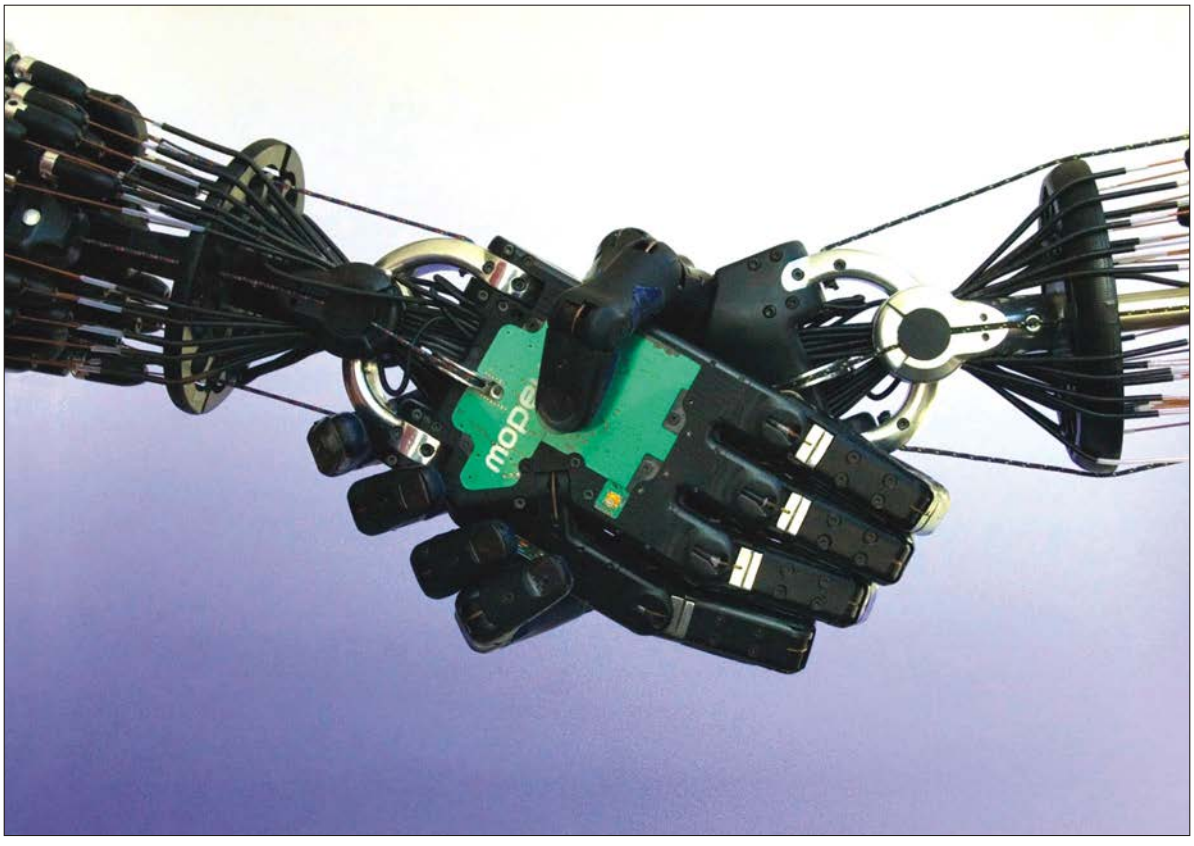

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 5 (4): 130-141, 2012
ISSN 1994-5450 / DOI: 10.3923/jai.2012.130.141

Dynamic Key Management Scheme for HWSN Using Efficient Pair Wise Key Distribution Technique

N. Sugandhi, S. Mirdula, D. Manivannan, R. Ranjini and D.H. Sharmili Minu
SASTRA University, India

Corresponding Author: N. Sugandhi, SASTRA University, India Tel: 9443739800

ABSTRACT

Wireless Sensor Network (WSN) is the well growing technology in the fields of defence, industrial automation, building automation, environmental forecasting, asset management, health care etc. In WSN, each and every node should be secured and this security is achieved by secure group communication. There are many key management techniques used to implement group communication in a secured manner but the key distribution is always being an issue in WSN because of limited capabilities and vulnerable nature of WSN. The proposed WSN totally uses three sort of keys namely Master key, session key and pair wise keys for secured communication are used in WSN. The main goal is to provide secured node to node communication by using efficient pair wise keying mechanism and it uses secret code for secure communication. It provides the better robustness, authentication and more security. The proposed WSN architecture has two hierarchy layers known as H end and L end sensor layers in a cluster. Secured communication between Low end node (L) to Low end node (L) and High end node (H) to High end node (H) follows efficient pair wise keying mechanism. To establish secured communication between Low end node (L) to High end node (H) and Cluster Head (CH) to Cluster Head (CH), new node key should be established before establishing pair wise keying mechanism. Master key is established for the broadcasting of Base Station (BS) to all other nodes. In performance analysis, computation, communication and storage cost are calculated and analysed.

Key words: Wireless sensor network, key management, key distribution, pair wise keying, low end and high end sensor nodes

INTRODUCTION

A Wireless Sensor Network (WSN) is composed of many self-organised autonomous devices called "sensors" which monitor the environment by measuring essential physical parameters such as temperature, pressure, sound, humidity etc. sensor nodes are very small, low power and low cost devices which has the ability to sense, process and communicate to neighbour nodes. It is scattered over the region where the sensor nodes are randomly deployed. WSN has variety of applications in the field of military, health care, environment and disaster management. It can be widely used in ecological aspects such as flood detection, fire detection etc. and miscellaneous aspects such as home application, theft detection and habitat monitoring (Chan *et al*., 2003). The main issues while designing WSN are Node deployment, localization, synchronization and node or link heterogeneity, data aggregation and data dissemination, fault tolerance, security, scalability, medium access

scheme, quality of service etc. WSN is a vulnerable network to various security attacks due to broadcasting nature through wireless medium so providing security is essential for protecting the confidentiality and integrity of communication in WSN (Acharya and Kumar, 2003). To provide the security while exchanging the data between sensor nodes, key is used. The key should not allow unauthorized access. It is more important to achieve security in WSN. These are used for encryption and decryption of messages. Any kind of information and protocols can be used to generate keys.

In WSN, key management provide the key setup, key establishment, distribution and revocation in sensor nodes. The nodes should have the properties such as Self organization, Confidentiality, Authentication, Robustness, Integrity, Synchronization, Data freshness, Flexibility, Accessibility, Scalability, Connectivity, Efficiency (Zaman *et al.*, 2012) and Survivability (Acharya and Kumar, 2003) for efficient key management.

Key distribution schemes are chosen depending on their distributed or hierarchical network architecture, communication methods such as unicast (pair wise), multicast (group wise), broadcast (network wise) (Eschenauer and Gligor, 2002). Security requirements like Authentication, confidentiality, robustness, accessibility, integrity etc and keying methods such as pre distributed mechanism or dynamic generation of pair wise, group wise or network wise methods. Pair wise keying mechanism provides best robustness and authentication between two nodes but it is not flexible (Ren *et al.*, 2011). Group keying mechanism provides group collaboration, multicast, scalability and flexibility but it is difficult to set up and lack in its storage. Network keying mechanism is very simple (Gowrishankar *et al.*, 2008). Using this, BS can broadcast its message to all its beloved sensor nodes. It is scalable and flexible but lack in its robustness.

These key distribution schemes are applicable for both distributed and hierarchical wireless sensor networks. The main difference is nothing but hierarchical WSN provides network wise keying mechanism which does not applicable for distributed WSN. In Distributed WSN, there is no specified architecture. Topology cannot be known before the node deployment. Nodes are randomly scattered over deployment region, then each node should discover the neighbour nodes within the communication range by exchanging key ID. In hierarchical WSN, the network forms the hierarchy in architecture. In this, powerful node is chosen as Base station. Hierarchy structure is formed based upon the capability of sensor nodes. Nodes which are having better resources known as Cluster head and also called as Key Generation Unit. Other nodes are simply called sensor nodes. It forms 2 layers. The first layer consists of H end (Higher layer) sensor nodes. The second layer consists of L end (Lower layer) sensor nodes (Vieira *et al.*, 2006).

Key establishment is essential in Wireless Sensor Network to ensure the network security. Several schemes were proposed earlier to give the brief outline of key distribution schemes. According to the application the distribution schemes are varied. According to the "Network structure" distribution schemes can be classified into Centralized Key distribution schemes and Distributed key distribution schemes. Another way of approach is based on sharing of key. It can be classified as Probabilistic and Deterministic approach. Eschenauer and Gligor (2002) proposed the innovative randomized approach "Key management scheme for distributed sensor Networks" which offers trust between the nodes. Before node deployment each node randomly selects its key and after deployment pair wise key is established for the identification of keys which they share (Camtepe and Yener, 2005).

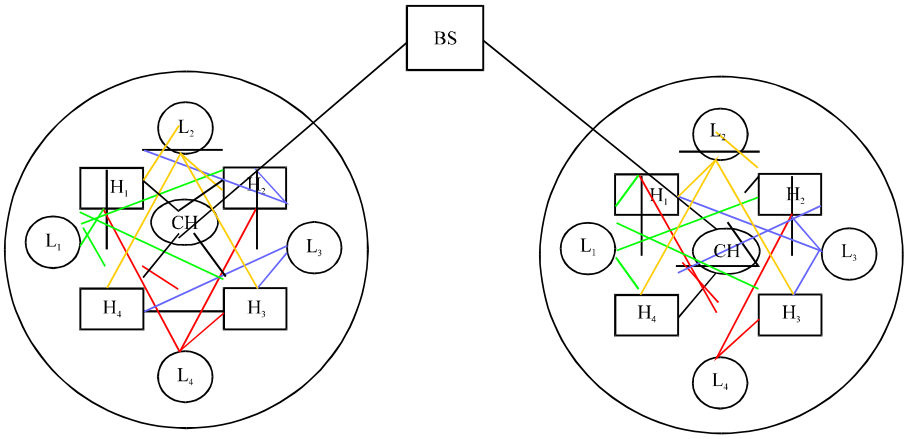

Fig. 1: Proposed WSN architecture

Chan *et al.* (2003) proposed a "Random key distribution scheme by using q-composite keys for sensor networks" (Du *et al.*, 2003). In this scheme, q set of common keys were introduced instead of using single key in order to increase the resiliency in the network. This approach is similar to Eschanauer and Gligor approach but 'q' set of keys only used in that. A novel key management scheme for wireless sensor network in which scheme LEAP (Localized Encryption and Authentication Protocol) is proposed. It provides better encryption and authentication to overcome the node limitations.

ASSUMPTIONS

For proposed method the following assumptions have been made:

- Base station is the top most powerful node in the WSN
- CH is the second powerful node in the cluster
- CH will never compromise with attackers
- High end sensor nodes are more powerful than Low end sensors node
- CH will dynamically change if necessary

PROPOSED STUDY

In proposed study, HWSN (Heterogeneous Wireless sensor network) comprises of different clusters includes L end sensor nodes, H end sensor nodes, CH and BS (Tuah *et al.*, 2012). BS is the most powerful unit which is used to monitor and control intra and inter cluster communication. Each cluster consists of one CH and more number of High and low end sensor nodes. CH is the head of all H and L sensor nodes.

L end sensor nodes act as normal node. Any one node from H sensors are selected as CH as per the request from them. CH have higher capacity, more computing power and better communication capability can be selected as CH.

Figure 1 represents that, all the High end sensor nodes are directly connected with CH. Low end sensor nodes are connected with all High end sensor nodes. All sort of communications (L-L, L-H, H-H and H-CH and CH-CH) are possible in the WSN. The intra cluster communication is controlled by CH and the inter cluster communication is taken care by BS.

SELECTION PROCESS OF CH

If anyone powerful node among H end nodes consider node i wants to be act as Cluster Head (CH), it will directly send the request message to the Base Station (BS). This message consists of node ID, authentication code, encrypted message with secret communication key (K_{BHi}) and random nonce. i.e.:

$Node\ Id_i$	R_{ni}	E_{KBH} (M)	S_{Ci}

Base Station receives the message from node i and it retrieves the secret communication key (K_{BHi}) from node id of i. Once the base station authenticates the node i as cluster head, then it communicates the information about CH to other nodes which are present within the sensor field through broadcasting techniques. This followed diagram represents the sequence flow between node and BS.

NODE REGISTRATION

Figure 2 gives the clear view of CH selection and registration process. In this, every node which received the message from base station wants to register the node information to cluster head. WSN comprises the nodes with same and different capabilities for example H and L end sensor nodes are registered with their information to the CH. Each node generates the message that includes node ID, cluster head ID, random nonce i and master key.

$Node\ Id_i$	$CH\ Id_i$	R_i	K_M

Each sensor node generates one packet that includes Node ID_i, E_{KBHi} (M), S_{Ci} (M). Cluster head receives all the message packets from each node and decrypts the message using master key, it

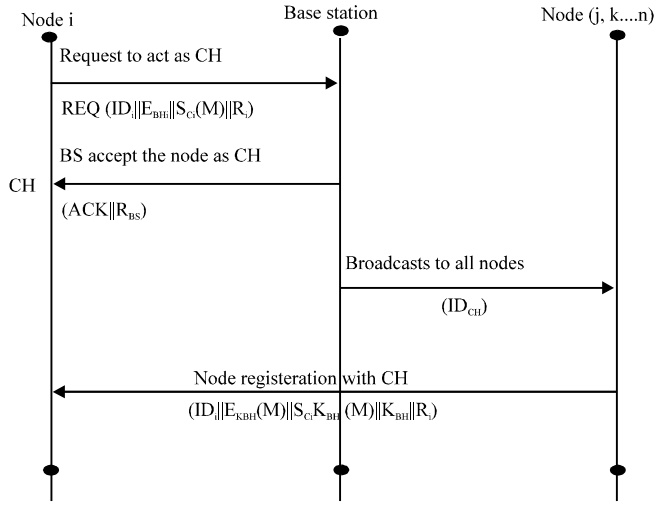

Fig. 2: Cluster head selection and registration process

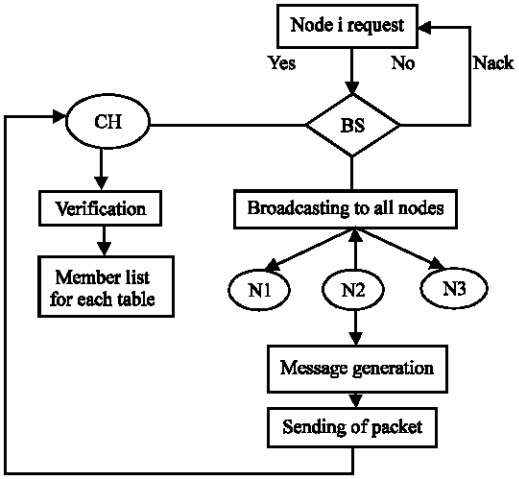

Fig. 3: Registration of individual node in WSN

verify authentication code message and individual node ID. At the final stage each cluster head in the sensor field will have their authenticated member nodes. Repeatedly each cluster head registers their individual group members and finally build their entire cluster. Figure 3 reflects the node registration process. Initially node i give the request to the base station. The base station broadcasts that information to all the nodes in the region. The message is generated by the corresponding node. The packet is send to cluster head and CH verifies the packet. It checks the node corresponding to the member list table or not. If the node present in the member list table then it sends the packet else negative acknowledgment given to the node.

DIVISION OF CLUSTERS

If more number of H and L sensor nodes is present in the sensor field, it can be splitted into two or more number of clusters. Division of clusters is needed for managing large number of sensor nodes. For each cluster, the powerful H node selected as cluster head and node registration process is carried out. In that cluster H end sensor layer and L end sensor layer will be formed on the basis of number of nodes. Cluster head to cluster head and nodes in one cluster to other cluster communication can also be possible because the communication is established between intra and inter clusters (Gao *et al*., 2012).

COMMUNICATION PROCESS

To establish the communication between any two nodes in the sensor field, a secret key should be loaded. Normally keying process is used to establish the secure communication between all sensor nodes but secure key distribution is always being an issue in WSN. To overcome this issue, BS has four sort of keys namely Master key K_{Mk}, Cluster head key CH_{ki}, Secret key between BS and H sensor node K_{BHi} and Secret key between BS and L sensor node $K_{BLi,}$ session key K_{SES}, for secure communication between L to L, H to H, L to H, H to CH and CH to CH, pair wise key is established (Abdullah, 2011).

PAIR WISE KEY ESTABLISHMENT

Low end sensor node to low end sensor node (L_i (L_1) to L_j (L_4)): In establishment of pair wise key between sensor nodes L_1 and L_4 in the sensor field, the following procedures are carried out. At

low end sensor node L_1, using session key K_{SES}, it encrypts the node information includes its node id L_1, near end High end sensor node id is H_1 and corresponding cluster head id CH_1 and generate the p-value:

$$p = E_{K\,SES}\ (L1 \| H1 \| CH1) \tag{1}$$

At low end sensor node L_4, using session key K_{SES}, L_4 encrypts the node information includes its node id L_4, near end H sensor node id is H_3 and corresponding cluster head id CH_1 and generate the Q-value.

$$Q = E_{K\,SES}\ (L4 \| H3 \| CH3) \tag{2}$$

The H sensor node information and cluster head information are used to authenticate and validate the information shared from low end sensor nodes to another end. L_1 generate random nonce LR_1 with respect to time. Then broadcast this with sensor node id L_1, H_1, CH_1 to all the nodes in the sensor field:

$$L_1 \| H_1 \| CH_1 \| LR_1 \tag{3}$$

L_4 receives (if it is in communication range) the message from L_1 and generates one Secret Code, $S_c = E_Q(L_1, R_1, H_1)$. Then, broadcast Secret Code S_c along with its node id. Now L_1 receives Secret Code S_c, node id L_4 and H_3. It checks S_c value, once S_c value matched then the key establishment taken place. Now sensor Node L_1 knows the Q value. At node L_1, the pair wise key is generated for communication between L_1 and L_4 using P and Q. For example:

$$\text{At node } L_3;\ L_1 \| H_1 \| CH_1 \| LR_1 \tag{4}$$

$$\text{At node } L_4;\ K_{PQ} = E_P\ (L_4 \| H_3) \tag{5}$$

Now, the value of P and Q are updated into K_{PQ}, Low end sensor nodes L_1 and L_4 will have common pair wise key K_{PQ} for data communication among the network. This is shown in Fig. 4.

Low end sensor node to high end sensor node ($L_i(L_1)$ to $H_i(H_1)$): Figure 5 gives the brief view of communication establishment between H end sensor nodes with L end sensor node, instead of pair wise key a new node key can be established. To load a new node key at Low end sensor node for data communication between sensor nodes L_1 and H_3 in the sensor field, the following procedures are carried out. The message is generated at low end sensor node, it has the following procedure, L_1 generates random nonce LR_1 with respect to time and generate Secret Code using Q.

Then it broadcast this value with sensor node id L_1, H_1, CH_1 to all the nodes in the sensor field. Using session key K_{SES} it encrypts sensor node id, High end node id, random nonce value, secret code and cluster head Information:

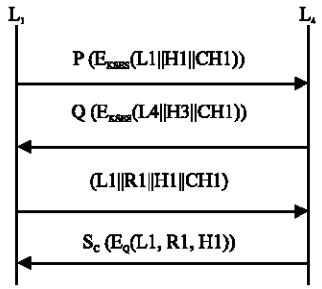

Fig. 4: Low end node to Low end node communication

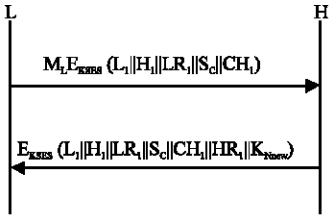

Fig. 5: Low end node to High end node communication

$$M_L = E_{K\,SES}\ (L_1 \| H_1 \| LR_1 \| S_C \| CH_1) \tag{6}$$

At high end node, one message is generated with the help of M_L and High end node id, Cluster head information, Random number generated by High end sensor node. It generates new node key for data communication between Low end sensors and high end sensor node. The message format of M_H is:

$$M_H = E_{K\,SES}\ (L_1 \| H_1 \| LR_1 \| S_C \| CH_1 \| HR_1 \| K_{N\,new}) \tag{7}$$

Then after sharing the random number of high end sensor node from low end sensor node, the new node key is established.

High end sensor node to high end sensor node ($H_i(H_1)$ to $H_j(H_4)$): In establishing pair wise key between sensor nodes H_1 and H_4 in the sensor field, the following procedures are carried out. At high end sensor node H_1, using session key K_{SES}, H_1 encrypts the node information includes its node id H_1 and corresponding cluster head id CH_1 and generate the 'X' value:

$$X = E_{K\,SES}\ (H_1 \| CH_1) \tag{8}$$

At high end sensor node H_4, using session key K_{SES}, H_4 encrypts the node information includes its node id H_4 and corresponding cluster head id CH_1 and generate the 'Y' value:

$$Y = E_{K\,SES}\ (H_4 \| CH_1) \tag{9}$$

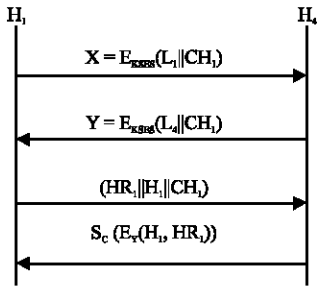

Fig. 6: High end node to High end node communication

The cluster head information is used to authenticate and validate the information shared from high end sensor nodes to another high end node. H_1 generate random nonce HR_1 with respect to time. Then broadcast this value with sensor node id H_1, CH_1 to all the nodes in the sensor field:

$$H_1 \| CH_1 \| HR_1 \tag{10}$$

H_4 receives the message from H_1 and generates one Secret Code:

$$S_C = E_Y\ (H_1, HR_1) \tag{11}$$

Then, broadcast Secret Code S_c along with its node id. Now H_1 receives Secret Code S_c, node id H_4. It checks S_c value, once S_c value matched then the key establishment taken place. Now sensor Node H_1 knows the Y value. At node H_1, the pair wise key is generated for communication between H_1 and H_4 using X and Y. For example:

$$\text{At node } H_1;\ K_{XY} = E_Y\ (H_1) \tag{12}$$

$$\text{At node } H_4;\ K_{XY} = E_X\ (H_4) \tag{13}$$

Now, the value of X and Y are updated into K_{XY}, High end sensor nodes H_1 and H_4 will have common pair wise key K_{XY} for data communication among the network. This is shown in Fig. 6. Similar procedure is followed for other node to node communication.

NODE ADDITION AND DELETION

If any node wants to join in the sensor network first it sends the joining request to BS. BS finds the location where to add that node. It checks the node capability and it ensures that it comes under whether H or L sensor layer. In this node architecture there are two layers below the cluster head. One is lower end sensor layer and other is higher end sensor layer. The location of node joining is at two places that will be based on the requirement of the application. The node may join in L end sensor layer (Lower layer) and H end sensor layer (Higher layer). CH will inform to all the nodes about the newly added node and finally CH will give information to BS. If a node gets added in H

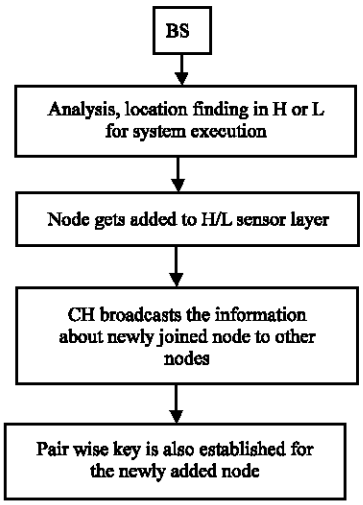

Fig. 7: Addition of new node

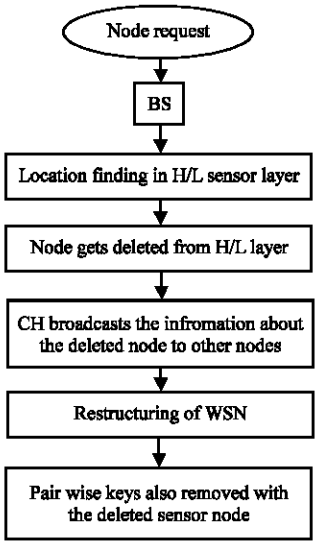

Fig. 8: Deletion of an existing node

or L sensor layer, it should establish the pair wise key for its further communication. Similar procedure is followed for node deletion. If the node gets deleted, then its pair wise keys are not used. In Fig. 7 and 8, the clear view of node addition and deletion is given.

KEY UPDATION

Sensor nodes in WSN are deployed in open and unattended environment. It is vulnerable to external attacks. If any node in sensor field compromise means, the node information and key used in sensor nodes are exposed to update the different keys used in the WSN. The secret communication for each node, master key and cluster head key and pair wise keys are updated and a new set of keys for all the entities are generated and that new values are securely distributed to all the entities in WSN. By using Mixed Column Technique (MCT) new keys are generated to update the old keys. Each byte of the column is mapped into new value. The mixed column

transformation is the function of all the four columns. This kind of transformation is represented by the variable called "STATE". The old key is multiplied with secret key to form the new key matrix. The final value is converted to hexadecimal value. It depends upon the new node joined or existing node may leave from the network. Using the MCT, the old keys are updated and finally all the new nodes must updated with new pair wise secret key:

$$\begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{012} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} \times \begin{bmatrix} N_{00} & N_{01} & N_{02} & N_{03} \\ N_{10} & N_{11} & N_{012} & N_{13} \\ N_{20} & N_{21} & N_{22} & N_{23} \\ N_{30} & N_{31} & N_{32} & N_{33} \end{bmatrix} = \begin{bmatrix} S'_{00} & S'_{01} & S'_{02} & S'_{03} \\ S'_{10} & S'_{11} & S'_{012} & S'_{13} \\ S'_{20} & S'_{21} & S'_{22} & S'_{23} \\ S'_{30} & S'_{31} & S'_{32} & S'_{33} \end{bmatrix}$$

Old key matrix Secret matrix New key matrix

PERFORMANCE ANALYSIS

The proposed scheme can be evaluated in terms of Computation, communication and storage with LEAP. The computation and communication cost can be calculated for H and L end sensor nodes but it is not essential for CH because it has enough capabilities. The total numbers of encrypted and decrypted messages are used to calculate the computation cost. In a network of size N and node connection degree d, the computation cost will be calculated by using following equation stated as:

$$(2d+1)\ N+4N$$

Here, pair wise key generation takes (2d+1) cost for computation of the entire nodes. 4N is the computation cost foe node keys generation. If N is fixed, then the cost will be depending on the nodes density and the complexity will be O (d).LEAP requires the computation costs of:

$$\frac{2\left((d-1)^2\right)}{N-1}+2$$

This proposed scheme provides less complexity while compared to LEAP and other mechanisms. The communication cost can be calculated by using number of transmission and reception of messages while node key and pair wise key generation. The communication cost will be obtained by using 2dN+3N equation.

The communication costs of LEAP is O (log N).The cost of storage can be calculated as per the possible number of keys present in each node. In proposed scheme, each node consists of one node key and D pair wise keys. So the storage cost will be calculated by equation D+1. But the LEAP requires 3D+2+L storage cost because it includes key chain cost. So the proposed scheme is efficient while considering computation, communication and storage cost of other schemes (Table 1).

Table 1: Comparison of proposed work with LEAP

	Proposed work	LEAP
Communication cost	2dN+3N	O (log N)
Computation cost	(2d+1) N+4N	$\frac{2\left((d-1)^2\right)}{N-1}+2$
Storage cost	D+1	3D+2+L

CONCLUSION

The proposed scheme provides better robustness, authentication and security for node to node communication by establishing efficient pair wise keying mechanism. It gives the clear view about the cluster head selection from H end sensor nodes, node registration, formations of clusters, node addition, deletion, efficient key distribution and key updation. It provides secured node to node communication between intra and inter cluster communication. In this proposed scheme all sort of communications are possible between L end sensor nodes, H end sensor nodes, CH and BS. It manages the communication, computation and storage cost effectively while comparing with other available key distribution schemes.

NOTATIONS

CH	=	Cluster head
BS	=	Base station
Id_i	=	Identification of node i
ID_{CH}	=	Identification of CH
R_{ni}	=	Random nonce for node i
R_{BS}	=	Random nonce for BS
T_i	=	Time bound
S_{ci}	=	Secret code
K_{BHi}	=	Secret Key from H end node to BS
K_{BLi}	=	Secret key between L end node to BS
K_M	=	Master key for broadcasting from BS to all the nodes
K_{SES}	=	Session key
K_{PQ}	=	Pair wise key between two nodes

REFERENCES

Abdullah, M.I., 2011. A key distribution and management scheme for hierarchical wireless sensor network. Int. J. Multimedia Ubiquitous Eng., 6: 1-12.

Acharya, D. and V. Kumar, 2003. Location aware pair-wise key generation schemes for wireless sensor networks. pp: 1-4. http://web.mst.edu/~cswebdb/Workshop-AFRL/Paper21909620.pdf

Camtepe, S.A. and B. Yener, 2005. Key distribution mechanisms for wireless sensor networks: A survey. Department of Computer Science, Rensselaer Polytechnic Institute, Technical Report TR-05-07.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Research in Security and Privacy, May 11-14, 2003, IEEE Computer Society, Washington, DC., pp: 197-213.

Du, W., J. Deng, Y.S. Han and P.K. Varshney, 2003. A pairwise key predistribution scheme for wireless sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, October 27-30, 2003, New York, NY, USA, 42-51.

Eschenauer, L. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, November 18-22, 2002, Washington, DC, USA, pp: 41-47.

Gao, C., X. Hu, B. Wang, H. Gao and W. Xiong, 2012. Data dissemination in wireless sensor networks with clustering method. Inform. Technol. J., 11: 1477-1483.

Gowrishankar, S., T.G. Basavaraju, D.H. Manjaiah and S.K. Sarkar, 2008. Issues in wireless sensor networks. Proceedings of the World Congress on Engineering, Volume 1, July 2-4, 2008, London, UK.

Ren, H., X. Sun, Z. Ruan and B. Wang, 2011. An efficient scheme against node capture attacks using secure pairwise key for sensor networks. Inform. Technol. J., 10: 71-79.

Tuah, N., M. Ismail and K. Jumari, 2012. An energy-efficient node-clustering algorithm in heterogeneous wireless sensor networks: A survey. J. Applied Sci., 12: 1332-1344.

Vieira, M.A.M., A.B. da Cunha and D.C. da Silva Jr., 2006. Designing wireless sensor nodes. Proceedings of the Workshop Embedded Computer System: Architectures Modelling and Simulation, July, 2006, Samos, Greek, pp: 99-108.

Zaman, N., L.T. Jung, F. Alsaade and T. Alghamdi, 2012. Wireless sensor network (WSN): Routing security, reliability and energy efficiency. J. Applied Sci., 12: 593-597.