Available online at www.sciencedirect.com

ScienceDirect

October 2017, 24(5): 16–22
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.bupt.edu.cn

New key pre-distribution scheme using symplectic geometry over finite fields for wireless sensor networks

Chen Shangdi[1] (✉), Wen Jiejing[2]

1. College of Science, Civil Aviation University of China, Tianjin 300300, China
2. The Chern Institute of Mathematics, Nankai University, Tianjin 300071, China

Abstract

To achieve secure communication in wireless sensor networks (WSNs), where sensor nodes with limited computation capability are randomly scattered over a hostile territory, various key pre-distribution schemes (KPSs) have been proposed. In this paper, a new KPS is proposed based on symplectic geometry over finite fields. A fixed dimensional subspace in a symplectic space represents a node, all 1-dimensional subspaces represent keys and every pair of nodes has shared keys. But this naive mapping does not guarantee a good network resiliency. Therefore, it is proposed an enhanced KPS where two nodes have to compute a pairwise key, only if they share at least q common keys. This approach enhances the resilience against nodes capture attacks. Compared with the existence of solution, the results show that new approach enhances the network scalability considerably, and achieves good connectivity and good overall performance.

Keywords pre-distribution scheme, symplectic geometry, WSNs

1 Introduction

Recent advances in micro-electro-mechanical systems and low power and highly integrated electronic devices have led developments and the extensive application of WSNs [1–2], which integrate wireless communication technology. Sensing technology and computer technology are considered as one of the most important technologies in the 21th century.

1.1 WSNs

Sensor networks consist of many tiny and inexpensive sensing devices, which have low battery power, low computational speed, limited memory capability and limited resources, and are scattered randomly in large numbers over a target area. They are increasingly used in numerous fields such as military, medical and industrial sectors. They are more and more involved in several sensitive applications which require sophisticated security services. Due to the resource limitations, existing security solutions for conventional networks could not be used in WSNs. So the security issue has become one of the main challenges for the resource constrained environment of WSNs.

Key management is a corner stone service for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is a challenging problem in WSNs. Based on public key solution, it provides efficient key management service in traditional networks, which is not suitable for WSNs because of limited resources.

1.2 KPSs for WSNs

Since this communication is taking place in a hostile environment, encryption should be used to achieve communication securely. In application, secure communication among sensor nodes requires authentication privacy and integrity. This requires that some security keys must

Received date: 26-06-2017
Corresponding author: Chen Shangdi, E-mail: 11csd@163.com
DOI: 10.1016/S1005-8885(17)60229-2

be established among the various nodes of the WSNs. There are three ways to establish pairwise secret keys between sensor nodes.

One method is to establish secret keys using public key protocols such as key agreement schemes. However, public key cryptography is generally regarded as being unsuitable in this setting due to expensive computational costs. Furthermore, public key cryptographic protocols such as authenticated key exchange requires a public key infrastructure which would impose additional computational overhead as well as increased storage requirements.

Another strategy is to have a trusted server, which can communicate with all nodes in the network. The trusted server shares a long-live key with every node and transmits session keys to sensor nodes on request, e.g., using Kerberos. This method can result in expensive costs for message relay, and it may not maintain a secure trusted server.

The third approach, which is the approach most commonly recommended for WSNs and followed in this paper, is to employ KPSs, where secret keys are installed in each node before the sensor nodes are deployed. The keys stored must be carefully selected in order to increase the probability that two neighboring sensor nodes have at least one common key.

A practical solution must find a suitable trade off between storage requirements and resiliency, i.e., security. A common approach is to give each node a different subset of keys chosen from a certain key space. There are three basic operations that need to be implemented: key pre-distribution, shared key discovery and path key establishment. Shared key discovery refers an algorithm that two neighboring nodes will use to determine if they share a common pairwise key or if they construct a shared pairwise key from their common shared information. When two nodes do not share a common pairwise key, they may use p paths, where each pair of nodes on the path share keys. A average path key length is an important performance metric and design consideration.

1.3 Related work

Eschenauer et al. [3] proposed a random KPS, where tens to hundreds of keys are uploaded to sensors before their deployment. The scheme defined a large key pool P and their identities are generated. Every node in the network receives a different random k-subset of k keys from P and their identities. If two sensor nodes share at least one common key, they can communicate securely. Furthermore, if two nodes share more than one common key, then they can choose any one of the common keys as their pairwise key. This scheme does not guarantee that any two nodes will be able to communicate directly.

Chan et al. [4] stipulated that two nodes will compute a pairwise key only if they share at least q common keys. The integer q is a prespecified intersection threshold. Given two nodes which have at least q common keys, they can use all their common keys to compute their pairwise key by means of an appropriate key derivation function.

In Ref. [5–6], the use of combinatorial designs in key pre-distribution sensor networks was first proposed by Camtepe et al. Ref. [6] proposed a deterministic pairwise KPS based on projective planes and generalized quadrangles. One limitation of this approach is that the network size is limited by the number of blocks in the set system.

Based on transversal designs, Lee et al. [7–8] gave a construction and a comprehensive account of key assignment schemes.

Mausumi et al. [9] proposed a general construction method for any given intersection threshold q ($q \geqslant 1$), and it is seen that for the case $q=1$, their construction covers the linear scheme of Lee et al.

Using unital design theory, Walid et al. [10] proposed that the basic mapping from unital design to KPSs gave birth to an extremely highly scalable scheme while providing low probability of sharing common keys.

Michelle et al. [11] showed some ways, in which graph theory can be used to support the design and analysis of KPSs.

Using t-design and combine two ω-key distribution patterns (KDPs), Chen et al. [12] gave a new ($\omega-1$)-KDP, which can provide secure communication in a large network and minimize the amount of key storage.

In this paper, 2ν-dimensional symplectic spaces are used over finite fields to construct a KPS for WSNs. An m-dimensional subspace in 2ν-dimensional symplectic spaces represents a node and all 1-dimensional subspaces, which are orthogonal to the m-dimensional subspace, represent the keys belonging to this node.

This paper is organized as follows. In Sect. 2, the mathematical structures are presented. In Sect. 3, some methods for constructing KPSs are proposed, and a creating key identifiers algorithm and a shared key