Hierarchical Key Management Schemes for Multicasting in Large Wireless Networks

H. Zhao, M. Strikis, V. Bharadwaj / John S. Baras

Problem Statement

- **Objective**: Study and design efficient and **Secure** Key Management Schemes for Multicasting in Large Wireless Networks
  - Efficient in that they minimize the total cost deriving from Communication Resources
  - User key storage
  - Computational Complexity
- **Principle**: Minimize the trade-off among Communication, Storage and Computation to achieve an *available* system that distributes the key updates reliably to all receivers
- **Secure**: in that it can:
  - Update the group key securely if it receives join or leave
  - Establish efficiently a shared secret among the legitimate receivers
- **Group** decision tree is used

Key Management in Large Wireless Multicast Network (design issues)

- Only legitimate group members have access to current group data
- Group key should be changed after every group membership update to the secret group requirement
- **Group Key Security**
  - **Forward Security**
  - **Backward Security**
- **Group key should be changed periodically**
- For a stable system, membership changes in key updates, data dissemination and reception must be handled in a way that no one participant affects the entire context of the communication. An efficient mechanism must be available
- **Macrotickets** can be used to achieve reliable group communication
- **Hierarchical Key Management Schemes** that take into account network topology, hierarchy, routing, and provide efficient and secure group communication

Hierarchical Key Management Model

- **GSC**: group security controller
- **GSA**: group security agent
- **members**: lowest layer
- **Independent subgroup key management**
- Update limited to subgroup
- **OSA**: OSA group, OSA in members
- **Frequency of broadcast**: from group members
  - Every GSC from OSA
  - GSC forwards OSA
- **Receives redissemination within group**
- When a node discovers a new group, it joins and becomes a new group
- **OSA**: receive and update group with different frequencies (lower) than members
- **Each** node in the group acquires similar patterns in frequency of moves, and in behavior

Organization Model Within a Group

- **Group Key Management Protocol (GKMP)**
  - **Single Group Key (SKG)**
  - **Group Key Distribution**
  - **Group Key Update**
  - **Group Key Security**
- **Data/groupBy Members**
  - Each group member knows all keys from the root node to the root node, but no other node in the group
- **Key Update (KU)**
  - Single key update from a root node
  - Group key update from a root node
  - **Node Join**
  - Node leaves group

Hierarchical Key Management Schemes: Design

- Single **Tree Key**: for the two groups of members (different modalities)
- **GSC** to **OAS**: Key Tree, each OSA (OAM, GSC)
- **GSC** to **GSC**: Key Tree, each cluster (GSC, GSC)
- **GSC** to **GSC**: Key Tree, single group member

**Hierarchical Key Management Schemes: Comparisons**

- **Class**: SKDC, OFT, ELK
- **Node Join**
- **Node Leave**
- **Key Update**
- **Performant key update in large multigroup with multiple selections**

Hierarchical Key Management Schemes: Comparisons

- **GSC Storage**: O(1)
- **GSC Storage**: O(1)
- **GSC Update**: O(1)
- **GSC Update**: O(1)
- **Add Group**: O(1)
- **Add Group**: O(1)
- **Add Group**: O(1)
- **Add Group**: O(1)

**Average Cost of Parameter Updates**

- **SKDC**: H, W, M
- **OFT**: H, W, M
- **ELK**: H, W, M

- **Node Join**
- **Node Leave**
- **Key Update**
- **Tree based schemes**

**Hierarchical Key Management Schemes: Comparisons**

- **SKDC**: group security controller
- **OFT**: group security agent
- **ELK**: lowest layer
- **Update limited to subgroup**
- **One GSC, n OSAs, m members**
- **Frequency of broadcast**: from group members
  - Every GSC from OSA
  - GSC forwards OSA
- **Receives redissemination within group**
- When a node discovers a new group, it joins and becomes a new group
- **OSA**: receive and update group with different frequencies (lower) than members
- **Each** node in the group acquires similar patterns in frequency of moves, and in behavior

**Hierarchical Key Management Model**

- **SKDC**: single key update
- **OFT**: multikey update
- **ELK**: multikey update

**Observations**

- **In the key broadcast queue**: the node broadcasts the key to the other group members
- **Join**: the member key is updated
- **Leave**: the member key is removed

**Efficient in communication vs. more keys to store for each member**

**Key update - members leave**

- \( (K_{i,j}, K_{j,i})_0 \)
- \( (K_{i,j}, K_{j,i})_0 \)

**Efficient in communication vs. more keys to store for each member**

- **SKDC**: O(1)
- **OFT**: O(n)
- **ELK**: O(n^2)

- **Average Cost of Parameter Updates**
  - **SKDC**: H, W, M
  - **OFT**: H, W, M
  - **ELK**: H, W, M

- **Key Update**
  - **Node Join**
  - **Node Leave**
  - **Tree based schemes**

- **Hierarchical Key Management Schemes**

- **SKDC**: group security controller
- **OFT**: group security agent
- **ELK**: lowest layer
- **Update limited to subgroup**
- **One GSC, n OSAs, m members**
- **Frequency of broadcast**: from group members
  - Every GSC from OSA
  - GSC forwards OSA
- **Receives redissemination within group**
- When a node discovers a new group, it joins and becomes a new group
- **OSA**: receive and update group with different frequencies (lower) than members
- **Each** node in the group acquires similar patterns in frequency of moves, and in behavior

**Hierarchical Key Management Model**

- **SKDC**: single key update
- **OFT**: multikey update
- **ELK**: multikey update

**Observations**

- **In the key broadcast queue**: the node broadcasts the key to the other group members
- **Join**: the member key is updated
- **Leave**: the member key is removed

**Efficient in communication vs. more keys to store for each member**

- **SKDC**: O(1)
- **OFT**: O(n)
- **ELK**: O(n^2)

- **Average Cost of Parameter Updates**
  - **SKDC**: H, W, M
  - **OFT**: H, W, M
  - **ELK**: H, W, M

- **Key Update**
  - **Node Join**
  - **Node Leave**
  - **Tree based schemes**

- **Hierarchical Key Management Schemes**

- **SKDC**: group security controller
- **OFT**: group security agent
- **ELK**: lowest layer
- **Update limited to subgroup**
- **One GSC, n OSAs, m members**
- **Frequency of broadcast**: from group members
  - Every GSC from OSA
  - GSC forwards OSA
- **Receives redissemination within group**
- When a node discovers a new group, it joins and becomes a new group
- **OSA**: receive and update group with different frequencies (lower) than members
- **Each** node in the group acquires similar patterns in frequency of moves, and in behavior