18].



32bits

8bits	8bits			16bits
Type (134)	Code			Cheksum
Cur hop limit	M	O	Reser ved	Router lifetime
Reachable Time				
Retrans Timer				
Options				

Fig. 8. The RA message structure.

In router advertisement flooding attack, attackers inundate the targeted victim with spoofed RA messages. On one hand, the victim will become compromised due to the new invalid configuration provided by the attacker. On the other hand, its resources will be totally consumed causing a denial of service.

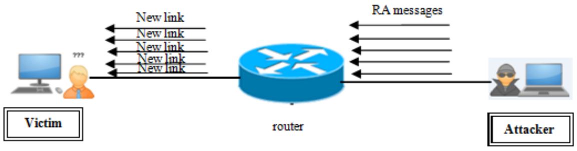
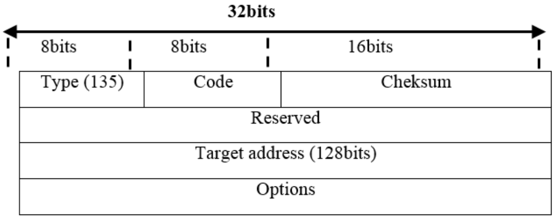


Fig. 9. Router advertisement flooding attack procedure.

- Neighbor Solicitation Flooding attack:

The ICMPv6 assigns a type of 135 to Neighbor Solicitation (NS) messages that having the general format of Figure 10 [18]. The NS messages are typically sent by users for the IPv6 address resolution purpose. When there isn't any restriction, all users, including anomalous and attackers, can proceed this task, and the destinations of such message normally respond with the Neighbor Advertisement (NA) messages including their IPv6 address. As a result, during a Neighbor solicitation flooding attack (Figure 11), the victim is overloaded and turns out of service when trying to serve all these requests.



32bits

8bits	8bits	16bits
Type (135)	Code	Cheksum
Reserved		
Target address (128bits)		
Options		

Fig. 10. : The NS message strusture.

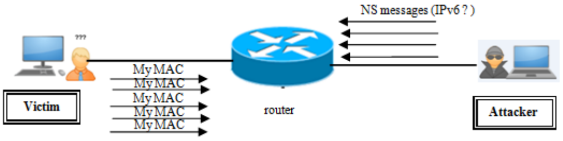
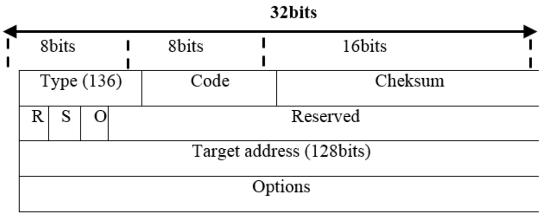


Fig. 11. : Neighbor solicitation floonding attack procedure.

- Neighbor Advertisement flooding attack

The Neighbor Advertisement (NA) messages are identified by a type field value fixed at 136, as illustrated in Figure 12 [18]. IPv6 users, generally, use the NA messages either as a response of the received neighbor solicitation requests (i.e., NS messages) or to report an eventual modification of link-layer addresses. Hence, the advertisement flooding attack can create a denial of service by exhausting the victim's resources or changing continuously their configuration. They can never communicate between them and their data can be redirected to the attacker itself.



32bits

8bits			8bits	16bits
Type (136)			Code	Cheksum
R	S	O	Reserved	
Target address (128bits)				
Options				

Fig. 12. : The NA message strusture.

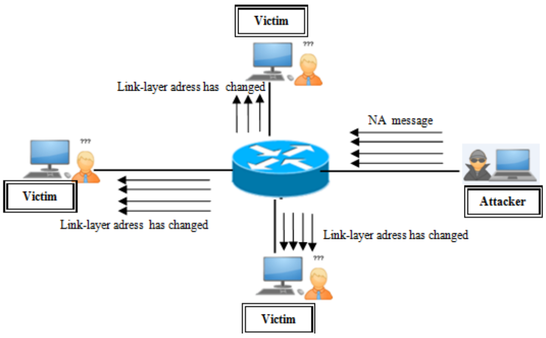

Victim
Link-layer adress has changed
NA message
Victim
Attacker
Link-layer adress has changed
Link-layer adress has changed
Victim

Fig. 13. Neighbor advertisement flooding attack

III. HD-BASED ANOMALY DETECTION MECHANISM

In this paper, we will utilize the HD metric to develop an anomaly detection mechanism to defend against various figures of DOS/DDOS attacks. HD an important statistical measure that can be used to quantify the dissimilarity or closeness between two probability density functions (PDFs) [19,20]. The dissimilarity between two probability distributions $p_1(x)$ and $p_2(x)$ is measured by the squared HD of $p_1(x)$ relative to $p_2(x)$, as follow:

$$HD^2\left(p_1(x), p_2(x)\right) = \frac{1}{2}\sum\left(\sqrt{p_1(x)} - \sqrt{p_{21}(x)}\right) \qquad (1)$$

which can be considered as the Euclidean norm of the difference of the square root vectors:

$$HD^2(p_1, p_2) = \frac{1}{\sqrt{2}} \parallel \sqrt{p_1} - \sqrt{p_2} \parallel^2 \qquad (2)$$

For univariate normal distributions $p_1(x)$ and $p_2(x)$ of a random variable x, $p_1 \sim N(\mu_0, \sigma_0)$ and $p_2 \sim N(\mu_1, \sigma_1)$ where μ_0 and μ_1 are the means and σ_0^2 , σ_1^2 are the variances for p_1 and p_2, the HD between p_1 and p_2 is given by:

$$HD^2(p_1, p_2) = 1 - \sqrt{\frac{2\sigma_0\sigma_1}{\sigma_0^2 + \sigma_1^2}}\, exp\left(-\frac{1}{4}\frac{(\mu_0 - \mu_1)^2}{\sigma_0^2 + \sigma_1^2}\right) \qquad (3)$$

When changes affect only on the mean (i.e., $\sigma_0^2 = \sigma_1^2$), Eq (3) can be rewritten as:

$$HD^2(p_1, p_2) = 1 - exp\left(-\frac{1}{8}\frac{(\mu_0 - \mu_1)^2}{\sigma_0^2}\right) \qquad (4)$$

When $p_1(x)$ and $p_2(x)$ are similar, the derived values of HD are mostly null. Otherwise, high values occur in the case of a great deviation between these distributions. This makes HD very practical in detecting networks traffic anomalies specifically that are resulting from DOS/DDOS attacks. Thereby, we use HD metric as an anomaly indicator. In absence of DOS/DDOS attacks, HD measures become closer to zero, while larger values of HD are obtained under the presence of those attacks. To automatically isolating and locating attacks, we set the detection threshold using Shewhart chart, which is commonly known as the three-sigma rule [21]. The upper control limit is determined as,

$$UCL_{HD} = \mu_0^{HD} + 3\sigma_0^{HD}$$

where μ_0^{HD} and σ_0^{HD} are the mean and standard deviation of HD measurements under anomaly-free case. When the i^th HD value is beyond the upper threshold, UCL_{HD} then we claim the presence of DOS/DDOS attacks. Else, the captured data falls in the normal conditions of traffic network.

IV. EXPERIMENT RESULTS

In this section, we evaluate the detection capacity of the HD-based detection mechanism in the presence of SYN flood, UDP flood and ICMPv6 attacks.

1) Case study (A)- detection SYN flooding attacks in DARPA99 traffic :

In this first experiment, we investigate the capability of HD-Shewhart in uncovering SYN flooding attacks in the DARPA99 traffic [22]. In DARPA 99 dataset, the traffic traces were collected from a simulated network similar to the real online network of a US air force base. This traffic provides three weeks of training traffic and two weeks of test traffic that introduce different categories of attacks. Here, we consider the SYN flooding DOS attacks in the traffic of the week 5: an attack in day 1 at 18:04:04 pm for 6mn51s, two attacks in day 2 at 11:48:42 am, and 18:16:05 pm and lasted 1s and 3mn26s, respectively [22].

Figure 14 (a) shows the HD-Shewhart detection result in the presence of SYN flooding DOS attacks occurred in week 5 day1. In this attack, the victim was overwhelmed by more than 2928 SYN segments/instance. Also, Figure 14(a) shows that the HD-Shewhart detects an anomalous behavior at the instance 150 in which some hosts have received about 39 SYN/s. Figure14 (b) reports the presence of two attacks in the second day of week 5. The two victims of these attacks were flooded by 3027 SYN/instance and 2564 SYN/instance, respectively. Results show that the SYN flooding DOS attacks were effectively detected by the HD-based approach.

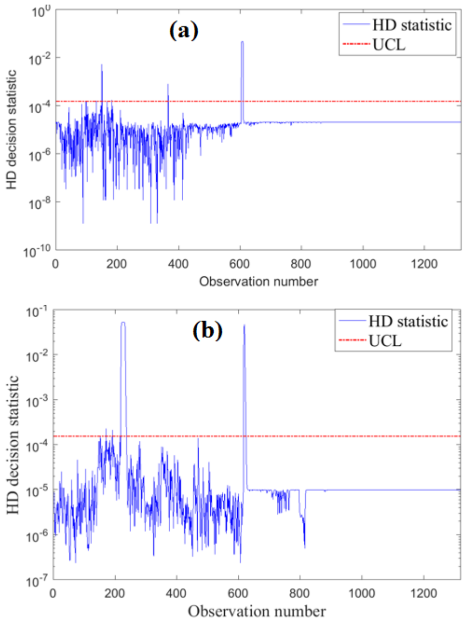


Fig. 14. Detection result of HD-Shewhart chart under SYN flooding DOS attacks (a) week 5/day 1, (b) week5/day2.

2) Case study (B): detection of UDP flood attacks in DARPA99 traffic:

Now, the detection capability of the HD-Shewhart approach is tested under the UDP flood attacks. The DARPA 99 dataset contains two UDP flood attacks in week 5 day1 [23]. These attacks targeted two different victims at 20:00:27 pm and lasted about 15mn. Figure 15 reports the detection result of such attacks. The results show that HD-Shewhart detects these attacks. Both of victims were inundated by more than 6494 datagram/instance. Also, these results (Figure 15) indicate other anomalies in the UDP traffic starting from the time instance 45. Indeed, a domain name problem was the origin of those anomalies.

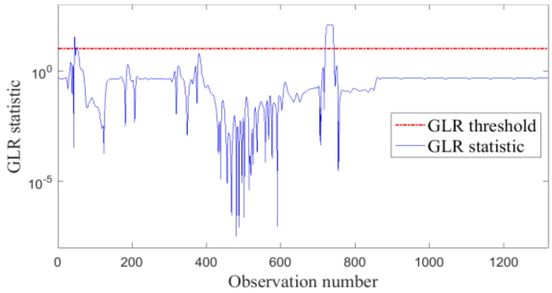


Fig. 15. Detection result of HD-Shewhart chart under UDP flood attacks (week 5/day 1).

3) Case study (C): detection of ICMPv6-based DOS flooding attacks:

Here, we investigate the capability of HD-Shewhart to mitigate different types of ICMPv6-based DOS attacks. Figure 16 shows the network used to generate the ICMPv6 traffic dataset. This topology was created under the network emulator GNS3 that connect real and virtual devices and run as well as real Cisco IOS images. The normal traffic contains 48 hours of ICMPv6 attack-free traffic. The anomalous traffic is generated using the THC toolkit and provides several ICMPv6-based DOS and DDOS flooding attacks [23]. Here, we consider the Router advertisement flooding, the Neighbor advertisement flooding, and neighbor solicitation flooding DOS attacks. Their time of appearance and duration are (1mn10s, 3s), (1mn20s, 4s) and (0s, 1s), respectively.

Figure 17 (a-c) and Figure 18(a-c) present the detection results using the three messages (RS, NA, and NS) and the total of ICMPv6 traffic, respectively. In both cases, HD-Shewhart has achieved a high rate of detection. The ICMPv6-based DOS attacks were detected correctly without false alarms.

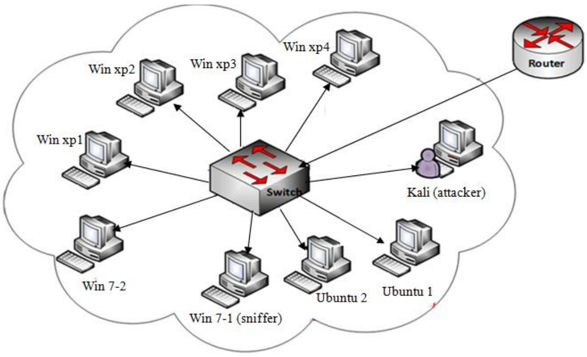


Fig. 16. Topology of the network used to generate ICMPv6 dataset.

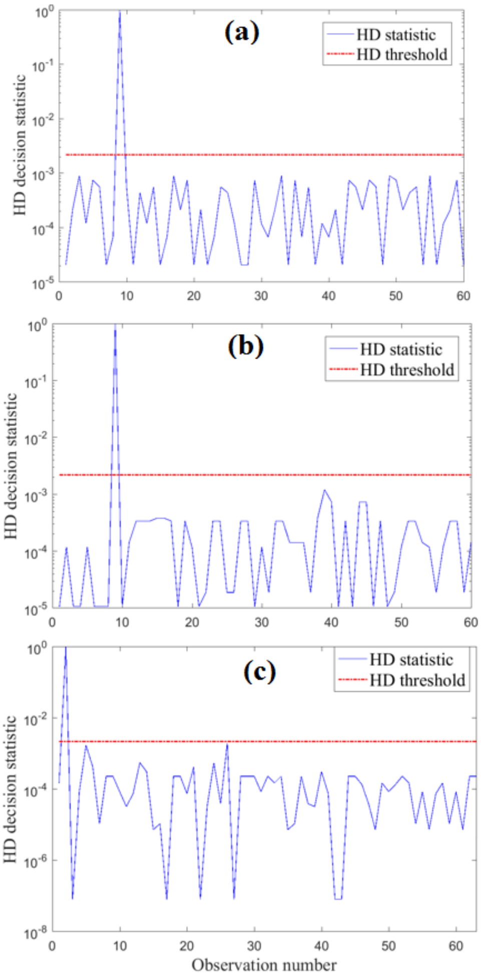


Fig. 17. Detection result of HD-Shewhart chart under ICMPv6-based DOS attacks (a) RA, (b) NA, (c) NS

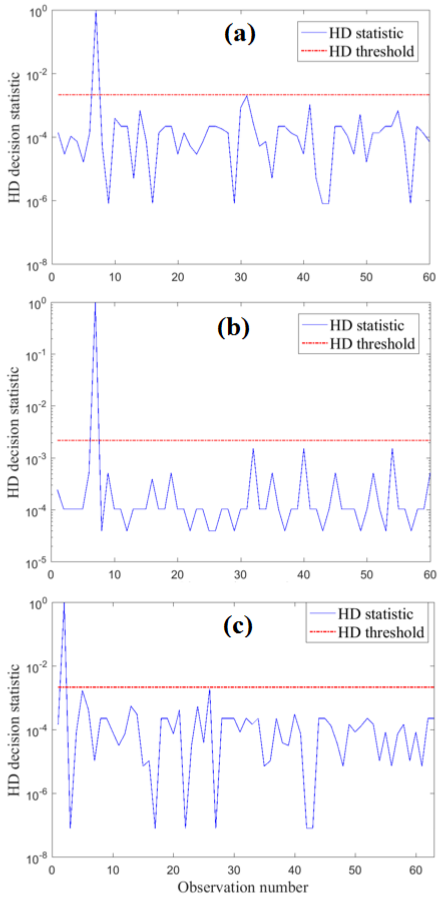


Fig. 18. Detection result of HD-Shewhart under ICMPv6-based DOS attacks by monoring of all ICMPv6 traffic (a) RA, (b) NA, (c) NS.

V. CONCLUSION

A methodology to detect Denial Of Service and Distributed Denial Of Service attacks based on Hellinger distance (HD) is developed in this paper. Precisely, HD is employed to discriminate between the attack-free traffic and the anomalous traffic. Then, the Shewhart chart is applied to HD measurements to reveal anomalous traffic. This methodology is evaluated using DARPA99 and ICMPv6 datasets. Results demonstrated that HD-Shewhart has good capability in detecting SYN and ICMPv6-based DOS/DDOS flooding attacks.

ACKNOWLEDGEMENT

The research reported in this publication was supported by funding from King Abdullah University of Science and Technology (KAUST) Office of Sponsored Research (OSR) under Award No: OSR-2015-CRG4-2582. The authors (Benamar Bouyeddou and Benamar Kadri) would like to thank the STIC Lab, Department of Telecommunications, Abou Bekr Belkaid University for the continued support during the research.

REFERENCES

[1] T.Ibragimov, O.Kupreev, E.Badovskaya, A.Gutnikov," DDOS attacks in Q2 2018," Kaspersky Lab, july 24, 2018.

[2] Bouyeddou, B., Harrou, F., Sun, Y. and Kadri, B. "Detecting SYN flood attacks via statistical monitoring charts: A comparative study." In Electrical Engineering-Boumerdes (ICEE-B), 2017 5th International Conference on, pp. 1-5. IEEE, 2017.

[3] Bouyeddou, B., Harrou, F., Sun, Y. and Kadri, B. "Detection of smurf flooding attacks using Kullback-Leibler-based scheme." In 2018 4th International Conference on Computer and Technology Applications (ICCTA), pp. 11-15. IEEE, 2018.

[4] K. Hussain,, H. Syed Jawad, D. Veena, N. Muhammad, and A. Muhammad Awais. "An Adaptive SYN Flooding attack Mitigation in DDOS Environment." International Journal of Computer Science and Network Security (IJCSNS) 16, 2016, PP.27-33.

[5] M.S. Al-hawawreh," SYN Flood Attack Detection in Cloud Environment Based on TCP/IP Header Statistical Features," 2017 8th International Conference on Information Technology (ICIT).

[6] C.Sun, C.Hu and B.Liu,"SACK2: effective SYN flood detection against skillful spoofs. IET Inf Secure 2012, 6(3):149–156.

[7] G.Ramadhan, Y.Kurniawan and C-S.Kim," Design of TCP SYN Flood DDoS Attack Detection Using Artificial Immune Systems," IEEE 6th International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, October 3-4, 2016.

[8] S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S. Palazzo, "Operetta: An OPEnflow-based REmedy to mitigate TCP SYNFLOOD attacks against Web servers," Comput. Netw., vol. 92, no. 1, pp. 89–100, 2015

[9] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (send)," Tech. Rep., 2005.

[10] M. Kassim and H. Kassim, "An analysis on bandwidth utilization and traffic pattern for network security management," Journal of International Proceedings on Computer Science and Information Technology, www. ipcsit. com, vol. 13, pp. 51–56, 2011.

[11] F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the neighbor discovery protocol," 2nd International Workshop on IPv6 Today-Technology and Deployment-IPv6TD 2007 , 2007.

[12] M. Zulkiflee, M. Azmi, S. Ahmad, S. Sahib, and M. Ghani, "A framework of features selection for ipv6 network attacks detection," WSEAS Trans Commun, vol. 14, no. 46, pp. 399–408, 2015.

[13] J. Wu, J. Bi, M. Bagnulo, F. Baker, and C. Vogt, "Source address validation improvement (SAVI) framework," 2013. Internet Draft.

[14] M. Basseville, Divergence measures for statistical data processing – anannotated bibliography, Signal Process. 93 (4) (2013) 621–633.

[15] I. Csiszár, P. Shields, Information Theory and Statistics: A Tutorial, NowPublishers Inc., 2004.

[16] W.M. Eddy," Defenses against TCP SYN flooding attacks," Internet protocol journal, vol 9, No 4, 2006.

[17] Ard JB Internet protocol version six (ipv6) at uc davis: traffic analysis with a security perspective. University of California, Davis, 2012

[18] T. Narten, E. Nordmark, W. Simpson and H. Soliman," Neighbor Discovery for IP version 6 (IPv6)," RFC4861, Sept., 2007

[19] M. Basseville, Divergence measures for statistical data processing – anannotated bibliography, Signal Process. 93 (4) (2013) 621–633.

[20] Harrou F, Madakyaru M, Sun Y. "Improved nonlinear fault detection strategy based on the Hellinger distance metric: Plug flow reactor monitoring." Energy and Buildings 143 (2017): 149-161.

[21] D.C. Montgomery « Introduction to Statistical Quality Control » 6th ed, Wiley, 2009

[22] https://www.ll.mit.edu/ideval/data/1999data.html

[23] O. E. Elejla, B.Belaton, M. Anbar, and A.Alnajjar, "A reference dataset for ICMPv6 flooding attacks," Journal of Engineering and applied sciences, vol. 11, no. 3, pp. 476–481, 2016.