Research on Trust Calculation Mechanism of Wireless Sensor Network of Internet of Things

Li Mo

Beijing University of Technology, No.100, Pingleyuan, Chaoyang District, Beijing, China

1985099402@qq.com

Keywords: Internet of Things; Wireless Sensor Network; Trust Management; Trust Assessment; Trusted Computing

Abstract: For IoT WSN security, this paper proposes a flexible, reliable, safe and universal trust computation mechanism of WSN of IoT. According to the characteristics of IoT WSN and comprehensively considering the basic properties of trust calculation, design principle of trust calculation, this section proposes a flexible, reliable, safe, universal trust calculation architecture and a specific trust calculation model TCMDII. Through simulation results, TCMDII model is a good reflection of the change in trust of node entity with the number of transactions, which is in line with the expected analysis; compared with EignRep model and PeerTrust model, TCMDII model is better in trust calculation cost and transaction success rate aspects.

Introduction

With the rapid development of information technology, the application scope of informatization has been extended continuously. IoT has been highlighted in the global scope.

As wireless communication, sensor technology, embedded application and microelectronics technology become mature, WSN can get information which people need at any time, any place, any environmental condition, lay a foundation for the development of IoT. Despite the wide range of potential applications value, due to the WSN in practical applications are often deployed in no one care and even hostile environment, its security problems are especial. In fact, the security issue has gradually become the main obstacle for the trend of WSN technology to large-scale and industrialized application [1,2]. Therefore, the research of WSN security technology has become one of the key points in the research of IoT security.

Traditional WSN security mechanism is mainly based on encryption and authentication technology, it is not suitable for resource-constrained WSN[3]. In this background, the research on the trust management mechanism of WSN with lower computational complexity and higher network internal attack resistance has emerged.

WSN trust management mechanism based on the intrusion detection module, trust evaluation as the core, trust evaluation results as a safety measure, can be used for various kinds of network communication and applications. The trust evaluation mechanism usually includes trust calculation and trust data collection, which is the core of the whole trust management system [4]. As the result of trust evaluation is usually applied to various security strategies of network, it has very important research value and significance [5]. However, there are still many defects and deficiencies in the existing trust evaluation mechanism of WSN. The trust evaluation mechanism usually includes trust data collection and trust calculation. The collected trust data needs to be processed through the trust computing model to obtain the final result of trust assessment. First of all, the traditional trust calculation model does not fully consider the characteristics of trust and the basic design principles of trust measurement, and its design method is not rigorous. Secondly, the existing calculation method without considering the characteristics of WSN that has limited calculation, energy and storage resources, cannot apply to applications environment of IoT WSN. Finally, the existing calculation method does not consider the security problems of WSN, for example, once the compromise node is included in the trusted node set, these compromise node may provide a false

recommendation trust, which directly affect the accuracy of calculation and assessment; in run time points are attacked, the internal configuration files of this node are tampered.

Therefore, this paper proposes a IoT WSN trust computation mechanism with low complexity and high reliability, after analyzing the basic characteristics of WSN and the design principle of trust computing model, and considering direct trust, indirect trust and intrinsic trust of nodes.

Design of IoT Trust Calculation Model

Trust Computing Architecture. According to the characteristics of IoT WSN and comprehensively considering the basic properties of trust calculation, design principle of trust calculation, this section proposes a flexible, reliable, safe, universal trust calculation architecture, as shown in Fig. 1.

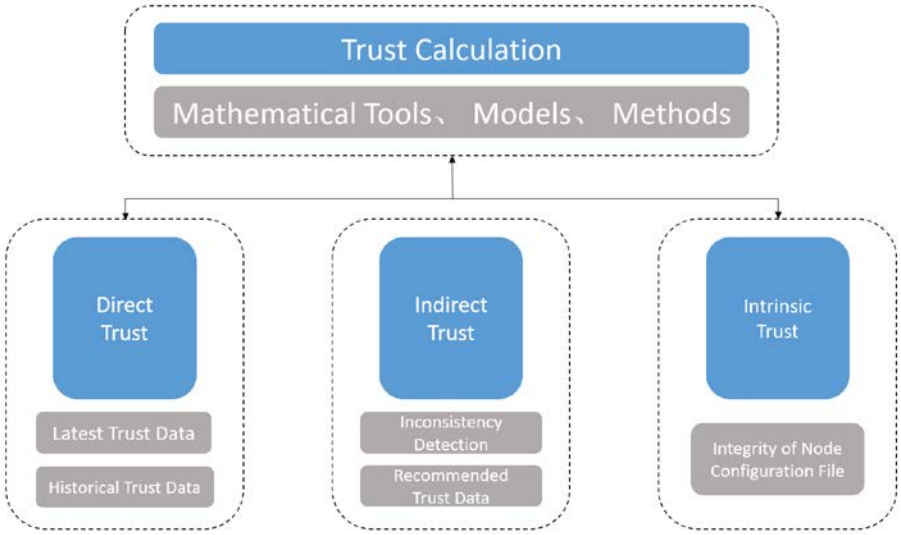

Fig. 1 Trust Calculation Structure.

In order to satisfy the need of distributed trust calculation, the trust value of each node is usually composed of three parts: direct trust, indirect trust and intrinsic trust. Assume that node i is the trust evaluating node, node j is the evaluated node. The direct trust of node i to node j indicates that node i uses the local management system to monitor the behavior of node j, and calculates the trust value according to its own test results. Taking into consideration the time attribute of trust, direct trust calculation can be further divided into two parts: the latest trust data unit and the historical trust data unit. The reliability of direct trust calculation can be improved by giving different weights to the latest data and historical data. The indirect trust of node i to node j indicates that node i gets the recommended trust value of node j by asking other nodes. Considering the overhead of node storage, communication and computation, the scheme in this paper selects the neighbor nodes of the evaluated node as the object to ask for indirect trust value. The intrinsic trust value of node j is obtained by dynamic measurement of the integrity of running perceived application of the current node j.

In order to obtain more accurate results of trust calculation, a certain mathematical method and model are needed to aggregate the direct trust value, the indirect trust value and the eigenvalue trust value.

Trust Calculation Model. In order to evaluate the trust value of IoT WSN, this section proposes a specific trust calculation model TCMDII. Node *i* is the trust evaluation node, node *j* is the evaluated node, and the trust value of node *i* to node j can be expressed as:

$$Trust_i(\mathrm{j})^l = \alpha \times Trust\_Direct_i(j)^{(l)} + \beta \times Trust\_Indirect_i(j)^l + \gamma \times Trust\_Intrinsic(j) \quad (1)$$

Among it, $\alpha+\beta+\gamma=1, \alpha>0, \beta>0, \gamma>0$. α , α , β , γ represent weight parameters of direct trust, indirect trust and the intrinsic trust respectively, they are related to the specific network security policy. As shown in formula(1), $Trust\_Direct_i(j)^{(l)}$, $Trust\_Indirect_i(j)^l$ and $Trust\_Intrinsic(j)$ represents the direct trust value, the indirect trust value and the intrinsic trust value of node j to node i respectively. In this model, $0 \le Trust_i(j) \le 1$, the higher the trust value is, the more reliable the node is. Choose [0,1] as a trust interval, rather than simply use the binary number 1 and 0 for trusted and untrusted, the main reason is the value of continuous interval on a certain performance measurement uncertainty aspects ability is better than the discrete values.

The calculation of direct trust value can be expressed as:

$$Trust\_Direct_i(j)^{(l)} = \zeta \times Trust\_Direct_i(j)^{(l-1)} + LocalMS_i(j)^l \tag{2}$$

Among it, $\zeta > 0$ is exponential decay time factor. $Trust\_Direct_i(j)^{(l-1)}$ denotes the direct trust value of node i to node j according to the historical behavior of node j. $LocalMS_i(j)^l$ denotes the trust evaluation of node i to node j for node j's current behavior by the local management system. Parameters ζ can be expressed as:

$$\zeta = e^{-\rho \times (t_c - t_{c-1})} \tag{3}$$

Among it, $t_c > t_{c-1} \ge 0, \rho > 0$. t_c represents the time point of the current trust calculation, t_{c-1} represents the last time when the trust calculation was completed. According to the formula (2) and (3), the historical trust value of the node will gradually decrease over time. Specific values ζ need to be determined based on context.

In the process of trust calculation, $LocalMS_i(j)^l$ can be further expressed as:

$$LocalMS_i(j)^l = \begin{cases} P_j(a), & for\ 0 < P_j(a) < 1 \\ N_j(a), & for\ -1 < N_j(a) < 0 \end{cases} \tag{4}$$

Among it, $P_j(a)$ and $N_j(a)$ respectively represent positive and negative comments for node j current behavior a by the local management system. In order to follow the design principle that "good reputation" is more difficult to obtain than "bad reputation", the absolute value of negative evaluation should always be greater than the absolute value of positive evaluation.

The indirect trust value of the node can be calculated by using the direct trust data between nodes and the trust chain relationship. The formula of indirect trust calculation can be expressed as:

$$\begin{aligned} Trust\_Indirect_i(j)^l &= \frac{\sum_{m \in C_j, m \ne i} Trust\_Direct_i(j)^{(l)}}{|C_j| - 1} \\ &= \frac{\sum_{m \in C_j, m \ne i} (Trust\_Direct_i(m)^{(l)} + Trust\_Intrinsic(\mathrm{m})) \times N_{\mathrm{m}} \times Trust\_Direct_m(\mathrm{j})^{(l)}}{|C_j| - 1} \end{aligned} \tag{5}$$

In the indirect trust section, C_j represents the neighbor node set of the evaluated node j, $|C_j|$ indicates the number of the neighbor nodes collection; N_{m} indicates that the weight factor ratio of the trust value of different neighbor nodes m to node j, $\sum_{m \in C_j, m \ne i} N_{\mathrm{m}} = 1$. N_{m} is related to the cooperation of node m and node j.

In this scheme, in order to filter out the false recommendation trust data provided by the compromised node, node i evaluates the node j by using the local management system, which is expressed as:

$$E_i(j)=\frac{\sum_{m\in C_j,m\neq i} Trust\_Direct_i(m)^{(l)}\times N_{\mathrm{m}}\times Trust\_Direct_m(\mathrm{j})^{(l)}+Trust\_Direct_i(j)^{(l)}}{\sum_{m\in C_j,m\neq i} Trust\_Direct_i(m)^{(l)}+1} \tag{6}$$

TCMSII uses threshold ε in each trust evaluation process to evaluate the recommended trust data. If $|Trust\_Direct_m(\mathrm{j})^{(l)}-E_i(j)|>\varepsilon$, it indicates that the recommended trust data may be affected by malicious attacks, it should be discarded.

The calculation formula of the intrinsic trust can be expressed as:

$$T_I(j)=\left\lfloor Lc\delta_1\delta_2\frac{\sum_{i=1}^{m} r\sigma_i}{m}\right\rfloor \tag{7}$$

Among it, L represents the total number of integrity levels. $c\delta_1$ and $c\delta_2$ respectively represents the integrity of the underlying hardware SNP of the perceived node j, the integrity of the perceived OS, $r\sigma_1, r\sigma_2 .....r\sigma_m$ is the sequence of perceived application integrity for the current operation.

Simulation Results and Analysis

The Trust Value Varies with the Number of Transactions. In the simulation experiment, each domain has four types of nodes, and the initial trust value is 0.4. The trust value of these entity nodes changes with the creating number of transactions between each other, as shown in Fig. 2.

As can be seen from Fig. 2, the confidence of absolute trust node and general trust node is increasing with the increase of transaction numbers; the trust of the critical trust node is in a wave shape; the trust of the impossible trust node decreases. TCMDII is a good reflection of the change in trust of node entity with the number of transactions, which is in line with the expected analysis.

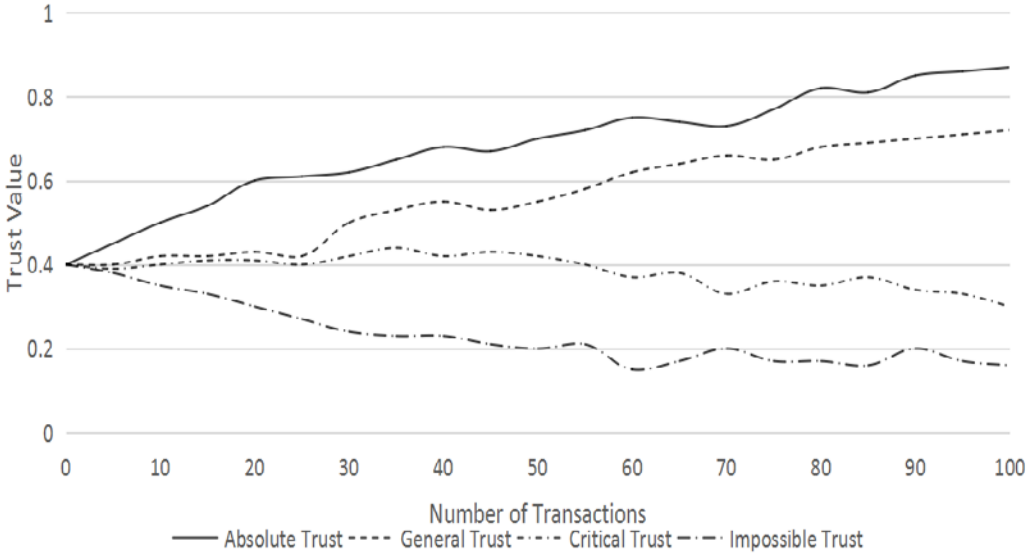

Fig. 2 The Change Figure of Node Trust Value with Increase of Transaction Number

Comparison of Trust Calculation Cost. The trust calculation cost mainly includes the request information of the trust subject, the recommendation information of the recommender and the information needed to find the trust calculation. The simulation experiment shows that, under different network nodes, the successful download rate of the general trust node is up to 90%, and the simulation results of the trust calculation cost of the three trust models are shown in Fig. 3.

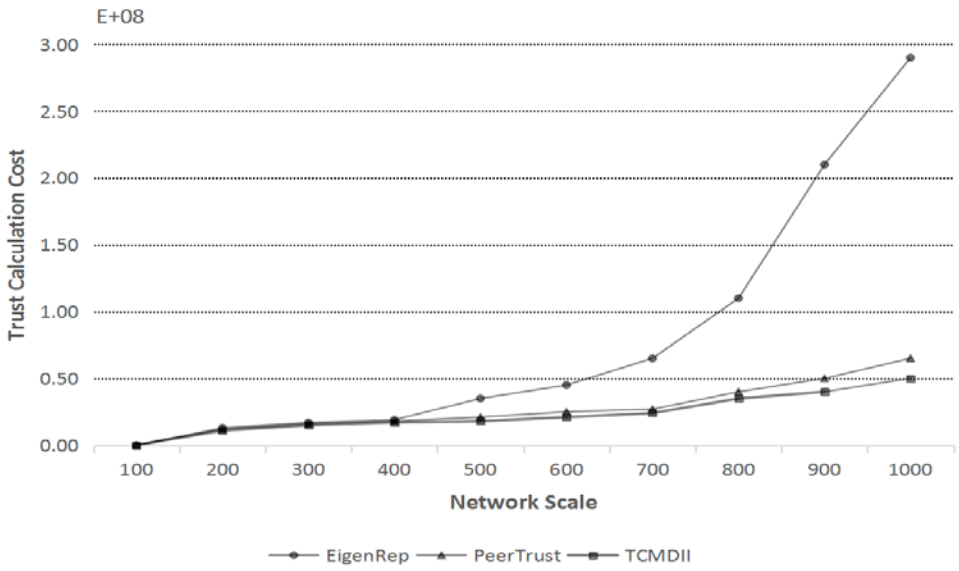

Fig. 3 Comparison of Trust Calculation Cost

As can be seen from Fig. 3, the trust calculation cost of the three models is very different, and the trust calculation cost of the EigenRep model is the largest, and the PeerTrust model is second, and the TCMDII cost proposed in this paper is the smallest. This TCMDII model nodes according to the degree of trust can be divided into four categories, reputation and trust less than the minimum threshold of node does not engage in transactions in the network. At the same time, using the theory of "broad space" makes the average trust path length is reduced, and introducing of trust merging method based on weighted tightness, make transactions through the least hop counts, trusted calculation cost minimum.

Comparison of Transaction Success Rate. The goal of TCMDII is to ensure that the trusted subject finds the trusted node as the trust object and successfully trades with it under the low trust calculation cost. Transaction success rate of trust subject and trust object is an important index of model. There are two types of attacks on malicious nodes: fraudulent transactions and malicious recommendations. Fig. 4 shows the comparison of the transaction success rate of the three models when the malicious nodes exist in different proportions.

In the simulation, assume that the absolute trust node provides a trusted file at 100% scale. The TCMDII, EigenRep, and PeerTrust model were selected with an 80% proportion of absolute trust nodes. It can be seen from Fig. 4 that when the proportion of malicious nodes in the model is 0, the transaction success rate can reach 90%. Along with the increase of the proportion of malicious nodes EigenRep model transaction success rate significantly decreased, when 50% of malicious nodes in the model, EigenRep model of transaction success rate fell to 55%. The transaction success rate of PeerTrust model is similar with TCMDII model in the situation with a small proportion of malicious nodes. TCMDII considers the reputation attributes of trust object in the trust network, trust transmission attenuation, trust decay with time, the weight of different trust levels in the trust path. A trust merge based on weighted closeness not only considers the number of trust paths and the number of hop counts in each trust path, but also considers the switching problem of trust source. TCMDII also penalizes nodes for deceptive trading and malicious recommendations, realizing the suppression of malicious nodes. Compared to the other two models, TCMDII can be more effective in suppressing deceptive transactions and malicious recommendations. In the case of 50% malicious nodes in the simulation experiment, the transaction success rate of the trust object and the trust subject selected in TCMDII can still reach about 75%, and the experimental results confirm the feasibility and effectiveness of TCMDII.

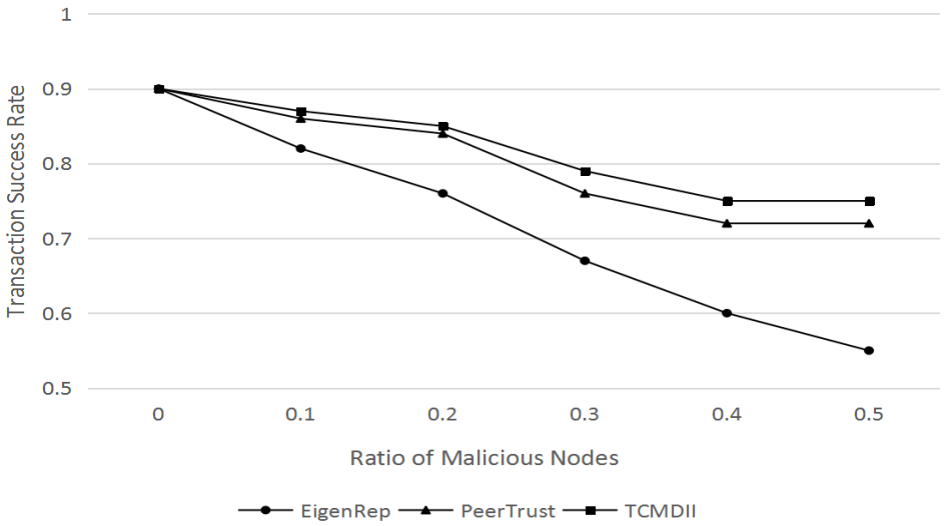

Fig. 4 Comparison of Transaction Success Rate

Conclusion

This paper puts forward a flexible, reliable, safe and universal IoT WSN trust computing mechanism. Analyzing the basic characteristics of WSN trust measurement and the design principle of trust computing model, synthetically considering direct trust, indirect trust and intrinsic trust, this paper proposes a low complexity and high reliability IoT WSN trust computation mechanism. For the problem which traditional calculation method consider without resource constraints, this paper proposes a lightweight TCMDII trust computation model with low complexity and just storing local trust information in evaluation node so that greatly reduce node resources loss. However, IoT WSN trust management related technology research is burgeoning and the future development has a long way to go. We can only make efforts to innovation, constantly invent and conquer new technical challenges in learning and referring on the basis of predecessors' research achievements in order to make WSN trust management mechanism in all kinds of network communication and application show greater value.

Reference

[1] J. 'Yick, b. Miikheijee and d. Ghosal. A ^ reless sensor network survey, Computer networks, 52 (12) : 2292-2330. 2008.

[2] I. Akyildiz, w. Su, y. Sankarasubramaniam and e. Cayirci. A survey on sensor networks. IEEE Communications magazine,40(8): 102-114,2002.

[3] J. Huang, L Uao and y. Chung. The Shielding wireless sensor network using Markovian intrusion Detection system with attack pattern milling. Information Sciences,231:32-44, 2013.

[4] H. Xia, Z. Jia, x. Li, etc. Trust prediction and Trust -based source routing in mobile AD hoc networks. AD hoc networks, 11(7):2096-2114, 2013.

[5] a. Menezes, R Oorschot and s. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.