Approach on Need of security in Mobile Ad-hoc Network

Miss. Pranita D. Pandit[1], Prof. Pranjali Deshmukh[2]

[1] P.R.Pote Collage of Engineering, SGBA University, Amravati

[2] P.R.Pote Collage of Engineering, SGBA University, Amravati

ABSTRACT

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network. In this article we focus on the fundamental security problem of protecting the network connectivity between mobile nodes in a MANET. This survey paper includes various issues, problems and vulnerabilities of MANET nodes during data communication.

Keywords:- Security, Mobile Ad-hoc Networks (MANETs), Neighborhood Discovery and Verification

1.INTRODUCTION

Mobile ad hoc network is a wireless network connected with autonomous mobile nodes which are self configured and dynamic. A mobile ad hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices connected by wireless. It consists of a collection of mobile hosts that may communicate with each another from time to time. In this communication is directly between nodes acting as a router. In Mobile Ad-Hoc Networks, Routes may be disconnected due to dynamic movement of nodes. Due to mobility in MANETs, each device is free to move independently in any direction, and will therefore change its links to other devices frequently [5]. Each device must forward traffic distinct to its own use, and therefore be a router. The primary challenge in construction of a MANET is equipping each device to continuously maintain the information required to properly direct the traffic. Most traditional mobile ad hoc network routing protocols were designed focusing on the efficiency and performance of the network [1].

1.1 Problems in Ad Hoc Network

A lot of research has been done in the past but the most significant contributions have been the Pretty Good Privacy and trust based security. None of the protocols have made a decent tradeoff between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols, but it has some basic problems in the ad hoc network which are given below.

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of this, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks [2].

2.SECURITY CHALLENGES

At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the primary concerns in order to provide secure communication between different nodes in a mobile ad hoc network environment. [8] A central vulnerability of MANET comes from Peer-to

Peer architecture in which each node acts like a router to forward packets to other nodes. Moreover, these nodes on network share the same opened environment that gives opportunity for malicious attackers. In [4] and [5], the challenges for MANET security can be summarized as Follows:

- Lacking of central points: because of characteristics of MANET such lacking gateways, routers, etc, the mobile nodes just know some neighbors in its range. This introduces new difficulties for security designs such as facing with the change of network topology, resource
- Mobility: MANET nodes can leave, join, and roam in the network on their own will, so the topology of network is changed frequently. Therefore, some security solutions to adapt with the change of topology. However, this also raises new problems for these systems.
- Wireless link: In wireless environment, a plenty of collision occurred when nodes send and receive the packets. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. In addition, some services such as routing protocols, broadcast services have to communicate with others in real-time, this can flood the network traffic.
- Limited resources: The mobile nodes like laptop, PDA are generally constraint in battery power, processing speed, storage, and memory capacity. Therefore, the operation of security solutions can be reduced the accuracy, efficiency such dropping packets, a numerous time for computation.
- Cooperativeness: MANET is a mobility network, so nodes have to communicate with others by using routing protocol such AODV, DSR…Therefore; this can make these protocol become target of attack.

3.ISSUE IN SECURING THE ROUTING PROTOCOLS

Securing the routing protocols for ad hoc networks is a very challenging task due its unique characteristics [9]. A brief discussion on how the characteristics causes' difficulty in providing security in ad hoc wireless network is given below.
Location information is an integral part of most wireless sensor network services such as geographical routing [2], and applications Such as target tracking and monitoring, it is of paramount importance to secure the localization process.[4]. The specific features of MANETs present challenge for security solutions. Many existing security solutions for conventional networks are ineffective and inefficient for many envisaged MANET deployment environments. Consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to MANETs. Since many routing protocols do not consider security, some research focuses on developing secure routing protocols or introducing security extensions to existing routing protocols [6]

4.BACKGROUND

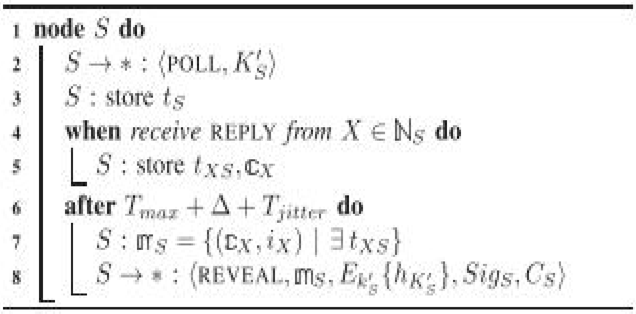
The specific features of MANETs present a challenge for security solutions. Many existing security solutions for conventional networks are ineffective and inefficient for many envisaged MANET deployment environments [7] consequently, researchers have been working for the last decade on developing new security solutions or changing current ones to be applicable to MANETs. Since many routing protocols do not consider security, some research focuses on developing secure routing protocols or introducing security extensions to the existing routing protocols. Routing protocols have been counter selfish activities by forcing the selfish nodes to cooperate.. In geographic routing, the forwarding decision at each node is based on the locations of the node's one-hop neighbors and location of the packet destination as well. A forwarding nodes therefore needs to maintain types of locations. Many works, e.g., GLS [2], Quorum System [4],have been discover and maintain the location of destination. However, the maintenance of one-hop neighbors' location has been often neglected. Some geographic routing schemes, e.g., simply assume that a forwarding node knows the location of its neighbors. The wireless network is wormholes or rely attack[3]. Wormholes may disturb communication, alert routing or include localization error. To overcome this problem many approaches properties for communications and can be roughly divided into solutions based on location, time, time and location, and network geometry. Other solutions rely on security properties achievable in specific scenarios. As wireless communications enable an ever-broadening spectrum of mobile computing applications, location or position information becomes increasingly important for those systems. Devices need to determine their own position, one to enable location-based or location-aware functionality and services [3].

5.RELATED WORK

Most previous ad hoc networking research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing [8]. The wormhole attack in wireless networks was independently introduced by Papadimitratos [2], Initial proposals to thwart wormhole attacks suggest using secure modulation of bits over the wireless channel that can be demodulated only by authorized nodes. This only defends against outside attackers who do not possess cryptographic keys [8]. In paper [10] a practical algorithm for wormhole detection. The algorithm is simple, localized, and is universal to node distributions and communication models. The simulation results have confirmed a near perfect detection performance whenever the network is connected with a high enough probability, for common connectivity and node distribution models. The expected algorithm will have a practical use in real-world deployments to enhance the robustness of wireless networks against wormhole attacks [10]. In [2], examined the main security issues in MANETs. They have most of the problems of wired networks and many more besides due to their specific features: dynamic topology, limited resources (*e.g.* bandwidth, power), lack of central management points. Firstly, presented specific vulnerabilities of this new environment. Then the attacks exploit these vulnerabilities and, possible proactive and reactive solutions used. Attacks are classified into passive and active attacks at the top level [1]. Since routing protocols on MANETs are insecure, After that, mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insider attacks are examined on our exemplar routing protocol AODV. Conventional security techniques are not directly applicable to MANETs due to their very nature. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. In [4], summarize secure routing approaches for MANETs. The difficulty of key management on this distributed and cooperative environment is also discussed. Furthermore surveyed intrusion detection systems with different detection techniques are used. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic. To propose security solutions well-suited to this new environment, recommend researchers investigate possible security risks to MANETs most roughly[6].

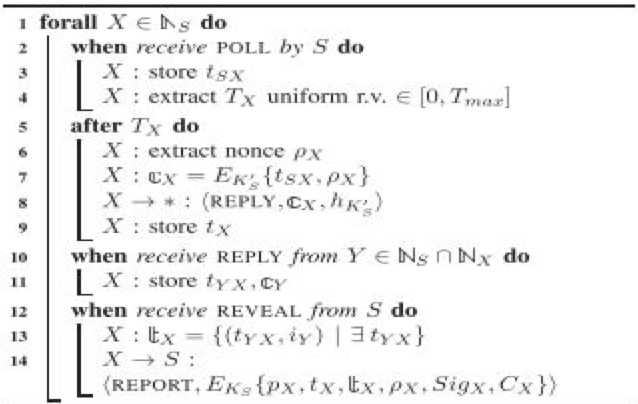
6.SECURITY PROTOCOL FOR MOBILE AD HOC NETWORK

For securing the basic technique are proposed. Firstly discover the secure neighborhood and then verify that neighborhood. Secure neighbor discovery deals with the identification of nodes with which a communication link can be established or that are within a given distance. The verification tests aim at avoiding false negatives and false positives as well as at minimizing the number of unverifiable nodes. The value pX is the current position of X, and INX is the current set of its communication neighbors. Proposed system denote by tX the time at which a node X starts a broadcast transmission and by tXY the time at which a node Y starts receiving it. Note that these time values refer to the actual instant at which the node starts transmitting/receiving the first bit of the message at the physical layer. To retrieve the exact transmission and reception time instants, avoiding the unpredictable latencies introduced by interrupt triggered at the driver's level, a solution such as that implemented in is required.3 Furthermore, the GPS receiver should be integrated in the 802.11 card; software defined radio solutions combining GPS and 802.11 capabilities are proposed, among others. Now, consider a verifier S that initiates the NPV protocol. The message exchange procedure is outlined in Algorithm 1 for S, and in Algorithm 2 for any of Ss communication neighbors



```
node $S$ do
    $S \to * : \langle \text{POLL}, K'_S \rangle$
    $S$ : store $t_S$
    when receive REPLY from $X \in \mathbb{N}_S$ do
        $S$ : store $t_{XS}, \mathbb{C}_X$
    after $T_{max} + \Delta + T_{jitter}$ do
        $S : \mathbb{M}_S = \{(\mathbb{C}_X, i_X) \mid \exists t_{XS}\}$
        $S \to * : \langle \text{REVEAL}, \mathbb{M}_S, E_{K'_S}\{h_{K'_S}\}, Sig_S, C_S \rangle$
```

Algorithm 1: Message Exchange Protocol :Verifier[11]



```
forall $X \in \mathbb{N}_S$ do
    when receive POLL by $S$ do
        $X$ : store $t_{SX}$
        $X$ : extract $T_X$ uniform r.v. $\in [0, T_{max}]$
    after $T_X$ do
        $X$ : extract nonce $\rho_X$
        $X : \mathbb{C}_X = E_{K'_S}\{t_{SX}, \rho_X\}$
        $X \to * : \langle \text{REPLY}, \mathbb{C}_X, h_{K'_S} \rangle$
        $X$ : store $t_X$
    when receive REPLY from $Y \in \mathbb{N}_S \cap \mathbb{N}_X$ do
        $X$ : store $t_{YX}, \mathbb{C}_Y$
    when receive REVEAL from $S$ do
        $X : \mathbb{L}_X = \{(t_{YX}, i_Y) \mid \exists t_{YX}\}$
        $X \to S$ :
        $\langle \text{REPORT}, E_{K_S}\{p_X, t_X, \mathbb{L}_X, \rho_X, Sig_X, C_X\} \rangle$
```

Algorithm 2: Message Exchange protocol :Any Neighbor [11]

POLL message. The verifier starts the protocol by broadcasting a POLL whose transmission time tS it stores locally (Algorithm 1, lines 2-3). The POLL is anonymous, since 1) it does not carry the identity of the verifier, 2) it is transmitted employing a fresh, software-generated MAC address, and 3) it contains a public keyK0 S taken from S's pool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node. We stress that keeping the identity of the verifier hidden is important in order to make our NPV robust to attacks (see the protocol analysis in Section 6). Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is needed; note that this is considered a part of emerging cooperative systems

7.CONCLUSION

This paper predicts an impending crisis in securing Ad Hoc network given a continuation of current trends that have been identified by many observers. But whereas other papers looking at the future of secure ad hoc networking have focused on specific algorithms that network more secure to be developed, this paper discusses the need to make ad hoc research more efficient through the verifying the neighborhood Techniques for finding neighbors effectively in a non priori trusted environment are identified. The proposed need will eventually provide security from This present a need of distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes and analysis showed, and we can design algorithm for protocol which is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. Hence the methods to securing ad hoc network have to be improved.

REFERENCES

[1] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf.(MILCOM), Nov. 2008.

[2] Shawkat K. Guirguis1, Youssef A. Othman "Simulation analysis of secure routing in Mobile Ad hoc networks"

[3] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Cˇ apkun, J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," IEEE Comm. Mag.,vol. 46, no. 2, Feb. 2008.

[4] Celia Li1, Zhuang Wang, Cungang Yang ,Secure Routing for Wireless Mesh Networks , International Journal of Network Security, Vol.12, No.3, May 2011

[5] J.Viji Gripsy , Dr. Anna Saro Vijendran ,A Survey on Security Analysis of Routing Protocols Global Journals Inc. (USA) , Volume 11.

[6] Sevil Şen, John A. Clark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks" Department of Computer Science, University of York, YO10 5DD, UK.

[7] Sevil Şen, John A. Clark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks**".**

[8] Muhammad Arshad Ali & Yasir Sarwar Muhammad Arshad Ali & Yasir "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions".

[9] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.

[11] Marco Fiore,Member, IEEE, Claudio Ettore Casetti, Member, IEEE, Carla-Fabiana Chiasserini,Senior Member, IEEE, and Panagiotis Papadimitratos, Member, IEEE "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks" **-** Ieee Transactions On Mobile Computing, Vol. 12, No. 2, February 2013.