Multi-Cast Key Management Protocols
Design, Specification, and Analysis

Christopher A. Wood

February 3, 2012

Agenda

1. Project goal
2. Review group key management problem
3. Protocol design limiting constraints
4. Viral protocol design and performance
5. ARK protocol design performance

Project Goal

Develop a practical method to support tactical group key establishment

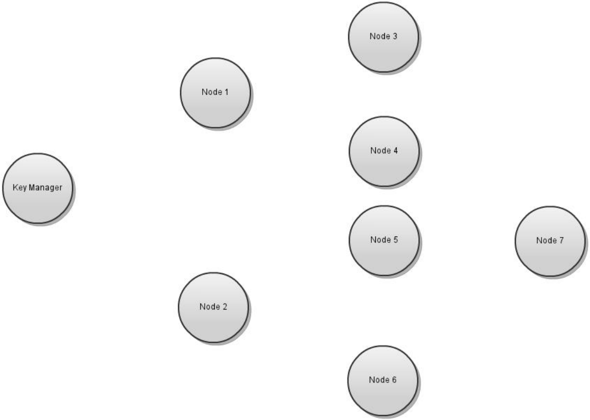
Group Key Management Problem

- Existing PKI based EKE and Authentication methods are inherently PtP protocols
- Previously proposed solutions to group and multi-case applications are limited
  - Most require the presence of a trusted server or network manager
  - PtP transactions can require up to 9 symmetric exchanges
  - Non-PtP based methods involve a great deal of pre-placed information
- Need to be secure against common attacks (e.g. Man in the Middle)

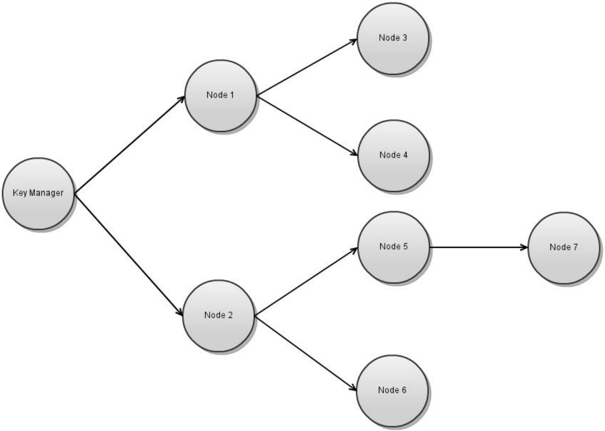
Group Key Management Problem

- Lack of pre-placed information calls for solutions with strong PKI-based Electronic Key Exchange (EKE) mechanisms
- EKE techniques suffer from the need for large key sizes
- Standardized EKE mechanisms are traditionally sequential for SA establishment among peers
- A complete EKE capability is required to enable widespread adoption by the military customer

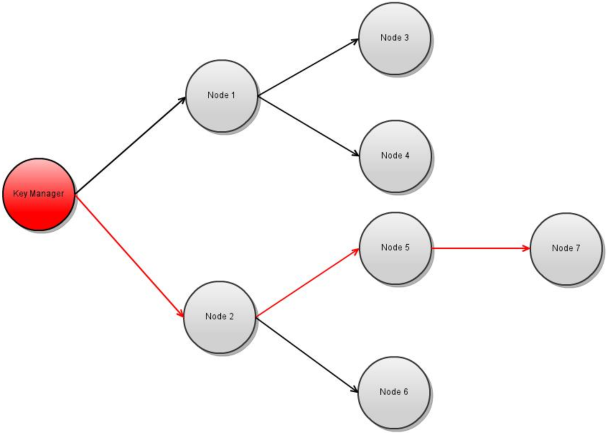
Multi-Cast Key Management



Multi-Cast Key Management



Multi-Cast Key Management



Design Constraints

1. Wireless channel is bandwidth constrained
2. Radio units are somewhat computationally constraintED
3. Limitations on shared secret and pre-placed information
4. Group membership can consist of the entire battlefield
5. Adding group members is easy, removing them requires full network rekey

Proposed Solutions

Two different protocols for targeting different deployment settings (wideband/multiband and narrowband channels)

1. Viral EKE Protocol
2. ARK EKE Protocol

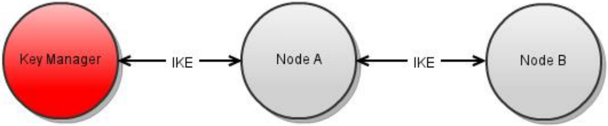
Viral EKE Protocol - Design Principles

- Re-key events are triggered from a single key manager, but the work is partially offloaded to the rest of the group
    - Key manager role is propogated throughout the members of the group to form pariwise security associations (SAs) that are then used to distribute the session key
    - Pairwise SA establishment can be done in parallel with members throughout the group
- Parallel implementation of the standardized Internel Key Exchange (IKE) protocol for ad-hoc group re-keys
    - Allows overhead of each exchange to be distributed among all members of the group
- Closely tied to the underlying data-link layer spanning tree orientation of groups to perform key distribution
- Support for an AUL to determine valid nodes is being integrated into the scheme

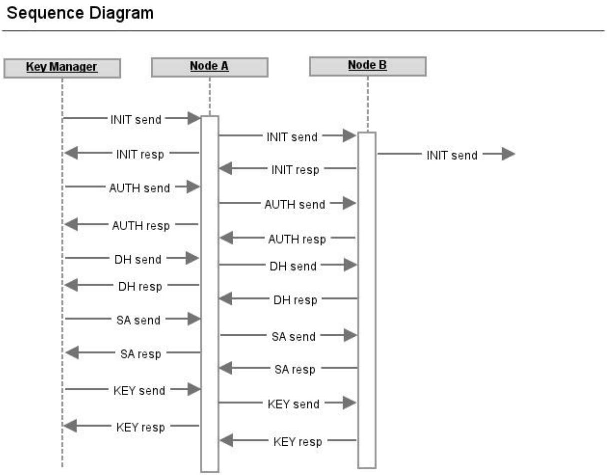
Viral EKE Protocol - Targets

- Targeted towards wideband and multiband networks
    - AN/PRC-117G, 30 Mhz - 2 Ghz RF channel bandwidth
    - SATCOM, Wideband (WB)
    - Data rates
        - On-air rates up to 10 Mbps

Viral EKE Protocol - Exchange Paths



Viral EKE Protocol - Exchange Paths



Sequence Diagram

Key Manager

Node A

Node B

INIT send

INIT send

INIT resp

INIT send

INIT resp

AUTH send

AUTH send

AUTH resp

AUTH resp

DH send

DH send

DH resp

DH resp

SA send

SA send

SA resp

SA resp

KEY send

KEY send

KEY resp

KEY resp

Viral EKE Protocol - Performance Review

- The group re-key time grows logarithmically with the number of allowed children in the transaction spanning tree
- Balanced spanning tree orientations with limited children nodes result in highest performance benchmarks

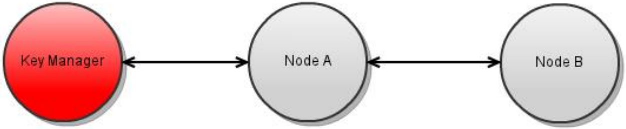
ARK EKE Protocol - Design Principles

- Automatic group key management with utilization of a one-way cryptosystem for key exchanges over the air
  - An asymmetric cipher is used with both the encryption and decryption key kept secret
  - This creates three kinds of users in the group
    - Sender - A member who can only encrypt messages
    - Receiver - A member who can only decrypt messages
    - Intruder - A member who possesses neither the encryption or decryption key and cannot encrypt or decrypt any messages.
- Encryption and decryption keys are stored as pre-placed information before the start of a mission
- Further pre-placed information (e.g. user authentication lists) can be added for additional security

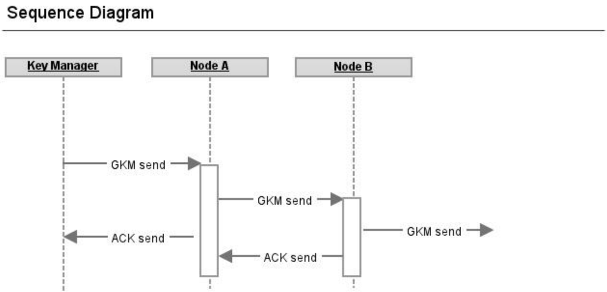
ARK EKE Protocol - Targets

- Targeted towards a tactical HF radio
  - 3 and 30 MHz, 3 KHz channels
  - Data rates
    - MIL-STD-188-110B (9600 bps and 12,800 bps uncoded)

ARK EKE Protocol - Exchange Paths



ARK EKE Protocol - Exchange Paths



ARK EKE Protocol - Performance Summary

- The group re-key time grows logarithmically with the number of allowed children in the transaction spanning tree
    - Since the group key is distributed in a single packet the prospect of parallel transactions to distribute communication overhead is not as significant as in the Viral technique
- Scalable to other target waveforms
    - The single group re-key message is all-inclusive and is suitable for any channel bandwidths at the cost of pre-placed information

Simulation Notes

- Manually introduced timing delays on packet transactions
  - Avoidance of signal interference
  - Emulation of TDMA ring access
- Computational overhead is estimated
  - Will likely change based on the properties of each physical unit used with each key management technique

Future Work

- Formal mathematical analysis of each protocol
  - Will be used for comparison with simulated results
- Security analysis of each protocol
  - Will be used to ensure the structure and content of key exchange messages is appropriate and not susceptible to compromising attacks