Nonparametric Kullback-Leibler distance-based method for networks intrusion detection

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

Fouzi Harrou[b] and Ying Sun[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@kaust.edu.sa

Abstract*—Anomaly detection enables identifying atypical events in network systems. Revealing denial of service (DOS) and distributed DOS (DDOS) is a critical security challenge confronting network technologies. This work advocates using Kullback-Leibler distance (KLD) to track DOS and DDOS flooding attacks, including SYN flood, UDP flood, and Smurf attacks. The proposed mechanism's key novelty is the amalgamation of the desirable characteristics of KLD with the sensitivity of an exponential smoothing algorithm. Notably, the use of exponentially smoothing is expected to improve the detector sensitivity to small anomalies. Besides, the proposed mechanism does not need knowledge about data distribution. Meanwhile, kernel density estimation usage to set a threshold for ES-KLD decision statistic improves the flexibility of the proposed mechanism. Tests on the publicly available DARPA99 dataset showing enhanced outputs of the developed approach in detecting cyber-attacks compared to other traditional monitoring procedures.

Keywords*—KL divergence, anomaly detection, SYN flood, UDP flood, Smurf.

I. INTRODUCTION

Over the past two decades, the emergence of information technology and communication systems (ICT) has significantly changed how information is accessed and communicated, mainly via IP (Internet Protocol) networks. This evolution has also led to society's dependence on information storage, processing, and sharing systems. The range of the supported services is in continuous growth, including a plethora of applications of connected objects (Internet of Things) and the management of sensitive systems and critical infrastructures [1]. Thus malfunctions in these systems can cause serious inconvenience, loss of productivity, economic burden, or even severe and irreparable damages. All over the years, critical industrial systems suffer significantly from cyber-attacks [2]. Essentially, anomalies in cyber systems are usually stemmed from intentionally malicious activities initiated by cyber attackers to dismantle the CIA (Confidentiality, Integrity, and Availability) triangle. DOS and DDOS attacks still among the significant menaces to different network architectures. They implement potent mechanisms and try to temporarily or even permanently interrupt the services of the targeted ICT system.

Accurately detecting cyber-attacks at an early stage in critical industrial systems is undoubtedly indispensable in improving their safety and productivity. Moreover, cyber-attacks detection is central to maintaining effective process operations and avoiding expensive maintenance [3-4]. Thus, numerous intrusion detection procedures have been developed in the literature. For instance, in [5], an IDS is proposed to detect DDOS attacks against HTTP servers using Bayesian networks. However, such a system can deal only with slow and restricted types of DDOS attacks. In [6], Virtual machines with the Barnyard tool are considered to reveal potential attacks in the cloud computing environment. It has been shown that with this solution, unregistered attacks cannot be detected. In [7], the authors employed entropy and granular computing to select the most relevant attributes to reveal DOS attacks effectively. However, the decision threshold is not clearly defined. In [8], a Support Vector Machine-based mechanism is adopted to identify ICMPv6 router advertisement DOS attacks. This mechanism is limited by the use of inappropriate attributes for the studied attacks. In [9], they focused on the DOS attacks in SDN networks by using an adequate setting of the timeout value and control plane bandwidth. However, the considered settings are ineffective when the network is under DDOS attacks. In [10], a deep learning detection scheme called TSDL (Two-Stage Deep Learning) based on stacked auto-encoders, and a soft-max classifier is introduced for cyber-attacks detection. In [11-12], statistical detection mechanisms relying on the continuous ranked probability score (CRPS) metric are proposed to distinguish several patterns of DOS and DDOS attacks. It has been shown that CRPS-based detectors have a promising performance to be used for online detection.

This work introduces an effective detector relying on KLD to identify DOS and DDOS attacks [13]. Notably, we exploit the high performance of KLD in quantifying the deviations from a reference probability distribution. Intuitively, values closer to zeros are expected for attack-free traffics and vice-versa. Then, the KLD measurements are exponentially smoothed (ES) to achieve higher detection rates. In the proposed system, to obtain a robust and adaptive ES-KLD scheme, the kernel density estimation (KDE) is employed to establish a nonparametric detection threshold of the ES-KLD. Several metrics of effectiveness are calculated to verify the performance of the ES-KLD, namely true positive rate (TPR), false-positive rate (FPR), accuracy, and AUC. Attack-free and abnormal traffic from the DARPA99 dataset are used to assess the performance of the designed method.

In Section II, we discuss the proposed procedure to detect DOS and DDOS attacks. Section III illustrates the obtained

experimental results. Finally, conclusions and future directions are highlighted in section IV.

II. ES-KLD DETECTION PROCEDURE

KLD is one of the most important information theory metrics. It is often employed to calculate the difference between two probability distributions. Precisely, between two Gaussian distributions $p_1 \sim \mathcal{N}(\mu_0, \sigma_0)$ and $p_2 \sim \mathcal{N}(\mu_1, \sigma_1)$, that have respectively means μ_0 and μ_1 and variances σ_0^2 and, σ_1^2, the KLD distance can be defined by the following formula [14]:

$$KLD(p_1 \backslash\backslash p_2) = \frac{1}{\sigma_0\sqrt{2\pi}} \int exp\left(\frac{(x-\mu_0)^2}{2\sigma_0^2}\right) \left[\log\frac{\sigma_1}{\sigma_0} - \frac{(x-\mu_0)^2}{2\sigma_0^2} + \frac{(x-\mu_1)^2}{2\sigma_1^2}\right] dx$$
$$= \frac{(\mu_1-\mu_0)^2}{2\sigma_1^2} + \frac{1}{2}\left(\log\frac{\sigma_1^2}{\sigma_0^2} + \frac{\sigma_0^2}{\sigma_1^2} - 1\right) \quad (1)$$

From (1), it is clear that the KLD metric takes small values for two similar distributions. On the other hand, large values will be recorded when the compared distributions are too different. Hence, KLD measurements can be exploited for anomaly-based DOS and DDOS attacks detection. First, traffic characteristics during attacks are too different from those of normal traffic, leading to increased KLD values. Then, to enhance the detection rate, we proceed with the exponential smoothing of the KLD measurements produced.

For each relevant measurement x_i in the captured traffic, we calculate the corresponding KLD value d_i using (1):

$$KLD = [d_1 \cdots d_n] \quad (2)$$

Then, the ES-KLD statistic will be computed as:

$$z_t^{KLD} = \nu d_t + (1-\nu) z_{t-1}^{KLD}, \quad (3)$$

where z_0^{KLD} is the anomaly-free mean of KLD vector, μ_0^{KLD}. $\nu (0 < \nu \leq 1)$ is the smoothing parameter.

Equation (3) can be expressed recursively as:

$$z_t^{KLD} = \nu \sum_{t=1}^{n} (1-\nu)^{n-t} d_t + (1-\nu)^n d_0, \quad (4)$$

Then, we utilize KDE to estimate the underlying probability density distribution (PDF). For ES-KLD z_t^{KLD} measurements, the estimated nonparametric PDF will be [15]:

$$p(z_t^{KLD}) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{z_t^{KLD} - z_i^{KLD}}{h}\right), \quad (5)$$

where z_i^{KLD} is the ith ES-KLD value. K refers to the kernel function [16]. h represents the smoothing bandwidth factor that determines the probability estimation quality. For n observations with the standard deviation σ, the optimal choice of h can be obtained from the following expression [17]: $h = 1.06\ \sigma n^{-0.2}$.

Finally, the (1-α)-th quantile of $p(z_t^{KLD})$defines the nonparametric detection threshold. Hence, attacks are spotted when the ES-KLD decision function overpass such threshold.

The overall KLD-ES procedure can be recapitulated as follow:

Phase I: Data preparation

Step 1: create relevant features measurements x_i

Step 2: Apply Z-Score transformation to relevant features measurements to get a mean of zero and variance of unity.

Phase II: Calculating ES-KLD sequences

Step 1: For each measurement x_i from the audited data, calculate KLD value d_i , KLD $= [d_1 \cdots d_n]$ as in equation (1).

Step 2: Calculate the ES-KLD values z_t^{KLD} as in equation (3): $z_t^{KLD} = \nu d_t + (1-\nu) z_{t-1}^{KLD}$,

Phase III: Attacks detection

Step 1: Estimate the PDF of z_t^{KLD} vector using KDE as follow:

$$p(z_t^{KLD}) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{z_t^{KLD} - z_i^{KLD}}{h}\right),$$

Step 2: Set the nonparametric detection threshold h_{kld} as the $(1-\alpha)$-th quantile of $p(z_t^{KLD})$. The trapezoidal rule is applied to compute the integration in the following equation:

$$h_{kld} = F_h\left(Z^{-1}(1-\alpha)\right)$$

Step 3: If $z_t^{KLD} > h_{kld}$ it is an anomalous traffic measurement, attack DOS/DDOS in progress.

III. EXPERIMENT RESULTS

We validate the ES-KLD method under different forms of DOS and DDOS attacks, namely the SYN flood, UDP flood, and Smurf attacks. SYN flood attacks are based on the TCP protocol (Transmission Control Protocol). As illustrated in Fig.1 (b), such an attack consists of inundating the victim with a massive flow of SYN segments forcing it to keep all memory resources in use, which denies access to legitimate clients [18]. In the UDP flood, the attacker uses the UDP (User Datagram Protocol) datagrams to overwhelm the victim, generally using a random port [19]. Smurf attack exploits the ICMP protocol. To perform this attack (Fig. 2), the attacker spoofs the victim's IP addressee to broadcast many ICMP Echo Request messages within a large network. In response, a massive flow of Echo-Reply messages will be returned to the victim, which exhausts its resources and turn it out of service [20].

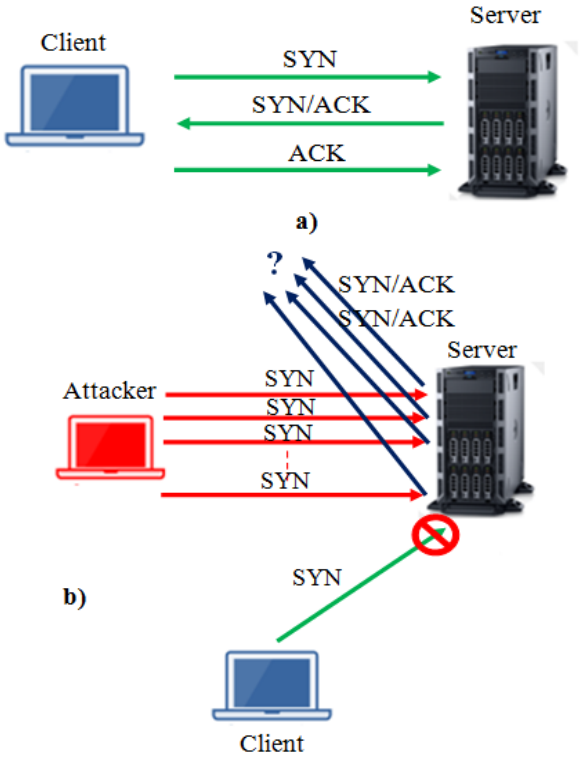

Fig. 1. Normal TCP connection (a), and SYN flood attack (b).

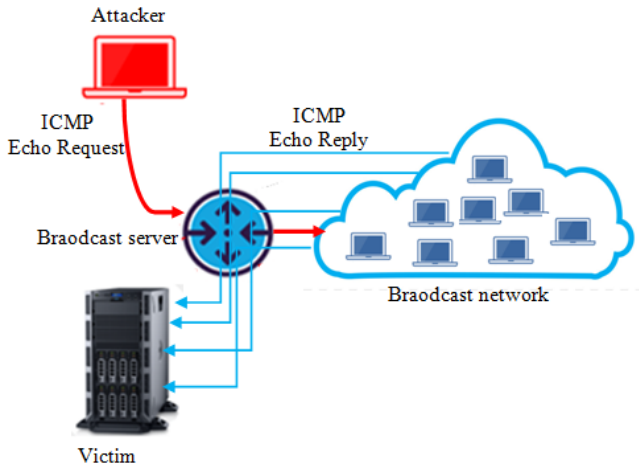

Fig. 2. Example of a Smurf attack.

The performances of the ES-KLD method are assessed using the DARPA99 dataset [21]. It comprises a considerable trace of IP network traffic. The normal data corresponds to three weeks of anomaly-free traffic, and the anomalous data consists of two weeks of traffics with different types of attacks.

The DARPA99 dataset provides different forms of DOS flooding attacks, including TCP SYN flood, UDP flood, and ICMP Smurf attacks, tabulated in Table 1.

TABLE 1. DOS ATTACKS CHARACTERISTICS IN THE DARPA99 DATASET

Attack		Week	Day	Instant of occurrence	Duration
TCP SYN flood	Attack 1	5	1	18:04:04	6mn51s
	Attack 2	5	2	11:48:42	1s
	Attack 3	5	2	18:16:05	3mn26s
UDP flood	Attack 1	5	1	20:00:27	15mn
	Attack 2	5	1	20:00:27	15mn
ICMP Smurf	Attack 1	4	1	21:34:16	1s
	Attack 2	4	1	21:34:26	1s
	Attack 3	4	3	18:29:25	1s
	Attack 4	4	5	08:45:18	2s
	Attack 5	5	1	09:33:00	2mn

Figures 4, 5, and 6 show the proposed ES-KLD method's performances in terms of TPR, FPR, accuracy, and AUC.

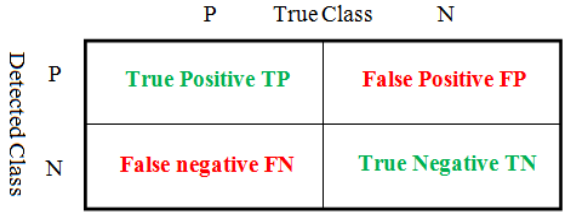

Fig. 3. The confusion matrix

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \quad (6)$$

$$FPR = \frac{FP}{FP + TN} \quad (7)$$

$$TPR = \frac{TP}{TP + FN} \quad (8)$$

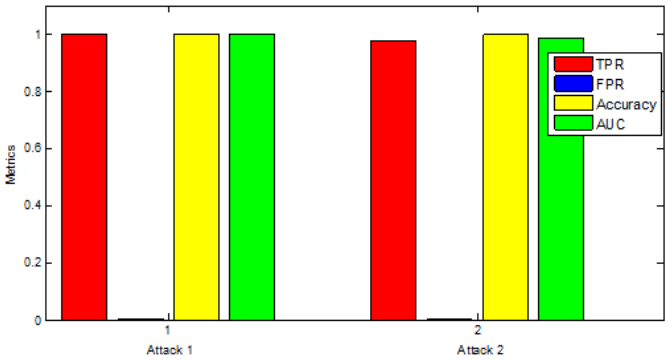

Fig. 4. ES-KLD performances under SYN flood attaks

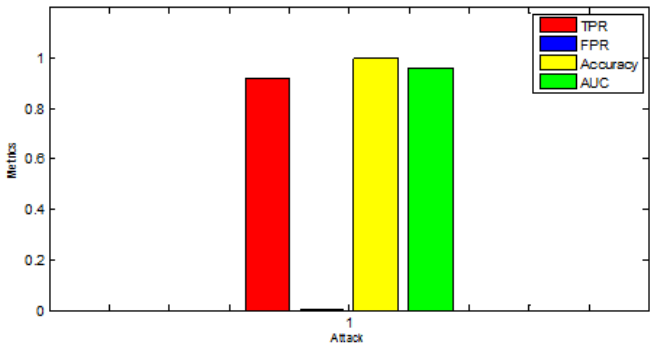

Fig. 5. ES-KLD performances under UDP flood attak

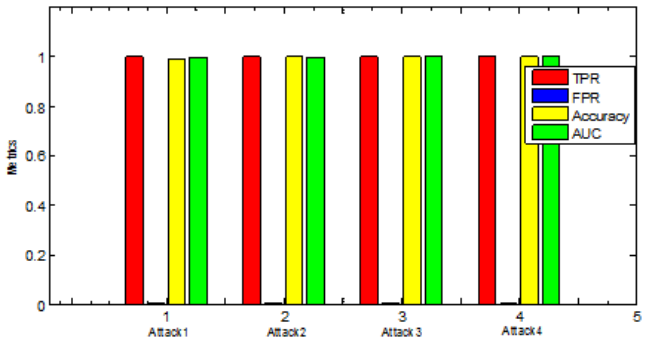

Fig. 6. ES-KLD performances under Smurf attaks

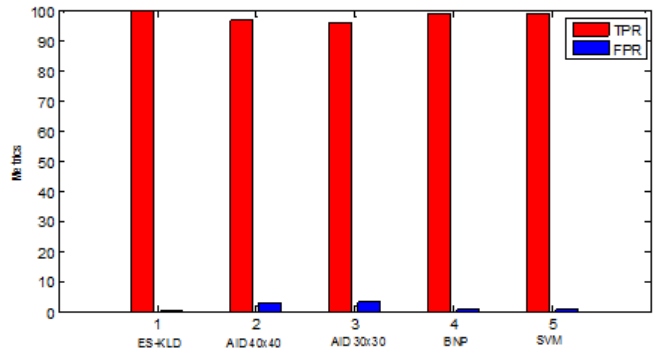

Fig. 7. Comparaison with some DOS detection appraoches under DARPA 99 TCP SYN flood attacks

The results reported in Figures 4-6 confirm the ES-KLD method's efficiency to distinguish SYN flood, UDP flood, and Smurf DOS/DDOS attacks with high TPR and small FPR.

Moreover, Figure 7 plots the ES-KLD mechanism performances versus those of some recently released schemes, which are AID [22], BPN [20], and SVM [23], during TCP SYN floods. As the figure illustrates, ES-KLD has allowed the highest detection performances, outperforming the other detection procedures.

IV. Conclusion

This paper presents a statistical detector to track down DOS and DDOS flooding attacks based on the KLD metric. The method essentially uses the exponentially smoothing KLD measurements (ES-KLD) metric to compute the mismatch of anomalous traffics from the reference (attack-free) traffic. Attacks are detected if the ES-KLD statistic exceeds the detection threshold, which has been nonparametrically fixed using KDE. The advantage of the ES-KLD detector consists of its flexibility and assumption-free. The ES-KLD method is applied to detect TCP SYN flood, UDP flood, and ICMP Smurf attacks included in the DARPA99 dataset traffics. Results demonstrate the high performances of ES-KLD compared to the traditional methods.

Insight of these promising detection results of ES-KLD, in future work, we plan investigating other types of DDOS attacks, such as low rate DOS and DDOS (LR-DOS/DDOS) attacks. In a future study, we also plan to develop efficient attack detection methods based on deep learning models, which have shown good performance in different areas to enhance detection performance [24-25].

Acknowledgement

This publication is based upon work supported by King Abdullah University of Science and Technology (KAUST), Office of Sponsored Research (OSR) under Award No: OSR-2019-CRG7-3800. 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] S. Bhatia, S. Behal, and I. Ahmed, “Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions, ” Versatile Cybersecurity, Advances in Information Security 72, Springer, 2018.

[2] M. Thottan, and C.Ji, “Anomaly Detection in IP Networks, ”IEEE transactions on signal processing, vol. 51, no. 8, august 2003.

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

[4] F. Harrou, . Bouyeddou, Y. Sun, and B. Kadri, 2018, November. A Method to Detect DOS and DDOS Attacks based on Generalized Likelihood Ratio Test. In 2018 International Conference on Applied Smart Systems (ICASS) (pp. 1-6). IEEE.

[5] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna, and R. Mahajan, ”Detection of DoS/DDoS attack against HTTP servers using naive Bayesian," International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 280-285, 2015.

[6] A. M. Lonea, D.E. Popescu, O. Prostean, and H, Tianfield,” Evalution of experiments on detecting distributed denial of service(DDoS) attacks in eucalyptus private cloud,”Soft Computing applications, vol 195, pp 367-379, 2013.

[7] S. Khan, A. Gani, A. W. Wahab, and P. K. Singh,”Features selecion of denial of Service Attacks using entropy and granular computing,” Arabian Journal for Science and Engineering, vol. 43, pp 499-508, 2018.

[8] M. Anbar, , A Machine Learning Approach to Detect Router Advertisement Flooding Attacks in Next-Generation IPv6 Networks,” Cognitive Computation, vol. 10, pp. 201–214, 2018

[9] R. Kandoi, M. Antikainen,”Denial of service attacks in openflow SDN networks,” IFIP/IEEE International Symposium on integrated network management(IM), pp. 1322-1326, 2015.

[10] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, “TSDL: A twostage deep learning model for efficient network intrusion detection,” IEEE Access, vol. 7, pp. 30373-30385, 2019.

[11] F. Harrou, B. Bouyeddou, Y. Sun, and B. Kadri,” Detecting cyber-attacks using a CRPS-based monitoring approach,” IEEE Symposium Series on Computationnal Intelligence (SSCI), pp. 618-622, 2018

[12] B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun,”DDOS-attacks detection using an efficient measurement-based statistical mechanism,” Engineering Science and Technology, an International Journal, vol.23(4), pp 870–878, 2020.

[13] S.Kullback, and R. A. Leibler,” On information and siffiency,” Annals of Matimatical statistics, vol, 22(1), pp. 79-86, 1951

[14] L.Pardo, “Statistical inference based on divergence measures”, Chapman and Hall/CRC, 2005.

[15] E.Martin, A.Morris,”Non-parametric confidence bounds for process performance monitoring charts”, Journal of Process Control, vol 6, pp 349–358, 1996.

[16] Y.C.Chen,”A tutorial on kernel density estimation and recent advances”, Biostatistics and Epidemiology, vol1, pp161–187, 2017.

[17] A.R.Mugdadi, I.A.Ahmad, “A bandwidth selection for kernel density estimation of functions of random variables,” Computational Statistics and Data Analysis, vol 47, pp 49–62, 2004.

[18] M.Bogdanoski, T.Suminoski, A.Risteski, “Analysis of the SYN flood DoS attack”, International Journal of Computer Network and Information Security, vol 5, pp 1–11, 2013.

[19] M. Aijaz, and S. Parveen, “Analysis of DoS and DDoS Attacks”, International Journal of Emerging Research in Management and Technology,vol. 5, no. 5, 2016.

[20] O.E.Elejla, M.Anbar, B.Belaton,”ICMPv6-based DoS and DDoS attacks and defense mechanisms”, IETE Technical Review, vol 34, pp390–407, 2017.

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

[22] J.Zheng, M.Hu, “An anomaly intrusion detection system based on vector quantization”, IEICE transactions on information and systems, vol 89, pp 201–210, 2006.

[23] C.D.McDermott,”Petrovski, A.: Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks”, international journal of computer networks and communications, vol 9, pp 45-56, 2017.

[24] Harrou, F., Hittawe, M.M., Sun, Y. and Beya, O., 2020. Malicious attacks detection in crowded areas using deep learning-based approach. IEEE Instrumentation & Measurement Magazine, 23(5), pp.57-62.

[25] Zeroual, A., Harrou, F., Dairi, A. and Sun, Y., 2020. Deep learning methods for forecasting COVID-19 time-Series data: A Comparative study. Chaos, Solitons & Fractals, 140, p.110121.