A New Secure Fuzzy Logic based Black Hole Attack Prevention System in MANET

Ira Nath
JIS College of Engg,
Kalyani, Nadia, 741235,
West Bengal, India

ABSTRACT
MANETs are accessible to various attacks [1]. Black hole attack is one kind of routing disturbing attacks [13] and can destroy a MANET partially or totally. In this paper Fuzzy Logic techniques have been used to detect black hole attacks and find out secure routing in wireless ad hoc networks. The proposed heuristic successfully detects the black hole in the network and this information is passed to other nodes also. AODV protocol has been chosen to test our algorithm and NS-3 as the simulation tool. This proposed method is compared with RRAF method [3]. The results of the simulation showed that the performance of the proposed method in this paper is noticeably improved. So, it is feasible that the fuzzy logic algorithm is applied to find out black holes for security purpose in MANET.

Keywords
Mobile Ad hoc network, AODV protocol, Fuzzy, Black hole attack.

1. INTRODUCTION
In MANETs security is a major issue. Various attacks in MANET are harmful for different routing protocols. Sometimes, whole network can be collapsed by different attacks. Among various attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). Wired security mechanisms are not applicable for MANET as it has no fixed infrastructure, with wireless links and mobile nodes. MANETs[2,4] are affected by various types of attacks such as Wormhole Attack, Sleep Deprivation Torture Attack, Jellyfish Attack, Misrouting Attack, Impersonation Attack, Routing Table Overflow Attack[16]etc. In this paper a new approach has been proposed for black hole detection and secure routing in a MANET. It detects existence of malicious nodes, finds out their exact position at any time instant t, selects route. Finally, the detected malicious node is listed in the black hole list and notices all other nodes in the network to stop any communication with them. As a result, the proposal can reduce packets loss that is caused by the malicious nodes and have better packet delivery ratio within less time period. The rest of the paper is organized as follows. In section 2, Black Hole attack in a MANET has been introduced. Next, in section 3 the proposed method has been developed. The implementation of the proposed method is done using Matlab-7.10.0.499(R2010a) in sec. 4 and Analysis the simulation result (in ns3 ver-3.11) is in section5. Finally, the conclusion is depicted in section 6.

2. BLACK HOLE ATTACK [5, 6, 10]
In MANET, a malignant node can attract all packets by falsely claiming itself as a fresh destination node. Now S starts data communication with M instead of D. In this way M behaves like a Black hole. In the following illustrated Fig.1, source node S wants to send data packets to a destination node D. So, S broadcasts RREQ. Node M is a malignant node which response with RREP first. Because, it has no checking part and demand itself as route to the destination and then assimilate them without forwarding them to the actual destination.

3. PROPOSED MODEL
This section presents a reliable black hole detection system between source and destination based on Fuzzy logic.

3.1 SFBH Method.
The two main parameters that make the black hole attack detection algorithm more reliable are direct trust value and throughput of each node. Before seeing the algorithm in detail, trust estimation mechanism is explained below.

3.1.1 Direct Trust.
In an ad hoc network, the relationship [3] of a node i to its neighbor node j can be any one of the following types-

a) Node i is a stranger to neighbor node (status of this node is considered as Low), their trust levels between each other will be low.

b) Node i is an acquaintance to neighbor node (status of this node is considered as Medium), their mutual trust levels are neither too low nor too high to be reliable.

c) Node i is a friend to neighbor node (status of this node is considered as High). the trust levels between them are reasonably high.

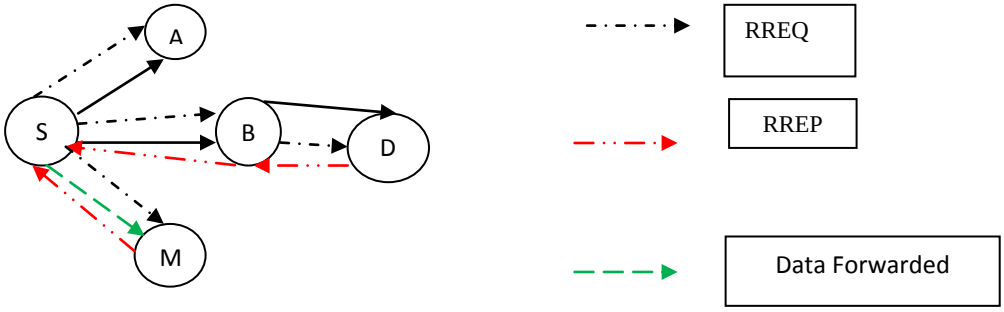

Figure1: Black hole attack in MANET

3.1.1 Throughput.

To calculate throughput values (TH) of a node source node (S) first sends false packets to the destination node. The malicious node must show its behavior according to its character. It may act as a black hole. In such cases the packets are dumped and not retransmitted. When the malicious node gets the false packet then it works according to its nature. If the node is not the black hole then it returns back the false packet after getting the request of return the packet to the sender. Otherwise the node acts like a dump and cannot returns back the false packet to the sender [15]. The throughput of the node is calculated as the ratio of number of packets forwarded by the number of packets received by the next nodes (NHN). "Direct Trust" values and "Throughput" values over a span of time for any node can be represented by a membership function. Fig. 2 represents the member function of black hole attack detection parameters for any node.

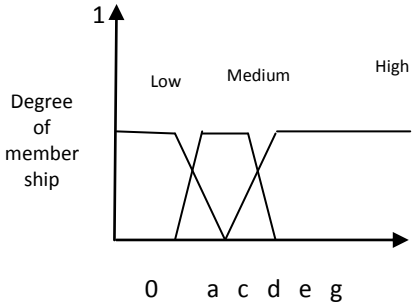

Figure.2: Trapezoidal-Shaped Membership function

$$low(x) = \begin{cases} 1 & x \le a \\ \dfrac{(d-x)*2}{(a+d)} & a \le x \le d \\ 0 & d \le x \end{cases}$$

$$high(x) = \begin{cases} 0 & d \ge x \\ \dfrac{[(x-d)*2]}{d+g} & d < x < g \\ 1 & g \le x \end{cases}$$

$$medium(x) = \begin{cases} 0 & x \le a \\ \dfrac{x-a}{c} & a \le x \le c \\ 1 & c \le x \le e \\ \dfrac{g-x}{e} & e < x < g \\ 0 & g \le x \end{cases}$$

Table1: Fuzzy Table

Rules	Direct Trust	Throughput	Node's current Status
Rule1	Low	low	Malicious
Rule2	Low	medium	Malicious
Rule3	Low	high	Trusted
Rule4	Medium	low	Malicious
Rule5	Medium	medium	Trusted
Rule6	Medium	high	Trusted
Rule7	High	high	Trusted
Rule8	High	low	Malicious
Rule9	High	medium	Trusted

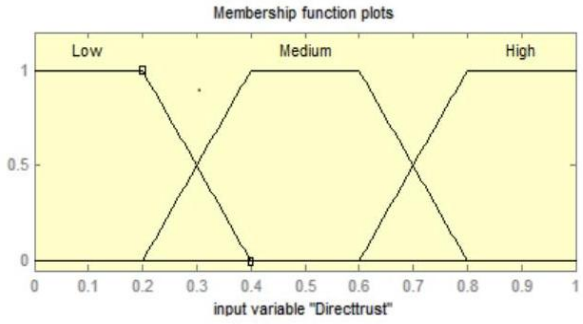

Figure 3: Membership functions for 'direct trust'

4. IMPLEMENTATION

Step1: Here Fuzzy Logic has been used for black hole attack detection of an ad-hoc wireless network. The proposed fuzzy logic based algorithm takes into account of two input variables, direct trust and throughput. The absolute value of each of these parameters can take a large range at different points on the network. In this paper the normalized values for each parameter has been considered.

Step 2: Now, "crisp" normalized values has been converted into fuzzy variables. For this, three fuzzy sets have been defined for each variable. The fuzzy sets, low (from 0 to 0.4), medium (from 0.2 to 0.8) and high (from 0.6 to 1.0) have been used for the input variables. The normalized value of each parameter is mapped into the fuzzy sets. Each value of the

input parameters will have some grade (low, medium, or high) of membership for each set. All the input parameters will have the same kind of characteristics [9, 14].

Step 3: The crisp values of the network parameters are considered to fuzzify them. To detect the existing black holes, an output linguistic variable is used.

Step 5: In Table 1, fuzzy input parameters are depicted to flourish the rules. One particular rule has been selected depending upon the different fuzzy values of the input parameters. Consequently, an output linguistic value of that specific rule has been recorded. This output linguistic value of the rules decides about the detection of black hole (malicious or trusted) in MANET.

Step 6: The secure route is selected after detecting the existence of black holes based on two important network parameters: direct trust and throughput of nodes of the network. The results are defined as malicious (from 0 to 0.444) and trusted (from 0.444 to 1.0).

Step 7: The defuzzified crisp value is calculated. The security of the whole network (source to destination) is maintained based upon two input parameters "direct trust" and "throughput". Fuzzy inference system (FIS) is used to design this framework. The four components of the FIS consist of the knowledge base, inference engine, fuzzification module and defuzzification module. The output of this framework is the status of a node which is either "malicious" or "trusted" depending on the outcome of the two input parameters. "Trusted" means the best next hop for communication in present situation.

Step 8: A node can degrade its status (either friend to acquaintance or friend to stranger etc.) that affects the second input parameter i.e. throughput drastically. So, some frequent interval throughput has to be checked. These parameters have been converted into corresponding linguistic values and based on the fuzzy rule base system the cumulative value of the "Derived Rules" has been calculated.

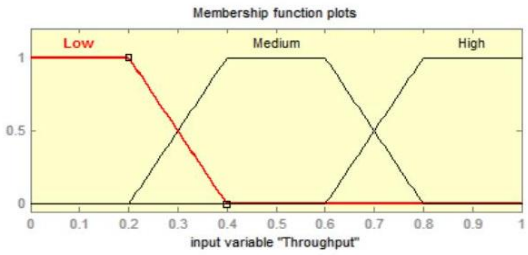

Figure.4: Membership functions for 'throughput'

Step 9: The converted input parameters (certain numeric form) are chosen randomly. From these values the cumulative value of nine rules has been formed. These cumulative values basically give information about the cumulative effect of the parameters on the status (either malicious or trusted) of the next hop node. Table 2 shows the various cumulative values for created nine rules.

Table 3: Tests Values

Direct Trust	Throughput	Result
9(High)	2(Low)	2.2(Malicious)
2.5(Low)	2.5(Low)	3.68(Malicious)
8.76(High)	8.76(High)	7.25(Trusted)

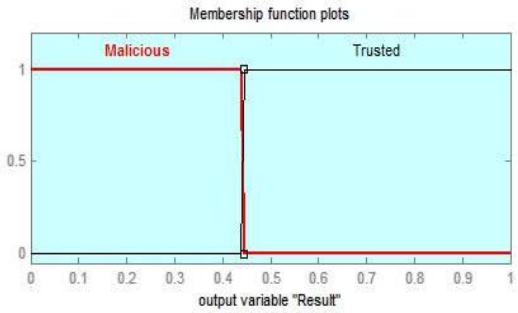

Figure.7: Membership functions for output 'Result'

Table 2: Cumulative Values for 9 Rules

Rules	Cumulative Values
1	3.5
2	3.6
3	7.25
4	2.2
5	7.25
6	3.6
7	3.6
8	7.25
9	7.25

5. EVALUATION OF PROPOSED METHOD

Table 3 shows the few results of our method RFBH with many test sets.

5.1Simulation

The proposed method (RFBH) has been simulated via NS-3(ver.3.11) [11,12]. The simulation environment is constructed by a 1500mx300m rectangular simulation area,1000 seconds simulation time, CBR traffic model, 2 second pause time, 60m/s maximum mobility, 250-meter transmission range, 4 malicious nodes and 60 nodes, distributed over the area. Simulation results have been compared with RRAF [3]. AODV routing protocol has been used for RFBH. The analysis is done based on network's packet delivery ratio and the network size.

5.2.1 Simulation Analysis and Results

Fig.5 shows the comparison of performance of two different fuzzy logic based black hole detection method. RFBH gives a better PDR with increasing number of nodes in the MANET. In RRAF methodology, two input network parameters are considered trust estimation and power consumption for secure routing between source and destination. But, these two inputs could not be the vital parameters for security purpose. Both the two methodologies consider trust as one input parameter. In this parameter any neighbor node may be any of the following status: friend, acquaintance and stranger. But motive (status) of any node can be changed (friend to acquaintance or friend to stranger) after some time interval. For this reason, throughput calculation after some time interval is essential. As if status of any node degrades from

friend to stranger, then throughput of this node must be less than its previous throughput value. Then this node can be identified as malicious by the proposed method RFBH. In this situation RRAF could not detect the malignant node from source to destination.

6. CONCLUSION

In this paper, an innovative scheme has been flourished for security of MANET in AODV against black hole attack. The implementation procedure is efficient enough for detection of malignant nodes. From the graphs it can be easily concluded that the performance of the RFBH under the presence of black hole attack is better than RRAF. The solution RFBH increases PDR with the increasing number of nodes of the network. Present experiment shows that the protocol is more powerful but obviously we need more trials and testing to judge its practical effectiveness in a large periphery. In future this proposed method can be used efficiently for various other attacks in MANETs with minor modifications of the proposed heuristic.

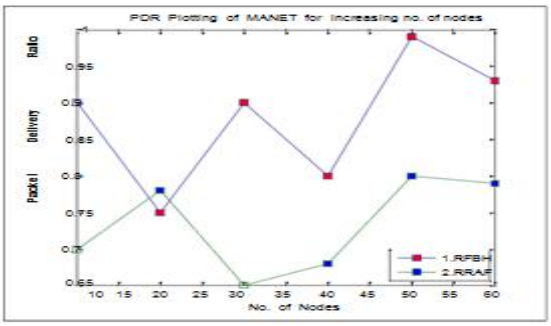

Fig.5: Performance graph

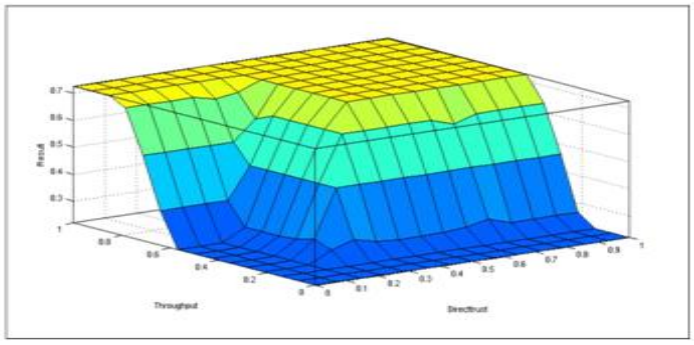

Fig.6:3D plot of the input parameters "direct trust" and "throughput"

7. REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei," A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks " Department of Computer Science and Engineering, Florida Atlantic University.

[2] J. Martin, Leo Manickam,"Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET"15th International Conference on Advanced Computing and Communications,2007 IEEE.

[3] Golnoosh Ghalavand, Arash Dana,Azadeh Ghalavand,Mahnaz Rezahosieni,"Reliable routing algorithm based on fuzzy logic for Mobile Adhoc Network",3rd International Conference on Advanced Computer Theory and Engineering(ICACTE),2010 IEEE.

[4] Manoj V, Mohammed Aaqib , Raghavendiran N and Vijayan R,"A Novel Security Framework Using Trust And Fuzzy Logic In Manet",International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[5] Ekta Kamboj, Harish Rohil,"Detection of Black Hole Attack on AODV in MANET Using Fuzzy Logic",Journal of Current Computer Science and Technology Vol. 1 Issue 6 [2011]316-318.

[6] Payal N. Raj, Prashant B. Swadas,anand,"dpraodv: a dyanamic learning system against blackhole attack in aodv based manet", ijcsi international journal of computer science issues, vol. 2, 2009,ISSN (Online): 1694-0784,ISSN (Printed): 1694-0814.

[7] Gasim Alandjani and Eric E. Johnson,"Fuzzy Routing in Ad Hoc Networks",IEEE 2003.

[8] Cuirong Wang, Shuyi Chen, Xiaozong Yang ,Yuan Gao,"Fuzzy logic-based dynamic routing management policies for mobile ad hoc networks",IEEE,2005.

[9] P.S.Banerjee J. Pal Choudhury S. R. Bhadrachaudhuri,"Routing based on Fuzzy Rule Base System and K-Means Clustering in Ad Hoc Wireless Network",International Journal of Computer Applications (0975 – 8887),Volume 35– No.4, December 2011.

[10] Kulbhushan, Jagpreet Singh,"Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET",IJCA Special Issue on "Network Security and Cryptography"NSC, 2011.

[11] [11] K. Fall; K. Varadhan, NS notes and documentation, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[12] ns-3 Tutorial, Release ns-3.11,ns-3 project, May 25, 2011.

[13] Jiwen Cai,Ping Yi,Jialin Chen, Zhiyang Wag, Ning Liu,"An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",2010 24th IEEE International Conference on Advanced Information Networking and Applications,Perth, Australia April 20-April 23,ISBN: 978-0-7695-4018-4.

[14] S. Garg,V. Bansal,"A New Bandwidth Efficient & Network Dependent On-Demand Routing Protocol For

[15] MANETs",Int. J. of Adv. Research in Com. Sc. and Software Engg,Vol.2, Issue 7, 2012,ISSN: 2277 128X.

[16] I. Nath, R.Chaki,"BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET",Int. J. of Adv. Research in Comp. Sc. and Software Engg, Vol. 2, Issue 8, 2012, ISSN: 2277 128X.

[17] S. Zihao, L. Shufen ,"A routing attack detection method for cluster wireless sensor networks",journal of theoretical and applied information technology,31 august, 2012. Vol. 42, No.2 © 2005 - 2012 JATIT & LLS. All rights reserved. ISSN: 1992-8645, E- ISSN: 1817-3195.