HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology,
an International Journal

journal homepage: www.elsevier.com/locate/jestch

Full Length Article

DDOS-attacks detection using an efficient measurement-based statistical mechanism

Benamar Bouyeddou [a,*], Benamar Kadri [a], Fouzi Harrou [b,*], Ying Sun [b]

[a] STIC Lab., Department of Telecommunications, Abou Bekr Belkaid University, Tlemcen, Algeria
[b] King Abdullah University of Science and Technology (KAUST) Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, Thuwal 23955-6900, Saudi Arabia

ARTICLE INFO

Article history:
Received 16 June 2019
Revised 19 March 2020
Accepted 8 May 2020
Available online 9 June 2020

Keywords:
TCP SYN flood
Smurf attack
ICMPv6_based DOS
CRPS metric
Anomaly detection

ABSTRACT

A monitoring mechanism is vital for detecting malicious attacks against cyber systems. Detecting denial of service (DOS) and distributed DOS (DDOS) is one of the most important security challenges facing network technologies. This paper introduces a reliable detection mechanism based on the continuous ranked probability score (CRPS) statistical metric and exponentially smoothing (ES) scheme for enabling efficient detection of DOS and DDOS attacks. In this regard, the CRPS is used to quantify the dissimilarity between a new observation and the distribution of normal traffic. The ES scheme, which is sensitive in detecting small changes, is applied to CRPS measurements for anomaly detection. Moreover, in CRPS-ES approach, a nonparametric decision threshold computed via kernel density estimation is used to suitably detect anomalies. Tests on three publically available datasets proclaim the efficiency of the proposed mechanism in detecting cyber-attacks.

1. Introduction

With the continuous evolution of the internet, several networks technologies have been developed including the internet of things [1,2] and software-defined networks [3,4]. However, these cyber systems are permanently subjected to attacks from external intruders that degrade their performance and prevent stakeholders from relevant information. Thus, a monitoring mechanism is vital for detecting malicious attacks against cyber systems. To this end, anomaly detection-based solutions that are already deployed on board of many systems (e.g., fraud detection, medicine, and industry) are offering relevant information to help provide real-time anomaly detection [5–7].

Malicious attackers can target individuals, companies and public institutions [8] (Fig. 1). Fig. 1 gives the distribution of targets in January 2019. It can be seen that a large number of attacks target single individuals (35.71%), before multiple targets (11.11%) and healthcare (9.52%).

All over the years, denial and distributed denial of service (DOS and DDOS) cyber-attacks increase continuously to become today one of the most challenging threats to networks technologies [9–11]. In such attacks, to suspend legal traffic, hacker compromises thousands of hosts that can include computers, servers, and IOT equipments, and then exploits them simultaneously to overload the victim's resources by a large amount of traffic (Fig. 2). Therefore, there is a need for automatic detection mechanisms to guarantee an appropriate level of quality of service and detect malicious attacks.

All over the years, several detection mechanisms have been developed to protect networks against different types of attacks (i.e., internal and external attacks) [12]. In [13], a rank correlation technique is proposed to detect Distributed Reflection Denial of Dervice (DRDoS attack) attacks. This approach is based on the assumption that the responsive flows from reflectors converging to the victim are linearly autocorrelated. Here, Spearman's rank correlation coefficient is used to filter the DRDoS attack. In [14], botnets were detected using a mixed distributed centralized network traffic capture. The efficiency of this approach depends on host collectors which can themselves be compromised. In [15], an approach based on Kullback-Leibler distance is proposed to identify malicious traffics responsible for potential DDoS attacks. However, this approach requires a full collaboration between different ISPs routers. Also, the decision threshold used to differentiate normal and abnormal traffics is fixed manually. In [16], a detection procedure is proposed to prevent the low rate TCP-based DOS attacks at edge routers using TCP Retransmission Timeout (RTO) and round-trip time (RTT) properties. In this detection

[*] Corresponding authors.
E-mail addresses: bouben81@yahoo.fr (B. Bouyeddou), fouzi.harrou@kaust.edu.sa (F. Harrou).

Peer review under responsibility of Karabuk University.

https://doi.org/10.1016/j.jestch.2020.05.002
2215-0986/© 2020 Karabuk University. Publishing services by Elsevier B.V.

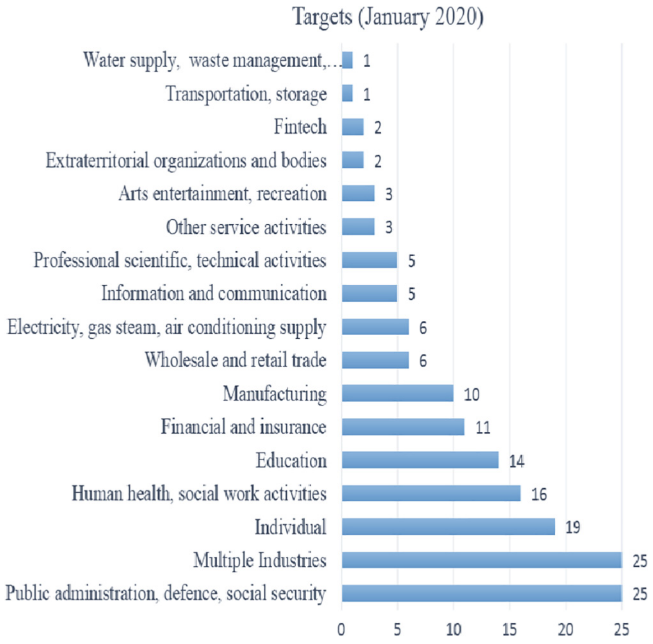

Fig. 1. Cyber-attack's targets in January 2020 [8].

system, routers are asked to perform these extrinsic functions and as a result, their performances can be strongly affected. In [17], an autoregressive integrated moving average model is constructed to discriminate the normal traffic from DoS and DDoS attacks for IP networks. Then, the local Lyapunov exponent is computed for the ratio between the number of packets and the number of IP sources and then used as an indicator from malicious traffic type. In [18], a min-cut set DDOS detection method is proposed based on the quality of service degradation measurements. However, such a strategy can fail recurrently to distinguish DDOS attacks from high traffic normal situations. Sahoo et al. [19] targeted DDOS attack against Software Defined Networks using the general entropy (GE) and other information distances (ID). However, the implementation of this approach requires normal traffics and manual detection thresholds. Zhang et al. [20] applied Kullback-Leibler divergence to detect the stealthy deception attacks in a cyber-physical system. However, this detection algorithm is designed based on the assumption that the inspected traffics are Gaussian distributed and the detection decision is based on a prefixed threshold. In [21], Zulkiflee et al. applied the Support Vector Machine (SVM) algorithm to the detection of router advertisement flooding DOS attacks. Unfortunately, limited attack characteristics can be provided using the SVM algorithm. In [22], the authors suggested a fuzzy logic-based technique to reveal SYN flooding attacks. However, the efficiency of this method is relying on the presence of expert knowledge. In [23], the Back-propagation neural network was proposed as an IPv6 based attack detection approach. Recently, deep learning-based methods turn out to play an important role in the literature for design intrusion detection systems [24–26]. For instance, in [24], a deep learning-based approach merging sparse autoencoder with SVM has been introduced for intrusion detection. In [25], a coupled method using hybrid spectral clustering and deep neural network ensemble algorithm has been proposed for intrusion detection. Such machine learning methods depend on the availability of input data, and their implementation is no easy task, especially for real-time applications.

Detecting DOS and DDOS is one of the most important security challenges facing network technologies [46]. Essentially, the abovementioned anomaly-based DOS and DDOS detections approaches have been partially or totally designed using distribution-based metrics, such as Kullback-Leibler divergence and general entropy. Nevertheless, these detection methods are generally based on the assumption that the distribution underlying the traffic network is Gaussian. Thus, these detection approaches provide suitable detections only if the traffic network data follows a normal distribution. However, traffic data from computer networks have generally non-Gaussian distribution. Generally speaking, violation of normality assumption can lead to a high false alarms rate [27]. Their second important limitation concerns the detection threshold that is either not used or manually predefined. In addition, these techniques are distribution-based and need a large dataset to accurately detect attacks, which makes them ineffective for online detection.

This paper introduces an innovative detection mechanism based on the continuous ranked probability score (CRPS) statistical metric and exponentially smoothing (ES) scheme for enabling efficient detection of DOS and DDOS attacks. Indeed, CRPS has been largely exploited in evaluating the quality of probabilistic forecast-

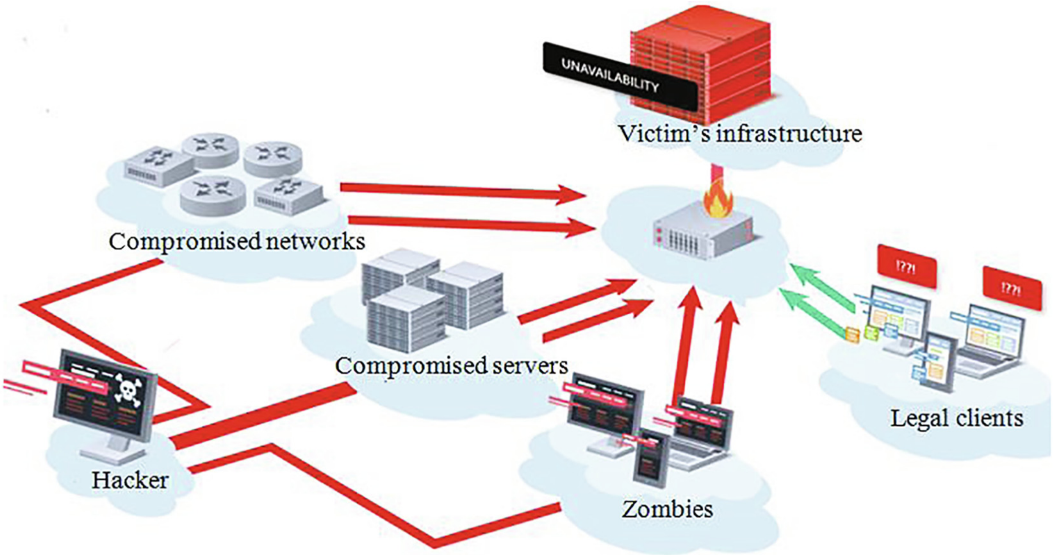

Fig. 2. General illustration of a cyber-attack.

ing [27]. In this regard, the CRPS is used to quantify the dissimilarity between a new observation and the distribution of normal traffic. Specifically, to detect the DOS and DDOS attacks, using CRPS-based approach, every new traffic network measure is compared to the reference attack free traffic distribution. This makes CRPS a suitable measure for real-time application compared to other distributional metrics like the χ^2 and the Kullback-Leibler which require the whole a priori data to be available to compute distributions of anomaly-free training and testing data. Till now, CRPS metric, however, has not been utilized in improving the detection of malicious DOS and DDOS attacks. Here, to enhance the detection efficiency, an exponential smoothing (ES) procedure is applied to the CRPS measurements. The major reason for exponentially smoothing CRPS measurements (CRPS-ES) is to include information from previous and current measurements in the decision process, which makes it efficient for uncovering small anomalies. Moreover, in CRPS-ES approach, a nonparametric decision threshold computed via kernel density estimation is used to suitably detect anomalies. Tests on two publically available datasets proclaim the capacity of the proposed method in uncovering cyber-attacks.

Motivated by the suitable performances of CRPS metric and to fix the aforementioned problems, we have designed the CRPS-ES mechanism with the following characteristics:

- There is no assumption about the normality of data and a more realistic estimation of traffic distribution is proposed. Specifically, we applied the kernel density estimation (KDE) to nonparametrically estimate the distribution underlying the CRPS-ES statistic.
- Attack detection is based on an automatic and nonparametric threshold. Here, ES is applied to CRPS measurements to set the detection threshold for uncovering attacks. CRPS-ES scheme considers the past data in the detection statistics which makes it sensitive to incipient attacks. Attacks are declared if the CRPS-ES measurements between the test traffic and the normal traffic exceed the detection threshold (Eq. (5)).
- CRPS-ES is more appropriate for real-time detection. Unlike the abovecited techniques, in the CRPS-ES mechanism, only the new traffic measurement is compared to the attack-free traffic distribution which makes it appropriate for real-time monitoring.
- Additionally, CRPS-ES is a protocol and network free method. This means that it can be applied to detect different types of flooding DOS and DDOS attacks and in all kinds of networks. Different flows can be separated and monitored independently according to the messages and protocols they include.

Next Section presents the proposed CRPS-ES-based anomaly detection mechanism. Section 3 verifies the effectiveness of the proposed method in detecting different DOS and DDOS attacks using two datasets. Finally, conclusions are given in Section 4.

2. The proposed anomaly detection mechanism

The CRPS metric has been broadly employed in probabilistic forecasting to verify the precision of forecasting [28]. It considers both the sharpness and accuracy of forecasting in the assessment of the forecasting precision. The desirable characteristic of CRPS is its ability in comparing a full distribution with an observation which makes it suitable for online anomaly detection. Basically, for detecting DOS and DDOS attacks using CRPS metric, every new traffic network measurement will be compared to the reference attack-free traffic distribution. Due to its sensitivity to changes, the CRPS is appropriate in quantifying the deviation of attacks from the normal traffic. Large values of CRPS reflect the presence of potential attacks in the monitored traffic.

For an observation × and the CDF, F of a probabilistic forecast variable, the CRPS distance is defined as [28–29]:

$$CRPS(F,x) = \int_{-\infty}^{\infty} (F(y) - 1\{y \geqslant x\})^2 \, dy \tag{1}$$

where $1\{y \geq x\}$ is the indicative function:

$$1(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \tag{2}$$

An illustration of the core idea of CRPS metric is given in Fig. 3. Fig. 3 presents the CDFs for the new observation and anomaly-free measurements. The CRPS represents the green colored area (Fig. 3).

It should be noted that when the distribution of attack-free traffic is Gaussian with mean μ and variance σ^2, CRPS has the following analytical formula [29–30],

$$CRPS(\mathcal{N}(\mu,\sigma^2),x) = \sigma\left[\frac{x-\sigma}{\sigma}\left(2\Phi\left(\frac{x-\sigma}{\sigma}\right)-1\right)+2\phi\left(\frac{x-\sigma}{\sigma}\right)-\frac{1}{\sqrt{\pi}}\right] \tag{3}$$

whereϕ and Φ represent the Gaussian probability density function and cumulative density function, respectively.

In fact, CRPS with small values close to zero refers to normal traffic. However, it is clear that the CRPS metric significantly grows during attacks. This fact makes the CRPS metric useful as an indicator to detect malicious attacks. Then, an exponential smoothing (ES) [31] scheme is applied to CRPS measurements to establish a decision threshold and flag the presence of attack traffics. In other words, in the proposed CRPS-ES mechanism CRPS sequences are exponentially smoothed to further improve its sensitivity to abnormal events (attacks). To do so, according to the targeted attack, the traffic's features (e.g., number of bytes, number of packets, and IP address) are used as the input variable of the CRPS-ES mechanism. Precisely, to detect SYN flood, Smurf and ICMPv6-based attacks, we applied CRPS-ES to the number of the SYN segments, ICMPv4 Echo reply and ICMPv6 messages received per sampling, respectively.

Let's define the sequence of CRPS measurements as computed in (1): CRPS = [d1… dn]. The ES-CRPS statistic is computed as:

$$z_t^{CRPS} = \upsilon d_t + (1-\upsilon) z_{t-1}^{CRPS} \tag{4}$$

where the initial value, Z_0^{CRPS} is the anomaly-free mean of CRPS vector, μ_0^{CRPS} . $(0 < v \preccurlyeq 1)$ is a forgetting parameter.

The CRPS-ES fault detection threshold is designed as [27],

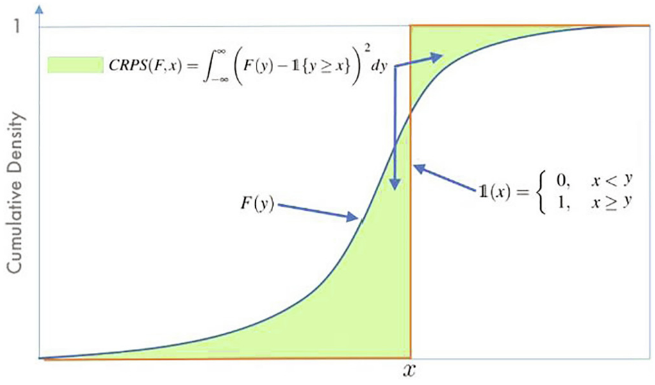

Fig. 3. A representative example of CRPS metric between an observation and CDF of reference data. CRPS(F; x) is the area delimited by 1(x) and F(y).

$$h_{ES} = \mu_0^{CRPS} + L\sigma_0^{CRPS}\sqrt{\frac{\nu}{(2-\upsilon)}}\left[1-(1-\nu)^{2t}\right], \tag{5}$$

where L denotes the width of the decision threshold.

It should be noticed that the parametric threshold in CRPS-ES scheme is calculated based on the normality assumption of the traffic data. However, the normality assumption of traffic data is not valid mainly due to the dynamic characteristics of network traffic. When the Gaussian assumption is not verified, the monitoring results would be inappropriate. To alleviate this problem, the distribution of CRPS-ES statistic could be estimated by using the kernel density estimation (KDE) [32], which is a nonparametric probability density estimation approach. In this approach, first, the distribution of the CRPS-ES statistic in Eq. (4) is estimated via univariate KDE using attack-free data. Around a point xi, the KDE is formulated as follow [32]:

$$\widehat{f}(x) = \frac{1}{nH}K\frac{(x-x_i)}{H} \tag{6}$$

where K is the kernel function, here the Gaussian kernel is used. n is the number of measurements; x is the considered data points. H is the kernel smoothing bandwidth which determines the estimation quality; its optimal value can be computed as following [33]:

$$H = 1.06\sigma n^{-0.2} \tag{7}$$

Then, the nonparametric threshold of the CRPS-ES mechanism is defined as the$(1-\alpha)$-th quantile of the estimated distribution. An anomaly is flagged when the CRPS-ES statistic exceeds the decision threshold.

The designed CRPS-ES scheme is briefly outlined next.

- **Step 1:** For every observation x_i in the testing dataset, compute the CRPS sequences.
- **Step 2:** Compute the CRPS-ES sequences based on Equation (4).
- **Step 3:** Estimate the distribution underlying CRPS-ES sequences via KDE.
- **Step 4:** From the distribution of CRPS-ES, we determine the threshold of CRPS-ES mechanism in a nonparametric way as the(1-α)-th quantile of the estimated distribution of CRPS-ES distances computed by KDE.
- **Step 5:** An attack is declared when the CRPS-ES statistic exceeds the detection threshold.

Overall, in the designed CRPS-ES-based anomaly detection strategy, firstly, different features (e.g., TCP segment, IP address, and ICMP messages) are extracted from the gathered network traffic according to the targeted attacks. Then, attack-free training data are used as input to the exponentially smoothed CRPS (CRPS-ES) metric. The detection threshold is computed non-parametrically based on the estimated CRPS-ES distribution using KDE. Next, to reveal DOS and DDOS attack that could be present in the tested traffic, the CRPS-ES values are continuously compared to the detection threshold previously calculated. Normal traffic in all observation is detected by CRPS-ES down to its detection limit. Abnormal traffic and eventually the presence of DOS and DDOS attack are all observation detected above the CRPS-ES threshold. The conceptual schematic of the proposed CRPS-ES mechanism is displayed in Fig. 4.

The designed CRPS-ES detection mechanism will be used to monitor DOS and DDOS attacks. Note that these types of attacks are still performed against the majority of actual networks and it is expected to persist with future technologies. For instance, by generating a very large number of half-open connections TCP SYN flooding attacks overload the victim server's memory resources, which make it unable to treat new connections [34]. On another hand, Smurf attack uses the pinging tool under both versions of the ICMP protocol (i.e., ICMPv4 and ICMPv6) [35–37]. It aims to overwhelm the victim with large traffic of Echo-Reply messages. Precisely, based on the victim's address, the attacker pings via a broadcast server all hosts that are located in the broadcast domain. As a result, all replies of these hosts will be redirected to the victim. Also, ICMPv6 can be exploited in different ways to perform DOS and DDOS attacks, such as invalidate the present configuration, unlimited demand for information and proposing new invalid links continuously with the neighbor advertisement, neighbor solicitation, and router advertisement messages, respectively [36].

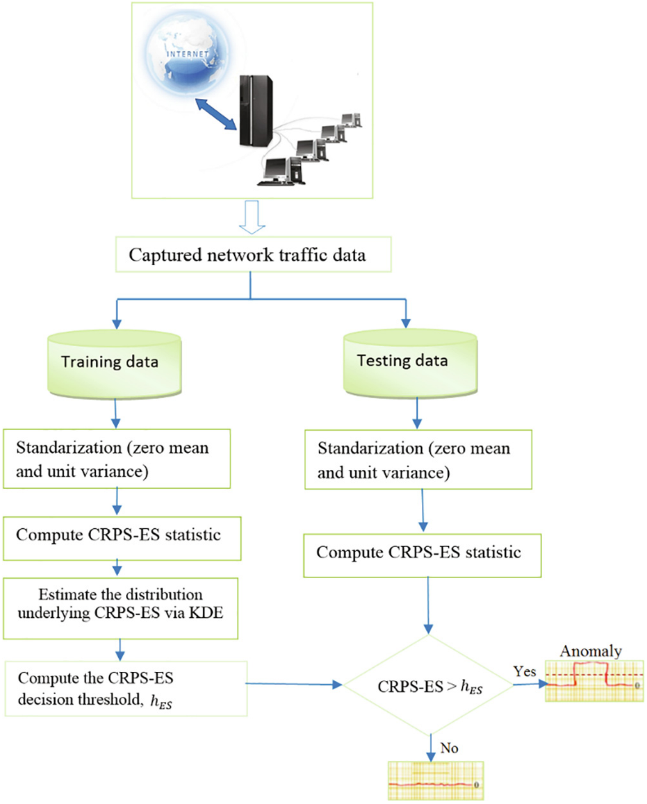
INTERNET
Captured network traffic data
Training data
Testing data
Standarization (zero mean and unit variance)
Standarization (zero mean and unit variance)
Compute CRPS-ES statistic
Compute CRPS-ES statistic
Estimate the distribution underlying CRPS-ES via KDE
Compute the CRPS-ES decision threshold, h_{ES}
CRPS-ES > h_{ES}
Yes
Anomaly
No

Fig. 4. Conceptual schematic of the CRPS-ES detection strategy.

3. Results and discussion

In this section, we evaluate the performance of the CRPS-based detection method. Specifically, we investigate the capacity of CRPS-ES to sense three types of most popular DOS and DDOS attacks which are the TCP SYN flooding, UDP flood, the Smurf attack, and the ICMPv6-based flooding attacks. The monitored network traffics are collected from the DARPA99, MAWI and ICMPv6 datasets.

3.1. DOS and DDOS attacks

TCP SYN flood attacks are still among the highest occurred cyber-attacks. These attacks are often launched by attackers to perform DOS/DDOS and shutdown systems, networks, and servers. TCP SYN flood attacks generate a massive number of half-open connections that exhaust the server's backlog queue and make it incapable to handle new TCP sessions including incoming requests from legitimate clients. Generally, to perform a TCP SYN flood attack, malicious users can either do not send the ACK segment or using a spoofed IP address [38]. A UDP flood DOS attack is created when the attacker sends a datagram to a random port on the target victim which will determine what is listening on the destination port. If the destination port is closed, then it will reply with an ICMP message to the spoofed source IP address reporting the destination port unreachable error. Finally, if enough UDP datagram are sent to closed ports, the victim and even hosts on the same segment will also be out of service due to the related large amount of traffic [39].

The ICMP amplification attacks also known as Smurf attacks are pertinent types of DDOS attacks, which can be based either on ICMPv4 or the ICMPv6 version, menace IPv4 as well as IPv6 technology [40]. Indeed, the Smurf attacks use broadcast servers to overwhelm their victims with a high rate of ICMP Echo-Reply messages. To accomplish such an attack, the attacker starts by spoofing the targeted victim's IP address, then sending ICMP Echo Request messages to the broadcast server which deliver them to all hosts. These last respond with the ICMP Echo-Reply message to the victim's IP address. A broadcast network can contain hundreds of hosts, hence, the victim will be flooded by a whole bunch of Echo-Reply messages that exhaust its resources and turn it out of service. The Neighbor Solicitation flood attacks consist of overload and turn out of service their victims when they trying to serve all neighbor solicitation requests. The Neighbor Advertisement flood attack is another type of DOS attack that is based on the ICMPv6 protocol. During such an attack, the attacker replies all NS messages announcing, continuously, that he already has the requested address. Finally, the Router Advertisement flood attack aims to alterate legitimate client's IP configuration using the ICMPv6 Router Advertisement (RA) messages with the ROUTER LIFETIME field set to 0 [40].

3.2. Detection results using DARPA99 dataset:

In this subsection, the capacity of CRPS-ES mechanism is verified in detecting TCP SYN flooding and Smurf attacks in the network traffic of DARPA99s dataset (www.ll.mit.edu/ideval/data/1999data.html).

In the scenario of a TCP SYN flooding attack, we consider three attacks. The first attack was in week 5, day 1 at 18h04mn04s and lasts 6mn51s. The second occurs in week 5, day 2 and starts at 11h38mn04s and with duration of 13mn41s. The third one occurs, also, in week 5, day 2 and was at 18h16mn05s for 3mn26s. The second scenario concerns the ICMP Smurf attacks. Precisely, we study five ICMP Smurf attacks, which have targeted the same victim during the fourth and fifth weeks. The beginning was with the week 4, in which two attacks of 1 s were initiated on day 1 at 21:34:16 pm and 21:34:26 pm, one attack of 1 s at 18:29:25 pm in day 3 and another attack of 2 s at 08:45:18 am on day 5. Finally, the victim was re-attacked again in week 5, day 1 at 09:33:00 am during 2mn.We refer to all these attacks as WiDi (i.e., Week i Day i) attack. The overall characteristics of such attacks are reported in Table 1. On the other hand, normal or attack-free data are about 1320 records corresponding to 22 h of the traffic network.

To detect TCP SYN flood attacks, the flow of SYN segments received by the victim are inspected. Since the dataset provides the whole network traffic with all exchanges, we have extracted and sampled the number of such segments using Wireshark and MySQL tools. Fig. 5(a) illustrates the detection based on the traffic of W5D1. The results show that the attack happened from records 605 to 611with a rate of 2928 SYN segments per observation time. It is clearly illustrated when the monitored traffic (i.e. traffic W5D1) is free from attacks, the CRPS measurements fall under the detection threshold (h_{es} = 0.7). This means that such traffic has similar behavior to normal attack-free traffic. On the other hand, large values of CRPS statistics are obtained when the inspected traffic includes TCP SYN attacks that are the cause of the detected attacks. During these attacks, the CRPS statistic was around 12 exceeding largely h_{es}. Fig. 5(b) shows the detection capability of the CRPS-ES mechanism in detecting the two attacks occurred on W5D2. In the first attack, the victim was overwhelmed by an average of 3027 SYN/observation time, and in the second attack, the victim was inundated by 10,256 SYN segments at each time instant. In this traffic, the detection threshold h_{es} = 0.51, where the two TCP SYN attacks have increased the CRPS statistics to 9.1 and 5.3, respectively.

The detection results of the CRPS-ES mechanism when applied to the received Echo Reply messages in the case of Smurf attacks are displayed in Fig. 6(a–d). Here, the detection procedure is based on the number of ICMP echo reply messages captured by the victim for each observation time. Fig. 6(a–d) indicates that the proposed algorithm is able to alert immediately all smurf attacks when they have happened. In Fig. 6(a), the victim has been inundated with 51,681 Echo Reply messages (Table 1, Attacks 1 and 2). Such inundation is revealed with CRPS value of 1.2 that is much higher than h_{es} = 0.015. In the Smurf attack occurred on W4D3, the targeted victim has received 4455 Echo Reply messages (Fig. 6(b)); the corresponding CRPS statistic equals 7, which clearly exceeds h_{es}. In the Smurf attack of W4D5 traffic (Fig. 6(c)), 4453 Echo Reply messages were simultaneously sent to the victim. In this case, Smurf attack is characterized by a CRPS statistic of 4. Finally, two attacks have been identified in the W5D1 traffic (Fig. 6(d)) by the proposed algorithm. The first attack targeted the victim at the instance 570 with 6000 (CRPS statistic = 3) Echo Reply messages, and the second attack was against the victim at the instance 1914 with 2655 (CRPS statistic = 1.2) Echo Reply messages.

In both scenarios, the detection threshold has small values, (h_{es} = 0.7) in the case of TCP SYN flood and (h_{es} = 0.51) for Smurf attack. In practice, this reflects the high sensitivity of the CRPS-ES mechanism. With such values, small, even very small, changes in traffic behavior can be revealed. This is a suitable characteristic, allows to CRPS-ES to deal with low to very low modern DOS and DDOS attacks (low rate DOS).

Table 1
DARPA99′s TCP SYN flooding and Smurf attacks characteristics.

Attack		Week	Day	Time of appearance	Duration
TCP SYN flood	Attack 1	5	1	18:04:04	6 mn 51 s
	Attack 2	5	2	11:48:42	1 s
	Attack 3	5	2	18:16:05	3 mn 2 6 s
UDP flood	Attack 1	5	1	20:00:27	15 mn
	Attack 2	5	1	20:00:27	15 mn
ICMP Smurf	Attack 1	4	1	21:34:16	1 s
	Attack 2	4	1	21:34:26	1 s
	Attack 3	4	3	18:29:25	1 s
	Attack 4	4	5	08:45:18	2 s
	Attack 5	5	1	09:33:00	2 mn

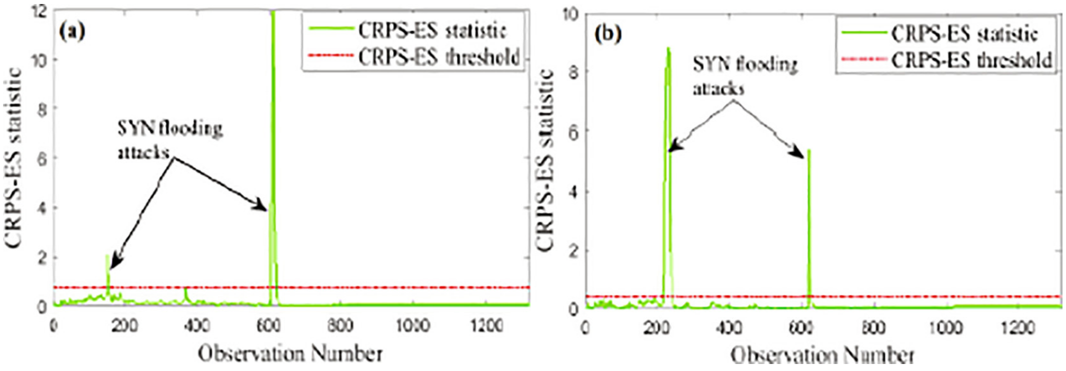

Fig. 5. CRPS-ES results when SYN flooding attacks occurred in (a) W5D1 SYN messages and (b) W5D2 SYN messages.

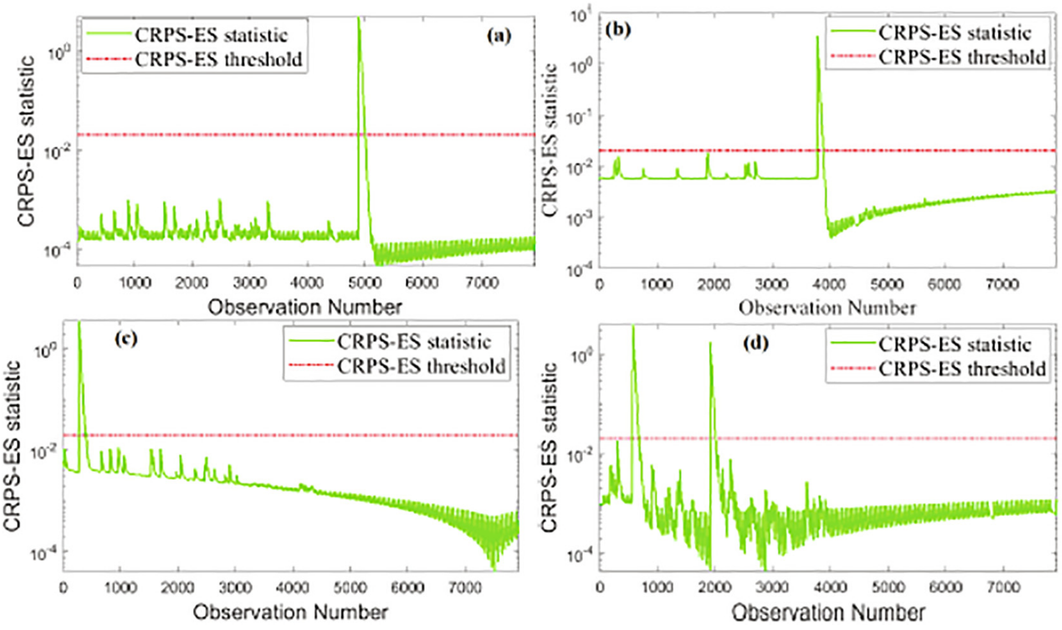

Fig. 6. CRPS-ES results when abnormal ICMP Echo Reply messages occurred on (a) W4d1, (b) W4d3, (c) W4d5 and (d) W5d1.

To assess quantitatively the detection efficiency of the CRPS-ES method, the following metrics will be used: true positive rate (TPR), false-positive rate (FPR), false-negative rate (FNR), and area under the curve (AUC). Table 2 provides a summary of the detection quality of the CRPS-ES mechanism when applied to DARPA dataset. Results in Table 2 highlight that the detection capability of the CRPS-ES mechanism by achieving a high TPR and lower FPR and FNR.

3.3. Detection results using MAWI dataset:

Here, we consider the scenarios of UDP flood and ping flood attacks using The MAWI (Measurement and Analysis on the WIDE Internet) dataset. MAWI dataset is real internet traffic provided by the MAWI Working Group Traffic repository. In this dataset, the traffic is captured from many *trans*-pacific links (i.e., sample point-A, sample point-C, sample point-D, and sample point-F)

Table 2
Performance of CRPS-ES method when using in DARPA99.

Attack		TPR (%)	FPR (%)	FNR (%)	AUC (%)
TCP SYN flood	Attack 1	100	0.18	0	99.91
	Attack 2	97.56	0.15	2	98.70
UDP flood	Attack 1	91.67	0.09	8.4	95.79
ICMP Smurf	Attack 1	100	0.45	0	99.77
	Attack 2	100	0.076	0	99.96
	Attack 3	100	0.076	0	99.96
	Attack 4	100	0.076	0	99.96

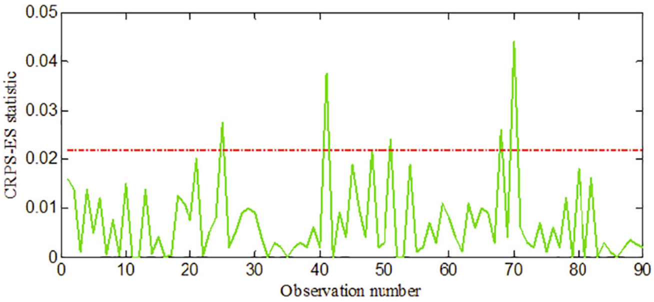

Fig. 7. CRPS-ES results when UDP flood attacks happened.

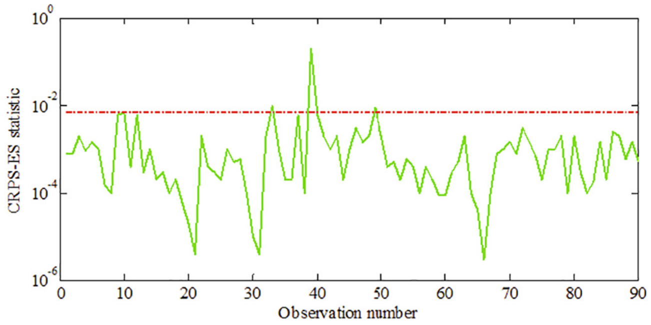

Fig. 8. CRPS-ES results when Ping flood attacks happened.

between the Japanese WIDE network and the USA. The sample point-F, which is the most used, provides a daily trace of 15 mn. In this study, TCPDUMP trace of January, 1st, 2010; 14 h 00 mn to 14 h 15 mn are used [41].

Fig. 7 illustrates the detection results of CRPS-ES in the presence of UDP flood attacks. The inspected traffic contains two attacks at instances 41 and 70. While the detection threshold h_{es} = 0.021, these two attacks are accurately detected and their corresponding CRPS measurements are 0.037 and 0.044, respectively. In their labeling, the authors claimed also the presence of some suspicious behaviors, which are revealed at instances 26, 54 and 67. Such behaviors resulted from the high activity of some users in instance 26, 26% of the total UDP traffic, which is related to the user 163.234.102.228. Effectively, the detection scheme returns these instances little more than the normal traffic has.

Fig. 8 presents the detection results of the CRPS-ES mechanism when applied to the Echo Request messages in the presence of Ping flood attacks. Three attacks are detected at instances 32, 39 and 48. These attacks correspond to the ICMP network scan, where most of the Echo Request messages are related to three addresses IP in 163.234.176.x and two address IP in 208.108.253.x, representing from 69.5% in instance 32 to 81.7% in instance 55. Here, h_{es} = 0.009 and CRPS-ES measurements during the three attacks were 0.011, 0.13 and 0.01 respectively. Therefore, a very small detection threshold has been established. Here, for the tow studied scenarios, UDP flood, and Ping flood, the detection thresholds were h_{es} = 0.021 and h_{es} = 0.009, respectively. That is means; CRPS-ES can correctly detect low rate attacks while considering such attacks.

Table 4
ICMPv6-based dos attacks characteristics.

Attack	Time of appearance	Duration
Router advertisement	imnlOs	3 s
Neighbor solicitation	Os	is
Neighbor advertisement	1 mn2Os	4 s

3.4. Detection results using ICMPv6 dataset

Here, the performance of CRPS-ES to reveal the ICMPv6-based DOS attacks is investigated. The dataset consists of a collection of ICMPv6 traffics that are generated under the GNS3 emulator [42]. Here, we consider three types of ICMPv6-based DOS attacks which are neighbor advertisement, neighbor solicitation, and router advertisement flooding attacks. Their details are recapitulated in Table 3. We studied 10mn of anomalous traffic, while the attack-free traffic is about 48 h. In this case, the number of each type of these messages is controlled to deal with the corresponding attack. As expected, high values of CRPS that exceed the detection threshold are obtained according to the presence of attacks. Fig. 9(a–c) displays the results of the CRPS-ES mechanism in the presence of ICMPv6-based DOS attacks namely neighbor advertisement, neighbor solicitation, and router advertisement, respectively. As illustrated, in this scenario, CRPS-ES statistics reach high values when different types of attacks happened. In that order, the corresponding (CRPS-ESstatistic, h_{es}) were (8, 0.02), (6, 0.018) and (9, 0.019). Indeed, attacks in this dataset are characterized by a large intensity, which makes them easy to detect by the proposed scheme. Nevertheless, CRPS-ES presented high sensitivity (i.e. very small h_{es}) and is adapted to deal with low rate attacks in this challenging environment.

Table 5 summarizes the detection performance of the CRPS-ES mechanism when applied to ICMPv6 datasets. Results testify that the proposed approach has a promising performance in detecting attacks in network traffic datasets.

Table 6 compares the performance of CRPS-ES mechanism with some state-of-the-art approaches namely Anomaly Intrusion Detection (AID) [43], Back Propagation Neural Network (BPN) [43], and Support Vector Machine (SVM) [44] when applied to DARPA 99 datasets. Results show that the considered TCP SYN flood attacks were appropriately detected using the CRPS-ES mechanism (i.e., true positive rate (TPR) = 100% and false positive rate (FPR) = 0.18%). Results in Table 4 indicate that the proposed approach outperforms these state-of-the-art methodologies.

4. Conclusion

The objective aim of this paper is designing an efficient scheme to suitably detect DOS and DDOS attacks. This integrated scheme combines the sensitivity of the exponential smoothing procedure and the good capacity of CRPS in separating normal and from abnormal features. Furthermore, a nonparametric threshold of

Table 3
reports the performance assessment of the CRPS-ES in terms of TPR, FPR, accuracy, and AUC according to the anomalous flows included in the MAWI dataset. Table 3: Performance of CRPS-ES method when using in Mawi dataset.

Attack		TPR (%)	FPR (%)	Accuracy (%)	AUC (%)
UDP flood	Attacks 1–2	1	0.035	0.967	0.982
Ping flood	Attacks 1	1	0	1	1
	Attacks 2	0.769	0.128	0.857	0.821

Table 5
Performance of CRPS-ES method when using in ICMPv6.

Attack	TPR (%)	FPR (%)	FNR (%)	AUC (%)
Neighbor advertisement	100	0	0	100
Neighbor solicitation	100	3.27	0	98.40
Router advertisement	100	0	0	100

Table 6
Performance of different methods: SYN flooding attacks in DARPA99.

Approach	TPR (%)	FPR (%)
CRPS-ES	100	0.18
AID 40 × 40 [43]	96.8	2.85
AID 30 × 30 [43]	96.3	3.15
BPN [44]	99.3	0.7
SVM [44]	99.2	0.84

the CRPS-ES statistic is computed via kernel density estimation method. This provides more flexibility to the CRPS-ES detector by relaxing assumptions about the distribution underlying the data. The effectiveness of the CRPS-ES is evaluated using the DARPA99, MAWI and ICMPv6 traffic network datasets. The results indicate that the integrated CRPS-ES showed good performance in comparison to other commonly used algorithms.

Despite the suitable results achieved by using the CRPS-ES approach for anomaly detection purpose, the work carried out in this paper raises a number of questions and provides some directions for future works. In particular, the following points merit consideration from researchers.

- The proposed CRPS-ES anomaly detection approach is for one scale (time scale) may not be suited for detecting abnormal events at several scales. However, most data form network systems generally contain relevant features and noise that have contributions in time and frequency. Therefore, as future work, we plan to develop a multiscale CRPS-ES approach that can offer improved detection capacity of this technique.
- Furthermore, to further improve cyber-attacks detection, in future works, it is planned to consider other parameters, such as IP source address, acknowledgment (ACK), reset (RST), finished (FIN) TCP segments, and ports, since DOS and DDOS attacks affect significantly these parameters [45]. It is intended to design a detection mechanism based on multivariate CRPS for enhanced detection performance.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

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-2019- CRG7-3800.

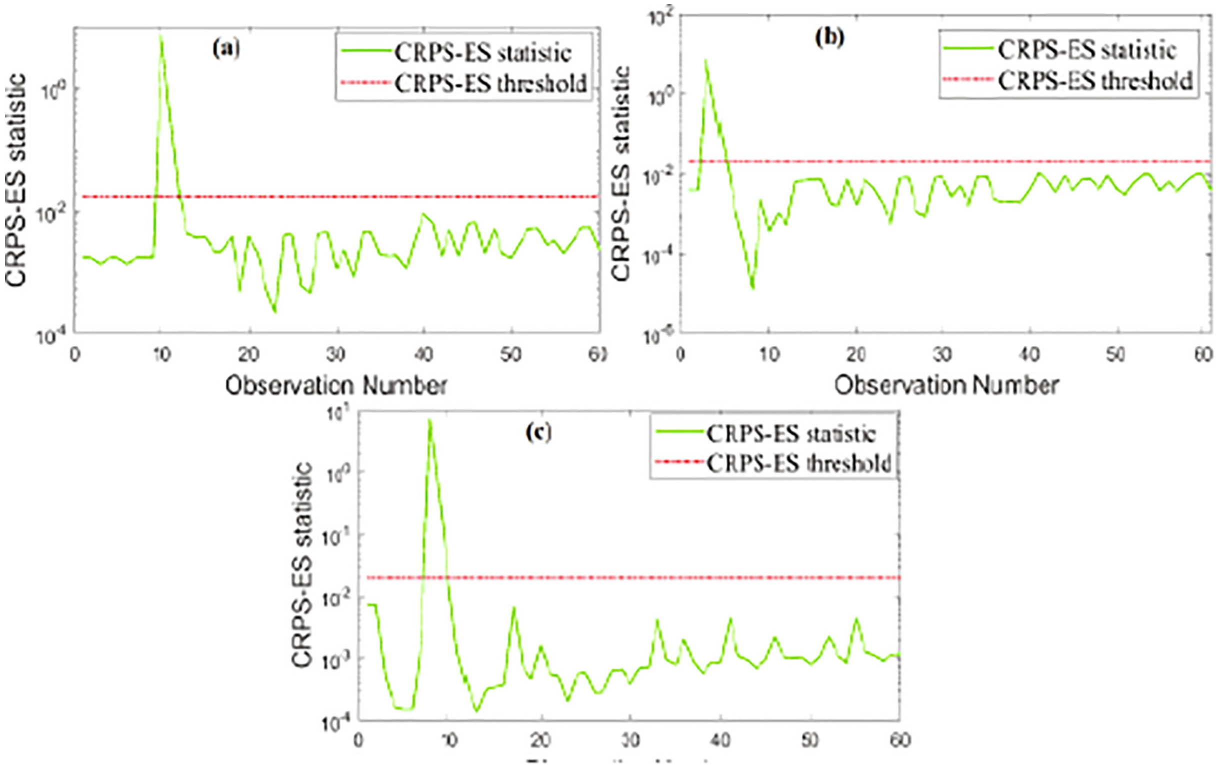

Fig. 9. CRPS-ES results when (a) neighbor advertisement flood, (b) neighbor solicitation flood attack and (c) router advertisement flood attack happened.

References

[1] G. Mois, S. Folea, T. Sanislav, Analysis of three IoT-based wireless sensors for environmental monitoring, IEEE Trans. Instrum. Meas. 66 (8) (2017) 2056–2064.

[2] I.Yaqoob, I-A- T.Hashem, A.Ahmed,S.M. A.Kazmi andC.S.Hong," Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges", Future Generation Computer Systems, Vol 92, March, 2019,

[3] A. Yassine, H. Rahimi, S. Shirmohammadi, Software defined network traffic measurement: current trends and challenges, IEEE Instrum. Meas. Mag. 18 (2) (2015) 42–50.

[4] Francisco J. Ros, Pedro M. Ruiz, On reliable controller placements in software-defined networks, Comput. Commun. 77 (2016) 41–51, https://doi.org/10.1016/j.comcom.2015.09.008.

[5] Alex G.C. de Sá, Adriano C.M. Pereira, Gisele L. Pappa, A customized classification algorithm for credit card fraud detection, Eng. Appl. Artif. Intell. 72 (2018) 21–29, https://doi.org/10.1016/j.engappai.2018.03.011.

[6] Désiré Sidibé, Shrinivasan Sankar, Guillaume Lemaître, Mojdeh Rastgoo, Joan Massich, Carol Y. Cheung, Gavin S.W. Tan, Dan Milea, Ecosse Lamoureux, Tien Y. Wong, Fabrice Mériaudeau, An anomaly detection approach for the identification of DME patients using spectral domain optical coherence tomography images, Comput. Methods Programs Biomed. 139 (2017) 109–117, https://doi.org/10.1016/j.cmpb.2016.11.001.

[7] P.L. Higueras, F.J. Sáez-Martínez, G. Lefebvre, R. Moilleron, Contaminated sites, waste management, and green chemistry: new challenges from monitoring to remediation, Environ. Sci. Pollut. Res. 26 (4) (2019) 3095–3099.

[8] P. Passeri,"February 2020 Cyber Attacks Statistics,"Hackmageddon, March,19, 2020.

[9] S.A. Abdullah, SEUI-64, bits an IPv6 addressing strategy to mitigate reconnaissance attacks, Eng. Sci. Technol. Int. J. 22 (2) (2019) 667–672.

[10] A. Rezai, P. Keshavarzi, Z. Moravej, Key management issue in SCADA networks: a review, Eng. Sci. Technol. Int. J. 20 (1) (2017) 354–363.

[11] B. Subba, S. Biswas, S. Karmakar, Intrusion detection in mobile ad-hoc networks: bayesian game formulation, Eng. Sci. Technol. Int. J. 19 (2) (2016) 782–799.

[12] J. Mirkovic, P. Reiher, A taxonomy of ddos attack and ddos defense mechanisms, ACM SIGCOMM Comput. Commun. Rev. 34 (2) (2004) 39–53.

[13] W. Wei, F. Chen, Y. Xia, G. Jin, A rank correlation based detection against distributed reflection DoS attacks, IEEE Commun. Lett. 17 (1) (2013) 173–175.

[14] L.Sheng, L. Zhiming, H. Jin, D.Gaoming and Huang Wen,"A Distributed Botnet Detecting Approach Based on Traffic Flow Analysis", Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp 124 – 128, 2012.

[15] Shui Yu, Wanlei Zhou, R. Doss, Information theory based detection against network behavior mimicking DDoS attacks, IEEE Commun. Lett. 12 (4) (2008) 318–321, https://doi.org/10.1109/LCOMM.2008.072049.

[16] A. Shevtekar, K. Anantharam, N. Ansari, Low rate TCP denial-of-service attack detection at edge routers, IEEE Commun. Lett. 9 (4) (2005) 363–365.

[17] S.M.T. Nezhad, M. Nazari, E.A. Gharavol, A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks, IEEE Commun. Lett. 20 (4) (2016) 700–703.

[18] F.Fang, L. Xiaoyan, W.Jia, T. XueJu, Z.Bo, H. JiYao and S. Yuan," Network Security Situation Evaluation Method for Distributed Denial of Service", Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp 16 – 21, 2012

[19] K.S. Sahoo, D. Puthal, M. Tiwary, J.J. Rodrigues, B. Sahoo, R. Dash, An early detection of low rate ddos attack to sdn based data center networks using information distance metrics, Future Gen. Comput. Syst. 89 (2018) 685–697.

[20] Q. Zhang, K. Liu, Y. Xia, A. Ma, Optimal stealthy deception attack against cyber-physical systems, IEEE Trans. Cybern. (2019).

[21] M. Zulkiflee, M. Azmi, S. Ahmad, S. Sahib, M. Ghani, A framework of features selection for ipv6 network attacks detection, WSEAS Trans. Commun. 14 (46) (2015) 399–408.

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

[23] R.M. Saad, M. Anbar, S. Manickam, E. Alomari, An intelligent icmpv6 ddos flooding-attack detection framework (v6iids) using back-propagation neural network, IETE 33 (2016) 1–12.

[24] M. Al-Qatf, Y. Lasheng, M. Al-Habib, K. Al-Sabahi, Deep learning approach combining sparse autoencoder with SVM for network intrusion detection, IEEE Access 6 (2018) 843–856.

[25] T. Ma, F. Wang, J. Cheng, Y. Yu, X. Chen, A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks, Sensors 16 (10) (2016) 1701.

[26] D. Papamartzivanos, F. G. Ḿarmol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," IEEE Access, vol. 7, pp. 13 546–13 560, 2019.

[27] I.W. Burr, The effect of non-normality on constants for X and R charts, Ind. Qual. Control 23 (11) (1967) 563–569.

[28] E.P. Grimit, T. Gneiting, V. Berrocal, N.A. Johnson, The continuous ranked probability score for circular variables and its application to mesoscale forecast ensemble verification, Quart. J. R. Meteorol. Soc. 132 (621C) (2006) 2925–2942.

[29] J.E. Matheson, R.L. Winkler, Scoring rules for continuous probability distributions, Manage. Sci. 22 (10) (1976) 1087–1096.

[30] F. Harrou, Y. Sun, M. Madakyaru, B. Bouyeddou, An improved multivariate chart using partial least squares with continuous ranked probability score, IEEE Sens. J. 18 (16) (2018) 6715–6726.

[31] F. Harrou, M.N. Nounou, Monitoring linear antenna arrays using an exponentially weighted moving average-based fault detection scheme, Syst. Sci. Control Eng. An Open Access J. 2 (1) (2014) 433–443.

[32] E. Martin, A. Morris, Non-parametric confidence bounds for process performance monitoring charts, J. Process Control 6 (6) (1996) 349–358.

[33] A.R. Mugdadi, I.A. Ahmad, A bandwidth selection for kernel density estimation of functions of random variables, Comput. Stat. Data Anal. 47 (1) (2004) 49–62.

[34] R. Mohammadi, R. Javidan, M. Conti, Slicots: an sdn-based lightweight countermeasure for tcp syn flooding attacks, IEEE Trans. Netw. Serv. Manage. 14 (2) (2017) 487–497.

[35] B. Bouyeddou, F. Harrou, Y. Sun and B. Kadri "Detection of Smurf Flooding Attacks Using Kullback-Leibler-based Scheme". ICCTA, istanbul, Turkey, May 3-5, 2018.

[36] F.Harrou, B.Bouyeddou,Y.Sun and B.Kadri « A Method to Detect DOS and DDOS Attacks based on Generalized Likelihood Ratio Test » International Conference on Applied Smart Systems, , Medea, Algeria, 24-25, November 2018.

[37] Bouyeddou, B., Harrou, F., Sun, Y. and Kadri, B., "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), 2017.

[38] M. Bogdanoski, T. Suminoski, A. Risteski, Analysis of the SYN flood DoS attack, Int. J. Comput. Netw. Inform. Secur. (IJCNIS) 5 (8) (2013) 1–11.

[39] J. Davida, C.Thomas,"Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic", Computers and Security Vol.82, pp 284-295, May 2019

[40] O.E. Elejla, M. Anbar, B. Belaton, ICMPv6-based DoS and DDoS attacks and defense mechanisms, IETE Tech. Rev. 34 (4) (2017) 390–407.

[41] http://www.fukuda-lab.org/mawilab/data.html.

[42] O.E. Elejla, B. Belaton, M. Anbar, A. Alnajjar, A reference dataset for icmpv6 flooding attacks, J Eng Appl Sci 11 (3) (2016) 476–481.

[43] J. Zheng, M. Hu, An anomaly intrusion detection system based on vector quantization, IEICE Trans. Inf. Syst. 89 (1) (2006) 201–210.

[44] C.D. McDermott, A. Petrovski, Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks, Int. J. Comput. Netw. Commun. 9 (4) (2017) 45–56.

[45] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: a survey, ACM Comput. Surv. (CSUR) 41 (3) (2009) 1–58.