Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 12, No. 1, 2025

A Blockchain-based Trust Management Model for IoV

Xudong Chen

College of Computer Science and Engineering, Chongqing University of Technology, Chongqing, China

Abstract: In this paper, we design a blockchain and social information-driven trust management model for the Internet of Vehicles (IoV), which effectively solves the problems of sparse node interactions, data dynamics, and malicious attacks faced by trust management in the IoV environment. The model utilizes a multi-dimensional assessment method of direct, indirect and global trust between entities, and dynamically constructs a reference list by quantifying social relationships such as ownership similarity between nodes in the connected car environment. A weighted fusion algorithm of direct trust, indirect trust and inter-cluster relative trust is proposed, combined with a lightweight consensus mechanism to achieve efficient updating of the trust value, and the storage method is optimized taking into account the blockchain storage performance limitation. After verification, the system can quickly identify and isolate malicious nodes under the premise of low cost and low latency, significantly improving the overall security and reliability of Telematics. The scheme also has better performance in terms of storage overhead and time required for consensus, and has the ability to withstand attacks such as singalongs.

Keywords: Blockchain; Trust Management; IoV; Smart Contract.

1. Introduction

There are several issues that need to be focused on when designing a trust management model for the IoT domain. First, due to the large number of device nodes included in the IoT environment, it is likely that a particular node has never directly interacted with most of the other entities, which makes inter-device interactions as well as utilizing feedback suggestions from other nodes of great significance for trust evaluation. However, obtaining feedback from all other nodes is impractical in real-world scenarios, not only because IoT devices are mostly resource-constrained, as it is extremely wasteful of computational resources to do so, even if resources are sufficient. For these reasons, there is an urgent need to design a lightweight algorithm and build a mechanism to help the model evaluate and filter the reference-value suggestions, so as to effectively reduce the number of interactions in the system and the cost incurred by executing smart contracts. In addition, given that IoT devices are constrained in terms of energy and computational resources, designing a lightweight algorithm not only helps to conserve resources, but also ensures that these devices will not be overburdened with computation when participating in the trust assessment, thus affecting the overall system performance.

Based on the above analysis, our contribution is as follows: based on the in-depth analysis of social information collected in IoT networks, we propose a blockchain and social information-driven trust management model (BBTMT) for Telematics. The model gives full play to the advantages of blockchain's distributed, untamperable and transparent nature, and constructs a distributed trust assessment solution suitable for the IoT environment. It is worth noting that the framework is not only applicable to IoT, but also has strong versatility and extensibility, which can provide technical support for other IoT application scenarios. In order to verify the effectiveness and feasibility of the proposed model, we implement the BBTMT model on a private blockchain platform based on Ether, and evaluate the model's performance in terms of malicious node detection, trust value update, and storage cost through a series of experiments. The experimental results show that BBTMT has advantages in the identification rate of malicious nodes, system accuracy, and cost-effectiveness compared with existing schemes.

2. Related Word and Preliminaries

Analyzing the social relationships of connected devices is an effective way to evaluate trust between entities in IoT systems[1]. The social IoT concept integrates the definitions of IoT networks and social networks and considers IoT objects as nodes connected through social connections[2]. Using this approach, the combination of social information with feedback data from prior behavior of nodes in the system can be a valuable source of information for assessing the trustworthiness of devices. Trust management in the Social Internet of Things has been studied by many researchers for a long time. Nitti et al[3] proposed two approaches for trust management in the Social Internet of Things: the subjective model and the objective model. These two modeling approaches have greatly inspired later researchers. In the former approach, each node calculates the trustworthiness of other nodes based on its direct experience and recommendations from mutual friends, which is noteworthy because this approach is applicable to localized information and small-scale networks. The latter approach utilizes Distributed Hash Tables (DHT) to store and share the trust information of the nodes so that any node can access the global trust data, whereas this approach is suitable for large-scale networks but increases the network burden. Truong et al[4] proposed a Trust Management Model (TM-SIoT) based on mutual evaluation method in order to assess the trustworthiness of the social IoT nodes. The model combines quality of service (QoS) and social relationship metrics and introduces a new time-aware trust metric. The authors verified that the model is able to provide reliable trust assessment in environments with 50% malicious nodes. Chen et al[5], after recognizing that traditional recommender systems are difficult to apply in social IoT environments facing issues such as data sparsity, dynamics, and heterogeneity, proposed an access service recommender scheme for the social IoT, which analyzes the social

relationships between devices and quality of service metrics by A comprehensive trust assessment model is constructed. In Chen et al[6], the authors proposed a multidimensional trust assessment model combining direct and indirect trust for social IoT. The model first filters candidate services based on social relationships then ranks them based on QoS scores and finally generates a recommendation list. However, the drawback is that a recommendation is shared with all other nodes after each interaction to help them make better decisions in the following interactions, but this creates more computational burden. Of course, all the above studies are centralized and have drawbacks such as single point of failure problem.

In the IoT ecosystem, decentralized approaches and trust assessment mechanisms play a vital role. Lately, blockchain technology has emerged as a strong candidate for enhancing the security, privacy, and dependability of IoT systems[7].Ahmed et al[8] proposed a blockchain-based privacy-preserving authentication and trust management framework by combining blockchain technology, cryptographic algorithms, and a distributed consensus mechanism, which achieves anonymous authentication of vehicle identities and dynamic evaluation of trust values. The authors' proposed solution framework provides a secure and efficient privacy protection and trust management solution for VANET, which can enhance the security and reliability of intelligent transportation systems. Tu et al[9] proposed a blockchain-based dynamic trust and reputation model, which utilizes a dynamic evaluation mechanism and distributed consensus algorithms to achieve real-time updating of the trust value of a device and dynamic reputation management. Du et al [10] proposed a dual-layer blockchain trust management mechanism (DLBTM), which can effectively identify malicious nodes through a dual-layer blockchain architecture and a logistic regression algorithm, and the system is able to identify at least 90% of malicious nodes over time. Considering the existing research on IoT trust management systems, a number of issues need to be addressed. First, a node is likely to have little or no interaction with most other nodes in the system. Due to this reason, this paper argues that research should focus on how to utilize the opinions of other nodes. In addition, the proposed solution should be designed to be lightweight and low-cost due to constraints such as limited resources of devices in the IoT environment.

In order to address these issues, in this study, we aim to design a blockchain-based trust management system that utilizes the social information of entities to provide a trust computation mechanism.

3. Proposed Solution

In the model, the blockchain is responsible for storing data about the trustworthiness of the nodes in the system and ensuring the integrity and immutability of the data. The delegator refers to the node used to assess the trustworthiness of other nodes, while the delegatee is the node being assessed. At the end of the evaluation process, the delegator will feedback the evaluation results to the blockchain. The generation of feedback data consists of two ways: one is dynamically generated through an independent feedback module, and the other is calculated and updated based on the historical behavior of the nodes in the system. Fig. 1 illustrates the overall overview of the designed framework. In this design, the nodes in the network realize trust assessment by interacting with the blockchain to ensure the transparency and security of the transaction and trust management process. The framework, which will be implemented in this paper, is deployed on the private chain of an Ethernet platform that stores transaction records and deploys smart contracts. The deployed smart contract is responsible for running the trust evaluation process on the blockchain, and the contract code is written in the Solidity language and deployed to run in the Ethernet-specific binary format.

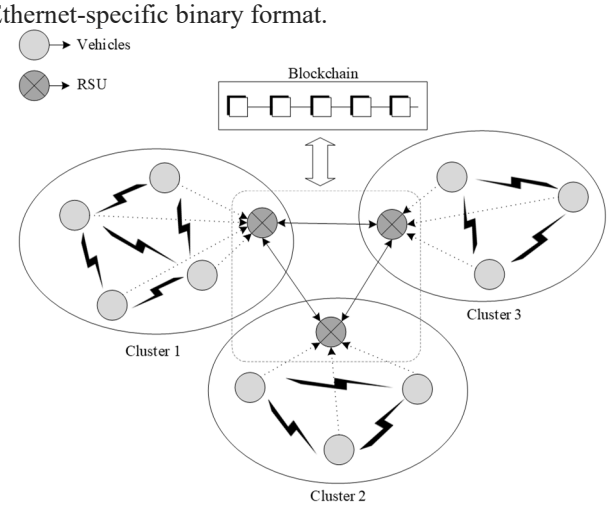

Fig 1. System architecture

The RSU that first discovers the correct random number within a specific region becomes the creator or miner of the new block. Once the block is generated, it is broadcast to all RSUs within that region. This allows every RSU in the area to independently verify the validity of the new block using the shared random number.

The trust assessment process of the social relationship analysis module is shown in Fig. 2, and the specific flow is explained as follows:

- The trustee sends a request to the blockchain, which verifies the trustee's identity.
- The smart contract evaluates the trust value using the trust evaluation algorithm.
- Based on the trust threshold, the result will be sent to the trustee and delegator nodes.
- The smart contract calculates the feedback about the request and updates the associated trust value based on the feedback.

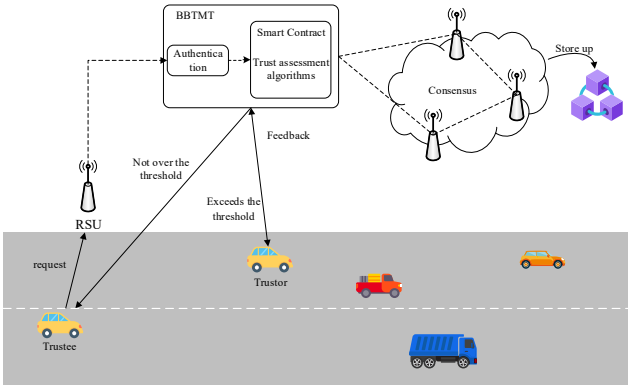

Fig 2. Flowchart of trust calculation

3.1. Reference Lists

In this section, this paper details the design methodology of

reference lists and introduces social ties (ST) as a metric to measure the social relationship between any two nodes in a network. To compute this metric, this paper integrates the following three key factors:

Ownership similarity: it is a measure of the strength of social ties between nodes with common ownership. In this method, multiple ownership is allowed, i.e., a device can be shared by multiple owners. Based on this, this paper defines the ownership similarity in this way. Let the sets of owners of node i and node j be O_i and O_j, respectively, where the respective primary owners are denoted as O_i^p and O_j^p, and the sets of partners are denoted as O_i^c and O_j^c, respectively, then the ownership similarity $ST_{ow}(i,j)$ of node i and node j can be expressed as:

$$\mathrm{ST}_{ow}(i,j) = \mu \times \delta(o_i^p, o_j^p) + (1-\mu) \times \frac{\left|O_i^c \cap O_j^c\right|}{\left|O_i^c \cup O_j^c\right|} \quad (1)$$

This similarity can be defined by the ratio of actual interactions n_{ij} between devices to the total possible interactions N_{ij}. For example, if 5 communication interactions actually occurred between two vehicles in the last 30 minutes and the total possible interactions are 10, their friendship similarity is 0.5. The node friendship similarity $ST_{fri}(i,j)$ can be expressed as:

$$ST_{fri}(i,j) = \frac{n_{ij}}{N_{ij}} \quad (2)$$

Owner friendship similarity: besides friendship between nodes, another type of friendship is defined between owners. This means that each owner can create a list of network node owners as its friend list. There may be a strong friendship similarity if there is a business cooperation between the owners of two vehicles (e.g., between different fleets of vehicles), or if there is a government vehicle, a shared car, or a cab company. Let the set of owners of node i and node j be O_i and O_j respectively, where the respective friend lists are denoted as $F(O_i)$ and $F(O_j)$, then the owner similarity $ST_{of}(i,j)$ of node i and node j can be expressed as:

$$ST_{of}(i,j) = \frac{|F(O_i) \cap F(O_j)|}{|F(O_i) \cup F(O_j)|} \quad (3)$$

In this paper, Jaccard's index[11] is used to assess the similarity between the above three lists for each pair of nodes and aggregated in order to define the following social relationships:

$$ST_{ij}(t) = \gamma \times ST_{ow}(i,j) + \eta \times ST_{fri}(i,j) + (1-\gamma-\eta) \times ST_{of}(i,j) \quad (4)$$

Above, is t time, ST_{ow}, ST_{fri} and ST_{of} are ownership similarity, node friendship similarity and owner friendship similarity respectively. The parameters γ and η are real numbers in the range [0,1] used to weight these factors. Node i adds node j to its reference list if ST_{ij} is greater than a defined threshold. Nodes can periodically update their reference lists based on their latest social information, and they can also refine their reference lists based on trust values.

3.2. Calculation of Direct Confidence Value

When initializing the system, the direct trust value DT_{ij} between all devices is set by default to an initial value of 1. This setting is suitable for cold-start scenarios with no historical interaction data, and the nodes dynamically update the trust value through a feedback evaluation mechanism during the subsequent process. The nodes utilize $f_{ij}(k)$ for modification, which is the feedback from node i about the k th access request from node j. The formula is as follows:

$$DT_{ij}(t) = \beta DT_{ij}(t-\Delta t) + (1-\beta) f_{ij}(k) \quad (5)$$

3.3. Calculation of inter-Cluster Relative Trust Value

The inter-cluster relative trust value ICT_i of a node i is computed by averaging the interaction frequency change ratio of that node with the interaction frequency change ratio of all other nodes within the same cluster. Assuming that there are N nodes in a cluster, the inter-cluster relative trust value of node i is denoted as ICT_i. the initial maximum of the inter-cluster relative trust value is the same as that of the direct trust value and is denoted as ICT_{max}. for $N-1$ nodes other than node i, the actual and standard interaction frequencies are denoted as M_j^{now} and M_j, respectively, and the change ratio of the interaction frequency is calculated according to Equation (6):

$$r_j = \left| \frac{M_j^{now} - M_j}{M_j} \right| \quad (6)$$

Then, the average value of the interaction frequency change ratio of these $N-1$ nodes is denoted as r_{Aver}, which can be calculated by Equation (7):

$$r_{Aver} = \sum_{j=1}^{N-1} \frac{r_j}{N-1} \quad (7)$$

The relative trust value ICT_i between clusters can be calculated by using Equation (8), and the upper limit of the difference between the interaction frequency change ratio of node i and the average of the interaction frequency change ratios of other nodes is K_{rrt}:

$$ICT_i(t) = ICT_{max} \times \varepsilon \quad (8)$$

Among them:

$$\varepsilon = \begin{cases} K_{\text{rrt}}, & r_{\text{Aver}} = 0 \\ 0, & |r - r_{\text{Aver}}| - K_{\text{rrt}} > 0 \\ \frac{\|r - r_{\text{Aver}}| - K_{\text{rrt}}|}{K_{\text{rrt}}}, & |r - r_{\text{Aver}}| - K_{\text{rrt}} \le 0 \end{cases} \quad (9)$$

It should be reminded that when calculating the average, only the nodes in the reference list are counted, and if the nodes are not in the reference list, they are not involved in the calculation of the average.

3.4. Calculation of Indirect Trust Value

In this part, indirect trust is defined as a weighted mean derived from the direct trust assessments of the trustee provided by the reference node:

$$IT_{ij}(t) = \frac{\sum_{k=1}^{K} w_{ik}(t) DT_{kj}(t)}{\sum_{k=1}^{K} w_{ik}(t)} \quad (10)$$

In the algorithm designed in this paper, the node i reference list contains K nodes. Among these reference nodes, the recommendation weights of each node are not equal, but are calculated based on the social connection between the delegator and the reference node as well as the direct trust value. Specifically, the recommendation weights are defined as shown below:

$$w_{ik} = \theta ST_{ik}(t) + (1-\theta) DT_{ik}(t) \quad (11)$$

3.5. Calculation of Indirect Trust Value

In the trust calculation process, the trust value of node i to node j is denoted as T_{ij}, where i is the delegator and j is the delegatee, and T_{ij} takes values between [0,1]. When $T_{ij} = 1$ it means that node j is completely trustworthy to node i, while when $T_{ij} = 0$ it represents completely untrustworthy. The formula for the trust value T_{ij} is given below:

$$T_{ij}(t) = \alpha DT_{ij}(t) + \lambda IT_{ij}(t) + (1-\alpha-\lambda) ICT_i(t) \quad (12)$$

4. Synthesize and Analyze

In the experimental design, this paper focuses on testing the performance of the proposed trust management model, mainly evaluating its ability to assess the trustworthiness of nodes and the success rate of detecting malicious nodes. Among them, this paper analyzes three performance metrics: the success rate of malicious node identification, the average trustworthiness of malicious nodes, and the cost of smart contract execution. The success rate is a measure of the percentage of malicious nodes that the system successfully detects out of the total malicious nodes. The average trustworthiness, on the other hand, evaluates whether the system is accurate in determining the trustworthiness of malicious nodes. And the cost of smart contract execution is calculated in terms of Gas, which is used to pay for transaction execution and contract invocation, and its specific value is calculated based on the computational resources consumed on the blockchain. With these metrics, this paper is able to comprehensively evaluate the performance of the proposed scheme in terms of malicious node detection, trust management, and computational overhead. Fig. 3 depicts the detection success rate of the system with different percentages of malicious nodes.

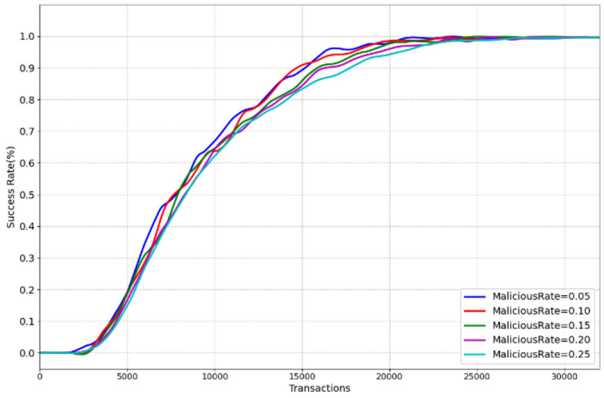

Fig 3. Success rate of detecting malicious nodes

In this paper, the Gas value of each process stage of the designed model is tested, including the smart contract deployment, node registration, trust value calculation and update stages, and the specific results are shown in Fig. 4. The results show that the Gas consumption required for smart contract deployment is the highest among all the phases, but this operation is performed only once at the beginning of the evaluation, so although the cost is high, the impact is minimal in the specific operation of the system. The relatively high Gas consumption for trust value computation compared to the node registration and update phases is mainly due to the fact that this phase requires more operations and data processing.

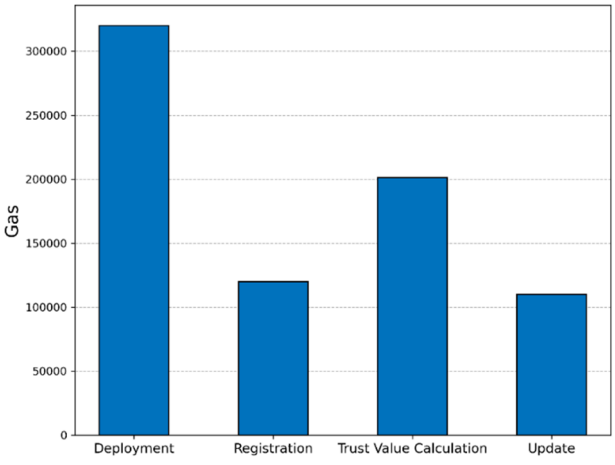

Fig 4. Gas consumption detail diagram

5. Conclusion

This paper presents a decentralized trust management model based on blockchain, designed to leverage social information for trust evaluation within a connected vehicle environment. The model incorporates social relationships between entities as supplementary data to improve the precision of trust computations. Nodes in the network evaluate the credibility of a given entity by collecting and analyzing feedback from peers. This process introduces minimal network overhead, thereby maintaining efficient communication. To optimize trust filtering, the model

integrates a lightweight algorithm that selectively processes reliable recommendations and restricts the frequency of interactions between nodes. By integrating blockchain technology, the framework ensures robust security and privacy protection. Simulation results demonstrate that the proposed approach effectively evaluates node trustworthiness and surpasses existing methods in terms of accuracy and cost efficiency.

References

[1] Atzori L, Iera A, Morabito G, et al. The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization[J]. Computer networks, 2012, 56(16): 3594-3608.

[2] Abdelghani W, Zayani C A, Amous I, et al. Trust management in social internet of things: a survey[C]//Social Media: The Good, the Bad, and the Ugly: 15th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2016, Swansea, UK, September 13–15, 2016, Proceedings 15. Springer International Publishing, 2016: 430-441.

[3] Nitti M, Girau R, Atzori L. Trustworthiness management in the social internet of things[J]. IEEE Transactions on knowledge and data engineering, 2013, 26(5): 1253-1266.

[4] Truong N B, Lee H, Askwith B, et al. Toward a trust evaluation mechanism in the social internet of things[J]. Sensors, 2017, 17(6): 1346.

[5] Chen Z, Ling R, Huang C M, et al. A scheme of access service recommendation for the Social Internet of Things[J]. International Journal of Communication Systems, 2016, 29(4): 694-706.

[6] Chen R, Bao F, Guo J. Trust-based service management for social internet of things systems[J]. IEEE transactions on dependable and secure computing, 2015, 13(6): 684-696.

[7] Laghari A A, Wu K, Laghari R A, et al. A review and state of art of Internet of Things (IoT)[J]. Archives of Computational Methods in Engineering, 2021: 1-19.

[8] Ahmed W, Di W, Mukathe D. Privacy-preserving blockchain-based authentication and trust management in VANETs[J]. IET Networks, 2022, 11(3-4): 89-111.

[9] Tu Z, Zhou H, Li K, et al. A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT[J]. Computer Networks, 2022, 218: 109404.

[10] Du G, Cao Y, Li J, et al. A blockchain-based trust-value management approach for secure information sharing in Internet of Vehicles[J]. IEEE Internet of Things Journal, 2023, 11(1): 333-344.

[11] Bag S, Kumar S K, Tiwari M K. An efficient recommendation generation using relevant Jaccard similarity[J]. Information Sciences, 2019, 483: 53-64.

[12] Mcauley J, Leskovec J. Discovering social circles in ego networks[J]. ACM Transactions on Knowledge Discovery from Data (TKDD), 2014, 8(1): 1-28.

[13] Bergstra J, Bengio Y. Random search for hyper-parameter optimization[J]. The journal of machine learning research, 2012, 13(1): 281-305.

[14] Abderrahim O B, Elhedhili M H, Saidane L. CTMS-SIOT: A context-based trust management system for the social Internet of Things [C]//2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2017: 1903-1908.

[15] Fortino G, Messina F, Rosaci D, et al. Using blockchain in a reputation-based model for grouping agents in the Internet of Things[J]. IEEE Transactions on Engineering Management, 2019, 67(4): 1231-1243.

[16] Hammi M T, Hammi B, Bellot P, et al. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT[J]. Computers & Security, 2018, 78: 126-142.

[17] Rafey S E A, Abdel-Hamid A, Abou El-Nasr M. CBSTM-IoT: Context-based social trust model for the Internet of Things[C]//2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT). IEEE, 2016: 1-8.

[18] Guleng S, Wu C, Chen X, et al. Decentralized trust evaluation in vehicular Internet of Things[J]. IEEE Access, 2019, 7: 15980-15988.

[19] Hbaieb A, Ayed S, Chaari L. Blockchain-based trust management approach for IoV[C]//International Conference on Advanced Information Networking and Applications. Cham: Springer International Publishing, 2021: 483-493.

[20] Mahmood A, Butler B, Zhang W E, et al. A hybrid trust management heuristic for VANETs[C]//2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2019: 748-752.

[21] Pal S, Hill A, Rabehaja T, et al. A blockchain-based trust management framework with verifiable interactions[J]. Computer Networks, 2021, 200: 108506.