Clustering Technique to Secure MANETs From Black Hole Attack

Mrs. Poornima B
IV Sem M. Tech Digital Communication & Networking
T. John Institute of Technology
Bengaluru, India

Mrs. Kalpana P S
Assistant professor, Dept. of ECE
T. John Institute of Technology
Bengaluru, India

***Abstract*—The goal of this project is to addresses Black Hole related security and performance issues in MANET. A cluster oriented concept is proposed to enhance security and efficiency that ensures optimum performance of MANET during black hole attack.Mobile Adhoc Network (MANET) consists of a collection of mobile nodes which do not require intervention of any existing infrastructure or centralized access point as base station. MANET routing protocol are mainly responsible for communication between mobile nodes. These Routing Protocols are highly vulnerable to various attacks on layers of OSI model. Therefore security of routing protocol becomes must. Major concentration in this project is on black hole attack, and attempt to show how black hole attack is prevented in MANET. The simulation of the proposed methodology is carried out using NS2 network simulator and the simulation results reflect the performance of scheme for detection and prevention of the black hole attack.**

Keywords—Computer Network; NS2 Simulator; MANET; Black Hole Attack

I. INTRODUCTION

The network simulators are used for performance analysis in the field of communication. With the help of simulation tools, both the time and cost of testing the functionality of network could be reduced and implementations are made easy.

NS2 simulator could be used to simulate various scenarios. However, the scope of this paper will be limited to study its significance in addressing Black Hole related security and performance issues in MANETs.

This methodology is simulated using NS2 simulator and the results reflect the performance of scheme for detection and prevention of the black hole attack.

Mobile Ad-hoc Networks, as it is often referred to as MANET, can be defined as mobile nodes organized in a dynamic topological infrastructure.Due to high mobility model MANET is mainly affected by two issues - security and performance. This paper focuses on the MANET security.

There are a number of methods and techniques available to provide the security for MANET environment. Clusteringtechnique enhances security and efficiency that ensures optimum performance of MANET during black hole attack.AODV is an on-demand routing network protocol which is specially designed for Ad-hoc networks and to implement Clustering technique. This paper intends to use NS2 simulator as an infrastructure for monitoring and communicating the mobile devices and prevent black-hole attack.

II. PROBLEM STATEMENT

A. Black Hole Attack

Black hole and wormhole is categorized as active 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 false route gets created.

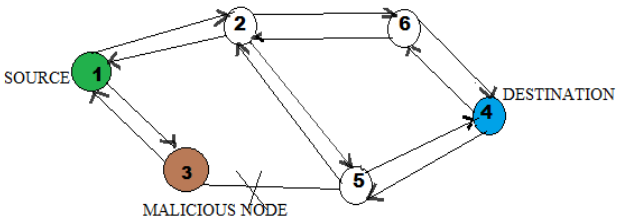


Fig 1. Black hole attack

B. Routing Protocols

Routing protocols can be divided into three groups. Proactive, reactive and hybrid protocols, depending on its routing topology. Proactive protocols are usually table driven. Examples: Optimized link state routing (OLSR), Destination Sequence Distance Vector (DSDV) protocols. Reactive or source initiated on demand protocols, they do not periodically update the routing information. It is transmitted to the nodes only when necessary. Example: Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example: Zone Routing Protocol (ZRP).

C. Related Work

Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks.

SudhirAgrawal, Sanjeev Jain, Sanjeev Shanna[1], proposed a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. In this method every node monitors neighboring nodes and calculates trust value on its neighboring nodes. If calculated trust value of a monitored node goes below defined threshold value previously, then the monitoring node assume it as malicious and avoids that node from the route path.

The test discloses that proposed scheme secures the AODV routing protocol for MANET by mitigating and avoiding black hole nodes.

Sudharson Kumar, Parthipan[2]developed a trust management scheme for securing the MANET. According to author Evaluating and quantifying Reputation stimulates collaboration in Mobile ad hoc Network (MANET). Absence of infrastructure nodes here to cooperate in order to provide the necessary network functionality, the given study is provides fully distributed reputation-based mechanisms that improve security in MANETS. That is implemented over cognitive and optimized method to calculate the Reputation of the Nodes. This study proposes Eigenvector & Degree centrality for evaluation of trust value. Simulation is given using NS2 over the Dynamic Source Routing (DSR) prototype, in the existence of Worm Hole Attack in highly mobile and hostile environment.

Survey of clustering algorithms for MANET, RatishAgarwal, Dr. Mahesh Molwani[3], proposed a methodical classification of these clustering schemes enables to better understand and make improvements. In MANET movement of nodes may quickly change the topology resulting in the increase of the overhead message in topology conservation. Protocols try to keep the number of nodes in a cluster around a predefined threshold to facilitate the optimal operation of the MAC protocol. The cluster head selection is invoked on-demand, and is targeted to reduce the communication costs.

III. The Proposed Algorithm

The proposed approach provides a clustered organization of MANET devices, where devices are classified in the following manner:

A. Simulation Methodology for Network Analysis

- Mobile nodes: These nodes are collection of the mobile devices and follow the law of independent mobility. These nodes are frequently participating in communication. It can be 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. The main objective of these cluster heads, to observe 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.Cluster heads (CH) are identified based on their residual energy and monitoring server by least packets dropped.

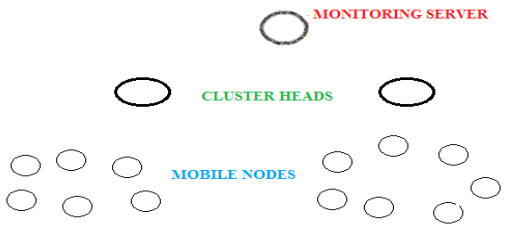


Fig 2. The proposed network

The arrangement of the nodes, cluster heads and monitoring servers are given in Fig 2. On the basis of their functionality of network, attack establishment 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.

B. Clustering Technique to Prevent Black-hole Attack

To simulate the entire communication, detection processand 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 in network.

- **Communication between external clusters:** During this process all the generated traffic goes through the clusters and server node. Server nodes monitor the nodes and traffic flow is observed.

- **Communication between unknown nodes:**During this communication traffic are flows according the second structure, 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.

IV. Experimental Results

This section of the given paper provides the implementation and obtained results from the simulation. NS2 network simulation which is given in this paper is based on the below given setup:

Properties	Values
Simulation area	1000X1000
Number of nodes	43
Node type	Wi-Fi
Mobility	Random2way
Link layer	LL
Mac layer	802_11
Channel	Wireless

TABLE I The Simulation Parameters

A. *Throughput*

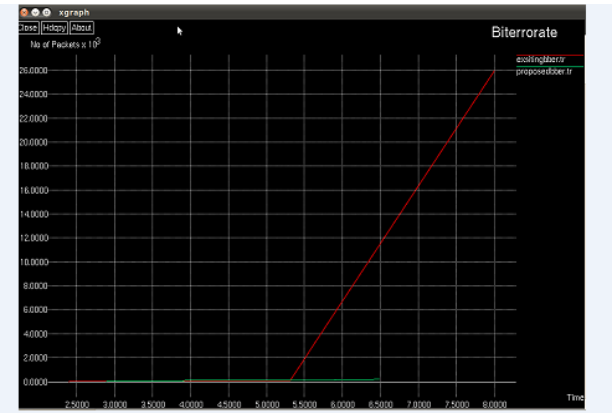
Throughput is the average rate of successful message delivery over a communication channel. This gives the fraction of the channel capacity used for data transmission. The graph for Throughput is shown.

B. *Packet Delivery Ratio*

Packet Delivery Ratio is Ratio of total number of packets received at the destination to the total number of packets sent. Under normal circumstances packet drop rate is zero percent. When the attack is launched its value goes to peak and after prevention of black hole attack drop rate start decreasing at rapid rate.

C. *Bit Error Rate*

The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Using this proposed method BER is almost constant is as shown in graph.



V. CONCLUSION

Using NS2 simulator, security and performance parameters in MANET can be successfully implemented and monitored. Clustering technique was simulated using NS2 Simulator to successfully enhance security and efficiency strategy and to ensure optimum performance of network in presence of black hole attack.

ACKNOWLEDGMENT

The author would like to thank the staff and students of the Electronics and Communication Department, T. John Institute of Technology for their guidance and support during the course work.

REFERENCES

[1] A Survey of Routing Attacks and Security Measures in Mobile Ad-HocNetworks, **Sudhir Agrawal, Sanjeev Jain, Sanjeev Shanna**, JOURNALOF COMPUTING, VOLUME 3, ISSUE I, JANUARY 2011, ISSN2151-9617

[2] 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

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

[4] Clustering of Mobile Ad Hoc Networks: An Approach for Black Hole Prevention, **Jitendra Sayner, Vinit Gupta**, 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), February 2014, INSPEC Accession Number: 14210937

AUTHOR PROFILE

Mrs. Poornima B is pursuing M.Tech degree in Digital Communication & Networking from T. John Institute of Technology, Bengaluru from Visvesvaraya Technological University. Her research interests include Computer Networks, MANET, Wireless Communication and Network Security.

Mrs. Kalpana P S is currently working as an Assistant Prof. at T. John Institute of Technology, Bengaluru. Her research interest includes routing and security in Advanced Computer Networks and MANETS.