

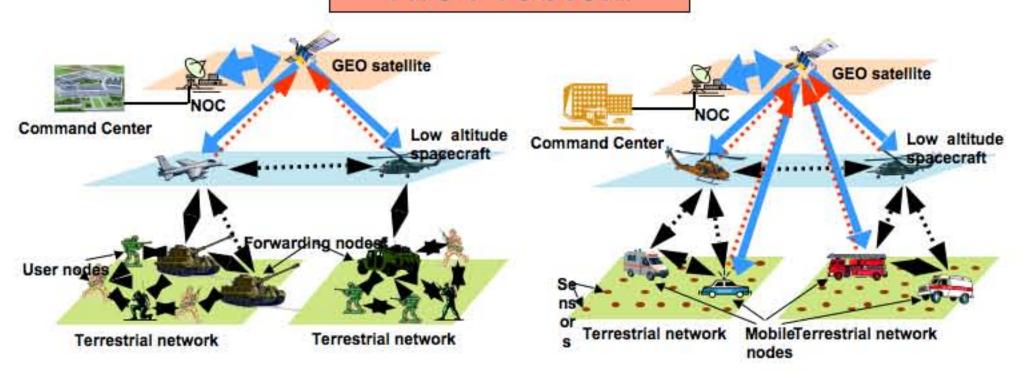
# The Institute for

# A Lightweight Certificate-based tems Authentication Protocol for Hybrid Networks Research



Ayan Roy-Chowdhury and John S. Baras

#### The Problem

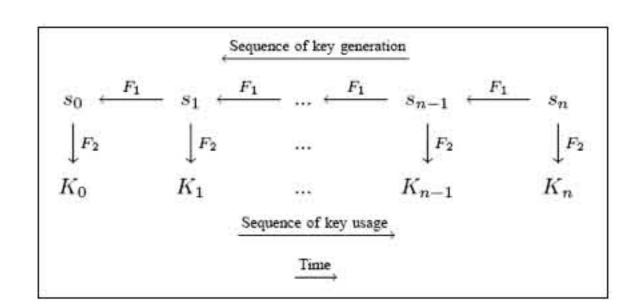


Source and message authentication for group communication in hybrid wireless/satellite networks:

- Necessary to prevent attacks on routing and application data.
- Enabling communication critical, especially for military battlef elds, 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.



# chain anchor (SA,O)IKCA,1 to+d time for Kcas MAC<sub>tKCA.1</sub>(..) MAC on the certificate -SIGN\_KCA(..)

#### **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.

#### 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.

#### Source A Receiver B Receiver C Generate CA CA Anchor Element Broadcast Key Chain Buffer s Buffer s Buffer s Generate key Compute Certificate for A Compute MAC on message Key Disclosure Buffer Mo CA Key Disclosure Buffer Mo Compute tK<sub>CA,1</sub> Compute tK<sub>CA.1</sub> Verfiy Cert (A) Verfiy Cert (A) Obtain sA 0 Obtain s<sub>A 0</sub> Compute s'A.0 Compute s'A.0 Verify MAC on M Verify MAC on M Buffer M Buffer M Source Key SA,1 Buffer M2 Buffer M Disclosure by CA Verify s<sub>A,1</sub> Verify s<sub>A,I</sub> Compute s<sub>A,I</sub> Compute s'A,1 Verify MAC on M<sub>1</sub> Verify MAC on M1

## 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.

### Analysis

- Secure against active attacks:  $O(2^k)$ complexity where  $k^2$  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.