International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

An Analysis of Location Independent Key Pre distribution Schemes for Wireless Sensor Network

Monjul Saikia[1] and Md. A Hussain[2]

North Eastern Regional Institute of Science and Technology
Nirjuli-791109, Arunachal Pradesh, India

Abstract - Security in wireless sensor network can be achieve by symmetric key encryption with minimum cost. The symmetric key encryption technique requires agreeing on one common secret key among two parties. Therefore it is essential to have a common key among sensor nodes. The key predistribution solves the purpose by assigning secret keys among sensor nodes. Due to high chance of physical capture of sensor nodes and lack of prior information of configuration after deployment makes key predistribution more challenging. Several key predistribution schemes have been proposed. In this paper we try to discuss the basics of key predistribution scheme and analyze different schemes proposed by researchers, along with some experimental results. Also we have discussed the properties need to be fulfilled for an efficient scheme.

Keywords: Sensor Network; KPS; Security; Connectivity; Resilience.

1. INTRODUCTION

The main objective of a WSN is to collect sensitive information from the physical world where human cannot survive. These networks of tiny devices can operate in any locations where wired network is possible. The wireless sensor networks are deployed to sense, process and distribute information of some target physical environments. Deployment strategy may dependent to the location of each sensor node or may be independent of the location. The deployment environment can be a controlled one or an uncontrolled. Security of sensor nodes is highly important when deployed in an uncontrolled environment as there may be high chance of node compromise by adversary.

2. KEY DISTRIBUTION SCHEMES FOUNDATIONS

The fundamental model for security for sensor network with Key Predistribution Schemes can be devided into four phases, namely

i) Key Predistribution phase
ii) Sensor Deployment phase
iii) Shared Key Discovery phase
iv) Pairwise Key Establishment phase

i) Key Predistribution phase: A centralized server is responsible for determining the keys to be preloaded into the sensor nodes. It first generates a large set of keys called key pool. From this set, keys are loaded to the sensor nodes based on some algorithm such that with minimum number of keys high connectivity can be achieved. With the set of keys loaded into the sensor nodes forms a key chain or key ring.

ii) Sensor Deployment phase: After keys are loaded to the sensor nodes these nodes are ready to deploy in target area. Number of sensors within the communication range *(n')* is usually much smaller than the deployed nodes *(N)*. Therefore, it is obvious that storing a common key which is not in communication range may lead to unnecessary storage for the sensor nodes.

iii) Shared Key Discovery phase: If a sensor node wants to communicate to other sensor node within its communication range, then they look up into their key chain for the preloaded common secret key. This phase is called a shared key discovery phase.

iv) Pair-wise Key Establishment phase: After discovering a shared key secure communication can progress with successive symmetric key encryption process. On the other hand if a node does have a pair-wise key with a destination node, the sensor node has to find a *key path* to setup their pair-wise key for secure communication with some routing mechanism.

3. EXISTING KEY DISTRIBUTION SCHEMES

Here we will discuss in details the various key predistribution schemes. Starting with a random key predistribution scheme proposed by Eschenauer and Gligor in 2002 a numerous number of schemes have been invented there after. Some of the location independent KPS is listed in the table-1. The schemes are said to be location independent in the sense that no prior information is available regarding location/coordinates of the sensor nodes prior to deployment.

Table 1: Location Independent KPS

Sl	*Schemes*	*Year*	*Authors*
1	Single key scheme	-	-
2	Fully pairwise key scheme	-	-
3	Blom's method	1984	R Blom
4	Method by Blundo et al.	1993	C. Blundo et. al.
5	Eschenauer and Gligor's method	2002	L Eschenauer et. al.
6	q-Composite scheme	2003	H Chan et. al.
7	Multiple space key pre-distribution scheme	2003	Du W et. al.
8	Polynomial pool-based key pre-distribution scheme	2003	Liu D et. al.
9	Pseudo-random function-based key pre-distribution scheme	2004	Pietro RD et. al.
10	Combinatorial design-based key pre-distribution scheme (BIBD-based method)	2004	S. A. Camtepe
11	PIKE: Peer Intermediaries for Key Establishment	2005	H Chan et. al.
12	Expander graph-based key pre-distribution scheme	2006	S. A. Camtepe et. al.
13	Combinatorial design-based key pre-distribution scheme (hybrid design-based method)	2007	S. A. Camtepe et. al.
14	Random assignment set selection key pre-distribution scheme	2007	Tague P et. al.
15	BABEL key pre-distribution scheme	2007	Deng J et. al.
16	Random perturbation-based key establishment scheme	2007	Zhang W et. al.
17	Non-interactive key establishment scheme	2010	Yu C-M et. al.

4. DISCUSSIONS AND EXPERIMENTS

Here, some of these schemes have been discussed with experimental results:

1. Single Key Predistribution Scheme [2]: It is a straight forward method of key predistribution scheme, where a single key is shared among all nodes. Therefore it is highly vulnerable to attacked. One node compromise will affect the entire network.

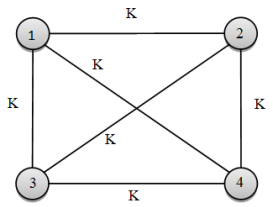

Fig -1: Single Key Predistribution

Figure 1 shows the comm. graph in Single Key Predistribution Scheme. In this approach a common key K is preloaded in all the sensor nodes. Any node can use the key to transmit information using the same secret key *K,* which can be shown using an *incidence graph*, as shown in figure 2.

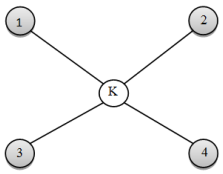

Fig - 2: Incidence Graph- Single Key Predistribution

Although the scheme is highly resource efficient, it has lowest resilience and may collapsed the network on single node capture.

2. Fully Pairwise Key Predistribution Scheme [2,11]: In fully pairwise key predistribution scheme, for each sensor node *n-1* keys are preloaded. Each key corresponds to key share with other nodes.

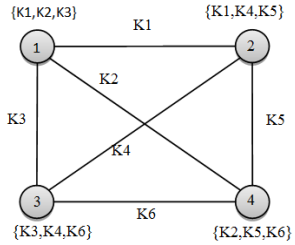

Fig - 3: Fully Pairwise Key Predistribution Scheme

Figure 3, shows key share among nodes and in figure 4 the respective incidence graph is shown.

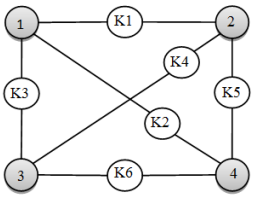

Fig - 4: Incidence Graph- Fully Pairwise Key Predistribution Scheme

3. Eschenauer and Gligor's Scheme [1, 2]: This is a type of randomly allocate key from a large set of keys to form the key chain.

For example, let total number of sensor nodes be N=10 and key pool set P = {1,2,3,4,5,6,7,8,9,10} and the key chain size is k = 3. The formation of key chain after random distribution can be seen as given in table -2.

Table 2: Key Ring

Node	Key Ring	Node	Key Ring
N#1	{1,7,7}	*N#6*	{1,2,9}
N#2	{2,2,5}	*N#7*	{9,4,9}
N#3	{2,5,5}	*N#8*	{10,5,6}
N#4	{1,1,10}	*N#9*	{8,5,6}
N#5	{8,8,8}	*N#10*	{3,4,3}

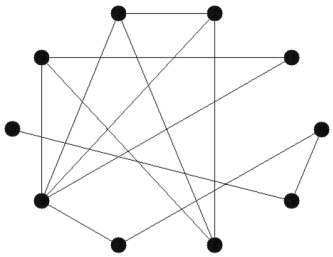

Fig -5: Key graph in the with 10 nodes

Table 3: Results: a) Number of nodes (n) b) Key Ring size (k) c) Probability P_{r_1} d) Maximum Hop e) Average Hop f) $fail_1$ g) $fail_2$

(a)	(b)	(c)	(d)	(e)	(f)	(g)
10	3	1.0000	1	1.000	0.300	0.510
20	3	0.7421	2	1.258	0.150	0.277
30	4	0.9211	2	1.079	0.200	0.360
40	6	0.9247	2	1.025	0.120	0.225
50	10	0.9394	2	1.001	0.100	0.190
60	10	0.9497	2	1.000	0.010	0.019
70	20	0.9954	3	1.000	0.020	0.039

4. Combinatorial design based Key Predistribution Scheme [9]: Combinatorial design technique can be used for key distribution for their special property of symmetricity.

For example a BIBD (7,7,3,3,1) is type of symmetric design which indicates, $v = 7$ elements, $b = 7$ blocks, each block contains $r = 3$ elements and each elements in $k = 3$ blocks and each pair of blocks has $\lambda = 1$ common elements. This arrangement can be used for key distribution.

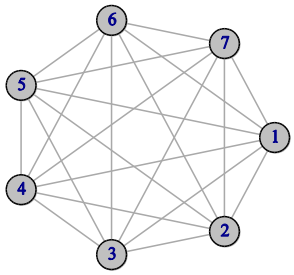

Fig -6: (a) BIBD (7,3,1) Key graph

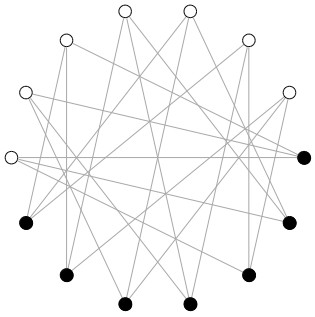

Fig -6: (b) Incidence graph

5. Expander Graph based Key Predistribution Scheme: A Ramanujan graph $X^{s,t}$ is a graph with number of nodes $n = t + 1$ and the degree of the graph k= $s + 1$, where both s and t are prime congruent to $1 mod 4$. Figure 7 shows a key graph with the use of $X^{5,19}$ Ramanujan graph where self loops and multiple edeges are deleted.

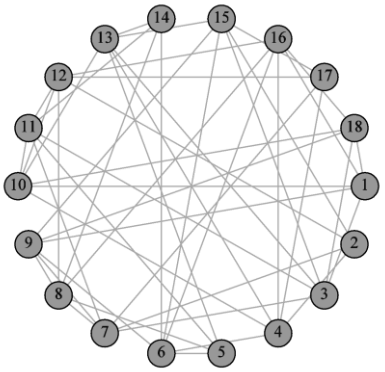

Fig -7: Expander graph X $^{5, 17}$

5. ANALYSIS OF THE KPS

A. Connectivity:

Figure 8 shows plot of connectivity probability that is having a common key between any two randomly chosen nodes in various schemes discussed above using a key chain of size 3. As the network size increases the probability of immediate key share decreases in every scheme.

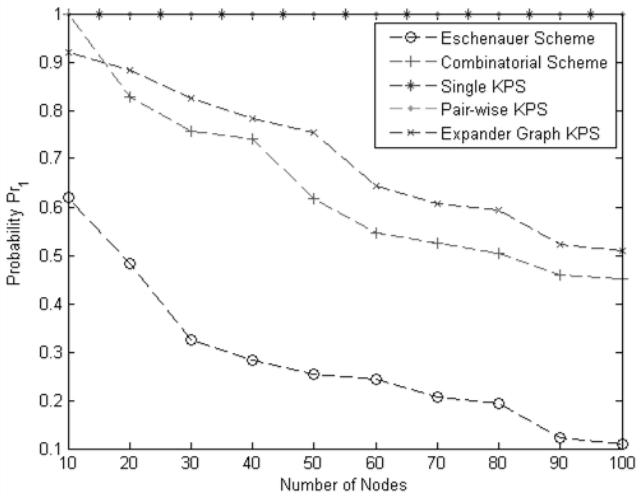

Fig -8: Plot of Probability Pr_1 or Connectivity

B. Resilience:

It is essential to minimise the number of nodes affected on any node compromised. The fraction of the network that can survive is called the resilience of the network and a plot for the same is shown in figure 9. As network size increases the probability of nodes affected decreases in case in all the approaches and therefore resilience of the network increases.

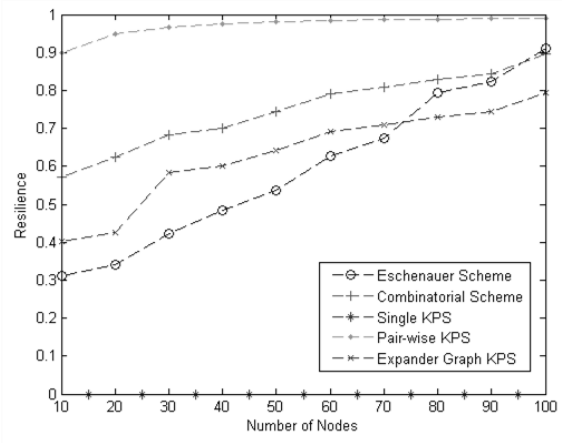

Fig -9: Plot of Resilience

5. Conclusion

The paper gives an overview of key predistribution scheme and comparison of various approaches. Combinatorial designed based KPS is found to be highly efficient compared the other scheme when connectivity is concerned. Single key distribution scheme is highly storage efficient but it has lowest resilience. Storage requirement in pair-wise KPS is very high but it gives perfect resilience to the network. Comparison of these method were shown in graph.

REFERENCES

[1] Eschenauer L, Gligor V. A key-management scheme for distributed sensor networks. In Proceedings of the Annual ACM Computer and Communications Security (CCS), 2002.

[2] Chi-Yuan Chen and Han-Chieh Chao "A survey of key distribution in wireless sensor networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; 7:2495–2508published online 13 July 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.354.

[3] ShlomoHoory, Nathan Linial, and AviWigderson. Expander graphs and their applications. In Bulletin of the American Mathematical Society, 43(04):439{562, August 2006.

[4] Michelle Kendall and Keith Martin "On the Role of Expander Graphs in Key Predistribution Schemes for Wireless Sensor Networks"Information Security Group, Royal Holloway,University of London, Egham, Surrey, TW20 0EX, UK.

[5] Friedrich Wilhelm Levi. Finite Geometrical Systems: six public lectures delivered in February, 1940, at theUniversity of Calcutta. The University of Calcutta, 1942.

[6] Coxeter, H. S. M. "Self-Dual Configurations and Regular Graphs." Bull. Amer. Math. Soc. 56, 413-455, 1950.

[7] Godsil, C. and Royle, G. "Incidence Graphs." §5.1 in Algebraic Graph Theory. New York: Springer-Verlag, pp. 78-79, 2001.

[8] Fan R. K. Chung. Spectral Graph Theory. American Mathematical Society, California State University, Fresno, 1994.

[9] Çamtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transaction on Networking 2007; 15(2): 346–358.

[10] Blom R. An optimal class of symmetric key generation systems. In Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 1984.

[11] Du W, Deng J, Han YS, Varshney P. A pairwise key pre-distriubtion scheme for wireless sensor networks. In Proceedings of the Annual ACM Computer and Communications Security (CCS), 2003.

[12] Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-secure key distribution for dynamic conferences. In Proceedings of the 29th International Cryptology Conference (CRYPTO), 1993.

[13] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In Proceedings of IEEE Symposium on Security and Privacy (S&P), 2003

[14] Seyit Ahmet Camtepe, Bulent Yener, and Moti Yung. Expander Graph Based Key Distribution Mechanisms in Wireless Sensor Networks. In ICC 06, IEEE International Conference on Communications, pages 2262-2267, 2006.

[15] A. Lubotzky, R. Phillips, and P. Sarnak, “Ramanujan graphs,” Combinatorica, vol. 8, no. 3.

BIOGRAPHY

Mr. Monjul Saikia has been serving as an Assistant Professor in the department of Computer Science and Engineering, NERIST (North Eastern Regional Institute of Science and Technology) a Deemed University under the Govt. of India, in Arunachal Pradesh, India since July 2007. He has completed his Masters of Technology from the Department Computer Science and Engineering, NERIST in the year of 2011. He did his Bachelor of Engineering from Jorhat Engineering College, Jorhat Assam, in 2005 in Computer Science discipline. Currently he is pursuing PhD in the Department of Electronics and Communication Engineering, NERIST under the guidance of Prof. Md. Anwar Hussain. His major research interests include Information Security, Cryptography, Image and Video Processing, VLSI etc. He is a member of professional societies like IEEE, CSI (India), IEI (India) and ISTE (India).

Prof. Md. Anwar Hussain, Professor in the Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology. He has done Ph.D (in Engineering) , Optical Fiber Commun

-cation from Jadavpur University, Kolkota in 2002 (Feb.). His area of research includes: High data rate wireless communication & networks, Routing & scheduling in Multi-hop wireless networks, Key distribution in Sensor networks, Multimedia data encryption & security, Mobile computing security, Time-series data modelling and prediction, Low power VLSI design, Climate change & modelling, Networks-on-Chip.