Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs

P.S.Hiremath
Dept of Computer Science (MCA),
KLE Technological University,
BVBCET, Hubballi-580031, India
hiremathps53@yahoo.com

Anuradha T
Dept of Computer Science and Engg,
PDA College of Engg
Kalaburagi, India
anuradhat26@gmail.com

Prakash Pattan
Dept of Computer Science and Engg,
PDA College of Engg
Kalaburagi, India
prakashpattan@gmail.com

***Abstract* — A MANET (mobile adhoc network) is a group of computing nodes or cell or other devices used for communication which are capable of communication among each other with no support of an infrastructure that is fixed. MANET in fact is self-sufficient group of cellular consumers which talk to each other with the help of cellular nodes, described by certain wireless links. In these applications, in order to offer quality services for MANETs, many routing protocols have been designed. In this paper, a novel method that detects and prevents the supportive black hole attack on MANETs is developed. The proposed method is based on adaptive fuzzy inference system for MANET in order to detect and prevent the cooperative black hole attack. The popular protocol utilized in MANET is on-demand distance vector (AODV) protocol, and is simulated using NS2. The simulated results of the proposed method are compared with that of an adaptive method [17], wherein source node checks all nodes activity by using DAT table that maintains from-node-to-next-node's information and declares black hole node by channel overhearing method. It is observed that the proposed method based on adaptive fuzzy logic system shows better performance as compared to adaptive method in terms of throughput, end-to-end delay and packet delivery ratio.**

Keywords— MANET; NS2 simulator; AODV routing protocol; adaptive fuzzy logic system; cooperative black hole attack.

I.INTRODUCTION

A MANET (mobile adhoc network) is an arbitrary set of nodes which are mobile and are able to communicate with one another wirelessly devoid of any centralized coordinator. Therefore, the function of a node is not only to work as a host, but also serves as a router. An adhoc routing protocol is utilized in order to set the routes and their maintenance there upon. MANETs have many diverse practical applications such as nature disaster areas, emergency operations, battlefield communication, campus networks, fleet in oceans, vehicular communication, etc. [1],[2]. The protocol creates the routes on demand basis and also removes the routes when nodes move away from accessible range. The main aim of the protocol is routing, which is designed to build and maintain a table of routes' information. For MANETs, several routing protocols have been developed. One of the key issues is routing among extremely active as well as widespread mobile nodes of MANET. The MANETs are free of infrastructures, self managing and quickly installable networks which are wireless. Thus, the security issue is a major concern in such networks, which necessitates the routing protocol to deal with attacks of certain types. One of the security attack is a black hole, which is an active attack and considered as an attack of high severity in MANET. By transmitting wrong information about routing to the victim nodes, this attack is generated in the nodes of routing tables to give rise to bogus route entries. In this way, black hole manages to absorb packets of data that were meant to be forwarded to destination. Hence, packets of data are dropped in the network, thereby affecting the network's performance. In this paper, the objective is to study black hole attack's effects in a MANET considering AODV routing protocol as specimen protocol.

The AODV protocol [3] is utilized when the end-to-end communication lacks an authentic dynamic route among nodes. The mobile nodes interchange the packets while routing among them whenever they want to. In this process, nodes maintain the routing table for all routes including routing information about short-lived routes. Nodes uphold a "precursor list" containing internet protocol address of all its neighbors which are most probable to utilize it for an upcoming hop in the table for routing. In order to work in a network, the protocol is designed in such a way that all nodes show high degree of trust among each other. AODV therefore allows active and self-governing, multiple hoping route in between cellular nodes in order to establish and uphold an adhoc network. AODV also facilitates the route construction and generally no node is required to keep the routes while not being in a dynamic communication.

The rest of the paper is organized as following: The discussion on black hole attacks is given in the Section II, the related work in the Section III and the proposed work in the Section IV. In the Section V, the simulation experimental

978-1-5090-1987-8/16/$31.00 ©2016 IEEE

outcomes along with the analysis of performance are presented. The conclusions are given in the Section VI.

The operation of networks by modifying the data or misrouting the data, whereas a passive attack does not alter the operation of data. The malicious router can also accomplish this attack selectively, by dropping packets for particular network destination. Black hole attack occurs through malicious node, which acts as a liar node in the network. This node always pretends as having fresh route to the destination. A packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. Because packets are routinely dropped from a loss network, the packet drop attack is very hard to detect and prevent. In the Fig. 1, the node X3 is a source node, wants to send data packet to destination and initiates the route discovery process. Additionally, X1 and X5 are the neighboring nodes. When source node sends RREQ packet, X1 node replies immediately with RREP packet to source node X3. In case, the response from the node X1 reaches to node X3 at the earliest, then source node ignores all other RREPs and starts to send data packets to X1 which absorbs all packets from X3 or loses; finally X1 becomes a black hole. However, if the malicious router begins dropping packets on a specific time period or over every n packet, it is often harder to detect because some traffic still flows across the network. Over a mobile adhoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

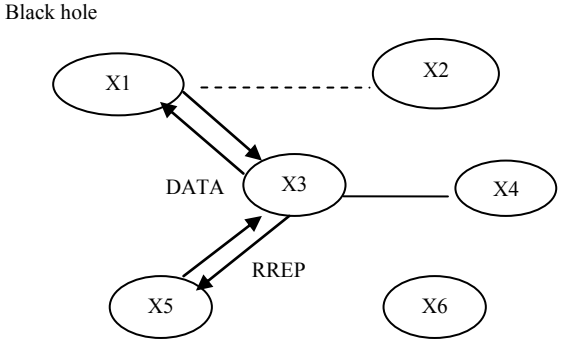

Fig.1 Black hole attack

A. Cooperative black hole attack

One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. One of the most widely used routing protocols in MANETs is the ad hoc on-demand distance vector (AODV)

II. BLACK HOLE ATTACK

In MANETs, attacks can be classified into two types, namely, active attacks and passive attacks. An active attack disturb routing protocol. It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well-known black hole attack.

III. RELATED WORK

There are many works reported in literature related to detection and prevention of single black hole attack, but very few works have been reported which have used natural reasoning system that uses fuzzy logic. In [4], the authors have attempted for black hole attack detection in MANET utilizing the fuzzy logic by using two factors: packet loss rate and data rate. The authors in [5] have improved the detection rate of IDS using fuzzy data mining technique for implementing fuzzy rules to detect anomaly and misuse type of attacks. The fuzzy based priority scheduler is developed in [6] and its performance is tested with multicast protocols in terms of quantitative metrics, namely, packet delivery ratio and end to end delay. The fuzzy logic based trusted AODV routing protocol is proposed in [7] and demonstrated that its performance is better than AODV in terms of routing overhead ratio, throughput, latency and packet loss. In [8], FL_TCP protocol is proposed, which shows improved performance compared to other TCP variants in terms of two factors ,namely, expected throughput and actual throughput. In MANETs, the mechanism for defending against a cooperative black hole attack is designed by making use of data routing information (DRI) and cross checking [9]. Fuzzy clustering algorithm is proposed in [10], that achieves much optimized energy consumption of network by reducing the number of re-election of cluster heads (CH) and also reducing the number of re-affiliation of nodes and selecting the best node as CH among current members of each cluster. The intrusion detection system (IDS) based on fuzzy logic to identify the malicious behaviour and the attack by a node is proposed in [11]. The new protocol based on AFTE (Adaptive Fuzzy Threshold Energy) for MANETs is designed in [12] and compared with its earlier work on LAEE (Load Aware Energy Efficient Protocol), which saves the mobile nodes energy and also improves the MANET's life time. Elimination of cooperative black hole and gray hole attacks using modified extended data routing information (EDRI) table in MANETs is discussed in [13]. Anomaly based fuzzy intrusion detection system for detecting packet dropping attack in MANETs is designed in [14], using sugeno-type fuzzy inference system and simulated by qualnet simulator 6.1 to analyze the results. In [15],[16], the authors have proposed detection of network attacks using fuzzy logic based on characteristics of different network anomalies, such as ratio of incoming traffic to outgoing traffic, packet size, etc. Every type of menace is characterized by a vector of fuzzy values describing the network state. A novel method called adaptive method for detection and prevention of cooperative black hole attack is proposed in [17], wherein source checks all nodes activity by using data access table (DAT) to maintain from

node to next node's information and declares black hole node by channel overhearing method. Performance comparison for threshold as well as cluster based methods to identify and avoid the cooperative black hole attack is proposed in [18] and the results of threshold based approach indicate better performance when compared with cluster based approach. The impact of black hole attack on network performance is simulated and analyzed in terms of metrics, namely, packet delivery ratio, normalized routing overhead and average end-to-end delay in [19]. The aforesaid literature survey reveals that the detection and prevention of cooperative black hole attack in a MANET needs to be addressed more effectively by an adaptive strategy incorporating fuzzy logic. The aim of the proposed method is primarily to detect and prevent cooperative black hole attack on the basis of a system of adaptive fuzzy inference making use of a fuzzy rule base. The fuzzy inference made by a node is capable of representing and processing imprecise or incomplete information about its neighboring nodes and then decide to which node data packets be transferred.

IV.PROPOSED METHODOLOGY

The proposed methodology employs an adaptive system of fuzzy inference to detect and prevent the black hole attack; the system of fuzzy logic is indeed an extension of logic to multivaluedness of state variables. In a MANET, it is assumed that each node maintains forward buffer and all nodes listen channel and read the content with capability of overhearing. Each node exchanges hello message to update neighbor information, by sending each time periodically data rate, data loss, trust value and energy along with hello message. While receiving hello packet from neighbor, it updates neighbor's all information. Each node shares the data with neighbors. Malicious node will not share the data. During the route establishment phase, each node maintains routing table to update current path, forward_ packet buffer to store the data packet forwarding count, DAT to maintain each from node and to node data report, reliable_node_list to verify node entry, if not, store it in DAT as unreliable, blacklist to remove further communication of black hole node from network. When source node receives data packet, it verifies its routing table to check destination towards next hop neighbor. While selecting next hop neighbor, a system of fuzzy interference is employed.

A. Fuzzy inference system (FIS)

The Fuzzy inference system (FIS) is a logical reasoning system. The FIS is capable of extracting a useful decision out of a given limited amount of raw data. The FIS is successfully applied in various problems, wherein there is demand for human like decision system to be adopted. There are two models of FIS, namely, Sugeno and Mamdani model [15]. It is expected in Mamdani model that the functions of output membership are the fuzzy sets. On the other hand, the Sugeno model expects the linear or constant output membership functions. In the proposed method, Sugeno model is employed, since the nature of problem in hand expects a constant output for a set of inputs. The Fig.2 depicts the proposed fuzzy inference system (FIS), which is configured with four input linguistic variables, namely, trust, data loss, data rate and energy that characterize the quality of next hop neighborhood. The impreciseness and lack of certainty similar to human reasoning can be handled easily by applying the fuzzy logic [15].

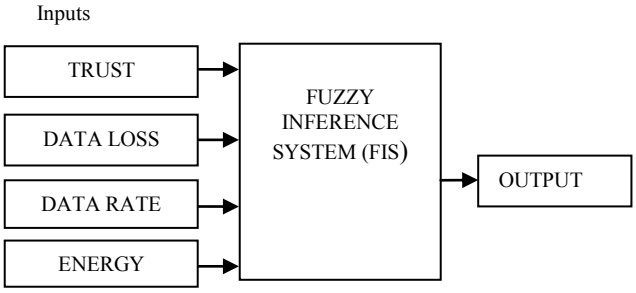

Fig.2. Fuzzy inference system (FIS)

The rules of fuzzy interference system are described below:

The linguistic hedges for the four input variables are: HIGH, MEDIUM, LOW, with the weights as defined in the Table I. Some sample if-then rules used in the fuzzy inference system are given below and the entire set of rules is given in the Table II.

Rule 1: IF (DATA_RATE = = MEDIUM AND LOSS = = HIGH AND ENERGY == LOW AND TRUST = = LOW) THEN OUTPUT=LOW.
Rule 2: IF (DATA_RATE = = MEDIUM AND LOSS = = LOW AND ENERGY = =HIGH AND TRUST = = HIGH) THEN OUTPUT=HIGH.
Rule 3: IF (DATA_RATE = = MEDIUM AND LOSS = = MEDIUM AND ENERGY = =LOW AND TRUST = = MEDIUM) THEN OUTPUT=MEDIUM.

.

Table I. LINGUISTIC VARIABLES AND VALUES FOR INPUT PARAMETERS

Input parameters	**Linguistic variables**	**Weights defined for linguistic variables**	**Type of membership functions used in proposed FIS**
Data Loss	LOW,MEDIUM, HIGH	LOW=0 to 0.3	Gaussian membership functions for all inputs. Output function is a constant membership function.
Data Rate	LOW,MEDIUM,HIGH	MEDIUM=0.3 to 0.6	
Energy	LOW,MEDIUM,HIGH	HIGH=0.6 to 1	
Trust	LOW,MEDIUM,HIGH		

B.Working procedure for detection and prevention of black hole attack

Select maximum resource next hop and update routing table to send data packet. If not, start route request and remove previous routing table. Black hole node has less resource so that the routing table is updated without black hole as next hop. Each intermediate node rebroadcasts and destination

Table II. FUZZY RULES TABLE

Data Loss	**Data Rate**	**Energy**	**Trust**	**Output(choosing next hop)**
MEDIUM	LOW	MEDIUM	LOW	LOW=Min_Resource_Nexthop
HIGH	HIGH	HIGH	HIGH	HIGH=Max_Resource_Nexthop
MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM=Avg_Resource_Nexthop
HIGH	LOW	LOW	LOW	LOW=Min_Resource_Nexthop
LOW	HIGH	MEDIUM	HIGH	HIGH=Max_Resource_Nexthop
LOW	LOW	LOW	LOW	LOW=Min_Resource_Nexthop
MEDIUM	MEDIUM	LOW	HIGH	MEDIUM=Avg_Resource_Nexthop
HIGH	MEDIUM	HIGH	LOW	HIGH=Max_Resource_Nexthop
MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM=Avg_Resource_Nexthop
LOW	MEDIUM	HIGH	MEDIUM	LOW=Min_Resource_Nexthop
HIGH	HIGH	HIGH	MEDIUM	HIGH=Max_Resource_Nexthop
LOW	HIGH	LOW	HIGH	MEDIUM=Avg_Resource_Nexthop

receives RREQ and sends RREP with each node next hop and data forwarding entry. Source collects RREP and verifies with its DAT for reliability. If node entry is available , update reliable list. If already route entry is available in DAT, source starts to send the packet in that route, else if for any node entry is not available it starts verification message with timer for reply of that verification about that intermediate node via another neighbor. If next neighbor has the record of forwarding any packet via that intermediate node and if neighbor node also does not have any entry to forwarding the packet via that intermediate node, then receive count and forward count will be 0 in both from node and to node. If source is not getting response within timer or has received verification reply with 0 values, then source rejects all nodes in the path and choose next path to forward data. If black hole is not available, then route is secure, else start black hole announcement as broadcast to all the concerned nodes in the network. Receiving node updates node entry in black list and rejects further communication from their respective node. The above process is presented in algorithmic form as following:

Algorithm:

Step 1: Let N be no. of nodes and x be the no. of black hole nodes. Suppose S is the Source node. Let DAT [17] be the array, which is a Boolean Variable used for routing.

Step 2: Input the values of N and x.

Step 3: Randomly assign x% nodes as black hole nodes among N nodes.

Step 4: The route discovery is initiated by S by propagation of the fake packet of RREQ with wrong destination address to black hole node.

Step 5: S receives data packet verifies its routing table to check destination towards next hop neighbor. While selecting next hop neighbor, apply fuzzy inference system to handle the nodes. The fuzzy scheduler applies fuzzy rule to compute and choose best next hop node based on exchanged Hello packet embedded with parameters as data rate, packet loss, energy and trust of respective node.

Step 6: Select maximum resource next hop and update routing table to send data packet. If not, start RREQ and remove previous routing table. Black hole node has less resource so that the routing table is updated without black hole as next hop.

Step 7: Each intermediate node rebroadcasts and destination receives RREQ and sends RREP with each node next hop and data forwarding entry. Source collects RREP and verifies with its DAT for reliability. If node entry is available, update reliable list. If already Route entry available in DAT, source starts to send the packet in that route, else if any node entry is not available it starts verification message with timer for reply of that verification about that intermediate node via another neighbor.

Step 8: If next neighbor has the record of forwarding any packet via that intermediate node and if neighbor nodes also not have any entry to forward the packet via that intermediate node, receive count and forward count will be 0 in both from node and to node.

Step 9: If source has not got response in time or received verification reply with 0 value, source rejects all nodes in path and chooses next path to forward data. Go to step 4.

Step 10: Repeat the steps from 4 to 9 until data packets reach the destination.

Step11: Compute the performance metrics, namely, throughput, packet delivery ratio and end to end delay.

Step12: Stop

V.EXPERIMENTAL RESULTS AND DISCUSSION

The simulation experiments of the proposed algorithm are conducted using NS-2.34 simulator with the simulation parameters chosen as mentioned in the Table III.

The efficiency of the proposed adaptive fuzzy inference method is analyzed on the basis of three performance metrics, namely, throughput, packet delivery ratio and end-to-end delay, in the presence of different percentage of black hole nodes (5%, 10%,15%, 20%, and 25%) in a network of total 200 nodes. The results are compared with that of the adaptive method in [17].

Table III.SIMULATION PARAMETERS AND THEIR VALUES USED IN EXPERIMENTATION

Parameters	Value
Packet size	512bytes
Simulator	NS-2.34
Transmission range	250mts
Node placement	Randomly
Number of black holes in terms of percentage	5%,10%,15%, 20% and 25% of total nodes
Simulation run time	100sec to 500sec
Number of Mobile Nodes	200 nodes
Topology	1000 * 1000 (m)
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)

(a) *Throughput:* The rate at which packets of data are sent successfully in the network in a second is called throughput. It is observed that, as the number of black holes increases, throughput continues to be decreased. There is improvement in performance due to detection and prevention of black hole attack. The throughput is increased by 36.05% by using the proposed method, in comparison with that of adaptive method in [17], in the presence of black hole attack with 5% of nodes as black holes. With the rise in concentration of black holes, there is reduction in throughput. As concentration of black hole nodes increases, the available paths are fewer leading to further reduction in throughput. The Table IV and the Fig.3 show the comparison of throughputs for the proposed adaptive fuzzy inference system and that for the adaptive method in [17], which reveals better results for adaptive fuzzy inference method.

Table IV. COMPARISON OF THROUGHPUTS OBTAINED BY VARYING NUMBER OF BLACK HOLE NODES X=5, 10, 15, 20 AND 25% OF N=200 NODES FOR THE ADAPTIVE METHOD AND PROPOSED ADAPTIVE FUZZY INFERENCE SYSTEM METHOD IN [17].

Number of black hole nodes (x%)	Throughput for adaptive method [17]	Throughput for adaptive fuzzy inference system method	Increase in Throughput (%)
5%	293280	458657	36.05%
10%	272640	324751	16.04%
15%	158240	211568	25.06%
20%	98400	128604	23.48%
25%	92420	98631	6.29%

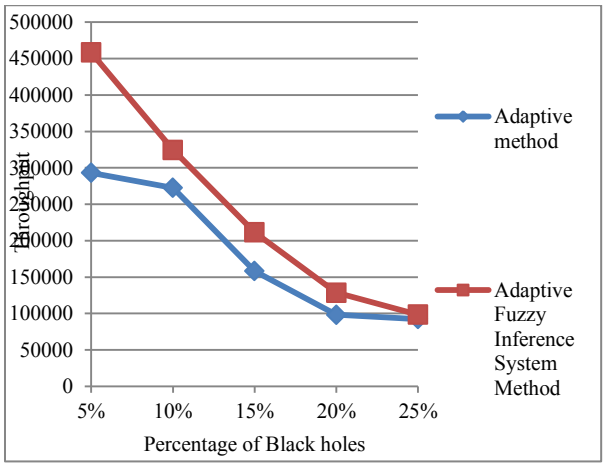

Fig. 3. Throughput for varying number of black hole nodes x=5, 10, 15, 20 and 25% of N=200 nodes: After detection and prevention of black hole attack using proposed adaptive fuzzy inference system method and the adaptive method in[17].

(b) *Packet delivery ratio (PDR) of packets*: It is the relative number of packets of data gained successfully at target to the total number of generated packets of data at the source. The Fig. 4 shows the PDR for varying number x of the black hole nodes (x=5, 10, 15, 20and 25% of total nodes N=200), after recognition and prevention of black hole nodes using the proposed method and the results are shown in the Table V. It is observed that there is an improvement in performance due to detection and avoidance of black hole nodes, as shown in the Table V. The PDR is increased by 98.63% by using the proposed method, in comparison with that of adaptive method [17], in the presence of black hole attack with 5% of nodes as black holes. As the concentration of black hole nodes increases, the performance degrades due to non availability of paths as nodes become black holes. It is observed in the Fig.4 that the results show better performance in case of adaptive fuzzy inference when compared with adaptive method in [17].

Table V. COMPARISON OF PACKET DELIVERY RATIO OBTAINED BY VARYING NUMBER OF BLACK HOLE NODES X=5, 10, 15, 20 AND 25% OF N=200 NODES FOR THE ADAPTIVE METHOD AND PROPOSED ADAPTIVE FUZZY INFERENCE SYSTEM METHOD IN [17].

Number of black holes (x %)	Pdr for adaptive method[17]	Pdr for adaptive fuzzy inference system method	Increase in pdr(%)
5%	95.76%	98.63%	2.87%
10%	93.81%	96.98%	03.26%
15%	92.89%	94.87%	02.08%
20%	90.53%	93.16%	02.82%
25%	87.72%	90.54%	03.11%

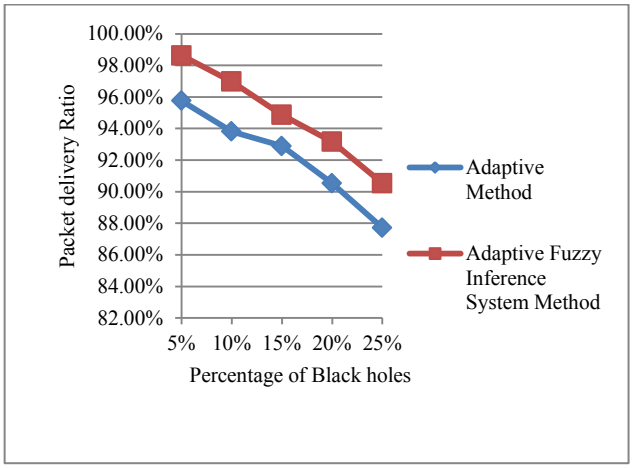

Fig 4. Comparison of packet delivery ratio (PDR) obtained by varying number of black hole nodes x=5, 10, 15, 20 and 25% of N=200 nodes for the proposed adaptive fuzzy inference method and the adaptive method in[17].

(c) *End to End (E2E) delay*: It is the mean time interval elapsed for a successful delivery of a packet from source node to the node at destination across a given network. The Fig. 5 shows E2E delay for certain number of nodes as black hole x=5, 10, 15, 20 and 25% of total nodes N=200, after finding and preventing attack of the black holes using the proposed adaptive fuzzy method. It is observed that there is a decrease in end to end delay because of the detection as well as prevention of attack of the black holes (Table VI). As the black hole nodes increase in the network, the performance degrades due to the non-availability of paths for data transmission.

Table VI. COMPARISON OF END TO END DELAY(E2E) OBTAINED BY ALTERING THE QUANTITY OF BLACK HOLE NODES X=5, 10, 15, 20 and 25% OF N=200 NODES FOR THE ADAPTIVE METHOD AND PROPOSED ADAPTIVE FUZZY INFERENCE SYSTEM METHOD IN [17].

Number of black holes (x %)	**E2E delay for adaptive method[17]**	**E2E delay for adaptive fuzzy inference system method**	**Decrease in E2E delay**
5%	0.556561	0.025565	0.530996
10%	0.343652	0.032847	0.310805
15%	1.453335	0.033001	1.420334
20%	3.871245	0.048610	3.822635
25%	4.135704	0.053124	4.08258

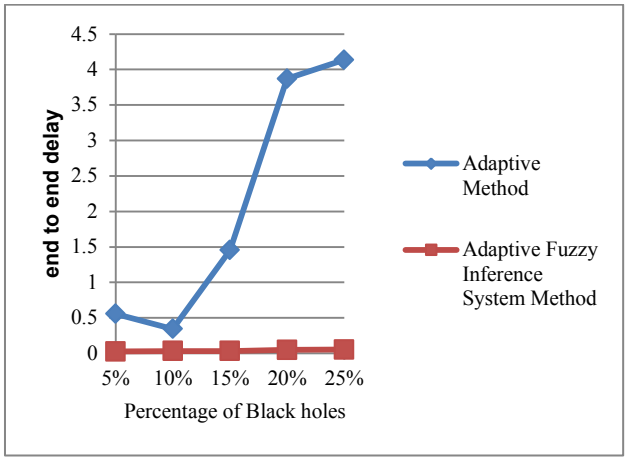

Fig 5. Comparison of end to end (E2E) delay obtained by changing number of black hole nodes x=5, 10, 15, 20 and 25% of N=200 nodes for the adaptive method and proposed adaptive fuzzy inference system method in[17].

VI. CONCLUSION

The proposed method is a novel efficient automatic method for detecting and avoiding cooperative black hole attack in MANETs. It is based on adaptive fuzzy inference system. The method is more effective and computationally inexpensive. Changes to the fuzzy inference system can be made with much ease by virtue of a simple learning process in framing fuzzy rule base. The fuzzy logic deals with such applications more accurately because of its resemblance to human decision making, that is, its ability to produce exact solution from incomplete or fairly inaccurate information. Results of simulation experiments show that the proposed method, which uses the fuzzy inference system, yields better results compared to the adaptive method in [17]. These results indicate that the proposed adaptive FIS is more promising in effectively and competently detecting and preventing different types of attacks in MANETS.

ACKNOWLEDGMENT

The authors are grateful to the reviewers for their helpful comments and suggestions, which improved the quality of the paper.

REFERENCES

[1] P Johnson "Routing Protocols for Mobile Ad-Hoc Networks- a comparative performance analysis", *Proc. ACM/IEEE Int Conf. on Mobile Computing and Networking (MobiCom'99), Seatle, WA*, Aug. 15-19, pp .195-206,1999.

[2] C Siva Ram Murthy and B.S Manoj, "Chapter-3 Ad-hoc Wireless Networks", in '*Ad-Hoc Wireless Networks: Architectures and Protocols*', (Prentice Hall, 1st Edition), pp.213-245, June 2000.

[3] C.E Perkins and E M Royer, "Ad-Hoc on-demand distance vector routing", *Proc. Second IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, Louisiana, USA, 25-26, pp.90-100, February 1999.

[4] Sonal and Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic", *International Journal of Science and Research (IJSR),* ISSN: 2319-7064,Vol 2 Issue8, pp.222-225, Aug 2013.

[5] Bharanidharan Shanmugam and Norbik Bashah Idris, "Improved Intrusion Detection System using Fuzzy Logic for Detection Anomaly and Misuse type of Attacks", *International Conference of Soft Computing and Pattern Recognition*, *IEEE*, pp.212-217, 2009.

[6] C Gomathy and S Shanmugavel, "Supporting QOS in MANET by a Fuzzy Priority Scheduler and Performance Analysis with Mixed Traffic", *International Conference on Fuzzy Systems*, ,IEEE, pp.31-36, 2005

[7] J Martin Leo Manickam and S Shanmugavel, "Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET", *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE, pp.39-44, 2007.

[8] K.T. Ibrahim, Nesar Ahmad and Salim Beg, "A Congestion Window Control mechanism based on Fuzzy Logic to improve TCP performance in MANETs", *International Conference on Computational Intelligence and Communication Systems*, IEEE, pp.21-26, 2011.

[9] Jay dip Sen, Sripad Koilakonda and Arijit Ukil, "A Mechanism for Detection of Cooperative Black hole Attack in Mobile Ad hoc Networks", *Second International Conference on Intelligent Systems, Modeling and Simulation*, IEEE, pp. 338-343, 2011.

[10] Ehsan Amiri, Ali Harounabadi and Seyed Javed Mirabedini, "Nodes clustering using Fuzzy logic to optimize energy consumption in Mobile Ad hoc Networks (MANET)", *Management Science Letters*, Growing Science, pp.3031-3040, 2012.

[11] Monita Wahengbam and Ningrinla Marchang, "Intrusion Detection in MANET using Fuzzy Logic", IEEE 2012.

[12] P.S.Hiremath and Shrihari M Joshi, "Energy Efficient Routing Protocol with Adaptive Fuzzy Threshold Energy for MANETs", *IRACST- International Journal of Computer Networks and Wireless Communication (IJCNWC),*Vol 2,No.3, pp.402-407, June 2012.

[13] A Vani Hiremani and M J Manisha, "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET", *IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, pp.944-948, 2013.

[14] C Alka, V. N. Tiwari and Anil kumar (SMIEEE), "Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad hoc Networks", *IEEE International Advance Computing Conference (IACC)*, pp.256- 261, 2014.

[15] C Alka, V. N. Tiwari and Anil kumar (SMIEEE), "A Reliable Solution against Packet Dropping Attack due to Malicious Nodes Using Fuzzy Logic in MANETs", *International Conference on Reliability, Optimization and Information Technology-ICROIT IEEE*, pp.178-181, 2014.

[16] D.K Levonevskiy, R.R. Fatkieva and S.R. Ryzhkov, "Network Attacks Detection Using Fuzzy Logic", *IEEE*, pp. 243-244, 2015.

[17] P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack in MANETs", *International Journal of Electrical and Electronics and Data Communication*, Volume-3, Issue-4, pp.1-7 , April-2015.

[18] P.S Hiremath and .AnuradhaT.,"Performance Comparison of Cluster based and Threshold based Algorithms for Detection and Prevention of Cooperative Black Hole Attack In MANETs", *International Journal of Advanced Networking and Applications*, Vol 6 Issue 3 ,pp. 2352-2358.

[19] B. Kondaiah and M. Nagendra, "A Black hole Attack on Performance of AODV Routing Protocol in Manet", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 11, pp.427-431, November 2015.