Key Predistribution for Heterogeneous Group of Sensor Nodes using Combinatorial Design

Monjul Saikia, Irani Acharjamayum and Anwar Hussain
Department of Computer Science and Engineering, North Eastern Regional Institute of Science and Technology
Nirjuli - 791109, Arunachal Pradesh, India; msk@nerist.ac.in, irani.acharj@gmail.com, ah@nerist.ac.in

Abstract

Objective: To design a key pre-distribution scheme for a heterogeneous group of sensor nodes with the help of combinatorial design for high resilience against node capture. Methods/Statistical analysis: Methodology used here is based on theory of balanced incomplete block design where a group of BIBD is used for each of the sensor groups and keys are distributed based on the orientation of these groups. Findings: Connectivity, Storage limitation and resilience are evaluated for the proposed scheme. Application/Improvements: Combinatorial design based scheme is proven to be most suitable method among various key pre-distribution schemes. Combinatorial design based scheme distributes keys to the sensor nodes according to Balanced Incomplete Block Design (BIBD). Use of combinatorial design improves the overall performance of the network.

Keywords: BIBD, Combinatorial Design, Key pre-distribution, Resilience, Wireless Sensor Network

1. Introduction

A Wireless Sensor Network is a network of sensor nodes with short communication range, low computation power, limited storage and limited power and are used in many real time applications. Symmetric key cryptography requires less computation power. If two nodes are to communicate securely, they need to store the same cryptographic key. Prior to deployment sensor nodes are loaded with secret keys and sensor node performs data encryption and forward the packets to next node. Due to high chance of attack in wireless sensor network security is major concern in such type of network. There are several types of attack in sensor network and a detail study can be found in. Various methodology have been developed for efficiently distribute keys among sensor nodes; a practical implementation of key predistribution schemes using combinatorial designs for distributed sensor networks is studied in. As coverage and connectivity are basic issues in such network; therefore special care needed to be taken. In some situations post deployment knowledge may be available and in some case no such information exists making key management scheme difficult to implement. Availability of prior deployment knowledge gives advantages in design of key predistribution schemes and a deterministic key management scheme for distributed sensor networks can be found in. Graphs are widely used to study the properties of key distribution scheme. Expander graphs are found to be having high connectivity among their vertices and key distribution using expander graph is studied in. Eschenauer and Gligor scheme is the first practical scheme for key distribution for wireless sensor network. In recent years many key distribution schemes have been proposed thereafter. In a combinatorial approach using balanced incomplete design technique can be found. Although pairwise keys

*Author for correspondence*
Key Predistribution for Heterogeneous Group of Sensor Nodes using Combinatorial Design

scheme requires a high storage it give perfect resilience in distributed sensor networks. The desirable metric for a good key distribution scheme is studied in [16][17]. Clustering of combinatorics for improving the performance over existing combinatorial design based key distribution is studied in [18].

2. Proposed Scheme

The proposed scheme is based on a special network scenario as depicted in Figure 1. Sensor nodes are deployed in nonuniform fashion. Therefore a traditional key distribution scheme is not suitable in this type of scenario. In our proposed scheme the sensor nodes are grouped and symmetric BIBD are formed. To form a link called bridge-link between these groups some common nodes are kept in each group. When any event detected at any of the sensor node the information passes through one or more groups to the base station via this bridge link.

In general, sensor nodes are assumed to be deployed into sensor network uniformly. Different group of sensor nodes are designed based on BIBD configuration and are deployed. For example, a group of nodes may be deployed to monitor a local area. There are some nodes in a group that share a common key with nodes of another group. The heterogeneous group of sensor nodes experience connectivity based on the availability of common key available among nodes of different groups. As nodes of heterogeneous groups are far from one another, their connectivity decreases i.e. secure communications occur within communication range.

In the network scenario given in figure 1. We have seen that sensor nodes that are in group I will have a secure communication with group II, IV, V because they are in communication range to each other. Group I will not be in communication range with group III, VI, VII, VIII, IX. Each group shares a common key with the other group that are in communication range.

3. KPS using Heterogeneous Group Sized BIBD

In the proposed combinatorial design group based approach total sensor nodes are divided into groups in such a way that each group forms an asymmetric BIBD. Randomly generated secret key is stored in an array called key pool. The size of the key pool is set to the total number of sensors in the network. Each heterogeneous group shares a common key among themselves. Algorithm flow chart is given in Figure 2.

Figure 1. Network Scenario with Different Network Size.

In general, sensor nodes are assumed to be deployed into sensor network uniformly. Different group of sensor nodes are designed based on BIBD configuration and are deployed. For example, a group of nodes may be deployed to monitor a local area. There are some nodes in a group that share a common key with nodes of another group. The heterogeneous group of sensor nodes experience connectivity based on the availability of common key available among nodes of different groups. As nodes of heterogeneous groups are far from one another, their connectivity decreases i.e. secure communications occur within communication range.

In the network scenario given in figure 1. We have seen that sensor nodes that are in group I will have a secure communication with group II, IV, V because they are in communication range to each other. Group I will not be in communication range with group III, VI, VII, VIII, IX. Each group shares a common key with the other group that are in communication range.

3. KPS using Heterogeneous Group Sized BIBD

In the proposed combinatorial design group based approach total sensor nodes are divided into groups in such a way that each group forms an asymmetric BIBD. Randomly generated secret key is stored in an array called key pool. The size of the key pool is set to the total number of sensors in the network. Each heterogeneous group shares a common key among themselves. Algorithm flow chart is given in Figure 2.

Algorithm 1:

| Step 1: | Input number of sensor in the network |
| Step 2: | Divide the group in such a way that each group makes a asymmetric BIBD |
| Step 3: | Keys are assigned to different BIBD groups based on key pool and different group of BIBDs choose a common key |
| Step 4: | Different group of BIBDs are designed based on BIBD configuration |
| Step 5: | The Key rings for different group of BIBDs are merged together |

Figure 2. Flow diagram for KPS using Heterogeneous Group Sized BIBD.
4. Implementation and Simulations

Balanced incomplete block design gives high connectivity among nodes. A BIBD (9,3,1) configuration is shown in Figure 3 where it is seen that 9 keys are distributed evenly among 12 nodes. As each sensor node contains exactly three keys therefore it can communicate to other three nodes securely. A group of two BIBD (7,3,1) sharing one common key between each set of keys is shown in Figure 4. An incidence graph shows how keys are shared by different nodes. Figure 5 shows an incidence graph for the two set of BIBD (13,4,1) configuration considering one key as common among the groups.

Figure 3. An Example of Combinatorial Design of a (9,3,1) Configuration.

Figure 4. Group of two BIBD (7,3,1) Sharing One Common Key between each Key Pool.

5. Experiments with Large Group of Network

Example: We have considered a network scenario of 9 heterogeneous BIBD groups i.e. (6,3,2) of 10 nodes, (7,3,1) of 7 nodes, (9,3,1) of 12 nodes, (15,3,1) of 35 nodes, (13,3,1) of 26 nodes, (10,3,2) of 30 nodes, (12,3,2) of 44 nodes, (11,3,3) of 55 nodes and (8,3,6) of 56 nodes. A key graph is drawn based on this network scenario where two sensor nodes will share a common key. Therefore, a total of 275 nodes are drawn.

In Figure 6 we can see that Group 1 are in communication range with Group 2,4,5 as this group shares a common key with the other 3 groups but not in communication range with other groups. A communication graph is drawn where two sensor nodes will communicate based on their communication range. In Figure 7 Node 1 can communicate with node 37. Similarly node 2 can communicate with node 164.

Based on the key graph and communication graph, we have drawn an intersection graph. In this intersection/secure communication graph of Figure 8 we have seen that node 1 is having secure communication with node 37 but node 2 are not in secure communication with node 164 because even though node 2 and node 164 are in communication range, they do not share a common key.
Key Predistribution for Heterogeneous Group of Sensor Nodes using Combinatorial Design

Figure 6. A Key Graph of a Network Scenario of 9 Heterogeneous Groups.

Figure 7. A Communication Graph of 275 Nodes.

Figure 8. An Intersection Graph/Secure Communication based on Key Graph and Communication Graph.

6. Analysis Based on Heterogeneous BIBDs

For secure communication packet need to be passed via several nodes. We perform a test to check how many hops are required for successful transmission. Table 1 gives the result for hop-count in various network size scenarios. Similarly a plot is shown in Figure 9. Direct link among nodes gives better connectivity for the network. Connectivity and average hop-count results were shown in Table 2 and an equivalent plot for connectivity is given in Figure 10. Resilience is the measure for resistance against attack. Figure 11 shows resilience against node capture in the network.

Table 1. Hop Count

| No. of nodes (N) | No. of groups | Key size | Hop-count |
|-----------------|---------------|----------|-----------|
|                 |               |          | 1 | 2 | 3 | 4 | 5 |
| 29              | 3             | 3        | 147 | 107 | 112 | 40 | 0 |
| 64              | 4             | 3        | 518 | 738 | 496 | 264 | 0 |
| 90              | 5             | 3        | 827 | 1754 | 1324 | 120 | 0 |
| 120             | 6             | 3        | 1260 | 2785 | 2639 | 456 | 0 |
| 164             | 7             | 3        | 1997 | 4534 | 5416 | 1419 | 0 |
| 219             | 8             | 3        | 3484 | 9185 | 10126 | 1076 | 0 |
| 275             | 9             | 3        | 5389 | 14185 | 15930 | 2171 | 0 |

Table 2. Key Connectivity and Average Hop

| No. of nodes (N) | No. of groups | Key size | Probability Pr | Average Hop |
|-----------------|---------------|----------|----------------|-------------|
| 29              | 3             | 3        | 0.3621         | 2.1108      |
| 64              | 4             | 3        | 0.2569         | 2.2510      |
| 90              | 5             | 3        | 0.2065         | 2.1840      |
| 120             | 6             | 3        | 0.1765         | 2.3209      |
| 164             | 7             | 3        | 0.1494         | 2.4681      |
| 219             | 8             | 3        | 0.1460         | 2.3684      |
| 275             | 9             | 3        | 0.1430         | 2.3950      |

Figure 9. A graph on Hop Count.
7. Conclusion

We propose a scheme based on heterogeneous group of BIBDs where sensor nodes are divided into some groups where each groups are a symmetric. As more number of groups of heterogeneous BIBDs is merged, connectivity to share keys among nodes becomes lesser as one block of a group is far from another block of different groups. Nodes in a sensor network will have a secure communication if they share a common key as well as if they are in communication range. Some analyses were done for hop count, probability, average hop, resilience etc. based on our proposed scheme.

8. References

1. Chen CY, Chao HC. A survey of key distribution in wireless sensor networks, Security and Communication Networks. 2011 July; 7(12):2495-2508. Crossref
2. Aysal TC, Barner KE. Sensor data cryptography in wireless sensor networks. IEEE Transactions on Information Forensics and Security. 2008; 3(2):273-89. Crossref
3. Giruka VC, Singhal M, Royalty J, Varanasi S. Security in wireless sensor networks. Wireless Communications and Mobile Computing. 2008; 8(1):1-24. Crossref
4. Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. IEEE Communications Surveys and Tutorials. 2006; 8(2):2-23. Crossref
5. Lee J, Stinson DR. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. ACM Transactions on Information and System Security (TISSEC). 2008; 11(2):5:1-5:35.
6. Camtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transaction on Networking. 2007; 15(2):346-58. Crossref
7. Zhu C, Zheng C, Shu L, Han G. A survey on coverage and connectivity issues in wireless sensor networks, Journal of Network and Computer Applications. 2012 March; 35(2):619-32. Crossref
8. Yu Z, Guan Y. A key management scheme using deployment knowledge for wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2008; 19(10):1411-25. Crossref
9. Lee J, Stinson D. Deterministic key predistribution schemes for distributed sensor networks. SAC, LNCS 3357. 2004; p. 294-307. Crossref
10. Linial N, Wigderson A. Israel: Hebrew University: Lecture Notes. Expander graphs and their applications. 2003 January; p. 1-81.
11. Hoory S, Linial N, Wigderson A. Expander graphs and their applications. Bulletin of the American Mathematical Society. 2006 August; 43(4):439-561. Crossref
12. Kundur D, Luh W, Okarafor UN, Zourntos T. Security and privacy for distributed multimedia sensor networks. Proceedings of the IEEE. 2008; 96(1):112-30. Crossref
13. Eschenauer L, Gligor V. A key-management scheme for distributed sensor networks. The Proceedings of the Annual ACM Computer and Communications Security (CCS). 2002; p. 41-47. Crossref
14. Shafiei H, Mehdizadeh A, Khonsari A, Khaoua MO. A combinatorial approach for key-distribution in wireless sensor networks. IEEE Global Telecommunications Conference IEEE. 2008; p. 1-5. Crossref
15. Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS 2003). 2003; p. 52-61. Crossref

16. Kendall M, Martin K. On the Role of Expander Graphs in Key Predistribution Schemes for Wireless Sensor Networks. Research in Cryptology: 4th Western European Workshop, WEWoRC. 2011; p. 62-82.

17. Saikia M, Acharjamayum I, Hussain Md. A review on desirable measures for good Key Pre-distribution Scheme in wireless sensor network. International Conference (ICGCIoT). 2015; p.129-34. Crossref

18. Saikia M, Hussain Md. Improving the performance of Key Pre-distribution Scheme in Sensor Network using Clustering of Combinatorics. IEEE International Conference ICCCA. 2016; 10(9):1-6. Crossref