A Vehicle Message Scheduling Scheme For Vehicle Trust Management

Qinwen Hu
School of Computer Science
The University of Auckland
New Zealand
qhu009@aucklanduni.ac.nz

Wanqing Tu
Department of Computer Science
Durham University
United kingdom
wanqing.tu@durham.ac.uk

***Abstract*—The trustworthiness of vehicle messages is a major focus in intelligent transportation research. Existing studies focus on enhancing the accuracy of credibility evaluation, overlooking that the transmission performance may affect the quality of vehicle messages which are essential for implementing credibility evaluation. This letter improves vehicle trust management in a dense vehicle network by regulating vehicle transmissions. Through strategically scheduling vehicle transmissions to avoid interference between vehicles while guaranteeing sufficient numbers of vehicles transmitting their sensor data, vehicle messages can reliably yet timely arrive at Road Side Units (RSUs) without missing reporting an event on the road.**

I. Introduction

In an intelligent transport network, vehicles automatically send messages to Road Side Units (RSUs) to report an emergency event, road conditions, traffic situations, keepalive Hellos, *etc.* These messages are then used by RSUs or other central intelligent devices to analyse the situations of vehicles and roads, so as to make appropriate action decisions for the transport network. The credibility/trustworthiness of vehicle messages is hence crucial for the smooth operations of intelligent transport networks.

Much research effort has been spent on various trustworthiness algorithms. Some studies focus on efficiently evaluating the received incident report by the centralised server [1], [2], while others [3], [4] discuss that how the surrounding vehicles use the received information or historic vehicle behaviours to update the credibility of the sending vehicle. However, no study considers that simultaneous transmissions of vehicle messages may interfere with each other due to the wireless broadcast property. Such interference easily causes packet loss, data errors, or long transmission delays [5], negatively affecting the report quality received at RSUs [6].

This letter investigates how to support accurate trust management in vehicle networks by improving vehicle transmission experience. In detail, an RSU in our system forms a detection zone to limit the number of vehicles sending reports to an RSU. Within each detection zone, vehicles are ranked based on their credibility. To select the vehicles that will report events, we use the ranking of vehicles inside a detection zone. In addition to referring to the ranking of vehicles within a detection zone, the distances between vehicles are taken into account in order to avoid the interference between vehicle transmissions.

Our Network Simulator 2 (NS2) simulation results show that our scheme greatly helps existing schemes [2], [4] to achieve a report loss rate $< 10\%$ with acceptable average report delays when vehicles send the emergency reports to the RSU.

II. Related Work

Many existing solutions for the trustworthiness of vehicle networks, the trustworthiness solutions utilize vehicles, RSUs, cloud servers and blockchain to monitor and record the malicious behaviours of reporting vehicles. For instance, the vehicular cloud in [2] is an emerging form of vehicular networks where cloud features are leveraged for enhanced computation and maintenance. However, the cloud solution is not practical to cope with large numbers of vehicles, resulting in high latency. To reduce the high latency, Huang *et al.* [7] introduced a recommendation based trust management solution to utilize direct or indirect communication among vehicles to share the misbehaviour of a reporting vehicle. Although the proposed solutions reduce the computation and transmission delays, it introduces new conspiracy attacks [8]. As a security solution for the consensus issue, the blockchain technology has been leveraged for trust establishment in vehicular networks. Yang *et al.* [4] proposed a decentralized trust management system that develops a blockchain based trustworthiness solution to address the consistent data issue. The existing solutions do not take into account the impact on quality of service (QoS) particularly in a dense traffic scenario [9], which may lead to a large transmission delay and a high report loss rate.

To the best of our knowledge, the state-of-the-art in the intelligent transport network does not take into account the impact of the transmission quality on the effectiveness of credibility evaluation or trust management. In particular, when multiple adjacent vehicles send the emergency reports simultaneously, the transmissions of their reports may interfere with each other due to the wireless broadcast property. Such interference easily causes packet loss, data error, or long transmission delays. We hence presents a new vehicle transmission scheme to address the concerns that have been overlooked in the literature.

III. The Vehicle Message Scheduling Algorithm (VMS)

Denote an RSU as R. In our system, instead of asking all vehicles to report a road event, R selects a subset of vehicles in its coverage to report a road event. The selection of this subset of vehicles is not trivial as it is hard to predict where on a road an event would happen and each vehicle has a limited accurate detection distance. Our idea is to divide the coverage of the RSU R into a controlled number of detection zones (DZs). Vehicles are dynamically allocated to these DZs based on their instantaneous locations. Within each DZ, the vehicle selection scheme is designed to select event reporting vehicles based on their rankings. Our VMS algorithm ensures that events can be detected and accurately reported no matter where on the road such events take place.

A. Formation of Detection Zones

The formation of DZs is implemented by R. In order to allow vehicles inside a DZ to accurately sense events in this zone, R forms DZs by referring to the accurate detection distance of vehicles. Meanwhile, in order to efficiently control the number of DZs within R's coverage, our DZs are in the shape of cubes (as shown in Fig. 1). This is because cubes not only may fully cover R's coverage without overlaps but also require relatively simple calculations as compared to other shapes.

Without loss of generality, assume R locates at $(0, 0, 0)$ and the accurate detection distance of vehicles in our system is d. R forms the first DZ by regarding itself as the central point of the cube. Then, in order to guarantee that any vehicles inside this DZ can accurately sense events in this zone, the longest distance in this DZ, i.e., the length of a diagonal line (shown by the blue dotted line in Fig.1), should be $\leq d$. To form the DZ as large as possible, helping to reduce the number of DZs, we use d as the length of a diagonal line in our DZs. Therefore, the sides of the DZ should have the length s as

$$(\sqrt{2}s)^2 + s^2 = d^2 \Rightarrow s = \frac{d}{\sqrt{3}}.$$

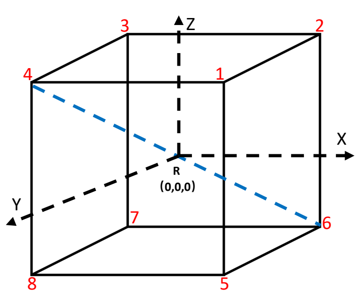

Fig. 1. An example of forming detection zones.

With the side value of the DZ, it is not hard to obtain the eight vertices as illustrated by red numbers in Fig.1. More specifically, the coordinates for vertex 1 are $(\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}})$, for vertex 2 are $(\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}})$, for vertex 3 are $(-\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}})$, for vertex 4 are $(-\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}})$, for vertex 5 are $(\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}})$, for vertex 6 are $(\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}})$, for vertex 7 are $(-\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}})$ and for vertex 8 are $(-\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}})$ respectively. These eight vertices define the first DZ.

Once the first DZ is established, R selects a face on this DZ to support the formation of further DZs. Without loss of generality, R first selects the face having the vertices 1, 2, 3, and 4. This next DZ is also a cube sharing the selected face with the first DZ. Therefore, the other four vertices of the second DZ are $(\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}} + \frac{d}{\sqrt{3}})$, $(\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}} + \frac{d}{\sqrt{3}})$, $(-\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}} + \frac{d}{\sqrt{3}})$, $(\frac{d}{2\sqrt{3}}, -\frac{d}{2\sqrt{3}}, \frac{d}{2\sqrt{3}} + \frac{d}{\sqrt{3}})$. The centre of the face formed by these four new vertices can be obtained as $(0, 0, \frac{d}{2\sqrt{3}} + \frac{d}{\sqrt{3}})$. We call the Euclidean distance between R and this centre as the distance covered by the two DZs (denoted as d'). If $r > d'$, where r is the radius of R's coverage, R forms another DZ sharing the latestly formed face. The procedure continues until $r \leq d'$.

R then starts the second procedure by forming a new DZ sharing the face defined by the vertices 1, 2, 5, and 6 on the first DZ, using the same procedure as above. R continues forming further DZs until the distance covered by all DZs formed in this second procedure is $\geq r$. When the second procedure completes, R starts the third procedure by forming a new DZ sharing the face defined by the vertices 1, 4, 5, and 8 on the first DZ. The third procedure completes once the distance covered by all DZs formed in this procedure is $\geq r$. Similarly, R forms more DZs by referring to other five faces on the first DZ.

We call all the space inside established DZs as covered space. Once the DZs along the six faces of the first DZ have been formed, R continues establishing new DZs in order to extend the covered space to the whole coverage of R. Without loss of generality, R uses the secondly established DZ as the reference DZ to continue the DZ formation along those faces on this reference zone that do not have adjacent DZs. If all the covered space by these new DZs and those already established DZs in previous procedures does not fill R's coverage, R uses the third established DZ as the reference zone to form more DZs. The process continues until the covered space by all DZs fills R's coverage. The formation of DZs then completes. We consider the z-axis when dividing DZ, because we consider that some vehicles may observe accidents from vertical space, such as vehicles on viaducts.

B. Vehicle-Zone Allocation and Vehicle Ranking

Once R has divided its coverage into a number of DZs, the next step is to allocate vehicles on the road to a DZ based on the vehicles location coordinates. Like most vehicle networks, in our system, vehicles periodically send Hello messages. A Hello message generated by our vehicles contains three fields: vehicle ID, the coordinates of vehicle's current location, and vehicle's speed. A vehicle may obtain its current location coordinates by global positioning system (GPS) [10], etc. R extracts the vehicle's current location coordinates from the periodical Hello messages.

Suppose a vehicle's current location is (x, y, z), R allocates this vehicle to a specific DZ by comparing (x, y, z) with DZs' coordinate boundaries. More specifically, for the ith DZ ($i \in [0, n-1]$), where n is the total number of DZs in R's coverage, we let $x_{i,min}$, $y_{i,min}$, and $z_{i,min}$ be the minimum values of all points in this DZ on the x, y and

z axes, respectively, and $x_{i,max}$, $y_{i,max}$, and $z_{i,max}$ be the maximum values. R compares x with $x_{i,min}$ and $x_{i,max}$, y with $y_{i,min}$ and $y_{i,max}$, and z with $z_{i,min}$ and $z_{i,max}$. The vehicle is allocated to the ith DZ only when the vehicle's coordinates meet $x_{i,min} \leq x \leq x_{i,max}$, $y_{i,min} \leq y \leq y_{i,max}$, and $z_{i,min} \leq z \leq z_{i,max}$. The relationship between a vehicle and a DZ is dynamic as the vehicle keeps moving. By the above way, based on the latest Hello messages, R dynamically maps vehicles to DZs. For vehicles allocated to the same DZ, R forms a ranking list by sorting all vehicles in descending order of their credibility.

A vehicle ranking list associated with a DZ dynamically changes when a vehicles enters or leaves the DZ as below.

1) When R receives a Hello message with a vehicle ID which is not currently on the ranking list for the DZ, R regards the vehicle as a new one entering into the DZ. R achieves the credibility of this vehicle from a blockchain, a cloud server, or other devices (depending on the employed vehicle trust management scheme [2], [4]). R then places the ID of this vehicle on the ranking list so that all vehicles in the DZ are ranked in the descending order of their credibility.
2) When R has not received a Hello message, for a time period (say 3 Hello periods), from a vehicle whose ID is on the ranking list of the DZ, R regards that the vehicle has left the DZ. The ID of the vehicle will hence be removed from the ranking list, and the ranking list will be re-ordered to include all vehicles in this DZ in the descending order of their credibility.

Through the above steps, R completes the process of vehicle ranking in each DZ based on their credibility.

C. Selection of Reporting Vehicles

Once the m vehicles belonging to the same DZ are ranked, R selects m' $(m' < m)$ vehicles as event reporting vehicles in this DZ. The first vehicle selected is the one on top of the ranking list. To select the remaining $(m' - 1)$ reporting vehicles, R not only refers to vehicles' credibility but also takes into account whether vehicles interfere with those selected reporting vehicles. In another words, R assigns a weight to each vehicle that has not been selected as a reporting vehicle. The weight of the ith non-reporting vehicle is expressed by

$$\omega_i = \frac{C_i}{\sum_{j=0}^{l-1} I_{i,j}}, \tag{1}$$

where $i \in [0, n-l-1]$, l is the number of currently selected reporting vehicles, C_i is the credibility of the ith non-reporting vehicle, $I_{i,j}$ is the interference index which indicates the interference relationship between the ith non-reporting vehicle and the jth reporting vehicles. If the ith non-reporting vehicle may interfere with the jth reporting vehicles, $I_{i,j} = 1$; otherwise, $I_{i,j} = 0$. The vehicle with the largest weight is selected a new reporting vehicle.

The weight of a non-overlapping vehicle may need to be updated when a new reporting vehicle is selected, as the interference index (in (1)) of this non-overlapping vehicle may changed if the new reporting vehicle transmits. At each time when the weights of all non-reporting vehicles are updated, R selects a non-reporting vehicle with the largest weight as a new reporting vehicle until m' reporting vehicles are selected. Then, in a similar way, R selects m' reporting vehicles for another DZ. Once all DZs have m' reporting vehicles selected, R completes the reporting vehicle selection procedure. The reporting vehicle selection procedure is periodic, following the periodic vehicle-zone allocations and vehicle ranking, because the relationship between vehicles and DZs is dynamic during vehicles' movement. When deciding the length of such periods, vehicles' driving speeds, the size of DZs, and the period of the Hello message should be referred to.

IV. Simulation Evaluation

In this section, by using NS2.35, we evaluate the following four schemes.

- The blockchain-based trust management (BCTM) [4]. It requires all vehicles that detect accidents/events to broadcast the incident reports to the RSU. The RSU aggregates the received reports and generates a trust rate for each event.
- VMS-BCTM. It applies the proposed VMS to BCTM to reduce the vehicle transmission interference.
- The neighborhood-based trust management (NBTM) [2]. It requires vehicles near to accident/event places to send event reports. The RSU to determine the trust levels of event reports based on the the credibility of reporting vehicles.
- VMS-NBTM. It applies the proposed VMS to NBTM to reduce the vehicle transmission interference.

We compare these four schemes along the two performance metrics below.

- Report loss rate (RLR). When multiple nearby vehicles send reports to their RSU simultaneously, reports generated by trustful vehicles may be lost due to transmission interference. A large RLR means that reports from trustful vehicles may be dropped, causing a wrong decision making at the RSU and hence affecting the trust management of a vehicle network. We calculate RLR by $RLR = \frac{R_t - R_r}{R_t}$, where R_t is the number of vehicles that send a report and R_r is the number of reports received at the RSU.
- Average report delay (ARD). A report delay refers to the time period from a vehicle sending this report to the RSU receiving this report. The average report delay is calculated by $\frac{\sum_{i=0}^{m-1} RD_i}{m}$, where m is the number of vehicles sending a report in a DZ and RD_i is the delay of the ith vehicle's report. Shorter ARDs are crucial for the RSU to make timely decisions.

The major parameters employed in our simulations are listed in Table I.

a) Evaluation of Report Loss Rate (RLR): we observe the RLR performance changes after increasing the number of vehicles from 3 to 23 for each DZ. As illustrated in Fig. 2, we evaluated four schemes that we listed above. BCTM generated the highest RLRs due to all vehicles inside the DZ

TABLE I
NS2 SIMULATION PARAMETERS

Parameters	Values
MAC standard	802_11
Antenna	OmniAntenna
The size of Hello or Report packets	100 bytes [11], [12]
The interval of Hello packets	100 ms [12]
Wireless bandwidth	1Mbps
The accurate detection range of vehicles	100 meters [13]

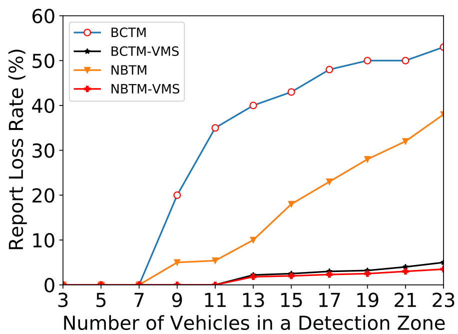

Fig. 2. Analysing the report loss rates by increasing the number of vehicles.

to broadcast a report to the RSU. Followed by NBTM, when DZ is not dense, RLR is not very high, but as the number of DZ vehicles increases, RLR is also increasing. In contrast, VMS-BCTM and VMS- NBTM minimise the RLR between 0% and 5% after increasing the number of vehicles in DZ. Such a significant improvement is because VMS considers the interference domain when selecting a vehicle. This approach reduces RLR caused by interference.

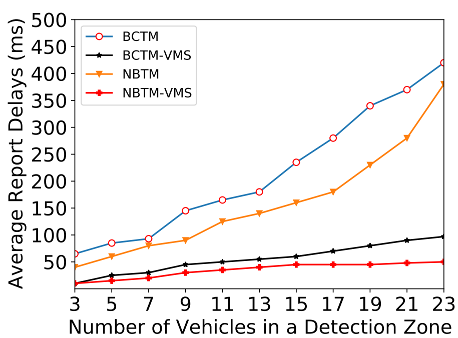

Fig. 3. Analysing the average report delays by increasing the vehicle density.

b) Average Report Delay (ARD): Fig. 3 shows how ARDs can be affected by vehicle density. The contention between these simultaneous reporting causes delays in delivering reports to the RSU. This is because the reporting vehicles in the same carrier sense need to check the channel status if it senses the channel state is busy. The reporting vehicle will wait until the line is idle for transmission, which will increase the transmission delay. The results show that as the number of vehicles in DZ increase, the ARDs of all four schemes increase. BCTM always generates the longest ARDs because all vehicles need to broadcast reports to the RSU. NBTM achieves slightly shorter ARDs (increasing from 40ms to 380ms) because less contentions take place between vehicle reporting activities, since only 50% vehicles send event reports with NBTM. For VMS-BCTM and VMS-NBTM, they both employ 30% vehicles to report events, helping them to achieve shorter ARDs than BCTM and NBTM. Between VMS-BCTM and VMS-NBTM, VMS-BCTM has slight longer ARDs because it asks more vehicles to report events than VMS-NBTM does.

V. CONCLUSION

A trustworthiness assessment is a key step to guarantee the security and reliability of information transmission in vehicle networks. Transmitting reports with short latency and low report loss rates in vehicle networks is the main issue that we explore in this letter. We present a vehicle message scheduling algorithm for the vehicle trust management system. With the aid of this solution, the existing trustworthiness solutions can achieve low latency and low loss rate when sending an incident report in the high-density area. The experiment results show that our vehicle message scheduling algorithm can surely help a existing trust management scheme to reduce (use the full term of ARD and RLR). Our next step is to optimise the propose scheme as well as take further security issues (*e.g.,* Sybil attacks or self-promoting attacks) into account.

REFERENCES

[1] J. Shen, C. Wang, J.-F. Lai, Y. Xiang, and P. Li, "Cate: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 213–11 226, 2019.
[2] C. Wang, L. Xiao, J. Shen, and R. Huang, "Neighborhood trustworthiness-based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 21, p. e4643, 2019.
[3] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in vanets," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, 2013.
[4] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.
[5] W. Tu, "Efficient wireless multimedia multicast in multi-rate multi-channel mesh networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 3, pp. 376–390, 2016.
[6] S. Minelli, P. Izdpanah, and S. Razavi, "Evaluation of connected vehicle impact on mobility and mode choice," *Journal of traffic and transportation engineering (English edition)*, vol. 2, no. 5, pp. 301–312, 2015.
[7] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25 408–25 420, 2017.
[8] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A survey on trust evaluation based on machine learning," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–36, 2020.
[9] B. Toghi, M. Saifuddin, M. Mughal, and Y. P. Fallah, "Spatio-temporal dynamics of cellular v2x communication in dense vehicular networks," in *2019 IEEE 2nd Connected and Automated Vehicles Symposium (CAVS)*. IEEE, 2019, pp. 1–5.
[10] E. Murakami and D. P. Wagner, "Can using global positioning system (gps) improve trip reporting?" *Transportation research part c: emerging technologies*, vol. 7, no. 2-3, pp. 149–165, 1999.
[11] M. A. Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for vehicular sensor networks," *Computer Networks*, vol. 137, pp. 27–36, 2018.
[12] T. ETSI, "102 637-2 (v1. 2.1): intelligent transport systems (its) vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *Vehicular Communications*, 2014.
[13] Y. Luo, J. Remillard, and D. Hoetzer, "Pedestrian detection in near-infrared night vision system," in *2010 IEEE Intelligent Vehicles Symposium*. IEEE, 2010, pp. 51–58.