Chapter 1
A Cross-Domain Security Model Based on Internet of Vehicles

Wei Ou, Meiyan Wei, Qin Yi, and Lihong Xiang

1.1 Introduction

The Internet of Vehicles (IoV) refers to the realization with the help of next-generation information and communication technologies to implement all-round network connection between vehicles and vehicles, vehicles and roads, vehicles and persons, and vehicles and service platforms. This technique not only can improve the transportation efficiency and driving experience but also enhances automatic driving ability and the level of intelligent vehicles. Build a new business format for automobiles and transportation services. Provide users with an integrated service which is comfortable, intelligent, energy-saving, safe, and efficient [1]. With "both ends-cloud" as the core, the Internet of Vehicles (IoV) is assisted by roadbed facilities, including intelligent networked vehicles, mobile intelligent terminals, Internet of Vehicles service platform, and other objects. It contains five communication scenarios: vehicle-human communication, vehicle-vehicle communication, vehicle-cloud communication, vehicle-road communication, and intra-vehicle communication [2].

Vehicle network is an ever-changing open network. There are a number of entities like floating cars and various types of driving test equipment in this open network. The most effective way to ensure the security of network is to build a trust mechanism based on the transmission and dissemination of trust. To ensure that the results are more accurate and closer to the real data, we measure and calculate the credibility of the target entity and then choose the data provided by the reliable entity as the processing object.

W. Ou (✉) · M. Wei · Q. Yi · L. Xiang
Hunan University of Science and Engineering, Yongzhou, China

H. Gao, Y. Yin (eds.), *Intelligent Mobile Service Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-50184-6_1

1.2 Background

With the continuous expansion of the application scope of Internet of Vehicles, attacks also increase correspondingly. There have been too many attack accidents in Internet of Vehicles. And the intelligent vehicle has become an important target of a hacker. In the recall of Fiat Chrysler automobile company in the United States, hackers used their technologies to break into the "uconnect" system of a running Cherokee Jeep and remotely controlled its acceleration and braking system, radio station, wiper, and other equipment of this car. The BMW digital service system ConnectedDrive has been invaded. Hackers can use the vulnerability to intrude into the vehicle remotely and wirelessly and open the door easily. Considering of Tesla Model S, security experts can open the door and drive away through the loopholes in Model S; at the same time, they can also send a "suicide" command to suddenly shut down the engine when it is running normally. People pursue the convenient, efficient, and pleasant driving experience brought by the IoV, while they also concern or even fear about it.

Security of Internet of Vehicles has been paid more and more attention and becomes a new research hotspot. The UN/WP29 established a special TFSC in 2016, which has formally listed the automobile information security in WP29's work schedule. The working group will carry out related works of automobile information security in three key areas: network security, data protection or personal privacy, and software wireless upgrade. Yifei Wang, CEO of Jidou Internet of Vehicles, said their products use the method of isolating the bottom layer of cars and adding a hardware firewall to ensure vehicles' security. In case of hacker's invasion, the hacker can't get the underlying information of the vehicle and cannot control the vehicle. And the relevant data of the vehicle can't be obtained and tampered with. At the software and cloud level, Jidou has also done lots of works and formed a comprehensive set of protection. However, most of these networking devices are connected by means of OBD interface and other forms. If hackers want to attack, they need to ensure that the OBD device is in vehicle and they cannot be far away from the vehicle. So the possibility of attacks is little.

Based on the comprehensive analysis of security incidents of IoV in recent years, there are three major risks [3]: ① The vehicle networking architecture is vulnerable to challenges of information security. ② Wireless communications is facing more complex communication environment. ③ There are more potential attack interfaces in security management of the cloud platform.

In this paper we focus on two technologies: the cross-domain security technologies and the trust evaluation method. In the security model of IoV, cross-domain technologies are used to realize transactions among different domains of IoV. The method of trust evaluation is used to ensure transactions security and construct a trustworthy environment for cross-domain of IoV.

1.3 Cross-Domain Security Model of IoV

1.3.1 Division of Security Domain

In order to meet needs of safety management, according to the vehicle networking architecture [4] and safety level and safety requirements, we divide the security domain into three layers: cross-domain application layer, cross-domain network layer, and cross-domain perceptual layer. By defining three security domains, we can effectively implement definitions of security scopes to centralize management of security threats and effectively improve the efficiency of transactions between two and more chains of IoV.

The reason that the security domain is divided in this paper is that the security domain has the three following advantages: (1) Security threats faced by the same security domain are similar, which can facilitate the classification of cross-domain security and effectively solve problems of cross-domain security. (2) The security domain mainly uses trusted computing security technologies to ensure the credibility of transaction chains, but different security domains have different technologies. Combined with technologies of various security domains, it is possible to achieve effective cross-domain security services. (3) In transactions of cross-domain security model, information is input and exchanged at the beginning of the transaction, and then it is processed in the security domain [5].

Figure 1.1 shows the division and protection system of cross-domain vehicle networking security domain.

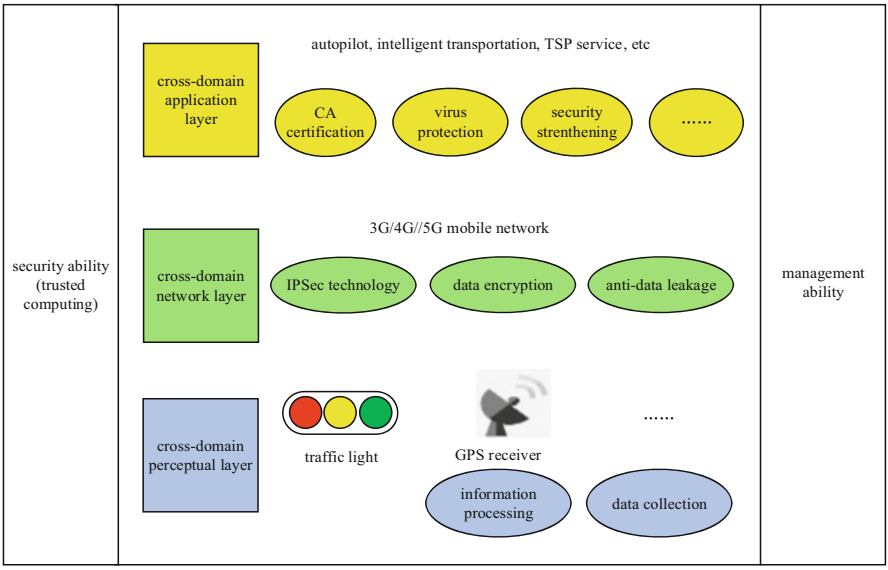

Fig. 1.1 Division and protection of security domain

1.3.2 Security Model

In order to ensure the credibility and security of IoV, we propose a cross-domain security model based on IoV. In our model the secure domain is divided into three layers, which includes the cross-domain application layer, the cross-domain network layer, and the cross-domain perception layer. The method of trust evaluation is used as the main technology of secure protection.

1.3.2.1 Model Structure

Communication characteristics of IoV restrict its security and communication ability [6]. Security ability of this model includes technologies such as trusted computing, which provides key management and identity authentication. It ensures the authenticity of vehicles' identity information in network, provides information protection, and ensures that the transmission data will not be damaged or distorted.

Cross-domain security architecture of Internet of Vehicles is shown in Fig. 1.2.

1.3.2.2 Protection Strategies of Security Domain

In cross-domain vehicle network, different security domains are facing different threats. In our paper, security problems and corresponding countermeasures are analyzed in three security domains. The three security domains include cross-domain application layer, cross-domain network layer, and cross-domain perception layer [7].

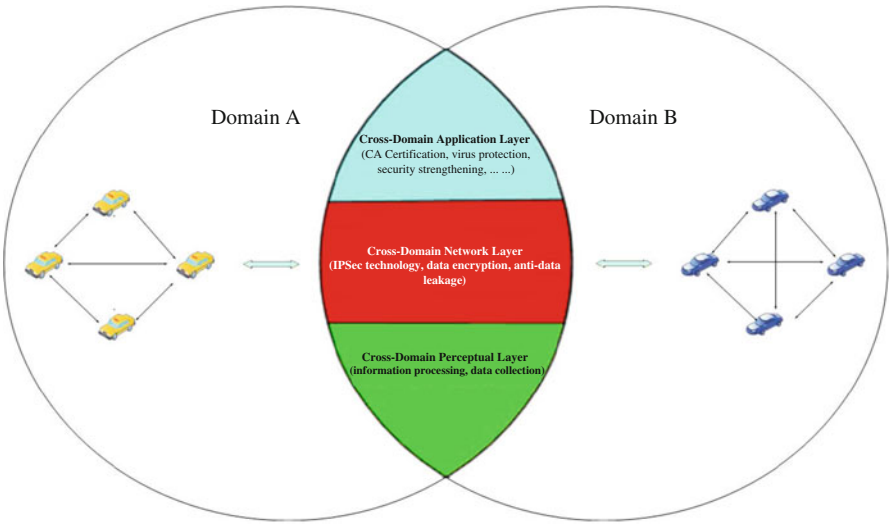

Fig. 1.2 Security architecture of Internet of Vehicles

1. **Security Protection of Cross-Domain Perception Layer**

In cross-domain vehicle networking, the perception layer undertakes the overall perception and collection of information of the onboard unit and the base station. When perceptual information is transferred to the transport layer, it is necessary to ensure the authenticity and effectiveness and availability. Base station [8] provides communication links for servers and terminals to complete interactions of data and control information between them. In general, the automatic identification technology RFID is used in the perception layer of cross-domain vehicle network. While in condition of wireless transmission, attackers can easily intercept or tamper with sensitive information when signals are transmitting between the nodes. Therefore, the protection design of cross-domain perception layer includes two parts: data collection and information processing. It is mainly guaranteed by designing a security protocol [9] which is suitable for the cross-domain perception layer of IoV. The specific process is explained as follows:

① The built-in reader in the base station continuously sends radio frequency signals covering a certain range. When a vehicle is found entering its RF range, it will send an authentication request BSHello and wait for this vehicle to receive it.
② Vehicles entering the working range of the base station will receive the message BSHello from the base station, including two random numbers R1 and R2, as well as the hash algorithms supported by the base station, which are selected for the vehicle units.
③ The onboard unit returns the message TagHello, which contains the hash algorithm selected by the onboard unit and the TagID of the electronic tag of the OBU.
④ After the base station certifies the validity of the vehicle unit, the session key for communications between two parties is calculated by a reasonable algorithm.
⑤ The base station sends the message BSResponse to inform the vehicle unit of the newly generated session key, which contains the initial key of the electronic tag of the OBU. It is used to verify the validity of the base station.
⑥ Application data are interactive between the base station and the vehicle unit, all of which use the agreed session key to encrypt application data to ensure information security.
⑦ When the onboard unit drives out of one base station range and enters another base station range, it will connect with the new base station by the same authentication way, discard the original session key, and record the new session key.

In Fig. 1.3 it shows the process of secure communication protocol between the OBU and the base station.

2. **Security Protection of Cross-Domain Network Layer**

Deployments of firewalls and intrusion detection systems can effectively prevent and detect kinds of network attacks, realize secure transmissions of vehicles' electronic information collected by front ends of IoV, and ensure the integrity

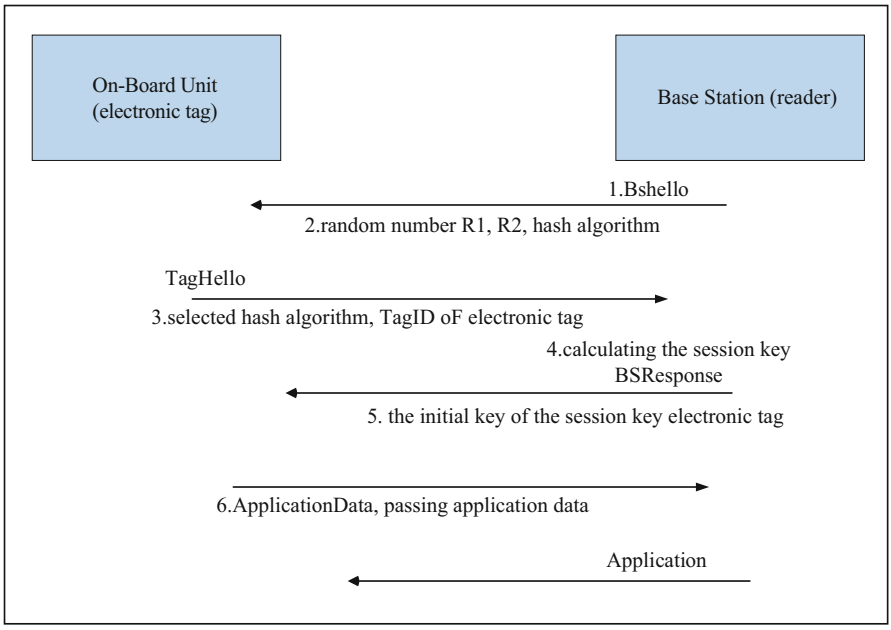

Fig. 1.3 Secure communication protocol between onboard unit and base station

and consistency of data. It is necessary to set the data center of the cross-domain vehicle networking as the center, construct the tunnel encryption system IPSec, and transmit the encrypted data collected by base stations of the cross-domain vehicle networking, so as to prevent the data illegally tampered and intercepted. In addition, for base stations transmitting information by way of wireless, the encrypted wireless tunnel should be used to upload the wireless basic information [10].

For internal security of vehicle networking [11, 12], data encryption technologies are generally used to solve problems of data confidentiality leakage. For the problem of camouflage and forgery, verifications of authenticity and legality of communication entities and data are required. For the problem of entities being tampered, effective methods are needed to protect the entity integrity. In the case of denial of service attacks, if attacks occur from outside, the attack behaviors can be detected and filtered by firewalls, gateways, etc. And the attack behaviors will be blocked out of subnet. If attacks occur in subnet, effective methods are needed to detect the attack behaviors so as to provide alarm information for users of IoV. The Internal security of IoV is directly related to the security of personal and property. A single means of protection can only meet partial needs. So it is necessary to combine a variety of different security strategies.

In Fig. 1.4 it shows the network security components in vehicles.

① Security Certification: Firstly, entities in vehicle networking are certified to protect the integrity of each ECU (electronic control unit) node. Secondly, mutual

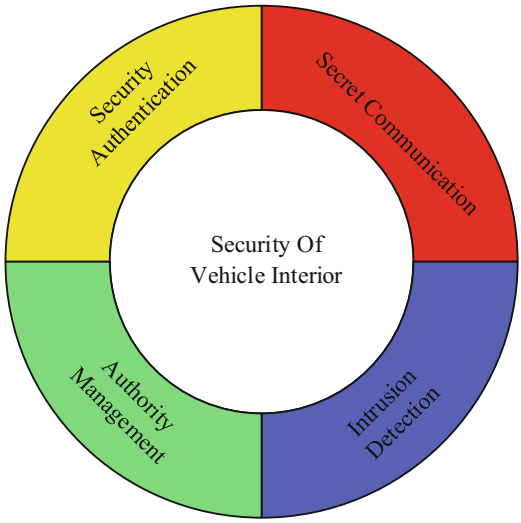

Fig. 1.4 Secure component in vehicles

certifications between each ECU node verify the compliance of each ECU node participating in communications. Based on these, the authenticity and integrity of the data in process of vehicle networking communications are verified.

② Confidential Communication: In process of communications of IoV, the data are encrypted to ensure the confidentiality.

③ Authority Management: During the design and implementation of vehicle networking, the access authority of each area should be managed and controlled. At the same time, it is necessary to filter the interactive data between subnets and control access authority of the CAN bus of the onboard entertainment system and other equipment. Access control and authority management are very important for system security.

④ Intrusion Detection: As a supplement, in addition to the passive defense of attacks, the intrusion detection mechanism should be more active. For the CAN bus of vehicle networking, by detecting whether there are illegal messages on the CAN bus, attack behaviors will be detected.

3. **Security Protection of Cross-Domain Application Layer**

① It is difficult to prevent and detect by firewalls and intrusion detections when internal users abuse network resources and use open services for unauthorized accesses, illegal operations, or unintentional damages. Therefore, it is necessary to deploy an audit system in the business application area and the storage backup area, so as to monitor and audit the access behaviors of all users.

② In condition of complex functions and huge codes, there are some security vulnerabilities and unknown "back-doors" in operating systems, database systems, application software systems, and some equipment systems, which are usually found. So it is necessary to deploy a vulnerability scanning system in the business application area and storage backup area of the data center to

detect services regularly. It is important to check configurations of operating systems and database systems of devices, potential secure hazards, and security risks. It is helpful for the security administrator to control possible safety events and eliminate potential secure hazards as much as possible. At the same time, the terminal patch distribution function and manual reinforcement should be performed.

③ In order to prevent the host system from being attacked by external or internal viruses, malicious codes, Trojans, etc., it is recommended to deploy antivirus system in network management area of the data center and install antivirus client programs on the terminal and server.

④ In order to protect the open application services of the operation data center, it needs to deploy another layer of application firewall on the basis of the external firewall protection to realize the security protection of the business application layer and avoid the system from various application attacks.

1.3.3 Construction of Inter-Domain Trust Relationship

1. **Calculation of Inter-Domain Recommendation Trust**

In security domains, inter-domain recommendation trust [13] refers to the recommendation of trust between trust agents that two nodes from different domains judge the trust of each other. If there is a direct transaction between the neighbor node and the target node, then the recommendation trust can be calculated. Conversely, if there are no direct transactions between neighboring node and target node (such as service providers), a recommendation trust path must be found by the domain agent. Here, the inter-domain trust relationship can be abstracted into a directed graph. Each node in the graph denotes a domain. The edges of the graph denote the trust relationship between each domain. Recorded as the directed graph, G = (V, e). The node (service applicant) needs to send a trust recommendation request to the domain agent and reports the basic information of the target node to the trust agent. After that, the trust agent has two things to do. One is to find the optimal path, and the other is to calculate the trust value of the target node. As shown in Fig. 1.5.

Describe the situation above as G = (V, E). We use the shortest path maximum trust method to choose the optimal path. Shown in Fig. 1.5, there are three paths: ta2-ta3-ta4, ta5-ta6, and ta7-ta8. First, choose the shortest path. We can see that ta5-ta6 and ta7-ta8 are the shortest paths. We then choose the maximum value of the trust from both paths. The calculation method of trust value is as below:

$$\mathrm{rtv}_{B_j}^{A_i} = \mathrm{dt}_{B_j}^{TA} * \prod_{k=m}^{n-1} \mathrm{rtv}_{TA_{k+1}}^{TA_k} \tag{1.1}$$

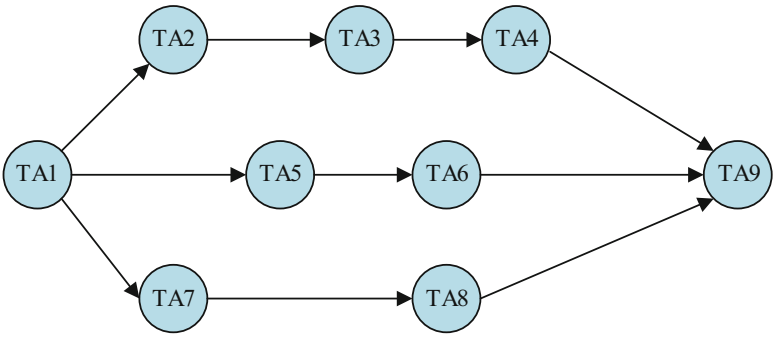

Fig. 1.5 Recommendation inter-domain trust

2. **Updating of Inter-Domain Trust**

If transactions between two nodes from different domains are successful, the recommended inter-domain trust value will increase; otherwise it will decrease. Considering of the specific increment or decrement, the number of successful or failed transactions between the nodes Ai and Bj should be the first priority.

$$\begin{cases} \mathrm{rtv}_B^A = H + \mu \times \varphi(s) & Transaction\ Successed \\ \mathrm{rtv}_B^A = H - \mu \times \varphi(f) & Transaction\ Failed \\ \varphi(x) = e^{-1/x} \end{cases} \tag{1.2}$$

3. **Trust Maintenance**

We manage the trust value of each node by setting the trust management unit. When the trust value of one node saved in unit changes, the management unit will update its trust value by the corresponding algorithm. After obtaining the direct trust, according to the calculation method of recommendation trust and overall trust, the corresponding values in the table can be obtained, and then generation and updating of the whole trust relationship table can be realized.

① **Construct Trust Relationship Table**

In each cluster, a table is designed for the fusion node to save trust values of all nodes in the cluster. According to the trust relationship between the fusion node and the source node, the corresponding trust value in this trust relationship table is determined. In addition, total trust in the table is the result of combining direct trust and recommendation trust.

In order to evaluate the trust value of a certain node, the fusion node will access and view the trust relationship table. If the trust value of a node is less than the setting threshold value, it means that this node is not trustworthy. And related communication will be terminated. Corresponding rules will be used to

Table 1.1 Trust relationship

Node	1	2	...	j
Direct trust	$DT_{p1}(t)$	$DT_{pj}(t)$	...	$DT_{pj}(t)$
Recommendation trust	$RT_{p1}(t)$	$RT_{pj}(t)$	...	$RT_{pj}(t)$
Total trust	$CT_{p1}(t)$	$CT_{pj}(t)$	...	$CT_{pj}(t)$

punish it, and the punishment record will be generated. If communications cannot be terminated, some effective evaluation methods should be referred, and related communications must be cautious.

Because of the time decay of trust, influences of time should be considered. That is, historical high trust value cannot reflect current trust of the node. Therefore, at a certain time t, the trust value obtained by the source node i from the fusion node p is expressed in the form of $(\cdot)T_{pi}(t)$ (Table 1.1).

In order to show that the fusion node p and the source node i do not have any historical interaction behaviors, the trust relationship table is initialized, and values in the table are set to the fixed values. At certain time t, when the fusion node p evaluates the source node i, the direct trust value is calculated according to the following formula:

$$DT_{pi}(t) = (1-\alpha)\, DT_{pi}(t_0) \times \beta(t - t_0) + \alpha \times LT_{pi}(t) \tag{1.3}$$

In formula (1.3), $(0 \le \alpha \le 1)$ represents weighting factor; $\beta(t - t_0)$ is the time decay factor. Considering the complexity of reality, the concept of trust level is introduced to evaluate the trust value. The trust level is defined as $LT_{pi}(t)$, which expresses the trust level of the fusion node p to the source node i at time t. It can be seen from the above formula that the effect of $LT_{pi}(t)$ on $DT_{pi}(t)$ can be adjusted by α. In Internet of Vehicles, fusion nodes use method of data analysis or system detection to evaluate specific behaviors of the source node i in a period of time $t - t_0$ and obtain the fixed parameter $LT_{pi}(t)$. At the same time, the detection system records all malicious behaviors of node i.

② Updating of Trust Value

The trust relationship table is obtained by calculations of trust values. In order to update values in the table in real time, the corresponding updating algorithm is proposed. During the first data fusion, the initial trust values of all nodes are set to 1. When the data fusion is finished, the new calculated value is used to replace current trust value in the table.

Firstly, the direct trust value of the source node i at time t is obtained according to the formula. Secondly, by analyzing the value, the node i is judged whether it is a malicious node and decided whether to continue to communicate. Finally, the evaluation results are counted, and the trust value of the source node is updated. We record the success and failure times of communications between the source node and the fusion node to evaluate the statistics. According to the results, we construct the following functions to complete the updating of trust value:

$$DT_{\mathrm{i}}(\mathrm{t}) = \begin{cases} DT_{\mathrm{i}}(\mathrm{t}) + \varepsilon_1 \mathrm{e}^{-1/x} & 0 < \varepsilon_1 < 1 \quad (F = 1) \\ DT_{\mathrm{i}}(\mathrm{t}) - \varepsilon_2 \mathrm{e}^{-1/x} & 0 < \varepsilon_2 < 1 \quad (F = 1) \end{cases} \tag{1.4}$$

In formula (1.4), ε_1 and ε_2 are the updating coefficient, x is the number of contacts, and F is the symbol of success or failure. When value of F is 1, it means communications are successful, and when value of F is 0, it means unsuccessful communications. It can be seen from the above formula that when communications are successful, direct trust values of nodes $DT_{\mathrm{i}}(\mathrm{t})$ will increase appropriately, while failure communications will cause the value to decrease appropriately.

Assuming ε_1 and ε_2 are fixed values. Times of success or failure communications directly determine increase or decrease of trust value. The larger value x, the faster the change of trust. From the subjective aspect, compared with success factors, failure factors have greater impact on the trust evaluation. So malicious nodes can be punished by setting the value of ε_2. When the direct trust value of the source node is less than the setting threshold, the trust value of the node is reduced by a large increase of ε_2; thus behaviors of malicious nodes are punished.

In summary, considering of actual communications, adjusting the update coefficient, and rewarding and punishing according to behaviors of nodes, finally the real-time updating of the trust relationship table is finished.

4. Evaluation Process

Firstly, according to similarity characteristics of information collected by adjacent nodes in vehicle networking, we perform the preliminary screening of trusted nodes. Secondly, we calculate trust values of all sensing nodes and complete the trust evaluation by grouping and fusing all nodes according to trust values.

When the source node uploads data to one node, this node needs to perform the following operations on the source node:

① Judge whether this node is an in-group node. Analyze the physical location of the source node. If the location of this node is similar or adjacent, it is an in-group node. According to the evaluation algorithm of in-group nodes, the node is preliminarily screened. If characteristics of this node are not met, further analysis will be carried out.
② Search the direct trust table. If information of this node exists, turn to ④. If not, the analysis will be continued.
③ Query the recommendation trust relationship table. If information of this node exists, turn to ④. If not, the uploaded data will be discarded, and the failure access will be recorded.
④ Trust evaluation. Calculate trust values of nodes. If the trust value is higher than the setting threshold, accept the uploaded data and turn to ⑤. Otherwise, discard the data.
⑤ Update the trust relationship table.

⑥ Remove the node from chain if the node's trust value is under the setting threshold.
⑦ Finish the evaluation and summarize all accesses.

The trust evaluation process of IoV is shown in Fig. 1.6.

1.3.4 Construction of CA Infrastructure

Framework of security infrastructure is shown in Fig. 1.7. In Fig. 1.7, the manufacturing factory is responsible for the production of related equipment of cross-domain vehicle networking, such as terminal equipment, roadside equipment, secure equipment in background system, etc. During the production process, the unique identification of the equipment will be written, which will not be changed in the whole life cycle of the equipment. In security production environment, the original authentication and authorization mechanism are written into the equipment, through which the default information of credit registration institution and credit authorization institution can be written into the equipment.

The registration authority is responsible for the certification of onboard equipment and roadside equipment. Only after the certification of relevant registration authority, the equipment can be used in the system. The registration authority first verifies whether the device is legal and then issues the certificate for the legal device, that is, the registration certificate. Authentication certificate is used to apply for terminal authorization certificate.

The authorized organization is responsible for the authorization of onboard equipment and roadside equipment. Only with the authorization of relevant authorized organization, these equipment can broadcast or receive the message of authorization permission in system. The authority first verifies the validity of the authentication certificate issued to the device and then issues the authorization certificate for the legitimate device, that is, the security message certificate or the service message certificate.

1.3.5 Basic Workflows of CA Management System of Model

1. The registration organization authenticates qualifications of equipment of IoV and service organizations and issues registration (authentication) certificates to authenticated entities
2. The equipment of cross-domain vehicle networking applies for the authorized functions of IoV to the authorized institution by the registration certificate.
3. The authorized organization issues the authorization certificate to the equipment of IoV according to its authentication certificate. Functions and safety operations that the equipment can perform are described in the authorization certificate.

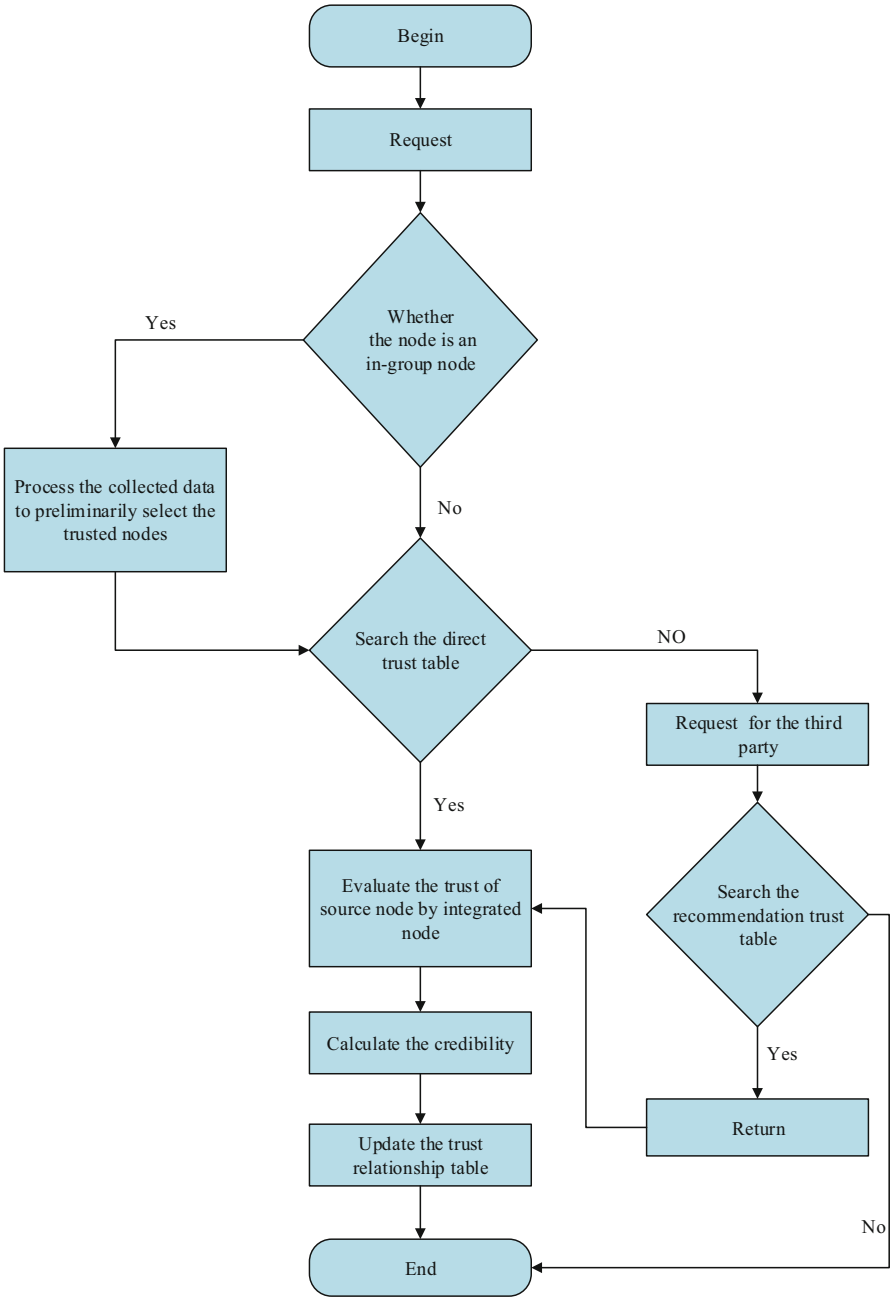

Fig. 1.6 Trust evaluation process

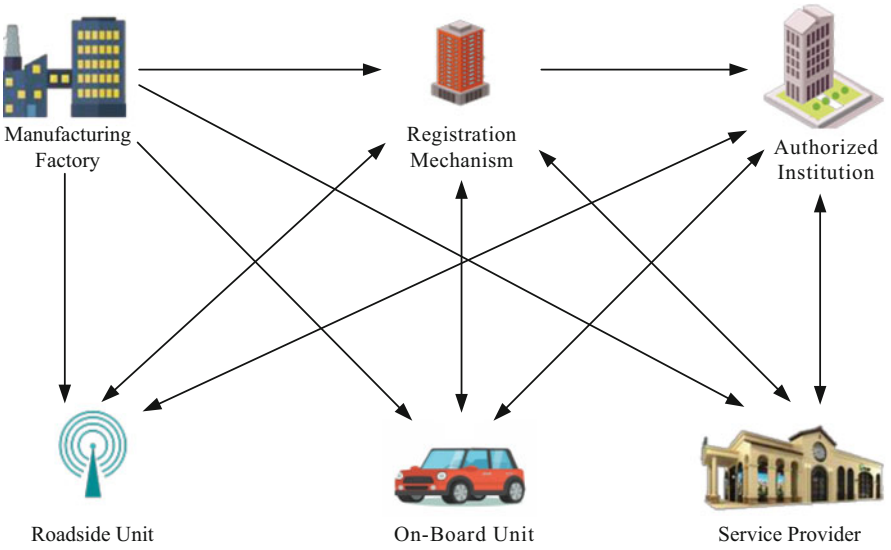

Fig. 1.7 Framework of security infrastructure

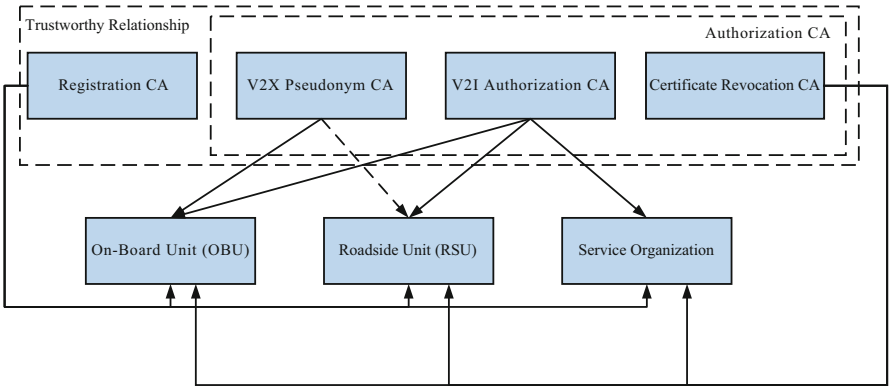

Fig. 1.8 Deployment of distributed security infrastructure

4. The equipment of IoV uses its authorization certificate and corresponding public and private keys to sign, verify, encrypt, and decrypt.

Aimed at active secure businesses for vehicles, we propose a PKI system consisting of Registration CA, V2X Pseudonym CA, V2I Authorization CA, and Certificate Revocation CA, realize active secure businesses for vehicles, and protect users' privacy in cross-domain vehicle networking. In Fig. 1.8 it shows a possible CA deployment scheme Distributed Security Infrastructure Deployment, which realizes a trusted PKI system by cross-certifications among CAs.

Functions of parts are as follows:

1. Registration CA. Responsible for issuing registration certificates to vehicle terminals, roadside units, service organizations, and other entities, which meet the conditions of network access. These entities use registration certificates to further apply to other authorized CA for certificates to achieve certain secure communication capabilities.
2. V2X Pseudonym CA. Responsible for issuing pseudonym certificates to vehicle terminals for anonymous communications in vehicle to vehicle. The certificates are used to sign and issue basic safety messages (BSM) to protect users' vehicle identity anonymously.
3. V2I Authorization CA. Responsible for issuing certificates to vehicle terminals, roadside units, and service organizations for secure communications between vehicles and roadside units.
4. Certificate Revocation CA. Responsible for issuing revocation lists of various certificates.

This distributed deployment scheme can be used to set different root CAs for different businesses. But it needs to construct trust relationships between different root CAs. It can be applied to the scenario that multiple parties jointly manage and maintain the vehicles in cross-domain of Internet of Vehicles. The schemes' advantage is that it is easy to be connected to the existing management mechanism and the corresponding functions can be added to the existing CA system.

1.4 Conclusion

In this paper we discuss related works on Internet of Vehicles. Based on these, we look forward to constructing a cross-domain security model of Internet of Vehicles. Firstly we introduce the security domain and analyze its divisions. Secondly we study the structure of cross-domain of Internet of Vehicles. Finally we divide the security domain of Internet of Vehicles into three layers which are cross-domain application layer, cross-domain network layer, and cross-domain perception layer. Also we analyze possible threats and the corresponding strategies in the three security domains and propose a cross-domain security model of Internet of Vehicles. At the same time, we study the trust relationship in IoV. The method of trust evaluation is used to ensure transactions security and construct a trustworthy environment for cross-domain.

In the next step, we will work closely with automobile manufacturers, pay more attention to industrial demands from automobile manufacturers, and seek more efficient and convenient security solutions. At the same time, we will build a test platform to promote the test verification and optimization of technical scheme in stages and provide test basis for the implementation of secure technical scheme.

Acknowledgments This project is completed under the support of the construct program of the applied characteristic discipline of Hunan University of Science and Engineering.

References

1. *Security of Internet of Vehicles [EB/OL]* (China Information and Communication Research Institute, 2017)
2. C. Shen, *Research on Communication Security and Privacy Protection in Internet of Vehicles [D]* (Beijing Jiaotong University, 2018)
3. C. Xu, Internet of vehicles information security threats and protection strategies [J]. Inf. Commun. **07**, 191–192 (2018)
4. R. Liu, *Research on Information Security and Privacy Protection Mechanism of Vehicle Network [D]* (University of Electronic Science and Technology of China, 2018)
5. Y. Jiang, *Quantitative Evaluated Model Based Security Domain between Network Security Strength and Network Delay [D]* (Hunan University of Technology, 2016)
6. W. Du, J. Deng, Y.S. Han, et al., A pairwise key pre-distribution scheme for wireless sensor networks [J]. J. ACM Trans. Inf. Syst. Secur. **8**(2), 228–258 (2005)
7. X. Wang, *Research on Model of Creditability-Based Data Fusion for Internet of Vehicles [D]* (Chang' an University, 2014)
8. Z. Yang, *Research on Security Mechanism and Key Technologies in Vehicular Networks [D]* (Beijing University of Posts and Telecommunications, 2019)
9. L. Bu, *Research on Safety Architecture of Expressway Internet of Vehicles System [D]* (Tianjin University, 2012)
10. N. Chen, Design and analysis of internet of vehicles safety protection system [J]. Comput. Dev. Appl. **27**(10), 32–34+37 (2014)
11. C. Wu. *Research on Key Technologies of Vehicle Internal Network Security for Internet of Vehicles [D]* (Southeast University, 2018)
12. X.L. Liu, *Research on OBU-based Multilevel Security Architecture and Communication Scheme for Internet of Vehicles [D]* (Jiangsu University, 2018)
13. Z. Zhang, *Study on Grid Multidimensional Trust Model Based on Fuzzy Comprehensive Evaluation [D]* (Qufu Normal University, 2014)