Multi Keying Mechanism for Security Framework in Clustered Wireless Sensor Network

Yugashree Bhadane[1], Chitra Rajendran[2]
[1]Department of Information Technology, DPCOE, Wagholi, Pune, Maharashtra, India
[2]Department of Information Technology, SCOE, Vadgaon, Pune, Maharashtra, India
Email – yugarb@gmail.com, chitrarajendran@gmail.com

Abstract: *Wireless sensor network (WSN) fits to the class of mobile ad-hoc network which entails of large number of sensor nodes that is deployed in the area of interest to achieve a particular task. WSN mentions a number of sensors for monitoring and recording the physical conditions of the environment. It has a varied range of application, like detecting and tracking the troops and tanks on battlefield, to observer the pollutants existing in environment, to measure the traffic flow on roads, tracing the personnel location in a building etc. In these applications the profound data of the sensor nodes must be protected with intense care as they are regularly deployed to argumentative environment. An important activity to safeguard the data integrity and to provide safe wireless communication via cryptography is the main role of key management and the environment that can provide secure communication along with less communication overhead is clustered based structure. This provides data confidentiality, integrity and authentication between the communicating nodes. It also prevents the malicious node imitating as a good node from spreading false information purposefully. This paper contains a detailed survey on various cluster based protocols and multi keying mechanism to secure wireless sensor network which provides security to WSN in all aspects of communication between sensor nodes. It also provides an enhanced technique of key management to provide efficient security and reducing overhead caused in communication.*

Key Words: *Wireless Sensor Network, Key Management, Cryptography, Security, Cluster*

1. INTRODUCTION:

Wireless Sensor Networks (WSN's) domain has gained more popularity in research field. The reason behind this popularity is not only due to its applications but due to its co-domain fields also such as security, authentication, key management, routing, data aggregation and disseminations etc. Sensor nodes are generally of large number of ultra-small autonomous devices. Every device that is called a sensor node has battery power and armed with integrated sensors, data processing capabilities and the radio communication is of short-range.The use of wireless sensor network are for wide variety of applications which includes military sensing and tracking, patient monitoring and tracking, smart environment, environmental monitoring etc. Security becomes a critical and extremely important task when the network is deployed to the hostile environment because they are susceptible to various types of malicious attacks. For example, an enemy or the adversary may listen to the traffic or may mislead information to some other node purposefully. In order to maintain a secure communication, the communication should be made secure by using encryption techniques and authenticate the nodes.

Maintaining the secrecy of the application is very important in wireless sensor network and to do this, keys are shared among the nodes and message is transmitted between nodes in encrypted format. There are various methods of keying that contains their own strengths and weakness. So, in-order to provide an efficient keying technique the combination various methods are preferred such as 'in-network generated keys', 'pre-deployed keys' and 'broadcast keys'. In wireless sensor network there are fundamentally three types of communication such as one to one communication, one-to-many communication and many to one communication. All these types of communication need to be protected by establishing various types of keys. By the combination of different keys the environment can be secured. Key management mechanisms are divided into two different classes on the basis of their capability by which they can update cryptographic keys, one is the static and other is dynamic. The static keys are pre-distributed and remain same in complete life time while in the dynamic key technique are distributed periodically while needed in the network.

The environment in wireless sensor network is in the form of flat which does not contains cluster environment and hierarchical form which forms clustered cluster environment. The flat structure has varying mechanism consisting of single key as well as multiple keys that are shared in the network among the nodes. Multiple keying mechanisms provide more security but the overhead in the initialization phase is more. In the hierarchical structure the key management is efficient as the number of keys that are shared in the network in less are compared to flat structure because the shared keys are only between the cluster head and the sensors and between the gateways but not among the sensors in the network.

In hierarchical clusterWSNs, the combination of sensor nodes form cluster and every cluster has a cluster head or gateway. This gateway node has more power in the form of its computational capability, its memory storage, communication range and more life time when compared to other nodes.

The rest of the paper contains Literature survey containing key distribution types, secure clustering process and existing secure cluster protocol. The third section contains proposed protocol and the fourth section is of the conclusion.

2. LITERATURE SURVEY:

In wireless sensor network, for communication between sensor nodes and there communication with the base station the environment can be clustered or it can be non-clustered. In the clustered environment the communication path is hierarchical structure. Due to this the path to transfer message to the base station is hierarchically upwards in direction. In the non-clustered environment for every node in the network separate path has to be discovered following multiple stages. While in the clustered environment path which needs to be followed is only from nodes to the cluster-head and from the cluster-head to the base station. This ensures efficiency in routing.

Even though the network is formed in clustered environment or the non-clustered environment, the security of the communication cannot maintained unless special security mechanism. Because unless provided with security mechanism the network will be prone to attacks that can compromise the complete environment. Keying mechanism is an efficient way to provide security to the wireless sensor network.

In WSN key management is an important area for research as it provides efficient security service in wireless sensor network. But as there are limited resources in the environment of WSN the implementation of key management mechanism is a difficult work. The initial phase where the keys distributed before the network is been deployed is called key pre-distribution. The next stage is the formation of secure session which is known as key establishment phase. After this is the phase of network formation. The phase of Node addition or node deletion works with the establishment of secure sessions with new nodes that are been added or removed[1].

When this key mechanism is combined with the clustered environment the security of the network is maintained and provides energy efficient and secure network.

1.1Key distribution types

a. **Master key approach**

One method for pre-loading of symmetric keys into the sensor nodes is master-key approach[2]. In this method, a unique symmetric key is pre-loaded in the memory of the sensor nodes. After being deployed every two nodes in the network use the same symmetric key to encrypt and to decrypt the data that is been traded among them. In this only one key is kept in the sensor, so there is no communication overhead for key establishment and thus this approach is efficient. But it requires more security; node capture attack is a treat for wireless sensor network. In this approach, even if a single node is seized, the entire network can be compromised. Example of this scheme is Localized Encryption and Authentication Protocol (LEAP)[3],[1] and Peer Intermediaries for Key Establishment (PIKE) [3].

b. **Pair-wise key approach**

Another method of pre-loading the symmetric key is pair-wise key based approach[4]. To make an assurance that two nodes contains a unique key among them a set of symmetric keys are preloaded into every sensor nodes. In the pair-wise key establishment scheme, every node create unique key with all other nodes. These keys have to be maintained in the memory by the nodes. Overhead on the nodes increases and cost required is also increased in memory's point of view. Hence, the mobility as well as the scalability is limited. This method provides efficient security as the node capture cannot modify or change the secure communication. But its drawback is that it has very large key storage overhead and hence it is no scalable. The fact that the sensor node has inadequate memory size this approach is not viable for deployment in real life.

c. **Public key cryptography**

Asymmetric key cryptography which is also known as public key cryptography is also used for key exchange. It requires two related keys, of which one is private and the second is public. This permits data to encrypt itself using public key and can be decrypted only using the private key. In the general case this approach is feasible with the proper selection of algorithm although it requires rigorous computation. Public key cryptography can be performed by RSA and ECC. Earlier until 2004, it was a belief that these methods are very costly, heavy weight and slow for WSNs. But in recent days researchers have provided an improvement in public key cryptography (PKC)so that it can be used with immense efficiency in WSNs. The use of ECC is feasible in WSNs as has faster calculation, small size of the key and compressed signature when compared to conventional PKC. Some of the ECC libraries are TinyECC which was proposed by Liu and Ning[5] and WMECC[5] which was proposed by Wang and Li[5].

d. **Random key approach**

In the scheme of random key pre-distribution there is absence of overhead of computation. But the overheard of communication with shared key detection depends on the number of keys stored in each sensor. An adjustment between network connectivity and key storage occurs in random key pattern. In order to achieve high network

connectivity some keys are preloaded in the sensor nodes. Peer Intermediaries for Key Establishment (PIKE) [3],[6] is an example of random key approach.

e. **Polynomial key approach**

The communication overhead in case of polynomial-key pre-distribution[7] is lesser as compared to random key distribution. But it cannot offer security for large scale networks to provide safety from the attack of node capture. Communication between two non-compromised nodes can be kept secure only if the number of nodes that is compromised is less than a critical value. If it more than critical value then the rivals can easily know the pair-wise keys by calculations.

f. **Location based key approach**

Location based key pre-distribution technique[2] is similar to that of random and polynomial distribution, but in this method to enhance the performance of the network, information about the deployment of the sensor is used. With an assumption that the location of the node can be predicted prior to deployment, this approach reach the same network connectivity with less number of keys stored in every sensor than previous schemes.

g. **BS based scheme**

Hierarchical key establishment scheme(HIKES) was proposed by Ibriq et al.[3]and is based on base station based scheme. In this method it is the Base station that acts as a central authority which is a trusted authority and it selects a node that is known as local trusted authority. This local trusted node authenticates the cluster member on behalf of the Base station.

h. **Clustered environment key scheme**

The Cluster-based Mobile Key Management Scheme (CMKMS)[8] is an example of protocol which has clustered environment and used to improve the scalability , mobility and efficiency of sensor nodes (SN).The network is subdivided into clusters. The node that contains maximum trust ability and efficiency is nominatedas Cluster Head (CH). The CH acts as a key manager and it aggregates information from all othernodes in the cluster. The work assumes that sensor nodes and CH can move from oneposition to another. The communication in between the SN andSN is intra-cluster communication, which is performed using SN-to-SN link. The transmission in between the CH and CH or CH and Base Station (BS) is inter-cluster communication, which is via CH-to-CHlink or CH to BS link. The key management algorithm here considers the CH as KM. The work assumes that nodes can move from one position to another, but CH and BS are fixed at one position.

So as to raise the life of the network and also to diminish the energy that is been consumed the network model with clustered environment. In this type of method of forming the cluster that reserves the energy of sensor node which follows multi-hop communication within a specific cluster and executing data gathering and fusion. Every cluster contains a head node which is known a cluster head that performs the task of assembling the data from all the nodes as transferring the aggregated message to the base station.

1.2 Secure clustering process

A serial process that promises the security goals that are confidentiality, availability and integrity are called secure clustering. This procedure contains of two steps, first is cluster building and the second is transmission of data. The first stage which is the building of cluster that begins with formation of cluster and cluster head is selected and the remaining nodes in the cluster are assigned to that cluster head. The second stage is of data transmission which ensures transmission of data in secure form. Even the data transmission works in two steps, the first is data aggregation and other is routing the data to base-station[9].

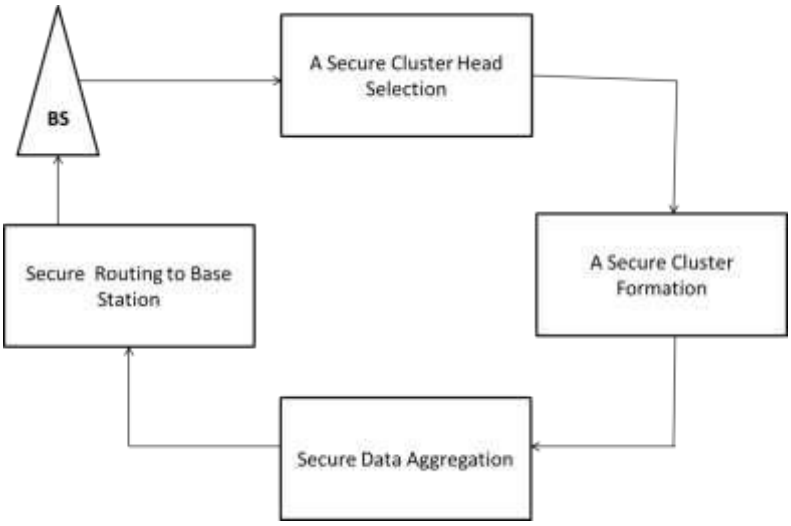


Fig.1: Secure clustering process

In the process of data aggregation, all the nodes within a cluster send the message or the data to cluster head then it is the responsibility of the cluster head to forward the data through a particular path.

1.3 Existing secure cluster protocols

a) LEACH

LEACH is scheme that a vigorous against many attacks when compared to other routing protocols and was proposed by WB Heinzelman[10].in LEACH protocol the process of self-organizing and re-clustering at every phase is performed[11]. In various other protocol which works on multi-hop communication where the common node aims to compromise the cluster head, in this method on the other hand links straight with the base station. Because of these specifications it becomes difficult for the adversaries to compromise the node in LEACH protocol and thus the life time of the network is increased. It cause a major issue such as failure of cluster head[12].

b) SLEACH

The very first version to build a secure environment to the LEACH is SLEACH[9] protocol. This protocol provides security against sinkhole, selective forwarding and flooding attacks. Each node in this algorithm has the similar characteristic in the case of its initial energy and its processing power and provides security by using symmetric-key. But the network performance and efficiency is reduced and lacks the guarantee of confidentiality and availability.

c) ESODR

This method provides a network contain clusters and every cluster is made up of cluster head, common nodes and gateways. To ensure security ESODR[9] combines the hash function, symmetric key cryptographic algorithm along with the public key cryptography. It provides better scalability and efficiency but requires large size of memory storage.

d) SecLEACH

An improvement to SLEACH protocol to secure node-to-node communication SecLEACH[9] was proposed. It presented symmetric key and one-way hash chain so as to provide better performance on efficiency and security. It provides confidentiality, integrity, authenticity and freshness but it lacks to provide method to provide security against compromised cluster head attack. It is also prone to key collision attack.

e) HT-LEACH

The protocol of hierarchical tree based routing on the basis of LEACH which is proposed by [10]BaoZhenshan et.al. is known as HT-LEACH. The algorithm in the protocol works in the stages namely formation of cluster, hierarchical route formation and the final is steady state. In this method when the energy is exhausted the node dies.

f) NSKM

With the usage of three different keys the method provide a secure clustering scheme and ensures efficient establishment as well as distribution of the keys with the pre-deployed keys, network generated keys and the BS broadcasted keys. It provides resistance against replay attack as well as node capture attack. NSKM[9] ensures that although the network is been attacked, data security is maintains and complete network will never be compromised. It does not provide security to active attacks such as sinkhole, as there is no provision for dynamic clustering.

g) AKM

This method ensures security with the usage of two keys such namely the pair-wise key between the nodes within the cluster and the other is network key and is based on cryptographic method. AKM[9] protocol provides security against node capture attack and ensures confidentiality as well as authentication. But before the network key is been refreshed and attack is network is been attacked then the complete network will be monitored.

h) SS-LEACH

SS-LEACH [13]was proposed by Wu et al. to provide security in routing and maintain the lifetime of the network. This protocol improves the energy-efficiency[14] but lacks to provide integrity and is prone to sinkhole and wormhole attack.

i) EGKMST[13]

It is based on hierarchical network architecture and uses symmetric keying method. It makes use of two keys, one is the group key and other is pairwise key. It provides security against resilience attack with low communication cost. But in real environment causes storage overhead.

Protocol	Advantage	Disadvantage
LEACH	Free from node compromise and increase network lifetime	Failure of cluster head
SLEACH	Security from attacks like sinkhole	Lacks confidentiality and availability
ESODR	Better scalability and efficiency	Large storage size memory
SecLEACH	Ensures confidentiality, integrity, authenticity and freshness	Key collision attack
HT-LEACH	Hierarchical routing	Node dies when energy is exhausted
NSKN	Ensures data security	No security from active attacks
AKM	Ensures confidentiality and authentication	Prone to network attacks
SS-LEACH	Secure routing and ensures the network lifetime	Lack integrity and prone to wormhole attack
EGKMST	Security against resilience attack	Storage overhead in real environment

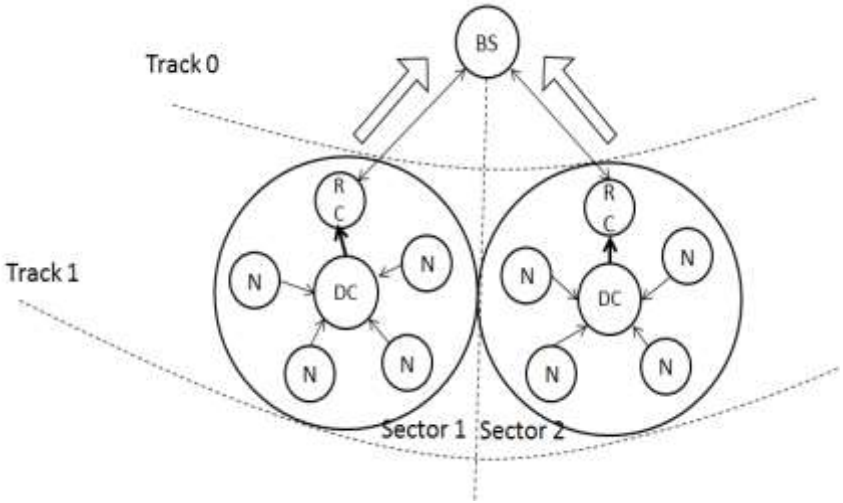
Table 1: Comparison of various protocols

The existing protocols have some advantages and some disadvantages. A new protocol is designed to overcome with these disadvantages and to ensure security using multiple keys and the environment is clustered.

3. WORKING OF A CLUSTERED WSN SYSTEM:

3.1 Cluster Formation Description

Energy consumption is a prime need in wireless sensor networks. As per or discussion in related works hierarchical routing helps in less energy consumption compare to flat routing networks and thus it's more efficient to use hierarchical routing network in WSN's. Here, we have used hierarchical network in cluster environment where we have divided wireless sensor networks in particular tracks and sectors[15]. Clusters are formed on the basis of energy consumption of the nodes and its nearness to the cluster head and the communication of these are on the basis of multi-hop communication. In a clustered environment, the number of message that is required to be send to the destination is less as compared to that of flat architecture. This is because all the data are aggregated and then it transmitted.



BS: Base Station
N:Common Node
DC:DCH(Data Cluster Head)
RC:RCH(Routing Cluster Head)

Fig. 2: Proposed Architecture

3.1.1 Cluster formation using RCH and DCH

As mentioned earlier the network is divided into tracks and sector which is done by the Base station (BS) and security is maintained in the network by using a secure key management. Base station is placed in track 0, while most of the nodes in track 1 assist as the Routing Cluster Head (RCH). Sectors are the subdivision of the tracks. Network requires some amount of energy and on the basis of this energy utilization the number of clusters is decided. Nodes belonging to same cluster can have direct communication with each other and consider each other as buddy. In this process, all the nodes acquire information about its own from the base station and then gains the details about the neighbours and also maintain a table which contains the buddy information. This is called the "buddy detection phase".

1) B_Level_id= 0{initialized}
2) N_Level_id= -1{initialized}
3) BS : Broadcast(B_Level_id) -> Nodes
4) If (N_Level_id=-1) ->N_Level_id=B_Level_id
   Else
      B_Level_id++
5) Broadcast the packet again

It is the Base station that broadcast a packet holding a level identity (B_Level_id) containing value 0 while every node has an identity i.e. N_Level_id and had its initial value -1 which will latter hold the level_id of the node. In order to start a communication, the BS broadcasts the node id in the form of message to every nodes that is present in the network and nodes sends the response as an acknowledgement to the base station.

In this method the charge of cluster head is divided into two clusters so that they can perform their individual responsibilities. Data cluster head (DCH) aggregates the data from all the nodes and also does many other works such as calculating the median etc.

After the process of categorization of the node,the charge of routing is divided into different clusters namely Data Cluster Head (DCH) and Routing Cluster Head (RCH). The work of aggregation of data, calculating median etc. is performed by DCH while the work of sending the data to the sink i.e. the process of communication is done by the RCH.

The selection of DCH is on the basis of median of distance. It allows locating a node which is optimally close to all the nodes in a particular cluster. And then the RCH is determined on the basis of residual battery-life of all nodes and the node that is close to BS in that sector.

DCH aggregates the data and sends that aggregated data to the RCH. These data packets are the transmitted to the BS by the RCH if it is in track1 else it will be sent to the nearest DCH or the RCH that belongs to the track of higher level in the hierarchy of track-sector.

3.1.2 DCH and RCH selection

1) Node: (Broadcast->N_Level_id , N_Sector_id) ->BS
2) For each sector id
   2.1. For four consecutive levels find the center of the distance by average of the distance od node from the BS
   2.2. Node nearest to the average distance is made the data cluster head
3) Node: (Own remaining energy) -> DCH
4) DCH: (Information of routing cluster head) -> RCH

In the creation of routing cluster head the communication from base station and nodes are not formed as the location of the nodes is computed from the base station with the help of localization technique. But for the formation of data cluster head, it is required to have the communication between the node and the base station.Taking average of distance from the nodes provides the distance of heavily populated area and the node that is near to that region id elected as the data cluster head.

Due to the formation of two clusters the energy loss is reduced and also lessens the frequency time for selection of new cluster head which is done regularly on the cluster arrangement if it contains only one cluster head in a cluster.

3.2 **Key Management Mechanism to ensure security**

It is not suitable to protect all the types of communication of wireless sensor network using single keying mechanism and to gain good keying mechanism there should be combination of various keys. The different types of key that can be used are "in-network key", "pre-deployed keys" and "broadcast key".

3.2.1 Types of Keys

After the process of "neighbour discovery" all the nodes get updated in their separate buddy information table. Then the base station starts the process of key distribution.

Types of Communication
Type 1: Node to Node communication i.e. N:N

Buddy Key (K_b) is used for N:N by all the node to communicate with each other in its own sector/cluster.

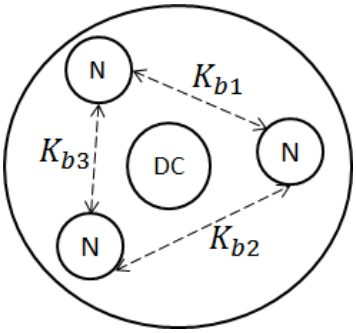


Fig. 3: Buddy key exchanges

Type 2: Base station to node communication i.e. BS:N

Nodes gets authenticated by the BS and then the BS issues Network Key (K_n) to all those nodes. For this, a node first sends the request for gaining network key to the BS. This request is sent by encrypting the request message by My-own-key (K_o)and to the response to this request, the Base station sends K_n to the node who has requested by encrypting it usingK_o.

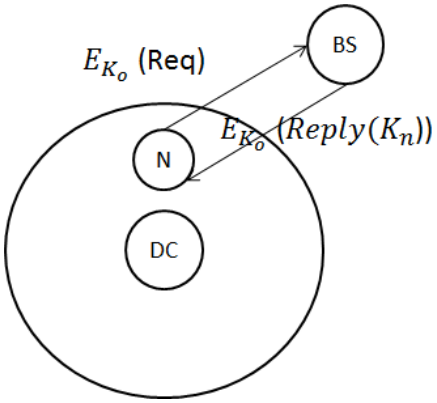


Fig.4: Node to Base Station

Only that node which is authenticated can decrypt this message and gain the network key.

Type 3: Node to Cluster Head communication i.e. N:CH
Network key is used for this type of communication

Type 4: Node to Base station communication i.e. N:BS
My-own-key (K_o) is used by all the nodes. Every node initially consists of its id, and this key is a function of node id, track id, sector id and residual id.

Type 5: DCH to RCH communication i.e. D:R
Cluster key (K_c) is calculated by the CHs to DCH to RCH communication

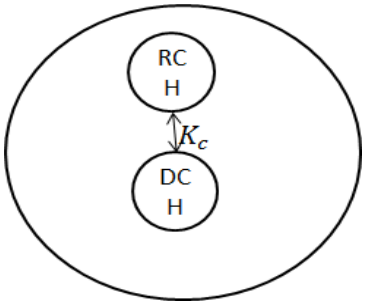


Fig. 5: Cluster Key Communication

Type 6: Cluster Head to BS communication i.e. CH:BS
After the nodes are authenticated as CHs by the BS Broadcast Key (K_{bro}) is issued by the BS.

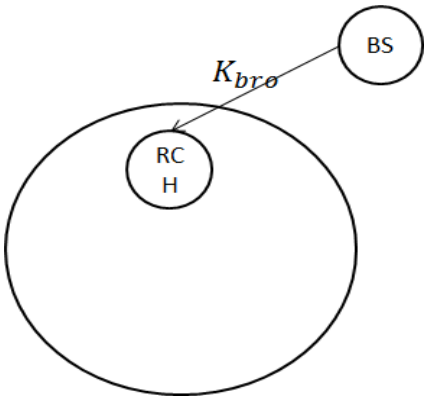


Fig.6: Broadcast Key

3.2.2 Security by the use of keys:

1) .Key distribution: All the keys are not dispersed by the BS. Keys such asK_b, K_c, K_o are computed by the node itself in the network.

2) Key usage

It is very important for every node to know or to calculate their own-key. It is also necessary for all the nodes to have the network key K_n which is used for encrypting and decrypting the message that is broadcasted by the BS periodically.

a) Initial message (M) create by node = {K_b, T , MAC , M}-> DCH
b) DCH Message (DCM) created by DCH ={K_c{K_b, T , MAC , aggregated(M) }}-> RCH
c) RCH Message (RCM) created by RCH ={K_{bro}{K_c{K_b, T , MAC , (DCM) }}}-> BS

The initial message is transmitted to the data cluster head along with the timestamp (T) and MAC by the common nodes. Timestamp is used to elude the replaying of the message which the MAC is used for authentication the message that is being transmitted. This message is send to the DCH using buddy key, this is because to every node the same sector the RCH/DCH will act as buddy neighbour.

The communication between DCH and RCH is by the use of cluster key. And this cluster key is create by the DCH and RCH and is not broadcasted by the BS using sector id, track id and its own key. If in the hierarchical form RCH does not communicate with the BS directly then the message is sent to the nearest RCH or the DCH of the above cluster.

All the messages are sent from the nodes to DCH and at the DCH all the messages get aggregated and transmitted to the RCH by encrypting it with the cluster key.

With this arrangement of the node along with the work division of cluster head into data cluster head and the routing cluster head the overhead on the single cluster head is reduced. Here even if one of the cluster head crashes its work can be performed by other. And usage of multiple keys provides protection from node capture attack. When compared to various protocols discussed in the literature survey, this protocol avoids the dependency on single cluster head and also dependency on symmetric key which causes lack in confidentiality and integrity.

4. ENHANCEMENT TO CLUSTERED PROTOCOL

Usage of five different key which uses different types of keys such as network key, pre-distributed key and broadcast make it difficult to maintain the keys by each node. This is because the buddy maintains a buddy table which contains the neighbour information of all the nodes within a cluster but the nodes are mobile so there is need to regularly update the buddy table which increases overhead. The broadcast key is issued by base station to the routing cluster head when the routing cluster head is selected but if the adversary claim to be as RCH it will receive the broadcast key. To avoid this drawback the network can provide security by using 3-level of security by the use of pre-distributed key and encryption at every level. This encryption can be performed using the XOR mechanism for encryption and the encrypted can verified about its authentication using Hashing function.

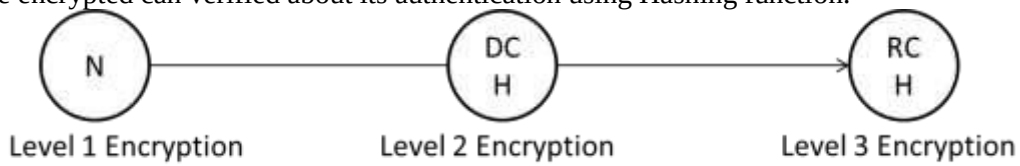


Figure: Three Level of Encryption

The message that has to be sent to the base station is first encrypted at the node, when it reaches the data cluster head it is again encrypted at the data cluster head. This encrypted message is then sent to the RCH where it is again encrypted by RCH and is finally send to BS. At the BS the message using the key of respective nodes because those keys are pre-shared with the base station. The possibility of the message being send by adversary can be avoided because the nodes are the pre-shared and authenticated. At the BS the message is decrypted in the reverse pattern to that in which it is encrypted. This reduced the packet size compared to the previous protocol as it does not require maintaining extra key issued from base station for being part of communication.

5. CONCLUSION:

This paper presents an efficient key management method to secure the wireless sensor network by using multiple keys and show the efficient communication by the use five different keys in hierarchical environment. Due to hierarchical architecture and data sent to base station after aggregation the number of message that is send in reduced to ensure efficient battery consumption. By dividing the network into tracks and sectors we gain a storage effective key management. As five different keys are used and the message that is transmitted along with the message authentication code the confidentiality, security and integrity is maintained. The overhead of maintaining five keys can be avoided using three level of encryption and also provide efficient security.

REFERENCES:

1. D. Jena, “A Secure Key Management Scheme for Hierarchical WSN,” vol. 6, no. 2, pp. 30–37, 2015.
2. Y. Cheng and D. P. Agrawal, “An improved key distribution mechanism for large-scale hierarchical wireless sensor networks,” vol. 5, pp. 35–48, 2007.
3. K. Sharma, “Security Model for Hierarchical Clustered Wireless Sensor Networks,” no. 5, pp. 85–97, 2011.
4. A. Bashir and A. H. Mir, “An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network,” 2013.
5. R. Azarderakhsh, A. Reyhani-masoleh, and Z. Abid, “A Key Management Scheme for Cluster Based Wireless Sensor Networks,” 2008.
6. C. Science and S. Engineering, “A Survey on key Generation and Pre-distribution Technique in wireless Sensor Network,” vol. 4, no. 2, pp. 576–579, 2014.
7. T. Laskar and D. Jena, “A Survey on Key Management Issues in WSN,” vol. 1, no. 5, pp. 74–77, 2012.
8. E. Science, “Cluster Based Mobile Key Management Scheme to Improve Scalability and Mobility in Wireless Sensor Networks,” pp. 22–26, 2015.
9. M. Elhoseny, H. K. El-minir, A. M. Riad, and X. Yuan, “Recent Advances of Secure Clustering Protocols in Wireless Sensor Networks,” vol. 2, no. 11, pp. 400–413, 2014.
10. P. History and V. Patel, “A SURVEY ON CLUSTER BASED KEY,” vol. 43, no. August, pp. 132–136, 2015.
11. M. Aslam, N. Javaid, A. Rahim, U. Nazir, A. Bibi, and Z. A. Khan, “Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks.”
12. A. Braman and G. R. Umapathi, “A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks : A survey,” vol. 3, no. 2, 2014.
13. A. Diop, Y. Qi, and Q. Wang, “Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks,” no. July, pp. 9–18, 2014.
14. H. M. Bhalodiya, S. Kargathara, and M. Meghani, “A Survey on Secure Hierarchical LEACH Protocol over Wireless Sensor Network,” vol. 10, no. 12, pp. 36–41, 2014.
15. N. Gautam, W. Lee, and J. Pyun, “Track-Sector Clustering for Energy Efficient Routing in Wireless Sensor Networks,” pp. 116–121, 2009.