A Scalable Public Key Management Scheme in Wireless Ad Hoc Networks for Mission-critical Applications*

Wenbo He, Ying Huang, Klara Nahrstedt, Whay C. Lee (Motorola)

Attributes of Secure Communication:
Confidentiality, authentication, integrity, non-repudiation, and security service availability

Challenges:
1. Vulnerability to Sybil Attack;
2. Unreliable Communications and Network Dynamics;
3. Large Scale;

What we need:
Scalable self-contained key management scheme

Secure Communication Protocol:
- Node ID indicates key combination
The private key combination pattern is unambiguously associated with the node.

![Diagram of Secure Communication Protocol]

- Encryption
Assuming destination is \( j \), then sender truncates message \( M \) into \( m \) pieces. Then the encryption is as follows:
\[
S_1 = E(publicKey_{j1}, M(1))
\]
\[
S_2 = E(publicKey_{j2}, M(2) \oplus M(1))
\]
\[
\vdots
\]
\[
S_m = E(publicKey_{jm}, M(m) \oplus M(m-1))
\]

- Decryption
\[
M_1 = D(privateKey_{j1}, S_1)
\]
\[
M_2 = D(privateKey_{j2}, S_2) \oplus M_1
\]
\[
\vdots
\]
\[
M_m = D(privateKey_{jm}, S_m) \oplus M_{m-1}
\]

Then receiver node \( j \) restores the message \( M \) by assembling \( M_1 + M_2 + ... + M_m \).

Key Allocation:
Isometric allocation of keys outperforms non-isometric allocation, where in an isometric key allocation, all nodes are assigned the same number of private keys.

Evaluation:
1. Small memory footprint
2. Almost zero communication overhead for authentication.
3. Resilience to break-ins (benchmark resilience)

Advantage:
1. This scheme uses self-contained key management scheme, which is able to prevent Sybil attack.
2. No communication overhead for authentication. The communication overhead is introduced only in the key maintenance process.
3. Small memory usage to store keys at each node.
4. The scheme offers good resilience of the whole network, since failure of any node does not affect the whole network.
5. We generalize the traditional public key management schemes, where each person holds only one private key.

Trade-off:
Trade computational power for computational efficiency and storage efficiency. (Battery can be charged periodically in mission-critical applications, where power is not a big issue.)

Locks: A, B, C, D, E are available to all users

Keys: a, b, c, d, e

Model:

![Diagram of Key Allocation]

* This work is supported by Motorola

http://cairo.cs.uiuc.edu