Long-term Reputation System for Vehicular Networking based on Vehicle's Daily Commute Routine

Soyoung Park*, Baber Aslam[§], Cliff C. Zou[§]
*Dept. of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea
[§]Dept. of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL, USA

***Abstract*—A vehicular network must ensure a trust relationship among participating "smart vehicles" (vehicles installed with wireless network devices) and roadside infrastructure in order to maximize the benefit provided by the network. In this paper, we present practical ways to provide reliable reputation scores for vehicles in a vehicular network. Because in most of the time, the majority of people drive their vehicles locally for their daily commute (to work places, schools, daycares, superstores, etc), most vehicles have their predefined constant daily trajectories. Based on this phenomenon, roadside infrastructure could rely on repeated daily observations of the same set of passing-by vehicles to build long-term reputation scores for these local "community" vehicles, in the similar way as the reputation built-up for people in a club or a church community. The proposed scheme does not require sufficient density of smart vehicles and only requires each smart vehicle has one secret and verifiable certificate. These features make it especially suitable for the initial deployment stage of vehicular network when the penetration rate of smart vehicles is very low and vehicle-based public-key infrastructure is not mature.**

***Keywords*—vehicular networking security, reputation system, initial deployment stage, roadside unit**

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a form of mobile ad-hoc network to provide communications among nearby vehicles and between vehicles and nearby roadside equipments [1]. Applications of VANET include emergency/safety warning, driving directions, cooperative driving, information exchange between nodes/vehicles, access to Internet, location aware advertising, on demand content, file sharing, etc [2][3]. For the success of all these applications, it is critical to ensure that VANET can provide reliable and secure data transmission, and full cooperation from all or most vehicles.

Most previously proposed VANET architectures and applications (including security architectures) have an implicit assumption that there are sufficient number of vehicles equipped with wireless devices (called "smart vehicles") on roads when a proposed architecture is deployed. Under this assumption, in most of the time VANET can rely on Vehicle-to-Vehicle (V2V) communication and multi-hop communication to achieve its functions and service.

This assumption, however, is not a realistic assumption during the long initial years of VANET deployment. Due to the huge population of existing non-smart vehicles and the long lifetime of vehicles, it will take years or even decades transition period before we could have a mature VANET environment where most vehicles are smart vehciles. Thus instead of focusing on mature VANET scenarios, it is more important to develop economical and feasible architectures that are suitable for VANET initial deployment stage.

Vehicular network is a special form of Mobile Ad Hoc Network (MANET). Researchers have long studied how to ensure honest and active participation of all mobile nodes in a MANET, and how to detect and control malicious or selfish nodes. "Reputation system" is the general term describing such a mechanism or architecture. Many reputation strategies have been proposed in the last decade. Ref. [4, 5] introduced a reputation system in peer-to-peer (P2P) networks in order to establish a trust relationship, and to encourage the cooperation, among peer nodes. Ref. [6] has introduced a method for evaluating the credibility of recommenders. Ref. [7] has suggested a method to make selfish nodes try to cooperate for correcting the error instead of going into a retaliation situation. Ref. [8] has proposed a trust establishment scheme for reliable data propagation over multi-hop routing. X. Wu el al. has recently proposed a group-based reputation system [9] for mobile P2P systems where peers with similar mobility are clustered into a group. To provide incentive for better cooperative nodes, hybrid schemes [10, 11] presented a reputation scheme based on a pricing-based model, which treats packet forwarding as a service that can be priced. Ref. [12] has proposed an instant observation based message transmission scheme for VANET. In most reputation systems, the behavior of each node is measured and reported by its neighbors, and its reputation score is calculated and maintained by all cooperative neighbors.

Considering the low density of smart vehicles during VANET initial deployment stage, this neighborhood-based reputation system design would not work anymore because a smart vehicle normally does not have any neighboring smart vehicles around it in most of the time. Facing this challenge, in this paper we present a novel reputation system based on the support from sparsely distributed RoadSide Units (RSUs) without relying on neighboring smart vehicles. The proposed reputation system exploits the fact that in most of the time, the majority of people drive their vehicles locally for their daily commute (to work places, schools, daycares, superstores, etc), and hence, most vehicles have their predefined constant daily trajectories. Among all smart vehicles passing by a roadside unit, a substantial fraction of them will be observed by the RSU repeatedly with daily frequency. From the perspective of an RSU, the daily commute vehicles passing through it form a relatively stable "virtual community". It is convenient and

feasible to let the RSU take charge of managing the long-term reputation scores for these commute vehicles, in the similar way as the reputation built-up for people in a club or a church community.

This proposed scheme does not require a sufficient density of smart vehicles on the roads to enable vehicle-to-vehicle multi-node communication, and it only requires each smart vehicle has one secret and verifiable certificate. These features make the proposed system especially suitable for the initial deployment stage of vehicular network when the penetration of smart vehicles is low and vehicle-based public-key infrastructure is not mature.

The paper is organized as follows. Section II introduces the VANET environment we are considering and some notations we use in the paper. In Section III, we present the proposed reputation system architecture, and then describe the detailed designs in Section IV. In Section V we discuss security attributes and finally conclude the paper in Section VI and also discuss some future work on this research topic.

II. System Model

A. VANET environment description

Our research focuses on the unique environment of the initial deployment stage of VANET. This critical transition period imposes many challenges to VANET design due to the lack of infrastructure, smart vehicles, and networking technology support. The VANET environment under consideration has the following features or assumptions:

- Vehicle-based public-key infrastructure exists but not mature, i.e., although each smart vehicle could have its own digital certificate, issuance, revocation, and management of each vehicle's certificate for the huge number dynamically-located smart vehicles are not likely to be built up in the initial deployment stage.
- Smart vehicles are equipped with on-board unit (OBU) for networking and computing. Additionally, they have GPS system for location detection and a digital map.
- RSUs along roads have their certificates. Due to their static locations and limited population, RSUs could have certificates that can be easily managed by local government or agency.
- Density of smart vehicles on roads is very low. In most time it is impossible to have multi-hop V2V communication. The dominant communication forms between a vehicle and an RSU, or between two vehicles that pass by each other in opposite direction of a road.

B. Notations and Function Definition

We define several notations and functions that we will use in formal description of our architecture.

Each vehicle V has its own unique identification ID_V, which is kept in secret and known only by the local authority such as local department of transportation. ID_V could be composed by, for example, the vehicle's license plate number plus registered driver's driver license number, or a unique random number assigned to the on-board wireless unit of the vehicle. The identification information could be installed in the vehicle's OBU by the local department of transportation when the driver registers her car by carrying the OBU device to the office. ID_V could be signed and encrypted by department of transportation so that when it is transmitted to an RSU, the RSU could verify the integrity of the ID without exposing the vehicle's private information.

A vehicle OBU could generate public/private key pairs. Denote V^+ as the public key and V^- as the private key of vehicle V. On the other hand, with public key R^+ and private key R^-, an RSU R has its digital certificate denoted by $Cert_R$.

We denote $Cert_{RA,V}$ as the "reputation certificate" for vehicle V, which contains the reputation score of vehicle V, signed by its "Agent RSU" R_A, which takes charge of managing the reputation score of this specific vehicle. The reputation score of vehicle V is denoted by S_V. $K(m)$ represents a general encryption function on message m using key K. If the reputation certificate of vehicle V only contains the reputation score S_V, then $Cert_{RA,V} = R_A^-(S_V)$. In addition, we define $Hash(m)$ as the hash value generated by applying a well-known hash function (such as MD5) on message m.

Because public-key cryptography is computational expensive, people do not directly use public/private key to do encryption of the actual large-size message. When using public key R^+ to encrypt a message m, the actual operation is to generate $<R^+(K), K(m)>$ where K is a randomly-generated symmetric session key; when using R^- to encrypt, the actual operation is to generate $<R^-(Hash(m)), m>$. In the rest of the paper we will simply use $R^+(m)$ and $R^-(m)$ to represent the actual encryption by public key and private key, respectively.

III. Proposed Architectures

The proposed reputation system relies on the support from roadside infrastructure. Considering the long initial deployment stage of VANET, we believe it is practical to consider two possible roadside unit infrastructures: the early stage of roadside infrastructure with RSUs that have no Internet access, and the later stage of roadside infrastructure with RSUs that all of them have Internet access.

At the very early stage of VANET deployment when there is no profit return, expenditure is the first concern in setting up roadside infrastructure. In the near future, cellular-based Internet access is still expensive. Therefore, it could be too expensive to provide Internet access, either through cellular network or wired links, to every roadside unit along roads, especially for RSUs in rural areas or along highways. For this reason, we believe the first generation of roadside infrastructure would be composed by cheap standalone boxes installed along the roads without any Internet access.

In the later phase of VANET initial deployment stage, as more people use VANET service and as the Internet access (such as wireless wide area access) becomes much economical, RSUs will be eventually upgraded to have Internet access in order to provide more efficient and rich services. In the following, we propose the corresponding reputation systems based on the above two roadside architectures, respectively.

A. Reputation System based on Isolated RSUs

We first introduce the reputation system design with the support from RSUs that do not have Internet access. In this case, RSUs have to rely on mobile vehicles to pass messages to each other, i.e., using moving smart vehicles to carry and forward messages between RSUs.

This format of communication is usually called "delay tolerant network" (DTN) [13]. Many researchers have studied routing and networking algorithms for DTN based on "store and forward" approach, such as [14, 15]. Therefore, we will not discuss how mobile vehicles carry and forward messages between RSUs in this paper. The major challenge of DTN is that message transmission time between two nodes is usually much longer than traditional network and greatly varies. However, this feature of communication is perfectly appropriate for our proposed reputation system since we rely on the long-term reputation values, not the short-term reputation scores, to build up our reputation system.

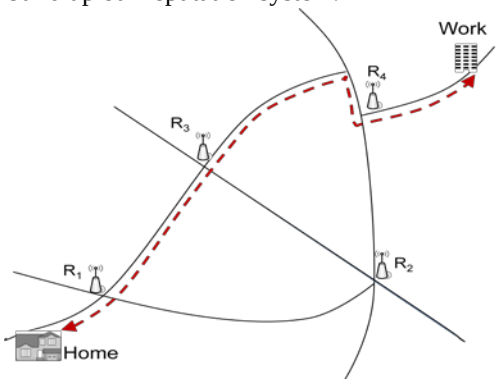

Fig. 1: Illustration of proposed reputation system. A vehicle has a constant daily commute route (the red dashed line) between home and work place, passing through RSUs R_1, R_3, R_4. One of these three RSUs will be designated as Agent RSU and the other two RSUs will keep monitoring the vehicle's daily behavior and feedback reputation update messages to the Agent RSU.

1) Architecture: Since RSUs cannot quickly communicate with each other due to the lack of Internet access, the reputation system has to be built in distributed way. Fig. 1 illustrates the reputation system architecture. For the specific vehicle commuting between home and work place shown in this figure, it is assigned to one of the three RSUs along its commute route (R_1, R_3, R_4) to be its "representative agent", which is called "Agent RSU". The Agent RSU takes charge of managing the reputation score of this specific vehicle. Which RSU is assigned as the Agent RSU for a vehicle can be either determined by the vehicle, or assigned by the RSU system.

An Agent RSU provides the reputation certificate that can be used by its represented vehicle—no other RSU in the same reputation administrative region will provide reputation certificate to this vehicle anymore. In this way, each vehicle will have one and only one RSU to manage its reputation score and issuance of reputation certificate. All other RSUs on the commute route could monitor the vehicle's behavior and provide reputation update messages to the Agent RSU.

Under this design, we have to make sure that each vehicle could have one and only one RSU as its Agent RSU in the same reputation administrative region (we will discuss more about cooperation across multiple reputation administrative regions in Section IV.C). Otherwise, a vehicle may conduct Sybil attack by designating multiple RSUs as its Agent RSUs to obtain multiple valid reputation certificates. To achieve this design objective, a vehicle needs to use its unique identification ID_V when registering itself to its Agent RSU. ID_V is secret and unknown to other vehicles, but can be verified by the RSU system. Once an RSU becomes the Agent RSU for vehicle V, it will broadcast a message to all RSUs in the local area to make sure that no other RSU will become Agent RSU for the same vehicle.

Because each vehicle has one and only one verifiable and secret ID_V, it cannot conduct Sybil attack by advertising different ID_V at different routes.

2) *Designating Agent RSU:* At the beginning, when vehicle V decides to use RSU R_A on its commute route as its Agent RSU, it communicates with the RSU R_A when passing through it as follows:

$V \rightarrow R_A$:	1.	Request to use the RSU as its Agent RSU
$R_A \rightarrow V$:	2.	$Cert_{R_A}$, which can be verified by V and V obtains R_A^+
$V \rightarrow R_A$:	3.	$R_A^+(ID_V, V^+)$
R_A:	4.	Verify that ID_V has no other Agent RSU in the same reputation administrative region
$R_A \rightarrow V$:	5.	$Cert_{R_A,V} = R_A^-(S_V, V^+)$, where initial reputation score S_V has its default value
$R_A \rightarrow$ other RSUs:	6.	$<R_A^-(Hash(ID_V)), Cert_{R_A}>$

Fig. 2: Procedure of assigning Agent RSU

In step 6, the Agent RSU broadcasts its agent role of vehicle V to every RSU in the same reputation administrative region. To protect the privacy and secrecy of a vehicle's ID_V from knowing by the other RSUs or other vehicles, the broadcast message only contains the hash value of ID_V. In this way, without knowing the vehicle's real ID, the other RSUs can easily verify (step 4) whether or not the same vehicle requests for Agent RSU again in the future.

In step 5 of the procedure, the reputation certificate $Cert_{R_A,V}$ contains vehicle V's self-generated public key V^+. In this way, if another vehicle eavesdrops $Cert_{R_A,V}$, it cannot use this reputation certificate since it does not have the corresponding private key V^- for message encryption.

The broadcast in step 6 could generate many messages if the reputation system in a region covers a large number of RSUs. However, since this broadcast is activated only once for each vehicle, in the long run step 6 will not put too much burden in the vehicular network.

3) *Reputation certificate update:* Every time when vehicle V passes its Agent RSU R_A, it will obtain its updated reputation certificate from RSU R_A. Suppose $Cert_{R_A,V} = R_A^-(S_V, V^+)$ represents the reputation certificate before the update, $Cert'_{R_A,V} = R_A^-(S'_V, V_n^+)$ represents the one after update. The reputation certificate update procedure is as follows:

$V \rightarrow R_A$:	1.	$<V^-(R_A^+(ID_V, V_n^+)), Cert_{R_A,V}>$
$R_A \rightarrow V$:	2.	$Cert'_{R_A,V} = R_A^-(S'_V, V_n^+)$

Fig. 3: Obtaining updated reputation certificate from Agent RSU

In step 1, vehicle V provides a new and different public key V_n^+ to be used in the new reputation certificate. In this way, a vehicle uses different encryption keys in communicating with other vehicles in different days, and hence, prevents being tracked by attackers over a long time. In addition, the first encryption using R_A^+ on (ID_V, V_n^+) is to keep the real identity ID_V confidential to Agent RSU. The second encryption using V^- is to make sure that only the real vehicle V with the correct previous reputation certificate $Cert_{RA,V}$ can send this request.

Containing $Cert_{RA,V}$ in the step 1 request can also prevent possible replay attack. If the request message in step 1 is replayed by an attacker after the real request from the vehicle V, the Agent RSU can easily know that the previous reputation certificate $Cert_{RA,V}$ in the request message is not up-to-date based on its database records.

4) *Reputation update message*: In the reputation system, all non-Agent RSUs along a vehicle's commute route will continue monitoring this vehicle's daily behavior. For example, they can observe whether this vehicle help the VANET by relaying messages between RSUs, whether the vehicle provides correct alert messages to RSU system about road congestion and accidents. With this daily monitoring, each non-Agent RSU could provide valuable reputation update messages to the vehicle's Agent RSU. Suppose RSU R_1 sends a reputation update message m to the vehicle's Agent RSU R_A, the message will have the following format:

$R_1 \rightarrow R_A$: $< Cert_{R1}, R_1^-(R_A^+(m)) >$

Since the message needs to be carried and forwarded by mobile vehicles, encrypting the message m first with R_A^+ will ensure that any relaying vehicle cannot read the reputation update message. To identify which vehicle this update message m is about, the message m contains the vehicle's reputation certificate $Cert_{RA,V}$, or its public key V^+. The vehicle's Agent RSU keeps a record of each registered vehicle's past public keys or reputation certificates.

5) *Use of reputation certificate*: Equipped with a valid reputation certificate $Cert_{RA,V} = R_A^-(S_V, V_1^+)$, a vehicle V_1 could send a message m to a neighboring vehicle V_2 (or an RSU along its route) in the following format:

$V_1 \rightarrow V_2$: $< V_1^-(m), Cert_{RA,V}, Cert_{RA} >$

The recipient vehicle V_2 could use the Agent RSU's certificate $Cert_{RA}$ to verify and obtain the sender's reputation score S_V and the sender's public key V_1^+ from $Cert_{RA,V}$, then use the public key V_1^+ to decrypt and obtain the message m. The recipient could determine whether to trust the received message m based on the sender's reputation score S_V.

B. Reputation System based on Internet-Accessible RSUs

We then introduce reputation system design for the scenario where all RSUs have Internet access. In this case, RSUs can quickly communicate with each other via Internet to exchange traffic information and vehicle's reputation update messages.

With this better roadside infrastructure support, the reputation system could be designed in a simpler way. It does not matter much whether the actual reputation system is managed in centralized way or distributed way. This is because, from the perspective of each vehicle, all RSUs and the Internet form a single virtual entity for information gathering and reputation management.

For this reason, we do not need to designate an Agent RSU for each vehicle. A vehicle could obtain its updated reputation certificate via any RSU. The reputation certificate update and the use of reputation certificate will follow the similar procedures as introduced in previous section A, and hence, we will not repeat the description again.

IV. System Designs

In this section, we introduce the detailed system design and how the system deals with a few identified challenges.

A. Reputation Score Computation

A vehicle's reputation score should be updated based on the vehicle's daily behavior and contribution to the whole VANET, such as whether the vehicle helps RSUs to pass data to other RSUs, whether it reports congestion or accident information to RSUs accurately, whether it cooperate with other vehicles in relaying messages, etc.

Reputation score S_V for vehicle V should be updated daily as:

$$S_V = S_V + 1 + C_V - D_V \quad (1)$$

where C_V represents the combined contribution of this vehicle to the VANET system in a day; D_V represents the combined negative impact of this vehicle. The values of contribution or negative impact are calculated based on the reputation update messages reported from all RSUs in the region.

Contribution of a vehicle could include: reporting congestions or accidents to RSUs, relaying messages between RSUs, relaying messages generated by RSUs to any vehicle it passes, etc. Negative impact includes both selfish behaviors, such as dropping relaying messages, not answering queries from RSUs or other vehicles, and malicious behaviors such as generating false alerts (how to detect selfish or malicious behaviors is out of the scope of this paper). How much weight given to each behavior in updating reputation score is determined by the actual application and design objectives.

The addition of 1 in the S_V update is because we should trust a vehicle more as long as it does not show any negative behavior. Similar to the people's relationship in a real world community, if a vehicle does not exhibit bad behavior in a time period, it will be less likely to generate malicious activities in the future.

B. Incentive Mechanism for Vehicular Participation

In order to encourage contribution and cooperation from all vehicles, an incentive mechanism is required to make the reputation system successful. A straightforward way is to provide financial benefit and service preference to vehicles that have better reputation scores. For example, the reputation system could be linked with toll-road payment system, and give more discount to vehicles with higher reputation scores. If vehicles rely on RSUs to access Internet, RSUs could allocate access bandwidth in proportion to vehicles' reputation scores.

C. Inter-Community Cooperation

In the initial deployment stage, VANET management will have a long transition period as well. At the beginning, each local county or town government may invest and set up VANET infrastructure and management system covering its own county or town region. Then as time goes on, the management region will gradually expand to either cover more geographical areas, or merge with neighborhood regions to form a larger VANET network.

Therefore, if a vehicle has a long daily commute route, which is true for a substantial fraction of commuters, at the very beginning time of VANET deployment stage, the vehicle may traverse through multiple VANET administrative regions, as illustrated in Fig. 4. Each region will have its own management and reputation system. Therefore, a vehicle may have multiple reputation scores; each one is generated and certified by one administrative region.

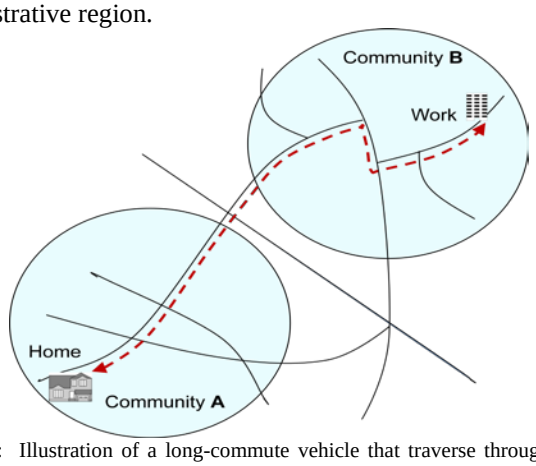

Fig. 4: Illustration of a long-commute vehicle that traverse through two VANET administrative regions. The vehicle could have two reputation scores managed by community A and B, respectively. The two administrative regions could cooperate in order to achieve a more accurate reputation measurement.

In order to have a better reputation measurement and management, neighboring VANET regions could cooperate with each other in updating reputation scores for their commute vehicles. For the environment where RSUs have no Internet access, the two Agent RSUs of a vehicle in Community A and B (illustrated in Fig. 4) could exchange their reputation scores of the vehicle. Suppose a vehicle's reputation scores in Community A and B are $S_{V,A}$ and $S_{V,B}$, respectively. The Agent RSU in Community A could update its reputation score $S_{V,A}$ based on the received $S_{V,B}$ from Community B as follows:

$$S_{V,A} = (1-\alpha)\, S_{V,A} + \alpha\, S_{V,B} \quad (2)$$

where α is the trust weight on the reputation score reported by the neighboring region, $0 \le \alpha \le 0.5$. If community A trusts more of the feedback from community B, α will become bigger. In addition, to realize the collaborations and authentications between RSUs among multiple regions, these regions should either share a common Certificate Authority, or have exchanged their RSUs' certificates beforehand.

D. Outside Vehicles

The proposed reputation system is based on local commute vehicles in their commute region. Besides these local commute vehicles, some outside vehicles will travel through a region from time to time. We can classify these outside vehicles into two classes:

- Have reputation certificates issued by their own commute regions and their commute regions have collaboration with the current region
- Have no verifiable reputation certificates

For the first class of vehicles, the current region could temporarily rely on the guest reputation certificate to determine a vehicle's reputation. In addition, any reputation update message generated by RSUs in this region could be forwarded to the vehicle's Agent RSU in its original region for reputation update.

For the second class of vehicles, a vehicle will have no credential and thus it can be treated with the default reputation score of a newcomer. The current region will not manage or keep any record for this vehicle since it may not traverse through the region again.

E. Commute Vehicles Using Alternative Route

Until now we have assumed that each commute vehicle has its predefined commute route; thus it passes through its Agent RSU each day and can obtain updated reputation certificate daily. However, from time to time, a commute vehicle may use alternative routes for its daily commute, or does not make the daily commute for several days. In this case, the vehicle cannot obtain updated reputation certificate daily from its Agent RSU.

For this reason, a reputation certificate should have a validation time, denoted by T_{valid}, that is longer than one or two days. Suppose vehicle V obtains its reputation certificate $Cert_{R_A,V}$ from its Agent RSU R_A at time T_{issue}, the reputation certificate should have the following format:

$$Cert_{R_A,V} = R_A^{-}(S_V, V^{+}, T_{valid}, T_{issue}, T_{update}) \quad (3)$$

Where T_{update} denotes how long after T_{issue} the reputation certificate is supposed to be updated. For most commute vehicles, T_{update} is one day if $Cert_{R_A,V}$ is generated between Monday to Thursday, and is three days if $Cert_{R_A,V}$ is generated on Friday (since the next commute time is the next Monday).

When vehicle V sends out a message together with its reputation certificate to another vehicle or RSU at time t, the recipient will make the following decision:

- If $t \le T_{issue} + T_{update}$, the sending vehicle V has a fresh reputation certificate. The recipient trusts the reputation value S_V completely.
- If $T_{issue} + T_{update} \le t \le T_{issue} + T_{valid}$, the sending vehicle V has an old reputation certificate that has not been updated according to its normal schedule, but it is still not expired yet. The recipient vehicle trusts the sender's reputation S_V with degraded confidence dependent on how old the reputation certificate is.
- If $t > T_{issue} + T_{valid}$, the reputation certificate is invalid. The recipient will not trust the sender.

V. Security Analysis

A. Privacy

In the proposed reputation system, a vehicle's true ID, ID_V, is only revealed to its Agent RSU. No other RSUs or vehicles

could know ID_V. In this way, a vehicle's identity could be protected. In addition, as we mentioned in the reputation update procedure shown in Fig. 3, a vehicle could change its public/private key pair in each updated reputation certificate. This will prevent a vehicle being tracked by attackers over multiple days based on its reputation certificate or public key.

One limitation is that since a reputation certificate is updated daily or after more than one day, the vehicle may be tracked by attackers within one day time period as long as the vehicle uses the same reputation certificate.

B. Non-repudiation (Liability)

All messages in VANET will be accompanied with reputation certificates. Because a reputation certificate contains the vehicle's public key, it could not be steal and used by other vehicles. Therefore, if a vehicle conducts malicious activities, from its reputation certificate we can easily find its Agent RSU, and then the Agent RSU will be able to identify the vehicle based on the vehicle's registered true ID.

If a vehicle conducts attacks without using its reputation certificate, the damage will be limited since no other vehicles or RSUs will trust the malicious vehicle's messages.

C. Reputation Revocation

If a vehicle conducts malicious attacks, its reputation certificate should be revoked and its reputation score should be updated as soon as possible. How to detect a vehicle's malicious activities is out of the scope of this paper. We will only discuss how the proposed reputation system reacts after a malicious vehicle is detected.

When a vehicle V is detected to be malicious by a nearby RSU R_1, based on the vehicle's reputation certificate $Cert_{R_A,V}$, RSU R_1 can extract information of the vehicle's Agent RSU R_A and then send a revocation request message to R_A. The revocation message will be encrypted by R_1^- so Agent RSU can trust this message.

Once the Agent RSU R_A receives the revocation request message, it will check its record to find out all currently valid reputation certificates assigned to vehicle V. As introduced in Section IV.E, when T_{valid} is larger than T_{update}, vehicle V may have several still valid reputation certificates. Then the Agent RSU broadcasts the revocation message that contains all currently valid reputation certificates of this malicious vehicle to all other RSUs in its reputation administrative region.

D. Sybil Attack

Sybil attack is an attack where multiple identities are forged to facilitate attack actions. As introduced above, a vehicle V may have several valid reputation certificates at the same time. However, the number of valid reputation certificates is very limited for conducting effective Sybil attack (such as 5 if the system allows a vehicle use its reputation certificate up to 5 days). In addition, according to the design description in Section IV.E, old reputation scores are trusted with degraded confidence levels. Thus this kind of Sybil attack will not cause much damage.

Sybil attacks in VANET scenario are mostly directed at generating false presence/congestion at a place or trying to authenticate false information with multiple identities. In this case all the messages from multiple Sybil IDs will have the reputation certificates given by the same Agent RSU with different validation periods, which makes it easy to detect such kind of Sybil attack.

VI. Conclusion

In this paper we introduced a novel but simple long-term reputation system for vehicular network that is especially designed for the unique and critical intitial deployment stage of VANET. It is built based on the fact that the majority of people drive their vehicles locally for their daily commute (to work places, schools, daycares, superstores, etc) in most of the time. Vehicles' predefined constant daily trajectories make it easy for RoadSide Units to monitor vehicles daily behaviors and update their reputation scores. The proposed reputation system fits well with the VANET initial deployment environment when smart vehicles have very low penetration rate and roadside infrastructure only provides very basic service support.

References

[1] H. Hartenstein, K. Laberteaux. "VANET Vehicular Applications and Inter-Networking Technologies", Wiley, 2010.

[2] Yi Qian, and Nader Moayeri, "Design Secure and Application-Oriented VANETs", Proceedings of IEEE VTC'2008-Spring, Singapore, 2008.

[3] M. Raya and J.-P. Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39--68, 2007.

[4] E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samariti and F. Violante, "A Reputation-based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. of the 9th ACM conference on Computer and Communications Security, pp. 207 – 216, 2002.

[5] F. Cornelli, E. Damiani, D. C. di Vimercati, et. al, "Choosing Reputable Servants in a P2P Networks, " Proc. of Int'l World Wide Web Conference, pp. 441-449, 2002.

[6] C. Tian and J. Cheng, "Building an Efficient Distributed Reputation Scheme for Peer-to-Peer Networks," Proc. of IEEE Int'l Symposium on Information Science and Engineering, pp. 285-288, 2008.

[7] J. J. Jaramillo and R. Srikant, "DARWIN: Distributed and Adaptive Reputation Mechanism for Wireless Ad-Hoc Networks," Proc. of ACM Int'l Conference on Mobile Computing and Networking, pp. 87-98, 2007.

[8] C. Zouridaki, B. L. Mark and R. K. Thomas, "Robust Cooperative Trust Establishment for MANETs," Proc. of ACM workshop on Security of ad hoc and sensor networks, pp. 23–34, Virginia, USA, 2006.

[9] X. Wu, J. He and F. Xu, "A Group-based Reputation Mechanism for Mobile P2P Networks," LNCS 3828, pp. 651-659, Springer Berlin / Heidelberg, 2005.

[10] Z. Li and H. Shen, "Analysis the cooperation strategies in mobile ad hoc networks," Proc. of IEEE Int'l Conference on Mobile Ad Hoc and Sensor Systems, pp. 880-885, 2008.

[11] H. Shen and Z. Li, "ARM: An Account-based Hierarchical Reputation Management System for Wireless Ad Hoc Networks," IEEE Int'l Conference on Distributed Computing Systems Workshops, 2008.

[12] Z. Wang and C. Chigan, "Cooperation Enhancement for message transmission in VANETs," Int'l Journal of Wireless Personal Communications, Vol. 43, No. 1, pp. 141 – 156, 2007.

[13] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", SIGCOMM, pp. 27-34, August 2003.

[14] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine. "MaxProp: Routing for vehicle-based disruption-tolerant networks". In Proc. IEEE INFOCOM, April 2006.

[15] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, J. Scott. "Impact of human mobility on opportunistic forwarding algorithms". IEEE Transactions on Mobile Computing, 6(6):606–620, 2007.