A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks

Jie Zhang[†] Chen Chen Robin Cohen
[†]*School of Computer Engineering, Nanyang Technological University, Singapore*
David R. Cheriton School of Computer Science, University of Waterloo, Canada
[†]*zhangj@ntu.edu.sg*

Abstract

In this paper, we present a trust-based framework for message propagation and evaluation in vehicular ad-hoc networks where peers share information regarding road condition or safety and others provide opinions about whether the information can be trusted. More specifically, our trust-based message propagation model collects and propagates peers' opinions in an efficient, secure and scalable way by dynamically controlling information dissemination. The trust-based message evaluation model allows peers to evaluate the information in a distributed and collaborative fashion by taking into account others' opinions. Experimental results demonstrate that our proposed framework promotes network scalability and system effectiveness in information evaluation under the pervasive presence of false information, which are the two essentially important factors for the popularization of vehicular networks.

1 Introduction

With the advance and wide deployment of wireless communication technologies, vehicle manufactures and research academia are heavily engaged in the blueprint of future vehicular ad-hoc networks (VANETs). Peers (vehicles) in a VANET communicate with each other by sharing road condition and safety information, to enhance passenger and road safety and to effectively route traffic through dense urban areas. Tremendous effort has been spent on the development of life-critical or road condition related systems, such as traffic view systems [12], safety message sharing [16], cooperative collision avoidance [4], and secure crash reporting [13]. These systems focus mainly on ensuring a reliable delivery of messages among peers. As a result, less focus has been placed on evaluating the quality of information that is sent by peers, in order to cope with reports from malicious peers which may compromise the network, without the assumption of a pervasively available infrastructure such as an online central authority or road side units. In addition, little concern has been focused on the design of a control mechanism where upon detection of false information, it should be immediately controlled to minimize its further negative effect on other peers in the network.

In this paper, we propose a trust-based message propagation and evaluation framework to support the effective evaluation of information sent by peers and the immediate control of false information in a VANET. More specifically, our trust-based message propagation collects peers' trust opinions about a message sent by a peer (message sender) during the propagation of the message. We improve on an existing cluster-based data routing mechanism by employing a secure and efficient identity-based aggregation scheme for the aggregation and propagation of the sender's message and the trust opinions. These trust opinions weighted by the trustworthiness of the peers modeled using a combination of role-based and experience-based trust metrics are used by cluster leaders to compute a majority opinion about the sender's message, in order to proactively detect false information. Malicious messages are dropped and controlled to a local minimum without further affecting other peers. Our trust-based message evaluation allows each peer to evaluate the trustworthiness of the message by also taking into account other peers'

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 4, pp. 3-15

trust opinions about the message and the peer-to-peer trust of these peers. The result of the evaluation derives an effective action decision for the peer.

We evaluate our framework in simulations of real life traffic scenarios by employing real maps with vehicle entities following traffic rules and road limits. Some entities involved in the simulations are possibly malicious and may send false information to mislead others or spread spam messages to jam the network. Experimental results demonstrate that our framework significantly improves network scalability by reducing the utilization of wireless bandwidth caused by a large number of malicious messages. Our system is also demonstrated to be effective in mitigating against malicious messages and protecting peers from being affected. Thus, our framework is particularly valuable in the deployment of VANETs by archiving a high level of scalability and effectiveness.

The rest of this paper is organized as follows. First, we give an overview of the data design and major components of our framework in Section 2. We then describe the scalable and secure trust opinion aggregation and propagation in Section 3. We also present peer-to-peer trust modeling in Section 4. Experimental simulations and analysis are conducted to evaluate our framework in Section5. After that, we survey and compare with some related work in Section 6. Finally, conclusions are highlighted and future research directions are pointed out in Section 7.

2 Overview

The basic idea of our framework is to evaluate and disseminate a message based on its quality. We design our framework in a way that messages can be evaluated in a distributed and collaborative fashion. At the same time, the dissemination distance of a particular message is largely dependent on its quality, so that messages of good quality propagate to the furthest distance while malicious data, such as spam, is controlled to a local minimum. We model the message quality using a trust-based approach. In other words, the quality of a message is mapped to a trustworthiness value, which can be computed from a collection of distributed feedback from other peers in the network. Specifically, during the message propagation, the peer who receives the message can instantly provide feedback, namely, a *trust opinion* generated from an equipped *analysis module*. A set of trust opinions are appended to the message during message propagation. For those who receive the message, their *action module* may decide to trust or distrust the message by computing its trustworthiness from an aggregated list of trust opinions. Apart from the trust modeling on data quality, we further model the behavior of vehicle entities using a *peer-to-peer trust* approach. In this section, we describe the data design and main components of our system.

Three types of messages are generated in our system: sender message, trust opinion, and aggregate message. A sender peer prepares a sender message: $M = [event, confidence, time, location]$. $confidence \in [0,1]$ provides flexibility in reporting an event – higher confidence indicates the sender itself is more confident in the reported event. $time \in N$ is a positive integer, and $location \in N \times N$ is a geographical coordinate, both being available from an equipped GPS device. Trust opinion: $O = [reaction, confidence]$, where $reaction \in \{trust, \neg trust\}$ and $confidence \in [0,1]$, is a message provided by a peer that serves as the evaluation of the sender message. Evaluation is conducted by comparing the reported event with the peer's current knowledge, which may come from a number of equipped car sensors, the local database, or even human interactions. An *analysis module* in our system provides such an opinion. Aggregated message: $A = [M, O_1, \ldots, O_n]$, is a combination of a sender message and a list of trust opinions from distinct peers.

Figure 1 illustrates the modular design of our trust-based framework composed of several major components. Message evaluation contains two modules: analysis module and action module. The analysis module generates trust opinions. It analyzes a sender message's validity, correctness and accuracy based on a peer's local knowledge, and attempts to provide a trust opinion of either "trust" or "¬trust". One

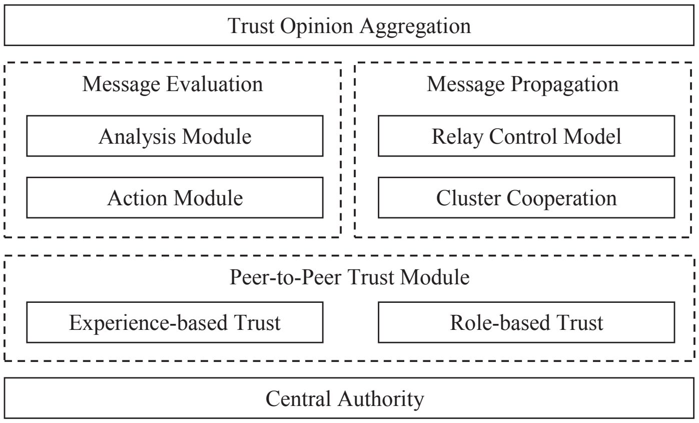


Figure 1: Design of Framework

important design principle is that the trust opinion should always be generated before any disclosure of the existing trust opinions in the aggregated message. In other words, the generation of the trust opinion is purely based on the peer's local knowledge, such as direct observations. By doing so, we are capable of coping with gambling peers who give trust opinions by strategically guessing the message trustworthiness from others' trust opinions so as to quickly and maliciously increase their trust. If a trust opinion can be provided, it is broadcasted and appended to the sender message. The action module is where a local decision is made. It derives a local action using a trust-based computation model that will be described in Section 3.3.

Message propagation consists of two components: cluster cooperation and the relay control model. Based on a cluster-based routing mechanism, the cluster cooperation serves as the foundation for message propagation and trust opinion aggregation. The relay control model works as a filter that controls the relay of messages. The trust opinion aggregation scheme ensures that message evaluation and propagation can be done with little interference on each other. It provides high flexibility that during message propagation, trust opinions can be aggregated in a secure, scalable and efficient fashion [1].

Peer-to-peer trust module manages the trustworthiness of peers. Motivated by the approach of [11, 10], we employ both *role-based trust* and *experience-based trust*. A minority of vehicles, such as police cars, are assigned by a specific role and a specific role-based trust value. For other vehicles, they are associated with experience-based trust. Each peer maintains experience-based trust for other peers. The offline central authority assigns roles and updates role-based trust, collects distributed experience-based trust from peers, and praises or punishes peers accordingly. We provide detailed descriptions of these major components in the following sections.

3 Trust Opinion Aggregation and Propagation

In this section, we describe how trust opinions from peers about a sender message can be effectively aggregated and propagated in the VANET, and also demonstrate how the trust opinions help a single peer to derive a local action decision about whether to follow the sender message.

3.1 Cluster-based Secure and Efficient Aggregation

To achieve scalable trust opinion aggregation, we rely on a cluster-based data routing mechanism. A number of cluster-based routing protocols have been proposed to achieve scalability for vehicle-to-vehicle messaging [7]. By grouping peers into multiple clusters, the system becomes scalable by having message relay done between cluster leaders instead of between two neighboring peers. To implement our message aggregation protocol, a secure and efficient aggregation scheme is required. We propose an aggregation scheme [1] that extends the identity-based aggregate signature algorithm whose details can be found in [5].

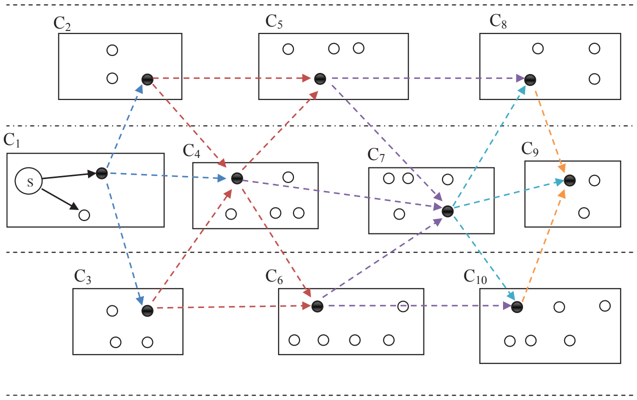


Figure 2: Cluster-based Message Propagation

As demonstrated by an example shown in Figure 2, vehicles (peers) are geographically grouped into 10 clusters, i.e. from C_1 to C_{10}. For each cluster C_i, a vehicle is randomly chosen from all cluster members (the white nodes) as the cluster leader L_i (the black nodes). Sender s in cluster C_1 broadcasts a message M to its members who will provide their trust opinions O_i immediately afterwards. After that, the cluster leader L_1 collects O_i and aggregates them into the aggregated message A. L_1 sends A to the next hop clusters C_2, C_3 and C_4. Upon reception of A, the cluster leader (e.g. L_4 here) broadcasts A to its cluster members, collects their trust opinions (if any), aggregates them together with the existing A into a new aggregated message A', and computes a relay decision about whether to relay A' to the next hop cluster C_5, C_6 and C_7.

3.2 Relay Control Model

Our relay decision is determined by the majority opinion: a message trusted by the majority should be relayed; otherwise it is to be dropped. Formally, let P be a set of peers whose trust opinions are "trust", $P = \{i|\ \mathrm{ID}_i \in A \text{ and } O_i = [trust, c_i] \in A\}$, and P' be a set of peers whose trust opinions are "¬trust", $P' = \{i|\ \mathrm{ID}_i \in A \text{ and } O_i = [\neg trust, c_i] \in A\}$. A relayer (cluster leader) L computes the weight of "trust" and "¬trust" opinions respectively as:

$$W_{trust} = \sum_{i \in P} c_i T_i, \quad W_{\neg trust} = \sum_{i \in P'} c_i T_i \tag{1}$$

and $T_i \geq \tau$, where τ is a trust threshold set by L, $c_i \in [0,1]$ is the confidence given by peer i, and T_i is the peer-to-peer trust of peer i. We will introduce the peer-to-peer trust in Section 4. Messages can be relayed only if

$$\frac{W_{trust}}{W_{trust} + W_{\neg trust}} > 1 - \varepsilon \tag{2}$$

where $\varepsilon \in [0,1]$ is a threshold set by the system to denote the maximum error rate allowed. ε is embedded in the protocol and can be adaptive to the current environment, situations and data types. For example, for more critical messages, such as car accidents, a lower error rate is appreciated.

3.3 Action Module

The action module derives a local decision for a peer to take an action towards a sender message from trust opinions for the message. Specifically, the aggregated trustworthiness of the message is computed and mapped to an action set $\{follow, \neg follow\}$. Let A denote the aggregated message, s denote the original sender, P denote the peers who contribute trust opinions of "trust", and P' denote the peers with opinions of "distrust". Let T_A denote the aggregated trustworthiness of the message A. The action module of peer p computes:

$$T_A = \frac{c_s + \sum\limits_{i \in P} c_i - \sum\limits_{i \in P'} c_i}{1 + |P| + |P'|} \tag{3}$$

where $c_s \in [0,1]$ is the sender's confidence in the sender message, $c_i \in [0,1]$ is the confidence in the trust opinion given by peer i, and $T_A \in (-1,1]$.

Considering that the sender is a different role from those who provide trust opinions, we employ a sender weight factor $\gamma > 0$ that determines how much weight is placed on the sender. Considering that the peer's honesty varies, we also employ the peer-to-peer trust module. Each peer i is associated with a trust metric $T_i \in [0,1]$. We combine the sender weight and the trustworthiness of each peer into the computation for the aggregated trustworthiness of the message A as follows:

$$T_A = \frac{\gamma c_s T_s + \sum\limits_{i \in P} c_i T_i - \sum\limits_{i \in P'} c_i T_i}{\gamma T_s + \sum\limits_{i \in P} T_i + \sum\limits_{i \in P'} T_i} \tag{4}$$

and $T_i \geq \tau$, where $\tau \in [0,1]$ is the trust threshold customized by each peer p. The trust threshold helps filter trust opinions from those peers that are not highly trusted. τ can be set to a higher value close to 1 so that only trust opinions from highly trusted peers will be used. In practice, the value of τ should be determined by the availability of trust opinions. For example, τ can be set higher when a larger number of trust opinions are available.

The action module implements a mapping $f_{action} : T_A \rightarrow \{follow, \neg follow\}$ that maps the trustworthiness of the message to an action. $f_{action} = follow$, if $T_A \geq \varphi$, otherwise $f_{action} = \neg follow$, where $\varphi \in [-1,1]$ is the action threshold. The value of φ can be personalized by each peer: a higher action threshold indicates the peer is more "cautious" of following other peers' advice and vice versa.

4 Peer-to-Peer Trust Module

In our system, each peer's trust is evaluated by a trust metric: either role-based trust or experience-based trust. Let $T_i \in [0,1]$ denote the peer-to-peer trust of peer i, we have $T_i = T_i^r$ if peer i has a role, otherwise $T_i = f(T_{i,p}^e)$ where $T_i^r \in [0,1]$ is the role-based trust of peer i, and $T_{i,p}^e \in [-1,1]$ is the experience-based trust of peer i from peer p's perspective. We map the value of T^e to the same range of T^r by employing a mapping function, e.g. $f(x) = (x+1)/2$.

It is known that although most vehicles are for personal purposes, a small number of entities have their specific responsibilities in the traffic system, e.g. police cars. Roles are assigned to them and it is reasonable to assign multiple levels of trust to different roles. These roles can be authority, such as traffic patrols, law enforcement, state or municipal police having the highest level of trust (i.e. $T^r = 1$), as used in our evaluation. Agents specialized in road condition related issues such as media (TV, radio or newspaper) traffic reporters, government licensed and certified instructors of driving schools etc. receive the expert role with the second highest level of trust (i.e. $T^r = 0.9$). Agents familiar with the traffic or road conditions of the area in consideration, e.g. local people who commute to work on certain roads or highways or have many years of driving experience with a good driving record (e.g. taxi drivers), are given the seniority role with the third highest level of trust (i.e. $T^r = 0.8$). For most of the peers who do not have a role (i.e. $T^r = 0.5$), we use the experience-based peer trust to dynamically reflect a peer's trustworthiness in the system. The behavior of a peer is evaluated by other peers, each of whom maintains trustworthiness for a list of peers in the system.

We denote the peer i's experience-based trust from p's perspective as $T^e_{i,p}$, whose value is in the range of $[-1,1]$. We simplify the notation of $T^e_{i,p}$ as T in the following formalization. Adapted from [11], if i's trust opinion leads to a correct decision of p, peer p increases the trust of i by

$$T \leftarrow \begin{cases} \lambda^t(1-c\alpha)T + c\alpha & \text{if } T \geq 0 \\ \lambda^{-t}(1+c\alpha)T + c\alpha & \text{if } T < 0 \end{cases} \tag{5}$$

otherwise, decreases T by

$$T \leftarrow \begin{cases} \lambda^t(1+c\beta)T - c\beta & \text{if } T \geq 0 \\ \lambda^{-t}(1-c\beta)T - c\beta & \text{if } T < 0 \end{cases} \tag{6}$$

where $\alpha, \beta \in (0,1)$ are increment and decrement factors, $c \in [0,1]$ is the confidence value placed by i in the message, $\lambda \in (0,1)$ is a forgetting factor, and $t \in [0,1]$ is the time closeness between the current interaction and the previous one. Our calculation of experience-based trust is scalable. It updates a peer's trustworthiness in a recursive manner. The computation of our experience-based trust is thus linear with respect to the number of times receiving trust opinions from a peer. And only the most recent trust value is needed to be stored and used for computation. We add the confidence c as an factor because peers, including the sender, play different roles in the message's trustworthiness by placing different confidence values. This can be explained by the design of Equation 4.

5 Evaluation

In this section, we present evaluation results of our trust-based framework through simulations. Implemented in C++, our simulation tool allows us to simulate real life traffic scenarios by employing real maps with vehicle entities following traffic rules, road limits, and a full list of customizable parameters defined in our trust model. Compared to other existing vehicular network simulation tools [8, 2, 9, 15], our tool is specially designed for trust modeling and cluster-based messaging among potentially thousands of nodes, and thus achieves more flexibility and consumes a low amount of computational resources.

We use a map of the East York area of Toronto where a snapshot of its small subarea is shown in Figure 3. Roads are partitioned into multiple road segments, and vehicles are clustered geographically by road segments. We set the length of road segment to 0.5 kilometers, because peers within such a distance can reliably communicate with each other, according to [17]. Vehicles are moving in the map in any possible directions and in different speeds. Entering a new road segment indicates that the peer is switching from one cluster to another.

We set values for different parameters for our trust modeling. The purposes and details of these parameters have been introduced in Sections 3 and 4. In our experiments, the sender weight factor γ is set to 2 to double the weight of a sender in message evaluation. Assuming that peer dishonesty is well tolerated by the system, we set the peer's trust threshold τ to 0.1, and the maximum error rate ε in the relay control model to 0.8. We also set $\beta/\alpha = 10$.

Additional parameters for simulating the vehicular network are also specified in our experiments. We simulate a total number of 1125 vehicle entities. We also set 2% of them as authority roles, such as police cars, road side units, and traffic controllers. The authority entities are fully reliable and trustworthy, and capable of providing other peers with valid observations and trust opinions. Average number of vehicles

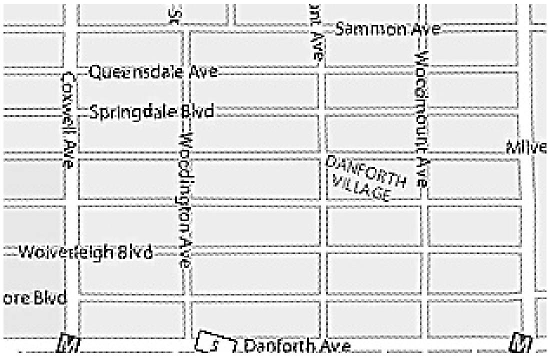


Figure 3: Map for Simulating VANET

per cluster is set to 5 to reflect the road situation in regular hours. The evaluation of effect of traffic density is left for future work. Vehicle speed is dependent on weather condition, traffic density, and speed limit of the road. To simplify our experiment, we assign a unique average speed to each road, where the vehicle's speed randomly varies ±10% from the average speed. As mentioned in Section2, the trust opinion is purely based on peer's local knowledge. In our experiment, we assume that all messages are observational. From this assumption, we further assume that the analysis module can provide trust opinions only when Δd, the geographical distance between the event and the peer, is smaller than d_{max}, the maximum distance for trust opinions. As a result, we can have the confidence value in the trust opinion determined by the geographical closeness: the closer the event is, the higher confidence value should be provided. In our experiment, confidence c is calculated as

$$c = \begin{cases} (d_{max} - \Delta d)/d_{max} & \text{if } \Delta d < d_{max} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

5.1 Scalability

Our trust model can improve network scalability by the relay control model, which detects and filters malicious messages during propagation. We evaluate the scalability by introducing the following attack model. Attackers abuse their local vehicular network by frequently sending spam messages, which could be out-of-date information or repeated messages. Spam messages might not be misleading but they take up a certain portion of wireless resources and lower the utilization rate of available bandwidth. Extra parameters for the evaluation of scalability are listed in Table1. Assuming that spam is easier to detect than misleading messages as the pattern of spams has less variety, we increase the detection rate of analysis module globally by setting it to the uniform distribution from 0.4 to 1.0. We also include fewer attackers by setting the percentage of spammers to 1%, each of whom sends one spam every 5 seconds, which is much more frequent than misleading messages.

Table 1: Extra Parameters for Evaluation of Scalability

Parameter Description	Value
percentage of spammers	1%
spam sending frequency	5 seconds / message
detection rate of analysis module	uniform distribution, [0.4, 1.0]

Our evaluation of scalability features in the average propagation distance of spam and global relay effectiveness. Both evaluation metrics compare the performance among five predefined scenarios as follows:

- Original: without regard to the trustworthiness of messages, they are simply relayed to the next hop, until the furthest allowed distance is reached;
- Relay Control (RC): a relay decision is made based on Equations 1 and 2 but without considering the role-based and experience-based trust;
- RC+Role: only role-based trust is involved for relay control;
- RC+Exp: only experience-based trust is used for relay control;
- RC+Role+Exp: both role-based trust and experience-based trust are used;
- 100% Detection: the ideal case where each peer detects all spam messages.

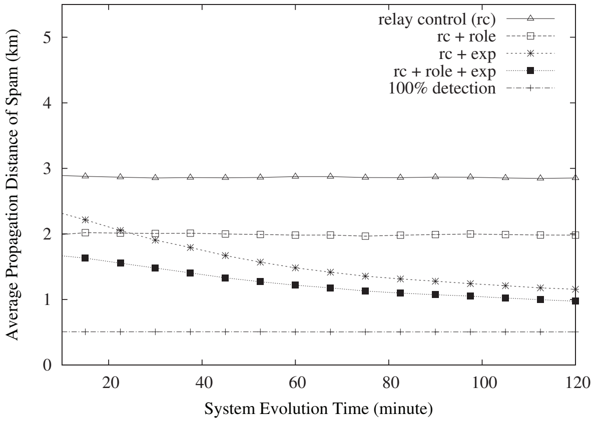


Figure 4: Propagation Distance of Spam

Based on the fact that the number of messages that can be relayed in a fixed period of time has an upper bound due to limited wireless channel resources, our system becomes more scalable as more normal messages can be relayed, which is achieved by detecting and controlling spam within a shorter distance. The maximum propagation distance without relay control is 5.5 km as defined in our experiment. The relay control reduces the distance of spam by nearly half, as observed in Figure4. Authority roles further restrict the spam within approximately 2 kilometers away from origin, due to the fact that authority roles have assisted its cluster relayer to drop the spam at an earlier phase of propagation. From the curves of RC+Exp and RC+Role+Exp, we can conclude that the experience-based trust plays a greater part in spam control as our experiment simulates for a longer time. This also explains why RC+Role achieves better performance at the beginning but is sooner overwhelmed by RC+Exp after 30 minutes of system time. The curves of RC+Exp and RC+Role+Exp demonstrate the trend of converging to the performance of 100% detection, under which scenario spam is always dropped and never relayed to neighbor clusters, in other words, restricted within 0.5 kilometers (the length of cluster defined in our experiment). As the experience-based trust of spammers is gradually decreased, their messages will not be trusted and not be relayed.

We also evaluate system scalability using the global relay effectiveness, which measures how effectively messages are relayed in the presence of a considerable amount of spam messages. Specifically,

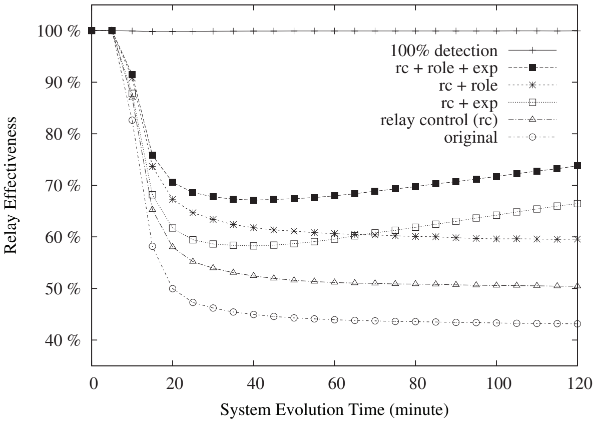


Figure 5: Global Relay Effectiveness

we define the global relay effectiveness $R = \frac{1}{N}\sum_{i=1}^{N} R_i$, where N is the total number of clusters, and R_i is the relay effectiveness for a single cluster C_i, which is computed as $R_i = (1 - S_i/M_i) \times 100\%$, where S_i is the number of relayed spam messages and M_i is the number of all relayed messages by cluster C_i. We illustrate the global relay effectiveness in Figure5. Spams are restricted from dissemination after we apply the relay control model. Role-based trust always improves the effectiveness in that spam messages are further restricted. The global relay effectiveness stops ceasing and begins to recover after 35 minutes if the experience-based trust is applied, as can be observed from curves RC+Role+Exp and RC+Exp. As peers become more experienced, the capability of the system to cope with spammers is strengthened.

5.2 Effectiveness

We evaluate the effectiveness of our system in terms of its capability of mitigating against malicious messages and protecting peers from being affected. We define the attack model where attackers jeopardize the network by broadcasting fake events, such as “traffic congestion here”, so as to cheat peers and maximize their own interest. We measure the average number of wrong actions per peer. An instance of “wrong action” indicates that one malicious message is trusted by a certain peer whose action module computes an action decision of “follow”.

Table 2: Extra Parameters for Evaluation of System Effectiveness

Parameter Description	Value
percentage of malicious peers	10%
frequency of malicious messages	30 seconds / message
analysis module’s detection rate	uniform distribution, [0.05, 0.95]

Extra parameters for evaluating system effectiveness are listed in Table2. 10% of peers in the system are attackers, each of whom sends a malicious message after every 30 seconds, which is approximately the time of driving from one cluster to another. Considering that the analysis module generates trust opinions, we define the detection rate d_{rate} as follows:

$$d_{rate} = Pr\{D|M\},\ D \text{ is a successful detection given a malicious message } M. \tag{8}$$

The analysis module generates a trust opinion of “distrust” upon a successful detection, otherwise “trust”. To better reflect the real situation, we assume that the capability to detect malicious messages varies among peers. In our experiment, the peer’s detection rate follows the uniform distribution in $[0.05, 0.95]$, except for those authority roles, whose detection rate is the highest and fixed to 1.

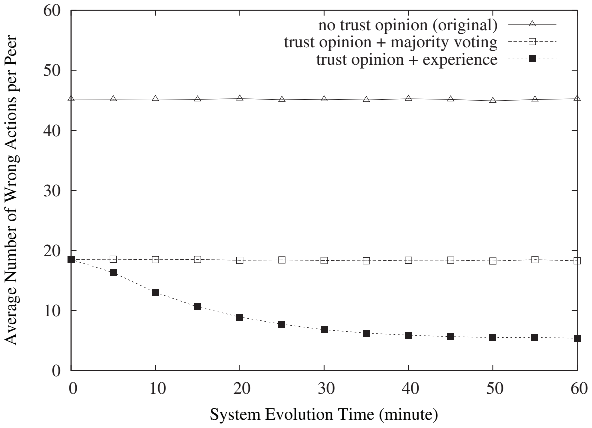


Figure 6: Effect of Trust Opinions

We measure the effect of trust opinions under three trust opinion modes:

- No trust opinions: The action module ignores all trust opinions. Specifically, when the peer is within the maximum distance where a trust opinion is available, the action module follows the reaction of the analysis module; otherwise, it simply follows the message;
- Trust opinions + majority voting: The action module computes a local action using Equation 3 without considering the trustworthiness of peers;
- Trust opinions + experience-based trust: A local action is computed from trust opinions by considering each peer’s trustworthiness using Equation 4.

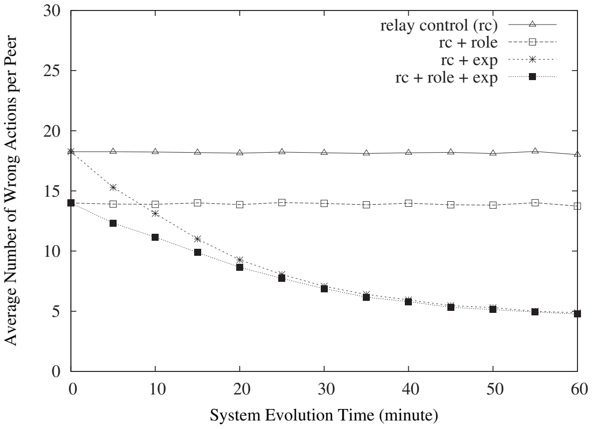


Figure 7: Effect of P2P Trust when Relay Control Model is on

We run the simulation for 60 minutes and sample the data after every 5 minutes. As shown in Figure 6, each peer makes an average number of approximately 46 wrong actions if trust opinions are excluded. However, this number drastically drops to 19 (i.e. by 65%) if trust opinions are considered. The employment of experience-based trust further decreases the number of wrong actions globally as the system evolves. This is because once a peer obtains its own experience after being cheated by a malicious message, it will update the experience-based trust for those who have provided trust opinions for that message. The malicious peers' trust is shortly decreased. As a result, the action module improves its accuracy by mitigating against malicious peers. We also evaluate the effect of our peer-to-peer trust model, as shown in Figures 7. Typically, we see that role-based trust reduces the number of wrong actions at all times.

6 Related Work

Golle et al. [6] propose an approach to detect and correct malicious data in vehicular networks. They assume that each vehicular peer is maintaining a model which consists of all the knowledge that the peer has about the network. Data is trusted if it agrees with the model with a high probability. Our work also provides high resistance and security against malicious entities using a fundamentally different way of message evaluation. Instead of relying on an assumed model and seeking explanations, messages in our model are evaluated in a distributed and collaborative fashion by collecting multiple opinions during their propagation.

Raya et al. [14] in their work employ trust into data evaluation in vehicular networks. In contrast to traditional views of entity-oriented trust, they proposed data-centric trust establishment that deals with the evaluation of trustworthiness of messages from other peers instead of vehicle entities themselves. Their work shares some commonalities with ours, such as the employment of data trust. One of the shortcomings of their work is that trust relationship in entities can never be reliably established. The data-centric trust has to be established again and again for each event, which may not be applicable to situations under the sparse environment where only limited evidence about the event is available. Our framework employs role-based trust to cope with the data sparsity problem.

Possibly the closest to our model, Dotzer [3] suggests building a distributed reputation model that exploits a notion called opinion piggybacking where each forwarding peer (of the message regarding an event) appends its own opinion about the trustworthiness of the data. They provide an algorithm that allows a peer to generate an opinion about the data based on aggregated opinions appended to the message and various other trust metrics including direct trust, indirect trust, sender based reputation level and Geo-Situation oriented reputation level. In our framework, we also introduce the trust-based message propagation to control the spread of malicious messages, in order to increase network scalability.

7 Conclusion and Future Work

We presented a novel trust-based message evaluation and propagation framework in VANETs, where a set of trust metrics, including trust opinions, experience-based trust and role-based trust, are used to model the quality of information shared by peers and the trust relationships between peers. Our proposed message evaluation approach is conducted in a distributed and collaborative fashion during message propagation, and effectively increases the overall data reliability and system effectiveness by proactively detecting malicious data. We propose that message relay controls should be trust-based, filtering malicious data to promote network scalability. Experimental results demonstrate that our approach works effectively and efficiently for the domain of vehicular networks.

Our framework depends on the existence of trust opinions generated by the analysis module. The design of such a module would involve much consideration from the perspective of hardware design, such as the design of tamper-proof devices, car sensors and human-computer interactive interfaces. Our trust aggregation and message propagation model is built on a cluster-based routing scheme where cluster leaders are responsible for judging whether to relay data based on the relay control model. For future work, we will consider the presence of malicious leaders who intentionally drop messages. We will investigate a set of detection and revocation mechanisms to cope with this issue by dynamically selecting trustworthy leaders or introducing backup leaders.

References

[1] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho. Secure and efficient trust opinion aggregation for vehicular ad-hoc networks. In *Proceedings of the IEEE 72nd Vehicular Technology Conference (VTC)*, 2010.

[2] D. R. Choffnes and F. E. Bustamante. An integrated mobility and traffic model for vehicular wireless networks. In *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 69–78, New York, NY, USA, 2005. ACM.

[3] F. Dotzer. Vars: A vehicle ad-hoc network reputation system. In *Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 2005.

[4] T. ElBatt, S. K. Goel, G. H. amd Hariharan Krishnan, and J. Parikh. Cooperative collision warning using dedicated short range wireless communications. In *Proceedings of the ACM international workshop on Vehicular ad hoc networks*, pages 1–9, 2006.

[5] C. Gentry and Z. Ramzan. Identity-based aggregate signatures. In *Proceedings of the International Conference on Theory and Practice of Public-Key Cryptography*, pages 257–273, 2006.

[6] P. Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in VANETs. In *Proceedings of the ACM international workshop on Vehicular ad hoc networks*, pages 29–37, 2004.

[7] T. D. Little and A. Agarwal. An information propagation scheme for VANETs. In *Proceedings of the IEEE Conference on Intelligent Transportation Systems*, 2005.

[8] C. Lochert, A. Barthels, A. Cervantes, M. Mauve, and M. Caliskan. Multiple simulator interlinking environment for IVC. In *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 87–88, New York, NY, USA, 2005. ACM.

[9] R. Mangharam, D. S. Weller, D. D. Stancil, R. Rajkumar, and J. S. Parikh. GrooveSim: a topography-accurate simulator for geographic routing in vehicular networks. In *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 59–68, New York, NY, USA, 2005. ACM.

[10] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. A multi-faceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks. *IEEE Transactions on Systems, Man, and Cybernetics–Part C: Applications and Reviews (SMCC), to appear*, 2010.

[11] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence Theory and Practice (IJCITP)*, 5(1), 2010.

[12] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode. Trafficview: Traffic data dissemination using car-to-car communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 8(3):6–19, 2004.

[13] S. U. Rahman and U. Hengartner. Secure crash reporting in vehicular ad hoc networks. In *Proceedings of the International Conference on Security and Privacy in Communication Networks*, pages 443–452, 2007.

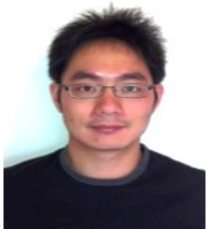
[14] M. Raya, P. Papadimitratos, V. D. Gligory, and J.-P. Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *Proceedings of the IEEE Conference on Computer Communications*, pages 1238–1246, 2008.

[15] A. K. Saha and D. B. Johnson. Modeling mobility for vehicular ad-hoc networks. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 91–92, New York, NY, USA, 2004. ACM.

[16] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the ACM international workshop on Vehicular ad hoc networks*, pages 19–28, 2004.

[17] J. Zhu and S. Roy. MAC for dedicated short range communications in intelligent transport system. *IEEE Communications Magazine*, 41(12):60–67, 2003.

Jie Zhang received his Ph.D. from the University of Waterloo in 2009. He is currently an Assistant Professor at the School of Computer Engineering, Nanyang Technological University, Singapore. His research interests include Artificial Intelligence and Multi-Agent Systems, Trust Modeling and Incentive Mechanisms, and Mobile and Vehicular Ad Hoc Networks.



Chen Chen received his Master of Mathematics in Computer Science from the University of Waterloo in 2009. He is currently a software design engineer at Microsoft. His research interests include Mobile Ad-hoc Networks, Security of Vehicular Communications and Trust Modeling of Vehicular Networks.

Robin Cohen is a Professor in the David R. Cheriton School of Computer Science, where she has been a faculty member since 1984. She conducts research in the artificial intelligence areas of multiagent systems (with a focus on trust modeling and e-commerce applications), user modeling and intelligent interaction. Professor Cohen has received the Award for Excellence in Graduate Supervision from the University of Waterloo in 2009 as well as an Award for Distinction in Teaching from the Faculty of Mathematics in 2008. She currently holds a David R. Cheriton Fellowship. In addition, from 2002-2005 she was the Associate Dean for Graduate Studies and Research in the Faculty of Mathematics and held a Faculty Fellowship.