Paper

An Efficient Hybrid Protocol Framework for DDoS Attack Detection and Mitigation Using Evolutionary Technique

T. Yerriswamy and Murtugudde Gururaj

School of CSE, REVA University, India

https://doi.org/10.26636/jtit.2022.165122

Abstract — The ever-increasing use of the Internet has created massive amounts network traffic, causing problems related to its scalability, controllability, and manageability. Sophisticated network-based denial of service (DoS) and distributed denial of service (DDoS) attacks increasingly pose a future threat. The literature proposes various methods that may help stop all HTTP DoS/DDoS assaults, but no optimal solution has been identified so far. Therefore, this paper attempts to fill the gap by proposing an alternative solution known as an efficient hybrid protocol framework for distributed DoS attack detection and mitigation (E-HPFDDM). Such an architecture addresses all aspects of these assaults by relaying on a three-layer mechanism. Layer 1 uses the outer advanced blocking (OAB) scheme which blocks unauthorized IP sources using an advanced backlisted table. Layer 2 is a validation layer that relies on the inner service trackback (IST) scheme to help determine whether the inbound request has been initiated by a legitimate or an illegitimate user. Layer 3 (inner layer) uses the deep entropy based (DEB) scheme to identify, classify and mitigate high-rate DDoS (HR-DDoS) and flash crowd (FC) attacks. The research shows that in contrast to earlier studies, the structure of the proposed system offers effective defense against DoS/DDoS assaults for web applications.

Keywords — deep entropy based scheme, denial of service, distributed denial of service, flash crowd, high-rate DDoS, inner service trackback, outer advanced blocking

1. Introduction

Availability of the network remains the most important security requirement. DDoS attacks may result in delaying access to resources, thus leading to network unavailability. The entire network or a single piece of network equipment (such as a switch) may be the target. On the other hand, it is the objective of DoS attacks to overwhelm the network with massive flows of data packets in order to render it inoperable or to degrade its performance [1]. A DoS/DDoS assault is both straightforward and effective, as the attack packets typically lack any precise characteristics that would help identify them.

Flash crowd (FC) is an increase in demand of a given service caused by authorized users making concurrent requests. FC saturates the server, resulting in a denial of service (DoS) assault that causes delays or takes down the site. From the perspective of the user's requests for the service, regardless of whether they are valid or not, FC may not be considered as an assault. It is considered an assault from the victim's or server-side perspective, as it negatively impacts the server's performance.

An LR-DDoS attack floods the victim machine with packets that have a low data rate in order to avoid detection by the existing anomaly-based intrusion detection techniques. Since LR-DDoS traffic is identical to normal flow of data, it can be concealed. Low-rate DDoS attacks usually rely on multiple low-rate assaults, such as those executed with the use of botnets.

This paper proposes an efficient hybrid protocol framework for DDoS detection and mitigation (E-HPFDDM), addressing all issues related to HTTP-based DoS/DDoS attacks. FC assaults are gradually reduced in effect by using the E-HPFDDM framework, which also immediately blocks high-rate DDoS. Furthermore, it protects web servers from assaults at several locations where data packets have ganged. The E-HPFDDM architecture performs the above tasks using a three-layer structure that efficiently detects, classifies and prevents HTTP DoS/DDoS attacks.

E-HPFDDM's first layer uses the OAB scheme and is configured at the edge router from which the packets are forwarded to the inner layers using applicable security measures. This scheme starts by matching incoming packets with the router's updated blacklist table. A packet is dropped if the incoming packet address matches the one on the blacklist and a notification message is sent to the user from the outer layer scheme. In other cases, the packets are moved to the next layer for further processing. This layer helps identify all the illegitimate addresses and directs the same to the outer layer in order to update the router's blacklist table. The two interconnected components make up the outer advanced blocking (OAB) strategy. In order to keep track of illegitimate IP sources, the updated blacklist table is used by IST and DEB schemes. If IP sources fail to pass the procedures defined in the initial component, they are rejected. The second element is a signaling strategy used by IST and DAE schemes to alert the OAB of potentially attacking IP sources, update the blacklist and block illegitimate IP sources during subsequent requests.

The second layer of E-HPFDDM framework uses the inner service traceback (IST) scheme that helps identify whether a given request has been initiated by a trusted user. It also

tracks the real IP source. The third layer of the HPFDDM framework uses the deep entropy based (DEB) scheme that helps detect anomalies and classifies DDoS attacks (e.g. HR-DDoS and FC attacks [2]). The DEB scheme uses the deep entropy-based algorithm for DDoS anomaly detection, classification, and mitigation. The DEB technique prevents traffic from entering the local network if it is determined to be a high-rate HTTP DoS/DDoS (HR-DDoS) attack. If the traffic is found to be of the FC type, the scheme lowers the connection timeout value, as per user requests, until the timeout value reaches zero, and simultaneously disables the HTTP connection's KeepAlive feature.

The contributions of this article include an experimental setup used for launching DDoS attacks, as well as an implementation of an efficient model that includes the strategies described above, such as defense mechanisms capable of detecting, preventing and mitigating DDoS attacks. This paper is organized as follows. Section 1 offers an overview of the E-HPFDDM framework. Section 2 presents the related works focusing on security protective frameworks, evolutionary techniques, DDoS detection, prevention, and attack mitigation techniques. Section 3 contains detailed information on the proposed E-HPFDDM technique. Section 4 presents results of an evaluation of the proposed framework based on ideal requirements applicable to a security system. Section 5 concludes the paper by presenting conclusions.

2. Literature Review

Ujjan *et al*. in [2] proposed a statistical model based on the entropy technique to analyze the flow of network traffic. Estimation of maximum entropy was proposed as a method for distinguishing between normal and malicious network traffic. Using a statistical-based entropy model, similar approaches to detecting DDoS attacks have been proposed. Dong *et al*. [3] proposed and characterized the various DDoS attacks in cloud and SDN networks. Lu *et al*. [4] proposed an efficient defense mechanism for DDoS attacks that identifies the intruder packets based on the entropy values and classifies, accordingly, the type of attack to be defended against.

Imran *et al*. [5], Alhijawi *et al*. [6] proposed an in-depth analysis of DoS prevention and mitigation techniques and divided them into three categories based on how malicious traffic was handled. The authors planned to develop a safe self-adaptive framework using machine learning-based techniques to detect DDoS assaults and retrieved network traffic properties based on the collected data.

Dong *et al*. [3] defined and characterized various DDoS attacks in cloud and in SDN networks, while Lu *et al*. [4] proposed an efficient defense mechanism for DDoS attacks that identifies the intruder packets based on the entropy values and accordingly classifies the type of attack to be defended against.

Imran *et al*. [5] and Alhijawi *et al*. [6] presented an in-depth analysis of DoS prevention and mitigation techniques and divided them into three categories based on how malicious traffic was handled. The aim was to develop a safe self-adaptive framework that uses techniques based on machine learning to detect DDoS assaults and retrieves network traffic properties based on the data collected. Cui *et al*. [7] and Mique *et al*. researched, in [8], an SVM-trained defense mechanism, known as cognitive entropy technique, that helps defend against DDoS attacks. In order to calculate the entropy value for the data packets flowing between the source and destination addresses, the method relied on the data flow table of the switch. Another concept of Sahay *et al*. [9], known as the ArOMA act, is a DDoS defense system automatically identifying assaults on centralized networks without human intervention. A unique NB classifier model was proposed for intrusion detection systems which are implemented using multi-agents that monitor network traffic and separate abnormal data from typical traffic. Another learning-driven detection mitigation (LEDEM) model used for detecting DDoS attacks has been proposed in [10]. It also relies on the machine learning technique [11].

Yerriswamy *et al*. [12] proposed a DDoS protection model that helps classify packets based on signatures in order to avoid DDoS attacks. The process is divided into four stages, namely signature extraction, signature classification, anomaly mitigation and signature reduction. The proposed simulation model used for DDoS attack mitigation used programmable commodity switches and the enhanced grey wolf optimizer (EGWO) for detection intrusions [13], [14]. Long *et al*. [15] presented a hybrid SSAE-SVM entropy-based model for DDoS attack detection and mitigation that analyzes the number of incoming packets on a concurrent basis. If the packet request from a single source exceeds the threshold value, the model will categorize it as an attack and such data will be skipped.

3. E-HPFDDM Framework

The literature survey showed that all current research concentrates on developing an efficient security model to adequately protect against all types of HTTP DoS/DDoS attacks. In general, the majority of studies failed to create a security model that is capable of defending against all DDoS assaults. In order to fill this gap, the proposed research provides an ideal security model that can protect against all of the mentioned threats. Furthermore, it should be able to track down and block the illegitimate IP sources as well. The proposed solution uses a security model (E-HPFDDM) that is integrated with evolutionary techniques capable of detecting, classifying, and mitigating all types of HTTP DoS/DDoS assaults.

The E-HPFDDM framework automatically stops network traffic that is entering a local network if it is determined to be a HR-DDoS attack. Otherwise, when the traffic is found to be an FC attack, the algorithm tries to reduce the connection timeout value. With the KeepAlive feature of the HTTP connection disabled, different layers of the framework work together and help protect the server from these HTTP-based DDoS assaults by executing their tasks in an efficient

manner. If all protocol tests have been passed, the packets are transferred to the next layer. If not, the packets are dropped. This process is repeated until data packets are delivered to the last layer.

E-HPFDDM is a three-layer architecture. The OAB scheme at the edge router makes up the first layer of the E-HPFDDM framework, while inner service traceback (IST) makes up the second layer. The deep entropy-based (DEB) layer is the third layer, as shown in Fig. 1.

The packets that are moved to the first layer of E-HPFDDM are compared with packets in the blacklist table and are dropped if they match with any of the packets in the blacklist table. Additionally, this research created the OAB shield, a protective component for AntiDDoS systems, using the OAB scheme. It combines the alerting method used by the IST shield and AntiDDoS subsystems to notify the OAB shield subsystem about the attacker's IP sources, so that the blacklist table may be updated periodically. The OAB system uses the blacklist database to store data packets identified by the IST scheme or DEB scheme, in the case of their failure. The other element is a signaling method that the IST and DEB schemes utilize to alert the OAB scheme about the attacking IP sources. By updating the OAB scheme's blacklist table, IST and DEB schemes ban these IP sources from serving requests in the future.

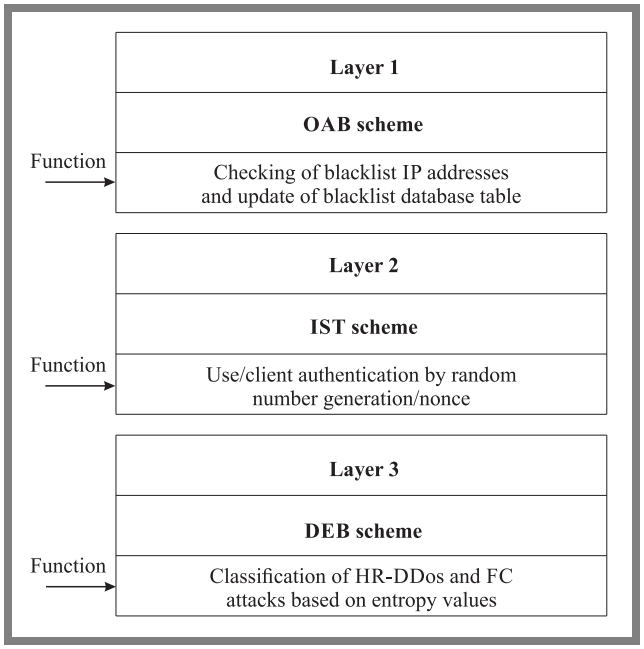

Fig. 1. Components of the E-HPFDDM framework.

E-HPFDDM's second layer uses the IST scheme that helps identify the whether the request has been initiated by a trusted user or an intruder, by validating the incoming requests. The first stage of the IST evaluates the incoming packets by scanning the header for distinct values which are only used by authorized requests. The IST scheme uses an authentication mechanism to produce a nonce value which is sent to the client or requester. The user must authenticate this nonce. If the authentication is successful, the data packet is moved to the next stage and the IP source is updated in the blacklist table.

If the intruder hacks the credentials of the victim and tries to enter the network as a trusted person, the model is trained to identify the intruder by relying on the particle swarm optimization (PSO) technique [16]–[20]. This technique allows each particle to learn its position and velocity from its neighbors.

Equation (1) represents the initial velocity, while Eqs. (2)-(5) represent the velocity of each particle that is updated based on the values of $X_{kd}(n)$ and $X_{jd}(n)$ for n iterations, until the best solution is generated for both personal best solution $P_{kd}(n)$ and the global solution $g_d(n)$:

$$R_i d(n) = X_{\mathrm{kd}}(n) - X_{\mathrm{jd}}(n), \tag{1}$$

$$R_i d(n+1) = \mathrm{CV}_{\mathrm{id}}(n) + C[P_{\mathrm{id}}(n) - X_{\mathrm{id}}(n)], \tag{2}$$

$$R_i d(n+1) = \omega V_{\mathrm{id}}(n) + C_(1) r_(1)[X_{\mathrm{id}}(n) - P_{\mathrm{id}}(n)] + C_(2) r_(2)[X_{\mathrm{id}}(n) - g_d(n)], \tag{3}$$

$$R_i d(n+1) = R_{\mathrm{id}}(n) + C_r[P_{\mathrm{kd}}(n) - X_{\mathrm{id}}(n)], \tag{4}$$

$$R_i d(n+1) = R_{\mathrm{id}}(n) + 0.5C[P_{\mathrm{kd}}(n) - X_{\mathrm{id}}(n) + P_{\mathrm{id}}(n) - X_{\mathrm{id}}(n)], \tag{5}$$

where C is the random value between 0 and 1, $X_{\mathrm{kd}}(n)$ and $X_{\mathrm{jd}}(n)$ are the particles that are randomly selected during n iterations, and $P_{\mathrm{kd}}(n)$ and $g_d(n)$ are the personal and global best solutions, respectively.

The number of source and destination IP addresses and port numbers are used as input in the initial attack detection module that is based on entropy. The values used, associated with the number of source IP addresses H_{sip}, destination IP addresses H_{dip}, source port numbers H_{sp}, and destination port numbers H_{dp}, were calculated for the first consecutive z packets using Eqs. (6)-(8). Then, the next adjacent z data packets are calculated using Algorithm 1.

Algorithm 1: Deep entropy-based algorithm for DDoS attack detection.

```
1: Input: user request's output: detection of DDoS
                                              attacks
2: Define the size of the window, Z
3: Collect sequence of data packets of size Z
4: H = {H_sip, H_dip,H_sp, H_dp}
5: If any data packet value of H exceeds
          the threshold value T, then indication
                                    of DDoS attack
6: End
```

Algorithm 1 provides a description of the module's computation procedure, while Algorithm 2 represents the deep entropy-based (DEB) technique. The DEB technique automatically stops network traffic that is entering the local network if it is determined to be HR-DDoS. Else, if the traffic is found to be an FC attack, the mechanism reduces the maximum connection timeout value, as per user requests, until the timeout value reaches zero and simultaneously disables the HTTP connection's KeepAlive feature.

The DEB scheme inspects the incoming data packet to detect HR-DDoS and FC assaults or, under regular conditions, by computing the entropy of all request as:

$$E = a \cdot \log_2 \frac{\text{number of uri counts}}{\text{total number of counts}}. \tag{6}$$

The specific source IP (sip) entropy values can be calculated using information entropy as:

$$E(\text{sip}_n) = \sum_{i=1}^{k} -p \cdot \text{sip}_n^i \cdot \log_2 p \cdot \text{sip}_n^i, \tag{7}$$

where k is the number of different source IP addresses.

The number of packets p_n with specific source address $n(\text{sip})$ for a given time t can be calculated as:

$$E(\text{sip}_n) = \sum_{i=1}^{k} -\frac{n \cdot \text{sip}_n^i}{p_n} \cdot \log_2 n \cdot \frac{\text{sip}_n^i}{p_n}. \tag{8}$$

The DEB scheme uses the Algorithm 2 that compares the obtained entropy values to the maximum threshold for HR-DDoS and FC assaults. All the incoming packets request will be blocked that have the threshold values exceeding the maximum calculated entropy values, then signaling strategy used by the AST and DAE schemes to alert the OAB scheme by updating of blacklist database and blocking of illegitimate IP sources on subsequent requests. As a result, the incoming requests are treated as legitimate.

Algorithm 2: Deep entropy-based algorithm for DDoS attack classification and mitigation.

```
1: Input: user request's, output: type of DDoS
          attack detection,
          classification and mitigation
2: Wait for user request
3: If request is NULL return declined
4:   Enable AntiDDoS service of DEB scheme at
           layer 3 of E-HPFDDM model
5:   Enable modAntiDDoS service for DDoS assaults
           detection
6:   If requested IP address is from
          whitelisted table return OK
7:   If requested remote IP address is blacklisted
          reject the remote IP from edge router
8:     Set entropy_result = ok
9:   If entropy threshold matches with the
           threshold of AntiDDoS HR_DDoS
           return blacklisted table to search
           for remote IP and reject the remote
           IP from edge router
10:  If entropy threshold matches with
           the threshold of
                  AntiDDosFlashCrowd
11:    Repeat the steps 10 to 16
12:    Decease timeout and MaxKeepAlive requests
13:    If (timeout == 0 && KeepAlive == off)
                                    return
14:    update remote_ip blacklist table
15:    reject the remote_ip from edge router
16:  End if
```

The DEB scheme uses the Algorithm 2 that compares the obtained entropy values to the maximum threshold for HR-DDoS and FC assaults. All the incoming packets request will be blocked that have the threshold values exceeding the maximum calculated entropy values, then signaling strategy used by the AST and DAE schemes to alert the OAB scheme by updating of blacklist database and blocking of illegitimate IP sources on subsequent requests. As a result, the incoming requests are treated as legitimate.

3.1. Evaluation of the E-HPFDDM Framework

Evaluation of the E-HPFDDM framework is performed during four different experimental tests of the AntiDDoS shield system. The first experiment covers the entry stage and relies on the OAB scheme. This will allow to check if illegitimate IP sources are blocked and if the blacklist is updated. The second experiment deals with the IST scheme that helps evaluate user authentication by deploying the nonce mechanism. The third and fourth experimental tests are done using the DEB scheme that helps detect and prevent HR-DDoS and FC assaults. The first and second experiments are conducted by simulating a large number of data packets that are both legitimate and illegitimate. An analysis has been performed to verify how effectively the model is classifying the data packets. The third and fourth experiments are conducted by launching a very large quantity of user requests, comparing the entropy threshold values and thereby analyzing how effectively the model is categorizing HR-DDoS and FC assaults. The experimental analysis has rendered positive results compared with existing security framework models. The simulation testbed is implemented using virtualization techniques allowing to share the resources during normal network usage [19], as illustrated in Fig. 2.

One of the following methods may be used to determine if an attack has occurred:

– Incoming data packets failing the validation tests performed by IST and DEB schemes. The incoming request must function according to its HTTP header parameters for the validation tests;
– The attacker launches an FC assault by flooding the web server with incoming data packets;
– The attacker launches a high-rate HR-DDoS assault by flooding the web application's cold web pages with many incoming requests;
– The incoming data packet requests are monitored by the edge router, so that the attacker's IP source can be blocked.

The simulation workflow is as follows:

– The client launches incoming data packet requests that are interpreted by the OAB scheme as requiring that the attacking source IP be blocked. The IST scheme authenticates the user by generation of nonce, and finally the DEB scheme detects and prevents HR-DDoS and FC assaults;
– The server responds to the particular incoming user requests after validating the distributed test plans;
– The OAB shield's router subsystem initially detects and analyses the IP source of incoming requests using the black-

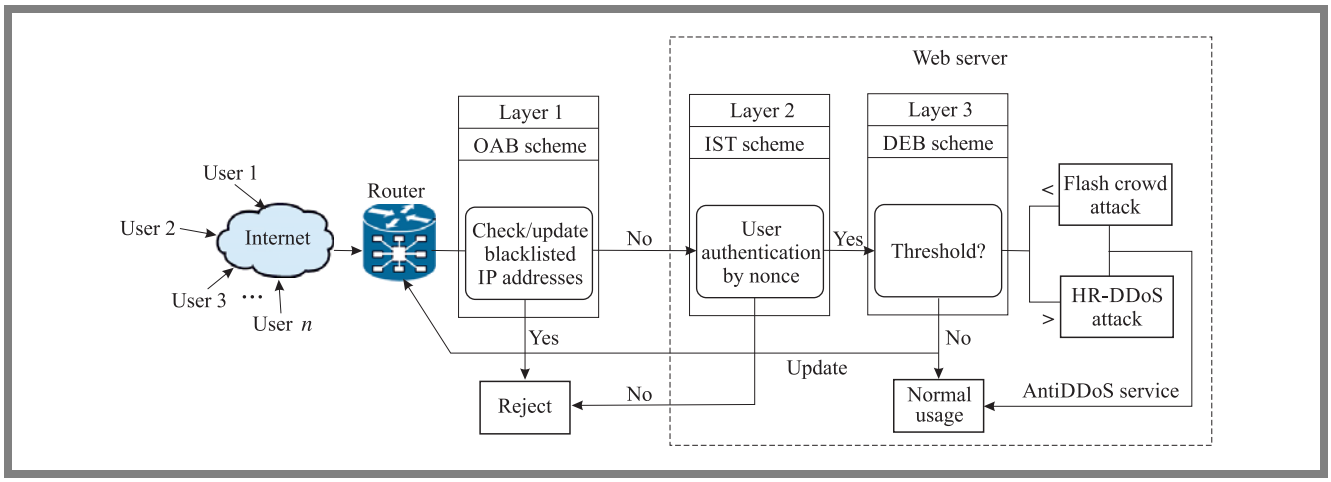

Fig. 2. Experimental setup and simulation model.

list table. The OAB shield immediately bans an attacking IP source by providing the "host unreachable" message to the requester. If not, a notification is sent to the server;

– The IST AntiDDoS system authenticates the incoming requests using the IST scheme and confirms that the request does not originate from an illegitimate user. This inbound request will move on to undergo a subsequent test within the IST shield subsystem, if it passes this human-launched test. If not, the IST shield subsystem instantly prevents it by sending the "HTTP forbidden" message to the requester. It must utilize the nonce that the IST shield subsystem gives back to address the issue appropriately.

The following AntiDDoS subsystem test will be run if the requester passes both tests. If not, the IST shield subsystem instantly prevents it by sending the "HTTP forbidden" message to the requester. Additionally, when the IST shield subsystem returns the "HTTP forbidden" message to the requester, it notifies the AOB shield subsystem, via signaling of the assaulting IP sources, thus helping update the blacklist table.

4. Results and Analysis

Evaluation of the E-HPFDDM framework is based on ideal requirements that a security system must comply with to defend against all categories of HTTP-based DoS and DDoS assaults. Based on the simulations, we may conclude that the E-HPFDDM framework's DEB scheme helps in categorizing HR-DDoS and FC assaults and, hence, helps protect the web server through the deep entropy-based algorithm capable of detecting, classifying and mitigating DDoS attacks. The experimental analysis has shown that the AntiDDoS module using the DEB scheme has detected and prevented 389,766 out of 410,000 FC attacks, thus being more efficient than existing security frameworks.

The E-HPFDDM framework's outer advanced blocking (OAB) scheme is quite capable of blocking attacker IP sources at the point of entry from the edge router. The experimental analysis has shown that the OAB scheme was successful in detecting and preventing all 410,000 attacking IP sources.

The HPFDDM framework's IST scheme is capable of validating an incoming request. The IST scheme determines whether a packet is legitimate and then passes the former while blocking the latter. It also includes a mechanism for tracing back and determining the true attacker IP source. The IST scheme uses the mechanism of nonce randomization and sends the packet to a user (rather than a bot) for authentication. The browser will authenticate the user using the nonce without any human action.

The HPFDDM framework moves the incoming data packets to the various layers and in each layer the packets have to be validated with various schemes (procedures) to defend against DDoS assaults, making the framework a collaborative, layered DDoS prevention solution. The layers of the framework collaborate and different schemes validate incoming data packets with special tests. Layer 2 helps provide nonce and authenticate the user. Similarly, the subsequent layer's DEB scheme performs the validation process with the use of special tests, such as entropy calculation, and accordingly classifies the type of DDoS assaults and attempts to mitigate the assaults accordingly.

The HPFDDM framework is easy to design and implement (this applies to all three layers) and the functionalities of each layer have been efficiently and independently distributed with proper coordination among the layers. The HPFDDM framework utilizes less bandwidth overhead when compared to existing network security solutions.

The HPFDDM framework supports the functionalities of all the layers, e.g. user authentication is performed in the application layer, using the nonce technique, and the detection and classification of DDoS assaults is performed in the network layer (e.g. HR-DDoS FC attacks).

The HPFDDM framework is integrated with evolutionary techniques, making it easier for the solution to adapt update dynamically, if needed. The IST scheme helps in updating the blacklist table when a non-legitimate IP address is detected and the DEB scheme helps in entropy calculations, based on which the DDoS attack table is updated if the DEB scheme detects HR-DDoS and FC attacks.

The designed HPFDDM framework that can support the evolutionary techniques like PSO that are integrated with DEB schemes which helps in DDoS attack detection and mitigating.

The individual layers of the E-HPFDDM framework (OAB, IST, and DEB) use very little memory for storage. The OAB layer of the E-HPFDDM framework uses much less memory for storing the blacklist table, whereas the IST layer of the E-HPFDDM framework consumes no memory at all, as all its functionalities are performed in real time. In addition, E-HPFDDM framework's DEB layer uses very little memory for storing web page-related information.

E-HPFDDM framework is resistant to spoofing assaults, as the IST scheme examines the incoming request's headers and nonce values to determine whether the requester is legitimate or illegitimate. If the requester fails these two tests, the user will be blocked immediately and the blacklist table will be updated.

5. Conclusion and Future Outlook

This study has proposed and developed an efficient hybrid protocol framework for DDoS attack detection and mitigation (E-HPFDDM), utilizing evolutionary techniques, and a unique efficient hybrid protection framework for defending against HTTP-based DoS/DDoS attacks. The unique architecture of the proposed framework eliminates all the flaws of the previous similar studies. It offers an innovative defense mechanism to safeguard online applications against all types of HTTP DoS/DDoS assaults, including high-rate HR-DDoS and FC. Additionally, it has a good ability to verify and track attacker IP sources and block them immediately, simultaneously updating the blacklist table. The E-HPFDDM framework is then assessed using the best guidelines applicable to defense systems that shield against all types of HTTP-based DoS and DDoS assaults. The simulations performed demonstrated that the E-HPFDDM framework was effective in fully meeting the applicable requirements. As the framework was unable to identify and defend against all FC assaults, a low rate of false negatives was experienced.

References

[1] A. Saravanan, S.S. Bama, S. Kadry, and L.K. Ramasamy, "A new framework to alleviate DDoS vulnerabilities in cloud computing", *International Journal of Electrical & Computer Engineering*, vol. 9, no. 5, pp. 4163–4175, 2019 (DOI: 10.11591/ijece.v9i5.pp4163-4175).

[2] R.M. Ujjan, Z. Pervez, K. Dahal, W.A. Khan, A.M. Khattak, and B. Hayat, "Entropy based features distribution for anti-DDoS model in SDN", *Sustainability*, vol. 13, no. 3, pp. 1–27, 2021 (DOI: 10.3390/su13031522).

[3] S. Dong, R. Jain, and K. Abbas, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments", *IEEE Access*, vol. 7, pp. 80813–80828, pp. 1–1, 2019 (DOI: 10.1109/ACCESS.2019.2922196).

[4] A. Alshamrani, A. Chowdhary, S. Pisharody, D. Lu, and D. Huang, "A defense system for defeating DDoS attacks in SDN based networks", *In proceedings of the ACM International Symposium on Mobility Management and Wireless Access*, pp. 83–92, 2017 (DOI: 10.1145/3132062.3132074).

[5] M. Imran, M.H. Durad, F.A. Khan, and A. Derhab, "Toward an optimal solution against denial of service attacks in software defined networks", *Future Gener. Comput. Syst.*, vol. 92, pp. 444–453, 2019 (DOI: 10.1016/j.future.2018.09.022).

[6] A. Bushra, A. Sufyan, E. Hany, B.S. Haythem, and A. Moussa, "A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets", *Computers & Electrical Engineering*, vol. 99, 2022 (DOI: 10.1016/j.compeleceng.2022.107706).

[7] J. Cui, M. Wang, Y. Luo, and H. Zhong, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN", *Future Generation Computer Systems*, vol. 97, 2019 (DOI: 10.1016/j.future.2019.02.037).

[8] M.A. Naagas, E.L. Mique, T.D. Palaoag, and J.S.D. Cruz, "Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack", *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593–600, 2018 (DOI: 10.11591/eei.v7i4.1349).

[9] R. Sahay, G. Blanc, Z. Zhang, H. Debar, "ArOMA: an SDN based autonomic DDoS mitigation framework", *Computers & Security*, vol. 70, pp. 482–499, 2017 (DOI: 10.1016/j.cose.2017.07.008).

[10] A. Mehmood, M. Mukherjee, S.H. Ahmed, H. Song, and K.M. Malik, "NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks", *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5156–5170 2018 (DOI: 10.1007/s11227-018-2413-7).

[11] N. Ravi and S.M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud", *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, 2020 (DOI: 10.1109/JIOT.2020.2973176).

[12] T. Yerriswamy and M. Gururaj, "Signature-based Traffic Classification for DDoS Attack Detection and Analysis of Mitigation for DDoS Attacks using Programmable Commodity Switches", *International Journal of Performability Engineering*, vol. 18, no. 7, pp. 529–536, 2022 (DOI: 10.23940/ijpe.22.07.p8.529536).

[13] T. Yerriswamy and M. Gururaj, "An Efficient Algorithm for Anomaly Intrusion Detection in a Network", *Global Transitions Proceedings*, vol. 2, 2021 (DOI: 10.1016/j.gltp.2021.08.066).

[14] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques", *International Journal of Distributed Sensor Networks*, vol. 13, 155014771774146, 2017 (DOI: 10.1177/1550147717741463).

[15] L. Zhang and J. Wang, "A hybrid method of entropy and SSAE-SVM based DDoS detection and mitigation mechanism in SDN", *Computers & Security*, vol. 115, 102604, 2022 (DOI: 10.1016/j.cose.2022.102604).

[16] Kamel Hasan and Abdullah Mahmood, "Distributed denial of service attacks detection for software defined networks based on evolutionary decision tree model", *Bulletin of Electrical Engineering and Informatics*, vol. 11, pp. 2322–2330, 2022, (DOI: 10.11591/eei.v11i4.3835).

[17] T. Islam, *et al.*, "A Socio-Technical and Co-evolutionary Framework for Reducing Human-Related Risks in Cyber Security and Cybercrime Ecosystems", *G. Wang, M.Z.A. Bhuiyan S. De Capitani di Vimercati, Y. Ren (eds), Dependability in Sensor, Cloud, and Big Data Systems and Applications. DependSys 2019. Communications in Computer and Information Science*, vol. 1123, 2019 (DOI: 10.1007/978-981-15-1304-6_22).

[18] T. Yerriswamy and M. Gururaj, "Study of evolutionary techniques in the field of network security", pp. 594–598, 2020 (DOI: 10.1109/ICSTCEE49637.2020.9277 082).

[19] S. Supreeth and K.K. Patil, "Hybrid Genetic Algorithm and Modified-Particle Swarm Optimization Algorithm (GA-MPSO) for Predicting Scheduling Virtual Machines in Educational Cloud Platforms", *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 7, pp. 208–225, 2022 (DOI: 10.3991/ijet.v17i07.29223).

[20] A. Pradhan, S.K. Bisoy, and A. Das, "A Survey on PSO Based Meta-Heuristic Scheduling Mechanism in Cloud Computing Environment", *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 8, pp. 4888–4901, 2021 (DOI: 10.1016/j.jksuci.2021.01.003).

T. Yerriswamy received B.E. degree in Information Science Engineering from VTU, Belagavi Karnataka, India in 2008 and M. Tech. degree in CNE from VTU in 2011. Now he is pursuing Ph.D. under VTU and working as Assistant Professor in school of CSE, REVA University, Bengaluru, India. His research interests include information and network security and soft computing.

E-mail: yssvce2123@gmail.com

School of CSE, REVA University, India

Murtugudde Gururaj received B.E. degree in Computer Science Engineering in 2000, M.Tech degree in IT in 2011 and Ph.D. in CSE in 2014. Currently working as Professor in school of CSE, REVA University, Bengaluru, India. His research interests include information and network security, big data analytics.

E-mail: gururajmurtu@gmail.com

School of CSE, REVA University, India