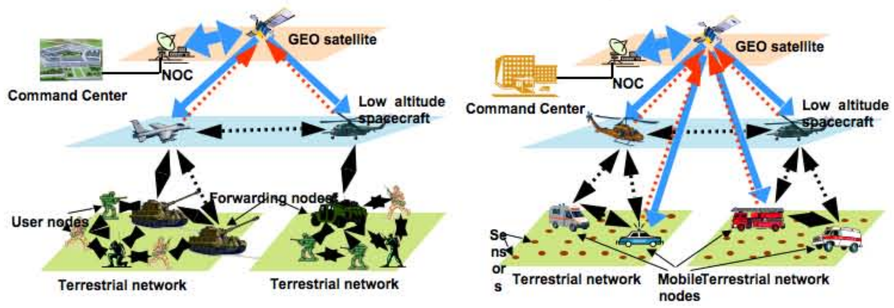
A Lightweight Certificate-based Authentication Protocol for Hybrid Networks

Ayan Roy-Chowdhury and John S. Baras

The Problem

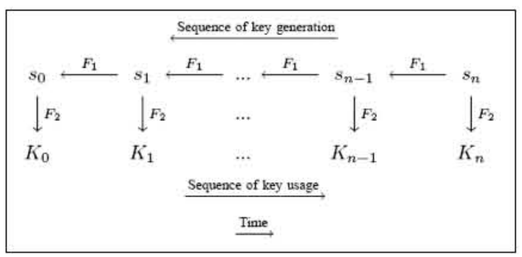


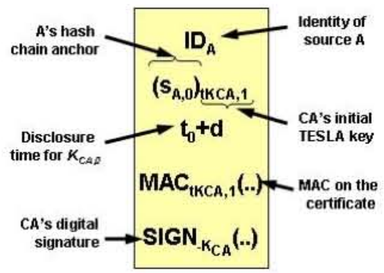
Source and message authentication for group communication in hybrid wireless/satellite networks:

- Necessary to prevent attacks on routing and application data.
- *Enabling* communication critical, especially for military battlefields, disaster relief.
- Pre-shared keys not scalable for groups.
- Traditional: public key-based digital signatures. But heavy computing load on nodes. Can drain energy of mobile users.

Proposed Solution

- Use key chains with TESLA certificates.
- Symmetric MACs authenticate messages; delayed disclosure of the MAC keys achieve asymmetry required in group communication.
- Satellite as the CA and proxy for group senders in disclosing keys.





The Protocol

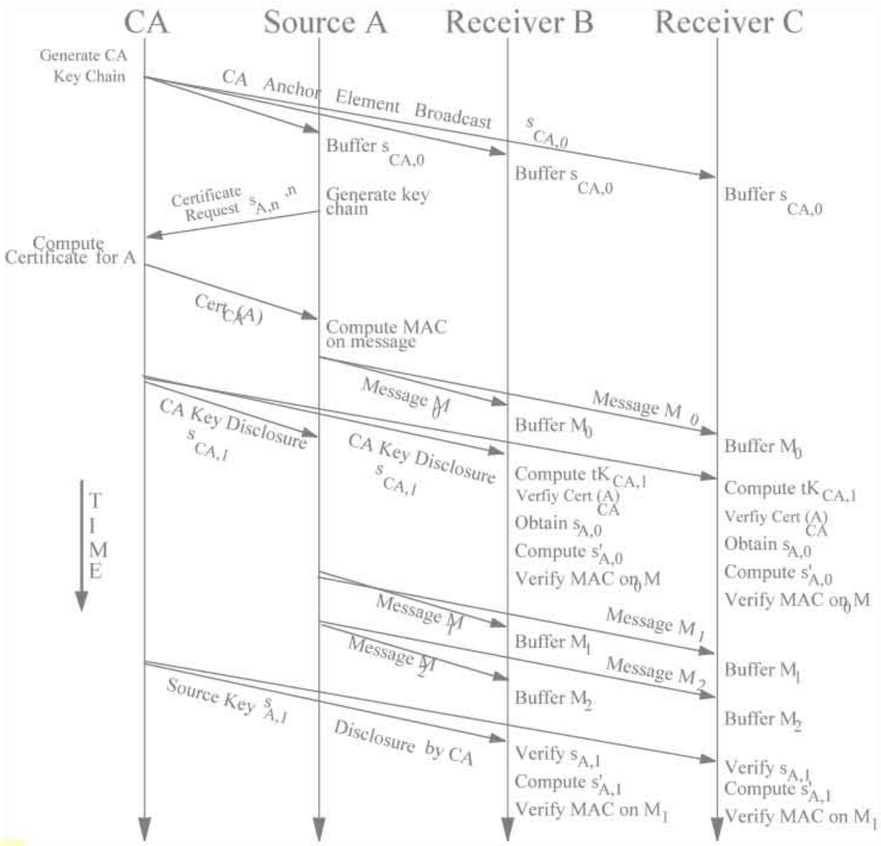
- CA generates TESLA certificate for each sender.
- CA's key commitment broadcast during setup.
- Sender attaches MACs to messages; MAC keys are from chain.
- Receivers check MAC validity – {is key still undisclosed? buffer message : discard message}.
- CA broadcasts own key element to "unlock" sender's key commitment.
- Subsequent keys from sender's chain broadcast by CA.

Feature Highlights

- Takes advantage of infrastructure present in network.
- Long certificate lifetime.
- Assumes no *a priori* secrets.
- Requires time sync with the satellite.
- Delegates most responsibilities to the node with most resources.
- Proxy disclosure helps faster key dissemination.
- Unaffected by node mobility.
- Bounded delay.

TESLA Certificate

- Binds key chain commitment of source to its identity.
- Specifies validity interval.
- Authenticated by CA's own key chain element.
- Sender requires one certificate for entire session.



Analysis

- Secure against active attacks: $O(2^k)$ complexity where $k \sim 160$ bits
- Protocol correctness proven by Strand Space analysis.
- Users perform exactly one signature verification, rest are MACs.
- ~49 times faster compared to RSA signatures per 512 byte message.