Wireless Sensor Network, **2010, 2, 373-380**
doi:10.4236/wsn.2010.24049 Published Online May 2010 (http://www.SciRP.org/journal/wsn)

Research on Beta Trust Model of Wireless Sensor Networks Based on Energy Load Balancing

Danwei Chen[1], Xizhou Yu[1], Xianghui Dong[2]
[1]*College of Computer*, *Nanjing University of Posts and Telecommunications*, *Nanjing*, *China*
[2]*ZTE Corporation*, *Shenzhen*, *China*
E-mail: *chendw@njupt.edu.cn*, *iyuxizhou@yahoo.com.cn*
Received February 27, 2010; *revised March* 18, 2010; *accepted March* 19, 2010

Abstract

This paper proposed beta trust model based on energy load balancing combines the recent achievements of the trust models in distributed networks, together with the characteristics of wireless sensor networks. The inter-node trust relation is established after an overall evaluation of node trust value based on the monitor results of the node packets forwarding behavior conducted by inter-node collaboration. Due to the node energy limitation in wireless sensor networks, energy load balancing mechanism is applied to prolong the node survival time. And the redundant routing protocol involves the presented trust model to develop the novel trust routing protocol of beta trust model based on energy load balancing. Simulation performance demonstrates that the beta trust model based on energy load balancing outperforms current schemes in energy consumption.

Keywords: Wireless Sensor Networks, Beta Trust Model, Trust Routing Protocol, Network Security, Trust Evaluation

1. Introduction

There are various attacking threats in Wireless Sensor Networks (WSNs) [1], which can be classified into routing protocol loopholes related attack, such as Sybil attack, false routing information attack, selective forwarding attack, Sinkhole attack, Wormhole attacks and fraudulent confirmation attack; and broadcast authentication loopholes related attack, such as HELLO flood attack, DOS attack and DDOS attack. Donggan Liu *et al.* proposed μTESLA [2] and solved the broadcast authentication loopholes related attack in most application scenario. The former type of attack, however, remains an open question for developing a generalized model for common applications. Center-less topology in WSNs determines that the nodes can not be authenticated uniformly by a third party. And the trust management system can be utilized in distributed network, aiming at establishing a trust network participated with trust nodes. Therefore, it is significant to develop a trust management system suitable for WSNs.

2. Basic Requirements for Trust System in WSNs

Trust nodes in WSNs shall constitute a trust network which can resist attack from hostile nodes effectively, and save node energy and network bandwidth to ensure network existence time and effectiveness. The designed trust model shall meet the following requirements:

1) Moderate protocol algorithm complexity. The time and space complexity of the protocol algorithm shall meet the process speed and storage space requirements. And digital signature and public key pair system are not suitable for WSNs.

2) Moderate protocol communication. The energy consumption from inter-node communication outgrows that from calculation within the node.

3) Trust evaluation effectiveness. The trust model shall evaluate the node trust value effectively and reflect the dynamic node trust value in time by monitoring the node behavior. Therefore, it is a challenge to reach a moderate balance between 2) and 3) so as to design an applicable trust system in WSNs.

4) Security in WSNs. The designed system shall be able to resist malicious attack, identify attack behavior from hostile node and take effective resisting actions.

3. Trust Evaluation Model

Blaze M. [3] firstly introduced the trust management for

the security in distributed system to solve the restriction using traditional encryption system. The early trust management engines are KeyNote [4] and RT framework [5]. Then trust management-based trust systems are applied in e-commerce, ad hoc network and peer network.

The network nodes in the WSNs are task-oriented, and functions as 1) transmitting nodes to collect the designated relevant information and report to the base station, or 2) forwarding nodes to forward data packet from other nodes to the base station. Considering encryption and digests are applied to guarantee the system confidentiality and integrity, the node trust values are based on the inter-node exchange behavior. Unlike the current trust systems, such as KeyNote, RT framework, eBay [6], CONFIDANT [7] and peer network, our model combines the direct and the indirect trust value to give an overall evaluation.

We established the trust model based on the node data forwarding statistics and the energy conservation. And the trust value of the routing node is evaluated by 1) the direct trust value from the lower-lever nodes and 2) the indirect trust value from the neighbor nodes.

Node trust value is computed through all the evaluations from other nodes, which avoids computing the exact local trust value and solves the dynamic trust value problem. It enhances the veracity of the trust mechanism and reflects the relativity of trust value and time. And chances are that some reliable nodes with high trust value would take on more forwarding tasks from neighbor nodes, which renders them more vulnerable to be trapped in energy exhaust. Our construction, however, takes this situation into consideration and achieves energy load balancing to prolong the network existence and enhance the effectiveness.

4. Beta Trust Model Based on Energy Load Balancing

4.1. Basic Description

The goal of the trust model is to choose credible node for routing information in order to ensure the data to reach the base station safely without losing packets maliciously. The evaluation of overall credibility of nodes in trust model would be involved in direct credibility and recommended credibility comprehensively (namely indirect credibility), where the previous is concluded from direct interaction with evaluated node, while the latter is inferred from others nodes to the evaluated node. While selecting next hop node in the consideration of energy load balancing of sensor network, we will take surplus energy ratio as a standard. The trust model is based on the following assumptions: 1) WSNs is safe after initialization and 2) after routing discovery, each node stores multiple routing paths to base station.

In the process of research, it needs two important terms derived from trust evaluation areas, namely credibility and reputation, where credibility means subjective expectations (usually a real number within 0-1) derived from A to B, and reputation based on the observation of an individual history behavior is an expectation for future behavior. This paper will also introduce a new term, the node energy surplus ratio, which means a ratio between the node surplus energy and initial total energy. For the sake of discussion, we define the expectation derived from future behaviors of B based on an observation of B history behaviors as direct credibility from A to B. The expectation is based on an observation of history behaviors and evaluation information derived from A to B, so we define such expectation of future behaviors of B deduced from the observation information from C to B achieved by A from C as indirect credibility of A to B, which is based on an observation of history behaviors and evaluation information from C to B.

In the stage of data transmission, nodes need to select routing paths, that is to say next hop node. Trust value obtained from the evaluation of trust system will be a basis of selecting routing, and the arbitrary node will try to choose neighbor nodes with high trust value and high energy surplus ratio as routing node. As for neighbor nodes whose trust value is lower than threshold value, the node will submit mistrust reports to base station. If base station receives the same mistrust report from different nodes to some node many times, it will exclude the node from routing table, so as to achieve the goal that the network consists of trusted nodes.

In the process of routing in WSNs, each node will generate a neighbors list, which stores other nodes identification (ID) within its communication region, meanwhile every ID corresponds to credibility. Therefore, every node has a credibility list, which saves the credibility of other nodes from this node. The credibility of node can be divided into two parts- direct credibility and indirect part, in which direct credibility is calculated from downstream nodes of routing announcement nodes according to the state of forwarding packets by routing announcement nodes; indirect credibility is deduced from neighbor nodes via monitoring the state of forwarding packets by routing announcement nodes. Combining direct credibility with indirect credibility, the total credibility of routing announcement nodes can be calculated so as to judge whether the node is trusted.

4.2. Establishment and Calculation of Node Trust

Trust value uses to judge whether monitored nodes are malicious; it is also an expectation for future behaviors of monitored nodes and has close relationship with past behaviors of monitored nodes. As an evaluation of past behaviors, reputation can use to calculate current trust

value. This paper will adapt reputation model to detect whether to exist malicious nodes.

Bayesian can calculate posterior probability via prior probability as shown in Equation (1) $P(B_j)$ means the prior probability, and $P(B_j \mid A)$ means the posterior probability. The priori probability is probability according to random events calculated from past experience. The posterior probability, after random experience, means an amendment for priori probability $P(B_j)$ under conditions of A resulted from random experience. Therefore, via combination the prior probability with the posterior probability, it can calculate probability of future possible completed tasks according to situation of past data forwarding completed by node.

$$P(B_j \mid A) = \frac{P(B_j)P(A \mid B_j)}{\sum_{i=1}^{n} P(B_i)P(A \mid B_i)},\ j = 1,2,...,n \tag{1}$$

where $B_j\ (j = 1,2,...,n)$ presents a combination of events, which means that a particular detecting node gets a special reputation value and $P(B_j) > 0$. A means a specific observed event.

In order to reflect dynamic changes of node trust values as time goes by, we need to improve accuracy of node trust evaluation. This paper will adopt a method of sending detected packets regularly to update reputation value. The event that packets forwarded by j from i is expressed as $(\theta_{ij})_t$ at the time t. The behavior that i observes the behaviors of j from $t-1$ to t is expressed as $(D_{ij})_t$. So it comes to the following formula:

$$P\left[(\theta_{ij})_t\right] = \frac{P\left[(\theta_{ij})_{t-1}\right]P\left[(D_{ij})_t \mid (\theta_{ij})_{t-1}\right]}{\sum_{l=0}^{t-1} P\left[(\theta_{ij})_l\right]P\left[(D_{ij})_t \mid (\theta_{ij})_l\right]} \tag{2}$$

$P\left[(\theta_{ij})_t\right]$ not only is the probability of an event that j completes tasks derived from i, but also is the prior probability of reputation derived from i to j, where this reputation is denoted as $(R_{ij})_t$. We can see that, $(R_{ij})_t$ is not only the posterior probability of node reputation at the time $t-1$, but also the priori probability at the time t.

On the assumption that i has assigned tasks to j for $m+n$ times, j has completed tasks for m times with the probability x, so the past reputation derived from i to j is belonged to binomial distribution $B(m+n,x)$. The priori probability of next task completed is belonged to homogeneous distribution $U(0,1)$ on (0, 1) under no previous knowledge. As for individual monitored node, the monitored node has only two types of behavior: forwarding data or not forwarding data. Therefore, the binomial distribution can be used to model for the monitored nodes. The probability of completing next task θ by j obeys that

$$P(\theta) = \frac{U(0,1)B(m+n,x)}{\sum_{l=0}^{t-1} P[(\theta_{ij})_l]P[(D_{ij})_t \mid (\theta_{ij})_l]} \tag{3}$$

So the posterior probability of completing next event θ by j will be as follows

$$P(\theta) = \frac{(m+n+1)!x^m(1-x)^n}{m!n!} \tag{4}$$

This paper draws on the experience of beta reputation system of e-commerce, and introduces establishment for node's trust model, because beta distribution expresses node's reputation. The probability density function of beta distribution can be described as follows

$$f(x \mid p,q) = \frac{1}{B(p,q)}x^{p-1}(1-x)^{q-1},\ 0 < x < 1,\ p > 0, q > 0 \tag{5}$$

where

$$B(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}\,dx,\ 0 < x < 1,\ p > 0, q > 0 \tag{6}$$

The beta-family of probability density functions is a continuous family of functions indexed by the two parameters p and q. The beta distribution $f(x \mid p,q)$ can be expressed using the gamma function Γ as

$$f(x \mid p,q) = \frac{\Gamma(p+q)}{\Gamma(p)\Gamma(q)}x^{p-1}(1-x)^{q-1},\quad 0 < x \le 1,\ p > 0,\ q > 0 \tag{7}$$

with the restriction that the probability variable $x \neq 0$ if $p \neq 1$, and $x \neq 1$ if $q < 1$. The probability expectation value of the beta distribution is given by

$$E(x) = \frac{p}{p+q} \tag{8}$$

Considering the property of gamma function, $\Gamma(m) = (m-1)!$, Equation (4) can be changed into:

$$P(\theta) = \frac{\Gamma(m+n+2)x^m(1-x)^n}{\Gamma(m+1)\Gamma(n+1)} \tag{9}$$

So $P(\theta)$ is subject to $\beta(m+1,n+1)$ distribution

compared Equation (7) with Equation (9) The reputation derived from i to j is that

$$R_{ij} = \beta(m+1, n+1) \tag{10}$$

The expectation of completing next task derived from i to j can be calculated by the previous formula, namely the credibility of i to j. Let the direct credibility denote as $(R_{ij})_D$, so the credibility of routing announcement node is calculated by its downstream nodes. Equation (12) can be deduced by the expectation of beta distribution Equation (11):

$$E[\beta(m+n)] = \frac{m}{m+n} \tag{11}$$

$$(R_{ij})_D = E[\beta(m+1, n+1)] = \frac{m+1}{m+n+2} \tag{12}$$

We suppose that m equals to kn, where k is set as 9, 5, 1, 1/5 and 1/9 respectively, so the relationship between the credibility and $m+n$ can be described as **Figure 1**.

We can see from **Figure 1** that node's credibility will increase as the number of tasks completed by node that the number of forwarding packets successfully increases; on the contrary, nodes credibility will be decrease as the number of uncompleted tasks that the number of forwarding packets unsuccessfully is larger. The behaviors of forwarding packets as a judge basis can reflect true situation of node.

4.3. The Initialization of Node Trust Value

For the sake of description, we introduce two concepts: routing node and non-routing node. Routing node is a type of next hop neighbor node selected to forward packets to the base station. Non-routing node means one of neighbor nodes except routing nodes. The credibility system mainly uses to ensure route security, therefore in order to save unnecessary expenses, the trust evaluation is only for routing nodes, however half trust attitude is adopted for non-routing nodes (that is to say that the credibility of non-routing nodes is set as 0.5). Note that non-routing node is not fixed, it is possible to become a routing node at some time, and when a non-routing node has been changed into a routing node, the system will re-evaluate the node's credibility.

We have detailed the ideas and methods of node's trust assessment in Section 4.2. This section will describe initialization of node trust value in beta credibility system based on energy load balancing. The node trust value of the system is between 0 and 1, which can evaluate comprehensively direct trust value and indirect trust

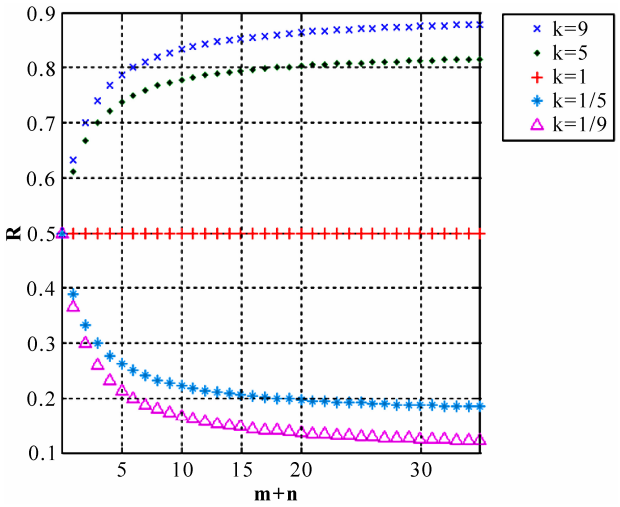

Figure 1. Impact on the credibility derived from the ratio between *m* and *n*.

value. The initialization of node trust values will start after establishment of WSNs and route discovery. Trust values of routing nodes will be initialized by trust detect mechanism, while trust values of non-routing nodes will be set as 0.5 initially. On the assumption that j is routing node of i, m means the number of packets forwarded by j successfully, and n represents the number of packets forwarded by j unsuccessfully, the direct trust value of i to j is that

$$(R_{ij})_D = E[\beta(m+1, n+1)] = \frac{m+1}{m+n+2} \tag{13}$$

Suppose k is a common neighbor node of i and j, m_j^k means the number of packets forwarded by j successfully in the process of trust detection by k, n_j^k means the number of packets forwarded by j unsuccessfully in the process of trust detection by k, R_{ik} represents general trusted assessment of i on k, then the indirect trust value of i to j is that

$$(R_{ij})_{ID} = \sum_k R_{ik} \frac{m_j^k + 1}{m_j^k + n_j^k + 2} \tag{14}$$

In the credibility system, one node has absolutely believed in its direct assessment for other nodes, while has reservedly trust in recommended assessment derived from other nodes for evaluated nodes. In order to prevent malicious slander or have a common conspiracy to enhance trust value of a malicious node, it should make a consideration of its trust of recommended nodes while combined with recommended credibility own. The overall credibility of i to j is that

$$R_{ij}=\begin{cases}0.5,\ j \text{ is a non-routing node},\\ \dfrac{\left(R_{ij}\right)_D+\sum_k R_{ik}\dfrac{m_j^{\,k}+1}{m_j^{\,k}+n_j^{\,k}+2}}{1+\sum_k R_{ik}},\ j \text{ is a routing node}\end{cases} \tag{15}$$

It can be seen from Equation (15) that R_{ij} directly depends on the ratio between m and n. The more this ratio is, the higher the trust value of node will be gotten; vice versa. It is in accord with the design of evaluating trust value of node via forwarding packets, and has a finer defensive effect for malicious loss packets of nodes.

4.4. The Update of Node Credibility Value

The behavior of node may change as time goes by, so the credibility system must update the trust values of nodes dynamically. The credibility system adopts a method of opening detection mechanism regularly to monitor changes of routing node's behaviors and update routing node trust value dynamically, so that reflect the changes of the sensor network in time and ensure the security of data transmission, as for non-routing node without updating.

Suppose that j is a routing node of i with m and n obtained in a new round of trust detection, we define the aging parameters ω_{age} as the impact on current trust evaluation derived from past detected data, then

$$m_{new}=m_{old}\times\omega_{age}+m \tag{16}$$

$$n_{new}=n_{old}\times\omega_{age}+n \tag{17}$$

Therefore the direct trust value of i to j can be updated that

$$\left(R_{ij}\right)_{Dnew}=\frac{m_{new}+1}{m_{new}+n_{new}+2} \tag{18}$$

In the credibility system, when considers historical behaviors of nodes, it should also take sensitivity of updating trust values into account and needs reflect the behavior changes of nodes in time. Therefore, we consider historical behaviors in direct trust while consider current behaviors in indirect trust. On the assumption that $\left(m_{jnew}^{k},n_{jnew}^{k}\right)$ is derived from monitoring of k on j in a new round of trust detection, then the overall trust value of i to j can be updated to Equation (19).

In the course of updating credibility system, we not only take reputation accumulated by history behaviors of nodes into account, but also need consider sensitivity of trust changes dynamically, so that it needs to reflect behavior changes of nodes in order to minimize the impact on network after some nodes being captured.

4.5. Trust Decision

The main objective of the credibility system is to select trust routing nodes and network topology excluding malicious nodes to ensure security of data transmission. At the same time, taken limitation of sensor node's power into account, neighbor nodes will regard the node as a routing node for a long time, and then the node's power may be run out quickly so that it may lead to partial failure of sensor network. In order to prevent above situation, it need consider energy load balancing. Therefore, trust decision is very important.

We suppose that E_j is residual energy rate of j, and ω_r, ω_e mean trust weights and energy weights respectively. The trust decision value, T_{ij}, is defined as

$$T_{ij}=\omega_r\times R_{ij}+\omega_e\times E_j \tag{20}$$

We define R_t as the trust threshold of system. When i makes a decision to select next hop routing node j, it obeys the following decision-making principles:

1) Select routing node with $R_{ij}>R_t$;

2) If many trust values are all higher than R_t, select one of nodes with the greatest T_{ij};

3) If many T_{ij} are same, choose one of routing nodes with the highest R_{ij};

4) If many R_{ij} are same, then choose one of routing nodes with the shortest routing path.

After above decision-making, the routing node has higher credibility with more remaining energy. The energy surplus ratio used in system also prevents the use of high-power devices from attacking via using energy defects of WSNs. As for one routing node with trust value lower than R_t, it will send a warning report to base station. If base station recesives the same of warning report from many nodes to a certain node, base station will

$$R_{ijnew}=\begin{cases}0.5,\ j \text{ is a non-routing node},\\ \dfrac{(R_{ij})_{Dnew}+\sum_k R_{iknew}\dfrac{m_{jnew}^{k}+1}{m_{jnew}^{k}+n_{jnew}^{k}+2}}{1+\sum_k R_{iknew}},\ j \text{ is a routing node}\end{cases} \tag{19}$$

exclude this node from network topology, so that the network consists of trust nodes.

5. Performance Analysis and Simulations of Trust Routing Protocol

5.1. Performance Analysis of TRP and INSENS

INSENS (INtrusion-tolerant routing protocol for wireless Sensor NetworkS) is a well-designed secure routing protocol, which achieve data efficient transmission by making use of redundant routing [9]. In WSNs, it is essential to save energy for the protocol designation; however, INSENS cannot overcome more waste of energy from sending packets multiply. We will introduce beta trust model into INSENS to set up the trust detection mechanism, evaluate routing node credibility, and make decision to choose some routing nodes to forward packets. We will analyze security of our protocol based on the beta trust model, called trust routing protocol (TRP) after introduction of trust management model and resist against current different typical attacks in WSNs.

In order to ensure packets to be forwarded to base station safely, the way of sending packets of INSENS is shown in **Figure 2** (redundant routing mode). A data packet is copied into a number of ectypes. The transmission path takes on a tree structure in network. Suppose that a certain node with H hops to base station has N ($N > 1$) routing paths, and each intermediate forwarding node has all N routing paths, and then including the number of packets sent by source nodes and intermediate forwarding nodes, the quantity of packets generated by sending a data packet is that

$$S = \sum_{i=1}^{i=H} N^i + N^H = 2N^H + \frac{N^H - N}{N - 1} \tag{21}$$

Whereas the quantity generated under TRP is that

$$S = H + 1 \tag{22}$$

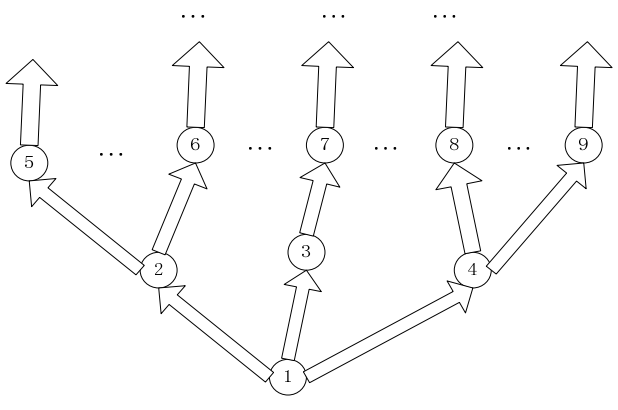

Figure 2. INSENS: redundant routing protocol mode.

As the expansion of network scale, INSENS will make network load increase exponentially, while the consumption of TRP for network resource will almost increase linearly. Thus, as long as proper control of communication consumption in the process of trust detection, the communication consumption of TRP is much smaller than INSENS. It can reduce node's energy consumption and save network resources greatly, and be conducive to network expansion. But the computing expense derived from introduction of trust evaluation system relative to communication expense is almost negligible.

5.2. Emulation of TRP and INSENS

The main goal of introducing beta trust model into INSENS is to give up the way of sending packets multiply via redundant routing path, and to adopt a way of trust routing paths to send packets, which reduces energy consumption of nodes and prolongs the survival time of network, meanwhile alleviates network load and saves communication resources.

In order to verify TRP described in this paper with an introduction of energy load balancing beta trust model whether satisfy the goal of this paper, this subsection will make simulations for TRP and INSENS, and compare the performance of two protocols according to simulations. The weights used in the simulation are set as follows: weight_old = 0.6, weight_trust = 0.8, weigth_energy = 0.2, R_t = 0.6.

The paper will adopt two following evaluation indexes to compare and analyze the performance of TRP and INSENS.

1) The number of transmitted packets

Under the same conditions of sending the same packets, compare the total quantity of packets sent by all nodes in the course of sending packets from source node to destination node, including packets sent by source node and forwarded by intermediate node. Because the energy consumption of network is mainly embodied in sending packets, this performance index can reflect not only the difference of energy consumption in the process of communication, but also the situation of network resources usage.

2) Packet loss

It means a ratio of the number of packets not received by destination node to the number of packets sent by source node. This performance index can reflect the impact on the protocol to network communication and whether it is applicable to WSNs. The protocol with higher packet loss is not obviously suitable to network communications.

This paper also includes simulation of dynamic changes of routing node trust value in order to verify two additional problems: first, the ability of TRP resisting malicious attacks; second, whether the node could dis-

cover malicious routing nodes on upstream then exclude them and select trust nodes. According to simulations, we design two following scenarios.

Scenario 1: Suppose that there is a coordinate system with base station at (0, 0). 100 nodes are distributed randomly within the range of 1000*1000m^2 in coordinate system, and node's communication distance is 250m. INSENS and TRP will generate redundant routing paths. For the sake of simplicity, the simulation will generate two routing paths for each node as possible, however some nodes may have a routing path because of topological structure. The system will select four nodes randomly to generate 4 cbr data streams, where each cbr data stream sends two packets per second, the length of one data packet is 512 bytes, and the simulation time is 30 seconds. In trust routing, it can be seen from **Figure 1**, when the number of packets detected by the system reaches 30, it is more accurate for evaluation of node trust value. Therefore, we select 30 packets sent by trust detection at a time in simulation. In this scenario, it will make a statistics about the number of transmitted packets as shown in **Figure 3** and packet loss as shown in **Figure 4** in INSENS and TRP respectively.

Figure 3 shows that although the number of packets sent by TRP is much more than INSENS in the initial stage, after 12 seconds the later surpassed the former and the gap between the two protocols becomes larger and larger as time goes by. Because TRP starts trust routing detection at the beginning and consume a certain amount of network resources, once completes trust detection, packets are forwarded in accordance with trust routing. However INSENS always forwards packets according to redundant routing. On the assumption that there are h hops between the node N_a and base station, and each node has two routing paths, then the total quantity of transmitted packets reaches about (3 * 2h-2) (2 + 22 + 23 + ... + 2 * 2h). Obviously, according to INSENS, middle nodes may discard duplicated packets, meanwhile because of signal conflict, network congestion and so on, it also drops some packets, and in fact the quantity of a packet transmitted in network may not reach (3 * 2h-2). **Figure 2** shows the network consumption of INSENS is much more than that of TRP when sending the same source packets, so the improvement derived from introduction of trust evaluation system indeed saves a lot of energy and network resources, extending survival time of WSNs and improving effectiveness of completing tasks.

It can be seen from **Figure 4**, the average packet loss of TRP is about 2.5%, which is higher than INSENS, because of WSNs with higher packet loss. In TRP, source packets are forwarded to base station only along a routing path, while in INSENS, source packets are spread over the network via redundant routing paths. There are many copies of packets sent to base station through multiple paths. Thus, INSENS has a slightly

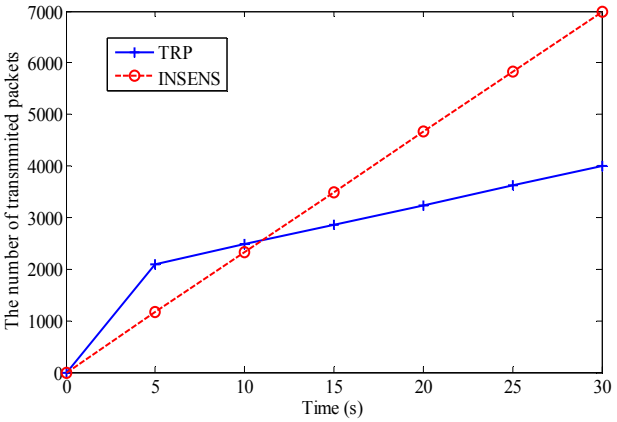

Figure 3. The number of transmitted packets.

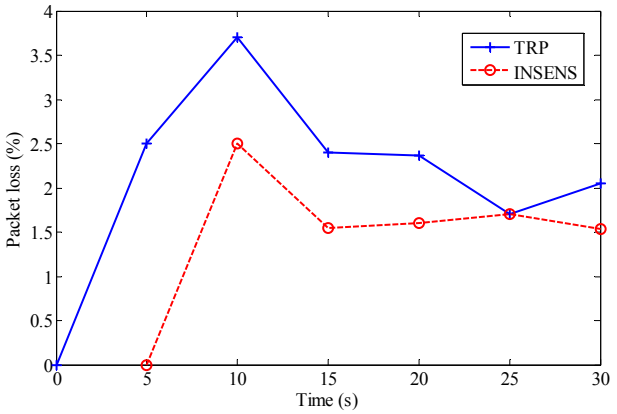

Figure 4. Packet loss.

lower packet loss. However, as expansion of network scale and frequency of sending packets raises, the consumption of INSENS for network resources will increase exponentially, also it will result in more serious network congestion and channel conflict, and its packet loss will increase greatly. Whereas the consumption of TRP for network resources under above mentioned situation will almost increase linearly, it is much better than INSENS in terms of network congestion and channel conflict.

Scenario 2: Suppose that there is a coordinate system with base station at (0, 0). 100 nodes are distributed randomly within the range of 1000*1000m^2 in coordinate system, and node's communication distance is 250m. The interval time of trust update is 30 seconds, and simulation time is 60 seconds. In TRP, base station generates three routing paths for N_V, of which the next hop nodes are N_A, N_B and N_C. In the initial stage, N_A, N_B and N_C are all healthy nodes, while N_B will be captured within 0 ~ 30 seconds, which will discard all packets without forwarding. In this simulation scenario, trust values of N_V to N_A, N_B and N_C can be shown in **Figure 5**.

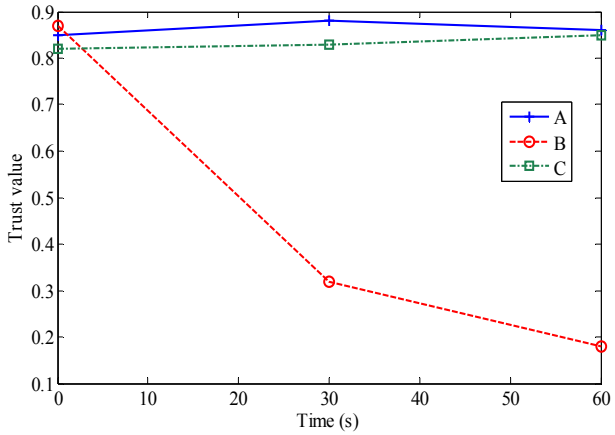

Figure 5. Trust values of N_V to N_A, N_B and N_C.

It can be seen from **Figure 5**, the healthy node has relative higher trust value at 0s, namely at the time of initialization. When updating trust at 30s and 60s, its trust value descends quickly due to that N_B is captured and discards packets maliciously, while N_A and N_C have still higher trust values. So we can see that trust value of this paper can evaluate node behaviors accurately, and detect malicious behaviors in time. The network may select trust nodes to cooperate and minimize harm resulted from malicious nodes as possible by trust assessment.

6. Conclusions

Nowadays it proves to be difficult to authenticate the network entity in distributed network environment, especially in resource-constrained WSNs. Dynamic trust management provides a novel solution of the security in distributed environment. Due to own features of WSNs, however, the traditional trust model fails to be applied in the WSNs.

This paper proposes the beta trust model based on energy load balancing, which is remarkable in computation, communication consumption and energy load balancing, combining with the trust system model and beta trust model in the e-commerce. The simulation results indicate that the evaluated node trust value reflects the node behaviors effectively. And our model achieves the expected security goal with low energy and network consumption in WSNs.

7. Acknowledgements

This work was sponsored by the National Natural Science Foundation of P.R. China (No. 60973139, 60773041, 60905040), the Natural Science Foundation of Jiangsu Province (BK2008451), Postdoctoral Foundation of Jiangsu Province (0801019C), Science & Technology Innovation Fund for Higher Education Institutions of Jiangsu Province (CX08B-085Z, CX08B-086Z), and the Six Kinds of Top Talent of Jiangsu Province (2008118).

8. References

[1] C. Karlof and D. Wanger, "Secure Routing in Wireless Sensor Networks: Attacks and Counter-Measures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, IEEE Computer Society, Anchorage, May 2003, pp. 113-127.

[2] D. Liu and P. Ning, "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks," *Technical Report*: *North Carolina State University at Raleigh*, September 2002.

[3] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management," *Proceedings of the* 17*th Symposium on Security and Privacy*, 1996.

[4] M. Blaze, J. Feigenbaum and J. Ioannidis, "The KeyNote Trust Management System," Version 2, *Internet Engineering Task Force*, September 1999.

[5] N. H. Li, J. C. Mitchell, W. H. Winsborough, "Design of a Role-Based Trust Management Framework," In Header, H. Ed., *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Washington, 2002, pp. 114-130.

[6] P. Resnick and R. Zeckhauser, "Trust among Strangers in Internet Transactions: Empirical Analysis of eBya's Reputation System," *National Bureau of Economic Research Workshop on Empirical Studies of Electronic Commerce*, 2000.

[7] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol," *Proceedings of ACM Mobihoc*, 2002.

[8] L. Xiong and L. Liu, "A reputation-Based Trust Model for Peer to Peer Ecommerce Communities," *IEEE Conference on E-Commerce*, 2003.

[9] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks," *Department of Computer Science Technical Report CU-CS*-939-02, University of Colorado, Boulder, 2006.

