Construction of Internet of things trusted group based on multidimensional attribute trust model

Jinghan Chen, Bei Gong, Yubo Wang and Yu Zhang

Abstract
Accurate prediction of the trust relationship is the basis for trusted access and secure interaction between Internet of things nodes. To evaluate the degree of trust, a trust metric is assigned to every node depending on its several attributes. Normal nodes in Internet of things tend to suffer collusion attacks from malicious nodes; thus, the accuracy of the trust measurement decreases. To enhance the security of interaction between massive Internet of things nodes, we propose a multidimensional attribute trust model and a dynamic maintenance mechanism of a trusted group. The proposed model provides a reference for the selection and evaluation of node multidimensional attribute factors to adapt to different Internet of things application scenarios. The dispersion of satisfaction records is used to discover abnormal data and weaken its influence on the calculation of the node’s comprehensive trust evaluation. The construction of trusted groups provides an architectural foundation for the application of group signature that maintains low network overhead. The performance of multidimensional attribute trust model and dynamic maintenance mechanism is verified using Netlogo. Simulation results show the efficiency of the proposed model to classify the malicious nodes and honest nodes, as well as to build a trusted group that could ensure honest nodes occupy the major proportion.

Keywords
Internet of things, trusted group, trust evaluation, multidimensional attribute, feedback control

Date received: 15 June 2020; accepted: 5 January 2021

Handling Editor: Peio Lopez Iturri

Introduction
IoT (Internet of things) consists of multiple information sensors. These entities interact with others to implement intelligent perception, recognition, and management of objects and process through various network access. It covers scenes in Smart Cyber-Physical Systems that require high connection density such as Smart Transportation, Smart City, Smart Grid, etc. IoT meets people’s needs for digital society and will further open the era of “Internet of Everything.”

Security is one of the main concerns in IoT. The IoT contains terminal devices that have strict requirements on network delay. These devices are related to personal safety, such as a wearable sphygmomanometer connected to the hospital. Attacks on IoT will endanger the personal safety and cause serious consequences. The focus of relevant research about security is mainly divided into two aspects: privacy preservation mechanism and trust evaluation scheme. For the former, scholars have proposed algorithms to conceal the physical status while maintaining a low resource consumption. As for the latter, an efficient and comprehensive interaction mechanism for trusted access of IoT nodes needs to be considered in a targeted manner.
Trusted access depends on an accurate prediction of the trust relationship. Researchers in related fields use different trust metric approaches to quantify the degree of trust between nodes as trust value. Trust value is mainly calculated with either direct or indirect evaluation. Behavioral attributes and weighting factors are considered to ensure the robustness of the trust computing process. Realistic application scenarios require to shorten the recommended trust chain and reduce the cost of trust assessment, and then enable efficient determination of node properties and interactive decision as well.

Trust model can be divided into two types of architectures: centralized and distributed frameworks. The centralized trust model delegated a central node to calculate trust value and manage other nodes. For the distributed trust model, each node completes the trust evaluation of other entities independently. Each node can be both a truster and a trustee. Considering the actual application situation, the trust model is required to minimize the operator’s security management costs and improve access efficiency. However, the evaluation factors of traditional trust models are less considered. Their limitations are greater and result in a greatly reduced practicality. A security strategy that provides corresponding security protection under low latency constraints and has less impact on its performance is required. Therefore, massive IoT nodes require more efficient, fine-grained, and reliable trust modeling. This has become a huge challenge for the security of trust access in IoT.

This article focuses on the multiple environments of IoT and proposes a fine-grained trust model. Also, we comprehensively consider the impact of malicious node attacks and camouflage behavior and the occasional abnormal behavior of normal nodes. The proposed trust model implements efficient prediction as well as interactive decision and management of trust relationships between entities.

There is a contradiction between network security performance and network energy consumption, and the computing and storage capabilities of nodes are limited. The approach to finding a balance between security and energy consumption to ensure the coexistence of performance advantages and security of the IoT requires further research. Considering that certain nodes among the massive IoT nodes of the same nature belong to a group and the group restricts individuals, it is possible to formulate individual trust evaluation rules by introducing group trust specifications. This method of constructing trust groups could also provide new ideas for fast and reliable access between massive IoT nodes. The main contributions of this article are as follows:

- We propose a multidimensional attribute factor selection and evaluation method to provide a more comprehensive reference for trust evaluation. Then we adopt the dispersion-based anomaly metric identification method to weaken the impact of the attack on the comprehensive credibility calculation and improve the success rate of node interaction.
- We propose a multidimensional attribute trust model (MATM) that combines centralized and distributed trust management to accurately measure the credibility of nodes.
- We provide a feasible trustworthy division scheme for massive IoT nodes. Through building a trustworthy group, we could reduce the cost of security verification. We also propose a dynamic maintenance mechanism (DMM) for trusted groups to further ensure reliability and effectiveness.

The rest of the article is organized as follows. Section “Related work” presents some existing related works. Section “Proposed trust model” details the proposed Trust Model. Section “Trusted group” shows the steps to build and maintain a trusted group. In section “Simulated results,” simulation results evaluate the performance of our trustworthy division scheme. The conclusion is given in section “Conclusion.”.

Related work

In this section, we review the existing trust models and observe their limitations and advantages. Trust is a concept derived from human sociology. In recent years, researchers in related research fields have given a variety of trust cognition modeling methods. Mike et al. correlated trust with risks and threats and established a direct link between trust and risk through trust research in multiple contexts.

Researchers built the trust model through their trust cognition and quantification; thus, the models reflected a different performance. Xie and Wei proposed a node dynamic trust evaluation method (IDTEM) for the IoT, characterized node behavior, and suppressed malicious recommendations. But IDTEM requires a detailed distinction between the cooperation modes of devices in specific application scenarios and has poor versatility. Ye et al. expressed the trust relationship between workers and requesters by constructing a crowdsourcing trust network CTN and analyzing threat patterns in the trust vector Worker Trust Vector (WTV) as a global trust score. Hu et al. added the core behavior to describe the behavior characteristics of the entity, and the risk evaluation factor is added during the calculation process, but the semantic model large-scale distributed system trust model (LSDM) proposed in the article does not completely cover the
concept of the trust model and gradually falls as the number of nodes increases. Pawar et al.\textsuperscript{11} proposed a reputation mechanism for computing cloud service providers, and trust uncertainty is more accurately described based on evidence.

The trust model is designed to complete the framework of trust evaluation. The trust model aims to solve internal attacks and to identify the malicious nodes and improve the reliability of the system. The focus of the research is the approach to improve the trust model on their performance. Based on the model responsible for trust computing and management tasks, the trust model is classified into centralized and distributed. We are going to discuss the limitations and advantages of both.

**Centralized trust model**

The centralized trust model includes a reputation center (certification center/trust center). Niu et al.\textsuperscript{12} proposed a trust model based on the cloud model which unifies the randomness and uncertainty of the trust description and can efficiently carry out trust propagation and merge operations, but the trust cloud synthesis algorithm among them has high computational complexity and low scalability. Mohsenzadeh et al.\textsuperscript{13} proposed a trust model based on fuzzy mathematics according to the success and failure interactions between cloud entities based on trust attributes and semantics. This model has a certain capability of collaborative deception identification and tolerance, but the accuracy of discrimination between honest and malicious entities is relatively low. As an extension of cloud computing, fog computing is considered to be a relatively more secure and efficient environment. Therefore, scholars have designed new trust evaluation scheme for the fog computing environment. Al-khafajiy et al.\textsuperscript{14} proposed a fog COMPUTERing Trust management (COMITMENT) approach to manage the trust level of nodes in fog computing environment, and the approach were able to reduce the malicious attacks.

At present, there are few studies on the centralized trust model, mainly due to its two serious shortcomings:

- **Poor scalability**: Centralized trust assessment requires an authentication mechanism that causes huge overhead and results in a decrease in performance.
- **Single point of failure**: The idea of the centralized trust model is concise, but it depends too much on the reliability and efficiency of the reputation center.

**Distributed trust model**

A distributed network is a robust mesh network composed of nodes distributed in different locations. Compared with a centralized network, it can effectively avoid single-point failures of important nodes.

Li et al.\textsuperscript{15} proposed an opportunistic network safe routing decision method based on trust mechanism, which relies on message carrying to realize the collection of evidence chain and uses trust vectors with signatures and timestamps to effectively feed back the trust degree of nodes. Wu et al.\textsuperscript{16} proposed a blockchain-based peer-to-peer (P2P) network trust model. The weight of the indirect trust degree is determined according to the reliability of the indirect trust degree of the evaluation node in the network. It has high flexibility and universality, but the model granularity is relatively coarse. You et al.\textsuperscript{17} revised the reliability of the recommended node based on the interaction satisfaction feedback, but its evaluation process relies heavily on local storage and cannot be effectively applied to scenarios where there is no local storage such as cross-domain and strange node interaction.

The trust model has multiple application scenarios. Ma and Li\textsuperscript{18} proposed an edge node credibility evaluation model based on integrated trust. This model can realize efficient edge calculation based on integrated trust and effectively process the massive data generated by network edge devices, but it lacks an accurate trust calculation process. Hasrouny et al.\textsuperscript{19} proposed a hybrid trust model (HTM) and a malicious behavior detection system (MDS). Based on vehicle behavior, trust measurement can effectively distinguish between malicious vehicles and honest vehicles, but this model is only applicable to VANET and is difficult to transplant. Jiang et al.\textsuperscript{20} proposed a trust model for distributed wireless sensor networks. In the calculation process of direct trust, various factors such as communication trust, energy trust, and data trust are considered to define trust reliability and familiarity. However, the model’s weight judgment on direct trust and recommended trust has certain limitations.

Moreover, there are several improvement methods to the existing trust model. The EigenTrust model\textsuperscript{21} is optimized using evolutionary game theory to model peer entities, and trading behaviors more accurately reflect the actual situation. Cho and Chen\textsuperscript{22} proposed a data-driven method used to reduce the resource consumption when selfish or malicious nodes exist. And the proposed trust framework is evaluated using random Petri nets, which makes the framework achieve a better node trust assessment accuracy and can be effectively used in delay-tolerant networks. Wang and Liu\textsuperscript{23} proposed a Bayesian modeling method aimed at the online detection of fault-
tolerant dynamic event areas in wireless sensor networks. The concepts of virtual community and trust index can be used as a reference for the construction of trusted groups in this article. Tariq et al.24 proposed an energy-efficient, software-defined-network-based Mobile Code-driven Trust Mechanism (MCTM) in order to solve the trust evaluation problems on Software-Defined Network (SDN) for SNs.

As the trust model continues to evolve, more factors are considered in the trust evaluation. This finally constitutes a trust framework with a mixture of multiple mechanisms. GeTrust25 is a P2P network trust model based on guarantee; the service node selects the guarantee node and provides reputation mortgage for the service. It combines the incentive mechanism and anonymous reputation management strategy and effectively improves the transaction success rate. Jayasinghe et al.26 proposed an effective modular hybrid trust framework, establishing trust based on entity reputation. Truong et al.27 used third-party opinions, experience, and direct observation as three trust indicators. It can clarify the concept of trust in the social IoT ecosystem and establish a reliable social network between the entities based on the owner, but it lacks practicality.

Table 1 shows the comparison between different trust models in related works and the properties of our proposed model.

Research on IoT is mainly focused on the development of communication transmission technology or trust modeling of specific networks and lacks trust models designed for the access characteristics of massive IoT nodes. The consideration of the attributes, factors, and weights that affect trust is incomplete. Hence, trust evaluation, trust management, social community construction, and feedback control are integrated to realize a comprehensive consideration and evaluation of trust. Based on the trust value calculation and with the concept of the trusted group, there is a flexible approach to finish the dynamic trust evaluation of massive IoT nodes. The approach should fasten the ability of trusted access and real-time autonomous feedback, which also provides new ideas for the research on the security solutions of massive IoT nodes. This will help to promote the stable operation of IoT and have important theoretical and practical significance for the development of IoT applications.

Proposed trust model

In this article, we propose an MATM to cover various IoT scenes and enhance the reliability of trust evaluation results. The description of related notations is shown in Table 2.

Direct trust value

Suppose that $P_1, P_2, ..., P_N$ are IoT nodes that interact in the network environment. The direct trust value of the node is the quantitative value of the trust evaluation calculated by the subject node with reference to the interaction result; the latter is based on the aggregation of multidimensional trust evaluation factor.

Multidimensional trust evaluation factor selection. The multidimensional trust evaluation result set of an IoT node can be described as a triple

$$\Omega = (\Omega E, \Omega B, \Omega O)$$

Among them, $\Omega E$ is an $l$-dimensional trust evaluation based on the node computing environment, which can be described as follows

$$\Omega E = (E_{v_1}, E_{v_2}, ..., E_{v_l})$$

where $E_{v_i}$ reflects the trust level of the subject node based on the node computing environment to the object node. After the connection is established, suppose that the communication process between $P_i$ and $P_j$ is $com_1, com_2, ..., com_q (com_1, com_2, ..., com_q$ belongs to $P_i, com_{x+1}, com_{x+2}, ..., com_q$ belongs to $P_j$). The set of permissions required to complete the interaction $com_{x+1}, com_{x+2}, ..., com_q$ is $\{ps_{x+1}, ps_{x+2}, ..., ps_q\}$.
The access permission of external nodes to interact with the node $P_i$ is $pa$, and then the trust level of the communication process $Ev_c$ can be described as

$$Ev_c(i,j) = \frac{1}{q - x - 1} \sum_{i = x + 1}^{q} ps_i \land pa \quad (3)$$

Similarly, suppose that the access permission granted by the node $P_j$ from an external node process is $pb$, and the evaluation function of the two-dimensional trust level of the node is

$$Ev_c(i,j) = \begin{cases} Ev_c^{y} = \frac{1}{q - x - 1} \sum_{i = x + 1}^{q} ps_i \land pa \\ Ev_c^{y} = \frac{1}{x} \sum_{i = 1}^{x} ps_i \land pb \end{cases} \quad (4)$$

where $Ev_c^{y}$ and $Ev_c^{y}$ are the trust evaluation of $P_i$ to $P_j$ and $P_j$ to $P_i$.

Among the triples, $\Omega B$ is the $m$-dimensional trust evaluation based on node behavior, which can be described as

$$\Omega B = (Ev_{b_1}, Ev_{b_2}, ..., Ev_{b_m}) \quad (5)$$

The $m$-dimensional trust evaluation based on node behavior can include the following parameters:

- **Identity verification**: Whether the node has completed identity verification.
- **Data packet forwarding rate**: During the interaction, the terminal node $P_i$ requests $N$ data packets from the node $P_j$, and the node $P_j$ forwards $n$ ($n \leq N$) data packets. After receiving the data packet, the node $P_j$ evaluates the node’s behavior based on the data packet forwarding rate. The trust evaluation on the number of forwarded packets is proportional to the data packet forwarding amount.
- **Data packet repetition rate**: The data packet repetition rate is also an important reference indicator for judging whether the node’s behavior is abnormal. When the data packet repetition rate is low, the node tends to be credible, and its satisfaction in forwarding data packet repetition rate will increase as the repetition rate decreases. As the repetition rate gradually approaches and exceeds the threshold of the service’s tolerable repetition rate, the more likely the node to behave abnormally, the more likely it will be considered as a malicious node.
- **Packet content**: The behavior of a node is monitored by its neighbors, so the phenomenon observed by the monitoring node can be deduced, that is, whether the node has tampered with the contents of the data packet. If the node does take malicious actions and illegally steals or tampers with information, it should reduce its credibility accordingly.
- **Transmission delay**: The transmission delay should fluctuate within the minimum range allowed by the network architecture. If the transmission delay of the node $P_j$ forwarding data packets to the node $P_i$ is less than the critical value specified by the system, the trust evaluation of node $P_j$ in transmission delay is considered to be a fine level. As the transmission delay exceeds the threshold and continues to rise, the node $P_j$ tends to cause a malicious attack.
- **Residual energy**: Due to the resource limitation of the IoT node itself, the node may not be able to provide effective forwarding services because it has consumed all the energy. To avoid determining such normal nodes as malicious nodes, the impact of the remaining energy of the node on the ability to forward data packets should be considered. The node determines its remaining energy and records, as well as sends the node’s maximum energy and remaining energy to its neighbors. The influence of the remaining energy of the node will be quantified as the remaining energy influence factor.
Life cycle: The subject node collects the most recent moments of neighboring nodes joining and exiting the system. Also, it calculates the survival time of each neighbor and the trust quantification value of the target node’s lifetime.

The $n$-dimensional trust evaluation of other attributes in the triple is determined according to the actual application scenario and can be described as

$$\Omega O = (Ev^1_o, Ev^2_o, ..., Ev^n_o)$$

This can include the following:

- Activeness: Periodically calculate the number of messages received from a node according to system attributes. The number should be equal to 1. If the number of messages sent during this period is greater than 1, it is required to consider whether it is a malicious node attack (Denial of Service (DoS) or other). If the number of messages is 0, consider whether it is marked as an inactive node (denying service or leaving the transmission radius).
- Signal strength: Signal strength helps to determine the location of the node.
- Direction: The direction of node movement is used to judge the tendency of a node to enter or leave a group.
- The number of trusted neighbor nodes: The number of neighbor nodes whose global trust value has achieved a certain threshold within the transmission radius of the node.

In practical applications, considering the network overhead and node energy constraints, the above attribute factors should be selected for evaluation according to the specific preferences of the network.

**Interaction satisfaction calculation.** Interaction satisfaction refers to the evaluation made by the subject node according to the multidimensional attribute factors of the object node after interaction. According to the source of satisfaction data during trust calculation, it is divided into subjective service satisfaction and historical service satisfaction. Satisfaction value ranges from [0,1]. 0 means entirely dissatisfied and 1 means absolutely satisfied.

The interaction satisfaction of the terminal node $P_i$ with the terminal node $P_j$ is $S^{ij}_c$, and its calculation method is the weighted sum of the multidimensional trust evaluation results. Referring to the work of Bullen, the interaction satisfaction will be calculated as follows

$$S^{ij}_c = \left[ \prod_{k=1}^n w_k Ev^k_c \right]^{1/n}$$

Considering that the node has certain self-interest preferences, the evaluation value of each trust aspect has a different impact on the overall trust evaluation. The weight coefficient $w_i$ represents the interest preference level in the $k$th trust aspect. The weight coefficient is described as

$$w = (w_1, w_2, ..., w_l + m)$$

$$\sum_{k=1}^{l+m} w_k = 1$$

**History interaction satisfaction.** After the interaction satisfaction calculation is completed, the node will store the calculated interaction satisfaction and update the historical interaction satisfaction record vector, which is described as

$$S^{ij}_{hvec} = \left( \langle t_1, S^{ij}_c \rangle^{(1)}, \langle t_2, S^{ij}_c \rangle^{(2)},..., \langle t_n, S^{ij}_c \rangle^{(n)} \right)$$

where $t_n$ is the interactive service timestamp, and $S^{ij}_{hvec}$ is the subjective satisfaction record of the last interactive service in $t_m$.

According to the cognitive habits in human psychology, trust relationships are time-sensitive, and their credibility dynamically decays with time. In the locally stored historical trust record vector $S^{ij}_{hvec}$, the time weighting coefficient is defined as

$$w^* = (w^*_1, w^*_2, ..., w^*_n)$$

$$w^*_i = h(t - t_0) = h(i)$$

where $h(t - t_0)$ is the time decay function, $h(t) \in [0,1]$. The time decay function can give the trust metric reasonable weight coefficients at different time points. The interaction satisfaction obtained by the newly generated interaction behavior should reflect the trust status of the node more than the old interaction satisfaction, so the time decay function can be defined as

$$h(i) = \begin{cases} 
1 & i = n \\
\frac{1}{\left(h(i - 1) = h(i) - \frac{1}{n}\right)} & 1 \leq i \leq n 
\end{cases}$$

The historical trust value is derived from the historical satisfaction record vector $S^{ij}_{hvec}$

$$T^{ij}_h = \sum_{k=1}^{n} \frac{W^*_k}{\sum_{i=1}^{l+m} W^*_i} \times S^{ij}_c$$

**Direct trust value and dispersion.** The direct trust value represents the evaluation of the subject node’s credibility based on the interaction result with the object node,
generally based on the comprehensive consideration of the interaction satisfaction and historical interaction satisfaction. The node-to-node direct trust value is calculated by the following equation

$$T_{ij}^D = \gamma S_h^j + (1 - \gamma)T_h^j$$

(13)

where $\gamma$ is the weight coefficient of satisfaction for this interaction ($0.5 \leq \gamma \leq 1$). We determine the specific value according to the discrete degree of the interaction satisfaction and the historical interaction satisfaction or the actual network environment application requirements; it generally takes 0.5.

Nodes may provide unstable services. Therefore, after calculating the direct trust value, the dispersion direct trust value relative to historical interaction satisfaction should also be calculated. These are used as the trust evaluation made by the subject node for itself and as the reference of subsequent reward and punishment mechanism. Referring to the work of You et al.,17 the dispersion could be calculated as

$$\rho_{ij} = \frac{1}{\sqrt{\frac{1}{n-1} \sum_{k=1}^{n-1} (T_{ij}^{Dk} - T_{ij}^D)^2} + 1}$$

(14)

The structure of the database table where the principal node is stored locally is shown in Table 3:

| Node ID | Timestamp | Historical interaction satisfaction vector | Direct trust value | Dispersion |
|---------|-----------|--------------------------------------------|-------------------|------------|
| j       | t         | $S_h^j$                                     | $T_{ij}^D$        | $\rho_{ij}$|

Proof of trust. After the end of the trust evaluation calculation process, the subject node generates a trust certificate about the object node and broadcasts it to the neighbor nodes. The proof of trust is expressed as

$$T_{message} = (Id_i, Id_j, T_{ij}, D_{ij}, T_{ij}^D, \rho_{ij}, D_{ij})$$

(15)

Among them, $Id_i$ and $Id_j$ are the unique identity of node $i$ and node $j$, respectively. $T_{ij}$ is the timestamp generated for the proof of trust, $T_{ij}^D$ is the direct trust value, $\rho_{ij}$ is the evaluation of the reliability of the direct trust value by the subject node, and $D_{ij}$ is the digital signature information. Through verifying the digital signature, we can guarantee the authenticity of the trust certificate.

Recommend trust value

After the initialization is completed, the interaction between nodes needs to calculate the recommended trust value based on the direct trust value provided by the neighbors. At the same time, the dispersion of the recommended trust value is calculated to assign the weight of the direct trust value and the recommended trust value, and the interactive decision is made according to the result

$$T_{ij}^r = \frac{1}{N} \sum_{k=1}^{N} T_{ij}^{Dk}$$

(16)

Similarly, we calculate the dispersion of the recommended trust value to evaluate the reliability of the recommended trust value. Determine the proportion of the direct trust value and the recommended trust value in the comprehensive calculation

$$\rho_{ij} = \frac{1}{\sqrt{\frac{1}{n-1} \sum_{k=1}^{n-1} (T_{ij}^{Dk} - T_{ij}^D)^2} + 1}$$

(17)

Total trust value

The node’s total trust value is the judgment basis for the interactive decision between nodes, which is calculated by the following equation

$$T_{total} = \beta T_{ij}^D + (1 - \beta)T_{ij}^r$$

(18)

where

$$\beta = \frac{\rho_{ij}}{\rho_{ij} + \rho_{ij}}$$

(19)

The subject node comprehensively calculates the total trust value of the object node based on the interaction history record stored by itself and the recommended trust value sent by the neighbor nodes. This value determines whether to interact with the node.

Global trust value

We screen the feedback behavior of malicious nodes and collect the direct trust value data of other nodes to the target node. The global trust value of the node could be calculated as follows

$$T_{global} = \frac{1}{C} \sum_{c \in C} \frac{\rho_{cj}}{\sum_{k \in C} \rho_{kj}} \times T_{ij}^D$$

(20)

When the global trust value $T_{global}$ of the target node reaches the threshold $\theta_0$ of the trusted group, it is
marked as a trusted node and admitted to the trusted group. The nodes in the trusted group still need to update the feedback of the direct trust value based on the behavior of other nodes to correct the credibility of the node in real time.

This model introduces multidimensional attribute factors and evaluates trust by service satisfaction, dispersion of direct trust value, and total trust value of nodes based on users’ behaviors. These factors are used to fine-grain the trust measurement of nodes. This model is designed to improve the trust access efficiency of massive IoT nodes and the trusted group. This approach is able to adapt to dynamic network changes and make up for the limitations and deficiencies of the traditional trust model.

**Trusted group**

The trusted group in IoT is a collection of nodes that satisfy certain rules. The user nodes in the network can be regarded as the mapping of creatures in nature. Creatures with certain properties will form a group. In the community, the default rules regulate the behavior of the individual. The individual should not disturb the normal survival order of the community because of their own interests. Otherwise, they will be punished by the community or directly expelled from the community. Following this mode, the trusted group is built based on the result of trust modeling. Arbitrary operations are banned in the trusted group. User nodes are required to output under the constraints of the group. Once the trusted group builds, the group will use a DMM to ensure the credibility of group members.

The process of establishing a trusted group in this article could be summarized as follows:

1. Evaluates the node and calculates the direct trust value by calculating the service satisfaction based on the multidimensional attribute evaluation factor.
2. Collects the direct trust value of the neighboring node to calculate the global trust value of the node.
3. Follows the group access limitation and constraints on individual nodes and maintains the dynamic credibility of the entire group.

**Construction of a trusted group**

The node enters the system and obtains an initial trust value of 0.5 (i.e. it cannot be judged as trustworthy or untrustworthy). Every node that enters the system must try to become a member of a trusted group. When nodes \( a, b \) become neighbors, according to their credibility, it is verified by the system to form a trusted group within a certain transmission radius if their global trust value achieves the group threshold \( \theta \). Node \( a \) becomes the GL (Group Leader) of the group, and \( b \) becomes the candidate GL. Node \( a \) will be responsible for the management of other neighboring nodes joining the group. When the GL leaves the trusted group transmission radius or leaves the group for other reasons, the most trusted node in the group becomes the new GL and manages the group members.

Trust evaluation is the foundation for the establishment of a trusted group. As shown in Figure 1, nodes obtain feedback on their trust value through interaction. The trusted group initialization node collects trust data and calculates its total trust value to determine whether to allow a new member to join.

When there enters a new member, the initialization node gives its group signature key. When an old member in the group exits, the initialization node generates a new group public key and broadcasts it to the group members. The members of the group use the same group public key to verify the signature generated by any group member using the group signature key, reducing the verification delay and overhead while also ensuring anonymity.

The construction of the trusted group satisfies the needs of massive IoT nodes to reduce verification overhead. It provides new ideas for fast trusted access between massive nodes.

**DMM of the trusted group**

**Trust value decay mechanism.** When the target node does not have any activity within a certain time window \( \phi \) (including requesting, providing services, and giving feedback), its trust value decay factor is calculated periodically according to the time difference \( t - t' \). \( t \) is the current time and \( t' \) is the last activity time of the node. \( \kappa \) is a parameter to control the decay rate. The credibility attenuation factor is expressed as

\[

v_t = \begin{cases} 
0, & \text{if } t - t' > \phi \\
\frac{0}{C_1}, & \text{otherwise}
\end{cases}
\]

(21)

**Historical statistics based on node feedback behavior.** When the error of the recommended trust value feedback by the node is beyond the set threshold \( \xi \), the node’s feedback behavior is considered abnormal this time. Otherwise, the feedback behavior is considered normal.

We use the beta probability density function to represent the posterior probability of binary events

\[
h(\theta | \alpha, \beta) = \frac{\Gamma(\alpha + \beta + 2)}{\Gamma(\alpha + 1) + \Gamma(\beta + 1)} \cdot \theta^\alpha \cdot (1 - \theta)^\beta \]

(\( \theta \in [0, 1], \alpha \geq 0, \beta \geq 0 \))
where $\alpha$ and $\beta$ represent the number of occurrences of normal behavior and abnormal behavior, respectively. The mathematical expectation of the node’s historical behavior statistics (i.e. the probability of normal behavior in the future when feedback) is

$$E(h(\theta|\alpha, \beta)) = \frac{\alpha + 1}{\alpha + \beta + 2} \quad (23)$$

**Reward and punishment mechanism.** Let $\rho_{kj}$ as the dispersion between the trust value feed back from the current node and the trust value of other nodes. When $\rho_{kj}$ is within the tolerance threshold $\lambda$, it reveals that the feedback is a normal trust assessment, and then accept the direct trust value of its feedback. When $\rho_{kj} \in (\lambda, 1]$, it reveals that the deviation is too large. The evaluation value may be due to the exaggeration/defamation attack behavior of malicious nodes.

Effective feedback behavior is required to ensure that the dispersion of the trust value is within the tolerance threshold. Referring to the work of You et al., the punishment factor according to the specific conditions of its feedback could be calculated as follows

$$P_{ui} = p \times E(h(\theta|\alpha, \beta)) \times \rho_{kj} \quad (24)$$

where $p$ is the penalty control factor, and $E(h(\theta|\alpha, \beta))$ is the historical statistics based on node feedback behavior. If the effective proportion of the node’s historical recommendation behavior is high, then a mistake will not cause the node’s credibility to be greatly reduced. But if the percentage of invalid feedback becomes higher, it will be difficult for nodes to improve their credibility in future feedback behaviors. We calculate the dispersion of the feedback value after a certain interaction accumulation. The greater the dispersion $\rho_{kj}$, the greater the deviation from other users’ trust evaluation of the target node, and the reliability of the node itself will be affected accordingly.

When the direct trust value returned by the node is valid ($\rho_{kj} \in [0, \lambda]$), where $\lambda$ is the tolerance threshold), the credibility reward is given to this node, and the reward factor is calculated based on equation (25)

$$R_i = \frac{y^v}{q}, \quad v>1, q>1 \quad (25)$$

where $1/q$ is the reward parameter for trust; by adjusting the value of this parameter, we could control the influence of reward mechanism on trust value. $v$ is the base of the trust reward and $\tau$ is the safe operating cycle.
for nodes. We set the above three parameters according to the actual needs of the network application.

**DMM algorithm.** To ensure the real-time credibility of the group, the above-mentioned time decay mechanism and the reward/punishment mechanism constitute a dynamic maintenance mechanism of the trusted group. The DMM algorithm is as follows:

**Algorithm GroupMemberDecision (j):**

1. If node j is inactive, then compute \( \nu \) as the trust degree attenuation factor
   
   \[ T \leftarrow \nu \times T \]

2. End if

3. If dispersion of the latest feedback trust value \( d \) > threshold of tolerance, then compute \( P \) as the trust degree punishment factor
   
   \[ T \leftarrow P \times T \]

4. Else compute \( R \) as the trust degree reward factor
   
   \[ T \leftarrow R \times T \]

5. Endif

6. If \( T \) < threshold of the trusted group, then drive out j from the trusted group

7. Else keep j in this trusted group

Through the above mechanism, the global trust value of the group members in the trusted group can be updated in real time. This mechanism effectively removes the member nodes with bad behavior and ensures the validity and correctness of the trusted group.

**Simulated results**

To prove the correctness of the model mentioned in this article, based on the research in the previous section, a virtual network environment was constructed using the simulation software Netlogo. In the simulation process, the node interaction behavior is simulated first, and a trusted group is constructed. When the initialization is successful, the node interaction result evolution simulation is performed according to the trust model.

Table 4. Simulation experiment parameter setting.

| Parameter | Value | Description          |
|-----------|-------|----------------------|
| N         | 300   | Number of nodes      |
| T         | 100   | Total time steps     |
| Malicious%| 10%, 15%, 20%, 25%, 30%, 40% | Proportion of malicious nodes |

**Experimental environment and settings**

There are three types of nodes in the network:

- **Honest nodes:** Always provide high-quality services and correct feedback as much as possible.
- **Malicious nodes:** Always provide low-quality services and exaggerated feedback value to members of the malicious team. For the nodes outside the team (honest nodes and dynamic nodes), the value of trust is defamatory.
- **Dynamic nodes:** The quality of service provided by such nodes dynamically changes with time and may act as honest nodes. The behavior of this type of nodes may be like malicious or honest. At the same time, correct feedback is made.

In detail, malicious nodes not only provide low-quality services, which interferes with the normal operation of the system as well as the feedback information. The feedback trust value of malicious nodes to the member of their malicious team is always 1. The feedback trust value to the members outside the malicious team is 0. The dispersion of feedback of the direct trust value is always submitted as 1 by the malicious node.

Honest nodes always provide high-quality services as much as possible and give correct feedback to interactive nodes when interacting.

The dynamic node will randomly behave like a malicious node or an honest node and will not be regarded as a part of the team by the malicious node. The existence of dynamic nodes will make the simulation experiment environment closer to the actual application environment.

Table 4 shows the parameter settings of the simulation experiment.

**Simulation results**

**Interaction success rate.** The success rate of node interaction is an important indicator for evaluating the performance of a trust model. To verify the effectiveness of
our proposed model (MATM), the IDTEM model of the recent research literature and the classic EigenTrust model were subjected to the same simulation experiment. The experimental results are shown in Figure 2.

As shown in Figure 2, the EigenTrust model is a classic trust management model and is a lack of consideration of other influencing factors, thus has the poorest performance on interaction success rate among the three models. The IDTEM model aims to suppress the malicious recommendation, and the interaction success rate results in a gentle decline. The proposed model in this article comprehensively evaluates the trust of nodes by

- Multidimensional attribute;
- Dispersion of trust value;
- Time decay.

Our trust model has significant advantage on interaction success rate, especially in low percentage of malicious nodes. As the proportion of malicious nodes increases, the impact of the exaggerated collaborative attacks and defamation attacks on the network environment is more obvious. These attacks result in the decline of the interaction success rate with the increase in the proportion of malicious nodes. However, our proposed trust model MATM still maintains the highest success rate among the compared models.

The efficiency of the proposed model. Since the global trust value of a node is the main basis for judging the identity of a node, the simulation makes a statistical calculation

![Figure 2. Node interaction success rate changes with the proportion of malicious nodes.](image)

![Figure 3. The average global trust value of honest, malicious, and dynamic nodes when N = 300: (a) malicious nodes account for 10%, (b) malicious nodes account for 20%, (c) malicious nodes account for 30%, and (d) malicious nodes account for 40%.](image)
of the average global trust value of various nodes, as shown in Figure 3.

The average global trust value is unified as a value from 0 to 1. It can be seen from Figure 3 that in the case where the malicious nodes account for a relatively low percentage (10%, 20%), the average global trust value of honest nodes is the highest, the value maintained above 0.8 after stabilization. Because of the instability of dynamic nodes, the average global trust value of dynamic nodes is below 0.7. As for the malicious nodes, the value is at a low level below 0.2, indicating the correctness of the trust assess method and the interactive decision of MATM.

When the malicious nodes account for 30%, the average global trust value of honest nodes will reduce to 0.7 due to the exaggeration/collaborative attacks and defamation attacks of malicious nodes. As for the dynamic nodes, they are greatly affected and entering a low trust value of 0.1–0.2. The average global trust value of malicious nodes has increased slightly, but it remains within the low trust value range of 0.2–0.3. In the case where malicious nodes account for 40%, the average global trust value of honest nodes remains above 0.55, while the value of malicious nodes is stable at 0.3–0.4. Dynamic nodes have their own behavior and are attacked by malicious nodes, resulting in the lowest average value.

Simulation results show that after a certain round of interaction, the credibility of various nodes will tend to be stable. At the same time, when the proportion of malicious nodes continues to increase, this model can still ensure that the average global trust value of honest nodes is above 0.5. It tends to be trusted as the average global trust value of malicious nodes is below 0.5.

The efficiency of the trusted group. To verify the validity of the trusted group, we also output the identification of members in the trusted group. As shown in Figure 4, malicious nodes account for 10%, 20%, 30%, and 40% of all nodes ($N = 300$), respectively.

Figure 4 demonstrates the correlation of the proportion of malicious nodes and the group composition. When the proportion of malicious nodes is relatively low (10%, 20%), more than 90% of the trusted group members are honest nodes. As the proportion of malicious nodes increases, the coordinated attacks of malicious nodes interfered with the acceptance of the trusted group. But the trusted group can still maintain more than 75% of the honest nodes. It illustrated that
the trusted group has the effectiveness of application in the system.

Conclusion

We proposed an MATM for the IoT trustworthiness relationship depending on the associate attributes of nodes. The trust relationship prediction is based on the trust value provided by nodes in a certain transmission radius. We adopted trust value dispersion in trust computing to protect normal nodes from collusion attacks by malicious nodes. According to the trust degree computed by the trust modeling process, we built the trusted group and selected the TL for the trust group to support the management of nodes. We designed a DMM that includes time decay, reward, and punishment strategies to update the trusted group with comprehensive trust status. This mechanism effectively guarantees the reliability and stability of trusted groups. Simulation results show that MATM could effectively screen malicious nodes from normal nodes, as well as respond to invalid feedback from malicious nodes. Compared with some existent trust model, our proposed model has better performance in interaction success rate. We also showed by simulation the efficiency of the trusted group and ensure that the honest nodes account for the majority of the trusted group. This article aims at resolving problems about incomplete consideration and large overhead under the traditional IoT security strategy.

Future work will distinguish the behavior of malicious nodes in detail and improve the performance of our proposed trust model. The selection of trusted group management nodes in the network environment and the calculation of comprehensive credibility will be further optimized to improve the trust evaluation scheme for trusted groups.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by National Key Research and Development Project (2019YFB2102303), National Natural Science Foundation of China (61971014) and Henan Key Research and Development Project (202102310522).

ORCID iD

Jinghan Chen https://orcid.org/0000-0002-5765-5118

References

1. Cai Z and Zheng X. A private and efficient mechanism for data uploading in smart cyber-physical systems. IEEE Trans Netw Sci Eng (TNSE) 2020; 7(2): 766–775.
2. Kaminaris SD, Tripliotakis E, Stavrokakis GS, et al. An intelligent data acquisition and transmission platform for the development of voyage and maintenance plans for ships. In: The fifth international conference on information, intelligence, systems and applications (IISA 2014), Chania, Crete, Greece, 7–9 July 2014. IEEE.
3. Pan Y, Deng XH and Shen HL. Credit distribution for influence maximization in online social networks with time constraint. In: Proceedings of 2015 IEEE International Conference on Smart City/SocialCom/SustainCom, Chengdu, China, 19–21 December 2015, pp. 255–260. Piscataway, NJ: IEEE.
4. Deng XH, He LF, Li X, et al. A reliable QoS-aware routing scheme for neighbor area network in smart grid. Peer Peer Netw Appl 2016; 9(4): 616–627.
5. Zheng X, and Cai Z. Privacy-preserved data sharing towards multiple parties in industrial IotIs. IEEE J Sel Areas Commun (JSAC) 2020; 38(5): 968–979.
6. Zheng X, Cai Z, and Li Y. Data linkage in smart IoT systems: a consideration from privacy perspective. IEEE Commun Mag. 2018; 56(9): 55–61.
7. Mike S, Gianluca C, Ken M, et al. Trust Modelling in 5G mobile networks. In: Proceedings of the 2018 workshop on security in softwarized networks: prospects and challenges (SecSoN’18), Budapest, Hungary, 20–24 August 2018, pp. 14-19. New York: ACM.
8. Xie LX and Wei RX. A dynamic trustworthiness assessment method for Internet of Things nodes. Comput Appl 2019; 3: 2597–2603.
9. Ye B, Wang Y and Liu L. Crowd defense: a trust vector-based threat defense model in crowdsourcing environments. In: Proceedings of the 2017 IEEE international conference on web service, Honolulu, HI, 25-30 June 2017, pp. 245-252. New York: IEEE.
10. Hu MS, Yang K and Jia ZJ. A semantic trust model of large-scale distributed system based on Ontology. In: Proceedings of the 30th Chinese control and decision conference, Shenyang, China, 9-11 June 2018, pp. 1738-1743. New York: IEEE.
11. Pawar PS, Rajarajan M, Nair SK, et al. Trust model for optimized cloud services. In: Proceedings of the Ifip international conference on trust management, Surat, India, 21-25 May 2012, paper no. 374, pp. 97–112. Berlin: Springer.
12. Niu B, You W, Tang H, et al. 5G network slice security trust degree calculation model. In: Proceedings of the IEEE international conference on computer and communications (ICCC), Chengdu, China, 13–16 December 2017, pp. 1150-1157. New York: IEEE.
13. Mohsenzadeh A, Motameni H and Er MJ. Retraction note to: a new trust evaluation algorithm between cloud entities based on fuzzy mathematics. Int J Fuzzy Syst 2019; 18: 659–672.
14. Al-khafajiy M, Baker T, Asim M, et al. COMITMENT: a fog computing trust management approach. J Parallel Dist Comput 2020; 137: 1–16.
15. Li F, Shi YL, Chen Z, et al. A trust-based approach to secure routing decisions for networks of opportunity. Softw J 2018; 29: 2829–2843.
16. Wu DY, Li Q, Yu X, et al. A peer-to-peer network trust model based on blockchain. Comput Sci 2019; 46: 138–147.
17. You J, Shangguan JL, Xu SK, et al. Distributed dynamic trust management model based on trust reliability. J Softw 2017; 28: 2354–2369.
18. Ma XY and Li XY. Trust evaluation model in edge computing based on integrated trust. In: Proceedings of the 2018 international conference on algorithms, computing and artificial intelligence (ACAI’18), (paper no. 26), Sanya, China, December 2018, pp. 1–6. New York: ACM. https://doi.org/10.1145/3302425.3302491
19. Hasrouny H, Samhat AE, Bassil C, et al. Trust model for secure group leader-based communications in VANET. Wireless Netw 2019; 25: 4639–4661.
20. Jiang J, Han G, Wang F, et al. An efficient distributed trust model for wireless sensor networks. Parallel Distrib Syst 2015; 26: 1228–1237.
21. Lu K, Wang J and Li M. An EigenTrust dynamic evolutionary model in P2P file-sharing systems. Peer Peer Netw Appl 2016; 9: 599–612.
22. Cho JH and Chen IR. PROVEST: provenance-based trust model for delay tolerant network. IEEE Trans Dependable Secure Comput 2018; 99: 151–165.
23. Wang J and Liu B. Online fault-tolerant dynamic event region detection in sensor networks via trust model. In: Proceedings of the 2017 IEEE wireless communications and networking conference (WCNC), San Francisco, CA, 19–22 March 2017, pp. 1-6. New York: IEEE.
24. Tariq N, Asim M, Maamar Z, et al. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT. J Parallel Distrib Comput 2019; 134: 198–206.
25. Meng X and Liu D. GeTrust: a guarantee-based trust model in chord-based P2P networks. IEEE Trans Dependable Secure Comput 15(1): 54–68. DOI: 10.1109/TDSC.2016.2530720.
26. Jayasinghe U, Otebolaku A, Um TW, et al. Data centric trust evaluation and prediction framework for IoT. In: Proceedings of the 2017 ITU kaleidoscope: challenges for A Data-driven Society, Nanjing, China, 27–29 November 2017, pp. 1-7. New York: IEEE.
27. Truong NB, Um TW, Zhou B, et al. From personal experience to global reputation for trust evaluation in the social internet of things. In: Proceedings of the global communication (GLOBECOM), Singapore, 4-8 December 2017, pp. 1-7. New York: IEEE.
28. Bullen PS. Handbook of means and their inequalities. Berlin: Springer Netherlands 2003.
29. Kamvar SD, Schlosser MT and Garcia -Molina H. The EigenTrust algorithm for reputation management in P2P networks. In: Proceedings of the 12th international conference on world wide web, Budapest, Hungary, May 2003, pp. 640-651. New York: ACM.