Wireless Personal Communications (2019) 105:121–143
https://doi.org/10.1007/s11277-018-6106-6

A Trust Scheme Based on Vehicles Reports of Events in VANETs

Jie Wan[1] · **Xiang Gu**[1] · **Jin Wang**[1] · **Liang Chen**[1]

Published online: 1 January 2019

Abstract
In this paper, we propose a scheme allow vehicles in a Vehicular Ad hoc Network share running information among them. We developed a mechanism that can help a vehicle to judge the trustworthiness of a message. We classify information into two types: one is emergency warning message, and the other is event reporting message. By collecting reports from other vehicles who pass through the place where an event occurs on claimed by a message, a vehicle can make a decision whether the message is true or false by using algorithms proposed in the paper. Simulation experiments show the scheme can work well and efficiently. The scheme can resist certain attacks that are hardly identified by other schemes as it avoids using vehicle's ID. It can also protect a driver's privacy in some extent which is a hot issue in recent research.

Keywords VANETs · Reputation · Trust mechanism

1 Introduction

With the development of economic and technology, Motor vehicle has become the main daily transport tool for almost everybody worldwide. But this also arises the risk of traffic injuries. It is estimated that motor vehicle collisions caused the death of around 60 million people during the twentieth century around the same number of World War II casualties. Moreover, road traffic crashes are predicted to result in the deaths of around 1.9 million people annually by 2020 if no action is taken [1]. Recently, many researchers focused on the development of intelligent transportation systems (ITS) to offer a safe, convenient and comfortable trip by using latest technologies such as wireless communication, sensors and actuators, global position system and smart terminals etc. A vehicle equipped with such hardware and software can inform and help drivers to avoid accidents on road or even control the vehicle when some emergencies happened suddenly.

Communication technology is the key component of ITS. Communications among entities on road are usually divided into two types, which are Vehicles to Vehicles (V2V) and Vehicles to Instruments (V2I). Entities are connected to each other to form

✉ Xiang Gu
gu.x@ntu.edu.cn

[1] School of Computer Science and Technology, Nantong University, Nantong 226019, China

a wireless network called Vehicle Ad Hoc Networks (VANETs), which are spontaneously created for data exchanging. Many types of applications can be implemented over VANETs, such as electronic braking, platooning and traffic information system [2].

Automatic drive is another application which may bring revolutionary changes to peoples' driving mode and it is now under development by many companies. Some well-known automobile manufactures have already embedded some early versions of auto-drive systems into their products such as the new 2014 Mercedes-Benz S-Class.

All those applications require high quality communication. There are two basic aspects to evaluate the quality level of communication among vehicles. One is reliability and the other is trustworthiness. Reliability denotes a message will be definitely received by the correct receiver once a vehicle sends it out. Trustworthiness refers to the content of a message is true. Attackers often intend to damage a VANET by these two aspects. Here as, in this paper, we aims at developing a mechanism that is able to address the issues caused by malicious attacks from the second aspect, that of the trustworthiness.

Attackers or malicious drivers may send out false information to fool other drivers and to mislead them alter their driving route. The purpose of these attacks can be making a mess on road, or reducing the number of vehicles before them to facilitate their own trip selfishly.

In order to protect the normal operation of a VANET and to resist false information injecting attacks, some trust mechanisms or reputation systems are proposed which we will discuss in detail in Sect. 2. The target of these systems is to find out dishonest drivers and false messages, to courage honest behaviors and to punish malicious behaviors.

Most trust mechanisms are based on historic data to build up a trust model. They observe their neighbors communication behaviors and infer those neighbors' actions in the future. There is a basic principle in their inference that a good vehicle may continue its good behavior in a high probability. Though those mechanisms can identify malicious vehicles and messages, they themselves become targets of new attackers. Some common attacks can be:

New comer attack: an attacker changes its ID and pretends to be a new comer to join into a VANET. It tries to wipe away negative records about it in this way [3].

Sybil attack: an attacker publishes many false messages by using different IDs. It tries to mislead others to believe that messages are sent out by different vehicles and thus the content of those messages are trustable [4].

Bad mouth attack: this kind of attack aims at a trust mechanism itself if the mechanism allows other neighbors to recommend their trust value about a vehicle under testing. An attacker may provide unfair high or low value to harm the mechanism [5].

Generally speaking, a practical trust mechanism should be able to resist those common attacks. Furthermore, it should also be able to deal with challenges which are caused by VANETs' features.

The first challenge is that the VANET is highly dynamic. As roads are always accessible from all directions, vehicles can join or leave a VANET easily almost at any time. This feature causes the topology of a VANET is doomed to be unstable.

The second challenge is that the connection between two vehicles is volatile and transient. Due to different speeds and directions, once the connection is broken, it can seldom be set up again in the future.

The third challenge is privacy protection. VANETs do bring convenience and safety to us, but it may also leak personal information unwittingly. An adversary can infer privacies of a driver by collecting information he sends out.

This paper is structured as follows. In Sect. 2, related works on trust mechanism among VANETs are discussed. In Sect. 3, our scheme is presented in detail. Section 4 evaluates the efficacy of our scheme. Section 5 demonstrates results of simulation experiments and proofs the scheme can work well. After that, this paper is concluded in Sect. 6.

2 Related Work

Many trust models in VANETs have been proposed in recent years. Those models can be organized into three categories: entity-oriented models, data-oriented models and combined models [6].

1. Entity-oriented models focus on vehicles themselves. Messages will be trusted if the vehicle which publishes them is trustable.

Li et al. [7] proposes an announcement scheme for VANETs based on a reputation system. All vehicles in a VANET have their reputation scores according to the reputation system. A vehicle's score is calculated by other vehicles according to its behaviors and is stored in a remote center reputation server. When a vehicle wants to publish a message, it must attach its reputation score that is digitally signed by the server to the message. The receivers will check this score and then trust it if its publisher's score is higher than a preset threshold. The authenticity of a message will be verified in the next tour and the result will influent the publisher's reputation score stored in the server.

Wei and Chen [8] proposes a reputation-based global trust establishment scheme. A reputation management center (RMC) is in charge of monitoring and calculating the vehicles' reputation value in a VANET. All vehicles send their observation about their neighbors to RMC. RMC utilizes central limit theory, which is a statistic principle to exclude those unreasonable observations and then get the reputation value of each vehicle. When a vehicle receives a message, it will consult RMC for the publisher's reputation and then determine whether to trust it or not.

The model in [9] is relying on the opinion of the last forwarder and delayed verification of the exchanged messages. When vehicle 'A' receives a message forwarded by vehicle 'B', it will multiple B's opinion by the trust value which A gives to B to form A's opinion to the message. This opinion is also the important basis for A to make decision whether to forward the message or not. Then this opinion will be verified later and the trust value of B will be adjusted according to the verification.

Minhas et al. [10] develops a multifaceted trust model that incorporates role-based trust, experience-based trust and majority-based trust. When a node receives a message, it will consult to nodes stored in a local matrix ordered by their roles and experience. Responses from those nodes will be used to calculate the trustiness of the message. And the nodes' order in the matrix will be adjusted according to how well their opinion consists with the calculation result. This model does not consider the highly dynamic feature of a VANET. Two vehicles may have little chance to exchange their information more than twice due to their different speeds and directions. The topology of a net is unstable and the link between two nodes is easy to be broken. These features make the stable communication among nodes in the matrix be a problem.

2. Data-oriented models focus on the content of the message. The author of Raya et al. [11] points out this method may be more suitable than others for an ephemeral network such as a VANET. Voting, D–S evidence theory and Bayesian method are common analysis tools in these kind models.

Dotzer et al. [12] proposes a VANET reputation system named VARS. In this system, every node which forwards a message will append its own opinion about the message's trustworthiness to the message, which is called opinion piggybacking. This opinion is generated from experience if the event contained in the message is detected by forwarder itself, from partial opinions attached to the message. The system is partly like a voting system. The majority opinion has more possibility to be adopted.

The main disadvantage of such approach is that the earlier opinion will have more influence as it has been recursively considered by later nodes. To address this issue, [13] proposes an improvement method. Each vehicle has different voting weight according to its distance from the original event. Vehicle that is closer to the event will have a higher weight. The distance is measured by hops in its algorithm. The opinion of a vehicle which observes the event directly will be given a weight as one, whereas a vehicle's opinion will be given a weight as α^n if the message has been forwarded n hops, here α is a preset discount factor.

Chen and Wei [14] uses Dempster–Shafer evidence theory to combine multiple messages about the event from different neighbors. It retrieves the sender's location from the beacon message, in order to examine whether the claimed event's location is trustable or not. The shortcoming of this method is that collecting messages about the same event from a vehicle's neighbors is time costly, so it is not suitable for a real-time application.

Wang et al. [15] models an urban map as a directed weighted graph. Each road segment is associated with a travelling time parameter as its weight. Every vehicle who passes through the segment reports its passing time to others. Each vehicle has a local database to store those road segments passing time. When new messages about the same segment are received, a vehicle uses Bayesian method to choose one message to update its local database.

3. Combined model is a hybrid model of entity-oriented and data-oriented model. When it judges the trustworthiness of a message, it takes the message sender's reputation and the content of the message into account at the same time.

Chen et al. [16] designs a mechanism to control the propagation of messages. It allows a vehicle to relay a message if the message is verified to be trustable or discard a message otherwise. A message is believed or disbelieved by vehicles on its propagation route. A vehicle collects those opinions and multiple them by corresponding vehicles' trust value. The trust value of a vehicle is based upon its role and its past behaviors. The mechanism compares the result with a predefined threshold. The more vehicles with high trust value believe the message, the higher probability the message will be accepted and delayed.

Koster et al. [17] categories information sources as many types, such as GPS-based path planning services, government authorities, digital information boards on freeways and vehicles on roads. It looks all vehicles as one united source whose trust level is the same as others. Then it calculates an event trust value which is generated by one or multiple sources according to a certain algorithm: if the event is reported by a single source, its trust value is calculated by synthesizing entities trust values among that source and trust values they

give to the event; if the event is reported by multiple sources, its trust value is the average of every single source's result. The paper uses Believe–Desire–Intention (BDI) framework to consider uncertainty of entities' believes.

Gerlach [18] considers that the daily route of a vehicle is always fixed and then RSUs it communicates with every day are also fixed. Those RSUs forms a VR (Virtual Ring) to store vehicles' reputation value in a distributed mode. When a vehicle receives a message, it can ask the VR for the generator's reputation. This is the method which is oriented to entity. If there is no response in a certain time, the vehicle will start the procedure to judge the trustworthiness of the message which is oriented to data.

In [19], entity is not a vehicle but a road segment. It divides a city into several neighbors and each neighbor contains many segments. A vehicle knows regular trust values of each segment in different time periods (for example, busy time period and idle time period), especially those segments which it often passes by. The basic trust values of a segment are calculated according to β distribution. When a vehicle receives a message about a segment, it compares it with its knowledges. If they are consist with each other, the message will be accepted. Otherwise, the vehicle will start a procedure which is data-oriented to judge the message and then modify its knowledge about the segment according to the judging result.

Privacy protecting is a hot issue which raises researchers' concerns in recent years. Most trust models in VANETs use vehicles' IDs during communications. It makes it possible to track a vehicle's behavior and route by analyzing messages which contains the pointed ID. To solve that issue, many methods are proposed and the most common one is to change a vehicle's ID frequently. [15, 16] discusses how to use pseudonyms and the method to change one's ID to make sure the information of a vehicle will not be got by unauthorized adversary in detail.

3 Trust Scheme

In this section, the trust scheme is described in detail. The scheme is decentralized and it focuses on event reporting mechanism. A vehicle may know whether an event is trustable or not by collecting all messages about the event.

3.1 Framework of the Scheme

The only entity in our scheme is vehicle itself. Road side units (RSU) and center servers are common facilities which are widely used in other papers. They may bring convenience to build up trust relationship among vehicles on roads in centralized reputation models. While considering the cost of base construction and the current situation of the road infrastructure, it can be inferred that intelligent transportation system on the base of vast RSUs may not appear in a short period. That's the reason why the scheme doesn't take them into account.

It is assumed that each vehicle involved in the scheme has been installed a kind of equipment named onboard unit (OBU). OBU refers to kinds of miniature embedded systems that can accomplish specific tasks. For example, OBU can be used for highway toll collection, location and navigation [20, 21]. A vehicle is assumed to have following capabilities with the help of OBU in this scheme.

It has wireless communication capability to send and receive messages, which enables communication with its neighbors directly. Here vehicle A is a neighbor of vehicle

B means A can send or receive message to or from B directly without forwarding by other vehicles. The maximum communication distance between A and B depends on the wireless communicating technology. In our scheme, Wi-Fi is embedded and the protocol is IEEE802.11p.

It is capable of planning a route to the destination with the help of the navigation & location system. It can change the pre-established route conveniently and quickly, according to the running state of the vehicle and the road condition it drives on. Furthermore it can judge whether a given coordinate is on the route that it will drive through or not. In the following section of this paper, such a coordinate is called in front of the vehicle.

It has capability to sense its position coordinate and speed in real time dynamically. But it is not guaranteed that all these data it sends out is true, as they may be tampered by a malicious driver.

It has sufficient computational capability and enough storage area to fulfill all algorithms proposed in this paper. It may but not necessarily has trusted hardware embedded into it to make sure no one can get or modify data stored in it even the driver himself. [7] mentions such hardware to perform cryptographic operations. By using the hardware, the position and speed data can be assumed to be true and then it can decrease the complexity of the scheme.

A vehicle only receives messages what are originally generated in front of it and then passes them to its upper layer. Otherwise it just forwards those messages according to the method described in Sect. 3.5 without any processing. That is to say, it ignores messages what are sent or forwarded by vehicles behind it. Relative position judgement between vehicle A and B can be implemented by the following method.

As Fig. 1 shows, assuming the coordinate of A at present is (x1, y1, z1), the coordinate of B is (x2, y2, z2). And a short time ago the coordinate of A' is (x0, y0, z0).

$$cos\alpha = \frac{(x2-x1)(x1-x0)+(y2-y1)(y1-y0)+(z2-z1)(z1-z0)}{\sqrt{(x2-x1)^2+(y2-y1)^2+(y2-y1)^2}\sqrt{(x1-x0)^2+(y1-y0)^2+(z1-z0)^2}} \tag{1}$$

If $\cos\alpha \geq 0$, vehicle B is in the front of A, else B is behind A. This judge method may bring a mistake in particular situation such as a sharp turning, as Fig. 2 shows. Such situation seldom occurs in urban area and in most highways. However, the misjudgment will not happen if there is a vehicle C between A and B. So the judge method is still acceptable.

The scheme assumes that all OBU in different vehicles that join into the vein can keep a relatively accurate global time. This can be achieved by time checking technology over Internet.

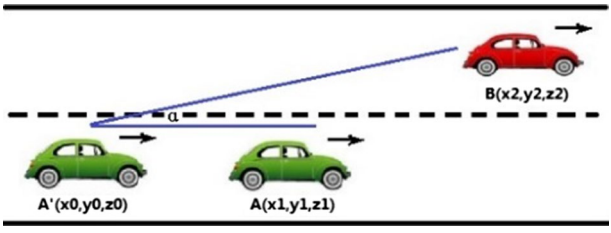


Fig. 1 Judgement of Front Position

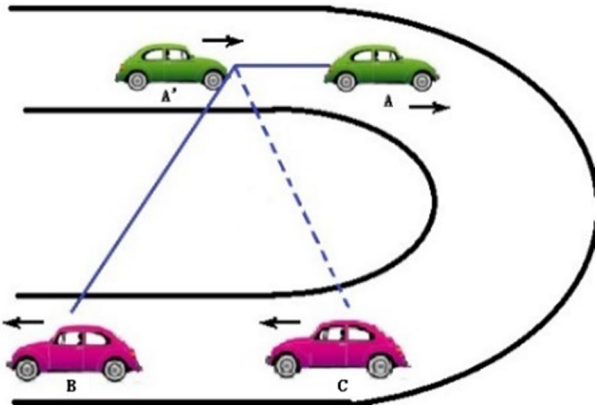


Fig. 2 Misjudgment of Front position

3.2 Messages

Messages in the scheme are classified into two types according to their different functionalities. One is emergency warning message (EWM), and the other one is event reporting message (ERM). Messages not related to this scheme are not considered.

Emergency warning messages encompass information such as vehicle braking, slowing down, turning, backing, lane changing and etc. These kinds of messages are always urgencies reflecting running state changing of a vehicle. They are used to inform the vehicles behind it to be aware of such alterations and to take proper corresponding actions as quickly as they can. Influences of EWMs are usually limited to a local place and they should be processed immediately. It is not necessary to judge whether the content of a EWM is true or not, as its impact is locally and momentarily. Furthermore a misjudgment may cause a disastrous result. The only factor should be taken into account is the distance between the original place of an EWM and the receiver. For example, a receiver may ignore an EWM if it occurs more than 200 meters away, otherwise the receiver should be aware and try to avoid a potential accident.

The structure of EWM is defined as EWM = {0, R, L, T, a_1 [, a_2,…]}, $a_{i\in}$ A,(i = 1,2,…), where '0' refers to an EWM message, R represents the road segment ID where it occurs, L denotes the location coordinate, T represents the time stamp when it happens, a1 represents the concrete content of an event. If more than one emergency events are taken place, events can be added to the back of a message, for example, a_2 is following a_1 in the previous expression of the EWM. Symbol '[]' means contents embraced by it are optional.

The meaning of a_i (i = 1,2,…) is advised to be pre-defined. All vehicles should obey the same definition; otherwise the content cannot be recognized by other receivers. An event set A should be build up carefully to make sure that all emergency events that may take place have already been included in the set. Each event in the set must be an atomic one, that is to say the event cannot be divided into smaller ones. The set is open and a new event can be added to it easily after seriously examining if necessary. The most frequently-occurring events will use smaller index numbers while occasionally events and new comers will occupy larger ones sequentially.

ERM contains two opposite types of events. The first one declares some events are currently occurring on the road, while the other indicates events that announced by former ERM is now disappeared. All events belong to the first type construct an event set E, and

all events belong to the second type form the set ¬E. Elements in two different sets have one-to-one mapping relationship. If there is one event e in set E, then there must be the only one anti-event ¬e in set ¬E.

Unlike EWM, ERM reflect the road condition rather than a vehicle running state. Those road conditions can be road blocking, accident on a road, maintenance of a road, abnormal climate around a road and etc. As road conditions are more complex than vehicle running states in this scheme, events in the set E need to be selected and designed more elaborately. It can be an atomic one just like EWM is, or it can also be a high-level one. For example, let event e_1 represents there is jam on the road, then $e_{1\text{-}1}$ can be used to represents the road is blocked entirely, $e_{1\text{-}2}$ represents vehicles can pass the road under the speed of 5 km, $e_{1\text{–}3}$ represents the speed of vehicles is under 10 km and etc. The lower level the event is, the more accurate conditions of the road it describes. Different level events can both be included in ERM. Just as it is mentioned before, anti-event $\neg e_1$ represents the road is clear at present. The meaning of events $\neg e_{1\text{–}1}$, $\neg e_{1\text{–}2}$ and $\neg e_{1\text{–}3}$ can be deduced in the same way. There is a little elastic in a such event designing method, a vehicle may not recognize event $e_{1\text{–}1}$, but it must know the corresponding higher level event is e_1 so it knows there is jam on the pointed road though it lost more details. The two ERM sets are also global uniform just as EWM set is.

The structure of ERM is defined as ERM = {1, R, L, T, $e_i|\neg e_i$}, $e_i \in$ E, ¬ei∈ ¬E. Here '1' represents it is an ERM message, R, L, T has the same meaning as EWM. The symbol 'l' means logic relationship OR. One ERM message carries only one event, it is different from EWM.

3.3 Database in OBU

There is a mini database in OBU to record necessary events that a vehicle receives. The structure of the database can be described as (R, $e_i|\neg e_i$, L, T, receive-Time). Symbols 'R', 'L', 'T', '$e_i|\neg e_i$' have the same meaning as they are in ERM. 'received-Time' represents the time when the record is inserted into the database. Item 'R' is the primary key and item '$e_i|\neg e_i$' is the secondary key of a record. All records in the database are sorted by these two keys.

The records in database are the most important basis to make decision whether a message is true. Some rules of the modification of the database are listed as following.

Only ERM can lead to the creation of a new record. An ERM that reports event e_i must be recorded if the road segment R included in the ERM is on the route of the vehicle and the event location L is in front of the vehicle. An ERM which reports event $\neg e_i$ on the road segment R will be recorded only if there is a corresponding record of event e_i on R in the database already. All other ERMs except these two situations will not be recorded. The database will never record any EWM.

All records indexed by R and $e_i|\neg e_i$ will be erased as soon as the event e_i on the R has been judged as true or false according to the scheme. These records will also be erased when the vehicle changes its route and the road segment R is no longer on its new route.

3.4 Message Publishing

In this paper, EWM and ERM are considered, any other messages are not taken into account in the scheme.

An EWM message can be generated and sent out at any time if necessary. It depends on the running state of a vehicle. State changing such as braking, lane changing etc. may leads to a EWM publishing automatically.

Same as ERM, an event in set E can also be generated at any time if a vehicle notices something happened on the road it passes by at present. For example, a vehicle may create a EWM message $E1=(1, R_1, L_1, T_1, e_1)$, which means there is traffic congestion on road segment R1 at time T_1. Then it will seek its local database to find out whether the event e1 on R_1 is recorded. The database is indexed by R and e_i as mentioned above. Event e_1 will be sent out at once if there is no such a similar record. Otherwise, OBU will inspect the latest record time that reports event e_1 on R_1 to determine whether a new ERM should be sent out or not. The interval time between two ERMs publishing of the same road state is recommended to be the time when the reporting vehicle can drive through 200 meters. This is a proper distance for a driver to observe ahead clearly.

The precondition of sending out an event $\neg e_1$ in set $\neg E$ is that there already exists a record of corresponding event e_1 in the database. In another word, publishing event $\neg e_1$ is triggered by a record of event e1. The interval time between two ERMs that report the same event $\neg e_1$ is the same as e1 reporting requirement.

Algorithm 1 demonstrates the procedure of messages publishing, as is described below.

```
Algorithm1:   Messages publishing
Input:        Event e in set A and set E|¬E
Output:       A EWM or ERW message or Null
1:   if (e ∈ A) {
2:     generate a EWM message eMessage=(0,R,L,T,e);
3:     send out E;
4:     }
5:   else if (e ∈ E) {
6:     if (exists records e in the database &&
7:        the latest time of records < 200/speed)
8:             return Null;
9:     else {
10:         generate a ERM message eMessage=(1,R,L,T,e);
11:       send out eMessage;
12:       }
13:    }
14:  else if (e∈ ¬E) {
15:    if (exists records e in the data base &&
16:       the latest time of records > 200/speed) {
17:       generate a ERM message eMessage=(1,R,L,T, ¬e);
18:       send out eMessage;
19:       }
20:  }
```

3.5 Messages Forwarding

An OBU deals different messages it receives with different forwarding strategies.

EWM messages will never be forwarded, which indicates a EWM message only has one hop live-time. A vehicle who receives a EWM message will reacts to it without forwarding it. It is reasonable because the running state changing of a vehicle is only meaningful to vehicles that are directly following it. A vehicle that receives a EWM message will generate and send out a new EWM message to inform vehicles directly behind it if the reaction leads to running state changing of it. A chain of EWM messages can be created under such situation, and the chain will not be broken given a vehicle keeps it's running state though it receives a EWM. It keeps its state may be just because it feels there is enough distance for it to avoid an accident. At this point, EWM messages chain stops propagating.

An OBU will forward an ERM message that contains an event e in set E it receives when all following conditions are met.

Firstly, the event e must be originally taken place in front of the vehicle that forwards the message. Here, the definition of "in front" can be expressed as formula (1). The OBU embedded in the vehicle will ignore all events behind it because it won't pass through those events points in a short time. Hence those events are insignificance to them. By this way, fewer broadcast messages will be generated and communication resources can be saved.

Secondly, the vehicle who will forward the message must be in the influence area of the event e. This is due to two reasons. One is that an event too far away is less meaningful to a vehicle. And another one is other vehicles pass through the event point later will publish new ERMs again if the road state reported by the ERM is kept without changing. Formula (2) gives out in which area vehicles should forward the event message.

$$(\alpha Range < (d \bmod Range) \leq Range) and (d < n\ Range) \tag{2}$$

In this formula, 'Range' is average communication range of an OBU; it depends on propagation model it used and topography around it. 'd' is the distance between the event place and the vehicle position. 'α' is a factor that ranges from (0,1); using 'α' can reduce the number of broadcast messages in the network. The value of 'α' is larger in sparse area than in urban area. 'n' is a factor that limits the maximum influence area of the event; the value of 'n' is smaller in urban area than in expressway area. Here we use times of communication range n instead of hops as is illustrated in [13]. It is because hops cannot express the size of an area precisely. The area will be smaller in high vehicle density areas whilst will be greater in sparse density areas.

Figure 3 shows the function of formula (2). Those vehicles in shadow should forward the event message.

Thirdly, there must be enough time intervals between two ERMs that report the same road segment state. It is recommended that the interval should be no less than Range/(m*average (vehicle speed)). The meaning of 'Range' is the same as described above. The value of parameter 'm' can be 1, 2, 3…. The bigger m is the lower interval time is. From

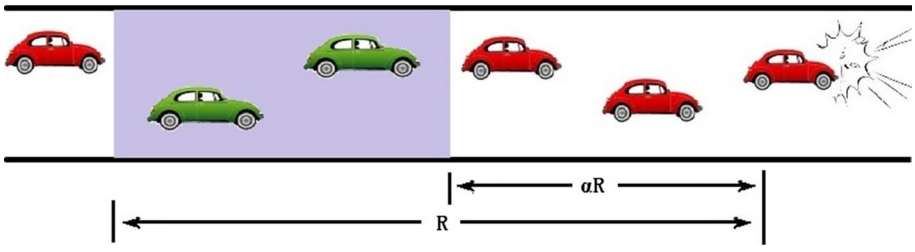


Fig. 3 The range of forwarding vehicles

simulation experiments, setting 'm' to 2 or 3 is proper to get the best output. This condition can help to avoid too many repeated ERMs in the network. Considering such a scenario, there is congestion on road segment A, and dozens of vehicles are jammed around A. According to the scheme, each vehicle sends out ERM message automatically until it passes through the point. As a result, dozens of ERMs what report the same event will be generated. The requirement of the minimum time interval can help to reduce propagation of these reduplicative ERMs. Another function of this condition is to avoid coordinated attacks. Though a number of malicious vehicles in a same area may publish the same false event messages at almost the same time, but only few of these messages will be propagated. Most of them will be lost due to lack of enough time intervals and the effect of the attack is weakened.

As to forwarding an event ¬e in set ¬E, there is the fourth requirement besides three conditions mentioned above. That is the opposite event e must already be recorded in the database on the OBU beforehand.

Algorithm 2 demonstrates the procedure of messages forwarding, as illustrated in the following algorithm

```
Algorithm2:   Messages forwarding
Input:        A EWM or ERW message
Output:       A ERW message or Null
1:   if (EWM)
2:       return Null;
3:   else if (ERM) {
4:      extract event e from the ERM message;
5:      if ((e∈ ¬E)&&(no corresponding event in set E))
6:          return Null;
7:       else {
8:          if ((event e is in front of the receiver) &&
9:              (the receiver is in the influence area) &&
10:             (the time interval is enough))
11:              forward the received ERM;
12:         }
13:  }
```

3.6 Message Receiving and Decision Making

When an OBU receives an EWM message which is published by a vehicle in front of it, it will trust it and decide whether to react to the message or not, depending on the distance between the message generator and itself. The purpose of an EWM message is to warn drivers behind it to be aware of potential accident. The effect of such a message is instantaneous. A malicious EWM message will not bring any damage to other vehicles because drivers of those being cheated vehicles will soon adjust their driving behavior after they realize the event that declared by a malicious EWM does not take place. On the other hand, there is no enough time to judge whether an event included in an EWM is true or false as an EWM usually reports an urgent event and needs to be reacted immediately.

When an OBU receives an ERM message, it checks it firstly. Those messages which could not pass check will be ignored and discarded directly.

There are three steps to check an ERM message. The first step is to check the parameters included in the ERM. Does the road segment 'R' consist with the location coordinate 'L'? A malicious vehicle may publish a false ERM message which claims a false road segment state at other place. By checking the consistence between 'R' and 'L', such malicious message can be detected. Does the location 'L' consist with the time 'T'? A malicious vehicle may modify its location coordinate to avoid being detected. By estimating the propagation time delay as [19] mentioned, such a malicious behavior can also be detected.

The second step is to check whether the point where the event is taken place is in front of the receiver. The vehicle will ignore an ERM message behind it.

The last step is to check whether the receiver will drive through the point later. As was mentioned in 3.1, an OBU plans a route to the destination at the beginning of the journey, so it knows all road segments it will drive through in the rest of the trip. If the road segment reported by an ERM message is not in the list of the route, the vehicle will ignore it.

These three steps are executed one by one. Once one step cannot be passed, the rest steps will not be executed and the total result is false.

An OBU will begin to process an ERM message after the message has been passed through the check. If the event included in the message is the first time to be received and it belongs to the set E, the OBU will record it in the local database and then begin to start decision making procedure. Otherwise the event will be recorded according to 3.3 descriptions.

The procedure of message receiving is described in Algorithm 3.

```
Algorithm3:   Messages receiving
Input:        A EWM or ERW message
Output:       Updating of the local database
1:   execute algorithm2 to forward the message;
2:   if (EWM)
3:      react to it;
4:   else if (ERM) {
5:      if (Parameters in the ERM are not consistent)
6:         exit;
7:      else if (EWM happens behind the vehicle)
8:         exit;
9:      else if (R in the EWM isn't in the route)
10:        exit;
11:     if (e ∈ E) {
12:        if (e doesn't exists in the local database) {
13:           start decision making procedure by
14:           starting a timer;
15:        }
16:        else
17:           update the record in the local database;
18:     }
19:     else if (e ∈ ¬E) {
20:        if (corresponding event in the set E
21:           does not exists in the local database)
22:           exit;
23:        else
24:           update the record in the local database;
25:     }
26:  }
```

Decision making procedure can be divided into two stages. The first stage is collecting all ERMs about event e |¬e and updating the local database. The second stage is making a judgement whether the event e is true or false. An OBU will finish the first stage and then turn to the second stage when the timer set in algorithm 3 line 17 is up or the OBU has already collected enough ERMs about event e|¬e. The procedure will also be cancelled when the vehicle passes through the road segment under determined.

The judgement is made according to all records of e|¬e in the local database. Suppose there are n records of event e and m records of event ¬e in the database. Assuming time is expressed as a integer number, the scheme marks receive-time of n records about event e as $t_1, t_2,\ldots, t_n$, and receive-time of m records about event ¬e as $\neg t_1, \neg t_2,\ldots, \neg t_m$. The event e can be trusted if the result of formula (3) is true, otherwise the event is false.

$$\sum_{i=1}^{n} t_i > \sum_{i=1}^{m} \neg t_i \tag{3}$$

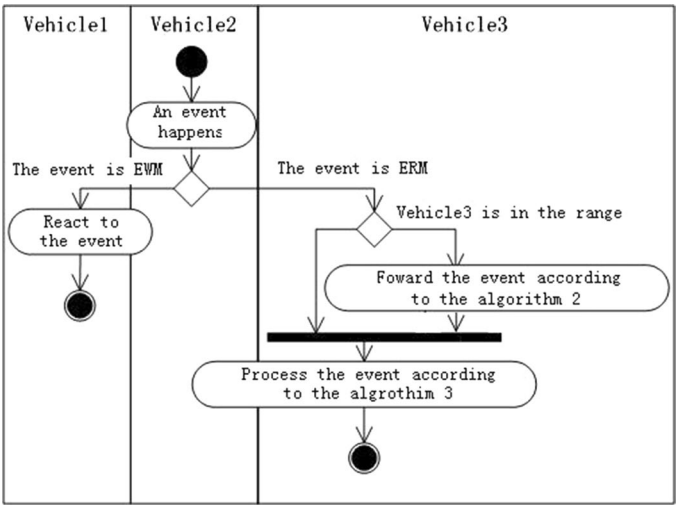


Fig. 4 Activity diagram of message publishing and processing

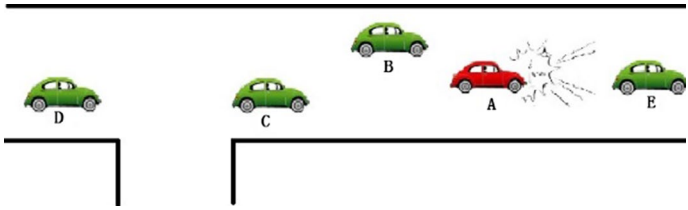


Fig. 5 Regional one way character

The formula implies that the latest ERM has more impact to the result as its receive-time is larger than old ERMs. This is consistent with the common sense that a fresh message is more valuable.

Figure 4 shows a brief flow of message publishing and processing procedure.

4 Scheme Analyses

In this section, we will introduce the feasibility of the scheme and demonstrate why it can resist some common adversary attacks.

Let's suppose vehicles that will pass through a pointed road segment marked as 'R' are all honest at the beginning of analysis for simplification. If there is no event happens on R, no message is to be generated. Now assuming something happens on R and a vehicle named A which firstly reaches the scene sends out the first ERM message to announce the event. A vehicle named B which is closely behind A receives the message, as Fig. 5 demonstrates, and then starts the decision making procedure as algorithm 3 line 17 in Sect. 3.6 describes. But because of lacking more ERMs to confirm the event, B will keep its direction and it will also arrive at R after a short time. If B is more than 200 meters from A, it will announce the same event to inform vehicles behind it as algorithm 1 that described in

Sect. 3.1. If the distance between A and B is less than 200 meters, it assumes another vehicle C will implement the same work. After that, vehicle D will receive at least two ERMs and formula (3) can work then.

In Fig. 5, vehicle B is a victim because it has no choice but to keep its direction to find out the truth of the event due to lacking of enough ERMs. D may encounter the same condition if B is too close to A. In practice, a vehicle cannot change its route arbitrarily at any time due to a road has always one direction in a local area. In Fig. 5, only D can make a turn as there is a cross in front of it. B and C must go ahead even they are informed an accident ahead of them. Therefore victims exist in the scheme is reasonable and acceptable.

The scheme stipulates that a vehicle can only publish an event that has already encountered. This rule prevents a malicious vehicle getting profit by publishing a false event. The location it wants to cheat others to believe something happens on will be behind it very soon. The only way to benefit from cheating is to tamper the road segment and the location coordinate in an ERM message. But such a malicious ERM message will fail to pass the check as discussed in Sect. 3.6.

Now let's add a malicious vehicle into the scenario. As Fig. 5 illustrated, A is a malicious one and it sends out a false event e on R that does not exist. Vehicle B, C and D receive this message and then start their decision making procedure. But because there is no more ERM messages to support the event e, the formula (3) will not be satisfied. When B, C and D drive through R, the decision making procedure will be cancelled as 3.6 mentions. That is to say, a single malicious event will be harmless in the network according the scheme.

What will happen if A sends out a false event ¬e? Such false message will not be taken into account by other vehicles unless they already received an opposite event e a short time ago. Then assuming event e did happen and vehicle E in front of A sent out an ERM to report it. Vehicle B may be cheated by false ¬e if not considering time interval requirement. Once B is cheated, it will keep its direction and then send out an event e once more to deny ¬e when it arrives at the R. And then C and D will realize the truth and make the right decision according to formula (3). Under such scenario, a misjudgment happens one time, but it is acceptable if local one-way directionality feature of a road segment is taken into account as we mention before.

Now add more malicious vehicles into the scenario. Some malicious vehicles whose locations are usually adjacent to each other may execute a collusion attack together. Those attackers will publish the same false event together or one by one in a collusion attack. Nevertheless, most of those malicious ERMs will not be forwarded due to time intervals among them cannot meet the requirement as algorithm 2 describes. Other vehicles in the direct communication area with those attackers may be cheated as algorithm 3 describes. However because their locations are near the place on where malicious ERMs announce the false event happened, they will soon find out the truth and then send out opposite events to inform vehicles behind them to avoid being cheated. That is to say, the negative affection of such an attack is limited to a small area according the scheme. On the other hand, attackers can get little profit from such an attack because they can only publish the event where they are on, the intension to execute the attack will be reduced.

The scheme avoids using vehicle's identifier and this will bring many benefits.

The most import benefit is that privacy of a vehicle can be protected. As we mention in part 1, privacy problem is caused mainly because a vehicle cannot join a network and take part in communication anonymously. A driver's personal information may be revealed by tracking information he sends out. But without ID, such tracking will be impossible because a tracker cannot identify who sends out the information on earth it captures.

Other benefits are many attacks based on ID in most trust mechanisms can be avoided such as Sybil attack, on–off attack, bad-mouth attack etc.

Under Sybil attack, a vehicle sends out a lot of false messages to other vehicles by using different fabric IDs. The attack simulates a lot of vehicles to report the same false event and tries to trick others to trust it. The core method of the attack is to act as multiple vehicles with different IDs. In our scheme, no ID is included in ERM messages. A malicious vehicle can only continuously send out false ERMs if it wants to execute Sybil attack. Then, most ERMs will be ignored due to their short time intervals. Furthermore, ERMs will be regarded as different events if an attacker passes through more than one road segments while it is executing the attack, and thus attacking affection is reduced.

When a malicious vehicle executes on–off attack, it alternates its role from a good rule observer to a violator time to time. Good behaviors are used to cover malicious actions to keep its reputation in the veins. In our scheme, such attack is nonsense without an ID. The trust calculation mechanism is totally different.

Bad mouth attack is also a kind of attack which needs to be addressed seriously in a reputation mechanism. An attacker may follow the communication protocols loyally but downgrade other vehicles' trust value arbitrarily to damage the reputation system of a network. But because our scheme does not use vehicles' ID, so it is impossible for a malicious vehicle to voice its opinion about another vehicle to others. Hence, bad mouth attack is unavailable in our scheme.

Lacking of ID information in messages makes it is difficult to implement point to point transmission. While considering messages in the scheme are all informing messages that must be broadcasted, this shortcoming is consequently forgivable and acceptable. As the main transmitting mode of the scheme is broadcast, some measures are adopted in order to decrease the number of messages in a vein.

As formula (2) shows in 3.5, only vehicles in particular area are allowed to forward messages. The decreasing of forwarding vehicles will reduce the duplicates of an ERM message accordingly. The larger parameter α is, the more area is allowed, and then the more vehicles may forward the message. The value of α must be selected carefully according to the current traffic state on roads. And it can be adjusted automatically by a vehicle itself. It is not required that the value of α is kept to the same value among the network.

The time interval embedded in Algorithm 2 is also a method to decrease the number of broadcast in the network. If an ERM is too close to a previous one, it will not be forwarded.

Only messages generated in front of a vehicle will be forwarded as 3.1 describes. This can also help to reduce the number of duplicates. Those messages which come from behind will just be ignored.

5 Simulation Experiments

In this section, we implement some simulation experiments to verify the effectiveness of our trust scheme. The experiment environment is constructed by OMNet++ (version 4.6), SUMO (version 0.21.0) and Veins (version 3.0). We choose OMNet++ as a basic network simulation platform which is an extensible, modular, and event-based simulator. SUMO is an open source, microscopic and space-continuous road traffic simulation. It is used to simulate vehicles' driving behavior, such as speeding up, speeding down, braking, lane turning etc., and road traffic in our experiments. Veins is an open source framework for running vehicular network simulations which is based on OMNet++ and SUMO.

We utilize the map of Nantong city, Jiangsu Province China from Open Street Map project, where a snapshot of its area is shown in Fig. 6.

The scenario is simulated as a series vehicles drive from Nantong government center to school of computer science and technology in Nantong University. The optimal route is marked using red line in Fig. 6 where road condition is the best, where vehicles can drive through with higher speed in those road segments. There also exists many side passes on which speed limit is much lower than the optimal one. For example, a route marked as yellow line is an alternative route. When optimal route is jammed, vehicles can turn to those side passes that drawn as black lines in Fig. 6.

We put three traffic lights on the map to simulate traffic congestion. If a vehicle stops more than 30 min, it will believe the road segment is jammed and then tries to change its routes. When traffic lights do not work, road segments are always clear for traffic.

Our simulation experiments use 802.11p as communication protocol and two-ray ground model as signal propagation model [22]. Main parameters of these experiments are listed in Table 1.

In order to verify the feasibility of our scheme, we compare the number of nodes which are cheated by malicious messages during their trip using our scheme with the result that does not using any trust mechanism. In this scenario, the traffic lights do not work.

As Fig. 7 shows, the number of being cheated nodes increase quickly with the growth of malicious vehicle rate. When the rate of malicious rate is greater than 30%, more than 90% vehicles will be cheated. While by using our scheme, even the malicious node rate is as high as 50%, the rate of being cheated nodes is still lower than 10%. The result shows that our scheme is feasible and effective. Though there is still no accurate survey on driver's behavior yet, [23] reports that 40% drivers cede way at intersections when they do not have to. According to that data, we believe about 40% drivers on road are altruistic and assume at least another 10% drivers are neutral. Therefore, the highest rate of malicious vehicles is set as 50% in these experiments. And because a vehicle is assigned to be a malicious role randomly in our experiment, the scenario has higher probability to generate more than two

Fig. 6 Map for simulating VANET

Table 1 Parameters for vehicular network simulation

Parameter description	Value
Total number of vehicles	300
Interval starting time between two vehicles	20 s
Approximate distance of the route	2600 m
Maximum speed of a vehicle	14 m/s
Maximum speed limit on high street	20 m/s
Maximum speed limit on side pass	10 m/s
Transmit power of the radio	20mW
Sensitivity to pick up signal	− 89 dB
Environment-dependent path loss exponent	2
Carrier wave frequency	5.89 GHz
Rate of malicious vehicles	0–50%
Maximum interval time between two malicious behavior	60 s

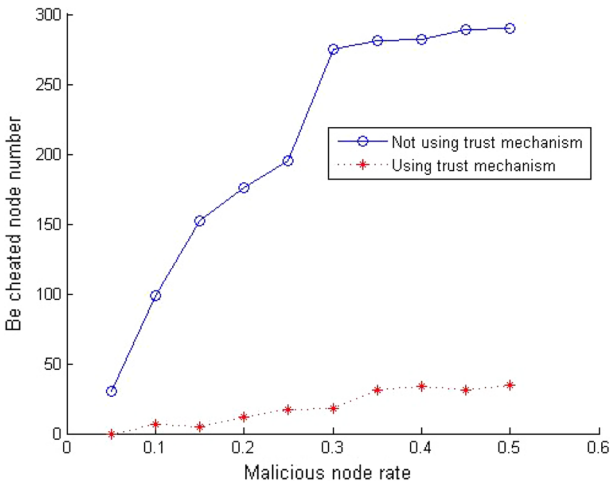


Fig. 7 Comparison of being cheated node number

malicious vehicles continuously when the malicious rate reaches 40% or higher. This offers opportunity for malicious vehicles to perform a collusion attack and in experiments we do observe collusion attack happens: more than two vehicles publish the same event almost at the same time at the same road segment. The result shows our scheme can resist this attack in some extent as is demonstrated in Sect. 4.

Reducing CO_2 emission of vehicles is a meaningful issue to enhance air quality around cities. We compare CO_2 emission of vehicles under two scenarios, one is using our trust scheme and another does not use. We adopt CO_2 emission computation model in experiments as [24] proposes. From Fig. 8, we can see that CO_2 emissions of vehicles using our scheme are more uniformly and lower. This is because vehicles that do not adopt trust mechanism are more easily to be cheated to change their route to low grade roads and has to spend more time to finish their trip and then more CO_2 is emitted accordingly.

The decision making time that mentioned in Sect. 3.6 has a direct impact on judgments' accuracy. Figure 9 shows the accuracy increases with the growth of waiting time period before making the decision. This is reasonable because with the extension of waiting time,

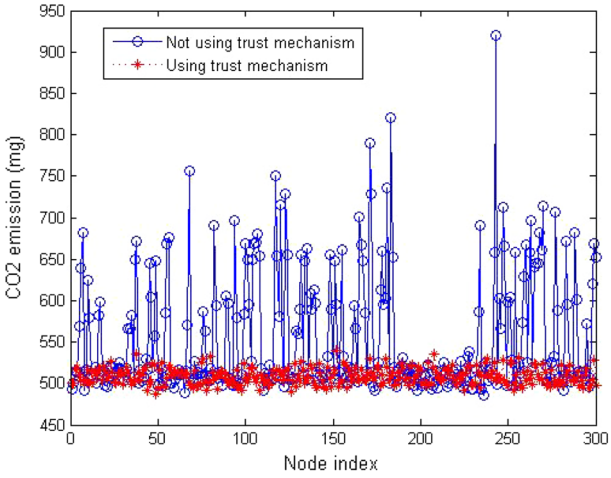


Fig. 8 Comparison of CO_2 emission

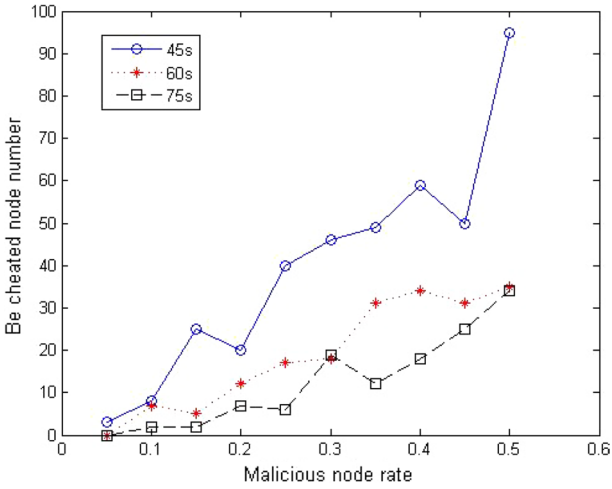


Fig. 9 Impact of different decision making time (traffic lights work)

a vehicle can collect more messages about the event to help it judges more accurately. While in some occasions, waiting time is difficult to be preset beforehand. For example, in sparse area, even the time is set to a relatively high value, a vehicle may still feel difficult to collect enough messages for judgement due to lacking of vehicles on that road segment. In such scenario, the trigger of decision making for a vehicle can be changed to a certain number of messages about the event it has collected.

Figure 9 shows results of scenarios where traffic lights work. That means there do exist congestions on road segments during simulations. While Fig. 10 shows results without traffic lights. Comparing these two figures, we may infer that our scheme works better in high ways, which have lower probability of traffic jams. In fact, the reason for higher successful cheated rate in Fig. 9 simulations is partly due to a malicious event turn to be true after the congestion it claims does happen later. It seems a vehicle is cheated but actually it makes a right decision. This statistical error is occurred due to a malicious event is published firstly. This error is harmless in practical scenario.

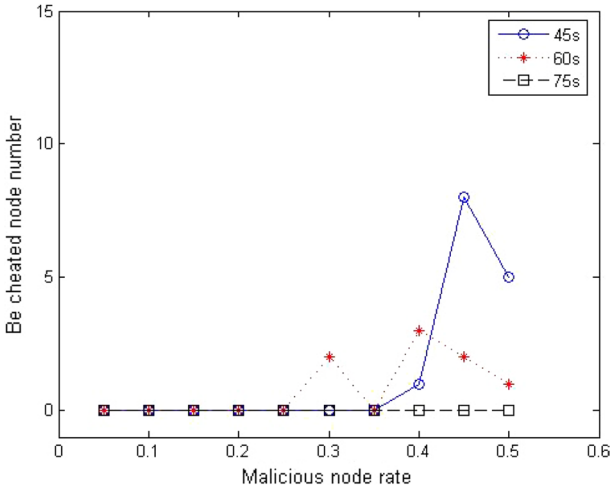


Fig. 10 Impact of different decision making time (traffic lights do not work)

Figures 11 and 12 shows the total time that vehicles take to accomplish their trip form Nantong government center to school of computer science and technology in Nantong University. Figures 11 and 12 shows that though the malicious rate increases, the total time is still maintained in a comparatively steady distribution. That indicates our scheme do work well.

6 Conclusions

In this paper, we propose a trust scheme used in VANETs to judge the trustworthiness of an event message. Unlike other trust models in VANETs, our scheme relies neither on stable communication links among vehicles what are unrealistic in practice, nor on RSUs what are still lack of large scale deployment nowadays. Our scheme takes advantage of local one way character of running vehicles and is partly like a kind of voting system in essence.

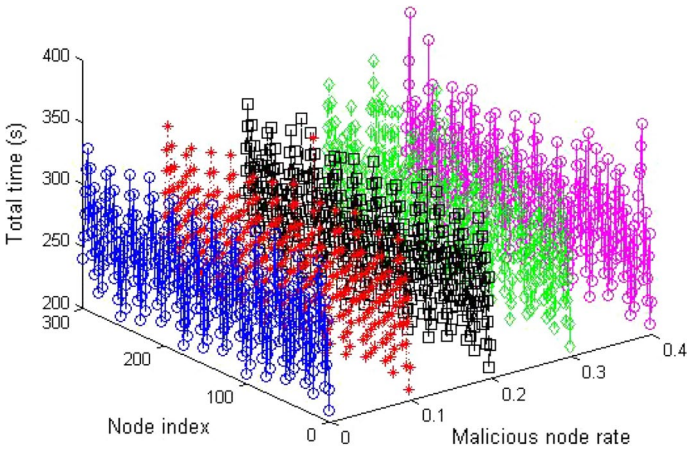


Fig. 11 Total time using to accomplish the trip (traffic lights work)

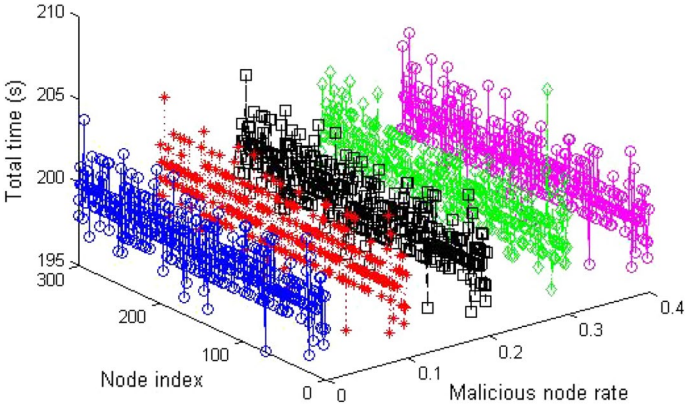


Fig. 12 Total time using to accomplish the trip (traffic lights do not work)

The scheme categorize event messages into two types: ERM and EWM. This allows a driver can deal urgent events at once and has enough time to verify road state reports.

Receiving a road state report starts a decision making procedure in our scheme. But one single malicious message cannot bring damages due to lacking more evidences to support it. The scheme can also resist many common attacks based on vehicles' IDs. Particularly the scheme can protect driver's privacy effectively, which is one major concern by many researchers.

Acknowledgements This work is supported by Jiangsu Overseas Research & Training Program for University Prominent Young &Middle-aged Teachers and Presidents Project, and in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions (15KJB520029) and the Science Foundation of Nantong of Jiangsu Grants (BK2014064). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

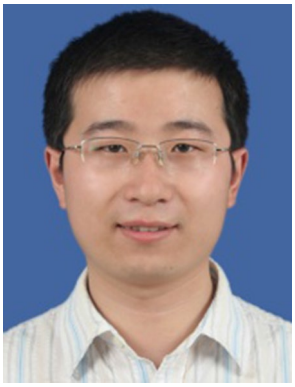
References

1. Wikipedia on Road Traffic Safety. http://en.wikipedia.org/wiki/Road-traffic_safety.10/24/2017.
2. Wikipedia on Vehicular ad hoc network. https://en.wikipedia.org/wiki/Vehicular_ad_hoc_network.10/24/2017.
3. Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation Systems. *Communications of the ACM, 43*(12), 45–48.
4. Douceur, J. (2002). The Sybil attack. In *Proceedings of the first international workshop on peer-to-peer systems (IPTPS).*
5. Dellarocas, C. (2000). Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In *Proceedings of the ACM conference on electronic commerce (EC)*, (pp. 150–157)
6. Zhang, J. (2011) A survey on trust management for VANETs. In: 2011 International conference on advanced information networking and applications (pp.105–112). IEEE
7. Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology, 61*(9), 4095–4108.
8. Wei, Y. C., & Chen, Y. M. (2014). Adaptive decision making for improving trust establishment in VANETS. In *16th Asia-Pacific network operation and management symposium (APNOMS)* (pp. 1–4)
9. Abdelaziz, K. C., Lagraa, N., & Lakas, A. (2014). Trust model with delayed verification for message relay in VANETs. In *Wireless communications and mobile computing conference (IWCMC)* (pp. 700–705)

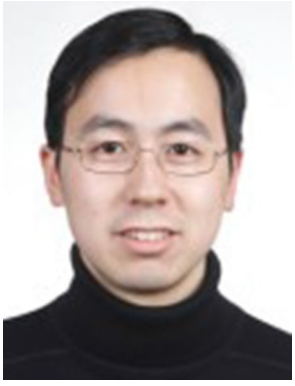
10. Minhas, U. F., Zhang, J., Tran, T., & Cohen, R. (2010). Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence: Theory and Practice (IJCITP), 5*(1), 03–15.
11. Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J. P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *Technical Report, LCS-REPORT-2007-003*.
12. Dotzer, F., Fischer, L., & Magiera, P. (2005). Vars, a vehicle ad hoc networks reputation system. In *Proceedings of the IEEE international symposium on a world of wireless, mobile and multimedia networks*.
13. Huang, Z., Ruj, S., Cavenahi, M. A., Stojmenovic, M., & Nayak, A. (2014). A scocial network approach to trust management in VANETs. *Peer-to-Peer Networking and Applications, 7*(3), 229–242.
14. Chen, Y.-M., & Wei, Y.-C. (2013). A beacon-based trust management system for enhancing user centric location privacy in VANETs. *Journal of Communications and Networks, 15*(2), 153–163.
15. Wang, G., & Wu, Y. (2014). BIBRM: A bayesian inference based road message trust model in vehicular ad hoc networks. In *2014 IEEE 13th international conference trust, security and privacy in computing and communications (TrustCom)* (pp. 481–486). IEEE.
16. Chen, C., Zhang, J., Cohen, R., & Ho, P. H. (2010). A trust-based message propagation and evaluation framework in VANETs. In *Proceedings of the international conference on information technology convergence and services*
17. Koster, A., Tettamanzi, A. G., Bazzan, A., & Pereira, C. D. C. (2013). Using trust and possibilistic reasoning to deal with untrustworthy communication in VANETs. In *IEEE-ITS2013* (pp 2355–2360). IEEE.
18. Gerlach, M. (2007) Trust for vehicular applications. In *8th International symposium on ISADS'07. Autonomous decentralized systems* (pp. 295–304)
19. Rostamzadeh, K., Nicanfar, H., Torabi, N., Gopalakrishnan, S., & Leung, V. (2015). A context-aware trust-based information dissemination framework for vehicular networks. *IEEE Internet of Things Journal, 2*(2), 121–132.
20. Chunjie, Y., Jinxu, G., & Xinyou, L. (2014). The design and realization of OBU in free-flow ETC system [C]. *Applied Mechanics and Materials, 556–562,* 2081–2084.
21. Azaola M., Moriana C., Navarro P., Valdes D., Bonardi L., Toledo M., & Cosmen J. (2013) Experimental evaluation for road user charging of GPS/GLONASS/MEMS OBU [C]. In *26th international technical meeting of the satellite division of the institute of navigation* (Vol. 1, pp. 656–666)
22. Sommer, C., Joerer, S., & Dressler, F. (2012). On the applicability of two-ray path loss models for vehicular networks simulation. *IEEE Vehicular Networking Conference (VNC), 2012,* 64–69.
23. Mujcic, R., & Frijters, P. (2011). Altrusim in society: Evidence from a natural experiment involving commuters. IZA Discussion Papers, Technical Report 5648. ftp.iza.org/dp5648.pdf
24. Santamaria, A. F., Sottile, C., De Rango, F., & Marano, S. (2015). Safety enhancement and carbon dioxide (CO2) reduction in VANETs. *Mobile Networks and Applications, 20*(2), 220–238.

Jie Wan currently works as a lecturer in the School of CS in Nantong University in China; her main research topics are Ambient Assisted Living and Human Activity Recognition. Dr. Wan completed her Ph.D. dissertation entitled "Ubiquitous Sensing in the Support of Ambient Assisted Living" at University College Dublin in 2015. Previously, she has worked as a research assistant with the COBWEB (Citizen Observatory WEB) consortium, an EU FP7 project in the citizen science domain.

Xiang Gu the corresponding author of this paper, is a professor in the school of CS in Nantong University. He received the Ph.D. degree from the School of Computer Science and Technology, University of Science and Technology of China, in 2004. He works as a post doctor in Nanjing University of Post and Telecommunication from 2010 to 2014. His current research interests include Vehicle ad hoc network, wireless sensor network, trust calculation, protocol engineering.



Jin Wang received the Ph.D. degree from Nanjing University of Science and Technology, China, in 2009. He is an associate professor in the School of CS in Nantong University. His research interests Include mobile and vehicular ad hoc networks, trust management and privacy protection. He is a member of the IEEE, the IEEE Computer Society and the ACM. He was an exchange scholar with the School of Computing, Informatics, Decision Systems Engineering, Arizona State University in 2014.



Liang Chen is currently an Assistant Professor in the School of CS in Nantong University, China. His research interests are Ad Hoc networks and congestion control.