A Muti-attributes-based Trust Model of Internet of Vehicle

Wei Ou[1], Entao Luo[1], Zhiyuan Tan[2], Lihong Xiang[1], Qin Yi[1], Chen Tian[1]

[1] Hunan University of Science and Engineering, Yongzhou, China
[2] School of Computing, Edinburgh Napier University Edinburgh, United Kingdom
ouwei1978430@163.com

Abstract. Internet of Vehicle (IoV) is an open network and it changes in constant, where there are large number of entities. Effective way to keep security of data in IoV is to establish a trustworthy mechanism. Through transmission and dissemination of trust, credibility of the entity of IoV is calculated and measured. In this paper a multi-attributes-based trust model is proposed. When the trust relationship between nodes is evaluated, overall experiences of the evaluator are considered as the main reference content, which have a significant restraining effect on malicious behaviors of bad nodes. Moreover, this model combines heuristic algorithm and takes the previous trust evaluation as an important reference content. Thus accuracy of evaluation of trust relationship is improved and sensitivity of this algorithm on behaviors of nodes is enhanced.

Keywords: Internet of Vehicle, Multidimensional Attributes, Direct Trust, Recommendation Trust, Trust Evaluation.

1 Introduction

Internet of Vehicle (IoV) refers to the realization of all-round network connection in vehicles, vehicles and persons, vehicles and vehicles, vehicles and roads, vehicles and service platforms with help of new generation of information and communication technologies. It improves the level of intelligent vehicles and automatic driving ability and constructs new business form of automobile and traffic services. It improves traffic efficiency and driving experiences, and provide users with intelligent, comfortable, safe, energy-saving and efficient comprehensive services [1]. Internet of Vehicle is centered on “both ends – cloud”, supplemented by roadbed facilities, including intelligent networked cars, mobile intelligent terminals, car networking service platforms and other objects. It involves five communication scenarios: vehicle-cloud communication, vehicle-vehicle communication, vehicle-to-person communication, vehicle-road communication, and in-vehicle communication [2]. As shown in Fig. 1.

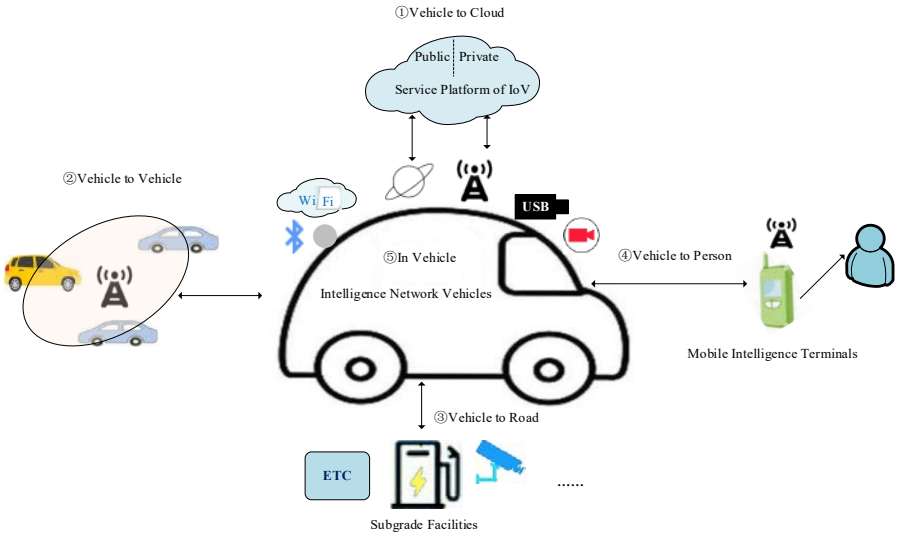

Fig. 1. Application Scene of IoV

Internet of Vehicle is an open network that is constantly changing. There are a large number of entities, such as floating cars and various types of drive test equipment. The effective way to ensure data security in network is to establish a trust mechanism, through the transmission and dissemination of trust. Calculating and measuring the credibility of the target entity, and selecting the data provided by the reliable entity as the object of processing is to ensure that the result is more accurate and close to the real data. At present, the trust model of Internet of Vehicle mainly has four problems: ① Lack of trust model to consider multi-application scenarios. ② Lack of trust calculation method to support dynamic update. ③ Lack of ability to adapt to a dynamic trust decision-making mechanism. ④ Lack of consideration for future communication environments.

2 Description of Trust Model

2.1 Basic Definitions

The multi-attributes-based trust model based on IoV [3][4] is shown in Fig. 2.

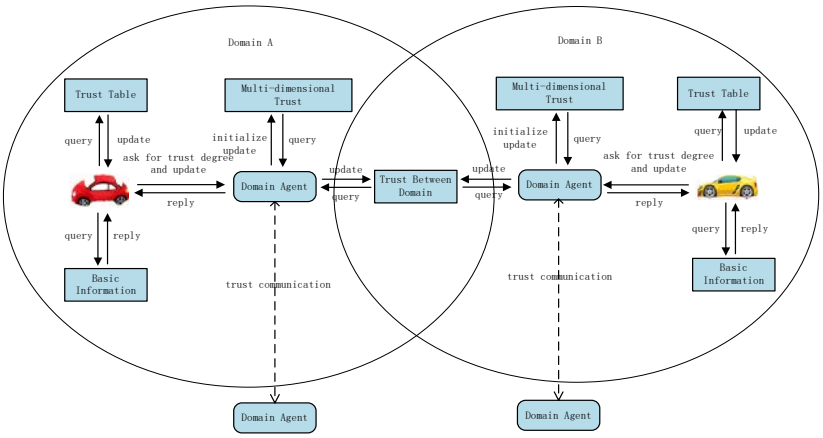

Fig. 2. Trust Model Based on Internet of Vehicle

Definition 1 Multidimensional vector A: $\overline{A}=[A_1, A_2, \cdots, A_i]$, $i \in N$. A_i represents the transaction trust of node A of IoV in terms of i.

Definition 2 If node A_{i} in domain A is not the first transaction with node B_{j} in domain B, $hdtv_{B_j}^{A_{\mathrm{i}}}$ represents the last historical direct trust between A_{i} and B_{j}. $dtv_{B_j}^{A_{\mathrm{i}}}$ represents the direct trust between A_{i} and B_{j}.

Definition 3 $\mathrm{dt}_{A_j}^{TA}$ represents the direct trust of domain agent to node A_{j}.

Definition 4 $\mathrm{rtv}_{A_i}^{A}$ represents the recommended trust of domain A to node A_{i}.

Definition 5 The recommended trust of domain A to domain B is defined as rtv_{B}^{A}. $\mathrm{rtv}_{B_j}^{A_i}$ represents the recommended trust of node A_{i} and node B_{j}.

Definition 6 $R\left(A_{\mathrm{i}}, A_{\mathrm{k}}\right)$ represents the recommended trust factor of node A_{i} to node A_{k}. Range of the value is [0, 1].

Definition 7 Domain maintains two tables, one is the trust table in the domain. Each node in the domain maintains a value of trust, which is used to describe performance of nodes in services. It is defined as $\mathrm{f}_{A-A_{\mathrm{i}}}$. It represents the trust value of the node A_{i} granted by the admin domain A.

Definition 8 The number of successful transactions between nodes are defined as S.

Definition 9 The number of unsuccessful transactions between nodes are defined as f.

2.2 Calculation of Trust

1)Initialization of Trust

For newly registered nodes, each domain agent is obliged to give them an appropriate initial trust value. If the trust value is too low, it will not meet the conditions of transactions between nodes. If the trust value is too high, some malicious nodes will use the method of re-registering node to improve their trust value, which will damage the programs of other nodes. Reference [5] sets the initial trust value of the newly joined node to 0.5, and then improves or reduces trust of the node according to its performance.

2)Calculation of Direct Trust

Direct trust refers to the direct transaction between two nodes in the past. Thus a direct trust relationship is established. The source of trust value is based on the transaction between two nodes.

Calculation of direct trust has the following two situations:

- Node A_{i} and node B_{j} have ever traded. For both parties, current trust can be calculated by direct trust of the latest history. Considering the time decay factor, direct trust of current two nodes is as shown in the following formula:

$$dtv_{B_j}^{A_i}=\mathrm{h}dtv_{B_j}^{A_i}*T(\Delta\mathrm{t},\ \sigma) \tag{1}$$

In formula (1), $T(\Delta\mathrm{t},\ \sigma)$ is time decay function, $\Delta\mathrm{t}$ is time difference between current time and the latest transaction, σ is type of transaction and it represents some kind of scientific calculation, data storage and file download. Time decay function is as follows:

$$T(\Delta\mathrm{t},\ \sigma)=\frac{1}{\Delta\mathrm{t}+1} \tag{2}$$

- When transaction between two nodes is completed, current trust between them needs to be calculated. Trust of a single service is shown in the following formula:

$$dtv_{B_j}^{A_i}=f(\sigma,\omega)=\sum_{k=1}^{n}\gamma_k\omega_k \tag{3}$$

In formula (3) ω represents dimension of service trust and γ_{k} represents the Kth dimension coefficient which satisfies the expression $\sum_{k=1}^{n}\gamma_k\omega_k$. This expression is suitable for any case regardless of whether there has been a transaction between two nodes.

3)Calculation of Recommendation Trust in Domain

Recommendation trust in domain, that is indirect trust in domain, refers to the fact that there has never been a direct transaction between two nodes in same domain. Source of trust value is based on recommendation and evaluation of other nodes. Calculation of recommendation trust in domain can be divided into the following two cases:

- Node A_i in domain needs to evaluate trust of another node A_j in another domain.

Firstly, neighbors of node A_i are asked whether they have had direct transactions with node A_j. If so, recommended trust between nodes is shown in the following formula:

$$\mathrm{rtv}_{A_j}^{A_i} = \frac{\sum_{k-1}^{n} \mathrm{rtv}_{A_k}^{A_i} * R(A_i, A_k) * dtv_{A_j}^{A_k}}{\sum_{k-1}^{n} \mathrm{rtv}_{A_k}^{A_i} * R(A_i, A_k)} \tag{4}$$

- If two transaction nodes belong to the same domain, they can directly ask domain agent TA (Trust Agent) of that domain. Nodes can trust domain agent completely, as shown in the following formula:

$$\mathrm{rtv}_{A_j}^{A_i} = dt_{A_j}^{TA} \tag{5}$$

4)Calculation of Recommendation Trust Between Domains

Recommendation trust between domains refers to trust recommendation between trust agents when two nodes that do not belong to the same domain judge each other's trust. If the neighbor node has a direct transaction with the target node, then the formula (4) and formula (5) can be used to calculate the trust. In contrary, if the neighbor node has no direct transaction with the target node (service provider), then the domain agent must find a recommended trust path. Here, we can abstract the trust relationship between domains into a directed graph. Each domain is represented by each node in the graph. The trust relationship between domains is represented by the edge of the graph. It is recorded as a directed graph G= (V, E). Nodes (service applicants) need to send requests of trust recommendation and basic information of target nodes to domain agents. Trust agent needs to find a recommendation path and calculate trust of target node. As shown in Fig. 3.

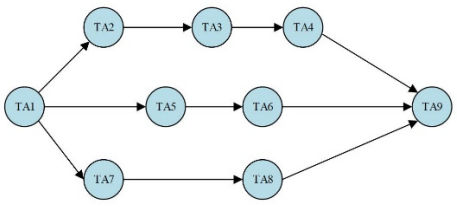

Fig. 3. Recommendation Trust Between Domains

Describe the above situation as G= (V, E). Here we use the method *the shortest path maximum trust value* to select the most suitable path. As shown in fig. 3, there are three paths: TA2-TA3-TA4, TA5-TA6 and TA7-TA8. Firstly the shortest path is selected. We can see that TA5-TA6 and TA7-TA8 are the shortest path. Then we select the maximum value of trust from the two paths. The method of calculating trust value is as follows:

$$\mathrm{rtv}_{B_j}^{A_i} = \mathrm{dt}_{B_j}^{TA} * \prod_{k=m}^{n-1} \mathrm{rtv}_{TA_{k+1}}^{TA_k} \tag{6}$$

2.3 Trust Updating

1)Trust Update of Nodes

After using services provided by node B_j, node A_i needs to update its own direct trust table to reflect changes of trust relationship between them. If node A_i is satisfied with the service of node B_j, it needs to improve the trust of node B_j .In contrary it needs to reduce its trust. As shown in the following:

$$\mathrm{hdtv}_{B_j}^{A_i} = \mathrm{dtv}_{B_j}^{A_i} = f(\sigma, \omega) = \sum_{k=1}^{n} \gamma_k \omega_k \tag{7}$$

Formula (7) is also applicable to the case that two nodes belong to the same domain.

2)Updating of Trust in Domain

Trust tables in domain agents need to be updated after the transaction between two nodes. If the transaction is successful, trust value of corresponding nodes will increase. On the contrary it decreases. As shown in the following:

$$\begin{cases} f_{A-A_i} = H + \mu \times \varphi(s) & \textit{Transaction Successed} \\ f_{A-A_i} = H - \mu \times \varphi(f) & \textit{Transaction Failed} \\ \varphi(x) = e^{-1/x} \end{cases} \tag{8}$$

In formula (8) $\mu(0 < \mu < 1)$ represents updating coefficient, *H* represents the trust value before updating, s and f represent the number of success and failure respectively. Referring to Beth model, we define $\varphi(x) = e^{-1/x}$ and make $\varphi(x)$ increases with increases of *x*. Because of $\mu(0 < \mu < 1)$, it can be concluded that the more number of

success is, the faster trust value increases. On the contrary the faster trust value decreases. When total trust value of a node is reduced to certain value, if it is less than zero, the domain agent will kick the node out.

For updating coefficient, the data in reference [6] is used as the updating coefficient of success transaction when μ_1=0.01. And when μ_2=0.1 it is used as the updating coefficient for failure transaction. The purpose is to reduce the trust value of malicious nodes when they provide services that harm other nodes.

3)Updating of Trust Between Domains

Assuming that two nodes from different domains trade with each other, if the transaction succeeds, the trust value between domains involved in the recommendation increases and on the contrary decreases. For the specific value of increase or decrease, it should be based on the number of success or failure transactions between nodes. As shown in the following:

$$\begin{cases} \mathrm{rtv}_B^A = H + \mu \times \varphi(s) & \textit{Transaction Successed} \\ \mathrm{rtv}_B^A = H - \mu \times \varphi(f) & \textit{Transaction Failed} \\ \varphi(x) = e^{-1/x} \end{cases} \tag{9}$$

3 Experiments

We demonstrate security and effectiveness of our algorithm through simulation experiments. The main verification contents are sensitivity and accuracy of our algorithm in describing the trust relationship between nodes of IoV.

The service providers of this experiment were randomly selected. The steps to provide the service are as follows: Firstly, we ensure that the first 30 services are of high quality, then provide 20 low quality services, at last provide 50 quality services. It can be known from experiments (as shown in Fig. 4) that through use of our calculation methods, the results of the experimental objects will change accordingly due to the quality of the service. Moreover, although the quality of service has risen to the previous level and the quantity provided has far exceeded the original level, its trust value cannot be restored to its original level. It can be seen that the algorithm can make rapid feedback on the situation of degraded service quality, thus effectively curbing the cheating trend of malicious nodes.

After completing the above experiment, 20% of the nodes were randomly selected as bad nodes, and 60% of them were normal nodes to provide good quality of service. In this experiment, the results calculated by model PathTrust show that the interest ratio between the normal node and the malicious node is almost the same (as shown in Fig. 5). It can be seen that the Path Trust algorithm has poor ability to constrain bad nodes, and the algorithm incorporates a penalty mechanism to control the benefits of bad nodes

below 60%. Compared with the Path Trust algorithm, bad nodes have a higher cost in our algorithm.

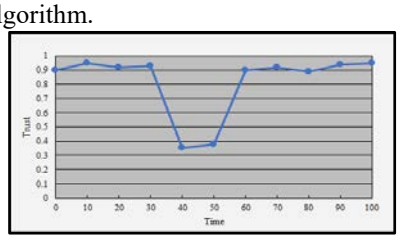

Fig. 4. Sensitivity and Accuracy

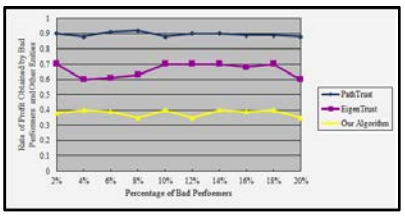

Fig. 5. Containment of Bad Nodes

4 Conclusion

In this paper the trust model of Internet of Vehicle is studied and analyzed. From aspects of trust initialization, trust calculation and trust updating, we propose a trust model for Internet of Vehicle. When evaluating the trust relationship between nodes, overall experiences of the evaluator are considered as the main reference content, which have a significant restraining effect on malicious behaviors of bad nodes. Moreover, our model combines heuristic algorithm and takes the previous trust evaluation as an important reference content. Thus accuracy of evaluation of trust relationship is improved and sensitivity of our algorithm on behaviors of nodes is enhanced.

ACKNOWLEDGEMENTS

This work was supported by the construct program of applied characteristic discipline in Hunan University of Science and Engineering.

References

1. Security of Internet of Vehicle[EB/OL]. China Information and Communication Research Institute, 2017.
2. Ziping Zhang. Study on Grid Multidimensional Trust Model Based on Fuzzy Comprehensive Evaluation[D]. Qufu Normal University, 2014. [2] Ziping Zhang. Study on Grid Multidimensional Trust Model Based on Fuzzy Comprehensive Evaluation[D]. Qufu Normal University, 2014.
3. Liping Wang, Shoubao Yang. A Trust Model in The Grid Environment[J]. Computer Engineering and Applications, 2004, 40, (23), 50-53.
4. M. Richardson.Trust Management for the Semantic Web,Proceedings of the Second International Semantic Web Conference [J].Sanibel Island, FL,2003, pp. 351-368.
5. J.Ahn, X.Sui. Identifying Beneficial Teammates Using Multi-dimensional Trust[C]. Proeeedings of the 7th intemational joint conference on Autonomous agents and multiagent systems, 2008:1469-1472.
6. Kun Li,Hao Jiang. A Trust Model with Classification Decision Attributes[J]. Computer Technology and Development, 2010, 20(03):36-39+43.