Lightweight Key Establishment & Management Protocol (KEMP) in Dynamic Sensor Networks

Update
draft-qiu-roll-kemp-01

Ying QIU, Jianying ZHOU, Feng BAO
Features

• Suitable for both static and dynamic WSN. Any pair of nodes can establish a key for secure communication.
  – Easily scalable

• A roaming note only deals with its closest router for security. No need to change the rest routing path to the base station.
  – Less signalling, hence less power cost

• Base station can manage the revocation list for lost or compromised roaming motes.
  – Stronger security

• System is scalable and resilient against node compromise.
  – Stronger security
Key Establishment

\[ req = \{ \text{src}=ID, \text{Dst}=BS, RT \parallel R_0 \parallel \text{MAC}(K_{BN}, ID\parallel RT\parallel R_0) \} \]  
(1)

\[ K_{NR} = H(K_{BN}, ID\parallel R_0 \parallel R_1) \]  
(2)

\[ aprv = \{ \text{src}=BS, \text{dst}=RT, E(K_{BR}, ID\parallel R_0 \parallel R_1 \parallel K_{NR}) \} \]  
(3)

\[ notice = \{ \text{src}=RT, \text{Dst}=ID, R_0 \parallel R_1 \parallel \text{MAC}(K_{NR}, RT\parallel ID\parallel R_0 \parallel R_1) \} \]  
(4)
Protocol

- **Shared key discovery:**
  - saving communication
  - each sensor only store a small set of keys randomly selected from a key pool at the deployment. Two nodes may use the key discovery protocol to find a common key from their own sets.

- **Key establishment and update:**
  - an efficient and scalable scheme to establish and update the keys among nodes.

- **Authentication and encryption:**
  - describe how to use node’s ID information to authenticate and encrypt the traffic packets.

- **Distribution Mode:**
  - the more hops, the poorer the traffic performance and the more energy consumption.
  - deploy the cluster heads as the sub-base-stations.

- **Key revocation:**
  - if a node is compromised, the base station should revoke the related keys from the database and inform the relevant nodes.

- **Node Bootstraps:**
  - \[ \text{req} = \{ \text{src} = \text{ID}, \text{Dst} = \text{BS}, \text{RT}_{\text{FIRST}} || R_0 || \text{MAC}(K_{BN}, \text{ID} || \text{RT}_{\text{FIRST}} || R_0) \} \]  
  (5)

- **Multiple Trust Domains:**
## Comparison

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Mobility</th>
<th>Pre-shared-Key</th>
<th>Revocation</th>
<th>Comm/Comp</th>
<th>Scable</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEMP</td>
<td>Support</td>
<td>option</td>
<td>easy</td>
<td>Mid/Mid</td>
<td>easy</td>
</tr>
<tr>
<td>AMIKEY</td>
<td>No</td>
<td>option</td>
<td>difficult</td>
<td>High/High</td>
<td>easy</td>
</tr>
<tr>
<td>DODAG</td>
<td>No</td>
<td>Need</td>
<td>?</td>
<td>Low/High</td>
<td>difficult</td>
</tr>
</tbody>
</table>
Future Works

• Define the transmission format.
• Feedback and improve.
Thanks

Q & A