On the Access Control Mechanism of Wireless Sensor Network

https://doi.org/10.3991/ijoe.v13i03.6862

Xiajun Ding
Quzhou University, Quzhou, China
dxj_yl@163.com

Xiaodan Jiang
Quzhou University, Quzhou, China
16282409@qq.com

Hongbo Bi
Quzhou University, Quzhou, China
174621403@qq.com

Jianwen Fang
Quzhou University, Quzhou, China
279679994@qq.com

Abstract—This paper puts forward an approach of access control based on unidirectional chain. For the purpose of increasing the number of users, improving the expandability of access ability, and resisting the attacks aiming at capturing users, the author proposes new methods of access control and a user access ability revocation based on the hash tree. Through analysis, evaluation and comparison, the author concludes that these approaches and methods require smaller computation, storage and communication overheads than the existing sensor network access control methods. Moreover, the proposed approaches and methods are able to resist node capture, as well as information replay requests and attacks.

Keywords—wireless sensor; access mechanism; user capture; hash tree

1 Introduction

As an important tool in the field of environmental testing, the sensor network can be used to monitor the environment, store the acquired data and offer environmental monitoring data to users [1]. To safeguard the access security of the network, it is of great necessity to set up proper access control mechanism [2]. Such a mechanism can prevent illegal access, which is an existential threat to the very safety of the sensor. In the absence of a proper access control mechanism, illegal intruders may use the sensor node to destroy network services [3]. To address the problem, effective access

control and access rights management mechanism are required for they lay the foundation for network access security.

In practical use, access control is of critical importance for the sensor network [4]. The access control mainly verifies the legitimacy of users and transfers the qualified users' request to the network server terminal. In the civilian areas, the sensor network is mainly used to provide users with environmental information request service. However, only the users with certain rights are allowed to send a request and get a response [5-6]. Similarly, in the military field, only the certified, acceptable military communication equipment is permitted to request sensor network services. The server terminal would issue the response signal after receiving the request. Nevertheless, there is a problem with the existing access control mechanism [7]. Relying on public key authentication, the mechanism imposes strict restrictions on resources, features low safety level, and consumes a lot of resources in the accessing process. Vulnerable to illegal attacks, the network access control mechanism is in urgent need of improvement.

The sensor network access control operates under the principle of pre-allocating the authentication information for each node. Based on such information, the sensor network can verify the users' identities when providing the access service. If the users pass the authentication, the network would accept the access request and provide corresponding services.

2 The service provision architecture of the sensor network

The server network is frequently applied to the field of monitoring. The cornerstone of the network architecture is a central server that provides one-to-many services [8-9]. The specific structure of the network is displayed in Figure 1.

The central server has the following main functions: allocating the authentication information for each node, configuring the access rights, and managing the entire network [10]. Any terminal accessing to the sensor network can be viewed as a user. Common terminals include tablet computers, smart phones, etc. To obtain necessary services, the users with access rights should send a request to the network.

3 The sensor network access control mechanism based on one-way key chain

3.1 The access control based on a single key chain

Among the various ways of network access control, the one-way key chain method mainly assigns each sensor node with the head of the key chain [11]. The users are allowed to send a service request with these keys after obtaining a certain number of keys. The sensor nodes then authenticate the users based on the pre-assigned keys, ensuring that they have the proper access rights. If the authentication is passed, the sensor network will respond to the request or reject it otherwise.

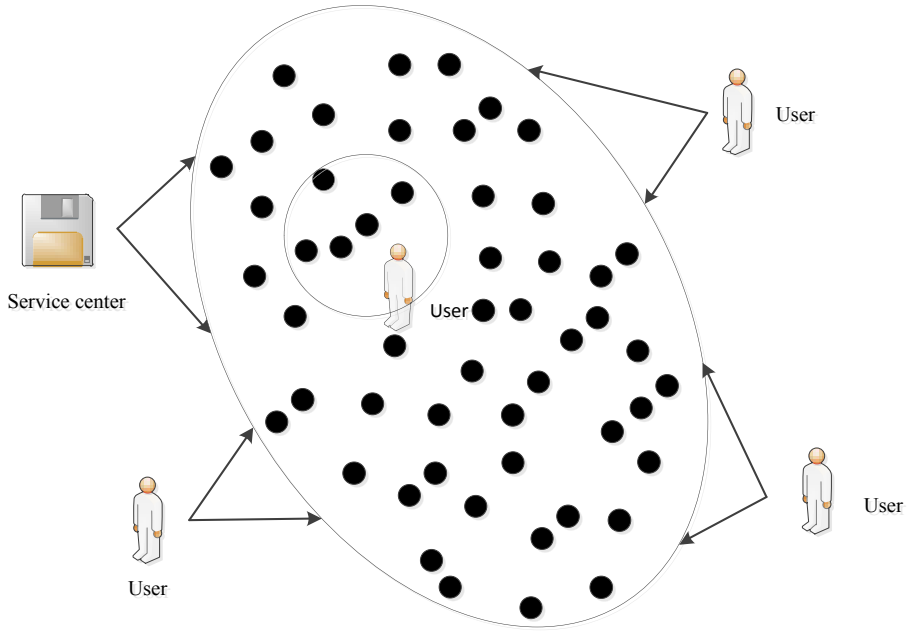

Fig. 1. The architecture of sensor network service

The keys are assigned in the following manner: generate a one-way key chain $K_0,\ldots, K_n$ of length n (Figure 2), randomly select the last key K_n in the chain using the central server, calculate KJ=F(j+1) by the one-way function F, and assign the corresponding head K0 to each node. Figure 2 displays how to generate the one-way key chain of length n.

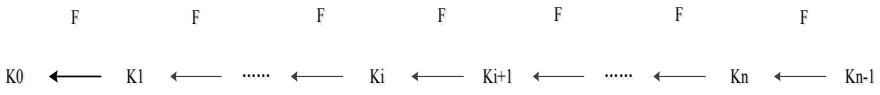

Fig. 2. One-way key chain

Based on a single key chain, the access control is not complex. See Figure 3 for more details.

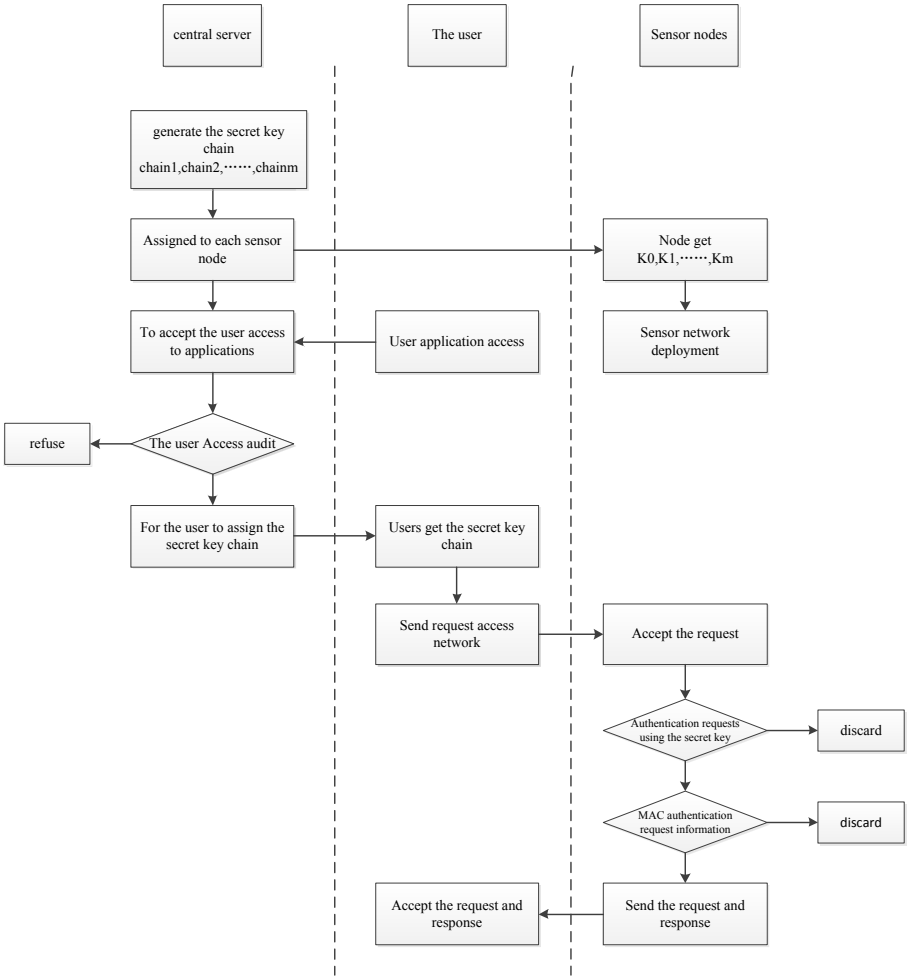

Fig. 3. The process of access control based on the single key chain

3.2 The access control based on multiple key chains

The previously mentioned mechanism controls the access based on a single key chain. In that case, only a single user is allowed to access the network. To make up for the defect, the access control mechanism based on multiple key chains has been invented, for which all key chains are independent from each other so that several users can issue requests concurrently.

The sensor network is often accessed by only a few dozens of users. Normally speaking, the users issue fewer than ten access requests. Suppose there are m one-way key chains in the access control mechanism, m users are permitted to request access simultaneously.

Under this mechanism, the central server generates a cluster of m key chains of length n in the same way as the previously mentioned mechanism. The specific process is illustrated in Figure 4.

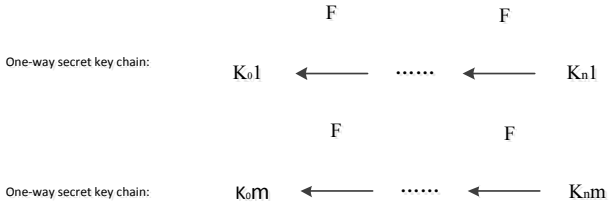

Fig. 4. The cluster of one-way key chains

See Figure 5 for the access control process based on multiple key chains.

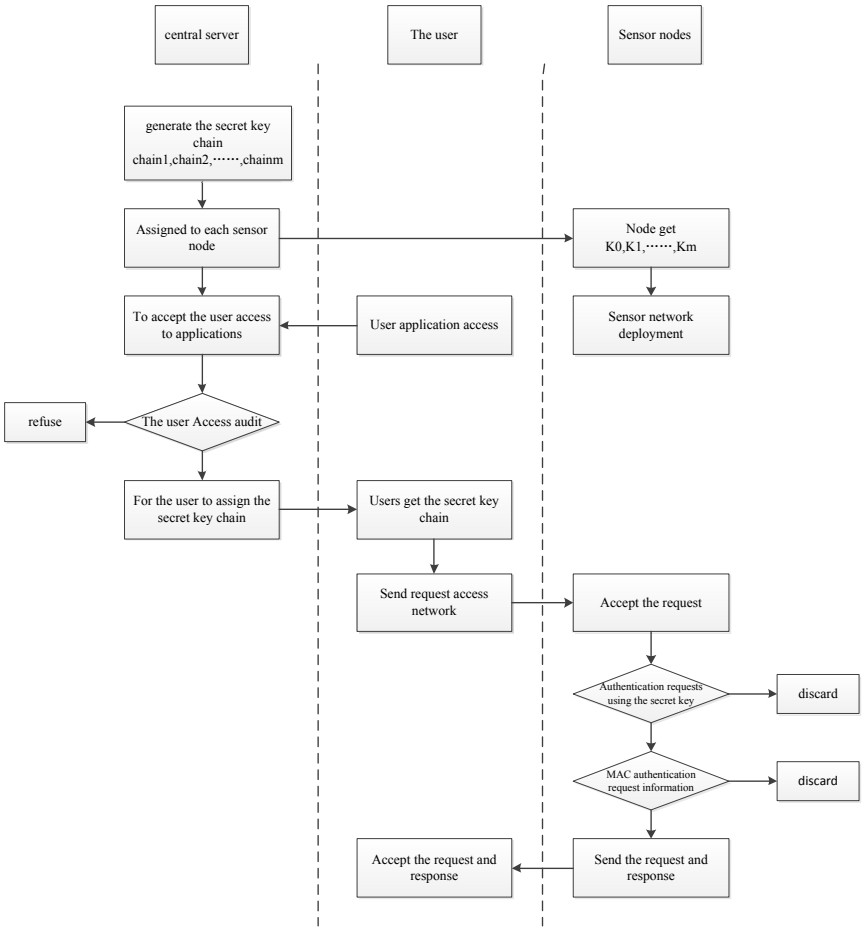

Fig. 5. The process of access control based on multiple key chains

3.3 Expandable Merkle hash tree access control

This access control mechanism is realized with the Merkle hash tree. For better expandability, the Merkle hash tree should have several layers. In this paper, two layers are adopted. The upper layer involves root assignment tree, and the lower layer, the head assignment sub-trees. The trees and sub-trees on both layers have corresponding leaf nodes. The leaf nodes function differently from layer to layer. Those of the upper layer mostly distribute root node information of each head assignment sub-tree of the lower layer. The information will be used during the authentication of users. In contrast, those of the lower layer distribute the head of each key chain, providing support to the identity authentication.

The central server usually generates far more key chains than the number of users. To facilitate the management, the key chains are divided into m groups. The grouping process goes as follows: suppose that the total number of key chains $m`=2^k$, obtain a number of head assignment sub-trees of the lower layer in a similar manner as described above with these key chains, and set up the root assignment trees of the upper layer based on the hash value of the root information corresponding to the sub-trees. Figure 6 is about the steps of the process.

Some more preparations are needed to authenticate users based on a group of key chains. The central server needs to assign the roots of the hash trees obtained on the basis of the group to each sensor node, and also the root allocation certificate. After receiving the certificate information, a sensor node will perform authentication according to the pre-set hash tree root certificate. In other words, the sensor node will verify the consistency between the roots of the actual assignment trees and the pre-assigned roots. The certificate should be deemed as legal if the actual roots are in line with the pre-assigned ones and be rejected if otherwise. If the certificate is accepted, the sensor node will extract the roots of sub-trees from the certificate and provide the corresponding services.

In order to access the network, the user is required to send the head assignment certificate of the corresponding key chain to the sensor node. After the sensor node identifies the head of the key chain from the certificate, the user will be able to access the network via the key chain. If the key chain obtained by the user conforms to the corresponding certificate, the user will pass the authentication. The key chain certificate is assigned in the following steps:

1. The user broadcasts the certificate $CDCertp_q$ to the sensor network.
2. Upon receiving the certificate, the network verifies the authenticity of the certificate in light of the root of the p-th Merkle sub-tree on the bottom layer. If the certificate is authentic, the network will extract the head of the key chain in the certificate. If not, the certificate will be discarded. The authentication compares the root obtained from the certificate and the root of the Merkle sub-tree. If the two are the same, the certificate should be regarded as legal. Otherwise, it should be discarded.

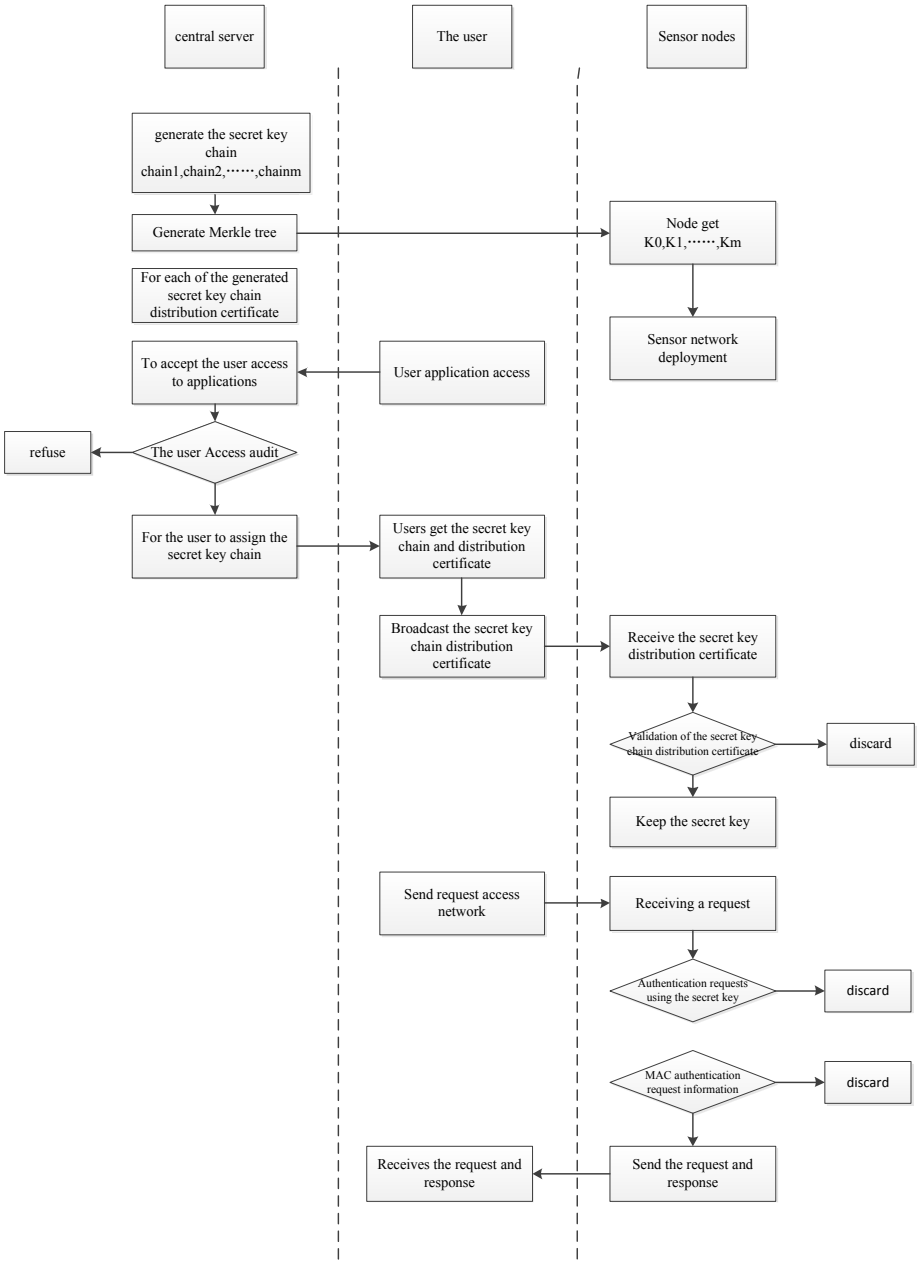

Fig. 6. The process of the access control based on Merkle tree

4 The analysis and comparison between different sensor network access control mechanisms

4.1 The access control based on a single key chain

Each of the above access control mechanisms has its own advantages/disadvantages and scope of application. Comparatively speaking, the access control based on a single key chain has much smaller overhead than that of the public key control mode. The former mechanism primarily relies on symmetric key calculation, in which the sensor node verifies the legitimacy of the user's request. This requires very simple interaction and a few communication overhead. Since the sensor node only needs a key and the ID of the key, there is a very small demand for storage space and highly efficient request verification, leaving no need for cached information.

The security of the control mechanism based on a single key chain mainly depends on the security of the one-way key chain. Because the sensor node immediately verifies the legitimacy of the user's request, this mechanism effectively prevents the defect of the traditional mechanism, under which it is impossible to carry out verification immediately and likely to cause illegal attacks. More importantly, in the control mechanism based on a single key chain, each key in the key chains is discarded after a single use, a great boost to the resistance against node capture attacks as well as information replay requests and attacks. However, every silver-lining has a cloud. Under this access control mechanism, an illegal user may obtain the sub-key chain assigned to the user by the central server, and the network server is unable to judge the legitimacy of such a request. As a solution to the flaw, the central server should assign a short sub-key chain each time so as to reduce the chance for an attacker to send a false request.

The poor expandability is the major shortcoming of this access control mechanism. It is expressed in two forms: first, only one user is allowed to send an access request in each period of time due to the use of a single key chain; second, the length of the key chain is much longer than that of other mechanisms.

4.2 The access control based on multiple key chains

The access control mechanism based on multiple key chains is invented to overcome the defect of the mechanism specified in the preceding section. Under this mechanism, the access efficiency is much higher because the users can request sensor network services concurrently. Coupled with its high expandability, the mechanism is applied in many areas.

In comparison with the access control based on a single key chain, the mechanism consumes the same communication and computing overhead. However, it consumes much higher storage overhead and has to store every head corresponding to each key chain.

There is no difference between the security level of the access control mechanism and the previous one. Moreover, when one of the key chains is under attack, other key chains won't be affected for each key chain is kept independently.

Despite its relatively extensive application, the control mechanism is limited by the large storage space and the need of saving multiple heads.

4.3 The access control based on Merkle hash tree

This control mechanism enables the central server to manage users more conveniently and to support concurrent access by multiple users. A significant drawback is the resulting storage overhead. With the introduction of the Merkle hash tree, the cost of storage resources is greatly reduced because it is only necessary to save the heads of the key chains in use while the heads can be assigned via such trees for the use of other key chains.

Under this mechanism, the sensor node needs to assign a certificate to the head of each key chain, and the hash operation is required for each authentication. However, the computing overhead is not very high since the number of key chains is generally much smaller than the number of user requests. So, this mechanism has the same communication overhead with the previous one. Even if the assignment of chain head to sensor node leads to additional communication overhead, the amount of the increase is rather small. Generally speaking, the access control mechanism boasts a small overhead because each sensor node only needs to store a hash value and the head of the key chain.

The one-way functions F and H are the main influencing factors of the security of this access control mechanism. Under this mechanism, the sensor node makes immediate judgment after receiving the certificate information, and therefore resists Dos attacks very effectively. Before sending an access request, the user is assigned a key chain and head assignment certificate, two tools for network access. After issuing the access request, the security of access control won't be affected by the capture of sensor node, and the attack on one user won't impact other users' access.

The number of leaf nodes determines how many key chains to be assigned to the user. Hence, it is necessary to set a proper number of leaf nodes. If there are too many leaf nodes, the numerous parameters contained in the nodes will hike up the amount of data being transmitted in the network and affect the transmission efficiency. If there are too few leaf nodes, it will reduce the access flexibility.

4.4 Expandable Merkle hash tree access control

This mechanism requires the sensor node to store the root values of many sub-trees. Each sub-tree contains a number of key chains, and each key chain corresponds to several users. Thus, the sensor node will consume a much larger storage space if there are many users. Like other mechanisms, the computing overhead of this mechanism is also very small. For the convenience of analysis, the number of key chains is assumed to be $m=2^{i+j}$. Under basic access control, the hash operation should be conducted for $1+\log m=1+i+j$ times to verify the authenticity of the certificate, a proof of

the small computing load. In the expanded mechanism, however, all key chains are divided into groups. Thanks to the limited number of sub-trees, the verification overhead is not large. Hence, the overall computing load is not high.

In this way, the expandability of the hash tree access control mechanism is improved. The access flexibility is also significantly improved because the central server can assign more authenticated key chains to users under the same conditions. When it comes to security, the mechanism is about the same as the previous one.

5 Conclusion

Access control is one of the main functions of the sensor network. The control of access requests ensures the security of network access. In actual use, the existing access control mechanism based on public keys requires a lot of overhead and fails to resist attacks effectively, especially the denial of service attacks. To address the problem, this paper compares and analyzes several types of service access control, and puts forward an access control mechanism based on unidirectional chain. The comparison mainly focuses on the computing and communication overhead and security of every access control mechanisms. The results show that all of the mechanisms have higher overhead and security than the sensor mechanism. The access control mechanism based on multiple key chains is a suitable choice for reducing the overhead and improving the flexibility. Besides, this paper develops corresponding access control ability revocation mechanism, aiming at preventing false request from illegal attackers who steal the legal access certificate of legal users.

6 References

[1] Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G. J. (2000). Protocols for self-organisation of a wireless sensor network. *Personal Communications IEEE*, 7(5), 16--27. https://doi.org/10.1109/98.878532

[2] Akkaya, K., Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3), 325-349. https://doi.org/10.1016/j.adhoc.2003.09.010

[3] Alkaraki, J. N., Kamal, A. E. (2013). Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6), 6-28. https://doi.org/10.1109/MWC.2004.1368893

[4] Karlof, C., Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3), 293-315. https://doi.org/10.1016/S1570-8705(03)00008-8

[5] Ye, W., Heidemann, J., Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 12(3), 493-506. https://doi.org/10.1109/TNET.2004.828953

[6] Zhou, Z., Ai, Q. (2005). A new energy-efficient hierarchical clustering algorithm for wireless sensor networks. *Proceedings of SPIE - The International Society for Optical Engineering*, 6011, 81-91. https://doi.org/10.1117/12.633945

[7] Ye, M., Li, C., Chen, G., Wu, J. (2007). Eecs: an energy efficient clustering scheme in wireless sensor networks. *Journal of Frontiers of Computer Science & Technology*, 3(2-3), 99-119.

[8] Xue, L., Guan, X. P., Liu, Z. X., Zheng, Q. C. (2010). A power- and coverage-aware clustering scheme for wireless sensor networks. *International Journal of Automation and Computing*, 7(4), 500-508. https://doi.org/10.1007/s11633-010-0533-5

[9] Jadhav, P., Satao, R. (2016). A survey on opportunistic routing protocols for wireless sensor networks. *Procedia Computer Science*, 79, 603-609. https://doi.org/10.1016/j.procs.2016.03.076

[10] Bhattacharyya, D., Kim, T. H., Pal, S. (2010). A comparative study of wireless sensor networks and their routing protocols. *Sensors*, 10(12), 10506-10523. https://doi.org/10.3390/s101210506

[11] Yu, J., Qi, Y., Wang, G., Gu, X. (2012). A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. *AEU - International Journal of Electronics and Communications*, 66(1), 54-61. https://doi.org/10.1016/j.aeue.2011.05.002

7 Acknowledgement

This study was supported by the projects of Science Technology Department of Zhejiang Province (No.2015C33230) and Science Technology Department of Zhejiang Province (No. 2016C31097) and Quzhou Science and Technology Bureau (No. 2015Y005) and Quzhou University teachers team construction fund (No. XNZQ201311) and Open laboratory project of Quzhou University (No. KFXM201511).

8 Authors

Xiajun Ding was born in Zhejiang, China, in 1980. He works in College of Electrical and information engineering, Quzhou University Quzhou 324000, China, and received the Master's degree in 2005 from Anhui University of Science and Technology. His interesting field is intelligent information processing (dxj_yl@163.com).

Xiaodan Jiang was born in Zhejiang, China, in 1981. He works in College of Electrical and information engineering, Quzhou University Quzhou 324000, China, and received the Master's degree in 2010 from Zhejiang University of Technology. Now she is pursuing the PH.D degree in Zhejiang University of Technology, Her interesting field is image processing (16282409@qq.com).

Hongbo Bi was born in Heilongjiang, China, in 1984. He works in College of Electrical and information engineering, Quzhou University Quzhou 324000, China, and received the Doctor's degree in 2015 from Zhejiang University of Technology. His interesting field is iterative learning control (174621403@qq.com).

Jianwen Fang was born in Zhejiang, China, in 1972. He works in College of Electrical and information engineering, Quzhou University Quzhou 324000, China, and received the Doctor's degree in 2013 from Zhejiang University. His interesting field is intelligent information processing, image processing (279679994@qq.com).

Article submitted 13 February 2017. Published as resubmitted by the authors 09 March 2017.