PERFORMANCE EVALUATION OF SECURE ROUTING FOR MOBILE AD HOC NETWORKS

Panos Papadimitratos and Zygmunt J. Haas
Cornell University

In open, collaborative and highly volatile networking environments, self-organizing infrastructures should be capable of operating in the presence of adversaries.

The secure discovery of the network topology is a prerequisite for safeguarding communication in a malicious setting.

In Mobile Ad hoc Networks (MANET), the routing protocol cannot be protected either by restricting the operation to fully trusted nodes or by employing intrusion detection mechanisms.

Our protocol relies solely on an end-to-end association between the two communicating nodes to secure the discovery of routes.

This works shows that:

- **The security enhancements introduced by our Secure Routing Protocol (SRP) have low cost**
- **SRP is efficient over a range of network instances**
- **SRP remains both effective and efficient when under attack**
- **SRP is capable of operating successfully even with a large number of adversaries actively disrupting its operation**

Methodology

Evaluate the operation of the **Secure Routing Protocol (SRP)** in both **benign** and **malicious** settings through detailed simulation.

Benign environment:
- Contrast the performance of SRP with a leading MANET reactive routing protocol, such as DSR, which does not take security into account.

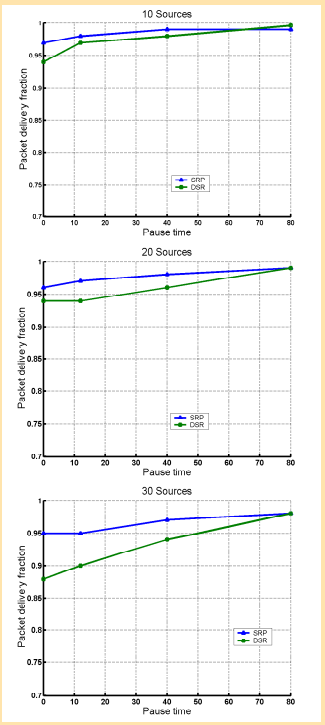
Malicious environment:
- Benchmark: Performance of SRP in the benign setting
- Implement attacks against against the route discovery
- Measure performance for different attack scenarios and numbers of adversaries.

Simulation Profile

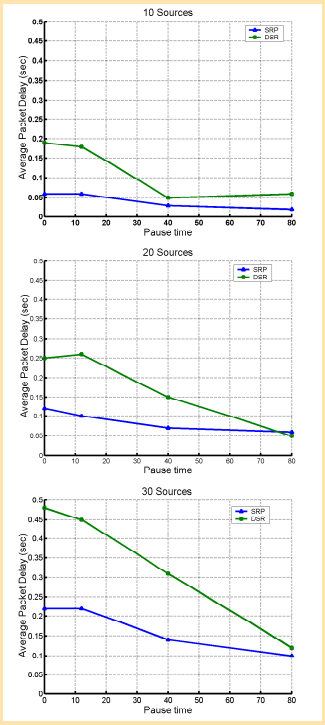
Nodes	50
Adversaries	5, 10, 15, 20, or 25 nodes
Measurements	10 random runs per benign setting, 15 random runs per malicious setting
Security Bindings	Single destination per source
Simulated time	120 sec
Mobility	Random waypoint; Pause times: 0, 12, 40, 80s
Load	10, 20, 30 CBR sources, Data payload: 64B 10 CBR sources in the malicious settings
Coverage Area	1500m-by-300m
PHY/MAC	802.11, DCF, 2Mbps, 250m
Tool	OPNET

Performance in a benign environment

- SRP performs weakly better than DSR
  - SRP & DSR deliver 95% of the data successfully
  - SRP achieves lower end-to-end data delivery delays than DSR for higher node mobility

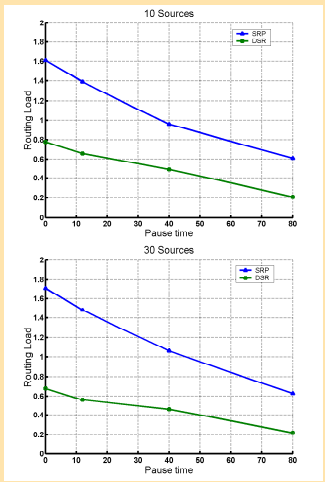


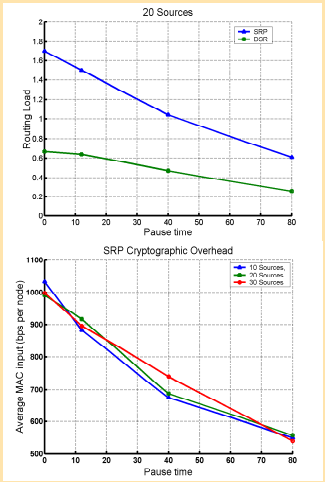
- **Packet Delivery Fraction**



- **End-to-End Packet Delay**

- SRP costs more than DSR
  - SRP has higher control traffic load than DSR
  - SRP requires cryptographic processing unlike DSR





- **Routing Load & Cryptographic Overhead**

PERFORMANCE EVALUATION OF SECURE ROUTING FOR MOBILE AD HOC NETWORKS

Panos Papadimitratos and Zygmunt J. Haas
Cornell University

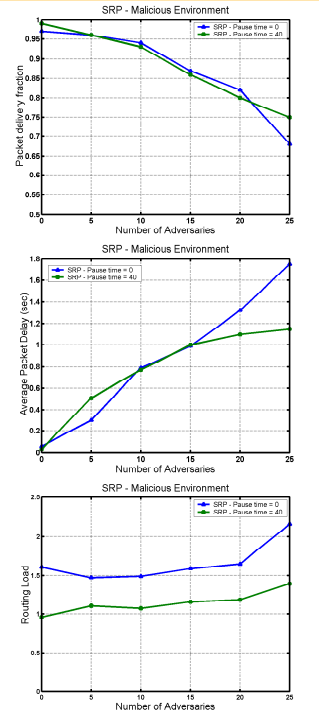
Performance in a malicious environment

• Attack Scenario 1: Corrupt the header of all route requests and re-broadcast
• Attack Scenario 2: Corrupt the accumulated route in all route request packets and re-broadcast. Forward corrupted replies to the querying node.

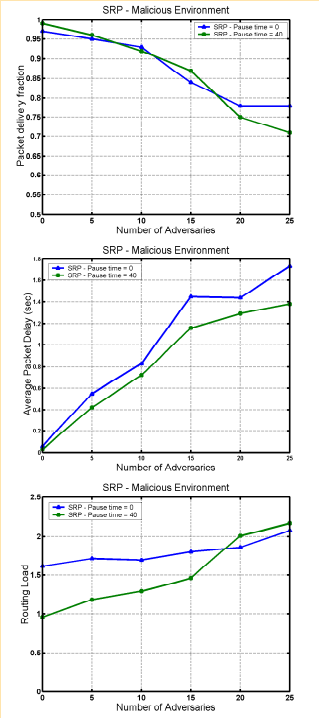
• SRP delivers a high percentage of data packets
  • More than 93% of the data packets are delivered when 20 % of the network nodes are malicious.
  • The rate of data loss increases slowly as the number of adversaries increases.

• SRP suffers from an increase in the end-to-end delay as the number of adversaries increases
  • In Scenario 2, a portion of the corrupted requests is replied by the destination.
  • In both scenarios, the propagation of corrupted route request packets forces intact request packets to be dropped as "previously seen."
  • Repeated route discoveries might be needed.
  • "Good," i.e., short and long-lived routes may not be discovered.

• SRP maintains routing low routing load
  • In Scenario 1, the routing load remains almost constant up to 40% of malicious nodes.
  • In Scenario 2, the routing load increases very slowly with the number of adversaries.



• **Attack Scenario 1**



• **Attack Scenario 2**

Conclusions

• SRP is efficient and effective
  •SRP delivers more than 95% of the data, with very low end-to-end delays and moderate increase in the routing load.

• SRP can be applied to resource-limited nodes
  • SRP imposes very limited processing overhead due to the cryptographic operations.

• SRP can operate successfully in the presence of adversaries
  • SRP delivers more than 93% of the data when 20% of the nodes are malicious and more than 70% of the data successfully even when half of the network nodes disrupt the route discovery.

• SRP relies solely on a single end-to-end security association per source-destination pair and does not make restrictive assumptions on the network membership and trust. It is capable of operating in an open, frequently changing, unknown network and provide factual, up-to-date, and authentic connectivity information.

• **SRP is a viable, practical protocol for secure discovery of routes over a broad range of MANET instances.**