Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.027910
Article

Tech Science Press

Progressive Transfer Learning-based Deep Q Network for DDOS Defence in WSN

S. Rameshkumar[1,*], R. Ganesan[2] and A. Merline[1]

[1]Department of Electronics and Communication Engineering, Sethu Institute of Technology, Virudhunagar, Tamilnadu, India
[2]Department of Electrical and Electronics Engineering, E. G. S. Pillay Engineering college, Nagapattinam, Tamilnadu, India
*Corresponding Author: S.Rameshkumar. Email: srameshkumarst@gmail.com
Received: 27 January 2022; Accepted: 02 April 2022

Abstract: In The Wireless Multimedia Sensor Network (WNSMs) have achieved popularity among diverse communities as a result of technological breakthroughs in sensor and current gadgets. By utilising portable technologies, it achieves solid and significant results in wireless communication, media transfer, and digital transmission. Sensor nodes have been used in agriculture and industry to detect characteristics such as temperature, moisture content, and other environmental conditions in recent decades. WNSMs have also made apps easier to use by giving devices self-governing access to send and process data connected with appropriate audio and video information. Many video sensor network studies focus on lowering power consumption and increasing transmission capacity, but the main demand is data reliability. Because of the obstacles in the sensor nodes, WMSN is subjected to a variety of attacks, including Denial of Service (DoS) attacks. Deep Convolutional Neural Network is designed with the state-action relationship mapping which is used to identify the DDOS Attackers present in the Wireless Sensor Networks for Smart Agriculture. The Proposed work it performs the data collection about the traffic conditions and identifies the deviation between the network conditions such as packet loss due to network congestion and the presence of attackers in the network. It reduces the attacker detection delay and improves the detection accuracy. In order to protect the network against DoS assaults, an improved machine learning technique must be offered. An efficient Deep Neural Network approach is provided for detecting DoS in WMSN. The required parameters are selected using an adaptive particle swarm optimization technique. The ratio of packet transmission, energy consumption, latency, network length, and throughput will be used to evaluate the approach's efficiency.

Keywords: DOS attack; wireless sensor networks for smart agriculture; deep neural network; machine learning technique

1 Introduction

Cloud Wireless sensor networks have been vulnerable to a variety of attacks that constitute a major danger to network security, DDOS attacks. Although some technology has learnt detection and

mitigation, the difficulty and cost of enhancing the finding of complicated detection processes is unfavourable. DDOS attacks produce a loss of quality of service (QoS) because malicious nodes can read the origin node or transfer more data, which dramatically overwhelms the system, allowing malicious nodes to develop numerous type of attacks. To address these network security flaws, we propose a new sinkhole detection approach to encourage the improvement of wireless sensor network QoS. The affected nodes can be confused with the routing mechanism in a DDOS attack. The channel between intruder nodes can be used by intruder nodes to transport packets from one location to another. As a result, the development's purpose is to increase data quality, reduce packet loss, and employ novel ways for detecting and preventing DDOS assaults on data sent from source to destination.

2 Related Work

To determine all permissible paths, the target node uses the network to deliver a data packet Route Request (RREQ). When attacker 1 receives the RREQ packet, it collaborates with attacker 2 to send it to the destination node, thus it sends it to attacker 2 and the target node across the DDOS link. Due to a DDOS link and collusion with the attacker, some of the RREP packets delivered by the destination node are returned to the target node. In order to use RREP packets securely, the collusive attacker transmits them to the target node.

DDOS attacks and low-latency connectivity from the heavy activate them in various parts of the message received by malicious nodes of the network. Due to the nature of wireless transmission, an attacker can generate a DDOS by listening to the radio transmission and sending a packet to himself on the other end of the DDOS, the joint attack. Tunnels can be built in a variety of ways, including covert channels (such as wire connections), pocket connections, and high-power transfer. Because the two smaller points are so near together, they can be compared to a smaller or smaller number, allowing the tunnel to enter the pocket as soon as it follows its typical path.

The attack master uses software framework and handles the types of attacks. The software initiates the process at master nodes and gains control of all the nodes in the network. It further decentralizes the control to the nodes at individual level. The algorithm proposed in paper will be able to handle the scenario for all types of DDoS attack. Considering the agricultural field the paper addresses with a solution of using algorithm for decentralizing the type of attacks. The autonomy is reached at all the nodes over a period of time.

To monitor environmental or physical factors such as temperature, soil moisture, humidity, and pre-transmission and data gathering for self-configuration centres or sinks, the wireless sensor network employs the following architecture. Data from a wireless network (base station) can be processed and analysed further. The majority of wireless sensor networks are found in hazardous and unstable situations. Sensor nodes are constrained by unreliable communication mediums and limited resources, necessitating the need of complex security methods.

Wireless multimedia sensor networks are a relatively new development in wireless sensor networks. It collects scalar parameters from the sensors that are used, with the ability to extract and process multimedia for transmission. Temperature, humidity, and soil moisture are among the variables collected from various sensor nodes. As a result, they are being investigated in a variety of domains, including agriculture, remote surveillance, and environmental monitoring [1]. Multimedia data is similarly large and consumes more power [2]. Wireless multimedia sensor networks, in general, need a lot of electricity [3]. A system must be developed with the goal of consuming the least amount of electricity possible. Because multimedia transmission costs more energy, present approaches are unable to meet high power demands. The method presents neural networks that can be adapted for use in a wireless multimedia network. In wireless sensor networks, previous research has focused on intrusion detection using neural networks. In this case, neural networks [4] have been altered for use with WMSN. In diverse domains, many intrusion

detection techniques have been developed for WSN [5]. Data mining, mobile agents, game theory, statistical, and genetic algorithms are all elements.

The asymmetry map was introduced by Anthony Tannoury, Rony Darazi, and colleagues [6] to collect a comprehensive view of multimedia data. Wireless multimedia sensor networks are a difficult technology to implement since they capture data connected to the real time environment. The sensor network keeps an eye on the area under monitoring. Depth information, which may be collected by 3D depth analysis, is essential in order to achieve clear view of the occurrence. In this study, a disparity map was built from several photos in order to monitor the object's depth information. Providing a successful real-time solution ensures a reduction in computation time. The sensors involved take images from the desired locations and build a disparity map based on stereo matching. The map reduces the impact of traffic on bandwidth, extending WMSN's lifespan. If the depth value of the target item is established, a comprehensive detection of the event can be carried out. Users can acquire 3D scene reconstruction as well as images referred to by nodes.

A Comparative Analysis of Wireless Sensor Networks with Wireless Multimedia Sensor Networks was proposed by Ahmed Mateen et al. [7]. This publication gives us a thorough overview of the WSN and WMSN comparison. In general, WSN adheres to low-cost, low-power, and high-density sensor nodes and base stations. Even though the nodes are small, they hold a lot of information. The sensors provide event detection, order processing, and data transfer while eliminating the shortcomings of conventional WSNs. in wireless multimedia sensor networks await, channel utilisation, throughput during the network's lifetime, and distortion are all fixed parameters that affect multimedia data. These parameers ensure that the networks are delivered as efficiently as possible. In the case of WMSN, the difficult element is ensuring resource constraints, high data rates, and a low energy delay limit. The research provided here was a comparison of different WSN and WMSN methods.

Wael Ali Hussein et al. [8] performed a design and performance analysis on the High Reliability-surest Routing protocol for Mobile Wireless Multimedia Sensor Networks. They've created a contract focused to scalar data, such as sensor data, which is far smaller than multimodal statistics. The research addressed the shortcomings of the current framework and proposed a design for mobile, trustworthy routing protocol-based networks. Following grabbing forwarding, it is a new routing protocol with varying strength throughput multipath routing protocol (GFTEM). The hop node with the highest throughput is chosen, and the destination should be closer. The proposed GFTEM's evaluation is compared to the existing routing protocols. In Wi-Fi networks, for example, the Ad-hoc On Demand Vector (AODV) routing protocol [9], the Dynamic MANET on Demand (DYMO) routing protocol [10], and the greedy perimeter stateless routing protocol [11]. The behaviour of contracts has been investigated using the OMNET++ simulator. It has been seen by the occurrence of delay, packet error rate, and residual energy. When compared to other routing protocols, GFTEM has a larger give up to halt procrastination and an excellent electricity-efficient packet loss ratio.

Support is provided by the application. For wireless sensor networks, Can et al. [12–14] developed a neural network-based intrusion detection system. WSN has been utilised for security in high-risk areas such as combat zones. Both physical and transmission security are provided by the WSN. WSN employs a variety of energy management measures, although there are still security flaws. Cyber-attacks are still a threat to some approaches. Security attacks, the use of more energy by running applications, the implementation of fault tolerance against nodes through attacks, the use of minimal power by the devices used, and the requirement to help scalability and mobility features are all examples of WSN limitations.

The embedded method is the next option, in which feature selection is dependent on training in the machine algorithm in concern. The third method is the filter method, which selects features based on general characteristics. Statistical criteria are used to rank features, and the highest-ranking features are chosen [15,16]. Consistency based feature selection (CNF) [16] and Correlation based feature selection

(CFS) [17–23] are the filtering methods employed. This work has presented a solution for WSN and artificial neural networks through intrusion detection. Flexibility, attack tolerance, and ability development are among the aspects covered. The study uses supervised learning as a learning technique, with the logistic function as the activation function. Tab. 1. Shows the limitations of existing works.

Table 1: Limitations of Existing methods

Author, Year	Methodology/Metrics	Limitation	Suggestion
S. Sontowski, 2020	1.Wi-Fi deauthentication attack detection scheme 2.Sniffing characteristics is observed	Have checked only for ARP,DNS Spooking attack	This could be extended for other type of attacks also. [24]
Mohamed Amine Ferrag, 2021	1.Convolutional neural networks, Deep neural networks, Recurrent neural networks 2.Precision,Recall	Real time analysis is not performed.	This could be extended for real time analysis through simulations. [25]
Ehud Doron, 2021	Dynamic Bandwidth Limiter scheme	Goodput is not measured during analysis	The approach could be extended with using schemes for cluster formation. [26]
AQEEL SAHI, 2017	LS-SVM Algorithm evaluated with CS_DDoSAccuracy, CS_DDoSSensitivity, CS_DDoSSpecificity	Throughput, packet loss is not measured.	The work can be extended with real time analysis together with model evaluation. [27,28]

3 Materials and Methods

Nodes in the sensor network are used to collect sensory information, do some processing, and send it to other nodes associated with the network. In Fig. 1, affected nodes can accept data packets from neighboring nodes and forward them elsewhere. This Denial of Service (DoS) attacks can easily affect the awareness of any node illegal in the network. An intruder can instead transfer each bit of the entire packet waiting to create a DDOS. Even if packet communications are confidential, they don't give themselves and do DDOS attacks. Deep Convolutional Neural Network is designed with the state-action relationship mapping which is used to identify the DDOS Attackers present in the network. It takes the node and network behaviourial parameters as input which includes (Packet Generation Rate, Drop ratio, Mismatch packet count, Unique data generation, Request pkts send and forward, Response send and forward) which significantly improves the performance of the detection strategy. In Fig. 2, set of sensor nodes are deployed in the network region to sense and report the environmental statistics. Then, it compares the proposed threshold FMPD and RTD, which is useful for reliable communication in the network. The detection time of a faulty sensor node is dependent on the secondary RTP and RTD numbers. The centralized controller device to collect the report from the sensor devices. The nodes which exhibits the malicious behaviour by performing the identity duplication and the fault data generation process. Therefore, for RTP RTD time measurement and evaluation, it is necessary to minimize the detection time, and the SNCET method must be detected to determine the DDOS attack in the network. The influence of the node, when receiving the data packet from the adjacent node, it can be transferred to another location. This DDOS attack is the most dangerous attack, it can give a quick effect to the consciousness of any illegal node in the network. Intruder, can transfer each bit of the entire packet that are waiting to create a DDOS instead. Even if packet

communications are confidential, they don't give themselves to DDOS attacks. Classification engine: It is designed by using the convolutional neural network which is executed in the sensor devices and in the basestation to perform the node behaviour classification process. The environmental monitoring, data transmission and the attacker node detection and elimination are performed in the WSN environment.

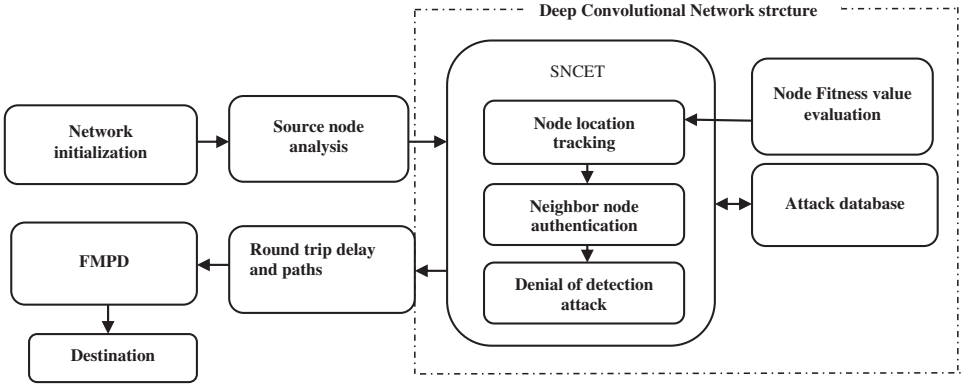

Figure 1: Proposed system block diagram

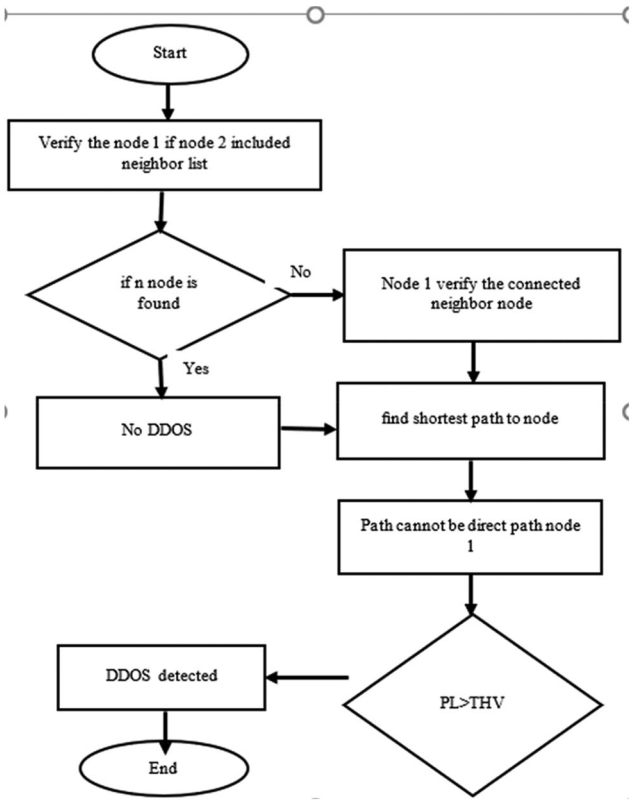

Figure 2: Static neighbor concentration estimation

3.1 Round Trip Delay and Paths

RTP is that the round trip delay of each node will change in different environments. In addition, due to the failure to change the sensor node. This delay is that it exceeds the threshold, or it may be infinite. The faulty node is determined by comparing the threshold and RTD. The detection time of a faulty sensor node is dependent on the secondary RTP and RTD numbers. Therefore, RTD time measurement and evaluation must be minimized in the detection time.

Round-Trip Path Selection Analysis

False nodes can be detected by comparing RTP with a threshold. The number of RTP designed by the sensor nodes of "t" is assumed by

$$t = G(G - t) \quad - - - - - \tag{1}$$

where t is the numbers of RTPs,

G is the network analysis time. The total number of nodes in the fault detection method is the time required to measure all RTDs in the wireless sensor network. This is all times except RTD. The equation for the t of RTP in analysis time is

$$Time\ (t)\ =\ RTD - 1 + RTD - 2 + \ \cdot\ \cdot\ \cdot + RTD - P\ (4)\ \ (t)\ =\ \sum\ RTDi\ \ - - - - \tag{2}$$

This FMPD is suitable for the minimum number of the best of the nodes in the path of before and after. When the network is initialized, all nodes must verify whether it is operating normally, and the delay time is used as the threshold time. The threshold time is based on the number of RTP nodes. The total analysis time will depend on the number of nodes in the network.

Step 1: Start

Step 2: Set time Rt1

Step 3: Rt2_i sensor node time

Step 4: The round trip time formulation to be calculate

Rt3_i = Rt2_i – Rt1.

Step 5: RTT threshold value formulation calculate

Rts_i = hop_ count Rt i _3

Step 5: If Rts_i < Rtth and hop count[i] = 2 = = true then

Based on the RTT of Rt3_i, calculate the average round trip time of the help path for all values of Rts_i. After comparing with the threshold of Rts_i, otherwise the threat does not generate a DDOS link, the total

RTT is less than the threshold RTT and if the road is not connected to a particular route with more than one DDOS, then the route is check if it is affected by the DDOS. Alternatively, several passes are sufficient for the consideration of the maximum number of RTP which, as many paths as the sensor node in wireless sensor networks exist, and reduces the RTP to error detection analysis. The selected RTP is equal to the analysis time in shortening the number of wireless sensor network nodes. The linear relationship between the analysis time of T and P induced by the RTP thus selected is called RTP linear and does not optimize the error detection time. The larger the sensor value and the RTP node g select large sensor network. Therefore, there is a need to further reduce the number of RTPs that make the FMPD method more efficient.

3.2 Static Neighbor Concentration Estimation Technique

All sensor nodes are assumed to be static. It is also assumed that for some initial interval malicious nodes are not present and every node safely establishes neighbor information. These two kinds of malicious nodes

create high-speed tunnels. One malicious node is located in one area and the second malicious node is located in another area. After the tunnel is created, the malicious node can discard the data packet and replace the data packet. Malicious nodes can analyze TRAF. In some initial intervals, malicious nodes do not participate in the network. Each node sends a message to all neighbors. When any node receives a message, it immediately sends a reply message. Therefore, each node creates its own neighbor list. Each node sends its list of one-hop vicinity of its neighbors. In this way, each node to create a two-hop neighbor list (neighbor list). At some point of time, suppose node 1 overhear packets from the new node, say node 2. Every node maintains two lists: true neighbor list and suspected neighbor list.

Node 1 first verifies that one of its neighbors is included in the neighbor list of node 1. To do this, node 1 finds the intersection of neighbors of its own with the neighbors of node 2. If any common neighbor is found, then attack is not present. If not found, then node A verifies that one of its one hop neighbors is directly connected to one of the one hop neighbors of node 2. To do this, node a finds the intersection of its one hop neighbor list with the one hop neighbor list of node 2. If any common neighbor is found, then no attack is present in the network. If not found, then node 1 asks all its one hop trusted neighbors to find shortest path to node 2. This path cannot be direct path and does not pass through node 1 and report the number of hop count. If for any path, no of hop count is less than or equal to the threshold value then attack is not present in the network.

3.3 DDOS Defence Using the Deep Convolutional Neural Network

Sensor network is constructed with number of sensor devices with one centralized base station. Wireless Sensor devices are deployed randomly in the network region and it is hierarchically connected with the BaseStation. Each devices perform the beacon message exchanging process to identify the neighbour nodes present in the network communication range. Base station send broadcast message as network-wide broadcast message in periodical manner, to all sensor nodes in the network. Sensor devices perform environmental sensing process to gather the information about the surrounding environment.

Sensor devices report the sensed data to the Base Station by constructing the route by using the Route Discovery process in the lower level of the communication. In the communication between sensor device to its basestation, Source node initiates the data transmission, and check for the routing table entry to forward the data packet.Since there is no multihop entry is present initially, source node performs the route discovery process by sending the route request message to destination as a network wide broadcast message.This message is broadcasted over the wireless medium and it is received by the neighbour nodes.Neighbour nodes validates the route request message for routing loop and freshness of the control message.Receiver nodes creates the reverse route entry to reach the source node with the corresponding seqno of the request message.

After the successful completion of route request validation, receiver nodes matches the destination node id with the current node id.If the match is not found, route request message is rebroadcasted over the medium until packet reaches the intended destination.Once the packet reaches the destination node, it constructs the route reply message with the exact reverse path of the request message.Reply message is originated by the destination node and unicasted to the corresponding forwarder nodes to reach the source node of the request message.While forwarding the reply message, intermediate and source node creates/updates the routing table entry to reach the destination node.If the link failure is occurred during the data transmission due to the channel unavailability, alternate route discovery process is executed to reconstruct the route to connect with the BaseStation. Sensor network is constructed with the set of packet intruder, packet dropper and dos attacker to generate fake data packets.

Deep Convolutional Neural Network Algorthim

Sensor network is constructed with the set of packet intruder, packet dropper and dos attacker to generate fake data packets.During the route discovery process, if the route request message is received by the attacker nodes then it creates falsified route reply to source node to capture the data packet.

The Malicious devices capture the data and discard it as well as flood the falsified data to reduce the QoS in the communication. The detection system in the devices are performs the data collection process that identifies the packet forwarding count and packet sent count and drop counts of the data forwarder.

In order to identify the behavioural variation of the devices, the normal behavioural pattern should be identified to perform the learning process in the deep convolutional neural network. Each node maintains the Traffic timer to collect and validate the ongoing traffic information in both sending and receving traffic rate.

During the monitoring process, the following informations are validated to determine the malicious nodes present in the sensor network.

1. Packet Generation Rate
2. Drop ratio
3. Mismatch packet count
4. Unique data generation
5. Request pkts send and forward
6. Response send and forward

These input values are obtained from the network and packet behaviour of all neighbour nodes, Monitoring nodes performs the neural network learning process.

For the estimation of successful ratio and tranmission delay, packet retransmission due to the link failure and its impact on the data packets are excluded.

The collected features of the data is classified by using the Deep Convolutional Neural Network.

Based on the monitoring periods, the input neuron of the DCNN is modeled with the multiple dimension based on the number of time period.

The input data is converted into the normalized data value using the minimum and maximum boundary values of the each input parameters.

The normalized minimum bound is assigned as negative unit value and maximum bound is assigned as positive unit value.

The input neuron is formed with the length of size of the column vector of the normalized data.

For each input, the unit state probability is computed to normalize the values into probability vector.

State-action relationship is formed with the behviourial mapping for each neuron based on the probability vector.

The relationship is formed using the statistical estimator including the mean, variance, standard deviation, and the expected boundary interms of lower and upper bound values for each parameters in each time units.

The convolutional layer formation is performed as iterative process which is initiated with the fixed iteration count.

It is generated using the Deep Generative Model which establishes the collaboration between the layers along with the sigmoid function and convolution kernel.

The average pooling is used by combining the current neuron value with the bias values.

Fully connected layer is formed by applying the lograthmic ratio of individual exponential value with cumulative exponential value of the term frequency with the inverse document frequency.

The logistic function using the sigmoid function is used to activate the output layer of the deep convolutional neural network.

The last layer functional value is computed by forming the unit diagonal matrix with the scalar product of the data input of the unbiased layer.

The biased output and the input matrix value is combined together to form the output value in the output layer.

The Sensitivity value is estimated as the negative product of the functional value computed using the diagonal matrix and the Net Input combined with the second product difference of the target value and the actual value.

It is validated based on the conditional probability of the individual behaviourial mapping with respect to the time series.

The condition probability is used to derived the individual activation probability and the activation is also requires the softmax function to discretized the values into final activation value.

From the formed neural network, the null and alternate hypothesis is formed and by validating the hypothetical situations of node behavior in the network.

These two hypothesis are representing the normal behavior and misbehavior of the nodes by formulating the various set of characterization possibility based on the current data transmission behaviour of the nodes.

4 Result and Discussion

In this part, it represents the use of NS2 network simulator DDOS attack simulation results. The tool checks that the first 100 nodes in the simulation field are more than 1,000 meters away and finds intruder nodes. Various parameters are checked each node. The node Deep Convolutional Neural Network algorithm for identifying the intruder in the entire geographic area. Tab. 2 shows the simulated factors DDOS attack.

Table 2: The runtime environment is setup with the following parameters

SIMULATION ENVIRONMENT PARAMETERS	
Number of nodes	50, 100, 150, 200, 250
MAC Type	MAC 802.11 DCF
Antenna Type	Omni Directional Antenna
Transmission Range	80 m
Type of Connection	UDP
Deployment Area	500 × 500 m^2
Traffic Type	CBR with Environmental Sensing
Traffic Interval	0.1, 0.15, 0.2, 0.25, 0.3 s
Application	Temperature, Humidity and Soil Moisture
Packet Size	512 Bytes
Connection Bandwidth	2 MB
Simulation Time	100, 125, 150, 175, 200 s

Tab. 2 represents the simulation parameters of the proposed WSN system. The parameters used during this analysis for computing the trust system have provided within Tab. 2. The performance of the DNN model has calculated by the subsequent metrics like packet loss, packet delivery magnitude relation, energy consumption, end-to-end delay, and mean packet latency. Fig. 3. represents the sensor node selction of the proposed Tracking-Learning-Detection Q Network (TLDQN) algrothim based on the sensor node the data collection about the traffic conditions and identifies the deviation between the network conditions are analysed. This section describes the node data transmission of singal of the WNS system using the proposed Tracking-Learning-Detection Q Network (TLDQN) algorthim which is shown in above Fig. 4.

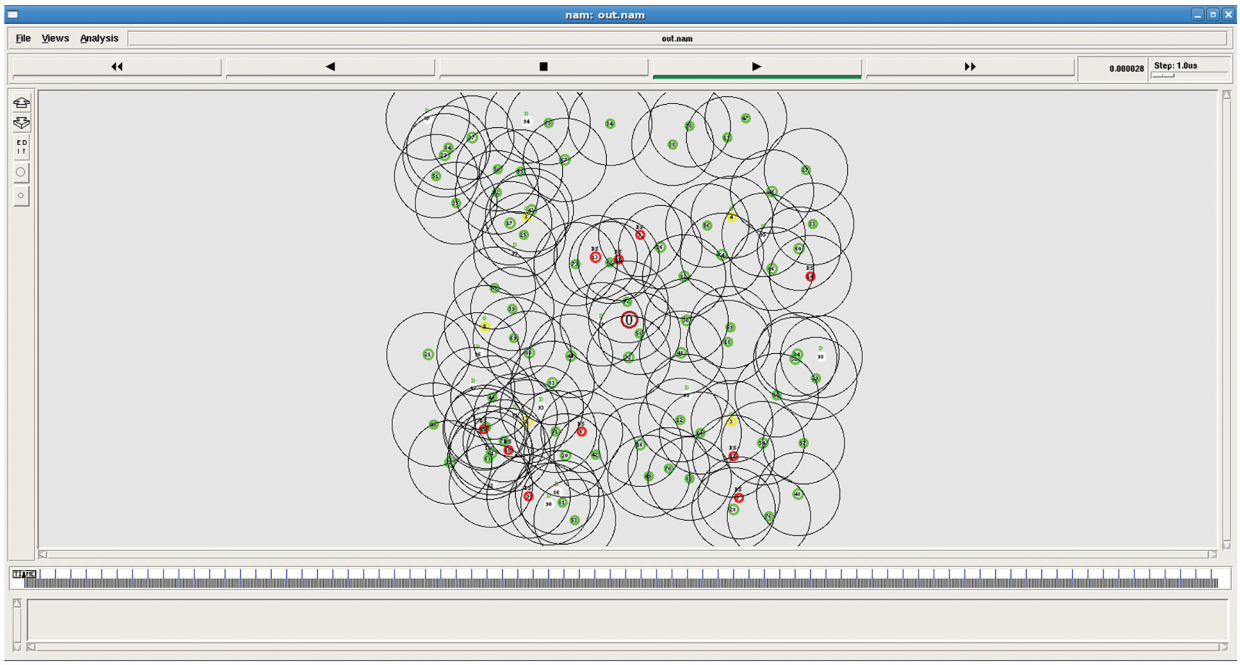

Figure 3: Sensor node

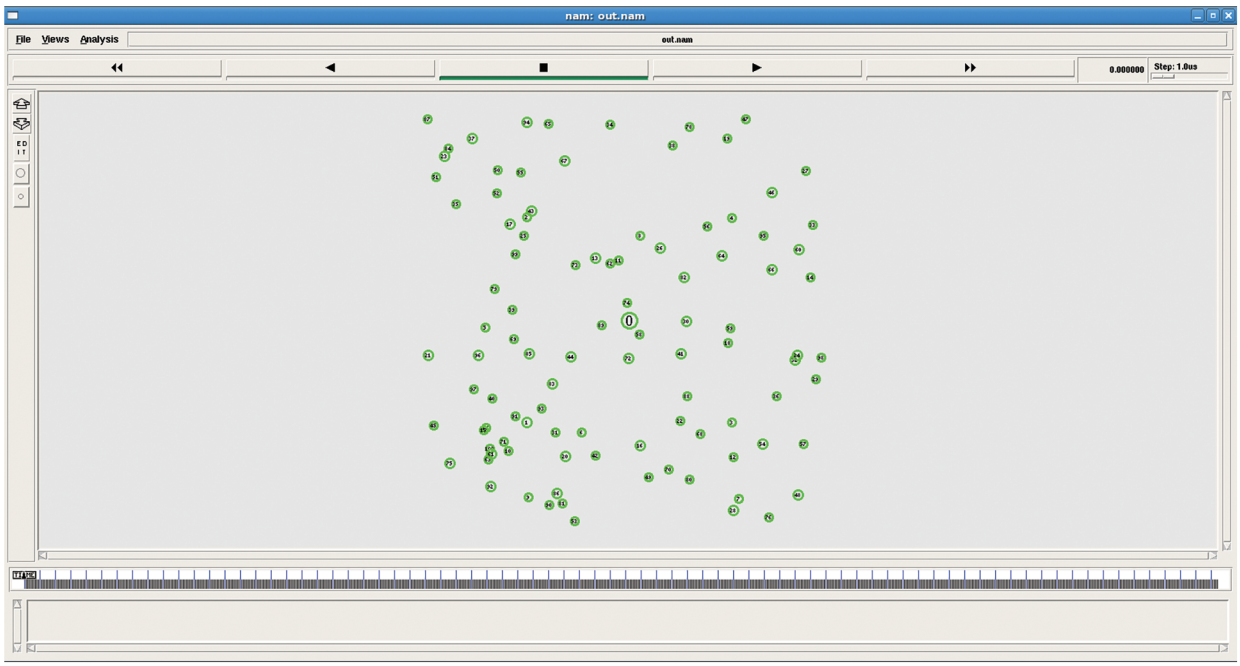

Figure 4: Initiating_communication

Fig. 5 represents the IOT communication data values from the different node attridbute,utilising this data sensor values are identified. Fig. 6 Attacker detection in the WSN system, the above figure represents there is two DDOS attack detection is identified in the WSN network. Fig. 7 presents the throughput analysis of the proposed Tracking-Learning-Detection Q Network (TLDQN) based WSN system. In this system both time and interval based throughput is analysed.

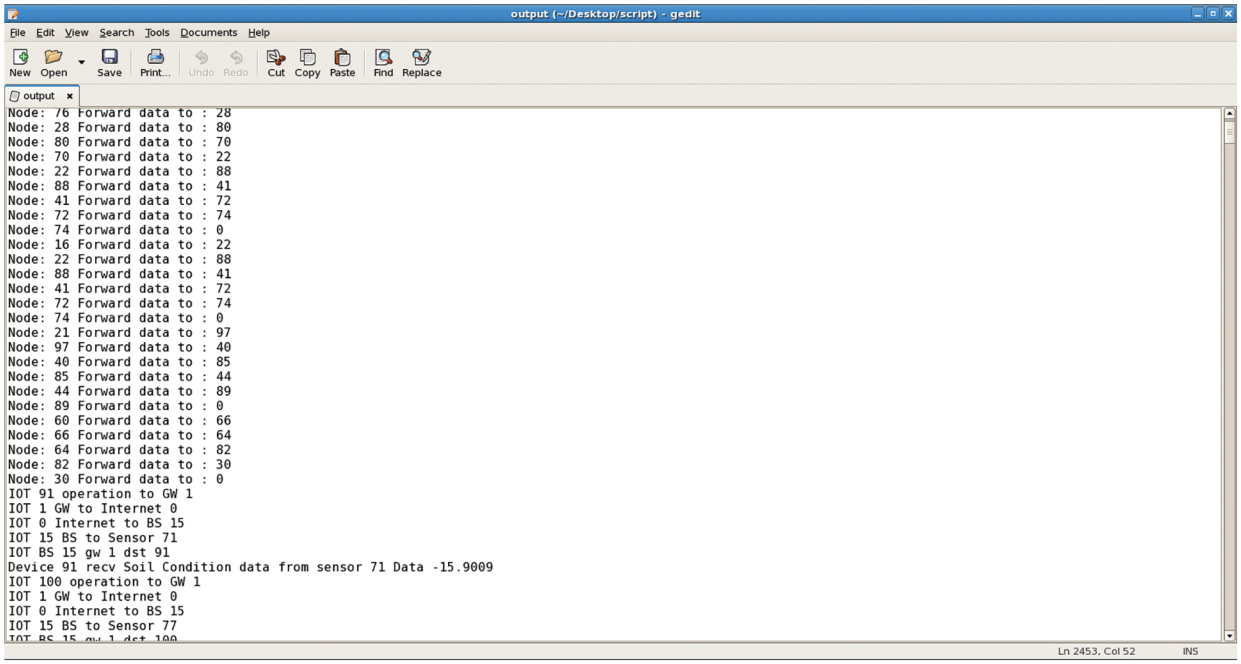

Figure 5: IOT communication

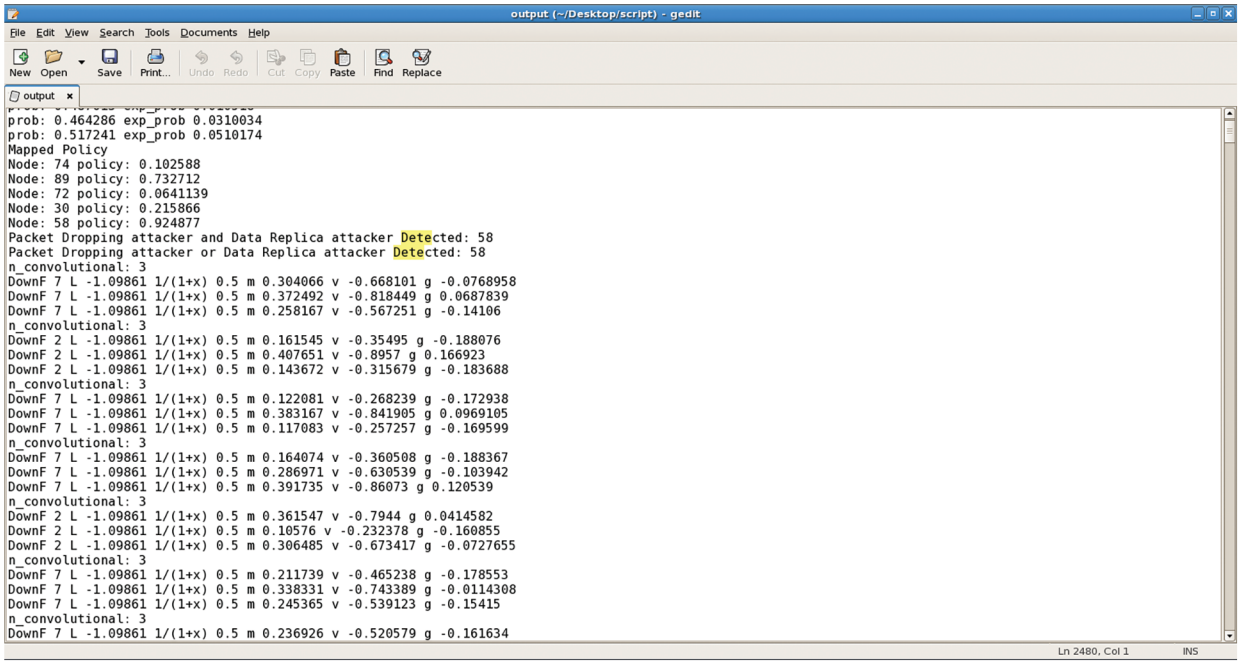

Figure 6: Attacker detection with TLDQN

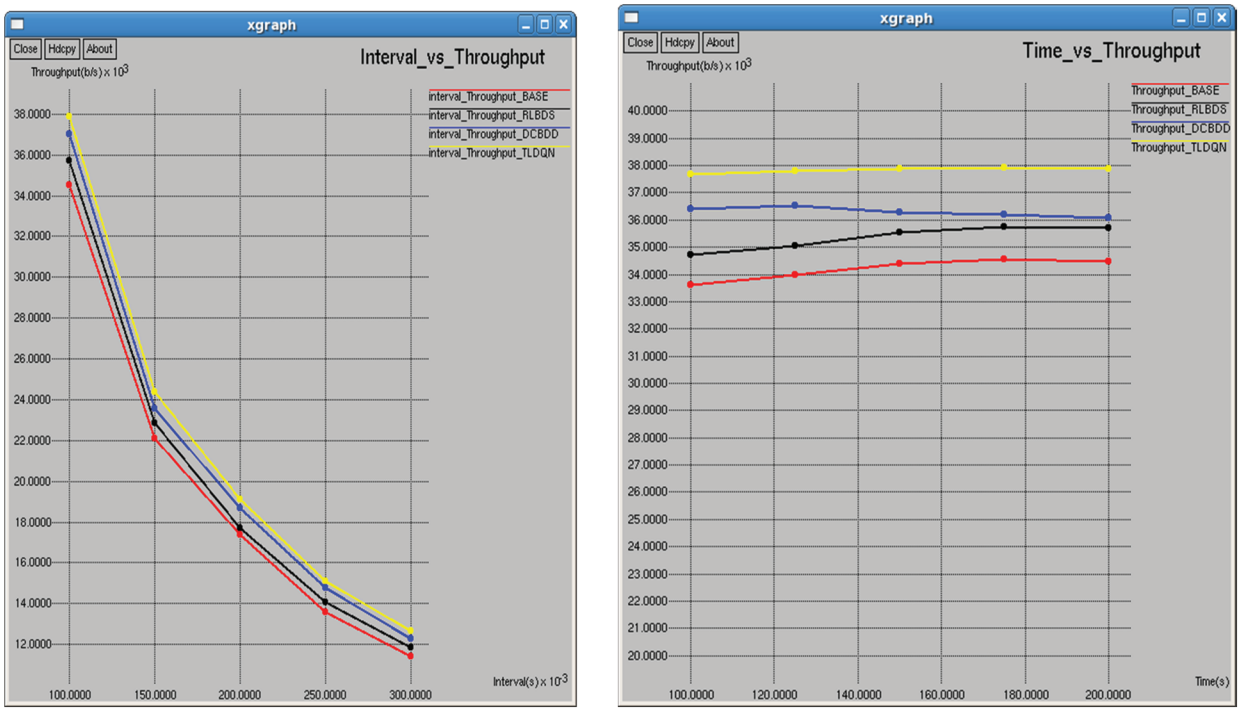

Figure 7: Throughput analysis

Throughput refers to the rate of success message is transmitted to the entire network, which is calculated by the rate of successfully reached the destination node of the packet. It is made per second (bps) data bits or measured. Fig. 8 shows the different overall throughput ratios of the method and it is obvious that the proposed TLDQN has achieved higher throughput than other methods.

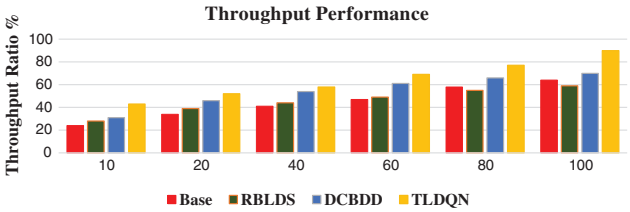

Figure 8: Analysis of throughput performance

Fig. 9. presents the transmission analysis of the proposed Tracking-Learning-Detection Q Network (TLDQN) based WSN system. In this system both time and interval based packet delivery ratio is analysed.

Transmission amount of the packet delivery ratio is defined by the source node and the received packet is the packet destination node. Fig. 10. describes the transmission ratio in the percentage between the proposed and existing systems, that the comparison of prevention methods in terms of Transmission Ratio. Base 75% Reference Broadcast Synchronization (RBLDS) in 85%, Distributed Cluster-Based (DCBDD) 90% and proposed Tracking-Learning-Detection Q Network (TLDQN) in 95%.

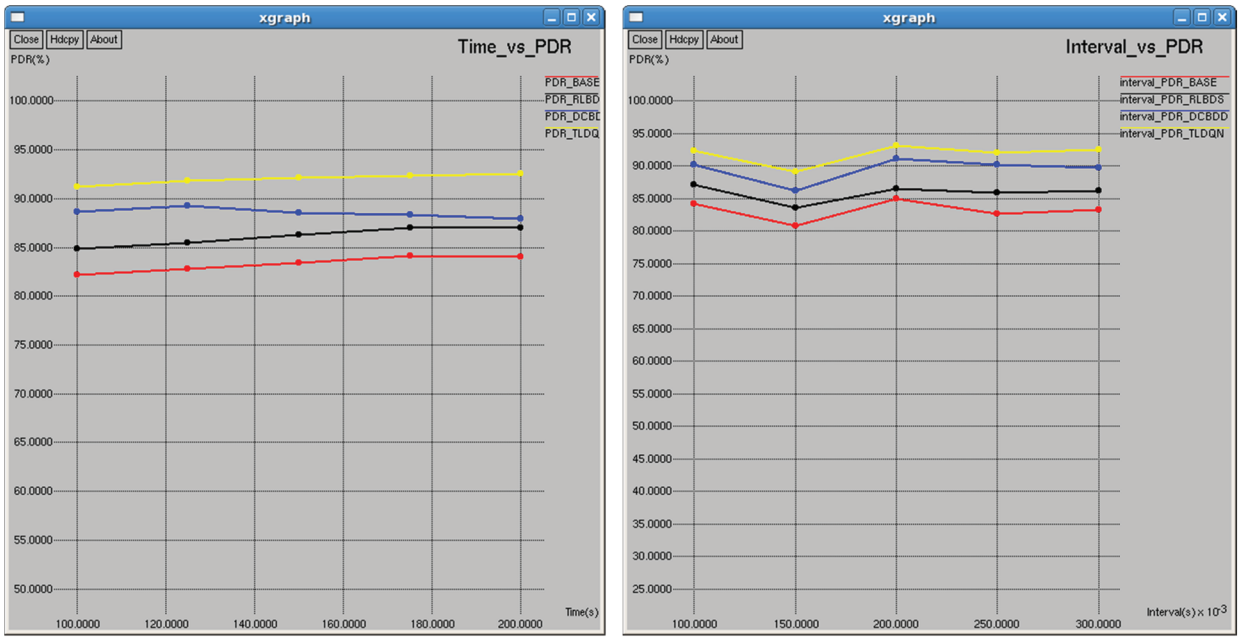

Figure 9: Thoughput analysis

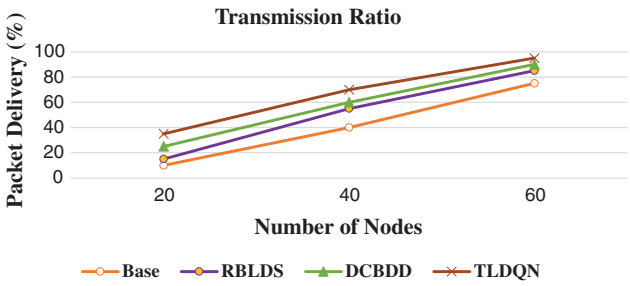

Figure 10: Transmission Ratio

Fig. 11 presents the DDOS attack detection analysis of the proposed Tracking-Learning-Detection Q Network (TLDQN) based WSN system. In this system both time and interval based DDOS attack detection analysis is analysed. Fig. 12 shows the comparison of DDOS detection accuracy. The results show that the proposed method has produced more accurate detection than other methods.

Comparison of the proposal shown in Fig. 13. with existing methods. The existing methods Base in 67%, RBLDS in 71%, DCBDD in 86%, and the proposed method TLDQN with 95%.

Figure 11: DDOS attack detection analysis

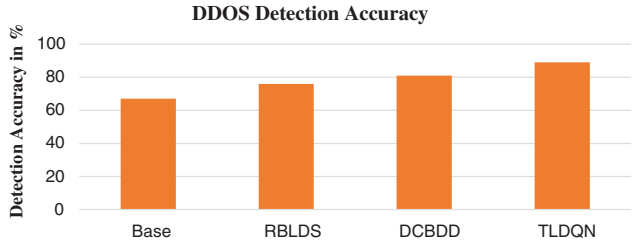

Figure 12: DDOS Detection Accuracy

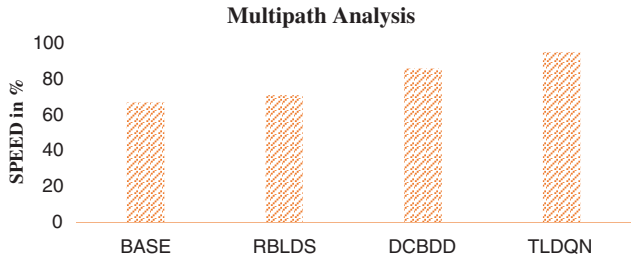

Figure 13: Multipath Analysis

5 Conclusion

WSN has various problems and those most unpredictable in nature DDOS attack. Detection of malicious nodes play an important role in this system. Detect malicious behavior based on the nodes of the node. Deep convolution Q network is based on a DDOS detection method that reduces the proposed overhead in the traditional way. Node maintains the history of their neighbors and their own position, sending or receiving a number of packets. According to details neighbor, the neighbor node density estimation suspect is malicious. This method checks the details of all neighbors and determines that the intruder's node is at on the network. DDOS attacks that identify and detect mainly in TLDQN networks of the proposed method. It is a difficult task to provide secure communications. Therefore, the determined mechanism, can be used to prevent and detect the DDOS attack, and RTT is estimated in order to complete all the mechanisms. TLDQN in analysis of throughput performance in 90 made per second

(bps) data bits, transmission ratio is 95%, DDOS detection accuracy 89%, and multipath analysis is 95%. The accuracy is around 88% considering the number of nodes to be 100,The accuracy is around 84% considering the number of nodes to be 120,The accuracy is around 82% considering the number of nodes to be 150.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. A. Ahmed, V. L. Popov and A. V. Topalov, "Environmental monitoring using a robotized wireless sensor network," *Journal of AI & Society*, vol. 33, no. 2, pp. 207–214, 2018.

[2] M. Dixit, K. Kulkarni, Pradeepkumar, S. Somasagar, C. Veerendra *et al.,* "Variable scaling factor based invisible image watermarking using hybrid DWT–SVD compression - decompression technique," in *Proc. of IEEE Students Conf. on Electrical, Electronics and Computer Science*, pp. 1–4, 2012.

[3] I. T. Almalkawi, M. G. Zapata, J. N. Al-Karaki and Morillo-Pozo, "Current trends and future directions sensors (Basel)," *Journal Wireless Multimedia Sensor Networks*, vol. 10, pp. 6662–6717, 2010.

[4] N. Vecoven, D. Ernst, A. Wehenkel and G. Drion, "Introducing neuromodulation in deep neural networks to learn adaptive behaviours," *PLOS ONE*, vol. 15, no. 1, pp. 538 – 538 557, 2020.

[5] H. H. Soliman, "A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks," *Egyptian Informatics Journal*, vol. 13, no. 3, pp. 225–238, 2012.

[6] D. Tannoury, D. Anthony, G. Rony, M. Christophe and M. Abdallah, "Efficient and accurate monitoring of the depth information," *Journal of Wireless Multimedia Sensor Network Based Surveillance*, vol. 1, pp. 1–4, 2017.

[7] S. Mateen, A. Ahmed, A. Maida, A. Azeem Akbar and A. Muhammad, "Comparative analysis of wireless sensor networks," *Journal Of Wireless Multimedia Sensor Networks*, pp. 80–83, 2017.

[8] W. Ali Hussein, M. Borhanuddin and H. Fazirulhisyam, "Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks," in *IEEE 13th Malaysia Int. Conf. on Communications (MICC)*, pp. 28–30, 2017.

[9] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop on Mobile Computing System and Applications (WMCSA '99) (New Orleans, LA.)*, vol. 25, pp. 90–100, 1999.

[10] B. Sukant Kishoro and S. Sarita, "Performance analysis of dynamic MANET on-demand (DYMO) routing protocol," *Special Issue of International Journal of Computer and Communication Technology*, vol. 1, no. 2, pp. 3–10, 2010.

[11] N. Abbas and F. Yu, "A traffic congestion control algorithm for wireless multimedia sensor networks," in *2018 IEEE Sensors*. New Delhi, pp. 1–4, 2018.

[12] C. Okan and S. Ozgur Koray, "A survey of intrusion detection systems in wireless sensor networks," in *6th Int. Conf. on Modeling, Simulation, and Applied Optimization (ICMSAO)*, vol. 1, pp. 1–6, 2015.

[13] A. Fragkiadakis, I. Askoxylakis and P. Chatziadam, "Denial-of-service attacks in wireless networks using off-the-shelf hardware," in *Distributed, Ambient, and Pervasive Interactions. DAPI 2014. Lecture Notes in Computer Science*, vol. 8530, 2014.

[14] M. Gniewkowski, "An overview of DoS and DDoS attack detection techniques," in *Theory and Applications of Dependable Computer Systems, Dep Co S-RELCOMEX 2020, Advances in Intelligent Systems and Computing*, In: W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk (Eds.), vol. 1173, 2020.

[15] W. Jacak, K. Pröll and S. Winkler, "Neural networks based feature selection in biological data analysis," in *Advanced Methods and Applications in Computational Intelligence. Topics in Intelligent Engineering and Informatics*, vol. 6, 2014.

[16] D. Mital and C. Sethu kumar, "Correlation based feature selection (CFS) technique to predict student performance," *International journal of Computer Networks & Communications*, vol. 6, no. 3, pp. 197–206, 2014.

[17] M. Hall and L. A. Smith, "Feature selection for machine learning: Comparing a correlation-based filter approach to the wrapper CFS: correlation-based feature," *Fifth Int. FLAIRS Conf.*, pp. 5–24, 1999.

[18] I. R. Widiasari, L. E. Nugroho and E. Widyawan, "Deep learning multilayer perceptron (MLP) for flood prediction model using wireless sensor network based hydrology time series data mining," in *2017 Int. Conf. on Innovative and Creative Information Technology (ICITech)*, Salatiga, pp. 1–5, 2017.

[19] S. Ramesh, C. Yaashuwanth and B. A. Muthukrishnan, "Enhanced approach using trust based decision making for secured wireless streaming video sensor networks," *Multimedia Tools and Applications*, vol. 79, no. 15-16, pp. 589–602, 2020.

[20] S. Ramesh, C. Yaashuwanth and B. A. Muthukrishnan, "Machine learning approach for secure communication in wireless video sensor networks against denial-of-service," *Multimedia Tools and Applications*, vol. 79, pp. 1520–1532, 2020.

[21] S. Ramesh, C. Yaashuwanth and B. A. Muthukrishnan, "QoS and QoE enhanced resource allocation for wireless video sensor networks using hybrid optimization algorithm," *International Journal of Parallel Programming*, vol. 48, no. 2, pp. 1807–1822, 2020.

[22] A. Emir Cil, Y. Kazim and B. Ali, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems with Applications*, vol. 169, no. 4, pp. 1–6, 2021.

[23] W. Sun, G. Z. Dai, X. R. Zhang, X. Z. He and X. Chen, "TBE-Net: A three-branch embed ding network with part-aware ability and feature complementary learning for vehicle re-identification," *IEEE Transactions on Intelligent Transportation Systems*, vol. 1, pp. 1–13, 2021.

[24] T. Senthil Kumar and K. L. Prakash, "A queueing model for e-Learning system," *Advances in Intelligent Systems and Computing*, vol. 325, pp. 89–94, 2015.

[25] S. Sontowski, M. Gupta, S. Chukkapalli, M. Abdelsalam, S. Mittal, *et al.,* "Cyber attacks on smart farming infrastructure," in *2020 IEEE 6th Int. Conf. on Collaboration andInternet Computing (CIC)*, vol. 1, pp. 135–143, 2020.

[26] F. Mohamed Amine, D. Lei Shu, D. Hamouda, C. Kim-Kwang, "Deep learning-based intrusion detection for distributed denial of service attack," Journal of Agriculture, vol. 11, pp. 221–235, 2021.

[27] E. Doron and A. Wool, "WDA: A web farm distributed denial of service attack attenuator," *Computer Networks*, no. 5, pp. 1037–1051, 2021.

[28] A. Sahi, D. Lai, Y. Li and D. Mohammed, "An Efficient DDoS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 3, pp. 56–74, 2017.