Journal of Network and Computer Applications 82 (2017) 114–127

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A novel key generation method for wireless sensor networks based on system of equations

Furui Zhan, Nianmin Yao*, Zhenguo Gao, Guozhen Tan

Dept. Computer Science and Technology, Dalian University of Technology, Dalian, China

ARTICLE INFO

Keywords:
Key generation
System of equations
Key connectivity
Key management
Wireless sensor networks

ABSTRACT

Many key management schemes were proposed for protecting wireless sensor networks (WSNs). While applying key management to the network, it is important to ensure that the efficiency of the network is not greatly affected by key connectivity. Poor connectivity might lead to many messages forwarding. Consequently, a large amount of energy of the involved nodes would be consumed during message forwarding, which is not suitable for the resources-constraint sensor nodes. In this work, we analyze the impact of key connectivity on the efficiency of communication. Then, a novel key generation method based on system of equations is proposed to improve key connectivity of key management. The involved equations are applied to establish secret keys and each node uses these keys for protecting their communication. The system of equations is constructed to have one and only one solution so that the unique solution can also be used to establish a shared hidden key for enhancing the association among nodes. As a result, neighbors can directly communicate with each other through the shared hidden key even though they do not have common keys. To differentiate from normal keys, keys generated by the proposed method are called associated-keys. According to the analyses, we recommend that systems of linear equations (linear systems) instead of systems of polynomial equations are used to realize the proposed method with respect to the computation complexity. Furthermore, we illustrate that linear systems of two variables are sufficient to generate keys for large scale of networks. The Exclusion Basis System (EBS) is used as a instance to illustrate the implementation of key management with associated-keys. The theoretical analyses and simulation results show that key management schemes with associated-keys have better key connectivity than the corresponding schemes with normal keys. Meanwhile, other performance metrics are unaffected.

1. Introduction

Nowadays, wireless sensor networks (WSNs) are applied into various fields (Rashid and Rehmani, 2015), such as military, transportation and healthcare. In these applications, the efficiency and security of communication are very important. Typically, key management is used as a critical security service for protecting WSNs (Ying et al., 2011).

According to Eltoweissy et al. (2006), a key management process consists of four components: key analysis, key assignment, key generation, and key distribution. The existing key management schemes can be classified into various categories, such as probabilistic schemes and deterministic schemes (Zhang and Varadharajan, 2010; He et al., 2013). For these schemes, key connectivity is an important metric which indicates the ability of secure communication after key management is applied. Accordingly, key connectivity significantly affects the efficiency and security of networks. For many key management schemes, key connectivity is lower than 1. Although key connectivity can achieve 1 in some schemes, these schemes either have many constraints or sacrifice other metrics, e.g., poor scalability or requirement of deployment knowledge. When key connectivity of the applied key management schemes is lower than 1, it is impossible to ensure that common keys can be discovered among all neighbors. As a result, many messages forwarding need to be processed, which leads to consuming a large amount of energy and other precious resources of sensor nodes. What's more, during messages forwarding, the authentication of nodes have to be implemented for guaranteeing the security of these processes. When key management is used for clustered WSNs, the implementation of clustering might be affected if its key connectivity is lower than 1. Therefore, the referred key connectivity is a critical metric of key management.

In this work, we focus on key connectivity of key management. Moreover, to enhance the key connectivity without sacrificing other metrics, a novel key generation method based on system of equations is

* Corresponding author.
E-mail addresses: izfree@mail.dlut.edu.cn (F. Zhan), lucos@dlut.edu.cn (N. Yao), gzg2012@dlut.edu.cn (Z. Gao), gztan@dlut.edu.cn (G. Tan).

http://dx.doi.org/10.1016/j.jnca.2017.01.019
Received 25 March 2016; Received in revised form 15 November 2016; Accepted 18 January 2017
Available online 21 January 2017

proposed. The main contributions of our work are described as follows:

- We analyze the impact of key connectivity on WSNs. Specifically, we illustrate the case where two neighbors, who do not have common keys, want to communicate with each other.
- To enhance key connectivity, we propose a novel key generation method based on system of equations. The system of equations is defined as eligible system (ES) when it has one and only one solution. Each equation in the applied eligible system is applied to generate a secret key for the network. The generated keys are called associated-keys in contrast to normal keys. As a result, the unique solution can be used to establish a shared hidden key for nodes and neighbors can establish secure link by the shared hidden key even when they do not have common keys. Both system of polynomial equations and system of linear equations are illustrated to implement the proposed method. Taking into account computation complexity, we recommend to use system of linear equations to generate secret keys for the network.
- We use linear system of two variables to illustrate the implementation of the proposed method and use the generated keys to achieve key management. Moreover, the Exclusion Basis System (EBS) (Eltoweissy et al., 2004) in conjunction with associated-keys is used as an instance of key management system.
- The theoretical analyses and simulations are conducted to evaluate the proposed method. During simulations, associated-keys are applied into different EBS (Eltoweissy et al., 2004) and Unital schemes (Bechkit et al., 2013) to create new key management schemes. Then, these schemes are compared with the corresponding schemes with normal keys. The results show that the proposed method can be used to enhance key connectivity of key management without sacrificing other metrics.

The remainder of this paper is organized as follows: in Section 2, we review the related work on key management. The impact of key connectivity is analyzed in Section 3. The key generation method based on system of equations is illustrated in Section 4. Section 5 describes the implementation of the proposed method. In Section 6, simulations are conducted to evaluate the performance of the proposed method. Finally, the conclusions of this work are described in Section 7.

2. Related work

Many key management schemes have been proposed for WSNs. Although some schemes apply asymmetric cryptography were proposed (Malan et al., 2004; Rajendiran et al., 2011; Nam et al., 2014), most schemes applied symmetric cryptography with respect to computation complexity and energy consumption. In this section, only the key management schemes based on symmetric cryptography are described.

2.1. RKP and RKP-based schemes

Eschenauer and Gligor proposed a random key pre-distribution scheme (RKP scheme) for wireless sensor networks (Eschenauer and Gligor, 2002). The scheme consists of three components: key pre-distribution, shared-key discovery and path-key establishment. In key pre-distribution phase, a large key pool is initialized and the identifiers of keys are determined. Each node randomly selects k keys to store. In the shared-key discovery phase, each node exchanges the identifiers of keys with neighbors and identifies the shared keys with neighbors. The path-key establishment phase is implemented if the shared keys cannot be found between the communicating parties. In this phase, several intermediate nodes capable of directly communicating with them are selected to accomplish the communication. This scheme is energy efficient, but the storage overheads are high. The key connectivity of this scheme can be figured out as

$$p' = 1 - \frac{(1 - \frac{k}{|S|})^{2(|S|-k+\frac{1}{2})}}{(1 - \frac{2k}{|S|})^{(|S|-2k+\frac{1}{2})}}$$

where $|S|$ denotes the size of key pool, and k is the number of keys stored in each node. p' is the key connectivity of this scheme. It can be found that the resulting connectivity is lower than 1.

Based on Eschenauer and Gligor (2002), Chan et al. proposed a modified scheme called q-composite keys scheme (Chan et al., 2003). In this solution, neighbors can establish a secure link only if they share at least q keys and thus the resilience against node capture is enhanced. In Du et al. (2003), a key pre-distribution scheme that combined the RKP scheme and Blom's scheme (Blom, 1985) was proposed to improve the resilience against node capture. Similarly, a key pre-distribution scheme based on the RKP scheme was proposed in Liu et al. (2005), where bivariate t-degree symmetric polynomials instead of matrix were used to generate shared keys between nodes.

2.2. EBS and EBS-based schemes

The Exclusion Basis System (EBS) is a combinatorial optimization methodology for group key management scheme (Eltoweissy et al., 2004). In EBS, each node is assigned k keys out of a pool of size $P = k + m (1 < k, m < n)$, where P is the size of key pool and n denotes the size of the network. That is, m keys are unknown to each node. According to Eltoweissy et al. (2004), the referred parameters have to meet the relationship $\binom{k+m}{k} \geq n$. As a result, if a node is compromised, this node can be evicted by broadcasting the rekeying messages which contain the replacement of k exposed keys and are encrypted by the corresponding m unknown keys. Consequently, the key system is updated.

Younis et al. proposed a location-aware dynamic key management scheme based on EBS (Younis et al., 2006). With the deployment information, the resilience can be enhanced by decreasing the Hamming distances of key strings stored by neighbors. In Eltoweissy et al. (2006), a novel dynamic key management scheme was proposed, which is called localized combinatorial keying (LOCK). This scheme is implemented in clustered WSNs and the polynomial keys are applied to enhance the resilience of key management. Besides, several key management schemes based on EBS have been proposed (Moharrum et al., 2006; Ying et al., 2011; Lo et al., 2009; Syed et al., 2010).

Comparing with RKP-based schemes, EBS-based schemes can efficiently evict the compromised node and update the key system. Therefore, these schemes can provide long-term and flexible protection for WSNs.

2.3. Combinatorial design schemes

Several key management schemes based on combinatorial design were proposed (Camtepe and Yener, 2007; Ruj et al., 2011, 2013; Bechkit et al., 2013). In Camtepe and Yener (2007), Camtepe et al. proposed a key pre-distribution scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). The SBIBD scheme performs good key connectivity. However, this scheme cannot be used for large scale networks. Pairwise and triple key distribution schemes were proposed by Ruj et al. in Ruj et al. (2011), where Steiner trade is applied for key establishment. The scheme is highly resilient against node capture attacks. In Bechkit et al. (2013), Bechkit proved that Ruj's scheme provided a low session key sharing probability and then proposed a new scheme based on unital design theory. The scheme provides high network scalability and good key sharing probability approximately lower bounded by $1 - e^{-1}$. Comparing with random key pre-distribution schemes, the key connectivity in combinatorial design schemes is improved. However, the construction of appropriate a combinatorial design for the given network. In addition, these schemes do not have