An Adaptive Multi-layered Approach for DoS Detection and Mitigation

Sowmya Ramesh, Subhiksha Selvarayan, Kanishq Sunil, and Chamundeswari Arumugam(✉)

Department of Computer Science and Engineering,
Sri Sivasubramaniya Nadar College of Engineering, Chennai, India
{sowmya18159,subhiksha18172,kanishq17069}@cse.ssn.edu.in,
chamundeswaria@ssn.edu.in

Abstract. A Denial of Service (DoS) attack imposes a heavy load on a system rendering it unavailable to the benign traffic. One of the most popular approaches to carry out the attack is to send a multitude of requests to the targeted site or network, causing the host or network to become unable to reply to the benign traffic or to respond slowly. The complexity and frequency of these attacks have been increasing in recent years. Hence, there is a need to design an efficient system that would detect any suspicious activity in the network and dispatch a timely and appropriate response to counter the same. In this paper, different design models and implementations of contemporary intrusion detection systems have been reviewed and analyzed for shortcomings. A multi-level design for an Intrusion Detection and Prevention System (IDPS) that aims to efficiently detect the DoS attack with minimal response time and high accuracy has been proposed. A UDP flood is simulated inside a virtual network environment to emulate the attack and the results demonstrate the successful detection and mitigation of the DoS attack.

Keywords: Denial of Service (DoS) · UDP flood attack · Intrusion Detection System · IDPS · Virtual network

1 Introduction

The Internet has transformed the way people communicate today. The facilities they provide are easy to use even though a large number of people are using them for their day-to-day activities [1]. The services they provide have extended to banking transactions, medicine, education, research, etc. The exponential growth in technology has also made them the primary targets for cyberattacks [2]. Security is a sensitive issue for all organizations and institutions as malicious users can exploit the design weaknesses of the network and steal confidential information making the organization lose millions of dollars [3]. Security threats like Denial of Service (DoS) attacks have profound effects on the server. They work by overwhelming the target's resources, making it unavailable to provide its intended

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12957, pp. 533–545, 2021.
https://doi.org/10.1007/978-3-030-87013-3_40

services for legitimate users [4]. Different open-source software and toolkits are made available to attack the target with fewer resources [5]. The attack is often challenging and complex to detect as they mimic legitimate traffic and downgrade the server [6]. Thus, a secure network is essential to uphold the safety and security of all services provided through the Internet. An Intrusion Detection Prevention System(IDPS) is a combination of both IDS(Intrusion Detection System) and IPS (Intrusion Prevention System). An IDS is a system that identifies suspicious network traffic, which cannot be detected by the traditional firewall, based on available data about previous attack history [7,8]. The attacks can be adversarial intrusions against IDS or simply a set of actions that violate the security policies associated with the IDS itself [9]. The IPS system can block the attack/threat in addition to detecting them [10].

The four common types of IDPS: Network-Based, Wireless, Network Behaviour Analysis System, and Host-Based IDPS are discussed in detail in [11]. A signature-based IDPS matches the signature of known attacks that have already been stored in the database and then identifies the attacks [12]. An anomaly-based IDPS first records the incoming traffic and details of normal traffic of the system [13].

A host-based IDPS system has been implemented that uses signature-based methods to detect abnormalities. The IDPS presented in this paper is capable of efficiently detecting and mitigating the attack. The type of DoS attack demonstrated in this paper is the User Datagram Protocol(UDP) flood attack. This volumetric DoS attack floods the server with UDP packets on either random or specified ports [14]. The server soon exhausts its resources by trying to process and reply to the overwhelming requests making it impossible to process legitimate traffic. The solution also compares the results with various previous solutions.

The rest of the paper has been organized as follows: Sect. 2 reviews the existing work and research done in this field. Section 3 presents the proposed methodology for the implementation of the Intrusion Detection and Prevention System. Section 4 presents the experimental results and performance evaluation of the proposed work. Finally, Sect. 5 provides the concluding remarks and gives some insight into future work.

2 Literature Survey

M. Nenova et al. [15] proposed a design for an IDS system based on some open-source IDS and IPS systems and they have tested the system designed against two common attacks, SQL injection and SYN flood attack. They have also performed bandwidth traffic analysis on the snort IDS and analyzed different firewall policies. They have used snort IDS and IPS software blade integrated with check point security Gateway to provide another layer of security in addition to the check point firewall technology. They have simulated the attack using web servers and FTP servers to carry out the tests. The signature for an SYN flood attack had been included in the IPS system and they have thus succeeded in

preventing the DOS attack as soon as it is detected. This solution relies heavily on the firewall system and the open-source technologies being used here since all the incoming packets are routed through the firewall using NAT. A successful attack on the firewall entry point or any downtime could lay the network bare to malicious activity.

M. M. Shurman et al. [16] proposed a hybrid design that combines a signature-based IDS and an anomaly-based IDS which monitors user behavior and classifies the network packets to detect DoS attacks as soon as it commences. The hybrid approach has a lot of benefits since signature-based IDS has a fast detection period but it can't detect unknown attacks like the anomaly-based IDS. Signature-based IDS also compensates for the high false-positive rate of the anomaly-based system. In their system, they relay the incoming traffic to the anomaly-based detector only if the incoming traffic pattern does not match any known attack signatures. The anomaly-based detector also adds the signature of an attack that it detects to the database thus enabling the system to detect the attack sooner the next time it repeats. As mentioned before, the anomaly-based detector could cause the overpopulation of the database with false-positive signatures and prevent valid attack signatures from getting stored in the database.

A. A. Titorenko et al. [17] examined the influence of different DoS attacks on Network Intrusion Detection Systems (NIDS) and proposed methods for strengthening the resistance to these attacks. As DoS and DDoS attacks are unpredictable, they complicate the development of prompt countermeasures. To improve the functioning of the IDS, they collected the percentage distribution of different kinds of attacks against IDS snort with default settings. Based on the received data, they proposed a mathematical model capable of selecting the configuration which will maximize the probability of successful attack detection and minimize false positives. The model was developed based on game theory which uses Hurwitz and Wald criterion for making decisions. They have also developed and presented the criteria for evaluating attack detection performance. If the necessary statistical data related to a particular situation is available, then the model developed will significantly increase the performance and fault tolerance of the IDS.

M. T. Kurniawan et al. [18] proposed a signature-based IDS that adopts a blocking approach that blocks all the packets from the attacker until the attacker cannot generate more packets. They implemented the IDS on a Wireless Sensor Network (WSN) that is vulnerable to DoS attacks. They have adopted the RREQ_RATELIMIT (Route Limit) calculation scheme for the implementation and blocking approach. The attack packet gets dropped when there is a DoS attack, then the RREQ (Route Request) request exceeds RREQ_RATELIMIT, which is 10 packages per second based on RFC. An RREQ_ACCEPT_LIMIT is set to not change the RREQ_RATELIMIT to a higher value. When RREQ exceeds RATE_ACCEPT_LIMIT, the request gets rejected. They have used the Quality of Service (QoS): delay, packet loss, throughput, and energy to determine the performance of the WSN in different scenarios.

Researchers have also worked on extending the protection offered by IDS to the cloud. This area has seen designs for various hybrid systems that combine signature-based and anomaly-based detection strategies come up. Kumar et al. [19] proposed a hybrid system that employs a packet sniffer, a feature extractor, and an SVM classifier to detect different flood-based DoS attacks in virtual machines hosted in a cloud environment. In his paper [20], Shubhra Dwivedi has proposed an IDS system which they called GOIDS. It selects features using Grasshopper Optimization Algorithm(GOA) and passes them to different classifiers to classify the attack. They have evaluated their model on the KDD and CIC-IDS datasets, widely used by many researchers working on anomaly-based detection strategies. Odusami et al. [21] proposed an anomaly-based detection strategy using LSTM to detect DDoS attacks on web servers. Another work that uses an LSTM based approach [22], where a hybrid model combined with CNN for weights training has been employed. Abushwereb et al. [23] compared the performance of various machine learning classifiers in detecting different types of DoS attacks. Kim et al. [24] proposed a way to create attack images by transforming numerical features like destination port and protocol type into grayscale and RGB images. Further, they employed a CNN model to classify the attacks based on the attack image.

Table 1 summarizes the existing work related to IDS. Extensive research has also been done to identify the shortcomings of the IDS system. One of the most commonly reported problems is that the system goes into action well after the system/service performance degrades or after it has become unavailable. Dos attack, in particular, is a huge threat because it is hard to determine the scale of the attack and take necessary measures to prevent it.

Table 1. Comparison of existing works and their detection methodology

Paper	SIDS	AIDS	Hybrid IDS	Detection strategy
M. Nenova et al. (2019)	✓	✖	✖	Signature based IPS system that uses open source intrusion detection software and tested against SQL injection and SYN flood attacks
M. M. Shurman et al. (2019)	✓	✓	✓	Incoming traffic is sent to the anomaly detector only if no matches are found in the known attack signature database
M. T. Kurniawan et al. (2020)	✓	✖	✖	Implemented a blocking approach based on RREQ rate limit to mitigate DoS attacks on a Wireless sensor network
Dwivedi et al. (2020)	✖	✓	✖	Anomaly based IDS that uses grasshopper optimization algorithm along with the C4.5 decision tree classifier
M Odusami et al. (2019)	✖	✓	✖	Proposed an LSTM based detection model to detect both low rate and high rate layer seven DDoS attacks with high accuracy and low false positive rate
Kim et al. (2020)	✖	✓	✖	CCN based detection model that performs binary and multi-class classification
Abushwereb et al. (2020)	✖	✓	✖	Compared the detection rate of various machine learning classifiers in detecting different attacks.TCP-SYN attacks were found to have the lowest detection rate
Smys et al. (2020)	✖	✓	✖	Proposed a hybrid model that combines an LSTM and CNN model to achieve a detection accuracy of 98%

3 Proposed Methodology

This paper proposes a new type of IDPS system that takes into consideration a lot of factors before disallowing access to the source host of a packet. The experiment has been carried out on an Ubuntu 20.04 Long Term Support (LTS) virtual machine. The hypervisor that was used for the experiment is VirtualBox and a network emulator, mininet, was used as the testbed to simulate different

variations of the DoS attack. The IDS system has been tuned to an optimal configuration based on the results of the experiment. All experiments have been tested on 3 hosts + Switch configuration. Figure 1 shows the network topology configured in mininet.

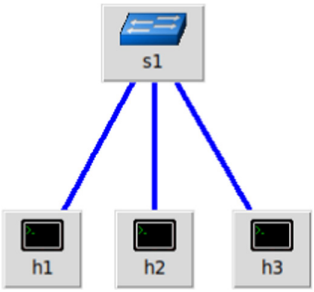


Fig. 1. Simulated network topology using mininet

The above topology has been simulated using mininet, which allows for rapid prototyping and experimentation of network configurations through its light virtualization technology. The virtual networking components and hosts support OpenFlow protocol for advanced routing use cases, but the experiments carried out in this paper use the legacy switch. Figure 2 shows the IP address of the host h3 being set. It also provides various other customization options like delay, bandwidth, loss %, and maximum queue size.

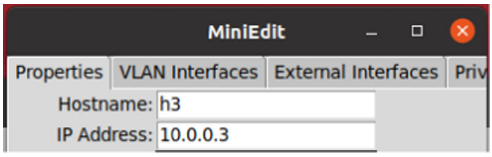


Fig. 2. Setting IP address for a host in the virtual network

The 3 hosts in the network topology have 3 different roles. Host node, h1, is the attacker. h2 takes on the role of the victim node and h3, which is of interest to us, is where the IDPS system is set up to act as a firewall. All packets that need to be sent to the victim node have to be routed through the IDPS system which allows us to perform packet filtering and analysis at h3. Figure 3 shows the high-level overview of the proposed IDPS.

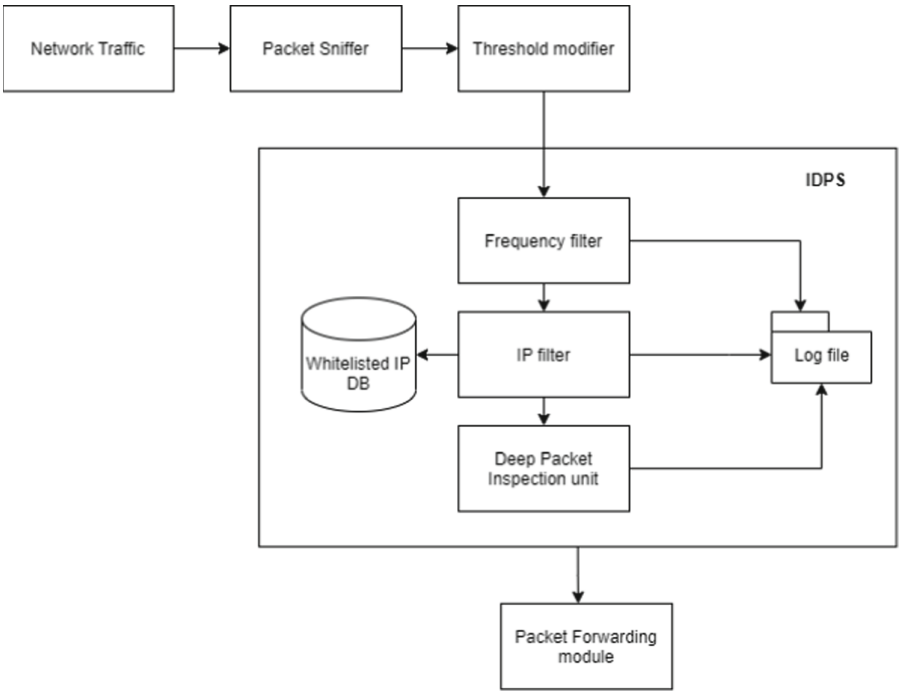


Fig. 3. Proposed design of intrusion detection and prevention system

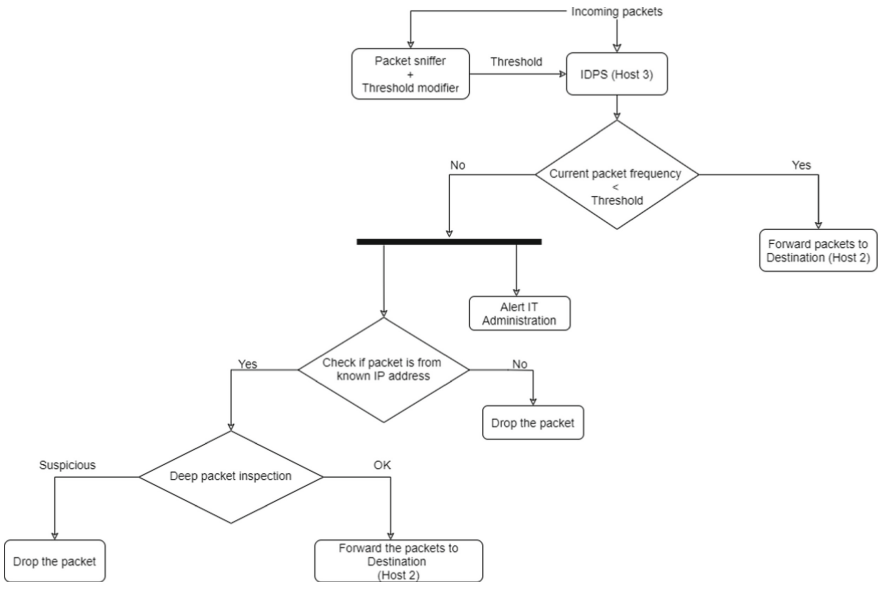


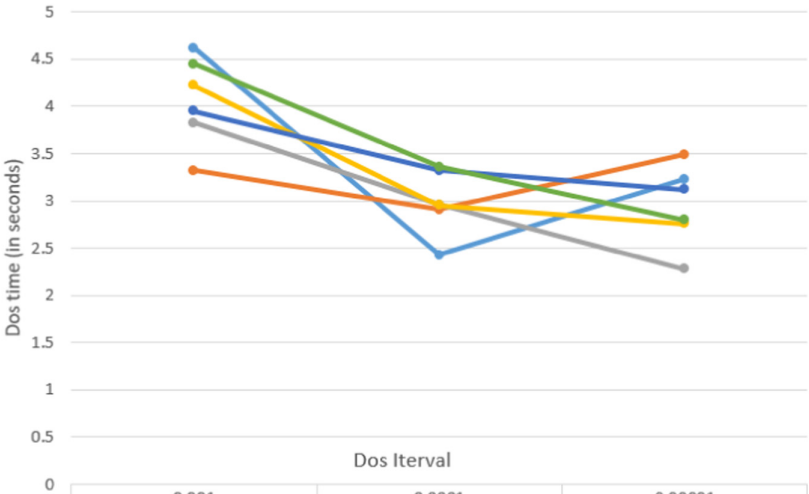
Fig. 4. Flowchart of adaptive multi-level approach

Figure 4 represents the flow of control within the IDPS system. The threshold modifier component calculates the incoming packet frequency at predefined intervals of time and updates the value for the allowed frequency threshold in the IDPS configuration. Since DoS detection by inspecting the frequency parameter alone can be inflexible and inaccurate at times, this dynamic threshold calculator will help to make adjustments according to a system's peak and off-peak hours, making the system adaptive to its network environment. If the frequency exceeds the set threshold, an alert is sent to the IT administrator and the packet undergoes further inspection. The source IP address of the packet is compared against a whitelist consisting of known and trusted IP addresses. On the occasion that it does not match, the packet gets dropped and the particular IP address is blocked until the administrator reviews the log file and decides on the further course of action. But if a match is found, it further undergoes Deep Packet Inspection (DPI) where the packet's header information and the payload are scrutinized thoroughly. If it gets classified as suspicious, the packet gets dropped, else it is forwarded to its destination.

4 Results and Discussion

After all the configurations have been made to the mininet virtual network, the python script for the IDPS is run on host 3, and the script for simulation of DoS attack is run on host 1. The attacker uses the packet manipulation library in python, scapy, to carry out the DoS attack by sending a flood of UDP packets. Scapy allows us to specify an "inter" parameter which represents the waiting time between two successive attack packets. The attack is simulated by varying this parameter.

Figure 5 illustrates the results observed when the DoS interval was varied over 6 iterations. Here, the DoS time refers to the amount of time (in seconds) it takes to reach 100% CPU utilization. It can be observed from the figure that as the interval decreases, the DoS time slumps for the interval - 0.0001 after which further decrease leads to erratic results as can be seen from the graph for the case of the last interval of 0.00001. Thus, the interval for the UDP flood has been set to the optimum value of 0.0001 after experimenting with different values.



	0.001	0.0001	0.00001
Iteration 1	4.62	2.43	3.23
Iteration 2	3.32	2.91	3.49
Iteration 3	3.83	2.96	2.28
Iteration 4	4.22	2.95	2.76
Iteration 5	3.95	3.32	3.12
Iteration 6	4.45	3.36	2.8

Fig. 5. Variation of DoS time with respect to DoS interval

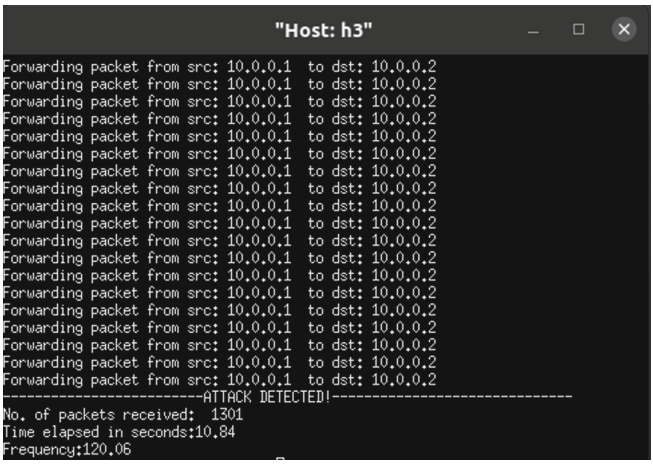


Fig. 6. IDPS attack detection

Figure 6 shows packets from the source routed to the destination through the IDPS (host 3). The IDPS checks if the frequency of the incoming packets is lesser than the threshold. The packets forwarded to the destination are the ones with frequency lesser than the threshold. If the frequency is higher, the IDPS flags the packet and sends it to the second level for further processing. It was observed that the dynamic frequency filter was able to adjust well to the different proportions of traffic. Around 60–70% of the malicious packets flagged by the first level were blocked successfully in the whitelisted IP filtering level. Only very few packets that employed IP spoofing techniques were able to make it to the final level. And in the final level, the packets get inspected thoroughly to detect whether it is malicious or not. The packets that get flagged as malicious are dropped and the IDPS system is successful in breaking the communication between the attacker and the victim.

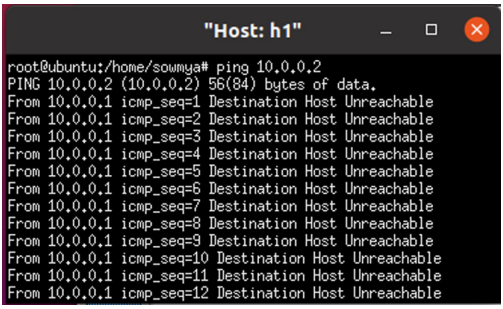


Fig. 7. Blocking of attacker's IP address

As it can be seen from Fig. 7, host h1's IP address has been blocked and it's now unable to send packets to the victim node.

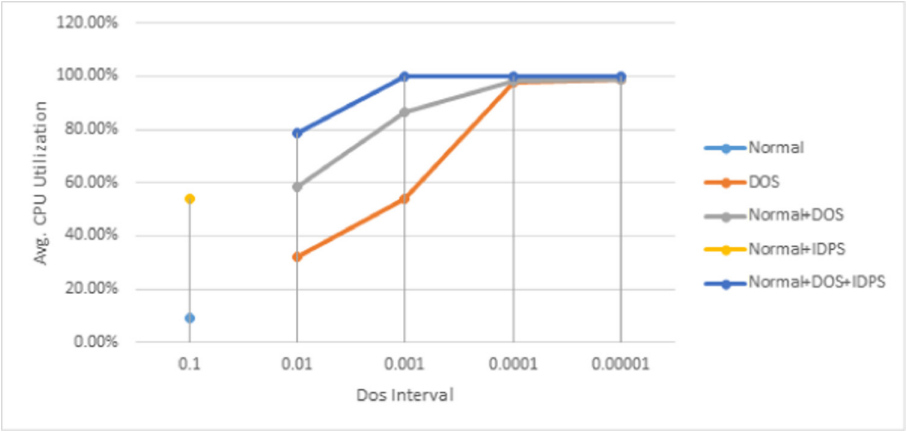


Fig. 8. The average CPU utilization of different levels of network traffic recorded for varying DoS intervals

Figure 8 depicts how the average CPU utilization varies for different combinations of traffic and usage against different DoS intervals. The CPU utilization has been measured using the htop command-line utility. It can be seen that the CPU utilization is just above 0% for normal traffic. With the simulation of the DoS attack, it is evident that the utilization increases from 30% and reaches maximum utilization when the interval is 0.0001, which is the optimal DoS interval for this experimental setup as mentioned previously. The utilization is higher when both normal and DoS traffic are fed into the system.

Table 2. High level overview of performance metrics of the proposed approach compared against generic IDS types.

Detection techniques	Accuracy	False positive Rate	False negative rate	Resource utilization	Detection rate for new attacks
Anomaly-based	Varies	High	Low	High	High
Signature-based	High	Low	High	Low	Low
Proposed model	High	Low	Low	Low	Moderate

Table 2 shows an overview of the performance comparison for different DoS detection techniques. The proposed methodology attributes its high accuracy and low false-positive rate to its innate quality of being a signature-based IDS. A packet gets flagged as suspicious only after multiple tests, and it does not try to guess the behavior or intention of the traffic like an anomaly-based system does. The proposed multi-level approach helps to reduce the false-positive rate significantly especially since a whitelisting strategy is used instead of a blacklisting one. Also, when compared to anomaly-based intrusion detection systems, the proposed signature-based IDPS has lower resource demand.

5 Conclusion

In this paper, an experimental approach to building an IDPS system that can successfully detect and prevent a DoS attack has been presented. The experimental proceedings show that the IDPS installed was successful in detecting the DoS attack and interrupting the communication between the attacker and the server by dropping all the malicious packets. It is also possible to configure the IDPS system by adjusting the frequency threshold based on the peak value when the attack happens. In this solution, three main levels are involved: the frequency-based filtering level, the whitelisted IP matching level, and the deep packet inspection level. The proposed method uses a signature-based detection

system in the second level of the inspection hierarchy and although it provides appreciable results in terms of detection rate, it is still slightly vulnerable to IP spoofing even with deep packet inspection. This provides more room for improvement, and one way to solve this problem would be to consider shifting to the more secure IPv6 protocol, which is inherently more reliable due to its encryption and authentication standards. As the transition to IPv6 might take a while, anomaly-based detection strategies could be integrated with the proposed system to form a hybrid IDPS to harden the system against zero-day attacks.

References

1. Damasevicius, R., Maskeliunas, R., Misra, S., Salaudeen, B., Azeez, N.: Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics **12**, 200 (2020). https://doi.org/10.1504/IJESDF.2020.10027595
2. Fidele, K., Syafei, W.S.: Denial of service (dos) attack identification and analyse using sniffing technique in the network environment. E3S Web Conf. 202, 15003 (2020). https://doi.org/10.1051/e3sconf/202020215003
3. Farooq, U.: Network security challenges (2018). https://doi.org/10.13140/RG.2.2.27478.34885
4. Madhuri, A., Ramana, A.L.: Attack patterns for detecting and preventing DDOS and replay attacks. Int. J. Eng. Sci. Technol. **2**, 4850–4859 (2010)
5. Zlomislić, V., Fertalj, K., Sruk, V.: Denial of service attacks, defences and research challenges. Clust. Comput. **20**(1), 661–671 (2017). https://doi.org/10.1007/s10586-017-0730-x
6. Odusami, M., Misra, S., Abayomi-Alli, O., Adebayo, A.A., Fernandez-Sanz, L.: A survey and meta-analysis of application-layer distributed denial-of-service attack. Int. J. Commun. Syst. 33 (2020). https://doi.org/10.1002/dac.4603
7. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity **2**(1), 1–22 (2019). https://doi.org/10.1186/s42400-019-0038-7
8. Titorenko, A.A., Frolov, A.A.: Analysis of modern intrusion detection system. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 142–143. IEEE (2018)
9. Anwar, S., Mohamad Zain, J., Zolkipli, M.F., Inayat, Z., Khan, S., Anthony, B., Chang, V.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms **10**(2), 39 (2017)
10. Yousufi, R.M., Lalwani, P., Potdar, M.: A network-based intrusion detection and prevention system with multi-mode counteractions. In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–6. IEEE (2017)
11. Scarfone, K., Mell, P., et al.: Guide to intrusion detection and prevention systems (idps). NIST Spec. Publ. **800**(2007), 94 (2007)
12. Acharya, A.A., Arpitha, K., Kumar, B.S.: An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in manet. Int. J. Eng. Technol. (IJET), **8**(2) (2016)
13. Barbhuiya, S., Kilpatrick, P., Nikolopoulos, D.S.: Droidlight: lightweight anomaly-based intrusion detection system for smartphone devices. In: Proceedings of the 21st International Conference on Distributed Computing and Networking, pp. 1–10 (2020)

14. Xiaoming, L., Sejdini, V., Chowdhury, H.: Denial of Service (DoS) Attack with UDP Flood. University of Windsor, Canada, School of Computer Science (2010)
15. Nenova, M., Atanasov, D., Kassev, K., Nenov, A.: Intrusion detection system model implementation against ddos attacks. In: 2019 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), pp. 1–4. IEEE (2019)
16. Shurman, M.M., Khrais, R.M., Yateem, A.A.: IoT denial-of-service attack detection and prevention using hybrid IDS. In: 2019 International Arab Conference on Information Technology (ACIT), pp. 252–254. IEEE (2019)
17. Titorenko, A.A., Goncharov, D.E.: Influence of dos attacks on intrusion detection systems. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 144–146. IEEE (2018)
18. Kurniawan, M.T., Yazid, S.: Mitigation and detection strategy of dos attack on wireless sensor network using blocking approach and intrusion detection system. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp. 1–5. IEEE (2020)
19. Kumar, R., Lal, S.P., Sharma, A.: Detecting denial of service attacks in the cloud. In: 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 309–316. IEEE (2016)
20. Dwivedi, S., Vardhan, M., Tripathi, S.: Defense against distributed dos attack detection by using intelligent evolutionary algorithm. Int. J. Comput. Appl. 1–11 (2020). https://doi.org/10.1080/1206212X.2020.1720951
21. Odusami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., Ahuja, R.: An improved model for alleviating layer seven distributed denial of service intrusion on webserver. J. Phys: Conf. Ser. **1235**, 012020 (2019). https://doi.org/10.1088/1742-6596/1235/1/012020
22. Smys, S., Basar, D., Wang, D.: Hybrid intrusion detection system for internet of things (IoT). J. ISMAC **2**, 190–199 (2020). https://doi.org/10.36548/jismac.2020.4.002
23. Abushwereb, M., Mustafa, M., Alkasassbeh, M., Qasaimeh, M.: Attack based dos attack detection using multiple classifier (2020)
24. Kim, J., Kim, J., Kim, H., Shim, M., Choi, E.: CNN-based network intrusion detection against denial-of-service attack. Electronics **9**, 916 (2020). https://doi.org/10.3390/electronics9060916