A Fuzzy Based Approach to Detect Black hole Attack

Poonam Yadav, Rakesh Kumar Gill, Naveen Kumar

***Abstract:** A Wireless network is a dynamic network with large no. of nodes. As the traffic increases over the network such type of network suffers from the problems like congestion and packet loss. But in case of Mobile network there is one more problem regarding the life of the network. A network can be affected from some Black hole attack over the network As a result some loss of information occur over the communication. The packet loss is acceptable up to some threshold value but as there is more packet loss we need some solution for this. The same solution is presented in this paper. Here we are presenting a fuzzy based decision to check a node is infected by Black hole attack or node. The proposed system will identify the attack over the node as well as provide the solution to reduce the data loss over the network.*

***Keywords:** Wireless, Mobile, Elimination, Black Hole, Fuzzy Rule*

I. INTRODUCTION

A mobile ad hoc network is a collection of mobile hosts that roams at will and communicates with each other. MANET has Multi-hop commutation capability. There is no centralized administration or a backbone network to support it. In these types of networks each node works as an independent router. Each host uses wireless RF transceivers as network interface. Example applications of MANET are emergency search-and-rescue operations; meetings or conventions where users need to deploy networks immediately without base stations or fixed network infrastructure.

Mobile ad-hoc networks are self organizing. They are fully decentralized means there is no central server exists in MANET environment. It is highly dynamic because topology of MANET changes rapidly. It has limited physical security as the broadcast nature of MANET lends itself to passive eavesdropping attacks without malicious nodes being detected. There are potentially frequent network partitions. This might imply that simply no path exists from a mobile node to another as the intermediate routing stations have moved too far apart.

As MANET become widely used, the security issue has become one of the primary concerns. The mobile hosts forming a MANET are normally mobile devices with limited physical protection and resources. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols.A mobile ad hoc network is a collection of mobile hosts that roams at will and communicates with each other. MANET has Multi-hop commutation capability. There is no centralized administration or a backbone network to support it. In these types of networks each node works as an independent router. Each host uses wireless RF transceivers as network interface. Example applications of MANET are emergency search-and-rescue operations; meetings or conventions where users need to deploy networks immediately without base stations or fixed network infrastructure.

Mobile ad-hoc networks are self organizing. They are fully decentralized means there is no central server exists in MANET environment. It is highly dynamic because topology of MANET changes rapidly. It has limited physical security as the broadcast nature of MANET lends itself to passive eavesdropping attacks without malicious nodes being detected. There are potentially frequent network partitions. This might imply that simply no path exists from a mobile node to another as the intermediate routing stations have moved too far apart.

As MANET become widely used, the security issue has become one of the primary concerns. The mobile hosts forming a MANET are normally mobile devices with limited physical protection and resources. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols.

A) Routing

It is the act of moving information from a source to a destination in an inter-network. During this process, at least one intermediate node within the inter-network is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internetwork. The later concept is called as packet switching which is straight forward, and the path determination could be very complex. Routing protocols use several metrics to calculate the best path for routing the packets to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet.

Manuscript received on July 09, 2012

Poonam yadav, Research scholar, Department of electronics & communication, MDU, Rohtak, India,

Rakesh Kumar Gill, Assistant Professor, Department of Electronics & Communication, GITM, Gurgaon, Haryana, India,

Naveen kumar, Research scholar, Department of electronics & communication, MDU, Rohtak, India,

B) AODV

It stands for ad-hoc on demand distance vector routing protocol. It is a reactive protocol. It makes the route when it is needed and does not require nodes to maintain the routes to various destinations that are not being used in communication. AODV enables multi- hop routing between participating mobile nodes wishing to establish and maintain an ad- hoc network. AODV is able to provide unicast, multicast and broadcast communication ability. Route tables are used in AODV to store applicable routing information. AODV utilizes both a route table for unicast routes and a multicast route table for multicast routes. The protocol is able to respond to topological changes that affect the active routes in a quick and timely manner.

C) Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the destination node of the packet that was intercepted. This attack can be easily implemented in AODV during the routing discovery process. Once the forged route has been established the malicious node is able to become a member of the active route and intercept the communication packets. The outcomes of this attack can vary. The malicious node can either stop after inserting the false route information in the network and aim in creating instability and unnecessary network traffic or drop all incoming application packet for the specific destination.

D) IDS

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved, is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator.

II LITERATURE SURVEY

Anomaly detection and mitigation for disaster area networks In this paper they address anomaly detection in intermittently connected mobile ad hoc networks in which there is little or no knowledge about the actors on the scene, and opportunistic contacts together with a store-and-forward mechanism are used to overcome temporary partitions. The approach uses a statistical method for detecting anomalies when running a manycast protocol for dissemination of important messages to k receivers. Simulation of the random walk gossip (RWG) protocol combined with detection and mitigation mechanisms is used to illustrate that resilience can be built into a network in a fully distributed and attack-agnostic manner, at a modest cost in terms of drop in delivery ratio and additional transmissions[1]. The approach is evaluated with attacks by adversaries that behave in a similar manner to fair nodes when invoking protocol actions. Debdutta Barman Roy, Rituparna Chaki and Nabendu Chaki 2009 BHIDS: a new, cluster based algorithm for black hole IDS In this paper, they present a new, cluster based Black Hole Intrusion Detection System (BHIDS) for mobile, *ad hoc* networks. The features that are considered for BHIDS include mobility of nodes, ariation in number of attacking nodes, packet delivery rate, density of the network, etc. The nodes in the network form a two-layered cluster[2]. This helps splitting the processing and communication overhead between the cluster heads at Layer 1 and 2. The proposed IDS algorithm has been tested on a simulated network using the NS simulator. The performance graphs show marked improvement as far as packet dropping is concerned. Hidehisa Nakayama, Nirwan Ansari , Abbas Jamalipour and Nei Kato 2007 Fault-resilient sensing in wireless sensor networks In this paper, based on clustering and routing optimization algorithms, they propose a new scheme called K-means and TSP-based mobility (KAT mobility). After clustering the sensor nodes, the proposed method navigates the mobile sink to traverse through the cluster centers according to the trajectory of an optimized route[3]. The mobile sink then collects the data from sensors at the visited clusters. Simulation results have demonstrated that the proposed scheme can provide not only better energy efficiency as compared to those obtained by conventional methods which assume random waypoint for the mobile sink, but also fault-resilience in case of malfunctions of some sensors due to attacks. J. Martin Leo Manickam and S. Shanmugavel 2007 Fuzzy Based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET In this paper, they evaluate the performance of their proposed Fuzzy based Trusted AODV routing protocol in a network, with varying number of malicious nodes. With the help of simulations, they demonstrate that the performance of the proposed protocol is better than AODV in terms of routing overhead ratio, throughput, latency and packet loss under similar attack conditions[4][5].

Carl Larsen and Maciej Zawodniok [8] Congestion in wireless sensor networks (WSN) may lead to packet losses or delayed delivery of important information rendering the WSN-based monitoring or control system useless. In this paper a routing-aware predictive congestion control (RPCC) yet decentralized scheme for WSN is presented that uses a combination of a hop by hop congestion control mechanism to maintain desired level of buffer occupancy, and a dynamic routing scheme that works in concert with the congestion control mechanism to forward the packets through less congested nodes. The proposed adaptive approach restricts the incoming traffic thus preventing buffer overflow while maintaining the rate through an adaptive back-off interval selection scheme.

Yao H. Ho , Kien A. Hua, Ning Jiang [14] In a Mobile Ad Hoc Network (MANET), communication connections need to adapt to frequent unpredictable topology changes due to the mobility, energy constraints, and limited computing power of the mobile hosts. we address this weakness by applying a cross-layer design, where the physical and MAC layer knowledge of the wireless medium is shared with higher layer, in order to provide efficient methods of establish and maintain routes. We proposed two connectionless-oriented dynamic route diversion techniques; and give simulation results, based on GloMoSim, to illustrate their performance advantage

Arabinda Nanda, Amiya Kumar Rath and Saroj Kumar [5] Rout. This paper presents a dynamic discover routing method for communication between sensor nodes and a base station in WSN. This method tolerates failures of arbitrary individual nodes in the network (node failure) or a small part of the network (area failure). Each node in the network does only local routing preservation, needs to record only its neighbour

Nodes' information, and incurs no extra routing overhead during failure free periods. It dynamically discovers new routes when an intermediate node or a small part of the network in the path from a sensor node to a base station fails.

We are trying to find all possible loops and eliminate the loops as far as possible in WSN.

III PROBLEM DEFINATION

We design intrusion detection system to detect the black hole attack on AODV in MANETs. This detection system is based on FUZZY LOGIC. The major issue in various detection systems is the use of only one factor for the identification of misbehavior of a node and also some detection systems use centralized approach for the detection purpose. We proposes a system in which the improvement is by making use of two factors i.e. destination sequence number and forward packet ratio for the detection system. We will use both these factors using Fuzzy Logic, which is a problem solving control system methodology. Fuzzy Logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, impressive, noisy or missing input information.

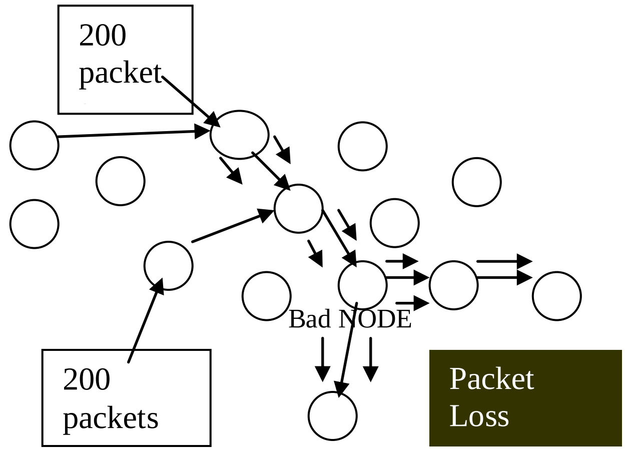

Figure 1: Heavy traffic load on Bad node

One of such implemented approach is to perform the blackhole detection, In such case the load will be shared by other nodes. The proposed algorithm to detect the blackhole attack is given as under

```
BlackHoleDetect(S,D)
/* S is the source node and D represents the Destination Node over the network*/
{
1) As transmission begin it will search for all the intermediate nodes and send data on to it.
2) Tthe intermediate node failed forwarding the probe message to the next node;
3) Fuzzify the Communication Rate on each Neighbor Node it will check the RESPONSE time for the intermediate node
        If(FuzzyRule(Response Time)> HIGH)
        {
        The Attacker Node is Detected.
        Update Neighbor Node Table & Routing Table for the Intermediate Nodes
        }
4) The unresponsive node is incapable of responding to the probe message.
5) The diagnosis algorithm will then be called to decide which one is the case.}
```

V CONCLUSION

The given purposed research will provide the solution of packet loss in case of blackhole attack over the network. The purposed work will first detect the black hole node using fuzzy rule. The fuzzy rule is implemented on response time of node communication. Now instead of transferring data on this node, it will be passing on from the surrounding nodes; it will only handle the transmission that is directed to it only. The algorithm will provide the better solution for reducing the data loss over the network

REFERENCES

1. Proceedings of IEEE GLOBECOM '01, 2001-11.K Whitehose, D Culler. Calibration as Parameter Estimation in Sensor Networks [C]. In: First ACM International Workshop on Wireless Sensor Networks and Application, Atlanta GA, 2002-09.
2. An Overview of Wireless Sensor Network and Applications V. Rajaravivarma, Yi Yang, and Tang Yang Computer Electronics, School of Technology 0-7803-7697-8/03/$17.000 2 008 IEEE
3. Ye W, Heidemann J, Estrin D, applications of wireless sensor networks. In: Proc 21St Int'l Annual Joint Conf IEEE Computer and Communications Societies (INFCOM 2002), New York, NY, June 2002.
4. Low Power Locating Algorithms For Wireless Sensors Network , Xiang-zhong Meng, Bing Wu, Hui Zhu and Yao-bin Yue Xiang-zhong Meng Proceedings of the 2006 IEEE
5. Node Sensing & Dynamic Discovering Routes for Wireless Networks Arabinda Nanda, Amiya Kumar Rath and Saroj Kumar (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010
6. Topological Hole Detection in Wireless Sensor Networks and its Application Stefan Funke Computer Science Department Gates Bldg. 375Stanford University, CA 94305, U.S.A.
7. Energy Aware Routing for Low Energy Ad Hoc Sensor Networks Rahul C. Shah and Jan M. Rabaey
8. Route Aware Predictive Congestion Control Protocol for Wireless Sensor Networks Carl Larsen, Maciej Zawodniok, Member, IEEE, and Sarangapani Jagannathan, Senior Member, IEEE Singapore, 1-3 October 2007.

AUTHORS PROFILE

Poonam yadav received her B.E degree in 2009from Department of Instrumentation & Control Engineering P.D.M, College of Engineering, bahadurgarh Haryana, India and pursuing her M.Tech degree from MDU ,rohtak, India. She is currently working as research scholar in Department of Electronics and Communication, GITM bilaspur, Haryana .Her research interest includes Wireless Communication and Digital Communication. She has 3 Years of teaching experience and had guided several B. Tech project.

Mr. Rakesh Kumar Gill obtained Master of Science (M.Sc.) in Electronics Science from Kurukshetra University, Kurukshetra in 2004. He received Master in Technology (M.Tech.) in ECE from Kurukshetra University, Kurukshetra in 2007. Currently, working at Gurgaon Institute of Technology and Management (GITM), Gurgaon as an Assistant Professor since 2007. He has published 3 research papers in national journal and conferences. The area of research is communication and VLSI design. He is member of ISTE.

Naveen kumar, received his B.E degree in 2008 from Department electronics & Communication Engineering Somany institute of tech & mngt., rewari, Haryana, India and pursuing his M.Tech degree from MDU,rohtak , India. He is currently working as research scholar in Department of Electronics and Communication, GITM bilaspur , haryana. His research interest includes Wireless Communication and Analog electronics. He has 4 Years of teaching experience and had guided several B. Tech project.