

Chaos based Secured Communication in Energy Efficient Wireless Sensor Networks

Nidarsh M P¹, Mrs. G Padmaja Devi²

¹ PG Scholar, Dept.of E&C, Malnad college of engineering, Karnataka, India

² Associate Professor, Dept.of E&C, Malnad college of engineering, Karnataka, India

Abstract - Wireless sensor networks has a important role in recent network technology, WSN which contains number of sensor nodes used to monitor physical and environmental condition such as temperature, sound, vibration, pressure, humidity, motion or pollutants, further it sends their data through the network to main location. Some of the sensor nodes are furnished with supported battery power through which it can furnish ample of operation and it can also communicate with other nodes. Increasing the lifetime of the wireless sensor network, power management part is essential for improving the performance of WSN. This paper proposes a chaotic encryption with clustered Low Energy Adoptive Cluster Head (LEACH) algorithm for wireless energy efficient networks which also reduces the consumption in WSN. The performance of the proposed work is evaluated and comparison is done.

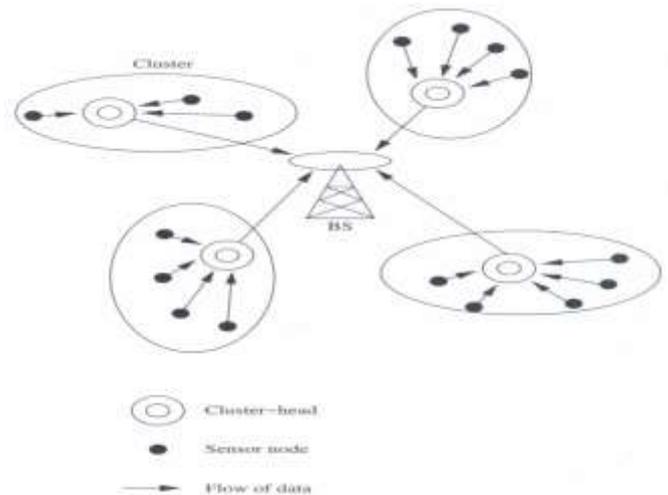


Fig -1: Cluster formation

Key Words: WSN, LEACH, Energy efficiency, network lifetime, chaotic encryption.

1. INTRODUCTION

Wireless Sensor Network is a type of network which self-organizes with a huge number of small sensors. The main aim of sensor node is to complete the packet transmission among itself within the network area, which can identify and notice the physical entity of real world environment. WSN contain of various number of sensor nodes which can further sense their locality and contact among themselves. Main characteristics of WSN nodes are contains tiny size, reasonable cost, less consumption of power, multi-functional such as it can perform sensing, data processing, routing and communicate easily in short distances. In abandoned hostile regions, these devices are implemented in general, but it becomes difficult to recharge the power source.

With the help of multiple clusters, sensor nodes are designed and organized in a proper manner. The cluster head is selected by several group of nodes, here each and every node can act has part of message transfer in between multiple nodes. At last, all nodes will go for sharing messages to base station by cluster head. Sensor networks always preferred to use cluster design, this in turn help us to capture for data gather and fusion operations by each of sensor nodes. It exchange message with cluster head which is going to send message to its nearest base station. The following figure 1 shows actual formation of cluster heads and selection of those are independent to each other.

In current situation of WSN correct use of battery power is not up to the mark, due to which there will be dissimilarity while sending the message to destination node from source node. So multi hop communication plays a major role as a part of its requirements. Sometimes it's preferred to use hierarchical routing during data transmission in order to improve sensor network lifetime. Cluster can be made by collecting group of nodes which helps to build hierarchical routing and cluster head to be selected by every cluster in its corresponding network. As a part of data transmission, cluster head liable for data collection from adjacent nodes and base station will go for receiving data.

2. RELATED WORK

WSN facing its own challenges and issues can be identified by the researchers. To improve the network life time, many protocols have been followed. Here [1] introduced the protocol called Low Energy Adoptive Cluster Head [LEACH]. Hence it help us to get improved the energy performance of network. Drawback here is that the performance is not up to the mark D.Aradhana, NagaveniB.Biradar and K. LingaRaj[2] proposed the novel method to get more number of clusters from the network. Here, they were using mobile agents from every cluster for sending data to cluster head instead of choosing nodes. These mobile nodes will collect data from all the nodes belong to network with that aggregation of data can be performed. The aggregated data will be received by the base station. The two components play a major role in this method, such as group array and ordinal array.

Clustering has been broadly considered in the network literature as well as in information processing [3-5].

N Eghbali [6] deals with nodes are facing problems like lack of unique address in sensor network and it is most important for collecting information from the sensors. Once the nodes have got dispersed, accesses to corresponding nodes get delayed. The nodes present in the network will become useless and leads to decay behind the obtained energy gets over. Hence the issues related to energy consumption and optimization is a greater challenge faced in real time network applications. Recently lots more have been appreciated towards it. D. T. Ho, T. A. Johansen, J. B. D. Sousa, E. I. Grøtli and P. B. Sujit, [7], done a comparison with earlier papers, this paper have an enhanced method. First of all using a special scheme called PSO and its get modified with optimal path selection for relay data. This paper uses a mixture of two multiple access methods to achieve communication such as TDMA and CSMA/CA and performance comparison can be done in better way.

Prof. Rajeev Vishwakarma, Apurva Bhalerao [8] discussed the concept of gaining reliability and energy consumption by doing setup of wireless sensor network in simulation. Based on some parameters of WSN, deciding the network stability in terms of energy and its existence. The particle swarm optimization is taken into consideration for optimizing the update time and hop distance. In order to improve the performance of WSN, the following parameters to be considered such as transmission power, used frequency, modulation technique and so on. NING WANG, WEI XIANG AND YUAN ZHOU, (Senior Member, IEEE) [9] illustrate the new method for to extend the lifetime of network using advanced particle swarm optimization algorithm. This is used to choose target nodes as a process of optimization. The set of rules formed to get better results for parameters like transmission distance and energy efficiency. This paper proposes a distributed sensor in better way and balanced system for clusters to enhance the network lifetime. In early days, optimal cluster layout can be obtained by applying several fitness functions with the use of PSO [10-12]. Wireless sensor network is have some clustering problems, PSO act has a solution to those problems by embedding it into some other algorithms [13]. Alaa SHETA, Basma Fathi SOLAIMAN [14] addressed the WSN problem facing to use energy resources efficiently and minimizing traffic during transmission by applying balanced load distribution. To solve this type of problem, proposed a new way of finding optimal distribution of cluster heads and sensors. Hence, consumption of energy inversely proposed to lifetime of network. This paper comes with the idea of introducing hybrid cluster algorithm with the help of particle swarm optimization and K-means clustering.

3. METHODOLOGY

Cluster head selection algorithm:

Step-1: Create Sensor Network Model.

Step-2: Assign initial energy to sensor nodes.

Step-3: Sort the nodes based on the distance from Base station.

Step-4: For round=1 assign cluster heads based on minimum distance from the base-station.

Step-5: Continue step-4 for allotted number of round and corresponding cluster heads get selected.

3.1 LEACH PROTOCOL

LEACH is network protocol and much essential to use. Since some nodes present in network is not at all useful when the battery dies. The LEACH protocol let us to find out the nodes lifespan and permitting to do minimal work it essentially used for data transmission

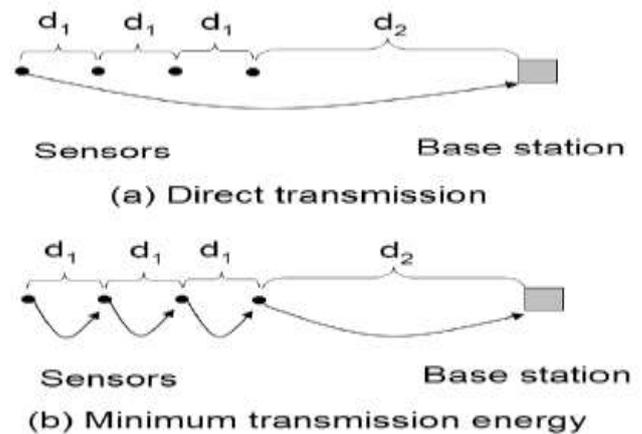


Fig -2: Direct v/s Minimum transmission

The energy used in direct transmission can be modeled by

$$dk(3d_1+d_2)^2$$

Whereas energy used for minimum transmission can also be modeled using

$$dk(3d_1^2+d_2^2)$$

Where d is energy dissipation

k is length of message in bits

Usually LEACH network is having two different stages such as set-up stage and steady stage. The set-up stage is meant for cluster heads selection and steady stage is used to maintain the cluster heads when the transmission of data is happening among nodes within the network. The Figure4 shows clear cut idea about using LEACH protocol by comparing with other cases. Here, second gives better arrangement since the network is accurately sectioned and neatly spaced out the cluster heads.

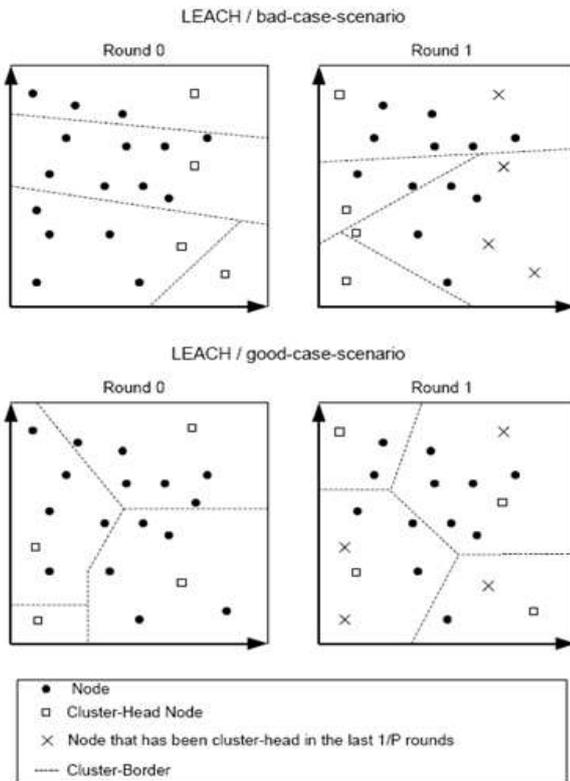


Fig -3: LEACH v/s bad-case scenario

$$\frac{dY}{dt} = Y(r - Z) - Y \quad (4)$$

$$\frac{dZ}{dt} = X * Y - b * Z \quad (5)$$

The System exhibits chaotic behavior when the parameters are having values $s = 10, r = 28$ and $b = \frac{8}{3}$

Chaotic Maps	Initial Conditions
2D Logistic Map	$x_0 = 0.1$
	$y_0 = 0.1$
	$r = 1$
3D Lorenz Map	$x_0 = 0.1$
	$y_0 = 0.1$
	$r = 28$
	$s = 10$
	$b = 8/3$

Table -1: Network Security Initial Conditions Parameters

3.2 CHAOTIC CRYPTOGRAPHY

3.2.1 Two Dimensional Logistic Map

The two dimensional logistic map is well known for its complicated chaotic behavior when compared to the one dimensional logistic map. It takes the input x_i, y_i and r in a plane and maps it to a new point. Mathematically it can be defined as

$$x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \quad (1)$$

$$y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \quad (2)$$

Where r is the system parameter x_i, y_i are the pair wise points. The map depends on three values namely x_0, y_0 and r whose corresponding initial values are $r = 1.19, x_0 = 0.8909$ and $y_0 = 0.3342$.

3.2.2 Three Dimensional Lorenz Map

The Lorenz equation can be represented in differential equations having chaotic behavior for certain parameters with initial conditions. Mathematically it can be defined as

$$\frac{dX}{dt} = s(X - Y) \quad (3)$$

3.2.3 Encryption Scheme

The proposed algorithm consists of two phases. The first phase includes Confusion which scrambles the data and the second phase includes Diffusion which modifies the data based on the chaotic sequences. The proposed crypto system is shown in Fig 1.

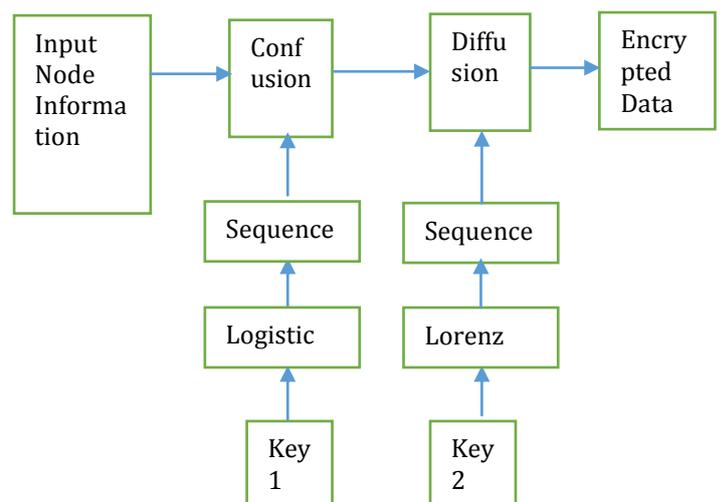


Fig -4: Network Encryption Scheme

3.2.4 Confusion

For a byte level confusion is done by interchanging the positions of the information based on the chaotic sequence generated by 2D logistic map.

The Nodal information X (row matrix) of size $1 \times N$ is taken as input for confusion.

The chaotic sequence are generated by 2D logistic map and arrange them in a row matrix of size $M \times 1$. Sort the obtained chaotic sequence in the ascending order and the index values are obtained in L1.

The rows of matrix X are shuffled based on the index values of L1 to achieve matrix Y.

3.2.5 Diffusion

Diffusion includes logical XOR operation between the confused data Y and the matrix containing the chaotic sequences obtained from the three-dimensional Lorenz map.

Generate chaotic sequences from the three-dimensional Lorenz map.

Convert the obtained sequences into integer value ranges from 0 to 255 and store them in a matrix Z1.

Logical XOR is performed between confused data Y with the matrix obtained from Lorenz map Z1 to achieve matrix H1 of size $1 \times N$.

The obtained encrypted matrix H1 is ready to transfer over the network.

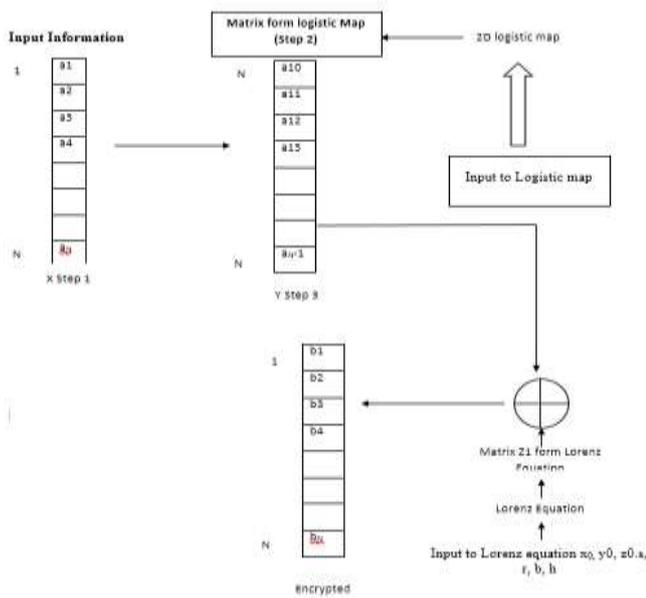


Fig -5: Block diagram of the proposed encryption technique

3.3 LIFE TIME OF THE CHAOS NETWORK

The proposed research work is further extended to evaluate the life time of the network. It includes energy conservation in each and every sensor node by makes use of clustering and supporting cluster head selection energy optimization algorithm. The supporting cluster head is chosen based on residual energy. To increase the WSN lifetime, energy optimization techniques and energy conservation measures are enhanced.

Parameters	Initial Values
Number of Nodes	100
Base station Location	(100,100)
Packet Length	2000
Initial Energy (E_0)	2 Joules
Tx Energy (E_{TX})	50×10^{-9} Joules
Rx Energy (E_{RX})	50×10^{-9} Joules
Data Aggregation Energy	5×10^{-9} Joules

Table -2: Energy Efficient Network Parameters

4. RESULTS AND DISCUSSIONS

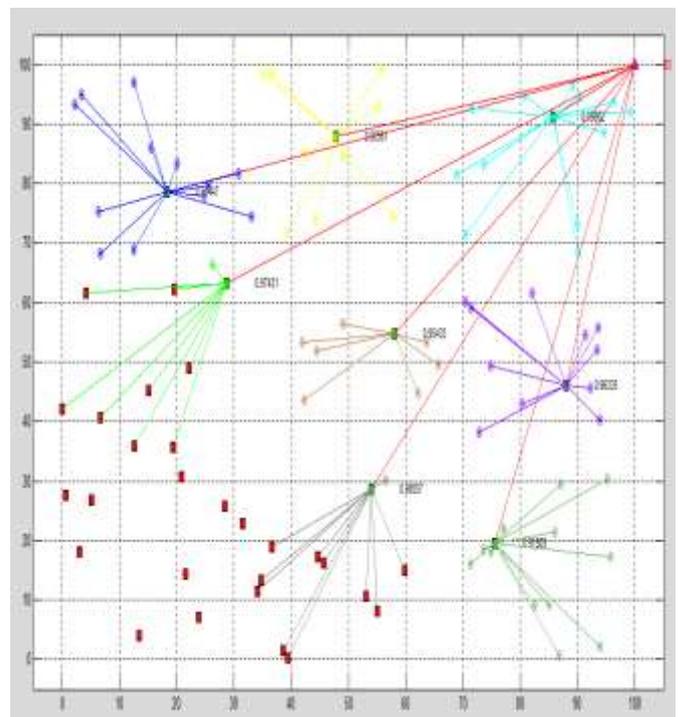


Fig -6: Distribution of Nodes and Cluster Formation

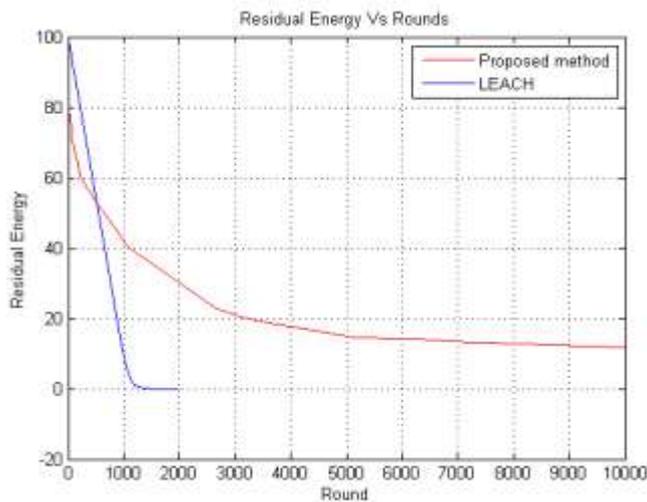


Fig -7: Residual Energy versus Number of Iterations

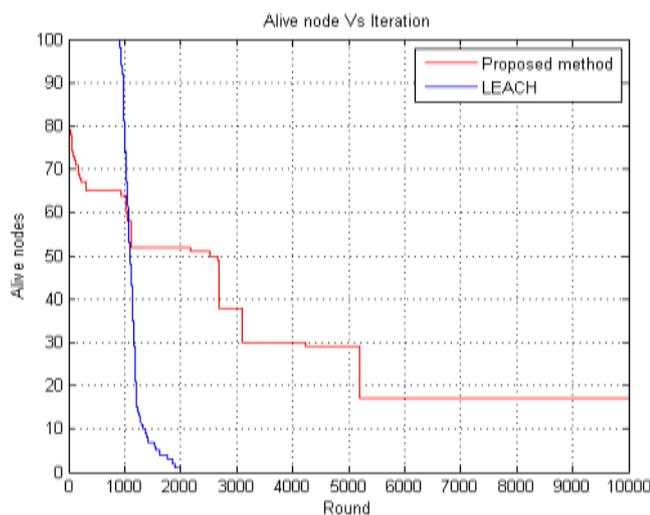


Fig -8: Number of Alive Nodes versus Number of Iterations

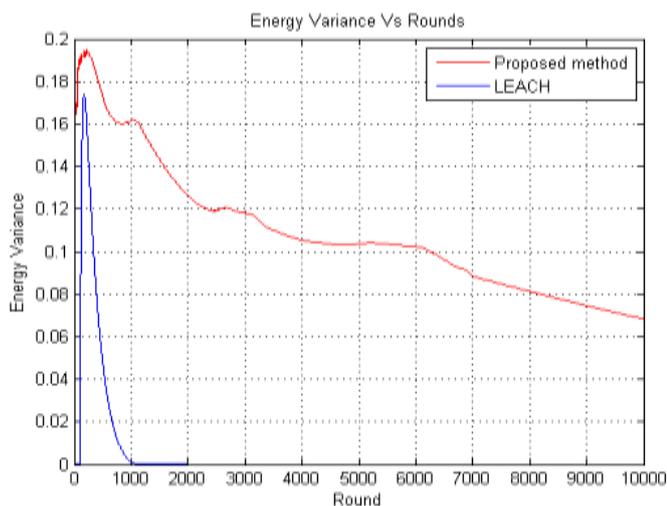


Fig -9: Energy Variance versus Number of Iterations

In order to evaluate the effect of network security on network life time various performance metrics are measured and compared with traditional LEACH technique. Residual Energy is evaluated in Figure 7 for both chaos based Clustered WSN and traditional LEACH algorithm and it is shown that Energy reduction is less when compared to LEACH. Figure 8 shows number of alive nodes when compared with the LEACH system.

Figure 9 shows Average energy variance of all nodes has less significant using proposed chaos based WSN.

5. CONCLUSIONS

The performance of WSN is improved by LEACH based clustering and cluster head selection method algorithms by increasing the residual energy, throughput, quantity of active nodes and packet delivery ratio. The better clustering algorithm builds clusters in a centralized manner within a base station and choice of cluster heads by using LEACH in dispersed manner. The performance metrics such as network lifetime, throughput, packet delivery ratio, delay, normalized overhead, total energy consumption and residual energy are estimated and compared with advanced clustering methodology. The simulation result shows that the projected Chaotic Encryption with Clustered LEACH scheme gives improved performance in order to reduce the total energy consumption and increasing the lifetime of WSN.

REFERENCES

- [1] Liu, Z., Liu, Z., and Wen, L. (2011). "A leach protocol for wireless sensor networks. In Advanced Computational Intelligence (IWACI)", 2011 Fourth International Workshop on, pages 766-769.
- [2] K. LingaRaj, D. Aradhana and Nagaveni B. Biradar, "Multiple mobile agents in wireless sensor networks using genetic algorithms", International Journal of Scientific and Engineering Research, vol3, 2012, pp1-5.
- [3] Low CP, Fang C, Mee J, Ang, YH. Load-balanced clustering algorithms for wireless sensor networks. In: IEEE International Conference on Communications; 24-28 June 2007; Glasgow, UK. New York, NY, USA: IEEE. pp. 3485-3490.
- [4] Gavalas D, Mpitziopoulos A, Pantziou G, Konstantopoulos C. An approach for near-optimal distributed data fusion in wireless sensor networks. Wirel Netw 2010; 16: 1407-1425.
- [5] Tan R, Xing G, Li, B, Wang J, Jia X. Exploiting data fusion to improve the coverage of wireless sensor networks. IEEE/ACM Tr Netw 2012; 20: 450-462.
- [6] N.Eghbali, "Performance Improvement of Information Dissemination Protocols in Sensor Networks

Through Data Aggregation, Computer Engineering and Information Technology Department”, 2007.PP 1-121.

- [7] D. T. Ho, E. I. Grøtli, P. B. Sujit, T. A. Johansen, and J. B. D. Sousa, “Cluster-based communication topology selection and UAV path planning in wireless sensor networks,” in Proc. of International Conference on Unmanned Aircraft Systems (ICUAS). Atlanta, GA, USA: IEEE, 2013.
- [8] Prof. Rajeev Vishwakarma, Apurva Bhalerao, “Performance of Wireless Sensor Network using Particle Swarm Optimization Algorithm”, International Journal of Computer Application (2250-1797) Volume 6– No.1, January- February 2016.
- [9] YUAN ZHOU, (Senior Member, IEEE), NING WANG, AND WEI XIANG, (Senior Member, IEEE), “Clustering Hierarchy Protocol in Wireless Sensor Networks Using an Improved PSO Algorithm”, date of publication December 1, 2016, date of current version March 13, 2017.
- [10] Latiff N, Tsimenidis C, Sharif B. Energy-aware clustering for wireless sensor networks using particle swarm optimization. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications; 3–7 September 2007; Athens, Greece. New York, NY, USA: IEEE. pp. 1-5.
- [11] Hou J, Fan X, Wang W, Jie J, Wang Y. Clustering strategy of wireless sensor networks based on improved discrete particle swarm optimization. In: IEEE Sixth International Conference on Natural Computation; 10–12 August 2010; Yantai, China. New York, NY, USA: IEEE. pp. 3866-3870.
- [12] Kulkarni R, Venayagamoorthy G. Particle swarm optimization in wireless sensor networks: a brief survey. IEEE TSyst Man Cy C 2011; 41: 262-267.
- [13] Karthikeyan M, Venkatalakshmi K. Energy conscious clustering of wireless sensor network using PSO incorporated cuckoo search. In: IEEE Third International Conference on Computing Communication Networking Technologies; 26–28 July 2012; Coimbatore, India. New York, NY, USA: IEEE. pp. 1-7.
- [14] Basma Fathi SOLAIMAN,, Alaa SHETA, “Energy optimization in wireless sensor networks using a hybrid K-means PSO clustering algorithm”, Turk Journal of Electrical Engineering & Computer Science(2016) 24: 2679 – 2695,doi:10.3906/elk-1403-293.