International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

A Survey on Key Pre-Distribution in WSN

Kuldeep Derashri, Dr. Naveen Chaudhary, Ms. Kalpana Jain

College of Technology and Engineering, Udaipur, Rajasthan, India

ABSTRACT

WSN is collection of thousands of small sensor nodes that have small capability of computation and communication of information into network. WSN implementation is different from other wireless network for this key distribution schemes also different in WSN. WSN has limited resources so resource management and effective utilization of that are very necessary. So secure channel establishment during computation is also tedious task in WSN and it cannot implement like other wireless network. WSN implements only that schemes for key establishment which provide lower key computation and distribution cost. I did survey on various key distribution schemes which mainly work for WSN like polynomial key pre-distribution, 3-level key distribution and location aware authentication & key distribution.

Keywords : Key Pre-Distribution, Wireless Sensor Network.

I. INTRODUCTION

Sensors are low power devices which use for the sensing environment variables like temperature, heat and sound etc. Sensors are used many areas such as battle fields, health monitoring, wastewater management and road light on-off, etc. Sensors are used to sense the environment variables and collect the information from environment and this information may be secret for this secure communication link is required to transfer data from sensor devices to base station. We can use various cryptography techniques for secure communication but there problem is that sensor devices works on low power and computation resources. Due to this key distribution in sensor networks cannot implement like other Ad-hoc networks. For this Key Pre-distribution scheme is mainly used for the sensor networks. [1]

Wireless Sensor network have following major challenges:

(i) Wireless communication
(ii) Resource Limitation
(iii) Large network make extra load on sensor nodes.
(iv) No fix infrastructure
(v) No fix topology for nodes deployment
(vi) Higher risk of physical attacks.

We have two types of cryptographic techniques for the secure key establishment:

(i) Symmetric key cryptography (one key for encryption and decryption)
(ii) Asymmetric key cryptography (two key one for encryption and another for decryption)

A Secure key establishment provide the following services:

(i) Authenticity
(ii) Confidentiality
(iii) Scalability
(iv) Integrity
(v) Flexibility

II. NETWORK MODEL

Wireless Sensor networks look like an ad-hoc network in this all nodes are connected together using wireless communication medium like radio signals. In this type of network no fixed connection establishes between nodes and the topology changed dynamically. In this network routing path change according to new nodes

added into the network and dies. WSN mainly used two types of network model: [2]

a. Hierarchical WSN (HWSN)

Hierarchical network as name suggests it is level based networks of sensor nodes. In this three levels of respectively base station, cluster heads, low level sensor nodes is defined.

(i) Base Station (Sink): It is the root node of Hierarchical network model and has higher computation capability and high power sources. It store the data of the all cluster head and manage the complete network.

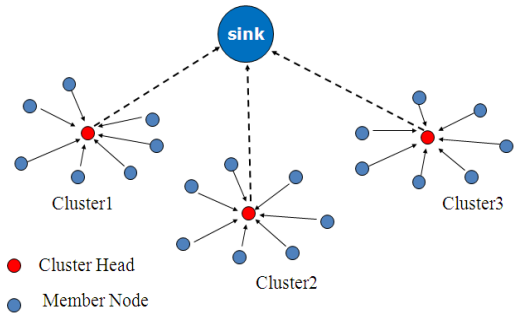

Fig 2.1.1:- Hierarchical WSN (HWSN)

(ii) Cluster Head: Cluster Head works as intermediate nodes between sensor nodes and base station it collects information from sensor nodes and then aggregate it and then send it to the base station.

(iii) Sensor node: It is the low level node which has limited resources and can perform limited computation task. It collects information from things at low level and then send to the cluster head.

Problem	Keying Style
Pairwise	BS oriented
	Master Key
Group-wise	Asymmetric keys
	Symmetric key
Network Wise	Master Key
	TESLA based

Table 2.1.1:- Keying Style for HWSN

b. Distributed WSN(DWSN)

DWSN is a distributed network in which we do not know network topology and routing information before deployment of nodes. On deployment the sensor node find out it's neighbors by scanning it's radio coverage area. In distributed WSN mainly used pairwise, group wise key Pre-distribution scheme for key establishment. [2]

DWSN uses three approaches for key distribution:

(i) Probabilistic: We select no. of keys randomly form key pool and then distributes in sensor nodes.

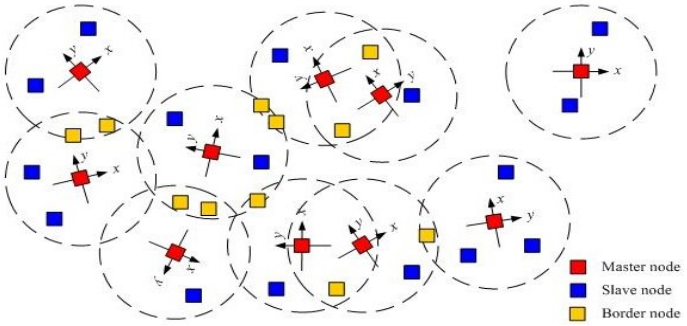

Fig 2.2.1:- Distributed WSN

(ii) Deterministic: deterministic processes use strong connectivity between keys in key selection from key pool.

(iii) Hybrid: It is the combination of probabilistic and deterministic approach to reach better resilience.

Problem	Approach	Mechanism	Keying Style
Pair-Wise	Probabilistic	Pre-Distribution	Random Key-chain
			Pairwise key
	Deterministic	Pre-Distribution	Pairwise key
			Combinatorial
		Dynamic Key Generation	Master Key
			Key Matrix
			Polynomial
	Hybrid	Pre-Distribution	Combinatorial
		Dynamic Key Generation	Key Matrix
			Polynomial
Group Wise	Deterministic	Dynamic Key Generation	Polynomial

Table 2.2.1:- Keying Style for DWSN

III. KEY DISTRIBUTION SURVEY

Sensor nodes establish pair-wise and group-wise keys by using various key generation techniques. Key Pre-distribution is the efficient technique for the WSN because all senor nodes have power and computation limitation. Pairwise key distribution performed by using following techniques:

Master key based key Pre-distribution Scheme

In this scheme, [3] session key establishes between nodes by using master key (K_m) for this first selects random nonce value at nodes and then this nonce values share between both pair of nodes (S_i, S_j) and then session key generates by applying key generation function on master key and nonce values at each sensor nodes $K_{i,j}=PRF(K_m|RN_i|RN_j)$. The main disadvantage of this scheme is that if master key is compromised then all communication become unsecure.[3]

Random Key Pre-distribution Scheme

Eschenauer and Gligor [4] proposed Random Key Pre-distribution scheme. This scheme is divided into three different phases: key Pre-distribution, Discover Shared-key and path-key establishment.

(i) Key Pre-distribution

In Key Pre-distribution phase we select K no. of keys from a Key pool |S| and then distribute at each sensor nodes. All these keys have it's identifier that also stored at sensor node. This set of keys at each node is known as key ring. When once we distribute keys rings to all sensor nodes then we select trusted nodes as controller nodes and save details of each sensor associated key ring and key identifiers.

(ii) Discover Shared-key

Once sensor nodes are initialized with key ring and deployed at respective place then node discovers it's neighbor nodes by using key identifiers.

(iii) Path-key establishment

This phase provides a link between those nodes which do not share common key. Assume if we have a sensor node x and z. If node x wants to communicate with node z but not any common key available between them. Then node x send a message to it's neighbor node y with which it share a common key then if node y share a common key with node z then node y establish a pairwise key K_{xz} between node x and z. At this time the node y works like a key distribution center and provide a communication link between node x and node z.

Q-Composite Random Key Pre-distribution Scheme

Chan, Perrig, and Song [5] have introduced Q-composite random key pre-distribution scheme. In this scheme two neighbor sensor nodes that wants to communicate share at least q no. of common keys to set up a communication link. If two nodes share more than one common keys then it is harder to break the communication link between them. In this scheme key distribution also follow like a random key distribution scheme in this we select K random keys from key pool this is known as key ring and then distribute at each sensor node. Next, we discover the no. of shared keys among two sensor nodes by broadcasting key identifiers of their keys. We can also use posing puzzle method for shared key discovery in this scheme m client posing puzzle like Merkle puzzle is issued for neighboring nodes and then if any node that gives

correct answer of that puzzle is identified as sharing the associated key.

Grid Based Key Pre-distribution Scheme

The Grid based Key Pre-distribution scheme [6] constructs a m x m grid in which the sensor node associated with each cross point of the grid. In this grid based key distribution we require 2m polynomials for the key distribution. If we have j no. of rows and i no. of columns then each row associated with polynomial $f_j^r(x,y)$ and each column associated with polynomial $f_i^c(x,y)$. In this distribution strategy each node of grid has two polynomials

$$\{f_i^c(x,y) , f_j^r(x,y)\}\ i,j=0,\ldots,m-1\}$$

Where $m = \lceil \sqrt{N} \rceil$ and N is the no. of sensor nodes in the network.

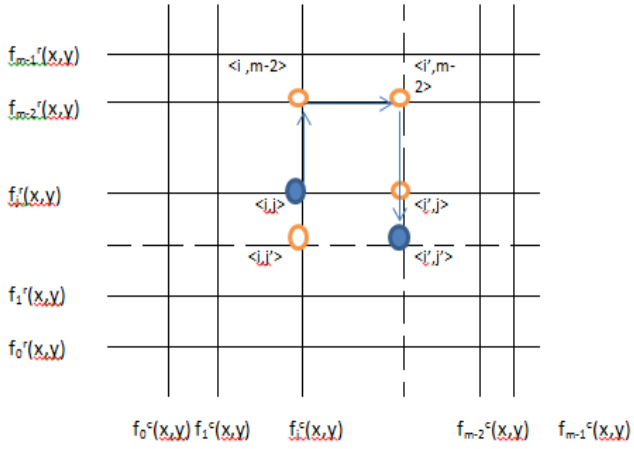

Fig 3.4.1: Grid [6]

Group based key Pre-distribution Scheme

Liu, Ning and Du [7-8] proposed a group based key pre-distribution without using nodes deployment knowledge. In this scheme we distribute sensor nodes in different groups but we can only assigned one node to one group and then we form cross groups by taking only one node from each group and we cannot assign one node to two or more than two cross group. They used two methods for key pre-distribution. In the first method, hash function was used. Nodes will share a common key if they belong to same group or same cross group. If the total nodes in network is N then we divide these nodes in m groups each having n nodes, N = n × m and each node of network store (m+n) /2 keys. Another method used symmetric bivariate polynomials which uniquely assign to each group and cross group. Every node store only two polynomial one belong to it's group and another belong to it's cross group. The pros of this scheme is that we do not have deployment knowledge of nodes but we can reach better node resiliency. The cons of this scheme is that it does not provide secure communication for cross group.

Polynomial Based Key Pre-distribution Scheme

In this scheme the setup server or base station generates a bivariate t-degree polynomial over a finite field F_q.

$$f(x,y)= \sum_{I,j=0}^{t} a_{ij}x^i y^j$$

Where q is a large prime number that enough to establish a cryptographic key between two nodes x and y which has the property f (x, y) = f (y, x). In this network deployment each node associated with a unique ID. Suppose we have two node that ID is 'i' and 'j' then setup server generates two polynomials respectively for that node f(i,y) and f(j,y) for that nodes. And when node 'i' wants to communicate with node 'j' then both compute the same key respectively f(i,j)=f(j,i).[9]

Polynomial pool based key pre-distribution Scheme

It is the advancement of polynomial key distribution scheme in this scheme we generates a set of n-degree polynomials is generated over a finite field GF(q) and form a key pool and then distribute each sensor node S_i to a subset of key pool F_i. We can select the subset of polynomial by applying probabilistic, deterministic and hybrid approach. If any node have the id of the node from which it wants to communicate and have common shared Polynomial with that node then easily communicate with that node.[10]

Three Level Key Pre-distribution Scheme

Three Level Polynomial Key distribution scheme used to provide the more security in sensor networks in this network mobile sinks are used instead of base stations. We have three level of sensor nodes in this scheme and used two different polynomial key sets to establish a communication link between different nodes of different levels. This level based polynomial key-distribution provides more security resilience. [11]

The algorithm consists following phases:

(i) Static and mobile polynomial key pre-distribution

(ii) Key discovery between mobile node and stationary node
(iii) Selecting shortest path among the feasible paths

(i) Polynomial Key Pre-distribution

Given a sensor network, let N = $\{N_1, N_2, N_3, \ldots..N\}$ be a set of n stationary sensor nodes. S =$\{S_1, S_2, S_3, \ldots, S_m\}$ be a set of m stationary access nodes and MS =$\{ MS_1, MS_2, MS_3, \ldots, MS_r \}$ be a set of r mobile sinks. A mobile polynomial pool M and a static polynomial pool S are generated. The mobile sinks and stationary access nodes are randomly given K_m polynomials and one polynomial (K_m>1) from M and all sensor nodes and the preselected stationary access nodes randomly pick a subset of $K_s$and K_{s-1} polynomials from S.

(ii) Key discovery between mobile node and stationary node

The pairwise key between sensor node u and mobile sink v is established by a stationary access node w.

Sensor node u find a stationary access node w which can establish pairwise key with mobile sink v by finding common mobile polynomial and with sensor node u by finding common static polynomial. To select a common polynomial sensor node broadcast it's polynomial IDs. When a secure path establish between u and v then mobile sink v sends the pairwise key k_c to node w in a message encrypted and authenticated with the shared pairwise key K_{vw} between v and w. Then again this key shared between w and u by using pairwise key K_{wu} between w and u. In this process we will use an intermediate node to establish a common key between sensor node and mobile sink.

(iii) Selecting the shortest path

The key establishment through direct or intermediate nodes may have more than one path between the sensor node and the mobile sink. We use the shortest path calculated with Dijkstra algorithm to use shortest distance. In other words, if the mobile polynomial key match between mobile sink and stationary access node and static polynomial key match between stationary nodes and stationary access nodes exist with different intermediate nodes then a shortest path is selected.

Location-Aware Authentication and Key-Distribution Scheme

In this scheme, each senor node establishes a communication link with neighbor node by identifying the location of that node. Remote Node RNs works as anchor nodes for sensor nodes to gather their neighborhood information. The RNs have large coverage area and it periodically broadcast beacons that are received by sensor nodes and used to authenticate neighbor nodes before establishing pairwise keys. In this major concept is that two sensors only established pairwise key if they received beacon message from at least one common RN.[13]

(i) Pre-deployment Phase

Network administrator configures all nodes with an initial key K_0 before deployment of nodes. RN used this key to secure the beacon messages. RN will be identified by unique id and generates a pair of private and public key by using elliptic curve public key techniques. Therefore, the network administrator selects an elliptic curve field E(Fp) where a p is a very large prime number, which generates a set of secret values $S=\{S_0,S_1,S_2,..S_{k-1}\}$, and calculates their corresponding public values $P=\{Y_0,Y_1,Y_2\ldots Y_{k-1}\}$where $Y=S_iG$, G is selected as an elliptic curve generator point. The Private key for RN_j is generated by applying the hash function on the identity of the RN_j

$m_j=Hash(Id_j)$
$m_j=\{m_{0j},m_{1j},\ldots.m_{kj}\}$then
Private Key $S_j=(\sum_{i=0}^{k-1} m_{ij}S_i)\mod(p)$

(ii) Location-based authentication and pairwise key establishment

Initially Sensing node SN_i will generate its private key, Si using the chosen elliptic curve field, $E(F_p)$ and then it's public key $Y_i=S_iG$. Then sensing node capture the beacon messages sending by the different RN_s. The node decipher this message using initial key K_0 and find out nonce and identity of the transmitted RN_s. Then sensing node computes an authentication key by applying the has function of nonce $K_j=Hash(n_j)$.
The node SN_i generates authentication code M_{ji}

$M_{ji}=Hash(K_j;Y_i)$ where Y_i=Public key of SN_i

The two nodes are considered neighbors if they are at least reachable by one common RN. In this case, the public key can be authenticated by one off the authentication keys, K_j shared with neighbor nodes.

(iii) Intra-cluster pairwise keys establishment

In intra cluster key establishment the pairwise key establish between RN and each SN_s. If SN_i wants to establish pairwise key with RN_j then first it calculate m_j of the RN. The Public key of RN is calculated by

$$P_j=\sum_{n=0}^{k-1} m_{nj}Y_n$$

The Pairwise key K_{ij} can be established by the following formula $K_{ij}=S_iP_j$. Where Si is the private key of sensor node S_i. Then Sensor node sends it's public key Y_i to the RN and the R_n generates $K_{ij}=S_jY_i$.

(iv) Group Key Establishment

RN_j calculates individual public key value Y_{ji} for each SN_i

$$Y_{ji}=S_j\sum_{n=1}^{Nj} Yn \text{ where } n\neq i$$

The Cluster key K_j can be determined by applying addition operation between Y_{ji} and in intra-cluster pairwise key.

$$K_j=K_{ij}+Y_{ji}$$

IV. CONCLUSION

In this survey paper I describe the pairwise key distribution that are suitable for the WSN. We generally avoid use of the public key cryptography in the WSN due to resource limitation but elliptic curve cryptography is exception which works better with less resources. In WSN security is big concern so we can do many advancement in this area which provide the greater security with less computation.

V. REFERENCES

[1]. Yong Ho Kim, Hwaseong Lee, and Dong Hoon Lee, A key distribution scheme for wireless sensor networks, 0-7695-3113-X/08 $25.00 © 2008 IEEE

[2]. S. A. Camtepe and B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: a Survey. Technical Report TR-05-07 (March 23, 2005).

[3]. Lai, B., Kim, S., and Verbauwhede, I. 2002. Scalable session key construction protocol for wireless sensor networks. In IEEE Workshop on Large Scale Real Time and Embedded Systems (LARTES).

[4]. L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proc. of the 9th ACM Conf. on Computer and Communications Security, pages 41–47, November 2002.

[5]. H. Chan, A. Perrig, and D. Song, "Random Keypre-distribution schemes for sensor networks,"Proc. of the 2003 IEEE Symposium on Security and Prvacy,, May 11-14 2003, pp.197-213.

[6]. Donggang Liu , Peng Ning. Establishing Pairwise keys in Distributed Sensor Network. CCS'03, October 27–31, 2003, Washington, DC, USA

[7]. 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.

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

[9]. Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. 1992.Perfectly-secure key distribution for dynamic conferences. In Crypto 92.

[10]. I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Sink mobility protocol for data collection in wireless sensor networks," Proc. of the 4th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC"06), pp. 52-59, 2006.

[11]. Tanuja R, Souparnika P Arudi*, S H Manjula*, K R Venugopal*, L M Patnaik**,TKP : Three Level Key Pre-distribution with Mobile Sinks for Wireless Sensor Networks, 2015 IEEE

[12]. Walid Abdallah and Noureddine Boudriga, A Location-Aware Authentication and Key Management Scheme for Wireless Sensor Networks, 2016 IEEE