Computer Networks 55 (2011) 1849–1863

Contents lists available at ScienceDirect

Computer Networks

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

A high performance and intrinsically secure key establishment protocol for wireless sensor networks

Ali Fanian [a,*], Mehdi Berenjkoub [a], Hossein Saidi [a], T. Aaron Gulliver [b]

[a] Department of Electrical and Computer Engineering Isfahan University of Technology (IUT) Isfahan, Iran
[b] Department of Electrical and Computer Engineering University of Victoria Victoria, BC Canada

ARTICLE INFO

Article history:
Received 1 April 2010
Received in revised form 16 December 2010
Accepted 25 January 2011
Available online 11 February 2011
Responsible Editor: J. Misic

Keywords:
Wireless sensor networks
Key management
Network security
Random key pre-distribution
Symmetric polynomials
Deployment knowledge

ABSTRACT

Key establishment among neighboring sensors is the most challenging issue for security services such as authentication and confidentiality in wireless sensor networks (WSNs). Many key establishment schemes have recently been proposed, but most have security or performance issues. In this paper, we propose a novel key establishment protocol which is suitable for low resource sensor nodes. In this protocol, each sensor has a secret key and some common keys with other sensors. A common key between two sensors is generated using the secret of one sensor and the identity of the other. This key is stored in one of the sensors, and the other sensor generates it when a secure connection is required. We develop the proposed protocol for different key distribution models. These models use pre-deployment knowledge to distribute the common keys among sensors. The proposed scheme is analyzed based on connectivity, scalability, memory consumption and resistance against attacks. In comparison with previous approaches, the proposed protocol is the most resilient against compromised node attacks. In addition, it has low memory requirements and low computational overhead.

1. Introduction

Wireless sensor networks usually comprise a number of sensors with limited resources. Each sensor includes sensing equipment, a data processing unit, a short range radio device and a battery [1–3]. These networks have been considered for various purposes including border security, military target tracking and scientific research in dangerous environments [4–6]. Since the sensors may reside in an unattended and/or hostile environment, security is a critical issue. An adversary could easily access the wireless channel and intercept the transmitted information, or distribute false information in the network. Under such circumstances, authentication and confidentiality should be used to achieve network security. Since authentication and confidentiality protocols require a shared key between entities, key management is one of the most challenging issues in wireless sensor networks (WSNs) [4].

In the literature, key management protocols are based on either symmetric or asymmetric cryptographic functions [4]. Due to resource limitations in the sensors, key management protocols based on public keys are not suitable [4,8]. Hence, key management protocols based on symmetric cryptographic functions have been extensively investigated [8–29]. There are two types of symmetric key management schemes based on an on-demand trust center or key pre-distribution. With an on-demand trust center, the center must generate common keys for every pair of nodes that wish to establish a secure connection. Due to the lack of an infrastructure in WSNs, this scheme is not suitable. With key pre-distribution, key material is distributed among all nodes prior to deployment. In this scheme, each node carries a set of keys to establish a secure connection with other nodes.

[*] Corresponding author.
E-mail addresses: Fanian@ec.iut.ac.ir (A. Fanian), Brnjkb@cc.iut.ac.ir (M. Berenjkoub), hsaidi@cc.iut.ac.ir (H. Saidi), agullive@ece.uvic.ca (T. Aaron Gulliver).

1389-1286/$ - see front matter Crown Copyright © 2011 Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2011.01.016

A number of key pre-distribution schemes have been developed. A very simple approach is to have a unique pre-loaded key that is shared among the nodes. Then all sensors can encrypt or decrypt data between themselves using this key. Due to its simplicity, this method is very efficient in regards to memory usage and processing overhead, but it suffers from a very serious security problem. If even one of the sensors is captured by an adversary, the security of the entire network will be compromised. Another simple approach, called the basic scheme, is to generate a distinct key between every pair of sensors and store these in the sensors. In this case, if N sensors are deployed in the network, each must store $N - 1$ keys. Despite ideal resilience, this scheme is not scalable, and is not memory efficient, particularly in large networks. In addition, after node deployment, if a new node wants to join the network, none of the previously deployed sensors will have a common key with the new node. Recently, many key establishment protocols have been proposed to address this problem [8–29], but as we will show most have security or performance issues. These schemes are based on random key pre-distribution, symmetric polynomials and/or the Blom scheme. As shown in the analysis section, with the protocols based on random key pre-distribution, an adversary can obtain the common key between non-compromised sensors by compromising some sensors. Thus, these schemes have a serious security problem. In the symmetric polynomial and/or Blom scheme, however, perfect security can be achieved but resource consumption is an issue. In this paper, we propose a novel key establishment protocol employing four key pre-distribution models for sensor networks with different requirements.

The rest of the paper is organized as follows. Section 2 reviews some required primitives including related work. Details of our key establishment protocol are discussed in Section 3. Performance evaluation and security analysis of the proposed protocol are presented in Section 4. Finally, some conclusions are given in Section 5.

2. Related work

Most of the proposed key establishment protocols in WSNs are based on random key pre-distribution, symmetric polynomials and/or the Blom scheme. In this section, we review some well known protocols based on these techniques.

2.1. Key establishment protocols based on random key pre-distribution

Eschenauer et al. [9] proposed a random key pre-distribution scheme for WSNs. In this approach, before deployment some keys from a large key pool are selected randomly and stored in the sensors. After deployment in the network, a pair of nodes may have a shared common key to establish a secure connection. If there is no common key between two sensors, they have to establish a key through an intermediate sensor node which has common keys with both sensors. In this method, there is a tradeoff between connectivity and security. Network connectivity is determined from the probability of direct key generation between two adjacent sensors. As the size of the key pool increases, connectivity decreases, but protocol security increases. Due to the distribution of random keys, it may not be possible to establish a common key between every pair of sensors.

Du et al. [10] proposed a deployment knowledge key management protocol (denoted Du-1), based on the approach in [9]. In this case, deployment knowledge is modeled using a Gaussian probability distribution function (pdf). Methods which do not use deployment knowledge such as in [9], assume a uniform pdf for the node distribution in the network. In this case, sensors can reside anywhere in the network with equal probability. In [10], the network area is divided into square cells and each cell corresponds to one group of sensors. The key pool is divided into sub key pools of size S, one for each cell, such that each sub key pool has some correlated keys with its neighboring sub key pools. Each sub key pool has αSc common keys with the horizontal and vertical neighboring sub key pools, and βSc common keys with the diagonal neighboring sub key pools, such that $4\alpha + 4\beta = 1$, with $\alpha > \beta$. Each sensor in a cell randomly selects m_R keys from its associated sub key pool.

2.2. Key establishment protocols based on symmetric polynomials

A symmetric polynomial [11–13] is a t-degree $(K + 1)$-variate polynomial defined as follows

$$f(x_1, x_2, \dots, x_{K+1}) = \sum_{i_1=0}^{t} \sum_{i_2=0}^{t} \dots \sum_{i_{k+1}=0}^{t} a_{i_1, i_2, \dots, i_k, i_{k+1}} \times x_1^{i_1} x_2^{i_2} \dots x_K^{i_K} x_{K+1}^{i_{K+1}}. \tag{1}$$

All coefficients of the polynomial are chosen from a finite field Fq, where q is a prime integer. The polynomial f is a symmetric polynomial so that [13]

$$f(x_1, x_2, \dots, x_{K+1}) = f(x_{\partial(1)}, x_{\partial(2)}, \dots, x_{\partial(K+1)}), \tag{2}$$

where ∂ denotes a permutation. Every node using the symmetric polynomial based protocol takes K credentials $(I_1, I_2, \dots, I_K)$ from the key management center, and these are stored in memory. The key management center must also compute the polynomial shares using the node credentials and the symmetric polynomial. The coefficients b_i stored in node memory as the polynomial share are computed as follows

$$f_u(x_{K+1}) = f(I_1, I_2, \dots, I_K, x_{K+1}) = \sum_{i=0}^{t} b_i x_{K+1}^{i}. \tag{3}$$

Every pair of nodes with only one mismatch in their identities can establish a shared key. Suppose the identities of nodes u and v have one mismatch in their identities $(c_1, c_2, \dots, c_{i-1}, u_i, c_{i+1}, \dots, c_K)$ and $(c_1, c_2, \dots, c_{i-1}, v_i, c_{i+1}, \dots, c_K)$, respectively. In order to compute a shared key, node u takes v_i as the input and computes $f_u(v_i)$, and node v takes u_i as the input and computes $f_v(u_i)$. Due to the polynomial symmetry, both nodes compute the same shared key. In [13] it was shown that in order to maintain perfect security in the WSN, the polynomial degree must satisfy