Group Key Management in WSN

Using a modified version of GDH.3 protocol

SAPIENZA
UNIVERSITÀ DI ROMA

Stefano Milani

Group key management

- **Computational group key secrecy**
- **Decisional group key secrecy**
- **Key independence**
  - **Forward secrecy**
  - **Backward secrecy**

Problems in WSN

We still need to ensure the presented security requirements, but:

- The protocol must require less computational power and less energy consumption as possible

- The amount of work must be equally distributed between all the group member

A modified GDH.3 protocol

This protocol need a hierarchical WSN composed by:

- **Base Station**
- **Group Leader**
- **Simple Nodes**

Key agreement (Step 1)

Given n nodes, where M_1 is the group leader, the key agreement is composed by two steps:

- Every nodes generates a secret k_i. M_1 selects a point P (using ECC) and sends to M_2 $Q_1 = k_1 P$. M_2 sends to M_3 $Q_2 = k_2 Q_1 = k_2 k_1 P$. This process is repeated until the node M_n is reached.
  M_n generates $Q_n = k_1 \ldots k_n P$ the shared secret.
  For each node M_i, k_i is the private key and Q_i is the public key.

Key agreement (Step 2)

- M_n encrypts Q_n with M_{n-1} public key Q_{n-1} and sends it to M_{n-1}, that can decrypt the message and acquire Q_n. Then it can repeat the procedure and sends the secret key to M_{n-2}, and so on so forth until every nodes receive the secret key.

Group formation

- It is used a distributed depth-first algorithm traversal algorithm to visit all nodes at least once.
- In this way it is created a virtual depth-first spanning tree that include all nodes. We need to maintain the tree balanced to guarantee the correctness of the protocol.

Join group

- When a node M_{n+1} wants to join the group, it must first authenticate with the base station, that assign to him an ID and contacts to the group leader.
- M_1 sends Q_n to the new node, that generate its private key k_{n+1} and the new secret key $Q_{n+1} = k_{n+1}Q_n$ and sends it back to M_1.
- The group leader inform all nodes about the new key with and $UPDATE$ message containing the new shared secret.

Leave group

When a node leaves the group the group leader M_1 generates a random value k'_n and computes the new shared key $Q'_n = k'_n Q_n$. Then it sends to all the nodes in the group the new key using the $UPDATE$ message.

Merge groups

- A group M' wants to join M, M_1 send the shared key to M_1' that becomes $M_{n+1}$and it starts the process to generates a new key among the nodes of M'.

- When the last node is reached it generates the new shared key and sends it back to all nodes like in Step 2 already discussed.

Partition group

When a partition group event occurs, the protocol simply reconstruct the depth-first search spanning tree of each group and a new key agreement is issued for the two resulting groups

Group maintenance

In order to handle the event of join, leave, merge and partition the virtual tree can degenerate into a spanning tree that no longer fulfills the depth-first search criteria.

In order to balance the tree and guarantee key freshness the group leader periodically restarts the depth-first search and generates a new shared key.

Judgment (1/2)

- The amount of work is distributed equally among all the nodes (only the group leader must do a bit of extra work).
- ECC used, optimal wrt computational power and so energy consumptions

Judgment (2/2)

- The periodical update of the shared key can be expensive if the number of nodes is high
- It can be possible to perform the update of key using an approach like the one used when a node leaves the group?
- Yes, but the periodical update of the key done like the initial key agreement ensure to maintain balanced the tree

Feasibility in LoRaWAN network (1/2)

With the actual architecture direct communication between devices can be an issue.

Star topology to connect devices, and they are authenticated with the Network Server and the Application Server.

Feasibility in LoRaWAN network (2/2)

With the architecture proposed in [2] we can use the the *concentrator* as base station, because it is provided a method to authenticate the single device with the gateway.

So in this case we can implement a more feasible communication between devices and use the proposed protocol to perform a group key agreement.

Conclusion

- The protocol covered every aspects of the group key management, and it is optimized for WSN.
- But it can be improved trying to avoid the use of the depth-first search tree, in a way in which we do not need to maintain balanced the tree.
- To implement the protocol in a LoRaWAN network we need to modify the actual architecture.

References

[1] Chatzigiannakis, Ioannis, Elisavet Konstantinou, Vasiliki Liagkou, and Paul Spirakis. "**Design, analysis and performance evaluation of group key establishment in wireless sensor networks.**" *Electronic Notes in Theoretical Computer Science* 171, no. 1 (2007): 17-31.

[2] Chatzigiannakis, Y., V. Liagkou, and P. Spirakis. **"Providing end-to-end secure communication in low-power wide area networks (LPWANs)."** In *2nd International Symposium on Cyber Security Cryptography and Machine Learning (CSCML 2018)*. 2018.