A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks

Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, Vahid Tarokh

A Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks

Walid Bechkit [‡], Yacine Challal [‡], Abdelmadjid Bouabdallah [‡] and Vahid Tarokh [§]

[‡] Compiegne University of Technology, HeuDiaSyc Laboratory, Compiegne, France

[§] Harvard university, School of Engineering and Applied Sciences, Cambridge, USA

Email: {wbechkit,ychallal,bouabdal}@hds.utc.fr, vahid@seas.harvard.edu

Abstract

Given the sensitivity of the potential WSN applications and because of resource limitations, key management emerges as a challenging issue for WSNs. One of the main concerns when designing a key management scheme is the network scalability. Indeed, the protocol should support a large number of nodes to enable a large scale deployment of the network. In this paper, we propose a new highly scalable key management scheme for WSNs which provides a good secure connectivity coverage. For this purpose, we make use for the first time of the unital design theory. We show that the basic mapping from unitals to key pre-distribution allows to achieve an extremely high network scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, we propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability lower bounded by $1 - e^{-1} \approx 0.632$. We conduct analytical analysis and simulations to compare our solution to main existing ones regarding different criteria including storage overhead, network scalability, network connectivity, average secure path length and network resiliency. The obtained results show that our approach enhances considerably the network scalability while providing high secure connectivity coverage and good overall performances. Moreover, the obtained results show that at equal network size, our solution reduces significantly the storage overhead compared to main existing solutions.

Index Terms

Wireless sensor networks, security, key management, network scalability, secure connectivity ~~coverage~~

I. Introduction

Nowadays, wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applica-

tions, sophisticated security services are required [1]. Key management is a corner stone 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 then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pairwise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution. Over the last decade, a host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed in the literature [2][3][4][5][6][7][8][9][10][11][12]. Nevertheless, in most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

In this work, our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, we make use, for the first time, of the unital design theory for efficient WSN key pre-distribution. Indeed, we propose a naive mapping from unital design to key pre-distribution and we show through analytical analysis that it allows to achieve an extremely high scalability. Nonetheless, this naive mapping does not guarantee a high key sharing probability. Therefore, we propose an enhanced unital-based key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability. A preliminary work and few discussions were presented in [13].

The contributions of our work are many folds and can be summarized in the following points:

- We review the main state of the art of symmetric key management schemes for WSNs that we classify into two categories: *probabilistic* schemes and *deterministic* ones. We further refine the classification into sub-categories with respect to the underlying concepts and techniques used in key exchange and agreement.
- We introduce, for the first time, the use of unital design theory in key pre-distribution for WSNs. We show that the basic mapping from unitals to key pre-distribution gives birth to an extremely highly scalable scheme while providing low probability of sharing common keys.

- We propose an enhanced unital-based key pre-distribution scheme in order to increase the network scalability while maintaining a good key sharing probability. We prove that adequate choice of our solution parameter should guarantee high key sharing probability lower bounded by $1 - e^{-1}$ while ensuring a high network scalability.
- We analyze and compare our new approach against main existing schemes, with respect to different criteria: storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency. The obtained results show that our solution enhances the network scalability while providing good overall network performances. Moreover, we show that at equal network size, our solution reduces significantly the storage overhead and thereby the energy consumption.

The remainder of this paper is organized as follows: section 2 presents related works on key management for WSNs. We give in section 3 a background on unital design and we propose a basic mapping from unitals to key pre-distribution for WSNs, we analyze the main performances of the resulting scheme. In section 4, we explain the enhanced scalable unital-based construction that we propose and we analyze its different performances. In section 5, we compare our approach to the existing ones regarding different criteria; we give and discuss theoretical and simulation results. In section 6, we end up this paper with some conclusions.

II. Related works: key management schemes for WSNs

Key management problems in WSNs have been extensively studied in the literature and several solutions have been proposed [14] [15]. In this work, we mainly classify symmetric schemes into two categories: *probabilistic* schemes and *deterministic* ones (see figure 1). In *deterministic* schemes, each two neighboring nodes are able to establish a direct secure link which ensures a total secure connectivity coverage. In *probabilistic* schemes, the secure connectivity is not guaranteed because it is conditioned by the existence of shared keys between neighboring nodes. We give in table I the definition of the five considered evaluation metrics, while we summarize in table II the main used symbols.

A. Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability. If two neighboring nodes cannot establish a secure

path composed of successive secure links.

Eschenauer and Gligor proposed in [2] the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node i exchanges with each of its neighbor j the list of key identifiers that it maintains. This allows node j to identify the keys that it shares with node i. If two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, they should determine a secure path which is composed by successive secure links. The values of the key ring size k and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised.

Chan et al. proposed in [3] a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution, two neighboring nodes can establish a secure link only if they share at least Q keys. The pairwise session key is calculated as the hash of all shared keys concatenated to each other: $K_{i,j} = Hash(K_{s_1} \| K_{s_2} \| ... \| K_{s_{q'}})$ where $K_{s_1}, K_{s_2}, ...K_{s_{q'}}$ are the q' shared keys between the two nodes i and j ($q' \geq Q$). This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the network secure connectivity coverage because neighboring nodes must have at least Q common keys to establish a secure link.

Chan et al. proposed also in [3] a perfect secure pairwise key pre-distribution scheme where they assign to each possible link between two nodes i and j a distinct key $K_{i,j}$. Prior to deployment, each node is pre-loaded with $P_c \times n$ keys, where n is the network size and P_c is the desired secure coverage probability. Since we use distinct keys to secure each pairwise link, the resiliency against node capture is perfect and each captured node does not reveal any information about external links. The main drawback of this scheme is the non scalability because the number of the stored keys depends linearly on the network size.

Du et al. proposed in [4] an enhanced random scheme assuming the node deployment knowledge. Nodes are organized in regional groups to which are assigned different key pools, each node selects its keys from the corresponding key pool. The key pools are constructed in such a way that neighboring

ones share more keys than distant pools. This approach allows to enhance the probability of sharing common keys as well as the resilience against node capture attacks. However, the application of this scheme is restrictive if the deployment knowledge is not possible.

In [6], Liu and Ning proposed a key management scheme in which nodes are pre-loaded with bivariate polynomials instead of keys. A global pool of symmetric bivariate polynomials $(f(x,y) = f(y,x))$ is generated off-line and each node i is pre-loaded with a subset of polynomials $f(i,y)$. If two neighboring nodes share a common polynomial, the session key is derived by computing the polynomial value at the neighbor identifier. This approach allows to compute distinct secret keys which enhances the resilience against node capture. However, it requires more memory to store the polynomials and induces more computational overhead.

In [16], Blom proposed a λ-secure symmetric key generation system in which each node i stores a column i and a row i of size $(\lambda+1)$ of two matrices G and $(D.G)^T$ respectively where : $D_{(\lambda+1)\times(\lambda+1)}$ is a symmetric matrix, $G_{(\lambda+1)\times n}$ is a public matrix and $(D.G)^T$ is a secret matrix. The matrix of pairwise keys of a group of n nodes is then $K = (D.G)^T.G$. Yu and Guan [7] used the Blom's scheme to key pre-distribution in group-based WSNs. Nodes are deployed into a grid and to each group is assigned a distinct secret matrix. Using deployment knowledge, the potential number of neighboring nodes decreases which requires less memory. The application of this solution gives good results in the case of node deployment knowledge which is not always possible.

In [8], Ruj et al. propose a trade-based key management scheme denoted Trade-KP. Given a finite set X of v elements, a *Steiner trade* $t-(v,k)$ is defined to be two *disjoint* sets T_1 and T_2 of k-elements blocks of X such that each set of t elements from X occurs in precisely the same number of blocks of T_1 as those of T_2, and no set of t elements from X is repeated more than once in any of T_1 or T_2. A steiner trade is said to be strong if any two blocks of T_1 and T_2 respectively intersects in at most two elements. Authors proposed a new trade construction: Having q a prime power and k $(4 \leq k < q)$, they construct T_1 and T_2 while the blocks of T_1 are represented by $t^1_{i,j} = \{(x, (xi+j)\ mod\ q) : 0 \leq x < k\}$, where $0 \leq i,j < q$, and the blocks of T_2 are represented by $t^2_{i,j} = \{(x, (x^2+xi+j)\ mod\ q) : 0 \leq x < k\}$, where $0 \leq i,j < q$. Authors proved that the proposed construction results in a $2-(qk,k)$ strong steiner trade. They proposed then a mapping to key pre-distribution where they associate to each element a distinct key and to each block of T_1 and T_2 a key ring. The key ring size is then equal to k and the scalability of the scheme is equal to $2q^2$.

After the deployment step, each two nodes can establish a direct secure link if they share exactly two common keys which are used to compute the pairwise session key. Based on the trade properties, authors prove that each pair of keys occurs either in exactly two nodes from T_1 and T_2 respectively or none of the nodes.

The main strength of the proposed scheme is the establishment of unique secret pairwise keys between connected nodes. However, this does not ensure a perfect network resilience as we prove later. Indeed, the attacker may construct a part of the global set of keys and then compute pairwise secret keys used to secure external links where the compromised nodes are not involved. Moreover, the proposed scheme provides a low session key sharing probability which does not exceed 0.25 as we show later.

B. Deterministic schemes

Deterministic schemes ensure that each node is able to establish a pair-wise key with all its neighbors. Many solutions were proposed to guarantee determinism.

A naive deterministic key pre-distribution scheme can be designed by assigning to each link (i,j) a distinct key $K_{i,j}$ and pre-loading each node with $(n-1)$ pairwise keys in which it is involved where n is the network size. It is obvious that this solution is not scalable for large WSNs. Choi et al. proposed in [17] an enhanced approach allowing to store only $(n+1)/2$ keys at each node. For that purpose, they propose to establish an order relation between node identifiers and propose a hash function based key establishment in order to store only half of the node symmetric keys while computing the other half at each node. This approach allows to reduce the required stored keys to the half of network size, however, it is obvious that this scheme remains non scalable enough.

LEAP [9] make use of a common transitory key which is preloaded into all nodes prior to deployment of the WSN. The transitory key is used to generate pairwise session keys and is cleared from the memory of nodes by the end of a short time interval after their deployment. LEAP is based on the assumption that a sensor node, after its deployment, is secure during a time T_{min} and cannot be compromised during this period of time. LEAP is then secure as far as this assumption is verified.

In [10], Çamtepe and Yener proposed a new deterministic key pre-distribution scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). The proposed mapping from SBIBD to key pre-distribution allows to construct m^2+m+1 key rings from a key pool S of m^2+m+1 keys such that each key ring contains $k=m+1$ keys and each two key rings shares exactly one common key.

The main strength of the Çamtepe scheme is the total secure connectivity, indeed each two nodes share exactly one common key. However, the SBIBD scheme does not scale to very large networks. Indeed, using key rings of $m+1$ keys we can generate only m^2+m+1 key rings. SBIBD based key pre-distribution was also used in [18] to guarantee intra-region secure communications in grid group WSNs.

In this work, we seek to design a scalable key management scheme which ensures a good secure coverage of large scale networks with a low key storage overhead. Basic schemes giving a perfect network resilience [3] [17] achieve a network scalability of $O(k)$ where k is the key ring size. The SBIBD [10] and the trade [8] based ones allow to achieve a network scalability of $O(k^2)$. In this work, we propose new solutions achieving a network scalability up to $O(k^4)$ when providing high secure connectivity coverage and good overall performances. For this purpose, we make use of the unital design theory in order to pre-distribute keys. We propose in what follows a basic mapping from unitals to key pre-distribution as well as an enhanced unital based scheme which achieves a good trade-off between scalability and connectivity.

III. Unital design for key pre-distribution in WSNs

WSNs are highly resource constrained. In particular, they suffer from reduced storage capacity. Therefore, it is essential to design smart techniques to build blocks of keys that will be embedded on the nodes to secure the network links. Nonetheless, in most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability, or degrade other performance metrics including secure connectivity and storage overhead. This motivates the use of unital design theory that allows a smart building of blocks with unique features that allow to cope with the scalability and connectivity issues.

In what follows, we start by providing the definition and the features of unital design theory. We explain then the basic mapping from unital to key pre-distribution and evaluate its performance metrics. We propose finally an enhanced unital-based scheme which achieves a good trade-off between scalability and connectivity.

A. Background: Unital Design

In combinatorics, the design theory deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties. Formally, A t-design (ν, b, r, k, λ) is

defined as follows : Given a finite set X of ν points (elements), we construct a family of b subsets of X, called blocks, such that each block has a size k, each point is contained in r blocks and each t points are contained together in exactly λ blocks. For instance, the symmetric Balanced Incomplete Block Design (SBIBD) presented above is a (ν, b, r, k, λ) design, where $\nu = b = m^2 + m + 1$, $r = k = m + 1$ and $\lambda = 1$.

A Unital design is a Steiner 2-design which consists of $b = m^2(m^3+1)/(m+1) = m^2(m^2-m+1)$ blocks, of a set of $v = m^3 + 1$ points [19]. Each block contains $m + 1$ points and each point is contained in $r = m^2$ blocks. Each pair of points is contained in exactly one block together. We denote the Unital by $2 - design(m^3 + 1, m^2(m^2 - m + 1), m^2, m + 1, 1)$ or by $(m^3 + 1, m + 1, 1)$ design for simplicity sake.

Without loss of generality, we focus in this paper on Hermitian unitals which exist for all m a prime power. Other construction for m not necessarily a prime power exist in literature [19]. Some Hermitian unital construction approaches were proposed in literature [20] [21].
A unital may be represented by its $v \times b$ incidence matrix that we call M. In this matrix rows represent the points P_i and columns represent blocks B_j. The matrix M is then defined as:

$$M_{ij} = \begin{cases} 1 & \text{if } P_i \in B_j \\ 0 & \text{otherwise} \end{cases}$$

We give in figure 2 an incidence matrix of a 2-(9,3,1) hermitian unital. It consists of 12 blocks of a set of 9 points. Each block contains 3 points and each point occurs in 4 blocks. Each pair of points is contained together in exactly one block.

B. A basic mapping from unitals to key pre-distribution for WSNs

In this subsection, we start by developing a simple scalable key pre-distribution scheme based on unital design that we denote by NU-KP for the naive unital-based key pre-distribution scheme. We propose a basic mapping in which we associate to each point of the unital a distinct key, to the global set of points the key pool and to each block a node key ring (see table III). We can then generate from a global key pool of $|S| = m^3 + 1$ keys, n key rings ($n = b = m^2(m^2 - m + 1)$) of size $k = m + 1$ keys each one.

Before the deployment phase, we generate the unital blocks corresponding to key rings. Each node is then pre-loaded with a distinct key ring as well as the corresponding key identifiers. After

the deployment step, each two neighboring nodes exchange the list of their key identifiers which allows to determine eventual common key. Using this basic approach, each two nodes share at most one common key. Indeed, referring to the unital properties, each pair of points is contained together in exactly one block which implies that two blocks cannot share more than one point. Hence, if two neighboring nodes share one common key, the latter is used as a pairwise key to secure the link; otherwise, nodes should determine secure paths which are composed of successive secure links.

C. Theoretical analysis

1) storage overhead: When using the proposed naive unital based version matching a unital of order m, each node is pre-loaded with one key ring corresponding to one block from the design, hence, each node is pre-loaded with $(m+1)$ disjoint keys. The memory required to store keys is then $l \times (m+1)$ where l is the key size.

2) Network scalability: From construction, the total number of possible key rings when using the naive unital based scheme is $n = \frac{m^2 \times (m^3+1)}{(m+1)} = m^2 \times (m^2 - m + 1)$, this is then the maximum number of supported nodes.

3) Direct secure connectivity coverage: When using the basic unital mapping, we know that each key is used in exactly m^2 key rings among the $m^2 \times (m^2 - m + 1)$ possible key rings. Let us consider two nodes u and v randomly selected. The node u is pre-loaded with a key ring KR_u of $m+1$ different keys. Each of them is contained in $m^2 - 1$ other key rings among the possible $m^2 \times (m^2 - m + 1) - 1$ ones. Knowing that two pair of keys occurs together in exactly one block, we find that the blocks containing two different keys of KR_u are completely disjoint. Hence, each node shares exactly one key with $(m+1) \times (m^2 - 1)$ nodes among the $m^2(m^2 - m + 1) - 1$ other possible nodes, Then, the probability P_c of sharing a common key can be calculated as follows:

$$\begin{aligned} P_c &= \frac{(m+1) \times (m^2-1)}{m^2(m^2 - m + 1) - 1} \\ &= \frac{(m+1)^2}{m^3 + m + 1} \end{aligned} \tag{1}$$

The evaluation of this naive solution shows clearly that the basic mapping from unitals to key pre-distribution gives a high network scalability which reaches $O(k^4)$. Moreover, given a network size n, this naive scheme allows to reduce the key ring size up to $\sqrt[4]{n}$. However, this naive solution results a low key sharing probability which tends to $O(\frac{1}{k})$. In order to improve the key sharing

probability while maintaining a good scalability improvement, we propose in the next section an enhanced scalable and efficient unital-based key pre-distribution for WSNs.

IV. A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION SCHEME FOR WSNS

In this section, we present a new unital-based key pre-distribution scheme for WSNs. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build the unital design blocks and pre-load each node with a number of blocks picked in a selective way.

A. Key Pre-distribution

Before the deployment step, we generate blocks of m order unital design, where each block corresponds to a key set. We pre-load then each node with t $completely$ $disjoint$ blocks where t is a protocol parameter that we will discuss later in this section. In lemma 1, we demonstrate the condition of existence of such t completely disjoint blocks among the unital blocks. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key. Contrary to this, pre-loading each two nodes with t disjoint unital blocks means that each two nodes share between zero and t^2 keys since each two unitals blocks share at most one element.

After the deployment step, each two neighbors exchange the identifiers of their keys in order to determine the common keys. If two neighboring nodes share one or more keys, we propose to compute the pairwise secret key as the hash of all their common keys concatenated to each other. The used hash function may be *SHA-1* [22] for instance. This approach enhances the network resiliency since the attacker have to compromise more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links. The major advantage of this approach is the improvement of the key sharing probability. As we will prove in next subsection, this approach allows to achieve a high secure connectivity coverage since each node is pre-loaded with t disjoint blocks. Moreover, this approach gives good network resiliency through the composite pairwise secret keys which reinforces secure links. In addition, we show that our solution maintains a high network scalability compared to existing solutions although it remains lower than that of the naive version.

B. Theoretical analysis

We denote in what follows by t-UKP the unital-based key pre-distribution scheme of parameter t (t is the number of pre-loaded blocks at each node). We note that the 1-UKP scheme matches the basic mapping presented in section 3.

1) storage overhead: When using the t-UKP scheme of order m, we pre-loaded each node with $t(m+1)$ distinct keys. Indeed, from the construction, we can see that t blocks pre-loaded in a given node are completely disjoint. So, each two blocks within a key ring do not intersect at any key. So, the memory required to store keys is then equal to $l \times t \times (m+1)$, where l is the key size.

2) Network scalability: Since each node is pre-loaded with t blocks from the $m^2 \times (m^2 - m + 1)$ possible blocks of the unital design, it is obvious that the maximum number of key rings that we can reach is equal to $n = \frac{m^2}{t}(m^2 - m + 1)$. This is the ideal case when all unital blocks are used. When using the random pre-distribution of unital blocks, we may generate a number of blocks slightly lower than this best value. We compute in what follows the minimum network size that can be supported by the random blocks distribution.

Lemma 1: Given $t \geq 2$, each set of $(t-1)(m+1)(m^2-1)+t$ blocks from an m order unital design contains at least one sub-set of t completely disjoint blocks.

Proof: As shown before, we know that each block of a unital design intersect with exactly $(m+1)(m^2-1)$ other blocks at one key. We prove the proposition by induction: for $t = 2$, let T be a set of $(m+1)(m^2-1)+2$ blocks of a unital design of order m and let us assume that each two blocks of T intersect at one point. So, each block of T intersects with the $(m+1)(m^2-1)+1$ other blocks in T which contradicts the fact that each block intersects with exactly $(m+1)(m^2-1)$ blocks of the global unital. Hence the proposition is true for $t = 2$.

Let us now assume that the proposition is true at the order t and check whether it is for $t+1$. Let T be a set of $t(m+1)(m^2-1)+t+1$ blocks of a unital of order m. Since the proposition is true at order t, it exists at least one subset T_0 of t disjoint blocks in T. Each of these blocks intersects with exactly $(m+1)(m^2-1)$ other blocks. So the maximum possible number of blocks which intersect with T_0 is $t(m+1)(m^2-1)$. Hence, among the remaining $t(m+1)(m^2-1)+1$ blocks of $T - T_0$, there exists at least one block which does not intersect with any block of T_0. We deduce that T contains at least $t+1$ completely disjoint blocks. ■

Proposition 1: Using the t-UKP scheme with a random pre-distribution of unital blocks, we

generate at least $\frac{m^2(m^2-m+1)-((t-1)(m^2-1)(m+1)+t)}{t}$ key rings.

Proof: Using a unital design of order m, the number of the generated blocks is equal to $m^2(m^2-m+1)$. From the t-UKP construction, we know that each key ring contains exactly t disjoint blocks. Following the lemma 1, we find that using the t-UKP scheme, we can generates at least $\frac{m^2(m^2-m+1)-((t-1)(m^2-1)(m+1)+t)}{t}$ key rings. ■

3) Direct secure connectivity coverage: We discuss in what follows the direct secure connectivity coverage of the t-UKP scheme.

Proposition 2: Given $t \geq 2$, using the t-UKP scheme, the secure connectivity coverage (the probability of key sharing between any two nodes) is given by: $P_c = 1 - (1 - \frac{(m+1)^2}{m^3+m+1})^{t^2}$

Proof: Let us consider two nodes u and v randomly selected. Each node is pre-loaded with a key ring containing t disjoint unital blocks: $KR_u = \{B_{u,1} \cup B_{u,2} \cup ... \cup B_{u,t}\}$ and $KR_v = \{B_{v,1} \cup B_{v,2} \cup ... \cup B_{v,t}\}$

Following equation (1) (Cf. Section 3.C), we find that the probability that two blocks $B_{u,p}$ and $B_{v,q}$ share one key is $\frac{(m+1)^2}{m^3+m+1}$ while the probability that they don't share any key is $(1 - \frac{(m+1)^2}{m^3+m+1})$.

Since all blocks of node u as well as those of node v are completely disjoint thanks to the proposed construction, the probability that the two nodes u and v don't share any key is then given by:

$$\begin{aligned} P(KR_u \cap KR_v = \emptyset) &= \prod_{p=1}^{t} \left(\prod_{q=1}^{t} P(B_{u,p} \cap B_{v,q} = \emptyset) \right) \\ &= \prod_{p=1}^{t} \left(\prod_{q=1}^{t} (1 - \frac{(m+1)^2}{m^3+m+1}) \right) \\ &= (1 - \frac{(m+1)^2}{m^3+m+1})^{t^2} \end{aligned}$$

The probability that two nodes share at least one key is then : $P_c = 1 - (1 - \frac{(m+1)^2}{m^3+m+1})^{t^2}$ ■

We plot and compare later the key sharing probability of the t-UKP scheme and show that we increase considerably the key sharing probability over the NU-KP scheme.

4) Network Resiliency: We analyze in what follows the network resiliency of the t-UKP scheme.

Lemma 2: Using the t-UKP scheme of order m, the probability $p(i)$ that two nodes share exactly i keys ($0 \leq i \leq t^2$) is:

$$p(i) = \binom{t^2}{i} \left(\frac{(m+1)^2}{m^3+m+1} \right)^i \times \left(1 - \frac{(m+1)^2}{m^3+m+1} \right)^{t^2-i}$$

Proof: Let us consider two nodes u and v randomly selected. Each node is pre-loaded with a key ring containing t disjoint unital blocks: $KR_u = \{B_{u,1} \cup B_{u,2} \cup ... \cup B_{u,t}\}$ and $KR_v = \{B_{v,1} \cup B_{v,2} \cup ... \cup B_{v,t}\}$

Let us consider $X_{p,q}$ the variable giving the number of shared keys between two unital blocks $B_{u,p}$ and $B_{v,q}$. Following equation (1) (Cf. Section 3.C), we find that $X_{p,q}$ takes only 1 and 0 values such that: $P(X_{p,q}=1)=\frac{(m+1)^2}{m^3+m+1}$ while: $P(X_{p,q}=0)=1-\frac{(m+1)^2}{m^3+m+1}$

$X_{p,q}$ follows then a Bernoulli distribution of parameter $(\frac{(m+1)^2}{m^3+m+1})$. The number of shared keys between KR_u and KR_v which represents $(\sum_{p=1}^{t}\sum_{q=1}^{t}X_{p,q})$ follows then a binomial distribution $(t^2,\frac{(m+1)^2}{m^3+m+1})$. So, $p(i)$ is given by :

$$p(i)=\binom{t^2}{i}\left(\frac{(m+1)^2}{m^3+m+1}\right)^i\times\left(1-\frac{(m+1)^2}{m^3+m+1}\right)^{t^2-i}$$

■

Proposition 3: When using the t-UKP scheme of order m, the network resiliency when x nodes are captured is:

$$R_x=1-\sum_{i=1}^{t^2}(1-\frac{\binom{m^3(m-1)}{x\times t}}{\binom{m^2(m^2-m+1)}{x\times t}})^i\frac{p(i)}{P_c} \tag{2}$$

Proof: We recall that $p(i)$ is the probability that two nodes share exactly i keys and that P_c is the probability that two nodes share at least one key. So, $P_c=\sum_{i=1}^{t^2}p(i)=1-p(0)$ which matches proposition 2.

Let us call LC, the event that a link is compromised, LC_i the event that a link secured with i keys is compromised and NC_x is the event that x nodes are compromised. Let us compute first $P(LC_i|NC_x)$. When using the t-UKP scheme, the compromise of x nodes reveals exactly $x\times t$ unital blocks. We know that each key occurs in in m^2 unital blocks among the total number of $m^2(m^2-m+1)$ blocks, the probability c that a key is uncompromised when x node are compromised is then the probability that the key does not occurs in any if the discovered blocks. So, we find that:

$$c=\frac{\binom{m^2(m^2-m+1)-m^2}{x\times t}}{\binom{m^2(m^2-m+1)}{x\times t}}=\frac{\binom{m^3(m-1)}{x\times t}}{\binom{m^2(m^2-m+1)}{x\times t}}$$

The probability of compromising a given secret key composed of i keys is then equal to $(1-c)^i$. So, the probability that a given link is compromised when it is secured with i keys and when x nodes are compromised is given by: $P(LC_k|NC_x)=(1-c)^i$. Let us now compute the resiliency of

the global network. This can be computed as the average probability that a link be uncompromised when x nodes are captured and is given by :

$R_x = 1 - P(LC|NC_x) = 1 - \sum_{i=1}^{t^2} P(LC_i|NC_x)\frac{p(i)}{P_c} = 1 - \sum_{i=1}^{t^2} (1-c)^i \frac{p(i)}{P_c}$ ■

C. Choice of the t value

As we showed through performance analysis, the pre-distribution of t unital blocks in each node instead of one allows at the same time enhancing the key sharing probability and computing composite pairwise secret keys witch reinforce secure links. On the other hand, the use of the t-UKP scheme multiplies the storage overhead and decreases the network scalability over the naive version. The choice of the t value depends then on the application requirement in order to obtain the best tradeoff. Indeed, when we do not need to establish a secure link between each pair of nodes or when the length of secure paths is not a major concern, low values of t can be chosen. For instance, in many-to one WSNs where the key sharing requirement is reduced to the child-parent relationship, low values of t can be used in order to reach an extremely high scalable deployment. On the other hand, when the key sharing probability and the length of secure paths are major concerns, t should be given a high value which allows to ensure a good key sharing probability.

In order to maintain a high key sharing probability and then low secure path length while maintaining a high scalability, we propose to choose $t = \sqrt{m}$. Without loss of generality, we assume that m is a perfect square, if it is not the case, we can refer to the nearest integer to the square root of m. Indeed, this value allows to maintain a high scalability of $O(\sqrt{m}m^3)$ with a storage overhead of $O(\sqrt{m}m)$. As we will prove, this choice allows to reach a very good key sharing probability lower bounded by $1 - e^{-1}$. We denote by UKP* the t-UKP scheme with $t = \sqrt{m}$ and we recall that a lower bound of the direct secure connectivity coverage of UKP* is a value L, such that the direct secure connectivity coverage of UKP* is always greater or equal to L for all m values.

Proposition 4: Let us consider the UKP* scheme (t-UKP with $t = \sqrt{m}$), the limit of the direct secure connectivity coverage as m tends to infinity is equal to $L = 1 - e^{-1}$ which is a lower bound of the direct secure connectivity coverage of UKP*.

Proof: : Following proposition 2, when using the UKP* (t-UKP with $t = \sqrt{m}$), the secure connectivity coverage is given by : $P_c = 1 - (1 - \frac{(m+1)^2}{m^3+m+1})^m$. Since $P_c(m)$ is a strictly decreasing function defined on the interval [0,1], the limit as m tends to infinity exists and is equal to L such

as: $(0 \leq L \leq 1)$. We have:

$$\begin{aligned}
L &= \lim_{m\to+\infty} 1-(1-\frac{(m+1)^2}{m^3+m+1})^m \\
1-L &= \lim_{m\to+\infty} (1-\frac{(m+1)^2}{m^3+m+1})^m \\
\ln(1-L) &= \lim_{m\to+\infty} m\times\ln(1-\frac{(m+1)^2}{m^3+m+1}) \\
\ln(1-L) &= \lim_{m\to+\infty} \frac{m\times(m+1)^2}{m^3+m+1}\times\frac{\ln(1-\frac{(m+1)^2}{m^3+m+1})}{\frac{(m+1)^2}{m^3+m+1}} \\
\ln(1-L) &= -1 \\
L &= 1-e^{-1}
\end{aligned}$$

So, the secure connectivity coverage function is a strictly decreasing function having a limit of $L = 1 - e^{-1} \approx 0.632$ as m tends to infinity. This limit L is then a lower bound of the direct secure connectivity coverage when using the UKP* scheme. ■

V. Performance Comparison

In this section, we compare the proposed unital-based schemes to existing schemes regarding different criteria (We recall that metric definitions are given in table I).

A. Network scalability at equal key ring size

We compare in figure 3 the scalability of the proposed unital based schemes against that of the SBIBD-KP and the Trade-KP ones. The network scalability of the t-UKP schemes is computed as the average value between the maximum and the minimum scalability. The network scalability of the SBIBD scheme is computed as $m^2 + m + 1$ where m is the SBIBD design order and $m + 1$ is the key ring size. We compute the salability of the Trade-KP scheme as $2q^2$ where q is the first prime power greater than the key ring size k, this value allows a achieve the best session key sharing probability using the Trade-KP scheme as we proved in [13]. The figure shows that at equal key ring size, the NU-KP scheme allows to enhance greatly the scalability compared to the other schemes; for instance the increase factor reaches 10000 compared to the SBIBD-KP scheme when the key ring size exceeds 100. Moreover, the figure shows that the t-UKP schemes achieve a high network scalability. We notice that the higher t is, the lower network scalability is. Nevertheless, 2-UKP and 3-UKP give better results than those of the SBIBD-KP and the Trade-KP solutions. Even we choose $t = \sqrt{m}$ as we propose (UKP*), the network scalability is enhanced. For instance, compared to

SBIBD-KP scheme, the increase factor reaches five when the key ring size equal to 150. We plot in figure 4 the same results separately with linear scales which illustrate clearly the network scalability enhancement when using our solutions.

Authors in [3], assess the network scalability of random schemes including the RKP and the Q-composite ones regarding to the desired network connectivity and to the network capacity to maintain secure links while some nodes are compromised. They defined for that a threshold f_m called the *limited global payoff requirement*. The later can be explained as the level of compromise past where the adversary gains an unacceptably information on the other pairwise secret keys. Depending on P_c and f_m they defined the maximum number supported network size. Authors present results for $P_c = 0.33$ and $f_m = 0.1$ and show that the network scalability with a key ring size of 100 is about 300 for RKP scheme and between 600 and 700 when using Q-composite schemes. The scalability of the same schemes with a key ring size of 400 is respectively of about 1200 and between 2700 and 2800. We can see clearly that our solutions allow to reach much better network scalability than the random schemes under the suggested parameters.

B. Key ring size at equal network size

In this subsection, we compare the required key ring size when using the unital-based, the SBIBD-KP and the Trade-KP schemes at equal network size. We compute for each network size the design order allowing to achieve the desired scalability and we deduce then the key ring size, the obtained results are reported in figure 5. The figure shows that at equal network size, the NU-KP scheme allows to reduce extremely the key ring size and then the storage overhead. Indeed the enhancement factor over the SBIBD-KP scheme reaches 20. When using the t-UKP schemes, the results show that the higher t is, the higher required key ring size is. However, this value remains significantly lower than the required key ring size of the SBIBD-KP and Trade-KP schemes. Moreover, we can see clearly in the figure, that at equal network size, the UKP* scheme provides very good key ring size compared the SBIBD-KP and the Trade-KP schemes. For instance, the key ring size may be reduced over a factor greater than two when using the UKP* compared to the SBIBD-KP scheme.

C. Energy consumption at equal network size

In this subsection, we compare the energy consumption induced by the direct secure link establishment phase. Since each node broadcasts its list of key identifiers, the energy consumption can be

computed as :

$E = \mathcal{E}_{tx} \cdot k \cdot log_2(|S|) + \eta \cdot \mathcal{E}_{rx} \cdot k \cdot log_2(|S|)$

where $\mathcal{E}_{tx}$ (resp. $\mathcal{E}_{rx}$) is the average energy consumed by the transmission (resp. reception) of one bit, k is the key ring size, η is the average number of neighbors and $log_2(|S|)$ represents the size of a key identifier in bits that we round up to the nearest byte size.

We compare the energy consumption of our solutions against SBIBD-KP and Trade-KP. The results plotted in figure 6 show that at equal network size, the NU-KP scheme consumes very small amount of energy to exchange the low number of key identifiers. We also note that the higher t is, the higher the consumed energy is. This is due to the increased number of stored keys and thereby the increased number of exchanged identifiers. Finally, the figure shows clearly that UKP* scheme consumes less energy than the SBIBD-KP and the Trade-KP schemes. This matches our expectation since the energy consumption is strongly correlated to the number of stored keys.

D. Network connectivity at equal key ring size

We compare in this subsection, the network secure connectivity coverage of the different schemes. First, we plot in figure 7 (a) the key sharing probability when using the unital based schemes (NU-KP, t-UKP and UKP*). The figure shows that the NU-KP scheme provides a bad direct secure connectivity coverage which decreases significantly when the key ring size increases. Indeed, the key sharing probability is low and tends to $O(\frac{1}{k})$ as k tends to infinity. Otherwise, the obtained results show that the higher t is, the better the direct secure connectivity coverage is. Indeed, loading nodes with many blocks from unital design allows to increase significantly the key sharing probability. The figure shows moreover that the UKP* scheme gives very good connectivity results. For instance, the direct secure connectivity coverage remains between 0.82 and 0.66 when the key ring size is between 10 and 150. As the key ring size is high, the direct secure connectivity of UKP* approaches $1 - e^{-1} \approx 0.632$, which we proved to be a lower bound.

In a second time, we compared the direct secure connectivity coverage of the UKP* to those of the other existing schemes. The Trade-KP scheme allows to reach a direct secure connectivity lower than 0.25. Indeed, we proved in [13] that the key sharing probability of the Ruj et al. Trade-KP scheme [8] is equal to $\frac{k(k-1)}{4q^2}$ where $4 \leq k < q$ and q is a prime power. k is the key ring size and we chose q to be the first prime power greater than k which ensures the best key sharing probability. The figure 7 (b) shows that the secure connectivity of the RKP* scheme remains much better than that

of Trade-KP one. Indeed the direct secure connectivity coverage of RKP* has a good lower bound of $L = 1 - e^{-1} \approx 0.632$ while that of the Trade-KP have an upper bound of 0.25. We compared also the secure connectivity of the UKP* scheme to those of the RKP and the Q-composite schemes. We assume for these random approaches that the global key pool size is equal to the square of the key ring size which allows to achieve a good network resiliency. The results show that UKP* scheme provides a better secure connectivity coverage than the RKP scheme and much better than the Q-composite schemes with $Q = 2$, $Q = 3$, etc. Indeed, using the Q-composite scheme, two nodes must share at least Q common keys to be able to establish a secure link which degrades significantly the secure connectivity coverage (see figure 7 (b)).

Although the unital-based scheme UKP* increases significantly the network scalability and provides a good key sharing probability greater than 0.632, this metric remains lower compared to SBIBD-KP which ensures a perfect key sharing probability. However, our scheme allows to attend a total secure connectivity thanks to the secure path establishment.

We also studied the average secure path length when using different key pre-distribution schemes including our solutions. For this purpose, we conducted simulations while referring to the results given in [23] in order to construct a grid deployment model which guarantees the network physical connectivity and coverage. The results showed that the UKP* scheme provides a good average secure path length between 1.18 and 1.36 when the key ring size is between 10 and 150. It does not exceed 1.37 even the key ring size is very high. In others terms, when using the UKP* scheme, two-thirds of possible links in the network will be secured directly while practically all the other third links can establish a 2-hop secure path. We give some numerical results about the average secure path length in the last subsection.

E. Network resiliency at equal key ring size

We compare in this subsection, the network resiliency of the unital-based schemes to those of the Trade-KP and the SBIBD-KP ones. We notice that the proposed trade based construction given in [8] allows to have a unique pairwise key per secure link, this key is computed as the hash of a unique pair of initial keys. However the overall network resiliency is not perfect because the compromise of some key rings may reveal other pairwise secret keys used to secure external links in which the compromised nodes are not involved. We proved that the resiliency of the Trade-KP scheme is given

by: (see proof in appendix A)

$$R_x = \frac{\binom{2q^2-4q+2}{x} + 4(q-1)\binom{2q^2-4q+2}{x-1}}{\binom{2q^2}{x}}$$

where x is the number of comprised nodes and q is the Ruj et al. trade construction parameter. On the other hand, following the study presented in [10], the network resiliency R_x of the SBIBD-KP scheme is given by:

$$R_x = \frac{\binom{m^2}{x}}{\binom{m^2+m+1}{x}}$$

Where m is the SBIBD design order. Finnaly, the network resiliency formula of unital based schemes was given in proposition 3.

We compare in figure 8 the network resiliency at equal number of compromised nodes for $|KR| = 68$. The figure shows that the NU-KP scheme provides a good resiliency compared to other schemes. Using the t-UKP, the higher t is, the lower network resiliency is at equal number of compromised nodes. This is due to the number of compromised unital blocks which is multiplied by t. On the other hand, the figure shows that the UKP* scheme improves the network resiliency over the SBIBD-KP scheme by 20%. It also gives a better network resiliency then the Trade-KP scheme when the number of compromised nodes exceeds 60.

F. Numerical results

We provide in table IV numerical results comparing network scalability, direct secure connectivity coverage, and average secure path length of the three schemes (SBIBD-KP, Trade-KP and UKP*) at equal key ring size. We notice that we provide the average network scalability (number of nodes) when using UKP* scheme. On the other hand, we compute the average secure path length based on simulations. We refer in these simulations to the results given in [23] in order to construct a grid deployment model which ensures the network physical connectivity and coverage. Numerical results show that the unital-based key pre-distribution scheme UKP* increases the network scalability over the SBIBD-KP and the Trade-KP scheme while maintaining high secure connectivity coverage. For

instance, the network maximum size is increased by a factor of 3 and 4.8 when the key ring size is equal to 68 and 140 respectively compared to the SBIBD-KP scheme. In addition, we maintain a high connectivity over 0.63 which ensures a low average secure path length which does not exceed 1.37.

VI. Conclusion

We proposed, in this work, a scalable key management scheme for WSNs. We make use, for the first time, of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows to achieve an extremely high network scalability while giving a low direct secure connectivity coverage. We proposed then an efficient scalable unital-based key pre-distribution scheme providing high network scalability and good secure connectivity coverage. We discuss the solution parameter and we propose adequate values giving a very good trade-off between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach provides a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency.

VII. Acknowledgement

This work is made as part of the Picardie regional project under reference I159C. The authors wish to thank the Picardie regional council in France and the European Regional Development Fund (ERDF) for funding and supporting this project.

Appendix A

Network resiliency of the trade-based key pre-distribution scheme

Using the Ruj et al. trade construction [8], the two sets T_1 and T_2 contain q^2 key rings each one. Let us assume that x nodes are compromised and let us compute the probability that a given pair of keys K_i and K_j is known (We recall that two nodes can establish a secure session key if they share exactly two common keys).

From construction, we know that each key occurs in exactly q blocks in T_1 and q blocks of T_2, and that each pair of keys occurs in one key ring from T_1 and one key ring from T_2. So, we find that among the $2q^2$ possible key rings, two contains the pair K_i and K_j, $2q-2$ contain only K_i, $2q-2$ contain only K_j and then $2q^2-4q+2$ do not contain any key of K_i and K_j.

So the probability that the pair K_i, K_j does not occur in any of the x discovered key rings is the probability that any key occurs in the discovered key rings plus the probability that only one key occurs in the discovered key rings. The network resiliency is then given by :

$$R_x = \frac{\binom{2q^2-4q+2}{x} + 2\binom{2q-2}{1}\binom{2q^2-4q+2}{x-1}}{\binom{2q^2}{x}} = \frac{\binom{2q^2-4q+2}{x} + 4(q-1)\binom{2q^2-4q+2}{x-1}}{\binom{2q^2}{x}}$$

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang. Securing wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials*, 10(1-4):6–28, 2008.

[2] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *ACM CCS*, pages 41–47, 2002.

[3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE SP*, pages 197 – 213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *IEEE INFOCOM*, pages 586–597, 2004.

[5] C. Castelluccia and A. Spognardi. A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks. In *IEEE Securecom*, pages 351–360, 2007.

[6] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In *ACM CCS*, pages 52–61, 2003.

[7] Z. Yu and Y. Guan. A robust group-based key management scheme for wireless sensor networks. In *IEEE WCNC*, pages 1915–1920, 2005.

[8] S. Ruj, A. Nayak, and I. Stojmenovic. Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs. In *IEEE INFOCOM*, pages 326–330, 2011.

[9] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *ACM CCS*, pages 62–72, 2003.

[10] S. A. Çamtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 15:346–358, 2007.

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. Spins: security protocols for sensor netowrks. In *ACM MOBICOM*, pages 189–199, 2001.

[12] B. Maala, Y. Challal, and A. Bouabdallah. Hero: Hierarchcal key management protocol for heterogeneous wsn. In *IFIP WSAN*, pages 125–136, 2008.

[13] W. Bechkit, Y. Challal, and A. Bouabdallah. A new scalable key pre-distribution scheme for wsn. In *IEEE ICCCN*, pages 1–7, 2012.

[14] J. Zhang and V. Varadharajan. Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications*, 33(2):63 – 75, 2010.

[15] S. A. Çamtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: a survey. *Technical Report TR-05-07*, March, 2005.

[16] R. Blom. An optimal class of symmetric key generation systems. In *Proceedings of the Eurocrypt 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques*, pages 335–338. Springer-Verlag, 1985.

[17] T. Choi, H. B. Acharya, and M. G. Gouda. The best keying protocol for sensor networks. In *IEEE WOWMOM*, pages 1–6, 2011.

[18] S. Ruj and B. Roy. Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks. *ACM Transactions on Sensor Networks*, 6:4:1–4:28, January 2010.

[19] E.F. Assmus and J.D. Key. *Designs and their codes*. Cambridge tracts in mathematics. Cambridge University Press, 1992.

[20] A. Betten, D. Betten, and V. D. Tonchev. Unitals and codes. *Discrete Mathematics*, 267(1-3):23–33, 2003.

[21] J. D. Key. Some applications of magma in designs and codes: Oval designs, hermitian unitals and generalized reed-muller codes. *Journal of Symbolic Computation*, 31(1/2):37–53, 2001.

[22] National Institute of Standards and Technology. Secure hash standard. *Federal Information Processing Standards Publication*, 1995.

[23] S. Shakkottai, R. Srikant, and N. Shroff. Unreliable sensor grids: coverage, connectivity and diameter. In *IEEE INFOCOM*, pages 1073–1083, 2003.

[24] M. Doddavenkatappa, M.C. Chan, and A. L. Ananda. A dual-radio framework for mac protocol implementation in wireless sensor networks. In *IEEE ICC*, pages 1–6, 2011.

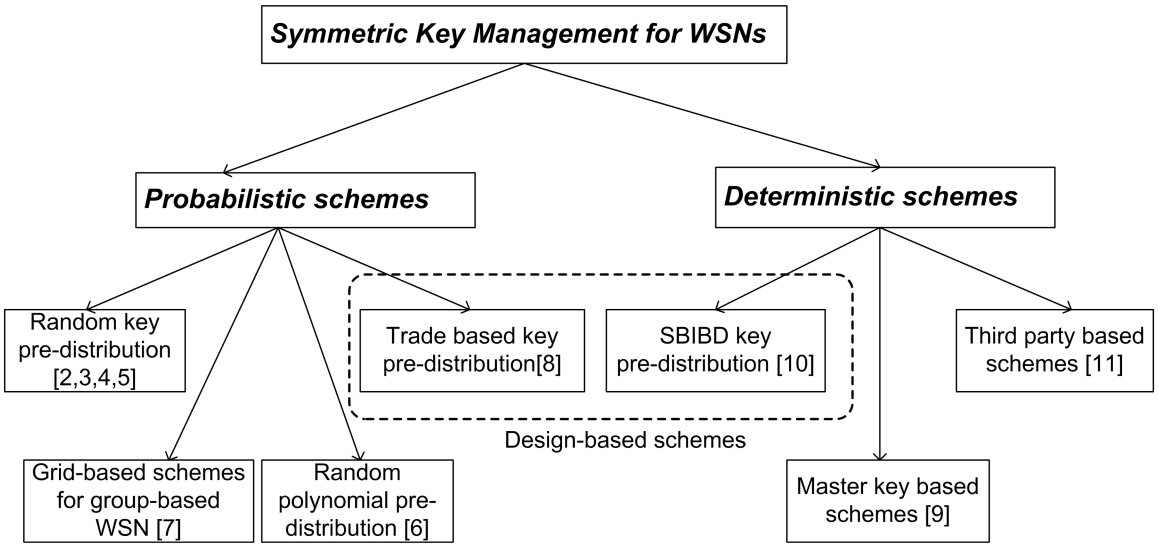

Fig. 1. Classification of symmetric key management schemes for WSNs

$$\begin{pmatrix} 1 & . & . & . & . & 1 & 1 & . & . & . & 1 & . \\ . & . & . & . & . & 1 & . & 1 & 1 & 1 & . & . \\ . & . & 1 & 1 & . & . & 1 & 1 & . & . & . & . \\ 1 & . & . & 1 & 1 & . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & 1 & . & . & 1 & . & 1 \\ . & . & 1 & . & . & . & . & . & 1 & . & 1 & 1 \\ . & 1 & 1 & . & 1 & 1 & . & . & . & . & . & . \\ 1 & 1 & . & . & . & . & . & 1 & . & . & . & 1 \\ . & 1 & . & 1 & . & . & . & . & . & 1 & 1 & . \end{pmatrix}$$

Fig. 2. Example of incidence matrix of a 2-(9,3,1) hermitian unital

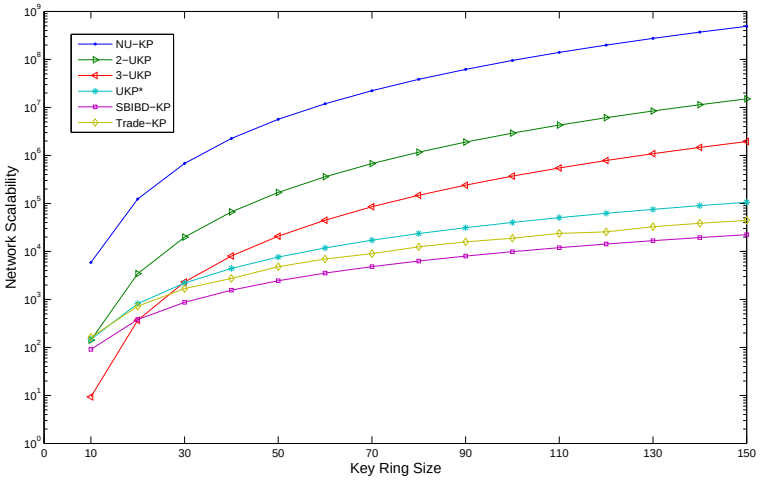

Fig. 3. Network scalability at equal key ring size

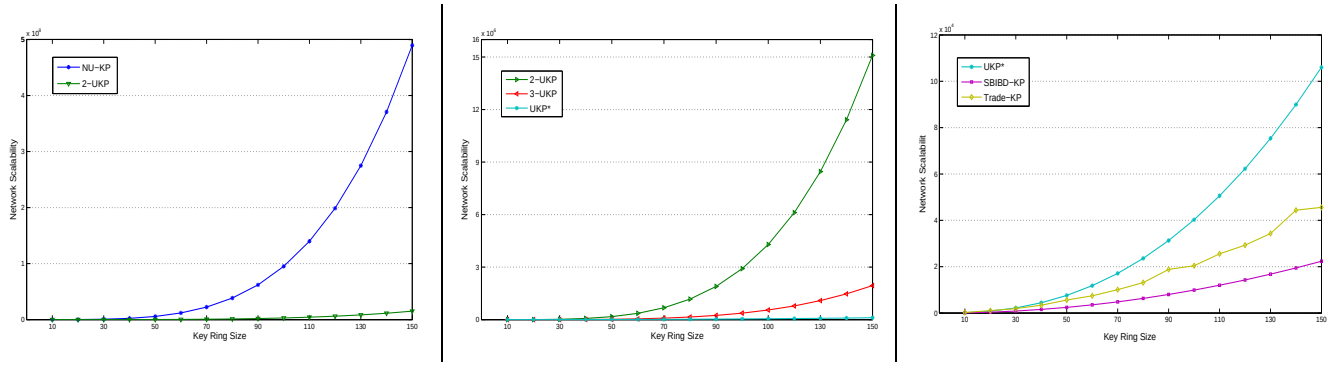

Fig. 4. Network scalability at equal key ring size (linear scale)

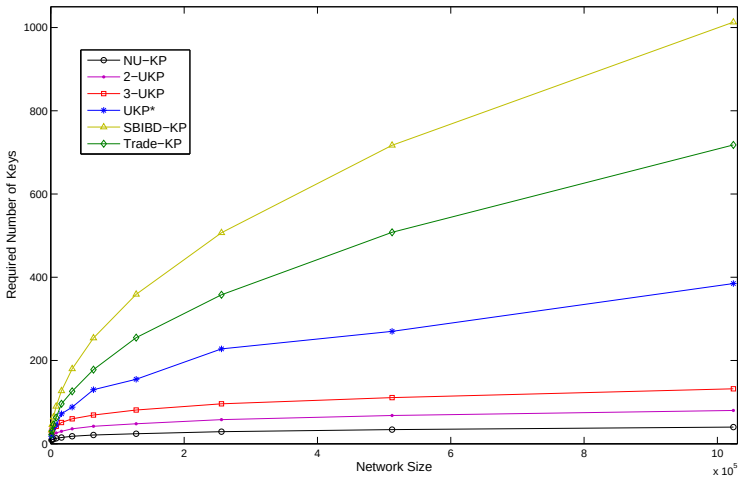

Fig. 5. Required key ring size at equal network size

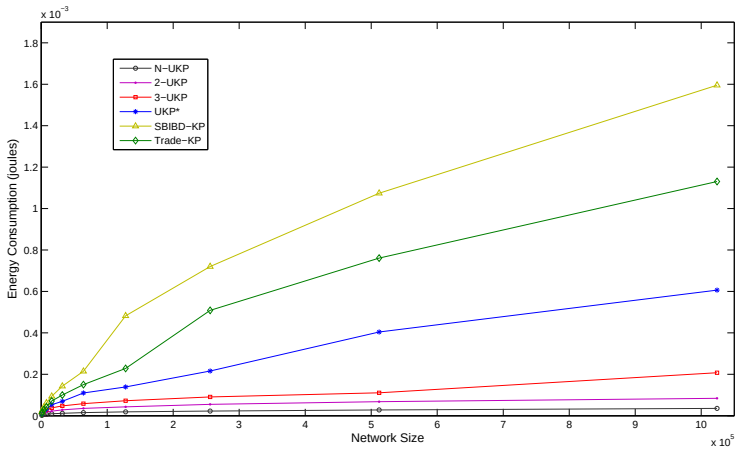

Fig. 6. Energy consumption at equal network size: we consider a grid deployment model [23] where η is set to $4\log(n)$ (n is the network size). The latter value ensures the physical network connectivity and coverage [23]. $\mathcal{E}_{tx}$ and $\mathcal{E}_{rx}$ are set to the values of CC1000 radio configuration, i.e. $1625\ nJ$ and $1156\ nJ$ resp. [24]

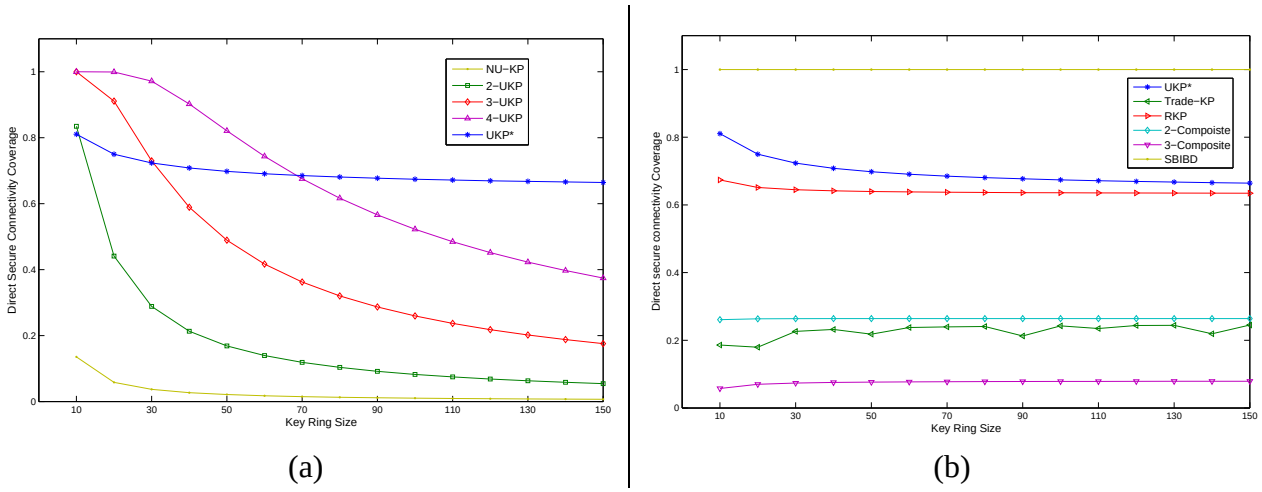

Fig. 7. Network connectivity at equal key ring size

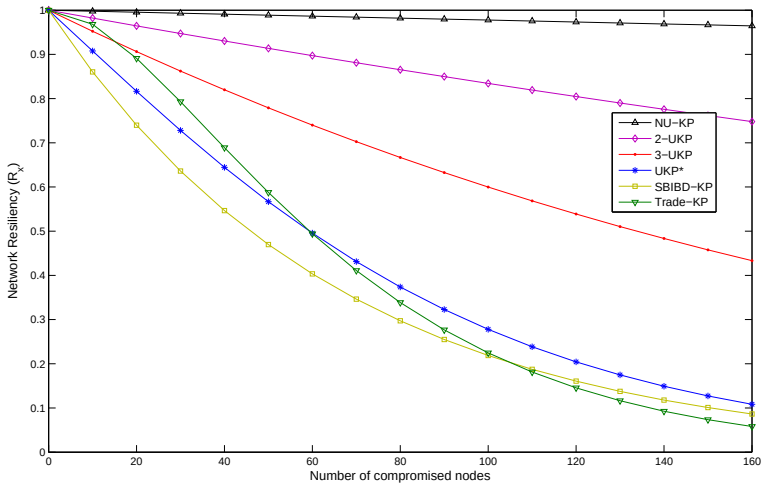

Fig. 8. Network resiliency at equal key ring size

TABLE I
EVALUATION METRICS

Performance Metric	Definition / Description
Network scalability	Represents the maximum number of generated key rings which corresponds to the maximum number of supported nodes.
Storage overhead	Measures the memory required to store keys in each node. We exclude the memory required to store the key identifiers since it is negligible compared to the key ring storage overhead (2-logarithm of the maximum number of keys).
Direct secure connectivity coverage	Defines the fraction of secured direct links among possible links in the network; it is computed as the probability that a given pair of neighboring nodes are able to establish a direct secure link.
Average secure path length	When two neighboring nodes have no common keys, they should establish a secure path composed of successive secure links. This metric measures the average length in hop count of these secure paths.
Network resiliency against node capture	We define the network *resiliency* R_x as the fraction of uncompromised external secure links when x sensor nodes are captured.

TABLE II
SUMMARY OF NOTATIONS

S	The global key pool
$\|S\|$	The size of the global key pool
KR_i	The key ring of node i
$\|KR_i\|$	The size of the node i key ring
n	The network size (number of nodes)
l	The key size
Q	The minimum number of common keys required to establish a secure link in the Q-composite scheme
m	The design order (SBIBD and Unital)
k	Key ring size & Block size of a given design
(q, k)	The two parameters of the Ruj et al. trade construction (k is also the block size)
$p(i)$	The probability that two nodes share exactly i keys in their subset of keys
P_c	The probability that two nodes can establish a secure link
R_x	The network resiliency when x nodes are captured

TABLE III
MAPPING FROM UNITAL DESIGN TO KEY PRE-DISTRIBUTION

Unital design	Key pre-distribution
X: Point set	S : Key pool
Blocks	Key rings ($< KR_i >$)
Size of a block ($k = m + 1$)	Size of a key ring ($k = \|KR_i\| = m + 1$)
Size of the object set X: $\nu = m^3 + 1$	Size of the key pool S: $\|S\| = m^3 + 1$
Number of generated blocks: $b = m^2(m^2 - m + 1)$	Number of generated key rings (supported nodes) : $n = m^2(m^2 - m + 1)$
Each point belongs to exactly m^2 blocks	Each key appears in exactly m^2 key rings

TABLE IV
COMPARISON OF UNITAL BASED SCHEMES TO SBIBD-KP SCHEME

K.R. Size	SBIBD-KP Scheme				Trade-KP scheme					UKP* scheme				
	m	Number of nodes	P_c	Avg. P. Lenght	q	k	Number of nodes	P_c	Avg. P. Lenght	m	t	Number of nodes	P_c	Avg. P. Lenght
30	29	871	1	1	31	30	1922	0.226	2.222	9	3	1704	0.73	1.271
68	67	4557	1	1	71	68	10082	0.226	2.093	16	4	13798	0.688	1.312
140	139	19461	1	1	149	140	44402	0.219	2.048	27	5	94343	0.637	1.362
228	227	51757	1	1	229	228	104882	0.247	1.941	37	6	282486	0.647	1.353