Consideration on Monitoring Scheme to Secure Link State Routing against Byzantine Attacks

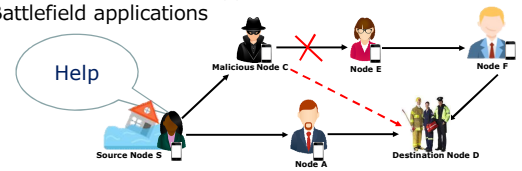
Babatunde Ojetunde D2†1, Naoki Shibata†1, Juntao Gao†1, Minoru Ito†1

†1 Nara Institute of Science and Technology

Background

Route Security: is essential in most applications where timely delivery of information is required.

- Disaster management applications,
- Battlefield applications



Routing protocols are still subjected **to attacks such as Byzantine attacks**, in which an attacker can:

- Interrupt route discovery
- Impersonate destination node
- Corrupt routing information
- Selectively or completely drop packets
- Inject fake packets into the network.

Existing schemes are too expensive for resource constrained networks.

Monitoring scheme is essential to secure the link state routing protocols against Byzantine attacks.

Our Approach

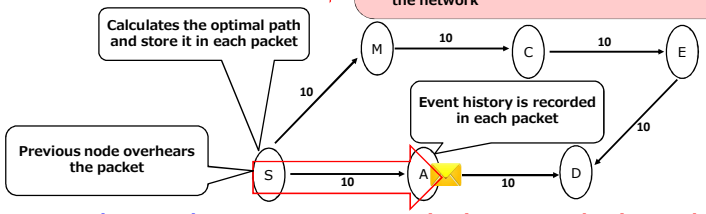
Secure Link State Routing: To secure packets route, we analyze the actions of each node within the network by monitoring intermediate nodes action on packets.

Our monitoring scheme adopts three main methods

a) Routing table formation
b) Monitoring scheme
c) Statistical hypothesis testing

Objectives

1. Secure packets route
2. Prevents Byzantine attacks
3. Guarantee communication among benign nodes
4. Detects malicious action of non-benign nodes in the network



- **Our scheme only guarantees communication among benign nodes**
  - Each node collects hello messages and digital signature from its neighbor
  - Neighboring nodes check if packets are forwarded correctly
  - Monitor nodes observe the packet dropping behavior of other nodes

Assumptions

1. All benign nodes are connected in the network topology.
2. All nodes have public and private keys
3. All links are not stable. i.e. Not all packets are received by the neighboring nodes.
4. All benign nodes know the link state of other benign nodes.
5. Change of probability for packet dropping is low.
6. A packet is dropped with probability q due to wireless channel fading during transmission between two benign nodes.

Proposed Method

By recording and checking the route information

- **Byzantine attacks are prevented**

a) Hello message verification

- Each node broadcasts its link quality to neighboring nodes periodically.
- This information is signed and cannot be forged

b) Monitoring Scheme

Previous node monitors the actions of intermediate nodes on each packet

- Previous nodes overhear forwarded packets
- Then checks if neighboring nodes are doing the right thing
  - By checking if packets are following the specified route
  - By checking if the delay is not too much

c) Statistical hypothesis testing

Monitor node confirms if a node is dropping packets intentionally

- Monitored nodes take the following steps

Assumes that the monitored node is benign
Sets significance level α to a predetermined value

⇩

Observes monitored node for N packets
Counts the number of dropped packets

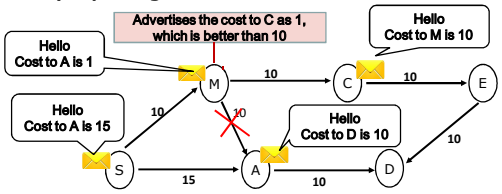
⇩

Calculates P value p

If $p \leq \alpha$, monitored node is detected as malicious
else monitored node is not malicious

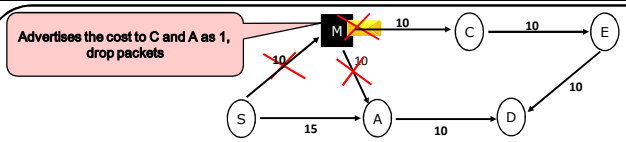
Prevention of Byzantine Attacks

1. **Corruption of Routing Table**
   - A malicious node reports false link quality
     - By reporting inconsistent information



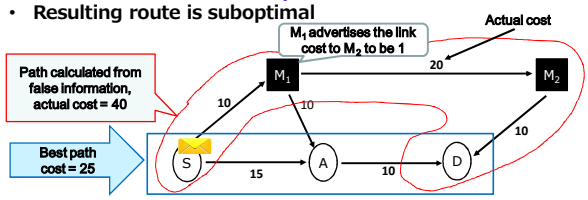
- When a node gets conflicting information
  - Compares all hello messages, digital signatures and timestamps collected
  - Exclude the link from its topology information
  - The worst link cost is used

2. **Packet Dropping**
   - A malicious node intentionally dropped packets
     - By injecting fake routing information to attract packets



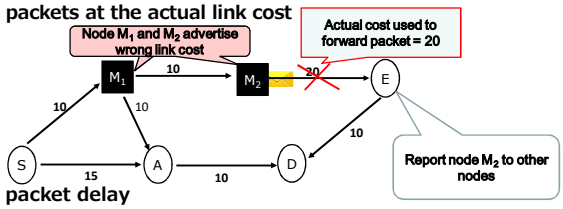
- Node S and A will not overhear the packet
  - After a predetermined time interval
  - Node M is detected as malicious by the statistical method
- Node M action is considered as malicious
  - The links between node S and A to node M is excluded

3. **Packet Tunneling**
   - A malicious node tunnels the packets to another malicious node
     - Resulting route is suboptimal



- Node S and A overhear the packet
  - Confirms if node M_2 is stored on the optimal path
    - By confirming the route history
- M_1 is detected as malicious
  - As M_2 is not on the optimal path
  - Node M_1 is reported to other nodes in the network

4. **Colluding Attack**
   - Node M_1 and M_2 collude to carry out malicious act
     - By reporting wrong link cost e.g. 1 and 2 respectively
     - Then forward packets at the actual link cost



- Node E detects packet delay
  - Checks the route history
  - Confirms the timestamp on the route history
- The link between node E and node M_2 is excluded

Simulation Metrics

We will evaluate our monitoring scheme from two perceptions

- Detection
  - Successful detection rate
  - False positive detection rate
- Performance
  - Packet delivery rate
  - Packet delay
  - Overheads