A Survey of Security in Wireless Sensor Network

Bhawana Singh
Department of computer science and engineering
Uttarakhand Technical University, Dehradun

ABSTRACT
Today, majority of people living in urban areas, Smart city concept become necessary. Smart city refer to the development of communication technologies (ICT), internet of thing (IOT) and provide solution to secure communication in cities. These services provide cities more efficient, confidential and reliable. Internet of network, connecting humans via cellular system, computers via objects or broadband connections and sensor connected via low cost data link. Sensing and communication techniques like wireless sensor network provide services such as monitoring and controlling the living environments. Wireless sensor network used to agriculture monitoring, water distribution, traffic monitoring, military surveillance, health monitoring etc. A wireless sensor network is a wireless network designed by sensor nodes that are spatially distributed and keep track of the physical environmental conditions. Wireless sensor network integrated with IOT and connected globally. This integration brings new threats, such as exposure of sensor node to attacks. In this context, authentication, confidentiality and secure key distribution must be place to end to end secure communication. Security achievement in wireless sensor network and prevention of compromising of node from attacker are important aspect of wireless sensor network .Wireless sensor network security system based on symmetric encryption. The main issues in these approaches are establishment of symmetric keys. Key pre-distribution in network refers, key distribution perform in sensor nodes before deployment of network. In this paper, we propose a new key pre-distribution scheme based on random pre-distribution. Comparative analysis demonstrates that proposed approach provide high security and reduce compromised node ratio.

Keywords
Smartcity, keymanagement,WSN, random key pre-distribution, security issues

1. INTRODUCTION
The world population lives in cities more than 50%and this percentage can be increase 70% by 2050.City infrastructure have many problem that can be solved by communication technology (ICT) and information security. Now days, communication technologies, information security and smart management is important part of smart city development [1].smart city concept include water supply, sanitation, transport system, waste management ,mobility and energy system[2]. Smart city concept includes new communication technology and services to improve the quality of life. Smart city acquired some components such as smart phones, networks, sensors to connect the people with mobiles, computers etc. Information communication technology used in the public place, home, work place, city. Wireless sensor network is a collection of large number of heterogeneous sensor devices that are scattered in large area, connected by wireless media. These sensors monitors physical and environmental conditions such as sound, temperature, vibration, pollution, pressure, air, motion, traffic and collects information to send central location wirelessly. Wireless sensor networks used in many applications such as health monitoring, waste management, animal control and military surveillance. WSN is auspicious technology to access information where sensor node placed. For secure wireless communication keys are needed to encrypt and to decrypt the message. Encryption and decryption are used to provide confidentiality, integrity and authentication. However, when sensor node capture by attacker, message can decrypt by attacker and send to other link of network. This type of attack called node compromising [3].

Symmetric cryptography is commonly used in WSN security. In this, common key share by two nodes for encryption and decryption of exchanged message. Symmetric key establishment is called key distribution [4].

WSN have many key distribution schemes. Two basic approaches are as follows-

- Plain global key scheme(PGK)
- Full pairwise key scheme(FPWK)

The both scheme use key pre-distribution method. These schemes do not require deployment knowledge.

In PGK, all nodes use a unique key. In FPWK, each node share special key with each other node in the network so every possible link have own keys.

PGK require limited memory but security level not high. FPWK has higher security but require large amount of memory and used in small network.

Research in recent years concentrated on key distribution techniques and several new schemes proposed.

- **Key pre-distribution**: There are many approaches for established secure communication between nodes .the most efficient techniques are key pre-distribution.

In this key distribution perform before network deployment. Each sensor node allocated with set of keys from pool of keys in space area before deployment area. For establishing communication link between two sensors node have at least one common key. [5].

Key pre-distribution techniques are depends on orders to provide for efficient result. WSN have some characteristics such as local connectivity, global connectivity and resilience.

In local connectivity, two node share key and establish secure communication. In global connectivity all node connected in network. Resilience, secure path when number of node compromised. Sensor node stores keys for another node.

Key pre-distribution schemes divide into three phases-

1. key distribution
2. shared key discovery

3. path key establishment

During these phase, every node selects secret keys from pool of keys and placed in node, then sensor node discover another node for communication if one or more common keys [6].

Key pre-distribution techniques have main three methods-

1. probabilistic
2. deterministic
3. hybrid

In the probabilistic method keys are selected randomly and placed into the nodes. In deterministic method, keys are selected from the pool using some patterns and placed into sensor node. [7]Hybrid techniques use both methods to select keys.

2. WSN

Wireless sensor network have group of sensor node that are spatially dispersed and sensing the physical environmental condition. Each sensor node Collects sensing information, organize and send to central location. In WSN, sensor monitors environmental conditions like sound, pollution, humidity, temperature, wind, traffic, pressure and so on[8].

Architecture of WSN

WSN consist number of nodes that are deployed in the network. WSN consist sensor nodes that monitors physical environmental condition and route data to sink or base station either through single hop or multi hop techniques [9].The sink or base station makes decision regarding collects sensing information and command send to the network for assign task to sensor.

End users may receive incorrect sensing information if sensor node attacks by attacker and perform decisions. That can be dangerous in some conditions such as battlefield surveillance and environmental monitoring system Therefore, proper security mechanism used to keep network secure [10].

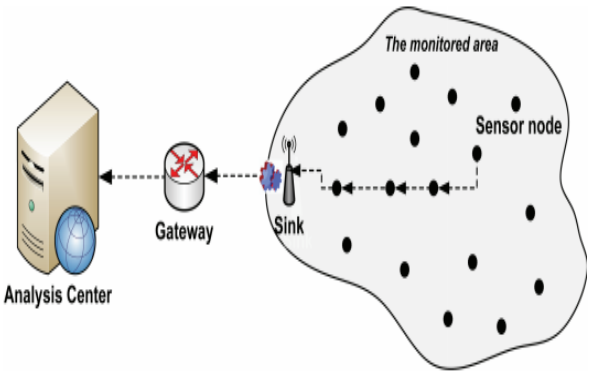

Fig1 architecture of WSN

3. SECURITY *REQUIREMENTS*

Security services in WSN, provides secure communication and prevents data and node from attacks. Most common security require given below:

Data confidentiality: Confidentiality ensures that unicast, multicast, broadcast messages should understand by expected recipient.

Data integrity: Integrity ensures that no message can be alter when message traverse sender to the receiver [11].

Authentication: This requirement ensures that data send by actual user and receive by expected user. Authentication ensures that communication must be performing between source and destination [12].

Availability: Data availability in WSN refer that sensor nodes have ability to sense and monitor network when communication channel present or not. Node periodically sends sensing information to sink node or base station, when sink node ask for data [13].Availability is important requirement of WSN because without data availability node cannot perform any task.

Data freshness: Each time every node in network sense new data. Data freshness ensures that data is organized in proper manner and data must be fresh.

Self-Organization: Each sensor node in WSN must have basic property such as Self-Organization and Self-healing. These features of WSN have security challenges .WSN is dynamic in nature so pre-installation of sharing key is impossible. In context of symmetric encryption WSN used a number of pre-distribution techniques. WSN is an Ad-HOC network which has no fix infrastructure means every node is independent in network. Thus, there is chance of attack increase in WSN.

Secure Management and Localization: WSN have number of heterogeneous node and sensing information. Co-ordination of node and management of sensing data is very essential for network. In WSN, sensor node transmitting sensing data and sink node store it. Sensor nodes automatically and correctly locate in WSN because when network is in fault condition and capture by attacker then accurate location of sensor node detect defective node and take decision accordingly.

Time Synchronization: WSN another most important security requirement is time synchronization. WSN have number of sensor nodes which continuously sense physical environmental condition and sensed data send to sink node thus each node perform its task within time because some task and computation require sequential execution in network.

Non –Repudiation: sensor node cannot deny transmitting of data even if data sent previously.

4. ATTACKS IN WSN

Sensor networks are suffered from various types of attacks. These attacks are categorized basic of different layers are given below:

1. **Attacks at physical layer**
   - Jamming: jamming occurs when external entity attacks sensor node with interference of radio frequencies that node used in WSN for communication [14].
   - Tempering: If node is compromise by attacker called tempering. It is also called node capturing. In this, sensor node physically modifies and destroys. Its program code and circuitry modify or node replace by defected node [15].
2. **Attacks on Link Layer**
   - Collision: Collision occurs when two nodes transmit packets on same frequency simultaneously. If packet collides, they are retransmitted or discarded [16].

- Exhaustion: compromise node consumes energy more than require by r89epeatedly sending of messages.

3. Attacks on Network Layer

- Selective forwarding (SF): All nodes in network will forward or receive messages to base station or sink node in multihop techniques. In this, corrupt node is created by attacker that drops some necessary messages intentionally when messages forward. Multiple path use in network to rout data from defense against attacker.

- Sinkhole attack: An attacker create corrupt node look better than other node in the network so nodes choose defected node to transmission of data [17].

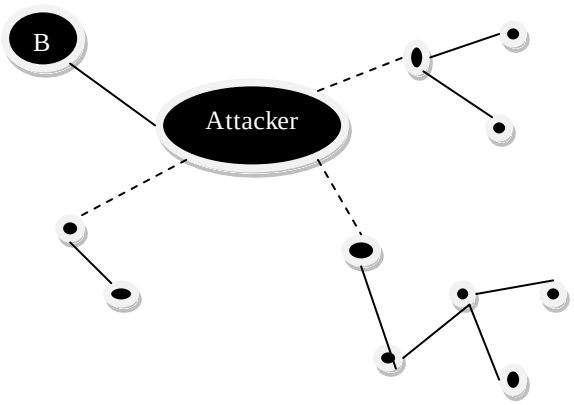

Fig 2 Sinkhole attack

Attacker continuously listen to requests for packets routes and insert wrong information between the communication nodes.

- Sybil attack: In this type of attack two or more than two node has same identity in the network. It is also known as clone attack [18].Clone node can drop data and send false data in network.

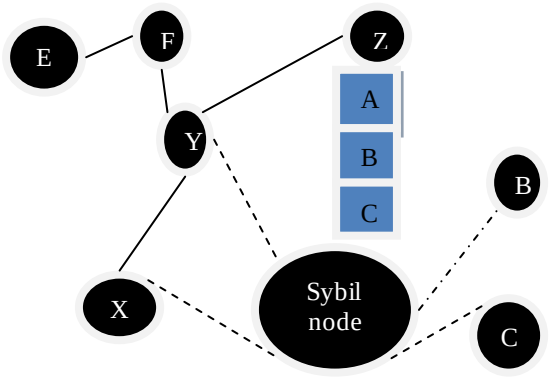

Fig.3 Sybil attack

- Acknowledgement spoofing (AS): When attacking node send wrong message to other node called acknowledgement spoofing.

- Wormhole Attack: In Wormhole attack communication disrupt in network. Packets capture by attacker in one location in network and tunnel them to another location which distributes them locally. The tunnel is either frequency link or wired link. It consist one or more defected nodes and a tunnel establish between them[19] This tunnel creates illusion that two end location of tunnel are close to each other.

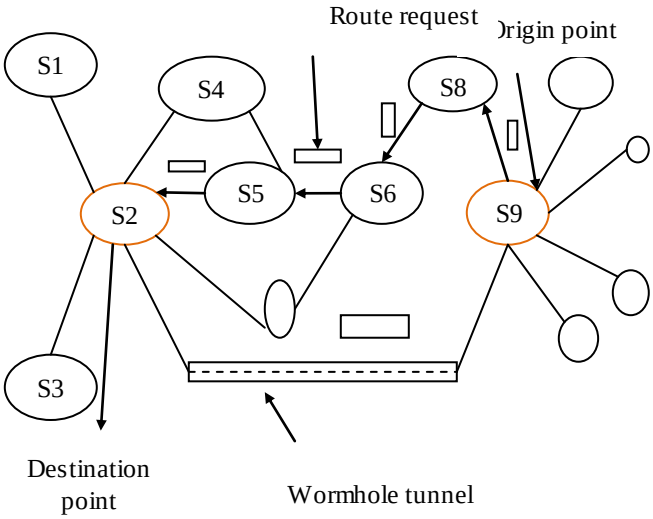

Fig.4 Wormhole attack

4 Attacks on Transport Layer

- Flooding attacks: it is a Denial of service attack (DOS).In this, network or node weighted down with packets or requests that send by attacker thus genuine connection request not processed. By flooding node buffer memory fills by attacker and once memory is full, no further connection cannot established thus results a denial of service attacks[20].

- De-Synchronization: When existing connection disrupt called De-synchronization.

Table: 1 attacks on WSN and countermeasures

Protocol Layer	Attacks	defenses
Physical	Jamming	Spread-spectrum, priority message, lower duty cycle, region mapping, mode change
	Node tampering or destruction	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	unfairness	Small frames
Network	Neglect and greed	Redundancy, probing
	Homing	Encryption, dummy, packets
	Misdirection	Egress filtering, authorization, monitoring

	Spoofing replaying, or altering routing control traffic and clustering	Authentication and antireplay protection secure cluster formation
	Selecting forwarding attack	Multipath routing
	Sinkholes	Geographic routing protocols
	Black holes	Authorization, monitoring, redundancy
	Sybil	Code attestation, resource testing, location verification ,key-based authentication
	Wormhole	Packet leashes, monitoring
	Hello flood	Pairwise authentication Geographic routing
	De-synchronization	authentication
Application	Overwhelming sensors	Sensor tuning Data aggregation
	Path based DoS	Authentication and antireplay protection, Authentication streams

5. TERMS AND NOTATIONS

We list the terms and notation in the paper below:

- N is the number of sensor nodes
- N' is the number of expected neighboring sensor node within communication range
- P is size of key pool.
- R is the number of key in a sensor node's key ring before deployment
- D is the expected number of secure links that are directly connected during key setup
- C is number of node attacks
- P_c is entire network connection probability after completing key setup.
- P' is probability of common keys of two node
- | is concatenation operator
- K_{PQ} is pairwise key establishment
- H(.) is one way hash function

6. KEY PRE-DISTRIBUTION SCHEMES

There are many types of key pre-distribution schemes for secure communication between nodes in network. In this scheme some set of keys are assigned to each sensor node before their deployment. After deployment of sensor nodes, at least one common key need sensor node for establish communication link with other sensor node.

In this section, we introduce types of key pre-distribution schemes in following subsections.

***A*. Random key pre-distribution scheme:** First random key pre-distribution presented by Eschenauer and Gligor[21].This scheme also called as basic scheme. In EG, key distribution is divided into 3 phases: key pre-distribution, shared –key discovery and path-key establishment [5].

I. Key Pre-distribution phase: A large key pool containing P keys and their identity are generated before deployment. Then set of R keys are selected are randomly selected from key pool and stored in sensor node memory. This set of R keys called key ring. The value of P and R defined the probability of setup a link between two nodes and number of secret keys that an attacker can get by compromising a node. Only a few keys stored in each node memory in a large size of network, so save storage space. These few keys are enough to share common key for establish communication link.

II. Shared key discovery phase: Once a node allotted with keys, they are placed in appreciated area where sensors needed such as hospitals, battlefield, traffic monitoring etc. Each node searches its neighbor which share at least on common keys for communication after deployment. There are many approach to know about whether two node share common key or not. The basic approach is that node broadcast their identifier list to other sensor nodes. If node share common keys, establish secure communication.

III. Path key establishment phase: A communication link establish only if they share one or more common keys .Path establishment phase provide communication link if node not able to share common keys. Eg. Node P wants to communicate with node Q but they not share common key. Now node P send message to R ask that it want to communicate with node Q. Then message encryption performs by common keys which shared between node P and node R. If node Q and R have share common keys then pairwise keys generate by node P and Q.R act like as key distribution center. After completion of key discovery phase, number of unused keys remaining in each node keys ring. These remaining keys are used for path establishment.

Necessary expected node degree D is calculated by Eschenauer and Gligor in terms of network N as:

$$D=(N-1)/N(\ln(N)-\ln(-\ln(C)))$$

From the formula D=O(log N).

***B* Q-Composite Random Key Pre-distribution Scheme:** In basic scheme, one common key needed by sensor node for establishing a secure communication link in the key setup phase. The subsequent scheme based on basic scheme is the Q-Composite random key pre-distribution [22] where at least P' common key necessary for setup communication link between nodes .In this scheme, R>1 then increase the number of keys

overlapping, so attacker face difficulty to break down the communication link in network. Size of key pool is increases and size of key ring in each node decrease. According to analysis [22], if small number of node is compromised, Q-Composite random key pre-distribution scheme provide higher level of security than EG. In the key pre-distribution phase of Q-composite scheme set of R keys are randomly selected from the P size key pool and store in each node's key ring. In the shared key discovery phase, node search common key for communication link establishment by using many type of methods. With this method, common key search by each node either transfer key identifier and or by selecting puzzle such as Merkle puzzle [23].In Merkel puzzle method, each key associate with puzzle to its entire neighboring node that issues by node. When node resolve the puzzle and give accurate answer then a path key established.

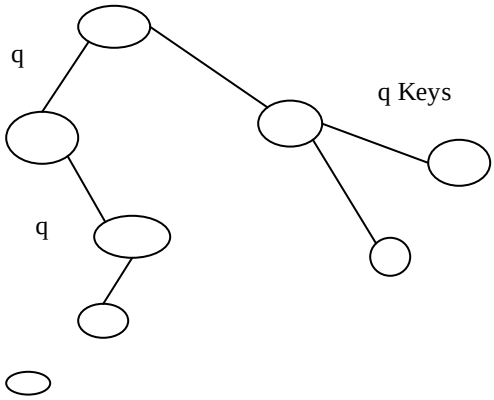

Fig.5 Shared key discovery and path key establishment

This scheme provides high security. Communication link establish when both node having q common keys. This scheme provide better resilience if nodes deploys in small network. Node cloning not handles by this scheme. For large network where key established and use any time composite modified bloom's distribution scheme is proposed. Bloom's distribution scheme is provide better resilience. In this Scheme pair wise key established which use single key space. The Bloom-based structure is modified that use numerous key spaces. In Improved bloom's q-composite distribution scheme generate pairs of common secret keys space to establish a link[24]. This scheme provides better solution for memory, scalability and good resilience in large network.

C Multipath key Reinforcement Scheme:

In basic scheme secret keys are randomly picked up from the key pool, communication link is not highly secure. When node is compromise by attacker it increase number of node threaten in network. So, secret keys should be updated when one node in compromise by attacker in network. This is implemented by using multiple paths in network for high security. If node X needed update keys with other node Y then uses all possible disjoint path to node Y. Suppose that there are L disjoint paths between X node to Y node and X produce K random values (k1,k2,k3…..kn).Each random values encryption key size is equal and transmit them into all possible disjoint paths to node Y[25]. After receiving of K random value by Node Y, It generates new encryption keys at same time. X node produce new secure communication path with M'= M+k1+k2+k3+…kn. Where M is the original keys.

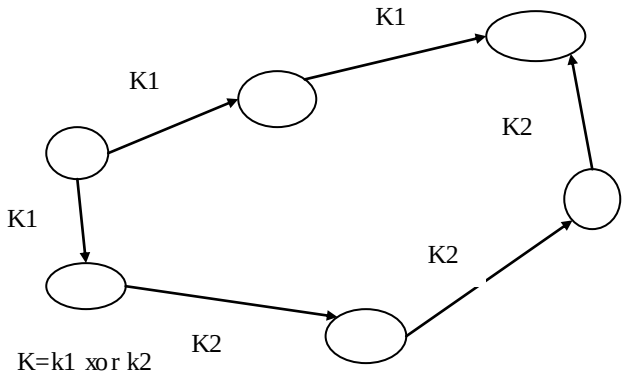

Fig 6 Multipath key reinforcement scheme

In this, attacker can only decrypt the information of compromise node and all other node is generating new keys. Greater number of K random values provides high security of new communication link.

If network size is greater, attackers have chance to eavesdropping and make communication link insecure. So 2-hop scheme of the multipath key reinforcement techniques introduced which contains only two paths and minimize the path length [26].

The Multipath key reinforcement scheme provides greater security than Q-composite technique but it create communication overhead which reduce battery life .In this, increase the possibility of denial of service attacks.

***D* Random Pairwise Key Scheme**

Random pairwise key scheme provide higher security than Q-composite or multipath scheme. It is extended version of pairwise key pre-distribution scheme. It overcome drawback of pairwise key scheme. Pairwise key scheme provide resilience to node cloning and node to node authentication but it only use for small size of network. If network size N, minimum connection possibility of two nose is P_c and number of keys are P thus $P=N*P_c$ [27].

Initialization and key Setup: In this scheme, node's key ring size is R keys and two nodes communicate with possibility P. In the initialization phase unique node identity generated that are n=R/P. Unused identity of node in network used in the future .Each node identity in network compared with another node identity that selected randomly then pairwise key makes by every pair of nodes. After completion of key generation, both nodes key ring stores new key and id of another node. After deployment of nodes, each node broadcast its identity to its immediate neighbors. Node search identity of neighboring node from their key ring and communicate if they share a common pairwise key. Cryptographic handshaking perform for Verification of key between nodes for establishing communication. If increase communications range the neighbors will be increase thus network size will be increase.so chances of denial of service attack can be increase [28]. Attacker introduce defected node which generate number of node identity randomly and flood network with rebroadcast identities. This type of attack can be minimizing by reduction of node which used for range extension.

Node revocation: Base station maintained node revocation in random pairwise scheme of key Pre-distribution scheme. Compromised node revoking in network used to avoid various types of attacks such as denial of service attacks, defected node inserting etc. If base station use performs node revocation in

network process may be slow because of high latency in sensor node communication. To overcome the drawback, a distributed node revocation scheme introduce for random pairwise scheme. Such scheme is possible if we assume that existence of mechanism where each sensor node enable to detect compromise node in network.

If node P detects that Q node to be compromised then it broadcast public vote to neighboring node against node Q. If P node observes that another node broadcast public vote against node Q in network then node P will disconnect its entire communication link with node Q. This process performs until all nodes disconnect their communication link with node Q in network. Therefore node Q deleted from network. Node that vote against node Q called the voting member of node Q .Here node share K pairwise keys with all other nodes thus there are K voting members of node Q[29].

***E* Polynomial pool based key Pre-distribution**

In this scheme, a pool of bivariate polynomials is generated randomly. Generation of bivariate polynomial mechanism is dependent on the polynomial pool based pre-distribution. In the key pre-distribution phase, setup server generates set of bivariate polynomial then each polynomial is assigned with particular identity for server. Server selected subset of polynomials and send to each sensor node in network.

In the key discovery phase, by sharing of similar polynomials sensor node find another node and generate common key. Polynomial pool-based scheme provide high security and flexibility compare to other schemes .This scheme can include large size of network.[30] The main challenge in this scheme is that two sensor node share same polynomial or not.

Polynomial pool has two approaches:

- Only one polynomial stores in polynomial pool
- All polynomials are 0-degree, polynomial pool generate keys pool just like EG scheme and Q-composite scheme.

Random Subset key Pre-distribution: In random subset key Pre-distribution polynomials are randomly selected from polynomial pool and assigned to each sensor node in network. In this each node creates unique pairwise keys which based on node's id .The random subset scheme working having same as polynomial pool base scheme in the three stages of key establishment. In the key pre-distribution phase, set of bivariate polynomial creates by setup server and assigned to each node in network. In the key discovery phase, each node determine the node with which share common key by using real time discovery approach as keys not pre-loaded before deployment. In the path key establishment phase, if and intermediate node shares common key with both source node and destination node then a source node send a message to mediator node to establishing a connection with destination node[31]. Communication link established between source nodes to destination node.

F. Group-Based key pre-distribution

In the group-based key pre-distribution scheme, same type of sensor node group establish pairwise key with each other. In this scheme all the node group in network shares a group key. Base station use group key to send message to all other group node. A key pre-distribution categorized into three parts:

- Pre-distribution
- Direct key establishment
- Path key establishment

A network consist N number of sensor nodes .this scheme involves constructing an m*m grid and 2m polynomials sets. m is the value of square root of N[32].

Deployment group Gi, key pre-distribution instance Di for establishing of pairwise key in Gi.

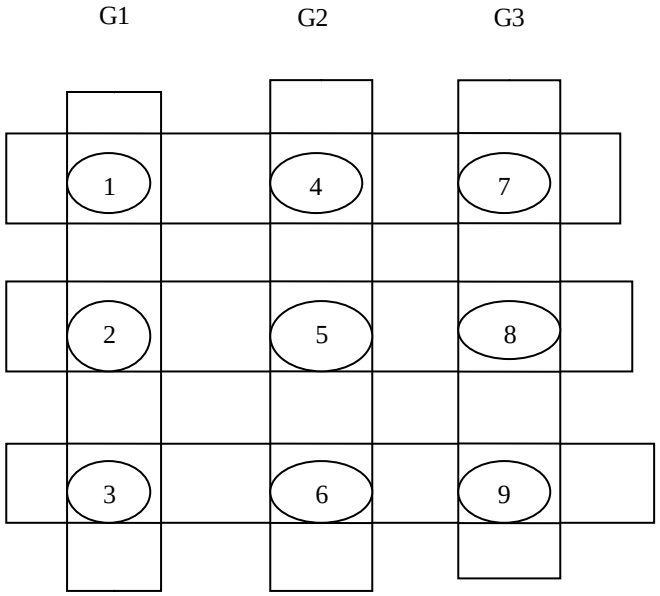

Fig.6 Group Construction

Group construction is needed to establishing pairwise keys between nodes.

Pre-distribution: In the first stage, bivariate polynomials create by setup server and assigned to each node in grid.

Direct key establishment: After the pre-distribution stage, direct key establishing between neighboring sensor nodes.

Path key establishment: When sensor node cannot establish a direct key then use path key establishment. In this searches the sequence of nodes to establish an indirect key. If node want to establish communication link with other node, it find for common rows and columns. By using row and column matches' polynomial shares, pairwise key established. If row and column not matches nodes find alternate path. In this scheme, source node and destination node have many numbers of intermediate nodes or many alternate paths [33].

E. Location Dependent key Management Scheme:

In location key management scheme, communication link establishment only depends on location of nodes in network. This scheme only used for static sensor network. Sensor node communicates with other sensor nodes via encrypted channel. Nodes can join network anytime. In this scheme some special node used which called as anchors node [34]. Anchors node transfer message at different level of power and these are tempering proof.

- Pre-deployment phase
- Initialization phase
- Communication phase

In key distribution phase, key server generates set of keys and placed into key pool then key subset loaded into each sensor node. Common key which share by sensor nodes for establish communication link. Anchor node not receive key from pool.

The anchor nodes and nodes are arbitrary scatter. Anchor node send beacon to other sensor node .After receiving beacon by sensor node generate new keys by using old keys and beacon message. After generation of new keys, original subset of keys and common keys which share by node are deleted from sensor node memory. Field is divided into same size cells and each cell assigned a single bivariate polynomial arbitrarily [35].

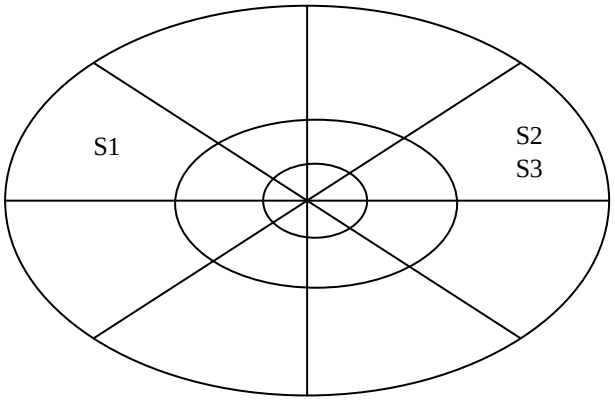

Fig.7 dividing field of an anchor node to 8 non-overlapping sectors

7. CONCLUSION

Security is an essential requirement for WSN, which is very challenging task .In this paper, we discuss a brief review on WSN, attacks and key distribution techniques for achieving security. The attacks in network mainly target the security goals such as integrity, authenticity, availability and confidentiality. Most of attacks in WSN are caused by the compromise nodes which insert false information in network. However, developing such detection mechanism and secret key mechanism is a great research challenge.

8. REFERENCES

[1] Meshal Alansheet.Imad F.T. Alshekly Abdul Rahman Alkandari.”smart city survey”june 2012.

[2] Schaffers H,Komnios N.,Pallot M.,Trouses B.,Nilsson M.,Oliveria A. “Smart Cities and the Future Internet:Towards Cooperation Frameworks for Open Innovation”2011.

[3] mohammed-Lamine Messai, Hamida Seba ” A Self-healing key pre-distribution scheme for multiphase wireless sensor networks,” 2017

[4] Saurabh Chandra, Sidharth Bhattacharya,Smita Paira SK Asfikul Alam “A study and analysis on Symmetric cryptographic” 27-29 november 2014.

[5] Y.xiao,V.K Rayi,Sun,S.Du,Fei Hu and M.Galloway”A survey of key management schemes in WSN,2007.

[6] Wu Haibing,Chen Dong,LiuPing,Li Mingxi,Yuan Hongwei Gao Haomin”WSN key Distribution Method Based on PTPP,11-13 july 2014.

[7] M.A.Simplicio-jr.,P.S.Barreto,C.B.MargiaT.C.Carvalho. ”A survey on key management mechanisms for distributed wireless sensor networks,2010.

[8] I.F.Akyildiz,W.Su,Y.Sankarasubramaniam,and E. Cayirce," Wireless sensor networks :a survey,March 2002.

[9] D.Estrin.”Instrumenting the world with Wirelsess Sensor Networks”May 2001.

[10] Yong Wang Garhan Attebury,and Byrav Ramamurthy,”a Survey of security issues in wireless sensor networks,2006.

[11] J.Alemdar,C.Ersoy,”wireless sensor networks for healthcare:A survey,”computer networks,2010.

[12] Mayank Saraogi,”Security in Wireless Sensor Network”,University of Tennessee,Knoxville.

[13] Hung,X,L,et al.,”An Energy-Efficient Secure Routing and key Management Scheme for Mobile Sinks in Wireless Sensor Networks using Deployment knowledge,2008.

[14] E.Shi and A. Perrig,”Designing secure sensor networks”,Wireless Communication Magazine, December 2004.

[15] X.Wang,W.Gu,K.Schosk,S.Chellappanand D. Xuan,” sensor network configuration under physical attacks”,Ohio State university,july 2004.

[16] Y.Zhou,Y.Fang and Y.Zhang:security wireless sensor network:A survey ,Ieee communication Surveys,2006.

[17] AI-Sakib Khan Pathan,Hyung Woo Lee,Choong Seon Hong,”Security in wireless sensor Networks:Issues and Challenges”,ICACT,February 2006.

[18] J.Newsome,E.Shi,D.Song and A.Perrig,”The Sybil attack in sensor networks:Analysis and defenses”,2004.

[19] C.Karlof and D.Wagner,”Secure routing in wireless sensor networks,IEEE Computer,2002.

[20] Sumitra, B.,C.R.Pethuru,and M.Misbahuddin.”A survey of cloud authentication attacks and solution approaches.”International jpurnal of innovative research in computer and communication engineering, 2014.

[21] V.Gligor and L.Eschenauer”A key-management scheme for distributed sensor networks,”in Computer and communication security ,2002.

[22] H.Chan,A.Perrig and D.Song ,”Random key predidtribution schemes for sensor networks ,”in symposium on security and privacy,mayn2003.

[23] Cui,V.Wen, M.Chen,W. and A.Woo,”security and development issues in a sensor network,”Ninja project,A scalable Internet services architecture,Berkeley.

[24] B.Zhou,Q.Li,S.Li,X.Wang and X.Sun”an efficient and scalable pairwise key predistribution scheme for sensor networks using deployment knowledge “computer communication ,2009.

[25] Y.S.Han, J.Deng ”Multipath key establishment for wireless sensor network using just enoughredundancy transmission “IEEE Transaction on dependable and secure computing,2008.

[26] S.D.Sandberg,M.B.Pursle ”Incremental redundancy tans-mission for meter or burst incremental –redundancy transmission for meteor –burst communication ,”IEEE Trans. communication ,1991.

[27] S.B.Wicker and M J.Bartz”Type-2 hybrid –ARO protocol using punctured MDS codes”.IEEE Trans. on communications, 1994.

[28] W.Du,Y.S.Han,J.Dengand“A pairwise key predistribution scheme for wireless sensor networks,in Proc .10th ACM

Conference on computer and communication security,2003.

[29] C.Blundo,A.Herzberg,A.D.Santis,S.Kutten,U.Vaccaro and M.Yung"perfectly-secure key distribution for dynamic conference"inProc.CRYPTO'92'12th annual international cryptology conference on advance in cryptologylondon,Springer,1992.

[30] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," Proc. of the IEEE InfoCom,2005.

[31] Chin-Luang Lei, Yen- Hua Liao AiNung Wang and Wen-Chi Tsai, "Tame Pool based Pairwise Key Pre-distribution for Large Scale Sensor Networks", February 2011, National Taiwan University.

[32] Liu, D., Ning, P "Establishing Pairwise keys in distributed sensor networks", In Proceedings of 10th ACM Conf. on Computer and Communications Security (CCS'03), 2003.

[33] Wood, A.,Stankovic, J. A., "Denial of Service in Sensor Networks", IEEE Computer, pp. 54-62, October 2002.

[34] Huang, D., Mehta, M., Mehdi, D, Harm and L. "Location-aware Key Management Scheme for Wireless Sensor Networks", Proc. of 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks. October 2004.