Efficient Group Key Management in Wireless LANs

Celia Li and Uyen Trang Nguyen
Computer Science and Engineering
York University
Outline

- Overview of group key management (GKM)
- Motivation and contributions
- Implementation of GKM protocols at the MAC layer
  - Logical key hierarchy (LKH)
  - One way function tree (OFT)
- Performance analysis
- Simulation results
- Conclusion
Overview of Group Key Management

- Group communications: 3 or more parties
- GKM provides secure generation, distributions and refreshing of group keys

- Group key
  - Only known to the current group members
  - Used to encrypt messages

- Membership changes trigger rekeying process
  - Join: a new group key must prevent the new member from decoding previous messages
  - Leave: a new group key must prevent former and current group members from decoding future messages
Logical Key Tree

LKH Join
\[ s \rightarrow \{C_1, C_2, \ldots, C_7\} : \{K'_1\}_{K_1} \]
\[ s \rightarrow \{C_5, C_6, C_7\} : \{K'_3\}_{K_3} \]
\[ s \rightarrow \{C_7\} : \{K'_7\}_{K_7} \]
\[ s \rightarrow \{C_8\} : \{K'_1, K'_3, K'_7\}_{K_{15}} \]

LKH Leave
\[ s \rightarrow \{C_1, C_2, C_3, C_4\} : \{K'_1\}_{K_2} \]
\[ s \rightarrow \{C_5, C_6, C_7\} : \{K'_1\}_{K'_3} \]
\[ s \rightarrow \{C_5, C_6\} : \{K'_3\}_{K_6} \]
\[ s \rightarrow \{C_7\} : \{K'_3\}_{K_7} \]
Group Key Management Approaches

- **Centralized GKM**
  - A group controller is responsible for key generation, key distribution and key refreshment
  - Typical algorithm: Logical Key Hierarchy (LKH) [1] and One-way Function Tree (OFT) [2]

- **Distributed GKM**
  - A multicast group is organized into smaller subgroups with multiple subgroup controllers
  - A subgroup controller is in charge of key computation and distribution

- **Contributory GKM**
  - No group controller
  - Each member contributes a share toward the group key
Our Motivation

- The communication cost of a group key update in 802.11i is $O(n)$ where $n$ is the number of associated members => not scalable.
- Centralized approach is most suitable and cost-effective for GKM at the MAC layer of a WMNs, because
  - an access point (AP) is a central controller that generates and distributes the group keys.
  - mobile devices connects to the AP are physically located close to it.
  - pairwise transient key (PTK) from 802.11i provides a secure communication channel between the AP and each of its associated mobile device.
Our Contributions

- We incorporate the LKH (logical key hierarchy) and OFT (one-way function tree) algorithms into the group key management protocol at the MAC layer.
  - Reduced key update latency from $O(n)$ to $O(\log n)$

- Group key update latencies of IEEE 802.11i, LKH, and OFT GKM are evaluated via numerical analyses and simulations.

- Numerical analyses and simulation results show that the LKH and OFT algorithms improve the latency of group key updates compared with 802.11i GKM.
LKH

LKH Join

\[ s \rightarrow \{C_1, C_2, \ldots, C_7\} : \{K'_1\}_{K_1} \]
\[ s \rightarrow \{C_5, C_6, C_7\} : \{K'_3\}_{K_3} \]
\[ s \rightarrow \{C_7\} : \{K'_7\}_{K_7} \]
\[ s \rightarrow \{C_8\} : \{K'_1, K'_3, K'_7\}_{K_{15}} \]

LKH Leave

\[ s \rightarrow \{C_1, C_2, C_3, C_4\} : \{K'_1\}_{K_2} \]
\[ s \rightarrow \{C_5, C_6, C_7\} : \{K'_1\}_{K'_3} \]
\[ s \rightarrow \{C_5, C_6\} : \{K'_3\}_{K_6} \]
\[ s \rightarrow \{C_7\} : \{K'_3\}_{K_7} \]
OFT

OFT Join
\[ s \rightarrow \{C_1, C_2, C_3, C_4\} : \{f(K_3')\}_{gK_2} \]
\[ s \rightarrow \{C_7\} : f(\kappa_{14}', f(\kappa_{15}))_{g\kappa_{14}} \]
\[ s \rightarrow \{C_5, C_6\} : \{f(K_7')\}_{gK_6} \]
\[ s \rightarrow \{C_8\} : f(\kappa_{14}', f(K_6), f(K_2))_{g\kappa_{15}} \]

OFT Leave
\[ s \rightarrow \{C_1, C_2, C_3, C_4\} : \{f(K_3')\}_{gK_2} \]
\[ s \rightarrow \{C_5, C_6\} : \{f(K_7')\}_{gK_6} \]
\[ s \rightarrow \{C_7\} : K_{7g(\kappa_7)} \]
## Performance Comparisons

### Computational Complexity

<table>
<thead>
<tr>
<th>Operation</th>
<th>802.11</th>
<th>LKH</th>
<th>OFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join</td>
<td>Encryption</td>
<td>$n$</td>
<td>$\log_2 n + 1$</td>
</tr>
<tr>
<td></td>
<td>Decryption</td>
<td>1</td>
<td>$\log_2 n$</td>
</tr>
<tr>
<td></td>
<td>Hashing</td>
<td></td>
<td>$3 \log_2 n + 2$</td>
</tr>
<tr>
<td>Leave</td>
<td>Encryption</td>
<td>$n$</td>
<td>$2 \log_2 n$</td>
</tr>
<tr>
<td></td>
<td>Decryption</td>
<td>1</td>
<td>$\log_2 n$</td>
</tr>
<tr>
<td></td>
<td>Hashing</td>
<td></td>
<td>$2 \log_2 n + 2$</td>
</tr>
</tbody>
</table>

### Communication Complexity

<table>
<thead>
<tr>
<th>Operation Algorithm</th>
<th>Unicast (number of keys)</th>
<th>Broadcast (number of keys)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11</td>
<td>$n$</td>
<td></td>
</tr>
<tr>
<td>LKH</td>
<td>$\log_2 n$</td>
<td>$\log_2 n$</td>
</tr>
<tr>
<td>OFT</td>
<td>$\log_2 n$</td>
<td>$\log_2 n + 1$</td>
</tr>
<tr>
<td>Leave</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11</td>
<td>$n$</td>
<td></td>
</tr>
<tr>
<td>LKH</td>
<td>$\log_2 n$</td>
<td>$2 \log_2 n$</td>
</tr>
<tr>
<td>OFT</td>
<td></td>
<td>$\log_2 n + 1$</td>
</tr>
</tbody>
</table>
# Simulation Using QualNet

## Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission range of MAPs</td>
<td>315m</td>
</tr>
<tr>
<td>Transmission range of mesh clients</td>
<td>304m</td>
</tr>
<tr>
<td>Movement model</td>
<td>Random way point</td>
</tr>
<tr>
<td>speed</td>
<td>10m/s</td>
</tr>
<tr>
<td>Simulation time</td>
<td>150s</td>
</tr>
<tr>
<td>Scenario dimensions</td>
<td>300m x 300m</td>
</tr>
<tr>
<td>Propagation fading model</td>
<td>none</td>
</tr>
<tr>
<td>Number of runs per data point</td>
<td>10</td>
</tr>
<tr>
<td>Confidence interval</td>
<td>95%</td>
</tr>
</tbody>
</table>
Varying Multicast Group Size

- Function of Multicast Group Size

(a) Group size from 1-50 - Join

(c) Group size from 1-50 - Leave
Varying Multicast Group Size (2)

Broadcast messages are sent 3 times.

(a) Group size from 1-50 - Join

(c) Group size from 1-50 - Leave
Varying Source Rate

- Function of Multicast Traffic Load

(a) The 50th member joins

(c) The 50th member leaves
Conclusion

- We apply LKH and OFT algorithms to GKM at the MAC layer in wireless LANs in order to improve its performance.

- We evaluate and compare the performance of the 802.11, LKH and OFT algorithms under realistic network settings using simulations.

- Our numerical analysis and simulation results confirm that the LKH and OFT algorithms reduce the re-keying latency of GKM in wireless LANs from linear time to logarithmic time.
References


Thank you!

Q & A
Extra Slides
### Implementation of LKH in Access Points

#### Table 1: Updated Keys and ID Changes

<table>
<thead>
<tr>
<th>7</th>
<th>14</th>
<th>1, ${K'_1}K_1$</th>
<th>3, ${K'_3}K_3$</th>
<th>14, ${K'<em>7}K</em>{14}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>C7’s node</td>
<td>ID is changed from 7 to 14</td>
<td>Updated Keys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) Broadcast message for client $C_1$ to $C_7$ after client $C_8$ joins the group.

<table>
<thead>
<tr>
<th>7</th>
<th>14</th>
<th>15, ${K'_1, K'_3, K'<em>7}K</em>{15}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>C7’s node</td>
<td>ID is changed from 7 to 14</td>
<td>Updated Keys</td>
</tr>
</tbody>
</table>

(b) Unicast message for client $C_8$ after client $C_8$ joins the group.

<table>
<thead>
<tr>
<th>14</th>
<th>7</th>
<th>2, ${K'_1}K_2$</th>
<th>3, ${K'_1}K_3$</th>
<th>6, ${K'_3}K_6$</th>
<th>7, ${K'_3}K_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>C7’s node</td>
<td>ID is changed from 7 to 14</td>
<td>Updated Keys</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(c) Broadcast message after client $C_8$ leaves the group.
## Implementation of OFT in Wireless Mesh Router

<table>
<thead>
<tr>
<th>Step</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>${f(K_3')}_{g(K_2)}$</td>
</tr>
<tr>
<td>6.</td>
<td>${f(K_7')}_{g(K_6)}$</td>
</tr>
<tr>
<td>14.</td>
<td>${\kappa_2', f(\kappa_{15})}<em>{g(K</em>{14})}$</td>
</tr>
</tbody>
</table>

---

**C_7’s node**

- **ID is changed from 7 to 14.**

- **Updated Keys**

(a) Broadcast message for client $C_1$ to $C_7$ after client $C_8$ joins the group.

<table>
<thead>
<tr>
<th>Step</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>${f(\kappa_{14}'), f(K_6), f(K_2)}<em>{g(\kappa</em>{15})}$</td>
</tr>
</tbody>
</table>

---

**C_7’s node**

- **ID is changed from 7 to 14.**

- **Updated Keys**

(b) Unicast message for client $C_8$ after client $C_8$ joins the group.

<table>
<thead>
<tr>
<th>Step</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>${f(K_3')}_{g(K_2)}$</td>
</tr>
<tr>
<td>2.</td>
<td>${f(K_3')}_{g(K_2)}$</td>
</tr>
<tr>
<td>6.</td>
<td>${f(\kappa_7')}_{g(K_6)}$</td>
</tr>
<tr>
<td>7.</td>
<td>${\kappa_7'}_{g(\kappa_7)}$</td>
</tr>
</tbody>
</table>

---

**C_7’s node**

- **ID is changed from 7 to 14.**

- **Updated Keys**

(c) Broadcast message after client $C_8$ leaves the group.