A Method to Detect DOS and DDOS Attacks based on Generalized Likelihood Ratio Test

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

Ying Sun[a] and Benamar Kadri[b]
[b]STIC Lab., Department of Telecommunications
Abou Bekr Belkaid University, Tlemcen, Algeria
e-mail: bouben81@yahoo.fr,

***Abstract*— Denial of service (DOS) and distributed DOS (DDOS) continue to be a significant concern in internet and networking systems. This paper targets to develop an anomaly detection mechanism based on the generalized likelihood ratio (GLR) scheme to detect TCP and ICMPv6 based DOS/DDOS attacks. The anomaly detection problem is addressed as a hypothesis testing problem. The proposed approach uses GLR test to monitor internet traffic for better detecting potential cyber-attacks. The decision threshold of GLR approach has been computed nonparametrically based on kernel density estimation. To evaluate the performance of this approach, two network traffic datasets have been used namely the DARPA99 and ICMPv6 datasets. Results highlight the efficiency of the proposed method.**

Keywords—SYN flooding, ICMPv6 attacks, DOS/DDOS GLR test, DARPA99 dataset, ICMPv6 dataset.

I. INTRODUCTION

Security issues in internet traffic is an important problem attracting both researchers and industrial practitioners. Denial of service (DOS) and distributed DOS (DDOS) attacks still represent a persistent security issue threatening modern information and communication technologies. These attacks can result in a serious problem even unrecoverable damages of the traffic network. Specifically, DOS and DDOS attacks could suspend temporarily or permanently the availability of networks and services. To achieve this objective, attackers generally overload the targeted victims with large network traffics. Recently, the Memcached DDoS attack on March 2018 has made the record with more than 1.7 Tb/s that turned out of service the famous Github platform [1].

All over the years, several methods have been developed for detecting DOS and DDOS attacks [2-3]. Nezhad et al. [4] proposed a detection technique based on the Auto-Regressive Integrated Moving average (ARIMA) and the chaotic theory. Meng et al. [5] used Markov chains to detect the applicative client's anomalous activities. Kansal et al. [6] designed a proxy-based approach called Early Detection and Isolation policy (EDIP) to identify illegitimate users and then prevent them from accessing the system. In [7], Xiang et al. recommend the utilization of information theory metrics to deal with low rate DOS/DDOS attacks. Semerci et al. [8] targeted the detection of DDOS attacks in Voice over IP (VOIP) applications using DCMP models. Bhatia [9] discussed the revelation of networks anomalies that are related either to high rate normal (i.e., rush-hour) and DOS/DDOS traffics. To this end, they monitored packets characteristics and victim's resources consumption. Divakaran et al. [10] incorporated a control mechanism to forward TCP connection requests at edge routers. Lukaseder et al. [11] exploited the software-defined network's properties to mitigate the distributed reflection DOS (DRDOS) attack, in particular, UDP-based flooding DDOS attacks which become more and more popular. Doshi et al. [12] studied the ability of machine learning techniques to handle DOS/DDOS launched against Internet of Things (IOT) equipments. Zhang et al. [13] implemented a protection mechanism of SDN resources. This solution consists, firstly, in eliminating, the invalid sources, and then tracking the resources utilization of valid users. Ramadhan et al. [14] combined the Artificial Immune System and the Dendritic Cell algorithm to detect TCP-based DOS and DDOS flooding attacks. To detect SYN flooding attacks, Tuncer et al. [15] applied the fuzzy logic to classify different TCP segments. Zulkiflee et al. [16] discriminated attacks in Internet Protocol version 6 (IPv6) networks using the SVM method. To track the users behind the ICMPv6-based DOS/DDOS, Conta et al. [17] added the ICMP traceback messages.

While the majority of emerging technologies (e.g., internet of things, cloud computing, and software-defined networks) run entirely or partially over the TCP/IP architecture, their vulnerabilities were well revealed. Particularly, to perform most of DOS and DDOS attacks, attackers have been principally and effectively exploited the TCP-based SYN flooding and ICMP-based attacks. To mitigate such attacks, we addressed the problem of TCP and ICMPv6 based DOS/DDOS attacks as a hypothesis testing problem. Specifically, we present in this paper an effective detection technique based on the generalized likelihood ratio (GLR) test [18-20]. Here, we exploit the high detection performance of GLR test to reveal unexpected network traffic anomalies which are caused eventually by DOS/DDOS flooding attacks. We validated our approach with the DARPA99's IPv4-based traffic and the ICMPv6 dataset.

The rest of this paper is organized as follows. Section II introduces the problem of TCP SYN and the ICMPv6-based flooding attacks. In section III, we present our GLR-based detection scheme. Section IV reports the evaluation results of the GLR test under DOS/DDOS flooding attacks. Finally, conclusions are presented in Section V.

II. TCP SYN AND ICMPV6-BASED FLOODING ATTACKS

A. TCP SYN flood attacks :

SYN flooding attacks have been extensively used for the last two decades and still remain on the top of DOS/DDOS

attacks. In the second quarter of 2018, around 80.2% of DOS/DDOS attacks are SYN flooding [21]. These attacks exploit the resource reservation mechanism when initializing a new TCP connection. To establish a connection with the TCP server [22], the client generates a Synchronization message (SYN) (Figure 1). The server, in turn, responds with the Synchronization/Acknowledgement (SYN/ACK) message and reserves some memory space to save the related information. Finally, the client confirms his request by acknowledging (ACK) the received SYN/ACK. Then, the connection is successfully established, and the server frees the reserved memory space (Figure 1). Otherwise, in the absence of client confirmation, the connection continues to be half-opened occupying the reserved memory space. Unfortunately, this vulnerability was perfectly exploited by attackers to trigger SYN flooding attacks (Figure 2). Filling up the victim's memory resource is the aim of attackers. They can exhaust the entire memory by initiating a sufficient number of SYN messages to cause a denial of service. Accordingly, the server will not be able to provide more connections. There are, in general, three different variants of SYN flooding attack. The basic one is the direct SYN flooding DOS attack in which the attacker uses its own IP address to sends SYN messages. To make it more effective, in the second variant of SYN flooding attacks, the attacker spoofs many IP addresses to bypass the eventual security mechanisms. The third way of that attack is the SYN flooding Distributed DOS attack (Figure 3). To do so, attacker manipulates several botnets and synchronizes them to launch simultaneously their attacks [23].

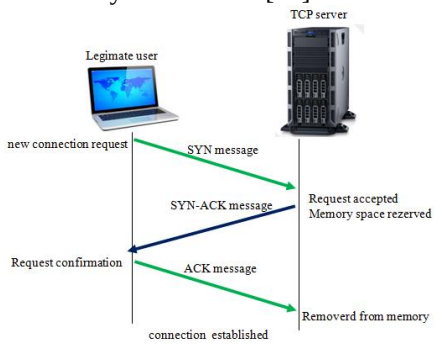


Fig. 1. Establissment process of a new TCP connection.

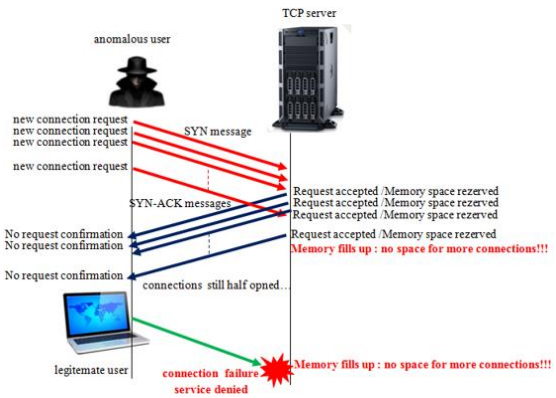


Fig. 2. SYN flooding DOS attack.

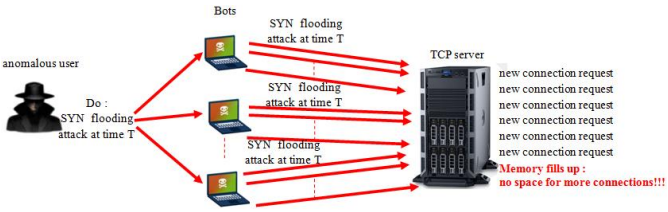


Fig. 3. SYN flooding DDOS attack.

B. ICMPv6-based DOS/ DDOS attacks :

With the universal success of the internet, different devices have been used online, which cause the depletion of the four bytes based addresses provided by the Internet Protocol version 4 (IPv4). To bypass this issue, the version six of internet protocol (IPv6) has adopted a new address plan with 16 bytes. There are more than sufficient IPv6 addresses that can support present and future technologies. Moreover, the IPv6 integrates other functionalities (e.g., routes management, data treatment, hosts auto-configuration, and end to end links). To this end, IPv6 delegates the Internet Control Message Protocol version six (ICMPv6) to make available most of the needed information such as neighborhood, routers and IP MAC translation [24]. The ICMPv6 is a core protocol in all IPv6-based networks. However, in term of security, it constitutes the origin of a non-negligible number of vulnerabilities, and attackers are already carried out many ICMPv6-based DOS/DDOS attacks. The most distinguished examples of those attacks include ping flood, Smurf and remote Smurf, routers and neighbors discovery attacks. We focus, in this paper, on the ICMPv6-based DOS/DDOS attacks against the discovery mechanism. This last concerns two fundamental operations. The first one is the determination of in-subnet routers to connect end users and assures their exchanges. Such users solicit the presence of routers via the Router solicitation (RS) message. The closest one replies with a Router Advertisement (RA) message providing the route's configuration. The second is the neighbor discovery operation, which is essentially useful in detecting duplicate IPv6 addresses and IPv6-MAC addresses translation. This operation is realized with the Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages. Fakes forms of these four ICMPv6 messages (i.e., RA, RS, NS, and NA) can affect network performance even creating a denial of service situations. Figure 4 illustrates a flooding DOS/DDOS attack in the IPv6 environment [25].

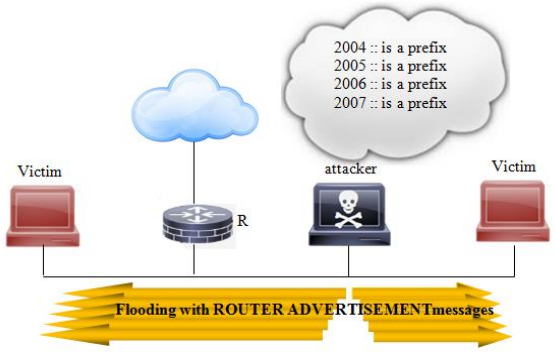


Fig. 4. ICMPv6 DOS attack using the RA message.

III. GLR-BASED APPROACH

The Generalized Likelihood Ratio (GLR) test is an important tool to discriminate between two composite hypotheses [26-27]. Assume that $Y = [y_1, y_2, \dots, y_n] \epsilon \mathbb{R}^n$ is a vector from one of two Gaussian distributions, $\mathcal{N}(0, \sigma^2 I_n)$ or $(\theta \neq 0, \sigma^2 I_n)$, where θ is the value of anomaly, and $\sigma^2 > 0$ is the variance. The main goal of GLR detector is choosing between the null hypothesis (i.e., free-attack situation), $\mathcal{H}_0 = \{Y \sim \mathcal{N}(0, \sigma^2 I_n)\}$, and the alternative hypothesis (i.e., anomalous traffic), $\mathcal{H}_1 = \{Y \sim \mathcal{N}(\theta \neq 0, \sigma^2 I_n)\}$. To do so, the GLR, $\mathfrak{L}(Y)$is compared to the threshold, $h(\alpha)$. If $\mathfrak{L}(Y)$is smaller than or equal to $h(\alpha)$, then we reject $\mathcal{H}_0$ and conclude that the data have provided significant evidence to support $\mathcal{H}_0$. The GLR statistic, $\mathfrak{L}(Y)$, is expressed as [26]:

$$\mathfrak{L}(Y) = 2 \log \frac{\sup_{\theta \epsilon \mathbb{R}^n} f_0(Y)}{f_{\theta=0}(Y)} \quad (1)$$

$$= 2 \log sup_\theta \left\{ exp\left\{ -\frac{\|Y-\theta\|_2^2}{2\sigma^2} \right\} / exp\left\{ -\frac{\|Y\|_2^2}{2\sigma^2} \right\} \right\}$$

Where $\|.\|_2^2$ is the Euclidean norm and $f_0(Y) = \frac{1}{(2\pi)^{\frac{n}{2}}\sigma^n} exp\left\{ -\frac{1}{2\sigma^2} \| Y - \theta \|_2^2 \right\}$ is the pdf of Y. Then (1) can be expressed as:

$$\mathfrak{L}(Y) = \frac{1}{\sigma^2}\left\{ \| Y - \hat{\theta} \|_2^2 + \| Y \|_2^2 \right\} \quad (2)$$

After estimating θ as $\hat{\theta} = arg\ \min_\theta \| Y - \theta \|_2^2 = Y$, we get,

$$\mathfrak{L}(Y) = \frac{1}{\sigma^2}\{ \| Y \|_2^2 \} \quad (3)$$

The threshold $h(\alpha)$ is determined to obtain the desired probability of false alarm, selected a priori.

$$\mathbb{p}_0\big(\mathfrak{L}(Y) \geq h(\alpha)\big) = \int_h^\infty f_0(y)dy = 1 - F_{\chi^2}(h) = \alpha \quad (4)$$

The power function is computed as:

$$\beta_{\delta^*}(c^2) = \mathbb{p}_0\big(\delta^*(Y)\big) = 1 - F_{1,\gamma(\theta)}(h)$$

where $F_{1,\gamma}(Y)$is the non central $\chi^2(1,\gamma)$ distribution with one degree of freedom, and the non-centrality parameter $\gamma(\theta) = \frac{1}{\sigma^2} \| P_H^\perp \theta \|_2^2$.

For non-Gaussian data, kernel density estimation (KDE) can be used to estimate the distribution of GLR. Then a nonparametric threshold of GLR approach is defined as the $(1-\alpha)$-th quantile of the estimated distribution of GLR obtained by KDE.

IV. PERFORMANCE EVLUATION

In this section, we evaluate the capability of the GLR-based method to uncover DOS/DDOS attacks using DARPA99 and ICMPv6 traffic datasets.

1) Case study (A): detection of DARPA99's SYN flooding attacks:

Here, we present the performance of the GLR test under the SYN flooding attacks in week 5 of the DARPA99 dataset. The DARPA 99 dataset is a collection of IPv4 traffics created by Lincoln Laboratory at Massachusetts Institute of Technology (MIT) under the sponsorship of Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL) [28]. The traffic traces were collected from a simulated network similar to the real online network of a US air force base. The dataset includes three weeks of training data and two weeks of test data that introduce different categories of DOS/DDOS attacks [28]. The week 5 provides three TCP SYN flood attacks that appear as follow: day 1 at 18:04:04 pm for 6mn51s, day 2 at 11:48:42 am and 18:16:05 pm for the duration of 1s and 3mn26s, respectively. As it is reported in Figure 5(a-b), the detection results show that GLR test has detected the three attacks without introducing false alarms. Figure 5(a) shows that the GLR test detects an abnormal traffic at the observation number 150.

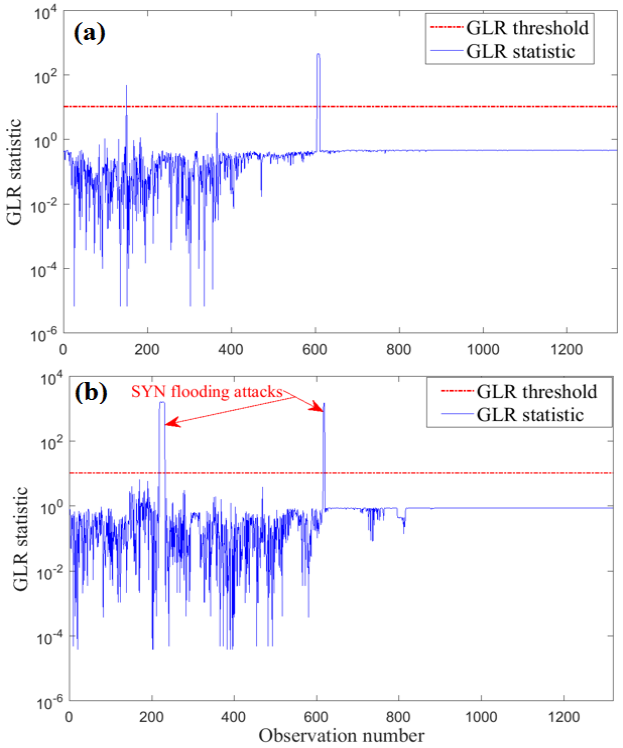


Fig. 5. Detection results of the GRL approach under SYN flooding attacks (a) week 5/day 1, (b) week5/day2.

2) Case study (B): detection of DARPA99's UDP flood attacks:

In this case study, we test the GLR approach in the presence of UDP flood attacks. In the traffic of week 5 day 1, there are two UDP flood attacks that are initiated at 20:00:27 pm for 15mn against two different victims. The detection result (Figure 6) illustrates that the UDP flood attacks are successfully detected, they appear between the observation number of 722 and 742. We can see also the presence of abnormal behavior at instance 45.

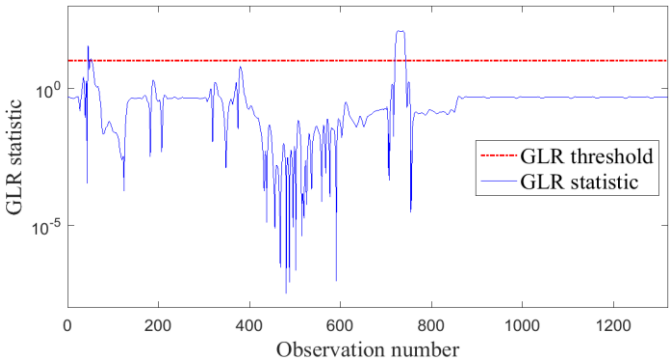


Fig. 6. Detection results of the GRL approach under UDP flood attacks (week 5/day1).

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

In this case study, we evaluate the capacity of the GLR approach in detecting ICMPv6-based DOS flooding attacks. Figure 7 introduces the network used to generate the ICMPv6 traffic dataset. This topology is 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 traffic that is completely free from attacks. The anomalous traffic is generated using the THC toolkit and provides several ICMPv6-based DOS and DDOS flooding attacks [29]. We consider the ICMPv6-based flooding attacks based on the RA, NS and NA messages. Table I reviews these attacks. From the detection results of Figure 8(a-c) and Figure 9(a-c), we conclude that monitoring either only the RA, NS, and NA or the ICMPv6 traffic messages allowed the detection of the different attacks.

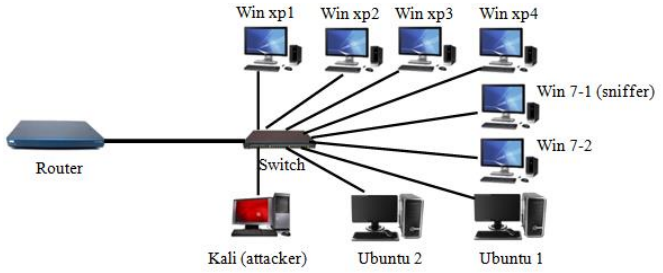


Fig. 7. Topology of the network used to generate ICMPv6 dataset.

TABLE I. ICMPV6-BASED FLOODING ATTACKS IN ICMPV6 TRAFFIC DATASET

Attack	*Time of appearance*	*Duration*
Router advertisement	1mn10s	3s
Neighbor solicitation	0s	1s
Neighbor advertisement	1mn20s	4s

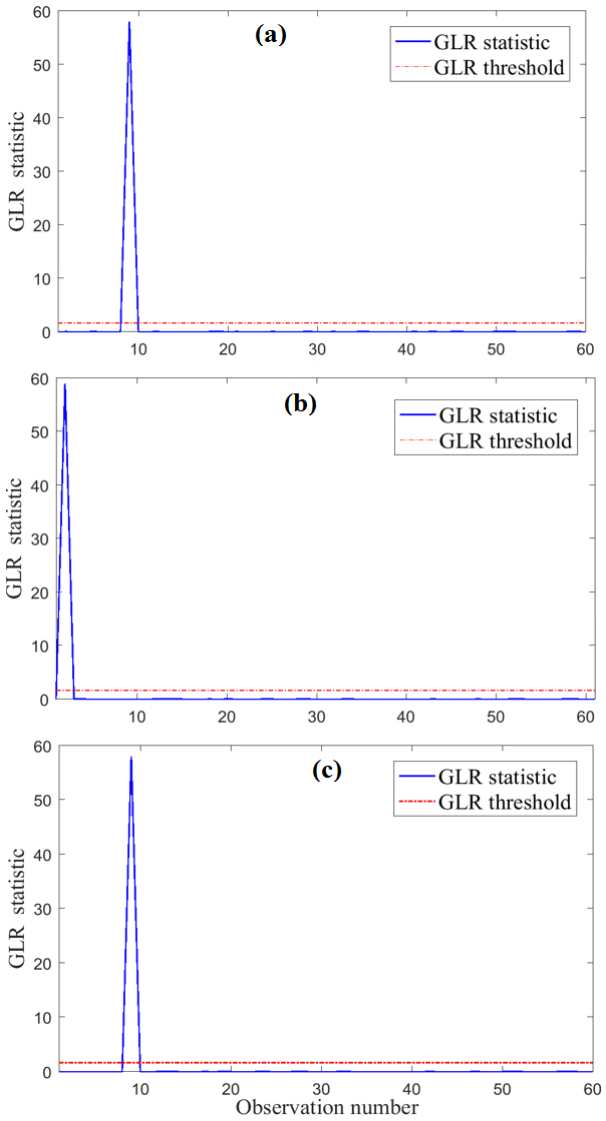
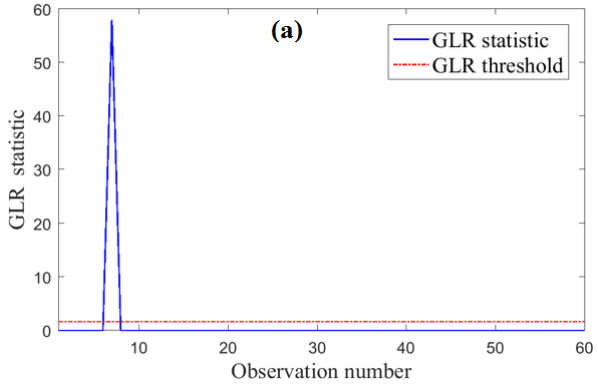


Fig. 8. Detection results of the GLR approach under ICMPv6-based DOS attacks by monitoring (a) RA, (b) NA, (c) NS.



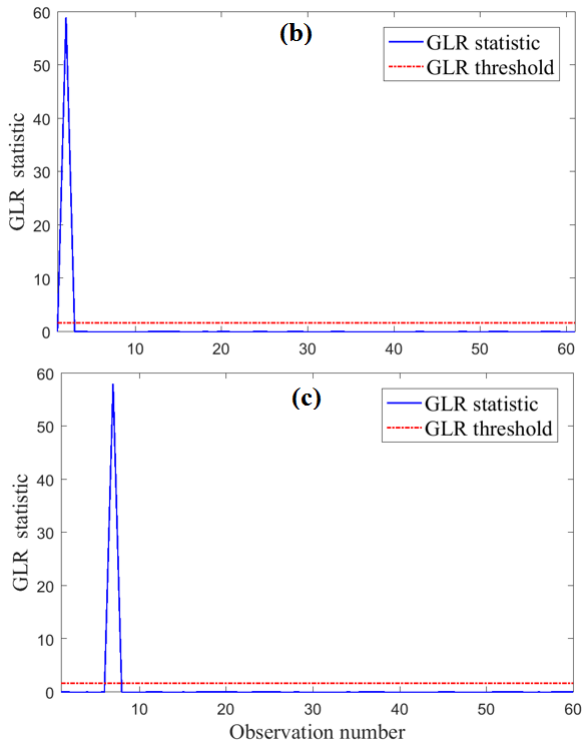


Fig. 9. Detection results of the GLR approach under ICMPv6-based DOS attacks by monitoring of all ICMPv6 traffic (a) RA attack, (b) NA attack, (c) NS attack.

V. CONCLUSION

In overall, this paper deals with security of the internet traffic with a focus on DOS/DDOS flooding attacks in IPv4/IPv6 based networks. We propose a statistical scheme to detect anomalies in internet traffic based on GLR hypothesis scheme. Specifically, we applied GLR approach to uncover attacks against TCP and ICMPv6 protocols. Here, the decision threshold of GLR test is computed nonparametricaly via kernel density estimation. We validated the performance of this GLR-based method under two different network traffics which are the DARPA99' IPv4 traffic and an ICMPv6 traffic. Results show the good performance of GLR test in detecting 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] M. Kumar, "1.7 Tbps DDoS Attack – Memcached UDP Reflections Set New Record," Accessed on 2018-04-02. [Online]. Available: https://thehackernews.com/2018/03/ddos-attack-memcached.html

[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] S.M.T.Nezhad, M. Nazari, and E.A. Gharavol,"A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks,", IEEE Comm. Letters, vol 20, no 4, Apr, 2016

[5] B.Meng, W.Andi, X.Jian and Z.Fucai," DDOS Attack Detection System based on Analysis of Users' Behaviors for Application Layer," IEEE CSE/EUC Conferences, vol1 ,pp 596 - 599 , 2017.

[6] V.Kansal and M.Dave," Proactive DDoS Attack Detection and Isolation," International Conference on Computer, Communications and Electronics, July 01-02, 2017

[7] Y.Xiang, K. Li, and W.Zhou," Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE trans on information and forensics and security, vol 6, no2, 2011.

[8] M.Semerci, A.T.Cemgil, and B.Sankur," An intelligent cyber security system against DDoS attacks in SIP networks," Computer Networks 136, pp 137–154, 2018.

[9] S.Bhatia, "Ensemble-based model for DDoS attack detection and flash event separation," Future Technologies Conference, pp 958–967, 2016.

[10] D. M. Divakaran, H. A. Murthy, and T. A. Gonsalves, "Detection of SYN flooding attacks using linear prediction analysis," in 14th IEEE International Conference on Networks, 2006. ICon'06, vol. 1. IEEE, 2006, pp. 1–6.

[11] Thomas Lukaseder, Kevin St¨olzle, Stephan Kleber, Benjamin Erb, Frank Kargl," An SDN-based Approach For Defending Against Reflective DDoS Attacks," Aug, 2018

[12] R.Doshi,N.Apthorpe and N. Feamster,"Machine Learning DDoS Detection for Consumer Internet of Things Devices,"Apr 2018

[13] Menghao Zhang, Jun Bi_, Jiasong Bai, Guanyu Li,"FloodShield: Securing the SDN Infrastructure Against Denial-of-Service Attacks", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering

[14] 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.

[15] T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in International Conference on Information Security and Assurance, 2008, pp. 321-325.

[16] 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.

[17] A. Conta and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification," 2006.

[18] F.Harrou, L.Fillatre and I.Nikiforov,"Anomaly detection/detectability for a linear model with a bounded nuisance parameter" Annual Reviews in Control, 38 (1), 32-44, 2014.

[19] Harrou, F., Zeroual, A. and Sun, Y. "Traffic congestion detection based on hybrid observer and GLR test." In 2018 Annual American Control Conference (ACC), pp. 604-609. IEEE, 2018.

[20] Harrou, F., Fillatre, L., Bobbia, M. and Nikiforov, I., "Statistical detection of abnormal ozone measurements based on constrained generalized likelihood ratio test." In Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on, pp. 4997-5002. IEEE, 2013.

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

[22] RFC 793,"Transmission Control Protocol".

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

[24] A. Conta and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification," 2006

[25] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms," IETE Technical Review, vol. 34, no. 4,pp. 390–407, 2017.

[26] F.Harrou, L.Fillatre and I.Nikiforov,"Anomaly detection/detectability for a linear model with a bounded nuisance parameter" Annual Reviews in Control, 38 (1), 32-44, 2014.

[27] F.Harrou, L.Fillatre and I.Nikiforov,"Bounded nuisance rejection and redundant sensor network", International Conference, System Identification and Control Problems, SICPRO'09, pp,786-795, 2009

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

[29] 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.