

Secure Link State Routing for Mobile Ad Hoc Networks

Papadimitratos and Haas
Cornell University

Presented By:
Karthik Narayan

narayanc@cs.fsu.edu

1

Introduction

- MANET technology opens the network to many security attacks
- Protocols that already exist are reactive protocols
- But proactive discovery can be more efficient
e.g..low mobility or frequent communication

narayanc@cs.fsu.edu

2



Goals of the paper

- Protocol secures the discovery and distribution of link state information in a MANET.
- To provide factual information against Byzantine behavior.
- Link states have connectivity information like scanning for multiple routes and better propagation of control traffic.
- Protocol is similar to the one for wired networks.
- Does not rely on the requirements of the robust flooding protocol.

narayanc@cs.fsu.edu

3



Definition of SLSP

- Is responsible for securing the discovery and distribution of a link state information.
- Scope may vary from secure neighborhood discovery to a network wide secure link state protocol.
- The nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops.

narayanc@cs.fsu.edu

4

Assumptions and network model

- Each node is equipped with a public/private key pair (Ev/Dv) and a single network interface per node within the MANET domain.
- Key certification is done by K nodes using threshold cryptography.
- Nodes are identified by the IP addresses and may be used to derive public keys.
- Nodes are equipped with a hash function and a public key cryptosystem.

narayanc@cs.fsu.edu

5

Assumptions contd.

- Adversaries may disrupt the protocol by exhibiting arbitrary malicious behavior or exploit the protocol for DOS
- But SLSP is concerned with securing the topology discovery and does not guarantee that adversaries who helped route discovery would disrupt the activity.

narayanc@cs.fsu.edu

6

Overview of the protocol

- Protocol protects the link state update packets from malicious alterations as the travel.
- It disallows fabricated links, nodes from masquerading their peers and etc.
- To counter the absence of a central key management system, each node distributes its certified public key periodically to nodes within its zone.
- SLSP defines a secure neighbor discovery that binds node V to its MAC and IP address and allows all other nodes within range to identify V.

narayanc@cs.fsu.edu

7

Overview contd.

Nodes advertise the state of their incident links by broadcasting periodically signed link state updates (LSU)

LSLP restricts that these be propagated within the zone of origin of the node.

Receiving nodes validate the updates, suppress duplicates and relay previously unseen packets that have not propagated R hops.

narayanc@cs.fsu.edu

8

Neighbor discovery

Each node commits to its MAC and IP and sends a hello message with these to its neighbors.

Receiving nodes validate this and retain the information.

Binding the MAC disallows nodes from appearing as multiple ones at the DLL and assist against DOS attack.

To achieve this Neighbor Lookup protocol (NLP) is proposed to be an integral part of SLSP.

narayanc@cs.fsu.edu

9

Neighbor discovery contd.

NLP maintains a mapping of IP and MAC of its neighbors

Identifies potential discrepancies such as use of a multiple IP address.

Measures the rates at which control packets are received. This is provided to the routing protocol.

This way nodes trying to overload the network can be discarded.

narayanc@cs.fsu.edu

10

Discovery contd.

- NLP extracts and retains the 48 bit hardware source address for each received frame with the IP. (This requires a simple modification of the device driver).
- Each node updates its table by retaining both addresses. Mapping between DLL and network interface address are retained in the table as long as the transmission from the neighbor is overheard.
- A timeout is also associated with each neighbor.

Discovered....?

NLP issues a notification to SLSP according to the content of a received packet in the event that

- A neighbor used a new IP address
- Two neighbors used the same IP address
- A node used the same MAC as the receiving node.

On receiving such information the protocol discards the packet.

Link state updates

- Identified by the IP of the originator.
- To ensure that this is propagated within a range R each node selects a random number X and calculates a hash chain $X_i = H_i(X)$
- $I = 1 \dots r$. $H_0(X) = X$
- It places X_r and X_1 in the `zone_radius` and the `hops_traversed` fields.
- Finally a signature is appended.

narayanc@cs.fsu.edu

13

Updates contd.

- Each receiving node checks if it has the public key of the broadcasting node, compares the `zone_radius` and `hops_traveled` fields when lesser floods its neighbors.
- Waiting for the timeout and flooding ensure against malicious nodes that perform operations like packet dropping.
- Localized flooding keeps transmission and processing overhead low.

narayanc@cs.fsu.edu

14

Public key distribution

- Nodes use PKD packets or attach their certified keys to LSU packets. These are flooded throughout the zone.
- The LSU based key broadcasts provides for a timely acquisition and validation of routing to nodes that move into a new zone.
- The broadcasts are times according to the network conditions and device characteristics.
- Nodes validate PKD packets only if they don't have the originators public key. They can decide not to validate it for other reasons.

narayanc@cs.fsu.edu

15

Protection from clogging DOS attacks

To guarantee responsiveness nodes maintain a priority ranking of their neighbors according to the rate of queries observed.

Highest priority is assigned to nodes generating lowest number of requests.

Quanta is assigned to priorities and finally very low priority queries are discarded.

Selfish nodes are throttled back first by their neighbours and then by nodes farther away.

narayanc@cs.fsu.edu

16

DOS contd.

- Non malicious nodes will be affected only for a period equal to the time it takes to update the priority.
- Malicious flooding of spurious PKD packets are countered by several mechanisms
- NLP imposes a lost neighbor timeout
- PKD will not propagate farther than R hops.
- Nodes can autonomous decide if they want to authenticate a public key.
- The penalizing priority exists.

narayanc@cs.fsu.edu

17

Residual Vulnerability

SLSP remains vulnerable to colluding attackers

For example M1 and M2 may convince their zone of a non existent link.

However we should remember that they will be able to fabricate a link only between themselves.

narayanc@cs.fsu.edu

18

Questions



narayanc@cs.fsu.edu

19