Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 1, February 2025, pp. 438~446
ISSN: 2302-9285, DOI: 10.11591/eei.v14i1.8377

Distributed denial-of-service attack detection short review: issues, challenges, and recommendations

AKM Ahasan Habib[1,2], Ahmed Imtiaz[3], Dhonita Tripura[3], Md. Omar Faruk[4], Md. Anwar Hossain[4], Iffat Ara[4], Sohag Sarker[4], A F M Zainul Abadin[1,4]
[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia
[2]North Garth Institute of Technology, Dhaka, Bangladesh
[3]Department of Computer Science and Engineering, Faculty of Science, Engineering and Technology, Rangamati Science and Technology University, Rangamati, Bangladesh
[4]Department of Information and Communication Engineering, Faculty of Engineering and Technology, Pabna University of Science and Technology, Pabna, Bangladesh

Article Info

Article history:

Received Feb 22, 2024
Revised Aug 19, 2024
Accepted Aug 25, 2024

Keywords:

Cyber attack
Cyber-physical system
Denial of service attack
Distributed denial-of-service attack
High-speed network

ABSTRACT

An attacker can attack a network in several methods when there are a lot of device connections. Distributed denial-of-service (DDoS) attacks could result from this circumstance, which could damage resources and corrupt data. Therefore, irregularity in traffic data must be detected to identify malicious behavior in a network, which is critical for maintaining the integrity of current cyber-physical systems (CPS) as well as network security. This article attempts to study and compare various approaches to detecting DDoS attacks and expresses data paths for packet filtering for high-speed networks (HSN) performance, using machine or deep learning techniques used in intrusion detection systems (IDSs) and flow-based IDSs. The study presents a comprehensive DDoS attack taxonomy, categorizes detection strategies, and highlights the HSN accuracy assessment features. By exposing the problems and difficulties associated with DDoS attacks on HSN, several investigation paths are proposed to assist researchers in determining and developing the best solution.

Corresponding Author:

A F M Zainul Abadin
Department of Information and Communication Engineering, Faculty of Engineering and Technology
Pabna University of Science and Technology
Pabna-6600, Bangladesh
Email: abadin.7@gmail.com

1. INTRODUCTION

The application range of the internet is expanding quickly due to the rise in network traffic caused by the introduction of gadgets like intelligent devices, remote sensors, self-driving cars with GPS connectivity, 5G data transfer, smartphones, and cloud computing [1]-[3]. Global internet users are approximately 4.66 billion people, which is nearly 59.5% of the world's population. The world's population uses smartphones in 66.6%, whereas 53.6% are used social media. It is concerning that there could be an increase in internet users, particularly in light of the security of the internet and the reliability of cyber-physical systems (CPS) [4]. Even if the internet improves convenience and helps with many aspects of life, there are numerous security hazards associated with it. Malicious cyberattacks, including deception, reply, denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks, are a common illustration of these hazards. Their goals and approaches diverge. While deception attacks attempt deceit and manipulation, replay attacks concentrate on capturing and exploiting legitimate data to obtain unauthorized access or

manipulate systems. DDoS attacks seek to interrupt availability. Furthermore, DDoS attacks are linked to compromised security and user privacy [5]-[8].

DDoS attacks usually originate from multiple connected devices. Through data bombardment from neighboring infrastructure, the attack might produce unexpected activity that stops the routine traffic of particular servers, services, and networks. It is challenging to determine a reliable source because of the massive volume of ongoing service requests that this unexpected activity generates for the servers and networks. For instance, an attacker can swiftly target thousands of devices on a broad scale in an internet of things (IoT) environment [9]-[11].

Time delay becomes a critical problem for a workable CPS communication network. Time delay attacks (TDAs) take advantage of the weakness of communication channels to potentially cause serious damage to a system. Several different methods proposed for TDA detection have only been investigated offline, and they are evaluated under the strict presumption that a workable solution for real-world scenarios will be developed [12]-[14]. Detecting DDoS attacks becomes more difficult on high-speed networks (HSNs). DDoS attacks might be volume-based, protocol-based, or application-layer attacks. Due to a packet linked to a system call and a copy approaching the transformation spreading throughout the network, context switching of network processing brought on by a DoS or DDoS attack can slow down network performance in HSNs, which are made up of fiber-based networks with data speeds of 100 Gbps [15]-[17].

Security threats have increased as a result of the increasing complexity of DDoS attack detection brought about by the speed at which data is being processed on networks. An example of a DDoS attack on an HSN is shown in Figure 1. In addition, the network speed and the variety of data types that enter it present significant problems for researchers trying to counter DDoS attacks. Numerous methods for detecting DDoS attacks have been introduced; namely, abnormal detection and misuse detection are the two main categories of detection [4], [18], [19]. There are restrictions on the parameters that can be chosen to identify network patterns in both detection algorithms. Misuse detection has the benefit of high accuracy; yet, it necessitates full network information. On the other hand, anomalous detection does not require prior knowledge of the network, but it also lacks the high accuracy that malicious activity detection provides.

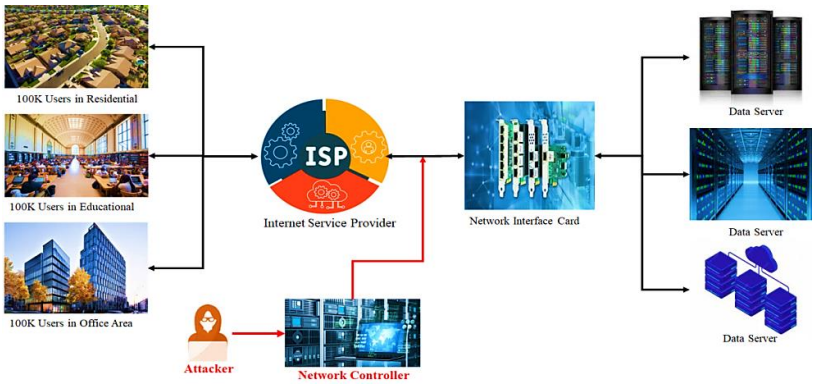

Figure 1. DDoS attack scenario

Survey methods: the purpose of this survey is to provide an easy-to-understand consideration, critical analysis, and recommendations for DDoS attack detection. As a result, the contributors have compiled the most recent and appropriate data, including important technologies, limitations, and research gaps. This survey uses four phases of screening and assessment to calculate the total number of published articles. The screening and evaluation of DDoS attack detection across several sources (i.e., Scopus, Research Gate, Google Scholars, and Web of Science database) is the first step in the systematic literature review and we found related 220 papers. Secondly, we searched our papers based on critical work and selected 95 papers. Thirdly, we select 45 published papers to read the abstract, introduction, and conclusion. Fourthly, we select 27 papers to read whole sections and content based on journal impact factors, citations, and review process. Finally, we considered and selected 51 articles to use as references and developed this review. The contribution of this study is bellowed; i) provide a short overview of DDoS attacks in HSN, attack types, identification, and detection techniques and ii) highlights the current issues, and challenges and recommends some ideas that will be helpful for future research.

This manuscript is organized as follows; section 2 discus DDoS attacks, types of attacks, and detection mechanisms. Section 3 presents the current issues and challenges. Section 4 illustrates the recommendations for future research. Finally, the manuscript is concluded in section 5.

2. DISTRIBUTED DENIAL-OF-SERVICE ATTACK

When a device or network is overloaded, it becomes unusable due to a DDoS attack. Attackers achieve this by flooding the target with more traffic beyond what is capable of handling, which leads to a failure and prevents it from being able to service its normal users. Attacks can be launched against any service that depends on a specific computer or network, including websites, online banking, email, and other services [6], [20]. A botnet is an assembly of automated programs or machines. Botnets are capable of direct attacks and sending commands remotely to individual bots. Every bot sends a request to a given IP address within a botnet, impacted network, or server, delaying normal traffic. Very short DDoS attacks are becoming more common. DDoS attacks in 2022 are expected to last 5–10 s on average, with a 24-hour episode capacity of 5 Gbps, according to Gcore research [4].

2.1. Types of distributed denial-of-service attack

DDoS attacks appear in a variety of forms, several classified multi-vector attacks. Other defense measures are necessary to classify these varied attacks. When it comes to internet services, taking down the weakest link might bring the entire system down. When an attacker overloads a resilient domain and name server with scam requests, it will not answer [21]-[24]. The DDOS attack types are present in Figure 2.

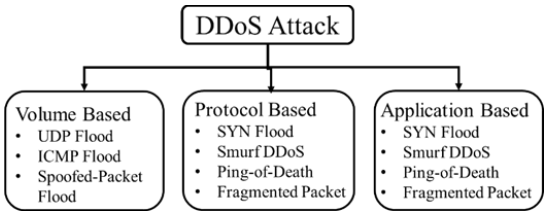

Figure 2. Types of DDoS attack

2.1.1. Zero-day attacks

These kinds of attacks take advantage of undiscovered hardware or network vulnerabilities. It may be difficult to fight against these vulnerabilities because neither the vendor nor the general public is aware of them yet [25], [26].

2.1.2. Reflection attacks

Reflection attacks, like amplification attacks, increase attack flow by exploiting weak protocols. Reflection attacks increase the volume of traffic by having the attacker send requests to outside servers, which then return responses to the target network. These kinds of DDoS attacks can happen on both HSN and low-speed networks. It's crucial to remember that they can be particularly damaging to HSN because of the volume of traffic they can produce [21], [27].

2.1.3. Domain name system amplification

Domain name system (DNS) amplification, or scalable DDoS attacks [4], [28], [29], use an efficient expanded reflection attack technique. Such attacks increase the external data flow, which saturates the bandwidth. The attackers bombard the system with information requests that result in enormous amounts of data and traffic. Subsequently, they fabricate the reply-to address to return the data to the server. During a DNS amplification attack, an attacker sends several relatively small messages to a publicly available DNS server via a botnet that originates from multiple different sources. These packets all contain long requests, like DNS name lookup requests. The DNS server subsequently responds to every one of the scattered inquiries with response packets which are forwarded back to the victim's DNS server, multiple orders of magnitude larger beyond the original request packet.

2.1.4. SYN flood

SYN flood attacks establish transmission control protocol (TCP) connections with servers and clients by eschewing the three-way handshake protocol. These connections are typically established by the client requesting synchronization from the server and concluding the exchange of keys with an acknowledgment from the server. SYN floods function by sending out synchronization requests quickly and then waiting for the server to respond with a definitive declaration [30]-[33]. A final acknowledgment completes the handshake after the client sends the server a synchronize request and the server responds via a

final acknowledging response. These synchronization requests are made by SYN floods, which cause the server to become unresponsive by not responding with a definitive declaration.

2.1.5. Ping of death

Compared to typical internet control message protocol (ICMP) echo ping flood attacks, ping-of-death attacks are different. The packet's maliciously designed content aims to bring about a server-side system breakdown. Because a typical ping flood attack is intended to overload the bandwidth through sheer volume, all the information it contains is essentially meaningless [34], [35]. Ping-of-death attacks take implement of the vulnerabilities in the target device by sending packets that disrupt or stop it. This methodology may be employed for protocols other than ICMP, such as TCP and user datagram protocol (UDP).

2.1.6. Application layer attack

HTTP flood attacks are DDoS attacks that target the application layer. The perpetrator routinely interacts with a web server or application by employing this technique [36], [37]. All of the communications that web browsers make pretend to be typical user activity, however, they have been planned to utilize the maximum server resources possible. The attacker's request could be anything from using GET queries to obtain the URLs of documents or images to using POST requests to initiate server operations to a database.

2.2. Identification of distributed denial-of-service attacks

A DDoS attack can be detected by incredibly sluggish or inaccessible services or websites. Analysis technologies can identify the location of DDoS attacks. Unexpected volumes of traffic coming from a particular IP range, for example, tend to overwhelm the traffic or network with a web browser, location, and specific device behavioral patterns directed towards a single page or endpoint [21], [24], [38]-[40]. As an example, the fundamental determination of DDoS attack flow is shown in Figure 3. A DDoS attack can be identified by three symptoms: a website that loads slowly or is unavailable; a network that suddenly loses internet access; or a computer that becomes unresponsive or slow. The first step in detecting a DDoS attack is to initialize the system parse rules library and create a two-dimensional linked list. The PostgreSQL interface for C application developers is called libpq, and it consists of a collection of library methods that allow apps to send requests to the PostgreSQL server and retrieve the responses. The packet is then captured, parsed, and compared to the database of the back-end server; if the result is found, it is taken; if not, the package is retrieved to the libpq interface.

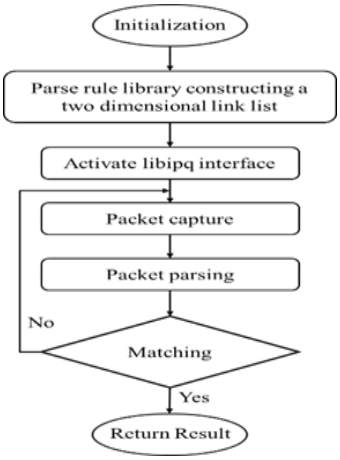

Figure 3. DDoS attack detection technique

2.3. Distributed denial-of-service attack detection technique

The DDoS attack effectively causes the services, computers, applications, and network to go offline and, aims to overload them with traffic. An internet-connected appliance running multiple bots is called a botnet. Botnets can be used to send spam, initiate DDoS attacks, steal data, and enable access within the equipment and its network to malicious parties. The software can be used by the administrator to oversee and administer a botnet [41]-[45]. Attackers induce the system to stop functioning or become inaccessible by using botnets of the compromised device on the network. Table 1 provides more details on different methods of detecting DDoS attacks.

DDoS attacks against systems are being detected and prevented using various technologies [4], [46]-[48]. To identify and stop DDoS attacks, these technologies keep an eye on event logs from multiple sources. The DDoS attack prevention tools are described in Table 2.

Table 1. Categorize based DDoS attack detection methods

Attack layer	Detection methods
Application layer	Support vector machine (SVM), signature base, entropy, bat algorithm, decision tree, naïve Bayesian (NB), fuzzy logic, genetic algorithm, long short-term memory (LSTM), low rate, k-nearest neighbors (KNN), information gain, a spatial, and temporal neighbor
Application and volume base	Fuzzy logic, genetic algorithm, SVM, and PCA-KNN
Transport and application layer	Fuzzy logic, divide and conquer, NB, SVM, KNN, low rate, random forest, rate limiting and allowing listing, and block-listing

Table 2. DDoS attack prevention tools

Tool	Outcome
HULK	Block traffic
Low orbit ion cannon (LOIC)	LOIC supervises the network stress and malware virus
Slow loris	Sending HTTP traffic data over the relevant server
SolarWinds SEM	Logs and events that SEM keeps track of are useful for attack post-breach investigations and mitigation
Tor's Hammer	Random selection HTML posts and POST attack
XOIC	Block the attack

3. ISSUES AND CHALLENGES

During our literature review, we found some issues and challenges for DDoS attacks that are summarized:

- The problems and outstanding research questions related to DDoS attacks in HSNs are explained in this section. DDoS attacks in HSN problems are classified according to variables i.e., packet size, packet drop, packet filtering, response time, traffic monitoring, and data processing. Three forms of DDoS attacks have been commonly identified: volume-based attacks, protocol attacks, and application-layer attacks. Based on the existing literature according to the DDoS attack classification, the issues and challenges are thoroughly explained. Application attacks happen at the 7^{th} level of the open systems interconnection (OSI) model. The attack begins with the attacker connecting with their target. Once a link has been established, the attacker takes advantage of the resources to overload the system with requests, which is an example of both HTTP floods and DNS floods [49], [50]. Volume attacks are directed at particular victims, most frequently service providers. To overwhelm the server, the attacker takes over the available bandwidth on the network and attacks it with packets. UDP flood and TCP flood attacks are two examples. Protocol attacks include flooding the server with erroneous data in an attempt to cause server crashes, data overflow, and the unavailability of server resources. Ping of death and border gateway protocol (BGP) are two examples [49], [51].
- The present study indicates the majority of methods in studies that identify and counteract high-frequency DDoS attacks have a low false-positive rate and good accuracy. Because of a discernible rise in the number of malicious traffic in the network, high-rate DDoS attacks are simple to anticipate. But a new kind of DDoS attack has emerged: stealthy attacks or low-rate. Because they resemble normal network traffic flow, these attacks are extremely difficult to identify and counter with low false-positive rates and excellent detection accuracy. Some studies only obtain poor results while attempting to detect low-rate DDoS attacks. Thus, there is an unmet research requirement to be done to identify and mitigate DDoS attacks with low false-positive rates and high accuracy.
- The majority of literature research' suggested security measures are predicated upon an architecture containing a single network operator. However, in the event of a DDoS attack, they are susceptible to a single point of collapse. On the other hand, load distribution, consistency, and scalability are far better in networked environments with distributed controllers than in an asymmetric or hierarchical architecture. Furthermore, using distributed controllers is capable of maintaining the network operating efficiently when the central control system starts to bottleneck due to a rise in the impact of DDoS attacks. These can remove single points of failure, lessen the effect of communication overhead and DDoS attacks, and facilitate the load balancer's ability to distribute traffic among several controllers. As a result, distributed SDN controller functioning is still an unsolved security issue that requires research.
- Beyond the DDoS attack mitigation, many preventative strategies occurred in network systems. It is more vital to avoid DDoS attacks rather than to identify and mitigate them by preventing their spread inside the network and utilizing its capabilities, as doing so will keep the SDN network's functioning from

diminishing. As such, preventing, detecting, and mitigating DDoS attacks remains a significant scientific challenge that requires attention.

4. RECOMMENDATIONS

Based on the literature review some significant points are highlighted for future study or research. That is presently bellowed:

- The SDN system or other emerging technologies currently feature numerous processing layers within their computational infrastructure which can handle training data at varying degrees of complexity, machine or deep learning-based techniques and methods fit easily. Thus, integrating findings or novel discoveries from machine or deep learning-based investigations into SDN security strategies has an exciting prospect.
- For networks like wireless sensor networks, mobile ad hoc networks (MANETs), and the IoT, with little memory and limited processing capability, and vulnerable to hacking attempts, lightweight models are essential. The need to create portable and efficient machine or deep learning models for such situations is anticipated to grow in the future.
- The SDN architecture's use of P4-programmed switches may reduce the overhead of the controller in the event of a DDoS attack. As a result, it represents perhaps the most potential avenues for future SDN security network prevention investigation.
- The continuing absence of safety features on IoT devices with the yearly evolution of botnet viruses demonstrates the permanence of DDoS attacks carried out by IoT devices.
- Overall, DDoS attacks have the potential to increase in frequency, complexity, and affordability.
- It was formerly unusual to employ obscure IoT equipment like CCTV cameras, thermostats, and smart refrigerators. Gadgets currently represent a significant concern since they may be used as botnets to launch DDoS attacks and interfere with or completely shut down a target's services.

5. CONCLUSION

The main focus of this article was to categorize DDoS assaults and the various kinds that can happen in a HSN. The DDoS problem is expanding quickly. To improve the detection accuracy through the use of the tracking and screening of compromised packets utilizing an express data path, this study looked at different currently available methods for identifying DDoS attacks, including traceback mechanisms, that are divided into reactive and proactive approaches, packet marking including application layer protocol analyses, deterministic packet marking (DPM), and probabilistic packet marking (PPM). The field of DDoS mitigation in HSN is rapidly advancing, with researchers creating effective and creative methods. The problems and remaining issues covered above present an ideal representation of where DDoS detection will go in the future.

ACKNOWLEDGMENTS

All authors acknowledge each other for their contribution and support. The author AKM Ahasan Habib and A F M Zainul Abadin are nominated Ph.D. fellow by the ICT division of the Ministry of Posts, Telecommunication and Information Technology, Bangladesh. They would like to acknowledge the division with deepest gratitude.

REFERENCES

[1] T. Wang, Y. Liang, X. Shen, X. Zheng, A. Mahmood, and Q. Z. Sheng, "Edge computing and sensor-cloud: overview, solutions, and directions," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1-37, 2023, doi: 10.1145/3582270.

[2] R. M. A. Haseeb-Ur-Rehman *et al.*, "Sensor cloud frameworks: state-of-the-art, taxonomy, and research issues," *IEEE Sensors Journal*, vol. 21, no. 20, pp. 22347-22370, 2021, doi: 10.1109/JSEN.2021.3090967.

[3] M. K. Hasan *et al.*, "Federated learning enables 6 G communication technology: requirements, applications, and integrated with intelligence framework," *Alexandria Engineering Journal*, vol. 91, pp. 658-668, 2024, doi: 10.1016/j.aej.2024.02.044.

[4] R. M. A. Haseeb-Ur-Rehman *et al.*, "High-speed network DDoS attack detection: a survey," *Sensors*, vol. 23, no. 15, pp. 1-25, 2023, doi: 10.3390/s23156850.

[5] A. A. Habib, M. K. Hasan, R. Hassan, S. Islam, R. Thakkar, and N. Vo, "Distributed denial-of-service attack detection for smart grid wide area measurement system: a hybrid machine learning technique," *Energy Reports*, vol. 9, pp. 638-646, 2023, doi: 10.1016/j.egyr.2023.05.087.

[6] M. K. Hasan, A. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports*, vol. 9, pp. 1318-1326, 2023, doi: 10.1016/j.egyr.2023.05.184.

[7] R. Balamurugan, B. A. Princy, D. Kanchana, M. Murugesan, A. J. Selsia, and M. Dinesh, "Implementation of an Effective methodology to avoid DDoS attacks using cybersecurity norms," *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 2024, pp. 1-6, doi: 10.1109/IITCEE59897.2024.10467703.

[8] A. A. Habib, M. K. Hasan, A. Alkhayyat, S. Islam, R. Sharma, and L. M. Alkwai, "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction," *Computers and Electrical Engineering*, vol. 107, p. 108638, 2023, doi: 10.1016/j.compeleceng.2023.108638.

[9] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, "DDoS attacks and machine-learning-based detection methods: a survey and taxonomy," *Engineering Reports*, vol. 5, no. 12, pp. 1-29, 2023, doi: 10.1002/eng2.12697.

[10] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the internet of things: opportunities and solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1775-1807, 2023, doi: 10.1109/COMST.2023.3280465.

[11] X.-H. Nguyen and K.-H. Le, "Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model," *Internet of Things*, vol. 23, p. 100851, 2023, doi: 10.1016/j.iot.2023.100851.

[12] P. Ganesh *et al.*, "Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3581-3593, 2021, doi: 10.1109/TSG.2021.3058682.

[13] F. Luo, Z. Wang, and B. Zhang, "Impact analysis and detection of time-delay attacks in time-sensitive networking," *Computer Networks*, vol. 234, pp. 1-14, 2023, doi: 10.1016/j.comnet.2023.109936.

[14] M. Moradi and A. H. Jahangir, "A petri net model for time-delay attack detection in precision time protocol-based networks," *IET Cyber-Physical Systems: Theory & Applications,* pp. 1-17, 2024, doi: 10.1049/cps2.12088.

[15] A. Iftikhar, K. N. Qureshi, M. Shiraz, and S. Albahli, "Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: a systematic literature review," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 9, pp. 1-39, 2023, doi: 10.1016/j.jksuci.2023.101788.

[16] W. Yu, D. Huang, and N. Qin, "Resilient coordinated data-driven control of multiple high-speed trains under fading measurements and denial-of-service attacks," *IEEE Transactions on Vehicular Technology*, vol. 27, no. 5, pp. 5690-5701, 2023, doi: 10.1109/TVT.2022.3231712.

[17] A. Z. Abadin, S. Sarker, M. S. Hosain, M. M. Ahmed, and A. Imtiaz, "A comprehensive study and analysis of different routing protocols for enterprise LAN," *International Journal of Science and Business*, vol. 5, no. 8, pp. 20-28, 2021.

[18] R. R. Papalkar and A. S. Alvi, "Analysis of defense techniques for DDos attacks in IoT–a review," *ECS Transactions*, vol. 107, no. 1, p. 3061, 2022, doi: 10.1149/10701.3061ecst.

[19] S. Saudagar and R. Ranawat, "Detecting vehicular networking node misbehaviour using machine learning," *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2023, pp. 1-3, doi: 10.1109/ICONAT57137.2023.10080114.

[20] H. Liao *et al.*, "A survey of deep learning technologies for intrusion detection in internet of things," *IEEE Access*, vol. 12, pp. 4745-4761, 2024, doi: 10.1109/ACCESS.2023.3349287.

[21] A. A. Alahmadi *et al.*, "DDoS attack detection in iot-based networks using machine learning models: a survey and research directions," *Electronics*, vol. 12, no. 14, pp. 1-24, 2023, doi: 10.3390/electronics12143103.

[22] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Computers & Security*, vol. 127, p. 103096, 2023, doi: 10.1016/j.cose.2023.103096

[23] E. Navruzov and A. Kabulov, "Detection and analysis types of DDoS attack," in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Toronto, Canada, 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[24] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, pp. 1-57, 2023, doi: 10.3390/jsan12040051.

[25] Y. Guo, "A review of machine learning-based zero-day attack detection: challenges and future directions," *Computer Communications*, vol. 198, pp. 175-185, 2023, doi: 10.1016/j.comcom.2022.11.001.

[26] M. Soltani, B. Ousat, M. J. Siavoshani, and A. H. Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," *Journal of Information Security and Applications*, vol. 76, p. 103516, 2023, doi: 10.1016/j.jisa.2023.103516.

[27] X. Liu, L. Zheng, S. Helal, W. Zhang, C. Jia, and J. Zhou, "A broad learning-based comprehensive defence against SSDP reflection attacks in IoTs," *Digital Communications and Networks*, vol. 9, no. 5, pp. 1180-1189, 2023, doi: 10.1016/j.dcan.2022.02.008.

[28] S. Adiwal, B. Rajendran, and S. D. Sudarsan, "DNS intrusion detection (DID) - A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks," *Franklin Open*, vol. 2, pp. 1-11, 2023, doi: 10.1016/j.fraope.2023.100010.

[29] Y. Dai, T. Huang, and S. Wang, "DAmpADF: a framework for DNS amplification attack defense based on Bloom filters and NAmpKeeper," *Computers & Security*, vol. 139, p. 103718, 2024, doi: 10.1016/j.cose.2024.103718.

[30] C.-H. Yang, J.-P. Wu, F.-Y. Lee, T.-Y. Lin, and M.-H. Tsai, "Detection and mitigation of SYN flooding attacks through SYN/ACK packets and Black/White lists," *Sensors*, vol. 23, no. 8, pp. 1-14, 2023, doi: 10.3390/s23083817.

[31] V. Nagaraju, A. Raaza, V. Rajendran, and D. Ravikumar, "Deep learning binary fruit fly algorithm for identifying SYN flood attack from TCP/IP," *Materials Today: Proceedings*, vol. 80, pp. 3086-3091, 2023, doi: 10.1016/j.matpr.2021.07.171.

[32] H. S. Bazzi, A. H. Nassar, I. M. Haidar, A. M. Haidar, and Z. Doughan, "ResNet-based detection of SYN Flood DDoS attacks," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 2024, pp. 1142-1147, doi: 10.1109/IC2PCT60090.2024.10486707.

[33] V. A. Shirsath, M. M. Chandane, C. Lal, and M. Conti, "SYNTROPY: TCP SYN DDoS attack detection for software defined network based on Rényi entropy," *Computer Networks*, vol. 244, p. 110327, 2024, doi: 10.1016/j.comnet.2024.110327.

[34] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in IoT networks," *Wireless Personal Communications*, vol. 112, pp. 2057-2070, 2020, doi: 10.1007/s11277-020-07139-y.

[35] J. David and C. Thomas, "Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic," *Computers & Security*, vol. 82, pp. 284-295, 2019, doi: 10.1016/j.cose.2019.01.002.

[36] S. Ahmed *et al.*, "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron," *Future Internet*, vol. 15, no. 2, pp. 1-24, 2023, doi: 10.3390/fi15020076.

[37] D. M. Sharif, H. Beitollahi, and M. Fazeli, "Detection of application-layer DDoS attacks produced by various freely accessible toolkits using machine learning," *IEEE Access*,vol. 11, pp. 51810-51819, 2023, doi: 10.1109/ACCESS.2023.3280122.

[38] C. S. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, and P. Papadopoulos, "Explainable AI-based DDOS attack identification method for IoT networks," *Computers*, vol. 12, no. 2, pp. 1-16, 2023, doi: 10.3390/computers12020032.

[39] T.-L. Nguyen, H. Kao, T.-T. Nguyen, M.-F. Horng, and C.-S. Shieh, "Unknown DDoS attack detection with fuzzy C-means clustering and spatial location constraint prototype loss," *Computers, Materials & Continua*, vol. 78, no. 2, pp. 2181-2205, 2024, doi: 10.32604/cmc.2024.047387.
[40] M. S. Raza, M. N. A. Sheikh, I.-S. Hwang, and M. S. Ab-Rahman, "Feature-selection-based DDoS attack detection using AI algorithms," *Telecom*, vol. 5, no. 2, pp. 333-346, 2024, doi: 10.3390/telecom5020017.
[41] M. A. Al-Shareeda, S. Manickam, and M. Ali, "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930-939, 2023, doi: 10.11591/eei.v12i2.4466.
[42] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Engineering Applications of Artificial Intelligence*, vol. 123, pp. 1-17, 2023, doi: 10.1016/j.engappai.2023.106432.
[43] S. Aktar and A. Y. Nur, "Towards DDoS attack detection using deep learning approach," *Computers & Security*, vol. 129, p. 103251, 2023, doi: 10.1016/j.cose.2023.103251.
[44] B. Bala and S. Behal, "AI techniques for IoT-based DDoS attack detection: taxonomies, comprehensive review and research challenges," *Computer science review*, vol. 52, p. 100631, 2024, doi: 10.1016/j.cosrev.2024.100631.
[45] M. Ouhssini, K. Afdel, E. Agherrabi, M. Akouhar, and A. Abarda, "DeepDefend: a comprehensive framework for DDoS attack detection and prevention in cloud computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 2, pp. 1-25, 2024, doi: 10.1016/j.jksuci.2024.101938.
[46] R. Chaganti, B. Bhushan, and V. Ravi, "A survey on blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions," *Computer Communications*, vol. 197, pp. 96-112, 2023, doi: 10.1016/j.comcom.2022.10.026.
[47] B. Ilyas, A. Kumar, M. A. Setitra, Z. A. Bensalem, and H. Lei, "Prevention of DDoS attacks using an optimized deep learning approach in blockchain technology," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 4, p. e4729, 2023, doi: 10.1002/ett.4729.
[48] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, vol. 8, pp. 1-17, 2024, doi: 10.1016/j.prime.2024.100543.
[49] B. Xie, Y. Wang, G. Wen, and X. Xu, "Application-layer DDoS Attack detection using explicit duration recurrent network-based application-layer protocol communication models," *International Journal of Intelligent Systems*, vol. 2023, pp. 1-13, 2023, doi: 10.1155/2023/2632678.
[50] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, and S. Kumar, "SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTM-CNN," *Transactions on Emerging Telecommunications Technologies*, 2023, doi: 10.1002/ett.4758.
[51] B. M. Yakubu, M. I. Khan, A. Khan, F. Jabeen, and G. Jeon, "Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home," *Digital Communications and Networks*, vol. 9, no. 2, pp. 383-392, 2023, doi: 10.1016/j.dcan.2023.01.013.

BIOGRAPHIES OF AUTHORS

AKM Ahasan Habib is a Ph.D. student at the Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. He has published more than 25 indexed papers in ranked journals and conference proceedings. His research interests include electric vehicles, energy storage and management systems, smart grid and cyber security systems, artificial intelligence, smart vehicular networks, smart grids, and industrial IoT. He is a reviewer in the Journal of Network and Computer Applications, Journal of Energy Storage, Applied Energy, SoftwareX, Energy Reports, IET wireless sensor systems, and so many others. He can be contacted at email: ahasan.diu.eee@gmail.com.

Ahmed Imtiaz has been working as Chairman and Assistant Professor in the Department of Computer Science and Engineering at Rangamati Science and Technology University, Bangladesh. He completed M.S. in information technology from Jahangirnagar University, Bangladesh. He received B.Sc. (Engg.) in information and communication engineering from Pabna University of Science and Technology, Bangladesh. His research interests include artificial intelligence, brain computer interface, embedded system, and computer networking. He can be contacted at email: Imtiazmain@gmail.com and imtiaz@rmstu.ac.bd.

Dhonita Tripura has been working as an Assistant Professor in the Department of Computer Science and Engineering at Rangamati Science and Technology University, Bangladesh. She completed both B.Sc. and M.Sc. in information technology from Jahangirnagar University, Bangladesh. Her research interests include artificial intelligence, machine learning, bioinformatics, and system security. She can be contacted at email: dtdhonitatripura@gmail.com and dhonitatripura@rmstu.ac.bd.

Md. Omar Faruk received the B.Sc., M.Sc., and the Ph.D. degree in applied physics and electronic engineering from University of Rajshahi, Bangladesh, in 1994, 1996 and 2012 respectively. He worked as an Assistant Instrument Engineer from 2001-2004, Instrument Engineer from 2004-2008, Senior Instrument Engineer from 2008-2011, and Principal Instrument Engineer from 2011-2013 at Science Workshop, University of Rajshahi, Rajshahi, Bangladesh. In 2013 he joined the Department of Information and Communication Engineering of the Pabna University of Science and Technology, Pabna, Bangladesh as an assistant professor. He was promoted to Associate Professor in 2019. His research interests include seismology, machine learning, and internet of things. He can be contacted at email: fom_06@yahoo.com, fom_06@pust.ac.bd.

Md. Anwar Hossain received B.Sc. (Honours) and M.Sc. degrees in information and communication engineering from the University of Rajshahi, Bangladesh in 2005 (held in 2007) and 2006 (held in 2008) respectively. He received his M.Phil. degree from the Pabna University of Science and Technology, Bangladesh in 2020. In 2010 he served as a Lecturer in the Department of Information and Communication Technology of Comilla University, Bangladesh. In 2012, he joined Pabna University of Science and Technology, Bangladesh as a faculty member, where he is currently serving as a Professor in the Department of Information and Communication Engineering. Now, he is a Ph.D. student in the Department of Information and Communication Engineering (ICE), Pabna University of Science and Technology (PUST), Bangladesh. His research interests include deep learning, machine learning, image classification, and natural language processing. He can be contacted at email: manwar.ice@gmail.com.

Iffat Ara was born in Pabna, Bangladesh, in 1986. She received her Master of Philosophy (M.Phil.) degree from Pabna University of Science and Technology (PUST) in 2019. She completed her M.Sc. and B.Sc. (Honours) degrees in Applied Physics and Electronic Engineering from the Rajshahi University, Bangladesh in 2010 and 2009, respectively. She is working as an Associate Professor in the Department of Information and Communication Engineering at Pabna University of Science and Technology, Pabna, Bangladesh. Currently, she is pursuing her Ph.D. degree in the Department of Electrical and Electronic Engineering, Rajshahi University, Bangladesh. Her research interests are related to the analysis of biomedical signal. She can be contacted at email: ara.iffat@ymail.com.

Sohag Sarker completed his undergraduate and graduate studies in information and communication engineering at the University of Rajshahi, Bangladesh, in 2009 and 2010, respectively. He earned his M.Phil. degree in wireless communication, specializing in downlink DAS based cooperative wireless communication system, from Pabna University of Science and Technology, Bangladesh, in 2019. Presently, he serves as an Associate Professor in the Department of Information and Communication Engineering at Pabna University of Science and Technology, Bangladesh, while concurrently pursuing a Ph.D. at the University of Rajshahi. His research interests span IoT, machine learning, deep learning, wireless communication, image processing, and computer vision. He can be contacted at email: sohagsarker5614@gmail.com and sohagsarker5614@pust.ac.bd.

A F M Zainul Abadin received the B.Sc. and the M.Sc. degrees in information and communication engineering from the University of Rajshahi, Bangladesh, in 2006 and 2007 respectively. He received the M.Phil. degree in wireless communication with the specialization of physical layer security assisted NOMA technology from Pabna University of Science and Technology, Bangladesh in 2021. Currently, he is an Associate Professor of Department of Information and Communication Engineering, Pabna University of Science and Technology, Bangladesh and a Ph.D. research fellow in the Universiti Kebangsaan Malaysia. His research interests include information security, image steganography, intelligent systems, data science, deep learning, image processing, and computer vision. He can be contacted at email: abadin.7@gmail.com and abadin.7@pust.ac.bd.