International Journal of Engineering and Applied Physics (IJEAP)
Vol. 1, No. 1, January 2020, pp. 1~8
ISSN: 2737-8071

A Review on Key Pre-distribution Schemes based on Combinatorial Designs for Internet of Things Security

Otmane EL MOUAATAMID[1], Mohamed LAHMER[2], Mostfa BELKASMI[3]
[1,3] ICES Team, Computer Science Department, National School of Computer Science and Systems Analysis (ENSIAS), Mohammed V University in Rabat
[2] Department of Computer, Information and Communication Systems Engineering Research Group, Higher School of Technology, Moulay Ismail University

Article Info

Article history:

Received Dec 1, 2020
Revised Dec 26, 2020
Accepted Dec 30, 2020

Keywords:

Internet of things
Key pre-distribution
Combinatorial designs
IoT security

ABSTRACT

This paper is a review of problems and challenges in the Internet of Things (IoT) security. The management of key pre-distribution is a cryptographic challenge in every kind of application where security is worried. In recent years there are many papers have proposed different schemes for security. We classify in this paper the existing solutions of key pre-distribution schemes, to categorize them, we draw a taxonomy and describe the key pre-distribution coming from combinatorial design and we give examples for that.

Corresponding Author:

Otmane EL MOUAATAMID
ICES Team, Computer Science Department, National School of Computer Science and Systems Analysis (ENSIAS), Mohammed V University in Rabat.
Email: otmane.elmouaatamid@gmail.com

1. INTRODUCTION

The IoT refers to heterogeneous devices (sensors, actuators, mobile, smart vehicles, RFID, embedded computers, and so on) based on standard communication protocols. As devices become more connected thanks to the IoT, security, and privacy have become the primary concern among consumers and businesses. In fact, one of the most important elements of the IoT paradigm is the wireless sensor network (WSN). In order to allow WSN to become an intrinsic part of the IoT in a secure way, several security challenges must be considered. The management of key is one of the crucial parts of the security in WSN. Key pre-distribution is a method to preloading keys in each sensor before their deployment [1]. Each sensor node is assigned a set of keys from the large pool of keys before deployment. After deployment the two nodes having at least one common key, then that node is able to establish a communication path with another node. There are a number of characteristics of WSNs on which key pre-distribution techniques depend on in order to provide better results. Many papers have categorized key pre-distribution scheme according to three approaches: probabilistic, deterministic and hybrid.

In this paper, we classify the various key pre-distribution schemes, and we discuss the different approaches long with their advantages and disadvantages we present a deterministic and hybrid approaches based on combinatorial design theory. Due to Balanced Incomplete Block Designs (BIBD) we can decide how many and which keys to assign to each key-chain before the sensor deployment [7]. The remainder of this paper organized as follows: In section II, we provide an overview of the security requirements. Section

III gives the classification of key pre-distribution approaches with a taxonomy. Section IV presents a detailed description of combinatorial design theory based key pre-distribution scheme. Finally, we give a brief conclusion and present some perspectives.

2. INTERNET OF THINGS SECURITY REQUIREMENTS

In order to allow WSN to become an intrinsic part of the IoT in a secure way, several security challenges must be considered [5]:

Authenticity: The process of determining whether someone or something is. In fact, which nodes or what it is declared to be. We distinguish two kinds of attacks related to authentication namely, impersonation attack where an attacker pretends to be another entity, and Sybil attack where the attacker uses different identities at the same time.

Integrity: Set of means and techniques to permit only nodes have access to the keys and only an assigned basethe station should privilege to change the keys. This would unauthorized nodes from obtaining and any updating of the information, Attacks related to data integrity are message alteration attack and messagefabrication attack.

Availability: Ensuring that the service provided by the Network, by any part of it, or by a single node of it must be available whenever needed. DoS Attacks on availability have different application methods but they have the same goal. The attacker aiming at an aggregator can make some part of the network losses its availability because the aggregator is responsible to provide the measurement of that network part.

Confidentiality: Concept to ensure that information canonly be read by authorized nodes. Attacks of confidentiality consist of accessing illegally to confidential data. A better key technique controls the compromised nodes to keep data from being further exposed.

Non-repudiation: Set of means and techniques to prove the involvement of an entity in data exchange. Attacks on non-repudiation consist of a denial of participation in all or part of communications and to cover their actions.

Privacy: The objective of this security requirement is to prevent private information from being leaked to malicious entities. Attacks on privacy are related to illegally gathering sensitive information about entities (e.g., eavesdropping).

3. CLASSIFICATION OF KEY PRE-DISTRIBUTION SCHEMES

In the literature, serval solutions have been proposed to solve the key management problems [1][2][3]. Key management is the management of cryptography keys in a cryptosystem. These may include symmetric or asymmetric keys. In a symmetric-key algorithm, the identical keys are used for encryption and decryption of the message. In asymmetric keys, there are two keys. One key is used for encryption and the second key is for decryption. In this paper, we focus on symmetric schemes and we classify key pre-distribution into three approaches: probabilistic, deterministic, and hybrid approach such as drawing in figure 1.

3.1. Probabilistic approach:

The key management based Probabilistic approach, in the network every two nodes neighboring can establish a secure link with some probability.

Eschenauer et al are proposed in [6] Random Key Pre-distribution scheme denotes by (RKP). RKP scheme consist of three phases: Key distribution, Shared key discovery and Path-key establishment. The first phase key distribution of this scheme consists of five steps: Generation of a large pool of $\mathscr{P}$ keys, a random drawing of k keys, loading of the keyring into the nodes, saving the key identifiers of a key ring and associated sensor identifier on a trusted controller. The second phase share key discovery, they share a key is that each node broadcast, it has in mind, the list of identifiers of the keys on their key ring. also there other various ways by which it can discover whether two nodes share a common key with each other or not. The third phase path-key establishment phase assigns a path key to select pairs of nodes in the network range that does not have a common key, but are connected by various links two or more at the end of theshared-key discovery stage. Path keys need not be generated by the nodes. Chakhlabati et al proposed in [4] another scheme for key management based probabilistic approachcalled Q-Composite Random Key pre-distribution Scheme. According to the basic scheme if any two neighboring nodes want to establish a secure link in the key setup phase are need to recover a single common key from their key rings. The procedure of the q-

composite key scheme is similar to that of the basic scheme, taking issue only in the size of key pool S and the fact that multiple keys are applied to establish communications instead of merely one. Closest Pair-wise Keys Pre-Distribution Scheme is based on pseudo random function (PRF) and a seignior key is shared between each node and the setup server where each node share the pairwise key with a number of other nodes whose has the closest positions of the sensor node [16, 17]. Random Key Pre-Distribution Scheme Using Node Deployment Knowledge is a scheme proposed in [18]. Also based the deployment knowledge the other scheme proposed in [17], Key Pre-Distribution Using Post-deployment Knowledge, The strategy aim is to improve the pairwise key pre-distribution in static sensor networks. Pre-distributed keys have priority based on post-deployment knowledge, following putting an excessive amount of pre-distributed keys to each sensor node, and eliminate low priority keys to avoid node compromise attacks and returns memory to the applications.

3.2. Deterministic approach:

Many solutions were proposed to guarantee determinism. Deterministic approach ensure that each sensor node is able to establish a pairwise key with all its neighbors' nodes. In our classification, we classify five fundamentals deterministic schemes: Polynomial based key pre-distribution, Matrix-based key pre-distribution schemes, Key pre-distribution based on graph theory, key pre-distribution scheme using codes and Combinatorial design-based key pre-distribution scheme.

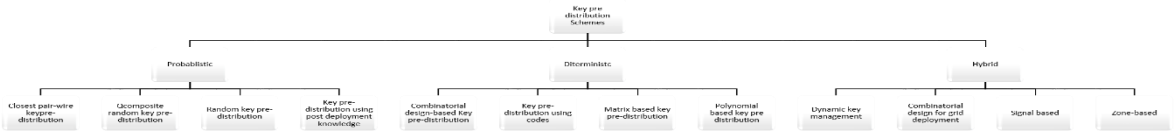


Figure 1. Key Pre-distribution schemes taxonomy

Polynomial based key pre-distribution: This system based on pairwise keys pre-distribution source. A several schemes proposed in [19] to solve some of the probabilistic pre-distribution schemes weakness. For example, any two nodes can establish a pair-wise key when there are nocompromised nodes; Even with some nodes compromised the other nodes of the network can continue establish pair wise keys; The node can see the usual keys and that permit to it choose with which can establish a pairwise key and thereby help reduce communication overhead.

Matrix-bas edkey pre-distribution schemes: There are many schemes proposed in matrix based key pre distribution. The principle of this schemes based on the size of the network. Bloom's concept [9] a network of size n all possible link keys can be typified as a n*n key matrix. Each node can store a diminished quantity of information, then that every couple of nodes can compute the correspond-ding area of the matrix and utilizes it as the link key.

Key pre-distribution based on graph theory: a several schemes based on graph theory are proposed such as treebased key pre-disitribution scheme, ID-based on-way function scheme [19], and Deterministic Multiple space Blom's scheme and others.

Key Predistribution Schemes using Codes: The others in [20] are proposed a novel technique of deterministic key pre-distribution in wireless sensor network using codes and they have presented a key pool based key pre-distribution scheme. The advantage of this construction is general and can be applied to any bloc code with suitable parameters. An example of Reed Solomon codes are used to generate key pre distribution. Let C a code of length n = q - 1, dimension k with alphabet in Q (such that |Q| = q), then the minimum distance d is given by d = n - k + 1. The number of codewords is q^k. For the i-th codeword (a_1; a_2; ; a_n) assign the keys (a_j ; j) with (j = 1; 2; ; n) to the i-th sensor. We map this design to sensor networks. So,

the network consist of q^k sensors, each having keys. We consider the problem of node compromise and calculate the resiliency of the network as the fraction of links broken and nodes disconnected.

Combinatorial design-based key pre-distributionscheme: This scheme is deterministic proposed by the authors in [7] allows determining how many chosen keys to designate to each key chain before the sensor network deployment. We will present the detail of this scheme in the next section and we will give some examples.

3.3. Hybrid approach:

key pre-distribution schemes-based hybrid approach are a combination of probabilistic and deterministic approaches. We can cite three hybrid schemes: Dynamic key management scheme for dynamic WSN, Key Construction and Key pre-distribution using combinatorial designs for Grid-group deployment scheme.

4. COMBINATORIAL DESIGN-BASED KEY PRE-DISTRIBUTION SCHEME

4.1. Block design

Let P be a v-set and suppose B is a collection of k-subsets (blocks of P with the property that each t-subset of P is contained in exactly λ of the elements of B. Then the ordered pair $D = (P; B)$ is called t-design or t - $(v; k; \lambda)$ The elements v of P are called points and the elements b of B are blocks. A regular design is one with a constant k points per block and r blocks containing each point. Thus, a regular design has six parameters: t, v, b, r, k and λ. Sometimes denoted as t - $(v; b; r; k; \lambda)$ design. However, the six parameters but are not independent but satisfy the two relations.

$$vr = bk$$

$$\lambda(v - 1) = r(k - 1)$$

4.2. Balanced incomplete block design.

Balanced Incomplete Block Design (BIBD) is also called a 2-Design. If $t \geq 2$ and $\lambda = 1$, then a t-design is called a Steiner system. A Steiner 2-design thus has the property that every pair of points v in the design occur together in exactly one block b of the design. A resolution of a design D is a partition of the blocks of D into classes such that each point of D is in precisely one block from each class; such a design is said to be resolvable. Every design can be described by a $v * b$ incidence matrix M where each column in M represents a b block Bj of the design and each row a v point Pi.

$$M_{ij} = \{^{1 if P_i \neq B_j}_{0 otherwise}$$

Block Design		***Key Pre-distribution***
Object (Point) Set	$\longrightarrow$	Key-Pool (P)
Object (Point) Set Size,v	$\longrightarrow$	Key-Pool Size $\|P\|$
A Block (Line)	$\longrightarrow$	Key-Chain
Blocks (Lines) b	$\longrightarrow$	Key Chains and, Sensor Nodes (N)
Objects (Points) in a Block (Line) k	$\longrightarrow$	Key in a Key-Chain (K)
Blocks (Lines) that an Object (Point) is in r	$\longrightarrow$	Key-Chains that a Key is in
Two Blocks (Lines) share λ Object (Points)	$\longrightarrow$	Two Key-Chains share (χ) Keys

Table 1. Basic mapping from Block design to key pre-distribution

4.3. Symmetric Balanced incomplete block design

In particular, a balanced incomplete block design is called Symmetric Balance Incomplete Block (SBIBD) design when $b = v$ and therefore $r = k$ [refe]. Symmetric ($v; k; \lambda$)-BIBD denoted by ($v; k; \lambda$)-SBIBD.

4.4. how to share key pre-distrubtion based SBIBD

Thus we use the projective space $PG(m; q)$. Consider a symmetric ($v; k; \lambda$)-design D. Let P be the set of points and B be the set of blocks of D. We also know that $jPj = v$ and $jBj = v$. Choose a point in P to be the secret. Call it xi . The blocks consist of the access structure of this secret sharing scheme. Distribute as shares the set of blocks not containing xi . Point xi is incident with k blocks and any two points occurs together in exactly λ blocks. So, there are ($v; k; \lambda$)-blocks both not containing xi and any two points not

occurring together. Consider ($v; k; \lambda$)-blocks who will combine their shares and let H be the set of combining. The points compute $P=H$ to find xi . That is find

$$P/H = x_i$$

So, the secret is recovered.

5. CONCLUSION (10 PT)

Provide a statement that what is expected, as stated in the "Introduction" chapter can ultimately result in "Results and Discussion" chapter, so there is compatibility. Moreover, it can also be added the prospect of the development of research results and application prospects of further studies into the next (based on result and discussion).

ACKNOWLEDGEMENTS (10 PT)

Xx xxx

REFERENCES (10 PT)

The main references are international journals and proceedings. All references should be to the most pertinent, up-to-date sources and the minimum of references are 25. References are written in IEEE style. Please use a consistent format for references – see examples below (9 pt):

[1] X. S. Li, *et al.*, "Analysis and Simplification of Three-Dimensional Space Vector PWM for Three-Phase Four-Leg Inverters," *IEEE Transactions on Industrial Electronics*, vol. 58, pp. 450-464, Feb 2011.

[2] R. Arulmozhiyal and K. Baskaran, "Implementation of a Fuzzy PI Controller for Speed Control of Induction Motors Using FPGA," *Journal of Power Electronics*, vol. 10, pp. 65-71, 2010.

[3] D. Zhang, *et al.*, "Common Mode Circulating Current Control of Interleaved Three-Phase Two-Level Voltage-Source Converters with Discontinuous Space-Vector Modulation," *2009 IEEE Energy Conversion Congress and Exposition*, Vols 1-6, pp. 3906-3912, 2009.

[4] Z. Yinhai, *et al.*, "A Novel SVPWM Modulation Scheme," in *Applied Power Electronics Conference and Exposition, 2009. APEC 2009. Twenty-Fourth Annual IEEE*, pp. 128-131, 2009.

[5] Ruj, Sushmita, and Bimal Roy. "Key predistribution schemes using codes in wireless sensor networks." In International Conference on Information Security and Cryptology, pp. 275-288. Springer, Berlin, Heidelberg, 2008.

BIOGRAPHIES OF AUTHORS (10 PT)

First author's Photo (3x4cm)	Xxxx (9 pt)
	Xxxx (9 pt)

Second author's photo(3x4cm)	
Thirth author's photo(3x4cm)	Xxxx (9 pt)

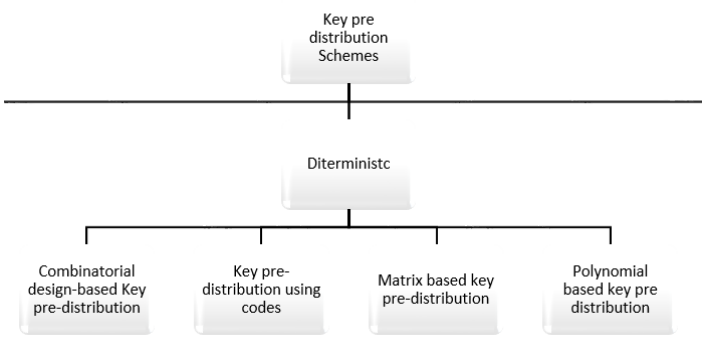
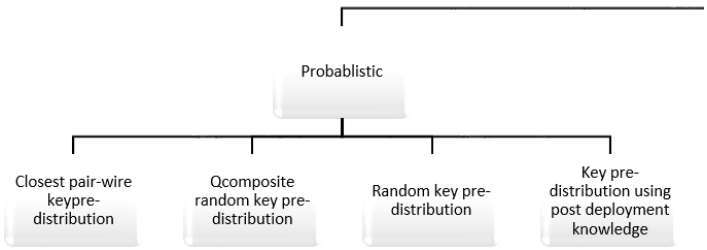
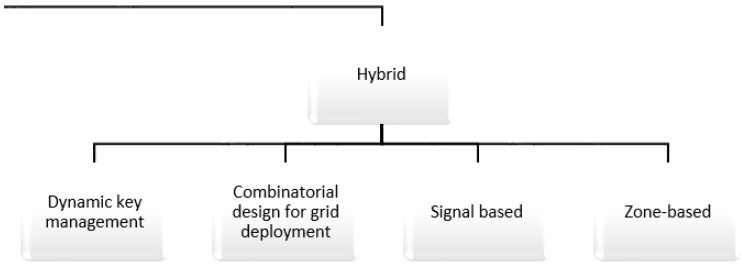


Figure 1. Key Pre-distribution schemes taxonomy



(a)


Hybrid
Dynamic key management
Combinatorial design for grid deployment
Signal based
Zone-based

(b)