Ad Hoc Networks 000 (2016) 1–12

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Using trust model to ensure reliable data acquisition in VANETs

Xuanxia Yao[a,*], Xinlei Zhang[b], Huansheng Ning[a], Pengjian Li[a]

[a] School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing, 100083, China
[b] Software Center, Bank of China, 100818, China

ARTICLE INFO

Article history:
Received 31 March 2016
Revised 20 October 2016
Accepted 24 October 2016
Available online xxx

Keywords:
VANETs
Entity-centric trust model
Data-centric trust model

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are usually used to reduce the traffic accidents, improve traffic efficiency and safety, promote commercial or infotainment products and etc. All the applications are based on the exchange of data among nodes, so not only reliable data delivery but also the authenticity and reliability of the data itself are prerequisite. For this purpose, a dynamic entity-centric trust model based on weight is firstly proposed according to the types of applications and the authority levels of nodes. The simulations results show that the trust model can enhance the security of the routing protocol GPSR with low delay and improve the success data delivery rate. On the basis of it, a simple data-centric trust model is constructed by employing the experiences and utility theory, which is simple enough to realize fast trust evaluation for the data in VANETs. The analyses show that it can reflect the data trustworthiness objectively and help vehicles to detect the false or bogus data.

1. Introduction

With the rapid development of networking, communication, embedded technology and automobile industry, more and more vehicles are equipped with smart devices or modules, GPS, Wi-Fi and other devices for value-added services, which make it possible to form Vehicular Ad Hoc Network(VANET) by vehicle to vehicle and vehicle to roadside unit communication. Since VANET can be used to reduce traffic accidents [1], improve traffic efficiency and safety and provide infotainment services as well by disseminating the related messages, it is thought to be one of the most important applications of Mobile Ad Hoc Networks (MANET) and draws many attentions from researchers.

The open, dynamic and distributed natures make VANETs face many challenges [2], such as, dishonest forwarding, false message propagation and so on. Security issues are very serious and can't be solved by the existing security solutions [3,4,5,6], which makes VANETs can't work efficiently. For one thing, all the applications are based on the exchange of data among entities [7] and the authenticity and reliability of data are of great importance. For the other, the peer data communication between nodes can affects data security directly. Trust is an efficient solution to address these problems [2]. A trust model is usually defined to help one node to evaluate the trustworthiness of the other node in the specific environment and can help a node to detect the dishonest or malicious nodes and false or bogus data. According to the evaluation object (data or entity), there are 2 major kinds of trust models in VANET, and they are entity-centric and data-centric [7]. The entity-centric trust models focus on evaluating the trustworthiness of vehicles to detect the dishonest and malicious nodes and ensure the reliable data delivery. And the data-centric trust model focus on evaluating the trustworthiness of the data reported by other vehicles to ensure the applications work securely and effectively. In addition, the entity trustworthiness [7,8] and data trustworthiness [9] always interplay with each other.

Modeling trust in VANETs faces many challenges. Firstly, the high dynamic makes it hard for a vehicle to evaluate either the reliability of the receiving data in real time or the trustworthiness of a vehicle. Secondly, the acentric and open natures make it difficult to collect enough information about the vehicles to be evaluated and establish a long and steady relationship among vehicles [7]. Thirdly, for specific applications in the context of VANETs, it is crucial to associate trust with vehicles and the data that they may report [10]. In order to evaluate the trustworthiness in time and improve the security and effectiveness of the applications in VANETs, we refer to the existing research achievements on trust in VANETs and try to establish trust models both in data and nodes to secure data acquisition.

In this paper, we focus mainly on 2 issues in VANETs. One is the conflict between the dynamic and trust modeling. And the other is the interaction between the data quality and the entity trustworthiness. Efforts and contributions are made from 4 aspects: 1) A dynamic entity-centric trust model based on data and node weight is proposed for VANETs by correlating data kinds to node

* Corresponding author.
E-mail addresses: yaoxuanxia@163.com (X. Yao), xinlei_0307@163.com (X. Zhang), ninghuansheng@ustb.edu.cn (H. Ning), lipengjian1990@163.com (P. Li).

http://dx.doi.org/10.1016/j.adhoc.2016.10.011
1570-8705/

types and introducing dynamical coefficient to balance the direct trust and the recommend trust; 2) Simulation and detailed analysis are made to validate the proposed entity-centric trust model. The results show that it can improving the reliability of data delivery by resisting the black-hole attack and the selective forwarding attack at the cost of a little lowering the performance of the routing protocol; 3) A lightweight data-centric trust model is presented for VANETs by exploring the traffic experience and utility theory to synthesize the relations among data, its reporter, location and time, which is simple enough to realize fast or timely trust evaluation; 4) Theory analyses on the proposed data-centric trust model shows that it can reflect the data trustworthiness objectively and help vehicles to acquire reliable data.

In the rest of this paper, we review the related work on trust model for VANETs in Section 2. Section 3 provides the system model and the related assumptions. Section 4 gives a detail description of the dynamic entity-centric trust model. Section 5 makes simulation and analysis on the proposed entity-centric trust model. Section 6 establishes and analyzes of a simple data-centric trust model for VANETs. Finally, Section 7 draws a conclusion.

2. Related work

Currently, researches on trust in VANETs can be classified into three directions: they are entity-centric trust, data-centric trust and combined trust. In addition, for the sake of evaluating trust objectively, researchers also do some work on trust metric.

2.1. Entity-centric trust

The entity-centric trust focuses on modeling the trustworthiness of nodes with the view of measuring their behavior's tendency and excluding the selfish or malicious nodes to ensure the reliable delivery of messages among peers [10,11], which is very important and useful in VANETs. For one thing, entity trust is the basic of data trust. For the other, reliable data can enhance the entity trust in turn. In addition, entity trust is also the fundamental measure to provide secure routing [12] for reliable data delivery in VANETs.

The existing entity-centric trust model computes trust value or reputation score usually based on the past direct interactions among nodes [13] and the recommendation given by other nodes [14]. The former is called direct trust and the latter is named recommend trust. For the sake of evaluating trust objectively, a static balance coefficient or weight is often used to leverage the proportion of direct and recommend trust. In addition, fuzzy logic, probability or Bayesian inference are often used to determine the trustworthiness, which are all based on the previous interaction information.

Nevertheless, the high dynamic of VANETs may lead to failure in collecting enough information about the neighbor or sender. Furthermore, the time-invariant or slow-evolving parameters as well as application-dependent nature of static entity-centric trust model make them not suitable for VANETs [8]. Although a few researches have been made on improving the dynamic of the entity trust model, they are either confined to adjust the time frame for updating trust in specific application [12] or very complicated [15].

In this paper, we focus on timely updating the direct trust instead of periodic updating it. For the sake of objective trust evaluation, we employ the weight notation and traffic experiences to describe the impacts that different nodes and data generate on the trust. At the same time, we introduce a dynamic balance coefficient between the direct and recommend trust, which is variable with the direct trust and context.

2.2. Data-centric trust

The data-centric trust is also called event-centric trust, which always focuses on evaluating the quality or trustworthiness of the data and detecting the false or bogus data in VANETs [16]. Many researchers think that it is more useful to establish trust in data rather than in the nodes reporting them [2,7,10,11]. For one thing, data are the basic of applications in VANETs. For the other, trusted safety and efficiency data along with their freshness and location relevance are very important and valuable to traffic [2].

Since data has the intrinsic dynamic nature, the existing data-centric trust models are often based on the context of the event and take time closeness, location closeness, the number of the reports on the same event, as well as the types of the events into consideration [11,17]. Considering that it is hard to decide whether the data is trustworthy or not just based on a single message, Raya et al. [2] proposed a framework for data-centric trust model based on collecting multiple reports related to the same data and combine them with their weights to make a decision. Wu et al. [17] put forward a RSU-aided completely data-centric trust model by synthesizing the distance from the vehicle to the event, maximum detection range of the vehicle, the number of sensors that can detect the event, the total number of sensors in the vehicle, and the weight of vehicle to determine the message's trustworthiness. Ding et al. [18] present an event-based reputation model to filter bogus warning messages by classifying nodes into different roles. Since each role has its own trust evaluation mechanism for the incoming traffic message, it is essentially a dynamic role-dependent trust evaluation model and can determine whether a traffic message is trustworthy or not.

Different models have different modeling idea, but their core business is basically identical, which is to determine the received data's trustworthiness. According to the summary in literature [2], the methods to establish trust for data-centric model mainly includes 5 techniques, which are Majority Voting (MV), Most Trusted Report (MTR), Weighted Voting (WV), Bayesian Inference (BI) and Dempster–Shafer Theory (DST). MV uses majority principle to determine the trustworthiness of the data. MTR employs the maximum principle to define the trust value of the data. WV combines all the votes for the same event with the votes' weight to compute the trustworthiness of it. BI is the most common technique for trust establishment, which evaluates the trustworthiness by the posterior probability and the new evidence of the event. DST is based on human reasoning and can deal with the uncertainty well. Although each technique has its own advantages, their common shortage is that it will take them much time to make trust decision.

In this paper, considering the data-centric trust affected by many factors in the context and the requirements for timely trust evaluation, we make 2 efforts. Firstly, we introduce a basic trust matrix, the notion of time influence degree and local influence degree based on traffic experiences to help simplify the trust model and trust evaluation. And then, we try to employ the utility theory to build the as simple as possible data-centric trust model.

2.3. Combined trust

The combined trust makes extensive use of entity trust to evaluate the trustworthiness of data and maintains entity trust over time [11]. Since data's trust evaluation is made on the basis of entity trust, the idea that a message is trusted if it has been evaluated to be trustworthy by many other trusted peer nodes [19] is accepted. In the existing combined trust models, entity trust and data trust usually interact with each other. The typical examples are RSU and beacon based trust management models [20,21], which establish entity trust by cross-checking the plausibility of

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

event messages and beacon messages. The purpose is to prorogate data opinions quickly. In addition, the model can prevent internal attackers from sending or forwarding forged messages.

At present, researches on combined trust model for VANETs is relative few. Most so-called combined trust models are usually comprised of the entity trust model and the data trust model but not their dynamic integration. For the sake of simplicity and description, we do not regard the simple interaction between the entity trust model and data trust model as combined trust model in this paper, but treat them as two trust models for different goals.

2.4. Trust metric

No matter what kind of trust model is, proper trust metrics are crucial to achieve objective and correct trust evaluation. According to literature [22], there are some attributes related to trust establishment in VANETs, which act as the trust metrics in many existing trust models. The most common used metric is the distance, including the distance from the vehicle to the event, between the receiver and the transmitter, the sender and RSU, and RSU and the event. Next is the time and the recommendation by other vehicles, and the time mainly refer to the interval between the event occurrence time and the report time. The number of senders and the type of the vehicle comes follow. In addition, the node's opinion/experience on the data or entity, the type of the event , vehicle's velocity, position and direction are also used in few trust models.

In this paper, we pay much attention to the dynamic attribute of VANETs. In the entity-centric trust model, we focus on the following three facts: 1) The application data is becoming more and more rich, and different data has different impact on traffic; 2) Different vehicles have different intentions, different type of vehicle plays different role and has different authority in traffic; 3) The majority of people drive their vehicles locally for their daily commute, and hence, most vehicles have their predefined constant daily trajectories [18]. In addition, the notion of weight is employed to estimate the direct trust and recommend trust. Furthermore, a dynamic balance coefficient is introduced to leverage the proportion of them with the context. At the same time, considering that trusted data is of great importance and depends on the trusted entity to a great extent in VANETs, we build a data-centric trust model based on the entity-centric trust model and put some emphasis on the distance, time and relations between node types and data types as well. Moreover, in the process of selecting trust metrics, we keep a watchful eye on the requirements for timely trust evaluation.

3. Models and assumptions

For the sake of description, the network model, application model and the security model used in this paper are illustrated as following.

3.1. Network model

In VANETs, the nodes are either vehicles or roadside units. And the majority nodes are all kinds of vehicles. Since vehicles always move at different speed for different destination, the topology of the VANET keeps changing. Based on the fact, many researchers think that a vehicle always meet strange vehicles in VANET or rarely meet a vehicle repeatedly. In fact, not only many people's travel habits always meet a specific distribution, but also a lot of people have the identical travel distribution and common or similar travel/activity range. In other words, they often cover the same section of a road in the similar time period in daily travelling. So it is assumed that different vehicles can meet with a certain probability, which is conformed with the factual and make it possible to collect the past interaction experiences to establish entity trust. In addition, some assumptions on the nodes in VANETs are also made as following.

All nodes are equipped with smart sensors, computing modules, wireless communication module, GPS and other devices needed to form VANET. And they can not only compute their location accurately but also perceive an traffic event correctly within certain range. The range is assumed to be 20 m and the communication radius of the node is assumed to be 200 m. Meanwhile, all nodes are synchronized without the time synchronization technique [23], in other words, they all use the same time-zone and their time is in error expected. The transportation authority organizations are responsible for issuing public certificates in the process of the node registration, checking nodes and their certificates periodically. Furthermore, the public key of the transportation authority organization is known to all vehicles in advance. For the sake of simplification, it is also assumed that the vehicle type is signed by the authority transportation organizations.

3.2. Application model

Applications in VANETs are various. According to the functionalities, they can be classified into three primary categories, which are safety application, efficiency application and infotainment application [2]. The safety application is used to increase public safety and protect individual life safety, such as rear-end accident warning, blind spot warning and so on. The efficiency application improves traffic efficiency, such as congestion control, parking information. The infotainment application refers to the commercial or entertainment related applications, such as advertisement and entertainment information sharing.

For the sake of simplification, each type of application is described by a key word set. For instance, set {rear-end accident, serious accident, breakdown, blind spot warning, icy-road, Wet-road, thick foggy, steep slope zone} denotes the safety application, set {congestion, road maintenance, road closed, parking, gas station} denotes the efficiency application, and set {coupon, song, music, scenic spot, restaurant, bar} denotes the infotainment application. An event or data description is a subset of the corresponding set. An application in VANET is assumed to be one of the three types, which is determined by the reporter and verified by the receiver. The application data disseminated in VANETs is assumed in the format of the Fig. 1.

All the items except for "Event Reporter Type" are generated automatically by the vehicle. " Event Reporter Type" includes the type of the node and the transportation authority department's signature on it, which are stored in the certificate issued by the transportation authority department. The signature on the type of the vehicle is denoted by Sign $(K_M,\text{hash}(ID_k)||\tau(v_k))$, where K_M is the private key for signature of the transportation authority department, ID_k is the identifier of the vehicle k, and $\tau(v_k)$ is the type of the vehicle.

3.3. Security model

Security is a key issue in VANETs. Since it is always caused by misbehaving nodes, selfish nodes and malicious nodes, trust is an efficient solution to it. Trust evaluation on entity and data are the core tasks of trust modeling.

The entity trustworthiness in VANETs is usually relative slow-evolving and impacted by the past interaction with other nodes. So the trust updating principles in the entity-centric trust model are assumed as: 1) The direct trust is updated only after the interaction between the two nodes changes. 2) Only when the di-

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

Event Type	Event Position	Event Time	The Type of the Event Reporter	Event Reporter Position	Event Description	The Hash of the Reporter Identifier(Hash(ID))	Reporter's Signature on the Data

Fig. 1. Data format.

rect trust value less than a threshold, should the recommendation and the comprehensive trust value be calculated. At the same time, it's better to make the entity-centric trust model be variable with the context so as to acclimatize it to the dynamic environment in VANETs.

The data trustworthiness in VANETs depends on many factors, such as the trustworthiness of the reporter or the forwarder, time closeness, location closeness and the relations between the data and the reporter as well. Unlike entity trust, data is driven by event, and data trust is dynamical or volatile in nature. It is very important for nodes to evaluate the incoming data's trustworthiness in real time. Accordingly, the data-centric trust model should be as simple as possible.

Without loss of generality, the trust value should be a number in [0,1]. The value 1 means completely trustworthy, 0.5 means half trust or uncertainty, and 0 means thoroughly untrustworthy.

4. The entity-centric trust model based on weight

Similar to the most existing entity-centric trust models [24,25], the trust value in the proposed entity trust model is based on the direct trust and the recommendation. And unlike the existing entity-centric trust models, the notion of weight is introduced to describe the different types of applications and nodes so as to help evaluate the direct trust and recommendation objectively. At the same time, a dynamical instead of a static balance coefficient is used to leverage the direct trust and recommend trust to acclimatize the dynamical environment in VANETs. For the sake of clarity, we give the weight definition in advance and describe the dynamical balance coefficient in the comprehensive trust evaluation.

4.1. Weight definition

In entity-centric trust models for VANETs, the trustworthiness of a node is closely related to its authority level and the type of the application data reported or forwarded by it. So we define the application data weight and node weight respectively.

4.1.1. Application data weight

Generally, different applications need different requirements for data trustworthiness, and different kinds of application data have different impacts on traffic, the public or individual safety. According to the catalogues of applications in Section 3.2 and the experiences in traffic, the traffic safety data is obviously the most important one for the public and individual safety; the traffic efficiency data is the second; and the infotainment data has the least impact on safety and traffic. For the sake of description, we denote the three types of application data with *S, E* and *I* respectively. Based on our experiences, comprehensive analyses on the security requirements of VANETs and the three kinds of application data's influences on traffic safety, the application data *x*'s weight $W_D(x)$ is defined by Eq. (1).

$$W_D(x) = \begin{cases} 1, & x = S \\ 0.8, & x = E \\ 0.5, & x = I \end{cases} \quad (1)$$

It should be noted that the application data's weight stands for its importance in VANETs. Any data transmitted in VANETs should belong to one of the three data types.

4.1.2. Node weight

Nodes in VANETs are various, including special vehicles (such as patrol wagon, ambulance, engineering vehicles and etc.), ordinary vehicles (such as private car, taxi and so on), and roadside infrastructures as well. According to the node's authority, we classify the nodes in VANETs into 3 types, which are high level nodes (denoted by *H*), medium level nodes (denoted by *M*) and low level nodes (denoted by *L*). The high level nodes mainly refer to the police wagon and the roadside unit. The authority level of the police wagon is obvious high. It should be stated that roadside units are always controlled directly by the authority organization and manage traffic on behalf of the authority management department, so they are also considered to be with high authority. Medium level nodes refer to vehicles for public services, such as bus, ambulance, road upkeep vehicles, engineering vehicles, sanitation trucks and etc., which are usually managed by specific department. Low level nodes refer to private car, taxi, freight vehicles and etc., which are controlled mainly by individuals and can move at liberty to some extent.

In general, the high level node and the data reported by it are usually with higher trustworthiness than the medium, low level node and their report. Moreover, a node's authority level is not only closely related to the trust value in entity-centric trust model, but also bound up with the data trustworthiness in data-centric trust model. Here, we pay much attention to the social meaning of the trust and the experiences in traffic, and define the node *x*'s weight $W_N(x)$ as Eq. (2).

$$W_N(x) = \begin{cases} 1, & x = H \\ 0.7, & x = M \\ 0.5, & x = L \end{cases} \quad (2)$$

The node's weight can reflect the trustworthiness of it and the data reported by it to some degree. A node in VANETs should belong to one of the three levels.

4.2. The entity-centric trust model description

The entity-centric trust model based on weight is designed for evaluating the trust value for the node in VANETs. For the sake of description and reading, some notations used in it are listed in Table 1.

Since the comprehensive trust value is co-determined by the direct trust and the recommendation. We describe the proposed trust model from the aspects of direct trust, recommendation and comprehensive trust respectively.

4.2.1. Direct trust

The direct trust is one nodes' subjective expectation to the other nodes' future behavior. Because of the dynamic in VANETs, there are two cases: one is that the two nodes have history interactive experiences; the other is that they have no history interaction record or they meet first time.

In the case of there being history interactive experiences between two nodes, the direct trust value is usually determined by the successful data forwarding rate. In general, the higher successful forwarding rate means the higher trustworthiness. But for the cunning nodes who may get high successful forwarding rate by only forwarding the data with low weight when infotainment data is more than safety and efficiency data, it is hard to get the objective and correct direct trust value. To deal with this problem, it's

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

Table 1
Notations.

Notations	Meaning
$N_A{}^B$	The total number of message/data that node A asked node B to forward.
$M_A{}^B$	The successful number of message/data that node B has forwarded for node A.
$W_D{}^x$	The weight of the data x, which is determined by Eq. (1).
$W_N{}^A$	The weight of node A, which is determined by Eq. (2).
$U_W{}^{A,B}$	The sum of all data's weight that node A asked node B to forward.
$S_W{}^{A,B}$	The sum of the data's weight that node B has successfully forwarded for node A.
$E_{TW}^{A,B}$	The average weight of all data that node A asked node B to forward, which can be computed by $E_{TW}^{A,B} = U_W{}^{A,B} / N_A{}^B$.
$E_{SW}^{A,B}$	The average weight of all data that node B has successfully forwarded for node A, which can be computed by $E_{SW}^{A,B} = S_W{}^{A,B} / M_A{}^B$.
$F_W{}^B$	Node B's malicious tendency, which is determined by Eq. (3).
$DT_A{}^B$	The direct trust value of node A to node B.
$RT_A{}^B$	The recommendation of node A to node B
$T_A{}^B$	The comprehensive trust value of node A to node B

necessary to identify the cunning nodes and design proper method to evaluate the trustworthiness. Here, we introduce the notion of malicious tendency to describe a node, which needs to be estimated before trust evaluation. Since the malicious tendency of a node is closely related to the average weight of the data failing to be forwarded, node *A* can evaluate node *B*'s malicious tendency by Eq. (3).

$$F_W^B = \left(U_W^{A,B} - S_W^{A,B}\right)/\left(N_A^B - M_A^B\right) \tag{3}$$

According to the experiences in traffic, we assume that the rough proportion of the safety, efficiency and infotainment data in VANETs are 0.2,.04 and 0.4 respectively. Combining with the weight of the three kinds application data, the mean weight of the data in VANETs can be computed by$(1\times0.2+0.8\times0.4+0.5\times0.4)=0.72$, which is set to be the threshold for determining whether a node is with malicious tendency or not. If $F_W{}^B < 0.72$, it indicates that the node has no malicious tendency, otherwise, it is considered to be with malicious tendency.

For the sake of security, the direct trust should also follow the rule of more punishments and less awards. Based on the above analysis, the node *A*'s direct trust for node *B* can be calculated by Eq. (4) after node *A* asks node *B* to forward a message *x* for it.

$$DT_A^B = \begin{cases} \dfrac{W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right)}{1 + E_{TW}^{A,B}/E_{SW}^{A,B}} + DT_A^B, F_W^B < 0.72 \\ W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right)/4 + DT_A^B, \\ \quad (Flag = 1) and (F_W^B \geq 0.72) \\ W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right) + DT_A^B, \\ \quad (Flag = -1) and (F_W^B \geq 0.72) \end{cases} \tag{4}$$

In Eq. (4), *Flag* is used to indicate whether the forwarding is success or not. If it is success, Flag is set to be 1, else it is set to be −1. Since $E_{TW}^{A,B}/E_{SW}^{A,B}$ can reflect the successful forwarding rate objectively, it is used to adjust the direct trust of the normal node *B*. When node *B* is with malicious tendency, that is $F_W{}^B \geq 0.72$, the reward strength for it should be much less than that for the normal one and the punishment strength should be much more than that for the normal node. For simplicity, we let the reward strength of the node with malicious tendency to be half that of the normal one and the punishment strength of it to be the double of the normal one.

In the case of no history interaction record between two nodes, the direct trust is usually set to 0.5, which means the uncertain trust relationship. But in our model, considering nodes' authority level, it is set to be the node's weight, which is more consistent with the actual conditions than the traditional practice.

4.2.2. Recommendation

The recommendation is from the third parties, which is used to avoid the subjectivity or one-sidedness of the trustworthiness or enhance its objectivity. Since it is mainly affected by the type of the third party, it is necessary to use multiple neighbors views to calculate it. Here, $RT_A{}^B$ is define by Eq. (5), which synthesizes node *A*'s direct trust value to other neighbors and other neighbors' comprehensive trust value to node *B*. At the same time, considering that nodes in different authority level have different influences on the recommendation, the recommender's weight is also combined into the construction of the recommendation. In addition, for the limitation of memory, the principle of least recently used(LRU) is recommended to manage the nodes having history interaction with it.

$$RT_A^B = \frac{\sum_{i=1}^{n} DT_A^{N_i} \cdot T_{N_i}^B \cdot W_N^{N_i}}{\sum_{i=1}^{n} DT_A^{N_i}}, \quad N_i \neq B \tag{5}$$

In Eq. (5), N_i is the *i*th neighbor of node *A*.

4.2.3. Comprehensive trust

Comprehensive trust is composed of direct trust and recommendation. The key issue is how to leverage the shares of them. Since a node usually has different past interactive with different node, the share of direct trust should not be fixed but change with the interactive node. Similarly, the recommendation has different impact on the comprehensive trust in different cases. For example, when node *A* is very familiar to node *B, A* will believe its direct trust to *B*, and the recommendation is not important or unnecessary. When node *B* is a strange node to *A* or its direct trust is less than the threshold, the recommendation is very important. Based on the facts, a dynamic balance coefficient α in [0,1] is introduced to adjust their impacts on the comprehensive trust. When node *A* wants to compute its trust value to node *B*, α is determined by Eq. (6).

$$\alpha = \begin{cases} 1, DT_A^B \in (0.7, 1] \text{or} DT_A^B \in [0, 0.3) \text{or} W_N^B = 1 \\ DT_A^B, DT_A^B \in [0.5, 0.7) \\ W_N^B \cdot DT_A^B, DT_A^B \in [0.3, 0.5) \end{cases} \tag{6}$$

It can be seen that α changes with $DT_A{}^B$ and/or $W_N{}^B$, which make it can balance the direct trust and recommendation dynamically and avoid unnecessary cost. For one thing, the direct trust is put enough attention, and for the other, the recommendation is utilized to estimate the entity trust when there are doubts in the node or the direct trust is not high enough.

Based on α, the dynamic entity trust model based on weight can be described by Eq. (7). It is obvious that T_A^B is between 0 and 1.

$$T_A{}^B = \alpha \cdot DT_A{}^B + (1-\alpha) RT_A{}^B \tag{7}$$

5. Simulation and analysis for entity-centric trust model

Since the entity-centric trust is the fundamental of the secure routing in VANETs, the proposed entity trust model based on weight will be validated in routing protocols. Among the numerous Ad Hoc routing protocols [26,27], GPSR is based on the

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

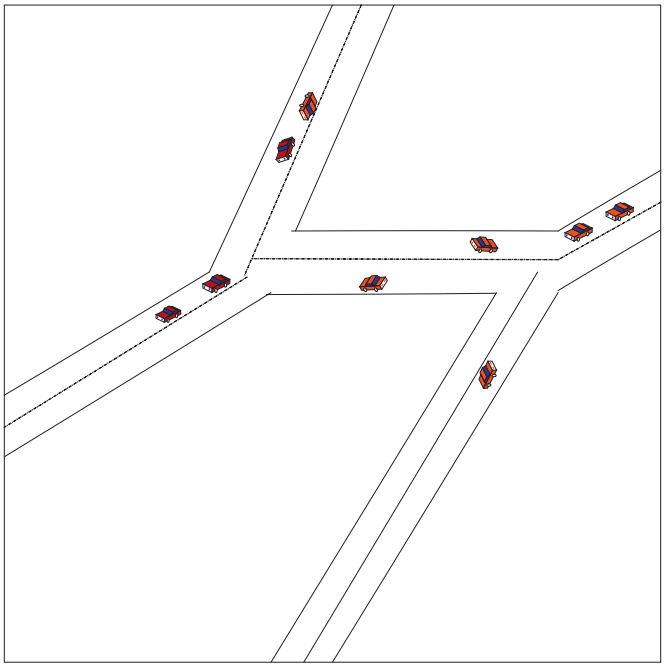


Fig. 2. The traffic topology sketch.

Table 2
Simulation environments and parameters.

Environment or parameters	Values
OS/Platform	Windows 7
Language	Java
Simulation area	1000 m × 1000 m
Routing protocol	GPSR, I-GPSR, T-GPSR
Number of nodes	50,70,90,110,130,150,170
The range of one hop	200 m
Bandwidth	2 Mbit/s
The Interval of Hello Packets	Uniform distribution(0.9,1.0)
The maximum size of a packet	4096 bit or 512 Byte
The interval of data packets	Exponential distribution(12 s)
Moving speed	0 m/s∼18 m/s
Simulation time	1000 s
Trust threshold	0.6

current location of nodes and closely related to trust, so the proposed trust model is applied in GPSR to construct a trust based GPSR (T-GPSR) for validation. Comparing with the original GPSR, T-GPSR just adds trust evaluation and increases the next hop selection condition related to the trust value. In addition, it should be stated that the neighbor node nearest to the destination refer to the furthest neighbor from the current node in VANETs.

5.1. Simulation environment

In order to make the simulation scenario be close to the real traffic environment, we take a traffic network generated by VanetMobiSim for example, and the corresponding traffic topology is shown in Fig. 2.

For the sake of clarity, the simulation environment and the related parameters are described in Table 2.

Considering the entity-centric trust model is mainly used to distinguish the malicious, cunning or selfish nodes and avoid interacting with them, the simulation experiments are made in the scenario without attack, the scenario with a black hole attack, and the scenario with a selective forwarding attack respectively. For the sake of comparison, three protocols based on GPSR (GPSR, I-GPRS [24] and T-GPSR) are simulated respectively in each scenario. The reason for selecting such 3 protocols is that they have the identical routing idea but different methods to deal with malicious nodes. In addition, the three main metrics of packet delivery ratio, the path length and the average end-to-end delay for the routing protocol are employed to evaluate the performance and show the trust model's impact on the routing protocol.

5.2. Comparative analysis

It should be stated that all the simulation data are the mean values of 10 times simulation results.

1) Scenario without attack

In the scenario without attack, the simulation results for the 3 GPSR-based routing protocols are shown in Fig. 3.

It can been seen from (a) and (b) of Fig. 3 that the packet delivery ratio and the path length of the 3 GPSR based protocols are roughly in line with each other. But for the average end-to-end delays in (c) of Fig. 3, only I-GPRS and T-GPRS are well in line with each other, and the original GPRS is slight lower than those of I-GPRS and T-GPRS, which is caused by the additional trust evaluation in I-GPRS and T-GPRS. Fortunately, just a little delay is increased. The results in the scenario without attack show that the proposed trust model can inevitably increase overhead but will not decrease the performance of the routing protocol distinctly.

2) Scenario with a blackhole attack

In the scenario with a black-hole attack, the malicious node will discard all the packets. The simulation results for the 3 GPSR based routing protocols are shown in Fig. 4.

It can been seen from (a), (b) and (c) of Fig. 4 that I-GPRS and T-GPRS are basically in line with each other in the data delivery ratio, the average path length and the average end-to-end delay, but GPSR is distinct different from them, the performances in all the 3 metrics are lower than I-GPRS and T-GPRS. The results indicates that both I-GPRS and T-GPRS can detect and isolate the malicious node, but the original GPRS can't.

Comparing (a) of Fig. 3 with (a) of Fig. 4, it is observed that the data delivery ratio of I-GPRS and T-GPRS are basically identical in the two scenario, which indicates that both of I-GPRS and T-GPRS can not only resist black-hole attack well but also keep the performance of the protocol in the normal level. On the contrary, the original GPRS shows much lower delivery ratio than that of the former two and its own in the scenario without attack. Because its forwarding strategy does not consider the trustworthiness of the next hop candidate, it may results in failure delivery when there is a malicious node in the VANET.

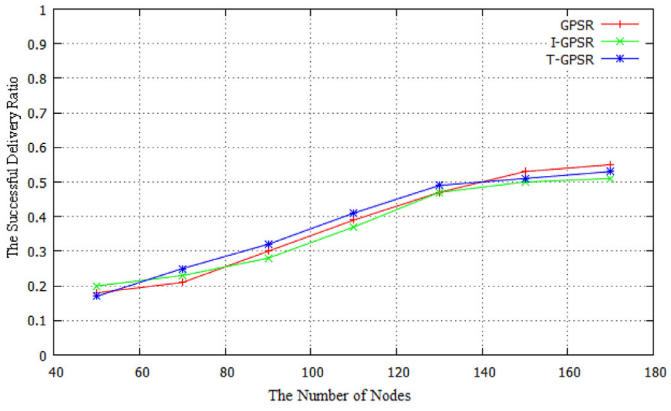
Comparing with the scenario without attack, the average path lengths of I-GSPR and T-GSPR in (b) of Fig. 4 increase a little, which may be caused by bypassing the malicious node. And the average path length of the original GPRS in(b) of Fig. 4 is similar to that in (b) of Fig. 3, the reason may be that all nodes are treated in the same way as in the scenario without attack and the black-hole node is rarely in the path by chance.

The average end-to-end delay of I-GSRP and T-GSRP in (c) of Fig. 4 are roughly in line with theirs in (c) of Fig. 1, which may because the malicious nodes in this scenario is not many enough, and they can work as in the normal network environment. But for the original GPSR, its the average end-to-end delay drop a little, which may be caused by some failure deliveries caused by the malicious node.

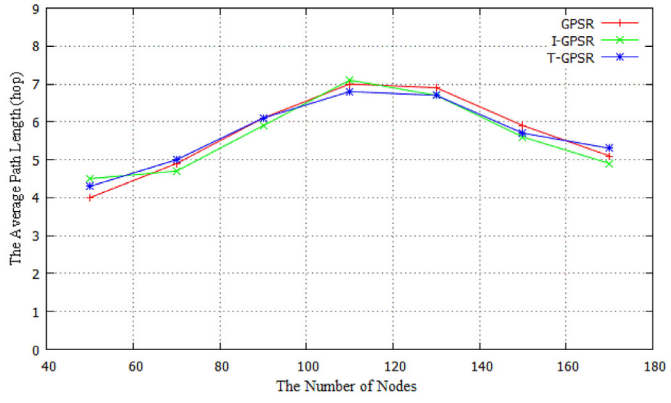
3) Scenario with a selective forwarding attack

In the scenario with a selective forwarding attack, the malicious node refers to the cunning, dishonest or selfish nodes, who only forward the low-weight, low-cost or the packets in their favor. The simulation results for the 3 GPSR based routing protocols are shown in Fig. 5.

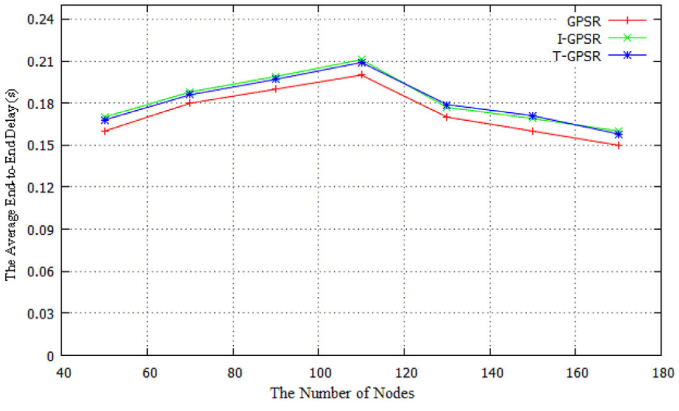
Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011



(a) The Data Delivery Ratio

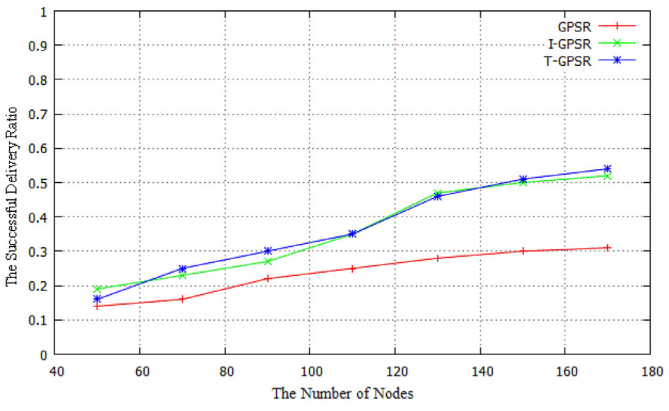


(b) The Average Path Length

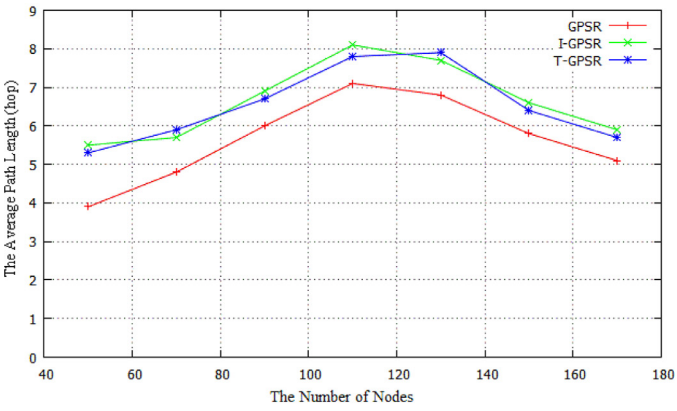


(c) The Average End-to-End Delay

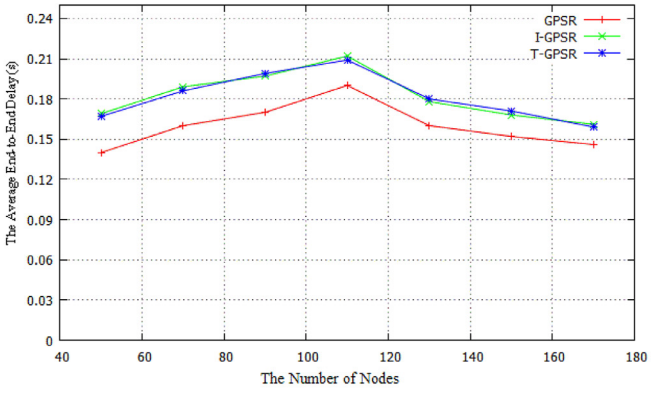
Fig. 3. Simulation results in the scenario without attack.



(a) The Packet delivery Ratio



(b) The Average Path Length



(c) The Average End-to-End Delay

Fig. 4. Simulation results in the scenario with a black-hole attack.

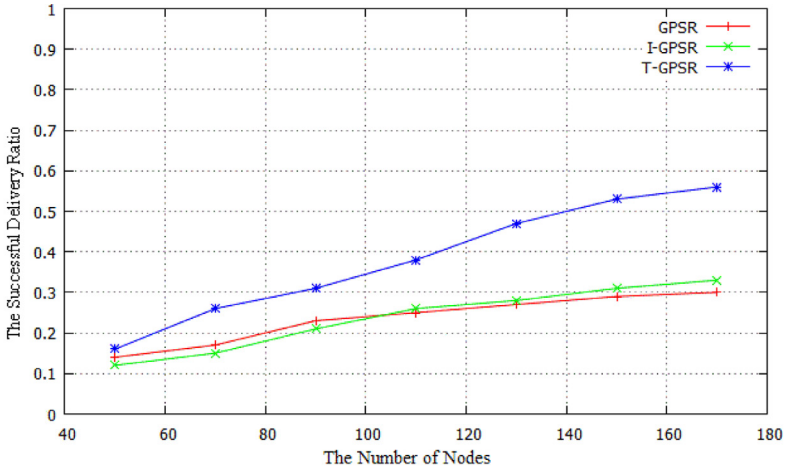
In (a) of Fig. 5, the data delivery ratio of the GPSR and I-GPSR are in line with each other, and the data delivery ratio of T-GPSR is basically identical to that in (a) of Fig. 3(the scenario without attack) but much better than that of the other two, which means that the GPSR and I-GPSR work in the similar way and neither of them can resist the selective forwarding attack. At the same time, it also indicates that T-GPSR can resist the selective forwarding attack or distinguish and bypass the selfish node.

In (b) of Fig. 5, the average path length of T-GPSR is clearly longer than that of the other two, which may be caused by T-GPSR bypassing the selfish node and the failure packet delivery in GPSR and I-GPSR.

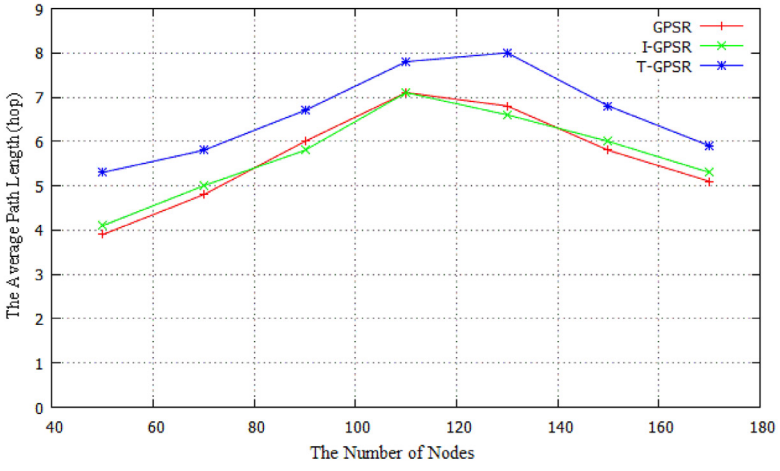
In (c) of Fig. 3, the average end-to-end delay of T-GPSR is the higher than that of I-GPSR, and that of GPSR is the lowest. The reason may be in 2 aspects. For one thing, although both of T-GPSR and I-GPSR need time to evaluate the trustworthiness of the next hop candidate, the cunning or selfish node is often considered to be normal node by I-GPSR but treated to be malicious node by T-GPSR. So T-GPSR has to take more time to distinguish the selfish node than I-GPSR. For the other, comparing with the original GPSR, I-GPSR needs time to evaluate the node's trustworthiness.

In addition, the average end-to-end delay of GPSR in (c) of Fig. 5 is basically in line with that in (c) of Fig. 4 and is lower than that in (c) of Fig. 3, this is because of the failure packet delivery caused by the malicious or selfish node.

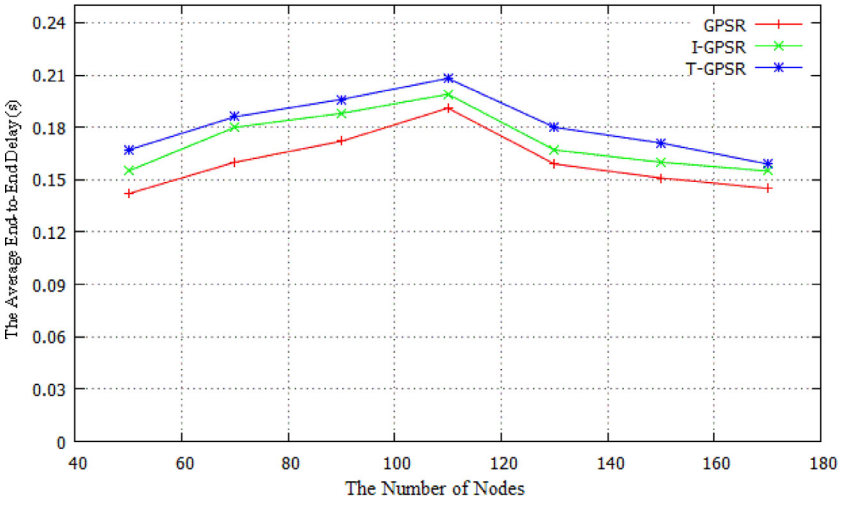
Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011



(a) The Packet delivery Ratio



(b) The Average Path Length



(c) The Average End-to-End Delay

Fig. 5. Simulation results in the scenario with a selective forwarding attack.

Table 3
Notations in data-centric trust model.

Notations	Meaning
B_λ^v	The trustworthiness of the report or data on event λ generated by node v.
T_A^B	The trustworthiness of node A to node B
$\tau(v)$	The type of node v, which is predefined and signed by the traffic management department
$\tau(\lambda)$	The type of the data/event λ, which is assigned by the reporter and verified by the receiver.
$M(\tau(v), \tau(\lambda))$	The default correlative trustworthiness of event λ and node v, which is from the basic trust matrix M_T, If there is no specific event or task, $M(\tau(v),\lambda)= W_N^v$.
$\mu_l(v,\lambda)$	The proximity in geographic location, which is described by the distance between the reporter v's position and the event λ's locality.
$\mu_t(v,\lambda)$	The proximity in time, which is described by the interval between the report generated by node v and the event λ occurrence.

6. Data-centric trust model

In VANETs, since data dissemination is required to be as quick as possible, it further demands the data trustworthiness evaluation method or technique as simple as possible. For this purpose, we need to predefine or quantize the main experiential factors in advance. At the same time, we try to employ the utility theory to coordinate the effectiveness of the main factors in data trust establishment instead of using the existing complicated trust evaluation techniques [9,15,17].

For the sake of description, some notations used in this model are listed in Table 3.

6.1. Impact factors definition

Similar to the existing data-centric trust model, the trustworthiness of the data is determined by many factors, such as the data reporter's trustworthiness, the correlative trustworthiness of the event and its reporter, the distance between the reporter's position and the event locality, the time interval between the event occurrence and the report generated, the weather conditions and the road conditions (such as icy road, wet road, road in repairing or maintaining and so on) etc.. According to the experience, the weather and road conditions can usually be obtained by vehicles directly and have relative limited impact on the trustworthiness of the received data, so we just focus on the former 4 factors in our model.

1) The data reporter's trustworthiness

The data reporter's trustworthiness refers to its trustworthiness or security status. In this paper, T_A^B (the trustworthiness of node *A* to node *B*) is evaluated by the proposed entity-centric trust model based on weight. The default trust value of it is its weight.

2) The correlative trustworthiness of the event and its reporter

The correlative trustworthiness of the event λ and its reporter *v* ($M(\tau(v),\tau(\lambda))$) is directed at such a fact: for a specific event/data, it is possible that a reporter with low authority may be more trustworthy than the one with high authority; or the vehicles at the same authority level have different trustworthiness. The reason may be the rough vehicle categories based on the authority. Considering different node in VANETs has different functions, we further classify nodes in VANETs into 10 kinds. In order to describe the initial/default trust value, a basic trust matrix M_T is used to combine the ten kinds of nodes with the three types of data. For clarity, the basic trust matrix M_T is described in the form of table, which is preset by the traffic experiences and shown in Table 4.

It should be stated that each initial/default trust value in M_T is the empirical value on the condition that the node is fully trusted.

Table 4
Basic trust matrix.

Nodes type	Safe app	Efficient app	Infotainment app
Roadside unit	1	1	1
Patrol wagon	1	1	0.7
Road upkeep vehicle	0.8	1	0.7
Ambulance	1	1	0.5
Bus	0.8	0.8	1
Engineering vehicles	0.7	0.8	0.5
Sanitation truck	0.7	0.8	0.7
Taxi	0.7	0.7	1
Private car	0.7	0.7	0.8
Freight vehicle	0.7	0.7	0.7

3) The proximity in geographic location

According to literature [9], the closer the reporter is to the location of an event, the more likely it is to have accurate information on the event, which makes the report more trustworthy. For safety and efficiency data, the impact of the distance proximity on the data trustworthiness is obvious. As a matter of experience, the influence of the distance μ_l between the reporter *v*'s position and the event λ's locality can be preset by experiences as Eq. (8).

$$\mu_l(v,\lambda) = \begin{cases} 1 & d \le 10m \\ 0.9 & 10m < d \le 20m \\ 0.8 & 20m < d \le 50m \\ 0.7 & 50m < d \le 100m \\ 0.6 & 100m < d \le 200m \\ 0.4 & 200m < d \le 500m \\ 0 & d > 500m \end{cases} \tag{8}$$

4) The proximity in time

Similar to the distance between the reporter's position and the event/data locality, the shorter interval between the event occurrence and the report generated, the more likely it can reflect the system status [9]. Accordingly, the data is more trustworthy. On the basis of the data from the traffic management department and experiences, the traffic event can usually be solved from 5 minutes to an hour, so the influence of the interval μ_t between the event occurrence and the report generated by node *v* can be preset as Eq. (9).

$$\mu_t(v,\lambda) = \begin{cases} 1 & t \le 5min \\ 0.9 & 5min < t \le 10min \\ 0.8 & 10min < t \le 20min \\ 0.7 & 20min < t \le 30min \\ 0.5 & 30min < t \le 45min \\ 0.3 & 45min < t \le 60min \\ 0 & t \ge 60min \end{cases} \tag{9}$$

6.2. Effective coefficients definition

Each factor has different impact on the data trustworthiness. In order to estimate the data trustworthiness correctly, it is necessary to determine the effective coefficient of each impact factor according to its utility in data trustworthiness.

Usually, the probability that an unbelievable node reports a trusted data is almost zero, which indicates that the trusted data reporter is the basic of guaranteeing the trusted data and should be given enough attention..

Since $M(\tau(v),\tau(\lambda))$ (the correlative trustworthiness of the event λ and its reporter *v*) depends on and changes with the trustworthiness of the reporter, we treat the product of the default correlative trust value in M_T and the current trustworthiness of the reporter as a new impact factor, which can not only represent the two main factors but also reflect the interaction between them. According to the experience and the existing research achievements, the new factor can basically determine the trustworthiness of the data, so

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

Table 5
Data trustworthiness evaluation in the three cases.

Reporter type	$T1_S$	$T2_S$	$T3_S$	$T1_E$	$T2_E$	$T3_E$	$T1_I$	$T2_I$	$T3_I$
Roadside unit	1	0.91	0.7	1	0.91	0.7	1	0.91	0.7
Patrol wagon	1	0.91	0.7	1	0.91	0.7	0.79	0.7	0.49
Road upkeep vehicle	0.692	0.602	0.392	0.79	0.7	0.49	0.643	0.553	0.343
Ambulance	0.79	0.7	0.49	0.79	0.7	0.49	0.545	0.455	0.245
Bus	0.692	0.602	0.392	0.692	0.602	0.392	0.79	0.7	0.49
Engineering vehicles	0.643	0.553	0.343	0.692	0.602	0.392	0.545	0.455	0.245
Sanitation truck	0.643	0.553	0.343	0.692	0.602	0.392	0.643	0.553	0.343
Taxi	0.545	0.455	0.245	0.545	0.455	0.245	0.65	0.56	0.35
Private car	0.545	0.455	0.245	0.545	0.455	0.245	0.58	0.49	0.28
Freight vehicle	0.545	0.455	0.245	0.545	0.455	0.245	0.545	0.455	0.245

its utility in data trustworthiness is preset to be 0.7. The proximity in geographic location and time are basically identical important to data trustworthiness, both of their utilities are set to be 0.15.

6.3. Data-centric trust model definition

Based on the above analysis and the basic utility theory, when node A receives a data report λ generated by node v, it can evaluate the data trustworthiness by Eq. (10).

$$B_{\lambda}^{v} = 0.7 \cdot T_{A}^{v} \cdot M(\tau(v), \tau(\lambda)) + 0.15 \cdot \mu_{l}(v, \lambda) + 0.15 \cdot \mu_{t}(v, \lambda) \tag{10}$$

It is obvious that the data-centric trust model is simple enough to realize fast trustworthiness evaluation. At the same time, all the factors are either predefined or determined with the data coming, and the data trustworthiness can be computed in real time. Since the trustworthiness of the same data from different reporters is usually different, the receiver can use the average of several trust values for the same event from different reporters as the final trust value.

6.4. Analysis

In order to verify the validity of the data-centric model, we take the 3 kinds of data from the 10 types of nodes as samples to estimate the data trustworthiness. For simplicity, we assume that the trustworthiness of the reporter is its weight. And the proximity in location and time are only considered three cases, which are the two extreme cases of the best and the worst, and the medium cases. The results are shown in Table 5, where $T1_X$ and $T3_X$ are the trustworthiness of the data type X when the proximity in location and time in the best and worst cases respectively; and $T2_X$ is the trustworthiness of the data type X when the proximity in location and time in the medium cases.

It can be seen from Table 5 that the trustworthiness of the data mainly determined by the trustworthiness of the reporter and the relation between it and the data. The proximity in location and time is used to amend the data trustworthiness. Different nodes usually have different impacts on the data trustworthiness. It should be noted that the data trust model is established mainly on experiences, and most of the parameters and default values are derived from the experiences in traffic. Although the results are basically in line with the real life, the data trustworthiness can be further processed according to the security requirements in practice so as to improve the quality of the data.

7. Conclusion

In order to acquire reliable data and make the applications work efficiently in the VANETs, a dynamic entity-centric trust model is firstly proposed on the basis of the applications catalogues and nodes authority levels. The proposed model can accommodate the dynamic environment in VANETs by introducing a dynamic adjustment factor α to balance the direct trust and recommendation. It is validated by being applied to the routing protocol GPSR and compared with I-GPSR and T-GPSR in three scenarios. The simulation results show that it can improve the reliable data delivery rate and resist black-hole attack and selective forwarding attack without causing distinct decrement in routing performances. Based on it, a data-centric trust model is put forward to evaluate the trustworthiness of the data. The analysis indicates that the data-centric trust model is simple enough to meet the requirement for fast trustworthiness evaluation. The data trustworthiness evaluations in different cases show it can work objectively and help the vehicles to improve the quality of the acquired data. But for the lots of experiences used in it, the data trust model should be further optimized in utility parameters and the default values in future.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grant No. 61471035 and 61601129. It was jointly supported by the Fundamental Research Funds for the Central Universities under Grant No. 06105031and Beijing Key Laboratory of Knowledge Engineering for Materials Science.

References

[1] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on Vehicular Ad Hoc Network, J. Netw. Comput Appl. 37 (2014) 380–392.
[2] M. Raya, J.-P. Hubaux, Securing Vehicular Ad Hoc Networks, J. Comput. Secur. 15 (1) (2007) 39–68.
[3] G. Yan, S. Olariu, M.C. Weigle, Providing VANET security through active position detection, Comput. Commun. 31 (12) (2008) 2883–2897.
[4] W. Dou, H.M. Wang, J. Yall, A recommendation based peer-to-peer trust model[J]., J. Software 15 (4) (2004) 571–583.
[5] J. He, Y. Liu, J. Wang, A robust model for trusted routing in VANETs, J. Wuhan Univ. 56 (2) (2010) 189–193 (Nat. Sci. Ed.).
[6] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, A. Tolba, A greedy model with small world for improving the robustness of heterogeneous Internet of things, Comput Netw. 101 (6) (2016) 127–143.
[7] S.A. Soleymani, A.H. Abdullah, W.H. Hassan, M.H. Anisi, S. Goudarzi, M.A.R. Baee, S. Mandala, Trust management in vehicular ad hoc network: a systematic review, EURASIP J. Wirel. Commun. Netw. (2015) 146.
[8] R.A. Shaikh, A.S. Alzahrani, Intrusion-aware trust model for Vehicular Ad Hoc Networks, Secur. Commun. Netw. 7 (11) (2014) 1652–1669.
[9] M. Raya, P. Papadimitratos, V.D. Gligor, J.P. Hubaux, On data-centric trust establishment in ephemeral Ad Hoc Networks, IEEE INFOCOM. (2008) 1912–1920.
[10] J. Zhang, Trust management for VANETs: challenges, desired properties and future directions, Int. J. Distrib. Syst. Technol. 3 (1) (2012) 48–62.
[11] J. Zhang, A survey on trust management for VANETs, 2011 International Conference on Advanced Information Networking and Applications.IEEE Computer Society, pp.105–112.
[12] Y. Xiao, S. Zheng, B. Sun, Trusted GPSR protocol without reputation faking in VANET, J. China Univ. Posts Telecommun. 22 (Oct (5)) (2015) 22–31.
[13] Z. Huang, S. Ruj, M.A. Cavenaghi, M. Stojmenovic, A. Nayak, A social network approach to trust management in VANETs, Peer-to-Peer Netw. 7 (3) (2014) 229–242.

[14] F.G. Mármol, G.M. Pérez, TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, J. Netw.Comput. Appl. 35 (3) (2012) 934–941.
[15] J. Finnson, J. Zhang, T. Tran, U.F. Minhas, R. Cohen, A framework for modeling trustworthiness of users in mobile Vehicular Ad-Hoc Networks and its validation through simulated traffic flow. UMAP 2012, LNCS 7379, pp.76–87.
[16] A. Ahmed, K. ABU Bakar, M.I. Channa, K. Haseeb, A.W. Khan, A survey on trust based detection and isolation of malicious nodes in Ad-Hoc and Sensor Networks, Front. Comput. Sci. 9 (2) (2015) 280–296.
[17] A. Wu, J. Ma, S. Zhang, in: The 7th International Conference On Communications, Networking and Mobile Computing (WiCOM). RATE: a RSU-aided scheme for data-centric trust establishment in VANETs, Wuhan, China, IEEE, 2011, pp. 1–6.
[18] Q. Ding, X. Li, M. Jiang, X. Zhou, A novel reputation management framework for Vehicular Ad Hoc Networks, Int. J. Multimedia Technol. 3 (2) (2013) 62–66.
[19] S. Gurung, D. Lin, A. Squicciarini, E. Bertino, Information-oriented trustworthiness evaluation in Vehicular Ad-Hoc Networks, in: Network and System Security-7th International Conference, NSS 2013, Madrid, Spain, Springer, 2013, pp. 94–108.
[20] Y.M. Chen, Y.C. Wei, A beacon-based trust management system for enhancing user centric location privacy in VANETs, J Commun Netw. 15 (2) (2013) 153–163.
[21] Y.C. Wei, Y.M. Chen, Human centric technology and service in smart space, HumanCom 2012, in: Reliability And Efficiency Improvement For Trust Management Model In VANETs, Springer, 2012, pp. 105–112.
[22] S. Ma, O. Wolfson, J. Lin, A survey on trust management for intelligent transportation system, in: Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science, Chicago, IL, USA, ACM, 2011, pp. 18–23.
[23] T. Qiu, C. Lin, W. Guo, Y. Zhang, STETS: a novel energy-efficient time synchronization scheme based on embedded networking devices, Microprocess. Microsyst. 39 (8) (2015) 1285–1295.
[24] K. Golestan, R. Soua, F. Karray, M.S. Kamel, A model for situation and threat/impact assessment in Vehicular Ad-hoc Networks, DIVANet'14, September 21-26, 2014 September 21–26.
[25] F. Dotzer, L. Fischer, P. Magiera, VARs: a vehicle Ad-Hoc Network reputation system [C]., in: Proceedings of the Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, IEEE Computer Society, 2005, pp. 454–456.
[26] M. Pophali, S. Mohod, T.S. Yengantiwar, Trust based opportunistic routing protocol for VANET communication, Int. J. Eng. Comput. Sci. 3 (8) (2014) 7408–7414.
[27] T. Qiu, W. Sun, Y. Bai, Y. Zhou, An efficient multi-path self-organizing strategy in Internet of things, Wirel. Pers. Commun. 73 (4) (2013) 1613–1629.

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011

Xuanxia Yao received her B.S. degree from Jiangsu University, M.S. and Ph.D. degree from University of Science and Technology Beijing (USTB), China. She is an associate professor in School of Computer and Communication Engineering. Her current research interests include network security, Ad Hoc Networks, Internet of Things and cloud computing. She is the author of one book, more than 20 articles.

Xinlei Zhang is working in the software center of Bank of China currently. She received her Master's Degree in Computer Science from University of Science and Technology Beijing, China, in 2015. Her research interests include wireless sensor networks, vehicular networks, delay tolerant networks, distributed algorithms and routing protocols.

Huansheng Ning received the BS degree from Anhui University in 1996 and the PhD degree from Beihang University in 2001. He is a professor in the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interests include Internet of Things, aviation security, electromagnetic sensing and computing. He has published more than 50 papers in journals, international conferences/workshops. He is a senior member of the IEEE

Pengjian Li received his B.S. degree in Computer Science and Technology from Qingdao Agricultural University in 2013. Now he is a Master candidate in School of Computer and Communication Engineering, University of Science and Technology Beijing. His research interests include network security, intelligent network and intelligent communication.

Please cite this article as: X. Yao et al., Using trust model to ensure reliable data acquisition in VANETs, Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.10.011