Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Key Pool Formation & Key Dissemination Scheme for WSN

Bhawna Jyoti, Ritu Mishra
Computer Science Department
Maharishi Markandeshwar University,
Solan, India

Abstract—A wireless sensor network is a collection of light-weight, low power, small size sensor nodes. Providing security for Wireless Sensor Networks (WSN) presents a unique challenge. Key Management is a security aspect that gets a great deal of attention in Wireless Sensor Networks. Key Management establishes the keys that are required for providing confidentiality, integrity and authentication requirements. A new key management scheme is proposed "Secure Key Pool Formation"(SKPF) for Wireless Sensor Networks. This scheme assumes that a pool of keys is originated at the B.S. that has specific number of keys generated randomly using a random number generator function. At the same time, the B.S. randomly generates key ID for uniquely identifying each key.Also each sensor is provided with group of keys of equal sizes, and these keys has to be picked randomly without removing any key from the key pool. This leads the sensors to have some sharing keys between each other which make node-node communication possible (these keys called sharing keys). Meanwhile, the B.S. provides each sensor with at least one unique key (named Master Key) which is to be used to communicate between each node and the B.S. This proposed scheme will provide security, where the CHs are choose on rotation basis in the network making it harder for intruders to know the routing elements and attack them.

Keywords— Wireless Sensor Networks, Clustering, LEACH, Random dissemination of keys, Security.

I. INTRODUCTION

The wireless sensor network is an emerging field having integrated approach of sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyberspace out into the physical world. As water flows to fill every room of a submerged ship, the mesh networking connectivity will seek out and exploit any possible communication path by hopping data from node to node in search of its destination. While the capabilities of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities.

The choice of a good security mechanism for wireless sensor networks depends on network application and environmental conditions. It also depends on other factors like sensor node processor performance, memory capacity and energy. While in traditional networks, standard security requirements, such as availability, integrity, authentication, and non-repudiation, are sufficient for security, in sensor networks but special security requirements such as message freshness, intrusion detection, intrusion tolerance, are necessary in addition.

II. BACKGROUND AND RELATED CONCEPTS

Key Management in WSN provides very critical security service which leads to the authentication and confidentiality of sensor nodes. But implementation of Key Management schemes in WSN which is a difficult task because of the vulnerabilities of the sensor nodes and their resource limitations. Security in WSN has following challenges:

(i) Wireless nature of communication and resource limitation on sensor nodes.

(ii) Very large and dense WSN having lack of fixed infrastructure.

(iii) Unknown network topology prior to deployment and suffers from high risk of physical attacks to unattended sensor networks.

Security solutions for deploying sensor networks has its roots on existence of strong and efficient key dissemination mechanisms. The sensor nodes have to adapt their environments, and establish a secure network by: (i) using pre-distributed keys or keying materials, (ii) exchanging information with their immediate neighbors, or (iii) exchanging information with computationally robust nodes.

There are various ways in which key management schemes can be classified in wireless sensor networks by considering different benchmarks[15][16]. Various researchers gave different taxonomies. Key management schemes can be broadly classified into dynamic or static solutions based on whether rekeying of administrative keys is enabled post network deployment or not. Schemes are also classified into homogeneous or heterogeneous schemes with regard to the role of network nodes in the key management process. Homogeneous schemes generally assume a flat network model, while heterogeneous schemes are intended for both flat and clustered networks. Another criterion is hierarchical [18]and distributed sensor networks[15] based on network models. Efficient ways of key distribution among the nodes within the cluster having separate controllers of each cluster are discussed in [17].Cluster based public infrastructure is used for lightweight implementation of public key infrastructure [18]. Clustering algorithm can be classified into two major categories: distributed and centralized clustering[21].A Mobility-Energy-Degree-Distance to the Base Station (MED-BS) Clustering Algorithm for the small-scale wireless Sensor Networks is discussed in [14]. A node with lower mobility, higher residual energy and closer to the base station is more likely elected as a cluster head. The members of each cluster communicate directly with their Cluster Heads (CHs) and each Cluster Head aggregates the received messages and transmits them directly to the base station which reduces the energy consumption and to balance the energy load among all nodes[14].

A platform is introduced in which public key cryptography is used to establish a secure link between sensor nodes and gateways. Instead of preloading a large number of keys into the sensor nodes, each node requests a session key from the gateway to establish a secure link with its neighbors after clustering phase which provides significant saving in storage space, transmission overhead, and perfect resilience against node capture[13].

Key dissemination in distributed wireless sensor networks uses three approaches probabilistic, deterministic [15]. The use of dynamic key management reduced the amount of key storage and computing which aims to prevent leakage of information by sensor nodes [4].Key pre-distribution phase[4][19][20] is an important starting phase where keys are distributed before the deployment of the network, i.e. during the node's manufacturing time. This is followed by the key establishment phase which refers to how nodes will establish a secure session. The network formation phase is then initiated. Node addition or Node deletion phase deals with establishment of secure sessions with new nodes being added or removed from the network.

LEACH was first proposed to reduce total energy consumption in sensor networks. It assumed that every node can directly communicate with a BS using a high enough transmitting power. LEACH consists of two phases : the setup phase (initial phase) and the steady state phase (real transmission phase) [2,19,20]. In the first phase, cluster heads are selected and clusters are formed, and in the second phase, the data transfer to the base station is held. During the first phase, the process of electing cluster heads is triggered to select future cluster heads. Thus, a predetermined fraction of nodes connected as cluster heads according either *0* or *1*. If the random number is less than a threshold *T_{s}* then the node becomes a cluster head in the current round, other- value will be elected as CH. wise the node n is expected to join the nearest cluster head in its neighborhood. The threshold is set as:

$$T(n) = \begin{cases} \dfrac{T}{1 - p(r \mod \dfrac{1}{p})} & \text{if } n \in G \\ 0 & \text{Otherwise} \end{cases}$$

where *r* is the current round number (starting from round 0), *P* the probability for each node to become cluster head and *G* the set of nodes that have not been cluster-head in the last 1/*p* round. The election probability of nodes *G* to become cluster heads increases in each round in the same epoch and becomes equal to 1 in the last round of the epoch.

III. PROPOSED KEY MANAGEMENT SCHEME

The success of a key management scheme is determined in by its ability to efficiently survive attacks on highly vulnerable and resource challenged sensor networks. A new key management scheme is proposed "Secure Key Pool Architecture[SKPA] for Wireless Sensor Networks. To define our problem statement, we are using a top-down approach .The main idea here is to break the whole problem into small problems at the beginning, and at the same time having the ability to apply different levels of security to the various sensor nodes at each level . To handle the security at different levels, we can divide it according to the type of communications that may appear in WSN, where we have node to node communication and node to B.S. communication. In order to have a secure network we need to secure these communications.

A.The Network Model

The basic idea for communication between cluster head and base station is that, Cluster heads (CHs) pass messages between groups of nodes (group for each CH) and the base station (BS).This proposed scheme will provide security, where the CHs are rotating from node to node in the network making it harder for intruders to know the routing elements and attack them.

This scheme assumes that a pool of keys is generated at the B.S. that has specific number of keys generated randomly using a random number generator function. At the same time, the B.S. randomly generates key ID for uniquely identifying each key. Then, we provide each sensor with group of keys with equal sizes for each sensor, and these keys has to be picked randomly without removing any key from the key pool. This leads the sensors to have some sharing keys between each other which make node-node communication possible (these keys called sharing keys). Meanwhile, the B.S. provides each sensor with at least one unique key (named Master Key) which is to be used to communicate between each node and the B.S. Some of the assumptions made in clustered for communicating in wireless sensor network are as following:

- The network is shaped by N sensors nodes deployed in square field and has designed cluster hierarchical topology. Sensor nodes are immobile.
- The base station is located outside the sensing field and is a fixed base station.
- Nodes are deployed randomly. This method is applicable for small networks.

- The base station location is pre-determined.
- The cluster head nodes are cognizant of its members and can communicate directly with them.
- Each sensor node communicates with their respective cluster.

Table 1: Notations used for proposed scheme

Symbol	Meaning
CH	Cluster head
BS	Base Station
ID	Identification
N	No of nodes
G	No. of Clusters
mkid	Master key ID for each node
T_n	Threshold function
r	current round number
p	The probability for each node to become cluster head

B. The Proposed algorithm

Key Generation Phase And Selection Of CH

Step 1: B.S. generates a pool of number of key IDs randomly using random number generator function.

$$B.S. \quad \longrightarrow \quad IDs$$

Step 2: B.S. assigns a specific flag that represents the first generation of key (i.e. 001 for example).

$$B.S.(flag) \ \longrightarrow \ IDs$$

Step 3: Each sensor node of a cluster is assigned with unique key ID and one unique master key to communicate between each node and the B.S.

$$B.S.IDs \quad \longrightarrow \quad NG + NG(mkid)$$

Step:4 Each sensor node is checked for the process of electing cluster heads in which node is triggered to select future cluster heads. A predetermined fraction of nodes connected as cluster heads according either *0* or *1*. If the random number is less than a threshold $T\_\{s\}$ then the node becomes a cluster head in in the current round, other- value will be elected as CH. wise the node n is expected to join the nearest cluster head in its neighborhood. The threshold is set as:

$$T(n)=\begin{cases}\dfrac{T}{1-p(r \bmod \dfrac{1}{p})} & if\ n\in G\\ 0 & \text{Otherwise}\end{cases}$$

where *r* is the current round number (starting from round 0), *P* the probability for each node to become cluster head and *G* the set of nodes that have not been cluster-head in the last 1/*p* round. The election probability of nodes *G* to become cluster heads increases in each round in the same epoch and becomes equal to 1 in the last round of the epoch.

$$From\ NG, select\ CH.$$

Step 5: Randomly, the B.S. may refresh its keys by calculating a new value of each key using its related old key, and one of the numbers that are previously distributed to the sensors. The new ID for the key will be the second generation flag plus the old key (i.e. 0010… for example). B.S. then distributes the new group of keys on its new sensors.

***Set Up Phase*:**

Step1: CH include the IDs of keys of sensor nodes in the key group.

$$IDs(NG)||\,CH$$

Step 2: Each of these ordinary nodes sends the message to CH requesting to join its group using MAC.

$$N\ msg\left(\ IDs(NG)||IDs(\ CH)\big|\big|r\big|\big|join_{reques\ t_{message}}\right) \longrightarrow \ CH$$

Step 3: Each CH then sends a confirmation message to approved nodes using MAC.

$$CHmsg(ID(CH)||\ confirm\_join\_group||IDNG) \quad \longrightarrow \quad Napproved$$

Steady Phase:

Step1 Each sensor node transmits message containing data to the CH using MAC.

$$N\ msg(\ ID(NG)||\ ID(\ CH)\ \ ||encrypted\ data) \ \longrightarrow \quad CH$$

Step 2: CH sends final data (aggregated data from all the nodes) to the BS using master key from ID of CH.

$CH\ msg(ID(CH)||ID(BS)||aggregated\ data\ from\ all\ nodes) \quad \longrightarrow \quad BS$

Algorithmic steps involved are:

Table 2:

- **Key Generation Phase And Selection Of CH:**

Step 1: $B.S. \quad \longrightarrow \quad IDs$

Step 2: $B.S.(flag) \quad \longrightarrow \quad IDs$

Step 3: $B.S.IDs \quad \longrightarrow \quad NG + NG(mkid)$

Step 4: $From\ NG, select\ CH.$

- **Set Up Phase:**

Step 1: $IDs(NG)||\ CH$

Step 2: $N\ msg\left(IDs(NG)||IDs(\ CH)\left|\left|r\right|\right|join_{reques\ t_{message}} \right) \longrightarrow \quad CH$

Step 3: $CHmsg(ID(CH)||\ confirm\_join\_group||IDNG) \quad \longrightarrow \quad Napproved$

- **Steady Phase:**

Step 1: $N\ msg(\ ID(NG)||\ ID(\ CH)\ \ ||encrypted\ data) \quad \longrightarrow \quad CH$

Step 2: $CH\ msg(ID(CH)||ID(BS)||aggregated\ data\ from\ all\ nodes) \quad \longrightarrow BS$

C. Flow Chart

- KEY GENERATION PHASE AND SELECTION OF CH

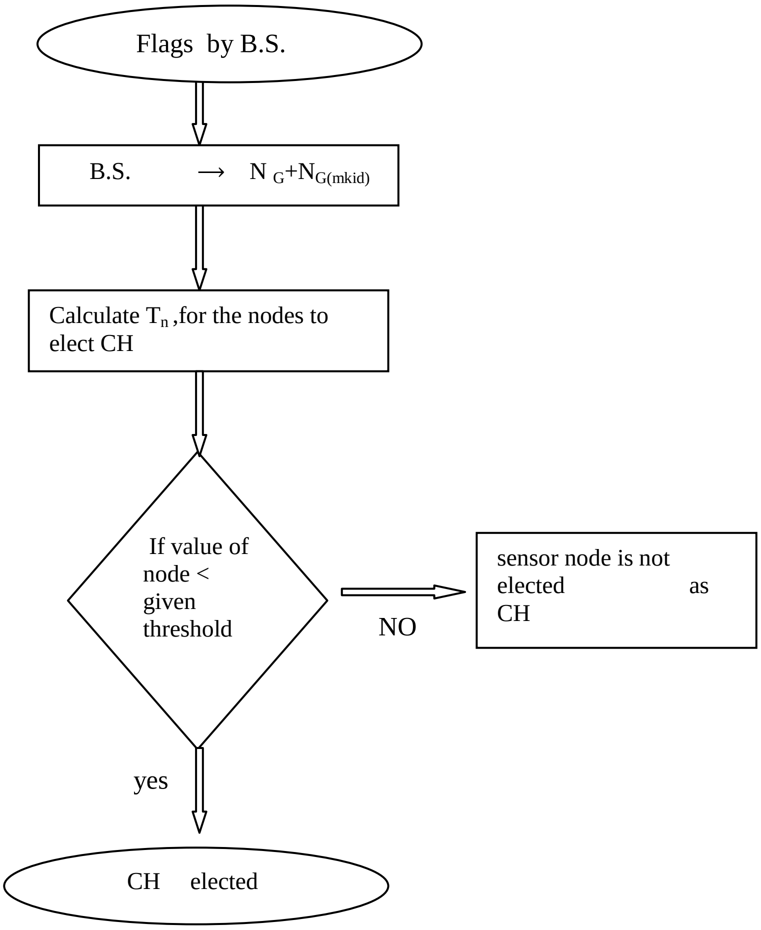
Flags by B.S.
B.S. ⟶ N_G+$N_{G(mkid)}$
Calculate T_n ,for the nodes to elect CH
If value of node < given threshold
NO
sensor node is not elected as CH
yes
CH elected

Fig. 1 Flow Chart of key generation phase

- Set Up Phase**:**

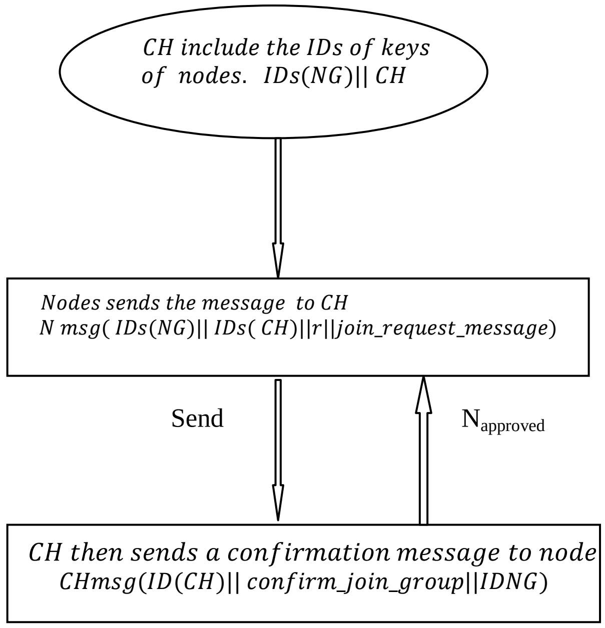
CH include the IDs of keys of nodes. IDs(NG)|| CH
Nodes sends the message to CH
N msg(IDs(NG)|| IDs(CH)||r||join_request_message)
Send
N approved
CH then sends a confirmation message to node
CHmsg(ID(CH)|| confirm_join_group||IDNG)

Fig.2 Flow Chart of set up phase

- Steady Phase

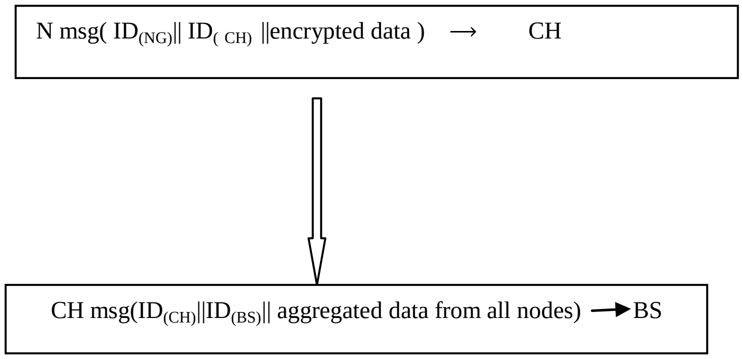
N msg(ID(NG)|| ID(CH) ||encrypted data) ⟶ CH
CH msg(ID(CH)||ID(BS)|| aggregated data from all nodes) ⟶BS

Fig.3 Flow Chart of steady phase.

IV EXPLANATION

This algorithm provides authenticity, confidentiality and freshness for node to node communication. Here, we are analyzing the immunity of the key dissemination scheme against the most known attacks in WSNs:

Data flow blocking: the key dissemination scheme uses random number function and assigning the keys from key pool by the base station which makes it difficult for an adversary to prevent the arrival of messages to sensor nodes.

Physical attacks: In hostile environment, some sensor nodes can be captured and tampered. Obviously, the most sensitive information is shared keys. The impact of such attack affects only secure links with immediate neighbors and not the whole network.

Replay attack: if an attacker tries to replay old messages, this does not hold because every node stores the last nonce and leads to security.

Black hole: if an attacker with high communication capabilities rebroadcasts a message, it cannot create a black hole in the WSN because it can't be authenticated by sensor nodes.

Sybil attack : even if an attackers takes multiple identities, this does not hold because it can’t be authenticated as there is a use of cluster head and secure key pool architecture.

The security level is not impacted by number of nodes present in network architecture but it depends upon the size of key group assigned for each node according to the total size of the key pool generated. In WSN, there is a fixed space for each node to store the key group selected from the key pool. This means the size of the group (GS) is fixed at the first time the network is built. Then, after GS is determined, the size of the key pool (PS) will affect the network in appropriate level of security and sharing keys probabilities as given in [21].

Security level= 1- size of group of sensor nodes in network architecture/size of pool of keys generated.

Since, we used the same technique to generate the key pool and to provide the key groups, then the issue of key sharing technique will get the same performance proposed by Sec-LEACH. Because all CHs use the same single hop to communicate with the B.S, then increasing the number of CH will lead to more power consumption. We follow the Key Distribution scheme used by Sec-LEACH to produce the sharing keys.

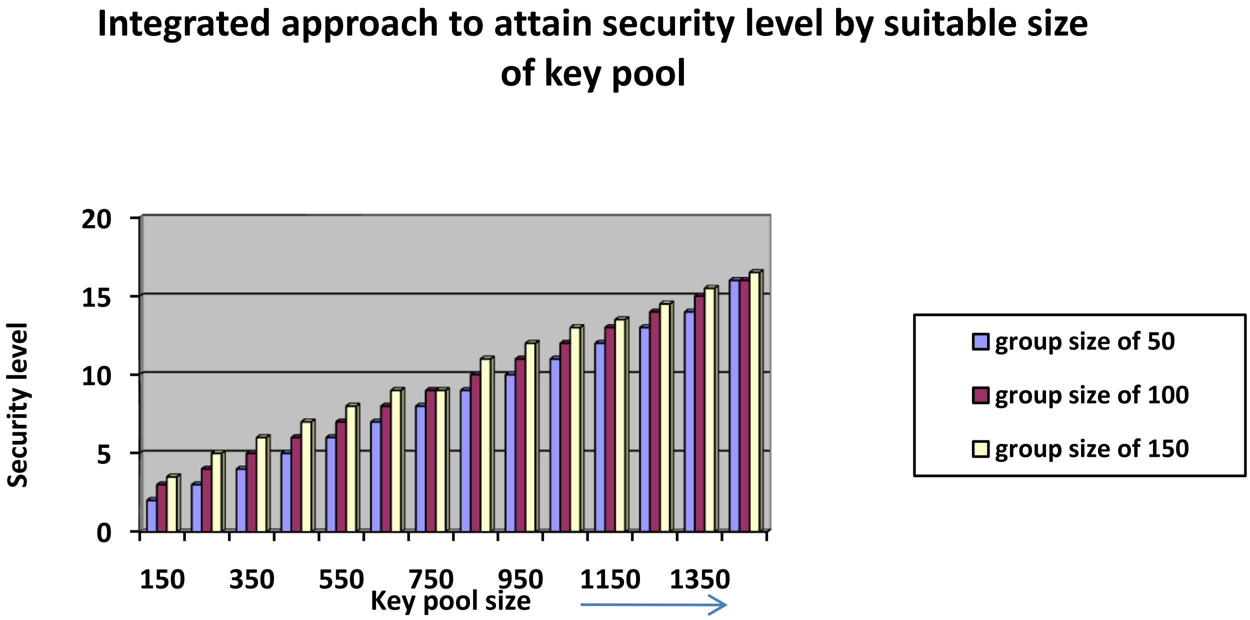

Fig. 4 Security Level Vs Key Pool Size

V. CONCLUSION

Our secure solution gives an efficient and better key dissemination method to the studied random key distribution schemes. It provides secure key pool architecture giving the sensors an alternative way to exchange new keys by refreshing the key pool. Security analysis explains that it can withstand several attacks against WSN. In the future, we will provide a formal proof of security properties for the proposed scheme.

REFERENCES

[1] Salim El Khediri, Nejah Nasri1, Anne Wei, Abdennaceur Kachouri," Probabilistic Energy Value for Clustering in Wireless Sensors Networks", Published online in *Scientific Research, Wireless Sensor Network,* 2013, 5, 26-32 February 2013.

[2] Mohammed A. Abuhelaleh and Khaled M. Elleithy, "Security In Wireless Sensor Networks: Key management Module In SOOAWSN", *International Journal of Network Security & Its Applications (IJNSA),* Vol.2, No.4, October 2010.

[3] P. Samundiswary, M. Raj Kumar Naik ," Performance Analysis of Deterministic Energy Efficient Clustering Protocol for WSN, *International Journal of Soft Computing and Engineering (IJSCE)* , Volume-2, Issue-6, January 2013.

[4] Pengcheng Zhao, Yong Xu, Min Nan, "A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks", Published online in *Scientific Research, Wireless Sensor Network,* 2012, 4, 197-201, August 2012.

[5] Baojiang Cui, Ziyue Wang,Tao Guo, Guowei Dong,Bing Zhao,"UBKM : A Usage-based Key Management Protocol for Distributed Sensor Networks" *,IEEE Conference Publications, Fourth International Conference on Emerging Intelligent Data and Web Technologies*,2013.

[6] Sudhanshu Tyagi , Neeraj Kumar ," A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks ,Journal of Network and Computer Applications ,Volume 36, Issue 2, March 2013, Pages 623–645.

[7] Qian Liao, Hao Zhu," An Energy Balanced Clustering Algorithm Based on LEACH Protocol", Proceedings of the 2nd International Conference On Systems Engineering and Modeling (ICSEM-13), 2013.

[8] Zhao Jinchao, "Research on Key Pre distribution Scheme of Wireless Sensor Networks*", IEEE Conference Publications, ,Fifth International Conference on Intelligent Computation Technology and Automation,2012.*

[9] Mohamed Helmy Megaheda, Prof. Dimitrios Makrakisb, Bidi Ying, "SurvSec: A New Security Architecture for Reliable Network Recovery from Base Station Failure of Surveillance WSN", *The 2nd International Conference on Ambient Systems, Networks and Technologies, ANT* ,2011, Procedia Computer Science 5 (2011) 141–148.

[10] Abderrahmen Guermazia, Mohamed Abidb," An Efficient Key Distribution Scheme to Secure Data-Centric Routing Protocols in Hierarchical Wireless Sensor Networks", *The 2nd International Conference on Ambient Systems, Networks and Technologies Procedia Computer Science* 5 (2011) 208–215.

[11] Nishi Sharma, Vandna Verma," Energy Efficient LEACH Protocol for Wireless Sensor Network, International Journal of Information & Network Security (IJINS) Vol.2, No.4, August 2013, pp. 333-338 .

[12] SEYIT A. C¸AMTEPE and B¨ ULENT YENER,"Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", *Technical Report TR-05-07, Department of Computer Science,* Rensselaer Polytechnic Institute March 23, 2005.

[13] Reza Azarderakhsh, Arash Reyhani-Masoleh, and Zine-Eddine Abid,” A Key Management Scheme for Cluster Based Wireless Sensor Networks”, *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*,2008.

[14] Awatef Ben Fradj Guiloufi, Nejah Nasri, Mohamed Alamine Ben Farah, Abdennaceur Kachouri,” MED-BS Clustering Algorithm for the Small-Scale Wireless Sensor Networks”, Published online in *Scientific Research, Wireless Sensor Network*, 2013, 5, 67-75.

[15] K.Gomathi , T.P.Senthilkumar ,”A Study on Security Challenges in Wireless Sensor Networks: Key management Approaches”, *International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 9– Sep 2013.*

[16] Ahmet Onur Durahim, Albert Levi,” Dynamic Resiliency Analysis of Key Predistribution in Wireless Sensor Networks, *ICC, page 1-6. IEEE, 2009.*

[17] Anvesh Reddy Aileni,”Cluster based Key Management in Wireless Sensor Networks”, ,Proceedings of 2nd Annual Conference on Theoretical and Applied Computer Science, November 2010.

[18] Benamar Kadri, Djilalli Moussaoui, Mohammed Feham, Abdellah Mhammed, "An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks" ,*Wireless Sensor Networks*,2012,4,155-161.

[19] S. H. Gajjar, K. S. Dasgupta, S. N. Pradhan, K. M. Vala “Lifetime Improvement of LEACH Protocol for Wireless Sensor Network”, *IEEE Conference Publications*, Nirma University International Conference On Engineering, Nuicone-2012, 06-08december, 2012

[20] Zhiming Yang, Junyi Liu, Xuhui Chen,” An Optimal Mechanism of LEACH Protocol for Wireless Sensor Networks”, 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, *IEEE Conference Publications,2009.*

[21] Xuxun Liu,” A Survey on Clustering Routing Protocols in Wireless Sensor Networks *Sensors* 2012, *12*, 11113-11153; doi:10.3390/s120811113.

[22] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro.” SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks, Fifth IEEE International Symposium on Network Computing and Applications (NCA'06) July 24-July 26,2006.