# A Survey of Secure Routing Techniques for MANET

**Ovais Ahmad Khan**
**National University of Computer and Emerging Sciences**
**Karachi Campus**
**ovais.khan@nu.edu.pk**

## Abstract

The current research on mobile ad hoc network has been focused on the routing issue with security considered only when vulnerabilities are detected. A short literature study over papers on ad hoc networking shows that many of the new generation ad hoc networking proposals are not yet able to address the security problems they face. This paper provides an overview of the prevalent threats to ad hoc network and provides a survey of the recently proposed secure routing protocols for mobile ad hoc networks.

## 1 Introduction

A mobile ad hoc network (MANET) is an autonomous system that consists of a variety of mobile hosts forming a temporary network without any fixed infrastructure. Since it is difficult to have dedicated routers and other infrastructure in such a network, all the nodes collaborate to form their own collaborative infrastructure. All the nodes as well as the routers can move about freely and thus the network topology is highly dynamic.

Large networks of fixed nodes are already helping us in our day to day activities. But at some places such networks are not desirable especially when the users are very sparse or very dense. MANET is also useful during disaster recovery, where fixed infrastructure might not be relied upon. They are also used for many other purposes such as in military operations.

The recent problems faced by the telecommunication and data communication infrastructure due to security breaches has shown that if security is not embedded into the basic infrastructure from the very beginning, then malicious users would exploit any available vulnerability.

Security requirements for the specific mission conceived for the MANET depends very much of the mission, but there are definitely some commonalities. We will be discussing such approaches in this paper.

Security can be perceived and implemented at various levels including data-link, network, transport and application layers. In this paper we will be covering secure routing.

The rest of the paper has been organized as follows. In Section 2, we will identify the various threats to the MANET and a survey of the possible prevention measures. In Section 3, we present a survey of recent research that has been done in order to perform routing securely. The discussion is concluded in Section 4.

## 2 Threats and Attacks

Reasons for making the MANET highly secure are many some of the vulnerabilities are described in [1] and [3] are as follows:

- Due to the very nature of wireless communication, the communication channel is highly insecure. Eavesdropping and masquerading are not very difficult.
- Node security is another major concern as mobile nodes can fall into hostile control. There have been widely reported cases of theft of cellular nodes, so MANET nodes would not be any safe. The node could be compromised and thus would act as a hostile node.
- Easy theft might also lead to node tampering. Tampered node might disrupt network operations or release critical information.
- The limited powers in the mobile nodes can lead to a simple denial of service attack where the attacker could create additional transmissions or expensive computations.
- The absence of infrastructure stops us from using the classical solutions based on certification authorities and on-line servers.
- The computational powers of the nodes also make the use of PKI during normal operations highly infeasible.
- Lack of fixed topology requires the routing protocols to be highly sophisticated. Securing such a protocol in the presence of hostile nodes present a challenge.

Thus, apart from the attacks prevalent in wired network, MANET needs to be prevented from a wide variety of attacks. These threats can be divided into to major categories, threats to the basic networking mechanisms and threats to the security mechanisms. A detailed coverage of the two types of attacks is present in [2]. It also presents various prevention mechanisms.

### *2.1 Attack on Basic Network Infrastructure*

The nodes of the ad hoc network are not assumed to be secured opposed to the nodes of fixed network where they are locked in cabinets. Thus, they have the additional risk of being captured and compromised. The wireless nature of the communication makes these vulnerable to eavesdropping and interference.

The co-operative nature of the ad hoc infrastructure also makes it more vulnerable. Thus a compromised device could be used to paralyze the whole network by not providing the correct information or providing false information.

Some attacks on the basic routing mechanism are described in [3]. The following attacks are possible:

- **Black Hole:** The black hole attack is briefly introduced in [16]. In the attack, 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:** In a wormhole attack, two malicious collaborating nodes which are connected through a private network, can record packets at one location in the

network and tunnel them to another location through the private network and retransmits them into the network [15].

- **Routing table overflow:** In a routing table overflow attack 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.
- **Sleep deprivation:** The sleep deprivation is briefly introduced in [14]. Usually, this attack is practical only in ad hoc networks, where battery life is a critical parameter. Battery powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack.
- **Location disclosure:** A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node.

Prevention of attacks on the routing mechanism will be discussed in detail in the next section.

One possible solution for preventing device tempering is to use smart cards to keep the user's information. The safety of smart card will then be an issue. In order to prevent the routing functions to be compromised, we can embed the software in the smart card. Again smart card will need to be temper proof. A less stringent version of tamper proof-ness would be tamper evidence.

In order to safeguard from node selfishness, we can enforce that service will be provided to the nodes which are contributing to the community. Nuggets [4] have been proposed which can be used for co-operative packet forwarding.

### *2.2 Attack on Security Mechanisms*

Most of the current methods of securing the network can come under attack in a MANET. Such attacks include replacing public keys, compromised private or shared keys. Definitely such threats are also present in fixed network, but the very nature of ad hoc network makes these harder to counter. Most importantly, counter-measures used in fixed networks are inappropriate for ad hoc network.

Key establishment is one of the major issues in MANET. Key may be established by either transportation or agreement. This may be simplified in the presence of central trusted authority or fixed on-line trusted server as is a practice in wired networks. Normally, such trusted and central authorities do not exist and thus various sophisticated mechanism have been proposed. A detailed coverage of such techniques is present in [3].

## 3 Secure Routing

The current research towards the design of secure routing protocols for MANET are mainly towards the on-demand routing protocols.

In this paper critical analysis of only four of the latest secure routing protocols, namely SRP, Ariadne, SEAD, ARAN will be discussed. A detailed analysis of two

older protocols, Ad Hoc On Demand routing Protocol (AODV) and Zone Routing Protocol (ZRP) is present in [3] and [12].

### *3.1 Secure Routing Protocol*

Secure Routing Protocol (SRP) [5] only counters malicious behavior that targets the discovery of topological information. It does not address the protection of data transmission which is handled separately by Secure Message Transmission Protocol (SMT).SRP provides the correct routing information regarding a pair of nodes provided they have prior security association.

SRP sends the route requests to the trusted destinations and replies are sent strictly through the same route. This minimal trust prevents the black hole attack. It also prevents the use of stale or incorrect routing information. A detailed analysis is available in [9].

SRP nevertheless, can not handle wormhole attacks. The solution is the use of packet leashes [15].

### *3.2 Secure Efficient Ad hoc Distance Vector Routing Protocol*

Secure Efficient Ad hoc Distance Vector Routing (SEAD) [7] is a distance vector routing protocol based on Destination Sequences Distance Vector ad hoc routing protocol (DSDV) [13]. In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks, efficient one-way hash functions is used and asymmetric cryptographic operations are not used in the protocol.

The basic idea of SEAD is to use one-way hash chains elements to authenticate the metric and the sequence number of a routing table. The chain can provide a lower bound on the metric, thus the attacker can not lower it. Additionally, the receiver of the routing information also authenticates the sender. The authentication could either be Message Authentication Codes or some broadcast authentication mechanism.

SEAD is robust against multiple uncoordinated attacks, but fails against the wormhole attack. The authors propose the use of TIK (TESLA with Instant Key disclosure) protocol.

### *3.3 Ariadne*

Ariadne, an on-demand routing protocol described in [6] relies on symmetric key cryptography and can withstand node compromises. It can authenticate routing messages using either shared secrets, digital signatures, or shared secrets in combination with broadcast authentication like TESLA [12]. Ariadne was also designed by the same team which designed SEAD.

The protocol enables the target to authenticate the route requests. The initiator includes a MAC computed with key over unique data, which can easily be verified by the target. A per-hop hashing technique is used to verify that no node is missing from the node list. Route maintenance is done using DSR. Ariadne has mechanisms to prevent unauthorized error messages and route misbehaviors.

Ariadne is immune to wormhole attack but only in its advanced version where TIK protocol is used for precise time synchronization between nodes. Under any other operation Ariadne can also suffer from wormhole attack.

### *3.4 Authenticated Routing for Ad hoc Networks*

Authenticated Routing for Ad hoc Networks (ARAN) [8] is an on-demand routing protocol that detects and protects against malicious actions carried out by third party and peers. ARAN uses public key cryptography to guarantee message authentication, integrity and non-repudiation. The use of public key cryptography, limits the protocols to managed-open environments where nodes could easily obtain the public key certificate from a trusted certification authority.

The source node initiates and route discovery packet which is verified by the destination node before a route reply packet being sent through the same patch to the source node where it is verified. Route maintenance is done through special error messages.

ARAN prevents impersonation attacks by providing end-to-end and hop-to-hop authentication of route discovery and reply messages. Non-repudiation and integrity are guaranteed through digital certificates. The only major problem lies in the use of asymmetric key cryptography which is highly costly and a trusted certification authority rarely exists in MANET. ARAN is also not immune to wormhole attack.

## 4 Conclusion

The importance of protecting the ad hoc network is clearly important in the light of prevalent threats. Security aspects form a very complex field due the dynamic and unpredictable nature of MANET.

All the protocols were designed for different conditions. SEAD is a distance vector routing protocol while the rest are on-demand routing protocols. ARAN has been designed for managed-open environments where a central trusted certification authority exists. It is noteworthy that most of these protocols can withstand most of the attacks except wormhole. Only Ariadne and SEAD, when used with TIK protocol for authentication are immune to it.

The best mechanism would be a combination of a solid routing protocol combined with a reliable authentication mechanism and sophisticated data-link layer security.

Many of the security requirements also depend on the application of MANET. Hostile environments demand efficient and strong mechanisms while friendlier ones can make use of such simple mechanisms as username and password. Combined with the limited processing capability and battery life of mobile devices, making a generic security mechanism is not feasible.

## 5 References

[1] Levente Buttyfin and Jean-Pierre Hubaux. Report on a Working Session on Security in Wireless Ad Hoc Networks. Mobile Computing and Communications Review, Volume 7, Number 1. 2003.

[2] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The Quest for Security in Mobile Ad Hoc Networks. Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, Long Beach, CA. 2001.

[3] Janne Lundberg. Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security, http://citeseer.nj.nec.com/400961.html. 2000.

[4] L. Buttyan and J.P. Hubaux. Enforcing service availability in mobile ad hoc networks. In Proceedings of MobiHoc, 2000.

[5] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad hoc Networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX. January 27-31, 2002.

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks. MobiCom 2002, Atlanta, Georgia, USA. September 23-28, 2002.

[7] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of the 10th Conference on Network Protocols (ICNP). November 2002.

[8] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, Calicoon, NY. June 2002.

[9] John D. Marshall, II. An Analysis of The Secure Routing Protocol For Mobile Ad Hoc Network Route Discovery: Using Intuitive Reasoning And Formal Verification. http://citeseer.nj.nec.com/marshall03analysis.html. 2003

[10] Yih-Chun Hu, Adrian Perrig, and David Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. ACM Workshop on Wireless Security (WiSe 2003), San Diego, California. September 19, 2003.

[11] Manel Guerrero Zapata and N. Asokan. Securing Ad-Hoc Routing Protocols. In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pp 1-10. September 2002.

[12] Vesa Karpijoki. Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security. http://citeseer.nj.nec.com/karpijoki01security.html. 2000.

[13] C. Perkins and E Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In *Proceedings of the ACM SIGCOMM Conference on Communication Architectures, Protocols, and Applications*, pp 234-244. August 1994.

[14] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Security Protocols, 7th International Workshop Proceedings*, Lecture Notes in Computer Science, 1999.

[15] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, CA. April 2003.

[16] Feiyi Wang, Brian Vetter and Shyhtsun Wu. Secure Routing Protocols: Theory and Practice. North Carolina State University. May 1997.