International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.5 (2016), pp.319-328
http://dx.doi.org/10.14257/ijmue.2016.11.5.29

Credit-Based Reliability Service Model in Wireless Communication Networks

Zonghai Ye

Minnan Science and Technology Institute, Fujian Normal University, Quanzhou, China
27078955@qq.com

Abstract

In wireless communication networks, the reliability is greatly important that it is independent of the radio transmission approach, unfortunately due to the failure-prone nature of wireless communication networks, the ability of providing a stable link and consistent quality of service (QoS) to end-users is a key issue. Currently credit-based reliability system becomes a very important security mechanism in the wireless adaptive communication network. This paper introduces a credit-based reliability service model which uses the credit space expressed by the WATCHDOG mechanism so as to access the wireless self-organized network. In this model, the transformation from credit space to reliability space is proposed and the key characteristics are revealed. Experiments are carried out to examine the proposed model. It is observed that, the proposed model is able to evaluate the service value under the credit-based reliability capacity.

Keywords: *Wireless Network, Credit-based Reliability, Communication, Service, Model*

1. Introduction

In wireless communication networks, the reliability is greatly important that it is independent of the radio transmission approach [1]. However, due to the failure-prone nature of wireless communication networks, the ability of providing a stable link and consistent quality of service (QoS) to end-users is a key issue [2-3]. In the wide definition of QoS, the reliability service is included [4-5]. That means in an adaptive wireless communication network, the service from the self-adaption grid is reliable, which is a basic to implement the wireless network. Unfortunately, the service reliability and security cannot be solved only considering the encryption and verification techniques, which are widely used to improve the network stability and data integrity through using the cryptography to evaluate the data [6-9]. Using this approach, the data confidentiality, tamper-resist, user authentication, and data safety could be ensured during the running of wireless communication network [10]. When facing the challenges of special characteristics of network and violation behaviors, it is very difficult to implement.

Currently credit-based reliability system becomes a very important security mechanism in the wireless adaptive communication network [11-12]. In the service-oriented wireless network architecture, the functionalities in each node are provided in the forms of services. How to evaluate the services provided from the nodes is crucial to keep the reliability of a wireless communication network. The reliability of wireless network is different comparing with the security issues, which focus on guaranteeing the anti-eavesdropping, tampering, and reality of the data transferred over the wireless channel. To ensure the network security, encryption and decryption technology, data masking, and backups are used [13-14]. However, these methodologies are not capable for solving the service reliability of the nodes in a wireless network. For example, due to the adaptability and distributed feature of wireless network, there are several new challenges: if some physical nodes are attacked intendedly so that the nodes could be used for controlling the other nodes without surveillance of the abused operations. Moreover, the inaccurate data or violations could be misused to mislead the served nodes.

Except the hostile attack to the nodes in wireless network, the system is easily influenced by the errors. For example, there will be several uncertain errors from the wireless devices and sensors. In these cases, these nodes in the wireless communication network cooperate with the event management may trigger poor performance or violation behaviors. These errors cannot be solved by the verification and encryption & decryption technology. Thus, a reliability service model may solve the challenge.

This paper introduces a credit-based reliability service model which uses the credit space expressed by the WATCHDOG mechanism so as to access the wireless self-organized network. In this model, the transformation from credit space to reliability space is proposed and the key characteristics are revealed. The credit includes two parts: reputation and trust. In the distributed computer network system, the reputation is defined as “A reputation system computes and publishes reputation scores for a set of objects (*e.g.* service providers, services, goods or entities) within a community or domain, based on a collection of opinions that other entities hold about the objects.” [15]. Trusted Network Connect or TNC is an open architecture for Network Access Control, was originally a network access control standard with a goal of multi-vendor endpoint policy enforcement [16]. There are several characteristics of the credit-based reliability:

1. Dynamic: reliable establishment in a certain time, based on the context of which changes with changes. Because this reliability is a dynamic change in the evolution of this evolutionary process may be one of evolution toward reliability, there may evolve toward one party does not reliable, the key lies in the context of environmental factors and a given time period.
2. Context: the existence of trust and specific context is directly related to, on leaving the specific scenarios, there is no sense of the reliable environment.
3. Subjectivity: reliability is an entity to another entity to make a subjective judgment, because of the different entities, standard, experience different, given the trust criteria are different.
4. Measurability: reliability under the circumstances reputation, the reputation of the subjective feeling can be quantified.
5. Weak-way transitive: it is general believed that the reliability has not fully transitive, such as A trusts B, B trusts C, A relies on C cannot be worked out. However, under certain constraints, such as a trust group, the trust has certain transitive. As recommended or "second-hand information" is the way a typical spread of reliability is reflected in the form of transitive trust.
6. Asymmetry: in the reliable system, reliability is unilateral, usually asymmetric. In addition, the level of reliability is generally not equal to the level of reliability.
7. Fuzziness: reliability is uncertain, unclear and inaccurate and other natural attributes.

Based on the analysis of credit reliability, in order to ensure the reliable service and the trust relation between each established service nodes, this paper proposes a trustworthy service network model. This model uses WATCHDOG mechanism to keep the observed behaviors from neighboring nodes to build up the credit system. By using the dimidiate credit value, the trust from neighboring nodes could be obtained.

The rest of this paper will be organized as follows. Section 2 presents the established credit space based on the WATCHDOG mechanism. Section 3

2. Credit Space

The credit C_{ij} from the collected data could be established and the reliability value $R_{ij} = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 2}$. Due to the hostile attack or hardware defects, several results cannot be recorded. This section presents the established credit space, reliability degree and reliability space.

2.1. Credit Space

The credit space is based on the data captured by WATCHDOG mechanism, each of which has a module to execute a specific function. In the wireless network, each function controls a possible event. p, n present the positive and negative amount respectively. The credit space is defined as a two integer space $RS = N \times N$, whose element is unique one to one relation $< p, n >$ value.

Definition 1. Credit Space. $RS = \{< p, n >| p, n \in N^+ \cup 0, t = p + n\}$, according to the Bayesian theory

$$P(B_i \mid A) = \frac{P(B_i)P(A|B_i)}{\sum_{i=1}^{\infty} P(B_i)P(A|B_i)} \quad (1)$$

And β distribution theory, a positive result possibility is:

$$P_{<p,n>}(x) = P(x \mid < p, n >) = \frac{P(<p,n>|x)P(x)}{\sum P(<p,n>|x)P(x)} = \frac{(p+n+1)!}{p!n!} x^p (1-x)^n \quad (2)$$

2.2 Reliability Degree

Assume that a node A sends some messages to the neighboring node B with the message amount t . During the transmission, some information is received correctly, while some is missing. If there are p numbers of message received correctly, the successful sending rate is p/t , the certainty factor (CF) is $c = 1$. The reliability degree based on the credit could be defined as follows.

Definition 2. Reliability degree. Based on the credit $< p, n >$, it is defined:

$$c(p, n) = \frac{1}{2}\int_0^1 \left|\frac{(p+n+1)!}{p!n!} x^p (1-x)^n - 1\right| dx \quad (3)$$

Where p, n and $t = p + n$ present the positive, negative, and total result.

2.3 Reliability Space

Definition 3. The reliability space $TS = (pt, nt, ut)$ meets the under condition:

$$\begin{cases} pt, nt, ut \ge 0 \\ pt + nt = c \\ pt + nt + ut = 1 \end{cases} \quad (4)$$

Where pt, nt, ut represent the positive reliability value, negative reliability value, and uncertain reliability value. Let $T(p, n) = (pt, nt, ut)$ denotes the transfer from the credit space to reliability space, then,

$$T = (pt(p, n), nt(p, n), ut(p, n)) \quad (5)$$

pt, nt, ut meets the condition:

$$\begin{cases} pt(p,n)=c\times\dfrac{p+1}{p+n+2} \\ nt(p,n)=c\times\dfrac{n+1}{p+n+2} \\ ut(p,n)=1-pt(p,n)-nt(p,n) \end{cases} \tag{6}$$

If the reliability is 1, the positive reliability value is $pt(p,n)=\frac{p+1}{p+n+2}$. Then, $T=\frac{p+1}{p+n+2}$ is the expectation value of positive possibility.

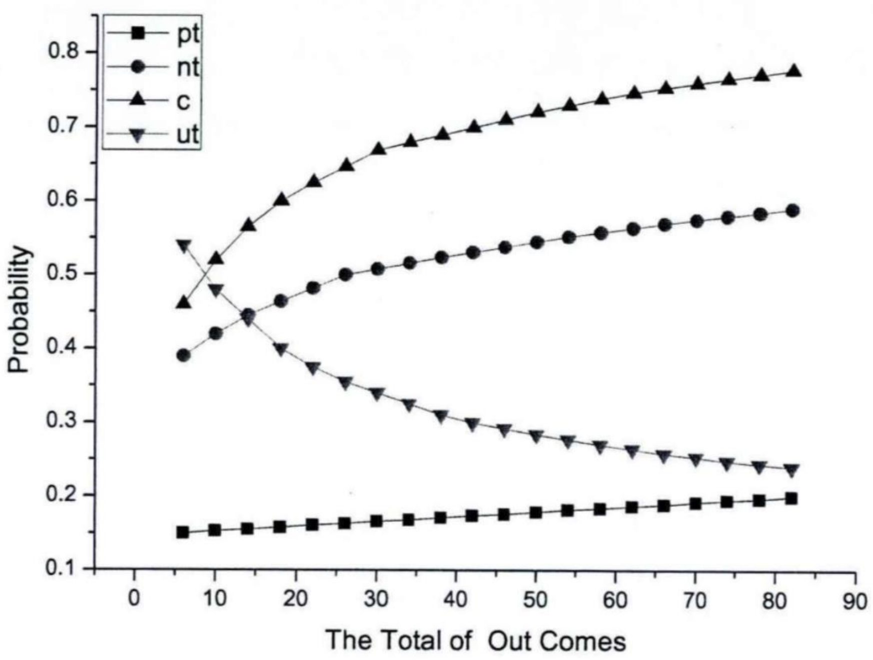

Figure 1. Analysis of pt,nt,c and ut

3. Analysis of the Credit-Based Reliability

Based on the definitions from Section 2, this section analyze the qualitative aspects of the credit-based reliability. The positive, negative, and total results, positive and negative reliability value and uncertain reliability value are detailed discussed.

3.1 Analysis of Scenario 1

If the positive and negative results are 0, the positive and negative reliability are 0. The uncertain reliability value is 1. From the definition of reliability degree, if the values of p,n are 0, then, $c=0$. According to the definition 3 reliability space, pt and nt are 0. Thus, $ut=1$.

Assume that the proportion $m=\frac{p+1}{p+n+2}$ is fixed, then when $t=p+n$ increases, pt,nt,c increase too, and ut decreases. The following Figure 1 shows the trends of pt,nt,c and ut.

According to the definition 2 and $m=\frac{p+1}{p+n+2}$, we can get:

$$c(t) = \int_0^1 |\frac{(t+1)!}{(mt+2m-1)!(t-mt-2m+1)!}x^{mt+2m-1}(1-x)^{t-mt-2m+1}-1|dx \qquad (7)$$

$\forall t > 0$, let $c'(t) > 0$ could be proofed the above equation. From the Figure 1, when $m = 0.25$ is fixed, total results increase, then positive and negative and reliability value increase, while the uncertain reliability decreases.

3.2 Analysis of Scenario 2

When the total results are fixed, when the positive result increases, the negative reliability decreases. When $p > n$, along with the increasing of positive result, reliability value increases too. When $p < n$, reliability degree will decrease when the positive result increases. When $p = n$, the reliability value is minimum.

When $p > n$, uncertain reliability decreases as the increasing of positive result. When $p < n$, uncertain reliability increases along with the positive result increases. When $p = n$, the uncertain reliability reaches the maximum value. Figure 2 presents the trends in scenario 2.

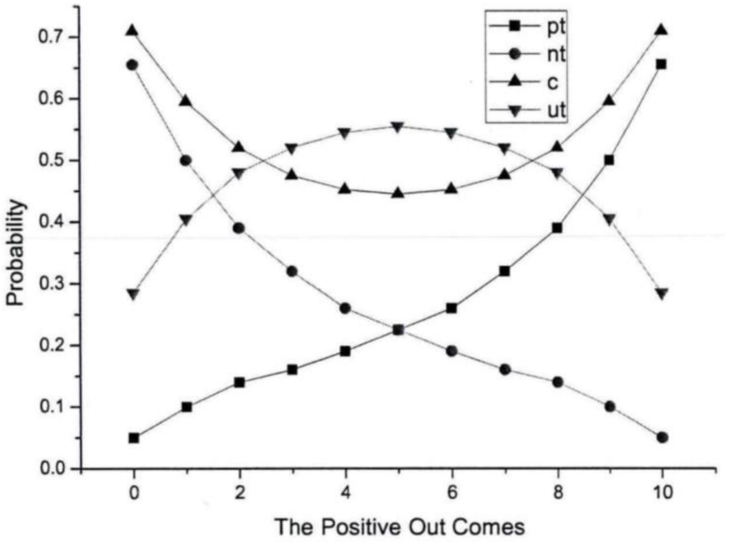

Figure 2. Trends of pt, nt, c and ut

According to the definition 2 and $t = p + n$, then we can get

$$c(p) = \int_0^1 |\frac{(t+1)!}{p!(t-p)!}x^{p}(1-x)^{t-p}-1|dx \qquad (8)$$

Finally we can find that when $2p < t$, $c'(p) < 0$ and when $2p > t$, $c'(p) > 0$. While, when $2p = t$, $c'(p) = 0$.

4. Credit-Based Reliability Service Model

4.1 Trust Service Wireless Network

Trust service wireless network (TSWN) runs on a device in each agent node which uses supervisor mechanism to monitor the node behaviors under the signal range. Figure 3 presents the four architecture of the TSWN and supervisor mechanism.

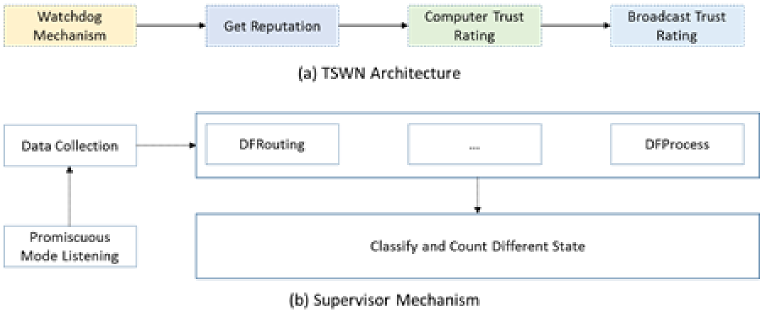

Figure 3. TSN Architecture

The supervisor mechanism is divided into three steps: (a) data collection: the agent nodes use the fixed time window to keep the behaviors' data; (b) data check: the collected data is put into different function modules such as DFRouting and DFProcess, which are responsible for monitor the transfer behaviors and service executions; (c) status classification: the positive and negative behaviors based on the defined reliability value are classified and counted.

4.2 Proposed Model

The model under the TSWN is established by calculating the following formulation:

$$\begin{cases} p(n) = p^{cur} + f_1(p(n-1), n(n-1)) \\ n(n) = n^{cur} + f_2(n(n-1), n(n-1)) \end{cases} \tag{9}$$

$p(n)$ is the sum of p^{cur} and $f_1(p(n-1), n(n-1))$, where p^{cur} is the positive result under the time window. $f_1(p(n-1), n(n-1))$ is the reliability value which is related to $n(n-1)$.

The model calculating the reliability and the node could circulate values through two steps. Firstly, the circulation approach could be determined. When the agent node finishes the calculation of the reliability, the value could be sent out in the next window initiation. Within the signal receiving area of the network nodes, the reliability value could be received and the nodes could work out whether to collaborate with the neighboring nodes. Secondly, the circulation approach could be driven. If the value of reliability is less than the pre-expected value of the threshold from the agent nodes, the nodes will stop the calculation of the reliability values. If the nodes are considered to be cooperated with, the hostile attack maybe used for hack the nodes which will make the network unstable or untrustable.

4.3 Attack Analysis

This section reports on an example to consider an attack under the TSWN. Assume that the attack follows four steps: (1) in the previous 5 time windows, 50 times good performance is worked out; (2) in the second 5 time windows, hostile attacks are performed; (3) during the third 5 time windows, it stops; (4) in the final 5 time windows, it performs good. The following equations are used for calculating the reliability

$$\begin{cases} f_1(p(n-1), n(n-1)) = p(n-1) \times \beta \\ f_2(n(n-1), n(n-1)) = n(n-1) \times \beta \end{cases} \tag{10}$$

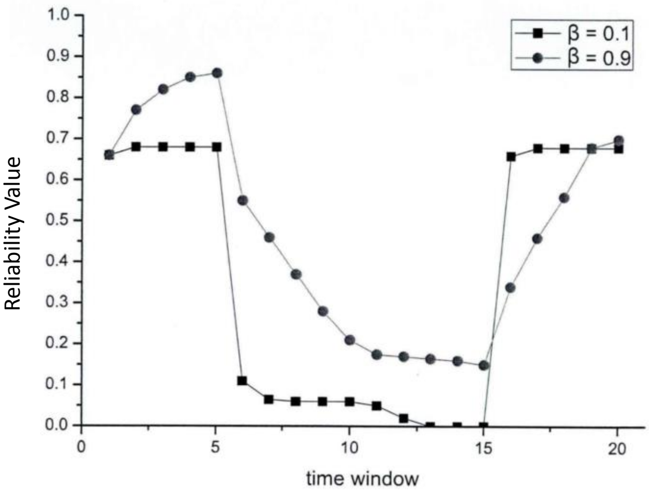

Figure 4. Reliability Along with β

Figure 4 presents the different reliability value along with β . Several observations could be obtained from the example of attack. First of all, when (10) has a bigger β value, for instance, when $\beta = 0.9$, in the step (2), the reliability value is greatly increasing comparing with $\beta = 0.1$. That means, using the model, it is easily to find out the hostile attack. The credit-based reliability service model could figure out the attacks to improve the services in a wireless network. Secondly, when the $\beta = 0.1$, in the first 5 time windows performance, the reliability value is a little bit less than when $\beta = 0.9$. However, at the last step, the value is bigger than when $\beta = 0.9$. Thus, the β will significantly influence the system reliability service in the evaluation. When we carrying the evaluation, the bigger value of β should be considered.

5. Experiments and Analysis

From the above establishment of the model, nodes in the wireless communication network may spend long time for interacting with each other to build up a friendly relationship so as to get high reliability degree to ensure the reliable service. Under this model, few hostile behaviors will ruin the built up reliability value. The key value of β will greatly influence the evaluation of the reliability service. In the experiment, we examine the equation (10) by converting into:

$$\begin{cases} f_1(p(n-1), n(n-1)) = p(n-1) \times \beta \\ f_2(n(n-1), n(n-1)) = n(n-1) \times (1-\beta) \end{cases} \quad (11)$$

(11) is used for examining the impact of β on reliability value. Figure 5 shows the experiment results with $\beta = 0.1$

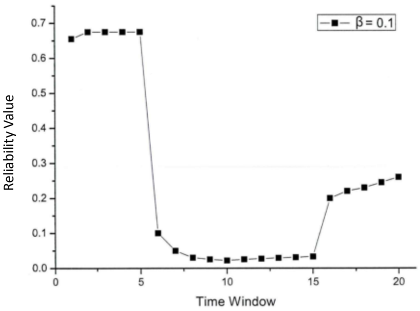

Figure 5. Impact of β on Reliability

After using the $(1-\beta)$ to replace β in f_2, it could be found from Figure 5, at the phase 2, the reliability value decreases sharply. When the nodes in step 4 perform good, the positive reliability value increases slightly that because in the phase 2, the hostile behaviors will be kept in the model. It implies that the reliability value will be greatly affected by β. The service of the network could be evaluated through the value of β.

In the experiment of validation of the proposed model, this section studies two scenarios: (1) node x_i and x_j, the reliability between them is PT_{ij} which is used for determining and analyzing the collaboration standard. (2) a node x_j owns several neighboring nodes x_A, x_B, x_C, x_D, x_E. x_j is a confliction behavior attack. If the node x_j performs hostilely, under the TSWN, the reliability value decreases sharply. When the perform of the nodes is good, the reliability may increase slightly. Figure 6 presents the results from the simulation.

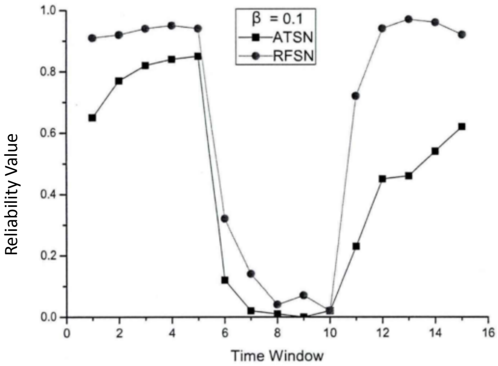

Figure 6. Experiment Results from Simulation

From Figure 6, since the hostile behavior data is kept, the reliability value then may be more reasonable by considering the historic data. In the time window 14, for example, the reliability is lower than that in the window 13. Because in the time window 14, the reliability value is bigger than in 13. From 6-10, the nodes have some hostile behaviors, so the reliability increases slightly after the nodes performs normally. The simulation of x_j has hostile behaviors to x_D, x_E. Then the reliability reaches the lowest value. It is observed that, the proposed model is able to evaluate the service value under the credit-based reliability capacity.

6. Summary

This paper introduces a credit-based reliability service model in wireless communication networks. The definition of credit space and reliability space are defined by using the WATCHDOG mechanism to evaluate the reliability value and the trusted behaviors in the network. As the wireless network application in our daily life, the accurate, reliable, and credit-based service is very important. Thus, the supervisor mechanism is adopted for enhancing the proposed model reliability service.

Future work will be carried out from several aspects. Firstly, this paper only talks about the hostile attack in the wireless communication network. Actually in practice, there are many types of attacks like vulnerability, misuse, *etc*. How to use the model to evaluate such attacks? The further research should be carried out. Secondly, more nodes could be examined by the model since this paper only considers limited nodes in the wireless network. Finally, the model could be extended to valuate other reliability such as information transfer in TCP/IP wired network or cables.

References

[1] B. Latré, B. Braem, I. Moerman, C. Blondia and P. Demeester, "A survey on wireless body area networks", Wireless Networks, vol. 17, **(2011)**, pp. 1-18.

[2] Z. Sheng, K. K. Leung and Z. Ding, "Cooperative wireless networks: from radio to network protocol designs", Communications Magazine, IEEE, vol. 49, **(2011)**, pp. 64-69.

[3] R. Y. Zhong, Q. Y. Dai, K. Zhou and X. B. Dai, "Design and Implementation of DMES Based on RFID", Proceeding of 2nd International Conference on Anti-counterfeiting, Security and Identification, Guiyang, **(2008)**, pp. 475-477.

[4] A. Agarwal and A. K. Jagannatham, "Optimal adaptive modulation for QoS constrained wireless networks with renewable energy sources", Wireless Communications Letters, IEEE, vol. 2, **(2013)**, pp. 78-81.

[5] R. Y. Zhong, G. Q. Huang, S. L. Lan, Q. Y. Dai, T. Zhang and C. Xu, "A two-level advanced production planning and scheduling model for RFID-enabled ubiquitous manufacturing", Advanced Engineering Informatics, http://dx.doi.org/10.1016/j.aei.2015.01.002, **(2015)**.

[6] M. Arifuzzaman, M. Matsumoto and T. Sato, "An intelligent hybrid MAC with traffic-differentiation-based QoS for wireless sensor networks", Sensors Journal, IEEE, vol. 13, **(2013)**, pp. 2391-2399.

[7] R. Y. Zhong, G. Q. Huang, S. Lan, Q. Dai, X. Chen and T. Zhang, "A big data approach for logistics trajectory discovery from RFID-enabled production data", International Journal of Production Economics, vol. 16, **(2015)**, pp. 260-272.

[8] R. Y. Zhong, G. Q. Huang, Q. Y. Dai and T. Zhang, "Mining SOTs and Dispatching Rules from RFID-enabled Real-time Shopfloor Production Data", Journal of Intelligent Manufacturing, vol. 25, **(2014)**, pp. 825-843.

[9] R. Y. Zhong, Q. Y. Dai, T. Qu, G. J. Hu and G. Q. Huang, "RFID-enabled Real-time Manufacturing Execution System for Mass-customization Production", Robotics and Computer-Integrated Manufacturing, vol. 29, **(2013)**, pp. 283-292.

[10] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks", Wireless Communications, IEEE Transactions on, vol. 13, **(2014)**, pp. 418-428.

[11] H. Zhu, X. Lin, R. Lu, Y. Fan and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks, Vehicular Technology", IEEE Transactions on, vol. 58, pp. 4628-4639, **(2009)**.

[12] R. Y. Zhong, "RFID-enabled Real-time Advanced Production Planning and Scheduling Using Data Mining", PhD Thesis, The University of Hong Kong, **(2013)**, pp. 1-221.

[13] L. Wang, S. Jajodia, A. Singhal, P. Cheng and S. Noel, "k-Zero day safety: A network security metric for measuring the risk of unknown vulnerabilities", Dependable and Secure Computing, IEEE Transactions on, vol. 11, **(2014)**, pp. 30-44.

[14] R. Y. Zhong and G. Q. Huang, "RFID-enabled Learning Supply Chain: A Smart Pedagogical Environment for TELD", International Journal of Engineering Education, **(2014)**, vol. 30, pp. 471-482.

[15] S. Sutariya and P. Modi, "A Review of Different Reputation Schemes to Thwart the Misbehaving Nodes in Mobile Ad Hoc Network", International Journal of Computer Science & Information Technologies, vol. 5, **(2014)**.

[16] J. Dubey and V. Tokekar, "Bayesian network based trust model with time window for Pure P2P computing systems", 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 219-223, **(2014)**.

Author

Ye Zonghai, He received bachelor's degree in electrical and industrial automation and master's degree in Signal and Information Processing degree. He is now a lecturer in Minnan Science and Technology Institute, Fujian Normal University, China. His current research interests are single chip processing, embedded technology, and network security. He has published more than 10 papers in various Journals and Conferences.