Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Detection and Isolation of Malicious and Hostile Nodes in MANETS

**Dr. Nasib Singh Gill*, Ekta**

*Department of Computer Science and Applications*

*&Maharishi Dayanand University, Rohtak, India*

***Abstract—A Mobile Ad-hoc Network (MANET) is a Wireless Technology. It consists of self organising Mobile nodes which consist of mobile transceiver. With the revolution in networking technology it's widely used in each and every sphere of life. Manets as infrastructureless networks are more prone to the attacks on their vulnerabilities. This paper consists of a detection of malicious nodes in the networks which leads to the jamming and often exhaust all channel resources. It introduces a new approach to detect and isolate the malafide nodes in the MANET networks keeping Delay and throughput of the network under consideration.***

***Keywords— MANET; Mobile nodes; Malicious nodes; delay; throughput***

## I. INTRODUCTION

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Now a days, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they approach each other. This allows e.g. participants at a meeting to share documents, presentations and other useful information. This kind of spontaneous, temporary network referred to as mobile ad hoc networks (MANETs) sometimes just called ad hoc networks or multi-hop wireless networks, and are expected to play an important role in our daily lives in near future. A MANET is combination of two words mobile (means portable) and adhoc (means temporary) which are oftenly used in mobile networking also called "short live" networks. In today's networking era, wireless technology is using the concept of mobile nodes which consists of inbuilt wireless-mobile routers and transceivers. Due to its infrastructureless nature, the mobile nodes are self organising and self configuring. The topology of the network varies automatically and maintained by nodes itself according to the present geographic position of the mobile nodes in the adhoc network. The performance of the MANETS depends on the routing protocols, battery consumption and bandwidth etc. There are several routing protocols used in MANETS which are widely categorised into two categories of reactive and proactive protocols. The open Medium, Dynamic characteristics and lack of central infrastructure as in infrastructure networks makes MANETs more receptive to various security threats that deteriorate the performance of the networks in terms of reliability and throughput of the network. Many times system vulnerabilities were exploiting by some hostile nodes which were often coined as malicious node. Thus, when a node breaches any of the security principles and is therefore under any attack then the behaviour of such node is said to be malicious. Several attacks were studied on MANETs by the researches which lead to the low system performance and leads to the wastage of system resources. Whereas several proposals were also made to detect the malicious nodes in the system. With the advent of changes in the technology the threats are increasing at a wide range which leads to the jamming of the network.

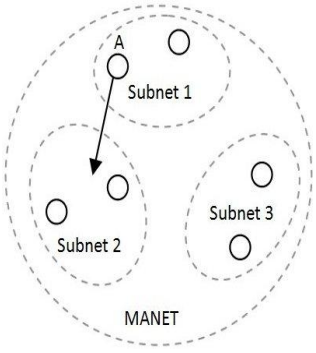


Fig.1 Example of an MANET network

## II. MANET STATUS

Ad hoc networking is not a new concept. As a technology for dynamic wireless networks, it has been deployed in military since 1970s. Commercial interest in such networks has recently grown due to the advances in wireless communications. A new working group for MANET has been formed within the Internet Engineering Task Force

 

(IETF), aiming to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments and develop a framework for running IP based protocols in ad hoc networks. The recent IEEE Standard 802.11 has increased the research interest in the field. Many international conferences and workshops have been held by e.g. IEEE and ACM. For instance, Mobil ad Hoc (The ACM Symposium on Mobile Ad Hoc Networking & Computing) has been one of the most important conferences of ACM SIGMOBILE (Special Interest Group on Mobility of Systems, Users, Data and Computing). Research in the area of ad hoc networking is receiving more attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and significant contributions [1].

## III. VULNERABILITIES IN MANETS

There are several vulnerabilities in the MANETs [2, 7]. Some of them are as following:-

- Unsecured Boundaries
- Compromised Nodal Threat
- Non availability of centralised Management facility
- Limited power supply
- Scalability

## IV. CONSIDERED NETWORK FEATURES

- PACKET DELIVERY RATIO (PDR): The ratio of the delivered packets at destination node to the sent packets by the source node.

- DELAY: The total time that a packet takes to reach its end –point destination.

- THROUGHPUT: The total amount of the packets passing through a network.

## V. ATTACKS IN MANETS

Securing mobile ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.[3]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

1. *External attack:-*
   External attacks are carried out by nodes that do not belong to the network. It causes congestion and sends false routing information or causes unavailability of services.
2. *Internal Attack*: -
   Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

- *Denial of Service attack*:
  This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.
- *Impersonation*:
  If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.
- *Eavesdropping*:
  This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

- *Routing Attacks:*
  The malicious node makes routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing *protocol* and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of *routing* information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.
- *Black hole Attack:*
  In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[4] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

 

- *Wormhole Attack*:
  In a wormhole attack, an attacker receives packets at one point in the network, ―tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole attack.
- *Replay Attack*:
  An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.
- *Jamming*:
  In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.
- *Man-in –the middle attack*:
  An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.
- *Gray-hole attack*:
  This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.[5,6]

## VI. PROPOSED APPROACH

Although there are several approaches present in MANETs which are designed to detect the attacks in the MANETs while we are presenting an easy approach of detecting the hostile or malafide or selfish or malicious nodes in the adhoc network.

In our proposed approach we deal with the jamming attack (for example jamming caused due to the flooding of packets). We have considered a Manet network in which there are numbers of nodes present which are communicating with each other and each node is recognized uniquely with its identification number of the node. We have considered two ways in which packets are transferred from source to destination:-

1. Initially at the first step the source (S) starts sending the pseudo (look alike ) packets also called fake messages for the route establishment from the source(S) to destination(D).
2. Once the process of route establishment is made , the source starts flooding the data packets in the network .
   When system senses some abnormal problem due to which the throughput of the system decreases and delay increases as a result the performance of system decreases then the system starts the following method:-

- The mobile node which received the data packets goes to the Monitor node (which monitors the network).
- The mobile node which starts the transmission called source node now generates the monitoring packets (ICMP control messages) that starts flooding the network.
- Mobile nodes which receive the data packets become the monitor node or supervisor node.
- Now , when the monitoring packets are received by the monitor node, they start monitoring the immediate intermediate nodes simultaneously in the network of mobile nodes from the source(S) to the destination(D).Now the immediate nodes acts as the new monitoring nodes also starts monitoring adjacent nodes. At the same time the monitor nodes finds out the malicious node which are exploiting the network resources and sending the packets greater than the threshold of the node and source generates alarm which hampers and discards the malafide node path from that network.
- While in this system monitor node sends packets on route but the sent packets are the random packets in the network. Now the nodes which receive the packets forward it to the destination and considered that path as a route between S and D.

The monitor nodes monitors the mobile nodes those drops the packets and follows some other path then the reliable path. Monitor nodes also discover the node which does not send the data packets to the D. When the monitor nodes which detect the malicious node sends its reply to a source node(S) and route nodes so that the source isolate the path of malafide or malicious node as rejected path and stop forwarding more packets.

## VII. CONCLUSIONS

As in MANETS, the mobile nodes are spread worldwide geographically so the detection of malicious nodes are difficult and harder to isolate. So in the proposed system we use a simple network features to detect the network malafide ill functioning nodes through the monitoring packets and hence isolate the path of malicious node. Hence it detects the attack and improves the system performance.

## REFERENCES

[1] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6.

 

[2] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6363043&ranges%3D2012_2012_p_Publication_Year%26queryText%3Djamming+attack+in+MANET
[3] http://www.ijceronline.com/papers/%28NCASSGC%29/AL189-194.pdf
[4] Broch,J., A.M David and B. David,1998. A Performance comparison of multi-hop wireless ad hoc network routing protocols. Proc.IEEE/ACM MOBICOM'98, pp: 85-97
[5] http://skirubame.ucoz.com/_ld/0/29_Topic_1-MANET_v.pdf
[6] http://www.ijceronline.com/papers/%28NCASSGC%29/AL189-194.pdf
[7] A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of AdHoc Wireless Networks (chapter 30), CRC press LLC, 2003.

 