Secure Lightweight Routing Protocol with Confidentiality Redundancy in Wireless Ad Hoc Networks (SLRCR)

M. Taheri, M. Imani, M. M. Hajikolaei, and M. Naderi

***Abstract*—Mobile ad hoc networks (MANETs) are independent self-organizing systems of mobile nodes or computers connected by wireless links and without using of any infrastructure like base stations or access points. Routing is a critical function in multi-hop mobile ad hoc networks. The most important requirement for MANET routing protocols is the ability to operate in adversarial environments. In this paper, we proposed Secure Lightweight Routing protocol with Confidentiality Redundancy in wireless ad hoc networks (SLRCR). This protocol consists of two phases: 1) Using of MAC and symmetric cryptography for nodes authentication and 2) using of μTESLA for Confidentiality redundancy. This protocol is lightweight and robust; also, it is able to prevent large number types of routing attacks.**

***Index Terms*—Wireless ad-hoc network, security, routing, hash function, confidentiality.**

I. Introduction

All Ad hoc wireless networks are decentralized in a way that the nodes themselves forward data to other nodes without any infrastructure in between. The nodes are able to organizing themselves; by discovering their neighbors also they can work as routers for the data transmission. Recently, ad hoc networks have been becoming greater attention as more applications are depending on them features. [1]-[3].

In MANET, routing is a challenging task, because of the dynamic topology caused by mobility, limitations in bandwidth, range and power [1], [4]. Security is a main factor concern in ad hoc routing protocols. Some of ad hoc routing protocols are insecure and vulnerable against routing attack, and some other have high overload in network. Too much of secure routing protocol in ad hoc networks focused in authentication and they disregarded the data confidentiality after rout discovery. Hence, in this paper we introduced Secure Lightweight Routing protocol with Confidentiality Redundancy in wireless ad hoc networks (SLRCR). This protocol has two phases: at the first step the source, destination and intermediate nodes authenticate by use of MAC and secret key algorithm, after in the next step, the protocol utilizes μTESLA [5] protocol for data confidentiality redundancy. We base the design of SLRCR in part on the Ariadne ad hoc network routing protocol. Our protocol (SLRCR) is robust against multiple attackers creating incorrect routing packet in any other node, even; it is able to prevent a large number types of active attackers or compromised nodes in the network. In order to support utilize of SLRCR with nodes of limited CPU processing capability, and to protect against Denial of Service attacks in which an attacker tries to cause other nodes to consume network bandwidth or processing time, we used one way hash functions and did not use asymmetric algorithm.

The rest of the paper is organized as follows: In Section II, we introduce related works for secure routing. In Section III we describe types of routing attack in wireless ad hoc networks. In Section IV we present the SLRCR protocol in details. Section V analyzes the security characteristics of our protocol and Section VI concludes the paper.

Manuscript received September 14, 2014; revised November 18, 2014.

The authors are with School of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran (e-mail: mahdi_taheri@elec.iust.ac.ir, moh.imani@ieee.org, Mustafa.mirzagoli.iust@gmail.com, m_naderi@iust.ac.ir).

II. Related Works

A. Principal Ad Hoc Routing Protocols

AODV and DSR are the most well known routing protocols for a MANET [2], [3]. They are reactive protocols that nodes in the network exchange routing information only when a communication must take place and keep this information update only as long as the communication continues. These protocols were not designed to be secure and both are vulnerable to a number of attacks including impersonation, modification, and fabrication [6]. In addition, these protocols lack security techniques to protect location information exchanged between nodes, exhibiting the exact location of nodes to other within range.

B. Secure Ad Hoc Routing Protocols

Mostly the existing secure routing protocols that have been proposed for ad hoc networks can be classified into two groups, those that utilize hash chains, and those that utilize of digital signature. In this ways, the nodes can efficiently authenticate the legitimate traffic and route discovery packets.

Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [4], is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol(DSDV) [7]. In SEAD protocol, efficient one-way hash chains but not digital signature are used in the authentication of the sequence number and the metric (hop count) field of a routing table update message.

Ariadne [6] is a secure on-demand ad hoc routing protocol based on DSR that prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial of Service attacks. In addition data authentication in this protocol is provided by three different techniques: digital signature, MACs, or TESLA.

DOI: 10.7763/IJIEE.2015.V5.540

The Secure Routing Protocol (SRP) [8] consists of several security extensions that can be applied to existing ad hoc routing protocols providing end-to-end authentication. The scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner. No assumption in SRP is made regarding the intermediate nodes, which may present arbitrary and malicious behavior.

The Authenticated Routing for Ad hoc Networks (ARAN) [9] based on AODV is a secure protocol that exploits cryptographic public-key certificates signed by a trusted authority, which associates its IP address with a public key in order to achieve the security goals of authentication and non-repudiation to the route discovery process. This protocol was high security overhead.

Securing AODV (SAODV) [10] proposes a set of extensions that secure the AODV routing packets. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information.

TABLE I: ROUTING ATTACK IN WIRELESS AD HOC NETWORKS

Attack	Defending Approach
Wormhole[12, 13]	Packet Leashes, Reputation Systems, Multipath Routing
Black Hole[14, 15]	Reputation Systems , Authentication Approaches
Sybil Attack	Passively Monitoring Traffic, Authentication Mechanisms
Routing Table Overflow [16]	Adaptive Route Table Updating
Rushing	(Secured Dynamic Source Routing) SDSR Scheme

Attacks against routing protocol in ad hoc networks can be classified into two groups in a different way:

TABLE II: TABLE OF VARIABLES AND NOTATION

k_i	Interval Keys In µTesla Protocol
$F(k_i)$	One Way Function For Ki Authentication
P_i	Received Message In I^{th} Time Interval
RDP	Rout Discovery Packet
REP	Rout Reply Packet
k_{AX}	The Nodes A And X Shared Key
N_A	Sequence Number Of Node A
H	The MAC Is Computed By Source Node Using Of K_{ax}
H	The MAC Is Computed By Intermediate Nodes Node
P	Distribution Key And Time Interval Information Packet
T_{NOW}	The Source Node Already Time
T_{int}	Interval Time
T_i	Start Time For Ith Time Interval
D	Delay

Passive attacks involve only eavesdropping on the data that is being communicated in the network. Examples of passive attacks include covert channels, traffic analysis, sniffing to compromised keys, etc. Active attacks which involve specific actions performed by adversaries, for instance, the replication, modification, and deletion of exchanged data among the nodes [11].

Attacks are also classified according to the facilities used by the attackers in external and internal attacks. External attacks are typically active attacks that try to cause congestion in the network, propagate incorrect routing information, prevent services from working properly, or shut down the network completely. External attacks can typically be prevented by using standard security mechanisms, such as firewalls, encryption, and other cryptography based algorithms, etc. Internal attacks typically more occurred by malicious nodes, and hard to can defiant this type of attacks. Some important of routing attacks and defending approach for them are listed in Table I [11], [17].

III. SLRCR PROTOCOL

A. Assumption

In this paper we assumed that network links were bidirectional; for example, if node A is able to transmit to node B, then B, is able to transmit to A. Wireless links are often bidirectional, and many MAC layers require bidirectional structure exchange to avoid collisions [6].
We assumed that all nodes have loosely synchronized clocks, because in this protocol we used of interval key for data confidentiality redundancy, we need to synchronization nodes [6].

In SLRCR protocol, we assumed that secret key generated and distributed between nodes. Hence, each node in network, have one secret key by another node. For example, secret key of the source and destination is K_{SD}.

In this research we have used µTESLA protocol for confidentiality redundancy, due to this fact; we assumed that the receiver and intermediate nodes are loosely time synchronized and they know k_0 (a commitment to the key chain) in an authenticated way.

B. One Way Function in µTESLA Protocol Description

Authenticated broadcast requires an asymmetric mechanism. Unfortunately, asymmetric cryptography mechanisms have high computation, communication, and storage overhead, which make their usage on resource constrained devices impractical. µTESLA overcomes this problem by presenting asymmetry through a delayed disclosure of symmetric keys, which results in an efficient broadcast authentication scheme [5].

Fig. 2 shows an example of µTESLA protocol. Each key of the key chain corresponds to a time interval and all packets sent within one time interval are authenticated with the same key. The time until keys of a particular interval are disclosed is 2 time intervals in this example.

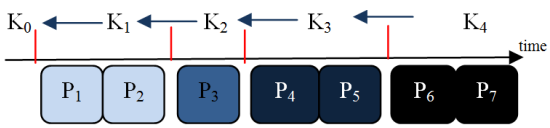

Fig. 1. Example of µTESLA protocol for message deycryption.

In this figure we assumed that packet p_1 and p_2 sent in interval 1 are encrypted with key k_1 and Packet p_3 is encrypted by using key k_2 in time interval 2. So far, when

the receiver received these packets, firstly, it authenticates key k_1 by verifying one way function $k_0 = F(k_1)$; then, if verifying was correct, the receiver can decrypt p_1 and p_2 with key k_1. Also, in other time interval, as soon as the node receives a key k_j of a previous time interval, it authenticates the key by checking that it matches the last authentic key it knows ki using a small number of applications of the one way function $k_i = F^{j-i}(k_j)$, If the check is successful, the new key k_j is authentic and the receiver can decrypt all packets that were sent within the time intervals *i* to *j*.

In this approach, instead of adding a disclosed key to each data packet, the key disclosure is independent from the packets broadcast, and is tied to time intervals. Within the context of µTESLA, the sender broadcasts the current key periodically in a special packet [5].

C. Routing in SLRCR Protocol

Most routing attacks we describe in Section III caused by malicious injection or changing of routing data by impersonation. To prevent these attacks, each node that interprets routing information must verify the origin and integrity of the data. SLRCR by use of secret key and one way hash function is able to achieve in this end. In the following discussion, we present the stages of routing by SLRCR protocol [4].

1) Rout request in SLRCR protocol

Here we assume that Fig. 2 is an example of MANET which in this network, the source node (A) want to established rout between own and destination node (X). Therefore the Source node begins route discovery to destination by broadcasting to its one hop neighbors a route discovery packet:

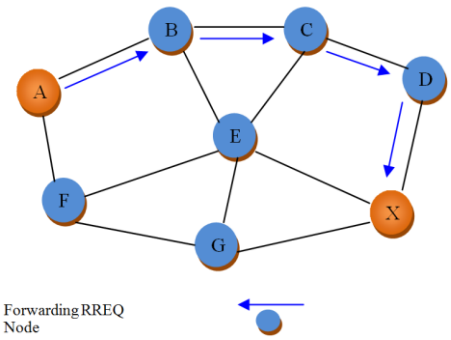

Fig. 2. Routing with SLRCR protocol in MANET.

$$A \rightarrow * \ [RDP, X, A, id, [P]k_{AX}, H] \quad (1)$$

This packet include a rout discovery packet (RDP), the source node identifier (id), destination node (X), source node (A), $[P]k_{AX}$ and H.
where:

$$H=MAC_{kAX}([P]k_{AX}, RDP, X, A)] \quad (2)$$

And

$$P=[N_A, T_{NOW}, k_i, T_i, T_{int}, D] \quad (3)$$

Here H was computed over these elements with a key was shared by the source and the destination (k_{AX}), that it utilizes for destination's authentication. Existence of P in rout request packet is because we can distribute key and interval time information for µTESLA protocol.

When the node B received the rout discovery packet as neighbor's A, it subsequently modified packet by following description and then rebroadcast it:

$$B \rightarrow * \ [RDP,X,A,id, (B,Nb), [P]k_{AX}, H, h0] \quad (4)$$

where:

$$h0 = MAC_{KBi}(B, N_b) \quad (5)$$

Here h_0 is computed by MAC algorithm and secret key of node B that disclosed later. Also, the node D modifies rout discovery packet then rebroadcasted it. When the node C received this packet, it computes h1 by:

$$h1 = MAC_{KCi}(B, C, N_c, N_b) \quad (6)$$

And then modifies rout discovery packet therefore rebroadcasted it:

$$C \rightarrow * \ [RDP, X,A, id, (B, C, N_c, N_b), [P]k_{AX}, H, (h0, h1)] \quad (7)$$

Each node along the path repeats these steps of modifying message and forward broadcasting it to receive the destination node. In this messages h0, h1, h2, … are involved digest of address and sequence number's nodes that they used for intermediate nodes authentication's.

2) Rout reply in SLRCR protocol

After receiving the RDP, the destination node unicasts a Reply (RREP) packet back along the reverse path to the source. The first node receives the RREP that was sent by node X to node D:

$$X \rightarrow D \ [REP, A, X, N_x, (B, C, D, N_B, N_C, N_D) N_x, Hd, (h_0, h_1, h_2)] \quad (8)$$

where in this packet Hd is:

$$Hd = MAC_{KAX}(REP, A, X, N_A, N_x, (B, C, D, N_B, N_C, N_D)) \quad (9)$$

That it utilized for destination authentication in RREP packet.

The sequence numbers that we used in thorough steps they are for node synchronization. The Nodes that received the REP forward the packet back to the predecessor from which they received the original RDP. Here the node D along the reverse path back to the source, appends its own MAC key and then forward it to the next hop (node C).

$$D \rightarrow C \ [REP, A, X, N_X, (B, C, D, N_B, N_C, N_D), Hd, (H_0, H_1, H_2), (k_{di})] \quad (10)$$

Also, the other intermediate node appends its own MAC key to the RREP packet and forwards it to the next hop. Extremity, RREP packet received to the source node in flowing form:

$$B \rightarrow A\ [REP, A, X, N_x, (B, C, D, N_B, N_C, N_D), Hd, (H_0, H_1, H_2), (k_{bi}, k_{ci}, k_{di})] \quad (11)$$

When the source receives the RREP, it verifies the H_is (H_0, H_1, H_2) by using of intermediate nodes MAC keys, and H_d by secret key (k_{AX}).

3) Rout maintenance in SLRCR protocol

Normal topology changes occur frequently in ad hoc wireless networks. Because of the mobility aspect of MANETs, the nodes might add or abandon the network; here the routs can broke. When routes was broke, route error messages will be sent from the position of the error towards the source node where a new route request may be initiated.

For example, in Fig. 3 we assumed that the node D moved and exited on radio range of the node C; in this case, the node C generates RERR message and sends it to the source node by intermediate nodes (nodes C, B):

$$C \rightarrow B\ [RERR, A, X, (C, N_c), MAC_{kci}\ (C, N_c)] \quad (12)$$

$$B \rightarrow C\ [RERR, A, X, (B, C, N_c, N_b), MAC_{kci}\ (C, N_c), MAC_{kbi}\ (B, C, N_c, N_b)] \quad (13)$$

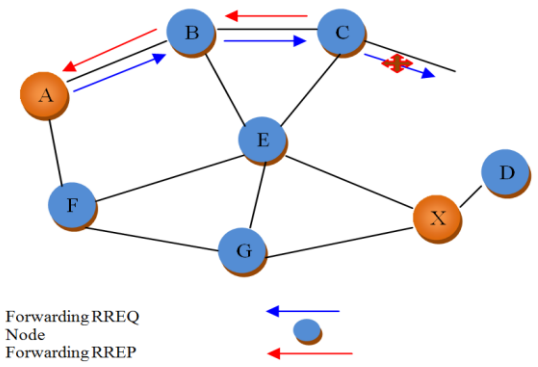

Fig. 3. Rout maintenancein SLRCR protocol.

When the source node A received RERR message, it verifies MACs by using of intermediate nodes MAC keys; then, the source node can attempt to use any other route it happens to know to destination node, or can invoke route discovery again to find a new route.

4) Confidentiality redundancy in SLRCR protocol

Too much of secure routing protocol in ad hoc networks focused in authentication, and they disregarded the data confidentiality after rout discovery. The excellent feature in SLRCR protocol is appointing the Confidentiality redundancy by use of one way function in µTESLA protocol. Since we mentioned in routing phase, P are send in rout request packet to the destination node through the intermediate nodes where it encrypted by secret key of source and destination node:

$$P = [N_A, T_{NOW}, k_i, T_i, T_{int}, D] \quad (14)$$

where P containing its current time T_{NOW} (for time synchronization), a key k_i of the one way function keys, and the starting time T_i of interval *i*, the duration T_{int} of a time interval, and sequence number of source node.

Previously we assumed that the initial key k_0 of one way function distributed between all nodes; hence, the destination node authenticate k_i by using of one way function:

$$K_0 = F^i(k_i) \quad (15)$$

Therefore, the new key k_i is authenticated. In this case, the receiver can decrypt all packets that were sent within this time intervals. The format of the packets that were sent in time interval i are:

$$[[M]k_i, MAC\ k_i\ ([M, k_i])] \quad (16)$$

In this message MAC was utilized to authenticate the node M by other intermediate node. When the time interval *i* is end; the k_i expired, in this time the source node send key k_{i+1} by using of:

$$A \rightarrow X: [N_A, T_{NOW}, k_{i+1}, T_{i+1}, T_{int}, D]k_{AX} \quad (17)$$

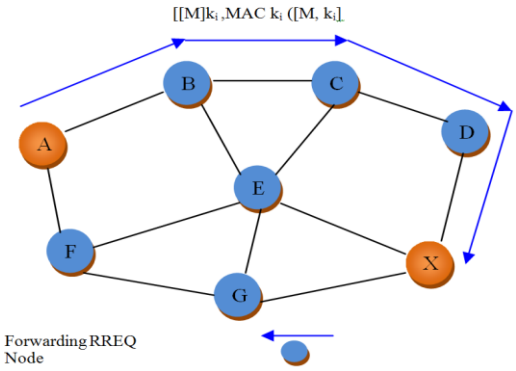

Fig. 4. Transfering the data packet in i^{th} time interval.

When destination receives this message, it authenticates key k_{i+1} with one way function, then the destination uses it for decrypts all packets that were sent within the time intervals *i*+1. Too, in subsequent time interval this process continues. Fig. 4 shows sending key in time interval *i*.

IV. Evaluation SLRCR Protocol

- *Security evaluation*: in the first phase of SLRCR protocol, the nodes are authenticated by MAC algorithm; hence, protocol is secure against the impersonation attacks (such as: black hole, syble, grey hole, DOS …). In the second phase of protocol, one way function of µTESLA protocol is utilized for encryption-decryption and data confidentiality redundancy. In this case, if some nodes compromised after rout establishment, they are not able eavesdrop the data packet. It is because; in SLRCR protocol, in every time interval is utilized apart key for data encryption-decryption. Table III compares our protocol in ability to attack detection by other secure protocols.
- *Overhead evaluation:* in SLRCR protocol we used of MAC and secret key algorithm for nodes authentication. Like a normal hash function, a MAC algorithm, maps an input of any length to a fixed-length bit string. Therefore, this approach is lightweight in compare with other secure protocol that they utilize digital signature and asymmetric algorithms such as ARAN protocol. The network's

overhead compared in Table IV for SLRCR protocol and other secure protocols.

TABLE III: SECURITY COMPARISON IN AD HOC ROUTING PROTOCOL

Criterion / Protocol	*Security*		
	Confidentiality redundancy	**authentication**	**overhead**
DSR	-	-	-
AODV	-	-	-
ARAN	-	Digital signature	High
SAODV	-	Hash function	Medium
Ariadne	-	digital signature, MACs, TESLA	Low
SLRCR	µTESLA	MACs	Low

TABLE IV: ABILITY TO ATTACK DETECTION IN AD HOC ROUTING PROTOCOL

Criterion / Protocol	**Attacks**		
	DOS	**Black hole**	**Wormhole**
DSR	vulnerable	Vulnerable	vulnerable
AODV	vulnerable	Vulnerable	vulnerable
ARAN	vulnerable	Resistant	vulnerable
SAODV	resistant	resistant	vulnerable
Ariadne	resistant	resistant	resistant
SLRCR	resistant	resistant	resistant

V. CONCLUSION

Based on vulnerability in Wireless Ad Hoc Networks, in this paper, we introduced SLRCR protocol for routing security. In this protocol we used of MAC and secret key algorithm to authenticated the nodes in rout discovery phase. By utilizing of in these algorithms, security overhead in routing phase decreased. The goal of second phase of protocol is confidentiality redundancy. For reaching in this end, we used of one way function in µTESLA protocol for key distribution and key authentication. By using of this approach, we can renew keys; hence, probability of eavesdropping diminished.

REFERENCES

[1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, 2008.

[2] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Computer Communications Review Proceedings of SIGCOMM*, 1996.

[3] C. E. Perkins and E. M. Royer, " Ad hoc on-demand distance vector routing," *IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, 1999.

[4] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *IEEE Workshop Mobile Comput*, pp. 3–13, 2002.

[5] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "Spins: Security protocols for sensor networks", in *Proc. Conference on Mobile Computing and Networking*, pp. 189–199, 2001.

[6] Y. C. Hu, D. B. Johnson, and A. Perrig, "Ariadne: A secure on-demand routing protocol for ad hoc wireless networks," *Wireless Networks*, pp. 21–38 2005.

[7] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," presented at the ACM Sigcomm, October 1994.

[8] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM WiSe, Atlanta*, pp. 1–10, 2002.

[9] L. Huaizhi and M. Singhal, "A secure routing protocol for wireless ad hoc networks," *IEEE International Conference on Network Protocols*, pp. 225-235, 2006.

[10] Zapata MG. Secure Ad Hoc On-demand Distance Vector (SAODV) Routing. IETF Internet Draft. [Online]. Available: http://www.ietf.org/internetdrafts/ draft guerrero-manet-saodv-00.txt, 2001.

[11] A. Mishra, *Security and Quality of Service in Ad Hoc Wireless Networks*, Cambridge University Press, pp. 10-152, 2008.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Jelected Jreas in Communications*, vol. 24, no. 2, pp. 370-380, 2006.

[13] M. taheri, M. Naderi, and M. B. Barekatain, "New approach for detection and defending the wormhole attacks in Wireless ad hoc networks," in *Proc. Electrical Engineering (ICEE), 2010 18th Iranian Conference*, pp. 331-335, 2010.

[14] S. Sharma and R. Gupta, "Simulation study of blackhole attack in the mobile ad hoc networks,", presented at International Conference on Network Applications, Protocols and Servise, 2008.

[15] I. Aad, J. P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/Acm Transactions on Networking*, vol. 16, no. 4, pp. 791-802, 2008.

[16] S. Li, Q. Liu, H, Chen, and M. Tan, "A new method to resist flooding attacks in ad hoc networks," *IEEE/Acm Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2006.

[17] M. Yu and M. Zhu, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments," *IEEE Transactions*, vol. 58, pp. 449–460, 2009.

Mohsen Imani received his BS degree in electrical engineering in 2004 from Shahrood University of Technology and his master degree in the same field from Iran University of Science and Technology (IUST) in 2011. He was a member of Secure System Lab at IUST from 2008 to 2011. His research interests are network security and communication networks. Currently he is doing his PhD in computer science at the University of Texas at Arlington.