Faith Based Routing in MANETS

Taruna[1], Alisha Sikri[2]Sneha[3]
[1] M.tech Scholar,[2] M.tech Scholar,[3] Assistant Professor
[1] Department of Computer Science,
[1] Gateway Institute of Engineering & Technology Sonepat, Haryana, India

Abstract - **Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes that is formed automatically in different topologies via wireless links without the help of a fixed infrastructure or centralized server. Furthermore in MANETs, the security of nodes is the responsibility of the nodes themselves. In this paper a novel approach is proposed for trust management in MANETs that is based on building the trust level by the nodes. Our main objective in this paper is to develop a robust trust mechanism and an efficient and reliable node detection technique.**

IndexTerms **- MANETs, Blackhole, Malicious user**

I. INTRODUCTION

Due to the rapid evolution of wireless local area network technologies such as Bluetooth, Wi-Fi, MANETs are becoming increasingly popular in various applications such as healthcare monitoring, collaborative and distributed computing, emergency dealing and military services[3].Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes) [6]. The mobile nodes allow communication among the nodes to forward the packets to each other.

Dynamic Source Routing (DSR) is used in multihop wireless ad hoc network and composed of two mechanisms of route discovery and Route maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the adhoc network [10].The ad hoc networks are vulnerable to attacks due to lack of centralized monitoring points [5]. Blackhole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node.

A. Security Services for Mobile Ad-Hoc Network

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, providing these services faced lots of challenges [12].Network. Due to special features of MANET, providing these services faced lots of challenges [12]. The security requirements for ad hoc networks are the same as for fixed networks, namely availability, integrity, confidentiality, authentication, and non-repudiation [5].

1. Availability:

According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary [12]. This security standard is challenged mainly during the denial-of-service attacks where all the nodes in the network can be the attack target and thus some selfish nodes do some of the network services unavailable, such as the routing protocol or the key management service [5].

2. Integrity:

According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them [12].Integrity guarantees the individuality of the messages when they are delivered, and thus can be maintained in two following ways:

- Malicious altering
- Accidental altering

A message can be deleted, replayed or revised by an adversary with malicious goal, which is admire as malicious altering [5].

3. Data Confidentiality

Confidentiality means that certain information is only use by those who have been authorized to access it. In other words, in order to keep the confidentiality of some confidential information, we require keeping them secret from all entities that do not have the privilege to access them [5]. According to this service, each node or application must have access to specified services that it has the permission to access [12].

4. Authenticity

Authenticity is basically assurance that participants in communication are trustworthy and not impersonators. It is required for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity [5]. According to this service, each node or application must have access to specified services that it has the permission to access [12].

5. Non Repudiation
Non Repudiation guarantees that the sender and the receiver of a message cannot refuse that they have ever sent or received such a message. This is helpful especially when we need to discriminate a node with some abnormal behavior. If a node gets identified that the message it has received is erroneous, then the incorrect message is used as evidence to notify other nodes that the node sending out the improper message must be compromised [5].

B. Types of Attacks

Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Following are the most important attacks in MANET:

1. Black Hole Attack:
A Black Hole attack is a type of routing attack in which malicious node shows itself with a shortest path to destination in a network by sending fake route reply to the source node. The black hole attack is an active insider attack having two properties: first, the attacker consumes the intercepted data packets without forwarding them. Second, the node exploits the mobile ad hoc routing protocol, to pretend itself as having a valid path to a destination node with the intention of intercepting packets [11].
In this attack, malicious node injects fault routing information to the network and leads packets toward itself and then intercepts or discards all of them.

2. Worm Hole Attack: In worm hole attack, malicious node records packets at one location of the network and send them to another location. Fault routing information could interrupt routes in the network. The way to secure MANET against this attack is using encryption and node location information.

3. Byzantine attack: In this attack, malicious node injects fault routing information to the network ,in order for locating the data packets into a loop. The network can be protected against this attack by authentication using various mechanisms like RSA authentication.

4. Snooping attack: The aim of this attack is to access other nodes packets without having any permission. As in MANET packets transmitted hop by hop, any malicious node can capture other packets.

5. Routing attack: In this attack, node's routing tables are tried to be modified or deleted by the malicious node. Using this attack, routing information table is destroyed in ordinal nodes by malicious node.
Therefore, packet overhead and processing time will get increased.

6. Resource consumption attack: In this attack, malicious node uses many ways to waste nodes or network resources. For instance, malicious node leads packets to a loop that consists of ordinal nodes. As a result, node's energy gets consumed for transmitting faulty packets. In addition, congestion and packet lost probability will increase.

7. Session hijacking: Session hijacking is a serious error and gives an opportunity to the malicious node to behave as an authorized system. Cryptography is one of the most efficient ways to defeat this attack.
8. Denial of service: In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. In addition, packet delay and congestion increases.

9. Jamming attack: Jamming attack is a kind of DOS attack. The objective of a jammer used is to interrupt with reliable wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

10. Modification Attack: In this attack, malicious nodes sniff the network for a certain period of time. Then, the wireless frequency is explored to use it for modifying packets. Man-in-the-middle is a kind of Modification attack.

11. Fabrication Attack: In fabrication attack, malicious node destroys routing table of nodes by injecting fault information. Malicious node creates fault routing paths. As a result, nodes send their packets in fault routes. Therefore, network resources wasted, packet delivery rate decreased and packet lost will growth.

12. Man-in-the-middle attack: In this attack, malicious node puts itself between source and destination to capture all packets and drops or modifies them. Authentication and cryptography are the mostly used to defeat this attack.

13. Gray Hole Attack: This attack is similar to black hole, in which malicious node drops all packets. In this attack, malicious node drops packets with different probabilities.

14. Traffic Analyse Attack: The goal of this attack is sniffing network traffic to use them in another attack or in a specific period of time. Malicious node captures all packets to use them afterwards [12].

II. LITERATURE SURVEY

RaihanaFerdous [1] proposed a network model based on sufficient backbone nodes with multiple long-range radios that are randomly scattered in the MANET. Every node has a unique ID by which it can be distinguished from others. Through a secure routing protocol, all the nodes (including backbone nodes) together compose a low-level network using a short range radio, which is referred to as the original network. Likewise, the backbone nodes additionally constitute a high level network, the backbone network, via a long-range radio. The original network is dynamically partitioned into a number of clusters by an effective clustering algorithm running on each node; each cluster has a backbone node elected as cluster head. Both backbone and non-backbone nodes may fail or become unavailable due to a system crash, power exhaust, or any other reason; however, the rest of the original network and backbone network should still be connected.

Ermanet al. [2] Introduced a robust and efficient securitymechanism for delay tolerant networks. The proposed security mechanism consists of a trust management mechanism and an iterative trust and reputation mechanism (ITRM). The trust management mechanism enables each network node to determine the trustworthiness of the nodes that it had a direct transaction. On the other hand, ITRM takes advantage of an iterative mechanism to detect and isolate the malicious nodes from the network in a short time.

Jing-Wei [3] proposed a routing scheme that will make use of our so-called data degree of secrecy to find suitable paths to be used to transfer the packets. This concept is borrowed from, where a new access control model (so-called fuzzy multi–level security) is designed, which provides a way to compute a quantified estimate of risk associated with a subject reading an object. Each subject is tagged with a sensitivity level that reflects its degree of trust, where trustworthiness means that the chance that the subject intentionally leaks the information is low. An object's sensitivity level indicates how sensitive the object is or the magnitude of the damage incurred by an unauthorized disclosure of the object.

Isaacet al.[4] proposed an enhanced trust-based multipath Dynamic Source Routing (DSR) protocol (so-called ETBMDSR) to securely transmit messages in MANETs. This method consists in a combination of soft-encryption, novel trust management strategy, and multipath DSR routing.
Simulation results are presented to validate the proposal, showing that our ETB-MDSR scheme outperforms a recently proposed Trust-Based Multipath DSR message scheme (TB-MDSR), in terms of route selection time.

Amolet al.[5] analyzed the effects of black holes by simulating the wireless ad-hoc network with and without a black hole node present in the network. To be able to do that, we innovate a new protocol, which we called "Modified AODV". This new protocol, modified AODV is inherited from the existing AODV routing protocol. In Watchdog mechanism, each node keeps two extra tables, one is known as pending packet table and another one is knows as node rating table. There are four fields in pending packet table, Packet ID, Next Hop, Expiry Time and Packet Destination.

Lathaet al.[6] developed a probability to wait and check the replies from all the neighboring nodes to find a safe route. The approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

Vishnuet al. [7] proposed a method to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly
selects one of the free IP addresses . The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.

III. PROBLEM FORMULATION

Mobile ad-hoc networks (MANETs) are dynamically configured, multi-hop wireless networks with varying topology. They can be widely employed in many fields like electronic commerce, secure brokering, distributed information retrieval, and telecommunication network services. Due to the mobility of MANETs, most nodes are supposed to be as small as possible to be carried out or to be easy to install in hostile places.

However, it is also true that a node may easily be stolen and become compromised. Thus, the trust between nodes in ad-hoc networks cannot be guaranteed. Furthermore, this problem may increase the chance to tamper the stolen node. It is also vulnerable since every node in MANET uses radio wave to communicate. It is very hard to detect any node since there is no explicit evidence. Secure routing is an important issue in MANETs. A particularly devastating attack in wireless networks is the black hole attack. The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. As a result, an efficient algorithm to detect black hole attack is important.

Mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multi-hop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in infrastructure based networks.

Several protocols for secure routing in ad hoc networks have been proposed in the literature. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. Secure routing is an important issue in MANETs. A particularly devastating attack in wireless networks is the black hole attack. The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. As a result, an efficient algorithm to detect black hole attack is important.

IV. PROPOSED METHOD

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node [7]. Secure ad hoc routing protocol has been used as a technique to enhance the MANET security. A common key encryption system is proposed for Dynamic Source Routing (DSR) to find the best
suited path [8].

TRUST FORMALIZATION OF NTM

Mobile ad-hoc networks (MANETs) have created problem in resource sharing as they are constructed via mobile nodes without any prior knowledge of the existing nodes which may not be trustworthy. In this paper it is assumed that trust is transitive and trust values are represented as binary rather than as a continuous-valued variable. In NTM scheme, we need to compute trust values by using the following equation [1] [9].

1. Here we are proposing a secure routing technique to deliver the data packets from source to destination.
2. In this technique, we have added nodes faith values according to its cooperation in delivering data packets.
3. For each node in the network, a faith value will be stored that represent the value of the faithfulness to each of its neighbour nodes. We will supply this value to each and every node in the network.
4. It will range from 0.1 to 1. 0.1 faith value means that the node will be preferred least to transfer data packets from source to destination. 0.1 faith value also indicates that the node is a malicious node that can harm the packet. 0.2, 0.3 indicates that these are selfish nodes and 1 indicates that the node will definitely transfer data packets.
5. We have applied dijkstra algorithm to find out the shortest route or path from source to destination.
6. We have supplied three input parameters to dijkstra algorithm. Source node, Destination node and nodes faith values.
7. We can calculate shortest path based on faith values and total distance or cost by using Dijkstra algorithm .

For calculation of faith values between two nodes. The equation is

$$faith(i,j)=1-((Z(i)+Z(j))/2); \quad (1)$$

Where Z (i) is the faith value of i^{th} node and Z(j) is the faith value of j^{th} node.
Every node which takes part in delivering the packet will be increased by 0.1 values.
The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node.

V. RESULTS

Simulation Parameters

The simulation was carried out in MATLAB R2008a. Simulation parameters are shown in table 1. We have 10 nodes for simulation and traffic type is random waypoint, where percentage of malicious node is 10% i.e. one node will act as blackhole in this simulation. The area for simulation is 50 m X 50 m.
The assumptions are node 1 will act as source and node 10 will act as destination, whereas node 9 will act as blackhole [18].

Table 1: Simulation Parameters

Number of Nodes	10
Terrain dimension	50 m x50 m

Traffic Type	Random waypoint
Simulation Rounds	100
% of malicious Nodes	10% of total nodes
MAC protocol	IEEE 802.11

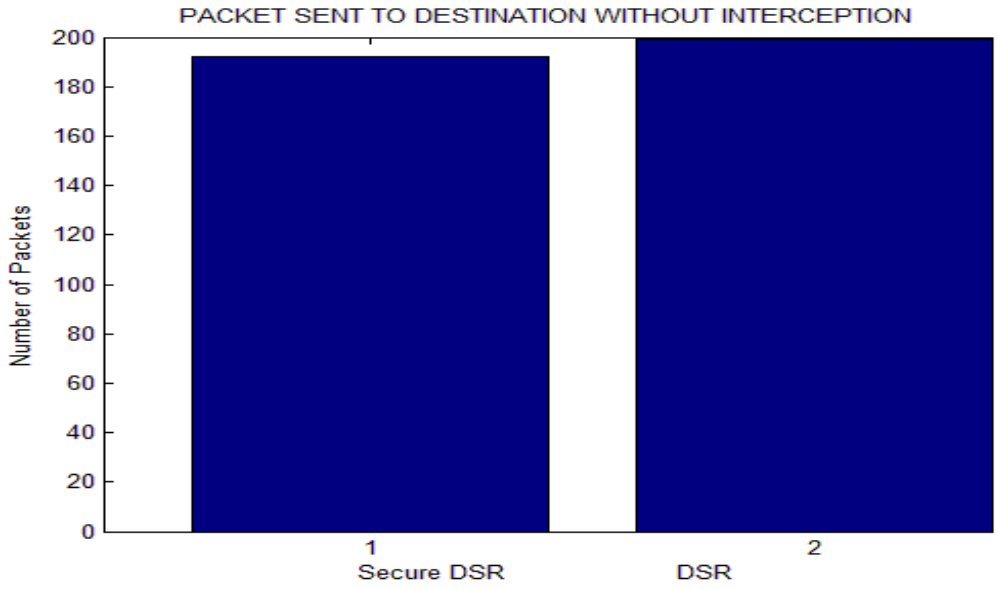

Figure 1.1: Packet sent to destination without interception though black hole

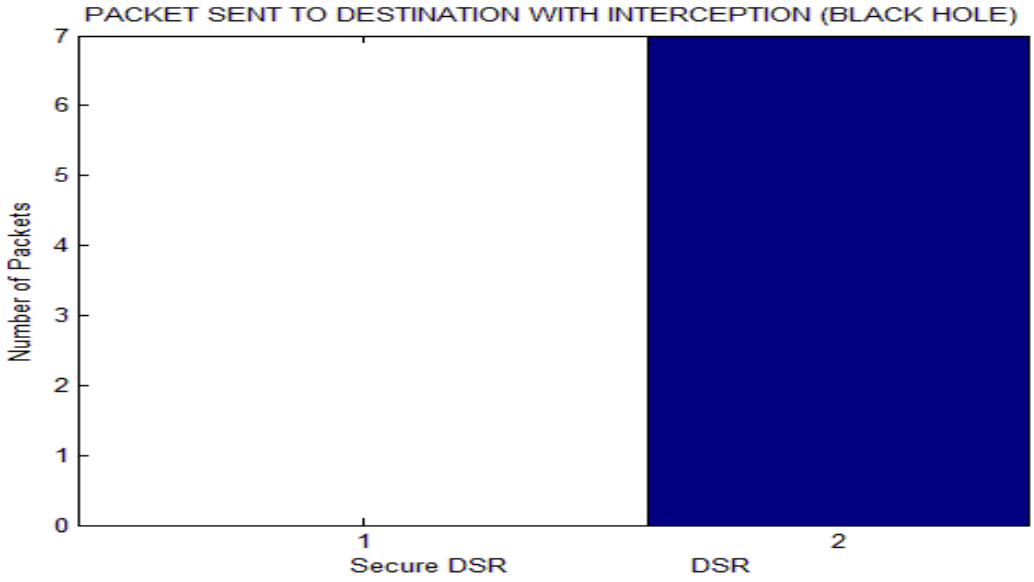

Figure 1.2 Packet sent to destination with interception using Black Hole

VI. CONCLUSION

The goal of this paper was to provide a simple node based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. Secure routing protocols is a crucial area towards security of MANET. The routing solutions for conventional networks are not sufficient to work efficiently in ad-hoc environment. In this dissertation, we have proposed a scheme to select secure route for data forwarding. This technique will avoid interception of messages through blackhole nodes. We have compared our results with DSR routing protocol, the results showed that Secure DSR will avoid routing of packets through blackhole nodes. The goal of this work is to provide a simple node based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. The model is simple, flexible and easy to be implemented.

After introducing and analyzing the concept of node-based trust in MANET, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability and reliability.

VII. REFRENCES

[1]. Raihana Ferdous, Vallipuram Muthukkumarasamy, Abdul Sattar, "Trust Management Scheme for Mobile Ad-HocNetworks", 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).
[2]. Erman Ayday, Hanseung Lee, Faramarz Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks", 978-1-4244-8180-4/10/$26.00 ©2010 IEEE.
[3]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks ", 978-1-4244-9268-8/11/$26.00 ©2011 IEEE.
[4]. Isaac Woungang, Mohammed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks", 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.
[5]. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.
[6]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in Manet", Journal Of Networks, Vol. 3, No. 5, May 2008.
[7]. Vishnu K, Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks", 2010 International Journal of Computer Applications (0975 - 8887).
[8]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.
[9].Raihana Ferdous, Vallipuram Muthukkumarasamy, Abdul Sattar, "A Node-based Trust Management Scheme for Mobile Ad-Hoc Networks", 978-0-7695-4159-4/10 $26.00 © 2010 IEEE DOI 10.1109/NSS.2010.67.
[10]. Saurabh Chandra, Ashish Xavier Das and A.K. Jaiswal, " QoS for Energy Efficient Routing Protocols in IEEE 802.11 Wireless Mobile Adhoc Network using Qualnet Simulator 6.1", International Journal of Current Engineering and Technology, Vol.4, No.3 (June 2014).
[11]. Meenakshi, Kapil Kumar Kaswan, " Simulation Of Black Hole Attack In Adhoc Network Using Ns2", International Journal of Technical Research (IJTR) Vol. 3, Issue 1, Mar-Apr 2014.
[12]. Ali Dorri, Seyed Reza Kamel, Esmailkheyrkhah, "Ali Dorri and Seyed Reza Kamel and Esmailkheyrkhah", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.