Research on Distributed Trust Management in IoT

Ying Wang, Dongfeng Wang, and Fengyin Li(✉)

School of Computer Science, Qufu Normal University, Rizhao 276826, China
Lfyin318@126.com

Abstract. Widely used Internet of Things (IoT) has led to close cooperation between electronic devices. It requires strong reliability and trustworthiness of the devices involved in the communication. However, current trust mechanisms have the following issues: (1) Heavily relying on a trusted third party, which may incur severe security issues if it is corrupted. (2) Malicious evaluations on the involved devices may bias the trustrank of the devices. By introducing the concept of risk management into the trust mechanism, we propose a trust mechanism for distributed IoT devices in this paper. In the proposed trust mechanism, trustrank is quantified by normative trust and risk measures. Performance analysis shows that the proposed trust mechanism has a higher probability of high trust device being selected and higher success rate of cooperation.

Keywords: Internet of Things · Trust management · Normative trust · Risk

1 Introduction

In recent years, IoT has been widely implemented. It is estimated that by 2025, the number of global IoT connections will reach 25.1 billion, and the market size will exceed 10 trillion Chinese yuan. Emerging technologies such as data mining, artificial intelligence and natural language processing are also increasingly being extended to IoT applications [1–3]. Therefore, the need for cooperation between IoT devices has been significantly increased [4]. However, the performance of IoT devices in the process of cooperation is uncertain. How to measure the performance of devices through trust data, so as to understand the recent performance of IoT devices, has become the focus of recent research.

An IoT device is expected to cooperate with the devices of high reliability. It is necessary to ensure not only the performance of the other devices, but also the trustworthiness of them, which is the criterion to examine the reliability of the devices before cooperation [5,6]. Because existing trust mechanisms heavily rely on the trusted third parties or additional trust assumptions, there are hidden security risks such as malicious modifications to the trusted data [7]. Moreover, most distributed trust systems have not considered the malicious evaluation on the IoT devices. Saied et al. proposed a trust management method using

L. Qi et al. (Eds.): CloudComp 2020, LNICST 363, pp. 111–119, 2021.
https://doi.org/10.1007/978-3-030-69992-5_9

environment-awareness [8]. From nodes' historical behaviors in different cooperation types, they obtained a comprehensive trustrank to handle any new task, but this process relies on a reliable trust management institution. By caching previous interaction summaries, Liu et al. proposed a verifiable method to solve the hierarchical trust problem of IoT systems [9], but this method needs to establish additional trusted third parties over different domains. Benkerrou et al. proposed an IoT trust evaluation method based on trust and honesty [10], but they assume that all master nodes in the domain are completely trusted. Based on blockchain technologies, Ren et al. proposed a trust management method suitable for distributed Internet of Things, but they did not consider the irresponsible malicious evaluation problems between malicious devices [11].

By introducing the theory of risk into trust management, we propose a trust management method for distributed IoT. The new mechanism does not rely on any trusted third party, and the process of trust establishment and management are entirely independent maintained by each IoT domain manager. The main contributions of our method are as follows:

Aiming at the problem of dependence on trusted third-party, an IoT trust mechanism based on normative trust and risk trust is proposed. This trust mechanism does not depend on any trusted third party, and all trust establishments and trust managements are completely managed and maintained by IoT domain managers and IoT devices.

2 Trust Management Model in Distributed Internet of Things

2.1 The Structure of System

According to the distributed IoT environment, we here design a decentralized distributed IoT architecture (as shown in Fig. 1). There are many different IoTs in the real environment, and each IoT has a management domain. Each management domain consists of a domain manager and all subordinate IoT devices. The domain manager manages all the IoT devices in the domain. IoT devices can communicate and cooperate with others in any management domain. Domain managers can collaborate with others on the exchanging data.

For each cooperation between domain managers and devices, a two-way evaluation is conducted based on the other party's performance. The gist for evaluation includes the device's communication success rate, data processing capability, transmission range, and network stability. The device can be evaluated based on the other party's overall performance. The communication success rate between the devices is considered as the main indicator of the devices' performance in this paper.

The architecture of the Internet of Things is generally divided into three layer: a perception layer, a network layer, and an application layer. The perception layer includes some wireless sensors and other smart terminal devices with data processing capabilities. We denote wireless sensors with the devices $D(x_i, y_n)$,

and denote Smart terminal devices with the domain manager $H(x_i)$ in this paper. Data exchange and communication between the device and the domain manager are implemented via the network layer.

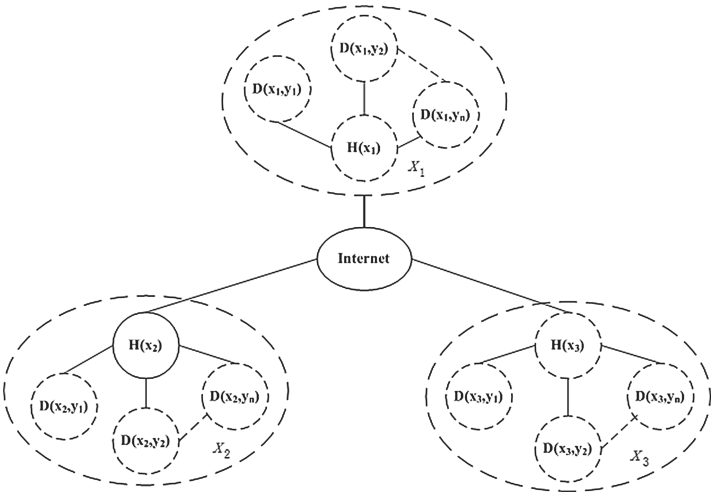

Fig. 1. Architecture of distributed IoT

In Fig. 1, x represents the IoT domain identifier, x_1, x_2, x_3 represent different IoT domain identifiers, $H(x)$ represents the domain manager of IoT domain x , $D(x, y_i)$ represents different IoT devices in the domain x, which is managed by $H(x)$, where $y_i \epsilon N^*(i = 1, 2, ..., n)$.

2.2 Trust Model

In order to describe the trustworthiness of IoT devices, this paper uses normative trust and risk measures to quantify trustrank. Normative trust defines the ability of a specific entity to earn credit by other entities, and the risk measure defines the stability level of a specific entity's credit performance in the past period. The concrete definition of the trust model is as follows.

Definition 1. Evaluation value
The evaluation value of $D(x_i, y_m)$ is denoted as $\delta(x_i, y_m, x_j, y_n, l)$, which refers to the evaluation of a given IoT device $D(x_i, y_m)$ by another IoT device $D(x_j, y_n)$. It is defined as follows.

$$\delta(x_i, y_m, x_j, y_n, l) = \begin{cases} 1 & Good\ performance \\ 0 & Ordinary\ performance \\ -1 & Poor\ performance \end{cases} \tag{1}$$

Where l indicates the serial number of the evaluation currently received by $D\,(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the evaluation value represents the evaluation value of $H(x_i)$, which refers to the evaluation of a domain manager $H(x_i)$ by another domain manager $H(x_i)$.

Definition 2. Trust scale
When receiving the kth evaluation, the trust scale of $D(x_i, y_m)$ is denoted as $TC(x_i, y_m, k)$, and it is iterated according to the evaluate value $\delta(x_i, y_m, x_j, y_n, l)$ given by other evaluators. It is defined as follows.

$$TC(x_i, y_m, k) = I + \sum_{i=1}^{k-1} \delta(x_i, y_m, x_j, y_n, l) \tag{2}$$

Where I is a trust initial value (we suppose $I = 50$ in our experiments for simplicity), $k \epsilon N^*$ represents the maximum serial number of the current evaluation received by $D(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the trust scale represents the trust scale of a domain manager $H(x_i)$, and it is iterated according to its evaluation value given by another domain manager $H(x_i)$.

Definition 3. Normative trustrank
The normative trustrank of $D(x_i, y_m)$ is denoted as $NT(x_i, y_m, k)$, which represents the standardized trustrank of device $D(x_i, y_m)$. It is defined as follows.

$$NT(x_i, y_m, k) = f(TC(x_i, y_m, k)) = \frac{1}{1 + e^{(-TC(x_i, y_m, k))}} \tag{3}$$

Where $x_i, x_j (i \neq j)$ represent different IoT domain identifiers, $y_i, y_j (i \neq j)$ represent different IoT devices and represents the $k \epsilon N^*$ maximum serial number of the current evaluations received by $D(x_i, y_m)$.

If the device numbers y_m and y_n are not given here, the normative trustrank represents the normative trustrank of a domain manager $H(x_i)$.

Definition 4. The mean value
The mean value of the trust of $D(x_i, y_m)$ is denoted as $MT(x_i, y_m, k, r)$, which represents the average value of the latest r normative trust of $D(x_i, y_m)$. It is defined as follows.

$$MT(x_i, y_m, k, r) = f(TC(x_i, y_m, k)) = \frac{\sum_{k'=k-r+1}^{k} NT(x_i, y_m, k')}{r} \tag{4}$$

Where $k \epsilon N^*$ represents the maximum evaluation serial number received by $H(x_i)$, and $r \epsilon N^*$ represents the number of $CD(x_i, y_m, k')$ included in the risk assessment.

If the device numbers y_m and y_n are not given here, this value represents the mean value of a domain manager $H(x_i)$, which represents the average value of the latest r normative trust of $H(x_i)$.

Definition 5. Risk value
The risk value of $D(x_i, y_m)$ is denoted as $RV(x_i, y_m, k, r)$, which is used to measure the risk of the credit performance of $D(x_i, y_m)$ in the history. Up to the maximum evaluation serial number k , the most recent r normative trustranks are taken into consideration, and the risk measure of definition $D(x_i, y_m)$ is as follows.

$$RV(x_i, y_m, k, r) = \sqrt{\frac{\sum_{k'=k-r+1}^{k} [NT(x_i, y_m, k') - MT(x_i, y_m, k, r)]^2}{r}} \tag{5}$$

Where $k \epsilon N^*$ represents the maximum evaluation serial number received by $D(x_i, y_m)$, and $r \epsilon N^*$ represents the number of $NT(x_i, y_m, k^{'})$ included in the risk assessment.

If the device numbers y_m and y_n are not given here, this value represents the risk value of a domain manager $H(x_i)$, which is used to measure the risk of the credit performance of $H(x_i)$ in the past.

Definition 6. Harmonic trustrank
The harmonic trustrank of $D(x_i, y_m)$ is denoted as $HT(x_i, y_m, k, r)$, which is used to represent the comprehensive trust evaluation of $D(x_i, y_m)$. Considering the normative trustrank and risk measure of $D(x_i, y_m)$, we define $HT(x_i, y_m, k, r)$ as follows.

$$HT(x_i, y_m, k, r) = \frac{NT(x_i, y_m, k)}{1 + NT(x_i, y_m, k) \times RV(x_i, y_m, k, r)} \tag{6}$$

If the device numbers y_m and y_n are not given here, this value represents the harmonic trustrank of a domain manager $H(x_i)$, which is used to represent the comprehensive trust evaluation of $H(x_i)$.

The architecture of the trust management model is shown in Fig. 2.

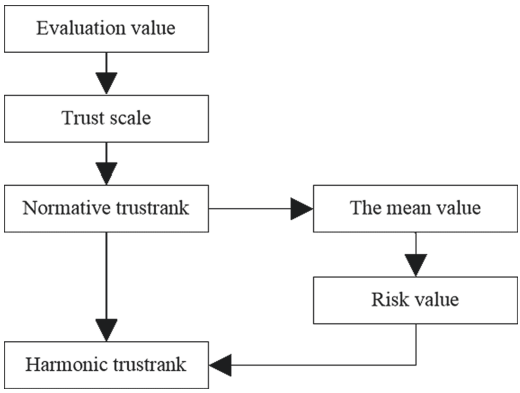

Fig. 2. Trust management model

3 Performance Evaluation

3.1 Trust Value Update

In order to test the effectiveness of the proposed scheme, simulation experiments are carried out to analyze the update rate of trustranks, the probability of the high trustrank equipment being selected and the success rate of the cooperation.

The experiment simulates three scenarios of the IoT domains and the corresponding IoT devices. The domain manager set is $H = \{H(x_1), H(x_2), H(x_3)\}$, including one malicious device and two benign devices. We used MATLAB to generate evaluation data for 50 device-to-device evaluations, simulating the trend of the trust data in the IoT trust model, the probability of high-trustrank devices being selected, and the success rate of cooperation between IoT devices. All the data are obtained by averaging the results of 10 iterations. The experimental results are shown in Figs. 3-7.

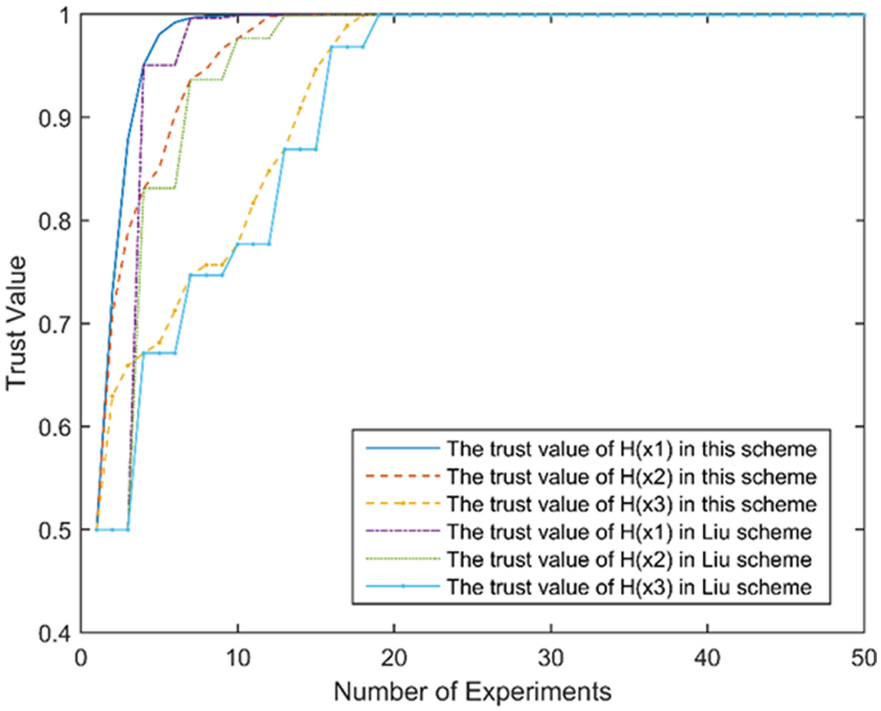

Fig. 3. Trend of trustranks of our scheme and Liu scheme.

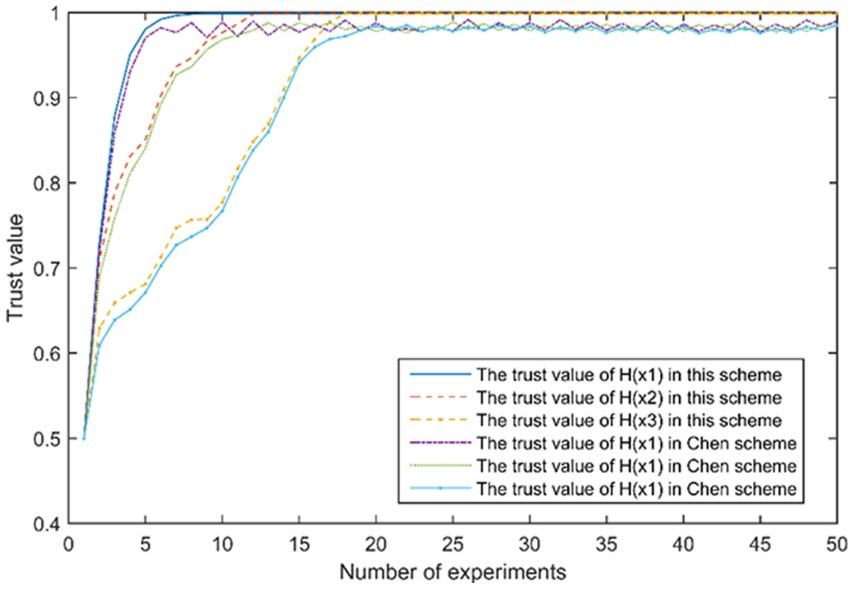

Fig. 4. Trend of trustranks of our scheme and Chen scheme

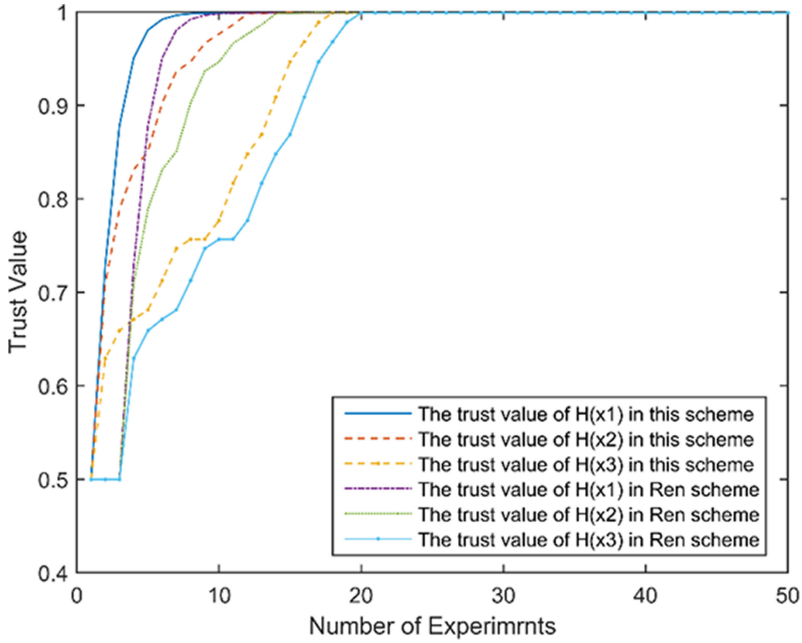

Fig. 5. Trend of trustranks of our scheme and Ren scheme

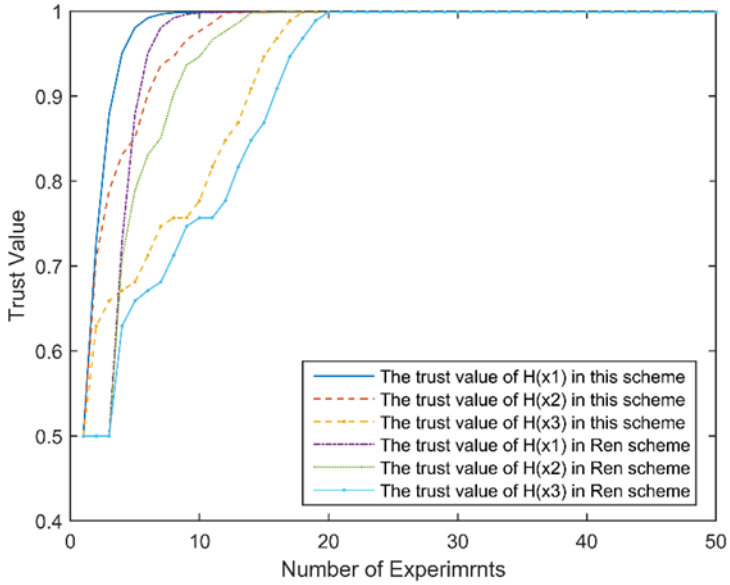

Fig. 6. Comparison of the probability of a high-trust device being selected

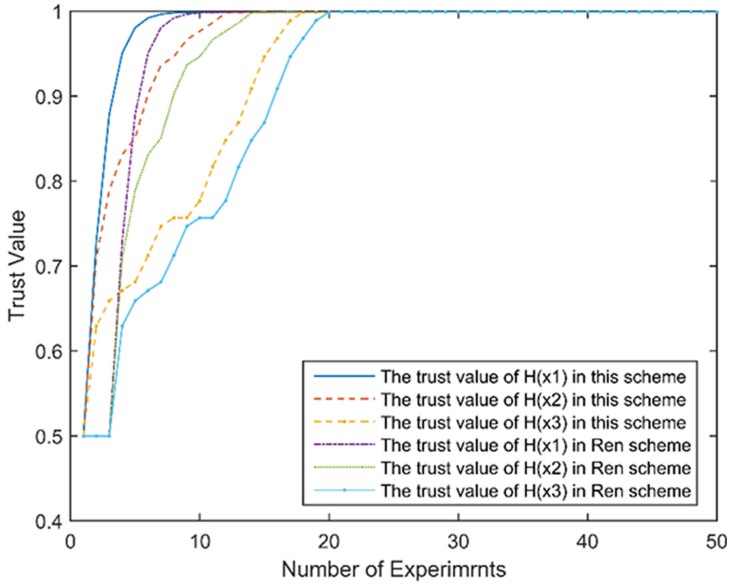

Fig. 7. Comparison of cooperation success rates between devices

4 Conclusion

To address the problems that a trust mechanism relies on the trusted third party or additional trust assumptions, and that the trust data is vulnerable to malicious attacks currently, in this paper, we quantified trust into normative trust and risk measure, which can construct a comprehensive review of normative trust, and we proposed a trust mechanism for distributed IoT, which realizes the identification and shielding of malicious evaluations between IoT devices, and can select the device that performs well and stable. Then it performs well in improving the success rate and reliability of cooperation on IoT devices. However, the mechanism in this paper has the problem of malicious evaluation on devices, and in this paper, how to work out this problem is the focus of the future work.

References

1. Yu, X., Wang, H., Zheng, X., Wang, Y.: Effective algorithms for vertical mining probabilistic frequent patterns in uncertain mobile environments. Int. J. Ad Hoc Ubiquit. Comput. **23**(3/4), 137 (2016)
2. Zheng, X., Hong, L.: A scalable coevolutionary multi-objective particle swarm optimizer. Int. J. Comput. Intell. Syst. **3**(5), 590–600 (2010)
3. Yu, X.-M., Feng, W.-Z., Wang, H., Chu, Q., Chen, Q.: An attention mechanism and multi-granularity-based Bi-LSTM model for Chinese Q&A system. Soft Comput. **24**(8), 5831–5845 (2019). https://doi.org/10.1007/s00500-019-04367-8
4. Wang, J.: Study of quantitative trust management model for the internet of things. Network Security Technology and Application (2014)
5. Feng, Y., Liu, Y., Gong, Y.: Trust system based on node behavior detection in internet of things. J. Commun. **35**(5), 8–15 (2014)
6. Li, X.: Design and analysis of revisable reputation evaluation system based on blockchain. Xi'an University of Electronic Science and Technology (2018)
7. Gu, L., Wang, J., Sun, B.: Trust management mechanism for internet of things. Chin. Commun. **11**(2), 148–156 (2014)
8. Saied, Y.B., Olivereau, A., Zeghlache, D., Laurent, M.: Trust management system design for the internet of things: a context-aware and multi- service approach. Comput. Secur. **39**, 351–365 (2013)
9. Liu, W.M., Yin, L.H., Fang, B.X., Zhang, H.L.: A hierarchical trust model for the internet of things. Chin. J. Comput. **35**(5), 846–855 (2012)
10. Benkerrou, H., Heddad, S.: Credit and honesty-based trust assessment for hierarchical collaborative IOT systems, pp. 295–299. IEEE (2017)
11. Ren, Y., Li, X., Liu, H., Cheng, Q., Ma, J.: Blockchain-based trust management framework for distributed internet of things. J. Comput. Res. Dev. **55**(7), 1462 (2018)