Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on key Generation and Pre-distribution Technique in wireless Sensor Network

Aher Nisha N.
M.E. (computer)
PVPIT, Pune, India.

Prof. N. D. Kale.
Asst. Prof.in Dept of Computer Engg.
PVPIT, Pune, India.

Abstract: ***Nowadays wireless sensor networks (WSN) have gained more popularity due to its various application areas. So security mechanism should be effective for it. As they are widely used in civilian as well as military applications the pre -distribution mechanism is also very effective. Key pre-distribution is kind of challenging task in WSN because neighbors of a node are unknown to each other after deployment. For communication to be secure there must be a common secure key or a common secure key path must be present. There are various techniques for the key distribution is present. In this survey paper we have reviewed these techniques along with the advantages and disadvantages of them.***

I. Introduction

Wireless sensor network is most widely used in the various fields like medical applications, military applications, wildlife tracking, weather checking applications, traffic control applications. Sensor nodes are used to detect enemy intrusion in battle field as well as they can be used to measure various environmental variables so in order to keep the information secret it is important to establish a secure communication between the sensor nodes. For secure communication between two sensor nodes a secret key is present. The sensor nodes have low processing power, less memory capacity and less battery life. Along with these constraints in WSN the wireless nature of network, unknown topology of network, and lack of fixed infrastructure use the cryptographic technique in wireless sensor network is some kind difficult task. We have to check the resource availability at each node. If we use symmetric key cryptography means if there are N nodes then there should be (N-1) keys in the network. This criteria should be maintained in whole network. In case if the value of N is large then the memory space is wasted to store the large key value.so it should not the memory efficient. If we use the public key cryptography system, it needs huge computation power but the sensor have less processing power so the public key cryptography system is not efficient in the WSN. Key pre-distribution technique is the most promising technique in wireless sensor network. In this key pre-distribution technique, each sensor node is assign set of keys from the large pool of keys before deployment, so that after deployment the two nodes which establish a communication to each other have at least one common key between them that key may be of higher probability and hence the secure communication will establish in the two nodes of WSN.

There are many key pre-distribution techniques developed nowadays. In this paper I have summarized some of them for wireless sensor network. In section 2 I have summarized some key pre-distribution techniques. In section 3 I have concluded paper and in section 4 some references I have used for this paper.

II. Key pre-distribution techniques

There are various key distribution techniques are implemented. Before going to these techniques here is some introduction about the key pre-distribution.

Key pre-distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position. Basically a key pre-distribution scheme has 3 phases:

1. Key distribution
2. Shared key discovery
3. Path-key establishment

During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key pre-distribution scheme used in creation. All the key pre-distribution schemes can be divided into three according to the way of choosing keys for each node from the key pool. They are :

1) Probabilistic: Keys are drawn randomly and placed into the sensors.
2) Deterministic: Keys are drawn based on some definite pattern.
3) Hybrid: Makes use of both the above techniques.

To discuss about the schemes in a better way we have divided them into some parts and we have discussed below about each part in respective subsections.

A. Basic schemes

First we will discuss about two basic schemes which though were not meant for WSN, have been used in context of WSN. Those two schemes are Blom's scheme and Blundo et al's scheme. Blom [1] proposed a key pre-distribution scheme that allows any two nodes of a group to find a pairwise key. The security parameter of the scheme is c, i.e., as long as no more than c nodes are compromised, and the network is perfectly secure. They have used one public matrix and one secret symmetric matrix to construct this scheme. Each node will have the share of those matrixes such that any two nodes can calculate a common key between them without knowing each other's secret matrix share. The problem with this scheme is that if more than c numbers of nodes are compromised, the whole network will be compromised.

In the scheme proposed by Blundo, Santis, Herzberg, Kutten, Vaccaro, Yung [2], they used a symmetric bivariate polynomial over some finite field GF (q). Symmetric bivariate polynomial is a polynomial P(x, y) E GF (q)[x, y] with the property that P (i, j) = P (j, i) for all i; j E GF (q). A node with ID Ui stores a share in P, which is a univariate polynomial fi(y) = P (i, y). In order to communicate with node Uj, it computes the common key Kij = fi (j) = fj (i); this process enables any two nodes to share a common key. If P has degree t, then each share consists of a degree t univariate polynomial; each node must then store the t + 1 coefficients of this polynomial. So, each node requires space for storing t+ 1 keys. If an adversary captures s nodes, where s < t, then it cannot get any information about keys established between uncompromised nodes. However, if it captures t + 1 or more nodes then all the keys of the network can be captured.

Eschenauer and Gligor first proposed a random key pre-distribution scheme [7] for WSN. They divided the key pre-distribution mechanism into three steps: key pre-distribution, shared-key discovery and path-key establishment. In this approach, a key ring for a node containing some fixed number of keys are chosen randomly without replacement from a key pool of large number of keys. Each node is assigned a key ring. The key identifiers of a key ring and corresponding sensor identifiers are stored in a trusted controller node. Now a shared key may not exist between two nodes. In that case, if there exists a path of nodes sharing keys pairwise between those two nodes, they may communicate via that path. They have also shown that for a network of 10000 nodes, a key ring containing 250 keys is enough for almost full connectivity. When sensor nodes are compromised, key revocation is needed. For this a controller node broadcasts a revocation message containing the list of identifiers of keys which have been compromised and all the nodes after getting the message removes the compromised keys from the key ring. The main advantages of this scheme are that the scheme is flexible, scalable, efficient and easy to implement. However, the main disadvantages are that it cannot be used in regions which are prone to massive node capture attack.

Chan Perrig and Song [3] modified Eschenauer and Gligor scheme. According to their q- composite scheme two nodes must share at-least q number of keys to have a secure path between them. The path key will be formed by the hash of all the common keys. Though for small number of node capture, resiliency was improved, the resiliency was affected drastically
as number of captured nodes increases.

B. Random pairwise scheme

In the random pairwise scheme, proposed by Chan, Perrig and Song [3], they have proposed that in a network of size N and minimum connection probability of two nodes is p, each node will store k number of keys where k = N * p. The key pre-distribution, shared key discovery and path key establishment is done as in [7]. Node revocations for compromised nodes are done by voting of all the nodes in the network with a suitable threshold parameter. But the disadvantage of this scheme is that it is not scalable and choosing the threshold value for node revocation is very important as it can lead to other problems.

The pairwise key scheme of Liu and Ning [9] is based on the polynomial pool based key pre-distribution by Blundo et al [2]. They have shown the calculation for the probability that two nodes share a common key. They have also shown the probability that a key is compromised. Later it was extended in [13] where they modified the scheme into a hypercube based key pre-distribution.

C. Grid-based key pre-distribution schemes

Chan & ferriq [3] was first to propose grid based key pre-distribution key ,in this scheme they placed the nodes of network in square grid this scheme is known as PIKE scheme. In this each node will have a secret pairwise key with the nodes which lie in the same row or same column the disadvantage of this scheme is high communication overhead.

In [19] , Kalidindi et. al. modified the PIKE scheme. They placed the nodes as well as the keys in a grid and divide the grid into some sub-grids. A node will have all the keys in its key chain which lie in its same row or column and which are in its same or neighboring sub-grids. Key needed to store in each node can be much less than [7] if number of subgrids are more. It will increase the resiliency but decrease the connectivity. The reverse will happen if number of sub-grids is lesser. Nodes belonging to the same sub-grid and in same row or same column share more keys. But they are not allowed to use all the common keys because capturing of one node of a row or column will reveal all the keys of that row and column.

Abedelaziz Mohaisen, YoungJae Maeng and DaeHun Nyang [15] proposed a 3-dimensional grid based key pre-distribution. According to their scheme, If the network size is N, then all the node of the network is arranged in a m * m *

m grid where m = N^1/3. Now 3N^1/3 symmetric polynomials will be distributed among the nodes in such a way that all the nodes with the same axis value owns the share of same corresponding polynomial. Two nodes having same axis value will share common polynomial and key can be prepared from that. The probability of connectivity is 3/m+1. Though the communication overhead is low in this scheme than the previous schemes, the resiliency is very poor.

Huang, Mehta, Medhi and Harn [8] proposed a grid-group based key pre-distribution scheme. This scheme is perfectly secure to random node capture as well as perfectly secure to selective node capture. Their approach is similar to Du et al using multiple space Blom's scheme.

Simonova, Ling and Wang discuss a homogeneous scheme in [16]. According to them, each grid in the network will have a disjoint key pool. Nodes from the same grid will communicate via this. There will another key pool called deployment key pool which will be constructed from neighboring key pools. Nodes from two neighboring grid can communicate via keys of the deployment key pool.

D. Group based key pre-distribution

Liu, Ning and Du observed that sensor nodes in the same group are usually close to each other and they proposed a group based key pre-distribution scheme without using deployment knowledge [12], [11]. They divide the nodes of a network into groups and then form cross groups taking exactly one sensor node from each group such that there will not be any common node between any two cross groups. They presented two instantiations of pre-distribution. In the first one, hash functions were used. Two nodes will share a common key if they are in same group or in same cross group. If the number of node in the network is N and they are divided into
n groups each containing m nodes, N = n * m and each node need to store m + n / 2 keys. In the second method, they used symmetric bivariate polynomials and assign a unique polynomial to each group and cross group. Every node will have share of the polynomials corresponding to their groups and cross groups. The advantages of this scheme are that it does not do not use deployment knowledge and give resiliency and connectivity similar to the deployment knowledge based schemes. The polynomial based schemes can be made scalable.
The framework can be used to improve any existing pre-distribution schemes.

The disadvantage of this scheme is that the probability of secure communication between cross-group neighbors is very less. The scheme is not suitable for networks which have small group size.

To overcome the problems of Liu et al's scheme [11], Martin Paterson and Stinson [13] proposed a group based design using resolvable transversal designs. To increase the cross group connectivity, they proposed that each node is contained in m cross groups rather than one. Though some additional storage is required. They did not give any algorithm for the construction of such designs.

E. Key pre-distribution using Deployment knowledge

Location dependent key pre-distribution were first proposed by Liu and Ning [10]. They proposed two schemes taking advantage of the location information. According to them, as sensors are deployed in group, nodes in the same group have higher probability of being deployed close to each other. In their first scheme, i.e., closest pairwise scheme, they proposed that a node will have pairwise keys with the nodes which are close to each other. In the second scheme, they used polynomial based key pre-distribution like [2]. They divide the nodes in groups and assign each group a unique symmetric bivariate polynomial. A node will have share of polynomials of its own group as well as its four neighbor groups. Common key can be calculated between the nodes who are in the same or neighboring groups like [2].

Du et al proposed a key pre-distribution scheme using deployment knowledge in [4]. This scheme is based on grid group deployment scheme where sensor nodes are deployed in groups such that a group of sensors are deployed in a single deployment point. The deployment model was given in [6]. They used Blom's scheme [1] for key pre-distribution in [5]. But they modified it into multiple key spaces. In their deployment scheme, If two groups are neighbors, then there will be some amount of overlap between their respective key pools, i.e., they will have some number of common keys in their key pools. But if two groups are far away from each other, then the overlap will decrease and it can be even zero. This scheme uses less number of keys and gives higher connectivity and better resiliency. But the complexity of this scheme is its main disadvantage.

F. Based Q-composite distribution

In [17], Shruthi p and M.B. Nirmala proposed a scheme which is secure modification of blom's scheme. In the master key scheme, any master key is the base to which the security mechanism holds for. They propose a modification to the existing scheme where q common keys (q > 1) are needed, instead of just one. By increasing the amount of key overlap required for key-setup, we increase the resilience of the network against node capture.
The proposed method use here is modified Bloom's scheme [1]. The reason that we don't prefer bloom's is that in the original Bloom's scheme all the computations involved in generating the keys are based on Vandermonde matrix which is a public matrix (P) and known to even the adversaries. Here, to make sure that any t+1 columns of P are linearly independent; all the values in the matrix are chosen to be distinct

G. Based on matrix based memory efficient technique

Blom [1] used the generator matrix of maximum distance separable (MDS) codes and a symmetric matrix to generate key spaces for all sensor nodes in network. In [18] Khan, Gabidulin, Honary, Ahmed uses the generator matrix of MRD (maximum rank distance) instead of MDS codes. The idea of this scheme is to store information at each node

before its deployment, so that it should be able to generate a common link key wherever it is required, with minimum information exchange. This scheme requires only one message to be transmitted by each side to generate a common link key. As all keys in the system are generated using a small amount of information, so dependencies among the key may exist. The advantages of this scheme are 1) it is efficient in terms of memory consumption. 2) in case of scalability, this scheme is capable of generating keys for the new nodes without changing any information on the previously deployed node. 3) This scheme provides minimum communication overhead to setup a pairwise key and this is without compromising on authenticity, integrity, and confidentiality of security.

III. Conclusion

Probabilistic schemes are scalable as we have seen and the deterministic schemes are simpler in case of computation and are better in connectivity and resiliency as they have great certainty. Schemes based on schemes of Blundo or Blom have a good value between security and storage. Resiliency of the schemes which use combinational structures is good. Many schemes are found after key management has been researched by various researches over the time. All the schemes have their own advantages and disadvantages as we discussed. Criteria for the scheme implementation should satisfy both requirements and resources. In case of military services security takes highest priority than in civilian application development of sensor network. Even though good amount of work is done in this area there are lots of opportunities which can improve sensor network utilization.

References

[1] Rolf Blom. An *optimal class of symmetric key generation systems*. In EUROCRYPT, pages 335–338, 1984.

[2] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung. *Perfectly-secure key distribution for dynamic conferences. In CRYPTO*, pages 471–486, 1992.

[3] Haowen Chan, Adrian Perrig, and Dawn Song. *Random key pre-distribution schemes for sensor networks*. In SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197, Washington, DC, USA, 2003. IEEE Computer Society.

[4] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney. *A key management scheme for wireless sensor networks using deployment knowledge.* In INFOCOM, 2004.

[5] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. *A pairwise key pre-distribution scheme for wireless sensor networks. In ACM Conference on Computer and Communications Security*, pages 42–51, 2003.

[6] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. *A key pre-distribution scheme for sensor networks using deployment knowledge.* IEEE Trans. Dependable Sec. Comput., 3(1):62–77, 2006.

[7] Laurent Eschenauer and Virgil D. Gligor. *A key-management scheme for distributed sensor networks.* In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47, New York, NY, USA, 2002. ACM.

[8] Dijiang Huang, Manish Mehta 0003, Deep Medhi, and Lein Harn.*Location-aware key management scheme for wireless sensor networks*.In SASN, pages 29–42, 2004.

[9] Donggang Liu and Peng Ning. *Establishing pairwise keys in distributed sensor networks*. In ACM Conference on Computer and Communications Security, pages 52–61, 2003.

[10] Donggang Liu and Peng Ning. *Location-based pairwise key establishments for static sensor networks*. In SASN, pages 72–82, 2003.

[11] Donggang Liu, Peng Ning, and Wenliang Du. *Group-based key pre-distribution in wireless sensor networks*. In Workshop on Wireless Security, pages 11–20, 2005.

[12] Donggang Liu, Peng Ning, and Wenliang Du. *Group-based key pre-distribution for wireless sensor networks*. TOSN, 4(2), 2008.

[13] Donggang Liu, Peng Ning, and Rongfang Li. *Establishing pairwise keys in distributed sensor networks*. ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005.

[14] Keith M. Martin, Maura B. Paterson, and Douglas R. Stinson. *Key pre-distribution for homogeneous wireless sensor networks with group deployment of nodes*, 2008.

[15] Abedelaziz Mohaisen, YoungJae Maeng, and DaeHun Nyang. *On gridbased key pre-distribution: Toward a better connectivity in wireless sensor network.* In PAKDD Workshops, pages 527–537, 2007.

[16] Katerina Simonova, Alan C. H. Ling, and Xiaoyang Sean Wang. *Location-aware key pre-distribution scheme for wide area wireless sensor networks.* In SASN, pages 157–168, 2006.

[17] Shruthi P., M.B.Nirmala. *Secured modified bloom's based q-composite key distribution for wireless sensor networks.* International Journal on Advanced Computer Theory and Engineering (IJACTE), 2(3): 2319 – 2526, 2013

[18] E Khan, E Gabidulin, B. Honary, A. Ahmed. Matrix *based symmetric key generation and pre-distribution scheme for wireless sensor network.* IET Wirel. Sens. Syst.,2(2):108-114,2012

[19] R. Kannan S.S. Iyengar R. Kalidindi and A. Durresi. *Sub-grid based key vector assignment: A key pre-distribution scheme for distributed sensor networks.* Journal of Pervasive Computing and Communications, 2(1):35–43, 2006.

