Motivation: Security in Mobile Ad Hoc Networks

Ad hoc networks
- mobile terminals (can be captured or compromised)
- wireless communications (passive eavesdropping and active interfering)
- no centralized management point (cooperation)

Problem: Key/User Authentication

How can a user $u$ obtain a valid public key of another user $v$ in the presence of an active attacker?

Existing solutions:
- Decentralized certificate authority to a subset of nodes
  Drawbacks:
  - Scalability
  - Availability
  - Central authority needs to be trusted by all the users
- Decentralized certificate authority to all the nodes
  Drawbacks:
  - The “Sybil” attack
  - Collusion
  - Scalability

Proposed approach: Self-Organized Public-Key Management

- public key cryptography/certificates
- users generate their keys and issue certificates
- no central certification authority
- no central certificate directories
- no specific role assigned to a subset of nodes
- no preinstalled keys/procedures

The inspiration for this approach comes from the PGP (Pretty Good Privacy)

Applications:
- Fully self-organized mobile ad hoc networks
- Mobile networks without permanent connectivity
- Distributed P2P systems (e.g., Gnutella)

Model

If a user $u$ believes that a given public key belongs to a user $v$, then $u$ can issue a public key certificate to $v$.

Certificate graph $G(V,E)$
- $V$ is a set of keys
- $E$ is the set of edges, where a directed edge $(K_u,K_v)$ is added if $u$ signed a public key certificate $(v,K_v)$ to user $v$.

Authentication via a chain of certificates

Self-Organized Public-Key Management

INITIALIZATION: users construct their local certificate repositories (store a subset of certificates)

USAGE: when a user $u$ wants to verify a public key of another user $v$, two users merge their local repositories and try to find paths of certificates between them in their merged certificate repositories

Example of a local repository algorithm: Maximum Degree

Nodes build their local repositories by choosing certificates that lead to the vertices with the highest degrees.

Performance evaluation:

(Maximum Degree on PGP certificate graph)

- Avg. shortest path in the merged repositories $= 8$
- Avg. shortest path in the PGP graph $= 6$

PGP certificate graph

PGP graph is the only known example of the self-organized certificate graph creation.

Conclusions

- We proposed a self-organized public-key management for mobile ad hoc networks.
- We showed that the PGP certificate graphs do exhibit small world phenomenon
- We proposed a model for the construction of PGP-like small world certificate graphs

Future work

- Coping with misbehavior of users
- Key revocation
- Analyzing the creation of trust between users
- Improvement of the certificate graph model