International Journal of Engineering & Technology, 7 (4) (2018) 4068-4072

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.18185
Research paper

Modified and secure adaptive clustering approach for autonomic wireless sensor network with minimum radio energy

Sandip Mandal [1] *, Rama Sushil [1]

[1] DIT University Dehradun India
**Corresponding author E-mail: sandy06.gcect@gmail.com*

Abstract

Wireless sensor networks are a trend of the past few years, and they involve deploying a large number of small nodes. The rapid advancement of wireless technology has enabled the development of small, powerful and expensive sensor nodes, which are capable of sensing, computation and wireless communication. The sensor networks can be used in environmental changes and report, health, military etc. Sensor nodes are limited in power, computational capacities and memory. For these reasons, researchers are currently focusing on the design of power-aware protocols and algorithms for sensor networks. Clustering based schemes are believed to be the most energy efficient routing protocols for wireless sensor networks. Clustering is grouping of similar objects or the process of finding a natural association among some specific objects or data. Clustering leverages the advantages of small transmit distances for most of nodes, requiring only a few nodes to transmit far distances to the sink/base station.
The main objective is to develop an energy efficient routing protocol based on clustering along with the reduction in energy consumption so that it improves network lifetime. In the first phase of this work, a number of energy efficient protocols have been studied. In this phase an energy efficient clustering scheme is developed modifying an existing clustering technique namely Low-Energy Adaptive Clustering Hierarchy (LEACH). Finally the performance of the present scheme is measured and compared with the LEACH and another existing scheme via MATLAB Simulation Tools. And the results clearly show that it's performed 17%-21 % better than existing protocols

Keywords: *Wireless Sensor Networks; Wormhole; Denial of Service; Routing Attacks; in-Band Wormhole.*

1. Introduction

LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that minimizes energy dissipation in sensor networks. The key features of LEACH are:

1) Localized coordination and control for cluster set-up and operation.
2) Randomized rotation of the cluster "base stations" or "Cluster-Heads" and the corresponding clusters.
3) Local compression to reduce global communication.

The use of clusters for transmitting data to the base station leverages the advantages of small transmit distance for most nodes, requiring only a few nodes to transmit far distances to the base station. However, LEACH outperforms classical clustering algorithms by using adaptive clusters and rotating cluster-heads, allowing the energy requirements of the system to be distributed among all the sensors. In addition, LEACH is able to perform local computation in each cluster to reduce the amount of data that must be transmitted to the base station. This achieves a large reduction in the energy dissipation, as computation is much cheaper than communication.
The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the base station occur. In order to minimize overhead, the steady-state phase is long compared to the set-up phase.

Advertisement Phase: Initially, when clusters are being created, each node decides whether or not to become a cluster-head for the current round. This decision is based on the suggested percentage of cluster heads for the network (determined a priori) and the number of times the node has been a cluster-head so far. This decision is made by the node (n) choosing a random number between 0 and 1. If the number is less than a threshold T(n), the node becomes a cluster-head for the current round. The threshold is set as:

$$T(n) = \begin{cases} \frac{p}{1-P*(rmod\frac{1}{p})} & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

Where p = the desired percentage of cluster heads (e.g., P =0:05), r = the current round, and G is the set of nodes that have not been cluster-heads in the last 1/P rounds.

Each node that has elected itself a cluster-head for the current round broadcasts an advertisement message to the rest of the nodes. For this "cluster-head-advertisement" phase, the cluster-heads use a CSMA MAC protocol, and all cluster-heads transmit their advertisement using the same transmit energy. The non-cluster-head nodes must keep their receivers on during this phase of set-up to hear the advertisements of all the cluster-head nodes. After this phase is complete, each non-cluster-head node decides the cluster to which it will belong for this round. After each node has decided to which cluster it belongs, it must inform the cluster-head node that it will be a member of the cluster. Each node

transmits this information back to the cluster-head again using a CSMA MAC protocol. Based upon the technique method is used to launch the attack, Wormhole attacks can be classified (Khalil et.al 2007) as shown in the figure 1.

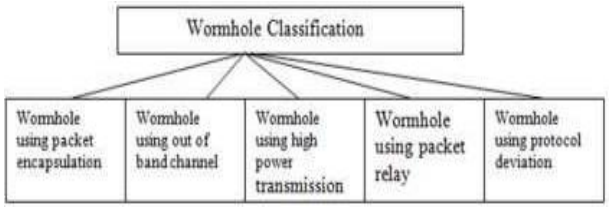

Fig. 1: Shows The Classification of Wormhole Attack Based Upon the Technique Used to Launch the Attack.

Steady-state Phase:
The cluster-head node receives all the messages for nodes that would like to be included in the cluster. Based on the number of nodes in the cluster, the cluster-head node creates a TDMA schedule telling each node when it can transmit. This schedule is broadcast back to the nodes in the cluster.
Once the clusters are created and the TDMA schedule is fixed, data transmission can begin. Assuming nodes always have data to send, they send it during their allocated transmission time to the cluster head. This transmission uses a minimal amount of energy (chosen based on the received strength of the cluster-head advertisement). The radio of each non-cluster-head node can be turned off until the node's allocated transmission time, thus minimizing energy dissipation in these nodes. The cluster-head node must keep its receiver on to receive all the data from the nodes in the cluster. When all the data has been received, the cluster head node performs signal processing functions to compress the data into a single signal. For example, if the data are audio or seismic signals, the cluster-head node can beam form the individual signals to generate a composite signal. This composite signal is sent to the base station. Since the base station is far away, this is a high-energy transmission. This is the steady-state operation of LEACH networks. After a certain time, which is determined a priori, the next round begins with each node determining if it should be a cluster-head for this round and advertising this information.

2. Proposed system model

In this scheme, LEACH protocol is modified by introducing a concept of temporary cluster head (TCH). At first, fixed no of nodes are chosen as TCH based on some energy threshold and next step, the cluster head (CH) selects. The operation of this scheme is broken up into rounds, where each round has two phases

i) Set-up phase
ii) Data transfer phase

i) Set-up Phase

To start with i.e. before any round starts, fixed numbers of temporary cluster heads are selected randomly. However, next time onwards whenever clusters will be formed, the particular number of nodes will be chosen as CHs for that number of clusters. These TCH are selected according to their residual energies. If residual energy of a node is greater than or equal to a threshold value T(n), the node is selected as TCH.. This choice of threshold value T(n) for becoming a temporary cluster head is based on the assumption that all nodes start with an equal amount of energy, and that all nodes have data to send during each frame. If nodes have different amounts of energy (or an event-driven model is used, whereby nodes only send data when some event occurs in the environment), the nodes with more energy should be cluster heads more often than the nodes with less energy, to ensure that all nodes die at approximately the same time. This can be achieved by setting the threshold of becoming a temporary cluster head

$$T(n) = \min\left\{\frac{E_i(t)}{E_{\text{total}}(t)}k, 1\right\}$$

Where $E_i(t)$ is the current energy of node and

$$E_{\text{total}}(t) = \sum_{i=1}^{N} E_i(t).$$

Once the TCH chosen, these TCH announce a temporary cluster head status messages. This advertisement message is a small message containing the node's ID and a header that distinguishes this message as an announcement message. Rest of the sensor nodes receive the status messages and choose their TCH based on the signal strength.
Every member nodes sends their Join-Request to their concern TCH using a carrier-sense multiple access (CSMA) MAC protocol. This join-request message (Join-REQ) contains 3 tuples. This message is consisting of the node's ID, the cluster head's ID and the node's location information.
Based on the residual energy of the nodes, five nodes (priori) are taken for choosing cluster head. Now compute the distance (d) between the five nodes with the help of their corresponding coordinate values.
Suppose two nodes are placed in (x1, y1) and (x2, y2) position. Then the distance between two node is = $\sqrt{}$ {(x1-x2)2+ (y1-y2)2}
The element of the table Ex. (2, 3) means the distance between two nodes (2 and 3).

Table 1: Distance between Nodes

Nodes	Distance between nodes			
1	(1,2)	(1,3)	(1,4)	(1,5)
2	(2,1)	(2,3)	(2,4)	(2,5)
3	(3,1)	(3,2)	(3,4)	(3,5)
4	(4,1)	(4,2)	(4,3)	(4,5)
5	(5,1)	(5,2)	(5,3)	(5,4)

From the above table, in which row the summation of the distance (d) is minimum, this particular node is selected as CH. Suppose in table, and between the five nodes the summation of distance is minimum in fourth row. So, I assume that the fourth node (which boxes in table) is selected as CH. After choosing the cluster head the TDMA schedule is created and informed to the member node. Now the clusters are formed and the steady state operation is start for a round.

ii) Steady state Phase:

TDMA schedule are fixed for the member nodes, now the data transmission are begin.
They send it during their allocated transmission time to the cluster head. The radio of each non-cluster-head node can be turned off until the node's allocated transmission time, thus minimizing energy dissipation in these nodes. The cluster-head node must keep its receiver on to receive all the data from the nodes in the cluster. After all the data has been received, the CH using the signal processing function for aggregating the data messages. Now the data transferred to the BS (base station/sink). After a certain time, which is determined a priori, the next round begins.
The cluster formation of Proposed Scheme is shown in Fig.2 with the help of MATLAB 7.1.

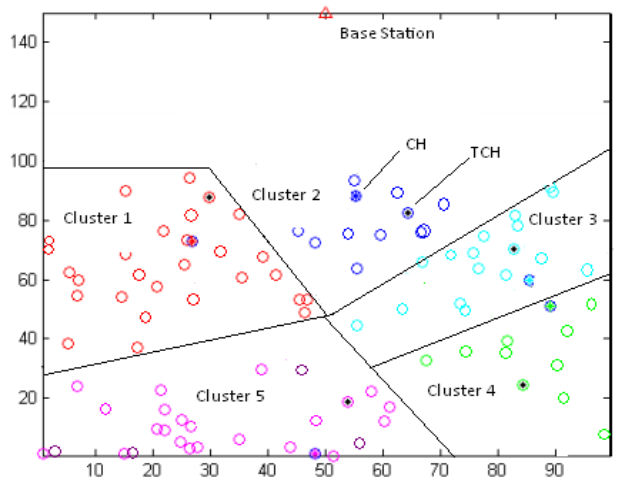

Fig. 2: Cluster Formation of Proposed Scheme.

Algorithm description of proposed scheme:

1) Start /* set up phase*/ /* round start*/
2) round-> 1 to rmax /* rmax->maximum round */
3) For Node(i) /* Node(i)->all node */
4) Check for dead node
5) if (Eres_energy<0) /* E_{res_energy}->residual energy */
6) dnode=dnode+1 /*dnode->no of dead node */
7) end if /*TCH Selection*/
8) if{Eres_energy>=T(n)} /*T(n)->threshold value*/
9) TCH->Node become temporary cluster head
10) end if
11) End for /*cluster formation*/
12) Compute signal strength & location info. for Node(n) /*Node (n)->node join to a particular cluster*/
13) Join Node (n) with location info.
14) End for /*CH Selection*/
15) for all cluster
16) for all Node(n)
17) Compute Eres_energy
18) Create list of 5 based on Eres_energy
19) Compute distance /*distance between the 5 nodes*/
20) CH->node with minimal distance between 5
21) Create TDMA /*TDMA->time slot*/
22) Inform all Node(n)
23) end for
24) end for /* Steady State Phase*/
25) Start data transmission with TDMA
26) Compute energy consumption of member nodes
27) Compute energy consumption of CHs
28) End of round /*end Steady State Phase */

3. Performance analysis of proposed scheme

The proposed scheme, uses the first order radio model values for energy consumption.

Energy consumed by a node for different tasks are as follows

In my work, I assume a simple model where the radio dissipates Eelec = 50 nJ/bit to run the transmitter or receiver circuitry and €amp = 100 pJ/bit/m2.

I also assume an r2 energy loss due to channel transmission. Thus, to transmit a k-bit message a distance (d) using our radio model, the radio expends

$$E_{Tx}(k,d) = E_{Tx-elec}(k) + E_{Tx-amp}(k,d)$$
$$E_{Tx}(k,d) = E_{elec} * k + \epsilon_{amp} * k * d^2$$

And to receive these messages expends

$$E_{Rx}(k) = E_{Rx-elec}(k)$$
$$E_{Rx}(k) = E_{elec} * k$$

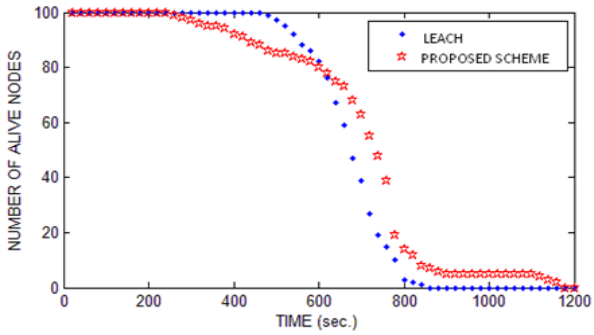

Fig. 3: No. of Alive Nodes in Proposed Scheme.

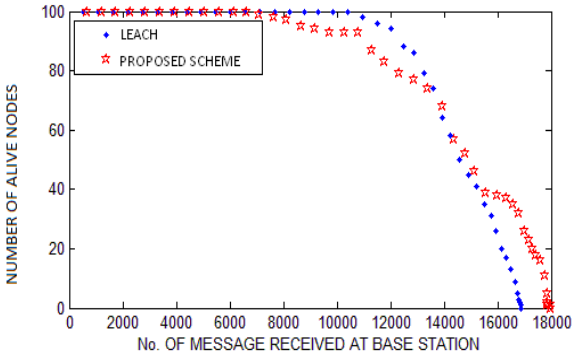

Fig. 4: No of Data Msg. Received at BS in Proposed Scheme.

From the results of various simulations performed as depicted in Figs. 3 and 4, it can be firmly stated that the proposed scheme outperforms than LEACH in term of network lifetime. From the simulation results, it could be explicitly mentioned that the network lifetime, defined in terms of time when the last node dies, is longer in case of Proposed Scheme with respect to LEACH.

It indicates that the last node dies after 8500 sec. in LEACH whereas the same event occurs after 1150 sec. in Proposed Scheme which is 35 % more than EEPSC.

Fig. 3 indicates that number of messages received at base station for any amount of energy consumed in the network is greater in proposed scheme than that in LEACH. Furthermore figure 3 and 4 clearly indicates the advantage of modified scheme over LEACH in terms of network lifetime.

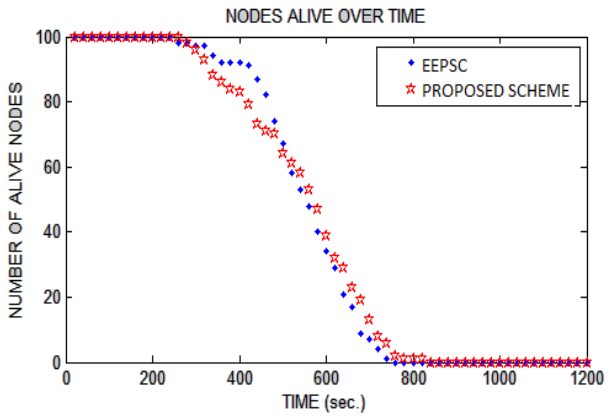

Fig. 5: Comparison between Noh of Alive Nodes between Proposed Scheme and EEPSC.

Fig. 6 indicates that the messages received at BS at any time in case of Proposed Scheme is either equal or greater with respect to EEPSC. Fig. 5 indicates that, the network lifetime, defined in terms of time when the last node dies, is longer in case of Proposed Scheme with respect to EEPSC.

It indicates that the last node dies after 710 sec. in EEPSC whereas the same event occurs after 830 sec. in Proposed Scheme which is 17 % more than EEPSC. So, from the above graphs it clearly

indicates the advantage of Proposed Scheme in terms of network lifetime.

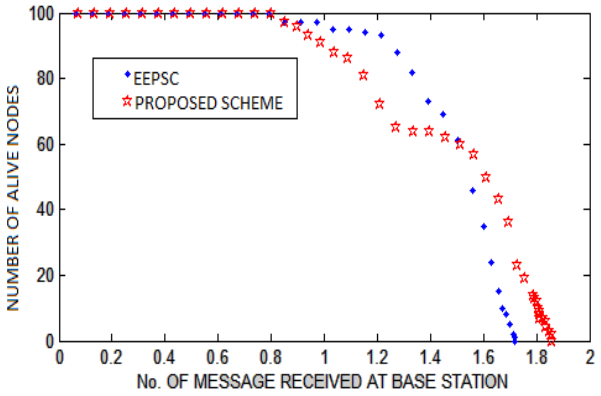

Fig. 6: Comparison between Noh of Data Msg. Received between Proposed Scheme And EEPSC.

Various parameters and their values used in simulation is shown in table 2:

Table 2: Radio Energy Dissipation Model.

Parameter	Parameter's Value
Network Area	100m x 100m
Base Station's Position	(50m, 175m)
Initial Energy for nodes	2 Joule
Number of deployed nodes	100
Size of data message	4000 bits
E_{DA}	5nJ
E_{elec}	50nJ
ϵ_{fs}	10pJ/bit/m^2
ϵ_{mp}	0.0013pj/bit/m^4

4. Conclusion

Efficient clustering strategy is a vital problem in this field of WSN. Moreover, in human accessible or in-accessible area, where sensors are not replace in short time gap, people must use some energy efficient clustering strategy and examined for better result.
Proposed Scheme is basically a modification of an existing scheme, LEACH (Low-Energy Adaptive Clustering Hierarchy). Concept of temporary-cluster-head (TCH) is being inherited from the EECPNL (Energy-Efficient Clustering Scheme to Prolong Sensor Network Lifetime) [14] to reduce the computational overhead of cluster head. Efficiency of the proposed scheme, is measured against LEACH [1] and EEPSC [4] via simulating a set of experiments in MATLAB 7.1 which validates the scheme in order to achieve better network lifetime and a better performance.
As a future extension of this work ,this type of cluster head choosing strategy , I may use in a number of energy efficient competitor scheme with some various node distribution like Poisson distribution, Sparse distribution etc. instead of random distribution in order to minimize the energy dissipation thus expanding the lifetime of network.

Acknowledgement

This research work was supported by the Department of Information Technology DIT University Dehradun India. We are very much thankful to Hon. Vice Chancellor, Prof. Dr. K. K. Raina and Dean RNC, Dr. S.K. Gupta for their motivational support.

References

[1] APrasannajit B, Anupama, Vindhykumari, Subhashini and Vinitha , "An Approach Towards Detection Of Wormhole Attack in Sensor Networks," Integrated Intelligent Computing (ICIIC) First International Conference on, IEEE , E-ISBN 978-0-7695-4152-5 pp 283-289 , 2010
[2] Karlof & Wanger, "Secure Routing in Wireless Sensor Network: Attacks and Countermeasures," First IEEE International Workshop on Sensor Network Protocols and Applications, SNPA, pp 113-127 2003
[3] Khalil, Bagchi, & Shroff, "LiteWorp: Detection And Isolation Of The Wormhole Attack in Static Multi hop Wireless Networks ," International Journal Of Computer And Telecommunications Networking, vol. 51(13),pp 3750-3772
[4] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, "22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp. 1976-1986 2003 https://doi.org/10.1109/INFCOM.2003.1209219.
[5] Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee and Heejo Lee," TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks, "4th IEEE conference on Consumer Communications and Networking Conference, pp. 593 – 598 https://doi.org/10.1109/CCNC.2007.122.
[6] J. Zhen and S. Srinivas, "Preventing replay attacks for secure routing in ad hoc networks, "Proceedings of 2nd Ad Hoc Networks & Wireless (ADHOCNOW'03), pp. 140—150,2003 https://doi.org/10.1007/978-3-540-39611-6_13.
[7] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks, "*Wise, Proceedings of the 2004 ACM workshop on Wireless security. ACM Press*, pp. 51−60 2004 https://doi.org/10.1145/1023646.1023657.
[8] S. Özdemir, M. Meghdadi, and Ý. Güler, "A time and trust based wormhole detection algorithm for wireless sensornetworks,"*3rd Information Security and Cryptology Conference (ISC'08)*, pp. 139−4, 2008
[9] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, Naghmeh Niknejad," Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks" *IEEE*,pp 122-128 , 2011
[10] Phillip Lee, Andrew Clark, Linda Bushnell1,and Radha Poovendran, "A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems ,"*IEEE Transactions on Automatic Control, Special Issue On Control of Cyber Physical Systems 2013*
[11] Yih-Chun Hu,Adrian Perrig and David B.johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of IEEE Infocom 2003, April 2003.
[12] Tuomas Aura,Pekka Nikander,and Jussipekka Leiwo. DOS-resistant authentication with client puzzles. Lecture Notes in Computer Science, 2133:170.177, 2001.
[13] Jiang changyong, Zhang jianming. "The selective forwarding attacks detection in WSNs". Computer Engineering, 2009, 35(21):140-143
[14] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., 2006.
[15] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S¸ekercio glu ," Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines", intelligent sensors, sensor networks and information ,3rd international conference ,pp 335 – 340,ISSNIP 2007 .
[16] Jeremy Brown and Xiaojiang Du. "Detection of selective forwarding attacks in heterogeneous sensor networks. " InICC, pages 1583–1587, 2008
[17] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, Oct. 2009
[18] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network", American Journal of Engineering and Applied Sciences 2 (2): 494- 500, 2009 https://doi.org/10.3844/ajeassp.2009.494.500.
[19] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song," Achieving Network Level Privacy in Wireless Sensor Networks ",Sensors 2010, 10, 1447-1472; https://doi.org/10.3390/s100301447.

[20] Guorui Li, Xiangdong Liu, and Cuirong Wang "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks"
[21] Fan Xiangning, Song Yulin. "Improvement on LEACH Protocol of Wireless Sensor Network", International Conference on Sensor Technologies and Applications, IEEE, SENSORCOMM.2007.21.
[22] D. Kumar, T.C. Aseri, R.B. Patel," EECDA: Energy Efficient Clustering and Data Aggregation Protocol for Heterogeneous Wireless Sensor Networking. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol. VI (2011), No. 1 (March), pp. 113-124.
[23] Gaojuan Fan, Ruchuan Wang, Haiping Huang, Lijuan Sun and Chao Sha," Coverage-Guaranteed Sensor Node Deployment Strategies for Wireless Sensor Networks" Sensors 2010, 10, 2064-2087. https://doi.org/10.3390/s100302064.
[24] Fan Xiangning, Song Yulin , " Improvement on LEACH Protocol of Wireless Sensor Network "Institute of RF-&-OE-ICs, School of Information Science and Engineering, Southeast University, Nanjing, 210096, China.
[25] M. Vahabi, M. F. A. Rasid, R. S. A. R. Abdullah, and M. H. F. Ghazvini," Adaptive Data Collection Algorithm for Wireless Sensor Networks" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.
[26] Wei Bo Hu Han, Ying Fu Wen," An Improved LEACH Protocol for Data Gathering and Aggregation in Wireless Sensor Networks" International Conference on Computer and Electrical Engineering, China, IEEE, ICCEE.2008.59.