Sensornet:
A Key Predistribution Scheme for Distributed Sensors using Nets

(This paper is presented in SENSOERNETS, 2017.)

Deepak Kumar Dalai[1] and Pinaki Sarkar[2]

[1] *School of Mathematical Sciences, National Institute of Science Education and Research, Bhubaneswar 752 050, INDIA*

[2] *Department of Computer Science and Automation, Indian Institute of Science, Bengaluru 560 012, INDIA*

deepak@niser.ac.in, pinakisark@csa.iisc.ernet.in

Keywords: Partial Spread, Net, Combinatorial Designs, Key Predistribution Scheme, Distributed Sensor Networks.

Abstract: Key management is an essential functionality for developing secure cryptosystems; particularly for implementations to low cost devices of a distributed sensor networks (DSN)–a prototype of Internet of Things (IoT). Low cost leads to constraints in various resources of constituent devices of a IoT (sensors of a DSN); thereby restricting implementations of computationally heavy public key cryptosystems. This leads to adaptation of the novel key predistribution trick in symmetric key platform to efficiently tackle the problem of key management for these resource starved networks. After a few initial proposals based on random graphs, most key predistribution schemes (KPS) use deterministic (combinatorial) approaches to assure essential design properties. Combinatorial designs like a $(v,b,r,k)-$configuration which forms a $\mu(v,b,r,k)-$CID are effective schemes to design KPS (Lee and Stinson, 2005). A net in a vector space is a set of cosets of certain kind of subspaces called partial spread. A $\mu(v,b,r,k)-$CID can be formed from a net. In this paper, we propose a key predistribution scheme for DSN, named as sensornet, using net. Effectiveness of sensornet in term of crucial metrics in comparison to other prominent schemes has been theoretically established.

1 INTRODUCTION

Distributed (Wireless) Sensor Networks (DSN) are regarded as revolutionary information gathering systems owing to their easy deployment and flexible topology. They are decentralized with numerous low-cost identical resource starved wireless devices, called sensors or nodes, that deal with sensory data. They are considered to be a nice prototype of Internet of Things (IoT) which is a sophisticated concept that aims to connect our world. This has boosted the study of such distributed networks in modern times.

Prominent scientific applications of IoT are smart homes, smart cities, smart grids, smart water networks, agriculture, health-care, etc. Of particular interest are applications of DSN to networks where security is a premium; For instance, security may be essential for certain sensitive scientific and military networks that are meant for (i) military surveillance, (ii) force protection arenas, (iii) self healing minefields, and so on. Primary tasks of devices of an IoT in any such application are to collect information from their surrounding, process and forward them to other devices. Depending on specific applications, they may be further required to (i) track and/or classify an object, (ii) determine parametric value(s) of a given location, etc. These sensitive task for such critical applications create the necessity of secure message exchange among the low cost IoT devices.

1.1 Type of Cryptosystem for KPS

Constraints in resources of constituent ordinary devices of any IoT (like sensors of DSN) make us opt for symmetric key cryptosystems (SKC) over their public key counterparts while designing security protocols for such networks. SKC require both the sender and receiver(s) to possess same encryption-decryption key before message exchange. Standard online key exchange techniques that involve public parameters are generally avoided due to their heavy computations.

One can think of two trivial key distribution techniques. First is to assign a single key for entire network devices. Second is to think of assigning pairwise distinct (symmetric) keys for every pair of devices. Former method is completely vulnerable to single point failure (compromise of even one sensor reveals this single system key). Whereas, the second

strategy overloads the memory of each sensor; since $\mathcal{N}-1$ keys are required to be stored per sensor for a network of size $\mathcal{N}$. This is particularly impractical for large networks (i.e., large value of $\mathcal{N}$).

Treating a node (or a few) as Trusted Authority (TA) is risky. This also makes the network prone to single point failure as capture of this authority (sensor) acting as a TA makes the system vulnerable. Thereby schemes like Kerberos are avoided while designing secure key management schemes for DSN.

These facts emphasizes the importance of employing an adequate key management scheme for such networks. This stalemate situation was wittily overcome in 2002 by Eschenauer and Gligor by introducing the concept of *key predistribution* that involves applications of SKC to sensor networks. Any key predistribution scheme primarily execute the following:

- **Key distribution**: Prior to deployment, keys are preloaded into sensors to form their *keyrings or key chains* from the collection of all network keys, called *key pool*. Each system key is marked with an unique identifier *(key id)*. Certain schemes (Ruj and Roy, 2008) consider *(node id)* as an unique function of all the key ids. These key or, node id are used during key establishment.
- **Key establishment**: The preloaded keys are established by a two steps process, described below:

  (i) *Shared key discovery phase* establishes the shared common key(s) among the participant nodes. This may be achieved by broadcasting the key ids of all keys contained in the nodes (or node id). On receiving each other's key ids, the sensors tally (or equate) them to trace their mutual shared key id(s), hence common shared key(s).

  (ii) *Path key establishment phase* establishes an optimized path key between a pair of nodes that do not share a common key. This process involves intermediate nodes. Refer to common intersection designs in Section 3.

Depending on whether the above processes are probabilistic or deterministic, such schemes are classified into two types: (a) *random* and (b) *deterministic*. Sections 2.1 and 2.2 present a brief overview of individual type of schemes.

1.2 Paper Organization

Observing the significant advantages of deterministic KPS during key management for low cost distributed networks, we set out to propose one such scheme. Our proposal uses net partial spreads (or, nets) in a finite vector space that have been well studied combinatorially and as such, we name the scheme as sensornet. After a brief literature survey on KPS in Section 2, we present preliminaries of combinatorial set systems in KPS, partial spreads and nets in Section 3. Section 4 presents the design of our scheme sensornet that adhere to the desirable criteria set out in Section 2.4. We analyze sensornet in terms of various performance metrics set out in Section 5 and thereby establish our scheme's efficiency in comparison to prominent proposals. We briefly summarize our work in Section 6 while stating related future research directions.

2 A BRIEF SURVEY OF KPS

This section presents a state-of-the art survey of prominent KPS. We split survey into three stage: (i) first generation random KPS, (ii) deterministic KPS, and (iii) advantages of later type over former. Thereby, we justify proposal of our new deterministic KPS adhering to design criteria set out in Section 2.4.

2.1 Random Key Predistribution Schemes (RKPS)

First generation KPS rely on random graph theory pioneered by Erdős and Rényi (Erdős and Rényi, 1960) to preload (symmetric) cryptographic keys into sensors. Therefore, keyrings are formed randomly. This leads to probabilistic key sharing and establishment. Later is achieved by either broadcast of key ids or challenge and response Refer to (Eschenauer and Gligor, 2002, Section 2.1). Earlier, Blom proposed the first key distribution scheme (Blom, 1985) in public key settings meant for resourceful ad hoc networks. Blom's schemes uses pairs of public-private matrices for key distribution. It cannot be applied to resource constraint sensor networks due to its heavy memory requirement to store huge vectors. Several researchers use variants of Blom's schemes to propose both random and deterministic KPS for DSN. Çamptepe and Yener (Çamtepe and Yener, 2005) provides an excellent survey of the random KPS.

2.2 Deterministic Key Predistribution Schemes (DKPS)

First deterministic KPS were proposed simultaneous by Çamtepe and Yener (Çamtepe and Yener, 2004), Lee and Stinson (Lee and Stinson, 2005) and Wei and Wu (Wei and Wu, 2004) in 2004. Wei and Wu (Wei and Wu, 2004) combines subset-based schemes with existing key distribution schemes such as (Blom, 1985) to obtain multiple key spaces. Çamtepe and

Yener (Çamtepe and Yener, 2004) exploits combinatorial designs like symmetric Balanced Incomplete Block Designs (BIBD), generalized quadrangles and projective planes (see (Lee and Stinson, 2005; Lee and Stinson, 2008; Paterson and Stinson, 2014)). The scheme of Lee and Stinson (Lee and Stinson, 2005) uses quadratic equation solving and can be viewed as a scalable extension of their later proposal using Transversal Design ($TD(k,p)$). This work further summarizes the necessary conditions for a combinatorial design to yield a deterministic KPS. Certain KPS exploit special structures like Reed Solomon code based KPS (Ruj and Roy, 2008) that permit alternate combinatorial description (Bag et al., 2012; Paterson and Stinson, 2014). In the same light, we show our scheme derived from the net of partial spreads (or nets) can yield nice combinatorial properties meant for designing deterministic KPS.

2.3 Advantages of DKPS over RKPS

Deterministic schemes have certain advantages over their random counterparts. For instance, a desired property of a randomized scheme may occur only with a certain probability whereas they can be proven to hold in a deterministic scheme (refer to (Lee and Stinson, 2005; Lee and Stinson, 2008; Paterson and Stinson, 2014)). This led to proposals of numerous deterministic KPS (Lee and Stinson, 2005; Lee and Stinson, 2008; Bag et al., 2012) etc. using various combinatorial tricks. Further the predictable nature of these combinatorial structures has been efficiently exploited to address design weaknesses of certain prominent KPS. For instance (Dhar and Sarkar, 2011; Bag et al., 2012) primarily address the connectivity aspect of (Ruj and Roy, 2008) by deterministic and random approaches respectively.

Contrary to these observations, Ruj and Pal (Ruj and Pal, 2016) state that random graph models are well suited for 'scalability' and 'resilience'. Thereby, they justify their proposals of random graph based preferential attachment models with degree bounds. They design various network using their model. All of their designs suffers from highly skewed load distribution, poor connectivity and resiliency; and hence, are inappropriate for (distributed) IoT applications.

In fact, sensitive IoT applications require protocols to yield equal distribution of tasks among peers. Moreover, to reduce hops and hence potential risks from node capture, it is more important to have connected networks that can not be guaranteed by random schemes. So we opt for deterministic protocols for security applications in IoT networks that assure predictable (high) connectivity; despite most of them having restricted scaling operations. This is a major area of study for most (deterministic) KPS proposals, including ours (recalled in Section 6).

Observe that the structure of the combinatorial objects used to design deterministic KPS can not directly model networks of any specified size $\mathcal{N}$. Usually, such structures result in designs having a specific pattern in the number of resultant blocks; viz. a prime power etc. Since $\mathcal{N}$ can be any number, a standard strategy is to consider the least prime power that is greater than the network size (i.e., $p^r \geq \mathcal{N}$). Then $\mathcal{N}$ subset are randomly selected to form the key rings of the resultant network nodes. Bose et al. (Bose et al., 2013) speculate that random removal of blocks may have a disadvantageous affect on the underlying design properties and hence become an issue of concern.

Fortunately, this claim of Bose et al. has been successfully challenged by Henry et al. (Henry et al., 2014). Through practical experiments, they establish that random removal of key rings of a combinatorial KPS has negligible effect with overwhelming probability. This work reestablishes the importance of combinatorial schemes.

2.4 Desirable Design Criteria

Devices of an IoT (for instance, sensors of a DSN) are highly prone to damage and/or physical capture. This is a crucial consideration while designing any KPS. Primary objectives of any KPS is to ensure that the resulting network:

1. has less number of keys per node, i.e., sizes of individual keyrings are less;
2. have large *node support*, i.e., support large number of network nodes;
3. has good (ideally full secure) *connectivity*. Secure connectivity (or, simply *connectivity*) is the ratio of number of (secure) links in eventual network to all possible links. A pair of nodes are said to be connected by a (secure) link if there exists at least one secret key between them;
4. is *resilient* against adversarial attacks. A prevailing method adopted in most existing works (Çamtepe and Yener, 2004; Lee and Stinson, 2005; Bag et al., 2012; Paterson and Stinson, 2014) is to show that the standard resiliency coefficient $\mathtt{fail}(t)$ is minimized. Our work will follow suit. The quantifier $\mathtt{fail}(t)$ measures the ratio of links broken after compromise of t sensors to the total number of links in the remaining network. Notationally, $\mathtt{fail}(t) = \frac{b_t}{u_t}$, where b_t is the number of links broken when t nodes are compro-

mised and u_t is the total number of links among uncompromised nodes of remaining network.

Ideally a KPS should have small keyrings, and yet support large number of nodes with appreciable resiliency, scalability and communication probability (or connectivity). However, renowned scientists proved the impossibility of constructing a *perfect KPS* that meets all these criteria (Lee and Stinson, 2005; Paterson and Stinson, 2014). This motivates several designs that are robust for specific purpose.

3 PRELIMINARY

This section introduces the definitions and notations that are required to describe our scheme; sensornet.

3.1 Combinatorial Set Systems and KPS

Use of different combinatorial designs to obtain deterministic KPS was primarily presented in the paper (Lee and Stinson, 2005). After that there have been several KPS proposals based on combinatorial designs. A survey on KPS in WSN is available in (Chen and Chao, 2011). Recently in a more technical survey, Paterson and Stinson (Paterson and Stinson, 2014) present an unified treatment of prominent combinatorial designs in terms of partially balanced $t-$design. Basic design theoretic concepts are below:

Let $\mathcal{X}$ be a finite set. The elements of $\mathcal{X}$ are called varieties. Each subset of $\mathcal{X}$ is termed as a block. Consider $\mathcal{A}$ to be a collection of blocks of $\mathcal{X}$. Then the pair $(\mathcal{X},\mathcal{A})$ is said to be a *set system or, a design*. $(\mathcal{X},\mathcal{A})$ is regular (of degree r) if each point is contained in r blocks. $(\mathcal{X},\mathcal{A})$ is uniform (of rank k) if all blocks have the same size, say k.
A design $(\mathcal{X},\mathcal{A})$ is said to form a $(v,b,r,k)-$*design* if

- $|\mathcal{X}| = v$ and $|\mathcal{A}| = b$;
- it is regular of degree r and uniform of rank k.

A $(v,b,r,k)-$design forms a $(v,b,r,k)-$*configuration* if any arbitrary pair of blocks intersect in *at most* one point. Moreover, if any pairs of varieties occur in exactly λ block, then a $(v,b,r,k)-$design forms a $(v,b,r,k,\lambda)-$BIBD (Balanced Incomplete Block Designs). These designs can be used to construct various KPS(see (Lee and Stinson, 2005)) by mapping:

1. the v varieties of $\mathcal{X}$ to the set of keys in the scheme (*:=key pool*),
2. b to the number of nodes in the system (*:=network size*),
3. k to the number of keys per node (*:=size of key rings*), and
4. r to the number of nodes sharing a key (*:=degree of the resultant KPS*).

The target is to construct KPS with identical burden on each sensor. This leads to opting for design with uniform rank (k) and regular degree (r); so that every *key ring* is of equal size (k) and same number of nodes (r) share each key for the resultant network.

The *block graph* $\Gamma_{\mathcal{A}}$ of the set design $(\mathcal{X},\mathcal{A})$ is defined with the vertex set $\mathcal{A}$ and edge set $E_{\mathcal{A}} = \{(A,B) : A,B \in \mathcal{A} \text{ and } A \cap B \neq \emptyset\}$. If the set design is regular of degree r and uniform of rank k, then the block graph $\Gamma_{\mathcal{A}}$ is $k(r-1)-$regular.

A $(v,b,r,k)-$configuration $(\mathcal{X},\mathcal{A})$ is said to form a $\mu-$*common intersection design ($\mu-$CID)* in case:

$$|\{A_\alpha \in \mathcal{A} : A_i \cap A_\alpha \neq \emptyset \text{ and } A_j \cap A_\alpha \neq \emptyset\}| \geq \mu$$

whenever $A_i \cap A_j = \emptyset$, $\forall\, i \neq j$. It is important to construct design that maximize the value of μ.

3.2 Partial Spread and Net

Let $\mathbb{F}_p$ be the finite field on p elements where p is a prime. Denote $V_n = \mathbb{F}_p^n$ to be the vector space over the field $\mathbb{F}_p$ with zero vector $\mathbf{0}$. Since the finite field $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_p$ which is isomorphic to $\mathbb{F}_p^n$ (see (Lidl and Niederreiter, 1997)), we interchange the notation as per its suitability. The isomorphism mapping can be considered as any mapping from a basis set of $\mathbb{F}_{p^n}$ (e.g., $\{1,\alpha,\cdots,\alpha^{n-1}\}$ where α is a primitive root in $\mathbb{F}_p^n$) to a basis set of $\mathbb{F}_p^n$. We consider $n = 2m$ to be an even integer throughout the paper.

A *partial spread* Σ of order s in V_n is a set of pairwise supplementary $m-$dimensional subspaces $E_1, E_2, \cdots, E_s$ of V_n i.e., $E_i \cap E_j = \{\mathbf{0}\}$ for all $1 \leq i < j \leq s$. A partial spreadΣ is a *spread* if $\cup_{i=1}^{s} E_i = V_n$. It is well known that a spread of V_n exists since m divides n (Lu, 2008); in which case $|\Sigma| = p^m + 1$. Therefore, from a given spread Σ each of the $\binom{p^m+1}{s}$ choices of s members of Σ provides a partial spreadof V_n. Note that a partial spreadmight not be a subset of a spread (Eisfeld and Storme, 2000). A detailed combinatorial study of spread can be found in the book (Johnson, 2010; Johnson et al., 2007).

Let E be a subspace of the vector space V_n. A coset of E in V_n is of the form $\alpha + E = \{\alpha + v : v \in V_n\}$ for an $\alpha \in V_n$. The set of cosets make a disjoint partition of V_n. The element α is called a coset representative of the coset $\alpha + E$. Since E is an additive group, any element from the $\alpha + E$ can be a coset representative the coset. Given a partial spread$\Sigma = \{E_1, E_2, \cdots, E_s\}$ in V_n, let $\overline{E}_i$ be a set of coset representatives of subspace E_i for $1 \leq i \leq s$. Then the set $\mathcal{A} = \{\alpha + E_i : \alpha \in \overline{E}_i \text{ and } 1 \leq i \leq s\}$ i.e., set of all cosets of subspaces $E_i, 1 \leq i \leq s$ is called a *net* in V_n.

See the book (Johnson et al., 2007) for the combinatorial study of net.

4 SENSORNET

Sensornet is a proposal for a KPS for distributed (wireless) sensors. The design of sensornet results from the forthcoming set design and Theorem 1.

Given a partial spread$\Sigma = \{E_1, E_2, \cdots, E_s\}$ in V_n, let $\overline{E}_i$ be a supplementary subspace of E_i in V_n for $1 \leq i \leq s$ (i.e., their direct sum $E_i \oplus \overline{E}_i = V_n$ and $E_i \cap \overline{E}_i = \{\mathbf{0}\}$). It can be checked that $\overline{E}_i$ is a set of coset representatives of E_i for $1 \leq i \leq s$. Note that the subspaces E_i's in a partial spreadare pairwise supplementary. So, any $E_j, j \neq i$ can be chosen as $\overline{E}_i$. Consider the set system $(\mathcal{X}, \mathcal{A})$ such that $\mathcal{X} = V_n$ and and the set of blocks $\mathcal{A} = \{\alpha + E_i : \alpha \in \overline{E}_i \text{ and } 1 \leq i \leq s\}$ which is a net in V_n.

Theorem 1. *Given any partial spreadΣ, the set design $(\mathcal{X}, \mathcal{A})$ is a $\mu(p^n, sp^m, s, p^m)-$CID where $\mu = (s-1)p^m$.*

Proof. Here $v = |\mathcal{X}| = p^n$. Consider two blocks $\alpha + E_i$ and $\beta + E_j$. Now we have the following cases.

1. If $i = j$, then
   (a) $\alpha + E_i = \beta + E_j$ if $\alpha = \beta$ or,
   (b) $(\alpha + E_i) \cap (\beta + E_j) = \emptyset$ if $\alpha \neq \beta$.
2. If $i \neq j$, then we shall show that $|(\alpha + E_i) \cap (\beta + E_j)| = 1$. Since E_i and E_j are supplementary to each other, the element $\alpha - \beta \in V_n$ can be uniquely expressed as -$u + v$ where $u \in E_i$ and $v \in E_j$. That is, $\alpha - \beta = -u + v$ which implies, $\alpha + u = \beta + v$ is the unique element in $(\alpha + E_i) \cap (\beta + E_j)$.

Therefore, the number of blocks i.e., the number of cosets is $b = sp^m$ and each block contains $k = p^m$ elements. Given a subspace $E_i, i \in \{1, 2, \cdots, s\}$, each element $u \in V_n$ belongs to exactly one coset of E_i. So, each $u \in V_n$ belongs to exactly s many blocks in $\mathcal{A}$. The set design $(\mathcal{X}, \mathcal{A})$ is regular with $r = s$. Here, every two distinct blocks intersect each other by at most one element which implies that $(\mathcal{X}, \mathcal{A})$ is a $(p^n, sp^m, s, p^m)-$configuration.

We see that two blocks $\alpha + E_i$ and $\beta + E_j$ do not intersect iff $i = j$ and $\alpha \neq \beta$ i.e., both are distinct cosets of same subspace E_i. For the case of non intersecting blocks $\alpha + E_i$ and $\beta + E_i$, $\alpha \neq \beta$, both blocks intersect all other blocks of the form $\gamma + E_j$ where $j \neq i$. Since there are $\mu = (s-1)p^m$ such blocks $\gamma + E_j$ in $\mathcal{A}$, $(\mathcal{X}, \mathcal{A})$ is a $(s-1)p^m(p^n, sp^m, s, p^m)-$CID. □

Here, the set of blocks (i.e., $\mathcal{A}$) of the scheme $(\mathcal{X}, \mathcal{A})$ forms a net in a vector space. We denote the scheme as *sensornet*.

It can be checked that the block graph of $(\mathcal{X}, \mathcal{A})$ is a strongly regular graph with parameters $(n = sp^m, r = (s-1)p^m, \lambda = (s-2)p^m, \mu = (s-1)p^m)$. Moreover, the block graph is a complete $s-$partite graph. In the study of finite geometry, the varieties together with the blocks (i.e., cosets) form the points and lines of an affine plane. Since two non-parallel lines (i.e., $\alpha + E_i$ and $\beta + E_j$ for $i \neq j$) intersects at one point, this set of cosets is called net.

4.1 Example of NETS

There are numerous constructions of spreads and partial spreads that can be found in literature, see (Johnson et al., 2007). Now we present a few spreads $\mathcal{S}$ in $\mathbb{F}_p^n$, where p is a prime. For a given s, any $\Sigma \subseteq \mathcal{S}$ such that $|\Sigma| = s$ forms a partial spread of order s. By Theorem 1, this partial spread yields a KPS.

Spread I: This is a classical example of a spread from the additive group of the finite field F_{p^n}. Since $n = 2m, \mathbb{F}_{p^m}$ is a subspace of $\mathbb{F}_{p^n}$ with respect to a basis. Let $\{\alpha_i : 1 \leq i \leq p^m + 1\}$ be a set of coset representative of the cosets of the subgroup $\mathbb{F}_{p^m}^*$ of the multiplicative group $\mathbb{F}_{p^n}^*$. Then the set $\mathcal{S}_I = \{S_i = \alpha_i \mathbb{F}_{p^m}, 1 \leq i \leq p^m + 1\}$ is a spread in $\mathbb{F}_{p^n}$.

Spread II: This example of spread is represented in bivariate form (Bu, 1980). For each $\alpha \in \mathbb{F}_{p^m}$, define a subspace U_α of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by $U_\alpha = \{(\alpha u, u) | u \in \mathbb{F}_p^m\}$ and $U_\infty = \{(u, \mathbf{0}) | u \in \mathbb{F}_p^m\}$. The set $\mathcal{S}_{II} = \{U_\alpha : \alpha \in \mathbb{F}_{p^m}\} \cup U_\infty$ constitute a spread in $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \simeq \mathbb{F}_{p^n}$.

Spread III: This example of spread is generated from pre-quasifield, which is defined as following. A system $Q = (V, +, \circ)$, with $|V|$ finite, is a pre-quasifield if the following axioms hold:

(1) $(V, +)$ is an abelian group, with identity $\mathbf{0}$.

(2) $(V^*, \circ)$ is a quasigroup where $V^* = V \setminus \{\mathbf{0}\}$. That is, for any $a \in V^*$, the left multiplication operator $a \circ x$ and the right multiplication operator $x \circ a$ are both bijective from V^* to V^*.

(3) $\forall x, y, z \in V : (x + y) \circ z = x \circ z + y \circ z$.

(4) $x \circ \mathbf{0} = \mathbf{0}$, $\forall x \in V$.

Now assuming $(\mathbb{F}_{p^m}, +, \circ)$ is a pre-quasifield, set $E_a = \{(x, a \circ x) : x \in \mathbb{F}_{p^m}\}$ for any $a \in \mathbb{F}_{p^m}$ and $E_\infty = \{(\mathbf{0}, x) : x \in \mathbb{F}_{p^m}\}$. Then it can be checked that $S_{III} = \{E_a : a \in \mathbb{F}_{p^m} \cup \{\infty\}\}$ is a spread in $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ (Johnson et al., 2007). Many pre-quasifields are available in literature. Refer to (Wu, 2013) for three types of pre-quasifields on set $\mathbb{F}_{2^m}$ and (Çeşmelioğlu et al., 2015) for a pre-quasifield on set $\mathbb{F}_{p^m}$.

Example 1. *Here, we present a simple KPS from the spread of type S_I. Take $V_n = \mathbb{F}_{3^2} = \mathbb{F}_3[x]/(x^2+1)$. Consider the subspace $\mathbb{F}_3 = \{0,1,2\}$ and $\{1,x,x+1,x+2\}$ a set of coset representatives of $\mathbb{F}_3^*$ in $\mathbb{F}_{3^2}$. Then $\mathcal{S}_I = \{\{0,1,2\},\{0,x,2x\},\{0,x+1,2x+2\},\{0,x+2,2x+1\}\}$ is a spread in $\mathbb{F}_3^2$. Consider a partial spread $\Sigma = \{E_1 = \{0,1,2\}, E_2 = \{0,x,2x\}\}$ with $\overline{E}_1 = E_2$ and $\overline{E}_2 = E_1$. Therefore, by Theorem 1, the set $\mathcal{X} = \mathbb{F}_3^2$ and the* net $\mathcal{A} = \{\{0,1,2\},\{x,x+1,x+2\},\{2x,2x+1,2x+2\},\{0,x,2x\},\{1,x+1,2x+1\},\{2,x+2,2x+2\}\}$ *forms a KPS $(\mathcal{X},\mathcal{A})$. The block graph of $(\mathcal{X},\mathcal{A})$ is the $K_{3,3}$.*

5 Analysis of Sensornet

In this section we present the values of some important metrics involved in our proposed scheme; sensornet.

5.1 Time and space complexities for key establishment (T_k, M_k)

For the key establishment between two nodes, the nodes need to discover a common key stored between them. For this purpose the nodes need to broadcast some data, which is required to trace the common key between two nodes. Since the sensor nodes have low memory and computation power, data and time requirement for key establishment are two very important factors to design a KPS. In this subsection we discuss the process of key establishment between two nodes and associated time and data requirement of the process. In case of path key establishment (refer to Section 1.1, both the concerned nodes have to find a common neighbor node with whom they discover their share key and establish connection via this neighbor. Let denote T_k and M_k be the time and memory complexity function for the key establishment in vector space V_n.

The blocks of sensornet forms a net, i.e., they are affine spaces. Hence, the nodes can be identified by their basis vectors and the key establishment is done using the node id. Let $\beta_i^1, \beta_i^2, \cdots, \beta_i^m$ be a basis set of the subspace E_i for $1 \le i \le s$. Then, the node $\alpha + E_i$ can be identified by the node id $(\alpha, \beta_i^1, \beta_i^2, \cdots, \beta_i^m)$. When the nodes $\alpha + E_i$ and $\beta + E_j$ need key establishment between them the following process can be followed.

Step 1: The nodes $\alpha + E_i$ and $\beta + E_j$ compare the last m vectors (i.e., the basis vectors) in their node id. If they are same then follow Step 3 otherwise follow Step 2.

Step 2: In this case, we have $E_i \neq E_j$ i.e., they share a common key. Let the common key is $\alpha + u = \beta + v$ where $u \in E_i$ and $v \in E_j$. Now we need to find u and v in terms of the basis vectors of E_i and E_j respectively. Here, $\alpha - \beta = v - u \in V_n$. Since E_i and E_j are supplementary subspaces in V_n, $\alpha - \beta$ can be uniquely expressed as a linear combination of the basis vectors of E_i and E_j. Let $\alpha - \beta = b_1\beta_i^1 + \cdots + b_m\beta_i^m + b_{m+1}\beta_j^1 + \cdots + b_n\beta_j^m$, where $b_i \in \mathbb{F}_p$. That is, $\alpha - b_1\beta_i^1 - \cdots - b_m\beta_i^m = \beta + b_{m+1}\beta_j^1 + \cdots + b_n\beta_j^m$. Hence, the common key is $\alpha - b_1\beta_i^1 - \cdots - b_m\beta_i^m \in E_i$ which is $\beta + b_{m+1}\beta_j^1 + \cdots + b_n\beta_j^m \in E_j$. The time complexity in this step is the time complexity to express $\alpha - \beta$ in terms of the basis vectors in a basis i.e., $O(n^3)$.

Step 3: In this case, the $E_i = E_j$ i.e., they do not share any common key. In this case, they have e to establish connection through another node with whom they share a key. That is, they have to find a node $\gamma + E_k$ where $k \neq i$. The probability of finding such a node using a random pick up is $\frac{s-1}{s}$ which is very high. Since both $\alpha + E_i$ and $\beta + E_j$ share a key with $\gamma + E_k$, each one do the same process described in Step 2 with $\gamma + E_k$ to discover their common key. After that $\alpha + E_i$ and $\beta + E_j$ can establish connection through $\gamma + E_k$. Hence, the time complexity in this case is too $O(n^3)$.

Therefore, each node has to spend $M_k = (m+1) * n * \log_2 p = O(n^2)$ bits of data for broadcasting of their identification and the time complexity to discover the common key(s) is $T_k = O(n^3)$. Note that in sensornet scheme, nodes have to broadcast only node id i.e., $O(n^2)$ bits instead of all (i.e., $O(rp^{\frac{n}{2}})$ many) key ids as broadcast by many other proposed schemes.

5.2 Key-node ratio (σ)

The *key-node ratio* is defined as $\sigma = \frac{k}{b}$. This ratio provides idea about the storage requirement of the scheme at each node with respect to the total number of nodes. With this metric we can compare the storage requirement of the schemes from different designs. It is desirable for this ratio σ to be as small as possible as lesser amount of memory required for key storage at each node. In sensornet $(\mathcal{X},\mathcal{A})$, key-node ratio $\sigma = \frac{p^m}{sp^m} = \frac{1}{s} = \frac{1}{|\Sigma|}$. If the size of partial spread is larger, then the storage requirement to store keys in sensornet is lesser.

5.3 Resiliency($\mathtt{fail}(t)$)

The schemes need to be well equipped to perform against adversarial attacks. To this end, the standard resiliency metric $\mathtt{fail}(t)$ need to be minimized. This is prevalent method adopted by most existing works (Bag et al., 2012; Çamtepe and Yener, 2004; Lee and Stinson, 2004; Lee and Stinson, 2005; Paterson and Stinson, 2014). The quantifier $\mathtt{fail}(t)$ measures the probability that a random link between two sensor nodes is broken due to the compromise of t other random nodes. Notationally, $\mathtt{fail}(t) = \dfrac{b_t}{u_t}$, where b_t is the number of links broken when t nodes are compromised and u_t is the total number of links among uncompromised nodes of remaining network. Theorem 2 is due to Lee and Stinson (Lee and Stinson, 2005, Section VIII) provides the formula to compute $\mathtt{fail}(t)$ for any $(v,b,r,k,1)-$configuration.

Theorem 2. *For any $(v,b,r,k,1)-$configuration, the value of the metric $\mathtt{fail}(t)$ on random compromise of t nodes is given by:*

$$\mathtt{fail}(t) = 1 - \left(\frac{b-r}{b-2}\right)^t. \tag{1}$$

Corollaries 1 is an immediate outcomes of substituting in Equation 1, the values of b and r, that sensornet achieves.

Corollary 1. *The value of the resilience $\mathtt{fail}(t)$ for the set design $(\mathcal{X},\mathcal{A})$ of the scheme sensornet, which is a $(p^n, sp^m, s, p^m)-$configuration is*

$$\mathtt{fail}(t) = 1 - \left(\frac{sp^m - s}{sp^m - 2}\right)^t.$$

In particular,

$$\mathtt{fail}(1) = \frac{s-2}{sp^m-2} = \frac{1}{p^m} - \frac{2p^m-2}{p^m(sp^m-2)} \approx p^{-m}.$$

The metric $\mathtt{fail}(1) = O(p^{-m})$ i.e., if a node N is compromised, then the probability that a link (which is not incident with N) fails is $O(p^{-m})$. Here, the size of the partial spread(i.e., s) has no significant effect on $\mathtt{fail}(1)$. As an example, if $n = 10$ and $p = 2$ (i.e., there are $2^{10} \approx 1000$ many nodes) then the value of $\mathtt{fail}(1) \approx 0.03$.

5.4 Connectivity(p_e)

We say two blocks in a set system are connected by $e-$links (or, are at a distance e) if the shortest path between them in the block graph includes e edges. Hence, we define the metric connectivity (or, connection probability) p_e of the network to be the probability that two nodes (placed in physical neighborhood) are connected by $e-$links for a positive integer e.

Observe that the value of e for a $\mu-$CID with $\mu > 1$ is either 1 (if they share a key) or 2 (if they do not share a key). The formulae for p_1 and p_2 are provided in (Lee and Stinson, 2005, Section VI), which are being formally restated in the following theorem. Let η denote the number of nodes in the intersection of the physical neighborhood of two given nodes.

Theorem 3. *The value of the matric connectivities of a $\mu(v,b,r,k)-$CID are given by $p_1 = \frac{k(r-1)}{b-1}$ and $p_2 \approx (1-p_1) \times \left(1 - \left(\frac{b-\mu-2}{b-2}\right)^\eta\right)$.*

The following corollary is an immediate outcome for our scheme by substituting the values of b, r, k and λ in Theorem 3.

Corollary 2. *The value of the metric connectivities for the set system $(\mathcal{X},\mathcal{A})$, which is a $(s-1)p^m - (p^n, sp^m, s, p^m)-$CID are*

$$p_1 \approx 1 - \frac{1}{s} \text{ and } p_2 \approx \frac{s^\eta - 1}{s^{\eta+1}}.$$

Proof. Now putting the value of $b = sp^m, r = s, k = p^m$ and $\mu = (s-1)p^m$ in p_1 and p_2, we have

$$p_1 = \frac{p^m(s-1)}{sp^m-1} = \frac{sp^m-p^m}{sp^m-1} = 1 - \frac{p^m-1}{sp^m-1} \approx 1 - \frac{1}{s}$$

$$\text{and } p_2 \approx \frac{1}{s}\left(1 - \left(\frac{sp^m-(s-1)p^m-2}{sp^m-2}\right)^\eta\right)$$

$$= \frac{1}{s}\left(1 - \left(\frac{p^m-2}{sp^m-2}\right)^\eta\right) \approx \frac{1}{s}\left(1 - \frac{1}{s^\eta}\right) = \frac{s^\eta-1}{s^{\eta+1}}.$$

□

The metric $p_1 \approx 1 - \frac{1}{s}$ i.e., the connectivity increases if the size of spread increases. Here, the size of base field (i.e., the value of p) has no significant effect on p_1. As an example, if $n = 10$, $p = 2$ (i.e., there are $2^{10} \approx 1000$ many nodes) and $s = 2^5$ then the value of $p_1 = 1 - 2^{-5}$.

5.5 Comparative Study

This subsection presents a comparative study of sensornet with prominent existing works with respect to connectivity, resilience and network scaling. Performance of sensornet with respect to other metric like storage, etc. has been discussed in previous section.

5.5.1 Connectivity and Resiliency Tradeoff:

The schemes with high connectivity (i.e., p_1) and resiliency (i.e., $\mathtt{fail}(1)$) as small as possible are preferred. As unfortunately, both the metrics behave in opposite way, it is a fundamental problem of trading off connectivity against resiliency. In (Dong et al.,

2011; Paterson and Stinson, 2014), the ratio $\rho = \frac{p_1}{\mathtt{fail}(1)}$ is considered for the comparison of several combinatorial designs. Therefore, the larger value of ρ confirms of higher connectivity and lower resiliency. It is desirable that the ratio ρ be as large as possible.

There have been several proposals for deterministic key predistribution schemes for wireless sensor networks based on various types of combinatorial structures such as designs and codes. The paper (Paterson and Stinson, 2014) proposes a general framework by unifying those structures into a new design, termed as "partially balanced t-designs(PBtD)". Although, our scheme sensornet falls into $2-(v,k,\lambda_0 = b,\lambda_1 = r)-$PBtD as a configuration, the generalization does not consider $\mu-$CIDs. Hence, being a $\mu-$CID, sensornet does not classify as PBtD by their description (Paterson and Stinson, 2014). There are few comparison tables of different schemes are provided in (Paterson and Stinson, 2014). In the following, we take data of TD(t,k,Q) with intersection threshold $\eta = 1$ from the paper (Paterson and Stinson, 2014) along with other designs to compare with the scheme sensornet.

Let consider the number of nodes in all the compared scheme is $\mathcal{N}$. Now we shall compare the asymptotic behavior of metrics $p_1, \mathtt{fail}(1)$ and the ratio ρ. The comparison is displayed in Table 1.

From this comparison table it is clear that the asymptotic behavior of the ratio ρ of sensornet $(\mathcal{X},\mathcal{A})$ is similar or better than all other schemes except the scheme $TD(3,k,q), k = q$ and Merging Block (MB) design of (Bag et al., 2012). Former scheme needs computation of some number theoretic problems during key agreement; while the later has significantly less (merging) block support (halved). Moreover, in our scheme $(\mathcal{X},\mathcal{A})$, the shared key discovery is done with time complexity $O((\log_p \mathcal{N})^3)$ and the amount of data need to be broadcast is $O((\log_p \mathcal{N})^2)$. This is an added advantage over most KPS that require key id comparisons during key discovery.

5.5.2 Scalability Comparison:

Sensornet $(\mathcal{X},\mathcal{A})$ can support large networks. This is because the choice n and respectively m and/or s are unbounded in theory. This may help in scaling networks designed by our schemes (prefix large values).

Scalability, otherwise is a major challenge in most deterministic KPS. For instance the schemes (Çamtepe and Yener, 2004; Lee and Stinson, 2004; Lee and Stinson, 2005; Lee and Stinson, 2008; Ruj and Roy, 2008) have restricted scaling. This owes to the fact that key establishment for these network require general solutions of polynomials. Therefore the complexity of the key establishment process increases with increment in degree of these polynomials. Random schemes can scalable arbitrarily (Ruj and Pal, 2016); at the expense of desirable parameters like connectivity, resilience, storage (key-node ratio), etc. Therefore we opt deterministic schemes while designing KPS (Paterson and Stinson, 2014). Also refer to Section 2.3.

6 CONCLUSION

Realizing the need of deterministic KPS with desirable properties (set out in Section 2.4) to address the problem of key management in low cost networks, we propose one such scheme. Since the scheme is constructed using nets in a vector space, we named as sensornet. Key establishment of sensornet is a great advantage over many other schemes. Although sensornet suffers from lack of full connectivity, it is very close to full connectivity for large size of partial spread. Moreover, the generic computations in Section 5.4 establish that connectivity of sensornet is good (either direct or $1-$hop path connectivity), it is preferable to have full connectivity or at least a deterministic path in case of $1-$hop connectivity. The sophisticated MB designs of (Bag et al., 2012; Dhar and Sarkar, 2011) establishes a deterministic $1-$hop connectivity for the Reed Solomon code based KPS (Ruj and Roy, 2008). These heavily design dependent works can certainly open the doors for future research by considering similar constructions over sensornet in place of other combinatorial design based schemes.

Table 1: Comparison of asymptotic behavior of different schemes.

Scheme	No. of nodes	p_1	$\mathtt{fail}(1)$	$\rho = \frac{p_1}{\mathtt{fail}(1)}$
$(\mathcal{X}, \mathcal{A})$ (sensornet)	$\mathcal{N} = sp^m$	$1 - \frac{1}{s}$	$p^{-m} = \mathcal{N}^{\frac{-1}{2}}$	$(1 - \frac{1}{s})\mathcal{N}^{\frac{1}{2}}$
$TD(2,k,q),\ k = cq$ (Paterson and Stinson, 2014)	$\mathcal{N} = q^2$	c	$\frac{1}{q} = \mathcal{N}^{\frac{-1}{2}}$	$c\mathcal{N}^{1/2}$
$TD(3,k,q),\ k = cq, c < 1$ (Paterson and Stinson, 2014)	$\mathcal{N} = q^3$	$\frac{c(2-c)}{2}$ $= c - \frac{c^2}{2}$	$\frac{2(1-c)}{(2-c)}\mathcal{N}^{\frac{-1}{3}}$	$\frac{c(2-c)^2}{4(1-c)}\mathcal{N}^{1/3}$
$TD(3,k,q), k = q$ (Paterson and Stinson, 2014)	$\mathcal{N} = q^3$	$1/2$	$5\mathcal{N}^{\frac{-2}{3}}$	$\frac{1}{10}\mathcal{N}^{\frac{2}{3}}$
$TD(4,k,q), k = cq$ (Paterson and Stinson, 2014)	$\mathcal{N} = q^4$	$\frac{c(c^2-3c+6)}{6}$	$\frac{3(c^2-2c+2)}{c^2-3c+6}\mathcal{N}^{\frac{-1}{4}}$	$\frac{c(c^2-3c+6)^2}{18(c^2-2c+2)}\mathcal{N}^{\frac{1}{4}}$
Symmetric BIBD (Çamtepe and Yener, 2004)	$\mathcal{N} = q^2 + q + 1$	1	$\mathcal{N}^{\frac{-1}{2}}$	$\mathcal{N}^{\frac{1}{2}}$
RS code based (Ruj and Roy, 2008)	$\mathcal{N} = q^2$	$\frac{q-1}{q+1}$	$\mathcal{N}^{\frac{-1}{2}}$	$\mathcal{N}^{\frac{1}{2}}$
MB designs for $TD(2kq)$ or RS code (Bag et al., 2012)	$\mathcal{N} = q^2/2$	1	$(2\mathcal{N})^{\frac{-1}{2}}$	$(2\mathcal{N})^{\frac{1}{2}}$

REFERENCES

Bag, S., Dhar, A., and Sarkar, P. (2012). 100% connectivity for location aware code based kpd in clustered wsn: Merging blocks. In *Information Security Conference, ISC 2012*, number 7483 in Lecture Notes in Computer Science, pages 136–150. Springer-Verlag.

Blom, R. (1985). An optimal class of symmetric key generation systems. In *Advances in Cryptology - Eurocrypt 1984*, number 209 in Lecture Notes in Computer Science, pages 335–338. Springer-Verlag.

Bose, M., Dey, A., and Mukerjee, R. (2013). Key predistribution schemes for distributed sensor networks via block designs. *Design, Codes and Cryptography*, 67(1):111–136.

Bu, T. (1980). Partitions of a vector space. *Discrete Mathematics*, 31:79–83.

Çamtepe, S. A. and Yener, B. (2004). Combinatorial design of key distribution mechanisms for wireless sensor networks. In *9th European Symposium on Research Computer Security, ESORICS 2004*, number 3193 in Lecture Notes in Computer Science, pages 293–308. Springer-Verlag.

Çamtepe, S. A. and Yener, B. (2005). Key distribution mechanisms for wireless sensor networks: a survey. Technical report, Rensselaer Polytechnic Institute. Available at www.cs.rpi.edu/research/pdf/05-07.pdf.

Çeşmelioğlu, A., Meidl, W., and Pott, A. (2015). Bent functions, spreads, and o-polynomials. *SIAM Journal of Discrete Mathematics*, 29(2):854–867.

Chen, C. Y. and Chao, H. C. (2011). A survey of key predistribution in wireless sensor networks. *Security and Communication Networks*, 7(12).

Dhar, A. and Sarkar, P. (2011). Full communication in a wireless sensor network by merging blocks of a key predistribution using reed solomon code. In *Proceedings of CCSEA 2011, CS & IT 02*, pages 389–400.

Dong, J. W., Pei, D. Y., and Wang, X. L. (2011). A class of key predistribution schemes based on orthogonal arrays. *Journal of Computer Science and Technology*, 23:825–831.

Eisfeld, J. and Storme, L. (2000). (partial) t-spreads and minimal t-covers in finite projective spaces. In Lecture notes for the Socrates Intensive Course on Finite Geometry and its Applications, University of Ghent.

Erdős, P. and Rényi, A. (1960). On the evolution of random graphs. Publication of the Mathematical Institute of the Hungarian Academy of Sciences.

Eschenauer, L. and Gligor, V. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of 9th ACM conference on computer and communications security*, pages 41–47. ACM press.

Henry, K. J., Paterson, M. B., and Stinson, D. R. (2014). Practical approaches to varying network size in combinatorial key predistribution schemes. In *Selected Areas in Cryptography (SAC) 2013*, number 8282 in Lecture Notes in Computer Science, pages 89–117. Springer-Verlag.

Johnson, N. L. (2010). *Combinatorics of Spreads and Parallelisms*. CRC Press.

Johnson, N. L., Jha, V., and Biliotti, M. (2007). *Handbook of Finite Translation Planes*, volume 289 of *Pure and Applied Mathematics*. Chapman & Hall/CRC.

Lee, J. and Stinson, D. R. (2004). Deterministic key predistribution schemes for distributed sensor networks. In *Selected Areas in Cryptography (SAC) 2004*, number 3357 in Lecture Notes in Computer Science, pages 294–307. Springer-Verlag.

Lee, J. and Stinson, D. R. (2005). A combinatorial approach to key predistribution for distributed sensor networks. In *IEEE Wireless Communications and Networking Conference, WCNC-2005*, pages 1200–1205.

Lee, J. and Stinson, D. R. (2008). On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Transactions on Information and System Security*, 11(2):854–867.

Lidl, R. and Niederreiter, H. (1997). *Finite fields*. Encyclopaedia of mathematics and its applications. Cambridge University Press.

Lu, H. Y. (2008). Partial spreads and hyperbent functions in odd characteristic. Master's thesis, Simon Fraser University.

Paterson, M. B. and Stinson, D. R. (2014). A unified approach to combinatorial key predistribution schemes for sensor networks. *Design, Codes and Cryptography*, 71(3):433–457.

Ruj, S. and Pal, A. (2016). Preferential attachment model with degree bound and its application to key predistribution in WSN. In *IEEE Conference on Advanced Information Networking and Applications, AINA 2016*, pages 677–683.

Ruj, S. and Roy, B. K. (2008). Key predistribution schemes using codes in wireless sensor networks. In *Information Security and Cryptology, Inscrypt 2008*, number 5487 in Lecture Notes in Computer Science, pages 275–288. Springer-Verlag.

Wei, R. and Wu, J. (2004). Product construction of key distribution schemes for sensor networks. In *Selected Areas in Cryptography (SAC) 2004*, number 3357 in Lecture Notes in Computer Science, pages 280–293. Springer-Verlag.

Wu, B. (2013). Ps bent functions constructed from finite pre-quasifield spreads. Available at http://arxiv.org/pdf/1308.3355.pdf.