A Multi-hop Reputation Announcement Scheme for VANETs

Zhiguang Cao[1,2], Qin Li[1], Hoon Wei Lim[3] and Jie Zhang[1]

***Abstract*— Vehicular ad hoc networks (VANETs) allow vehicles to generate and broadcast messages to inform nearby vehicles about road conditions. We propose a multi-hop announcement scheme for VANETs which supports message broadcasting and forwarding. In this scheme, we propose two algorithms to evaluate the reliability of messages and aggregate the reputation scores respectively. The major principle of the reliability evaluation algorithm is *Dempster-Shafter Theory* and the reputation aggregation algorithm is a variant of weighted averaging function. To balance the message coverage area and the cost of forwarding messages, we also provide a message forwarding criterion. The proposed multi-hop scheme offers satisfactory robustness and preserves privacy property. Most importantly, the multi-hop scheme not only guarantees better message flexibility, but also can generate more satisfactory message drop rate. In addition, in the message forward criterion of our multi-hop scheme, it is up to vehicles (i.e., user friendly) to regulate the trade-off between the message utility rate and the maximal message broadcasting bandwidth, based on their real needs.**

I. INTRODUCTION

A vehicular ad hoc network (VANET) is formed by mobile nodes embedded within vehicles and roadside infrastructure in an ad hoc way. There has been active research in VANETs from both academia and industry, e.g. [1], [2], [3], [4], [5]. We call an information system that facilitates vehicles to generate and broadcast safety and traffic information in VANETs an *announcement scheme*. In an announcement scheme, vehicles either periodically broadcast vehicle self-status messages (beacons) about their current position, speed and direction, or generate and broadcast messages when they detect an event such as traffic congestion or accident [2], [6]. We say a message is *reliable* if it reflects reality. Unreliable messages may result in various consequences, such as journey delays or accidents. Unreliable messages may be a result of vehicle hardware malfunction. They 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. It is therefore critical for the announcement scheme to discriminate the unreliable messages.

There have been a number of announcement schemes proposed to evaluate the reliability of messages in VANETs, categorized into two main groups: *threshold* approach, and *reputation-based* approach. A majority of announcement schemes, e.g. [1], [2], [4], use the threshold method: a message is believed reliable if the same message has been announced by multiple vehicles whose number exceeds a threshold within a time interval. These schemes in general suffer from one critical problem: a lack of immediate evaluation. Upon receiving a message, a vehicle has to wait until it receives the same message from a sufficient number of distinct vehicles, before taking the message into consideration. This time delay is undesirable for VANETs, especially when messages are time critical. On the other hand, there also have been several reputation-based approaches, such as [3], [7], [8]. Almost all reputation-based approaches adopt a decentralized infrastructure, since only they seem suitable for the distributed and highly mobile environment of VANET. But the scheme in [7] has shown the advantages of using a centralized architecture with an off-line central server.

The reputation-based announcement scheme proposed in [7] aims to provide message reliability evaluation, accountability and robustness. This scheme relies on a centralized reputation system with an offline trusted authority. The reliability of a message is evaluated according to the reputation of the vehicle that generates this message. The message is considered reliable if the vehicle has a sufficiently high reputation. It has an important performance advantage: *immediate evaluation*. Upon receiving a message, a receiving vehicle is able to immediately evaluate the reliability of the message without assistance from other vehicles. It enables the receiving vehicle to respond quickly according to the message. Moreover, it is often easier to manage, control, and secure this kind of centralized system, therefore it is more desirable than the decentralized schemes in [3] and [8].

The single-hop scheme in [7] seems more desirable, however, it suffers from several problems: it only supports *single-hop* message broadcast, and a message broadcast by a vehicle can be utilized by vehicles only in proximity (within the wireless communication range). Therefore it limits the propagation of those event-driven messages, which may need to be disseminated to vehicles in a greater geographical area [9]. Moreover, in the single-hop scheme, the receiving vehicle simply rejects the messages if the time-discounted reputation score of the broadcasting vehicle is too low. But it does not address the important problem on how to handle if the messages disagree with each other when their corresponding reputation scores are all high. In real life, the messages regarding the same event broadcast or forwarded by different vehicles do not always fully agree with each other, and more importantly, believing wrong messages may cause unexpected traffic danger, it is therefore

[1] Zhiguang Cao, Qin Li and Jie Zhang are with the School of Computer Engineering, Nanyang Technological University, Singapore(caoz0005@e.ntu.edu.sg, {qin.li, zhangj}@ntu.edu.sg).

[2] Zhiguang Cao is with the Interdisciplinary Graduate School, Nanyang Technological University, Singapore(caoz0005@e.ntu.edu.sg).

[3] Hoon Wei Lim is with the School of Computing, National University of Singapore, Singapore(hoonwei@nus.edu.sg).

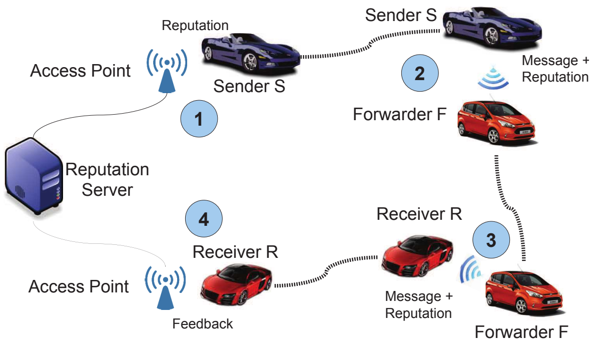


Fig. 1: Multi-Hop Reputation Announcement Structure

non-trivial to solve this problem. In this paper, we propose a multi-hop reputation announcement scheme to addressed the aforementioned problems.

II. Multi-Hop Reputation Announcement Scheme

In this section, we first introduce the structure of multi-hop reputation announcement scheme, and then we elaborate the algorithms required in this scheme.

A. *Structure of Multi-Hop Reputation Announcement Scheme*

Our proposed system consists of three types of entities: a *reputation server*, *access points* and *vehicles*. The reputation server is a centralized trusted authority, which collects and aggregates feedback, produces and propagates reputation. It is also in charge of admitting vehicles into and revoking them from the system. Access points are the physical wireless communication devices connected with the reputation server, acting as a convenient and frequent communication interface between vehicles and reputation server. They are always installed at locations frequently visited by 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 and a wireless communication device for short-range radio communication and that the reputation server and each vehicle are equipped with a clock. As illustrated in Fig. 1, when the sender S plans to broadcast a message, it first retrieves its own reputation certificate (including reputation score) from reputation server through access point, and sends it with the message to the neighboring receiver R. R may evaluate the reliability of the message and provide corresponding feedback to reputation server through access points, and it may also forward message(s) as well as the reputation score(s) to its neighbors within the wireless communication range.

B. *Time Discount Function*

Our scheme needs a time discount function, denoted by TDF. It is a non-increasing function whose range is $[0, 1]$.

$$\mathsf{TDF}(t) = \begin{cases} 1 - t/\Psi_{td} & \text{if } t < \Psi_{td}; \\ 0 & \text{if } t \geq \Psi_{td}, \end{cases} \tag{1}$$

where $\Psi_{td} > 0$ is a configurable parameter, determining how quickly the time discount function decreases as t increases. Then the discounted reputation score when vehicle V_k receives the message is denoted as follows:

$$rs_{V_i^k} = rs_{V_i} \cdot \mathsf{TDF}(t_r - t_c) \tag{2}$$

where rs_{V_i} is the reputation score of the vehicle V_i who broadcasts the message, t_r and t_c are the message receiving time and the reputation certificate retrieving time of V_i.

C. *Message Reliability Evaluation Algorithm*

Our scheme allows messages to fully or partially agree or disagree with each other for the same event, because the descriptions of the same observation are likely to be subjective. We propose a message reliability evaluation algorithm MREA to judge the message reliability, which uses Dempster-Shafer theory (DST) of evidence.

1) Dempster-Shafer Theory (DST): DST explicitly handles evidence, in which lack of belief in any particular hypothesis is allowed and reflects a state of uncertainty. This leads to the intuitive process of narrowing a hypothesis, in which initially most weight is given to uncertainty and replaced with belief as evidence accumulates [10].

Definition 1: A frame of discernment, denoted by Θ, is the set of possibilities under consideration.
Let evidence M mean that the given party considers a specified event to be trustworthy. Then, there are only two possibilities. That is, $\Theta = \{M, \neg M\}$, where $\neg M$ is the complementary set of M with respect to Θ.

Definition 2: Basic probability assignment (bpa) is a function $m :\mapsto [0, 1]$, where $m(\emptyset) = 0$ ($\emptyset$ refers to the empty set) and $\sum_{\hat{A} \subset \Theta} m(\hat{A}) = 1$.
Thus, $m(\{M\}) + m(\{\neg M\}) + m(\{M, \neg M\}) = 1$. A bpa is similar to a probability assignment except that its domain is the subsets and not the members of Θ.

For $\hat{A} \subset \Theta$, the *belief function* $\mathsf{Bel}(\hat{A})$ is defined as the sum of the beliefs committed to the possibilities in $\hat{A}$:

$$\mathsf{Bel}(\{M, \neg M\}) = m(\{M\}) + m(\{\neg M\}) + m(\{M, \neg M\}) = 1 \tag{3}$$

2) Message Belief Function: In our scheme, we take each message, which is the description of one specified event, as an evidence M. When a vehicle V_i broadcasts a message M_j, we assign the discounted reputation score r_i(computed by Eq. 2) of V_i as the bpa value of message M_j:

$$\begin{cases} m_i(\{M_j\}) = r_i \\ m_i(\{\neg M_j\}) + m_i(\{M_j, \neg M_j\}) = 1 - r_i \end{cases} \tag{4}$$

where $m_i(\{M_j\})$ indicates message M_j's belief value supported by V_i.

3) Combining Belief Functions: DST allows one to combine evidence from different sources and arrive at a degree of belief that takes into account all the available evidence. Considering that the message may fully or partially agree or disagree with each other, the belief value of the intersected information π_j and empty set $\emptyset$ by a set of vehicles $V_0, ..., V_{N-1}$ are combined as:

$$m_{0,...,N-1}(\{\pi_j\}) = \sum_{X_0 \cap ... \cap X_{N-1} = \{\pi_j\}} m_0(X_0) \times ... \times m_{N-1}(X_{N-1}) \tag{5}$$

$$m_{0,...,N-1}(\emptyset) = \sum_{X_0 \cap ... \cap X_{N-1} = \emptyset} m_0(X_0) \times ... \times m_{N-1}(X_{N-1}) \tag{6}$$

where $X_i = \{M_i\}$ or $\{\neg M_i\}$. In DST, the belief value of $\emptyset$ should be zero [11]. Thus, if the sum of all $m_{0,\ ...,N-1}(\emptyset)$ is non-zero, standard normalization should be implemented as:

$$B_{\pi_j} = \frac{1}{1 - m_{sum}(\emptyset)} m_{0,...,N-1}(\{\pi_j\}) \tag{7}$$

where m_{sum} is the sum of all bpa values of empty set, and B_{π_j} is the final belief value of each information π_j. However, if m_{sum} is larger than a threshold, standard normalization should be ignored and final belief value of each information π_j can be simply obtained as follows:

$$B_{\pi_j} = m_{0,...,N-1}(\{\pi_j\}) \tag{8}$$

4) Reliability Evaluation: Based on above descriptions, when a vehicle V_r receives multiple messages, it first uses location and time information to identify the messages regarding the same event. Then V_r assesses the reliability of these messages using DST, described by Algorithm 1.

Algorithm 1 Message Reliability Evaluation Algorithm *(MREA)*

```
Input:
    Message matrix $\Omega_{N\times 2}$ (1st column is message $M$, 2nd column is reputation score $r$);
    Threshold $T_1$;
Output:
    Information $\pi$ with maximum belief value;
Compute belief value of each possible intersected information $\pi_j$ by Eq. 5;
Compute belief value of each possible intersected information $\emptyset$ by Eq. 6;
Compute the sum of all belief value of $\emptyset$, $m_{sum}(\emptyset)$;
for each information $\pi_j$ do
    if $m_{sum}(\emptyset) \leq T_1$ then
        Perform standard normalization for $B_{\pi_j}$ by Eq. 7;
    else
        Compute $B_{\pi_j}$ by Eq. 8;
    end if
end for
Compute the maximum belief value: $B_{\pi}^{max} \leftarrow Max(\{B_{\pi_0}, ...\})$;
return Information $\pi$ with maximum belief value.
```

As to judge whether the information π is reliable, we assume threshold T_2. If $B_{\pi}^{max}$is larger than T_2, V_r considers π as reliable and some actions will be taken upon it, where T_1 and T_2 are both configurable parameters.

D. Reputation Aggregation for Vehicles

Our scheme requires a reputation aggregate algorithm *RAA* to compute the latest reputation score rs_{V_i} for vehicle V_i. The server first selects all feedback reported for vehicle V_i whose corresponding message tuple was broadcast from time $\mathbb{T}$ in the past up to the present time, where $\mathbb{T}$ is a configurable parameter. More formally, let t_a denote the time when this aggregation is running. Then the algorithm *RAA* selects a subset of feedback $\mathcal{F}$, where

$$\mathcal{F} = \{F : (id_{V_b} = id_{V_i}) \wedge (t_b \geq t_a - \mathbb{T})\} \tag{9}$$

where id_{V_b} denotes the ID of broadcasting vehicles. The feedback whose corresponding message was broadcast earlier than time $\mathbb{T}$ in the past is ignored and deleted for the sake of data storage efficiency.

Multiple feedback reported by one vehicle V_k for V_i is aggregated into one intermediate value $\hat{r}_{V_i^k}$. Let $\mathcal{F}_{V_i^k}$ denote the set of feedback reported by the vehicle V_k for V_i and whose corresponding message was broadcast from time $\mathbb{T}$ in the past up until the present time:

$$\mathcal{F}_{V_i^k} = \{F : (id_{V_b} = id_{V_i}) \wedge (id_{V_f} = id_{V_k}) \wedge (t_b \geq t_a - \mathbb{T})\} \tag{10}$$

where id_{V_f} denotes the *ID* of vehicles who provide feedback. The value $\hat{r}_{V_i}$ can be aggregated using a weighted average:

$$\hat{r}_{V_i^k} = \frac{\sum_{F \in \mathcal{F}_{V_i^k}} fr \cdot (\mathbb{T} - (t_a - t_b))}{\sum_{F \in \mathcal{F}_{V_i^k}} (\mathbb{T} - (t_a - t_b))} \tag{11}$$

which gives the more recent feedback greater weight than the less recent feedback. Considering the message of the same event may overlap each other, the message broadcast by one vehicle may be only partially correct. So the feedback value fr could be any number between 0 and 1. Let $\mathcal{V}_i$ denote the set of vehicles who have each reported at least one feedback for V_i in the past $\mathbb{T}$ time, then the value $\hat{r}_{V_i^k}$ is computed for each vehicle $V_k \in \mathcal{V}_i$.

Suppose that it is a positive feedback if fr is greater than Ψ_{fp}, and a negative feedback if fr is smaller than Ψ_{fn}, where Ψ_{fp} and Ψ_{fn} are configurable parameters. Let $\mathcal{V}_i^-$ denote the set of vehicles reporting at least one negative feedback for V_i in the past $\mathbb{T}$ time, then the latest reputation score rs_{V_i} is computed as follows:

$$rs_{V_i} = \begin{cases} \frac{\sum_{V_k \in \mathcal{V}_i} \hat{r}_{V_i}}{|\mathcal{V}_i|} & \text{if } |\mathcal{V}_i^-| < \Psi_{nf}; \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

where Ψ_{nf} is a configurable parameter.

E. Message Forwarding Criterion

We require one message forwarding criterion, which acts as the threshold for vehicle V_k to decide whether or not to forward the messages with regard to the same event E.

Intuitively, when V_k is far away from the location of E, it may believe the neighboring vehicles are not interested in E, and therefore discards the messages; Otherwise, V_k will forward the messages to the neighboring vehicles. Suppose D_{re} denotes the distance between current location of vehicle V_k and location of event E. Then the criterion is stated as: If $1/D_{re} > D_{fwd}$, V_k forwards the messages; Otherwise, V_k discards them, where D_{fwd} is a configurable parameter.

F. Aggregate Signature Scheme

We require one secure aggregate signature scheme with two different key sets, denoted by $\mathsf{AS}_1 = (\mathsf{KeyGen}_1,\mathsf{Sign}_1,\mathsf{Aggr}_1,\mathsf{Verify}_1)$ and $\mathsf{AS}_2 = (\mathsf{KeyGen}_2,\mathsf{Sign}_2,\mathsf{Aggr}_2, \mathsf{Verify}_2)$, where KeyGen, Sign, Aggr, and Verify denote key generation, signing, aggregation, and verification algorithms, respectively. The scheme AS_2 will be used by the server to endorse the reputation scores [12].

III. Running Procedure for the Proposed Scheme

In this section, we provide details to set up the whole multi-hop reputation announcement scheme.

System initialization. When a new system is set up, the reputation server: 1) installs the message reliability evaluation algorithm MREA, and the reputation aggregation algorithm RAA; 2) installs the aggregate algorithms AS_1, and AS_2; 3) generates its own public and private key pair (pk_S, sk_S) using KeyGen_2 and keeps the private key sk_S confidential; 4) regulates its clock; and 5) creates a database to store reported feedback. 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.

Vehicle registration. When a new vehicle V_i chooses to join the system, it is initialized as follows. The reputation server: 1) retrieves its unique identifier id_i assigned by a vehicle administrative authority; 2) generates a public and private key pair, denoted by (pk_i, sk_i), for the vehicle using the algorithm KeyGen_1; 3) sends the private key sk_i to the vehicle in a confidential channel; 4) creates a record in its database for vehicle V_i. In addition, the vehicle: 6) regulates its clock; 7) installs the aggregate signature scheme AS_1; 8) stores its own secret key sk_i, and the thresholds Ψ_{rs}.

Reputation retrieval. When a vehicle V_i drives into 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_i sends its identity id_i to the server via the access point; 2) The reputation server generates a *reputation certificate* C for the vehicle, where $C = (pk_i, t_i^r, r_i, \sigma_i)$, in which t_i^r denotes the time when C is generated and it is obtained from the reputation server's clock, r_i denotes the reputation score of V_i at time t_i^r, and $\sigma_i = Sign_2(sk_S|pk_i, t_i^r, r_i)$ denotes a digital signature using the algorithm Sign_2 and private key sk_S on (pk_i, t_i^r, r_i); 3) The reputation server sends C to V_i via the access point; 4) Once V_i obtains C, it stores the reputation certificate locally.

Message broadcast. In this phase, V_i generates a message m_i regarding an event E and broadcasts it to its neighbouring vehicles. This is described as follows: 1) V_i retrieves the current time, denoted by t_i^m, and determines the *time to live* of the message m_i, denoted by ttl_i; 2) V_i generates a signature $\theta_i = Sign_1(sk_i|m_i, t_i^m, ttl_i, r_i, t_i^r)$; 3) V_i forms a *message tuple* $M_i = (m_i, t_i^m, ttl_i, r_i, t_i^r, pk_i, \delta_i, \theta_i)$, and broadcasts M_i to its neighboring vehicles.

Message reliability verification. It uses location and time information to identify the messages regarding the same event and uses *MREA* to evaluate their reliability.

Message aggregation and forward. The vehicle V_k carries the messages regarding event E when it travels to other places. V_k decides whether to forward these messages based on Message Forwarding Criterion. If V_k believes the current neighboring vehicles are interested in E, it will forward the messages as follows: Suppose V_k receives multiple message tuples $M_1, M_2, \cdots, M_J$ concerning the same event E. Then $M_1, M_2, \cdots, M_J$ are aggregated into M_1^J:

$$M_1^J = \begin{pmatrix} m_1, & t_1^m, & ttl_1, & r_1, & t_1^r, & pk_1, & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \\ m_J, & t_J^m, & ttl_J, & r_J, & t_J^r, & pk_J, & \sigma_1^J, & \theta_1^J \end{pmatrix}$$

which would be forwarded. If V_k believes that the current neighboring vehicles are not interested in the event E, it will discard the messages.

Reputation update. After collecting the feedback set for vehicle V_i, the reputation server employs *RAA* to update V_i's reputation score timely.

Vehicle revocation. A vehicle would be revoked by the reputation server if $|\mathcal{V}^-| > \Psi_{nf}$. Once a vehicle is revoked, the reputation server will not provide new reputation certificates for it. At the same time, the reputation server will not consider feedback reported by the revoked vehicle as valid.

IV. Performance Analysis

In this section, we analyze the performance of our announcement scheme comprehensively.

A. Security of the Scheme

This section shows that our proposed multi-hop scheme preserves the desirable robustness and privacy properties.

1) *Robustness of the scheme.* The multi-hop scheme provides strong robustness against external adversaries conducting message fraud and reputation manipulation, because an external adversary is not able to forge a valid reputation certificate C or message tuple M. It also provides strong robustness against internal adversaries, because the vehicle always explores a group of messages instead of a single message to judge whether the event is happening, which greatly prevents internal adversaries from succeeding.

2) *Privacy of the scheme.* Privacy is always an important criterion of an announcement scheme for VANETs. Although privacy is not the focus of this paper, it is worth noting that the multi-hop 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 provides the 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 server to pre-embed 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.

B. Message Flexibility

It is easy to arrive that the complexity of *MREA* is $O(2^N)$ in worst case. Because messages may fully or partially agree with each other, each possible message intersection should be considered. But on the other hand, this algorithm dose not limit the number of message categories. The event descriptions are likely to be very subjective because each vehicle may have its own opinion about the same event. No matter how many different descriptions about the same event there are, *MREA* can compute all the possible intersected information π and their belief values. This way, the vehicle could describe the event more flexibly, which is useful and consistent with real traffic situation.

C. Simulation Analysis

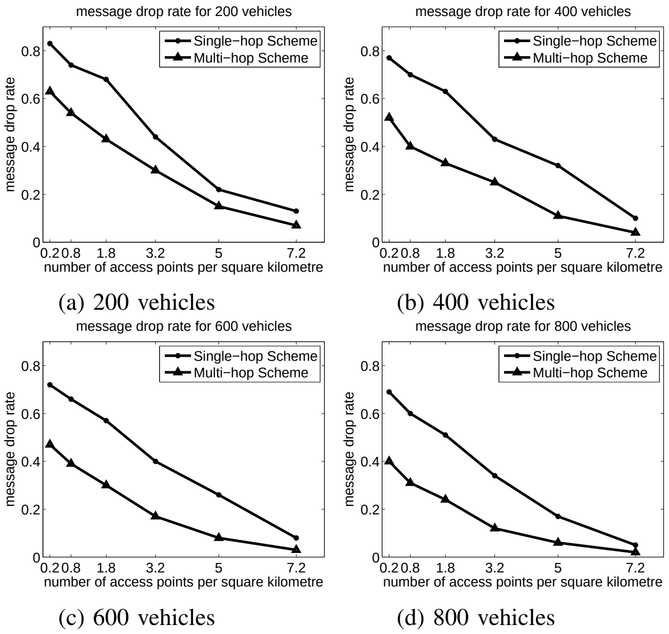
In this section, we compare the performance of our multi-hop announcement scheme with that of single-hop. We employ the event-based real street map vehicular network simulator GrooveNet [13] to implement the announcement.

1) Simulation Settings: In this simulation, we choose a road network with area of $80km^2$, which is part of Pittsburgh city. Detailed configuration is stated as follows: (1) access points are randomly populated over the selected urban area; the radius of the wireless communication range is $0.5km$; (2) vehicles are also randomly populated over the selected urban area, and they all comply with the *car-following* rule when moving. In addition, they traverse the road network based on a *sightseeing* model; (3) road events happened randomly from the beginning to the end of the experiment. The lasting time for any event is randomly set from 1 to 120s; (4) a vehicle broadcasts a message with regard to the event it experienced, along with its latest reputation certificate; (5) when receiving a message, a vehicle decides whether or not to forward it to the neighbouring vehicle after evaluating it; it will also provide the feedback about this message to reputation server after experiencing the event; (7) the reputation server initializes the reputation score randomly within the range [0,1], updates all the reputation score based on the feedback it received and the update period is 5 min; (8) each message capacity is $0.5Kb$.

2) Message Drop Rate:

Definition 3: Message Drop Rate is the average rate that reliable messages are rejected by a receiving vehicle after reliability evaluation.

Fig. 2 shows the results of message drop rate with respect to the different density of access points and vehicles, for both single-hop and multi-hop schemes. Looking into single-hop and multi-hop schemes comparatively, the results in Fig. 2 show that the message drop rate of multi-hop scheme is usually lower than that of single-hop scheme for all cases we studied. The multi-hop scheme uses *MREA* to evaluate the message reliability based on a group of messages. Even if one vehicle sends a true message with very low discounted reputation score, *MREA* is still able to decide that the message is likely to be true, because *MREA* takes advantage of numbers of messages instead of a single message to judge whether the reported event is happening. It increases the probability that the true message would be considered as reliable even the reputation score of the sending vehicle is low. Consequently, the reputation server will aggregate a higher reputation score for this vehicle since it sends a true message and should accordingly receive more favorable feedback. Thus it reduces the chance that the true message would be rejected. However, in the single-hop scheme, the receiving vehicle would reject the true message directly just because the discounted reputation score of the sending vehicle is too low.



(a) 200 vehicles

(b) 400 vehicles

(c) 600 vehicles

(d) 800 vehicles

Fig. 2: Message drop rate with different density of access points and vehicles

3) Message Utility Rate and Maximum Message Broadcasting Bandwidth:

Definition 4: We suppose N_E denotes the number of all vehicles which experienced the event E before it expired, and N_E^U denotes the number of all vehicles which received message regarding E before experienced it, then Message Utility Rate is the ratio of N_E^U over N_E.

Definition 5: Maximum Message Broadcasting Bandwidth is equal to the largest capacity of all messages needed to broadcast or forward at one moment.

Fig. 3 shows the results of message utility rate and maximum message broadcasting bandwidth with respect to different D_{fwd} (the distance threshold to forward the message or not), for both single-hop and multi-hop schemes. Looking into the left sub-figure, the Message Utility Rate

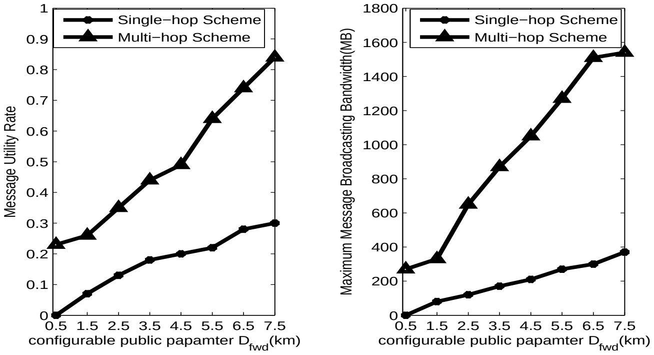


Fig. 3: Message utility rate and maximum message broadcasting bandwidth with different D_{fwd}

grows with the increase of D_{fwd} for both single-hop and multi-hop schemes. It is naturally acceptable because if one vehicle is allowed to broad or forward messages with regard to event E at more distant locations, then most of the vehicles which later experienced the event E will stand a larger chance to have already received relevant message before arriving that place. However, the message utility rate for the multi-hop scheme is always larger than that of the single-hop scheme. Obviously, it is reasonable given that in the multi-hop scheme, both broadcasting and forwarding messages are allowed and therefore more neighboring vehicles will receive those messages with higher chance while forwarding is forbidden in the single-hop scheme. Looking into the right figure, the maximum message broadcasting bandwidth also grows with the increase of D_{fwd} for both the single-hop and multi-hop schemes. It is straightforward because if one vehicle is allowed to broadcast or forward messages with regard to event E at more distant locations, more neighboring vehicles are also likely to forward them again after receiving these messages. It means that at one moment, the broadcasting channel needs larger bandwidth to successfully process all these messages. Further, the maximum message broadcasting bandwidth for the multi-hop scheme is always larger than that of the single-hop scheme, which means that the multi-hop scheme broadcasting system is much more burdensome. This is caused by the forwarding function, at the price of other advantageous performance in the multi-hop scheme, especially the higher message utility rate. Higher message utility rate and lower maximum message broadcasting bandwidth are preferred. It is a trade-off and could be controlled by the vehicle itself in the multi-hop scheme by regulating D_{fwd}.

V. Conclusion and Future Work

This paper extended the single-hop reputation announcement into a multi-hop version that enables carry-and-forward message propagation. In this scheme, we use Dempster-Shafer theory to evaluate the reliability of messages and it guarantees better message flexibility and satisfactory message drop rate. The message utility rate and maximum message broadcasting bandwidth in multi-hop scheme cannot simultaneously dominate that of single-hop, because the maximal message broadcasting bandwidth always becomes large with the increase of message utility rate. However, this trade-off is up to vehicles to regulate based on their real needs. It is therefore more user friendly and flexible than single-hop. Moreover, the multi-hop scheme provides incentive for vehicles to participate in forwarding messages and at the same time maintains the robustness and privacy property of the single-hop scheme. However, there are still some aspects to be improved: (1) the computation complexity for *MREA* is exponential in the worst case. We will try to reduce it in future. (2) The message forwarding criterion is merely decided by distance parameter. It is more desirable to also consider the road network structure and the driving direction.

Acknowledgment

This work is supported by Dr. Jie Zhang's project funded by the MOE AcRF Tier 1. We also appreciate the advice given by Dr. Hongliang Guo.

References

[1] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 4, pp. 1876–1886, 2009.

[2] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in vanets," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 67–75, ACM, 2006.

[3] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM)*, 2008.

[4] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 559–573, 2010.

[5] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty," in *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, vol. 2, pp. 243–247, IEEE, 2010.

[6] J. Zhang, "A survey on trust management for vanets," in *Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pp. 105–112, IEEE, 2011.

[7] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for vanets," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 9, pp. 4095–4108, 2012.

[8] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 41, no. 3, pp. 407–420, 2011.

[9] A. Festag, P. Papadimitratos, and T. Tielert, "Design and performance of secure geocast for vehicular communication," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 5, pp. 2456–2471, 2010.

[10] H. E. Kyburg Jr, "Bayesian and non-bayesian evidential updating," *Artificial Intelligence*, vol. 31, no. 3, pp. 271–293, 1987.

[11] B. Yu and M. P. Singh, "Detecting deception in reputation management," in *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*, pp. 73–80, ACM, 2003.

[12] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in cryptology-EUROCRYPT*, pp. 416–432, Springer, 2003.

[13] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai, "Groovenet: A hybrid simulator for vehicle-to-vehicle networks," in *Proceedings of the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp. 1–8, IEEE, 2006.