International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 10, October-2015

Detection of Black Hole for Improving Efficiency of MANET using Energy-based Clustering

Madhura S D[1],
[1]M.Tech, CS&E,
Malnad College of Engineering,
Karnataka, India

Dr. B. Ramesh[2]
[2]HOD Department of CSE,
Malnad College of Engineering,
Karnataka, India

Abstract:- **MANET is a self configuring network which consists of wireless mobile nodes. In MANET for establishing a route each node acts as a router. Due to this mobility, providing security is the major issue in MANET as the network is prone to numerous attacks. Black hole attack is one such attack where the malicious node drops the packet in the network by giving false replay for a request and does not contain any path to the destination. To improve efficiency and security of the network, cluster oriented concept is proposed, where clustering approach in AODV routing protocol for preventing black hole is used. The simulation is done using NS2 network simulator.**

INTRODUCTION

Mobile Ad-hoc network (MANET) consists of numerous mobile nodes which has the capacity to perform various functions like routing, service discovery and packet forwarding without an established infrastructure.

The nodes in MANET are interdependent which helps to forward packets from source to destination. Thus, for transmission of packets in the network there is a need for quick deployment of the nodes to establish a route, which is an important issue in MANET. There are various routing protocols. Mainly routing protocols are divided into three different categories: Proactive protocols, Reactive protocols and Hybrid protocols.

Proactive routing protocols: In this type, a table is maintained which consists of list of all possible destination nodes and frequently exchanges routing messages, so that the information in the routing table is up-to-date is correct. These protocols are also called as table-driven protocols. Examples of proactive protocols are OLSR, DSDV protocol.

Reactive protocols are also called as On-Demand routing protocols, because only on demand route determination procedure is invoked. That means, when there is a need for data packets transmission then only routes are determined between the nodes. Examples are AODV and DSR protocols.

Hybrid protocols combine proactive with reactive protocols, so that to the destination best path is provided.

Attacks on MANET

There are mainly two different types of attacks:

Passive attack: Attacker does not actively participate in the network. It silently listens to the network so that it gets information about what is going on in the network.

Active attack: Attacker will act as an internal node in the network and thus by actively participating in the network it affects the normal operation of the network. Intruder may modify or drop the original packets. Black hole attack is one type of attack under active attack.

Black Hole Attack

Black hole attack is one type of attack that generally occurs in the Reactive protocols. A black hole node is the malicious node that attracts the packets by falsely claiming that it has shortest and fresh route to reach the destination. Thus, if the malicious node is able to insert itself between any communicating nodes, then this node is able to do anything with the packets. It can drop the packets between them, or otherwise use its place on the route as the first step in a man-in-the-middle attack.

Introduction to AODV

AODV is an On-Demand protocol which is used to determine the path to destination only after when there is demand for forwarding packets. All mobile nodes work in cooperation in finding path to destination, by using different control messages. Control messages are Route request (RREQ), Route Replay (RREP), Route Error (RERR) which are used to establish path to destination i.e., in route discovery process. Whenever a source node wants a path to destination then it broadcasts RREQ message which will be received by intermediate nodes of the source node. The intermediate nodes broadcast this RREQ message to neighbours, which is continued till the packet is received by destination node.

LITERATURE SURVEY

[1]A Survey of Attacks in MANET Manjeet Singh Research Scholar (Dept. of CSE) SGGSW University , Fatehgarh Sahib Punjab, India .Gaganpreet Kaur Assistant Professor (Deptt. of CSE) SGGSW University , Fatehga.

MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces In order to make communication among nodes, the nodes dynamically establish paths among one another. The nature and structure of such networks makes it attractive to various types of attackers. Security is a major concern for protected communication

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

between mobile nodes. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self-organizing capabilities, is some of MANET's biggest strengths, as well as their biggest security weaknesses.

[2]A Survey of routing attacks in mobile Ad hoc networks Bounpadith Kannahavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, Tohoku University Abbas Jamalipur, University of Sydney.

Recently, mobile ad hoc networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET is a particularly challenging task compared to a conventional network. Early work in MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, sever efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious. In this article, we investigate the state-of-the-art of security issues in MANET. In particular, we examine routing attacks, such as link spoofing as well as countermeasures against such attacks in existing MANET protocols.

[3]A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Network Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma.

Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. The absence of a central management agency or a fixed infrastructure is a key feature of MANETs. These the destination, to intimate the number of data packets it sends to the destination. Then packet count and transmitted data both are compared and the difference is found out.

PROPOSED METHODOLOGY

The whole network is divided into four numbers of clusters. They are categorized into three different types.

1. Cluster member: These members are the normal nodes that may communicate with each other. These nodes also help to route the packets within the network.

nodes communicate with each other by interchange of packets, which for those nodes not in wireless range goes hop by hop. Due to lack of a defined central authority, securitizing the routing process becomes a challenging task thereby leaving MANETs vulnerable to attacks, which results in deterioration in the performance characteristics as well as raises a serious question mark about the reliability of such networks. In this project we have attempted to present an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works.

[4]Towards Robust and Effective Trust Management for Security: A Survey Dongxia Wang, Tim Muller, Yang Liu, and Jie Zhang School of Computer Engineering Nanyang Technological University, Singapore.

There is a need for robust and effective trust management. Different security problems result in different requirements to the design of trust management, and the existing attacks in trust management for security are yet to be solved. In this project, we first propose a framework to classify desired properties of trust management for each type of security problems. We then investigate typical representative attacks and existing solutions in trust management for security. By considering both these security properties and attacks on trust management systems, our work serves to propel the design of more effective and robust trust management systems for security.

[5]"Detecting black hole attack on AODV protocol" Satoshi kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto.

A new detection method based on dynamically updated training data. Single black hole attack is prevented. Improvement over detection rate and false positive rate. AODV protocol is used but there is delay in the network.

[6] "Modified DSR protocol for detection and removal of selective black hole attack in MANET" M.Mohanapriya and L.Krishnamurthi.

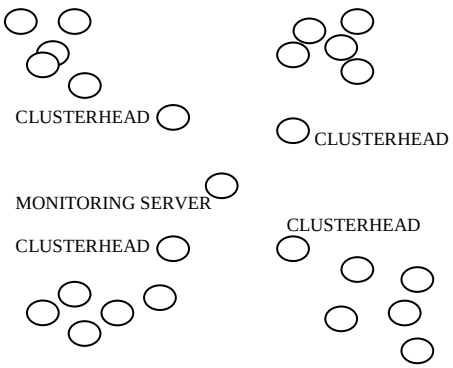
Modified Dynamic source Routing Protocol (MSDR) was presented to detect and prevent selective black hole attack. The source node selects the first shortest path to

2. Cluster Head: Cluster is also a node which is selected based on its residual energy. That means, the node with highest energy is selected as cluster head which monitors all nodes in its cluster.

3. Monitoring server: Server is monitoring the whole network. The node with least drop is selected as monitoring server. Server maintains information like distance, energy and of all nodes.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

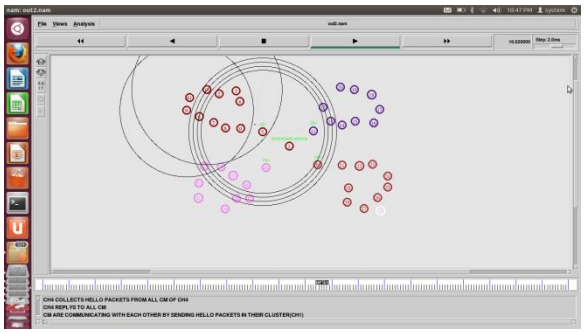
Schematic representation of all nodes in the network.



The clusters are formed randomly by selecting few nodes and from those nodes the cluster head and the monitoring node is selected based on parameters like highest residual energy and least drop. The design part of the network consists of a four cluster heads for each cluster and a monitoring node, such that the cluster head acts a check in and checkout point for the data flow that is transferring within and outside the network, and also monitors the data flow, the monitoring node acts as an overall supervision of the network.

Once the cluster formation is done the nodes in a cluster interact with each other and ping to cluster head and start establishing communications with it. The cluster heads and monitoring server is considered as trusted node, this enables secure routing in a MANET and limits the probability of vulnerability.

The source node starts data packets to destination. Cluster head checks the number of packets sent and received by each node. If there is difference and difference is greater than 30% then the node is considered as malicious node.



EXPERIMENTAL RESULTS

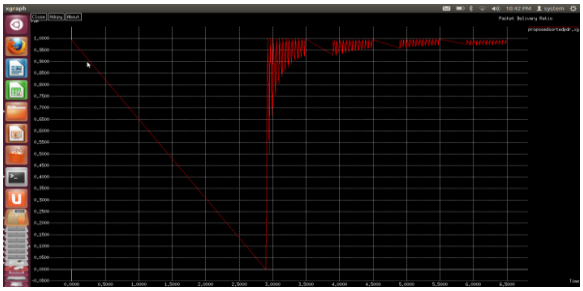
This section of the given paper provides the implementation and obtained results from the implemented simulation. NS2 network Simulation which is given in this paper is based on the below simulation setup.

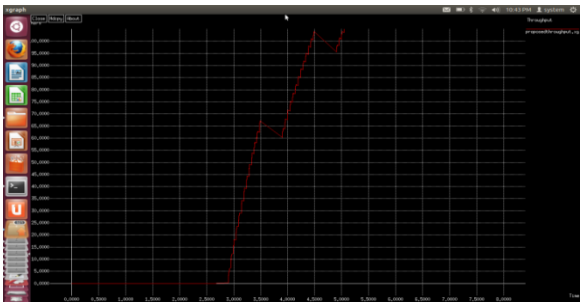
Simulation parameters

Parameter	Value
Simulator	NS-2
Number of nodes	42
Channel	Wireless channel
Traffic type	CBR
Routing Protocol	AODV
MAC type	802.11 MAC layer
Packet size	256 bytes

Throughput: The number of packets delivered per second

Packet Delivery Ratio: The number of packets delivered with respect to time.





CONCLUSION

Black hole attack is a major security problem of mobile adhoc Network (MANET). In this paper, we have presented an approach to detect such type of attack by having cluster infrastructure. This mainly focuses on secured and efficient mechanism to prevent Black hole attack in such a way that the throughput and packet delivery ration can be increased.

REFERENCES

[1] A Survey of Attacks in MANET Manjeet Singh Research Scholar (Deptt. of CSE) SGGSW University , Fatehgarh Sahib Punjab, India .Gaganpreet Kaur.

[2] A Survey of routing attacks in mobile Ad hoc networks Bounpadith Kannahavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, Tohoku University Abbas Jamalipur, and University of Sydney.

[3] A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Network Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma.

[4] Towards Robust and Effective Trust Management for Security: A Survey Dongxia Wang, Tim Muller, Yang Liu, and Jie Zhang.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)