Outsider Attack Prevention in Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks

S.Kavitha [1]

Research Scholar[1],

Department of Computer Applications,
Dr.SNS Rajalakshmi College of Arts & Science,
Coimbatore-641 049, India

E.Bharathi [2]

Assistant Professor[2],

Department of Computer Science,
Dr.SNS Rajalakshmi College of Arts & Science,
Coimbatore – 641 049, India

ABSTRACT

A mobile ad hoc network (MANET) is a self-configuring network without a central coordinator of mobile devices connected by wireless. MANET frequently changes its topology as it is infrastructure less network. The security challenges in MANET have become a primary concern to provide secure communication. Attacks on MANET disrupt network performance and reliability. Based on the nature of attack interaction, the attacks against MANET are classified into active and passive attacks. Attackers against a network are classified into two groups: insider and outsider. Outsider attacker is not a legitimate user of the network, whereas an insider attacker is an authorized node and a part of the routing mechanism on MANETs. In this paper, we discuss about attackers from outside the network using passive attack which are prevented by not entering into the nodes in the network [1]. The protocol used in this paper is USOR and it is implemented on ns2.

Keywords: MANET, USOR, Security, Mobile Ad hoc Network, Prevention of attacker.

1. Introduction

Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of communication infrastructure may potentially cause the entire network to become vulnerable to security reaches. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. The attacks can either be used to analyze the traffic through the network or to drop packets selectively or completely to affect the flow of information. Attack in participating mode is more difficult, yet once it is launched, it is also hard to detect. Due to openness of MANET, nodes move in any direction joins or leave the network at any time, and also the transfer medium that is electromagnetic spectrum can be publicly accessed without restriction. In such a term selfish/malicious nodes are more likely to appear.

Selfish nodes are characterized by their reluctance to spend resources to cooperate on its behalf. Malicious nodes attack the network's availability through common techniques such as flooding, denial of service (DoS) etc. Because of the difficulties in MANET such as dynamic network topology, constraint battery resources, security solutions that have been deployed for wired networks are not directly portable to ad hoc networks. Many secure routing protocols were developed to protect routing protocols from malicious behaviors. The Vulnerabilities of MANETs are Dynamic Topology, Wireless Links, Cooperativeness, Lack of clear line of defense, Limited Resources [7].

2. Cryptography and Security

The base requirements for a secured networking are secure protocols. The secured protocols are design with the cryptographic algorithms in order to be securely and reliably implemented. A basic understanding of symmetric and asymmetric (or public key) encryption, key chains, message authentication, digital signatures, and threshold cryptography are useful to appreciate the possibilities and consequences of these methods.

In order to define attacks a traditional understanding of host and network security is presumed as well. A system is considered secure if it ensures integrity, confidentiality, availability, and accountability for all its actions [8]. Any action that assaults this security is considered the attack.

3. Attacks in MANET

Mobile Ad hoc networks are vulnerable to various types of attacks not only from outside but also within the network itself. Ad hoc network are mainly subjected to two different levels of attacks [7]. The first level of attack on the routing of the ad hoc network that is on routing and second level of attacks tries to damage the security mechanisms employed in the network [1]. Attacks in MANETs are categorized into two major types.

3.1 Internal Attacks

Internal attacks directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes [1, 2].Internal attacks becomes more difficult to handle than compare to external attacks, because internal attacks occurs on more trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify.

3.2 External attacks

External attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two types.

3.2.1 Passive attacks

MANETs are more susceptible to passive attacks. A passive attack does not alter or change the data transmitted within the network. But it includes the non permitted “listening” to the network traffic or accumulates data from it. Passive attacker does not stop the operation of a routing protocol but attempts to discover the important information from routed traffic [2, 5].Detection of such type of attacks is difficult since the operation of network itself does not get affected. In order to overcome these types of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

3.2.2 Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be washed out by outside sources that do not belong to the network. Internal attacks are originated from malicious nodes which are part of the network, internal attacks are more vulnerable and hard to detect than external attacks[2,6].These attacks generate non permitted access to network that helps the attacker to make changes such as alternation of packets, DOS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes will change the entire routing information by advertising itself as having shortest path to the destination.

4. Unobservable Secure On-Demand Routing Protocol (USOR)

The Unobservable Secure On-Demand Routing Protocol(USOR) an efficient privacy maintain routing protocol that achieves content unobservability by employing anonymous key establishment based on group signature[4]. The protocol contains both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only the valid nodes in the network can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. In this scheme a node can establish a key with each of its neighbors, and then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor node distinguishes that the encrypted packet is intended for itself and not for other node by trial decryption. In order to support both broadcast and unicast, a group key and a pair-wise key are required. The setup of USOR is simple that is each node has to obtain a group signature signing key and an ID-based private key from an offline key server. With USOR protocol transfer of data with high security and avoids hacking unlike data security, and it also provides the basic packet security. As a result, USOR comprises two Phases, the anonymous trust establishment and unobservable route discovery [4].Fig 1 shows the propagation of route request and path of route reply of USOR protocol.

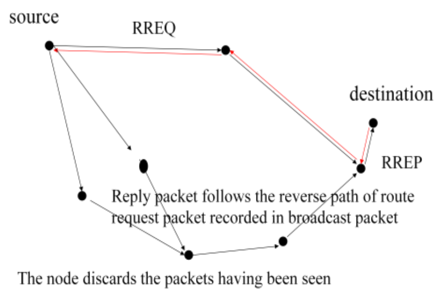
source
RREQ
destination
RREP
Reply packet follows the reverse path of route request packet recorded in broadcast packet
The node discards the packets having been seen

Fig 1: Propagation of Route request (RREQ) and path of Route Reply (RREP).

5. Prevention of outside attacker

In this paper, we analyze the outsider attack. This is major issue of the MANET is to prevent the outsider attack as any node is independent to join in the network and nodes in the network can quit from the network there is a chance of entrance of new nodes which is malicious nodes. The prevention code in the USOR protocol prevents the malicious nodes from being joining in the network and only the trust worthy nodes can join the network. This prevents the passive attack that it does not hack the information from the network. In our implementation Two Malicious nodes try to enter into the network and it is prevented by the attack code in USOR protocol. In this project, an Unobservable routing protocol USOR based on group signature and ID based cryptosystem for Ad -hoc network is implemented. The security analysis demonstrates that USOR not only provides strong privacy protection, it is performs high resistant against attacks due to node compromise.

6. Simulation Environment

The proposed routing protocol with outside attacker prevention code has been implemented by the Network Simulator2 (NS2). The Network Simulator is mainly utilized to implement the routing protocols in the networking. The main focus of our analysis is prevention of malicious node from outside the network. The simulation results are shown below.

Simulation Time	30sec
Scenario dimension	1000*1000
Number of Nodes	14
Average Node Speed	4
Traffic Type	512 byte CBR Traffic
Routing Protocol	USOR

Table 1: Stimulation Specification

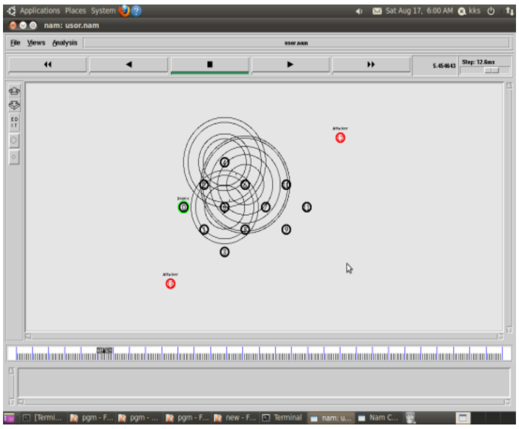

Fig 2: Topology Formation with outside attackers

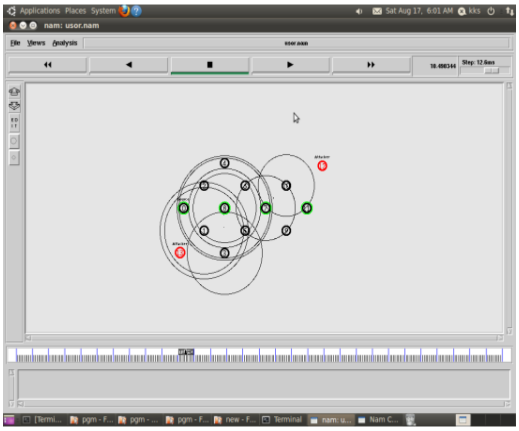

Fig 3: Malicious Nodes are prevented from entering Network

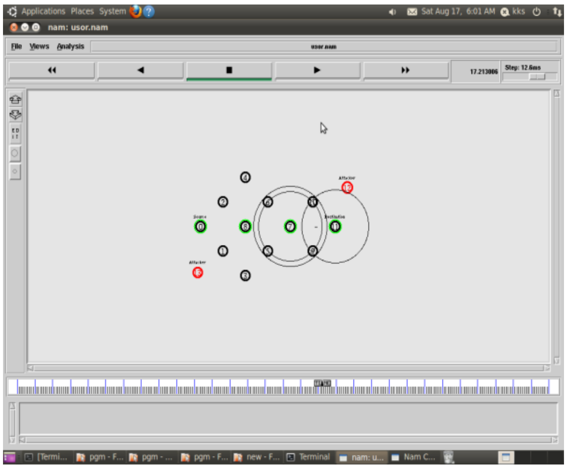

Fig 4: Route Discovery by the trust worthy node in the network

In the stimulated result Fig 2, 3, 4 two attackers from the outside are prevented from entering into the secure network and the node based on its trust worthy level can enter into the network. The red color is the malicious node and black color node is trust worthy node, green indicates the path from source to destination the shortest path with USOR protocol.

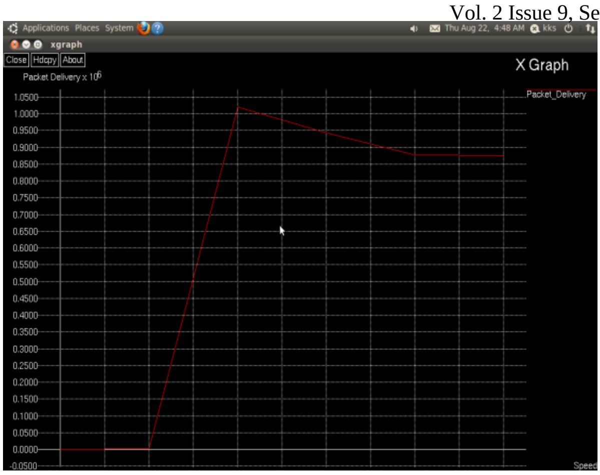

Fig 5: Packet Delivery Ratio

The ratio of packet delivery is high with the increase in speed and after a limit the delivery ratio is stable and loss is packet is below 0 so, no packet loss.

6. Conclusion and Future work

The proposed work attempts to prevent the malicious node from outside the network and the trusted nodes a dynamically entered with privacy preserved routing in mobile ad hoc networks. The packet delivery is high for a certain speed and remains stable. Future work is based on the inside attackers and active attacks with the USOR protocol.

References:

1]. MohammadIlyas, “The Handbook of Ad Hoc Wireless Networks”,

2]. Amitabh Mishra, “SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS” (chapter 1, 3), ISBN-13 978-0-521-87824-1 Handbook.

3]. Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller, “Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs)”

4]. USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 5, MAY 2012

5]. Ad hoc network specific attacks held by Adam Burg.

6]. Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, “Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey.

7]. MANET: Vulnerabilities, Challenges, Attacks, Application”, International Journal of Computational Engineering & Management, Vol. 11, January2011.

8]. William Stallings, “cryptography and network security”, Fourth Edition.