Security

→ Routing attacks

Modification: malicious nodes announces better routes than the other nodes in order to be inserted in the network.

(change route seq. number, hop count)

DOS attacks with modified routes and changes packet headers so it doesn't reach destination

Impersionation: Usurpation of the identification of another node to perform changes.

Spoofing MAC addresses, creating loops and leaving nodes unreachable.

Fabrication: generates false traffic to disturb network (false route messages, corrupting route state, routing table overflow, replay attack, black hole attack (0 metric route).

Key management

-> Symmetric cipher

- ✓ fast and secure
- ✓ longer keys -> longer security
- × requires the share of secret key
- × complex administration

-> Asymetric cipher (PKE)

- ✓ no need to share keys
- ✓ scalable and versitle
- × computationally intensive
- × certificate authority
- × confidential private keys

-> Key management in ad-hoc networks

Vulnerable mobile nodes.

Mobility induced unstable network topology

NO infrastructure to send key info to nodes.

→ Self-organized public key management (SOPKM)

Users issue certificates based on personal acquaintance (certificates stored and distributed by users themselves)

Has a repository for updated and expired certs.

Public keys and public-key certs:

If a user u believes that a given public key k_v belongs to a user v, then u can issue a public-key certificate in which k_v is bound to v with the signature of u. (and validity)

Each certificate is stored at least twice: by the issuer and the user.

Updating repositories:

Exchanging certificates between nodes, where each node multicasts its certificate graphs to it's physical neighbours (hash of ids).

Users share public keys when they meet.

A user who wants to find the public key of other has to find the chain of valid public key certificates leading to that user.

Revocation

Certificates can be explicitly revoked or implicity (expiration)

Malicious users

Certificate exchange mechanisms allows nodes to virtually gather all certificates

They cross-check the user-key bindings in the certificats to detect inconsistencies.

→ Self-securing ad-hoc wireless networks (SSAWN)

Achieve high security scenario.

High access ratio

Efficient communication

localized trust model : an entity is trusted if any k trusted entities claim so within a time period. (usually among 1-hop neighbors).

shared secrets: use of RSA. Use of Public key and Global Secret key (SK).

SN is used to sign certificats for all nodes and can be verified by the well-known public key.

Each node has a part of the secret.

- By collecting k partiall certificates, combines them together to generate the full new certificate
- Nodes without valid certificates are denied from acces to the network.

Reputation appraaches

Explore reliability of each node:

- how node handles packet forwarding
- level of trust
- reputation information exchanged periodically among neighbours

Routing and comms through high rep. nodes.

Protect network traffic from misbehaving nodes and minimize interaction.

There are friendly, selfish and bad nodes.

→ Reputation

Combination of first-hand reputation (neighbours) and second-hand reputation (info from neighbours).

Probability of well-transmitted packets.

Deviation test to detect false reports.

- Trust value : α

T = trustworth

NT = non-trustworthy

$$\alpha = \frac{T}{T+N}$$

- Merge first and second-hand reputation:

Reputation of node B seen by A is the first-hand rep plus the trust factor of second-hand rep of B seen by C (and others second-hand reps).

$$R_{AB} = F_{AB} + \alpha F_{CB}$$

- normal operation of network

. Choice of nodes to form a path uses the reputation of nodes

- Choice of nodes to join certificate graph user reputation. (+)

- Choice of nodes to get the very pairs or very pairs user reputation (+).

- Reputation of nodes can change over time.