ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

# Obtaining Security and Energy Efficiency for Leach-Clustering Protocol in Wireless Sensor Network

**Nakul Sorout[1], Mahesh Singh[2],**

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India[1]
Assit. Prof., Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India [2]

**ABSTRACT**
With the growing utilization of Wireless Sensor Networks (WSN) in more and more areas, data transfer security becomes a important issue in research area. The secret key cryptography is not capable to offer security in WSN provided the nature of deployment area in the most applications. Key distribution lies an important. Currently several public key cryptography based algorithms have been explained. In these, first are homomorphism algorithms but their cost is very high on scarce resource in WSN such as Battery life. This paper introduces a novel encryption strategy for obtaining security and energy efficiency for LEACH-C protocol in WSN. The introduced strategy employs a hybrid method consisting both kind of encryption strategies such as public key cryptography and secret key cryptography both. In the introduced strategy the session key is distributed to several nodes utilizing public key cryptography mechanism which improves network security and also consumes low energy. For data aggregation plain mechanism (in-network data aggregation) is employed. The introduced mechanism is compared with public key cryptography with hidden data aggregation and in network data aggregation. The result tells that the introduced mechanism obtained higher energy efficiency in comparison of other two comparable mechanisms without adjusting security environment in data transfer.

**KEYWORDS:** secret Key Cryptography, public Key Cryptography, LEACH-C, hidden Data Aggregation, In Network Aggregation.

## I. INTRODUCTION

Wireless sensor networks (WSNs) are consisted of large no. of densely deployed sensors. A key characteristic of these networks is that their nodes are unavailable. WSNs can be used in a broad variety of applications needing either a particular kind of sensor or a mixture of sensor types [2]. The class of environmental monitoring applications concentrates on physical variables i.e. lighting conditions, temperature, motion, noise, object presence and mechanical stress. The Class of surveillance applications concentrates on determining location sensing, crucial events and object tracking. Hence, for example, homogeneous WSNs could be used to monitor vibrations and focuses on a large structure i.e. oil rig or a ship. On the other side, homeland security applications would need a heterogeneous WSNs containing of various types of sensors involving biochemical sensors, radiation sensors and digital video cameras, managed by a set of base stations [3]. Other potential target domains for heterogeneous WSNs involve habitat monitoring, battlefield surveillance and health monitoring.

**Types of Sensor Networks**

**A. *Terrestrial WSNs***

In these, nodes are distributed in a provided region either in an ad hoc way (sensor nodes are randomly positioned into the target area by discarding it from plane) or in pre-planned way (sensor nodes are positioned according to optimal placement, grid placement, 2-d and 3-d placement models). However battery power is restricted and it cannot be recharged, terrestrial sensor nodes must be offered with an optional power source i.e. solar cells [4].

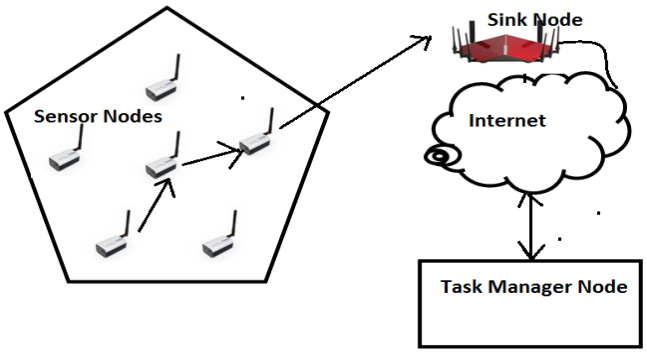


**Figure 1: Wireless Sensor networks (WSN)**

**B. *Underground WSNs***

In these, sensor nodes are forgotten underground or in a mine or cave that monitors the underground situations. Sink nodes are positioned above the ground to send the collected information from the sensor nodes to the base station. These are more costly as compared to the terrestrial sensor networks because suitable nodes are to be chosen that can confirm

reliable communication through rock, soil, water and other mineral contents [3].

**C. *Underwater WSNs***

In these, vehicles and sensor nodes are positioned underwater. Autonomous vehicles are utilized for collecting the data from the sensor nodes. Sparse deployment of nodes is performed in this network. Main issues that come under this while communicating are long propagation delay, restricted bandwidth and signal fading issue [4].

**D. *Multimedia WSNs***

In these, low cost sensor nodes are fitted with microphones and cameras. These nodes are positioned in a pre-planned way to confirm coverage. Problems in these networks are requirement of high energy consumption, high bandwidth, data processing, quality of service provisioning and compression mechanisms, and cross layer design [7].

## II. MOTIVATION

In a sensor particle a small amount of resources are remained for security to be enforced. This is not sufficient to even keep the variables for asymmetric public key based cryptographic algorithms i.e. RSA and Diffie-Hellman. Therefore public key based systems are not suitable for sensor networks. Due to the resource constraints another solution is to utilize global keys. This is viable but a global key based system does not offer the required level of security. In opposite, complete pair-wise keying among nodes offers the best possible security, but it is not suitable for sensor network because of the resource restrictions [5].

The easiest mechanism of key distribution is to preload a single network-wide key into all nodes before enforcement [14]. Only one single key is saved in the nodes' memory and once enforced in the network, there is no requirement for a node to perform key exchange or key discovery however all the nodes in communication coverage area can transfer messages employing the key which they already share. On the other side, this strategy suffers a serious disadvantage that adjustment of a single node would lead compromise of the whole network by the shared key. Hence it fails in offering the basic secure need of a sensor network by building it easy for an antagonist attempting to attack [8].

An alternative key distribution strategy is fully pair-wise keys strategy, such as each node in the sensor network shares a different key with each other node in the network. The major problem with this pair-wise key strategy is its poor scalability. The no. of keys that must be saved in every node is proportional to the total no. of network nodes. However sensor nodes are resource-restrained, this brings important overhead which restricts the mechanism's availability except for it can only be efficiently utilized in smaller networks.

The mechanism of Kerberos-like key distribution is famous in some networks environment. In sensor networks, we can employ a authorized, protected station as an arbiter to offer connection keys to sensor nodes. The sensor nodes manifest themselves to the base station, after which the base station produces a connection key and forwards it to both parties in a secure manner. An example of this type of protocol is SNEP, which is part of the SPINS security infrastructure [6] [7]. Since, this type of mechanisms suffers high energy consumption, which makes it available in most sensor network applications.

The introduced work is about to employ some security methods in LEACH-C protocol to offer a full proof security by employing more rounds of transmission to BS and less energy. For this, various choices are introduced to enhance the complete security scenario and consume less energy. At last, introduced methods are defined and these are compared for energy consumption.

## III. LITERATURE REVIEW

**Kumar & Pal. 2013:-** The scope of this research paper is the protocol aided LEACH (A-LEACH) which obtains uniform and decreased distribution of dissipated energy by distinguishing the tasks of data aggregation and routing. It presents the idea of helper nodes which guide cluster heads for multi-hop routing. A novel algorithm has been developed to provide energy effective multi-hop route establishment for helper nodes to arrive base station. The suggested protocol increases the network lifetime, reduces total energy dissipation in the network and distributes dissipation among sensor nodes, cluster heads and helper nodes vis-à-vis LEACH. This is supported by results of simulation. Helper nodes in assisted LEACH (A-LEACH) protocol has enhanced the network lifetime by distributing the reduced energy dissipation across the nodes. Simulation results and theoretical analysis ensure this.

**Aslam, M., et al. 2012:-** The main stress of his study is how to explore routing protocols work for increasing the life time, and how quality of routing protocol is enhanced for WSN. In hierarchical routing protocols entire network is classified into several clusters. One node in every cluster plays leading part. The only node is the cluster node that can communicate to base station in clustering routing protocols. This importantly decreases the routing overhead of normal nodes because normal nodes have to transmit to cluster-head only. Significant research work has been done in these diffrent clustering routing protocols in order to increase the lifetime and data delivery features.

**S.Ahmed,M., et al. 2011:-**The main motive of this research paper is to introduced a clustering algorithm for sensor networks ,called Low Energy Adaptive Clustering) Hierarchy(LEACH). LEACH forms clusters by using distributed algorithm, where a node makes autonomous decisions without any centralized control. IMODLEACH protocol which is an extension to the MODLEACH protocol. Simulation resuls indicate that iMODLEACH in terms of network Life-time and packets transferred to base station; that can be further utilized in other clustering routing protocols for better efficiency.

## IV. TYPES OF WSN PROTOCOLS

**1.E-LEACH protocol:**

Energy-LEACH protocol enhances the CH selection mechanism. It builds residual energy of node as the significant metric which selects whether the nodes turn into CH or not after the first round [9]. Similar to LEACH protocol, E-LEACH is classified into rounds, in the first round, each node has the same possibility to turn into CH, that mean nodes are chosen as CHs in a random way, in the next rounds, the residual energy of every node is different after one round communication and taken into consideration

for choosing the CHs. That mean nodes have more energy will become a CHs instead of nodes with less energy.

**2. TL-LEACH:** In LEACH protocol, the CH gathers and combines data from sensors in its own cluster and directly forwards the information to the BS. CH might be positioned farther from the BS, so it utilizes most of its energy for transmitting and because it is always on it will die faster as compared to other nodes. A novel version of LEACH known as Two-level Leach was suggested. In this protocol; CH gathers data from other cluster members as real LEACH, but instead of transfer data to the BS directly, it utilizes one of the CHs that stays between CH and the BS as a relay station [7].

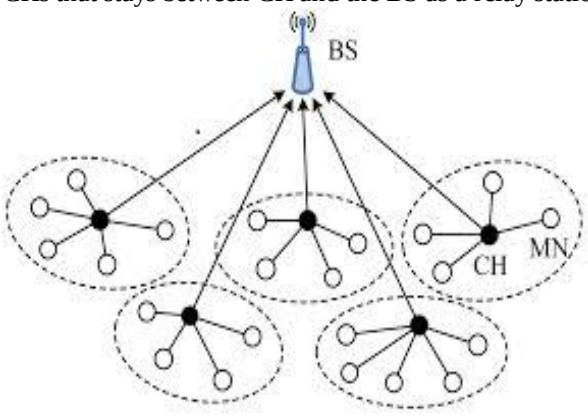


**Fig. 2: TL-LEACH**

**3. M-LEACH protocol:** In LEACH, Every CH directly communicates with Base Station irrespective the distance between BS and CH. It will take lot of its energy if the distance is greater. On the other side, Multi hop-LEACH protocol chooses optimum path between the BS and CH through other CHs and utilize these CHs as a relay station to transmit data over through them [8]. First, multi-hop communication is followed among CHs. Then, consequent to the chosen optimum route, these CHs transmit data to the corresponding CH which is closest to BS. At last, this CH forwards data to BS. M-LEACH protocol performs almost the same as LEACH protocol, only builds communication mode from single hop to multi-hop between BS and CHs.

**4. LEACH-C protocol:** LEACH provides no assurance about the placement and/or no. of cluster heads. In [13], an improvement over the LEACH protocol was introduced. The protocol, known as LEACH-C, utilizes a centralized clustering algorithm and the same steady-state phase as LEACH. LEACH-C protocol can generate better performance by distributing the cluster heads over the network. At the time of set-up phase of LEACH-C, every node forwards information about its current position (possibly determined utilizing GPS) and residual energy level to the sink. In summation to finding good clusters, the sink requires to assure that the energy load is evenly dispersed among all the nodes. To do this, sink calculates the average node energy, and computes which nodes have energy lower than this average. Once the cluster heads and related clusters are determined, the sink forwards a message that achieves the cluster head ID for every node. If a cluster head ID same as its own ID, the node is a cluster head; else the node determines its TDMA slot for data transmission and goes sleep until its time to transmit data. The steady-state phase of LEACH-C is same as that of the LEACH protocol.

**5. V-LEACH:** In our novel version of LEACH protocol, the cluster consists; CH (responsible only for forwarding data that is obtained from the cluster members to the Base Station), vice-CH (the node that will become a cluster CH in situation of CH dies), cluster nodes (collecting data from environment and forward it to the CH). In the real leach, the CH is always on obtaining data from cluster members, combine these data and then forward it to the Base station that might be positioned farther from it. The CH will die faster as compared to the other nodes in the cluster due to its operation of obtaining, forwarding and overhearing. When the CH die, the cluster will become waste because the data collected by cluster nodes will never arrive the base station.

In our proposed protocol, along with having a CH in the cluster, there is a vice-CH that takes the CH role when the CH dies because the reasons we provided above.

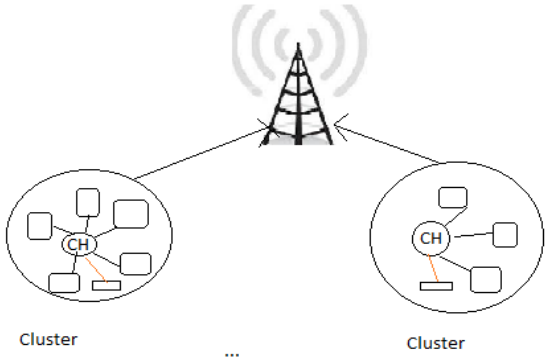


**Fig. 3: VLEACH**

By doing this, cluster nodes data will always arrive the Base Station; no requirement to elect a new CH every time the CH dies. This will extend the total lifetime of network

## V. METHODOLOGY

This section talks about methodology for simulation and several methods of encryption those can be employed in WSN and their energy consumption nature. These encryption methods consists both kinds of encryption mechanisms; private key cryptography and public key cryptography. Our primary idea in this thesis is to build a tradeoff between energy and security needs in WSN.

There are two main methods for data encryption which offer authentication and security for data. Secret key cryptography (SKC) offers high level of security and uses less resources in comparison of public key cryptography (PKC), but key distribution and management is an important issue of SKC [15]. It also doesn't offer authentication and sends this activity on the shoulders of third party which is not feasible for Wireless Sensor Network scenario. The PKC offers authentication as well as data but makes complicated computation and uses more energy in comparison of SKC. Public Key cryptographic Algorithms (Homomorphic encryption) is a kind of encryption which permits particular types of computations to be enforced on cipher text and achieve an encrypted result which decrypted matches the result of operations made on the plaintext. For example, one person could sum two encrypted numbers and then another

person could decrypt the result, without either of them being capable to discover the individual numbers value.

Data aggregation is a necessary data processing primitive in sensor networks. Sensor nodes send data towards the sink node. Sensor nodes nearest to the sink node obtain data from nodes which are far; they integrate the information into brief digests. The integrated data is encrypted utilizing Privacy Homomorphism algorithms. This makes enable end-to-end security. Hence implements integrity and confidentiality to the data being forwarded. This result into important energy savings over having every node sends their respective readings directly to the sink node.

## VI. PROPOSED SIMULATION OF ENCRYPTION SCHEMES

In this paper, we have taken three encryption mechanisms for simulation. These are explained in the subsequent paragraphs.

**Scheme 1: Public Key Cryptography Scheme with concealed data aggregation (PKC-CDA):**

In the first mechanism, the sensor nodes encrypt data employing RSA homomorphism algorithm signature generation. Cluster heads integrate the complete data into one without decrypting it and again forwarding data to base station. This kind of mechanism is also known as Public Key Cryptography Scheme (PKC) with hidden data aggregation.

**Scheme 2: Public Key Cryptography Scheme with using in-network data aggregation (PKCINA):**

In this mechanism, the sensor nodes encrypt a novel produced session key employing homomorphism algorithm signature. The sensor node utilize this session key to encrypt data employing AES algorithm and then homomorphism encrypted session key and session key encrypted data is forwarded to the Cluster heads(CHs). CHs decrypt data employing session key which is fetched by CH's own private key and then integrate the complete data into one and again employ homomorphism encryption for forwarding session key and session key encrypted data to BS. This kind of mechanism is also known as Homomorphism Encryption Scheme (HES) employing in-network data integration or simply Public Key Cryptography Scheme with employing in-network data aggregation (PKC-INA)

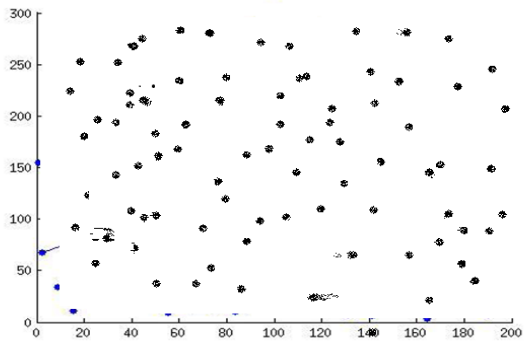


**Figure 4 WSN Node Deployments**

**Scheme 3: Key distribution on based scheme (KDS):**

In this mechanism, Base Station first distributes a common session key for every round which is encrypted by each node's public keys. Every sensor node decrypts the session key employing its own private key. This is also known as key Exchange method. Once distribution of key is finished data can be forwarded to CH and BS employing SKC's AES Algorithm. We call this Key Distribution based Scheme (KDS).

## VII. LEACH SIMULATIONS - ALGORITHM

100 nodes positions are produced in a random manner in a 200*200 m2 area and a BS is also positioned at (100, 300) position. This deployment result is illustrated in figure 5 and 6. The Base station (BS) is very far from the node deployment region. In the beginning each node is having equal energy such as 5000 Joules and all nodes are live nodes.

The algorithm for above deployment and simulation is provided below:

**Step 1:** produce the network architecture with required parameters

**Step 1.1** makes the field Area

**Step 1.1.1** x and y Coordinates of the base station

bsX=x coordination of BS

bsY=y coordination of BS

**Step 1.1.2** Create the node model in a random manner.

x coordination of nodes

y coordination of nodes

**Step 1.1.3** in starting there are no cluster heads, only nodes 1 for 'N' =non-CH node, 2 for 'C' = CH node,3 for 'D'= Dead node

**Step 1.2** Energy Model (all values in Joules)

- Specify Initial Energy of node
- Specify Energy for transferring/ receiving of each bit (ETX)
- Transmit/receive Amplifier types

**Step 2:** plot field area with its nodes and BS

**Step 3:** for every round

**Step 3.1** Create the new node architecture employing max energy leach algorithm (LEACH-C) in starting of every round.

Max Energy leach algorithm in which nodes are chosen CHs with respect to their remaining energy and no. of CHs is fixed as p*liveNodes. [9].

**Step 3.2:** if (any cluster is formed during round)

Find Energy dissipation patterns for nodes (Ref section 4.10)

End if

End for

Step 4: Display no. of packets forwarded from CH, energy dissipation per round and dead node pattern for every round.

At last, when clusters are formed then packets are forwarded from non-CH nodes to CH nodes and finally CHs nodes forward their packets to BS. The CHs also uses energy in data integration and receiving. All nodes use transmitting energy. Energy dissipation for nodes is a distance factor from BS. This chooses whether to utilize free space or multipath transmitter.

## VIII. RESULT AND DISCUSSION

This table shows the results achieved from the experiments performed according to the setup described in the previous section. Three algorithms have been carried out in this paper. In the first algorithm, sensor nodes change data employing RSA based homomorphism algorithm signature production. Cluster heads integrate the complete data into one without

decrypting it and again forwarding data to BS. This kind of mechanism is also known as Public Key Cryptography method (PKC) with hidden data aggregation (PKC-CDA).
Further a novel method is taken in which a newly created session key utilizing RSA homomorphism algorithm signature. The sensor node employ this session key to encrypt data utilizing AES algorithm and then RSA encrypted session key and session key encrypted data is forwarded to the Cluster heads(CHs). CHs decrypt data utilizing session key which is fetched by CH's own private key and then integrate the complete data into one and again utilize RSA encryption for forwarding session key and session key encrypted data to BS. This kind of mechanism is also known as Homomorphism Encryption based Scheme (HES) utilizing in-network data aggregation or Public Key Cryptography Scheme (PKC) with in-network data aggregation (PKC-INA).
Third algorithm employs RSA based key distribution in which BS first distributes a share session key for every round which is encrypted by every node's public keys. Every sensor node decrypts the session key utilizing its own private key. This is also known as key exchange method. We call this Key Distribution based Scheme (KDS).
The fundamental routing protocol for these methods is Max Energy Leach which is effective in energy equip-distribution in the network which helps in longer life time and detained death of network. In this scheme a static no. of CHs are chosen depending on the residual energy of nodes that are active. The active non-CH nodes become a part of cluster with the closest CH. Once clusters are made CHs gathers data from its cluster nodes and forward it to BS by adopting one of the above explained methods of data encryption. This method is also known as LEACH-C. In the table it is clearly described that introduced SCHEME3: (RSA Key Exchange Based LEACH-C) performs better in comparison of other schemes. The RSA Key Exchange Based LEACH-C performs about five times better as compared to other methods. If we take a network dead if 40% nodes are dead then RSA Key Exchange Based LEACH-C is performing better as compared to other methods. If we take 80% dead node standard for network life then still performs better as compared to other two algorithms.

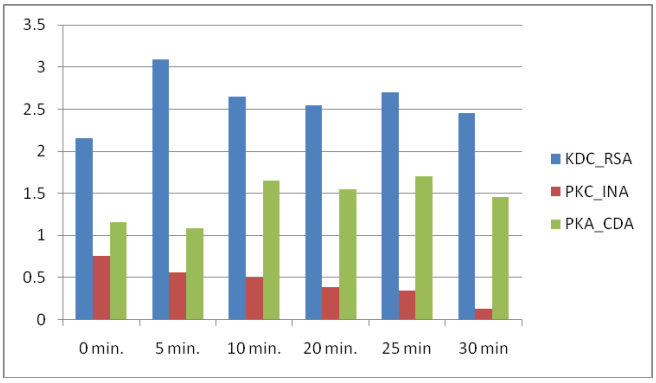


**Figure 5: Results for no of packet sent to BS**

If we take number of packets forwarded to BS then RSA Key Exchange Based LEACH-C scheme is clearly best. This has forwarded maximum no. of packets to BS. This is also right if we take the ratio between packet forwarded and number of rounds executed by the algorithm. This can be assured by the figures 5 to 6.

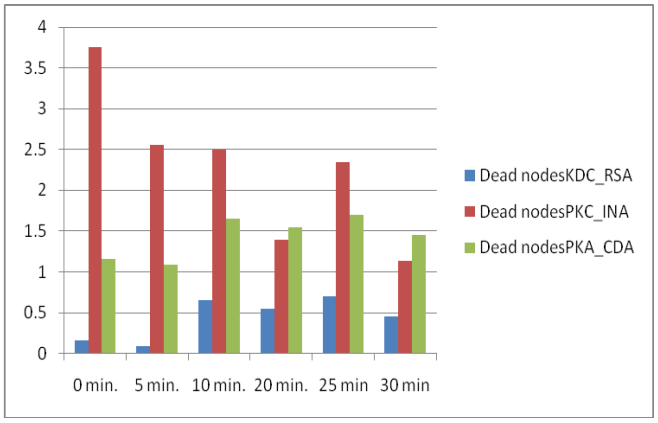


**Figure 6: Results for No of dead nodes**

## IX. CONCLUSION

In this paper we have evaluated performance of three cryptographic methods for protected data routing in WSN. Simulation parameters for performance evaluation are Dead Nodes, Residual Energy, Packets forwarded to BS. These simulation parameters are illustrated in above figures and are drawn against no. of rounds. If we take residual energy and total no. of rounds then introduced RSA Key Exchange Based LEACH-C performs better as compared to other two methods. But residual energy at the end of total no. of round tells that Max Energy LEACH most uniformly distributed energy dissipation between nodes in all the methods due to utilization of LEACH-C in all methods. In these experiments we have observed that better performance can be obtained utilizing RSA based key distribution for offering high security with very high energy efficiency. Though public key cryptography based method i.e. PKC with CDA offer very high security but its cost is very high.

## REFERENCES

[1] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, *Wireless Communication and Mobile Computing*, Vol. 4,No 6,pp.623-637,2009.

[2] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", *International Journal of Engineering* ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.

[3] Xuanxia Yao, XueFeng Zheng, "A Secure Routing Scheme for Static Wireless Sensor Networks", *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol.2, pp.776-780, 2008

[4] Rayala Upendar Rao, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", *International Journal of Computer Applications*, Vol. 55, Issue. 7, pp.48-52, October 2012

[5] Bhoopathy, V. and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks*", International Journal of Engineering Research and Applications (IJERA),* Vol. 2, Issue 2, pp.466-474,Mar-Apr 2012.

[6] K.S.Arikumar, K.Thirumoorthy, "Improved User Authentication in Wireless Sensor Networks", 2011 IEEE.

[7] Wassim Drira," A Hybrid Authentication and Key Establishment Scheme for WBAN", *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Vol. 2, No.3, pp.78-83, 2012

[8] Asha Rani Mishra, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," *International Journal of Engineering Research & Technology (IJERT)* ,Vol. 1 Issue 3, pp. 2-3,May-2012.

[9] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", *International conference on Information, Networking and Automation(ICINA)*,Kunming, IEEE, pp. 215-218, 2010.

[10] Shohreh Ahvar1, Mehdi Mahdavi, " EEQR: An Energy Efficient Query-Based Routing Protocol for Wireless Sensor Networks", *Journal of Advances in Computer Research* ,Vol. 2, No. 3, pp. 25-38, August 2011.

[11] Heissenbütte lM., T. Braun, M. Wälchli, and T. Bernoulli, "Optimized stateless broadcasting in wireless multi-hop networks," *in proceeding of 4th IEEE international conference on Infocom Barcelona*,2006,pp. 234-250.

[12] Sommer, C.; Dietrich, I.; Dressler, F. "Realistic Simulation of Network Protocols in WSN Scenarios" in *Proceedings of International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 3, 2008, pp. 217-223.

[13] TsengY.C., Y.S. Chen, and J.P. Sheu, "The broadcast storm problem in a Wireless Sensor Networks, *" In Proceeding of the 5th ACM/IEEE International Conference on Mobile Computing and Networking*, NY, USA,1999, pp. 51-162.

[14] KorkmazG., E. Ekici, F. Ozgüner, and U. Ozgüner, "Urban multi-hop broadcast protocolforWireless Sensor Networks," *In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks*, NY, USA, 2004,pp. 76-85.

[15] Rajive Bagrodia, Richard Meyer, Mineo Takai, Yu an Chen, Xiang Zeng, Jay Martin, andHa Yoon Song. "A parallel simulation environment for complex systems"*in Proceedings of the 1st ACM international workshop on ad hoc networks; 2004*; Pages: 66 – 75.

[16] v Brian D. Noble, Jungkeun Yoon ,Mingyan Liu, Minkyong Kim, "Building realisticmobility models in Wireless Sensor Networks", in *Proceeding of the ACM International* Conference On Mobile Systems, Applications And Services, pp. 177-190, 2006.

[17] Fan Li and Yu Wang; " Survey of Routing in Wireless Sensor Networks",in *Proceedings ofIEEE Wireless Sensor Networks Technology Magazine, Volume 2, Issue 2, June 2007*; pp. 12-22.

[18] *Jahanzeb Farooq, Bilal Rauf "*Implementation and Evaluation of IEEE 802.11e WirelessLAN in GloMoSim" *In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks*, NY, USA, 2004,pp. 76-85.

[19] Yue Liu, Jun Bi, Ju Yang; "Research onWireless Sensor Networks"in *Proceedings of* Chinese Control and Decision Conference (CCDC), 2009, pp.4430 – 4435

[20] Abedi, O.; Berangi, R.; Azgomi, M.A., "Improving Route Stability and Overhead on AODV Routing Protocol and Make it Usable forWireless Sensor Networks," in *Proceedings of 29th IEEE International Conference onWireless Sensor Networks*,June 2009, pp.464,467.

[21] Chowdhury, S.I.; Won-Il Lee; Youn-Sang Choi; Guen-Young Kee; Jae-Young Pyun, "Performance evaluation of reactive routing protocols inWireless Sensor Networks," *in proceeding of Communications (APCC), 2011 17th Asia-Pacific Conference onad hoc networks ,2011*, pp.559,564.

[22] Sun Xi; Xia-Miao Li, "Study of the Feasibility of Wireless Sensor Networks and its Routing Protocols," *in proceeding of Wireless Communications, Networking and Mobile Computing, 2008. 4th International Conference on ad hoc networks*, 2008, pp.1-4.

[23] Vinod Namboodiri, Manish Agarwal, Lixin Gao; "A Study on the Feasibility of Mobile Gateways for Wireless Sensor Networks", *in proceeding of Wireless Communications Networking and Mobile Computing 6th International Conference on* 2010,Sept. 2010, pp.1,4, 23-25.

[24] Siva D., Abu B. Sesay, and Witold A. Krzymie´n, "A Design on Routing Protocol in Sensor Networks Based on Clustering Optimization" *In Proceedings of 2nd International Conference on Future Computer and Communication*,2010, pp 473-477.

[25] C. Y. Wan, S. B. Eisenman, and A. T. Campbell,, "CODA: Congestion Detection and Avoidance in Sensor Networks," *In Proceedings of FirstACM Conference on Embedded Networked Sensor Systems*,2003,pp.266-279.

[26] R.U.Anitha, P. Kamalakkannan ,"Enhanced Cluster Based Routing Protocol for MobileNodes in Wireless Sensor Network" *In Proceedings of 2013 International Conference onPattern Recognition, Informatics and Mobile Engineering (PRIME)*, 2006,PP 187-193.

[27] Samera. B. Awwad, cheekyunng and Nor K. Noordin "Cluster Based Routing (CBR) Protocol with Adaptive Scheduling for Mobility and Energy Awareness in Wireless Sensor Network," *In Proceedings of Proceedings of the Asia Pacific Advanced Network*,2009, pp 34-46.

[28] R. Balasubramaniyan , Dr. M. Chandrasekaran "A New Fuzzy Based Clustering algorithm for Wireless Mobile Ad-Hoc Sensor Networks "*In Proceedings of 2013 International Conference on Computer Communication and Informatics*,2013, pp 31-37