A Technique for Communication of Distance Node on Key Pre-distribution in Wireless Sensor Networks

Sourav Kanti Addya [1] and Ashok Kumar Turuk [2]
Department of Computer Science & Engineering
National Institute of Technology, Rourkela, India
Email: {[1] kanti.sourav, [2] akturuk}@gmail.com
November 2010

***Abstract*- Sensor nodes are tiny devices, with less computational power and memory capacity. For secure communication, the secret keys must be built into the nodes before deployment. Distribution of keys among the sensor nodes is a challenging task. Numbers of sensor nodes are usually much higher than the number of keys available. In this paper we use Steiner Triple system (STS) which is a combinatorial design to distribute the keys among the sensor nodes. As the keys are built into the nodes, no path key establishment phase is required for secure communication. Hence nodes can communicate using the built in secret keys. Thus, a faster communication is achieved. However, STS is not an appropriate candidate for large networks, where sensors are not within the communication range of each other. To overcome this we propose a cluster based key pre-distribution using Steiner Triple System. We evaluated the resiliency of our proposed system and found to have a better resiliency.**

***Index Term* - WSN, Key Pre-distribution, Steiner system, Steiner Triple System, Sensor networks.**

I. INTRODUCTION

Wireless sensor network is a collection of spatially distributed autonomous sensor nodes cooperatively monitoring the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of WSN was originally motivated by military applications such as battlefield surveillance. A sensor node has mainly four basic components: (i) Processing unit, (ii) Sensing unit, (iii) Transceiver unit and (iv) Power unit. It is a fact that individual sensor nodes have limited resources; they are capable of achieving worthy task of good volume when they work together in a group. For secure communication between any two sensors nodes, is needed a shared secret key. The distribution of keys among the sensor nodes is a challenging task, as the numbers of nodes are much higher than the available keys. Key pre-distribution in sensor nodes may be: - i) probabilistic, ii) deterministic or iii) hybrid. Eschenauer et al. [1] first proposed the probabilistic key pre-distribution. It depends on probabilistic key sharing among the nodes of a random graph. It needs a key establishment phase where two neighbouring nodes exchange messages to find a common key between them. Unlike schemes that use dedicated pair-wise keys, it may be possible in this solution that same key is used to secure more than one links. Eschenauer et al. [1] scheme has a key generation and distribution phase. To reduce the burden of key generation and distribution, a set of keys are pre distributed into every sensor nodes before their deployment in the network.

There are several schemes for key distribution [2], such as

A. Single key for the whole WSN:

In this scheme there is only one secret key for the whole network. Nodes communicate using this key. The problem associated with this method is, if the secret key gets compromised, then the secure communication in the network gets compromised.

B. Each node keeps shared key for every other node:

In this scheme each node keeps a secret key for every other node in the network. That is each node maintains n-1 numbers of keys. Compromise of any node will merely disconnect that node from the whole network. This will not affect the rest of the network. However, this scheme is not scalable with increase in the number of nodes. For larger number of nodes, large numbers of keys are to be maintained at each node, which demands more memory. As memory contained in sensor nodes, maintaining larger number of keys is not possible.

C. Public key cryptosystem:

Use of public key cryptosystem demands high processing power. Hence it is no efficient for wireless sensor network [2]. Gura et al proposed the implementation of RSA and ECC on a 8 bit processor. However, it consumes more processing power [3].

D. Key pre-distribution:

In key pre-distribution, a set of keys is built into the node from a key pool before deployment. The number of keys deployed in each sensor nodes is very small as number in compared to the number of nodes in the network. There are three phases in key pre-distribution scheme: (i) key pre-distribution, (ii) shared key-discovery and (iii) path key establishment.

DOI: 01.IJRTET 04.01.115

In key pre-distribution phase a set of keys is chosen from a key pool following some predetermined technique. Thus, each sensor node is assigned a set of keys, called key chain, before their deployment in the network. In shared key discovery phase if two nodes want to communicate and they are within the radio frequency range of each other then they established a common key between them. There may or may not be more than one common key between two nodes.

Path key establishment phase occurs if there is no common key between two nodes. A secure path is established between source and destination, such that every pair of adjacent nodes on the path has a secure common key [4].

Several schemes for key-pre distribution have been proposed for wireless sensor networks using both probabilistic and deterministic approach. Eschenauer and Gligor [1] in the year 2002 for the first time proposed a random key pre-distribution scheme in which keys are drawn from a key pool. In the year 2004, Camtepe and Yener [4] proposed a deterministic key pre-distribution scheme using combinatorial design. Lee and Stinson [5] used transversal design for pre-distribution. Chakraborty ,Mitra and Roy [2] describe the resiliency of the network. The various KPS schemes are classified into the following categories [6] (i) Eschenauer and Gligor's scheme, (ii) q-composite scheme, (iii) Camtepe and Yener's scheme, (iv) Lee and Stinson's scheme, and (v) Chakrabarti, Maitra and Roy's scheme. A comparison between different schemes is shown in Table 1.

In this paper we have proposed a key pre-distribution using *STS*. We have shown that *STS* is more suitable for smaller network. For larger network, we divide the network into numbers of overlapped cluster and distribute the keys using *STS* within the clusters.

Rest of the paper is organised as follows. In Section 2 we discussed the basic of Combinatorial design and Steiner system. The proposed key pre-distribution using *STS* is discussed in Section 3. Cluster based scheme for larger network is discussed in Section 4 and some conclusions are drawn in Section 5.

II. PRRELIMINARIES

A. Basics of Combinatorial Design

Combinatorial design theory is to arranging elements of a finite set into subsets to satisfy certain properties [7]. Members of a universal set S in a combinatorial design are usually called treatments, or varieties, and the chosen subsets are called blocks. For the sake of completeness, we reproduce two definitions of combinatorial design as given in [8].

Definition 1. A design is a pair (X, A) such that the following properties are satisfied:

(i) X is a set of elements called points, and

(ii) A is a collection (i.e., multiset) of nonempty subsets of X called blocks.

If two blocks in a design are identical, they are said to be repeated blocks. A is referred as a multiset of blocks rather than a set. A design is said to be a *simple design* if it does not contain repeated blocks.

Definition 2. Let v, k, λ *be positive integers such that* $v > k \geq 2$. A *(v, k, λ)-* balanced incomplete block design (*which we abbreviate to (v, k, λ)-* BIBD) *is a design (X, A) such that following properties are satisfied:*

(i) $|X| = v$,

(ii) each block contains exactly k points, and

(iii) every pair of distinct points is contained in exactly λ block.

The third property in the above definition is known as "balance" property. A BIBD is called an *incomplete block* design because the value of $k < v$, and hence all its block are *incomplete blocks*.

DOI: 01.IJRTET 04.01.115

TABLE I.
COMPARISON BETWEEN DIFFERENT SCHEMES

Sl. No.	Name/ Proposed person	Types of key pre-distribution	Proposed year	Main parameters	Remarks
1	Eschenauer and Gligor	Probabilistic	2002	n= total no of nodes k= size of key ring p= size of key pool	First distribute the keys among sensor nodes.
2	q-Composit / Chan et al.	Probabilistic	2003	-	Two nodes compute a pairwise key only if they share at least *q* common keys.
3	Cmatepe and Yener	Deterministic	2004	-	First applied Combinatorial design mainly *SBIBD*.
4	Lee and Stinson	Deterministic	2004	v= key pool size b= number of sensor nodes r= number of sensor nodes in which a given key occurs k= number of keys in a nodes	First applied Transversal design
5	Chakraborty, Mitra and Roy	Deterministic	2006	v= key pool size b= number of sensor nodes r= number of sensor nodes in which a given key occurs k= number of keys in a nodes λ= number of nodes which contain a given pair of keys	Give proper definition of Resiliency in terms of E(s) and V(s). They merged the blocks randomly to avoiding intra node common keys as much as possible

B. Steiner System

In combinatorial mathematics, a Steiner system (named after Jakob Steiner) is a type of block design. A Steiner system *S(t, k, v)* is a set *X* of *v* points, and a collection of subset of *X* of size *k* (called *blocks*), such that any *t* points of *X* are in exactly one of the blocks. An *S(2, 3, n)* is called a *Steiner triple system*, and its blocks are called triples. *projective plane*, $v = n^2 + n + 1$, $k = n + 1$, $t = 2$, and the blocks are simply lines.

The number *r* of blocks containing a point in a *S(t, k, v)* Steiner system is independent of the point. In fact,

$$r = \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}},$$

where $\binom{n}{k}$ is a binomial coefficient. The total number of blocks *b* is also determined and is given by

$$b = \frac{vr}{k}.$$

These number is also satisfy $v \leq b$ and $k \leq r$.

III. STEINER TRIPLE SYSTEM FOR KEY PRE-DISTRIBUTION

In this section we will illustrate the key pre- distribution using *Steiner Triple System*, which is special case of *Steiner System*. A *Steiner System S(t, k, v)* is a set X of *v* points, and a collection of subset of X of size *k* (called blocks), such that any *t* points of X are in exactly one of the blocks. If there is a *Steiner System S (t, k, v)*, then *v=1* or *x mod x(x-1)* where *x* is *prime power* greater than 1.For *Steiner Triple System* the value of t=2 and x=3. A *Steiner Triple System S(2, 3, v)* must have *v= 6k+1 or 6k+3* where *k* is any positive integer. For an integer *k*, there exists *Steiner Triple System S (2, 3, 6k+1)* and *S (2, 3, 6k+3)* [7, 8].

For key pre-distribution using *Steiner Triple System*, *v = Total number of keys, x = Number of keys in each node or blocks, t = number of points are occur in exactly one of the blocks*.

In our illustration we consider a *Steiner Triple System S (2, 3, 7)*. Where t=2, k=3, *v*=7. The size of our key pool *v =7*, each block/node have 3 number of keys and any pair of keys are occur in exactly one of the blocks.

In key per-distribution, we first group the keys into blocks and assign each block to not more than one node. Possible combination of keys is assigned to node such that it satisfies the *STS* condition. Using a key pool many arrangement of key can be possible. Some possible arrangement and one such assignment is shown in Table:2. In our present case each block will have 3 keys. The grouping of keys into blocks and the assignment of each block in sensor nodes are shown in Table: 3. For example, node *n2* has the key chain *{1, 5, 4}*.

DOI: 01.IJRTET 04.01.115

TABLE II.
ARRANGEMENT OF KEYS

Key pool	{1,2,3,4,5,6,7}
Possible combinations of keys	123, 124, 125, 126,127, 134, 135, 136, 137,145, 146, 147, 156, 157, 167,234, 235, 236,237, 245, 246, 247, 256, 257,267, 345, 346, 347, 356, 357, 367, 456, 457, 467, 567
Some possible set of key chain satisfying *STS* conditions	{123, 145, 167, 246, 257, 356, 347}
	{124, 137, 156, 235, 267, 346, 457}

TABLE III.
ASSIGNMENT OF BLOCKS INTO NODES

Block	Assigned Node
{1,2,3}	n1
{1,5,4}	n2
{1,6,7}	n3
{2,5,7}	n4
{6,5,3}	n5
{2,6,4}	n6
{3,4,7}	n7

We assume that sensor nodes are within the communication range of each other and all sensor nodes are stationary. Any two nodes can communicate using the common key between them. Since a common key exists between every pair of nodes and they are within the communication range of each other. The apriori *path key establishment* phase is not required.

The connection probability or connectivity is defined as the probability that there is a common key between them. In this case the total possible links are ${}^{7}C_{2} = 21$. The connection probability in the example that we have considered is exactly one.

A. Analysis and Comparison

We have compared our approach with that of *Lee and Stinson* [5, 6] approach. In the proposed approach for every pair of nodes there exist at least one common key and no apriori *path key establishment* phase is required.

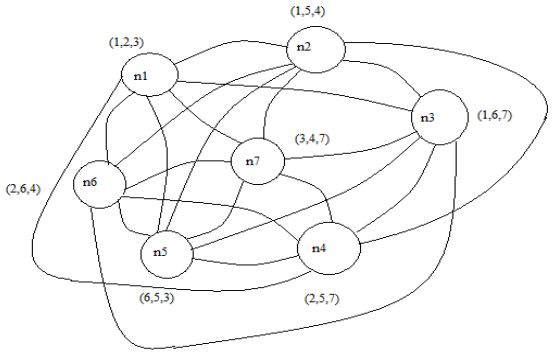

Figure 1. A sensor network of seven sensor nodes

Therefore nodes communicate directly among each other. For the same example that we have considered, 60% of nodes communicate directly and 40% communicate via some intermediate nodes in *Lee and Stinson* approach [5, 6]. Communication will be faster in the proposed scheme as no intermediate nodes are involved in communication between pairs. However, the proposed scheme is suitable for a smaller network where the nodes are within the communication range of each other. For a larger network the key pool size *i.e.* value of *v* becomes very large. A large number of key chain is harder to accommodate in sensor nodes with limited memory. For a larger network the nodes may not be within the communication range of each other. So, the proposed scheme cannot be applied to a larger network where the nodes are not within the communication range of each other. To overcome this problem we proposed a cluster based scheme in Section 4.

IV. CLUSTER BASED SCHEME FOR LARGE SENSOR NETWORK

For a larger network we divided the nodes into overlapped clusters as mentioned in [9]. Between two clusters there exist common node called *gateway node*, which have a common key for both clusters. Two nodes in different clusters communicate through the gateway node. We use the proposed key pre-distribution scheme for key distribution within a cluster.

For illustration of clustering scheme we consider an eighteen node sensor network as shown in Figure 2. The network is partitioned into three overlap cluster as mentioned in [9]. Node *n5, n6* and *n11* are the gateway nodes.

For key pre-distribution we select

i. The same key pool for all clusters, and
ii. Different key pool for different clusters.

A. Clustering using same key pool

In this scheme we use the same key pool in all clusters. The distribution of keys among the sensor nodes in other different cluster are shown in Table 4.

Nodes within the same cluster (intra cluster) communicate directly as they are within the communication range and shared a common key between them. For communication among nodes in different cluster (inter cluster) a *path key establishment* phase is required. Inter cluster communication is trivial. Inter cluster communication is illustrated with an example.

Suppose, node *n3* of *cluster 1* wants to communicate with node *n10* of *cluster 2*. The key chain assigned to *n3* in *cluster 1* is *f3, 5, 6g* and *n10* in *cluster 2* is *f1, 4, 6g* as shown in Table 4. Though nodes *n3* and *n10* have a common key between them but they resides in different clusters. So, a *path key establishment* phase is required prior to the communication. The path key is established using the gateway node *n5*. Nodes *n3* and *n5*

DOI: 01.IJRTET 04.01.115

communicated using their common key *3*. Node *n5* and *n10* communicate using their common key *4*. Node *n10* generates a temporary key and send it to node *n3* via gateway node *n5*. Hereafter, node *n3* and node *n10* communicate using the temporary key.

Form the above example we can see that we distribute same seven keys among eighteen different nodes of three clusters. For the different combinations of keys the possible key chain or block will be different.

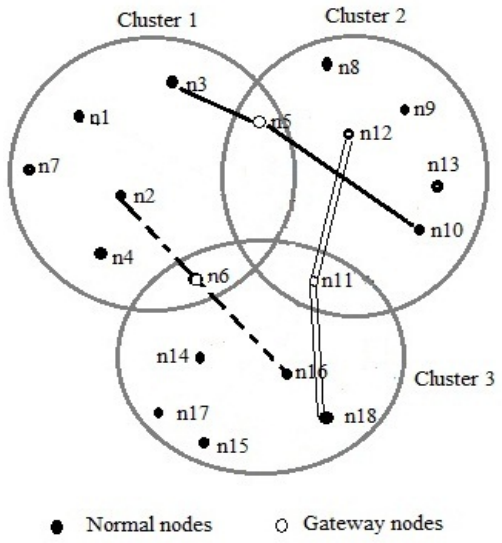

Figure 2. A sensor network with three overlapped clusters

B. Clustering using different key pool

In this scheme we use different key pools for different clusters. This scheme defers from the previous scheme mentioned in subsection 4.1 in two aspects:

i. No two nodes in different clusters have a common key.

ii. The gateway odes carry two sets of key chain from each cluster.

TABLE IV.
DISTRIBUTION OF KEYS AMONG THE NODES IN DIFFERENT CLUSTER

Cluster 1		Cluster 2		Cluster 3	
Node	Assigned Key chain	Node	Assigned Key chain	Node	Assigned Key chain
n1	{1,4,5}	n5	{3,4,7}	n6	{1,6,7}
n2	{1,2,3}	n8	{1,2,7}	n11	{2,3,6}
n3	{3,5,6}	n9	{1,3,5}	n14	{1,2,5}
n4	{2,4,6}	n10	{1,4,6}	n15	{1,3,4}
n5	{3,4,7}	n11	{2,3,6}	n16	{2,4,6}
n6	{1,6,7}	n12	{2,4,5}	n17	{3,5,7}
n7	{2,5,7}	n13	{5,6,7}	n18	{4,5,6}

Distributions of keys among the nodes in different clusters are shown in Table 5. The intra cluster communication is trivial. Inter cluster communication is done as explained in subsection 4.1.

C. Analysis and Comparison with existing approach

We analysed the resiliency in two different cluster based schemes; one that uses the same key pool and the other that uses different key pool.

Suppose node *n1* in *cluster 1* gets compromised. Than the keys *{1, 4, 5} associated* with *node 1* also gets compromised. All link pairs using key *1, 4* and *5* is broken in *cluster 1*. In *cluster 2* and *cluster 3* the links using *1, 4* and *5* is also broken. The resiliency in *cluster 1, cluster 2* and *cluster 3* are 0.5714, 0.5714 and 0.5714 respectively. This also happen for the same key pool.

For different key pool; the links in *cluster 1* only gets compromised. No links in *cluster 2* and *cluster 3* gets compromised. So, a better security and resiliency obtained using different key pool.

TABLE V.
DISTRIBUTION OF KEYS FROM DIFFERENT KEY POOLS AMONG THE NODES IN DIFFERENT CLUSTER.

Cluster 1 Key pool={1,2,3,4,5,6,7}		Cluster 2 Key pool={A,B,C,D,E,F,G}		Cluster 3 Key pool={a,b,c,d,e,f,g}	
Node	Assigned Key chain	Node	Assigned Key chain	Node	Assigned Key chain
n1	{1,2,3}	n12	{B,F,G}	n16	{a,b,d}
n2	{1,4,5}	n8	{A,B,C}	n17	{c,d,f}
n3	{1,6,7}	n9	{A,D,E}	n14	{a,c,g}
n4	{2,4,6}	n10	{A,F,G}	n15	{b,c,e}
n5	{3,4,7,C,E,F}	n11	{B,D,F,a,d,e}	n6	{b,f,g,3,5,6}
n6	{3,5,6,b,f,g}	n5	{3,4,7,C,E,F}	n11	{a,d,e,B,D,F}
n7	{2,5,7}	n13	{C,D,G}	n18	{d.e,g}

V. CONCLUSION

We proposed a key pre-distribution using *STS*. In the proposed technique no *path key establishment* phase is required for a smaller network, where nodes are within the communication range. Since no *path key establishment* is required, a faster communication is possible.

STS is not suitable for a larger network, where all nodes are not within the communication range of each other. For a larger network we divided it into number of overlapping clusters. Within each cluster, we distributed the keys using *STS*. We observed that using different key pool, for different clusters a better resiliency is achieved.

DOI: 01.IJRTET 04.01.115

REFERENCES

[1] Laurent Eschenauer and Virgil D. Gligor. A Key management Scheme For Distributed Sensor Networks. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 41–47. ACM, 2002.

[2] Chakrabarti Dibyendu, Maitra Subhamoy, and Roy Bimal. A Key Pre-distribution Scheme For Wireless Sensor Networks:Merging Blocks In Combinatorial Design. *International Journal Information Security.*, 5(2):105–114, 2006.

[3] Nils Gura, Arun Patel, Arvinderpal Wander, HansEberle, and Sheueling Chang Shantz. ComparingElliptic Curve Cryptography and Rsa On 8-bit Cpus.In Marc Joye and Jean-Jacques Quisquater, editors,*CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 119–132. Springer, 2004.

[4] Seyit A.amtepe and Blent Yener. Combinatorial Design Of Key Distribution Mechanisms For Wireless Sensor Networks. In *9th European Symposium On Research Computer Security*, pages 293–308, 2004.

[5] Jooyoung Lee and Douglas R. Stinson. Deterministic Key Pre-distribution Schemes For Distributedsensor Networks. In *Selected Areas in Cryptography, Lecture Notes in Computer Science*, pages 294–307, 2004.

[6] Jooyoung Lee and Douglas R. Stinson. On The Construction Of Practical Key Pre-distribution Schemes For Distributed Sensor Networks Using Combinatorial Designs. *ACM Transactions on Information and System Security (TISSEC)*, 11(2):1– 35, 2008.

[7] A P Street and D J Street. *Combinatorics of experi- mental design*. Oxford University Press, Inc.,New York, NY, USA, 1986.

[8] Douglas R. Stinson. *Combinatorial Designs: Construction and Analysis*. Springer Verlag,2003. [9] Rajesh Krishnan and David Starobinski. Efficient Clustering Algorithms For Self-organizing Wireless Sensor Networks. *Ad Hoc Networks*, 4(1):36–59, 2006.

[10] Keith M. Martin. On the Applicability of Combinatorial Designs to key predistribution for wireless sensor networks. In Yeow Meng Chee, Chao Li,San Ling, Huaxiong Wang, and Chaoping Xing,editors, *IWCC*, volume 5557 of *Lecture Notes in Computer Science*, pages 124–145. Springer,2009.

DOI: 01.IJRTET 04.01.115