ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

# Design and Analysis of Fuzzy Based Wormhole Detection in MANET

[1] Abhijit Ghanshyam Raut [2] D. Vydeki
[1] M.tech (VIT University, Chennai, India) [2] Associate Professor (VIT University, Chennai, India)

***Abstract:*--Currently, wireless communication is becoming a major part of our day today life. Due to immense growth in the turf of wireless communications, different types of wireless networks such as Vehicular Ad-Hoc Networks (VANET), Mobile Ad-Hoc Networks (MANET) play a key role in communication systems. MANETs are the ones having free mobile nodes which can traverse throughout the system and can be a host, furthermore a router for transmitting /forwarding data packets to the distant node. As this system lacks centralized coordinator and is a self-organized, self-healing network without infrastructure, their adaptive nature and frequently changing topology it is more likely endangered to different security attacks such as black hole attack, wormhole attack etc. This paper emphases on providing a solution for secure transmission through the network. In this paper, we aimed at detecting wormhole attack in MANET using Fuzzy Inference System. As it is one of the dangerous active attacks on the network layer of MANET, in which data packet can get lost or replayed within the system by the wormhole nodes which can be more than a pair and are situated at different points within the system. To detect the wormhole nodes in the system, we have measured parameters such as No. of dropped packets, Reply packets, Forwarded packets to collect the data for analysis. The key objective of our paper is to detect the presence of wormhole attack in MANET. This is done by proposing soft computing algorithms such as Fuzzy Inference System (FIS). The suggested algorithm identifies wormhole nodes based on the above parameters.**

***Keywords*:--MANET, Wormhole attack, AODV protocol, Soft computing algorithms.**

## I. INTRODUCTION

Over the past few years, due to the expeditious growth in the telecommunication sector, wireless networks have developed rapidly. Wireless networks have various benefits w.r.t wired networks. Mobility and ease of deployment have been the two largest attractions of wireless communications. Especially Mobile Ad-Hoc Networks (MANET) have become an important area of research these days. It is a supportive engagement of gathering of mobile nodes without any requirement of the centralized access point or existing infrastructure. The term Ad-Hoc means that there is no permanent infrastructure for forwarding/routing packets. As there is no source, every node is responsible for the reliability of the network. Least configuration and rapid deployment make Ad-Hoc networks useful for various applications. It has applications in different networking environments such as personal area networking, military environments, civil environments, emergency operations.

Even though MANET is believed as a robust and scalable network infrastructure, due to its dynamic changing topology, lack of central authority, shared radio channel, rapid node mobility and limited accessibility of resources, it has numerous concerns in several areas such as security, confidentiality, integrity, resilience etc. Among various types of attacks, a wormhole attack is one of the dangerous and most specific types of attack. It has one or more malicious nodes and a tunnel between them. In this, the attacker node seizes the packet from one location and tunnels it to further distantly located node which distributes them nearby. The tunnel is either a wired connection or high-frequency linkage which creates misapprehension that the two ends of the tunnel are close to each other. It can fake a route which is shorter than the original route within the network. It can replay, a loose data packet which may affect route performance in different ways degrading the network's performance. Its mechanism is shown in Fig.1.

***Wormhole attack can be propelled using several modes:***

1. Wormhole using Encapsulation: In Encapsulation mode, one pernicious hub sends the RREQ packet to another conspiring hub at a far off position in the system. This second plotting hub retransmits the RREQ packet. The neighbor hubs of second conniving hub get the RREQ and drop any extra authentic demand that may come later on veritable multihop ways. This outcome in framing wormhole burrow from source to goal through the conspiring hubs.

2. Wormhole using Out of Band Channel: In this sort, the opponents will associate his hubs with broad range quick associations and this can be either a long range remote connection with various radio frequencies or a quickly wired connection. These are best in class and harming in light of the fact that the more extended and speedier the wormhole, the activity can be sent through more hubs pulled into it and the more harm and interruption can happen to the system.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

3. Wormhole using High Transmission: In this sort, when a specific conniving hub gets an RREQ, it transmits the demand at a higher power level, a capacity which is inaccessible to different hubs in the system. Whichever hub that reacts to the powerful communicate, it rebroadcasts it towards goal. It increments pernicious hubs in the ways from source to goal even without conspiring hub's interest.

4. Wormhole using Packet Relay: This type can be propelled by the even single malicious node. In which a colluding node relays packets between two far away nodes to prove them that they are neighbors. Cooperation by a higher no. of colluding nodes helps to expand the neighbor list of a target node to several hops.

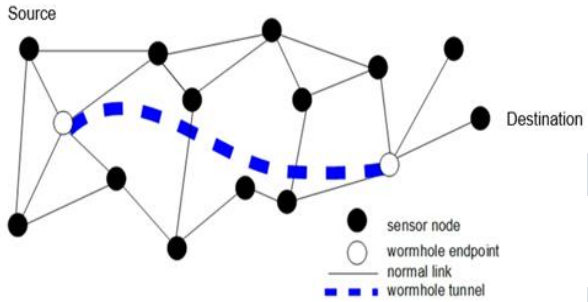


***Fig.1. Wormhole attack mechanism in MANET***

## II. RELATED WORKS

1. Time and Location Based Approach: Authors of [1], proposed a universal method of parcel chains, geographic and temporal - to recognize wormhole attack presented. In geographic chains, hub area data is utilized to tie the separation a parcel can cross. Since wormhole attacks can influence restriction, the area data must be acquired through an out-of-band component, for example, GPS. Promote, the "lawful" separation a parcel can cross is not generally simple to decide. In any case, in worldly rope, to a great degree exact universally synchronized timekeepers are utilized to tie the spread time of bundles that could be difficult to acquire especially in ease sensor equipment. Be that as it may, notwithstanding when accessible, such planning examination will most likely be unable to distinguish physical layer wormhole occurrences. In this manner, Wormhole attack is distinguished by identifying the crisscross between the time stamp contrasts figured and area distinction retained.
2. Connectivity-Based Approach: In [2], a compelling technique entitled WAP (Wormhole Attack Prevention), which is a diagrammatic theoretical system for demonstrating wormhole connections and inferring the essential and adequate circumstances for recognizing then safeguarding contrary to wormhole attacks was introduced. This arrangement ought to build a correspondence chart that scope of the system hubs. When wormhole hub is recognized, the source hub records them in a wormhole hub list. In any case, the proposed technique depends on end-to-end signature verification of steering packets, subsequently, they could bring about huge overhead and lacks exact contrasted with those methodologies. These systems shielding MANETs from future wormhole attack from a similar hub.
3. Statistics Based Approach: DelPHI tradition focuses on the deferrals in light of different courses to a beneficiary. Thus, a sender can check whether there are any harmful center points sitting along its approaches to a recipient endeavoring to dispatch wormhole ambushes. The procured deferrals and curtsy check information of certain split ways are used to pick whether a particular path midst these disjoint courses is under a wormhole ambush. In any case, it can't pinpoint the zone of a wormhole. Furthermore, in light of the way that every center point, including wormhole centers, changes the lengths of the courses, wormhole centers can change the course length, particularly with the objective that they can't be distinguished. [3]
4. Mix-mode Approach: The investigators have proposed an approach called RTT-TC that relies on upon topological relationships (accessibility) and round trek time estimations. They have used the AODV coordinating tradition. In this system, a neighbor list contains two pieces: Trusted and Suspected center points. They used RTT estimations remembering the ultimate objective to get the assume list, then use the topological examination procedure to find veritable neighbors from the hypothesized list. Really, this approach has a high acknowledgment rate and does not require any clock synchronization or excellent contraptions yet rather has high message overhead.[4]

## III. PROPOSED ALGORITHM

This paper put forwards a mechanism to provide wormhole free path from source to destination. For that simulation of various scenarios with a varying number of nodes and wormhole nodes is done. To analyze the change in the behavior of the network, we have inserted wormholes in the network and then simulated different scenarios. After

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

these simulations, the generated data is taken into Fuzzy Inference System (FIS) through Matlab. Fuzzy Inference System is the one in which output is generated on mapping the fuzzy input sets. Here we have used credit based allocation system in which initially a credit is given and it is incremented if the value at a node for a particular parameter is greater than the threshold value, otherwise credit assigned will be zero. The final credit (FC) of every node is calculated as the sum of the individual parameter credits. All the parameter values and the final credit values of all the nodes form the input data set. In this research work, Sugeno method of FIS is used as it has excellent computational efficiency also it works fine with optimization plus adaptive techniques. The 'genfis2' function in Matlab generates an FIS using the clustered input and related membership functions. Subtractive clustering is used in a genfis2 function to provide a fast, one-pass method to take input-output training data and generate a Sugeno-type fuzzy inference system that models the data behavior. The FIS applies the various fuzzy 'if-then' rules appropriately on data set, created on the input and credit values, and generated standard deviation (STD) which is used to tell how measurements for a group are spread out from the average and produces results as the defuzzified output for each node as shown in Fig.2.

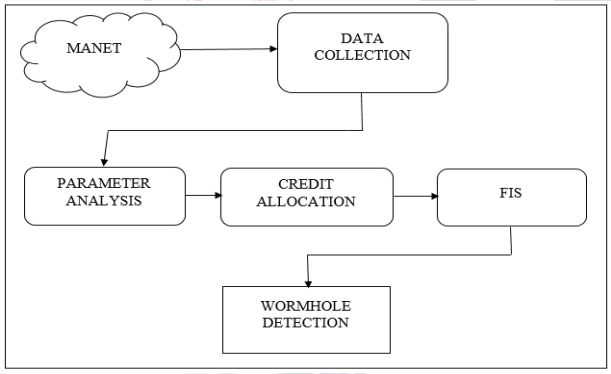


*Fig.2. Flow diagram of detection system using FIS*

## IV. METHODOLOGY FOR EVALUATION

1. Simulation Environment: For the simulations, we use NS-2 (v-2.35) network simulator. NS-2 provides realistic implementations of various network protocols. The execution of the protocol has been carried out using C++ language in the backend and tcl language in the frontend on the Ubuntu Linux 15.10 operating system. The IEEE 802.11 algorithm has been used at the physical and data link layer. Two Ray Ground radio propagation model is used with the wireless channel. AODV routing protocol is used at the network layer. UDP is used at the transport layer. Entire data packets are CBR (continuous bit rate) packets. The size of the packet is 1024 bytes. The communication range for normal nodes is 250 m while for wormhole attackers it is 1500 m. The antenna type used Omni antenna. The packets transmission rate is 1 Mbps. The terrain area is 1000m × 1000m with 25, 50, 75 and 100 nodes. Such networks with varying traffic intensities are simulated. With increasing traffic conditions, we have also increased a number of wormhole pairs for different networks. For each network size, 3 scenarios are replicated with varying traffic intensities and a varying number of wormhole nodes. The simulation duration is 50sec.
2. Metrics used for Simulation: To evaluate the potential of our proposed solution, various scenarios are created by varying the no. of nodes and wormhole nodes. In these simulations we evaluated the following metrics:
   a. **No. of Dropped Packets-** Number of data packets dropped by each mobile node.
   b. **No. of Reply Packets-** Number of route reply packets (RREP) sent by each node.
   c. **No. of Forwarded Packets-** Number of route request packets (RREQ) forwarded by each node.

   Table 1 gives the various simulation scenarios. It can be realized from table 1 that four different MANETs are simulated, each with a different number of wormhole nodes and various traffic intensities. The analysis parameters mentioned above are extracted from these simulated networks.

***Table 1. Values for Simulated Network***

| Network Size | Wormhole Nodes | Traffic Intensity |
|---|---|---|
| 25 | 4 (2 Pairs) | 3 Flows |
| 50 | 6 (3 Pairs) | 5 Flows |
| 75 | 6 (3 Pairs) | 7 Flows |
| 100 | 8 (4 Pairs) | 10 Flows |

## V. RESULTS AND DISCUSSIONS

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Figures (3), (4) and (5) are the outputs of FIS generated in Matlab for different no. of nodes and the wormhole nodes associated with it. The spikes below the STD value indicates the node number of wormholes. The output of one scenario for different no. of nodes is shown.

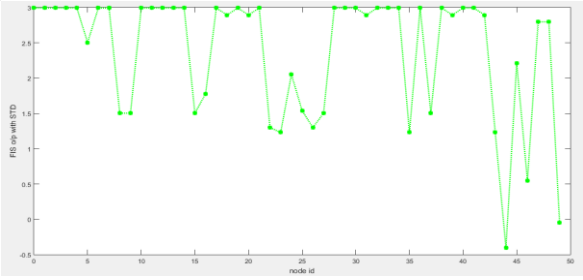

*Fig.3. Detection output generated using FIS (50 nodes)*

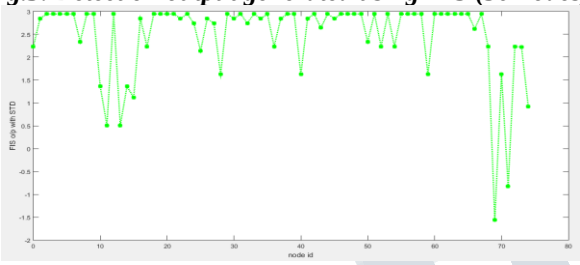

*Fig.4. Detection output generated using FIS (75 nodes)*

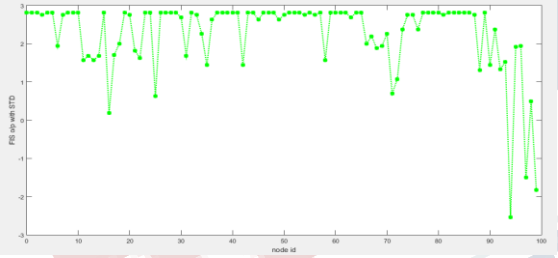

*Fig.5. Detection output generated using FIS (100 nodes*)

We have carried out performance analysis of the projected scheme. The accuracy is computed in terms of two parameters as:

1. True Positive Rate (TPR) - is the amount of the number of wormhole nodes correctly identified.
2. False Positive Rate (FPR) - is the amount of the number of normal nodes identified as malicious nodes.

The computation of these parameters is carried out, using equations (1), (2).

$$TPR = \frac{TP}{\text{Total no. of wormhole nodes}} \quad (1)$$

$$FPR = \frac{FP}{\text{Total no. of non-wormhole nodes}} \quad (2)$$

Where TP = no. of true positives
FP = no. of false positives

On the basis of these parameters, a chart is prepared showing average values of TPR and FPR for different network scenarios as seen in Fig.6.

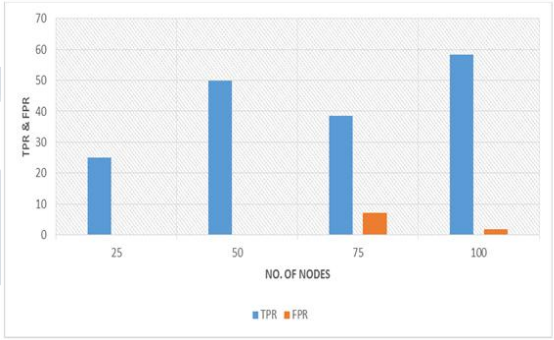


*Fig.6. Performance analysis using TPR and FPR*

## VI. CONCLUSION AND FUTURE WORK

This paper analyzed from a set of simulated MANETs, the different parameters such as the number of dropped packets, the number of reply packets, and the number of forwarded packets for every node. By checking the anomalies in the extracted data the wormhole nodes are detected. A credit allocation scheme improves the decision-making process. The extracted data set and the corresponding credit values are given as input to the FIS, where detection of wormhole nodes can be done efficiently. The performance analysis is carried out based on the detection process. The results show that an average FPR of 2.235 and TPR of 42.5. Moreover, the FPR value goes on increasing with a number of nodes in the network. The accuracy of the detection system can be increased to lower the FPR using other soft computing techniques.

## REFERENCES

1) Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless

networks", INFOCOM 2003. Twenty- …, vol. 00, no. C, 2003.

2) S. Choi, D. Kim, D. Lee, and J. Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", 2008 IEEE Int. Conf. Sens. Networks, Ubiquitous, Trust. *Comput. (sutc 2008)*, pp. 343–348, Jun. 2008.

3) H. Chiu and K. Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks", Wirel. Pervasive Comput. 2006 1st …, no. 852, 2006.

4) M. R. Alam and K. S. Chan, "RTT-TC: A topological comparison based method to detect wormhole attacks in MANET", Int. Conf. Commun. Technol. Proceedings, ICCT, pp. 991–994, 2010.Tutorial on Network Simulator v2.35.

5) Anal Patel, Nimisha Patel, Rajan Patel, "Defending Against Wormhole Attack in MANET", 2015 Fifth International Conference on Communication Systems and Network Technologies.

6) S.Nivedha, S.Sankara Narayanan, "Detection and Prevention Of Wormhole Attack In MANET Using New Fresh Algorithm", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015.

7) Vikas Kumar Upadhyay, Rajesh K ShukJa, Rajshree Dubey, "Detection And Prevention Of Wormholes In Mobile Ad-Hoc Networks Using Hybrid Methodology", 978-1-4799-3064-7/14/$31. 00©20 14 IEEE.