ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.4

Detecting Attacks in MANET using Secure Zone Routing Protocol

K.Murali[1], M.Rahul[2], G.Venkateshwaran[3], Dr.S.Pariselvam[4]
UG student[1, 2, 3], Associate Professor[4]
Department of Computer Science and Engineering
Manakula Vinayagar Institute of Technology, Puducherry, India

Abstract:
MANET is a wireless network of mobile devices that has the ability to self-configure and self organize and it is characterized by an absence of centralized administration and network infrastructure. In this paper, 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. In order to fulfill these objectives, both efficient key management and secure neighbor mechanisms have been designed to be performed prior to the functioning of the protocol.

I. INTRODUCTION

The attractive features of networks such as open medium, dynamic topology, absence of central authorities, and distributed cooperation hold the promise of revolutionizing the ad-hoc networks across a range of civil, scientific, military and industrial applications. However, these characteristics make MANET networks vulnerable to different types of attacks and make implementing security in ad-hoc network a challenging task. 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.

MOBILE AD HOC NETWORK (MANET)

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. 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 WORKS

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. Our 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, in particular, 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 in order to extend the remote nodes and 28 the entire network. In our work, we are interested by trust as security solution for OLSR protocol. This 29 approach fits 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 consists 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]. Two measures to counter attacks against OLSR: prevention that solves some protocol's vulnerabilities and countermeasures that treat misbehavior and inconsistency concerned by the vulnerabilities that have not been solved with prevention measures. The resulting mechanisms allow resolving the OLSR vulnerabilities which are due to the easy usurpation of node's identity, and the lack of links verification at the neighborhood discovery [6]. Collusion Attack is an attack against Mobile Ad Hoc Networks and is based on Optimised Link State Routing (OLSR) Protocol. In this attack, two attacking nodes collude to prevent routes to a target node from being established in the network. Packet Delivery Ratio (PDR) of nodes 2-hops away from the victim drops to 0%. Multi Point Relay (MPR) selection process in OLSR is exploited to achieve route denial. In this paper, propose a novel attack resistant method named Forced MPR Switching OLSR (FMS-OLSR), in which, whenever a node observes symptoms of the attack, it temporarily blacklists potential attackers [7]. Mobile ad hoc networks (MANETs) are well known to be vulnerable to various attacks due to their lack of centralized control, and their dynamic topology and energy constrained operation. Much research in securing MANETs has focused on proposals which detect and prevent a specific kind of attack such as sleep deprivation, black hole, grey hole, rushing or sybil attacks. In this paper propose a generalized intrusion detection and prevention mechanism. We use a combination of anomaly-based and knowledge based intrusion detection to secure MANETs from a wide variety of attacks [8]. Mobile ad hoc networks are vulnerable to a variety of network layer attacks such as black hole, gray hole, sleep deprivation & rushing attacks. In this paper we present an intrusion detection & adaptive response mechanism for MANETs that detects a range of attacks and provides an effective response with low network degradation. We consider the deficiencies of a fixed response to an intrusion; and we overcome these deficiencies with a flexible response scheme that depends on the measured confidence in the attack, the severity of attack and the degradation in network performance [9]. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network [10]. OLSR relies on the cooperation between network nodes, it is susceptible to a few colluding rogue nodes, and in some cases even a single malicious node can cause routing.

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 the processors of most ad-hoc devices are becoming more powerful and can perform these computations.

A. 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.

B. 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.

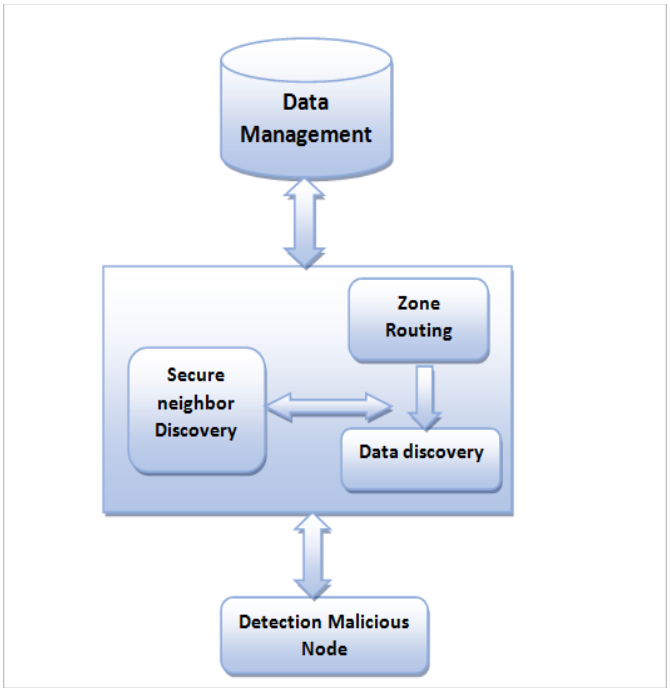


Figure.1. System Architecture

IV. IMPLEMENTATION

- The SZRP is simulated for 35 nodes spread randomly in a 1200 * 1200m area network; transmission range for each node is random.

- Nodes are positioned randomly on the plane. Nodes start its travel from a random location to a random direction with a random speed.

Node Creation

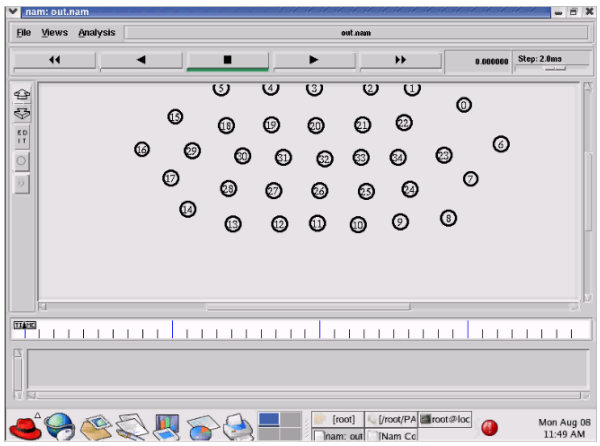


Figure.2. Node Creation

The node is designed to move in a three dimensional topology. However the third dimension (Z) is not used. That is the node is assumed to move always on a flat terrain with Z always equal to 0. Thus the node has X, Y, Z(=0) co-ordinates that is continually adjusted as the node moves.

Neighbor discovery and data transmission

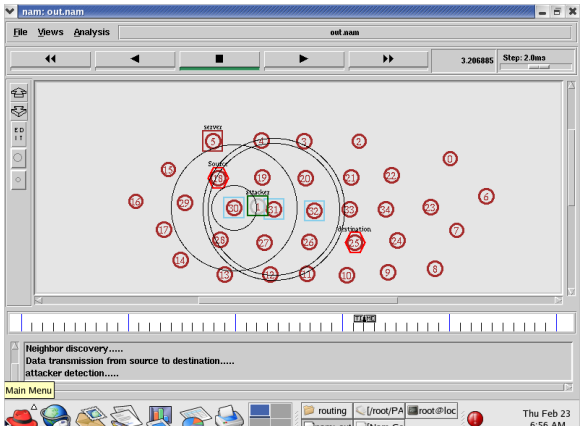
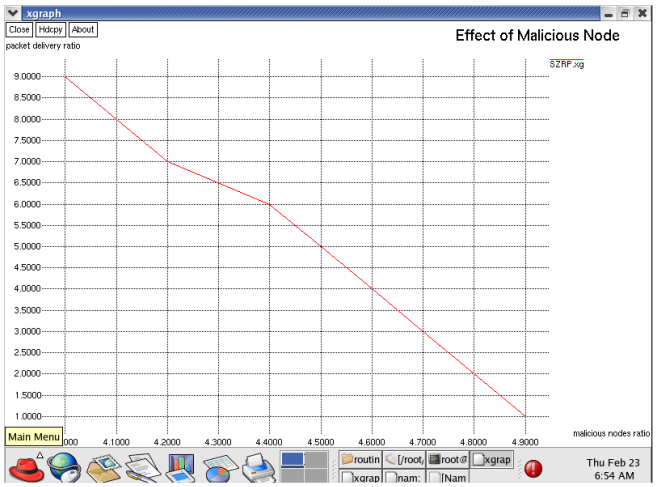


Figure.3. Neighbor discovery and data transmission

Secure neighbor discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network. The transmission at each hop along the route is counted as one transmission.

Effect of malicious node



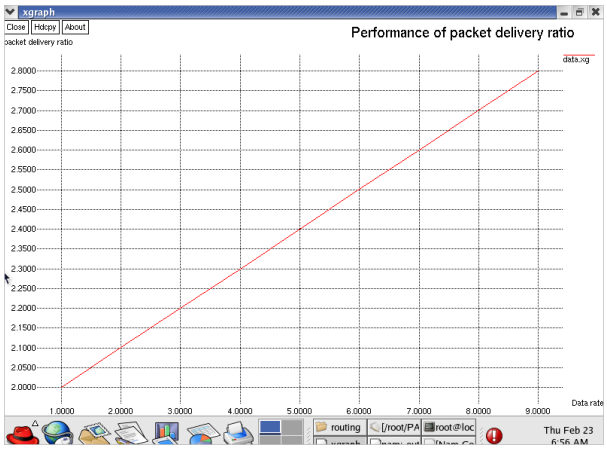


Figure.4.Effect of malicious node

The delivery packet ratio of low mobility networks increases as the data rate increases as expected since the discovered route to the destination will not change during transmitting the packets, and thus the success of delivering the packet to the same destination will increase and detect effect of malicious node.

V. CONCLUSIONS

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.

VI. 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]. A. Adnane, C. Bidan, and R. de Sousa, "Trust-based countermeasures for securing olsr protocol," in Computational Science and Engineering, 2009. CSE '09. International Conference on, vol. 2, Aug 2009, pp. 745– 752.

[7]. P. Suresh, R. Kaur, M. Gaur, and V. Laxmi, "Collusion attack resistance through forced mpr switching in olsr," in Wireless Days (WD), 2010 IFIP, Oct 2010, pp. 1–5.

[8]. A. Nadeem and M. Howarth, "Protection of manets from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, vol. 52, no. 4, pp. 2047–2058, 2013.

[9]. A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for manets," Ad Hoc Networks, vol. 13, Part B, no. 0, pp. 368 – 380, 2014.

[10]. A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," Communications Surveys Tutorials, IEEE, vol. 15, no. 4, pp. 2027–2045, Fourth 2013.