Toward VANET Utopia: A New Privacy Preserving Trustworthiness Management Scheme for VANET

Junggab Son*, Donghyun Kim*, HyungGeun Oh†, Dongsoo Ha‡, Wonjun Lee§
*Department of Computer Science, Kennesaw State University, Marietta, GA 30060
Email: {json, donghyun.kim}@kennesaw.edu
†National Security Research Institute, South Korea
Email: hgoh@nsr.re.kr
‡Department of Computer Science and Engineering, Hanyang University, Ansan, South Korea
Email: hds@hanyang.ac.kr
§Network Research Lab., School of Information Security, Korea University, Seoul, South Korea
Email: wlee@korea.ac.kr

***Abstract*—In vehicular ad hoc network (VANET), vehicles are connected in a self-organized manner to collect and share various traffic data about the road condition, accidents, traffic congestions, and other related events, This data can be used to improve the driving quality, however VANET vehicles may receive unreliable data broadcasted by malicious vehicles which may result in unsafe driving and accidents. Many schemes were proposed to deal with such unreliable data. A reputation-based scheme is one of the most promising in determining reliability of messages in a timely manner. Dealing with the privacy presents another challenge in VANET, as malicious vehicles must be detected and their reputation is assigned and updated while preserving their privacy. The system must be able to identify the malicious responses by continuously sending evaluation messages. To address these issues, this paper presents a novel reputation-based message evaluation scheme which guarantees the reliability of the messages as well as the privacy of vehicles. The paper presents some analyses results on the robustness of the scheme against plausible attacks.**

I. Introduction

A vehicular ad hoc network (VANET) illustrates the spontaneous creation of a wireless network of vehicles [1], [2]. VANET is created by connecting roadside units and vehicles embedded on-board modules in a self-organized manner [3], [4]. VANET vehicles collect and broadcast various data and information during their operation. This data include, but are not limited to, the road condition, traffic jams, accidents, abnormal weather condition, and other related events [5]. The so called *traffic information* provided by VANET can be used for the convenience of drivers [6]. In recent years, VANET has attracted significant attention due to the emergence of self-driving vehicles which can collect the traffic information from VANETs to determine the driving condition ahead [7].

Reliability of traffic information is one of the most important issues in VANET and must be guaranteed for the safety of vehicles. Generally, traffic information is considered reliable if it reflects the reality of current states [23]. Unreliable information may lead vehicles to unsafe situations such as hardware malfunction, unintended location, delays in the journey, or even accidents. In recent years, most schemes such as threshold-based [12], network modeling-based [18], and reputation-based approaches were proposed to deal with the reliability problem [19].

The reputation based scheme which utilizes the social networks services (SNSs) to address reliability issue is the most promising solution where vehicles can immediately determine reliability of received data. When a vehicle collects information and broadcasts it to others, it must send the information alongside the vehicles *reputation value*. Receiving vehicles can determine whether the information is reliable based on the reputation value of the broadcaster. Upon receiving data, the vehicles send evaluation messages about the information they have received. Positive messages on reliability of information result in higher credibility of the sender as it adds to their reputation value of that sender. While ensuring reliability of information, it is critical to preserve the vehicles privacy as part of the VANETs process [8], [9], [10]. The invasion of vehicle privacy, especially location privacy, may place the drivers of vehicles in unpleasant situations [11]. For example, a driver may be led to an unintended location based on advertisements, spams, blackmails, a situation with damaging social reputation, financial loss, and even stalking or physical violence. This privacy problem makes the design of the reputation-based reliability management system more challenging.

Updating reputation value of vehicles anonymously presents the most significant challenge. A vehicles reputation value must be updated to reflect the reliability of messages it is broadcasting. However, it is challenging to determine the broadcaster of traffic information and sent it the issued evaluation value. In addition, an adversary may perform various types of attacks taking advantage of the privacy. For example, the adversary may control its own reputation value by sending many positive evaluation messages. It is also possible that the adversary sends false information without restraint. A privacy preserving reputation management system must be able to deal with these problems. We define the following requirements based on our comprehensive survey.

The most significant problem is how to update reputation value of anonymous vehicles. A vehicle's reputation value must be updated to reflect its behavior. However, it is hard

to find where traffic information comes from and where an issued evaluation value sends to. In addition, an adversary may perform various kinds of attacks during hiding behind the privacy. For example, the adversary may control its own reputation value by sending many positive evaluation messages. It is also possible that the adversary sends false information without restraint. A privacy preserving reputation management system must be able to deal with these problems, and we define following requirements based on our comprehensive survey.

(a) **Privacy preservation**: The VANET reputation system must preserve vehicles privacy data such as their identity, locations, and reputation information. It also prevents plausible attacks which is based on anonymity.
(b) **Reputation management**: A reputation system has to manage reputation value for all vehicles in the system while preserving their privacy. Every vehicle must use a legitimate and verifiable reputation value and the issued evaluation value must be counted to represent validity.

To resolve the privacy issue, Chen et al. proposed a privacy aware reputation scheme for VANETs [24]. This scheme was designed based on the reputation system proposed by Li et al. [23], and can provide anonymity of vehicles and unlink ability of messages broadcasted by the same vehicle. However, this scheme assumed a reputation trusted server to address the reputation update issues, which is considered as very strong assumption in a real world application.

Contributions of this paper. This paper proposes a new cryptographical approach to resolve both the privacy and trustworthiness management problem for VANETs. The contributions of this paper are as follows:

(a) **Anonymous communication**: To preserve vehicles privacy, we adopt a pseudonym-based communication, where each vehicle uses a randomly generated pseudonym for anonymity. In addition, the approach requires every vehicle in the system to frequently change the pseudonym to achieve higher privacy.
(b) **Verifiable reputation value**: We design the reputation system to operate by a given timed session. A reputation management server issues the sessions secret, and only a legitimate reputation value can pass the verification process.
(c) **Enforcing update**: Before starting a new session, a server merges the received evaluation values issued for a pseudonym to create a list and will make vehicles retrieve their evaluation values. Following this, every vehicle will use this evaluation value to update its reputation value by merging the two values. A vehicle that didnt go through this update process cannot pass the reputation verification process. Our scheme can preserve vehicles privacy from the server without the need for a fully trusted model.

This paper is organized as follows. Section II introduces related work, Section III provides the system model, threats models, and security and privacy goals that are considered in this paper. Section IV provides some important background and Section V will describe the main contribution of the paper which is a new privacy-preserving reputation system. Section VI provides the evaluation for the proposed scheme and Section VII provides the summary and future research directions.

II. Related work

One of the important issues in VANET applications is checking the reliability of a message sent by another vehicle. To address this problem, several schemes were proposed to evaluate the reliability of VANET broadcasted messages. These schemes can be classified into three major categories of threshold-based models [12], [13], [14], [15], [16], [17], network modeling scheme[18], and reputation-based models [19], [20], [21], [22], [23].

In the threshold-based model, a vehicle considers a message reliable if the number of vehicles that sent a message with the same contents within a set time interval is larger than a given threshold. The most challenging problem in this model is that the vehicle has to wait until sufficient number of messages is received to reach the threshold even in case of an emergency. In other words, a reasonable threshold value has to be set for this process to be effective.

A vehicle in the network modeling scheme maintains a network model of vehicles in VANET and is used to evaluate message reliability. A received message can be considered as valid if it is consistent with and satisfying the network model. However, this scheme can be impractical in that vehicles must maintain a wide knowledge of the network, which may change rapidly.

Many schemes were proposed to provide reliability based on the reputation of the broadcaster. In these schemes, a vehicle sends traffic information with its reputation value, and then other vehicles judge whether the information is valid or not based on the reputation value of the broadcaster. The reputation-based approach is one of the most promising schemes as the receiving vehicles can decide about the reliability of messages solely based on the reputation value of its broadcaster [23]. Dotzer et al. proposed an opinion piggybacking mechanism that uses the receiving vehicles opinion about the reliability of messages [20]. Minhas et al. proposed a reliability evaluation scheme based on the combination of three trust models: role-based, experience-based, and majority-based trust [21]. Schemidt et al. proposed a reliability evaluation scheme based on a vehicles behavior [22]. In this scheme, a vehicles behavior such as movement and position in the past and present can be accumulated to determine trustworthiness. Li et al. proposed a reputation-based announcement scheme to evaluate reliability of messages [23]. This scheme accumulates feedbacks from other vehicles at a centralized server and uses them to determine the reliability of a vehicle.

The above schemes cannot prevent privacy infringement of vehicles which is one of the most important issues in VANET. To address this problem, Chen et al. proposed a privacy-aware reputation-based announcement scheme [24]. The scheme presented in [23] provides privacy of a vehicle

using a secure group signature scheme and a secure probabilistic encryption scheme. In this scheme, vehicles use a group signature when they send traffic information, and use the probabilistic encryption to hide the identity while the vehicles communicate with a server that is a fully trusted entity. Generally speaking, a fully trusted entity is impractical as it is difficult to implement it in a real world application.

III. Problem Description

This section describes the system model, security model, and problem statement.

A. System Model

Fig. 11 illustrates the system model for the system presented on this paper. The system model has four different entities: message broadcasting vehicle, message evaluation vehicle, local reputation server, and reputation management server. In a real application, a vehicle can be a sender as well as a receiver. However, we divide the vehicles into two different categories of a message broadcasting vehicle and a message evaluation vehicle. Since the two vehicles have different roles in our system model, this will help improve the understanding of the proposed scheme.

Message broadcasting vehicle (MBV): In our system model, an MBV has the role of sending various traffic information to other vehicles for driving convenience. This information includes, but is not limited to, traffic congestions, accidents, abnormal weather, road condition, and other related events. The MBV broadcasts to the other vehicles through a road side unit or an ad-hoc network. Although the information from the MBV is helpful in dealing with an abnormal situation, there might be a problem with the validity of the broadcasted information. To solve this problem we make MBVs to add their reputation record, thus other vehicles can accept or reject the information based on that record.

Message evaluation vehicle (MEV): As a MEV drives on the road, it maintains connections with a RSU or other vehicles to obtain traffic information on its route. The MEV receives traffic information along with the senders reputation record and decides whether to accept or reject the information based on that reputation record. Once a message is accepted, the MEV evaluates the traffic information and sends it to the reputation management server. We call this message an evaluation message. If the evaluation message was valid, the MEV gives it a positive score, otherwise the message receives a negative score.

Reputation management server (RMS): In our system model, a RMS manages the reputations of all of the MBVs. If the system would design a vehicle to merge the evaluation messages and update the reputation record, that vehicle can easily forge the records. To prevent this, we make the RMS manage evaluation messages. The RMS receives evaluation messages from the vehicles and classifies and accumulates the messages for each of the vehicles. Then, the RMS makes timestamp and signature for the other vehicles to confirm the validity of their reputation records.

B. Threat models

For the purpose of this research, we consider every vehicle as a potential adversary. In this research, the adversaries have limited capabilities and can only access the publicly available information. Also, they are limited to a normal on-board unit on a vehicle. For the RMS, we assume an honest-but-curious model that follows the given protocol correctly, but may try to obtain information from the communicated or stored data as much as possible. Based on this condition, we consider the following attacks that can be done by the adversaries.

Attacks on privacy: Generally speaking, VANET systems should consider two types of privacy, the location privacy and the identity privacy. An attacker may have interest in a vehicles location information. In a VANET system, the traffic information should be sent along with the location information for other vehicles to recognize the location where the event has occurred. Thus, an attacker can obtain the location information of the broadcasting vehicle by eavesdropping its messages. If the attacker already has the vehicles identity or can obtain it through other means, the location privacy of the vehicle owner will be seriously invaded. More seriously, the attacker can analyze the vehicles travelling pattern and predict the future location by collecting long term traffic information.

Attacks on reputation message: Generally speaking, VANET systems should consider two types of privacy, the location privacy and the identity privacy. An attacker may have interest in a vehicles location information. In a VANET system, the traffic information should be sent along with the location information for other vehicles to recognize the location where the event has occurred. Thus, an attacker can obtain the location information of the broadcasting vehicle by eavesdropping its messages. If the attacker already has the vehicles identity or can obtain it through other means, the location privacy of the vehicle owner will be seriously invaded. More seriously, the attacker can analyze the vehicles travelling pattern and predict the future location by collecting long term traffic information.

Attacks on evaluation message: After a traffic information is received, a MEV evaluates the information and generates an evaluation message. Since the evaluation message directly affects a vehicles reputation, a malicious user may try to forge that evaluation message. If an attacker broadcasted false traffic information, the attackers evaluation messages do not receive positive evaluation, hence reputation record will be lowered. In such a case, the attacker also can also try to add good evaluation messages multiple times in order to improve its reputation record.

C. Security and Privacy Goals

Based on the system and threat models, we designed a scheme that satisfies the following security and privacy goals.

Anonymity: The proposed scheme should hide the vehicles identity to preserve privacy. Vehicles broadcast traffic information and evaluation messages during operation, thus It must be impossible for an adversary to obtain the identity of the originator of a message even from a set of collected messages.

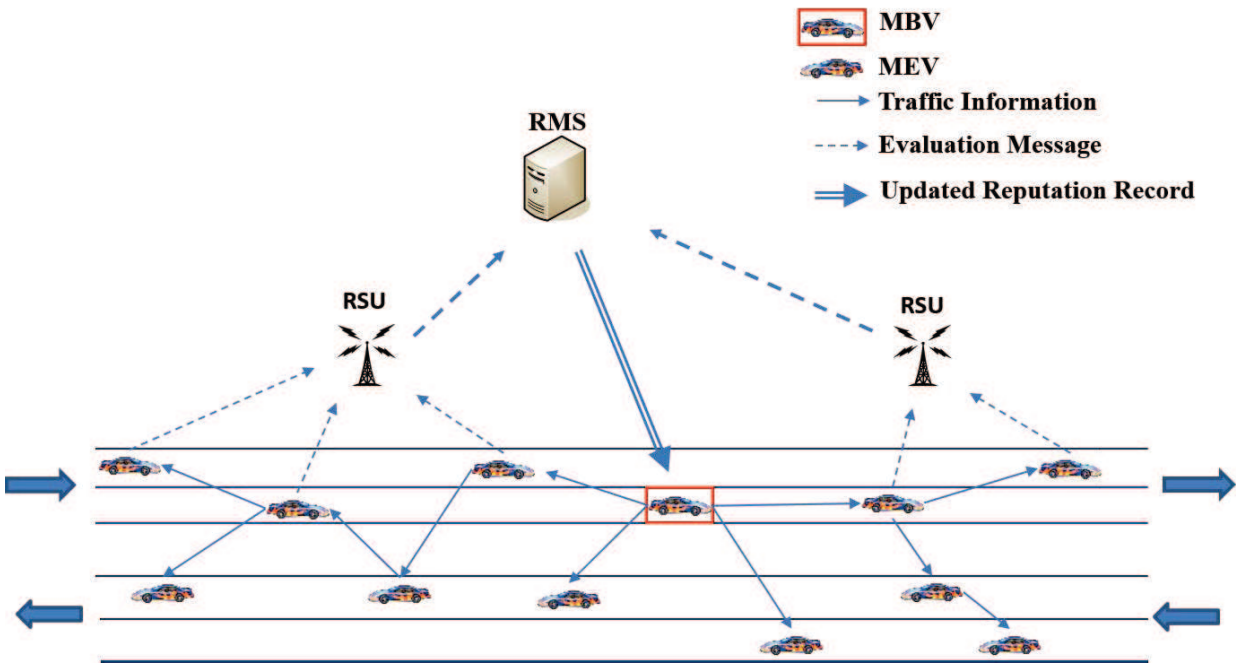

Fig. 1: System Model

Security of reputation values: When a vehicle broadcast traffic information, it must use a legitimate reputation value that is certified by the reputation server. The reputation value must be unforgeable by the vehicle or other adversaries to guarantee the reliability of traffic information.

Robustness against denial of update: An adversary vehicle may try to skip the reputation update process after sending unreliable information. Doing this, the adversary can maintain a good reputation score and keep sending the false information successfully. The reputation system must have robustness against denial of update attack.

Robustness against reply attack: An adversary vehicle may send a positive evaluation message repeatedly with the objective to increase its own reputation value. Also, an adversary may keep sending a negative evaluation message to lower the reputation value of a target vehicle. The reputation system must have robustness against the reply attack.

IV. Preliminaries

In this section, we introduce three important preliminaries used in our scheme. We also introduce the notations used in this paper as Table I.

Definition 1 (DDHP)**.** *The decisional diffie-dellman problem (DDHP) [25] states that, given g^a and g^b for uniformly and independently chosen $a, b \in \mathbb{Z}_q$, the value g^{ab} looks like a random element in $\mathbb{G}$.*

This intuitive notion is formally stated by saying that the following two probability distributions are computationally indistinguishable (in the security parameter, $n = log(q)$):

(a) (g^a, g^b, g^{ab}), where a and b are randomly and independently chosen from $\mathbb{Z}_q$.

TABLE I: Notations.

Notation	Description
q	k-bit prime number
$\mathbb{Z}_q$	Integers modulo q
$\mathbb{G}, \mathbb{G}_T$	Cyclic group with prime order q
e	Bilinear pairing that satisfies with $\mathbb{G} \times \mathbb{G}_T$
g	Generator of $\mathbb{G}$
pk, sk	Public/private key pair of RMS
UID	Unique ID of an MBV
p_i	A pseudonym as anonymous ID
R_B	A reputation value of MBV
e_i	An evaluation value of MEV
TI	Traffic information
$H(\cdot)$	A cryptographic one way hash function that satisfies $\{0,1\}^* \rightarrow \mathbb{G}$

(b) (g^a, g^b, g^c), where a, b, c are randomly and independently chosen from $\mathbb{Z}_q$.

Definition 2 (Bilinear map)**.** *A bilinear map is a map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties [26], [27].*

(a) Computable: there exists an efficiently computable algorithm for computing e,

(b) Bilinear: for all $h_1, h_2 \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p, e(h_1^a, h_2^b) = e(h_1, h_2)^{ab}$, and

(c) Nondegenerate: $e(g, g) \neq 1$, where g is a generator of $\mathbb{G}$.

Definition 3 (DBDH)**.** *The decisional bilinear diffie-hellman (DBDH) problem in groups $(\mathbb{G}, \mathbb{G}_T)$ is, given a tuple $(g, g^a, g^b, g^c, Z) \in \mathbb{G}^4 \times \mathbb{G}_T$ with unknown $a, b, c \in_R \mathbb{Z}_q$, whether $Z = e(g, g)^{abc}$. A polynomial-time algorithm $\mathcal{B}$ has advantage ϵ in solving the DBDH problem in groups $(\mathbb{G}, \mathbb{G}_T)$,*

if

$$|(Pr[(g, g^a, g^b, g^c, \mathbb{Z} = e(g,g)^{abc}) = 1] - Pr[(g, g^a, g^b, b^c, \mathbb{Z} = e(g,g)^d) = 1])| \geq \epsilon,$$

where the probability is taken over the random choices of $a, b, c, d \in \mathbb{Z}_q$*, the random choice of* g *in* $\mathbb{G}$*, and random bits consumed by* $\mathcal{B}$*.*

V. A NEW PRIVACY PRESERVING REPUTATION SYSTEM

The aim of this paper is to design a new reputation with privacy preservation. The proposed scheme must satisfy the security and privacy model as described in Section III. Our scheme is consist of the following five procedures: initialization, broadcasting traffic information, generation of evaluation messages, accumulating evaluation messages, and reputation update. Fig. 2 depicts the overall procedure of the proposed scheme.

A. Setup

On a security parameter 1^k, the setup process first determines $(q, \mathbb{G}, \mathbb{G}_T, e)$. Next, it chooses $g \in_R \mathbb{G}$, and three hash functions $H() : \{0,1\}^* \rightarrow \mathbb{G}$. The global parameters are

$$((q, \mathbb{G}, \mathbb{G}_T, e), H()).$$

Since using the public key cryptosystem for vehicles may cause invasion of privacy, we use a public/private key pair only for RMS. The RMS generates a public/private key pair (pk, sk). It picks $sk \in_R \mathbb{Z}_q$, and computes g^{sk}. The private key is sk and the public key is $pk = g^{sk}$.

Next, the RMS sets a time interval for the session. We assume that the RMS manages reputation value by the session. Every vehicle has to connect with the RMS by RSU or cellular networks and update its own reputation values at the end of the session. Since the proposed scheme focuses on cryptographic approach, we do not consider synchronization of sessions between the RMS and the vehicles. Also, length of a session is a matter of implementation and are not considered it in this paper.

B. Registration

When a vehicle joins our system, it sends a unique ID to the RMS. We assume that every vehicle has a unique ID that is used only for registration purpose. Without this registration stage, a malicious vehicle can make fake IDs to send unreliable messages. For this reason, we permit only one ID per vehicle and to ensure the privacy of vehicles, we use a pseudonym as anonymous ID. A vehicle generates a new pseudonym for each session using a pseudo random number generator. Vehicles must use different pseudonyms for each of their sessions. The different pseudonym is used to break the linkability between a vehicles information in one session to that of another session. Doing this, it will be difficult for an adversary to obtain information on a certain vehicle in another session, even if the adversary succeeded to find the pseudonym in another session. The initialization procedure is as follows.

1) The vehicle generates a temporary key t_k, picks a random number ℓ, encrypts it with the public key of RMS $t_k \cdot pk^\ell, g^\ell$.
2) The vehicle sends $E_{t_k}\{UID\}, t_k \cdot pk^\ell, g^\ell$ to RMS as meaning of joining. At this point, $E_k\{\cdot\}$ is a symmetric encryption using key k.
3) If the RMS received these messages, it checks existence and validity of the UID. If passed, the RMS decrypts $t_k = t_k \cdot pk^\ell / g^{\ell \cdot sk}$. The RMS generates a default reputation value R and signature of the reputation $\sigma_R = e(g^R, H(UID)^{sk})^{ss_i}$, where $ss_i \in \mathbb{Z}_q$ is session secret of current session, which is generated by the RMS.
4) The RMS sends $E_{t_k}\{R\}$, $E_{t_k}\{H(UID)^{sk}\}$ and $E_{t_k}\{\sigma_R\}$ to the vehicle. Note that every vehicle must perform the initialization procedure when it joins the system. A signature of reputation value has a hashed UID to prevent misuse by adversaries.

Note that the every vehicle must perform the initialization procedure when it joins to the system. A signed reputation value has a hashed UID to prevent misuse by adversaries.

C. Broadcasting Traffic Information

While a MBV drives on the road, it collects different types of information through installed sensors. This traffic information, TI, is transformed into a typical messages in VANET, and broadcasted to its neighboring vehicles. We assume that the RMS manages a session and it issues a session notification value ss_i' to verify the reputation values. For the ss_i', the RMS first picks a α, and computes $ss_i' = ss_i \cdot \alpha$. Then the RMS publish α and $g^{ss_i'}$ to all vehicles in the system. All of the vehicles in our scheme must obtain this session secret when a new session start. The traffic information verification procedure is described as follows.

1) The MBV first generates a pseudonym to preserve the privacy. The MBV computes its pseudonym p_B, and validity information V_{p_B}: $p_B = H(UID)^\gamma$, $V_{p_B} = H(UID)^{sk \cdot \gamma}$.
2) The MBV broadcasts the TI with the pseudonym, the validity information, the reputation value, and signed reputation: $p_B, V_{p_B} R$, σ_R^γ.
3) In case if a vehicle receives the TI and wants to check validity of pseudonym, it can be verified as follows:

$$e(p_B, pk) \stackrel{?}{=} e(V_{p_B}, g).$$

4) And then the receiving vehicle first checks the reliability of the TI using the reputation value R. If it is high enough, the vehicle can verify the validity of the reputation value as follows:

$$e(pk^{ss_i'}, p_B^R) \stackrel{?}{=} \sigma_R^{\gamma \cdot \alpha}$$

5) If the equation is valid, then the vehicle accepts the message, otherwise it rejects that.

Note that the correctness of the equation in the procedure 3) can be described as follows. The left side of equation can be re-written as $e(pk^{ss_i'}, H(UID)^\gamma)^R$, which is same as right side.

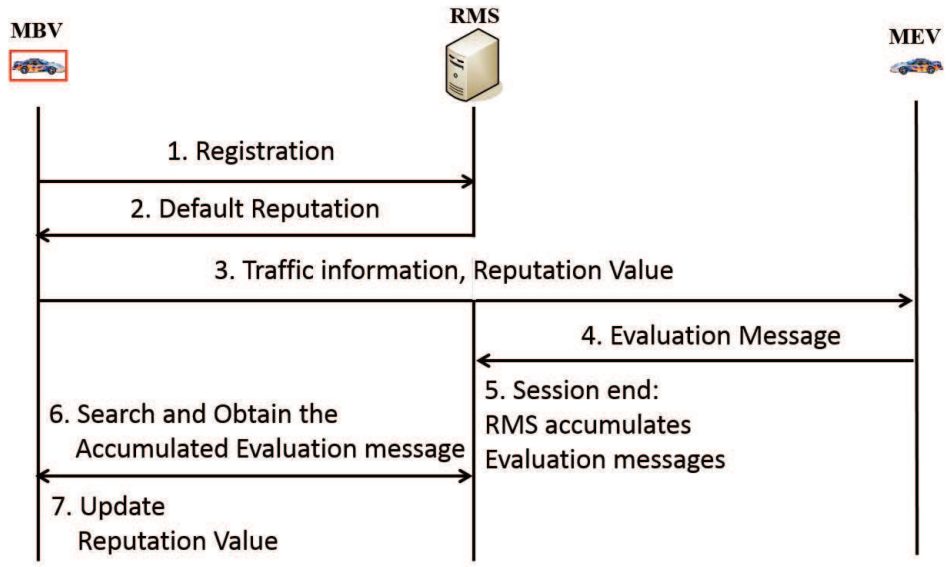

Fig. 2: The flow diagram of the proposed scheme

D. Generation of Evaluation Messages

If a MEV who uses p_V as a pseudonym wants to send feedback of a receiving information, the p_V computes and sends an evaluation message to the RMS. The evaluation message can be computed as follows.

1) The MEV generates a evaluation message $e_v \in \{0, 1\}$, which represents only binary number for simplicity. The MEV sets $e_v = 1$ in case if the information was reliable, and $e_v = 0$ in case if the information was unreliable.
2) The MEV computes $H(p_B||e_v)$ for the integrity and sends $p_V, p_B, e_v, H(p_B||e_v)$ with its reputation value to the RMS.
3) The RMS checks validity of the evaluation message. The verification procedure is the same as that of the verifying a reputation value procedure. If it is valid, the RMS accepts the evaluation value, otherwise it rejects that.

In this procedure, the RMS accepts and stores the evaluation messages for the current session only and that can be verified by the session notification value. In addition, a repeated evaluation message will be determined easily due to the reputation value of MEVs.

E. Accumulating Evaluation Messages

After a session is completed, the RMS accumulates the evaluation messages. An important issue is knowing which entity has the role of accumulating the evaluation messages. If a vehicle performs the procedure, it is easy to forge the evaluation message and deny updates. On the other hand, if the RMS performs the procedure and sends it to every vehicles, it is hard to preserve the privacy of vehicles. To solve this problem, in our proposed scheme the RMS performs accumulating procedure and posts the result on the server. Then, vehicles connect to the server and obtain the evaluation result. The RMS can accumulate the evaluation messages as follows.

1) When an evaluation message from a vehicle p_E is received by the RMS, the RMS can check validity of its pseudonym as follows: $e(p_E, pk) \stackrel{?}{=} e(V_{p_E}, g)$.
2) The RMS sorts the evaluation messages by p_B
3) Then, the RMS accumulates the evaluation messages given for the pseudonym p_B: $M_{p_B} = \sum_{i=1}^{n} e_v$, where n is the number of evaluation messages for the p_B.
4) The RMS picks $\alpha_{i+1} \in_R \mathbb{G}$, generates a new secret ss_{i+1} for next session, $ss_{i+1} = ss_i + \beta$, and computes $\sigma_M = e(g, p_B)^{M_{p_B} \cdot ss_{i+1}}$
5) Finally, the RMS post $p_B, M_{p_B}, \beta, \sigma_M$ on the server.

In this procedure, the RMS must post an accumulated evaluation message for all vehicles even for the cases where no information is assigned.

A vehicle without a signature of a reputation value cannot pass the reputation verification process, therefore, we assume that all vehicles would send an evaluation message themselves. At the same time, we use this feature to revoke vehicles. In such a case, if a vehicle receives a very low evaluation, the RMS can revoke the vehicle by skipping its accumulation process.

F. Reputation Update

In our scheme, all vehicles are forced to update their reputation value by themselves. Otherwise, the session secret of the reputation verification message is not updated which consequently will result in the failure of the verification process from MEVs. In such a case, they have to search their accumulated evaluation message using a pseudonym they have

used in the previous session. Once found, the MEV can update the reputation value as follows:

$$\begin{aligned} R' &= R + M_{p_B}, \\ \sigma_{R'} &= \sigma_R^{\gamma \cdot \beta} \cdot \sigma_M \\ &= e(g, H(UID)^{sk\gamma})^{ss_i \cdot \beta} \cdot e(g, H(UID)^{sk\gamma})^{ss_{i+1} \cdot M_{p_B}} \\ &= e(g, H(UID)^{sk\gamma})^{ss_{i+1} \cdot (R + M_{p_B})} \\ &= e(g, H(UID)^{sk\gamma})^{ss_{i+1} \cdot R'} \end{aligned}$$

The RMS can rule out a vehicle that did not update its reputation value by issuing a new session notification value ss_{i+1}, which was described in Section V.C. A new pseudonym for next session, the MBV picks a random secret $\gamma' \in_R \mathbb{G}$ and computes $H(UID)^{sk \cdot \gamma'}$. The new pseudonym p'_B will be $H(UID)^{sk \cdot \gamma'}$.

VI. Analysis

In this section, we analyze the security and privacy of our scheme in the presence of adversaries and attacks as they were defined in Section III. III.

A. Anonymity

Claim 1: The pseudonym-based communication proposed in this paper provides anonymity.

Proof. Vehicles in our scheme generate and use a pseudonym as anonymous IDs. The pseudonym, which is represented as $H(UID)^{sk \cdot \gamma}$, can be divided into two parts, where the first part is $H(UID)^{sk}$ and second is a random number γ. To obtain any of two values, an attacker needs to solve a discrete logarithm which is well-known unsolvable polynomial time problem. Thus, it is very hard for attackers to obtain $H(UID)$s or random numbers associated with that pseudonym. In addition, assuming that the random numbers are uniformly and independently chosen from $\mathbb{Z}_q$. The value $H(UID)^{sk}$ can be rewritten as $g^{a \cdot sk}$, where g is a generator of $\mathbb{G}$, hence the $g^{a \cdot sk}$ is another generator of $\mathbb{G}$. This guarantees that the pseudonyms that are represented as $\hat{g}_1^{\gamma}, \hat{g}_2^{\gamma}, \ldots$ has polynomial-time indistinguishability under the DDHP This means that the attackers cannot obtain a relation between the pseudonyms.

A vehicle in our scheme uses one pseudonym per session. If the time period of a session is short, our scheme can provide better privacy, but this creates an overhead for updating the reputation values at the RMS as well as on vehicles. On the other hand, a longer session provides a worse privacy. Therefore, our scheme has a tradeoff between privacy and efficiency and finding the most appropriate time period is critically important. □

Claim 2: An attacker cannot reveal an identity of target vehicle from a set of pseudonyms.

Proof. To obtain an identity from communication channels, the best thing that an attacker can do is to obtain the $E_{t_k}\{UID\}$ at the initialization phase, and cryptanalyzes it to get the UID. Otherwise, the attacker should obtain $H(UID)$ from a signature of reputation value, and obtain UID by cryptanalyzing it. We assume that the attacker has similar level of computing ability as a normal vehicle. Usually, the vehicle's computation resource is not sufficient to cryptanalyze the symmetric encryption such as AES and one way hash functions. Therefore, it is computationally difficult to obtain an identity from pseudonyms or other messages. □

B. Robustness against Reputation Value Fraud

Claim: The reputation value in our system is unforgeable.

Proof. The aim of this type of attack is improving the attackers reputation value which might have been devalued after sending unreliable information. To improve the reputation value, an attacker can engage in any of following strategies:

1) The attacker merges accumulated evaluation messages repeatedly at the reputation update phase. In this case, the reputation value may increase. However, this attack will fail at the verification process of the broadcasting traffic information phase due to the signature of reputation messages.
2) The attacker uses the reputation value of other vehicles. This attack will be blocked after a new session started. The attacker cannot obtain the UID or $H(UID)$ of other vehicles, thus it will fail at the reputation update phase and discarded by receiving vehicles.
3) The attacker uses the accumulated evaluation value of other vehicles to improve its reputation value. Every signature of reputation value has $H(UID)$ for other users to prevent attacks on the reputation value. Similar to the previous attempt, this attack will fail at the reputation update phase and discarded by receiving vehicles.

□

This ensures that our scheme has robustness against fraudulent and plausible reputation value attacks.

C. Robustness against Denial of Update

Claim: Our scheme can revoke an attacker who has avoided the reputation update procedure.

Proof. As the aforementioned revocation strategy, a reputation value which has not been updated cannot pass the verification process of the broadcasting traffic information phase. To pass the verification process, the attacker needs to forge the signature of reputation value, which is already verified in the previous proof. Hence, our scheme has robustness against denial of update attack. □

D. Robustness against Reply Attack

Claim: The proposed scheme has robust against evaluation message reply attack, which is to improve the reputation value of an attacker.

Proof. In the proposed scheme, the procedure of sending evaluation messages also checks the reputation of the originating vehicle. A valid evaluation message which has passed the verification process should be stored at the RMS with

its reputation value. When the RMS performs sorting to accumulate the messages after a session is completed, the replied messages can be detected by the RMS. Also, it is possible that the RMS assigns a penalty to the violators. □

VII. Conclusion

This paper proposed a new reputation-based message reliability system which can preserve the privacy of vehicles in VANETs. In order to preserve vehicles privacy, we designed a cryptographic scheme in which the VNET vehicles use a pseudonym as anonymous ID and a new pseudonym for each of their sessions. To make an unforgeable and undeniable system, we proposed a centralized server to manage the overall reputation system. For each session, the RMS issues a session notification value and to deny updating a reputation value, the session-based management makes an adversary difficult. Evaluation messages sent by MEVs is accumulated by the RMS which has the job of accumulating it to the evaluation message. The evaluation message will be used to update a vehicles reputation value. A vehicle that did not perform the update process cannot pass the reputation verification process, which means that our scheme can figure out an unauthorized vehicles access. In addition, we also proved our schemes robustness against plausible attacks while helping to determine whether a receiving message is reliable or not.

Acknowledgment

This research was supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2015R1D1A1A09058200). This research was also supported in part by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. B0717-16-0132, Making the Smart Wearable Devices Secure).

References

[1] X. Guan, Y. Huang, Z. Cai, and T. Ohtsuki, "Intersection-based Forwarding Protocol for Vehicular Ad Hoc Networks," *Telecommunication Systems*, vol. 62, no. 1, pp. 67-76, May 2015.

[2] Y. Huang, M. Chen, Z. Cai, X. Guan, T. Ohtsuki, and Y. Zhang, "Capacity Analysis for Urban Vehicular Ad Hoc Networks with Graph-Theory Based Construction,"*in Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-5, 2015.

[3] X. Wang, L. Guo, C. Ai, J. Li, and Z. Cai, "An Urban Area-Oriented Traffic Information Query Strategy in VANETs," *in Proceedings of the 8th International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, pp. 313-324, 2013.

[4] Y. Huang, X. Guan, Z. Cai, and T. Ohtsuki, "Multicast Capacity Analysis for Social-Proximity Urban Bus-Assisted VANETs," *in Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, pp. 6138-6142, 2013.

[5] F. Terroso-Saenz, M. Valdes-Velda, C. Solomayor-Martinez, and R. Toledo-Moreo, "A Cooperative Approach to Traffic Congestion Detection with Complex Envent Processing and VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 2, pp. 914-929, Feb. 2012.

[6] F. Bai and B. Krishnamachari, "Exploiting the Wisdom of the Crowd: Localized, Distributed Information-Centric VANETs," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 138-146, May 2010.

[7] B. Fleming, "An Overview of Advnaces in Automotive Electronics," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 4-9, Mar. 2014.

[8] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510-524, Aug. 2012.

[9] J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938-948, Apr. 2015.

[10] B. Amro, Y. Saygin, and A. Levi, "Enhancing Privacy in Collaborative Traffic-Monitoring Systems using Autonomous Location Update," *IET Intelligent Transport Systems*, vol. 7, no. 4, pp. 388-395, Dec. 2013.

[11] M. Li, H. Zhu, Z. Gao, S. Chen, L. Yu, S. Hu, and K. Ren, "All Your Location are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking," *in Proceeings of the 15th ACM Internation Symposium on Mobile Ad Hoc Networking and Computing*, pp. 43-52, 2014.

[12] L. Chen, S. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," *IEEE Journal of Selected Area Communications*, vol. 29, no. 3, pp. 605-615, Mar. 2011.

[13] V. Daza, J. Domingo-Ferrer, F. Seb, and A. Viejo, "Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876-1886, May 2009.

[14] G. Kounga, T. Walter, and S. Lachmund, "Providing Reliability of Anonymous Information in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2977-2989, Jul. 2009.

[15] M. Raya, A. Aziz, and J. Hubaux, "Efficient Secure Aggregation in VANETs," *in Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, pp. 67-75, 2006.

[16] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559-573, Feb. 2010.

[17] 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 Communication Magazine*, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[18] P. Golle, D. H. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," *in Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 29-37, 2004.

[19] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks," *in Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems-Workshops*, pp. 1-8, 2006.

[20] F. Dotzer, L. Fischer, and P. Magiera, "VARS: A Vehicle Ad Hoc Network Reputation System," *in Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, pp. 454-456, 2005.

[21] U. Minhas, J. Zhang, T. tran, and R. Cohen, "Towards Expanded Trust Management for Agents in Vehicular Ad Hoc Networks," *International Journal of Computational Intelligence: Theory and Practice*, vol. 5, no. 1, pp. 3-15, 2010.

[22] R. Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer, "Vehicle Behavior Analysis to Enhace Security in VANETs," *in Proceedings of the 4th IEEE Workshop on Vehicle-to-Vehicle Communications*, pp. 1-8, 2008.

[23] Q. Li, A. Malip, K. M. Martin, S. L. Ng, and J. Zhang, "A Reputation-Based Announcement Scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095-4108, Nov. 2012.

[24] L. Chen, Q. Li, K. M. Martin, and S. L. Ng, "A Privacy-Aware Reputation-Based Announcement Scheme for VANETs," *in Proceedings of the 5th International Symposium on Wireless Vehicular Communications*, pp. 1-5, 2013.

[25] D. Boneh, "The Decision Diffie-Hellman Problem," in *Proceedings of the 3rd Algorithmic Number Theory Symposium. Lecture Notes in Computer Science*, vol. 1423, pp. 48-63, 1998.

[26] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," in *Proceedings of the 7th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT)*, pp. 514-532, 2001.

[27] Hazewinkel, Michiel, "Bilinear Mapping," *Encyclopedia of Mathematics, Springer*, 2001.