NTDA: The Mitigation of Denial of Service (DoS) Cyberattack Based on Network Traffic Detection Approach

Muhannad Tahboush[1*], Adel Hamdan[2], Firas Alzobi[3], Moath Husni[4], Mohammad Adawy[5]
Information and Networks Systems Department, The World Islamic Sciences and Education University, Amman, Jordan[1, 3, 5]
Computer Science Department, The World Islamic Sciences and Education University, Amman, Jordan[2]
Software Engineering Department, The World Islamic Sciences and Education University, Amman, Jordan[4]

***Abstract*—Security is one of the important aspects which is used to protect data availability from being compromised. Denial of service (DoS) attack is a common type of cyberattack and becomes serious security threats to information systems and current computer networks. DoS aims to explicit attempts that will consume and disrupt victim resources to limit access to information services by flooding a target system with a high volume of traffic, thereby preventing the availability of the resources to the legitimate users. However, several solutions were developed to overcome the DoS attack, but still suffer from limitations such as requiring additional hardware, fail to provide a unified solution and incur a high delay of detection accuracy. Therefore, the network traffic detection approach (NTDA) is proposed to detect the DoS attack in a more optimistic manner based on various scenarios. First, the high network traffic measurements and mean deviation, second scenario relied on the transmission rate per second (TPS) of the sender. The proposed algorithm NTDA was simulated using MATLAB R2020a. The performance metrics taken into consideration are false negative rate, accuracy, detection rate and true positive rate. The simulation results show that the performance parameters of proposed NTDA algorithm outperformed in DoS detection the other well-known algorithms.**

Keywords—Network security; DoS attack; cyberattack; network traffic

I. Introduction

Cybersecurity has become an important issue in this era, because of continuously increasing the volume of sensitive data and valuable assets that have been targeted by cybercriminals. Therefore, it’s important to protect user information and resources by preventing cybercriminals from gaining this sensitive information [1]. The network layer is susceptible to different types of cyberattack and threats that can be used to disrupt the legitimate communications such as Denial of Service (DoS) attacks [2] that occur in online business and transaction systems. DoS attacks have become the major threat to current information security and network resources due to the deliberate exploitation of system vulnerabilities of a victim at the required time [3], [4]. DoS as the name suggests the attacker prevents or denies the services of the authorized user. Attacks can be initiated by intentionally exploiting the system vulnerabilities of a victim and overloaded with a large amount of unnecessary network traffic to occupy certain resources such as network bandwidth and memory [5], [6], disabling the proper functioning of the network and consume the victim resources as illustrated in Fig. 1.

In a denial-of-service attack, a single computer can be used to accomplish the attack. Whereas many recent DoS attacks have been launched through many malicious attempts distributed across on the internet or networks that have been infected with malware and become part of a botnet, this type of attack is called distributed denial of service (DDoS) attack [7], [8]. In DDoS, the attackers become more sophisticated and informed to destroy the target system. of occurrence way, DDoS attacks can be launched by botnet, proxy, or spoofing IP [9].

These attacks are lethal because they can bypass traditional intrusion detection systems to produce more network traffic. They have particular characteristics and traits, such as a low average rate and use of TCP as attack traffic, which allows them to avoid detection [10]. The objectives of a DoS attack can be classified as [11]:

- Consuming the network bandwidth through massive attacks by sending massive amounts of traffic.
- Consume many available resources by sending specific types of packets, so that the target system will not provide service to normal users.
- Flooding packets crash or overload the network.

Over the years, various security mechanisms have been proposed to overcome the DoS attack such as statistical-based approaches, intrusion detection system (IDS) and machine learning (ML) approaches, etc [12], but they still suffer from limitations of detection accuracy, require more learning time to produce accurate results, and increase the false negative rate.

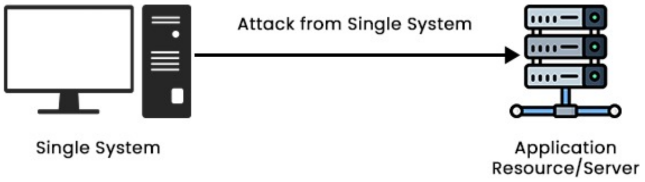

Fig. 1. Implementation of DoS attack.

To solve this problem, NTDA technique has been employed which will distinguish the legitimate traffic from attack traffic in the sense of the appropriate DoS attack based on the request message counter and mean deviation in the network traffic and then, the detection operations will determine the transmissions rate per second (TPS). To provide the requirements protection of information and to address cybersecurity challenges. Therefore, understanding how attacks evolve is an essential step in developing appropriate systems to detect and mitigate DoS attacks.

In this paper, it’s important to analyzed the data traffic behavior of the DoS attack in order to provide suggestions for DoS detection in the network environments. Furthermore, several challenges need to find a solution by the proposed NTDA algorithm. These challenges are, failing to provide higher detection accuracy and detection rate. In addition, it faces difficulty in providing a lower false negative rate. Therefore, the proposed algorithm NTDA was implemented to detect the DoS attack with an accurate level of detection to prevent this attack from sending a flood of requests to their victim host. Thus, the contributions of this study are summarized as follows:

1) First, we formulate the problem of DoS attack detection and propose a secure detection algorithm against DoS attack in the network. The NTDA can detect the attacker using various detection scenarios and improve detection accuracy.

2) The proposed algorithm employs mean deviation for each client to classify network traffic.

3) Provide a low false negative rate (FNR) due to the threshold-based detection and measure the TPS, which improves the performance and detection accuracy.

4) The performance of NTDA has been simulated and compared with a well-known DoS detection algorithm. The outcomes show that our algorithm outperforms the current compared algorithms.

The remaining of this paper is organized as follows. In Section I, will describe the introduction. Section II about the related works. Section III describes detailed information about technical preliminaries and background. Section IV shows the proposed detection algorithm. Section V describes the security analysis. Section VI provides result comparison and evaluation. Section VII is a summary. Finally, Section VIII concludes the paper.

II. Related Work

Several algorithms and myriad solutions have been developed against DoS attacks. Some of these algorithms are based on statistical approaches and others are based on machine learning approaches, etc. However, the literature will address some of the main solutions against DoS attacks and provide an illustration about the relevant literature reviewed.

Yu et al. [13] suggest DoS attack mitigation using trust management, especially using session flooding. They measured four user-specific trust metrics after each connection. The metrics are. First, short-term trust. Second, long-term trust. Third, negative trust, and fourth abusive trust. All metrics were combined to generate an overall trust score that is used to determine whether or not to accept the user's next request. After final analysis, they find out that their lightweight engine had negligible overhead and an acceptable level of throughput overhead of based on the typical number of user sessions.

The authors in study [14] carry out the DDoS detection with increased expenditure of time using non-asymptotic fuzzy estimators. The estimator is implemented based on the average package time between milestones. The problem is consisting into two parts: First for actual DDoS detection and the other for identifying the victims' IP addresses. The first part was carried out using real-time hard limits for DDoS detection. Part two, identifying victims' IP addresses is done with relatively few restrictions. The aim is to identify victims' IP addresses in time to activate further anti-intrusion applications. The affected hosts used packet arrival time as the primary statistic to determine DDoS attacks.

The research article in study [15] proposes a DoS attack detection algorithm based on the maximum likelihood criterion based on random neural networks (RNN). The detection mechanism will select a set of offline traffic characteristics to derive estimates and estimate probability coefficients. It measures the characteristics of the incoming traffic and then a decision will be made based on each characteristic. Finally, a global decision is made by employing recursive look-ahead and RNN architectures.

The authors in study [16] suggest a detection method for DoS attacks that relied on a multi-layered framework approach. The proposed system architecture consists of two parts: training set generation and real-time layer IDS. The first part uses the Knowledge Discovery and Data Mining (KDD), while the second method uses a multi-layer real-time IDS engine. Classify the packet between an attack and a normal packet. This set of modules progresses through various levels. First, the signature engine captures the packet signature and extracts features from the incoming packets accordingly. Then, based on the selected features, data is loaded from the dataset and classification is performed using the refined K-means algorithm and Naive Bayes clustering algorithm.

Dapeng Wu et al. proposed in [17] an innovative approach is proposed that can detect DDoS attacks and identify the used packets in the attack. The proposed mechanism used anti-DDoS edge system that scans traffic only on edge routers on the ISP's network. A novelty in our approach is, firstly, feature extraction based on temporal correlation and secondly, detection based on spatial correlation. Using these algorithms, our scheme can detect DDoS attacks in a more accurate manner and determine the attack packets without changing the existing IP forwarding mechanisms on routers.

III. Technical Preliminaries and Background

In this section, we will characterize the preliminary measures used in this research that are necessary to successfully achieve this research.

A. DoS Attack Models

Denial of Service (DoS) is basically a cyberattack targeting a specific server or network that is designed to prevent legitimate access from using a specific network application and its resource such as a website, web service and network system. The DoS attack flooding the victim host with a high amount of traffics at the same time [18]. In addition, DoS attacks can consume battery-powered of a mobile device in a situation of high traffic in wireless transmission. Therefore, it leads to crashing the servers or slowing them down and makes the services unavailable to legitimate users as shown in Fig. 2, where the attacker floods the website or victim with suspicious traffic to make the service unavailable [19], [20]. In DoS attack only requires a website address and/or an IP address to carry out the attack. There are various types of DoS attacks such as SYN Flood, IP spoofing DoS attacks.

1) SYN flood attack: The SYN flood or (TCP handshaking) attack is one of the most well-known DoS attacks that sends numerous false TCP connection requests, exhausting the resources of the attacked site. SYN flooding works by exploiting weaknesses in TCP protocol that are employed to establish a connection between hosts. This type of SYN flood attack is carried out through a three-way handshaking. Fig. 3 illustrates the mechanism of the SYN flooding attack. When establish a connection in TCP three-way handshaking process of TCP network connection, the SYN packets will send to the destination, it becomes in offline mode or down, then the server unable to receive ACK packets from the client after sending the SYN+ACK acknowledgment, so the server usually tries to establish the connection again and have to wait a while [21]. The uncompleted connection will be discarded, and the waiting time is called the SYN timeout. When attackers generate and use large volume of spoofed or falsifies IP addresses, it leads that the available resources of the server will be consumed due to the large number of connections, which will eventually cause an overloaded and cannot or prevent responding normally [21], [22].

2) IP spoofing DoS attacks: Assume a legitimate user willing to connect to the destination, the attacker will establish a TCP connection and mask it with his own IP address, while the normal user's IP address creates a TCP data segment with an RST bit is sent to the destination. After receiving the data, the server clears the buffer of all existing connections, considering the connection with the bad packet. If authorized users need to resend their data, they must log in again. The attacker generates many fake IP addresses by sending RST data packet to the destination, thus, no service will be provided to the legitimate users and victim's server is vulnerable to denial-of-service attacks [21], [23].

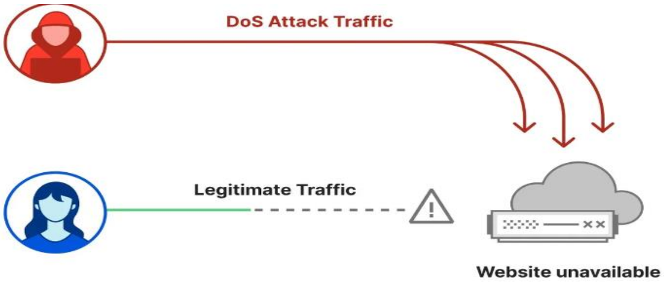

Fig. 2. DoS attack model.

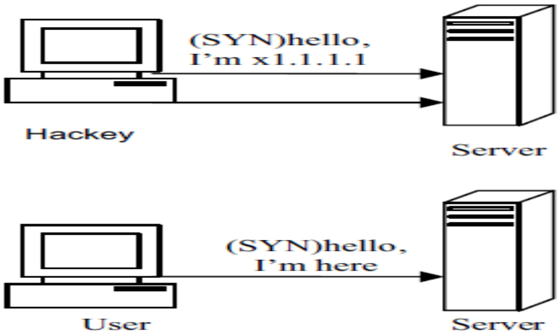

Fig. 3. SYN Flood attack mechanism.

Overall, DoS attacks rely on the direct or indirect depletion of resources on the target side by generating high traffic, resulting in outages that negatively impact service availability and continuity.

B. *DoS Traffic Behavior*

DoS attacks aim to generate an excessively large volume of network traffic to overwhelm the target. Therefore, the normal traffic is unable to be processed because large traffic significantly affects bandwidth availability and attack detection performance [21]. Therefore, it's important to recognize the DoS attack level and analyze the behavior of traffic. Moreover, during DoS attacks, a drastic change in the current traffic is observed compared to the normal traffic of the previous time interval [24]. Therefore, it's important to monitor and analyze the traffic in the network.

IV. The Proposed Detection Algorithm

The proposed network traffic detection approach (NTDA) is based on the detection of the high volume of network traffic which consists of two different scenarios applied against DoS attack to all requests that are routed to the target or centralized server. The primary scenario will use high traffic detection to be able to distinguish between legitimate traffic and high attack traffic by employing a request message counter and mean deviation, while the secondary scenario is based on the mathematical model for measuring the TPS of the sender. The procedures of the proposed algorithm are presented as follows.

Step 1: Employ a Request Message Counter (RMC) that increases one when the server receives the same RM from the same user.

Step 2: After that, a mean deviation technique is used to detect abnormal or high network traffic from a single IP address to classify the existence of high traffic.

Step 3: Determine the existence of an attack by applying the threshold value and TPS for DoS attack.

A. *Assumptions*

This section presents some assumptions about the network connections and adversarial capabilities of the proposed research in NTDA.

Assumption 1: The communications architecture will be based on TCP/IP for information exchange.

Assumption 2: Attacker establishes only one connection towards a victim host.

Assumption 3: The attacker does not implement any address spoofing mechanisms.

Assumption 4: Our proposed approach achieves high detection accuracy in DoS attacks in real-time without requiring hardware components.

B. Detection Based on Network Traffic

The primary scenario is based on high traffic detection and analysis the network congestion to distinguish between normal data traffic from large attack traffic. The attacker needs to flood the target with a large volume of requests to break down the effectiveness of a network by disconnecting the host, bandwidth depletion and making websites and remaining online resources unavailable to legitimate users. The detection starts when the user sends a request message (RM) containing user identification (UID) for a certain period (Pc) to the target server (TS). Then, the TS receives the RM and checks the message status if it is normal or abnormal by the following steps:

1) Each user in the network has a request message counter (RMC) that increases by "one" when the TS receives the same RM from the same user as shown in Eq. (1).

$$RMCi = RMC_i + 1 \tag{1}$$

2) Based on the value of (RMC*i*) in Eq. (1), the TS calculates the meaning of the number RM received from all clients for a certain period as in Eq. (2).

$$MRM = \frac{\sum_i^N (RMCi)}{N} \tag{2}$$

3) Then, the TS calculates the mean deviation for RMC for all available clients, thus using Eq. (1) and Eq. (2) to find the MDi as in Eq. (3).

$$MDi = |\, RMCi - MRM \,| \tag{3}$$

4) Finally, the TS decides the status of RM is normal when the specific RMC is away from the mean and the attack does not exist, while the status of RM is abnormal when the specific RMC is close to the mean, it means an abnormal rise in incoming network traffic. Then the TS will block the suspicious IP source address from accessing the network. The detection of high-traffic pseudocode shown in (Algorithm 1).

Algorithm.1: Pseudocode for high traffic detection

```
Input: RMC
Output: Classified the data traffic, normal or abnormal.
Start
    Determine Pc
    While (Pc != 0) {
    Client i send RM that contains UID to TS during Pc
    TS receives RM and determines client sender.
    RMCi = RMCi + 1
    }
    $M_{RM} = \frac{\sum_i^N (RMCi)}{N}$
    MDi = | RMCi – $M_{RM}$ |
    If (RMCi >> $M_{RM}$)  then {
        RM transmitted from client i is normal.
        DoS_Detected = FALSE
    } Else
    If (RMCi  <<  $M_{RM}$ ) then {
        RM transmitted from client i is abnormal.
        IP address is added to the suspected list
        Go to Algorithm 2
    }
End
```

However, DoS attacks generate an unusual and excessively high volume of attack traffic in order to overwhelm the target or victim. Algorithm 1 is responsible for determine the behavior and classification of the incoming packet weather high or normal traffic to provide an accurate DoS detection schema. However, if the attacker has been detected through (Algorithm 1), the IP address will be added to the suspected list and the detection processes will move to the (Algorithm 2). Otherwise, if the attacker cannot be detected, the IP address is classified as a trusted IP address list.

C. Detection Based on Transmission Rate

To illustrate this secondary scenario that plays an important role in the proposed NTDA algorithm, it's an important aspect to identify several requests toward the victim host. This scenario relied on the requests from the source IP address. Continuing with the previous detection scenario, it’s important to recognize the number of transmissions rate per second (TPS) toward the destination victim to distinguish the type of incoming packet. Therefore, it’s important to determine the workload of individual servers for websites. It has been found that the number of transmissions toward the victim server can be taken into consideration. Thus, to classify the transmission requests, the average attack rate is considered in the detection algorithm as the threshold value as illustrated in Algorithm 2.

Algorithm.2: DoS Detection Process

```
Input: TPS value, IP Address
Output: determination of high traffic, DoS detection.
Start
    Detection Operation of DoS attack
    If (TPS > threshold value) then
        DoS_Detected = TRUE
    Else
        DoS_Detected = FALSE
    Add IP address to the trusted list
    End
End
```

However, after a high traffic detection scenario toward the destination victim as clarified in (Algorithm 1), the detection process will continue with the secondary scenario and the IP address will be added to the suspected record list. The process starts when comparing the TPS to the threshold value to find out the existence of DoS attack in the requests process. If the TPS is higher than the threshold value, it means that many attack packets are generated toward the destination and the attack exists in the request processes. However, when the TPS is lower than the threshold value, the request operations are coming from legitimate source and DoS attack does not exist. Thus, the IP address will be added to the trusted list. As shown in the Eq. (4) if we assume that X=TPS.

$$F(TPS) = \begin{cases} 1, & TPS \geq Threshold, \\ 0, & TPS < Threshold, \end{cases} \quad (4)$$

where, F (TPS) is DoS_Detected.

However, by taking advantage of the proposed algorithm, DoS attacks can be overcome by mitigating the attack and this confirms our claim that a DoS attack is still a critical threat and can stop the services of the legitimate users.

D. Threshold-based Detection

The idea of employing threshold value in the algorithm is that the attack is declared when the rate of transmission become higher than threshold, otherwise, declare attack does not exist. Note that the second scenario of the discovery process is performed on the sender side. By varying the feature value threshold, we can obtain different values of false negative probability and detection probability. The threshold value will be compared with TPS in the secondary scenario. The threshold was selected based on the number of users who targeted the server as well as the number of requests required for each user. Therefore, to count the number of requests for each user (*i*), it will be calculated using Eq. (5).

$$NoRi = NoRi + 1. \quad (5)$$

where, NoR*i* is the number of requests for each user (*i*), the following formula is used to calculate the threshold.

$$\text{Threshold} = \frac{\sum_{i=1}^{n} NoR\_i}{n} \quad (6)$$

where, n is the number of users who target the server (requests sent to the server). Thus, the threshold value varying depending on the number of users and request toward the target that obtained by using Eq. (6).

V. Security Analysis of the Proposed Detection Algorithm

(DoS) attack is a type of cyberattack that consider as the most threatening list of dangerous attack due to its ability to overload the network resources and lead to the shutdown of the services from legitimate users. In addition, DoS attack has major negative effect of WSN and mobile node for consuming their limited battery [19], [26]. Due to the proposed various detection scenarios, NTDA can prevail over security breach which allow the assailant to exploit it and access the network and distort its behavior. In reference to the second scenario of detection that has been designed to ensure the existence of DoS attack, which is considered as continuing of the primary scenario. All IP addresses that are contained in the suspected list will be examined through the secondary scenario to complete their detection against DoS attacks [25]. These results activate detection even through the operational phase of the network. In this part, an analysis carried out of the NTDA security against DoS attacks.

VI. Results Comparison and Evaluation

This section presents the performance evaluation and accuracy of the detection method NTDA against DoS attack. The proposed experiments have been implemented using MATLAB R2020a environment. The performance parameters that will be used to evaluate the proposed algorithms and analyze the detection system performance is false negative rate, detection rate, true positive rate and accuracy. To evaluate the effectiveness of the detection system NTDA algorithm, we compare its performance with most common detection algorithm under DoS attack.

A. Detection Accuracy

One of the important parts of detection, it is the percentage of the total number of attacks that has been labeled and actually detected of packets as illustrated in Eq. (7).

$$Accuracy = \frac{TP}{TP+FP} \times 100 \quad (7)$$

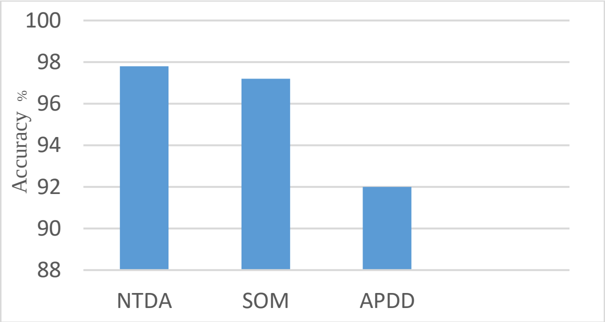

Fig. 4. Detection accuracy.

In Fig. 4, shows the detection accuracy graph of the proposed algorithm compared with SOM [27] and APDD [28] detection algorithms, it has been found that the accuracy test significantly increases and rises up to (97.8 %) as compared with other algorithms. The reason behind that, is the smallest amount of threshold value will reduce the suspicious requests toward the victim and enables the NTDA to recognize the modification of the attacker identities and lower false negative rate, whereas the SOM and APDD are based on traffic flow features and detection in big data that lead to higher delay and have lower detection accuracy. Moreover, SOM technique has limited detection throughput which will reduce the accuracy against DoS attacks.

B. False Negative Rate (FNR)

The false negative rate is the proportion of infected packets that are falsely considered or detected as safe or legitimate packets as illustrated in Eq. (8). A false negative was considered more threatening than a false positive, due to the removing a false positive link will lead in losing a valid communication link without compromising security. Thereby, a false negative makes the network insecure.

$$FNR = \frac{TPR+TNR}{ALL} \times 100 \quad (8)$$

where, All = TPR+TNR+FPR+FNR

Fig. 5 shows the false negative rate (FNR) of the proposed algorithm. The NTDA shows the lowest value and decreases slowly to reach zero in FNR compared with other algorithms as in [27] and [29] which makes the NTDA perform well and efficiently in detection process. The reason behind that is that the smallest optimal threshold value that was used in the secondary scenario can reduce the FNR. Thus, NTDA improved its performance in the FNR compared with other algorithms.

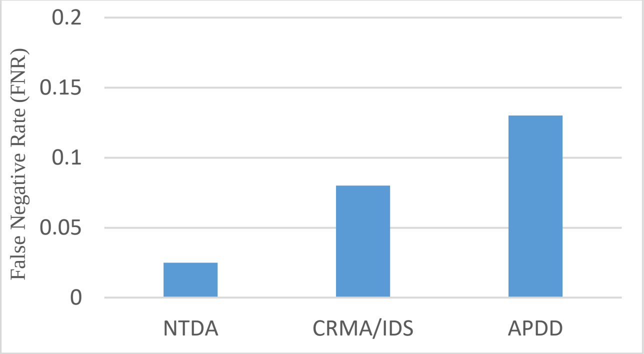

Fig. 5. False negative rate.

C. Detection Rate (DR)

DR represents the ratio between the number of detected threat packages and the actual number of threat packages. Thus, high detection rate provide large number of malicious packets can be detected as defined in the next Eq. (9).

$$Detection\ Rate = \frac{TP}{TP+FN} \times 100 \qquad (9)$$

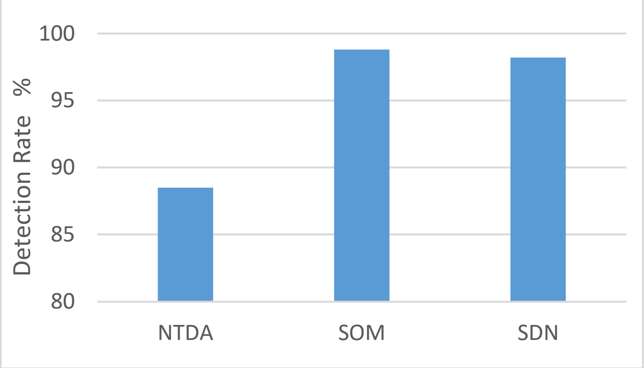

Fig. 6. Detection rate.

Fig. 6 shows the performance appraisal rate of successfully achieved detected DoS for NTDA algorithm and its effectiveness against given attacks. NTDA rigorously enforced proved a successful high detection rate (89%) which is considered an acceptable rate of detection in comparison with [27] and [30] that has slight increase in the detection rate. The reason behind that is due to the low delay and FNR that keep the performance of the proposed approach about 89%, Therefore it is intelligible that the proposed security system has an expectant DoS detection rate.

D. True Positive Rate (TPR)

The True Positive Rate (TPR) value is obtained from the number of DoS attack data that is successfully detected or classified as an attack as illustrated in Eq. (10). Thus, TPR has an effect on measuring the performance of the proposed method.

$$TPR = \frac{TP}{(TP+FN)} \qquad (10)$$

The proposed algorithm NTDA worked as expected, and the generated true positive rate (TPR) is compared with other algorithms such as [29] and [28]. Fig. 7 shows that the NTDA proposed algorithm provide slightly a higher true positive rate compared with other detection algorithm which gives sufficient improvement in detection over other algorithms. This is because the system has the ability to detect DoS with a high percentage of malicious packets.

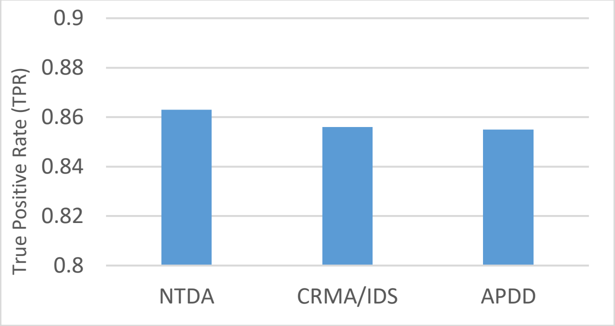

Fig. 7. True positive rate.

VII. Summary

In this part, it's important to present the efficiency and performance of the NTDA in a network environment that was analyzed using MATLAB R2020a. The proposed NTDA algorithm was compared with the most common DoS detection algorithms in terms of false negative rate, accuracy, detection rate, and true positive rate as well when exposed to several attack instances. The experimental outcomes can be concluded as follows:

1) The NTDA algorithm provides detection accuracy approximately of 98% compared with other algorithms that have lower accuracy.

2) The NTDA provides a lower value of false negative rate that plays an important role in preventing leaving the network insecure. The value of FNR is close to zero because of the smallest value of the threshold.

3) The NTDA provides the highest value of TPR compared with other algorithms and it has the ability to detect the real attackers and distinguish normal and abnormal network traffic.

VIII. Conclusion

This research examines the adversarial impact on network resources of DoS attacks as one of the major threats to cybersecurity as well as to ensure sustainable and secure systems. Attack traffic traces are suitable for evaluating DoS detection security systems. Network Traffic Detection Approach (NTDA) has been proposed to provide accurate detection and mitigation for DoS attacks. The detection algorithm is based on two various scenarios, the primary scenario will detect the network's high traffic measurements and the secondary scenario uses mathematical models to detect suspicious traffic using transmission rate of the sender. The simulation outcomes have intelligibly proved that the NTDA detection algorithm has higher detection performance, efficiency and accuracy. The NTDA detection method ensures that the DoS attack is combated. However, the proposed NTDA algorithm generally outperformed other detection methods. In the future, focusing on other approaches that provide significant flexibility and additional accurate detection performance in networks that are based on various features.

REFERENCES

[1] S. Suresh and V. K. Kiran, “Prevention of Dos and DDoS Attack Using Cryptographic Techniques,” pp. 93–96, 2016, doi: 10.17148/IJARCCE.

[2] S. Sinha and K. G, "Network layer DoS Attack on IoT System and location identification of the attacker," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 22-27, doi: 10.1109/ICIRCA51532.2021.9545071.

[3] M. Tahboush, M. Agoyi, and A. Esaid, “Multistage security detection in mobile ad-hoc network (MANET),” Int. J. Eng. Trends Technol., vol. 68, no. 11, pp. 97–104, 2020, doi: 10.14445/22315381/IJETT-V68I11P213.

[4] K. Nagesh, R. Sumathy, P. Devakumar, and K. Sathiyamurthy, “A Survey on Denial of Service Attacks and Preclusions,” vol. 11, no. 4, pp. 1–15, 2017, doi: 10.4018/IJISP.2017100101.

[5] Q. Gu and S. Marcos, “Denial of Service Attacks Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline,” pp. 1–28.

[6] Almomani, Omar. "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms." Symmetry 12, no. 6 (2020): 1046.

[7] V. Zlomislić, K. Fertalj, and V. Sruk, “Denial of service attacks: An overview,” 2014, doi: 10.1109/CISTI.2014.6876979.

[8] Almomani, Omar. "A Hybrid Model Using Bio-Inspired Metaheuristic Algorithms for Network Intrusion Detection System." Computers, Materials & Continua 68, no. 1 (2021).

[9] X. Jing, Z. Yan, X. Jiang, and W. Pedrycz, “Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch,” Inf. Fusion, vol. 51, pp. 100–113, 2019, doi: 10.1016/j.inffus.2018.10.013.

[10] H. P. Alahari, “Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT,” no. Icisc, pp. 72–81, 2019.

[11] M. Salunke, R. Kabra, and A. Kumar, “Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm,” pp. 372–377, 2015.

[12] Smadi, sami, mohammad alauthman, omar almomani, adeep saaidah, and firas alzobi. "Application layer denial of services attack detection based on stacknet." Int. J 3929, no. 3936 (2020): 2278-3091.

[13] J. Y. C. Fang and L. L. Z. Li, “Mitigating application layer distributed denial of service attacks via effective trust management,” vol. 4, no. April, pp. 1952–1962, 2010, doi: 10.1049/iet-com.2009.0809.

[14] S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, “Real time DDoS detection using fuzzy estimators,” Comput. Secur., vol. 31, no. 6, pp. 782–790, 2012, doi: 10.1016/j.cose.2012.06.002.

[15] O. Lay, “A Denial of Service Detector based on Maximum Likelihood Detection and the Random Neural Network,” vol. 50, no. 6, 2007, doi: 10.1093/comjnl/bxm066.

[16] K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, “Robust and efficient detection of DDoS attacks for large-scale internet,” vol. 51, pp. 5036–5056, 2007, doi: 10.1016/j.comnet.2007.08.008.

[17] A. Prakash, M. Satish, T. S. Sai, and N. Bhalaji, “Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture,” vol. 87, pp. 275–280, 2016, doi: 10.1016/j.procs.2016.05.161.

[18] Z. Li et al., "Denial of Service (DoS) Attack Detection: Performance Comparison of Supervised Machine Learning Algorithms," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Calgary, AB, Canada, 2020, pp. 469-474, doi: 10.1109.

[19] M. Tahboush, M. Adawy, and O. Aloqaily, “PEO-AODV : Preserving Energy Optimization Based on Modified AODV Routing Protocol for MANET,” vol. 15, no. 2, 2023, doi: 10.15849/IJASCA.230720.18.

[20] A. Sanmorino and S. Yazid, “DDoS Attack Detection Method and Mitigation Using Pattern of the Flow,” pp. 12–16, 2013.

[21] L. Jingna, "An analysis on DoS attack and defense technology," 2012 7th International Conference on Computer Science & Education (ICCSE), Melbourne, VIC, Australia, 2012, pp. 1102-1105, doi: 10.1109/ICCSE.2012.6295258.

[22] V. Bukac and V. Matyas, “Analyzing traffic features of common standalone DoS attack tools, Conference: Security, Privacy, and Applied Cryptography Engineering, 2015, vol. 9354, pp. 21–40, doi: 10.1007/978-3-319-24126-5_2.

[23] Mohammad, Adel Hamdan, Tariq Alwada'n, Omar Almomani, Sami Smadi, and Nidhal ElOmari. "Bio-inspired hybrid feature selection model for intrusion detection." Computers, Materials and Continua 73, no. 1 (2022): 133-150

[24] Z. Li et al., “Denial of Service (DoS) Attack Detection : Performance Comparison of Supervised Machine Learning Algorithms,” pp. 469–474, 2020, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00088.

[25] Smadi, sami, mohammad alauthman, omar almomani, adeep saaidah, and firas alzobi. "Application layer denial of services attack detection based on stacknet." Int. J 3929, no. 3936 (2020): 2278-3091.

[26] Aslan, Ömer & Aktug, Semih & Ozkan Okay, Merve & Yılmaz, Abdullah & Akin, Erdal. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 2023, 12. 1-42. 10.3390/electronics12061333.

[27] R. Braga, E. Mota, and A. Passito, “Lightweight DDoS flooding attack detection using NOX/OpenFlow,” Proc. - Conf. Local Comput. Networks, LCN, no. October, pp. 408–415, 2010, doi: 10.1109/LCN.2010.5735752.

[28] X. Liu, J. Ren, H. He, B. Zhang, Q. Wang, and Z. Zheng, “All-Packets-Based Multi-Rate DDoS Attack Detection Method in ISP Layer,” Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/7551107.

[29] H. Bai, X. Zhang, and F. Liu, “Intrusion detection algorithm based on change rates of multiple attributes for WSN,” Wirel. Commun. Mob. Comput., vol. 2020, 2020, doi: 10.1155/2020/8898847.

[30] R. Durner, C. Lorenz, M. Wiedemann, and W. Kellerer, “Detecting and mitigating denial of service attacks against the data plane in software defined networks,” 2017 IEEE Conf. Netw. Softwarization Softwarization Sustain. a Hyper-Connected World en Route to 5G, NetSoft 2017, 2017, doi: 10.1109/NETSOFT.2017.8004229.