Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)

L. Ertaul[1], D. Ibrahim[2]
[1]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA, Levent.Ertaul@csueastbay.edu
[2]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA, dibrahim@arcsight.com

Abstract- *Mobile Ad hoc networks (MANETs) have several advantages compared to traditional wireless networks. These include ease of deployment, speed of deployment and decreased dependency on a fixed infrastructure. There have been many studies done in this area to improve the quality and efficiency of the routing protocols in MANETs. However unique characteristics of MANETs topology such as open peer-to-peer architecture, dynamic network topology, shared wireless medium and limited resource (battery, memory and computation power) pose a number of non-trivial challenges to security design. These challenges and characteristics require MANETs to provide broad protection and desirable network performance. In this paper, we examine the available secure routing protocols in MANETs such as Secure On-Demand Routing Protocol – Ariadne, Secure Ad hoc On-demand Distance Vector routing protocol – SAODV, Security Aware Routing Protocol – SAR, Secure Efficient Distance Vector Routing – SEAD, Securing the Destination Sequenced Distance Vector Routing Protocol – SDSDV, Secure Link State Routing protocol – SLSP, On-Demand Secure Routing Protocol Resilient to Byzantine Failures, Authenticated Routing for Ad-hoc Networks – ARAN, Secure Position Aided Ad hoc Routing – SPAAR. We identify the advantages and disadvantages of each protocol, we compare them based on some security parameters, and also we discuss some open challenges present in ad hoc secure routing.*

Keywords —MANETs, secure routing protocols, ad hoc security.

1 Introduction

IN MANET'S world, devices such as laptops, PCs, cellular phones, appliances with ad hoc communication capability link together on the fly to create a network. This technology is the key to solving today's most common communication problems such as having a fixed infrastructure, and centralized, organized connectivity, etc. MANET is a self-configuring network of mobile routers and associated hosts connected by wireless links. The routers (mobile devices, nodes) are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. The network appears on-demand, automatically and instantly, and data hops from ad-hoc device to device till it reaches its destination, the network updates and reconfigures itself to keep nodes connected. The network topology changes when a node joins in or moves out. Packet forwarding, routing, and other network operations are carried out the by the individual nodes themselves [2].

In MANETs with each node acting as a router and dynamically changing topology the availability is not always guaranteed. It is also not guaranteed that the path between two nodes would be free of malicious nodes. The wireless links between nodes are highly susceptible to link attacks (passive eavesdropping, active interfering, etc). Stringent resource constrains in MANETs may also affect the quality of security when excessive computations is required to perform some encryption. These vulnerabilities and characteristic make a case to build a security solution, which provides security services like authentication, confidentiality, integrity, non-repudiation and availability. In order to achieve this goal we need a mechanism that provides security in each layer of the protocol. [1], [2]

Protection of MANETs can be divided into these two categories, protection of the routing functionality (secure ad hoc routing) and protection of the data in transmission (secure packet forwarding). The way of approaching the MANETs protection can also be divided into two categories, proactive and reactive. Proactive approach attempts to prevent an attacker from launching attacks, through cryptographic techniques. In reactive approach it seeks to detect threat and react accordingly. [1]

The main objective of this paper is to give an overview of secure routing protocols, security analysis of each protocol, and also comparison of those secure routing protocols. The remainder of this paper is structured into six sections. Section 2 introduces the routing protocols in MANETs. Section 3 explains the security attacks and challenges. Section 4 discusses how secure routing protocols work. Section 5 discusses the security analysis of each secure routing protocol. Section 6 compares the secure routing protocols and Section 7 addresses the open challenges.

2 Routing in MANETs

Routing protocols in MANETs can be divided into proactive, reactive and hybrid protocols, depending on the network topology.

Proactive protocols are also called table-driven routing protocols. They attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Some of the table-driven ad-hoc routing protocols are Destination-Sequenced Distance-Vector (DSDV) [4], Wireless Routing Protocol (WRP) [3], and Clusterhead Gateway Switch Routing (CGSR) [3]. In small networks, proactive routing can be efficient, as normal communication does not involve any delay in the route setup. When the size of the network increases, this scheme is quite cumbersome, as the number of routes in the network increase to ratio $O(n^2)$, where n is the number of nodes in the network. Maintaining huge routing tables requires storage space, network bandwidth and processing time, all of which are scarce in MANETs [26]. Major problem with proactive routing is that if the topology of the network changes or when a new node enters or an old node leaves the network, a node that moves to a new location must make its presence known to all the neighboring nodes. All the peers in the network need to find a new optimal route to the node and vice versa. Because of the broadcast property of route request this causes a huge overhead and potential delay to the traffic in the network [27].

Reactive protocols also called on-demand-driven routing protocol. In contrary with table-driven routing protocols, they do not update the routing information periodically. It creates routes only when desired by the source node. Some of the on-demand-driven routing protocols are Ad-hoc On-Demand Distance Vector Routing (AODV) [3], [5], Dynamic Source Routing (DSR) [3], [6]. A problem with on-demand routing is keeping up with the nodes in the network. Because of the reactive nature, nodes do not have to announce their arrival of departure from the network. This means that the intended recipient might already have left the network when the sender wants to initiate transmission. A route request still has to be transmitted throughout the whole network, consuming resources of all the nodes. Reactive protocol can be improved by using promiscuous route discovery [26].

Hybrid protocols make use of both reactive and proactive approaches. They typically dynamically switch between proactive and reactive parts of the protocol. For instance, table-driven protocols can be used between networks and on-demand protocols inside the network or vice versa. Example is the Zone Routing Protocol (ZRP) [19], [18]. A form of hybrid routing is cluster base routing. Cluster base routing means that a group of closely located nodes form a cluster. The nodes choose a cluster head that is responsible for all routing to nodes outside the cluster [26].

Many secure routing protocols that are available now, are secure extension of one of the routing protocols described .

3 Security of MANETs

In MANET environment the security of each individual network node is very important due to pervasive nature of MANETs. A network node will not always be under the control of their owners and as a result physical security of the node becomes a very important issue. [5]

Lack of support infrastructure may prevent the application of standard techniques for key agreement. Due to dynamically changing topology the availability is not always guaranteed. Set of nodes could be compromised in such a way that incorrect behavior cannot be directly detected. Due to freely roaming nodes, it is difficult to have a clear picture of the network membership. Consequently, in large scaled networks no form of established trust relationships among the nodes can be assumed. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, leakage of secured information, data tampering, impersonation, message reply, and denial of service. All these characteristics and vulnerabilities of MANETs, poses many challenges to build a secure MANET. [1], [2]

There are two levels of attacks to MANETs. Attacks on the basic functionality of the MANET, such as routing, and attacks on the information on transit. Attacks on the MANETs routing can be categorized into two groups: internal attacks and external attacks. External attacks then again can be divided into passive attacks and active attacks. Passive attacks usually are the result of eavesdropping of data, and active attacks on the other hand involve actions performed by malicious nodes. [2]

Internal Attacks are severe threat to MANETs. The attack may broadcast wrong routing information to other nodes within the network. A compromised node is categorized as an internal attack. Detecting such wrong information in routing is difficult because compromised nodes are able generate valid signatures using their private keys. Dedifferentiating between and actual attacker and a change in topology may be problematic because the topology of the MANETs dynamically changes. [2]

External Passive attacks on routing involve unauthorized “listening” to the routing protocols. The attack might be an attempt to gain routing information from which the attacker could extrapolate data about the positions of each node in relation the others. The attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routed traffic. Active attacks on the network from outside sources are meant to degrade or prevent message flow between the nodes. Active external attacks on the ad hoc routing protocol can collectively be describe as denial-of-service (DoS) attacks, causing a degradation or complete halt in communication between nodes. To perform an active attack, the attacker must be able to inject arbitrary packets in to the network. An

active attacker most of the time can be detected this makes active attacks a less inviting option for most attackers. Some types of active attacks that can be easily performed against MANETs are Black hole, routing table over flow, sleep deprivation, and location disclosure [2].

Threats on data packets include interruption, interception and subversion, modification and fabrication [2].

The main challenge of MANETs comes from their open peer-to-peer architecture. Each mobile node in MANETs may function as a router and forward packets for other nodes. Therefore, the wireless channel is accessible to both users and attackers. The stringent resource constraints in MANETs constitute other non-trivial challenges. The wireless channel is bandwidth constrained and shared among multiple networking entities. Since the mobile devices are typically powered by batteries, they may have very limited energy resources. The network topology is also highly dynamic as nodes frequently join or leave the network, and roam in the network on their own will. Mobile users may request for anytime, anywhere security services they move from one place to another. [1], [2]

The security schema that can solve the open challenges present in the MANETs need to work within its own resource limitations in terms of computation capability, memory, communication capacity, and energy supply. First the security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single layer solution is possible to thwart all potential attacks. Second, the security solution should thwart threat from both outsider and insider. Third, the security should encompass all three components of prevention, detection, and reaction. Last the solution should be practical and affordable in a highly dynamic and resource constrained networking scenario [1][2].

A secure communication protocol suite is a newly proposed approach to provide secure communications in MANETs. The approach provides completed security solution at the network layer, with building blocks selected among the Neighbor Lookup Protocol (PLP), the Secure Routing Protocol (SRP), and the Secure Link State Routing Protocol (SLSP) to secure discovery of routes, and the Secure Message Transmission (SMT) protocol, the Secure Single Path (SSP) protocol to secure the transmission of data. [22]

4 Secure Routing in MANETs

The operation of secure routing plays a very important role in MANETs security due to absence of fixed infrastructure. Traditional Internet routing protocols cannot be applied in the MANETs context in terms of not having clear line of defense [20]. Although the appropriate design could provide increased assurance of security by using CA, digital signature, hop-by-hop validation of control traffic, it will not be practical for MANETs since mobile nodes lack sufficient computation power to perform such expensive operations. [21]

Current efforts toward the design of secure routing protocols are mainly oriented to reactive (on-demand) routing protocols such as DSR [24] or AODV [5]. On-demand routing protocols have been demonstrated to perform better with significantly lower overhead than proactive protocols in many scenarios [23]. In this section we will discuss Secure On-Demand Routing Protocol – Ariadne, Secure Ad hoc On-demand Distance Vector routing protocol – SAODV, Secure Efficient Distance Vector Routing – SEAD, Securing the Destination Sequenced Distance Vector Routing Protocol – SDSDV, Secure Routing Protocol – SRP, Secure Link State Routing protocol – SLSP, On-Demand Secure Routing Protocol Resilient to Byzantine Failures, Authenticated Routing for Ad-hoc Networks – ARAN, Secure Position Aided Ad hoc Routing – SPAAR, Security Aware Routing Protocol – SAR.

Source Routing – For source routing protocols such as DSR, the main challenge is to ensure that each intermediate node cannot remove existing nodes from or ad extra nodes to the route. A secure extension of DSR is Ariadne [7].

Ariadne authenticates routing messages using one of three schemes. Shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signature. Mainly it uses a one-way Message Authentication Code (MAC) key chain TESLA [16]. Araidne assumes that the network links are bidirectional, and network may drop, corrupt, reorder or duplicate packets. Each node must be able to estimate the end-to-end estimation time to any other node in the network. It disregards physical attacks and medium access control attacks. Ariadne assumes nodes to be constrained nodes in which all nodes have loosely synchronized clocks. [7]

Assuming sender and receiver share non-TESLA secret keys for message authentication, initiator floods the network with route REQUEST, including a MAC computed with end-to-end key. The target verifies the authenticity and freshness of request using shared key and returns a route REPLY. To authenticate data Araidne uses TESLA keys where each hop authenticates new information in the request; target buffers the request until intermediate nodes release TESLA keys. One-way hash function verifies that no hop was omitted to check if attacker removed a node from the node list in a REQUEST. ROUTE REQUEST packet contains eight fields: <ROUTE REQUEST, initiator, target, id, time interval, hash chain, node list, MAC list> as shown in Figure 1. Upon receiving a ROUTE REQUEST, a node, first processes a request only if it is new, second processes the request only if its time interval is valid, and third modifies the request and rebroadcasts it (appends its address to the node list, replaces the hash chain with H [A, hash chain], appends MAC of entire REQUEST to MAC list using K_{Ai} where i is the index for the time interval specified in the REQUEST). When the target receives the ROUTE REQUEST, first it checks the validity of the request (determining that the key from the time

interval have not been disclosed yet and hash chain is correct), then returns ROUTE REPLY containing eight fields <ROUTE REPLY, target, initiator, time interval, node list, MAC list, target MAC, key list> [7].

S: $h_0 = MAC_{K_{SD}}(REQUEST, S, D, id, ti)$

$S \rightarrow *$: < REQUEST, S, D, id, ti, h_0, (), () >

A: $h_1 = H[A, h_0]$

$M_A = MAC_{K_{Ati}}(REQUEST, S, D, id, ti, h_1, (A), ())$

$A \rightarrow *$: < REQUEST, S, D, id, ti, $\underline{h_1}$, ($\underline{A}$), ($\underline{M_A}$) >

B: $h_2 = H[B, h_1]$

$M_B = MAC_{K_{Bti}}(REQUEST, S, D, id, ti, h_2, (A, B), (M_A))$

$B \rightarrow *$: < REQUEST, S, D, id, ti, $\underline{h_2}$, (A, $\underline{B}$), (M_A, $\underline{M_B}$) >

C: $h_3 = H[C, h_2]$

$M_C = MAC_{K_{Cti}}(REQUEST, S, D, id, ti, h_3, (A, B, C), M_A, M_B))$

$C \rightarrow *$: < REQUEST, S, D, id, ti, $\underline{h_3}$, (A, B, $\underline{C}$), (M_A, M_B, $\underline{M_c}$) >

D: $M_D = MAC_{K_{DS}}(REPLY, D, S, id, ti, (A, B, C), M_A, M_B, M_C))$

$D \rightarrow C$: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_c), M_D, () >

$C \rightarrow B$: <REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_c), M_D, ($\underline{K_{Cti}}$)>

$B \rightarrow A$: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_c), M_D, (K_{Cti}, K_{Bti}) >

$A \rightarrow S$: < REPLY, D, S, ti, (A, B, C), (M_A, M_B, M_c), M_D, (K_{Cti}, K_{Bti}, K_{Ati}) >

A and B are communicating nodes, K_{AB} and K_{BA} secret MAC keys shared between A and B, MAC_{KAB} (M) is computation of MAC of message M using key K_{AB}.

Figure. 1 - An example of how the Ariadne protocol works.

Node forwarding ROUTE REPLY waits until it can disclose the TESLA key from specified interval, then appends that key to the key list. When initiator receives ROUTE REPLY it verifies each key in the key list is valid, verifies that the target MAC is valid and verifies that each MAC in the MAC list is valid, using TESLA key. [7]

Distance Vector Routing – For distance vector routing protocols, like AODV and DSDV, the main challenge is that each intermediate node has to advertise the routing metric correctly. SAODV is a protocol designed to secure AODV. It uses digital signature to authenticate non-mutable fields of a route request (RREQ) and route reply (RREP) and uses one-way hash chains to authenticate the hop counts. It extends RREQ, RREQ, RREP-ACK and RERR packets with signature extensions [12]. Concerning to RREQ and RREP messages there are two alternatives: The first one in which only final destinations are allowed to reply a RREQ, and the second in which there is no such limitation. When a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating a reverse route to that host. And only if the signature is fine they store the reverse route. The final destination node signs the RREP with its private key, Intermediate and final nodes again verify the signature before creating or updating forward path, also storing the signature with the route entry [12]. In the second one, when a RREQ is sent, the sender signs the message. Intermediate nodes verify the signature before creating or updating a reverse route to that host. And, again, only if the signature is fine they store the reverse route. But the difference is that the RREQ message has also a second signature that is always stored with the reverse route. This second signature needs to be added in the gratuitous RREPs of that RREQ and in regular RREPs to future RREQs that the node might reply as an intermediate node. An intermediate node that wants to reply a RREQ needs not only the correct route, but also the signature corresponding to that route to add it in the RREP and the lifetime that came in the same message the signature. When this happens, it generates the RREP, (adding the stored signature and lifetime) signs the actual lifetime and sends it. All the nodes that receive the RREP and that update the route store the RERR also use digital signatures to sign the whole message and neighbors can verify it. Neighboring nodes should never update its destination sequence number based on RERR message. [12]

SEAD - is a proactive secure routing protocol based on DSDV-SQ-protocol. It does not rely on asymmetric encryption primitive but instead it relies on one-way hash chain for security. The algorithm expects that there is some authenticated and secure way to deliver the initial key K_N. This could be done by key delivery in advance or by using public key encryption and signatures for key delivery. The basic idea of SEAD is, to authenticate the sequence number and metric of a routing table update message using hash chains elements. In addition, the receiver also authenticates the sender ensuring that the routing information originates from the correct node. The source of each routing update message in SEAD must also be authenticated since an attacker may be able to create routing loops through the impersonation attack. There are two different approaches proposed such as broadcast authentication mechanism, TESLA and Message Authentication Codes [8], [23].

SDSDV - is a well-behaved node can successfully detect a malicious routing update with any sequence number fraud and any distance fraud, provided that no two nodes are in collusion. SDSDV requires cryptographic mechanisms for entity and message authentication [32].

Link State Routing – For Link State Routing protocols like Optimized Link State Routing Protocol (OLSR) operates as a table driven and proactive protocol, exchanging topology information with other nodes of the network regularly. The nodes, which are selected as a multipoint relay (MPR) by some neighbor nodes announce this information periodically in their control messages. Thereby, a node announces to the network, that it has reach-ability to the nodes, which have selected it as MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. The protocol uses the MPRs to facilitate efficient flooding of control messages in the network.

SLSP- is responsible securing the discovery and distribution of a link state information. The nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops. In SLSP

protocol each node is assumed to be equipped with public/private key pair and single network interface per node within the MANETs domain. Key certification is done by K nodes using threshold cryptography. Nodes are identified by the IP addresses and maybe used to derive public keys. Nodes are equipped with public key crypto system. Each node seeks to learn and update its neighborhood by neighbor lookup protocol (NLP) and periodically floods Link State Update (LSU) packets to propagate link state information [1], [9].

Other Routing Protocols – There are other secure routing protocols that do not belong to the categories described above. We will discuss them in following paragraphs.

SRP is another protocol extension that can be applied to any of the most commonly used protocols today. The basic idea of SRP is to set up a security association (SA) between the source and the destination node. The SA is usually set up by negotiating a shared key based on the other party's public key. After that the key can be used to encrypt and decrypt the messages. The routing path is always sent along with the packets, unencrypted since none of the intermediate nodes have knowledge of the shared key, it requires existing CA, a managed open environment. [28]

Byzantine Failure Resilient Protocol proposes to flood both route requests and route replies in order to defend against Byzantine failures [1], [11]. There are five steps for route discovery. Request Initiation, the source creates and sings the request. Request Propagation, the request propagate to the destination via flooding. Request Receipt/Response Initiation, the destination verifies the authenticity of the request and creates and signs a response. Response Propagation, the node computes the total weight of the path. During Response Receipt, when the source receives a response, it performs the same computation and verification as the intermediate nodes as described in the response propagation step [1], [11].

ARAN ensures that each node knows the correct next hop on a route to the destination by public key cryptography. It has five components, Certification, Authenticated Route Discovery, Authenticated Route Set up, Route Maintenance, and Key Revocation [10]. Certification requires use of trusted certificate server T. Before entering the network, each node needs to request a certificate from T. Node A receives certificate in the format shown in figure 2, step (a).

During the Authenticated Route Discovery process, a source A begins route instantiation to destination X by broadcasting a route discovery packet (RDP). Let B the neighbor that receives the RPD, which it subsequently rebroadcast a message shown in figure 2, step (b). Let C be the neighbor that receives B_S broadcast. C subsequently broadcasts a message shown in figure 2, step (c). Each node along the path repeats these steps of validating previous node's signature, removing the previous node's certificate and signature, recording the previous nodes IP address, signing the original contents of message, appending its own certificate and forward broadcasting the message [10]. During Authenticated Route Setup, after receiving RDP, the destination unicasts a reply REP packet along reverse path to source. Let D be the first node that receives the RDP sent by X, the message content is shown in figure 2, step (d). Let D's next hop to source be C, the content of the packet is shown in figure 2, step (e). The packet that B receives from is shown in figure 2, step (f). When source receives REP, it verifies destination's signature and nonce returned by the destination. During the Route Maintenance, when no traffic occurs on an existing route for sometime, that route is deactivated in routing table. Data received on an inactive route causes node to generate Error (ERR) message that travel reverse path towards the source. All ERR messages must be signed, the freshness or the ERR message is ensured by timestamp and nonce. For Key revocation, in the event that a certificate needs to be revoked, the trusted certificate server T sends a broadcast message to the ad hoc group announcing the revocation, shown in figure 2, step (g).

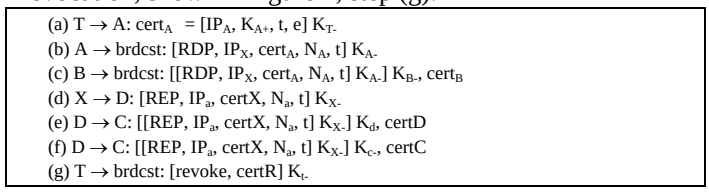

Figure.2 – The sequence of secure routing message exchange in ARAN

The **SPAAR** protocol was developed with the classical managed-hostile environment in mind, thus meant to provide a very high level of security, and sometimes at the cost of performance. Among other things, SPAAR also requires that each device to use a GPS locator to determine its position, although some leeway is given to nodes using a so-called "locator-proxy" if absolute security is not required. In SPAAR packets are only accepted between neighboring nodes one hop away from each other, this is to avoid the "invisible node-attack". The basic transmission procedure is quite similar to ARAN, although the group neighborhood key is used for encryption in order to ensure one-hop communication only. Since all nodes also have information on their location they only forward RREQs if their position is closer to the destination position [29].

SAR takes an approach to routing that incorporates security level of nodes into traditional routing metrics. In most protocols the length of the route is the only metric used. It does not target any protocol, but it rather provides security at a more generalized level of security. The goal is exposing security to the application and to the routing protocol. SAR uses AODV or DSR as a base protocol; it embeds the security metric into RREQ packet itself and changes the forwarding behavior of the protocol. When intermediate nodes receive an RREQ packet with a particular security metric or trust level, the node can only process the packet or forward it if it can provide the required security or trust level [25].

5 Security Analysis of Secure Routing Protocols in MANETs

The Advantage of using Ariadne is that any alternation of the node list can be detected. The disadvantages of Ariadne are that, first, there are certain attacks such as wormhole attack, and cache poisoning attack cannot be prevented. Second, the key exchange is very complicated [7].

The Advantages of using SAODV are that following attacks can be prevented. Impersonating source and destination nodes, forging RERR message to claim it is the source and sending it to the destination (this can be prevented by using digital signatures in SAODV). Reducing the hop count to increase the chance of being in the route path between source and destination (this can be prevented by using one-way hash chain for hop authentication). Replay, delay attacks can be prevented by sequence number system. Disadvantage of using SAODV are that malicious code node can pass the received authenticator and hop count without changing them. Two malicious nodes can claim they have link between them, and they can achieve having certain traffic through them. Use of public key cryptography imposes a high processing overhead. It is possible that intermediate node can corrupt the route discovery. There is also trivial exposure to be compromised on the IP portion of the SAODV traffic.

The advantage of SAR is that it enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. Disadvantages of SAR include, it does not state anything about how to use or implement the security level as a metric. Route discovery process may fail due to not having proper security clearance even though there exists a connectivity path to the desired destination.

The advantage of using SEAD is that it is robust against multiple uncoordinated attackers, active attackers or compromised nodes. It uses efficient, inexpensive cryptographic primitives and this plays an important role in computation and bandwidth-constrained nodes. The disadvantages are taht it doesn't provide a way to prevent an attacker from tampering with "next hop" or "destination" columns. Instead, it relies on doing neighbor authentication, which is bad. Hash chains are consumed very fast, either new h_n needs to be released very often or the hash chain has to be rather long.

The Advantages of using SDSDV are that data integrity is protected, data origin is authenticated, a route with a falsified destination can be detected, an advertised route with a falsified sequence number can be detected, an advertised route with a falsified distance can be detected, an advertise route with a falsified next hop can be detected and a route update with misinformation can be detected. The disadvantage is that it produces higher network overhead. However SDSDV compare to SEAD, it has several advantages. SDSDV can authenticate smaller sequence numbers, SEAD cannot. SDSDV can authenticate longer, same shorter cost metric, SEAD cannot. SDSDV can resist to 2-node collusion, SEAD cannot.

The Advantage of SLSP is that it is less vulnerable to DoS attacks. Nodes can decide if they want to authenticate the public key or not. The disadvantage of SLSP is that it remains vulnerable to colluding attackers.

The Advantages of SRP are that it guarantees the discovery of correct connectivity information over an unknown network in the presence of malicious node, confidentiality is protected, it has less processing overheads, route signaling cannot be spoofed, fabricated routing messages cannot be injected into network, routing messages in transit cannot be altered, routing loops cannot be formed through malicious actions, and routes cannot be redirected from shortest path thru malicious nodes. The disadvantage of the protocol is that it exposes network structure with unencrypted routing path; Susceptible to "invisible node attack". [28]

The Advantage of Byzantine failure resilient protocol is that, as long as there is fault free path, even in a highly adversarial controlled network, it will be discovered after bounded numbers of faults have been occurred. The disadvantage of the protocol is that it is difficult to design a scheme that is resilient to large number of adversaries. [11]

The advantages of ARAN are that it is secure as long as CA is not compromised, confidentiality is guaranteed because of public key encryption, network structure is not exposed, and it is resistant to most of the attacks. The disadvantages are that it requires extra memory, it has high processing overhead for encryption, and does not use hop count, so the discovered path may not be optimal. [10]

The only real security disadvantage currently discovered in SPAAR is that the usage of the certificate server and the extreme need to keep this server uncompromised. Also, issues still exist with compromised nodes already having valid certificates. [29]

6 Comparison of Secure Routing Protocols

Table 1 takes different security parameters and shows how the secure routing protocols in MANETs differ from each other.

7 Conclusions

These secure routing protocols provide many approaches to secure the MANETs, however there are still many open challenges remain unsolved. First, most of the secure routing protocols are designed with certain known attacks in mind. When an unknown attack is encountered, these protocols may collapse. Second, achieving higher security always requires more computation on each mobile node. In MANETs environment, resources are very limited, thus there will always be a trade between more security and more performance. Third, one security solution is being chosen based on which security aspects are most important in that

environment. However, in many ways these security schemes are not exclusive to one another. Forth, until now, many secure routing, data packet forwarding and link layer security solutions are proposed. However not all these security solutions provide complete security for MANETs.

Protocols	Secret Keys	MAC	Digital Signature	Hash Chain	Cryptographic mechanism	Assumptions	Verification mechanism
Ariadne	Secret MAC keys K_{SD} between sender and receiver	MAC $_{Ksd}$	—	TESLA keys authenticate messages. It uses hash-chain to generate these keys	—	Nodes have loosely synchronized clocks	MAC verification mechanism
SAODV	Public and private key pair for each node	—	Sender uses digital signature to sign the messages	One way hash chain to authenticate hop counts	—	Network should he Key Distribution System	Digital signature verification mechanism
SEAD	Initial secret key K_N for hash function	—	—	Authenticates the sequence number and routing table metric by one way has chain	—	Secure way of delivering initial secret key K_N	Hash chain verification
SDSDV	Different Pair-wise K_{ij} shared secret key between all the nodes	Node i sends MAC_{Kij} to node j	—	—		Public Key Infrastructure	MAC verification mechanism
SLSP	Public and private key pair for each node	MAC	—	—	Threshold cryptography	Single network interface per node	Threshold cryptography for key certification; MAC verification mechanism;
SRP	SA between source and destination	MAC calculation with K_{ST}	—	—	—	Secure way of delivering the SA	MAC verification mechanism
Secure protocol resilient to Byzantaine failures	Pair-wise secret key established on demand	—	Digital signature is used to authenticate the source	—		Public key infrastructure or CA	Digital signature verification mechanism
ARAN	Public and private key pair for each node	—	—	—	Public key cryptography	Trusted certificate server	Public key cryptography verification mechanism
SPAAR	Public and private key pair for each node; Group neighborhood key	—	—	—	Public key cryptography	Trusted certificate server	Public key cryptography verification mechanism

Table 1 Comparison of Secure Routing Protocols in MANETs

8 References

[1] Y. Hao et al., "Security In Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 2004.

[2] A. Mishra, and K. Nadkarni, "Security in MANETs", The handbook of wireless ad hoc networks, 2002

[3] C-K. Toh, "MANETs: protocols and systems", Prentice Hall, 2002

[4] C. Perkins, and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", ACM SGCOMM, 1994.

[5] C. Perkins and E. Royer, "Ad hoc On-Demand Distance Vector Routing", 2nd IEEE Wksp. Mobile Comp. Sys. And Apps., 1999.

[6] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad hoc Wireless Networks", Mobile Computing, T Imielinski and H. Korth, Ed., Kluwer, 1996.

[7] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure On-demand Routing Protocol for Ad hoc Networks", ACM MOBICOM, 2002.

[8] Y. Hu, D. Johnson and A. Perring, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," IEEE WMCSA, 2002.

[9] P. Papadimitratos, and Z. Haas, "Secure link State Routing for Mobile Ad hoc Networks", IEEE Wksp. Security and Assurance in Ad hoc Networks, 2003.

[10] B. Hahill et l., "A Secure Protocol for Ad Hoc Networks", OEEE CNP, 2002.

[11] B. Awerbuch et al., "Ad hoc On-Demand Distance Vector Routing Protocol Resilient to Byzantine Failures", ACM Wise, 2002.

[12] Z. Manle Guerrero, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing", August 2001.http://www.cs.ucsb.edu/~ebelding/txt/saodv.txt

[13] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM MOBICOM, 2000.

[14] H. Yang, X. Meng, and S. Lu, "Self-Organized Network Layer Security in Mobile d Hoc Networks", ACM Wise, 2002.

[15] H. Chun, and P. Adrain, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, June 2004

[16] A. Perrig et al., "The TESLA Broadcast Authentication Protocol", RSA CryptoBytes, vol. 5, no. 2, 2002, --.2-13.

[17] M. Zapata, and N. Asokan, "Securing Routing Protocols", ACM Wise, 2002

[18] Z. Haas and M. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", in IETF MANETS Draft, June 1999.

[19] Vesa Karpijoki, "Security in Ad Hoc Networks", Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

[20] P. Papadimitratos and Z.J. Haas, "Securing the Internet Routing Infrastructure", IEEEE communications Magazine, 40(10), Oct, 2002.

[21] "Securing MANETs", The handbook of wireless ad hoc networks, 2002

[22] Panagiotis Papadimitratos, Zygmunt J. Haas, "Secure Communication Protocol Suite", http://people.cornell.edu/pages/pp59/Pages/srp_boom.html

[23] Pietro Michiardi, Refik Molva, "Ad Hoc Network Security", Mobile Ad Hoc Networking, 2004 Institute of Electrical and Electronics Engineers, Inc.

[24] D. B. Johnson and D. A. Maltaz, "Dynamic Source Routing", in Ad Hoc Wireless Networks, Mobile Computing, T. Imielinski and H Korth (Eds.), Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996

[25] Seung Yi, Prasad Naldurg and Robin Kravets, "Security-Aware Ad hoc Routing for Wireless Networks", UIUCDCS-R-2001-2241August 2001.

[26] E. Royer and C. Toh, "A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks", Apr, 1999

[27] Kai Inkinen, "New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes", Helsinki University of Technology, Laboratory of Multimedia

[28] Panagiotis Papadimitratos, and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proceedings of SCS Communications Networks and Distributes Systems Modeling and Simulation Conference, CNDS 2002.

[29] Alec Yasinsac and Stephen Carter, "Secure Position Aided Ad hoc Routing", Florida State University, 2002. http://www.cs.fsu.edu/~yasinsac/Papers/CY02.pdf

[30] Elizabeth M, Belding-Royer, "Routing Approaches in Mobile Ad hoc Networks", Mobile Ad Hoc Networking, 2004 Institute of Electrical and Electronics Engineers,

[31] P. Papadimitratos and Z.J. Haas. "Secure Message Transmission in Mobile Ad Hoc Networks." Elsevier Ad Hoc Networks Journal, vol. 1, no. 1, July 2003.

[32] Tao Wan, Evangelos Kranakis, P.C. van Oorschot, "Securing the Destination Sequenced Distance Vector Routing Protocol (S-DSDV)", http://www.scs.carleton.ca/~canccom/Publications/tao-sdsdv.pdf