This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET

Hao Hu, *Student Member, IEEE,* Rongxing Lu, *Senior Member, IEEE,* Zonghua Zhang and Jun Shao

***Abstract*—The fast development of intelligent transportation paves the way for innovative techniques in highway, and an entirely new driving pattern of highway vehicular platooning might offer a solution to our long haunted problem of road congestion, travel comfort and road safety. In this vehicular platooning system, a platoon head vehicle provides platoon service to its user vehicles. However, some badly-behaved platoon head vehicles may put the platoon in danger, which makes it crucial for user vehicles to distinguish and avoid them. In this paper, we propose a reliable trust-based platoon service recommendation scheme, called REPLACE, to help the user vehicles avoid choosing badly-behaved platoon head vehicles. Specifically, at the core of REPLACE, a reputation system is designed for the platoon head vehicles by collecting and modeling their user vehicle's feedbacks. Then an iterative filtering algorithm is designed to deal with the untruthful feedbacks from user vehicles. A detailed security analysis is given to show that our proposed REPLACE scheme is secure and robust against badmouth, ballot-stuffing, newcomer and on-off attacks existing in VANETs. In addition, we conduct extensive experiments to demonstrate the correctness, accuracy and robustness of our proposed scheme.**

***Index Terms*—VANET, Vehicular Platooning, Trust, Reputation System, Robustness.**

I. Introduction

With the advance of automobile technology, vehicle manufactures and research academia are heavily engaged in the blueprint of highway vehicular platooning [1]. By linking vehicles into a train-like group, the platooning liberates drivers from the tedium of driving. Besides, this newly emerging highway platooning technique is characterized by enhanced road safety, improved traffic efficiency and less energy consumption due to air drag reduction [2]. Compared to the way of constructing roads, platoon-based driving pattern is a more sustainable and less costly way to alleviate traffic congestion and reduce accidents, which envisions one of the future intelligent transportation systems (ITS). With so significant innovative benefits to achieve, many researchers have shown great interests in the initiative: as a California traffic automation program, PATH [3] is motivated by the need to produce a significant increase in the capacity of a highway lane to meet the increasing travel demand with a minimum new infrastructure construction. SARTRE [4], supported by European Commission, is a project aiming at reducing fuel consumption, increasing safety, efficiency and driver convenience and comfort. Energy ITS [5] is a national ITS project by Japanese Ministry of Economy, Trade and Industry in 2008 to mitigate the problem of lacking skilled drivers.

Though much effort has been invested by engineers and researchers to make such a platooning system work, the challenge of ensuring the security of the system still remains to be tackled before the beauty of platooning can be fully appreciated by its large audience [6]. Without security guarantee, some badly-behaved or malicious platoon head vehicles may jeopardize the system by providing low quality services or even put the user vehicles in dangerous situations [7]. Therefore, how to identify those badly-behaved or malicious platoon head vehicles has become a fundamental requirement in securing vehicular platooning.

In this paper, we propose a reliable trust-based platoon service recommendation scheme, which is termed REPLACE, to rank the platoon head vehicles by establishing a trust and reputation system. In this system, the server uses the feedbacks collected from user vehicles to compute the reputation scores of platoon head vehicles. By doing so, the well-behaved and badly-behaved platoon head vehicles are clearly distinguished according to their reputation scores and then the server will recommend a reliable platoon head vehicle to the user vehicle. However, the system is potentially subject to malicious user vehicles who might give untruthful feedbacks. To mitigate the negative impacts of those malicious user vehicles, we design an iterative filtering algorithm for our REPLACE scheme to exclude their feedbacks. Specifically, the main contributions of this paper are threefold:

- First, we take advantage of the unique features of VANET [8]–[10], e.g., high dynamics, hybrid architecture, vehicle-to-infrastructure (V-2-I) and vehicle-to-vehicle (V-2-V) communications, to propose our REPLACE scheme. Specifically, the high dynamics ensure the real-time update of feedbacks. The hybrid architecture, i.e., vehicles, road side units (RSUs), server and trust authority (TA), enables the storage of feedbacks and computation of reputation scores. Besides, vehicular communications also lay a foundation for platooning service requests and platoon control.
- Second, we design an evaluation mechanism by utilizing performance feedbacks provided by user vehicles as the trust metrics to measure the quality of services of platoon head vehicles. To the best of our knowledge, it is the first attempt to develop a trust and reputation system

H. Hu and R. Lu are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, (e-mail: hhu002@e.ntu.edu.sg, rxlu@ntu.edu.sg)

Z. Zhang is with the IMT/TELECOM Lille, CNRS UMR 5157 SAMOVAR Lab, France, (e-mail: zonghua.zhang@telecom-lille.fr)

J. Shao is with the Department of Information Security, Zhejiang Gongshang University, Hangzhou 310018, China (e-mail: chn.junshao@gmail.com)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

for describing the services of platoon head vehicles, eventually leading to the optimal selection of platoon head vehicles. In particular, the system is developed on the Dirichlet distribution, ensuring high accuracy and dynamics.

- Third, we mitigate the effect of malicious user vehicles' feedbacks by proposing an iterative filtering algorithm to exclude those attackers from our evaluation mechanism. In doing so, the evaluation of the behavior of platnoon head vehicles becomes more accurate, ultimately enabling REPLACE to be resistant against some sophisticated attacks.

The remainder of this paper is organized as follows. In Section II, we formalize the system model and trust model considered in our work, and identify our design goals. In Section III, we briefly recall the Beta distribution and Dirichlet distribution which have been applied in the trust and reputation system. In Section IV, the REPLACE scheme is presented in details, along with the rationale that it can help the query vehicles to choose the highly reliable platoon head vehicles. Security analysis is then introduced in Section V, and the performance evaluation is in Section VI. Finally, we give the related work in Section VII and draw conclusions in Section VIII.

II. System Model, Trust Model and Design Goals

In this section, we formalize the system model, trust model and identify our design goals.

A. System Model

We consider a flourish stage of VANETs where road side units (RSUs) are widely deployed, and each vehicle is equipped with an on board unit (OBU). In particular, the system model of our proposed REPLACE scheme consists of a top trust authority (TA), a server, some stationary road side units (RSUs) and vehicles traveling on the roads equipped with OBUs, as shown in Fig. 1.

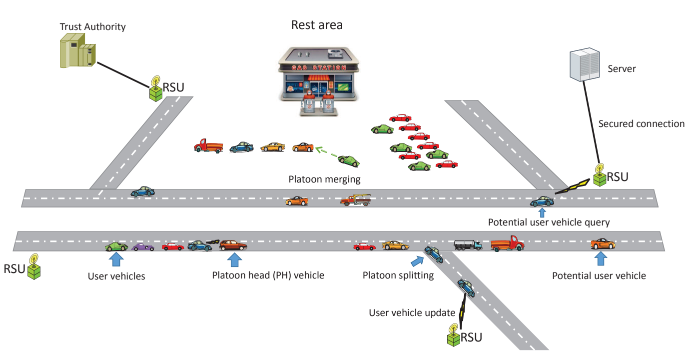


Fig. 1. System model under consideration

TA: Trust authority plays a significant role in the whole system, which takes charge of registration of the server, all RSUs and vehicles.

Server: In general, the server has a high storing and computational capability which stores the feedback data table, trust table and reputation table for the whole system. Using the data in those tables, the server also calculates the trust scores for user vehicles and reputation scores for platoon head vehicles. Specifically, every time when a potential user vehicle requests to join a platoon, server will respond this request by recommending the most trusted platoon head vehicle.

RSUs: RSUs are connected through wired lines and secured channels to the server and TA, meanwhile, they provide wireless connections to the vehicles. Both the feedbacks of user vehicles and trip information updates of platoon head vehicles will be forwarded through RSUs to TA or server. From this point of view, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, we assume that RSUs are widely deployed along the roads to cover the whole area which ensures that the vehicles are able to update the information timely when driving on the roads. In some areas where RSUs are sparsely deployed, the update of the feedbacks and traveling information of platoon head vehicles are delayed, the accuracy of our proposed REPLACE scheme will be decreased. But in the long run, the scheme is still efficient.

Vehicles: The vehicles can be regarded as a group of highly mobile nodes equipped with OBUs which allow them to communicate with other vehicles or RSUs. Through V-2-I communication, a vehicle updates its own traveling information or uploads feedback scores to the server when passing RSUs. The drivers on the vehicles can choose either to drive individually or to join a platoon. Vehicles can be further divided into three categories as follows:

- *PH Vehicles:* In the system, there are a number of m_k platoon head vehicles who form a set $\mathcal{P} = \{ph_1, ph_2, \ldots, ph_{m_k}\}$. The platoon head vehicles take the full control of the whole platoon when driving on the road, they are responsible for the safety, user experience of all platoon user vehicles. More importantly, their behaviors affect the whole road's condition and operation efficiency. It is easy to imagine that such vital roles in the platoon system can only be played by some qualified vehicles which are driven by experienced and capable drivers.
- *Potential user Vehicles:* Except for the PH vehicles, all the other individually driving vehicles can be regarded as potential user vehicles once they drive on the road until they decide to join a platoon.
- *User Vehicles:* In order to reach the destination in a more comfortable and energy saving way, those potential user vehicles have the option to join a platoon via our proposed REPLACE scheme to be a user vehicle v_j. A total number of m_j user vehicles the road form a set $\mathcal{V}$, where $\mathcal{V} = \{v_1, v_2, \ldots, v_{m_j}\}$.

B. Trust Model

In our trust model, we make some assumptions and define the trust levels of different roles in the system model.

- TA: Trust authority maintains the public and private keys of the network which is fully trusted by all roles in the system.

- Server: We assume that server is under so strong physical protection that it is impossible for any attacker to compromise.
- RSUs: RSUs are subordinated to server via reliable communication channel, it will never disclose any internal information without permissions. However, we do not rule out the possibility that a portion of RSUs at the road side are compromised or the attackers even deploy bogus RSUs. Nevertheless, the TA can inspect all RSUs at high level: once the RSUs are compromised, they will be recovered or revoked in the next time slot by TA.
- PH Vehicles: Although PH vehicles are driven by experienced drivers, it does not mean that we can trust them equally since their performances vary for different drivers. Even for the same PH vehicle, its performance changes in different periods and different trips. Besides, PH vehicles may also be compromised by adversaries and provide poor platoon service deliberately. However, we assume that the future behaviors of PH vehicles can be expected according to its historical performances.
- User vehicles: A user vehicle is required to provide a feedback on the PH vehicle's performance after each trip. However, we can not directly use their opinions at all times. The reasons are: first, user vehicles have different capabilities of providing feedbacks, even in the same trip, some of them are able to provide more accurate feedbacks than others; second, some of the user vehicles are compromised to make biased feedbacks, with an intention to disrupt the whole system, while others may collude with each other to give untruthful feedbacks for their own benefits.

C. Design Goals

Different from traditional wireless networks, VANET heavily involves and is affected by human factors. In other words, the behaviors of platoon head vehicles are unpredictable, which makes it hard for potential user vehicles to choose a reliable platoon service when facing multiple platoon head vehicles nearby. To tackle this challenge, three design goals are desirable in the development of our REPLACE scheme. Specifically,

1) **Accurate PH vehicle performance evaluation:** Judging from the platoon service qualities of PH vehicles, there are always relatively badly-behaved PH vehicles on the road. Some of those behaviors may downgrade the user vehicles' experience, others may even put the platoon members in danger. In practice, many reasons lead to the poor performance of PH vehicles, such as poor driving habits, selfishness or intentional attacks. Sometimes PH vehicles drive carelessly or provide bad service only because the lack of supervision in the system. In all the above cases, a performance evaluation scheme is expected to either punish the attackers or motivate careless drivers to provide as best service as they can. In addition, to make the result more accurate, the evaluating scores given by user vehicles should be sufficiently fine-grained and smooth.
2) **Reliable platoon service recommendation:** Under such a situation where reliable and unreliable vehicles are mixed, the selection of PH vehicle is a significant issue. To help the potential user vehicles avoid badly-behaved vehicles, our scheme should be able to accurately distinguish between well-behaved and badly-behaved PH vehicles so as to recommend the most reliable PH vehicles.
3) **Robustness against malicious user vehicles:** To build the reputation of PH vehicles, the platoon user vehicles are asked to provide the feedbacks about the performance of PH vehicles in a series of trips. However, some malicious user vehicles can intentionally manipulate the feedbacks or collude with each other to provide bogus feedbacks deliberately. Such attacks will eventually subvert the evaluation process of PH vehicles, resulting in the untruthful evaluations on PH vehicles. Other malicious user vehicles may behave well and badly alternatively. After accumulating high trust value, they start doing bad things. Our proposed scheme should be able to filter out those unfair feedbacks and resist against those malicious attacks.

III. Preliminaries

In this section, we briefly outline the Beta distribution and Dirichlet distribution [11] which will serve as the basis of our proposed scheme.

A. Beta Distribution

Defined on the interval of [0,1], beta distribution is a family of continuous probability distributions indexed by two parameters α and β. A random variable X beta-distributed with parameters α and β can be denoted by: $X \sim Beta(\alpha, \beta)$. Given that Gamma function is an extension of the factorial function where $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1}e^{-x}dx$. The probability density function (PDF) $f(x|\alpha,\beta)$ can be expressed by using gamma function Γ as: $f(x|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1}$, where $0 \leq x \leq 1$, $\alpha > 0$, $\beta > 0$. The probability expectation value of the beta distribution is given by:$E(x) = \frac{\alpha}{\alpha+\beta}$.

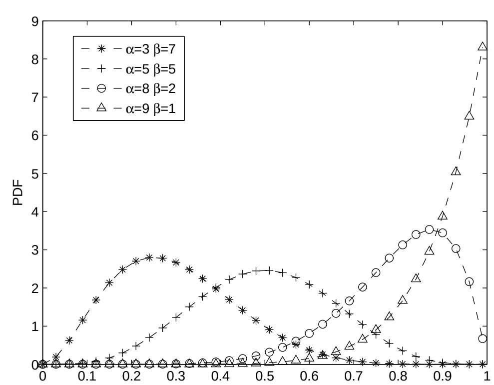


Fig. 2. PDF of beta distribution with parameter α and β

Fig. 2 shows the PDF of beta distribution with different parameters α and β. It expresses the uncertain probability

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

that a process will produce positive outcomes in future. Take an example, when $\alpha = 8$, $\beta = 2$, according to expectation equation, the probability expectation value of this type of beta distribution is $E(x) = 0.8$, which can be interpreted as the relative frequency of positive outcome is somewhat uncertain and that the most likely value is 0.8.

B. Dirichlet Distribution

The Dirichlet distribution is a family of continuous multivariate probability distributions parameterized by a priori parameter vector $\overrightarrow{\alpha}$. It is the conjugate prior distribution for the parameters of the multinomial distribution. In case of a binary state space, it is determined by the Beta distribution [12]. Generally, we can use the Dirichlet distribution to describe the probability distribution over a k-component random variable $\overrightarrow{X} = \{X_1, X_2, \cdots, X_k\}$. If $\overrightarrow{p} = \{p_1, p_2, \cdots, p_k\}$ is the probability distribution vector of X, it satisfies $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i$ $(1 \leq i \leq k, \theta_i \in [0, 1], \theta_{i+1} > \theta_i)$. The Dirichlet distribution captures a sequence of observations of k possible outcomes, those observations serve as the prior parameter $\overrightarrow{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, which denote the cumulative observations and initial beliefs of X. $\overrightarrow{p}$ is a k-dimensional random variable and $\overrightarrow{\alpha}$ is a k-dimensional random observation variable. The probability density function is given by:

$$f(\overrightarrow{p}|\overrightarrow{\alpha}) = \frac{\Gamma(\Sigma_{i=1}^{k}\alpha_i)}{\prod_{i=1}^{k}\Gamma(\alpha_i)}\prod_{i=1}^{k}p_i^{\alpha_i-1} \tag{1}$$

where $0 \leq p_1, p_2, \cdots, p_k \leq 1$; $\sum_{i=1}^{k} p_i = 1$; $\alpha_1, \alpha_2, \ldots, \alpha_k > 0$. The expected value of the probability that X to be x_i given the observations vector $\overrightarrow{\alpha}$ is given by: $E(p_i|\overrightarrow{\alpha}) = \frac{\alpha_i}{\sum_{i=1}^{k}\alpha_i}$. Furthermore, if we let $\alpha_0 = \sum_{i=1}^{k}\alpha_i$, the variance of the event of X to be x_i is given by: $Var[X = x_i] = \frac{\alpha_i(\alpha_0-\alpha_i)}{\alpha_0^2(\alpha_0+1)}$. If $i \neq j$, the covariance is: $Cov[X = x_i, X = x_j] = \frac{-\alpha_i\alpha_j}{\alpha_0^2(\alpha_0+1)}$.

C. Trust and Reputation

Trust: Trust is defined as a particular level of subjective probability with which an agent assesses another agent or a group of agents who will perform a particular action before it can monitor such action (or independently of its capacity ever to be able to monitor it) and in a context in which it affects its own action [13]. When we say someone is trustworthy, we implicitly mean that it will perform an action within our expectation so that we can cooperate with it. It can be represented as a particular expectation regarding the behaviors.

Reputation: The term reputation can be described as a long term collective measure of trust which can be used to decide whether a vehicle is malicious or honest. It is an abstract definition that reflects the observations of all members in a particular entity.

IV. Proposed REPLACE Scheme

In this section, we propose our REPLACE scheme which consists of five parts: system initialization, quality of feedbacks calculation, Dirichlet-based model, trustworthiness of user vehicles and reputation of PH vehicles. The architecture of our proposed scheme is shown in Fig. 3.

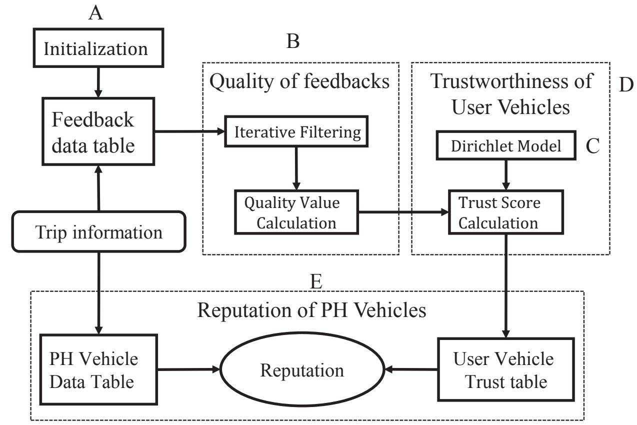


Fig. 3. Architecture of REPLACE Scheme

A. System Initialization

Given the security parameters, TA first generates and publishes its own public key PK_{TA}, the public keys of RSUs and vehicles are their IDs. Before an RSU or a vehicle registers itself to the system, it submits its identity to TA to obtain its private key SK_{RSU} or SK_v.

Let $\mathcal{T}$ be the set of trips with the total number of m_i so that $\mathcal{T} = \{Tr_1, Tr_2, \ldots, Tr_{m_i}\}$. After a user vehicle $v_j \in \mathcal{V}$ uses the platoon service provided by a PH vehicle $ph_k \in \mathcal{P}$ in trip $Tr_i \in \mathcal{T}$, it is required to provide a feedback of that trip Tr_i, which is denoted by $f_j^i(\in [0, 1])$. This feedback together with the PH vehicle ID ph_k, trip ID Tr_i and trip time t_i will be uploaded to server, where i denotes the sequence number of trips, t_i is the beginning time of Tr_i. We note that since the feedback data keeps being updated, m_i, m_j and m_k increase by time. However, when calculations are conducted, the server collects the data in a time window so that at that time the feedback data table can be regarded as static without any new records coming in.

As shown in the Fig. 4(a), the server will establish such a feedback data table which stores the feedbacks from all user vehicles in each trip Tr_i. The trips will be arranged in sequence, e.g., $\{Tr_1, Tr_2, \cdots, Tr_i, \cdots\}$, this table will be updated once a new piece of record is uploaded. Another trust table is also established by the server to record all of the user vehicle identity $v_j \in \mathcal{V}$ and their trust scores $T_j (j = 1, 2, ..., m_j)$, which is shown in Fig. 4(b). Those trust scores are used to describe the reliability and accuracy of v_j's feedbacks. We will describe the calculation of these trust scores later, but initially, $T_j = T_0 (j = 1, 2, ..., m_j)$. T_0 will not be given a high value to resist against newcomer attack. The reputation scores Rep_k of PH vehicles are also initialized as $Rep_k = Rep_0$.

B. Quality of Feedbacks

In order to evaluate the quality of user vehicle v_j's feedback in trip Tr_i, we first calculate the integrated feedback of the trip Tr_i, denoted by TR_i, which could be regarded as a real performance of the PH vehicle in Tr_i by combining all feedbacks about Tr_i together. Then TR_i will be compared to f_j^i, a greater difference leads to a lower quality value of this

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

Trip	User Vehicle	PH Vehicle	Time	Feedback
⋮	⋮	⋮	⋮	⋮
Tr_i	v_j	ph_k	t_i	f_j^i
⋮	⋮	⋮	⋮	⋮

(a) Feedback Data Table

User Vehicle ID	Trust Score
⋮	⋮
v_j	T_j
⋮	⋮

(b) User Vehicle Trust Table

PH Vehicle	Trip ID	User Vehicle ID	Feedback
	⋮	⋮	⋯
		⋮	⋯
ph_k	Tr_i	v_j	f_j^i
		⋮	⋯
	⋮	⋮	⋯

(c) PH Vehicle Data Table

Fig. 4. Tables that are established and updated by the server

feedback f_j^i. It is obvious that the accuracy of TR_i determines the accuracy of the quality value on feedback.

However, due to the existence of badmouth or ballot-stuffing attackers in the user vehicles who always give untruthful feedbacks, those feedbacks in the feedback data table can never be used directly to compute TR_i. Therefore, before calculating the quality values of feedbacks, we develop an iterative filtering algorithm which is able to exclude the feedbacks from attackers. Specifically, we achieve our goals in two steps:

1) *Filtering out untruthful feedbacks:* The relationship between the user vehicles and the trips is depicted in Fig. 5.

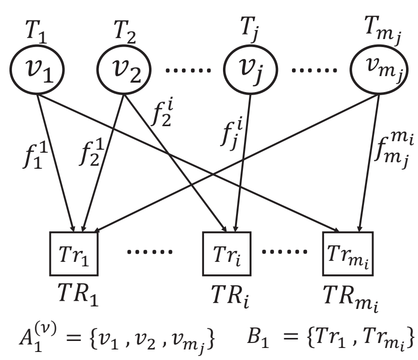


Fig. 5. User vehicles give feedbacks on trips

Inspired by the work of [14], in our proposed iterative filtering algorithm, we use the circles and squares to represent the user vehicles and trips respectively. Assume that the feedback graph has m_i trips and m_j user vehicles in total. If a user vehicle v_j gives a feedback on trip Tr_i, we place an arrowed solid line from v_j to Tr_i. At each iteration, the collection of all feedbacks of a trip will be combined to estimate the value of integrated feedback on the trip in that round. Once the values of integrated feedbacks are estimated, in next iteration, those values will be used to determine the quality values of the user vehicles' feedbacks.

Each trip comprises different user vehicles, we use $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{m_i}$ to represent the set of user vehicles of trip $Tr_1, Tr_2, \cdots, Tr_{m_i}$ respectively. The sets will be updated after each iteration because some of the user vehicles will be in blacklist after iteration. We denote ν to be the round number of the iteration. $\mathcal{A}_i^{(\nu)}$ denotes the set of user vehicles of trip Tr_i after the ν^{th} round. In the very beginning, we can easily get $\mathcal{A}_i^{(0)}$, $i \in \{1, 2, \cdots, m_i\}$ from the feedback data table. Similarly, for each user vehicle who takes part in different trips, we use $\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_{m_j}$ to represent the set of trips that the user vehicles $v_1, v_2, \cdots, v_{m_j}$ take part in. At the ν^{th} round, the iterative algorithm will be executed, we computed the integrated feedback of Tr_i as:

$$TR_i^{(\nu+1)} = \frac{\sum_{v_j \in \mathcal{A}_i^{(\nu)}} T_j \cdot f_j^i}{\sum_{v_j \in \mathcal{A}_i^{(\nu)}} T_j} \tag{2}$$

where $\mathcal{A}_i^{(\nu)}$ is the set of all user vehicles in trip Tr_i at the ν^{th} round. T_j represents the trust score of a user vehicles v_j.

Then we compute the inconsistency factor $C_j^{(\nu+1)}$ for each user vehicle v_j using the integrated feedbacks of each trip $TR_i^{(\nu+1)}$. For v_j, since it gives feedbacks to different trips at different times, the time factor should be incorporated as well:

$$C_j^{(\nu+1)} = \frac{\sum_{Tr_i \in \mathcal{B}_j^{(\nu)}} \lambda^{t-t_i} \cdot |f_j^i - TR_i^{(\nu+1)}|}{\sum_{Tr_i \in \mathcal{B}_j^{(\nu)}} \lambda^{t-t_i}} \tag{3}$$

where λ and t_i are the fading parameter and the beginning time of the trip Tr_i. After computing the inconsistency factors of all user vehicles, we select those whose inconsistency factors are greater than a specific threshold $C_{threshold}$ and remove them from the $\mathcal{A}_i$ in the next round. The iteration stops when the difference between $TR_i^{(\nu+1)}$ and $TR_i^{(\nu)}$ is smaller than a threshold $TR_{threshold} (\in [0, 1])$.

2) *Quality value calculation of feedbacks:* To measure the quality of feedback quantitatively, we use a function $QVal (\in [0, 1])$ to represent the quality values of feedbacks. For a user vehicle v_j in trip Tr_i, its feedback is given by f_j^i, we assume that the trips's integrated feedback TR_i converges at the ν^{th} round. The quality value of v_j's feedback f_j^i can be represented as:

$$QVal = 1 - |f_j^i - TR_i^{(\nu)}|^{\nu \cdot c_1} \tag{4}$$

Note that ν is the number of rounds to get a convergent integrated feedback, the larger is ν, the more malicious user vehicles exist, the more difficult it is to give a feedback accurately. Hence ν can be used as an award to the quality value of feedback when there are more malicious user vehicles. c_1 controls the award sensitivity, with larger values representing more awards to the quality values.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

Algorithm 1 Iterative filtering

Input: Records in the feedback data table
Output: Trip Tr_i's integrated feedback TR_i

$\nu \Leftarrow 0$
$difference \Leftarrow 100$
while $difference \geq TR_{threshold}$ **do**
  for $Tr_i \in \mathcal{T}$ **do**
    calculate $TR_i^{(\nu+1)}$
  end for
  for $v_j \in \mathcal{A}_i^{(\nu)}$ **do**
    calculate $C_j^{(\nu+1)}$
  end for
  for $Tr_i \in \mathcal{T}$ **do**
    for $v_j \in \mathcal{A}_i^{(\nu)}$ **do**
      if $C_j^{(\nu+1)} > C_{threshold}$ **then**
        remove v_j from $\mathcal{A}_i^{(\nu)}$ to form $\mathcal{A}_i^{(\nu+1)}$
      end if
    end for
  end for
  $difference = TR_j^{(\nu+1)} - TR_j^{(\nu)}$
  $\nu = \nu + 1$
end while
return $TR_i^{(\nu+1)}$

C. Dirichlet-based Model

A Dirichlet distribution is based on initial belief on an unknown event according to prior distribution. It provides a solid mathematical foundation for measuring the uncertainty of feedbacks based on historical data. Compared to Beta distribution which is more appropriate in a binary satisfaction level [15], Dirichlet distribution is more appropriate for multi-valued satisfaction levels [16]. In our case, the evaluation trustworthiness of user vehicles are described by continuous trust values. Therefore, we use Dirichlet distribution to estimate the quality values of user vehicle' feedbacks in the future and then build our trust model accordingly.

For a specific user vehicle v_j, let X $(0 \leq X \leq 1)$ be the continuous random variable denoting the quality value of v_j's feedback. In order to classify the historical and future quality values, we also denote a number of l satisfaction levels of feedbacks as a set $\{\theta_1, \theta_2, \cdots, \theta_l\}$ $(\theta_i \in (0,1], i \in [1,l], \theta_i < \theta_{i+1})$. Let $\overrightarrow{p} = \{p_1, p_2, \cdots, p_l\}(\sum_{i=1}^{l} p_i = 1)$ be the probability distribution vector of X with respect to satisfaction levels, so that we have $P\{\theta_{i-1} < X_i \leq \theta_i\} = p_i (i = 1, 2, \cdots, l)$. To make it more mathematically precise, we define $\theta_0 = 0$ when $i = 1$, $X_i = 0$ is categorized into θ_1.

Following the steps in Section IV-B, the server is able to calculate the quality values of v_j's historical feedbacks, then we let $\overrightarrow{\gamma} = \{\gamma_1, \gamma_2, \cdots, \gamma_l\}$ denote the vector of cumulative historical data and initial belief of X. With a posterior Dirichlet distribution, $\overrightarrow{p}$ can be modeled as:

$$f(\overrightarrow{p}|\xi) = Dir(\overrightarrow{p}|\overrightarrow{\gamma}) = \frac{\Gamma(\Sigma_{i=1}^{l}\gamma_i)}{\prod_{i=1}^{l}\Gamma(\gamma_i)} \prod_{i=1}^{l} p_i^{\gamma_i - 1} \quad (5)$$

where ξ denotes the background information represented by $\overrightarrow{\gamma}$. Let:$\gamma_0 = \sum_{i=1}^{l}\gamma_i$. The expected value of the probability of $X_i \in (\theta_{i-1}, \theta_i]$ with the historical distribution of quality values is given by:

$$E(p_i|\overrightarrow{\gamma}) = \frac{\gamma_i}{\gamma_0} \quad (6)$$

Consider the time factor of historical quality values, we introduce a forgetting factor β to give greater weight to more recent quality values:

$$\overrightarrow{\gamma^{(n)}} = \begin{cases} \overrightarrow{S}^{(0)} & (n = 0) \\ \sum_{i=1}^{n} \beta^{t-t_i}\overrightarrow{S}^{(i)} + c_0\overrightarrow{S}^{(0)} & (n \geq 1) \end{cases} \quad (7)$$

where n is the total number of historical quality values; $\overrightarrow{S^{(0)}}$ is the initial belief vector when $n = 0$. Since no prior information is available, all elements of $\overrightarrow{S^{(0)}}$ have equal probability which makes $\overrightarrow{S^{(0)}} = (\frac{1}{l}, \frac{1}{l}, \cdots, \frac{1}{l})$. Parameter $c_0 > 0$ is a weight on the initial beliefs. In the i^{th} trip of v_j $(Tr_i \in \mathcal{B}_j, 1 \leq i \leq n)$, $\overrightarrow{S^{(i)}}$ denotes the satisfaction level of its quality value, which contains only one element set to 1 corresponding to the selected satisfaction level and all the other $k-1$ elements set to 0. t_i stands for the beginning time when the i^{th} trip took place and t is the moment of running the algorithm. The forgetting factor is $\beta \in [0,1]$, smaller β means that the system is easier to forget the historical records and vice versa. In order to defend against on-off attack [17], we choose an adaptive value as β:

$$\beta = c_3 \cdot (1 - T_j) \quad (8)$$

c_3 is a parameter to control the forgetting factor, the larger value of c_3 makes the system more forgettable about the historical behaviors and vice versa. From the equation we can see that when v_j has a high trust value, its forgetting factor is small, which means that those good behaviors of giving truthful feedbacks will be easily forgotten. On the contrary, once v_j performs as a malicious attacker, its trust value gets lower and forgetting factor becomes larger. This means that all of those bad behaviors will be memorized and it takes even longer time for v_j to build up a high trust value again.

D. Trustworthiness of a User Vehicle

For an arbitrary user vehicle v_j, to evaluate its trustworthiness when giving feedbacks, we assign the weight ω_i to each satisfaction level $\theta_i (i \in [1,k])$. Let p_i denote the probability that the quality value of v_j's feedback is categorized into the satisfaction level of θ_i. $\overrightarrow{p} = (p_1, p_2, \cdots, p_k)|\sum_{i=1}^{k} p_i = 1$. We model $\overrightarrow{p}$ using equations in Section IV-C. Let Y be the random variable denoting the weighted average of the probability of each satisfaction level in $\overrightarrow{p}$, the trust score T_j of v_j is represented as:

$$T_j = E[Y] = \sum_{i=1}^{k} \omega_i E[p_i] = \frac{1}{\gamma_0}\sum_{i=1}^{k}\omega_i\gamma_i \quad (9)$$

where γ_i is the cumulated evidence that v_j's feedback's quality value is with satisfaction level of θ_i. Using the trust scores of user vehicles, the server updates the trust table in Fig. 4.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

E. Reputation of PH Vehicles

In order to calculate the reputation of a PH vehicle which reflects the opinions from all user vehicles, a feedback table specific for each PH vehicle is designed. As shown in Fig. 4(c), for a PH vehicle ph_k in the system, it records all trips of ph_k and the feedbacks from each user vehicle in the corresponding trip. Let $\mathcal{C}_k$ be the set of all trip IDs for ph_k. For a specific trip $Tr_i \in \mathcal{C}_k$, as defined before, $\mathcal{A}_i$ is the set of all user vehicle IDs in that trip.

The reputation of ph_k can be calculated by aggregating all the feedbacks of ph_k's user vehicles based on the trustworthiness of those user vehicles. Using the weight majority method, ph_k's reputation score is given by:

$$Rep_k = \frac{\sum_{Tr_i \in \mathcal{C}_k} \sum_{v_j \in \mathcal{A}_i, T_j \geq T_{TH}} \eta^{t-t_i} \cdot T_j \cdot f_j^i}{\sum_{Tr_i \in \mathcal{C}_k} (\sum_{v_j \in \mathcal{A}_i, T_j \geq T_{TH}} \eta^{t-t_i} \cdot T_j)} \quad (10)$$

where η is the forgetting factor of the outdated feedbacks in accumulation. To make the aggregated evaluation more accurate, the requesting vehicle applies a threshold $T_{threshold}$ on choosing user vehicles' feedback for ph_k.

V. Security Analysis

In this section, we analyze the security properties of our proposed REPLACE scheme. Specifically, some attack strategies will be described followed by the resilience analysis against those attacks:

Resilience to badmouth attack: In the proposed REPLACE scheme, a badmouth attack is meant that a collective of user vehicles always give lower feedback scores to the well performed PH vehicles. In some cases the badmouth user vehicles originate by selfish drivers who attempt to lower the high reputation of well performed PH vehicles with the hope of improving their own chances to be PH vehicles. To prevent those attacks, the proposed REPLACE scheme incorporates an iterative filtering algorithm to find out the untruthful feedback providers and then remove their feedbacks.

Resilience to ballot-stuffing attack: Similar to the badmouth attack, another group of malicious user vehicles may collude to increase the reputation values of PH vehicles with low reputations by always giving them good feedbacks no matter what their performances are. It could be mounted by a group of malicious vehicles to favor their allies. Similar to the badmouth attack, our defense against ballot-stuffing attacks relies on the iterative filtering algorithm to exclude the feedbacks from ballot-stuffing attackers.

Resilience to rough RSU attack: Although all the deployed RSUs are trusted in the system, an adversary could place rogue RSUs along the roads which intentionally drop the feedback data that should be uploaded to the server to degrade the trustworthy environment of VANET. In our proposed REPLACE scheme, V-2-I communication implicitly achieves mutual authentication by establishing a non-interactive session key. If an RSU is a rogue RSU, it cannot successfully generate the session key. Therefore, rogue RSU attack can be countered in the REPLACE scheme.

Resilience to newcomer attack: The newcomer attacks occur when a malicious user vehicles abandon their low trusted old IDs and register new IDs to launch new attacks [18]. This type of attack is mitigated in two ways: on one hand, our proposed scheme assigns low initial trust scores to the new IDs so it requires a longer time for the new user vehicles to accumulate high trust scores; on the other hand, in VANET, the user vehicle ID is connected to the driving license in real world, which makes it harder for a malicious driver to spoof ID easily.

Resilience to on-off attack: User vehicles may behave well and badly alternatively with the hope to hide themselves by building up high trust or reputation scores before launching attacks. Those attackers exploit the forgetting factor of the system to launch attacks. Specifically, user vehicles may give truthful feedbacks at first, in order to accumulate trustworthiness. When their trust scores get high enough, they launch attacks and remain silent thereafter. Since the system forgets about the past behaviors gradually, their trust scores recover slowly and they repeat the steps above. Those attackers are hard to be detected using the traditional method, but we handle this problem by adopting an adaptive forgetting factor in our proposed REPLACE scheme. The method is inspired by a common human nature: it takes long time to build up trust among others and only a few bad behaviors will ruin it. The method is effective in mitigating the on-off attacker in our VANET system.

VI. Performance Evaluation

We will evaluate the performance of our proposed REPLACE scheme in this section, the numerical data are generated in Matlab. The performance metrics used in the evaluation are: i) trust scores in terms of the round for different user vehicles; ii) reputation scores' variations with round for PH vehicles with different performances; iii) detection rate variations with round of badmouth and ballot-stuffing attackers.

A. Simulation Settings

We design a simulation to evaluate our proposed REPLACE scheme in which only a set of key factors are considered and specified in order to validate the performance of platoon head vehicles and the feedback accuracy of user vehicles. It is worth noting that the selected factors are not related to the movement of vehicles and the packets collision problems. In this case, we simulate the proposed scheme in the environment of MATLAB where there are a total number of m_j user vehicles and m_k PH vehicles. To ensure the fairness, we suggest that each PH vehicle provides n times of service in each round, and in each service the same amount of user vehicles take part in the trip. A total number of N rounds will be run for evaluation.

B. Modeling the PH Vehicles and User Vehicles

Due to the lack of real data, we need to model the malicious behaviors of not only PH vehicles but also user vehicles in order to test the performance of our system.

- **Performance quality level (PQL) of PH vehicles:** We define a parameter as performance quality level (PQL)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

TABLE I
SIMULATION PARAMETER SETTINGS

Notation	Definition	Value
m_j	user vehicle number	100
m_k	PH vehicle number	20
n	service times per vehicle per round	4
N	number of rounds	50, 100
c_0	initial belief weight	1
c_1	award sensitivity	1
c_2	variance sensitivity	10
c_3	forgetting factor parameter	0.5
$C_{threshold}$	inconsistency threshold	0.3
$TR_{threshold}$	stability threshold	0.1
$T_{threshold}$	trust threshold	0.3
T_0	initial trust score	0.5
Rep_0	initial reputation score	0.5
q_{bm}	percentage of badmouth attackers	10%, 40%
q_{bs}	percentage of ballot-stuffing attackers	5%, 20%
l_{ph}	performance quality level	0.8, 0.98
l_v	feedback accuracy level	0.92, 1

$l_{ph} \in [0, 1]$ to describe the capability of a PH vehicle to provide high quality services. A PH vehicle with higher l_{ph} may provide higher quality services. Specifically, given a PH vehicle with l_{ph}, we use the beta distribution to describe the performance quality variable X of that PH vehicle, the probability density function of beta distribution can be expressed as:

$$f(x|\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} \tag{11}$$

where $\Gamma(\alpha) = \int_0^\infty x^{\alpha-1}e^{-x}dx$. $f(x|\alpha, \beta)$ is the probability that a PH vehicle with PQL of l_{ph} provides a service with the quality value of $x \in [0, 1]$. Higher values of l_{ph} imply that the PH vehicle provides a higher quality service. To achieve this goal, we define α and β as follows:

$$\begin{aligned} \alpha &= c_2 \cdot l_{ph} \\ \beta &= c_2 \cdot (1 - l_{ph}) \end{aligned} \tag{12}$$

where c_2 is the parameter to control the variance of the distribution, when c_2 is given a larger value, the performance quality values will have a larger variance and vice versa. For a PH vehicle with PQL of l_{ph}, the above model has the property of generating a service quality score which follows a beta distribution with the expectation $E(X) = l_{ph}$. We assume that all of the PH vehicles are relatively experienced drivers so that we set l_{ph} with the range from 0.8 to 1. If there are malicious PH vehicles, we give lower l_{ph} values to them and the performance of our proposed scheme will be better.

- **Feedback accuracy level (FAL) of user vehicles:** The capability of a user vehicle to give an accurate feedback regarding the performance of a PH vehicle can be determined by another parameter l_v: feedback accuracy level (FAL). Given a performance score of x, the user vehicle with FAL of l_v gives evaluation as follows:

$$eva = x \pm 10\% \cdot x \cdot (1 - l_v) \tag{13}$$

From the experience we find that the evaluation errors always exist which could be regarded as a random noise added to the real performance score with the mean value of x. As shown in the equation, the errors are controlled by l_v. When there are no attackers, all of those user vehicles are honest, so $l_v \in [0.8, 1]$.

C. Modeling Attackers in User Vehicles

- **Badmouth/Ballot-stuffing attackers:** In the simulation, the badmouth attackers always evaluate the PH vehicles with the score of “0” while ballot-stuffing attackers give “1” to all PH vehicles. The ratio of badmouth attackers and ballot-stuffing attackers in all user vehicles are q_{bm} and q_{bs} respectively.
- **On-off attackers:** The on-off attackers accumulate a high trust score before they launch the badmouth attacks, at round 20 they turn on until round 40, later their trust scores recovery to a high level gradually and then they repeat the step above.

D. Reputation Scores of PH Vehicles

In the first experiment, we study the effectiveness of our proposed REPLACE scheme regarding reputation scores without any attackers. That says, all user vehicles are honest to provide truthful feedbacks though their evaluating abilities vary. We do simulation in the whole system for 50 rounds and track the reputation scores of two different PH vehicles with different performance quality levels. Fig. 6 shows the reputation changes with round. The PH vehicles with different PQLs are able to be distinguished by our scheme.

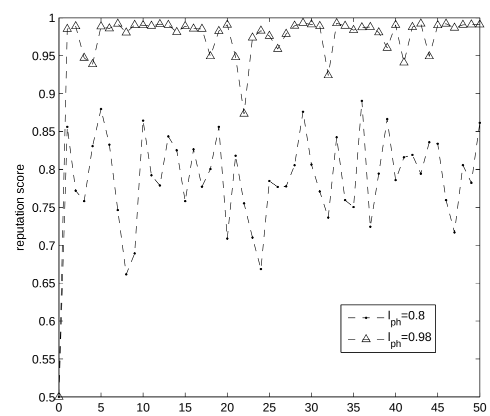


Fig. 6. Reputation scores comparison between PH vehicle with $l_{ph} = 0.8$ and $l_{ph} = 0.92$

E. Trust Scores of User Vehicles

The goal of this experiment is to compare the trust scores of malicious and honest user vehicles with different feedback accuracy levels. For a better comparison, we choose two honest users with FAL of $l_v = 1$ and $l_v = 0.92$ respectively. Besides, another two attackers who launch badmouth and ballot-stuffing attacks are also put in the system. After “50” rounds, we plot their trust scores in Fig. 7.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

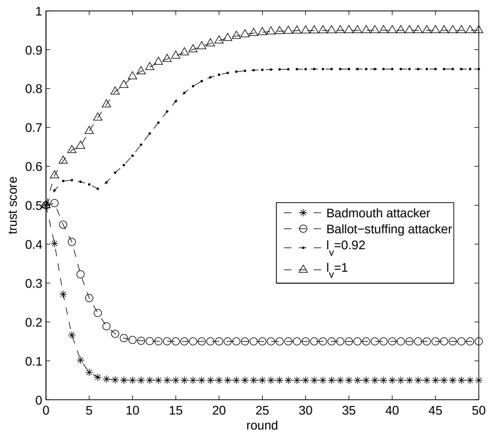


Fig. 7. Trust scores comparison between honest user vehicles with $l_v = 0.92$, $l_v = 1$ and malicious attackers

We notice that the trust scores of all user vehicles converge after "20" rounds. It is obvious that the honest user vehicles with $l_v = 1$ and $l_v = 0.92$ get the highest trust scores after the experiments, on the contrary, both of the attackers get the low trust scores. We also notice that a user vehicle with larger FAL will achieve higher trust score, which shows the effectiveness of our trust model to identify user vehicles according to their actual FALs. Besides, the converged trust scores of badmouth attacker is a little lower than ballot-stuffing attacker, the reason is that PH vehicles in the system provide service with PQL between 0.8 and 1, so that badmouth attackers who always give "0" to all services will suffer more punishments.

F. Robustness of Our Proposed Scheme

In this experiment, we study the robustness of our proposed scheme against different types of attackers.

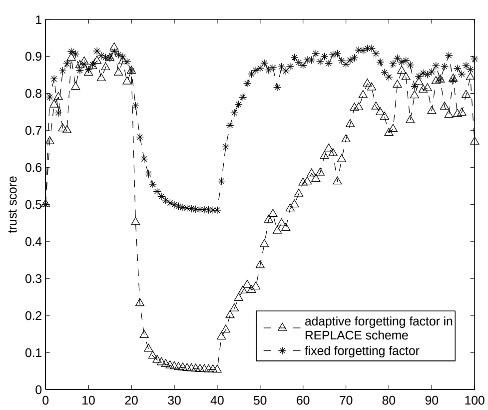


Fig. 8. Trust score comparison of the same on-off attacker under REPLACE scheme with adaptive forgetting factor and under another scheme with fixed forgetting factor

One possible threat is the on-off attack when a user vehicle is compromised. In this scenario, the compromised vehicle will perform as usual to gain high trust score and then suddenly turn to badmouth vehicle and launches attacks. We simulate this case by putting on-off attacker in our system, the attacker with an initial trust $T = 0.5$ behaves honestly in the first 20 rounds. After that, it launches badmouth attack for another 20 rounds and then turn off the attack. Fig. 8 shows the trust scores of one on-off attacker with a fixed forgetting factor and another with an adaptive forgetting factor which is utilized in our proposed scheme. From the figure, we can find that the system with a fixed forgetting factor is more vulnerable to on-off attackers since the attacker recovers after only 10 rounds once it stops launching attacks. On the contrary, in our proposed scheme, when the attacker builds up high trust score at first, its forgetting factor is a small value, resulting in a steep decrease of its trust score once the attacker starts launching attacks. With the decrease of the trust score, its forgetting factor will increase, which means it remembers more of the previous performance. As a result, the recovery of the attacker's trust score will be very slow. From the figure, we can see that to beat the proposed adaptive forgetting factor with parameter $c_1 = 0.5$, the on-off attacker spends five times of rounds to recover than beating the usual fixed forgetting factor. The method is very effective in protecting the system against on-off attackers.

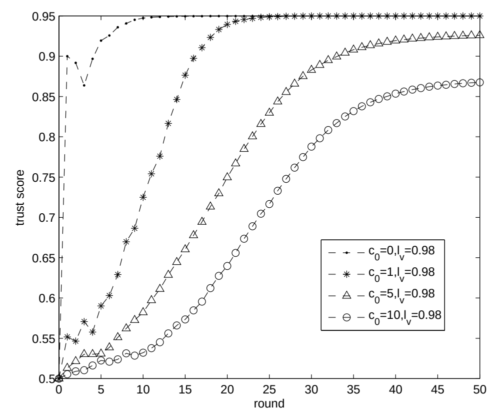


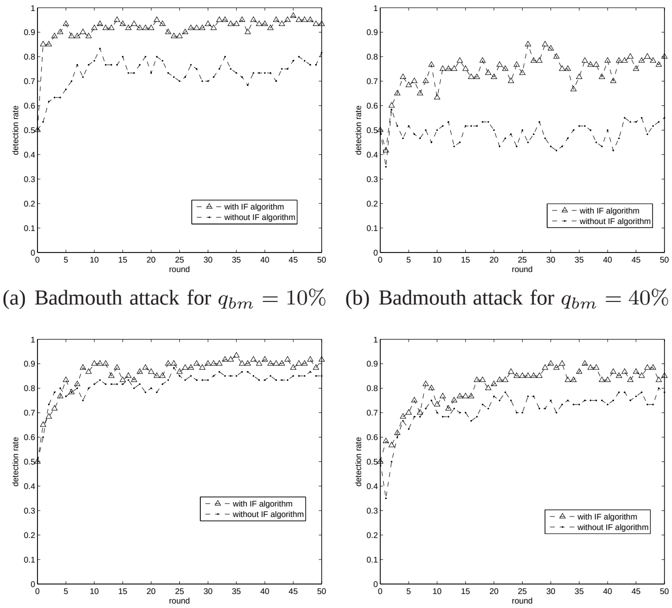
Fig. 9. Trust scores comparison of a newcomer attacker with different c_0 values

Fig. 9 shows the robustness of our scheme against newcomer attacks. As described in Section IV-C, c_0 is the constant to control the initial prior feedback quality value. $c_0 = 0$ means no initial values. In this case the newcomer will gain trust very fast and converge soon, and the system will also be vulnerable to newcomer attack. When we give higher initial prior feedback quality value c_0 to the user vehicles in the trust system, it takes longer time for a newcomer to accumulate a converged trust value. By choosing c_0 properly, the system is able to resist against newcomer attacks without affecting the trust evaluation of the other user vehicles.

To demonstrate the robustness of our proposed scheme against badmouth and ballot-stuffing attacks, we simulate these two cases separately. We define the top 20% number of user vehicles with the highest l_v as "good user vehicles". After the service, all user vehicles will re-ranked, then the detection rate can be defined as the ratio of "good user vehicles" who still remain top 20% in the new ranking list.

We set the percentage of badmouth attackers q_{bm} in the system as 10% and 40% respectively, the result is shown in Fig. 10(a) and 10(b). From the figures, we can find that our scheme with iterative filtering (IF) algorithm performs

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology



(a) Badmouth attack for $q_{bm} = 10\%$ (b) Badmouth attack for $q_{bm} = 40\%$

(c) Ballot-stuffing attack for $q_{bs} = 5\%$ (d) Ballot-stuffing attack for $q_{bs} = 20\%$

Fig. 10. Resilience to badmouth attacker and ballot-stuffing attack by comparing detection rate between REPLACE scheme with and without iterative filtering algorithm

better than the system without IF algorithm. The detection rate reaches 90% even when the badmouth ratio is 10%. Similarly, in Fig. 10(c) and 10(d), our system still performs better given that the ballot-stuffing ratio q_{bs} are 5% and 20%. Compare the two experiments, we may find that our system is more tolerable against badmouth attack than ballot-stuffing attack. This finding can be explained as follows: the PH vehicle always provides services with high qualities, hence the strategy of badmouth attacker is more easily exposed. In a word, the experiment shows that our scheme is very robust against both badmouth and ballot-stuffing attacks.

VII. Related Work

Platoon-based driving pattern attracts much attention due to its potential to improve the road capacity and energy efficiency [19]. Among all of issues in platooning technique, how to manage the platooning system has always been an urgent topic [20].

However, none of the platoon management models solve the problem of reliable PH vehicle selection. To solve the problem of reliable PH vehicle selection and then help user vehicles avoid badly-behaved PH vehicles, a possible solution could be evaluating the trustworthiness of the PH and user vehicles. Trust and reputation models in VANET have been studied by many researchers [21]–[23]. Patwardhan et al. [21] present a distributed reputation management scheme for VANET, which enables vehicles to quickly adapt to changing local conditions and provides a bootstrapping method for establishing trust relationships. However, the lack of scalability and robustness makes it hard to be applied in the platoon scenario. Different from traditional entity-based trust model, Raya et al. [22] suggest a data-oriented trust establishment framework. By combining trust values of each piece of data together, their framework deals well with ephemerality and functions well in sparse areas. However, in our platoon scenario, the large amount of feedback data make their framework less efficient. Chen et al. [23] propose a trust-based message propagation and evaluation framework in VANET, however, the lack of robustness has also been its weakness.

Combining the above platoon management models and trust models together, our proposed REPLACE scheme is focused on evaluating the platoon head vehicles based on their performances. Specifically, there are several aspects which make our proposed scheme different: first, we establish a reputation system as a long-term evaluation metric of evaluation. Second, a recommendation scheme is developed to solve the problem of distrust on unknown platoon head vehicles. Third, our proposed scheme is resistable against several sophisticated attacks for reputation systems, such as badmouth attacks, newcomer attacks and on-off attacks.

VIII. Conclusion

In this paper, we have proposed a recommendation scheme for user vehicles to select platoon head vehicle before joining a platoon. Considering the uncertainties of human behaviors, the scheme is reputation-based using the weighted majority method by adding up all of the historical feedbacks from the user vehicles together. It is well perceived that the feedbacks from the user vehicles could also be untrusted. To be concrete, we establish a trust system to evaluate the reliability of user vehicles by adapting the Dirichlet density function to deal with the uncertainties of user vehicles' feedbacks and then to estimate their future behaviors. Furthermore, the iterative filtering algorithm is incorporated to resist against badmouth and ballot-stuffing attacks, and the adaptive forgetting factor protects the system against on-off attacks. The main results of this paper demonstrated that the scheme is effective in distinguishing platoon head vehicles even when their performances have slight differences. Our simulations also suggeste that the proposed REPLACE scheme is robust against different types of attackers. In the future work, we will target on preserving the privacy of feedback data and trust data that are stored and computed in the server.

Acknowledgment

This research is supported by the research grant S15-1105-RF-LLF URBAN from the Economic Development Board, Singapore, for the project of Development Of NTU/NXP Smart Mobility Test-bed, and ZJNSF No.LR13F020003.

References

[1] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, "Overview of platooning systems," in *Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012)*, 2012.

[2] A. A. Alam, A. Gattami, and K. H. Johansson, "An experimental study on the fuel reduction potential of heavy duty vehicle platooning," in *13th International IEEE Conference on Intelligent Transportation Systems (ITSC), 2010*. IEEE, 2010, pp. 306–311.

[3] F. Browand, J. McArthur, and C. Radovich, "Fuel saving achieved in the field test of two tandem trucks," *California Partners for Advanced Transit and Highways (PATH)*, 2004.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2565001, IEEE Transactions on Vehicular Technology

[4] C. Bergenhem, Q. Huang, A. Benmimoun, and T. Robinson, "Challenges of platooning on public motorways," in *17th world congress on intelligent transport systems*, 2010, pp. 1–12.

[5] S. Tsugawa, S. Kato, and K. Aoki, "An automated truck platoon for energy saving," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2011*. IEEE, 2011, pp. 4109–4114.

[6] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016. [Online]. Available: http://dx.doi.org/10.1109/MNET.2016.7437026

[7] H. Hu, R. Lu, and Z. Zhang, "Tpsq: Trust-based platoon service query via vehicular communications," *Peer-to-Peer Networking and Applications*, pp. 1–16, 2015.

[8] R. Du, C. Chen, B. Yang, N. Lu, X. Guan, and X. Shen, "Effective urban traffic monitoring by vehicular sensor networks," *IEEE Trans. Vehicular Technology*, vol. 64, no. 1, pp. 273–286, 2015. [Online]. Available: http://dx.doi.org/10.1109/TVT.2014.2321010

[9] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Vehicular Technology*, to appear.

[10] H. Hu, R. Lu, and Z. Zhang, "Vtrust: A robust trust framework for relay selection in hybrid vehicular communications," in *2015 IEEE Global Communications Conference, GLOBECOM 2015, San Diego, CA, USA, December 6-10, 2015*, 2015, pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/GLOCOM.2014.7417027

[11] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Rubin, *Bayesian data analysis*. Taylor & Francis, 2014, vol. 2.

[12] A. Jøsang and J. Haller, "Dirichlet reputation systems," in *The Second International Conference on Availability, Reliability and Security, 2007. ARES 2007.* IEEE, 2007, pp. 112–119.

[13] D. Gambetta *et al.*, "Can we trust trust," *Trust: Making and breaking cooperative relations*, vol. 13, pp. 213–237, 2000.

[14] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Trans. Mob. Comput.*, vol. 11, no. 9, pp. 1514–1531, 2012. [Online]. Available: http://dx.doi.org/10.1109/TMC.2011.160

[15] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, 2002, pp. 2502–2511.

[16] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Network and Service Management*, vol. 8, no. 2, pp. 79–91, 2011. [Online]. Available: http://dx.doi.org/10.1109/TNSM.2011.050311.100028

[17] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 23-29 April 2006, Barcelona, Catalunya, Spain*, 2006.

[18] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[19] L. Xu, L. Y. Wang, G. G. Yin, and H. Zhang, "Communication information structures and contents for enhanced safety of highway vehicle platoons," *IEEE Trans. Vehicular Technology*, vol. 63, no. 9, pp. 4206–4220, 2014. [Online]. Available: http://dx.doi.org/10.1109/TVT.2014.2311384

[20] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 263–284, 2016. [Online]. Available: http://dx.doi.org/10.1109/COMST.2015.2410831

[21] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *3rd Annual International ICST Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MOBIQUITOUS 2006, San Jose, California, USA, July 17-21, 2006*, 2006, pp. 1–8. [Online]. Available: http://dx.doi.org/10.1109/MOBIQ.2006.340422

[22] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[23] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in vanets," in *2010 2nd International Conference on Information Technology Convergence and Services (ITCS)*. IEEE, 2010, pp. 1–8.

Hao Hu (S'15) received the B.Eng. degree in electronic engineering from University of Electronic Science and Technology of China, Chengdu, China, in 2012. He is currently pursuing Ph.D. degree in School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include trust and reputation, VANET.

Rongxing Lu (S'09-M'11-SM'15) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012. From May 2012 to April 2013, he was a Postdoctoral Fellow with the University of Waterloo. Since May 2013, he has been an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include computer network security, mobile and wireless communication security, and applied cryptography. Dr. Lu was the recipient of the Canada Governor General Gold Metal.

Zonghua Zhang is currently an associate professor of IMT/TELECOM Lille of France, he is also affiliated with CNRS SAMOVAR UMR 5157 as a research associate. Previously, he worked as an expert researcher at the Information Security Research Center of National Institute of Information and Communications Technology (NICT), Japan from April, 2008 to April, 2010. Even earlier, he spent two years for post-doc research at the University of Waterloo, Canada and INRIA, France after earning his Ph.D. degree in information science from Japan Advanced Institute of Science and Technology (JAIST) in 2006. His research interests cover anomaly detection, network forensics and attacks mitigation in different types of computer and communication networks and services, with current targeting scenarios SDN, NFV, ITS, and eHealth. Zonghua actively participates in organizing many international conferences, and he is on the editorial board of Computers & Security, IEEE Communications Magazine, Security and Communications Network, and International Journal of Network Security.

Jun Shao received the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, in 2008. He was a Postdoctoral Fellow with the School of Information Sciences and Technology, Pennsylvania State University, State College, PA, USA, from 2008 to 2010. He is currently an Associate Professor with the Department of Information Security, Zhejiang Gongshang University, Hangzhou, China. His research interests include network security and applied cryptography.