REVIEW ON KEY PREDISTRIBUTION SCHEMES IN WIRELESS SENSOR NETWORKS

Neetu Rani and Manik Gupta

Department of Computer Engineering, Chitkara University, Himachal Pradesh

ABSTRACT

A wireless sensor network consist distributed sensors which are used to monitor physical or environmental conditions like temperature, sound, pressure and so on. Wireless sensor network are used in future in many applications like military, investigation teams, researches and so on. Security is the main issue in wireless sensor network. Sensor network arrange several types of data packets, packets of routing protocols and packets of key management protocols. Key management is the most effective method for providing better security against several types of attacks. This paper discusses the various key pre-distribution approaches along with their advantages and disadvantages.

KEYWORDS

Key management, key pre-distribution, combinatorial design, Resiliency.

1. INTRODUCTION

A wireless sensor network consist distributed sensors which are used to monitor physical or environmental conditions like temperature, sound, pressure and so on. Then the monitored data is transfer to the main location via network. Wireless sensor network are used in future in many applications like military, investigation teams, researches and so on. Security is the main issue in wireless sensor network. Sensor network arrange several types of data packets, packets of routing protocols and packets of key management protocols. Different types of keys are used to provide the secure data communication over the network. A key is a variable value that is applied using an algorithm to a string or block of unencrypted text to create encrypted text or to decrypt encrypted text. Key management is the management of cryptography keys in a cryptosystem. These may include symmetric or asymmetric keys. In symmetric key algorithm the identical keys are used for encryption and decryption of the message. In asymmetric keys there are two keys. One key is used for encryption and second key is used for decryption. The key establishment technique for the secure communication provides confidentiality, scalability, integrity, authenticity and flexibility.

Authenticity: The key establishment technique provides authenticity in the network through which the receiver node should recognize the assigned identity of the sender node.

Confidentiality: The key establishment technique should protect the data from unauthorized parties. An attacker may try to attack a sensor network by getting the secret keys to obtain data. A better key technique controls the compromised nodes to keep data from being further exposed.

DOI:10.5121/ijassn.2016.6101

Scalibilty:The key management technique provide high security features for small networks and also preserve these characteristics when applied to larger network..

Integrity: Integrity means only the permitted nodes have access to the keys and only an assigned base station should privilege to change the keys. This would prevent unauthorized nodes from obtaining knowledge and any updation of the information.

Flexibility: Flexibility means Key establishment function well in any kind of atmospheres and provides dynamic deployment of nodes. It means key establishment technique should be useful in many applications and allow addition of nodes at any time.

Key Predistribution: There are many techniques for creating a secure communication between nodes. The most effective technique is key predistribution .In key predistribution method certain keys are preloaded into each sensor before their deployement [1].Each sensor node is assigned with a set of keys from the large pool of keys before deployment. After deployment the two nodes having at least one common key, then that node is able to establish a communication path with another node. There are a number of characteristics of WSNs on which key predistribution techniques are depends in order to provide the better results. These are local, global connectivity and resiliency.

Local connectivity means the possibility that any two sensor nodes should have a shared key with which they can start a secure connection to communicate. Global connectivity is the part of nodes that are in the largest connected graph over the number of all nodes.

Resiliency protects the paths when a number of nodes are compromised. Other issues in the design of WSN are computational cost and hardware cost.

Computational cost is the sum of computation done through these phases. Hardware cost includes the cost of the memory and battery in all nodes.

Basically a key pre-distribution scheme consists of 3 phases:

- Key distribution
- Shared key discovery
- Path-key establishment

During these phases, secret keys are created and placed in sensor nodes. Then each sensor node searches the area in its communication range in order to discover another node to communicate A secure connection is established when two nodes discover one or more common keys, these keys are different in each scheme of key predistribution, then the communication is done on that link between those two nodes. Then routes are recognized by joining these links to produce a connected graph.

All the key pre-distribution techniques divided according to three ways. These methods are:

1) Probabilistic
2) Deterministic
3) Hybrid

In the Probabilistic methods keys are chosen on the random basis and then placed into the sensor nodes.

In the deterministic method some patterns are used to select the keys from the large pool.
The hybrid technique uses both the deterministic and hybrid method to select the keys.

2. KEY PREDISTRIBUTION SCHEMES

There are various types of key predistribution schemes. This review paper presents various key predistribution methods along with their advantages and disadvantages.

2.1 Random Key Predistribution Scheme

The random key predistribution scheme also known as basic scheme. This technique proposed by Eschenauer et al [2].A large pool of keys is created, from this pool keys are randomly chosen and stored in every sensor node. Any two nodes which find common keys can use these shared key for secure communication. Three phases are needed to set up the communication keys [1].

2.1.1 Key Pre-Distribution

In the key pre-distribution phase each sensor node carries k different keys, which are randomly chosen from a big key pool The key pool consist of two parameters key pool size K and key chains L.The key pool consist of L different key chains$K = \cup ci(i = o, \ldots., L - 1)$and $Ci \cap Cj = \emptyset(i \neq j)$. The key chain is created via unique generation key gi and by creating seed by using keyed hash algorithm. Thus lth key from the key chain is calculated as: $Kci, l = H^{i}(seed, gi)$[3].
In the key ring loading phase the key rings are assigned to each nodes. It contains two parts R1 and R2 where R1 is the creation of key chains and R2 is the set of the random keys from different key chains[4].For node i,Ri=Ri,1∪ Ri, 2.This set of k keys is called key ring and each key has an equivalent identifier. The shared-key discovery phase occurs when the sensor nodes are installed into the recognized area. In this phase each node determines its neighbours in radio range with which it shares mutual keys. At the end of shared-key discovery stage, links are established between nodes that are not only in radio range but also sharing common keys[2].In this scheme, the random-graph theory[5] is used to design a key pre-distribution scheme.

2.1.2 Shared key discovery

When the sensor nodes deployed in the respective places, then each sensor node search its neighbors with which it can share common keys. There are various ways by which it can determine whether two nodes node share a common key with each other or not. The nodes broadcast list of the key identifier to other nodes. If a node finds out that it can share a common key with a specific node, then it can use this key for secure communication range in order to discover another node to communicate. A secure link is established when two nodes discover one or more common keys, these keys are different in each scheme of key predistribution. Then the communication is done on that link between those two nodes. Then routes are recognized by joining these links to produce a connected graph.

2.1.3 Path key establishment

The path key establishment stage provide link between two nodes when they are not able to share a common key.e.g If the node A wants to communicate with node but these nodes do not have a common key between them. Now node A can send a message to node C saying that it wants to communicate with node B.Then encrypted message is created by using the common key shared between node A and C, if node C has a common key with node B then it can generate a pairwise key for node A and B.Thus it acts like a key distribution center. After the accomplishment of

shared key discovery stage, number of unused keys remains left in the sensor key ring these keys are used by each sensor node for path key establishment.

In the new proposed scheme [4] key chain is created by using the keyed hash function [3].Hence key inside the key chain maintain the following relation with other keys which are in the same key chain $Kci, l = H(kci, l-1, gi), Kci, l+1 = H(Kci, l, gi), \ldots$So, it is difficult to compute Kci from Kci,l+1 or Kci,l-1 without know the secret key gi.Thus this scheme provide better safety against attacks. The new scheme offer good resiliency while requiring a much smaller key ring size when related with Eschenauer and Gligor's.This scheme is much scalable to the bigger network areas.

Advantages of the random scheme proposed by Eschenauer et al.
This scheme is flexible, efficient and simple to employ, provide good scalability.

Disadvantages

This scheme do not provide node to node authentication.
It cannot be used in environments demanding highest security

2.2 Q-Composite Random Key Predistribution Scheme

In the basic scheme any two adjacent nodes need to find a single common key from their key rings to establish a secure link in the key-setup phase. The variation to the basic scheme is the Q-Composite Random Key Predistribution Scheme, where q common keys are needed to establish the secure link between nodes [1].In this scheme the numbers of keys overlap increased, so it is difficult for an adversary to break down the communication link. This scheme use 9 common keys between the communication nodes wherever Q is >1.Since it increases the quantity of keys which are shared between each node, thus is becomes the difficult for an attacker to break down the network [6].In this scheme the size of the pool is increased from which key ring is selected and the size of the key ring is decresed.So it become difficult for an attacker to attack on the network.

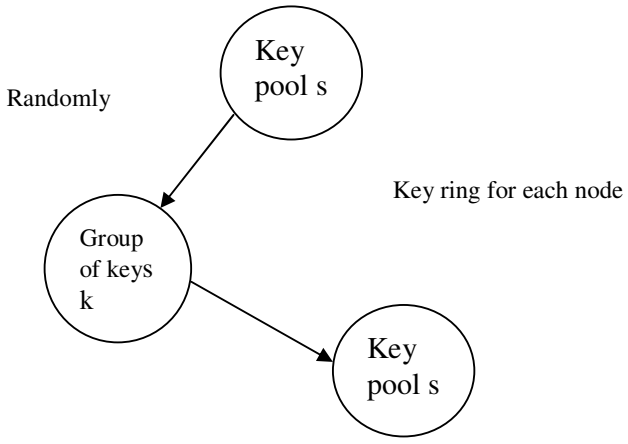


Figure1.key predistribution setup phase

In the key predistribution phase of the Basic and Q-Composite Schemes k arbitrary keys are chosen from the key pool and store in each node's key ring. During the shared-key discovery

stage, the nodes find the common keys which they share with the other nodes by using various methods. Either the nodes transmit their key identifiers or by choosing the Merkle puzzle [7].In this method the node issues m number of puzzles that is one for each key to all its neighbors.A path key is established when node resolves the puzzle and answers with an accurate answer.

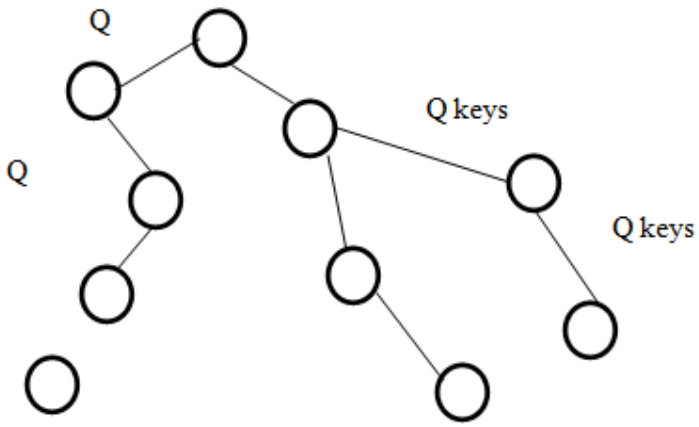


Figure2. Shared key discovery and path key establishment

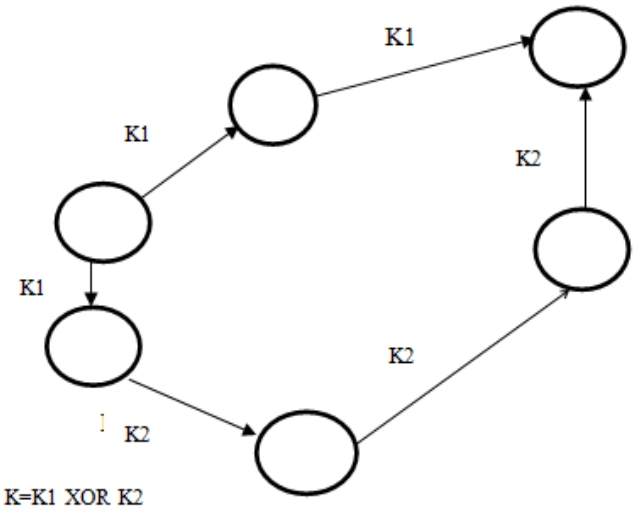
This method provides more security but not so fast. The key set up phase is accomplished only if both the nodes having q common keys. Then the path among the nodes is recognized. This phase known, path key establishment. When a small number of nodes deployed in the network then this scheme provides better resilience. This method cannot handle the node duplication. When the key is established it can be used anytime-composite modified bloom's distribution scheme is proposed to provide good network resilience and used for large network size [8].In the Bloom's scheme only a single key space is used for establishment of pair wise key. The Bloom-based scheme (BB) extends the Bloom's scheme by using multiple key spaces. In the MBBQ scheme q pairs of secret are produced from the common key spaces to create a link. When q = 1, m = M, and $\lambda = 0$ then MBBQ scheme is equal to the basic scheme and when q >1,m = M, and $\lambda = 0$ then this scheme is equal to QC scheme[8].Modified bloom's q-composite distribution scheme offer better solution for memory, overhead and scalability issues when matched to the other distribution techniques and provides very good resilience in the large network size.

2.3 Multipath Key Reinforcement Scheme

The Multipath Reinforcement Scheme [9] provides good security. In the basic scheme the keys are randomly selected from the key pool, so the link establishment in this scheme is not very much secure. It increase the number of threaten node in the network when one node is compromised by the attacker. So when the one node is compromised the values of the communication keys should be updated.

Because of the random selection of the keys from the key pool, the path establish after the key discovery phase is not so much secure. When one node is compromised then it put effects on the multiple nodes. In order to resolve this limitation the communication key among the nodes must be updated. This is implemented by using multiple independent paths for high security purpose. If node A wants an updated key with another node B,then node A can use all disjointed path which

are possible towards node B.After establishment of new node, if an adversary compromises all the nodes which are used to creation of key then he can decrypt the communication path. If the size of the network is very large then a chance is created for an adversary to eavesdrop thus make the whole communication path insecure. A 2-hop technique of the multipath key reinforcement technique consist only 2 paths to decrease the path length by via disjointed paths [1].



[10]

Figure3.Multipath key reinforcement technique

In random key pre-distribution techniques of WSN, the keys are randomly selected from a large key pool and loaded on the sensors before the deployment. After deployment, each sensor node attempts to find a common key that is shared by itself and shared by its neighbours to establish a link key to protect the wireless communication between the networks. The drawback of this scheme is that it some neighbour nodes do not share any common key. In order to establish a link key among these neighbours the multi-hop safe path might be used to provide the security.

But the limitation of this scheme is that sensor compromised on the way which makes this scheme insecure. To overcome this limitation Just Enough Redundancy Transmission (JERT) scheme is used, which uses the maximum distance separable (MDS) codes to solve the problem. When one round of the JERT scheme fails, the succeeding round of broadcast should provide the receiver just enough redundancy signs so that it can accurate the faults which were created by the compromised paths. In the JERT scheme the secret link key is programmed in (n, k) MDS code and transferred through multiple multi-hop routes. The MDS code is that code in which hamming distance dmin is used across pairs of distinct code words such this distance satisfy the condition that is dmin=n-k+1.Here n is the length of the code and k is the dimension of the code. In MDS code (n,k,n-k+1) each code word include n symbols which contain k information symbols. Here the n-k symbols are known as parity check or the redundancy of the code [11] [12].MDS codes provide the largest possible minimum Hamming among code words and it can correct lots of errors. The JERT technique is very efficient and resistant against node compromised.

The Multipath Key Reinforcement Scheme provides better security than the basic or the Q-composite technique. The limitation of this scheme is that it creates communication overhead which reduces the battery life. Increase the opportunity for an adversary to launch denial of service attacks.

2.4. Random Pairwise Key Scheme

The random pairwise key predistribution scheme is the modified version of the pairwise key predistribution scheme. In this scheme the sensor nodes are provided with different security level and the negotiated sensor nodes cannot disclose the key information in the sensor nodes which have greater security level [12].The pairwise key establishment technique is very efficient technique because it provides Many additional features, including node to node authentication and resilience to node duplication. This scheme can be effectively used for small networks. The random pairwise scheme is developed to overcome the drawback of pairwise key predistribution scheme. The random pairwise scheme contain that if there is a network of size N and the minimum connection possibility of two nodes is p then each node store k number of keys thus k=N*P [13].

2.4.1 Initialization and key setup in the random pairwise keys scheme

In this scheme size of node's key rings is m keys and the possibility of two nodes communicate securely is p. The random pairwise keys scheme works as follows:

In the initialization phase of pre-deployment total n = m /p unique node identities are created. The real size of the network might be smaller than n.The node identities that are unused are used for the addition of additional nodes in the network in the future. The identity of each node is compared with another randomly selected node identity .Then the pairwise key is generated for every pair of nodes. After this the generated key along with ID of another node is stored in the key rings of both the nodes.

In the post-deployment phase of key setup firstly each node broadcast its node identity to its neighbours. By increasing the real communications radius the number of neighbours can be increased thus the size of the network can be increase. But this process of range extension increase denial of service attacks in the network .The adversary introduce foreign nodes into the network to generate random node identities which flood the network with rebroadcast identities. This make the whole scheme very slow and inefficient .Such types of attacks can be minimized by restricting the number of hops which are used for range extension.

2.4.2 Support for distributed node revocation

In the random pairwise scheme of key predistribution, node revocation can be maintained through base stations [14].Revoking of the compromised nodes from the network helps to avoid various types of attacks such as denial of service attacks, inserting clones and dropping authentic reports etc. The revocation of the sensor nodes through the base station may be a slow process because of high latency in communication with the sensor nodes. To overcome the drawbacks associated with a base station dependent revocation protocol a distributed node revocation scheme for the random pairwise scheme is introduced. This scheme is possible if there will be any mechanism in each sensor node by which they can detect if the neighbour nodes have been compromised. If node x finds a certain node y to be compromised then it casts a public vote against node y.If a threshold of such votes have been cast against node y by another nodes in the network, then the node x will disconnect all its communication with node y.This process proceed until all the nodes in the network disconnect their links with node y therefore deleting' node y from the

network. All the nodes that vote against node y are known as voting member of node y, the node share k pairwise keys with other nodes thus there are k voting member of node y.The node revocations of the negotiated nodes are implemented via voting of all the nodes in the network with appropriate threshold parametrs.But this technique is not scalable and threshold value for node revocation is selected very carefully because it can leads the others problems.

Advantages

The advantage of this scheme is that it offers better security compared with other schemes, it provides perfect resilience to node capture as the keys that are used by each node are unique.
This scheme provides resistance against node capture.

Disadvantages

The disadvantage of this scheme is that it is not useful for large size network.
It does not fulfil scalability requirements.

2.5 Polynomial Pool Based Key Predistribution

In this scheme a pool of randomly generated bivariate polynomials is created. The technique which is used to generate this bivariate polynomial is depending on the polynomial based key-predistribution [11].In the key predistribution stage of polynomial technique the setup server creates a set of bivariate polynomial over the field of Fq.Then each polynomial is assigned with a particular identity for the server. A subset of such polynomials are then chosen by the server and retained in each of the network nodes. In the key discovery phase each sensor node searches another node with which it share the similar bivariate polynomials then both the nodes creates a common key. The main issue is to find whether two nodes share similar polynomial or not. For this there are two techniques are used. Predistribution and Real-time discovery.

There are two cases of the polynomial pool.

1. The polynomial pool takes only one polynomial, the overall framework degenerates into the polynomial-based key pre distribution.
2. While all the polynomials are 0-degree ones, the polynomial pool degenerates into a key pool just like basic scheme and the q- Composite scheme.

2.5.1 Random Subset assignment key pre-distribution [11][12]

In the predistribution stage the information of the nodes with which each node will share a polynomial is pre-loaded. The limitation of this scheme is that it does not provide the flexibility of addition of new nodes into a network and it leaves the network susceptible to attack. The information is redistributed in this method; an attacker can attack a node and gain access to the stored data. After key discovery if two nodes do not discover a common polynomial share they must communicate using a path key. If node A wants to communicate with node B and the two nodes do not have a common polynomial share, node A find a route through which it can communicate with node B and any node can then send a request to establish a pairwise key for communication. The issue with this stage is that intermediary nodes should be able to communicate with both nodes. There are two techniques for finding intermediary nodes: predistribution and real-time discovery. The main issue in this technique is that how to allocate polynomial shares to dissimilar classes of nodes.

2.5.2. Connectivity for polynomial pool based scheme

The degree of polynomial is larger than one and the same polynomial can produce multiple keys at dissimilar nodes. Thus the total number of keys that A1 node can share with all A2 nodes is the combination of the number of shared polynomials among node A1 and A2.Based on this statement first compute the probability that a A1 node shares i polynomials with A2 node denoted as p (i).Let S be the size of the polynomial pool, suppose P1 and P2 be the number of polynomials that can be stored in A1 node and in A2 node, respectively. We can calculate p(i) as follows:

$$P(i)= \frac{\binom{s}{i}\binom{s-i}{pi-1}\binom{s-p1}{p2-i}}{\binom{S}{P1}\binom{S}{P2}} \qquad [13]$$

Thus finally the connectivity for the polynomial-pool based key management technique Can be calculated by:

$$Cp(q) = 1 - \sum_{i=0}^{q-1} pn2(i) \qquad [14]$$

Polynomial Pool-Based Key Predistribution using random subsets provides greater security and flexibility as compared with other schemes. The Polynomial Pool-Based technique offers many advantages over Random Pair wise. In this scheme sensors can be added dynamically without checking the already deployed sensors.

Advantages of this scheme are that it allows the network to develop to larger size after deployment. The Disadvantage of this scheme is that if more than t polynomials are compromised by the attackers then the whole network leads to compromise.

2.6 Group Based Key Pre distribution Scheme

In the group-based key pre distribution scheme sensor nodes in the same deployment group can establish pairwise key with each other. A group based key predistribution scheme is produced to handle the pairwise key establishment among the sensor nodes in dissimilar groups. In this system all the nodes of a network share a group key. Once the base station transmits a protected message it uses the group key. A key predistribution is divided into three parts:

- Predistribution
- Direct key establishment
- Path Key Establishment

Predistribution For each deployment group Gi, there is a need of key predistribution instance Di for establishment of the pairwise key in Gi.Such key predistribution instances are known as in-group (key predistribution) instances. The in-group instance Di might be the instance of any existing key predistribution scheme.

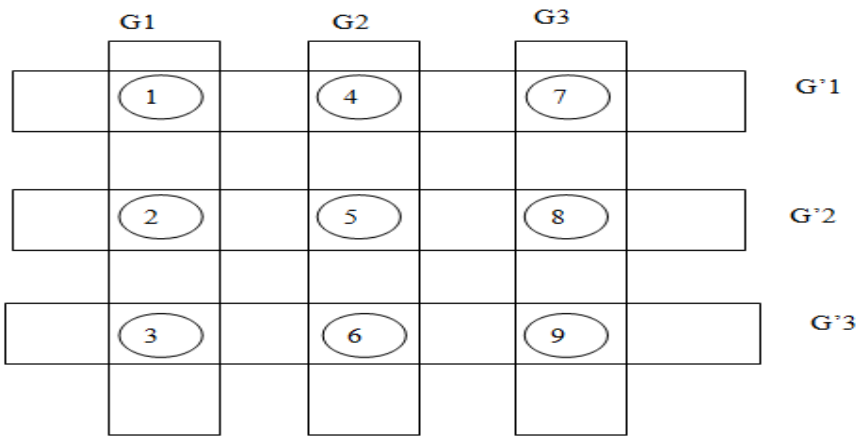


Figure 4.Group Construction [15]

2.6.1. Group construction

Groups are constructed to establish the pairwise key between sensor nodes. There is only one sensor node in each group and in different cross groups and there are no common nodes. A predistribution instance is created to establish the pairwise wise key in GI. Hence each cross group provides a link for any two deployment groups.

2.6.2. Direct Key Establishment.

After the predistribution step direct key establishment between neighbouring sensors node is established. The key is established between two key predistribution instances, in between group instances and between cross group instance. If the sensor nodes deployed in the same group then they can follow direct key establishment of the in -group instance. If the sensor nodes are not deployed in the same group but they belong to same cross group then they can follow direct key establishment of the cross-group instance.

Path Key Establishment:

The sensor nodes which cannot establish a direct key, they use a path key establishment in order to find the sequence of other nodes in order to establish an indirect key. Every message among two sensor nodes is encrypted and authenticated via direct key established between them. If two sensor nodes are deployed in the same group Gi then they maintain the path key establishment in Di [16].

Disadvantages

The communication between cross-group neighbours is not very much secure. This scheme is not suitable for those networks which have small group size. In order to resolve this problem a group based design using resolvable transversal design is proposed. This method proposed that in order to increase the cross group connectivity, each node is contained in m cross groups instead of just one group.

2.7 Location Dependent Key Management Scheme

In location dependent key management technique the creation of the links totally depends on the location of the sensor nodes. This key management scheme is used for static sensor networks. This scheme provides the keys to sensor nodes according to the location of the sensor nodes. This

is done without getting any knowledge about the location of the sensors. In this scheme nodes can be added to the network anytime through the lifetime of the sensor network [17].

The nodes which are used are statics. The nodes can communicate with each other only via encrypted channels and nodes can join the network anytime. The nodes which are used in this scheme are capable of transmitting at different power levels. There are some special nodes which are known as anchors nodes are used in this scheme. The anchor nodes are same as other sensor nodes, but the only difference is that anchor node transfers messages at different power level and they are tampering proof [18].Steps involve in this scheme:

- Pre-deployment phase
- Initialization phase
- Communication phase

In the predistribution phase a set of keys used by the nodes is computes by the key server. Then the keys are placed into key pool. After this the sensor nodes are loaded with a subset of such keys along with a single common key which is share by every sensor node. The anchor nodes cannot receive any key from the key pool. The next two phases occur after the deployment of the nodes in the environment. The nodes and the anchor nodes are arbitrarily dispersed. The anchor nodes transfer a beacon at different power level. The sensor nodes obtain these beacons and generate new keys by using old keys along with beacon received from the anchor node. After creation of new keys the original subset of keys is deleted from the memory of the sensor node. The common key is deleted by the nodes share by them. The target field is divided into a number of same-shaped and equal-sized cells. Each cell is allocated a single bivariate polynomial arbitrarily. Before deployment, each sensor node redeploys the polynomial shares by its home cell and neighbouring cells. Triangle-based arrangement can accomplish the greatest security property. In LDK scheme beacons getting by a sensor depends on the distance of the sensor from ANs.When a single sub key which is stored on many nodes is compromised then the chance is increased to compromise that link which that sub key. Consider three sensor nodes S1, S2 and S3 shown in figure.

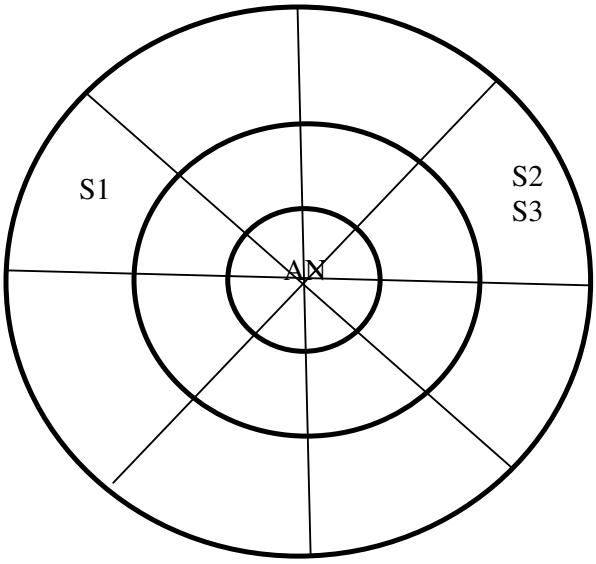


Figure5. Dividing the adjacent area of an anchor node to 8 non-overlapping sectors.

2.7.1 SDLK

When the anchor node i.e. AN transfer a beacons all three sensor nodes will gets the beacon, then they calculate a common key Kcomm which depends on received nonce. But there are two issues of this common key. Firstly in this scheme there is limited communication range between each sensor so there is no direct link between nodes S1 with other two nodes. Thus knowing common key Kcomm by sensor node S1 does not provide any connectivity. If node S1 compromised then common key Kcomm also compromised. This increase the vulnerability of the link between S2 and S3.These problems can avoid by limiting the transmission of the beacons. For this each arbitrary anchor node divides its corresponding area to Nb sectors. For example in figure the anchor node divides its adjacent area to 8 sectors. Within each sensor the anchor transfer dissimilar set of beacons in Np different power levels. Other sectors do not accept such beacons due to directed propagation. In LDK scheme as the power level increase then the usage of memory also increased. To use the memory in effective way the sensor node should save a sub key when the sub key is common with its nearby neighbours. The sectorization enlarges the overall sub key pool but does not degrade memory. As the exposed sub keys are used to protect some other links among non-compromised nodes these links may become vulnerable. So, the problem of compromise ratio arises.

Advantages of LDK: The advantage of this scheme is that the compromised nodes do not influence nodes in different position of the network. If an attacker compromises a node then it is not able to communicate with other nodes which are devoted to different anchor nodes.

The compromised nodes can affect other nodes which are local but cannot affect the entire network.

Disadvantages

In this scheme an adversary can create a denial of service attack by jamming the anchor node and by transmitting the false beacons. So the anchor nodes dispersed randomly in the environment.

2.8. Hypercubemultivariate Key Predistribution Scheme

This scheme basically a threshold based scheme in which a hypercube is designed. IN this scheme multivariate polynomial is designed to each point on the hypercube. The points that are assigned to sensors are unique points [19].A direct key is established between any two sensors. This scheme ensure that if there is no compromised node present in the network then a pairwise key can be established between two sensor nodes and the nodes can communicate with each other [19].In MKPS scheme a larger set of symmetric polynomial is created by the sink before the network deployement.Each sensor node is assigned by an ID that contain nonnegative integers. Such IDs allocate d-1variate polynomial to each node. For each node polynomials are stored in the memory. Two nodes share the similar d-1 multivariate polynomials with IDs at the hamming distance of one from other. Now the nodes can establish d-1 common keys. Two layers of the MKPS are used to provide connectivity to the network for inter and intra-cell communications. This scheme consists of two phases, setup phase and link key establishment phase. The setup phase performed by the sink before network deployment and the link key establishment phase is accomplished after the network deployement.Every two nodes having hamming distance of one from each other can create a link key. The adversary compromise all d-1 shared keys connected two arbitrary nodes in order to compromise the link key that is established among them.

2.9 Key Predistribution Using Combinatorial Design

Combinatorial design means arrangement of finite set elements into patterns which include subset, words, and arrays according to specified rules. The main object which is used in

combinatorial design in BIBD (Balanced incomplete block design).A BIBD is an arrangement of v different objects into b block. Here every block contain k different objects.A BIBD is an arrangement of (B,V).Here B is the group of blocks, subset and V is the set of elements. The elements that are from different groups occur in one group. For example {1,2,3}, {1,4,5}, {1,6,7},{2,4,6},{2,5,7},{3,4,7} and {3,5,6} are Bibd with (7,7,3,3,1) It means there are 7 objects and 7 blocks. Every object consist 3 objects and each object occur in 3 blocks. The BIBD has its own restriction. The number of sensor nodes which are included in this design should have prime power. It limits the use of this technique [10].

The combinatorial design is used in those applications where large number of sensor nodes is deployed. In this scheme key chains are allocated to sensor node before their deployement.After deployment a pseudo random number is assigned to sensor nodes [20].

The advantage of this scheme is that every pair of sensor node directly communicates with each other. This scheme provides greatest resilience against node capture attack.
Limitations:

In [20] when a new node entered the network it was preloaded with the key which was fixed and was not updated with time. So any malicious node could enter the network by capturing the preloaded key and could gradually capture the network key set by sniffing the network

The key distribution mechanism uses the symmetric key technique that is implemented with single key. This could be captured easily if the key set was already compromised by the adversary.

Therefore a new key management technique is required in which the key sets are not static throughout the life of the network. This would also prevent the attacks by the adversary.

2.10 Babel Key Predistribution Scheme

When the probabilistic key distribution techniques are used, there is often a possibility that two sensor nodes cannot directly create their shared key. The path key establishment is used to deal with this problem. When si establish shared key with x sensor nodes by using path key establishment then different secure links should be found. It increases the communication overhead.BABEL key predistribution is designed to reduce such communication overhead. In this scheme when si establish the shared keys with x sensor nodes by using path key establishments and such nodes firstly broadcast the Merkle puzzles into the whole network. The aim of this transmission is to search the sensor nodes whose key ring overlapped with si and with x sensor nodes. When this sensor nodes sj is found then it can used as a common medium between si and another x sensor nodes which are connected [21].

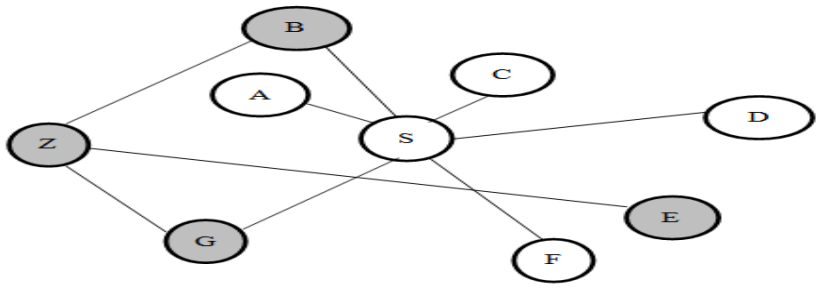


Figure 6.Babel key predistribution scheme

3. COMPARISON

Key establishment is the main cryptographic primitive in all application where security is the main concern. Key management is the most effective method for providing better security against several types of attacks. All the keys have their own limitations and advantages according to the area in which they are deployed. The following table showing the comparison of different methods of key predistribution.

Schemes	Storage Overhead	Computation Overhead	Communication Overhead
qComposite scheme	O(r)	O(r)	O(r)
Multiple space key predistribution scheme	O(λ * τ)	O(λ * τ)	O(λ * τ)
Polynomial pool based key predistribution scheme	O(t*|Fi|)	O(t*|Fi|)	O(t*|Fi|)
Combinatorial design based key predistribution scheme (BIBD based method)	O(r)	O(r)	O(r)
Random assignment set selection key Predistribution scheme	O(n0.5)	O(1)	O(n0.5)
BABEL key predistribution scheme	O(r)	O(r)	O(r)
Group based key distribution scheme	O(r)	O(r)	O(r)
LKE Key distribution scheme	O(d) in service node and(1) in sensor node	O(dt) in service node and O(t) in sensor node	O(d) in service node and O(1) in sensor node

4. CONCLUSION

The probabilistic schemes are scalable in nature whereas deterministic techniques are not scalable. But benefit of deterministic schemes is that they are simpler in terms of calculation and also provide good resiliency and better connectivity due its certainty. Schemes which are using combinational arrangements are good in terms of resiliency. All key management techniques have their own benefits as well as shortcomings. So the techniques which fulfil both requirements and resources only those techniques should implement. Security should be a big priority in military services as compared with civilian application of wireless sensor network. Furthermore there are lots of chances in this field so that constrained resources of wireless sensor network can be efficiently used and network utilization can be improved.

REFERENCES

[1] Y. Xiao, V. K Rayi, Sun, X. Du, Fei Hu, and M. Galloway,(2007) "A Survey of Key Management Schemes in Wireless Sensor Networks" Journal computer communications, Vol. 30, No 11-12, pp 2314-2341.

[2] Escenauer L,Gligor vd,(2002)"a key management scheme for distributed sensor networks", conference on computer and communication security proceedings of the 9th ACM conference on computer and communication security,Washington,DC,USA.

[3] Zhu S, Xu S, Setia S, Jajodia S,(2003)"Establishing pair-wise key for secure communication in ad hoc networks A probabilis-tic approach" In Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP'03), Atlanta, Georgia, November 4–7..

[4] Kui Ren, Kai Zeng and Wenjing Lou,(2006)" A new approach for random key pre-distribution in large-scale wireless sensor networks", wireless communications and mobile computing, Vol 6,No 3 ,pp307-318.

[5] Spencer,J. (2000)"The Strange Logic of Random Graphs, Algorithms and Combinatorics", NO.22, Springer- Verlag.

[6] S.Sibi, A. R Thamizarasi,(2013), "Key Pre-Distribution Methods of Wireless Sensor Networks" International journal of Scientific & Engineering Research, Vol 4, No [7]M.Chen, W.Cui, V.Wen, and A.Woo,"Security and Deployment Issues in a Sensor Network",Ninja Project, a scalable Internet services architecture , Berkeley.

[8] Shruthi. P, M. B. Nirmala & A. S Manjunath,(2013)" Secured Modified Bloom's based Q-composite Key Distribution for Wireless Sensor Networks", International Journal on Advanced Computer Theory and Engineering (IJACTE), Vol.2, No.5, pp2319 – 2526.

[9] J.Deng ,Y.S.Han ,(2008) "Multipath Key Establishment for Wireless Sensor Networks Using Just-Enough Redundancy Transmission" IEEE Transactions on Dependable and Secure Computing, Volume 5, No 3, pp 177-190.

[10] Chi-Yuan chen, Han-Chen chao,(2011),"a survey of key distribution in wireless sensor networks", published online in wiley online library.

[11] M.B.Pursle,S.D.Sandberg,(1991)"Incremental–redundancy transmission for meter or burst Incremental-redundancy transmission for meteor-burst communications,"IEEE Trans. on Communications,Vol.39, No.5, pp689–702.

[12] S.B.Wicker and M. J. Bartz,(1994)"Type-II hybrid-ARQ protocols using punctured MDS codes", IEEE Trans. on Communications, vol. 42, no. 2/3/4, pp 1431–1440.

[13] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung,(1992) "Perfectly-secure key Distribution For dynamic conferences," inProc. CRYPTO '92: 12th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag,pp 471–486.

[14] W.Du, J.Deng,Y.S. Han and P.K.Varshney,(2003)"A pairwise key predistribution scheme for wireless sensor networks," in Proc.10th ACM Conference on Computer and Communications Security.

[15] D.Liu,P.Ning,W.Du,(2008)"Group-Based Key Predistribution for Wireless Sensor Networks"ACM Transactions on Sensor Networks, Vol. 4, No. 2.

[16] F.Anjum,"Location dependent key management using random key-predistribution in sensor networks", Proceedings of the 5th ACM workshop on Wireless security. pp 21-
[17]J.Wang,L.Xia,J.Jing,"Analysis for Location-Based Key Pre-distribution in wireless Sensor Networks", proceedings of the 2009 Second International Conference on Information and Computing Science ,Vol. 02 ,pp 297-300.

[18] F.Delgosha,F.Fekri,"key predistribution in wireless sensor networks using multivariate polynomials"0- 03- 9012-1/05/$20.00 ©2005 IEEE.

[19] S.Akhbarifar and A.M. Rahmani,(2014) "A Survey on key pre-distribution Schemes for security in Wireless Sensor Networks", International Journal of Computer Networks and Communications Security, Vol. 2, No. 12, pp 423–442.

[20] M. Javanbakht,H.Erfani, H.H. S.Javadi and P.Daneshjoo,(2014) "Key Predistribution Scheme for Clustered Hierarchical Wireless Sensor Networks based on Combinatorial Design", Published online in Wiley Online Library, Vol. 7, No 11, pp 2003–2014.

[21] Chi-yua chen and Han-Chieh chao ,(2014)"A survey of key distribution in wireless sensor networks", Security and Communication Networks,Vol .7, No. 12, pp 2495–2508.