A Fuzzy Based Control over Malicious Nodes in Manet

Vinod Kumar
M.Tech. , Netaji Subhas Institute of Technology, University of Delhi
New Delhi, India

Prof. Satbir Jain
Netaji Subhas Institute of Technology, University of Delhi
New Delhi, India

Abstract: A mobile ad-hoc network (MANET) is a kind of self-organizing, self-configuring and infra-structureless wireless system. Devices in MANET join and leave the network asynchronously. The Dynamic topology, decentralized control, mobile communications structure renders wireless ad-hoc network vulnerable to various type of attacks. We presents a fuzzy based control technique to detect and mitigate a type of attack, namely malicious packet dropping, in wireless ad-hoc network. A malicious node can promise to forward packets but drop or delay them. In our technique, every node in the mobile ad-hoc network send the route request and wait for the acknowledgment. The requesting node analyze the behavior of unknown node using fuzzy technique and on basis of result the node take this node in the route of the packet. Subsequently, node state information can be utilized by the routing protocol to bypass those malicious nodes. Our method shows that in a moderately changing network, this technique can detect most of the malicious nodes with a relatively high positive rate. The packet delivery rate in the MANET can also be increased accordingly.

Keywords: MANET, Fuzzy logic control, Black hole attack, Cooperative Black hole Attack.

I. Introduction

A mobile ad-hoc network (MANET) is a self-configuring infra structure less network of mobile devices connected by wireless link. Ad-hoc is Latin word and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet.

MANETs are a kind of wireless ad-hoc network that usually has a routable networking environment on top of a link layer ad hoc network. Since mobile nodes in Mobile ad hoc network can move arbitrarily the topology may change frequently at unpredictable times. Transmission and reception parameters may Also impact the topology. The routing algorithm must react quickly to topological changes as per the degree of trust of a node or a complete path between a source and a destination pair. Nodes in Mobile ad hoc network communicate over wireless links. Therefore efficient calculation of trust is a major issue in mobile ad hoc networks because an ad hoc network depends on cooperative and trusting nature of its nodes. As the nodes are dynamic the number of nodes in route selection is always changing thus the degree of trust also changes. Survival of ad hoc networks depends on cooperative and trusting nature of its nodes.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

Black hole Attack:

In Mobile Ad hoc Network 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. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

Cooperative Black-hole Attack:

It is a type of attack in which blackhole nodes act in a group together . For example when multiple black hole nodes are acting in coordination with each other, the first black hole node refers to the one of its team mates in the next hop . This type of attack harm the system very much and affect the throughput of the system. The nodes in the following fig. With H are malicious nodes that act in coordination with each other.

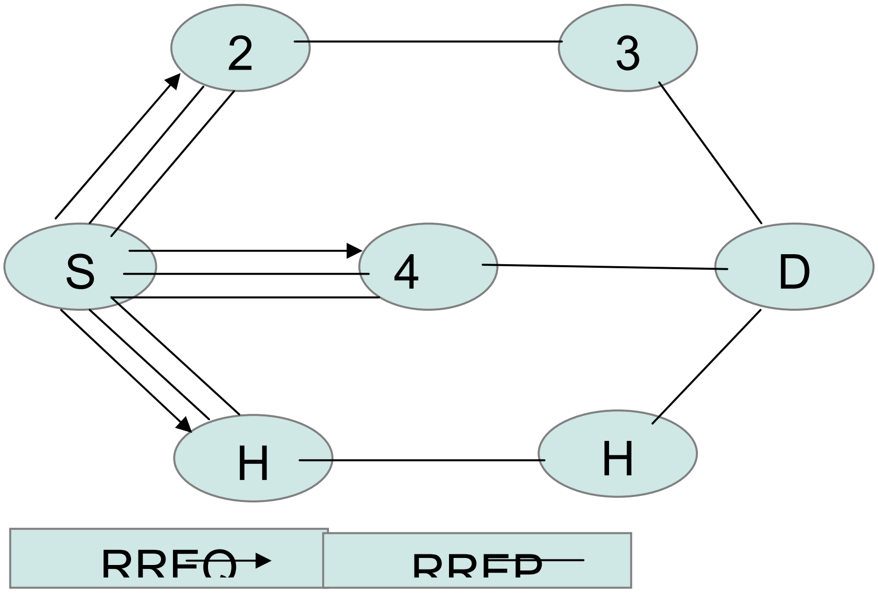

Figure 1. Attack Scenario

II. Fuzzy Logic

Fuzzy logic starts with and builds on a set of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. This simplifies the job of the system designer and the computer, and results in much more accurate representations of the way systems behave in the real world.

Additional benefits of fuzzy logic include its simplicity and its flexibility. Fuzzy logic can handle problems with imprecise and incomplete data, and it can model nonlinear functions of arbitrary complexity. “If you don’t have a good plant model, or if the system is changing, then fuzzy will produce a better solution than conventional control techniques,” says Bob Varley, a Senior Systems Engineer at Harris Corp., an aerospace company in Palm Bay, Florida. Fuzzy logic models, called fuzzy inference systems, consist of a number of conditional “if-then” rules. For the designer who understands the system, these rules are easy to write, and as many rules as necessary can be supplied to describe the system adequately (although typically only a moderate number of rules are needed).

In fuzzy logic, unlike standard conditional logic, the truth of any statement is a matter of degree. (How cold is it? How high should we set the heat?) We are familiar with inference rules of the form p -> q (p implies q). With fuzzy logic, it’s possible to say (.5* p) -> (.5 * q). For example, for the rule if (weather is cold) then (heat is on), both variables, cold and on, map to ranges of values.

Fuzzy inference systems rely on membership functions to explain to the computer how to calculate the correct value between 0 and 1. The degree to which any fuzzy statement is true is denoted by a value between 0 and 1.

In our proposed scheme of defending against black hole attack we proposed the fuzzy controller for getting rid of this type of attack.

III. PREVIOUS WORK

In [10], Deng et al. proposed a solution for individual black holes. But they have not considered the cooperative black hole attacks. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution can not prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply “yes” for both questions. Then the source will trust on next hop and send data through the replied node which is a black hole node.

In [11], Yin et al. proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further. Hesiri Weerasinghe and Huirong Fu [12] simulated the algorithm proposed by [3] with several changes to improve the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the process. They also simulated AODV [17] and the solution proposed by [3] and compared them with [10].

In DPRAODV [4], they have designed a novel method to detect black hole attack: DPRAODV, which isolates that malicious node from the network. The agent stores the Destination sequence number of incoming route reply packets (RREPs) in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval as in [5].the solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. DPRAODV does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet.

IV. PROPOSED WORK

In this section we introduced the improvement of the selection of the shortest route to the destination and protocol discussed the most reliable and secure route to the destination based on the trust values of all nodes. In this paper we present the fuzzy based controller for detecting the secure route by nature of association of nodes. The nodes can be bad(B), good(G), and well known(WN). These properties can be changed with time based on the the behavior of the nodes. The behavior of the node can be vary depending on the environment it is used. We present the extension of association based routing on AODV protocol to improve the existing implementation. We have taken three values for different type of nodes as given in the figure.

Here we have created membership function for type of node given.

We have three types of nodes.

1. Bad
2. Good
3. Well Known

For example at x=1 the node is bad with value 1 but at x=1.5 the membership value of bad node will be 0.3 and the membership value of good will be 0.3 also. We have given different value for bad,good and well known node for which membership value vary between 0 and 1;

$$\theta(x):X[0\ 4]\rightarrow[0\ 1]$$

We have assigned three different range for each type of node.
A node is bad if X=0 to 0.3 with membership value Y=0 to 1.
A node is good if X=0.2 to 0.6 with membership value Y=0 to 1.
A node is well known if X=0.5 to 1 with membership value Y=0 to 1.

For the given value of X and the membership value for this value is checked and examined based on the membership value which node is bad, good and well known.

These values can be changed with time depending on the behavior of the node. The values of X is chosen based on the environment in which we are using the system.

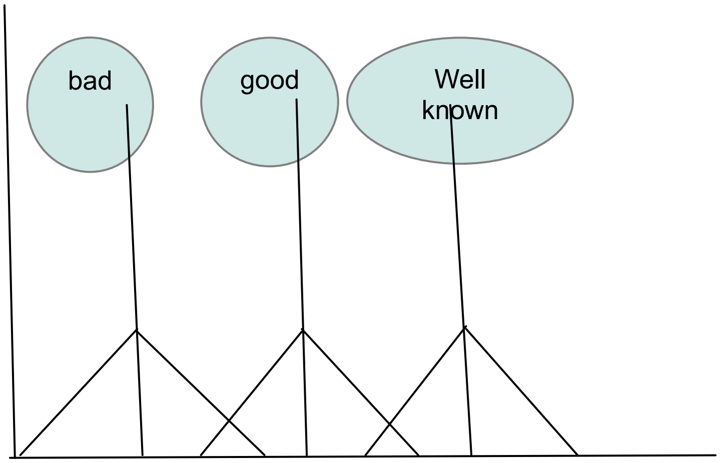

Figure 2.

Membership function for bad nodes.

F1(AV) = { 1 when AV Є [0, r]
{ A(r-x)+1 when AV Є [r, r+1/A)
{ 0 otherwise
where r=0.15
A=6.6

2. Membership function for good node
F1(AV) = { A1(AV-r)+1 when AV Є [r-1/A1, r]
{ A1(r-AV)+1 when AV Є [r, r+1/A1)
{ 0 otherwise
where r=0.4
A1=5

3. Membership function for well known node
F1(AV) = { A1(AV-r)+1 when AV Є [r-1/A1, r]
{ 1 when AV Є [r>=0.7]
where r=0.7
A1=5

Membership Function for different nodes given in following figure.

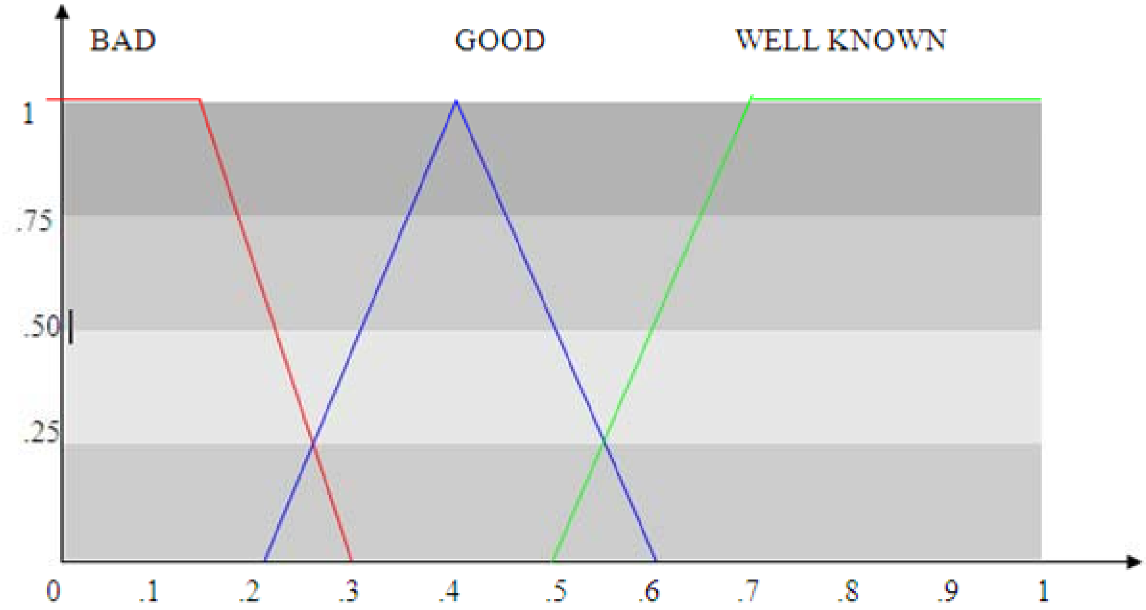

Figure 3 Membership function for each type of nodes.

Trust value of the particular node depends on the following formula.

$$AS = \tanh (P1+P2+A) \qquad (1)$$

Where
AS=Association Type

P1=Ratio of Number of packets forwarded successfully by neighbour node to the total number of packets to be forwarded by neighbour node.
P2=Ratio of number of packets received from a node but originated from others to total number of packets received from it.
A = Acknowledgement bit(0 or 1).

```
Routing Algorithm:
Notations:
SN: Source Node       IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
Reliable Node: The node through which the SN has routed data
SN broadcasts RREQ
SN receives RREP
IF (The membership grade of well known node is > the membership grade of  good nodes)
   {  node is well known
      Route data packets (Secure Route)
  }
 ELSE
  {
      Node is good
      Route data packets (Secure Route)
  }

 IF (The membership grade of good node is > the membership grade of  bad nodes)
```

```
{   Then node is good known
    Route data packets (Secure Route)
}
ELSE
{  Node is bad
   Insecure route
    Node may be black hole node
} while(IN in not a reliable node)
```

V. SIMULATION SETUP

SIMULATION PARAMETERS

Examined protocols	AODV
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000 Number of Nodes 16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

VI. RESULT

The red line give the throughput without applying fuzzy based algorithm. The Red line give the throughput under fuzzy based algorithm. From given figure we can see that using this algorithms we can increase throughput and avoid the black hole attack.

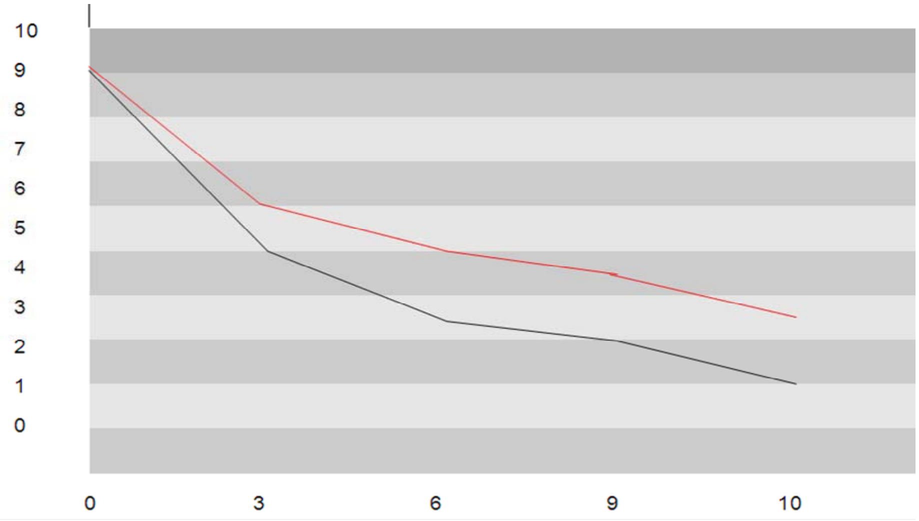

Figure 4

VII. CONCLUSION

In this paper we have given fuzzy based trust value routing algorithm to deal with black-hole and cooperative black-hole attack that are caused by malicious nodes. We believe that this model is a requirement for the formation and efficient operation of ad hoc networks. This paper represents the first step of our research to analyze the cooperative black-hole attack using fuzzy control over the proposed scheme to analyze its performance.

REFRENCES

[1] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," IEEE Communications, vol. 10, no. 40, October 2002, pp. 60-68. Digital Object Identifier 10.1109/MCOM.2002.1039858

[2] Bracha Hod, "Cooperative and Reliable Packet- Forwarding On top of AODV", www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard,"Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks", www.cs.ndsu.nodak.edu/~nygard/research/BlackHoleMA NET.pdf 2003

[4] Payal N. Raj, Prashant B. Swadas "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet" IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007

[6] Piyush Agrawal and R. K. Ghosh "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks "Proceedings of the 2nd international conference on Ubiquitous information management and communication, Suwon, Korea, ISBN: 978-1-59593-993-7, Pages: 310- 314, 2008.

[7] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" © 2011 ACADEMY PUBLISHER 97 ACMSE'04,April 2- ,2004,Huntsville,AL,USA.

[8] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch "Detecting Black-hole Attack in Mobile Ad Hoc Network". 5Th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[11] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", IEEE SUTC 2006 Taiwan, 5-7 June 2006.

[12] Hesiri Weerasinghe and Huirong Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" International Journal of Software Engineering and Its Applications ,pp 39-54,Vol. 2, No. 3, July 2008

[13] C.E.Perkins and E.M.Royer "Ad hoc on demand distance vector routing", Proceedings of IEEE Workshop on Mobile computing systems and Applications 1999, pp. 90- 100, February 1999.

[14] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness and robustness in Mobile ad hoc networks. In proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network–based processing, Pages 403 – 410. Canary Islands, Spain. January 2002. IEEE Computer Society.

[15] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in Mobile ad hoc networks. In Proceedings of MOBICOM 2000. Pages 255- 265, 2000.

[16] N.Bhalaji, A.Shanmugam "Association between nodes to Combat Blackhole attack in DSR based MANET" in Proceedings of Sixth IEEE-IFIP International conference on WOCN, April 28-30, 2009, Cairo, ISBN: 978-1-4244- 4704-6, DOI: 10.1109/WOCN.2009.5010579

[17] N.Bhalaji, Dr.A.Shanmugam "Reliable Routing against selective packet drop attack ".