6-2-2013

A Trust Model for Vehicular Network-Based Incident Reports

Cong Liao
University of Pennsylvania

Jian Chang
University of Pennsylvania, jianchan@cis.upenn.edu

Insup Lee
University of Pennsylvania, lee@cis.upenn.edu

Krishna K. Venkatasubramanian
Worcester Polytechnic Institute, kven@wpi.edu

Recommended Citation

Cong Liao, Jian Chang, Insup Lee, and Krishna K. Venkatasubramanian, "A Trust Model for Vehicular Network-Based Incident Reports", *5th IEEE International Symposium on Wireless Vehicular Communications: WiVeC 2013* , 1-5. June 2013. http://dx.doi.org/10.1109/wivec.2013.6698224

IEEE Symposium on Wireless Vehicular Communications: WiVeC, 2-3 June 2013, Dresden, Germany.

A Trust Model for Vehicular Network-Based Incident Reports

Abstract
Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) networks are ephemeral, short-duration wireless networks that have the potential to improve the overall driving experience through the exchange of information between vehicles. V2V and V2I networks operate primarily by distributing real-time incident reports regarding potential traffic problems such as traffic jams, accidents, bad roads and so on to other vehicles in their vicinity over a multi-hop network. However, given the presence of malicious entities, blindly trusting such incident reports (even the one received through a cryptographically secure channel) can lead to undesirable consequences. In this paper, we propose an approach to determine the likelihood of the accuracy of V2V incident reports based on the trustworthiness of the report originator and those vehicles that forward it. The proposed approach takes advantage of existing road-side units (RSU) based V2I communication infrastructure deployed and managed by central traffic authorities, which can be used to collect vehicle behavior information in a *crowd-sourced*fashion for constructing a more comprehensive view of vehicle trustworthiness. For validating our scheme, we implemented a V2V/V2I trust simulator by extending an existing V2V simulator with trust management capabilities. Preliminary analysis of the model shows promising results. By combining our trust modeling technique with a threshold-based decision strategy, we observed on average 85% accuracy.

Keywords
Connected Vehicles, Trust Management, Vehicular Networks

Disciplines
Computer Engineering | Computer Sciences

Comments
IEEE Symposium on Wireless Vehicular Communications: WiVeC, 2-3 June 2013, Dresden, Germany.

A Trust Model for Vehicular Network-Based Incident Reports

Cong Liao, Jian Chang, and Insup Lee
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA, 19104
Email: {liaocong, jianchan, lee}@cis.upenn.edu

Krishna K. Venkatasubramanian
Department of Computer Science
Worcester Polytechnic Institute
Worcester, MA, 01609
Email: kven@wpi.edu

***Abstract*—Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) networks are ephemeral, short-duration wireless networks that have the potential to improve the overall driving experience through the exchange of information between vehicles. V2V and V2I networks operate primarily by distributing real-time incident reports regarding potential traffic problems such as traffic jams, accidents, bad roads and so on to other vehicles in their vicinity over a multi-hop network. However, given the presence of malicious entities, blindly trusting such incident reports (even the one received through a cryptographically secure channel) can lead to undesirable consequences. In this paper, we propose an approach to determine the likelihood of the accuracy of V2V incident reports based on the trustworthiness of the report originator and those vehicles that forward it. The proposed approach takes advantage of existing road-side units (RSU) based V2I communication infrastructure deployed and managed by central traffic authorities, which can be used to collect vehicle behavior information in a *crowd-sourced* fashion for constructing a more comprehensive view of vehicle trustworthiness. For validating our scheme, we implemented a V2V/V2I trust simulator by extending an existing V2V simulator with trust management capabilities. Preliminary analysis of the model shows promising results. By combining our trust modeling technique with a threshold-based decision strategy, we observed on average 85% accuracy.**

***Index Terms*—Connected Vehicles, Trust Management, Vehicular Networks**

I. Introduction

With the rapid development of wireless communication technologies, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) networks are increasingly becoming commonplace. Such networks possess an enormous potential in improving driving safety and traffic conditions by sharing road and traffic information, called *incident reports*, among vehicles in real-time. The collaboration fostered by V2V communication enables individual vehicles to be more effective in handling accidents and traffic congestions than they could by themselves. However, the benefits of this V2V setup cannot be fully realized unless one can effectively defend against malicious or dysfunctional nodes (*i.e.,* vehicles), which will be inevitably present in its open environment. Such nodes, collectively termed as *attackers*, may introduce fake or erroneous information within the network that selectively benefit themselves, cause nuisance, and even harm others. Ensuring information trustworthiness is therefore essential in V2V and V2I networks.

The authors acknowledge the support of the US Department of Transportation under the University Transportation Center program.

In the paper, we explore an approach that facilitates more reliable and effective trust decisions of the incident repots received over V2V networks. This is done based on global trust information aggregated by a central authority through the road-side units based V2I infrastructure. Upon observing an incident, a vehicle broadcasts a V2V message with an incident report (*e.g.,* accident, traffic congestion, broken bridge) to other vehicles within its communication range. Each vehicle receiving the incident report is then required to execute three tasks: (1) whether to accept the received incident report, based on its likelihood of being accurate; (2) if accepted, compute an endorsement opinion, which signifies the level of endorsement, on the incident report message; and (3) attach the computed endorsement to the incident report and forward it down-stream. With the proposed approach, these two decisions are made based the trust score of the report originator and forwarders. The trust score is computed by a central authority by aggregating vehicle behavior history w.r.t. incident report accuracy. To facilitate the trust score computation, received incident reports are voluntarily provided to the central authority over the V2I channel in a *crowd-sourced* fashion by the vehicles in the system. We rely on the crowd-sourced model as it has provided highly effective traffic related information as demonstrated by real-world services such as Google Maps.

We validated our proposed model using simulation. There is a considerable dearth of available platforms to validate trust management solutions for vehicular networks. Consequently, we implement a *V2V/V2I trust simulator* by significantly extending the GrooveNet simulation platform [1] with trust management modules. The idea was not only to validate our current approach, but also provide a flexible platform for researchers to test and compare different trust modeling techniques. Initial simulation results of our approach based a Bayesian trust computation function have yielded encouraging results. We have observed clear separation in the trust score obtained for different vehicle behavior pattern. And by combining our trust modeling technique with a threshold-based decision strategy, we obtain on average 85% accuracy in determining its accuracy.

The *contributions* of this work are two-fold: (1) a new trust model for vehicular networks leveraging the increasing presence of V2I channels and crowd-sourcing capabilities, and (2) an V2V/V2I trust simulator for validating the trust management proposals for vehicular networks. The rest of the paper is organized as follows: Section II presents the related work. Section III presents the problem statement followed by Section

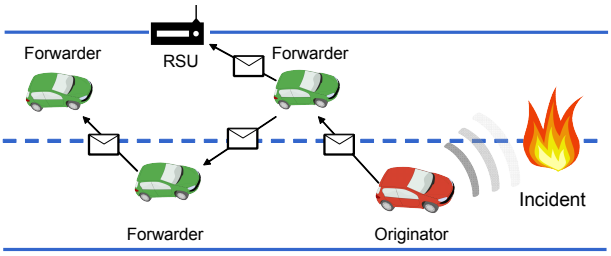

Fig. 1. Example Scenario of V2V-based Incident Report

IV the trust model. Section V presents our new V2V/V2I trust simulator. Section VI presents some preliminary results. In Section VII, we conclude the paper.

II. Related Work

Trust Management is a very broad field of research. An overview of general trust management approaches can be found in [2], [3]. It is important to note that for different application domains, trust management approaches are often highly customized to address application-specific requirements or constraints. As observed in [4], only a few approaches have been proposed in the literature to address trust issues in vehicular networks. Some of the prominent approaches for V2V trust are [5], [6], [7], which focus on using local information available from the vehicles in the vicinity and simple consensus schemes to decide whether to trust received messages over the V2V network. We believe this provides an inherently myopic world-view and therefore is ill-suited for making good trust decisions. With the proliferation of road-side unit (RSU) based V2I channels and the increasing crowd-sourcing capabilities, it is possible to collect and manage a more comprehensive and global view of vehicle behavior, which existing solutions fail to consider. Finally, though much work has been done in trust modeling, little work has been done in providing a platform for testing the strategies developed in this regard. To the best of our knowledge we are the first to provide a trust simulator platform for vehicular networks that can be very useful for validating various trust modeling techniques and trust decision making strategies.

III. System Model and Problem Statement

In this paper, we focus on a typical application scenario of a V2V network – propagation of real-time *incident report*. In this scenario, an incident can randomly occur at any place and time, which can have negative impacts on the traffic within a designated area around the incident site. Examples of incident include car accidents, bad road or weather conditions, *etc.*. In order to enhance road safety, incident information sharing through V2V and/or V2I network in real-time can be very useful to ensure timely management of traffic and to mitigate other undesirable externalities.

An simple scenario of the incident report generation and usage is illustrate in Figure 1. A vehicle driving on the road detects the occurrence of one or more incidents and automatically generates and forwards an incident report to other vehicles within its V2V communication range. The incident report message contains the description of the incident (*e.g.,* time, location, severity level, *etc.*) to informs other vehicles. In this paper, we call the vehicle, which serves as the original source of incident report messages, the *originator*. Upon receiving an incident report message, the receiving vehicle can make driving decisions based on it. Further, it may choose to forward this message to neighboring vehicles within its communication range to further propagate the information. We call all the vehicles on the message propagation path except the originator, the *receivers*. And we call all intermediate vehicles on the message propagation path, the *forwarders*. Many communication protocols have been proposed in the literature to facilitate the routing of such incident reports and other messages over V2V networks [8], [9], [10]. Besides V2V communications, RSUs and other infrastructure facilities may also participate in this process to either relay the message further when the vehicle density is low [11], or play an important role in crypto-key distribution process for secure the V2V communication [12]. However, none of these schemes focus on providing mechanism to ensure the accuracy of the incident report itself. The accuracy of the incident report is crucial to ensure the effectiveness of such real-time information sharing capability. It is easy to imagine an attack scenario, where malicious entities introduce false or misleading incident information causing adverse traffic conditions. The problem being studied in this paper is "how can one evaluate the accuracy of the traffic incident information shared by individual vehicles within a V2V network?"

IV. Trust Model

The key idea proposed in this paper is to construct a trust model for each vehicle participating (*i.e.,* originating and forwarding) the V2V-based incident report propagation. This trust model is designed to compute a *trust score* that represents the likelihood that a vehicle originates or forwards accurate incident reports to other vehicles. In this section, we provide an overview of the main elements of this trust model including our assumptions about the overall system, behavior exhibited by the vehicles and the trust modeling process. Please note that, in this work, we assume that all messages exchanged over the V2V and V2I network are cryptographically protected. The focus of this work is therefore solely on computing effective trust score for the vehicles.

A. Vehicle Behavior Collection & System Assumptions

Due to the ephemeral nature of V2V networks, no individual vehicle can have a sufficient view of other vehicle's incident report behavior to effectively reason about trustworthiness. However, if one can design an effective mechanism to collect observation and experiences about individual vehicles, it would greatly facilitate the process of aggregating partial and incomplete information into meaningful global picture. Based on the observation above, we assume a *vehicle behavior information collection infrastructure* (VBII) by taking advantage of existing V2I communication channels. With such an infrastructure, local RSUs can be used by vehicles to provide a central authority (*e.g.,* regional traffic management centers) with the incident reports its received from other vehicles. The central authority can correlate such vehicle behavior with its own database of traffic incidents with the benefit of hindsight to reason about a vehicle's trustworthiness.

Upon receiving an incident report, a vehicle can use the trust score of the originator and the forwarders obtained from

the central authority for making its decisions regarding: (1) whether to accept the received incident report, based on its likelihood of being accurate; and (2) if accepted, to compute an endorsement opinion on the incident report message before forwarding it down-stream. To ensure the viability of the proposed scheme, we make three assumptions.

First, although the central authority cannot know about the occurrence of traffic incidents in real-time, it will know the *ground truth* information of an incident after a certain period of delay T_{delay}. This assumption is very reasonable and realistic since in the event of traffic incidents, the local traffic management center is informed of such an occurrence, and an official record on the incident is maintained. In the future, we would like to incorporate other reliable ground truth sources. For instance, by combining the usage of loop detectors and traffic cameras, regional traffic management authority can achieve near real-time detection of incidents.

Second, vehicles will report back the behavior of other vehicles they observe (*i.e.,* the incident reports they receive and the endorsement opinions expressed by the originator and various forwarders) to the central authority. This crowd-sourcing of traffic information is relatively common, and it has already been used by services such as Google Maps. We therefore assume that the percentage of vehicles providing such feedback will be relatively high. Please note that in our scenario the incident detection is an *automatic and mandatory* process. The reporting of the incident reports (also called feedback) to the central authority is voluntary.

Last but not the least, we assume the existence of an unique identifier system for vehicles. Concretely, it can be in form of an e-license, which also embeds other vehicle information (*e.g.,* vehicle purpose, owner, *etc.*). Several proposals on implementing such ID systems has been available, and some states in US have already made some initial progress.

To facilitate this vehicle behavior collection process, we requires that all incident reports carry the IDs of the originator and the forwarders. Additionally, the incident report has an opinion field that stores one's endorsement of the report accuracy. The value range of the opinion is $(0, 1)$, where 1 (or 0) indicates the *max* (or *min*) belief of the incident report message. When a vehicle is within the communication range of a RSU, it can voluntarily report back to the central authority about the incident messages it has originated or received, using the V2I communication channel. To ensure authenticity, integrity, and accountability of the vehicle behavior tracking process, one can use the Public Key Infrastructure (PKI) as part of the vehicle ID system that covers all the participant vehicles managed by the central authority.

B. Trust Modeling & Trust-based Decision Making

The central authority computes the trustworthiness of the vehicles based on the vehicle behavior information it receives and the ground truth of incident is revealed as time evolves. The trust score T has two representations in our system: a vector representation and a scalar representation, similar to the proposal in [13]. The vector representation of T is a triple (t, c, f). The value t is the measured trust computed based on the vehicle behavior history of providing accurate incident reports. The value f is the default trust obtained using static information about the vehicle such as vehicle type (*e.g.,*

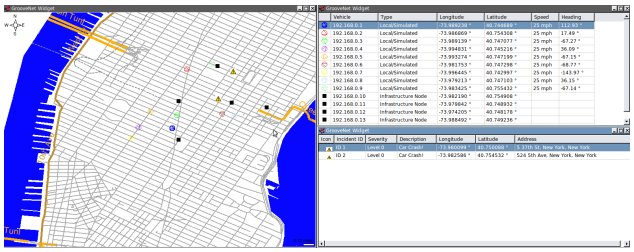

Fig. 2. Screen-shot of the V2V/V2I Trust Simulator

ambulance, police car), vehicle ownership history (*e.g.,* Carfax report). It is easy for the central authority to obtain these static information about individual vehicles, and the default trust can be used in lieu of measured trust, when little vehicle behavior information is available. The default trust f can also be used as an effective mechanism to encode existing trust schemes, such as role-based trust management [14]. For instance, known types of trustworthy vehicles like police vehicles, can be given full trust by default, which is very useful for trust bootstrapping. We can convert the vector presentation of T into its scalar representation using the following equation:

$$T_{scalar} = t * c + (1 - c) * f$$

Where the value c is a weight factor to determine how much measured trust and default trust contributes in the scalar representation. It is our plan to evaluate various approaches to compute the measured trust as a part of this work. As an initial step, we have designed a trust model based on Bayesian statistics. Essentially, the Bayesian trust model computes an probability estimation t by assuming the vehicle behavior can be modeled as an independent and identically distributed random variable. At any given time, for all the incidents with known ground truth, the trust value t of a vehicle v is computed by the following equation:

$$t = \frac{\sum O_c^v}{\sum O_c^v + \sum O_i^v}$$

Here, $\sum O_c^v$ is the sum of endorsement opinions expressed by vehicle v on incident reports that *correctly* match with the ground truth of incident (*i.e.,* the occurrence of the reported incidents is known to be truthful). Similarly, $\sum O_i^v$ is the sum of endorsement opinions expressed by vehicle v on incident reports that *mismatch* with the ground truth of incident. Despite the simplicity, our preliminary evaluation shows very promising results of its effectiveness, as shown in Section VI.

The vehicle trust score is periodically updated by the central authority and distributed to vehicles in the scalar form using V2I channels through RSUs. When a vehicle is within the communication range of certain RSU, it can actively query the central authority to obtain the most updated trust score of all the vehicles observed by the authority. The obtained trust score can be used by vehicles for making more informed trust decisions. In this regard, a simple strategy is to compare the trust score of the originator of a received incident report to a predefined trust threshold $t_{threshold}$. We have evaluated this trust decision strategy in Section VI. It is our plan to design and exercise more sophisticated strategies in future research.

V. V2V/V2I Trust Simulator

Seeing the dearth of platforms available for simulating trust in V2V networks, we decided to build a V2V/V2I trust simulator. In this regard, we considerably extended an open-source hybrid-network simulator called GrooveNet [1] with trust modeling capabilities. The screen-shot of our simulation system is shown in 2. In the simulator *Vehicle* is the principal entity in the simulator (shown as color circles in Figure 2). All properties of the vehicle including its start-point, movement and communication capabilities are managed by the underlying GrooveNet simulator. This section provides a overview of the principal extensions that we have made to GrooveNet as part of implementing the trust simulator.

Simulation Manager: The entire simulation process is controlled by a simulation manager, which is in charge of the creating, loading, saving and running simulations. All the entities used in the simulation (*e.g.,* vehicles, infrastructures, incidents, trust models) can be configured through an XML simulation configuration file. The design of a simulation manager and an XML configuration file allows the repeatability of experiments – one of the primary requirements of a simulator. One can easily replay the same scenario setup for many different trust modeling techniques in order to perform comparison studies.

Vehicle Roles: In GrooveNet each vehicle in the system is identified with an unique IP address. However, as part of the trust simulator we add the notion of *roles* to the vehicles to encode different behavior patterns of incident detection, incident reporting and message forwarding. By default, vehicles in our simulator can have one of three built-in roles:

1) *Authority:* An authority vehicle detects and honestly reports incidents as it patrols the map randomly. It only forwards the incident report message from other authority vehicles.
2) *Normal:* A normal vehicle acts properly by following the traffic rules. It selectively forwards messages believed to be accurate, and drops the ones it deems inaccurate. It also actively reports all incident messages it has received back to RSUs.
3) *Attacker:* An attacker maliciously affects the vehicular networks by means of intentionally reporting fake incidents and suppressing the propagation of the accurate messages it receives. And it never reports back to RSUs.

Please note that, this is not an exhaustive set of roles that the vehicles can exist in our system. Other roles can be added or existing ones modified easily to enable the simulation of more diverse vehicle behaviors.

Incident Model & Incident Detection: In our system, incidents reports are generated as a result of incident detection. We added the notion of incident to GrooveNet (shown as yellow warning signs in Figure 2), which is described with attributes such as start time, duration, geographic location, severity, *etc.* in the XML simulation configuration file. In real-world scenario, incident detection is primarily done using driver input and/or various types of sensors such as RADARs, LIDARs, and cameras embedded in vehicles [15], [16]. For simplicity, our simulator abstracted this out and defined a configurable parameter called *detection diameter* for each vehicle. The detection diameter is the geographical distance between the location of the incident and current position of the vehicle along its moving direction. An incident will be detected if it is in the range of the vehicle's detection diameter along its direction. This allows to cater for vehicle having different sensing systems and therefore different detection capabilities.

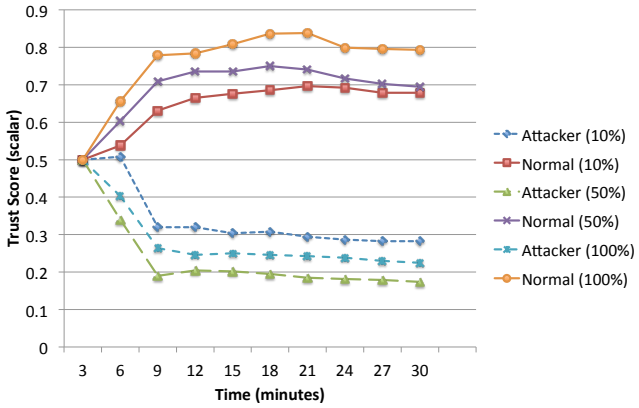

Fig. 3. Average Trust Score trend for vehicles with attackers and normal role at various percentages of incident report feedback

Infrastructure Model & Trust Modeling Module The RSU model (shown as black squares in Figure 2) is part of the VBII and has similar communication capacity as the vehicle model. However, it does not have the mobility model since all RSUs are stationary at fixed locations. Although RSUs will not join the process of incident report propagation, it is capable of collecting vehicle behavior information and sending trust scores back to vehicles. In our simulator we also have the notion of a configurable time delay T_{delay}, infrastructures will know the ground truth of the reported incidents, which can be used for computing the measured trust t of vehicles. The default trust computation module used by the simulator is the one described in Section IV. This module can be easily replaced with other trust modeling techniques as needed.

VI. Preliminary Evaluation

In order to validate our approach setup, we set up a simulation scenario with 70 vehicles in total using the map of New York city. We have 50 vehicles with normal role type, 10 vehicles with attacker role, and 10 with authority role. For attacker vehicles, the frequency of sending incorrect incident reports was set to 30 seconds/message. Normal vehicles only accepted and forward a received incident report if the trust-score of the originator is greater at least 0.7 (*i.e.,* $t_{threshold} = 0.7$). Further, any incident report forwarded by a user has an endorsement opinion associated with it, which is computed as $AVG_{t_{max}} * t_{max}$. Here, $AVG_{t_{max}}$ is the average endorsement opinion expressed by vehicles with the highest trust score (t_{max}) among the originator and forwarders of the incident report. Authority vehicles are always assigned with the highest trust score set to 1 by the central authority. Further, they only accept and forward messages from other authority vehicles with an endorsement opinion of 1.

Our simulation introduced 20 incidents with average duration 20 minutes over the map with random starting time. We assume the ground truth of the incidents are known after a five-minute delay (*i.e.,* $T_{delay} = 5\ mins$). The start location of vehicles, the location of RSUs and incident occurrence are evenly distributed over the map area. Figure 3 shows the trend

of average trust score of vehicles with normal and attacker role types under different levels of crowd-sourced indent feedback ratio. Both the attackers and the normal vehicles begin with a trust score of 0.5. As we can see, after an initial "bootstrapping" time (approximate equal to T_{delay}), the trust score of the two role types evolve in two different directions. After around 15 minutes, the trust value begin to settle, and we can see the clear separation between the two curves, respective of different feedback ratio. When the feedback ratio is low, it takes longer for the system to separate the attacker form the normal. Also, the separation margin is narrower.

Additionally, we have also measured the accuracy of trust decisions. For normal vehicles, a simple threshold-based decision strategy is able to achieve around 85% of decision accuracy with 4% average false positive rate (*i.e.,* trust incorrect incident reports) and 21% average false negative rate (distrust correct incident reports). The root cause for the false positive is due to the mixed behavior patterns of attackers – before the trust score converges within a stable range, some attackers can have relatively high trust values temporarily. The root cause for the false negative is due to two main reasons : (1) the low trust scores of attackers lead to other vehicles to distrust even the correct incident reports originated by them; and (2) during the trust bootstrapping stage, normal vehicles are assigned with the default trust value (*i.e.,* 0.5), which is lower than the trust decision threshold. However, we can see that both the trust bootstrapping and temporary trust value fluctuation is short-lived in our experiment (*i.e.,* around 15 minutes), and we can achieve 1% false positive rate and 9.6% false negative rate, when the trust value converges.

These results demonstrate our approach which relies on a more centralized, crowd-sourced vehicle behavior monitoring is clearly promising. These are only preliminary results, a more thorough analysis of the approach by varying the number of vehicles, attackers and attacker behaviors is being performed. An interesting analysis in this regard would be the communication and storage overhead for setups with large amount of vehicles and frequent interactions. We also plan to explore different trust modeling techniques and trust decision strategies using our setup and also perform a more detailed comparison with the existing trust modeling approaches.

VII. Conclusion

In this paper, we proposed an trust-based approach to determine the likelihood of information accuracy under V2V-based incident report setting. By taking advantage of V2I channels between vehicles and central traffic authorities, we can construct a global view of individual vehicles trustworthiness in a crowd-sourced fashion, which overcomes the lack of vehicle behavior information due to the inherent ephemeral nature of vehicular networks. We also significantly extended an existing simulation platform with trust modeling capabilities to validate our approach. Our preliminary evaluation shows promising result on the effectiveness of the proposed approach. In the future, there are three directions that we would like to explore: (1) we plan on using our new simulator for a more thorough analysis of the proposed approach and compare the proposed approach with existing trust management proposals for vehicular networks; (2) we would like to improve of the communication overhead, the impact of unreliable communication channel, and the cost of infrastructure deployment; (3) we would like to further study the trade-off of security and privacy issues introduced by using unique identifiers and PKIs.

References

[1] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai, "Groovenet: A hybrid simulator for vehicle-to-vehicle networks," in *Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference on*, july 2006, pp. 1 –8.

[2] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Proceedings of the Third international conference on Trust Management*, ser. iTrust'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 77–92.

[3] P. Zhang, A. Durresi, and L. Barolli, "Survey of trust management on various networks," in *Proceedings of the 2011 International Conference on Complex, Intelligent, and Software Intensive Systems*, ser. CISIS '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 219–226. [Online]. Available: http://dx.doi.org/10.1109/CISIS.2011.122

[4] J. Zhang, "A survey on trust management for vanets," in *Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications*, ser. AINA '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 105–112. [Online]. Available: http://dx.doi.org/10.1109/AINA.2011.86

[5] M. Gerlach, "Trust for vehicular applications," in *Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems*, ser. ISADS '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 295–304. [Online]. Available: http://dx.doi.org/10.1109/ISADS.2007.76

[6] Z. Huang, S. Ruj, M. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in vanets," *Peer-to-Peer Networking and Applications*, pp. 1–14, 2012. [Online]. Available: http://dx.doi.org/10.1007/s12083-012-0136-8

[7] M. Raya, P. Papadimitratos, V. D. Gligor, and J. pierre Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE CONFERENCE ON COMPUTER COMMUNICATIONS*, 2008, pp. 1238–1246.

[8] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *Comm. Mag.*, vol. 44, no. 1, pp. 74–82, Jan. 2006. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2006.1580935

[9] F. Yu and S. Biswas, "Self-configuring tdma protocols for enhancing vehicle safety with dsrc based vehicle-to-vehicle communications," *IEEE J.Sel. A. Commun.*, vol. 25, no. 8, pp. 1526–1537, Oct. 2007. [Online]. Available: http://dx.doi.org/10.1109/JSAC.2007.071004

[10] K. Naito, K. Sato, K. Mori, and H. Kobayashi, "Proposal of distribution scheme for vehicle information in its networks," in *Proceedings of the 2009 Eighth International Conference on Networks*, ser. ICN '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 427–433. [Online]. Available: http://dx.doi.org/10.1109/ICN.2009.30

[11] T. Sukuvaara, P. Nurmi, M. Hippi, R. Autio, D. Stepanova, P. Eloranta, L. Riihentupa, and K. Kauvo, "Wireless traffic safety network for incident and weather information," in *Proceedings of the first ACM international symposium on Design and analysis of intelligent vehicular networks and applications*, ser. DIVANet '11. New York, NY, USA: ACM, 2011, pp. 9–14. [Online]. Available: http://doi.acm.org/10.1145/2069000.2069003

[12] C.-H. Yeh, Y.-M. Huang, T.-I. Wang, and H.-H. Chen, "Descv–a secure wireless communication scheme for vehicle ad hoc networking," *Mob. Netw. Appl.*, vol. 14, no. 5, pp. 611–624, Oct. 2009. [Online]. Available: http://dx.doi.org/10.1007/s11036-008-0138-1

[13] S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan, "Certainlogic: A logic for modeling trust and uncertainty (short paper)," in *In Proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST 2011)*. Springer, Jun 2011.

[14] M. Reith, J. Niu, and W. H. Winsborough, "Role-based trust management security policy analysis and correction environment (rt-space)," in *Companion of the 30th international conference on Software engineering*, ser. ICSE Companion '08. New York, NY, USA: ACM, 2008, pp. 929–930. [Online]. Available: http://doi.acm.org/10.1145/1370175.1370192

[15] B.-F. Wu, C.-C. Kao, C.-C. Liu, C.-J. Fan, and C.-J. Chen, "The vision-based vehicle detection and incident detection system in hsueh-shan tunnel," in *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on*, 30 2008-july 2 2008, pp. 1394 –1399.

[16] L. Yu, L. Yu, J. Wang, Y. Qi, and H. Wen, "Back-propagation neural network for traffic incident detection based on fusion of loop detector and probe vehicle data," in *Natural Computation, 2008. ICNC '08. Fourth International Conference on*, vol. 3, oct. 2008, pp. 116 –120.