Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 125348, 10 pages
doi:10.1155/2009/125348

Research Article

A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks

Nai-Wei Lo and Hsiao-Chien Tsai

Department of Information Management, National Taiwan University of Science and Technology, No. 43, Section 4, Keelung Road., Taipei 106, Taiwan

Correspondence should be addressed to Hsiao-Chien Tsai, d9609102@mail.ntust.edu.tw

Received 28 February 2009; Accepted 15 September 2009

Recommended by Naveen Chilamkurti

Traffic safety applications on vehicular ad hoc networks (VANETs) have drawn a lot of attention in recent years with their promising functions on car accident reduction, real-time traffic information support, and enhancement of comfortable driving experience on roadways. However, an inaccurate traffic warning message will impact drivers' decisions, waste drivers' time and fuel in their vehicles, and even invoke serious car accidents. To enable eco-friendly driving VANET environments, that is, to save fuel and time in this context, we proposed an event-based reputation system to prevent the spread of false traffic warning messages. In this system, a dynamic reputation evaluation mechanism is introduced to determine whether an incoming traffic message is significant and trustworthy to the driver. The proposed system is characterized and evaluated through experimental simulations. The simulation results show that, with a proper reputation adaptation mechanism and appropriate threshold settings, our proposed system can effectively prevent false messages spread on various VANET environments.

1. Introduction

There are 1.2 million people killed and as many as 50 million people injured in traffic accidents each year [1]. In order to preserve people's lives, traffic safety applications [2] on vehicular ad hoc networks [3] have been developed in recent years by broadcasting real-time warning messages [4] (e.g., car accident, traffic jam, obstacle detection, etc.) through vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication channels from one vehicle (or base station) to other vehicles in order to notify drivers to avoid awful traffic situations in advance [5–7].

Traffic safety applications enhance the safety of drivers on the road. However, a false traffic warning message, that is, the message with inaccurate traffic information, will impact drivers' behaviors and increase the occurrence possibility of traffic accidents. A malicious attacker can create bogus traffic warning messages and cause intelligent collisions [8]. In addition, false warning messages can waste drivers' time and fuel of vehicles [9, 10]. To prevent false traffic warning messages spread on VANET, various secure communication protocols and systems [8, 9, 11, 12] have been proposed to ensure message authentication and message integrity. On the other hand, to determine whether the traffic event reported by a warning message is really occurred, voting schemes [10] and data-centric trust establishment mechanism [13] have been proposed recently to evaluate the trustworthiness of the message content.

In previously published works, generally vehicles are assumed to be able to detect traffic events along the road all the time. However, this simple assumption may not be practical in a real world. First of all, some types of traffic events (e.g., traffic jam) usually change their status such as location, size, or intensity over time [4]. In consequence, an inaccurate warning message may be broadcast if the corresponding traffic safety application does not consider the dynamics of event status. Secondly, sensors used to detect traffic events on a vehicle may have different levels of detection capabilities, which are dependent on corresponding manufacture specifications. When vehicles encounter the same traffic event, those who only equipped with less powerful sensors may not be able to detect the event as

others do. In addition, the detection ratio of traffic event is affected by vehicle mobility. As data collections on sensors are performed between each sampling period of time, there exists the possibility that a vehicle cannot sense or record an encountered traffic event during its high-speed movement.

In order to filter out inaccurate messages caused by the dynamics of traffic event and vehicles with different detection capabilities on embedded sensors, and false messages spread by malicious attackers in VANET, an event-based reputation system is introduced in this paper. Our design concept is to determine whether a traffic event exists and how long it lasts through distributed vehicle observations. The status of a traffic event is stored and managed in each vehicle which has encountered it or is aware of it from received messages. A traffic event will be broadcast by a vehicle through message transmission only if this event has accumulated enough reputation credits on event intensity and event reliability in this vehicle. We evaluate and analyze the performance of the proposed system by performing network simulation experiments. The simulation results reveal that the event-based reputation system is applicable to most VANET environments and can successfully filter out false traffic warning messages. Consequently, our reputation system can improve the safety of drivers on the road.

The rest of this paper is organized as follows. In Section 2, related work is discussed. In Section 3, we describe the system model on which our reputation system is based. The proposed event-based reputation system is introduced in Section 4. The results and analyses of simulation experiments for the proposed reputation system are presented in Section 5. Finally, we give the conclusion in Section 6.

2. Related Work

The fraud message problem of traffic safety application on VANET has been studied extensively. Various secure communication protocols have been proposed to provide message authentication and integrity [8, 9, 11, 12]. In the following, we review the development progress on reputation evaluation scheme based on recently published research works [10, 13–16].

Golle et al. [14] proposed a general approach to evaluate the validity of message data generated in VANET. In their scheme, every vehicle builds a model for VANET environment in which specific rules and statistical properties are implemented to validate message data received from other vehicles. The same concept for trustworthiness evaluation is also adopted later in [11, 17]. Golle et al. assumed that a node (vehicle) always trusts the data generated from its own onboard sensors. In consequence, errors from sensor-generated data, caused by malfunctioned sensors, dynamics of traffic events (e.g. the speed of a vehicle is too fast for its sensors to detect surrounding environment and gather meaningful or error-free data), and data manipulation from a malicious attacker (vehicle), were not considered in their system model. As their system model requires offline construction and parameter calibration, system flexibility and scalability may become an issue.

Picconi et al. [15] proposed a solution to validate an aggregated message with probabilistic signature checking mechanism. The proposed scheme is used to verify vehicle-related information such as the current speed and geographic location, not traffic events occurred along the road. In addition, a malicious vehicle may be able to circumvent the checking scheme if its false messages are far less than all transmitted messages in a VANET.

In general, it is difficult for a vehicle to determine the plausibility of a reported traffic event solely. In [16] Raya et al. applied message aggregation and group communication to validate a reported traffic event. The main idea is to provide a vehicle more evidence about a reported traffic event by collecting and analyzing multiple incoming messages from different vehicles. The main challenge of this paper is how to dynamically form and maintain a vehicle group with the characteristic of high mobility. The concept of message aggregation is also adopted by Ostermaier et al. in [10]. The authors proposed four voting schemes on local danger warning service. Their simulation results showed that one of the four schemes, called majority of freshest votes with a threshold, sounds promising. However, the dynamics of traffic events and the differences of sensor capabilities may cause some sensors to collect inaccurate information when vehicles pass the same event location. In consequence, it is hard for voting vehicles to achieve an agreement on a reported traffic event and to further evaluate the event correspondingly based on the voting scheme.

Maya et al. [13] proposed a data-centric trust establishment framework and applied it to the traffic safety application in VANET. The novel concept in [13] is to evaluate the trustiness of sensed data or received messages rather than the trust of individual vehicle. However, the authors did not consider the effect introduced by the dynamics of traffic events. A vehicle may not detect an occurred traffic event or may collect imprecise data due to its sensor limitation when passing the occurrence location of this traffic event; consequently, for a vehicle, the evaluation result on the trustiness of generated data (or received messages) regarding to the observed (or reported) traffic event may not be fully accurate and trustworthy.

In summary, if we consider a practical VANET environment, inaccurate or imprecise traffic information caused by dynamics of traffic events, differences of sensor capabilities, and interference of vehicle mobility will be generated and aggregated to a reputation (or trust establishment) system almost inevitably. Under such situations, related trust evaluation systems and frameworks from previous research works cannot function properly and effectively since aggregated imprecise messages will produce false alarms to traffic safety applications. In Sections 3 and 4, we propose an event-based reputation system to provide accurate and reliable traffic information to vehicle drivers and resist the false alarm effect from fraud messages spread in the network at the same time.

3. Model of Reputation System

3.1. Network Model. Traditional traffic safety applications collect traffic related information with roadside

infrastructure and transmit traffic information to traffic operation centers through wired network. Because the cost for deployment and management is relatively high, traditional traffic safety applications are only deployed in certain areas. In brief, the traditional solution is not economic and eco-friendl, and cannot provide traffic information for drivers' safety effectively and pervasively. As a VANET does not require high-cost infrastructure and centralized traffic operation center to collect traffic events, a VANET is more economic than traditional wired network solution. Furthermore, in a VANET environment, traffic information is collected and distributed by each vehicle; therefore, real-time and effective traffic information can be broadcast in a driver-concerned local area quickly and pervasively. Thus, we adopt VANETs as our network environment. As the proposed event-based reputation system will be implemented in the application layer of OSI (Open System Interconnection) network architecture, the proposed system is independent from lower OSI layers. Actually, the system can leverage novel wireless technologies (e.g., WiMAX, IEEE 802.11p) to improve its overall performance as new wireless technologies or standards provide longer transmission range, larger bandwidth, and better mechanisms (e.g., routing schemes).

3.2. Models of Vehicle and Its Traffic Safety Application. We assume that each vehicle equips with a positioning device, such as GPS (Global Positioning System). Multiple sensors with various data collection capabilities are installed in every vehicle. The details of data collection techniques of sensors are beyond the scope of this paper. Vehicle mobility and device specification make the event detection capability among similar sensors different with each other. In terms of vehicle mobility, as traffic-related data collection with sensors is not performed in real time, it is possible for an on-board sensor to overlook or miss the event signal when the speed of the vehicle is over a certain sensor threshold. On the other hand, a sensor can detect the same event many times when the vehicle is moving slowly. In terms of device specification, the event detection capability of a sensor is mainly dependent on its manufacture specification. When vehicles encounter the same traffic event, vehicles with better sensors can easily detect the event but the others cannot.

When the value of an event data gathered by a sensor is over the predefined safety threshold, the information is sent to the traffic safety application in the vehicle. Based on the evaluation results from the proposed reputation system, the traffic safety application will determine to broadcast traffic warning messages to neighboring vehicles or not. The transmission distance of a broadcast message depends on the type of traffic event or the configuration of the traffic safety application. The neighbors that received the warning messages can autonomously determine how to react based on their own traffic safety application and preconfigured policies. We assume that the type definition and granularity of a traffic event is properly defined and agreed among various traffic safety applications in advance. Traffic event information with slight difference (below a predefined threshold), such as observed timestamp, will be viewed as the same traffic event.

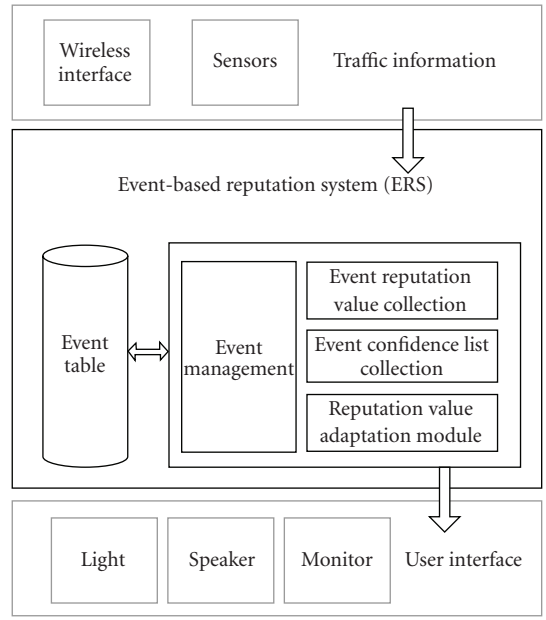

Figure 1: System architecture of the proposed event-based reputation system.

4. Event-Based Reputation System

Our event-based reputation system (ERS) is enlightened by the cooperation enforcement schemes proposed in mobile ad hoc networks [18], where nodes collaboratively observe neighbors and broadcast warnings if misbehaved nodes were discovered. The system architecture is illustrated in Figure 1.

4.1. System Overview. ERS is composed of three interfaces, four functionalities, and one repository for table storage. Traffic information comes either from received messages via wireless interface or from on-board sensors. The event table in ERS stores all received and derived traffic event information including event identity, type of traffic event, occurrence timestamp, event location, message transmission range, event reputation value, and event confidence list. In the event table, each record entry stores a distinct traffic event. Event reputation value defines the intensity degree of a traffic event and its initial value is always set to zero. A simple algorithm is adopted to compute the value of event reputation for a specific traffic event: (1) every time the given vehicle's ERS detects this event with its on-board sensors, the value is increased by one; (2) when the given ERS receives a traffic warning message from another vehicle, the ERS adds the event reputation value in the received message into the field of event reputation value at the same event record in the event table or creates a new event record in the event table. Event confidence value indicates the reliability extent of a traffic event and the value is the number of distinct vehicles whose messages, regarding to the same traffic event, have been received by the given vehicle's ERS. In addition, the definition of event confidence list is a string list of the identities of distinct vehicles which encounter the same traffic event. When a given vehicle encounters a traffic event

and detects it, the given ERS will append its vehicle's identity into the event confidence list field at the corresponding event entry. Similarly, when a given vehicle receives a traffic warning message, the content of event confidence list in the message will be appended in the event confidence list field at the corresponding event entry. In an event record, event identity represents the identity of traffic event. Type of traffic event implies the predefined event type of this event. Occurrence timestamp and event location indicate the time and location when a traffic event is detected by a vehicle. Message transmission range represents the predefined transmission distance in hop count for the traffic warning message.

The four functions supported in the ERS are event management, reputation value adaptation module, event reputation value collection, and event confidence list collection. We will introduce the first two functions in the next subsection. For the two collection functions, we have briefly illustrated how these functions work as previously stated in this subsection. Here we want to introduce two important thresholds used in ERS, that is, event reputation threshold and event confidence threshold. Event reputation threshold is used to set up the barrier for event intensity. If the event reputation value of a traffic event is higher than the predefined event reputation threshold, then the intensity of this event is sufficiently strong enough to indicate the continuous existence of this event. Otherwise, the event might not still exist anymore, even though it did occur sometime before. Event confidence threshold is used to set up the bottom line for event reliability. If the event confidence value of a traffic event is higher than the predefined event confidence threshold, then it indicates that there were sufficient amounts of vehicles that encountered the same traffic event and the occurrence plausibility of this event is much more reliable. By properly setting these thresholds and other configurable system parameters, the ERS can provide accurate and reliable traffic information to vehicle drivers. If a given ERS detects the event reputation value and the event confidence value of a traffic event is over the corresponding event reputation threshold and event confidence threshold, which indicate that the traffic event really exists and is still there, the ERS will send this event information through the user interface to notify the driver and at the same time broadcast a traffic warning message with current event reputation value and the corresponding confidence list to nearby vehicles.

4.2. Traffic Event Management. As the status of a traffic event changes dynamically and the detection capabilities of sensors in various kinds of vehicles are different, a vehicle not detecting new traffic event at a specific location and time does not imply that there is no event occurred now or before. Therefore, some traffic safety applications [10, 13] actively send traffic revocation messages to inform other vehicles when an event is resolved. However, this mechanism might provide wrong event information to other vehicles if the sending vehicle of the original revocation message misjudges the event status. In order to eliminate the weakness of event message revocation scheme, the reputation value adaptation mechanism is introduced in ERS.

The reputation value adaptation mechanism utilizes two functions to control the corresponding event reputation value of a detected event during the event's lifetime so that the event status (resolved or not) is reflected by its reputation value. The first function is the reputation value suppression function which sets the event reputation value of an event record as the event reputation threshold if the reputation value of this event record is greater than the predefined reputation threshold. Reputation value suppression function helps ERS to control the maximum value of reputation measurement.

The second function is the reputation value degradation function which is used to decrease the event reputation value of an event record in the event table according to the length of event lifetime. As time passes, the existence possibility of an unresolved traffic event decreases very quickly. For each event record in the event table, a distinct software timer starting with the predefined time period T_d is invoked to trigger the reputation value degradation function automatically when the timer is expired. The updated event reputation value of an event record is calculated by the reputation value degradation function. Equation (1) indicates the reputation degradation formula in which R_u represents the updated reputation value, R_p means the previous reputation value before the timer expired, $D(\,)$ is a preselected degradation function to control the degradation speed of an event reputation value, and N_{te} indicates the total number of timer expiration times for an event record since it has been updated last time. Notice that for an event record the ERS resets the value of corresponding N_{te} to zero when the ERS has received the same event message later from others or detected the same event by itself. When the event reputation value of an event record decreases to zero, the ERS will remove the corresponding traffic warning notification on the user interface and the event entry in the event table:

$$R_u = R_p - D(N_{\text{te}}). \tag{1}$$

In general, these two functions in the reputation adaptation mechanism, that is, the algorithm for reputation value accumulation and the degradation function $D(\,)$ for reputation decrease, can be flexibly defined and constructed based on practical VANET environments in real world.

4.3. Configuration of Event Reputation Threshold and Event Confidence Threshold. Configuration of event reputation threshold and event confidence threshold in an ERS are dependent on the sensor capability of a vehicle and the type characteristics of a traffic event. In general, there are some design criteria and guidelines to help vehicle manufacturers or drivers determine these two thresholds. For example, when instant notification of event occurrence is more important than event reliability and event continuity in situations such as emergency braking event and speed decrease event, both thresholds should be set to a lower value. On the contrary, if event reliability and event continuity are more important than instant notification of event occurrence in

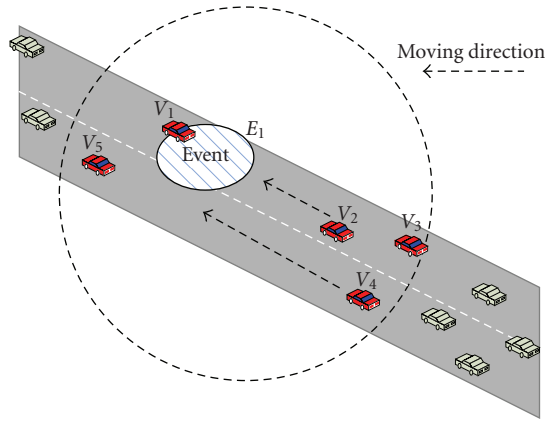

Figure 2: A vehicle (V_1) encounters a traffic event (E_1) and transmits the traffic warning message to other vehicles.

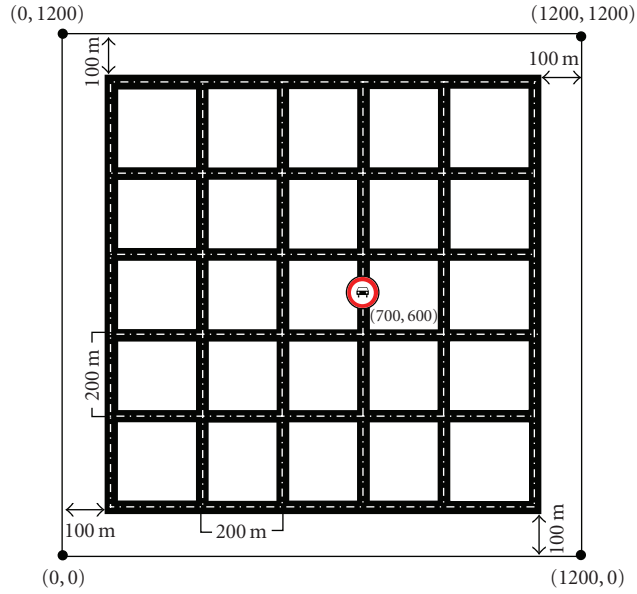

Figure 3: The street map used in our simulations. The location coordinate of the marked traffic event is at (700, 600).

situations such as vehicle accident event and traffic jam event, both thresholds should be set to a higher value. Therefore, we suggest that different pairs of event reputation threshold and event confidence threshold should be preconfigured in an ERS based on various event types and sensor capability of vehicle.

4.4. An Illustrated Example. We adopt a simple example to illustrate the operation flow of the ERS in this subsection. Assume that all vehicles have ERS installed and configured with the event reputation threshold, the event confidence threshold, and the message transmission range (in hop count) been set as 8, 2, and 3, respectively.

As shown in Figure 2, there is a traffic event E_1 on a road. Assume that the vehicle V_1 passes the location of event E_1 and the sensors on V_1 have detected E_1 3 times along the path. In consequence, the ERS in V_1 stores this traffic information, sets the reputation value of this event as 3 (i.e., $R^{v1} = 3$), and inserts its vehicle identity V_1 into the event confidence list in the corresponding event entry. Next, V_1 generates a new traffic warning message for the event E_1 that includes the traffic information, the reputation value $R^{v1} = 3$, and the confident list $[V_1]$. Then V_1 broadcasts the traffic warning message to its neighbors. Assume vehicles V_2, V_3, V_4, and V_5 have received this traffic warning message. All four of them will record this event E_1 and store the corresponding traffic information, the event reputation value ($R^{v2} = R^{v3} = R^{v4} = R^{v5} = R^{v1} = 3$), and the event confidence list (each vehicle is $[V_1]$ in this case) into their individual event tables; however, the ERS systems in these four vehicles will not notify their drivers this incoming traffic information and also not forward it, even though the message transmission range of this event does not reach to zero (i.e., $3 - 1 = 2$), because both the event reputation value and the event confidence value of this event do not reach the preconfigured thresholds.

Assume that vehicles V_2, V_3, and V_4 keep moving toward the location of event E_1 after receiving the warning message from V_1. Before V_2 encounters E_1, the event reputation values of event E_1 in V_2, V_3, V_4, and V_5 all decrease to 1 duo to the execution of event reputation degradation function in each vehicle. Suppose that when V_2 passes the location of E_1, its sensors detect E_1 8 times. Then V_2 updates the reputation value of this event to 9 (i.e., $1 + 8 = 9$) and adds its identity to the confidence list of this event $[V_1, V_2]$ in the event record. As the event reputation value of E_1 in V_2 is greater than the preconfigured reputation threshold, the reputation suppression function in the ERS is invoked to reset the reputation value to 8. Now, in V_2 the event reputation value and the number of vehicle identities in the event confidence list for the event E_1 have both reached the reputation threshold and the confidence threshold. Therefore, the ERS in V_2 will send the information of this reliable traffic event E_1 through the user interface to notify its driver and then broadcast this traffic warning message with the reputation value $R^{v2} = 8$ and the confidence list $[V_1, V_2]$ to neighbor vehicles. Vehicles that receive this traffic warning message from V_2 will repeat the same operation process of V_2 as described previously.

5. System Evaluation

Network simulator ns-2 [19] is used to evaluate system performance of the proposed event-based reputation system (ERS). IEEE 802.11b DCF is adopted for the MAC layer setting in our simulations. Omnidirectional antenna with 250-meter transmission range is assumed. The simulation scenario is set in a grid-typed street map. As shown in Figure 3, the map is constructed by 5×5 street blocks and the size of each block is 200 square meters. For each simulation 100 vehicle nodes are generated and randomly placed on roads in the scenario map. The traffic event is assumed to be at location coordinate (700, 600). To reflect the dynamic status of a traffic event, the simulating event will occur at the 100th second and be resolved at the 400th second based on our simulation settings. The simulation time in

each run is 700 seconds. Each measured result (point) in the following diagrams is an average number obtained from 500 replications of simulation runs.

We develop a new vehicle mobility model called random intersection, which is inspired by the traffic sign model proposed in [20], to simulate the dynamic status of a vehicle driving around in an urban area. In the beginning each vehicle is randomly assigned a moving speed between 10 km/h and $S_{\max}$ km/h with a randomly determined driving direction from its location, where $S_{\max}$ is the maximal moving speed predefined in the simulation environment. In our scenario map, all road intersections have traffic lights. When a vehicle approaches a road intersection, it will encounter a traffic light. The probability for a vehicle to stop at a traffic light is set to 50%. The duration of a red light is randomly decided between 0 and 40 seconds. To simulate traffic delay situation at intersections, a vehicle always stops for 2 seconds at an intersection. Note that this time duration is independent with traffic light signals. Once the time duration for a vehicle to stop at an intersection is expired, the vehicle randomly reselects its moving speed within the preconfigured speed range and its next moving direction. Note that the speed legends in the following simulation figures all indicate the maximal moving speed of a vehicle.

The sampling interval of on-board sensors in a vehicle is set to one second and event detection distance is set to 16 meters in total; that is, sensors installed at the head and the rear of a vehicle can both detect events occurred in front of them less than 8 meters away. The parameter setting for on-board sensors makes the event detection capability of each vehicle depending on its moving speed. For ERS settings, the time period to trigger the reputation value degradation function is set to 15 seconds (i.e., $T_d = 15$).

5.1. Effect of Vehicle Mobility and Traffic Density. In VANET environments, high vehicle mobility situation and low traffic density situation are main performance challenges for application systems. To evaluate the applicability of ERS under high vehicle mobility and low traffic density situations, we analyze the average accumulation speed for vehicles on event reputation value and event confidence value under different vehicle mobility and traffic density. Here we define the average event reputation value as the average of the two largest event reputation values among all vehicles at a specific simulation timestamp. A similar definition for the average event confidence value is applied. The reason is that in a VANET the vehicle with the highest reputation value and confidence value of an occurred event will be the first node to broadcast the traffic warning message to others.

For this part of simulation experiments, we intentionally disable the reputation value suppression function and the message forwarding module in the ERS. The reputation degradation function is set as a constant (i.e., $D(N_{\text{te}}) = 1$). These settings simplify our experimental environment, reduce the amount of output data, and allow us to concentrate on effect analysis.

Figure 4 shows the accumulation speed of average event reputation value to vehicles under different vehicle mobilities. It is obvious that the increment of event reputation value in an ERS is faster when vehicle mobility is low in a VANET. As the sampling interval of on-board sensors in a vehicle is set as one second, vehicles passing the event with a low speed such as 20 km/h can detect the event many times in general. Contrarily, when vehicles pass the event at a high speed such as 100 km/h, their on-board sensors may not be able to react in time and detect the event. Consequently, the corresponding accumulation speed of event reputation value becomes slower. The accumulation speed of average event confidence value to vehicles under different vehicle mobilities is shown in Figure 5. Contrary to the simulation results on event reputation value, the increment of the event confidence value in an ERS is faster when vehicles move at a high-speed. As vehicles move faster, the event will be encountered by those vehicles in a shorter time period; in consequence, the identity of each vehicle will be added to the event confidence list field of the corresponding event record in its event table. When vehicle speed varies from 60 km/h to 100 km/h, the increment of average event confidence value is not proportional to the increase of vehicle speed. This is because when a vehicle moves faster, the traffic lights are encountered sooner. A high speed vehicle takes much more portion of its driving time to wait for traffic lights.

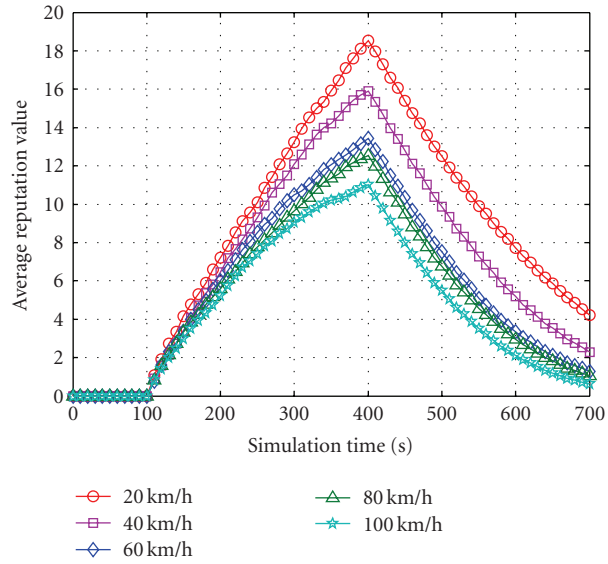

Figure 4: Average accumulation speed of event reputation value to vehicles under different vehicle mobilities.

As the event will be resolved at the 400th second based on our simulation settings, it is reasonable that the average event reputation value to vehicles decreases linearly starting from 400 seconds. The linear decrease is caused by the setting of the reputation value degradation function which is set as a constant ($D(N_{\text{te}}) = 1$) in this experiment. The ERS in a vehicle will delete the corresponding event confidence list when the event reputation value becomes zero. Therefore, the decrement trend of average event confidence value in Figure 5 is similar to the decrement trend of average event reputation value in Figure 4.

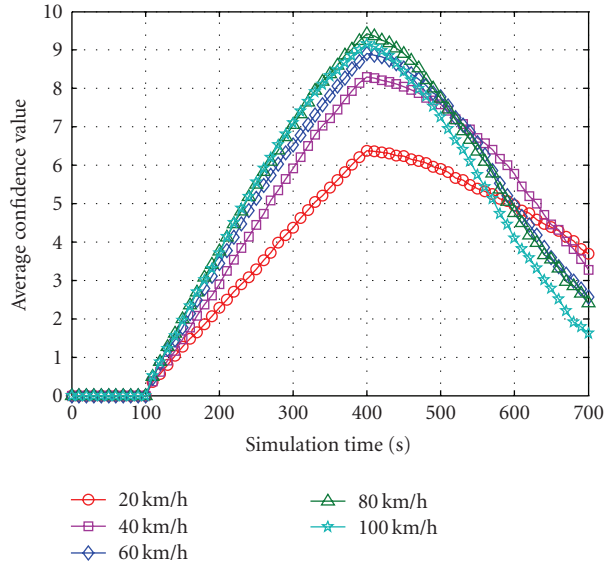

Figure 5: Average accumulation speed of event confidence value to vehicles under different vehicle mobilities.

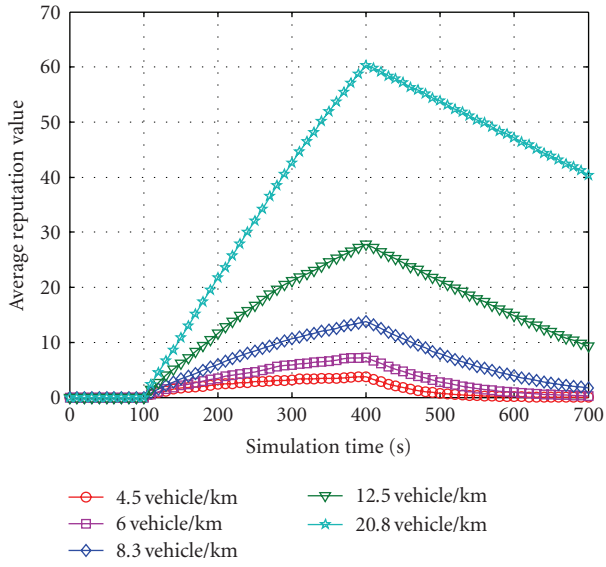

Figure 6: Average accumulation speed of event reputation value to vehicles under different traffic densities.

To evaluate the effect of traffic density to ERS, we perform another set of simulation experiments by only varying the size of street map between 3×3 blocks and 7×7 blocks. As the total number of vehicles is the same as before (i.e., 100 vehicles), the traffic density in the network varies between 4.5 vehicles/km and 20.8 vehicles/km. Figures 6 and 7 show that the accumulation speeds of average event reputation value and average event confidence value raise significantly when the traffic density increases. The reason is that a lot of traffic warning messages are generated from vehicles which have encountered the traffic event; consequently, the corresponding event reputation value and event confidence

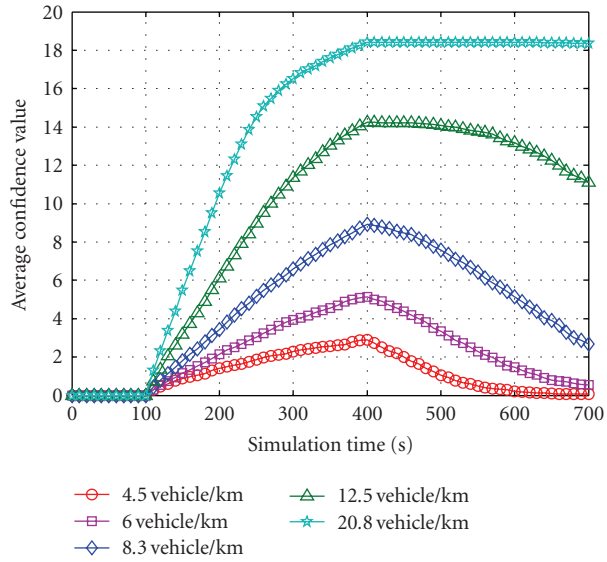

Figure 7: Average accumulation speed of event confidence value to vehicles under different traffic densities.

value of vehicles located nearby the traffic event are accumulated fast. In brief, we show that ERS is very sensitive and effective to high traffic density environments. Under our simulation environment configuration, the accumulation speeds for both event reputation value and event confidence value are much slower in low traffic density situations compared with the speeds in high traffic density cases. In practical situations, the accumulation speeds for both ERS parameters under low traffic density environments are affected by other variable factors such as the traffic event duration, the physical range (extent) of the traffic event, the detection capability of on-board sensors in a vehicle, the message transmission range of wireless interface in a vehicle, and the moving speed of a vehicle. Based on the design logic, the ERS requires more reliable or accountable information from other vehicles and its senor components to derive correct and precise warning information. Therefore, in general it will take more time for ERS to react in a low traffic density environment. To get better performance in low traffic density environments, the ERS can associate with high event resolution sensors, utilize more efficient protocols in lower OSI layer such as IEEE 802.11p standard (WAVE), and extend the wireless transmission range of the vehicle with more powerful wireless signal amplifier.

5.2. Effect of Degradation Function. In this subsection we want to explore the effect caused by the degradation function $D(\,)$ and learn how to select a proper degradation function for ERS. As shown in Figure 6, after the event is resolved at the 400th second, the average reputation value decreases very slow, where the degradation function is set as a constant (i.e., $D(N_{te}) = 1$). To explore the effect of degradation function to the decrease speed of event reputation value, we execute another experiment by setting the degradation function to Fibonacci number function $D(N_{te}) = Fibonacci(N_{te})$ and 2-based exponent function $D(N_{te}) = 2^{N_{te}}$, where $Fibonacci(N_{te})$

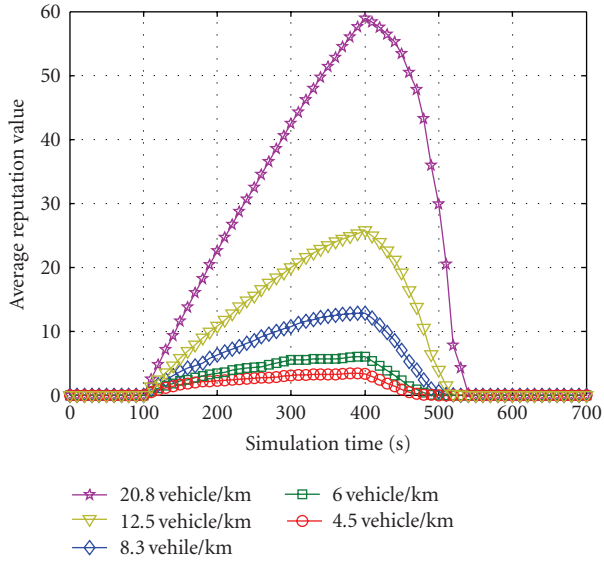

Figure 8: Fibonacci number function is adopted as the degradation function, $D(N_{te}) = Fibonacci(N_{te})$.

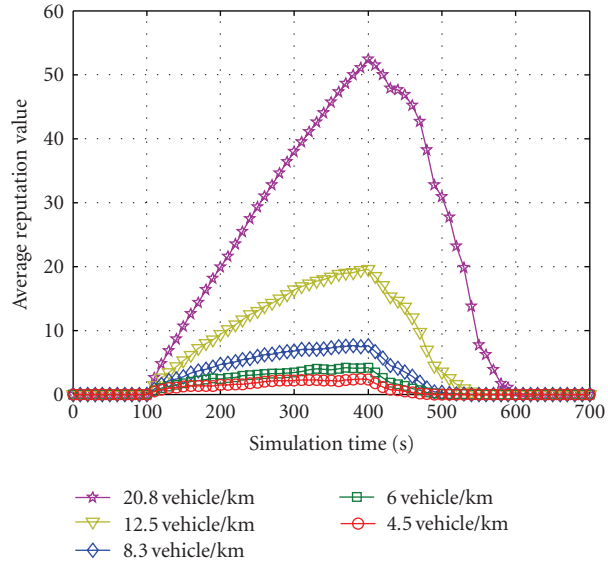

Figure 9: 2-based exponent function is adopted as the degradation function, $D(N_{te}) = 2^{N_{te}}$.

indicates the corresponding value of *Fibonacci Sequence* in the index N_{te}.

The simulation results for Fibonacci number function and 2-based exponent function are shown in Figures 8 and 9, respectively. It is obvious that both nonlinear degradation functions provide much better decrease speed on average event reputation value after the event is resolved in comparison with linear degradation function. In addition, both functions do not affect the accumulation speed on average event reputation value much while the event exists. Therefore, based on our simulation results, to improve the ERS performance a nonlinear degradation function should be considered instead of a linear one when installing and configuring an ERS.

5.3. Effect of False Traffic Warning Message. To explore the effectiveness of ERS against false message flooding attack, we perform the third set of simulation experiments in this subsection. The message transmission range field in a warning message is set to 3 hops in length. The event reputation threshold and event confidence threshold is set to 9 and 4 in the ERS, respectively. Reputation value adaptation mechanism in the ERS is fully activated in this experiment. During simulation executions, there is a randomly selected vehicle node to broadcast traffic warning messages with inaccurate content every 20 seconds. The content of these false traffic warning messages is generated randomly. A vehicle will broadcast a traffic warning message for an event when the corresponding event intensity and event reliability have reached the reputation and confidence thresholds defined in its ERS system.

A vehicle trusting the content of received warning messages and notifying its driver the false event is defined as a message-affected vehicle. The average number of message-affected vehicles is adopted to measure the influence of false

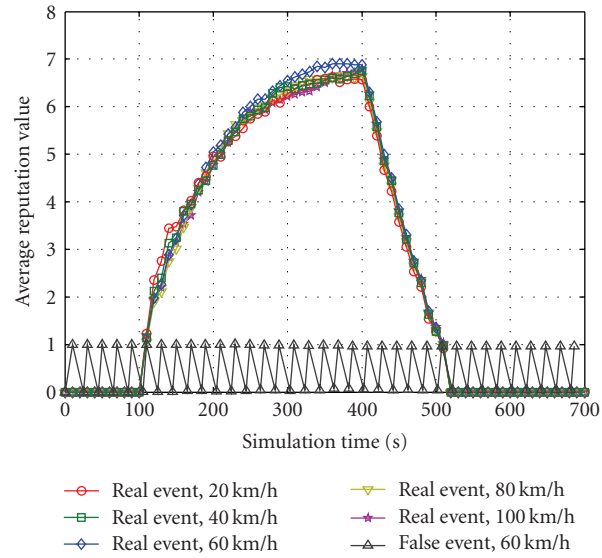

Figure 10: The comparison of average reputation value between a real event and a false event.

messages to ERS. In Figure 10, the average reputation value of a real traffic event accumulates rapidly in all kinds of vehicle mobility environments when the event exists. On the contrary, the average reputation value of a false traffic event oscillates between zero and one in all kinds of vehicle mobility environments. For clearness and simplicity, we only show the average reputation value of a false event with the maximal vehicle speed set as 60 km/h in Figure 10. Once the event reputation value and event confidence value of a real event in a vehicle reach the reputation threshold and the confidence threshold, the corresponding traffic warning message will be broadcast up to 3 hops away. Figure 11 shows the number of vehicles affected by a real traffic

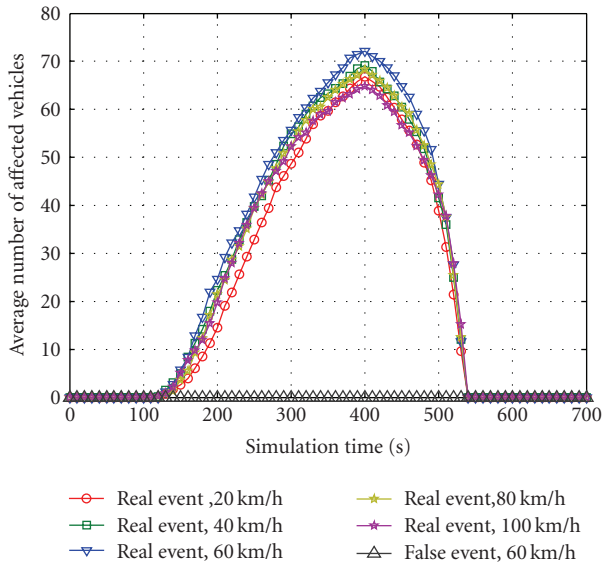

Figure 11: The comparison of the number of affected vehicles between a real event and a false event.

event increases very fast. On the other hand, the false messages generated from a malicious node does not affect the judgments of other vehicles at all, since their sensors do not detect the fraud traffic event on the road and consequently their ERS systems do not accumulate the event reputation value and event confidence value for the false event.

In Figure 10, the average reputation value for the real event is always under the event reputation threshold (which is 9) while at the same time the average number of affected vehicles in Figure 11 keeps increasing steadily during the event's lifetime. This is because the reputation value suppression function in the ERS is activated to control the maximal reputation value stored in an event record.

In summary, the simulation results show that our proposed event-based reputation system can dynamically collect event information, determine the plausibility and timeliness of an event, and broadcast accurate and reliable traffic warning messages in most VANET environments.

6. Conclusion

Traffic safety applications on vehicular ad hoc networks have attracted significant attention in recent years as they improve driving quality, drivers' comfort, and drivers' safety. To enable the massive usage of traffic safety application, it is necessary to prevent false traffic warning alarms spread on VANETs which will strongly affect drivers' behaviors and put drivers and passengers in danger. To eliminate the concern on traffic message plausibility, we propose the event-based reputation system (ERS) which utilizes cooperative event observation mechanism and reputation adaptation scheme along with event confidence threshold and event reputation threshold to evaluate the event intensity and event reliability at the same time. Experimental simulations show that the proposed system can prevent false traffic warning messages spread to the network and the system with its configuration flexibility is applicable to most VANET environments.

References

[1] World Health Organization, *World Report on Road Traffic Injury Prevention*, WHO, Geneva, Switzerland, 2004.

[2] J. Luo and J. P. Hubaux, "A survey of inter-vehicle communication," Tech. Rep. IC/2004/24, EPFL, Lausanne, Switzerland, 2004.

[3] J. J. Blum, A. Eskandarian, and L. J. Huffman, "Challenges of intervehicle ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 347–351, 2004.

[4] F. Dötzer, M. Strassberger, and T. Kosch, "Classification for traffic related inter-vehicle messaging," in *Proceedings of the 5th IEEE International Conference on ITS Telecommunications (ITST '07)*, Brest, France, June 2005.

[5] 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*, vol. 8, no. 3, pp. 6–19, 2004.

[6] W. Chen and S. Cai, "Ad hoc peer-to-peer network architecture for vehicle safety communications," *IEEE Communications Magazine*, vol. 43, no. 4, pp. 100–107, 2005.

[7] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE Communications Magazine*, vol. 44, no. 1, pp. 74–82, 2006.

[8] P. Papadimitratos, L. Buttyan, T. Holczer, et al., "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[9] F. Kargl, P. Papadimitratos, L. Buttyan, et al., "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[10] B. Ostermaier, F. Dötzer, and M. Strassberger, "Enhancing the security of local danger warnings in VANETs—a simulative analysis of voting schemes," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES '07)*, pp. 422–431, Pheonix, Ariz, USA, April 2007.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[12] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," in *Proceedings of 5th International Conference on Ad-Hoc Networks & Wireless*, vol. 4104 of *Lecture Notes in Computer Science*, pp. 266–279, Ottawa, Canada, August 2006.

[13] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08)*, pp. 1238–1246, April 2008.

[14] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04)*, pp. 29–37, Philadelphia, Pa, USA, October 2004.

[15] F. Picconi, N. Ravi, M. Gruteser, and L. Iftode, "Probabilistic validation of aggregated data in vehicular ad-hoc networks," in *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, pp. 76–85, Los Angeles, Calif, USA, 2006.

[16] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, pp. 67–75, Los Angeles, Calif, USA, 2006.

[17] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—a message plausibility problem," in *Proceedings of the 2nd IEEE Workshop on Automotive Networking and Applications (AutoNet '07)*, pp. 1–8, Washington, DC, USA, November 2007.

[18] G. F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 319–332, 2006.

[19] K. Fall and K. Varadhan, "The *ns*-2 manual," the VINT Project, April 2002, http://www.isi.edu/nsnam/ns/doc.

[20] A. Mahajan, N. Potnis, K. Gopalan, and A. I. A. Wang, "Evaluation of mobility models for vehicular ad-hoc network simulations," in *Proceedings of the IEEE International Workshop on Next Generation Wireless Networks (WoNGeN '06)*, Bangalore, India, December 2006.