The 8th International Scientific Conference
eLearning and software for Education
Bucharest, April 26-27, 2012
10.5682/2066-026X-12-113

OLSRBOOK: A PRIVACY-PRESERVING MOBILE SOCIAL NETWORK LEVERAGING ON SECURING THE OLSR ROUTING PROTOCOL

Mohamed Amine FERRAG, Mehdi NAFA, Salim GHANMI
Badji Mokhtar University - Annaba, Algeria
E-mail: mohamed.amine.ferrag@gmail.com[1], mehdi.nafaa@gmail.com[2], ghanemisalim@yahoo.com[3]

Abstract*: Social networking mobile Ad Hoc have no centralized infrastructure, so it is difficult to provide authentication services. Much work is ongoing and no complete solution to secure mobile ad hoc networks against attack has been made to date. This problem remains a major problem facing today's researchers in the field of ad hoc networks. Through this article, we proposed a security scheme for mobile ad hoc social networks where OLSR is the routing protocol .We have chosen the OLSR routing protocol because it is the most widely used ad hoc community. In general the attacker can delete, modify, copy control messages to send false messages. Our scheme consists of detecting the type of attack, the checks and then ends with alert the nodes of mobile social network. These three elements is based on the addition of five messages " Hreq , Hrep, HAlert, Probing and ACKprob" in the OLSR protocol. For the exchange of a package of Hreq , Hrep and HAlert ; and to provide authentication as well confidentiality. We have proposed the dual use of public key encryption; the message will be decrypted only by the true recipient and to ensure safe exchange of a package of Probing and ACKprob, we proposed an architecture through the use of RSA and MD5 to sign messages. The proposed solution is easy to deploy and requires no time synchronization or location information nor does it require any special equipment or complex calculation.*

Keywords: *Social networks, Mobile Ad Hoc Networks, OLSR, MD5, RSA, Cryptography.*

I. INTRODUCTION

Wireless ad hoc network is a system in which computer systems that compose it can communicate independently via radio waves. Computer systems, or nodes, to exchange information directly, or should the node they want to reach is out of reach, through intermediate nodes. The routing function in these systems is essential as it is for each node to form their own picture of the network topology. The problem of security of these ad hoc networks is a subject topical.

There are primarily two types of routing protocol in ad hoc networks. The reactive routing protocols (AODV, DSR) that initiates the search for a route when trying to reach a destination that is not contained in the routing table. The proactive routing protocols (OLSR, FSR) that maintain regularly update the information in the routing table with route discovery requests. Note that the hybrid algorithms exist. They then make use of both protocols under different conditions.

Two types of algorithms used to maintain accurate routing tables. This is the distance vector algorithms and link state. In general, the route discovery is as follows. When a node wants to transmit a message to another node it broadcasts a route request different denominations according to the protocols. The road was then built as and when his discovery to the recipient once attached can return a message back to sender. The road is then set and the actual data exchange can take place. In the absence of authentication, confidentiality, integrity, etc. Ensuring the smooth running of these protocols, network stability can be greatly compromised.

Much work is ongoing and no filling solution from end to end security of an ad hoc network has been presented to date. The objective is indeed complex. The issue of privacy is almost solved but major gaps remain in terms of routing protocols. For this reason, the subject of this article focuses on the security of routing protocols. We have chosen the OLSR routing protocol because it is the most widely used in ad hoc community.

The design consideration for MANET made a number of differences with the traditional centralized networks, namely: (i) Dynamic Toplogy [8] ; (ii) Resource Contraints [11] ; (iii) Low Cost ; (iv) Limited physical.

MANET is subject to a number of attacks. For example, an attacker in the MANET node may not be willing to route packets to other nodes. On the other hand, more sophisticated attacks against MANET routing can disrupt the route discovery. In addition, they may interfere with maintaining ride disobedient routing protocols. Blackhole Attack [17] , Byzantine Attack [2] , Wormhole Attack [3] [1], and Spoofing Attack [4] are illustrations of various threats for MANET that will be detected and avoided by our security scheme.

For the purposes of group communication security, cryptography has been integrated in MANETs. Among the most popular techniques, symmetric [9] [10] and public key infrastructure (PKI) [12] [13] [14] [15] [16].

The following section states related work. We analyze the different requirements for secure mobile social networks being and present OlsrsBook. Our new approach to privacy preserving services of social networks with the proposed level security routing protocol OLSR.

II. RELATED WORK

Many researchers address problems related to online social network [24] [25] [26] [27] [28]. Contrary to our type of social network that is completely mobile. In this section, we present the relevant research.

2.1. Attacks against MANETs

MANETs are vulnerable to different attacks than other types of networks. These cons are easier to implement because in an ad hoc network, can neither control access to the transmission medium, or define the boundaries of the network.

The routing protocol, specific to MANET and essential to its operation, it is a favorite target. Taxonomy of attacks against WLAN is divided into two classes: passive attacks and active attacks. Passive attacks are based on access by an unauthorized node, to frames that traverse the network to collect information without altering the data exchanged. Passive listening is to view the content of messages exchanged between two nodes. Traffic analysis is to destroy for the different exchange networks, information on the organization or network configuration. Active attacks aim to enable to a node authorized to modify a message.

2.2. Vulnerability analysis of the Optimized Link State Routing Protocol

In ad hoc mobile networks, routing operations are entirely the responsibility nodes that comprise them. Unlike wired networks where operations are generally performed by physical devices dedicated interconnection and managed by a legitimate administration. The key concept used in the protocol is the use of multipoint relays (MPR). It functions as a proactive protocol, topology information with other network nodes are exchanged regularly. But as the nodes are independent, the rules defined by the protocol may appear and cause distortion of the view of the network topology built.

In [1], we presented a summary of the attacks against OLSR. Now, we will present mechanisms against measures that exists in the literature and we end with a table summarizing the

existing solutions. The table (Tab1) summarizes existing solutions to secure the routing protocol OLSR.

Tab1e 1. Existing solutions to secure the OLSR routing protocol and analysis

Attacks			Loss of connectivity	Loss of message	Target	Semantic properties of OLSR [2]	AdvSig [19]	Environment or trusted third party	OlsrBooK	
									Time	Signature
Generation trafic incorrect	HELLO	Usurpation identity	X	X	All nodes	Yes	No	Yes		Yes
		Usurpation link	X		Nodes in the direct vicinity of the opponent	Yes	Yes	Yes		Yes
	TC	Usurpation identity	X	X	All nodes	Yes	No	Yes		Yes
		Usurpation link	X		Subset of node	Yes	Yes	Yes		Yes
	Attaque ANSN		X	X		No	No	Yes		Yes
Relaying traffic incorrect	Changing message		X			Non	Yes	Yes		Yes
	black hole		X	X	nodes specific	No	No	Possible		Yes
	Replay		X	X		No	Yes	Yes		Yes
	Wormhole		X		Subset of nodes close to the hole	No	No	Possible as the black hole	Yes [1]	
	MPR		X	X	Specific nodes	No	No	Yes		Yes

Authentication. One example of these protocols is SEAD [18] (security extensions to DSDV where they offered protection against alterations of mutable fields, namely the metric field and the sequence number field), secure (OLSR extension OLSR). This extension is primarily to discriminate nodes that are part of the network nodes that do not belong. The disadvantage major of the proposed method is based on a key management infrastructure more or less adapted to the environment of mobile ad hoc and do not address issues related to the behavior of internal nodes in the network.

An Advanced Signature System For OLSR. This approach is based on cryptography, where the direct impact is to ensure network integrity and potentially avoid malicious nodes in the establishment phase of the roads. The solution requires no modification of the standard OLSR messages but this approach's weakness raised by Chen [19] is no certificate and its proof is required in the reporting phase of an asymmetric link. However, the method based solely on the target node for the detection of anomalies but the proposed method does not locate an attack.

Approach based on an identification system intrusion IDS. In [20], the authors have proposed a simple security against attack: (1) For manufacturing / modification of TC messages, (2) For state change links in the HELLO messages. However, the method based solely on the target node for the detection of anomalies but the proposed method does not locate an attack. One disadvantage of this method is that warning messages should be disseminated through the network so that each node can make routing decisions adapted.

Approach based on the correlation of information in the HELLO messages and TC. This is a generalization of the method proposed previously. In this proposal, no modification of the protocol is required. The idea proposed by Wang. One advantage of this approach is it requires changes in the format of protocol messages, but validation of the approach is not formal it means the effectiveness of the approach is verified by experiment. In [21] and then taken by Cuppens in [22] is to derive security properties for the routing protocol OLSR from the correlation of information contained in the TC and HELLO messages. One advantage of this approach is it requires changes in the format of protocol messages, but validation of the approach is not formal it means the effectiveness of the approach is verified by experiment.

Secure processor (Environment confidence). This approach is based on trusted third parties. The latter, on board each of the nodes being part of the network, is responsible for operations of core routing protocol such as the generation and processing of control messages and the storage of data collected. One advantage of this approach is that only the control information generated by the third party is considered valid on the network. But to consider possible attacks in the retransmission phase.

III. OLSRBOOK

In this section, we describe our security scheme for mobile ad hoc social networks using OLSR as routing protocol. In our approach, nodes initially try to detect suspicious links and verification of the attack and finish by informing nodes that there's an attack in the social network.

3.1. Overview of our schematic

The architecture of our system OLSRBooK is shown in Figure 1. OLSRBook consists of two layers: (a) a physical layer of ad hoc network and (b) a layer of virtual social network. In the network layer (virtual) social are connected by virtual links where OLSR is used as routing protocol.

In the network layer (virtual) social are connected by virtual links where OLSR is used as routing protocol.

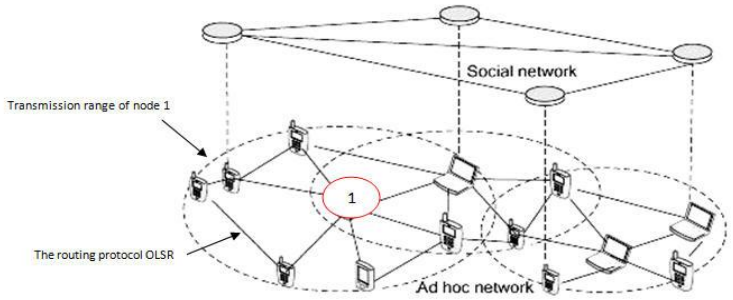

Figure 1. Presentation of the system OLSRBook

Each virtual link is to a communication channel which may be composed of several hops. Once the friendly relations are established, friends can perform social such as resource sharing, sending messages, and navigation from each other. Below we detail the essential elements our security architecture. The figure.3 represents our approach to detect and verify attacks.

3.2. Detect suspicious links:

The OLSR is optimized by the use of multipoint relays. The latter are selected nodes which send messages to the diffusion process during the flood. The use of MPR significantly reduces the overhead messages compared to a classical flooding mechanism, where each node transmits each message when it receives the first copy of the message [23].

Generally the attacker can delete, modify, copy control messages to send false messages. However, one of the characteristics of attacks against OLSR packet latency is relatively longer than the propagation time (the attack of the black hole and wormhole).

This is not a sufficient condition for the existence of an attack, because the transmission of packets affected by various factors such as congestion. This is why we added more messages to check the attack.

To infer suspicious links, we define two packages new control for OLSR [23] "Hreq & Hrep" (Fig. 2), they have the same format of the HELLO message, but we added a field to detect suspicious links from other attacks that do not characterize by latency time.

- Reserved: This field should be "0000000000000000".
- Htime: Interval of issuance of messages Hreq,
- Willingness: to force the passage of a node in MPR
- Link Code: Code identifying the type of link (no information, symmetric, asymmetric) between the sender and the interfaces listed ("Neighbor Interface Address").
- Champ_sig: Detects malicious and check links.

Figure 2. Datagram Message Hreq, Hrep, Probing, ACKprobing

A, B: Two nodes in a social network.

1: The exchange of public keys for public announcement.

2a ... d: Distribution of secret keys with privacy and authentication.

3.4: The exchange of two messages Hreq and Hrep to detect suspicious links.

5.6: The exchange of two messages Probing and ACKprobing to verification of suspicious links.

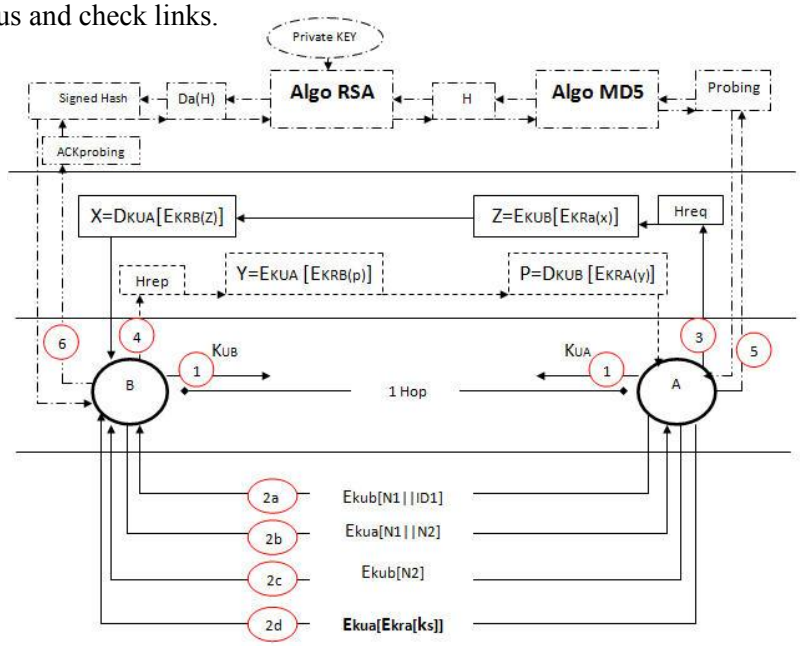

Figure 3. Our security scheme for social networks fully mobile using OLSR routing protocol

After each transmission of N message (The value of N can be adjusted depending on the level of security), a node encrypts the field "Champ_sig" of message Hreq and sends. When a node receives a Hreq, it decrypts the field value "Champ_sig" and it records the address of the sender i and time Δi. To avoid overloading the network with too many messages Hrep, we propose to delay responses to several requests until it is planned to send its normal HELLO message. The node receives a Hreq, it decrypts the message and checks if this contains information about Hreq at each of its requests, if there is no information about its previous requests, the node addresses the Hreq received as a normal Hello message else the node control the arrival time of received Hreq and the arrival in the waiting period specified; the node performs the link between itself and the node that sent the Hrep as suspicious and stops communicating with this node until the end of the verification procedure.

3.3. Verification of suspicious links:

After the detection of suspicious links, the node that detected the suspicious link runs the verification procedure. To this end, two new messages "Probing & ACKprob" are added to OLSR that have the same format of HELLO message. A node crypt with MD5 and RSA (Fig 3, 5-6) and sending the message to Probing all of its suspected nodes. When a node receives the message Probing, decrypts it, then he prepares a message to meet ACKprobing. If the node receives a packet of Probing has no information on the status of the source node, it fails to send the ACKprob. After receiving the message by the sender it checks the validity of the message ACKprob before using the information it contains. After the detection and verification of the attack, it sends HAlert to inform other nodes and then judge around him according to the algorithm *ProvedSuspicous()*.With this architecture is based on the addition of messages and signatures, OLSRBooK can detect all attacks against OLSR. (TAB1)

Algorithm ProvedSuspicious() :

```
i=1 ; time=n ;
While (i<>0) do
   If (distance=proved and ACKprob=proved) Then Begin
                                                i=0 ;
                                               Call AcceptInformation() ;
                                               End;
  Else if (distance=suspicious and ACKprob=suspicious) Then begin
                                                          i=0;
                                                         Call Remove_node_one_hop() ;
                                                         Call Remove_node_two_hop() ;
                                                          End;
       Else if time= 0 Then begin
                              i=0;
                              Call Remove_node_one_hop() ;
                              Call Remove_node_two_hop() ;
                              End;
            Else time=time-1;
End While;
```

We proposed OLSRBooK secure architecture for fully mobile social networks where OLSR is used as routing protocol. This structure is based on securing the OLSR routing protocol. The proposed solution is easy to deploy and requires no time synchronization or location information; nor does it require any special equipment or complex calculation. For future work is to study the performance of our system OLSRBooK .

References

[1] Mohamed Amine Ferrag , Mehdi Nafaa , Securing the OLSR routing protocol for Ad Hoc Networks Detecting and Avoiding Wormhole Attack ,Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Volume 2 , April Edition, 2011.

[2] Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H, Anon-demande secure routing protocol resilient to bayzantine failures. In: WiSE 2002: Proceeding of the first ACM workshop on wireless security, New Yourk, USA: ACM; 2002. P. 21-30.

[3] Maheshwari R, Gao J, Das SR. Detecting wormhole attacks in wireless networks using connectivity information. In : 26th annual IEEE conference on computer communications (INFOCOM '07). Anchorage, Alaska, USA : IEEE Press; May 2007. P. 107-15.

[4] Sanzgiri K, Levine BN, Shields C, Dahill B, Belding-Royer EM. A secure routing protocol for ad hoc networks. In: IEEE international conference on network protocols, 2002. P. 78-87

[6] T. Karygiannis and L. Owens. Wireless network security. NIST Special Publication 800-48, National Institue Of Standards and technology-NIST- Technology Administration U.S Departement of Commerce, Novembre 2002.

[7] Qing Chen and Zubair Md. Fadullah . A clique-based secure admission control scheme for Mobile Ad Hoc Networks (MANETs) . Journal of Network and Camputer Application 34 (2011) 1827-1835

[8] Chen L, Kudla C. Identity based authenticated key agreement protocols from parings. In : Proceedings of the 16th IEEE computer security foundations workshop, 2003. P.219-33.

[9] Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory 1976;22(6):644-54.

[10] Bhaskar R, Augot D, Adjih C. Agdh (Asymmetric group diffie hellman) an efficient and dynamic group key agreement protocol for Ad Hoc networks. In : New technologies mobility and security (NTMS) conference. Paris, France, May 2007.

[11] He S, Chen J, Sun Y, Yau D, Yip N-K. On optimal information capture by energy constrained mobile sensors. IEEE Trans Veh Technol 2010;59(5):2472-84.

[12] Capkun S, Buttay L, Hubaux J-P. Self-organized public-key management for mobile ad hoc networks. IEEE Trans Mobile Comput 2003;2(1) ; 52-64.

[13] Zhou L, Haas Z. Securing ad hoc networks. Technical Report, Ithaca, NY, USA : 1999.

[14] Yi S, Kravets R, Moca: mobile certificate authority for wireless Ad hoc networks. In : Second annual PKI research workshop. Gaithersburg, MD, USA 2003.

[15] Rachedi A, Benslimane A, Guang I, Assi C. A confident community to secure mobile ad-hoc networks. In : ICC 2007. Glasgow, Scotland, UK, 2007.

[16] Rachedi A Benslimane A. A secure architecture for mobile ad hoc networks. In: Seconde international conference on mobile ad hoc and sensor networks MSN 2006. Springer's Lecture Notes in Computer Science. Hong Kong, China, Decembre 2006. P. 424-35.

[17] Ad I, Hubaux J-P, Knightly EW. Impact of denial of service attacks on Ad Hoc networks. IEEE/ACM Trans Netw 2008; 16(4): 791-802.

[18] Wei-Shen Lai , Chu-Hsing Lin, Jung-Chun Liu, Yen-Lin Huang and Mei-Chun Chou. I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks. International Journal of Multimedia Ubiquitous Engineering . Vol. 3, No. 4, October, 2008.

[19] Chen L, Xue X, and Leneutre J . A lightweight mechanism to secure olsr. In IMECS (2006°, pp. 887-895.
[20] Fourati, A., and Khaldoun, A. A. An ids rst line of defense for ad ho c networks. In Wireless Communications and Networking Conference, WCNC 2007 (March 1115 2007), IEEE , pp. 26192624.
[21] Wang, M., Lamont, L., Mason, P., and Gorlatova, M. An effective intrusion detection approach for OLSR manet protocol. pp . 55-60.
[22] Cuppens, F., Cuppens-Boulahia, N., Nuon, S., And Ramard, T. Property based intrusion detection to secure olsr. In ICWMC'07 ; Proceeding of the Third International Conference on Wireless and Mobile Communications (Washington, DC, USA, 2007), IEEE Computer Society, p. 52.
[23] T. Clausen and P. Jacquet.Optimized link state routing protocol.http://ietf.org/internet-drafts /draft-ietf-manet-olsr-11.txt, July 2003.
[24] S. Guha, K. Tang, and P. Francis, "NOYB: Privacy in Online Social Networks," Online Social Net., 2008, pp. 49–54.
[25] C. M. A. Yeung et al., "Decentralization: The Future of Online Social Networking," Future Social Net., 2009.
[26] R. Baden et al., "Persona: An Online Social Network with User-Defined Privacy," ACM SIGCOMM, Barcelona, Spain, Aug. 2009.
[27] S. Buchegger et al., "PeerSoN: P2P Social Networking," Social Net. Sys., 2009.
[28] M. Rogers and S. Bhatti, "How to Disappear Completely: A Survey of Private Peer-to-Peer Networks," 2007.