

An Enhanced Reputation-Based Scheme for Securing OLSR

Hongzhi Jiao

Faculty of Engineering and Science



Outline

- Overview of security in ad hoc networks
- Motivation
- OLSR-related
- Proposed scheme
- Conclusion

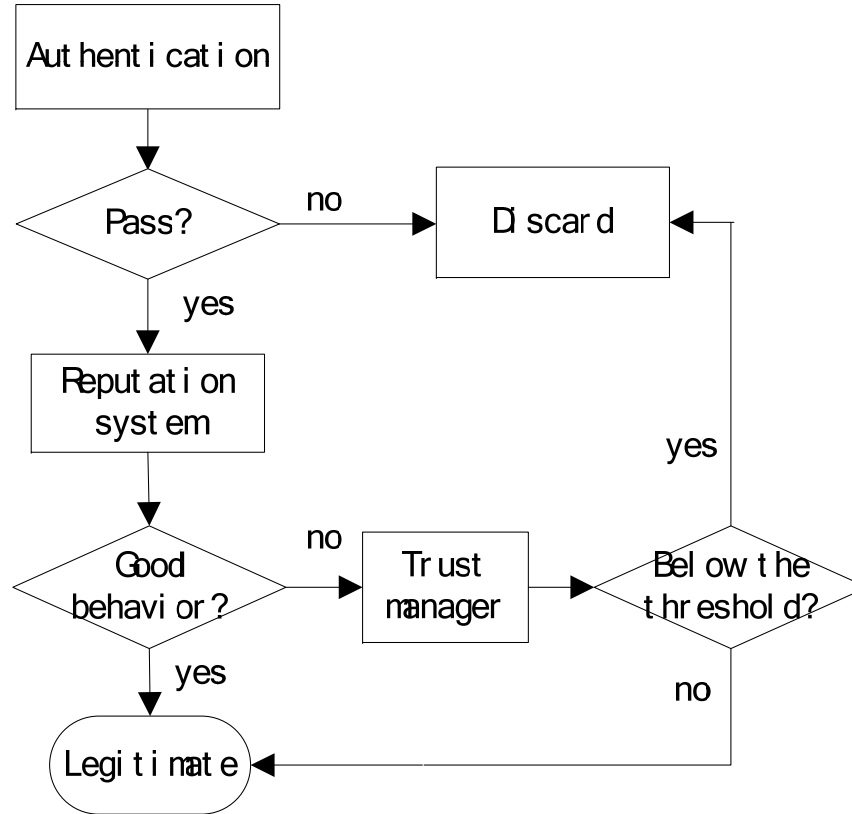
Overview

- Security is a chain, it is only as secure as the weakest part in the chain. Missing a single component may significantly degrade the strength of the overall security solution.
- Shared wireless medium environments of MANET opens the network to numerous security attacks which can actively disrupt the routing protocol and disable communication.
- Means used to deal with security attacks:
 - Prevent - Detect - Recover
- Both security strength and network performance are important, a good trade-off between two dimensions should be considered.

Two basic approaches to protect MANETs

- Proactive: attempt to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques.
- Use authentication to prevent the potential attacks
- Reactive: the reactive approach seek to detect security threats posterior and react accordingly.
- Apply the reputation system detective mechanism as a reactive way to ensure the highest security level.

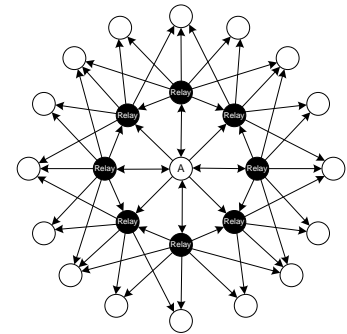
Motivation



- We propose a combined two-step scheme including both authentication and reputation-based forwarding node selection to secure OLSR protocol.

OLSR Introduction

- A proactive link state routing-protocol
- Neighbor sensing
 - Periodic HELLO messages
- Optimization through Multipoint Relay (MPR)
 - MPR selected among one-hop neighbors
 - Message flooding overhead optimized
- Link State dissemination
 - Regular broadcast of link state information (TC messages)
- Internet connectivity through HNA messages
- Routing table calculation
 - Hop-count based



Security Vulnerabilities of OLSR i

- Jamming:

Jamming is used to describe the deliberate use of radio noise or signals in an attempt to disrupt communications. Jamming allows intruder nodes to overwhelm the wireless medium and cause all other nodes in range to continuously back off.

These attacks aim at preventing control traffic from diffusing and thus can prevent nodes from calculating correct routes.

Security Vulnerabilities of OLSR ii

- Node identity spoofing

Node misbehaving, like 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 a misbehaving node sends control messages while pretending to be another node.

Security Vulnerabilities of OLSR iii

- Misbehaving of HELLO Messages

- ***Withholding message***

If an intruder intentionally withholds information about a symmetric neighbor link in its HELLO message and the targeted neighbor does not have any other connection to the MANET, that neighbor will become disconnected from the network. Even if the targeted neighbor has other nodes to provide connectivity to the MANET, this attack may cause non-optimal routes to be calculated.

- ***Spoofing message***

- The spoofed neighbors may or may not exist elsewhere in the MANET.
- Upon receiving such a HELLO message, the intruder's neighbor nodes will select the intruder as an MPR in an attempt to reach the spoofed two-hop neighbor.
- The MPR calculation algorithm of OLSR will preferentially select one-hop neighbors which uniquely provide connectivity to a node in the two-hop neighbor set.
- Therefore an intruder can use this attack to become the only MPR for its neighborhood.

- False advertisement of symmetric/asymmetric link

This attack can introduce non-optimal routes into MANETs. For example, if the link type of a neighbor is mis-advertised as ASYM while it is actually SYM, it will effect other nodes' MPR calculations.

Furthermore, if a node incorrectly advertises its MPR set, routes may be lost.

Security Vulnerabilities of OLSR iv

- Misbehaving of TC Messages

- ***Spoofing MPR Selector Links***

An intruder can spoof MPR selector links by adding extra MPR selectors in its TC messages. If such an MPR selector already existed elsewhere in the network, then packets destined to that node may be sent to the intruder first. The intruder is free to drop, modify, and/or monitor those packets. In the case where the MPR selector does not exist elsewhere in the MANET, this attack could still cause an overflow of the routing table.

- Withholding MPR Selector Links

If the targeted node has selected only the intruder as an MPR, that node will be disconnected from the MANET.

If other valid MPRs were also selected, then that node will remain connected through them, however optimal routes may be lost.

Another way an intruder can withhold a TC message is to set the TTL field to a small value, rather than 255 as suggested in the OLSR RFC. This will prevent a TC message from being flooded through the entire MANET.

- Tampering with TC Messages

An intruder could also tamper with a TC message before relaying it: inserting MPR selectors into or deleting MPR selectors from it; changing its source IP address

The effects of modifying these fields are similar to incorrectly generating TC messages. Message tampering attacks can be prevented through message authenticity mechanisms such as digital signatures.

Security consideration of OLSR

- Lead to authentication: In order to verify that the node is actually the one it claims to be, we should set up identity authentication before two nodes begin to establish the neighbor relationship
- Lead to reputation system: We need to be able to verify that the arrived routing packet has not been modified during forwarding
- Considering both authentication and reputation in the scheme, we could achieve higher security level.

Elliptic curve cryptography

- Elliptic curve cryptography (ECC) is a public key cryptograph.
- A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.
- Due to the advantages such as shorter key length, low bandwidth requirements, faster processing speed, elliptic curve cryptograph is applied in the authentication process to ensure the illegitimate nodes out of aggressing.

Reputation-based scheme in OLSR

- A network is not secure enough if the node is only authenticated by using the encryption.
- A reputation-based scheme will make the reactive routing protocol work inefficient as it costs more time to establish the reputation status.
- With respect to proactive routing protocol, this problem seems not more emergent than in the reactive case.

Message Seq.No	MPR Seq.No	Link Type	Reserved	Link Message size	Reputation Status	Neighbour Address
----------------	------------	-----------	----------	-------------------	-------------------	-------------------	-------

Message Seq.No	MSSN	Hop Count	Reputation Status	Traffic Type	Originator Address	Reserved	MPR Selector Address
----------------	------	-----------	-------------------	--------------	--------------------	----------	----------------------	-------

- The HELLO and TC message packet format are extended to carry a reputation status for each neighbor.

The monitoring module

- By modifying the HELLO and TC message, each node is able to independently monitor the packet forwarding activities of its neighbor nodes.
- Firstly, we update the neighbor relationship establishment periodically so that only the nodes which have passed the authentication can become legal neighbors.
- Secondly, each node takes charge of monitoring its own neighboring nodes.
- Given the consideration that attacks like dropping or withholding message make message could not be received by the destination node on time, some messages maybe late, even dropped directly, we regard it as a misbehavior if a message does not get to the receiver within a predefined time interval.

Our proposed strategy

- In our scheme, the reputation level is represented by a value between 0 and 1 where 1 indicates the highest reputation level.
- In the beginning, after the authentication phase has passed, the reputation level for all nodes are assumed to be 1.
- The node reputation level will then decrease once misbehavior happened.
- In order to introduce fewer burdens on protocol overhead, we collect the reputation information directly by the extended HELLO message.
- Message Seq.No is the unique identity of the HELLO message.
- Each node maintains a reputation table for storing its one-hop neighborhood reputation information.

Reputation rating i

- A node can use the reputation level it established for other nodes to evaluate the security of the route to the destination.

- Reputation level: $REP_initial(A, B) = \frac{\# \text{forwarded}}{\# \text{sent}}$

$$REP(A, B) = \delta \times REP_{history}(A, B) + (1 - \delta) \times REP_{current}(A, B) \quad (0 < \delta < 1)$$

- The value $REP(A, B)$ is a weighted sum consisting of two parts. The first part describes the history reputation level, which already stored in node A's reputation table. The second part denotes the new reputation status of node B.

Reputation rating ii

- Usually, the reputation value more depends on the current value, so we set δ to be a small value.
- By considering the history and current reputation values, the evaluation will be consistent and seamless.
- The threshold of $REP(A,B)$ is also used to guarantee the trade-off between the security level and network performance.

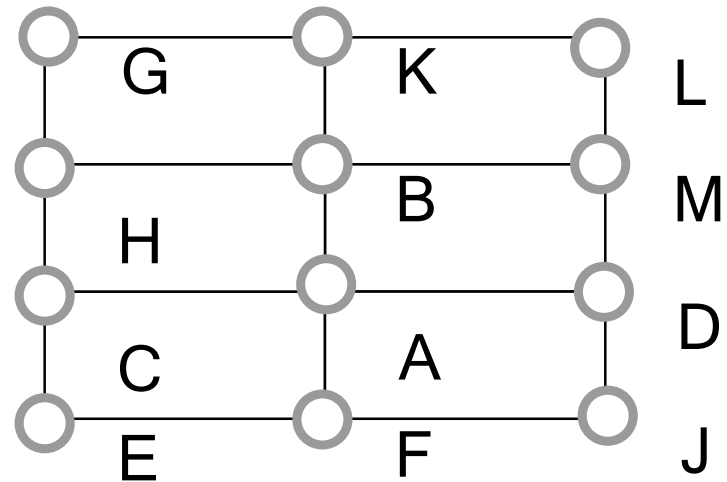
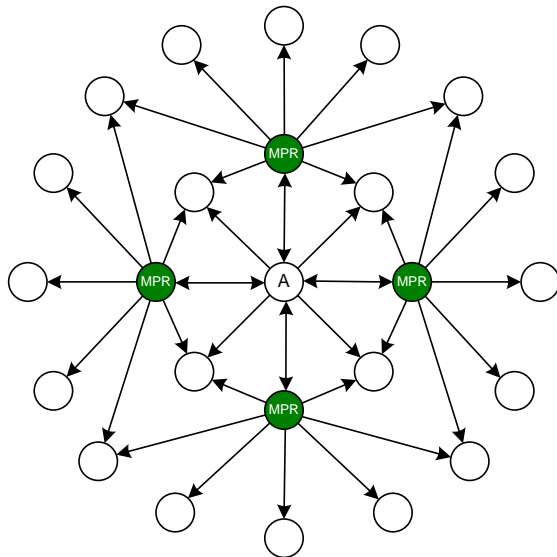
MPR selection based on reputation level

- We assumed that reputation value updates every 20 second, and the time interval of sending HELLO and TC message are respectively 2s and 5s.

T(s) \ Reputation	B	H	F	D
0	1	1	1	1
t_0	0.9	0.95	0.95	1
t_1	0.9	0.95	0.9	0.8
\vdots	\vdots	\vdots	\vdots	\vdots
t_k	0.55	0.8	0.7	0.75
\vdots	\vdots	\vdots	\vdots	\vdots

Reputation table of node A

- Since the TC message transmits the network topology information which is more important than the HELLO message, the reputation value will decrease more sharply when misbehavior is found in MPR node.
- The re-selection of MPR nodes could prevent the intruder managing to become an MPR to launch an attack, thus strengthening the security of MPR nodes.



Conclusion and future work

- We introduce a multi-fence security solution for optimized link state routing protocol, in which authentication and encryption are considered as the first level of defense, reputation-based trust management is as the second step of the scheme.
- This method achieves balance between security strength and network performance.
- Extend the method to other routing protocols.

*Thank you
for your attention*

...