IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 38-41

Detecting Node Attacks in MANET using Secure Zone Routing Protocol

Sara Begum
Department of Electronics Engineering
Terna Engineering College
Nerul, Navi Mumbai, India

Abstract: *A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or indirectly depending on nodes in the network. As the nodes in the MANETs having mobility the position of nodes can changes as per the movements of the nodes, hence the network topology of a MANETs may change dynamically. Due to the dynamic change in topology, computing the route is a challenging task. During the network process the nodes consumes energy and utilizes the other resources of the network, but in the process of networking some nodes may attack. Because of this, unnecessary wastage of energy and resources may result and security and performance of the network can be affected. Here in this work, we proposed an algorithm to establish route in such a way to detect and avoid misbehavior nodes. This reduces unnecessary wastage of energy and resources also provide security and improve the performance of the network and present Zone Routing Protocol (ZRP) the most popular routing protocol. The importance of the proposed solution lies in the fact that it ensures security as needed by providing a comprehensive architecture of Secure Zone Routing Protocol (SZRP) based on efficient secure neighbor discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network.*
Keywords: *neighbor discover, Pathrater, Watchdog*

I. Introduction

In the past few years, we have seen a rapid expansion in the field of mobile computing due to the proliferation of inexpensive, widely available wireless devices. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks (WLANs), not considering the great potential offered by mobile ad hoc networking. A mobile ad hoc network (MANETS) is an autonomous collection of mobile devices (laptops, smart phones, sensors, Bluetooth, etc.) that communicate with each other over wireless links and cooperate in a distributed manner to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications.

The main security problems that need to be dealt with in MANET networks include: authenticated devices, the secure routing in multi-hop networks, and the secure transfer of data. This means that the receiver should be able to confirm that the identity of the source or the sender (i.e., one hop previous node) is indeed who or what it claims to be. It also means that the receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

II. Related Work

A mobile ad hoc network (MANET) is a wireless communication network which does not rely on a pre-existing infrastructure or any centralized management. Securing the exchanges in MANETs is compulsory to guarantee a widespread development of services for this kind of networks. The deployment of any security policy requires the definition of a trust model that defines who trusts who and how. This work aims to provide a fully distributed trust model for mobile ad hoc networks. In this paper, we propose a fully distributed public key certificate management system based on trust graphs and threshold cryptography. It permits users to issue public key certificates, and to perform authentication via certificates' chains without any centralized management or trusted authorities [1]. The trust is always present implicitly in the protocols based on cooperation between the 26 entities involved in routing operations in Ad hoc networks. Indeed, as the wireless range of such nodes 27 is limited, the nodes mutually cooperate with their neighbors to extend the remote nodes and 28 the entire network.

In our work, we are interested by trust as security solution for OLSR protocol. These 29 approachesfit particularly with characteristics of ad hoc networks [2]. A mobile ad hoc network (MANET) refers to a network designed for special applications for which it is difficult to use a backbone network. In MANETs, applications are mostly involved with sensitive and secret information. Since MANET assumes a trusted environment for routing, security is a major issue. In this paper we analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against a specific type of denial-of-service (DOS) attack called node isolation attack. Analyzing the attack, we propose a mechanism called enhanced OLSR (EOLSR) protocol which is a trust-based technique to secure the OLSR nodes against the attack [3]. Optimized Link State Routing is a routing protocol that has been extensively studied for mobile ad-hoc networks. Link spoofing, which disturbs the routing service, is one of the critical security problems related to the OLSR protocol. Existing approaches against link spoofing attack have several drawbacks. In this paper, propose an LT-OLSR protocol that broadcasts Hello messages to neighbors within two-hops to defend networks against link spoofing attacks [4]. Mobile Ad hoc network is consisting of mobile nodes and can organize them self without requiring any infrastructure. Due to wireless communication any node can join or leave network which causes lot of security constraint and due to limited battery, many researchers are doing researches on energy saving routing in MANET. In OLSR there is need of selecting MPR set, which minimize unnecessary broadcast in network, that conserve energy of node in network [5].

III. Secure Zone Routing Protocol

For proposed design to be suitable for a MANET, the following design goals such as:

- Few computational steps to reserve the limited power of all ad-hoc devices since too many computational steps will drain the battery.
- Balanced protocol, which means that all nodes should perform approximately the same number of heavily computations.
- Few packets flow with small size since large packets are spitted into several packets to match the available communication bandwidth where sending many packets contradicts with the previous design goal.
- Restricted number of heavy computations, such as modular exponentiations, to save battery power although theprocessors of most ad-hoc devices are becoming more powerful and can perform these computations.

3.1 Secure neighbor discovery

In wireless networks, each node needs to know its neighbors to make routing decisions; it stores neighbor information in its routing table that contains the address of the neighbor, and the link state. In MANETs, nodes use neighbor discovery protocol to discover surrounding nodes they can directly communicate with across the wireless channel with signal propagation speed by considering the location or round trip information.

3.2 Secure routing packets

Once achieve secure information exchange, we can further secure the underlying routing protocol in wireless ad-hoc networks. Security services in MANETs belong to two kinds of massages: the routing massages and the data messages. Both have a different nature and different security needs. We focus here on securing routing because data messages are point -to-point and can be protected with any point-to-point security system. On the other hand, routing messages are sent to intermediate neighbors, processed, possibly modified, and resent. Moreover, as a result of processing of routing message, a node might modify its routing table. This creates the need for both the end-to-end and the intermediate nodes to be able to authenticate the information contained in the routing messages.

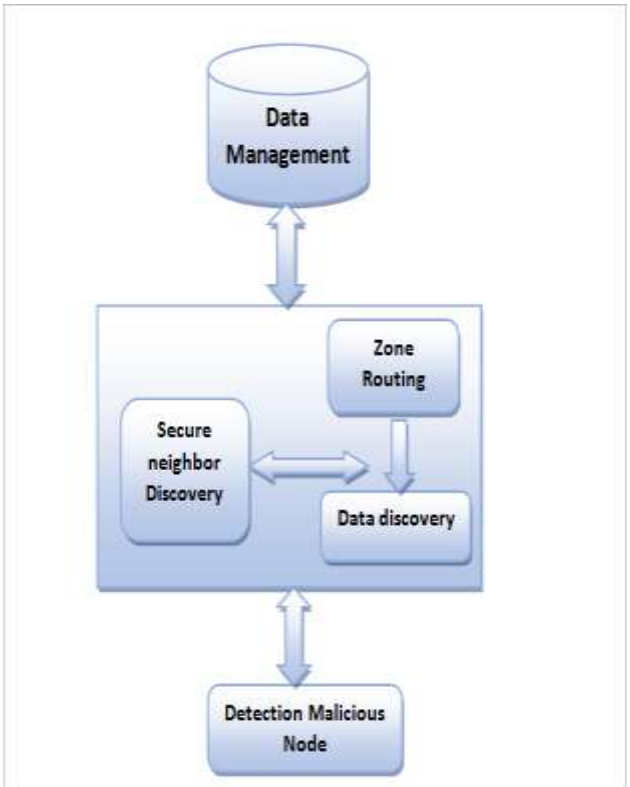

Fig. 1 System Architecture

Two components are used to identify the misbehaving nodes:

- Watchdog: Runs on every node to keep track of the behavior of the other nodes.
- Pathrater: Uses the Watchdog information to find out the reliable routes.

Watchdog Detects misbehaving nodes by overhearing transmission

- Maintain a buffer of recently sent packets
- Compare each overheard packet with the packet in the buffer to see if there is a match
- If a packet remained for longer than timeout, increments a failure tally for the node responsible
- If the tally exceeds a threshold, the node is determined to be misbehaving and the source will be notified

Watchdog Advantages

- Can detect misbehavior at the forwarding level

Pathrater

- Each node maintains a rating for every other node it knows about in the network
- It calculates a path metric by averaging the node ratings in the path
- The metric gives a comparison of the overall reliability of different paths
- If there are multiple paths to the same destination, it choose the path with the highest metric

IV. Conclusion

This paper is dedicated to implement the security of zone routing protocol; a hybrid protocol that aims to address the problems of excess bandwidth and long route request delay of proactive and reactive routing protocols, respectively. For this purpose, carefully analyzed the secured protocol proposed with respect to reactive and proactive routing protocols.

References

[1] M. Omar, Y. Challal, and A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks," *Computers & Security*, *vol. 28*, pp. 199 – 214, 2009.

[2] A. Adnane, C. Bidan, and R. T. de Sousa Júnior, "Trust-based security for the olsr routing protocol," *Computer Communications, vol. 36*, no. 10, pp. 1159–1171, 2013

[3] M. Marimuthu and I. Krishnamurthi, "Enhanced olsr for defense against dos attack in ad hoc networks," *Communications and Networks, Journal of, vol. 15,* no. 1, pp. 31–37, Feb 2013.

[4] Y. Jeon, T.-H. Kim, Y. Kim, and J. Kim, "Lt-olsr: Attack-tolerant olsr against link spoofing," in Proceedings of the *2012 IEEE 37th Conference on Local Computer Networks (LCN 2012)*, ser. LCN '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 216–219.

[5] D. Malik, K. Mahajan, and M. Rizvi, "Security for node isolation attack on olsr by modifying mpr selection process," in *Networks Soft Computing (ICNSC), 2014 First International Conference on,* Aug 2014, pp. 102–106.

[6] Liu, K. and Deng, J. and Varshney, P.K. and Balakrishnan, K., ―An acknowledgment-based approach for the detection of routing misbehavior in MANETs‖, Mobile Computing, *IEEE Transactions volume=6,* number=5, pages=536–550, year=2007, publisher=IEEE