Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

LNT: A logical neighbor tree secure group communication scheme for wireless sensor networks

Omar Cheikhrouhou [a,*], Anis Koubâa [b,c], Gianluca Dini [e], Hani Alzaid [d], Mohamed Abid [a]

[a] CES Research Unit, National School of Engineers of Sfax, University of Sfax, Tunisia
[b] CISTER Research Unit, Polytechnic Institute of Porto (ISEP/IPP), Portugal
[c] COINS Research Group, Al-Imam Mohamed bin Saud University, Riyadh, Saudi Arabia
[d] Computer Research Institute, King Abdulaziz City for Science and Technology, Saudi Arabia
[e] Dipartimento di Ingegneria della Informazione, University of Pisa, Via Diotisalvi 2, 56100 PISA, Italy

ARTICLE INFO

Article history:
Received 20 November 2011
Received in revised form 21 March 2012
Accepted 24 March 2012
Available online 18 April 2012

Keywords:
Secure group communication (SGC)
Wireless sensor networks (WSNs)
Group key management
Simulation
Analysis

ABSTRACT

Secure group communication is a paradigm that primarily designates one-to-many communication security. The proposed works relevant to secure group communication have predominantly considered the whole network as being a single group managed by a central powerful node capable of supporting heavy communication, computation and storage cost. However, a typical Wireless Sensor Network (WSN) may contain several groups, and each one is maintained by a sensor node (the group controller) with constrained resources. Moreover, the previously proposed schemes require a multicast routing support to deliver the rekeying messages. Nevertheless, multicast routing can incur heavy storage and communication overheads in the case of a wireless sensor network. Due to these two major limitations, we have reckoned it necessary to propose a new secure group communication with a lightweight rekeying process. Our proposal overcomes the two limitations mentioned above, and can be applied to a homogeneous WSN with resource-constrained nodes with no need for a multicast routing support. Actually, the analysis and simulation results have clearly demonstrated that our scheme outperforms the previous well-known solutions.

1. Introduction

Wireless sensor networks are generally deployed in a wide area for the purpose of monitoring some environmental parameters, such as lightweight, humidity, temperature, and pressure. In some applications, different security levels and services are often required for each type of information. For this purpose, the network would be divided into several groups, each of which is responsible for reporting certain specific data. Inside each single group, a one-to-many communication type might be needed, for example, when the group controller sends commands/queries to all group members. Moreover, there are some applications in which in-network processing is needed, for instance, to reduce the communication cost. As a matter of fact, in-network processing enables to send aggregated information instead of large streams of raw data. For this aim, nodes need to communicate among themselves in order to produce such a type of aggregated information.

In some critical applications, e.g. healthcare, group communication has to be protected. Generally, secure group communication could be achieved through the use of a group key shared among the group members. The group key can be managed in either a centralized manner, a distributed manner, or a contributed manner [1,2]. In the centralized approach, the group controller generates the group key and delivers it to all the group members. In the distributed approach, the group is divided into smaller subgroups each of which is managed locally. However, as

* Corresponding author.
E-mail addresses: omar.cheikhrouhou@isetsf.rnu.tn (O. Cheikhrouhou), aska@isep.ipp.pt (A. Koubâa), g.dini@iet.unipi.it (G. Dini), hmalzaid@kacst.edu.sa (H. Alzaid), mohamed.abid@enis.rnu.tn (M. Abid).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.03.019

each subgroup has its different key, this approach presents the limits of translating the encrypted data when forwarded from one subgroup to another. In other words, encrypted messages need to be decrypted whenever they reach another subgroup in order to make use of the transmitted data if in-network processing is available. Therefore, it may introduce a computation overhead. As for the contributed approach, each group member contributes in the computation of the group key which leads to a heavy complexity and communication cost.

Taking into account the limitations of the distributed and contributed approach, many schemes have opted to the centralized approach. The trivial solution to deliver the group key, in the centralized approach, is to send it by unicast to each group member. However, this solution requires an $O(n)$ communication cost complexity, where n is the number of group members. So, numerous schemes have been proposed for the sake of reducing the communication, computation and storage cost needed for the rekeying process [3–7].

However, the majority of the proposed schemes assume that the group controller is a powerful node such as a PC or a base station. Actually, they consider the whole network as being a single group managed by the base station. However, this presents a restrictive definition of a group and a network model. As a matter of fact, in some applications several groups managed by resource-constrained sensor nodes might be needed. In addition, the proposed schemes such as [3–6] suppose that the network has a multicast routing support to deliver the rekeying messages in a multicast way. However, multicast routing introduces a heavy overhead and communication cost for maintaining the multicast table and the multicast routes. Moreover, the rekeying messages used in the majority of previous schemes present some security vulnerabilities. For example, some schemes such as LKH [3], and TKH [5], are not protected against replay attacks. Hence, an attacker can replay a revealed group key in order to intercept the communication. Revoked nodes can also replay an old group key in order to rejoin the group. In addition, some schemes [3,5,6] do not consider rekeying messages authentication which makes them vulnerable to messages injection attacks.

As a matter of fact, the previous schemes' limitations, described above, have given us ground to conceive a new secure group communication scheme. The strengths of the proposed scheme are that it can be applied to a group with a resource-constrained group controller, does not require a multicast routing support and is robust against possible attacks.

1.1. Contribution

This paper proposes a secure group communication scheme that allows sensor nodes belonging to the same group to communicate securely. The proposed scheme is composed of two main components: the group membership management and the group key management. The group membership management component defines in a secure manner the group creation, the group join and the group leave processes. The group key management component presents a lightweight method to update the group key after each membership change for the sake of guaranteeing forward and backward secrecy properties. The proposed method is based on the construction of a logical neighbor tree that helps to share the task of rekeying messages distribution among the group members. Therefore, our scheme eliminates the necessity of a powerful group controller and so that can fit resource-constrained sensor nodes.

The idea of secure group communication with resource-constrained group controller was first addressed by Cheikhrouhou et al. in their paper RiSeG [8,9]. Yet, the proposed scheme presents an $O(n)$ latency in the rekeying process and, therefore, cannot endure large scale WSNs. Moreover, RiSeG requires synchronization between nodes in order to avoid replay attacks. However, synchronization is a hard task to be achieved in a WSN [10].

As an improvement, a Logical Neighbor Tree (LNT) is proposed in order to distribute the key update messages. Actually, the LNT scheme enables to reduce the key update latency from $O(n)$ to $O(log(n))$. In addition, LNT eliminates the requirement of node synchronization.

In summary, LNT is distinguished by the following features:

- The concept of group is application-based, i.e., groups reflect the application needs.
- The group controller could be a sensor node with constrained resources.
- The LNT scheme proposes the membership management and the group key management in an efficient and secure way.

1.2. Roadmap

The remainder of this paper is organized as follows: Section 2 presents relevant work to secure group communication in WSNs. Section 3 presents the network model, the adversarial model, requirements and assumptions used in our work. Section 4 gives an overview of the LNT scheme and its design principles. Sections 5–7 describe the LNT membership management, the logical neighbor tree formation and the LNT rekeying process, respectively. Section 8 presents a comparison between the LNT rekeying process and other well-known group key management schemes namely, LKH [3], TKH [5], and RiSeG [8]. Section 9 presents a security analysis of the LNT scheme. Finally, we conclude and give possible future work.

2. Related work

In the literature, there are a few works that detail a complete secure group communication schemes with its different components. The proposed SGC schemes in the recent decade are [11,12,8,9].

In [11], the authors proposed SLIMCAST: a secure level key infrastructure for multicast to protect data confidentiality via hop-by-hop re-encryption and mitigate the DoS-based flooding attack through an intrusion detection and deletion mechanism. The SLIMCAST protocol divides a group routing tree into levels and branches in a clustered