Journal of Network and Computer Applications 61 (2016) 115–132

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Secure Group Communication in Wireless Sensor Networks: A survey

Omar Cheikhrouhou [a,b,*]

[a] CES Lab, ENIS, University of Sfax, Tunisia
[b] College of Computers and Information Technology, Taif University, Saudi Arabia

ARTICLE INFO

Article history:
Received 25 January 2015
Received in revised form
1 October 2015
Accepted 26 October 2015
Available online 10 November 2015

Keywords:
Secure Group Communication (SGC)
Wireless Sensor Networks (WSN)
Group key management
Security
Survey

ABSTRACT

Wireless Sensor Networks (WSN) consist of a large number of sensor nodes which are often deployed in an unattended harsh environment. As they are exposed to a wide range of attacks, sensor-based applications have then to be secured. In this paper, we present an up-to-date survey of different Secure Group Communication (SGC) schemes in WSN. We examine both components of the existing SGC schemes, namely the group key management and the group membership management, and discuss their performance and security level. In addition, we classify existing schemes into three different approaches: centralized, contributory, and hybrid. Additionally, we provide recommendations on which scheme to use for specific WSN constraints and specific application requirements. Finally, we point out the challenges that researchers have to address while giving them directions to potential solutions.

Contents

1. Introduction

Wireless Sensor Networks consist of a large number of sensor nodes which are often deployed in an unattended harsh environment. Each sensor node has to sense specific phenomena and report it towards a central node (base station). Because of its limited physical resources, it has to achieve its goals with minimal memory usage, energy consumption, and computation cost. In addition, sensor nodes may self-organize into groups to cooperate for the gathering of specific information or the accomplishment of a specific task. Since these nodes are usually operating in an unattended environment without any physical protection, and communicating with wireless connection, they are exposed to a wide range of attacks. Sensor-based applications have then to be secured. In particular, in broad critical applications, the information exchanged between group members (sensor nodes) needs

[*] Correspondence address: CES Lab, ENIS, University of Sfax, Tunisia.
E-mail address: o.cheikhrouhou@tu.edu.sa

http://dx.doi.org/10.1016/j.jnca.2015.10.011
1084-8045/© 2015 Elsevier Ltd. All rights reserved.

higher level of security. In military applications for instance, groups of sensors cooperate to track a target (Steed and Milton, 2008). Therefore, these sensor nodes may exchange information related to the position of this target. If an attacker injects false messages, it can disturb the operation of this application. In medical applications also, patient's physiological parameters collected by a group of sensor nodes must be kept confidential and protected (Vassis et al., 2010). Secure Group Communication is also necessary to provide location privacy, which is of utmost interest in military, homeland security and animal monitoring applications (Abuzneid et al., 2015; Chen and Lou, 2015). Consequently, a Secure Group Communication (SGC) scheme must be applied to protect the communication inside the group from potential attacks (such as eavesdropping, injecting, and modifying messages) (Cheikhrouhou et al., 2011b, 2012; Sakarindr and Ansari, 2007).

Although SGC problems have been well studied in traditional networks, there are still challenging issues when it comes to WSNs due to their inherent characteristics such as constrained resources (e.g., low power, low memory, and low CPU), wireless medium (e.g., no physical access control to the medium), and low bandwidth and transmission range. Therefore several solutions have been proposed in the last decade to address these challenging issues. We have classified the existing proposed solutions into three categories: centralized, contributory and hybrid. In centralized SGC schemes, a central trusted entity is responsible for the management of the group. In particular, it has to manage the joining and leaving of nodes and the renewing of the group key. In the centralized approach, the group controller (GC) carries most of the workload and so represents a single point of failure and becomes a point of target. In the contributory approach (known also as the distributed approach), all group members collaborate for the management of the group rather than delegating the task to a central entity. In contrast with the centralized approach, the contributory approach has the advantage of fault-tolerance but at the expense of the computational cost. Regarding the hybrid approach, some tasks are done by a central entity while others are done collaboratively, which should bring both efficiency and failure-tolerance.

Most current surveys focus whether on centralized (Naranjo and Casado, 2012) or contributory (Manulis, 2005; Bresson and Manulis, 2008) schemes. Very few quality works have surveyed more than one category (He et al., 2013). To our knowledge, none of the current surveys has addressed and compared the three types of SGC schemes.

Moreover, a SGC scheme consists of two main components: the group key management and the group membership management. Regarding group key management, which is the core problem of SGC, several quality surveys have been published (Sakarindr and Ansari, 2007; Xiao et al., 2007; Klaoudatou et al., 2011; Naranjo and Casado, 2012; He et al., 2013). As for the group membership management problem, it did not get similar attention. Since group membership management is also a fundamental component in SGC schemes, we present in this survey current works while considering both components. To our knowledge, none of the existing surveys have tackled both of them. In addition, existing surveys either investigate general key management schemes in WSNs (Xiao et al., 2007; Annapurna and Siddappa, 2015) or are limited to a specific type of group key management schemes (Klaoudatou et al., 2011; Naranjo and Casado, 2012; He et al., 2013). Indeed, Xiao et al. (2007) classify schemes according to seven techniques of key management: Single network-wide key, Pairwise key establishment, Trusted base station, Public key schemes, Key predistribution schemes, Dynamic key management, and Hierarchical key managements. As for Klaoudatou et al. (2011) it focuses only on cluster-based approaches. While Naranjo and Casado (2012) address only centralized group key management schemes. He et al. (2013) discuss only centralized and distributed dynamic key management schemes.

This paper first summarizes our contributions in Section 2. Section 3 presents a brief background on SGC. Section 4 provides an overview of existing SGC approaches and discusses their strengths, weaknesses, and performance. Section 5 gives some recommendations on how to select the most appropriate SGC for a given application. Section 6 points out the main challenges and research opportunities of SGC. Finally, Section 7 concludes the survey.

2. Contribution

The motivation of this paper is to present an updated survey of different SGC schemes in WSN. Our first contribution is to study both components (group key management and group membership management) of the different SGC schemes by discussing their performance and efficiency according to several criteria, namely, storage requirements, communication cost, computation cost, network model, the used cryptography type and the key update frequency. Moreover, we study schemes according to the SGC requirements discussed in Section 3. Unlike similar surveys, we classify schemes to three different approaches: centralized, contributory, and hybrid. The second contribution consists of providing readers with recommendations on which scheme to use for specific WSN constraints and specific application requirements. As third contribution, we point out the challenges that researchers have to address while giving them directions to potential solutions.

3. Background on secure group communication

In this section, we present a general background on secure group communication in WSNs. First, we enumerate the possible attacks that can affect group communication in WSNs. Second, we explain the main requirements that a Secure Group Communication (SGC) scheme must achieve to avoid these attacks.

3.1. Group communication attacks

Group communication in WSNs is vulnerable to several attacks due to the inherent characteristics of such networks. In what follows, we enumerate the possible attacks that may target group communication in WSNs (Sakarindr and Ansari, 2007).

- *Replay attack*: An attacker may replay an old message to gain access to a group or to disturb the operation of a group. When an attacker intercepts a successful authentication message of a legitimate member, it can re-send this message in order to gain access to the group. A solution to mitigate the replay attack is to add a sequence number or nonce (random number used once) to the message to prove its freshness (Sakarindr and Ansari, 2007; Venkatraman et al., 2013).
- *Impersonation attack*: An attacker may impersonate another group member's identity to establish a connection or launch other attacks inside the group; the attacker may also use the victim's identity to establish a connection with other nodes or to launch other attacks on behalf of the victim. There are several softwares capable of reprogramming the devices to forge the MAC and network addresses. A solution to mitigate this attack is to authenticate node and messages' source (Sakarindr and Ansari, 2007; Venkatraman et al., 2013).
- *Injecting false message*: An attacker may inject a false message to disturb the operation inside a group. For example, an attacker