Journal of Network and Computer Applications 34 (2011) 80–88

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

# A mutual-healing key distribution scheme in wireless sensor networks

Biming Tian [a], Song Han [a], Jiankun Hu [b,*], Tharam Dillon [a]

[a] DEBI Institute, Curtin University, Perth 6845, Australia
[b] School of Computer Science and IT, RMIT University, Melbourne 3001, Australia

ARTICLE INFO

*Article history:*
Received 22 January 2010
Received in revised form
1 September 2010
Accepted 5 September 2010

*Keywords:*
Sensor network
Security
Self-healing
Key distribution

ABSTRACT

How to establish secure session keys is one of the central tasks for wireless sensor network communications. General key distribution schemes for traditional computer networks could not be directly shifted to wireless sensor network environments as broadcast messages may be lost due to sensor network internal factors or external attacks. Self-healing key distribution schemes, therefore, have been proposed to address packet loss issues since 2002. The essential issue that self-healing key distribution mechanism addressed is the fixed-number of broadcast messages (excluding the last broadcast message) loss. In other words, a node could not recover its new session keys if a node has missed more than a fixed number broadcast messages or the last broadcast message in a self-healing key distribution scheme for wireless sensor networks. This paper aims to address this emerged issue and provide a new key distribution scheme: mutual-healing key distribution scheme for wireless sensor networks. This mutual-healing key distribution can enable a node in a wireless sensor network to recover its new session key although its last broadcast message was lost. A formal definition for mutual-healing key distribution will also be proposed in this paper. The proposed mutual-healing key distribution scheme is based on bilinear pairings. The scheme is collusion-free for any coalition of non-authorized nodes. Each node's private key has nothing to do with the number of revoked nodes and can be reused as long as it is not disclosed. The storage overhead for each node is a constant.



## 1. Introduction

Key management including key distribution and key update is significant for maintaining private communications in any dynamic networks (Balenson et al., 1999; Ku and Chen, 2003; Staddon et al., 2002; Liu et al., 2003; Jiang et al., 2007; Han et al., 2007; Han et al., 2009; Hong and Kang, 2005; Hu and Han, 2009; Hu et al., 2010; Eltoweissy et al., 2004a; Lu et al., 2006; Sufi et al., 2010; Xi et al., 2010). Wireless sensor networks, especially mobile ad hoc networks, as one of dynamic networks, therefore rely on a secure key management. This is because membership frequently changes in large dynamic group communications of wireless sensor networks. In order to keep the security of communications, the session key has to be updated on each membership change. Therefore, one of the important questions is how to distribute and update session keys in a secure and efficient way for large dynamic wireless sensor networks. In recent years, many schemes on distributing session keys for large group communication have been proposed. These existing schemes focused on different key updating mechanism. For example, LKH (Logical Key Hierarchy)-based schemes (Wong et al., 2000) and OFT (One-way Function Tree) based schemes (Balenson et al., 1999; Ku and Chen, 2003) devote to reduce the size of the rekeying message. Broadcast encryption addresses the problem of sending encrypted messages to a large node group so that the encrypted messages can only be decrypted by a dynamic changing privileged subset (Fiat and Tessa, 2001; Halevy and Shamir, 2002; Naor and Pinkas, 2000). EBS (Exclusion Basis System) based approach was proposed in Eltoweissy et al. (2004b), and then be put into use for sensor networks in Eltoweissy et al. (2004a) and Moharrum et al. (2006). The members store less number of keys than LKH tree for the multicast group of the same size. All these literatures supposed that underlying networks are reliable. However, how to distribute session keys for unreliable wireless networks, in a manner that is resistant to packet loss, is an issue that has not been addressed deeply.

Packet loss happens frequently in wireless sensor networks. The key distribution broadcast for a particular session might never reach some nodes. A naive solution is requesting re-transmission. On the one hand, both requesting and re-transmission messages would incur more communication overhead. In a very large communication group, such individual interactions place a heavy burden on the group manager. On the other hand, nodes may reveal their current locations by sending messages in some high security environments. All these issues can be addressed by self-healing key distribution schemes (Staddon et al., 2002; Liu et al., 2003; Blundo et al., 2004; More et al., 2003;

* Corresponding author. Tel.: +61 3 99259793; fax: +61 3 9662 1617.
*E-mail addresses:* biming.tian@cbs.curtin.edu.au (B. Tian), song.han@cbs.curtin.edu.au (S. Han), jiankun@cs.rmit.edu.au (J. Hu), haram.dillon@cbs.curtin.edu.au (T. Dillon).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.09.002