Detecting SYN Flood Attacks via Statistical Monitoring Charts: A Comparative Study

Benamar Bouyeddou[a], Fouzi Harrou[b], *Member, IEEE*
[a]STIC Lab., Department of Telecommunications,
Abou Bekr Belkaid University, Tlemcen, Algeria
Email: bouben81@yahoo.fr, benamarkadri@yahoo.fr

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

***Abstract*—Accurate detection of cyber-attacks plays a central role in safeguarding computer networks and information systems. This paper addresses the problem of detecting SYN flood attacks, which are the most popular Denial of Service (DoS) attacks. Here, we compare the detection capacity of three commonly monitoring charts namely, a Shewhart chart, a Cumulative Sum (CUSUM) control chart and exponentially weighted moving average (EWMA) chart, in detecting SYN flood attacks. The comparison study is conducted using the publicly available benchmark datasets: the 1999 DARPA Intrusion Detection Evaluation Datasets.**

***Keywords*—SYN flood attacks; Accurate detection; Control charts; Cyber-attacks.**

I. Introduction

Cyber-attacks can seriously affect the security of a computer and network system [1]. Indeed, cyber-attacks on networks and systems become a fundamental challenge for individuals as well as for companies and states [2]. Denial of service (DOS) and Distributed DOS (DDOS) attacks, which are pre-eminent types of cyber-attacks, aiming to interrupt servers availability and suspend user's access to a computer network. Recently, numerous cyber-attacks occurred in different services worldwide including the US candidates' campaign websites (April 2016), the Rio Olympics games (September 2015), Brian Krebs (September 2015), the US DNS service provider (October 2015), which caused the disruption of many services, such as Twitter, Amazon, Netflix, New York Times, and CNN, and the Russian Banking System (November 2016). In addition, many attacks were launched, in the last years, against different organizations, such as Yahoo, MasterCard and Bank of America [3].

In practice, there are various types of DOS and DDOS attacks. Some attacks, such as SYN flood, UDP flood, and Ping flood and Smurf, exhaust network or server resources by sending large volumes of traffic. Other type of attacks, such as teardrop and Ping of death, use malformed packets (i.e., total length more than 64 Ko and wrong offset) [4]. TCP SYN flood is still the most commonly occurred attack; it was used in more than 75% of attacks launched in the fourth quarter of 2016. To guarantee the availability and confidentiality of cyber systems, SYN flood attacks have to be reliably detected and isolated in a timely manner and then removed before they affect the performance of the monitored cyber system.

In the last two decades, several anomaly detection methods have been developed to detect SYN flood attacks. Wang et al. (2002) applied a non-parametric CUSUM method to detect SYN flooding attacks at leaf router (i.e., when the number of SYN segment is much higher than the number of FIN/RST segments) [5]. Divakaran et al. (2016) proposed an approach to detect SYN flooding based on the linear prediction analysis using the difference of outgoing SYN and incoming SYN/ACK segments [6]. Nashat et al. (2008) developed an approach for detecting TCP SYN flooding attacks by using SYN and SYN/ACK segments with packets header information [7]. In this approach, the Counting Bloom filter (CBF) has been used to classify all incoming SYN/ACK segments, and then CUSUM chart has been applied to make a final decision [7]. Vasilios et al. (2004) applied two anomaly detection algorithms, adaptive threshold and CUSUM algorithm, to detect SYN flooding attacks based on SYN segments [8]. Other approaches are based machine learning methods to detect DOS attacks, such as neural network [9], support vector machines [10] and K-Nearest Neighbors [11].

It is crucial to accurately detect cyber-attacks. Statistical process monitoring charts are some of the tools that have been applied to achieve this objective [12]. It is a major tool for monitoring sequential systems to make sure that they work stably and satisfactory. In this paper, we compare three commonly statistical charts, Shewhart, CUSUM and EWMA charts, in detecting SYN flood flooding attacks. The goal of this paper is therefore to assess the performance of three monitoring charts to detect cyber-attack, by using the publicly available benchmark dataset, such as the 1999 DARPA Intrusion Detection Evaluation Dataset.

The remainder of this paper is organized as follows. In Section II we review the essential elements of SYN flood DOS/DDOS attacks. In Section III we introduce the three statistical anomaly detection methods. Section IV investigate the method's effectiveness in detecting SYN floods attacks, simulation results were carried out using DARPA99 dataset. Finally, conclusions and discussions are presented in Section V.

II. SYN flood attacks

During a normal TCP connection (Figure 1), the client requests a new connection by sending a SYN (synchronize)

segment to the server. To acknowledge this request, the server replies with a SYN/ACK segment and keep (add) the request in (to) the backlog queue, built in its system memory to maintain all half-open connections. Then, the client returns to the server an ACK segment, and the connection is established, and the server removes this request from the backlog queue. This mechanism is known as the TCP three-way handshake. Of course, any connection request will remain in the backlog queue until the server receives the client's ACK. It means that if the server does not receive the ACK segment the connection remains half-open (i.e., keeping some resource in the backlog queue) for some time up to the TCP connection timeout (usually about 75s) [5]. This is exactly the point exploited by SYN flood attacks.

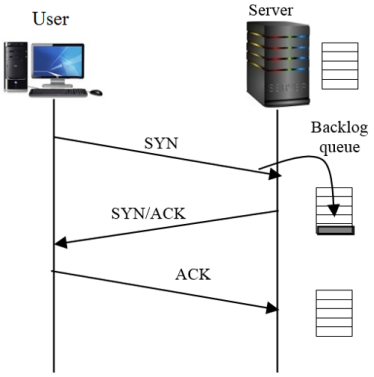

Figure 1. TCP Three-way handshake.

In TCP SYN flood attacks, the attacker creates a large number of half-open connections, enough to reach the backlog queue limit. So, the victim server is not able to accept more connection requests, even from legitimate clients, and the services provided by this server are denied. Usually, two different strategies are used by attackers to perform SYN flood DOS attack [13], [14]. (i) The attacker initiates multiple SYN segments without sending client ACK; it just ignores the received SYN-ACK (Figure 2). (ii) The attacker uses a spoofed source IP address to connect to the victim server. The server will send the SYN/ACK to the spoofed source address. Since the spoofed source is inaccessible or did not send the SYN request, the server will never receive the client ACK. In the case of DDOS using TCP SYN flooding, the attacker use numerous zombie machines simultaneously. Each zombie can launch a TCP SYN DOS attack [14].

III. Univariate statistical monitoring charts

Statistical monitoring charts are extensively studied and widely used in industry [12], [15]–[18]. In this section, we review the most commonly used charts namely: Shewhart, CUSUM and EWMA charts.

A. Shewhart Control Charts:

Shewhart chart has been proposed by Walter Shewhart [12]. Let consider, $X_i(i = 1, \ldots, n)$, n observations that are independent and identically distributed from a $\mathcal{N}(\mu, \sigma^2)$ process,

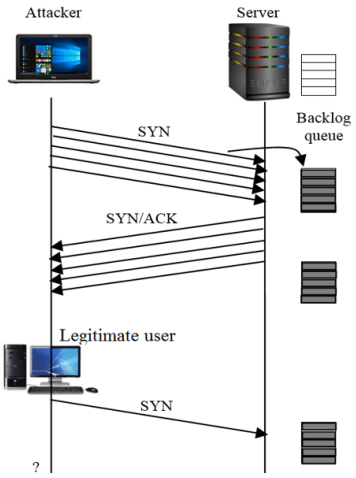

Figure 2. Schematic illustration of a TCP SYN flood attack.

the control limits are established as,

$$CL = \mu_0, LCL, UCL = \mu_0 \pm k\sigma, \tag{1}$$

where μ_0 and σ_0 are mean and standard deviation of x under anomaly-free case. UCL (upper control limit) and LCL (lower control limit) represent the control limits used to detect anomalies. k is the width of control limit, generally k is set to be 3, i.e., 99.73% of the observations fall in the control limits [12]. Shewhart charts are suitable in detecting large mean shifts. However, they are insensitive to small and moderate mean shifts [19].

B. CUSUM Control Charts

CUSUM plot of the cumulative differences C_i between observations values and the target mean μ_0 [12]:

$$C_i = \sum_{j}^{i} (\bar{x}_j - \mu_0). \tag{2}$$

In the tabular version of CUSUM, this accumulation is represented by two characteristics C_i^+ and C_i^- called one sided upper and lower cusums, and used to detect positive and negative shifts respectively.

$$C_i^+ = \max[0, x_i - (\mu_0 + K) + C_{i-1}^+], \tag{3}$$
$$C_i^- = \max[0, (\mu_0 - K) - x_i + C_{i-1}^-], \tag{4}$$
$$H = 5\sigma, \tag{5}$$

K is a tuning parameter (also known as the allowance factor), reflect the sensitivity of CUSUM to the magnitude of shift that wants to detect. Typically, it value is the half of difference between μ_0 and out-of-control value μ_1. CUSUM charts are more appropriate, for detecting small shifts. When either C_i^+ or C_i^- exceed the decision interval H, the process is considered to be out of control [12].

C. EWMA Control Charts:

The EWMA charting statistic is computed at each observation time point as follows [12],

$$z_i = \lambda x_i + (1-\lambda) z_{i-1}, \tag{6}$$

where x_i is the present sample, z_0 represents the anomaly-free mean, μ_0. λ $(0 < \lambda \leq 1)$is a smoothing parameter. When it close to 0, that is mean more samples are considered and EWMA tends to detect small shift. When it close to 1, in this case, EWMA can detect large shift [12]. When λ reach 1, EWMA becomes equivalent to Shewhart chart. The EWMA control limits are defined as,

$$LCL, UCL = \mu_0 \pm L\sigma \sqrt{(\frac{\lambda}{(2-\lambda)}[1-(1-\lambda)^{2i}]}. \tag{7}$$

IV. Application

In this section, we investigate the effectiveness of the anomaly detection methods Shewhart, CUSUM and EWMA in detecting SYN flood attacks, a comparative study is presented.

A. Description of DARPA99 dataset

The DARPA 99 dataset is one of the most important dataset used to evaluate intrusion detection systems. It has been generated 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) [20]. It presents the traffic captured in a real network which simulates the real network of a military Air Force base. Figure 3 shows the topology of such network. Machines on the left simulate the military base network (the inside network), while machines on the right simulate the Internet (the outside network). A Cisco router connects the inside and outside networks.

Victims represent servers on the Air Force base which are the targets for attacks. Pascal running Solaris 2.5, a shell or login server provides Telnet, SMTP (Send Mail Transfer Protocol), SSH (Secure Shell) and FTP (File Transfer Protocol) services. Zeno, running SunOS 4.1.4, is base file server and ran send mail and allowed file sharing between users via an FTP server. Marx, running RedHat 5.0, is the web server, it serves the Base's homepage for both the Internet and internal use (an Apache web server was used). Hume, a Windows NT 4.0 Server, was equipped with IIS, provides FTP, gopher, web servers and several other utilities includes a mail server, called MailSrv. Kant running a Windows98. The web server ,Aesop, running RedHat 5.0 is the Internet web server and appears to be thousands of individual Internet web servers. Inside and outside virtual hosts are used to spoof different IP addresses [21].

Two real workstations, one with Linux RedHat 5.0 and one with Windows NT4.0, are used as inside attackers. Three other real workstations, two with Linux RedHat 5.2 and one with Windows NT4.0, are used as outside attackers. Several types of attacks generated in this data including Denial of Service (DOS) attacks [21].

To collect the network traffic, two sniffers were setup on the network. Locke, the insider sniffer, running Solaris 2.6 and used to capture network traffic on the inside network. The outsider sniffer, Solomon, running, also, Solaris 2.6 and used to capture network traffic to and from the Air Force base. For both sniffers, the UNIX Tcpdump was used to collect the traffic. Five weeks of data were collected. Each week consisted of five days, Monday through Friday, with 22 hours each day, 8:00 a.m. to 6:00 a.m [21].

B. Detection of SYN flood attacks using Shewhart,CUSUM and EWMA:

Using DARPA 99 data, we extracted a new dataset containing only SYN segments (DARPA99/SYN). This data contains three weeks of training data and two weeks of testing data [21]. Using these data we also generate some SYN flood attacks (low intensity and high intensity). To detect SYN flood attacks using different monitoring charts, we adopted the following procedure:

(1) We use training data of DARPA99/SYN to calculate the control limits CL/UCL/LCL of Shewhart, CUSUM, and EWMA charts.
(2) For the tuning parameters of EWMA, we have used the popular choices: $L = 2.7$ and $\lambda = 0.1$
(3) For testing data, we compute the decision statistics of Shewhart (sample value), CUSUM (C_i^+ and C_i^-) and EWMA (z_i).
(4) If the obtained decision statistics exceed the control limits, then SYN flood attack is declared.

1) Case study (A)- Low intensity SYN flood attacks (LISF): In this case study we assess the detection performance of the three control charts in the presence of low intensity attacks. Indeed, low intensity attacks are characterized by low increase of number of SYN segments per observation time compared to the normal traffic situation. Here, each three hours, we introduce two minutes of low intensity SYN flood attacks (around 125 segments/observation). Monitoring results of the three charts are shown in Figure 4(a-c). Figure 4(a) shows that the Shewhart cannot detect these SYN flood attacks with low intensity. On other hand, EWMA and CUSUM successfully detect these attacks (see Figure 4(b-c)).

2) Case study (B)- High intensity SYN flood attacks (HISF): In this case study, we generated intermittent SYN flood attacks; with high-intensity of 520 segments/observation in a period of 2 minutes and repeated each 3 hours. As expected all monitoring chart can detect these attacks with high intensity (Figure 5).

3) DARPA 99 SYN flood attacks (DARPA (w5,d2)): In this case study, we compare the three charts in detecting SYN flood attacks occured on week 5, day 2 of DARPA 99 dataset [20]. There are two attacks occurred in week 5, day 2. The first starts at 11h38mn04s against Marx (@:172.16.114.50) with a duration of 13mn41s. The second was at 18h16mn05s against the router (@IP: 192.168.1.1) for 3mn26s. Monitoring results of the three charts are shown in Figure 6(a-c). The three chart can successfully detect these attacks (Figure 6(a-c)).

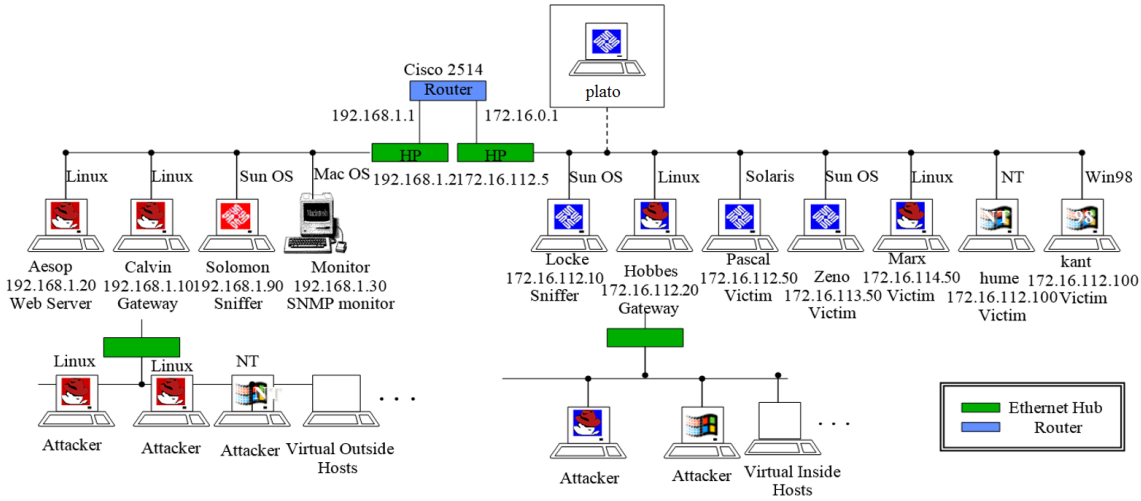

Figure 3. DARPA 99 network topology.

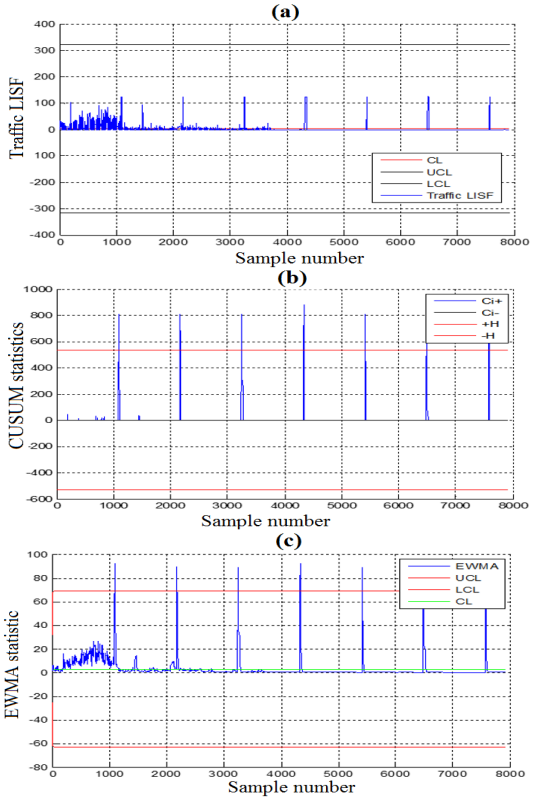

Figure 4. Detection results of Shewhart chart (a), CUSUM chart (b) and EWMA chart (c) in the presence of a low intensity SYN flood attacks.

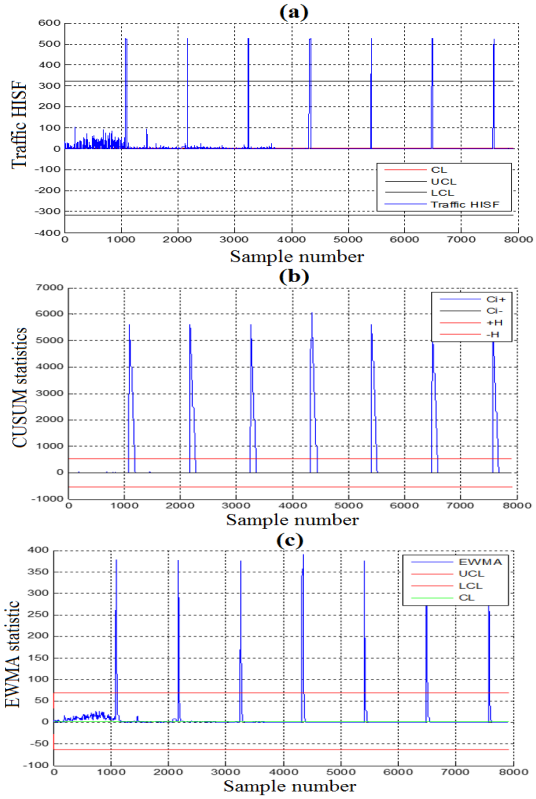

Figure 5. Results of Shewhart chart (a), CUSUM chart (b) and EWMA chart (c) in the presence of a high intensity SYN flood attacks.

In summary, results shown that Shewhart charts are well effective in detecting attacks with high-intensity (Figures 5(a) and 6(a)). However, Shewhart chart is not able to detect low-intensity SYN flood attacks (Figure 4(a)). This is mainly due to its decision based only on the actual observation. On the other hand, results also show the capacity of CUSUM and EWMA charts in detecting low-intensity SYN flood attacks (see Figures 4, 5 and 6). CUSUM and EWMA charts incorporate information from the entire process history, rather than just the most recent observations so that they are more sensitive to low-intensity SYN flood attacks.

V. Conclusion

In this paper, three univariate monitoring charts, Shewhart, CUSUM and EWMA, are used to detect SYN flood attacks. The comparison study is conducted using the 1999 DARPA dataset. Results show that Shewhart chart is suitable for detecting SYN flood attacks with high intensity. However, it

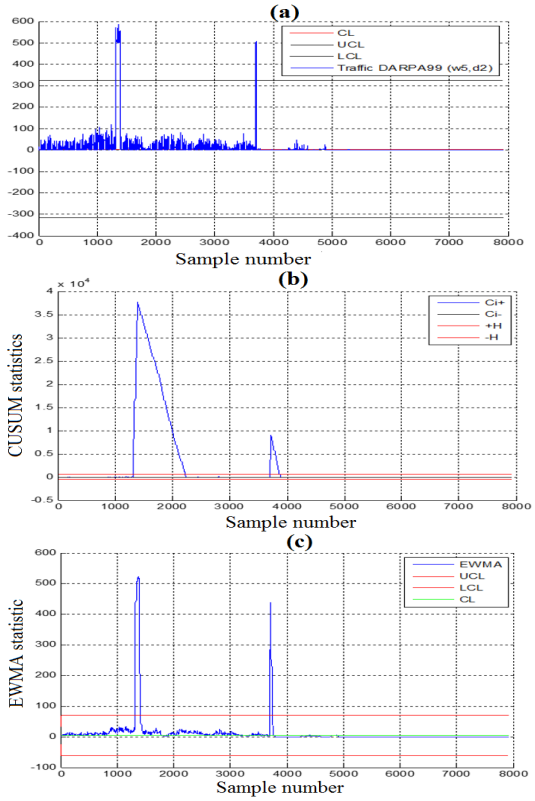

Figure 6. Detection result of Shewhart chart (a), CUSUM chart (b) and EWMA chart (c) for DARPA 99 SYN flood attack in the second day of week 5.

exhibited a poor performance in detecting attacks with low intensity. This is mainly due to the fact that Shewhart chart uses only the actual observation to make a decision about the status of the inspected network. CUSUM and EWMA schemes, which are based on a decision rule that takes into account information from past observations with that of current observations, shown an improved performance compared to Shewart chart, particularly in detecting SYN flood attack, especially for low-intensity SYN flood.

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[16] F. Harrou, M. Madakyaru, Y. Sun, and S. Khadraoui, "Improved detection of incipient anomalies via multivariate memory monitoring charts: Application to an air flow heating system," *Applied Thermal Engineering*, vol. 109, pp. 65–74, 2016.

[17] N. Zerrouki, F. Harrou, Y. Sun, and A. Houacine, "Accelerometer and camera-based strategy for improved human fall detection," *Journal of medical systems*, vol. 40, no. 12, p. 284, 2016.

[18] E. Garoudja, F. Harrou, Y. Sun, K. Kara, A. Chouder, and S. Silvestre, "Statistical fault detection in photovoltaic systems," *Solar Energy*, vol. 150, pp. 485–499, 2017.

[19] 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.

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

[21] 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.