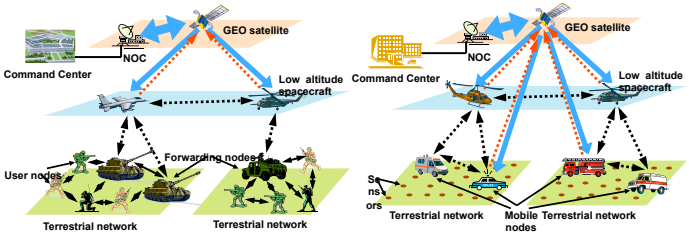
A Lightweight Certificate-based Source Authentication Protocol for Hybrid Networks

Ayan Roy-Chowdhury and John S. Baras

The Institute for Systems Research

University of Maryland

The Problem

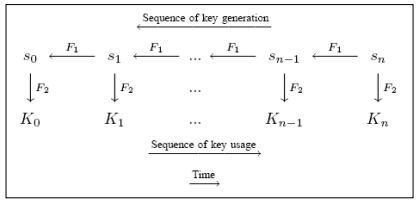


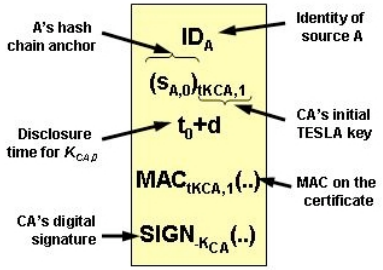
Source authentication and message integrity for group communication in hybrid satellite/wireless networks:

- Necessary for correct information dissemination in hostile environments (military battlefields, disaster relief).
- Pre-shared keys not scalable for large groups.
- Traditional public key-based digital signatures: heavy computing load on nodes; rapidly drain energy of mobile users.

Proposed Solution

- Broadcast authentication with key chains anchored by *extended TESLA certificates*.
- Certificate Authority used to certify identity of source.
- Symmetric MACs authenticate messages; *delayed disclosure of the MAC keys achieve asymmetry* required in group communication.
- Authentication protocol uses hybrid infrastructure:
  - ➢ satellite is the CA and proxy node for group senders in disclosing keys
  - ➢ satellite node also used to design a probabilistic non-repudiation mechanism.





The Authentication 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.

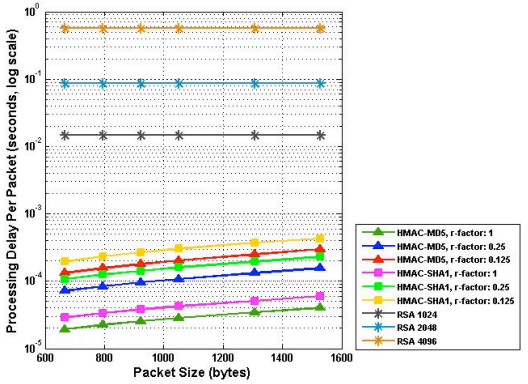
Probabilistic Non-repudiation

- Anchor elements of *n* key chains in each TESLA certificate for source.
- Source includes *n* MACs with each message.
- At key disclosure time, CA broadcasts only one MAC key, randomly selected from *n* available.
- Receiver accepts if key verifies one of *n* MACs.
- Non-repudiation at later instant in time:
  - ➢ CA discloses one of *n-1 previously undisclosed* MAC keys.
  - ➢ Probability of a key being disclosed by CA: *r-factor = 1/n*
  - ➢ Maximum number of successful non-repudiations for well-behaved source is *n-1*.

Extended TESLA Certificate

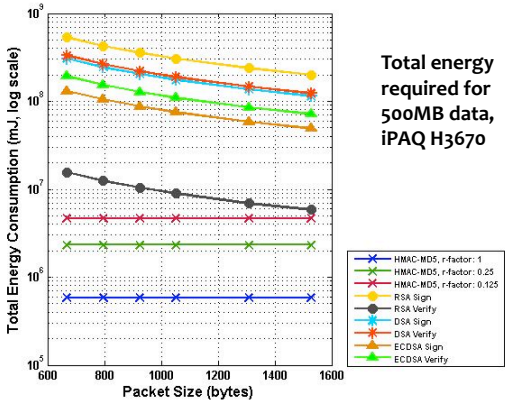
- Authenticates anchor element of source's MAC key chain.
- Specifies validity interval.
- Authenticated by CA's own key chain element.
- Sender requires one certificate for entire session.

Processing Delay Comparison Per Packet



500MB data, PIII 500MHz, 1 processor clock tick per operation

Energy Requirement Comparison



Total energy required for 500MB data, iPAQ H3670

Further information: University of Maryland Invention Disclosure IS-2008-135, Office of Technology Commercialization, University of Maryland College Park.