INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 10(2):248-262, April, 2015.

A Comprehensive Trust Model Based on Multi-factors for WSNs

N. Wang, Y. Chen

Na Wang
1. MoE Research Engineering Center for Software/
Hardware Co-Design Technology and Application
East China Normal University
No.3663 North Zhongshan Rd, Shanghai
2. Faculty of Engineering
Shanghai Second Polytechnic University
No.2360 Jinhai Rd, Shanghai
wnoffice@126.com

Yixiang Chen*
MoE Research Engineering Center for Software/
Hardware Co-Design Technology and Application
East China Normal University
No.3663 North Zhongshan Rd, Shanghai 200062 China
*Corresponding author: yxchen@sei.ecnu.edu.cn

Abstract: The goal of this paper is to introduce a novel trust model for wireless sensor networks. This trust model calculates trust value of nodes through two kinds of trusts: private trust and interactive trust of a node. Private trust focuses on the past record of a node's sensing and its remaining energy. Interactive trust cares for the interaction of a node with its neighbors. This trust model can recognize faulty nodes inside a network, reduce their impaction to data acquisition, and select a trust routing for precise data transmission. A simulation is given and shows that this trust model has a higher performance than TMS and ECCR in some aspects. But it consumes more energy than ECCR for its comprehensive structure of data.

Keywords: Wireless Sensor Networks, Trust Model, Private trust, interactive trust, Trust routing.

1 Introduction and related work

A wireless sensor network (WSN, shortly) consists normally of thousands of tiny embedded computers which are equipped with a specific type of sensor to sense information from the surrounding environment. The collected information is relayed from sensor to sensor, using a secure multi-hop routing protocol, until the data reaches the desired destination node, which is called as a sink. The WSN technology has been applied in many areas, such as industry, environment, seismology, construction, transportation, military warfare, traffic control and agriculture [1].

Sensor nodes in WSNs suffer often from resource constraints such as low computational capability, limited storage capacity, limited communication bandwidth, and the use of insecure communication channel. WSNs are also prone to varied types of attacks [4–8] such as black hole attack and sniffing attack. Cryptographic solutions can successfully defend against outsider attack but may fail under insider malicious attacks. This vulnerability along with the cooperative nature of sensor networks requires one for assessing the trust relationships among the nodes in the network [10].

Recently, some researches focusing on trust in WSN have been practiced based on different background such as GTMS [12], RFSN [13], HATWA [14] and [15]. But all the above schemas are based on either routing or data sensing respectively. In [13], a method considering key factors in running of WSN is proposed. But the researches are far from adequate. In [11], NBBTE (Node

Copyright © 2006-2015 by CCC Publications

Behavioral Strategies Banding Belief Theory of the Trust Evaluation Algorithm) is proposed, which integrates the approach of nodes behavioral strategies and modified evidence theory. The same authors as in [11] proposed in [3] a TMS schema based on the method in [11]. Direct trust value on each neighbor node is calculated by considering trust factors which are defined according to node behaviors in order to detect malicious attacks. At the same time, recommended trust value from common neighbor nodes is obtained through conditional transitivity and the weight of each recommendation is obtained by revised D-S evidence theory. Both [11] and [3] consider factors of received packets rate, successfully sending packets rate, packets forwarding rate, data consistency, time frequency, node availability and security grade. Data consistency is defined that the packets sent among neighbor nodes are similar in the same area according to the application. Time factor is defined that the size of time grade is dependent on the specific situation. If it is established too large, then integrated trust value is affected by history heavily. On the contrary, if it is established too small, then trust value relies on a single period overly. Except for the above three factors, others factors mainly aims on communication. The multi-factors in [11] make a progress in trust management for WSN. With regardless of the core algorithm in [11], the factors considered are reasonable and adequate to compute trust value of a common node. But it does not deal with the relationship of the factors. The reference [2] introduces a notion of trust evaluation to build trust mechanism for each node inside network.

About routing, in order to improve reliability, some multipath routing technologies have been mentioned. The k heavier path is used between the source node and purpose and the packet is divided into different packet to transmit in [19]. In literature [20], they take to adjacent cluster head number as a topological construction weights, looking forward to a constant approximate rate based minimum network connected dominating sets, but this method does not consider cluster head of network node energy influence on the performance of the whole. According to the size of the nodes energy to network between the influence of choice, the literature [21] considers energy as weights, ensure constant approximation rate at the same time as a priority high-energy node cluster of communication between nodes, and, to some extent, improve the network energy efficiency, but it ignores the routing communication costs between clusters, existence of high communication costs of premature failure of the head node limitations. In [22], defining link reliability strategy constructed by remain energy, and communication cost of nodes as topology weight to synthetically reflect the energy efficiency of dominator, an Energy-radio and communication cost route (ECCR) is proposed to solve the problem that the average energy consumption in cluster and minimum communication cost. The author takes both node residual energy and distance into account to compete cluster head, at the same time, in order to reduce the cluster head energy cost, link reliability and hop are used to establish topological structure. The experimental results show that the algorithm not only has the energy saved characters, but also ensures the reliability of topology links and extends the network life-cycle efficiently. But ECCR focus on energy efficiency but not data precision while trust may decide which route is trust for transmission to get more precise data, so the performance can be improved in view of trust value.

In order to meet both data and energy requirement, it is necessary to build a trust model based on multi-factors which consider data, communication, clock and energy to help more application such as data aggregation, fault detection and route selection. The contribution of this paper is:

1. Create a node trust model based on interactive factors and private factors.

2. Give a routing algorithm to compute routing trust based on nodes' trust value.

3. Apply our model in fault detection.

4. Evaluate and compare our model with other models.

This paper introduces a novel trust model for wireless sensor networks. This trust model calculates trust value of nodes through two kinds of trusts: private trust and interactive trust. Private trust focuses on the past record of a node's sensing and its remaining energy. Interaction trust cares for the interaction of a node with its neighbors. This trust model can recognize faulty nodes inside a network, reduce their impaction to data acquisition, and select a trust routing for precise data transmission. A simulation is given and shows that this trust model has a higher performance than TMS and ECCR in some aspects. But it consumes more energy than ECCR for its comprehensive structure of data.

The rest of the paper is organized as follows. The definitions and models are proposed in section 2 and 3. The routing algorithm based on our trust model is depicted in Section 4 and we apply this model in fault detection on section 5. The comparison and evaluation of our trust model with other models are given in Sections 6. The conclusions and future work are presented in Sections 7.

2 Definition of key attributes for trust in wireless sensor networks

In order to defeat various attacks, we have to take all kinds of factors that depend on the interactions between neighbor nodes into account. However, there is an obvious trade-off between the number of factors and the energy consumption. In this paper, we pay attention on four key attributes which are called as to be connectivity, consistency, synchronization and adequacy to the node's trust. Since the structure of WSN is divided into inner indicating the level within one cluster and outer intra indicating the level between clusters heads. The structure is shown in Figure 1.

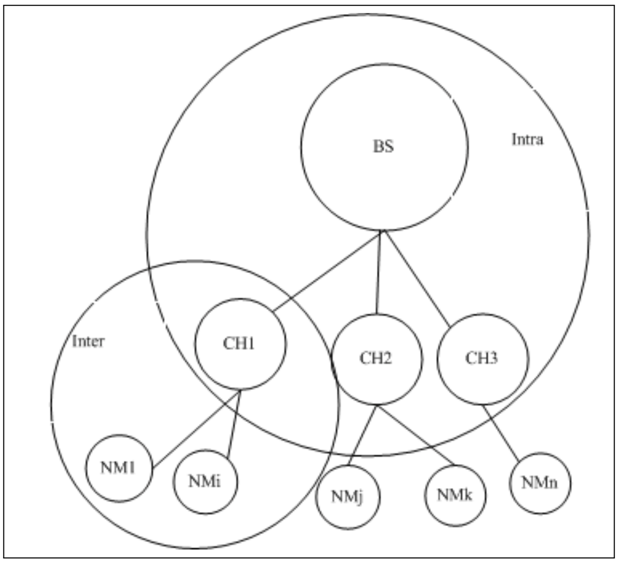

Figure 1: The structure of WSN

We focus on the evaluation of nodes in one cluster and then use the same method to evaluate the trust between cluster heads. Before doing it, we depict the running process of stages within a WSN as follows.

Event-driving stage: When there is a request of detecting in a certain field from sink node, sink node will send a sensing order to its neighbor nodes.

Self-organizing stage: The nodes received the request will be as the first level cluster heads. And the cluster heads will select their members according to cluster protocol such as LEACH.

Detecting stage: Member node senses data after receiving the request message from its cluster head. The sensing action is frequent according to the sampling period.

Communication stage: member node sends its data to the cluster head and its neighbors. In this stage, interaction and data aggregation are crucial to trust value. When a member node sends data to other nodes, there will be two cases that are successful connection and failed connection with regard to communication. And the data sent from a certain member node may have two results comparing with other data that is consistent and inconsistent with regard to data. Furthermore, the sensing moment should take into account when measure data consistency since data has time attribute.

Data aggregation: After data exchange, each node has the information of its neighbors and cluster head has the information of all members in cluster. In order to reduce information and energy consumption, data from member nodes will be aggregated in head with certain format and will be sent to high-level head.

Convergence stage: Data from each level head will be aggregated and sent hierarchically till to the sink.

During the process, attacks such as bad mouth and fault such as hardware fault may influence the result of aggregation. Both attack and fault are called abnormal cases in this paper. In order to exclude the abnormal nodes, one of the resolve methods is giving a trust value to each node. When the trust value is keeping lower for certain duration, it should be deleted from the network. Since the communication and sensing are the main action in WSN, the interaction and data should be regarded as the main parameters to construct trust value.

3 Node trust model based on multi-factors

In this section, we divide node trust into two parts: interactive trust and private trust. Interactive trust describes the trust of a node's interaction with its neighbor nodes based on interactive factors. Private trust focuses on describing a node's nature reputation based on private factors.

3.1 Introduction of factors

In WSN, there are interactions between nodes, so we abstract interactive factors. During the interactions, data including its time attribute will be exchanged in cluster head. We call them as interaction, data and time. Considering the factors, we should give a combined trust model. But as the relations between factors are not simple, traditional model cannot be applied here. Generally, relations between two factors are divided into three classes that are promoted, opposite and uncorrelated. Promoted relationship means the promoting of A will make B promote. Opposite relationship means the promoting of A will make B decline. And uncorrelated relationship means the change of A will make no influence on B. The factors within this paper have relationship as depicted in Table 1. Table 1 describes the relationship of interactive factors which involve success interaction between nodes, data similarity between nodes and approximate sensing time of two nodes. Here, symbol plus means promoted relation between two factors, minus means opposite relation and blank means uncorrelated relation. It is shown in table 1 that when valid interaction increased, similar data will increase (Here, we consume general case that normal data is more than fault data). Time which is an attribute of data has the same relation with other factors as data.

Table 1: Relationships between interactive factors

	Interaction	Data	Time
Interaction		+	+
Data	+		+
Time	+	+	

Table 2: private factors

Factors:	Data	Energy

We also consider the private factors of a node in this paper. Table 2 describes the private factors for a single node in which the variation of sensing data in a period and remaining energy are taken into account. The data factor relates the data correctness and energy factor relates to the node's working ability. We give a reward coefficient to correct data and a penalty coefficient to error data. Energy is a natural factor that can deduce from initial energy and remaining energy. It decides whether the node is running.

3.2 Interactive factors

We define the interactive factors as:

Interaction: When considering the number of continuous communication during t, we compute it as

$$\mathrm{DCT}_{i,j}(\Delta t) = \left\lfloor \Big(\frac{100 \cdot s_{i,j}(\Delta t)}{s_{i,j}(\Delta t) + f_{i,j}(\Delta t)}\Big)\Big(\frac{1}{\sqrt{f_{i,j}(\Delta t)}}\Big) \right\rfloor. \tag{1}$$

In order to compress the size of data for energy consumption reduction, the trust value is multiplied by 100 and get integer. Where, $s_{i,k}(\Delta t)$ is the success number of communication between node i and j in time Δt, and $f_{i,j}(\Delta t)$ is the failure number of communication between node i and j in time Δt. When failure number is larger than success number, we may think that these two nodes i and j are distrust. We make the value decline sharply by dividing $\sqrt{f_{i,j}(\Delta t)}$. Specially, if $f_{i,j}(\Delta t) = 0$, we set $\mathrm{DCT}_{i,j}(\Delta t) = 100$ [16].

Data:

$$\mathrm{DST}_{i,j}(\Delta t) = \left\lfloor \Big(\frac{100 \cdot c_{i,j}(\Delta t)}{c_{i,j}(\Delta t) + d_{i,j}(\Delta t)}\Big)\Big(\frac{1}{\sqrt{d_{i,j}(\Delta t)}}\Big) \right\rfloor. \tag{2}$$

$$c_{i,j} = \frac{X_i X_j}{X_i^2 + X_j^2 - X_i X_j}. \tag{3}$$

$c_{i,j}(\Delta t)$ is the total number of similar data comparison of node i with j in Δt time, and $d_{i,j}(\Delta t)$ is the total number of dissimilar data comparison. X_i is sensing data of node i. Specially, if $d_{i,j}(\Delta t) = 0$, we set $\mathrm{DST}_{i,j}(\Delta t) = 100$.

Time:

$$T_{i,j} = \left\lfloor \frac{100 \cdot T_i T_j}{T_i^2 + T_j^2 - T_i T_j} \right\rfloor. \tag{4}$$

The factors above can fulfill the complexity of trust evaluation. Furthermore, the factors will change with the elapse of time not only by themselves but by other factors.

3.3 Interactive trust related to interactive factors

Now, we present the interactive trust based on interactive factors. Interactive factors mentioned above are abstracted from WSN which are crucial when computing the trust value between nodes. In order to depict the relations and factors' importance in the model, we use a weighted trust model to compute trust value between two nodes as formula (5).

$$T_I = \Big\lfloor \prod_{i=1}^{n} y_i^{\alpha_i} \Big\rfloor \qquad \Big(\sum_{i=1}^{n} \alpha_i = 1\Big). \tag{5}$$

T_I presents the direct interactive trust between two nodes, and y_i is value of the ith factors with its weight α_i. Here, y_i indicates four factors which come from formula (1)-(4). Since α_1 is the weight of factors, its value should display the importance of a factor in T_I. With considering the relations described in table 1, we use reciprocal matrix to decide each factor's weight.

For example, from the perspective of optimization, the approach of measuring sort vector according to reciprocal matrix is based on the fact that when $A = \big(a_{i,j}\big)_{n\times n}$ is a reciprocal matrix, $A\omega = n\omega$ and $\omega = \big(\omega_1, \omega_2, \ldots, \omega_n\big)^T$ where $\big(a_{i,j}\big) = {}^{\omega_i}/_{\omega_j}$.

In our paper, we set the reciprocal matrix based on table 1 as Figure2. And use method naming right characteristic root to calculate weight vector as:

(Interaction, Data, Time)=(0.5869, 0.3238, 0.0893).

$$\begin{bmatrix} 1 & 2 & 6 \\ 1/2 & 1 & 4 \\ 1/6 & 1/4 & 1 \end{bmatrix}$$

Figure 2: Reciprocal matrix

3.4 Private trust based on private factors

In WSN, a node's private trust will depend on its previous action. This private trust must be penalized when its sensing data is deviated far from the average and be awarded when its sensing data is correctly consecutively. For example, a fire can start near a sensor, so that sensor will read values higher than its neighbors at round one. If this is the case, and a large penalty is given to the sensor then it will considered as a fault node where in fact it is not. In our work, the node will be penalized with a small factor and will be rewarded in the next round, since the average will tend to be that of a disaster state. Private trust has a combination method that is shown in formula (6).

$$T_p = \begin{cases} \theta_1 \cdot T_{p-1} + \theta_2 \cdot F + \theta_3 \cdot (\mathrm{e}^{-R} - 1) + \theta_4 \cdot E, & \text{if } D > \text{threshold;} \\ T_{p-1}, & \text{if } D \leq \text{threshold.} \end{cases} \tag{6}$$

In this formula, $\theta_1 + \theta_2 + \theta_3 + \theta_4 = 1$. F presents the number of consecutive same sensing out of a predefined number whose value varies between 0 and 1, T_{p-1} is the last trust value in the previous round, D is the deviation from normal value of sensing, R is the number of misreading and E is whether the node can be found by its parent. θ_2 and θ_3 are reward and penalty coefficient respectively whose value can vary between 0 and 1. E is deduced from ${}^{E_r}/_{E_i}$ where E_r is remaining energy and E_i is initial energy. When ${}^{E_r}/_{E_i}$ is lower than that can support transmit, E is set as -1, otherwise, E is set as 0.

Once T_p is equal to 0, the node is regarded as faulty to be deleted from the network. Once ${}^{E_r}/_{E_i}$ is equal to 0, the node is out of work to be deleted.

In order to keep consistent with T_I, T_p should be multiplied by 100 to get an integer too.

4 Routing algorithm based on multi-factors

4.1 Double-weight trust diagram

When consider nodes in one cluster, we get a $G = (V, E, W_v, W_E)$ consisting of vertexes V, edges E and weight W. Each vertex is a node and each edge is the connection of two neighbors. We set private trust of a node as the vertex weight and interactive trust as the edge trust. The Figure 3 is a double-weight trust diagram.

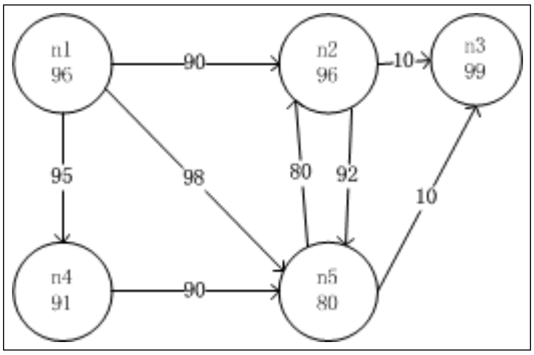

Figure 3: Double-weight trust diagram

In this diagram, node $n1$ has its private trust 0.96 and three interactive trusts 90, 95, 95 with $n1$, $n4$ and $n5$ respectively. It is assumed that $n3$ is the cluster head, when $n1$ transmits its sensing data to cluster head, it can route as $\{1, 2, 3\}$, $\{1, 5, 3\}$, $\{1, 4, 5, 3\}$, $\{1, 2, 5, 3\}$, $\{1, 5, 2, 3\}$ and $\{1, 4, 5, 2, 3\}$. Here, we do not consider circle since the circle can't increase the trust of a routing. In order to select the most trustful routing, we must compute the trust of each routing.

4.2 Routing trust

In [18], Chen et al propose a matrix-based computing method for max-mean measurement. The model defines a series of matrices $S^k = (s^k_{uv})_n$ for max-mean degree inductively as $S^1 = A$ and $S^k = A \odot S^{k-1}$, for any $k2$,

$$s^k_{uv} = \begin{cases} 0, & u = v; \\ {}^1/_k \max\{a_{ur} \oplus s^{k-1}_{uv}\}, & \text{otherwise.} \end{cases} \tag{7}$$

Where

$$a \oplus b = \begin{cases} 0, & \min\{a, b\} = 0; \\ a + b, & \text{otherwise.} \end{cases} \tag{8}$$

Our trust diagram in Figure 3 describes the private trust and interactive trust respectively, but, when selecting a route, a combined trust should be considered. We indicate private trust as P_t and interactive trust as I_t, then the combined trust can be computed through formula (9).

$$C_t = \sqrt{P_t \cdot I_t}. \tag{9}$$

The trust matrix for Fig.1 is as Figure 4.

$$\begin{pmatrix} 0 & 93 & 0 & 95 & 95 \\ 0 & 0 & 92 & 0 & 92 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 91 \\ 0 & 80 & 30 & 0 & 0 \end{pmatrix}$$

Figure 4: Trust matrix for figure.3

According to formula (7) and (8), the six routing trust is shown in Table 3.

Table 3: routing trust for Figure.3

Routing	$\{1,2,3\}$	$\{1,5,3\}$	$\{1,4,5,3\}$	$\{1,2,5,3\}$	$\{1,5,2,3\}$	$\{1,4,5,2,3\}$
Trust	92	93	72	71	89	89

It is clearly that, if precise is prior to length, routing $\{1,5,3\}$ should be selected as routing between $n1$ and the cluster head $n3$.

5 Application of our model in fault detection

One of the critical tasks in designing a wireless sensor network is to monitor, detect, and report various useful occurrences of events in the network domain which is determined by the result of data aggregation. But sensor nodes are neither reliable nor stabile due to outer factors as environment and inner factors as energy. Then fault detection is critical to the efficiency of data aggregation scheme. In our former work [18], we present an improved k-means data aggregation algorithm considering the proposal of outliers. Each cluster includes three types of sets: aggregation data set, fault data set and abnormal data set. Abnormal nodes can be detected according to the aggregation result. But the detection of fault nodes is completed in a hierarchical structure till the level of sink.

When trust value reserved as an attribute of a node, the detection of fault node and outlier during data aggregation can deduce from trust values. If a node's private value is higher than a threshold, it is regarded as a normal node. When nodes are not regarded as normal, they may be outlier or abnormal nodes which must be recognized with using interactive value. If its interactive trust is higher than a threshold while its private trust is low, it may be the case that the node is located on the edge of the event area and detects an event such as fire or insect pest. Otherwise, it must be a fault node. The process is described in Figure 5.

6 Validations and evaluations

6.1 Properties of T_I

As interactive trust value is depended on multi-factors, the value of each factor should impact the trust value. That is to say the increasing of factors' value can lead to the increasing of interactive trust value. In another aspect, impacting of one factor must be limited. Generally, trust value is set as a real that lower than 1. We can prove the property above.

Assertion 1. $T_I \leq 1$.

Proof: In formula (5): $T_I = \prod_{i=1}^{n} y_i^{\alpha_i} \quad \left(\sum_{i=1}^{n} \alpha_i = 1\right)$, y_i means interaction, data or time.

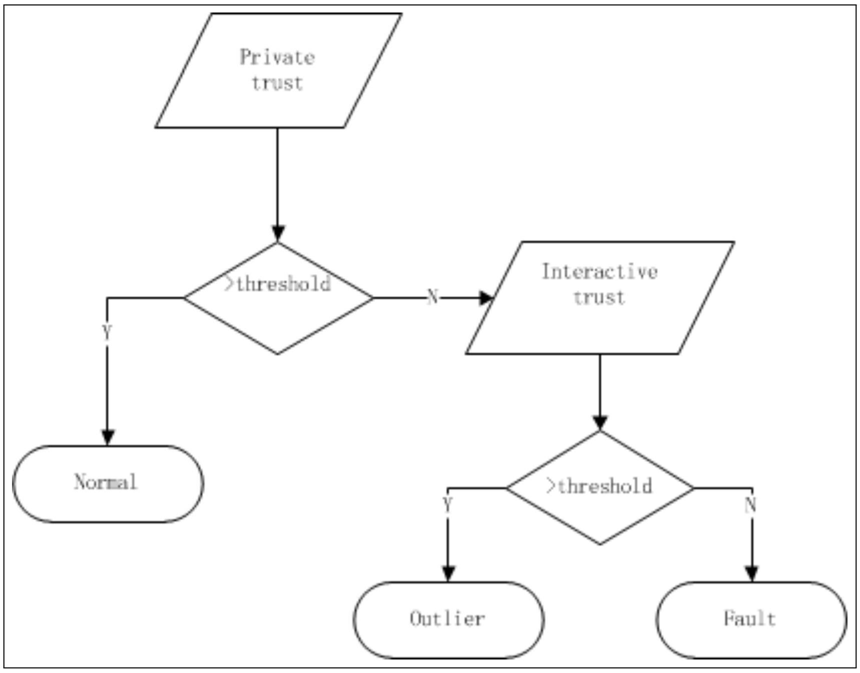

Figure 5: Process of fault detection based on trust

According to formula (1), (2) and (4):
Interaction ≤ 1;
Data ≤ 1;
Time ≤ 1;
$\sum_{i=1}^{n} \alpha_i = 1$, $\alpha_i \leq 1$.
Then $T_I \leq 1$. □

Assertion 2. T_I is monotone.

Proof:

$$\bar{T_I} = \alpha_i \cdot y_i^{\alpha_i - 1} \cdot y_1^{\alpha_1} \cdot \cdots \cdot y_{i-1}^{\alpha_{i-1}} \cdot y_{i+1}^{\alpha_{i+1}} \cdot \cdots \cdot y_n^{\alpha_n} \geq 0.$$

□

This attribute ensure that the increasing of factors' value can lead to the increasing of interactive trust value.

Assertion 3. T_I is agglomerate.

Proof:

$$\bar{\bar{T_I}} = \alpha_i(\alpha_i) \cdot y_i^{\alpha_i - 2} \cdot y_1^{\alpha_1} \cdot \cdots \cdot y_{i-1}^{\alpha_{i-1}} \cdot y_{i+1}^{\alpha_{i+1}} \cdot \cdots \cdot y_n^{\alpha_n} \leq 0.$$

□

This attribute ensure that impacting of one factor is limited.

6.2 Properties and evaluation of T_p

In formula (6), the initial private trust value is 1, with the running of WSN, the value either keeps unchanged or iterates with the penalty and reward coefficients which make the value being lower than 1. If we set $\theta_2 = 0.5$ and $\theta_3 = 0.5$, where the same 0.5 has different impact on correct reading and misreading since the misreading is depicted in exponential manner. When a round of simulating is set as 10 reading and initial value of trust is set as 1, the private trust value of normal node, event node and fault node is shown in Figure 6. If we only consider data, normal nodes' private trust will not change during the process, while event nodes' will decline at the beginning of event, then raise at the next round since the penalty will offset by the reward. Fault nodes' trust will decline immediately until reaching zero and the nodes will be deleted from the network.

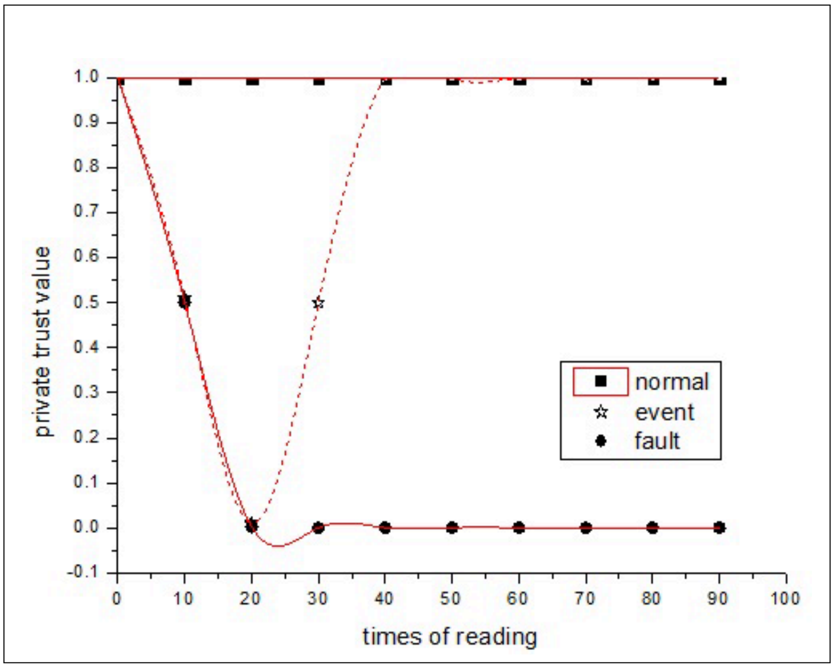

Figure 6: Private trust value for different nodes

6.3 Evaluation of routing selection based on our model

In WSN, it is important to choose a routing protocol, because the efficient routing paths between the sensor node and the sink change with time, especially in case of considering different factors. The above greedy forwarding is a candidate because it is simple and efficient about data transmission. In greedy forwarding, each node just needs to know three pieces of information: the trust value of its own and interaction with neighbors, its location, the location of neighbors. The relative location is displayed in Figure 3 by directed arc, the direction is from nodes farther away from destination to nodes nearer to the destination. The impacts of interaction trust based on channel failure rate and private trust base on sensing failure rate on routing reliability can be described in Figure 7.

Our simulation experiment is based on ns3. Fifty sensor nodes are distributed in a space of 500×700, and the communication radius is set as 60. Each node has two to five neighbors in the experiment and the node's location is already known. The detailed value is shown in Table 4. The comparison of routing reliability for ECCR and our model with different fault rate is shown in Figure 8. Here, reliability displays valid interaction and precise data transmission. We can get that our model has a higher reliability than ECCR in the whole. Especially, when there are fault nodes in routing, our model is effected little in reliability while ECCR's reliability declines a lot just because it does not consider sensing failure caused by faulty nodes. But our model selects normal nodes with high private trust to transmit data to a neighbor node having highest interaction trust with it.

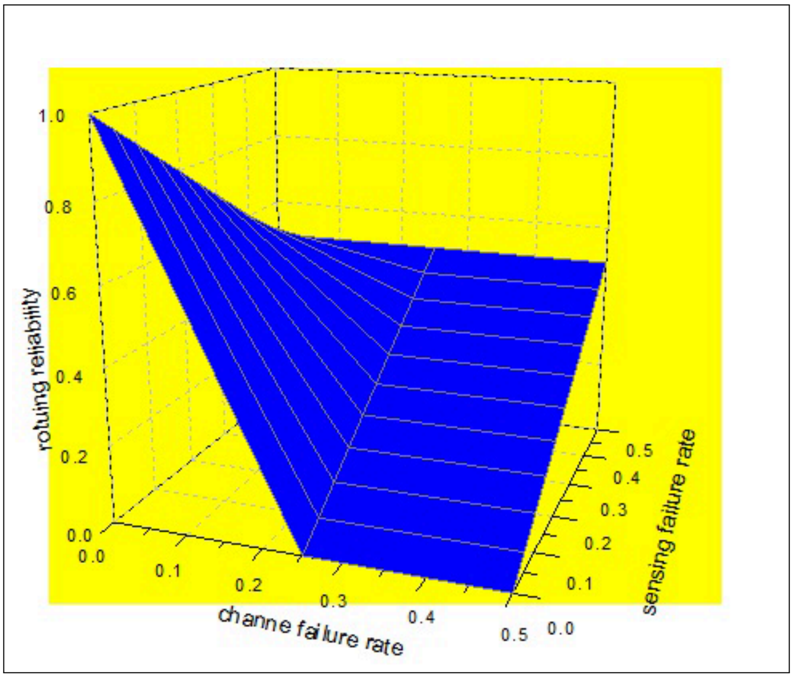

Figure 7: Relationship between reliability and failure rate

Table 4: Values in evaluation

Symbol	Description	values
N	Number of nodes	50
n	Number of CMs in a cluster	6-8
m	Number of CM's neighbors	4-6
θ_1	History trust coefficient	0.9
θ_2	Reward coefficient	0.04
θ_3	Penalty coefficient	0.05
θ_4	Energy coefficient	0.01
t	Threshold for E	0.1

Except for reliability, energy consumption is another important merit to measure the routing protocol based on the trust model. The structure of data is shown in Table 5. Simulation result shown in Figure 9 indicates that the energy consumption of ours models is higher than ECCR because our model keeps a larger size of data than ECCR since ECCR does not consider sensing data. It also indicates that the fault rate impacts a lot in our model because when a node is faulty, its private trust value is computed by the iterated part in formula (6).

Table 5: Structure of data in our model

Node ID	The size of interaction		The size of similar		The size of trust	
	$S_{i,j}$	$F_{i,j}$	$c_{i,j}$	$d_{x,y}$	Interactive	Private
2 bytes	1 bytes	1 bytes	1 bytes	1 bytes	1 bytes	1 bytes
The size of time | The size of sensing data | The size of energy						

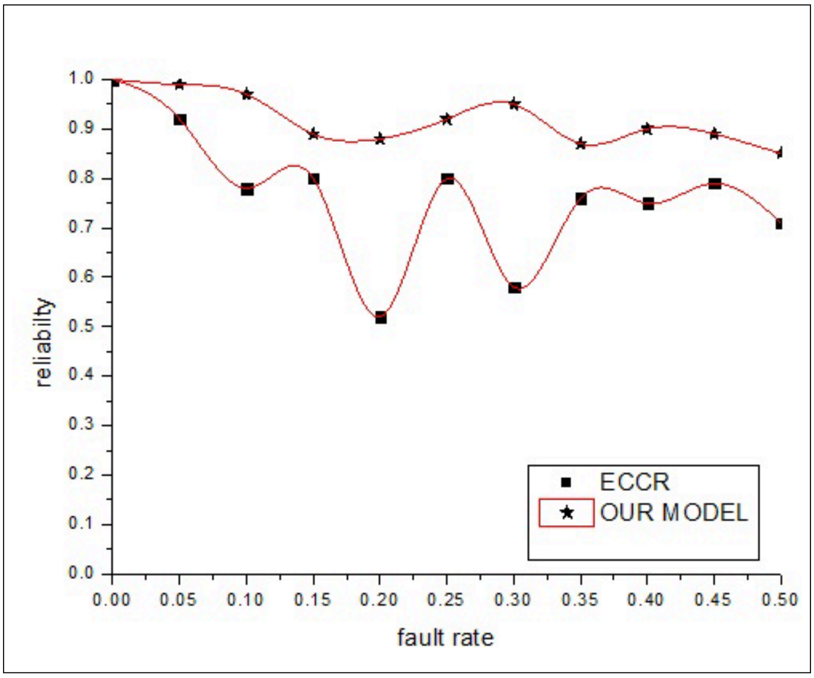

Figure 8: Reliability of different fault rate

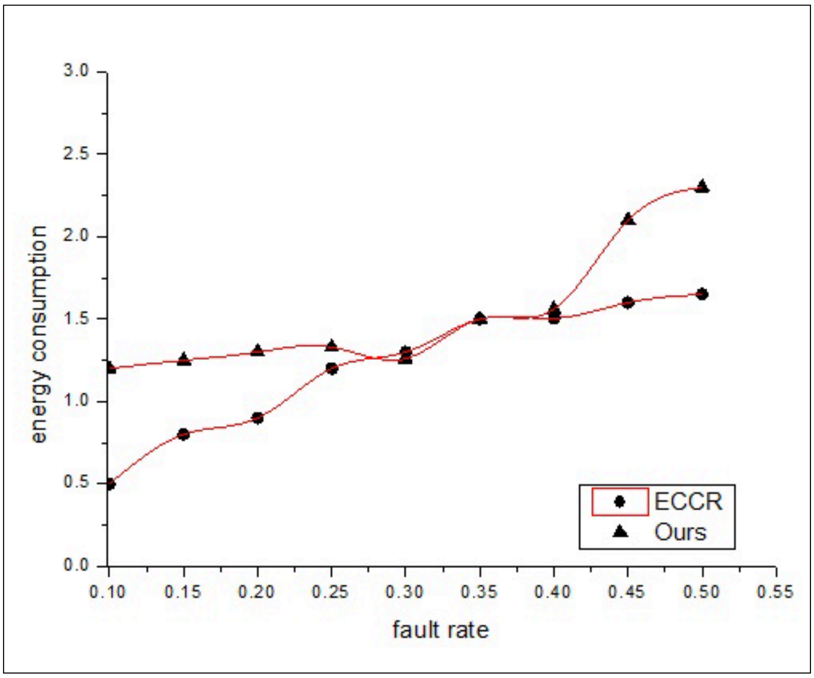

Figure 9: Energy cost of different fault rate

6.4 Evaluation of fault detection based on our model

In this subsection, we compare our model with TMS since TMS is an outstanding trust model considering different factors in WSN. The result is shown in Figure 10 which indicates that the detection of our model is higher than TMS during the running time because we introduce private trust to rapidly judge a fault node. But the fluctuation is larger than TMS due to the temporary malicious judge of event nodes.

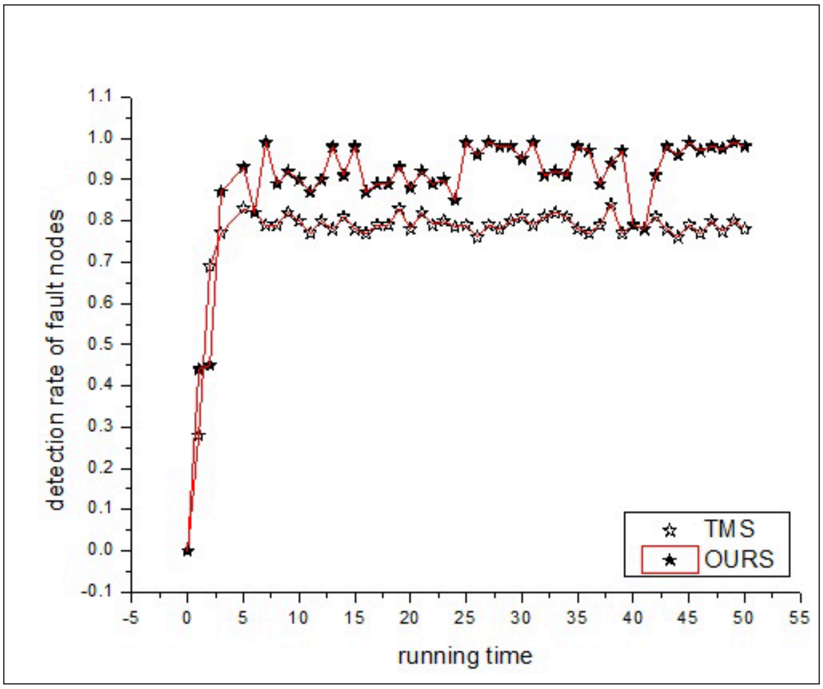

Figure 10: Detection rate within running time

7 Conclusion and future work

In this paper, a trust model based on multi-factors is proposed. It defines multi-factors in WSN to help build trust model including private trust and interactive trust. Private trust focuses on the past record, current record and remaining energy of a node and interactive trust focuses on the interaction of a node with its neighbors. Interactive factors include communication, data and time to keep nodes connective, consistent and synchronized. Private factors include data and energy to ensure a node consistent with itself and keeping active when working. The validation shows the increasing of factors' value can lead to the increasing of interactive trust value and the impacting of one factor is limited. Using the two types of trusts, a routing trust algorithm is proposed that is expressed as a two-weight diagram. With the routing model, a node can transmit its sensing data more accurately to the cluster head or sink than ECCR, but consume more energy. Furthermore, the trust model can be used in fault detection and the simulation results comparing with TMS show that the proposed model can rapidly detect fault and effectively raise fault detection rate with a fluctuation due to event nodes. In the future, we will pay more attention on the application of the model and algorithm this paper proposed to real wireless sensor network, for example, the environment detecting.

Acknowledgements

This work is supported by the National Basic Research Program of China (Grant No. 2011CB302802) and the Innovation Group Project of the National Natural Science Foundation(Grant No. 61321064). The National Natural Science Foundation of China (Grant No. 61370100). Shanghai Knowledge Service Platform Project (No. ZF1213). Wang acknowledges the supported of the key discipline of Shanghai second polytechnic University named software engineering (No.XXKZD1301). The authors would like to thank the referees for their invaluable comments and suggestions.

Bibliography

[1] Osman Khalid, Samee U.Khan(2013); Comparative study of trust and reputation systems for wireless sensor networks, *Secutity and Communication Networks*, 6(6):669-688.

[2] Xiang Gu, Jianlina Qiu, Jina Wang(2012); Research on Trust Model of Sensor Nodes in WSNs, *Procedia Engineering*, 29(2012):909-913.

[3] Renjian Feng, Shenyun Che, Xiao Wang, Ning Yu(2013); Trust Management Scheme Based on D-S Evidence Theory for Wireless Sensor Networks, *International Journal of Distributed Sensor Networks*, 2013(2013):9-18.

[4] K.Hoffman, D.Zage, C.Nita-Rotaru(2009); A survey of attack and defense techniques for reputation systems, *ACM Computing Surveys*, 42(1):1-31.

[5] C.Karlof, D.Wagner(2012); Secure routing in wireless sensor networks, *International Journal of Computer Science Issues*, 9(1): 187Â¨C191.

[6] J.Lopez, R. Roman, C.Alcaraz(2009); Analysis of security threats, requirements, technologies and standards in wireless sensor networks, *Foundations of Security Analysis and Design*, 25(2):289-338.

[7] B.Xiao, B.Yu(2006); Detecting selective forwarding attacks in wireless sensor networks, *In Proceedings of the 20th International Parallel and Distributed Processing Symposium*, 2006(2006):1-8.

[8] Y.Yu, K.Li, W.Zhou, P.Li(2012); Trust mechanisms in wireless sensor networks: attack analysis and countermeasures, *Journal of Network and Computer Applications*, 35(3): 867-880.

[9] E.Aivaloglou, S.Gritzalis, C.Skianis(2008); Trust establishment in sensor networks: behaviour-based, certificate-based and a combinational approach, *International Journal of Systems Engineering*, 16(5): 128-148.

[10] R Feng, X Xu, X Zhou, J Wan(2011); A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory, *Sensors*, 11(2):1345-1360.

[11] Riaz Ahmed, S.Jameel(2009); Group-based trust management scheme for clustered wireless sensor networks, *IEEE Transactions on Parallel and Distributed Systems*, 20(11): 1698-1712.

[12] Ganeriwal(2008); Reputation-Based Framework for High Integrity Sensor Networks, *In Proceedings of ACM workshop security of ad hoc and sensor networks*, 4(3): 66-72.

[13] V.R. Sarma Dhulipala, N.Karthik, RM.Chandrasekaran(2013); A Novel Heuristic Approach Based TrustWorthy Architecture for Wireless Sensor Networks, *Wireless Pers Commun*, 18(3):189-205.

[14] Na Wang, YiXiang Chen(2013); A Fault-Event Detection Model Using Trust Matrix in WSN, *Sensors & Transducers journal*, 158(11):190-194.

[15] Na Wang, Yanxia Pang(2014); An improved light-weight trust model in WSN, *Computer Modeling & New Technologies*, 18(4):57-61.

[16] Hongwei Tao, Yixiang Chen(2010); Another Metric Model for Trustworthiness of Softwares Based on Partition, *Advances in Intelligent and Soft Computing*, 82(2010):695-705.

[17] Yixiang Chen, TianMing Bu, Min Zhang, Hong Zhu(2010); Measurement of Trust Transitivity in Trustworthy Networks, *Journal of Emerging Technologies in Web Intelligence*, 2(4):319-325.

[18] Na Wang, YuePing Wu(2013); Data aggregation for failure tolerance in wireless sensor network, *Applied Mechanics and Materials*, 347(2013): 965-969.

[19] C.Intanagonwiwat, R.Govindan, D.Estrin(2000); A scalable and robust communication paradigm for sensor networks, *In Proc. Sixth Annual International Conference on Mobile Computing and Networks*, 28(2000): 238-249.

[20] L Ruan, H W Du, X H Jia, et al(2004); A greedy approximation for minimum connected dominating sets, *Theoretical Computer Science*, 329(1-3): 325-330.

[21] Y Tang, M T Zhou(2007); Maximal independent set based distributed algorithm for minimum connected dominating set, *Acta Electronica Sinica*, 35(5): 868-874.

[22] Machado Kassio, Rosario Denis(2013); A routing protocol based on energy and link quality for internet of things applications, *Sensors*, 13(2):1942-1964.