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

Prevention of Black Hole Attacks in Virtualized Cloud Network Using Trust-Aware Energy Efficient AODV Routing With Firefly Based AI Technique

Priyanka, Saurabh Kumar, Amandeep Kaur

Abstract: ***Cloud networks are very widespread and unreliable because of the amount of VMs and presented nodes in their Virtual Cloud Network. Nodes might connect and revoke networks at any time. Resilience is a advantage of cloud computing, but it has many safety issues in routing and transmitting information between messages. VCN research is very similar to the portable ad-hoc network (MANET), which depends on the collaboration of all involved nodes to provide fundamental activities. Many safety assaults and risks exploit the safety of information transmission due to the decentralized environment in VCN and MANET. Malicious nodes can interfere and use information during wireless communications. Numbers of methods are there that has a diverse effect on such attacks for malicious nodes. Varied attacks are susceptible to security, but Black hole assault is one of the most common effective assaults, as fraudulent nodes dump all incoming emails reducing network performance and reliability. A black hole node is designed to lampoon every node in the network that conveys with some other node by saying it always has the easiest route to the target node. In this manuscript, a secure routing discovery method has been presented using Ad hoc on demand distance vector (AODV) routing protocol. For the detection of attack in the cloud, the concept of Artificial Intelligence (AI) has been used. Therefore, in this research, Artificial Neural Network (ANN) and Support Vector Machine (SVM)is adapted to determine Packet Delivery Ratio (PDR), Delay and Throughput measures. The comparative examination has been conducted to depict the proposed FNN-AODV effectiveness. There is an enhancement of 61.01% in FNN-AODV and 5.08% enhancement in Throughput in proposed FNN-AODV than R-AODV, 6.26% enhancement in PDR for FNN-AODV than R-AODV and 10.8% is the decrement in delay in FNN-AODV than of R-AODV.***

Index Terms: ***Cloud Computing,Black hole attack AODV routing protocol, Artificial Intelligence, Throughput , Delay , Packet Delivery ratio***

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

Priyanka Sharma*, Department of Information and technology,University Institute of Engineering and Technology,Panjab University, Chandigarh, India.

Saurabh Kumar, Computer Science and Engineering, Chitkara University, Punjab, India.

Amandeep Kaur,Computer Science and Engineering, Chitkara University/ Punjab, India.

I. INTRODUCTION

The cloud is a technology that is booming in the computer field. Its aims are to access software applications and information technology in an information connection. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are packaged together to form a cloud [1]. Each of the mentioned services is cloud computing services provided by cloud. These services are hosted by the cloud service provider in the data centre for an association or individual users to use the service over a network connection. A cloud service provider is a company that provides numerous services in the cloud. Chief providers of cloud services are; Sales, AWS, Cisco, Google, IBM (software), Apple, Oracle, Microsoft (Azure), Rack space, SAP and Verizon (the latter won the Terre logo). However, Apple and Sales force are involved in offering their hold apps instead of hosting apps for others. A corporation like IBM, Microsoft, SAP and Google present all three services of the cloud, while others offer two or one cloud service [2]. The major drawback in the cloud is the security attack. It arises because of the issue of data storage at diverse geographical fields in cloud computing. So, in this research, to cop up with this, in this research work, AODV routing protocol has been used. The AODV protocol has become popular in the demand protocols due to routing without loop over the years; it requiresless broadcasting than the DSDV protocol. However, if the designers of the AODV did not take into account security reasons, the enemy would be able to attack AODV; additionally, many attacks can be performed without compromising the AODV protocol rules [3].

Cloud networks are very extensive and unreliable due to the flexibility of the amount of VMs and presented nodes in their virtual cloud networks which can join and revoke networks at any instant. Resilience is an benefit of cloud computing, but it has many safety problems in routing and data transmission between messages. VCN job is very comparable to the Ad-Hoc portable network (MANET), which depends on the collaboration of all involved nodes to provide fundamental operations[3]. Many safety assaults and risks exploit the safety of information transmission due to the distributed environment in VCN as well as MANET.

Many safety assaults and risks exploit the safety of information transmission due to the distributed environment in VCN as well as MANET. Since we consider shifting Ad-Hoc networks as portion of our personal VCN, due to their auto-configuration and peer-maintenance capacities,
they are getting a ton of publicity Since we consider shifting Ad-Hoc networks as portion of our personal VCN, due to their auto-configuration and peer-maintenance capacities, they are getting a ton of publicity. Security has become a significant problem in offering safe communication between virtual machines (created through these cellular devices) and cloud information centers in possibly hostile environments[5]. As we have discovered from latest studies, personal VCN wireless nodes have higher safety problems than traditional connected nodes in the network. For tracking, a reliable routing protocol setting has been presumed in a wireless ad-hoc-based network that is component of a personal VCN, but a big quantity of ad-hoc network use is operated without confidence. This paper deals with the mitigation of black hole attack by using Firefly algorithm and Neural Network by considering the AODV routing protocol [5].

II. THEORETICAL BACKGROUND

In this segment, the working of Black hole attack has been discussed with the delineation of AODV routing protocol.

A. Black Hole attack

Private cloud networks are susceptible to multiple assaults. General assault kinds are the risks against physical, MAC and network levels, which are the most significant elements for the wired and wireless communication system. Ad-Hoc networks in Private cloud [6].
In a Black hole attack, an attacker declares an effective shortest path towards the destination by transferring inconsistent routing information. In a reply from a dissimilar node through the route discovery process, the starting node judges the path from the malicious node as a real node with an update path to the destination. Accordingly, a fake route has been created through this node [7]. An attacker reverts as denials of service by absorbing the traffic because it interrupts and rejects the packets that are forwarded via it. Fig. 1 illustrates the nature of a black hole of Z attacker, which drops the packets transferred by S as Source to D as a destination [8].

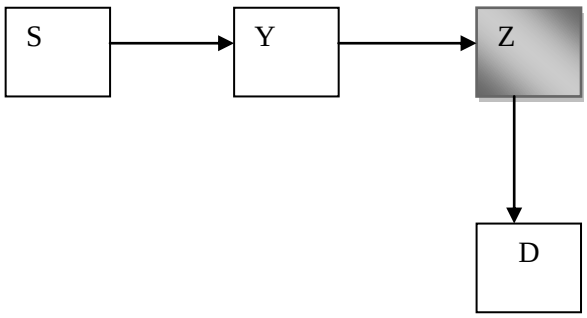

Fig. 1.Behavior of Black hole attack

B. AODV Overview

It is a response protocol where the route discovery process is launched by the origin node to lay the path to the target before beginning the chat session [9].It does not participate in periodic routing table exchanges, such as active protocols; due to the nature of on-demand, nodes do not have to maintain routes to other nodes until they desire to communicate with numerous nodes. Every node once in a while sends a HELLO message to the neigh bouring node to announce its presence. An entire route has been monitored by the subsequent hop node. Due to the concept of serial numbers borrowed from DSDV, AODV generates acyclic routes.

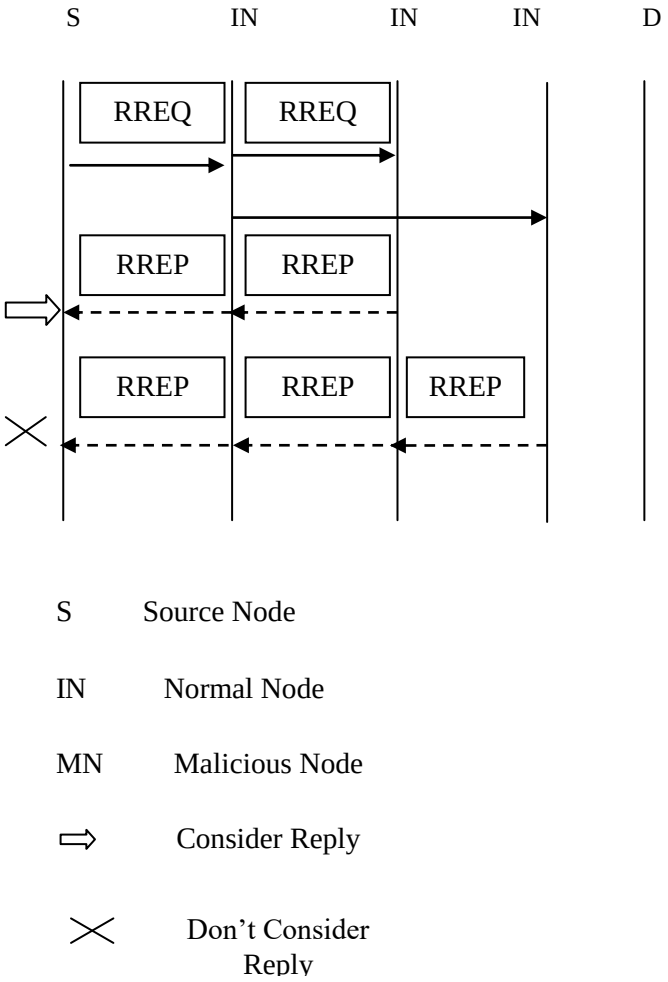

Fig. 2. AODV route discovery process

AODV uses three control packets: RREQ (Routing Request), RREP (Routing Answer), and RERR (Route Error). When the origin node needs to communicate with a target node that is not its neighbor, it transmits the RREQ packet and initiates the path finding procedure[10]. The RREQ maintains to be retransmitted to the neighbors with the marginal nodes until it is formed by the target itself or by a third node with adequate novel paths to the destination[11]. The node selects RREQ and generates RREP and returns it to the origin node's reverse path. When the node sees a connection outage or gets a packet to be transmitted to its location without an effective path, it generates an RERR packet[12]. RREQ and RREP are thus used across the path exploration stage and RERR is used during the path storage stage.

If a node obtains a control packet connected with a part icular node, it compares the sequence number with the sequence number of the routing table; if it is larger, the routing table is updated, and otherwise, the control packet is discarded. The operation of AODV under normal conditions is shown in Fig. 2; the source node S broadcasts RREQ to find the route to destination node D.

Two intermediate nodes INs sends RREPs on the reverse path in response to RREQ [13]. S considers the route established to D by the update and shorter route represented by one of the RREPs; the other RREPs are discarded.

III. RELATED WORK

Numerous scientists have identified extensive methods to eliminate black hole attacks, and few of them are described below:

The author used the TAODV (trust-based ad # # hesive network) strategy in [1] to avoid black hole assaults. All service provider nodes are initialized with a range of 0.7. When the initiative broadcasts RREQ and gets the route through RREP, it first checks the sequence number and then checks the trust node's trust index. If the value is less than 0.7, the node is said to be a black hole node and is blacklisted. Select a node with a high confidence index to relay messages. If the packet is delivered to the destination, the trust index value increases, otherwise it decreases. The author [2] proposed a resource node RREP packet that waits for multiple intersections. At this standby time, the node sends the packet in the buffer. When the RREP comes across more than one node, the exact destination is removed. Some berries should be shared at multiple intersections. The starting point, using these routes, determines the route of destination if no key is shown on this recurring route, waits for the other route response. This solution provides the best route for destinations but is experiencing an increased delay time. [3], the AODV protocol is con Fig.d with a trusted function. The increments are classified as reliable, most reliable and invalid based on a secure function. By this method, a trust mask is stored by each node. This table retains confidence in a particular horn with its neighbours. The function used for valid valuation is T = tanh (r1 + r2), where r1 and r2 are two calculated values. The source node controls the trust status to search for the destination. Some counterfeit packages are sent to update your trust status. The author [4] offers a solution that stores each node DRI stand. This is a table where you have access to each node and whether your specific neighbour is received through this neighbour and has node packages. Prices may be 0 or 1. In the table,it is updated when packages are received through a custom node or custom node. This table is refreshed while looking for a reliable way. In [5], the author has proposed a method that has created the N node network. The time of the node encounter with neighbours and the breakdown of the connection between the TV node and the neighbour. Neighbour node list is stored for each node. Hint value is computed with h = tb-te. When h is excessive or threshold value, the situation is defined as another black hole node associated with a fair node. By using this, a list of fair junctions can be provided, and packages can be sent through these fair knots. [6] Has proposed Ant Colony Optimization (ACO) with the packets to perform the shortest route assignment. The node that receives an ant packet checks the row number in the routing table. If the sequence number in the backup packet is greater than the routing table, the node is considered to be malicious. An alarming package is transferred to all the neighbors, including a list of all malicious nodes to be called. [7] Have presented a method to make the source independent of its neighbor. It introduces RREP to the goal management and is called as MRREP. When the RREQ arrives at the destination, it responds with MRREP. The malicious node always sent a fraudulent response to the highest number of digits, but the malicious node can be used to prevent the target id idle, and the black hole attack will be prevented. The author [8] has proposed a technique of waiting for the RREP, which was sending a false RREQ and equaling half the RREP's waiting period. The non-malicious node has never reacted to fraudulent RREQ, so, the intersections that respond to be harmful and has be added to the black hole node list. [9] Has utilized a method that listened to each node's neighbors in an extraordinary way that each node checks the forward delivery of the package sent to the neighbor. It uses the next node-transmitting storage mechanism to confirm packet forward transmission. If the node cannot strike the similar package, then the adjacent node is considered to be malicious and the packet is considered low. This decreases the value of the neighbouring node using T = 1 - D / F, where T is the threshold value among 0 and 1, D represents the dropping packets with a node, and F shows the total packets sent to this node. The authors [10] have suggested that the RREP be used to detect the major difference among the sequence number of the source node and destination. They adapt the receiving node number to the initial node queue number, and if the differences are superior to the two, then the node is considered as attacking node and has to be abandoned instantly. In [11], the author has presented an article based on Intrusion Detection with Anomaly that could be utilized in the prevention of black hole attack. The author [12] has utilized a fidelity table in which the nodes could be assigned for measuring the reliability of the node. When the level of fidelity came to zero, then it could be taken as malicious nodes and later gets the elimination. In [13], the author has utilized the zone routing protocol as a hybrid protocol for taking benefits of residual routing protocols. Each node has its individual zone for the connection maintenance. [14] have presented a technique that lessens overhead. The author has utilized the manner of ID with numerous agents in the communication of network with the server or with one another being accountable for the provision of information transmitted for analysis, monitoring and for the attack. [15] has utilized the model of static key distribution than of distributing dynamically and the selection of key is based on hop count value and this method lessens the overhead. [18] Has considered virtualized cloud network for the prevention of black hole attack by considering reactive and proactive protocols. The effect of black hole attack on VCN performance with MANET is executed. It has been found that AODV is more vulnerable to black hole attack than DSR.

The aim of this article is to develop a secure network has been designed considering AODV routing protocol. But AODV lone cannot examine the intermediate node's behavior in the network, so, Firefly and neural network is considered. The aim of the firefly algorithm is to examine the behavior of the intermediate node with the fitness function. The neural network has been used as a classifier.

IV. PROPOSED FRAMEWORK

This section delineated the proposed work flow for the detection and mitigation of black hole attack using Firefly and ANN algorithms in a virtualized cloud network:

Step 1: A private cloud network has been designed for with some specified dimensions. For the network deployment, 1000X 1000 dimensions as height and width are considered. Initially, number of nodes are produced in the network with X and Y network co-ordinates.

Step 2: The source and destination are defined after private cloud network creation from N nodes with the co-ordinates.

Step 3: The initialization of each node coverage nodes has been taken place with source and destination.

Step 4: The code has been build up for AODV routing protocol for discovering the route amongst source and destination node.

Step 5: Firefly algorithm is being considered for the process of route discovery and the selection of the best route as per the coverage set.

Step 6: The fitness function of the firefly algorithm is designed as per the necessitate information.

Step 7: When there is the discovery of route between the source and the destination then the intruder or the attacker using ANN has been checked and when the attacker is being discovered then the cache routing table has been identified and is saved.

Step 8: The attacker types are identified from attacker activities perspective and the attacker presentation from the attacker is verified for the better result achievement

Step 9: For the depiction of the effectiveness of the research work, QoS measures, such as Packet Delivery Ratio (PDR), Delay and Throughput are computed.

Below the algorithms are defined that are considered for the simulation of the proposed work:

Algorithm 1 defines the process used for network deployment in private cloud network. In this research, the network is designed with an area of 1000 and 1000 square meter. The coordinates of the nodes are defined along with the source and the destination.

Algorithm 1: Network deployment algorithm

1. Describe height as 1000
2. Describe width as 1000
3. Describe N nodes for network simulation
4. For i = 1 to N
   Plot_node(i)=co-ordinate(X, Y)
   Describe node name as N (i)
   Source_Node as random (N)
   Destination_Node as random (N)
5. If Source_Node == Destination_Node
   Source_Node = random(N)
   Destination_Node = random (N)
6. Else
   Source_Node = Source_Node
   Destination_Node = Destination_Node
7. End
8. Describe Source_Node as source
9. Describe Destination_Node as a destination
10. End

Algorithm 1 is used to create a private cloud network using some specific height and width of the network and after that, a node is considered as a source node and another node is consider as the destination node. Based on the created private network, the simulation of the proposed network becomes possible, so, for the simulation coverage area of nodes is calculated using algorithm-2.

Algorithm 2: Coverage area formation algorithm and routing algorithm

1. Describe Coverage_set= $\frac{20*\text{width of network}}{100}$
2. For i = 1 to N
   Coverage _set(i) = Coverage_set(N)
   Coverage_list(N, i) = Coverage_set(i)
   End
   For i = 1 to N
   Route (1) = Source_Node
   Route (i) = Source_Node(Coverage_se(N))
   If Coverage_set(Source_Node) == empty
   Subsequent_node = random
   End
   Iterate while the destination is not discovered
   Route (end) = Destination_Node
   End

The coverage area of each node along with the route formation process is described in algorithm 2. Using the concept of the coverage area of nodes, route discovery process became easy and the route from the source node is initiated. The routing process is repeated until the destination node is not discovered.

Algorithm 3: Firefly Algorithm

Input: Other Respondents (OR)
Output: Optimized Data
Fly_Light=[Energy_Consumtion (OR), Operating_Time (OR)]
$\text{Fly}_{\text{Threshold}} = \sum_{i=1}^{n} \text{Fly}_{\text{light}}$
Fly_(Flash_time)=Time_(to_Respond)
If Fly_Threshold*Fly_(Flash_Time)<Fly_Light
Ignore
Else
Fly_(Light_Diff)=Fly_Light-Fly_Threshold*Fly_(Flash_Time)
Addition of Fly_(Light_Diff) to Possible List
Determine Index. Minimum (Fly_(Light_Diff))
Choosen . Node=Index.Id
End If
Return: Optimized nodes
End

Now to optimize route that is to select the best route among different routs optimization algorithm named as Firefly algorithm is used. The algorithm process is defined in algorithm 3.

After that, ANN is used to classify the black hole attack within the route. The basic structure of ANN is given in Fig. 3.Fig. 3 represents the training structure of the artificial neural network. The artificial neural network has three layers named as the input layer, hidden layer, and output layer. The parameters such as epoch, time, performance, gradient, mutation and validation check are shown in the red box.

After the execution of parameters, the process of training completes. From the Fig., it is evident that training of neural network terminated only when the execution of the validation parameter is completed. Here the results show that in 10th iterations, the best validation checks achieved is 6 with the performance of 1.27X10-19.

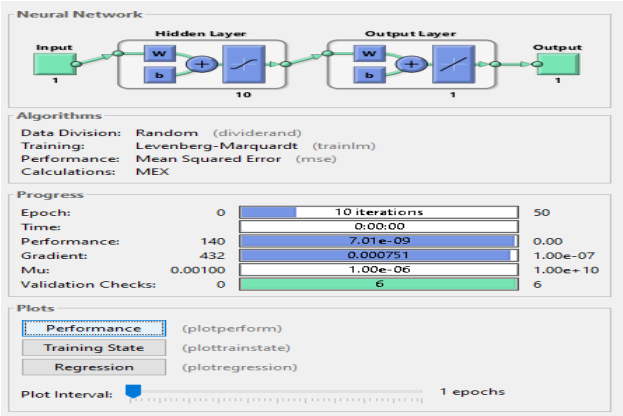

Fig. 3.Training structure of ANN

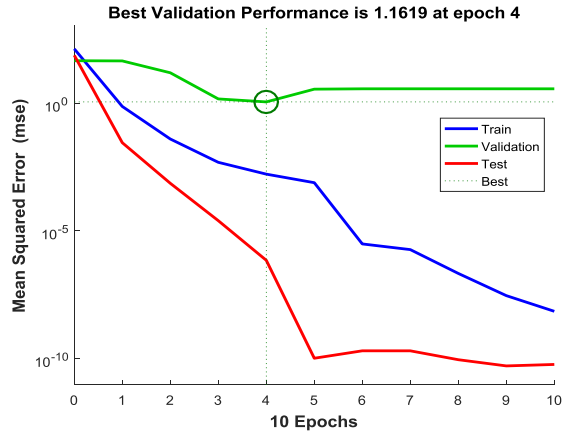

Fig. 4.Performance of ANN for 10 iterations

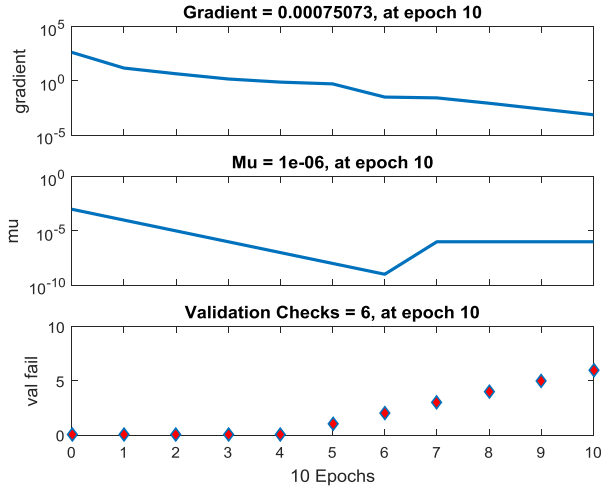

Fig. 5.Training state for 10 Iterations

Fig. 5 displays the training state graph for three parameters such as validation failure, mutation and gradient for 10 iterations. The input which is given to the neural network is represented by gradient value, which is about 0.00075073. The x-axis represents the number of iterations and y-axis represents the ANN parameter values. Mutation value=0.000001 is added to the gradient value in order to adjust the input to obtain the desired output. The neural network checks the validation up to maximum of 6 iterations to obtain the best result.

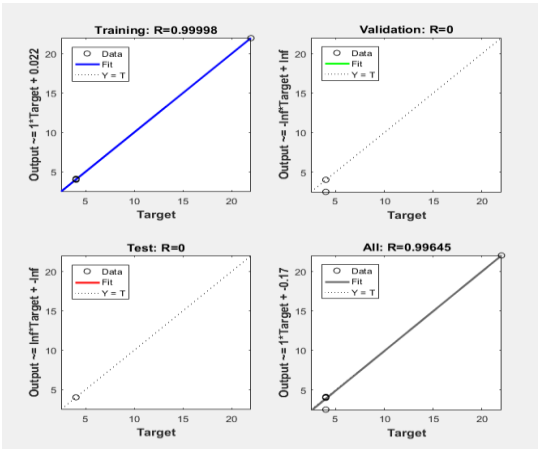

Fig. 6. Regression for 10 iterations

Fig. 6 represents the training of four communities using ANN classifiers such as training data, testing data, valid data and regression data. Form the Fig. it is clear that the training of the system is better because of the value of regression R s near to the 1.

Algorithm 4: Artificial Neural Network Algorithm

Load nodes optimize properties
Initialize the ANN
Describe parameters
Training data as optimize_data
Group = Attacker and Real node
Epoch as1000
Training algorithm=LM
Performance measures as MSE
Neurons=50
Network=neuro f_t (Training dta, group , neuron)
Net= Train (training data, net, group)
Classification=

$$\begin{cases} \text{Attacker; when properties not match} \\ \text{Real node; when match} \end{cases}$$

Return {Classified node as a attacker}

The optimized properties are applied as an input to the input layer of ANN. The working of ANN in the algorithmic form is illustrated in Algorithm 4. This algorithm is used to classify the attacker in the defined network.

V. RESULT AND ANALYSIS

This section defines the results obtained after the evaluation of the mitigation of black hole attack in MANET. The parameters, such as Throughput, Delay and PDR are computed to depict the efficiency of the proposed work and the comparative analyses are also conducted to illustrate its fruitfulness.

Fig. 7 and Table 1 depicts the comparison of proposed work with respect to throughput with conventional methods. The comparison has been drawn by considered 40 nodes. Throughput depicts the number of packets received at the destination point by means of simulation time.

Table 1.Throughput comparison

Number of nodes	Throughput			
	R-AODV [16]	RID-AODV [17]	AODV [18]	FNN-AODV [Proposed]
10	4.5	4.3	3.56	4.8
20	4.6	1.5	6.43	7.7
30	4.9	1.3	8.34	9.0
40	4.5	1.1	10.24	12.9

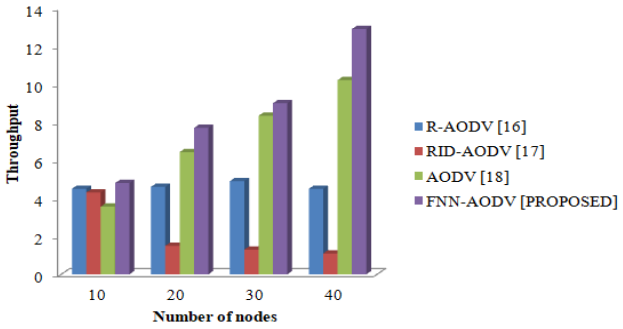

Fig. 7. Comparative analysis of proposed throughput with conventional methods [16], [17] and [18]

The calculation of throughput is in kbps. 8.6 kbps is the average value of Throughput for FNN-AODV, 1.84 bps is the average value of Throughput for RID-AODV [17], 4.48kbps is the average value of Throughput for R-AODV [16] and 7.14 kbps is the average throughput value of [18]. 78.60% is an enhancement in throughput of FNN-AODV than RID-AODV, 47.90 % is an enhancement in throughput of FNN-AODV than R-AODV whereas 16.97% is an enhancement in throughput of FNN-AODV than AODV.

Table 2.PDR comparison

Number of nodes	PDR		
	R-AODV [16]	AODV [18]	FNN-AODV [Proposed]
10	0.85	0.93	0.94
20	0.85	0.94	0.95
30	0.87	0.95	0.96
40	0.88	0.95	0.97

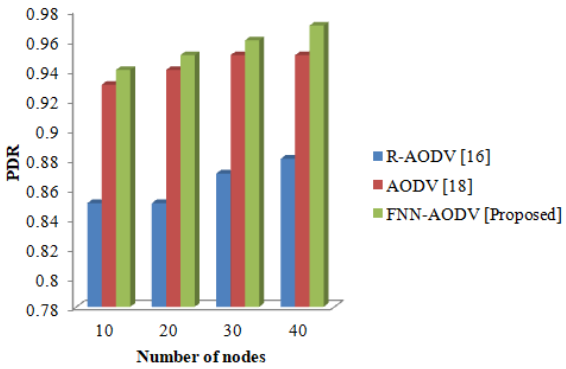

Fig. 8.Comparative analysis of PDR for proposed FNN-AODV with Conventional Methods [16] and [18]

Fig. 8 and Table 2 illustrates the comparison of PDR for conventional methods [16], [18] and proposed FNN-AODV. The comparison has been drawn by considered 40 nodes. PDR defined the proportion of packets that are efficiently sent to the destination by the sender. 0.95 is the average value of PDR for FNN-AODV, 0.94 is the average value of PDR for [18] and 0.862 is the average value of PDR for R-AODV [16]. 1.05% is an enhancement of PDR of proposed FNN-AODV than [18] and 9.26 % is an improvement in PDR of proposed FNN-AODV than [16].

Table 3.End to end delay comparison

Number of nodes	End to End delay	
	R-AODV [16]	FNN-AODV [Proposed]
10	57	50
20	56	49
30	53	51
40	49	40
50	44	41

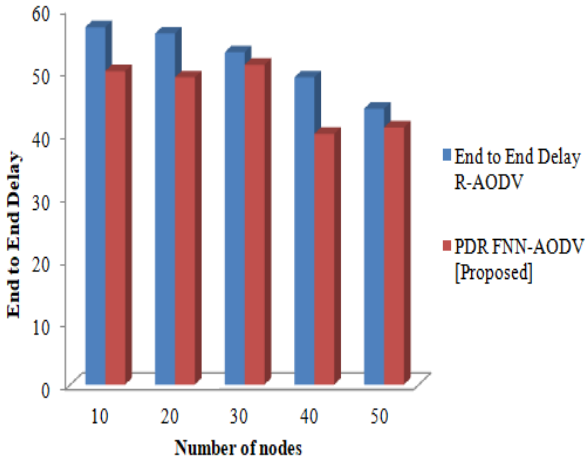

Fig. 5.Comparative analysis of Delay or proposed FNN-AODV and Conventional R-AODV [16]

Fig. 5 and Table 3 illustrates the comparison of Delay for conventional method [16] and proposed FNN-AODV. The comparison has been drawn by considered 50 nodes. Delay is the time taken for the packet data to send over a network from a source node to destination node.

So, the routes are utilized in the network with less probability of delay for enhanced presented work performance. 51.8 is the average value for R-AODV for Delay and 46.2 is the average value of FNN-AODV proposed value. 10.8% is the decrement in delay in FNN-AODV than of R-AODV.

VI. CONCLUSION

For the security from Black hole attack in cloud, public and private clouds are addressed. Wireless network are susceptible to numerous attacks because of the nodes and environment physical characteristics. This research has presented FNN-AODV mechanism for the detection and prevention of black hole attack in virtual cloud network. AODV routing protocol has been adapted for the route detection. Firefly and ANN are utilized for the optimization of novel and authentic algorithm and for the production of safe and stable data transmission. For the route enhancement process, Firefly has been considered and for the detection of attacker, ANN has been used. Measures, viz. Throughput, PDR and Delay are addressed for the depiction of FNN-AODV efficiency and the comparative analysis is also conducted. An improvement has been noticed in all scenarios and productive results have been seen.

REFERENCES

1. A. Jain, U. Prajapati and P. Chouhan, “Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario”, *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, IEEE, pp. 1-4,2016.
2. N. Sharma and A. Sharma, “The Black-Hole Node Attack in MANET”, *Second International Conference on Advanced Computing & Communication Technologies*, Rohtak, Haryana, pp. 546-550,2012.
3. S. Singh, A. Mishra and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm”, *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, pp. 1-6,2016.
4. Antony Devassy and K. Jayanthi, “Prevention of black hole attack in mobile ad-hoc networks using mn-id broadcasting”, International Journal of Modern Engineering Research, Vol. 2, No.3, pp.1017-1021, 2012.
5. Pooja and R. K. Chauhan, “An assessment based approach to detect black hole attack in MANET”, *International Conference on Computing, Communication & Automation*, Noida, pp. 552-557,2015.
6. Pooja and R. K. Chauhan, “An assessment based approach to detect black hole attack in MANET”, *International Conference on Computing, Communication & Automation*, Noida, pp. 552-557, 2015.
7. Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, “Detection and prevention of blackhole attack in manet using aco”, IJCSNS International Journal of Computer Science and Network Security, Vol. 12, No.5, pp.21-24, 2012.
8. S. S. Narayanan and S. Radhakrishnan, “Secure AODV to combat black hole attack in MANET”, *International Conference on Recent Trends in Information Technology (ICRTIT)*, Chennai, IEEE, pp. 447-452,2013.
9. Sathish M, Arumugam K, S. N. Pari and Harikrishnan V S, “Detection of single and collaborative black hole attack in MANET”, *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, pp. 2040-2044, , 2016,
10. F. Thachil and K. C. Shet, “A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET”, *International Conference on Computing Sciences*, Phagwara, 2012, pp. 281-285.
11. Pooja Jaiswal, and Rakesh Kumar, “Prevention of black hole attack in MANET”, International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2,No.5, pp. 599-606,2012.
12. Y. F. Alem and Z. C. Xuan, “Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection”, 2nd International Conference on Future Computer and Communication, Wuha, pp. V3-672-V3-676,2010.
13. H. Weerasinghe and H. Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Future Generation Communication and Networking, Jeju, pp. 362-367, 2007.
14. S. S. Rajput and M. C. Trivedi, "Securing Zone Routing Protocol in MANET Using Authentication Technique”, International Conference on Computational Intelligence and Communication Networks, Bhopal, pp. 872-87,2014.
15. K. V. Arya and S. S. Rajput, “Securing AODV routing protocol in MANET using NMAC with HBKS technique”, International Conference on Signal Processing and Integrated Networks (SPIN), Noida, , pp. 281-285,2014.
16. Debdutta BarmanRoy and Rituparna Chakim, “Detection of blackhole attack in manet by specialized mobile agent”, International Journal of Computer Applications, Vol. 40, No.13, pp.1–6, 2012.
17. Prakhar Gupta, Pratyaksh Goel, Pranjali Varshney and Nitin Tyagi, “Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET”, In Smart Innovations in Communication and Computational Sciences, Springer, Singapore, pp. 271-279,2018 .
18. Rushdi A. Hamamreh, “Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks”, In Recent Advances in Cryptography and Network Security. IntechOpen, pp.25-41, 2018.
19. Kamaljit Kaur and Gaurav Raj, “Comparative Analysis of Black Hole Attack over Cloud Network using AODV and DSDV”, In Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, ACM, pp. 706-710, 2012.
20. Raj Gaurav, Kamaljit Kaur, “Secure Cloud Communication for Effective Cost Management System Through MSBE”, International Journal on Cloud Computing: Services and Architecture, Vol. 2, No.3, 2012.

AUTHORS PROFILE

Priyanka Sharma is a research scholar(M.E., Information Technology at University Institute of Engineering and Technology,Panjab University, Chandigarh) Her research interest includes cloud computing and Wireless networks. Her official email id is arohi.sharma.6.01@gmail.com

Saurabh Kumar is a research scholar(Ph.D., Computer Science, and Engineering, CURIN) at Chitkara University (Punjab) and also working as an operational director at Smart Tech Technologies for the last 7 years. The author has a number of publications in the area of Cloud Computing, Sensor Networks, and Security Frameworks. He is also an active blogger of Cloud and Machine Learning. His official mail id would be weth.smarttech@gmail.com

Amandeep Kaur is an Associate Professor in the Department of Computer Applications at Chitkara University, Punjab India and completed her Ph.D. in 2016 in computer science and engineering. She is having 11 years of experience in the same field. Her research interest includes Software Engineering, Agent-based web services, and Wireless Sensor Network.For Contact Information, her official email id is amandeep.bhullar@chitkara.edu.in