Wireless Networks (2019) 25:1185–1199
https://doi.org/10.1007/s11276-018-1698-z

A new hybrid key pre-distribution scheme for wireless sensor networks

Alok Kumar[1] · Alwyn Roshan Pais[1]

Published online: 9 March 2018

Abstract
This article presents a novel hybrid key pre-distribution scheme based on combinatorial design keys and pair-wise keys. For the presented scheme, the deployment zone is cleft into equal-sized cells. We use the combinatorial design based keys to secure intra-cell communication, which helps to maintain low key storage overhead in the network. For inter-cell communication, each cell maintain multiple associations with all the other cells within communication range and these associations are secured with pair-wise keys. This helps to ensure high resiliency against compromised sensor nodes in the network. We provide in-depth analysis for the presented scheme. We measure the resiliency of the presented scheme by calculating fraction of links effected and fraction of nodes disconnected when adversary compromises some sensor nodes in the network. We find that the presented scheme has high resiliency than majority of existing schemes. Our presented scheme also has low storage overhead than existing schemes.

Keywords Combinatorial design · Pair-wise keys · Key pre-distribution · Secure communication · Wireless sensor networks (WSNs)

1 Introduction

In recent times, wireless sensor network (WSNs) have attracted lot of attention for providing backbone to many mission critical applications like, alarm systems, health monitoring and surveillance, etc. [1, 2]. WSN normally consists of large number of sensor nodes and a base station, where base station gathers data from all the sensor nodes. Sensor nodes are usually battery powered and have limited storage and computational capabilities. As WSNs are deployed in inhospitable environments, they are prone to many attacks [2]. Thus, communication between the sensor nodes can easily be monitored and altered by an adversary. To secure the communication between sensor nodes, messages should be sent in encrypted format. Because of limited computation capabilities of sensor nodes, symmetric encryption is more viable option. For symmetric encryption of the messages, secret keys are accredited to all the sensor nodes. Key pre-distribution is a method to assign secrets keys to all the sensor nodes at the time of stationing.

Key pre-distribution can be done in many ways, easiest of all is to assign a single secret key to all the sensor nodes. But the security of whole network can break instantly if adversary is able to capture this secret key. More practical approach for key pre-distribution is assignment of unique pair-wise keys to each link between sensor nodes in the network. The resiliency of such setup is very high, as compromising of any pair-wise key has no effect on remaining network. But pair-wise keys based setup has huge key storage overhead, as each sensor node needs to maintain keys with all the other sensor nodes in the network. Combinatorial design based key pre-distribution is like a middle ground, where we compromise resiliency of the network for saving storage overhead. Such design includes assignment of set of keys to all the sensor nodes in such a way that any given pair of key-sets have some shared keys.

In this article we introduce a new deterministic hybrid key pre-distribution scheme for homogeneous network. In recent times many pair-wise keys based schemes [3, 4] and combinatorial design based schemes [5–8] have been

✉ Alok Kumar
alok_21@outlook.com

Alwyn Roshan Pais
alwyn.pais@gmail.com

[1] Information Security Research Lab, Department of Computer Science and Engineering, National Institute of Technology Karnataka - Surathkal, Surathkal, Karnataka, India

introduced, but all of them have their own associated drawbacks. We in our scheme use both pair-wise keys and combinatorial design based keys to present a novel hybrid key pre-distribution scheme. Our scheme takes advantages of both the worlds (pair-wise keys and combinatorial design based keys), but does not inherit disadvantages of the both. In the presented scheme we use combinatorial design based keys for intra-cell communication. For inter-cell communication, we maintain multiple associations between each pair of cells within communication range and these associations are secured using pair-wise keys. This helped us in obtaining much higher resiliency than [5–8] and very less storage overhead than [3, 4, 9].

1.1 Related work

Many key pre-distribution schemes have been introduced which either use combinatorial designs or pair-wise keys to allocate keys to the sensor nodes. Polynomial based key sharing mechanism was presented by Blundo et al. [10], where nodes use polynomial evaluation to retrieve the pair-wise keys. This method of key assignment was inherited by Liu and Ning [3, 4] to assign keys to all the sensor nodes in the network. These schemes were one of the first schemes which used deployment knowledge for key pre-distribution.

A new method of key pre-distribution was formulated by Blom [11] which used symmetric matrices. For the scheme two matrices were maintained, a public matrix and a private matrix. Sensor nodes uses the private matrix's row with the public matrix to identify shared secret keys. Using multiple key spaces, Du et al. [12] proposed a multi space blom scheme. Further authors used deployment knowledge to propose an improved scheme [13]. Huang and Medhi [14] and Huang et al. [15] adopted multiple space blom filter and location knowledge of sensor nodes to introduce a new key pre-distribution scheme.

Simonova et al. [9] discussed two pre-distribution schemes, one for homogeneous networks and other for heterogeneous networks. In both the networks two key pools are maintained namely, deployment key pool and original key pool. Each cell maintains a unique original key pool, whereas fixed number of cells share deployment key pool.

In Ruj and Roy [5], authors presented a new key pre-distribution scheme based on combinatorial design. For key assignment in the network, authors used transversal design. Authors used a heterogeneous network having two types of sensor nodes, ordinary sensor nodes and agents. Within a particular cell ordinary sensor nodes can communicate directly. For communication across the cells agents are used. Bag [6] proposed another combinatorial design based scheme for heterogeneous networks. His scheme had multiple agents in each cell opposite to fixed number of agents in scheme [5]. Bag and Roy [7] proposed another combinatorial design based key pre-distribution scheme which adopted Blom's [11] scheme. Another combinatorial design based key pre-distribution scheme was formulated by Mitra et al. [8], which used projective planes and pair-wise connectivity.

1.2 Organization

The remaining article is structured as follows: Sect. 2 provides the basic concepts needed for the presented scheme. Section 3 explains the presented scheme. In-depth analysis of presented scheme is given in Sect. 4. Section 5 provides comparison of the presented scheme with existing schemes. Finally, Sect. 6 provides the conclusion and future work for the proposed scheme.

2 Preliminaries

2.1 Combinatorial design

A set system [16] is a 2-tuple *(X,A)*, where X is a flock of elements and A is set of subsets of X. This set of subsets is also called *blocks*. A Balanced Incomplete Block Design (BIBD) is formulated by (v, b, r, k, λ), where v is the total number of elements in X and b is the total number of blocks. Such design fulfill following properties:

- Every element of X is present in r blocks,
- Each block has k elements,
- Each pair of element of X is present in exactly λ blocks.

A BIBD is called *Symmetric Design* or Symmetric BIBD when v=b. It can also be shown that in a Symmetric BIBD k=r [16].

A difference set $(v, k, \lambda)(mod v)$ is a set $D = \{d_1, d_2, \ldots, d_k\}$, where d_k represents distinct elements of Z_v, such that each element d, where $d \neq 0$ can be expressed in the form $d = d_i - d_j (mod\ v)$ in exactly λ ways [16, Defination 2.1.1]. Using the difference set D, blocks for symmetric design (v, k, λ) can be easily obtained by $D, D+1, D+2, D+3, \ldots, D+(v-1)(mod\ v)$ [16, Theorem 2.5.2].

A multiplier (q) [17] of a given difference set (D) for (v, k, λ) in an Abelian group $(G, +)$ satisfies following properties:

- q is a prime number such that $gcd(q, v) = 1$,
- $q > \lambda$ such that $k - \lambda \equiv 0 (mod\ q)$.

2.2 Lee sphere region

For understanding *Lee sphere* we consider a deployment area which is divided into equal-sized cells. A *Lee sphere* [18] for the given Lee distance ρ, centered at any particular cell consists of all the other cells which lie within ρ distance from the chosen cell. Distance between any two cells can be observed as *Manhattan distance* [19] between them, where sum of horizontal and vertical distance between any two cells is the distance between them. For simplicity, we take centers of two cells to find the distance between them. For example in Fig. 1, highlighted region shows *Lee sphere* region of cell C_{13} with Lee distance $\rho = 2$.

2.3 Bloom filter

Bloom Filter [20] is a renowned data structure, which is used to verify membership of elements efficiently. Given an element, by adopting bloom filter we can find whether a particular element is present in a predefined set or not. Bloom filter uses a set $T = \{t_1, t_2, t_3 \ldots, t_x\}$, a string of size f-bits and s independent hash functions $(H_1, H_2, \ldots H_s)$. Each hash function (H_i) takes an item (t_i) as input and maps it uniformly in the range $\{0, 1, 2 \ldots f-1\}$, each of which represents a bit in a f-bit string. Initially all the bits of f-bit string are set to 0. For each element in the set T, hashing is done with all the hash functions and their corresponding values are set to 1 in the f-bit string. This process is repeated for all the elements in the set T. If there are x hash functions in total and s items in the set, then finally xs bits are set in the f-bit string.

Table 1 presents the notations used in this article.

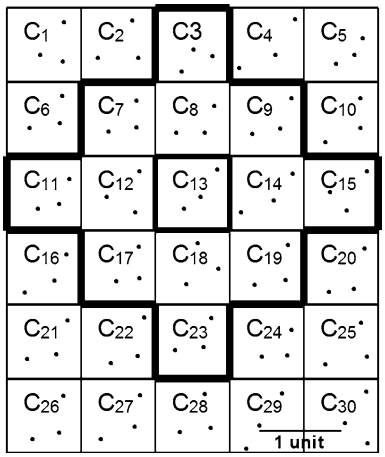

Fig. 1 Deployment of 30 cells and $\rho = 2$. Highlighted region shows cells which are within *Lee sphere* of C_{13}

3 Proposed scheme

We now present the key pre-distribution scheme followed by the shared key discovery in the network. For the proposed scheme, we presume sensor nodes are evenly distributed in the network and the whole network is further split into identical-sized cells. Total number of cells in the network are N.

3.1 Outline

In the presented scheme, all sensor nodes in a cell can directly communicate with each other. Further, sensor nodes of a particular cell can also communicate with sensor nodes in other cells which are within its communication range. For considering the communication range of sensor nodes we use *Lee Sphere* (Sect. 2.2), where sensor nodes of a particular cell only communicates with sensor nodes of another cell which are within it's Lee sphere region. At the time of deployment, a fixed number of sensor nodes (known as *cell identifiers*) in each cell are assigned ρ and (x_c, y_c), where ρ is the chosen lee distance and (x_c, y_c) is center of the cell where these sensor nodes are deployed. After the deployment, *cell identifiers* in particular cell C_i collaborate with other *cell identifiers* in neighboring cells to identify cells which are within its *Lee Sphere* (refer Fig. 1). We observe that only the center of each cell is used by *cell identifiers* for calculations of *Lee Sphere*. Thus, actual deployment location of *cell identifiers* in each cell do not affect the calculations of *Lee Sphere* until *cell identifiers* are deployed in correct cell. So, the proposed scheme is more tolerant to errors in the deployment knowledge when compared with grid based scheme like [5–9].

Communication in the whole network is secured by secret keys. For securing intra-cell communication, we use combinatorial design based keys. For securing inter-cell communication we use pair-wise keys. Both of these are discussed in Sects. 3.3 and 3.4 respectively. But prior to that we discuss reasons for choosing combinatorial design based keys over pair-wise keys for intra-cell communication.

3.2 Choosing combinatorial design based keys over pair-wise keys

In pair-wise keys, all the sensor nodes in communication range have unique pair-wise key. Precisely, this is same as random assignment of a secret key to each link between sensor nodes. This method of key assignment provides high resiliency, as compromising of a sensor node do-not effect remaining network. Downside of such design is huge key storage overhead, which can be troublesome for limited storage sensor nodes. If n sensor nodes want to communicate

Table 1 Notations

N	Total number of cells in network
n	Number of nodes in a particular cell
$k+1$	Number of keys assigned to each node
ρ	Lee distance
P_i	Set of keys assigned in a particular cell
C_i	(i)th cell in the network
K	Sensor nodes compromised in the network including cluster heads
K'	Heads compromised in the network
r_i	Heads compromised in cell C_i
K_i	Sensor nodes compromised in cell C_i
(x_c, y_c)	Center location of a particular cell
SP	Security parameter

with each other, $n(n-1)/2$ total secret keys are required where each sensor node stores $n-1$ keys. For example, if we have 7 sensor nodes we require total 21 unique pair-wise keys and each sensor node stores 6 keys.

On the other hand, *combinatorial design* based key assignment, assigns set of keys to each sensor node in such a way that any given pair of key-sets have some shared keys. Construction of such key-sets follows certain properties as discussed in Sect. 2.1. Consider $(v, k, \lambda) = (7, 3, 1)$ *Symmetric Design*, keys sets for such design will be: {1,2,4},{2,3,5}, {3,4,6}, {4,5,7}, {5,6,1}, {6,7,2}, {7,1,3}. Construction details for key-sets are given in Sect. 3.3. We can observe that any pair of key-set has one key in common and we use only 7 keys to create these key-sets. These key-sets can be assigned to 7 different sensor nodes to secure communication between them, where each sensor node is assigned only 3 keys. This design reduces key storage overhead in the network, where only 7 unique keys are required to ensure communication between 7 sensor nodes.

3.3 Key pre-distribution for intra-cell communication

In this section we discuss a new combinatorial design for intra-cell communication. For the proposed scheme, each cell has n sensor nodes which can directly communicate with each other. Each sensor node is allocated a set of keys chosen from a key pool also known as key-sets. Two sensor nodes share common secret keys in their key-sets to ensure secure communication. The *symmetric design* (Sect. 2.1) is adopted for creation of key-sets. For a symmetric design, each cell has k^2+k+1 sensor nodes and each sensor node is allocated $k+1$ keys, where k is prime. If in any case, the number of sensor nodes (n) is not of the form k^2+k+1 for any prime number k, then we opt for smallest prime number k which satisfies $n <= k^2+k+1$.

For the construction of Symmetric design of the form $(k^2+k+1, k+1, 1)$, we use *Difference method* (Sect. 2.1). The process starts with identification of multiplier of given difference set (D) for (v, k, λ) symmetric design in an *Abelian group* $(Z_v, +)$. This multiplier is used to find all the orbits of Z, where Z represents an Abelian group $(Z_v, +)$. These multiple orbits can be used to derive the desired difference set of fixed size $k+1$. Finally, the derived difference set is used to create all the key blocks or key-sets. These key blocks can be randomly assigned to all the sensor nodes in the cell. Blocks construction using difference set is much easier and simpler than given in schemes [5, 21]. The construction of the blocks using difference sets is given in Algorithm 1.

Algorithm 1: Blocks generation using symmetric design

Input: Symmetric design (v, k, λ) where $\lambda = 1$
Output: k^2+k+1 blocks of keys, each block has $k+1$ keys and any two blocks have one shared key

Find Multiplier (a) for difference set.
Compute all the orbits by mapping $x \longmapsto ax \bmod v$.
Find $difference\ set\ \{d_1, d_2, \ldots, d_{k+1}\}$ of $(k+1)$ length using the orbits.
for $j \leftarrow 1$ *to* (k^2+k+1) **do**
    $Block_j = \{d_1, d_2, \ldots, d_{k+1}\}$
    for $i \leftarrow 1$ *to* $(k+1)$ **do**
        $\{d_i = (d_i + 1) mod (k^2+k+1)\}$
    end for
end for

First three steps find the difference set for given $(k^2 + k + 1, k + 1, 1)$ symmetric design, which take $O(k^2) = O(n)$ time. Steps 4–9 generate the blocks, which take $O(k^3) = O(n^{1.5})$ time. The time complexity of the proposed technique is same as other symmetric based techniques such as given in [5, 21]. This process of key blocks creation and assignment of key blocks to all the sensor nodes is repeated for all the cells. If P_i denotes all the keys assigned in a particular cell and all the cells use different key pool, then $P_i \cap P_{i'} = \emptyset$ for all $i \neq i'$. Thus, nodes compromised in a particular cell have no effect on the remaining network.

Algorithm 2: Key assignment to heads in the cell

Input: Cell (C_i), Security Parameter (SP) and Lee Distance (ρ)
Output: SP associations each with all the cells within Lee Sphere (ρ) for cell C_i

```
1  Identification of neighboring cells within lee sphere region of cell (C_i) by cell identifiers nodes.
2  List of cells (m) within Lee sphere region of cell C_i .
3  for j ← 1 to m do
4      if C_i has not done association with cell C_j in previous steps then
5          for i ← 1 to SP do
6              Randomlly select node k_i ∈ C_i such that node k_i is not a head
7              Randomlly select node k_j ∈ C_j such that node k_j is not a head
8              Assign key to k_i and k_j
9          end for
10 end for
```

3.4 Key pre-distribution for inter-cell communication

For inter-cell communication in the proposed scheme we use pair-wise keys. Each cell maintain multiple associations with all the other cells which are within its communication range. The associations can be used by any sensor node to communicate with sensor node in other cells. These associations are secured with pair-wise keys. Sensor nodes for creating these associations are randomly selected from all the sensor nodes in the cell and are called heads. Moreover, a sensor node can be associated with a maximum of one sensor node present in another cells. The number of associations between any two cells is fixed and can be termed as security parameter for the scheme. *Cell identifiers* collaborate with each other to identify cells which are within lee sphere region. Further in a particular cell, *cell identifiers* and sensor nodes collaborate together to create the associations with all the cells within lee sphere region.

A sensor node n_i is the head for a cell C_i, if it has a key with some sensor node n_j present in cell C_j where cell C_i and C_j are within communicate range. *Cell identifiers* of both cells C_i and C_j collaborate together to identify whether C_i and C_j are within lee distance or not. If the total number of sensor nodes present in a cell are n and ρ represents given Lee distance, then the maximum value of SP for the network can be given by $n >= SP(2\rho(\rho + 1))$. The total heads chosen in a particular cell will be $SP(2\rho(\rho + 1))$ and each head will be storing just one extra key than other non-head sensor nodes in a particular cell. All the keys used in the whole network are unique. Construction algorithm for the same is given in Algorithm 2 which takes $O(m)$ time, where m is the total number of cells in communication range.

We maintain multiple associations within any two cells in communication range, where at the time of communication any one association is selected randomly. Thus, job of communication between any two cells is equally divided between all the associations. This ensures that no particular association has to overwork, culminating in almost equal utilization of battery power in heads.

3.5 Shared key discovery in the network

Shared key discovery inside a particular cell for intra-cell communication takes place using Bloom filter [20]. For implementation of bloom filter, each sensor node is assigned fixed number of hash functions at the time of deployment. For bloom filter, key-set assigned to each sensor node represents the set T. Each sensor node uses its key-set with the hash functions to set particular bits in the f-bit string.

This f-bit string is then broadcasted by each sensor node in the cell. The broadcasted f-bit string is used by all the other sensor nodes to identify the common secret key. So, each sensor node can use hash functions and the key-set with broadcasted f-bit string to identify the common secret key. Procedure for shared key discovery is given in Algorithm 3. Shared key discovery using hash functions takes $O(k) = O(\sqrt{n})$ time. The only information needed for shared key discovery is broadcasted f-bit string from all

the sensor nodes in the cell. Thus, communication overhead for shared key discovery is $O(f)$ bits which is much less than schemes [22, 23], but is more than schemes [5, 6].

Key pre-distribution in schemes [5, 6] is based on transversal designs, where all the sensor nodes are indexed by (a, b, c) where $a, b, c \in GF(k)$. On the basis of these indexes, keys are assigned to all the sensor nodes. For shared key discovery, sensor node broadcasts their indexes in the cell which can be used with shared key discovery algorithm to identify the shared key. Any other sensor node can use the broadcasted index and its own index with shared key algorithm to identify shared key. As all the identifiers are broadcasted in the network, adversary can easily get all the broadcasted indexes. As the shared key discovery algorithm requires two indexes to identify the shared key between them, adversary can use any two received indexes to identify the shared key between those two indexes. But in the proposed scheme, we use bloom filter for shared key discovery. Thus, even after obtaining all the f-bit broadcasted strings adversary cannot identify the shared key between any two sensor nodes. So despite the fact that our proposed scheme has more overhead for shared key discovery, our scheme provides more secure shared key discovery between any two sensor nodes.

Algorithm 3: Identification of shared key using f-bit string

Input: Broadcasted f-bit string
Output: Shared key K_j, if any shared key exists
1 Each node have independent hash functions $(H_1, H_2, \ldots . H_s)$.
2 **for** $j \leftarrow 1$ *to* $(k+1)$ **do**
3 **for** $i \leftarrow 1$ *to* s **do**
4 $x_i = H_i(k_j)$
5 end for
  if $\forall x$: f-bit string$(x) == 1$ **then**
  Shared key is k_j
  else
  It is not the shared key
  end if
6 end for

In the proposed scheme, we create multiple association between all the cells within communication range. These associations are secured with pair-wise keys. Thus shared key discovery is not required for inter-cell communication.

4 Analysis

Now we inspect the security aspects of the presented scheme. We perform analysis of presented scheme in terms of well-known measures i.e. E(s) and V(s). These are the most widely used and standard measures for analyzing any key pre-distribution scheme. But prior to that, we will discuss false positive associated with bloom filter [20].

4.1 False positive for bloom filter

In some cases, over a given set of elements more than one hash functions can map to same bits in the given f-bit string. So in rare cases, an element t' such that $(t' \notin T)$ has all its hash values set in the f-bit string, this is termed as false positive of Bloom filter. Probability of any bit in the f-bit string to be 0, if all the hash functions maps uniform random values can be given by $P = (1 - (\frac{1}{f}))^{xs}$, where xs represents total bits set to 1 in f-bit string. Finally, the probability of false positive for the f-bit string can be given by Eq. 1.

$$P = \left\{1 - \left\{1 - \left(\frac{1}{f}\right)^{xs}\right\}\right\}^{s} \tag{1}$$

From Eq. 1, we observe that the false positive is very marginal and we can neglect it if we use sufficiently large f-bit string.

4.2 Estimation of E(s)

When s sensor nodes are compromised in the network, $E(s)$ can be defined as ratio of total links effected to the total number of links in the network. Mathematically, $E(s) = \frac{links\ effected}{total\ link}$, when s sensor nodes are compromised. Here the term "effected" implies that link cannot be used in further communication. Let the total number of sensor nodes compromised randomly are K, out of these K sensor nodes number of heads compromised are K'. We first study local resiliency $El(K)$ (fraction of intra-links effected when K sensor nodes are compromised), then we study global resiliency $Eg(K')$ (fractions of inter-links effected when K' heads are compromised) and finally we study $Eo(K)$ (fraction of links (intra-links and inter-links) effected when K sensor nodes are compromised in the network).

4.2.1 Estimation of local resiliency *El*(*K*)

The proposed key pre-distribution scheme makes sure that each sensor node shares a key with all the other sensor nodes in a particular cell. To ensure this, in each cell a particular key is allocated to exactly $k+1$ sensor nodes. So, if a key k is compromised, then total links effected are $k(k+1)/2$. We also know each sensor node has $k+1$ keys, so if a sensor node is compromised then total intra-links disrupted are $k(k+1)^2/2$. Finally if total number of sensor nodes compromised in the network are K, then total links effected are $K(k(k+1)^2/2)$. This represents the upper most limit of links which can be effected when K sensor nodes are compromised. As multiple compromised nodes from same cell will have same keys, total individual keys exposed will be less and thus less links will

Table 2 Theoretical and experimental values of $El(K)$ for the proposed scheme

n	N	k	K	$El(K)$ experimental	$El(K)$ theoretical
8	25	3	20	0.123	0.246
25	25	5	20	0.148	0.154
49	49	7	30	0.0827	0.0859
289	289	17	500	0.0963	0.1014
361	361	19	700	0.0966	0.1017
529	529	23	900	0.0712	0.0738
841	841	29	1100	0.0440	0.0450
961	961	31	1300	0.0426	0.0435
1369	1369	37	1500	0.0291	0.0295

be effected in the network. Local resiliency of the network can be given by Eq. 2,

$$El(K) = \frac{K\{k(k+1)^2/2\}}{N\binom{k^2+k+1}{2}} \tag{2}$$

where N represents total cells in the network and $\binom{k^2+k+1}{2}$ represents total links in a particular cell. This equation can be further simplified to obtain Eq. 3.

$$El(K) = \frac{K(k+1)}{N(k^2+k+1)} \tag{3}$$

Table 2 gives the theoretical and experimental results for the same. These results are obtained by choosing K randomly from the network over 100 iterations.

4.2.2 Estimation of global resiliency $Eg(K')$

In the proposed scheme, sensor node of a particular cell can also communicate with sensor nodes present in other cell which are within its communication range. The number of cells within communication range of a particular cell can be given by $2\rho(\rho+1)$, where ρ is *Lee distance*. The inter-cell communication has to be done through multiple associations maintained with all the cells in communication range. These associations are assigned pair-wise keys to provide end to end secure communication. All the pair-wise keys used in the whole network are unique, thus an association will be secure until one of its end point is compromised. Each cell has equal number of associations with all the cells in its communication range and is denoted by SP (security parameter). Thus, two cells can communicate securely until all these SP associations are effected by compromised nodes. If we assume total heads compromised in a particular cell are r, then r associations will be broken and in worst case total r / SP inter-links will be broken. Thus global resiliency for a cell can be given by $Eg(r) \leq \frac{r}{2\rho(\rho+1)}$. The global resiliency of the entire network can be given by $Eg(K') \leq \sum_{i=0}^{N} \frac{r_i}{2\rho(\rho+1)SP}$. This can further be simplified to get $Eg(K') \leq \frac{\sum_{i=0}^{N} r_i}{2N\rho(\rho+1)SP}$. Now, if total number of nodes compromised in a cell C_i are K_i and total sensor nodes in each cell are n, then probability (P_{k_i}) that r_i heads are compromised in cell C_i when K_i nodes are captured is given by Eq. 4.

$$P_{k_i} = \frac{\binom{2\rho(\rho+1)SP}{r_i}\binom{n-(2\rho(\rho+1)SP)}{K_i-r_i}}{\binom{n}{K_i}} \tag{4}$$

Accordingly, the expected number of heads compromised in cell C_i, when K_i nodes are compromised can be calculated by Eq. 5, where $EXP()$ represents expectation operator.

$$EXP(r_i) = \sum_{i=0}^{2\rho(\rho+1)SP} r_i \frac{\binom{2\rho(\rho+1)SP}{r_i}\binom{n-(2\rho(\rho+1)SP)}{K_i-r_i}}{\binom{n}{K_i}} \tag{5}$$

Equation 5 can further be modified to get Eq. 6.

$$EXP(r_i) = \sum_{i=1}^{2\rho(\rho+1)SP} 2\rho(\rho+1))SP \frac{\binom{2\rho(\rho+1)SP-1}{r_i-1}\binom{n-(2\rho(\rho+1)SP)}{K_i-r_i}}{\binom{n}{K_i}} \tag{6}$$

Finally we can derive Eq. 7

$$EXP(r_i) = 2\rho(\rho+1))SP \sum_{i=1}^{2\rho(\rho+1)SP} \frac{\binom{2\rho(\rho+1)SP-1}{r_i-1}\binom{n-(2\rho(\rho+1)SP)}{K_i-r_i}}{\binom{n}{K_i}} \tag{7}$$

The value of $EXP(r_i)$ from Eq. 7 can be assigned to the global resiliency to get Eq. 8.

$$Eg(EXP(K')) \leq \frac{1}{N}\sum_{C_i=0}^{N}\sum_{r_i=1}^{2\rho(\rho+1)SP} \frac{\binom{2\rho(\rho+1)SP-1}{r_i-1}\binom{n-(2\rho(\rho+1)SP)}{K_i-r_i}}{\binom{n}{K_i}} \tag{8}$$

The experimental results for $Eg(K')$ are given in Table 3. These results are obtained by choosing K' randomly from the network over 100 iterations. We can clearly observe that because of the use of pair-wise keys for inter-cell communication our scheme shows very high resiliency against compromised heads. Further the proposed scheme is equally efficient for sparse and dense networks.

Table 3 Experimental values of $Eg(K')$ for the proposed scheme

n	N	ρ	k	SP	K'	$Eg(K')$ experimental
8	25	1	2	3	20	0.050
25	25	1	5	5	150	0.075
49	49	1	7	5	300	0.0714
289	289	4	17	5	10,000	0.0281
361	361	5	19	5	20,000	0.0057
529	529	5	23	5	40,000	0.0146
841	841	6	29	5	60,000	0.0026
961	961	7	31	5	80,000	0.0016

Figure 2 provides performance of the proposed scheme with certain values of parameters. In the figure we can observe that resiliency of the proposed scheme increases if we increase the security parameter (SP).

4.2.3 Estimation of overall resiliency *Eo*(*K*)

Now we will study overall resiliency of the presented scheme. Firstly we discuss all the cases which account to effected links in the network when some sensor nodes are compromised in the network. The cases are as follows:

1. Intra-links disrupted because of compromised nodes in a cell (local resiliency).
2. Inter-links disrupted because of compromised heads in a cell (global resiliency).
3. Inter-links disrupted because of compromised keys in the key-set of any head.
4. Inter-links disrupted because of compromised keys in the key-set of head present in other cell with whom particular cell maintains association.

The first and second cases are the scenarios we discussed in local and global resiliency respectively. Third and fourth cases make the study of overall resiliency very important. Each head has two types of keys, one key-set for ensuring secure communication within its cell and other is single key used to secure the association. In global resiliency we studied effect of any head compromise, but we did not study what happens if some keys from the key-set of a particular head are compromised. So, in both third and fourth cases if some of the keys from the key-set are compromised in any pair of heads which maintain an association, then that association cannot secure inter-cell communication between all the sensor nodes in two cells. Thus effecting overall resiliency of the network.

Theoretical bound for $Eo(K)$ is very difficult to estimate because it depends on multiple parameters including position and type of sensor nodes being compromised. Moreover, all the cases (1–4) which effect the links (inter-links and intra-links) in the network are inter-dependent. Thus, effect of any particular case cannot be quantified. Finally the effect of third and forth cases cannot be predicted, because we cannot predict how many keys from the key-set of a particular head will be compromised at any point of time. We give experimental results for overall resiliency of the network in Table 4. These results are obtained by choosing K randomly from the network over 100 iterations. Figure 3 provides the results of $Eo(K)$ for different network sizes.

4.3 Estimation of V(s)

When a sensor node is compromised by an adversary, keys stored in the sensor nodes are revealed. In some cases all the keys allocated to a non-compromised node can be also

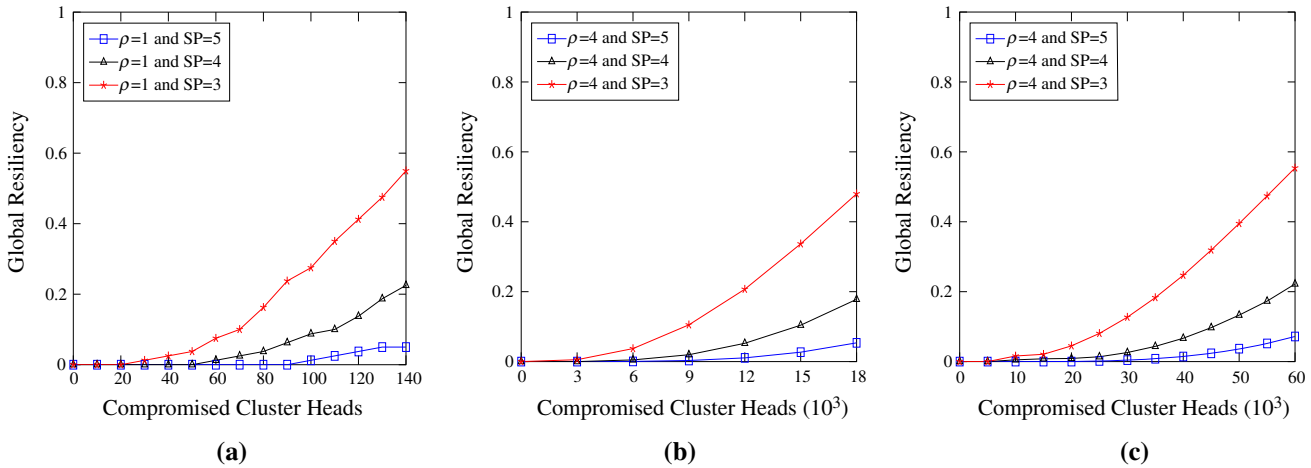

Fig. 2 Global resiliency of the proposed scheme when K' cluster heads are compromised. **a** $N = 25$ and $n = 25$, **b** $N = 289$ and $n = 289$, **c** $N = 529$ and $n = 529$

Table 4 Experimental values of $Eo(K)$ for the proposed scheme

n	N	ρ	k	SP	K	$Eo(K)$ experimental
8	25	1	2	3	10	0.0611
25	25	1	5	5	100	0.170
49	49	1	7	5	200	0.0651
289	289	4	17	5	3000	0.0467
361	361	4	19	5	4000	0.0326
529	529	5	23	5	5000	0.0120
841	841	6	29	5	8000	0.0049
961	961	7	31	5	10,000	0.0054

revealed, this happens when multiple sensor nodes sharing keys with this non-compromised node are compromised. Now, this node cannot communicate with other nodes in the network, thus it is disconnected from the network. When s sensor nodes are compromised, $V(s)$ can be defined as ratio of total nodes disconnected to the total number of nodes in the network. Mathematically, $V(s) = \frac{nodes\ disconnected}{total\ nodes}$, when s sensor nodes are compromised. This parameter was formulated by Ruj and Roy [5]. We are using the same parameter to analyze our scheme. We first study nodes disconnected $Vl(K)$ (fraction of nodes disconnected when K sensor nodes are compromised), then we study cells disconnected $Vg(K')$ (fractions of cells disconnected when K' heads are compromised) and finally we study $Vo(K)$ (fraction of total disconnections (nodes and cells) when K sensor nodes are compromised).

4.3.1 Estimation of nodes disconnected $Vl(K)$

The proposed key pre-distribution scheme makes sure that each node shares a key with all the sensor nodes in a particular cell. To ensure this, in each cell a particular key is allocated to exactly $k+1$ sensor nodes and each sensor node is allocated $k+1$ keys. So, to disconnect a sensor node from the network all its $k+1$ keys should be compromised. To fulfill such demand, minimum $k+1$ sensor nodes sharing those keys should be compromised in the same cell. If an adversary compromises K sensor nodes in the network, then on an average K/N sensor nodes are compromised in the same cell. So to disconnect a sensor node, K should fulfill $K/N > k+1$, or more precisely $K > N(k+1)$. As our scheme is also based on combinatorial design similar to schemes like [5, 6], results are similar to these schemes.

4.3.2 Estimation of cells disconnected $Vg(K')$

In the proposed scheme, inter-cell communication takes place through multiple associations maintained with all the cells in communication range. To disconnect a cell from the network all its associations should be broken. If the number of compromised heads in each cell are same and in each cell r_i heads are compromised, then not compromised heads in a particular cell C_i will be $(2\rho(\rho+1)SP - r_i)$. To disconnect cell C_i from the network, these non-compromised associations should be effected from neighboring cells. If the number of non-effected associations between neighboring cell C_j and C_i are N_j, then probability $(P_{r_j}^{N_j})$ that these N_j heads will be effected because of r_j heads compromised in cell C_j is given by Eq. 9.

$$P_{r_j}^{N_j} = \frac{\binom{N_j}{N_j}\binom{2\rho(\rho+1)SP - N_j}{r_j - N_j}}{\binom{2\rho(\rho+1)SP}{r_j}} \tag{9}$$

This can further be simplified to get Eq. 10.

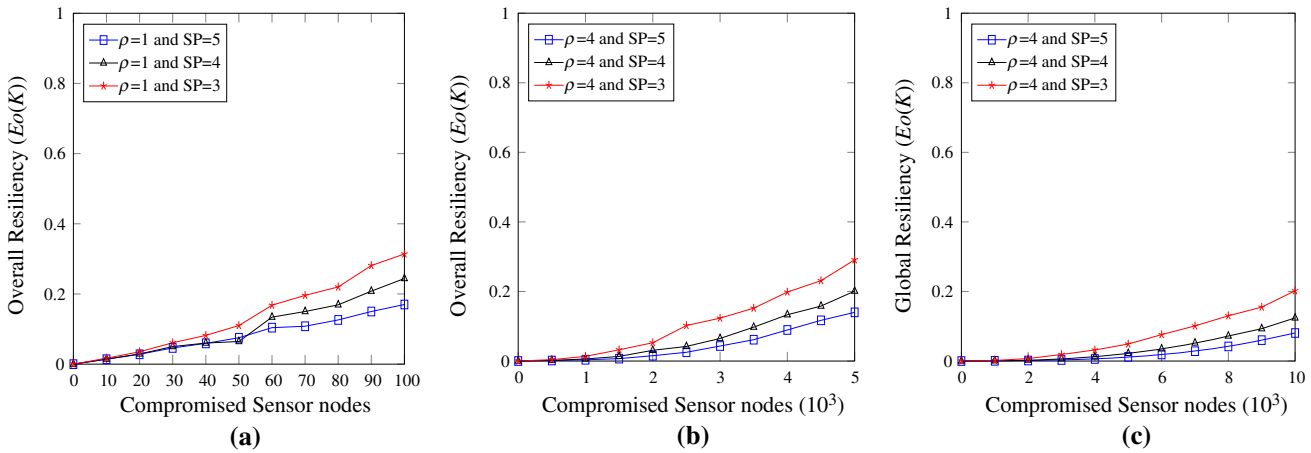

Fig. 3 Overall resiliency ($Eo(K)$) of the proposed scheme when K sensor nodes are compromised. **a** $N = 25$ and $n = 25$, **b** $N = 289$ and $n = 289$, **c** $N = 529$ and $n = 529$

$$P_{r_j}^{N_j} = \frac{\binom{2\rho(\rho+1)SP - N_j}{r_j - N_j}}{\binom{2\rho(\rho+1)SP}{r_j}} \tag{10}$$

Further probability to effect all the non-compromised heads of cell C_i from all the neighboring cells can be given by Eq. 11.

$$P(r_i) = \prod_{i=1}^{2\rho(\rho+1))} \frac{\binom{2\rho(\rho+1)SP - N_i}{r_i - N_i}}{\binom{2\rho(\rho+1)SP}{r_i}} \tag{11}$$

This is the probability of cell C_i to be disconnected from the network when r_i heads were compromised in C_i and all neighboring cells of C_i. Finally $Vg(K') = EXP(P(r_i))$, where EXP() represents expectation operator. The performance of proposed scheme in terms of $Vg(K')$ with different parameter values is laid out in Table 5. These results are obtained by choosing K' randomly in the network over 100 iterations. We observe that the proposed scheme has very low cells disconnection rate and it is practically impossible to disconnect a cell from the remaining network.

4.3.3 Estimation of overall disconnections *Vo*(*K*)

Finally we study overall disconnections in the network when a fixed number of sensor nodes are compromised in the network. For the study we take into account all the sensor nodes and cells in the network. In overall resiliency (Sect. 4.2.3), we noticed many new cases which effects inter-links between the cells. Those cases apply also in study of nodes and cells disconnected in the network. We take all the cases into consideration, where cells can be compromised because of compromised associations from neighboring cells and because of all keys compromised in the key-set of a particular head.

Similar to Overall resiliency $Eo(K)$, the theoretical bound for $Vo(K)$ is very difficult to estimate because it depends on multiple parameters including position and type of sensor nodes being compromised. We provide the experimental results for overall disconnections including nodes disconnected and cells disconnected when K sensor nodes are compromised in the network. The number of sensor nodes disconnected in the network are always same as local sensor nodes disconnected $Vl(K)$. The effect of case (3 and 4) from $Eo(K)$ is only on cells disconnected in the network. Thus for calculating experimental results for $Vo(K)$ we only consider total cells disconnected in the network. Table 6 provides the experimental results for the same. These results are obtained by choosing K randomly from the network over 100 iterations. We can observe from the table that only 4 cells on average are disconnected from the network $(N = 361, n = 361, \rho = 4, SP = 4)$ when around 45,000 sensor nodes are compromised in the network. Moreover the fraction of cells disconnected also decreases with the increase in SP.

Table 5 Experimental values of cells disconnected $Vg(K')$ for the proposed scheme

n	N	ρ	SP	k	K'	$Vg(K')$
8	25	1	2	3	75	0.12
25	25	1	4	5	200	0.16
25	25	1	5	5	200	0.04
49	49	1	4	7	400	0.122
49	49	1	5	7	400	0.0204
289	289	4	4	17	35,000	0.0588
289	289	4	5	17	35,000	0.0034
529	529	5	4	23	105,000	0.0207
529	529	5	5	23	105,000	0.0094
841	841	6	4	29	140,000	0
961	961	7	4	31	175,000	0

4.4 Minimum supported density of sensor nodes

In the proposed scheme, for inter-cell communication multiple associations are maintained between cells within communication range. To identify the cells in communication range we use *lee-sphere* (ρ), where minimum value of ρ is 1. Thus when $\rho = 1$, a particular cell can communicate with at-most 4 other neighboring cells. Further, for the proposed scheme number of associations between any two cells is given by *Security Parameter* (*SP*). Minimum *SP* value in the proposed scheme for any network size is 2, to ensure compromising of single head node do-not disconnect two cells. To fulfill above conditions number of sensor nodes in a particular cell should be at-least 8. In such network where $n = 8, \rho = 1, SP = 2$, a particular sensor node can communicate with 7 other sensor nodes in the same cell and 32 sensor nodes in neighboring cells. This is the minimum density of sensor nodes in the network where the proposed scheme can be implemented.

4.5 Energy requirements for the proposed scheme

In the proposed scheme, if a sensor node in a particular cell wants to communicate with sensor node in other cell, it sends the encrypted message to the chosen association. After receiving the packet, association decrypts the packet using key shared with the source node, encrypt it again

with secret key shared with associated node in other cell and forwards it. When association in target cell receives the packet, it decrypts the message, again encrypts with secret key of the target sensor node and sends it to the target node. Target sensor node decrypts the message upon receiving it. So, ideally (no packets are dropped in the network) total energy required in successfully sending and receiving messages in between any two cells can be given by,

$$E_{proposed} \leq (SP.E_{pair\ wise}) + P\{3(E^p_{encr} + E^p_{decr}) + 3(E^p_{send} + E^p_{receive})\} \quad (12)$$

where $E_{pairwise}$ is the energy required to assign pair-wise key to nodes of the association, E^p_{encr} and E^p_{decr} are the energy required for encryption and decryption of message of length p bytes, E^p_{send} and $E^p_{receive}$ are the energy required for sending and receiving p bytes of message and P are the total number of messages sent in the network.

On the other hand, if we do not use the proposed scheme and if a sensor node in a particular cell want to send data to sensor node in other cell following steps are taken. Firstly pair-wise key is established between source and destination nodes. Than source can send the encrypted message to the target. Target sensor node can decrypt the message upon receiving it. So, total energy required in successfully sending and receiving messages in between any two cells where proposed scheme is not used can be given by,

$$E_{without} = \sum_{i=1}^{P} \begin{cases} E_{total} & \text{If pair-wise key exist between source and destination} \\ E_{pair\ wise} + E_{total} & \text{otherwise} \end{cases}$$

where $E_{total} = (E^p_{encr} + E^p_{decr}) + (E^p_{send} + E^p_{receive})$.

Consider an example $N = 2, SP = 5, n = 25, p = 64$ bytes and $P = 50$. For the sensor nodes we use MICAz [24] sensor nodes, which has $E^p_{send} = 1.04$ mJ and $E^p_{receive} = 1.2$ mJ. For encryption we use AES-128 where MICAz sensor node consumes $E^p_{encr} = 0.078$ mJ and $E^p_{decr} = 0.19$ mJ [25]. For pair-wise key assignment in the network, we use SOK [26] which has $E_{pairwise} = 69.26$ mJ for MICAz sensor nodes. For the calculations of $E_{without}$ the probability for source and destination having pair-wise key because of previous communications is .2. Finally, after calculations energy requirements in both the cases are $E_{proposed} = 722.5$ mJ and $E_{without} = 2895.8$ mJ. So we can observe that the proposed scheme has very less energy requirements when compared with network implemented without proposed scheme. This is mainly because of the use of fixed associations between two cells for inter-cell communication in place of establishing individual pair-wise keys between source and destination.

Table 6 Experimental values of fraction of cells disconnected $Vo(K)$ for the proposed scheme

n	N	ρ	SP	k	K	$Vo(K)$
8	25	1	2	3	75	0.08
25	25	1	4	5	200	0.08
25	25	1	5	5	200	0.04
49	49	1	4	7	800	0.102
49	49	1	5	7	800	0.0408
289	289	4	4	17	15,000	0.0138
289	289	4	5	17	15,000	0
529	529	5	4	23	45,000	0.0094
529	529	5	5	23	45,000	0.0018
841	841	6	4	29	100,000	0.0011
841	841	6	5	29	100,000	0
961	961	7	4	31	150,000	0.0343
961	961	7	5	31	150,000	0.0184

In the proposed scheme heads have to participate in each message transfer in the network, which leads to extra energy consumption in heads. So, extra energy consumed by each head can be given by,

$$E_{headoverhead} = E_{pair\ wise} + (P/SP).E_{total} \quad (13)$$

where $(P\ /\ SP)$ are total messages forwarded by a particular head. But from the above example it is evident that irrespective of heads energy overhead the proposed scheme is highly energy efficient.

5 Comparison with existing schemes

In this section we present a comparative analysis of the presented scheme with existing schemes in terms of communication overhead, storage overhead and resiliency. Table 7 gives detailed analysis for the same. Table 8 provides the key storage overhead of all the existing scheme and the proposed scheme. Figure 4 provides the

Table 7 Comparison of existing schemes with the proposed scheme

Schemes	Types of keys	Deployment type	Network type	Storage overhead	Resiliency
Lie and Ning [3, 4] (LN)	Pair-wise	Cell based	Homogeneous	Very high	Very high
Huang et al. [15] (HMMH)	Key pool	Grid-cell	Homogeneous	Very high	Very low
Simonova et al. [9] (SLW)	Combinatorial design	Grid-cell	Homogeneous/heterogeneous	High	Very low
Ruj and Roy [5] (RR)	Combinatorial design	Grid-Cell	Heterogeneous	Low	Moderate
Bag [6] (SB)	Combinatorial design	Grid-cell	Heterogeneous	Low	Moderate
Bag and Roy [7] (BR)	Combinatorial design	Grid-cell	Heterogeneous	Low	Very high
Mitra et al. [8] (MMD)	Combinatorial design	Grid	Homogeneous	Very low	Very low
Proposed scheme	Hybrid	Cell	Homogeneous	Very low	Very high

Table 8 Key Storage Overhead in different schemes

Schemes	Keys in each sensor node	Keys in each head	Connectivity
Lie and Ning [3, 4] (LN)	121	126	0.92
Huang et al. [15] (HMMH)	68	68	0.52
Simonova et al. [9] (SLW)	20	40	0.80
Ruj and Roy [5] (RR)	12	24	1
Bag [6] (SB)	12	21	1
Bag and Roy [7] (BR)	12	24	1
Mitra et al. [8] (MMD)	15	15	1
Proposed	12	13	1

(1) Parameters for LN scheme are $\gamma = 121$ and $\mu = 5$, (2) parameters for HMMH scheme are $\tau = 2, \omega = 7$, and $n_z = 100$, parameters for SLW scheme are $p = 11, k = 16$ and $m = 4$, (4) parameters for RR scheme are $p = 11$ and $k = 12$, (5) parameters for SB scheme are $p = 11$ and $q = 11$, (6) parameters for MMD scheme are $r = 121$ and $p = 11$, (7) parameters for the proposed scheme are $\rho = 3, SP = 4$. The total number of sensor nodes for LN, MMD is 14,641, for HMMH is 10,000, for RR, BR, proposed scheme is 16,093, for SLW is 12,100 and for SB is 16,055

comparison of resiliency for existing schemes with the proposed scheme.

Liu and Ning [3, 4] introduced a key pre-distribution scheme for group based deployment in a homogeneous network. The scheme used pair-wise keys in each group, thus storage overhead was very high. If each cell has n sensor nodes, then number of keys allocated to each sensor node is $O(n^2)$. But in the presented scheme we used combinatorial design for key assignment inside the cells for intra-cell communication, thus maximum number of keys allocated to any sensor node in presented scheme is $O(\sqrt{n})$.

Huang et al. [15] adopted multiple space blom's scheme to propose a new key pre-distribution scheme for homogeneous network. In their scheme, sensor nodes in a particular cell can do intra-cell communication with probability > 0.5. Our scheme ensures that each sensor node can communicate with all the sensor nodes in the same cell with a probability of 1. Thus our scheme reduces the overhead and delay for communication within cells.

Based on transversal design [17], Simonova et al. [9] proposed a new key pre-distribution scheme for heterogeneous network. There are two types of sensor nodes in the network namely, weak nodes and strong nodes. Weak nodes in the same cell can communicate directly with each other and strong nodes are used for inter-cell communication. In the scheme [9], the number of strong nodes are dependent on size of the network. But in the proposed scheme number of heads can be fixed in advance and only depends on security parameter (SP) and Lee sphere region (ρ). Moreover, resiliency of the proposed scheme is much higher than scheme [9].

Ruj and Roy [5] proposed a new key pre-distribution scheme for heterogeneous network based on Campte and Yener's scheme [21]. In the scheme, there are two types of sensor nodes namely, sensor nodes and agents. Any two cells in the network communicate using agents, where multiple agents share either one, two or three keys. Thus if any agent is compromised, many inter-links are affected in the network. But in the proposed scheme, we adopt pair-wise keys for inter-cell communication, thus compromising of any head in the network has no effect on other links. So,

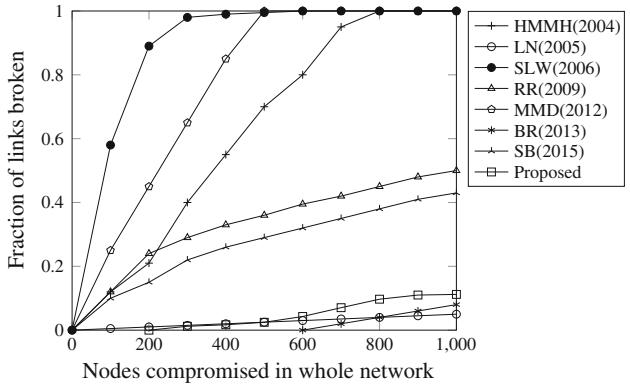

Fig. 4 Comparison of Simonova et al. [9] (SLW), Huang et al. [15] (HMMH), Lie and Ning [3] (LN), [4], Ruj and Roy [5] (RR), Bag [6] (SB), Bag and Roy [7] (BR), Mitra et al. [8] (MMD) and the Proposed scheme. (1) Parameters for SLW scheme are $p = 11, k = 16$ and $m = 4$, (2) parameters for HMMH scheme are $k = 200, \tau = 3$ and $\omega = 27$, (3) parameters for LN scheme are $L = 1, m = 60$ and $k = 200$, (4) parameters for RR scheme are $k = 12$, (5) parameters for SB scheme are $q = 13$, (6) parameters for BR scheme are $p = 11$ and $c = 4$, (7) parameters for MMD scheme are $p = 15$, (8) parameters for the proposed scheme are $\rho = 3, SP = 4$. The total number of sensor nodes for SLW is 12,100, for HMMH, DDHV, LN is 10,000, for MMD is 10,032, for RR, BR, proposed scheme is 16,093, for SB is 16,055

the proposed scheme has very high resiliency when compared with scheme [5].

Bag [6] proposed a key pre-distribution scheme much similar to Ruj and Roy's scheme [5]. In the scheme, each cell had variable number of agents depending on sensor node density and network size. Thus their scheme has huge number of agents for inter-cell communication and as keys stored in each agent are assigned using combinatorial design, the number of keys stored in agent is very high. Our proposed scheme has fixed number of heads in each cell based on chosen security parameter (SP) and Lee sphere region (ρ). Moreover, we used pair-wise keys to create associations for inter-cell communication, where each head is only associated with one head from other cell. Thus keys assigned to heads for inter-cell communication is only 1 which is much lower than scheme [6].

Mitra et al. [8] proposed a new combinatorial design based key pre-distribution scheme. Authors used projective planes and pair-wise connectivity to assign keys to each sensor nodes, thus key storage overhead is much lower. But the network used in the scheme is not divided into cells, thus resiliency of the scheme is very poor. Our scheme has very high resiliency against compromised nodes with minimal key storage overhead.

Bag and Roy [7] proposed another combinatorial design based key pre-distribution scheme for heterogeneous networks. The scheme has only one super node in each cell which is responsible for inter-cell communication. So if any super node gets compromised, a particular cell will be disconnected from the network. But in the proposed scheme, we maintain multiple associations with each neighboring cell, thus compromising of even multiple heads has minimal effect on the whole network. Moreover the scheme [7] presumes that super nodes can only be compromised when all other sensor nodes have been compromised in a particular cell. But for actual WSNs this assumption is superficial. In our scheme, we take equal probability for sensor nodes and heads being compromised by an adversary.

Table 8 provides the storage overhead of existing schemes and from the table we can observe that the proposed scheme has least storage overhead. But this reduction in storage overhead does not affect the resiliency of the whole system. Our proposed scheme performs much better than majority of combinatorial design based key pre-distribution schemes. Figure 4 gives the comparison of the resiliency of several schemes with the proposed scheme.

5.1 Scalability

Scalability in any network can be done in two ways, either by increasing the density of the sensor node in same network or by expanding the network in further geographical region. In the proposed scheme we use combinatorial design based keys for intra-cell communication, where before key pre-distribution we need to fix the value of k and according to k the key-sets are formed. So, the value of k should be decided keeping in mind for further increase in density of sensor nodes in each cell. This helps to keep unused key-sets in each cell for introduction of new sensor nodes in future. Thus, the proposed scheme provide good scalability in terms of density increase. For inter-cell communication we use pair-wise keys, where all the cells maintain fixed number of associations with all the other cells which are within communication range. So, if we introduce any new cell in the network, we only need to create these associations with other cells. As these associations are secured with pair-wise keys, associations can be created on-the-go if we wish to expand the network. For intra-cell communication in new cells we can use same key pre-distribution discussed in Sect. 3.3. Thus, scalability of the proposed scheme in terms of network expansion is very good. Compared with other combinatorial design based schemes such as [5–9] proposed scheme provides much easier scalability options.

6 Conclusion and future work

In this article, we proposed a novel hybrid key pre-distribution scheme based on combinatorial design and pair-wise keys. For the proposed scheme the whole deployment

region is divided into equal-sized cells and sensor node in the same cell can communicate with each other directly. To ensure secure direct communication within each cell, we assign combinatorial design based keys to all the sensor nodes. Moreover, sensors nodes can also communicate with sensor nodes in other cells which are within its communication range. For ensuring inter-cell communication, we maintain multiple associations between any two cells within communication range, thus sensor nodes of a particular cell can use any one of these associations to communicate with sensor nodes in other cells. For creating these associations, sensor nodes are chosen randomly from the cell and they are assigned pair-wise keys. As each node can become associated with maximum one sensor node in other cell, only one extra key is stored by each head. This helps in obtaining minimum key storage overhead than all the existing schemes. As all the pair-wise keys used in the network are unique, compromising of any association has no effect on remaining associations. Thus we observed that our scheme is highly resilient to compromised sensor nodes. We performed a detailed analysis of the proposed scheme and we observed that our scheme has high resiliency than majority of existing schemes.

In the proposed scheme we observed that head have more energy requirements than normal sensor nodes. This can lead to energy dis-balance in the network where at a given point of time some sensor nodes have more energy and some have very less energy. In future, we would like to figure out solutions to reduce energy consumption in heads.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, *40*(8), 102–114.
2. Kumar, A., & Pais, A. R. (2017). En-route filtering techniques in wireless sensor networks: A survey. *Wireless Personal Communications*, *96*(1), 697–739.
3. Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, *8*(1), 41–77.
4. Liu, D., & Ning, P. (2005). Improving key predistribution with deployment knowledge in static sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *1*(2), 204–239.
5. Ruj, S., & Roy, B. (2009). Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *6*(1), 4.
6. Bag, S. (2015). A new key predistribution scheme for grid-group deployment of wireless sensor networks. *Adhoc & Sensor Wireless Networks*, *27*, 313–329.
7. Bag, S., & Roy, B. (2013). A new key predistribution scheme for general and grid-group deployment of wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, *2013*(1), 145.
8. Mitra, S., Mukhopadhyay, S., & Dutta, R. (2012). A flexible deterministic approach to key pre-distribution in grid based wsns. In *International conference on ad hoc networks* (pp. 164–179). Berlin: Springer
9. Simonova, K., Ling, A. C., & Wang, X. S. (2006). Location-aware key predistribution scheme for wide area wireless sensor networks. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks* (pp. 157–168). ACM.
10. Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1992) Perfectly-secure key distribution for dynamic conferences. In *Annual international cryptology conference* (pp. 471–486). Berlin: Springer.
11. Blom, R. (1984). An optimal class of symmetric key generation systems. In *Workshop on the theory and application of of cryptographic techniques* (pp. 335–338). Berlin: Springer.
12. Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, *8*(2), 228–258.
13. Du, W., Deng, J., Han, Y. S., & Varshney, P. K. (2006). A key predistribution scheme for sensor networks using deployment knowledge. *IEEE Transactions on Dependable and Secure Computing*, *3*(1), 62–77.
14. Huang, D., & Medhi, D. (2007). Secure pairwise key establishment in large-scale sensor networks: An area partitioning and multigroup key predistribution approach. *ACM Transactions on Sensor Networks (TOSN)*, *3*(3), 16.
15. Huang, D., Mehta, M., Medhi, D., & Harn, L. (2004). Location-aware key management scheme for wireless sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 29–42). ACM.
16. Anderson, I. (1990). *Combinatorial designs: Construction methods*. Amsterdam: Ellis Horwood.
17. Stinson, D. R. (2007). *Combinatorial designs: Constructions and analysis*. Berlin: Springer.
18. Blackburn, S. R., Etzion, T., Martin, K. M., & Paterson, M. B. (2008). Efficient key predistribution for grid-based wireless sensor networks. In *International conference on information theoretic security* (pp. 54–69). Berlin: Springer.
19. Black, P. E. (2006). Manhattan distance. *Dictionary of Algorithms and Data Structures*, *18*, 2012.
20. Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, *13*(7), 422–426.
21. Çamtepe, S. A., & Yener, B. (2007). Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking*, *15*(2), 346–358.
22. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security* (pp. 41–47). ACM.
23. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *2003 Symposium on security and privacy, 2003 Proceedings* (pp. 197–213). IEEE.
24. Datasheet, M. (2006). *Crossbow technology inc* (p. 50). San Jose, CA.
25. Kim, J. M., Lee, H. S., Yi, J., & Park, M. (2016). Power adaptive data encryption for energy-efficient and secure communication in solar-powered wireless sensor networks. *Journal of Sensors*. https://doi.org/10.1155/2016/2678269.

26. Galindo, D., Roman, R., & Lopez, J. (2012). On the energy cost of authenticated key agreement in wireless sensor networks. *Wireless Communications and Mobile Computing*, *12*(1), 133–143.

Alok Kumar is Research Scholar in Department of Computer Science and Engineering, NITK Surathkal, India. He completed his B.Tech. (Computer Science and Engg.) from Maharishi Dayanand University, India and M.Tech. (Information Security) from Thapar University, India. His area of interest include Information Security, Network Security and Wireless Sensor Networks.

Alwyn Roshan Pais is Assistant Professor in Department of Computer Science and Engineering, NITK Surathkal, India. He completed his B.Tech. (CSE) from Mangalore University, India, M.Tech. (CSE) from IIT Bombay, India and Ph.D. from NITK, India. His area of interest include Information Security, Image Processing and Computer Vision.