International Journal For Technological Research In Engineering
Volume 1, Issue 8, April-2014 *ISSN (Online): 2347 - 4718*

SECURITY AGAINST SPOOFING ATTACK USING SOLSR PROTOCOL

Ms.Hina Jani[1], Ms. Meghavi Gandhi[2], Mrs. Hiteshi Diwanji[3]
[1,2]Networking and Communication, Rollwala Computer Center, Gujarat, India.
[3]Department of Computer Engineering, L.D Engineering College, Gujarat, India.

Abstract: MANET has become successful in grabbing the eyeballs of many researchers in networking area. Among the different routing protocols OLSR assumes that all the nodes in the network topology are trusted i.e. authenticated. However, in hostile environment OLSR is vulnerable to various kind of attacks such as spoofing, worm hole attack and colluding misrelay attack. Among different schemes such as hybrid protection of OLSR, Signature Scheme, Secure OLSR (SOLSR), we have implemented SOLSR. Using Hash (along with ceaser cipher encryption) we check the authenticity of nodes and thereby detect and recover spoofing attack. Also by implementing SOLSR along with our Hash Scheme the throughput and packet delivery ratio is of network increased and end to end delay of network is decreased.

Index Terms: MANET, OLSR, SOLSR, Hash, Spoofing attack.

I. INTRODUCTION

There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks. The infrastructure less networks is known as Mobile Ad-hoc Networks (MANET).These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner [1, 3].

Security is an important concern in wireless ad-hoc networks. Due to wireless and distributed topology, ad-hoc networks deals with the communication with its neighbours so number of attacks are possible. There are different routing protocols are used in MANET to secure network against some attacks. OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of the link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature [4, 6, and 7].

OLSR minimizes the overhead caused by flooding of control traffic by using only selected nodes, called Multi-Point Relays (MPR), to retransmit control messages [5]. OLSR uses HELLO and TC messages. HELLO messages are used in neighbour discovery. The Topology Control (TC) messages for continuous maintain of the routes to all destinations in the network. It is vulnerable to attacks like Spoofing, Worm hole attack and Colluding Misrelay attack. Although some of these attacks are solved but issue of spoofing is not totally solved.

In this paper, we propose a new security aware OLSR which is a security extension for current OLSR protocol. Now as we are focusing on detecting and recovering from Spoofing attack and making OLSR secure from this attack, different schemes are available. Among different schemes such as hybrid protection of OLSR, Signature Scheme, Secure OLSR (SOLSR), we have implemented SOLSR.

Using Hash (along with cesar cipher encryption) we check the authenticity of nodes and thereby detect and recover spoofing attack. Also by implementing SOLSR along with our Hash Scheme the throughput and packet delivery ratio is of network increased and end to end delay of network is decreased. The encryption technique used in implementing hash is cesar cipher.

II. OVERVIEW OF THE OPTIMIZED LINK SOURCE ROUTING (OLSR) PROTOCOL

OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of the link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature [4, 7].

OLSR minimizes the overhead caused by flooding of control traffic by using only selected nodes, called Multi-Point Relays (MPR), to retransmit control messages [5]. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Upon receiving an update message, the node determines the routes (sequence of hops) toward its known nodes. Each node selects its MPRs from the set of its neighbours saved in the Neighbour list. The set covers nodes with a distance of two hops. The idea is that whenever the node broadcasts the message, only the nodes included in its MPR set are responsible for broadcasting the message. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route.

Control traffic in OLSR is exchanged through two different types of messages: 'Hello' and 'TC' messages. Hello messages are exchanged periodically between neighbour nodes, to detect links between neighbours, to detect the identity of neighbours and to signal MPR selection. TC messages are periodically broadcasted to the whole network, to signal link state information to all nodes [6].

III. ATTACKS ON OLSR PROTOCOL

A. Node identity Spoofing

Node misbehaving, likes masquerading vulnerabilities or identity spoofing in the OLSR protocol allows an intruder pretend to use the IP address of another node. Identity Spoofing implies that the misbehaving node sends control messages while pretending to be another node.

B. Link Spoofing Attack

In this attack, a malicious node advertises that it has a direct link with a faraway node in its HELLO message or TC message to intercept the control/data traffic or disrupt routing operation.

C. Wormhole Attack

In this attack, a pair of colluding attackers record packet at one location and replay them at another location using private high speed network. The seriousness of this attack is that it can be launched even against all communications which provides authenticity and confidentiality.

Malicious nodes *M1 and M2 work in collusion to tunnel routing* packets, e.g., HELLO messages and TC messages between nodes *A and B. This will cause nodes A and B to believe* that they are direct neighbours (1-hop neighbours). This will also cause nodes *C, D, E to conclude that nodes B is* their 2-hop neighbours. As a result, all data traffic from *C, D, E to B will be routed the wormhole link which is* believed to be the shortest route.

D. Colluding Misrelay Attack

The misrelay attack which is launched by one malicious node can be detected by overhearing approach. However, in colluding misrelay attack, multiple attackers work in collusion to misrelay packet to avoid being detected by these overhearing schemes.

IV. RELATED WORK ON OLSR SECURITY

There is some work done to provide the security to OLSR protocols. The description of the different approaches is given below.

A. Hybrid protection of OLSR

It's using The Hash Chain for providing the security to the routing protocol. In this approach we calculate the Hash of some Initial value up to total no of Hop count and distribute it to the entire network. And the sender node sends the one time hash of initial value to the next neighbour which is MPR of it. Now the intermediate node calculate the difference of TTL and Hop count and doing the hash of received hash value up to calculated difference time. If both the value is same then there is no malicious node changed the value in between them. If both the value is not same then there is some malicious node and it changed the value of Hop count and TTL for making the path to itself.

B. Signature Scheme

And other approach is [8] provide the security with the help of signature scheme. And the approach provides the authentication between the two nodes. For providing the signature the approach use the two functions. First one is for signature and the second is for verification

1. Sign (nodeid, key, message) A signature for a message can be verified in a node using a function:
2. Verify (originator id, key, message, signature).

To prevent malicious nodes from injecting incorrect information into the OLSR network, the originator of each control generates an additional security element called signature message and transmitted with the control message. A timestamp is associated with each signature in order to estimate message freshness. Thus, upon receiving the control message, a node can determine if the message originates from a trusted node, or if message integrity is preserved. Signatures are separate entities from OLSR control traffic: while OLSR control messages perform the purpose of acquiring and distributing topological information, signatures serve to validate information origin or integrity.

C. Secure OLSR

This security scheme is work on two levels. In the first level we just concern on the hello message and try to stop the unauthorized nodes to participate in the route creation process and in the second level try to implement the hash chain in the OLSR to secure from the other attack possible in the OLSR protocols.

The steps are as

1. Encryption algorithm
2. Hash chain

There we take some assumption for the network. We assume that the secrete key between the nodes is distributed by any physical method or any cryptography scheme.

D. Security From Various Attacks

The table describe the security provided by the different security schemes at various attacks. Here we concerned the 5 different attack and check that the security schemes are efficient against them or not [10].

S.No	Attacks	Hybrid Scheme	Signature Scheme	SOLSR
1.	Wormhole attack	Yes	No	Yes
2.	Black hole	Yes	No	Yes
3.	Id spoofing	No	Yes	Yes
4.	Replay	No	Yes	No
5.	Route corruption	Yes	No	Yes

Table. 1. Verification using hash.

V. IMPLEMENTATION OF SECURITY AWARE OLSR (SOLSR)

In this section, we propose a security aware OLSR (SAOLSR), an improved version of current OLSR in terms of security [7]. The goal of our approach is to assure that routing traffic generated/forwarded by a node can be successfully received by all its 2-hop neighbours and to enable each node to verify the existence of link advertised by its 1-hop neighbours.

Implementation of SOLSR Scheme has following advantages like:

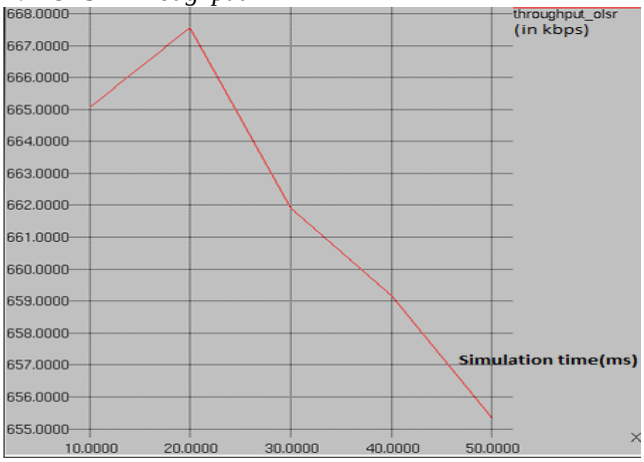
1. It provides node to node authentication between the nodes.
2. It provides the source to destination authentication.
3. It provides safety from attacks for external nodes.
4. A node can use the previous send message to other place.
5. SOLSR provides integrity.

Security wise the SOLSR provide the more security than the other two approaches but the complexity of it is more than the other two approaches.

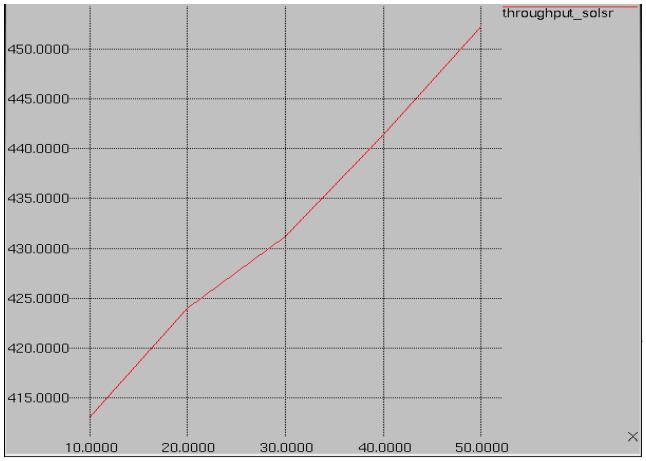
Using Hash (along with cesar cipher encryption) we check the authenticity of nodes and thereby detect and recover spoofing attack. Also by implementing SOLSR along with our Hash Scheme the throughput and packet delivery ratio is of network increased and end to end delay of network is decreased. The encryption technique used in implementing hash is cesar cipher

.

A. OLSR Throughput

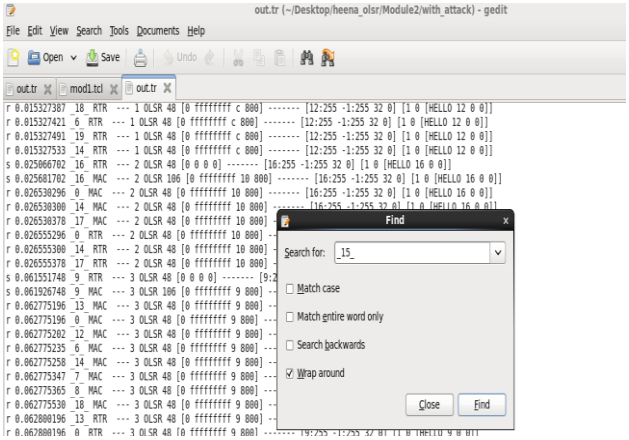


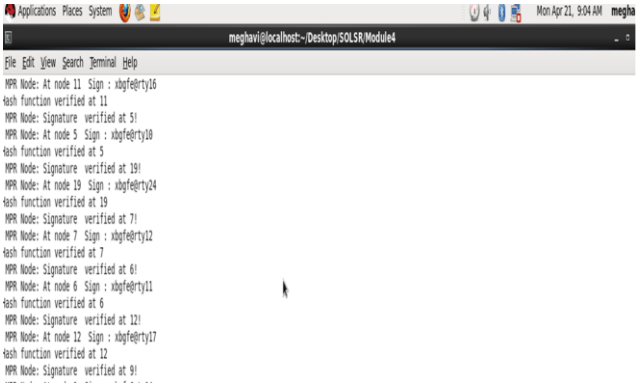
B. SOLSR Throughput



D. Spoofing attack

In our NS2 simulator we have the trace files to check the logs. Due to the spoofing attack, node 15 will be missing in our trace file. Instead of node no 15 node 0 will be shown.





By securing OLSR and using the secure scheme there is markable increase in throughput and packet delivery ratio and decrease in end to end delay.

VI. CONCLUSION AND FUTURE SCOPE

Security Aware OLSR (SA-OLSR) is a security extension to the original OLSR protocol.

The main advantage of our approach is that it does not require any specialized hardware such as GPS and does not require complete knowledge of the whole network while being able to protect several kinds of attacks. To validate analysis, we implemented our proposed solution on a network simulator- NS2.

Simulation results show that the attack can bring a devastating impact on the current OLSR. It also shows that the proposed security mechanism provides an effective protection against this kind of attack.

We secured OLSR by using the hash functions, thereby authenticating MPR nodes in the network and assuring that the communication being carried out between the nodes in the network is reliable. We also conclude that by securing OLSR and using the secure scheme there is makeable increase in

throughput and pdr and decreasing in end to end delay. Thus by using SOLSR efficiency of the network is increased.

In future one can implement other hash schemes such as MD5, SHA-1 as well as other digital signature schemes. But utmost care is to be taken as MANET deals with the dynamic topology.

REFERENCES

[1] Adjih, D. Raffo, and P. Muhlethaler,"Attacks Against OLSR: Distributed Key Management for Security," 2nd OLSR Interop/ Workshop, Palaiseau, France, July 28-29, 2005.
[2] Raffo,"Security Schemes for the OLSR Protocol for Ad Hoc Networks," Ph.D. thesis, Universite Paris, 2005.
[3] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Analysis of the Node Isolation Attack against OLSR-based Mobile Ad Hoc Network," 7th International Symposium on Computer Networks (ISCN), pp. 30-35, Istabul, Turkey, Jun. 2006. [10] D. Dhillon, J. Zhu, J. Richards, T. Randhawa,"Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs," in IWCMC 2006.
[4] M. Wang, L. Lamont, P. Mason, M. Gorlatova,"An effective Intrusion Detection Approach for OLSR MANET Protocol," 1st IEEE ICNP Workshop on Secure Network Protocols (NPSec 2005).
[5] Raffo, C. Adjih, T. Clausen, P. Muhlethaler,"Securing OLSR Using Node Locations," in Proceedings of 2005 European Wireless (EW 2005), Nicosia, Cyprus, 2005.
[6] A J. P. Vilela and J. Barros,"A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks," Proc. Of the 15th IST Mobile and Wireless Communications Summit, Mykonos, Greece, June 2006.
[7] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks," IEEE Global Telecommunications Conference 2006 (Globecom), San Francisco, USA, Nov. 2006.
[8] F. Nait-Abdesselem, J.K. Yoo and B. Bensaou, "Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol," IEEE Wireless Communications and Networking Conference (IEEE WCNC), March 2007.
[9] The Vint Project, "The Network Simulator - ns-2," see Ztp://www.isi.edu/nsnam/ns/index.html/.
[10] RFC 3626 [OLSR]
[11] RFC SOLSR

