Noname manuscript No.
(will be inserted by the editor)

PTRS: A Privacy-Preserving Trust-based Relay Selection Scheme in VANETs

Hao Hu · Rongxing Lu · Cheng Huang · Zonghua Zhang

Received: date / Accepted: date

Abstract As one of the essential components of Intelligent Transport Systems (ITS), Vehicular Ad Hoc Network (VANET) plays a significant role in enabling various on-road applications, most of which primarily rely on two-hop Vehicle-to-Infrastructure communications. To make such communications reliable and secure, it is significant to ensure that only the trustworthy vehicles are selected as relays. To tackle this challenge, this paper proposes a robust trust-based relay selection scheme, called PTRS, which, based on Dirichlet distribution, systematically integrates a set of unique features of VANET, e.g., hybrid architecture, high dynamics, into the traditional reputation system, with an objective to effectively differentiate the trust levels of the vehicles, meanwhile, preserving robustness. Besides, the location privacy of vehicles are preserved in our proposed scheme by using the technique of pseudonyms and trust levels instead of explicit reputation scores. Detailed security analysis is conducted, which shows that the proposed PTRS scheme is secure and robust against several sophisticated attacks in VANETs. In addition, a set of extensive simulations are carried out, demonstrating its effectiveness and accuracy.

H. Hu
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 50 Nanyang Avenue, Singapore 639798
E-mail: hhu002@e.ntu.edu.sg

R. Lu
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 50 Nanyang Avenue, Singapore 639798
E-mail: rxlu@ntu.edu.sg

C. Huang
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 50 Nanyang Avenue, Singapore 639798
E-mail: huangcheng@ntu.edu.sg

Z. Zhang
Institut Mines-Telecom/TELECOM Lille, CNRS UMR 5157 SAMOVAR Lab
E-mail: zonghua.zhang@telecom-lille.fr

Keywords Location Privacy · Vehicular Ad Hoc Networks · Robust · Trust

1 Introduction

Significant efforts were made recently for enabling safety, traffic management, and commercial applications in VANET [1]. Envisioned as one of the most promising approaches to implement intelligent transportation systems (ITS), VANET has the potential to enhance road safety and reduce traffic congestion due to its hybrid infrastructures [2–4]. This hybrid infrastructure includes road side units (RSUs) deployed along the roads and on board units (OBUs) equipped in mobile vehicles, which enables not only vehicle-to-vehicle (V-2-V) but also vehicle-to-infrastructure (V-2-I) communications.

Due to the high cost of RSUs, they can only be deployed in some of the downtown areas where many vehicles pass by. We consider a scenario when a vehicle is traveling in a rural area and no RSUs are deployed nearby, and this vehicle would like to send an urgent message to RSU by asking other vehicles nearby to relay the message. However, vehicles are not always reliable when relaying messages. For example, they may relay the messages after a long delay or even drop the messages, leading to low relay ratio. The problem can be settled by incorporating trust which allows each vehicle to detect malicious relay vehicles who drop messages deliberately, and to give incentives to encourage reliable vehicles [5].

Meanwhile, location privacy has always been a concern in VANET since the locations of the vehicles are closely related to the drivers of those vehicles [6]. To achieve location privacy, a very popular approach in VANET is that vehicles periodically change their pseudonyms when broadcasting messages [1, 7, 8], since the pseudonyms make the location information in a period unlinkable to a specific vehicle. However, pseudonyms do not always ensure privacy, as an example shown in Fig. 2, a requesting vehicle (the red vehicle) is asking another vehicle for relaying its message among a few candidate vehicles nearby. At time t, two candidate vehicles V_i and V_j respond to the requesting vehicle by sending their own pseudonyms together with their reputation scores, then after a short while at time $t + \Delta t$, their pseudonyms are changed from PID_A and PID_C to PID_B and PID_D respectively, the requesting vehicle can still link V_i and V_j by associating their reputation scores even though their pseudonyms have been changed. Because the reputation update interval is long enough so that in the period before update, the reputation score of a vehicle can be regarded as unchanged. Hence, candidate vehicles' location privacy are exposed. Therefore, it is compelling for us to build a trust system through which vehicles take its advantages without sacrificing their privacies.

In this paper, to facilitate vehicles to improve relay ratio while achieving location privacy, we propose a privacy-preserving trust-based relay selection scheme, called PTRS. This scheme can help a vehicle to efficiently detect the malicious or selfish vehicles who drop packets deliberately by establishing a trust model to measure the reliability of a vehicle when relaying a message.

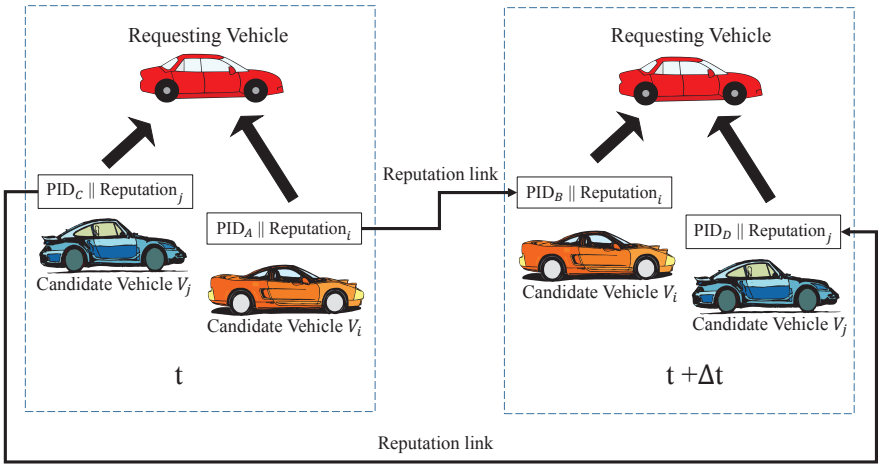


Fig. 1 Reputation score are associated despite the change of pseudonyms

Meanwhile, the proposed scheme is characterized by its ability to preserve the location privacy of vehicles. Specifically, our work features the follows:

- First, our designed scheme takes advantages of the already-existing centralized infrastructure in VANET by considering its unique characteristics: high dynamic, hybrid infrastructure and ephemeral link. It allows us to design a secure and efficient relay selection scheme.
- Second, we build a trust-based relay selection scheme through which a requesting vehicle is able to quickly decide whether a candidate vehicle is reliable to relay a message by verifying whether its trust level meets a threshold which is set by this requesting vehicle. This trust level reflects the extent to which a candidate vehicle has been a successful relay in the past. It also reflects the likelihood that it will relay a message successfully in the future.
- Finally, we design a request-response scheme using pseudonyms combined with trust-based system that allows a requesting vehicle to authenticate the candidate vehicle anonymously, and then judge whether this candidate vehicle's reputation score satisfies its requirement without knowing the exact reputation score. In this way, the candidate vehicle's reputation score is concealed and its location privacy is preserved in the process of reputation score sharing. Besides, to deal with the cheating behavior of candidate vehicles in sharing their reputation scores, the TA is able to check whether a candidate vehicle cheats the requesting vehicle by submitting an exaggerated reputation score afterwards. The candidate vehicle will be punished once their cheating behavior is detected. .

The remainder of this paper is organized as follows. In Section **??**, we formalize the system model, trust model and threat model considered in our work, and identify our design goals. In Section 3, we briefly recall the bilinear pairing and the Dirichlet distribution which have been applied in the trust and repu-

tation system. In Section 4, the PTRS scheme is presented in details, together with the rationale how it can help the requesting vehicles to choose a highly reliable relay vehicle without knowing its reputation score. Security analysis is then presented in Section 5, and the performance analysis is given in Section 6. Finally, we present the related work in Section 7 and draw conclusions in Section 8.

2 Problem Statement

In this section, we define the problem by formalizing the system model, threat model and design goal.

2.1 System Model

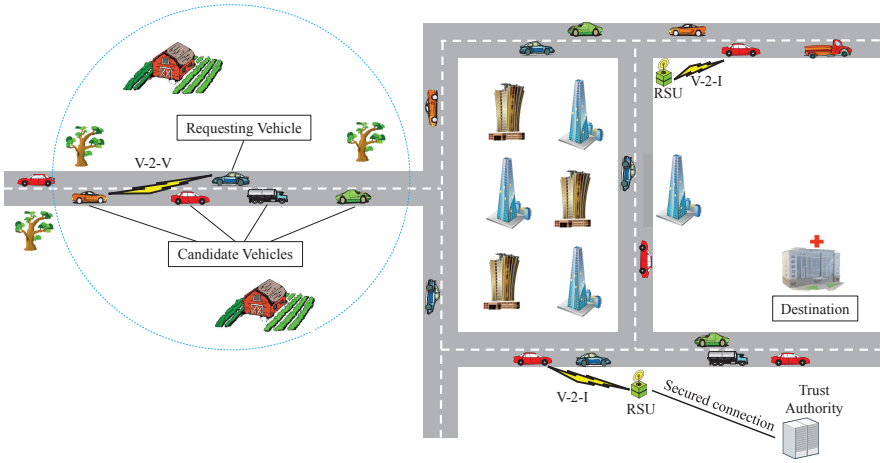


Fig. 2 System model under consideration

The system model is illustrated in Fig.2, which consists of three roles: the top TA (trust authority), the immobile RSUs (road side units) at the road side and the mobile vehicles equipped with OBUs (on board units). Specifically, we consider a scenario when a vehicle wants to transmit a packet to the destination in VANET without the existence of RSUs, which is common in rural areas or highways.

TA: TA takes charge of the registration of all RSUs and the vehicles, which also maintains the evaluation records and trust values of all vehicles in the system model. TA is assumed to have sufficient computation and storage capability.

RSUs: The RSUs are subordinated by the TA, which are connected to the TA through wired lines and secureed channels. Equipped with wireless devices,

RSUs are able to exchange data with the passing-by vehicles. However, due to the high cost of RSU installment and maintenance, especially in the early stage of VANET, no RSUs are deployed at the crossroads where traffic flow is small.

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 with RSUs. Through V-2-I communication, a vehicle retrieves the updates of its own trust levels or uploads feedbacks to the server when passing by RSUs. Through V-2-V communication, a vehicle broadcasts the relay requirement to nearby vehicles and transmits the messages to a chosen relay vehicle. In this case, the vehicles can be further divided into two categories:

- *Requesting Vehicle:* After authentication in the system through TA, any authorized vehicle can be a requesting vehicle whenever it wants to relay a message through the nearby vehicles to a specific destination.
- *Candidate Vehicle:* A candidate vehicle is the vehicle within the transmission range of the requesting vehicle, whenever a requesting vehicle broadcasts its relaying request, the candidate vehicle will firstly respond if it is interested to relay the message. This response message includes the candidate vehicle's pseudo identity and reputation score. Later, the requesting vehicle will decide which candidate vehicle to chose as a relay vehicle according to its reputation score.

2.2 Trust Model

In our trust model, we make some assumptions and define the trust levels of different roles in the system model, besides, we also define the attack models

- *TA:* Trust authority maintains the public keys, private keys and trust records of the network, we assume that it is fully trusted by all roles in the system since it is under strong physical protection.
- *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.
- *Requesting Vehicles:* We assume that the requesting vehicles are honest but curious about the privacy of the candidate vehicles. Besides, they are also honest when evaluate the relay vehicles who have accomplished their tasks.
- *Candidate Vehicles:* The candidate vehicles are driven by human, which means that the behaviors of vehicles are actually the behaviors of human beings. As a result, some of the vehicles will be selfish when asked to relay a message due to their limited storage space and energy. To make

things worse, a small fraction of vehicles may even be compromised by the adversaries who drop the packets deliberately when they promise to relay the message. Because of those selfish or malicious behaviors, the relay ratio of the system will decrease greatly.

2.3 Threat Model

Specifically, we consider the adversary can launch the following types of attacks to either invade the privacy of vehicles or degrade the message relay efficiency of the whole VANET.

- *Impersonation attack:* The adversary impersonates a candidate vehicle to ask for relaying the message. However, this candidate vehicle may not be qualified in the system. Once chosen as relays, these unqualified vehicles may drop the messages intentionally.
- *Packets dropping attack:* The adversary is able to control a small fraction of the vehicles in the system who ask for taking the responsibility to relay the messages and then drop the packets deliberately.
- *Packets analysis attack:* The adversary eavesdrops the transmission of a message and tries to analyze the message.
- *Reputation link attack:* We assume that the requesting vehicles are honest but curious. If the reputation score of a candidate vehicle is directly given to the requesting vehicle, the location privacy and traveling path and of this candidate vehicle will be exposed since the requesting vehicle can still derive that it belongs to the same vehicle from the same reputation score collected in different locations even though the pseudo-id has changed.

2.4 Design Goal

Based on the given models, our goal is to design a trust-based relay selection scheme in VANET which is effective in distinguishing the malicious or selfish vehicles who drop relay messages deliberately, and finally improve the relay ratio. At the same time, the proposed scheme preserves the location privacy of the vehicles. Specifically, the following objectives need to be achieved:

- *The relay ratio improvement:* In the VANET, vehicles are selfish, they could firstly promise to relay a message but then drop it in order to save energy and communication cost. Besides, another possible case is that when a vehicle requests to relay a message, no vehicle responds even they are able to relay the message. In addition, packets dropping attacks exist due to malicious vehicles controlled by adversary. With the existence of those vehicles, if a requesting vehicle chooses a relay vehicle randomly from candidate vehicles, the relay ratio will be low, finally leading to the failure of the system. Therefore, the proposed scheme should be able to improve the message relay ratio of the system by helping the requesting vehicle choose

a more reliable candidate vehicle as a relay as well as defending against the aforementioned attacks.
- *Achieving the location privacy preservation:* The location privacy of a vehicle is very sensitive since it is closely related to the location its driver. For example, if the adversary is able to track the location of a vehicle, it may probably infer that the driver is not at home. More serious results will be caused when the adversary studies the path of a vehicle and learns the living pattern of that driver. Our proposed scheme should be able to resist against privacy-related attack and preserve the location privacy of vehicles.
- *Anonymous authentication to participant vehicles:* As introduced before, the impersonation attack decreases the relay ratio in the system. To tackle this problem without disclosing the privacy of vehicles, our proposed scheme employs an anonymous authentication mechanism to resist against impersonation attack and ensure that the participant vehicles are all qualified.

3 Preliminaries

3.1 Bilinear Pairing

Let $(\mathbb{G}, \times)$ and $(\mathbb{G}_T, \times)$ be two multiplicative cyclic groups of the same prime order q. Then, a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ will satisfy the following properties: i) Bilinear: Let $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$, then $e(g^a, h^b) = e(g, h)^{ab}$, ii) Non-degenerated: Let $g \in \mathbb{G}$ be a generator in $\mathbb{G}$, then $e(g, g) \neq 1_{\mathbb{G}_T}$, and iii) Computable: Let $g, h \in \mathbb{G}$, then $e(g, h)$ can be efficiently computed.

Definition 1 (Bilinear Parameter Generator) A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as its input, and outputs a 5-tuple $(q, g, \mathbb{G}, \mathbb{G}_T, e)$, where q is a κ-bit prime number, $(\mathbb{G}, \mathbb{G}_T)$ are two multiplicative groups of the same order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map.

3.2 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 [9]. 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: $Cov[X = x_i, X = x_j] = \frac{-\alpha_i\alpha_j}{\alpha_0^2(\alpha_0+1)}$.

4 Proposed PTRS Scheme

In this section, we propose PTRS scheme, a privacy-preserving trust-based relay selection scheme in VANET, which is mainly comprised of four phases: system initialization, privacy-preserving relay selection protocol, performance report and trust management.

4.1 Initialization

The trust authority (TA) takes charge of bootstrapping the whole system and generating the public and private keys for vehicles and road side units (RSUs). Specifically, the bootstrapping steps are executed as follows:

- Given a security parameter κ, the TA firstly generates the bilinear parameters $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{G}en(\kappa)$. Then TA chooses a random number $p \in \mathbb{Z}_q^*$ as its master key. In addition, TA chooses a secure symmetric encryption algorithm $E(\cdot)$, such as AES encryption and a secure asymmetric encryption algorithm $Enc(\cdot)$, such as ElGamal encryption. After that, the system parameters will be published, including $(q, g, \mathbb{G}, \mathbb{G}_T, e)$.
- Afterwards, when a vehicle $v_i \in \mathcal{V} = \{v_1, v_2, \cdots, v_n\}$ with real identity ID_i wants to register itself in the system, TA generates a set of m pseudonyms and their corresponding public and secret key pairs in this way:
  1. TA randomly chooses a set of m numbers $\{x_{i1}, x_{i2}, \cdots, x_{im} \in \mathbb{Z}_q^*\}$ as the secret keys of m pseudonyms. To compute their corresponding public keys, TA chooses a set of random values $\{s_{i1}, s_{i2}, \cdots, s_{im} \in \mathbb{Z}_q^*\}$, and computes certificates $\theta_{i1} = e(g,g)^{p^2 \cdot s_{i1}^2}, \theta_{i2} = e(g,g)^{p^2 \cdot s_{i2}^2}, \cdots, \theta_{im} = e(g,g)^{p^2 \cdot s_{im}^2}$, then computes $y_{i1} = \theta_{i1}^{x_{i1}}, y_{i2} = \theta_{i2}^{x_{i2}}, \cdots, y_{im} = \theta_{im}^{x_{im}}$. For any pseudo-id PID_{i1} with a secret key x_{i1}, its public key comprises two parts: $\theta_{i1} = e(g,g)^{p^2 \cdot s_{i1}^2}$ and $y_{i1} = \theta_{i1}^{x_{i1}}$.

2. TA chooses a symmetric key k_0 and the secure symmetric encryption algorithm $E_{k_0}()$ with secret key k_0 to compute the set of m pseudo-id for v_i: $\{PID_{i1} = E_{k_0}(ID_i||x_{i1}), PID_{i2} = E_{k_0}(ID_i||x_{i2}), \cdots, PID_{im} = E_{k_0}(ID_i||x_{im})\}$. Then TA assigns the whole set of pseudo-ids and their corresponding public and secret key pairs to v_i. Besides, TA also passes a set of specific certificates $\{g^{p \cdot s_{i1}}, g^{p \cdot s_{i2}}, \cdots, g^{p \cdot s_{im}}\}$ corresponding to the set of pseudo-ids to v_i.

– In addition, for each vehicle $v_i \in \mathcal{V}$, TA assigns an initial reputation score $R_i = R_0$ and an initial trust level $T_i = T_0$ to it.

4.2 Privacy-preserving Relay Selection Protocol

In order to achieve the relay selection without revealing the vehicles' privacy, our proposed scheme uses pseudo-ids and trust level instead of real IDs and accurate reputation scores. To be specific, a requesting vehicle v_B would like to choose a relay vehicle from the nearby candidate vehicles. If there is a candidate vehicle v_A with pseudo-id PID_A, trust level T_A and private-public key pair $(x_A; \theta_A = e(g,g)^{p^2 \cdot s_A^2}, y_A = \theta_A^{x_A})$ who wants to relay the message, it follows the request-response protocol shown in Fig. 3.

Participant vehicle v_A (ID_A, PID_A, T_A)		Requesting vehicle v_B (m, y_r)
1) $x_A \in \mathbb{Z}_q^*, \theta_A = e(g,g)^{p^2 \cdot x_A^2}$ $y_A = \theta_A^{x_A}$ $C_1 = g^{p \cdot r \cdot (H(t) + x_A) \cdot x_A}$ $C_2 = g^{p \cdot r^{-1} \cdot x_A}$	$\xrightarrow{\textbf{req1}:=\{C_1;C_2\}}$	
2)		checks $e(C_1, C_2) \stackrel{?}{=} \theta_A^{H(t)} \cdot y_A$
3)		If it holds, computes $(a_1, a_2, \cdots, a_n)$, chooses threshold T_1
	$\xleftarrow{\textbf{res1}:=\{(g^{a_0}, g^{a_1}, g^{a_2}, \cdots, g^{a_n}); T_1\}}$	
4) If $T_A \geq T_1$, computes $C = \prod_{i=0}^{n} (g^{a_i})^{T_A^i}$	$\xrightarrow{\textbf{req2}:=C}$	
5)		checks $C \stackrel{?}{=} g^{r_0}$
6)		$\sigma_B = Enc_{x_B}(m)$ $M = (E_{k_r}(m)\|\|Enc_{y_r}(k_r)\|\|\sigma_B\|\|t_0\|\|L)$
	$\xleftarrow{\textbf{res2}:=M}$	

Fig. 3 Privacy-preserving relay selection protocol

Step 1: Before relaying a message, the candidate vehicle v_A firstly needs to verify itself for v_B to show that it is an authorized vehicle by TA. Therefore, v_A chooses a random number $r \in \mathbb{Z}_q^*$ and uses current time stamp t and the certificate $g^{p \cdot s_A}$, which is awarded by TA, to compute $C_1 = g^{p \cdot r \cdot (H(t)+x_A) \cdot s_A} \in \mathbb{G}$ and $C_2 = g^{p \cdot r^{-1} \cdot s_A} \in \mathbb{G}$ and sends **req1**:= $\{C_1; C_2\}$.

Step 2: After receiving **req1**:= $\{C_1; C_2\}$, v_B verifies the eligibility of v_A by checking the equation $e(C_1, C_2) \stackrel{?}{=} \theta_A^{H(t)} \cdot y_A$, where t is the current time and y_A is public key of vehicle v_A. If it holds, v_B responds to v_A in the next step. Otherwise, v_B neglects v_A's request.

Step 3: Once v_B verifies that v_A is authorized, it responds to v_A by checking whether v_A's trust level matches v_B's requirement. Specifically, v_B chooses a threshold T_1 as its requirement. Since the trust level is a set of discrete values, any trust level which is no smaller than T_1 could be included in the vector: $(T_1, T_2, \cdots, T_n)$. By checking whether v_A's trust level is in this vector, v_B is able to see whether v_A meets its requirement even without knowing v_A's trust level. To achieve this, v_B chooses a random value $r_0 \in \mathbb{Z}_q^*$, a random variable $y \in \mathbb{Z}_q^*$ and conducts the computation:

$$\begin{aligned} & f(y) \\ & = \prod_{i=1}^{n} (y - T_i) + r_0 \\ & = y^n + \sum_{i=1}^{n} (-T_i) y^{n-1} + \cdots + (-1)^n \prod_{i=1}^{n} T_i + r_0 \\ & = a_n \cdot y^n + a_{n-1} \cdot y^{n-1} + \cdots + a_1 \cdot y + a_0 \end{aligned} \tag{2}$$

Then v_B sends **res1**:= $\{(g^{a_0}, g^{a_1}, g^{a_2}, \cdots, g^{a_n}); T_1\}$ back to v_A.

Step 4: v_A checks whether its own trust level T_A satisfies the threshold T_1 provided by v_B, if $T_A \geq T_1$, v_A computes $C = \prod_{i=0}^{n} (g^{a_i})^{T_A^i}$ and sends **req2**:=C to v_B to ask for relaying the message.

Step 5: When receiving **req2**:=C, v_B checks the relation $C \stackrel{?}{=} g^{r_0}$. If it holds, v_B accepts the request from v_A and responds to v_A in the next step.

Step 6: To ensure the confidentiality and integrity of the relayed message m, v_B encrypts it using the symmetric encryption algorithm $E()$ and a randomly chosen symmetric key k_r to form $E_{k_r}(m)$, and attaches its signature $\sigma_B = Enc_{x_B}(m)$. The symmetric key k_r is encrypted with the receiver's public key y_r to form $Enc_{y_r}(k_r)$ and combined in the message. Besides, the destination location L and a deadline t_0 are also attached, if v_B relayed the message to the receiver in destination location within t_0, the relay is successful, otherwise it fails. Hence v_B responds **res2**:=M where $M = (E_{k_r}(m)||Enc_{y_r}(k_r)||\sigma_B||t_0||L)$.

Correctness Analysis: Due to the bilinear paring property, the equation will hold on the following relations:

$$
\begin{aligned}
& e(C_1, C_2) \\
&= e(g^{p \cdot r \cdot (H(t)+x_A) \cdot s_A}, g^{p \cdot r^{-1} \cdot s_A}) \\
&= e(g,g)^{p^2 \cdot s_A^2 \cdot (H(t)+x_A)} \\
&= [e(g,g)^{p^2 \cdot s_A^2}]^{H(t)} \cdot [e(g,g)^{p^2 \cdot s_A^2}]^{x_A} \\
&= \theta_A^{H(t)} \cdot y_A
\end{aligned} \tag{3}
$$

$$
\begin{aligned}
C &= \prod_{i=0}^{n} (g^{a_i})^{T_A^i} \\
&= g^{a_n \cdot y^n + a_{n-1} \cdot y^{n-1} + \cdots + a_1 \cdot y + a_0} \\
&= g^{(T_A)^n + \sum_{i=1}^{n} (-1) \cdot T_i \cdot (T_A)^{n-1} \cdots + (-1)^n \prod_{i=1}^{n} T_i} \\
&= g^{\prod_{i=1}^{n} (T_A - T_i) + r_0}
\end{aligned} \tag{4}
$$

For any T_i, if $T_A = T_i (i = 1, 2, \cdots, n)$, then $C = g^{r_0}$.

4.3 Performance Report

When v_A is selected as a relay vehicle, it manages to relay the message as fast as possible. Once the message is successfully relayed to the destination, the requesting vehicle v_B will be notified immediately. Then v_B gives a report regarding the performance of v_A at this time. Once v_B passes by an RSU, it uploads this report about this task by submitting $(PID_A||T_1||f)$ to TA, where $f \in [0, 1]$ is the feedback score to evaluate how successful the relay is by considering factors like the delay and distance. If the relay fails, $f = 0$.

4.4 Trust Management

In this section, we will first introduce how the feedbacks of vehicles are verified and then how the reputation scores are computed based on those feedbacks, later we describe how to convert reputation scores to trust levels and how to update trust levels.

4.4.1 Feedback Verification

Upon receiving a performance report $(PID_A||T_1||f)$ in 4.3, TA will perform the following procedure to verify the feedback score f:

(a) TA searches for the real ID of v_A from PID_A and finds its corresponding trust level T_A.
(b) TA compares T_A with the submitted threshold T_1, if $T_A \geq T_1$, the submitted feedback score f is accepted, otherwise $f = 0$.

4.4.2 Feedback Aggregation

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 [10], Dirichlet distribution is more appropriate for multi-valued satisfaction levels [11]. In our case, the evaluation trustworthiness of user vehicles are described by continuous trust values. Therefore, we use Dirichlet distribution to estimate the performance of candidate vehicles in the future and then build our trust model accordingly.

For a specific candidate vehicle v_A, let X $(0 \leq X \leq 1)$ be the continuous random variable denoting the feedback score of v_A's performance. In order to classify the historical and future feedback scores, 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.

As described in Section 4.3, once v_A finishes many tasks, the TA is able to collect v_A's historical feedback scores from its performance reports, then we let $\overrightarrow{\gamma} = \{\gamma_1, \gamma_2, \cdots, \gamma_l\}$ denote the vector of cumulative feedback score and initial belief of X. With a posterior Dirichlet distribution, $\overrightarrow{p}$ can be modeled as:

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

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 feedback scores is given by:

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

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

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

where n is the total number of historical feedback scores, $\overrightarrow{S^{(0)}}$ 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} task of $v_A (i \in [1,n])$, $\overrightarrow{S^{(i)}}$ denotes the satisfaction level of its feedback score, which contains only one

element set to 1 corresponding to the selected satisfaction level and all the other $l-1$ elements set to 0. t_i stands for the time when the i^{th} task 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 [12], we choose an adaptive value as β:

$$\beta = c_0 \cdot (1 - R_A) \tag{8}$$

c_0 is a parameter to control the forgetting factor, the larger value of c_0 makes the system more forgettable about the historical behaviors and vice versa. From the equation we can see that when v_A has a high reputation score, its forgetting factor is small, which means that those good performances will be easily forgotten. On the contrary, once v_A provides a low quality relay or drops the packet, its reputation score gets lower and forgetting factor becomes larger. This means that all of those poor performances will be memorized and it takes even longer time for v_A to build up a high reputation score again.

4.4.3 Reputation Score of a Candidate Vehicle

For an arbitrary candidate vehicle v_A, to evaluate its trustworthiness when serving as relay vehicle, we assign the weight ω_i to each satisfaction level $\theta_i (i \in [1,l])$. Let p_i denote the probability that v_A's feedback score is categorized into the satisfaction level of θ_i. $\overrightarrow{p} = (p_1, p_2, \cdots, p_l) | \sum_{i=1}^{l} p_i = 1$. We model $\overrightarrow{p}$ using equations in Section 4.4.2. Let Y be the random variable denoting the weighted average of the probability of each feedback score in $\overrightarrow{p}$, the reputation score R_A of v_A is represented as:

$$R_A = E[Y] = \sum_{i=1}^{l} \omega_i E[p_i] = \frac{1}{\gamma_0} \sum_{i=1}^{l} \omega_i \gamma_i \tag{9}$$

where γ_i is the cumulated evidence that v_A's feedback score is with satisfaction level of θ_i.

4.4.4 Trust Level of a Candidate Vehicle

As explained in Section 1, the system will suffer from reputation link attack if vehicles use the reputation scores directly in the vehicular communications. In our proposed PTRS scheme, a discrete trust level is used instead of accurate reputation score, in this section, we describe how to convert reputation score to trust level: first, TA chooses the total number of trust levels, m. Then, for a candidate vehicle v_A with reputation score of R_A, its trust level T_A can be easily calculated as: $T_A = i$, for $(i-1)/m < R_A \leq i/m$, where integer $i \in [1,m]$.

4.4.5 Trust Update

The trust update frequency is decided by TA, when there are more tasks in the system, TA will ask the vehicles to update their trust levels more frequently, and vice versa. When vehicle v_A drives into the wireless range of an RSU, it retrieves its own updated trust level T_A from TA via RSU. v_A uses it in task request, as shown in Section 4.2, before the next update.

5 Security Analysis

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

5.1 Resilience to Reputation Link Attack

We consider the honest but curious requesting vehicles who know the reputation score of a candidate vehicle. Although pseudo-id makes the candidate vehicle anonymous, and the different locations of a candidate vehicle are unlinkable once it changes its pseudo-id. There still exists a risk that a candidate vehicle can be linked by a requesting vehicle according to its reputation score given that the reputation score remains unchanged in a long period. Clearly, in this case, the location information is disclosed and the candidate vehicle could be tracked. In our proposed PTRS scheme, when requesting vehicle v_B wants to know whether a candidate vehicle v_A's reputation score satisfies its requirement, it does not ask for reputation score directly. Instead, it provides the reputation score requirement to v_B and let v_B compute $C = \prod_{i=0}^{n} (g^{a_i})^{T_A^i}$. Then, by checking $C \stackrel{?}{=} g^{r_0}$, v_B is able to know whether v_A meets its reputation requirement even without knowing the exact reputation score of v_A. In addition, r is randomly chosen from $\mathbb{Z}_q^*$, $C_1 = g^{p \cdot r \cdot (H(t)+x_A) \cdot s_A}$ and $C_2 = g^{p \cdot r^{-1} \cdot s_A}$ are unlinkable.

5.2 Resilience to Packets Dropping Attack

Due to the existence of feedback scheme, the selfish or malicious vehicles who drop packets when relaying messages will get negative feedbacks, if they keep behaving in that way, those negative feedbacks will accumulate and finally lead to a low trust score and trust level. Thus, it will be less likely for them to be chosen to relay messages in the future since they will hardly meet the trust level requirement by a requesting vehicle. In this way, those reliable vehicles who seldom drop packets will be chosen to relay the messages, thus the scheme is resistable against packet dropping attack.

5.3 Resilience to Packets Analysis Attack

In our proposed PTRS scheme, the requesting vehicle v_B has encrypted the message m into $M = (E_{k_r}(m)||Enc_{y_r}(k_r)||\sigma_B||t_0||L)$. Without knowing the receiver's secret key x_r, the adversary is unable to recover m from the packet analysis. In addition, because the pseudo-id is used in the scheme, no identity information will be disclosed. Therefore, our proposed PTRS scheme is resistable against packet analysis attack.

5.4 Resilience to Fake Reputation Attack

In Section 4.2 *step 4*, v_A integrates its own trust level T_A into C. However, a small fraction of vehicles controlled by the adversary may cheat by using $T_A\prime$. In this case, our proposed scheme is still efficient in tracking those dishonest vehicles and punish them. The inspection is executed by TA, as shown in Section 4.4.1 when a performance report is submitted, TA firstly finds the real ID of the relay vehicle v_A from its pseudo-id PID_A, then retrieves the trust level T_A and compares it with the threshold T_1. If $T_A < T_1$, which means that v_A launches a fake reputation attack by using an untruthful trust level in task request, TA will punish v_A by recording this task as an unsuccessful relay no matter how successful this relay is.

6 Performance Evaluation

In this section, we study the performance of PTRS scheme using a custom simulator built in Java. The performance metrics used in our proposed scheme are: *message delivery ratio* defined as the ratio of messages successfully relayed to the destination with respect to total number of messages generated by vehicles in a period, and *detection ratio* defined as the ratio of the number of detected malicious vehicles with respect to the total number of malicious vehicles in a specific time period.

6.1 Simulation Setup

To simulate the vehicular network, an area of $10km \times 10km$ is created with roads that are equally laid with distance of $2km$ in between. Later, one RSU with transmission radius of $1000m$ is deployed at an intersection of the map denoting the urban area. Finally, a total number of N vehicles with transmission radius of 300 meters are deployed, as shown in Fig. 4. We also choose $m = 10$ as the total number of trust levels, and let all vehicles choose relay vehicles using the trust level threshold L.

Mobility model. Since vehicles are driven along the roads, we can model the mobility of the vehicles in this way: vehicles firstly randomly choose a destination and then follow the shortest path map based movement [13] at

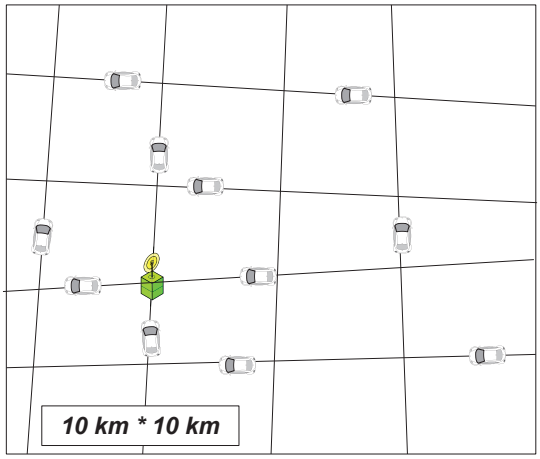


Fig. 4 Map for simulation

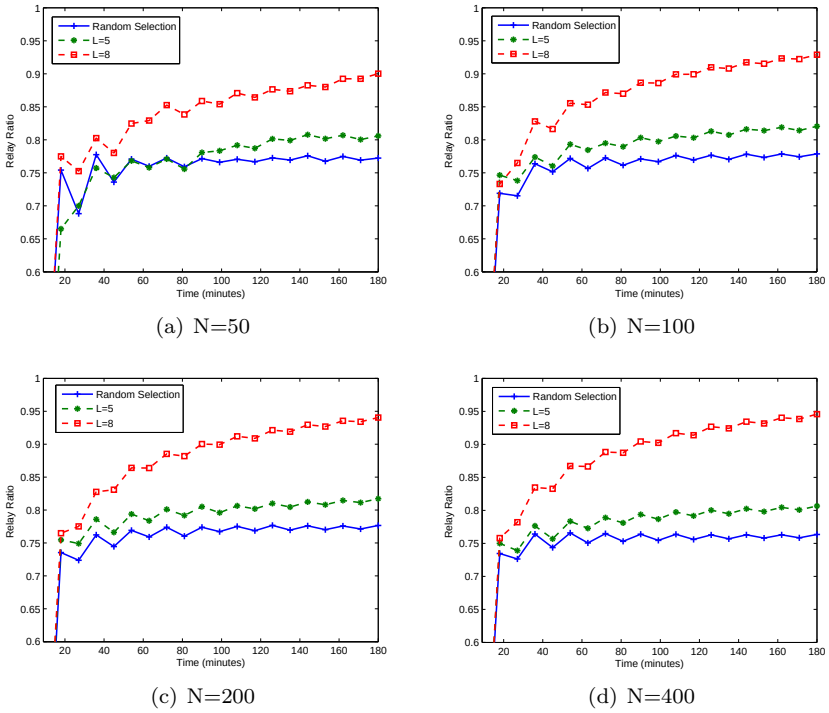
Table 1 SIMULATION SETTINGS

Parameter	**Setting**
Simulation	
area	$10000 \times 10000\ m^2$
duration	3 hours
number of trust levels	$m = 10$
RSU	
number	1
transmission radius	$1000m$
Vehicles	
total number	$N = 50, 100, 200, 400$
transmission radius	$300m$
velocity	$36km/h$
trust level threshold	$L = 5, 8$
message generation interval per vehicle	1 piece / 6 min
malicious vehicles proportion	$30\%, 40\%, 50\%, 60\%$
drop probability	$\rho = 20\%, 30\%, 40\%, 50\%$

a constant speed of $36km/h$. After reaching the destination, they stop for 5 minutes, and then choose a new random destination to repeat the above. During the random walk, once a vehicle is selected as the relay vehicle, it changes its route immediately and follows the shortest path to the RSU for relaying the message. After that, it recovers to drive following the random walk model.

Adversary model. We assume that the malicious vehicles follow the same mobility model as the normal vehicles, and the only difference is that after they accept to relay the message, they drop the relayed messages with a probability ρ. The proportion of malicious vehicles, defined as the number of malicious vehicles to the total number of vehicles, is another variable in the simulation.

The detailed parameter settings are summarized in Table 1. We conduct the simulations with different L and compares it with random selection under



(a) N=50 (b) N=100

(c) N=200 (d) N=400

Fig. 5 Relay ratio versus specific time period with different trust level thresholds

different N, and then we perform the simulation with different ρ and malicious proportion. For each case, we run the simulation for 3 hours, and the average performance results over 10 runs are reported.

6.2 Simulation Results

6.2.1 Relay Ratio

In Fig. 5, we compare the relay ratio of the vehicular ad hoc network with different relay selection policies, i.e., random selection, PTRS scheme with trust level threshold $L = 5$ and $L = 8$, under different vehicle number $N = 50, 100, 200, 400$ and malicious proportion of 50% with dropping probability of 50%. From the figure, we can see that the relay ratio is very low when relay vehicles are chosen randomly. By contrast, after adopting our proposed PTRS scheme, the relay ratio can be improved from 75% to 95%, which demonstrates the effectiveness of our proposed scheme in improving the message relay ratio. From the figure, it can be also seen that the relay ratio increases with the increase of vehicle number N and trust level threshold L. The reason is that when there are more vehicles, more messages will be generated and the mali-

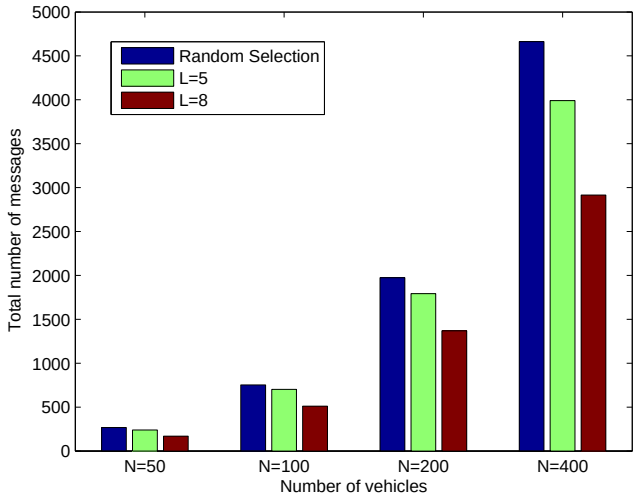


Fig. 6 Total number of messages generated in 3 hours with different relay selection policies

cious vehicles have more chances to relay messages and then be detected by the scheme, which finally makes them be excluded in the relay selection. At the same time, when trust level threshold L is higher, better behaved vehicles are chosen and they increase the relay ratio of the network. However, from Fig. 6, we find that the total number of generated messages will decrease when trust level threshold increases because in this case, the requesting vehicles have less chances to meet a qualified relay vehicle among its nearby candidate vehicles when their requirements are higher. Combine the above two figures together, we can find that there is always a trade-off between the utility and efficiency of our proposed scheme.

6.2.2 Detection Ratio

Fig. 7 depicts the detection ratio variations within 3 hours for different total number of vehicles. From the figure, we can see that the detection ratio converges to nearly 100% as time increases; at the same time, it converges faster when the total vehicle number increases. The reason is similar to the above: more vehicles generate more messages which gives malicious vehicles more chances to relay messages and then be detected by the scheme.

We further compare the detection ratios with different malicious proportion in terms of different dropping probability in Fig. 8. From the comparisons, we can see that with the same malicious proportion, detection ratio increases as dropping probability increases. Because malicious vehicles with higher dropping probability are more easily detected. Intuitively, when malicious proportion is higher, the detection ratio is higher. However, by observing the figure, we find that the detection ratio reaches its highest as malicious proportion

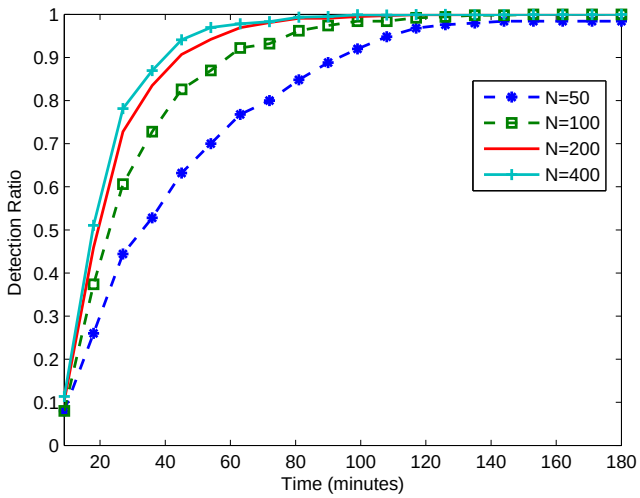
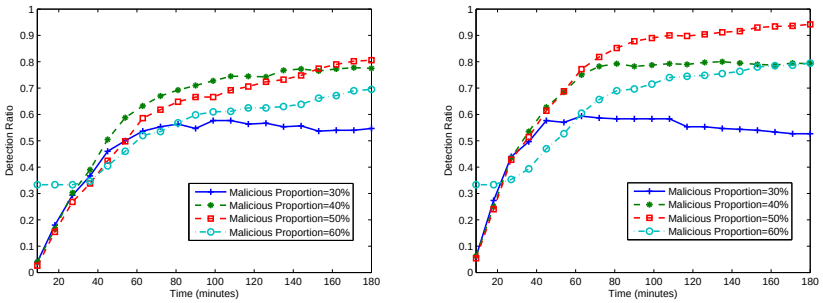
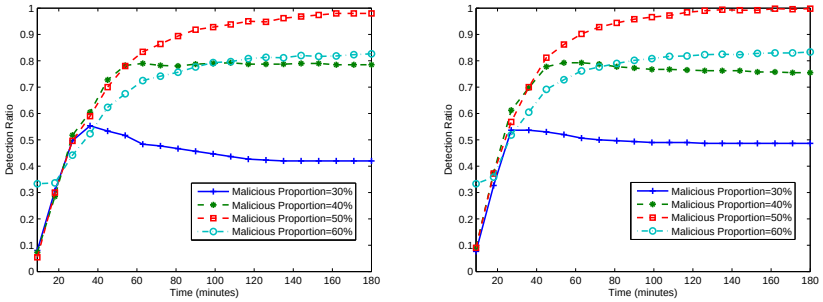


Fig. 7 Detection ratio versus time with trust level threshold L=8



(a) Dropping probability ρ=20%

(b) Dropping probability ρ=30%



(c) Dropping probability ρ=40%

(d) Dropping probability ρ=50%

Fig. 8 Detection ratio varies with time under different malicious vehicle proportions

increases to 50%. After that, the detection ratio decreases as the malicious proportion increases. The reason is that when malicious proportion exceeds 50%, the system will be overturned.

7 Related Work

To date much research effort has been paid to preserve the privacy of vehicles in vehicular communications [6, 14, 15]. Similar to our work, a simple method is to use pseudonyms, which however may cause many issues. In [6], Lu et al. consider a scenario when the pseudonyms are changed at improper location or time, for example, on the road. In this way, the location and velocity information embedded in the safety messages could still provide a clue for an adversary to link the pseudonyms, which leads to privacy leakage. To cope with this issue, they propose a strategy to change the pseudonyms at social spots where many vehicles gather, e,g., intersections when the traffic light turns red and parking lots neat a shopping mall. This solution is reasonable because when vehicles gather at those social spots, their velocities and locations are the same and the location privacy will be achieved. However, this method is not applicable to our scenario because unlike velocity and location, the reputation score of a vehicle is unchangeable in a period. In [14], Lu et. al proposes a social-based privacy-preserving packet forwarding protocol for vehicular DTN. In this protocol, a road side unit is used to help store and forward packets for vehicles. This proposed protocol, based on conditional privacy-preserving authentication (CPPA) technique, is robust against packet analysis, packet tracing and black hole attacks. The experimental results show that the SPRING protocol efficiently improves the delivery ratio, lowers the average delay and preserves the privacy of vehicles. This work has the same idea on "packet forwarding" to improve the delivery ratio like ours. However, it does not consider the reliability of relays. Another efficient conditional privacy preservation protocol is proposed in [15], to address the issue of anonymous authentication with authority traceability. The work is characterized by short-time anonymous key generation to solve the problem of key storage, fast safety message verification and efficient tracking algorithm.

Another recent group of papers look at how to ensure the trustworthiness of messages in propagation [16–19] or reliability of vehicle relay [20]. One way to address this problem is to collect the opinions or endorsements on the message in its propagation. For example, Li and Malip proposed a message announcement scheme [16]. In this scheme, the message receiver is able to evaluate the message reliability based on sender's reputation. Upon receiving each message, the receiver will evaluate by giving a feedback report. Later the sender vehicle's reputation will be aggregated based on those feedback reports from receivers. The system takes advantages of a centralized structure in VANET, which is similar to our proposed scheme. This work is also robust against both external and internal adversaries to a reasonably good level. Zhang proposes a message propagation model [17] to collect and propagate peers' opinions. The peers are

able to make local decisions on whether to follow the information by evaluating both its trust level and others' opinions. Since the framework is manipulated in a distributed and collaborative way, it shows great scalability. Experimental results also show the effectiveness of the proposed scheme. However, neither of these works consider the privacy issue of vehicles in message exchange, and the assumption that a cluster leader is always reliable in forwarding messages is not always practical in the real world. Another direction to this problem is laid on the technique of group signature and secret sharing. In [18], Daza proposes a privacy-preserving vehicle-generated announcement scheme to protect the system against both internal and external attacks. Specifically, a prior approach is used to thwart fake announcement launched by internal attacks and reduces the verification cost of endorsed messages to one signature verification. A (t, n)-threshold signature is used to verify an announcement only when at least t out of n vehicles endorse the message. Finally, a compound protocol is proposed combining three privacy-preserving variants together. Wu et al. propose a privacy-preserving system to guarantee message trustworthiness in vehicle-to-vehicle communications [19]. When a message-linkable group signature (MLGS) is produced and attached which ensures the vehicle anonymity. Later, after the endorsements for a message are aggregated, a threshold authentication mechanism will be executed to help vehicles decide whether to trust the message. To speed up the validation of authenticated messages, a batch message processing approach is used. Though the privacy issue has been considered, the misbehaviors of vehicles are not taken into account, neither do the system provide any incentives to the vehicles participating in the evaluations of messages.

Based on the investigations above, how to achieve anonymity and trust at the same time has been a challenging research issue which attracts researchers' attention, some of the works have been done in the context of participatory sensing [21–24]. In [21], Wang et al. propose an anonymous reputation management protocol to solve the problem of "trust without identity" in mobile sensing. In this protocol, the blind signature technique is used to achieve anonymity. Besides, by issuing a reputation certificate, the server will only know who wants to participant without knowing its actual sensing report. In [22], the authors present a way to transfer the reputation values belonging to the same user between its different pseudonyms. This kind of transfer is manipulated by a trusted server, which also maintains a list of mappings between real user identities and all the associated pseudonyms. Another similar solution is proposed in [23], called IncngniSense. In this framework, blind signature is used to generate periodic pseudonyms and a reputation transfer based on cloaking mechanism is presented.

In contrast to the existing solutions, though our work relies on a trust authority to update and manage reputation scores and trust levels, anonymous authentication and verification are conducted between two parties to meet the dynamic requirements of VANET. Our trust model is developed on existing technique of trust management scheme. In particular, the work directly related

to the ours is the Dirichlet-based trust model proposed by Fung et al. in [11] and Josang in [9].

8 Conclusion

In this paper, we have developed a scheme in order to help a vehicle choose another reliable vehicle for relaying a message. By establishing a Dirichlet-based trust model, the proposed PTRS scheme improves the relay ratio of the whole network. In addition, we introduced a trust-based request-response scheme when a requesting vehicle wants to select a relay among candidate vehicles which is able to preserve the privacy of a candidate vehicle. Detailed security analyses have shown that our proposed PTRS scheme is resistant against most attacks launched by selfish or malicious attackers. Through extensive performance evaluation, we have demonstrated that the proposed PTRS scheme can improve the relay ratio with the presence of selfish or malicious attackers.

Acknowledgements 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.

References

1. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007. [Online]. Available: http://iospress.metapress.com/index/ch4d4dg8yl2qhr0w.pdf
2. R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2014.02.020
3. 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.
4. H. Hu, R. Lu, Z. Zhang, and H. Zhu, "Replace: A reliable trust-based platoon service recommendation scheme in vanet," *IEEE Transactions on Vehicular Technology*, to appear.
5. J. Zhang, "A survey on trust management for vanets," in *IEEE International Conference on Advanced Information Networking and Applications (AINA), 2011.* IEEE, 2011, pp. 105–112.
6. R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE T. Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012. [Online]. Available: http://dx.doi.org/10.1109/TVT.2011.2162864
7. L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Security and Privacy in Ad-hoc and Sensor Networks*. Springer, 2007, pp. 129–141.
8. C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *vehicular Technology, IEEE Transactions on*, vol. 57, no. 6, pp. 3357–3368, 2008.
9. A. Jøsang and J. Haller, "Dirichlet reputation systems," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on.* IEEE, 2007, pp. 112–119.
10. A. Jsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, 2002, pp. 2502–2511.

11. C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Transactions on Network and Service Management*, vol. 8, no. 2, pp. 79–91, 2011. [Online]. Available: http://dx.doi.org/10.1109/TNSM.2011.050311.100028
12. 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.
13. R. Lu, X. Lin, H. Zhu, X. S. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 4, pp. 1483–1493, 2010.
14. R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM 2010. 29th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 15-19 March 2010, San Diego, CA, USA*, 2010, pp. 632–640. [Online]. Available: http://dx.doi.org/10.1109/INFCOM.2010.5462161
15. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.
16. Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang, "A reputation-based announcement scheme for vanets," *IEEE T. Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012. [Online]. Available: http://dx.doi.org/10.1109/TVT.2012.2209903
17. J. Zhang, C. Chen, and R. Cohen, "Trust modeling for message relay control and local action decision making in vanets," *Security and Communication Networks*, vol. 6, no. 1, pp. 1–14, 2013.
18. V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *IEEE T. Vehicular Technology*, vol. 58, no. 4, pp. 1876–1886, 2009. [Online]. Available: http://dx.doi.org/10.1109/TVT.2008.2002581
19. Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE T. Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010. [Online]. Available: http://dx.doi.org/10.1109/TVT.2009.2034669
20. H. Hu, R. Lu, and Z. Zhang, "Vtrust: A robust trust framework for relay selection in hybrid vehicular communications," in *Globecom'15*, San Diego, CA, USA, 2015.
21. X. O. Wang, W. Cheng, P. Mohapatra, and T. F. Abdelzaher, "Artsense: Anonymous reputation and trust in participatory sensing," in *Proceedings of the IEEE INFOCOM 2013, Turin, Italy, April 14-19, 2013*, 2013, pp. 2517–2525. [Online]. Available: http://dx.doi.org/10.1109/INFCOM.2013.6567058
22. K. L. Huang, S. S. Kanhere, and W. Hu, "A privacy-preserving reputation system for participatory sensing," in *37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, October 22-25, 2012*, 2012, pp. 10–18. [Online]. Available: http://dx.doi.org/10.1109/LCN.2012.6423585
23. D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "Incognisense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervasive and Mobile Computing*, vol. 9, no. 3, pp. 353–371, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2013.01.003
24. Q. Li and G. Cao, "Providing efficient privacy-aware incentives for mobile sensing," in *IEEE 34th International Conference on Distributed Computing Systems, ICDCS 2014, Madrid, Spain, June 30 - July 3, 2014*, 2014, pp. 208–217. [Online]. Available: http://dx.doi.org/10.1109/ICDCS.2014.29