Poster Abstract: A Secure Group Communication Mechanism in Cluster-Tree Wireless Sensor Networks

Olfa Gaddour[1], Anis Koubâa[2,3], Omar Cheikhrouhou[1], Mohamed Abid[1]
[1]Research unit CES, National school of Engineers of Sfax-Tunisia
[2]IPP-HURRAY! Research Group, Polytechnic Institute of Porto,Rua Antnio Bernardino de Almeida, 431, 4200-072 Porto, Portugal
[3]Al-Imam Muhammad Ibn Saud University, Computer Science Dept., 11681 Riyadh, Saudi Arabia
olfagaddour@yahoo.fr , akoubaa@dei.isep.ipp.pt, enis01amor@yahoo.fr, mohamed.abid@enis.rnu.tn

***Abstract*—Security is a challenging issue in Wireless Sensor Networks (*WSNs*) due to the dual impact of their inherent constraints and their operation in open and harsh environments. We briefly present SeGCom, a new security mechanism for group communications in cluster-tree WSNs. We define a group as a set of sensor nodes in the cluster-tree network sharing the same sensory information. Our objective is to limit the access to the group data exclusively to the members that have securely joined the group.**

I. Introduction

Wireless Sensor Networks (*WSNs*) are composed of energy-constrained nodes embedding limited transmission, processing and sensing capabilities. As *WSNs* are basically deployed in hostile environments, security becomes extremely important, since sensor nodes are exposed to different types of malicious attacks.

Security in *WSNs* has attracted several research studies that have addressed various security problems. The security problem in *WSNs* becomes even more challenging when dealing with the *group* security, as this grouping impose additional overhead in terms of network management. In this poster, we focus on securing group communications in *cluster-tree WSNs*, where a *group* is defined as a set of sensor nodes sharing a common private information.

II. SeGCom Description

A. Network Model

We consider a multi-tiered architecture which contains a special node called Base Station (*BS*) which define the entire network, some special nodes that may have the ability to associate from other nodes which are called cluster-heads (*CH*) and end devices (*ED*) with no ability to associate with other devices. This architecture is shown in Fig. 1.

In Fig. 2, we identify two groups in the cluster-tree network. The first group is represented by black squares (e.g. for temperature data traffic) and the other is represented by gray triangles (e.g. for light data traffic).

B. Pre-deployment settings

Our work relies on the polynomial-based key pre-distribution scheme proposed by Blundo et *al.* in [1]. This scheme uses a symmetric bi-variate polynomial to generate secure pairwise keys for any two nodes knowing each other's identity.

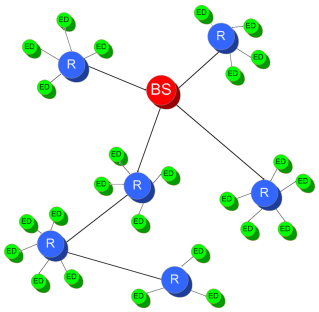

Fig. 1. The Network Model

C. Group Creation

1) Group initiation: We consider a new grouping concept as compared to previous works. A *group* refers to a set of sensors that produce the same type of traffic. Fig. 2 illustrates our grouping concept in a cluster-tree *WSN*.

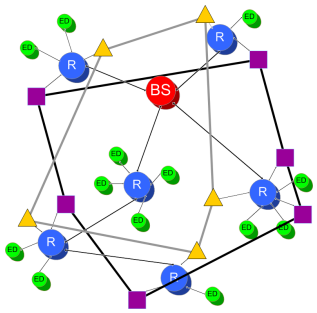

Fig. 2. An example of a WSN containing two groups

2) Group controller creation: A node that wants to join a given nonexistent group must send a *join-request* message to the *BS*. After authenticating the request, the *BS* sends a *join-confirmation* message and a set flag *GC-flag*. After receiving the flag, the designated *GC* sends a request to *BS* to obtain

the G_{id}. After receiving the G_{id}, the *GC* generates a random key K_g as the group key.

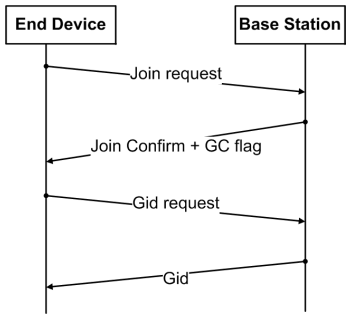

Fig. 3. Message Sequence Diagram between an ED wanting to form a group and the BS

3) Group Join: After the designation of the *GC*, the subsequent group joining requests must be directed to (and handled) by the *GC*. Nodes will know about the existence of the group upon the reception of group identifier sent by an authenticated broadcast using the μTESLA proposed in [2].

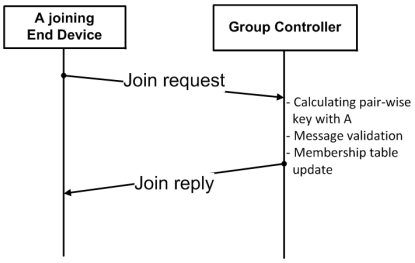

Fig. 4. Message Sequence Diagram between an ED and the GC

After receiving the broadcasted group identifier G_{id}, a node *A* that wants to join the group calculates the pair-wise key shared with the *GC*, according to the Blundo mechanism. The node *A* then sends a *join-request* message to the group controller *GC*, which has the following structure:

$$ID_A|G_{id}|MAC(K_{A,GC}, ID_A, G_{id})) \quad (1)$$

In the second step, the *GC* sends a *join-response* message with the following structure:

$$\{K_g, add_{gr}\}_{K_{A,GC}} \quad (2)$$

4) Group Leave: A node leave may be initiated by the node itself upon sending a leave-request message to its group controller, or initiated by the group controller, which may delete the node from the group.

The group leave operation when initiated by a leaving end device is shown in Fig. 5.

III. Evaluation

A. Performance Analysis

1) Storage cost: The additional computation overhead for calculating the pairwise key is almost negligible (requires *t* modular additions and *t* modular multiplications over F_q). To use Blundo's theory, each sensor node *i* needs to store a *t*-degree polynomial $f(i, x)$, which occupies *(t + 1)* log *q* storage space. As a result, if a key is of *q*-bits, a regular sensor node has to store *(t+2)* keys.

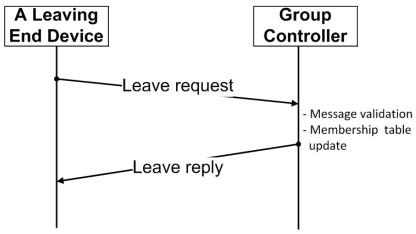

Fig. 5. The Leaving Operation

2) Communication cost: The proposed scheme requires one global broadcast for sending the group controller identifier. The *GC* may receive *N* join requests and needs to send the group key to *N* members. Thus, to set up the group key among *N* members, it requires *2N* unicasts and one global broadcast.

B. Security analysis

- *Security of the GC*: Only the base station can authorize a node to act as a group controller We used μTESLA to perform authenticated broadcast between a *GC* and all nodes in the network. This scheme guarantees the authentication and the freshness of the packets sent by the GC.
- *Protection against replay attacks*: An intruder can hear the join or leave requests and replay it byte-by-byte to the *GC*. This request is automatically rejected by the *GC* because the member already exists in the membership table. Thus, replay attacks is not possible in both *join* and *leave* operations.
- *Prevention against decoding previous and future messages within a group*: the forward secrecy and the backward secrecy are guaranteed by updating the group key in each join and leave operations.

IV. Conclusion

In this poster, we have proposed, SeGCom, a simple yet efficient new mechanism for supporting secure group communication in cluster-tree Wireless Sensor Networks (*WSNs*), where a group is defined as a set of sensor nodes producing the same type of sensory data. Our analysis shows that the proposed scheme is efficient in terms of computations, which is adequate for constrained-resources *WSNs*. In addition, we have shown that SeGCom is immune against several attacks.

References

[1] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," vol. 740, pp. 471–486, 1993.

[2] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," pp. 2–3, 2002.