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

Update

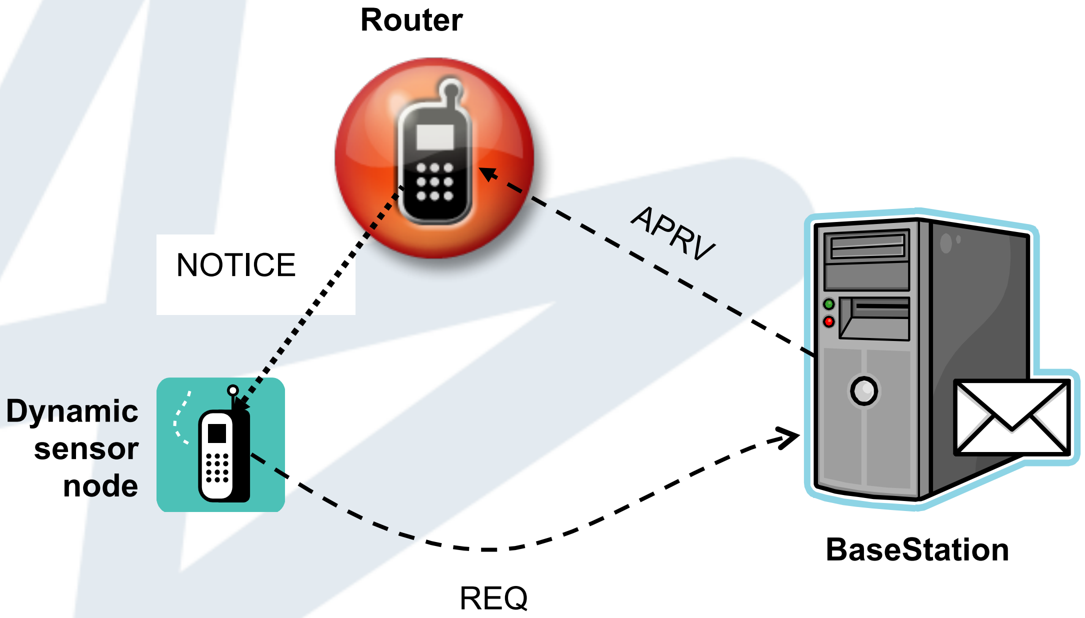
draft-qiu-roll-kemp-01

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



$$req = \{src=ID,\ Dst= BS,\ \ RT \,||\, R_0 \,||\, MAC(K_{BN},\ ID||RT||R_0)\ \} \qquad (1)$$

$$K_{NR} = H(K_{BN},\ ID||\ R_0 \,||\, R_1\ ) \qquad (2)$$

$$aprv = \{src=BS,\ dst=RT,\ \ E(K_{BR},\ ID||R_0||R_1||\ K_{NR}\ )\} \qquad (3)$$

$$notice = \{src=RT,\ Dst=ID,\ R_0 \,||\, R_1 \,||\, MAC(K_{NR},\ RT||ID||\ R_0||R_1\ )\} \qquad (4)$$

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:
  - $req = \{src=ID, Dst= BS, \; RT_{FRIST} || R_0 || MAC(K_{BN}, ID || RT_{FRIST} || R_0) \}$ (5)
- Multiple Trust Domains:

Comparison

Protocol	Mobility	Pre-shared-Key	Revocation	Comm/ Comp	Scable
KEMP	Support	option	easy	Mid/Mid	easy
AMIKEY	No	option	difficult	High/High	easy
DODAG	No	Need	?	Low/High	difficult

Future Works

- Define the transmission format.
- Feedback and improve.

Thanks

Q & A