International Journal of Engineering & Technology, 7 (2.32) (2018) 5-9

International Journal of Engineering & Technology

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

Research paper



Multi-level Structured Tree based Routing for Energy Efficiency in WSN

Dr. Thirupathi Regula[1*] , Dr. Mohammed Ali Hussain[2]

[1]*Lecturer, Department of Information Technology, Higher College of Technology, Muscat, Sultanate of Oman.*
[2]*Professor, Dept. of ECM, Koneru Lakshmaiah Education Foundation, Guntur Dist., Andhra Pradesh, India.*
**Corresponding author E-mail: regula.thirupathi@hct.edu.om*

Abstract

The manuscript should contain an abstract. The abstract should be self-contained and citation-free and should not exceed 200 words. The abstract should state the purpose, approach, results and conclusions of the work. The author should assume that the reader has some knowledge of the subject but has not read the paper. Thus, the abstract should be intelligible and complete in it-self (no numerical references); it should not cite figures, tables, or sections of the paper. The abstract should be written using third person instead of first person.

1. Introduction

Wireless sensor networks consists of nodes as sensors which are interconnected each other for performing data aggregation. The node sensor are devices which perceive the environmental data attributes like pressure, heat, motion , smoke , moisture etc. There are various types of applications in WSN which actually are based on functionality of nodes[1,2]. Where security issues is also an important area of research within WSN before. Security reliability mechanisms are the key providers for exchange of data for security. TLS, RSA and Kerberos which exist even before WSN. Whereas these protocols does not involves constraints of resource as important cause[3]. Here resource usage is minimized based on integrity, confidential, authenticity and availability should be maintain in all categories of WSN[5]. In order to manage the reliability, authentication, confident and availability in a network[6], we all attacks and method are not limited in various types of WSNs.

Managing of key is the vital part related to security issues in WSN, which provides a security issues related to target based on WSN applications which gives less overheads and gain less overheads in sensor networks.

It is important in a WSN to have a managing key strategy, that give security as per the guidelines and application related to WSN and which should provide fewer overheads in sensor nodes. Energy efficiency and secure communications is the based in WSN which consists of various levels of groups, in which every cluster contains of number of sensor devises. To achieve various levels of communications, depending on various groups based on system communication and clusters, effective total key management are used for exchanging the information between systems that finally provides the security among multiple clusters based on performance. Here key and key-management methods presents in the literature based on clusters and cluster-based communication is learnt[4].

Likewise efficiency energy factor and security are the main challenging areas of research in WSN applications. The primary factor and essential vulnerable are the threats related to energy and security scenarios which disrupt the network system communications. Our proposed method provides a joint technique for energy related problem and security issues. Out paper mainly emphasis on addressing the energy constraints and attack occurred in security related to Sybil.

Discussion of Section II about the available techniques used in energy and security are studied based on the literature survey, the proposed study problem is discussed briefly in section III. The model of proposed in studies in IV section and also the study of benchmark and outcome algorithm in section V. Section VI and VII discusses the result outcomes and comparative study. In Section VII we conclude and remark the future study of the proposed

2. Existing Work

Various survey related to energy efficiency are done along with security optimality in WSAN and WSN. This is mentioned below.

Chenti .C and others, developed a routing algorithm protocol to provide energy efficiency in WSN[7]. The output of this provides an effective delivery rate of packets without any link failure, this algorithm doesn't provide any security features. Recent study has been formulated by Takaishikaand others, are developed a technique which provide data aggregation to process data efficiently based on energy efficiency which mainly focuses on small sensor networks[8]. Related works have be carried out by Matin Rahman, the author proposed an algorithm for increasing the life of the network which uses Swam algorithm[9]. This approach has the capability of increasing the energy only of 40% based on performance bench marking. Energy addressing issues and life time reliability studies have been done by Heet and others, proposed a model based on greedy technique for estimating the coverage of sensor nodes[10]. The output of this provides less probability failure with very high reliable rates in life of network. He later compared the proposed algorithm with LEACH based on routing variant algorithm, he also addresses the issues related to energy issues. Xiong and Lihi, presented an ideal related to integration of smart

Copyright © 2016 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

devices using sensors in a network related to Internet of Things[11], he also included a security related cryptography communication for effective communicate and safe. However, the output is mainly compared with process time without check the QoS attributes based on throughput and packet loss. The basic study focuses on security was provided by chot et al, developed a techniques of mitigation to increase trust and security related to data redundancy and efficiency in energy trade off[12]. Hong et al, have developed a method that aims for mitigating attack of phantom[13]. The result of the study was computed with certain parameters of security and consumption of energy factor[14].

3. Problem Identification

The identification of the problem is done with the study of the proposed as follows

1. It is very difficult in computing complex task based on issues of energy and security threats jointly
2. The existing work done are mainly focused on energy efficiency which is very much lesser than LEACH, this has given various reasons in problem identification.
3. The techniques do not identify security addressing.
4. They posses the same problem faced in LEACH based on clustering.
5. Complexity of computational is focused very less.
6. This has not been performed in large scalar network.
7. The available crypto key protocols are too complex for execution on sensor nodes, the main protocols are MD5/MD4/SHA2/SHA1.

4. Proposed Model

The motivation has provided use to develop a joint address system problem based on energy effective and information aggregation secured method. The designed model named as Multi-Level secured routing based on tree in terms of efficient energy using theory of probability for energy ensuring efficiency and authentication of routing network mechanism in WSN.

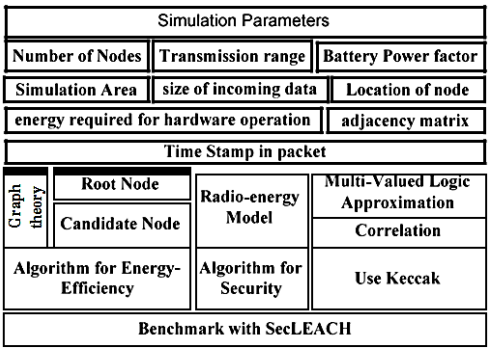


Figure 1 Proposed Schema of STREE

The main contribution of proposed work is explained in Figure 1, which is,

1. To gain energy consumption optimal using multi-level tree structure approach
2. To gain crypto secure protocol with less cost and effective against Kecakk and Sybila
3. To validate the comparison over the proposed with SecLEACH based on energy efficiency and security issues.

By studying the issues related to the crypto security and energy in WSN, Multi-Level tree approach is considered as

The block diagram MSTREE designed has be done using two phases, where the phase 1 address the model of communication and phase two address the model of security.

The motivation has been done based on routing of hierarchical protocols; we have used a radio dissipation energy model in energy efficiency model. In our work, we developed a model which dissipates transmitter, which run whole of the network using electronic radio which supplies power to the sensors and dissipates energy receiver which run on electronic radio.

The main focus in this part is for model design, which evaluates the efficient security and cost energy in WSN application.

A. Addressing Energy Problem

MSTREE is based on multi-level logic value which chooses an optimal factor in identifying the energy efficiency in a hierarchical routing process in WSN. This algorithm uses a multi- layered clustering approach using tree structure logic for a approximation of single tree logic.

Single-Tree logic Approximation: it uses a energy model of radio based on attributes related to data gathering in this phase related as (ETX, ERX, E amp etc.) the value are ensured based on the value of highest weight gained by the traffic flow based on tree hierarchy performance and flow factor.

The main and crucial factor is approximation of clustering done from the root to the candidate node, this consideration is done based on attributes related to power factor and spatial attributes.

Approximation of clustering is done on each stage of multi-level of tree structure in routing for gathering of information and updating of data between the root nodes based on power and coordinates of the nodes, having a group cluster relationship between them[15]. The main root nodes or sub-tree nodes will communication among themselves between the candidate nodes in an each cluster tree, which provides flexibility and reduces fewer overheads. Mainly in WSN overheads are occurred due to data redundancy and duplicate energy deletion.

Likewise to reduce and avoid redundancy in data in a WSN , where each root node collects the data-information through candidate nodes using the source of power, coordinates and matrix of adjacency based on time stamp and nodes which are co-related for packet movement or forward. Hence, redundancy data at a large scale is mitigated in single tree logic approximation method which will preserve energy lead in a tree structure. This factor of approximation uses the mitigate stage of network reduction in overhead and depletion related to information and will allowto use reliable communication between the nodes of candidate from root nodes to heretical single node of network.

Multi logic Tree Calculation:- It is the optimization process to single logic tree calculation to further extend the weighted factors of the tree. This method uses the best approximation on multi-level root nodes in finding the weight factor Certain issues related to overhead are reduce with the usage of single logic hierarchical structure. At this stage this method is applicable to large tree structure which is changing dynamically of certain order.

Our work adopts the assumption are based usually on sensor network, based on base mobile station of some degrades the clustering performance with required energy and for delivery of data successful[16].

This phase of assuming states the node root are at sufficient distance from each level of tree , where each root node in a sub-tree may be selfish in forward the data packet due to energy efficient.

The assumption has been done with following two goals, i) the nodes which are compromised will not delivery the packets but it drops the packets under each level and ii) the sensor nodes which possess less battery power don't forward the packet data , but it retains the power from the level of tree routing structure.

These types of issues are not notified in root node, which is identified in candidate node, but which is shown in delivering the data at the sensor nodes. Hence we use multi-level structure in finding the density of the node and its factor of density in identifying the energy required factor of batter power, pivotal zonal factor and factor of contiguity.

The pivotal zonal factor is evaluated using correleation of spatial using the root node between multiple hop tree structure node topology.

MSTREE mainly focuses on technique of cryptographic light weight method for data aggregation and security process. In this phase, nodes of the candidate and root nodes will be provided the set based on random method indexers that are provided to the nodes.

The model which has been considered will reduce attack of Sybil which won't steal identity of the sensor-nodes. The main determination is to authenticate the devises, so that if whichever compromise of nodes occurs, they cannot access the node resource or certain operation of packet forward has be done or restricted. Thus the issues of indexers will solve this problem. MSTREE performs symmetric key incorporating between the nodes used for communication within them. In our model MSTREE, we consider both static and dynamic key used for mobile investigation based on scenarios of vulnerability.

The design of a scheme is done in such a manner that it gives variable size of key using randomized key, where the previous works say they , we have to use a specific key and its size as unique. This can be done and adviser or attacker cannot guess the key size before cryptanalysis performance. We have identified an interesting security algorithm based on interest of case in solving the issues related to security in WSN. It is observed that common key is the main target in attack of Sybil in sensor nodes. Hence we use a key which encrypts the common key in reducing the attack of secure in WSN. This method not only reduces the attacks in wireless sensor nodes internally or externally.

3. Implementation Algorithm

MSTREE is normal implemented in NS-2 on 32 bit computer on window 7 OS as a platform design. The algorithm is implementing based on design of MSTREE into 2 parts. i) Energy efficiency addressing issue ii) issue related to security on the network.

Algorithm for Energy Effectiveness

Input:

N:	Number of Nodes,
T_x	Transmission range
A:	Simulation Area,
j:	size of incomingdata,
ı:	energy required for hardware operation to process 1 bit of data,
$L_{x,y}$:	Location of node,
A_{mat}	adjacency matrix,
T_{stamp}:	Time Stamp in packet,
R_{node}:	Root Node,
C_{node}:	Candidate Node

Output: Nodes count with efficient energy

Start

1. Deploy simulation area by initializing N, T_x and B_F
2. Calculation of tree weight by Single-Value Logic Approximation to graph G=(V, E)
3. Elect the base of root Arg_{Max} (E_{ex})
4. Build the IJ-threshold of tree G_{IJ}
5. for(j value1 to k) do
6. elect the node from tree i.e. $n_j$from G_{IJ}
7. differentiate $n_j$and elect as cluster head and make clusters K as $C(n_1),\ldots\ldots C(n_{k-1})$
8. Build the matrix to store particular data of single treeM_{unit_hop}= Unique (χ)|χ ={B_F, $L_{x,y}$, A_{mat},T_{stamp}}
9. Initiate communication between root node to every nde and update $M_{unit_hop.}$
10. If communication information matche with $M_{unit_hop.}$
11. Abandon updating $M_{unit_hop.}$.
12. Re-predict the Node density.
13. Predict the ZPF=$Cor_{spat}(R_{node}, C_{node})$
14. Evaluate CF={$Cor_{spat}(C_{node}), T_{stamp}$} //Reduce Overhead
15. If B_F<0,
16. death of flag node
17. Else
18. Predict the remaining Nodes as Entire Node to node death. Stop.

Algorithm 1 highlights

1. Describes the energy degeneracy extenuationmethod
2. The algorithm molded in a random manner which is similar with real time consequence
3. Tree structure is built by the use of graph and maps the sensor nodes with roots in WSNs, then treated by single valued reasoning as well as multi valued reasoningestimation.
4. Algorithm calculates the minimum energy required to process 1 bit data and selection of root node is done by step 4, and later applies the cluster calculation method
5. Neighbor nodes are selected by graph threshold factor GIJ
6. Matrix Munit_hopis record the all transaction routing information
7. Step 15 and 16 calculate the perform optimization of energy efficiency

Sybil attack MitigationAlgorithm

Input: χ: indexers,χ_1: B_F,χ_2: Node ID,χ_3: Public Key
Output: Encrypted Common Key
Start:
1. Initialize the nodes with random indexers (χ)
χ_n=rand(χ_1, χ_2, χ_3)
2. Randomize the size of the key
//Perform authentication
3. If $node_x(\chi_3)$==$node_y(\chi_3)$
4. Don't Generate key and abort connection
5. Else
6. Generate secret key as:

$$S_{key1}= | node_x(\chi_1)- node_y(\chi_1) |^2+4.(node_x(\chi_2)- node_y(\chi_2))$$

7. *if* ($\sqrt{S_{key1}}\neq 0$)

$$K_{nodes} \square | (node_x(\theta 1)-node_y(\theta 2)) \square \square \sqrt{S_{key1}}|$$

2

8. If (K_{nodes}<key-chain)
9. S_{key2}=Max(2||key-chain(K_{nodes}))
10. Generate Common Key
$S_{com_key}=[S_{key2}||\chi_n]$
11. Perform encryption to key
S_{enc_key}=h(S_{com_key})//keccak

End

Algorithm 2 Highlights

1. Describes about mitigation of Sybil attack
2. All the nodes designed with random values $\chi 1$, $\chi 2$, …….χn etc, where $\chi 1$ is battery power aspect, $\chi 2$ isID of Node and $\chi 3$ is Public Key.
3. Values of attributes ($\chi 1$, $\chi 2$, $\chi 3$) changing in every communication
4. Group based communication is achieved by assumption that every sensor node contain certain public keys
5. Authentication process enabled by broadcasting of RREQ control packet
6. The interesting point behind the assumption of indexers is that with every cycle of data communication, all

After evaluating keys for each node using this approach it is compared with existing key chains to generate common key. Finally, the common key is further encrypted using advanced cryptographic hash function called as keccak.

4. Result Discussion

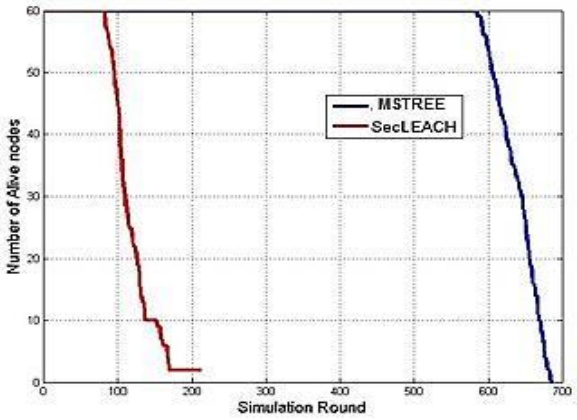


Figure 2 Evaluation of Alive Nodes

Performance analysis of proposed work is compared with existing work with respect to energy efficiency as well as security. Hence, we choose to consider SecLEACH that has been pioneered by Oliveira et al[17]. Fig.2 shows that STREE is capable of ensuring retention of maximum number of sensor nodes upto 85% in comparison with SecLEACH that has only 14% energy conservation out of 600 simulation analysis.

The major motive behind this is that SecLEACH accomplishes compound key delivery system without ample speaking the key size. Moreover, the key generation process is performed by i) key pre-distribution, ii) shared-key discovery, iii)path-key founding.

Here STREE is very simple in operation due to simple one process key management system and cryptography, where the sizes of keys are climbable rendering to the susceptibilities recognized in the network apart from Sybil attack.

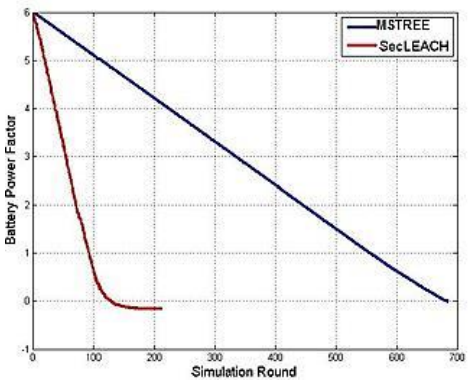


Figure 3 Evaluation of Battery Power Factor

Figure 2, gives the results of power battery factor for identifying the in order to know the drain energy rate of battery. The output of it shows in Figure 3, that SecLEACH is found descent in gradual imminent related to curve of energy and which is around 220 steps, the overall. The network eventually dies with very high security.

The main reason identified with facts of SecLEACH which leads to system overheads and efficiency in energy, MSTREE which is proposed will not compromise the attack of Sybil and give better efficiency in energy of the network.

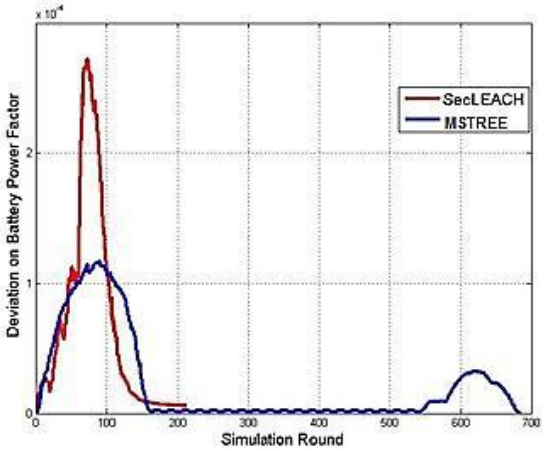


Figure 4 Deviation of Battery Power Factor

Figure 4 shows the examination of the nonconformity in the Battery Power Factor for both SecLEACH and STREE. While process is being approved out by using SecLEACH, it was originate that there is unexpected variation of energy foremost to advanced debauchery of energy.

The major reason behind hand this is SecLEACH reflects big pools of keys and their IDs that are predefined. However, nobody of the node IDs vicissitudes as they just signify the sensor node, whereas in STREE, we select to reflect indexer which saves in altering at each round of communication with actual less overhead and safeguarding advanced level of security.

Although STREE has fluctuation in Battery Power Factor, but it is quite stabilized as compared to conventional SecLEACH.

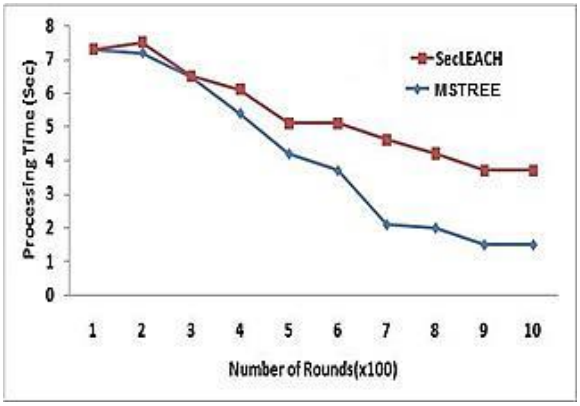


Figure 5 Evaluation of Processing Time

Figure 5, provides the processing analysis time over conventional SecLEACH, which is based on clustering normal technique over the proposed MSTREE using cluster head and selected process. Likewise, the technique of encryption provides a very high number of possibilities iteratively based on routing information with node id for identification of attacks as and even we don't compromise the proposed stolen attack is compared over SecLEACH.

Hence, time computation is higher in computation time over processing time.

The proposed MSTREE at the starting stage of processing the logic of single value approximation, for improving the processing time it goes not show improvement around two hundred rounds of simulation of which 1100 rounds are done to simulate.

As multi-level approximation logic is gained by re-adjusting the topology matrix of adjacency to reduce the redundancy of data migration. Hence MSTREE performs better in flexibility both in energy and at security level too.

5. Conclusion

Security ensuring is the challenging issue related to efficiency of energy which has very less investigation in WSN. The basic issues are related to security and energy efficiency effectiveness based on topology and sensor node balance. To evaluate the issue, we propose a STREE routing hierarchical protocol which mitigate the issues of security and energy in a very large scale networks.

The unsettled network in wireless sensor network related to energy and balance is done approximately using cryptographic analysis, this method developed provides security related to Sybil and lethal attacks made on nodes. This method addresses the issues of routing and energy. The multi-level tree routing provides provides a balance in energy and routing and take care of security issues in routing the structure topology. The algorithm is compared with the existing SecLEACH protocol which preserves energy and provides security better compared to other in processing time and deviation. The future work can be extended in considering the delay routing technique based on worm hole and etc.

References

[1] I. M. M. El Emary, S. Ramakrishnan, 'Wireless Sensor Networks: From Theory to Applications', CRC Press, Computers, 799 pages, 2013

[2] V. C. Gungor, G.P. Hancke, "Industrial Wireless Sensor Networks: Applications, Protocols, and Standards", CRC Press, Computers, 406 pages, 2013.

[3] Allen, Christopher, and Tim Dierks. "The TLS protocol version 1.0." The Internet Society, RFC 2246, 1999.

[4] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM, no. 2 pp. 120-126, 1978.

[5] I. Dubrawsky, "How to Cheat at Securing Your Network", Syngress, Computers, 432 pages, 2011.

[6] Kohl, John T., B. Clifford Neuman, and Y. Theodore. "The evolution of the Kerberos authentication service." IEEE Computer Society, 1994

[7] X. Chen, Z. Dai, W. Li, and H. Shi, "Performance Guaranteed Routing Protocols for Asymmetric Sensor Networks", IEEE Transactions OnEmerging Topics In Computing, Vol.1, No. 1, June 2013.

[8] D. Takaishi, H. Nishiyama, N. Kato, R. Miura, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks", IEEE Transactions on Emerging Topics In Computing, Vol.2, No.3,September 2014.

[9] Md.N. Rahman, M A Matin, "Efficient Algorithm for Prolonging Network Lifetime of Wireless Sensor Networks", IEEE- TsinghuaScience And Technology, Vol.16, No.6, December 2011.

[10] J.He, S. Ji, Y. Pan, Y. Li, "Reliable and Energy Efficient Target Coverage for Wireless Sensor Networks", IEEE- Tsinghua Science AndTechnology, Vol.16, No.5, October 2011.

[11] F. Li and P. Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things", IEEE SensorsJournal, Vol. 13, No. 10, October 2013.

[12] Y. Cho and G. Qu, Y. Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks", IEEE Symposium on Security and Privacy Workshops, DOI 10.1109/SPW.2012.32 134, 2014.

[13] J.N Long, M. Dong, K. Ota, and A. Liu, "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks", IEEE-Access, Vol.2, 2014.

[14] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocols for Wireless Microsensor Networks", Proceedings of the 33rd Hawaaian International Conference on Systems Science (HICSS), January 2000.

[15] M.F. Balcan_ A. Blum, A. Gupta, "Approximate Clustering without the Approximation", Proceedings of the twentieth Annual ACM-SIAMSymposium on Discrete Algorithms, pp. 1068-1077, 2009.

[16] M. Lehsaini, H. Guyennet, and M. Feham, "CES: Cluster-based Energy-efficient Scheme for Mobile Wireless Sensor Networks", Springer-IFIPInternational Federation for Information Processing, Vol.264; pp. 13–24, 2008.

[17] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, A. A. F. Loureiro, "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", Proceedings of the Fifth IEEEInternational Symposium on Network Computing and Applications,pp.145-154, 2006.