Hindawi Publishing Corporation
Journal of Sensors
Volume 2014, Article ID 649392, 10 pages
http://dx.doi.org/10.1155/2014/649392

Research Article

BeTrust: A Dynamic Trust Model Based on Bayesian Inference and Tsallis Entropy for Medical Sensor Networks

Yan Gao[1,2] and Wenfen Liu[1,2]

[1]*Zhengzhou Institute of Information Science and Technology, Zhengzhou 450002, China*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China*

Correspondence should be addressed to Yan Gao; gaoyan_yangao@163.com

Received 24 July 2014; Revised 11 November 2014; Accepted 11 November 2014; Published 3 December 2014

Academic Editor: Romeo Bernini

With the rapid development and application of medical sensor networks, the security has become a big challenge to be resolved. Trust mechanism as a method of "soft security" has been proposed to guarantee the network security. Trust models to compute the trustworthiness of single node and each path are constructed, respectively, in this paper. For the trust relationship between nodes, trust value in every interval is quantified based on Bayesian inference. A node estimates the parameters of prior distribution by using the collected recommendation information and obtains the posterior distribution combined with direct interactions. Further, the weights of trust values are allocated through using the ordered weighted vector twice and overall trust degree is represented. With the associated properties of Tsallis entropy, the definition of path Tsallis entropy is put forward, which can comprehensively measure the uncertainty of each path. Then a method to calculate the credibility of each path is derived. The simulation results show that the proposed models can correctly reflect the dynamic of node behavior, quickly identify the malicious attacks, and effectively avoid such path containing low-trust nodes so as to enhance the robustness.

1. Introduction

Nowadays, with the rapid development of wireless communication technology and wearable medical sensors, the wireless medical sensor network becomes a promising technology and is changing the way people seek medical treatment [1]. For electronic health, the development of medical sensor networks (MSNs) is very necessary. Patient health status can be remotely sensed, processed in real time, and transferred to the hospital or medical centre, which will take the place of face-to-face diagnosis [2]. There are many successful cases in real life, such as emergency electronic health, family monitoring, transmission of medical data, and remote surgery [3]. However, due to the sensitivity of the medical data and the openness of the wireless channel to communicate, medical sensor networks are exposed to many potential threats. Consequently, how to guarantee their security has become a big challenge to be resolved [4].

Owing to these unique characteristics of MSNs and vulnerability to a wide variety of abnormal node behaviours, the traditional cryptography techniques [5] cannot meet the requirements of security and credibility. As a consequence, medical data are extremely likely to be freely modified or discarded by the attackers; for instance, compromised nodes may inject error messages and malicious nodes probably intercept and modify information, inject false information, replay old messages, and send a large number of false packages to block communication channel. Accordingly, trust management as a kind of soft security mechanism [6] has been introduced for the sake of solving the aforesaid problems. TrE proposed by Boukerche and Ren [7] is the first trust evaluation model applied to medical sensor networks, which is put forward for secure multicast routing. In consideration of the unique operation and security requirements, combining the simple cryptographic mechanisms with dynamic trust management, He et al. suggested an application-independent and distributed trust evaluation model for MSNs to guarantee the security of medical sensor networks [8]. In addition, ReTrust, an attack-resistant and lightweight trust management protocol, was designed specifically for MSNs with a two-tier architecture [9].

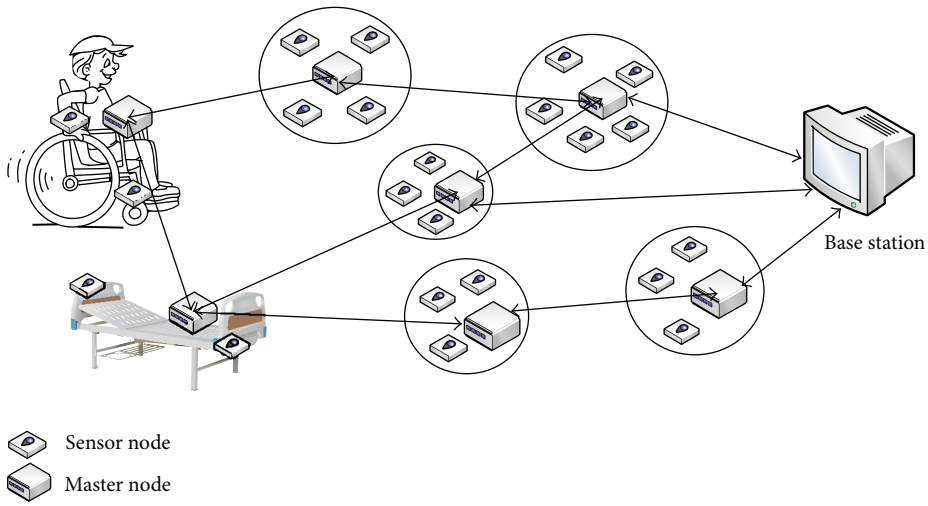

Figure 1: The two-layer architecture of MSNs.

Although the existing researches have made great progress, they are still in need of improvements in the following aspects. For one thing, these studies mainly focus on the establishment of trust models with regard to a single node, which are simple and coarse-grained. As is known to all, medical data are diverse and are of different importance. Thus they should be distinguished and the more important data should be transmitted through the more trustworthy nodes and paths. For this reason, it is very necessary to construct a fine-grained trust model according to the importance of medical data to investigate the credibility of a single node, which can effectively avoid the strategic attacks. In order to achieve this purpose, Bayesian inference is adopted to measure the credibility of a single node in each interval, in which the interactions from neighbour nodes are used to obtain the prior information and the direct interactions are used to get the posterior distribution to estimate the trust value.

For another aspect, these works did not specify the measurement of the trust about the paths with several intermediate nodes from the source master nodes to the base station. The aforementioned trust model of single node is the basis of the path trust model. Building trust relationship between network nodes can be used to develop high-level security solutions as auxiliary, such as security routing. Therefore, based on trust degrees of network nodes, a trust evaluation model with Tsallis entropy to measure the trustworthiness of each path is proposed in this paper. In the last respect, in the process of integrating several trust values into overall trust degree, the corresponding weights are obtained by using the ordered weighted vector twice, in which time sequence and relative size order are viewed as the induced factor, respectively. The medical data and packets are interchangeable hereinafter.

The structure of this paper is as follows. Section 2 simply reviews the two-layer architecture model for MSNs given in [9] and traditional cryptography techniques are introduced to guarantee the security of medical data. Based on Bayesian inference, a method to measure the credibility of single node with different importance is developed in Section 3. On this basis, with the properties of Tsallis entropy, path Tsallis entropy is defined to measure the uncertainty of each path from the source master nodes to the base station, and then the trustworthiness of each path is put forward in Section 4. Simulation experiments and result analysis are presented in Section 5.

2. The Architecture of MSNs and Involved Cryptography Techniques

2.1. The Two-Layer Architecture of MSNs. The two-layer architecture was proposed applicable to medical sensor networks [9]. The whole MSN is composed of several clusters, and each cluster comprises a master node and a certain amount of sensor nodes. Each sensor node is mainly responsible for perception to acquire relevant medical data, and then it delivers these data to the master node within its own cluster. All the master nodes have sufficient storage, computing, and energy resources. After gathering the medical data from some sensor nodes in the cluster, each master node takes charge of transmitting them to the base station through selecting the most trustworthy routing. Every sensor node only communicates with the master node in the cluster, while the master node can communicate and exchange information with the neighbour master nodes, and thus all the sensor nodes and master nodes constitute a two-layer and multihop network. It is specific as shown in Figure 1.

2.2. Involved Cryptography Techniques. As mentioned above, dynamic trust management must be combined with traditional cryptography techniques to ensure the security and credibility of MSNs. The proposed trust model is conducted based on some simple symmetric encryption/decryption

algorithms and public key cryptography. These are described in detail as follows.

(1) Due to some characteristics such as small capacity and limited resources, each sensor node employs the lightweight cryptography techniques [10] to encrypt medical data and then transmits them to the master node in its own cluster. Every master node is responsible for key distribution and update by adopting the public key techniques. All the sensor nodes in a cluster are with different keys.

(2) Different from the sensor nodes, each master node contains adequate resources and capacity, so that it is able to take advantage of general symmetric cryptography techniques to encrypt/decrypt the data. There are additional three kinds of keys in each master node. Firstly, one key is distributed and updated by the base station, which is similarly generated through some public key technique. The medical data collected from sensor nodes are encrypted with this key and further delivered to the base station. Secondly, a multicast key is applied between a master node and its neighbor master nodes. When it wants to send request information to some neighbor nodes, the master node encrypts the information with this key. Finally, a pairwise key between master nodes is necessary. When the neighbors return information corresponding to the request information, the key is used to encrypt the reply information. The multicast key cannot be substituted for this key in order to prevent other neighbor nodes to hijack or tamper the reply messages.

3. Computing the Credibility of Master Nodes

3.1. The Representation and Storage of Interaction Information. In the MSNs, a database and a trust evaluation system are built in each master node i. The database is used to store the interaction information with other neighbor master nodes and the trust evaluation system is established to measure the credibility of neighbor nodes and the paths from the master node to the base station. Denote $N(i)$ as a set including all the neighbor master nodes of node i. For any $j \in N(i)$, after delivering the packets to j, node i can record the forwarding information of node j with a quad $(j, g, r_{i,j}^g, \tau(r_{i,j}^g))$ in the database. The meaning of each symbol in the quad is specified as follows: the symbol g indicates the importance grade of packets whose value space is $\Omega = \{1, 2, \ldots, G\}$, and the greater the value, the more important the packets; $r_{i,j}^g$ represents the forwarding result, and

$$r_{i,j}^g = \begin{cases} 1, & \text{node } j \text{ forwards the packets} \\ & \text{to the next node successfully} \\ 0, & \text{else;} \end{cases} \quad (1)$$

$\tau(r_{i,j}^g)$ is the forwarding timestamp. Assuming that the current moment is t and action_g represents forwarding packets with importance g, trust degree $T_t\{i : j, \text{action}_g\}$ is defined as the probability that node i expects that node j will perform action_g at the current moment. Therefore, the credibility of node j from the perspective of node i can be expressed by a multidimensional vector:

$$T_t\{i : j\} = \left(T_t\{i : j, \text{action}_1\}, T_t\{i : j, \text{action}_2\}, \ldots, T_t\{i : j, \text{action}_G\}\right). \quad (2)$$

Hereinafter, abbreviate $T_t\{i : j, \text{action}_g\} = T_t^g(i, j)$, $g \in \Omega$.

As we know, trust has the characteristics of time decay; that is, the interaction results farther from the current moment have the weaker influence on the current trust value. As a consequence, those interactions only in a certain period close to the current time are necessary to be analyzed so as to obtain the current trust degree. Given $\Delta t > 0$ and $d^* > 0$, $d = \lfloor t/\Delta t \rfloor$, the time range in which these interaction records are considered is specified as

$$[u\Delta t, t) = [d\Delta t, t) \bigcup_{k=u}^{d-1} [k\Delta t, (k+1)\Delta t), \quad (3)$$

where $u = \max\{d - d^*, 0\}$. For convenience, set $\Lambda_k = [k\Delta t, k\Delta t + \Delta t_k)$, $u \le k \le d$, in which

$$\Delta t_k = \begin{cases} \Delta t, & u \le k \le d-1 \\ t - d\Delta t, & k = d. \end{cases} \quad (4)$$

Based on the above, node i first calculates the corresponding trust value $T_{t,k}^g(i, j)$ in each interval Λ_k, and then $\{T_{t,k}^g(i, j),\ u \le k \le d\}$ are weighted to get the overall trust degree of node j.

3.2. Computation of $T_{t,k}^g(i, j)$ Based on Bayesian Inference. For any $u \le k \le d$, the event $A_k^g(j)$ represents that node j forwards packets of importance g successfully in the interval Λ_k, whose probability is denoted by $\theta_k^g(j) = P(A_k^g(j))$. Assume random variable $X_k^g(j)$ is the number of $A_k^g(j)$ occurrence in n independent observations; $X_k^g(j)$ obeys the binomial distribution $b(n, \theta_k^g(j))$. Denote $R_{i,j}^g(k) = \{r_{i,j}^g : \tau(r_{i,j}^g) \in \Lambda_k\}$ and $N(i, j) = N(i) \cap N(j)$ represents the common neighbor master nodes of nodes i and j. In order to derive $T_{t,k}^g(i, j)$, it is crucial that node i combines $R_{i,j}^g(k)$ with $\bigcup_{v \in N(i,j)} R_{v,j}^g(k)$ to deduce the estimation $\tilde{\theta}_k^g(j)$ of $\theta_k^g(j)$. In the following, Bayesian inference [11] is adopted to obtain the estimation $\tilde{\theta}_k^g(j)$. Since the conjugate prior distribution of $\theta_k^g(j)$ is Beta distribution $B(\alpha_k, \beta_k)$, node i views $\{R_{v,j}^g(k),\ v \in N(i, j)\}$ as the prior information to estimate the two hyper parameters α_k and β_k with the method of prior moment, integrates the direct interactions $R_{i,j}^g(k)$ to acquire the posterior distribution, and computes its expectation as the estimation of $\theta_k^g(j)$. From the above mentioned, $T_{t,k}^g(i, j)$ is derived based on Bayesian inference through the following steps.

Step 1. Master node i checks whether there are common neighbor nodes with node j; if $N(i, j) = \phi$, then skip to Step 4; else, it sends trust request information to all the common neighbors.

Step 2. For any $v \in N(i,j)$, after receiving the request information, node v looks over its own interaction records and calculates an estimation $\theta^g_{t,k}(v,j)$ of $\theta^g_k(j)$ in every interval Λ_k:

$$\theta^g_{t,k}(v,j) = \frac{N_k\left(r^g_{v,j}=1\right)}{N_k\left(r^g_{v,j}=1\right)+N_k\left(r^g_{v,j}=0\right)}, \tag{5}$$

in which $N_k(r^g_{v,j}=\sigma) = |\{r^g_{v,j} : r^g_{v,j} \in R^g_{v,j}(k), r^g_{v,j}=\sigma\}|, \sigma = 0,1$. In particular, if $R^g_{v,j}(k)=\phi$, denote $\theta^g_{t,k}(v,j)=-1$. Then node v returns this information $\Theta^g_t(v,j) = \{\theta^g_{t,k}(v,j),\ u \le k \le d\}$ to node i.

Step 3. After receiving $\{\Theta^g_t(v,j), v \in N(i,j)\}$, node i computes the estimation values of parameters about Beta distribution with the method of prior moment. Set

$$B^g_{t,k}(i,j) = \left\{v : v \in N(i,j), \theta^g_{t,k}(v,j) \ne -1\right\}; \tag{6}$$

then

$$\begin{aligned}\overline{\theta}^g_{t,k}(j) &= \frac{1}{\left|B^g_{t,k}(i,j)\right|}\sum_{v\in B^g_{t,k}(i,j)}\theta^g_{t,k}(v,j),\\ S^g_{t,k}(j)^2 &= \frac{1}{\left|B^g_{t,k}(i,j)\right|-1}\sum_{v\in B^g_{t,k}(i,j)}\left(\overline{\theta}^g_{t,k}(j)-\theta^g_{t,k}(v,j)\right)^2.\end{aligned} \tag{7}$$

Therefore, the estimation values of hyper parameters α_k and β_k are

$$\begin{aligned}\widehat{\alpha}_k &= \overline{\theta}^g_{t,k}(j)\left(\frac{\left(1-\overline{\theta}^g_{t,k}(j)\right)\overline{\theta}^g_{t,k}(j)}{S^g_{t,k}(j)^2}-1\right),\\ \widehat{\beta}_k &= \left(1-\overline{\theta}^g_{t,k}(j)\right)\left(\frac{\left(1-\overline{\theta}^g_{t,k}(j)\right)\overline{\theta}^g_{t,k}(j)}{S^g_{t,k}(j)^2}-1\right).\end{aligned} \tag{8}$$

Step 4. When $N(i,j)=\phi$, set $(\widetilde{\alpha}_k, \widetilde{\beta}_k) = (1,1)$; otherwise $(\widetilde{\alpha}_k, \widetilde{\beta}_k) = (\widehat{\alpha}_k, \widehat{\beta}_k)$. Then Beta distribution $B(\widetilde{\alpha}_k, \widetilde{\beta}_k)$ is viewed as the prior distribution of $\theta^g_k(j)$. Node i checks its own interaction information $R^g_{i,j}(k)$ as the posterior information in each interval Λ_k and obtains trust value $T^g_{t,k}(i,j)$. In the case that $R^g_{i,j}(k)=\phi$

$$T^g_{t,k}(i,j) = \widetilde{\theta}^g_k(j) = E\left[\theta^g_k(j)\right] = \frac{\widetilde{\alpha}_k}{\widetilde{\alpha}_k+\widetilde{\beta}_k}. \tag{9}$$

While $R^g_{i,j}(k) \ne \phi$, combining $B(\widetilde{\alpha}_k, \widetilde{\beta}_k)$ as the prior distribution with the interaction record $R^g_{i,j}(k)$, the posterior distribution of $\theta^g_k(j)$ is

$$\begin{aligned}&\pi\left(\theta^g_k(j) \mid R^g_{i,j}(k)\right)\\ &\quad= \frac{\Gamma\left(N_k\left(r^g_{i,j}=1\right)+N_k\left(r^g_{i,j}=0\right)+\widetilde{\alpha}_k+\widetilde{\beta}_k\right)}{\Gamma\left(N_k\left(r^g_{i,j}=1\right)+\widetilde{\alpha}_k\right)\Gamma\left(N_k\left(r^g_{i,j}=0\right)+\widetilde{\beta}_k\right)}\\ &\qquad\times\theta^g_k(j)^{N_k(r^g_{i,j}=1)+\widetilde{\alpha}_k-1}\left(1-\theta^g_k(j)\right)^{N_k(r^g_{i,j}=0)+\widetilde{\beta}_k-1}.\end{aligned} \tag{10}$$

Thus trust value $T^g_{t,k}(i,j)$ is further given as

$$\begin{aligned}T^g_{t,k}(i,j) &= \widetilde{\theta}^g_k(j) = E\left[\theta^g_k(j)\right]\\ &= \frac{N_k\left(r^g_{i,j}=1\right)+\widetilde{\alpha}_k}{N_k\left(r^g_{i,j}=1\right)+N_k\left(r^g_{i,j}=0\right)+\widetilde{\alpha}_k+\widetilde{\beta}_k}.\end{aligned} \tag{11}$$

Although there are generally 3 kinds of Bayesian estimation based on the posterior distribution, the mean square error is minimized if the posterior mean is viewed as the Bayesian estimation. And in the case of the binomial distribution, the posterior mean value is more appropriate than maximum posterior estimation; therefore, formulas (9) and (11) both adopt the posterior mean values as the estimation $\widetilde{\theta}^g_k(j)$. At this point, node i obtains the trust values of node j in all the intervals; that is, $\{(\Lambda_k, T^g_{t,k}(i,j)),\ u \le k \le d\}$.

3.3. Weights Setting and Computation of Overall Trust Degree. Based on $\{(\Lambda_k, T^g_{t,k}(i,j)),\ u \le k \le d\}$, node i computes the overall trust degree of j by allocating the corresponding weights described in the following.

Definition 1 (overall trust degree). In the view of node i, the overall trust degree of node j at the current moment t is

$$T^g_t(i,j) = \sum_{k=1}^{d-u+1}\omega_k T^g_{t,k+u-1}(i,j). \tag{12}$$

In formula (12), $\omega_k \in [0,1]$ $(1 \le k \le d-u+1)$ and $\sum_{k=1}^{d-u+1}\omega_k = 1$.

The setting of weight coefficients is critical and two factors are mainly considered. On the one hand, due to the characteristics of time decay, the influence of $T^g_{t,k+u-1}(i,j)$ on the overall trust degree $T^g_t(i,j)$ dynamically attenuates as time evolves, so that $T^g_{t,k+u-1}(i,j)$ far from the present moment should be assigned a lower weight. That is to say, the smaller the k, the lower the corresponding weight. On the other hand, in order to punish the malicious behaviors, the lower trust value in the sequence $\{T^g_{t,k+u-1}(i,j),\ 1 \le k \le d-u+1\}$ should be given a higher weight. Based on the above two aspects, the weights are expressed twice using an ordered weighted vector. First of all, the induced ordered weighted averaging (IOWA) operator is introduced.

Definition 2 (IOWA operation [12]). Assume $\langle s_1, a_1\rangle, \langle s_2, a_2\rangle, \ldots, \langle s_m, a_m\rangle$ are m two-dimensional arrays. Denote

$$f\left(\langle s_1,a_1\rangle, \langle s_2,a_2\rangle, \ldots, \langle s_m,a_m\rangle\right) = \sum_{z=1}^{m}\mu_z a_{s\text{-index}(z)}; \tag{13}$$

then the function f is an m-dimensional ordered weighted averaging operation induced by $s_1, s_2, \ldots, s_m$, where s-index(z) is the subscript of the zth one among $s_1, s_2, \ldots, s_m$ arranged in increasing order of size and $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$ is named as an ordered weighted vector.

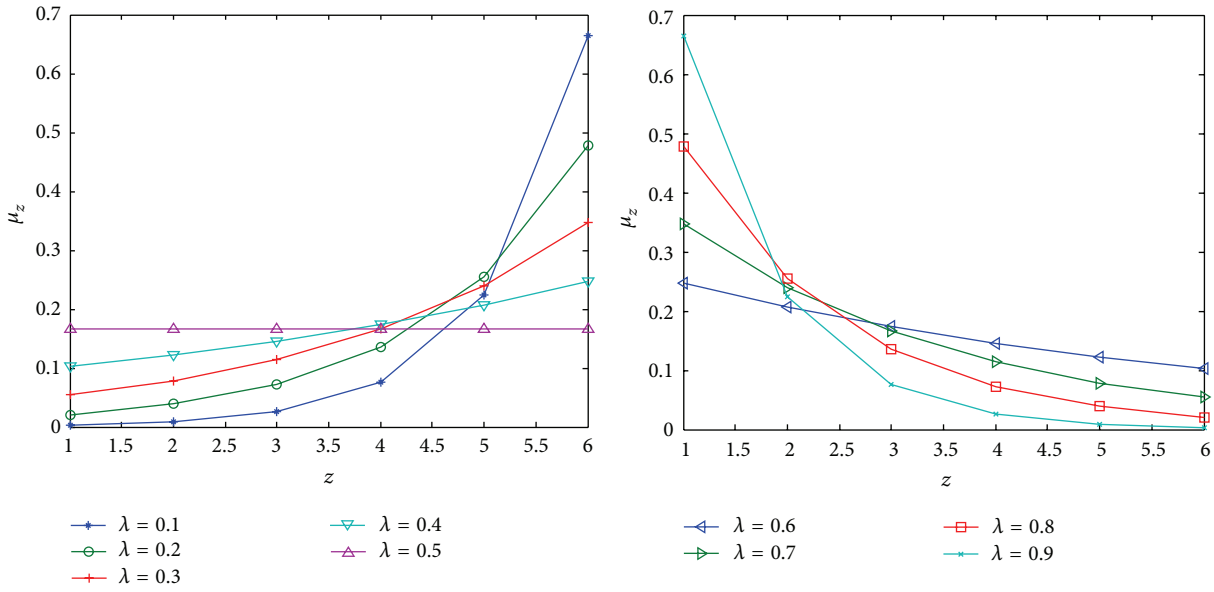

FIGURE 2: The changes of μ as λ varies.

Currently calculating the weighted vector based on maximum discrete degree is one better method, with which the vector is achieved as

$$\begin{aligned}
&\mu_1 \left((m-1)\lambda + 1 - m\mu_1\right)^m \\
&\quad = \left((m-1)\lambda\right)^{m-1} \left(\left((m-1)\lambda - m\right)\mu_1 + 1\right), \\
&\mu_m = \frac{\left((m-1)\lambda - m\right)\mu_1 + 1}{(m-1)\lambda + 1 - m\mu_1}, \\
&\mu_z = \sqrt[m-1]{{\mu_1}^{m-z}{\mu_m}^{z-1}}, \quad 2 \le z \le m,
\end{aligned} \tag{14}$$

$\lambda \in [0, 1]$. In practice, choose a proper value for λ and then calculate $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$ according to formula (14).

For example, set $m = 6$; the vector $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$ changes as λ varies, as detailed in Figure 2.

From Figure 2, the distributions of the corresponding weights are symmetric with λ and $1 - \lambda$, and they strictly monotonically increase and descend when $\lambda < 0.5$ and $\lambda > 0.5$, respectively. However, the rates of ascent or descent are different when λ takes different values.

Through the above analysis, the weights can be allocated twice using an ordered weighted vector. Set $m = d - u + 1$. To begin with, in consideration with time decay, the order of time corresponding to the sequence of trust values $\{T^g_{t,k+u-1}(i,j)\}$ is regarded as the induced factor s_z; then the order value of $T^g_{t,k+u-1}(i,j)$ is k, $1 \le k \le d - u + 1$. Secondly, $\{T^g_{t,k+u-1}(i,j),\ 1 \le k \le d-u+1\}$ are rearranged in descending order of size, and the induced factor s_z is the relative sequence of trust values $T^g_{t,k+u-1}(i,j)$. If a few trust values are the same, they are carried out in accordance with the time order. It's detailed as follows. For any $1 \le k \le d - u + 1$, denote

$$\begin{aligned}
\Sigma_{>k} &= \left\{h : T^g_{t,h+u-1}(i,j) > T^g_{t,k+u-1}(i,j)\right\}, \\
\Sigma_{=k} &= \left\{h : T^g_{t,h+u-1}(i,j) = T^g_{t,k+u-1}(i,j),\ h > k\right\};
\end{aligned} \tag{15}$$

then the relative sequence value of $T^g_{t,k+u-1}(i,j)$ is $y_k = |\Sigma_{>k}| + |\Sigma_{=k}| + 1$. Therefore, each trust value $T^g_{t,k+u-1}(i,j)$ corresponds to a sequence array (k, y_k). From Figure 2, given $m = d-u+1$ and $\lambda < 0.5$, $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$ can be computed from formula (14); then the corresponding weight of trust value $T^g_{t,k+u-1}(i,j)$ is represented by

$$\omega_k = \frac{\mu_k \mu_{y_k}}{\sum_{k=1}^{d-u+1} \mu_k \mu_{y_k}}, \quad 1 \le k \le d - u + 1. \tag{16}$$

Substituting (16) into formula (12), the overall trust degree of node j is

$$\begin{aligned}
T^g_t(i,j) &= \sum_{k=1}^{d-u+1} \omega_k T^g_{t,k+u-1}(i,j) \\
&= \sum_{k=1}^{d-u+1} \frac{\mu_k \mu_{y_k}}{\sum_{k=1}^{d-u+1} \mu_k \mu_{y_k}} T^g_{t,k+u-1}(i,j).
\end{aligned} \tag{17}$$

4. Routing Credibility Based on Tsallis Entropy

After a master node MN collects the data from some sensor nodes in the cluster, MN needs to transmit these data to the base station safely and credibly. Consequently how to

select the most reliable path is a very critical problem. On the foundation of trust degrees between several intermediate master nodes, a method based on path Tsallis entropy is presented to measure the credibility of each path in this section.

4.1. Analysis of the Existing Research Methods. Assume that there are multiple paths from a source master node to the base station, in which the trust degrees of intermediate nodes can be obtained from Section 3. Then to select the most trustworthy path is usually by the following ways.

Method 1. Suppose that $l = \mathrm{MN} \rightarrow \mathrm{Mn}_1 \rightarrow \cdots \rightarrow \mathrm{Mn}_K \rightarrow \mathrm{BS}$ is a path; the minimum of trust degrees of all the intermediate nodes in path l is viewed as the path trust degree:

$$T(\mathrm{MN}, l) = \min\left\{T_t^g\left(\mathrm{Mn}_{r-1}, \mathrm{Mn}_r\right),\ 1 \le r \le K\right\}, \quad (18)$$

where $\mathrm{Mn}_0 = \mathrm{MN}$. The method is mainly based on "Cannikin law"; that is to say, as long as one of the intermediate nodes fails in forwarding the data, then the whole path is not credible. However, this method has a certain disadvantage. For example, there are two disjoint paths from the source master node to the base station, denoted by $l_k = \mathrm{MN} \rightarrow \mathrm{Mn}_{k,1} \rightarrow \mathrm{Mn}_{k,2} \rightarrow \mathrm{Mn}_{k,3} \rightarrow \mathrm{BS}$, in which the trust degrees of all the intermediate nodes are $\{0.8, 0.7, 0.8\}$ and $\{0.65, 0.95, 0.95\}$, respectively. From formula (18), the trust degree of each path is $T(\mathrm{MN}, l_1) = 0.7$ and $T(\mathrm{MN}, l_2) = 0.65$ separately, so the path l_1 is regarded as the most trustworthy path and will be selected to transmit the data. Nevertheless, considering trust degrees of the other two nodes, path l_2 is more credible than l_1 apparently.

Method 2. The most trustworthy path is chosen via the hop-by-hop way. The source master node first delivers the data to the most trustworthy neighbor node. After it receives, the neighbor node similarly chooses its own neighbor with the highest trust degree to transmit, and so on for all the intermediate nodes until the data reach the base station. However, the optimality of each hop does not necessarily make the whole path optimal. It can be verified still with the example in Method 1. Due to the fact that $T(\mathrm{MN}, \mathrm{Mn}_{1,1}) = 0.8 > T(\mathrm{MN}, \mathrm{Mn}_{2,1}) = 0.65$, the source MN delivers the data to node $\mathrm{MN}_{1,1}$, and then the data only pass the intermediate nodes $\mathrm{MN}_{1,2}$ and $\mathrm{MN}_{1,3}$ successively to the base station. Obviously, $T(\mathrm{MN}_{1,1}, \mathrm{Mn}_{1,2}) > T(\mathrm{MN}_{2,1}, \mathrm{Mn}_{2,2})$ and $T(\mathrm{MN}_{1,2}, \mathrm{Mn}_{1,3}) > T(\mathrm{MN}_{2,2}, \mathrm{Mn}_{2,3})$; thus the probability that the data successfully go through $\mathrm{MN}_{1,2}$ and $\mathrm{MN}_{1,3}$ is far less than $\mathrm{MN}_{2,2}$ and $\mathrm{MN}_{2,3}$.

From the above discussion, the trust degree of each path should be measured by comprehensive analysis of all the intermediate nodes, which ensures that the selected path is optimal at the most extent.

4.2. A Routing Trust Model Based on Path Tsallis Entropy. Through some associated properties of Tsallis entropy, path Tsallis entropy is put forward to measure the uncertainty of the whole path, which can synthesize the credibility of all the intermediate nodes. On that basis, trust degree of each path is calculated.

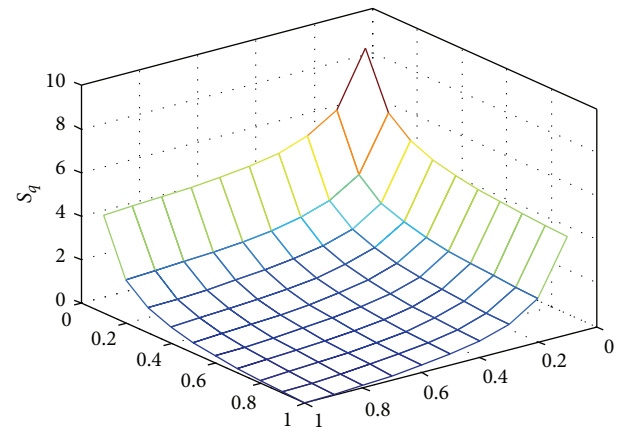

FIGURE 3: $S_q^g(l,t)$ with the different trust degrees of two nodes.

Definition 3 (Tsallis entropy [13]). Assume that $\{p_k,\ 1 \le k \le K\}$ is a discrete probability distribution; the Tsallis entropy is defined as

$$S_q = \frac{1 - \sum_{k=1}^{K} {p_k}^q}{q-1}, \quad q < 0. \quad (19)$$

By simply computing, it is known that $\lim_{q\to 1} S_q = -\sum_{k=1}^{K} p_k \ln p_k$, the right side of which is the classical Shannon entropy. From [13], S_q has the following property.

Property 1. The function S_q is convex when $q < 0$ and it is concave when $q > 0$.

Based on this, the path Tsallis entropy is proposed which is mainly to measure the uncertainty of each path.

Definition 4 (path Tsallis entropy). The path Tsallis entropy of $l = \mathrm{MN} \rightarrow \mathrm{Mn}_1 \rightarrow \cdots \rightarrow \mathrm{Mn}_K \rightarrow \mathrm{BS}$ is denoted by

$$S_q^g(l,t) = \frac{K - \sum_{k=1}^{K} T_t^g\left(\mathrm{Mn}_{k-1}, \mathrm{Mn}_k\right)^q}{q-1}, \quad q < 0. \quad (20)$$

Given $q = -1$ and $K = 2$, the path Tsallis entropy $S_q^g(l,t)$ varies when trust degrees of the two intermediate nodes take different values in the range $(0, 1)$ shown in Figure 3.

From formula (20) and Figure 3, $S_q^g(l,t)$ is a comprehensive value integrating trust degrees of all the intermediate master nodes with the length K of each path. The calculation shows that $S_q^g(l,t) > 0$ and $S_q^g(l,t)$ becomes smaller when trust degrees of all the intermediate nodes are higher, more uniformly distributed and the length of a path is shorter, which represents that a path has lower uncertainty.

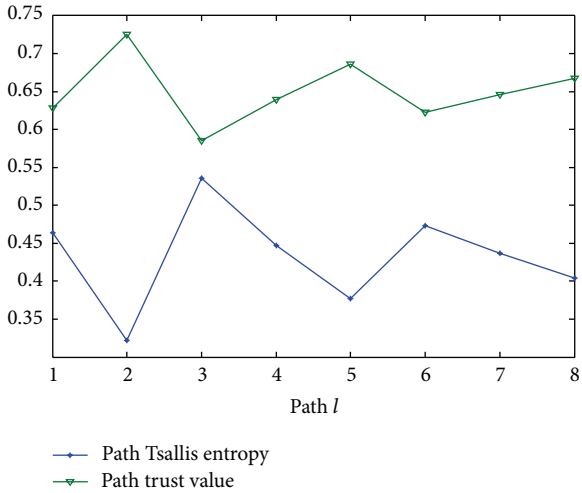

FIGURE 4: $S_q^g(l,t)$ and $T_{t,q}^g(\mathrm{MN},l)$ of different paths.

Definition 5 (path trust degree). The trust degree of path l is measured by

$$T_{t,q}^{g}(\mathrm{MN},l) = e^{-S_q^g(l,t)} = e^{-(K-\sum_{k=1}^{K} T_t^g(\mathrm{Mn}_{k-1},\mathrm{Mn}_k)^q)/(q-1)}, \quad q<0. \tag{21}$$

Due to the fact that $S_q^g(l,t) > 0$, $T_{t,q}^g(\mathrm{MN},l) = e^{-S_q^g(l,t)} \in (0,1)$. The smaller the $S_q^g(l,t)$, the larger the $T_{t,q}^g(\mathrm{MN},l)$, which shows that a path is more credible.

For example, suppose there are multiple paths: $l_h = \{0.65, 0.95, 0.95, 0.7 + 0.1 \times (h-3)\}$, $(3 \le h \le 5)$, $l_h = \{0.65, 0.95, 0.95, 0.95, 0.8 + 0.05 \times (h-6)\}$ $(6 \le h \le 8)$, and l_h $(h = 1, 2)$ is the same as in Method 1. Given $q = -1$, the path Tsallis entropy and trust degree of each path are detailed in Figure 4.

To sum up, assume that there are L paths from a source master node MN to the base station, denoted by $\Omega_{\mathrm{path}} = \{l_h, 1 \le h \le L\}$; then the most trustworthy path is

$$l_{\mathrm{opt}} = \arg\max_{l} \left\{ T_{t,q}^{g}(\mathrm{MN},l),\ l \in \Omega_{\mathrm{path}} \right\}. \tag{22}$$

Therefore, the source master node utilizes the most trustworthy path l_{opt} to transmit the medical data to the base station.

5. Simulation Experiment and Result Analysis

In this section, several experiments are carried out in order to verify the performance of the proposed trust models. Experiment 1 is conducted to test the accuracy and dynamic of the trust model of single node under the circumstance that the behavior of single node changes dynamically. The robustness of resisting the strategic malicious attack is analyzed in Experiment 2. Subsequently the performance of path trust model based on Tsallis entropy is compared with the other two routing ways mentioned in Section 4.1. The packets are assumed to be equally important in the former three experiments. In the end, the proposed trust models are evaluated with differently important packets. To begin with, the preset values of associated parameters involved are listed in Table 1.

TABLE 1: Parameters in the proposed trust models.

Parameters	Value
d^*	5
λ	0.3
q	−1

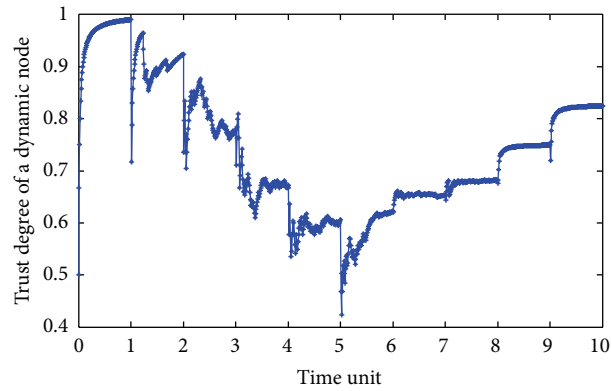

FIGURE 5: The trust degree of a dynamical node.

5.1. Dynamic of Trust Model about Single Node. This experiment is carried out to verify the performance of trust model based on single master node i. It is assumed that there is only a kind of packets with the same importance, and the accuracy and dynamic are investigated in the following settings. The experiment proceeds within 10 time units, and there are 500 packets going through node i in each time unit. The probabilities that node i forwards packets to the next node successfully are set as $\{1, 0.9, 0.8, 0.7, 0.6, 0.7, 0.8, 0.9, 1, 1\}$ in the 10 time units, respectively. Then the trust degree of node i varies with the change of the probabilities as in Figure 5.

When the probability varies dynamically from 1 to 0.6, the trust degrees descend obviously from the left part of Figure 5. The trust degree fluctuates near the corresponding probability in the first 5 time units. This result means that the proposed trust model of single node is adaptable dynamically and is able to quickly reflect the variation of node behavior in the downward trend. However, the trust degree increases very slowly when the node behaves from bad to good in the right part. This phenomenon justifies that it is necessary to take much more time for the purpose of accumulating the trust degree.

5.2. Robustness of Resisting Strategic Attacks. The strategic malicious attack is a type of threat that malicious nodes which are aware of the presence of trust models launch. A malicious node behaves very well in the first several time units to increase its trust degree, and then it launches some attacks in the subsequent time units, such as discarding the packets with a certain probability. In this experiment, assume

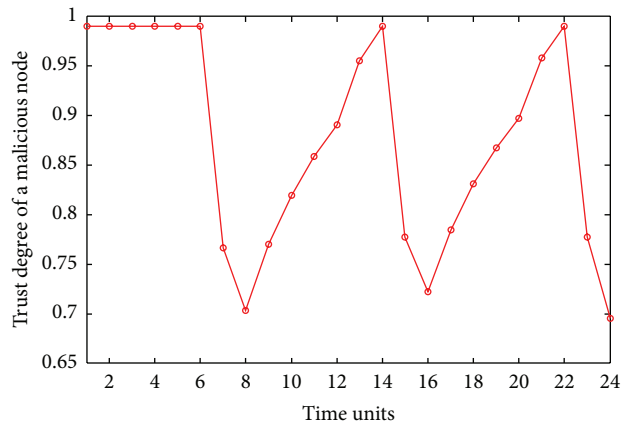

FIGURE 6: The trust degree of a malicious node.

that a malicious node is honest in every 6 time units and becomes bad in the following 2 time units; that is, it will discard packets with probability 0.3. The trust degree varies with the periodical change of node behavior in Figure 6.

In the first 6 time units, the node forwards the packets honestly; hence its trust degree is nearly equal to 1. But starting from the 7th unit, it behaves maliciously and cannot deliver packets with probability 0.3. It can be found that the trust degree has sunk to 0.76 at the end of the 7th time unit. In the case that this malicious node continues its bad behavior, trust degree further falls to 0.7 in the 8th unit. Therefore, this tendency indicates that the proposed trust model is very sensitive to respond to abnormal behaviors. However, when this node behaves from bad to well, the rising speeding of trust degree is relatively low from the 9th to 14th unit and trust degree achieves 1 until the 14th unit. A similar situation occurs among the subsequent 8 time units. From the foregoing, the proposed trust model is able to identify the malicious behavior quickly so as to avoid it and prevent the packet delivery failure.

5.3. Accuracy of Path Trust Model. In order to measure the accuracy of path trust model, 20 master nodes and a base station are deployed in the MSN. These master nodes send packets to the base station according to a certain rate, and the base station computes the average successful delivery rate

$$\mathrm{SDR} = \frac{N_{\mathrm{accepted}}}{N_{\mathrm{emit}}}, \tag{23}$$

in which N_{accepted} denotes the total number of packets accepted by the base station and N_{emit} represents the total number of packets emitted by the 20 source master nodes. There are 10% and 30% malicious nodes in the experiment, which cannot deliver the packets successfully with probability 0.2. The comparison of SDR between the proposed trust model (denoted by PTE model) and the other routing ways under these situations is shown in Figure 7.

In the left half of Figure 7, the SDRs are given when there are 10 percent malicious nodes. The SDR of PTE model is almost 0.9 and is much higher than the other two routing ways. Even when 30% malicious nodes exist in the MSN, the SDR of the PTE model still is able to achieve 70% as shown in the right of Figure 7, while the SDRs with the other ways have reduced to around 45%. Therefore, the PTE model is able to ensure that the packets are transmitted to the base station successfully with higher probability.

5.4. Efficiency of Trust Models with Differently Important Packets. In this experiment, the situation that there are 3 kinds of packets with importance 1, 2, and 3, respectively, is analyzed. Assume that there are two types of nodes which successfully forward packets of importance g with probability b_g^k:

$$b_g^1 = \begin{cases} 0.95, & g = 1 \\ 0.8, & g = 2 \\ 0.6, & g = 3, \end{cases} \qquad b_g^2 = \begin{cases} 0.85, & g = 1 \\ 0.75, & g = 2 \\ 0.66, & g = 3. \end{cases} \tag{24}$$

The trust degrees of the two types of nodes are presented in Figure 8.

In Figure 8, the corresponding curve of "type k with none" represents trust degree of single node of type k when there is no difference between packets, and hence it is an integrated value. The "type k with imp g" curve shows the trustworthiness that a node of type k successfully forwards the packets of importance g, respectively. Obviously, the integrated trust degree of a node of type 1 is much higher than type 2. Therefore, the node of type 1 would be selected to deliver the packets if the importance of packets is not distinguished. There is no problem to transmit the packets with importance 1 and 2. Nevertheless, due to $b_3^2 > b_3^1$, the packets with importance 3 are likely to be discarded when going through a node of type 1 compared with type 2.

Additionally, suppose that there are two paths from a source master node to the base station. A node of type 1 is in a path and a node of type 2 is in the other path. Assume that the other intermediate nodes can deliver the packets successfully. The source master node randomly sends 300 packets with different importance to the base station. One way is that the source node selects the path with the node of type 1 to transmit the data, and the other is choosing the corresponding path according to the importance of packets. The successful packet delivery rates of the two ways are analyzed in Figure 9.

From Figure 9, the rate is higher when the importance of packets is considered. The path with a node of type 1 is selected when forwarding the packets with importance 1 and 2, and the other path is used for delivering the packets with importance 3. The most reliable path is found for differently important packets transmitted to the base station. Therefore, the successful packet delivery rate gets some improvement.

6. Conclusions

In this paper, a security and trust model is proposed as applicable to medical sensor networks. First of all, considering the importance of packets, the trust value of single node in each interval is derived based on Bayesian inference

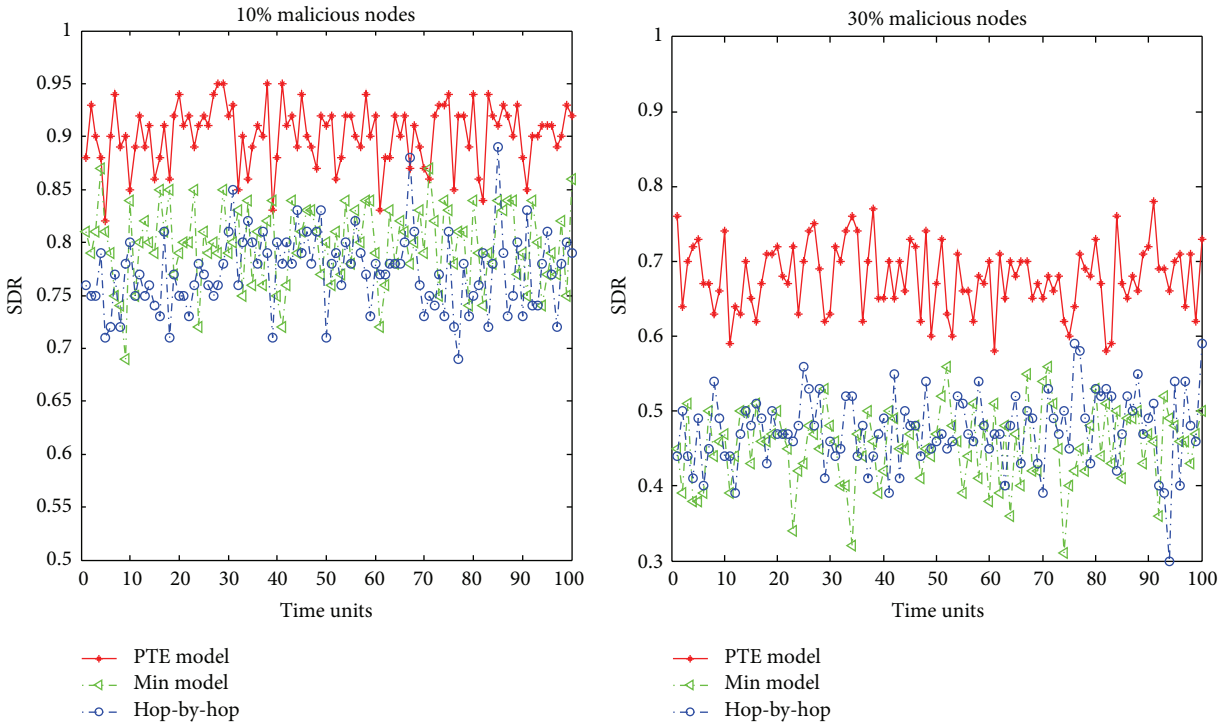

Figure 7: The SDR with different trusted routing ways.

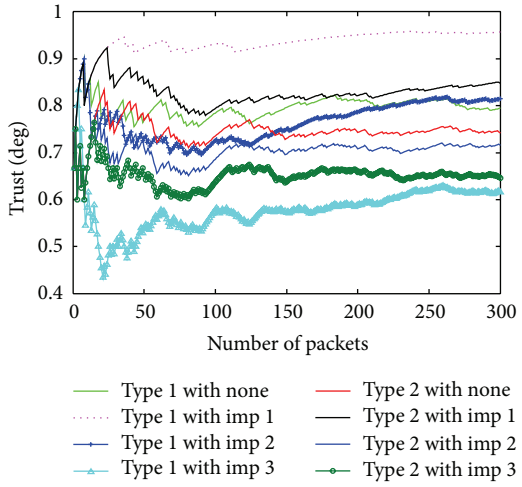

Figure 8: Trust degrees associated with importance.

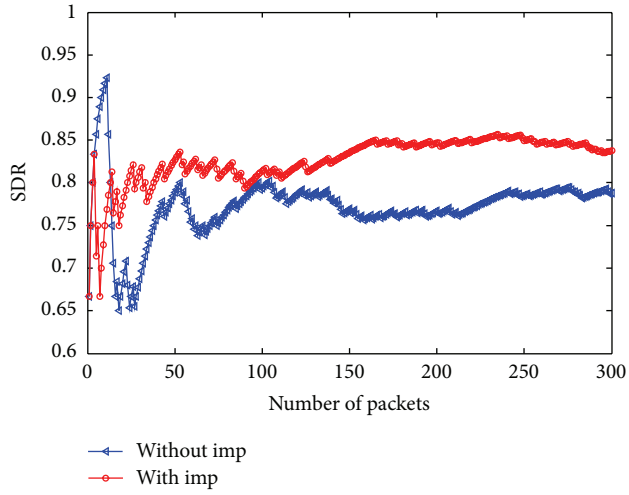

Figure 9: The SDRs with some kinds of packets.

in which the interactions of neighbor nodes are viewed as prior information and then the posterior distribution is obtained, combined with direct interactions. The corresponding weights are further distributed through the ordered weighted vector twice to obtain the overall trust degree. On that basis, with the relevant properties of Tsallis entropy, path Tsallis entropy is defined to measure the uncertainty of each path and the trust degree of each path is shown. Subsequently, each source master node selects the most trustworthy path to forward it to the base station according to the importance of packets. The simulation results show that the proposed trust model is able to accurately reflect the dynamic of node behavior, identify quickly malicious behaviors, and achieve higher successful packets delivery rate so as to effectively improve the dynamic adaptability and robustness.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The research work was supported by National Basic Research Program of China (973 Program) under Grant no. 2012CB315905.

References

[1] N. Patil and A. Mulla, "Medical application based on wireless sensor network," *International Journal of Computer Science and Communication Engineering*, vol. 2, no. 2, pp. 43–46, 2013.

[2] R. D. Caytiles and S. Park, "A study of the design of wireless medical sensor network based u-healthcare system," *International Journal of Bio-Science and Bio-Technology*, vol. 6, no. 3, pp. 91–96, 2014.

[3] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561–5595, 2011.

[4] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[5] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[6] K. S. Barber and J. Kim, "Soft security: isolating unreliable agents from society," in *Trust, Reputation, and Security: Theories and Practice*, pp. 224–233, Springer, Berlin, Germany, 2003.

[7] A. Boukerche and Y. L. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 387–399, 2009.

[8] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1164–1175, 2012.

[9] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[10] J. Y. Lee, W. C. Lin, and Y. H. Huang, "A lightweight authentication protocol for internet of things," in *Proceedings of the International Symposium on Next-Generation Electronics*, pp. 1–2, Kwei-Shan Tao-Yuan, Taiwan, May 2014.

[11] J. O. Berger, *Statistical Decision Theory and Bayesian Analysis*, Springer, 2nd edition, 2010.

[12] R. R. Yager and D. P. Filev, "Induced ordered weighted averaging operators," *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, vol. 29, no. 2, pp. 141–150, 1999.

[13] C. Tsallis, "Possible generalization of Boltzmann-Gibbs statistics," *Journal of Statistical Physics*, vol. 52, no. 1-2, pp. 479–487, 1988.