Black Hole Attack Detection using Fuzzy Logic

Sonal[1], **Kiran Narang**[2]

[1, 2] Hindu College of Engineering, Sonepat, Haryana, India

Abstract: ***MANET is a dynamic network with large number of mobile nodes .As the traffic increases over the manet it will leads to number of problems i.e congestion and packet loss .This congestion and packet loss problems occurs due to the attack in manet .one of attack is black hole attack .As a result some packet loss over the network and slows the communication process.In this paper we are providing the solution against black hole attack which is based on fuzzy rule .fuzzy rule based solution identify the infected node as well as provide the solution to reduce data loss over network.***

Keywords: MANET, Fuzzy logic, Black hole attack , Packet loss, Data rate.

1. Introduction

Mobile Ad hoc NETworks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e. routing functionality will be incorporated into mobile nodes. MANET is more vulnerable than wired network due to mobile nodes, threats from malicious nodes inside the network. Because of vulnerabilities, MANET is more prone to malicious attacks. MANET has following vulnerabilities.

- **Lack of centralized node**: MANET doesn't have a centralized node. The lack of centralized makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.
- **Resource availability**: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.
- **Scalability**: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
- **Dynamic topology**: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.
- **Limited power supply**: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
- **Bandwidth constraint:** Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.
- **Adversary inside the Network**: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.
- **No predefined Boundary**: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

2. Black hole attack in MANET

Attacks on MANETs can be divided into two categories, passive and active attacks. An active attack alters the operation of networks by modifying and interrupting data. A passive attack does not disturb the operation of networks.

In black hole attack, black hole node acts like black hole in the universe. In this attack black hole node absorbs all the Here we assume that if nodes are in their vicinity, they can traffic towards itself and doesn't forward to other nodes. Whenever, source node wants to send packet to the destination important issue. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node. Two types of black hole attack can be described in order to distinguish the kind of black hole Attack

2.1 Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

2.2 External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route

3. Routing in MANETS with and without Black hole Node

Generally routing in MANET is done either by table driven routing protocol or ad hoc on demand distance vector routing protocol. In case of table driven process, each and every node in MANETs maintains some up-to-date information about the network. Every node has the information about latest network topology, any changes happened to the network is generally propagated to the network, accordingly node updates their routing table .But this kind of protocol creates several problems to the network in terms of bandwidth overhead, wastage of battery power of the nodes, entry of unnecessary redundant route etc. Due to these difficulties, ad hoc on demand distance vector (AODV) routing protocol is preferred. In this protocol, routing tables are dynamically created when needed. So, whenever source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When destination sends a RREP packet to source through shortest path, the source sends data through this path. Though it looks very simple, but this kind of protocol suffers from several vulnerabilities of attack. If the path cannot be established then RERR messages is generated. AODV protocol is very much acquainted with dynamic network condition, low processing and memory overleaf, less bandwidth wastage with small control messages. Due to these kinds of reasons AODV becomes one of the most popular protocols in MANETs. Whenever a RREQ packet is generated by the source, every node that receives the RREQ packet will check whether this packet is meant for them or not. If so, immediately they will generate RREP message, otherwise every node tries to forward the packet to their neighbor to reach destination, if their routing table doesn't contain valid entry to destination. If the routing table contains valid entry to destination then next step is to check the destination sequence number. Usually destination sequence number is maintained by every node. Its value depends on network traffic and participation of node in packet forwarding. If the destination sequence number is same for more than one RREP then it goes for the specific path where number of hops to reach destination is lesser. Thus higher the sequence number implies the fresh route to destination. In case if the source receives multiple RREP then it decides the path where sequence number is higher

4. Literature Survey

Monita Wahengbam, Ningrinla Marchang [1] performed a work on "Intrusion Detection in MANET using the Fuzzy Logic".Fuzzy rule is implemenating during the analysis phase to detect the misbehavior over the network. The work will analyze the traffic over a node and take a fuzzy decision regarding the node reliability. The parameters in paper are number of successful data transmitted over the node, number of packets lost. Elmar Gerhards-Padilla, Marko Jahnke et.al[2]performed a work," Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs". In this work Author present TOGBAD a new centralised approach, using topology graphs to identify nodes attempting to create a black hole. Author use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network.

Latha Tamilselvan, Dr. V Sankaranarayanan et.al [4] "Prevention of Co-operative Black Hole Attack in MANET" gave an approach to combat the Black hole attack. In MANET, the absence of a fixed infrastructure, thus nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack .In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Their approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a ‘Black hole’ and is eliminated. The percentage of packets received through our system is better than that in AODV in presence of cooperative black hole attack. The solution is simulated using the Global Sensor Simulator and is found to achieve the required security with minimal delay & overhead.

Rajib Das, Dr. Bipul Syam Purkayastha et.al [6] performed a work,” Security Measures for Black Hole Attack in MANET: An Approach”. In this paper, Author give an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Presented aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node in the MANET at the beginning.

Jathe S.R, Dakhane D.M. [7] performed a work,” A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques”. Communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this paper Author studied the details about black hole attack, and comparison of different black hole attack techniques.

Rashid Sheikhl, Mahakal Singh Chande et.al [8] gave a paper on “Security Issues in MANET: A Review” In the paper author described security issues like No predefmed Boundary, Adversary inside the Network, Changing scale etc.and security criteria.Also explaned the intrusion detection systems and Privacy- preservation in MANET using Secure Multiparty Computation solution .

Ochola EO, Eloff MM [9] performed a work, ”A Review of Black Hole Attack on AODV Routing in MANET”. Black Hole attacks are launched by participating malicious nodes that agree to forward data packets to destination but eavesdrop or drop the packets intentionally, which not only compromise the network, but also degrade network performance. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. The route updates are shared not on a periodic but on an as requirement basis. The control packets create a potential vulnerability that is frequently exploited by malicious nodes. The paper further analyses the impact of Black Hole attack in AODV performance.

5. Purposed Work and Methodology

Mobile Ad-Hoc network is one of most common ad-hoc network with lot of problems related to congestion and routing. We are providing one of the solutions to secure the transmission over the network. Security aspects play an important role in almost all of the application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. The proposed system is about to design an intrusion detection system to detect the black hole attack on MANET This detection system is based on FUZZY LOGIC. We propose an IDS system in which improvement is by making use of two factors i.e. Packet Loss rate, Data Rate. We will use both factors using Fuzzy logic which is problem solving control system .Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, noisy or missing information. We proposed an algorithm which is based on above factors .In this algorithm firstly we define the network with N number of nodes and we set source node to S and destination node D and after that we we let current node is as source node .we repeat the steps until current node is not equal to destination node. In this now we find the list of neighboring nodes of current node. We identify the parameter s of each neighbor node i.e. packet loss, data rate. In this purposed algorithm we use the concept of Priority, only high priority nodes take part in communication. For priority we define the three steps at sender side.

Step 1: Packet loss is low and data rate is high then priority is high.
Step 2: Packet loss is medium and data rate is high then priority is medium.
Step 3: Packet loss is low and data rate is low then priority is low.

We set priority at receiver side also when the energy of any node is low then set the priority of node is low and node do not take part in communication. We increase the priority of node that they take part in communication. We are providing the condition Data Transmitted from the node is greater than THRESHOLD and Rate of node is also greater than THRESHOLD then increase the level of priority.

5.1 Algorithm to Detect Black Hole

```
1. Define a Network with N number of nodes
2. Define the Source Node S and Destination Node D
3. Set CurNode=S as Current Node
4. While CurNode <> DestNode
       a. [Repeat Steps 5 to 40]
5. Identify the list of neighbouring nodes to CurNode called
       Ne(1),Ne(2)…..Ne(M)
6. For i=1 to M
7. {
8. Idenitfy the Analysis parameter for Each Neighbour called
       PacketLossrate, DataRate
9. [Sender End Fuzzy Logic]
10.  Fuzzify these rules under the fuzzification process
11.  If ( Fuzzy(PacketLossrate(Ne(i)),Low) and
       Fuzzy(DataRate(Ne(i)),High)
12.  {
13.  Set Priority(Ne(i))=High
14.  }
15.  Else If ( Fuzzy(PacketLossrate(Ne(i)),Medium) and
       Fuzzy(DataRate(Ne(i)),Medium)
16.  {
17.  Set Priority(Ne(i))=Medium
18.  }
19.  Else If ( Fuzzy(PacketLossrate(Ne(i)),Low) and
       Fuzzy(DataRate(Ne(i)),Low)
20.  {
21.  Set Priority(Ne(i))=Low.(black hole node found)
```

```
        }
    }
    Find the List of High Priority Recievers from the Neighbor List called P(1),P(2)….P(K)
    [Receiver level Fuzzy Logic]
    For i=1 to K
    {
        If(Energy(P(i))=Low )
        {
            Set Priority (P(i))=Low
        }
        If(DataTransmitted(P(i))>THRESHOLD and Rate(P(i))>THRESHOLD)
        {
            Set Priority(P(i))=priority(P(i))+1
        }
    }

    Find the Node with Max Priority called Node p
    Set CurNode=p
}
```

6. Conclusion

The purposed algorithm will provide the solution of packet loss and data rate against the black hole attack in network. The purposed work will firstly detect the black hole attack using the fuzzy logic. The fuzzy logic is implemented on packet loss and data rate at time of node communication. Now in this it will send the packet from surrounding nodes. This algorithm will provide the better solution.

7. Acknowledgment

I would like to give my sincere gratitude to my guide Ms. Kiran Narang who guided me throughout, to complete this topic.

References

[1] Monita Wahengbam,” Intrusion Detection in MANET using Fuzzy Logic”, 978-1-4577-0748-3/12/$26.00 © 2012 IEEE

[2] Elmar Gerhards-Padilla,” Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs”, 32nd IEEE Conference on Local Computer Networks 0742-1303/07© 2007 IEEE

[3] Sanjay Ramaswamy Huirong Fu” Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks

[4] Latha Tamilselvan “Prevention of Co-operative Black Hole Attack in MANET” JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[5] K.Selvavinayaki, K.K.Shyam Shankar” “Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANET”International Journal of Computer Applications (0975-8887).volume7-volume11, October 2010.

[6] Rajib Das,” Security Measures for Black Hole Attack in MANET: An Approach”, International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462

[7] Jathe S.R, Dakhane D.M ,” A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques “International Journal of Cryptography and Security ISSN: 2249-7013 & E-ISSN: 2249-7021

[8] Rashid Sheikhl, Mahakal Singh Chande et.al [8] gave a paper on “Security Issues in MANET: Review” 978-1-4244-7202-4/10/$26.00 ©2010 IEEE

[9] Ochola EO,” A Review of Black Hole Attack on AODV Routing in MANET

[10] Isaac Woungang,,” Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks”, 978-1-4673-1550-0/12/$31.00 ©2012 IEEE

Author Profile

Ms. Kiran Narang is presently working as Assistant Professor in Hindu College of Engineering, Sonepat. She posses qualifications of B.Tech, M.Tech. She has been published many papers in National/ International journals and holds a teaching experience of approximate 10 years. Her research areas are in Wireless Networks, Computer Architecture and Data Structure.

Ms. Sonal has completed her B.Tech degree in Computer Science from Maharishi Dayanand University, Rohtak in year 2011. She is pursuing Hindu College of Engineering, Sonepat from 2011. Her research interests are in Mobile ad hoc networks and computer networks.