Secure Routing Protocols for Mobile Ad Hoc Networks

Houda Moudni[1], Mohamed Er-rouidi[1]
[1] *Faculty of Sciences and Technology*
Sultan Moulay Slimane University
Beni Mellal, Morocco
{h.moudni, m.errouidi}@usms.ma

Hicham Mouncif[2], Benachir El Hadadi[2]
[2] *Faculty Polydisciplinary*
Sultan Moulay Slimane University
Beni Mellal, Morocco
{hmouncif, benachirelhadadi}@yahoo.fr

***Abstract*— Mobile Ad hoc NETwork (MANET) is a collection of self-organizing mobile nodes without any help of centralized administration or established infrastructure. Due to this characteristic, MANETs are particularly vulnerable to various security threats. In addition, the design of most MANET routing protocols assumes that there is no malicious node in the network. Hence, several efforts and researches have been made toward the design of a secure and robust routing protocol for ad hoc networks. In this paper, we discuss the major attacks that can target the operation of ad hoc routing protocol. A detailed survey of the well-known secured ad hoc routing protocols for mobile ad hoc networks is presented. In order to analyze the existent solutions for securing ad hoc routing protocols in a structured manner, we have classified them into three categories: solutions based on cryptography, solutions based on one-way hash chain and hybrid solutions. This paper also gives a brief summary and comparison of various protocols available for secured routing in MANET.**

Keywords—Mobile Ad hoc network; routing protocols; routing attacks; security; secure ad hoc routing protocols.

I. INTRODUCTION

A Mobile Ad Hoc network consists of nodes that are able to communicate with each other through wireless mediums. These nodes operate not only as an end system, but also as a router to forward packets to others, without the aid of any existing infrastructure or centralized administration. Therefore, these networks have a dynamic topology since all the nodes can easily join or leave the network at any time. These features make MANET useful and practical, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network to replace another which falls down after a disaster like an earthquake.

In order to provide connectivity in a mobile ad hoc network all nodes have to perform routing of network traffic. Although numerous ad hoc routing protocols have been proposed such as Destination-Sequenced Distance-Vector (DSDV) [1], Optimized Link State Routing Protocol (OLSR) [2], Dynamic Source Routing (DSR) [3] and Ad hoc On Demand Distance Vector (AODV) [4], which assumed an environment where all the nodes are perfectly cooperative and trustworthy and no security mechanism has been considered. Unfortunately, MANETs may not be such a friendly environment due to multi-hop communication and the lack of centralized administration. Besides, malicious nodes can freely join the network and cause various performance degradation, as interfering the routing information or listen to the network communication.

To secure an ad hoc network, we consider the following attributes: availability, data confidentiality, data integrity, authentication and non-repudiation. These countermeasures considered to reduce or eliminate the security vulnerabilities and attacks in the network. In the literature, several secure ad hoc routing protocols have been proposed. In this paper, we present a detailed survey of the well-known routing protocols in terms of security and identify their limitations.

The rest of this paper is organized as follows: in Section 2, we present the possible attacks that malicious nodes can use for disrupting the operation of a routing protocol in a mobile ad hoc network. Section 3 analyzes the already proposed secure ad hoc routing protocols that exist in the literature and present their operational principles. Section 4 briefly gives a summary and comparison of the various secure routing protocols. Then, we conclude our discussion in Section 5.

II. ROUTING ATTACKS IN MANETS

Due to characteristics of mobile ad-hoc networks, MANETs are more vulnerable to be attacked than wired networks. We can distinguish two principal categories of attacks: passive and active attacks. A passive attack does not disrupt the operation of the protocol, but attempts to listen to valuable information in the traffic. Instead, an active attack disrupts the operation of the protocol in order to degrade the network performance, gain unauthorized access, and restrict availability. A brief overview of several well-known routing attacks [5, 6, 7, 8] is presented below.

a) Passive Eavesdropping Attack: The purpose of eavesdropping attack is to listen the secret or confidential routing information that should be kept secret during the communication. From the information it captures, it is able to discover potentially sensitive topology information about the network. In general, the eavesdropping is easier in mobile ad-hoc network, due to the open nature of the communication medium.

978-1-4673-7689-1/16/$31.00 ©2016 IEEE

b) Routing Data Manipulation Attack: A manipulation attack occurs when a malicious node alters the information it receives before forwarding it to the next node. Without any integrity measures the next receiving node will be unable to see any evidence of tampering, and hence, will process the incorrect information.

c) Replay Attack: A replay attack is a form of active attack in which a malicious node stores routing information and then later retransmits the stored information. This attack targets the freshness of routes, also used to undermine poorly designed security solutions.

d) Black Hole Attack: In a black hole attack, a malicious node uses the routing protocol to advertise a shortest path to a node, thus intercepting the communicating packets passing through the malicious node. As a result, instead of normally forwarding the packets that it receives, the malicious drops all packets.

e) Flooding Attack: In this attack, a malicious node aims to flood the network with a large number of RREQs in a short period to non-existent destinations in the network, and then causes severe degradation of network performance.

f) Rushing Attack: This kind of attack can be carried out against on-demand routing protocols that use duplicate suppression in their operations. Rushing node exploits this mechanism by quickly forwarding route discovery packets in order to be included in the discovered routes.

g) Tunnelling/Wormhole Attack: The Wormhole attack occurs when an attacker receives packets at one point in the network, then "tunnels" them to another point in the network; the colluding can communicate directly over long distances.

h) Sybil attack: In Sybil attack, a single node appears in the network with multiple identities. These false identities can be used to play different type of attack in the network. This attack also poses a significant threat to geographic routing protocol.

i) Denial of Service: This attack targets the availability of the node. An adversary floods an amount of data in order to consume network bandwidth or to consume the resources of a particular node. Specific instances of denial of service attacks include the overflow of the routing table and the sleep deprivation torture.

III. SECURED ROUTING PROTOCOL IN MANET

There exist several proposals that attempt to counter the security threats mentioned in the previous section, and provide protection against malicious attacks and selfish behaviors. These proposed solutions are either an integration of security mechanisms into existing protocols (e.g. AODV and OLSR), or a new stand-alone protocols. Among the security mechanisms for ad-hoc networks used nowadays, there are two techniques:

- Prevention technique: This mechanism involves protocols that prohibit the attacking node to initiate any action. These approaches usually require encryption techniques to provide authentication, integrity, etc.
- Detection and Reaction: These solutions attempt to identify any malicious activities in the network and take proper action against such nodes. (e.g. Byzantine Algorithm [9], Core [10], Confidant [11], Watchdog and Pathrater [12]).

In this paper, we will focus on the prevention techniques. Therefore, to analyze the existing solutions in structured way we have classified them into three categories; solutions based on cryptography, solutions based on one-way hash chain and hybrid solutions. For the solutions based on cryptography, there are two sub-categories; solutions based on symmetric cryptography and solutions based on asymmetric cryptography.

A. Symmetric cryptography solutions

1) Secure Routing Protocol (SRP)

The Secure Routing Protocol (SRP) developed by Papadimitratos and Haas [13], is a protocol designed to secure the on-demand routing protocols that utilize broadcasting as its route querying method. The authors mentioned that can be applied as an extension of a multitude of existing reactive routing protocols, in particular the DSR [3]. A security association (SA) is required between a source node and a destination node. It is assumed that the SA can be established by using a shared key between the two communicating nodes.

A SRP Header as shown in Fig. 1 is added to the packet of the basis routing protocol. The source node initiates the route discovery, by sending a route request packet that identified by a query sequence number (QSEQ), a random query identifier (QID), and the output of a key hashed function. The key hash function takes IP header, the header of the basic routing protocol, and the shared key.

The intermediate nodes broadcast the packet to the neighboring nodes and update their routing table. However, if they have the same QID in their routing table, the query is dropped. When the query has reached to the destination node, it verifies that the query is not outdated or replayed through the QSEQ and it checks for the security metrics by calculating of the keyed hash. After verifying, the destination node generates a number of replies with different routes, so that it provides the source with an as diverse topology picture as possible. These replies packets include the path information from source to destination, the QSEQ and QID numbers. The security metrics of the reply are ensured through the same method as the route request, by calculating the Message Authentication Code (MAC). After receiving the reply packet, source node checks the QSEQ and QID numbers, then calculates the MAC and compares the output with the MAC field of the SRP header.

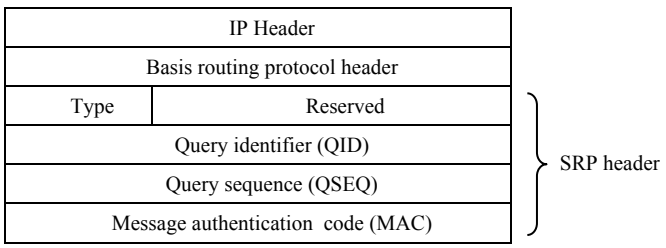

Fig. 1. SRP Packet header

According to a successful verification, source node is assured that the request is reached to the destination and that the reply was not corrupted on its way from the source to the destination.

The route error message packet is generated by an intermediate node that discovers broken links. This packet is source-routed to the source node along the prefix of the route being reported as broken. When the node receives a route error packet, it compares the route taken by the packet with the prefix of the corresponding route. However, malicious nodes can also send a route error messages. Therefore SRP provides minimal protection for route maintenance errors.

SRP can ensure proper connectivity information if a set of malicious nodes mount attacks against the protocol concurrently, but it remains weak against the wormhole attack.

2) Security aware Ad hoc Routing protocol (SAR)

The Security-aware Ad hoc Routing (SAR) protocol [14] is an approach to ad hoc routing that incorporates security attributes as parameters into route discovery. However, traditional non-secure routing protocols find out the shortest path between two nodes, while SAR can discover a path with desired security attributes. For instance, the criterion for a valid route can be when each node in the route must have a particular shared key.

SAR can be extended to any on-demand ad hoc routing protocols (such as AODV or DSR) in order to integrate the security metric into the route request messages. An implementation of SAR based on AODV is presented by the authors. The route request packet has an additional field (RQ_SEC_REQUIREMENT) that indicates the required security level of the route that she wishes to discover. This field is only set once by the sender and does not change during the route discovery. An intermediate node that receives the packet checks if it can satisfy the security requirement. If the node can provide the required security, thus it can participate in the routing and the route request packet is forwarded to its own neighbors, updating a new field called RQ_SEC_GURANTEE to indicate the maximum level of security it can provide. And if the intermediate node can't satisfy the security requirement, it simply drops the route request packet. When the destination node receives the route request packet, it can be sure of the existence of a route from the source to the destination and this route satisfies the security requirements defined by the sender. The destination node sends a route reply packet with an additional field (RP_SEC_GUARANTEE) that indicates the maximum security available over the path. Then the value of the RQ_SEC_GURANTEE field is copied to RP_SEC_GUARANTEE. The reply packet goes back along the reverse path and the intermediate nodes that are allowed to participate in the routing, update its routing table according to the AODV specification and also record the new RP_SEC_GUARANTEE value. This value indicates the maximum security available on the cached forward path.

A major disadvantage in SAR is that it involves significant overhead to the routing process, since each intermediate node has to perform encryption/decryption operation.

B. Asymmetric cryptography solutions

1) Authenticated Routing for Ad hoc Networks (ARAN)

The Authenticated Routing for Ad hoc Networks (ARAN), described in [15], is a secure routing protocol based on the on-demand protocols. ARAN utilizes a cryptographic mechanism in order to achieve security goals of authentication, message integrity and non-repudiation.

It consists of two distinct operational stages; the first stage is the preliminary certification process that requires the existence of a trusted certificate authority (CA). All nodes that want to connect to the network must contact the certification authority and request a certificate for its address and public key. This certification authority distributes its public key to all the nodes in the network. The second operational stage of the protocol is the route discovery process that provided end-to-end authentication. This ensures that the intended destination was indeed reached. The initiator node starts the communication by broadcasting a route discovery packet (RDP) to its neighbors. The RDP includes a packet type identifier ("RDP"), the certificate of the initiating node, a nonce, a timestamp, and the address of the destination node, all signed with the initiating node's private key. Every intermediate node validates the signature and verifies that the source's certificate has not expired, updates its routing table with the neighbor from which it received the RDP, signs the contents of the message, appends its own certificate, and forwards the message to its neighbors after removing the certificate and the signature of the previous node. The signature prevents spoofing attacks that may alter routes or form loops. After receiving the RDP, the destination node replies with a reply packet (REP). The REP contains a packet type identifier ("REP"), the address of the source node, the destination's certificate, a nonce, and the associated timestamp. Furthermore, the destination node signs the REP. Similar to the route discovery, each node removes the certificate and signature of the previous hop and replaces them with its own before forwarding it to the next hop, except that the REP is unicasted along the reverse path. When the source receives the REP, it verifies the destination's signature and the nonce returned by the destination. Fig. 2 illustrates the process of route discovery in ARAN.

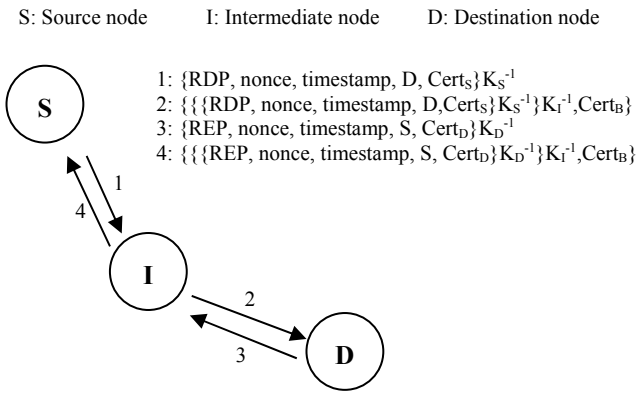

Fig. 2. Route discovery in the ARAN protocol

Route maintenance is realized in ARAN by ERR messages that are signed by the nodes that generate them in order to report broken links. Then, it forwarded along the reverse path toward the source without modification. Replay attacks are ensured by a nonce and a timestamp including in the ERR message. While the ERR messages are signed, malicious nodes cannot generate false broken link reports. Consequently, non-repudiation is provided. As shown in Fig. 3.

A certificate needs to be revoked when limited-time certificates is achieved. The trusted certification server broadcasts a revocation message to the network. All receiving nodes re-broadcasts this message it to its neighbors. The authors mentioned that this method is not failsafe, since a revocation message might not be propagated by the malicious node creating a partition in the network.

The ARAN protocol provides both node-to-node and end-to-end authentication, that guarantee a protection from modification, impersonation, and fabrication attacks. However, due to heavy asymmetric cryptographic operations and large routing packets, ARAN suffers from a higher overall routing load and higher latency in route discovery.

C. *Prevention using One-Way Hash Chains*

1) Secure Efficient Ad hoc Distance vector (SEAD)

The Secure Efficient Ad hoc Distance vector (SEAD) [16] is a secure ad hoc network routing protocol based on the design of the DSDV [1] routing protocol, in particular, on the DSDV-SQ version of this protocol. SEAD uses a hash chain to authenticate hop counts and sequence numbers and does not involve any asymmetric cryptographic operations.

In SEAD, each node creates its hash chain by applying a one-way hash function to a random value. Furthermore, particular elements from the hash chain are used to secure the updates of the routing protocol. However, the protocol is based on the assumption of the existence of a certain mechanism in order to authenticate one element of a hash chain between two nodes. Hence, when a node sends or transmits a routing update, it includes one value from the hash chain for each entry in that update. In a way that a node includes the address of the destination node, the metric and the sequence number of the destination from its routing table, and the hash value to the hash of the hash value received in the routing update entry from which it learned that route to that destination. If the update concerns itself, the node includes its own address, it sets the metric to 0 and the sequence number to the next sequence number, and the hash value to the first element in its own hash chain corresponding to that sequence number. Nodes receiving a routing update check the authentication of each entry of the message, by hashing the hash value received of each entry the correct number of times and it is compared to the prior authentic hash value. According to this comparison the routing update is either accepted as authenticated or discarded. Using this technique, other nodes can only increase the metric in a routing update, but not to decrease it.

SEAD is robust against multiple uncoordinated attackers trying to create an incorrect routing state in any other node, even in spite of compromised nodes or active attackers.

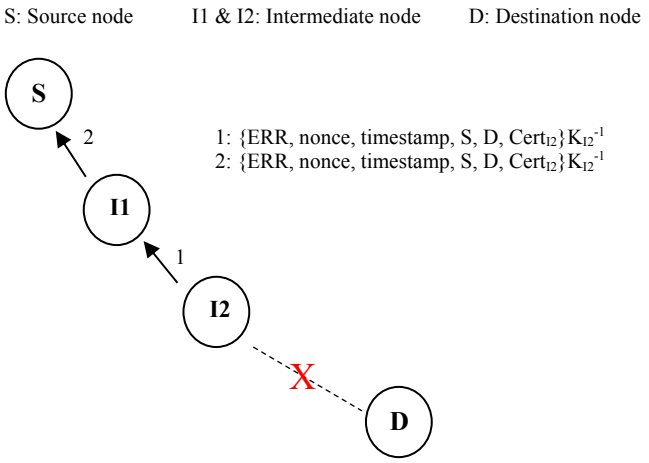

Fig. 3. Route maintenance in the ARAN protocol

Additionally, SEAD proposes two different methods to authenticate the source of each routing update message in order to avoid the creation of routing loops. The first one requires clock synchronization between the nodes that participate in the ad hoc network, and employs broadcast authentication mechanisms such as TESLA [17], HORS [18] or TIK [19]. The second method assumes a shared secret key among each pair of nodes in order to use a message authentication code (MAC) between the nodes for the authentication of a routing update message.

The routing protocol SEAD provides strong protection against attackers trying to create incorrect routing state, but fails against the wormhole attack.

2) Ariadne

Ariadne [20] is a secure reactive ad hoc routing protocol based on the DSR [3]; this protocol is developed by the same authors in the SEAD protocol described above. Instead of employing the hop by hop security mechanisms as in the protocol SEAD, the proposal Ariadne follows an end-to-end approach.

The design of Ariadne can be viewed as having three stages: Authentication of ROUTE REQUEST by target, techniques for authenticating data in ROUTE REQUEST and ROUTE REPLY, and Per-hop hashing technique.

- Authentication of ROUTE REQUESTs by target: this stage consists to verify the authenticity of the ROUTE REQUEST, that it is filled when the initiator node includes a MAC computed with a shared key over unique data, for example a timestamp, in the ROUTE REQUEST.
- Techniques for authenticating data in ROUTE REQUEST and ROUTE REPLY: this stage allows the initiator node to authenticate each individual node in the node list of the ROUTE REPLY. Also the target node can authenticate each node in the node list of the ROUTE REQUEST, in order to ROUTE REPLY will return only along the paths that contain legitimate nodes. According to the authors, authentication can be performed by using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes

combined with the TESLA [17] broadcast authentication protocol which requires loose time synchronization, or a digital signature.

- Per-hop hashing technique: A one-way hash function is used to verify that no node was removed from the node list in the ROUTE REQUEST. To change or remove a previous hop, an attacker must be able to invert the one-way hash function, which has been proved computationally impracticable.

Ariadne provides a good defense against attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, it also prevents many types of Denial-of-Service attacks. Additionally, Ariadne relies only on highly efficient symmetric cryptography.

Ariadne is a robust protocol based on DSR, it provides end-to-end security mechanisms for ad hoc routing protocol. The most important requirement of Ariadne with TESLA is the existence of clock synchronization in the ad hoc network. However, the basic Ariadne protocol can be affected by a wormhole and rushing attacks.

D. Hybrid solutions

1) Secure Ad hoc On-demand Distance Vector protocol (SAODV)

The Secure Ad hoc On-demand Distance Vector protocol (SAODV) is an extension to AODV routing protocol [21]. The proposed extensions utilize cryptographic signatures for authenticating the non-mutable fields of the messages, and one way hash chain for secure the hop-count field within the RREQ and RREP messages, which is the only mutable field of an AODV message. The protocol requires the existence of a key management mechanism that allows for every node to obtain public keys from the other nodes that participate in the ad hoc network.

The information relative to the signatures and the hash chains is transmitted with the AODV message as an extension message that the authors refer to as Signature Extension. These SAODV extensions consist of the following fields. The *hash function* field indicates which hash function has to be used. The field *max hop count* specifies the maximum number of nodes a packet is allowed to go through. The field *hash* is a randomly generated number called as seed. Finally, the *top hash* field is calculated by hashing the value in the Hash field Max Hop Count times. The format of the SAODV signature extensions is shown in Fig. 4.

Type	Length	Hash function	Max Hop Count
Top Hash			
Signature			
Hash			

Fig. 4. SAODV protocol header

Every time a node originates a route request or a route reply AODV packet generates a random number (seed) and sets the hash field to the seed value, sets the max hop count field to the time to live (TTL) field from the IP header, specifies the hash function field by the identifier of the hash function that it is going to use, and applies the hash function to the seed max hop count times, the calculated result sets to the top hash field. Furthermore, the node digitally signs all fields of the message, except the hop count field from the AODV header and the hash field from the SAODV extension header. After receiving a route request or a route reply, the intermediate node verifies the hop count AODV field by comparing the result of the hashing max hop count minus hop count times to the hash field with the value of the top hash field. If the check fails, the packet will be dropped by the node. The intermediate node hashes one time the old value of the Hash field in the Signature Extension, before rebroadcasting a RREQ message to its neighbors or forwarding a RREP.

The authors mentioned that the main problem in applying digital signatures is that AODV allows intermediate nodes to reply RREQ messages if they have a fresh route to the destination. For solving this problem, the authors suggest two solutions. The first one is to forward the RREQ message since intermediate nodes cannot sign its RREP message. The second solution consists of using the double signature extension described in [21] to reply to a route request.

For the broken links an error message (RERR) is generated by the nodes. Every node that generates or forwards a route error message use digital signatures to sign the whole message, except the destination sequence numbers. And any neighbor that receives it verifies the signature.

The security features provided by SAODV include integrity, authentication and non-repudiation. Nevertheless, due to the use of asymmetric cryptography, SAODV suffers from degradation of the performance. In addition, SAODV is affected by the Wormhole attack. And a hop count authentication by using hash chains is not perfect while a malicious node might forward a message without increase the hop count.

2) Secure Link State Routing Protocol (SLSP)

The Secure Link State Routing Protocol (SLSP) [22] is a proposed scheme for securing proactive routing for mobile ad hoc networks and the distribution of link state information for locals and network-wide scoped topologies. SLSP can be used as either as a stand-alone solution for proactive link-state routing, or as a part of the hybrid routing framework when combined with a reactive ad hoc routing protocol. However, The SLSP requires the existence of an asymmetric key pair for every network interface of a node.

There are three major steps in SLSP: public key distribution, neighbor discovery, and link state updates.

- Public key distribution: To function efficiently without central key management, each node broadcasts its public key to nodes within its zone using signed public key distribution (PKD) packets. Then

receiving nodes validate their subsequent link state updates from the source node.

- Neighbor discovery: Link state information of the node is also broadcast periodically using the Neighbor Lookup Protocol (NLP), an internal part of SLSP. Every node sends its MAC address and IP address of the current network interface, to its neighbors by broadcasting signed NLP hello messages. A node's NLP generates a notification to inform SLSP when suspicious discrepancies are observed, such as two neighbors used the same IP address, or a node uses the same MAC address as the detecting node, etc. While receiving the notification, the routing protocol discards immediately the suspicious packets.
- Link state updates: Link state update (LSU) packets are identified by the IP address of the initiating node and include a 32-bit sequence number, which provides an ample space of updates. Each update includes a hop count representing the number of hops traveled by the SLSP updates. A hash chain is used to authenticate the hop count, and the hash chain values are performed through the hash chain's anchor, which is included in the digitally signed part of an LSU message. Upon the reception of the LSU, the nodes check the attached signature using a public key of the originating node. The hops_traversed field of the LSU is set to hashed hops_traversed, the TTL is decremented, and the packet is rebroadcast.

SLSP is robust against denial of service attacks, while every node maintains a priority ranking of their neighboring nodes according to the rate of control traffic they have observed. Neighbor nodes that generate update packets with the highest rate are given lowest priorities and vice versa.

The routing protocol SLSP provides secure proactive topology discovery for mobile ad hoc networks. The protocol guarantees a protection from individual malicious nodes. However, it remains vulnerable to colluding attackers that fabricate non-existing links between themselves and flood this information to their neighbors.

IV. Summary and comparison of various secure Ad Hoc routing protocols

In this section, a comparative summary of the previously presented secure ad hoc routing protocols is given below in Table 1. We concluded that there is no single routing protocol that provides protection against all forms of routing attacks. In addition, the achievable security level is highly dependent on both the assumptions and operational requirements.

V. Conclusion and future work

In this paper, we have presented the most known protocols for securing the routing function in mobile ad hoc networks. The analysis of the various proposed routing protocols has demonstrated that the inherent characteristics of ad hoc networks, such as rapidly changing topologies and lack of infrastructure, introduce further difficulties to the already complicated problem of secure routing. Our study shows that, none of the proposals of secure routing protocols are able to accomplish all security goals. In addition, security overhead comes mainly from the computational complexity of the cryptographic algorithms used in constantly repeated routing procedures. In future work, we will propose improvements in AODV routing protocol for secure network layer communication in MANETs.

References

[1] Perkins, C. E., & Bhagwat, P. (1994, October). *Highly dynamic destination-sequenced distance-vector routing (DSDV)* for mobile computers. In ACM SIGCOMM computer communication review (Vol. 24, No. 4, pp. 234-244). ACM.

[2] Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)*(No. RFC 3626).

[3] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile computing* (pp. 153-181). Springer US.

[4] Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561).

[5] Kapur, R. K., & Khatri, S. K. (2015, March). Analysis of attacks on routing protocols in MANETs. In *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in* (pp. 791-798). IEEE.

TABLE I. Comparison Table of Secure Routing Protocols

Secured Routing Protocol		SRP	SAR	ARAN	SEAD	ARIADNE	SAODV	SLSP
Secure From:	**Modification**	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Fabrication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Impersonation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Worm hole attack	No	No	No	No	Yes	No	No
	Selfish nodes	No	No	No	No	No	No	No

[6] Rajakumar, P., Prasanna, V. T., & Pitchaikkannu, A. (2014, February). Security attacks and detection schemes in MANET. In *Electronics and Communication Systems (ICECS), 2014 International Conference on* (pp. 1-6). IEEE.

[7] Khan, M. S., Jadoon, Q. K., & Khan, M. I. (2015). A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks. In *Mobile and Wireless Technology 2015* (pp. 137-145). Springer Berlin Heidelberg.

[8] Saeed, A., Raza, A., & Abbas, H. (2014, June). A Survey on Network Layer Attacks and AODV Defense in Mobile Ad Hoc Networks. In *Software Security and Reliability-Companion (SERE-C), 2014 IEEE Eighth International Conference on* (pp. 185-191). IEEE.

[9] Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002, September). An on-demand secure routing protocol resilient to byzantine failures. In*Proceedings of the 1st ACM workshop on Wireless security* (pp. 21-30). ACM.

[10] Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Advanced Communications and Multimedia Security* (pp. 107-121). Springer US.

[11] Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* (pp. 226-236). ACM.

[12] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.

[13] Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In *the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002* (pp. 193-204).

[14] Yi, S., Naldurg, P., & Kravets, R. (2001, October). Security-aware ad hoc routing for wireless networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing* (pp. 299-302). ACM.

[15] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Royer, E. M. B. (2002, November). A secure routing protocol for ad hoc networks. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on* (pp. 78-87). IEEE.

[16] Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad hoc networks*,*1*(1), 175-192.

[17] Perrig, A., Canetti, R., Song, D., & Tygar, J. D. (2001, February). Efficient and secure source authentication for multicast. In *Network and Distributed System Security Symposium, NDSS* (Vol. 1, pp. 35-46).

[18] Reyzin, L., & Reyzin, N. (2002, July). Better than BiBa: Short one-time signatures with fast signing and verifying. In *Information Security and Privacy*(pp. 144-153). Springer Berlin Heidelberg.

[19] Perrig, A., Hu, Y. C., & Johnson, D. B. (2001, December). Wormhole protection in wireless ad hoc networks. In *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking*.

[20] Hu, Y. C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless networks*, *11*(1-2), 21-38.

[21] Zapata, M. G., & Asokan, N. (2002, September). Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on Wireless security* (pp. 1-10). ACM.

[22] Papadimitratos, P., & Haas, Z. J. (2003, January). Secure link state routing for mobile ad hoc networks. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on* (pp. 379-383). IEEE.