International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secure Multi-Path Communication through Dynamic Path Identifiers to Prevent Denial-of-Service Flooding Attacks

Ashok Kumar Yadav [1], Vijaya Bhaskar. Ch [2], Nagaraju .M [3], J Emerson Raja [4], Sachin S. Pund [5], Ms. Alka Kumari [6]

Submitted: 01/11/2022 **Revised:** 13/01/2023 **Accepted:** 31/01/2023

Abstract: Denial of service is characterized by the explicit attempt of the attackers to prevent legitimate user services. With the distributed denial-of-service multiple machines are deployed machines in the network. The denial of service affects the packet stream with the key resources rendering the legitimate clients to provide the ultimate access to the arbitrary damage. In DDoS environment the attacks are distributed with the largescale attempt the malicious users for the enormous number of network packets. The proposed model uses the weighted adaptive cache clustering (WACC) model for the denial of service flooding attacks in the network. The proposed WACC model uses the adaptive model in the estimation of the attack scenario in the network. The proposed WACC model exhibits the reduced False positive Rate, throughput and response rate. The proposed WACC model achieves the maximal delay of 35.41 ms while the conventional TEV achieves the maximal packet delay of 38.15ms and EMC provides the 42.69ms. The estimation expressed that the proposed WACC model achieves a higher throughput value of 88.35%. The analysis concluded that the proposed WACC model achieves improved performance for the prevention of denial-of-services flooding attacks.

Keywords: *Denial of Service, Flooding Attack, Weighted Adaptive Model, Security*

1. Introduction

Distributed denial-of-service attacks (DDoS) are observed as a severe threat to the defense scheme for the combat process [1]. The attackers in the network alter the security system tools for handling the new attacks in the network. The field of DoS and flooding attacks affects the hard process to resolve the problem of global view [2 -4]. The DDoS structure of the taxonomy of operation for the attack evaluation. The process of flooding and DoS attacks impacts on the complete performance it is necessary to evaluate the data sense for the taxonomy of the attack and appear as the taxonomy for the different attacks [5]. At present, potential threats are associated with the current mechanism. At first, the presence of DoS attack elects the brunt attack with the reception. Secondly, through the daemon attack agents in the network. The program agents focused on the targeted victim for the actual data. The DoS and flooding attack comprises of the host computer deployment for the targeted devices [6].

The deployment of the attacker in the network through DoS and flooding attack to access the gain in the host computer [7]. Finally, the third components compriseof the DoS attack with the master control program for the coordinate attacks. Finally, with the presence of the real attacker mastermind in the presence in the network. With the controlled master scheme the real attacker is lies in the attack scenes. The DoS environment in the distributed environment is presented as follows [8 - 10]:

1. The attacker in the real time environment the messages are controlled by the master program
2. Through control message program “execute: message are received and propagated with the DoS command in the control environment.
3. Upon the reception of the attacker command the daemons begin to victim and considered as attack.

Generally, the DoS attack comprises of the 4 components

[1]*Professor, Department of Computer Application, Galgotias University, Greater Noida, Uttar Pradesh, India.*
ashok.yadav@galgotiasuniversity.edu.in
0000-0003-4807-2698
[2]*Sreenidhi Institute of Science and Technology, Information Technology, Hyderabad, India.*
Vijayabhaskar.ch@gmail.com
0000-0002-2108-5993
[3]*Sreenidhi Institute of Science and Technology, Information Technology, Hyderabad, India.*
nagarajucse11@gmail.com
0000-0003-4147-0108
[4]*Senior Lecturer, Faculty of Engineering and Technology, Multimedia University, Selangor, Malaysia.*
emerson.raja@mmu.edu.my
https://orcid.org/0000-0002-4512-0802
[5]*Assistant Professor, Department of Industrial Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India.*
pundss@rknec.edu
https://orcid.org/0000-0002-5616-2469
[6]*Assistant Professor, School of Eng.&IT, ARKA Jain University, Jamshedpur, Jharkhand, India.*
alka.k@arkajainuniversity.ac.in
0000-0002-0471-3759

for the processing. Initially, the consideration of host with selection of the brunt attack in the receiver. Secondly, DoSattack comprises of the daemon agents for the processingwhere program agents are actually conducted for the victim target [11]. The agent in the attackers are installed in the host computers where the secondary victims affects the computer and target. The deployed task comprises of the attacker gain processs with the host computer infiltrate. Thirdly, the component is distributed in the control master of the program for the attack coordinate. Finally, the actual attacker computes the master program with the attacker module in the attack scenario. This paper focused on the DoS and flooding attack in the network using the WACC model for the security improvement in the networking environment.

2. Related Works

In [12]described the wireless ad hoc network with the collection of the two or more equipmentfor wireless communication to increase the capability of the network. Even though vast range of research is conducted for the mobile ad hic architecture with the flawed model. In [13] evaluated the different DoS attacks in the network. The estimation is based on the consideration of the defense principles with the different DoS attacks. The developed model integrate the victim based DoS defense scheme with the packet transmission through mitigation of the attacks. The process of funnel is evaluated based on the destination node to eliminate the node congestion for the access link in the node. The proposed model integrates the collaboration between the nodes with the overhead and delay in the load. With the funneling model the DoS traffic is estimated for the integration of the Statistical Filtering against DDoS Attacks. In [14] presented a DoS scheme for the large-scale distributed environment to prevent and evaluate the flood attacks in the vast range of packet count in the network. The proposed DoS model comprises of the estimation of the bandwidth for resources, power computation and so on. The estimation of the legitimate information in the network are evaluated based on the deteriorated model. The developed model uses the hop-count filtering, statistical and rate-limiting approach. Through the consideration of the wired communication in the network the effective mechanism is evaluated in the MANET for the prevention of the DoS and flooding attacks in the network. The vulnerability of the MANET is computed based on the statistical filtering analysis through provision of the DoS attacks in the network.

In [15] described the computation of the DoS attack in the e-commerce companies in the active scanning for the attackers in the network. With the futured DoS attacks in the future evaluation is computed for the improved security. In [16] the DoS attacks are computed based on the information provision in the network to address the different level with the derivative of the potential global solution through the incentive framework.

3. Weighted Adaptive Cache Clustering (WACC) Model for the DoS attack Prevention

The proposed WACC model comprises of the prevention of the DoS and flooding attack with the on-demand ad hoc networking environment. In the wireless networking environment few of the attackers are malicious and some nodes are dropped for the forwarding of the all data packet without any congestion.

Consider WACC of the node as DoS and flooding attack as if $(n_i=(naddress_{i+1})\%$ &&$(n_j=(naddress_{j+1})<\beta)$

Where,

$n_i$stated as thei^{th} node for the established session,

$n_j$neighboring node weight involved in the communication environment

β defined as the node weights with the computation of the distance in the communication. The established communication range of nodes is defined as 0, 4, 8, 12, 16, 20, 24, 28 etc for the malicious node. Those node in the network leads to packet dropping and data forwarding in the network environment.

The WACC model update the weights to the Cache to evaluate the presence of the DoS attack in the network model with the computation of the statistics Forward Percentage (FP) for the sufficient period of time T as presented in equation (1)

$$FP_m = \frac{Actual\ Packets\ Forwarded}{Forwarded\ Packets} \quad (1)$$

In the WACC the FP computes the packet forwarded over the transmitted information ranges from the M to m with forwarding. The $FP_i = 0$ need to be evaluated for the denominator for the Unconditional Packet Dropping with the attack identification. In the WACC model the node monitoring is computed with the monitored node m as the process is presented in the figure 1.

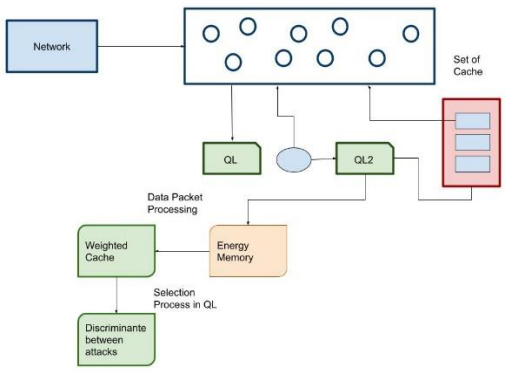

Fig. 1: WACC model in the DoS attack

A flag status is employed inDDoS-FC method for mentioning QL that is already visited and able to transmit the request packet to other nearest QL. This process is repeated for all other QLs until they are totally gettingverified. In addition, visited QL is removed from the packet only when data request packet accomplishes its QL. Data packet is forwarded to QL, followed by data packet is sent to carrier nodes CN. Then the data packet is sent to corresponding source mobile element.

Algorithm 1: WACC path identifier model for attack prevention

Let DReq denote data request made by source mobile element SMEi to identify the destination DMEiwith reply represented as DRep

For i = 1 to m

For j = 1 to n

For k = 1 to s

If (QL found for SMEi) then

Forward to CNk

Send reply DRep to SMEi

Else

Place request DReq to the server

Send reply DRep to SMEi

End for (//k)

End for (//j)

End for (//i)

Repeat

If $SME_i < \delta_i$

MEi = suspicious mode

Else

MEi = normal mode

MEi = QL

QL = QL[MEi+ 1]

End if

Until (δj<δi)

The data packet processing algorithm is explained to ignore the harmful data requests in the network. At first, for each mobile element, destination mobile element and carried node, Query List is identified. If the Query List is identified, then corresponding QL is removed as earlierthe data packet is forwarded to the carried nodes. Followed by, data packet reply is sentto respective source mobile element. In case, the Query List is not identified for source mobile element, then the data packet request process will be verified with other QLs, finally followed by server which currently becomes the carrier node.Subsequently, the DReprequest is sent to the corresponding source mobile element. Data packet processing is carried out until all the QL elements are to be checked. At the time of performing this scenario, server removes data request packet obtained from mobile element to avoid damaging requests for accessing data. This in turns, the DDoS-FC method achieves maximum response rate and minimum false positive alarm.

Step 1: Counting Filter (C-1): Computes the SYN packets evaluated for the connection in the network

Step 2: Counting Filter (C-2): With the packets SYN the connection need to perform three-way handshake estimation.

Step 3: Counting Filter(C-3): Records the packet SYN

The mitigation scheme starts working once detecting SYN floods. If a SYN packet is received, its 4-tuple is extracted as an item and queried from the three Counting Filter.

4. Results and Discussion

The performance of the proposed WACC model is evaluated in the NS3 simulation environment. The proposed model is constructed in the network topology with the incorporation of the source and destination nodes in the network. Table 1 incorporates the simulation setting for the proposed WACC model and parameter values are provided.

Table 1: Simulation Setting

Parameters	Value
Area	1000*1000 m
Node Count	500
Duration of Simulation	500 sec
Repetition count	8 times
Transmission range for communication	1000 m
Physical/Mac layer	IEEE 802
Pause time	120 sec
Model for mobility	Random waypoint model
Movement of Nodes	3 – 15 m/s
Data sending rate	2.3 kbps
Packet size	2 mega byte

As shown in table 1, NS3 simulation modeled a network in a 1000m * 1000 m area with 500 nodes (i.e., mobile

elements). Radio broadcast range for every node was assumed to be 1000 m. Velocity of each mobile node is considered from the rage of 3 - 15 m/s. Mobility of the mobile nodes is considered as arbitrary. Performance of the proposed DDoS-FC is measured with the factors such as average packet delay, throughput, response rate and false positive alarms.Average packet delay in DDoS-FC is defined as the time delay between transmitting and receiving of packets to mobile elements (i.e., nodes) in a network. Average Packet Delay (APD) is mathematically formulated as in equation (2).

$$APD = Packet\ Recieved\ time - packet\ transmitetd\ time \quad (2)$$

From (2),APD is measured as the difference between packet transmission time and packet received time. It is measured in terms of milliseconds (ms). If average packet delay is low, then the method willsaid to be more efficient.

Throughput is measured as the ratio of successful packet delivery among mobile elements (nodes) over a communication medium to total number of packets. Throughput is mathematically formulated as in equation (3).

$$Throughput = \frac{Number\ of\ Packets\ successfully\ delivered}{Total\ number\ of\ Packets} * 100 \quad (3)$$

From (3), the computation of the percentage (%) if the value is higher than the technique is more efficient.

Response rate (RR) is measured as the ratio of response obtained using carrier nodes to total number of available carrier nodes. Response rate is mathematically formulated as in equation (4)

$$RR = \frac{Obtained\ Response\ Node\ Obtained}{Total\ carrier\ node\ available} * 100 \quad (4)$$

From (4), represented as in the measured in the % with the higher RR the performance is more efficient.

False Positive Alarm (FPA) is calculated as the ratio between number of incorrectly identified false crowd events as DDoS attacks (false positives) and total number of actual DDoS attacks. False positive alarm is mathematically formulated as in equation (5)

$$FPA = \frac{Incorrectly\ identified\ false\ DDoS\ crowd}{Total\ DDoS\ attack} * 100 \quad (5)$$

The performance of the proposed WACC model is comparatively examined with the TEV and EMC model. The node ranges between 0 – 100 for the examination is computed based on the average packet delay as in table 2.

Table 2: Comparison of Average Packet Delay

Number of nodes	Average Packet Delay(ms)		
	TEV	EMC	Proposed WACC
10	27.42	31.24	23.15
20	28.55	32.51	25.36
30	30.24	33.84	26.51
40	31.48	35.07	27.39
50	32.26	36.59	29.72
60	33.17	37.46	30.24
70	35.06	39.04	31.47
80	36.84	40.62	32.69
90	37.43	41.84	34.85
100	38.15	42.69	35.41

In the figure 2 the comparison of the proposed WACC model with the existing mode is presented. In the table 3 the comparative analysis of the throughput is presented. The figure 3 provides the comparative analysis of the through estimated for the proposed WACC model with the existing TEV and EMC model.

Table 3: Comparison of Throughput

Number of Nodes	Throughput (%)		
	TEV	EMC	Proposed WACC
10	69.42	61.58	75.26
20	70.47	63.87	76.35
30	71.63	64.46	78.41
40	72.84	65.63	79.16
50	73.19	66.18	80.49
60	75.04	68.09	81.55
70	76.64	69.84	83.48
80	78.18	71.15	85.69
90	79.54	72.74	86.73
100	81.77	74.48	88.35

The estimation of the response rate of the system for the different model is computed for the varying number of packets as presented in the table 4.

Table 4: Comparison of Response Rate

Number of packets	Response Rate (%)		
	TEV	EMC	Proposed WACC
50	58.54	52.18	65.15
100	61.26	55.63	67.29
150	63.57	57.48	70.36
200	64.81	59.76	71.59
250	67.19	61.29	73.48
300	69.47	62.46	75.96
350	72.09	65.22	79.15
400	74.56	67.41	82.18
450	76.72	69.83	84.67
500	77.93	72.14	85.51

Through the examination of the packets the response rate is evaluated for the TEV and EMC model for the varying packet count. The estimated value is measured as the 85.51% for the packet count of 500. In the table 5 the false positive alarm for the proposed WACC model is presented.

Table 5: Comparison of False Positive Alarm

Number of Nodes	False positive alarm (%)		
	TEV	EMC	Proposed WACC
10	26.24	30.14	20.15
20	28.43	32.48	23.42
30	31.49	35.12	25.63
40	33.58	38.24	28.47
50	35.76	40.15	31.53
60	37.68	41.59	33.18
70	40.07	43.62	36.71
80	42.57	47.68	38.46
90	45.86	49.17	41.68
100	47.19	51.48	43.83

The figure 2 – 5 provides the comparative analysis of the proposed WACC model with the existing TEV and EMC mode is provided for the average packet delay, throughput, response rate and false positive alarm.

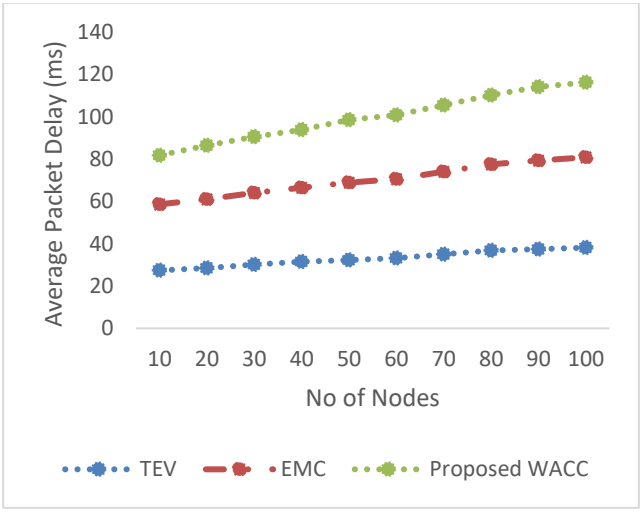

Fig. 2: Comparison of Average Packet Delay

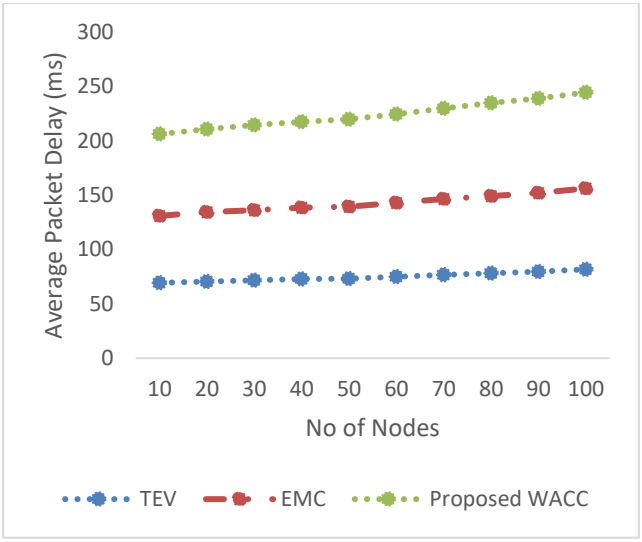

Fig. 3: Comparison of Throughput

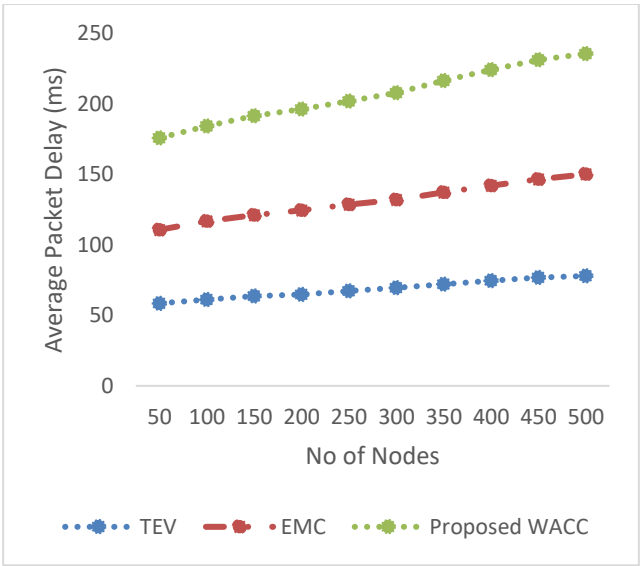

Fig. 4: Comparison of Response Rate

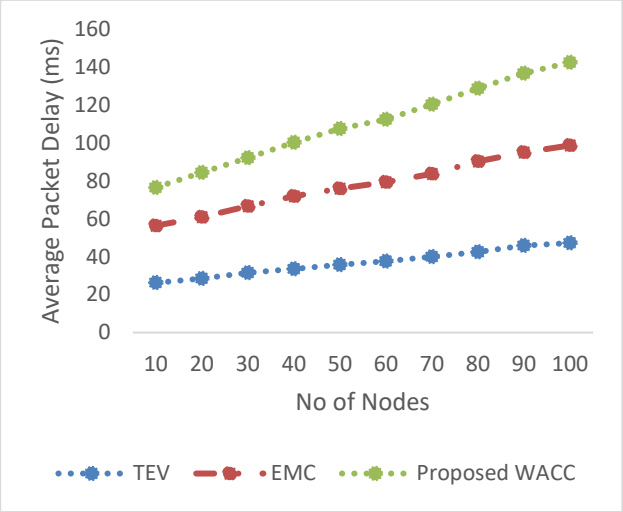

Fig. 5: Comparison of False Positive alarm

The proposed WACC model evaluate the DoS and flooding attack method effectively utilizes an adaptive caching system to discover DDoS attacks in a network. Adaptive cache mechanism offers reliable caching scheme in network environments by performing the reduction of network traffic. In proposed WACC architecture, server needs to be updated with the aim of protecting the network traffic. WACCmethod adjusts the process of caching a data item and updating it using server with respect to the requests placed by mobile element in hybrid network environment. Carrier nodes and query list are mainly employed in the process of discriminating DDoS attack and flash crowds using adaptive cache mechanism. With the objective of improving response rate and reducing false positive alarm, proposed WACCmethod follows pro-active load distribution scheme.

5. Conclusion

Denial of Service and flooding attack affects the performance of the network affects data in the network. To evaluate the performance of the network proposed WACC model update the information in the cache. The cache computes the attack characteristics in the network to prevent the attack in the DoS and flooding attack. The Performance of WACCmethod is evaluated in terms of throughput, average packet delay, false positive alarm and response rate. From experimental results, it is observed that WACCscheme achieves better result and provides a better caching scheme in network environment by reducing false alarm rate and improving response rate. The developed mode decreases the packet delay ~4% with the improved throughput value of ~3% than the conventional technique.

References:

[1] Kurian, S., & Ramasamy, L. (2021). Securing Service Discovery from Denial of Service Attack in Mobile Ad Hoc Network (MANET). *International Journal of Computer Networks and Applications*, *8*(5), 619-633.

[2] Islam, M. N. U., Fahmin, A., Hossain, M., & Atiquzzaman, M. (2021). Denial-of-service attacks on wireless sensor network and defense techniques. *Wireless Personal Communications*, *116*(3), 1993-2021.

[3] Xu, Y., Deng, G., Zhang, T., Qiu, H., & Bao, Y. (2021). Novel denial-of-service attacks against cloud-based multi-robot systems. *Information Sciences*, *576*, 329-344.

[4] Radain, D., Almalki, S., Alsaadi, H., & Salama, S. (2021, March). A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing. In *2021 International Conference of Women in Data Science at Taif University (WiDSTaif)* (pp. 1-6). IEEE.

[5] Thangavel, S., & Kannan, S. (2022). Detection and trace back of low and high volume of distributed denial-of-service attack based on statistical measures. *Concurrency and Computation: Practice and Experience*, *34*(8), e5428.

[6] Tripathi, N., & Hubballi, N. (2021). Application layer denial-of-service attacks and defense mechanisms: a survey. *ACM Computing Surveys (CSUR)*, *54*(4), 1-33.

[7] Alamiedy, T. A., Anbar, M. F., Belaton, B., Kabla, A. H., & Khudayer, B. H. (2021, August). Ensemble Feature Selection Approach for Detecting Denial of Service Attacks in RPL Networks. In *International Conference on Advances in Cyber Security* (pp. 340-360). Springer, Singapore.

[8] Gupta, B. B., Chaudhary, P., Chang, X., & Nedjah, N. (2022). Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering*, *98*, 107726.

[9] Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, *4*(4), 482-503.

[10] Muhammad, A. W., Foozy, C. F. M., & Azhari, A. (2020). Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection. *International Journal of Artificial Intelligence Research*, *4*(1), 1-8.

[11] Gohil, M., & Kumar, S. (2020, December). Evaluation of classification algorithms for distributed denial of service attack detection. In *2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)* (pp. 138-141). IEEE.

[12] Alhaidari, F. A., & Alrehan, A. M. (2021). A simulation work for generating a novel dataset to detect distributed denial of service attacks on Vehicular Ad hoc NETwork systems. *International Journal of Distributed Sensor Networks*, *17*(3), 15501477211000287.

[13] Mihoub, A., Fredj, O. B., Cheikhrouhou, O., Derhab, A., & Krichen, M. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Computers & Electrical Engineering*, *98*, 107716.

[14] Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236-42264.

[15] Kuadey, N. A. E., Maale, G. T., Kwantwi, T., Sun, G., & Liu, G. (2021). DeepSecure: Detection of Distributed Denial of Service Attacks on 5G Network Slicing—Deep Learning Approach. *IEEE Wireless Communications Letters*, *11*(3), 488-492.

[16] Maranhão, J. P. A., da Costa, J. P. C., Javidi, E., de Andrade, C. A. B., & de Sousa Jr, R. T. (2021). Tensor based framework for Distributed Denial of Service attack detection. *Journal of Network and Computer Applications*, *174*, 102894.