Dynamic Trust Model for Vehicular Cyber-Physical Systems

Hongzhuan Zhao[1,2], Dihua Sun[1], Hang Yue[3], Min Zhao[1], Senlin Cheng[1]
(Corresponding author: Dihua Sun)

Key Laboratory of Cyber Physical Social Dependable Service Computation & Chongqing University[1]
Area A, No.174, Shazheng street, Shapingba district, Chongqing, China
(Email: corresponding_d3sun@163.com)
School Architecture and Transportation Engineering & Guilin University of electronic Technology[2]
No.1, Jingji road, Qixing district, Guilin Guangxi, China
Johns Hopkins Healthcare LLC & Glen Burnie[3]
Johns Hopkins HealthCare LLC, 6704 Curtis Court Glen Burnie, MD 21060, USA
(Received Oct. 26, 2016; revised and accepted Feb. 20 & Mar. 28, 2017)

Abstract

Trust is a useful model for the interactions of Vehicular Ad Hoc Network (VANET) in Vehicular Cyber-Physical System (VCPS). Given a dynamic nature in transportation, traditional static trust models cannot effectively create the trust relationship among moving vehicles, and cannot handle quickly and dynamically the frequent vehicular interactions in a network topology. A novel trust model of VANET in VCPS is proposed to theorize the trust relationship in the dynamic traffic environment and perform a verification through an improved trust chain and some trusted computing theories. This trust model developed can improve the vehicular interaction security and the driving safety and resist malicious attacks and deceptions. Another, the vehicular trustworthiness is evaluated for the trust model development. The simulation experimental results show that the proposed trust model has a better performance for transportation applications than traditional models.

Keywords: Pervasive Trust Management Model; Trust Model; Trust-based Secure Service Discovery Model; Vehicular Ad Hoc Network; Vehicular Cyber-Physical System

1 Introduction

Transportation is a dynamic environment, consists of static roadways and moving objects (e.g. running vehicles and walking pedestrians) [39]. The dynamic transportation environment has a requirement on VANET for an efficient and effective interaction or communication among vehicles. But traditional methods in the wireless networks view moving vehicles as static or low-speed moving nodes. Using VANET the Vehicle to Vehicle (V2V) communication can obtain sufficient information in traffic cyber systems, and can realize a cooperative driving in traffic physical systems [16]. VCPS is the integration of the vehicular cyber system and the vehicular physical system [30, 43]. VANET in VCPS contains a series of wireless and independent moving nodes (i.e. vehicles) and temporarily form a network without a pre-existing infrastructure.

Intelligent Transport System (ITS) consists of different transportation systems, such as advanced traveler information system, advanced traffic management system, advanced transit system, and so on [35, 38]. For the development of the next generation ITSs, VCPSs, with the spread of mobile computing and communicating devices, are expected to solve some problems related to dynamic traffic moving objects [24]. Another, there are some security and trust problems related to VANET. The potential spoofing, eavesdropping, denial-of-service and impersonation attack lower the user trust on the cyber system services, and cause the safety and efficiency problems on the physical systems [7]. The trust approaches of static nodes, such as PKI [5] and CA [8], cannot meet with the demand of dynamic vehicular interactions.

Given a dynamic nature in transportation, it is hypothesized that a more efficient VANET in VCPS is required to guarantee dynamic trust interactions among vehicles with the adequate security and reliability [21]. The aim of this paper is to innovatively design a distributed dynamic trust model to describe the logic relationship among moving vehicles. The trust model can resist malicious attacks and deceptions based on the evaluation and certification mechanisms. Moreover, the proposed distributed trust architecture can reduce the communication load of moving vehicles.

Section 2 reviews the related literature. Section 3 depicts the detailed description and analysis of the trust

model process. The experimental simulation analysis is detailed in Section 4. Finally, Section 5 gives a brief discussion and some concluding remarks.

2 Literature Review

Some researches discusses the security issues and the potential solutions for the trust model development. For instances, the research [17] offers a novel communication method that cannot easily be subjected to network sniffing, thereby addressing the issue of security. Nevertheless, the scheme does not prevent malicious nodes from selectively forwarding packets or from other malicious behavior; although the study [6] gives an improved scheme to solve the impersonation attack and a malicious user can generate a valid signature on behalf of the other vehicles, the mechanism does not consider every nodes function and the global characteristics adequately; a secure and distributed certification system architecture for safety message authentication in VANET [26]. Moreover, this system can resist the false public-key certification. However, this study lacks the trust process in the entire system; the paper [9] uses the confidence intervals to manage uncertain information in the assessment of trust and reputation in ubiquitous network environments. Unfortunately, the characteristics of the focused environment has not been discussed in this study; in terms of the message receiver's authenticity and user privacy preservation, the research [19] eliminates the vulnerabilities in Chuang-Lee's scheme [11], and creates a trust-extended authentication scheme in VANET. Yet this research considers a little about the service levels.

In terms of the location-based verification security, the authors in the paper [28] make a summary about some previous researches related to map or Geographic Information Systems (GIS) [1, 12, 14, 22, 41, 42], and then proposes the Location Information Verification cum Security (LIVES) based on Transferable Belief Model (TBM). This map-based model includes two verification layers: the first layer depends on the concept of virtual tiles on roads and received signal strength; the second layer depends on the trust of neighboring vehicles computed using TBM. LIVES makes an improvement on the verification security in the map-based realistic network environments. However, all of the above location-based or map-based models ignore the time dimension or do not adequately employ time parameters for the trust model development. Considering the security verification of the real-time vehicular networks, these models are difficult to meet with the demand of dynamic vehicular interactions.

Another, data mining algorithms are applied into trust models. Take, for examples, the paper [29] creates a trust-based authentication scheme for the cluster-based VANETs. For the selection of cluster heads, the trust degree of each node is estimated based on the vehicles clustered. But it lacks the process of local interaction among mobile nodes; the study [4] utilizes a weighted clustering trust model algorithm for the development of Mobile Ad Hoc Networks (MANETs) trust. However, this study does not describe the local behaviors in details; the paper [32] uses the logic regression to model dynamic trust for service-oriented MANETs and dynamically estimate the service provider trust depending on the distinct behavior patterns [20]. But the proposed model does not detail the global trust relationship; a fuzzy-based dynamic trust model with the time slice scheme is developed to guarantee that a reliable node possess enough time to enjoy its services [33]. Nevertheless, the trust relationship is ignored.

Besides the above two dynamic trust models, Pervasive Trust Management (PTM) [3] describes dynamic inter-domain and trust model with the support of the Dempster-Shafer evidence theory, and uses the probability weighted average method for evaluating trustworthiness. PTM has several advantages: a) the trustworthiness of PTM rises slowly with the increase of the real trust behaviors and reduces sharply with the increase of the malicious trust behaviors; b) the trustworthiness changes dynamically according to different time and context information, and shows the dynamic characteristics of the trust process; and c) the algorithm can suitably describe the characteristics of VANET in VCPS. The disadvantages of PTM include: a) it cannot fit different requirements in various environments because of the static trust domain; and b) it cannot handle the uncertainty of certain nodes certification if missing data.

As a hybrid model, Trust-based Secure Service Discovery Model (TSSDM) [2] allows both of secure and non-secure service discoveries to handle the security issues related to the sharing communication and service. This model also permits mutual trust for the service discovery and sharing, even the service sharing with unknown entities. TSSDM have the following features: a) due to the good adaptive ability, different service levels from TSSDM have different trust levels. Also, different service levels provide different security levels. But the information load is heavy; and b) when the unknown entities join in TSSDM, this model would offer the risk certification mechanism to verify the unknown entities. However, the trustworthiness calculation only depends on the service time.

The above overall analysis reveals that previous research studies have not well developed the distributed trust model for dynamic vehicular interactions and service requirement discoveries, and have not adequately explored the evaluation and certification mechanisms for the malicious attacks and deceptions of moving vehicles. The trust model developed is expected to avoid the disadvantages of these models, but also keep their advantages. In contrast to existing models, PTM and TSSDM is better that the other models for transportation moving object-based trust verification. It is necessary to design experimental analyses for the comparison of the proposed model with both PTM and TSSDM. The next section gives the processes of the proposed trust model in details.

3 Trust Model Processes

There are four processes in the proposed trust model, and they are the trusted VANET initialization in VCPS, the service requirement discovery, the distributed evaluation and certification, and the trust transition based on the computing theories [27, 31]. The execution of these trust processes can achieve the vehicular verification and make the whole VANET trusted.

3.1 Trusted VANET Initialization

The system initialization dealer has a long-term stable trust relationship with vehicles [13]. Each vehicle obtains its own private share from the system initialization dealer. Generated by the system initialization dealer, each private share $S(i)$ is a randomly $(k-1)$ degree polynomial function, which is shown as follows:

$$S(i) = a_0 + a_1 x^1 + ... \quad + a_{k-1} x^{k-1} (\mathrm{mod}\varphi)$$

Where i is the unique identifier of Vehicle i in VANET; each private share is evaluated as $S(i)$; φ is a large prime number; and the initial key of the trusted VANET is $S_0 = a_0(\mathrm{mod}\ \varphi)$.

When an unknown vehicle was accessing the trust system, the system would send a public key with a trust evidence to the system initialization dealer, and request a certification for this public key. The system initialization dealer verifies the certification request via the calculation of the partial private share [10] in Equation (1):

$$\begin{aligned} S(i|j) &= S(j) \prod_{r=1, r\neq j}^{k} \frac{i-r}{j-r} (\mathrm{mod}\varphi) + \\ &\quad \sum_{r=1, r\neq j}^{k} \eta(j-r) S(jr) (\mathrm{mod}\varphi). \quad (1) \end{aligned}$$

$$\eta(j-r) = \begin{cases} 1, & j-r > 0 \\ 0, & j-r = 0 \\ -1, & j-r < 0 \end{cases} \quad (2)$$

Where j is the ID of the system initialization dealer; each pair of vehicles$(j,\ r)$ in the system exchange a number *S(jr)*; and *(j-r)* is the sign function.

After all vehicles obtain their individual private shares, each node of VANET would generate a partial certificate to other nodes. It would form a trust graph composed of partial certificates. Given that there are sparse social trust relationships among initial vehicles, the system would be fully functional, and no infrastructure would be expected, the system dealer would not be needed any longer [25]. Figure 1 illustrates the process of the trusted VANET initialization with the trust graph.

3.2 Service Requirement Discovery

The main role of the service requirement discovery is to handle the service applications. As a host, the trusted vehicle of VANET in VCPS evaluates if the trustworthiness of the guest vehicle satisfies the requirements of a certain service level or not via the trust certification. The host would gain the recommendations from the neighboring vehicles, and the recommendation information is the estimation information of the guest trustworthiness. It is the initialization mechanism for the trustworthiness of the unknown applied vehicles.

The different service levels have different security levels, and the security level Q_i maps the required service level S_i. The security factor with the range [0, 1] indicates the relationship between Q_i and S_i. Also, the proposed trust model uses a communication encrypted threshold CT and an authorized intervention threshold AT. When x>CT, the communication data would be encrypted; when x>AT, even though the guests satisfy the trust verification requirements, the interaction would be authorized by the host [23]. The trust mapping between Q_i and S_i is defined as follows:

$$Q_i(x) = \begin{cases} S_n, a_n < x \leq 1 \\ S_{n-1}, a_{n-1} \leq x < a_n \\ ... \\ S_k, A_T < x \\ ... \\ S_{k-1}, C_T < x \\ ... \\ 1, a_1 \leq x < a_2 \\ 0, 0 \leq x < a_1 \end{cases}$$

The security requirements are used for the selection of the above independent coefficients $a_1, a_2, ..., a_{n-1}, a_n \in [0, \varphi - 1]$. The security factors from the security requirements would improve the flexibility and self-adaptability of the proposed trust model. Besides, the communication encryption threshold and the authorized intervention threshold would determine different security and service levels.

3.3 Distributed Evaluation and Certification

On the basis of PTM and TSSDM, the collaborative trustworthiness between the host and the guest is estimated using the metrics, these metrics are related to the recommendation information from neighbored vehicles. The combination of the evaluation and certification mechanisms would be valid to identify the false recommendation. Given that each vehicle has a unique ID, the number of vehicles in VANET is n, and Vh_1,Vh_2,...,Vh_n as a vehicle set, the trust set of VANET in VCPS is given as [44]:

$$\begin{aligned} T_i = &[t(Vh_i, Vh_1) t(Vh_i, Vh_2) \\ &..., t(Vh_i, Vh_{i-1}), t(Vh_i, Vh_{i+1}), ..., t(Vh_i, Vh_n)] \end{aligned}$$

Where t(Vh_i, Vh_k) is the trustworthiness between the host Vh_i and the guest Vh_k, t(Vh_i, Vh_k) = null means

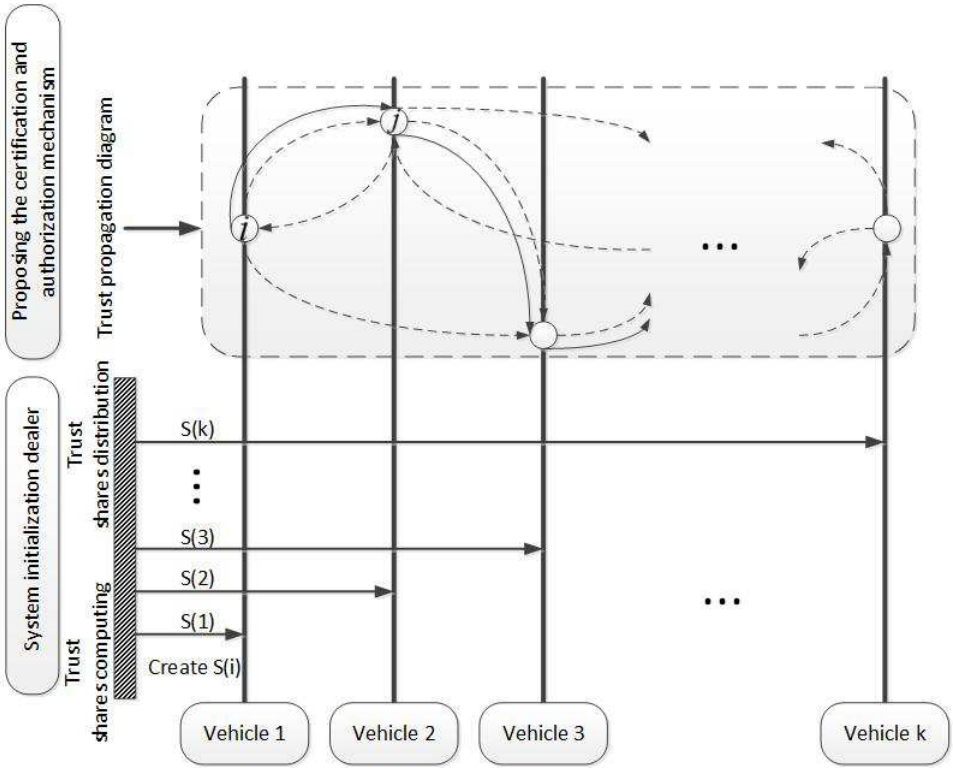

Figure 1: Trusted VANET initialization process

that the host Vh_i does not know the guest Vh_k for $1 \leq k \leq n$, $k \neq i$.

The vehicle set T_i denoted by S_{T_i} is the set of all the vehicles T with $t(Ti, T) \neq null$. The common vehicles set of T_i and T_j are given as follows:

$$\begin{cases} C(T_i,T) = [t(T_i,T_{k_1}), t(T_i,T_{k_2}), ..., t(T_i,T_{k_m})] \\ C(T,T_i) = [t(T_i,T_{k_1}), t(T_i,T_{k_2}), ..., t(T_i,T_{k_m})] \\ (T_{k_1}, T_{k_2}, ..., T_{k_m}) = S_{T_i} \bigcap S_{T_j} \end{cases}$$

Where $C(T_i, T)$ is the trustworthiness of T_i for all the common vehicles on T_i and T_j , and $C(T, T_i)$ is the trustworthiness of the common vehicles on T_i. This method can find the common vehicles on T_j.

The collaborative trustworthiness has a transitive property. If A_1 trusted A_2 and A_2 trusted B, then A_1 would trust B. Given that A_2 was an intermediary note, if A_2 was maliciously attacked and tampered, the entire trust chain from A_1 to B would be invalid. Figure 2 gives the comparison of the collaborative trust mechanism and the single trust mechanism.

The trustworthiness recommendation for the interaction between T_i and T_j is described as follows:

$$RIV(T_i,T_j) = \begin{cases} \frac{\gamma \cdot \overrightarrow{C(T_i,T)} \cdot \overrightarrow{C(T,T_j)}}{m}, S_{T_i} \bigcap S_{T_j} \neq \phi \\ 0, S_{T_i} \bigcap S_{T_j} = \phi \\ (m = |S_{T_i} \bigcap S_{T_j}|) \end{cases}$$

Where γ is the weight of the trustworthiness recommendation; $\overrightarrow{C(T_i,T)} \cdot \overrightarrow{C(T,T_j)}$ is the dot product of the collaborative trustworthiness betweenT_i and T_j; and $0 \leq RIV(T_i,T_j) \leq 1$ for any two trust sets T_i and T_j.

Given that and represent the number of the interactions between T_i and T_j with the limit of m, the confidence FIV on RIV for the vehicle sets T_i and T_j is given as follows:

$$\begin{cases} FIV(T_i,T_j) = \frac{(1-\frac{1}{m+\lambda})+(1-\frac{1}{N_{T_i}+\lambda})}{2} \\ FIV(T_j,T_i) = \frac{(1-\frac{1}{m+\lambda})+(1-\frac{1}{N_{T_j}+\lambda})}{2} \end{cases}$$

λ is an attenuation factor, the more trustworthiness comes from the higher number of common vehicles in both of sets and the higher number of the historical interactions among the vehicles. The historical interaction evaluation of T_i and T_j is described in the Equation (3):

$$HIE(T_i,T_j) = 1 - \frac{1}{\max\{\beta \cdot [\omega_{SI} SI(T_i,T_j) - \omega_{FI} FI(T_i,T_j)], 0\} + 1}, \quad \lambda = 1 \tag{3}$$

Where β is the time sensitive factor, $SI(T_i,T_j)$ is the number of successful historical interactions using the perspective of T_i, $FI(T_i,T_j)$ is the number of failed interactions. It is the same to define T_j.

As the time stamp between vehicular sets P and T, $\tau_{(P,T)}$ is the interaction weight at the current time, but it would be smaller with the elapsing time. The evaluation

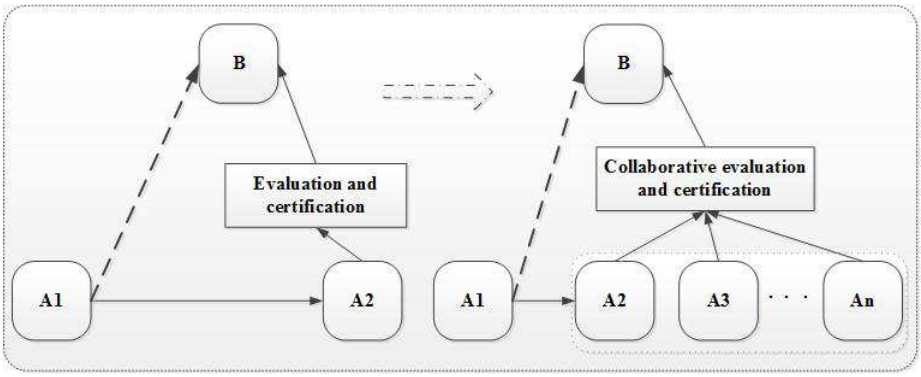

Figure 2: Collaborative and single trust mechanisms

of T_i and T_j is described as follows:

$$TTE(T_i, T_j) = \frac{m}{\sum_{z=1}^{m} \frac{\triangle\tau(T_j, T_{k_z})}{\triangle\tau}}$$

Where $\triangle\ \tau$ is the threshold time interval; the interaction between T_i and T_j at time τ; and $\triangle\ \tau(T_i, T_{k_z}) = \tau - \tau(T_i, T_{k_z}), \{T_{k_1}, T_{k_2}, ..., T_{k_m}\} = S_{T_i} \bigcap S_{T_j}$. The trustworthiness is evaluated by the weighted arithmetic mean of *RIV, FIV, HIE, and TTE.*
The trustworthiness of T_i and T_j is calculated in the following equation:

$$TR(T_i, T_j) = \frac{w_1[RIV(T_i, T_j)](\frac{FIV(T_i, T_j) + TTE(T_i, T_j)}{2}) + w_2[HIE(T_i, T_j)]}{w_1 + w_2}$$

3.4 Trust Transition

The improved Noninterference model [18] is used to design the trust transition mechanism with the support of the trusted computing theories. S represents the trust system of VANET, and the trust system contains the evaluated and certified vehicles, i.e. Vh_1, Vh_2,..., Vh_n.

$$S = \{Vh_1, Vh_2, ..., Vh_n\}$$

D is the true subset of S, D is the security domain mapped to the vehicles of the trust VANET. The trust relationship of VANET is described in Equation (4), and $Vhi \rightarrow Vhj$ means that Vhi has successfully verified Vh_j (i.e. Vh_i trusts Vh_j).

$$Vh_i \rightarrow Vh_j \in D \times D. \quad (4)$$

The trust chain of VANET is described in Equation (5), and Vhroot is the root of the trust delivering system and it is the beginning point of the trust chain.

$$Vh_{root} \rightarrow Vh_1 \rightarrow Vh_2 \rightarrow \cdots \rightarrow Vh_n, Vh_i \subset D. \quad (5)$$

The trust chain can be realized based on the preloading measurement technology of the trust computing theory (see Equation (6)). Remark(Vh_i,Vh_j) is the remark operation of the Vh_j verification using Vh_i, and expect(Vh_j) is the expected trustworthiness of Vh_j.

$$Remark(Vh_i, Vh_j) = expect(Vh_j) \Rightarrow Vh_i \rightarrow Vh_j. \quad (6)$$

Similar to the expected value expect(Vh_j), when Vh_i got the remark value of Vh_j via the remark operation, Vh_i would trust Vh_j. The trust relationship of VANET would be delivered from Vh_i to Vh_j. The role of the host would be delivered to Vh_j.

If $\forall Vh_1, Vh_2, Vh_3 \in S$, $[Vh_i \rightarrow Vh_j]$, $Vh_1, Vh_2 \in Vh_i$,$Vh_3 \in Vh_j$ and $Vh_1 \sim\succ Vh_2 \bigcup Vh_2 \sim\succ Vh_3 \Rightarrow Vh_1 \sim\succ Vh_3$, then the trust system of VANET would produce the unexpected interference via the transitivity between different domains and the trust chain would be invalid.

If $\forall Vh_i, Vh_j \subset D$, $Vh_1, Vh_2 \in Vh_i \bigcup Vh_3 \in Vh_j$ and $Vh_1 \sim\succ Vh_2 \bigcup Vh_2 \sim\succ Vh_3 \not=> Vh_1 \sim\succ Vh_3$, then $Vh_i \xrightarrow{intransitive\ noninterference} Vh_j \in D \times D$, and $Vh_i \xrightarrow{intransitive\ noninterference} Vh_j$ would be the intransitive noninterference relationship in $D \times D$. So there is not any unexpected interference in the trust VANET.

The intransitive noninterference relationship describes that there is just the direct interference relationship among the vehicles of VANET in VCPS. If the original trust chain of Trusted Computing Group (TCG) lacked enough security then it would cause an invalid trust chain, as described in Equation (7):

$$Remark(Vh_i, Vh_j) = expect(Vh_j) \not=> Vh_i \rightarrow Vh_j \quad (7)$$

With the aim of guaranteeing that vehicles move without interference and the vehicular data flows between different clusters in the trust VANET are restricted by a certain security policy, the trust chain delivery model is developed to construct effectively the trust chain. The proposed trust chain delivery model is given as follows:

$$Vh_i \xrightarrow{intransitive\ noninterference} Vh_j \bigcup Remark(Vh_i, Vh_j) = expect(Vh_j) \Rightarrow Vh_i \rightarrow Vh_j.$$

The trust chain delivery model reveals that the trust chain can be constructed and the trust relationship can be delivered, when vehicles communicate with each other and satisfy the intransitive noninterference relationships. The theorem development would fit the logic relationship of the intransitive noninterference, and guarantee the valid trust chain establishment and delivery. The four theorems are described as follows:

1) The domains of the trust VANET should keep the output-consistence. It means that the output influence of an inner interaction only relays on the view of the interaction domain in the trust VANET;

2) Caused by the interaction among vehicles, the influence of the trust VANET is just related to the previous view of the interaction domain, as described in Equation (8):

$$\begin{aligned} &Vh_i \overset{dom(Vh_{\text{int}eraction})}{\sim} Vh_j \wedge \\ &(contents(step(Vh_i, Vh_{\text{int}eraction}), Vh_{guest})) \neq \\ &contents(Vh_i, Vh_{guest}) \\ &\vee contents(step(Vh_j, Vh_{\text{int}eraction}), Vh_{guest}) \neq \\ &contents(Vh_j, Vh_{guest})) \\ &\rightarrow contents(step(Vh_i, Vh_{\text{int}eraction}), Vh_{guest}) = \\ &contents(step(Vh_j, Vh_{\text{int}eraction}), Vh_{guest}) \end{aligned} \tag{8}$$

Where contents(step(Vh_i, $Vh_{interaction}$), Vh_{guest}) is the trustworthiness of the guest Vh_{guest} in the state step(Vh_i, $Vh_{interaction}$) of the trust VANET, the single-step state transition function step(Vh_i, $Vh_{interaction}$) is the state of Vh_i after the interaction $Vh_{interaction}$ occurring among vehicles;

3) If the interaction among vehicles changed the value of the guest, then the interaction domain would modify the states of the guest, as described in Equation (9):

$$\begin{aligned} &(contents(step(Vh_i, Vh_{\text{int}eraction}), Vh_{guest})) \neq \\ &\qquad contents(Vh_i, Vh_{guest}) \\ &\rightarrow Vh_{guest} \in alter(dom(Vh_{\text{int}eraction}), Vh_i) \end{aligned} \tag{9}$$

Where alter(dom(Vh_i, $Vh_{interaction}$) is the altering set of the guest, and it can be modified under the state of Vh_i in dom($Vh_{interaction}$) of the trust VANET;

4) Any two domains in the trust VANET should satisfy the logic relationship of Equation (10):

$$\begin{aligned} &\exists Vh_{guest} \in N, Vh_{guest} \in alter(Vh_u, Vh_i) \wedge \\ &Vh_{guest} \in observe(Vh_v, Vh_i) \rightarrow \tilde{u} > v \end{aligned} \tag{10}$$

Where Vh_u and Vh_i are two interaction domains, observe(Vh_v, Vh_i) is the observing set of the guest, and this observing set can be monitored under the state Vh_i of the trust VANET in dom($Vh_{interaction}$).

Given that VI_c is the process of vehicular information collection, VI_s is the process of the vehicular information spreading,VI_p is the process of vehicular information processing and VI_d is the process of vehicular decision-making, the trust chain delivery model can be given in Equations (11) and (12). And the trust transition model of VANET in VCPS is shown in Figure 3:

$$\begin{aligned} &(VI_c^{root} \rightarrow VI_s^{root} \rightarrow VI_p^{root} \rightarrow VI_d^{root}) \bigcup \\ &VI_c^i \rightarrow VI_s^i \rightarrow VI_p^i \rightarrow VI_d^i \end{aligned} \tag{11}$$

$$Vh_{root} \bigcup Vh_1 \rightarrow Vh_2 \rightarrow \cdots \rightarrow Vh_n. \tag{12}$$

As the trust chain extends, the axiom of the trust decays is measured by the trustworthiness of a route, and the trust information of a remote vehicle is propagated by intermediate vehicles [34]. The trustworthiness $TC_{rn(cd)}(t)$ of the chain is calculated below:

$$TC_{rn(cd)}(t) = \prod (TC_t(T_i, T_j) | T_i, T_j \in Dand\ T_i \rightarrow T_j)$$

Where *Tr(c)* is the root, *Tn(d)* is the end of the trust, T_i and T_j are any two adjacent interaction vehicles, and $T_i \rightarrow T_j$ means that T_j is the next-hop node of T_i. T_r represents Vhroot, Tc represents VI_c^i, T_n represents Vh_n and T_d represent VI_d^i.

In addition, all intermediate vehicles are considered for the trustworthiness evaluation in the trust chains. The load conditions of VANET may be changed occasionally during the trustworthiness propagation, the trust would be changed accordingly. The latest arriving information would be used to calculate $TC_{rn(cd)}(t)$ of the trust chain, the scheme is adaptive to the change of VANET conditions, and the source information can be correctly delivered for a "propagation" in a timely manner. If one vehicle cheated another vehicle using false information when they interact with each other, vehicles could not accurately perceive current situation, the false information with security problem in cyber system may cause some physical safety problems, such as vehicle rear-end, crash, rollover, and so on.

4 Experimental Simulation Study

The simulation and calculation tools (Opnet Modeler 14.5 and Matlab 2014a) are used to analyze the characteristics of the trust model. There are totally 25 times simulation experiments for the calculation of the average trustworthiness. In the spatial-temporal interactions of VANET in VCPS, and are two time conversion factors, and both of their initial values are 0.5. The initial value of the spatial factor is 0. When the service level requirement factor S is 0.5, the host vehicle A and the guest vehicle B implement two times interaction during their initialization. The first interaction is the increasing trustworthiness behavior and

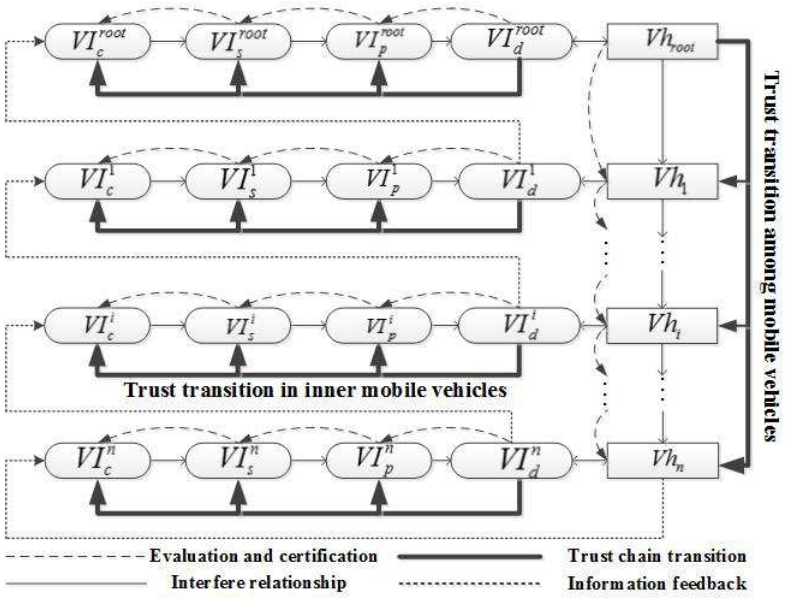

Figure 3: Trust transition model of VANET in VCPS

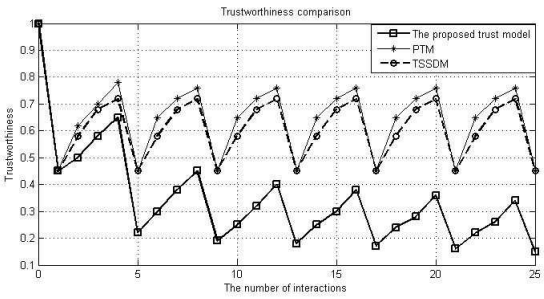

Figure 4: Capacity of resisting malicious deception in time dimension

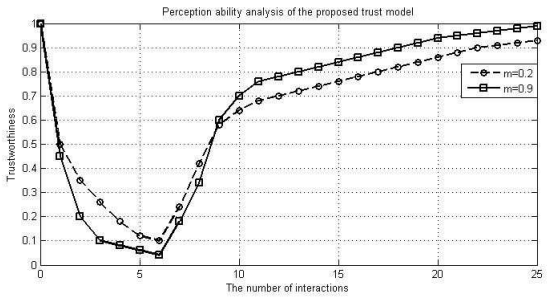

Figure 5: Perception ability in spatial dimension

the second interaction is the decreasing trustworthiness behavior. When the service level requirement factor S is 0.2, the guest B responses to the low service level requirements and continuously interacts with the host A for three times for the improvement of its trustworthiness. After obtaining the high trustworthiness, the guest B attacks the host A at a high service level domain, when the service level requirement factor S is 0.8 [15]. Figure 4 illustrates that the trustworthiness values of the proposed trust model, PTM and TSSDM between the host A and the guest B in a time dimension. The guest trustworthiness in the first scenario is some lower than two other trust models. With the trust increasing behaviors on the low service level requirements, the trustworthiness accumulation of the malicious node is much slower. With the trust decreasing behaviors on the important high service level requirements, the trustworthiness has a sharp decrease. So the proposed trust model can better resist the malicious deception in time.

Another, in a spatial dimension the proposed trust model uses the security sensitive factor to describe the perception ability of the vehicular status and traffic environment in VANET. The initialization information of the parameters is that the host vehicle A and the guest vehicle B implement their interaction for two times with λ =0.5, S=0.5 and m=0.5. One interaction is an increasing trustworthiness, and another interaction is a decreasing trustworthiness. And then they have six interactions in the decreasing trustworthiness behaviors and nineteen interactions in the increasing trustworthiness behaviors for both of m=0.2 and m =0.9 (see Figure 5). The interaction information and the tendency of the trustworthiness between A and B, the data with m=0.9 is more sensitive than m=0.2. The trustworthiness of the guest more sharply reduces with the decreasing trustworthiness interaction and more quickly increases with the increasing trustworthiness interaction in spatial dimension. The proposed trust model uses the service level requirement factor S to describe the perception ability in different service levels. It means that different service qualities may have different trustworthiness values during the interac-

tion among vehicles. The initialization information of the parameters is that the initial values of the time factors (i.e. β and λ) are 0.5, and the initial value of the spatial factor is 0. The host A and the guest B have two interactions when S=0.5. One interaction is the increasing trustworthiness behavior, and another interaction is the decreasing trustworthiness behavior. After that, the host A and the guest B have twenty-five interactions (see Table 1).

Table 1: Interaction parameters of Host A and Guest B

Interaction times	Service level requirement factor S	Trustworthiness decreasing (0) or increasing behaviors (1)
1	0.3	1
2	0.2	0
3	0.8	1
4	0.9	0
5	0.3	1
6	0.5	0
7	0.9	1
8	0.8	0
9	0.7	1
10	0.8	0
11	0.5	1
12	0.8	0
13	0.7	1
14	0.9	0
15	0.5	1
16	0.8	0
17	0.7	1
18	0.8	0
19	0.9	1
20	0.8	0
21	0.5	1
22	0.9	0
23	0.8	1
24	0.7	0
25	0.6	1

Figure 6 describes the changes of the trustworthiness between the host A and the guest B during the interaction process. The trustworthiness curve of the proposed model has a sharper fluctuation than both of PTM and TSSDM. It means that the proposed model is more sensitive to the service level requirement factor than PTM and TSSDM.

For the comparison of the proposed trust model with PTM and TSSDM in different maximum vehicular velocities. The time stamp period is denoted by (P,T), and the attenuation factor is denoted by . The moving vehicle uses the random waypoint model, and in this model each packet starts from a location to another at a random velocity [34]. The random waypoint model is used to describe the moving vehicle and Table 2 lists the fixed simulation parameters. As shown in the study [24], the simulation area consists of 66 sub-grid areas, and the range of communication endpoints (R) is 250 m.

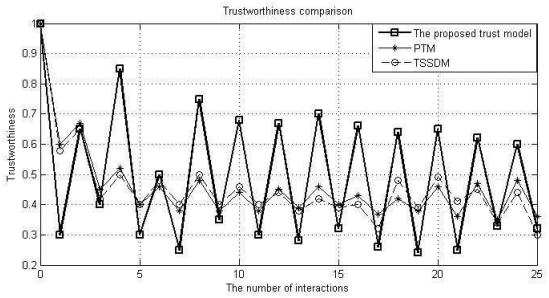

Figure 6: Perception ability in service levels

Also, three metrics, such as packet propagation ratio, average V2V latency and throughput of VANET, are used to evaluate the proposed model [33]. The calculation method of packet propagation ratio is that the number of the data packets delivered to the destination vehicles is divided by those sent by root vehicles; average V2V latency is the average time taken by the data packets from the starting points to the destinations; and throughput of VANET is the amount of the interaction information between the starting points and the destinations.

The propagation ratio of the proposed trust model is higher than PTM and TSSDM in any maximum velocity from 0 m/s to 30 m/s (see Figure 7). The packet propagation ratios in the three models have a more significant difference at low maximum velocities than at high maximum velocities. It means that the proposed trust model is more stable, this model can propagate more information to adjacent vehicles or infrastructures in a short time and can adapt to the dynamic changes related to the topology of the VANET. Figure 8 illustrates that the average V2V latency values rise with the increase of the maximum velocity. During the vehicular initialization of the trusted VANET, the trust chain roots are invalid more remarkably, and the trust chain roots initiate more trust chain rediscoveries before data interactions. The proposed trust model has a lower average V2V latency than PTM, and has a similar average V2V latency to TSSDM. It reveals that the proposed trust model can resist malicious deception more sensitively in the simulations than PTM, and it would be useful for the delay risk decline in the delivery of the failed interactive information packets. A lower packet propagation ratio means a less throughput of VANET. Figure 9 shows that the proposed trust model has a higher throughput than PTM and TSSDM over the whole range of the maximum velocity. It shows that the proposed trust model can bear more complex interaction contents, and it would reduce packet loss ratio of regional information spillover. From the above overall comparison the proposed model have a better performance than two other models in the experimental simulation analysis.

Table 2: Fixed simulation parameters

Parameters	Meaning	Value
simulation time	he period of simulation process	800 s
the number of nodes	the number of simulation vehicles	25
moving vehicular model	each packet starts from a location to another at a random speed	random waypoint
pause time	once the destination is reached, another destination is randomly chosen after a pause time	5 s
packet size	data payload size	512 bytes
$\tau_{(P,T)}$	the period of time stamp	30 s
λ	the attenuation factor	0.9
experiment times	the number of simulation times	25

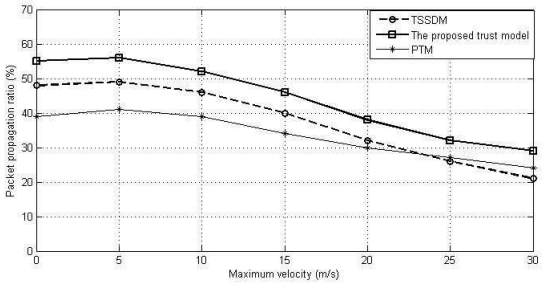

Figure 7: Packet propagation ratio

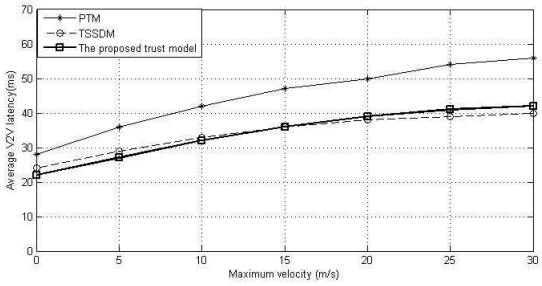

Figure 8: Average V2V latency

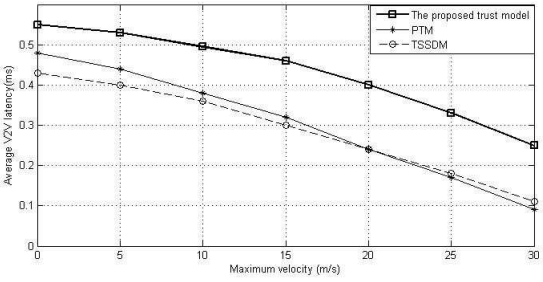

Figure 9: Packet propagation ratio

5 Concluding Remarks

This study discusses the development of the dynamic and distributed trust model for VANET in VCPS. This proposed trust model can describe the dynamic trust relationship among moving vehicles using the trust chain with a high accuracy. The trust chain can propagate the trust relationship based on the cryptography technology and the intransitive noninterference theory. Also, the verification mechanism developed can improve the reliability of the trust system. In addition, the distributed trust architecture in this new trust model can reduce the vehicular communication loads. The further research may focus on the combination of artificial intelligence and spatio-temporal databases [36, 37, 40] for the development of the proposed dynamic trust model in this study.

Acknowledgments

The authors gratefully acknowledge the research funding support from the National Natural Science Foundation of China (NSFC) (Grant No. 61573075), the core projects of Chongqing City 151 science and technology (Grant No. cstc2013jcsf-zdzxqqX0003), National Key R&D Program(Grant No.2016YFB0100904), Scientific and Technological Research Program of Chongqing Municipal Education Commission(Grant No.KJ1503301) and the Fundamental Research Funds of China Central Universities (Grant No. 106112014CDJZR178801).

References

[1] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET," *IEEE Transaction on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, 2012.

[2] S. I. Ahamed and S. Moushumi, "A trust-based secure service discovery (TSSD) model for pervasive computing," *Computer Communications*, vol. 31, no. 18, pp. 4281–4293, 2008.

[3] F. Almenrez, A. Marn, C. Campo, and C. Garcia, "PTM: A pervasive trust management model for dynamic open environments," in *The First Workshop on Pervasive Security, Privacy and Trust (PSPT'04)*, vol. 4, no. 7, pp. 1–8, 2004.

[4] M. Ashwin, S. Kamalraj, and M. Azath, "Weighted clustering trust model for mobile ad hoc networks," *Wireless Personal Communications*, vol. 3, no. 6, pp. 6–17, 2016.

[5] Q. H. Bai, Y. Zheng, L. N. Zhao, H. Chun, and C. Y. Cheng, "Research on mechanism of PKI trust model," *Applied Mechanics and Material, Trans Tech Publications*, vol. 536, pp. 694–697, 2014.

[6] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[7] B. S. Bhati and V. Pallapa, "Performance analysis of location privacy preserving scheme for MANETs," *International Journal of Network Security*, vol. 18, no. 4, pp. 736–749, 2016.

[8] J. Braun, F. Volk, J. Classen, J. Buchmann, and M. Mhlhuser, "CA trust management for the web PKI," *International Journal of Network Security*, vol. 22, no. 6, pp. 913–959, 2014.

[9] G. Carullo, A. Castiglione, G. Cattaneo, A. De Santis, U. Fiore, and F. Palmieri, "Feeltrust: Providing trustworthy communications in ubiquitous mobile environment," in *IEEE 27th International Conference on Advanced Information Networking and Applications (AINA'13)*, pp. 1113–1120, 2013.

[10] J. H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2014.

[11] M. C. Chuang and J. F. Lee., "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 1758–1761, 2014.

[12] R. G. Engoulu, M. Bellache, and S. Pierre, "Vanet security surveys," *Computer Communications*, vol. 44, no. 1, pp. 1–13, 2014.

[13] F. Zhang, Z. P. Jia, H. Xia. Li, H. M. Sha Edwin, "Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and markov SCGM(1,1) model," *Computer Communications*, vol. 35, no. 5, pp. 589–596, 2012.

[14] M. Fiore, C. Casetti, and C. F. Chiasserini, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289–303, 2013.

[15] H. Hu, R. Lu, Z. Zhang, and J. Shao, "Replace: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, 2016.

[16] D. Jia, K. Lu, and J. Wang., "On the network connectivity of platoon-based vehicular cyber-physical systems," *Transportation Research Part C: Emerging Technologies*, vol. 40, pp. 215–230, 2014.

[17] Y. Kobayashi, K. Totani, K. Utsu, and H. Ishii, "Achieving secure communication over manet using secret sharing schemes," *Journal of Supercomputing*, vol. 72, no. 3, pp. 1215–1225, 2016.

[18] X. Kong and Y. Zhuang., "Research on trust chain transfer model based on dynamic intransitive noninterference," *Journal of Convergence Information Technology*, vol. 7, no. 21, pp. 157–163, 2012.

[19] S. Kumari, M. Karuppiah, X. Li, F. Wu, A. K. Das, and V. Odelu, "An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4255–4271, 2016.

[20] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[21] J. Lin, Y. Wu, G. Wu, and J. Xu, "An adaptive approach for multi-agent formation control in MANET based on CPS perspective," *Journal of Networks*, vol. 9, no. 5, pp. 1169–1177, 2014.

[22] C. Malandrino, F. Borgiattino and C. Casetti, "Verification and inference of positions in vehicular networks through anonymous beaconing," *IEEE Transaction on Mobile Computing*, vol. 13, no. 10, pp. 2415–2428, 2014.

[23] D. Marudhadevi, V. N. Dhatchayani, and S. Shankar, "A trust evaluation model for cloud computing using service level agreement," *The Computer Journal*, vol. 58, no. 10, pp. 2225–2232, 2014.

[24] M. N. Mejri, J. Ben-Othman, and M. Hamdi., "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 11, no. 2, pp. 53–66, 2014.

[25] M. Omar, C. Yacine, and B. Abdelmadjid, "Reliable and fully distributed trust model for mobile ad hoc networks," *Computers and Security*, vol. 28, no. 3, pp. 199–214, 2009.

[26] T. Oulhaci, M. Omar, F. Harzine, and I. Harfi, "Secure and distributed certification system architecture for safety message authentication in VANET," *Telecommunication Systems*, vol. 64, no. 4, pp. 679–694, 2016.

[27] H. Peng, D. Zhao, and Y. Yu, "Trust model based on trusted computing for distributed heterogeneous networks," *Computer Science*, vol. 10, no. 8, pp. 66–69, 2014.

[28] D. K. Sheet, O. Kaiwartya, A. H. Abdullah, Y. Cao, A. N. Hassan, and S. Kumar, "Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks," *IET Intelligent Transport Systems*, vol. 11, no. 2, pp. 53–60, 2017.

[29] R. Sugumar, A. Rengarajan, and C. Jayakumar., "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)," *Wireless Networks*, vol. 29, no. 7, pp. 1–10, 2016.

[30] D. Sun, H. Zhao, H. Yue, M. Zhao, S. Cheng, and W. Han, "ST TD outlier detection," *IET Intelligent Transport Systems*, vol. 11, no. 4, 2017.
[31] Y. Uzunay and B. Kemal, "Trust-in-the-middle: towards establishing trustworthiness of authentication proxies using trusted computing," *Computer Science*, vol. arXiv preprint arXiv:1511.05682, pp. 1–32, 2014.
[32] Y. C. Wang, Y.and Lu, I. R. Chen, and J. H. Cho, "Logittrust: A logit regression-based trust model for mobile ad hoc networks," in *The 6th ASE International Conference on Privacy, Security, Risk and Trust*, pp. 1–10, Boston, MA, Mar. 2014.
[33] G. Wu, Z. Du, Y. Hu, T. Jung, U. Fiore, and K. Yim, "A dynamic trust model exploiting the time slice in WSNs," *Soft Computing*, vol. 18, no. 9, pp. 1829–1840, 2014.
[34] H. Xia, Z. Jia, X. Li, L. Ju, and H. M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, no. 7, pp. 2096–2114, 2013.
[35] H. Yue, "Advanced traveler information inquiry, archiving, and decision making system," in *The 12th Guangzhou Convention of Overseas Chinese Scholars Science and Technology*, Guangdong, China, Dec. 2009.
[36] H. Yue, "Archiving capability of spatio-temporal data in different highway railroad grade crossing (HRGC) databases," in *The 20th Annual Intelligent Transportation System*, Houston, America, May 2012.
[37] H. Yue, E. Jones, and P. Z. Revesz, "Use of local polynomial regression models for average traffic speed estimation and forecasting in linear constraint databases," in *The 17th International Symposium on Temporal Representation and Reasoning*, pp. 154–161, Paris, France, Nov. 2010.
[38] H. Yue and R. Yang, "Development of intelligent transportation systems and plan of integrated information system," *Journal of Wuhan University of Technology*, vol. 29, no. 4, pp. 560–563, 2005.
[39] H. Yue and P. Z. Revesz, "TVICS: An efficient traffic video information converting system," in *The 19th International Symposium on Temporal Representation and Reasoning (TIME'12)*, pp. 141–148, Leicester, UK, Dec. 2012.
[40] H. Yue, L. R. Rilett, and P. Z. Revesz, "Spatio-temporal traffic video data archiving and retrieval system," *GeoInformatica*, vol. 20, no. 1, pp. 59–94, 2016.
[41] Y. Zeng, J. Cao, and J. Hong, "Secure localization and location verification in wireless sensor networks: A survey," *Journal of Supercomputing*, vol. 64, no. 3, pp. 685–701, 2013.
[42] P. Zhang, Z. Zhang, and A. Boukerche, "Cooperative location verification for vehicular ad-hoc networks," in *Proceedings of IEEE International Conference on Communications (ICC'12)*, pp. 37–41, Ottawa, ON, Canada, July 2012.
[43] H. Zhao, D. Sun, H. Yue, M. Zhao, and S. Cheng, "Using CSTPNS to model traffic control CPS," *IET Software*, vol. 11, no. 3, 2017.
[44] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 10, no. 3, pp. 59–68, 2015.

Biography

Hongzhuan Zhao(1985-), Male, is an Assistant Professor at School Architecture and Transportation Engineering, Guilin University of Electronic Technology, Guangxi, China. He gained Ph.D. from Chongqing University, China in 2016. His current work focuses on some research topics related to ITS, Cyber-Physical System (CPS), reliable perception, and trusted interaction.

Dihua Sun (1962-), Male, is a Professor at College of Automation, Chongqing University. He gained the B.S. from Huazhong University of Science and Technology in 1982, China, and obtained M.S. and PH.D. from Chongqing University, China, in 1989 and 1997, respectively. His research interests include CPS, ITS, computer-based control, data analysis and decision support.

Hang Yue (1977-), Male, obtained his M.S. degree in Transportation Engineering and Minors in Statistics and Geography from University of Nebraska-Lincoln in 2012 and M.S. degree in Computer Software Engineering from Zhejiang University in 2005. He served as a Data Analyst at AirSage Inc. in 2013, and a Data Scientist at Charter Global Inc. in 2014. He is currently a Data Analyst at Johns Hopkins Health Care LLC. His research interests are machine learning, big data business intelligence, data warehouse, data visualization, GIS, and spatio-temporal databases.

Min Zhao (1980-), Female, is an Associate Professor at College of Automation, Chongqing University. She gained Ph.D. from Chongqing University, China in 2010. Her research interests include CPS, ITS and the traffic image processing.

Senlin Cheng (1968-), Male, is an Associate Professor at College of Automation, Chongqing University. He gained Ph.D. from Chongqing University, China in 1999. His research interests include CPS, ITS and wireless location technology.