International Journal of Future Generation Communication and Networking
Vol. 9, No. 10 (2016), pp. 227-236
http://dx.doi.org/10.14257/ijfgcn.2016.9.10.20

Routing Algorithms for Wireless Sensor Network Based on the Mechanism of Energy Threshold Self-Partition

Qin Meng[1] and He Guoping[2]

[1]*Linyi University, Linyi, 276000, China*
[2]*shandong academy of sciences, Shandong, jinan,250014*
E-mail: qinmeng2004@163.com

Abstract

Based on low energy consumption and high privacy protection required by range query in two-level wireless sensor network, this paper proposes a kind of secure probabilistic range query (SPRQ). SPRQ is made up of data encryption, prefix member verification and probabilistic neighbor verification and spate query and transmission process. It can ensure completing range query without disclosing privacy. The analysis and simulation result indicate that compared with other safety agreement, SPRQ has lower energy consumption when it ensures the safety of range query.

Keywords*: Wireless sensor network; Energy aware; Query; Energy consumption; Privacy protection agreement*

1. Introduction

With the constant application and development of Wireless Sensor Networks (WSNs), data query task on it is more and safety requirement I data query process is more important. WSNs data query can gather part of effective data or specific data collected by WSNs to Sink (sink node) rapidly. Then, Sink analyzes and computes query result so as to control WSNs or make other decisions. There are two big types of WSNs data query. One is simple query. Conduct simply query operation for WSNs collected data. At present, the research focus is mainly range query, Top-k query, skyline query and based type query. These queries are simple and have strong universality. It can be adaptable to different WSNs, so it has better research value; the other is complicated query. The query process is complicated. It needs special query strategy and the universality is not strong. It is usually for certain WSNs. WSNs data query is widely used for military, environment, medical care, commerce and emergent scene, *etc*. so the safety must be fully assured. WSNs has the energy limitation bottleneck, in order to ensure long enough life cycle, it should realize safety performance in the case of consuming energy as lower as possible. WSNs range query is data query of inquiring data with range. The query is simple and practical. It's used widely and it has guidance meaning on other simple queries. This paper proposes a kind of SPRQ based on WSNs. It ensures query privacy through prefix member verification technology [1-2] and verifies the completeness of query result by utilizing probabilistic neighbor verification technology [3]; separates query process from transmission process as far as possible to reduce traffic (reduce energy consumption) and strengthen the applicability of WSNs.

2. Network Model

WSNs SPRQ, namely privacy protection research is mainly based on two-level wireless sensor network model [10] (Diagram 1), there is no exception for range query. SPRQ is an agreement based on this model.

ISSN: 2233-7857 IJFGCN

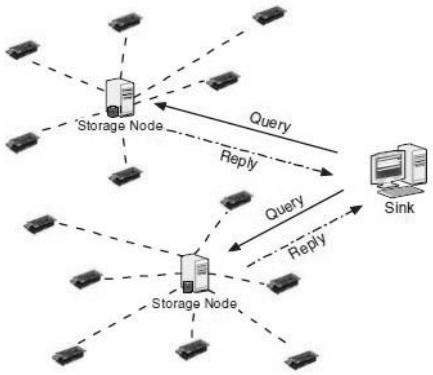

Diagram 1. Two-level Wireless Sensor Network Model

As is shown in Diagram 1, high level of network model is made up of storage node. Storage node is sensor node with bigger storage space and stronger computing power; bottom level is made of a large quantity of common sensor nodes. Common node resources are limited and the cost is low. Data query process is as follows: query requirement of users is transmitted to storage node through Sink, common node collects data, transmits data to storage node for storage and then make query computation on storage node. At last, reply the qualified query result to Sink and return to users in the end.

There are following advantages for WSNs to select two-level model: ① common sensor node just transmit the collected data to nearby storage node rather than Sink node via long path. It reduces energy consumption greatly and avoids Sink node encountering traffic bottle neck. ② Sink only communicate with storage node and can get query result. This makes query process more efficiently.

3. WSNs SPRQ (Secure Probabilistic Range Query)

For WSNs, energy consumption is usually the handicap of considering whether to take safety strategy or not. The objective of SPRQ is to reduce the energy consumption as far as possible at the time of ensuring safety of query.

3.1. Key Technology

3.1.1. Data Encryption: In SPRQ, every common sensor node *si* will share a secret key *ki* with Sink and *ki* is replaced regularly. Data *d1,⋯,dn* collected by common node are encrypted by *ki* in the process of query. Even if it completes query process, collect query result and upload to storage node of Sink, it cannot get specific data information either. Thus, it ensures privacy of data.

3.1.2. Prefix Member Verification: In the case that storage node cannot identify specific data, but it still need complete query process, so it need apply prefix member verification technology.

Prefix member verification technology translate the condition that whether verification data conforms to range query into comparison of data item. For example, whether 12 conforms to the range query [11, 15]. Binary representation of 12 is expressed as 1100. Firstly, construct prefix family, get {1100 110* 11** 1*** ****}, then quantize prefix and get {11001 11010 11100 11000 10000}; Meanwhile, binary representation of [11, 15] is expressed as [1011,1111], namely {1011 1100 1101 1110 1111}. Firstly, prefix and get {1011 11**}, then quantize prefix and get {10111 11100}. In the final prefix quantization group, if they have the same item 11100, it indicates that data 12 conforms to range query

[11, 15]. Or else, if there is no the same data item, it indicates that the data doesn't conform to the condition of range query.

In SPRQ, prefix member verification technology is applied to three hash functions. Three hash functions are Φ, Ψ and Ω respectively.

3.1.3. Probabilistic Neighbor Verification: The query result completeness verification of SPRQ is realized through probabilistic neighbor verification. That is, after common node *si* gets query result, generate message (*t,i,len*)), and transmit this message to nearby neighbor node. Of them, *t* is time slot, *I* is sensor No., *l* is the number of data item satisfying the query. Then for each neighbor node, add (*t,i,len)* to self-query result with certain probability *p* at random and upload with encryption. After receiving query result, Sink verifies query result completeness according to each (*t,i,len*).

3.2. SPRQ One-dimensional Data Query Process: According to the different dimensions of data items, WSNs range query can be classified as one-dimensional data query and multi-dimensional data query. One-dimensional data query process is simplest. With the increasing of dimension, energy consumption of multi-dimensional data query usually increases exponentially. SPRQ should avoid this situation as far as possible and improve energy consumption state of different dimensions.

The specific realization process of algorithm in this paper is expressed with pseudo code, called Algorithm 1:

Algorithm 1 Low communication cost data storage algorithm of unattended operation sensor network

Input: k no. of source data package Xv, $v = 1,\ldots, k$.

Output n No, of storage data package Yu, $u = 1,\ldots, n$.

Start

1: Initialization phase

2: For each data node v = 1to k

3: Add overhead bit rate, *IDv* No. and oriented random walk step number counter variable N for source data package X; set original value $N = 0$；

4: For each data node u = 1to n

5: Initialize the value of each storage data package: $Yu = 0$；

6: Initialize the current times of each source data package Xv and access node u: $cv(u) = 1$；

7: Distributed storage phase

8: For each data node v = 1to k

9: Receive X according to probability $a\ln k/k$ and update self storage data package: $Yv = Yv \oplus Xv$；

10: Transmit source data package X to one neighbor node according to oriented random walk rule

11: $cv(v) = cv(v) + 1$；

12: For each data node u = 1to n

13: For source data package Xj arriving at node u

14: If Xj accesses node u for the first time

15: For node u , receive X according to probability $a\ln k/k$ and update self storage data package: $Yu = Yu \oplus Xj$；

16: $cj(u) = cj(u) + 1$；

17: $N = N + 1$；

18: If $N < cn$,

19: Node u transmits source data package X to one neighbor node according to oriented random walk rule

20: Else

21: Node *u* discards *Xj*；

End

There are two important parameters in Algorithm 1: one is oriented random walk step number, namely the times of each source data package transmitted in network. It is set up in Algorithm 1 as *cn*, counted with variable *N*; whenever one time transmitted by data package, the value of *N* will plus 1. When $N > cn$, source data package is discarded, no longer transmitted. Another parameter is the probability that each node receives a newly arrived source data package. It is set up in Algorithm 1 as $a\ln k/k$. These two parameters have important impact on the performance of algorithm. Specific analysis will be below:

After completing Algorithm 1, none source data package will be stored in network. Each node stores a storage data package.

Specific query details are as follows:

① Common node *si* receives certain data, sorts them and gets *d1,⋯,dn,*, applies the first hash function Ψ to encrypt them, get fixed message code $\Psi(d1,\cdots,dn)$ and send it to storage node. When Sink wants to query $\{t,[a,b]\}$, it will use another function Ω to process query range and then send $\{t, \Omega([a,b])\}$ to storage node.

② When storage node processes query, it uses the third function Φ. When $\Phi(j, \Psi(d1,\cdots,dn), \Omega([a,b]))$ is true, it indicates *dj* meets the query condition; if it is false, it indicates that *dj* cannot meet the query condition, so it should be discarded. Storage node feedbacks the minimum data and maximum number and data quantity *(min_d,max_d,len)I* to *si*.

③ After *si* receiving feedback result, find out all intermediate data *dmin_d,⋯,dmax_d* including number *min_d* and *max_d* in queue, add *dmin-1* (if *min_d-1*<1 , then *dmin_d-1* =-1), (if *max_d+1>n* , then *dmax_d+1* =∞). *si* generates message *(t,i,len)* and transmit the message to nearby neighbor nodes. Of them, *t* is time slot, *I* is sensor number, *len* is data times meeting the query.

④ If *si* receives message *(t, i_neighbor,len)* sent by neighbor node si_neighbor, it will add this message to query result needed to upload with a certain probability *p*. That is uploading *{(t, i_neighbor,len)p,dmin_d,⋯,dmax_d} ki* finally. Of them, *ki* is shared secret key of *si* and Sink.

The uploaded data passes through storage node and arrives at Sink. Sink verifies the completeness of all query results. So far, SPRQ comes to an end.

3.3. SPRQ Multi-dimensional Data Query Process

In actual application, range query is usually for multi-dimensional data, so it's necessary for SPRQ agreement applied to multidimensional data query. SPRQ multidimensional query process is briefly described below:

① Common node *si* receives n No.s of m-dimensional data *(d11,d12,⋯,d1m),⋯,(dn1,dn2,⋯,dnm)*, applies the first hash function Ψ to encrypt them, get fixed message code $\Psi(d11,\cdots,dn1)$, $\Psi(d12,\cdots,dn2)$, $\Psi(d1m,\cdots,dnm)$and send it to storage node. When Sink wants to query $\{t,([a1,b1],\cdots,[am,bm])\}$, it will use another function Ω to process query range and then send $\{t, \Omega([a1,b1]), \cdots\Omega([am,bm])\}$ to storage node.

② When storage node processes query, it uses the third function Φ. When$\Phi(j, \Psi(d1t,\cdots,dnt), \Omega([at,bt]))$ is true (of them, $1=<t<=m$), it indicates *dj* meets the query condition in dimension *t*; if it is false, it indicates that *dj* cannot meet the query condition in dimension *t*, so it should be discarded. After completing all dimensions, intersection with the number will get final query result, and storage node number these data meeting query condition with *{(min_d1,max_d1),⋯, (min_dm,min_dm),len}I* and feedbacks them to *si*.

In query process, *si* sorts uploaded data as per random value of certain dimension. After receiving feedback result, find out all data conforming to condition according to query result and encrypt them.

The query process of ③ and ④ is the same as one-dimensional data query.

4. Performance Analysis

4.1. Safety Analysis

The data quantity of common node is small. If it is trapped, the impact on global query is not great, so it mainly consider the situation after storage node is trapped, for this reason, to verify the safety performance of SPRQ.

Query result has been encrypted, so storage cannot gain effective query data after trapped. The trapped storage node can discard data and change query result (*min_d,max_d,len*). These two damages can be detected by sink in completeness verification.

4.2. Energy Consumption Analysis

Compared with previous range query agreement, SPRQ has some improvement. One reason is the result of separating query process from transmission query result process. Thus, the data disagreeing with condition will not be uploaded on storage node. It reduces a great number of data transmission quantities. That is, reducing energy consumption that common node sends data as well as reducing energy consumption needed by storage node to receive data. It reduces energy consumption of secure range query obviously.

4.3. Simulation Experiment

This paper uses original data set to simulate SPRQ and SafeQ on MATLAB platform. There are 100 common nodes distributed at random in the area of 300mm wide x 300mm long and 4 storage nodes are distributed evenly. There is a Sink node in the middle. Suppose effective transmission distance of sensor node is 75m. By utilizing TAG algorithm to set up route path, it takes 1.8 jump for each common node to transmit data to storage node. There are average 20 neighbor nodes and the probability of sending verification message to each neighbor node is 0.4. In simulation experiment, energy consumption value means specific energy consumption divides by time, namely a value to weigh energy consumption level similar to power; effective query ratio is the proportion of effective data quantity of final query result on storage node and energy consumed. It reflects the utilization rate of agreement network energy.

The experiment mainly makes contrast of energy consumption of different dimensional data queried by SPRQ and SafeQ. In order to guarantee the correctness of experimental result, all experiments apply the same actual data set. One-dimensional data set and two-dimensional data set are one dimension and two dimensions stripped from three-dimensional data set. That is, the query result data item quantity received by different-dimensional experiments in the unit time should be the same.

4.3.1. One-dimensional Data Query: The first group experiment is the contrast situation of energy consumption by SPRQ and SafeQ in one-dimensional data query state.

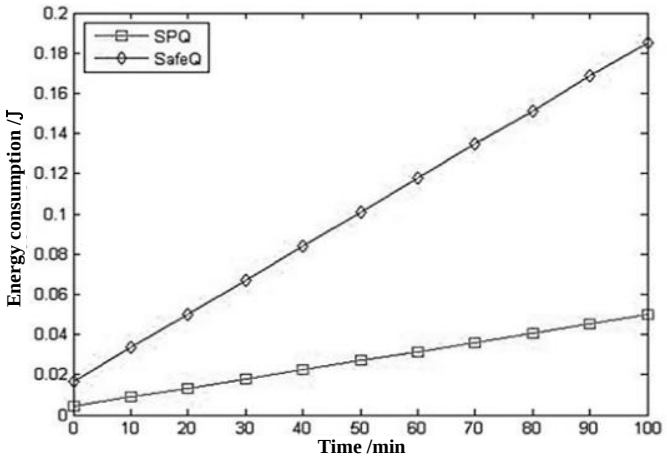

Diagram 2. Average Energy Consumption Contrast of Common Node Queried by One-dimensional Data

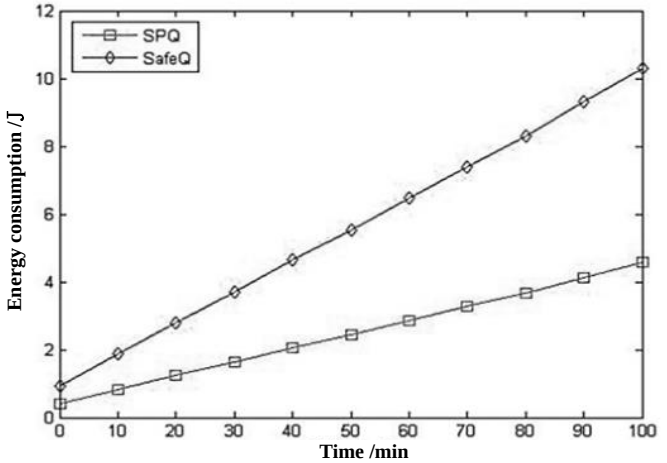

Diagram 3. Average Energy Consumption Contrast of Storage Node Queried by One-dimensional Data

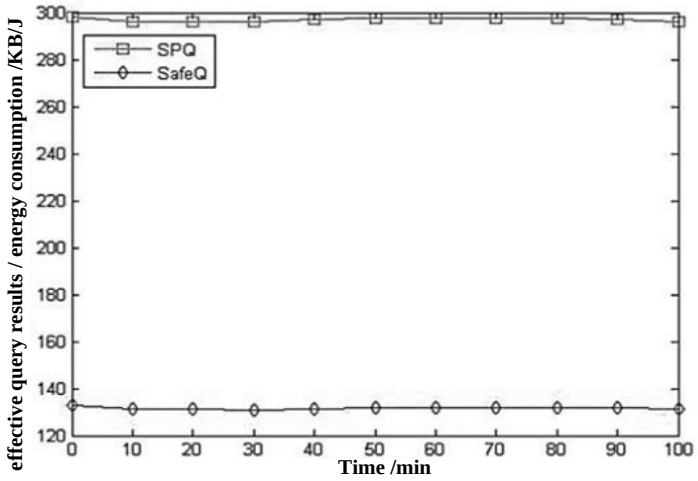

Diagram 4. Contrast of Effective Query Ratio Queried by One-dimensional Data

Through experimental result diagram, it could be say that, for one-dimensional data query, in the situation of the same data set source, energy consumption value of common node by SPRQ is 3.2 times lower than that by SafeQ; energy consumption value of storage node by SPRQ is 2.5 times lower than that by SafeQ. Effective query ratio of SPRQ is 2.2 times of SafeQ. In the situation of one-dimensional data, SPRQ energy consumption level is lower than SafeQ obviously.

4.3.2. Multi-Dimensional Data Query: The second group experiment is the contrast situation of energy consumption by SPRQ and SafeQ in multi-dimensional data query state (this experiment uses three-dimensional data).

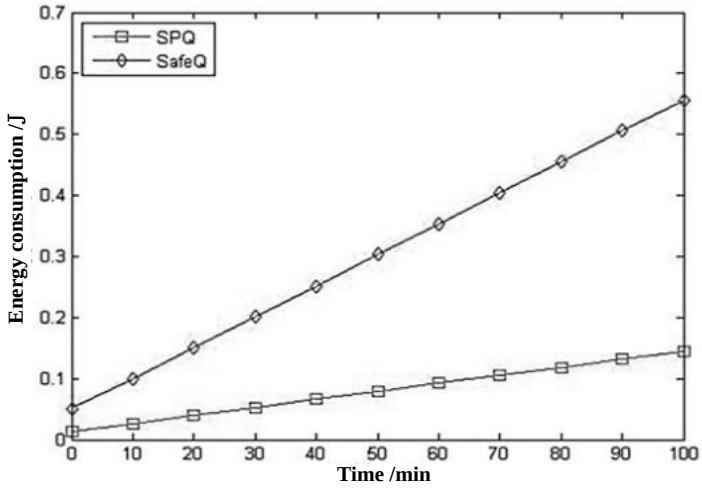

Diagram 5. Average Energy Consumption Contrast of Common Node Queried by Three-dimensional Data

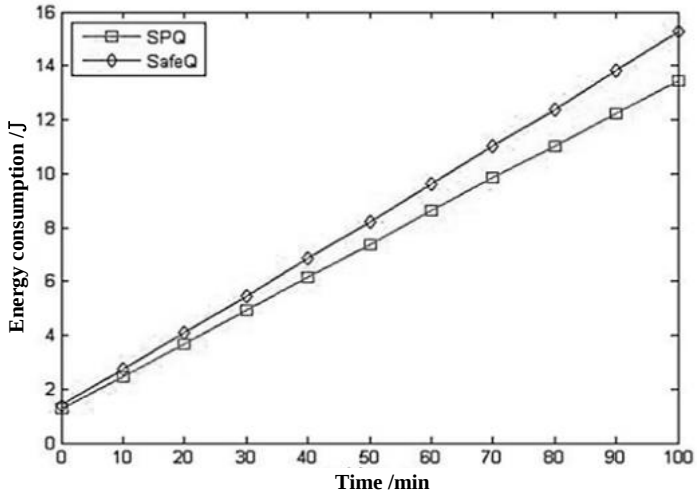

Diagram 6. Average Energy Consumption Contrast of Storage Node Queried by Three-dimensional Data

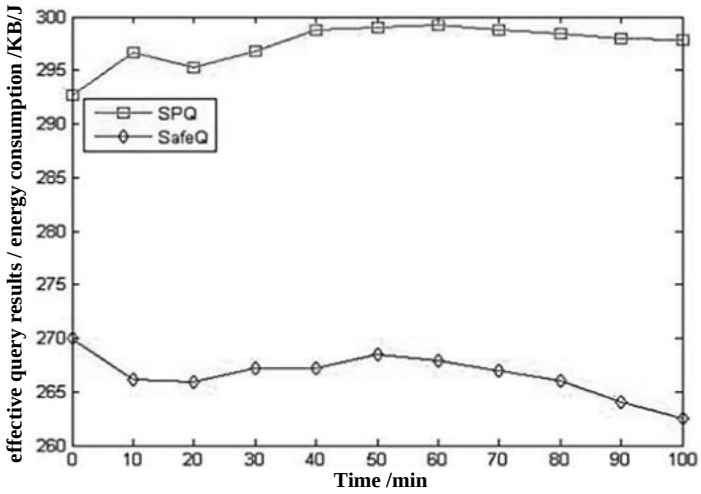

Diagram 7. Contrast of Effective Query Ratio Queried by Three-dimensional Data

Through experiment 2 result diagram, it could be say that, for three-dimensional data query, in the situation of the same data set source, energy consumption value of common node by SPRQ is 3.64 times lower than that by SafeQ; energy consumption value of storage node by SPRQ is 1.17 times lower than that by SafeQ. Effective query ratio of SPRQ is 1.1 times of SafeQ. In the situation of one-dimensional data, SPRQ energy consumption level is lower than SafeQ obviously.

4.2.3. Different Dimensional Data Query Comparison: The second group experiment is the contrast situation of energy consumption by SPRQ and SafeQ in different-dimensional data query state.

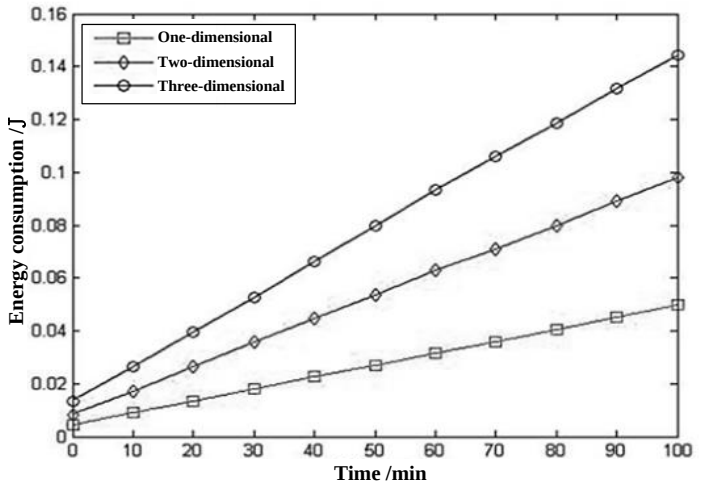

Diagram 8. Average Energy Consumption Contrast of Common Node Queried by Different-Dimensional Data

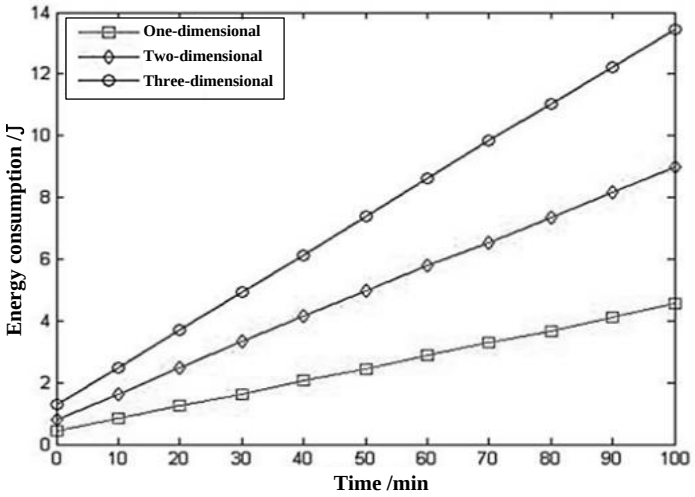

Diagram 9. Average Energy Consumption Contrast of Storage Node Queried by Different -Dimensional Data

Through result diagram contrast, it could be say that in the situation of the same data set source, when querying three kinds of dimensional data, the energy consumption of SPRQ common node appears linear growth; when querying three kinds of dimensional data, the energy consumption of SPRQ storage node appears linear growth. That is, in the situation of multi-dimensional data query, energy-saving power of SPRQ is outstanding as well.

5. Conclusion

Data privacy protection of SPRQ agreement proposed in this paper will be realized through prefix member verification technology. Data completeness verification is mainly completed by probabilistic neighbor verification. In addition, it takes a series of communication strategy to reduce traffic, namely energy consumption to make it superior to current SafeQ and range query based on barrel mode. Compared with current agreement, the energy consumption of SPRQ is lower and the safety performance is better, but compared with query strategy without privacy protection, energy consumption is still higher. It needs seek for safety strategy or communication method further to reduce energy consumption so that safety data query can be promoted better.

References

[1] J. Hu and Z. Gao, "Modules identification in gene positive networks of hepatocellular carcinoma using Pearson agglomerative method and Pearson cohesion coupling modularity", Journal of Applied Mathematics, **(2012)**.
[2] D Jiang, Z. Xu and Z. Chen, "Joint time-frequency sparse estimation of large-scale network traffic", Computer Networks, vol. 55, no. 15, **(2011)**, pp. 3533-3547.
[3] J. Hu, Z. Gao and W. Pan, "Multiangle Social Network Recommendation Algorithms and Similarity Network Evaluation", Journal of Applied Mathematics, **(2013)**.
[4] M. Zhou, G. Bao, Y. Geng, B. Alkandari and X. Li, "Polyp detection and radius measurement in small intestine using video capsule endoscopy", 2014 7th International Conference on Biomedical Engineering and Informatics (BMEI), **(2014)**.
[5] G. Yan, Y. Lv, Q. Wang and Y. Geng, "Routing algorithm based on delay rate in wireless cognitive radio network", Journal of Networks, vol. 9, no. 4, **(2014)**, pp. 948-955.
[6] Y. Lin, J. Yang and Z. Lv, "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things", Sensors, vol. 15, no. 8, **(2015)**, pp. 20925-20944.
[7] K. Wang, X. Zhou and T. Li, "Optimizing load balancing and data-locality with data-aware scheduling", Big Data (Big Data), 2014 IEEE International Conference on. IEEE, **(2014)**, pp. 119-128.

[8] L. Zhang, B. He and J. Sun, "Double Image Multi-Encryption Algorithm Based on Fractional Chaotic Time Series", Journal of Computational and Theoretical Nanoscience, vol. 12, **(2015)**, pp. 1-7.
[9] T. Su, Z. Lv and S. Gao, "3d seabed: 3d modeling and visualization platform for the seabed", Multimedia and Expo Workshops (ICMEW), 2014 IEEE International Conference on. IEEE, **(2014)**, pp. 1-6.
[10] Y. Geng, J. Chen, R. Fu, G. Bao and K. Pahlavan, "Enlighten wearable physiological monitoring systems: On-body rf characteristics based human motion classification using a support vector machine", IEEE transactions on mobile computing, vol. 1, no. 1, **(2015)**, pp. 1-15.
[11] Z. Lv, A. Halawani and S. Feng, "Multimodal hand and foot gesture interaction for handheld devices", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11, no. 1s, **(2014)**, p. 10.
[12] G. Liu, Y. Geng and K. Pahlavan, "Effects of calibration RFID tags on performance of inertial navigation in indoor environment", 2015 International Conference on Computing, Networking and Communications (ICNC), **(2015)**
[13] J. He, Y. Geng, Y. Wan, S. Li and K. Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", IEEE Sensor Journal, vol. 13, no. 10, **(2013)**, pp. 3826-3836.
[14] W. Huang and Y. Geng, "Identification Method of Attack Path Based on Immune Intrusion Detection", Journal of Networks, vol. 9, no. 4, **(2014)**, pp. 964-971.
[15] X. Li, Z. Lv and J. Hu, "XEarth: A 3D GIS Platform for managing massive city information", Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on. IEEE, **(2015)**, pp. 1-6.

Authors

Qin Meng, he received her M.S. degree in software engineering from Shandong University of Science and Technology, China. He is currently a lecturer in the Linyi University. He research interest is mainly in the area of Computer Software, Mechanical and Electrical Integration. He has published several research papers in scholarly journals in the above research areas.

