A Reputation-Based Announcement Scheme for VANETs

Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, and Jie Zhang

***Abstract*—Vehicular ad hoc networks (VANETs) allow vehicles to generate and broadcast messages to inform nearby vehicles about road conditions, such as traffic congestion and accidents. Neighboring vehicles can utilize this information, which may improve road safety and traffic efficiency. However, messages generated by vehicles may not be reliable. We propose a novel announcement scheme for VANETs based on a reputation system that allows evaluation of message reliability. We present a secure and efficient scheme that is robust and fault tolerant against temporary unavailability of the central server.**

***Index Terms*—Announcement scheme, message reliability, reputation system, vehicular ad hoc networks.**

I. Introduction

A VEHICULAR ad hoc network (VANET) is formed by roadside infrastructure and mobile nodes embedded within vehicles that are connected in a self-organized way. Active research in VANETs is demonstrated by numerous papers in the academic literature, for example, [1]–[19] and ongoing projects [20], [21] in the industry. VANETs allow vehicles to generate and broadcast messages about road conditions, such as traffic congestion, accidents, and road conditions. We call these kinds of messages road-related messages and a scheme that facilitates vehicles to generate and broadcast road-related messages an announcement scheme. Broadcast of road-related messages may help vehicles to be aware of the situation ahead of them and, as a result, may provide a safer driving environment. In addition, it also has the capability to improve efficiency of traffic on road networks. However, these benefits can only be realized if the road-related messages generated by vehicles are reliable.

We say that a message is reliable if it reflects reality. Unreliable messages may result in various consequences, for example, journey delays or accidents. Unreliable messages may be the result of vehicle hardware malfunction. For example, if a sensor in a vehicle is faulty, then the messages generated based on the information provided by the faulty sensor may be false. Unreliable messages can also be generated intentionally. For example, some vehicles may generate and broadcast false road congestion messages with the intention to deceive other vehicles into avoiding certain routes. In the extreme case, unreliable message may lead to injuries and even deaths. Hence, evaluation of the reliability of vehicle-generated messages is of importance in VANETs.

In a large VANET environment, vehicles are assumed to have a weak (or no) trust relationship with each other [2]. This raises the question: how do vehicles decide whether to rely on a message? In this paper, we address this problem by proposing a novel reputation-based announcement scheme for VANETs. The reliability of a message is evaluated according to the reputation of the vehicle that generates this message. A message is considered reliable if the vehicle that generates the message has a sufficiently high reputation. The reputation of a vehicle is represented by a numerical score. This reflects the extent to which the vehicle has announced reliable messages in the past. It is computed based on feedback reported by other vehicles. Feedback contains a numerical score representing the feedback-reporting vehicle's evaluation of the reliability of the message. The score is collected, updated, and certified by a trusted party (e.g., a reputation server). The reputation score evolves, as time elapses, based on the reliability of messages that the vehicle announces. Vehicles tend to give positive feedback for reliable messages. This increases the reputation score. Meanwhile, a reputation score decreases when negative feedback is reported.

The rest of this paper is organized as follows. We discuss related work in Section II. In Section III, we introduce the entities involved in our scheme and their relationships. We also introduce the notation and algorithms needed in our scheme and show how to initialize a system that applies our scheme. We then elaborate our scheme in Section IV. We analyze the robustness of the scheme in Section V. In Section VI, we discuss other properties of our scheme and some related issues. In Section VII, we analyze the performance of our announcement scheme. Section VIII shows some possible approaches to extending the scheme. We conclude in Section IX and discuss future work.

II. Related Work

There have been a number of announcement schemes proposed to evaluate the reliability of announcement messages in VANETs. Generally, a message is considered reliable if 1) the

Manuscript received January 10, 2012; revised April 27, 2012 and June 13, 2012; accepted June 25, 2012. Date of publication July 23, 2012; date of current version November 6, 2012. The work of Q. Li, while he was with the School of Computer Engineering, Nanyang Technological University, and the work of J. Zhang was supported by the Ministry of Education Singapore Tier-1 Funding under Grant M4010265.020. The work of A. Malip was supported in part by the University of Malaya and in part by the Ministry of Higher Education Malaysia. The review of this paper was coordinated by Prof. J. Deng.

Q. Li and J. Zhang are with the School of Computer Engineering, Nanyang Technological University, Singapore 639798 (e-mail: qin.li.2008@live.rhul.ac.uk; zhangj@ntu.edu.sg).

A. Malip, K. M. Martin, and S.-L. Ng are with the Information Security Group, Royal Holloway, University of London, TW20 0EX Surrey, U.K. (e-mail: amizah.malip.2008@live.rhul.ac.uk; keith.martin@rhul.ac.uk; s.ng@rhul.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2012.2209903

integrity of the message is valid, 2) the message was generated and announced by a legitimate vehicle, and 3) there is a means of "measuring" message reliability.

Digital signatures are commonly used to satisfy the first two requirements [1]–[3], [5], [6], [9], [10], [12], [14], [18], [19]. To achieve the third requirement, different techniques have been proposed. These include the threshold method [2], [3], [10], [14], [19], network modeling [6], and trust-based and reputation-based models [1], [5], [12], [18]. We will discuss those most closely related to our work.

A majority of the schemes in the literature uses the threshold method, for example, [2], [3], [10], [14], [19], and [22]. In this mechanism, a vehicle accepts a message if it receives messages with the same content that have been announced by a number of distinct vehicles that exceed a threshold within a time interval. The threshold may be a fixed system-wide parameter [3], [14] or a flexible parameter [2], [10], [19]. The threshold has to be chosen carefully. It should not be so high that insufficient endorsement occurs and vehicles are not able to utilize the information received. It should not be so low that the decision may be affected by the presence of adversaries. In our scheme, we do not require multiple messages from other vehicles to evaluate the reliability of a message. Indeed, we may only need to verify one message provided that the reputation of the announcing vehicle is sufficiently high. This allows vehicles to make decisions and act upon messages quickly.

Golle *et al.* [6] proposed the evaluation of message reliability by modeling the network. They present a scheme that allows vehicles to detect and correct malicious messages in VANETs. Vehicles are assumed to maintain a "model" of the VANET, which contains all the knowledge that the vehicles possess about the VANET. A vehicle can then compare the messages received against the model of the VANET. A message that is consistent and agrees with the vehicle's model is likely to be accepted as valid. Inconsistent messages are addressed using a heuristic approach. A vehicle will search for explanations for the inconsistent messages and rank all possible explanations according to the heuristic approach. The message with the highest scoring explanation will be validated. However, requiring vehicles to possess a wide knowledge of the network may be infeasible and impractical. In our work, we propose a simpler and more practical model. We evaluate messages based on the simple principle of reputation, where the reliability of a message generated by a vehicle is reflected by its reputation score.

Several trust- and reputation-based models, for example, [1], [5], [12], and [18], have been presented in the literature. In these schemes, a decentralized infrastructure is adopted. However, the issue associated with decentralized infrastructures is that robustness is often not guaranteed.

In [5], Dötzer *et al.* proposed a reputation system based on a mechanism called opinion piggybacking. In this approach, a vehicle generates a message and broadcasts it to neighboring vehicles. A receiving vehicle will append its own opinion about the reliability of the message, which may be based on the content of the message or the aggregated opinions already appended to the message. Upon receiving a message, a vehicle is required to compute and aggregate previous opinions appended to the message before it decides and generates its own opinion. This may create a computational burden on receiving vehicles. In addition, details of implementation such as the initialization of the reputation system and the updating of reputation scores of vehicles were not discussed. Issues of revocation and robustness against possible collusion of adversaries were also not addressed.

In the scheme of Minhas *et al.* [12], message reliability is evaluated by a hybrid approach to model the trustworthiness of the message generator. In this scheme, vehicle trustworthiness is modeled based on the combination of three trust models: 1) role-based trust; 2) experience-based trust; and 3) majority-based trust. Role-based trust exploits certain predefined roles that are enabled through the identification of vehicles. For example, vehicles may have more trust toward traffic patrol or law enforcement authorities compared with other vehicles. To avoid impersonation attacks, each vehicle is required to possess a certificate that includes its name, role, and public key, issued by a trusted authority for authentication purposes. Majority-based trust is similar to the threshold method that we discussed earlier. Experience-based trust is established based on direct interactions: A vehicle determines who to trust based on how truthful they have been in their past interactions. However, such a model requires vehicles to establish a long-term relationship with each other, which may not be practical in a large VANET environment. Furthermore, it also requires vehicles to store information regarding vehicles that they have encountered in the past. This may lead to storage problems. A similar approach of experienced-based trust was proposed by Patwardhan *et al.* [1].

Schmidt *et al.* proposed a framework for vehicle behavior analysis in [18]. A vehicle's behavior refers to all observable information, including its movement and position in the past and present. A receiving vehicle accumulates a sequence of messages from a broadcasting vehicle, and these may provide sufficient information for behavior analysis. The result of this analysis will help to determine a vehicle as trustworthy, neutral, or untrustworthy. In this approach, vehicles are required to make observations before a decision can be made. This may not be desirable in VANETs, since vehicles are not able to act quickly upon the messages received.

Compared with these trust- and reputation-based approaches, our work features the follows.

1) We take advantage of the already-existing centralized infrastructure in a highly dynamic and distributed environment of VANETs. This allows us to design a secure and efficient announcement scheme.
2) We design a comprehensive announcement scheme using a reputation system that allows evaluation of message reliability that is practical, efficient, and robust against adversaries. Vehicles may provide feedback for messages received. These feedbacks accumulate to a vehicle's reputation score. Hence, short-term encounters between vehicles may lead to long-term trust, which is represented by reputation scores.
3) Vehicles can quickly decide whether to rely on a message or not based on the reputation score. The reputation score

reflects the extent to which a vehicle has announced reliable messages in the past, which reflects the likelihood that it will announce reliable messages in the future.

Here, we focus only on the research related to the issue of evaluating message reliability for an announcement scheme in VANETs. For other issues, see [2], [10], [23], and [24] for wider overviews of the topic.

III. Preliminaries

In this section, we introduce the entities involved in our scheme and their relationships. We also introduce some algorithms and notation. Finally, we will describe how to initialize the system.

A. Entities

Our system consists of three types of entity: 1) a reputation server; 2) access points; and 3) vehicles.

1) Reputation Server: We rely on a centralized reputation server that we assume is a trusted authority. One role of the reputation server is to maintain the reputation of vehicles. This includes collecting feedback, aggregating feedback to produce reputation, and propagating reputation. The reputation server is also in charge of admitting vehicles into and revoking them from the system.

There are several justifications for adopting a centralized architecture. First, it is a common practice that vehicles are regulated and governed by some centralized authority, such as the Driver and Vehicle Licensing Agency in the United Kingdom. Hence, it is natural to adopt a centralized architecture. In addition, a centralized architecture has some advantages over a decentralized system. For example, it is often easier to manage, control, and secure a centralized system.

We assume that the reputation server is equipped with a clock.

2) Access Points: Our scheme relies on access points, which are physical wireless communication devices. These are connected with the reputation server, acting as a communication interface between vehicles and the reputation server. The purpose of access points is to allow vehicles to communicate with the centralized reputation server in a convenient and frequent manner. It is worth noting that our scheme does not require a vehicle to be able to communicate with the reputation server all the time. Further, our scheme does not require a secure communication channel between an access point and the reputation server in the normal running of the scheme. Rather, it suffices that a public communication channel connects an access point and the reputation server.

We envisage that access points are installed at locations frequently visited by vehicles such as fuel stations, service stations, and traffic lights. The number of access points required depends on the size of the system, the road topology and traffic patterns, etc.

3) Vehicles: Vehicles are the end users of the system. They broadcast and receive messages to and from their neighboring vehicles. In our scheme, a vehicle comprises the actual vehicle and its human user. We assume that there is no prior trust between vehicles. Upon receipt of a message, the receiving vehicle needs to evaluate the reliability of the message before considering how to act upon it.

We assume that a vehicle is equipped with a computing device called an onboard unit (OBU), which has wireless communication capability to broadcast and receive messages to and from other OBUs on neighboring vehicles. In addition, we assume that trusted hardware is embedded as part of an OBU so that no secret data can be learned by anyone, including the vehicle itself. The trusted hardware can securely store keys and perform embedded cryptographic operations, such as digital signatures. We also assume that a secure clock is embedded within the trusted hardware.

B. Algorithm Components and Notation

The algorithms needed in our scheme are described as follows.

1) Our scheme requires a reputation aggregation algorithm Aggr. It computes a reputation score for each vehicle based on feedback reported by other vehicles. We will discuss it in more detail in Section IV-F.
2) We need a time discount function, denoted by $\mathsf{TimeDiscount}$. It is a nonincreasing function whose range is [0, 1]. It takes as input a nonnegative value representing a time difference and outputs a number between 0 and 1. One simple example is
$$\mathsf{TimeDiscount}(t) = \begin{cases} 1 - t/\Psi_{\mathrm{td}}, & \text{if } t < \Psi_{\mathrm{td}} \\ 0, & \text{if } t \geq \Psi_{\mathrm{td}} \end{cases}$$
where $\Psi_{\mathrm{td}} > 0$ is a public parameter, determining how quickly the time discount function decreases as t increases.
3) We require two secure digital signature schemes, denoted by $\mathsf{DS}_1 = (\mathsf{KeyGen}_1, \mathsf{Sign}_1, \mathsf{Verify}_1)$ and $\mathsf{DS}_2 = (\mathsf{KeyGen}_2, \mathsf{Sign}_2, \mathsf{Verify}_2)$, where KeyGen, Sign, and Verify denote key generation, signing, and verification algorithms, respectively. We use two digital signature schemes because they will be used for different purposes, and hence, there may be different requirements for each scheme.
4) We require a secure cryptographic hash function denoted by H.
5) We require a secure message authentication code (MAC) algorithm denoted by MAC.
6) We also require a vehicle clock regulation protocol denoted by VCRP. It consists of a server-side protocol, denoted by VCRP_S, and a vehicle-side protocol, denoted by VCRP_V. The purpose of VCRP is to ensure that only the reputation server is able to regulate the secure clock embedded in the trusted hardware of a vehicle. An entity authentication protocol can be applied to achieve the protocol VCRP.
7) We require three configurable public parameters Ψ_{rs}, Ψ_t, and $\mathbb{T}$. The parameter Ψ_{rs} acts as a threshold and is used by a vehicle to determine whether another vehicle is reputable. It is a constant between 0 and 1. The parameter Ψ_t also acts as a threshold and is used to determine

whether a message tuple is sufficiently fresh for feedback reporting. The parameter $\mathbb{T}$ is a large time interval over which a sufficiently large number of vehicles report feedback relating to a vehicle.

C. Initialization of the System

The initialization of the system includes initialization of the reputation server, new vehicles, and new access points.

1) Initialization of the Reputation Server: When a new announcement scheme is set up, the reputation server is initialized as follows.

1) It installs the reputation aggregation algorithm Aggr.
2) It installs the algorithms KeyGen_1, Sign_1, KeyGen_2, and Verify_2.
3) It generates its own public and private key pair (pk_S, sk_S) using KeyGen_1. The private key sk_S is then kept confidential.
4) It installs the server-side protocol $\mathsf{VCRP_S}$.
5) It regulates its own clock.
6) It creates a database that will store the following data for every vehicle in the system: the identity, public key, MAC key, current reputation score, and all feedback reported for the vehicle.

2) Admission of New Vehicles: When a new vehicle V chooses to join the system, it is initialized as follows.

1) It assigns it a unique identifier, denoted by id_V.
2) It generates a public and private key pair, which are denoted by (pk_V, sk_V), for the vehicle using the algorithm KeyGen_2.
3) It generates a MAC key mk_V for the vehicle.
4) It embeds the private key sk_V, the MAC key mk_V, and the algorithm Sign_2 into the trusted hardware of the vehicle. It also embeds the vehicle clock regulation algorithm $\mathsf{VCRP_V}$ into the trusted hardware. We require that the confidentiality of sk_V and mk_V is protected during the embedding.
5) It applies the server-side protocol $\mathsf{VCRP_S}$ to send a clock regulation instruction to regulate the clock embedded within the trusted hardware of V.
6) It installs the hash function H, the algorithms Verify_1 and Verify_2, its own public key pk_S, and the thresholds Ψ_{rs} and Ψ_t into the OBU of the vehicle. Note that these are not necessarily installed into the trusted hardware of the vehicle.
7) It creates a record in its database for vehicle V containing id_V, pk_V, and mk_V. The initial reputation score field is set to 0, and the feedback field is left empty.

3) Installation of New Access Points: When a new access point is installed in the system, a communication channel needs to be established between the access point and the reputation server. Subsequently, the access point serves as a communication interface between vehicles and the reputation server.

IV. Operation of the Announcement Scheme

We describe our scheme by showing how the reputation of a vehicle is formed, propagated, updated, and utilized to determine the reliability of a message sent by the vehicle. The operation of the scheme consists of the following phases: reputation certificate retrieval, message announcement, message reliability evaluation, feedback reporting, reputation update, and vehicle revocation.

A. Reputation Certificate Retrieval

In this phase, a vehicle retrieves its latest reputation certificate from the reputation server. When a vehicle V_b drives into the wireless communication range of an access point, it retrieves its own reputation certificate from the central server via the access point as follows:

1) V_b sends its identity id_{V_b} to the server via the access point.
2) The reputation server generates a reputation certificate C for the vehicle, where

$$C = (id_{V_b}, pk_{V_b}, t_c, rs_{V_b}, \sigma)$$

in which t_c denotes the time when C is generated, and it is obtained from the reputation server's clock, rs_{V_b} denotes the reputation score of V_b at time t_c, and $\sigma = \mathsf{Sign}_1(id_{V_b}, pk_{V_b}, t_c, rs_{V_b})_{sk_S}$ denotes a digital signature using the algorithm Sign_1 and private key sk_S on $(id_{V_b}, pk_{V_b}, t_c, rs_{V_b})$.
3) The reputation server sends C to V_b via the access point.
4) Once V_b obtains C, it stores the reputation certificate locally. Previously obtained reputation certificates can then be deleted.

Note that in this procedure, V_b is not required to authenticate itself to the reputation server. This is because the reputation certificate is not confidential and can be retrieved by any vehicle. We will show later that there is no point in one vehicle retrieving the reputation certificate of another vehicle.

In addition, V_b does not need to retrieve a new reputation certificate every time it meets an access point. It only needs to do so when its time-discounted reputation value $rs_{V_b} \cdot \mathsf{TimeDiscount}(t - t_c)$, where t denotes the current time, will be less than the reputation threshold Ψ_{rs} before it meets another access point in the future.

B. Message Broadcast

In this phase, V_b generates a road-related message and broadcasts it to its neighboring vehicles. This is described as follows.

1) V_b converts the information obtained, for example, from its sensors or driver, into a message m. The technical detail of how this is done is beyond the scope of this paper. It computes the hash value $\mathsf{H}(m)$, which it then submits to its trusted hardware.
2) The trusted hardware retrieves the current time t_b from its embedded clock and generates a time-stamped signature θ, where

$$\theta = \mathsf{Sign}_2\left(t_b, \mathsf{H}(m)\right)_{sk_{V_b}}$$

and V_b outputs t_b and θ.

3) V_b forms a message tuple M, where

$$M = (m, t_b, \theta, C)$$

and V_b broadcasts M to its neighboring vehicles.

C. Message Reliability Evaluation

Upon receiving the message tuple $M = (m, t_b, \theta, C)$, a receiving vehicle V_r performs the following procedure:

1) V_r submits θ to its trusted hardware.
2) The trusted hardware retrieves the current time t_r from its embedded clock, stores the tuple (t_r, θ), and then outputs t_r to V_r.
3) V_r checks the following:
   a) whether the time-discounted reputation score is acceptable, i.e.,

$$rs_{V_b} \cdot \mathsf{TimeDiscount}(t_r - t_c) \geq \Psi_{rs}$$

   where t_c is extracted from C;
   b) whether the message tuple M is sufficiently fresh, i.e., $t_r - t_b \leq \Psi_t$;
   c) whether $\sigma \in C$ is valid, by using the verification algorithm Verify_1 and the public key of the reputation server pk_S;
   d) whether θ is valid, by using the verification algorithm Verify_2 and the public key pk_{V_b}, which can be extracted from C.

   If all checks are positive, then vehicle V_b is considered to be reputable. Message m is thus considered as reliable and can be taken into consideration. The message tuple M is stored for future feedback reporting. Otherwise, V_b is not considered to be reputable, and m is not considered to be reliable. However, if at least Steps 3b, 3c, and 3d are positive, then the message tuple M is still stored for future feedback reporting; otherwise, it is discarded.

D. Feedback Reporting

In this phase, when vehicle V_r has its own experience about the event that the message m describes, it is able to judge the reliability of the message. Then, if V_r wants to report feedback to the reputation server, it performs the following procedure.

1) V_r generates a feedback rating $fr \in \{0, 1\}$, where $fr = 1$ represents that m is reliable, while $fr = 0$ represents that m is false. In this paper, we only use binary feedback rating for simplicity.
2) V_r submits $(id_{V_b}, id_{V_r}, fr, t_b, \mathsf{H}(m), \theta)$ to its trusted hardware.
3) The trusted hardware retrieves t_r from the tuple (t_r, θ) that was previously stored during the message reliability evaluation phase and computes a MAC value δ, where

$$\delta = \mathsf{MAC}\left(id_{V_b}, id_{V_r}, fr, t_b, t_r, \mathsf{H}(m), \theta\right)_{mk_{V_r}}$$

   and the trusted hardware then outputs t_r and δ.
4) V_r forms a feedback tuple F, where

$$F = (id_{V_b}, id_{V_r}, fr, t_b, t_r, \mathsf{H}(m), \theta, \delta).$$

   We say that F is positive feedback if $fr = 1$ and negative feedback if $fr = 0$.
5) When V_r drives into wireless communication range of an access point, it sends the feedback tuple F to the reputation server via the access point.

Note that V_r is not required to authenticate itself to the reputation server during feedback upload. This is because F contains the MAC value θ, which can only be generated by V_r and the reputation server.

E. Reputation Update

In this phase, the reputation server updates the reputation score rs_{V_b} of vehicle V_b on receipt of a feedback tuple $F = (id_{V_b}, id_{V_r}, fr, t_b, t_r, \mathsf{H}(m), \theta, \delta)$ as follows:

1) The reputation server first checks the following:
   a) whether $t_r - t_b \leq \Psi_t$;
   b) whether δ is valid, by computing a MAC on the tuple $(id_{V_b}, id_{V_r}, fr, t_b, t_r, \mathsf{H}(m), \theta)$ using mk_{V_r} and checking whether it matches δ;
   c) whether θ is valid, by using the algorithm Verify_2 and pk_{V_b}.

   If any check fails, then this procedure is terminated, and F is discarded.
   1) If the checks pass, then the reputation server considers the feedback tuple F as valid and stores it in the database.
   2) The reputation server applies the reputation aggregation algorithm Aggr on all stored feedback relating to V_b to compute the latest reputation score rs_{V_b} for vehicle V_b. It then replaces the previous reputation score in the database with rs_{V_b}.

F. Reputation Aggregation Algorithm

In this section, we discuss how the reputation aggregation algorithm Aggr works. We will show how Aggr produces the latest reputation score rs_V for vehicle V based on all stored feedback as follows.

1) The aggregation algorithm Aggr first selects all feedback reported for V whose corresponding message tuple was broadcast from time $\mathbb{T}$ in the past up to the present time. More formally, let t_a denote the time when this aggregation is running. The algorithm Aggr selects a subset of feedback $\mathcal{F}$, where

$$\mathcal{F} = \{F : (id_{V_b} = id_V) \wedge (t_b \geq t_a - \mathbb{T})\}.$$

   The feedback whose corresponding message was broadcast earlier than time $\mathbb{T}$ in the past is ignored and deleted if necessary for the sake of data storage efficiency.
2) Multiple feedback reported by one vehicle V_i for V is aggregated into one intermediate value $\hat{r}_{V_i}$. Let $\mathcal{F}_{V_i}$ denote the set of feedback reported by the vehicle V_i for V and whose corresponding message was broadcast from time $\mathbb{T}$ in the past up until the present time, i.e.,

$$\mathcal{F}_{V_i} = \{F : (id_{V_b} = id_V) \wedge (id_{V_r} = id_{V_i}) \wedge (t_b \geq t_a - \mathbb{T})\}.$$

The value $\hat{r}_{V_i}$ can be aggregated using a weighted average as follows:

$$\hat{r}_{V_i} = \frac{\sum_{F \in \mathcal{F}_{V_i}} fr \cdot (\mathbb{T} - (t_a - t_b))}{\sum_{F \in \mathcal{F}_{V_i}} (\mathbb{T} - (t_a - t_b))}. \quad (1)$$

This gives the more recent feedback greater weight than the less recent feedback.Let $\mathcal{V}$ denote the set of vehicles that have each reported at least one feedback for V in the past $\mathbb{T}$ time, i.e.,

$$\mathcal{V} = \{V_i : (id_{V_b} = id_V) \wedge (id_{V_r} = id_{V_i}) \text{ for some } F \in \mathcal{F}\}.$$

The value $\hat{r}_{V_i}$ is computed for each vehicle $V_i \in \mathcal{V}$.

3) Let $\mathcal{V}^-$ denote the set of vehicles reporting at least one negative feedback for V in the past $\mathbb{T}$ time, i.e.,

$$\mathcal{V}^- = \{V_i : (id_{V_b} = id_V) \wedge (id_{V_r} = id_{V_i}) \wedge (fr = 0) \text{ for some } F \in \mathcal{F}\}.$$

The latest reputation score rs_V is computed as follows:

$$rs_V = \begin{cases} \frac{\sum_{V_i \in \mathcal{V}} \hat{r}_{V_i}}{|\mathcal{V}|}, & \text{if } |\mathcal{V}^-| < \Psi_{nf} \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

where Ψ_{nf} is a configurable public parameter. Its impact on the robustness of the scheme and its configuration will be discussed in Section V-B. The intuition of this equation is that rs_V is computed as the average of $\hat{r}_{V_i}$ if not too many vehicles reporting negative feedback for V in the past $\mathbb{T}$ time; otherwise, rs_V decreases to 0, indicating that V has conducted a message fraud attack, which will be discussed in Section V-B.

G. Vehicle Revocation

The reputation server revokes a vehicle from the system if $|\mathcal{V}^-| < \Psi_{nf}$. If a vehicle is revoked, then the reputation server stops providing new reputation certificates for it. Feedback reported by the revoked vehicle will not be considered as valid. Note that previously issued reputation certificates will gradually expire as time elapses.

V. Robustness Analysis

In this section, we analyze the robustness of our scheme in the presence of adversaries with respect to the following attacks.

1) Message fraud. In this attack, an adversary deceives a vehicle complying with the scheme into believing that a false message m' is reliable.
2) Reputation manipulation. In this attack, an adversary unfairly inflates or deflates the reputation score of a target vehicle. This target vehicle can be the adversary itself.

Note that reputation manipulation may lead to message fraud, since an adversarial vehicle can get its reputation unfairly inflated by a reputation manipulation attack and then launch a message fraud attack.

We categorize adversaries into two groups.

1) External adversaries attack the system without joining as legitimate vehicles.
2) Internal adversaries are legitimate vehicles that attack the system.

We define a notion of robustness: an announcement scheme provides (Φ_{MF}, Φ_{RM}) robustness if we have the following.

1) Φ_{MF} is the maximum number of vehicles that an adversary can deceive during a time period of length $\mathbb{T}$ without itself getting revoked. This evaluates the extent to which the scheme is robust against a message fraud attack.
2) Φ_{RM} is the maximum value by which the reputation score of a vehicle can be unfairly manipulated (increased or decreased) by adversaries. This evaluates the extent to which the scheme is robust against a reputation manipulation attack.

We say that an announcement scheme provides strong robustness if it provides (0, 0) robustness, i.e., $\Phi_{MF} = 0$ and $\Phi_{RM} = 0$.

A. Robustness Against External Adversaries

1) Robustness Against Message Fraud:

Claim 1: Our proposed scheme provides strong robustness against external adversaries conducting message fraud.

Proof: To perpetrate a message fraud attack, an external adversary can engage in any of the following strategies.

1) Obtain a valid reputation certificate C for a vehicle V and then forge a message tuple $M' = (m', t_b, \theta, C)$ containing a false message m' in the name of V.
2) Forge a reputation certificate C', and then, create a valid message tuple $M' = (m', t, \theta, C')$ containing a false message m'.
3) Corrupt a vehicle V that is about to generate and broadcast a message tuple $M = (m, t_b, \theta, C)$, and then, replace m with a false message m' so that V will generate and broadcast $M' = (m', t_b, \theta, C)$.

An external adversary is not able to forge a valid reputation certificate C or a valid message tuple M, unless the adversary has access to either the private key sk_S or sk_V. Hence, assuming that the digital signature schemes used are secure and the reputation server and vehicles manage keys appropriately, then the adversary is not able to succeed using the first two strategies. It is also reasonable to assume that an external adversary is not able to corrupt a vehicle to replace the message m generated by the vehicle with a false message m' before the message tuple M is generated. Hence, we can regard our scheme as providing strong robustness against message fraud attacks. ■

2) Robustness Against Reputation Manipulation:

Claim 2: Our proposed scheme provides strong robustness against external adversaries conducting reputation manipulation.

Proof: To conduct a reputation manipulation attack, an external adversary can engage in any of the following strategies.

1) Forge and report valid feedback in the name of vehicle V_r for a target vehicle V with its own choice of feedback rating.

2) Corrupt a vehicle V_r that is about to generate and report a feedback $F = (id_V, id_{V_r}, fr, t_b, t_r, \mathsf{H}(m), \theta, \delta)$ for the target vehicle V and replace fr with a value of its own choice.
3) Corrupt the reputation server and directly modify the stored reputation score rs_V of the target vehicle V.

Forging valid feedback involves forging a valid MAC value δ generated using the MAC key of a legitimate vehicle. Assuming the use of a secure MAC algorithm and that vehicles manage their MAC keys appropriately, an external adversary is not able to forge δ using the first strategy. It is also reasonable to assume that that an external adversary is not able to corrupt a vehicle to replace fr with a false feedback rating or corrupt the reputation server to modify the stored reputation score. Hence, our scheme provides strong robustness against external adversaries conducting reputation manipulation attacks. ■

B. Robustness Against Internal Adversaries

It is straightforward to see that our scheme does not provide strong robustness against internal adversaries. This is because an internal adversary with a time-discounted reputation score greater than Ψ_{rs} can deceive its neighboring vehicles into believing that a false message m' is reliable. Further, when an internal adversary receives a message tuple $M = (m, t_{V_b}, \theta, C)$ from a target vehicle, it can always intentionally report false feedback. In this section, we will analyze to what extent our scheme is robust against internal adversaries.

1) Robustness Against Reputation Manipulation: We consider the worst situation where all adversaries collude together to attack the same target vehicle V with the same goal (to inflate or deflate the reputation score of V). Recall that to form a valid feedback, an internal adversary has to obtain a valid message tuple $M = (m, t_b, \sigma, C)$ generated by V and obtain it before time $t_b + \Psi_t$. We assume that Ψ_t is set such that only those vehicles physically within wireless communication range of a broadcasting vehicle are able to obtain a valid message tuple before time $t_b + \Psi_t$.

Claim 3: Let $\mathcal{V}$ denote all vehicles that have each reported at least one valid feedback relating to V, and let $\mathcal{V}_a \subseteq \mathcal{V}$ denote all internal adversaries among $\mathcal{V}$. The robustness against internal adversaries conducting reputation manipulation is $\Phi_{RM} = |\mathcal{V}_a|/|\mathcal{V}|$.

Proof: Let $V_a \in \mathcal{V}_a$ be an internal adversary and $\hat{r}_{V_a}$ be the intermediate value aggregated from all feedback reported by V_a for V, according to (1). It is easily seen that all false feedback reported by V_a for V only changes the intermediate value $\hat{r}_{V_a}$. The maximum influence of the intermediate value $\hat{r}_{V_a}$ on the reputation score rs of the target vehicle V is equal to $1/(|\mathcal{V}|)$. Hence, the maximum extent of reputation manipulation due to one internal adversary is $1/(|\mathcal{V}|)$. Therefore, the maximum extent of reputation manipulation due to all members of $\mathcal{V}_a$ is equal to $(|\mathcal{V}_a|/|\mathcal{V}|)$, i.e., $\Phi_{RM} = |\mathcal{V}_a|/|\mathcal{V}|$. ■

If $|\mathcal{V}_a|$ is relatively small compared with the size of $\mathcal{V}$, then the maximum unfair impact of internal adversaries conducting reputation manipulating attack is still small. In this case, $\mathcal{V}_a$ only adds a small noise into the reputation score of the target vehicle. It is reasonable to assume that in a VANET, there is only a small proportion of internal adversaries compared with the entire population of vehicles. Hence, the unfair impact of internal adversaries conducting reputation manipulating attack remains small.

2) Robustness Against Message Fraud: With respect to a message fraud attack, apart from those strategies mentioned in Section V-A, which can be used by external adversaries, internal adversaries have an additional attack strategy. This strategy is for an internal adversary to exploit its own reputation, as described in the beginning of this section. However, an internal adversary cannot use this strategy to conduct message fraud persistently.

Claim 4: Let p denote the overall probability that vehicles will report negative feedback upon being deceived by a false message. Let the public parameter Ψ_{nf} be set such that $\Psi_{nf} = |\mathcal{V}_a| + \Delta$, where Δ is a safe margin. The robustness against internal adversaries conducting message fraud is $\Phi_{MF} = |\mathcal{V}_a| + \Delta/p$.

Proof: If an internal adversary deceives more than $(\Psi_{nf})/p$ vehicles during a time period of length $\mathbb{T}$, then the number of negative feedbacks reported for it is likely to be greater than Ψ_{nf}. This results in its reputation score decreasing to 0, as shown in (2). The internal adversary will thus be revoked. Hence, the maximum number of vehicles that an internal adversary can deceive during a time period of length $\mathbb{T}$ without getting revoked is equal to $(\Psi_{nf})/p$.

Note that a vehicle is revoked if $|\mathcal{V}^-| \geq \Psi_{nf}$. Given $\Psi_{nf} = |\mathcal{V}_a| + \Delta$, then $|\mathcal{V}^-| < \Psi_{nf}$, meaning that the internal adversaries $\mathcal{V}_a$ are not able to get the target vehicle V revoked by reputation manipulation. The robustness of the scheme against an internal adversary conducting message fraud is $\Phi_{MF} = |\mathcal{V}_a| + \Delta/p$. ■

By combining Claims 3 and 4, we can conclude that our scheme is $(\Phi_{MF} = |\mathcal{V}_a| + \Delta/p, \Phi_{RM} = |\mathcal{V}_a|/|\mathcal{V}|)$ robust against internal adversaries.

VI. Discussion

In this section, we discuss other properties and issues related to our scheme.

A. Fault Tolerance

One important advantage of our scheme is its fault tolerance. This is shown from two perspectives: 1) temporary unavailability of the reputation server and 2) temporary unavailability of access points.

Recall that during the message broadcast and message reliability evaluation phases, the reputation server is not involved. In other words, the reputation server is offline with respect to message broadcast and message reliability evaluation. From the perspective of a vehicle, the reputation server is only needed for reputation certificate retrieval and feedback reporting. The temporary unavailability of the reputation server only affects those vehicles that happen to retrieve their reputation certificates when the reputation server is unavailable. These vehicles have to continue using their existing reputation certificates. This negative effect only lasts until they successfully retrieve their new reputation certificates the next time that the reputation

server is available again. The operation of the system is largely unaffected during the time when the reputation server is temporarily unavailable.

Access points that become temporarily unavailable also do not greatly affect the operation of the system. An unavailable access point only affects those vehicles that happen to drive into wireless communication range of the access point for retrieving reputation certificates. In most cases, vehicles can be expected to drive into wireless communication range of another working access point within a reasonable time period.

B. Privacy

Privacy is often an important criteria of an announcement scheme for VANETs. There has been active research into this topic, e.g., [2], [10], [23], [25], and [26]. While privacy has not been the main focus of this paper, it is worth noting that this scheme provides a certain level of privacy for vehicles, as follows.

1) The identity of a vehicle can easily be anonymized by using a pseudonym instead of the real identity. Our scheme then provides a vehicle with anonymity with respect to all entities except for the reputation server.
2) It is possible for the reputation server to issue multiple pseudonyms and public keys for a vehicle. This requires the reputation server to preembed multiple private keys into the trusted hardware of the vehicle. This provides the vehicle with an extent of unlikability with respect to messages broadcast: other entities (except for the reputation server) cannot link messages broadcast under different pseudonyms.
3) The reputation server does not learn messages from feedback, as only the hash value of a message is contained in the feedback (see Section IV-D).

C. Incentive to Participation

One issue is a vehicle's incentive for participating in the announcement scheme. This has two facets, as follows.

1) Vehicles may lack incentive to broadcast a message to other vehicles. This directly reduces the utilization of the announcement scheme.
2) Vehicles may lack incentive to provide feedback. This results in degradation of the accuracy and robustness of the scheme, the latter arising since the probability that vehicles will report negative feedback upon being deceived by a false message is reduced.

One possible approach to increase the vehicles' participation is to introduce some incentives. For example, the reputation server can introduce some policy that rewards a vehicle, with some points for example, if it constantly has a high reputation score or reports a large amount of feedback. Because the reputation server acts as the central authority and maintains all reputation and feedback information, it is easy for the reputation server to introduce such rewarding policy.

D. Bootstrapping

Another issue is bootstrapping a new vehicle. In our scheme, we specify that the initial reputation score of a new vehicle is zero. This configuration often causes a bootstrapping problem in a reputation system, where a newcomer has difficulty establishing its reputation. However, in our scheme, a new vehicle with zero initial reputation score is still able to establish its reputation. This is because, although messages broadcast by the new vehicle will not be considered as reliable, the receiving vehicles are still able to report feedback for these messages. Gradually, the new vehicle will be able to establish its own reputation.

It is also worth noting that assigning zero initial reputation score to a new vehicle, as described in our scheme, is conservative. The purpose of this is to discourage a vehicle with bad reputation from whitewashing its reputation by rejoining the system with a new identity. This is useful when the cost of rejoining the system with a new identity is negligible. However, in a VANET, it is often difficult or costly for a vehicle to reenter the system with a different identity. In this case, a new vehicle could be initialized with a positive reputation, thus alleviating the bootstrapping problem.

E. Use of Data Mining Techniques

Data mining techniques could be used to further improve the accuracy and robustness of our scheme. In our scheme, all feedback is kept by the reputation server. This makes it possible for the reputation server to using data mining techniques to distinguish false feedback from honest feedback and vehicles reporting false feedback from those reporting honest feedback. In addition, the richness of feedback may aid data mining techniques to improve the detection accuracy. For example, we have the following.

1) Feedback is linked to its reporting vehicle.
2) Time information is contained in feedback.
3) Feedback reported by different vehicles regarding the same message can be linked together (as they share the same $\mathsf{H}(m)$ entry in feedback tuple).

Such rich information may help data mining techniques to improve the detection accuracy.

F. Incorporating Trusted Vehicles

In reality, some vehicles are widely regarded as trustworthy, such as police vehicles, fire vehicles, and ambulances. Messages broadcast by trusted vehicles can be considered as reliable. In our scheme, it is easy to take into consideration trusted vehicles. A simple solution, for example, is that the reputation server initializes a trusted vehicle with a high reputation score, such as 1.

VII. Performance Analysis

In this section, we analyze the performance of our announcement scheme. We first show some simulation results and then compare our scheme with other announcement schemes in terms of performance.

A. Simulation

In this section, we show some simulation results about the performance of our announcement scheme. This is evaluated from the following aspects.

1) Message drop rate: The average rate that reliable messages are rejected by a receiving vehicle due to low reputation scores of broadcasting vehicles after time discount, as described in Section IV-C.
2) Temporary unavailability of the reputation server: The average increase of message drop rate due to the temporary unavailability of the reputation server.
3) Temporary unavailability of access points: The average increase of message drop rate due to the temporary unavailability of some access points.

We use an event-based real street map vehicular network simulator called GrooveNet [27] and extend it to incorporate our scheme into the simulator. The road network used in simulations is an urban area of 10 km^2 chosen from the city of Pittsburgh, PA. These map data are extracted from the U.S. Census Bureau's TIGER/Line database [28]. The communication range is 30 min. The duration of each experiment is 30 min. The configurations of these simulations are in line with many studies in the literature, such as [19].

An experiment is configured and then conducted as follows.

1) Access points are generated and populated randomly over the selected road network.
2) Vehicles are generated, populated randomly, and move in the selected road network. Their mobility models are as follows: A vehicle follows the vehicle in front, and a vehicle moves at the speed limit of a street when it is leading on the street. Their trip models are as follows: a vehicle randomly moves until it is 10 km from its starting point; the vehicle then takes the shortest path back to the starting point and starts again along a different path.
3) Road events randomly occur in the road network throughout the experiment. The time that an event will last is set randomly from 1 to 120 s.
4) Vehicles that are sufficiently close to an event can "experience" the event. The distance for a vehicle to experience an event is set randomly from 1 to 100 m.
5) A vehicle broadcasts a message regarding an event that it experiences, along with its latest reputation certificate.
6) A message receiving vehicle determines whether it accepts the received message by evaluating the reputation of the broadcasting vehicle, as specified in Section IV-C. The reputation threshold parameter Ψ_{rs} is set conservatively to 0.8. The time discount parameter Ψ_{td} is set conservatively to 1 h. Note that Ψ_{td} in a real-world implementation should be much longer than 1 h, perhaps a few days or even longer. The purpose of setting it to 1 h is to make the effect of the time discount function more visible during the experiments as well as to make it in line with 30 min of experiment time.
7) A message receiving vehicle may report feedback if it later experiences the event described by the message within the time when the event still exists. The probability that the vehicle will report a feedback is set conservatively to 0.1.
8) When a vehicle moves into communication range of an access point, it retrieves and then updates its latest reputation certificate and reports all feedback that it has generated and not yet reported.
9) The reputation server updates the reputation of each vehicle based on feedback received from all vehicles and generates a new reputation certificate accordingly, as specified by Sections IV-E and F. The time interval $\mathbb{T}$ is set to 10 min. Note that $\mathbb{T}$ in a real-world implementation should be much longer than 10 min: perhaps weeks or even longer. The purpose of setting such a short time interval $\mathbb{T}$ in the experiments is, again, to make it in line with 30 min of experiment time.

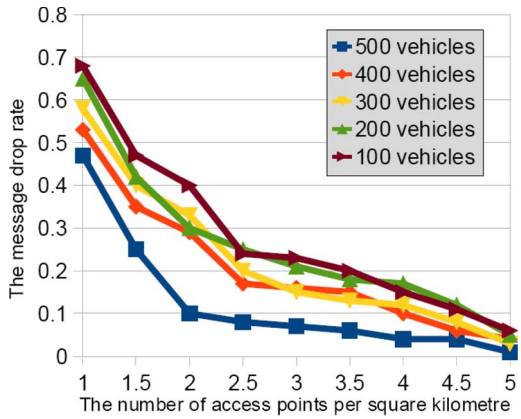


Fig. 1. Decrease of message drop rate due to the increase of access point density.

Fig. 1 shows the simulation results of message drop rate with respect to the different density of access points and vehicles. From Fig. 1, the results of experiments show that the message drop rate decreases when the density of access points increases. A sharp decrease of message drop rate is seen when the number of access points is increased from 1 to 2 km^{-2}. Then, the decrease of message drop rate becomes relatively slow when the number of access points is increased from 2 to 5 km^{-2}. This is natural since if there are more access points, then vehicles tend to encounter them more often and thus tend to retrieve the latest reputation certificate more frequently from the reputation server. As a result, vehicles tend to broadcast messages with more "fresh" reputation certificates, and the reputation scores will tend to be discounted less by the receiving vehicles using the time discount function TimeDiscount. This results in less rejection of reliable messages and thus a decrease in the message drop rate.

The density of vehicles also impacts on the message drop rate. We observe a decrease of message drop rate when the density of vehicles increases. A modest but noticeable decrease is seen when the density of vehicles increases from 100 to 500 vehicles in the selected road network of 10 km^{-2}. This is reasonable because more feedback tends to be reported for a vehicle in a vehicle-dense road network. Consequently, it is more likely that feedback whose corresponding message tuple was broadcast within the past $\mathbb{T}$ time is reported for a

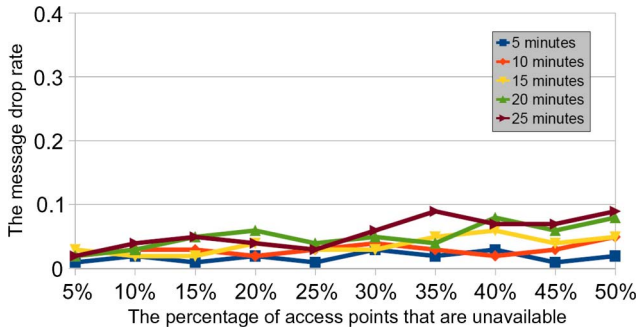


Fig. 2. Increase of message drop rate due to temporary unavailabilities of the reputation server.

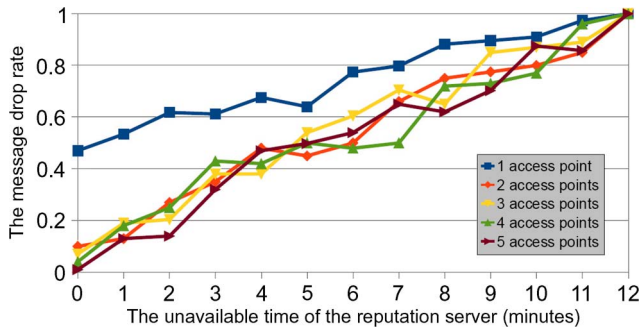


Fig. 3. Increase of message drop rate due to temporary unavailabilities of some access points.

vehicle, and thus, a reputation certificate becomes available for the vehicle. This results in the reliable messages broadcast subsequently by the vehicle being accepted by the receiving vehicles, given that the broadcasting vehicle has a sufficiently high reputation score. Hence, we observe a decrease in the message drop rate.

However, this observed difference in the message drop rate due to the density of vehicles may not be as significant as shown in our experiments. This is because in our experiments, the time interval $\mathbb{T}$ is set to 10 min, which is much shorter compared to a real-world implementation. This causes a reputation certificate to be less likely available to a vehicle compared with an implementation with a much longer $\mathbb{T}$.

In addition, in our simulations, the communication range of a vehicle and an access point is set conservatively to 300 m. If it is set to 1000 m, the maximum communication range of the standard 802.11p, then the message drop rate should further decrease. This is because vehicles can "meet" an access point and retrieve the latest reputation certificate more frequently.

Fig. 2 shows the simulation results of the increase of the message drop rate due to the temporary unavailability of the reputation server with respect to various densities of access points. In these experiments, we deployed and populated 500 simulated vehicles. From Fig. 2, the results of the experiments show that the increase of the message drop rate is approximately proportional to the unavailable time of the reputation server when the unavailable time is less than 12 min. When the unavailable time reaches 12 min, the message drop rate increases to 1. This is reasonable because in our experiments we set the time discount parameter Ψ_{td} to 1 h and the reputation threshold parameter Ψ_{rs} to 0.8. With these configurations, the time-discounted reputation score of a vehicle cannot exceed the reputation threshold if the reputation certificate was obtained from the reputation server more than 12 min ago.

However, in a real-world implementation in which a much longer time discount parameter Ψ_{td} is expected, the rate of increase in the message drop rate due to temporary unavailabilities of the reputation server is expected to be significantly slower compared to the experiments. The minimum unavailable time of the reputation server that will result in a complete message drop is expected to extend long beyond 12 min.

Fig. 3 shows the simulation results of the increase of the message drop rate due to the temporary unavailability of some access points. In these experiments, we deployed and populated 500 simulated vehicles and 50 access points. We examined the increase in the message drop rate caused by various proportions of access points being unavailable for different periods of time, i.e., from 5 to 25 min. From Fig. 3, the results of the experiments show that the temporary unavailable access points slightly contribute to the increase in the message drop rate. This is reasonable, since when a vehicle comes across an unavailable access point, it can later retrieve its reputation certificate and report feedback via another working access point.

B. Performance Comparison

In this section, our scheme is compared with threshold schemes, which have been the mainstream announcement schemes. Our performance comparison focuses on communication overhead and processing delay. We choose two typical threshold-based schemes [2], [22] to represent threshold-based schemes, since their performance results are available in their papers.

With respect to the communication overhead, in our scheme, a message is accompanied by one identifier, two time stamps, one public key, two digital signatures, and one reputation sore. If we implement the digital signature schemes DS_1 and DS_2 using the standard IEEE 1609.2 ECDSA over NIST P-224 curve signature scheme, which has 112-bit security level, then a public key and a signature is 28 and 56 B, respectively [29]. If we choose ECDSA over NIST P-192 curve signature scheme, which has 80-bit security level, then a public key and a signature is 24 and 48 B, respectively [29]. If we further use 4, 8, and 1 B to represent an identifier, a time stamp, and a reputation score, respectively, then the communication overhead of our scheme with 112- and 80-bit security levels are $4+8+8+28+56+56+1=161$ bytes and $4+8+8+24+48+48+1=141$ bytes, respectively. In comparison, in the threshold scheme of [2], a message is accompanied by one signature of at least 160 B to achieve 80-bit security level. In the other threshold scheme of [22], a message is accompanied by one time stamp, one public key, and two signatures. If ECDSA over NIST P-192 curve signature scheme is adopted to achieve 80-bit security level, and the time stamp takes 8 B, then the communication overhead of this scheme is $8+24+48+48=128$ bytes.

With respect to the processing delay, signing and verification of an ECDSA over NIST P-224 curve signature take

3.3 and 6.5 ms, respectively, on a Pentium II 400 MHz machine [29]. Signing and verification of an ECDSA over NIST P-192 curve signature take 2.1 and 4.3 ms, respectively, on the same machine [29]. For our scheme, the processing of one message involves one signing (sender) and two verifications (recipient), which takes $3.3 + 6.5 + 6.5 = 16.3$ ms for 112-bit security level and $2.1 + 4.3 + 4.3 = 10.7$ ms for 80-bit security level. In comparison, in the threshold scheme of [2], signing and verification of a signature take at least 8.1 and 25.5 ms, respectively, on an Intel Pentium IV 3.0-GHz machine. The processing of one message involves one signing (sender) and one verification (recipient), which takes $8.1 + 25.5$ ms $= 33.6$ ms for 80-bit security level. In the other threshold scheme of [22], the processing of one message involves one signing (sender) and two verifications (recipient), which takes $2.1 + 4.3 + 4.3 =$ 10.7 ms for 80-bit security level.

Our comparison results show that with respect to the communication overhead and processing delay on one message, our scheme is similar to threshold-based schemes. However, note that in our scheme, a receiving vehicle requires only one message to trigger an action, whereas for a threshold-based scheme, multiple messages are required. Thus, by considering the overall communication overhead and processing delay, our scheme significantly outperforms threshold schemes.

Regarding the network modeling approach [6] and the trust- and reputation-based approaches [1], [5], [12], [18] that were discussed in Section II, these schemes are still at a conceptual level and lack technical details and performance evaluation. We thus cannot provide a detailed performance comparison between our schemes and these schemes.

VIII. Extended and Simplified Variants

In this section, we discuss some possible approaches to extend our standard scheme to increase its efficiency and flexibility. We will discuss how to facilitate multiple message broadcast to improve efficiency and how to enable a richer reputation evaluation to improve flexibility.

We also demonstrate how the proposed scheme can be simplified to reduce some of the hardware requirements on vehicles. The price for such simplification is weakened robustness against internal adversaries. We will discuss a simplified variant that does not require vehicles to have a secure clock and another simplified variant where vehicles do not require either a secure clock or a trusted hardware.

A. Multiple Message Broadcast

In this section, we discuss how to facilitate multiple message broadcasts to improve the efficiency of our scheme. In the standard scheme, a message tuple contains only one message m. If vehicle V_b intends to broadcast n messages $(m_1, m_2, \ldots, m_n)$, it has to generate n message tuples. A receiving vehicle then has to evaluate the reliability of each individual message tuple. In this section, we extend the standard scheme to facilitate multiple message broadcasts.

Suppose vehicle V_b wants to broadcast a message vector $\mathcal{M} = (m_1, m_2, \ldots, m_n)$ containing n messages. We briefly describe the modification of the standard scheme as follows. During the message broadcast phase, V_b computes the hash value $\mathsf{H}(m_i)$ for every $m_i \in \mathcal{M}$. It then computes a hash value as follows:

$$h = \mathsf{H}\left(\mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n)\right).$$

It then submits h to the trusted hardware to obtain a time-stamped signature $\theta = \mathsf{Sign}_2(t_b, h)_{sk_{V_b}}$. Then, a message tuple $M = (\mathcal{M}, t_b, \theta, C)$ is formed. During the message reliability evaluation phase, a receiving vehicle V_r checks the validity of θ on the tuple $(t_b, \mathsf{H}(\mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n)))$.

During the feedback reporting phase, V_r first generates a feedback rating vector $R = (fr_1, fr_2, \ldots, fr_n)$. If it provides a feedback rating for message m_i, then it assigns $fr_i \in \{0, 1\}$; otherwise, it assigns fr_i with $\perp$, which denotes that it assigns no rating for message m_i. Then, V_r submits the following to its trusted hardware:

$$(id_{V_b}, id_{V_r}, R, t_b, \mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n), \theta).$$

This is to obtain a MAC value δ as follows:

$$\delta = \mathsf{MAC}\left(id_{V_b}, id_{V_r}, R, t_b, t_r \right. \\ \left. \mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n), \theta\right)_{mk_{V_r}}.$$

Finally, V_r forms a feedback tuple as follows:

$$F = (id_{V_b}, id_{V_r}, R, t_b, t_r, \mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n), \theta, \delta).$$

During the reputation update phase, if all verifications are successful, then the reputation server uses all feedback ratings $fr_i \neq \perp$ to update the reputation score of V_b.

By adopting this extension, a vehicle is able to simultaneously broadcast multiple messages. A receiving vehicle can also simultaneously verify the reliability of all messages in a message vector. Moreover, the additional computational cost of this extension is negligible. This is because the additional computation involves only hash operations, which are significantly faster than the digital signature operations used in the standard scheme. Compared with the standard scheme, the broadcasting vehicle in this extended scheme only performs n extra hash operations to broadcast a message vector with n messages. A receiving vehicle also only performs n extra hash operations to verify the reliability of all messages in the message vector.

On the other hand, this extension incurs some additional communication overhead when a receiving vehicle reports a feedback tuple to the reputation server. A feedback tuple has to include the feedback rating for every message $fr_1, fr_2, \ldots, fr_n$ and the hash value of every message $\mathsf{H}(m_1), \mathsf{H}(m_2), \ldots, \mathsf{H}(m_n)$. The length of a feedback tuple in this extension is longer than that of the standard scheme.

B. Multilevel Reputation Evaluation

In this section, we discuss how to enable a richer reputation evaluation to improve the flexibility of the scheme. In the standard scheme, a vehicle maintains only one threshold

Ψ_{rs} to compare against the time-discounted reputation score when making a decision as to whether a received message is reliable. However, some messages tend to be more critical than others. We may accept a critical message only if it is provided by a highly reputable vehicle. Similarly, we may accept an unimportant message if it is provided by a reasonably reputable vehicle.

The standard scheme can easily be extended to facilitate the aforementioned multilevel reputation evaluation. The reputation server simply installs multiple thresholds $(\Psi_{rs}^1, \Psi_{rs}^2, \ldots, \Psi_{rs}^n)$ into each vehicle. These correspond to different levels of importance for different messages. When a vehicle receives a message, it just selects the corresponding threshold to compare against the time-discounted reputation score.

C. Simplified Variant 1

In our standard scheme, we assume that each vehicle is equipped with a secure clock. In this section, we relax this assumption: we assume that each vehicle has a clock that is not protected by the trusted hardware, i.e., the vehicle is able to modify the time information output by the clock. We outline this simplified variant by modifying the standard scheme as follows.

The vehicle clock regulation protocol VCRP and the public parameter Ψ_t are no longer required. Vehicles periodically synchronize their clocks with the reputation server. During the message broadcast phase, V_b retrieves the current time t_b from its clock, which is not protected by the trusted hardware. During the message reliability evaluation phase, Steps 1, 2, and 3b are removed. During the feedback reporting phase, V_r forms a feedback tuple $F = (id_{V_b}, id_{V_r}, t_b, fr, \mathsf{H}(m), \theta, \delta)$. Note that t_r in the standard scheme is removed in this variant. During the reputation update phase, Step 1a is removed.

This variant still provides strong robustness against external adversaries but it is less robust against internal adversaries. In this variant, the restriction removed from the standard scheme is that a vehicle is only able to generate valid feedback if it receives a message tuple before the time $t_b + \Psi_t$. Removing this restriction means that there is no time limitation on receiving a message tuple to generate valid feedback. Hence, internal adversaries can engage in the following strategy. Once an internal adversary obtains a message from the target vehicle, it later forwards it to another internal adversary when they drive within wireless communication range of each other. This message tuple can be further propagated to other internal adversaries in the same manner. All internal adversaries receiving the message tuple, regardless of the receiving time, report feedback relating to the target vehicle.

Let $\mathcal{V}_a'$ denote the set of internal adversaries obtaining at least one message tuple generated by the target vehicle. The robustness of this variant becomes $(\Phi_{MF} = |\mathcal{V}_a'|/p, \Phi_{RM} = |\mathcal{V}_a'|/|\mathcal{V}|)$, by the same argument in Section V-B. It is straightforward to see that the size of $\mathcal{V}_a'$ is greater than or equal to that of $\mathcal{V}_a$. Hence, the robustness of this variant may be less than that of the standard scheme. However, if the size of $\mathcal{V}_a'$ is still sufficiently small such that $\Phi_{MF} = |\mathcal{V}_a'|/p$ and $\Phi_{RM} = |\mathcal{V}_a'|/|\mathcal{V}|$ are still acceptable, then this variant can be an option for implementation.

D. Simplified Variant 2

In this variant, we remove the restriction from the standard scheme that each vehicle is equipped with trusted hardware and a secure clock. Instead, we assume that the OBU of a vehicle is equipped with a computing device without trusted hardware storage and a nonprotected clock. Note that in this variant, we do not assume that the OBU has a tamper-resistant device. Hence, the vehicle itself is able to access its private key and MAC key, which is prevented in the standard scheme. We outline this variant by modifying the standard scheme as follows.

The vehicle clock regulation protocol VCRP and the public parameter Ψ_t are no longer required. Vehicles themselves periodically synchronize their clocks with the reputation server. During admission of a new vehicle, the reputation server sends its private key and MAC key over a secure channel to the vehicle. These are no longer kept confidential from the vehicle. During the message broadcast phase, V_b retrieves the current time t_b from the nonprotected clock. Instead of the trusted hardware, V_b itself generates the signature $\theta = \mathsf{Sign}_2(t_b, \mathsf{H}(m))_{sk_{V_b}}$. During the message reliability evaluation phase, Steps 1, 2, and 3b are removed. During the feedback reporting phase, Step 2 is removed. During the reputation update phase, Step 1a is removed.

This variant also provides strong robustness against external adversaries. However, it is less robust against internal adversaries than the standard scheme and Variant 1. In this variant, the restriction further removed from Variant 1 is that a vehicle is not able to access its private key and MAC key. Removing this restriction means that internal adversaries can engage in another strategy. An internal adversary distributes its MAC key to another colluding internal adversary. Consequently, one internal adversary is able to generate feedback on behalf of another colluding internal adversary. This provides internal adversaries with a convenient way of conducting a reputation manipulation attack. Given every internal adversary possesses the MAC key of every other internal adversary from a colluding group, once an internal adversary receives a message tuple from a target vehicle, it can generate and report feedback on behalf of every colluding internal adversary.

Let $\mathcal{V}_a^*$ denote the set of all internal adversaries. Then, the robustness of this variant becomes $(\Phi_{MF} = |\mathcal{V}_a^*|/p, \Phi_{RM} = |\mathcal{V}_a^*|/|\mathcal{V}|)$. It is easily seen that $|\mathcal{V}_a| \leq |\mathcal{V}_a'| \leq |\mathcal{V}_a^*|$. Hence, the robustness of this variant may be less than that of the standard scheme and Variant 1. However, if the size of $\mathcal{V}_a^*$ is relatively small compared with that of $\mathcal{V}$, then Variant 2 is also another option for implementation.

IX. Conclusion and Future Work

In this paper, we have presented a novel reputation-based announcement scheme for VANETs to evaluate message reliability. We have shown that our scheme is robust against

external adversaries and robust against internal adversaries to a reasonably good level.

In future work, it might be of interest to investigate the following aspects.

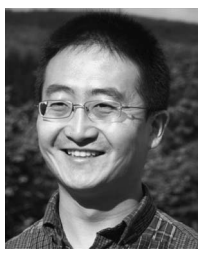
1) Although the current scheme already provides a certain level of privacy, it might be of interest to further enhance the privacy protection of the scheme.
2) In the current scheme, a vehicle and its human driver are represented by a single entity. It might be of interest to extend our scheme to reflect the potentially different reputations of human drivers and vehicles separately.
3) In the current scheme, a message broadcast by a vehicle is only utilized by its neighboring vehicles. It might be of interest to extend the current scheme in such a way that a message can be utilized by vehicles in a greater area.
4) In this paper, we present a simple feedback aggregation algorithm based on binary feedback ratings. It might be of interest to investigate alternative approaches that allow continuous feedback ratings and thus provide richer results.
5) It might be interest to investigate some concrete data mining techniques that can be used to further improve the robustness of the scheme.

ACKNOWLEDGMENT

The majority of Q. Li's work was done while he was with the Information Security Group, Royal Holloway, University of London, Egham, Surrey, U.K.

REFERENCES

[1] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.*, 2006, pp. 1–8.
[2] L. Chen, S. Ng, and G. Wang, "Threshold anonymous announcement in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 605–615, Mar. 2011.
[3] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car generated announcements in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, May 2009.
[4] J. Domingo-Ferrer and Q. Wu, "Safety and privacy in vehicular communications," in *Privacy in Location-based Applications*. Berlin, Germany: Springer-Verlag, 2009, pp. 173–189.
[5] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad hoc network reputation system," in *Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, 2005, vol. 1, pp. 454–456.
[6] P. Golle, D. H. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.
[7] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.
[8] J. Hubaux, P. Papadimitratos, and M. Raya, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.
[9] T. H. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "VANET alert endorsement using multi-source filters," in *Proc. 7th ACM Int. Workshop VANET*, New York, 2010, pp. 51–60.
[10] G. Kounga, T. Walter, and S. Lachmund, "Proving reliability of anonymous information in VANETs," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2977–2989, Jul. 2009.
[11] X. Lin, X. Sun, and P. Ho, "GSIS: Secure vehicular communications with privacy preserving," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2006.
[12] U. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad hoc networks," *Int. J. Comput. Intell. Theory Pract.*, vol. 5, no. 1, pp. 3–15, Jun. 2010.
[13] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop HotNets-IV*, College Park, MD, 2005.
[14] M. Raya, A. Aziz, and J. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. 3rd Int. Workshop Veh. Ad Hoc Netw.*, 2006, pp. 67–75.
[15] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. SASN*, 2005, pp. 11–21.
[16] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[17] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, 2008, pp. 1238–1246.
[18] R. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in VANETs," in *Proc. 4th Workshop V2VCOM*, Eindhoven, The Netherlands, 2008.
[19] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.
[20] C2CC, The Car-to-Car Communication Consortium, 2011. [Online]. Available: http://www.car-to-car.org
[21] R. Kroh, A. Kung, and F. Kargl, "VANETs security requirements," Secure Vehicle Communication (SeVeCom), Belgium, U.K., Tech. Rep., 2006.
[22] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.
[23] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw.*, 2007, pp. 19–28.
[24] P. Wex, J. Breuer, A. Held, T. Leinmüller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proc. IEEE VTC Spring*, 2008, pp. 2800–2804.
[25] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proc. Privacy Enhanc. Technol.*, vol. 3856, *Lecture Notes in Computer Science*, Berlin, Germany: Springer-Verlag, 2005, pp. 197–209.
[26] P. Papadimitratos, L. Buttyan, J. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proc. 7th ITST*, 2007, pp. 1–6.
[27] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai, "Groovenet: A hybrid simulator for vehicle-to-vehicle networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.—Netw. Serv.*, 2006, pp. 1–8.
[28] *TIGER/Line Database*, U.S. Census Bureau, Washington, DC, 2011. [Online]. Available: http://www.census.gov/geo/www/tiger
[29] M. Brown, D. Hankerson, J. López, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," in *Proc. CT-RSA*, 2001, pp. 250–265.



Qin Li received the Ph.D. degree in information security from the Royal Holloway, University of London, Surrey, U.K., in 2012.

He is currently a Postdoctoral Research Fellow with the Nanyang Technological University, Singapore. His research interests include reputation-based systems, cryptographic applications, and trust management.

Amizah Malip received the M.Sc. degree in mathematics of cryptography and communications in 2008 from the Royal Holloway, University of London, Surrey, U.K., where she is currently working toward the Ph.D. degree in information security.

Her research topics include wireless and network security, cryptographic protocols, usability, and privacy.

Keith M. Martin received the B.Sc. (Hons) degree in mathematics from the University of Glasgow, Glasgow, U.K., in 1988 and the Ph.D. degree from the Royal Holloway, University of London, Surrey, U.K., in 1991.

Between 1992 and 1996, he held a Research Fellowship with the University of Adelaide, Adelaide, Australia, where he investigated the mathematical modeling of cryptographic key distribution problems. In 1996, he joined the COSIC Research Group, Katholieke Universiteit Leuven, Leuven, Belgium, where he worked on the security for third-generation mobile communications. He rejoined Royal Holloway, University of London, in January 2000 and became a Professor of information security in 2007 and Director of the Information Security Group in 2010. He is the author of the recently published *Everyday Cryptography* by Oxford University Press. His current research interests include key management, cryptographic applications, and securing lightweight networks.

Dr. Martin is a previous Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY in the area of Complexity and Cryptography, as well as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. As well as conventional teaching, he is a designer and module leader on Royal Holloways distance learning M.Sc. Information Security program.

Siaw-Lynn Ng received the B.Sc. (Hons.) degree in mathematics from the University of Adelaide, Adelaide, Australia, in 1995 and the Ph.D. degree in mathematics from the Royal Holloway, University of London, Surrey, U.K., in 1999.

She joined the Information Security Group, Royal Holloway, University of London, as a Postdoctoral Research Assistant and is currently a Lecturer with the group. Her main research interests are in combinatorics and information security.

Jie Zhang received the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2009.

He is currently an Assistant Professor with the School of Computer Engineering, Nanyang Technological University, Singapore. His research interests include artificial intelligence and multiagent systems, trust modeling and incentive mechanisms, and mobile and vehicular ad hoc networks.