Coordinates based Keying Scheme for WSN Security

Sweety Dhureja[1], Kailash Patidar[2]

[1]Research Scholar, CSE Dept. SSSUTMS, Sehore, MP, India
[2]SHead of Department, CSE Dept. SSSUTMS, Sehore, MP, India

---***---

Abstract - Wireless sensor networks (WSN) are capable of work in a vast range of communication/sensing application while it uses radio frequencies to communicate with each other. Data is shared using public radio communication channel from which one can steal information. For protecting data in WSN cryptography is the key methodology that almost every WSN incorporate in Network. The paper here presents a conceptual approach for cryptographic key distribution scheme that depends on physical location of WSN node of network. Presented keying scheme is a pre distributed key scheme while node calculate the encryption key based on public identifier that are stored in node internal memory.

Key Words: WSN, Network Security, Cryptography, Key Distribution Scheme, Global Positioning System (GPS).

1. INTRODUCTION

Wireless sensor networks is the group of individual sensors nodes that collectively work to sense dedicated field's physical conditions like temperature, humidity, sound etc. A sensor network is Ad-Hoc in nature and limited to resources connected to it. A sensor node is comprises of some controller unit, memory element, sensing element, radio wave communication unit, and power supply that collectively perform some task of sensing in network. Sensor nodes are limited to power constrains and memory due to its low size requirement in application. A sensor network is meant to share sensing information among each node and to the sink node of network. A sink node is the central node that is responsible to communicate, collect, and control the network controller receives information form sensor node a controller unit maybe automatic or semiautomatic mechanism that control the entire sensor system using the same sink node[1] [3].

Figure 1 shows a basic structure of WSN in which communication from sink node to sensor node F has been established using wireless links [3]. The most important part of a WSN is communication which is wireless radio waves that are openly available in nature and this information can be stolen by any unauthorized person or attacker in network. This information should be protected by means of some security features in addition with basic communication methodology and principles.

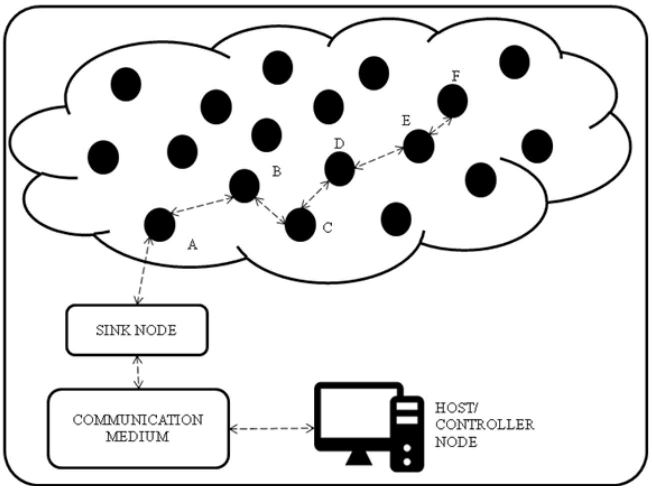


Fig -1: Basic Structure of WSN

There are various researches in the field of network/ information securities have been carried out and are discussed below. Security in each types of network is essential from development phase of network ARPANET till now [2]. The primary objectives of security standard are known as CIAA (Confidentiality Integrity, Authentication, and Availability). First is Confidentiality: To conceal a message from passive attackers while message communicated throughout sensor nodes in network is the most important aspect of network security. A sensor node must not leak its data to its neighboring unauthorized nodes. Second is Integrity: It is intended to be detecting that the message sent has not been tempered, altered or changed. Even after data confidentiality has been maintained it is still possible to alter information to generate a false result. Third is Availability: It determines node ability to use the resources and the network availability to for the message to communicate in network. Fourth is Authentication: it ensures the origin and identification. There are two different mechanisms symmetric and asymmetric with the help of which data authentication is maintained [4]. These are primary objective of any security system while there are some secondary goals that make more secure communication system; these are Data Freshness, Time Synchronization, Self Organization, and Secure Localization. These are some additional security features that ensures about data secrecy.

2. WSN ATTACKS

WSN's are prone to attacks are due to the broadcast nature of communication medium and also due to nodes are placed in dangerous or hostile environment. Attacks are primarily classified in active and passive attacks and Figure 2 shows attacks in WSN. Node Outage: It is the situation in which node stopped functioning. Node Replications Attack: In this type of attack a node new node is added into network while copying any other nodes identity. Physical Attack: As sensor nodes are placed in remote and hostile outdoor environment and so it is prone to physical attacks that include node/sensor damage battery drain etc. Message Corruption: If any message is affected alteration attack its integrity is compromised. Node Malfunctioning: In some cases nodes may produce inaccurate data which compromises with integrity of data in the network. Node Subversion: In such case a particular node may capture and cryptographic key information can be stealing by attacker. Denial of Service: It is the unintentional failure of nodes in the network DoS are of various types in various layers of operation. Routing Attacks: This type of attacks are related to network layer of communication protocol and it may break the entire network system these are of various type few of them are Selective Forwarding, Sinkhole Attack, Sybil Attack, Wormhole Attack etc. These are the attacks that a WSN may face normally and thus affects the entire network or a part of network [6].

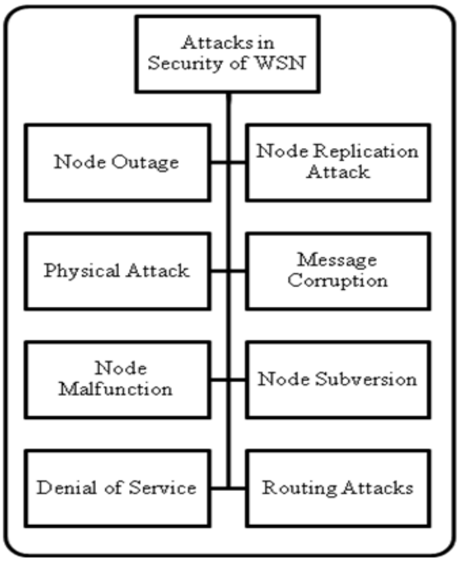


Fig -2: Attacks in WSN

3. SECURITY MECHANISM

Mechanism to sense, prevent and recuperate from security attacks are known as security mechanism. A wide range of secretary management mechanisms are available these are broadly divided into two classes low level and high level figure 3 shows the generalized classification of security mechanism [5] [7].

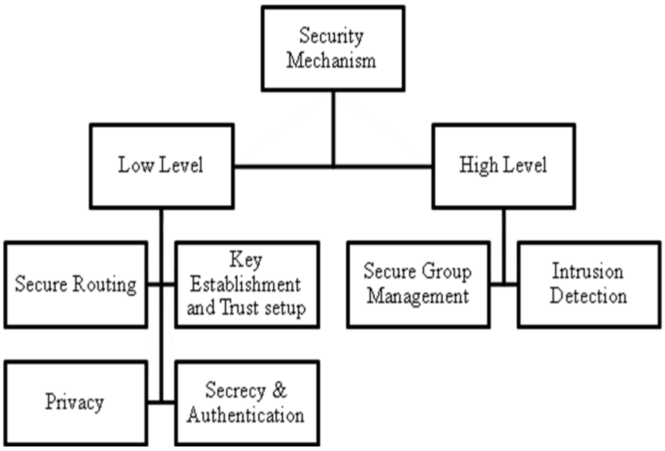


Fig -3: Security Mechanism

- Low Level: low level security primitives are discussed here; Secure Routing: it is the most crucial part of any network it includes routing and forwarding of data by injecting a false detail of destination node to improve this simple authentication may remove the chance of routing error. Key Establishment and Trust Setup: while setting up any network a cryptographic key establishment is needed this will ensures data secrecy and node trust. Secrecy & Authentication: while maintaining secrecy cryptography is the key defense technique, with the help this data authentication and secrecy is maintained. Privacy: like many other networking system a sensor network should also be forced to maintain privacy of network and nodes too [5] [7].

- High Level: high level security primitives are discussed here. Secure group management: each node in WSNs are limited to computing an communicational capabilities however group nodes may collectively perform data aggregation and analysis while these nodes are changing continuously. Some secure network management some sort of secure group communication and key computation is required with the help which group communication secrecy is maintained. Intrusion Detection: a network must be capable of detection of any intrusion in network sub group communication using a group communication key can be a promising approach for this [5] [7].

4. CRYPTOGRAPHY AND CRYPTO KEYS

It is the process of converting a plain text data word into a cipher text is known as cryptography. Cryptography is done by applying some mathematical algorithm that produces a scrambled output of any input data this scrambled data is then transmitted through communication channel [8]. On the other hand recipient node decrypts the scrambled data to find actual data. These processes are synchronized by means of a keying mechanism the data is encrypted and decrypted using the keys assigned to it. These keys are known as crypto keys. A data encryption/decryption may be done by same key or may have different key on the basis of key cryptography is divided into two parts. Symmetric (i.e. same key for encryption and decryption) and asymmetric (i.e. different key for encryption and decryption). Figure 4 shows a basic cryptosystem [9].

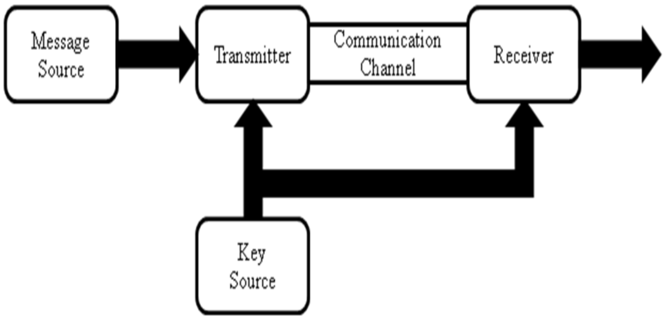


Fig -4: Basic Crypto System

5. KEY DISTRIBUTION SCHEME

There are two different types of keying system first is pre distribution key and post deployment. In Pre-distribution keying scheme, key to each node is distributed before the deployment of network to all nodes in the network. Second is Post-Distribution keying scheme, in this type of key distribution scheme individual nodes are provided by its nearby nodes key and a group key in the network [10]. Moreover there are various keying scheme that that fall into these two main classes, these are: Quantum Key Distribution (QKD), Matrix Based Key Distribution, Group Key Distribution, Blom's key distribution scheme etc. Few of them are discussed in this section. Random Key Distribution: It is a pre-distribution keying scheme in which a set of random keys are selected from the pool this set is known as key-ring tow nodes may share one or more key by the virtue of which data is encrypted in and sent in the network. From the key ring a path key is generated and is defines the data flow in the network [11]. Group Key Distribution scheme: in this type of cryptosystem a secure key is shared within the group of nodes and is sub divided by physical address or other keying subsystem in the network [12]. Blom's Key Distribution Scheme: it is a symmetric keying system in this cryptosystem a key is supplied by a secure key provider between source and destination node in the network to make a channel to share data.

6. COORDINATES BASED KEY SCHEME (CBK SCHEME)

In this section a new key distribution scheme is discussed. CBK scheme is fall into the pre distribution key model this keying system is depends on networks physical size governed by GPS coordinates of network, and limited to static type architecture of network. There are two phases in this type of keying crypto system these are Setup Phase and Communication Phase.

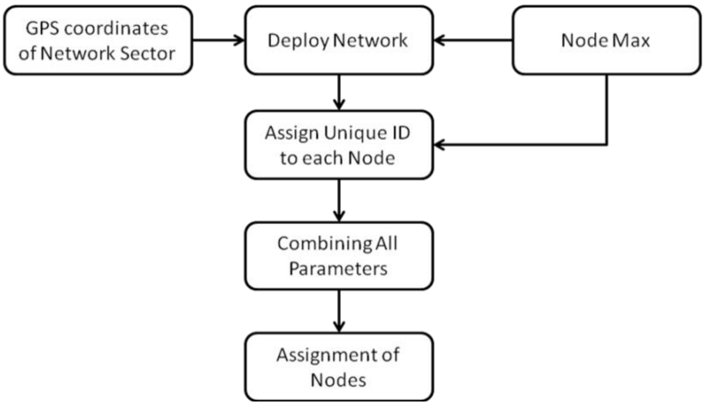


Fig -5: Setup Phase of Network

Figure 5 shows the network setup phase, first key generation and node assignment is done by network it first requires the GPS coordinates of network sector and maximum number of nodes that will be active part of network. After both input from developer key for each node is generated that includes the required parameters and unique identification of node. This generated key is then assigned to nodes into the network. Second phase is communication phase which is subdivided into two phases first is encryption key generation and data transmission shown in figure 6, and second is Decryption Key and power calculation phase shown in figure 7.

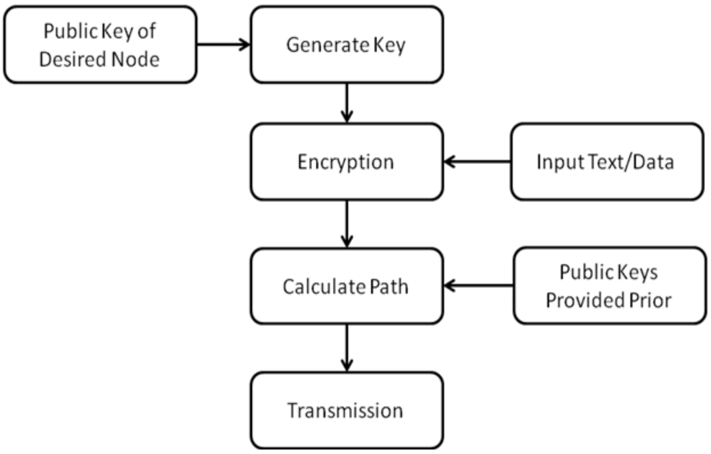


Fig -6: Encryption key generation and data transmission

Phase 1: First of all it takes public key of destination node and then it generate encryption key, in this stage node replaces personal identification details from its private key with the public key of destination node. Then it takes message and then converts it into cipher text. After which path calculation is done from which the communication takeplace.

Phase 2: In this case receiver receives data and decrypt using the private key of node, converts cipher data into plain text figure 7, shows the decryption system.

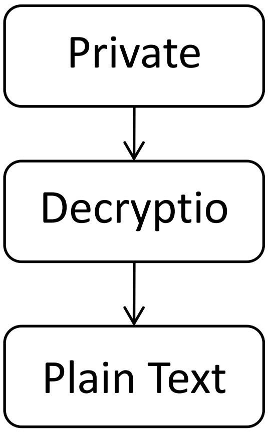
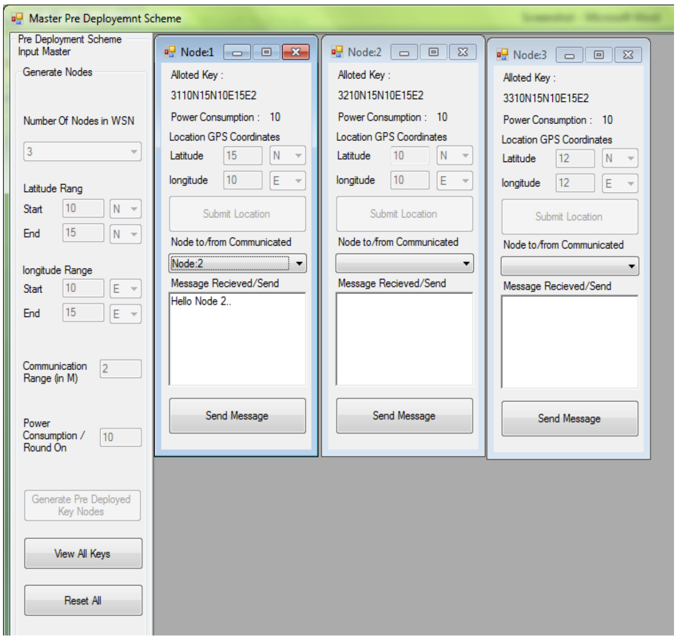


Fig -7: Decryption

To represent the idea of physical keying system the entire keying scheme we have developed a software representation of WSN is shown in figure 8 in which physical parameters coordinates are entered manually by developer and select the number of nodes into the network after this developer has to click on deploy network button which results in sub windows representing Nodes into the network which has its own physical location range input that defines the location of node after filling details of all nodes network is fully setup and after that message can send while message has been typed into Message Receive/Send Textbox and then click on Send Message Button. Figure 9 shows the communicated message which encrypted by Node 1 and decrypted by Node 2 by using DES encryption and decryption algorithm using that uses a 24 bit long encryption and decryption key that has generated by CBK scheme.


Master Pre Deployemnt Scheme
Pre Deployment Scheme Input Master
Generate Nodes
Submit Location
Send Message
Generate Pre Deployed Key Nodes
View All Keys
Reset All

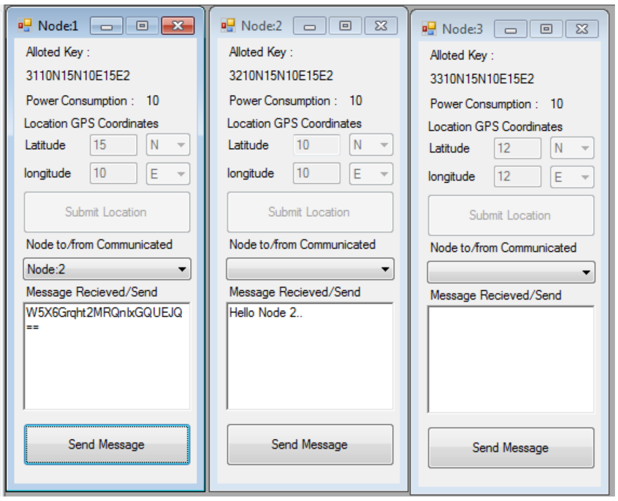
Number Of Nodes in WSN: 3
Latitude Rang Start: 10 N, End: 15 N
longitude Range Start: 10 E, End: 15 E
Communication Range (in M): 2
Power Consumption / Round On: 10

Node:1 Alloted Key : 3110N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 15 N, longitude 10 E, Node to/from Communicated: Node:2, Message Recieved/Send: Hello Node 2..

Node:2 Alloted Key : 3210N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 10 N, longitude 10 E

Node:3 Alloted Key : 3310N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 12 N, longitude 12 E

Fig -8: Fully Setup Network



Node:1 Alloted Key : 3110N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 15 N, longitude 10 E, Node to/from Communicated: Node:2, Message Recieved/Send: W5X6Grqht2MRQnlxGQUEJQ ==

Node:2 Alloted Key : 3210N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 10 N, longitude 10 E, Message Recieved/Send: Hello Node 2..

Node:3 Alloted Key : 3310N15N10E15E2, Power Consumption : 10, Location GPS Coordinates Latitude 12 N, longitude 12 E

Fig -9: Data Received

Table -1: comparative overview of CBK scheme with other schemes

S No	Features	Our System	DES	3DES	BLOWFISH	CAST-128
1	Key Length	Variable according to Encryption Technique used	56 Bits	168 Bits	32-448 Bits	128/ 256 Bits
2	Location Parameter with Key	Yes	No			
3	Keying Type	Mixed in Nature	Pre-distribution			
4	Addition of new node Flexibility	Complete reconfiguration required	Runtime			
5	Post Network Deployment key calculation	Yes: Using unique name of source	No			

7. CONCLUSION

With table 1 we have concluded CBK. The advancement and limitation of CBK approach that uses physical location parameters while limited in terms of node addition and substitution as network is completely fixed in terms of node location and field size. The main idea behind CBK scheme is pre-deployment of encryption and decryption keys while CBK uses a mixed approach for key distribution, in CBK private key and public identifiers are pre-distributed to all nodes each node is then generate a key similar to private key of destination node and encrypt and sent to destination node.

8. FUTURE SCOPE

CBK scheme is tested and applied using software application which is slightly differ from actual physical implementation of network for which one can apply this networking scheme into a physical network thus reliability test can be done. Another enhancement can also be done by making incorporating new/replacement node addition feature in runtime.

REFERENCES

[1] Rathee, Pinki, and Sanjeev Indora. "An Object Tracking Mechanism in Wireless Sensor Networks." (2017).

[2] "History and Architecture of Wireless Sensor Networks for Ubiquitous Computing", Vandana Jindal, D.A.V College, Bathind, IJARCET, Volume 7, Issue 2, February 2018, ISSN: 2278 – 1323

[3] D Rathee, Pinki, and Sanjeev Indora. "An Object Tracking Mechanism in Wireless Sensor Networks." (2017).

[4] "Wireless Sensor Networks Concepts, Application, Experimentation and Analysis", Fahmy, H.M.A., 2016, ISBN: 978-981-10-0411-7,

[5] Padmavathi, Dr G., and Mrs Shanmugapriya. "A survey of attacks, security mechanisms and challenges in wireless sensor networks." arXiv preprint arXiv:0909.0576 (2009).

[6] Sen, Jaydip. "A survey on wireless sensor network security." arXiv preprint arXiv:1011.1529 (2010).

[7] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[8] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.

[9] Needham, Roger M., and Michael D. Schroeder. "Using encryption for authentication in large networks of computers." Communications of the ACM 21.12 (1978): 993-999.

[10] Burmester, Mike, and Yvo Desmedt. "A secure and efficient conference key distribution system." Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994.

[11] Chan, Haowen, Adrian Perrig, and Dawn Song. "Random key predistribution schemes for sensor networks." Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.

[12] Anzai, Jun, Natsume Matsuzaki, and Tsutomu Matsumoto. "A quick group key distribution scheme with "entity revocation"." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 1999.