Ad Hoc Networks 73 (2018) 40–50

Contents lists available at ScienceDirect

Ad Hoc Networks

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

# Key predistribution schemes for wireless sensor networks based on combinations of orthogonal arrays☆

Qiang Gao[a,b,*], Wenping Ma[b], Wei Luo[b]

[a] College of Mathematics and Information Science, Henan Normal University, Xinxiang, 453007, China
[b] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China

ARTICLE INFO

*Article history:*
Received 21 December 2016
Revised 6 November 2017
Accepted 14 February 2018
Available online 15 February 2018

*Keywords:*
Wireless sensor network
Key predistribution scheme
Combinatorial design
Orthogonal array

ABSTRACT

In general, combinatorial key predistribution schemes (KPSs) have higher local connectivity but lower resilience against a node capture attack than random KPSs for a given key storage. We seek to find an approach to improving the weakness of combinatorial KPSs while maintaining the strength as much as possible. In this paper, by combining a class of saturated symmetric orthogonal arrays (OAs), a family of KPSs are proposed and the explicit formulas for local connectivity and resilience of the resulting KPSs are also derived. KPSs are typically designed to provide a trade-off between the key storage, the local connectivity and the resilience. It is found that in the resulting schemes, any two nodes can communicate directly with each other and for a given key storage, the resilience against node capture increases as the number of OAs increases so that the resilience can be enhanced without degrading the other two metrics.



## 1. Introduction

WSNs have a wide range of applications [1], including environmental monitoring, health care, traffic control, target tracking and military purposes and so on. These applications require that communications in WSNs must be secure. However, the sensor nodes in WSNs have restricted resources such as battery power, storage and computational capabilities and so on. Hence, for many WSNs, public key cryptography is unsuitable due to its expensive computational costs. A recommended approach is to make use of a KPS, where secret keys are installed in each sensor node before deployment.

In the seminal paper [13], Eschenauer and Gligor proposed a probabilistic KPS, commonly called the basic scheme. In the seminal scheme of Eschenauer and Gligor, there are three phases: key predistribution, shared-key discovery and path-key establishment. First, a large pool of keys and their key identifiers are generated. Then a fixed number of keys randomly chosen from the key pool, along with their key identifiers, are stored in each sensor node prior to deployment. After deployment of the WSN, any two sensor nodes in communication range look for their common keys. If they share one or more common keys, they can select one of them as their secret key or use all of them to compute a pairwise secret key for cryptography communication. A successive sequence of nodes is called a path, where any two adjacent nodes share at least one common key. If a pair of nodes within wireless communication range do not share any key, they need to find a path between them to ensure that they can communication in an encrypted form. The $\eta$-composite scheme, a generalization of the basic scheme, was proposed by Chan, Perring and Song [8]. In this scheme, two nodes will compute a pairwise key only if they share at least $\eta$ common keys, where the integer $\eta \geq 1$ is a pre-specified intersection threshold. (In the basic scheme, $\eta = 1$.) Çamtepe and Yener [6] first proposed the use of combinatorial designs in key predistribution for sensor networks, using symmetric balanced incomplete block design (in particular, finite projective planes (FPPs)) and generalized quadrangles (GQs). Many researchers appreciated the advantages of combinatorial KPSs and continued to further develop this area. Some related work is presented in Table 1. For more details on other approaches the readers can refer to [7,9,26,27,31] for a brief survey.

Due to the limited resources at each sensor, KPSs are typically designed for WSNs to provide a trade-off between three conflicting metrics which are widely used to analyse KPSs. The three metrics are the key storage requirement for each node, the local connectivity and the resilience. Compared to random KPSs, combinatorial KPSs typically have higher local connectivity and lower resilience against node capture for a given key storage. To improve the weakness of combinatorial KPSs, we propose a family of KPSs based on combinations of a class of saturated symmetric OAs. In

☆ This work was supported by National Science Foundation of China under grant No. 61373171 and The 111 Project under grant No. B08038.

* Corresponding author.
*E-mail addresses:* gaoqiang8612@126.com (Q. Gao), wp_ma@mail.xidian.edu.cn (W. Ma), rovid008@163.com (W. Luo).

https://doi.org/10.1016/j.adhoc.2018.02.006
1570-8705/

**Table 1**
Some related work.

| Schemes | References |
|---|---|
| Blom's method based on matrices | [2] |
| Method by Blundo et al. based on polynomials | [3] |
| The basic scheme | [13] |
| $\eta$-composite scheme | [8] |
| Two pairwise KPSs by using sensors' expected locations | [23] |
| KPSs based on FPPs and GQs | [6] |
| ID-based one-way function schemes, multiple space Blom's scheme | [20] |
| Combinatorial constructions for KPSs | [21] |
| KPSs based on polynomial pools | [24] |
| KPSs based on partially balanced incomplete block designs (PBIBDs) | [32] |
| KPSs based on 3-designs | [10] |
| KPSs based on OAs | [11] |
| KPSs based on transversal designs (TDs) | [16,22] |
| Group-based KPSs | [25,28] |
| KPSs based on rational normal curves | [30] |
| Hash chain-based schemes | [12,19] |
| KPSs by combining $\eta$ designs | [4] |
| KPSs based on partially balanced $t$-designs (PB$t$Ds) | [29] |
| Broadcast-enhanced KPSs | [18] |
| KPSs based on graph theory | [17] |

the KPSs based on this class of saturated symmetric OAs, any pair of nodes can communicate with each other directly. In the resulting schemes, the local connectivity is maintained and for a given key storage , the resilience increases as the number of OAs increases. That is, one can enhance the resilience against a node capture attack while maintaining the other two metrics.

The rest of this paper is organized as follows. In Section 2, some basics on combinatorial KPSs are provided. Section 3 presents a family of KPSs based on combinations of OAs and the expressions for the metrics of the resulting KPSs. In Section 4, some examples are given to illustrate the applications of the formulas. In Section 5, we analyze the resulting KPSs and compare them with some existing ones. Finally, the conclusion of this paper is described in Section 6.

## 2. Preliminaries

In this section, we revisit some related theoretic background which will be used throughout the rest of the paper. First, we begin with definition of a design.

### 2.1. Combinatorial KPSs

**Definition 2.1** [33]**.** A design is a pair $(X, \mathcal{A})$ such that the following properties are satisfied:

1. $X$ is a set of elements called points, and
2. $\mathcal{A}$ is a collection (i.e., multiset) of nonempty subsets of X called blocks.

The degree of a point $x \in X$ is the number of blocks containing $x$. $(X, \mathcal{A})$ is regular if all points have the same degree. The rank of $(X, \mathcal{A})$ is the size of the largest block. $(X, \mathcal{A})$ is said to be uniform if all blocks have the same size.

Any combinatorial design can be used to establish a KPS for a sensor network. Assume the sensor network has $b$ sensor nodes denoted by $N_1, N_2, \ldots, N_b$. Suppose that $X = \{x_1, x_2, \ldots, x_v\}$ and $\mathcal{A} = \{A_1, A_2, \ldots, A_b\}$. We identify the $v$ points in $X$ and the $b$ blocks in $\mathcal{A}$ with a set of $v$ keys and the $b$ sensor nodes, respectively. That is, for $1 \le i \le v$, a key $K_i$ is chosen uniformly at random from some specified key space, then, for $1 \le j \le b$, the sensor node $N_j$ receives the set of keys $\{K_i | x_i \in A_j\}$. Then the sensor nodes are deployed randomly over a certain area.

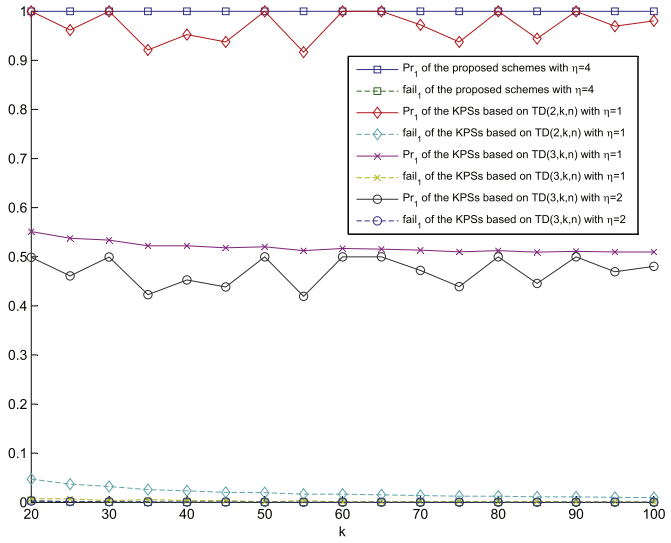


**Fig. 1.** Plot of the values of $Pr_1$ and $fail_1$ of the proposed KPSs with $\eta = 4$ and the KPSs based on TD($t$, $k$, $n$)s, where $n$ is the smallest prime power such that $n \ge k - 1$.

After deployment, if two nodes are within each other's communication range and have at least $\eta$ common keys, then they can communicate with each other securely and directly. To improve the resilience of KPSs, all the common keys shared by a pair of nodes are used to compute secret key. Assume that $K_{a_1}$, $K_{a_2}$, ..., $K_{a_c}$ are the common keys shared by two nodes $N_i$ and $N_j$, where $a_1 < a_2 < \cdots < a_c$ and $c \ge \eta$. Then they can compute the secret key which is used to secure the communication between them,

$$K_{ij} = h(K_{a_1} \parallel K_{a_2} \parallel \cdots \parallel K_{a_c} \parallel i \parallel j),$$

using an appropriate key derivation function $h$.

We assume that an adversary compromises each node with equal probability in this paper. An adversary can compromise some sensor nodes in the network randomly and learn the keys stored in them. For the combinatorial KPSs, after the compromise of $s$ random nodes corresponding to $s$ blocks $B_1$, $B_2$, ..., $B_s$, a link formed by a pair of nodes corresponding to two blocks $A_1$ and $A_2$ such that $|A_1 \cap A_2| \ge \eta$ will be broken if for $1 \le u \le s$ and $1 \le v \le 2$, $B_u \ne A_v$ and

$$A_1 \cap A_2 \subseteq \bigcup_{u=1}^{s} B_u.$$

### 2.2. Main metrics of KPSs

In a KPS, there are mainly four metrics for evaluating it.

*Size of network.* The network size is the number of nodes in the network. A combinatorial design having $b$ blocks can be used to construct a KPS for a network having no more than $b$ nodes.

*Key storage.* The key storage is the number of keys stored in each node. For a combinatorial KPS, the number of keys stored per node is equal to the rank of the design, commonly denoted by $k$. We want to minimize key storage.

*Network connectivity.* We usually consider the local connectivity since the locations of nodes are typically unknown. It is usual to measure local connectivity of networks by computing the probability that a randomly chosen pair of nodes form a link (i.e. share $\eta$ common temporal keys). This probability is commonly denoted by $Pr_1$. It is usually desirable to maximize connectivity.