Effect on Vehicle Safety of Nonexistent or Silenced Basic Safety Messages

George P. Corser, *Member, IEEE,* Alejandro Arenas, Huirong Fu, *Member, IEEE*

***Abstract*—In future vehicular ad-hoc networks (VANETs), Basic Safety Messages (BSMs) would be transmitted by all vehicles every 100ms in order to help prevent inter-vehicle crashes. At first not all vehicles would contain the hardware and software necessary to transmit BSMs; there would be an interval when only a percentage of vehicles would transmit. Further, even after all vehicles install the equipment, some privacy researchers recommend silent periods, spans of time during which vehicles deliberately cease transmissions. This is because BSMs may expose vehicle locations to wireless surveillance, and silent periods could thwart eavesdroppers. Whether due to lack of equipment or due to privacy protocols, silent periods would defeat safety provided by BSMs. This paper quantifies this tradeoff, presenting the Safety-Silence Tradeoff Equation, and showing an inverse exponential relationship between the proportion of vehicles transmitting BSMs and the proportion of potential collisions between vehicles unprotected by BSMs.**

***Index Terms*—dedicated short range communications, DSRC, vehicular ad-hoc network, VANET, basic safety message, BSM, silent period, safety, privacy**

I. Introduction

AUTOMOBILES and other vehicles will soon include network equipment, effectively turning roadways into moving communication systems. One of the primary objectives of such systems is safety.

In vehicular ad-hoc networks (VANETs), certain wireless communications called Basic Safety Messages (BSMs) would be transmitted in order to help prevent crashes between vehicles. Accurate global positioning systems (GPS) installed in each vehicle would provide precise location data for BSMs. Every fraction of a second, each vehicle could compute future positions of its neighboring vehicles and avoid impending inter-vehicle collisions. In this way VANETs may one day prevent death and injury, reduce insurance costs, and may also reduce transportation costs by enabling new traffic management systems.

VANET equipment is expected to take time to roll out. To prevent a crash between two cars, the equipment must be operational in both cars. To obtain full safety value from a VANET requires equipment to be operational in all cars. It will take time to achieve near-full implementation. To our knowledge no study has been done to compute the cost of delaying such a rollout.

Further, VANETs raise privacy concerns because they would transmit data which may also be used for unwanted surveillance. Researchers have proposed protocols to protect against surveillance, but many protocols require periodic *silent periods*, spans of time when vehicles cease transmissions, thereby disabling VANET safety benefits. To our knowledge no study has been done to compute the cost of implementing these silent periods.

This research addresses the following problem: the tradeoff between safety and silence. The safety-silence tradeoff problem is important because society values both safety and privacy. Without a quantitative measure for the tradeoff it is difficult for individuals and policymakers to weigh necessary compromises between the two.

The problem is complicated also because VANETs do not work exactly like conventional networks. First, the networks are in motion, following mobility patterns of cars and trucks. Second, the protocols differ. Corporate and home networks, for example, depend on static MAC addresses and TCP/IP, but safety systems in VANETs use new protocols in which MAC addresses are dynamic—they can be changed by the vehicle in transit. In the United Stated the new protocols are part of Dedicated Short Range Communications (DSRC) / Wireless Access in Vehicular Environments (DSRC/WAVE). WAVE Short Message Protocol (WSMP) was created to improve communication speed. Dynamic MAC addressing was added specifically to enable privacy protocols. The BSM for example is part of a protocol called SAE J2735.

The primary contribution of this paper is the presentation and proof of the *Safety-Silence Tradeoff Equation*. Also presented are illustrations and examples of applications of the equation. To our knowledge no method has yet been proposed to compute this tradeoff in vehicular contexts. There are some works on the mathematics of privacy [15] and computational privacy [14], but they do not include discussions of the cost tradeoff between safety and silent periods.

The rest of this paper is organized as follows. Section II presents background for the VANET privacy problem, establishing the necessity of silent periods. Section III presents mathematical analysis and proof. Section IV presents an illustration and Section V discusses practical considerations. Section VI presents results of simulations to evaluate performance of the equation. Section VII concludes the paper.

G. P. Corser is with Saginaw Valley State University, University Center, MI 48710 USA (e-mail: gpcorser@svsu.edu).

A. D. Arenas is with Saginaw Valley State University, University Center, MI 48710 USA (e-mail: adarenas@svsu.edu).

H. Fu is with Oakland University, Rochester, MI 48309 USA (e-mail: fu@oakland.edu).

II. Background

The privacy issue is not moot because of E911. It is possible for motorists to confuse traffic monitors using DSRC even if the devices or trade them with other people. However, US DOT by requiring DSRC in vehicles may not allow drivers to turn systems off except for specific privacy purposes for which provisions have been made in IEEE 1609.2. Moreover, the Principle of Least Privilege remains a well-respected, fundamental and enforceable information security policy. It dictates that privacy defenders cannot fail to protect location data from one attacker simply because another potential attacker has access. Transportation monitors would work on DSRC systems completely independently from E911 system. Transportation monitors should only be given access to such data if it is deemed important by whoever sets up the transportation system. The same would be true for LBSs such as WAZE. If WAZE executives were to allow its administrators to casually monitor drivers, the company may be exposed to legal risks. Plus, there may be a moral issue, or even a business perception issue.

VANETs depend on vehicles each having access to accurate Global Positioning System data. Vehicles transmit their positions to each other using vehicle-to-vehicle (V2V) communications. Vehicles may communicate with application servers, such as Location Based Services (LBS) via wired roadside units (RSU) using vehicle-to-infrastructure (V2I) communications. See Fig. 1. However, as far as their effect on safety is concerned, silent periods are relevant only within V2V communications.

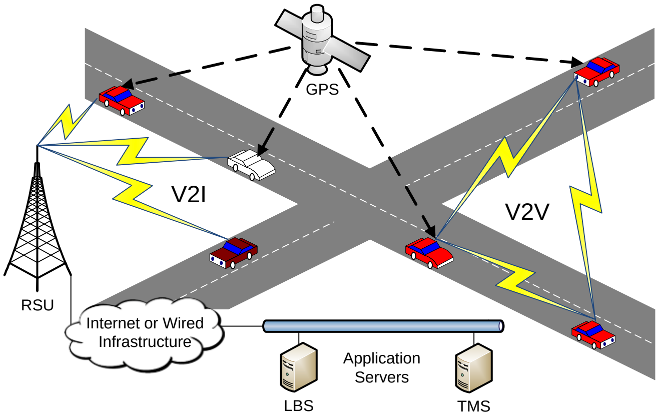

Fig. 1. System model

Among the earliest and most cited papers [1] in the field of vehicular ad hoc network privacy are recommendations that privacy protection schemes include silent periods. Recent work has suggested privacy protocols be executed at “social spots” such as traffic lights and intersections [16].

These and other recommendations were founded partly on the results of seminal work in mix zones [2]. Silent periods and mix zones operate together. Vehicles cease transmitting and change positions, then begin transmitting again using different identifiers. Silent periods and mix zones have been proven to be effective, and some even suggest in cases where one mix zone is not enough, use multiple cascading mix zones for even more privacy protection [3]. The problem of silent periods and mix zones has been studied for at least the past ten years [6-12].

If the US Department of Transportation mandates the implementation of VANETs, as they are expected to do, not all vehicles will transmit basic safety messages (BSMs). At some point in time, at a given intersection or other potential collision point, perhaps only half of the vehicles will have VANET equipment installed. Even after full deployment vehicles will go radio silent when implementing privacy protocols. What’s the risk?

III. Mathematical Analysis

The probability of a crash between vehicles can be estimated by examining the number of possible crash combinations in a given geographical area during a given time frame. Assuming the probability of a crash is different when vehicles are not transmitting BSMs, then given certain assumptions, the probability of at least one crash in a region R during a time Δt is as follows. This is the ***Safety-Silence Tradeoff Equation***.

$$prob_{R,\Delta t}(crash \geq 1) = \\ 1-(1-p_b)^{\binom{b}{2}}(1-p_u)^{\binom{n}{2}-\binom{b}{2}} \quad (1)$$

Proof. Let p_b be the probability of a crash between two vehicles both transmitting BSMs. By the Complement Rule the probability of any particular two such vehicles not crashing is $(1-p_b)$.

By definition of combination, the total number of potential crashes between any two of n vehicles is $\binom{n}{2}$. Therefore the number of potential crashes between any two of b vehicles is $\binom{b}{2}$, where b is the number of vehicles in R transmitting BSMs during Δt.

By the Multiplication Rule the probability of all b vehicles not crashing is the product of the probabilities of each potential crash not occurring, i.e. $prob_b(no\ crashes) = (1-p_b)^{\binom{b}{2}}$.

Define n as the total number of pairs in R during Δt. Then the total number of pairs is $\binom{n}{2}$. The number of possible crashes of unprotected vehicles, vehicle pairs where at least one of the vehicles is not transmitting BSMs, is $\binom{n}{2}-\binom{b}{2}$, and $prob_u(no\ crashes) = (1-p_u)^{\binom{n}{2}-\binom{b}{2}}$.

This analysis assumes that if vehicles have OBUs they transit BSMs, otherwise they do not. With privacy protocols operating on OBUs there are 4 possibilities, (a) both transmitting, (b) both not transmitting, (c) receiving vehicle is not transmitting but other vehicle is transmitting, and (d) receiving vehicle is transmitting but other vehicle is not transmitting. The four-possibility scenario is not considered here due to space limitations.

The probability of three vehicles crashing would be the probability of one pair crashing multiplied by the probability of another pair crashing in the same region R during the same time, Δt. Since probabilities, p_b and p_u, are extremely small, it can be assumed that the probability of three cars crashing is negligible. That is, $p_b^2 \approx 0$, $p_b^2 \approx 0$, and $p_b p_u \approx 0$.

The probability of at least one crash, $prob_{R,\Delta t}(crash \geq 1)$, is $prob_b(no\ crashes)prob_u(no\ crashes)$, which reduces to (1). QED.

About 40% of all accidents in the US occurred at intersections in 2006, 8,500 of which were fatal and 900,000 of which were injurious [17]. In Japan, in 1997, 60% of accidents occur at intersections. Based on a study of 150 four-legged intersections in the Tokyo metropolitan area, researchers observed that the average probability of a vehicle encountering an obstacle vehicle was 0.339 and the average probability of a following vehicle driver's failure was 0.0000002 [18]. These vehicles were not outfitted with on-board units (OBUs), the devices that transmit BSMs. No data are available regarding accident probabilities of vehicles with OBUs installed, however one recent NHTSA report estimated that V2V could one day address 79% of vehicle crashes [19]. From this we can roughly estimate that the probability of a crash at an intersection without any BSMs is 0.339 times 0.0000002, or 0.0000000678, and the probability of a crash at an intersection with all vehicles transmitting BSMs is (1-0.79) times 0.0000000678, or 0.00000001423.

IV. Illustration

The maximum number of possible collision combinations rises exponentially with the number of vehicles. If we choose *n*=10 we can vary *b* to see the relationship between *b*, the number of vehicles transmitting BSMs, and *n*, the total number of vehicles in region *R*.

Fig. 3 shows that if 5 of 10 (50%) vehicles transmit BSMs, 35 out of 45 (78%) collisions remain possible. One could conclude that if a large percentage of vehicles would enter a silent period, then neighboring vehicles might do likewise since the marginal loss in collision protection would be at a minimum.

V. Practical Considerations

With four vehicles at a four-way stop, there are 28 possible impact points but $\binom{4}{2}$=6 possible collisions between two vehicles. See Fig. 4. The equation does not count the number of potential impact points, rather, it counts only the number of combinations of pairs of vehicles.

The safety-silence tradeoff equation predicts the probability of at least one collision is 1 - (1 - p_b) (1 - p_u)^5 where p_b and p_u are as defined in Section III and assuming *n*=4 and *b*=2.

With six vehicles, an intersection of one two-lane road and one four-lane road, there are 56 possible impact points assuming expected traffic flow. See Fig. 5. Three possibilities are ruled out in the model: A cannot collide with E, C cannot collide with F, and E cannot collide with F. Therefore, there are $\binom{6}{2}$ - 3 = 12 possible collisions between two vehicles.

Suppose A, B and C do not transmit BSMs, but D, E, and F do. Then $prob_b(no\ crashes) = (1-p_b)^{\binom{3}{2}-1} = (1-p_b)^2$ and $prob_u(no\ crashes) = (1-p_u)^{\binom{6}{2}-3-\binom{3}{2}} = (1-p_u)^{10}$.

In sum, impossible collision combinations must be subtracted from the exponent in the safety-silence tradeoff equation. This can be accomplished by including constants.

Let the quantities, c_b and c_n, be the number of logistically impossible collision combinations between vehicles both transmitting BSMs and between all vehicles, respectively. Then the modified equation would be as follows.

$$prob_{R,\Delta t}(crash \geq 1) = \\ 1-(1-p_b)^{\binom{b}{2}-c_b}(1-p_u)^{\binom{n}{2}-c_n-\binom{b}{2}+c_b} \qquad (2)$$

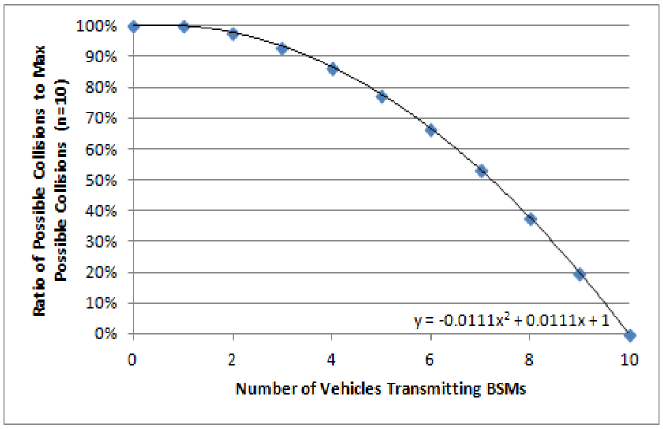

Fig. 3. An inverse exponential relationship exists between the proportion of vehicles transmitting BSMs and the proportion of potential collisions unprotected by BSMs. Under assumptions, if 5 of 10 (50%) vehicles transmit BSMs, 35 out of 45 (78%) collisions remain possible.

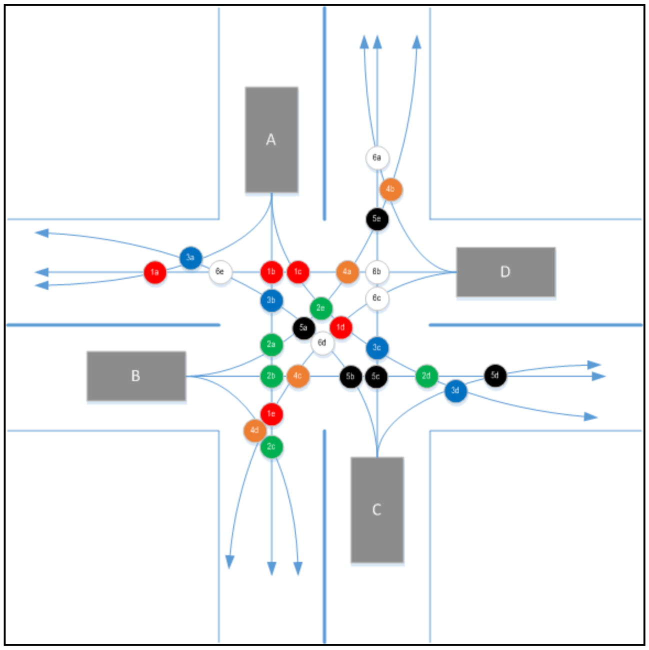

Fig. 4. Four vehicles at an intersection of two two-lane roads (Class 1 simulation scenario)

VI. Simulations

Simulated and computed results were compared for two types of intersections, Class 1 and Class 2, as pictured in Fig. 4 and Fig. 5, respectively. All possible values for *b* and *n* were computed and simulated. No combinations were removed using constants as in (2); all computations were pure, as in (1). Probabilities and other simulation parameters were set according to Table I. There were 1000 simulation runs per scenario.

TABLE I
SIMULATION PARAMETERS

Parameters	Values
Intersections, vehicle quantities (n) and vehicles sending BSMs (b)	Class 1: n=4 vehicles at an intersection of two two-lane roads (as in Fig. 4), $0 \le b \le 4$ Class 2: n=6 vehicles at an intersection of a two-lane and a four-lane road (as in Fig. 5), $0 \le b \le 6$
p_b, p_u	Scenario A: p_b=.1, p_u =.2 Scenario B: p_b=.01, p_u =.02 Scenario C: p_b=.001, p_u=.002

Comparison of computed versus simulated results showed that the equation estimated simulation results accurately. However, as probabilities become increasingly small computations become less accurate. Numerical methods will need to be employed in order to maintain numerical precision.

Fig. 6 shows the results for Class 1 intersection simulations with probability scenarios A, B and C as defined in Table I. Fig. 7 shows results from Class 2 intersection simulations. Fig. 6 and Fig. 7 echo a pattern similar to that shown in Fig. 3, except the reduction in the probability of at least one crash occurs even more gradually with the increase in the ratio of the number of vehicles transmitting BSMs to the total number of vehicles in the system.

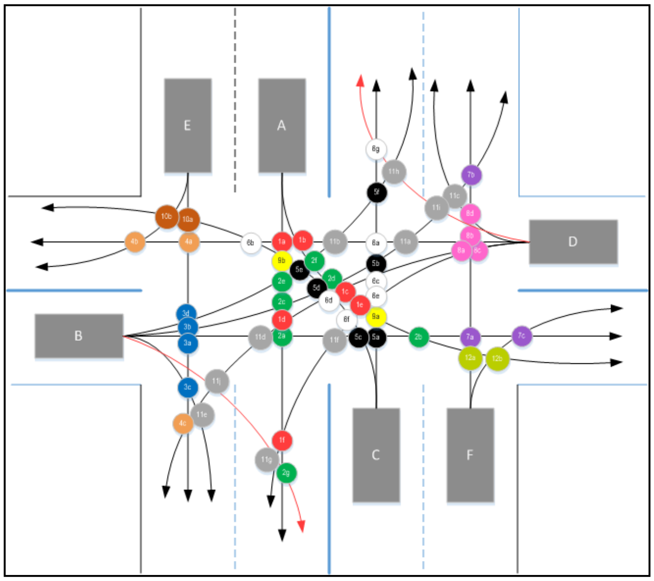

Fig. 5. Six vehicles at an intersection of a two-lane and a four-lane road (Class 2 simulation scenario)

Figures 6 and 7 assume intersections are full, i.e. all possible positions of vehicle in an intersection have a vehicle present and waiting to enter the intersection. It may be more likely that one or more possible positions are unfilled. Consider the diagram in Fig. 4. It may be that positions A, B and C are occupied, but D is vacant; there is no car at position D. In this case all vehicle combinations involving D cannot produce crashes.

A simulation was also run using a Class 1 intersection under Scenario A as defined in Table I. See Fig. 8.

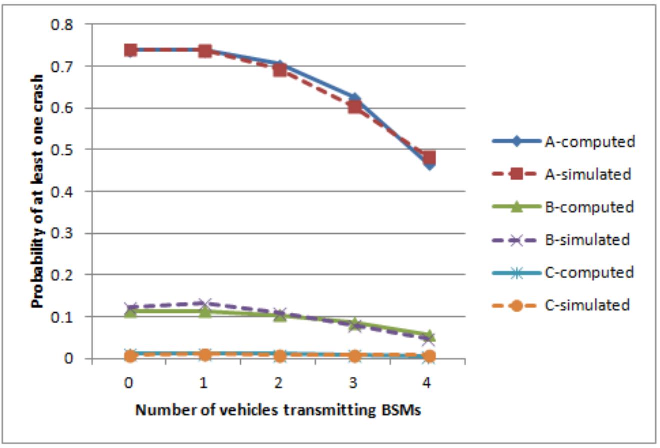

Fig. 6: Intersection Class 1, probability scenarios A, B and C

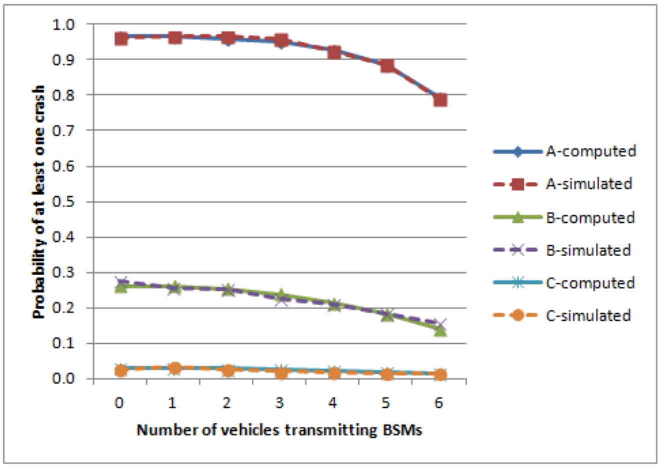

Fig. 7: Intersection Class 2, probability scenarios A, B and C

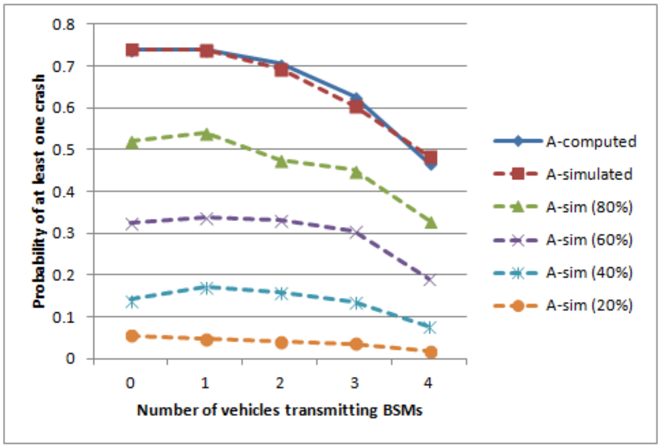

Fig. 8. Class1 intersection with simulation Scenario A at five levels of intersection density, 100%, 80%, 60%, 40% and 20%. The results show a near-linear relationship between the percentage of vehicles positions occupied at a 4-way stop intersection and the probability of at least one crash at that intersection.

Simulations were run using extremely high probabilities because simulations using probabilities in the realistic range would not hold numerical precision. However, computed and simulated results showed clearly similar patterns. See Figs. 6, 7 and 8. If these patterns hold in smaller probabilities then the Safety-Silence Tradeoff Equation may serve as a useful back-of-the-napkin estimator.

VII. Conclusion and Future Work

This paper has shown the following. First, an inverse exponential relationship exists between the proportion of vehicles transmitting BSMs and the proportion of potential collisions unprotected by BSMs. This is a straightforward computation of combinations of crashes possible between vehicles in a region. The conclusion from this observation is, if privacy protocols must include a silent period, then perhaps *as many vehicles as possible* should execute privacy protocols when *any* vehicles decide to go transmission silent. This is because the marginal loss in collision protection is greatest when one single vehicle decides not to transmit BSMs while all others do.

Second, the Safety-Silence Tradeoff Equation might provide a rough estimate of the cost of VANET privacy methods that require silent periods. This can be done by computing the likelihood of crashes between combinations of vehicles at intersections. In order to accomplish this in practice, future work would necessarily include gathering statistics to obtain accurate probabilities in different intersection situations and developing numerical techniques to maintain computational precision when applying the probabilities, p_b and p_u. The specific probabilities, p_b and p_u, will likely differ given a range of factors including location, weather conditions, and the types of vehicles in the region.

Third, in practice some combinations of potential collisions might be eliminated. The equation can be modified to accommodate these scenarios by the inclusion of certain constants. Careful analysis of historical vehicle crash data would be required in order to accomplish this in practice. There may even be a need to develop a handbook or other database for crash probabilities between vehicles at different types of intersections, including which combinations can be ignored.

Fourth, traffic density affects the computation. If intersections are not full of cars, probabilities of crashes are lower. Sophisticated traffic management systems of the future, armed with hyper-accurate historical data of past crashes, and vehicle densities, might be able to inform vehicles seeking privacy using silent periods of the optimal (safest) times and locations to execute the protocols.

Finally, transmission silence could occur because the dissemination of on-board units (OBUs) has not reached a high level of saturation in a particular geographical area. During this ramp-up interval the use of privacy protocols which require silent periods would be less risky than in intervals or locations of full saturation. These risks should be monitored as conditions change over time and space.

Acknowledgement

This paper is based in part upon work supported by Saginaw Valley State University (SVSU) Undergraduate Research Program [13] as part of a faculty-led research grant. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of SVSU.

References

[1] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). CARAVAN: Providing location privacy for VANET. WASHINGTON UNIV SEATTLE DEPT OF ELECTRICAL ENGINEERING.

[2] Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 46–55 (2003).

[3] Beresford, A.R., Stajano, F.: Mix zones: user privacy in location-aware services. In: Pervasive Computing and Communications Workshops, pp. 127–131 (2004)

[4] Freudiger, J., Shokri, R., & Hubaux, J. P. (2009, January). On the optimal placement of mix zones. In Privacy enhancing technologies (pp. 216-234). Springer Berlin Heidelberg.

[5] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." Journal of Computer Security 15.1 (2007): 39-68.

[6] Huang, L., Matsuura, K., Yamane, H., & Sezaki, K. (2005, March). Enhancing wireless location privacy using silent period. In Wireless Communications and Networking Conference, 2005 IEEE (Vol. 2, pp. 1187-1192). IEEE.

[7] Buttyán, L., Holczer, T., & Vajda, I. (2007). On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In Security and Privacy in Ad-hoc and Sensor Networks (pp. 129-141). Springer Berlin Heidelberg.

[8] Dok, H., Echevarria, R., & Fu, H. (2009). Privacy Issues for Vehicular Ad-Hoc Network. In Communication and Networking (pp. 370-383). Springer Berlin Heidelberg.

[9] Studer, A., Shi, E., Bai, F., & Perrig, A. (2009, June). TACKing together efficient authentication, revocation, and privacy in VANETs. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on (pp. 1-9). IEEE.

[10] Tomandl, A., Scheuer, F., & Federrath, H. (2012, October). Simulation-based evaluation of techniques for privacy protection in VANETs. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on (pp. 165-172). IEEE.

[11] Sun, Y., Zhang, B., Zhao, B., Su, X., & Su, J. (2014). Mix-zones optimal deployment for protecting location privacy in VANET. Peer-to-Peer Networking and Applications, 1-14.

[12] Emara, K., Woerndl, W., & Schlichter, J. (2015). On evaluation of location privacy preserving schemes for VANET safety applications. Computer Communications, 63, 11-23.

[13] http://www.svsu.edu/ugrp.

[14] Krumm, J. (2009). A survey of computational location privacy. Personal and Ubiquitous Computing, 13(6), 391-399.

[15] Katirai, H. (2006). A theory and toolkit for the mathematics of privacy: methods for anonymizing data while minimizing information loss (Doctoral dissertation, Massachusetts Institute of Technology).

[16] Lu, R., Li, X., Luan, T. H., Liang, X., & Shen, X. (2012). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. Vehicular Technology, IEEE Transactions on, 61(1), 86-96.

[17] Burnett, Nathaniel P., and Anuj Sharma. "Role of information on probability of traffic conflict on the onset of yellow." (2011).

[18] Wang, Yinhai, Hitoshi Ieda, and Fred Mannering. "Estimating rear-end accident probabilities at signalized intersections: occurrence-mechanism approach." Journal of Transportation engineering 129.4 (2003): 377-384.

[19] Harding, John, et al. Vehicle-to-vehicle communications: Readiness of v2v technology for application. No. DOT HS 812 014. 2014.