A Distributed Key Management Protocol for Wireless Sensor Network

Vishal Choudhary[1(✉)] and S. Taruna[2]

[1] Banasthali University, Vanasthali, Rajasthan, India
vishalhim@yahoo.com
[2] Computer Science, JK Lakshmipat University, Jaipur, India
staruna71@yahoo.com

Abstract. In sensor network where large group of nodes share the information, in such scenario it's difficult to scale the application, in addition security in wireless sensor network often vary with purpose and context, but in broad-spectrum, security for wireless sensor networks should centered on the protection of the data itself and the network communications between the nodes. Privacy, reliability and validation are the most important data security concerns. Traditional cryptographic methods are not promising on resource limited sensor nodes. Node initiated key management is a novel idea where rather than base station or key distribution center initiate the security algorithm. We can give control to sensor nodes or cluster head for securing communicating nodes with in a sensor network. It is a non centralized key management method which is more robust than other methods. in this paper we proposed the proactive key management which guarantee efficiency, robustness, and dynamic clustering.

Keywords: Cryptography · Random graph theory
Key distribution and management · Intrusion detection system
Sensor network

1 Introduction

There are certain problem pre-exist with key distribution, like private-key cryptography requires shared, secret between each communicating parties. So how to exchange the keys first time securely is a difficult task. In sensor network where large group of nodes share the information, in such scenario it's difficult to scale the application. Another problem is related to storage if there are n numbers of nodes and each node need to store up to $n - 1$ keys. Here storage requirement are directly related to amount of nodes participating in communication. In order to deal with storage problem there is a need for central authority that can distribute the keys a per requirements of sensor nodes. Such that each node can directly correspond with central authority which is known as key distribution center, each node should have to store only one secret key for communication with key distribution center and then key distribution center provides the secure link in between the communicating nodes. This is an indirect authentication scheme. But here deadlock like situation can occur, this scheme unable to provide the complete distributed environment of computing and communication.

A. K. Luhach et al. (Eds.): ICAICR 2018, CCIS 956, pp. 243–256, 2019.
https://doi.org/10.1007/978-981-13-3143-5_21

Only single point of failure can make the entire system halt. In order to reduce the problem associate with private key cryptography, the public key encryption scheme was developed; where the sender will encrypt the information with receiver's public key. The message cannot be decrypted by anybody who doesn't have the corresponding private key. Public-key distribution and deployment is easy. Also public-key reduces the need to store many different secret keys. if there are large numbers of pairs want to communicate secretly all need to store only one key and its most suitable technique for open environment. We have discussed various key distribution techniques in order to device the efficient algorithm for key distribution.

2 Background: Overview of Basic Key Pre-distribution Scheme

There are different key distribution and management scheme discussed in literature few of them are discussed here.

2.1 Single Network Distributed Key

In single network distributed or master key approach same key is loaded in all sensor nodes prior to deployment. After that same key is applied for encryption and decryption for data [1]. The main advantages in this approach are that, it is simple and need minimum storage requirement. But the security resistance throughout network can be damaged while attackers crack any sensor in the network.

2.2 Key Distribution by Trusted Base Station Scheme

The trusted secure base station is essential component of WSN. The sensor nodes validate itself to base station [1]. The base station produces a connection key and transmits to both communication nodes. It is similar to Kerberos [2] before deployment a distinct symmetric key is induced for every node in the WSN. This key is saved in the sensor memory and will acts as authentication entity for the node and assist encrypted transmission in between the sensor and base station. But this protocol needs consistent communication in between both entities.

2.3 Elliptical Curve Cryptography

The main problem with public key cryptography is complexity in key generation and exchange. ECC was invented by Victor Miller and Neal Koblitz [3]. The benefit of ECC over other public key cryptography technique is that the hard mathematical equation in ECC takes exponential time. Whereas best public key algorithm (RSA, Diffie-Hellman) takes sub exponential time. Elliptical curve cryptography is promising key generation technique where key size is drastically reduced without negotiating with the security of the network. The smaller key size makes the encryption and decryption more efficient and fast.

2.4 Random Key Pre-distribution

Sensor nodes are placed in hostile environment and some time they are scattered randomly and thus key-setup methods may not presume prior knowledge of the deployment. Eschenauer and Gligor projected [4, 5] in this technique each node gets an arbitrary set of keys from key pool to form key ring afore deployment, to make communication prosperous the communicating nodes find one mundane key within their subset to share secret data. "This method was developed on the theoretical foundation of random graph [22]. A random graph is formed by a group of n vertices as initial nodes and subsequently adding edges as joint between them randomly. a arbitrary graph is specified by notation G(n, p) in which every possible edge occurs freely with possibility p. To obtain complete connected graph, each pair of node should have comparatively minimum probability P_0 for making a straightforward channel. During operation of sensor network in real environment, a key-setup operation is implemented. In this stage entire set of nodes determine their acquaintance and use the common key. Key exploration procedure is followed by handing over a small identity to every key afore making operational in field. The nodes which recognizes the shared key ring can authenticate their acquaintance by transmitting a challenging question and verifying the result. For that link mutual key is the key for particular link" [22].

2.5 q-Composite Keys Scheme

In this scheme sub set of P desultory keys are culled out of immensely colossal key pool, further for every sensor m arbitrary keys are culled from P and stored in the sensor nodes' key ring. During the opening phase, each sensor node must agnize mutual keys with each of its acquaintance. This is done by local broadcasting a key identifier. every node can discover each acquaintance n with whom it uses at most q keys [4, 12]. In order to engender the transmission link key k, it uses hashing of all common keys. The keys hashing predicated on the order in which its occurs in the pristine key group P. key initialization is not done between nodes that have common keys fewer than q keys. It is found from analysis as the number of needed key overlap grow, it turns aggressively harder for an assailant to break a association. But, in order to optimize the given feasibility p of two nodes will share adequate keys to make a secure association, it is essential to decrease the key pool size |P|.it is found that the q synthesized keys scheme provides enough resistance counter to node capture when the number of nodes snatching is diminutive.

2.6 Polynomial Strategies of Key Pool in Key Distribution

Polynomial predicated key distribution is an efficacious technique in order to minimize the amount of data sharing and each pair of node can efficiently compute the shared key. Polynomial predicated key distribution is λ collision resistance, which denotes that as possible as less than λ nodes are conciliate rest part of network is protected [10, 11, 15]. Polynomial strategies utilizes a symmetric binary polynomial over finite field GF (q). A sensor that have ID i reserve a portion in P containing the uni-variate polynomial $f_i(y)$ equals to P(i, y). In case to exchanging the message with node j, it calculate the

prevalent key k_{ij} equal to $f_i(j)$ that further equals to $f_j(i)$ this procedure "enable two communicating entities to apportion a prevalent key.

2.7 Grid-Based Key Sharing and Distribution

In grid-predicated key sharing consists of identical sensors arranged in such a way that it composes a grid. Within maximum communication radius r. a sensor node can converse precisely among all entities inside the circle of range r that circumvents it [13]. Let k be predetermined group whose numbers we reference as keys to a group G of wireless sensors, and each have enough memory to contain m keys, subsequent deployment the nodes from G to form a wireless sensor network. A key pre-distribution scheme for wireless sensor network w is a mapping $G \rightarrow K^m$ that designate up to m keys from K to every node in G. Every node stocks the keys designated to it in its recollection afore deployment. After the nodes are deployment two communicating nodes contribute one or more prevalent elements of k that can be acclimated to engender a prevalent key. The nodes that do not apportion a prevalent key may depend on intermediary nodes with whom they both disseminate a key in order to converse securely.

2.8 Hypercube Based Key Distribution and Management Scheme

It is an elongated version of polynomial predicated key distribution. In this method afore deployment, the entities are arranged in three dimensional hypercube like structure. The fundamental pool of key spaces is engendered like multi space polynomial scheme [9]. There after the nodes within a given dimension are nominated with a polynomial structure from the ditto key space and hence are capable to compose shared pair sagacious key directly. If both nodes X and Y wish to establish a dyad sapient key, all indicators of nodes within all dimensional are correlated and if at minimum one index is matched then a key can be precisely ingrained. Otherwise rest entities are requested for alliance such that virtual link from x to y can be composed (X; k1;k2;k3;;;;;;Kn;Y), where X is able to establish direct pair sagacious key with K_1, K_i with K_{i+1} and K_n with Y, key is engendered at X and conveyed with re-encryptions over intermediate nodes K_i to node Y with incrementing dimension of hypercube number such path withal increases and if minimal one non-negotiate path subsists, and a secure pair of key can be established.

2.9 Deployment Knowledge in Key Management

In deployment cognizance scheme, it is supposed that sensor entities are immobile after deployment. The sensor nodes can reside at points around "positioning point as the point location where a sensor entities are operational [7]. It is postulated that target opeartional area is two dimensional rectangular regions with size X.Y and the inception point is the upper left rectangular corner. The probability density functions for the target of entity I for i = 1…… N, over the bi- dimensional space is represented by fi(x, y), where $x \in [0, X]$ and $y \in [0, Y]$.

2.10 Location Aware Key Dissemination

In location dependent key dissemination scheme sensor entities can be integrated at any time. Afore deployment a master key is embedded in all sensors. After setup in operational field each sensor node utilizes this key to achieve a group of subset-keys predicated on the nonce acknowledged from pairing nodes [9]. Utilizing the set of prevalent subset-keys with each acquaintance, a sensor will engenders distinctive keys for each and every communicating path with others nodes. After this the nodes expunges the prevalent key in order to evade capturing from adversaries. In the time of starting phase each sensor node transmit a periodic signal at dissimilar energy level, each periodic signal enclose a dissimilar nonce encapsulated utilizing the prevalent key k fragmented in between all entities. Each entity receives a set of periodic signal predicated on the comparative position of the sensor node from sundry nodes. The sensor entity then drives sub-keys utilizing an amalgamation of the mundane key set k and the received set of nonce's. The key updation is carry out by each sensor entity predicated on location this is due to sensors that are not in the same position, receives different set of nonces. Thus final sub-keys must be unique.

2.11 Combinatorial Key Management Using Location

It is a lightweight combinatorial design for key administration for clustered sensor network which is additionally kenned as SHELL. In SHELL, here the probability of node capture is reduced as physical location is utilized in computing the keys of a node [14]. Here any node with in a cluster can directly communicate through the doorway nodes which are central ascendancy of individual cluster. The gateway nodes are puissant enough to converse with the individual node with in a cluster and invoke the key management functions. Each switch node can communicate with at minimum two other switch entities in the network. The gateway uses three different kinds of keys. The first category of key is a prior loaded key that sanctions the switch node to directly communicate with key distribution node. The second type of keys sanctions the different bypass and hub nodes to communicate. The third key type sanctions the bridge to communicate with all of the sensor entities in the cluster. The key distribution node is surmised that it is unable to be compromised it acts a key repository, authenticate bridge node and sensor nodes, distribute keys to all other nodes, and it perform key updation when needed. If any node get compromised. A key revocation is initialized and the gateway node watches the node in its cluster for failure and key distribution node do same thing for bridge nodes.

3 Distributed Key Management

3.1 Key Management Techniques

Key administration in WSN is a complicated process due to nature of sensor nodes and its deployment in the multifarious environment [18]. Some of key management techniques are highlighted as:

(a) **Universal key:** In this scheme, only "single key is publically shared by the whole network. To transmit a packet, it is encrypted with this shared key. Once the information is received, it is decoded with the same key. It is an energy proficient way" of key distribution. Here data is encrypted only one time by the sender and decrypted only one time by the receiver. However, it provides limited security. Here only hacking of single key leads to compromise of whole network which converse with this unique key. Intruder can also insert duplicate node in network.

(b) **Pair wise key node:** Each node store an separate key for correspondence with its neighboring node [6, 8, 19]. On the off chance that there are k neighbors for a sensor node, at that point it has k exceptional key in memory to speak with its neighbors. In this arrangement, a node that communicates something specific needs to encode the message with a key neighbor who gets the data. The neighboring node unscrambles data and re-encode with the key comparing to the accompanying beneficiary. This procedure gives sufficient security because of localization of keys. In any case, it's not vitality productive as encryption and decoding at every node increment computation overhead and consume more energy additionally require more storage at every node.

(c) **Combine insightful key gathering:** here each bunch of node speak with unique keys inside its cluster [17]. In this method there is pacification between security and energy proficiency. It confines the quantity of encryption in correspondences. Anyway it enhances computation of cluster head, which need to decode and encode the information. To be viable, we need to" progressively change the CHs keeping in mind the end goal to limiting the energy consumption.

(d) **Singular key:** In this technique, each node has its own particular key to scramble the data [16]. Here each node sends the encrypted data that can only be decrypted by sink node. it can provide the robust security but main problem here is the overhead faced by sink node to decrypt as separate packet need separate decryption key. That is key decryption algorithm is quite complicated at sink node. Also key revocation and distribution is problem.

3.2 Key Generation

Key generation and distribution plays major role in protecting the sensor network. For each round if key distribution center insert new keys in the sensor nodes then computations and communication is high. In order to optimize the performance of sensor network we have to set the protocol when and where to updates the keys. We need an intelligent system which can take the decisions to update the keys based on suspicious behavior of node. Also there is problem for delay in updating the keys due to certain communication problems with in network. The main advantages of dynamic regeneration keys are that it keeps the sensor network secure.

3.3 Localization

Sensor network localization calculates approximately the location of sensor node with initially unknown location. Localization based key distribution needs exact position of sensor node that can be augmented with the help of GPS. The distance of each node can

be calculated with received signal strength from base station. Location aware sensor can improve the energy efficiency. Here nodes can be optimized with distance from base station. The nodes near base station can be switched to low power as compared to node that is very far from base station.

4 Interruption Discovery Framework (IDS)

An interruption discovery framework (IDS) screens suspicious exercises beyond ordinary and unsurprising behaviour, "It depends on the presumption that there exists a reasonable separation in the activities of an intruder and approved client in the system to such an extent that an IDS can coordinate it with pre-chosen or conceivable learned strategy [20]. In view of the examination IDS can distinguish unauthorized activities. Intrusion is an unapproved action inside a system. On the off chance that intrusion goes undetected from beginning state i.e. the time when an intruder endeavor to break the system then it might be unsafe and enemy can take control over the whole system. Once the assault is recognized in the system then IDS raise the flag to advise the base station to make the move for securing the framework (Fig. 1) [22].

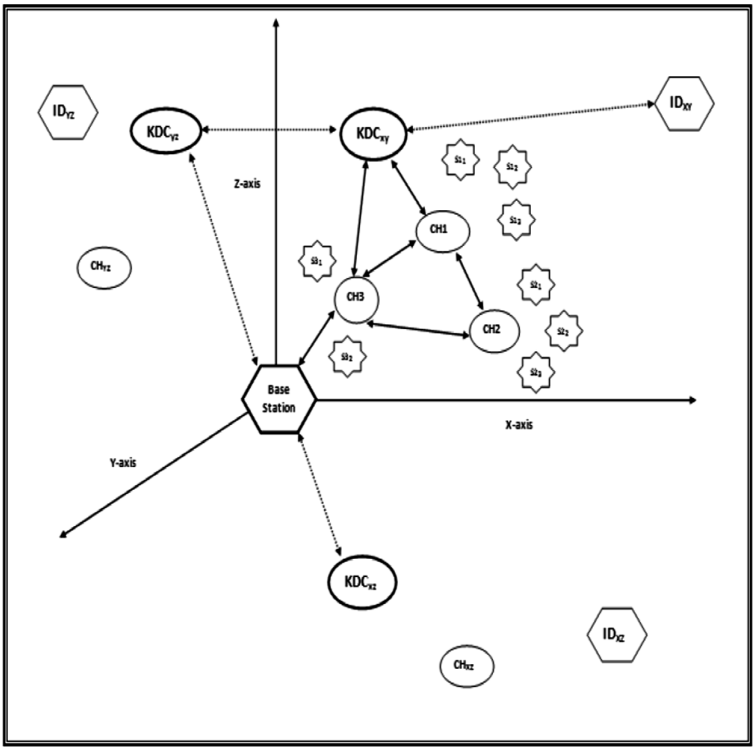

Fig. 1. Interruption discovery framework (IDS) consists of following steps: regular checks on intrusion in network, on detecting suspicious activity inform the key distribution center (KDC), KDC updates key, registering the updated key status in base station.

5 Hashing

We can use the interesting properties of hashing technique. The hash function is one way and hash function is without crash to keep the dynamic attack that changes and retransmits the message. Key updates in light of key chains where each key is gotten by applying a hash formula on next key in chain". Here all keys require not be put in sensor nodes rather that a counter will produce the keys by simply picking an arbitrary number with in a predefined set. Verification of keys id done by checking the hash result. Unapproved client or assailants unfit to ascertain hash values.

5.1 Dynamic Hash Function

The values that are stored in hash table is calculated with a hash function. During the communication process the hash table needs to be expanded or shrink. Such a function is known as dynamic hash function. The ideal cryptographic hash function has following main properties.

I. It is deterministic in context of reuse of same function. That is hash function uses the randomized number that is generated once when a process starts also the input to be hashed and this function is valid only in single run. If the value still persists in next cycle then it cannot be treated as valid hash value. Since in next cycle the random value might differ.
II. The hash function must be quick to compute the hash value for any given communication cycle.
III. It must be impossible to decode the message that is encrypted with hash value except by trying all possible values with in a hash set.
IV. It must be infeasible that two communication processes uses the same hash value.

6 Key Set up in Sensor Network

Node Initiated key management is a novel idea where rather than base station, key distribution center initiate the security algorithm. The control can be given to sensor nodes or cluster head for securing the sensor network. Sensor node is more prone to attacks than base station or key distribution center. So the sensor node if empowered with minute modification in its stored key then it can dynamically update its key. Here sensor node is augmented with a random number generator which is augmented with time stamp protocol with in predefined set. Hash function can calculate and update the key in node before transmission of message from sensor node. Sensor node can encrypt the message with it and same hash function stored in base station can take care for decryption if the key fall within its set. Dynamic update of keys by sensor node makes the network more robust. Although main limitation here is the extra load on sensor node. But the algorithm on sensor node is not so complicated that it may drain out the battery life faster (Fig. 2).

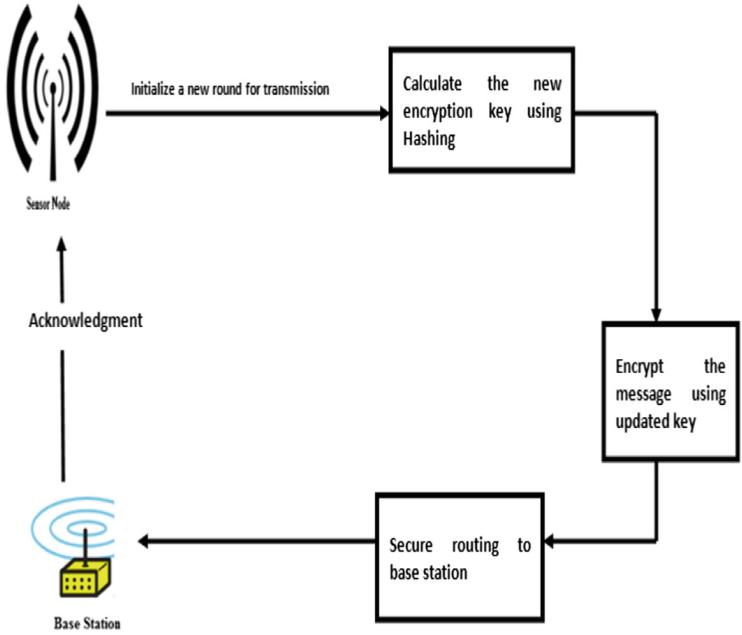

Fig. 2. Proactive key update

During network boot up the following key management process will be initiated.

I. **Communication between base station and key distribution center**

During boot up process base station transmits a key ring with in the specified hash function to key distribution center (KDC). The key distribution center authenticates and acknowledges the key ring with base station.

$$B(K_i \parallel KDC_{key}) <----------> KDC(Ki \parallel B)$$

Here base station (B) encrypted the key ring (K_i) with key distribution center master key (KDC_{key}).

II. **Communication in between KDC and cluster head**

Key distribution center encrypt the key ring with cluster head identification number Ksj. i.e. secret key of cluster head and broadcast in network. Cluster head send acknowledgement to key distribution center.

$$KDC\ (Ki \parallel K_{sj}) <----------> CH(K_{sj} \parallel KDC_{key})$$

III. Communication between sensor node and cluster head

Cluster head allot the key values to sensor nodes by processing the certification code for itself and its group nodes by utilizing one way hashing method with its n members" as follows.

$$H_1 = H(K_1, K_{sj})$$
$$H_2 = H(K_2, H_1)$$
$$\text{----------}$$
$$H_n = H(K_i, H_{n-1})$$

Where K_{sj} is cluster head own secret key and K_{i-1}, K_{i-2}, K_{i-n} are secret keys of sensor nodes with in a cluster group.

In the next phase cluster head transmit its member identification numbers and their hash values H_n to base station by encrypting with K_{sj}. Since base station has all identification numbers and their key values it can decrypt the message from the sensor nodes (Fig. 3).

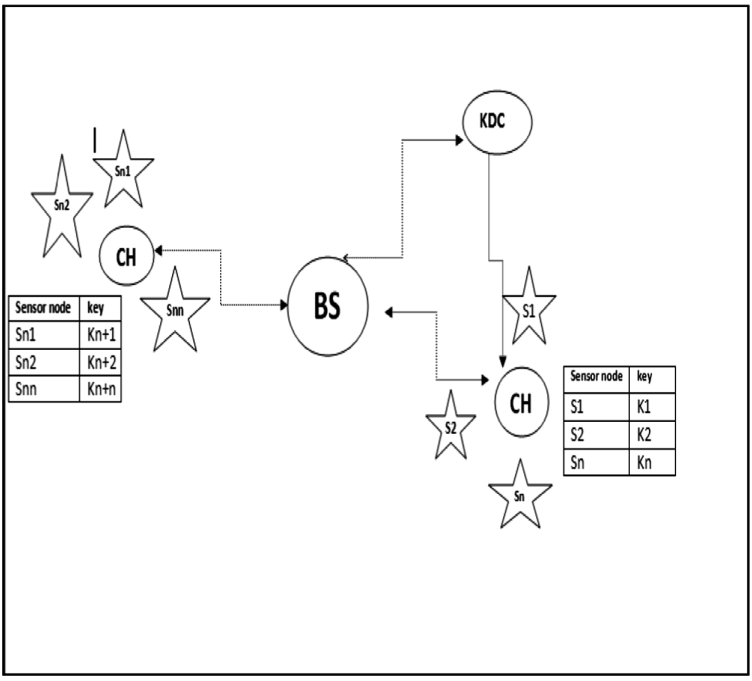

Fig. 3. The figure depicts the mapping in between base station, cluster head and key distribution center. Cluster head have their member table which stores the private key of each sensor node. The member table is updated periodically.

7 Real Time Key Updates in Sensor Network

In order to create a secure transmission" it is necessary to revise the "session key Ksi. Session key is associated with time period for each transmission" cycle. There is a need to update the session key periodically. To updates the keys in sensor nodes cluster head CH broadcast a random number Rt at time t before node capturing time T_{cap} i.e. ($t << T_{cap}$) here random number Rt is a function of time period. All nodes under the cluster head updates their key using one way hash method and get rid of the old keys.

The sensor node S scans the time interval t.

$$\text{for} \quad S\text{<--------}CH\ (R_i)$$
$$\text{do}$$
$$S \text{ <--------} F(S, H[t_i])$$

i.e. update in sensor is a function of time cycle. The updated keys now in sensor nodes will be

$$Ks_i\text{-}t1 = H(K_{si}, Rt_1)$$
$$Ks_i\text{-}t2 = H(Ks_i\text{–}t1, Rt_2)$$
$$\text{----------}$$
$$Ks_i\text{-}tn = H(Ks_i\text{-}tn\text{-}1, Rt_n)$$

8 Data Transmission Phase

The sensor node with in a cluster head encode the information packet by utilizing its own private key Ksi. Ksi became the session key to exchange message with cluster head. As cluster head node gets all undisclosed key of its nodes, it can decode data from any node *i* if it is a component of the cluster. The data packet format as" follows:

ID_i	$E_{KSi}(M)$	$M_{ACKSi}(M)$

Where M is sensed data for sensor node, $E_{KSi}(M)$ is the encoded information and $M_{ACKSi}(M)$ is the message validation code. When cluster head (CH) transmits data packets to base station (BS) for execution. It encrypts the packet using its own session key along with insertion of its identification number. If the distance in between cluster head and base station is multihop, then intermediate node just relay the data packets to base station.

If a sensor node would not obtain the broadcasted arbitrary number due to defective wireless channel then it cannot encrypt the message using the latest key and this node can be understood as a intruder node or may be a hacked node to cluster head. Then the proposed method manages this condition as follows.

Each sensor node starts its counter to count the transmission cycle. If a node does not receive any broadcast acknowledgement from base station with in time T_{cap}, it without delay sends a message to its cluster head using previous updated key and last received broadcast number Rt. Cluster head updates the old key Ksi-n-1 with new update key Ksi-n and register this update in base station.

In order to balance the energy consumption re-clustering will take place within the sensor network. After definite time period old cluster will breaks down and new cluster will be formed.re-clustering is done by base station here base station sends a special broadcast message to all its cluster heads to erase its member table. After that a node with energy greater than thrash hold energy is selected as a cluster head and a new member table is formed. All key distribution and management process restarts.

9 Accomplishing Security Goals

Secure key administration and calculation must accomplish the security objectives [21] i.e. honesty, privacy, Availability and freshness to moderate assaults and intimidation as much as expected. These objectives can be outlined as the accompanying:

- Integrity: Data must not be adjusted in transmission way, and insurances must be taken to ensure that information can't be changed by unapproved party. To guarantee that information scopes to the proposed recipient with no modification, a method like hash capacity can be utilized.
- Confidentiality: Confidentiality stays away from vulnerable data from achieving the wrong goal, while ensuring that exclusive the correct collector can in certainty get it. Along these lines, while transmission the information in the system, nobody can comprehend with the exception of" proposed beneficiary.
- Availability: Availability requires that information are accessible to approved gatherings. It is a "necessity proposed to guarantee that WSN work at the named time and administration isn't denied to approve hubs when they ask for them. Along these lines, with accessibility system ought to be accessible even within the sight of assaults.
- Freshness: replay assault abuses the freshness in which assailant retransmits an old message to possess framework assets or befuddling the" collector. Freshness protect that no old message have been replayed.

10 Conclusion

Security in wireless sensor network often vary with purpose and context, but in broad-spectrum, security for wireless sensor networks should centered on the protection of the data itself and the network communications between the nodes. Privacy, reliability and validation are the most important data security concerns. Key management is major concern for security in wireless sensor network. The nodes in sensor network cannot rely on centralized security system like Kerberos. Also tradition cryptographic methods are not promising on resource limited sensor nodes. Node initiated key management is

a novel idea where rather than base station or key distribution center initiate the security algorithm. We can give control to sensor nodes or cluster head for securing communicating nodes with in a sensor network. It is a non centralized key management method which is more robust than other methods. Proactive key management must guarantee efficiency, robustness, and dynamic clustering.

References

1. Chan, H., Perrig, A., Song, D.: Key distribution techniques for sensor networks. In: Znati, T., et al. (eds.) Wireless Sensor Networks (2004)
2. Miller, S.P., Neuman, C., Schiller, J.I., Saltzer, J.H.: Kerberos authentication and authorization system. In: Project Athena Technical Plan (1987). Page section E.2.1
3. Huang, X., Shah, P., Sharma, D.: Fast algorithm in ECC for wireless sensor network. In: Proceeding of the International Multiconference of Engineers and Computer Scientist, vol. 2 (2010)
4. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of Symposium on Security and Privacy (2003)
5. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communication Security, November 2002
6. Du, W., Deng, J., Han, Y., Varsney, P.: A pairwise key pre distribution system for wireless sensor networks. In: Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003), pp. 42–51, October 2003
7. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: INFOCOM, 2004, April 2004
8. Du, W., Deng, J., Han, Y.S., Varshney, P.K.: A pairwise key pre-distribution for wireless sensor networks. In: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003), Washington, DC, USA, pp. 42–51 (2003)
9. Faghani, M.R., Motahari, S.M.: Sectorized location dependent key management. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 12–14 October 2009
10. Boneh, D., Corrigan-Gibbs, H.: Bivariate polynomials modulo composites and their applications. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 42–62. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_3
11. Sen, J.: A survey on wireless sensor network security. Int. J. Commun. Netw. Secur. (IJCNIS) **1**(2), 55–78 (2009)
12. Azarderakhsh, R., et al.: A key management scheme for cluster base wireless sensor networks. In: IEEE International Conference on Embedded and Ubiquitous Computing (2008)
13. Blackburn, S.R., Etzion, T., Martin, K.M., Paterson, M.B.: Efficient key predistribution for grid-based wireless sensor networks. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 54–69. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85093-9_6
14. Younis, M.F., et al.: Location-aware combinatorial key management scheme for clustered sensor networks. IEEE Trans. Parallel Distrib. Syst. **17**(8), 865–882 (2006)
15. Magar, A.A.: A Survey about key pre-distribution scheme in wireless sensor networks. Int. J. Eng. Res. General Sci. **2**(6) (2014). ISSN 2091-2730

16. Cui, B., Wang, Z., Zhao, B., Liang, X., Ding, Y.: Enhanced key management protocols for wireless sensor networks. Mob. Inf. Syst. **2015**, 10 p. https://doi.org/10.1155/2015/627548. Article ID 627548
17. Kun, M., Li, L.: An efficient pair wise key predistribution scheme for wireless sensor networks. J. Netw. **9**(2), 277 (2014)
18. Lee, J., et al.: Key management issues in wireless sensor networks: current proposals and future developments. IEEE Wirel. Commun. Mag. **14**(5), 76-85 (2007)
19. Diop, A., Qi, Y., Wang, Q., Hussain, S.: An efficient and secure key management scheme for hierarchical wireless sensor networks. Int. J. Comput. Commun. Eng. **1**(4), 365 (2012)
20. Alrajeh, N., Khan, S., Shams, B.: Intrusion detection systems in wireless sensor networks: a review. Int. J. Distrib. Sens. Netw. **9**, 167575 (2013)
21. Gaubatz, G., Kaps, J.-P. Sunar, B.: Public key cryptography in sensor networks. Revisited in 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004) (2004)
22. Choudhary, V., Taruna, S.: Improved key distribution and management in wireless sensor network. J. Wirel. Commun. **1**(1), 16–22 (2016)