Reputation-based Trust Model in Vehicular Ad Hoc Networks

Qing Ding
School of Software Engineering
University of Science and Technology of China
Hefei China
dingqing@ustc.edu.cn

Ming Jiang
School of Software Engineering
University of Science and Technology of China
Hefei China
jjmm@ustc.edu.cn

Xi Li
School of Software Engineering
University of Science and Technology of China
Hefei China
llxx@ustc.edu.cn

XueHai Zhou
School of Software Engineering
University of Science and Technology of China
Hefei China
xhzhou@ustc.edu.cn

Abstract—Vehicular Ad Hoc Networks (VANETs) are received more and more researchers' attention with their promising functions in road safety by exchanging real-time warning messages through vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. However, an inaccurate traffic warning message will impact drivers' decisions, misguide drivers' behavior, and even invoke serious car accidents. In this paper, we proposed an event-based reputation model to filter bogus warning messages. Our solution is classifying all vehicles encounter the same traffic event different roles. A dynamic role-dependent reputation evaluation mechanism is presented to determine whether an incoming traffic message is significant and trustworthy to the driver. The simulation results show that our proposed system can effectively prevent false messages spread on VANET environments.

Keywords-VANET;Trust;Event-based

I. INTRODUCTION

In recent years, traffic safety applications [1] on Vehicular Ad Hoc Networks (VANETs) [2] have been developed to enhance the safety of drivers and improve mobility. VANETs are a subclass of MANETs, which would perform crucial functions in road safety, such as detection of traffic accidents and reduction of traffic congestions by exchanging real-time warning messages through vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. However, in this environment, a malicious attacker can create bogus traffic warning messages to impact other drivers' behaviors and cause intelligent collisions [3]. To determine whether the traffic event reported by a warning message is really occurred and prevent false traffic warning messages spread on VANET, various secure communication protocols and trust systems have been proposed. However trust establishment is a major challenge in VANETs, since VANETs have several distinctive properties compared to standard ad hoc networks.

In this paper, we develop a novel trust model for VANETs. The rest of this paper is structured as follows. The related work is introduced in section 2. In section 3,

978-1-4244-7555-1/10/$26.00 ©2010 IEEE

the event-based reputation model is detailedly discussed. We give the details about the reputation value computational formula in section 4. In section 5, we show the initial simulation results. The final section summarizes the paper and gives the suggestion for future works.

II. Related Work

In [4], trust establishment is divided into two major categories: it can either statically rely on a security infrastructure or be built up dynamically in a self-organizing manner. The former process mainly relies on classical global certificate-based systems. The latter process lacks of this global knowledge and needs to take advantage of other trust supporting mechanisms.

Recently most proposals on VANET security [5-9] provide the option of using Public Key Infrastructure (PKI) services in authentication while preserving traceability and revocation once such credentials are misused. For these systems, the design of mechanisms to disseminate the revocation information across VANETs is the main challenge. Due to the network volatility and scale, the overhead of querying a server to obtain timely revocation status could be impractically high since there is not a permanent connection to this infrastructure. Different aspects of revocation were discussed in [7-9].

Establishing reputation systems is also a good choice to establish trust. We can find many examples in ad hoc networks [10-14]. There are also some papers about reputation establishment in VANETs [15-18]. Vehicle Ad-Hoc Reputation System (VARS) [15] presents a message protocol that opinions are appended for packet forwarding, then everyone can makes use of these opinions to calculate reputation. Anand et al. [16] propose a context-aware reputation management system that provides a bootstrapping process to build trust relationships and stimulates proactive collaboration. However, such relatively "static" reputation maintenance scheme is not suitable for the highly dynamic VANETs. In [17], a data-centric trust establishment framework is proposed. The novel concept is to evaluate the trustiness of sensed data or received messages rather than the trust of individual vehicle. However, the authors did not consider the effect introduced by the dynamics of traffic events. Nai-Wei Lo et al. [18] also proposed an event-based reputation system architecture in VANETs. But the reputation value computing mechanism of a traffic event is only depending on frequency that this event is detected by a vehicle within a pre-defined duration. It seems not sufficient for a complex application environment.

In this paper, we design an event-based reputation system to filter out bogus messages spread by malicious attackers in VANETs. In contrast to Nai-Wei's method, we propose a more complex model which categorizes all vehicles encounter the same traffic event to different roles. Reputation functions are designed for these different roles. Each role has own reputation evaluation mechanism to determine whether an incoming traffic message is trusted.

III. Reputation Model

A. *Role Definition*

First, depending on the different role vehicles played encounter the same traffic event, we categorize them as shown in figure 1.

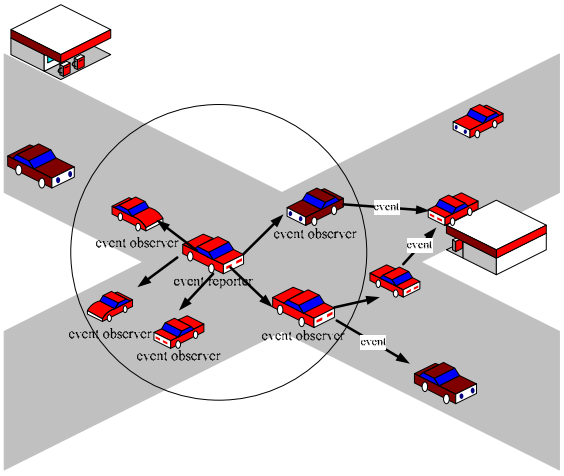

Figure 1. Categorize Member

- *Event Reporter (ER):* we call a vehicle an event reporter, if it can perceive incident by equipped sensors, then send alarm messages to other neighboring vehicles.
- *Event Observer (EO)*: within one hop of an

event reporter, vehicles can observe the behavior of event reporter when they receive the event message from it. We call these vehicles event observers.

- *Event Participant (EP):* we call other vehicles beyond one hop of an event reporter as event participants, since they can receive and forward the event message, but it is impossible to identify the behavior of event reporter.

B. Event Propagation

In our model, traffic information comes both from received messages via wireless interface and on-board sensors. Every vehicle has an event table which stores all received and derived traffic event information, such as event ID, event type, occurrence timestamp, event location, transmission range, and event reputation value. In the event table, each record entry stores a distinct traffic event. A sensor can detect the same event many times after a traffic event occurrence, then these detect event messages are assigned a unique ID.

When an ER encounters a traffic event, traffic-related data will be collected by sensors in this vehicle. Depending on the detect frequency, ER can estimate the severity of this traffic event and set the reputation value of it. If this value is over the predefined threshold, the event message will be sent to the traffic safety application in the vehicle and to all neighbors in one hop, namely EO.

In our design, EO is a very important role to identify bogus event messages. When an EO receives a traffic warning message from an ER, it will first store this message into the event table if there is no the same ID record in the table. Within ΔT time, this EO can receive the event message with this ID n times from this ER. By observing succeeding behavior of ER in this phase, an EO can estimate the truthfulness of this event message though it does not encounter the event directly. Intuitively, if the behavior of ER matches the typical behavior model related to the traffic event type, the event message is considered as trusty. For example, when an ER sends an "obstacle" type event message, the "correct" corresponding driver behavior should be "decelerate" or "change lane". So if an EO found other behaviors of an ER except standard behavior model, it is reasonable to confer that this event message from the ER maybe bogus. Then the reputation value of this event message is set to low by this EO. At the same time, this EO maybe receive many event messages with this ID from other ERs, EOs and EPs, we give a complex formula to integrate all these second-hand information in next section.

For an EP, it only can receive messages from EOs and other EPs. In next section, we also give a formula to calculate reputation value of event messages for EPs.

IV. Reputation Calculation

We mainly deal with the computational aspects of trust values in this section. Since there are different application contexts, and different roles of the vehicles involved in the same traffic event, we design various reputation functions matching these characters below.

A. Reputation Value of Event Calculated by ERs

For ERs, information from sensors is only available data source to calculate reputation value of an event. Incorporating the event type, and event frequency, an ER *i* computes the reputation value of an event j by Eq.1.

$$\mathrm{R}_{\mathrm{j}}^{\mathrm{ER_i}} = C_e \frac{E_f}{E_s} \tag{1}$$

where C_e is a pre-defined reputation value constant in accordance with event type, E_f is the real event frequency received from sensors, and E_S is the standard frequency for this type of event.

B. Reputation Value of Event Calculated by EOs

For an EO, it should collect enough information to discriminate bogus messages when it receives messages from an ER. The available information includes the reputation value of the event sent by ERs, succeeding behavior of ERs observed by this EO, and the reputation value of the event sent by other EOs. We ignore the impact of EPs. For an event *j*, the reputation value calculated by the EO *i* is presented by Eq.2.

$$R_j^{EO_i}(t) = \alpha \frac{\sum_{k \in M} D_k(\nabla t) * R_j^{ER_k}}{m} + \beta \frac{\sum_{o_l \neq o_i} R_j^{EO_l}(\nabla t)}{n} \quad (2)$$

where $D_k(\nabla t)$ is the degree of ER k's behavior deviation within ΔT time after the event message is sent. How to get $D_k(\nabla t)$ will be discussed in another paper. $R_j^{ER_k}$ is the reputation value of event j calculated by ER k in the message. $R_j^{EO_i}(\nabla t)$ is the reputation value of event j calculated by any EO l cexcept EO i in the message. m is the number of all ERs sent the message to EO i, and n is the number of all EOs sent the message to EO i within ΔT time. α and β is the weight, and α+β=1. In general, the observation to ERs' behavior plays more important role in the process of computing reputation value. So α is bigger.

C. *Reputation Value of Event Calculated by EPs*

For an EP, by integrating data from EOs and EPs, we give the reputation value calculation formula by Eq.3.

$$R_j^{EP_n}(t) = \alpha \frac{\sum_{o \in k} R_j^{EO_o}(\nabla t)}{k} + \beta \frac{\sum_{m \in l} R_j^{EP_m}(\nabla t)}{l} \quad (3)$$

where $R_j^{EO_o}(\nabla t)$ is the reputation value of event j calculated by an EO *o*, and $R_j^{EP_m}(\nabla t)$ is the reputation value of event j calculated by an EP *m*. k is the number of all EOs sent the message to this EP, and l is the number of all EPs sent the message to this EP within ΔT time. Similarly, α+β=1, and α is bigger in most cases.

V. Simulation Results

VANETs simulator TraNS [19] is used to evaluate system performance of the proposed event-based reputation system. The simulation scenario is set in a grid-typed street map. As shown in Figure 2, the map is constructed by 5 × 5 street blocks and each is a 150 meters square. We simulate movement of vehicles in this area as the random waypoint model with speeds ranging from 10 m/s to 40 m/s and pause times from 0 to 30s, for a simulation period of 800 seconds. Vehicles randomly placed on roads in the scenario map. Transmission range of vehicles is 100m. Both source nodes and relay nodes can be bad vehicles will try to send a misleading message. Each measured result is an average number obtained from 100 replications of simulation runs.

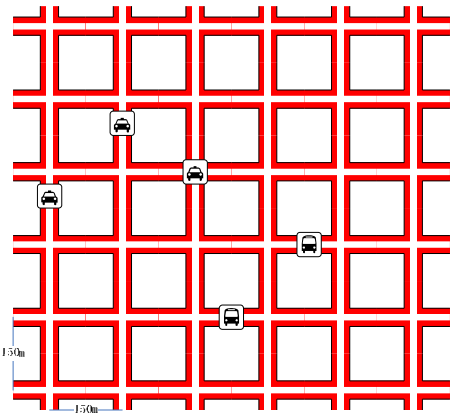

Figure 2. The Street Map Used in Simulations.

A. *Effect of Numerous False Messages.*

In this scenario, our aim is to measure the availability of data, the reliability of data, and the response times of data in the global view. We evaluate efficiency and validity of the model when there are 0%, 20%, and 40% bad nodes respectively in the system.

Fig. 3 shows the average ratios of number of messages from untrusted sources (MU), number of messages validated (MV), number of messages invalidated (MI) to the total number of messages in the simulation, when the number of vehicles is 50, 100, 150 and 200 respectively. We define the ratio of malicious sources to all bad nodes is 25%. It can be observed that MI declines with the increase in total number of vehicles. This is reasonable since the traffic density has a positive influence to the message deliver. It also can be seen that MI increases and MV decreases as the number of bad nodes increases. However the resilience and merit of the reputation model

is highlighted by the fact that the decreases of MV can be seen to be somewhat slow. The reason is that the message received from unknown sources was later validated. The bogus message from bad source or bad relay nodes can be marked by later nodes with high possibility even the number of bad nodes has somewhat high.

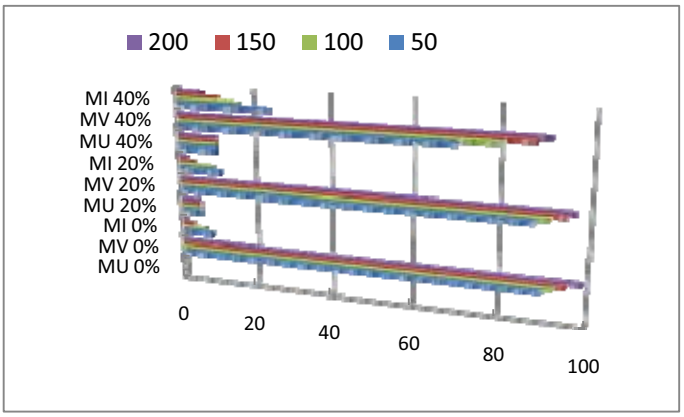

Figure 3. the Number of Affected Vehicles

B. Effect of Single False Message.

To test the effectiveness of our model against false message flooding attack more carefully, we first perform the simulation below to measure the influence of false messages to our model. During simulation executions, there is a randomly selected vehicle node to broadcast bogus traffic messages every 10 seconds. Other vehicles receive this message, validate it respectively, and forward it again. The vehicle trusts this message and notifies its driver this false event is defined as a message affected vehicle. Figure 4 shows the number of vehicles affected by a real traffic event increases quickly during the diffusion of message. On the other hand, benefiting from our reputation computational model, the false messages generated from a malicious source does not affect other vehicles essentially. In Figure 5, the average reputation value of a real traffic event keeps high in all kinds of vehicle mobility environments. On the contrary, in Figure 6, the average reputation value of a false traffic event which is high at the beginning of simulation declines quickly and oscillates between -0.6 and -0.8 in all kinds of vehicle mobility environments.

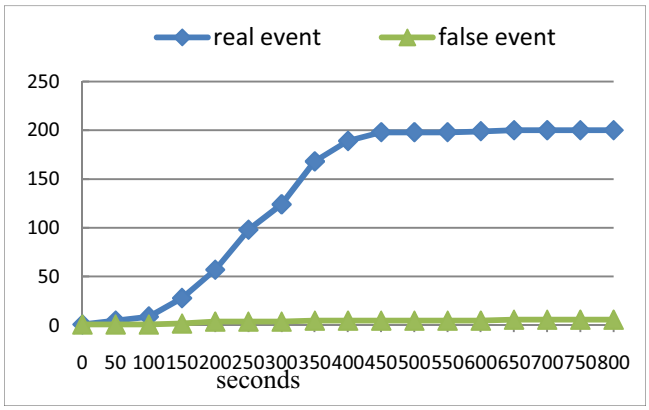

Figure 4. the Number of Affected Vehicles

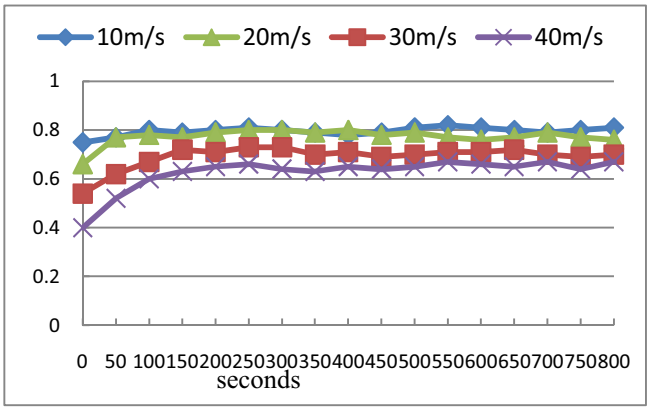

Figure 5. Average Reputation Value of a Real Traffic Event

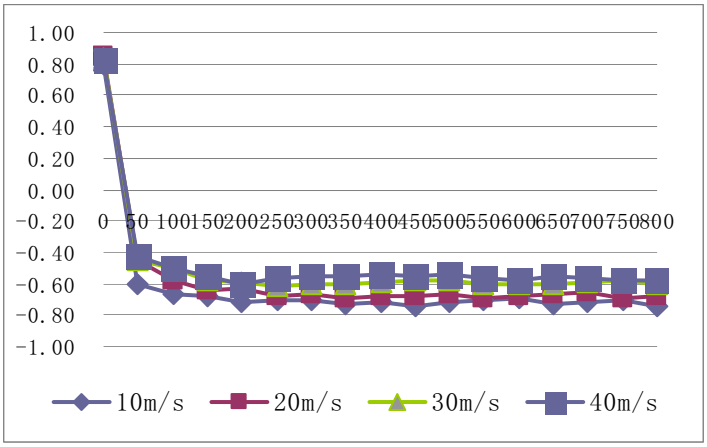

Figure 6. Average Reputation Value of a False Traffic Event

In summary, the simulation results show that our proposed event-based reputation system can be competent for filtering bogus message, and propagating accurate and reliable traffic warning messages in most VANET environments.

VI. Conclusions and Future Works

In this paper, an event-based reputation model is presented to enhance trust for Vehicular Ad Hoc Networks. The proposed model takes the impact of the location of vehicles into account. All vehicles encounter the same traffic event are classified to different roles. For different roles, we design different computational models to calculate this events' reputation value. A dynamic role-dependent reputation evaluation mechanism is presented to filter bogus warning messages. Network simulation experiments show that significant performance gains can be gotten using this framework.

For the future work, first we are planning to evaluate the impact of various weights in equation (2) and (3) and further introduce fuzzy theory into calculating reputation value of an event. Moreover, the random waypoint model adopted in this simulation is not very suitable for VANETs environment. So a new mobility model for VANETs should be presented. We can apply this model to differentiate misbehavior of vehicles.

Reference

[1] J. Luo and J. P. Hubaux, "A survey of inter-vehicle communication," Tech. Rep. IC/2004/24, EPFL, Lausanne, Switzerland, 2004

[2] J. J. Blum, A. Eskandarian, and L. J. Huffman, "Challenges of intervehicle ad hoc networks," IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, pp. 347–351, 2004

[3] F. D¨otzer, M. Strassberger, and T. Kosch, "Classification for traffic related inter-vehicle messaging," in Proceedings of the 5th IEEE International Conference on ITS Telecommunication (ITST '07), Brest, France, June 2005.

[4] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller and Luca Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks", 67th IEEE Vehicular Technology Conference (VTC2008-Spring), Marina Bay, Singapore, May 11–14, 2008.

[5] M. Raya, J.-P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (1) (2007) 39−68. special issue on Security of Ad Hoc and Sensor Networks.

[6] J. Sun, C. Zhang, Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks", in: Proc. IEEE Military Communications Conf., October, 2007, pp. 1−7.

[7] IEEE P1609.2 Version 1 – "Standard for Wireless Access in Vehicular Environments−Security Services for Applications and Management Messages". In development, 2006.

[8] X. Lin, X. Sun, P.-H. Ho, X. Shen, "GSIS: a secure and privacypreserving protocol for vehicular communications", IEEE Trans. Vehicular Tech. 56 (6) (2007) 3442−3456.

[9] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A localized certificate revocation scheme for mobile ad hoc networks", Ad Hoc Networks, 6(1):17–31, January 2008.

[10] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of Nodes: Fairness In Dynamic Ad-hoc networks," in Proc of MobiHoc. ACM, 2002, pp. 226–236.

[11] S. Buchegger and J.-Y. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in Proc. of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'03), 2003.

[12] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[13] Haiying Shen, Ze Li, "ARM: An Account-Based Hierarchical Reputation Management System for Wireless Ad Hoc Networks", Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on, 17-20 June 2008, On page(s): 370-375.

[14] Ciszkowski T, Kotulski Z, "Distributed Reputation Management in Collaborative Environment of Anonymous MANETs", EUROCON, 2007. The International Conference on "Computer as a Tool", 9-12 Sept. 2007, On page(s): 1028-1033.

[15] F. Dotzer, L. Fischer, and P. Magiera, "VARS:AVehilceAd-hoc networkReputation System", sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), pp. 454–456, 2005.

[16] Patwardhan, Anand Joshi, Anupam Finin, Tim Yesha, Yelena , "A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks", Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference 17-21 July 2006, On page(s): 1-8

[17] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08), pp. 1238–1246, April 2008.

[18] Nai-Wei Lo and Hsiao-Chien Tsai, "A Reputation Systemfor Traffic Safety Event on Vehicular Ad Hoc Networks", EURASIP Journal onWireless Communications and Networking Volume 2009, Article ID 125348, 10 pages.

[19] Michal Piorkowski, Maxim Raya，C.: "TraNS: Realistic Joint Traffic and Network Simulator for VANETs", ACM SIGMOBILE Mobile Computing and Communications Review, Volume 12, Issue 1 (January 2008)