

Current state of secure routing for mobile ad hoc networks

Patroklos Argyroudis
argp@cs.tcd.ie

Networks and Telecommunications Research Group
Department of Computer Science
University of Dublin, Trinity College

Outline

- Introduction, the need for secure routing
- Security problems with existing ad hoc routing protocols
- Security requirements for ad hoc routing protocols
- Proposed solutions

Introduction

- Challenges (not present in wired networks):
 - No centrally administered secure routers
 - No strict security policies
 - Highly dynamic nature of mobile ad hoc networks
 - Current ad hoc routing protocols trust all participating nodes

Problem

- Secure ad hoc routing protocols are difficult to design:
 - Existing protocols are optimised to spread routing information quickly as the network changes
 - Security mechanisms consume resources and can delay or even prevent successful exchanges of routing information

Security problems with existing ad hoc routing protocols

- Attacks against ad hoc routing protocols can be active or passive
- A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic
- An active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes

Specific attacks

- Location disclosure: reveals information regarding the location of nodes, or the structure of the network
- Black hole: an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it
- Replay attack: an attacker sends old advertisements to a node causing it to update its routing table with stale routes
- Wormhole: an attacker records packets at one location in the network, and tunnels them to another location, routing can be disrupted when only routing control messages are tunneled

Security requirements for ad hoc routing protocols

- Certain discovery: if a route between two nodes exists it should always be found
- Isolation: misbehaving nodes should be identified and isolated from routing
- Location privacy: protect information about node location and network structure
- Self-stabilisation: the routing protocol should be able to recover from any problem without human intervention
- Byzantine robustness: should be able to function properly even if some participating nodes are disrupting its operation
- Lightweight computations

Proposed solutions: IPsec

- Many ad hoc routing protocol specifications suggest IPsec, however:
 - It is too complex
 - Not designed concurrently with the basic protocol, thus may leave unpredictable and undetectable vulnerabilities in the system
 - Produces additional configuration overhead

Proposed solutions: TIARA

- TIARA (Techniques for intrusion resistant ad hoc routing protocols): a set of design techniques mainly against denial-of-service attacks
 - Multi path routing: discover and maintain all routes for data flow
 - Each node has a policy that defines the list of authorised flows that can be forwarded by the node
 - Sequence numbers: provide a countermeasure for replay attacks
 - Fast authentication instead of IPsec, but no guidelines on how to realise it

Proposed solutions: SAR

- SAR (Secure aware ad hoc routing):
 - Introduces a negotiable metric to discover secure routes
 - Security properties like time stamp, sequence number, authentication, integrity, etc. have a cost and performance penalty, thus affect the secure route discovery
 - The security metric is embedded into RREQ packets
 - A RREQ can be processed or forwarded only if the node can provide the required security (or has the required authorisation)

Proposed solutions: ARAN

- ARAN (Authenticated routing for ad hoc networks):
 - Requires a trusted certification authority
 - Every node that forwards a RREQ or a RREP must also sign it (in addition to heavyweight computations, the size of the routing messages increases at each hop)
 - Prone to replay attacks if the nodes do not have time synchronisation (difficult to achieve, especially in an ad hoc environment)

Proposed solutions: SRP

- SRP (Secure routing protocol for mobile ad hoc networks):
 - Can be applied to existing protocols, like DSR
 - Requires that for every route discovery the source and the destination to have a SA between them
 - Does not mention route error messages, thus any node can forge error messages with other nodes as source

Other proposed solutions

- SEAD (Secure efficient distance vector routing for mobile ad hoc networks): employs hash chains to authenticate hop counts and sequence numbers
- Ariadne: same operational principles as SEAD, but based on DSR
- Both require clock synchronisation between the participating nodes which is an unrealistic requirement for ad hoc environments

Summary

- If there is no security in the routing protocol active attackers can easily exploit, even completely disable, an ad hoc network
- Current ad hoc routing protocols are completely insecure
- Existing secure routing mechanisms are either too expensive or have unrealistic requirements
- It is difficult to find a general idea that can provide security against all kinds of attacks