A Group-Based Deterministic Key Predistribution Scheme for Wireless Sensor Network

No Institute Given

Abstract. We present a deterministic key pre-distribution scheme for wireless sensor network using combinatorial designs adapting a group and cluster based approach. Clusters are formed by taking a collection of nodes, and those clusters are further taken collectively to form groups. Three types of communications enable us to achieve connectivity of desired level. Our scheme provides better resilience (both in case of node and links) as compared to some other schemes, while keeping the number of secret keys to be stored at each node significantly less.

Keywords : Deterministic approach, projective planes, key pre-distribution.

1 Introduction

Wireless Sensor Network (WSN) is made up of a large number (hundreds to thousands) of wireless sensor nodes. Initially the evolution of WSN was motivated by the military applications, but now-a-days it plays an active role in industrial application areas, health care machines, traffic control etc. Sensor nodes are densely distributed in the intended region for monitoring physical and environmental conditions. They gather information and actively transmit the collected data to the desired location through the network by communicating among themselves. Messages or data are exchanged among the nodes through secret keys already stored at them. The geographical topology of the sensor nodes in the network remains unpredictable as they are plotted in very hostile regions (say, in border line of a country, deployed from air crafts to track enemy movements). Post-deployment key assignment to the nodes is therefore not a wise idea. The process of assigning keys to the nodes prior to their deployment in the target region is termed as *Key Pre-Distribution* (KPD). Usually, keys are chosen from a large key-pool and then they are loaded at the nodes. Combinatorial design is one of the mathematical tools used for key pre-distribution.

Previous Work:
Random key pre-distribution in Wireless Sensor Network was introduced by Eschenauer and Gligor [7]. Their scheme is known as *basic scheme*. Later Chan, Perrig and Song [5] proposed a modified version of the basic scheme, where it has been assumed that two nodes can communicate if they share q common keys. $q = 1$ refers to the basic scheme.

Camptepe and Yener [1] were first to introduce combinatorial designs as one of the key pre-distribution techniques. They adapted a deterministic approach using finite projective planes and generalized quadrangles. The deterministic approach is advantageous as any two nodes share a common key with certainty but looses the scalability. To sustain scalability, the authors proposed a hybrid (combination of both probabilistic and deterministic) scheme later to achieve better results.

In 2005, Lee and Stinson [8] proposed a key pre-distribution scheme on group-divisible design or Transversal design. It is observed that 60% of the nodes communicate through a single hop path and almost all rest of the 40% nodes are connected by double-hop path. One of the drawbacks is that the scheme provides poor resilience. Later, in 2008, quadratic schemes were developed in [10] based on Transversal designs and the method described in [8] was referred as linear schemes.

Chakrabarti et al. [3] proposed a probabilistic key pre-distribution scheme in 2005. The blocks of the combinatorial design were constructed as proposed by Lee et al. [8]. The sensor nodes are then formed by merging those blocks randomly. The chance of sharing common keys between two nodes is increased by merging. The scheme in [3] provides better resilience as compared to the Lee-Stinson scheme [8] at the cost of large key-chain size in each node.

3-design is considered to be the underlying combinatorial design of the key pre-distribution scheme proposed by Dong et al. in [6]. Keys are assigned to the sensor nodes in the network by Möbius planes. This scheme provides better connectivity than the scheme proposed by Lee-Stinson [10] and better memory requirement as compared to Camptepe-Yener scheme [1]. The prime drawback of the scheme is that resilience reduces rapidly with the increasing number of compromised nodes.

Ruj et al. [11] proposed a deterministic key pre-distribution scheme based on Partially Balanced Incomplete Block Design. The authors claim that this scheme gives better resilience than that of [8] storing less than $\sqrt{N}$ keys to the nodes where N is the network size. But to store that many keys to the nodes for a very large network is also expensive.

Our contribution
We propose a deterministic key pre-distribution scheme. The network is divided into a few groups, each group is a collection of a number of clusters, where clusters are composed of sensor nodes. The nodes are of two types depending on the type of keys they contain. The large key pool is divided into three disjoint parts. One part is used for the communication between the nodes from two clusters belonging to two different groups; second part is kept for the communication between the nodes from two clusters within a particular group. A particular combinatorial design is used to distribute the keys for these two types of communication. Before loading the keys to the nodes, the keys are pre-fixed or suffixed with their cluster and group indices respectively for Type II and Type I communication to avoid overlapping when it is not required. The remaining part of the key-pool is used for communication between the nodes, within a cluster; projective planes are used for key pre-distribution in each of the clusters. These three types of communication establish a trade-off between connectivity and resilience. Since the network is partitioned into groups and clusters, the memory requirement is very less for this case.

2 Preliminaries

2.1 Definitions

Some useful definitions from combinatorial designs are discussed in this section.

Definition 2.1 *A* set-system *is defined as a pair* (X, A) *such that*
(i) *X is a set of points or elements,*
(ii) *A is a subset of the power set of X (i.e. collection of non-empty subsets or blocks of X).*
The degree *(denoted by r) of $x \in X$ is the number of blocks of A containing x; the* rank *(denoted by k) is the size of the largest block in A.*
(X, A) is said to be regular *and* uniform *if all the points in X have the same degree and all the blocks in A have the same size respectively. A regular, uniform set-system with $|X| = v$, $|A| = b$ is known as a* (v, b, r, k)-design .

Definition 2.2 *A (v, b, r, k)-design in which any set of t points is contained in exactly λ blocks, is known as a* t - (v, b, r, k, λ)-design *which is often denoted as* t - (v, b, λ)-design.

Definition 2.3 *In* dual *design, the points and blocks are interchanged. The dual of a (v, b, r, k)-design is a (b, v, k, r)-design. A* symmetric design *is a self-dual design with $b = v$ and $k = r$.*

Definition 2.4 *A symmetric* 2 - $(n^2+n+1, n^2+n+1, n+1, n+1, 1)$*-design is known as a* finite symmetric projective plane of order n. *Precisely, it is a pair of a set of $\big(n^2+n+1\big)$ points and a set of $\big(n^2+n+1\big)$ lines, where each line contains $(n+1)$ points and each point occurs in $(n+1)$ lines.*

2.2 Discussions on Projective Plane

A projective plane of order n is defined as a pair of two sets: a set of n^2+n+1 points and a set of n^2+n+1 lines so that each line contains $n+1$ points, each point is contained in $n+1$ lines. Further, any two points is contained in one and only one line and any two lines intersect in exactly one point. When a set of nodes is assigned keys according to a projective plane, where the points correspond to the keys and the lines are associated with the key-chains of each node. As a result a network of size N can be designed with only $O(\sqrt{N})$ keys per node such that any two nodes in the network is directly connected. Existence of a projective plane of order p is certain when p is prime [14]. Smallest projective plane (of order 2) is a $(7, 3, 1)$-design. Projective plane of order 3, a $(13, 4, 1)$-design is a pair of sets (X, A), where $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$,
$A = \{(1, 2, 3, 4); (1, 5, 6, 7); (1, 8, 9, 10); (1, 11, 12, 13); (2, 5, 8, 11); (2, 6, 9, 13); (2, 7, 10, 12); (3, 5, 10, 13);$
$(3, 6, 8, 12); (3, 7, 9, 11); (4, 5, 9, 12); (4, 6, 10, 11); (4, 7, 8, 13)\}$.
We consider the key-pool to be X, and the nodes as the blocks of A. Now, initially to accommodate a network of size N, order of the projective plane p is chosen in such a way that $p^2 + p + 1 \geq N$. Even

if all the blocks of the parent set A are not present in the network, any two nodes in the network will be still directly connected. If we want to develop a network of size 10 and choose any 10 blocks say, $\{(1,2,3,4);(1,5,6,7);(1,8,9,10);(1,11,12,13);(2,5,8,11);(2,6,9,13);$ $(2,7,10,12);(3,5,10,13);(3,6,8,12);(3,7,9,11);(4,5,9,12)$, it won't affect the nature of the connectivity in the network. This is very beneficial, as there is a huge gap between the affordable sizes of the networks when p has to be increased to the next prime to introduce some new nodes in the network.

We shall make use of this property later in the scheme.

2.3 Notations

We use the following notation:

G_p	p^{th} group on the network, $p \in \{1, 2, \cdots, a\}$
$C_{p,q}$	q^{th} cluster in the p^{th} group in the network, $p \in \{1, 2, \cdots, a\}, \quad q \in \{1, 2, \cdots, b\}$
$N^A_{p,q,r}$	r^{th} Type A node in the cluster C_{pq}, where $1 \le p \le a,\ 1 \le q \le b,\ 1 \le r \le c_1$
$N^B_{p,q,r}$	r^{th} Type B node in the cluster C_{pq}, where $1 \le p \le a,\ 1 \le q \le b,\ 1 \le r \le c_2$
N	Total number of nodes in the network
K	Key-pool for Type I and Type II keys, where each key is of the form (x, y)
$(j \parallel x \parallel y)$	The Type I keys assigned to the Type A nodes, where j denotes the cluster-index
$(x \parallel y \parallel i)$	The Type II keys assigned to the Type B nodes, where i denotes the group-index

Henceforth we shall use $N_{p,q,r}$ or N_{pqr} and $C_{p,q}$ or C_{pq} interchangeably throughout the paper.

3 Proposed Scheme

We divide the whole network into a groups, each group is further distributed into b clusters, each of which is composed of c sensor nodes. The network consists of two types of nodes: Type A and Type B. Let there be c_1 Type A and c_2 Type B nodes ($c = c_1 + c_2$) within each cluster. Therefore, total number of nodes in the network is $ab(c_1 + c_2)$. Three types of communication are considered here:

- Type I : Communication of the nodes from two clusters belonging to two different groups i.e., communication between the clusters and between the groups. This is inter-cluster and inter-group communication.
- Type II: Communication of the nodes from two clusters within a group i.e., communication between the clusters within a group. This is inter-cluster intra-group communication.
- Type III: Communication between the nodes within a cluster. This is intra-cluster (which obviously follows intra-group also) communication.

The distributed keys are accordingly categorized into three types - Type X keys enabling Type X communication, where X = I, II, III. It is further assumed that each Type A node contains Type I and Type III keys and each Type B node contains Type II and Type III keys only.

3.1 KPD Between the Clusters of Different Groups :

To enable Type I communications, we adapt the following key pre-distribution mechanism. There are a groups in the network. Type I communication is a cluster-wise communication among the groups, i.e. at a time exactly one cluster from each group is chosen to take part in the communication. KPD is done in such a manner that two Type A nodes chosen from two clusters C_{p_1,q_1} and C_{p_2,q_2} may establish a Type I communication between them if $q_1 = q_2$ but $p_1 \neq p_2$. This implies that two Type A nodes within the same cluster do not share any common Type I key.

Let us suppose that we want to give k_1 Type I keys to each of the Type A nodes. To assign the keys to the node $N^A_{p,q,r}$, keys of the form $\{(x, (x^q + xp + r) \mod m_1) : 0 \le x \le k_1 - 1\}$ are chosen from the key-pool K. For each of the k_1 chosen pairs of the form (x, y), the actual key is taken as the concatenation of the components of the chosen pair with the cluster index q of the corresponding node. Therefore, the node $N^A_{p,q,r}$ gets Type I keys of the form $(q \parallel x \parallel y)$. Concatenation of the cluster index ensures that two nodes from different group will not communicate by Type I keys unless they have different cluster indices.

3.2 KPD Between the Clusters within a Group :

This enables Type II Communication which is an inter-cluster communication within same group. Two Type B nodes chosen from the clusters C_{p_1,q_1} and C_{p_2,q_2} may have a common Type II key if $p_1 = p_2$ but $q_1 \neq q_2$. Similar to the Type I communication, it is assumed that Type II communication between two Type B nodes is established if they belong to the different clusters of same group and two Type B nodes within the same cluster do not share any common Type II key. There are bc_2 Type B nodes within a particular group. Let us suppose that we want to give k_2 Type II keys to each of the Type B nodes. To assign the keys to the node $N^B_{p,q,r}$, keys of the form $\{(x, (x^p + xq + r) \mod m_2) : 0 \leq x \leq k_2 - 1\}$ are chosen from the key-pool K. For each of the k_2 chosen pairs of the form (x, y), the actual key is taken as the concatenation of the group index p with the components of the chosen pair (x, y). Therefore, the node $N^B_{p,q,r}$ gets Type II keys of the form $(x \parallel y \parallel p)$. Concatenation with the group index ensures that two nodes from the same group will not communicate by Type II keys unless they have different cluster indices.

3.3 KPD Within a Cluster :

To enable Type III Communication, let us assume that Type III keys are assigned to the nodes for communication between the nodes within a particular cluster. Type III keys are distributed to all the c nodes within a cluster according to a projective plane $(n^2 + n + 1, n + 1, 1)$ such that $n^2 + n + 1 \approx c_1 + c_2$. This ensures that all the nodes within a cluster are directly connected to each other.

We provide the algorithm below for assigning Type I and Type II keys to Type A and Type B nodes of the network.

Assignment of Type I and Type II keys to the node $N^S_{p,q,r}$

Input: *Number of groups a and Number of clusters in each group b; Number of Type A nodes c_1 and Number of Type B nodes c_2 in each cluster; Number of Type I keys k_1 and number of Type II keys k_2 to be stored at each node.*
Output: *Key chain of the node $N^S_{p,q,r}$ containing Type I and Type II keys.*
procedure Key Pre-Distribution

Algorithm 3.1

```
for $p := 1$ to $a$ do
  for $q := 1$ to $b$ do
    if $S := A$ do then
      set $m_1 := max(a, b, c_1)$;
      for $r := 1$ to $c_1$ do
        for $x := 1$ to $k_1$ do
          $y = (x^q + xp + r) \mod m_1$;
          Assign key to the node $N^S_{p,q,r}$
        end do
      end do
    else
      set $m_2 := max(a, b, c_2)$;
      for $r := 1$ to $c_2$ do
        for $x := 1$ to $k_2$ do
          $y = (x^p + xq + r) \mod m_2$;
          Assign key $(x \parallel y \parallel p)$ to the node $N^S_{p,q,r}$
        end do
      end do
    end if
  end do
end do
end Key Pre-Distribution
```

3.4 Illustration

Let N=240. We consider $a = 3,\ b = 5, c = 16 : c_1 = 7,\ c_2 = 9$. Here $m_1 = max(3, 5, 7) = 7$ and $m_2 = max(3, 5, 9) = 9$. Let $k_1 = 3$ and $k_2 = 3$. The key-chains of all the nodes are given below in detail. For convenience, Type I and Type II keys $(q \parallel x \parallel y)$ and $(x \parallel y \parallel p)$ are referred to as qxy and xyp in the following tables.
Type I communication

	$N^A_{1,1,1}$	$N^A_{1,1,2}$	$N^A_{1,1,3}$	$N^A_{1,1,4}$	$N^A_{1,1,5}$	$N^A_{1,1,6}$	$N^A_{1,1,7}$
$C_{1,1}$:	113	114	115	116	110	111	112
	125	126	120	121	122	123	124
	130	131	132	133	134	135	136

	$N^A_{2,1,1}$	$N^A_{2,1,2}$	$N^A_{2,1,3}$	$N^A_{2,1,4}$	$N^A_{2,1,5}$	$N^A_{2,1,6}$	$N^A_{2,1,7}$
$C_{2,1}$:	114	115	116	110	111	112	113
	120	121	122	123	124	125	126
	133	134	135	136	130	131	132

	$N^A_{3,1,1}$	$N^A_{3,1,2}$	$N^A_{3,1,3}$	$N^A_{3,1,4}$	$N^A_{3,1,5}$	$N^A_{3,1,6}$	$N^A_{3,1,7}$
$C_{3,1}$:	115	116	110	111	112	113	114
	122	123	124	125	126	120	121
	136	130	131	132	133	134	135

KPS to the 1^{st} Cluster of each Group.

	$N^A_{1,2,1}$	$N^A_{1,2,2}$	$N^A_{1,2,3}$	$N^A_{1,2,4}$	$N^A_{1,2,5}$	$N^A_{1,2,6}$	$N^A_{1,2,7}$
$C_{1,2}$:	213	214	215	216	210	211	212
	220	221	222	223	224	225	226
	236	230	231	232	233	234	235

	$N^A_{2,2,1}$	$N^A_{2,2,2}$	$N^A_{2,2,3}$	$N^A_{2,2,4}$	$N^A_{2,2,5}$	$N^A_{2,2,6}$	$N^A_{2,2,7}$
$C_{2,2}$:	214	215	216	210	211	212	213
	222	223	224	225	226	220	221
	232	233	234	235	236	230	231

	$N^A_{3,2,1}$	$N^A_{3,2,2}$	$N^A_{3,2,3}$	$N^A_{3,2,4}$	$N^A_{3,2,5}$	$N^A_{3,2,6}$	$N^A_{3,2,7}$
$C_{3,2}$:	215	216	210	211	212	213	214
	224	225	226	220	221	222	223
	235	236	230	231	232	233	234

KPS to the 2^{nd} Cluster of each Group.

	$N^A_{1,3,1}$	$N^A_{1,3,2}$	$N^A_{1,3,3}$	$N^A_{1,3,4}$	$N^A_{1,3,5}$	$N^A_{1,3,6}$	$N^A_{1,3,7}$
$C_{1,3}$:	313	314	315	316	310	311	312
	324	325	326	320	321	322	323
	333	334	335	336	330	331	332

	$N^A_{2,3,1}$	$N^A_{2,3,2}$	$N^A_{2,3,3}$	$N^A_{2,3,4}$	$N^A_{2,3,5}$	$N^A_{2,3,6}$	$N^A_{2,3,7}$
$C_{2,3}$:	314	315	316	310	311	312	313
	326	320	321	322	323	324	325
	336	330	331	332	333	334	335

	$N^A_{3,3,1}$	$N^A_{3,3,2}$	$N^A_{3,3,3}$	$N^A_{3,3,4}$	$N^A_{3,3,5}$	$N^A_{3,3,6}$	$N^A_{3,3,7}$
$C_{3,3}$:	315	316	310	311	312	313	314
	321	322	323	324	325	326	320
	332	333	334	335	336	330	331

KPS to the 3^{rd} Cluster of each Group.

	$N^A_{1,4,1}$	$N^A_{1,4,2}$	$N^A_{1,4,3}$	$N^A_{1,4,4}$	$N^A_{1,4,5}$	$N^A_{1,4,6}$	$N^A_{1,4,7}$
$C_{1,4}$:	413	414	415	416	410	412	413
	425	426	420	421	422	423	424
	431	432	433	434	435	436	430

	$N^A_{2,4,1}$	$N^A_{2,4,2}$	$N^A_{2,4,3}$	$N^A_{2,4,4}$	$N^A_{2,4,5}$	$N^A_{2,4,6}$	$N^A_{2,4,7}$
$C_{2,4}$:	414	415	416	410	411	412	413
	420	421	422	423	424	425	426
	434	435	436	430	431	432	433

	$N^A_{3,4,1}$	$N^A_{3,4,2}$	$N^A_{3,4,3}$	$N^A_{3,4,4}$	$N^A_{3,4,5}$	$N^A_{3,4,6}$	$N^A_{3,4,7}$
$C_{3,4}$:	415	416	410	411	412	413	414
	422	423	424	425	426	420	421
	430	431	432	433	434	435	436

KPS to the 4^{th} Cluster of each Group.

	$N^A_{1,5,1}$	$N^A_{1,5,2}$	$N^A_{1,5,3}$	$N^A_{1,5,4}$	$N^A_{1,5,5}$	$N^A_{1,5,6}$	$N^A_{1,5,7}$
$C_{1,5}$:	513	514	515	516	510	511	512
	520	521	522	523	524	525	526
	532	533	534	535	536	530	531

	$N^A_{2,5,1}$	$N^A_{2,5,2}$	$N^A_{2,5,3}$	$N^A_{2,5,4}$	$N^A_{2,5,5}$	$N^A_{2,5,6}$	$N^A_{2,5,7}$
$C_{2,5}$:	514	515	516	510	511	512	513
	524	525	526	520	521	522	523
	535	536	530	531	532	533	534

	$N^A_{3,5,1}$	$N^A_{3,5,2}$	$N^A_{3,5,3}$	$N^A_{3,5,4}$	$N^A_{3,5,5}$	$N^A_{3,5,6}$	$N^A_{3,5,7}$
$C_{3,5}$:	515	516	510	511	512	513	514
	524	525	526	520	521	522	523
	531	532	533	534	535	536	530

KPS to the 4^{th} Cluster of each Group.

Type II communication

	$N^B_{1,1,1}$	$N^B_{1,1,2}$	$N^B_{1,1,3}$	$N^B_{1,1,4}$	$N^B_{1,1,5}$	$N^B_{1,1,6}$	$N^B_{1,1,7}$	$N^B_{1,1,8}$	$N^B_{1,1,9}$
$C_{1,1}$:	131	141	151	161	171	181	101	111	121
	251	261	271	281	201	211	221	231	241
	371	381	301	311	321	331	341	351	361

	$N^B_{1,2,1}$	$N^B_{1,2,2}$	$N^B_{1,2,3}$	$N^B_{1,2,4}$	$N^B_{1,2,5}$	$N^B_{1,2,6}$	$N^B_{1,2,7}$	$N^B_{1,2,8}$	$N^B_{1,2,9}$
$C_{1,2}$:	141	151	161	171	181	101	111	121	131
	271	281	201	211	221	231	241	251	261
	311	321	331	341	351	361	371	381	301

	$N^B_{1,3,1}$	$N^B_{1,3,2}$	$N^B_{1,3,3}$	$N^B_{1,3,4}$	$N^B_{1,3,5}$	$N^B_{1,3,6}$	$N^B_{1,3,7}$	$N^B_{1,3,8}$	$N^B_{1,3,9}$
$C_{1,3}$:	151	161	171	181	101	111	121	131	141
	201	211	221	231	241	251	261	271	281
	341	351	361	371	381	301	311	321	331

	$N^B_{1,4,1}$	$N^B_{1,4,2}$	$N^B_{1,4,3}$	$N^B_{1,4,4}$	$N^B_{1,4,5}$	$N^B_{1,4,6}$	$N^B_{1,4,7}$	$N^B_{1,4,8}$	$N^B_{1,4,9}$
$C_{1,4}$:	161	171	181	101	111	121	131	141	151
	221	231	241	251	261	271	281	201	211
	371	381	301	311	321	331	341	351	361

	$N^B_{1,5,1}$	$N^B_{1,5,2}$	$N^B_{1,5,3}$	$N^B_{1,5,4}$	$N^B_{1,5,5}$	$N^B_{1,5,6}$	$N^B_{1,5,7}$	$N^B_{1,5,8}$	$N^B_{1,5,9}$
$C_{1,5}$:	171	181	101	111	121	131	141	151	161
	241	251	261	271	281	201	211	221	231
	311	321	331	341	351	361	371	381	301

KPS to the nodes of Group 1

	$N^B_{2,1,1}$	$N^B_{2,1,2}$	$N^B_{2,1,3}$	$N^B_{2,1,4}$	$N^B_{2,1,5}$	$N^B_{2,1,6}$	$N^B_{2,1,7}$	$N^B_{2,1,8}$	$N^B_{2,1,9}$
$C_{2,1}$:	132	142	152	162	172	182	102	112	122
	272	282	202	212	222	232	242	252	262
	342	352	362	372	382	302	312	322	332

	$N^B_{2,2,1}$	$N^B_{2,2,2}$	$N^B_{2,2,3}$	$N^B_{2,2,4}$	$N^B_{2,2,5}$	$N^B_{2,2,6}$	$N^B_{2,2,7}$	$N^B_{2,2,8}$	$N^B_{2,2,9}$
$C_{2,2}$:	142	152	162	172	182	102	112	122	132
	202	212	222	232	242	252	262	272	282
	372	382	303	312	322	332	342	352	362

	$N^B_{2,3,1}$	$N^B_{2,3,2}$	$N^B_{2,3,3}$	$N^B_{2,3,4}$	$N^B_{2,3,5}$	$N^B_{2,3,6}$	$N^B_{2,3,7}$	$N^B_{2,3,8}$	$N^B_{2,3,9}$
$C_{2,3}$:	152	162	172	182	102	112	122	132	142
	222	232	242	252	262	272	282	202	212
	312	322	332	342	352	362	372	382	302

	$N^B_{2,4,1}$	$N^B_{2,4,2}$	$N^B_{2,4,3}$	$N^B_{2,4,4}$	$N^B_{2,4,5}$	$N^B_{2,4,6}$	$N^B_{2,4,7}$	$N^B_{2,4,8}$	$N^B_{2,4,9}$
$C_{2,4}$:	162	172	182	102	112	122	132	142	152
	242	252	262	272	282	202	212	222	232
	342	352	362	372	382	302	312	322	332

	$N^B_{2,5,1}$	$N^B_{2,5,2}$	$N^B_{2,5,3}$	$N^B_{2,5,4}$	$N^B_{2,5,5}$	$N^B_{2,5,6}$	$N^B_{2,5,7}$	$N^B_{2,5,8}$	$N^B_{2,5,9}$
$C_{2,5}$:	172	182	102	112	122	132	142	152	162
	262	272	282	202	212	222	232	242	252
	372	382	302	312	322	332	342	352	362

KPS to the nodes of Group 2

	$N^B_{3,1,1}$	$N^B_{3,1,2}$	$N^B_{3,1,3}$	$N^B_{3,1,4}$	$N^B_{3,1,5}$	$N^B_{3,1,6}$	$N^B_{3,1,7}$	$N^B_{3,1,8}$	$N^B_{3,1,9}$
$C_{3,1}$:	133	143	153	163	173	183	103	113	123
	223	233	243	253	263	273	283	203	213
	343	353	363	373	383	303	313	323	333

	$N^B_{3,2,1}$	$N^B_{3,2,2}$	$N^B_{3,2,3}$	$N^B_{3,2,4}$	$N^B_{3,2,5}$	$N^B_{3,2,6}$	$N^B_{3,2,7}$	$N^B_{3,2,8}$	$N^B_{3,2,9}$
$C_{3,2}$:	143	153	163	173	183	103	113	123	133
	243	253	263	273	283	203	213	223	233
	373	383	303	313	323	333	343	353	363

	$N^B_{3,3,1}$	$N^B_{3,3,2}$	$N^B_{3,3,3}$	$N^B_{3,3,4}$	$N^B_{3,3,5}$	$N^B_{3,3,6}$	$N^B_{3,3,7}$	$N^B_{3,3,8}$	$N^B_{3,3,9}$
$C_{3,3}$:	153	163	173	183	103	113	123	133	143
	263	273	283	203	213	223	233	243	253
	313	323	333	343	353	363	373	383	303

	$N^B_{3,4,1}$	$N^B_{3,4,2}$	$N^B_{3,4,3}$	$N^B_{3,4,4}$	$N^B_{3,4,5}$	$N^B_{3,4,6}$	$N^B_{3,4,7}$	$N^B_{3,4,8}$	$N^B_{3,4,9}$
$C_{3,4}$:	163	173	183	103	113	123	133	143	153
	283	203	213	223	233	243	253	263	273
	343	353	363	373	383	303	313	323	333

	$N^B_{3,5,1}$	$N^B_{3,5,2}$	$N^B_{3,5,3}$	$N^B_{3,5,4}$	$N^B_{3,5,5}$	$N^B_{3,5,6}$	$N^B_{3,5,7}$	$N^B_{3,5,8}$	$N^B_{3,5,9}$
$C_{3,5}$:	173	183	103	113	123	133	143	153	163
	213	223	233	243	253	263	273	283	203
	373	383	303	313	323	343	353	363	373

KPS to the nodes of Group 3

The Type III key distribution the sixteen nodes of $C_{1,1}$ (according to projective plane) is given below. Type III keys are different from Type I and Type II keys, hence a large key-pool is chosen for Type III keys. For each cluster, a distinct sub-pool of Type III are chosen. In the following table we show the Type III keys to the nodes of $C_{1,1}$. The sub-pool is given by $\{k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18}, k_{19}, k_{20}, k_{21}, k_{22}, k_{23}, k_{24}, k_{25}, k_{26}, k_{27}, k_{28}, k_{29}, k_{30}, k_{31}\}$.

Node	Type III keys	Node	Type III keys
$N^A_{1,1,1}$	$k_1, k_2, k_3, k_4, k_5, k_6$	$N^B_{1,1,2}$	$k_2, k_9, k_{14}, k_{19}, k_{24}, k_{29}$
$N^A_{1,1,2}$	$k_1, k_7, k_8, k_9, k_{10}, k_{11}$	$N^B_{1,1,3}$	$k_2, k_{10}, k_{15}, k_{20}, k_{25}, k_{30}$
$N^A_{1,1,3}$	$k_1, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}$	$N^B_{1,1,4}$	$k_2, k_{11}, k_{16}, k_{21}, k_{26}, k_{31}$
$N^A_{1,1,4}$	$k_1, k_{17}, k_{18}, k_{19}, k_{20}, k_{21}$	$N^B_{1,1,5}$	$k_3, k_7, k_{16}, k_{20}, k_{24}, k_{28}$
$N^A_{1,1,5}$	$k_1, k_{22}, k_{23}, k_{24}, k_{25}, k_{26}$	$N^B_{1,1,6}$	$k_3, k_8, k_{12}, k_{21}, k_{25}, k_{29}$
$N^A_{1,1,6}$	$k_1, k_{27}, k_{28}, k_{29}, k_{30}, k_{31}$	$N^B_{1,1,7}$	$k_3, k_9, k_{13}, k_{17}, k_{26}, k_{30}$
$N^A_{1,1,7}$	$k_2, k_7, k_{12}, k_{17}, k_{22}, k_{27}$	$N^B_{1,1,8}$	$k_3, k_{10}, k_{14}, k_{18}, k_{22}, k_{31}$
$N^B_{1,1,1}$	$k_2, k_8, k_{13}, k_{18}, k_{23}, k_{28}$	$N^B_{1,1,9}$	$k_3, k_{11}, k_{15}, k_{19}, k_{23}, k_{27}$

Table 1. KPS of Type III keys to the nodes of C_{11}

Therefore, in this case, Node $N^A_{1,1,1}$ has three Type I keys $\{113, 125, 130\}$, six Type III keys $\{k_1, k_2, k_3, k_4, k_5, k_6\}$ and no Type II keys. On the otherhand, the node $N^B_{1,1,1}$ contains three Type II keys $\{131, 251, 371\}$ and six Type III keys $\{k_2, k_8, k_{13}, k_{18}, k_{23}, k_{28}\}$ and no Type I keys.

4 Analysis

In this section we will discuss how the network performs on the basis of three different parameters: Resilience, Connectivity and Memory. Then we provide an example to relate these three parameters.

4.1 Memory

We note that there are two types of nodes: Type A and Type B. Now there are k_1 Type I keys in each Type A node and k_2 Type II keys in each Type B node. Type III keys are distributed on the basis of a projective plane $(n^2 + n + 1, n + 1, 1)$ where $(n^2 + n + 1) \approx (c_1 + c_2)$. From the property of projective planes [14], it follows that to establish a connection among m nodes, with a key-pool of size m, each node needs to store $O(\sqrt{m})$ keys. Therefore, number of Type III keys to be stored in each node is $\approx \sqrt{c_1 + c_2}$. Hence memory requirement for each node is $(k_1 + \sqrt{c_1 + c_2})$ or $(k_2 + \sqrt{c_1 + c_2})$.

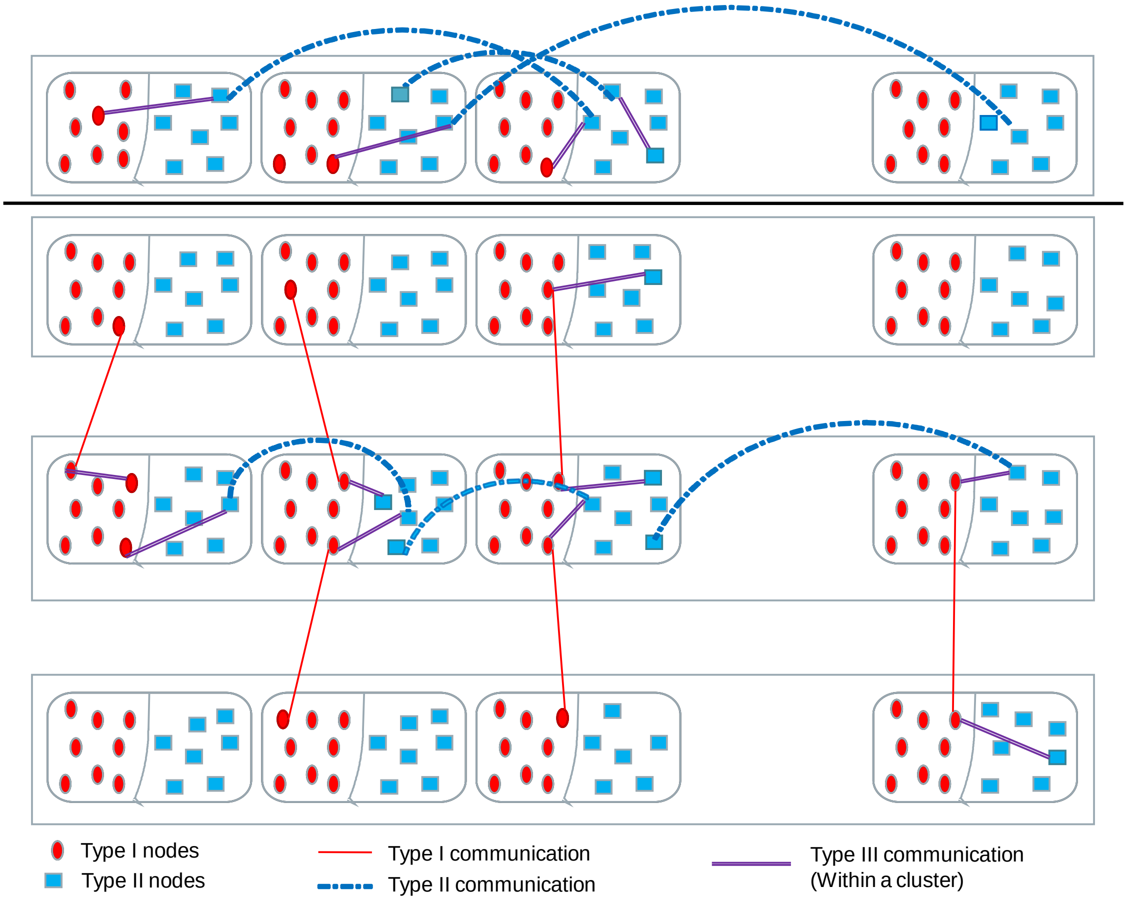

Fig. 1. Type I and Type II connectivity of the network.

4.2 Connectivity

The connectivity of the network is shown in Figure 1. Due to insufficiency of space, only 3 out of a groups, 4 out of b clusters and 8 Type A and 7 Type B nodes are shown.

Single Hop: All the nodes within a cluster are connected to each other through a projective plane. Any node in the network is connected to exactly $c_1 + c_2 - 1$ nodes by Type III keys. Any Type B node contains k_2 Type II keys with each of which it is connected to $(b - 1)$ nodes (exactly one from each of the other clusters from the particular group). Hence, each Type B node is connected to $k_2(b - 1)$ nodes. Similarly, each Type A node is connected to $k_1(a - 1)$ nodes. Therefore, we conclude that any node in the network is connected to either $(c_1 + c_2 + k_1(a - 1) - 1)$ nodes or $(c_1 + c_2 + k_2(b - 1) - 1)$ nodes by single hop path.

Double Hop: Any Type A node is connected to $(k_1)^2(a - 1)$ nodes by Type I keys and any Type B node is connected to $(k_2)^2(b - 1)$ nodes by Type II keys in double hop paths.

Multi Hop: It is known that the nodes who do not share any common key can communicate via a number of intermediate nodes, the path thus established between the two communicating nodes are called multi-hop path. It is observed that each Type A node is connected to $(k_1)^l(a - 1)$ nodes by Type I keys and any Type B node is connected to $(k_2)^l(b - 1)$ nodes by Type II keys in l-hop paths.

Suppose two nodes A and B are chosen randomly from the network. If they share a common key then they can communicate through a direct path. If the nodes do not share a common key then they find some intermediate node C which shares a common key both the nodes A and B; $A - C - B$ is the 2-hop path between the nodes through which they communicate. If two nodes are required to establish a connection between the nodes A and B then the path is referred to be a 3-hop path. If there are $k - 1$ intermediate nodes between the communicating nodes then we call it a k-hop path.

Two nodes chosen randomly communicates via a direct or multi-hop path. The length of the path depends on three factors: (i) The indices of the clusters they belong to, (ii) the indices of the groups they belong to and (iii) the types of the communicating nodes. We summarize the details in Table 2.

1. Within a Group
- *A.* **Within Same Cluster** : Any two nodes are connected by direct path
- *B.* **Between Two Clusters**
  - *(i)* Both nodes are of Type A : connected by 3-hop path
  - *(ii)* Both nodes are of Type B : connected by direct or 2-hop path
  - *(iii)* One node is of Type A and
    the other node is of Type B : connected by 2-hop path

2. Between Two Different Groups
- *A.* **Cluster Index Same** :
  - *(i)* Both nodes are of Type A : connected by 1-hop or 2-hop path
  - *(ii)* Both nodes are of Type B : connected by 3-hop path
  - *(iii)* One node is of Type A and
    the other node is of Type B : connected by 2-hop path
- *B.* **Cluster Index Different** :
  - *(i)* Both nodes are of Type A : connected by 4-hop path
  - *(ii)* Both nodes are of Type B : connected by 4-hop path
  - *(iii)* One node is of Type A and
    the other node is of Type B : connected by 3-hop path

Table 2. Description of multi-hop paths in the network.

Theorem 4.1 *Two nodes from the same cluster do not share any common key other than Type III.*

Proof. We consider the network with a groups, b clusters in each group. Suppose there are c_1 Type A nodes and c_2 Type B nodes in each cluster. $m_1 = max(a, b, c_1)$ and $m_2 = max(a, b, c_2)$. Let us consider two nodes as $N^{s_1}_{p_1,q_1,r_1}$ and $N^{s_2}_{p_2,q_2,r_2}$. Since the nodes belong to the same cluster we can take p_1=p_2=p and q_1=q_2=q. Thus the nodes can be considered as $N^{s_1}_{p,q,r_1}$ and $N^{s_2}_{p,q,r_2}$ where $r_1 \neq r_2$. We consider the following possible cases:
Case (i): When $s_1 = s_2$=A,
Any key of the nodes is of the form $(q \parallel x \parallel y)$ where $y = (x^q + xp + r) \mod m_1$.
Suppose $(q \parallel x_1 \parallel y_1)$ is a key of the node $N^A_{pqr_1}$ and $(q \parallel x_2 \parallel y_2)$ belongs to the key chain of the node $N^A_{pqr_2}$. If the nodes share a common key then we must have $(q \parallel x_1 \parallel y_1)$=$(q \parallel x_2 \parallel y_2)$ i.e., x_1^q+x_1p+$r_1 \equiv x_2^q$+x_2p+r_1(mod m_1). Now, according to the construction, for any two nodes within the same cluster having same keys, we must have $x_1 = x_2$. Thus, we arrive at a contradiction $r_1 = r_2$. This ensures that any two Type A nodes from the same cluster do not share a common key.
Case (ii): When $s_1 = s_2$=B,
Similarly, we take any key of the nodes is of the form $(x \parallel y \parallel p)$ and , where $y = (x^p + xq + r) \mod m_2$.
Suppose $(x_1 \parallel y_1 \parallel p)$ is a key of the node N^B_{p,q,r_1} and $(x_2 \parallel y_2 \parallel p)$ is a key of the node N^B_{p,q,r_2}. The two nodes sharing a common key leads us to $(x_1 \parallel y_1 \parallel p)$=$(x_2 \parallel y_2 \parallel p)$ i.e., $x_1^p + x_1q + r_1 \equiv x_2^p + x_2q + r_1$(mod m_2). Following the similar arguments as above we arrive at a contradiction $r_1 = r_2$. This ensures that any two Type B nodes from the same cluster do not share a common key.
Case (iii): When $s_1 = A$ and $s_2 = B$ (or otherwise),
The keys of $N^{s_1}_{p,q,r_1}$ is of the form $(q \parallel x \parallel y)$ where $y = (x^q + xp + r) \mod m_1$ and keys of $N^{s_2}_{p,q,r_2}$ is of the form $(x \parallel y \parallel p)$ and, where $y = (x^p + xq + r) \mod m_2$. Thus from the key structure of the above nodes, it follows that they do not share any common key, as their key-pools are disjoint.

Hence, we see that for any of the possible cases, any two nodes from the same cluster cannot share a common key. This completes the proof. □

Theorem 4.2 *The total number of single hop paths in the network is given by:*

$$L_1 = \frac{1}{2}ab\{k_1c_1(a-1) + k_2c_2(b-1) + (c_1+c_2)(c_1+c_2-1)\} \tag{1}$$

Proof. From Table 2 it follows that there is a possibility of existence of an 1-hop path between two nodes when the following conditions are satisfied:

(i) Both the nodes (of any type) belong to the same cluster. This is due to Type III communication.
(ii) Group index is same but the Cluster indices are different and both are of Type B. This is due to Type II communication.
(iii) Cluster index is same but the Group indices are different and both are of Type A. This is due to Type I communication.

Now we discuss below these cases elaborately.
Case(i): In this case the existence of a one-hop path is certain and it is independent of the number of keys stored at each node. All the nodes within a particular cluster are directly connected by a direct path of Type III communication. Hence there are $\frac{1}{2}(c_1 + c_2)(c_1 + c_2 - 1)$ number of single hop paths within a particular cluster and consequently, total number of Type III single hop paths in the whole network is

$$\frac{1}{2}ab(c_1 + c_2)(c_1 + c_2 - 1) \tag{2}$$

Case(ii): The length of the path between two nodes of Type B belonging to the different clusters of same group may be one or two. Therefore, the number of one hop paths depends on the number of Type II keys stored at the nodes, since this is Type II communication. From the key distribution procedure, it follows that a Type B node can communicate to k_2 Type B nodes from each of the other clusters within the same group in a single-hop path, when k_2 Type II keys are stored at them, i.e., each Type B node is connected to $(b-1)k_2$ nodes within a group. This holds true for all the Type B nodes in the network. Within a group, there are bc_2 Type B nodes. Hence, the number of Type II single hop path within a group is $\frac{1}{2}(b-1)k_2bc_2 = \frac{1}{2}bk_2c_2(b-1)$. Since, all the groups are identical and there are a groups in the network, we have the total number of Type II single hop paths within the network is

$$\frac{1}{2}abk_2c_2(b-1) \tag{3}$$

Case(iii): This is very similar to Case (ii). The length of the path between two nodes of Type A with same cluster index and different group index may be one or two. Similarly, the number of one hop path depends on the number of Type I keys stored at the nodes. It is also known that a Type A node will be communicating to k_1 Type A nodes from each of the other clusters corresponding to different groups. Since there are ac_1 Type A nodes collectively from the same cluster of different groups, there are $\frac{1}{2}ak_1c_1(a-1)$ Type I single hop paths corresponding to each cluster. Hence, the total number of Type I single hop paths within the network is

$$\frac{1}{2}abk_1c_1(a-1) \tag{4}$$

Combining the expressions obtained in eqn.s (2), (3) and (4) we get the desired expression as in eqn (1). □

Theorem 4.3 *The total number of 2-hop paths in the network is given by:*

$$L_2 = \frac{1}{2}ab\{c_1(c_1-k_1)(a-1) + c_2(c_2-k_2)(b-1) + 2c_1c_2(a+b-2)\} \tag{5}$$

Proof. From Table 2 it follows that there is a possibility of existence of an 2-hop path between two nodes when the following conditions are satisfied:

(i) Group index is same but the Cluster indices are different and one node is of Type A and the other is of Type B : This is due to Type II communication.
(ii) Group index is same but the Cluster indices are different and both are of Type B : This is due to Type II communication.
(iii)Cluster index is same but the Group indices are different and one node is of Type A and the other is of Type B : This is due to Type I communication.
(iv) Cluster index is same but the Group indices are different and both are of Type A : This is due to Type I communication.

Now we discuss the cases in detail as follows
Case(i): For a particular group, we fix any two clusters, then the number of pairs of a Type A and a Type B nodes can be chosen in $2c_1c_2$ ways. The number of such pairs of clusters within a particular group is $\frac{1}{2}b(b-1)$. Since, there are a identical groups, the number of 2-hop paths in the networks under this case is

$$ab(b-1)c_1c_2 \tag{6}$$

Case(ii): In this case the paths obtained between any two nodes is of maximum length two, i.e., it may be a single-hop or 2-hop path. First, let us consider two clusters within a particular group. total number of possible paths between two Type B nodes chosen respectively from the clusters is c_2^2, out of which, c_2k_2 are single hop paths. therefore, exact number of two hop paths is $c_2(c_2-k_2)$. Now the pair of two clusters can be chosen in $\frac{1}{2}b(b-1)$ ways. This hold true for all the groups in the network. Hence, the number of two-hop paths in the network under this case is

$$c_2(c_2-k_2) \times \frac{1}{2}b(b-1) \times a = \frac{1}{2}abc_2(c_2-k_2)(b-1) \tag{7}$$

Case(iii): This case is very similar to case (i). we can consider case (i) as a row-wise operation, then this one is the same operation along the columns of the networks. Hence proceeding in the similar manner we get the number of 2-hop paths in the networks under this case as

$$ab(a-1)c_1c_2 \tag{8}$$

Case(iv): This case is very similar to Case (ii), the concepts of clusters and groups are swaped and parameters are changed accordingly. Proceeding in a similar manner we get the number of two-hop paths in this case as

$$c_1(c_1-k_1) \times \frac{1}{2}a(a-1) \times b = \frac{1}{2}abc_1(c_1-k_1)(a-1) \tag{9}$$

Combining the expressions obtained in eqn.s (6), (7), (8) and (9) we get the desired expression as in eqn (5). □

Theorem 4.4 *The total number of 3-hop paths in the network is given by:*

$$L_3 = \frac{1}{2}ab\{(b-1)c_1^2 + (a-1)c_2^2 + 2(a-1)(b-1)c_1c_2\} \tag{10}$$

Proof. From Table 2 we observe that there is a 3-hop path between two nodes in each of the following cases:

(i) Group index is same but Cluster indices are different and both the nodes are of Type A - a combination of Type II and Type III communication.
(ii) Group indices are different, Cluster index is same and both the nodes are of Type B - a combination of Type I and Type III communication.
(iii) Both Group indices and Cluster indices are different and one node is of Type A and the other node is of Type B - a combination of Type I, Type II and Type III communication.

Now we discuss the cases further as follows
Case(i): There are c_1 Type A nodes within a cluster. If we fix two clusters within a group, then the number of pairs of two Type A nodes is c_1^2. The pairs of clusters can be chosen in $\frac{1}{2}b(b-1)$ ways. Hence, within a group, there are $\frac{1}{2}b(b-1)c_1^2$ 3-hop paths. As there are a identical groups within the network, the number of 3-hop paths under this case in the whole network is

$$\frac{1}{2}ab(b-1)c_1^2 \tag{11}$$

Case(ii): There are c_2 Type B nodes within a cluster. If we fix two clusters out of the set of the clusters along the same column from all the groups, then the number of pairs of two Type B nodes is c_2^2. The pairs of clusters (i.e., actually the pairs of groups) can be chosen in $\frac{1}{2}a(a-1)$ ways. Hence, corresponding to a particular cluster, there are $\frac{1}{2}a(a-1)c_2^2$ 3-hop paths. Since corresponding to each cluster we can establish such paths, which are very similar, the number of three hop paths under this case in the whole network is

$$\frac{1}{2}ab(a-1)c_2^2 \tag{12}$$

Case(iii): There are c_1 Type A and c_2 Type B nodes within a cluster. If we fix two clusters then the number of pairs of a Type A and Type B nodes is $2c_1c_2$. A pair of two clusters with their group indices and cluster indices unequal, can be chosen from the network in $ab(a-1)(b-1)$ ways. Hence the number of three hop paths under this case in the whole network is

$$ab(a-1)(b-1)c_1c_2 \tag{13}$$

Adding the results obtained in eqn.s (11), (12) and (13) we get the desired expression as in eqn (10). □

Theorem 4.5 *The total number of 4-hop paths in the network is given by:*

$$L_4 = \frac{1}{2}ab(a-1)(b-1)(c_1^2 + c_2^2) \tag{14}$$

Proof. From Table 2 it follows that there is a 4-hop path between two nodes when any of the following conditions are satisfied:

(i) Group indices and Cluster indices are different and both the nodes are of Type A
(ii) Group indices and Cluster indices are different and both the nodes are of Type B

The clusters of the nodes are chosen in a way that their cluster indices and group indices are unequal. Thus, for a fixed cluster, there are $(a-1)(b-1)$ clusters such that the above conditions are satisfied. Therefore, there are $\frac{1}{2}ab(a-1)(b-1)$ pairs of such clusters.
Case(i): Each cluster contains c_1 Type A nodes, therefore, between two such pairs of clusters there are c_1^2 such pairs of Type A nodes. This holds true for a particular pair of cluster, and since all the clusters are uniform and there are $\frac{1}{2}ab(a-1)(b-1)$ such pairs of clusters, the number of 4-hop paths in this case is given by: $\frac{1}{2}ab(a-1)(b-1)c_1^2$.
Case (ii): As each cluster contains c_2 Type B nodes, following the similar arguments as in Case (i), there are $\frac{1}{2}ab(a-1)(b-1)c_2^2$ more 4-hop paths.
Thus, the total number of 4-hop paths is the summation of the paths obtained in the above two cases. □

Theorems 1, 5, 10 and 14 give the number of single-hop, 2-hop and 3-hop paths in the network. With the help of which we provide an expression for average path-length between two nodes in the network, as follows, given by:

$$d = \frac{L_1 \times 1 + L_2 \times 2 + L_3 \times 3 + L_4 \times 4}{L_1 + L_2 + L_3 + L_4} \tag{15}$$

4.3 Resilience

When a few nodes are compromised by the adversary, the effect is observed on both nodes and links. We discuss both the cases in the following:

Node-Disconnection

Lemma 4.6 *The number of nodes that become disconnected when s nodes are compromised is*

$$v_1(s) = \frac{s}{(c_1+c_2)}\{\frac{c_1}{(a-1)k_1+\sqrt{c_1+c_2}} + \frac{c_2}{(b-1)k_2+\sqrt{c_1+c_2}}\}$$

Proof. Each Type A node contains k_1 Type I keys, with each of which it is connected to $a-1$ nodes and $\sqrt{c_1+c_2}$ nodes by Type III keys. Therefore, each Type A node is connected to $(a-1)k_1+\sqrt{c_1+c_2}$ Type A nodes. Which implies that to disconnect only one Type A node, $(a-1)k_1+\sqrt{c_1+c_2}$ Type A nodes should be compromised. Thus, when s Type A nodes are compromised, $\frac{s}{(a-1)k_1+\sqrt{c_1+c_2}}$ Type A nodes are disconnected.

Proceeding in a similar manner we find that each Type B node is connected to $(b-1)k_2+\sqrt{c_1+c_2}$ Type B nodes, and hence, when s Type B nodes are compromised, $\frac{s}{(b-1)k_2+\sqrt{c_1+c_2}}$ Type B nodes are disconnected.

But, the ratio of Type A and Type B nodes in the network is $c_1 : c_2$. Therefore, we have the average number of disconnected nodes when s nodes are compromised $= \frac{s}{(c_1+c_2)}\{\frac{c_1}{(a-1)k_1+\sqrt{c_1+c_2}} + \frac{c_2}{(b-1)k_2+\sqrt{c_1+c_2}}\}$.
□

Now, we discuss below the effect of adversarial attack on node-disconnection.
The portion of nodes that become disconnected when s nodes are compromised is given by:

$$V(s) = \frac{v_1(s)}{N-s} = \frac{s\left[\frac{c_1}{(a-1)k_1+\sqrt{c_1+c_2}} + \frac{c_2}{(b-1)k_2+\sqrt{c_1+c_2}}\right]}{(c_1+c_2)(N-s)}$$

Comparison of Node-disconnections with an existing scheme:

	N	s	$V(s)$	N	s	$V(s)$
[12]	2041	100	0.0003867	2041	150	0.098
Ours	2040	100	0.0004540	2040	150	0.0007
[12]	5041	150	0.0762	5041	200	0.01139
Ours	5040	150	0.000114	5040	200	0.000153

Link-failure We calculate the resilience by the formula proposed by Lee-Stinson [8] as follows:

$$fail(s) = 1 - \left(1 - \frac{r-2}{n-2}\right)^s$$

where r is the number of nodes to which each node can communicate directly and n denotes the total number of nodes in the network. We define $fail_1(s)$, $fail_2(s)$ and $fail_3(s)$ for Type I, Type II and Type III communication respectively as follows:

$$fail_1(s) = 1 - \left(1 - \frac{(a-1)k_1-2}{abc_1-2}\right)^s$$

$$fail_2(s) = 1 - \left(1 - \frac{(b-1)k_2-2}{abc_2-2}\right)^s$$

$$fail_3(s) = 1 - \left(1 - \frac{c_1+c_2-3}{ab(c_1+c_2)-2}\right)^s.$$

Overall Failure:

The Type I, Type II and Type III nodes within the network are in the ratio $c_1 : c_2 : (c_1+c_2)$. Therefore, average overall failure, denoted by $fail(s)$, is given as:

$$fail(s) = \frac{c_1 fail_1(s) + c_2 fail_2(s) + (c_1+c_2) fail_3(s)}{2(c_1+c_2)}$$

4.4 Example : Resilience of the scheme

We consider a particular network, where
number of groups in the network $a = 5$; number of clusters in each group $b = 15$; Type A nodes in each cluster $c_1 = 10$; Type B nodes in each cluster $c_2 = 18$; Type I keys in each Type A node $k_1 = 3$; Type B keys in each Type B node $k_2 = 5$; total number of nodes in the network $N = 2100$.

Resilience: If s nodes are compromised, how the rest of the network is affected has been shown in the following table.

s	$fail(s)$	s	$fail(s)$	s	$fail(s)$	s	$fail(s)$
10	0.005748	80	0.400137	150	0.723276	500	0.996314
20	0.032442	90	0.459076	200	0.847436	550	0.998022
30	0.079110	100	0.513712	250	0.917214	600	0.998937
40	0.138573	110	0.563937	300	0.955421	700	0.999692
50	0.204230	120	0.609812	350	0.976077	800	0.999910
60	0.271437	130	0.651505	400	0.987177	900	0.999974
70	0.337297	140	0.689241	450	0.993127	1000	0.999992

Table 3. How the network collapses with increasing number of compromised nodes

Connectivity: Type A nodes are connected to 40 nodes by single hop path and 120 nodes by double hop path. Type B nodes are connected to 98 nodes by single hop path and 490 nodes by double hop path.

Memory: Type A nodes needs to store 8 keys and Type B nodes needs to store 10 keys respectively.

It is very obvious from the distribution procedure that connectivity of Type I and Type II communication can be increased to the desired level by increasing the number of Type I and Type II keys in the nodes, which will affect the resilience due to Type I and Type II communication, but Type III communication will remain unaffected.

4.5 Example : Overall Performance of the Scheme

Here we consider another set of values for the parameters to establish another network. The overall performance of our scheme is shown in Table 4.5. The notation used in Table 4.5 are as follows:

a	Number of groups in the network
b	Number of clusters in each group
c_1	Number of Type A nodes in each cluster.
c_2	Number of Type B nodes in each cluster.
k_1	Number of Type I keys stored in each Type A node.
k_2	Number of Type II keys stored in each Type B node.
N	Total number of nodes in the network
L	Total number of paths in the network
L_i	Total number of i-hop $(i = 1, 2, 3, 4)$ paths in the network
d	Average path length
$p(c)$	connection probability, where $p(c) = \frac{L_1}{L}$
s	number of compromised nodes
$V(s)$	Portion of nodes disconnected when s nodes are compromised.

5 Performance

In this section we shall concentrate on comparing the performance of our scheme with other existing schemes.

a	b	c_1	c_2	k_1	k_2	N	L	L_1	L_2	L_3	L_4	d	$p(c)$	s	$V(s)$
3	4	5	6	4	4	132	8646	1596	1812	3042	2196	2.675	0.18459	10	0.006211
3	4	5	6	5	5	132	8646	1830	1578	3042	2196	2.648	0.211659	10	.005239
4	5	50	52	20	30	2040	2079780	221020	429160	805120	624480	2.8813	0.106271	100	0.00562
4	5	50	52	48	48	2040	2079780	323820	326360	805120	624480	2.8319	0.155699	100	0.000294
5	8	56	70	10	10	5040	12698280	483000	2493680	5221440	4500160	3.0819	0.038037	100	0.000314
5	8	56	70	49	49	5040	12698280	1138200	1838480	5221440	4500160	3.0303	0.089634	200	0.000153

Table 4. Overall performance

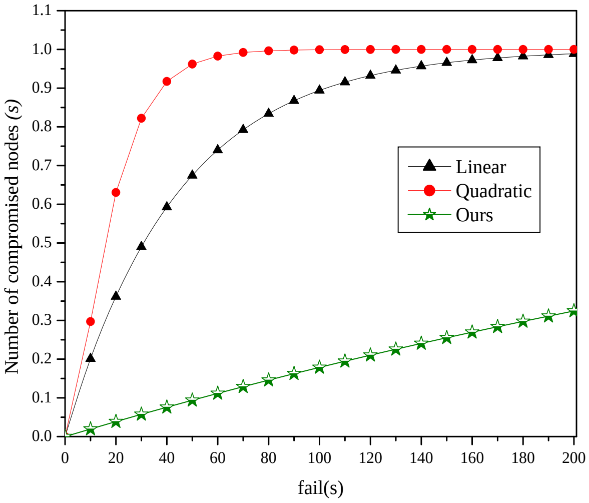

Fig. 2. Comparison of resilience with some of the existing schemes

	[8]	[3]	[11]	[10]	Ours
N	1849	2550	2415	2197	2100
k	30	≤ 28	136	30	7
$fail(10)$	0.201070	0.213388	0.0724	0.297077	0.019569

Table 5. Comparison of resilience with some of the existing schemes

In Table 5, we provide the comparison based on the resilience of our scheme with that of Lee-Stinson linear scheme [8], Chakrabarti et al. scheme [3], Ruj-Roy scheme [11] and Lee-Stinson quadratic scheme [10], where N denotes total number of nodes in the network and k denotes total number of keys present in each node. To keep up total number of nodes N in the network in our scheme comparable with other schemes, we consider the network with the following:
number of groups $a = 10$, number of clusters $b = 15$, number of Type A nodes $c_1 = 5$ and number of Type B nodes $c_2 = 8$. The details have been mentioned in the table.

Figure. 2 comprises scheme with Lee-Stinson linear scheme [8] and Lee-Stinson quadratic scheme [10] for 10 - 200 compromised nodes. It is very evident from the figure that the networks incorporated on other schemes collapses rapidly compared to ours.

6 Conclusion

The network is divided into groups of clusters and clusters of nodes. The key-pool consists of three types of keys to set-off communications. It is found that our scheme outperforms some of the existing schemes.

Obtained results show that the provides enhanced resilience - both on nodes and links. The memory requirement for each node is also diminutive with reasonable connectivity. Therefore, by subdividing the network, an advantageous trade-off between the parameters is obtained.

References

1. Camptepe S. A., Yener B.: Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. *ESORICS, 3193, pp: 293-308,* Springer, (2004).
2. Camptepe S. A., Yener B.: Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. *ACM Trans. Netw. 15(2), pp: 346-358,* (2007).
3. Chakrabarti D., Maitra S., Roy B.: A Key Scheme for Wireless Sensor Networks: Merging Blocks in combinatorial Design. *ISC, LNCS, vol. 3650, pp: 89-103,* Springer, (2005).
4. Chakrabarti D., Seberry J.: Combinatorial Structures for Design of Wireless Sensor Networks. *ACNS, LNCS, vol. 3989, pp: 365-374,* Springer, (2006).
5. Chan H., Perrig A., Song D. X.: Random Key Predistribution Schemes for Sensor Network. *In IEEE Symposium on Security and Privacy, pp: 197-213*, (2003).
6. Dong J., Pei D., Wang X.: A Key Predistribution Scheme Based on 3-designs. *Inscrypt 2007, LNCS, vol. 4990, pp: 81-92,* Springer, (2008).
7. Eschenauer L., Gligor V. D. : A Key-management Scheme for Distributed Sensor Networks. *ACM CCS, pp: 41-47.* ACM, (2002).
8. Lee J., Stinson D. R.,: A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks. *In IEEE Wireless Communications and Networking Conference , pp: 1200-1205,* (2005).
9. Lee J., Stinson D. R.,: Common Intersection Designs. *International Journal of Combinatorial Designs , vol. 14, pp: 251-169,* (2006).
10. Lee J., Stinson D. R.,: On The Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs. *ACM Trans. Inf. Syst. Secur., 11(2),* (2008).
11. Ruj S., Roy B.: Key Predistributions Using Partially Balanced Designs in Wireless Sensor Networks. *ISPA, LNCS, vol. 4742, pp: 431-445,* Springer, (2007).
12. Ruj S., Roy B.: Key Predistributions Schemes Using Codes in Wireless Sensor Networks. *Inscrypt 2008, LNCS, vol. 5487, pp: 275-288*,2008.
13. Stinson D.R., *Cryptography : Theory and Practice.* CRC Press, 2002.
14. Stinson D.R., *Combinatorial Designs: Constructions and Analysis.* Springer, New York, 2003.