A Secure and Efficient Link State Routing Protocol for Ad Hoc Networks

Lin Chen, Jean Leneutre, Jean-Jacques Puig
Departement INFRES - CNRS LTCR-UMR5141
Ecole Nationale Supérieure des Télécommunications
46, Rue Barrault, 75634 Paris Cedex 13, France
{Lin.Chen, Jean.Leneutre, Puig}@enst.fr

Abstract

Routing protocols in ad hoc networks are vulnerable to various attacks. Many solutions have been proposed to secure ad hoc routing protocols in recent research but often at the price of significant traffic and processing overhead, which may be undesirable for ad hoc networks with limited bandwidth and processing power. In this paper, we present and evaluate a secure and efficient link state routing protocol for ad hoc networks (SELRAN). We propose Secure Link State Update Procedure (SLSUP) and Secure Neighbor Establishment Procedure (SNEP) in SELRAN to counter external and internal uncoordinated attacks. We also use counter-based mechanism to reduce the broadcast overhead of the LSU packets in SELRAN, which makes SELRAN efficient in resource-constraint environments such as ad hoc networks. Analysis and simulation results show that SELRAN effectively thwarts a wide range of attacks to ad hoc routing, and is able to maintain high packet delivery ratio even in hostile environments.

1 Introduction

A mobile ad hoc network is an autonomous collection of mobile nodes communicating with each other over wireless links and cooperating in a distributed way in order to provide the necessary network functionality in the absence of a fixed infrastructure. A routing protocol in such networks finds routes between nodes, allowing a packet to be forwarded through other nodes towards its destination. Due do their nature, ad hoc networks are more vulnerable to various attacks than traditional wired network. Unfortunately, almost all the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic, which may be easily exploited by attackers to disrupt the routing protocol and disable communication.

Designing secure and efficient ad hoc routing protocols is a challenging task due to the highly dynamic nature of ad hoc networks and the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power of each individual node in the network. Existing insecure ad hoc routing protocols are often highly optimized to spread routing information quickly as topology changes, requiring more rapid and often more frequent routing protocol interaction between nodes than in traditional wired and static networks. Expensive and cumbersome security mechanisms may delay or prevent such exchanges of routing information, thus reducing its effectiveness, and consuming significantly network or node resources.

In this paper, we present and evaluate our secure and efficient link state routing protocol for ad hoc networks (SELRAN), which is efficient in terms of traffic and processing overhead and powerful to protect the integrity of the network topology against a wide range of uncoordinated external and internal attacks to the routing protocol. The following argument push us to focus on link state ad hoc routing: first it inherits the advantage of proactive routing protocols in terms of routing delay and is especially suited for ad hoc networks with low to medium mobility, high connection rates and frequent communication with a large portion of the network nodes; secondly, it is intrinsically more robust to malicious attacks than its distant vector peer.

The paper is organized as follows. Section 2 reviews related work. In Section 3, we present SELRAN in detail. Section 4 and 5 provide security analysis and performance evaluation on SELRAN. Section 6 concludes the paper.

2 Related Work

Recently, a number of solutions have been proposed to secure wireless ad hoc routing protocols [1], [8], [9], but most of them are designed for reactive protocols. To the best of our knowledge, only a few secure routing protocols or enhancements are proposed in the scope of link state proactive ad hoc routing.

SLSP [3], based on asymmetric key pairs, secures the discovery and the distribution of link state information both for locally and network-wide topologies.

0-7695-2629-2/06/$20.00 (c) 2006 IEEE

Unfortunately, it is based on erroneous assumptions that each node cannot impersonate the MAC address of other nodes and that all the wireless links are symmetric.

ADVSIG [4] is proposed to secure OLSR [7] against both external and internal uncoordinated attacks. The core idea is that if node *A* declares a symmetric link with node *B*, it should include a proof signed by *B* obtained from previous HELLO messages sent by *B*. This proof-based mechanism requires each node to perform a large number of asymmetric cryptographic operations to generate and verify proofs and thus may significantly degrade the performance of OLSR.

3 Secure and Efficient Link State Routing Protocol for Ad hoc Networks (SELRAN)

Given the vulnerability of ad hoc routing protocols to various attacks and the problems of existing solutions for secure link state routing protocols, we propose our secure and efficient link state routing protocol for ad hoc networks (SELRAN) which provides secure and efficient proactive topology discovery for ad hoc networks. From the security point of view, it can detect and thwart uncoordinated external and internal attacks and ensure the network topology integrity. From the performance point of view, it is highly optimized for ad hoc networks to run efficiently with limited resources and bandwidth.

3.1 Assumptions and Attacker Model

We consider a wireless mobile ad hoc network consisting of a number of networking nodes that may roam freely, remain stationary for a period of time, join and leave the network, or fail at any time. Each node has a unique ID. Nodes perform peer-to-peer communication over shared, bandwidth constrained, error-prone, and multi-hop wireless channel which may be lossy, asymmetric, and prone to interference.

We assume that each node processes an authentic private/public key pair. The setup of authentic keys can be achieved by a trusted certificate server or by PGP-like certificates. Nodes can also broadcast their certified key periodically in case where a central CA is not available.

Attackers to ad hoc routing may disrupt the operation of the routing protocol by exhibiting arbitrary malicious behaviors: e.g., replay, forge, corrupt routing control messages to influence the topology view of benign nodes. These attacks can be classified as external attacks and internal attacks based on the information the attackers have. External attacks are launched by attackers who do not have the cryptographic credentials (e.g. the keys used by cryptographic primitives) that are necessary to participate in the routing process. Internal attacks are launched by attackers who have compromised legitimate nodes, and therefore have access to the cryptographic keys owned by those nodes. Obviously internal attacks are far more difficult to detect and sometimes cannot be countered by pure cryptographic primitives. SELRAN aims to thwart both internal and external attacks under the condition that the attackers do not collaborate.

Possible attacks to routing protocols
Routing message forgery
Routing message alteration
Routing message replay
Spoofing
Collusion (e.g. wormhole)
Deny of service (DoS)

3.2 Overview

SELRAN aims to run securely and efficiently in presence of uncoordinated malicious attackers by meeting the following requirements:

1. Routing messages cannot be spoofed.
2. Routing messages cannot be altered or replayed.
3. Forged topology information can be detected.
4. The routing protocol itself is efficient for ad hoc networks.

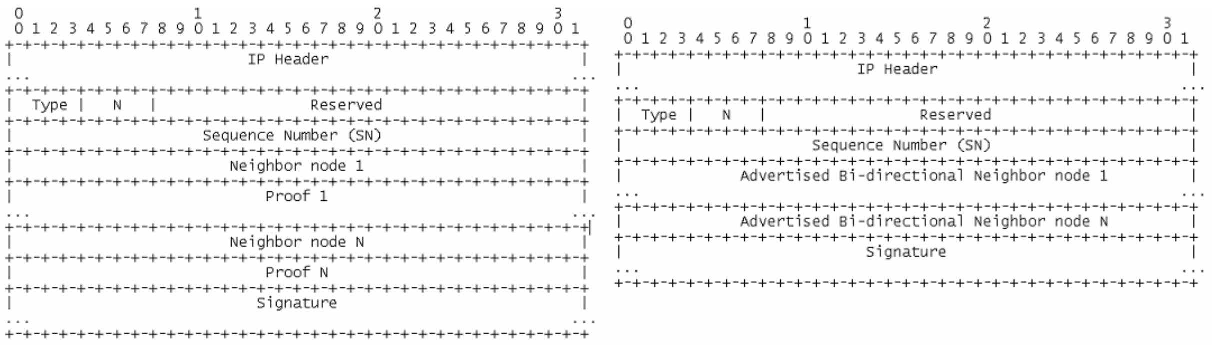
To achieve these goals, SELRAN uses digital signatures to ensure the authentication and the integrity of the routing messages and counter external attacks such as malicious alteration. Internal attacks cannot be countered by pure cryptographic primitives. Hence more sophisticated Secure Link State Update Procedure (SLSUP) and Secure Neighbor Establishment Procedure (SNEP) are proposed to detect them. Finally, we optimize the LSU packets broadcast process to make SELRAN suitable and efficient for ad hoc networks.

3.3 Secure Link State Update Procedure (SLSUP)

SLSUP is the core function of SELRAN through which each node updates its routing table according to the topology information in the received link state update packets (LSU), which are broadcast into the network periodically.

An LSU is identified by its sender and the sequence number (SN) that increases by 1 each LSU. The use of SN can counter replay attacks and ensure that each LSU is processed once.

Besides the global signature, we introduce a new mechanism to counter the forgery of the topology information in LSU by internal attackers. Each node i is responsible for detecting the attack launched by any internal attacker declaring forged link with it. Basically, i performs the following check when receiving an LSU: if a link is declared between i and the sender of the LSU, but the sender is not a neighbor of i, i broadcasts a signed alert message to notify all participants of the network that the forged link does not exist. On receiving the alert message, other nodes recalculate their routing tables by removing the forged link.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           IP Header                           |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type  |   N   |                  Reserved                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Sequence Number (SN)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Neighbor node 1                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Proof 1                             |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Neighbor node N                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Proof N                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Signature                            |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           IP Header                           |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type  |   N   |                  Reserved                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Sequence Number (SN)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Advertised Bi-directional Neighbor node 1           |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Advertised Bi-directional Neighbor node N           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Signature                            |
...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1. Routing message format: HELLO (left), LSU (right), TYPE: message type, N: number of declared neighbor nodes. The TTL and Hop

A random delay is added to the scheduled emission time of each LSU to avoid the transmission collision. The same mechanism is applied in the following SNEP to avoid the emission collision of HELLO messages.

3.4 Secure Neighbor Establishment Procedure (SNEP)

In SNEP, each node detects the neighbor nodes with which it has bi-directional links and securely establishes the neighborhood relationship with them. Most of current solutions base themselves on the assumption that links in ad hoc networks are bi-directional. In fact this assumption is erroneous due to the following reasons:

1. The instable nature of radio channels may make some wireless links uni-directional.
2. A malicious attacker may use a more powerful antenna than other nodes to establish uni-directional links with them and then declare those links bi-directional. The attack cannot be detected under the above assumption.

SNEP should counter this link spoofing attack.

In SNEP, only links that are declared and checked in both directions are validated.

Each node A periodically broadcasts HELLO messages to its neighbor nodes which contain: (1) the list of nodes L from which it has received the HELLO messages recently; (2) for each node B in L, the hash value of the combination of the recently received HELLO message from B, m_B, and the identity of A: $h(h(m_B), A)$. The hash value serves as a proof that the link $B \rightarrow A$ really exists. When node B receives the HELLO message with B in L and the correspondent proof $h(h(m_B), A)$ from A, it verifies the proof. In case of success, it can be sure that link AB is bi-directional and thus validates A as its neighbor node. Note that the identity of A is needed in the hash operation, otherwise the proof may be reused by an attacker to declare that it can hear B. The following scheme gives an example of the establishment of a bi-directional link in SNEP[1].

1. $A \rightarrow * (B): \{\emptyset, \emptyset\}_{SA}$
2. $B \rightarrow * (A): \{A, h(h(M_1), B)\}_{SB}$
3. $A \rightarrow * (B): \{B, h(h(M_2), A)\}_{SA}$

The global HELLO message is signed by its sender to ensure its integrity. Upon receiving the second HELLO message M_2, A is sure that the link AB is bi-directional. Upon receiving the third HELLO message M_3, B is sure that the link AB is bi-directional.

SNEP thus provides a lightweight mechanism to establish neighbor relationship, only requiring that each node buffers the hash values of recently sent and received HELLO messages.

3.5 LSU Broadcast Optimization

The broadcast algorithm of the LSU packets is a crucial component of link state routing protocols, especially for ad hoc networks where bandwidth and processing resources are limited. In classic link state routing protocols,

[1] In the example, $A \rightarrow * (B): M$ indicates A broadcasts message M which is received by B. The format of HELLO messages in SELRAN is {list of nodes from which A has received the HELLO messages recently, list of the proofs}, Ø indicates that the correspondent list is empty

broadcast is realized by flooding, in which each node retransmits each received unique LSU packet exactly once. Pure flooding may lead to serious bandwidth congestion and inefficient use of node resources, which may further cause detrimental effect on such resource limited environment as ad hoc networks. Therefore, an efficient LSU broadcast mechanism is needed in SELARN to minimize the number of retransmissions while ensuring that every broadcast LSU reaches each node in the network.

Recently, a number of researchers have proposed more efficient broadcasting techniques which can be classified into two main catalogues: the first catalogue is totally localized without any additional information, an example is counter-based broadcast algorithm proposed in [2]; the second catalogue, slightly outperforms the first one, is based on neighbor knowledge (1-hop and 2-hop) or other additional information such as location and relative distance, an example is multi-point relay (MPR) technique used by OLSR. In SELRAN, we choose the first catalogue in that the second catalogue needs neighbor knowledge or other additional information that may require expensive or cumbersome security mechanisms to secure. These security mechanisms may reduce the effectiveness of the routing protocol or further significantly consume massive network and node resources. For example, in ADVSIG, a large number of asymmetric cryptographic operations need to be performed to protect the forgery of the 2-hop neighbor nodes, which may degrade the performance of OLSR to great extent as shown later in Section 5. The above argument pushes us to choose counter-based scheme, the approach which achieves high reachability with the least retransmission overhead among all approaches in the first catalogue.

Specifically, a counter *c* is used to keep track of the number of times the LSU packet is received. A counter threshold *C* is chosen. When $c<C$, the rebroadcast is inhibited. The scheme is presented below:

1. Initialize counter $c = 1$ when a LSU packet msg is heard for the first time.
2. Calculate a random delay uniformly distributed in $[0, T_{max}]$ and schedules to transmit msg when the delay timer expires.
3. During the random delay, if msg is received, increase *c* by one. If $c \geq C$, cancel the transmission of msg.

By adopting the above scheme, the LSU broadcast algorithm in SELRAN is simple and intrinsically adaptive to network topology.

4 Security Analysis

Ideally, a secure routing protocol should be resistant against all potential attacks. In reality, given the highly dynamic nature of ad hoc networks and the different scenarios of their application, it is difficult even impossible to design a solution that can counter all kinds of attacks in all possible application scenarios. In this section, we discuss the security properties of our approach under different attacks.

Routing message alteration: SELRAN uses digital signatures to ensure the authentication and integrity of the routing messages HELLO and LSU. Any illegal alteration will lead to signature check failures and the altered messages are discarded by receivers.

Routing message replay: The replay of LSUs are detected by the sequence number (SN) check. The LSUs with old SN are regarded as out-of-date. Since ad hoc networks are usually temporary local networks, we argue that the 32-bit space for SN is large enough to prevent the roundup problem. The replay of HELLO messages can be detected because the attacker cannot provide up-to-date proof without altering the replayed HELLO massage.

Routing message forgery: Attackers may forge LSUs with incorrect topology information such as non-existent bi-directional links. This kind of attacks is thwarted by the alert mechanism. Two points need further explanation:

1. A node may send alert messages to deny the links with its neighbors although the links do exist. This behavior shows the unwillingness of this node to participate in the routing process. We regard it as selfish behavior rather than attacks and as a result, the node will be isolated from the network.
2. An attacker may declare bi-directional links with non-existent nodes in LSUs. The attack cannot be detected since no alert is generated by non-existent nodes. However, this attack cannot disturb the proper operation of the routing process under the condition that the attackers do not collaborate because no packets will be routed to non-existent nodes.

Furthermore, we can limit the maximum number of links advertised in an LSU to prevent a malicious node from declaring too many forged links to poison the receivers's routing tables.

Spoofing: An attacker may spoof the address of other nodes and retransmit repeatedly the received LSUs, aiming to disable the nodes around it to further retransmit the LSUs in that a node receiving more than *C* duplicates cancels its retransmission according to the broadcast algorithm in SELRAN. Due to the connection redundancy of ad hoc networks, the impact of this attack is limited since the LSUs can reach the network via other unattacked routes. Furthermore, each node increases its counter only when the LSU comes from its neighbors, thus increasing the difficulty for attackers to launch spoofing attacks because they have to spoof different addresses to attack different nodes.

Collusion: The colluding attacks such as wormhole attacks cannot be countered by SELRAN. [6] proposes the packet leash scheme to counter wormhole attacks, but a strict time synchronization is needed.

Deny of service: An attacker may emit a massive amount of routing messages to consume the resources of other nodes and deprive them from participating in routing process. In order to counter the DoS attack and guarantee the responsiveness to the routing protocol, the solution proposed in [3] can be used in SELRAN. The basic idea is that each node maintains a priority ranking of their neighbor nodes according to the rate of the routing message they generate. The highest priority is assigned to the nodes generating or relaying routing messages at the lowest rate and vice versa. Quanta are allocated proportionally to the priorities and non-serviced, low priority packets are eventually discarded.

We do not address repeater attacks in which an attacker behaves as a repeater by relaying all routing messages between two normal nodes *A* and *B* but dropping all or some of data packets. In fact this attack is not an attack to the routing protocol because from the topology's point of view, there does exist a link between *A* and *B* via a repeater. Therefore the attack should be countered by other mechanisms such as watchdog or packet leash other than a secure routing protocol.

5 Performance Evaluation

5.1 Simulation Methodology

We implement SELRAN in NS-2.28 [5] and evaluate its performance by carrying out a set of simulations (30 simulations, each lasts 250s). The simulation field is 1500m*300m, where 50 nodes move according to the random way-point model. The nodes speed is set uniformly distributed in [0, 15m/s] with 20s of pause time. The traffic pattern is 32 random sessions (the source and destination are randomly chosen for each session) of constant bit rate (CBR) flow at a rate of 10 packets per second, and 512 bytes per packet in size. The hash function and digital signing function are MD5 (128 bits) and RSA (1024 bits) respectively. The LSU and HELLO intervals are set to 5s and 2s. T_{max} is set to 0.5s. We also simulate OLSR and its secure enhancement, ADVSIG, and compare SELRAN with ADVSIG since they aim to provide the same level of security.

In order to simulate the impact of signature and verification operations on the performance, we add the correspondent delay when processing and sending messages taking into consideration the heterogeneity of ad hoc networks in which nodes has different processing capacity: we attribute to each node a random processing time in [0.2ms, 150ms] for signing operation and in [0.1ms, 100ms] for verification operation.

We observe the following metrics to measure the performance of different routing protocols:

1. *LSU/TC pkt broadcast overhead* is the number of LSU/TC[2].
2. *Routing message overhead* is the ratio of the total overhead of routing messages generated and relayed in the network including the correspondent security overhead (in byte) over the received data (in byte).
3. *Data packet delivery ratio* is the ratio of the data packets generated by the CBR sources that are delivered to the destinations.
4. *Average end-to-end delay* of data packets is the average delay between the emission of the data packet by the CBR source and its arrival at its destination.
5. *Average route length* is the average length (number of hops) of the CBR sessions.

5.2 Simulation Results

Table 1 shows the performance of simulated protocols without attackers. Generally we can see from the table that SELRAN achieves good performance with reasonable security overhead. SELRAN achieves about 60% delivery ratio, slightly higher than OLSR and ADVSIG. From the result, we can also see that choosing the counter threshold *C* to be 2 achieves the best performance in our simulated scenarios. In terms of the LSU/TC packets broadcast overhead, the MPR technique used in OLSR and ADVSIG slightly outperforms the counter-based scheme used in SELRAN, but taking the security overhead into consideration, we can see that SELRAN can avoid heavy security mechanisms to secure the 2-hop neighbor node information, thus generating significantly less routing

[2] In OLSR, the link state update packets are called Topology Change (TC) messages

message overhead than ADVSIG, as shown by the metric Routing message overhead in Table 1.

We also evaluate the performance of the simulated protocols in hostile environment where 20% of the nodes in the network is compromised. They forge LSU/TC and HELLO messages to declare non-existent symmetric links with other nodes randomly selected from the normal nodes. Then they behave as black-holes by dropping all data packets. We can see from the simulation result that the attacks cause detrimental effects on the performance of OLSR, which shows the necessity of building a secure routing protocol to guard against malicious attacks. The result of ADVSIG is not satisfactory either due to the large number of expensive cryptographic operations it performs. In contrast, SELRAN shows good resistance to the attacks and is still able to achieve nearly 50% in terms of packet delivery ratio.

6 Conclusion

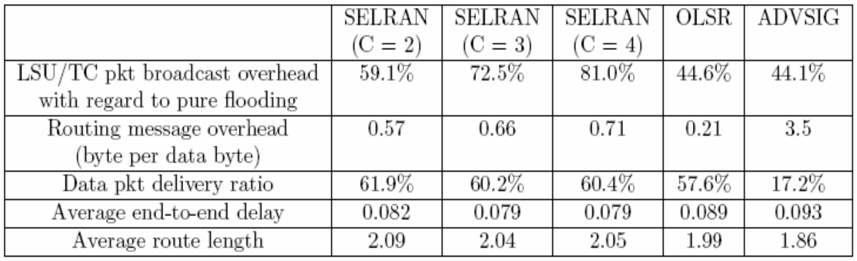
Nowadays the security of ad hoc networks may become one of the bottlenecks of its potential applications especially in open environment. We argue that security and its impact on performance should be taken into consideration in the design of routing protocols for ad hoc networks.

Our protocol, SELRAN, is a secure and efficient link state routing protocol for ad hoc networks. By implementing the Secure Link State Update Procedure (SLSUP) and the Secure Neighbor Establishment Procedure (SNEP), SELRAN is resistant to both external and internal uncoordinated attacks. By using the counter-based broadcast mechanism, SELRAN reduces significantly the retransmission overhead of LSUs. This feature is especially desirable in ad hoc networks where bandwidth and processing resources are limited.

Our future work includes implementing different possible attacks and test SELRAN in a more hostile environment and improving SELRAN to counter coordinated attacks.

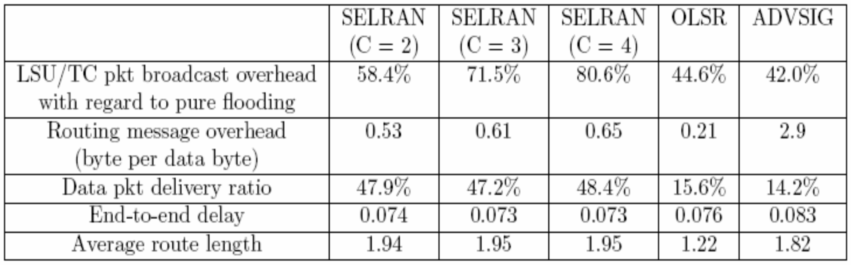
Reference

1. P. Papadimitratos, Z. Haas. Secure routing for mobile ad hoc networks. Proc. of 7th SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS02), 2002.
2. S. Ni, Y. Tseng, Y. Chen, J. Sheu, The broadcast storm problem in a mobile ad hoc network, Proc. of MobiComm, August, 1999.
3. P. Papadimitratos, and Z.J. Haas. Secure Link State Routing for Mobile Ad hoc Networks. IEEE Workshop on Security and Assurance in Ad hoc Networks, 2003.
4. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler. An advanced signature system for OLSR. Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), Washington, USA, 2004.
5. NS2. http://www.isi.edu/nsnam/ns/.
6. Y. Hu, A. Perrig, D. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. Proc. of IEEE INFOCOM, San Francisco, USA, 2003.
7. Optimized link state routing protocol (OLSR). October 2003. RFC 3626, Experimental.
8. Y.-C. Hu, A. Perrig, and D.B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. Proc. 8th ACM Conf. Mobile Computing and Networking (Mobicom02), Atlanta, USA, 2002.
9. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer. A Secure Routing Protocol for Ad hoc Networks. Proc. 10th IEEE International Conference on Network Protocols (ICNP`02), IEEE Press, 2002.



	SELRAN (C = 2)	SELRAN (C = 3)	SELRAN (C = 4)	OLSR	ADVSIG
LSU/TC pkt broadcast overhead with regard to pure flooding	59.1%	72.5%	81.0%	44.6%	44.1%
Routing message overhead (byte per data byte)	0.57	0.66	0.71	0.21	3.5
Data pkt delivery ratio	61.9%	60.2%	60.4%	57.6%	17.2%
Average end-to-end delay	0.082	0.079	0.079	0.089	0.093
Average route length	2.09	2.04	2.05	1.99	1.86

TABLE I Performance without attackers



	SELRAN (C = 2)	SELRAN (C = 3)	SELRAN (C = 4)	OLSR	ADVSIG
LSU/TC pkt broadcast overhead with regard to pure flooding	58.4%	71.5%	80.6%	44.6%	42.0%
Routing message overhead (byte per data byte)	0.53	0.61	0.65	0.21	2.9
Data pkt delivery ratio	47.9%	47.2%	48.4%	15.6%	14.2%
End-to-end delay	0.074	0.073	0.073	0.076	0.083
Average route length	1.94	1.95	1.95	1.22	1.82

TABLE II Performance with 20% of nodes being attackers