Solutions for Secure Routing in Mobile Ad Hoc Network (MANET): A Survey

Aaditya Jain¹ & Dr. Bala Buksh²

¹M.Tech. Scholar, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University Kota, Rajasthan, India.
²Professor, Department of Computer Science & Engg., R. N. Modi Engineering College, Rajasthan Technical University Kota, Rajasthan, India.

Abstract: Now a day’s mobility is becoming increasingly important for users of computing systems, science and technology has made it possibly more powerful. In wireless communication mobile computing support like access points is not available in all locations, due to high cost, low expected usage, poor performance. This may happen during outdoor conferences or in emergency situations like natural disasters and military services in inaccessible places. If mobile users want to communicate without a support structure, they must form new class of network called Mobile Ad Hoc Network (MANET). In this paper we briefly discuss about the concept of MANET and various solutions for performing secure routing in MANET.

Keyword– MANET, AODV, DSR, CSRP.

1. Introduction

Mobile Ad hoc Network (MANET) is an infrastructure less autonomous system of mobile nodes connected by wireless links. Each node not only acts as end system, but also as a router to forward packets. The nodes are free to move and organize themselves and change topology dynamically as shown in figure 1. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. The mobility of nodes in MANETs increases the complexity of the routing protocols and the degree of connection’s flexibility. However, the flexibility of allowing nodes to join, leave, and transfer data to the network pose security challenges. MANET is more vulnerable due to the lack of central authority. Different mechanisms have been proposed using various cryptographic techniques to counter measure the routing attacks against MANET. In this paper we discuss about various routing protocols with their basic functionalities.

Figure 1. Dynamic topology in MANET

2. Routing Strategies in MANET

The security issues in MANET are mostly concentrated in two parts establishing secure route and securely data transmission [1]. Routing protocol in MANET is not free from attacks. So to communicate securely we need a secure routing algorithm first, otherwise only secure data communication cannot meet with all security aspects of MANET. Basically three types of strategies used for routing in MANET: Proactive, Reactive and Hybrid [2].

2.1. Proactive Routing Protocol

Proactive routing protocols are also called as table driven routing protocols. All the routes to each destination are maintained in an up-to-date table. If any Changes made in the network topology are continually updated as they occur. Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP) comes in this category.

2.2. Reactive Routing Protocol

Reactive routing protocol is also known as on demand routing protocol. In this protocol route is discovered whenever it is needed. Nodes initiate route discovery on demand basis. Source node sees its route cache for the available route from source to destination if the route is not available then it initiates route discovery process. Ad Hoc On
Demand Distance Vector (AODV) routing, Dynamic Source Routing (DSR) are two basic strategies used in this protocol.

2.2.1. AODV Routing Protocol. In AODV routing protocol, source node flood the route request (RREQ) to its neighbour nodes to reach the destination. Intermediate nodes check its destination node if the node itself is not the destination then it rebroadcast the RREQ packet in similar manner until it reaches the destination [3]. On receiving the RREQ, destination node generates the RREP packet and replies it through the reverse path in unicast manner.

![Figure 2. AODV routing strategy](image)

2.2.2. DSR Routing Protocol. DSR routing protocol is almost similar to the AODV routing protocol, except that each intermediate node that broadcasts a route request (RREQ) packet adds its own address identifier to a list carried in the packet [4].

![Fig 3. DSR routing strategy](image)

2.3. Hybrid Routing Protocol

It is a trade-off between proactive and reactive protocols. Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So the concept of Hybrid Protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Sharp Hybrid Adaptive Routing Protocol (SHARP), Zone routing protocol (ZRP) comes in this category.

3. Proposed Solutions for Secure Routing

There exist several proposals that attempt to architect a secure routing protocol for MANET networks, in order to offer protection against the various routing attacks.

K. Sanzgiri et al. proposed a secure routing protocol called “Authenticated Routing for Ad Hoc Network (ARAN)” in [5]. It is an on-demand secure routing protocol detects and protects against authentication, message integrity and non-repudiation. It uses asymmetric key cryptography. ARAN requires trusted certification server, the certificate accommodates the IP address of the node, its public key and a time-stamp of when the certificate was created and a time at which the certificate expires along with the signature by certification authority. But the disadvantages of ARAN are it uses the central authority (Certification Authority) and it can't protect against wormhole attack.

Yih-Chun Hu et al. proposed a protocol called “Secure Efficient Ad hoc Distance vector (SEAD)” in [6]. It is a secure ad hoc network routing protocol based on the design of the Destination Sequenced Distance Vector (DSDV) algorithm. In order to find the shortest path between two nodes, the distance vector routing protocols utilize a distributed version of the Bellman-Ford algorithm. The SEAD routing protocol employs the use of hash chains to authenticate hop counts and sequence numbers. Applying repeatedly a one-way hash function to a random value creates a hash chain. The elements of such a chain are used to secure the updates of the routing protocol. SEAD requires the existence of an authentication and key distribution scheme in order to authenticate one element of a hash chain between two nodes.

Manel Guerrero Zapata proposed a routing protocol called “Secure Ad Hoc On-Demand Distance Vector (SAODV)” Routing in [7]. It is a extension of AODV protocol. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and non repudiation. But in ad hoc network each node will know the others public key so it a challenge.

Adrian Perrig et al. proposed a secure on demand ad hoc routing protocol called “ARIADNE” in [8]. It is based on dynamic source routing protocol and provides point-to-point authentication of a routing packets using a message authentication code (MAC) and a shared key between nodes. For
broadcasting RREQ packets it uses TESLA broadcast authentication protocol. TESLA keys are distributed to the participating nodes via an online key distribution center. The Ariadne protocol also specifies a mechanism for securing route maintenance, which ensures the validity of route error messages concerning broken links in the ad hoc network. The most important requirement of Ariadne is the existence of clock synchronization in the ad hoc network.

Panagiotis Papadimitratos et al. proposed routing protocol called “Secure Link State Routing Protocol (SLSP)” in [9]. It is based on proactive routing protocol and to function effectively without central key management authority, SLSP enables each node to periodically broadcast its public key to nodes within its zone. The main operational requirement of SLSP is the existence of an asymmetric key pair for every network interface of a node. Participating nodes are identified by the IP addresses of their interfaces. To achieve the goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP. SLSP limits its scope to secure only the process of topology discovery; parties that participate in it and decide to misbehave during data transmission are not detected or penalized. As mentioned by the authors, SLSP is vulnerable to colluding attackers that fabricate non-existing links between themselves and flood this information to their neighboring nodes.

J. Lundberg proposed “on demand secure routing protocol resilient to byzantine failures (OSRP)” in [10]. This protocol is able to function in the presence of colluding nodes introducing byzantine failures in the process of routing. Their approach is based on the detection of faulty links after log n faults have occurred, where n is the length of the route. The protocol bases on demand route discovery on weight values of paths, and the paths that are identified as malicious are assigned increased weights. The protocol is separated into three different phases: route discovery with fault avoidance, byzantine fault detection, and link weight management. The metric upon which path selection is based consists of link weights, where high weights represent an unreliable path. Every node that participates in the network is required to maintain a weight list and update it according to the results of the fault detection phase. As the authors note, a limitation rests in the inability of the protocol to prevent wormhole attacks. However, if the wormhole link demonstrates byzantine behavior then the protocol will detect it and avoid it.

Vincent Park et al. proposed a protocol based on, on demand routing called “Temporally Ordered Routing Algorithm (TORA)” [11]. It is a reactive routing protocol with some proactive enhancements where a link between nodes is established creating a Directed Acyclic Graph (DAG) of the route from the source node to the destination. This protocol uses a link reversal model in route discovery. A route discovery query is broadcasted and propagated throughout the network until it reaches the destination or a node that has information about how to reach the destination. TORA defines a parameter, termed height. Height is a measure of the distance of the responding node’s distance up to the required destination node. In the route discovery phase, this parameter is returned to the querying node. As the query response propagates back, each intermediate node updates its TORA table with the route and height to the destination node. The source node then uses the height to select the best route toward the destination. This protocol has an interesting property that it frequently chooses the most convenient route, rather than the shortest route. For all these attempts, TORA tries to minimize the routing management traffic overhead.

S. K. Bhoi et al. proposed on demand based “Centralized Secure Routing Protocol (CSRP)” in [12]. The main idea behind CSRP algorithm is its centralized architecture which consists of a Master Node (MN) which manages and controls the whole data communication and security in the network. Here, we have assumed MN as a genuine node and it is trusted by every other node. Another assumption we have considered is the use of a third party (organization) which sets the general nodes in an area by placing a secret key (SK). SK is common in MN and general nodes. It places the public keys e, n and hash function in MN and it also places the signature S in the general nodes. For example, if a malicious node wants to communicate or wants to enter into the area then it has to verify its identity which is easy for the MN to clearly identify the genuine node and imposter node.

If a node wants to communicate with another node in MANET then the MN will generate a session key between them. For generation of session key between two nodes N1 and N2, N1 has to send request to MN for establishing a session key K_{MN2} with N2 (neighbor). This process continues until we reach the destination. Then we flood the RREQ requests to the trusted neighboring nodes. Then we continue the process until we reach the destination. We consider the RREQ which reach first and then we send a RREP from destination to source through the route taken by first RREQ. The data with the route as header is relayed by encrypting it with the session key of the two nodes and it is decrypted with the same session key on other end. This process continues till the destination is attained. This is how the data is relayed securely from source to destination.
4. Conclusion

In the current era of wireless network, popularity of MANET is increasing at a very fast pace. Reason for this increased attention is the wide range of multimedia applications running in an infrastructure less environment. Because of the infrastructure less environment, limited power and dynamic topology it becomes very difficult to provide a secure routing environment in MANET. Various solutions which are proposed in recent years are describes in this paper but prevention from all attacks still an open challenge problem.

5. References