Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 2815039, 1 page
http://dx.doi.org/10.1155/2016/2815039

Retraction

Retracted: Data Fusion Based on Node Trust Evaluation in Wireless Sensor Networks

Journal of Sensors

Received 15 November 2016; Accepted 15 November 2016

At the request of the authors, the article titled "Data Fusion Based on Node Trust Evaluation in Wireless Sensor Networks" [1] has been retracted. The article was found to contain errors, as the Matlab code underlying the results in part 3 and Figures 2–6 of the article was found to produce incorrect results, meaning that the conclusions cannot be relied on.

References

[1] Z. Jianming, L. Fan, and L. Qiuyuan, "Data fusion based on node trust evaluation in wireless sensor networks," *Journal of Sensors*, vol. 2014, Article ID 391401, 7 pages, 2014.

Hindawi Publishing Corporation
Journal of Sensors
Volume 2014, Article ID 391401, 7 pages
http://dx.doi.org/10.1155/2014/391401

Research Article

Data Fusion Based on Node Trust Evaluation in Wireless Sensor Networks

Zhou Jianming, Liu Fan, and Lu Qiuyuan

School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

Correspondence should be addressed to Zhou Jianming; zhoujm@bit.edu.cn

Received 5 May 2014; Revised 26 June 2014; Accepted 30 June 2014; Published 17 July 2014

Academic Editor: Junjie Chen

Abnormal behavior detection and trust evaluation mode of traditional sensor node have a single function without considering all the factors, and the trust value algorithm is relatively complicated. To avoid these above disadvantages, a trust evaluation model based on the autonomous behavior of sensor node is proposed in this paper. Each sensor node has the monitoring privilege and obligation. Neighboring sensor nodes can monitor each other. Their direct and indirect trust values can be achieved by using a relatively simple calculation method, the synthesis trust value of which could be got according to the composition rule of D-S evidence theory. Firstly, the cluster head assigns different weighted value for the data from each sensor node, then the weight vector is set according to the synthesis trust value, the data fusion processing is executed, and finally the cluster head sensor node transmits the fused result to the base station. Simulation experiment results demonstrate that the trust evaluation model can rapidly, exactly, and effectively recognize malicious sensor node and avoid malicious sensor node becoming cluster head sensor node. The proposed algorithm can greatly increase the safety and accuracy of data fusion, improve communication efficiency, save energy of sensor node, suit different application fields, and deploy environments.

1. Introduction

As an important element of Internet of Things, wireless sensor networks (WSN) are composed of many compact microsensors. They have a lot of advantages, for instance, wireless communication, data processing, and real-time monitoring as well as the several characteristics such as self-organization [1], universality, simple and easy operation, and strong adaptability. They have been widely applied in many application fields such as military surveillance tracking, environmental monitoring report, and medical real-time observation [2]. Achieving safe, effective, and quick data fusion is the key to ensure that WSNs obtain accurate information. However, it is easy to produce malicious sensor node. Due to random, jumping, and uncontrollable sensor nodes in real-time dynamic environment, the maliciously attachment causes a serious threat to the security of WSNs. So, how to realize the data fusion in WSNs becomes an urgent problem. In WSNs, the data cannot reach to the fusion center sensor node at the same time, which means the fusion sensor nodes have to wait the arrival of data. Different WSNs applications have different information extracting requirements, which include the maximum tolerable time T of data transmission. If data required from the sensing region exceed the maximum delay time T, the information is invalid for user. So, how to allocate reasonably delay into each fusion sensor node and how to achieve the best effect information fusion become a noticeable problem.

In WSNs, the malicious sensor node includes not only the external malicious node deployed by attacker in network region, but also the trapped or controlled sensor node. Since outside malicious sensor nodes do not possess network key, these sensor nodes cannot adopt the identity authentication and obtain the initial trust. So, the traditional password authentication system can dispose effectively. Conversely, the trapped or controlled sensor nodes (the internal malicious sensor nodes) have the network key and the certain trust foundation, which make the traditional password authentication system invalid, so it is easy for the node to launch attacks. Generally speaking, any sensor node can be the malicious sensor node in WSNs, so it is necessary for each sensor node to make safety certification and to ensure the data safety

in WSNs. Therefore, it is an effective way for identifying and eliminating the malicious sensor node especially setting several identification nodes, but it has some disadvantages, such as high cost, low efficiency, and long period. Since WSNs cannot effectively detect security problems caused by the internal malicious nodes, Verellen et al. proposed a WSNs security routing algorithm [3] based on reliability, which is a hierarchical routing trust model and can detect malicious attacks from sensor nodes within the network, and exclude it from the network. Cevher et al. proposed an algorithm based on a trust value of neighbor nodes [4]. According to the trust value of each node, the model is a self-organized clustering algorithm. Each cluster node directionally transmits data into a trusted cluster head node to realize data fusion and improve the security. A reputation model MA&TP-BRSN for evaluating behaviors of sensor nodes in WSN is proposed by Zhong et al. [5]. Aiming at various attack types, the methods calculate and integrate the given credibility. The above methods mainly cause some problems.

(1) The function of anomaly behavior detection and reputation evaluation module is single.

(2) When calculating the trust value of node, not all factors are properly considered and the trust value algorithm is fairly complicated.

(3) The diversity, complexity, and variety of node's attack behavior are not properly considered, so it is difficult to identify and eliminate the malicious node [6–10].

To avoid the above problems, this paper proposes a trust evaluation model based on the autonomous behavior of node without reference. Each node has the monitoring privilege and obligation. Any neighboring sensor nodes can monitor each other in region. Their direct and indirect trust values can be achieved by using relatively simple calculation method. Then, their synthesis trust value can be got according to the composition rule of D-S evidence theory. So, this method can rapidly, exactly, and effectively recognize malicious node and avoid malicious node becoming cluster head node. All the neighboring sensor nodes are clustered by self-organization, and the cluster head sensor node can be selected as the node for data fusion automatically. The sensor node in each cluster transmits the acquired data into its cluster head directionally; then, the cluster head assigns the different weighted value for the data and execute the data fusion processing progress. Finally, the cluster head transmits the fused result to the base station. Compared with the traditional identity authentication mechanism, the proposed algorithm can increase the safety and accuracy of data fusion, improve communication efficiency, and save sensor node energy. In view of the different proportion of attack behaviors in different application fields and deployment environments, the weight vector would be set when the synthesis trust value is calculated, so the validity of the trust evaluation model and algorithm are improved in various actual situations.

2. The Node Trust Evaluation Model

Multisensor data fusion is a new data processing method by adopting several or multiclass sensors in one system, which is a multidisciplinary new technology, and mainly refers to the theories, including signal processing, probability statistic, information theory, pattern recognition, artificial intelligence, and fuzzy mathematics. Thus, multisensor data fusion technology is a relatively complicated system project and it is difficult to give a unified, comprehensive, and accurate definition about that. With the development of data fusion technology, sensor technology, and computer application technology, most experts think that multisensor data fusion can be defined relatively exactly; that is, to make full use of multisensor information resource in different time-space, the computer technology is adopted to perform automatic analysis, synthesis, dominance, and application to the obtained multi-sensor observation information according to time sequence under a certain criteria and it can get the consistent explanation and the measured description for finishing the needed decision-making and estimation task. Hence, the multisensor system and computer system are the hardware foundation of data fusion, multisource data are the processing object of data fusion, and the coordinating optimization and comprehensive treatment are the kernel of data fusion.

2.1. The Direct Trust Value Calculation. Thus, the direct trust between the node i and its adjacent node j can be defined as follows.

Definition 1. The quaternion (E_i, E_j, d, t) is adopted to denote trust relationship, where E_i and E_j are entities (node i and j) which need to build trust relationship, d is interaction data, and t is interaction time.

Definition 2. The direct trust of the node is vector D, $D = \{S_{i,j}(t), T_{i,j}(t), U_{i,j}(t)\}$, where, $S_{i,j}(t)$ denotes the data repetition factor, $T_{i,j}(t)$ denotes the data output factor, and $U_{i,j}(t)$ denotes the data similarity (correlation). The calculation equation is described as follows:

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

$$T_{i,j}(t) = \frac{\left|p_{i,j}(t) - \Delta p(t)\right|}{p_{i,j}(t)}, \tag{1}$$

$$U_{i,j}(t) = \exp\left[-b\left[z_i(t) - z_j(t)\right]^2\right],$$

where $p_{i,j}(t)$ denotes the output data quantity in t time, $sp_{i,j}(t)$ denotes the data repetition quantity, $\Delta p(t)$ is the dynamic reference value of data quantity, $z_i(t)$ and $z_j(t)$ are separately the output of its own monitoring value, and b is the comparison coefficient.

The above 3 factors take different proportions of data fusion in various application fields and different actual demand. Comprehensive consideration was needed to avoid

the single function of trust model. This paper adopts the weighted averages method to realize the trade-off. The weighted value is $W = \{w_s, w_t, w_u\}^T$, so the sensor node's direct trust after trade-off is $D' = DW$. In the initial time of WSNs, there is no data interaction in each node, so the initial value is $D' = \{0, 0, 1\}$ and the node will finish the real-time update of D' according to the WSN's update cycle Δt.

With the variation of space and time, sensor node trust degree would make no exception, which shows that it will decrease with the increasing of sensor nodes' space and weaken with the increase of interaction time. Because WSNs possess strong convergence, the adjacent nodes will always keep in an effective interaction distance. Thus, the influence of node space's dynamic change can be ignored, but nothing can stop the time. Therefore, interaction time is an important factor and its influence on the weakening of trust degree should be considered.

Definition 3. The obtained trust value in the recent moment is taken as the maximum value l. And the trust value with longer interval time influences less on the present value. The time-weakening function is

$$f(k) = \begin{cases} f(k-1) - \dfrac{1}{n}, & 1 \le k < n, \\ 1, & k = n. \end{cases} \tag{2}$$

To sum up, the calculation equation of adjacent node's direct trust value is

$$D''_{i,j}(t_{n+1}) = \frac{D'_{i,j}(t_{n+1}) + f(n) D'_{i,j}(t_n)}{2}. \tag{3}$$

The phase difference between t_{n+1} and t_n is an update cycle Δt; namely, the node's direct trust value is the average value between the attenuated trust value in last cycle and the present trust value. The time-weakening function $f(k)$ not only ensures the continuity of trust value calculation but also adjusts the proportion of the last cycle's trust value, which can insure the time-efficiency of trust value to the greatest extent.

2.2. The Indirect Trust Value Calculation. Obviously, if node i only performs trust evaluation on node j's behavior (direct trust value) which is monitored by it, the evaluation result will have a certain one-sidedness and be not comprehensive. Besides, the direct trust relationship will not be always built among sensor nodes. Therefore, it must adopt the trust value obtained through the recommendation of node j's other adjacent nodes and get the indirect trust value after comprehensive calculation.

Definition 4. In order to finish the comprehensive and accurate evaluation on node j's behavior, sensor node i requests node j's other adjacent sensor nodes to send their direct trust values to node j and then gets the indirect trust value of node i to node j, according to the composition rule of D-S evidence theory, which is taken as vector I.

Let I denote the indirect trust value between node i and node j. Here, node k is one of the adjacent nodes of node j. So, combining (3), the indirect trust value I at t time can be calculated by the following equation:

$$I_{i,j}(t) = \frac{\sum D''_{i,k}(t) D''_{k,i}(t)}{\sum D''_{i,k}(t)}. \tag{4}$$

2.3. The Comprehensive Trust Value Calculation. In the trust evaluation of node, it neither relies solely on the direct trust degree nor unilaterally considers the indirect trust degree, so it should make a trade-off between these two sides and get the comprehensive trust degree.

Definition 5. Assume that an entity carries out the trust evaluation belonging to the other entity. Let λ represent the weighted value of direct trust degree. Then, the weighted value of indirect trust degree is $1-\lambda$. Thus, the comprehensive trust degree Ω can be equal to $\lambda D + (1-\lambda) I$.

Based on the above definition, we can further quantify the entity and get the comprehensive trust value of the entity E_i to entity E_j:

$$\Omega_{i,j} = \lambda D''_{i,j} + \frac{1}{n} \sum_{i \in Q} I_{i,j}, \tag{5}$$

where Q is the collection of node j's adjacent nodes and n is the quantity of entity nodes in this collection.

It starts to collect data after the node deployment in clustered WSNs. It realizes the data fusion through three steps approximately in the traditional identity authentication and cipher communication mechanism.

The first step is the identity authentication and communication between the adjacent cluster nodes.

(1) Flood the Hello packets of sensor nodes in IOT.

(2) Perform the identity authentication.

(3) If it is successful, the communication link and the share key will be built. Otherwise, they will not be built.

(4) Send and transfer the encrypted data of sensor nodes.

(5) The receiver sensor node receives the decrypted data and feeds back the acknowledgement information;

The second step is the identity authentication and communication between the sensor node in cluster and the cluster head node of the same cluster.

(1) The node in cluster sends its own ID and the requesting random code to the cluster head node.

(2) The cluster head node searches for the ID of node in the trusted ID list. If it exists, it will generate the random feedback code and send it to this node by the encrypted share key. Otherwise, it will carry out the identity authentication on the sensor node, build share key, and send the feedback random code by encryption.

(3) The cluster node encrypts and transmits the data.

(4) The cluster node receives and decrypts data and feeds back the OK information.

The third step is the identity authentication and communication between the cluster head node and base station.

(1) The cluster head node sends its own ID encrypted by the share key and requesting random code to the base station.

(2) The base station searches for the ID of cluster head node in the trusted ID list. If it exists, it will send the random feedback code in encryption method.

(3) The cluster head node encrypts and transmits the data after receiving the feedback random code.

(4) The base station receives and decrypts data and sends the acknowledgement information and receives the random code.

On the basis of the sensor node trust evaluation model, all sensor nodes in neighborhood are clustered by self-organizing during each data fusion cycle (in each round), and the cluster head sensor node can be selected automatically as the sensor node for data fusion. The node in each cluster directionally transmits the acquired data into its cluster head; then, the cluster head assigns the different weighted value for the data from each node and executes the data fusion processing; finally, the cluster head transmits the fused result into base station. The specific algorithm is as follows.

(1) The cluster head node E_i sends and submits the data request to the adjacent node E_j within cluster.

(2) Sensor node E_j analyzes the ID of requesting data package and judges whether E_i is the cluster head node of the cluster. If it is the head, the collected data DATE_j will be sent to sensor node E_i; if the judgment is negative, the requesting package will be discarded.

(3) The cluster head node E_i requests node E_j's other adjacent nodes E_k to give their own direct trust values to E_i, where $E_k \in \mathrm{Cluster}_i$ ($\mathrm{Cluster}_i$ denotes the node collection of the cluster where the cluster head node i is).

(4) The cluster head node E_i gets its comprehensive trust value to node E_j according to (3), (4), and (5) and gives a weighted value DATE_j according to the comprehensive trust value.

(5) It adopts the same way to the collected data of other cluster sensor nodes and the data from each sensor node will be sent to the base station after fusion according to the weighted value.

3. The Stimulation Experiment and Result Analysis

The paper constructs the mathematical model and the algorithm stimulation with MATLAB platform. The sensor node's quantity is set to 100 and they are randomly deployed in the square region of 100 m $*$ 100 m; the node's communication radius is 10 m and the Sink node locates in the center of this region. The distribution diagram of WSNs nodes is shown in Figure 1, where the solid spot denotes the normal node and the hollow spot denotes the malicious node. In the experiment environment, we suppose the normal sensor nodes occupy 90% of all the nodes and the malicious nodes occupy 10%, as well as 5% are the malicious cluster head sensor nodes and 5% are malicious cluster member sensor nodes. The malicious cluster nodes trick their adjacent sensor nodes into joining the cluster by widely releasing false data request information and the malicious member nodes interfere with the data transmission and fusion in the cluster by decreasing datum size, modifying data package, and repeatedly sending the same data. The node communication round is 100, the bandwidth is 1 Mb, and the package size is 256 b, and the parameter $b = 5$ is adopted in (1).

Relationship curve between trust degree of malicious nodes and communication rounds number is shown in Figure 2. From Figure 2, we can find that the trust degree average value of the normal node would increase with the increase of communication rounds. When the communication rounds increase to a certain degree, which are about 55, the trust degree average value tends to convergence. Nevertheless, with the increase of communication rounds, the trust degree average value of the malicious node is on the steady decrease. When the communication rounds increase to a certain degree, which are about 55, the trust degree average value of the malicious node also tends to convergence at 20%. Figure 2 demonstrates that the trust value of the malicious node decreases obviously after a few aggressive behaviors, which can be seen through other nodes in the region. The influence of its aggressive behaviors including the decreasing of datum size, modifying data package, and repeatedly sending the same data on the data fusion for WSN gets smaller along with it. From this, we can see that this trust evaluation model can recognize the malicious nodes quickly and further prevent its aggressive behaviors. Figure 3 offers the relationship of trust degree average value and communication rounds in the situation that the proportion of normal node and malicious node does not change. Therefore, we can see that this trust mode possesses the fine evaluation accuracy and integrity.

The trust evaluation model in our work emphatically considers 3 primary aggressive behaviors, namely, decreasing datum size, modifying data package, and repeatedly sending the same data. In different application fields and environments of WSNs, the above 3 aggressive behaviors take different proportions. Then, we set up the weighted value vector $W = \{w_s, w_t, w_u\}^T$ and fix its own weight in the comprehensive trust according to the current situation. In the experiment, the three values $\{0.2, 0.2, 0.6\}$, $\{0.3, 0.4, 0.3\}$, and $\{0.4, 0.4, 0.2\}$ are adopted to separately denote state A, state B, and state C. The ratios of the recognized malicious nodes are compared in different weights. In the stimulation experiment, decreasing data size, modifying data package, and repeatedly sending the same data are stimulated and the distribution density of the malicious node is set artificially in the linear

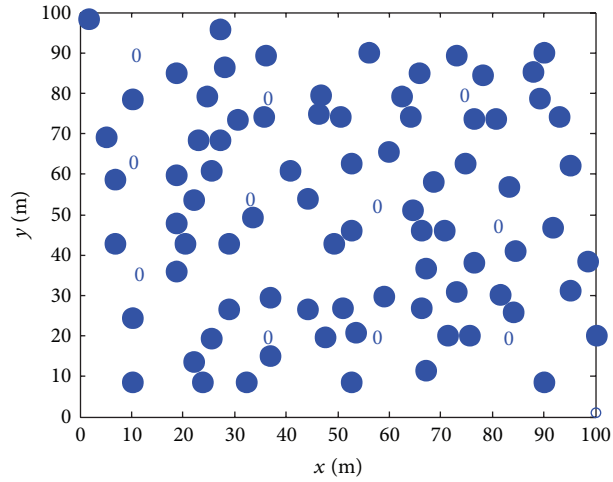

Figure 1: Distribution diagram of WSNs nodes.

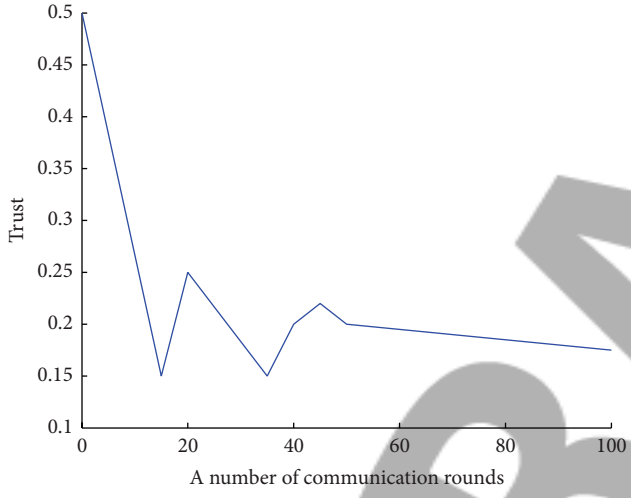

Figure 2: Trust degree of malicious nodes and communication rounds number.

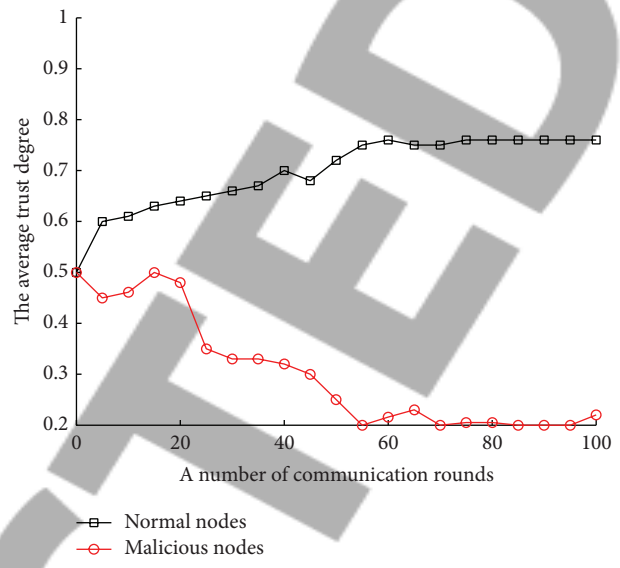

Figure 3: Average value of trust degree and communication rounds.

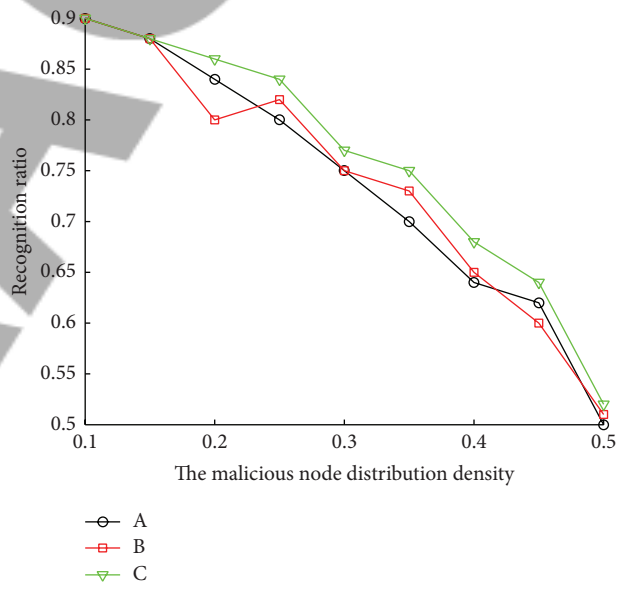

Figure 4: Recognition ratio of A, B, and C situation in different distribution density.

increase, which test that the algorithm can identify the probability of malicious node's aggressive behaviors. Recognition ratio of A, B, and C situation in different distribution density is shown in Figure 4. From the figure, we can see, in different weights (namely, different fields and environments), the trust evaluation model and data fusion algorithm in this paper can both accurately recognize the malicious node. The curve presents a decline trend, which means that, with the increase of the malicious node's distribution density, more and more malicious nodes are eliminated from WSNs.

We obtain the statistics of the 10 experiments by using the traditional algorithms and the proposed strategies respectively. It can be seen that the death time of head node of the proposed algorithm is superior to the traditional algorithm as shown in Figure 5, which reflects superiority of the network lifetime with the proposed scheme.

Based on the statistics frequency, the average path credibility of the traditional scheme and the proposed scheme was compared as shown in Figure 6. We found that the performance of the proposed scheme is better than the traditional scheme because it did not consider the node trust evaluation in WSNs.

In conclusion, the reorganization of malicious sensor node and avoiding malicious sensor node with the proposed trust evaluation model are provided with real time, accuracy and effectiveness. Specially, the proposed algorithm has better safety and accuracy of data fusion, communication efficiency, and energy efficiency than traditional scheme, as well as it suits different application fields and deploy environments.

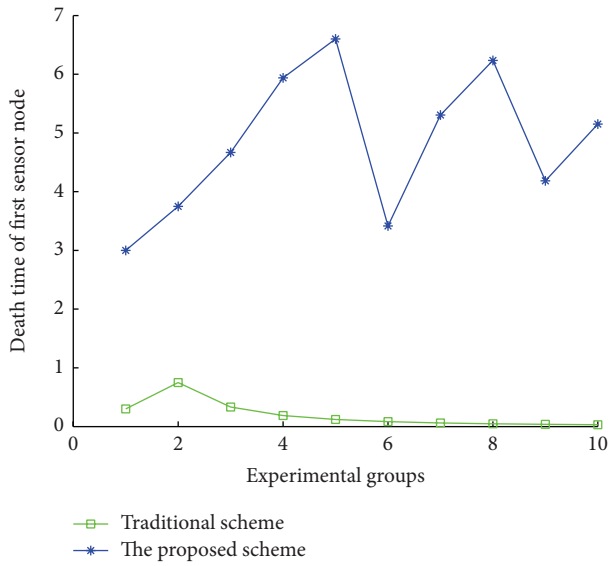

Figure 5: Comparison of death time of first sensor node with two schemes.

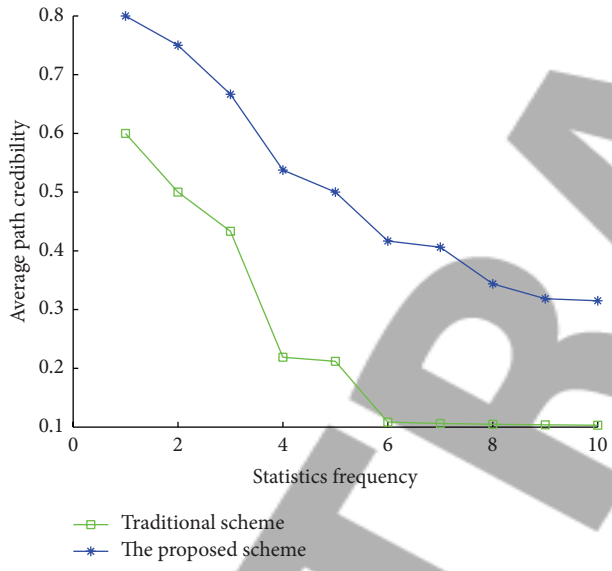

Figure 6: Comparison of average path credibility with two schemes.

4. Conclusions

The legitimacy of sensor node is the key of realizing data security fusion for WSNs. The traditional node abnormal behavior detection and the trust evaluation mode possess the single function, not all factors are properly considered, the trust value algorithm is relatively complicated, and so forth. Aiming at the above disadvantages, a trust evaluation model without reference based on the autonomous behavior of node is proposed, where each sensor node has the monitoring privilege and monitored obligation, as well as any neighboring nodes can monitor each other in the region close to the sensor node. Their direct and indirect trust values can be achieved by using relatively simple calculation method; then, their synthesis trust value could be obtained by the composition rule of D-S evidence theory. All the sensor nodes in neighborhood are clustered by self-organizing, and the cluster head node can be selected automatically as the sensor node for data fusion. The sensor node in each cluster directionally transmits the acquired data to its cluster head; then, the cluster head assigns the different weighted value for the data from each node and executes the data fusion processing; finally, the cluster head transmits the fused result into base station. The simulation experiment results demonstrate the trust evaluation model can rapidly, exactly, and effectively recognize malicious node and avoid malicious node becoming cluster head node. In view of the different proportion of attack behaviors in different application fields and deployment environments, the weight vector would be set when the synthesis trust value is calculated, so the experiment shows the trust evaluation model has the validity and the algorithm could be improved in various actual situations.

Conflict of Interests

The authors declare that they have no financial and personal relationships with other people or organizations that can inappropriately influence their work and that there are no professional or other personal interests of any nature or kind in any product, service, and/or company that could be construed as influencing the position presented in, or the review of, this paper.

References

[1] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization in distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 1, pp. 61–91, 2004.

[2] T. R. Willoughby, P. A. Kupelian, J. Pouliot et al., "Target localization and real-time tracking using the Calypso 4D localization system in patients with localized prostate cancer," *International Journal of Radiation Oncology, Biology, Physics*, vol. 65, no. 2, pp. 528–534, 2006.

[3] D. Verellen, G. Soete, N. Linthout et al., "Quality assurance of a system for improved target localization and patient set-up that combines real-time infrared tracking and stereoscopic X-ray imaging," *Radiotherapy and Oncology*, vol. 67, no. 1, pp. 129–141, 2003.

[4] V. Cevher, M. F. Duarte, and R. G. Baraniuk, "Distributed target localization via spatial sparsity," in *Proceedings of the 16th European Signal Processing Conference (EUSIPCO '08)*, Lausanne, Switzerland, August 2008.

[5] S. Zhong, K. Xia, X. Yin, and J. Chang, "The representation and simulation for reasoning about action based on Colored Petri Net," in *Proceedings of the 2nd IEEE International Conference on Information Management and Engineering (ICIME '10)*, pp. 480–483, Chengdu, China, April 2010.

[6] D. Le, Y. Jin, K. Xia, and G. Bai, "Adaptive error control mechanism based on link layer frame importance valuation for wireless multimedia sensor networks," in *Proceedings of the 2nd International Conference on Advanced Computer Control (ICACC '10)*, vol. 1, pp. 465–470, IEEE, March 2010.

[7] K. Xia, J. Cai, and Y. Wu, "Research on improved network data fault-tolerant transmission optimization algorithm," *Journal of Convergence Information Technology*, vol. 7, no. 19, pp. 114–120, 2012.

[8] K. Xia, Y. Wu, X. Ren, and Y. Jin, "Research in clustering algorithm for diseases analysis," *Journal of Networks*, vol. 8, no. 7, pp. 1632–1639, 2013.

[9] Y. Yao, J. Chang, and K. Xia, "A case of parallel EEG data processing upon a Beowulf cluster," in *Proceedings of the 15th International Conference on Parallel and Distributed Systems (ICPADS '09)*, pp. 799–803, Shenzhen, China, December 2009.

[10] K.-J. Xia, Y. F. Yao, J. Y. Chang, and S. Zhong, "An edge detection improved algorithm based on morphology and wavelet transform," in *Proceedings of the 2nd International Conference on Computer and Automation Engineering (ICCAE '10)*, vol. 1, 2010.