International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Secure Mobile Ad hoc on Reactive Routing Protocols

Pardeep Nehra
Department of Computer Science
E-Mail:- par.nehra82@yahoo.com

Abstract: *Ad hoc wireless networks assume no pre-deployed infrastructure is available for routing packets end-to-end in a network, and instead rely on intermediary peers. Securing ad hoc routing presents challenges because each user brings to the network their own mobile unit, without the centralized policy or control of a traditional network. Especially, Security flaws of routing protocol may cause severe problems under ad hoc network. In this paper we briefly present the most popular on-demand routing protocol ADOV and potential security problems of AODV. Then, this paper analyzes security requirements for ad hoc routing protocols and proposed solutions.*

Keywords: MANET, ARAN, AODV, SAR, SRP.

Introduction:

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. 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. We focus here on *on-demand* (or reactive) routing protocol for ad hoc networks, in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. On-demand routing protocols have been demonstrated to perform better with significantly lower overheads than periodic (or proactive) routing protocols in many situations, since they are able to react quickly to the many changes that may occur in node connectivity, yet are able to reduce (or eliminate) routing overhead in periods or areas of the network in which changes are less frequent.

Related Work:

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins

and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand to secure ad hoc networks by using misbehavior detection schemes. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving (especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures); and second, it has no real means to guarantee the integrity and authentication of the routing messages. He proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. He proposed a protocol (SRP) that can be applied to several existing routing protocols . SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. Securing the AODV protocol has been made by Zapata with his SAODV. This is the background of secure routing protocols for the AODV routing protocol. In this paper I review all these routing protocols.

Exploits allowed by existing protocols:

Current ad hoc routing protocols also inherently trust all participants because most of them are based on the routing protocols of wired networks. Thus, most ad hoc routing protocols are cooperative and depend on neighboring nodes to route packets. However, this naïve trust model allows a malicious attacker to paralyze an entire ad hoc network by easy way, such as inserting erroneous routing information. To achieve availability of ad hoc networks, routing protocols should be robust against this kind of malicious attacks. Then, let's look at the common security threats in ad hoc routing protocols. There are two sources of attacks to routing protocols. The first one is done by external attackers.

1. **Passive attack:**

It means that the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect.

2. **Active attack:**

Besides the passive attack, this active attack is performed by the attacker who can inject arbitrary packets into the network. The goal may be to attract packets destined to other nodes

to the attacker for analysis or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. But, a stealth attack, which is proposed in recent paper, enables the attacker to do the same kind of active attack with hiding his existence.

Security Requirements of Ad hoc Networks:

A good secure routing algorithm prevents each of the exploits presented it must ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation. In sum, all secure ad hoc routing protocols must satisfy the following requirements to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries. The term security protocol traditionally refers to authentication protocols, or cryptographic protocols, where the goal is to securely share information (e.g., a message or a session key) between two nodes. Security analysis for authentication protocols evaluates if it is possible for a third party (i.e., the adversary) to obtain access to the protected key, regardless of intermediate nodes within the communication path. Conversely, security evaluations for MANET secure routing protocols must consider actions taken by intermediate nodes.

Secure Ad hoc Routing:

There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned in the previous section. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR and AODV). As we will see, the design of these solutions focuses on providing counter measures against specific attacks, or sets of attacks. Furthermore, a common design principle in all the examined proposals is the performance-security trade-off balance. Since routing is an essential function of ad hoc networks, the integrated security procedures should not hinder its operation.

1. **ARAN:**

ARAN was proposed targeting to combat attacks including unauthorized participation, spoofed route signaling, alteration of routing messages, replay attacks, etc. Similar to other secure routing protocols, ARAN is also a security adds on over on-demand routing protocols. It provides authentication, message integrity and non-repudiation as part of minimal security policy for ad hoc environment.

2. SAODV:

SAODV proposed for assume that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. How this is achieved depends on the key management scheme.

3. SAR:

There is another approach to secure the ad hoc routing protocol motivated from traditional wired routing matrices where same security levels of nodes incorporate each other. Instead of discovering the shortest path between two nodes, Security Aware Ad Hoc Routing (SAR) protocol can discover a path with desired security attributes, such as a path through nodes a particular shared key. For this purpose to determining a secure route, the information in the routing messages must be protected against alteration that can change routing behavior. One of the merits SAR has is that it can be implemented based on any on-demand ad hoc routing protocol with suitable modification. The security metric can be embedded into RREQ packet. It also showed the practical implementation and experimental data by mixing with AODV.

4. SRP:

SRP focus on bi-directional communication between a pair of nodes. A security association (SA) between the source node S and the destination node T is assumed. The trust relationship could be instantiated, for example, by the knowledge of the public key of the other communicating end. The two nodes can negotiate a shared secret key, e.g., via the Elliptic Curve Diffie-Hellman algorithm, and then, using the SA, verify that the principal that participated in the exchange was indeed the trusted node. For the rest of the discussion, we assume the existence of a shared key KST. The SA is bi-directional in that the shared key can be used for control (data) traffic flow in both directions. Relevant state has to be maintained for each direction though. SRP consists of several security extensions that can be applied to existing ad hoc routing protocols providing end-to-end authentication. The operational requirement of SRP is the existence of a security association between every source and destination node. The security association is used to establish a shared secret between the two nodes, and the non-mutable fields of the exchanged routing messages are protected by this shared secret.

Protocols	Attacks					
	Location disclosure	**Black hole**	**Replay**	**Wormhole**	**Denial-of-service**	**Routing table poisoning**
ARAN	NO	NO	YES	NO	NO	YES
SAODV	NO	NO	YES	NO	NO	YES
SAR	NO	NO	YES	NO	NO	YES
SRP	NO	NO	YES	NO	YES	YES

Defense against attacks

Conclusion: Secure Routing is one of the most basic and important tasks in a collaborative computer network. This review presented the security flaws of AODV and routing protocols which provide security over the AODV. However, a difficult problem is how to guarantee these desirable properties. Neither simulations nor test bed implementations can ensure the quality required for these protocols. As an alternative to these methods, some researchers have successfully investigated the use of formal verification as a mean to guarantee the quality of routing protocols. Formal verification is a technique that assures a system has, or has not, a given property, based on a formal specification of the system under evaluation. We conclude that more work is needed towards a formal model based on solid mathematical grounds that can precisely give a definition for secure ad hoc routing. This will allow researchers to formally prove whether a proposed protocol satisfies the definition under

certain assumptions and will make the comparison between the properties of each proposal an easier and well-structured process.

REFERENCES:

1. Das S. Perkins C.E., Belding-Royer E.M. Ad-hoc on-demand distance vector (aodv) routing. RFC 3561, IETF Network Working Group, 2003.

2. L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.

3. S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pages 255–265, 2000.

4. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78-87.

5. J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

6. J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

7. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.

8. P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

9. M.G. Zapata, and N. Asokan, "Secure Ad hoc On-Demand Distance Vector Routing," *ACM Mobile Computing and Communications Review*, vol. 3, no. 6, July 2002, pp. 106-10

10. Mitchell, J. C., Mitchell, M., Stern, U. : Automated Analysis of Cryptographic Protocols Using Murphi. IEEE Symposium on Security and Privacy. (1997) 141–151

11. Dolev, D., Yao, A.C.: On the security of public key protocols. IEEE Transactions on Information Theory. 29(12) (1983) 198–208

12. W. Diffie, M.E. Hellman, "New directions in cryptography," IEEE Transactions in Information Theory, 1976.

13. Zheng Yan, "Security in Ad Hoc Networks", Networking Laboratory, Helsinki University of Technology, 2001