Computer Networks 55 (2011) 2534–2544

Contents lists available at ScienceDirect

Computer Networks

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

A scalable and robust key pre-distribution scheme with network coding for sensor data storage

Rongfei Zeng [a], Yixin Jiang [a], Chuang Lin [a], Yanfei Fan [b], Xuemin (Sherman) Shen [b,*]

[a] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[b] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

ARTICLE INFO

Article history:
Received 12 January 2011
Accepted 23 March 2011
Available online 4 May 2011
Responsible Editor: I.F. Akyildiz

Keywords:
Distributed sensor data storage
Key pre-distribution
Network coding
Matrix decomposition

ABSTRACT

In this paper, we propose a scalable and robust key pre-distribution scheme based on network coding and matrix decomposition for distributed sensor data storage. As a promising information dissemination technique, network coding is suitable for the key information exchange due to the reduced number of transmissions and the enhanced robustness. Matrix decomposition can help to exchange key information without any central nodes and location knowledge. Our scheme uses LU matrix decomposition to decompose a shared key into two vectors R and C. The vector R is held privately by the sensor, while the other vector C is protected and disseminated using network coding. The combination of network coding and matrix decomposition enhances the scalability, improves the communication performance, and increases the robustness for sensor data storage networks. Extensive theoretical analysis and simulative results both demonstrate the efficacy and efficiency of the proposed key pre-distribution scheme in distributed sensor data storage.

1. Introduction

Recently, security and privacy issues have gained increasing attention in distributed sensor data storage [1] which is extensively applied to the reliable and privacy-preserving access to confidential data in wireless sensor networks (WSNs). As an indispensable security and privacy component, key management is in charge of providing shared encryption and authentication keys for securing connections between vulnerable nodes in sensor data storage.

A variety of key management schemes have been proposed in the past few years [2–22]. The traditional trusted-server schemes rely on trusted online servers to establish shared keys between nodes. However, such central online infrastructure may not exist in sensor data storage networks. The self-enforcing schemes depend on asymmetric cryptography (e.g., Diffie–Hellman and RSA [2]) to negotiate pairwise keys, making the self-enforcing schemes infeasible in sensor data storage due to sensors' limited computational and energy resources [3–5]. The key pre-distribution schemes have been demonstrated to be more practical in WSNs [6,7]. Having some key information installed in nodes before deployment, the key pre-distribution schemes can be further classified into three types: the shared-key schemes, the location-aware schemes, and the pairwise schemes with structure key pool. Eschenauer et al. [7] first propose a probabilistic shared-key pre-distribution scheme, the security of which is further enhanced in [8–10]. The group-based and grip-based schemes leverage location knowledge to improve the security and performance [11–13]. The pairwise schemes with structure key pool adopt symmetric matrices, bivariate polynomials, and matrix decomposition in the key pre-distribution [2,14–19]. Recently, Oliveira

* Corresponding author. Tel.: +1 519 888 4567x32691; fax: +1 519 746 3077.
E-mail addresses: zengrf@csnet1.cs.tsinghua.edu.cn (R. Zeng), yxjiang@csnet1.cs.tsinghua.edu.cn (Y. Jiang), clin@csnet1.cs.tsinghua.edu.cn (C. Lin), yfan@bbcr.uwaterloo.ca (Y. Fan), xshen@bbcr.waterloo.ca (Xuemin (Sherman) Shen).

1389-1286/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.03.018

et al. propose an efficient key pre-distribution scheme based on network coding (NC) [20].

However, the previous approaches cannot be directly applied to distributed sensor data storage, since sensor data storage networks have the following unique characteristics: (1) Vulnerable sensors may suffer from Byzantine failures and various attacks (e.g., collusion attacks and node-compromised attacks), thus the key pre-distribution scheme should be robust; (2) The communication bandwidth is more limited than other resources (e.g., memory) in sensor data storage, requiring the key pre-distribution scheme to be communication-efficient; and (3) The central online infrastructure and location information may not be available in sensor data storage [1,23]. In summary, the key pre-distribution scheme should be scalable, robust, efficient, and location-knowledge-free.

In this paper, we propose a robust and scalable key pre-distribution scheme based on network coding and matrix decomposition for distributed sensor data storage. As a promising information dissemination approach, NC is suitable for the key information exchange due to the reduced number of transmissions and the enhanced robustness. Matrix decomposition can be utilized to exchange key information without any central nodes and location knowledge. Our scheme uses LU matrix decomposition to decompose a shared key into two vectors R and C. The vector R is held privately by the sensor, while the other vector C is protected and disseminated using NC. In summary, the combination of network coding and matrix decomposition enhances the scalability, improves the communication performance, and increases the robustness for sensor data storage networks.

Our main contributions are threefold: (1) *Robustness*: We uses NC and matrix decomposition to enhance the robustness of key pre-distribution scheme for sensor data storage in hostile scenarios. The proposed scheme is proved to be secure against node-compromised attacks and resilient against collusion attacks; (2) *Efficiency*: It is demonstrated by theoretical analysis that the performance, such as the expected transmission number and local connectivity, are significantly improved. Compared with the traditional matrix decomposition scheme [14], our scheme remarkably reduces the communication overhead by 25% and guarantees the local connectivity as well; and (3) *Scalability*: The proposed scheme achieves security-enhanced and efficient key dissemination without the need for online central nodes and location information, making the scheme more scalable in distributed sensor data storage. Finally, to the best of our knowledge, this is the first research work to comprehensively consider the robustness, efficiency, and scalability in the key pre-distribution scheme for sensor data storage networks.

The remainder of the paper is organized as follows. Section 2 surveys related work, and Section 3 introduces the system model, threat model, and the preliminaries. In Section 4, we present the proposed scheme based on NC and matrix decomposition. We also present the features and extensions in Section 5. Security analysis and performance evaluations are given in Section 6 and Section 7, respectively. Section 8 concludes the paper.

2. Related work

Key management plays an important role in establishing secure communications in WSNs. In general, there are three types of key management schemes: the trusted-server schemes, the self-enforcing schemes, and the key pre-distribution schemes. Due to the lack of central online infrastructure, the trusted-server schemes cannot be directly applied to WSNs. The self-enforcing schemes depend on asymmetric cryptography, such as Diffie-Hellman and RSA [2], to negotiate pairwise keys. As a novel self-enforcing scheme, the ID-based cryptography enables two nodes to establish their shared keys by performing energy-consuming pairing operations [3–5]. With the increasing number of sensor nodes, the scalability of this scheme is a main concern due to the computation-limited sensors. Some recent work demonstrates that key pre-distribution schemes offer practical solutions to the key management problem in sensor networks [7]. The key pre-distribution schemes can be further categorized into the following types: (1) the shared-key schemes, (2) the location-aware schemes, and (3) the pairwise schemes with structured key pool.

Eschenauer et al. [7] first propose a probabilistic key pre-distribution scheme, which uniformly pre-distributes a large global set of keys so that each node has a key subset in the memory and two neighbors can negotiate a probabilistic key by intersecting their key subsets. Chan et al. extend this classic scheme and present a q-composite scheme to reduce the impact of compromised nodes [8]. The techniques, including key index notification, challenge-response, and pseudo-random key index transformation, have also been used to improve the security and performance in the key discovery phase [9,10].

As the typical location-aware schemes, group-based schemes and grip-based schemes leverage prior deployment knowledge to lower the impact of node-compromised attacks, increase the local connectivity, and reduce storage and computational overheads [11–13]. However, due to the randomness of deployment, obtaining such location information might not be feasible for sensor data storage.

The pairwise key pre-distribution schemes with structured key pool are proposed to improve the resilience against various attacks. Blom et al. propose a novel λ-secure key pre-distribution scheme based on a symmetric matrix of size $(\lambda+1)\times(\lambda+1)$ over $GF(q)$ [15]. Du et al. enhance the security of Blom's scheme by introducing multiple key spaces in [2]. In [30], nodes are organized into a n-dimensional hypercube, and Blundo's polynomial [18] is used in each dimension. The techniques of trivariate and multivariate symmetric polynomials are also applied to the key pre-distribution in WSNs [11,19]. Dai et al. use matrix decomposition and polynomial-based approach to guarantee that any two nodes can negotiate a pairwise key in [14]. Qamtepe et al. present two classes of combinatorial designs, i.e., symmetric balanced incomplete block designs and generalized quadrangles, in the key pre-distribution of WSNs [9]. Recently, network coding has also been applied to the pairwise key pre-distribution scheme