A Computationally-Efficient Construction for the Matrix-Based Key Distribution in Sensor Network

Abedelaziz Mohaisen, Nam-Su Jho, and Dowon Hong

Cryptography Research Team, Information Security Division  
Electronics and Telecommunication Research Institute  
Daejeon 305-700, Korea  
{a.mohaisen,nsjho,dwhong}@etri.re.kr

Abstract. Key pre-distribution in wireless sensor network is aimed at delivering keys to sensor networks at the low expense of computation, communication, and memory while providing a high degree of security expressed by network resiliency to node capture. In this paper, we introduce a computationally efficient construction for the symmetric matrix-based key distribution. Particularly, this work introduces an original modification over the well known DDHV scheme (by Du et al.). Our modification shows that using a specific structures for the public matrix instead of fully random matrix with elements in $\mathbb{Z}_q$ can reduce the computation overhead for generating the key information and the key itself at the expense of small memory overhead. Our modification guarantees the same level of security for restricted network size. We show an extensive security analysis of the provided scheme in different settings and compare to the relevant works in the literature to demonstrate its merit.

Keywords: wireless sensor network, key distribution, computation efficiency, security.

1 Introduction

The security of wireless sensor network (WSN) is a challenging issue where both asymmetric (public) and symmetric key based algorithms are considered as possible solutions. However, because the public key based algorithms on the typical sensor nodes still require considerable amount of computation that is translated into processing time, symmetric key based algorithms that utilize the same key at the side of the sender and the receiver are favored for security the WSN. Particularly, these algorithms are shown to be computationally light and appropriate for sensors nodes. To use such algorithms in WSN, symmetric keys need to be distribution among the legitimate nodes in the network. However, because of the

* This work was supported by the IT R&D program of MIC/IITA. [2005-Y-001-05, Development of next generation security technology].

** Corresponding Author.
WSN’s frail infrastructure, traditional symmetric key distribution schemes that utilize key distribution centers (KDC) or trust third part (TTP) are obviously infeasible. To make the use of these algorithms in WSN possible, the concept of key pre-distribution (KPD) has emerged. In KPD, set of keys or keying materials are assigned to each node and used at the running time of the network to ensure secure communication. Several KPD schemes have been introduced in the literature for securing WSN. These schemes range from the graph-based cryptographic keys assignment such like the works by Eschenauer et al. in [1], Chan et al in [2], Hwang et al. in [3], Çamtepe et al. [4] and Mohaisen et al. in [5] to the more sophisticated online key generation schemes such like works by Du et al in [6], Liu et al. in [7] and [8], Mohaisen et al in [9] and [10], among others. In this paper, we review some of these schemes and provide a construction based on one of it to reduce its resources’ consumption while maintaining the same level of security and connectivity.

Our original contribution in this article is a construction based on DDHV scheme [6] to reduce the used computation overhead at the expense of small communication and memory overhead. Our contributions therefore are summarized as follows: (1) We introduce a special construction for the public matrix used in [6] that reduces the computation overhead with a small additional communication and memory overhead which are yet comparable to other schemes. (2) We show a concrete evaluation for the soundness of the scheme, the security achieved and the resources evaluation. (3) To show a comparison between the modified DDHV scheme (OR-DDHV) and the original work, we introduce an extensive study that compares both schemes along with a few others from the literature with instantiated network scenarios and parameters.

The rest of this paper is organized as follows: section 2 introduces an overview of DDHV scheme followed by our scheme in section 3, section 4 introduces the analysis of both schemes where we show the overhead evaluation in terms of communication, computation and memory followed by the security analysis. Finally, section 5 draws a concluding remarks.

## 2 Overview of DDHV Scheme

The DDHV scheme in [6] utilizes Blom’s linear construction in [11] with Eschenauer and Gligor’s random key assignment concept in [1]. Both DDHV and Blom’s schemes are based on the symmetry property of matrices to provide symmetric pairwise keys for the pairs of communicating nodes. DDHV scheme differs from the Blom scheme in that it utilizes multiple spaces for generating the key. In this paper, we will explain the discuss the symmetric matrix-based component of DDHV since our modification is directly related to it. Also, modifications applied on the core of DDHV scheme can be utilized for the multiple space case.

Basically, a symmetric matrix of size $N \times N$ can be used for storing the different $N^2$ keys used for securing communication within the entire network of size $N$ where each node $s_i$ can have a row in that matrix. If two nodes $s_i$ and $s_j$ would like to communicate securely, they use the corresponding elements to