International Journal of Engineering & Technology, 7 (4.39) (2018) 123-127

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Development of Hybrid Approach for Receiver Location Privacy in WSN

Premananda B.S.[1]*, Sindhudhar K.L.[2]

[1,2] R.V. College of Engineering,
Bengaluru, India
**Corresponding author E-mail: premanandabs@gmail.com:*

Abstract

The various security protocols in wireless sensor networks (WSNs) provide confidentiality for the content of message but the contextual information remains exposed. The exposed contextual information can be utilized by the adversary to deliver attack or derive the sensitive information such as location of the sink nodes, source node and monitored objects. In applications such as military and research institutions the security is of greater importance and very crucial. In sensor network the base station (BS) acts as a gateway between the sensor nodes and the control unit. The vital data sensed by the sensor nodes finally reaches the BS. Hence, BS is a major target of attack. By knowing the physical location of the BS an attacker can alter or destroy the BS intern results in the failure of the entire sensor network. There is a need for routing algorithm which can effectively camouflage the location of the BS. In this paper a hybrid algorithm which provides location privacy of the BS has been proposed. The results infer that the proposed algorithm is independent of quantity of the traffic and an adversary will have less than 4 % chance of locating the physical location of the BS. The sensor nodes also exhibited limited energy consumption.

Keywords*: Energy; Location privacy; Contextual Information; Sink node; Wireless Sensor Networks.*

1. Introduction

A WSN is a self-oriented autonomous network comprising of numerous sensor nodes and BS's. The sensor node senses the information from the surrounding environment and finally the sensed information reaches the BS. In WSN each sensor node has a limited amount of energy. When a sensor loses power it is unable to communicate to its neighbours, sense data and finally becomes a failure one. The sensor nodes are hardware constrained and has limited lifetime. Anonymity can be defined as the state of being not identifiable within a set of subjects with potentially the similar attributes as the original subject.

The sensor node comprises of sensing, processing and communication unit which are having control from a battery unit [1]. The components of a typical sensor node are portrayed in the Figure 1. The sensing unit consists of actual sensor and analog to digital converter. The processing unit mainly connected with a small storage unit. A sensor can sense the data from its surrounding and store them.

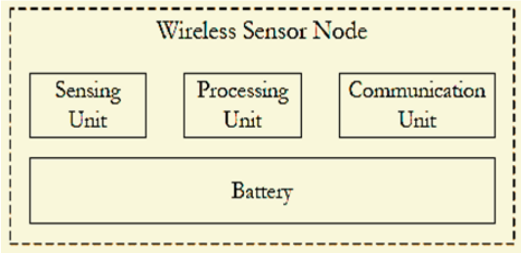

Figure 1: Components of a typical sensor node

Processing unit executes the required protocol in an autonomous manner. The communication unit is mainly concerned with the transmission and sensing of the information. The battery unit supplies all segments with the required amount of power. In many applications of the sensor networks, the nodes are inaccessible to replace the batteries where the battery life determines the lifetime of a sensor node. In wireless nodes more amount of energy is consumed for modulation and demodulation purposes. Hence the sensor nodes are battery constrained and having limited hardware resources.

In applications such as military or research organizations the security is a noteworthy issue of concern [2]. Various protocols were proposed over security for the confidentiality of the content of the information but without considering the contextual information into account. The contextual information acquired by the adversary through traffic pattern analysis can reveal the vital information such as location of the sensed objects, source node location and BS location. By knowing the physical location of the BS or the source node adversary can render false data or may alter the BS results in complete failure of the entire network [3]. Hence the location privacy of the BS is very essential and crucial.

The location privacy in WSNs plays a very important role and can be divided into source location privacy and receiver location privacy. The proposed paper is concentrated on the receiver location privacy with less energy dissipation suitable for battery constrained applications. A hybrid algorithm which provides routing and location privacy of the BS has been proposed.

Organization of the paper is as follows: The 1st section provided an introduction of wireless networks and privacy issues in WSN. Literature review is discussed in section 2. The 3rd section gives information about the methodology of proposed algorithm. The 4th section deals with the results and analysis. The 5th section comprises of conclusions derived with future scope.

2. Literature Review

Some of the important techniques presented on previous research works have been reviewed for developing a routing algorithm which can effectively camouflage BS location. The proposed paper mainly concentrates on the receiver location privacy.

WSN, a component of wide-spread computing, are being utilized on a vast scale to screen constant ecological status [4]. The sensors work under extraordinary energy imperatives and are composed by keeping an application in mind. Designing a wireless sensor is a great task and includes evaluating various distinctive parameters required by the objective application, which incorporates antenna range, memory, security, security, computational capacity, programming interface, size, power and applications.

Compared issues of cluster arrangement and choice between various protocols for information accumulation and transmission, focussed on two issues [5]. One of the issues is to find out number of clusters required to capably expend accessible sources for a sensor network and other is to choose number of cluster heads (CH's) to conceal sensor network more capably. A few clustering algorithms, for example, LEACH, DEEC and SEP have been investigated with the destinations of energy minimization, increased connectivity and route path and network life span.

Nikolaos *et al.,* [6] introduced a strategy to counter an attack by transforming the pattern of traffic in the WSN. The approach presented different duplicate sinks and deceptive packets with the goal that nodes other than the BS are resembled as the destination for all traffic. They used a heuristic approach to decide the most suitable deceptive sink count and arrangement for a network. Dynamic load-adjusting trees are shaped to recognize and adjust the topology to route packets to the duplicate sinks while expanding the network lifetime

Sangho *et al.,* [7] presented a steady rate broadcast scheme for guaranteeing the location protection of the BS. The scheme balanced traffic patterns of the sensor network to manage packet dropping and limited the routing data of every sensor node to manage node trading off. Additionally they reduced the overhead of the sensor network by proposing a forwarder-driven broadcast scheme that permitted effective various broadcasts with minimal buffer utilization. In scenarios other than BS anonymity techniques, [8] evaluated the network performance of MANET routing protocols with various models. However they failed to address the security mechanism for MANETs in military applications.

Shortest path algorithm for sensor network has been presented in [9]. The most limited route found by utilizing distance vector routing algorithm. The distance vector is the qualification of bellman-ford algorithm. Sensor nodes are made progressively to stay away from the circle development, malicious nodes and interruption assaults and furthermore enhanced the execution of distance vector by instating variable randomly.

The literature review provided information about different approaches which were presented in a view of privacy in sensor networks. The approaches like clustering, broadcasting and shortest path algorithm have given new ideas and paved the way for developing new hybrid algorithm.

3. Proposed Approach

A hybrid algorithm which provides sink node (BS) anonymity has been proposed in this paper. Anonymity of the BS is very important to protect from intruders. A hierarchical mechanism known as clustering has been used in the proposed algorithm [2]. Clustering facilitates the nodes with limited usage of energy, proper coverage with efficient transmission range. The Figure 2 illustrates the methodology of the proposed algorithm.

The initial step in the proposed algorithm is to deploy sensors and formation of clusters. Once the sensors nodes are deployed randomly (100x100 square meter area), the energy values are assigned for each sensor node. The transmission and reception energy costs are considered as 50 nJ. The BS energy is assumed to be 2 J and senor nodes having energy of 0.5 J. After deploying the sensor nodes the CH's are choosen randomly. The nodes are included in the clusters of a particular CH based on the sensing range i.e. 60 meter [2]. In the proposed approach, the sensing range and the transmission range are assumed to be the same. The distance matrix is calculated for each CH to sensor nodes, the nodes within the sensing or transmission range are included as a cluster member.

Based on the coordinate (i, j) of rectangular coordinate system the distance has been calculated and the calculation formula is

$$d(i,j) = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \quad (1)$$

The goal of the proposed algorithm is to guarantee that N sensor nodes in the network have same traffic pattern as that of the BS, let us consider SN as the set of sensor nodes, where i denotes the quantity of the sensor node.

$$SN = \{SN_{1,} SN_{2\,\ldots} SNi\} \quad (2)$$

The quantity of cluster heads are given by j and are denoted as

$$CH= \{CH_{1,} CH_{2\ldots} CHj\} \quad (3)$$

The quantity of cluster members are denoted by k and the sensor nodes are denoted as

$$CM= \{M_{1,} M_{2\ldots} M_k\}$$

$$SN \equiv CH \cup CM \text{ and } i = j + k \quad (4)$$

The clustering imposes a certain amount of energy burden on the CHs hence the cluster heads are made to rotate after a certain amount of messages sent.

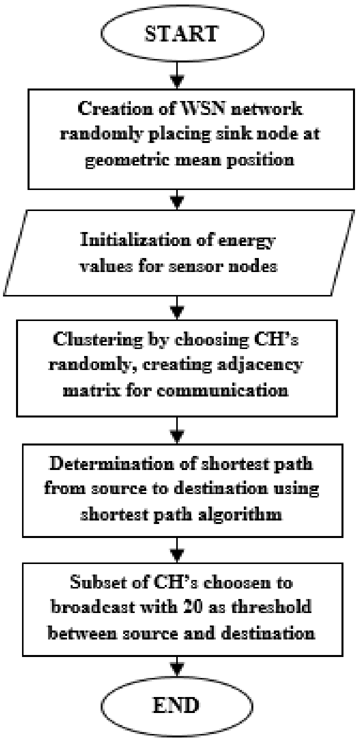
START
Creation of WSN network randomly placing sink node at geometric mean position
Initialization of energy values for sensor nodes
Clustering by choosing CH's randomly, creating adjacency matrix for communication
Determination of shortest path from source to destination using shortest path algorithm
Subset of CH's choosen to broadcast with 20 as threshold between source and destination
END

Figure 2: Flowchart of the proposed algorithm

The rotation of CH increases the overall life time of the sensor. While forwarding the data the CH can either forward the data to the next node or broadcast within its cluster. In the proposed algorithm the CHs are chosen to broadcast.

The BS CH broadcast the message it receives so that BS being a member receives the message.

$$B_{ch} = \{Bc_1, Bc_{2\ldots}\ B_{cm} \text{ and } B_{ch}\} Є\ CH \quad (5)$$

Using broadcasting of information to sensor nodes other than the BS, there can a situation where the other sensor nodes resemble the BS through means of traffic. Here, a threshold of twenty nodes has been set for broadcast. Once the number of node broadcast reaches 20, no additional broadcast cluster heads are chosen. Depending on the number of node broadcasts the anonymity factor of BS is calculated.

Anonymity factor is a parameter used to calculate the level of privacy w.r.t. location of the BS. The total number of node broadcast is given by β and anonymity factor is given by $AF_{topology}$:

$$\beta = \sum_{i=1}^{m} Number\ of\ node\ broadcast\ (bCi) \quad (6)$$

$$AF_{topology} = \frac{1}{average(\beta)} \quad (7)$$

In order to find the optimal location of the BS in the deployed area, the optimal geometric median location given in [10] is considered. The energy consumption of nodes is compared with the random position and center position of the BS as depicted in the Table I. The optimal geometric location i.e. (22.62, 51.06) meter is obtained. Average energy consumed is 0.01658 Joules for five different cases.

For the (50, 50) meter location, energy consumption is 0.0718 Joules and for (20, 60) meter location energy consumption is 0.0172 Joules. The geometric median location way showed minimal energy consumption compared to other random locations. Hence, location is computed using geometric median location for the BS.

Table I: Determining optimal BS location

Energy utilization at different position of BS (J)		
(20,60) (random)	**(50,50) (center)**	**(22.62,51.06) (median)**
0.0174	0.0171	0.0175
0.0165	0.0174	0.0162
0.0172	0.0169	0.0163
0.0176	0.0178	0.0163

4. Results and Analysis

For the analysis of results, four topologies of sensor network are generated. Topologies indicate different physical ad-hoc locations of the sensor nodes. The traffic has been routed over the sensor network at different traffic volumes such as: 5000, 10000, 15000 and 20000 volume of messages. Five trials have been conducted on each topology with different volumes of traffic.

A trial is known as the set of traffic volume routed over the sensor topology, where the topology remains the same but the role played by the each sensor node will change (whether a node is a CH or cluster member). In simulations, none of the nodes were allowed to die for simplicity purpose. From the simulations, the resulting anonymity level of the BS for the proposed algorithm has been evaluated. The Figure 3 illustrates the anonymity factor of trials for the topology-1.

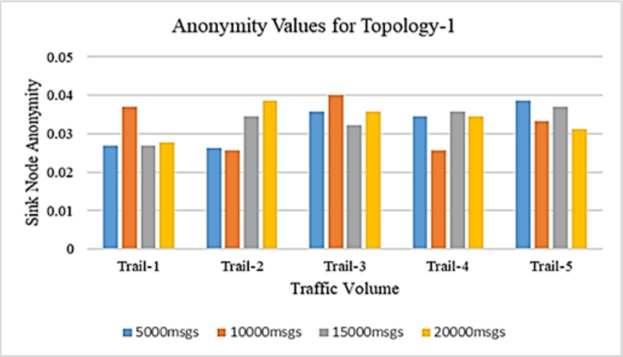

Figure 3: Anonymity value for the topology-1

The sink node anonymity values depicted in the Figure 3 demonstrates that the average anonymity values across the five trials for topology-1 are 0.0324, 0.0323, 0.0333 and 0.0345 respectively for 5000, 10000, 15000 and 20000 messages. The anonymity values are almost consistent and don't vary with the increase in the number of messages transmitted. Lower the anonymity value higher will be the security.

The energy is consumed during transmission, reception of data and for processing during the formation of clusters. The energy expended by the each sensor node is illustrated in Figure 4. For discussion, the energy consumed for 20000 messages has been analysed here. For the topology-1 an average energy of 16.9 mJ has been expended for the transmission of 20000 messages.

The Figure 5 depicts the anonymity factor of all trials obtained for the topology-2. In the topology-2 the location of the sensor nodes across the topology remains the same. For the different trials obtained the average anonymity factor as 0.0347, 0.0339, 0.0356 and 0.0376 respectively for 5000, 10000, 15000 and 20000 messages as depicted in the Figure 5. The anonymity value for the all the topology is almost consistent across the different trails. The anonymity value is not showing any trends when compared with the topology-1.

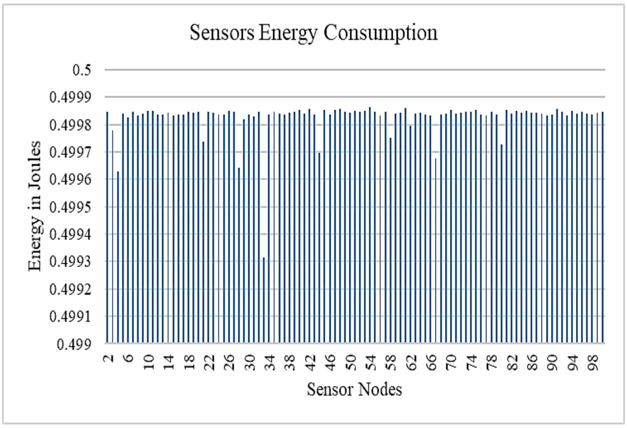

Figure 4: Energy expended by the sensor nodes for the topology-1

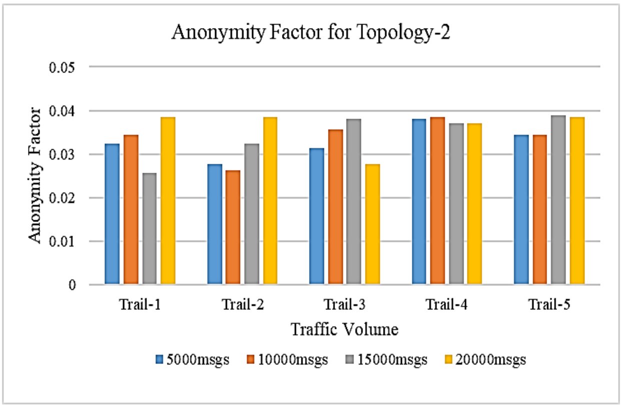

Figure 5: Anonymity factor for the topology-2

The Figure 6 demonstrates the energy utilization of the nodes for the transmission of 20000 messages in topology-2. For the transmission of 20000 messages an average energy of 16.6 mJ is expended by the sensor nodes. The results may vary slightly from topology to topology due to the different locations of the sensor nodes but the anonymity factor remained consistent.

The anonymity factor in the Figure 7 exemplifies that the anonymity factor decreases with the decrease in the number of CH's. This is due to the fact that as the number of CH's decreases the number of node members to be included in a particular cluster increases results in more number of node broadcasts. The number of node broadcasts is directly proportional to the anonymity factor.

The energy values in the Figure 8 demonstrate the variation in the energy consumption with respect to the different number of CH's. The energy consumption is decreasing as the number of CH's increases because the decrease in number of CH's results in more number of CM's in a particular cluster. Hence, the number of node broadcast increases causing more energy consumption.

The variation of energy consumption by the sensor nodes w.r.t. number of messages transmitted is illustrated in Figure 9. The results infers that the as the traffic volume increases the energy utilization by the nodes also increases. As the number of messages increases more energy will be consumed for transmission and reception. Increase in messages results in increased transmission and reception costs.

The comparison of anonymity factor with the various topologies is illustrated in Figure 10. The results exemplifies that the anonymity factor over the various topologies remains consistent. The anonymity of the BS is independent of the number of messages transmitted. Anonymity factor is consistent over different traffic volumes and in all cases it is < 0.037 (4 %). If the algorithm is dependent on messages transmitted it will add a major constraint for the practical implementation of the algorithm.

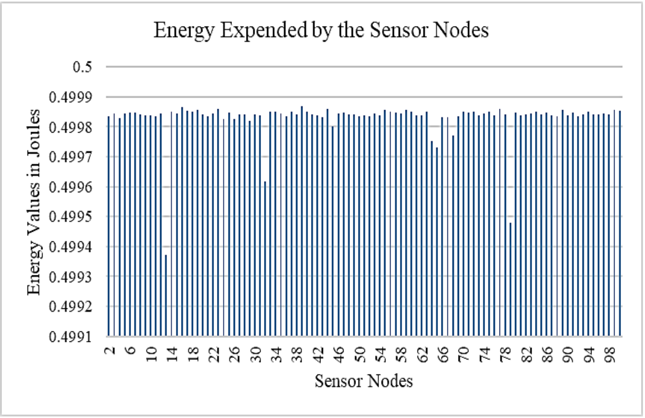

Figure 6: Energy consumed by the sensor nodes for the topology-2 (20,000 messages).

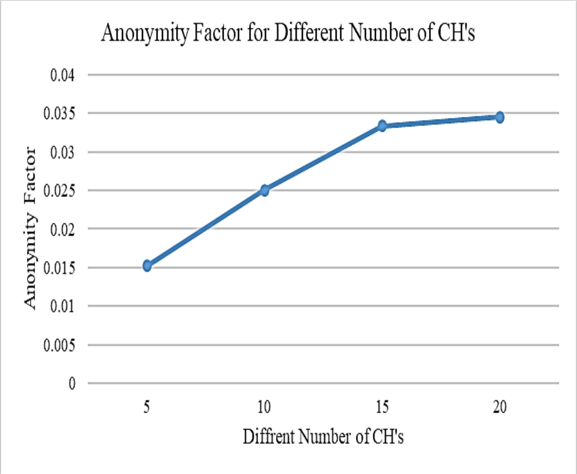

Figure 7: Anonymity factor for different number of CH's

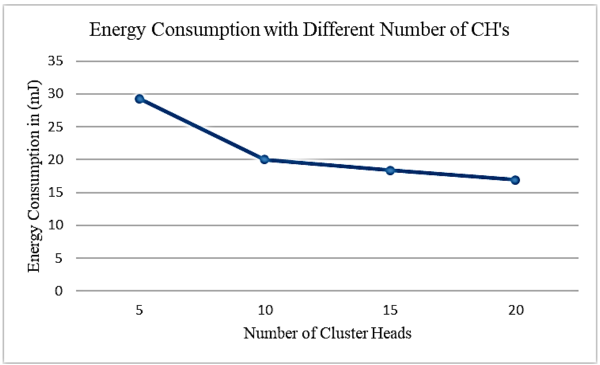

Figure 8: Energy consumption for different number of CH's

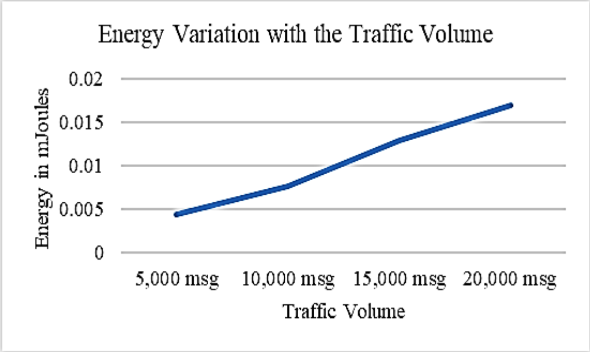

Figure 9: Energy consumption comparison for various topologies

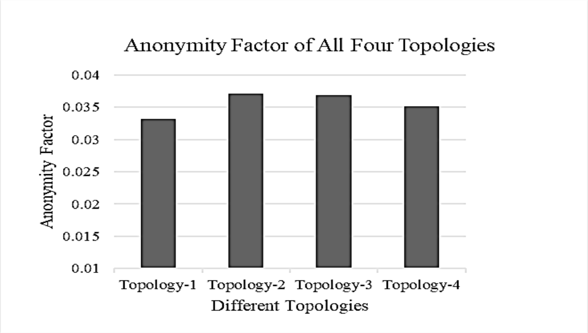

Figure 10: Comparison of anonymity factor for various topologies

The results discussed, exemplifies that the anonymity factor of the BS is not dependent on the quantity of messages transmitted. The energy utilization increases with the increase in quantity of messages. As the number of CH's decreases the anonymity factor decreases. Lesser the anonymity gives more security but the energy consumption increases since energy is the main criteria in the sensor networks. Hence, there is a trade-off for choosing optimal number of CH's for energy conservation.

5. Conclusions

WSNs are gaining their importance due to its huge applications in remote sensing and measuring. The acquired information by the sensor will be very crucial in fields such as military applications. Hence, the privacy of BS which acts as a collector of information is very important. The proposed algorithm for BS location privacy exhibited robust performance with the varying traffic volumes. The optimal location of the BS has obtained by less energy consumption. A global intruder is having less than 4 % chance of finding the actual location of the BS. The proposed algorithm effectively camouflages the location of the BS with the varying topologies and in different energy constraint conditions. As a future scope along with the modern network security techniques contextual privacy techniques can also be integrated.

References

[1] Ruben Rios del Pozo (2014), “Protecting Contextual Information in WSNs: Source- and Receiver-Location Privacy Solutions”, Ph.D. Thesis, Academic Project, University of Malaga.

[2] Sindhudhar K.L. and Premananda B.S. (2018), “Development of Hybrid Algorithm for Masquerading Sink Node Location in WSN” *in Proceedings of the International Conference on Emerging Research in Electronics, Computer Science and Technology*, ICERECT-2018, Mandya, India.

[3] Pallavi S., and Kanika S. (2016), “Improved Development of Energy Efficient Routing Algorithm for Privacy Preservation of Sink in WSN,” *International Research Journal of Engineering and Technology*, vol. 3, pp. 21-27.

[4] Vidyasagar Potdar, Atif Sharif and Elizabeth Chang (2009), “Wireless Sensor Networks: A Survey”, *in Proceedings of IEEE International Conference on Advanced Information Networking and Applications*, vol. 5, pp. 12-19.

[5] Fareed *et al*. (2012), “Optimal Number of Cluster Head Selection for Efficient Distribution of Sources”, *in Proceedings of 7th International Conference on Broadband, Wireless Computing, Communication and Applications*, vol. 3, pp. 21-28.

[6] N. Baroutis and M. Younis (2015), “Using Fake Sinks and Deceptive Relays to Boost Base-Station Anonymity in Wireless Sensor Network”, *in Proceedings of IEEE 40th International Conference on Local Computer Networks*, vol. 10, pp. 109-116.

[7] Sangho Lee, Jong K., and Yoonho K. (2009), “Preserving Source and Sink-location Privacy in Sensor Networks”, *International Journal on Computer Science and Information Systems*, vol. 2, pp. 16-21.

[8] Usha R., Premananda B.S., and Viswavardhan Reddy K. (2017), “Network Performance Analysis of MANET Routing Protocols with Various Mobility Models,” *in Proceedings of 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology*, vol. 6, pp. 511-515.

[9] Anu Dahiya and Vinit Kumar (2015), “Performance Measurement of Dijkstra using WSN: A Review”, *International Journal of Engineering, Applied and Management Sciences Paradigms*, vol. 12, pp. 741-753.

[10] Yahya Kord Tamandani, Mohammad Ubaidullah Bokhari and Mohammad Zarif Kord (2016), “Computing Geometric Median to Locate the Sink Node with the Aim of Extending the Lifetime of Wireless Sensor Networks”, *Journal of Egyptian Informatics, Cairo University*, vol. 4, pp. 1-7.

[11] L. Malathi, R.K. Gnanamurthy and Chandrasekaran (2015), “Energy Efficient Data Collection through Hybrid Unequal Clustering for Wireless Sensor Networks”, *Elsevier Journal on Computer and Electrical Engineering*, vol. 4, pp. 1-13.

[12] Alejandro (2015), “Privacy of Contextual Information in Wireless Sensor Networks,” Ph.D. Thesis, Department of Electrical and Computer Science, University of Arizona.