Zhou *et al. EURASIP Journal on Wireless Communications and Networking* [redacted]
DOI 10.1186/s13638-015-0257-x

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A security authentication method based on trust evaluation in VANETs

Ao Zhou[1*], Jinglin Li[1], Qibo Sun[1], Cunqun Fan[2], Tao Lei[1] and Fangchun Yang[1]

Abstract

Vehicular *ad hoc* networks (VANETs) have a high degree of openness. Therefore, if a new vehicle node wants to access the network, we need to validate the vehicle node carefully to ensure the security of the entire networking. There are a large number of vehicle nodes, and the strange degree among the nodes is very high in VANETs. In addition, VANETs are human-oriented networks. All vehicle nodes in the VANET have the right to decide whether to accept a new node. To attack this challenge, this paper proposes a security authentication method based on trust evaluation. The security authentication method consists of two parts: secure authentication based on direct trust evaluation and secure authentication based on indirect trust evaluation. In the direct trust evaluation, the security vector model is established based on the security behaviors of the new vehicle node. The historical security evaluation from the authority units (AU) is collected to calculate the final direct trust. In the indirect trust evaluation, the trust degree is calculated based on the recommendation trust vectors from the vehicle nodes in the network. The method employs correlation coefficient for distinguishing the malicious vehicle. Then, the recommendations from the malicious vehicle nodes are removed. The final recommended trust is gained by calculating the average recommendation trusts of remained vehicle nodes. Simulation results show the advantage of our proposed method.

Keywords: VANETs; Direct trust; Indirect trust; Correlation coefficient; Security

1 Introduction

VANETs have a high degree of openness [1]. Therefore, VANET needs face a diverse of security threats [2,3]. Firstly, through accessing the VANETs, the attacker can conduct privacy spy and obtain the moving track of the vehicles [4]. Secondly, some attackers release some false news (such as traffic accidents, road congestion, etc.) [5], and the false news can lead to chaotic traffic and accidents. What is more, the openness and highly dynamic of VANETs make the malicious attacks easy to implement and difficult to detect [6]. Due to the application characteristics and application scenarios of VANETs, these attacks can threat the information security and the property safety of users [7]. Therefore, how to accurately authenticate the new accessing vehicle node is becoming an urgently required research problem [8].

Current trust management researches are focused on message evaluation and user privacy protecting. The message evaluation can stop delivering of false message and enhance the security of VANETs. Although the trust management can be applied in VANETs to comprehensively improve the security and reliability of VANETs, these methods cannot fundamentally solve the problem. What is more, previous studies do not consider the 'suggestion' from existing nodes when validating the new accessing node. Because the VANETs are human-oriented user groups, the vehicle nodes in VANETs can subjectively judge whether to accept the new accessing node. To solve the problem and improve the accuracy of trust evaluation, this paper proposes a security authentication method based on trust evaluation. Our method does security authentication based on both direct trust evaluation and indirect trust evaluation. In the direct trust evaluation, in order to objectively determine whether the vehicle node can access the VANET, we calculate the direct trust value based on historical security behavior information. In the indirect trust evaluation, the indirect trust is calculated based on the recommendation trust from other vehicle nodes in the VANETs. Simulation results show the advantage of our method.

*Correspondence: hellozhouao@gmail.com
[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
Full list of author information is available at the end of the article

The rest of this paper is organized as follows. Section 2 introduces related work. Section 3 shows our proposed security authentication method. Evaluation of the method is explained in Section 4. Section 5 concludes the paper.

2 Related work

There are plenty of trust management and encrypted authentication methods in literature. We will only review some notable work due to space limitation.

Biswas, et al. [9] proposed a safety message authentication scheme for VANETs. The scheme adopts an ID-based verification and signature mechanism. A certificate-less public key verification is offered by an ID-based technique. The message authentication is provided by a proxy signature. In this scheme, the standard ECDSA is incorporated with an ID-based proxy signature framework for the road-side unit originated messages. The transfer of signed message is specially handled to ensure the security and reliability of applications.

The work [10] pointed out that the characteristics and the security requirements of VANETs are quite different from standard *ad hoc* networks. Especially, trust management in VANETs is an urgently research problem. The paper concludes the advantage and disadvantage when adopting ordinary methods of network and standard *ad hoc* networks.

To protect the VANETs against attackers and defend VANETs against misbehavior, a threshold signature-based mechanism was proposed by the work [11]. The work also presents a privacy-preserving defense mechanism based on the threshold authentication. The paper does systematic analysis to show the strong point and the efficiency of the proposed mechanism.

The work [12] pointed out that evaluating the safety and trust level of vehicles is important to ensure the reliability of applications. The work also points out that traditional trust level is evaluated by monitoring the message generation and the behavior of the other vehicle nodes. However, the attacker can interrupt the regular communication among vehicles by creating a case of None Line of Sight. In addition, the case of None Line of Sight can prevent vehicles from monitoring other vehicle nodes. To solve the problem, the work proposes a location information-based trust evaluation model. The model can be used to evaluate the trust level of other vehicle nodes.

The emerging of VANET is to support the communication of vehicles on roads. The network allows arbitrary vehicles to broadcast traffic accident and other *ad hoc* messages. Because the attackers may release some false news, the work [13] pointed out that the concern of security and privacy needs to be taken into consideration. Therefore, all messages should be verified. However, the validation process should not reveal the real identity of vehicles. To solve the problem, a software-based solution is proposed in this paper. The method uses only two shared secret, therefore, the proposed method can satisfy the requirement. A group communication protocol is also proposed in this paper to allow communication between vehicles in the same group with a high level of security.

Certification and proof-of-work system are two basic mechanisms that have been used in security mechanisms. Palomar et al. [14] proposed a method based on the two mechanisms to provide safe communication environment and combat spam.

To guide the drivers to desired destinations, Chim et al. [4] made use of the online real-time road information collected by the vehicle nodes. When the method calculates the best route for drivers, the information source is authenticated to avoid attack. At the same time, the privacy of the drivers is protected. All nodes, including the trusted authority, cannot obtain the destination of the driver.

The release of wrong information can lead to injury to the lives of the drivers. Therefore, the Sybil attack is a serious threat in VANETs. The paper [15] proposed a Sybil attack detection algorithm to solve the problem. The algorithm is based on signature mechanism in VANETs. In the moving process, each vehicle node gathers the digital signatures at the same time; all the collected signature vectors are analyzed and compared to detect the Sybil attack.

To measure the integrity degree of security scheme in VANETs, Azogu et al. [16] proposed an asymmetric profit-loss Markov model. In the proposed asymmetric Markov model, the loss denotes the negative effect a vitiated data fragment is received by a device. Profit represents the positive effect when a vitiated data fragment is detected and disregarded. Markov chain records change of system behavior that reacts to profit and loss asymmetrically. The model adopts a black-box method when measuring the integrity level. In other words, the model does not need to know the implementation details of each security scheme. Therefore, the model is very suitable for real world applications.

There are a large number of well-performed trust evaluation methods. Nevertheless, there is lack of comprehensive security authentication method for VANETs. In addition, previous studies do not take the subjective recommendation into consideration. Different from current methods, our method can solve the problem. We will present the detail of our method in the next section.

3 Multi-level security certification of VANETs

To ensure the security of the VANETs, this paper presents a comprehensive vehicle node security authentication

method. The proposed security authentication method consists of two main parts: the direct trust evaluation and the indirect trust evaluation. When a vehicle wants to access the Internet through the roadside base station, the direct trust evaluation method is adopted to validate the vehicle node. In order to objectively determine whether the vehicle node can access the VANET, the trust of the node is directly evaluated based on the historical evaluations from the authority unit (AU). When a group of vehicles form a wireless network to communicate information with each other, the indirect trust evaluation method can decide whether to accept a new vehicle node. The indirect trust evaluation mechanism of the vehicle node is established based on the recommended trust from other nodes in VANETs. The indirect trust evaluation lets the nodes within the network decide the acceptance of the new access vehicle node. We will show the detail of the trust evaluation in this section.

3.1 Security authentication based on direct trust evaluation

Vehicles need to access the VANETs to obtain the needed information. We need to validate the new vehicle nodes when they access the VANET. This section proposes a direct trust evaluation method based on historical security event record. In the interaction of AUs and vehicle nodes, the security events are recorded to the database. All AUs can access the Internet. The AUs belonging to the same organization can share the same database. We can make use of the recorded events to evaluate the new vehicle node and further determine whether the vehicle is credible. Because we try to calculate the direct trust of vehicle node based on the historical security events, we will discuss how to analyze the recorded historical events in detail.

3.1.1 The security vector model

The VANET can support plenty of applications. For the inherent characteristics of the vehicle, the security events of the vehicle node are very complex. There are a large number of security events. But these security events can be classified into several types, for example: physical security events, information privacy security events, information-disruptive events, et al. Therefore, security behaviors of the vehicle node can be subdivided. All security behaviors of the vehicle are classified to a security event type $VANET\_Event_n$. We now introduce the security vector.

Definition 1. The security vector is defined by the following:

$$\text{Security\_Vector} = < \text{VE}_1, \text{VE}_2, \ldots, \text{VE}_n > \quad (1)$$

All vehicle node security events are classified based on the security vector, and each event belongs to a corresponding security component E_i. Each security component, respectively, reflects the security level of the corresponding security events.

The security vector can reflect the security level of the vehicle nodes. In VANETs environment, the security events of the vehicle nodes are very complex, and how to classify the security events is also very complex. An accurate security component partition can reflect the security of the vehicle more accurately. For example, personal security events should have a higher level compared to other security events, and information privacy security events should have a higher level compared to the interference events.

3.1.2 Trust evaluation based on the historical security events

In VANETs, security evaluation based on the historical events is an important part of the direct trust evaluation. If there is no insecure event of the vehicle node in the record, the vehicle node is trustworthy to some extent.

Vehicle nodes and roadside fixed access points need to exchange application data and other information with AU, so AU can evaluate the security of the vehicle node. The security event information of vehicle node is saved on the local server, and AU can evaluate the vehicle node based on the information. The evaluation data has its own specific format as follows:

$$\text{Event} = \{\text{VID, AUID, VANET\_Event, EventID, Security, Time}\}\, \text{sig}_{AU} \quad (2)$$

where VID and AUID represent the ID of the evaluated node. *VANET_Event* represents the security event component. *EventID* represents the security event ID. *Security* represents the security value of the vehicle node. *Time* represents timestamp of the system. sig_{AU} represents the private key signature of AU.

Definition 2. Vehicle historical security degree VHS:

$$P_{V_{Ei}} = \frac{1}{n} \sum_j (\text{Event}_j.\text{Security}), \text{Event}_j.\text{VANET\_Event is Ei} \quad (3)$$

where $Security_i$ represents the security degree evaluated by AU. n represents the number of events belonging to E_i. The events long before may have little relevance to current security. Therefore, only recent events are considered. The 'period of validity' of the events can be decided by the AU owner. P_v can represent the average security degree of a vehicle node evaluated by AU.

The time complexity of the direct trust evaluation method is $O(n)$. n is the number of recent history events.

3.2 Security authentication based on indirect trust evaluation

When a group of vehicles form a wireless network to communicate information with each other, the vehicle nodes in the network have the right to determine whether to accept the new vehicle node. The vehicle network is largely similar to the interpersonal network. In interpersonal network, the acceptance of a new node mainly depends on the trust value and the recommendation of other individuals. Therefore, the trust value of the vehicle node depends on the recommendation trust from other nodes in the network. However, some selfish vehicle nodes in the VANET may maliciously deny the new vehicle node. The condition is unfavorable for the VANET. We need to distinguish the malicious nodes before calculating the indirect trust value. Based on above analysis, we propose an indirect trust evaluation method. In the indirect trust evaluation, we make use of the correlation coefficient of the recommendation trust value to distinguish the malicious nodes. All the recommendation trust values from the malicious nodes are removed. We do not take the suggestion of malicious nodes into consideration when calculating the indirect trust value.

3.2.1 The recommendation trust vector model

The security behaviors of vehicle nodes are diverseness and complexity. The security behavior of vehicles generally include: safety drive, information security, information authenticity, information accuracy, etc. All security behaviors can be quantized. The recommendation node scores the access node in each security behavior. All the scores are stored in a vector. The vector is called recommendation trust vector in our paper.

Definition 3. The recommendation trust vector is defined by the following:

$$\text{Trust\_Vector}_n = \left\langle P_{S1}^{XB}(t), P_{S2}^{XB}(t), \ldots, P_{Sm}^{XB}(t) \right\rangle \tag{4}$$

It represents recommendation trust vector from node X to node B. X denotes the X^{th} recommendation node, and B denotes the node to be evaluated. S_i denotes the i^{th} type of security event. $P_{Si}^{XB}(t)$ is called the trust component. The trust component denotes the score for a type of security behavior. The score from a vehicle node may change with time. A vehicle node may give a different score for the same access node at different time. Therefore, we give each score a timestamp. t represents the specific timestamp when node X gives the score.

In VANET, the score from different recommendation nodes is quite different and denotes the subjective will of each recommendation node. Some vehicle nodes in the VANET may maliciously give a low score to the vehicle node. However, the maliciousness can be detected by analyzing each recommendation trust component P_{Si} carefully. In this way, we can evaluate the trust of the vehicle node more accurately. The detail will be discussed in the next section.

3.2.2 Trust evaluation based on the recommendation trust value

The score from recommendation vehicle nodes may not consist with the real behavior of the new accessing node. VANET is an open network and faces many risks. Some inner and outer factors may cause some node to become selfish and malicious. In general, we can divide the recommendation node into two types: general recommendation node and malicious recommendation node. The inconsistency is mainly caused by the malicious recommendation node. To eliminate the influence of malicious recommendation nodes, we propose a malicious recommendation node detection method. Firstly, the method calculates the average recommendation trust vector. The average recommendation trust vector can be obtained by calculating the mean score of each trust component. Then, by analyzing the correlation coefficient between average recommendation trust vector and recommendation trust vector of each recommendation node, we can detect the malicious recommendation node. The recommendation nodes that have a relatively larger deviation are the malicious recommendation nodes. The average recommendation trust vector can be calculated by the following:

$$\text{Trust\_Vector}_{\text{average}} = \left\langle P_{S1}^{B}(t), P_{S2}^{B}(t), \ldots, P_{Sm}^{B}(t) \right\rangle \tag{5}$$

where $P_{Sm}^{B}(t) = \frac{1}{n} \sum_{x \in \text{network}} \left[P_{Sm}^{xB}(t) \right]$, x denotes the xth recommendation node, and n represents the number of recommendation nodes.

All existing vehicle nodes in the VANET should send their recommendation trust vectors. A vehicle node can send a blank vector to give up the right. After receiving the recommendation trust vector from all vehicle nodes in the VANET, we need to compare each recommendation trust vector with the average recommendation trust vector. In this way, we can distinguish malicious recommendation nodes. Linear interpolation method is a basic method to solve the problem. However, this method is obviously not able to accurately distinguish the malicious recommendation nodes. Therefore, we will adopt a correlation coefficient based method to solve the problem. Firstly, we will introduce the definition of the correlation coefficient:

Definition 4. (Correlation coefficient) The correlation coefficient ρ is an index which represents the degree of correlation between variables. The correlation coefficient is larger than -1 and smaller than 1. When the value of

$|\rho|$ is large, the error Q is small; and the linear correlation degree between variables is high. When the value of $|\rho|$ is small, the error Q is large; and the linear correlation degree between variables is low. When there are two sample functions X and Y, the cross-correlation of X and Y can be calculated by the following:

$$\rho_{xy} = \frac{\sum_{i=1}^{N}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i - \bar{Y})^2}} \tag{6}$$

To express our work more concisely, we employ T_V instead of *Trust_Vector* in the rest of our paper. The correlation coefficient between average recommendation trust vector and a single vehicle node recommendation trust vector can be calculated by the following:

$$\mathrm{Cov}(T\_V_a, T\_V_n) = E(T\_V_a, T\_V_n) - E(T\_V_a)E(T\_V_n) \tag{7}$$

$$\rho_{xy} = \frac{\mathrm{Cov}(T\_V_a, T\_V_n)}{\sqrt{D(T\_V_a)}\sqrt{D(T\_V_n)}} \tag{8}$$

To distinguish the malicious nodes, we will do a quantitative comparison based on the correlation coefficient. We set two thresholds to divide the range of $|\rho|$ into three intervals. Then, we determine whether the vehicle node is in a trusted state. Suppose the two thresholds are $\Delta\rho_1$ and $\Delta\rho_2$. The three intervals are $(0, 1 - \Delta\rho_1 - \Delta\rho_2]$, $(1 - \Delta\rho_1 - \Delta\rho_2, 1 - \Delta\rho_1]$, and $(1 - \Delta\rho_1, 1)$.

- When the correlation coefficient ρ_{ns} of T_V_a and T_V_n belongs to $(1 - \Delta\rho_1, 1)$, T_V_a and T_V_n are close to linear correlation. Therefore, we can consider that the node recommendation trust consists with the average recommendation trust. We think the recommendation trust of the node is reasonable. The recommendation node is not a malicious node.
- When the correlation coefficient ρ_{ns} of T_V_a and T_V_n belongs to $(1 - \Delta\rho_1 - \Delta\rho_2, 1 - \Delta\rho_1]$, the linear relationship between T_V_a and T_V_n is not so obvious. Therefore, the reasonableness of the recommended trust value needs a further discussion. We introduce a norm method to discuss reasonableness of the recommendation trust. The single recommendation trust vector and average recommendation trust vector are normalized by using the following equations:

$$\|T\_V_n\| = \sqrt{T\_V_n, T\_V_n} = \sqrt{P_{S1}^{XB}(t)^2 + P_{S2}^{XB}(t)^2, \ldots, P_{Sm}^{XB}(t)^2} \tag{9}$$

$$\|T\_V_a\| = \sqrt{T\_V_a, T\_V_a} = \sqrt{P_{S1}^{B}(t)^2 + P_{S2}^{B}(t)^2, \ldots, P_{Sm}^{B}(t)^2} \tag{10}$$

The deviation between $\|T\_V_n\|$ and $\|T\_V_a\|$ can be calculated by the following:

$$\Delta\|T\_V\| = |\|T\_V_n\| - \|T\_V_a\||| \tag{11}$$

We set the minimum deviation of normalized trust vector as $\|T\_V\|'_{\min}$. When $\Delta\|T\_V\| > \|T\_V\|'_{\min}$, we think the recommendation node is not trusted. Otherwise, the deviation is small. We think that the recommendation node is in a temporary trusted state.

- When the correlation coefficient ρ_{ns} of T_V_a and T_V_n belongs to $(0, 1 - \Delta\rho_1 - \Delta\rho_2]$, T_V_a and T_V_n do not show a linear relationship. Therefore, we can consider that the deviation is very large. We think the recommendation trust value of the node is unreasonable. The recommendation node is a malicious node.

The value of $\Delta\rho_1$ and $\Delta\rho_2$ can be adjusted according to the actual situation. We will discuss the problem in the experimental section.

3.2.3 The recommendation trust

After distinguishing the malicious nodes, we can obtain the unreasonable recommendation trust vector. The unreasonable recommendation trust vectors should be abandoned. When calculating the average recommendation trust value, we just use the reasonable recommendation trust vectors. The formula is as follows:

$$\mathrm{Trust\_Vector}_B = \left\langle P_{S1}^{B}(t), P_{S2}^{B}(t), \ldots, P_{Sj}^{B}(t) \right\rangle \tag{12}$$

where $Trust\_Vector_B$ is the average recommendation trust vector from other vehicle nodes. The trust value of the target node can be evaluated according to the above equation. Then, whether to accept the access node can be determined based on the vector.

The time complexity of the average recommendation trust vector calculation is O(m*n). n is the number of recommendation nodes, and m is the number of security event type. The time complexity of the correlation coefficient calculation is O(m*n). The time complexity of the malicious node detection is $O(n)$. The time complexity of the final recommendation trust calculation is O(m*n). Therefore, the time complexity of the indirect trust evaluation method is O(m*n).

4 Experimental results

We proposed a security authentication method based on trust evaluation. The method is composed of two parts: Firstly, direct trust evaluation is presented based on historical security event record. Secondly, the vehicle nodes in the network can determine whether to accept the new vehicle node. To verify the effectiveness of our method,

we implement our method in Matlab and conduct experiments on it. The following sections first outline the experimental setting. We then discuss the results and show the advantage of our method.

4.1 Experimental setup

The physical machine configurations of our experiments are as follows: CPU core is i3-2310M 2.10 GHz, RAM is 2 GB, and operating system is Windows 7. The method is implemented in Matlab 7.1.

There are 80 target nodes when we do the direct trust evaluation simulation experiment. Then, all the security events are divided into five levels in the security settings, and the security weights are as follows: 0.1, 0.15, 0.2, 0.25, 0.3. The security degree of target nodes is calculated as follow:

$$\text{Security}_i = 0.1V_{E1} + 0.15V_{E2} + 0.2V_{E3} + 0.25V_{E4} + 0.3V_{E5} \tag{13}$$

There are 20 recommendation vehicle nodes when we do the indirect trust evaluation simulation experiment. All the security events are divided into five levels, and their security weights are as follows: 0.1, 0.15, 0.2, 0.3, 0.35. The security degree of target nodes can be calculate by the following:

$$\text{Trust}_B = 0.1P^B_{S1}(t) + 0.15P^B_{S2}(t) + 0.2P^B_{S3}(t) + 0.3P^B_{S4}(t) + 0.35P^B_{S5}(t) \tag{14}$$

4.2 Experimental results

To verify the accuracy of the proposed method, we discuss the result from two aspects. We first study the results on direct trust evaluation experiment. Then, we discuss the results on indirect trust evaluation experiment.

4.2.1 Direct trust evaluation

Figure 1 shows the security degree distribution of the 80 nodes, and Figure 2 shows the number of nodes that can be trusted in after the minimum accepted security degree has been selected.

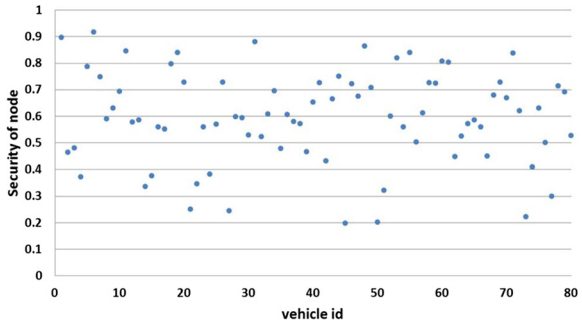

Figure 1 Distribution of security degree.

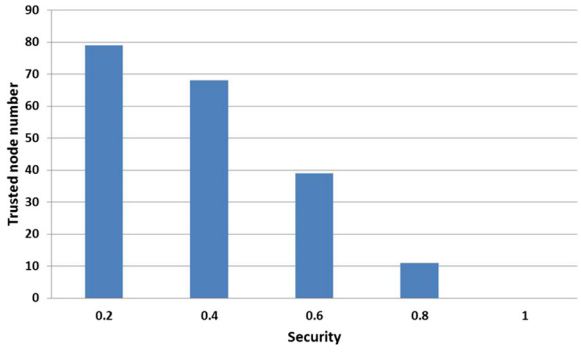

Figure 2 Trusted node number.

As shown in Figure 1, on various security degrees, how to distinguish the security of nodes is relatively obvious. As shown in Figure 2, the security degree of most nodes is greater than 0.5. When the minimum accepted security degree is 0.2, there are 79 nodes than can meet the security demands. When the minimum accepted security degree is 0.4, there are 68 nodes that can meet the security demands. When the minimum accepted security degree is 0.6, there are 39 nodes that can meet the security demands. When the minimum accepted security degree is 0.8, there are 11 nodes that can meet the security demands.

After calculating the security degree of the nodes, you can decide the appropriate minimum accepted security degree based on the actual situation.

4.2.2 Indirect trust evaluation

To study the performance of our indirect trust evaluation method (ITE), we compare ITE with an indirect trust evaluation method without malicious nodes detecting (WMD). Different from ITE, WMD does not detect malicious nodes and remove the malicious recommendation trust vectors.

When we evaluate the node by using ITE, all existing vehicle nodes in the VANET should send their recommendation trust vectors. The correlation coefficient values of all recommendation trust vectors are shown in Figure 3.

As shown in Figure 3, there are four nodes whose recommendation trust vector correlation coefficient is smaller than 0.6. There is a high chance that the four nodes are malicious nodes and may reject new nodes viciously. Among 20 recommendation nodes, there are 16 recommendation nodes whose recommendation trust vector correlation coefficient is larger than 0.6. It indicates that trust vectors from these 16 recommendation nodes consist with the overall distribution of trust vector. Therefore, there is a high chance that these recommendation nodes are not malicious. Therefore, we set $\Delta\rho_1 = 0.4$ and

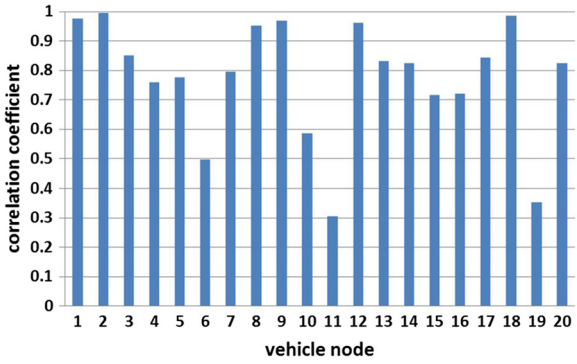

Figure 3 The correlation coefficient of trust vector.

$\Delta\rho_2 = 0.2$. The larger $\Delta\rho_1$ and $\Delta\rho_2$ are, the lesser recommendation nodes that can meet the demands. In the real environment, the value of $\Delta\rho_1$ and $\Delta\rho_2$ can be adjusted according to the actual situation.

Figure 4 shows the trust degree of the ten target nodes. We set $\Delta\rho_1 = 0.4$ and $\Delta\rho_2 = 0.2$. As shown in Figure 4, when employing ITE, the trust degree of the targets nodes is higher than WMD. That is because LTE employs correlation coefficient for distinguishing the malicious recommendation trust vector. LTE abandons the unreasonable recommendation trust first when calculating the final trust degree. As shown in Figure 4, there are nine nodes whose trust degree is greater than 0.6, there are seven nodes whose trust degree is greater than 0.7, and there are six nodes whose trust degree is greater than 0.8. A higher trust degree means more nodes in the network trust the new node. Therefore, there is higher chance that the node is more trustworthy than other nodes. As we can see from the above discussion, our method can accurately evaluate the vehicle nodes.

5 Conclusions

Because of the openness of VANETs, the network needs to face many security risks. If a new vehicle node wants to access the VANET, we need to validate the new vehicle node to improve the security of the VANET. We propose a security authentication method based on trust evaluation. Firstly, when a vehicle wants to access the Internet through the roadside base station, we evaluate the access node by employing the direct trust evaluation. Based on the historical security event record, the direct security degree of the new vehicle node is determined. When a group of vehicles form a wireless network to communicate information with each other, we adopt the indirect trust evaluation mechanism to evaluate the new vehicle node. All vehicle nodes in the network can determine whether to accept the new vehicle node. Each node sends a vector to show its recommendation trust value. Based on the correlation coefficient, we distinguish the malicious vehicle nodes and remove all recommendation trust value from the malicious vehicle nodes. Then, the indirect trust value is calculated by averaging all the remaining recommendation trust values. Simulation results show our method can accurately validate the vehicle node.

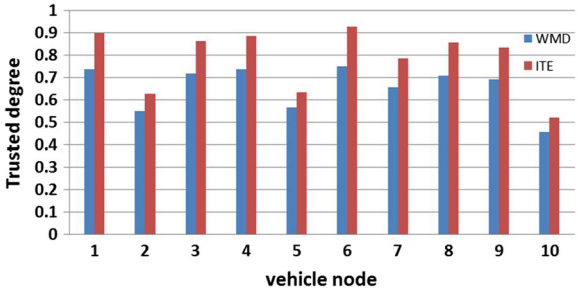

Figure 4 Trust degree.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
The work presented in this study is supported by NSFC (61202435, 61472047); Beijing Natural Science Foundation (4132048).

Author details
[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China. [2]National Satellite Meteorological Centre, China Meteorological Administration, Beijing 100876, China.

Received: 21 October 2014 Accepted: 7 January 2015
Published online: 10 March 2015

References

1. H Hartenstein, K Laberteaux, *VANET: Vehicular Applications and Inter-networking Technologies*. (Wiley Online Library, Hoboken, 2010)
2. A Buchenscheit, F Schaub, F Kargl, M Weber, in *Vehicular Networking Conference (VNC), 2009 IEEE*. A VANET-based emergency vehicle warning system (IEEE Piscataway, 2009), pp. 1–8
3. S Wang, C Fan, C-H Hsu, Q Sun, F Yang, A vertical handoff method via self-selection decision tree for internet of vehicles. IEEE Syst. J. **pp**(99), 1–10 (2014)
4. T Chim, S Yiu, L Hui, V Li, Vspn: VANET-based secure and privacy-preserving navigation. Compt. IEEE Trans. **63**(2), 510–524 (2012)
5. S Xi, X-M Li, in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference On*. Study of the feasibility of VANET and its routing protocols (IEEE, Piscataway, 2008), pp. 1–4
6. A Mahajan, N Potnis, K Gopalan, A Wang, in *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*. Modeling VANET deployment in urban settings (ACM, New York, 2007), pp. 151–158
7. K Sampigethaya, M Li, L Huang, R Poovendran, Amoeba: robust location privacy scheme for vanet. Sel. Areas Commun. IEEE J. **25**(8), 1569–1589 (2007)
8. K Sampigethaya, L Huang, M Li, R Poovendran, K Matsuura, K Sezaki, Caravan: Providing location privacy for vanet. Technical report, DTIC Document (2005)
9. S Biswas, J Misic, V Misic, in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference On*. ID-based safety message authentication for security and trust in vehicular networks (IEEE, Piscataway, 2011), pp. 323–331
10. P Wex, J Breuer, A Held, T Leinmuller, L Delgrossi, in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*. Trust issues for vehicular ad hoc networks (IEEE, Piscataway, 2008), pp. 2800–2804

11. J Sun, C Zhang, Y Zhang, Y Fang, An identity-based security system for user privacy in vehicular ad hoc networks. Parallel Distributed Syst. IEEE Trans. **21**(9), 1227–1239 (2010)
12. O Abumansoor, A Boukerche, in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. Towards a secure trust model for vehicular ad hoc networks services (IEEE, Piscataway, 2011), pp. 1–5
13. TW Chim, S-M Yiu, LC Hui, VO Li, Specs: Secure and privacy enhancing communications schemes for vanets. Ad Hoc Networks. **9**(2), 189–203 (2011)
14. E Palomar, JM de Fuentes, AI González-Tablas, A Alcaide, Hindering false event dissemination in vanets with proof-of-work mechanisms. Transportation Res. Part C: Emerging Technol. **23**, 85–97 (2012)
15. C Chen, W Han, X Wang, Sybil attack detection based on signature vectors in vanets. Int. J. Crit. Comput.-Based Syst. **2**(1), 25–37 (2011)
16. IK Azogu, MT Ferreira, H Liu, in *Global Communications Conference (GLOBECOM), 2012 IEEE*. A security metric for vanet content delivery (IEEE, Piscataway, 2012), pp. 991–996