www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11854-11858

Black Hole detection and avoidance in mobile Adhoc Networks

Asha Guddadavar , Bagali Ashvini A

Computer Networks
Siet,
Bijapur, Karnataka, India
Guddadavar.Asha03@Gmail.Com

Digital Communication And Networking.
Bldea College Of Engineering,
Bijapur,Karanataka,India
Aa.Bagali90@Gmail.Com

***Abstract*— The paper evolved out to address issues in MANET like security and performance. This paper proposes a cluster based concept to improve security and efficiency and guarantees the optimum utilization of the network resources. Performance proposed of MANET in presence of black hole attack. The simulation of the proposed methodology is carried out using NS2 network simulator and the simulation results reflects the performance of scheme for detection and prevention of the black hole.**

Keywords—MANET; blackhole; performane; security; NS2; performance.

I. INTRODUCTION

An ad hoc network is a wireless network without any fixed infrastructure. It is a group of mobile hosts without the required involvement of any offered infrastructure or centralized access point such as a base station. There are various challenges that are faced in the Ad hoc environment. AODV [1] is an on demand routing network protocols which is specially design for Ad hoc network. Ad hoc network offer great flexibility, higher throughput, lower operating cost and better coverage because of collection of independent nodes. Mobile ad hoc networks consist of mobile nodes, which can communicate with each other and nodes can enter and leave the network anytime due to the short transmission range of MANETs, routes between nodes may consist of one or more hops.

Thus each node may either work as a router or depend on some other node for routing. Fig 1 below shows a simple ad hoc network with three mobile hosts using wireless interfaces. Host A and C are out of range from each other's wireless transmitter. When exchanging packets, they may use the routing services of host B to forward packets since B is within the transmission range of both of them. [2]

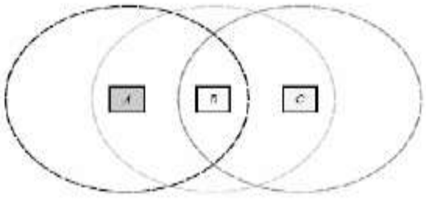

Fig 1: Mobile ADHOC with 3 mobile nodes

According to observations there are two main issues first security and second is performance. This project focuses on the MANET security. A passive attack does not disrupt proper operation of the network. Attacker watches data exchanged in network without altering it. The requirement of privacy can be violated if an attacker is also able to interpret the data gathered. Discovery of passive attacks is very difficult for the operation of the network itself does not get affected. A way of preventing this kind of problems is to use powerful encryption mechanisms to encrypt the data being conveyed, thus making it impossible for eavesdroppers to obtain any useful information from the data overheard. An active attack tries to alter or destroy the data, thus the normal functioning of the network is disrupted. These can be classified into two categories external attacks and internal attacks**.** External attacks are supported by nodes that do not belong to the network. These attacks prevented by using standard security mechanisms such as encryption techniques and firewalls. In internal attacks compromised nodes that are actually part of the network. Meanwhile the attackers are part of the network as authorized nodes, by the property internal attacks are more severe and difficult to detect when compared to external attacks

II. ATTACKS ON MANET

A. ACTIVE ATTACK

Black hole Attack**:** In this attack, a malicious user uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Attacker receives the requests for routes in a flooding based protocol. While attacker receives a route request to the destination node, it creates a reply consisting of a short route. If attacker's reply reaches the initiating node before the reply from the actual node, a fake route gets created. If the malicious device has been able to insert itself between the communicating nodes, then this node is able to do anything with the packets. It can drop the packets between them to perform a denial-of-service attack, or otherwise use its place on the route as the first step in a man-in-the-middle attack. [3]

In Black hole attack more than one node can be malicious. Paper proposed a novel architecture of A Forced Routing Information Modification Model prevents Black hole attacks in wireless MANET by introducing automatic error correction in routing information that leads the node to select correct path thus secure transmission will take place between source and destination**.** In this model they assume that network is centralized. Routing protocol AODV is used. Two technologies are used for communication between sever and access points and the access points to nodes. This leads the node to modify its routing table, so node will divert its traffic towards access point and the communication will be started between node and server through access point. The black hole attack has been met, using automatic modification in the routing table of node.

Each node in MANET has to rely on each other in order to forward packets, so highly supportive nodes are required to ensure that initiated data transmission process. However, it is hard to encourage cooperativeness among nodes for each node owns limited resources that need to be secure. These specific nodes are also known as selfish nodes refuse to help other nodes in forwarding packets due to the anxiety of having resource degradation such as exhausted battery power and limited processor ability. This issue has aroused several issues in MANET: routing, security, Quality of Service (QoS), resource management and auto-configuration.

*B. **DoS ATTACK***

DoS attack possible in wireless ad-hoc networks, in this attack; an attacker sends a false RREP packet to a source node that initiated a route discovery, posing itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward all of its data packets to the attacker, which originally was intended for the genuine destination. The attacker, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other. The attacker’s device will be referred to as a malicious node (i.e. black hole attack). [3]

III. MOTIVATION

In Black hole attack more than one node can be malicious. Proposed model is a novel architecture of A Forced Routing Information Modification Model prevents Black hole attacks in wireless MANET by introducing automatic error correction in routing information that leads the node to select correct path thus secure transmission will take place between source and destination. In this model they assume that network is centralized. Popular protocol AODV is used.

There are various challenges that are faced in the Ad hoc environment. AODV is an on demand routing network protocols which is specially design for Ad hoc network. Ad hoc network offer great flexibility, higher throughput, lower operating cost and better coverage because of collection of independent nodes. [4]

IV. RELATED WORK

A. Clustering of MANET

The proposed approach is provides a clustered organization of MANET devices, where devices are categorized in the following manner.

- **Mobile nodes**: These nodes are collection of the mobile devices and follow the law of independent mobility. These nodes are frequently participating in communication. Additionally able to send, receive and route data during communication.
- **Cluster heads:** These nodes are basically static access points which installed separately. These nodes are participating in communication when intra-cluster communication occurs. [5] The primary objective of these cluster heads, to monitor the communication between trusted nodes, when new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes.
- **Monitoring server:** This device is used to calculate the trust value for securing the network from attack.

B. Node Arrangement

The arrangement of the nodes are given by fig 2, where arrangements of above given nodes are provided. On the basis of their functionality of network attack formation and detection process is described. Black hole attack is described in above sections, according to the characteristics of malicious node during black hole deployment, node just receive data packets but never forward further destination nodes. Thus if server only check all node activity for sending and receiving of packets then server is able to detect the malicious node.

<u>Important terms:</u>

- **SERVER**
- **CLUSTER HEADS**
- **MOBILE NODES**

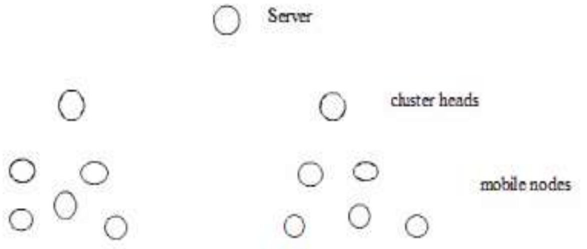

Fig 2: Node arrangement in MANETs

C. Prevention

To simulate the complete communication, detection process and elimination process of malicious node we provide three step scenarios.

1. **Communication between internal clusters**: In this scenario mobile nodes are communicating with each other, As the MANET devices communicating.

2. **Communication between external clusters:** During this process all the generated traffic is go through the clusters and server node. By which the nodes and traffic flow is monitored.

3. **Communication between unknown nodes:** During this communication first time traffic are flows according the second scenario, and traffic and data monitored. If this node only receives packets and never forward the packets to neighbor nodes then this node is eliminated from the network and marked as malicious node.

V EXISTING SYSTEM

An active attack tries to alter or destroy the data, thus the normal functioning of the network is disrupted. These can be classified into two categories external attacks and internal attacks. External attacks are supported by nodes that do not belong to the network. These attacks prevented by using standard security mechanisms such as encryption techniques and firewalls. In internal attacks compromised nodes that are actually part of the network. Meanwhile the attackers are part of the network as authorized nodes, by the property internal attacks are more severe and difficult to detect when compared to external attacks. [6] [7]

Attacker receives the requests for routes in a flooding based protocol. While attacker receives a route request to the destination node, it creates a reply consisting of a short route. If attacker's reply reaches the initiating node before the reply from the actual node, a fake route gets created. If the malicious device has been able to insert itself between the communicating nodes, then this node is able to do anything with the packets. It can drop the packets between them to perform a denial-of-service attack, or otherwise use its place on the route as the first step in a man-in-the-middle attack.

A. DISADVANTAGES OF EXISTING SYSTEM

1. The node to modify its routing table, so node will divert its traffic towards access point and the communication will be started between node and server through access point.
2. Cluster infrastructure not maintained in existing system (i.e. randomly nodes are deployed therefore no secure communication).
3. Malicious user uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. So there will be packet drop (:packet loss)

VI PROPOSED SYSTEM

The proposed approach is provides a clustered organization of MANET devices, where devices are categorized in the following manner. Then paste down the

*a) **Mobile nodes:** These nodes are collection of the mobile devices and follow the law of independent mobility. These nodes are frequently participating in communication. Additionally able to send, receive and route data during communication.*

*b) **Cluster heads:** These nodes are basically static access points which installed separately. These nodes are participating in communication when intra-cluster communication occurs. The primary objective of these cluster heads, to monitor the communication between trusted nodes,*

when new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes.

*c) **Monitoring server:** This device is used to calculate the trust value for securing the network from attack. That is performed using MANET Black hole characteristics.*

B. Advantages of proposed system

1) To simulate the complete communication, detection process and elimination process of malicious node we provide three step scenarios.

- **Communication between internal clusters:** In this scenario mobile nodes are communicating with each other, As the MANET devices communicating.
- **Communication between external clusters:** During this process all the generated traffic is go through the clusters and server node. By which the nodes and traffic flow is monitored**.**
- **Communication between unknown nodes:** During this communication first time traffic are flows according the second scenario, and traffic and data monitored. If this node only receives packets and never forward the packets to neighbor nodes then this node is eliminated from the network and marked as malicious node. [8]

2) Proposed system provides a cluster oriented infrastructure for monitoring and communicating the mobile devices. [9]

3) In the proposed system we make cluster head for each cluster: which is used to monitor the communication between trusted nodes, when new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes**.**

4) Monitoring server: This device is used to calculate the trust value for securing the network from attack [which is not used in existing].

VII EXPERIMENTAL RESULTS

This section of paper emphasis on results obtain after simulation of black hole detection and avoidance TABLE I below lists the simulator parameters ad its value on which simulation is carried on NS2.

TABLE I. SIMULATION PARAMETERS

Properties	***Values***
Simualtion Area	800X800
Number of Nodes	20
Node Type	wireless
Mobiltiy	Random
LinkLayer	LL
MAC Layer	802.11
Antenna	Onmi
Channel	Wireless

On above configured wireless node configurations Fig 2 depicts a scenario of black-hole nodes, which fools nodes of the topography by false advertising itself as nearest node to destination , hence all nodes forward packets to back-hole node which in turn start dropping all packets.

C.

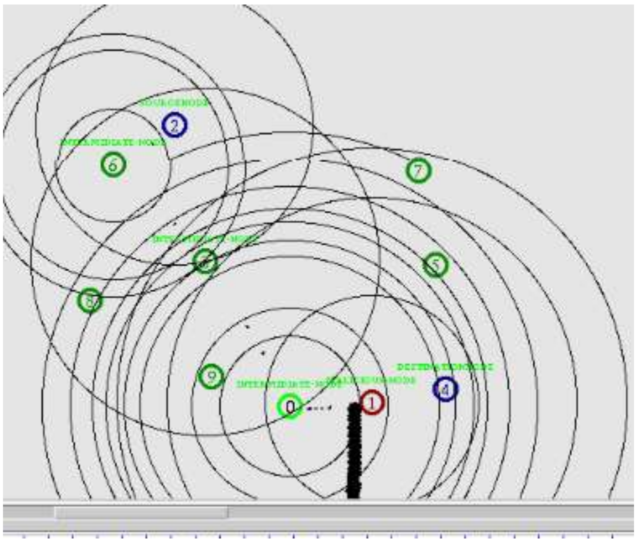

Fig 3: Packet drop due to black hole attack

During attacks no packets flow between source and destination and throughput is zero for said reason. Proposed system detects the attacker and avoids the throughput to become zero

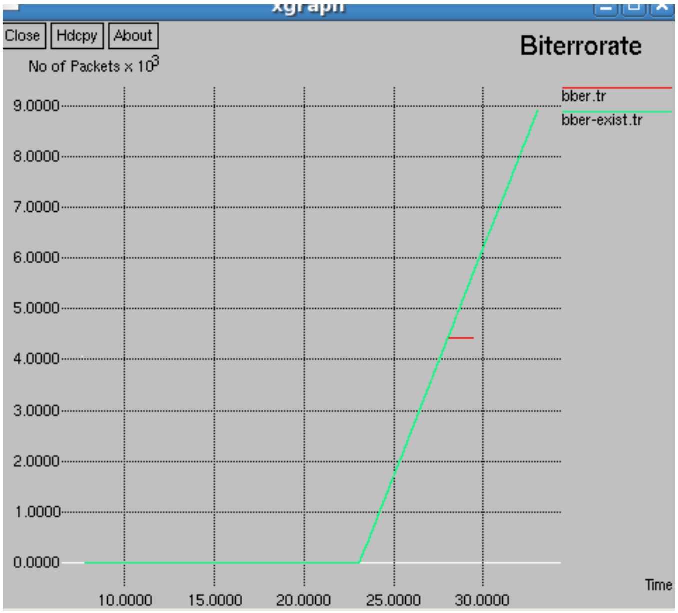

Fig 4: Bit Error Rate

Fig 5, below shows the overhead packet been exchanged in network for avoiding the black hole attack in MANETS. And Fig 6, below shows the PDR (Packet Delivery Ration) comparison between Black hole attacked network topology and same topology with avoids black hole attack according to the proposed model

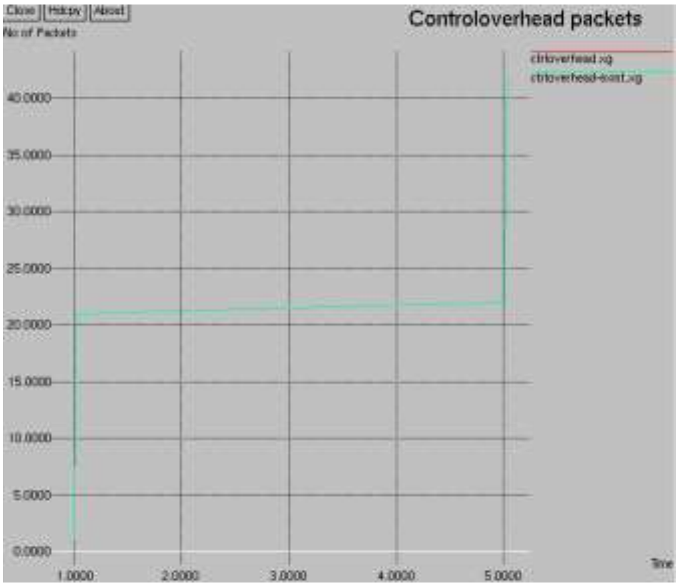

Fig 5: control over packet while avoiding Black hole attack

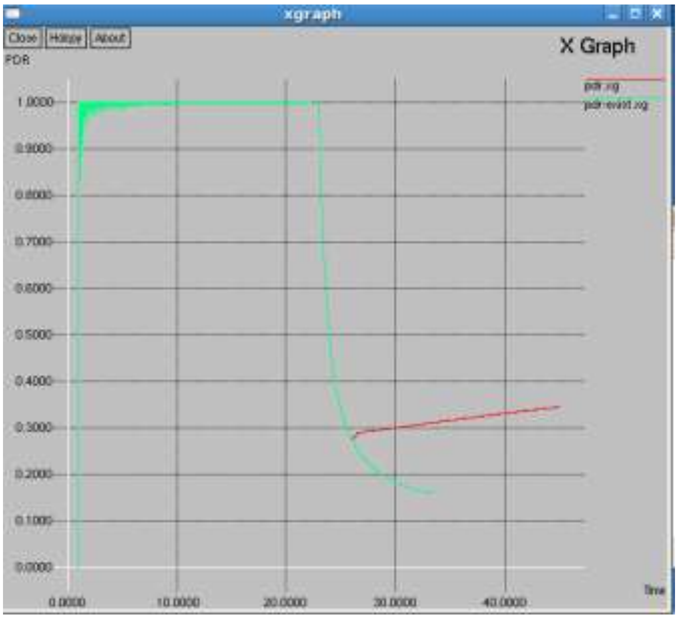

Fig 6: Packet Deliver Ratio Comparison on attack and after attack avoidance

REFERENCES

[1] A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, Sudhir Agrawal, Sanjeev Jain, Sanjeev Shanna, JOURNALOF COMPUTING, VOLUME 3, ISSUE I, JANUARY 2011, ISSN 2151-9617.

[2] A Survey of Mobile Ad Hoc Network Attacks, PRADlP M. JA W ANDHIY A, MANGESH M. GHONGE, DR. M.S.AU, PROF. J.S. DESHPANDE, International Journal of Engineering Science and Technology, Vol. 2(9), 2010, 4063-4071.

[3] A Joint Design for Topology and Security in MANETs with Cooperative Communications, Quansheng Guan, F. Richard Yu, Shengming Jiang and Victor C.M. Leung, 978-1-61284-231-8/111$26.00 ©2011 IEEE.

[4] SOPE: Self-Organized Protocol for Evaluating Trust in MANET using Eigen TrustAlgorithm, Sudharson Kumar,Parthipan.V,978-1-4244- 8679 3111/$26.00 ©2011 IEEE.

[5] Black Hole Attack and Their Counter Measure Based on Trust Management in Manet: A Survey, U. Venkanna, R.LeelaVe\usami, Proc. oflnt. Coni, on Advances in Recent Technologies in Communication and Computing 2011.

[6] A trust based approach for AODV protocol to mitigate black hole attack in MANET, Fidel Thachil, K C Shet, 978-0-7695-4817-3/12 $26.00 © 2012 IEEE.

[7] A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network, Muhammad Raza I and Syed IrfanHyder, 978-1-4577-1929-5112/$26.00 ©20 I I IEEE.

[8] A Friend Mechanism for Mobile Ad Hoc Networks, ShukorAbdRazak NormaliaSamian, MohdAizainiMaarof, 978-0-7695-3324-7/08 $25.00 © 2008 IEEE, DOl 10.11 09/IAS.2008.27.

[9] Survey of clustering algorithms for MANET, RatishAgarwal, Dr. Mahesh Molwani, 1 International Journal on Computer Science and Engineering Vol.I(2), 2009, 98-104.