Short Paper: Establishing Trust in a Vehicular Network

Raquel G. Machado* and Krishna Venkatasubramanian†
*Department of Electrical and Computer Engineering, † Department of Computer Science
Worcester Polytechnic Institute, Worcester, MA 01609-2280, USA, E-mail: {raquel, kven }@wpi.edu

***Abstract*—This work aims to formulate a procedure to establish a graded trust system within autonomous vehicular networks. A trust management system in VANETs typically falls into one of two categories: centralized or distributed. Our solution is a hybrid system which merges the two canonical designs of a centralized and distributed structure that utilizes to capabilities of both systems. In this paper we provide the design of a trust system that takes into account both central and local evaluations to establish trust. In order to validate the trust system we design a simulation model in MATLAB that captures the interaction between different vehicles and between the vehicles and the Central Authority. The simulations show a high decision performance for the trust management system and validate the proposed scheme as a coherent grading system.**

I. Introduction

Research in trust management for VANETs typically falls into one of two categories: centralized or distributed. In a centralized trust management, a central authority (CA) such as the department of transportation is tasked with maintaininag the trust scores of the vehicles. In [1], [2] centralized trust management systems are implemented. In [3], the authors use a reputation-based system in which the road-side units (RSUs) observe and evaluate actions of vehicles along commuter paths throughout the network. To maintain freshness of the reputation scores for individual vehicles, a user of the system must first query the central authority to obtain the latest information. In [4], the trust management is performed by the CA using reports from the vehicles themselves. The problems with this centralized approach are: (1) A single point of failure; (2) The lack of access to the central authority in areas with minimal RSU coverage will prevent the effective use of the trust-scores computed; and (3) Managing the trust-scores for all the vehicles within a system and providing access to it at all times may prove prohibitively expensive.

Consequently, most of the work in this domain is focused on the distributed trust management case. A fundamental characteristic of distributed trust management is that the trust-scores computed for a neighbor is ephemeral, as storing and maintaining evaluations for all vehicles in the network is not feasible. In [5]–[7], only local information is used for the trust systems. The problem with a distributed approach is the myopic view it provides for a vehicle's behavior. As there is not much information of how a vehicle has behaved in the past, a vehicle receiving alerts from another vehicle has to inherently trust the information for the VANET to be useful, unless it can be refuted by neighbors. In isolated settings where there are not many neighboring vehicles, the distributed system has the potential to introduce a lot of errors.

In this regard, our solution aims to aggregate advantages of both centralized and distributed trust score computation to obtain a hybrid solution for the trust problem in VANETs. The contributions of the paper are two fold: (1) a hybrid scheme for trust computation in VANETs that combines both centralized and local trust scores as needed, and (2) a simulation environment for trust management on VANETs. Our results demonstrate that our hybrid approach has the potential to improve upon the existing approaches in measuring the trustworthiness of the message received over VANETS. The rest of the paper is organized as follows. In Section II, we present the system model and the solution description. Section III presents the design validation approach with the simulation model, while Section IV presents the results obtained for different simulation scenarios. Section V concludes the paper.

II. System and Threat Model

There are two basic types of entities in our system, the vehicle and the central authority. The vehicles in our model are moving from one location on a map to another and have the ability to observe their environment in an automated manner and communicate with vehicles that are within a particular distance from them over a wireless channel. The central authority has several road-side units (RSUs) placed on the side of the road which communicate with the passing vehicles and exchange traffic and other information with them.

We categorize the messages exchanged within the VANET into two types: alerts or reports. Urgent messages about "bad" *events* such as road congestion or accidents are considered *alert messages*. Alert signals are in general time-critical and are sent from one vehicle to another in response to an incident. *Reports*, on the other hand, are messages that describe the ground-truth of an incident that was reported earlier. These messages are expressly exchanged between the alert receiving vehicles and the central authority via the RSU. The principal task of the vehicles in our model are three fold: (1) if they observe an incident (e.g., traffic jam, accident etc.) they inform the vehicles around them; (2) if they receive information about an incident from another vehicle, they determine whether the information is to be accepted or not based on a local trust-score (LTS - computed based on past experiences) and a global trust-score (GTS - provided by the CA); and (3) report to the central authority via the RSUs the ground-truth about an incident for which an alert was received based on its own experience of the incident. The central authority, on the other hand, is responsible for keeping track of all the alert messages received and for computing the GTS for the vehicles based on

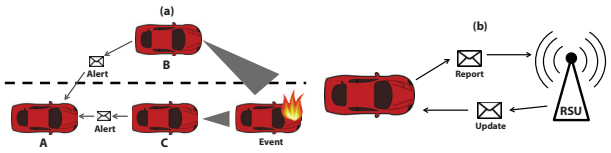


Fig. 1: Interactions of the entities in our proposed system. In (a), B and C spot an event in the road and send alert messages to A. It decides whether to accept the alerts based on their trust-scores. In (b), A sends the reports about the communication with B and C and receives an updated GTS.

inputs from many vehicles. This GTS is then disseminated to the vehicles through the RSUs as needed. In this paper, we assume that the RSU deployment is sparse to highlight the advantages of the hybrid trust-score system. The trust-scores are timestamped, concatenated with a vehicle-specific certificate, and signed by the central authority. We assume that the central authority is the root of trust for this entire system. In the rest of the paper, we use the term *sender* to denote the vehicle that issues an alert and *receiver* to denote the vehicle that receives the alert and wants to verify its veracity.

We assume the presence of adversaries in the VANET. The aim of the adversaries is to introduce bogus alert or update messages. In this work we are interested in active adversaries: those who generate or manipulate data in the network, rather than simply monitor it. The considered adversary model is a simple one; we only consider simple cases of dishonesty, leaving the analysis of other types of threats, as spoofing and collusion attacks, for future work. Further, we assume that the adversary is an insider (a vehicle node) which can do no direct preparatory physical harm to the other vehicles in the network (e.g. cutting vehicles break lines) but may intend physical harm to come as a result of a traffic accident. In this case, the adversary can actively lie by telling other cars information that might lead to undesirable actions.

As the focus of this work is on the application level, communication, security and other lower layer aspects are not analyzed. For example, since the scope of the paper focus on the "quality" of the alerts, we make standard assumptions about the actual physical-layer technology by which vehicles communicate within the VANET or with the central authority. We assume that the wireless communication within the VANETs and with Roadside Units (RSUs) is carried out using the 5.9 GHz Dedicated Short Range Communication (DSRC) standard. Moreover, since some security in DSRC is provided for by IEEE 1609.2, we also assume that the security aspects other than trustworthiness (authentication, encryption, etc.) are already taken care by the IEEE standard.

III. Solution Description

We aim to develop a system that enables a vehicle to evaluate the veracity of alert messages received over a VANET infrastructure from other vehicles in its proximity. In this regard, we take a trust-based approach to addressing the issue, where an alert is accepted as true, provided the sender of the alert is trustworthy with respect to issuing legitimate alerts. The approach that we take to compute the trustworthiness of the alert announcing vehicle is a hybrid one. That is, the trustworthiness is computed both at the local (receiving vehicle) and at a global (central authority) level. The local trust-score is computed by vehicles based on its own experience of the alert that was issued. The LTS is computed without any external feedback about the sender of the alert, and requires the self-verification of the reported alert event, which may or may not be possible. The global trust-score on the other hand is computed based on reports obtained from multiple vehicles that received a particular alert message. In this paper, both LTS and GTS range from 0 to 1. Figure 1 shows a diagram depicting the interactions between the entities in this system.

A. Local Evaluation

Local evaluation is the process by which a vehicle iteratively refines their LTS of vehicles from whom they receive alert messages. For example, if the sender reports an icy spot on the road ahead, the receiver might soon pass the spot and judge this claim. If the claim made by the vehicle is judged true, then the vehicles' trust grade is increased as follows:

$$lts_x^y(k+1) = lts_x^y(k) + \alpha \cdot (1 - lts_x^y(k)) \quad (1)$$

Otherwise, the vehicles' trust grade is decreased.

$$lts_x^y(k+1) = lts_x^y(k) - \beta \cdot (1 - lts_x^y(k)) \quad (2)$$

Here, $lts_x^y(i)$ is the local trust score that vehicle x has on vehicle y after i alerts have been received from y. The values $\alpha, \beta \in (0, 1)$ are scaling parameters for the cases where the alerts are found to be true and false, respectively. In general, we want to choose α to be small. This reduces the chances of a malicious entity from acquiring reputation fast and then misusing it. On the other hand, the value of β should also be relatively small, because the ground-truth assessment of an event may not be accurate.

B. Central Evaluation

The central authority maintains a global trust-score (GTS) for each vehicle in the system. The GTS of each vehicle is computed based on the updates that the receivers send to the CA, for the alerts issued by the vehicles. The updates are computed based on the receiver's evaluation of the ground-truth of the event associated with the alert. Therefore, for every alert received, the receiver first makes a decision to accept or reject the alert based on the GTS in the alert and the pre-computed LTS for the sender. If the receiver eventually reaches the point where the event specified in the alert happened, it will evaluate whether the information alert was correct or not. It will then create an update for the event for the sender with the information regarding the correctness of the alert. Conceptually, the report sent to the CA contains the alert messages corresponding to the report along with their corresponding identification number of the sender and a binary value signifying the measured ground-truth of the event in the alert.

The CA uses an evaluation function to determine the GTS of a vehicle. The function is a convex combination of: (1) the average score (a_{gts}) calculated based on the vehicles' past GTS and (2) the current score (c_{gts}) calculated based on the "recently" (we will expand on this in the next section) received

updates for alerts issued by a vehicle since the previous GTS computation. More formally, for a vehicle x:

$$gts(x) = \gamma a_{gts}(x) + (1-\gamma)c_{gts}(x) \quad (3)$$

Here, γ is a parameter that defines how much weight should be given to the historic GTS of the vehicle. We desire the central grade for a vehicle to be slow-changing, so at any given moment the historical component of a vehicles' trustworthiness should weigh most heavily in determining its grade. This corresponds to a γ close to 1. To calculate this parameter, we use a decreasing convex function that converges asymptotically. In this paper, we calculate the parameter γ based on the variance of the historic GTS. The intent is to reward consistent behavior from a vehicle. We use the following function to computer the value of γ:

$$\gamma = 0.5 \times e^{(-\tau * v)} + 0.5, \quad (4)$$

where v is the variance of the historic GTS calculated using a window of some constant length L over previous central evaluation grades, and τ is the parameter that indicates the inertia of the system.

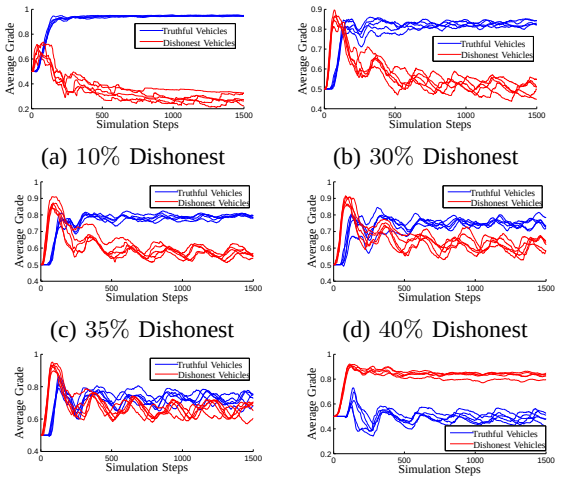
To calculate c_{gts} based on the recently received update, the CA uses the grades attributed by other vehicles, and it analyzes reports provided by the vehicles about events relevant to the update. When passing a road-side unit, the vehicles transmit the reports on the events that they witnessed and their evaluation of other vehicles' behavior in relation to those events. For each vehicle issuing an alert for the event, the CA will receive updates from all vehicles who received the alert and later observed the event and were able to analyze the truthfulness of the event. Formally speaking, the c_{gts} score of a vehicle x if computed using the following equation:

$$c_{gts}(x) = \sum_{y} \frac{gts(y) \times b_y}{\sum_y gts(y)} \quad (5)$$

Here, $y \in Y$, where Y is the set of receivers who received at least one alert issued by vehicle x since the last time its GTS was computed, $gts(y)$ is y's current GTS, and b_y is a binary value (0 or 1) representing y's verification of vehicle x's alert . Each report will be weighed by the receiver's GTS, allowing more trustworthy vehicles to have greater impact on the current score. The c_{gts} score will then be used to update current GTS of vehicle x. Note that, based on the time the first update is received for a given event, we define a deadline d_e for an event e, after which, reports about an event will not be taken into consideration for computing c_{gts}. The threshold d_e determines which updates are "recent" enough to be included and can be modified for each event e.

IV. Design Validation

To validate our approach, we implemented our own simulator with the intent of focusing on simulating scenarios that are significant to test our trust system. We simulate a short, simple one-way segment of road in each run of the simulation. As we are focused on the trustworthiness of vehicles, this setup suffices for our purposes. The simulator takes as parameter the road length, which defines the distance between the single entry and exit location pair. The average density of RSUs in the stretch of road is taken as another simulation parameter.



(a) 10% Dishonest (b) 30% Dishonest

(c) 35% Dishonest (d) 40% Dishonest

(e) 45% Dishonest (f) 70% Dishonest

Fig. 2: Average Vehicle Grades in the Central Authority

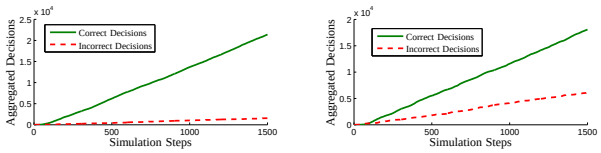
The positions of the RSUs along the road are randomly chosen according to a distribution which factors in this RSU density parameter. We simulate a set of roads with respect to a randomly drawn universe of vehicles.

When the simulation is started, each vehicle has an initial trust-score of 0.5 and a behavior pattern indicating its likelihood of being honest or dishonest. A road segment is initialized according to its length and RSU density parameters and then populated with vehicles. At each discrete moment in time, a random vehicle is selected from the universe of vehicles, entering the road with some probability taken as another parameter of our simulation. The velocity of each vehicle is constant until it leaves the road; vehicles velocities can be 1 or 2 road slots/simulation steps. In addition to the entry/exit of vehicles in the road, at each instant of time, an event can be generated in a given location of the road with a certain probability.

V. Simulations

The primary objective of the simulator is to show the feasibility of implementing such trust system. We set up different simulation environments to demonstrate the efficiency of the grade system and the impact of using both local and central evaluation systems in making good decisions. There are two simulation scenarios. The first shows the correspondence between the percentage and of "honest" and "dishonest" vehicles and the grades attributed to them, and the second shows the impact of the percentage of "dishonest" vehicles in the road on the quality of the decisions the vehicles take regarding the generated events. The parameters' values used in the simulation are: $\alpha = 0.2$, $\beta = 0.7$, $\tau = 0.5$ and $d_e = 3$ steps.

In Figure 2, we show the evolution of the vehicles' grades in the Central Authority for different percentages of "dishonest" vehicles in the road. The percentages shown in this figure were chosen to showcase the degradation of the system in face of an increasing number of adversaries. Each line represents the average grade of all vehicles from each type of disposition for a given run of the simulator. For this figure, 5 different runs of



(a) 10%-Aggregated Decisions (b) 30%-Aggregated Decisions

Fig. 3: Local Decisions

the simulator were performed and 12 RSUs were distributed along a road with 100 slots length.

The average grades of the "honest" vehicles converge to values above 0.9 and "dishonest" vehicles grades converge to below 0.5, when there are 10% of "dishonest" vehicles in the road. It can be noticed that there is a very clear distinction between the two different types of vehicles. As the percentage of "dishonest" vehicles increases, the converging grades for the different types of vehicles approximate to each other, as expected. With 35% of "dishonest" vehicles it is still possible to obtain a clear separation between the two types of vehicles, but with 40% no clear grade distinction exists anymore. Note that with 45% of "dishonest" vehicles, the grades of "honest" and "dishonest" vehicles get mixed up. After that, the grading system breaks and "dishonest" vehicles are awarded with high grades, while "honest" vehicles receive low grades, as shown in the extreme case of 70% "dishonest" vehicles in the road.

Before reaching a rate of 40% "dishonest" vehicles, the central grading system can be efficiently judge the disposition of vehicles based on their grade once the system converged. After 40% the system becomes overwhelmed and the grades do not reflect good judgment anymore. In a real scenario though, the presence of so many malicious vehicles should be a very rare event; it is fairly reasonable to claim that our grading system would perform well in the majority of real-life scenarios.

The ultimate objective of the system is for the vehicles to take the right decisions when a given action is necessary. In the context of vehicle networks, a bad decision might have serious consequences, such as road accidents. Thus, another way to validate the proposed trust system is by evaluating the decisions taken by the vehicles, about the generated events.

In Figure 3, the information on the local decisions is shown. Notice that the slope of the cumulative correct decisions is much steeper than the slope of the cumulative incorrect decisions, for both scenarios. This means that the vehicles keep making correct decisions at a higher rate than incorrect decisions. Both graphs attest the good performance in terms of local decisions of the proposed system.

In addition to the evolution of the local decisions performed by the vehicles, it is also important to analyze the statistics of the results provided by these decisions. Table I shows the true positive, true negative, false positive and false negative information for the simulation scenarios with 10%, 20% and 30% of malicious vehicles. As expected, the percentages of true positives and true negatives decrease with the increase in the percentage of malicious vehicles. As already mentioned before, the number of malicious vehicles have a great impact

Statistics	Percentage of Dishonest vehicles 30%	20%	10%
True Positive	41.11%	43.45%	47.57%
True Negative	43.68%	46.09%	48.53%
False Positive	7.47%	5.11%	2.48%
False Negative	7.74%	5.35%	2.34%

TABLE I: Statistics for the local decisions

in the proposed grade system and naturally also impacts the quality of the decisions taken by the vehicles. In general, the percentages of correct decisions solidly surpasses the percentages of bad decisions for all tested scenarios. Even though the percentages of false negatives and false positives range from 7.74% to 2.34% in this table, these values were calculated based on all interactions of the simulation, including those before the convergence of the system. As expected, these values also decrease with the percentage of "dishonest" vehicles in the simulation scenarios. In this sense, it is possible to guarantee a good performance of the proposed system in these cases.

VI. Conclusion and Future Work

We propose a trust system for Vehicular Networks that takes into consideration both central and local evaluation systems to make decisions. The proposed system uses the local and central components to exchange information to update the vehicles trust scores that ultimately will be used to take action regarding events that may occur in the road. With this intent, two trust evaluation algorithms are implemented: local evaluation and central evaluation. The simulation results show the efficacy of the proposed grading system and demonstrated a good decision performance for the system for scenarios with up to 35% of malicious vehicles. Future work for this paper includes changes in the adversary model in the simulator, a deeper analysis on the local evaluation impact in the system performance along with focus on privacy-preserving use of pseudonyms. In addition, we will also include a standard network simulator for more detailed analysis of the proposed system.

References

[1] A. Wu, J. Ma, and S. Zhang, "Rate: A rsu-aided scheme for data-centric trust establishment in vanets," in *7th International Conf. on Wireless Communications, Networking and Mobile Computing (WiCOM)*, 2011.

[2] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in *Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking*, 2008, pp. 88–89.

[3] S. Park, B. Aslam, and C. Zou, "Long-term reputation system for vehicular networking based on vehicle's daily commute routine," in *IEEE Consumer Communications and Networking Conference (CCNC)*, 2011.

[4] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in *IEEE WiVeC 2013*, Dresden, Germany, June,2013.

[5] Z. Huang, S. Ruj, M. Cavenaghi, and A. Nayak, "Limitations of trust management schemes in vanet and countermeasures," in *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, 2011, pp. 1228 –1232.

[6] U. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty," in *IEEE/WIC/ACM International Conf. on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 2010, pp. 243 –247.

[7] Y.-C. Wei and Y.-M. Chen, "An efficient trust management system for balancing the safety and location privacy in vanets," in *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 393–400.