An Embedded Dynamic Security Networking Technology Based on Quick Jump and Trust

Yong Hu*

Information Engineering Department, Chongqing College of Water Resources and Electric Engineering Chongqing, 402160, P.R. China

Abstract: Safe and efficient networking of embedded systems was the integration development bottleneck for the next generation of embedded systems and network systems. In conventional networking technology embedded systems, either the network security or network efficient was ignored, so a better performance cannot be achieved. An embedded dynamic security networking technology based on quick jump and trust was proposed, and the multiple network nodes based on a random beating of fast switching was used to achieve optimal network search, when the Web search was completed, the trust mechanisms was taken to protect the security of the network system access, while achieving rapid network and security. A set of 10-nodes was used to test the system, the result shows that with quick jump and trust, the systems security risk distribution can be accurately detected, enabling fast and secure network, so it has good network system security application.

Keywords: Embedded system, quick jump, security networking, trust.

1. INTRODUCTON

With the rapid development of embedded technologies and modern Internet technologies, the way that making convenience Internet technology used in embedded systems technology has been widely applied. That Internet technologies used in embedded system is a great improvement both for embedded systems technology and the Internet technology. Embedded systems supported by Internet technologies can easily handle all kinds of information at anytime and anywhere, and then upload information online to get more information through online interaction; and Internet technology supported by embedded system will make infinite space expand for the development of Internet technology. A key question is applying Internet technology in embedded systems to quickly implement networking and security networking, which is the development constraint of next-generation network systems and embedded Systems. Wireless communication has brought great convenience to networking, but the openness of wireless radiation has brought a huge security risk to the wireless network. So it is a very important development bottleneck that how to achieve security under fast networking.

In reference [1], LiuJun has put forward a cognitive wireless ad-hoc network topology control algorithm which supports network coding, building redundant topology structure based on shortest path algorithm of network coding, analysis of system functions, optimizing the topology structure, and the algorithm can improve the reusability of the wireless resources, strengthening the anti-damage performance of the network, but the algorithm is complex and the real-time performance is very poor, which can not be well used in the rapid dynamic networking. Jiao Xian-long has proposed a wireless ad-hoc network coding method with heuristic algorithm, using basic thoughts of the greedy collection configuration heuristic algorithm and greedy set covering heuristic algorithm to mine the opportunity of network coding as much as possible, after improving, the algorithm enhances the performance of existing broadcasting algorithm, and the improvement of the system performance exceeds the performance of existing network coding method. The algorithm uses the thoughts of greedy system, inspiring and digging, but the inspiring thought has certain divergence characteristics, which can't fully ensure convergence of the system [2]. Document [3] has proposed a research and simulation method of optimal hotspot network communication technology of wireless wifi, realizing the algorithm by adopting the method of the structure of the distance between the hotspot and gravity center of the weights, and the result of the experiment can effectively improve the efficiency of communication, but when the distance of the system appears outliers, the weighted method according to the distance weights would not be the real state of reaction system, so the adaptively of the algorithm is questionable [3]. Literature [4] has proposed self-healing network and protocol implementation method based on ZigBee, on the basis of ZigBee in wireless communication, by self-healing network protocol design to achieve network technology with large network capacity and small time delay, and the system has certain forward-looking research significance for embedded system networking technology [4]. Reference [5] has studied the topology control strategy research progress of wireless ad-hoc network, through controlling the series way in communication between network nodes in the system and the transmission range of nodes, so as to improve the life cycle and efficiency of the whole network system, achieving the goal of system optimization. This article has analyzed the topology and process of the network in details, but the lacking of effective network stability support [5]. Literature [6] has put up forward a technology of mobile base station developing and application based on 3G wireless IP network TETRA, on the basis of mobile communication technologies, then obtaining the conclusion that the network method based on 3G wireless IP is superior to other methods, but with complexity of algorithm and adaptively differential [6].

In view of the above problem that quickness and security cannot both be ensured, this paper proposes an embedded system security network technology based on fast jump dynamic network and trust, along networking, based on the random jitter between multiple network nodes, quickly switching, to optimize the network search, and through the trust mechanism to guarantee the security of network system access, at the same time achieving the rapidity and security of the network. Finally use a set of 10 nodes to test the system, verifying the performance of the system.

2. DYNAMIC NETWORK TECHNOLOGY WITH QUICK JUMP

Dynamic network technology with quick jump is a kind of optimization search method on account of random jitter between multiple network nodes, quickly switch and fast networking. Compared with other network technologies, the method of the article has significantly improved in the field of recognition rate and misjudgment rate.

Being used in the dynamic network, quick jump technology, firstly, initializes a group of random network nodes as the network node terminals in initial dynamic network task distribution, and then finds the optimal solution through iteration, namely the optimization task distribution of dynamic network. In each iteration, the network nodes update their iteration steps by monitoring two variables. Assume that the number of initial client network nodes is composed by population of a network nodes community being *m* [7], among them, position of the i_{th} terminal network node in the d_{th} dimension is defined as x_{id}, and query speed of networking is defined as v_{id}, the optimal task quantity being current searched by dynamic network terminal network node is P_{id}, the optimal effect of task allocation by dynamic network terminal is P_{gd}.

The network system is described as:

$$V_{id}^{t+1} = V_{id}^{t} + c_1 r_1 (p_{id} - x_{id}) + c_2 r_2 (p_{gd} - x_{gd}) \tag{1}$$

$$x_{id}^{t+1} = x_{id}^{t} + V_{id}^{t+1} \tag{2}$$

Among them:

r_1------number of random distribution;

r_2------number of random distribution;

c_1------constant;

c_2------constant;

In order to improve the anti disturbance performance of the algorithm, add momentum inertia coefficient ω to improve the ability of out calculator to local extremum in the middle of dynamic network implemention. The modified equation is defined as:

$$V_{id}^{t+1} = wV_{id}^{t} + c_1 r_1 (p_{id} - x_{id}) + c_2 r_2 (p_{gd} - x_{gd}) \tag{3}$$

In addition, in order to control iterative speed of ion optimization algorithm in the middle of dynamic network [8], adding restriction factor α to control the speed, then the optimization algorithm of dynamic network is defined as:

$$x_{id}^{t+1} = x_{id}^{t} + \alpha V_{id}^{t+1} \tag{4}$$

Then the weighting system standard between two network nodes which networks with each other is defined as:

$$\begin{cases} \varphi_1 = r_1 c_1 \\ \varphi_2 = r_2 c_2 \\ \varphi = \varphi_1 + \varphi_2 \\ p = \dfrac{\varphi_1 p_0 + \varphi_2 g}{\varphi_1 + \varphi_2} \end{cases} \tag{5}$$

In practical application, the network nodes are simplified as:

$$v(t+1) = \omega v(t) + \varphi(p - x(t)) \tag{6}$$

$$x(t+1) = x(t) + v(t+1) \tag{7}$$

Simplifying network node optimization algorithm is used in dynamic network to realize task distribution, which can not only reduce computational complexity, but also improve the efficiency of system [9, 10]. Excluding the speed of network node in the network algorithm cannot achieve precise control in the speed control.

$$x(t+2) = (\varphi - w - 1)x(t+1) + wx(t) \tag{8}$$

Realizing the information sharing and networking between network nodes is defined as:

$$x_{id}^{t+1} = wx_{id}^{t} + c_1 r_1 (p_{id} - x_{id}^{t}) + c_2 r_2 (p_{gd} - x_{id}^{t}) \tag{9}$$

The solution of dynamic networking with quickly jumps after deformation is defined as:

$$x(t+1) + (\varphi - w)x(t) = \varphi p \tag{10}$$

Through the above analysis and calculation, we can achieve the task scheduling of network nodes in a dynamic network.

The analysis on reasons of the convergence there may be when task allocation under local minima is as follows:

$$\lim_{t \to +\infty} x(t) = p^* = \frac{r_1 c_1}{r_1 c_1 + r_2 c_2} p_0 + \frac{r_2 c_2}{r_1 c_1 + r_2 c_2} p_g \tag{11}$$

As r_1, r_2 are submitted to uniform distribution, the average behavior of task scheduling and distribution of the sys-

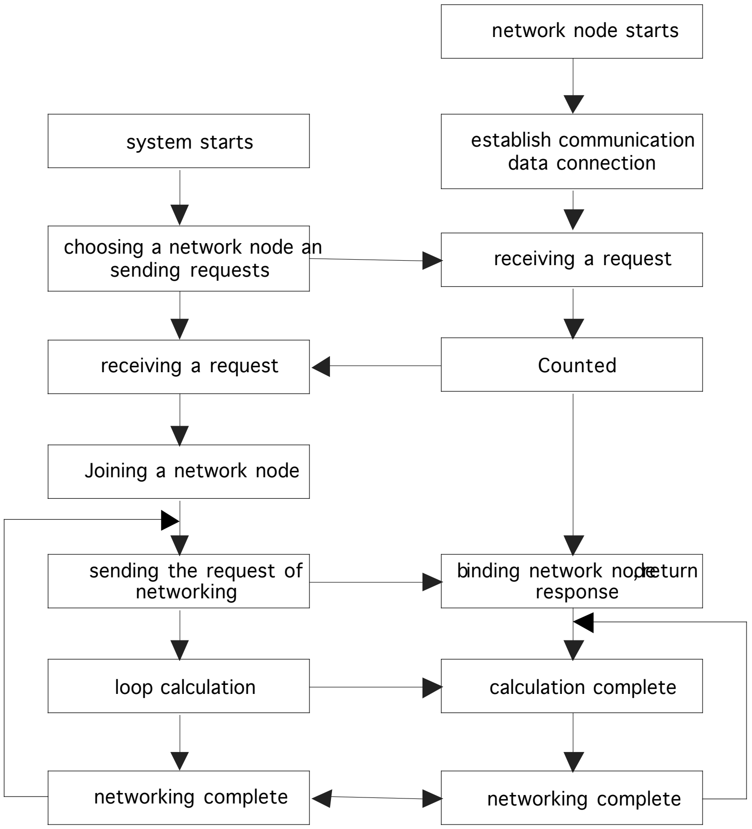

Fig. (1). Flow chart of dynamic networking.

tem in a dynamic network can be defined through observation of the expectations, which is:

$$\lim_{t\to+\infty} x(t) = p^* = \frac{c_1 p_0 + c_2 p_g}{c_1 + c_2} = (1-a)p_0 + ap_g \quad (12)$$

The process for dynamic networking with the technology of quick jump is shown in Fig. (**1**).

After system network nodes start, it begins to select a network node, and then checks the current assignment status of the network node, if the network node is not networked, then send the corresponding networking request, and if the network node has already networked, then skip the network node or wait. At the same time, after the network node is requested, according to its own actual condition, if can be calculated, then the control system switches into network mode, after the network node is networked, then the network data of the system can be exchanged.

3. SECURITY NETWORKING WITH EMBEDDED SYSTEM

Technology of networking with embedded system uses wireless sensor network. In the wireless network, an important problem is how to realize the security of the network, that is, the illegal network node organizations cannot make network and the legal network nodes can be normal access to the system. Malicious network nodes include both the external network malicious network nodes deployed by the attack in network area and its internal network nodes captured or controlled in a wireless network with embedded network. For the external network malicious network node, they cannot undertake authentication [11-13] and own initial trust with the internal network nodes because they don't have a network key, so the traditional password authentication system can effectively cope with. On the contrary, for the network nodes captured or controlled by the networks themselves, namely the malicious network nodes in internal network, they own the network key, having a certain trust with the normal network nodes, so the traditional password authentication mechanism doesn't work, easier to attack. Relatively speaking, any internal network nodes can all be malicious network nodes, so necessary data authentication is needed to take safety certification for each network node, ensuring the security of data in the embedded wireless network. Therefore, setting up a number of screening network nodes to identify and weed out malicious network nodes in the embedded wireless network is one of the theoretical methods.

In terms of screening network nodes, there is a trust record between multiple access network nodes, and itcan directly understand the security of the information through the accumulation of trust.

The attacks of malicious network nodes can be roughly divided into direct attack and indirect attack, the behavior of direct attack mainly includs fully or partially discarding packets, changing the contents or ID of packets, transmitting packets freely and sending false packets, etc. The behavior of indirect aggression mainly includes deliberately reducing the credit value of the normal neighbor network nodes, raising the credit value of the malicious network nodes, changing the new logo to add group network, etc. Considering monitoring and computability, this article analyzes the attack behavior from the aspects of the number of the packets, the repetition rate of the data contents, data similarity and correlation with neighborhood network nodes, so the definition of direct trust between network node i and its neighbor network node j can be given. Trust relationship is expressed by $\left(E_i, E_j, d, t\right)$, among them, E_i, E_j are entities that need to build trust relationship (*i.e.*, network nodes i and j), d is the data for interaction, t is the time needed for interaction. Direct trust for network nodes is vector D, which is expressed as:

$$D=\left\{S_{i,j}\left(t\right),T_{i,j}\left(t\right),U_{i,j}\left(t\right)\right\} \tag{13}$$

In which, $S_{i,j}\left(t\right)$represents factors of data repeat, $T_{i,j}\left(t\right)$represents factors of data output, $U_{i,j}\left(t\right)$ represents the similarity of data(correlation), the computation formula is as follows:

$$S_{i,j}\left(t\right)=\frac{p_{i,j}\left(t\right)-sp_{i,j}\left(t\right)}{p_{i,j}\left(t\right)} \tag{14}$$

Among them:

$p_{i,j}\left(t\right)$---- number of output data at time t ;

$sp_{i,j}\left(t\right)$ ---- quantity of data repeat ;

$\Delta p\left(t\right)$ ---- dynamic reference value of data quantity ;

$z_i\left(t\right)$, $z_j\left(t\right)$ ---- the output of their monitoring values, respectively;

b ---- comparing coefficient.

Value the trust obtained by the nearest moment s the maximum 1, then the trust value with the longer time interval has the smaller impact on the current time, the time-weaken the functions are as follows:

$$f\left(k\right)=\begin{cases} f\left(k-1\right)-\dfrac{1}{n},1\le k<n \\ 1,k=n \end{cases} \tag{15}$$

To sum up, the direct trust value computation formula of neighbor network nodes is:

$$D''_{i,j}\left(t_{n+1}\right)=\frac{D'_{i,j}\left(t_{n+1}\right)+f\left(n\right)D'_{i,j}\left(t_n\right)}{2} \tag{16}$$

An update cycle differs time t_{n+1} and time t_n , namely, the direct trust value of network node is the average value of the trust value for the previous cycle after the attenuation and the current trust, time-weakened function not only ensures the continuity of trust value computation, but also adjusts the proportion of trust value of the previous cycle, this calculation method can maximally ensure the efficiency of the trust value.

Obviously, if the network nodes i does trust evaluation only according to its own monitoring to the behavior of the network node j (direct trust value), the evaluation result will be biased and lack of comprehensive. Moreover, sometimes there is not necessarily to establish direct trust relationship between network nodes. So, there is a must to obtain trust values recommended by other network nodes who are neighbors of network node j , achieving the indirect trust value after comprehensive calculation.

To achieve a comprehensive and accurate assess of the behavior of the network node j , network node i requests the of the other neighbor network nodes of network node j to send their own direct trust value to network node j , and then obtains the indirect trust value of network node i to network node j based on the synthetic rules of evidence theory, which is set to vector I .

Assume network node k is one of the other neighbor network nodes of network node j , and then the indirect trust value I of network node i to network node j at time t is calculated by the following calculation:

$$I_{i,j}\left(t\right)=\frac{\sum D''_{i,k}\left(t\right)D''_{k,j}\left(t\right)}{\sum D''_{i,k}\left(t\right)} \tag{17}$$

when the indirect trust value I is lower than the setting threshold, the network node is taken as the malicious node, whereas trust node. Through the trust evaluation method between nodes above, it can be very good to realize security defense in network nodes and guarantee the network security in wireless network.

4. SIMULATION AND ANALYSIS OF RESULTS

4.1. Simulation Environment Description

In order to test security network performance with embedded system based on dynamic network technology with rapid jump, using a set of testing systems with 10 nodes, on account of comprehensive evaluation standard, set up the performance of network security protection as the foundation to measure the standards of systems.

Detailed parameters of node distribution are shown in Table **1**.

Among them, the active node with more jump times belongs to actively searching node, and the passive node with less jump times belongs to passively searching node.

The detection rate and false positive rate of Attack detection is two important indexes to evaluate the effect of detection in intrusion detection mechanism. This paper uses two indicators to measure the detection effect of dynamic security network technology based on embedded system with rapid jump and trust value, and the performance indicators of various attack detection are shown in Table **2**.

Table 1. The node parameter distribution.

Node Number	Node Attribute	Jump Times	Security
node 1	active node	5	0.63
node 2	passive node	1	0.34
node 3	active node	6	0.67
node 4	passive node	1	0.56
node 5	active node	8	0.96
node 6	active node	6	0.46
node 7	passive node	1	0.72
node 8	active node	9	0.46
node 9	active node	7	0.65
node 10	passive node	1	0.78

Table 2. Test results of dynamic security network technology in this paper.

Attack Type	Rate of Detection (%)	Rate of Misjudgment (%)
Isolated nodes	92	4.2
Fake cluster head	92.4	3.9
Wormhole	91.2	5.1
Clusters merge with no response	93.2	3.7
Swarming	88.8	3.5

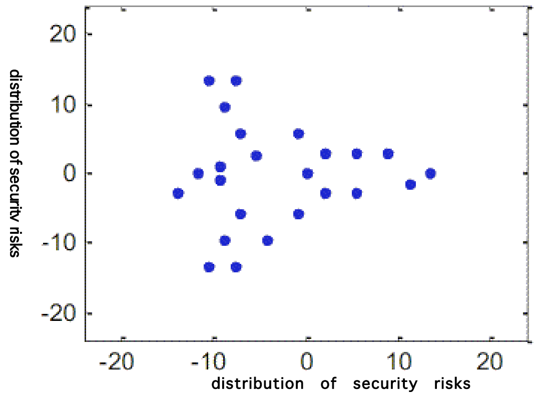

Fig. (2). Distribution of security risks.

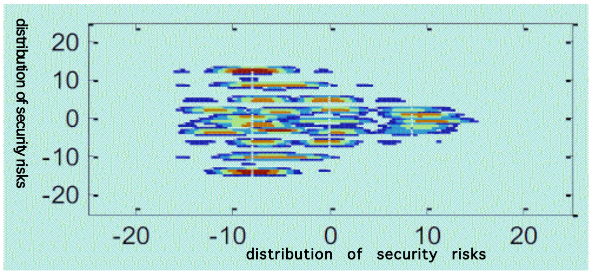

Fig. (3). The security performance of conventional method.

It can be seen from the above table that detection rate of embedded dynamic security network technology based on jump and trust value has remained at about 90% and misjudgment rate is basically lower than 5% facing with a variety of attack, which shows that the detection mechanism has high detection rate and low.

4.2. Result Analysis

In a simulation plane distributing 10 nodes, there is a relationship of random jitter network request and response with each other between nodes, through the jump change, the system can quickly find safe and reliable network nodes needed to network in a relatively short period of time, realizing normal communication and data transmission between the nodes after the completion of networking.

The distribution of security risks of the testing network is shown in Fig. (**2**), and the dot in the figure is the place where security risks are. The coordinate unit is pt.

Security performance of the conventional method is shown in Fig. (**3**), wherein the coordinate unit is pt.

Security performance of the dynamic networking with fast jump is shown in Fig. (**4**), which coordinate unit is pt.

It can be seen from the comparison of Figs. (**3 and 4**) that the security risk distribution of the system turns into large planar distribution around the security risks designed by the

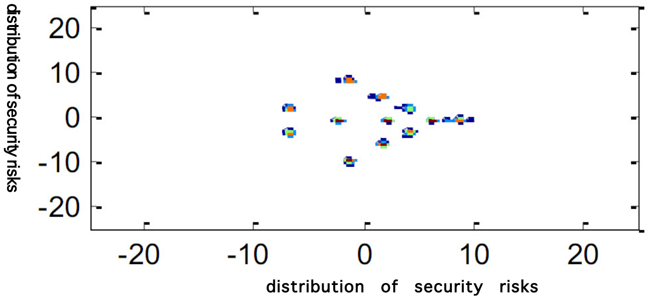

Fig. (4). Security performance of networking with fast jump.

simulation after safety protection with traditional method in Fig. (**3**), that is to say, the safety protection is very difficult through the traditional method and can't accomplish accurate protection against potential safety hazard. In Fig. (**4**), the security risks of the system have been accurate positioning into a point through networking based on fast jump, which can realize accurate safety protection. It is very important to the security networking of embedded system.

Security index comparison curve of 10 nodes is shown in Fig. (**5**).

It can be seen from Fig. (**5**) that the security indexes of the system which networks based on rapid jump technology are higher than that of the traditional methods, so the security of the system is greatly increased.

4.3. Algorithm Performance Test

In order to further verify the superiority of this algorithm, the following experiment is carried out. The experimental environment is constituted by a master scheduling server and six processing servers, a network address translation (NAT) needed when conducting safety protection, safety protection processing server according to the frequency of CPU, memory size and speed of storage, the number of request packets the client launches, we use this algorithm and traditional algorithm to dispatch NAT operation respectively. The results are shown in Fig. (**6**) below.

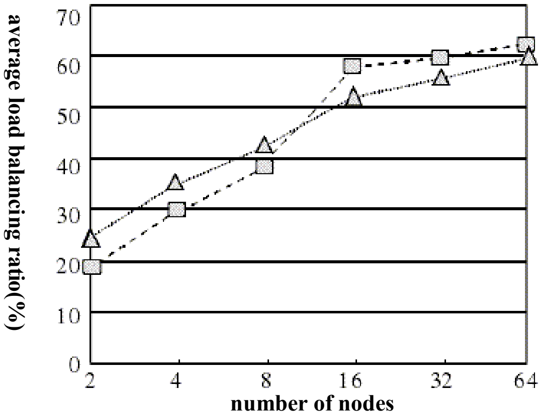

Fig. (6). Comparison of number of nodes and the average load balancing ratio of all nodes.

In Fig. (**6**) above, the triangle represents algorithm in this paper, the experimental results show that with the increase of tasks of safety protection, the processing power of each nodes to security protection task reinforces after using the algorithm in this paper, and the load is leveling off in the whole system, and the load balancing ratio improves in a degree.

CONCLUSION

Under the development of modern wireless network technology, safe and fast embedded system networking is the bottleneck in the development of embedded system and network system integration. Traditional embedded system networking technology cannot have both the rapidity and security of network system, which can't adapt to the development of next generation network technology well. So this paper proposes a security network technology with embedded system based on dynamic network with fast jump and trust value, both quickness and security of network. The system adopts optimized network search method based on random jitter between multiple network nodes and quickly switches, through the trust mechanism to guarantee the secure access

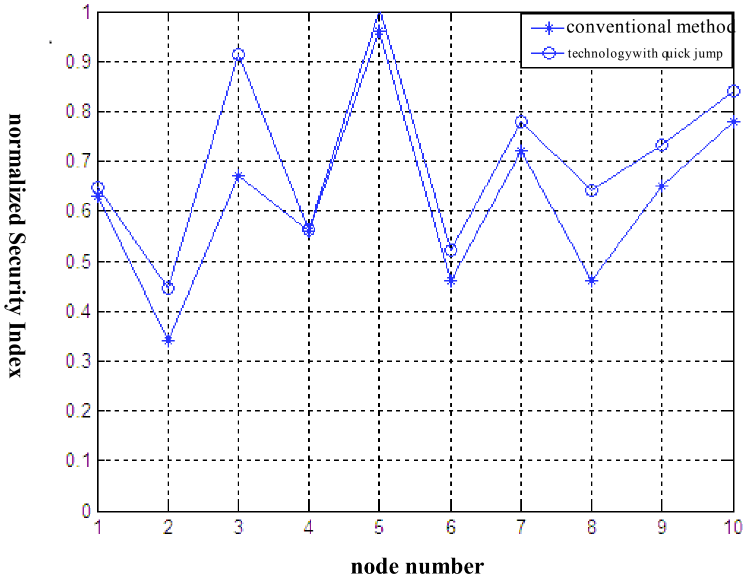

Fig. (5). Comparison of security index.

of network system when the network search is completed and achieving the rapidity and security of the network at the same time. Using the system with a group of 10 nodes to test, the experiment results show that the system safety hazard distribution can be detected accurately with the network technology based on fast jump and the trust value, so as to realize rapid and safe access to the network, which can be good application to network system protection.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] J. Liu, "Topology control algorithm backing for network coding in cognitive wireless ad-hoc networks," *Journal on Communications*, vol. 34, no. 5, pp. 136-142, 2013.

[2] X. Jiao, X. Wang, and X. Zhou, "Network coding method using heuristic algorithm for wireless ad-hoc networks," *Journal of Software*, vol. 21, no. 11, pp. 2892-2906, 2010.

[3] H. Fang, "Optimal wireless Wifi hot spot of network communication technology research and simulation," *Computer Simulation*, vol. 30, no. 7, pp. 269-273, 2013.

[4] L. Zhou, Y. Chen, and T. Feng "Self-healing network organization and protocol implementation based on ZigBee technology," *Communications Technology*, vol. 45, no. 2, pp. 1-4, 2012.

[5] F. Wang, and Y. Zhang, "Research development of control strategy for wireless ad-hoc networks," *Computer Science*, vol. 34, no. 10, pp. 70-73, 2007.

[6] Y. Xiao, "Development and application of TETRA mobile base station based on 3G wireless IP Networking," *Science and Technology Innovation Herald*, vol. 9, pp. 27-29, 2011.

[7] Y. Liu "Design of information processing system architecture based on cloud computing," *Bulletin of Science and Technology,* vol. 28, no. 18, pp. 100-102, 2012.

[8] C. da Wang, J. Shi-guang, "Security in wireless network," *Computer Science*, vol. 33, no. 7, pp. 121-125, 2006.

[9] X. Lei, and J. Tian, "The information flow clustering model and algorithm based on artificial Bee colony mechanism of PPI network," *Chinese Journal of Computers*, vol. 35, no. 1, pp. 134-145, 2012.

[10] Z. Hu, and M. Zhao, "Simulation on traveling salesman problem(TSP) based on artificial Bee colony algorithm," *Transactions of Beijing Institute of Technology*, vol. 29, no. 11, pp. 978-982, 2009.

[11] C. Liu, and C. Ye, "Bat algorithm with chaotic search strategy and analysis of its property," *Journal of System Simulation*, vol. 25, no. 6, pp. 1183-1195, 2013.

[12] H. Zeng, C. Zhang, and D. Zhang, "Application layer QoS control and testing method for audio/video delivery over space network," *Journal of the Graduate School of the Chinese Academy of Sciences*, vol. 28, no. 1, pp. 108-114, 2011.

[13] Z. Wang, Y. He, and J. Han, "Distributed receding horizon control algorithm on relative states," *Journal of System Simulation*, vol. 25, no. 2, pp. 280-293, 2013.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014