Impact of V2X privacy strategies on intersection collision avoidance systems

Stéphanie Lefèvre, Jonathan Petit, Ruzena Bajcsy, Christian Laugier, Frank Kargl

Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems

Stéphanie Lefèvre*‡, Jonathan Petit†, Ruzena Bajcsy*, Christian Laugier‡, Frank Kargl†§
*Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, USA
†Distributed and Embedded Security Group, University of Twente, The Netherlands
‡Inria Grenoble Rhône-Alpes, Saint-Ismier, France
§Institute of Distributed Systems, Ulm University, Germany
slefevre@berkeley.edu, j.petit@utwente.nl, bajcsy@eecs.berkeley.edu,
christian.laugier@inria.fr, frank.kargl@uni-ulm.de

***Abstract*—User privacy is a requirement for wireless vehicular communications, and a number of privacy protection strategies have already been developed and standardized. In particular, methods relying on the use of temporary pseudonyms and silent periods have proved their ability to confuse attackers who would attempt to track vehicles. In addition to their ability to protect privacy, it is important to ensure that these privacy strategies do not hinder the safety applications which rely on vehicular communications. This paper addresses this concern and presents an experimental analysis of the impact of privacy strategies on Intersection Collision Avoidance (ICA) systems. We simulate traffic scenarios at a road intersection and compare the ability of a collision avoidance system to avoid collisions for different pseudonym change schemes. The privacy level is analyzed, as well as the influence of the duration of the silent period on the safety performance of the ICA system. The results highlight the need to jointly design safety applications and privacy strategies.**

***Index Terms*—Vehicular communication networks, privacy strategies, silent period, safety applications, collision avoidance systems.**

I. Introduction

Wireless vehicular communications (or Vehicle-to-X communications, V2X) open new opportunities for safety-related applications and Intelligent Transportation Systems. The sharing of information such as road conditions and current trajectories allows a vehicle to perceive its environment beyond the field of view of its on-board sensors, leading to a better situation awareness. Studies have shown that the potential of V2X-based safety systems should be greater than standalone safety systems [1], and that V2X applications may potentially address up to 81% of crash scenarios [2]. The potential of V2X for safety has also been demonstrated by a number of Field Operational Tests in Europe [3], the US [4], and Japan [5].

Another aspect of V2X-based applications is the privacy and security of information. Privacy is required in order to ensure acceptance by users [6]. In addition, the sharing of information between vehicles is expected to have an impact on traffic safety, therefore this information must be secured [7]. For this reason authentication mechanisms are mandatory for vehicular communications, so that receivers can verify that the sender is an authorized vehicle. However, if no privacy protection is implemented on top of the authentication mechanism, then any vehicle can be remotely tracked by eavesdropping on the communication channel. Information about the authenticated drivers could be inferred (home address, work, medical condition, etc.), jeopardizing their privacy. One solution to protect the user while allowing authentication mechanisms is to sign messages using temporary identifiers, namely pseudonyms. However defining strategies for pseudonym change is not trivial. A simple periodic change would be easy to circumvent [8], therefore some more advanced pseudonym change strategies have been proposed involving random pseudonym changes and a "silent period" after each change.

These privacy protection schemes are not without consequences for safety applications. Such applications make decisions (e.g. warning drivers of an upcoming danger) based on their current estimation of the state of the real world, and this representation is created from the information contained in beacons received from other vehicles. Therefore, interruptions in the transmission of information will impact the decision-making process. If a silent period is scheduled to start at a safety-critical moment, it could result in safety systems not intervening when they should have, namely a "missed intervention". From a user and safety perspective, this is not acceptable.

In this paper we address this issue and evaluate the impact of pseudonym change strategies on V2X-based collision avoidance systems. In particular we focus on Intersection Collision Avoidance (ICA) systems. This choice is motivated by the considerable potential of V2X-based safety applications to reduce the number of crashes at road intersections, compared to standalone safety systems. Indeed, a major issue for safety applications at road intersections is the potential occlusion of part of the scene due to the geometry of the intersection, the presence of obstacles like trees, buildings, etc. Some of the other vehicles can be detected by on-board exteroceptive sensors such as cameras, radars, or lidars, but others will be occluded or simply be beyond the field of view of the sensors. V2X communications do not suffer from this limitation and the hope is that this will help reducing the number of intersection-related accidents, which currently represent 40 to 50 percent of road accidents in most countries [9], [10].

The rest of the paper is organized as follows. Section II presents related work addressing the impact of network and security mechanisms on cooperative collision avoidance applications. Section III describes the main pseudonym change strategies and introduces the concept of *silent period*. In Section IV we describe the methodology used to conduct our evaluation. Section V presents the results of our simulations. Finally, Section VI draws conclusions and presents future work.

II. Related Work

Haas and Hu [11] analyzed the ability of a V2X-based intersection collision warning application to warn drivers sufficiently in advance of a potential collision that the involved drivers can stop. Especially, they investigated the reliability requirements of VANET communications, and evaluated the impact of different transmission powers and authentication mechanisms on the ability to avoid crashes. This work demonstrates the impact of network and security mechanisms on safety applications.

Petit and Mammeri [12] analyzed the impact of authentication mechanisms (namely ECDSA) on the braking distance and the delay of decision in cooperative collision warning applications. Their results highlight the significant consequences of security mechanisms on the performance of safety applications.

Our work differs from the aforementioned papers in that we analyze the impact of privacy mechanisms on collision avoidance systems. More specifically, we analyze the effect of pseudonym change strategies involving silent periods on the ability to predict and avoid collisions.

III. Pseudonym Schemes

The current set of vehicular communication standards in Europe [13]–[15] mandates the use of asymmetric cryptography for authentication mechanisms, namely the Elliptic Curve Digital Signature Algorithm (ECDSA) with P-256 elliptic curve. Unfortunately, authentication mechanisms break user privacy as every receiver learns the identity of the sender. Therefore, a short-term credential –*pseudonym*– should be implemented in order to prevent authentication mechanisms from easing vehicle tracking. The pseudonym has to be changed frequently to ensure a sufficient level of privacy [16]. The ETSI TS 102 867 standard recommends changing one's pseudonym every five minutes [17].

In the US, the SAE J2735 standard [18] defines the Probe Segment Number (PSN), which enables users to share trajectory information for a limited amount of time or over a limited distance. To ensure privacy, the PSN is changed by a vehicle every 120 seconds or 1 km, whichever comes last.

However, as soon as the attacker knows the period of pseudonym changes –which is easy to assess– tracking becomes trivial [8]. In order to avoid this issue brought by fixed pseudonym change periods, vehicles can change their pseudonym randomly [19]. As a result, an adversary cannot forecast the next pseudonym change. However, tracking is still possible if only one or few vehicles change pseudonyms at a specific time and location, because all other neighbors keep the same identity. Thus, linking the new and old pseudonym of the vehicle that performed the change is still trivial. A solution is to introduce a *silent period* (i.e., the vehicle stops broadcasting information) after each pseudonym change [20]–[23]. The silent period makes tracking attacks more complex. For example, if a vehicle changes its pseudonym before entering an intersection and then stays silent for some time, it becomes very difficult to assess the new position of the vehicle. In the current SAE J2735 standard [18] each new PSN comes with a random silent period (named *changeover gap*) with a duration of 50 to 250 m or 3 to 13 seconds, whichever comes first.

To further harden tracking attacks, Gerlach and Güttler [24] proposed a *mix-context* approach where vehicles change their pseudonyms when they detect a favorable context, such as a favorable number of neighbors, their speeds and directions. To identify the best opportunity to change pseudonyms, a threshold on the minimum entropy has to be defined either by the user or by an application.

IV. Methodology

This section describes the methodology used to conduct our analysis. We first describe the addressed scenarios and how the simulations are run. The second part of this section introduces the safety application considered in this analysis and describes the collision avoidance system.

A. Simulating road intersection scenarios

1) Generating trajectories: The PreScan simulator [25] is used to create a two-way-stop intersection layout and to simulate trajectories for vehicles traversing it. PreScan can generate both non-colliding and colliding pairs of trajectories, and the user can synchronize the trajectories of two vehicles so that they intersect at a specific location.

Four different scenarios are defined, each of them involving an "Ego Vehicle" (EV) driving on the main road towards the intersection and an "Other Vehicle" (OV) approaching the intersection from a secondary road and performing various maneuvers. The scenarios are illustrated in Fig. 1. Scenarios 1, 2, and 3 are *collision* scenarios where the EV and the OV collide after the OV violated the stop sign. They were selected because they cover 60% of all accident scenarios at road intersections in Europe [9]. Such accidents are typically caused by the driver of the OV failing to notice the presence of the stop sign, or misjudging the speed and distance of the EV [26]. Scenario 4 is a *no-collision* scenario where the OV stops at the stop line and yields to the EV.

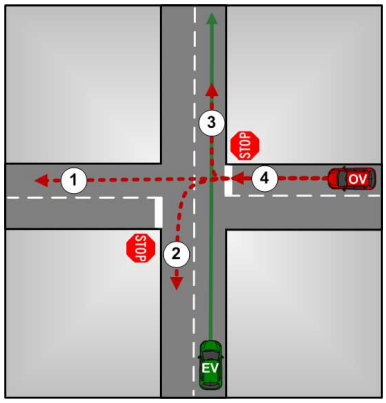

Fig. 1. The four simulated scenarios. For each scenario the maneuver of the "Ego Vehicle" (EV) is shown in plain green and the maneuver of the "Other Vehicle" (OV) is shown in dotted red.

2) Simulating privacy strategies: We simulate 3 different privacy protection strategies, described below.

The "*Fixed ID*" strategy assigns a fixed pseudonym to a vehicle for the entire duration of a trip (i.e. a new pseudonym is assigned to the vehicle every time it starts). Testing this case will give us a reference for how well the collision avoidance system performs when there is no pseudonym change and no silent period during a trip.

The "*Baseline*" strategy follows the recommendations of the SAE J2735 standard [18]. Pseudonyms are changed every $T_{chg} = 120$ seconds and are followed by a silent period of random duration T_{sil} comprised between 0 and 13 seconds. Even if silent periods of duration shorter than 3 seconds are not considered in [18], we include them in our tests in order to analyze the impact of the silent period duration on the safety system.

The "*Adaptive*" strategy is a modified version of the *Baseline* strategy where the risk of the situation is taken into account to decide whether or not vehicle i should be allowed to change pseudonym at time t. It relies on the computation of the probability $P(\textit{safety\_guaranteed}_{i,t})$, where the binary variable $\textit{safety\_guaranteed}_{i,t} \in \{0,1\}$ corresponds to the current ability of the collision avoidance system to keep vehicle i on a collision-free trajectory. A pseudonym change at time t with a silent period of duration T_{sil} is authorized if and only if:

$$P(\textit{safety\_guaranteed}_{i,t+T_{sil}}) \geq P(\textit{safety\_guaranteed}_{i,t}) \quad (1)$$

The idea here is to authorize a pseudonym change and silent period only if it will not affect the performance of the safety application. The computation of the terms in Eq. 1 will be detailed in the next section, after the description of the collision avoidance system.
By comparing the impact of these three privacy strategies on a collision avoidance application, we will be able to assess whether the standard "pseudonym change + silent period" strategy, here named *Baseline* strategy, affects the safety performance of the ICA system. It is also expected that the results will show whether the addition of a simple metric such as Eq. 1 is enough to prevent a loss of safety performance while providing some privacy protection.
In order to implement these strategies in practice, each time we run a new simulation of one of our scenarios it is necessary to define the time instant of the last pseudonym change for vehicle i. In the remaining of this paper, this time instant will be called $t_{chg,i}$. For the *Fixed ID* strategy, the last pseudonym change occurred at the beginning of the current trip. This is modeled by sampling $t_{chg,i}$ from a uniform distribution: $t_{chg,i} \sim t_{init} - \textit{unif}(0, 2 \times T_{avg})$ where t_{init} is the current time at the beginning of the simulation and $T_{avg} = 21$ minutes is the average duration of a trip [27]. For the *Baseline* and *Adaptive* strategies $t_{chg,i}$ is sampled from a uniform distribution $t_{chg,i} \sim t_{init} - \textit{unif}(0, T_{chg})$ where $T_{chg} = 120$ seconds is the period of pseudonym changes. It is assumed that the *Adaptive* strategy authorized the last pseudonym change prior to the beginning of our test instances.

3) Generating multiple instances: A total of 10200 *collision* instances and 6300 *no-collision* instances were simulated, by varying the following parameters:

- Scenario (see Section IV-A1)
- Acceleration / deceleration profiles of the EV and OV in order to simulate different driving styles
- Privacy strategy (see Section IV-A2)
- Pseudonym change time and duration of the silent period (generated as described in Section IV-A2).

The generated instances are 9.5 seconds long on average; the shortest and longest ones are 8 and 10 seconds long respectively.
The wireless communication link between the vehicles was assumed to never suffer packet losses and to provide instantaneous data transmission. The impact of network disturbances on safety applications has been investigated in the past [28], [29] and is out of the scope of this study, since we wish to evaluate the direct impact of the different privacy strategies on the safety application.

B. V2X-based collision avoidance system

Several ICA systems have been proposed in the past which rely on V2X communications, e.g. [30]–[32]. The system used in this work is based on our previous work [32] where we proposed to evaluate the risk of a situation by estimating and comparing the intentions of the different drivers in the intersection area. The advantage of this approach is that it takes into account the dependencies between the motion of the different vehicles, which leads to a better assessment of the intentions of the drivers [33]. The approach was tested both in simulation [32] and in field experiments [33]. A brief description of the method is provided below.

1) Probabilistic motion model: The joint motion of vehicles in a traffic scene is modeled by a Dynamic Bayesian Network (DBN) using four categories of variables:

- $I_{i,t}$ represents the maneuver being performed by vehicle i at time t (e.g. turn left, stop). We call it I as in "Intention", since the maneuver performed by a vehicle reflects the *intended maneuver* of the driver.
- $E_{i,t}$ represents the maneuver that vehicle i is expected to perform at time t according to the traffic laws (e.g. turn left, stop). We call it E as in "Expectation", since it represents the *expected maneuver*.
- $\Phi_{i,t}$ represents the *physical state* of vehicle i at time t (e.g. position, speed).
- $Z_{i,t}$ represents the *measurements* available about vehicle i at time t. They often correspond to a noisy version of a subset of the *physical state* variables.

$I_{i,t}$, $E_{i,t}$, and $\Phi_{i,t}$ are hidden variables, while $Z_{i,t}$ is observed. For more clarity in the equations, in the remaining of this paper factored stated will be used to represent the conjunction of variables for the N vehicles in the scene, e.g. $Z_t \triangleq (Z_{1,t}...Z_{N,t})$.
The proposed joint distribution of the DBN over all the vehicles is as follows [32]:

$$\begin{aligned} &P(E_{0:t_{end}} I_{0:t_{end}} \Phi_{0:t_{end}} Z_{0:t_{end}}) = P(E_0 I_0 \Phi_0 Z_0) \\ &\times \prod_{t=1}^{t_{end}} \times \prod_{i=1}^{N} [P(E_{i,t}|I_{t-1}\Phi_{t-1}) \times P(I_{i,t}|I_{i,t-1}E_{i,t}) \\ &\times P(\Phi_{i,t}|\Phi_{i,t-1}I_{i,t}) \times P(Z_{i,t}|\Phi_{i,t})] \end{aligned} \tag{2}$$

which corresponds to a classic Markov state-space model linking $I_{i,t}$, $\Phi_{i,t}$, and $Z_{i,t}$, augmented by the *expected maneuver* $E_{i,t}$ which is derived from the previous situational context $(I_{t-1}\Phi_{t-1})$ and has an influence on the intended maneuver $I_{i,t}$. For the interested reader more details about this model can be found in the previously published papers describing this DBN [32], [33].

2) Bayesian inference for risk estimation: Inference on variables in the DBN described above is performed using a particle filter, which means that at each timestep the probability density function of the hidden variables I_t, E_t, and Φ_t is approximated by a set of weighted samples called particles. The set of K particles at time t is denoted:

$$\{H_{k,t}, w_{k,t}\}_{k=1:K} \tag{3}$$

with $H_{k,t}$ the state of particle k at time t, and $w_{k,t}$ the weight of particle k at time t.
The risk estimation algorithm proposed in [32] exploits the fact that 90% of road accidents are caused by driver error [26]. The probability of a collision in the future is computed as the probability that the intentions of drivers differ from what is expected of them:

$$P(\exists i \in N :\ I_{i,t} \neq E_{i,t}|Z_{0:t}) \tag{4}$$

Using the particle filter, this inference can be performed by summing up the weights of the current particles which verify the condition $(\exists i \in N :\ I_{i,t} \neq E_{i,t})$.

3) Autonomous emergency braking: The collision avoidance application proposed in [32] triggers autonomous emergency braking if and only if the probability of a collision is higher than a threshold, i.e. iff:

$$P(\exists i \in N :\ I_{i,t} \neq E_{i,t}|Z_{0:t}) > \gamma \tag{5}$$

The threshold γ was set after a precision / recall analysis [32]. The application runs in real-time on a dedicated dual core 2.26 GHz processor PC with 400 particles for the filter and with new observations Z_t made available very 200 ms.

4) Computation of P(safety_guaranteed): For the *Adaptive* privacy strategy introduced in Section IV-A2, it is necessary to compute the probability P(*safety_guaranteed*). First of all we define the Time-To-Collision (TTC), and the Time-To-Stop (TTS). The TTC can be computed as the time that is left until a collision occurs if both vehicles involved in the collision continue on the same course and at the same speed [34]. The TTS corresponds to the time needed by a vehicle to reach a full stop after the ICA system intervenes, and can be computed as follows [9]:

$$TTS_{i,t} = \frac{s_{i,t}}{\delta} + T_{machine} \tag{6}$$

with $s_{i,t}$ the speed of the vehicle i at time t, $\delta = 7\,\text{m/s}^2$ the deceleration applied by the ICA system, and $T_{machine} = 0.4\,\text{s}$ the average braking system response time [9].
The probability $P(safety\_guaranteed_{i,t})$ that the collision avoidance system is currently able to keep the vehicle i on a collision-free trajectory can be computed by summing up the weights of the current particles which verify the condition $(TTC_{i,t} > TTS_{i,t})$. The probability $P(safety\_guaranteed_{i,t+T_{sil}})$ that the collision avoidance system will able to keep the vehicle on a collision-free trajectory after a silent period of duration T_{sil} is computed by assuming constant speed during the silent period and summing up the weights of the current particles which verify the condition $(TTC_{i,t} - T_{sil} > TTS_{i,t})$.

V. Results

A. Evaluation metrics

In order to compare the three privacy strategies described in Section IV-A2 when applied to the scenarios defined in Section IV-A1, we define metrics to evaluate both the level

of privacy and the safety performance of the ICA application. The metrics are defined below.

1) Rate of missed interventions: It is computed as $\frac{NM}{NC}$, with NM the number of *collision* instances where the ICA system never intervened before the collision occurred and NC the number of *collision* instances.

2) Rate of avoided collisions: It is computed as $\frac{NA}{NC}$, with NA the number of *collision* instances where the ICA system intervened and successfully avoided the collision and NC the number of *collision* instances.

3) Rate of failed interventions: It is computed as $\frac{NF}{NC}$, with $NF = NC - NM - NA$ the number of *collision* instances where the ICA system intervened before the collision occurred but was not able to avoid the collision and NC the number of *collision* instances. Failed interventions, although not desirable, are still preferable to missed interventions. Indeed the system's intervention, even if triggered too late to avoid the accident, can be useful to mitigate the collision.

4) Average privacy level: It is a unitless number computed over both *collision* and *no-collision* instances using the *user-centric location privacy model* introduced by Freudiger et al. [35]. In this model the privacy level of vehicle i is defined based on the *location privacy loss function* $\beta_i(t, t_{chg,i}, T_{sil,i}) : (\mathbb{R}^+, \mathbb{R}^+, \mathbb{R}^+) \rightarrow \mathbb{R}^+$ where t is the current time, $t_{chg,i} \leq t$ is the time of the last pseudonym change of vehicle i, and $T_{sil,i}$ is the duration of the silent period following the last pseudonym change. The privacy loss is set to zero after a change of pseudonym, remains zero for the duration of the silent period, then increases linearly with time according to a sensitivity parameter, $0 < \lambda < 1$ until it reaches a maximum $A_{max,i}(t_{chg,i})$. Thus, the privacy loss function is defined as follows:

$$\beta_i(t, t_{chg,i}, T_{sil,i}) = \begin{cases} 0 & \text{for } t_{chg,i} \leq t < t_{bro,i} \\ \lambda \cdot (t - t_{bro,i}) & \text{for } t_{bro,i} \leq t < t_{max,i} \\ A_{max,i}(t_{chg,i}) & \text{for } t_{max,i} \leq t \end{cases} \quad (7)$$

where $t_{bro,i} = t_{chg,i} + T_{sil,i}$ is the time at which the vehicle starts broadcasting again after a pseudonym change and a silent period, and $t_{max,i} = \frac{A_{max,i}(t_{chg,i})}{\lambda} + t_{bro,i}$ is the time when the function reaches the maximal privacy loss. Fig. 2 illustrates the evolution of the function β_i with time.
Using β_i, the privacy level $A_i(t)$ for vehicle i at time t is then computed as:

$$A_i(t) = A_{max,i}(t_{chg,i}) - \beta_i(t, t_{chg,i}, T_{sil,i}), t \geq t_{chg,i} \quad (8)$$

In practice it is generally assumed that $A_{max,i}(t_{chg,i}) = log_2(N)$, with N the number of vehicles. Therefore in our case since $N = 2$ the privacy level computation simplifies to:

$$A_i(t) = 1 - \beta_i(t, t_{chg,i}, T_{sil,i}), t > t_{chg,i} \quad (9)$$

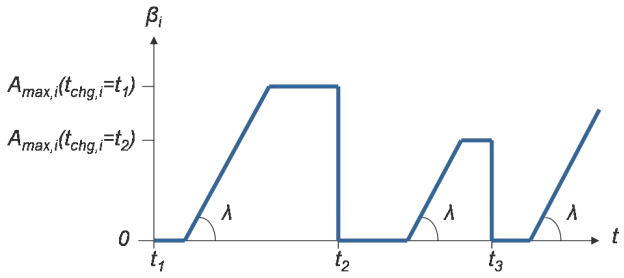

Fig. 2. Location privacy loss function β_i as a function of time. Vehicle i changes pseudonym at times $t_{chg,i} = t_1, t_2, t_3$. Each pseudonym change is followed by a silent period of random duration where the privacy loss remains zero. At the end of the silent period the privacy loss increases linearly until it reaches a maximum $A_{max,i}(t_{chg,i})$.

TABLE I
COMPARISON OF THE PRIVACY STRATEGIES DEFINED IN SECTION IV-A2 OVER ALL INSTANCES DESCRIBED IN SECTION IV-A3.

	Fixed ID	*Baseline*	*Adaptive*
Missed interventions	0.0%	30.5%	0.0%
Avoided collisions	83.0%	56.3%	83.0%
Failed interventions	17.0%	13.2%	17.0%
Average privacy level	0.37	0.98	0.94

λ models the tracking power of the adversary, therefore a higher value of λ corresponds to a faster decrease of privacy loss. As advised in [36], we use $\lambda = 0.0005$, which means that the location privacy level is equal to zero after approximately 30 minutes without a pseudonym change. In other words, it assumes that after 30 minutes an attacker can track a vehicle and identify the driver.

B. Comparative evaluation of privacy strategies

The rate of missed interventions, avoided collisions, failed interventions, and average privacy level are shown in Table I for the three tested privacy strategies.

The *Fixed ID* strategy never misses an intervention and is able to avoid 83% of the crashes. In 17% of the *collision* instances the ICA system intervened but triggering the emergency braking was not enough to avoid the collision. Typically, this happens when the OV slows down as if to stop when approaching the intersection and then accelerates at the last moment instead of stopping. The average privacy level obtained with no pseudonym changes is 0.37. Using Eq. 9, we find that this average privacy level is equivalent to the privacy level obtained after a 21 minutes long trip when the pseudonym stays fixed for the entire duration of the trip.

When applied on the same scenario instances, the *Baseline* strategy reaches an average privacy level of 0.98. Using Eq. 9, we find that this average privacy level is equivalent to the privacy level obtained after a 40 seconds long trip when the pseudonym stays fixed for the entire duration of the trip. This improvement is brought by the introduction of pseudonym changes and silent periods, but is not without consequences on the performance of the ICA system. Indeed, the *Baseline* strategy has a high rate of missed interventions (30.5%) and

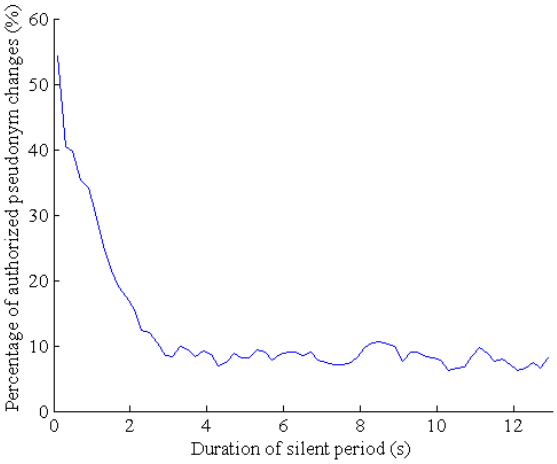

Fig. 3. *Adaptive* strategy: Percentage of authorized pseudonym changes for the Other Vehicle as a function of the duration of the silent period.

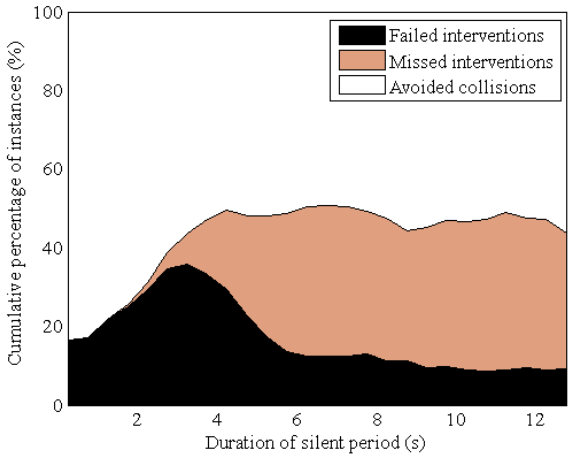

Fig. 4. *Baseline* strategy: Percentage of missed interventions, avoided collisions, and failed interventions as a function of the duration of the silent period.

a rate of avoided collisions which is 26.7% lower than the rate obtained by the *Fixed ID* strategy. The rate of failed interventions is lower for the *Baseline* strategy, but this is because some of the collisions that the *Fixed ID* strategy failed to avoid are now missed altogether by the *Baseline* strategy. The performance differences between the two strategies can be explained by the random occurrence of pseudonym changes and silent periods in the *Baseline* strategy. If a vehicle stops broadcasting information at a critical moment during *collision* instances, the ICA system may detect the danger too late.

The *Adaptive* strategy handles that issue by authorizing pseudonym changes only if they do not affect the safety application (see Section IV-A2). The results show that adding this simple check is sufficient to restore the performance of the ICA system. As with the *Fixed ID* strategy, there are no missed interventions and 83% of collisions are avoided. The difference is that thanks to the pseudonym changes and silent periods, the privacy of users is much better protected: using Eq. 9, we find that a privacy level of 0.94 is equivalent to the privacy level obtained after a 2 minutes long trip when the pseudonym stays fixed for the entire duration of the trip.

C. Impact of the silent period

In this section we analyze further the results described above and investigate the decisions made by the *Adaptive* strategy to authorize or deny pseudonym changes with random silent periods. Fig. 3 shows that the percentage of authorized pseudonym changes drops quickly from 55% to 15% as the silent period increases from 0.1 to 2 seconds. For longer silent periods, 10% of pseudonym changes are authorized on average. Intuitively these observations can be explained by the fact that traffic at road intersections is highly dynamic: situations can become dangerous very quickly, and long silent periods can result in vehicles crossing intersections without broadcasting any information. This is incompatible with the objective of the ICA to ensure safety, and explains why the

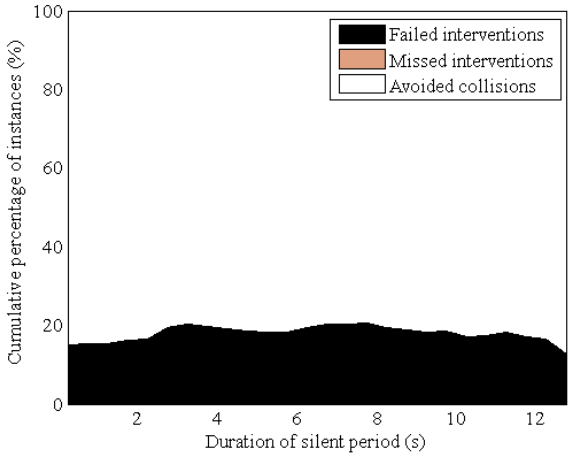

Fig. 5. *Adaptive* strategy: Percentage of missed interventions, avoided collisions, and failed interventions as a function of the duration of the silent period.

Adaptive strategy denies most pseudonym changes with silent periods longer than 2 seconds.

In order to verify this intuition we look at the distribution of missed interventions, avoided collisions, and failed interventions for different durations of the silent period. Fig. 4 shows that introducing silent periods of duration smaller than 2 seconds leads to a slight increase of the rate of failed interventions for the *Baseline* strategy: 23% failed interventions on average against of 17% for the *Fixed ID* strategy. However these short silent periods do not result in missed interventions. For silent periods of duration comprised between 2 and 3 seconds, the rate of failed interventions keeps on rising and some missed interventions start occurring. For silent periods longer than 3 seconds, and as the duration increases, failed interventions are replaced by missed interventions. These observations confirm that silent periods longer than 2 seconds strongly affect

the tested safety application, and explain why the *Adaptive* strategy rejects most of the pseudonym changes associated with long silent periods. By doing so, missed interventions are avoided and the rate of failed interventions is kept at the same level as the *Fixed ID* strategy, i.e. 17%, as shown in Fig. 5.

D. Discussion

The main goal of this paper was to analyze the impact of privacy strategies on V2X safety applications, and the results presented above highlight the necessity of a joint design. That is, the requirements of safety applications should be taken into account when designing privacy strategies, and pseudonym change schemes should be accounted for when designing safety applications which rely on V2X communications. This collaboration is necessary in order to ensure that vehicular communications and safety applications do not neutralize each other, but instead, work together toward safer roads.

For example, the analysis conducted in this paper shows that the ICA application described in [32] requires silent periods to be shorter than two seconds in order to operate correctly in conjunction with the SAE J2735 standard (implemented here under the name "*Baseline* strategy"). The results also indicate that the addition of simple rules which authorize or not a pseudonym change depending on the context (implemented here under the name "*Adaptive* strategy") leads to major safety improvements compared to the SAE J2735 standard alone. Of course these results cannot be generalized to all V2X-based safety applications, since communication requirements may vary depending on the location (e.g. highway, rural road, intersection) and the application (e.g. collision avoidance, obstacle warning, emergency vehicle warning). We believe that studies similar to this one should be conducted in order to determine some "rules of thumb" around the design of V2X safety applications and privacy strategies to ensure that they work well together.

These studies could also explore new metrics to evaluate the safety and privacy levels. Indeed, the privacy loss function used in Eq. 7 only considers a linear increase. In order to represent a more realistic privacy loss, this function could for example consider the number of messages sent with the same pseudonym, the number of encountered neighbors (e.g, anonymity set size), or even the vehicle's mobility [37].

VI. Conclusion and Future Work

Privacy is crucial in vehicular communications in order to ensure acceptance by users. To this end, the use of temporary pseudonyms has been proposed to provide a tradeoff between data privacy and security. However, this privacy mechanism is not without consequences for safety applications. In this paper we investigated the impact of pseudonym change strategies on V2X-based Intersection Collision Avoidance (ICA) systems. We considered three privacy strategies and evaluated their performance both in terms of privacy and in terms of impact on the collision avoidance system. We found that the ICA system studied in this paper can operate correctly in conjunction with the SAE J2735 standard only if silent periods are shorter than two seconds. We also found that an "adaptive" strategy which takes into account the probability of a collision to decide whether a pseudonym change should be authorized or not provides a good compromise between ICA safety and privacy level. Future work should include similar investigations for other scenarios and other safety applications. It will be useful to consider a larger road network with more vehicles and various road topologies, so as to test more complex privacy strategies.

Acknowledgement

J. Petit received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement No. 269994. This work was also partially supported by the National Science Foundation under grant No. 1239323.

References

[1] J. Ibañez-Guzmàn, C. Laugier, J.-D. Yoder, and S. Thrun, *Handbook of intelligent vehicles*. Springer, 2012, ch. Autonomous driving: context and state-of-the-art, pp. 1271–1310.

[2] U.S. Department of Transportation - National Highway Traffic Safety Administration, "Frequency of target crashes for IntelliDrive safety systems," Report DOT-HS-811-381, 2010.

[3] DRIVE-C2X project, http://www.drive-c2x.eu/project.

[4] Safety Pilot project, http://www.its.dot.gov/safety_pilot.

[5] T. Inagaki, "Technological and legal considerations for the design of interactions between human driver and advanced driver assistance systems," in *NeTWork Workshop: Control and Accountability in Highly Automated Systems*, 2011, pp. 1–12.

[6] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in *Symposium on Secure Computing, IEEE International Conference on Privacy, Security, Risk, and Trust (PASSAT '09)*, 2009, pp. 139–145.

[7] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[8] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *19th USENIX Conference Security (USENIX Sec '10)*, 2010, pp. 1–16.

[9] PReVENT project - INTERSAFE subproject, "Requirements for intersection safety applications," Deliverable D40.4, 2005.

[10] C. Frye, "International cooperation to prevent collisions at intersections," *Public Roads Magazine*, vol. 65, no. 1, 2005.

[11] J. J. Haas and Y.-C. Hu, "Communication requirements for crash avoidance," in *ACM international workshop on VehiculAr InterNETworking (VANET '10)*, 2010, pp. 1–10.

[12] J. Petit and Z. Mammeri, "Dynamic consensus for secured vehicular ad hoc networks," in *7th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '11)*, 2011, pp. 1–8.

[13] ETSI TC ITS, "ETSI TS 102 731 v1.1.1 - intelligent transport systems (ITS); security; security services and architecture," Standard, TC ITS, 2010, http://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60-/ts_102731v010101p.pdf.

[14] ——, "ETSI TS 102 941 v1.1.1 - intelligent transport systems (ITS); security; trust and privacy management," Standard, TC ITS, 2012, http://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60-/ts_102941v010101p.pdf.

[15] ——, "ETSI TS 103 097 v1.1.1 - intelligent transport systems (ITS); security; security header and certificate formats," Standard, TC ITS, 2013, http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.01.01_60-/ts_103097v010101p.pdf.
[16] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *7th International Conference Wireless On-demand Network Systems and Services (WONS '10)*, 2010, pp. 176–183.
[17] ETSI TC ITS, "ETSI TS 102 867 v1.1.1 - intelligent transport systems (ITS); security; stage 3 mapping for ieee 1609.2," Standard, TC ITS, 2012, http://www.etsi.org/deliver/etsi_ts/102800_102899/102867/01.01.01_60-/ts_102867v010101p.pdf.
[18] SAE International, "SAE J2735 V1.1.1 - Dedicated Short Range Communications (DSRC) Message Set Dictionary," Standard, 2009.
[19] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," in *International Conference Network Computing and Information Security (NCIS '11)*, 2011, pp. 141–145.
[20] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.
[21] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," in *3rd Workshop on Embedded Security in Cars (ESCAR '05)*, 2005, pp. 1–15.
[22] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," in *2nd IEEE Vehicular Networking Conference (VNC '10)*, 2010, pp. 174–181.
[23] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs," in *1st IEEE Vehicular Networking Conference (VNC '09)*, 2009, pp. 1–8.
[24] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real," in *IEEE 65th Vehicular Technology Conference (VTC '07-Spring)*, 2007, pp. 2521–2525.
[25] TASS - PreScan, http://www.tass-safe.com/prescan.
[26] TRACE project, "Accident causation and pre-accidental driving situations - In-depth accident causation analysis," Deliverable D2.2, 2008.
[27] UK Department for Transport, "National travel survey 2010," National Travel Survey statistics, https://www.gov.uk/government/publications/national-travel-survey-2010.
[28] F. Bai and H. Krishnan, "Reliability analysis of DSRC wireless communication for vehicle safety applications," in *IEEE Intelligent Transportation Systems Conference (ITSC '06)*, 2006, pp. 355–362.
[29] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance evaluation of safety applications over DSRC vehicular ad hoc networks," in *ACM international workshop on VehiculAr InterNETworking (VANET '04)*, 2004, pp. 1–9.
[30] CICAS project, http://www.its.dot.gov/cicas/index.htm.
[31] B. Roessler and K. Fuerstenberg, "First European STREP on cooperative intersection safety INTERSAFE-2," in *IEEE Intelligent Transportation Systems Conference (ITSC '10)*, 2010, pp. 422–427.
[32] S. Lefèvre, C. Laugier, and J. Ibañez-Guzmàn, "Evaluating risk at road intersections by detecting conflicting intentions," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS '12)*, 2012, pp. 4841–4846.
[33] ——, "Risk assessment at road intersections: comparing intention and expectation," in *IEEE Intelligent Vehicles Symposium (IV '12)*, 2012, pp. 165–171.
[34] K. Vogel, "A comparison of headway and time to collision as safety indicators," *Accident Analysis & Prevention*, vol. 35, no. 3, pp. 427–433, 2003.
[35] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *ACM Conference on Computer and Communications Security (CCS '09)*, 2009, pp. 324–337.
[36] J. Freudiger, M. Manshaei, J.-P. Hubaux, and D. Parkes, "Non-cooperative location privacy," *Dependable and Secure Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 84–98, 2013.
[37] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *IEEE Intelligent Vehicles Symposium (IV '07)*, 2007, pp. 541–546.