Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 48 (4) 809-814 (2016)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

A Hybrid Energy Efficient Technique to Improve Source Location Privacy in Wireless Sensor Networks

H. JAVED, S. ULLAH, H. FARMAN, M. ZESHAN, S. KHAN*

Department of Computer Science, University of Peshawar, Pakistan

Received 8th April 2016 and Revised 29th September 2016

Abstract- Wireless sensor networks are prone to security issues such as privacy. Lately a lot of attention has been given to privacy by the researchers due to threats from attacker to access important information. Similarly Wireless Sensor Network (WSN) deployed for object monitoring or tracking purposes are prone to be attacked by an adversary by locating the source node. Which highlights an important Privacy issue called source location Privacy. Different techniques are proposed for preserving Source Location Privacy such as introducing dummy traffic using Phantom Nodes or having multiple fake sources which improves privacy, but at the cost of high energy consumption, and end-to-end latency. This paper proposes a hybrid approach by combining multipath and phantom nodes, avoiding fake packets or fake sources, which improve privacy, energy consumption, and end-to-end latency. In addition Analytic Hierarchal Process (AHP) method is used for the phantom node selection process. AHP is a several criterion choice building process in which large problem splits into smaller sub problems (factors). The simulation outcome confirms that the proposed technique overwhelmed the deficiencies in existing techniques and improves source location privacy, end-to-end latency and reduces energy consumption.

Keywords: Wireless Sensor Networks, Event Detection, Privacy, Analytical Hierarchy Process, Source Location Privacy

1. INTRODUCTION

In the last decade, developments in the area of wireless communication technologies, Micro-Electro-Mechanical-Systems (MEMS), and distributed computing jointly brought the occurrence of wireless sensor networks. Which is comprised of tiny devices having limited resources such as low power batteries (Akyildiz *et. al.* 2002, Vidhya and Kumar. 2015), short communication range (Navarro *et. al.* 2014) and low memory storage (Hill. 2003). Even with constraints on resources wireless sensor networks are used in different application scenarios ranging from military (Kamat *et. al.* 2005), health care and object monitoring applications (Long *et. al.* 2014, Chen and Lou. 2015).

In object tracking or monitoring application scenarios, WSN is deployed to monitor presence of an object. In this case object can be anything such as human, enemy soldier or an endangered animal (Kamat *et. al.* 2005, Ozturk *et. al.* 2004). For this type of application where sensor nodes senses an object and sends information to the base station (Sink node) (Hill. 2003, Rios *et. al.* 2015) through multi-hop communication. Consider an application scenario called panda hunter game introduced by (Kamat *et. al.* 2005, Ozturk *et. al.* 2004). In Panda Hunter Game scenario wireless sensor network is established to monitor the presence of panda. Sensor node which senses the Panda becomes a source node, and sends information related to the panda to base station by using multi-hop communication. There is also an attacker whose aim is to find location of the Panda by analyzing traffic flow from source to Sink and harm the panda. In the above mentioned application scenario source node location privacy becomes an important issue because an attacker can locate the target by locating source node. Kamat and his coworker have a famous privacy preservation technique, called phantom routing (Kamat *et. al.*2005). Phantom routing technique uses phantom nodes to mislead the adversary from the source node. Emergence of phantom routing was followed by many techniques but Long and Chen have introduced their state-of-the-art techniques i.e. tree-based diversionary tree-routing and forward random walk which are considered to be more effective in terms of energy consumption, privacy, and end-to-end latency as compared to Phantom Routing (Long *et. al.* 2014, Chen and Lou. 2015).

Existing techniques results in high energy consumption, and high end-to-end latency due to flooding of fake packets from Phantom node to Sink node and excessive computation at route selection,

+Correspondence Author Email: SIFAT. Ullah, sifatmstudent@upesh.edu.pk
*Department of Electrical Engineering, University of Engineering and Technology, Peshawar, Pakistan

therefore this research work proposes a technique to reduce energy consumption, enhance source location privacy and improve end-to-end latency. The proposed technique will have more than one phantom node, where each phantom node will further have multiple routes to the Sink. Every time one route will be selected for forwarding a packet in order to hide source node location from adversary.

This paper is structured as section II comprises literature review and section III is dedicated to source location privacy. In section IV the proposed technique is presented. Section V illustrates performance evaluation and results. The last section concludes this paper and discusses future directions.

2. SOURCE NODE LOCATION PRIVACY

In this section, major goal of the proposed scheme is presented which is to accomplish a high safety period by a low end-to-end latency and reduced energy consumption. Consider a common scenario introduced by called "Panda Hunter Game" (Kamat *et. al.* 2005) shown in Fig. 1. Panda hunter game comprises of a source node, sensor nodes, phantom nodes and a Sink. Source Node senses activities of the panda and generates events to the Sink node by forwarding these events through intermediate nodes. This paper modified this scenario by using two phantom nodes which have multiple routes to the Sink. There is an adversary as well who is trying to break source node location privacy to locate the target with the final aim of killing the target. All the sensor nodes which are used in this monitoring game have same resources, such as equal battery power, equal capacity, equal sensing range denoted as R, similar communication and computation abilities. Along with sensor nodes there is Sink node which has higher resources as compared to the sensor nodes. After deployment of WSN once a Source Node detects the panda it starts flooding a route request packet to create routes from Source Node to Phantom Node and from Phantom Node to the Sink node. Upon receiving route request packet each node adds its energy level, hop count from Source Node to Phantom Node, and from Phantom Node to sink node. After creation of Phantom Nodes and multiple routes then Source Node will start forwarding events generated at the Source Node to the Sink Node.

In this paper an adversary is also considered which is equipped with a spectrum analyzer to locate the immediate sender of the packet (Kamat *et. al.* 2005, Ozturk *et. al.* 2004, Conti *et. al.* 2013). There are two types of adversaries which threaten contextual privacy: Local Adversaries, and Global Adversaries (Li *et. al.* 2009). Local Adversary can only monitor packets transmitted in a network locally while global adversary is capable of monitoring the whole network. Local adversaries use backtracking to trace the packets transmitted while the global adversary can eavesdrop the whole network packets. The adversary has the following characteristics proposed by (Kamat *et. al.* 2005, Long *et. al.* 2014, Chen and Lou. 2015). In this Scenario local adversary is considered to be the attacker equipped with resources higher than sensor nodes such as have large memory to store the tracing information, higher energy and a spectrum analyzer to locate the immediate sender of the packet transmitted (Conti *et. al.* 2013, Li *et. al.* 2009).

1. Adversary can move back and forth in the network upon detecting some communication in the network.
2. Attacker cannot see the inside of the packet as it is encoded with some security technique.
3. An adversary cannot disturb the normal working of the network by destroying or compromising a sensor node.
4. The speed of a packet transmitted in the network is considered to be higher than the speed of movement of the adversary therefore an adversary can only trace a packet to only one hop.
5. Adversary have enough knowledge about the routing strategy used by the proposed technique, i.e. Kirchhoff's Principle (Trappe *et. al.* 2007).

An adversary stays near the Sink node and monitors communication from intermediate sensor nodes to the Sink node. When an adversary detects some transmission from intermediate node to the Sink then it moves toward that immediate sender of the packet using backtracking. An adversary stays on that intermediate sensor node until it detects transmission of packets to this sensor node or for a specific time, and then if there is no communication for that specific time then adversary comes back to the Sink node. Adversary can store the location of the node it visited previously and if it moves to the other sensor node that information is updated with the location of the newly visited node.

3. PROPOSED TECHNIQUE

In panda hunter game, presence of a target animal means there is a threat from the attacker/adversary hence source node location becomes important and need to be protected. A routing protocol is required be implemented for this purpose which can hide source node location from the attacker.

This section discusses the proposed technique in details. The technique proposed in this paper has a source node, intermediate sensor nodes, phantom node

and a Sink as shown in **(Fig 1)**. Source node on detection of the adversary starts creating multiple routes to phantom node by broadcasting a route request packet. Upon receiving this packet intermediate nodes will add their energy level, hop count from source node to phantom node, and hop count from phantom node to the Sink. There will be more than one phantom node with multiple routes from it to the sink node. Using these multiple routes Source Node will forward packets to the Sink which will have information about different actions and activities of the target. These multiple routes may include short or long routes but selection of routes is random from source to phantom node and then to the Sink.

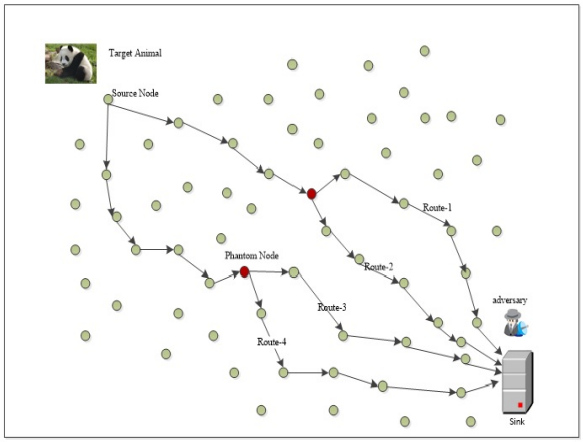


Fig. 1. Proposed Technique Scenario

Algorithm1: Hybrid Phantom Routing

Routes creation and nodes selection from source to Phantom node

- Source node ns broadcast route_req packet.
- Intermediate node ni receives route_req packet update, Energy=Ei, distance=ds.
- Select Phantom node using AHP method.
- Build multiple routes from source node ns to phantom node np
- Build multiple routes from Phantom node np to sink node.

Routes creation and nodes selection from Phantom node to Sink node

- Initialization: next_hop = null
- Build multiple routes from source node ns to phantom node np using algorithm 1.
- Build multiple routes from Phantom node np to sink node ns
- **While** receive a message m **do**
- Randomly select a route in multiple routes.
- Forward the receive packet to next_hop.
- **end while**

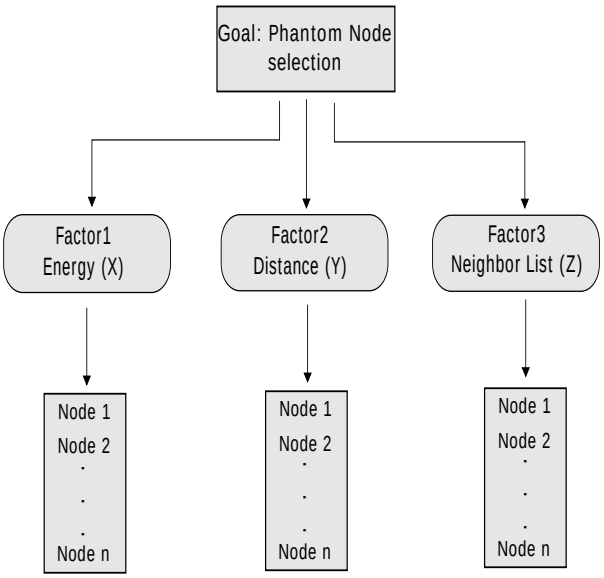


Fig. 2. AHP method for Phantom Node Selection

In the proposed technique phantom node is selected on basis of three metrics or factors, which are energy, distance from Source or Sink node in terms of hop count, neighbor list as shown in Fig 2. These factors can be defined as:

Energy(X)

Energy can be defined as the remaining energy of the sensor node as primary energy of entirely the sensor nodes except Sink node is same.

Distance(Y)

Distance can be measured in terms of hop count from the source node or Sink node because if phantom node is much closer to source node then privacy will breach while if it's closer to Sink node then adversary can easily locate it, therefore phantom node should be located at some hop distance from Sink and source.

Neighbor list (Z)

Neighbor list contains sensor nodes which are closer to a phantom node and can be used for transmission as intermediate nodes. Neighbor list shouldn't contain less than 3 neighbors because if there are less number of nodes in neighbor list then privacy can breach.

Analytic Hierarchical Process (AHP) (Saaty. 1987, Saaty. 2004, Yin *et. al.* 2006) is a multi-criterion choice building process in which large problem splits into smaller sub problems (factors). On the basis of importance of these factors to the main problem a best choice is selected. In this paper, AHP uses the following three stages to select phantom nodes from all the sensor node in whole network.

1. Gather data and verbalize Phantom Node Selection as decision hierarchy of autonomous factors mentioned above.
2. Compute the comparative native weights of Factors or choices for selection of Phantom Node.
3. Produce the overhead outcomes to attain the complete weightiness of each substitute sensor node and pick the node with leading weight as Phantom Node.

Decision pyramid of the phantom node selection contains goal at the top which is phantom node selection followed by criteria or factors for the goal in next level, at bottom level options or alternative sensor nodes are weighed.

Calculating Local weights:

Local weights are estimated as weight of each element to the objective and weight of each contestant to the element. Same procedure will be used for both weights.

Making pairwise comparison

All the three factors are compared under the top most goal, the comparison is done by questions: which element is further significant? , how considerable? Comparison is presented by the following matrix P shown in Eq-1.

$$p = \begin{array}{c} \\ x \\ y \\ z \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} p_{x/x} & p_{x/y} & p_{x/z} \\ p_{y/x} & p_{y/y} & p_{y/z} \\ p_{z/x} & p_{z/y} & p_{z/z} \end{pmatrix} \end{array} \quad (1)$$

Where $P_{i/j}$ represents the fraction of i^{th} and j^{th} factor weight. The necessary scale from 1-9 is presented in table-1, which is used for ranking.

Calculating Weight vector

For matrix P we can write its eigenvalue equivalence as $PV=\lambda V$, where V is a non-zero eigenvector and λ is scalar called eigenvalue. Standardization of eigenvector V, the component of vector V can be considered as the local weight of individual choice element, represented in Eq-2

$$v_J^T = \{v_x \quad v_y \quad v_z\} \quad (2)$$

Consistency Check

Matrix P will be consistent if all the elements in matrix P satisfies the equations as shown in Eq-3 and Eq-4.

$$p_{\frac{i}{j}} \cdot p_{\frac{j}{i}} = 1 \quad (3)$$

$$p_{\frac{i}{k}} \cdot p_{\frac{k}{i}} = p_{\frac{i}{j}} \quad (4).$$

Unluckily the evaluation metrics are not perfectly consistent due to different judgments of scale. Therefore these difference of judgment can be perceived by using Consistency Radio (CR), well-defined as the relation of Consistency Index (CI) to the random index (RI) which is given in table-1. CI can be obtained by Eq-5

$$CI = \frac{(\lambda - n)}{n-1} \quad (5)$$

Where

$$\lambda = \left(\frac{1}{n}\right) \sum_{i=1}^{n} \frac{pv_i}{v_i} \quad (6)$$

Table 1. Fundamental Scales from 1 to 9

No of rating	Verbal Judgment Preferences	Explanation
1	Satisfactory	Energy level is low but distance and neighbor list is medium
3	Fair	Energy level is medium, distance and neighbor list is medium
5	Good	Energy level is high while either distance or neighbor list will be low
7	Very good	Energy level is high, neighbor list is high and distance is high as well.
9	Excellent	Energy is level is high, neighbor list is high and distance is medium.

2, 4, 6, 8 specify the intermediate value of overhead pairwise comparison.

Table 2. Consistency Index

Dimension	1,2	3	4	5	6	7	8	9
RI	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45

Calculating Global Weights

Now for topmost goal selection of Phantom Node weights of factors can be obtained from V_j as well as weightage of substitute sensor nodes toward each element. Hence it is supposed that three sensor nodes which can be selected as Phantom Nodes then weights for all three factors for each sensor node can be given as a matrix given Eq-7.

$$Gn_{\frac{i}{j}} = \begin{pmatrix} p_{1/x} & p_{1/y} & p_{1/z} \\ p_{2/x} & p_{2/y} & p_{2/z} \\ p_{3/x} & p_{3/y} & p_{3/z} \end{pmatrix} \quad (7)$$

Global weight of each sensor node can be attained by multiplying local weight to its matching parent. Then concluding weight matrix in the representation of G_{n_i} is calculated as follows in Eq-8

$$G_{n_i} = G_{n_{\frac{i}{j}}}.G_j \quad (8)$$

Where weight of each sensor node can be calculated as:

$$G_{n_i} = \sum_{j=1}^{3} G_{n_{\frac{i}{j}}}.G_j \quad (9)$$

Hence the larger the weight of a sensor node will be more suitable to be selected as Phantom Node among sensor nodes in the network shown in Eq-9. By this way we can select most suitable phantom node among sensor nodes unlike other techniques which uses hop count from source node or sink node as a parameter for phantom node selection.

4. PERFORMANCE EVALUATION

For performance evaluation the proposed technique is implemented on OMNeT++ 4.6 to demonstrate its effectiveness safety period, end-to-end latency and energy consumption. Proposed technique is compared with state of the art techniques tree-based diversionary tree Routing (Long *et. al.* 2014), phantom routing (Kamat *et. al.* 2005), forward random walk (Chen and Lou. 2015), which are using fake sources and multiple paths at the cost of high energy consumption and high end-to-end latency.

Network setup

Wireless Sensor Network is created by evenly arranging 100 sensor nodes in area of *1500 X 1500 m*^{2}. The message range of individually node is set to *50m* and source node generates a packet after each *10s*. Energy of each sensor node is considered to be *20 joules* while Sink have higher energy of *40 joules* (Long *et. al*. 2014). Source node is selected as the target which comes near to a sensor node while phantom nodes are considered to be at a distance of h-hops from the Source Node according to (Kamat *et. al*. 2005) and Sink node is selected at the time of deployment. After the deployment multiple routes from source node to phantom node and then to the Sink are determined according to the proposed technique.

Simulation Results

(Fig 3) shows that end-to-end latency which is defined as the average time taken by a packet to travel from source node to sink node using different routes. The end-to-end latency of the proposed technique is less than tree-based diversionary tree routing and forward random walk. Because proposed technique avoid fake packets transmission and excessive computation, which results with improved end-to-end latency as compared to the existing techniques (Long *et. al.* 2014) which uses sources generating fake packets. Beside fake packets some of the existing techniques (Chen and Lou. 2015) uses excessive computation which also results with low end-to-end Latency.

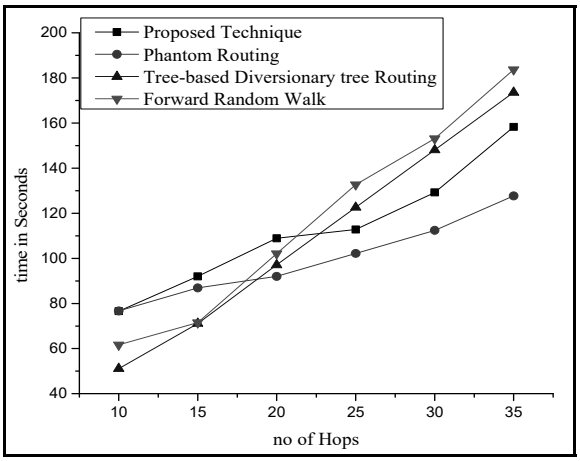


Fig. 2. Comparison of end-to-end latency of proposed technique with existing techniques

(Fig 4) shows energy consumption which can be calculated by the total number of packets including real and fake packets communicated in the network at certain time *T*. The energy consumption of the proposed technique is lower than phantom routing technique and tree-based diversionary tree routing.The reason behind low energy consumption by the proposed technique is that there is only real packets transferred in the whole network unlike in other two techniques(Kamat *et. al.* 2005, Long *et. al.* 2014), which uses dummy traffic to mislead the adversary. Similarly privacy is determined by a term called safety period is defined as the time at which the adversary starts eavesdropping on first packet till it captures the source or target moves from the source node, because when the target moves from the source node then it will not remain as a source node.

(Fig 5) illustrates safety period of phantom routing is higher than the proposed technique initially but safety period of proposed technique improves later than all of the three techniques which shows that source location privacy can be enhanced more if the number of nodes are increased. Safety period of the proposed technique is higher because there are multiple routes which will easily mislead the adversary from source node.

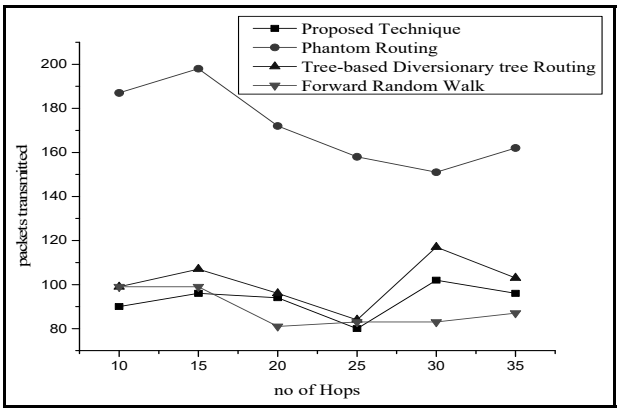


Fig. 3. Comparison of energy consumption of proposed technique with existing techniques

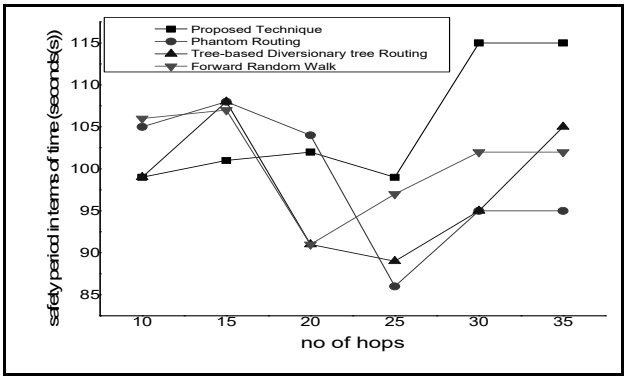


Fig. 4. Comparison of source location privacy in terms of safety period

5. CONCLUSION

The Source node location privacy is a critical problem in the WSN-based monitoring applications. Therefore, in this paper a hybrid technique is introduced which can hide location of the source node from the local adversary by using multiple routes and phantom nodes. Proposed technique is implemented on OMNeT++ 4.6 and evaluated in terms of end-to-end latency, energy consumption and safety period. Simulation results proves that the proposed technique performs better than the state-of-the-art techniques. Since proposed technique only hides location of the source node, as future work it is expected to enhance this technique for end-to-end location privacy of both source node and sink.

REFERENCES:

Akyildiz, I. F., W. Su, Y. Sankarasubramaniam, and E. Cayirci. (2002). A survey on sensor networks. *Communications magazine, IEEE,* 40(8): 102-114.

Chen H. and W. Lou. (2015). On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks. *Pervasive and Mobile Computing,* 16(A): 36-50.

Navarro, M., and Y. Liang. (2014). Energy profile for environmental monitoring wireless sensor networks. In *IEEE Colombian Conference on Communications and Computing (COLCOM)*: 1-6, Bogota.

Conti, M., J. Willemsen, and B. Crispo. (2013). Providing source location privacy in wireless sensor networks: a survey. *Communications Surveys & Tutorials, IEEE,* 15(3): 1238-1280.

Hill, J. L. (2003). System architecture for wireless sensor networks. PhD. Dissertation, University of California at Berkeley.

Kamat, P., Y. Zhang, W. Trappe, and C. Ozturk. (2005). Enhancing source-location privacy in sensor network routing. In *Proceedings of 25th IEEE International Conference on Distributed Computing Systems, 2005 (ICDCS 2005)*: 599-608, Columbus, OH.

Long, J., M. Dong, K. Ota, and A. Liu. (2014). Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. *IEEE, Access,* 2: 633-651.

Li, N., N. Zhang, S. K. Das, and B. Thuraisingham. (2009). Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks,*

Ozturk, C., Y. Zhang, W. Trappe, and M. Ott. (2004). Source-location privacy for networks of energy-constrained sensors. In *Proceedings of Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems*: 68-72, Vienna, Austria.

Rios, R., J. Cuellar, and J. Lopez. (2015). Probabilistic receiver-location privacy protection in wireless sensor networks. *Information Sciences,* 321: 205–223.

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling,* 9(3): 161-176. DOI:10.1016/0270-0255(87) 90473-8.

Saaty, T. L. (2004). Decision making—the analytic hierarchy and network processes (AHP/ANP). *Journal of systems science and systems engineering,* 13(1): 1-35.

Vidhya, S., and A. Kumaar. (2015). Reducing the Energy Consumption in Wirelsess Sensor Networks using sink relocation Mechanism. *ARPN Journal of Engineering and Applied Sciences,* 10(10): 4662-4665.

Yin, Y., J. Shi, Y. Li, and P. Zhang. (2006). Cluster head selection using analytical hierarchy process for wireless sensor networks. In *IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, 2006*: 1-5, Helsinki