Computer Communications 112 (2017) 131–140

Contents lists available at ScienceDirect

Computer Communications

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

Mutual healing enabled group-key distribution protocol in Wireless Sensor Networks

Sarita Agrawal*, Manik Lal Das

Dhirubhai Ambani Institute of Information and Communication Technology Gandhinagar, Gujarat, India

ARTICLE INFO

Article history:
Received 15 March 2017
Revised 14 June 2017
Accepted 22 August 2017
Available online 25 August 2017

Keywords:
Wireless sensor networks
Mutual-healing
Chinese remainder theorem
Authentication

ABSTRACT

The unreliable wireless medium for communication within a Wireless Sensor Network (WSN) necessitates equipping the sensor nodes with shared secrets to protect the communication en-route. In order to establish a dynamic session secret amongst a group of sensor nodes in a WSN, group-key broadcast is found to be a workable solution. However, when a node misses one or more group-key broadcast messages, rebroadcasting results in additional energy consumption at node end and increased network traffic as well. Self-healing mechanism is, therefore, used to recover the lost broadcasts using a future session broadcast. A node, that has missed multiple consecutive broadcasts and does not want to wait for a future broadcast, can obtain the session key through mutual-healing with the help of a neighbor node. In this paper, we present a secure and efficient mutual-healing protocol that uses Chinese remainder theorem(CRT) based secret sharing for group key broadcast. During mutual-healing, mutual authentication and key confirmation are provided. The probability of an unauthorized member retrieving a past session key through self-healing or responding to a mutual-healing request as a neighbor node is shown negligible. The experimental results show that the proposed protocol provides significant performance improvement in terms of computation, communication and storage overhead as compared to existing mutual-healing protocols.

1. Introduction

Wireless Sensor Network (WSN) consists of a large number of tiny sensor nodes. These nodes collaboratively work for a specific task of monitoring some physical or environmental phenomena and provide the information on-request or periodically to base station that is a central trusted authority and a link between external user and the WSN. The nodes in a WSN are resource constrained in terms of communication and computation capability and storage. Usually operated by batteries, these nodes communicate on wireless medium that makes the nodes vulnerable to routing attacks such as worm hole and sink hole. The nodes may also be susceptible to node subversion or node capture attacks due to their unattended deployment in hostile environments for applications such as military battle field surveillance, forest fire detection and so on. For several WSN applications, including health care and battle field surveillance, the information exchanged within the network may demand the secrecy of the information be ensured. Moreover, the communication within the network must happen only amongst the authorized nodes in the network. A node receiving any message should be able to ensure the authenticity of the sender as well as the message. In WSN, the secure communication may happen either via pair-wise secrets [1] that are shared only between a pair of nodes or, by using a common secret that may be shared within a group of nodes. The distribution of secret may happen before deployment or it may take place post-deployment. Group-key broadcast is a commonly used approach to share a group secret to a set of nodes by a central authority [2]. However, the group key broadcast does not serve the purpose in case a node does not receive the broadcast message. Re-broadcasting of the messages is not a cost-effective solution. This issue in group key broadcast got researchers' attention and the self-healing was proposed as a way to help a node obtain the missed broadcast without involving the distribution authority. In self-healing, a node who had missed some broadcast can retrieve the key shared in that broadcast using a subsequent broadcast. Thus, the node need not to send an explicit request to the distributing authority for getting the missed broadcast. For a resource constrained node, saving on the communication cost for an explicit request to distributing authority is significant. However, there is a possibility of a node missing multiple consecutive broadcasts and can not afford to wait for a future broadcast. Also, the node may require to have the current broad-

* Corresponding author.
E-mail addresses: sarita_agrawal@daiict.ac.in (S. Agrawal), maniklal_das@daiict.ac.in (M.L. Das).

http://dx.doi.org/10.1016/j.comcom.2017.08.014
0140-3664/© 2017 Elsevier B.V. All rights reserved.

cast in the current session itself without requesting the same from the distributing authority. In such cases, mutual-healing comes to rescue. With mutual-healing, a node may request its immediate neighbors to share the missing broadcast. A neighbor node, having received the requested broadcast, may respond after ensuring the mutual authentication with the requesting node. The existing mutual-healing protocols [3,4] are based on bilinear pairing that is costly for resource constrained sensor nodes. Since mutual-healing is inevitable in case a node missing a broadcast does not want to wait for future broadcasts, we realized the need of providing mutual-healing to sensor nodes in secure and efficient manner. In this paper, we propose a mutual-healing protocol that uses Chinese remainder theorem based secret sharing for group key broadcast. The proposed protocol provides authentication, resistance to impersonation attack and resistance to replay attack along with secure self-healing and mutual-healing with reduced communication, computation and storage overhead as compared to the existing mutual-healing protocols.

The remainder of the paper is organized as follows. In Section 2 we present the background and the related work. Section 3 describes the proposed protocol in detail. In Section 4, we give security and performance analysis. We conclude the work in Section 5.

2. Background and related work

The concept of mutual-healing in wireless sensor networks was first introduced by Tian et al. in 2011 [3]. They proposed a mutual-healing enabled group-key broadcast protocol using bilinear pairing that allows a node to recover a missed key by taking help of a neighbor node in the same session. Although, mutual-healing in wireless sensor networks is not a widely researched topic, there are numerous self-healing protocols proposed in the literature. Staddon et al. introduced the idea of self-healing group key distribution in [5] that addresses secure group communication in unreliable networks deployed for applications such as military surveillance. Since then, the researchers have proposed various self-healing protocols using exponential arithmetic [5] [6], polynomial based approach [7–9], access polynomials [10] and so on. A detailed survey on self-healing enabled group-key distribution protocols is presented by Rams et al. in [2]. The survey reveals that although polynomial based algorithms are efficient and simple, some information about pre-distributed user data is disclosed and such data can not be re-used. This weakness is not shown in exponent based algorithms, however, as compared to polynomial based protocols, exponent based algorithms are computationally heavy and do not provide backward secrecy. The most efficient one-way hash chain based protocols fail to provide collusion-resistance property. Tian et al. [3] proposed a self-healing protocol that addresses forward secrecy, backward secrecy and collusion resistance, but their protocol demands high computation cost due to bilinear pairing calculations. To reduce the communication overhead in the self-healing protocol given by Tian et al. [3], Hassan et al. [11] proposed hash chain based approach. However, with [11], whenever a new user joins in a session *j*, the seed value is changed and thus an existing valid user does not have any means to retrieve the key for session *j*-1 from session *j* broadcast if a session key broadcast for session *j*-1 is lost. Therefore, mutual-healing is inevitable in such cases.

Self-healing group-key distribution with extended revocation capability is proposed by Rams and Pacyna [12] that requires the nodes to evaluate polynomial for recovering the update polynomial broadcasted by GM and perform exponential computation to obtain the session key. Chen et al. [13] proposed a one-way hash chain based scheme and the authors claim that the scheme provides *mt*-wise forward secrecy, backward secrecy and resistance to *mt*-wise collusion attack (where *m* is total number of sessions and *t* is the maximum number of revoked users). However, Guo et al. [14] identified that in the scheme given by Chen et al. [13], a revoked user is capable of recovering the personal secrets of authorized users of a current session. Therefore, a revoked user has access to the key of the current session for which it is not an authorized member and proposed scheme [13] does not provide forward security and collusion resistance. Wang et al. [15] had proposed a self-healing group key distribution scheme using access-polynomial wherein the self-healing is provided by binding the joining time of a user with its capability to recover group keys of previous sessions. It was claimed that their scheme [15] satisfies all basic security properties namely backward and forward secrecy and resistance to collusion attack. However, Zheng and Guo [16] observed that some revoked users can recover the current session's session key and therefore the Wang et al. scheme [15] does not provide forward secrecy.

LiSH+, a robust and efficient group key management scheme is proposed by Jiang et al. [17] to address the issue of transmission security and availability in Supervisory Control And Data Acquisition (SCADA) group communications. The proposed scheme [17] provides self-healing capability with collusion resistance and *t*-revocation property. The backward and forward secrecy is ensured using a dual direction hash chain. Sun et al. [18] proposed two self-healing key management schemes that are based on modified access polynomial and, provide enhanced collusion resistance and broadcast authentication. The authors have first introduced two different types of attacks that break security of access polynomials. Then, two schemes are proposed and through theoretical analysis the authors validated their schemes to be having δ self-healing capability for the self-healing window size δ. The schemes proposed by Sun et al. [18] avoid the weaknesses of access polynomials and provide enhanced collusion resistance along with forward and backward security. Guo et al. [19] proposed Exponential arithmetic based Self-healing Group Key Distribution (E-SGKD) scheme with backward secrecy and resistance to collusion attack with reduced storage overhead as compared to existing E-SGKD schemes. We note that these self-healing schemes [12–19] do not address the mutual-healing in group key distribution.

Tian et al. [3] proposed the notion of mutual-healing using neighboring nodes in WSN. A node that missed a broadcast message in current session can broadcast an authentication request message to its one-hop neighbors with its own identity, location and the identity of the current session, all in plain forms. Upon receiving such request, a neighbor node verifies that the request is indeed from a one-hop neighbor. The responding node computes a pair-wise key using pre-loaded location based secret, encrypts the current session broadcast with the pair-wise key and respond to mutual-healing request. When response is received, the requesting node verifies the neighbor's location, computes pair-wise key and retrieves the required broadcast. However, both mutual-healing request and response communications in [3] are found vulnerable to known-location attacks as the node location is communicated in plain. The pair-wise key used for authentication purpose is computed using bilinear pairing incurring increased computation overhead. Agrawal et al. [20] proposed an improvement over mutual healing in [3] by reducing the cost overhead and enhancing the security with features of key confirmation and secure node location.

As the basis of the self-healing protocols is group-key broadcast, we studied various group-key broadcast protocols such as in [21–25] and found that the Chinese remainder theorem (CRT) based approach offers light-weight solution to group-key broadcast problem in wireless sensor network, as it uses symmetric-key cryptography. Zheng et al. [26] and Zhou et al. [27] proposed group-key management schemes using CRT. However, they did not con-