ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

A Survey of Secure General Self- Organised Tree Based Energy-Balance Routing Protocol for Wireless Sensor Network

Mahesh R. Darekar, Prof. Mininath K. Nighot

Department of Computer Engineering, KJCOEMR, Pune, India

ABSTRACT: Wireless Sensor networks is a system collection of huge number of low cost sensor nodes spread over the geographic area in order to sense the data. This network is used to collect data and transmit the messages to base station(sink). WSNs have become major area of research in computational theory due to its wide range of applications. But due to limited battery power the energy consumption has become major limitations of WSNs pro-tocols. In order to overcome these problems and to improve the performance of network need not only to minimize total energy consumption but also to balance energy consumption and load in order to improve network lifetime. Researchers have proposed many protocols such as LEACH, HEED, PEGASIS,TBC and PEDAP. In this paper, we propose a General Self-Organized Tree-Based Energy-Balance routing protocol which builds a routing tree using a process where, for each round, BS assigns a root node and broadcasts this selection to all sensor nodes. Each and every node selects its parent by considering only itself and its neighbors information, thus making GSTEB a dynamic protocol. Simulation results show that General Self-Organized Tree-Based Energy-Balance routing(GSTEB) protocol has a better performance than other protocols in balancing energy consumption, thus prolonging the lifetime of WSN. Now we are providing security with SHA-1 hashing algorithm and 3 way Encryption and Decryption for secure broadcasting information from root node to sensor nodes.

KEYWORDS: Index Terms Energy-balance, network lifetime, routing protocol, self-organized, SHA-1 hash Algorithm,3 way Encryption and Decryption, wireless sensor network.

I. INTRODUCTION

Wireless networks allow their hosts or nodes to transfer data wirelessly over long distances via radio communications with-out the constraints of wired networks. Using the advancement in Micro-Electro-Mechanical Systems (MEMS)-based sensor technology, low-power wireless communication[2], [3], [4] and low-power digital electronics; it is now feasible to produce wireless sensor nodes in quantity at low price. Wireless sensor network systems have been widely used for monitoring environmental or physical properties over a large area, e.g., temperature, pressure, luminosity and vibration. Sensor nodes are widely used to collect information in many applications such as surveillance , tracking at critical facilities, volcano monitoring , permafrost monitoring and monitoring animal habitats .WSN consists of low-cost sensor nodes having lim-ited battery power, and the battery replacement is not simple for WSN having thousands of physically embedded nodes, so an energy efficient routing protocol should be employed to have a long network lifetime. wireless sensor nodes are deployed randomly and densely in a target region, especially where the physical environment is so harsh that the macro-sensor counterparts cannot be deployed. The network cannot work properly due to insufficient battery power. It requires the data fusion processing in order to reduce the data redundancy collected from the sensor nodes. Data aggregation helps to reduce the traffic load thereby conserving the energy in the sensor nodes. PEGASIS [8], PEDAP [9] and TBC [18] are typical protocols based on this assumption and perform far better than LEACH [5], [6] and HEED [7] in this case.

In General, there are quite some applications in which the length of the message transmitted by a parent node depends not only on the length of its own, but also on the lengths of the messages received from its child nodes. In this paper, we propose a General Self-Organized Tree based Energy Balance routing protocol (GSTEB).We consider a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

situation in which the network collects information periodically from a terrain where each node continually senses the environment and sends the data back to BS.

Usually there are two definitions for network lifetime: a) The time from the beginning of the network operation to the death of the first node in the network. b) The time from the beginning of the network operation to the death of the last node in the network.

In this paper, we adopt the first definition. Moreover, we consider two extreme cases in data fusion: Case (1) The data between any sensor nodes can be totally fused. Each node transmits the same volume of data no matter how much data it receives from its children. Case (2) The data cant be fused. The length of message transmitted by each relay node is the sum of its own sensed data and received data from its children The remainder of the paper is organized as follows: Section II reviews related works. Section III describes the architectures and details of GSTEB. System analysis discussed in Section IV. Finally, Section V represents Implementation And Require-ment specification,Section VI concludes the paper.

II. REVIEW OF LITERATURE

GSTEB (General Self-Organized Tree-Based Energy-Balance Routing Protocol for Wireless Sensor Network) is a dynamic protocol in which routing tree is build using the process where in each round, BS selects a root node and broadcasts this assortment to all sensor nodes in the network. Then, each node selects its own parent by considering itself and its neighbors information. Simulation results have shown that GSTEB gives a better performance than other protocols in balancing energy consumption, thereby extending the network lifetime.

In LEACH (Low-Energy Adaptive clustering Hierar-chy)[5],[6] sensors nodes are organized to form clusters and in each cluster one sensor node acts as the cluster-head. In LEACH protocol the first node dies over 8 times later than the first node death in direct transmission and the last node dies 3 times later than the last node death in other protocols. HEED (hybrid, energy-efficient, distributed clustering algorithm) [7] is an improvement over the LEACH protocol on the manner of how the cluster heads are selected. HEED protocol ensures that there is only one CH within a certain range, so there is uniform distribution of the cluster heads in the network which will result in minimum energy consumption thereby enhancing the network lifetime. HEED protocol is suitable only when the nodes have different initial energy.LEACH and HEED greatly reduce total energy consumption. However, LEACH and HEED consume energy heavily in the head nodes, which makes the head nodes die quickly. S. Lindsey et al. proposed an algorithm related to LEACH, and it is called PEGASIS [8].

PEGASIS (Power-Efficient Gathering in Sensor Information Systems) [8] is a near Optimal power efficient chain-based protocol that uses GREEDY algorithm. In PEGASIS protocol all the sensor nodes in the network form a chain in which, the (I mod Nth) node is selected as the leader, which directly communicates with the base station in round i. N is the total amount of nodes. PEGASIS protocol reduces the amount of data for long-distance transmission which prolongs the network lifetime.Tree-Based Clustering (TBC) [18] is an improvement over LEACH protocol. TBC forms various clusters in the same way as LEACH forms. In TBC, the nodes within a cluster construct a routing tree where the cluster-head is the root of the tree. The height and the number of levels of the tree is decided according to the distance of the member nodes to the cluster head. For tree configuration, the cluster-head uses the distance information between the member nodes and itself. Each node is location-aware, it can estimate the distance between the root and itself. Every cluster is divided into some levels. The distance of a node to the root is the basis for determining its level in the cluster. The cluster-head is at level-0(root) and a node in level will choose the node in and nearest to itself as its parent node. Data transfer simultaneously happens between the nodes in two neighboring levels, and each node fuses the received data and transmits it to its parent. TBC is an excellent protocol in which each node records the information of its neighbor nodes and accordingly builds topography, which is similar to GSTEB.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

PEDAP (Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks)[9] is a tree-based routing protocol that makes all the sensor nodes in the network form a minimum spanning tree which costs minimum energy consumption for data transmitting. It also has another version called PEDAP-PA which slightly increases energy for data transmitting but balances energy consumption per node. PEDAP has the same network assumptions as PEGASIS and uses data fusion. However, both PEDAP and PEDAP-PA are protocols that need BS to build the topography which will cause a large amount of energy waste. This is because if the network needs BS to build the topography, BS should send a lot of information to the sensor nodes, including what time is the Time Division Multiple Access (TDMA) slot, who are their child nodes and who are their parent nodes.

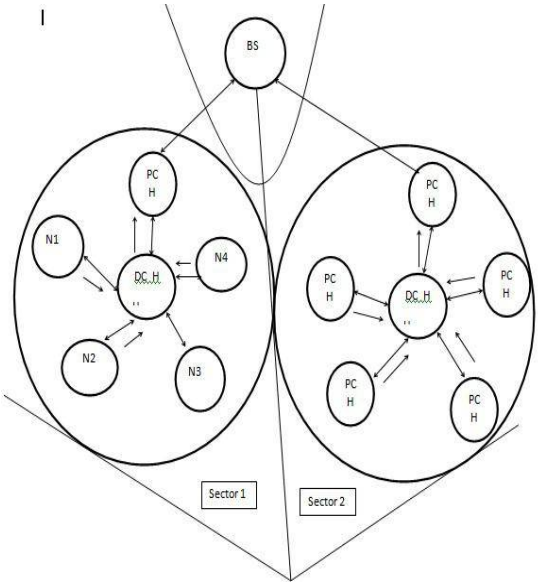

Fig. 1. System architecture

A) DCH: data cluster head

Begin:

Step 0: Every nodes sends its track id and sector id to its BS through broadcasting.
Step 1: For every sector id

1.1: Find center of distance by taking average of distance of node from BS.

1.2: Find the node which is nearest to node and make it as data cluster head.
Step 2: DCH sends the information of routing cluster to one which is appointed as RCH. End.

B) RCH: Routing cluster head

The Routing cluster head (RCH) is selected to the node
which is at minimum distance from the BS. For j=1 to n If (node[j] Min) Min=node[j] RCH=Min

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Then they modify their tables. If no such packet is received in the time slot, the network will start the next round.

GENERAL SELF-ORGANIZED TREE BASED ENERGYBALANCE ROUTING PROTOCOL

The operation of GSTEB is divided into[1]

Initial Phase

In This Phase BS assigns a root node and broadcasts its ID and its coordinates to all sensor nodes. Then in Tree Constructing Phase, the network computes the path either by transmitting the path information from BS to sensor nodes or by having the same tree structure being dynamically and individually built by each node. GSTEB[1] can change the root and reconstruct the routing tree with short delay and low energy consumption. In Self-Organized Data Collecting and Transmitting Phase, after the routing tree is constructed, each sensor node collects information to generate a DATAPKT which needs to be transmitted to BS.

Tree Constructing Phase

For each round,GSTEB performs the following steps to build a routing tree. Between two different cases there are some differences in the steps of routing tree constructing: Step 1: BS assigns a node as root and broadcasts root ID and root coordinates to all sensor nodes.

Self-Organized Data Collecting and Transmitting Phase At this phase after the routing tree is constructed, each sensor node collects information to generate a DATAPKT which needs to be transmitted to BS. TDMA and Frequency Hopping Spread Spectrum (FHSS) are both applied. This phase is divided into several TDMA time slots. In a time slot, only the leaf nodes try to send their DATAPKT. After a node receives all the data from its child nodes, this node itself serves as a leaf node and tries to send the fused data in the next time slot. Each node knows the ID of its parent node. In each time slot, in order to reduce communication interference, we apply FHSS in which each child node communicates with its parent node using the frequency hopping sequence determined by its parent node ID. Each TDMA time slot is divided into three segments.

Information Exchanging Phase.

since each node needs to generate and transmit a DATAPKT in each round, it may exhaust its energy and die. The dying of any sensor node can influence the topography. So the nodes that are going to die need to inform others. The process is also divided into time slots. In each time slot, the nodes whose energy is going to be exhausted will compute a random delay which makes only one node broadcast in this time slot. When the delay is ended, these nodes are trying to broadcast a packet to the whole network. While all other nodes are monitoring the channel, they will receive this packet and perform an ID check.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

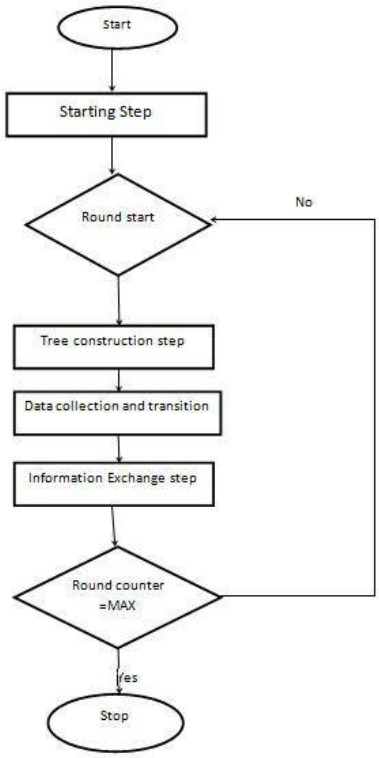

Fig. 2. GSTEB Flowchart

IV. SYSTEM ANALYSIS

3 Way Encryption And Decryption :

3 Way encryption is efficient in wide range of platforms from 8-bit processors to specialized hardware.It resembles more mathematical feature which enable all the decryption exactly the same way as the encryption.

It is a block cipher Symmetric key encryption. 96 bit block as input and 96 bit key. XOR and re-arrangement are the basic operations. Ensures total security in online transactions.provides additional security to protect customers order information such as credit card numbers.

SHA-1 hash Algorithm: Purpose: Authentication

SHA-1 is a cryptographic hash function designed by United states NSA. It produces 160 bit hash value known as Meessage Digest. Verify that received messages come

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

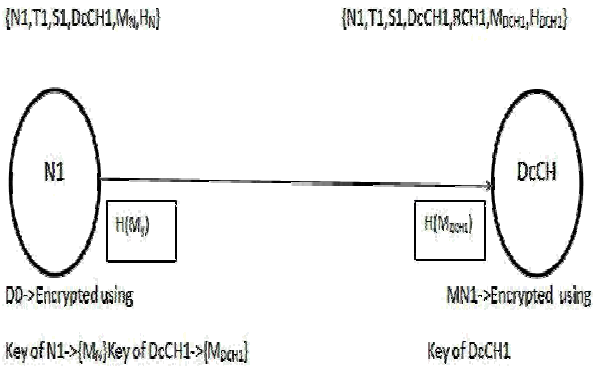

Fig. 3. a

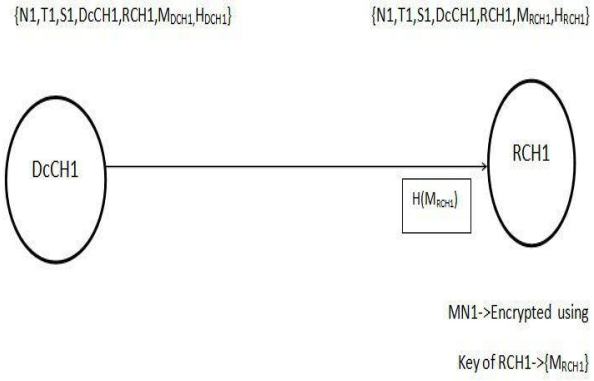

Fig. 4. b

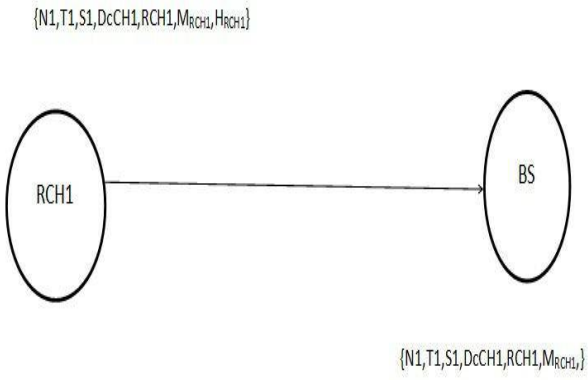

Fig. 5. c

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

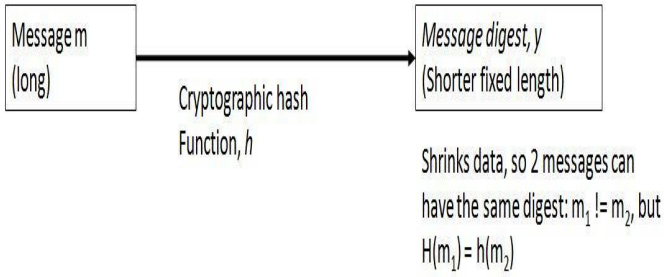

Fig. 6.

Message is padded with a 1 and as many 0s as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length...

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions.

SHA1 requires 80 processing functions defined as: f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 t

19)
f(t;B,C,D) = B XOR C XOR D (20 t 39)

f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 t 59)

f(t;B,C,D) = B XOR C XOR D (60 t 79) Step 4: Prepare Processing Constants....

SHA1 requires 80 processing constant words.

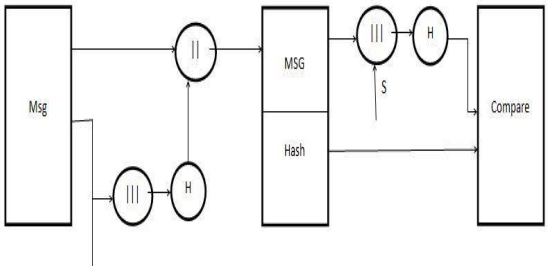

Fig. 7. Basic Hash Function

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

from the alleged source and have not been altered. Also verify the sequence and timing. Digital Signature is used to combat denial of receipt of a message by either the source or destination. Applications: Integrity checking- virus or malware scanning. Public key algorithms- Digital signatures Authentication- Secure web connections. PGP, S/MIME,SSH.

Goal is to provide unique Fingerprint or Message Digest of the message.

SHA-1 (160 bit message) Algorithm Framework

Step 1: Append Padding Bits.

V. IMPLEMENTATION DETAILS

Input: BS assign root node and Broadcast its ID and Co-ordinates to all sensor nodes.

Construction Tree: Construct the Tree compute path. Improved GSTEB: We are applying SHA-1 and three way Encryption Decryption security mechanism On GSTEB for security purpose.

Expected Output:

TABLE I

NODE VS DELAY

No of Nodes	Delay
80	4.7
100	5
120	4.6
140	5.2

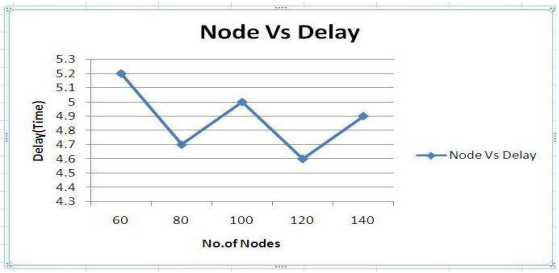

Fig. 8. Node vs Delay

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

TABLE II

NODE VS PDR

No of Nodes	PDR
50	21
75	42
125	73
150	75

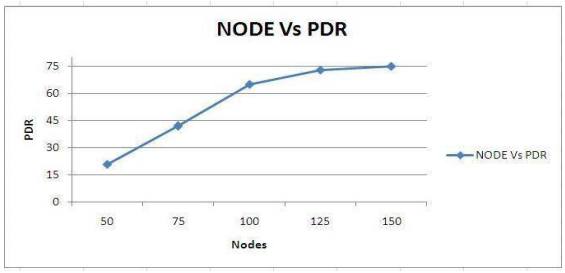

Fig. 9. Node vs PDR

Finally after the routing tree is constructed each sensor node collects information to generate a DATAPKT which needs to be transmitted to BS.

TABLE III

REQUIREMENT SPECIFICATION

Processor	Core 2 Duo
RAM	2 GB
HDD	80 GB
Operating System	Linux
Language	Java/C++
Simulator	NS2

VI. CONCLUSION

In this work, We introducing a new secured and tree based routing protocol for WSN. The proposed technique uses a SHA-1 Hash algorithm for exchanging information between BS and sensor nodes so to preserve integrity of broadcast data.

ACKNOWLEDGMENT

I express great many thanks to Prof. Mr. M.K. Nighot for their great efforts of supervising and leading me, to accomplish this fine work. To college and department staff, they were great source of support and encouragement. To my friends and family, for their warm, kind encourages and loves. To every person gave us something too light my pathway, I thanks for believing in me.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

REFERENCES

[1] Zhao Han, Jie Wu, Jie Zhang, Liefeng Liu, and Kaiyun Tian, A General Self-Organised Tree-Based Energy-Balance Routing Protocol For Wireless Sensor Network, IEEE Transactions On Nuclear Science, Vol.62,No.2,April2014.
[2] K. Akkaya and M. Younis, A survey of routing protocols in wireless sensor networks, Elsevier Ad Hoc Network J., vol. 3/3, pp. 325349, 2005.
[3] I. F. Akyildiz et al, Wireless sensor networks: A survey, Computer Netw., vol. 38, pp. 393422, Mar. 2002.
[4] Sohrabi et al., Protocols for self-organization of a wireless sensor network, IEEE Personal Commun., vol. 7, no. 5, pp. 1627,Oct. 2000.
[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy efficient communication protocols for wireless microsensor networks, in Proc. 33rd Hawaii Int. Conf. System Sci., Jan. 2000, pp. 30053014.
[6] W. B. Heinzelman, A. Chandrakasan, and H. Balakrishanan, An application-specific protocol architechture for wireless microsensor net-works, IEEE Trans.Wireless Commun, vol. 1, no. 4, pp. 660670,Oct. 2002.
[7] O. Younis and S. Fahmy, HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, IEEE Trans. Mobile Computing, vol. 3, no. 4, pp. 660669, 2004.
[8] S. Lindsey and C. Raghavendra, Pegasis: Power-efficient gathering in sensor information systems, in Proc. IEEE Aerospace Conf., 2002, vol. 3, pp. 11251130.
[9] H. O. Tan and I. Korpeoglu, Power efficient data gathering and aggrega-tion in wireless sensor networks, SIGMOD Rec., vol. 32, no. 4, pp.6671, 2003.
[10] S. S. Satapathy and N. Sarma, TREEPSI: Tree based energy efficient protocol for sensor information, in Proc. IFIP Int. Conf., Apr. 2006, pp. 1113.
[11] I. F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks: A survey, Computer Netw.s, vol. 38, no. 4, pp.393422, 2002.
[12] R. Szewczyk, J. Polastre, A.Mainwaring, and D. Culler, Lessons from sensor network expedition, in Proc. 1st European Workshop on Wireless Sensor Networks EWSN 04, Germany, Jan. 19-21, 2004.
[13] Lessons from sensor network expedition, in Proc. 1st European Work-shop on Wireless Sensor Networks EWSN 04, Germany, Jan. 19-21, 2004.
[14] J. H. Chang and L. Tassiulas, Energy conserving routing in wireless ad hoc networks, in Proc. IEEE INFOCOM, 2000, vol. 1, pp. 2231
[15] G. Mankar and S. T. Bodkhe, Traffic aware energy efficient routing protocol, in Proc. 3rd ICECT, 2011, vol. 6, pp. 316320.
[16] N. Tabassum, Q. E. K. Mamun, and Y. Urano, COSEN: A chain oriented sensor network for efficient data collection, in Proc. IEEE ITCC, Apr. 2006, pp. 262267.
[17] M. Liu, J. Cao, G. Chen, and X.Wang, An energy-aware routing protocol in wireless sensor networks, Sensors, vol. 9, pp. 445462, 2009
[18] K. T. Kim and H. Y. Youn, Tree-Based Clustering(TBC) for energy efficient wireless sensor networks, in Proc. AINA 2010, 2010, pp. 680685.