International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34035-34041

Performance Analysis of Secure Leach Based Clustering Protocol in Wireless Sensor Networks

Prof. P. Sasikumar[1] and Prof. K. S. Preetha[2]

School of Electronics Engineering, VIT University[12]

Abstract
In wireless sensor networks clustering is one of the techniques used for energy efficiency. LEACH (Low-energy adaptive clustering hierarchy) is a widely used clustering based routing protocol used for energy efficiency by rotating cluster heads in rounds. But in this protocol, wireless sensor networks are vulnerable to security attacks. To establish security, Secure-LEACH protocol uses shared keys between base station and sensor nodes. These keys are used to generate message authentication code, through which the base station verifies authenticity of the nodes. Secure-LEACH prevents intruders from participating in the network as cluster heads. It also enables the base station to discard any detected bogus messages. Secure-LEACH protects the network from outsider attackers

Keywords:Clustering, LEACH, Secure-LEACH, Traffic, Energy

I. Introduction

These Wireless sensor networks (WSNs) consist of sink base stations (BSs) (presently we use more than one base station to collect data) and a large number of sensors nodes. These sensors nodes are deployed over an area of interest for monitoring certain phenomena. The BS main function is to collect the data from all sensor nodes, and study it so that it can analyze about the activity in the area of interest. WSNs have a self-organizing mechanism which allows the nodes to implement its network topology by itself because the sensor nodes in WSNs should be operated stably in the irregular deploying fields whose environment is so difficult to be approached. The sensor nodes in WSNs have limited power resources. Sensor is considered to be dead if its battery is depleted and is removed from the network. Therefore, using the energy efficiently is an important design objective for wireless sensor networks.

To achieve this objective, protocols based on clustering such as LEACH protocol [1] are used. LEACH is a hierarchical clustering protocol that provides energy efficiency. In this protocol, Cluster Heads are chosen randomly and are periodically rotated. This leads to balanced energy load in the network and prolongs the life cycle of the entire network. In LEACH, the entire network is grouped into clusters, with a cluster head for every cluster. The cluster heads reduce the total energy consumption of the network by effectively forwarding the sensor data to BS. The cluster heads are elected based on the desired percentage of the current round number and cluster heads. Cluster heads change after each round.

Another problem is wireless sensor networks (WSNs) [2] are often deployed in unattended, harsh or hostile environments. In such conditions, sensor networks are vulnerable to various security attacks. As a result, security and protection of sensors against malicious behaviors is important. Although LEACH [2] has advantages such as energy efficiency, it is prone to several security attacks. Many passive and active attacks can be launched against it. For example, because LEACH depends heavily on Cluster Heads, an intruder may attempt to become a CH and drop the messages totally or selectively, or inject bogus data in aggregated results [2]. Therefore, security of this protocol has to be enhanced to prevent attackers from interrupting its operations.

Many secure versions of LEACH protocol [2] have been designed and proposed in the literature. The proposed secure LEACH schemes can be classified into the cryptographic-based and trust-based solutions. The cryptographic-based secure LEACH protocols are used to deal with outsider attackers and the trust-based secure LEACH protocols are used to deal with insider attackers. An outsider attacker does not have access to any cryptographic materials or keys of the network where as an insider attacker has access to cryptographic material of the network [2].

A number of cryptographic- based secure LEACH protocols use asymmetric key cryptography. The protocol proposed in [4], Authentication Confidentiality cluster based secure routing protocol. It uses asymmetric key cryptography, which requires a node to have two keys: a public key and a private key. Although the protocol provides data confidentiality in addition to authentication, the high computational requirement because of asymmetric key cryptography makes it not efficient for the wireless sensor networks. Similarly, the efficient security model of routing protocol (ESMR) proposed in [5] also uses asymmetric key cryptography technique. In this work, a secure LEACH protocol is implemented based on symmetric key cryptography as it is energy efficient than the asymmetric key cryptography.

I.1. Characteristics of wireless Sensor Networks

- Limited power: As mentioned in previous sections, Sensor nodes in WSN run on batteries which are generally non-replaceable. Hence, the power in WSN is considered to be limited.
- Ability to cope with node failures: A node may fail due to many reasons such as hardware failures, exhausted batteries etc. When a failure node occurs,

other nodes should create another route to the destination, which does not involve the dead node.
- Heterogeneity of nodes: WSN can have variety of nodes like primary sensor node, sink nodes, Cluster heads etc.
- Large scale of deployment: WSN are used to sense data in particular area. These areas can vary from few meters to kilometers.
- Mobility of nodes: The sensor nodes, base station can be either stationary or mobile.
- Communication failures: Communication failures generally occur due to disability to correct node failure, busy channel traffic etc.

I.2. Security in WSN:

Security in WSN is the degree of protection to safeguard network [2], sensors and their transmitted data against various attackers and malicious nodes. Security mainly deals with providing the following service in the network [2]:

- DATA CONFIDENTIALITY [2]: This property ensures that sensed and transmitted information is never revealed to unauthorized nodes. Data privacy can be achieved in hop by-hop or end- to-end basis.
- DATA INTEGRITY: ensures that the content of a message has not been altered, either maliciously or by accident, during transmission process.
- AUTHENTICATION: allows the receiver to verify that messages are sent by the valid sensor nodes.
- NON-REPUDIATION: ensures that a transferred packet has been sent and received by the person claiming to have sent and received the packet.
- AVAILABILITY [2]: ensured that services offered by WSN or a single sensor node must be available whenever required. Some schemes achieve this property by the use of multi path routing and others use self-healing to diagnose and react.

I.3. Attacks on Wireless Sensor Networks

Wireless sensor networks are prone to many security attacks. Few of them are:

SELECTIVE FORWARDING: A received messages is sent to its destination, faithfully by an honest node. But, a malicious node may not forward certain messages to ensure that the message doesn't reach the intended destination. This is called selective forwarding attack. In this attack, malicious node drops all message packets that arrive to it [19]. But there is a possibility that the neighboring nodes would consider such nodes as dead nodes and chose another route. So, these nodes cleverly forward certain messages only. Hence, the risk of revealing the adversary is minimized. Selective forwarding attacks are more effective when the attacker explicitly includes itself in the routing path of the data. Other ways of implementing selective forwarding is by jamming or causing collision on the transmitting information.

HELLO FLOOD ATTACK: In many protocols, HELLO packets are broadcasted by the sensor nodes to announce it to the neighbors that it is within their transmission range. But false HELLO packets can be broadcasted by an adversary .As a result [19], the neighboring nodes will consider it to be within their range while the adversary may not be in its transmission range. In such cases, nodes would be unnecessarily transmitting the message and draining their energy. The targets of such attacks are protocols which rely upon exchange of location information between the nodes.

SYBIL ATTACK: A single node presenting multiple identities to the other nodes in the network is called Sybil attack. In Sybil attack, Routes thought to be going through different nodes would actually be going through the same adversary node and thereby the running an endless loop. Sybil attack is threat to location-based routing protocol. By Sybil attack [19], protocols where require exchange of location information is required, would be affected. It is because adversary nodes, when Sybil attack is launched, would be exchanging multiple sets of coordinates, rather than a single set of coordinates and hence can be in more than one place at a time.

An improved secure routing protocol based on clustering was proposed in [6] based on LEACH protocol and clustering method in which system security is integrated into sensor node and clusters are changed dynamically and periodically according to node mobility, and it is different with the traditional encryption mechanism by using key clustering homemade management to reach the overall security. The simulation results show that the proposed secure routing protocol improve the survivability of node more efficiently in a harsh sensor network environment. Through clustering management dynamically the author [6] has shown the immunity of WSNs has been enhanced, and it can be concluded that this routing protocol improved the network security effectively.

In Development of a secure, energy efficient and reliable routing protocol [7] considering the security and mobility as major constraints, energy efficiency as well as sufficient security to the mobile sensor networks was addressed. Simulation results shown that the SEER-MWSN protocol has less Energy dissipated and more network lifetime, Packet Delivery Ratio, Throughput and Delay than the existing LEACH Mobile and LEACH-Mobile-Enhanced [7] protocols

Hybrid approach for energy optimization in wireless sensor networks using ABC and firefly algorithms [8] have analyzed the life time and residual energy of the network based on optimization algorithms. Clustering is one of the best approaches used in many of the WSN routing algorithms where the appropriate cluster head to be selected for energy optimization. The proposed energy optimization algorithms are firefly and hybrid which is seen to provide better performance than traditional algorithm like direct transmission and LEACH (Low Energy Adaptive Clustering Hierarchy) protocols. The hybrid algorithm is formed [8] by combining the Artificial Bee colony ABC and firefly optimization algorithm. The proposed technique improves the life time of the network, residual energy and throughput of the wireless sensor network

In secure and efficient routing protocol for wireless sensor networks design [9] handles routing arithmetic based on grids. Many equilateral hexagons consist of the sensing area in which nodes are equally distributed. It selects the first cluster heads and chooses one second head sensor from them in each grid. Along a routing comprised of second head sensors, the arithmetic transmits the messages in a multi-jumping manner. The strategy improves the WSNs security [9]

Key establishment protocols for secure communication in clustered sensor networks, proposed two deterministic key establishment protocols to counter the vulnerabilities of LEACH protocol. These protocols are called polynomial based key establishment protocol (PBKEP) and hash-based key establishment protocol (HBKEP) [10]. These protocols ensure that it is always possible to establish a secret key with the current CH in every round of LEACH clustering protocol. The protocols also ensure that a malicious node cannot join the cluster at any round. The clusters are formed only among the legitimate nodes. Also any malicious node pretending as CH will not succeed as no other legitimate node will choose that as CH.

I.4. Clustering

Wireless sensor nodes are grouped into clusters for better network scalability. Every cluster have an organizational leader called cluster-head (CH).A CH[20] can be chosen by the network designer or can be elected by the sensors in a cluster .It can be one of the sensor nodes or a node that has richer resources. The membership of cluster can be permanent or temporary. It can form a second tier network or may just communicate the message to intended destinations such as a base-station or a command center.

I.4.1. ADVANTAGES OF CLUSTERING

- It improves network scalability.
- Clustering localizes the route set up within the cluster and thereby,[20] reducing the size of the routing table which is stored at the respective nodes.
- Clustering bounds the scope of inter-cluster interactions to CHs and thereby avoids unnecessary exchange of messages among sensor nodes. This conserves communication bandwidth.
- Clustering stabilizes the network topology of sensors level and hence reduces topology maintenance overhead. Sensor nodes have to only connect with their CHs and are not be affected by changes at inter-CH tier level.
- Optimized management strategies are implemented by CH, to enhance network operation and extend the battery life of the sensors and network lifetime.
- To reduce rate of energy consumption, CH schedules activities such that dormant nodes can go to power sleep mode
- Moreover, a CH aggregates the data sent by the sensor nodes in its cluster. By this the number of relayed packets decreases.

I.4.2. *Important Attributes in Clustering*

Clustering schemes are often used to achieve certain characteristics for the generated clusters[20]. These characteristics can be related to how it relates to others of the cluster or the internal structure of the cluster. The important attributes are

CLUSTER COUNT: In some protocols, the number of CH's are predetermined hence setting number of clusters. Picking CHs randomly from the distributed sensors[20] generally gives variable number of clusters.

STABILITY: Depending on the cluster count clustering scheme can be adaptive or fixed. If cluster count varies, the node membership changes with time and clustering scheme is adaptive[20]. Else, it is considered as fixed as sensor nodes belong to same cluster and cluster number stays same entirely

INTRA-CLUSTER TOPOLOGY: In few clustering protocols, sensor nodes directly communicate to their respective CH. But, sometimes when sensor node communication range is low , multi-hop sensor-to-CH connectivity is necessary.

INTER-CH CONNECTIVITY: Some times when BS is not in communication range of CH, the clustering schemes has to establish an inter-CH route to reach BS from each CH .In some cases it is assumed that CH can communicate directly with BS.

I.4.3. *Cluster-head Capabilities:*

The clustering approach is influenced by the network model. The network model also influences in network processing and node capabilities. CH attributes that act an important role in clustering schemes are:

MOBILITY: Sensor nodes membership changes dynamically if a CH is mobile, since the clusters have to be maintained continuously. However, a fixed CH generally have stable clusters and thereby improving intra and inter-cluster network management[20]. CHs can sometimes travel for some distance to shift itself for improving network performance.

NODE TYPES: As specified above, CH can be similar to other nodes or can sometimes be richer in resources.

ROLE: A CH can simply communicate the messages send by sensors in its cluster, aggregating them few times. Otherwise it can itself act as base-station. In such cases it can take action necessary actions on defaulters or adversaries.

I.4.4. Clustering Process

The entire clustering process and main characteristics change significantly based on clustering schemes. Some of the important attributes are:

METHODOLOGY: Clustering is done without coordination in a distributed manner[20],when CH are similar to other nodes. In some cases, a centralized authority divides the nodes to controls the cluster membership. Hybrid schemes are found when CHs are richer in resources. In such cases, inter-CHs coordination is done in a distributed manner, and each CH gas responsibility of forming its own cluster.

OBJECTIVE OF NODE GROUPING: There are many objectives for clustering such as load balancing[20], fault-tolerance, network connectivity and many more.

CLUSTER-HEAD SELECTION: As mentioned above, CHs can be chosen randomly among the nodes or can be pre-assigned.

ALGORITHM COMPLEXITY: Based on methodology and objective many clustering algorithms have been proposed. The convergence rate and complexity of such algorithms may vary.

II. LEACH Protocol

II.1. Operation of LEACH Protocol

The operation of LEACH is broken up into rounds. Each round has two phases:

i. Set-up Phase
ii. Steady-state phase

In set-up phase the clusters are organized. The set-up phase is subdivided into three phases: Advertisement phase, Cluster setup phase and Broadcast schedule phase. In the steady state phase the sensors transfer their sensed data to base station in multi-hop propagation through cluster heads. The steady-state phase is long compared to the set-up phase.

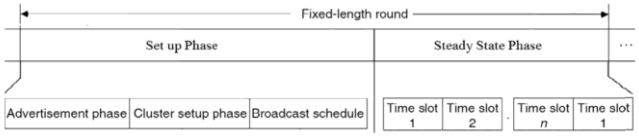

Fig.1. Phases in LEACH protocol

The threshold [6] is calculated as:

$$T(n) = \frac{P}{1 - P\left(r \bmod \frac{1}{P}\right)} if\ n \in G$$

where
P : desired percentage of cluster head r : current round number
G: the set of nodes that have not been cluster-heads in the last 1/P rounds

After every set of (1/P) rounds all the sensor nodes are again allowed to become cluster heads. Nodes that were cluster heads in previous rounds cannot become cluster heads again and as a result there are fewer nodes that are eligible to become cluster-heads with every increasing round. Therefore, the probability of a node being elected as cluster head increases with every round.

III. Secure- LEACH Protocol

In Secure-LEACH protocol, base station and sensor nodes share cryptographic keys to secure the communication between them. Using these keys the sensor nodes and base station generate a MAC (message authentication code), which is used to authenticate the origin and integrity of messages sent by sensor nodes.

III.1. *Message Authentication Code*

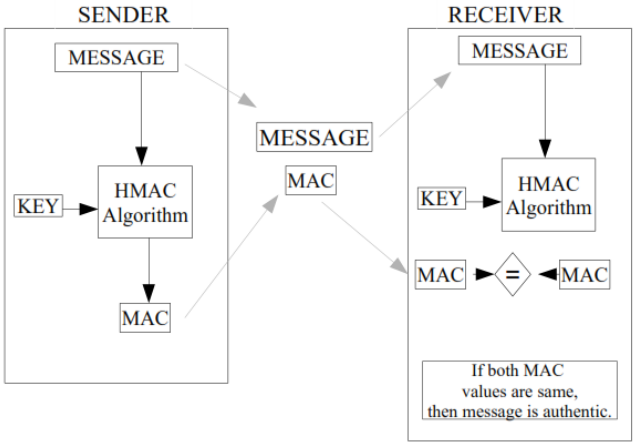

Fig.2. Message authentication code generation

III.2. *Key Generation*

The keys shared between base station and sensor nodes are generated by RSA generator. RSA generator is a cryptographically secure Pseudo Random Number Generator.

III.2.1. *RSA ALGORITHM:*

Initially a seed, x_0, is assumed such that it is a positive integer.

- Choose two large prime numbers *p* and *q*.
- Initialize *n* and equate it to the product of *p* and *q*.
- Choose a number '*b*' such that it is relatively prime to *(p-1)*(q-1)*.
- Generate a series of required number of intergers using the following formula. $x_i = (x_i\text{-}1 \wedge b) \bmod n$;for $i \geq 1$
- Generate a series of binary numbers as follows: $y_i = x_i \bmod 2$
- The generated pseudo-random sequence of *K* bits $Y = (y_1, y_2, \ldots y_k)$ is the required key.
- Different keys can be generated by using different seed or p and q values.

III.3. *Operation of Secure LEACH protocol*

In secure LEACH protocol, every node is preloaded with two keys: a symmetric key that is shared with the base station; and a group key that is shared by all members of the network with the base station. Likewise in LEACH, Secure LEACH also operates in rounds with each round starting with set-up round and followed by steady-state round. The set-up round is divided into three phases: Advertisement phase, Cluster setup phase and Broadcast schedule phase [2].

III.3.1. *ADVERTISEMENT PHASE*

In this phase, every node decides either to become a cluster-head or remain a normal node for the current round. Every node n generates a random number in the interval [0,1]. If the generated random number is less than the threshold value, T(n), the node is selected as a cluster-head for the current round. The threshold is calculated as [11]:

$$T(n) = \frac{P}{1 - P\left(r \bmod \frac{1}{p}\right)} if\ n \in G$$

where
P : desired percentage of cluster head r : current round number
G : the set of nodes that have not been cluster-heads in the last 1/P rounds

Once a node decides to be a cluster head, the node broadcasts a secure advertisement message. A secure advertisement message is a concatenation of the node's ID and a message authentication code produced with the symmetric key shared between node and the base station. All the non-cluster head nodes receive these broadcasts. They then analyze the signal strength of every secure advertisement message. The base station collects all the advertisement messages and checks their authenticity using message authentication code. After all the secure advertisement messages are processed by the base station, it creates a list consisting of cluster heads that are authenticated and broadcasts the list along with a MAC value generated using the group key.

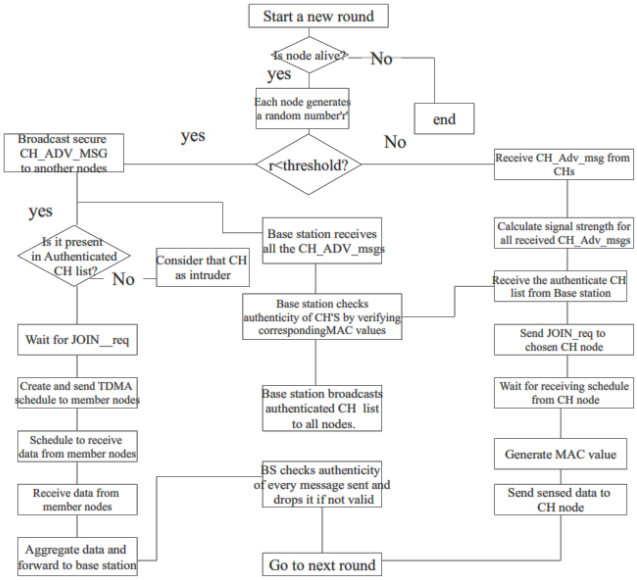

Fig.3.Flow Chart of Secure-LEACH protocol

IV. Simulation

Figure 4 shows the sensor network model for LEACH. It consists of 20 nodes represented by 'o', a base station located at the center of the network represented by '*' and one intruder represented by '**'.The sensor network has 20 nodes and the intruder is represented as 21 node.

TABLE I SIMULATION PARAMETERS

Network Area	(100*100)m
Sink position	(50,50)m
Number of sensors	20
Initial Energy of each node	0.5J
The desired percentage of CHs (p)	0.2
The electronic energy (Eelec)	50nJ/bit
The amplifier energy (Eamp)	100pJ/bit
Energy dissipated for data aggregation	5nJ/bit/signal
Packet Length for LEACH	2000
Packet Length for Secure-LEACH	2160
Energy consumed for MAC generation	2*(10^-4)J

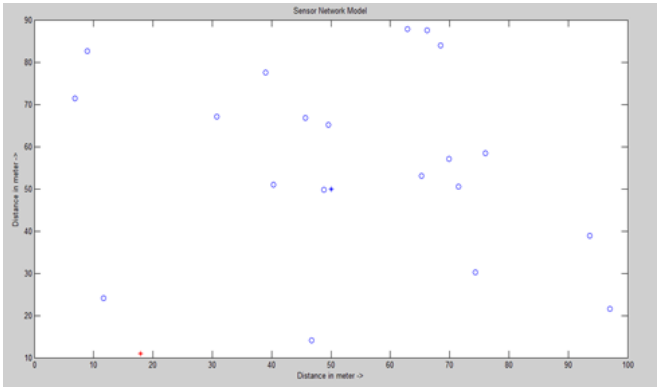

Figure 4 Sensor Network Model for LEACH with intruder

The sensor network model consists of 20 nodes represented by 'o', a base station located at the center of the network represented by '*' and three intruders represented by '**'. In the simulation if the MAC values generated by base station with all its shared keys does not match the MAC value sent by node, then it is represented as '00'. Although Secure-LEACH prevents intruder from becoming cluster head, it does not prevent intruders from sending bogus data directly to the base station. In round 3, two intruders' node 21 and node 22 send bogus messages to base station. The base station does not find a matched MAC value for messages sent by intruders and the two messages are discarded.

Although Secure-LEACH prevents intruder from becoming cluster head, it does not prevent intruders from cluster members. Intruders node 21, node 22 and node 23 become cluster members with cluster head as node 8, node 9 and node 12 respectively. But when the bogus messages from these nodes are forwarded to base station by cluster heads, they validity of its MAC value fails and messages are discarded.

From figure 5 and 6, it is clear that energy consumption is greater in secure LEACH than LEACH protocol. The energy consumption is greater in secure LEACH because length of message is longer is secure LEACH and MAC value is generated for all the messages.

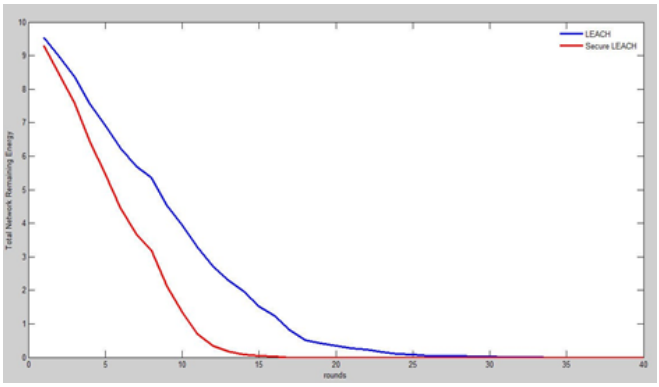

Figure 5 Node Residual Energy vsRounds

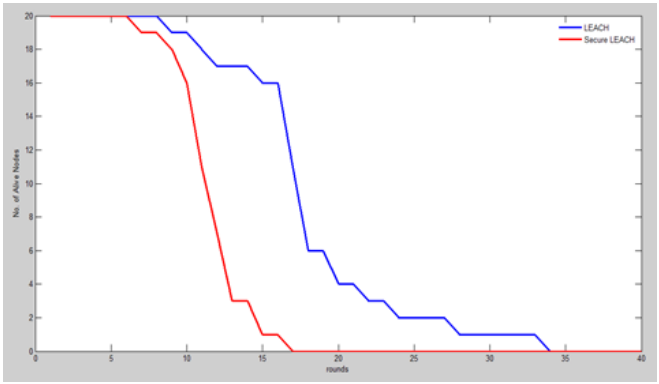

Figure 6 Number of Alive Nodes vsRounds

V. Conclusion

Secure-LEACH protocol prevents intruders from becoming Cluster heads. This feature protects the network against selective forwarding attack and hello flood attack. Instead of trying to become cluster head, intruders can become cluster members or directly send bogus data to the base station. In either case the bogus messages fails the validity check of MAC value and the base station discards the message. Secure-LEACH protocol provides the network with data authentication and data integrity with the help MAC (message authentication code) algorithm. This protocol provides resilience against only outsider attackers, which do not have access to any cryptographic material or keys of the network. The secure LEACH protocol cannot detect a insider attacker which has access to cryptographic material of the network. The protocol should be improved so that it can protect the network from both outsider and insider attackers.

References

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "*Energy efficient communication protocol for wireless microsensor networks*," in Proceedings of the 33rd Hawaii Int. Conf. on System Sciences, 2000, pp. 3005–3014

[2] Mohammad Masdari, SadeghMohammadzadehBazarchi, MoazamBidaki, "Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks", *Journal of Network and Computer Applications, Volume 36*, Issue 4, July 2013, pp. 1243–1260

[3] Mohammad Reza Rohbanian, Mohammad Rafi Kharazmi, AlirezaKeshavarz-Haddad, ManijeKeshtgary, "*Watchdog - LEACH: A new method based on LEACH protocol to Secure Clustered Wireless Sensor Networks*", internet source - http://arxiv.org/ftp/arxiv/papers/1310/1310.3637.pdf

[4] Srinath, R, Reddy, A.V, Srinivasan, R, "*AC: Cluster Based Secure Routing Protocol for WSN*", Third International Conference on Networking and Services, 2007,pp. 45

[5] Suraj Sharma, Sanjay Kumar Jena , "*A survey on secure hierarchical routing protocols in wireless sensor networks*", Proceeding of the 2011 International Conference on Communication, Computing & Security (ICCCS '11), 2011, pp. 146-151

[6] Chen, L. , Chen, L. , "An improved secure routing protocol based on clustering for Wireless Sensor Networks", *Lecture Notes in Electrical Engineering, Volume 237*, 2014, pp. 995-1001

[7] Anitha, R.U, Kadhar Nawaz, G.M, "Development of a secure, energy efficient and reliable routing protocol for mobile wireless sensor networks", *International Review on Computers and Software, Volume 9*, Issue 3, 2014, pp. 487-494

[8] Shankar. T, Shanmugavel. S, "Hybrid approach for energy optimization in wireless sensor networks using ABC and firefly algorithms", *International Review on Computers and Software, Volume 8*, Issue 10, October 2013, pp. 2335-2341

[9] Wang S, Zhang Y, Wei L, "*A secure and efficient routing protocol for wireless sensor networks*", presented at 2013 International Conference on Communication Technology, ICCT 2013, published by WIT Transactions on Information and Communication Technologies, Volume 51, 2014, pp. 705-711

[10] Poornima, A.S, Amberker, B.B, "Key establishment protocols for secure communication in clustered sensor networks", *International Journal of Communication Networks and Distributed Systems, Volume 11*, Issue 2, 2013, pp. 120-138

[11] Barolli L, Ando, H, Xhafa F, Durresi, A, Miho R, Koyama A, "*Evaluation of an Intelligent Fuzzy-Based Cluster Head Selection System for WSNs Using Different Parameters*", IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), 2011, pp. 388 - 395

[12] D. J. Dechene, A. El Jardali, M. Luccini, A. Sauer, "*A Survey of Clustering Algorithms for wireless Sensor Networks*", Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th International Conference, 2008, pp. 295 – 300.

[13] H. Zhang, J. Chen and J. Hu, "*An efficiency security model of routing protocol in wireless sensor*

networks", In 2008 Second Asia International Conference on Modeling and Simulation, Washington, DC, USA, 2008, pp. 59–64.

[14] Jennifer Yick, Biswanath Mukherjee and DipakGhosal, "Wireless sensor network survey", *Computer Networks,Volume 52*, Issue 12, 22 August 2008, pp. 2292–2330

[15] Meena Malik, Dr.Yudhvir Singh and Anshu Arora, "Analysis of LEACH Protocol in Wireless Sensor Networks", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3*, Issue 2, February2013, pp. 178-183.

[16] M. Bellare , R. Canetti and H. Krawczyk "*Message Authentication using Hash Functions - The HMAC Construction*", RSA Laboratories CryptoBytes, vol. 2, no. 1, 1996

[17] Santosh IrappaShirol, Ashok Kumar. N and Kalmesh M. Waderhatti, 2013, "Advanced-LEACH Protocol of Wireless Sensor Network*", International Journal of Engineering Trends and Technology (IJETT), Volume 4*, Issue 6, 2013, pp. 2261-2264

[18] Yan X, Xi J, Chicharo J. F. and Yu Y, "*An energy-aware multilevel clustering algorithm for wireless sensor networks*", International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008, pp. 387-392.

[19] Taran Deep Singh Pawa, *Analysis of Low Energy Adaptive Clustering Hierarchy (LEACH) protocol*, B.Tech Thesis, Department of Computer Science and Engineering, National Institute of Technology, Rourkela-769 008, Orissa, India, 2011.

[20] Ameer Ahmed Abbasi, Mohamed Younis, "A survey on clustering algorithms for wireless sensor networks", *Computer Communications, Volume 30*, Issues 14–15, 15 October 2007, Pages 2826–2841