A Trust-based Message Propagation and Evaluation Framework in VANETs

Chen Chen[†], Jie Zhang[*], Robin Cohen[†], and Pin-Han Ho[‡]

[†]School of Computer Science, University of Waterloo, Canada
[*]School of Computer Engineering, Nanyang Technological University, Singapore
[‡]Dept. of Electrical and Computer Engineering, University of Waterloo, Canada
{c32chen}@uwaterloo.ca

Abstract. In this paper, we present a trust-based message propagation and evaluation framework 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 road condition related systems, such as traffic view systems [1]. 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' 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.

2 Trust Opinion Aggregation and Propagation

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

2.1 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 [2]. By grouping peers into multiple clusters, the system becomes scalable by having message relay done between cluster leaders instead of between two neighboring peers. As demonstrated by an example shown in Figure 1, 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

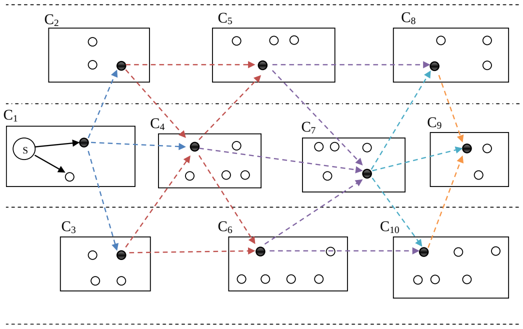


Fig. 1: Cluster-based Message Propagation

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.

2.2 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", $P = \{i | \text{ ID}_i \in A \text{ and } O_i = [trust, c_i] \in A\}$, and P' be a set of peers whose trust opinions are "¬trust", $P' = \{i | \text{ ID}_i \in A \text{ and } O_i = [\neg trust, c_i] \in A\}$. 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 3. 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.

2.3 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:

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

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:

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

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.

3 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 police cars, as used in our evaluation. For most of the peers who do not have a role, 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 [3], 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.

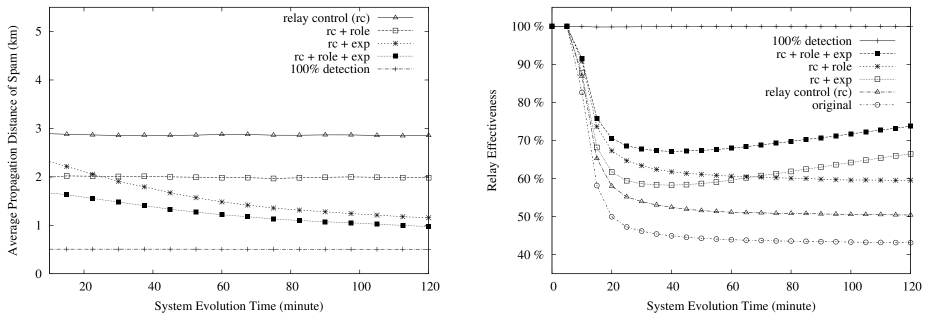
4 Evaluation

In this section, we present evaluation results of our trust-based framework through simulations of real life traffic scenarios.

4.1 Scalability

We evaluate the scalability by introducing the following attack model. Attackers abuse their local vehicular network by frequently sending spam messages. 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: a) relay control (rc): a relay decision is made based on Equations 1 and 2 but without considering the role-based and experience-based trust; b) rc + role: only role-based trust is involved for relay control; c) rc + exp: only experience-based trust is used for relay control; d) rc + role + exp: both role-based trust and experience-based trust are used; e) 100% detection: the ideal case where each peer detects all spam messages.

The relay control reduces the distance of spam by nearly half, as observed in Figure 2(a). 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.



(a) **(b)**

Fig. 2: (a) Propagation Distance of Spam; (b) Global Relay Effectiveness

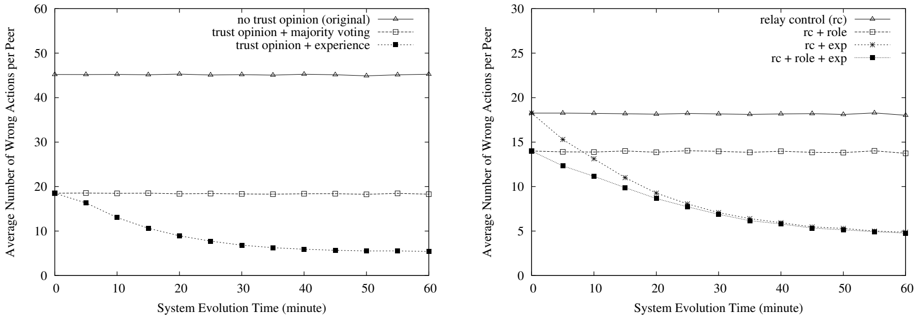
We also evaluate system scalability using the global relay effectiveness. Specifically, we define the global relay effectiveness $R = \frac{1}{N}\sum_{i=1}^{N} R_i$, where N is the total number of clusters, and R_i is the relay effectiveness for a single cluster C_i, which is computed as $R_i = (1 - S_i/M_i) \times 100\%$, 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 Figure 2(b). 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.

4.2 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.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".

We measure the effect of trust opinions under three trust opinion modes: a) no trust opinions: The action module ignores all trust opinions; b) trust opinions + majority voting: the action module computes a local action using Equation 3 without considering the trustworthiness of peers; c) trust opinions + experience-based trust: a local action is computed from trust opinions by considering each peer's trustworthiness using Equation 4.

We run the simulation for 60 minutes and sample the data after every 5 minutes. As shown in Figure 3(a), 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. We also evaluate the effect of our peer-to-peer trust model, as shown in Figures 3(b). Typically, we see that role-based trust reduces the number of wrong actions at all times.



(a) **(b)**

Fig. 3: (a) Effect of Trust Opinions; (b) Effect of Peer-to-Peer Trust

5 Related Work

Golle et al. [4] 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. [5] 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.

6 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. 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. Nadeem, T., Dashtinezhad, S., Liao, C., Iftode, L.: Trafficview: Traffic data dissemination using car-to-car communication. ACM SIGMOBILE Mobile Computing and Communications Review **8**(3) (2004) 6–19
2. Little, T.D., Agarwal, A.: An information propagation scheme for VANETs. In: Proceedings of the IEEE Conference on Intelligent Transportation Systems. (2005)
3. Minhas, U.F., Zhang, J., Tran, T., Cohen, R.: Towards expanded trust management for agents in vehicular ad-hoc networks. International Journal of Computational Intelligence (IJCI), accepted (2009)
4. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the ACM international workshop on Vehicular ad hoc networks. (2004) 29–37
5. Raya, M., Papadimitratos, P., Gligory, V.D., Hubaux, J.P.: On data-centric trust establishment in ephemeral ad hoc networks. In: Proceedings of the IEEE Conference on Computer Communications. (2008) 1238–1246