International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Ddos Attack Detection and Prevention using Aodv Routing Mechanism and FFBP Neural Network in a Manet

Jasmine Batra, C. Rama Krishna

Abstract*: Security is considered as the most important feature in a Mobile Ad-hoc Network (MANET). There are different types of attacks which may affect the data transmission in MANET but Distributed Denial of Service (DDoS) attack is one of the complex and harsh worthy in a MANET. In the existing work, it has been found that the researchers have utilized Support Vector Machine (SVM) and fuzzy logic as a classification algorithm to identify the DoS attack in MANET. The problem with SVM and Fuzzy logic is that they are more complex and more time consuming mechanism to detect attackers. Also, in the existing work, Optimized Link State Routing (OLSR) routing protocol is used to find route and it is a searching mechanism which does not include the concept of trust routing table and hence the searching mechanism consumes more energy. To solve the mentioned problems, we are presenting a machine learning approach that is Feed Forward Back Propagation Neural Network (FFBPNN) as a classifier and Ad hoc On-Demand Distance Vector(AODV) routing protocol for route discovery to shield the network from Distributed Denial of Service (DDoS) attack. The MANET is trained using FFBPNN. Therefore, when malicious node appears in the network, the node is identified on the basis of the node properties like energy consumption and delay. The route is changed by discarding the malicious nodes from the route and hence the network is protected. The throughputs, PDR have been increased by 60.71%, 53.57% and delay has been reduced by 42.21%.

***Index Terms*: MANET, AODV, FFBPNN, DDoS, PDR, Throughput, Delay, Energy Consumption.**

I. INTRODUCTION

MANET is a compilation of autonomous users who are communicating in relatively limited bandwidth. These networks are considered as new networks that have all moving nodes that can correspond with one and other with no BS (Base Station). In this kind of network, moving nodes will provide the user and application traffic that helps to carry out the control as well as the routing protocols [1].

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
Jasmine Batra*, M.E, Department of Computer Science, NITTTR, Chandigarh
Dr. C Rama Krishna, Ph.D. from IIT Kharagpur, M.Tech. from CUSAT, Cochin B.Tech. from JNTU Govt. College of Engg., Anantapur

Fig. 1 demonstrates the network formed by different mobile devices like mobile phones and laptop. Every device has its own coverage area denoted by a dotted line. The coverage area defines the range of transmitting a packet from one device to another device. As depicted in Fig., source node broadcast data to mobile that comes in its coverage range. Then mobile broadcast data to the other mobile device that comes in its communication range.
In this way, the data is transmitted from one device to another device until the data reaches the actual destination device [2].

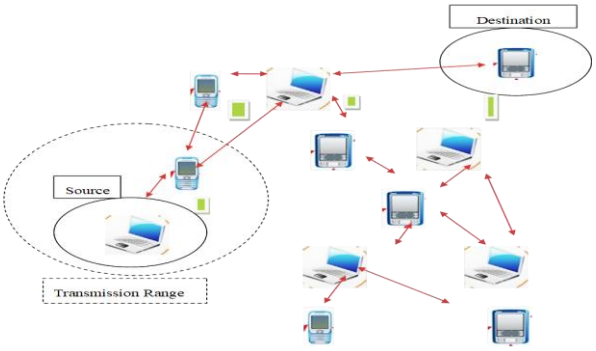


Fig. 1 Mobile Ad-Hoc Network [3]

The routing in MANET plays a significant role and forms route by considering that the nodes are working in a co-operative way, with the assumption that the nodes are secured from attackers. Because of this property of the routing algorithm, any malicious impostor may penetrate the network and act as a routing agent, and ultimately produces interference in the network [4]. These kinds of nodes are very difficult to recognize, as the identification of attacker inside the network is more challenging to identify instead of recognizing the attacker outside the network area.
In this research work, a to protect the network from a DDoS attack secure MANET is designed. According to this, an attack strives for the prevention of genuine and approved users from the services provided by the network. The DDoS attack can affect the network in several ways. The typical approach is to transfer the packets to some centralized resource that exists on the network for no longer availability to all network nodes and as the outcome, the network will not execute in the way it is destined to work [5]. It gives result as a service failure to the end users. Server or network host cannot find return address of the attacker while sending validation of approval, due to this the server has to before disconnecting the link.

More authentic packets are sent by the sender with invalid return address, at the time when connection is disconnected by server [6].Therefore, it is necessary to prevent the network from DDoS attack. In this research, to detect and prevent the network from DDoS attacks, AODV as a routing protocol and FFBPNN is used as a classifier [7].

II. RELATED WORK

The authors have worked to design a secure network, by detecting and removing various attacks like DoS attack, gray hole attack, black hole attack from the network using different techniques. The techniques like optimization and classification along with route discovery mechanism have been discussed.

Shams et al. [8] presented an IDS (Intrusion Detection System) to identify MANET's DoS attack. To detect and remove DoS attack, SVM has been utilized as a classification algorithm. From the experiment, it has been analyzed that the proposed IDS sense and remove the DoS attack with high detection rate and less computing time. Also, it has been observed that the detection rate has not been affected by the node movement and network's size. Alsumayt et al. [9] presented a new technique named "monitoring detection and rehabilitation" to prevent the network from DoS attack. This technique is based on measuring the number of actual values that the sensor node can be trustworthy or not. The technique which has been proposed is compared with the existing "trust enhanced anonymous-on-demand routing protocol" and it is concluded that the scheme has performed better by means of PDR i.e. it has been increased by 20.87.Chhabra et al. [10] introduced a technique to prevent network from DoS attack using AODV mechanism. This approach is mainly used for the minimization of routing overhead, but, if there is more than one malicious node in network, the system becomes slow.

Zakariaa et al. [11] proposed a firefly as an optimization scheme to discover the smallest route among source and destination node along with a queuing model. The queuing analysis network has been utilized to determine the minimum response time among the source nodes with the destination node. Therefore to obtain the best path among nodes of origin and destination node, the authors have integrated the firefly optimization algorithm and analyzed the queuing. Anbarasan et al. [12] presented a LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol to provide security in the MANET in case of extra resource addition in the network. LEACH protocol group the nodes that consist of CH (Cluster Head) and CM (Cluster Manager) that used to transfer data between the nodes. The energy has been saved by utilizing the LEACH protocol and hence increases the battery life. Also, the concept of encryption has been added to provide the additional security in MANET from DoS attack. Doss et al. [13] have used the SVM technique to detect and remove jelly fish attack in MANET. This attack is one of the most sophisticated attacks found in MANET that degrades the entire network performance. SVM has been used to train the system based on the packet forwarding behavior. Therefore, the proposed technique has been utilized to find the trust and secure route for transferring data packet. The proposed algorithm's result has been compared with a different existing algorithm such as ABC (Artificial Bee Colony) by means of different metrics like throughput, PDR, delay and it has also been analyzed that the proposed jelly fish attack detection approach perform better as compared to the ABC algorithm. The delay upto 8% has been increased using the jelly fish attack detection approach.

From the existing work, on the basis of security risks feasibility is divided into two parts. The first one is that the relative position of attacker does not vary, thus it is easy to locate the intruder. In the next, when intruder and its intruded nodes are scattered and moving, the network head find itself very fussy for identification of intruder in this particular situation. In the existing work, routing protocol that are used utilizes more energy for transmission of data and are based on the searching scheme. Therefore, improvement in routing mechanism is required. Also, the classification algorithms that are used are time consuming and complex. The DDoS attacker is a smart attacker because it does not let the network know that is under menace. The intruder keeps on dropping packets continuously and the network keeps on trying to identify about the situation of network. At this time a variation in the machine learning algorithm seems to be advantageous. The machine learning algorithm trains itself by using the data of the network and tries to co-relate the data which are currently available with the best suitable structure of the network to detect malicious behavior. The evaluation of the network will be based on QoS parameters [14].

III. PROPOSED APPROACH USING AODV ROUTING MECHANISM AND FFBP NEURAL NETWORK (AODV_FFBPNN MODEL)

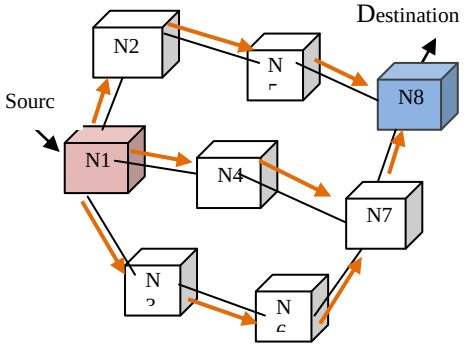
In the proposed work, the detection of DDoS attack is carried out using an artificial intelligence technique. Initially, AODV routing protocol has been used to create a secure route from the source to destination along with table driven property. Then, FFBPNN is used as a classifier to detect the DDoS attacker nodes using nodes basic properties. Prevention of network from attacker nodes has been done by discarding the detected attacker nodes from the route using AODV routing protocol. Feed Forward Back Propagation Neural Network speeds up the data transmission rate more than that of the fictitious node based approach. The description of used techniques is described below:

A. AODV

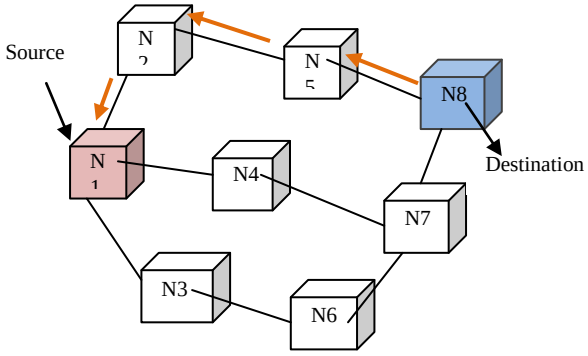
AODV is an on-demand routing protocol or a reactive protocol [12]. It uses the destination sequence number to provide a new loop-free path to the destination. Unlike table-driven protocols, it does not maintain the state of the network through continuous updates. This method helps reduce the size of routing table and number of messages. AODV provides multicast and uni-cast connections in an ad-hoc network. One of the main functions of AODV is to respond quickly when it finds that the link in active path is down [15].There are three control messages types for the maintenance of the route as defined beneath:

- RREQ (ROUTE REQUEST)
- RREP (ROUTE REPLY)
- RRER (ROUTE ERROR MESSAGE)

While passing RREQ, the intermediate nodes register the route tables at neighbor address from where the initial broadcasting packet was taken with the development of the reverse path. When the extra RREQ copies are obtained, then the process of discarding of packets starts. When RREQ arrives at the destination node with an adequate route, the intermediate or destination node sends back the RREP as depicted in Fig. 2(a) [16].



(a) Propagation of RREQ



(b) Path of the RREP to source

Fig. 2 AODV Route Discovery Process [17]

When RREP is routed reverse having back path, the nodes within the path initiated the forward path entry into the routing table pointing towards the node when RREP arrives. These entries represent the active forward route. The route entry also deletes those routes that do not exist for the defined route lifespan. As RREP is passed on the path obtained by AODV, RREQ sustains the symmetric link usage as depicted in Fig. 2(b) [17].

B. FFBPNN

It is an algebraic model or the computational model whose functioning depends on biological neural networks.

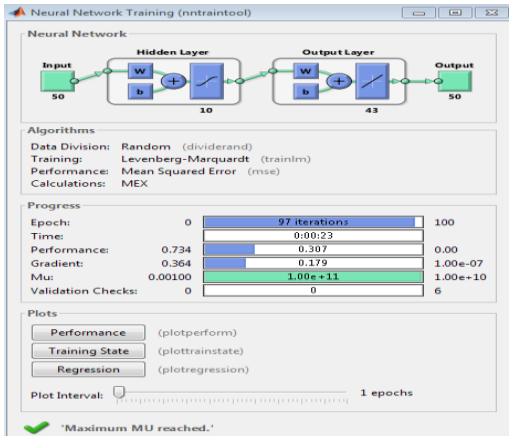


Fig. 3 FFBPNN Structure

In this research, the properties of the node such as collision rate, the position of (x,y) coordinates of nodes, energy consumed by the nodes are provided as input to input layer ofthe ANN structure. Initially, the ANN is trained as per these properties and after training, the network is ready for detection of DDoS attack [18]. The training structure of the FFBPNN depicts in Fig. 3.

Table 1 Parameters for Training of Network using Back Propagation Model

Parameter	Value
Input layer (neurons)	50
Hidden layer (neurons)	10
Number of hidden layers	1
Output layer (neurons)	43
Epoch	97
Performance	0.734
Gradient	0.364
Mutation	0.00100
Validation Check	0

The fundamental network structure of ANN is a fully-fledged feed-based network based on the backpropagation model, which is a static mapping to exit the spreading pattern of the error propagation. In this research, FFBPNN consists of 50 numbers of input data, which is considered as input training data of FFBPNN with 10 hidden neurons, which is used to carry the information from one layer to other layer and 43 output data that represents the class of communicating nodes. Neurons in the hidden layer are selected in a way that underfitting and overfitting should not occur and class of communication nodes are automatically adjusted according to the neurons of hidden layer.

In this research, FFBPNN is trained based on the energy the nodes consume and delay occurs during the transmission of data. The decision of data transfer from a node to the other node has been taken on the basis of energy consumption and delay. Initially, energy consumption of each node is determined and if it exceeds 5 mJ then the node is assumed as an attacker node and data is not transmitted to that node.

After this, the delay parameter has been analyzed; if the delay is also more than 5 ms then also that node is considered an attacker node. In case, when the energy consumption and delay is less than 5 mJ and 5ms respectively, then the nodes are considered as a normal node and data transmission takes place. The threshold level is decided for a particular simulation iteration based on communicating nodes, which are participating in network for data transmission and threshold level is defined using average value of all participating nodes in the network.

The Mean Squared Error (MSE) determines during the training of the network as shown in Fig. 4. The network has been trained with 96th iteration with a minimum error of about 0.5.

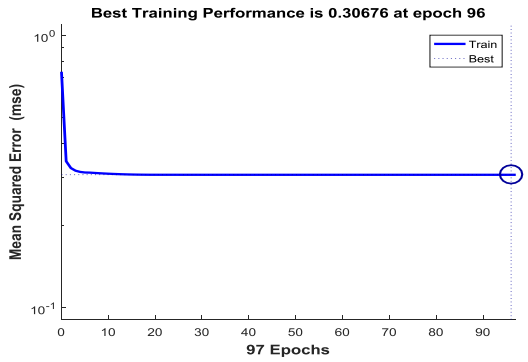


Fig. 4 Performance of FFBPNN

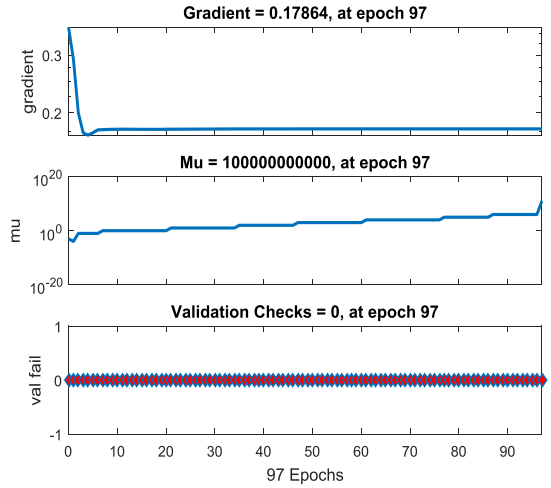


Fig. 5 Training state of FFBPNN

The training of FFBPNN has been examined using the parameters, as shown in Fig. 5. The training state has been tested using mutation, gradient and validation failure. In this research, the gradient and mutation of about 0.17864, 1011 with zero validation check has been obtained. The smaller value of gradient represents that the segregation among normal and attacker node is done properly, as it represents the nature of property towards their target. Here, mutation represents the bias value which is added during the target selection done by FFBPNN. Validation check value represents the numbers of iterations to validate the training data.

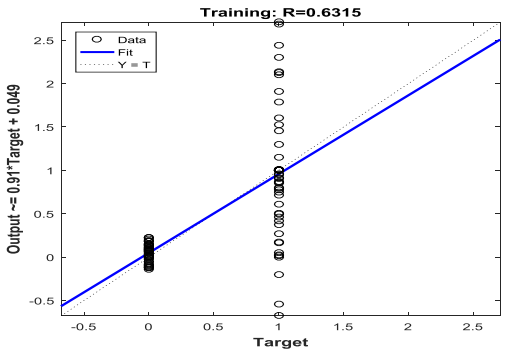


Fig. 6 Regression state of FFBPNN

Fig. 6, represents the regression of the training performance. The data of network is denoted by circle and their training slope is represented with blue color and their fitness is represented dotted line. If the training slope is near to the fitness line, then the training accuracy consider as maximum.

The proposed algorithm is named as AODV_FFBPNN, which is written below.

Algorithm: AODV_FFBPNN
Input: Number Nodes and Coverage Area
Output: Optimized Route from sourceto destination
Initialization of variables
S: Source Node
D: Destination Node
NNAd: Neighbour Node Address
RREQ: Route Request
RREP: Route Reply
RCTable: Reply Collect Table
While (destination not found)
Source broadcast RREQ to neighbour nodes
If NNAd is destination node, then
RREP reverts to the source node
Else
Repeat the broadcasting process until destination not found
End
Route=NNAd
Check route intermediates nodes using FFBPNN
InitializeFFBPNN **parameters**
→Node properties as a Training Data (TD)
→Nodes number as a Target (T)
→ Number of neurons (N=10)
→ Epoch (Iterations)
→Performance Parameters: MSE, Mutation, Gradient and Validation
→ Training Algorithm: Levenberg-Marquardt (Trainlm)
Net=newff(TD, T, N)
Net.trainparam.epochs=100
Net.divideParam.trainRatio = 70%
Net.divideParam.valRatio = 15%
Net.divideParam.testRatio = 15%
Net=train(Net,TD,T)
List of Authenticated Node=sim(net,Training_data)
Acount=1
AffectedNode= [] // Assign empty variable
For l=1→ List of Authenticated Node
If node is Authenticated
AffNodeNum=l

AffectedNode(Acount)=AffNodeNum
Acount=Acount+1
End
End
NewNode=1
For m=1→Total AffectedNode
NewNode(m)=CovSet(AffectedNode(m))
End
Return: Optimized Route from source to destination
End

IV. EXPERIMENTAL SETUP

To test the network performance in the presence of DDoS attack using prevention algorithm and without any prevention is demonstrated in this section. The network has been designed in MATLAB software using network, artificial intelligence tool boxes along with a graphical toolboxes which is known as curve fitting. To create network, network toolbox is used, for detection and prevention of network artificial intelligence toolbox is used with graphical toolbox, which is used for the representation of performance parameters.

The designed network for 50 nodes is shown in Fig. 7.

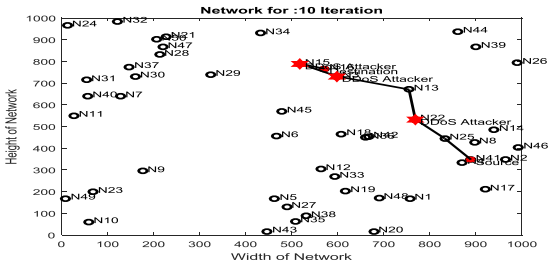


Fig. 7 Designed Network

In Fig. 7, node 41 is source node and node 15 is a destination node. For the data transmission, a route is created using AODV routing protocol. Node 14 sends "Hello" packet or RREQ message to its nearby nodes. "Hello" message includes source address, destination address and hop count. In this case, node 25, node 8, node 2 and node 46 receives "Hello" packet. All nodes except node 25 deny that the destination is not in its zone and next RREQ message has been sent by node 25, as destination node is in its range.

A similar process is re-casted until the target or destination is not determined. After the detection of the destination node, source node starts data transmission. In this network, node 22 and node13 are the attacker nodes that are being identified by the FFBPNN, but behave like genuine nodes and starts dropping data packets. To protect the network from DDoS attack and increase the throughput FFBPNN is used. The parameter is measured with and without prevention as discussed in the subsequent section.

V. RESULT AND DISCUSSIONS

During the simulation process, the parameters that are measured before and after prevention are throughput, delay packet delivery ratio and energy consumption. The throughput of the designed network for 10 rounds is shown in Fig. 8. The x-axis and the y-axis defined the number of rounds and throughput (%) with prevention technique and without prevention. From the graph, it is understandable that the throughput while utilizing the FFBPNN algorithm is high as compared to the throughput obtained without any prevention algorithm. In most of the rounds, throughput value is best by utilizing the FFBPNN as classifier but in few rounds it is same or better, because the intermediates nodes of route are not affected by attackers.

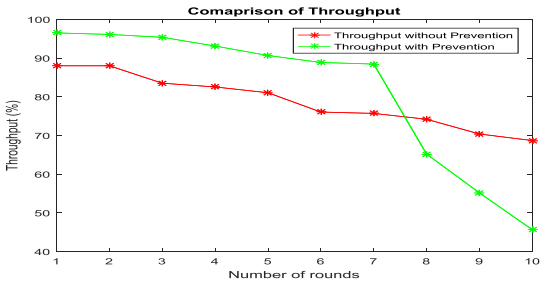


Fig. 8 Throughputof AODV_FFBPNN model

The average values of throughput observed for the designed network with prevention algorithm and without prevention algorithm are 81.49 and 78.80 respectively. Thus, an increase of 3.41 % has been analyzed this is due to the utilization of FFBPNN as a classification technique to distinguish between the normal and attacker node. The throughput is increased as the FFBPNN detect the DDoS attacker node and hence change the route of data transmission.

PDR is used to measure the rate of the total number of packets arrived at target node (N15) to the total number of a packet sent from the source node (N41). The comparison of PDR obtained with and without FFBPNN is shown in Fig. 9. From the Fig. it is clear that initially PDR is same up to second round this is because there is no attacker node found in the communication route. After that PDR starts decreasing when there is no prevention algorithm is used this is because the attacker node drops data packet. It has been examined that PDR of proposed work is more as compared to the PDR without FFBPNN. In most of the rounds, PDR of proposed model is more by utilizing the FFBPNN as classifier but in few rounds it is same, because the intermediates nodes of route are not affected by attackers and transmitted data properly.

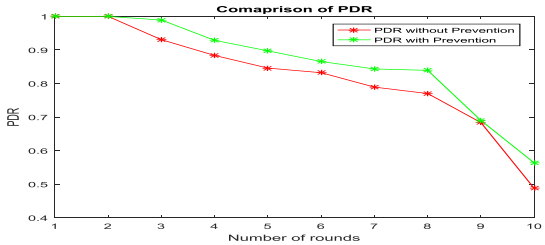


Fig. 9 PDR of AODV_FFBPNN model

The average of PDR obtained without and with FFBPNN are 0.82234 and 0.86173 respectively. Hence, the PDR using FFBPNN has been increased by 4.79 %.

Delay is used to determine the average delay o ccur during the transmission of data from

source node (N41) to destination node (N15). From the graph plotted in Fig. 10, it is observed that in the presence of attacker node (DDoS), the data reached at the destination node would be late as compared to the data reached at the destination while the network is prevented from the DDoS attacker node.From the graph it is clearly seen that when prevention algorithm is applied the packets reach at their respective destination with smaller delay. But, after 7th iteration there is a minor variation seen for the delay observed with and without prevention algorithm, this is because the communicating nodes are not properly affected by attacker so they take less time for the data transmission.

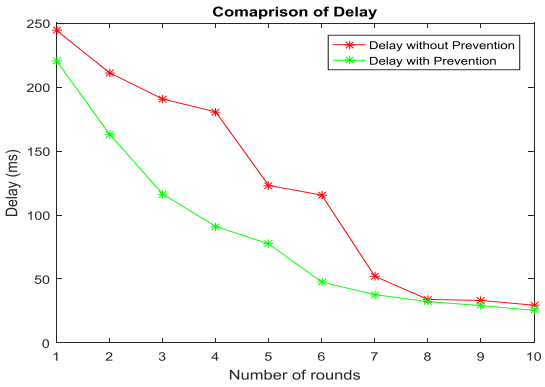


Fig. 10 Delay of AODV_FFBPNN model

The average value of delay observed without and with prevention are 121.45 ms and 84.13 ms respectively. Thus, there is reduction in end to end delay of about 30.73 %.

The energy consumption of the nodes during the data transmission process from node 15 to node 41 is shown in Fig. 11 in the graphical form. The energy consumption is less after preventing the network from the DDoS attack as compared to the network while attacker nodes are present. In most of the rounds, energy consumed by communicating nodes is less by utilizing the FFBPNN as classifier.

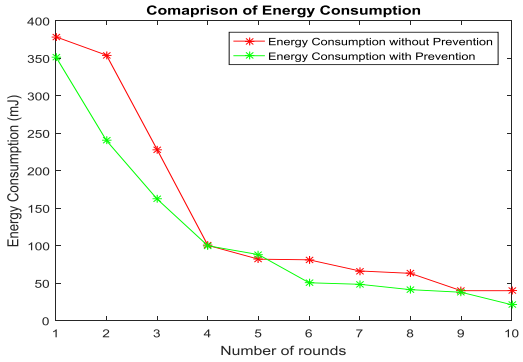


Fig. 11 Energy consumption of AODV_FFBPNN model

The average value of energy consumption measured during the experiment while FFBPNN is applied and in the absence of FFBPNNare143.45 mJ and 114.24 mJ respectively. From this, it has been concluded that there is a reduction of approximately 20.36 % while using FFBPNN in the network.

A. Comparison of our proposed work with Bhuvaneswari et al. [19, 2018]

The comparison of proposed work has been performed with the work done by Bhuvaneswari et al. in 2018. In their article, the authors have proposed an OLSR routing protocol for the prevention of the network from DoS attack. The malicious nodes have been identified by using their "HELLO" message as well as the Topology Control (TC) messages sent from the node at regular interval of time. It has been observed that as the network size increases the overhead becomes negligible in such case OLSR protocol performs well and hence increases the security of the network. It has been examined that the performance parameters like throughput, PDR are less in the presence of the attack when no fictitious node included. With the number of nodes increasing, there is an enhancement of network performance.

Table 2 Comparison of Throughput and PDR and Delay (%).

Parameters	Proposed Work (AODV_FFBPNN)	Bhuvaneswari et al. [19]
Throughput (%)	81.49	56
PDR(%)	86.173	56
Delay(%)	61.86	35.75

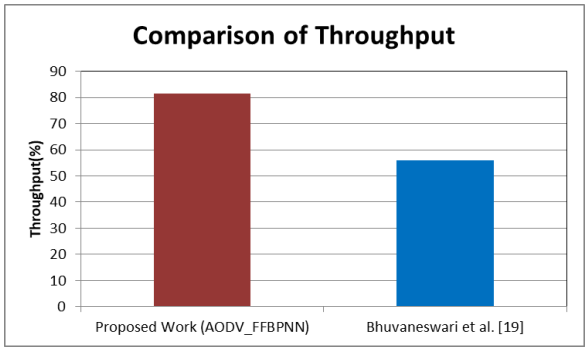


Fig. 12 Throughput Comparison of AODV_FFBPNN with Bhuvaneswari et al.[19] model

Fig. 12 defines the comparison graph for throughput values using FFBPNN and analyzed by Bhuvaneswari et al.[19] using OLSR as a routing protocol. From the graph, it has been observed that using FFBPNN the throughput has been increased by 45.52%. This is due to the proper selection of route as FFBPNN helps to distinguish among attacker node and genuine node.

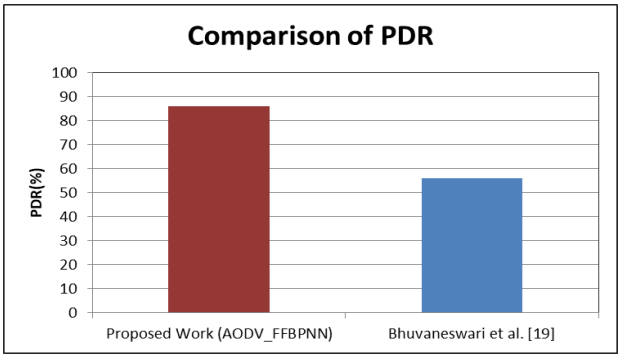


Fig. 13 PDR Comparison of AODV_FFBPNN model with Bhuvaneswari et al.[19] model

The comparison of PDR using AODV with FFBPNN and with OLSR as a routing mechanism has been shown in Fig.

13. From the graph, it has been

examined that the PDR has been increased using an artificial intelligence technique. This is due to the fact that FFBPNN classifies the attack as well as protects the network from DDoS attack. Hence, the percentage increase in PDR using FFBPNN has been obtained at about 53.88 %.

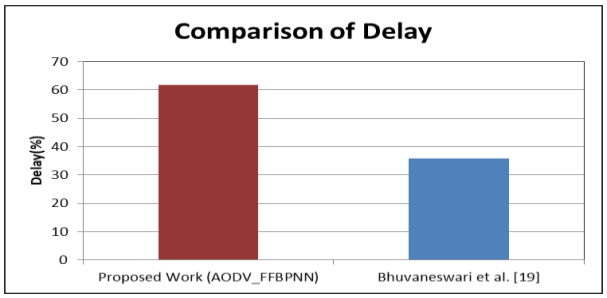


Fig. 14Delay Comparison of AODV_FFBPNN model with Bhuvaneswari et al.[19] model

The percentage reduction during the data transmission has been computed by delay parameters and is measured on the average basis. From the Fig., the percentage reduction in delay using FFBPNN is more compared to existing work and hence there is a reduction of 42.21% has been obtained.

VI. CONCLUSIONS

This paper presents a model for MANET to prevent network from type of DoS attacks. So in this paper we focus on the DDoS attack is an event that reduces or eliminates the potential of the network to fulfill its expected function. These threats affect the network bandwidth by allocating the available bandwidth of the actual user to the unauthorized user. The effect of these attacks will be temporarily prevented from blocking the service network information. Therefore, in this research work, a DDoS attack detection and prevention system is designed by utilizing the machine learning approach. The route between source and destination node has been discovered by utilizing on-demand route discovery mechanism which is a trust worthy routing model. In MANET, FFBPNN is used to train the network on the basis of the node's properties like energy consumption and delay. During the training, first priority of network is based on the energy consumption and if FFBPNN not able to detect the intermediate nodes in route, then the concept of node's delay is used. Also, the performance parameters has been computed and compared with the existing work to show the efficiency of the proposed work. From the experiment, it has been analyzed that the throughput, PDR and reduction in delay has been increased by 60.71 %, 53.57%.and 42.21 % respectively.

REFERENCES

1. Feng, Fang, Xin Liu, Binbin Yong, Rui Zhou, and Qingguo Zhou, "Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device," *Ad Hoc Networks*, vol. 84, pp. 82-89, 2019.
2. Misra, Sudip, Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, and Pushkar Gupta, "A low overhead default tolerant routing algorithm for mobile Ad Hoc networks: A scheme and its simulation analysis," *Simulation modelling practice and theory*, vol. 18, no. 5, pp. 637-649, 2010.
3. Kout, Akram, Said Labed, and SalimChikhi, "AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks," *Wireless Networks*, vol. 24, no. 7, pp. 2509-2519, 2018.
4. M. Walia and R. K. Challa, "Performance Analysis of Cross-Layer MAC and Routing Protocols in MANETs," *Second International Conference on Computer and Network Technology*, pp. 53-59, 2010.
5. Srivastava, Prakash, and Rakesh Kumar, "A Timestamp-Based Adaptive Gateway Discovery Algorithm for Ubiquitous Internet Access in MANET," *Next-Generation Networks*, pp. 153-162, 2018.
6. Abolhasan, Mehran, TadeuszWysocki, and ErykDutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc networks*, pp.1-22, 2014.
7. Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, no. 1, pp. 4-16, 2011.
8. Shams, Erfan A., and AhmetRizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Networks*, vol. 24, no. 5, pp. 1821-1829, 2018.
9. Alsumayt, Albandari, John Haggerty, and Ahmad Lotfi, "Evaluation of Detection Method to Mitigate DoS Attacks in MANETs," *1st International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-5, 2018.
10. Chhabra, Meghna, and B. B. Gupta, "An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET)," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, no. 10, pp. 2033-2039, 2014.
11. Zakariaa, AznidaHayati, MdYazidMohdSamana, Ahmad Shukri M. Noora, and HasniHassanb, "Finding shortest routing solution in mobile ad hoc networks using firefly algorithm and queuing network analysis," *JurnalTeknologi*, vol. 77, no. 18, pp. 17-22, 2015.
12. Anbarasan, M., S. Prakash, A. Antonidoss, and M. Anand., "Improved encryption protocol for secure communication in trusted MANETs against denial of service attacks," *Multimedia Tools and Applications*, pp. 1-21, 2018.
13. Doss, Srinath, AnandNayyar, G. Suseendran, SudeepTanwar, AshishKhanna, and Pham Huy Thong, "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," *IEEE Access*, vol. 6, pp. 56954-56965, 2018.
14. Iyengar NC, Banerjee A, and Ganapathy G, "A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment," *International journal of communication networks and Information security*, vol. 6, no. 3, pp. 233-245, 2014.
15. Von Mulert J, Welch I, and Seah WK, "Security threats and solutions in MANETs: A case study using AODV and SAODV," *Journal of network and computer applications*, vol. 35, no. 4, pp. 1249-1259, 2012.
16. Sharma P, Sharma N, and Singh R, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network," *International Journal of Computer Applications*, vol. 41, no. 21, pp. 16-21, 2012.
17. Jain HR, and Sharma SK, "Improved energy efficient secure multipath AODV routing protocol for MANET," *International Conference on Advances in Engineering &Technology Research (ICAETR) IEEE*, pp. 1-9, 2014.
18. Nadeem, Adnan, and Michael P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp.2027-2045, 2013.
19. Bhuvaneswari R., and R. Ramachandran, "Denial of service attack solution in OLSR basedmanet by varying number of fictitious nodes," *Cluster Computing*, pp. 1-11, 2018.

AUTHORS PROFILE

Jasmine Batra, M.E, Department of Computer Science, NITTTR, Chandigarh

Dr. C Rama Krishna, Ph.D. from IIT Kharagpur, M.Tech. from CUSAT, Cochin B.Tech. from JNTU Govt. College of Engg., Anantapur
.

Retrieval Number: B3155078219/19©BEIESP
DOI: 10.35940/ijrte.B3155.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication