Research Journal of Applied Sciences, Engineering and Technology 5(17): 4406-4410, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 08, 2012 Accepted: December 21, 2012 Published: May 01, 2013

Detecting the Incorrect Safety Message in VANETS

[1, 2]Huibin Xu, [3]Limin Hua, [4]Yumei Ning and [1]Xiaoping Xue
[1]Department of Electronics and Information, Tongji University, Shanghai 200092, China
[2]Shanghai Normal University Tianhua College, Shanghai 201815, China
[3]School of Distance Learning, Zhengzhou University, Zhengzhou 450001, China
[4]School of Computer Science and Technology, Xidian University, Xi'an 710071, China

Abstract: There always are some vehicles (nodes) to demonstrate various misdemeanours, such as, modifying data, transmitting fraudulent data about road congestion or vehicle, due to the distinct characteristics of Vehicular Ad-Hoc Networks (VANETs). Those malicious data from safety message have the potential to damage in VANETs. Therefore, the received safety message should be verified before the message is accepted and relayed. In this study, we address the challenge by detecting incorrect safety message. We propose a novel approach to deal with evaluating the trustworthiness of safety message reported by neighbor vehicles by detecting the consistency between the actions and the words (safety message). If it is inconsistent, the safety message is recognized as incorrect message; otherwise, the message is accepted and relayed. Moreover, the safety precaution is considered to protect itself and minimize the losses. Simulation results show that our proposed method can detect effectively the incorrect safety message. The detection ration is about 90% when the number of malicious vehicles is small.

Keywords: Data validation, incorrect message, safety message, VANETS

INTRODUCTION

We are witnessing an unmistakable convergence of Vehicular Ad-hoc Networks (VANETs) and Intelligent Transportation Systems (ITS) that is poised to produce a revolutionary leap by making our transportation safer and the driving experience more enjoyable (Chang *et al*., 2012). In the fielded ITS infrastructure, VANETs are capable of enhancing the awareness of traffic by propagating, aggregating and disseminating newest information about existing or impending traffic events. VANETs are a type of mobile ad-hoc networks which provide communications among nearby vehicles and between vehicles and nearby fixed Road Side Units (RSU). VANETs improve road safety and offer value-added services to drives on the street. Thanks to its good features, VANETs has become one of the promising research fields in recent years (Yousefi *et al*., 2006).

VANETs present the capability of providing local information in near-real time, e.g., road closures, current traffic conditions, road conditions, etc. Such information may help vehicles to be aware of the situation ahead of them, meanwhile, those information has high utility only in a particular area and is time sensitive (Patwardhan *et al*., 2006). Therefore, it is important to be able to quickly ascertain its reliability. However, in large-scale VANETs there is no guarantee that all nodes are benign; there always are malicious nodes that relaying malicious information. In addition, since VANETs have some distinct characters, such as, fast moving, short lived connection. Hence, detecting malicious information is more challenging task (Philippe *et al*., 2004). Only when information reported by neighbor node is correct and reliable, safer driving application in VANET is guaranteed. As a result, the message from neighbor nodes should be verified before receiving node propagates the message.

The property of message is taken into account and the message is classified into safety message and unsafety message. Node in a VANET communicates with each other by safety message to enhance passenger and road safety and to effectively route traffic (Xuan and Wada, 2012). Unsafety message are generally provided by RSU and On-Board Unit (OBU) and mainly use vehicle-infrastructure (VI) communications to share traffic information and weather information (Lee *et al*., 2011).

In VANETs, a key issue that is how to deal with the message. For example, if a vehicle sends the message that there is congestion at a certain road, should other vehicles believe that this information is correct and take corresponding action (Zhen *et al*., 2012).

Newsome *et al*. (2004) address the malicious data posed by the Sybil attack (Hub and Apkun, 2004) in wireless sensor network. In their schemes, the malicious information is detected by the position

Corresponding Author: Huibin Xu, Department of Electronics and Information, Tongji University, Shanghai 200092, China

verification. The network verifies the position of each node. Identities that come from the same location are assumed to belong to one and the same participant. However, this approach is not developed to VANETs due to the mobility of nodes. Assumption that nodes are static is not reasonable.

Philippe *et al*. (2004) study detecting the malicious data and propose a general approach to evaluating the validity of VANETs data. In their approach, a node searches for possible explanations for the data it has collected. Explanations are scored when data is consistent with the node's model of the VANET. The highest scoring explanations of the data are accepted. However, the proposed approach is based on assumption that each node maintains a model of the VANETs, which contain all the knowledge that the node has of the VANETs.

Raya *et al*. (2007) proposed a scheme to detect and revoke malicious vehicles. In their schemes, each vehicle has a pseudonym and there is one corresponding public, private key pair and a certificate issued by the CA. When one vehicle is deem to malicious vehicle, its certificates are revoked. Their scheme is comprise of RTC (Revocation of Trusted Component), MDS (Misbehavior Detection System) and LEAVE (Local Revocation Protocol by Voting Evaluators). MDS and LEAVE must are an honest majority. The scheme has limitations. If there are more malicious vehicles than benign vehicles, the system performance slides down.

Ghosh *et al*. (2010) proposed a scheme by comparing the expected and actual trajectory to decide if a vehicle is sending the correct Post Crash Notification (PCN) alert. The expected trajectory has been modeled using node's possible behavior. For example, a lazy node might not take any action until it is very close to the site of crash. On the other hand a risk-averse node might move away very far from the site of crash. There are three aspects to be noted: the modeling of expected trajectory, the reported position of the node and the actual position of the node. However, the scheme is based on the assumption that a vehicle always sends valid location information. It is unreasonable since that the vehicles might send wrong location information and compel other vehicles to believe that their trajectory is what is expected. Even a small change in position can make a huge difference, for example lane change.

In this study, we evaluate the consistency between action and words (safety message) of sending vehicles to verify the trustworthiness of message reported by neighbour vehicles.

DESCRIPTION SCHEMES

In this study, the message from neighbour nodes is classified into safety message and unsafety message. Safety message is sharing to enhance passenger and road safety and to effectively route traffic. Unsafety message is about traffic information and weather information, etc. When a node receives a message, the message should be verified before it is relayed. If the content of the message is concerning safety issue, the trustworthiness of the message is evaluated. For unsafety message, the trustworthiness is based on the node-trust value. In this section, we discuss how to evaluate the trustworthiness of data from safety message.

In most situations, nodes pursue self-interests to send wrong information, e.g., for gaining access to a particular lane. Nodes might report false information on congestion, accident or road block. Nodes not have intentions of causing accidents and they only pursue convenient. Without loss of generality, we assume that nodes send false message because of self-interests in this study. Inspired by Ruj and Marcos (2011), the safety messages are classified three classes, which is as follow?

- **Emergency Electronic Brake lights (EEBL):** A vehicle is decelerating rapidly and rear vehicles should capture this information to prevent rear-end collisions;
- **Post Crash Notification (PCN):** A vehicle warns other vehicles on the road that an accident has already occurred. Vehicles should change lane or stop;
- **Post Decrease Speed Notification (PDSN):** Warning that a vehicle should slow down for some situations, such as, road conditions like "ice" or unwanted debris on the road; near schools and hospitals.

MESSAGE FORMAT

In VANETs, a node can transmit several types of messages. We deal only with two types: safety message and beacon message.

A safety message, denoted by $M_s$is seven elements:

$$M_s = \left(p_{it}, K, L_j, t, C_{it}, T_f, v_{it}\right) \quad (1)$$

where,

p_{it} = The pseudonym of the vehicle v_i which generated the safety message at time *t*. Each vehicle is access to CA and pseudonyms is pre-downloaded and stored

K = The type of safety message, which can be one of the safety messages discussed above

L_j = The location of the event E_j for which the safety message was emerged

t = The time at which the safety message had been transmit

C_{it} = The location of the vehicle v_i which observed and emerged the safety message at time t
T_f = Period of freshness which a threshold time after T_f a message becomes stale
T_f = Specified in accordance with the type of safety message
v_{it} = The speed of vehicle v_i at time t

A vehicle (e.g., v_k) receives a safety message from a neighbour vehicle (e.g., v_h) at the time t_1 and makes the decision whether relay the safety message generated at time t_0. If $t_1 - t_0 > T_f$, then it means that v_h had sent the safety message long back and has become stale. Therefore, v_k discards the safety message. If the safety message is fresh, then the action of v_h after it send the safety message is observed. If the action conflicts with message, v_k takes no action and discards the message. The v_h is considered as misbehaving vehicle. We establish the incentive system of reward and punishment. These misbehaving vehicles like v_h are recognized as malicious vehicle. Once it is malicious vehicle, it is revoked in whole network and no vehicle accepts its message.
A beacon message is denoted by M_b:

$$M_b = (p_{it}, t, c_{it}, v_{it}) \quad (2)$$

where,
p_{it} = The pseudonym of the vehicle
t = The time at which the beacon was sent
c_{it} = The location of the vehicle
v_{it} = The speed of vehicle v_i at time t

HOW TO DETECT THE INCONSISTENCE

According to the assume that most misbehaving vehicles arise out of selfish reasons, we evaluate the consistency between the actions and the words (safety message). For three kind's specific safety message, corresponding action is definite. In addition, for the sake of security, we use safety precautions in our scheme. Once receiving a safety message, vehicles go slow and detect the consistency. That is, vehicles trust the safety message before there is not sufficient evidence that the message is inauthentic.

For PCN, consider the scenarios depicted in Fig. 1: the vehicle v_1 generated a safety message M_s about accident in the front. Its neighbour vehicle v_2 and v_3 received the message M_s. If the reported accident is verified. v_1 should slow down and change lane. So v_2 and v_3 observed the action of v_1. If v_1 keeps on walking without decelerating, the message M_s from v_1 is unreal. How to observe the action and detect the inconsistency. We make use of the beacon message. After receiving a safety message M_s, v_2 and v_3 wait for beacon message from v_1 .they slow down as they wait. For a time period of Δt, v_2 and v_3 received the beacon message. They

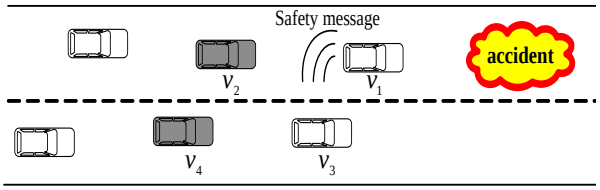

Fig. 1: PCN

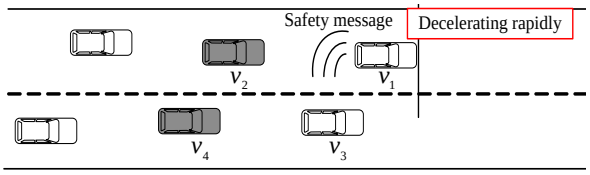

Fig. 2: EEBL

check the location C_{it} in the safety message and the location $C_{it1}(t_1 = t + \Delta t)$ in the beacon message and computer the difference between v_{it} in the safety message and v_{it1} in the beacon message. If, $v_{it1} - v_{it} \geq 0$ the vehicle v_1 was not slowing down, which indicate that v_1 past through accident location without decelerating? If $v_{it1} - v_{it} \leq 0$, we computer the acceleration $\alpha(\alpha < 0)$:

$$\alpha = \frac{v_{it1} - v_{it}}{\Delta t} \quad (3)$$

We define the acceleration threshold α_{th}, if equal (3) hold:

$$|\alpha| < \alpha_{th} \quad (4)$$

Vehicle v_1 is not enough to slow down. Therefore, if $v_{it1} - v_{it} \leq 0$ or $|\alpha| < \alpha_{th}$ holds, the safety message reported by v_1 is untrust. v_1 is recognized as misbehaving vehicle.

For EEBL, consider the scenarios depicted in Fig. 2: vehicle v_1 generated a safety message M_s which warn other vehicles about decelerating rapidly in the front. Similarly, v_2 and v_3 receive it and slow down, while check the consistency between action and words by analyzing the data from safety message and beacon message. For EEBL, if v_1 actually is not decelerating rapidly, namely, the safety message is untrue, v_1 must speed off and do not slow down, otherwise, rear vehicle (e.g., v_2) may rear-ended, which bring harm to v_1. So, compared with PCN, detecting the misbehaving vehicle is easy in scenarios for EEBL.

For PDSN, consider the scenarios depicted in Fig. 3. This kind safety message alert rear vehicle of going slow because of school or hospital in the front. After receiving the message, rear vehicles slow down and verify the trustworthiness of message by the method above.

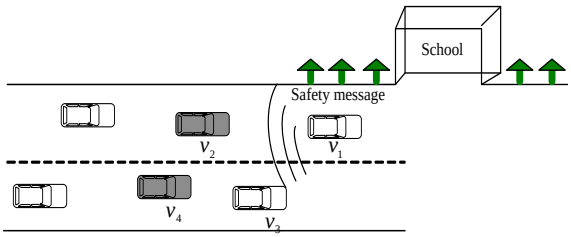

Fig. 3: PDSN

Table 1: Varying simulation parameters

Test no	Malicious vehicles	Maximum speed, m/s	α_{th}, m/s^2	δ_{th}, m
1	3	0~30	7.5	4
2	0-4	20	7.5	4

During the course of analysis above, we assumed that position and speed information send in the safety and beacon message is correct. However, a smart malicious vehicle will also send incorrect position and speed information, along with the inauthentic safety message. Therefore, how to detect incorrect position and speed information is key. For incorrect position information, we can use position verification by RSSI (Xue and Liu, 2011) (received signal strength indicator) method. Moreover, we verify the restricted relationship of distance, speed and time. Based on the data from message, at time t, the location and speed of vehicle v_i is c_{it} and v_{it}, respectively. At time t_1, the location and speed of vehicle v_i is c_{it1} and v_{it1}, respectively. Let $\Delta t = t_1 - t$. s = c_{it1}. s = c_{it1} - c_{it}. Motion of vehicle is deemed to uniformly accelerated motion during Δt, as the time interval is very short. Let the acceleration $\alpha_i = v_{it1} - v_{it}$ /Δt. On the basis of the knowledge in physics, $s = v_{it}\ \Delta t + 1/2\alpha_i \Delta t^2$. Due to the influence of test's error, s and $v_{it}\ \Delta t + 1/2\ \alpha_i\ \Delta\ t^2$ did not share equally. So, let:

$$\delta = s - (v_{it}\Delta t + \frac{1}{2}a_i\Delta t^2) = (c_{it1} - c_{it}) - (v_{it}\Delta t + \frac{1}{2}a_i\Delta t^2) \quad (5)$$

We define an error threshold δ_{th}, if $\delta > \delta_{th}$, then the position and speed of information from message (safety message and beacon) is incorrect. The sending vehicle is recognized as misbehaving vehicle.

ESTABLISH OF MODEL AND SIMULATION

In our scheme, MATLAB is used in our simulation. We assume a 4 lane situation and each lane is 3.75 m wide. According to DSRC (Dedicated Short Range Communications), the transmission range of all vehicles is 300 m. The number of total vehicles and malicious vehicles is set. There are 11 vehicles in our simulation which are randomly placed in an area of 15m×500m, as shown in Fig. 4.

Table 1 shows the simulation parameters. We use Detection ratio to evaluate the performance of our scheme. Detection ratio: the ratio of the number of incorrect safety message which is identified correctly to the actual number of all safety = message in the network. Each malicious vehicle generated two incorrect safety messages and sent.

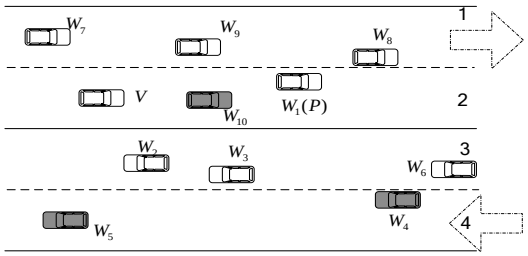

Fig. 4: Simulation model

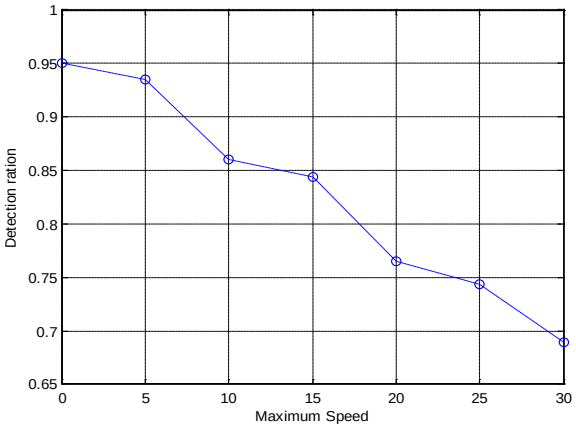

Fig. 5: Detection ratio vs maximum speed

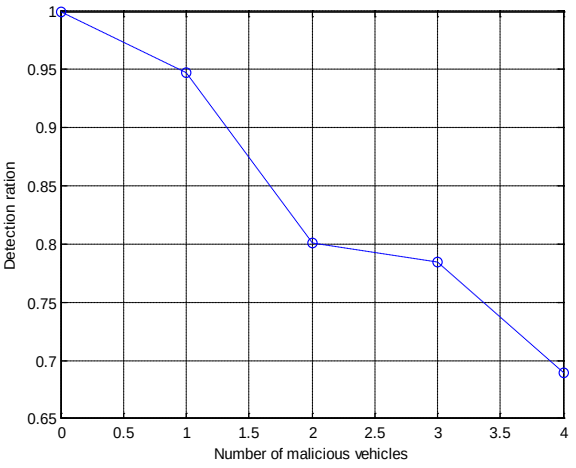

Fig. 6: Detection ratio vs number of malicious vehicles

In the first test, we evaluate the Detection ratio as the maximum speed of vehicles varies from 0 to 30 m/s. As shown in Fig. 5, the Detection ratio of our proposed scheme declines remarkably as vehicles speed up. The smaller the speed is, the time-evaluating the action of vehicles is longer. It is easy to detect the malicious vehicles.

In the second test, we evaluate the Detection ratio as the number of malicious vehicles varied from 0 to 4. As shown in Fig. 6, the Detection ratio of our proposed scheme declines remarkably as malicious vehicles increased. The greater the number of malicious vehicles, the more incorrect safety message is sent in the network. It is more difficult to detect the malicious messages.

CONCLUSION

We have proposed a novel approach to detect incorrect safety message in a VANET. The approach relies on using data from safety message and beacon message, collected by vehicles in the VANET, shared with immediate neighbors and propagated to a neighboring region. The data provides speed and location information, allowing each neighbor vehicle to process the data and detect malicious information and discard it. Vehicle checks the validity of the data from message. The location information is verified by the RSSI, the speed information is verified by the relationship between location and speed. Moreover, the consistence between the action and words is evaluated. If inconsistencies arise, the vehicle is considered as malicious vehicle and the message is discarded. Simulation results show that the proposed scheme is effective and efficient to detect the incorrect safety message.

In the future, we will conduct more research on improving the performance under severe environments. We will struggle to find a algorithm that can deal with the situation with the density of malicious vehicles and the maintain the high accuracy.

ACKNOWLEDGMENT

The research described here is supported by National Natural Science Foundation of China under Grant (N0.60972036).

REFERENCES

Chang, S., Y. Qi, Z. Hongzi, Z. Jizhong and S. Xuemin, 2012. Footprint: detecting sybil attacks in urban vehicular networks. IEEE T. Parall. Distrib. Syst., 23(6): 1103-1114.

Ghosh, M., A. Varghese, A. Gupta and A.A. Kherani, 2010. Detecting misbehaviors in vanet with integrated root-cause analysis. Ad Hoc Netw., 8(7): 778-790.

Hub, A.J. and C.S. Apkun, 2004. The security and privacy of smart vehicles. IEEE Secur. Priv., 2(3): 49-52.

Lee, D.H., S.N. Bai and T.W. Kim, 2011. Enhanced selective forwarding scheme for alert message propagation in VANETs. Int. J. Autom. Technol., 12(2): 251-264.

Newsome, J., E. Shi, D. Song and A. Perrig, 2004. The sybil attack in sensor networks: Analysis and defenses. Proceeding of the 3rd International Symposium on Information Processing in Sensor Networks, 2: 259-268.

Patwardhan, A., A. Joshi, T. Finin and Y. Yesha, 2006. A data intensive reputation management scheme for vehicular ad hoc networks. Network. Serv., 32(4): 281-289.

Philippe, G., G. Dan and S. Jessica, 2004. Detecting and correcting malicious data in VANETs. Proceeding of the 1st ACM International workshop on Vehicular Ad Hoc Networks (VANET 04). ACM New York, USA, pp: 29-37.

Raya, M., P. Papadimitratos and I. Aad, 2007. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE J. Select. Areas Commun., 25(8): 1557-1568.

Ruj, S.S. and A. Marcos, 2011. On data-centric misbehavior detection in VANETs. Veh. Technol. Conf., 3(6): 1-5.

Xuan, L. and A. Wada 2012. A framework for trust and policy management for a secure internet and its proof-of-concept implementation. Proc. IEEE/IFIP Netw., 2(6): 1159-1166.

Xue, X.P. and M.Y. Liu, 2011. Time slice-based location verification for VANET. China Commun., 12(4): 23-37.

Yousefi, S., M.S. Mousavi and M. Fathy, 2006. Vehicular ad hoc networks: Challenges and perspectives. Proc. ITS Telecomm., 3(12): 761-766.

Zhen, H., S.R. Su and A. Marcos, 2012. A social network approach to trust management in VANETs. Peer-to-peer Netw. Appl., 10(8): 1-14.