A Review of Secure Ad-hoc Routing

Tannu Arora[1], Deepika Arora[2]

**[1] Computer Science, M.D.U/GIET,
Sonipat, Haryana, India**
tannu.arora@gmail.com

**[2] Computer Science, C.D.L.U,
Sirsa, Haryana, India**
deepika_arora_deepu@yahoo.com

Abstract

An ad-hoc network is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network. The emergence of the Mobile Ad Hoc Networking (*MANET*) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. Mobile Ad hoc Networks are assortment of mobile terminals or nodes, allowing no stationary infrastructure and centralized administration**.** In this paper, we present a survey of existing and secure ad hoc routing protocols for wireless networks and then compare them in the trusted environment. We briefly present the most popular protocols for ad-hoc networks. A performance evaluation of routing protocol is very cumbersome due to various metrics involving dynamic topologies, mobility, routing limited resources, security etc. In this paper, various existing routing protocols are reviewed. The goal of this paper is to show the limitations of existing unsecure ad-hoc protocols which are more vulnerable to various kind of attacks.

Keywords: *Ad hoc Network, MANET, Security, Routing Protocols*

1. Introduction

Wireless networks consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, cellular networks and satellite networks. Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. 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. Figure 1 shows three nodes where ad hoc network where every node is connected to wireless, and work as access point to forward and receive data.

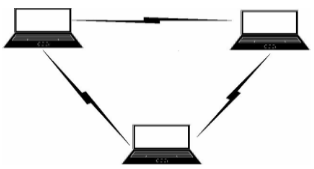


Fig. 1: Ad-hoc Network

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. On the other hand, a similar concept without infrastructure can be observed in the Peer-to-Peer networking area. In this case the IP-layer provides the basic communication medium, which enables IP capable terminals to reach anyone and anything attached to the IP-network. Peer-to-Peer and mobile ad hoc networks are established on a different basis. Peer-to-Peer is based on an IP network and Mobile Ad Hoc networks are based on a mobile radio network. However both networks hold similarities concerning their routing and network management principles.

2. Review of Routing Protocols in Ad-Hoc Network

Routing in mobile ad hoc networks faces additional problems and challenges, when compared to routing in traditional wired networks with fixed infrastructure. Mobile ad hoc network does not rely upon any fixed support infrastructure. By varying distance, connectivity and disconnectivity of nodes can be controlled. So, routing is very important issue in ad-hoc networks. Each node in the network must be able to take care of routing of the data and can discover multihop paths. Routing in mobile ad hoc networks faces additional problems and challenges, when compared to routing in traditional wired networks with fixed infrastructure.

2.1 Proactive and Reactive Routing Protocols

Ad Hoc routing protocols can be broadly classified as being Proactive (Table-Driven) or Reactive (On- Demand).

In a *Proactive routing protocol*, all the routes to each destination are kept in an up-to-date table. Changes in the network topology are continually updated as they occur. The disadvantage of proactive routing algorithms is the number of required topology updates within a time period. In case the number of nodes belonging to a network rises over a certain threshold, this kind of routing algorithm is not feasible anymore.

In the *Reactive routing protocol*, a connection between two nodes is only created when it is asked for by a source. When a route is found, it is kept by a route maintenance procedure until the destination no longer exists or is indeed. The following table 1 presents a comparison between proactive and reactive routing protocols.

Table 1: Proactive Versus Reactive Protocols

Protocol	**Proactive**	**Reactive**
Advantages	**A route can be selected immediately without delay.**	• **Lower bandwidth** • **Effective route maintenance.**
Disadvantages	**Takes a lot more bandwidth**	• **Higher latencies w.r.to route.**

Figure 2 shows the ad -hoc Networks routing protocols list:

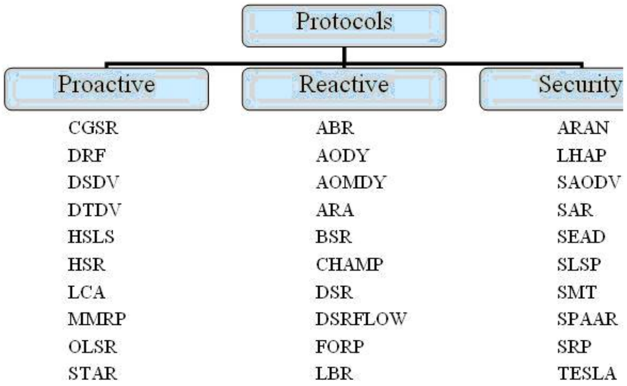


Fig. 2: Ad Hoc Networks Routing Protocols List

2.2 DSDV

The Destination Sequenced Distance Vector[3] Routing protocol is the best known protocol for a proactive routing scheme. It is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways:- a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent.

Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon.

2.3 WRP

The Wireless Routing Protocol (WRP) is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list. WRP, similar to DSDV, inherits the properties of the distributed Bellman-Ford algorithm. Since WRP, like DSDV, maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network. It differs from DSDV in table maintenance and in the update procedures. While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information. The tables that are maintained by a node are the following: distance table (DT), routing table (RT), link cost table (LCT), and a message retransmission list (MRL).

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor. WRP requires large memory storage and resources in maintaining its tables. The protocol is not suitable for large mobile ad hoc networks as it suffers from limited scalability.

2.4 DSR

The Dynamic Source Routing[3] is one of the major on demand routing algorithms. It is based on the concept of source routing. The protocol includes two major phases: route discovery and route maintenance. The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet.

The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet.

2.5 AODV

Ad hoc On-Demand Distance Vector Routing[7] is also an on demand routing algorithm, but in contrast to DSR not source based routing, but every hop of a route maintains the next hop information by its own. Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 3). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 4), the nodes along the path enter the forward route into their tables.

If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

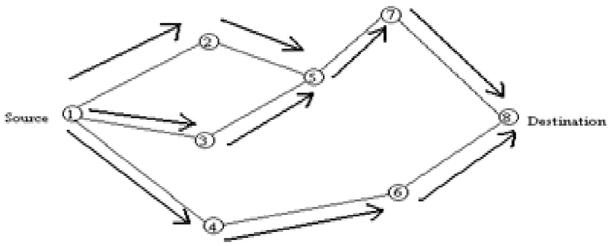


Fig. 3: Propagation of Route Request (RREQ) Packet

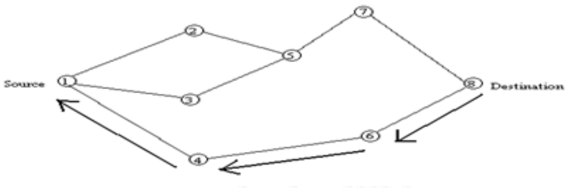


Fig. 4: Path taken by Route Reply (RREP) Packet

3. Attacks targeting Routing Protocols

There are basically two types of security threats to a routing protocol, external and internal attackers. An external attacker can be in the form of an adversary who injects erroneous information into the network and cause the routing to stop functioning properly. The internal attacker is a node that has been compromised, which might feed other nodes with incorrect information.

3.1 Active and Passive Attacks

Security exposures of Ad Hoc routing protocols are due to two different types of attacks: active and passive attacks. In active attacks, the misbehaving node has to bear some energy costs in order to perform some harmful operation. In passive attacks, it is mainly about lack of cooperation with the purpose of energy saving. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

3.2 Malicious and Selfish Nodes in MANETs

Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network by simply not participating in the network operation.

In existing Ad Hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. Malicious nodes can easily perpetrate integrity attacks by simply altering protocol fields in order to subvert traffic, deny communication t legitimate nodes (denial of service) and compromise the integrity of routing computations in general. As a result the attacker can cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination increasing communication delays.

A special case of integrity attacks is spoofing whereby a malicious node impersonates a legitimate node due to the lack of authentication in the current Ad Hoc routing protocols. The main result of spoofing attacks is the misrepresentation of the network topology that possibly causes network loops or partitioning.

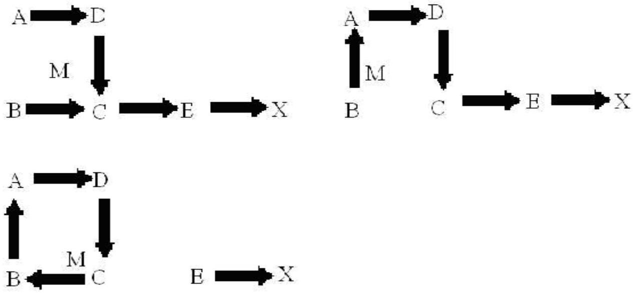


Fig 5: Impersonation in creating Loops

In figure 5, a malicious attacker M can form a routing loop so that none of the four nodes can reach the destination. To start the attack, M changes its MAC address to match A's, moves closer to B and out of the range of A. It then sends an RREP to B that contains a hop count to X that is less than the one sent by C, for example zero. B therefore changes its route to the destination, X, to go through A. M then changes its MAC address to match B's, moves closer to C and out of range of B, and then sends to C an RREP with a hop count to X lower than what was advertised by E. C then routes to X through B. At this point a loop is formed and X is unreachable from the four nodes.

Lack of integrity and authentication in routing protocols can further be exploited through "fabrication" referring to the generation of bogus routing messages. Fabrication attacks cannot be detected without strong authentication means and can cause severe problems ranging from denial of service to route subversion.

3.3 Routing Protocols' Security Requirements

To solve security issue in an Ad Hoc network and make it secure we have to look at a number of requirements that have to be achieved. These requirements are: availability, confidentiality, integrity, authentication and the non-repudiation.

- **Availability:** The network must at all times be available to send and receive messages despite if it is under attack. An attack can be in the form of a denial of service or an employed jamming to interface with the communication. The node itself can also be the problem to availability.

- **Confidentiality**: Provides secrecy to sensitive material being sent over the network. This is especially important in a military scenario where strategic and tactical information is sent. If this information is sent. If this information would fall into enemy hands it could have devastating ramifications.

- **Integrity:** It ensures that messages being sent over the network are not corrupted. Possible attacks that would compromise the integrity are malicious attacks on the network or benign failures in the form of radio signal failures.

- **Authentication:** It ensures the identity of the nodes in the network. If A is sending to B, A knows that it is B who is receiving the message. Also B knows that it is A who is sending the message. If the authentication is not working, it is possible for an outsider to masquerade a node and then be able to send and receive messages without anybody noticing it, thus gaining access to sensitive information.

- **Non-Repudiation:** It makes possible for a receiving node to identify another node as the origin of a message.The sender cannot deny having sent the message and are therefore responsible for its contents. It is particularly useful for detection of compromised nodes.

4. Secure Ad Hoc Routing Protocols

Securing protocols for mobile ad hoc networks presents unique challenges due to characteristics such as lack of pre-deployed infrastructure, centralized policy and control.

4.1 ARAN

Authenticated Routing for Ad hoc Networks[2] makes use of cryptographic certificates to offer routing security. ARAN is an on-demand protocol. Nodes keep track of whether routes are active. When no traffic has occurred on an existing route for that route's lifetime, the route is simply deactivated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message that travels the reverse path toward the source. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR messages must be signed.

ARAN introduces *authentication*, *message integrity*, and *non-repudiation* to routing in an ad hoc environment as a part of a minimal security policy. ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. The protocol is simple compared to most non-secured ad hoc routing protocols. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source.

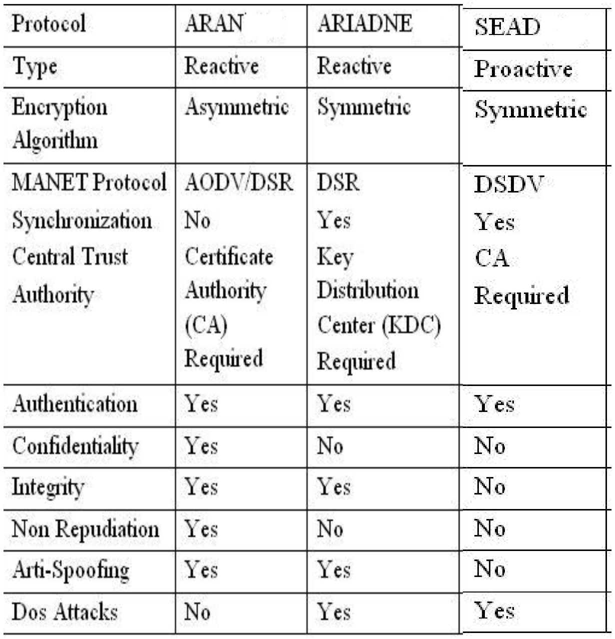
4.2 ARIDANE

A new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks.

4.3 SEAD

Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this review, we evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD)[2], a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV).

Table 2: Secure Ad Hoc Routing Protocols Comparison



Protocol	ARAN	ARIADNE	SEAD
Type	Reactive	Reactive	Proactive
Encryption Algorithm	Asymmetric	Symmetric	Symmetric
MANET Protocol	AODV/DSR	DSR	DSDV
Synchronization	No	Yes	Yes
Central Trust Authority	Certificate Authority (CA) Required	Key Distribution Center (KDC) Required	CA Required
Authentication	Yes	Yes	Yes
Confidentiality	Yes	No	No
Integrity	Yes	Yes	No
Non Repudiation	Yes	No	No
Arti-Spoofing	Yes	Yes	No
Dos Attacks	No	Yes	Yes

In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

As a result, in the table 2, a comparison between some of the most established secure routing protocols[2] with respect to some performance and security parameters is given so that to facilitate the choice of one of them to work on.

5. Conclusion

Security exposures of ad-hoc routing protocols are due to different types of attacks. Existing ad hoc routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of-service attacks. In existing Ad Hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. On the other hand, there are some secure routing protocols that developed in past years, which provides a solution for securing routing in the managed-open environment. Examples of such protocols are ARAN, ARIDANE and SEAD. However their security and performance parameters differ from one another in some respect but they provide a trusted environment for routing as compared to other proactive and reactive routing protocols.

References

[1] 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

[2] Karan Singh, R. S. Yadav, Ranvijay, A Review Paper on Ad-hoc Network Security**,** International Journal of Computer Science and Security, Volume (1): Issue (1)

[3] Umang Singh**,** Secure Routing Protocols In Mobile Ad-hoc Network-A Survey and Taxanomy, International Journal of Reviews in Computing, 30th September 2011. Vol. 7

[4] P. Papadimitratos, "Secure Routing: Methods for Protecting Routing Infrastructures – A Survey," work in progress.

[5] Y.-C. Hu, D. B. Johnson, and A. Perrig., *"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks"* In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, page 3. IEEE Computer Society, 2002.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine October 2002.

[7] C. Perkins, "Ad-hoc on-demand distance vector routing," in MILCOM '97 panel on Ad Hoc Networks., Nov. 1997.

[8] C. Perkins, E. Royer, "Ad hoc On demand Distance Vector Routing", Proceeding of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999

[9] C. Perkins, E. Royer, and S. Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF Internet draft, draft-ietf-manet-aodv-09.txt, November 2001.