Reliability and Efficiency Improvement for Trust Management Model in VANETs

Yu-Chih Wei[1,2] and Yi-Ming Chen[1]

[1] Dept. of Information Management, National Central University, Taoyuan, Taiwan, R.O.C
[2] Telecommunication Laboratories, Chunghwa Telecom Co., Ltd, Taoyuan, Taiwan, R.O.C
vickrey@cht.com.tw, cym@cc.ncu.edu.tw

Abstract. In VANETs, how to determine the trustworthiness of event messages has received a great deal of attentions in recent years for improving the safety and location privacy of vehicles. Among these research studies, the accuracy and delay of trustworthiness decision are both important problems. In this paper, we propose a road-side unit (RSU) and beacon-based trust management model, called RaBTM, which aims to prorogate message opinions quickly while thwart internal attackers to send or forwarding forged messages in privacy-enhanced VANETs. To evaluate the reliability and efficiency of the proposed system, we conducted a set of simulations under alteration attacks and bogus message attacks with various adversary ratios. The simulation results show that the proposed RaBTM is highly resilient to adversarial attacks and performs at least 20% better than weighted vote (WV) scheme.

Keywords: VANET, RSU-aided, Trust, Safety.

1 Introduction

With vehicular ad-hoc networks (VANETs), vehicles are able to communicate with each other via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. In order to enhance drive safety, many VANETs safety applications require vehicles to periodically broadcast single-hop messages to other vehicles. These periodic broadcast messages are called beacon messages. In addition to beacon message, vehicles also broadcast event-driven warning messages, such as Electronic Emergency Break Lights (EEBL), and Post-Crash Notifications (PCN) etc. [1], to neighboring vehicles. These event-driven warning messages are called event messages. If these event messages were abused, however, it may raise new safety risks for the whole transportation system [2].

To overcome the safety threats of VANETs mentioned above, one common method is message authentication. For ensuring the integrity of transmitted messages, cryptographic mechanisms have been widely employed to protect VANETs against unauthorized message alterations. However, the message authentication method can only ensure that messages are sent from legitimate senders, but cannot prevent a legitimate sender from broadcasting bogus or altered messages malevolently to other

James J. (Jong Hyuk) Park et al. (eds.), *Human Centric Technology and Service in Smart Space,*
LNEE 182, pp. 105–112, DOI: 10.1007/978-94-007-5085-2_14,

vehicles. These bogus or altered messages not only decrease the transportation efficiency, but also in the worst cases, they may cause accidental events that can threaten human life. Another common method to treat the safety threat of VANET is to establish trust relationships and detect malevolent behavior in VANETs [3], this method enables vehicles to distinguish trustworthy vehicles or messages from untrustworthy ones, therefore reducing the risk of vehicles being misguided by other malicious vehicles. However, there is still a big challenge for the success of this method. If adversaries do not alter original event message but just forward opposite opinions faster than the trustworthy vehicles do, a vehicle will be misled due to more malicious vehicles forward and provide their opinions to support the bogus messages or opposite the normal messages.

To overcome the problems encountered by above methods, in this paper, we propose a novel RSU and Beacon-based trust management model called RaBTM. With RSU's assistance, the proposed system can perform reliably and efficiently with high malicious vehicle rate. We have conducted a set of simulations. All simulations considered different attack models, including alteration attacks and bogus message attacks. The simulation results show that the performance of the proposed RaBTM is at least 20% better than that of WV method [4], and the decision delay is reduced by more than 22%.

The rest of this paper is organized as following: Section 2 describes the related work. Section 3 depicts the RSU aided trust management model. Section 4 describes the evaluation methods and simulation results of the proposed system, and Section 5 presents our conclusions and future work.

2 Related Work

In VANETs, entity trust is the traditional notion of trust. Dotzer *et al.* [3] proposed a distributed entity-centric reputation system named VARS, which can share trust opinions among neighboring vehicles in VANETs. In their proposed system, every message forwarder appends their opinion about the vehicle's trustworthiness to the message. However, VARS is not suitable in an ephemeral environment for the message size will become larger and larger due to the piggybacking of opinions. Based on the assumption that most vehicles are honest and will not endorse any message containing false data [5]. Ostermaier *et al.* [4] proposed a simple and straightforward voting scheme to evaluate the plausibility of received hazard messages. Lo and Tsai [6] also proposed an event-based reputation system to prevent the spread of false traffic warning messages in VANETs. They introduced a dynamic reputation-evaluation mechanism to determine the trustworthiness of the event messages. In order to overcome the dependence of slow-to-change entity trust, Raya *et al.* [7] proposed a data-centric trust management model for VANETs. In their proposed system, data trustworthiness would focus on data per se, such as position and timestamp of event message, rather than merely on the trustworthiness of the data-reporting vehicles. They also evaluated some decision logic, such as voting, Bayesian inference (BI) and the Dempster-Shafer Theory (DST). Their model, however, focuses only on the data and they do not leverage the trustworthiness of sender or forwarder of event messages.

Existing researches on reputation systems [3-7] for VANETs mainly collect event-based messages for decision-making, while neglecting beacon messages, which are also useful in determining the trustworthiness of event messages in reputation systems. To remedy this shortcoming, we propose an RSU-aided hybrid trust mechanism, which allows both OBUs and RSUs to construct entity trust by cross-checking the plausibility of event messages and beacon messages. Although, Wu *et al.* has also proposed an RSU-aided scheme, named RATE [8], the data delivery delay was a major problem. This delay comes from three phases of RATE process, which includes data collection phase, data analysis phase and the data dissemination. In our proposed system, we overcome this delay problem by leverage the RSUs' fast opinion trustworthiness calculations. In the next section, we will introduce our proposed method in detail.

3 Methodology

3.1 RSU Aided Trust Management

In trust management model, neighbor vehicles' opinions are still very important for a vehicle to make decision. However, as mentioned above, how to deal with the large volume of fast responded opposite opinions is still a big challenge for existing researches, which only rely on V2V communications. To deal with this challenge, we adopt both V2V and V2I communications. Generally, RSU plays an important role in VANETs applications. They are responsible for providing more reliable trustworthiness information or assisting in forwarding messages to other vehicles within transmission radius. RSUs are always placed on the roadside that OBUs can exchange messages with them. Messages transmitted from RSUs are much more trustworthy than those from other vehicles [8]. As shown in Fig. 1, when a vehicle is on the road, it periodically disseminates beacon messages that can be gathered by the near RSUs, along with event messages. If RSUs can provide trustworthiness information regarding the vehicles near it, this will be very helpful for vehicles' to decide which message is trustworthier. However, not every RSU can collect enough information to give its opinions to neighboring vehicles, and in worse case, some RSUs may be cheated by malicious vehicles. Take Fig. 1 as an example, vehicle *S* has a traffic accident and immediately transmits a PCN event message to other vehicles. After vehicle *S* broadcasts the PCN event message, vehicles *A, B, C, D, E,* and *F* will receive this PCN message. If vehicles *D, E,* and *F* recognize that this message will not influence other vehicles, they will not forward the event message and drop it. Assuming that vehicles *A* and *B* are honest one, and vehicle *C* is an attacker. When honest vehicles *A* and *B* forward the PCN message with their positive opinion to vehicle *R*, malicious vehicle *C* may forward this PCN message with the opposite opinion to disturb vehicle *R*'s decision. In the RSU-aided scheme, vehicle *R* can receive forwarded indirect event messages with their opinions from both RSU_2 and RSU_5. Assuming that when a RSU is closer to the original event message sender, it is more likely to collect more helpful

information and to reduce the likelihood of being cheated. In the example of vehicle R, the received opinion message from RSU_5 is more useful than that of RSU_2. This is because the distance between message sender S and RSU_5 is much closer than the distance between S and RSU_2. To give a more quantitative measure for a vehicle to evaluate the opinion confidence of RSUs, we propose a distance-based RSU opinion confidence calculation method. Here, the confidence of RSU's opinion O_{rsu} , which can provide the OBUs with relevant information to decide about the transmission of the result in the network, is calculated as:

$$O_{rsu} = \sum_{r \in R}^{|R|} T_{devt}^{r,s} \frac{(D_{tot} - d_{r,s})}{D_{tot}(|R|-1)} \tag{1}$$

R is the set of RSUs that receive the original event message and $|R|$ is the number of elements in the set R. T_{devt} is the direct trust value of vehicle r and s which calculated by Tanimoto coefficient to get the similarity between historical beacon message and received event message [9]. D_{tot} is the total distance from sender s to all of the RSUs positions. $d_{r,s}$ is the distance between the RSU_r and the position of the event message sender s. To avoid being cheated by malicious vehicles, in our proposed scheme, RSUs only give opinions to the original event message and forward them to other vehicles.

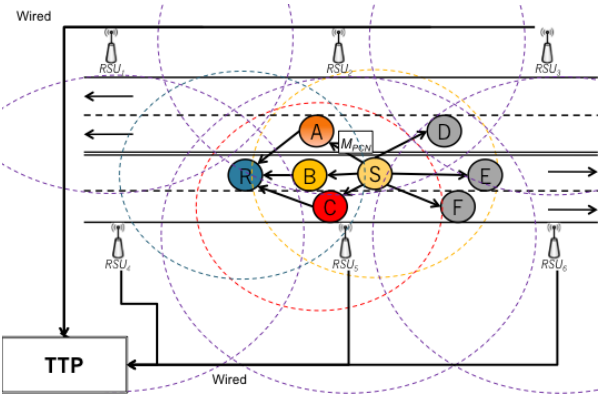

Fig. 1. Illustration of the relation of vehicle's OBUs and RSUs

Due to the infrastructure cost, it is difficult to cover the full area of roads with a large number of RSUs. [10] In some areas having low-density deployment of RSUs, such as suburbs or areas with sparse populations, may prevent some vehicles from receiving RSUs' opinions of event messages. To take this circumstance into consideration, we define (2) to resolve this problem.

$$T_{oval}(e) = \begin{cases} (1-\gamma)T_{ds} + \gamma O_{rsu} & , if\ (|R|>0) \\ T_{ds} & , otherwise \end{cases} \tag{2}$$

As shown in (2), if an observation vehicle can receive event opinions from RSUs, the overall event trust value T_{oval} is composite with T_{ds} and O_{rsu} with γ where γ is a constant. Otherwise, if an observation vehicle does not receive any event opinions from RSUs, it uses the T_{ds} for the overall event trust value to make its forwarding decisions and opinions. After the observation vehicle calculates the overall event trust value T_{oval} from data sources. It will make a decision based on the threshold of trust degree T_{thld}.

3.2 Trust Combining

When a vehicle receives direct event message or indirect event message opinions transmitted from multiple vehicles, an effective method to combine these received opinions of is needed. VANETs are ephemeral and fast-movement networks, in which there is not always a fixed infrastructure available to support security mechanisms. Besides, event messages may be lost due to the high uncertainty of the VANET. Thus, vehicles have to organize the trustworthiness of each vehicle and implement security protection schemes themselves. The Dempster-Shafer evidence combination method provides a convenient numerical computing method for aggregating multiple pieces of data [11]. In addition, DST does not require prior probability to compute the posterior probability of an event message, something that is difficult to determine in practice [12]. Hence, DST is more suitable for dealing with the problems of uncertainty, and it minimizes the performance downgrade introduced by node mobility. In this paper, in order to accommodate the nature of uncertainty of VANETs, we adopt DST for opinion combination. The combined trust value T_{ds} corresponding to an event is represented as in (3):

$$T_{ds}(i) = \bigoplus_{n=1}^{|N|} m_n(H_i) \tag{3}$$

where N is the set of vehicles that are the forwarders or senders of the received message, and $|N|$ is the number of vehicles in N.

4 Performance Evaluation

4.1 Adversary Model and Evaluation Method

In this paper, we consider an adversary to be a vehicle equipped with an OBU in a certain area of the VANET. The attacker can actively participate in the network and violate the integrity of messages, such as by broadcasting or forwarding malicious messages. Focused attack models are alteration attacks and bogus message attacks [13]. In alteration attacks, malicious vehicles modify or forge the opinion and trustworthiness of a multi-hop event messages, and then forward this message to others. In Bogus message attacks, malicious vehicles can generate and broadcast malicious event messages to other vehicles in the vicinity. In order to simulate the different adversary models in our proposed scheme, the attack behavior of an attack vehicle can be simulated through the assignment of attack functions. Three function parameters δ, ε, ω have been used in the adversary models: δ is the rate of

misbehavior vehicle, and ε is the alteration attack rate, and ω represents the bogus message rate.

In this paper, we adopt F-measure (denoted as F) [14], as shown in (4) to measure the overall performance of the proposed scheme. It is important to evaluate precision and recall in conjunction, owing to the easiness of optimizing either one separately. The F-measure is a weighted combination of precision, and its value ranges from 0 to 1.

$$F = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

We simulate the proposed system using ns-2 with the MAC layer parameters of IEEE 802.11. For each simulation, vehicles are randomly generated with random trip on paths routed across the street map. We then set out large-scale simulation with larger map to 5x5 street map. Then roads set to 3 lanes and maximum vehicle number set to 300 vehicles. In the comparison experiments, we take the performance of the WV method as a comparison baseline. In addition to WV, we also take our previous work BTM [9] into this comparison. Besides, in order to evaluate the detection delay of the proposed system, we also evaluate the time delay between the first event message received time and the decision making time.

4.2 Simulation Results

Effect of Detection Result

We evaluate the performance of the proposed scheme for different rates of misbehaving vehicles δ with $\varepsilon=0.5$ and $\omega=1$ under FSP with a beaconing interval of 1 second. As shown in Fig. 2(a), with a higher rate of the adversary vehicles, the detection results worsened. However, we can also see that the proposed RaBTM system can perform better than WV and BTM. The overall results for F are still more than 0.7 with an adversary ratio of up to 90%. The average F value of the proposed system is greater than 11.8% in comparison with the WV method. Furthermore, RaBTM is also outperforms than our previous work by almost 2.6%. In addition to the misbehaving vehicle rate, we also simulate with different densities. In Fig.2(b), we simulate with different number of vehicles on the same topology, ranging from 30 to 300 vehicles. The greater the number of vehicles on the road is, the higher the density of the topology is. In Fig. 2(b), we can see that the influence of the detection rate on density will degrade the RaBTM and BTM scheme more than WV scheme. However, RaBTM can still perform better than the BTM and WV schemes. The average detection rate in RaBTM is higher than that of WV by about 14.1%. This could indicate that our proposed system can still suit a high-density environment.

Effect of Detection Delay

As shown in Fig. 2(c), we can observe that the decision delay of the proposed system is still shorter than those of the WV and BTM schemes. Although the detection delays are get shorter due to the low delay in disturbing malicious event messages, RaBTM

can also provide shorter detection delays without degrade decision rate than other schemes. And as shown in Fig. 2(d), the decision delay of the proposed system can still show low latency in low-density circumstances. This is because that when a vehicle receives a RSU's opinion, it can quickly make a decision because the reliability is much higher than in other vehicles. Although there are fewer event opinions in low-density circumstances, a vehicle can still get assistance from RSUs to make decision. We can also see that in low-density circumstances, RaBTM has lower detection delay than other schemes. In Fig. 2(d), take 30 vehicles as an example, the detection delay is shorter than other schemes by over 100 milliseconds a performance improvement of about 50%.

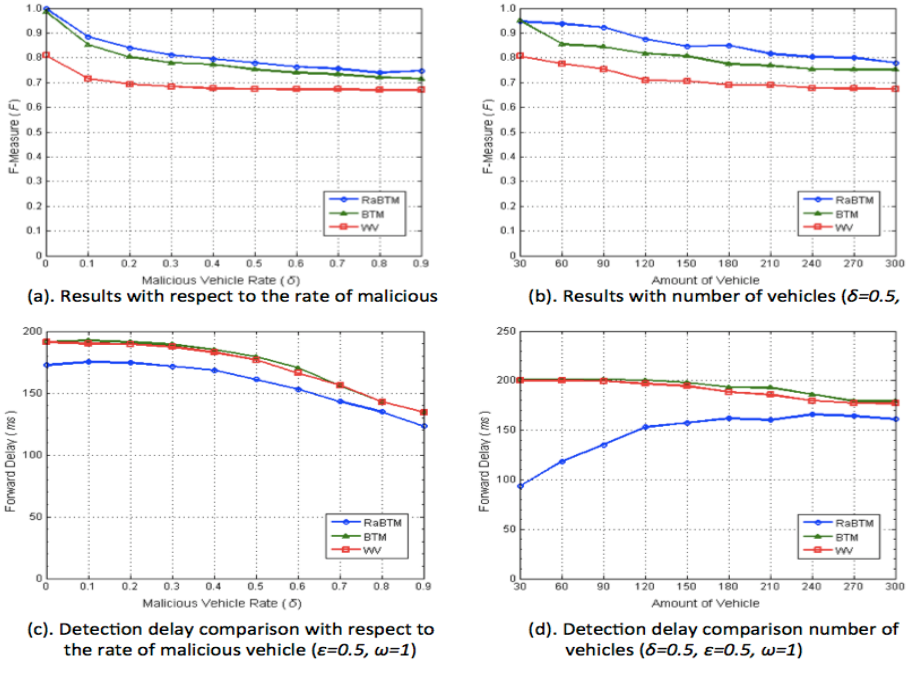

Fig. 2. Simulation results on detection performance

5 Conclusion

In this paper, we propose an RSU and beacon-based trust management model called RaBTM that aims to quickly make decisions and thwart internal malicious attackers more precisely in location privacy-enhanced VANETs. In this system, a vehicle cannot only utilize beacon messages and event messages to determine the trustworthiness of event messages from VANETs but also get assistance from RSUs' reliable opinions. The simulation results show that the proposed system is highly resilient to various attacks, such as alteration attacks and bogus attacks. Another important

contribution of our proposed system is that it can make decisions quickly and give opinions with a short delay. In our evaluation, the average F-measure value of the proposed system is 20% greater and the detection delay is 22% shorter than those of the WV method. Thus, we can conclude that the proposed RSU and beacon-based trust management model can not only withstand trust attack models, but also perform with higher efficiency than the WV and BTM schemes.

References

1. The CAMP Vehicle Safety Communications Consortium: Vehicle Safety Communications Project Task 3 Final Report: Identify intelligent vehicle safety applications enabled by DSRC. National HighwayTraffic Safety Administration (2005)
2. Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P., Shen, X.: Security in vehicular ad hoc networks. IEEE on Communications Magazine 46, 88–95 (2008)
3. Dotzer, F., Fischer, L., Magiera, P.: VARS: A Vehicle Ad-Hoc Network Reputation System. In: Proceedings of the Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, pp. 454–456. IEEE Computer Society (2005)
4. Ostermaier, B., Dotzer, F., Strassberger, M.: Enhancing the Security of Local Danger Warnings in VANETs - A Simulative Analysis of Voting Schemes. In: Proceedings of the The Second International Conference on Availability, Reliability and Security, pp. 422–431. IEEE Computer Society, Vienna (2007)
5. Wu, Q., Domingo-Ferrer, J., Gonzaìlez-Nicolaìs, U.R.: Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications. IEEE Transactions on Vehicular Technology 59, 559–573 (2010)
6. Lo, N.-W., Tsai, H.-C.: A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks. EURASIP Journal on Wireless Communications and Networking 2009 (2009)
7. Raya, M., Papadimitratos, P., Gligor, V.D., Hubaux, J.-P.: On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In: The 27th Conference on Computer Communications, IEEE INFOCOM 2008, Phoenix, AZ, pp. 1238–1246 (2008)
8. Aifeng, W., Jianqing, M., Shiyong, Z.: RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs. In: 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1–6 (2011)
9. Wei, Y.-C., Chen, Y.-M., Shan, H.-L.: Beacon-based trust management for location privacy enhancement VANETs. In: 2011 13th Asia-Pacific on Network Operations and Management Symposium (APNOMS), Taipei, Taiwan, pp. 1–8 (2011)
10. Abdrabou, A., Weihua, Z.: Probabilistic Delay Control and Road Side Unit Placement for Vehicular Ad Hoc Networks with Disrupted Connectivity. IEEE Journal on Selected Areas in Communications 29, 129–139 (2011)
11. Chen, T.M., Venkataramanan, V.: Dempster-Shafer theory for intrusion detection in ad hoc networks. IEEE on Internet Computing 9, 35–41 (2005)
12. Li, W., Joshi, A.: Outlier Detection in Ad Hoc Networks Using Dempster-Shafer Theory. In: Proceedings of the 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware. IEEE Computer Society (2009)
13. Aslam, B., Park, S., Zou, C., Turgut, D.: Secure Traffic Data Propagation in Vehicular Ad hoc Networks. Int. J. Ad Hoc and Ubiquitous Computing 6, 24–39 (2010)
14. Yang, Y., Liu, X.: A re-examination of text categorization methods. In: Proceedings of the 22nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 42–49. ACM, Berkeley (1999)