Babylonian Journal of Networking
Vol.2023, **pp.** 1-10
DOI: https://doi.org/10.58496/BJN/2023/001; ISSN: xxxx-xxxx
https://mesopotamian.press/journals/index.php/BJN/index

Research Article

Node Intrusion Tendency Recognition Using Network Level Features Based Deep Learning Approach

Janan Farag Yonan[1,*,], Nagham Amjed Abdul Zahra[2,]

[1] *University of Information Technology and Communications (UOITC), Baghdad, Iraq*
[2] *Dept. Of Computer Technologies Engineering, AL-Esraa University Baghdad, Iraq*

ARTICLE INFO

Article History
Received 09 Nov 2022
Accepted 05 Jan 2023
Published 23 Jan 2023

Keywords
Analytical Networking
Deep Learning
CNN
DoS
DDoS
FFNN
CBPNN

ABSTRACT

Adhoc network is highly susceptible for intrusion attacks due to the simplified access control and compacted network stack. Malicious node recognition in Mobile adhoc network (MANET) is challengeable due to nodes mobility and limited coverage of nodes. Thus, link may keep fluctuating throughout the communication period. In this paper, deep analytic model is made for extracting attacker node behaviors from networking point of view. Attributed such as link durations, re-healing time and number of received packets (by attacker) was the main features of this work. Later, deep learning paradigm is integrated to perform attacker node recognition. Data obtained from network analytical model is used to train three different models namely Feed forward neural network (FFNN), Cascade backpropagation neural network (CBPNN) and Convolutional neural network (CNN). Attacker node recognition accuracy of 85.5

1. INTRODUCTION

Computer networks are suspected to multiple operation challenges, most of those challenges are related to the security. Denial of service attacks (DoS) are representing the activity performed by the malicious nodes (attacker) on the network and hence impairing the network operations. Those attacks are usually mimicking the identity of a local node inside the network and act authentic receiver inside the network. it is then receiving the payload from the other noes and either dropping it or forwarding it to another unauthorized destination. Therefore, network will experience very big-time delay which degrade the throughput and led the network failure. The intrusion attacks involving several dangerous consequences manifested by their invisibility (silent attacks) which makes it difficult to prevent [1]. Attack is mimicking the behaviors of internal nodes to perform their malicious activity thus extra efforts required to recognize the attacker node behaviors. At [2], approaches such a Multi-Layer Perceptron (MLP) neural network with backpropagation are used for recognizing attacks alike low rate DoS which is difficult to be recognized by the regular recognition methods. A distributed denial of service (DDoS) attack is creating havoc on cloud computing networks, potentially harm cloud service availability. It's important to understand that DDoS cannot be detected using traditional detection methods. A DDoS attack detection system has been built using an updated Self-adaptive evolutionary extreme learning machine (SaE-ELM). The SaE-ELM model now includes two new features [3].

(SDN) is predicted to dramatically improve the cloud's capabilities to block DDoS attacks. DDoS attack prevention by utilising SDN's potential features, which include the ability to facilitate a global network perspective, effective network

* *Corresponding author. Email: jananfarag@gmail.com*

traffic analysis, and an improved rule updating process. The threat of DDoS on a software defined network (SDN) can be mitigated by utilising the SDN's features [4]. One of the major issues that service providers have is dealing with DoS attacks that target the application layer using slow traffic rates. To detect slow DoS attacks on HTTP, a deep classification approach based on flow data has been developed [5].

Another kind of attack known as a zero-day attack is described at [6] as weak software or applications that pose a hazard to commercial or organizational networks. A hidden Markov model is used to produce the features associated with zero-day attack behaviors. Then there's a deep learning model for attack detection and prevention in the cloud platform. The described model has been put into real-world application.

In many practical applications, security is a critical consideration in wireless sensor networks. The MAC layer attack is discussed at [7]; neural networks (NN) and support vector machines (SVM) are utilized to identify such attacks.

Due to the nonlinear nature of interruption activities, irregular traffic patterns, and numerous qualities in the issue space, the DoS attack detection framework is quite complicated. For feature identification, the Oppositional Crow Search Algorithm (OCSA) was used, and for classification, the RNN was used [8]. In this paper, it is aimed to discriminate the attacker nodes through monitoring their activity and isolating it using automatic attack prevention approach. Mobility of nodes is not considered in previous research work. It is realized that majority of attack prevention measures are valid with static nodes. However, senior is totally changed with mobility nodes. Behaviors of the attacker nodes are turned into more randomicity which cannot be traced using the traditional features of malicious attacks. Malicious attack in mobile adhoc network is being addressed in this work using signal hidden layer neural network.

2. PACKET NETWORKS

The process of data transmission in computer networks is regulated by a mechanism known as two-way handshaking. In the context of communication systems, there exists a transmission process involving two entities: the source nodes and the sink node. It is noteworthy that each individual source node demonstrates a willingness to transmit its payload to the sink node [9]. In the context of packet networks, the payload originating from a specific node is divided into smaller units known as packets, as illustrated in Figure 1. In order to facilitate the transmission of packets across nodes, it is necessary to assign certain information to each packet. This information includes the source address, destination address, packet sequence number, acknowledgment number, and MAC number. The aforementioned data is incorporated into the header of each packet and serves as a reference for the journey of the packets from the source node to the sink node.

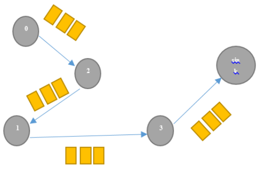

Fig. 1. Arrangement of packets network.

The packets originating from node 0 are being directed towards the sink node via the path 0-2-1-3-sink. Figure 2 illustrates the headers present in each packet overhead. The aforementioned section contains information such as source address, destination address, packet sequence number, acknowledgment address, and MAC number, which are utilised for the purpose of directing data packets among the nodes [10]. The allocation of header information is carried out by the routing protocol, and the quantity of data in the packet's overhead is one of the limiting factors affecting performance. The inclusion of additional information in the header of a packet will result in an increase in the payload size, consequently leading to a noticeable delay.

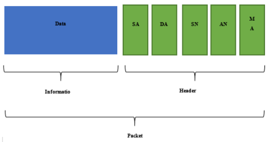

Fig. 2. header and data payload structure of a packet.

The header may contain pertinent information that aids in the prevention of malicious attacks within the network. The MAC address is a crucial component within the header, as it pertains to the unique MAC protocol address of each node.

It is worth noting that the MAC address cannot be falsified by malicious nodes [11]. The sequence number (SA) and acknowledgment number are utilised in accordance with the routing table, which is established in each node through the routing protocol. It is also associated with the bidirectional handshake process that guarantees the delivery of packets without any loss.

3. INTRUSION BEHAVIORS IN MANT

Mobile adhoc network (MANET) is involving data exchange over mobile nodes using adhoc stack [12]. This network is suspected to malicious attacks such as denial of service (DoS) attack which utmost degrade network resources. Node with DoS tendency is joining network by approaching to the network coverage and due to routing nature of adhoc network, this node will be able to listen to all signaling information. Malicious node is pretending as authentic receiver to the data packets by replying back by receiving request message to the broadcasted routing request [13]. Link is then initiated between the sending node and this malicious node where all data packets from the sending node is heading to the malicious node [14]. To this end, malicious node behaviors might change according to the nature of attack and goal of this attack [15]. Generally, malicious attack may buffer all sent packets to drop it down where the actual receiver will not get access to the required data. Furthermore, some malicious attacks are acting in other way to degrade the network resources by triggering the time out event where transmitting node is kept under excessive time delay to which prevent other nodes to get link to it. However, DoS and intrusion activity of the malicious node can be recognized by monitoring the network nodes behaviors. Hence, malicious node could be blocked upon successful and accurate recognition. Such nodes are being recognized by monitoring the time delay and the transmission time taken for the entire routing process [16]. So, it they said time is exceeding particular threshold; sending node might halt existing transmission. In most of the cases, malicious node will remain active after every halt since adhoc network is working with weak/simple management stack. Therefore, malicious node will have good chance to reattack other nodes or even the same node after each rebroadcast. From above, node may remain alert for malicious behaviors and block such behaviors if discovered at any time of transmission. several alternatives were in use to combat malicious activity, most powerful approach is by intellecting of nodes where it can detect such attack and potentially block it. For the MANET, nodes are in continuous mobility and communicate with each other with respect to coverage of each node. Cooperative transmission is obvious in MANET where out of coverage node can receive data through a relay node through multiple hobs [17]. However, MANET is again susceptible to malicious attacks same as other types of networks; in here, malicious node will conduct malicious activity either through direct link (single hop) or through retransmission (cooperative transmission through multiple hop). Another renovated problem is seen in MANET that roles of blocking malicious nodes is totally different. In other word, while attacking node is moving and the victim node is also moving then chances for recognizing the attacker node will be less comparatively with situation of static nodes. Direct connectivity between the attacker and the victim nodes might not remain constant for entire link duration. Attacker node is conducting indirect malicious attack through relay node when direct link drops (see Figure 3).

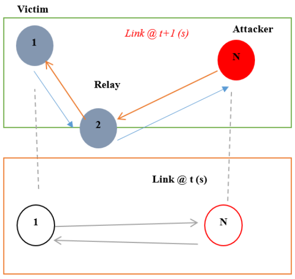

Fig. 3. a demonstration of victim-attack mobility at two different time of link duration.

4. BEHAVIORS TRACKING

Attacker node is tending to be none traceable in mobility senior since link keeps fluctuating along the simulation/communication duration. However, in order to trace the activity of attacker node in mobility event, several features are monitored. Those features are measured with respect to link established between victim and attacker node at presence of many other nodes. Features namely: link duration, re-healing time and average time delay are considered to trace out the attacker node. Link duration is measured as time taken to packet to reach the attacker node from the victim node. Since both nodes are mobilizing then link disconnection is probable here and time taken for the attacker node to resume the communication with the victim (either directly or indirectly) is termed as re-healing time. From the other hand, one vital feature is being monitored called average queuing time which represents the time taken by the attacker to acknowledge the reception of the packets from the victim. Model with specifications illustrated in Table 1 is prepared for tracing the aforementioned features.

[scale=0.4]
TABLE I. simulated model configurations and parameters.

Particle	**Details**
Number of nodes	50
Number of attacking nodes	4
Number of victim nodes	1
Workspace arena	1000m x 1000m
Routing protocol	AODV
Simulation time	30 s
Antenna	Omni directional
Node coverage	80 m
Nodes speed	Variable (10, 20, 30, 40, 50 km/h)
Node movement	Random
Transmission type	Cooperative

4.1 Link Duration

Victim-attacker connectivity keeps on varying along simulation time due to their mobility and node coverage limit e.g. 80 m omnidirectional. Knowing above fact, Victim-attacker nodes are not always connected. After conducting the proposed model (Table 1), it is realized that only 154 times the Victim-attacker nodes are getting along. Furthermore, the impact of nodes speed is realized as well while monitoring the link duration (Equation 1). The impact of speed variation of nodes is obvious in link duration (see Figure 2).

$$LD = T_a^t + T_s^t \tag{1}$$

Where, LD:is link duration, T_a^t: time (seconds) of receiption acknowledgment and T_s^t: time (seconds) when packet is sent. The faster node speed the longer as the faster nodes might return to coverage point quicker than slow moving nodes. Average link duration is measured as well (see Figure 3), average link duration is increased when node speeds is increased and the peak link duration is realized at 50 km/h speed.

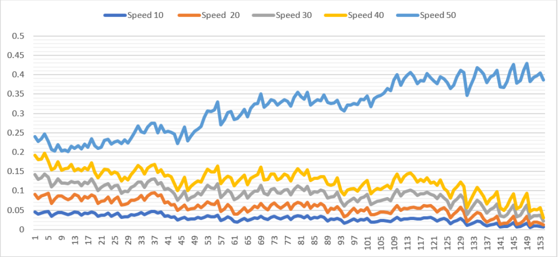

Fig. 4. instantaneous link duration versus number of active links between attacker and victim nodes.

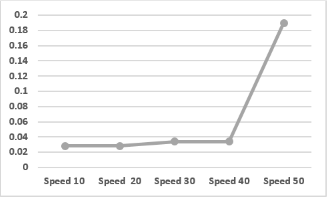

Fig. 5. average link duration versus speed of nodes.

4.2 Re-healing Time

As active connection is a function of node coverage which permits any two nodes to remain connected, link goes down if any of nodes headed out of the coverage zoon (limit). Time taken for the node to retain the connection is termed as re-healing time. This is given in Equation 2.

$$T_r h = T_a^{t+1} - T_s^t \tag{2}$$

Where, $T^{(}_{a}t + 1)$: is acknowledgment time of packet receiving after link is getting repaired, T_s^t: is the time when packet was sent before link getting drop.

TABLE II. re-healing time (second) measured for different speeds.

No	Speed10	Speed20	Speed30	Speed40	Speed50
1	0.0082301	0.00823013	0.00162005	0.00162005	0.01053951
2	0.0047776	0.00477763	0.00203458	0.00203458	0.00280399
3	0.0015540	0.00155402	0.01229111	0.01229111	0.00823924
4	0.0129075	0.0129075	0.00764681	0.00764681	0.00706576
5	0.0051427	0.00514272	0.00333577	0.00333577	0.00054488
6	0.0023669	0.00236698	0.00191931	0.00191931	0.00227419
7	0.0022379	0.00223794	0.00927927	0.00927927	0.00344242
8	0.0115669	0.01156696	0.00394734	0.00394734	0.00253112
9	0.0086812	0.00868125	0.00493853	0.00493853	0.00564228
10	0.0046240	0.00462402	0.00170531	0.00170531	0.01114388
11	0.0109631	0.01096315	0.00550282	0.00550282	0.01660625
12	0.0069299	0.00692999	0.00283909	0.00283909	0.00252758
13	0.0036239	0.00362394	0.00091811	0.00091811	0.00242978
14	0.0084014	0.00840144	0.00942925	0.00942925	0.00146127

According to Table 2, number of times that attacker node resumed the link with victim node is 15. The average of re-healing time is depicted in Figure 4. Re-healing time is reduced when speed is increased. The faster node (attacker or victim) will reduce the chances of resuming the malicious activity since nodes required enough time for new link initiation.

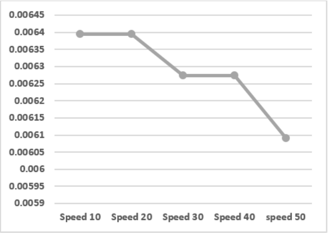

Fig. 6. Average attacker-victim link re-healing time versus nodes speed.

4.3 Average Received Packets

Packets heading from victim into attacker node is realized decreasing when nodes move faster (see Figure 5). This is measured through using Equation 3.

$$Rx_{mean} = sum_0^{T_{sim}} x \tag{3}$$

Where $T_s im$: simulation time (seconds), x: received packet counter.

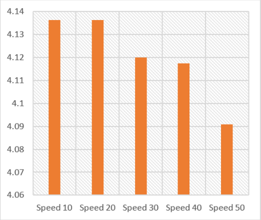

Fig. 7. average number of received packets from victim node towards attacker node.

5. INTELLIGENT MONITORING

For prevention measures, artificial intelligence has proven a noteworthy performance. There is fluctuation in the accuracy of attack detection in AI paradigms and such is related to the uncertainty of attacker node behaviors. In MANET attack prevention, deep learning is called here for enabling attacker node behaviors recognition at every node in the network. Artificial neural network (ANN) is known by its ability to learn complex problems and provide solutions by simply learning the infrastructure (hidden) relationships of the input stings [18]. For simple single hidden layer ANN (net) shown in Figure 6, supervised learning is to be initiated by providing both input vector $r = [r_1, r_2, r_3, \ldots, r_i]$ and target vector $T = [T_1, T_2, T_3, \ldots, T_i]$. Weight coefficients that intermediate the layers can be adjusted for meeting the output at minimum error [18, 19]. Error to be identified by obtaining the correlation between the resultant vector and target vector. Where r stands for random variable at $S^{\prime}0$

$$R = net(r) \tag{4}$$

$$R = Wr + b \tag{5}$$

Where R is the put vector and b is model bias. Hence, net may adjust W coefficients in order to achieve best correlation between R and T [20]. In other word, learning process is about finding the minimal value of Equation (7).

$$e = R - T \tag{6}$$

$$MSE = ({}_{(}n = 1)^{i} e(n)^{2})/i \tag{7}$$

Where e is the error vector and MSE is mean square error; MSE is considered as metric for training/learning performance [21, 22]. net is trained on guessing the velocity value that yields the best possible attacker node behaviors recognition. Attack recognition accuracy is representing the percentage of the number of correct decisions made by the AI model (CD) with respect to the total decisions made by it (TD) (see Equation 8).

$$Accuracy = \frac{CD}{TD}x100 \tag{8}$$

Three ANN models are used for this system:

- Feed Forward Neural Network (FFNN)
- Convolutional Neural Network (CNN)
- Cascade Backpropagation Neural Network (CBPNN)

5.1 Data Preparation

All models are being trained using node's behaviors dataset that made using the features obtained from simulation model, e.g. (link durations, re-healing times and number of received packets from victim by attacker node. Therefore, models are established using the configurations given at Table 3 where attacker node recognition performance can be measured.

6. RESULTS

Best model is showing high accuracy performance is the CNN model which achieved 86 percent of forecasting accuracy. Respectively, all the other parameters such as MSE, MAE, RMSE and Time and the lowest in case of CNN over the other FFNN and CBPNN. The same is depicted by Figures 6, 7 and 8.

TABLE III. Artificial neural network configurations.

Particle	**Details**
Number of hidden layers	Two (2)
Training method	LM
Number of epochs	100
Maximum gradient	1×10^{-30}
Performance metric (training)	Mean square error (MSE)
Target training performance (MSE)	1×10^{-20}
ANN types (respectively)	FFNN, CNN, CBPNN

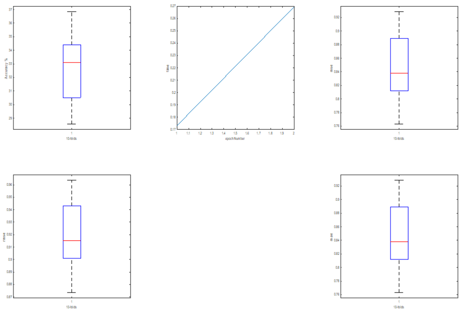

Fig. 8. FFNN performance metrics.

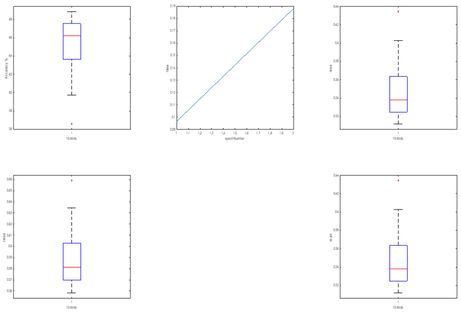

Fig. 9. CBPNN performance metrics.

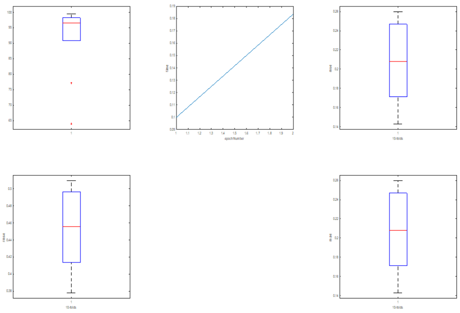

Fig. 10. CNN performance metrics.

TABLE IV. Performance comparison with previous studies.

Ref.	Method	Performance
[23]	Using Multi-Layer Perceptron (MLP) neural network with backpropagation, K-Nearest Neighbors (K-NN), Support Vector Machine (SVM), and Multinomial Naive Bayes (MNB) to discover the attack.	F1-score is used as the performance metric. Results show the best F1-score of 98.04%.
[24]	DDoS attack detection system based on an improved Self-adaptive evolutionary extreme learning machine (SaE-ELM). SaE-ELM model is improved by incorporating two more features.	Best detection accuracy is achieved, equal to 97.99%. Several datasets are used to examine the proposed system, and the system has yielded different accuracy for every dataset.
[25]	Deep classification model using flow data is proposed to detect slow DoS attack on HTTP.	The classifier is evaluated using CICIDS2017 dataset. The results obtained show that the classifier can obtain 96.61% accuracy.
Ours*	Network level features analysis for denial-of-service attack detection	Accuracy: 99.12%

7. CONCLUSION

Malicious nodes that join adhoc network are quite dangerous from network perspectives. Since it can join network and snoop on the communication and as a result it can mimic the identity of any of the authentic nodes in order to get access to the data packets. In this paper, malicious node is being monitored sing the deep analytical information from the network level which represents information regarding link durations, re-healing time and number of received packets. The case of attacker node monitoring in MANET has considered as challengeable task due to nodes mobility thus, dataset to train AI models for attack detection is formed using the mentioned network level features. Three deep learning models were in use namely: FFNN, CBPNN and CNN. Best recognition accuracy is drawn by CNN model with 99.12

Conflicts Of Interest

None

Funding

None

Acknowledgment

None

References

[1] T. Kim and W. Pak, "Real-time network intrusion detection using deferred decision and hybrid classifier," Future Generation Computer Systems, vol. 132, 2022.

[2] V. de M. Rios et al., "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," Computer Networks, vol. 186, 2021.

[3] G. S. Kushwah et al., "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," Computers Security, vol. 105, 2021.

[4] P. Harikrishna et al., "Rival-Model Penalized Self-Organizing Map enforced DDoS attack prevention mechanism for software-defined network-based cloud computing environment," Journal of Parallel and Distributed Computing, vol. 154, 2021.

[5] N. Muraleedharan and B. Janet, "A deep learning-based HTTP slow DoS classification approach using flow data," ICT Express, vol. 7, 2021.

[6] Y. Aoudni et al., "Cloud security-based attack detection using transductive learning integrated with Hidden Markov Model," Pattern Recognition Letters, vol. 157, 2022.

[7] D. Yu et al., "Service Attack Improvement in Wireless Sensor Network Based on Machine Learning," Microprocessors and Microsystems, vol. 80, 2021.

[8] R. S. Theja et al., "An efficient metaheuristic algorithm-based feature selection and recurrent neural network for DoS attack detection in cloud computing environment," Applied Soft Computing Journal, vol. 100, 2021.

[9] C. Modi et al., "A survey of intrusion detection techniques in cloud," Proc. J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42-57, 2013, Elsevier.

[10] B. Wang et al., "DDoS attack protection in the era of cloud computing and software-defined networking," in Proceedings of the Computer Networks, vol. 81, IEEE, Raleigh, NC, USA, 2015, pp. 1092-1648.

[11] C. Modi et al., "A survey on security issues and solutions at different layers of cloud computing," Proc. J. Supercomput., vol. 63, no. 2, pp. 561-592, 2013, Springer.

[12] S. Yu et al., "Can we beat DDoS attacks in clouds," Proc. IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2245-2254, 2014, IEEE.

[13] A. Girma et al., "Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment," in Proceedings of the 12th International Conference on Information Technology-New Generations (ITNG), IEEE, Las Vegas, NV, USA, 2015, pp. 212-217.

[14] A. Chonka et al., "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," Proc. J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1097-1107, 2011, Elsevier.

[15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Proc. J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, 2011, Elsevier.

[16] M. T. Khorshed et al., "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Proc. Future Gener. Comput. Syst., vol. 28, no. 6, pp. 833-851, 2012, Elsevier.

[17] J. Choi et al., "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment," Proc. Soft Comput., vol. 18, no. 9, pp. 1697-1703, 2014, Springer.

[18] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack its effect in cloud environment," in Proceedings of the Procedia Computer Science, vol. 49, Elsevier, 2015, pp. 202-210.

[19] Q. Chen et al., "CBF: a packet filtering method for DDoS attack defense in cloud environment," in Proceedings of the Ninth International Conference in Dependable, Autonomic and Secure Computing (DASC), IEEE, Sydney, NSW, Australia, 2011, pp. 427-434.

[20] R. Lua and K. C. Yow, "Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network," Proc. IEEE Netw., vol. 25, no. 4, pp. 28-33, 2011, IEEE.

[21] E. Anitha and S. Malliga, "A packet marking approach to protect cloud environment against DDoS attacks," in Proceedings of the 20th International Conference on Information Communication and Embedded Systems (ICICES), IEEE, Chennai, India, 2013, pp. 367-370.

[22] S. S. Chapade et al., "Securing cloud servers against flooding-based DDoS attacks," in Proceedings of the Communication Systems and Network Technologies (CSNT), IEEE, Gwalior, India, 2013, pp. 524-528.

[23] V. de M. Rios et al., "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," Computer Networks, 2021.

[24] G. S. Kushwah et al., "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," Computers Security, 2021.

[25] P. Harikrishna et al., "Rival-Model Penalized Self-Organizing Map enforced DDoS attack prevention mechanism for software-defined network-based cloud computing environment," Journal of Parallel and Distributed Computing, 2021.