Communication Requirements for Crash Avoidance

Jason J. Haas
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, Illinois, U.S.A.
jjhaas2@illinois.edu

Yih-Chun Hu
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, Illinois, U.S.A.
yihchun@illinois.edu

ABSTRACT

Safety applications are a driving force behind VANET deployment. Automobile manufacturers, government organizations, and consortia of the two have been investigating using VANETs for safety applications. Though VANETs are in large part designed for safety applications, researchers do not yet know the communication requirements of VANET safety messages. As a result, protocol designers have relied on generic network success metrics, such as packet delivery ratio, to evaluate their protocols. However, a more useful metric is the ability of currently proposed VANET schemes (e.g., for authentication, power control, etc.) to allow vehicles to receive safety messages and warn their drivers sufficiently in advance of an accident so that the driver can avoid the accident. Besides the basic safety message service, researchers have proposed other VANET mechanisms and services including mix zones [2, 5] and silent periods [18, 8, 17] to enhance vehicle privacy, intelligent transportation systems [24], and commercial applications [12]. However, these applications face a similar question: will a VANET be able to support these services and still achieve the safety goals for which the VANET was designed?

Previous attempts at answering the above questions have been made using small test beds without any collisions and using vehicle kinematics and message reception probabilities. However, each of these approaches lack the realism (i.e., actual crashes) and scale that VANETs will have. In this paper, we present our results from simulating two vehicular safety applications. We simulated crash scenarios and determined the probability that vehicles could avoid the crashes. Additionally, we measured the communication requirements needed for those probabilities.

Categories and Subject Descriptors

I.6.5 [**Simulation and Modeling**]: Model Development;
C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Experimentation, Performance, Reliability

VANET'10, September 24, 2010, Chicago, Illinois, USA.

Keywords

vehicular networks, VANET, safety, communication, simulation, metrics

1. INTRODUCTION

Safety applications are one of the driving forces behind the anticipated deployment of VANETs, due to their expected impact in reducing the loss of life and economic cost of vehicular accidents. Because of the relative importance of safety applications, researchers have studied the effects of various mechanisms such as authentication mechanisms [21, 7] and power control [23, 13] on VANET communication reliability. To address another key concern about the privacy of information broadcast in basic safety messages, researchers have proposed using privacy preserving mechanisms such as silent periods [18, 8, 17] and mix zones [2, 5]. Additionally, researchers have envisioned other services that would use VANETs. Such services could support intelligent transportation systems [24] or commercial applications such as advertisement dissemination [12]. All of these proposed mechanisms and services have an impact on the reliability of communication among vehicles in a VANET. For example, any protocol that adds additional overhead, or limits the rate or power with which a vehicle sends a basic safety message will impact the effectiveness of safety applications. Though previous work describes such mechanisms, often for safety messages, a critical question is, given any set of deployed mechanisms, how well will safety applications work?

Previous attempts at answering this question have relied on small-scale simulation, or test beds that do not use actual collisions. Additionally, there has been a decoupling of network performance measurement from safety application performance. In general, previous approaches for analyzing safety application communication requirements have lacked both realism and scale. However, due to the high cost of an extensive VANET test bed with moving vehicles and DSRC radios, an extensive large-scale evaluation of safety application communication requirements would be prohibitively expensive. Furthermore, to test such protocols in collision environments would be even more expensive and quite hazardous, since safety applications are designed to yield warnings only in actual emergency situations. Thus, triggering such an application would require putting a vehicle in a potentially hazardous situation.

In this work, we develop a simulation framework for analyzing the safety application communication requirements in a way that addresses the problems of both realism and scale. Specifically, we model intersection collision warning (ICW) and emergency brake warning (EBW) safety applications. We use an existing VANET simulator [7] to conduct simulations of vehicles on a large scale. In our simulations, we inject accidents at intersections into the traffic traces, model two safety applications, and model the responses

taken by drivers. We run our safety application simulations in various scenarios, and present our results. Our scenarios varied vehicles' transmission powers and authentication mechanisms, and contained different numbers of vehicles. Additionally, we show the communication requirements for predicting and (usually) preventing the injected collisions.

We organize the remainder of the paper as follows. In Section 2, we present related work, which we follow in Section 3 with an overview of how we approached the problem of analyzing safety application performance requirements. Next, we detail our simulation setup and experimental parameters in Section 4. We present our results in Section 5, and conclude in Section 6.

2. PREVIOUS WORK

Bai and Krishnan [1] provided field measurements of DSRC performance on freeways and an "open-field" test track, using these measurements to argue about the reliability of various safety applications. The authors developed an equation based upon the probability of correctly receiving a safety message at a specified distance (d),

$$P(\text{application success}, d) = 1 - (1 - P(\text{communication success}, d))^{\frac{T}{t}}$$

T is the window of time during which an application must receive a packet for it to function properly, and t is the period between safety messages. As a result of the authors' field tests, they observe that the probability of a packet drop seems to be independent from packet to packet, resulting in the formulation of the equation above. The authors assert values for T for a few safety applications, but do not provide evidence supporting their claims. They propose using the above equation, calling it the *T-window reliability*, as a metric for safety application reliability. However, the distance in this equation is static, while vehicles in crash situations are anything but.

Huang and Tan [10] also performed field tests, using two vehicles equipped with DSRC radios and DGPS receivers, and that used extended Kalman filters to estimate the other vehicle's trajectory in a collision scenario. The authors develop a mathematical framework for deciding when to present collision warnings to drivers based on the probabilities of collision, taking into account the statistics of sensor measurement errors. Using the data gathered from the sensors and their corresponding error statistics, the authors simulate potential collision scenarios, also making use of the data measured by Bai and Krishnan (which we described in the previous paragraph). The authors also include communication errors, i.e., packet drops, in their simulations. The authors conclude that under their setup broadcasting safety messages at 5 Hz with a packet delivery ratio of at least 0.5, their collision warning system is tolerant to communication losses and delays. The authors only use two vehicles in their simulations, and they make use of communication reliability data based on three vehicles. Additionally, the field test data that the authors use did not result in actual collisions. In another paper [22], the authors describe more of how they simulated various crash types (e.g., intersection violation).

Nekovee [15] developed a deterministic model for deciding if a vehicle collision would occur using vehicle kinematics, driver reaction time, and communication delay. The model applies to only rear-end collisions and only incorporates two vehicles, which initially travel at the same speed. Nekovee numerically evaluates the maximum allowed communication delay using an intelligent driver model based on traffic theory for various road conditions (i.e., coefficients of friction for icy, wet, muddy, and dry roads). In these equations, both drivers' strategies for avoiding the collision is to engage in maximum braking. In these evaluations, Nekovee models PHY-layer effects as a combination of deterministic two-ray path loss and log-normal fading. Instead of simulating MAC-layer effects, Nekovee simply models MAC-layer interference as an additional loss probability. The scope of these numerical evaluations do not include other crash scenarios, such as intersection violations or lane changes, and they do not encompass a realistic scenario where there could be many other vehicles.

Shladover [20] analyzed cooperative intersection collision avoidance systems (CICAS). He described three different intersections: rural, suburban, and urban. Each of these intersections had traffic that was progressively more dense, and correspondingly, Shladover concludes that the urban intersection scenario would result in the worst case communication requirements (i.e., most vehicles sending information resulting in higher channel congestion). He specifically notes that due to intersections being spaced closer together in the urban area, network traffic from one intersection competes with traffic from neighboring intersections. Shladover does not provide any analysis of communication latency for CICAS.

Numerous authors have proposed methods for congestion control [16, 9], with the goal of improving the reliability of VANET safety application communication. Specifically, Huang et al. [9] propose various distributed rate or congestion control algorithms. The authors investigate their proposals via simulation in a scenario consisting of a single, isolated freeway, presenting the estimation error of vehicles' estimators. In the authors' simulations, error can grow because of two sources: noisy measurements and stale information, the latter of which can be exacerbated by the rate control algorithms. While the authors present the statistics of these errors and simulate more vehicles than the previous work we discussed above, they do not relate their errors to safety application performance (e.g., collisions avoided).

Yin et al. [25] provide early simulation results measuring the latency and throughput of VANET safety messages. The authors take a network-centric point of view and do not simulate actual safety applications.

3. OUR APPROACH

Our approach is distinct from the prior work because we inject actual accident scenarios into traces, simulate the impact of collision-inducing mobility on network traffic, and we consider scenarios that include a large number of vehicles, not just the vehicles involved in the accident. To provide results with more vehicles, we used an existing VANET simulator [7] to conduct simulations of vehicles on a large scale, injecting accidents into traffic traces. Performing large-scale simulations including accidents has significant advantages over or provides enhancements to the previous work in this area. Simulation allows us to evaluate the reliability of communication at varying distances rather than at a static distance. Because the simulator we used accurately models MAC-layer effects, our work has added realism which previous work did not have. Due to the large-scale nature of the simulations we performed, we can more accurately evaluate the impact of interference and network congestion on the communications of the vehicles involved in accidents.

Through simulation we investigated the reliability requirements of VANET communication in various scenarios. Specifically, we implemented two safety applications and simulated their performance. Our techniques can be expanded to evaluate how various road conditions, traffic densities, driver reaction times, and maximum braking decelerations impact the effectiveness of VANET safety applications. Thus, our work provides a framework for auto

manufacturers, government agencies, and researchers alike to evaluate communication options and their effects on safety applications. Additionally, we use this framework to evaluate an implementation of two safety applications to show their communication requirements.

Collision Modeling Summary.

Because our approach provides a methodology for mapping network performance to application performance, our results will shed light on many other results published in the VANET community. Specifically, we can determine whether the results of the network and application layer performance measurements from earlier work show that VANETs in such scenarios will reliably support safety applications [21, 7].

Additionally, this work provides a baseline for evaluating the effects of other VANET mechanisms and protocols on safety applications, such as mix-zones and silent periods, power control algorithms, or congestion control algorithms. Since most current research on VANETs merely measures network-specific performance metrics, researchers often do not know the extent to which safety applications are impacted. Furthermore, without a guarantee of effectiveness, governments and manufacturers deploying VANETs may be hesitant to deploy a system, or may choose one that does not function as intended at full market penetration.

4. METHODOLOGY

In this section, we introduce our methodology for carrying out our evaluation via simulation. We also describe how we implemented our ICW and EBW safety applications in the simulator. The following structure outlines the methods we used to analyze safety application communication requirements.

- Analyzed recordings of actual crashes, observing vehicles traveling with constant velocities (no deceleration)
- Obtained SUMO traces on a city grid map using randomized vehicle traffic flows that start and end at peripheral road spurs
- Converted SUMO output to simulator input, removing all potential collisions
- Verified no collision warnings from collision-free data (no false positives)
- Inserted collisions into trace data
- Simulated collision traces and measured results

4.1 Crash Data Analysis

We began our work by observing driver behavior in data from actual roadway crashes. This data was obtained from video recordings of an intersection in Louisville, Kentucky.[1] An analyzed version of this information is freely available online, though only a small subset of the number of collisions recorded is available.[2] The main observation that we made concerning this data was that the involved vehicles maintained a constant velocity right up to the time of collision. This behavior tells us that the involved drivers were completely unaware of the impending crash beforehand. Furthermore, this obliviousness validates the intended goal of safety applications such as ICW that being the ability to restore a driver's attention to the road. Consequently, we modeled our driver behavior in the collisions we generated based on this behavior. In other words, in our injected collisions, the involved drivers maintain a constant velocity.

[1]See `http://www.e-archives.ky.gov/pubs/transportation/tc_rpt/ktc_05_09_spr_277_03_1f.pdf`.

[2]See `http://path.berkeley.edu/~zuwhan/ztracker/index.html`.

4.2 Crash-Free Scenarios

Trace Sources.

There are a number of sources for realistic vehicle traces that are freely available online and that have been used in previous VANET simulations [7, 14]. However, these traces are unusable for our purposes of simulating safety applications because these traces do not respect the physical extents of vehicles; that is, these traces run vehicles on top of each other. Thus, these traces do not allow for control experiments and injecting specific modes and restrictions on collisions. Additionally, these data sets consist of only a small number of traces, which prevents us from being able to sufficiently vary traffic density and physical network size. Consequently, we turned to using traces generated by traffic simulators.

We evaluated both VanetMobiSim [6] and SUMO [11] traffic simulators. We eliminated the former because it exhibited the same faults (i.e., vehicles being run on top of each other) as the realistic vehicle traces. SUMO also exhibited some of this behavior of not respecting the physical extents of vehicles, though to a lesser degree. Thus, we chose SUMO to generate our crash-free scenarios.

Trace Generation.

We used SUMO to generate an urban layout of roads placed on a grid, as we show in Figure 1. Each block was approximately 150 meters long, each road consisted of 2 lanes in each direction, and each intersection was controlled by a traffic light. To generate traffic, we specified traffic flows. We randomly chose the starting and ending location that specified each flow, and each of these locations was chosen to be on at a peripheral road spur of the grid. (Road spurs are the sections of road connected to only one intersection at the peripheral of our simulation area.) We then used SUMO to route the traffic and generate vehicle traces.

Next, we converted the SUMO trace output to the format of our simulator. To do this, we interpolated vehicle positions at a granularity of 0.1 seconds. In our interpolation, we forced vehicles to have a constant acceleration between the starting and ending points of the interpolation.

To eliminate any undesired crashes from our initial traces, we removed all vehicles that came within 3 meters of each other. We found this to largely occur as a result of simultaneous left-hand turns. Two vehicles making left-hand turns from opposite directions frequently resulted in collisions because SUMO placed the connecting segments of road (on which the left turns were performed) too close to each other for these vehicles to perform this operation simultaneously. Since the vehicles simply appear on the roadway, they may collide with vehicles already traveling on the roadway. Thus, we added the road spurs as safe areas for vehicles to enter and exit the simulation area, that is, where they will not unintentionally collide with other vehicles.

4.3 Collision Injection

To inject collisions of the desired type (i.e., intersection collisions) into our traffic traces, we modified vehicle behavior in the generated traces, subject to certain criteria. Specifically, we required colliding vehicles to collide at a minimum angle of 30°, and

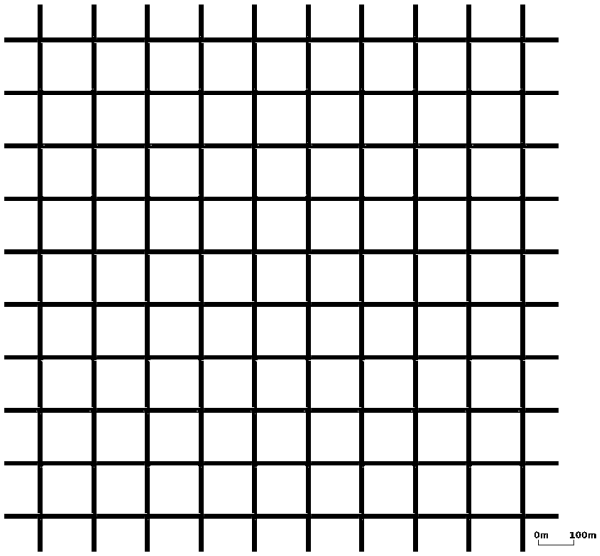


Figure 1: Urban simulation area

traveling with a minimum speed of 7 m/s. We chose these criteria because we wanted to ensure collisions occurred at intersections and were representative of more severe collisions, respectively.

After a collision, the involved vehicles simply stop. All of the other vehicles continue to move normally after a crash. We did not modify the movements of other vehicles in the traces we generated during or after a collision in order to investigate possible pile-up results of vehicles braking. Vehicles can and do change their trajectories during and after a collision, which we will discuss in further detail when we discuss follow-on collision avoidance and our EBW implementation in Sections 4.7 and 4.8 below.

4.4 Crash Simulation

We used the traces with our injected crashes in our simulations evaluating safety application communication requirements. We implemented an ICW safety application in the Illinois VANET simulator [7]. We simulated vehicles sending timestamped safety messages containing the source vehicle's position, velocity, and acceleration, sent at a rate of 10 Hz. Vehicles tracked other surrounding vehicles within a range of 100 meters. Our ICW safety application used vehicle dynamics to predict when a potential collision would occur. The intended output of our ICW application was presenting a warning to the vehicle's driver. In order to reduce false positives, the ICW application only alerts the driver after the vehicle predicts a collision two consecutive times. We will detail our ICW safety application implementation in Section 4.7 below. We chose to implement the ICW application because that was the only accident situation for which we had actual data (i.e., the video recordings from Louisville, Kentucky), and on which we could base our accident injection.

4.5 Vehicle Parameterization

In order to conduct our simulations, we needed to parameterize various vehicle properties, such as, the maximum possible deceleration and driver reaction time. Table 1 shows a summary of the parameters we set and the values of each that we used. We obtained many of these parameters from previous work.

We chose our coefficient of friction based on work done at the U.S. National Highway Traffic Safety Administration (NHTSA) [19]. We chose to use the minimum measured dry pavement coefficient of friction. Due to how we generated our vehicle traces using SUMO, we needed a coefficient of friction this high so that the dynamics of vehicles generated by SUMO were possible, i.e., so that under normal circumstances, without any injected collisions, normal vehicle decelerations were below the maximum braking deceleration.

Table 1: Simulation vehicle parameters

Parameter	Setting
Simulation duration	1000 seconds
Crash-free period	300 seconds
Warm-up period	30 seconds
Number of flows	5, 10, 15, 20
Number of vehicles per flow	40, 80
Coefficient of friction	0.89
Driver reaction time	0.5 seconds
Transmission power	0, 10 dBm
Authentication mechanism	ECDSA, TESLA

Consiglio et al. emulated a driving environment for test subjects, measuring their reaction time with different distractions [4]. Specifically, they measured the time required to respond to a visual stimulus and begin braking. We use a single value upper bound from their work, rounded to the nearest 0.1 seconds.

4.6 Network Parameters

We specified a warm up period of 30 seconds before we started gathering network statistics. All simulations were 1000 seconds long. We varied vehicles' transmission power settings across simulations; that is, within a simulation all vehicles used 0 dBm or all vehicles used 10 dBm for their transmission power. In all of our simulations, we used either TESLA with attached key releases or ECDSA for the authentication mechanism (as was developed in previous work [7]). This variant of TESLA has a minimum 100 ms latency to verify a packet, whereas the verification delay for ECDSA is essentially 0 since the network density is low enough to not result in significant delay due to computation. Consequently, we wanted to investigate whether TESLA's minimum delay would impair the ICW safety application. We simulated vehicles using a Core 2 processor for performing verifications, as was used in previous work [7]. We used a Nakagami fading model parameterized based on previous channel measurements [3]. For each setting (i.e., number of vehicle flows, number of vehicles per flow, transmission power, authentication mechanism), we ran approximately 200 simulations, each with different randomly chosen vehicle flows and different collisions.

4.7 ICW Safety Application Implementation

In order to test the ICW safety application, we needed to implement it in our simulator, the details of which are as follows. Vehicles kept a path history of other vehicles from which they received packets. We used a history of 5 packets. Vehicles also kept a projection of the future trajectory of these vehicles based on a constant-acceleration model (i.e., the tracked vehicle continues with the accelerations it broadcast in its last received safety beacon). If vehicles were within 2.75 meters of each other at some point along their projected trajectories, then a collision is possible.

To reduce the false positives generated from our detection algorithm, we implemented the following restrictions in identifying potential collisions. If the speed of an involved vehicle at the time of collision was less than 7 m/s (15.7 mph), we considered the ve-

hicle to be going slow enough to not warn the driver. We limited the speed in this way because vehicles traveling this slowly are able to make course changes (i.e., turn) easily, which they may be in the process of doing. Additionally, at such low speeds, drivers will have longer amounts of time to observe other vehicles that might cause collisions. Next, if the involved vehicles were already decelerating at at least 0.5 m/s^2, then we considered those drivers already aware of an approaching intersection, and so we did not warn the driver in this case. Additionally, we wanted to eliminate false positives resulting from both turning and lane changing. To do this, we calculated the rate of change of the angle of vehicles' headings across vehicles' path histories. If this rate of change was larger than 1.4 degrees/s, we considered the vehicle to be initiating a lane change or a turn. Additionally, if the angle of collision was less than 30 degrees, we considered the vehicle to be changing lanes and that it will not result in an intersection collision. Finally, we required the following two criteria hold before warning the driver. First, the driver must not be able to stop without maximum braking if the driver begins maximum braking within 0.6 seconds (a driver reaction time of 0.5 seconds plus 0.1 seconds of safety margin). Second, two possible warnings (as fits the above criteria so far) must be detected at least 0.1 seconds apart (the time period of safety beacons). If all the above criteria were satisfied, then we warned the driver, and after the duration of a driver reaction time, the driver initiated maximum braking to avoid the collision. When the driver initiated maximum braking, we set a flag in packets transmitted from that vehicle so that safety beacon packets will warn other drivers that the initiating driver is emergency braking.

We tuned the above parameters to minimize the occurrance of false positives resulting from our simulations of our base vehicle traces before any collisions were injected. In an actual ICW safety application implementation, vehicles might additionally use map information or other on-board sensor information, which could additionally be shared in safety beacons, such as steering wheel angle. These additional data sources could be used in addition to or as a replacement for some of the above criteria that we used. We leave the use of such data sources, further refinement of application-specific criteria, and other safety applications for future work. We consider it necessary that we simulated an ICW safety application with few false positives because the total hours of simulated vehicle driving is many orders of magnitude less than the number of hours actual vehicles drive daily. Additionally, false positives represent a significant hinderance to the effectiveness of VANET safety applications. Specifically, the more false positives that are presented to users, the more likely it is that the users will ignore the safety system that presented the erroneous warning. Thus, the safety system will result in reduced effectiveness.

4.8 Follow-On Collision Avoidance

Due to space and time constraints, we did not fully implement an Emergency Brake Warning (EBW) safety application, which we leave for future work, as we mentioned above. However, to analyze the possibility of follow-on crashes or pile-ups, we implemented a basic version of the EBW safety application. In our implementation, drivers who receive an EBW (from a safety beacon packet containing this flag being set) also engage in maximum braking after the duration of a driver reaction time. We consider this a possible driver reaction to seeing a warning presented by the vehicle, that is a "knee-jerk" type reaction. We then measured whether there were follow-on crashes (i.e., a pile-up) up to 30 seconds after the initial issued warning. We consider pile-up collisions occurring later than this time horizon to not be sufficiently realistic since we are not modeling attentive drivers that could visually observe brake lights.

5. RESULTS

We now present the results of our simulations. Specifically, we will show safety application performance, crash mitigation, communication requirements, and false postive rates.

5.1 Intersection Crash Avoidance

Figure 2 shows the probabilities that a vehicle can avoid our injected collisions for the two transmission powers and authentication mechanisms we simulated, and for the different traffic flows and effective densities. For each vehicle flow setting (x-axis), we show the probabilities (y-axis) for each authentication mechanism and transmission power setting we simulated. The error bars show the 95% confidence intervals.

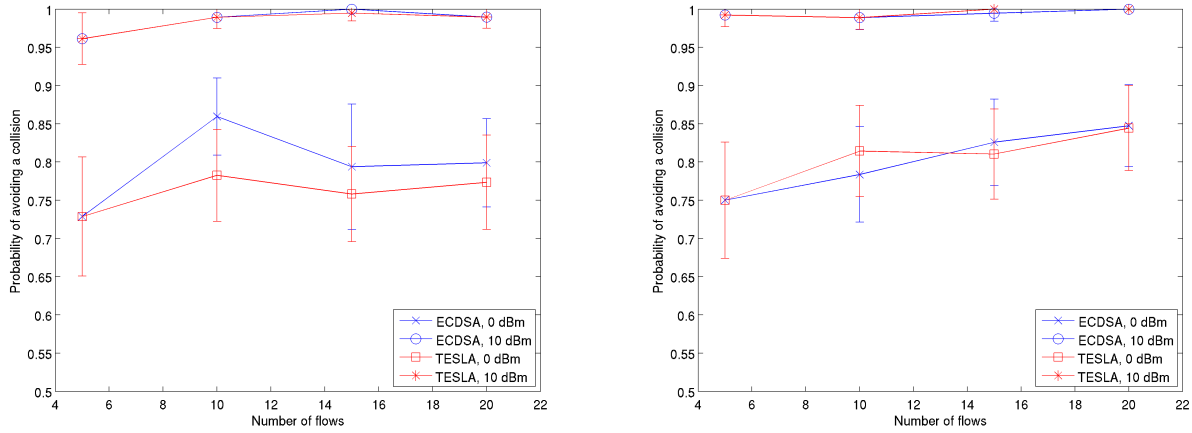
Both of these figures show that decreasing transmission power from 10 dBm to 0 dBm results in a lower probability of avoiding a collision, that is, being able to predict the collision and warn the driver sufficiently far in advance of a potential collision. The probability that the initial collision is avoided does not degrade with more vehicle traffic for the range of settings we explored. On the contrary, with increasing vehicle traffic density, the reliability of the ICW safety application appears to increase at the lower, 0 dBm transmission power setting, though it still results in fewer collisions being avoided compared to 10 dBm. However, across all simulated scenarios, a significant fraction of collisions due to otherwise oblivious drivers can be eliminated. For all the tested number of flows with 40 vehicles per flow, using 10 dBm transmission power with either authentication mechanism results in at least 96% of intersection collisions being avoided. For 80 vehicles per flow, the fraction of avoided collisions increases to 99%.

No setting we simulated shows a statistically significant difference between the performance of ECDSA and TESLA in terms of avoiding collisions at intersections. However, we will show results below when we discuss false positives that do indicate a difference between these two authentication mechanisms.

5.2 Pile-up Collision Avoidance

Figure 3 shows the probabilities for safety application warnings being presented to drivers (either from our ICW implementation or from warnings issued by other braking vehicles) and drivers avoiding pile-up crashes after an initial crash for the same scenarios as in Figure 2. For each vehicle flow setting (x-axis), we show the probabilities (y-axis) for each authentication mechanism and transmission power setting we simulated. The error bars show the 95% confidence intervals. For some of the collisions in our results no warnings were presented to the involved drivers, and so their vehicles did not decelerate. Because these simulations resulted in drivers not being warned and the collision not being avoided, we did not consider any resulting pile-ups from these simulation runs.

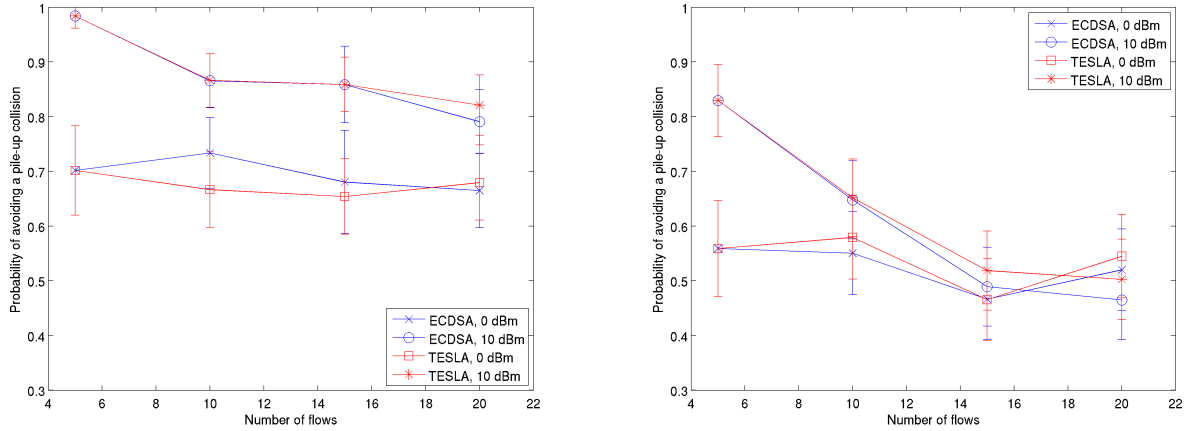
Figure 3 shows different trends for the different transmission powers as vehicle density increases. As the vehicle traffic density increases, the probability that all post-collision pile-up type accidents are avoided decreases noticeably for 10 dBm transmission power. For all vehicle density settings with 40 vehicles per flow except 20 flows, the probability of avoiding a pile-up collision decreases with increasing vehicle traffic density. With 20 flows and 80 vehicles per flow, 0 dBm transmission power results in more pile-up collisions being avoided. This is likely to occur because of the higher vehicle traffic density resulting in a more well-connected network and consequently a quicker response to EBWs. Addition-



(a) 40 vehicles per flow

(b) 80 vehicles per flow

Figure 2: Probability of crash avoidance in our ICW safety application for all simulated vehicle density settings.



(a) 40 vehicles per flow

(b) 80 vehicles per flow

Figure 3: Probability of post-collision pile-up avoidance in our EBW and ICW safety applications for all simulated vehicle density settings.

ally, 10 dBm transmission power results in more congestion than 0 dBm.

While the trends of degrading performance in terms of avoiding pile-up collisions as vehicle density increases reflects increased network congestion, the trend in an actual deployment scenario is not likely to be as steep. Since we simulated drivers relying on only warning messages to initiate braking to avoid a pile-up accident, we omitted other significant accident-avoidance mechanisms, such as drivers reacting to seeing tail lights or being able to swerve to avoid an accident.

5.3 Message Reception Times and Distances

Figure 4 shows the cumulative distribution functions (CDF) for message reception time and distance of the last message received before a warning was issued to a driver for the simulations that resulted in the collision being predicted, using each transmission power we simulated, and using either ECDSA or TESLA for authentication. The message times shown are relative to when the warning was presented to the driver for the scenarios (i.e., how long before the warning the last message was received). The message distances are the distance between sender and receiver at the time of transmission. We only show the most dense traffic settings from our simulations since the results were not significantly different across our various traffic density settings. Some CDFs in Figure 4 do not reach 1 because some simulations resulted in false negatives (i.e., the injected collision not being predicted), thus, there is no time or distance at which the message prior to the warning was received.

Figure 4 shows that 10 dBm transmission power results in almost all messages using TESLA authentication being delivered between 0.1 and 0.2 seconds before the collision was predicted and the driver warned. No message is delivered less than 0.1 seconds before the warning was issued because we simulated using TESLA with attached key releases. Releasing keys attached to the following safety message implies that the minimum verification latency for verifying a packet is 0.1 seconds. The lower transmission power of 0 dBm results in packets being received with less reliability, and thus a receiving vehicle must use information from older packets to predict a collision. We expect that scenarios with more road

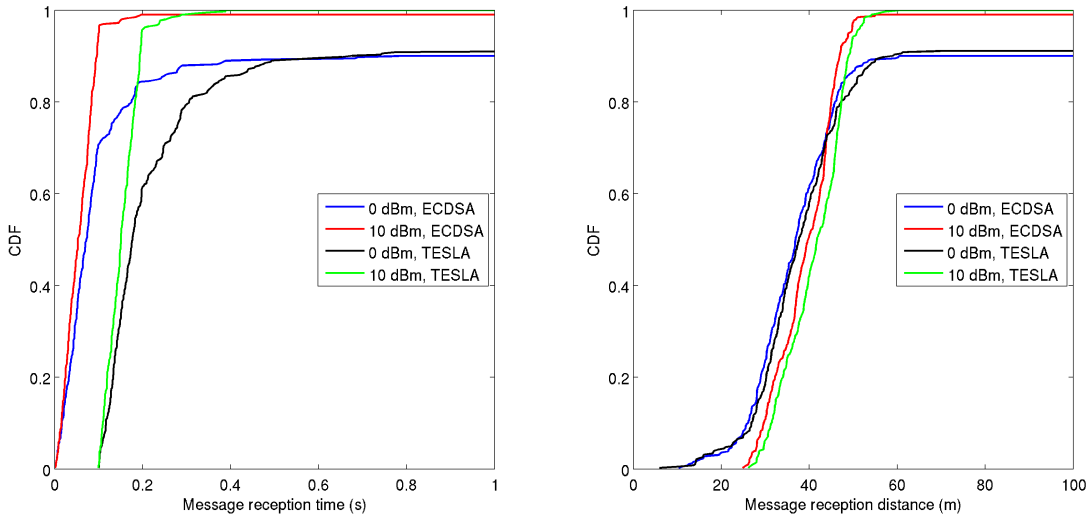


Figure 4: CDF of the time relative to when the warning was presented to the driver and the distance the last message was received from the other vehicle involved in the collision, using 20 flows and 80 vehicles per flow, for each simulated transmission power and authentication mechanism.

traffic (more flows) may result in a reversal of roles between the two transmission powers. In other words, with more congested roadways, there will be more loss due to interference at the higher power setting, which may result in fewer packets being received from a potentially-colliding vehicle and so packets that are more stale will be used in predicting a collision.

Figure 4 shows that using ECDSA for authentication resulted in the safety messages that are used to predict collisions being received less distant from the time the warnings were issued (smaller message reception times) and with less distance between the involved vehicles (shorter distances) compared to using TESLA for authentication. This is intuitive because in the scenarios we simulated, there is effectively no verification delay using ECDSA for authentication, whereas messages authenticated with TESLA are delayed for verification at least by 0.1 seconds, and thus, older messages must be used to predict collisions, if warnings are issued at the same time independent of authentication mechanism.

Additionally, Figure 4 shows that almost all messages that are used to predict potential collisions are received within a window of 20-60 meters. Thus, this range is the window of distances in which network performance most directly relates to safety application performance (at least for the safety applications we present here).

5.4 Vehicle Speed Investigation

Figure 5 shows the vehicle final speeds at the time of collision in meters per second and the speed reduction as a result of drivers reacting to provided warnings in meters per second for 20 flows and 80 vehicles per flow. We omit the corresponding figures for our other vehicle traffic density settings since they are extremely similar to the one we show in Figure 5. In this figure, we show the CDF of the final vehicle velocity and the complimentary cumulative distribution function (CCDF) of vehicles' reduction in speed. Figure 5 does not have any data for 10 dBm transmission power because the collisions that resulted with this power setting came from false negatives; that is, the collision is not detected, and as such exhibited no reduction in speed. This absence was largely the case across all of our vehicle density settings. The plot of the reduction in speed for vehicles in Figure 5 shows that most vehicles that do not avoid the intersection collision but do predict it can reduce their speed by at least 5 m/s. Thus, the severity of the crash can be significantly mitigated, even in the case where the crash is not avoided.

5.5 Network Performance Comparison

Figure 6 shows the fraction of packets successfully received at the network layer versus distance for our least dense and most dense vehicle traffic settings, using each transmission power and each authentication mechanism. Additionally, we included data from simulating the 8:45 am trace of Lankershim Boulevard, which we have previously used [7]. We included this trace to provide a map between network performance using real-world trace data and synthetic trace data. We re-simulated the Lankershim Boulevard traffic using parameters for the Nakagami fading model based on previous work [3]. We have omitted error bars in these figures for the purpose of improving figure clarity. The data series from Lankershim Boulevard are labeled as "Lank" in these figures. The data for ECDSA and TESLA using 5 flows, 40 vehicles per flow (Figure 6(a)) significantly overlap and thus are almost indistinguishable in the graph.

Comparing the two traffic density settings, there is a reversal of network performance beyond a certain distance between 0 dBm and 10 dBm transmission power. That is, as vehicle traffic density increases and beyond some *cross-over distance*, the probability that a packet is successfully received is higher for 0 dBm than for 10 dBm, which was not the case with lighter vehicle traffic. Previously, we noted that for any combination of settings, the safety message that triggers or is used to trigger a warning almost always is transmitted from a distance of approximately 20 to 60 meters. Additionally, above we observed that 10 dBm transmission power always results in the intersection collision being avoided with higher probability than with 0 dBm. Because these cross-over distances are beyond the range within which vehicles receive almost all of the messages they use to predict a collision and finally warn their drivers, the application layer performance (i.e., avoiding collisions)

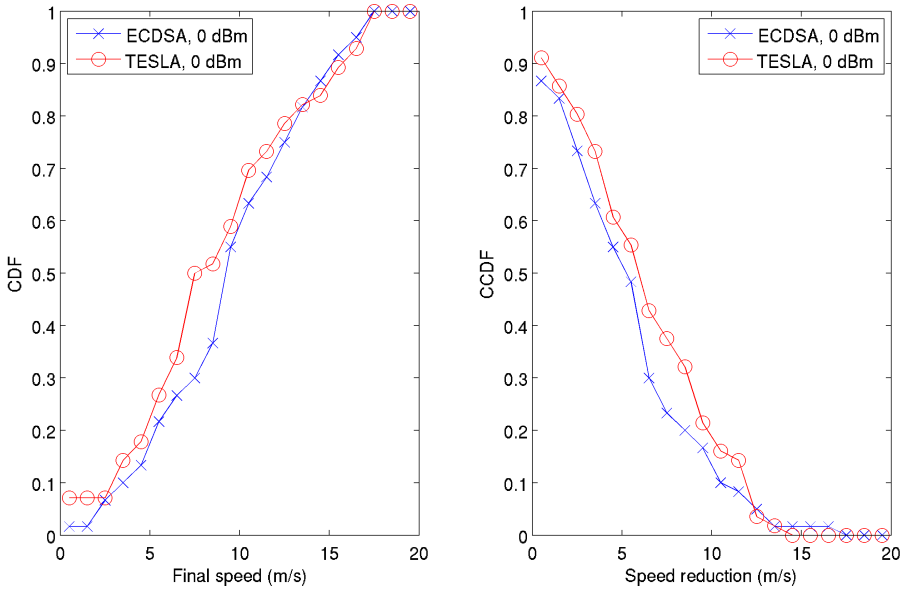


Figure 5: Crashed vehicle speed in our simulated ICW safety application for 20 vehicle flows and 80 vehicles per flow.

is lower for 0 dBm compared to 10 dBm. For the two traffic density settings we present here, the cross-over distances were 165 meters and 100 meters for 5 flows, 40 vehicles per flow and 20 flows, 80 vehicles per flow, respectively.

Figure 6(a) shows that our lightest density setting (i.e., 5 flows, 40 vehicles per flow) is far less dense and results in a far less congested network compared to that predicted by the Lankershim data set. Contrastingly, Figure 6(b) shows that our heaviest density setting (i.e., 20 flows, 80 vehicles per flow) results in a more congested network compared to that predicted by the Lankershim data set. However, upon visual comparison between our most dense setting and Lankershim, we observed far different densities. The Lankershim trace is very limited in extent (i.e., about 490 meters long with light cross traffic), but vehicles are more densely packed than in our densest traces. On the other hand, our densest traces consist of more vehicles, but the vehicles are spread across a larger area. Thus, the network congestion is worse in our densest trace but does not yet represent a worst-case scenario, and also may not yet represent a common rush hour scenario. Furthermore, comparing previous results using congested freeway data [7], we observe that even Lankershim does not represent the most dense vehicle traffic that exitsts. Consequently, we expect that further increasing the vehicle traffic density is both reasonable and to be expected in the real world. Thus, the cross-over distance between two transmission powers, as we have seen with 0 dBm and 10 dBm transmission power, is likely to continue to move to shorter distances.

5.6 False Positives

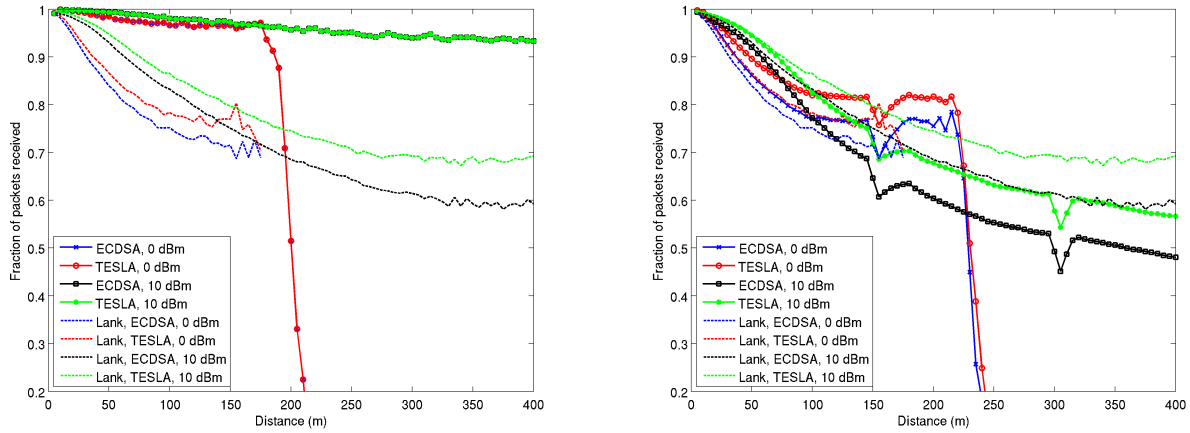
Despite the additional detection criteria, we did not eliminate all false positives from our simulations. False positives still occurred, though only in a small fraction of our simulations. Figure 7 shows the fraction of simulations that resulted in false positives. The error bars show the 95% confidence intervals. This data shows that in many scenarios, TESLA results in more false positives than ECDSA, though the observed probabilities are within error bars of each other. Upon further investigation, we found that these false positives generally result from a vehicle not receiving a fresh packet from a vehicle, which would have indicated the transmitting vehicle is slowing down as it approaches an intersection, while the stale packet does not indicate the transmitting vehicle is at all slowing down.

Thus, the latency of TESLA can result in more false positives than using ECDSA, in the safety applications as we implemented them and using the traces we used. The rate at which false positives occur due to TESLA's minimum latency of 0.1 seconds may or may not accurately reflect real-world performance. The rate at which drivers decelerate in the initial traces is controlled by a parameter set in SUMO. However, the resulting deceleration profile may not accurately reflect actual drivers. Further study to match the generated SUMO driving profiles to actual driver deceleration profiles might result in less of a difference between ECDSA and TESLA in terms of the rate of false positives.

To put the data shown in Figure 7 in a broader context, we calculated the total number of vehicle-hours we simulated. We simulated 92,700 hours of vehicle operation. During this time, using ECDSA resulted in 19 false positives and, using TESLA resulted in 34 false positives. Thus, the mean time between false positives for ECDSA and TESLA were 4900 and 2700 hours of operation, respectively.

6. CONCLUSIONS

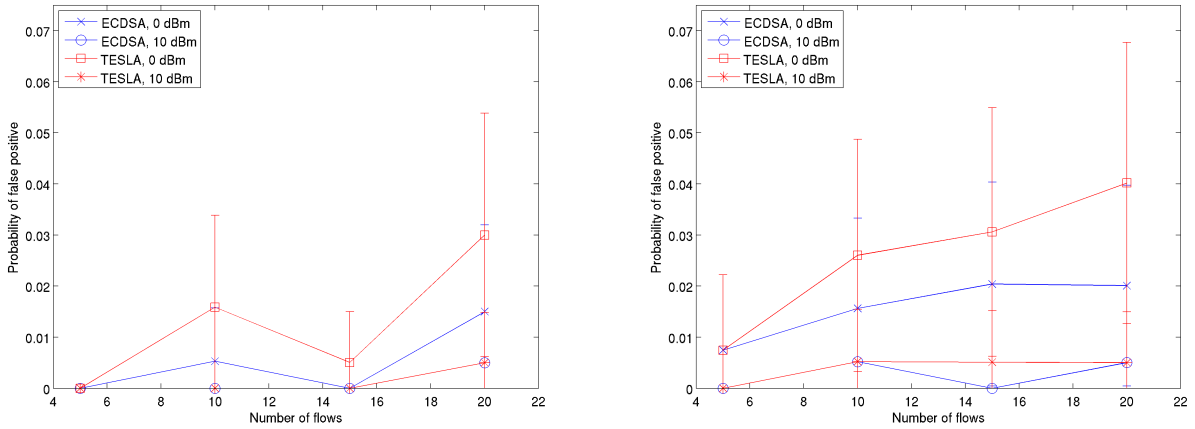
In this paper, we proposed a simulation framework for evaluating VANET safety applications and the corresponding settings of their constituent components (e.g., transmission power, authentication mechanism). Using this framework, we analyzed the ability of an intersection collision warning (ICW) safety application to successfully warn drivers sufficiently in advance of a potential collision so that the involved driver can stop. Our results show that for the light vehicle traffic situations we simulated, a large fraction of intersection collisions between unaware drivers could be avoided by employing VANET ICW safety applications. Additionally, even in collisions that were detected by our ICW application but were not avoided, the resulting damage was significantly mitigated as



(a) 5 flows, 40 vehicles per flow

(b) 20 flows, 80 vehicles per flow

Figure 6: Fraction of network layer packets received versus distance for various vehicle densities and Lankershim Boulevard.



(a) 40 vehicles per flow

(b) 80 vehicles per flow

Figure 7: Probability of a false positive in our simulated ICW safety application for all simulated vehicle traffic density settings.

the involved vehicles' speeds were significantly reduced by their drivers reacting to our simulated warnings before the actual collision occurred. We analyzed and presented the communication requirements for our ICW implementation, comparing our results to previous results and real traffic densities. Finally, we investigated the rate at which false positives occur in our implemented ICW safety application. We found that the additional latency of TESLA (compared to ECDSA) resulted in an increased false positive rate due to stale packets not indicating attentive driver behavior.

As we mentioned in Section 4, additional sources of information that were unavailable to us or that we did not make use of (e.g., steering wheel angle, or map data) could also be used in deployed instances of ICW safety applications. Using these data sources may also lead to collisions being predicted earlier and a higher fraction of accidents being avoided.

Having constructed the framework that we used in this paper, we believe that our framework will allow automobile manufacturers or government agencies to evaluate safety applications in a low cost and accurate manner in the future. Our simulation framework directly answers questions regarding whether specific mechanisms, protocols, or settings will result in sufficiently reliable communication to support safety applications.

7. REFERENCES

[1] Fan Bai and H. Krishnan. Reliability analysis of DSRC wireless communication for vehicle safety applications. In *Intelligent Transportation Systems Conference, 2006. ITSC '06. IEEE*, pages 355–362, Sept. 2006.

[2] Alastair R. Beresford and Frank Stajano. Mix zones: User privacy in location-aware services. In *PERCOMW '04: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, page 127, Washington, DC, USA, 2004. IEEE Computer Society.

[3] Lin Cheng, B.E. Henty, D.D. Stancil, Fan Bai, and P. Mudalige. Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band. *IEEE Journal on Selected Areas in Communications*, 25(8):1501–1516, October 2007.

[4] William Consiglio, Peter Driscoll, Matthew Witte, and William P. Berg. Effect of cellular telephone conversations and other potential interference on reaction time in a braking response. *Accident Analysis & Prevention*, 35(4):495 – 500, 2003.

[5] Julien Feudiger, Maxim Raya, Márk Félegyházi, Pano Papadimitratos, and Jean-Pierre Hubaux. Mix-Zones for Location Privacy in Vehicular Networks. In *WiN-ITS 2007*, August 2007.

[6] M. Fiore, J. Harri, F. Filali, and C. Bonnet. Vehicular mobility simulation for VANETs. *Simulation Symposium, 2007. ANSS '07. 40th Annual*, pages 301–309, March 2007.

[7] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. Real-world VANET security protocol performance. In *Proceedings of the IEEE Globecom 2009, Symposium on Selected Areas in Communications*. IEEE, December 2009.

[8] Y. Hu and H. J. Wang. A framework for location privacy in wireless networks. Bejing, China, April 2005. ACM.

[9] Ching-Ling Huang, Yaser P. Fallah, Raja Sengupta, and Hariharan Krishnan. Information dissemination control for cooperative active safety applications in vehicular ad-hoc networks. In *GLOBECOM'09: Proceedings of the 28th IEEE conference on Global Telecommunications*, pages 4085–4090, Piscataway, NJ, USA, 2009. IEEE Press.

[10] Jihua Huang and Han-Shue Tan. Impact of communication reliability on a cooperative collision warning system. In *Intelligent Transportation Systems Conference, 2007. ITSC 2007. IEEE*, pages 355–360, Sep. 30-Oct. 3 2007.

[11] Daniel Krajzewicz, Georg Hertkorn, C. RÃűssel, and Peter Wagner. SUMO (Simulation of Urban MObility) - an open-source traffic simulation. 2002.

[12] Suk-Bok Lee, Gabriel Pan, Joon-Sang Park, Mario Gerla, and Songwu Lu. Secure incentives for commercial ad dissemination in vehicular networks. In *MobiHoc 2007*, pages 150–159, Montréal, Québec, Canada, September 2007.

[13] Jens Mittag, Felix Schmidt-Eisenlohr, Moritz Killat, Jérôme Härri, and Hannes Hartenstein. Analysis and design of effective and low-overhead transmission power control for VANETs. In *VANET '08: Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, pages 39–48, New York, NY, USA, 2008. ACM.

[14] Valery Naumov, Rainer Baumann, and Thomas Gross. An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. In *MobiHoc '06: Proceedings of the 7th ACM International Symposium on Mobile ad hoc Networking and Computing*, pages 108–119, New York, NY, USA, 2006. ACM.

[15] M. Nekovee. Quantifying performance requirements of vehicle-to-vehicle communication protocols for rear-end collision avoidance. In *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, pages 1–5, April 2009.

[16] C. L. Robinson, L. Caminiti, D. Caveney, and K. Laberteaux. Efficient coordination and transmission of data for cooperative vehicular safety applications. In *VANET '06: Proceedings of the Third International Workshop on Vehicular ad hoc Networks*, pages 10–19, New York, NY, USA, 2006. ACM.

[17] K. Sampigethaya, Mingyan Li, Leping Huang, and R. Poovendran. AMOEBA: Robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589, Oct. 2007.

[18] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. *Proceedings of the 3rd Annual Conference on Embedded Security in Cars (escar 2005)*, November 2005.

[19] Gregory A. Schultz and Michael J. Babinchak. Consumer braking information initiative–methodology study phase i (accessed april 2010). Technical Report ATC-8170, National Highway Traffic Safety Administration (NHTSA) – Aberdeen Test Center, Fall 1998.

[20] Steven E. Shladover. Effects of traffic density on communication requirements for cooperative intersection collision avoidance systems (CICAS). Technical Report UCB-ITS-PWP-2005-1, Institute of Transportation Studies, University of California, Berkeley, March 2005.

[21] Ahren Studer, Fan Bai, Bhargav Bellur, and Adrian Perrig. Flexible, extensible, and efficient VANET authentication. *Proceedings of the 6th Annual Conference on Embedded Security in Cars (escar 2008)*, November 2008.

[22] H.-S. Tan and Jihua Huang. DGPS-based vehicle-to-vehicle cooperative collision warning: Engineering feasibility viewpoints. *IEEE Transactions on Intelligent Transportation Systems*, 7(4):415–428, December 2006.

[23] M. Torrent-Moreno, P. Santi, and H. Hartenstein. Distributed fair transmit power adjustment for vehicular ad hoc networks. *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, 2:479–488, Sept. 2006.

[24] Yi Yang and Rajive Bagrodia. Evaluation of VANET-based advanced intelligent transportation systems. In *VANET '09: Proceedings of the Sixth ACM International Workshop on VehiculAr InterNETworking*, pages 3–12, New York, NY, USA, 2009. ACM.

[25] Jijun Yin, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In *VANET '04: Proceedings of the First ACM International Workshop on Vehicular ad hoc Networks*, pages 1–9, New York, NY, USA, 2004. ACM.