Detecting cyber-attacks using a CRPS-based monitoring approach

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

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

***Abstract*—Cyber-attacks can seriously affect the security of computers and network systems. Thus, developing an efficient anomaly detection mechanism is crucial for information protection and cyber security. To accurately detect TCP SYN flood attacks, two statistical schemes based on the continuous ranked probability score (CRPS) metric have been designed in this paper. Specifically, by integrating the CRPS measure with two conventional charts, Shewhart and the exponentially weighted moving average (EWMA) charts, novel anomaly detection strategies were developed: CRPS-Shewhart and CRPS-EWMA. The efficiency of the proposed methods has been verified using the 1999 DARPA intrusion detection evaluation datasets.**

***Keywords*—DoS, TCP SYN Flood, cyber-attack, CRPS, statistical anomaly detection, DARPA99 dataset.**

I. Introduction

Computer networks and internet are continuously exposed to many viruses and cyber-attacks [1], [2]. Denial of service and distributed denial of service (i.e., DOS and DDOS) attacks attemp to disrupt networks' availability and suspend the usability of their hosted services [3]. In last few years, several cyber-attacks were performed against different targets, such as the American presidential election, the Rio De Janero Olympics games, the US Domain Name System (DYN), the Russian Banking System, Qatar News Agency, the US department of defense, the Android users, the NSA and the German armed forces [4].

Practically, flooding cyber-attacks, such as DOS and DDOS attacks (e.g., TCP SYN flooding, UDP flooding and ICMP-amplification) overwhelm the network's infrastructures with an important volume of traffic [5]. Other types of DOS and DDOS attacks, such as IP fragmentation, Land and Ping of death, utilize a deformed message (e.g., size exceeds 64 Ko, wrong fragments and wrong IP address) [6]. TCP SYN flood are usually exploited by attackers. It was used in more than 75% of attacks launched between september and december 2016. Hence, To reinforce the security of networks systems, SYN flooding attack must be reliably and correctely identified before they slowdown the performance of the inspected system.

Due to the increasing need for improved cybersecurity, several techniques aimed at detecting SYN flood attacks have been proposed. In [7], a non-parametric CUSUM algorithm was used in detecting SYN flooding attacks at leaf router. The method in [8] the linear prediction analysis and the difference between outgoing SYN and incoming SYN/ACK segments to detect SYN flood. In [9], the detection of TCP SYN flooding attack has been achieved based on SYN and SYN/ACK segments with the consideration of packets header information. In [10], an adaptive threshold-based approach and CUSUM algorithm were used to detect SYN Flooding Attacks based on SYN segments. In [11], TCP connection requests are controlled by the firewall which forwards them to a server only if it receives the client ACK. However, with this solution, the firewall risks to be overloaded and the related network becomes more vulnerable. In [12], SYN flood attacks are identified according to the periodicity of a signal created from the incoming TCP traffic. Unfortunately, a high rate of false alarms can be introduced and get an appropriate modeling of the normal TCP flow. Schuba et al. [13] analyzed the network traffic to build an IP-based trust mechanism. Basicevis et .al [14] proposed an approach based on the Tsallis entropy. In the literature, there has been much discussion on machine learning algotithms to mitigate DOS attacks including support vector machines [15], neural network [16] and K-Nearest Neighbors [17].

Detection of SYN flood attacks is significant for guaranteeing cyber security and information protection. The main focus in this paper is to design an anomaly detection mechanism that can detect SYN flood attacks. Towards this end, we exploit advantages of statistical monitoring charts, such as Shewhart and the exponentially weighted moving average (EWMA) charts [18]–[20], and the benefit of the continuous ranked probability score (CRPS) metric [21], [22]. Specifically, we propose two statistical monitoring charts to detect SYN flood attacks: CRPS-Shewhart and CRPS-EWMA. To assess the performance of these two charts, we used the 1999 DARPA intrusion detection evaluation dataset.

In Section II we present the basic idea of SYN flooding attack. In Section III, we briefly review the introduced CRPS-based monitoring charts. Section IV reports the experimental results using DARPA99 dataset. Finally, Section V concludes this paper.

II. SYN FLOOD ATTACKS

SYN flood attack stills the most popular to perform a DOS/DDoS attack against any TCP-based services such as Web servers, FTP servers or Mail servers. To request a new connection, user sends, to the server, a synchronization segment (SYN) (Figure 1). Then, to acknowledge (ACK) this synchronization demande, the server responds with the SYNchronization's ACKnwoledgement segemnt (i.e., SYN-ACK) and put this session in the backlog queue rezerved to the half-open sessions. Finally, the user confirms his request by the ACK segment and the session is established. It is notable that any connection request will remain in the backlog queue until the server receives the user's acknowledgment. otherwise, the session will remain half-open until his lifetime expires [7].

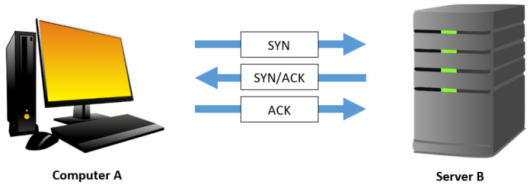

Figure 1. Schematic illustration of TCP connection steps.

To create a TCP SYN flood attack, attackers create important stream of half-open sesssions, enough to saturate the victim's ressources. Accordingly, the victim cannot handle more sessions, even from legitimate users, and the hosted services become pratically inaccessible. There are two different strategies to carry out such attack [23], [24]: (1) hacker sends many SYN and ignores the SYN-ACK from the server (Figure 2). (2) hacker spoofs an IP address to establish a connecion with the victim which should acknwoledge this request and sends the SYN-ACK to the fake address. Since this fake IP address is unreachable or did not initiated such connection request, the victim will never receive the user's Acknowledgement. To achieve SYN flood DDOS attack, the attacker compromises numerous zombie machines and then exploits them to attack simultaneously the target server. Each zombie launch, obviously, a SYN flood DOS attack [24].

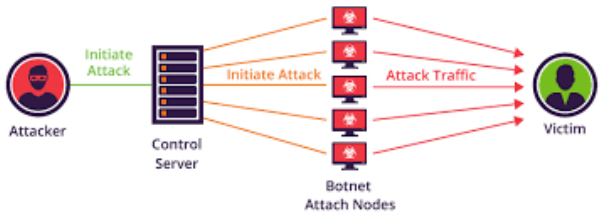

Figure 2. A procedure of SYN flooding attacks.

III. CRPS-BASED MONITORING CHARTS

To develop an effective anomaly detection mechanism, we have merged the CRPS measure with two commonly statistical schemes, Shewhart and EWMA. The CRPS quantify the deviation between the actual observation and the cumulative distribution of the training data [25]. CRPS has a good sensitivity to changes and it is relevant for online monitoring.

The main reason of using CRPS metric in anomaly detection is its capability to measure the distance between a full distribution and an observation [21] (Figure 3). The CRPS between the observation, x, and the CDF, F, is computed as [21], where

$$CRPS(F,x) = \int_{-\infty}^{\infty} \Big(F(y) - \mathbb{1}\{y \geq x\} \Big)^2 dy, \qquad (1)$$

$\mathbb{1}\{.\}$ represents the indicative function that attains the value 1 if $x < y$ and the value 0 otherwise. In the case of Gaussian distribution, the CRPS metric is given by where ϕ and Φ are

$$\begin{aligned} CRPS(\mathcal{N}(\mu,\sigma^2),x) &= \sigma\Bigg[\frac{x-\sigma}{\sigma}\Big(2\Phi(\frac{x-\sigma}{\sigma})-1\Big) \\ &\quad +2\phi(\frac{x-\sigma}{\sigma}) - \frac{1}{\sqrt{\pi}}\Bigg], \qquad (2) \end{aligned}$$

respectively the standard Gaussian PDF and CDF.

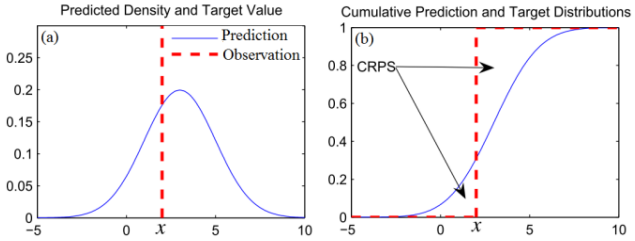

Figure 3. An illustration of CRPS: PDF (a) and (b) CDF.

A. CRPS-Shewhart detection mechanism

Shewhart monitoring procedure was first introduced by Walter Shewhart for quality control [26], [27]. It is appropriate to reveal anomalies with large mean shifts. Unfortunately, it is not sensitive to uncover small changes [28]. In the proposed CRPS-Shewhart mechanism, Shewhart scheme is employed to monitor CRPS measurements for anomaly detection. Generally speaking, when the i-th CRPS value is beyond the control limits, then the inspected network is normal. Otherwise, we signal the presence of an abnormal event (attack) in the network. The CRPS-Shewhart thresholds are defined as,

$$LCL_s, UCL_s = \mu_0^{CRPS} \pm 3\sigma_0^{CRPS}, \qquad (3)$$

where μ_0^{CRPS} and σ_0^{CRPS} represent the mean and standard deviation of CRPS measurements in the absence of anomalies.

B. CRPS-EWMA detection mechanism

In CRPS-EWMA chart, EWMA scheme is used to monitor CRPS measurements for anomaly detection. The CRPS-EWMA detection rule is calculated as follows [26],

$$z_i^{CRPS} = \lambda CRPS_i + (1-\lambda) z_{i-1}^{CRPS}, \qquad (4)$$

where $CRPS_i$ is the present CRPS measurement, z_0^{CRPS} represents the anomaly-free mean of CRPS measurements, μ_0^{CRPS}. λ $(0 < \lambda \leq 1)$ is a smoothing parameter. Generally, it is selected between 0.1 and 0.3 to detect small changes [26]. The CRPS-EWMA thresholds are given by,

$$LCL, UCL = \mu_0^{CRPS} \pm L\sigma_0^{CRPS}\sqrt{(\frac{\lambda}{(2-\lambda)}[1-(1-\lambda)^{2i}]}. \quad (5)$$

IV. Experimental results

This section reports on the efficiency of the proposed CRPS-based EWMA and Shewhart mechanisms to uncover SYN flooding attacks. Our proposed mechanisms are compared with the conventional Shewhart and EWMA charts. To this end, we performed experiments on the DARPA 99 dataset [29].

A. Description of DARPA99 dataset

Now, the detection capacity of the introduced mechanisms is evaluated using the DARPA 99 dataset, which is one of well-known datasets used for assessing intrusion detection mechanisms [29]. The topology of the network used to generate this data is illustrated in Figure 4. It comprises five weeks of data (3 weeks of attack-free data and 2 weeks of testing data) [30].

B. Detection of SYN flood attacks:

The following steps have been conducted to detect possible attacks in the DARPA99 dataset.

(1) We compute the control limits of each chart using training data of DARPA99/SYN.
(2) We selected $L = 2.7$ and $\lambda = 0.1$ in EWMA-based detection mechanisms, which provide sensitive detection capacity to small changes.
(3) We calculate the decision rules of CRPS-Shewhart, CRPS-EWMA, EWMA and Shewhart chart for testing data.
(4) We signal SYN flood attacks when the decision rules overpass the decision thresholds.

1) Scenario with intermittent SYN flood attacks with different intensities: In this scenario, we investigate the ability of the CRPS-Shewhart and CRPS-EWMA mechanisms to detect intermittent SYN flood attacks with different intensities. Intermittent SYN flood attacks occur and disappear repeatedly. Ten minutes of SYN flooding is incorporated in the testing data every three hours. Figure 5(a-d) illustrates the results of the studied mechanisms. Figure 5(a) and Figure 5(c) show that Shewhart and CRPS-based charts detect these attacks but with several false alarms. On another hand, CRPS-EWMA chart detects these attacks without false alarms (Figure 5(d)). It can be see that the CRPS-based mechanisms are more efficient than the conventional charts (Figure 5). Due to their high sensitivity, they can detect even attacks with lower intensities. This behavior confirms the ability of CRPS to reveal small anomalous traffic.

2) DARPA 99 SYN flood attacks: Here, we investigate the ability of CRPS-based Shewhart and EWMA mechanisms to detect SYN flood attacks occurred on the traffic of week 5, day 2 of DARPA 99 data [29]. This traffic data includes two attacks. The first starts at 11h38mn04s against Marx (@IP:172.16.114.50) with a duration of 13mn41s. The second attack was at 18h16mn05s against the router (@IP: 192.168.1.1) for 3mn26s. Figure 6(a-d) illustrates the detection results of the four procedures. Results show that the proposed method CRPS-EWMA outperformed Shewhart, EWMA and CRPS-Shewhart, and exhibited the highest accuracy. The CRPS-EWMA scheme correctly detect these attacks without false alarms.

V. Conclusion

We design efficient anomaly detection mechanisms to detect SYN flood DOS and DDOS attacks. These mechanisms merges the benfits of CRPS metric and univariate monitoring schemes, Shewhart and EWMA. CRPS is applied to measure the deviation between the actual observation and the distribution of the anomaly-free data. EWMA and Shewhart schemes are applied to CRPS measurements to uncover denial of service SYN flood attacks. We assessed the detection capability of these charts via the publicly available DARPA 99 dataset. Results indicate that CRPS-Shewhart and CRPS-EWMA present higher sensibility than Shewhart and EWMA chart in detecting SYN flood 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] S. Singh and S. Silakari, "A survey of cyber-attack detection systems," *International Journal of Computer Science and Network Security*, vol. 9, no. 5, pp. 1–10, 2009.

[2] M. E. Manna and A. Amphawan, "Review of syn-flooding attack detection mechanism," *arXiv preprint arXiv:1202.1761*, 2012.

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

[4] K. Arora, K. Kumar, and M. Sachdeva, "Impact analysis of recent ddos attacks," *International Journal on Computer Science and Engineering*, vol. 3, no. 2, pp. 877–883, 2011.

[5] B. Bouyeddou, F. Harrou, Y. Sun, and B. Kadri, "Detection of smurf flooding attacks using kullback-leibler-based scheme," in *2018 4th International Conference on Computer and Technology Applications (ICCTA)*. IEEE, 2018, pp. 11–15.

[6] S. Deore and A. Patil, "Survey denial of service classification and attack with protect mechanism for TCP SYN flooding attacks," *IRJET*, vol. 3, no. 5, 2016.

[7] H. Wang, D. Zhang, and K. G. Shin, "Detecting syn flooding attacks," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2002, pp. 1530–1539.

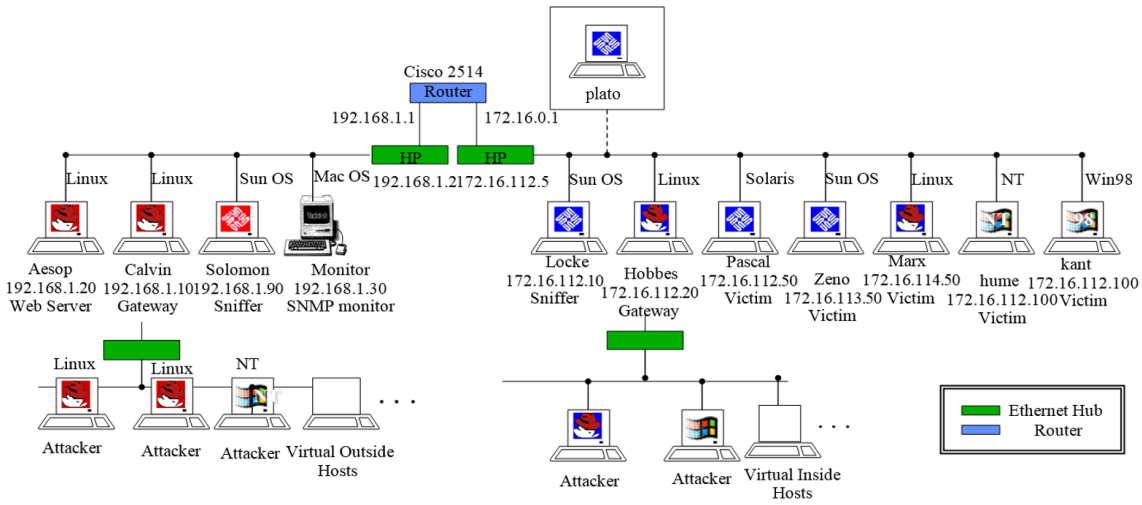

Figure 4. Illustration of the topology of the studied DARPA 99 network.

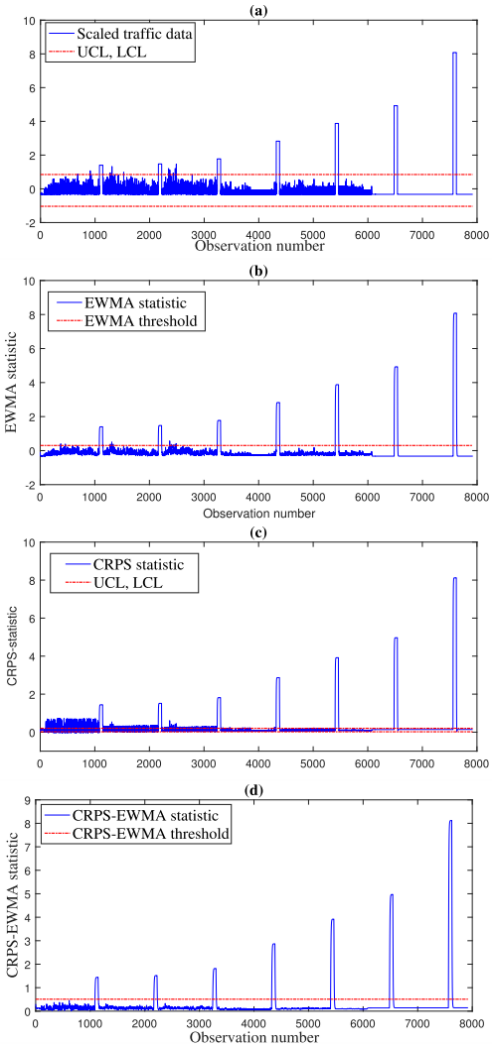

Figure 5. Results of Shewhart (a), EWMA (b), CRPS-Shewhart (c) and CRPS-EWMA mechanisms (d) in the presence of intermittent SYN flood attacks.

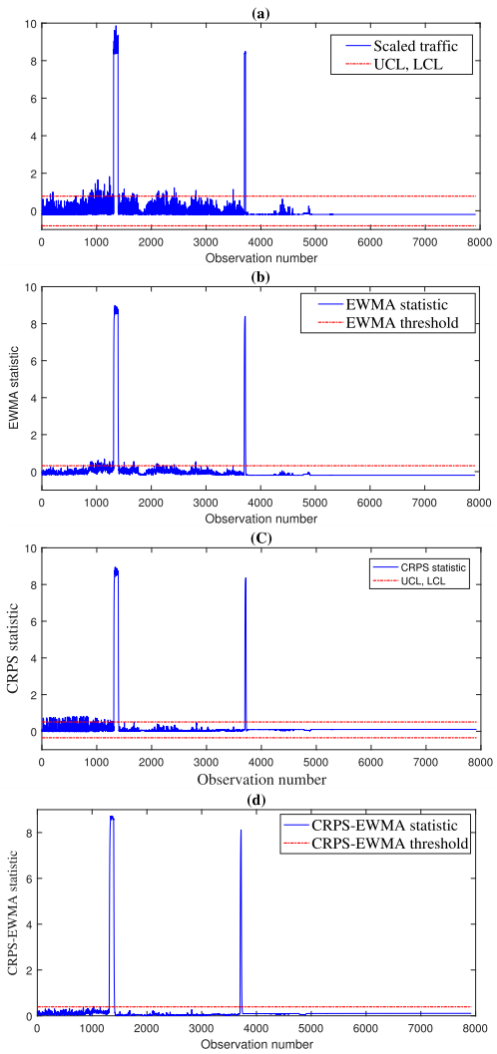

Figure 6. Results of Shewhart (a), EWMA (b), CRPS-Shewhart (c) and CRPS-EWMA mechanisms (d) for DARPA 99 SYN flood attack in the second day of week 5.

[8] 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.

[9] D. Nashat, X. Jiang, and S. Horiguchi, "Detecting SYN flooding agents under any type of ip spoofing," in *IEEE International Conference on e-Business Engineering, ICEBE'08*. IEEE, 2008, pp. 499–505.

[10] V. A. Siris and F. Papagalou, "Application of anomaly detection algorithms for detecting SYN flooding attacks," in *IEEE Global Telecommunications Conference, GLOBECOM'04*, vol. 4. IEEE, 2004, pp. 2050–2054.

[11] *Check Point Software Technologies Ltd., SynDefender*. [Online]. Available: http://www.checkpoint.com/products/firewall-1

[12] C.-M. Cheng, H. Kung, and K.-S. Tan, "Use of spectral analysis in defense against DoS attacks," in *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, vol. 3. IEEE, 2002, pp. 2143–2148.

[13] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*. IEEE, 1997, pp. 208–223.

[14] I. Basicevic, S. Ocovaj, and M. Popovic, "Use of tsallis entropy in detection of SYN flood DoS attacks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3634–3640, 2015.

[15] T. Subbulakshmi, S. Shalinie, and A. Ramamoorthi, "Detection and classification of DDoS attacks using machine learning algorithms," *European Journal of Scientific Research*, vol. 47, no. 3, pp. 334–346, 2010.

[16] C. Jirapummin, N. Wattanapongsakorn, and P. Kanthamanon, "Hybrid neural networks for intrusion detection system," in *Proc. of ITC–CSCC*, 2002, pp. 928–931.

[17] Y. Li, B. Fang, L. Guo, and Y. Chen, "Network anomaly detection based on TCM-KNN algorithm," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*. ACM, 2007, pp. 13–19.

[18] F. Harrou, M. N. Nounou, H. N. Nounou, and M. Madakyaru, "PLS-based EWMA fault detection strategy for process monitoring," *Journal of Loss Prevention in the Process Industries*, vol. 36, pp. 108–119, 2015.

[19] F. Harrou, Y. Sun, and M. Madakyaru, "Kullback-leibler distance-based enhanced detection of incipient anomalies," *Journal of Loss Prevention in the Process Industries*, vol. 44, pp. 73–87, 2016.

[20] F. Kadri, F. Harrou, S. Chaabane, Y. Sun, and C. Tahon, "Seasonal ARMA-based SPC charts for anomaly detection: Application to emergency department systems," *Neurocomputing*, vol. 173, pp. 2102–2114, 2016.

[21] E. P. Grimit, T. Gneiting, V. Berrocal, and N. A. Johnson, "The continuous ranked probability score for circular variables and its application to mesoscale forecast ensemble verification," *Quarterly Journal of the Royal Meteorological Society*, vol. 132, no. 621C, pp. 2925–2942, 2006.

[22] F. Harrou, Y. Sun, M. Madakyaru, and B. Bouyedou, "An improved multivariate chart using partial least squares with continuous ranked probability score," *IEEE Sensors Journal*, vol. 18, no. 16, pp. 6715–6726, 2018.

[23] H. Salunkhe, S. Jadhav, and V. Bhosale, "Analysis and review of TCP SYN flood attack on network with its detection and performance metrics," *IJERT*, vol. 6, no. 1, pp. 250–256, 2017.

[24] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN flood DoS attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 8, p. 1, 2013.

[25] J. E. Matheson and R. L. Winkler, "Scoring rules for continuous probability distributions," *Management science*, vol. 22, no. 10, pp. 1087–1096, 1976.

[26] D. Montgomery, *Introduction to statistical quality control*. John Wiley & Sons, 2007.

[27] B. Khaldi, F. Harrou, F. Cherif, and Y. Sun, "Monitoring a robot swarm using a data-driven fault detection approach," *Robotics and Autonomous Systems*, vol. 97, pp. 193–203, 2017.

[28] A. Zeroual, F. Harrou, Y. Sun, and N. Messai, "Monitoring road traffic congestion using a macroscopic traffic model and a statistical monitoring scheme," *Sustainable Cities and Society*, vol. 35, pp. 494–510, 2017.

[29] [Online]. Available: https://www.ll.mit.edu/ideval/data/1999data.html

[30] J. W. Haines, R. P. Lippmann, D. J. Fried, M. Zissman, and E. Tran, "1999 darpa intrusion detection evaluation: Design and procedures," MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, Tech. Rep., 2001.