

Quote of the day

"If you drink, don't drive...
Don't even putt."

-Dean Martin

Bonus quote!

"Bigamy is having one wife too many.
Monogamy is the same."

- Oscar Wilde

1

Secure Position Aided Adhoc Routing (SPAAR)

Part 1

By: Stephen Carter

Outline

- Introduction and Terminology
- Motivation
- Secure routing & High risk environments
- SPAAR details

3

Introduction

- What is SPAAR?
 - SPAAR is a family of protocols designed to *secure ad hoc routing* for a *high-risk environment* that utilizes position information to improve performance & security.

4

Terminology

- **Outsider attacks:** Attacks by unknown malicious nodes
- **Insider attacks:** Attacks by authorized nodes on the network that have been compromised. (much harder to detect)
- **SPAAR's goal:** Prevent outsider attacks, minimize potential for damage by insider attacks

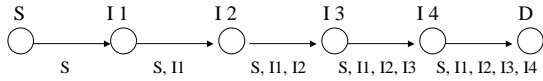
5

Motivation for SPAAR

- Most ad hoc routing protocols are not secure (unencrypted routing messages)
- A few claim to be secure, but do not satisfy the security requirements desired for a high-risk MANET (SRP, I.N. attack)
- SRP Attack, Wormhole Attack

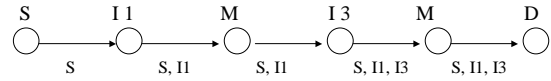
6

SRP Attack



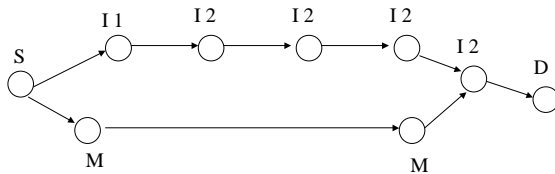
7

SRP Attack (cont)



8

Wormhole Attack



9

Motivation for SPAAR (cont)

- The use of position information in routing protocols can greatly reduce overhead of the route discovery process
- Current position aided routing protocols are very insecure (maybe the most insecure of all) because they pass location information in the clear

10

What is a secure routing protocol?

- A routing protocol may be considered “secure” if it meets the *security requirements* of the environment it was designed for.

11

What is a secure routing protocol? (cont)

1. Fabricated routing messages cannot be injected into network
2. Routing messages cannot be altered in transit, except for those changes that must be made according to the normal functionality of the routing protocol
3. Routing loops cannot be formed through malicious action
4. Routes cannot be redirected from the shortest path by malicious action

12

What is a high-risk environment?

- Security is a major concern, possibly the primary concern
- Malicious nodes expected
- Risk of node capture or destruction (compromised nodes)
- Example: Military environments, tactical ad hoc networks, battlefield scenario

13

What is a high-risk environment? (cont)

- Extra requirements for secure routing protocols in a high-risk environment:
 5. Unauthorized nodes should be excluded from route computation and discovery
 6. Network topology must not be exposed neither to adversaries nor to unauthorized nodes by the routing messages

14

SPAAR Details

- Hop by hop cryptography is used, therefore the protocol is expensive and should only be used in environments that require the highest level of security
- Security associations exist between a node and its neighbors (neighbor group)
- Important parts of SPAAR:
 - The Neighbor Table
 - The Destination Table
 - The Route discovery process
 - Route Maintenance

15

SPAAR Neighbor Table

- Nodes maintain a neighbor table containing:
 - Neighbor ID
 - Neighbor's Public Key
 - Neighbor's Group Decryption key
 - Most Recent Location
 - Transmission Range
 - Table Update Sequence Number
- A node will not accept routing packets unless they are from a registered neighbor (neighbor in the neighbor table)

16

SPAAR Route Discovery

- Source node S broadcasts an *encrypted* RREQ containing
 - RREQ sequence number
 - Destination ID
 - S's distance to destination D
 - D's position coordinates with a TUSN
- Upon receiving a RREQ, an intermediate node
 - Decrypts the RREQ with the appropriate decryption key
 - Determines if it *or any of its neighbors* are closer than the node it received the RREQ from (checks timestamp/seq #)
 - If not, it discards the RREQ. If so, encrypts and forwards
- This process is repeated until the RREQ reaches the destination (the node with the destination in its neighbor table)

17

SPAAR Route Discovery (cont)

- Destination D constructs, signs, and encrypts a RREP containing
 - RREQ sequence number
 - D's position coordinates and a new TUSN
 - D's velocity
- The RREP propagates back to the source along the reverse path in the same manner as it did toward the destination (hop-by-hop cryptography)
- Assuming a path existed, the source receives RREP with the destination's new position and velocity (and a new TUSN)

18

Coming in Part 2

- Details of how SPAAR securely maintains neighbor table
- Key management details
- Other stuff...