SECURING DATA IN AD HOC NETWORKS USING MULTIPATH ROUTING

R.Vidhya[1] and G. P. Ramesh Kumar[2]
[1]Research Scholar, SNR Sons College, Coimbatore, India
[2]Prof & Head, Department of Computer Science, SNR Sons College, Coimbatore, India

ABSTRACT

Development of handheld features and mobile telephony makes Ad hoc networks widely adopted, but security remains a complicated issue. Recently, there are several proposed solutions treating authentication, availability, secure routing and intrusion detection etc, in Ad hoc networks. In this paper we introduce a securing data protocol in Ad hoc networks, SDMP protocol. This solution increases the robustness of transmitted data confidentiality by exploiting the existence of multiple paths between nodes in an Ad hoc network. This paper also includes an overview of current solutions and vulnerabilities and attacks in Ad hoc networks.

I. INTRODUCTION

WLANs (Wireless Local Area Networks) provide an alternative to the traditional LANs where users can access shared data or exchange information without looking for a place to plug in. In recent years, demands for greater mobility and the military's need for sensor networks have popularized the notion of infrastructure less or Ad hoc networks.

Mobile Ad hoc networks are self organizing network architectures in which a collection of mobile nodes with wireless network interfaces may form a temporary network without the aid of any established infrastructure or centralized administration. According to the IETF definition [1], a mobile Ad hoc network is an autonomous system of mobile routers connected by wireless links. This union forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably [2].This allows for greater mobility and dynamic allocation of nodes structures. Ad hoc networks are becoming popular because of the fast development of the mobile hand-held and portable devices. Many research projects are studying this domain to develop it more and more, and some of the proposals are introduced in industry of mobile and wireless devices. The nodes in an Ad hoc network communicate without wired connections among themselves by creating a network "on the fly". While tactical military communications was the first application of Ad hoc networks, there are a growing number of non-military applications, such as search-and-rescue, conferencing, and home networking.

Ad hoc networks have several characteristics: dynamic topology, infrastructure less, variable capacity links, and energy-constrained operation.

From the characteristics of Ad hoc networks, we can deduce issues that exist in this kind of networks [3]. Because of their specific characteristics, Ad hoc networks present a lot of issues for which solutions must been found and researchers must bring many studies. Limited bandwidth, energy constraints, high cost, security and no compatibility between different proposed norms are some of encountered problems in this type of networks. One of important issues that must attract researchers' attention is security.

In wireless mobile Ad hoc networks, security depends on several parameters (authentication, confidentiality, integrity, non repudiation and availability) and concerns two aspects: routing security and data security. These two aspects are exposed to many vulnerabilities and attacks. The organization of the rest of this paper is as follows. In next section we quote most important vulnerabilities and attacks faced in Ad hoc networks.

II. VULNERABILITIES AND ATTACKS IN AD HOC NETWORKS

In security domain, new vulnerabilities appear with Ad hoc technology. Nodes become easier to be stolen since they are mobile, the computing capacity is limited. That makes using heavy solutions, as PKI [4][5], not very practice. Also, Ad hoc networks services are provisional and batteries are a limited alimentation resource what makes a Denial of Service attack by consumption of energy very possible [6].

Ad hoc networks are exposed to many possible attacks. We can classify these attacks into two kinds: Passive attacks and Active attacks [7].

In passive attacks [8], attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. Defending against such attacks is difficult, because it is usually impossible to detect eavesdropping in a wireless environment. Furthermore, routing infor- mation can reveal relationships between nodes or disclose their IP addresses.

If a route to a particular node is requested more often than to other nodes, the attacker might expect that the node is important for the functioning of the network, and disabling it could bring the entire network down. While passive attacks are rarely detectable, active ones can often be detected.

An active attack can mainly be:

- Black hole attacks [9]. A malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.
- Wormhole attacks. In this type of attacks, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them there into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.
- Routing tables overflow attacks [8]. Here the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. It seems that proactive algorithms are more vulnerable to table overflow attacks than reactive algorithms because they attempt to discover routing information every time.
- Sleep deprivation attacks [11]. Because battery life is a critical parameter in Ad hoc networks, devices try to conserve energy by transmitting only when necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding necessary packets to the node using, for example, a black hole attack.
- Location disclosure attacks. It's an attack which can reveal something about the nodes location or the structure of the network. The attack can be as simple as using an equivalent of the trace route command on UNIX systems. In this attack, the attacker knows which nodes are situated on the route to the target node.
- Denial of service attacks [6]. Such attacks, generally, flood the network making it crashing or congested. Also, wormhole, routing table overflow and sleep deprivation attacks might fall into this attacks category.
- Impersonation attacks [12]. If authentication is not supported, compromised nodes may be able to send false routing information, masqueraded as some others, etc.

III. RELATED WORK

Recently, there are several researches about many security aspects in Ad hoc networks. We find for example IPsec [13], WEP (Wireless Equivalent Privacy) [14], Distributed Trust model [15], Key Agreement model [16], the Resurrecting Duckling solution, or using threshold cryptography as in solution cited in [18]. As Secure Routing solutions, we can cite SAODV or SRP. Intrusion Detection solutions as architecture proposed in an important researches area in Ad hoc security too.

There is no global solution for all kinds of Ad hoc networks, and no one is enough resistant for all important vulnerabilities. There are partial solutions only for specific issues.

We can classify existing approaches into four principal categories:

1. Trust Models
2. Key Management Models

3. Routing Protocols Security
4. Intrusion Detection Systems

We expose some important proposals from every category:

3.1 Distributed Trust Model

This proposal is based on the concept of trust. It adopts a decentralized approach to trust management, generalizes the notion of trust, reduces ambiguity by using explicit trust statement and makes easier the exchange of trust-related information via a Recommendation Protocol [15]. Trust categories and values are assigned to entities. There is no absolute trust in this model. An entity trust degree or value can be changed by a new recommendation. The Recommendation Protocol is used in this model to exchange trust information. Entities that are able to execute the Recommendation Protocol are called agents. With decentralization, each agent is allowed to take responsibility for its own fate and choose its own trusted recommenders. Trust relationships exist only within each agent's own database. Agents use trust categories to express trust towards other agents and store reputation records in their private databases to use them to generate recommendations to other agents.

In this solution, memory requirements for storing reputations, and the behavior of the Recommendation Protocol are issues that have been not treated.

3.2 Resurrecting Duckling Security Policy

This policy has been presented in [11] then extended in [17]. The basic concept in this approach is that between two devices, it can exist a master/slave relation. Master and slave share a common secret. This association can be only broken by the master. Duckling will recognize as mother the first entity sending him a secret key on a protected channel. This procedure is called Imprinting. It will obey always its mother, which says to him with which it can speak, by subjecting the slave an access control checklist. If the link is stopped by the master with one of his slaves or if a network anomaly happened, the slave state becomes death. It can be resurrected by accepting a new imprinting operation. There is a hierarchy of master/slaves because a slave has the right to become master. The root is a person who controls all the devices. This solution is only effective for devices with weak processors and limited capacity.

3.3 Key Agreement Based Password

The work developed in [16] draws up the scenario of a group wishing to provide a secured session in a conference room without the support of any infrastructure. The properties of the protocol of this solution are:

- **The shared secret.** Only the entities that know an initial password, called Weak Password, are able to know the Session Key. It is necessary that even if an attacker compromises a member of the group and is in possession of all secret information, it cannot be able to recover the session key.
- **Key agreement**. The session key generated is by the contribution of all the entities.
- **Tolerance** with interruption attempts. The protocol should not be vulnerable to an attack which tries to introduce a message. It is supposed that the possibility of modifying or removing a message in a similar network is very improbable.

The approach describes that there is a Weak Password that the entire group will have (for example by writing it on a table), each member contributes, then, to create a part of the session key and signs this data by the weak password.

This secured session key makes it possible to establish a secured channel without any centralized trust or infrastructure. This solution is adapted, therefore, to the case of conferences and meetings, where there are not a great number of nodes. It is rather strong solution since it does not have a strong shared key. But this model is not sufficient for more complicated environments. By imagining a group of people who do not know each other all and who want to communicate confidentially only between them, one finds that this model becomes invalid in this case. Another problem emerges if nodes are located in various places; the distribution of the Weak Password will not be possible any more.

3.4 Distributed Public Key Management

Among the few schema and methods of security suggested for Ad hoc networks, there is a method

based on a principle of cryptography appeared in the Seventies: the Threshold Cryptography [22]. The principle is purely mathematical and was combined with other technical to obtain a security model for Ad hoc networks. The method suggested is that quoted in [18]. Since in an Ad hoc network, there are no centralized entity and trust relations between nodes, this solution proposes a key management scheme by distributing trust on an aggregate of nodes.

In this model, key management service with an (n,t+1) configuration $(n \geq 3t+1)^1$, consists of n special nodes, which are called Servers. The n servers share the ability to sign certificates. The service can tolerate t compromised servers, that's why we say that it employs an (n, t+1) threshold cryptography scheme. The private key k of the service is divided into n shares (s_1, s_2, …, s_n), assigning one share to each server. To sign a certificate, each server generates a partial signature using its private key share and submits the partial signature to a Combiner which is able to compute the signature for the certificate. A compromised server could generate an incorrect partial signature. Use of this partial signature would yield an invalid signature. Fortunately, a combiner can verify the validity of a computed signature using the service public key. If verification fails, the combiner tries another set of partial signatures. This process continues until the combiner constructs the correct signature from at least t+1 correct partial signatures.

Besides threshold signature, this key management service also employs share refreshing to tolerate mobile adversaries and to adapt its configuration to the network changes. New shares do not depend on old ones, so the adversary cannot combine old shares with new ones to recover the private key of the service. Thus, the adversary is challenged to compromise t+1 server between two periodic refreshing. The base of this method is solid, but it deals with only the problem of certificates signature and distribution of certification authority. With this method one is sure that no adversary will be able to generate correct certificates. The authentication problem is well dealt but confidentiality needs more solidity. In addition to that, this method is onerous. Each time there is a secured exchange, it is necessary to call upon at least t+1 server, in addition of the Combiner process.

3.5 Secure Routing Protocol for Mobile Ad Hoc Networks

An important aspect of Ad hoc networks security is routing security. The discussed Secure Routing Protocol (SRP) in counters malicious behavior that targets the discovery of topological information. SRP provides correct routing information (factual, up-to-date, and authentic connectivity information regarding a pair of nodes that wish to communicate in a secure manner). SRP discovers one or more routes whose correctness can be verified. Route requests propagate verifiably to the sought, trusted destination. Route replies are returned strictly over the reversed route, as accumulated in the route request packet. There is an interaction of the protocol with the IP layer functionality.

The reported path is the one placed in the reply packet by the destination, and the corresponding connectivity information is correct, since the reply was relayed along the reverse of the discovered route. In the same paper, Papadimitratos and Haas suggest to protect data transmission by using their Protocol named Secure Message Transmission Protocol (SMT), which provides, according to them, a flexible end-to-end secure data forwarding scheme that can naturally complements SRP. They use methodology of to proof their protocol authentication correctness and a performance evaluation of SRP under different kinds of attacks is available in [26]. They ensure that attackers cannot impersonate the destination and redirect data traffic, cannot respond with stale or corrupted routing information, are prevented from broadcasting forged control packets to obstruct the later propagation of legitimate queries, and are unable to influence the topological knowledge of benign nodes. But in, authors make analysis of SRP and proof by employing BAN logic that the source can't guarantee that the identified route is non-corrupted as said Papadimitratos and Haas in. They introduce an attack which demonstrates SRP's vulnerabilities and propose a solution based on the watchdog scheme to make SRP more efficient.

IV. INTRUSION DETECTION

In authors examine the vulnerabilities of wireless networks and argue that intrusion detection is a very important element in the security architecture for mobile computing environment. They developed such architecture and evaluated a key mechanism in this architecture, anomaly detection

for mobile ad-hoc network, through simulation experiments. Intrusion prevention measures, such as encryption and authentication, can be used in Ad hoc networks to reduce intrusion, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys. In their architecture, they suggest that intrusion detection and response systems should be both distributed and cooperative to suite the needs of mobile Ad hoc networks. Also, every node participates in intrusion detection and response. So there are individual IDS (Intrusion Detection Systems) agents placed on each and every node. It detects intrusion from local traces and initiates response.

If anomaly is detected in the local data, neighboring IDS agents will cooperatively participate in global intrusion detection actions. For their experimental results, they use Dynamic Source Routing (DSR) protocol, Ad hoc On Demand Vector Routing (AODV) protocol, and Destination Sequenced Distance-Vector Routing (DSDV) protocol. They demonstrate that this anomaly detection approach can work well on different Ad hoc networks, but there are some limits on detection capabilities as the mobility level. In this paper, we propose a solution to ensure data confidentiality. We focused Ad hoc networks data security transmission aspect and will detail Securing Data based MultiPath routing (Secured Data based MultiPath) protocol.

V. CONCLUSION

In this paper, we proposed a solution that treats data confidentiality problem by exploiting a very important Ad hoc network characteristic which is MultiPath. Our proposal improves data security robustly without being heavy. It takes profit from existing Ad hoc networks' characteristics and doesn't modify existing lower layers protocols. This solution can be combined with other solutions which ensure other security aspects than confidentiality. We are carrying out tests and evaluations to emphasize its performances to ensure security.

REFERENCES

[1] B.Shrader May 2002 A proposed definition of Adhoc Royal Institute of Technology (KTH), Stockholm, Swede

[2] M. M. Lehmus. May 2000. Requirements of Ad hoc Network Protocols. Technical report, Electrical Engineering, Helsinki University of Technology.

[3] A. Qayyum. Nov 2000. Analysis and evaluation of channel access schemes and routing protocols for wireless networks. Ph.D report. Dep Computer Science, Paris XI, Paris Sud University.

[4] W.Diffie, and M. Hellman. November 1976. New Directions in Cryptography. IEEE Transactions on Information Theory. 22(6): 644-654.

[5] P. Guttmann. August 2002. PKI: It's Not Dead, Just Resting. IEEE Computer. 41-49.

[6] H. Li, Z. Chen, X. Qin, C. Li, and H. Tan. April 2002. Secure Routing in Wired Networks and Wireless Ad Hoc Networks. Technical Report, Department of Computer Science, University of Kentucky.

BIOGRAPHY

R. Vidhya received M.Sc (IT), SNR SONS College, Coimbatore, MBA Pondicherry University, M. Phil Bharathiar University Coimbatore. She has published 2 International Journals. She has published 11 National Conference and 5 International Conference. His area of interest in Networks Security and Information Security.

G. P. Ramesh Kumar received MCA, M. Phil, about to submit Pursuing Ph.D under the guidance of Dr. Antony Selvadoss Thanamani in VMRF University Chennai. He is having 17 Years of teaching Experience. He has published 5 National Journals and 2 International Journals. He has published 22 National Conference and 3 International Conference. His area of interest in Networks Security and Information Security. He is a member of ISTE and CSI.