

Security Aware Ad-hoc Routing (SAR)

A paper by Yi, Naldurg, and Kravets

Introduction

- SAR is an approach to routing that incorporates ***security levels*** of nodes into traditional routing metrics.
- The goal of SAR is to characterize and explicitly represent the trust values and trust relationships associated with ad hoc nodes and use these values to make routing decisions (to ensure data is routed through a secure route).

Introduction (cont)

- The notion of an ***integrated security metric*** is introduced. This metric is a combination of security attributes and trust levels.
- Existing ad hoc algorithms may be augmented with this integrated metric to influence route discovery
- The route discovery mechanism will then find nodes that match particular security attributes and trust levels. Only nodes that provide the *required* level of security can generate or propagate route requests, updates, or replies.

Motivation

- High risk ad-hoc networks (Battlefield Scenario)
 - In these types of networks, finding a route with specific security attributes is generally more relevant than finding the shortest route between two nodes
 - Nodes (applications) must be able to specify the quality of protection or security attributes of their ad-hoc route with respect to metrics that are relevant to them
 - Example: A general's route discovery protocol could embed "rank" as a metric to establish a route that avoids privates (or any nodes of lower rank)

Protocol Description

- An *on-demand* base protocol is used such as DSR or AODV
- Security metric is embedded in the RREQ packet that changes the forwarding behavior of the protocol (with respect to RREQs)
- Intermediate nodes receive a RREQ packet with a particular security metric or trust level
- “SAR ensures that this node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level.”

Protocol Description (cont)

- If an end-to-end path with the required security attributes can be found, a RREP is sent from an intermediate node or the eventual destination

SAODV

- RREQ packets have an additional field called RQ_SEC_REQUIREMENT that indicates the required security level, for the route the sender wishes to discover
- When a node receives a RREQ packet, the protocol first checks to see if the node can satisfy the security requirement indicated
- If the node is secure enough to participate in routing, SAODV behaves as AODV and the RREQ is forwarded to its neighbors

SAODV (cont)

- When an intermediate node decides to forward a request, a new field in the RREQ called RQ_SEC_GUARANTEE is updated. This field indicates the *maximum* level of security afforded by the paths discovered.
- This can be useful for security aware applications to get more detailed information about the quality of security for the paths discovered.

SAODV (cont)

- To guarantee cooperation of nodes, the RREQ headers are encrypted
 - It is assumed that a group key distribution mechanism is already in place
 - Nodes that belong to the same level in the trust hierarchy should be able to decrypt and re-encrypt the headers when necessary

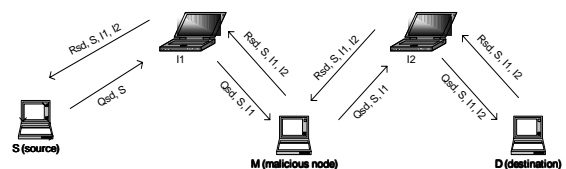
SAODV (cont)

- The arrival of a RREP packet at the destination indicates the presence of a path from the sender to the receiver, that satisfies the senders security requirement
- The destination node sends a RREP as in AODV but with the RQ_SEC_GUARANTEE added
- The RREP is also encrypted so that only nodes belonging to the particular trust level can process the packet
- When the RREP arrives at an intermediate node on the reverse path, intermediate nodes that are allowed to participate update their routing tables (as in AODV) and also record the RQ_SEC_GUARANTEE

Observations

- SAR is (in my opinion) the best secure routing protocol for tactical MANETs so far
- A combination of SAR and SRP may be ideal
- SAR may be vulnerable to the attack we discovered on SRP

Attack on SRP



*Qsd is the SRP header for a query searching for t and initiated by s

*I1 and I2 are not in range of each other, however both are in range of M (malicious node)