Anonymity based clustering routing protocol for Wireless Sensor Networks

Alaa M. Ghazy , Hala B. Nafea, and Fayez W. Zaki
Department of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Egypt

Abstract—The wireless sensor networks (WSN) is a distributed network so that it helps in gathering the information in a particular area. This region usually deployed in accessible places to provide solutions to a wide range of applications such as environmental, medical and structural monitoring. The central node used for gathering information is known as the sink node. Two major obstacles are associated with developing WSN. These are the anonymity of sink node and the restricted battery power of the network. This paper proposes an energy harvesting model for wireless Cluster Head sensor nodes. This model uses the super capacitor which provides more lifetime for the sensor node. Moreover, the proposed model can improve network security by implementing a protocol that can hide the location of the sink node. the raised profile of the sink node makes it possible to be as a high target for attack. MATLAB simulation and Multisum programs are used in simulation for the proposed model.

Index Terms— wireless sensor network, a sink node, energy harvesting..

1 INTRODUCTION

WSNs can be considered as ad-hoc networks where the sensors are located in data collection regions. It monitors an event or collects some physical information from its region of interest. Afterward, it processes the collected data using a tiny embedded processor for sending it to the collector of central data. The Source node is used to transmit data processed to the destination node called a sink node. The sink node anonymity (security) and restricted battery power of each sensor node are the most challenges facing the implementation of WSN. That's why clustering can be used to improve sink node anonymity and minimizing energy consumed, then increase lifetime by using energy harvesting. Energy harvesting is one of the sources of energy in WSNs is found to be most reliable [1]. Sensor Network can collect information in interest region then transmit it to the sink node. The received data is aggregated by the sink node and transferred to the control site. This paper aims at achieving sink node anonymity, in addition, to increase lifetime for wireless cluster head sensor nodes and overcome restricted battery power by using energy harvesting method. In recent days, Wireless sensor networks are divided into many areas of interest. Such as biomedical applications, habitat sensing, seismic monitoring, military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, process control, inventory management, distributed robotics, weather sensing, environment monitoring, and national border monitoring. A shortlist of sensor applications and usage are found in [2]. This paper focuses on military applications, where the site is of an unusual problem in WSNs. protecting the sink site may be achieved using security mechanisms like packet encryption and key management…., etc. For this reason, specific protocols must be included to skip the site of the sink node. There is another challenge in WSN, which is limiting battery power. So, this paper overcomes the limited battery power by using super capacitor in order to handle the current surge to increase lifetime for the network.

2 REVIEW OF RELATED WORK

To Protect and defend a WSN, one must understand the layering architecture of the network. The common network layering model is the open system interconnection (OSI) shown in Fig.1 [2]. Anonymity strategies usually implemented at the network layer, where it requires specific multi-hop routing protocols to be achieved. Two types of system anonymity are considered. These are source-location anonymity and sink location anonymity. The sink node anonymity may be achieved by four methods defined as1) Deceptive packets[4],2) Location Privacy Routing [5],3) Randomized Routing with Hidden Address[6]and4) K-Anonymity [7]. This paper used The K- Anonymity method to achieve the Sink node anonymity

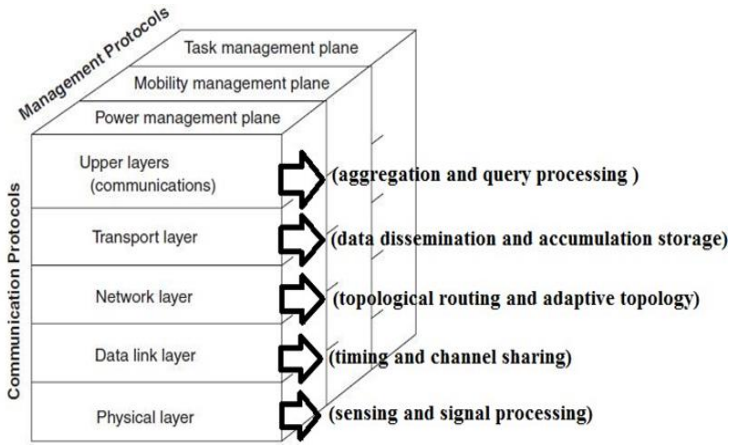

Fig.1: Sensor network protocol stack.[2]

3 SYSTEM MODEL

In the work performed here it is assumed that a square cell of area (100 x100) square meters, in which there are 100 nodes randomly distributed throughout the entire area. The sensor node has a data rate of one megabit per second and a packet length of eight-bit. The sink node is placed at a location of 25x75meters in two dimensions acting as a gateway between the multi-hop WSN and the wired or wireless infrastructure where the collected information is analyzed as shown in Fig.2

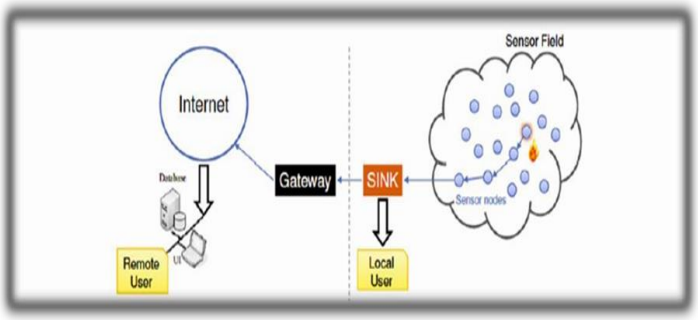

Fig.2 Agateway between WSN and the wired infrastructure.

The first step of the K-Anonymity method is shown in figure 3. Each sensor allows exchange of data with all nodes inside a fixed transmission zone of 40 meters in all directions. The power of all nodes is a fixed value of 0 .5 Watt, except the sink node. It has more power resource and processing to handle relaying of information and traffic volume outside the WSN. The transmitting and receiving communication power are both fixed at 5x 10-7W, and the processing power is5x10-8W. when the network is first deployed[9]. When the network is formed, it is necessary to make the collection of sensors can communicate to each other internally, and to another collection inside the WSN called (Clustering). The Clustering depends on the election of Cluster Head (CH) and the transmitting area for sensor nodes. Each sensor may be chosen as a CH with probability p except sink node, where it is always a cluster member in the WSN and never elected as CH. The first collection of cluster head can be generated by setting probability p=0.2. This value was experimentally determined so most of the cluster heads are elected in the first iteration, while the additional two iterations serve to make sure that no nodes are isolated in the WSN. At the end of the first iteration, nodes are classified into three categories first, node is cluster Head where they are responsible for their Cluster members second, node is within range of a Cluster Head (Cluster Member) third, node isn't a Cluster Head or within range of a Cluster Head as shown in Fig.4.

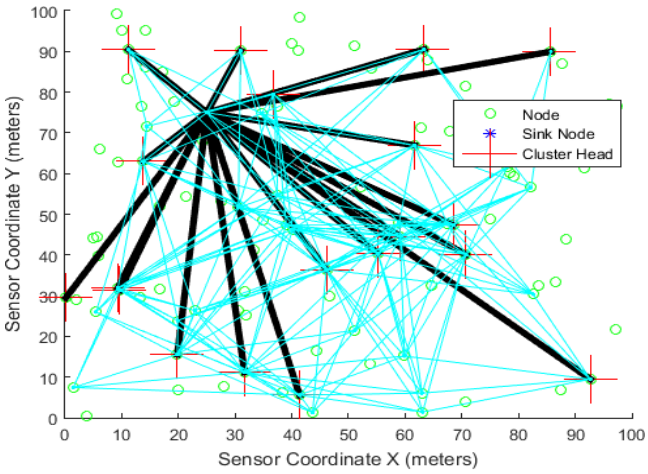

Fig. 4: First Iteration of WSN

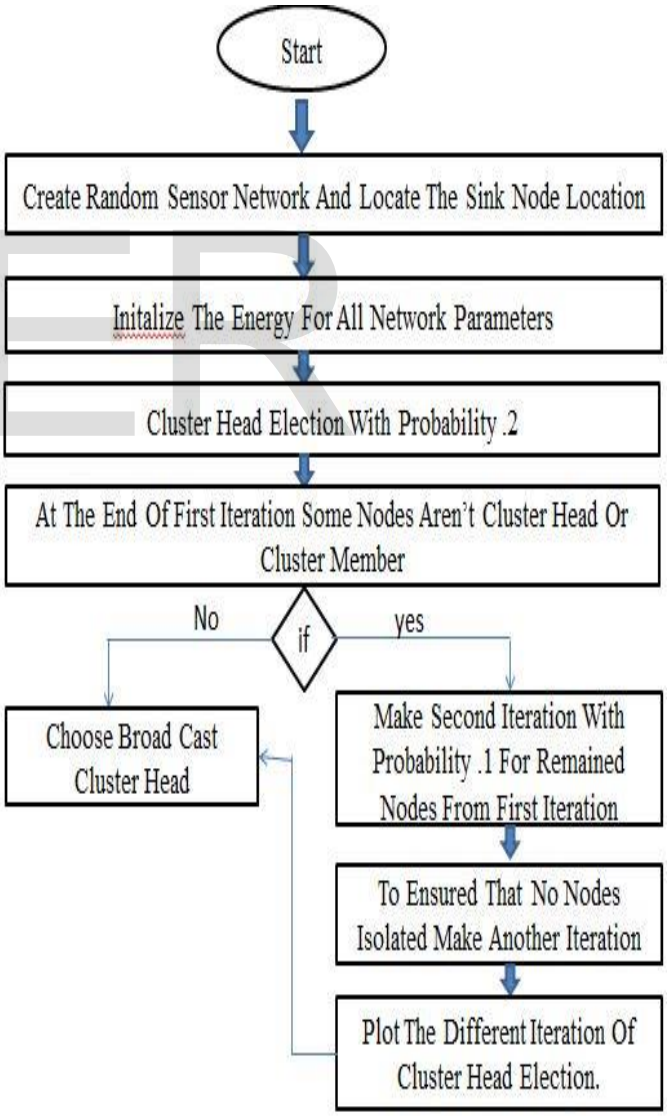

Fig .3: The flow chart of the first step of K-Anonymity

When the first iteration is finished, some nodes aren't elected to become cluster heads and didn't join with any clustering as a Cluster member. So, there is a need for a second Iteration for the remained nodes from the first iteration which are not chosen as cluster heads or within range of a cluster head by fixed probability of p=0.1. As a result of the second iteration more cluster head is formed, as shown in Fig. 5

Additional iterations may be performed to sure no nodes are remained isolated in the simulation area. The importance of additional iteration is the possibility of using another initial probability. The second iteration steps can be renewed as supplemental iterative steps if desired. At the end of the third iteration, one must be sure that all nodes have become either Cluster Head or Cluster Member and no nodes are isolated in the simulation area. After the third iteration, some nodes of cluster head are chosen to broadcast its data to each node in their cluster and to the next cluster head. As shown in Fig.6

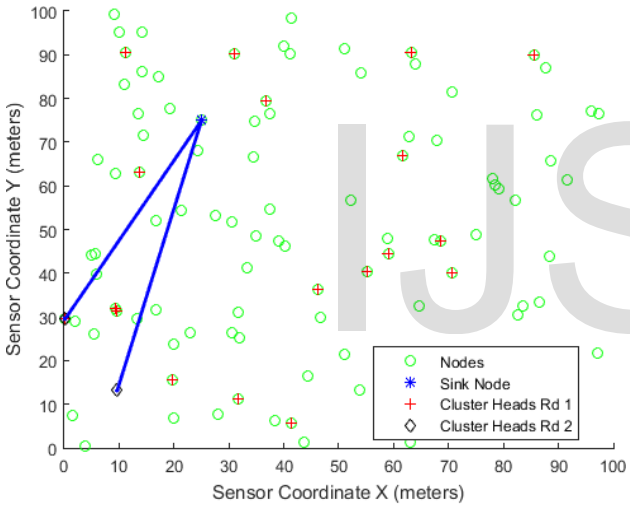

Fig.5: The Second Iteration

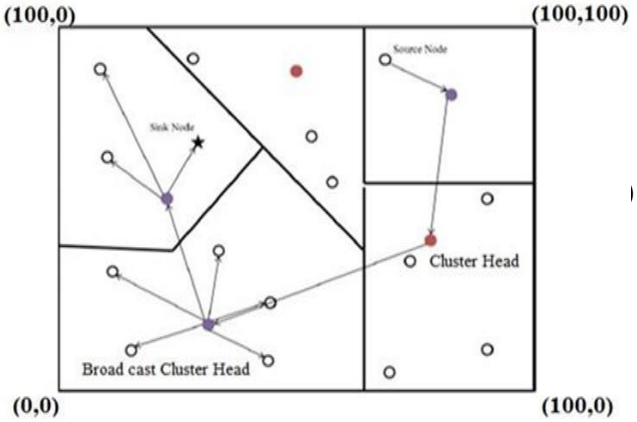

Fig.6: Dijkstra's Routing Algorithm and broadcast cluster head

The second step of the K-Anonymity method is shown in figure 7. Choosing a broadcast cluster head (BCCH) depends on the maximum remaining power for the CH and the number of cluster members of each cluster group

$$BCCH = \{bc1, bc2, ..., bcm\} \text{ and } BCCH \subseteq CH \quad (1)$$

Where bc1 ,bc2,……..bcm are cluster heads with maximum power remaining, CH are the cluster heads.

A threshold of nodes must be chosen to broadcast the received data into their cluster to ensure a desired level of anonymity required. The number of nodes that broadcast its date received is correlated to the anonymity of the sink node as shown in equation 3. The sink node cluster head(SNCH) always broadcast the received date to their members these members include sink node, via broadcasting the received data to nodes other than the sink node. This makes a situation in which multiple nodes will be like the sink node. These multiple nodes will act like sink node. Attacker can't use traffic volume to set the location of the sink node, therefore, the attacking cost of each node will be higher than attacking one node. The importance of the cluster head is to calculate routes from the source node to the sink node. The cluster head uses Dijkstra's Routing Algorithm [8],[9] to establish routing paths after BroadCast Cluster Head(BCCH) is chosen. Dijkstra Algorithm is used to find the shortest path to the sink node and the path which has low cost from source to destination using Euclidian distance theory

$$Dis(CH_1,CH_2)=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2} \quad (2)$$

Where (x1,y1),(x2,y2) are the position of CH1 and CH2 respectively and Dis(CH1, CH2) is the distance between the two cluster heads. It is considered as the cost between two CHs. The most power-efficient route is the resulting route through the WSN. When any node sense data it transmits to the nearest cluster head in the same cluster then the cluster head are responsible for routing this data to another cluster head untile it reach the sink node. The role of Cluster Head (CH) should be rotated in the WSN to make anonymity and load balancing. The CHs are rotated if Cluster Head Consume 1% of its initial power value, Eo/100 where Eo=0.5 w for all node, or the sink node cluster head (SNCH) receives 1000 messages. The rotating of CHs increase the sink node privacy. This situation makes the sink node location hard to be found. Anonymity factor of sink node is defined as AF :

$$AF = (1/\beta) \quad (3)$$

Where β is The total number of nodes broadcast to it which can be calculated as :

$$\beta = \sum_{i=1}^{n} members\ (bc_i) \quad (4)$$

Where $members_{bc_i}$ are the member nodes of each cluster heads with maximum power remaining

$$AF_{topolgy} = 1/average\beta \quad (5)$$

All sensor nodes which are classified into source node can process the data in addition to transmit this data to Cluster Head, which looking for the shortest path to reach the Sink Node Cluster Head. The power consumption for transmitting one message through the network is given by[9].

$$ER\ CM = ECM - EP - ET \quad (6)$$

Where ER CM is the remaining power of cluster head member, ECM is the power of cluster member, EP is the power of processing and ET is the power of transmitting. All sensor nodes classified as Cluster Head can receive data from source nodes in addition to looking for the shortest path to reach the SNCH through network is given by[9].

$$ERCH = ECH - ET - EP - ER \quad (7)$$

Where ERCH is the remaining power of cluster head, ECH is the power of cluster head, and ER is the power of receiving. All sensor nodes classified into broadcast cluster head can process data and receive data from other nodes then transmit this data to its members through the network. The remaining power of broadcast cluster head is given by[9].

$$ERBCCH = ECH - ER - EP - (ET \times MCH) \quad (8)$$

Where E_{RBCCH} is the remaining power of broadcast cluster head and MCH is the member of cluster head.

4 PROPOSED ENERGY HARVESTING MODEL

By choosing the most efficient path that consumes minimum power by the WSN to achieve anonymity of the sink node, there will be an urgent need for energy harvesting scheme using a super capacitor to get rid of the battery and increase the lifetime of sensor[10],[11]. The energy harvesting system consists of two stages defined as energy collection stage and energy storage stage. The energy collection part consists of a solar array, and the energy storage part consists of super capacitor device as shown in Fig. 8.

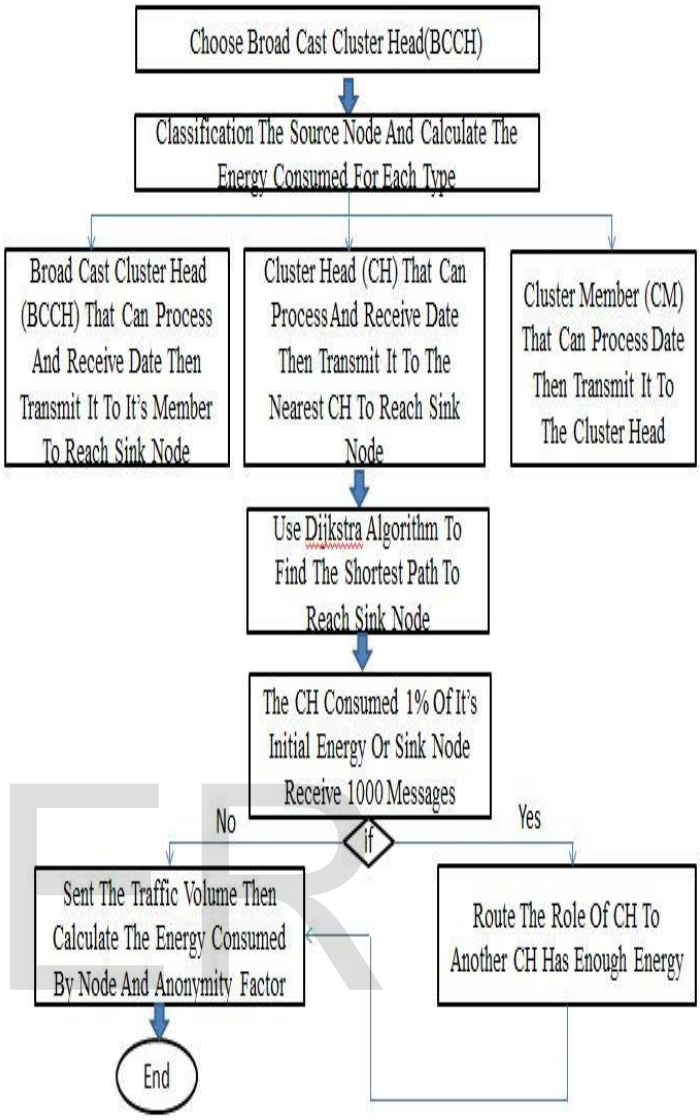

Fig.7: The flow chart of the second step of K-Anonymity

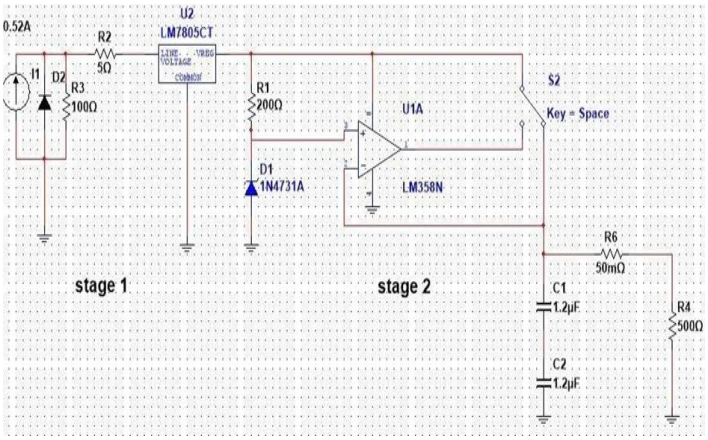

Fig. 8: Modeling of energy harvesting in the wireless sensor node.

The energy collection stage is subdivided into two basic parts. The first part contains the current source which represents the current produced from electron-hole pair recombination due to solar radiation. The diode represents the solar cell's P-N junction characteristics. The solar panel produces current and voltage of 0.52A and 5.82V respectively. R3 is the parallel resistance of the semiconductor materials used to consume little amount of current flow, and diode current. R2 is the series resistance of the metals used in the solar cell leads and contacts. Typically, R3>> R2. The second part is the voltage regulator LM7805. It is used to overvoltage protection of the super capacitor. In the circuit used here, a shunt regulator is considered. It is usually used because of its simplicity and low cost. The energy storage stage contains the Charging Circuit which uses switch and charge controller operational amplifier LM358. The switch used to charge and discharge the super capacitors. LM358 is configured as a comparator that feeds super capacitors and the load resistor. The super capacitors feeds the wireless sensor node and it is used to serve as a power supply source to the sensor node that can operate from 3volt to 5volt. Inthis model, two series capacitor are used each one has a capacity of 1.2 µfarad and different values of load resistor to reach the maximum time of discharge as shown in figure 8. The values of the load resistors are 150, 250, 350, 450 and 537Ω. When the switch is closed, the super capacitor begins to charge until 5voltage. At the moment of an open switch, the capacitor starts to discharge according to the equation.

$$Vo(t) = Vx\, e^{-t/rc} \qquad (9)$$

Where Vo(t) is a function of discharge time, Vx is the voltage on the capacitor when it starts discharge (5V), t is the time of discharge, r is the load resistor and c is the capacity of the capacitor. Fig.8 illustrates the effect of different values of load resistor on the discharge time of the super capacitor. Moreover, it can be noticed in fig.8,that with load resistor R=537Ω this provides the largest discharging time, while with load resistor R=450Ω, it has discharge time less than using load resistor R=537Ω and greater than load resistor R=350Ω. On the other hand, the load resistor R=150Ω results the smallest discharge time. Therefore, the most effective discharge time is obtained when the load resistance R=537Ω. This modeling of energy harvesting using super capacitor allows increasing traffic volume that can be transmitted through the network by one to ten than the conventional method. In addition, to decrease the average anonymity factor from .04 by using conventional method to 0.02 using energy harvesting model despite the average power consumption has not changed significantly.

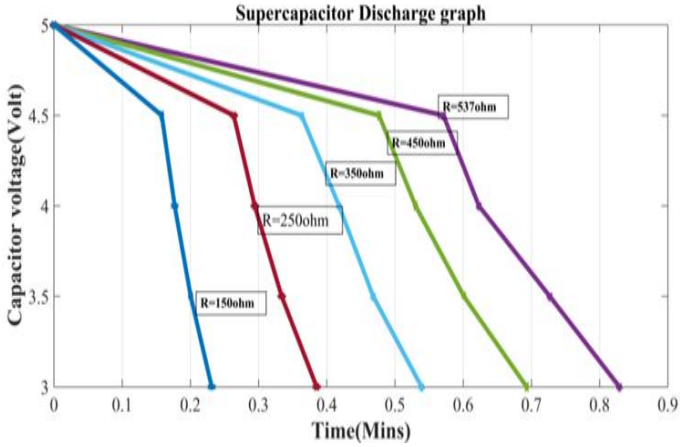

Fig. 9:Discharge capacitor the different load resistor

A simulation experiment is conducted to ensure the effectiveness of the energy harvesting scheme upon the sensor lifetime and the results are shown in table3

TABLE3: RESULTS OF DISCHARGE VOLTAGE MODELING

The voltage across the capacitor(V) after a certain time of discharge	Discharge duration of super capacitor (minutes)
5	0
4.5	0.571
4	0.623
3.5	0.727
3	0.829

5. SIMULATION RESULT

In the simulation study reported here two traffic scenarios were .In the first scenario has four different volumes from 5000 to 20000 messages without energy harvesting model. In the second scenario has four different volumes 312500,375000,437500 and 500000 messages with

energy harvesting scheme applied .using traffic volume5000,10000,15000and 20000messages generated five trials, ten trials, fifteen trials, and twenty trials through WSN respectively. The first five trials from all traffic volume are considered as case study in this simulation .The average power consumed by each nodes in first scenario were shown in figure 10

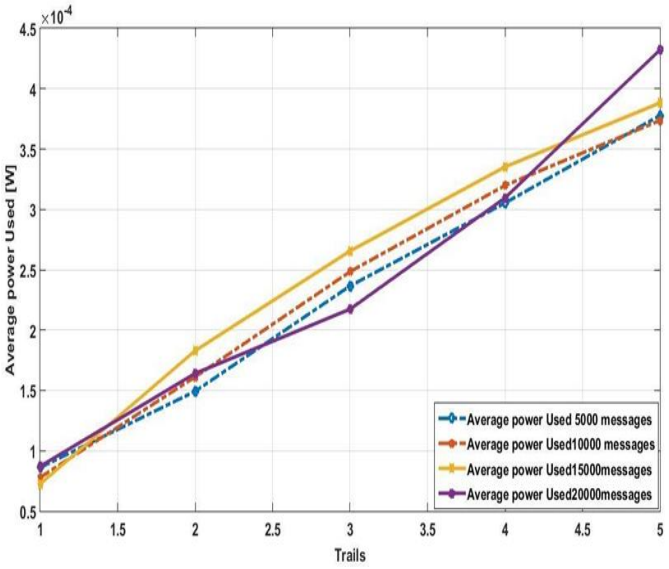

Figure 10 .Average Power Used by the node in (first scenario

In fig.10 can be noticed that results were very homogeneous to each other. The average Power used by the nodes through the five trials increases with the increase in traffic volume , but the average power consumed through 15000 messages is greater than 20000 messages in trail 2, but no points being large outliers. by taking the average value of average power consumed through the five trails were 8.1037x10-5 , 1.6442x10-4, 2.59455x10-4, 3.3077x10-4 and 4.061125x10-4 respectively by difference 3.5x10-4.

In the second scenario(energy harvesting model), It is found that the CHs are routed if Cluster Head power reach to 0.4031w or the sink node cluster head (SNCH) receives 62500 messages instead of 0.4989w and 1000 messages in first scenario(without energy harvesting). The average power used were shown in figure11

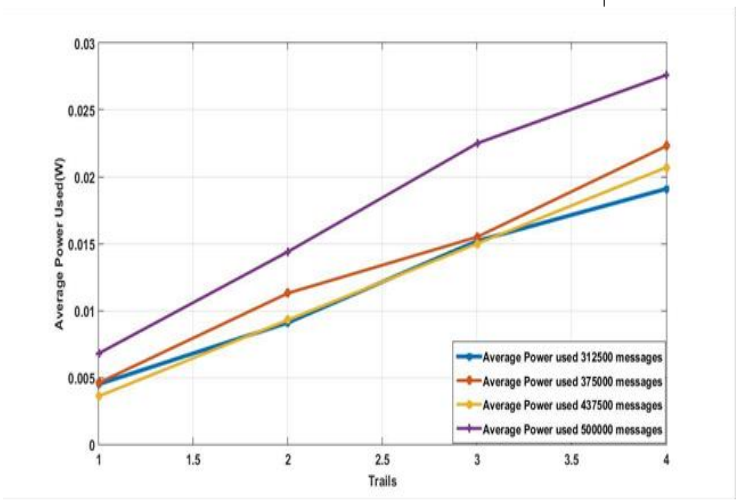

Figure 11 .Average Power Used by the node in (second scenario)

In fig 11 can be noticed that the maximum value of average power used was 0.0276 through using traffic volume 500000 and the minimum value was 0.0036 through using traffic volume 437500 by taking the average value of average power used for trails were 4.875x10-3, 0.011025,0.0169875and 0.022425 respectively by difference 0.01755.In energy harvesting model, the average power used does not increase in large scale although increase the traffic volume .In the view of the maximum energy used through the WSN without using energy harvesting model these results were shown in figure 12.

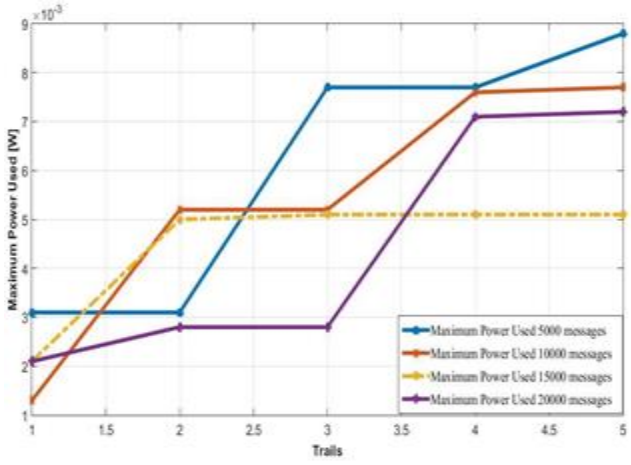

Figure 12. Max power Used in the (first scenario)

In fig 12 can be noticed that maximum power used by a node varies more than average power used. It is difficult to predict it as there are a lot of roles are chosen random creating more difference. The average value of max power used for trails were 2.15x10-3, 4.025x10-3, 5.2x10-3,6.875x10-3 and 7.2x10-3 respectively by difference 5.05x 10-3.

After used energy harvesting model in all different traffic volumes through the wireless sensor network. The maximum power used were shown in figure 13.

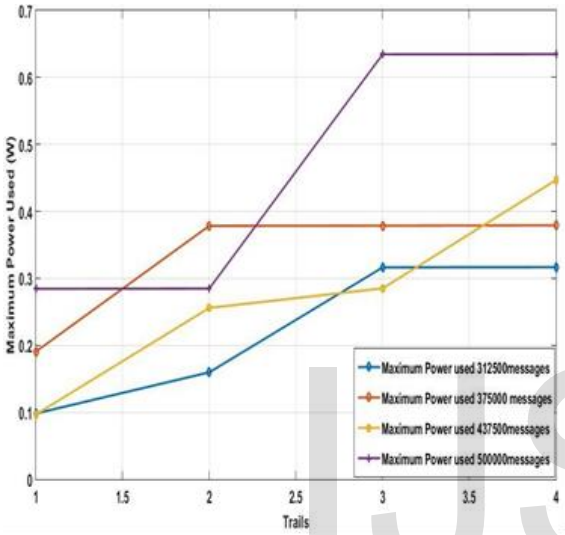

Figure 13. Max Power Used in the (second scenario)

In fig 13 can be noticed that the maximum and minimum value of maximum power used were 0.06348 and 0.0969 through using traffic volume 500000 and 437500 respectively by difference 0.5379.

by taking the average value of maximum power consumed were0 .167575,0.269725,0.4037and 0.4444 respectively by difference 0.276825. On the other hand the minimum energy used using first scenario were shown in figure 14.

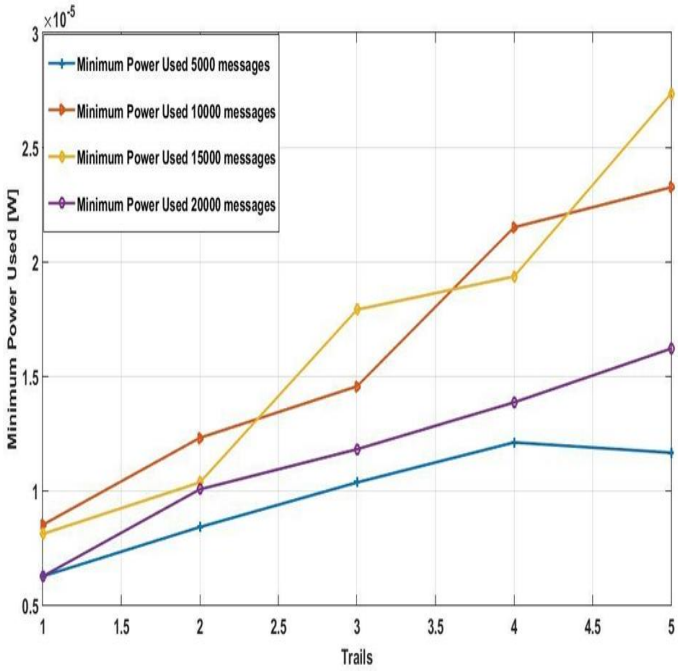

Figure 14. Minimum Power Used in (first scenario)

In fig 14 can be noticed that the minimum power used by a node increases as the traffic volume increase from 5000 messages to 20000 messages in all trails .by taking the average value of minimum power consumed for trails were 7.275x10-6, 1.0275x10-5,

1.365x10-5, 1.67x10-5 and 1.96125x10-5 respectively with difference 1.23375x10-5.

After used energy harvesting model using super capacitor through WSN found that the minimum power used as shown in figure 15.

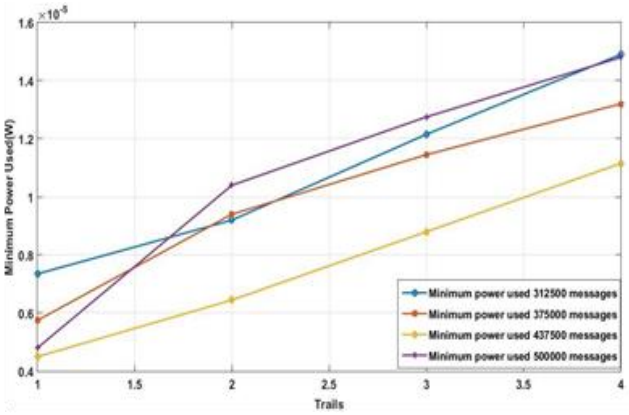

Figure 15. Minimum Power Used in(second scenario)

In fig 15 can be noticed that the maximum and minimum value of minimum power consumed were 1.49x10-5 and 4.5x10-6 using the traffic volume 312500 messages and 437500 messages respectively .by taking the average value of minimum power consumed were 7.4187x10-6, 1.143125x10-5, 1.12875x10-5 and 1.35125x10-5 respectively with difference 6.0938x10-6.

At the first scenario found that the anonymity factor (1/β) was less than 4 %.This is mean that an adversary conduct the traffic analysis less than four percent in finding chance of the sink node on the first guess. These results were shown in figure16.

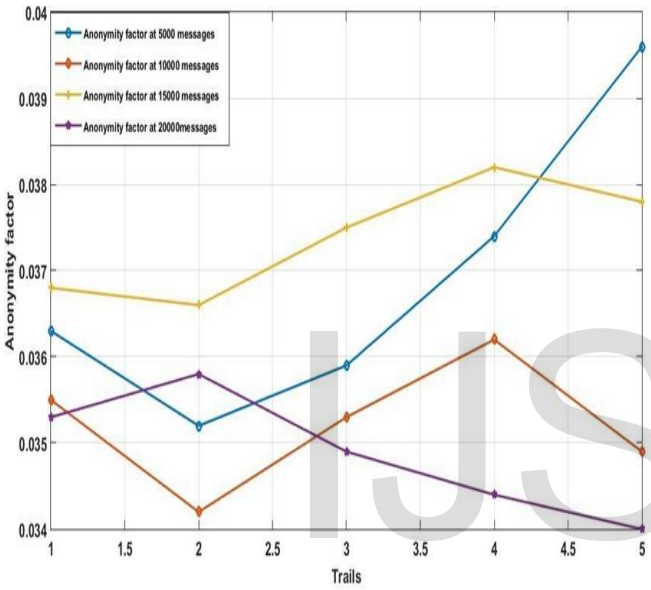

Figure 16. Anonymity factor in(first scenario) without energy harvesting

After using energy harvesting model using super capacitor through the different traffic volumes found that the anonymity factor (1/β) is decreased, this decrease an adversary opportunity to find the sink node on the first guess. These results were shown in figure 17.

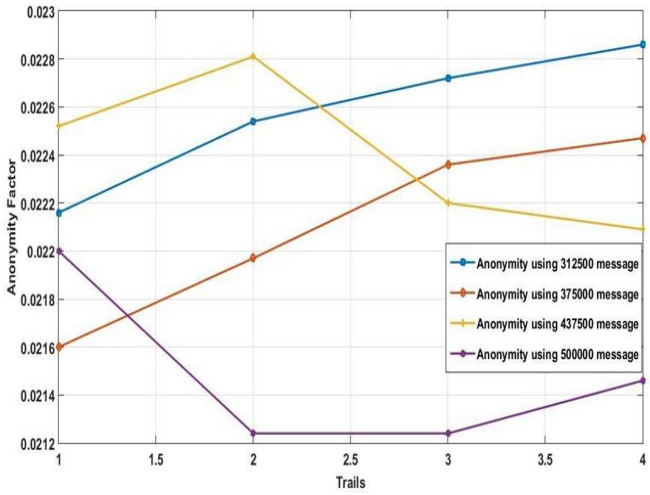

Figure 17. Anonymity factor in (second scenario) using energy harvesting

6 CONCLUSIONS AND FUTURE WORK

In this paper, Dijkstra's routing algorithm a clustering algorithm for WSN were adopted and implemented to maintain sink node anonymity. Moreover, an energy harvesting scheme was also introduced to increase the network life time. In the study it was found that the factor of anonymity is independent of the traffic volume .The average anonymity across the five trail in all traffic volume was 0.03609. So, the adversary conduct the traffic analysis of deployed WSN has less than four percent in finding chance of the sink node on the first guess. Using energy harvesting with super capacitor at all traffic volumes, it is found that the average anonymity was 0.0217. These results are promising because of decreasing the chance of finding the sink node on the first guess. Also, energy harvesting provides power independence to wireless sensor devices without the use of expensive wires, or batteries that will need replacement every now and then to increase the performance of life time of wireless sensor network. It is found also that the cluster head routes if it consumes one percent of its initial value or sink node receives 1000 messages. After using super capacitor the cluster head rotate if the power of cluster head reach to 0.4031W, or sink node receives 62500 messages

References

[1]Babayo, A. A., Anisi, M. H., & Ali, I. A review on energy management schemes in energy harvesting wireless sensor networks. *Renewable and Sustainable Energy Reviews*, *76*, 1176-1184(2017).

[2]Akkaya, K., & Younis, M. A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, *3*(3), 325-349(2005).

[3]Tang, C., & Raghavendra, C. S. Compression techniques for wireless sensor networks. In *Wireless sensor networks* (pp. 207-231). Springer, Boston, MA.(2004).

[4]Ebrahimi, Y., & Younis, M. Using deceptive packets to increase base-station anonymity in wireless sensor network. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International* (pp. 842-847). IEEE.(2011).

[5]Jian, Y., Chen, S., Zhang, Z., & Zhang, L. A novel scheme for protecting receiver's location privacy in wireless sensor networks. *IEEE Transactions on Wireless Communications*, *7*(10).(2008).

[6]Ngai, E. C. H. On providing sink anonymity for sensor networks. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly* (pp. 269-273). ACM.(2009).

[7]Chai, G., Xu, M., Xu, W., & Lin, Z. Enhancing sink-location privacy in wireless sensor networks through k-anonymity. *International Journal of Distributed Sensor Networks*, *8*(4), 648058.(2012).

[8]Hart, C. Graph Theory Topics in Computer Networking. *University of Houston-Downtown, Department Computer and Mathematical Sciences, Senior Project*.(2013).

[9]Callanan, A. F. *Achieving sink node anonymity under energy constraints in Wireless Sensor Networks*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.(2014).

[10] Habibu, H., Zungeru, A. M., Susan, A. A., & Gerald, I. Energy harvesting wireless sensor networks: Design and modeling. *International Journal of Wireless & Mobile Networks*, *6*(5), 17.(2014).

[11] Parks, A. N., Sample, A. P., Zhao, Y., & Smith, J. R. A wireless sensing platform utilizing ambient RF energy. In *Power Amplifiers for Wireless and Radio Applications (PAWR), 2013 IEEE Topical Conference on* (pp. 160-162)(2013).