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 academica 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
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 platoon 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 system. In Section V, the performance evaluation is introduced. In Section VI, 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.

![System model under consideration](image)

**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 $\alpha$ and $\beta$. A random variable $X$ beta-distributed with parameters $\alpha$ and $\beta$ 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 $\Gamma$ 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 $\alpha$ and $\beta$.](image)
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 \( \alpha \). 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 de-
scribe the probability distribution over a \( k \)-component random
variable \( X = \{X_1, X_2, \cdots, X_k\} \). If \( \vec{p} = \{p_1, p_2, \cdots, p_k\} \) 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 pa-
rameter \( \vec{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_k) \), which denote the cumulative
observations and initial beliefs of \( X \). \( \vec{p} \) is a \( k \)-dimensional
random variable and \( \vec{\alpha} \) is a \( k \)-dimensional random observation
variable. The probability density function is given by:

\[
f(\vec{p}|\vec{\alpha}) = \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} p_i^{\alpha_i-1}
\]

where \( 0 < p_1, p_2, \cdots, p_k \leq 1; \sum_{i=1}^{k} p_i = 1; \alpha_1, \alpha_2, \cdots, \alpha_k > 0 \). The expected value of the probability
that \( X \) to be \( x_i \) given the observations vector \( \vec{\alpha} \) is given by:

\[
E(p_i|\vec{\alpha}) = \frac{\alpha_i}{\alpha_i + \sum_{j=1}^{k} \alpha_j}
\]

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:

\[
Var[X = x_i] = \frac{\alpha_i(\alpha_0-\alpha_i)}{(\alpha_i+\sum_{j=1}^{k} \alpha_j)(\alpha_0+1)}
\]

If \( i \neq j \), the covariance is:

\[
Cov[X = x_i, X = x_j] = \frac{\alpha_i \alpha_j}{(2\alpha_0+\sum_{j=1}^{k} \alpha_j)(\alpha_0+1)}.
\]

### 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.

#### A. System Initialization

![Fig. 3. Architecture of REPLACE Scheme](image)

- **Initialization**
  - Feedback data table
  - Trip information

- **Quality of Feedbacks**
  - Iterative Filtering
  - Quality Value Calculation

- **Trustworthiness of User Vehicles**
  - Dirichlet Model
  - Trust Score Calculation

- **Reputation of PH Vehicles**
  - PH Vehicle Data Table
  - Reputation

- **User Vehicle Trust table**

#### B. Quality of Feedbacks

In order to evaluate the quality of user vehicle \( v_j \)’s feedback in
trip \( T_{ri} \), we first calculate the integrated feedback of the
trip \( T_{ri} \), denoted by \( Tr_{i} \), which could be regarded as a
real performance of the PH vehicle in \( T_{ri} \) by combining all
feedbacks about \( T_{ri} \) together. Then \( Tr_{i} \) will be compared to
\( f_{j} \), a greater difference leads to a lower quality value of this
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.

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 $A_1, A_2, \cdots, A_{m_1}$ to represent the set of user vehicles of trip $TR_1, TR_2, \cdots, TR_{m_1}$ respectively. The sets will be updated after each iteration because some of the user vehicles will be in blacklist after iteration. We denote $\nu$ to be the round number of the iteration. $A_i^{(\nu)}$ denotes the set of user vehicles of trip $TR_i$ after the $\nu^{th}$ round. In the very beginning, we can easily get $A_i^{(0)}$, $i \in \{1,2, \cdots, m_1\}$ from the feedback data table. Similarly, for each user vehicle who takes part in different trips, we use $B_1, B_2, \cdots, B_{m_j}$ to represent the set of trips that the user vehicles $v_1, v_2, \cdots, v_{m_j}$ take part in. At the $\nu^{th}$ round, the iterative algorithm will be executed, we computed the integrated feedback of $TR_i$ as:

$$TR_i^{(\nu+1)} = \frac{\sum_{T_R \in A_i^{(\nu)}} T_R \cdot f_j^i}{\sum_{T_R \in A_i^{(\nu)}} T_R}$$

(2)

where $A_i^{(\nu)}$ is the set of all user vehicles in trip $TR_i$ at the $\nu^{th}$ round. $T_R$ represents the trust score of a user vehicle $v_j$.

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:

$$C_j^{(\nu+1)} = \frac{\sum_{T_R \in B_j^{(\nu)}} \lambda^{t_i} \cdot |f_j^i - TR_i^{(\nu+1)}|}{\sum_{T_R \in B_j^{(\nu)}} \lambda^{t_i}}$$

(3)

where $\lambda$ 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 $A_i$ 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 trip’s integrated feedback $TR_i$ converges at the $\nu^{th}$ round. The quality value of $v_j$’s feedback $f_j^i$ can be represented as:

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

(4)

Note that $\nu$ is the number of rounds to get a convergent integrated feedback, the larger is $\nu$, the more malicious user vehicles exist, the more difficult it is to give a feedback accurately. Hence $\nu$ 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.
Algorithm 1 Iterative filtering

Input: Records in the feedback data table
Output: Trip $TR_i$’s integrated feedback $TR_i^{(ν+1)}$
1: $ν \leftarrow 0$
2: difference $\leftarrow 100$
3: while difference $\geq TR_{threshold}$ do
4: for $TR_i \in T$ do
5: calculate $TR_i^{(ν+1)}$
6: end for
7: for $v_j \in A_i^{(ν)}$ do
8: calculate $C_j^{(ν+1)}$
9: end for
10: for $TR_i \in T$ do
11: for $v_j \in A_i^{(ν)}$ do
12: if $C_j^{(ν+1)} > C_{threshold}$ then
13: remove $v_j$ from $A_i^{(ν)}$ to form $A_i^{(ν+1)}$
14: end if
15: end for
16: end for
17: difference $= TR_i^{(ν+1)} - TR_i^{(ν)}$
18: $ν \leftarrow ν + 1$
19: end while
20: return $TR_i^{(ν+1)}$

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 $\{θ_1, θ_2, \cdots, θ_l\}$ ($θ_i \in (0, 1], i \in [1, l], θ_1 < θ_{i+1}$). Let $\vec{p} = \{p_1, p_2, \cdots, p_l\}$ ($\sum_{i=1}^l p_i = 1$) be the probability distribution vector of $X$ with respect to satisfaction levels, so that we have $P(θ_{i-1} < X_i \leq θ_i) = p_i (i = 1, 2, \cdots, l)$. Let $\vec{γ}$ be the vector of cumulative historical data and initial belief of $X$. With a posterior Dirichlet distribution, $\vec{p}$ can be modeled as:

$$f(\vec{p} | \vec{γ}) = Dir(\vec{p} | \vec{γ}) = \frac{\Gamma(\sum_{i=1}^l γ_i)}{\prod_{i=1}^l Γ(γ_i)} \prod_{i=1}^l p_i^{γ_i-1} \tag{5}$$

where $ξ$ denotes the background information represented by $\vec{γ}$. Let $γ_0 = \sum_{i=1}^l γ_i$. The expected value of the probability of $X_i \in (θ_{i-1}, θ_i)$ with the historical distribution of quality values is given by:

$$E(p_i | \vec{γ}) = \frac{γ_i}{γ_0} \tag{6}$$

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

$$\vec{γ}(n) = \begin{cases} \frac{S(0)}{n}, & (n = 0) \\ \sum_{i=1}^n β^{t-i} S(i) + c_0 S(0), & (n \geq 1) \end{cases} \tag{7}$$

where $n$ is the total number of historical quality values; $S(0)$ is the initial belief vector when $n = 0$. Since no prior information is available, all elements of $S(0)$ have equal probability which makes $S(0) = (1, 1, \cdots, 1)$. Parameter $c_0 > 0$ is a weight on the initial beliefs. In the $i^{th}$ trip of $v_j$ ($TR_i \in B_j, 1 \leq i \leq n$), $S(i)$ 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 $β \in [0, 1]$, 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 $β$:

$$β = c_3 \cdot (1 - T_j) \tag{8}$$

$c_3$ 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 $θ_i (i \in [1, k])$. Let $p_i$ denote the probability that the quality value of $v_j$’s feedback is categorized into the satisfaction level of $θ_i$. $\vec{p} = (p_1, p_2, \cdots, p_k)$) $∑_{i=1}^k p_i = 1$. We model $\vec{p}$ using equations in Section IV-C. Let $Y$ be the random variable denoting the weighted average of the probability of each satisfaction level in $\vec{p}$, the trust score $T_j$ of $v_j$ is represented as:

$$T_j = E[Y] = \sum_{i=1}^k ω_i E[p_i] = \frac{1}{γ_0} \sum_{i=1}^k ω_i γ_i \tag{9}$$

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.
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 \( p_{hk} \) in the system, it records all trips of \( p_{hk} \) and the feedbacks from each user vehicle in the corresponding trip. Let \( C_k \) be the set of all trip IDs for \( p_{hk} \). For a specific trip \( T_{ri} \in C_k \), as defined before, \( A_i \) is the set of all user vehicle IDs in that trip.

The reputation of \( p_{hk} \) can be calculated by aggregating all the feedbacks of \( p_{hk} \)’s user vehicles based on the trustworthiness of those user vehicles. Using the weight majority method, \( p_{hk} \)’s reputation score is given by:

\[
\text{Rep}_{hk} = \frac{\sum_{T_{ri} \in C_k} \sum_{v_i \in A_i, T_j \geq T_{ri}} \eta^{t_f - t_i} \cdot f_j}{\sum_{T_{ri} \in C_k} \sum_{v_i \in A_i, T_j \geq T_{ri}} \eta^{t_f - t_i} \cdot T_j}
\]

where \( \eta \) 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 \( p_{hk} \).

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 performing 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 exclude the feedbacks from 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 then 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 for 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)
TABLE I
SIMULATION PARAMETER SETTINGS

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m_j )</td>
<td>user vehicle number</td>
<td>100</td>
</tr>
<tr>
<td>( m_p )</td>
<td>PH vehicle number</td>
<td>20</td>
</tr>
<tr>
<td>( n )</td>
<td>service times per vehicle per round</td>
<td>4</td>
</tr>
<tr>
<td>( N )</td>
<td>number of rounds</td>
<td>50, 100</td>
</tr>
<tr>
<td>( c_0 )</td>
<td>initial belief weight</td>
<td>1</td>
</tr>
<tr>
<td>( c_1 )</td>
<td>award sensitivity</td>
<td>0.5</td>
</tr>
<tr>
<td>( c_2 )</td>
<td>variance sensitivity</td>
<td>0.3</td>
</tr>
<tr>
<td>( C_{\text{threshold}} )</td>
<td>inconsistency threshold</td>
<td>0.3</td>
</tr>
<tr>
<td>( T_{\text{threshold}} )</td>
<td>stability threshold</td>
<td>0.1</td>
</tr>
<tr>
<td>( T_{\text{threshold}} )</td>
<td>trust threshold</td>
<td>0.3</td>
</tr>
<tr>
<td>( T_0 )</td>
<td>initial trust score</td>
<td>0.5</td>
</tr>
<tr>
<td>( \text{Rep}_0 )</td>
<td>initial reputation score</td>
<td>0.5</td>
</tr>
<tr>
<td>( q_{\text{bs}} )</td>
<td>percentage of ballot-stuffing attackers</td>
<td>10%</td>
</tr>
<tr>
<td>( q_{\text{bs}} )</td>
<td>percentage of badmouth attackers</td>
<td>40%</td>
</tr>
<tr>
<td>( l_{ph} )</td>
<td>performance quality level</td>
<td>0.8, 0.98</td>
</tr>
<tr>
<td>( l_v )</td>
<td>feedback accuracy level</td>
<td>0.92, 1</td>
</tr>
</tbody>
</table>

\( l_{ph} \in [0, 1] \) 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:

\[
f(x|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}
\]

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 \( \alpha \) and \( \beta \) as follows:

\[
\alpha = c_2 \cdot l_{ph} \\
\beta = c_2 \cdot (1 - l_{ph})
\]

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:

\[
eva = x \pm 10\% \cdot x \cdot (1 - l_v)
\]

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 \( q_{\text{bs}} \) and \( q_{\text{bs}} \) 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.

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.
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.

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 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...
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 suggest 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**


[23] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, “A trust modeling frame-


[29] C. Bergenhem, Q. Huang, A. Bennimoun, and T. Robinson, “Chal-


[34] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Reputation


[43] Jun Shao received the Ph.D. degree from Shanghai

[46] Zonghua Zhang is currently an associate profes-

[48] Rongxing Lu (S’09-M’11-SM’15) received the

[51] 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 Engineer-
ing, Nanyang Technological University, Singapore.
His research interests include trust and reputation,
VANET.

[54] Zonghua Zhang

[57] Jun Shao

[59] Rongxing Lu