

## Security Routing Protocol (SRP) for MANETs

A paper by P. Papadimitratos and Z. Haas

Stephen Carter  
April 2, 2002

## Quote of the day

"I feel sorry for people who don't drink. When they wake up in the morning, that's as good as they're going to feel all day. "

- Frank Sinatra

## Motivation

- Two problems typically not address by fixed network routing protocols
  - Lack of a fixed infrastructure
  - Frequent changes to network topology
- Most proposed ad-hoc routing schemes do not deal with security
  - AODV, WRP, DSR....

## MANET Routing Threats

- Malicious nodes could:
  - Corrupt in transit RR and cause data to be misrouted
  - Replay old routing information
  - Advertise incorrect routing information
- The nature of Ad-hoc networks magnifies the effects of such actions and makes malicious nodes very **hard to detect**

## SRP

- Guarantees that a node initiating route discovery will be able to *identify* and *discard* replies providing false topological information
- Guarantees acquisition of correct topological information in a timely manner

## SRC Proposed Scheme

- Assumptions
  - A security association (SA) between the source node S and the destination node T
  - The existence of a shared key Kst
  - End nodes able to use static (non-volatile) memory
  - Links are bi-directional

## SRC Proposed Scheme (cont)

- Route Request Packet (RRP)
  - Source node send route request packet to initiate route discovery
  - This packet is identified by two identifiers
    - Query sequence number
    - Random query identifier
  - Source, Destination, Identifiers, and Kst are input to the Message Authentication Code (MAC)
  - Identities of traversed intermediate nodes are accumulated in the RRP

## SRC Proposed Scheme (cont)

- Intermediate nodes job:
  - Relay route requests
  - Maintain limited state information so they can discard previously seen route requests
  - Provide feedback in the event of a path breakage

## SRC Proposed Scheme (cont)

- Destination node
  - Receives route request and constructs route reply
  - Calculates a MAC for the route reply
  - Returns the packet to the source *S* over the *reverse* of the route accumulated in the RRP
  - The querying node then validates the replies and updates it's topology view

## Observations

- Intermediate nodes may not reply to or tamper with RRP's (and get away with it). They do not possess the key *Kst* to generate a MAC
- The route reply MAC provides integrity protection for the route reply packets
- The *query identifiers* are used by intermediate nodes to check for replay attacks
- If a query identifier matches one used in the past, the intermediate node discards the query packet

## Observations (Cont)

- A replayed RRP could reach the end node depending on the limitation imposed by the size of the query identifier table on the intermediate nodes. In this case the end node would realize the *query sequence number* (qsn) matched an earlier qsn, and discard the packet.
- Query identifiers are unique and random therefore a malicious node could not fabricate queries (route requests) in an attempt to get intermediate nodes to discard legitimate route requests in the future.

The end