Secure Key Pre-distribution in Wireless Sensor Networks Using Combinatorial Design and Traversal Design Based Key Distribution

Saba Khalid, Faiyaz Ahmad, Mohd. Rizwan Beg

Department of Computer Science and Engineering, Integral University, Lucknow,226026, India
E-mail : sksabask@gmail.com, faiyaz.ahamad@gmail.com, rizwan.beg@gmail.com

Abstract - Security is an indispensable concern in Wireless Sensor Network (WSN) due to the presence of potential adversaries. For secure communication in infrastructureless sensor nodes various key predistribution have been proposed. In this paper we have evaluated various existing deterministic, probabilistic and hybrid type of key pre-distribution and dynamic key generation algorithms for distributing pair-wise, group-wise and network-wise keys and we have propose a key predistribution scheme using deterministic approach based on combinatorial design and traversal design which will improve the resiliency and achieve sufficient level of security in the network.This design can be used where large number of nodes are to be deployed in the WSN.

Keywords *— Sensor nodes(SN), Combinatorial design, Key pre-distribution scheme(KPS), Resiliency, Symmetric balanced incomplete block design(SBIBD), Traversal design*

I. INTRODUCTION

Sensor networks is a distributed adhoc network of collection of sensor nodes which are inexpensive devices having low battery power, low computation speed, limited memory capability and limited resources. Motivation of this paper is to evaluate the different key distribution solutions. On the basis of application types network architectures are classified such as distributed or hierarchical, communication styles such as pair-wise (unicast),group-wise (multicast) or network-wise (broadcast), security requirements such as authentication, confidentiality or integrity, and (iv) keying requirements such as pre-distributed or dynamically generated pair-wise, group-wise or network-wise keys. Key management services provide and manage the basic security material for satisfying the previously mentioned security services. In this paper we have presented a new KPS that uses combinatorial design and traversal design.

The rest of the paper is organised as in section II, deals with a brief background of combinatorial design theory. KPS is presented in section III. Section IV discusses and evaluates scalability issues and effects of node compromise in sensor networks. Finally in section V, the paper concludes with future work.

II. BACKGROUND: RELATED WORK

WSN consists of low power nodes which are randomly deployed and can effectively communicate to each other within a particular radio frequency range. According to their capability of communication nodes are classifieds as: (i) base stations (ii) cluster heads (iii) sensor nodes. For secure communication in SN keys can be either pre-distributed or online key exchange protocols can be used. Online key distribution scheme cannot be used as it requires public-key cryptography schemes which require more computational power. So the better option is to use key pre-distribution methods which are more secure and much faster.

Initially in WSN for security issues keys were distributed using a third trusted party called base stations (BS) proposed by Perrig et al. [1].Key distribution using this technique was not scalable and BS became a point of compromise. A KPS enables a SN to establish key without the use of BS. The simplest technique was to pre load the network with a single network wide key before deployment. But the disadvantage with this technique was that it was not scalable and comprise of a single node leads to compromise of all nodes in the network.

Inspired by the above idea Zhu. et. al [2] described pair wise key establishment scheme which relied on the assumption that no key will be compromised at the initial phase of sensor deployment and all sensors will erase their network wide key after initial phase. This scheme lacks scalability. The next step was using trivial pair-wise KPS but was limited in memory size and scalability. In the quest for security in KPS in SN Eschenauer and Gligor [3] proposed random key pre-distribution scheme where tens to hundreds of keys were uploaded to SN before deployment. This scheme addresses unnecessary storage problem, initially a large key pool P is generated K keys are drawn randomly from P and stored in SN. This technique does not guarantee that any two nodes will be able to communicate directly. In order to establish a pairwise key two SN only needs to identity the common keys that they may share. If direct communication is not possible then a path needs to be established between two nodes. This makes communication power consuming and slower. Chan et al [4] proposed a modification of the scheme of [3] they extended this idea by allowing two sensors to setup a pair wise key only when they share at least q common keys.

This increased resiliency against node capture. Resiliency means the robustness under adverse conditions. Di Pietro et al. [5] applied a geometric random model for key pre-distribution, which further enhances the performance of previous KPSs. Hwang and Kim [6] proposed a method to improve performance of previous schemes by trading-off a very small number of isolated nodes.

In deterministic key pre-distribution, keys are placed in sensor nodes in a predetermined manner .The pioneering work of Camtepe *et al.* in [7] propose a deterministic pair wise key pre-distribution scheme based on expander graphs and projective planes. Lee and Stinson [8] used transversal designs, Chakrabarty, Maitra and Roy [9] used merging blocks constructed from transversal designs.

Here we have consider a deterministic key predistribution scheme based on combinatorial designs. The design finds application where a large number of sensor nodes are to be deployed. Also by suitably choosing the parameters of the design, it can be ensured that every pair of nodes within communication range can communicate directly, thus making communication efficient and less error-prone. The main advantage of this scheme is that it is resilient to selective node capture attack and node fabrication attack.

A: Theory on combinatorial design

Combinatorial design theory [7] is interested in arranging elements of a finite set into subsets to satisfy certain properties. A *Balanced Incomplete Block Design (BIBD)* is one of such designs. A *BIBD* is an arrangement of *v* distinct objects into *b* blocks such that each block contains exactly *k* distinct objects, each object occurs in exactly *r* different blocks, and every pair of distinct objects occurs together in exactly λ blocks. The design can be expressed as (v, k, λ), or equivalently (v, b, r, k, λ), where: $\lambda (v - 1) = r (k - 1)$ and $b. k = v. r$

A BIBD is called Symmetric BIBD or Symmetric Design when b = v. A Symmetric Design has four properties:

1. Every block contains k = r elements

2. Every element occurs in r = k blocks

3. Every pair of elements occurs in λ blocks

4. Every pair of blocks intersects in λ elements.

B: Projective plane

A Finite Projective Plane [9] consists of a finite set P of points and a set of subsets of P, called lines. For an integer n where $n \geq 2$, there are exactly n^2+ n + 1 point, and exactly n^2 + n + 1 line. If we consider lines as blocks and points as objects, then a Finite Projective Plane of order n is a Symmetric Design with parameters (n^2 + n + 1, n+ 1, 1) Finite Projective Plane of order n has four properties [8]:

1. Given any two distinct points, there is exactly one line incident with both of them.
2. Given any two distinct lines, there is exactly one point incident with both of them.
3. Every point has n+1 line through it.
4. Every line contains n+1 point.

A projective plane is therefore a symmetric (n^2 + n + 1, n+1, 1) block design.

A finite projective plane [8] exists when the order n is a power of a prime, i.e., for n = p1. It is conjectured that these are the only possible projective planes, but proving this remains one of the most important unsolved problems in combinatorics. The smallest finite projective plane is of order n = 2, consists of the configuration known as the Fano plane. This Fano plane, is denoted PG (2, 2).

A: Traversal design

A transversal design TD (k, n) [$k \geq 2$ and $n \geq 1$] is a triple (X, G, B) such that the following properties are satisfied:

1. X is a set of k. n elements called points,

2. G is a partition of X into k subsets of size n called groups,
3. B is a set of k-subsets of X called blocks,
4. Any group and any block contain exactly one common point, and
5. Every pair of points from distinct groups is contained in exactly one block.

III. COMBINATORIAL AND TRAVERSAL DESIGN BASED KPS

Combinatorial design provides an appropriate balance of key content in various sensor nodes. Using this strategy maximum number of nodes pair can communicate directly using pair wise common key. Transversal Design is such a combinatorial Design which offers a deterministic nature of key distribution. A pattern of key ids is seen in this type of distribution of keys. Lee and Stinson[8] first time proposed the application of Transversal Design for Key Pre-Distribution in WSN .The result is less communication with a balance distribution in the establishment of secure communication. As the property of TD yields maximum one pair wise key among node pair, therefore compromise of single key or node leads to the compromise of all the nodes and links having the same key and yields breaking of link and leads to victim nodes. Hence in adverse condition the resiliency is less due to the presence of single common key in the network.The term resiliency [16] refers to sustainability of the SN when some of its node have been compromised by the attacker. It is the security measure of a particular design and is measured by the parameter L(s): fraction of communication links compromise on compromise of randomly selected s number of node. Chakrabarti, Roy, and Maitra[9] has modified this scheme and proposed that instead of immediately considering each blocks as sensor node after distribution of keys using Transversal Design, a number of blocks can be merged to form a node yielding the probability of more than one common key between a pair of nodes. Therefore, during any adverse condition the probability of link breaking is least between a node pair. However, it increases memory space requirement which can be accommodated [9]. Additionally this scheme increases the resiliency. Selection of blocks for merging to form a node is purely random. Due to this randomness, the content of blocks in a node is random i.e. unpredictable.

During common key establishment between node pair an amount of communication cost O (x) is introduced, if number of blocks in each node is n. We have modified this part and proposed a deterministic scheme. In which we follow a peculiar rule for merging blocks to form a node. Since block selection is deterministic a pattern of blocks is formed in each node. Consequently, to uncover blocks for a specific node ,no extra communication cost is incurred during key establishment phase. Simulation and determination of the various parameters is performed. For simulation C Language is used as the platform.

A. *ANALYSING THE APPROACH OF LEE AND STINSON'S SCHEME*

Lee and Stinson have used the concept of TD for key predistribution in WSN as a result there is a pattern in key ids in each node.On studying and simulating the scheme provided by Lee and Stinson using C Language certain important parameters were studied like L(s) : Fraction of links which have been compromised due to the compromise of s number of nodes. The results obtain use (v, b, r, k) based transversal design, where v = 3232, b = 10201, r = 101, k = 32.

Maximum number of connection could be 104050200.

Number of initial links detected = 16070800.

Average number of common keys between node pair = 1.000000.

Therefore connectivity of the design is 0.164482, i.e. almost 16%.

The average value of L(s) = 0.3476, i.e. almost 34% where s =40.

TABLE I

showing outcome of L(s) for Lee and Stinson's scheme

S=4	L(s)= 0.0381
S=8	L(s)=0.0754
S=12	L(s)=0.0115
S=16	L(s)=0.1480
S=20	L(s)=0.1790
S=24	L(s)=0.2125
S=28	L(s)=0.2560
S=32	L(s)=0.2720
S=36	L(s)=0.3018
S=40	L(s)=0.3476

B. *ANALYSING THE APPROACH OF CHAKRABARTI, ROY AND MAITRA'S SCHEME*

According to Lee and Stinson's scheme, any node pair can share 0 or 1 key[8]. Merging of nodes to form a new node increases the number of common keys between a pair. Chakrabarti, Roy, and Maitra provide one scheme where they randomly choose x number of blocks and merged to form a new node. They have chosen the blocks in such a way that there will be no inter node connectivity. As they have chosen randomly, for some cases they could not avoid the occurrence of inter node connectivity.

After forming a number of nodes they revised their scheme by introducing MOVE function to increase connectivity between different pairs in the network. MOVE increases the connectivity by exchanging blocks between maximum linked pair with zero linked pair.

On simulating this scheme the following parameters were studied L(S): Fraction of links get compromise on compromise of s number of nodes and Average number of common keys between a pair. The experiment result shows that the resiliency is much higher than the scheme provides by Lee and Stinson. But to store keys for each nodes need more storage. However, they have shown that consumed storage space is within the limits of a sensor node. The results obtained for various parameters are

- Maximum number of connection could be 3249974.
- Number of initial links detected is 3242103.
- Average number of common keys between a pair is 5.0195006.
- Therefore, connectivity of the design is 0.997589, i.e. almost 100%.
- The average value of L(s) = 0.0197, i.e. almost 2%, where s = 10 and equivalent to 40 blocks.

TABLE II

Outcome of L(s) for Chakrabarti, Ray and Matra's scheme

S=1	L(s)= 0.0010
S=2	L(s)= 0.0018
S=3	L(s)= 0.0028
S=4	L(s)= 0.0040
S=5	L(s)= 0.0062
S=6	L(s)= 0.0079
S=7	L(s)= 0.0100
S=8	L(s)= 0.129
S=9	L(s)= 0.0165
S=10	L(s)= 0.0197

C. *KEY DISTRIBUTION*

Chakrabarty, Roy and Maitra's scheme improves some parameters. However, it is observed that they have used randomly selected blocks to merge for forming node. Therefore, a particular node will be having no particular block id. On the time of shared key discovery between a pair of nodes, they have to broadcast all the block ids to the other nodes. This is yielding a communication cost O(x)[1], (x is the number of blocks to be merged to form a node) in addition to the request for communication which is O(1). Sending all the block ids cannot be avoided due to the randomness of the scheme. Observing this limitation, we propose a deterministic scheme for merging of block to form a node. The property of transversal design for arrangement of a set of elements into a number of subsets focuses the fact that the probability of repeating an element for consecutive blocks is much less. With such knowledge merging z ($1 \leq x \geq p$) number of blocks to form a node leads to much less probability for occurrence of intra-node repetition of same element. On the basis of this assumption, we considered x number of consecutive blocks for merging to form a node which helps to avoid any intra-node common key. This increases the connectivity of the entire network as well. Again as x number of consecutive blocks are merged, there is a pattern of block ids in a particular node. Therefore, to find out block ids for a particular node id there is no need to exchange block id which consumes an amount of communication effort. Nodes can themselves compute block ids of their counterparts. As this scheme is a deterministic, the communication cost is only O(1), that needs to request for communication by any of the node in the pair, which is much less than O(x). Note that the communication cost in this scheme is a constant value in comparison with scheme by Chakrabarti, Roy and Maitra where communication cost is a variable figure. On getting the node id of the requesting node, a node can easily determine the block ids of the other node which will take O(x) cost for computation time in average. After obtaining the block ids rest is to discover the shared keys, would take O(x^2log2^2r) time. Therefore, average computation cost for key establishment is O(x) + O(x^2log2^2r), i.e. O(x^2log2^2r), which is same as the scheme proposed by Chakrabarti, Roy, and Maitra. However, communication cost is much less which is one of the key requirements for these computational intensive devices. The algorithm for merging nodes is as follows:

```
/* Input: A block ids set
Output: A  node ids set
c=counter
t blocks= total number of blocks
u= number of blocks to be merged
k= number of keys stored by each block */
```

```
    Start of  blocks merging
    C = 0;
    For i = 0 to t blocks-1 do
        For j = 0 to u-1 do
            For s = 0 to k-1 do
            Start
                Noderepository[i][j*k+s].1 = block[c][s].1;
                /*Store  first part of the key id*/
                Noderepository[i][j*k+s].2= block[c][s].2;
                /*Store second part of the key id*/
            End For
        End For
        C++;
    End For
End of  blocks merging
```

The experimented result are obtained using the design (v = 3232, b = 10201, r = 101, k = 32) and x = 4, is given below.

The total number of nodes which has formed is 2550 each having 128 number of keys.

Average number of common keys between two nodes 5.520075.

Maximum number of connection could be 3249975.

Number of initial links detected 2955867.

Therefore, connectivity of the design is 0.909465, i.e. almost 91%.

The average value of L(s) = 0.1552, i.e. almost 16%, where s = 10 and equivalent to 40 blocks.

TABLE III

Result of E(s) for proposed scheme

S=1	E(s)= 0.0080
S=2	E(s)= 0.0178
S=3	E(s)= 0.0300
S=4	E(s)= 0.0443
S=5	E(s)= 0.0578
S=6	E(s)= 0.0800
S=7	E(s)= 0.0960
S=8	E(s)= 0.1125
S=9	E(s)= 0.1455
S=10	E(s)= 0.1557

D. KEY EXCHANGE

Any pair wishes to communicate with each other send a request message to its counterpart, which then including the sender discovers the common key between them. According to the proposed scheme, they don't need to send any extra information. They generate the block ids of the others using the above algorithm which needs the node id only of the other node. On discovering the block ids, they can compare all the blocks with their own blocks for finding any common key using the algorithm proposed by Lee and Stinson. After discovering the common key, if any, they can start communication using that key. In case of a pair which does not have any common key, they have to generate a key temporarily and need to exchange through one or more intermediate nodes. This process is referred as path key establishment.

IV. COMPUTATIONAL RESULTS

When we compare our scheme wee see that our scheme requires computation of O(1) to calculate shared keys. This is because our scheme broadcast only node identifier whereas other schemes have to share key identifiers. Though scheme proposed by Chakrabarti, Roy,and Maitra consumes a variable communication cost O(x), where x is the number of blocks to be merge to form a node. Again, though the scheme proposed by Lee and Stinson consumes O(1) as the communication cost, it still suffers from less Resiliency. Computation for key discovery is same i.e. O(x^2log2^2r) in this scheme as well as for Chakrabarti, Roy and Maitra and Lee & Stinson. The average number of common keys in each pair of node is almost 5 in this scheme as well as in [9], whereas scheme proposed by Lee and Stinson[8] has only 1 key. This is the main advantage of merging blocks to form node. Connectivity of this scheme is almost 91% which is almost same with the scheme proposed by [9]. Nevertheless, connectivity of the proposed scheme is much better than the scheme proposed by [8]. The resiliency is best in Chakrabarti, Roy and Maitra's scheme. Given the limited memory space and battery constraint our scheme shows reasonable resilience and better node connectivity especially when a large number of nodes have been compromised.

Node pair within a radio frequency range can communicate with each other, provided they have a common key between them. In probabilistic schemes this is not possible as nodes are chosen randomly. We see in our deterministic scheme any two nodes share at least one key. So there is full connectivity in the network.

V. SECURITY ISSUES IN WSN

WSN inherits security problems due to :-

(i) Wireless nature of communication,

(ii) Limitation of capability of individual sensor nodes,

(iii) Large size of the sensor networks,

(iv) Unknown and dynamic network topology, and

(v) Easy chance of physical attack.

This results a challenge to design any efficient key management scheme. We have tried to evaluate scheme in terms of its resilience against node collusion and selective node capture attack. If a node is directly involved in node collusion, e.g., because of being captured by an outside adversary or re-programmed to do harm to the whole network, we say the node is *compromised*. We have tried to answer the question that when certain nodes are compromised, how much could they influence the rest of the network if their key information has been retrieved and analyzed.

Our scheme is resilient to selective node capture attack , during this attack the attacker comprise those nodes whose keys have not already been compromised. Amid shared key discovery phase only node identifiers are broadcasted, key identifiers are not exchanged. Hence attacker at any stage cannot know which key identifiers are present in which node. Thus attacker cannot gain any information using this attack.

VI. CONCLUSION

On studying and comparing different schemes we find that merging of blocks to form node improves a number of parameters such as resiliency, average number of common key between a node pair, connectivity of the network etc. Only limitation is that the memory usage is significantly large, however this requirement is easily adaptable. Many existing schemes including [9] merge randomly therefore communication cost for key discovery is more and equivalent to O(x), which we have tried to reduce by proposing a deterministic scheme. This is one of the major requirements for a wireless sensor network.

Future direction of work will be to further study our scheme from other perspectives, such as computational overheads and investigate approaches to increase resilience by revising the merging strategy.

ACKNOWLEDGMENT

The authors would like to thank Mr. Shish Ahmad for his valuable comments and persistent efforts.

REFERENCE :

[1] Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar. SPINS: Security protocols for sensor networks. In Proc. of MOBICOM, 2001

[2] S. Zhu, S. Setia and S. Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In. Proc. of the ACM CCS Conference, pp. 62-72. 2003

[3] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proc. of the 9th ACM CCS conference, pp. 41 – 47, 2002

[4] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In Proc. of the IEEE Symposium on Security and Privacy, p. 197, 2003M.

[5] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi. Connectivity Properties of Secure Wireless Sensor Networks. In Proc. of the 2nd ACM SASN workshop, pp. 53 – 58. 2004.

[6] J. Hwang and Y. Kim. Revisiting random key predistribution schemes for wireless sensor networks. In Proc. Of the 2nd ACM SASN workshop, pp. 43 – 52. 2004

[7] .S. A. Camtepe and Bülent Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. In Proc. of Computer Security- ESORICS, Springer-Verlag, LNCS 3193, 2004, pp 293-308.

[8] J. Lee, and D. R. Stinson. Deterministic Key Predistribution Schemes for Distributed Sensor Networks. In Proc. 11th International Workshop, SAC 2004, pp. 294-307.

[9] D. Chakrabarti, S. Maitra, and B. K. Roy. A key predistribution scheme for wireless sensor networks: merging blocks in combinatorial design. Int. J. Inf. Sec., 5(2):105–114, 2006.

[10] David Sánchez Sánchez, Heribert Baldus. A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks .In Proc of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks,2005, IEEE.

[11] H. Shafiei, A. Mehdizadeh, A. Khonsari and M. Ould-Khaoua. A Combinatorial Approach for Key-Distribution in Wireless Sensor Networks. In Proc of the IEEE "GLOBECOM” 2008.

[12] SushmitaRuj, Jennifer Seberry and Bimal Roy. Key Predistribution Schemes Using Block Designs in Wireless Sensor Networks. In proc of

International Conference on Computational Science and Engineering, 2009.

[13] W. Stallings, Cryptography and Network Security- PrinCiples and Practices, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2003.

[14] Yingshu Li, My T. Thai, Weili Wu. Wireless Sensor Networks and Applications.Springer,2008

[15] Anupam Pattanayak, B. Majhi. Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited. Cryptology eprint Archive. Report 2009/131. 2009

[16] Anupam Pattnayak, "Deterministic Merging of Blocks in Combinatorial Design based Key Predistribution in Distributed Wireless Sensor Netwo," M. Eng. thesis, National Institute of Technology, Orissa, India, May, 2009.

[17] Subhasish Dhal, "Application of Traversal Design and Secure Path Key Establishment for Key Pre-Distribution in WSN", M.Eng. thesis, National Institute of Technology, Orissa, India, May, 2009 .