Fourth International Conference on Electronics, Communication and Aerospace Technology (ICECA-2020)
IEEE Xplore Part Number: CFP20J88-ART; ISBN: 978-1-7281-6387-1

Legitimate-path Formation for AODV under black hole attack in MANETs

Fahmina Taranum
Computer Science and Engineering
MJCET, Osmania University
Hyderabad, India
ftaranum@mjcollege.ac.in

Zainab Abid
Computer Science and Engineering
MJCET, Osmania University
Hyderabad, India
zainababid021@gmail.com

Khaleel Ur Rahman Khan
Computer Science and Engineering
Ace Engineering College, JNTU
Hyderabad, India
khaleelrkhan@gmail.com

***Abstract*—Mobile Ad-hoc Network (MANET) owing to their very open characteristics are being very attractive and adaptive. With the openness comes security issues to be dealt. The most usual attack in mobile ad-hoc network is the black-hole attack. It advertises false path as shortest and newest to the destined node. On gathering packets containing data will drop them and does not send it to the destination. This paper proposes an algorithm to overcome such an attack under Ad-hoc On-demand Distance Vector (AODV) routing protocol in MANETs. The proposal aims to detect and avoid black-hole attack by using the parameters of AODV routing protocol in its enhanced form of route recovery. The proposed algorithm has two different scenarios, where first comes the detection then the avoidance. The simulation results are obtained from NS-2 to authenticate the effectiveness of proposed technique in comparison with the existing protocols in the existence of black-hole attack with respect to change in simulation end time and active number of attackers. The implementation is assessed based on delay, delivery ratio, drop, overhead, throughput and packet forwarding ratio. The results obtained from network simulator are mapped to form a dataset, which is then validated on a modelled fuzzy inference system using MatLab software.**

Keywords—Mobile Ad-hoc network, security, black-hole attack, AODV, detect, avoid, NS-2, fuzzy inference system,MatLab

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a set of mobile nodes, which are actively and randomly positioned in a fashion that causes the link to change on a frequent basis. To provide communication between the nodes a through the routes routing protocol is used. Effective and accurate route establishment among set of nodes, so that data packets may be sent in a well-timed manner to serve the purpose of the routing protocol [1]. It is an ad-hoc network which is self-organized, without any pre-arrangement and self-configurable where the nodes move arbitrarily. Dynamic node movement in any direction causes link changes repeatedly [2]. MANET are appropriate for infrastructure-less or problematic or expensive to arrange or when network is required quickly. They are applicable in situations such as in emergency rescue processes during natural disasters, meetings, conferences, and combat zone communication between mobile vehicles and/or warriors.

Designing right and proper protocol to discover routes and handle frequent topology deviations in MANETs can boost the effectiveness of the network [3]. There are three broad classification of routing protocols. The first category is the proactive routing protocol which stores the routes for each node before the need. The second category is reactive routing protocol which finds route only when the need arises. The third category is the hybrid which is the combination of both proactive and reactive. The Routing and management of network are the two significant operations of networking. All types of communication network have security as its major reason to worry about. Such networks are inclined towards spiteful attacks because of its unique characteristics [4]. Though the open- nature of MANET makes it very attractive and vulnerable to attacks. To avoid different types of attacks many different detection prevention techniques have been proposed. The paper proposes a mechanism that plants, detects and avoid black-hole attack in MANETs.

The proposal's key idea is that it uses insecure AODV routing protocol and add security in routing. The mechanism aims in obtaining a valid path from source to destination. Detection is done by using delay as a parameter and authentication is provided using the validity of route parameters. The comparison between existing AODV protocol and the proposed work is it has enhanced AODV with respect to various parameters that shows how the performance of the system is enhanced. Further, for reasoning the results obtained from simulator, which are analyzed on a modelled fuzzy inference system that determines whether the network is secure or not.

II. CONCEPTUAL INFORMATION

A. AODV Routing Protocol

Ad-hoc on-demand distance vector [5] is an on-demand routing protocol for MANETs that creates route to destination only when required. AODV works in two states that are route discovery and route maintenance.

In the Route Discovery state, the control messages used are Route Request (RREQ) and Route Reply (RREP). The initiation of route discovery process is done through the source node that sends RREQ packet to the next hop neighbors once the need to forward data packets towards the destination node arises or when a legitimate route to the destination is not available. The neighbor nodes further rebroadcast the RREQ to their neighbor's until it gets a path to the destination or reaches the destination. When destination gets RREQ it unicasts RREP packets backwards to the source. Source node on receiving RREP starts sending data packets to the destined node. Routing table is updated if a shorter route to the destined node is found.

In the figure 1- [6] the route discovery for AODV is performed where S denotes source node, D denotes destination node. Here when S desires to send data packets to D it initially performs Route Request (RREQ) by sending RREQ packets to

its one hop neighbors to see whether it is the destined node or has a path to it. If so, Route Reply (RREP) message is forwarded back to the source so as to obtain a path from source to destination to transfer the data packets.

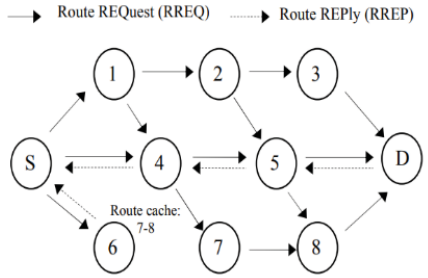

Figure 1: Route Discovery process for AODV [6]

In route maintenance state it uses Route Error (RERR) control message which is forwarded by the node which detects link failure and sent it to the node which initiated the Route Request. Upon receiving such message, the source node re-launches the route discovery process even if it receives the RERR, if a new route is still desired. Hello packets dissemination between the nodes helps in maintaining neighborhood information.

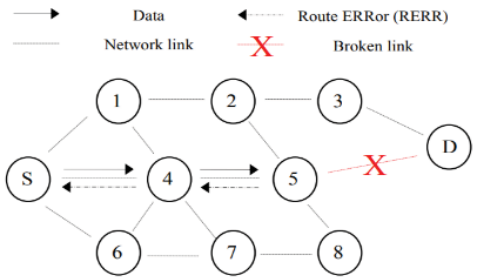

Figure 2: Route maintenance in AODV [6]

In the figure 2, [6] it shows the route maintenance process in case of a broken link. Where the link from node 5 to destination D is broken. So, node 5 sends RERR message to source S to inform about the broken link.

B. Black-Hole Attack

Black-hole attack is a form of Denial of Service (DoS) attack that aims to forward data packets to an attacker node in a network. Upon success it drops, modify contents, or forward it to another malicious node [7]. It is a security attack on MANET where a black-hole node presents itself to own the shortest route to the destination. Thereby dropping packets without sending it to the required destination node. If attacker drops data packets it is known as full data dropping attack [8]. Execution of black-hole attack using AODV protocol comprises of two phases. Which are discussed below:

Phase 1: Attacker node sends fake RREP with highest sequence number.

Phase 2: Dropping the received packets rather than sending forward [9].

Black hole node aims to avoid data packet to reach the specified destination node. In AODV the freshness of route is concluded by destination sequence number. In black hole attack the attacker node sets value of its destination sequence number of higher than that present in RREQ packet. The black hole attack first performs advertisement in order to send a bogus RREP to the initiating node where the aforementioned can get signal to forward the data. Upon successfully making source believe that it has either route to the target node or it is itself the destined node, the source forwards data packets. The attacker node on receiving the data packets deny to forward the packets, instead drop them thereby creating massive attack on the network as well as degrading the network performance. If multiple coordinated attacker nodes are used, it is called cooperative Blackhole attack [5].

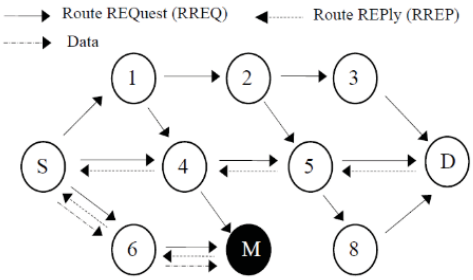

Figure 3: Black hole attack in MANET [6]

Figure 3, [6] illustrates an instance of black hole attack under AODV routing protocol where M denotes malicious node, S source and D destination. M being the malicious node presents itself to have shortest route towards D. The AODV routing protocol works on the protocol of taking the shortest path based on the number of hops and sequence number of the RREP packet. The Source node sends the RREQ message and accepts the fake RREP, it then forwards the data packets towards M via intermediate nodes. On receiving data packets, the malicious node does not forward the data instead it drops all the data. The malicious node M interrupts the successful transmission of data thereby causing a hole in the network. It becomes easier for any attacker node to intrudes into the network in case of reactive routing protocol such as AODV [10].

C. Fuzzy Inference System

Fuzzy logic is a way of representing information in human mind form. Fuzzy logic lets us deal with multi-valued logic by providing results within the range 0 to 1. Output attained is in degree fashion.

Fuzzy inference system is a process of interpretation of variables in an input vector grounded on defined rules to obtain a defuzzified output value. It maps input value to an output value using fuzzy logic. It is the crucial part of a fuzzy logic system possessing the right decision making as its main agenda. The rules are conditional based as "IF…THEN" which uses "OR" or "AND" to form a rule using different input variables. The output of the system is every time a fuzzy set regardless of its input value which can be either fuzzy or

crisp. A defuzzification unit converts fuzzy variables into crisp variables.

A fuzzy inference system has four modules and the outline of these modules is represented in the Figure 4. The components are fuzzification interface, knowledge base comprising of database and rule base, a decision-making unit and a defuzzification interface. The fuzzification interface converts the crisp value into fuzzy value. The knowledge base consists of the rules and membership functions. Decision-making unit bases actions on rules defined. The defuzzification interface changes a fuzzy value to a crisp value.

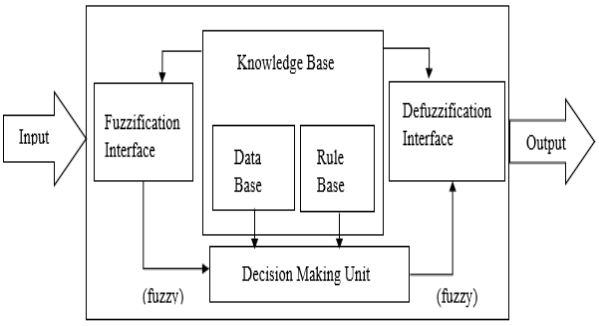

Figure 4: Fuzzy Inference System

III. Related Work

In [11] Raj et. al performed detection using threshold value and then prevents by updating the threshold value. It uses ALARM packet in order to inform other nodes and isolate the malicious node. It checks if the destination sequence number value is more than the threshold value if so, it is thought to be spiteful node.

In [12] Zhang et. al presented a mechanism which uses special reply (SREP) packet and special request (SREQ) packets which source and legitimate destination exchanges in order to detect any attacker node. If a node doesn't forward SREP packet, then it is suspected to be malicious and action is taken by neighboring nodes.

In [13] Arunmozhi et. al proposed neighborhood route monitoring table which is maintained to keep track of RREQ out time and RREP in time. The difference between the two intervals is taken to obtain diff_time which is compared to min_time. If diff_time is less than minimum time it is suspected to be black hole node else believed to be a reliable node.

In [14] Kumar et. al put forward an Intrusion Detection Technique that has been carried out to detect and isolate black-hole attack for AODV routing protocol. The authors here use the delays as parameters to decide the authenticity of the node. It uses Destination sequence number and hop count threshold in order to finalize whether the node is intruder or not.

In [15] Verma et. al implemented a clustering algorithm which applied in order to create different clusters for malicious and non-malicious nodes. Using clustering, nodes that are malicious are added to malicious table. Such nodes are not included in the path to send data to the destination.

In [16] Luong et. al presented a Valid Route Authentication mechanism which checks for three conditions to select a route as valid. It uses parameters such as Destination Sequence number and number of hops. It defines validity of route if it is actual neighbor, Normal route and Destination Sequence Number value are satisfied.

In [17] Bisen et. al used Fuzzy Inference System (FIS) which performs the training and testing based on node characteristics values. The parameters are set to have some range in terms of low, good and best according to which a node is declared as normal or attacker.

In [18] Tiwari et al. modelled Sugeno Fuzzy Inference System to detect and isolate packet dropping attack. Simulation results from Qualnet simulator are taken as inputs and output for the FIS to determine nature of nodes.

In [19] Kumar et. al designed an Intrusion Detection Technique in order to detect packet dropping attack using fuzzy parameters extracted from network simulated in Qualnet simulator. If detected another module comes into picture which isolates the malicious node.

The point that is not highlighted by the researchers is that, intruder's detection rate is not stable with increase in the number of nodes. It causes overhead due to different classification techniques and requires additional parameters which causes overhead.

IV. Proposed Mechanism

Black hole attacks are the most widespread form of attack that an ad hoc network encounter. Basically, it does not provide the service to the required destination rather than getting an access and dropping the data. Thereby creating a hole in the network which causes denial and degradation. The proposed mechanism includes two phases in order to boost the pre-defined AODV, that is detection of black hole attack and route validation. The novelty of the proposed mechanism is that it not only creates a secure path but also validates its work using soft computing technique that is fuzzy logic. The role of the fuzzy logic acts as a decision maker which helps us knowing whether the network is secure or not.

Figure 5 shows the network flow for the proposed mechanism which shows the detection and validation are performed at source node 1.

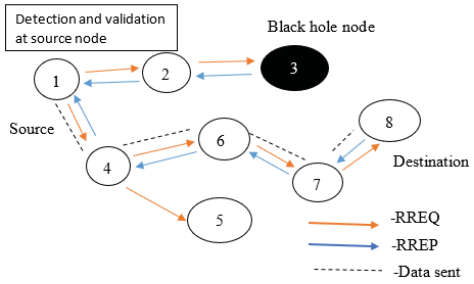

Figure 5: Enhanced Authenticated AODV

Figure 6 depicts the flow chart for the proposed mechanism which shows how the process of path formation takes place.

The first step in enhancing AODV is detection that is done based on delay parameter in order to check whether the reply is from legitimate or malicious node. So, per hop time for the RREQ packet is taken as a parameter to determine whether the RREP for the RREQ is real or fake. The assumption made here is that the malicious node upon receiving the RREQ does not perform any processing or queueing delays and directly sends a reply back to source claiming it to be the required destination. So, a threshold of about 3 secs is taken to check the nature of the node originating the RREP. The condition taken here is that if the time taken by RREQ per hop time is less than the defined threshold satisfied then node is assumed to be attacker.

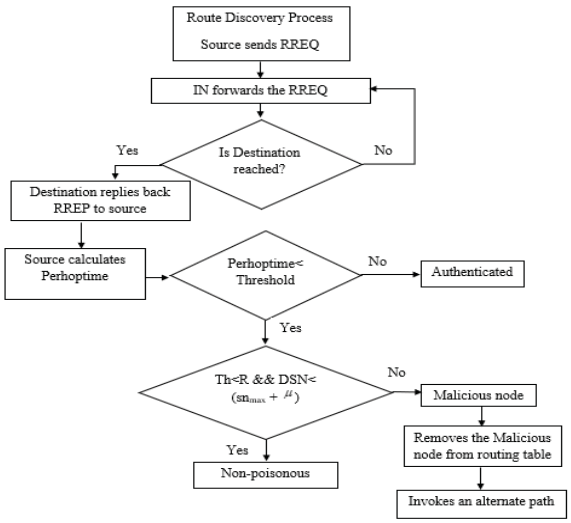

Figure 6: Flow chart for E-AODV

The validation is carried out so as to ensure the legitimacy of each node in the route by using parameters such as distance between the nodes, hop count and destination sequence number. First, it checks whether every two nodes in the path are within the range by calculating the distance between the node using the node coordinates. Secondly, it tests whether the Route Reply destination sequence number is valid or not. To do so it checks if the destination sequence number is less than the sum of maximum value of the sequence number in the routing table along with the count of data flows. If aforementioned conditions are fulfilled, then path is said to be legitimate else it has malicious node in it.

These additional mechanisms added to AODV enhances its performance by providing security to an insecure routing protocol. The conventional AODV does not check for the validity of the nodes across the path as well as the Sequence number of the RREP in comparison to the routing table and also the time taken in processing the RREQ, which makes it different from the proposal enhanced. The second part of the implementation of the proposal is modelling of a Fuzzy Inference System that determines whether the network is secure or not, based on three parameters extracted from the network simulator. The parameters taken as inputs to the Fuzzy Inference System are Packet Delivery Ratio, Overhead, Residual Energy, Drop and Packet Forwarding Ratio which are obtained from the trace files of the network simulator.

The FIS is modelled using these parameters as inputs, rules are defined in order to check whether the network is secure or not and finally concludes as secure which determines the results. The phases involved in developing a FIS and determining the nature of the network are as:

Step 1: Extracting Parameters from network simulator.

Step 2: Defining Variables

Input: Packet Delivery Ratio, Overhead, Residual Energy, Drop, Packet Forwarding Ratio.

Output: Secure.

Step 3: Defining Membership functions for the variables.

Gaussian membership function is employed.

$$y = gaussmf\,(x, params) \quad (1)$$

Equation 1 membership function value using gaussian membership function. Where x is the input and params is the mean and standard deviation. They are defined as:

Packet Delivery ratio: Good, Bad

Overhead, RE, Drop, PFR: Low, High

Step 4: Defining rules are in "IF…THEN" format.

Step 5: Simulate the results.

V. Result Analysis

The proposed mechanism described is simulated using NS-2.34 simulator and the comparative analysis with respect to existing approaches for different performances are plotted using x-graph [21]. The scenarios are modelled in the presence of black-hole nodes in the existing system, and compared with proposed mechanism. AODV routing protocol is enhanced to make it a secure routing protocol. The network environment is simulated in a 750 m× 750 m terrain size with random-way point as mobility model.

The two different scenarios defined for detection and avoidance using set destination tool is used for movement files in NS-2. The random traffic pattern for the environment is setup externally using CBRGEN for both the approaches. The outcomes of the implemented mechanism are evaluated with the basic AODV and valid route authentication as implemented in [13]. The results are compared with simulation end time and the number of active attackers.

Table 1:Simulation parameters along with their values

Parameters	Value
Simulator	Network Simulator-2.34
MAC	IEEE 802.11
Routing Protocol	AODV, VRA-AODV, EAAODV
Number of nodes	20
Attacker nodes	1 to 5
Speed	5ms
Queue	DropTail/PriQueue
Queue Length	150
Traffic Type	CBR
Propagation Model	Two Ray Ground
Mobility Model	Random-Way Point
Bandwidth	2.05 Mb
Packet size	512 bytes

Data rate	Val(att)*10 bps
Antenna	Omni Directional
Simulation time	25, 50, 75, 100
Simulation Area	750X750

The simulation parameters used are shown in Table 1. The simulation parameters are extracted from the definitions given in the TCL file. Two ray ground is selected to predict path losses between nodes

A. Delay

Delay is determined as the difference in time, the data packets take to move from source to destination it is measured in seconds.

$$Delay = D[t] - S[t] \quad (2)$$

Where D[t]=time at which data packets reaches the destination

S[t]= time at which data packet is sent by the source

Figure 7 shows the performance of delay when both detection and avoidance is applied with respect to change in simulation time.Here in EA-AODV the delay is about 0.02 sec whereas as for VRA-AODV[16] it is 44 secs and 42 secs for AODV. This shows high improvement in terms of delay compared to the existing protocols.

Figure 7: Delay v/s simulation end time

B. Delivery Ratio

Delivery ratio is defined as the ratio of successfully received data packets at destination to actually sent data packets by source.

$$Delivery\ Ratio = \frac{Number\ of\ successfully\ received\ packets}{number\ of\ sent\ data\ packets} \times 100 \quad (3)$$

Figure 8 and 9 shows performance when both techniques are applied with respect to change in attackers and simulation time. In both the figures it is analyzed that the delivery ratio is in the range 98 to 100.

In figure 8 the conventional AODV has maximum of 28% delivery ratio whereas the EA-AODV has maximum of 100%.

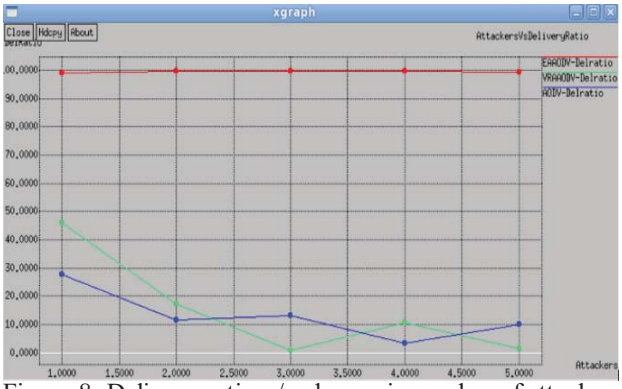

Figure 8: Delivery ratio v/s change in number of attackers

In figure 9 conventional AODV has maximum of 12% delivery ratio whereas the EA-AODV has 100%. The performance is increased with successful reception of data packets with both change in number of attackers and time.

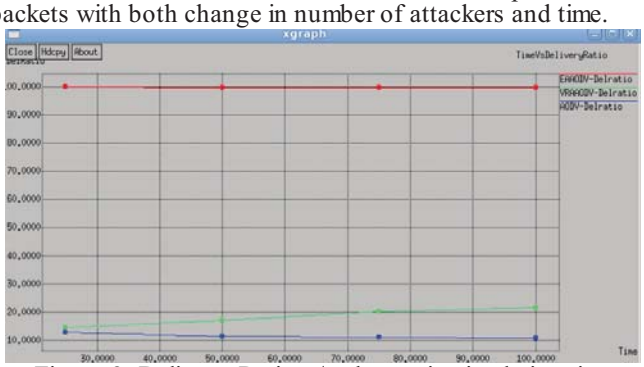

Figure 9: Delivery Ratio v/s change in simulation time

C. Drop

Drop is the difference between the number of successfully sent data packets and actual received data packets. It is measured in number of packets.

$$Drop = Number\ of\ data\ packets\ sent - Number\ of\ data\ packets\ received\ successfully \quad (4)$$

From Figure 10, it is extracted that the drop is nearly 0, whereas for existing protocols it is 5000 to 6000 with maximum attackers.

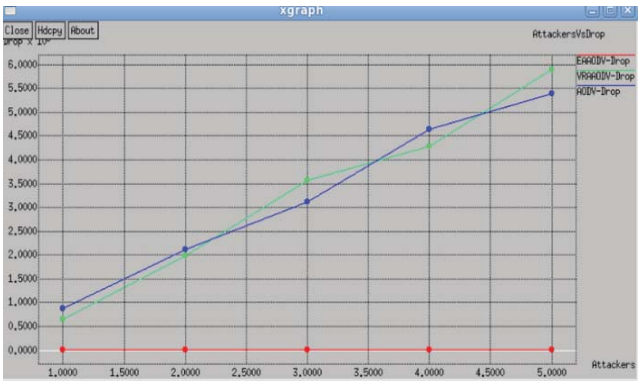

Figure 10: Drop v/s change in number of attackers

Figure 11 shows negligible drop for EA-AODV whereas for existing protocols it is 3500 to 4500. Both the results

shows that the drop has been sigificantly improved with the proposed mechanism.

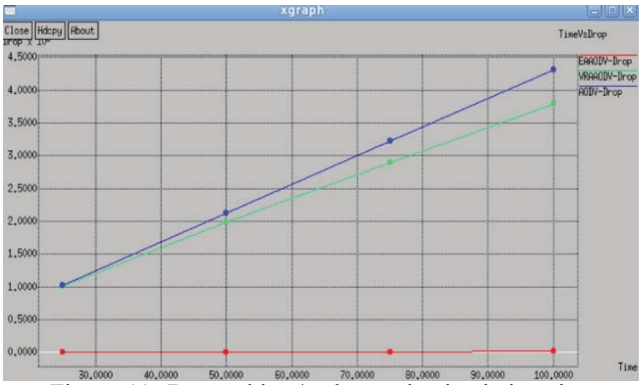

Figure 11: Drop with v/s change in simulation time

D. Overhead

Overhead is determined by the total number of routing packets to the number of received data packets. It is measured in number of packets.

$$Overhead = \frac{Number\ of\ routing\ packets}{Number\ of\ received\ data\ packets} \quad (5)$$

In Figure 12, it shows a maximum overhead of 9 packets for EA-AODV, 889 for VRA-AODV and 166 packets for AODV. Confirming a maximum overhead at VRA.

Figure 12: Overhead v/s change in number of attackers

In figure 13 it shows the number of overhead packets for AODV are 60, VRA-AODV are 40 and EA-AODV are 6. Overhead caused due to extra routing packets is decreased when compared to the existing protocols.

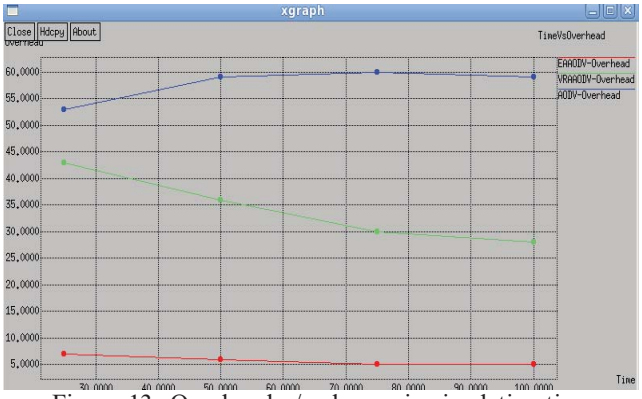

Figure 13: Overhead v/s change in simulation time

E. Throughput

Throughput is determined by the received data packets in an instant of time. It is measured in bits per sec(bps).

$$Throughput = \frac{Number\ of\ receive\ packets\ \times packet\ size}{Simulation\ time} \quad (6)$$

From figure 14 it is seen that for existing protocols the throughput is nearly 50 kbps whereas for the EA-AODV it is 300 kbps.From figure 15 analysis obtained is that throughput for AODV is nearly 40 kbps, VRA-AODV is above 80 kbps and EA-AODV is 260 kbps.

Throughput which determines the number of successfully received packets in particular time shows how the throughout is increased with number of attackers and simulation time.

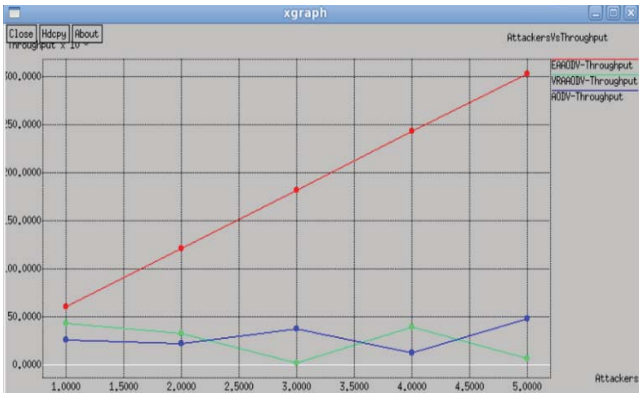

Figure 14: Throughput v/s change in number of attackers

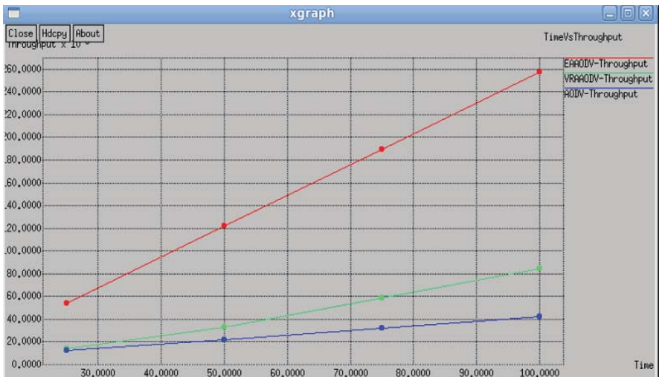

Figure 15: Throughput v/s change in simulation time

Throughput which determines the number of successfully received packets in particular time shows how the throughout is increased with number of attackers and simulation time.

F. Packet Forwarding Ratio

Packet Forwarding ratio determines the number total of received data packets to the total number of data packets forwarded without being subject to holding them back or dropping them.

$$Packet\ Forwarding\ Ratio = \frac{Number\ of\ received\ data\ packets}{Number\ of\ forwarded\ data\ packets} \quad (7)$$

From figure 16 it can be seen that with increase in number of attackers, Packet forwarding ratio decreases but for the EA-AODV it is maximum of 76% whereas for the VRA-AODV is 39.9% and AODV is 39.7.

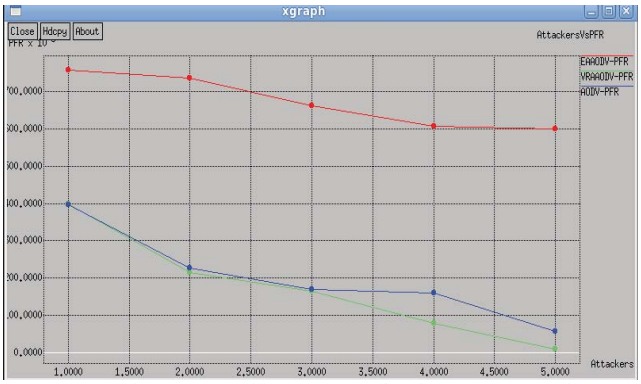

Figure 16: Packet Forwarding Ratio v/s change in simulation time

Figure 17: Packet Forwarding Ratio v/s change in simulation time

From figure 17, the interpretation is that by keeping attackers as 2 throughout the Packet forwarding ratio increases with an increase in simulation time. For EA-AODV maximum value is nearly 70%, VRA-AODV is 28.9% and AODV is 17.77%. Packet forwarding ratio shows how a node successfully forwards the packet when it receives them. The proposed mechanism shows increase in packet forwarding ratio when compared to the existing protocols.

The results obtained from the network simulator trace files are plotted using X-graph shows that the enhanced AODV is better in performance in terms of Delay, Delivery Ratio, Drop, Overhead, Throughput and Packet Forwarding Ratio as the security increases with enhancement. The enhancement to the existing protocol adds security to the insecure routing protocol.

The results are further justified using MatLab R2020a to give contrast between the secure and insecure routing protocol by simulating results on the modelled fuzzy inference system by giving a defuzzified value for the given inputs from the simulator.

Figure 18 takes the inputs [27.5,28,933,870,22.6] in a matrix form to get a defuzzified output for the network as 0.446 which shows that the network is insecure.

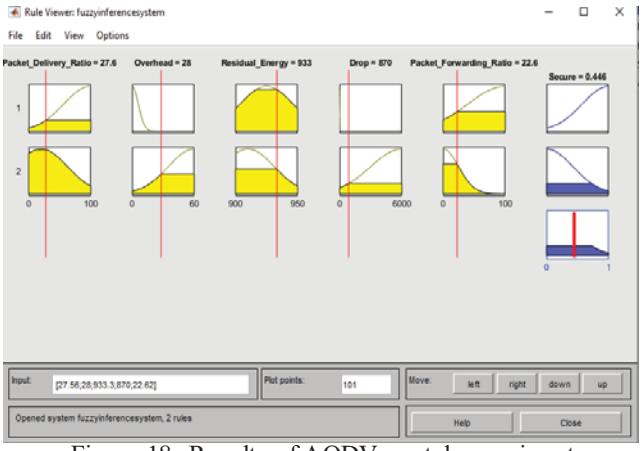

Figure 18: Results of AODV are taken as input

Figure 19 takes values from the enhanced-AODV trace file as input to the FIS as [100,6,942,6,59.9] in matrix form to get a defuzzified output with value as 0.635 which shows that the network is secure.

Figure 20 takes the inputs [99.2,6,940,6,66.2] in a matrix form to get a defuzzified output for the network as 0.635 which shows that the network is secure.

Figure 21 takes the inputs [99.8,5,926,6,75.8] in a matrix form to get a defuzzified output for the network as 0.65 which shows that the network is secure.

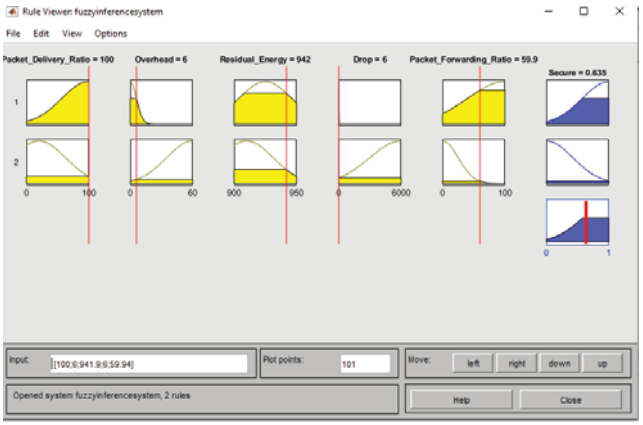

Figure 19: Results of Enhanced AODV are taken as Input

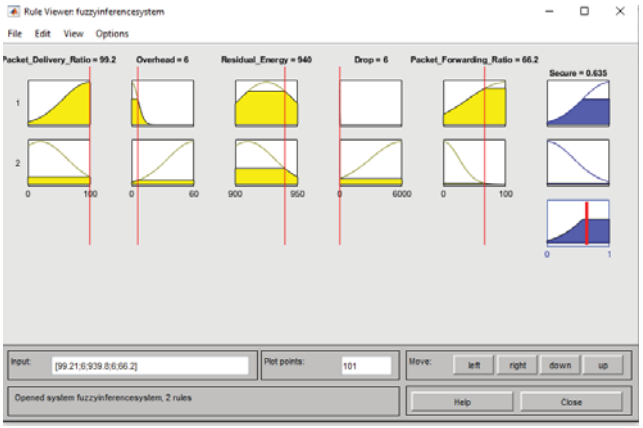

Figure 20: Results of Enhanced AODV are taken as Input

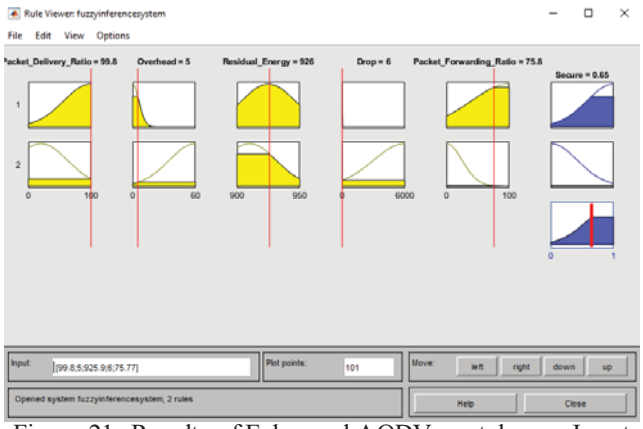

Figure 21: Results of Enhanced AODV are taken as Input

Hence it is seen that the modelled fuzzy inference system is capable of differentaiting whether the network is secure or not based on the input variables provided. The enhanced authenticated-AODV performs well with respect to various parameters which shows the the network is secure.

VI. Conclusion And Future Work

In this paper a new secure routing protocol which performs detection and avoidance of malicious node in MANET at source node is implemented. The Ad hoc On-demand Distance Vector protocol (AODV) is improved thereby adding security to it by creating a legitimate route with no malicious node. The mechanism mainly revolves around the per hop time of the RREQ packet along with the distance, hop count and RREP destination sequence number. The mechanism helps in obtaining legitimate path without any extra control packets and overhead caused due to it. The proposed mechanism compares the results with the one proposed by Vo TT et al. in [13] and existing AODV with varying time and number of attackers. It is evaluated from the outcomes that the implementation of the proposed Enhanced AODV is much better with increase in throughput, high packet Delivery Ratio, lower delay, less overhead, lower drop and high packet forwarding ratio compared to the existing ones. The simulation results are further justified using fuzzy inference system modelled to determine whether the network is secure or not. It increases the authentication of the defined mechanism by further validating it with the fuzzy system. The work can be further enhanced by detecting co-operative black-hole attack and using diverse parameters for delay so as to detect malicious activity and validate the same using fuzzy inference system.

References

[1] D. P. I. I. Ismail and M. H. F. Ja'afar, "Mobile ad hoc network overview," Asia-Pacific Conference on Applied Electromagnetics, Melaka, pp.1-8, 2007.
[2] https://en.wikipedia.org/wiki/Wireless_ad_hoc_network
[3] Tabatabaei, S., Behravesh, R., "New Approaches to Routing in Mobile Ad hoc Networks," Wireless Pers Commun 97, pp. 2167–2190 ,2017.
[4] S. Biswas, Neogy S. and T Nag "Trust based energy-efficient detection and avoidance of black hole attack to ensure secure routing in MANETs," Applications and Innovations in Mobile Computing (AIMoC), pp. 157-164, Kolkata, 2014.
[5] Perkins, C., Belding-Royer, E., & Das, S. "Ad hoc on-demand distance vector (AODV) routing" No. RFC 3561, 2003.
[6] Hadadi B, H. Moudni, M. Er-rouidi and H. Mouncif, "Performance analysis of Ad hoc On-Demand Distance Vector routing protocol in MANET under the influence of routing attacks," International Conference on Electrical and Information Technologies (ICEIT), Tangiers, pp. 536-542, 2016.
[7] M. N. Aydin, K. Tohma and A Turgut, "A realistic modelling of the sinkhole and black hole attacks in cluster-based Wireless Sensor Networks," International Journal of Electronics and Electrical Engineering, vol. 4, no. 1, pp. 74-78, February 2016.
[8] Dr. Bachala Sathyanarayana and Kondaiah R., "Trust-based GNF System for Intrusion Detection and SA-Firefly Integrated PSO Algorithm for Secure Routing in Mobile Ad-hoc Network," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8, pp. 5722-5735, 2018.
[9] Ahmed, Osman and A Hanan, "Description of Black Hole Attack Behaviour in Mobile Ad hoc Network," International Journal of Computer Networks and Communications Security, no. 12, pp. 322-329, 2016.
[10] Jaiswal, R., & Sharma, S. "A novel approach for detecting and eliminating cooperative blackhole attack using advanced DRI table in Ad hoc network" Proceedings of IEEE 3rd International Conference on Advance Computing (IACC), pp. 499–504,2013.
[11] B. Swadas and Raj, P. N., "DPR-AODV: A dynamic learning system against blackhole attack in Ad-hoc On-Demand Distance Vector based Mobile Ad-hoc Network," International Journal of Computer Science Issues, pp.54–59,2009.
[12] Y. Sekiya Y. Wakahara and Zhang X, "Proposal of a method to detect black hole attack in Mobile Ad hoc Network," International Symposium on Autonomous Decentralized Systems, pp. 1-6, 2009.
[13] S. A. Arunmozhi and Venkataramani Y., "Black-Hole Attack Detection and Performance Improvement in MANETs," Information Security Journal", Vol. 21, No. 3, pp. 150-158,2012.
[14] D. Kamlesh and K Sunil, "Intrusion detection technique for black hole attack in Mobile Ad-hoc Networks," International Journal of Information Privacy, Security & Integrity, Vol. 2, No. 2, pp.81–101,2015.
[15] A. Kush, Verma, Deepak Jain and Renu, "Intrusion detection using Route Reply messages of Ad-Hoc On-demand Distance Vector routing protocol," International Journal of Applied Engineering Research, pp. 1956-1961,2017.
[16] Vo TT, Luong TN," VRA-AODV: Routing protocol detects Blackhole and Grayhole attacks in Mobile Ad hoc Network," Journal of Computers, pp. 222-236, 2018.
[17] Dhanjay Bisen and Sanjeev Sharma, "Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET", Springer, National Academy Science Letters, Vol. 41, pp 1-6,2017.
[18] K. Anil, C. Alka, and Tiwari N., "Design an anomaly-based fuzzy-IDS for packet dropping attack in MANETs", IEEE International Advance Computing Conference, pp. 256-261,2014.
[19] A. Chaudhary, V. Tiwari, and A. Kumar, "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in Mobile Ad-hoc Networks", International Conference on Reliability Optimization and Information Technology, pp. 178-181,2014.
[20] Fahmina T et al., ""Detection and Interception of Black hole attack with Justification using Anomaly based Intrusion detection system in MANETs", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S11, September 2019, Pg. No. 2392-2398
[21] Fahmina T et al.," Detection and prevention of black hole attack using Dymo in Manets", Journal of Mobile Computing, Communications & Mobile Networks, Vol 5, No.2, September 2018, Pg. No. 9-16
[22] Fahmina T et al. Proposals on Network Layer Attacks and Their Mitigation Strategies on MANET, International Journal of Recent Technology and Engineering, ISSN: 2277-3878, Volume-7, Issue-6S, March 2019, Pg. No. 16-21