EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

An Experimental Analysis of Secure-Energy Trade-Off using Optimized Routing Protocol In modern-secure-WSN

S.Venkataramana[1,*], B.V.D.S. Sekhar[1], Bh.V.S.Ramakrishnam Raju[1], V.V.S.S.S. Chakravarthy[2], G.Srinivas[3]

[1] Department of Information Technology, S.R.K.R. Engineering College, Bhimavaram, A.P, India.
[2] Department of ECE, Raghu Institute of Technology, Dakamarri, Visakhapatnam, A.P, India.
[3] Department of CSE, GITAM University, Visakhapatnam, A.P, India.

Abstract

In modern secure Wireless Sensor Networks (WSN), the sensor-nodes need extra energy owing to secure transmission of perceived information. So the energy-utilization of sensor-node should calculate while transfer the sensed-attributes securely to network. In this experimentation, we are proposing a revised Low Energy Adaptive Clustering Hierarchy (LEACH) protocol as LEATCH along secure information transmission (privacy and node authentication) in various levels using Quality of Protection Modeling Language (QoPML), which balance the Security-Energy trade-offs. This research experimentally analyzes the impact of data privacy, authentication operations on energy-utilization at sensor-node level while applying a LEACH & LEATCH. The obtained outcomes indicate the optimized LEATCH is outperforming correlated to the basic Leach with respect to minimal energy-utilization, time efficiency and expands life-time of modern-secure-WSNs.

Keywords: Modern-WSN, Energy Efficiency, QoPML, SAMA and LEACH Protocol.

Received on 15 July 2019, accepted on 18 January 2020, published on 06 February 2020

doi: 10.4108/eai.13-7-2018.163094

*Corresponding author. Email:svramana@srkrec.ac.in

1. Introduction

The modern-secured-WSN is containing many sensor-nodes, tiny battery-powered gadgets. Their role intends observe, perceive and grasps the info from different ecological-objects and from environment and relay the sensed information securely (by security protocol) directed toward Base-Station (BS) for more investigation [1]. As modern-secure-WSNs contain immense tiny sensor-nodes with minimal energy, so, a routing mechanism has to layout for retaining energy of sensor-nodes in modern-secure-WSN systems.

LEACH method is best hierarchical-routing method, which introduces aggregating the information; it's a turning point in grouping routing techniques. Most of hierarchical-routing methods have drafted working on the perception of LEACH [2. As per figure 1, Cluster_Head (CH) analysis with sensor estimation achieves powerful data communication with server to CH analysis.

To expand system life-time, each component's individual energy must save and for apply new mechanisms while designing modern secure WSN [2][3]. Therefore, it is better to use clustering approaches preferably directly communicating between sensor-nodes to BS that requires more sensor-energy. In modern-secure-WSN applications, activities sensed by many receptors neighbouring the event and distant from the BS or central location. Then, the establishing of short-range interaction (as in Figure-1) brings obligatorily to information packages being submitted through additional nodes along a multi-hop direction in Wi-

Fi indicator systems [4]. Sensor uses their energy mainly for three functions: Data Acquisition, information aggregation & Communication.

1. Acquisition: Mostly energy-utilization is minimal for observing and grasping the information. Nevertheless, it differs in significant ratios depends on characteristics of sensed-data being tracked [5].
2. Information processing: The burring of energy is minimal as correlated to Communication [6]
3. Communication: Here, sending information confidentially and receiving info from authenticated sources in modern-Secure-WSNs. To maintain privacy and node-level authentication in transmission requires more sensor-energy.

Thence, the consumed sensor-energy has to forecast at node-level. The interpretation of energy-consumption has to exercise by different models or tests. We suggest QoPML can exercise the consequence of above operations in energy-consumption and life-span of targeted network. The QoPML proven as a better alternative relate to similar models like Scyther, Avispa, Proveraif and UML-security and provides Secure-Energy tradeoffs for complicated modern-secure-WSN applications [7].

An excellent routing approach can minimize the energy-consumption at node level hence increase the life-time of the modern-secure-WSN without improving computational complexness. Since, modern-secure-WSN applications are energy restricted networks. Therefore, to work out on these issues, in turn, different adequate redirecting methods have developed such as LEACH, HEED and PAMAS [8].

The aim of the redirecting methods in modern-WSNs, have to implement an approach to save energy by effective transmitting of accumulated info to the BS. Normally in WS-Network, all sensor-nodes have to transfer their individually perceived info to the Base-Station directly. In most of the times, sensor-node has to act as router to pass on the information of adjacent sensor-node to BS. It drains more energy.

The LEACH is the better and well-known routing protocols in WSN systems. LEACH partitioned the whole Network as several clusters. It has many rounds. The operations in individual round considered as a unit and performed as two stages named set-up and steady-state for burning of unnecessary energy. First phase incorporates setting of new clusters and nomination of CH later second phase includes the data communication more lengthened than first phase.

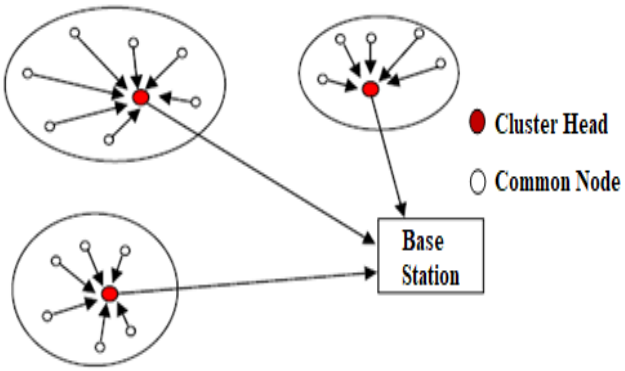

Figure 1. LEACH protocol configurations in real-time WSNs.

The design of existing LEACH is to split the structure of network as clusters regarding their perceived attributes by sensor-nodes and make randomly one as local CHs to accumulate and relay to the Base-Station. This scheme preserves vitality of sensor-node, because CHs transmitting the fused-info to BS on behalf of all sensor-nodes. However the nomination of CHs is random, and thus unable to sustain (save) energy in peculiar situations. In this scenario, we recommend some modifications especially in the nomination of CHs along with an empirical analysis of Secure-Energy Trade-off in modern-Secure-WSN.

The document is composed as Section-2 manifest the energy evaluation model in modern-Secure-WSN. Section-3 clarifies modification of CH selection in real time modern-Secure-WSN. Section-4 highlights Simulation and experimental facts and energy retaining procedure in modern-Secure-WSN. Section-5 illuminates the overall conclusions.

2. Background Approach

The QoPML uses to know the impact of security aspects on energy-utilization of a protocol in modern-Secure-WSN. By QoPML, Energy-utilization indicates by aggregation of energy-utilization all sensor-nodes for CPU (security and mathematical functions) and communicating operations (observing, receiving and transmitting) from batteries of sensor-nodes [6]. The energy-utilization of every operation (CPU/Communication) estimated as:

$$E_{OP} = T * I * V \qquad (1)$$

In the above Eq.1, refers as energy-utilization of operation (CPU/Communication), indicates index of CPU/Communication functionalities, as operation time, indicate as the current, and refer the host's voltage. QoPML as analyzes the total consumed energy by each host:

$$E_H = E_{G_{CPU}} E_{H_{CPU}} + E_{H_{COMM}} \quad (2)$$

In Eq. 2, refers to host energy-utilization, and E_H refers to energy-utilized by total operations (Processor and Communication) respectively.

The QoPML presents electic_current in three Communicating operations: transmitting-current, receiving-current, observing-current. The listening-current refers the consumed current by host in waiting state. The consumed current in transmission phase is dividing as: the transmitting and receiving current considering that hosts may use different electric currents for receiving & transmitting data (e.g., the transmitting current of receptors can differ based on signal's strength) [7]. So, node life-time $NL($ of node for a network refers as follows:

$$NL(G, v) = \frac{E_r(v)}{E_{CPU}(v) + E_{COMM}(v)} \quad (3)$$

In Eq. 3, refer node residual-energy, E_{CP} refers total energy-utilization by all CPU operations and E_{COM} refers total energy-utilization for Communicational operations of sensor-node .

The sum of complete Communication & CPU operations:

$$E_{CPU}(v) = \sum_{i=CPU} E_i(v) \quad (4)$$

$$E_{COMM}(v) = \sum_{i=COMM} E_i(v) \quad (5)$$

The lowest life-time of sensor-node referred as network's life-time (NL(G).

The energy imbalance caused by Security aspects and proper energy intake (energy efficiency) is attained by choosing utmost efficient method including security aspects at the needed stage in a given device of time [9].

Through this experimental evaluation, everybody can examine the tradeoffs between the energy-efficiency while protecting information. In addition, this experimental evaluation permits to generate events to deal with situations that require higher efficiency and higher security [10]. The events, such as substantial variation in surrounding attributes (e.g.; whether change, unsuspected communication) requires more security that influence the performance [11].

3. New Enhanced Algorithm Using Leach

LEACH is a flexible clustering redirecting method introduced by Wendi B. Heinzelman, et al [6,16]. It is self-adaptive and cluster-based routing criteria [12][13]. The nomination of Cluster_Head is random, so, the energy-utilization of Cluster_Head is varies considering sensing-range (distance) between Cluster_Heads and BS. Cluster_Heads verifies the authenticity of common nodes then gather the sensed-info and fuse within own clusters thus pass on the fused information securely to the BS. It means that CH has to check the authentication of each node, provide privacy to aggregated info and relay it to BS.

If the chosen Cluster_Head is far distant from the Base-Station will utilize additional energy because of long-range data transmission. In such scenarios, the CH present energy is minimal; the CH will die soon for their excessive energy loss. So the Cluster will isolate from the network. To address these issues, this paper exercises an enhanced technique to minimize the energy burdens of such Cluster_Heads and provide node level authentication during cluster formation and message privacy during data transmission using QOPML. In addition to the above implementation this work also implemented calculation of energy consumption of each node in the entire network. Hence we calculated residual energy of every node in each round.

Low Energy Adaptive level-Two-CH Clustering Hierarchy (LEATCH) is an enhanced one build upon LEACH Method; the creating clusters and choosing Cluster_Head is almost identical as LEACH technique but the finalizing the Cluster_Head is peculiar in LEATCH.

1. If the average_energy(E_{avg}) of all nodes in the cluster is higher than the residual_energy (E_{res}) of Cluster_Head in that cluster, i.e. $E_{avg} > E_{res}$, $Where\ E_{avg} = \sum_1^N E(i)_{res}$ or the average-distance (d_{avg}) is shorter than the distance of CH and BS is (d_i), i.e. $d_{avg} < d_i$, $where\ d_{avg} = \sum_1^N d_i$ is the average_distance of entire nodes' distance to BS. In this situation, the non-Cluster_Head node with highest residual_energy in that cluster will become as another CH (level-Two-CH)[14].

2. Otherwise, the nomination of level-Two-CH is unnecessary.

Usually the Steadystate phase depletes higher energy than Set-up phase [6]. Suppose the cluster has Two Cluster_Heads, then primary Cluster_Head check the authenticity of common nodes before gather information and handover them to corresponding level-Two-CH i.e., additional Cluster_Head, then the level-Two-CH accepts the responsibility to aggregating the info and provides privacy. Then the level-Two-CH initiates TDMA schedule to complete the Steady State phase.

Suppose the Cluster without level-Two-CH then, the Cluster_Head will do the entire process.

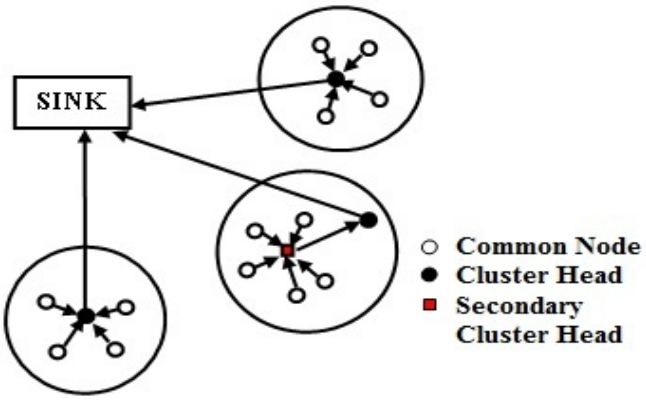

Figure 2. New Routing technique (LEATCH)

The LEATCH algorithm time-line process of modern-Secure-WSN as depicted below.

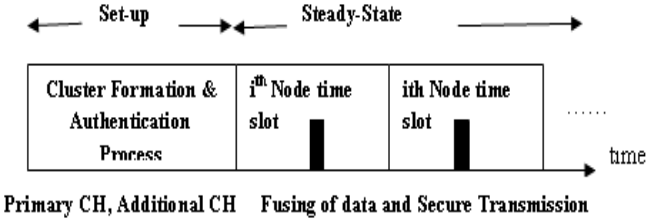

Figure 3. LEATCH protocol Process

As in Figure 3 both CH and level-Two-CH (if necessary) are formed in Set-up State. During Set-up phase, each node authentication process is executed. During Steady State phase, data fusing, implementation of secure transmission (privacy) and formation of TDMA frame is executed. Hence in the Steady-state phase utilizes high energy than the set-up phase [5], especially in the long-distance information transferring. Accordingly, the level-Two-CH will balance the load and it eliminates imbalance of energy-utilization of entire network.

4. Simulation Results

This content uses NS-3 as simulator platform to construct the QoPML secure network, and emulate LEACH technique and optimized LEATCH method. In same network, security aspects (authentication and privacy) provided by the SAMA based on ECC Protocol, efficient LEATCH are analyzed by QoPML Energy model [9]. Therefore, we examine the enhanced method efficiency in two aspects: the energy-utilization and life-time the modern- secure-WSNs. The total duration between the starting of simulation to death of last sensor-node is referred as the Network's life-time.

Simulation guidelines:

(i) Sensor-nodes are evenly spread within field of Square-shape.
(ii) All Sensors have same initial-energy, level & sensing power is same, separate ID number throughout the simulation.
(iii) Sensor-nodes have limited energy, unattended after deployment and fixed located.
(iv) Base_Station fixed at center of field and the sensor-nodes will communicated along BS using single-hop or multi hop.

Table 1. Different parameters in Simulation

Parameters	Value
Size of Packet	40000 bits
Area	100*100
Sensor-nodes	200
E_{elec}	50 njoul per bit
Initial-State-Energy	0.5 joul
ε_{mp}	0.013 pJ/bit/m4
ε_{fs}	10 pJ/bit/m2
CH probability	p=7%
BS Location	(50,50)
EDA	5nJoul per bit

4.1 Investigation under experimental setup:

200 sensor_nodes evenly distributed in 100m*100m, square region. The Base_Staion is placed at the coordinates of (50, 50), the centre of simulation area. The Figure-4 shows the Sensor-node position in the simulation and the nodes' are evenly distributed.

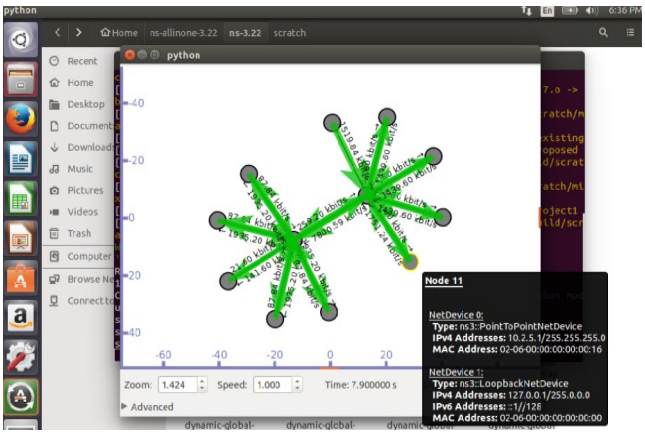

Figure 4. Sensor-Node position in simulation.

The set-up and steadystate stage ie., Cluster Formation, CH election and Data transmission securely in modern-Secure-WSN are shown in figures 5,6 and 7.

4.2 Implementation Results of LEATCH Protocol

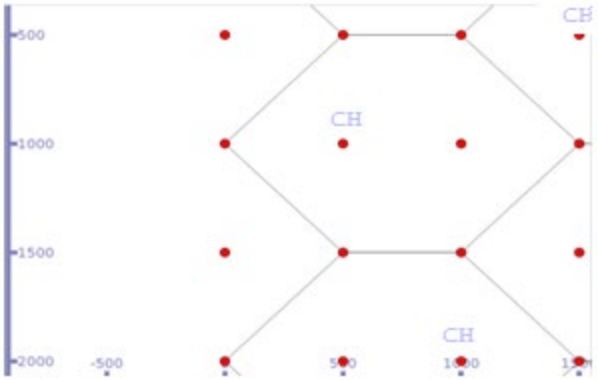

Figure 5. Cluster Generation

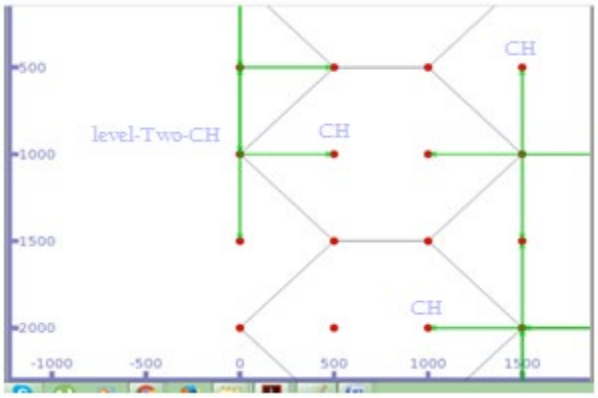

Figure 6. CH, level-Two-CH Nomination

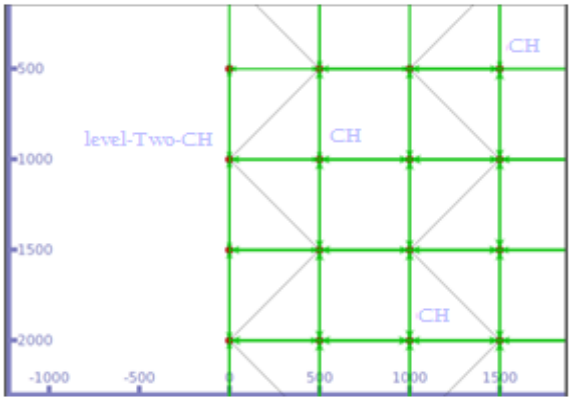

Figure 7. Steady-state Phase

In our simulation, Fig. 5 represents hexagonal distribution of nodes and cluster formation. Fig.6 depicts the additional CH nomination and Fig. 7 shows the steady-state phase.

The lifespan of WSNetwork defines the living time-period from the initiation of simulator to sufficient time when the final sensor-node dies. Two periods are defined for system life-time in secure-WSN as stable and unstable. The period between the starting of the simulation and the first node died is called Stable. The period between end of simulation and death of first node is called unstable.

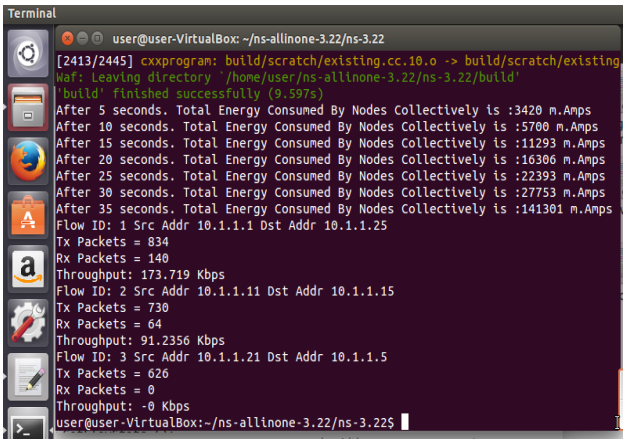

Figure 8. Energy-Utilization w.r.t. QoPML

In Fig. 8 shows, the simulation results carried out using QoPML for calculation of energy utilization by nodes in the network without implementation of any routing protocols.

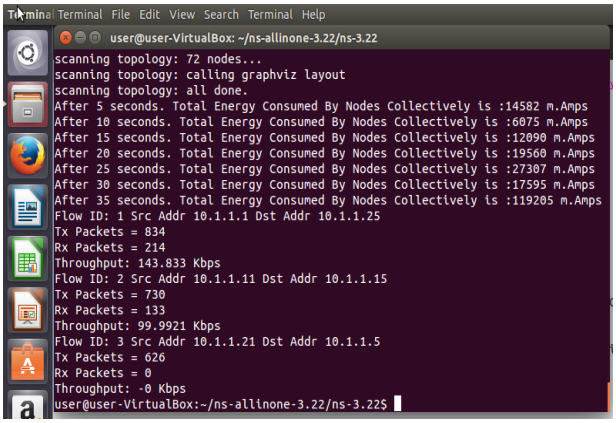

Figure 9. Energy-Utilization w.r.t. LEACH

In Fig. 9 represents, the simulation results carried out using QoPML for calculation of energy utilization by nodes in the network with implementation of LEACH protocol.

In Fig. 10 shows, the simulation results carried out using QoPML for calculation of energy utilization by nodes in the network with implementation of LEATCH protocol.

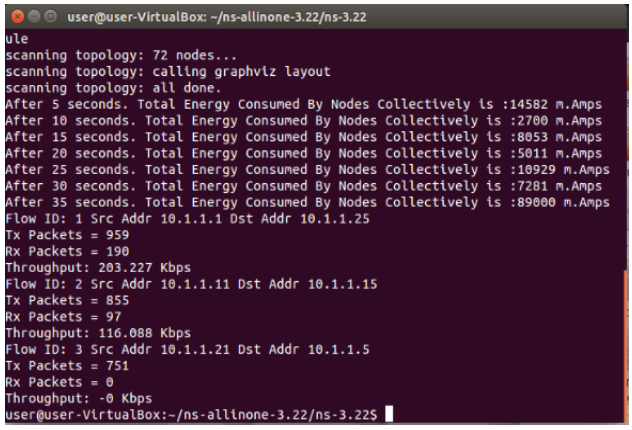

Figure 10. Energy-Utilization w.r.t. LEATCH

LEATCH protocol reduces the energy-utilization of few CH's whose residual_energy is low or is at a distant place from BS by setting level-Two-CH. From the simulation experimental outcomes, we tabulated our outcomes and evidenced that our new LEATCH protocol outperformed than old LEACH in Table 2.

Table 2. Energy results with respect to node communication

No. of Rounds w.r.t. Time Intervals	QoPML (m.Amps)	LEACH (m.Amps)	LEATCH (m.Amps)
50	3420	14582	14582
100	5700	6075	2700
150	11293	12090	8053
200	16306	19560	2011
250	22393	27307	10929
300	27753	17595	7281

Our improved LEACH gives better energy-utilization levels as depicted in Table 2 w.r.t host to host secure transmission in modern-secure-WSNs. After 50 rounds our proposed method consumes more energy but efficiency increased as number of rounds increased and in the same line the number of dead nodes are less.

Communication Results W.R.T to Time:

Time comparison results in Wireless Sensor Networks with nodes communication with respect to time for packets dropping in the middle of data transmission by hop by hop communication. Table 3 shows analysis results with respect to time in data communication between nodes.

Table 3. Time efficiency with respect to node communication

No. of Rounds w.r.t. Time Intervals	QoPML (Seconds)	LEACH (Seconds)	LEATCH (Seconds)
10	0.9	1.2	1.8
20	1.1	1.9	2.4
30	2.1	2.8	3.6
40	3.06	3.9	4.5
50	3.4	4.2	4.5
60	3.9	4.8	5.7

As per the results depicted in Table 3, LEATCH outperformed in terms of time taken for the first to die compared to other two protocols. After 10 rounds, the proposed method took 50% more time for the death of first node and after 60 rounds the proposed method took 46% more time for the death of first node. Whenever the number of rounds increased then the number of outcomes in real-time data transmission of the host to host communication with respect to time in our modified LEACH protocol gives efficient communication without loss of data delivery in WSN.

5. Conclusion

In this experimentation, we conclude total energy-utilization in direct transmission using QoPML (with security aspects) gradually increased throughout simulation period. In this context, comparing LEATCH and LEACH, after 50 rounds of simulation both protocols consumed same energy, our proposed LEATCH protocol has outperformed after 300 rounds of simulation in terms of saving energy which is 36% when compared to QoPML and after 300 rounds of simulation LEATCH has conserved around 56% of energy when compared to LEACH. In the same line we additionally implemented node authentication, message privacy and calculation of energy consumed by each node in the network for each round of simulation when compared to traditional LEACH and LEACH-TLCH protocols [4, 14]. This experimental research is suitable for small-scale WSNs. This can be enhances by implementing dynamic routing for large-scale Secure-WSNs. And this work can be extended for dynamic load balancing by using Evolutionary Computing Tools [15].

References

[1] Chunyao FU1, Zhifang JIANG1, Wei WEI2and Ang WEI*3, "An Energy Balanced Algorithm of LEACH Protocol in WSN", in Proceedings in IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[2] Ian F. Akyildiz, Weilian Su, and Yogesh Sankarasubramaniam, et al. "Wireless Sensor Network: A survey", Computer Networks, Vol.38(4) pp: 393-422, 2003.

[3] R.A.Roseline and Dr. P.Sumathi, "Energy Efficient Routing Protocol and Algorithms for Wireless Sensor Networks-A Survey", in Global Journal of Computer Science and Technology, vol.11, December 2011.

[4] Heinzelman W, Chandrakasan A, Balakrishnan H, "Energy Efficient Communication Protocol for Wireless Microsensor Networks", In Proceedings of the 33rd Hawaii International Conference on System Sciences. Maui: IEEE Computer Society, Vol.2: pp: 3005-3014, 2000.

[5] Cui Li Ju, Hailing, Miao Yong, Li Tianpu, Liu Wei and Zhao Ze, "Overview of Wireless Sensor Networks", Journal of Computer Research and Development; Jan' 2005.

[6] W. R. Heinzelman, A. Chandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", in Proceedings of the 33rd Hawali International Conference on System Sciences-2000, Jan'2000.

[7] Damian Rusinek, Bogban Ksiezopolsk and Adam Wierzbicki, "Security Trade-Off and Energy Efficiency Analysis in Wireless Sensor Networks", International Journal of distributed Sensor Networks; February' 2015.

[8] T. Rault, A. Bouabdallah, and Y. Challal "Energy efficiency in wireless sensor networks: a top-down survey", in Computer Networks, vol. 67, pp. 104–122, 2014.

[9] S.Venkataramana, P. V.G.D. Prasad Reddy, S. Krishna Rao, "Secure Energy Tradeoff with low power consumption in data transmission of Wireless Sensor Networks", ARPN Journal of Engineering & Applied Sciences, ISSN: 1819-6608, Vol. 11, No. 7, Page No: 4310-4316, April'2016.

[10] S.Venkataramana, P. V.G.D. Prasad Reddy, S. Krishna Rao, "Energy Based Topology Control in Wireless Sensor Networks", in International Journal of Applied Engineering Research, Vol. 11, No. 7, pp 5091-5096, 2016.

[11] B. Ksiezopolski and Z. Kotulski, "Adaptable security mechanism for dynamic environments", in Computers & Security, Vol. 26, No.3, pp. 246–255, 2007.

[12] J. Haapola, Z. Shelby, C. Pomalaza-R´aez, and P. M'ah'onen, "Cross-layer energy analysis of multi- hop wireless sensor networks", in Proc. 2nd European Workshop on Wireless Sensor Networks, pp. 33-44, January 2005.

[13] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part ICarrier sense multiple-access modes and their throughput-delay characteristics", in IEEE Trans. Commun., vol. 23, no. 12, pp. 1400-1416.

[14] K. Yang, Y. Wu, and H. Zhou, "An Energy Balanced Algorithm of LEACH Protocol in WSN," in International Journal of Computer Science Issues, Vol 10, Issue 1, pp. 354-359, Jan' 2013.

[15] BVDS Sekhar, PVGD Prasad Reddy, GPS Varma "Performance Of Secure And Robust Watermarking Using Evolutionary Computing Technique" JGIM, Vol 25, Issue 4, pp: 61-79, 2017.

[16] AmineRais, KhalidBouragba, and Mohammed Ouzzif "Routing and Clustering of Sensor Nodes in the Honeycomb Architecture" Vol 2019, pp 1-12, Mar'2019