M. Bachmann, L. Hernández Acosta, J. Götz, D. Reinhardt and K. David. Collision Avoidance for Vulnerable Road Users: Privacy vs. Survival? Proceedings of the 16th Symposium on Network Operations and Management (NOMS), 2022.

Collision Avoidance for Vulnerable Road Users: Privacy versus Survival? *

Marek Bachmann, Luca Hernández Acosta*, Johann Götz, Delphine Reinhardt*, and Klaus David
Chair for Communication Technology (ComTec), University of Kassel, Kassel, Germany
*Computer Security and Privacy (CSP), University of Göttingen, Göttingen, Germany

***Abstract*—A promising approach to further increase the safety of Vulnerable Road Users (VRUs) are *cooperative* collision avoidance systems. Cooperative collision avoidance systems actively integrate the VRUs in collision detection by using movement data from a VRU's mobile device. While in recent years great attention was payed to solve technical challenges, e.g., regarding communication and sensor accuracy, little attention was payed to threats of privacy. However, the use and collection of such data poses certain privacy risks to the VRU. These privacy risks cannot be addressed by encryption alone. While some pseudonymisation approaches are used to protect the identity and location of VRUs, in this paper, we analyse to which extent the perturbation of movement data, specifically the speed data, can prevent the linkage of this data to a particular VRU, thus reducing the probability that this specific VRU can be identified. At the same time, we evaluate the trade-off between the probability of User Identification and the probability of collision detection. The evaluation is based on a standardised urban collision scenario between pedestrians and vehicles from the European New Car Assessment Programme. Our results show that privacy and "survival" are not mutually exclusive.**

***Index Terms*—privacy, data, collision avoidance, vulnerable road user**

I. Introduction

According to the "Global status report on road safety 2018" by the World Health Organization (WHO), Vulnerable Road Users (VRUs) represent more than half of all road traffic deaths, while pedestrians and cyclists make up for 26% [1]. Currently available car-based collision avoidance systems are already helpful to lower the risks of fatalities and severe injuries, but have considerable limitations especially when there is no "line-of-sight" between the vehicle and a VRU [2]. A promising approach to further increase the safety of VRUs are *cooperative* collision avoidance systems. In a cooperative collision avoidance system data from a VRU's personal mobile/wearable device, like their smartphone or smartwatch, are exchanged with data from other road users, such as cars, in order to determine the risk of an impending collision. To calculate the collision risk, at least the current linear movement information, such as position, speed, and direction, is necessary which can be derived from Global Navigation Satellite System (GNSS).

Simultaneously, such movement data can reveal information about VRUs, including their current location and other personal characteristics, such as age, health conditions [3]–[6], routines [7], and behavior [8]–[10], resulting in an increased risk for their privacy.

To prevent exploitation of confidential information about the system users by external attackers during data exchange, the use of data encryption is feasible. However, internal participants, such as other VRUs or a central server, have access to this linear movement data to perform collision detection. Thus, encryption alone is not sufficient to protect users' privacy as the data has to be accessible by the respective participants as described in more detail in Section III.

As a result, protecting privacy is more than ensuring confidentiality and covers different aspects such as the protection of user information against honest-but-curious participants.

In this paper, we propose and evaluate a speed data perturbation approach for the protection of the system users' privacy against honest-but-curious system participants. In this approach we are adding a normal distributed error to the speed values and explore whether the perturbed data can still be linked to the original data. We focus on reducing the exposure risk of private VRU information by perturbing the measured speed before this information leaves the mobile device. Following this approach, the risk of exposure of private information is reduced against honest-but-curious system providers in case of a client-server architecture and against other VRUs in case of a peer-to-peer architecture.

In parallel we analyse the impact of speed data perturbation on the probability of collision detection in terms of Missed and False Alarms. By doing so, we investigate whether both, privacy and "survival" of VRUs, can be achieved using standardised scenarios based on the European New Car Assessment Programme (Euro NCAP) [11].

The remainder of this paper is structured as follows: In Section II, the related work about privacy threats in cooperative collision avoidance systems and existing privacy-preserving solutions are reviewed. We then discuss the threat model for different system architectures of a cooperative collision avoidance system in Section III. In Section IV, we introduce a data perturbation approach and three *Key Performance Indicators* (KPIs), namely the probability of User Identification, the probability of a Missed and a False Alarm. The impact of speed perturbation on the three KPIs is then evaluated and discussed in Section V. Finally, in Section VI our conclusion is given.

*The final publication is available at IEEE Xplore via http://dx.doi.org/10.1109/NOMS54207.2022.9789710

II. Related Work

Studies, such as [12]–[15], have revealed threats to privacy resulting from road safety applications and other daily activities. Sensor data exploits have been found to reveal the identity of drivers and pedestrians: In [16], drivers could be deanonymised by analysing how the driver depressed the brake pedal using the pedal position sensor of the in-build controller-area-network. A different publication by H. M. Thang *et al.* [17] showed that pedestrians could be identified from their gait by using the accelerometer data of their mobile device.

Location and acceleration data has further been used to gather insights on the VRU's routine, health status and behaviour [5], [7], [9]. While accelerometer data can also allow to detect the decline of an elderly's walking performance and infer clinical regression [5], other privacy issues, such as information about habits, routines and personal associations (e.g. the child's school, regular trips to the doctor), can be revealed using location data [7].

To prevent honest-but-curious internal adversaries from viewing decrypted data in order to perform certain computations, homomorphic encryption could be used to allow computations to be performed on the encrypted data. However, homomorphic encryption is highly computational and might therefore only support limited functionalities [18] and does not fit to the requirements in terms of a real time collision avoidance system [19].

Several pseudonymisation methods have been introduced to protect privacy in collision avoidance systems [13], [14]. S. Lefèvre *et al.* [13] investigate different pseudonymisation schemes in road intersection scenarios and their impact on privacy by frequently changing drivers' pseudonyms. I.B. Jemaa *et al.* [14], on the other hand, investigate the impact of such pseudonymisation approaches on safety applications. Both have stated that the frequency of pseudonym changes can be obtained by an attacker, which can then be exploited to re-identify the drivers. To avoid it, silent periods, in which no pseudonym is exchanged, can be introduced to reduce the probability of tracking drivers over time.

In order to obfuscate the trajectory of people inside buildings and in road traffic, perturbation methods based on differential privacy were proposed [20], [21]. X. Zhao *et al.* [20] proposed a clustering based differential privacy approach, which adds noise to trajectory data. They investigated how privacy is impacted using different attacker models. A privacy platform for pedestrian dead reckoning was proposed by T. Feng *et al.* [21]. To calculate trajectories, they used data from Inertial Measurement Units (IMUs), such as accelerometer, gyroscope and magnetometer, and used perturbation in order to add noise and calculate pseudo-trajectories. While these studies explore the potential of differential privacy by adding noise to the movement data in indoor as well as in clustering scenarios where data is aggregated and later on analysed to obtain similarities and anomalies in datasets, the main difference in our research is that we are explicitly exploring the impact of differential privacy in a cooperative collision avoidance scenario focusing only on the perturbation of the speed data.

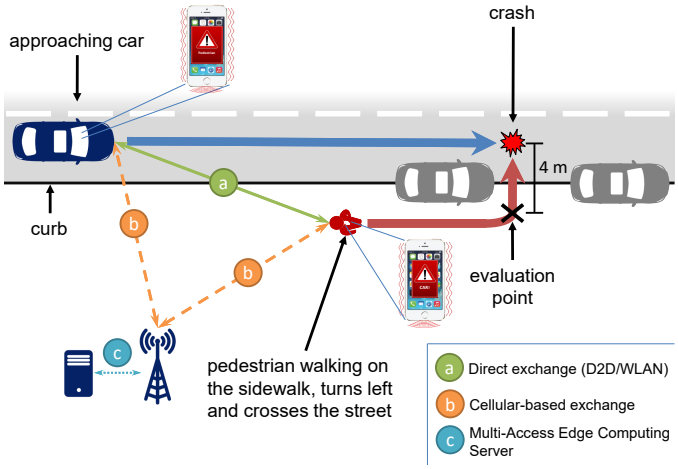

Fig. 1. Sketch of a hybrid cooperative VRU collision avoidance system for an urban collision scenario

To the best of our knowledge, the impact of data perturbation on collision detection has not yet been investigated. As a result, analysis of how data perturbation can impact the performance of collision detection algorithms in cooperative collision avoidance systems constitutes a new contribution to this field.

III. System Architectures and Threat Model

As shown in Fig. 1, in a cooperative collision avoidance system, the exchange of information can be direct (a), e.g. via wireless local area network (WLAN) or device-to-device (D2D) communication in 5G, or cellular-based (b) with an optional server, e.g., a Multi-Access Edge Computing (MEC) server (c). The algorithms for detecting collisions can be used directly on devices, or at a server. Also a combination of direct and cellular communication is possible allowing to dynamically switch between the server or the devices for collision detection calculation. Therefore, three types of architectures can be identified in terms of data exchange: client-server, peer-to-peer, and hybrid. The exchanged data can be protected against external attackers in any of these architectures by using encrypted communication. In any architecture, however, internal participants could be interested in gaining insights about other participants for purposes different from the original collision detection [22], thus threatening their privacy. In the following, we therefore adopt an honest-but-curious threat model. These honest-but-curious participants, such as the server and other VRUs, do not perform active attacks, but only listen to information they legitimately obtain [23], [24]. In what follows, we describe the possible threats in different architectures.

A. Client-Server Architecture

Movement information that is shared by VRUs with a server can be observed by the provider of the system. Despite the use

of this data to ensure collision detection, the provider may use this data for further analysis to derive personal characteristics, such as age or health status, associated with the respective VRU [3]–[6].

B. Peer-to-Peer Architecture

In a peer-to-peer architecture, data is not sent to a central server but shared directly with system participants in proximity. Therefore, other participants obtain the speed data and can leverage it to try to identify the participants over time in case of multiple encounters and specific speeds, or derive other insights about them, if they are not already able to visually observe them.

C. Hybrid Architecture

Since a hybrid architecture is a mix of client-server and peer-to-peer architectures, the threats posed by these architectures can also be found in a hybrid approach. This means that a hybrid architecture potentially poses the highest risk to privacy as data might be observable from different entities.

In summary, the roles played by the system participants in endangering others' privacy depends on the architectures involved. In terms of privacy, we have identified system providers and road users, such as drivers and VRUs, as potential attackers that gain information about others by design.

IV. Impact of data Perturbation on Collision Detection Performance

Based on Sec. III, we assume that honest-but-curious participants have access to a VRU's decrypted movement data. Our goal is hence to investigate how perturbing the data before leaving the device can preserve privacy, while maintaining the collision detection performance. To this end, we introduce the following three performance indicators. It should be noted that for our investigation, we focus on perturbing the VRU speed data in a client/server architecture.

A. Perturbation Approach

The idea of speed perturbation is to make it more difficult for a system participant to identify an individual VRU based on the VRU's known walking speed. If this speed is characteristic of an invidual VRU, it can help a system participant in linking different data to the same VRU over time, thus opening the door to the inference of additional insights about the VRU. To evaluate the speed perturbation approach, we assume a simple cooperative VRU collision avoidance system which uses collision detection for a car (c) and a pedestrian (p) based on the extrapolation of their linear movement as previously published in [25]:

Assuming linear movement, the future position $\mathbf{r}_i(t) = (x_{t_i}.y_{t_i})^T$ for the road users $i \in \{p, c\}$, depending on an extrapolating time t is given by the linear movement equation

$$\mathbf{r}_i(t) = v_i \cdot t \cdot \begin{pmatrix} \sin\phi_i \\ \cos\phi_i \end{pmatrix} + \mathbf{r}_{0_i} \tag{1}$$

where v_i is the speed, ϕ_i is the direction, and $\mathbf{r}_{0_i} = (x_i, y_i)^T$ is the current position.

Based on eq. (1), an impending collision is detected if there is a time t for which the geometry of road user p intersects with the geometry of the road user c. If there is such a t, then t is the *time-to-collision* (TTC).

Since eq. (1) is completely defined by the parameters $\mathbf{r}_{0_i}, \phi_i, v_i$, a 3-tuple

$$\mathbf{m}_i = (\mathbf{r}_{0_i}, \phi_i, v_i) \tag{2}$$

is used for referring to a specific linear movement equation in the form of eq. (1). We call $\mathbf{m}_i$ the movement vector of road user i. Accordingly, a binary function $\mathrm{col}(\mathbf{m}_p, \mathbf{m}_c)$ is used that evaluates if there is an impeding collision as follows:

$$\mathrm{col}(\mathbf{m}_p, \mathbf{m}_c) = \begin{cases} 1 & , \text{ if TTC} \geq 0 \\ 0 & , \text{ else} \end{cases} \tag{3}$$

The idea of speed perturbation is to add a normally distributed random speed perturbation value $\Delta v \sim \mathcal{N}(0, \sigma_{per}^2)$ for the pedestrian:

$$\mathbf{m}_p = (\mathbf{r}_p, \phi_p, (v_p + \Delta v)) \tag{4}$$

We refer to the standard deviation σ_{per} of the normal distribution as the perturbation rate.

B. Probability of User Identification

To explore the impact of the perturbation on VRU privacy, we consider the probability for identifying a pedestrian among others based on his/her walking speed. In our simulation, this is done by creating a set of ground truth pedestrian speed values (V_{gt}) of n different pedestrians with random normal distributed walking speeds $S \sim \mathcal{N}(\mu_s, \sigma_s^2)$ with $\mu_s = 1.4\,m/s$ and $\sigma_s = 1\,m/s$, shown in eq. (5).

$$V_{gt} = \{S_i\}, 1 \leq i \leq n,\, i \in \mathbb{N} \tag{5}$$

Our approach for perturbation is to add an additional error to the speed measurement of the pedestrian's movement. Since it was shown that measurement errors in recognising VRU movement on mobile devices can be approximated by normal distributions [25], we use normal distributed random values $P \sim \mathcal{N}(0, \sigma_{per}^2)$ to perturb each speed value which results in the set V_{per}, see eq. (6).

$$V_{per} = \{v_{per_i} | v_{per_i} = (v_i + P_i), v_i \in V_{gt}\} \tag{6}$$

To determine the results of the perturbation effect on speed data, we compare the ground truth speed data set (V_{gt}) for all pedestrians with the perturbed speed data (V_{per}) by calculating the difference between all elements of V_{gt} and V_{per}. In detail, we iterate over every element $v_{per} \in V_{per}$ and compare it with every element $v_{gt} \in V_{gt}$. By obtaining the minimum difference (Δ_{min}) we find the most similar pair of elements, shown in eq. (7).

$$\begin{aligned} \Delta_{min} = \arg\min\{v | v = |v_{gt_i} - v_{per_i}|, v_{gt_i} \in V_{gt}, \\ v_{per_i} \in V_{per}\}, 1 \leq i \leq n, i \in \mathbb{N} \end{aligned} \tag{7}$$

Thus, the probability of User Identification (P_{UI}) is defined as the percentage of false identified pedestrians of the total pedestrian count, see eq. (8),

$$P_{UI} = 1 - \frac{m}{n} \tag{8}$$

where m is the number of falsely identified pedestrians and n is the total number of pedestrians. The calculation of the number of falsely identified pedestrians (m) and P_{UI} is given in Algorithm 1. We assume that the higher we set the perturbation rate, the higher the number of falsely identified pedestrians (m), since more and more perturbed speed values are different from their ground truth value. In order to observe not only one sample, we repeat the process and compute expected values by performing multiple calculations with randomised walking speeds.

Algorithm 1 Evaluation of P_{UI} for n pedestrians

Input Perturbation rate (σ_{per}), Number of pedestrians (n)
Output P_{UI}

$v_{gt}[n]$ // Array of ground truth pedestrians' speeds
$v_{per}[n]$ // Array of perturbed pedestrians' speeds
for $i := 1, \ldots, n$ **do**
    $v_{gt}[i]$:= rand.normal(1.4, 1)
    $v_{per}[i]$:= $v_{gt}[i]$ + rand.normal(0, σ^2_{per})
$m := 0$ // Number of falsely identified pedestrians
for $i := 1, \ldots, n$ **do**
    $\Delta_{min} := \infty$
    for $j := 1, \ldots, n$ **do**
        $\Delta = |v_{per}[i] - v_{gt}[j]|$
        if $\Delta < \Delta_{min}$ **then**
            $\Delta_{min} := \Delta$
            identifiedPedestrian := j
    if identifiedPedestrian $\neq i$ **then**
        m++ // Wrong pedestrian identified
return $(1 - (m/n))$

C. Probability of Missed and False Alarms

When inaccurate movement data is used, caused by random measurement errors or random perturbation values, there is a certain probability that an impending collision might not be detected depending on the magnitude of the random inaccuracy. In the context of collision detection probability, perturbation of movement data is equivalent to an additional measurement error. An additional perturbation of speed applied on a measured movement vector $\mathbf{m}_p$, see eq. (2), of the pedestrian can therefore be expressed as eq. (9),

$$\mathbf{m}_p = \mathbf{m}_{p_{gt}} + \mathbf{m}_{p_e} + ((0\,,0), 0, \Delta v) \tag{9}$$

where $\mathbf{m}_{p_{gt}} = (\mathbf{r}_{p_{gt}}, \phi_{p_{gt}}, v_{p_{gt}})$ is the ground truth, i.e. the real, movement vector of the pedestrian, $m_{p_e} = \big((x_e, y_e)^T, \phi_e, v_e)\big)$ is the physical measurement error and $\Delta\mathbf{m}_p$ is the total inaccuracy due to measurement errors and additional speed perturbation.

TABLE I
ERROR MODEL FOR THE COOPERATIVE SYSTEM

Position error	$\boldsymbol{XY}_e \sim \mathcal{N}\left(\mathbf{0}, \begin{pmatrix} 0.44\,m & 0\,m \\ 0\,m & 0.44\,m \end{pmatrix}\right)$
Direction error	$\Phi_e \sim \mathcal{N}(0, 8.6\,^\circ)$
Total speed error	$\bar{V} \sim \mathcal{N}(0, (\sigma^2_{V_e} + \sigma^2_{per}))$

$$\Delta\mathbf{m}_p = \mathbf{m}_p - \mathbf{m}_{p_{gt}} = \big((x_e, y_e)^T, \phi_e, v_e + \Delta v\big) \tag{10}$$

Thus, to determine the probability that an impending collision is not detected due to movement recognition errors in a crash scenario depending on perturbed movement data, we use the "Probability of a Missed Alarm" (P_{MA}) which is specified in eq. (11).

$$P_{MA} = 1 - \sum_{\mathbf{m}_p \in M_{col}} P(\mathbf{m}_p) \tag{11}$$

Likewise, to determine the probability that a collision is falsely detected in a non-crash scenario, we use the "Probability of a False Alarm" (P_{FA}) which is specified in eq. (12). Both calculations for P_{MA} and P_{FA} were introduced in [26].

$$P_{FA} = \sum_{\mathbf{m}_p \in M_{col}} P(\mathbf{m}_p) \tag{12}$$

In both calculations, M_{col} is the set of all movement vectors $\mathbf{m}_p$ for which $\mathrm{col}(\mathbf{m}_p, \mathbf{m}_c) = 1$ (eq. (3)). $P(\mathbf{m}_p)$ is determined by eq. (13),

$$P(\mathbf{m}_p) = p_{\mathbf{XY}_e}(x_e, y_e) \cdot p_{\Phi_e}(\phi_e) \cdot p_{\bar{V}}(v_e + \Delta v) \tag{13}$$

where $\mathbf{XY}_e \sim \mathcal{N}(0, \sigma^2_{\mathbf{XY}_e})$ and $\Phi_e \sim \mathcal{N}(0, \sigma^2_{\Phi_e})$ are normal distributed random variables to model the measurement error for position and direction, respectively. In this context $V_e \sim \mathcal{N}(0, \sigma_{V_e})$ is the normal distributed random variable for the speed measurement error. But since the distributions of the physical speed measurement error and speed perturbation are independent, the probability of the total speed inaccuracy $(v_e + \Delta v)$ can directly be modeled as $\bar{V} \sim \mathcal{N}(0, (\sigma^2_{V_e} + \sigma^2_{per}))$. We will therefore use eq. (14)

$$\sigma_{\bar{V}} = \sqrt{\sigma^2_{V_e} + \sigma^2_{per}} \tag{14}$$

as the measure for the total speed inaccuracy comprising physical speed measurement error and speed perturbation.

V. RESULTS

To find the impact of speed perturbation on P_{UI} and P_{MA}, we conducted simulations for the crash scenarios "Crash Scenario 25%" (CRASH-25), "Crash Scenario 50%" (CRASH-50) and "Crash Scenario 75%" (CRASH-75). These scenarios are based on a standardised, representative urban collision scenario called "Car-to-Pedestrian Nearside Child 50%" (CPNC-50) from the European New Car Assessment Programme (Euro

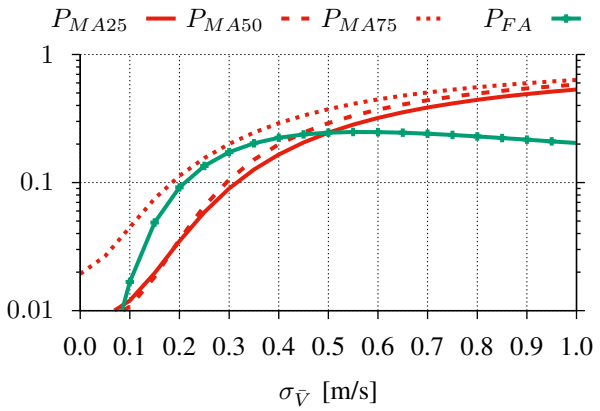

Fig. 2. Probability of a Missed (P_{MA25}, P_{MA50}, P_{MA75}) and False Alarm (P_{FA}) based on Euro NCAP depending on the total speed inaccuracy $\sigma_{\bar{V}}$

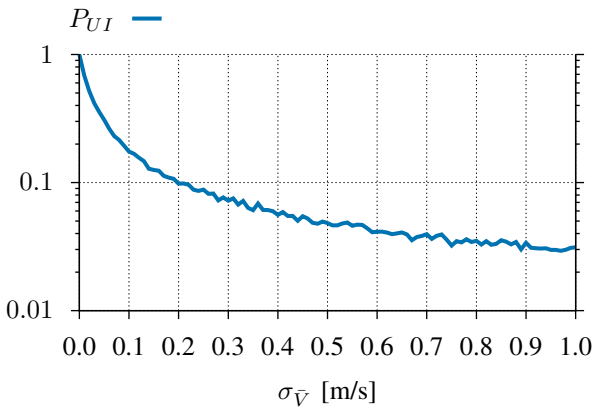

Fig. 3. Probability of User Identification (P_{UI}) for $n = 100$ pedestrians depending on the total speed inaccuracy $\sigma_{\bar{V}}$

NCAP) [11]. A sketch of the CRASH-50 scenario is shown in Fig. 1, in which a pedestrian is walking on a side walk and turns left to cross the street at a right angle. While walking, data is collected via a mobile device. The number in the scenario name, i.e., 50, refers to the impact position at the percentage of the vehicle's frontal structure width that will strike the VRU when no braking action is applied.

The Missed Alarm Probability for the 25%, 50%, and 75% collision scenarios are referred as P_{MA25}, P_{MA50}, and P_{MA75}, respectively. For convenience the following notation $P_{\{MA*\}}$ will be used to refer to all of the three collision scenarios.

For P_{FA}, the simulations were conducted based on a non-crash scenario during which the pedestrian reaches a minimum distance of $1.5\,m$ to the vehicle's frontal left structure without having a collision with the vehicle.

One simulation consists of one pedestrian represented by a circle geometry with a radius of $0.5\,m$ and a car with a rectangle geometry with a width of $2\,m$ and a length of $4\,m$, and lasts for 10 seconds. During the simulation, the speed data of the walking pedestrian's smartphone were gathered with a sampling rate of 1Hz. For each sample, this process was repeated 100 times in order to obtain the pedestrian's expected speed value. The values of $P_{\{MA*\}}$ or P_{FA} were calculated when the pedestrians were at the evaluation point, as shown in Fig. 1.

The simulations were repeated for $n = 100$ pedestrians separately, each with its own specific speed, randomly generated according to the normal distributed variable $S \sim \mathcal{N}(1.4, 1)$ and rounded to four decimal places, to calculate P_{UI}. In that way each pedestrian could easily be identified when its speed would be measured exactly. This represents the worst case scenario in terms of privacy protection, as equal speeds between participants would add additional protection.

Since it has to be assumed that any movement measurement will have a certain amount of inaccuracy, we evaluated the impact of speed perturbation in terms of the total speed inaccuracy $\sigma_{\bar{V}}$ which is an arbitrary combination of physical speed measurement accuracy (σ_{V_e}) and an additional speed perturbation rate (σ_{per}).

TABLE II
CHANGE IN THE PROBABILITY OF USER IDENTIFICATION (ΔP_{UI}), PROBABILITY OF A MISSED ALARM ($\Delta P_{MA\{25,50,75\}}$) AND PROBABILITY OF A FALSE ALARM (ΔP_{FA}) WITHIN DIFFERENT INTERVALS OF THE TOTAL SPEED INACCURACY $\sigma_{\bar{V}}$

$\sigma_{\bar{V}}\,\frac{m}{s}$	ΔP_{UI}	ΔP_{MA50}	ΔP_{FA}	ΔP_{MA25}	ΔP_{MA75}
$[\mathbf{0.0, 0.1}]$	$\mathbf{-0.823}$	$\mathbf{+0.003}$	$\mathbf{+0.016}$	$+0.004$	$+0.025$
$[0.0, 0.2]$	-0.900	$+0.028$	$+0.091$	$+0.027$	$+0.094$
$[0.0, 0.5]$	-0.950	$+0.283$	$+0.245$	$+0.237$	$+0.355$
$[0.0, 1.0]$	-0.967	$+0.610$	$+0.190$	$+0.528$	$+0.643$

As error models to calculate the $P_{\{MA*\}}$ and P_{FA} values for the cooperative collision avoidance system in accordance to eq. (13), we assumed zero-mean normal distributions, as shown in in Table I. We choose these accuracy values based on the findings for the minimum required movement recognition accuracy for cooperative VRU collision avoidance system from [25].

The probability of User Identification (P_{UI}), the Missed Alarm probabilities for the 25%, 50%, and 75% scenarios ($P_{\{MA*\}}$) and the probability of a False Alarm (P_{FA}) were calculated for values of the total speed inaccuracy $\sigma_{\bar{V}}$ in the interval of $[0.0\,\frac{m}{s}, 2.0\,\frac{m}{s}]$.

The resulting values for $P_{\{MA*\}}$ and P_{FA} are shown in Fig. 2 and the resulting values for P_{UI} are shown in Fig. 3. In Table II, it can be seen that within the interval $\sigma_{\bar{V}} \in [0.0,\ 0.1]$ the $P_{\{MA*\}}$ only slightly increases by at most 0.025. The P_{FA} in the non-crash scenario remains below 0.02 in the this interval. On the contrary, within this interval, the P_{UI} decreases significantly by ≈ 0.82 and then decreases further continuously, as shown in Fig. 3. However, increasing $\sigma_{\bar{V}}$ also effects $P_{\{MA*\}}$ to continuously increases towards 1.0, since the amount of pedestrian movement trajectories, which

lead to a collision with the car, becomes increasingly smaller compared to those which do not lead to a collision.

VI. Conclusion

In this paper, we have presented and evaluated an approach for protecting the privacy of vulnerable road users (VRUs) in cooperative collision avoidance systems. In this approach, the speed measured on the VRUs' mobile device is perturbed before leaving the device. We show that this approach makes it more difficult for an honest-but-curious system participant, e.g., system providers and other VRUs to be able to identify another VRU, which could obviously not be prevented by only encrypting the communication link.

We argued that in terms of collision detection the perturbation of speed can be interpreted and handled as an additional sensor error for speed recognition. Thus we evaluated the impact of speed perturbation in terms of total speed inaccuracy ($\sigma_{\bar{V}}$) as a combination of physical speed measurement error and additional speed perturbation.

Based on the simulations of collision and non-collision scenarios from Euro NCAP [11], it was shown, that within the interval $\sigma_{\bar{V}} \in [0.0,\ 0.1]$ of the total speed inaccuracy, the probability of User Identification can be considerably reduced by 0.82, while the probability of a Missed and False Alarm only slightly increases at most by 0.025 in the crash scenarios and by 0.016 in the non-crash scenario, respectively.

Therefore we conclude that privacy and "survival" of VRUs are not mutually exclusive. In fact, in terms of privacy protection, with the given parameters in the investigated scenarios, having a certain amount of movement data inaccuracy is advantageous due to the tolerance regarding the total speed inaccuracy for collision detection which is composed from physical measurement errors and further perturbation. The amount of additional perturbation depends on the inaccuracy due to physical measurement errors. From a privacy perspective, if this inaccuracy is low, additional perturbation should be added.

References

[1] World Health Organization, "Global Status Report on Road Safety 2018," Geneva, Switzerland.

[2] M. Bachmann, M. Morold, S. Engel, J. Götz *et al.*, "Camera vs. Cooperative VRU Collision Avoidance," in *Proc. 2020 IEEE 91st Veh. Technol. Conf. (VTC2020-Spring)*, Antwerp, Belgium, May 2020, pp. 1–5.

[3] M. Schimpl, C. Moore, C. Lederer, A. Neuhaus *et al.*, "Association Between Walking Speed and Age in Healthy, Free-Living Individuals Using Mobile Accelerometry—a Cross-Sectional Study," *PloS ONE*, vol. 6, no. 8, pp. 1–7, Aug. 2011.

[4] A. Middleton, S. L. Fritz, and M. Lusardi, "Walking Speed: The Functional Vital Sign," *Journal of Aging and Physical Activity*, vol. 23, no. 2, pp. 314–322, 2015.

[5] M. Jehn, A. Schmidt-Trucksäess, T. Schuster, H. Hanssen *et al.*, "Accelerometer-based Quantification of 6-Minute Walk Test Performance in Patients With Chronic Heart Failure: Applicability in Telemedicine," *Journal of Cardiac Failure*, vol. 15, no. 4, pp. 334–340, May 2009.

[6] J. Juen, Q. Cheng, V. Prieto-Centurion, J. A. Krishnan *et al.*, "Health monitors for chronic disease by gait analysis with mobile phones," *Telemedicine and E-Health*, vol. 20, no. 11, pp. 1035–1041, 2014.

[7] K. Shilton, "Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection," *Communications of the ACM*, vol. 52, no. 11, pp. 48–53, 2009.

[8] E. Papadimitriou, D. I. Tselentis, and G. Yannis, "Analysis of driving behaviour characteristics based on smartphone data," *Proc. of 7th Transport Research Arena (TRA)*, pp. 16–19, 2018.

[9] Y. Xun, J. Liu, N. Kato, Y. Fang *et al.*, "Automobile Driver Fingerprinting: A New Machine Learning based Authentication Scheme," *IEEE Transactions on Industrial Informatics (T-IINF)*, vol. 16, no. 2, pp. 1417–1426, Feb. 2020.

[10] J. Cordero, J. Aguilar, K. Aguilar, D. Chávez *et al.*, "Recognition of the driving style in vehicle drivers," *Sensors*, vol. 20, no. 9, p. 2597, 2020.

[11] European New Car Assessment Programme (Euro NCAP). (2020, Jun.) Test Protocol - AEB VRU systems (Version 3.0.3). Checked 14.12.2020. [Online]. Available: https://cdn.euroncap.com/media/58226/euro-ncap-aeb-vru-test-protocol-v303.pdf

[12] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *Security and Privacy in Ad-hoc and Sensor Networks*. Berlin, Heidelberg, Germany: Springer, 2007, pp. 129–141.

[13] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier *et al.*, "Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems," in *Proc. of the 5th IEEE Vehicular Networking Conference (VNC)*, Dec. 2013, pp. 71–78.

[14] I. B. Jemaa, A. Kaiser, and B. Lonc, "Study of the Impact of Pseudonym Change Mechanisms on Vehicular Safety," in *Proc. of the 9th Vehicular Networking Conference (VNC)*, Turin, Italy, Nov. 2017, pp. 259–262.

[15] L. Nkenyereye, C. H. Liu, and J. Song, "Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles," *Future Generation Computer Systems*, vol. 95, pp. 488–499, 2019.

[16] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, "Automobile Driver Fingerprinting," *Proc. of the 3rd Symposium on Privacy Enhancing Technologies (PoPETS)*, vol. 2016, no. 1, pp. 34–50, 2016.

[17] H. M. Thang, V. Q. Viet, N. D. Thuc, and D. Choi, "Gait Identification using Accelerometer on Mobile Phone," in *Proc. of the 1st IEEE International Conference on Control, Automation and Information Sciences (ICCAIS)*, Saigon, Vietnam, Nov. 2012, pp. 344–348.

[18] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can Homomorphic Encryption Be Practical?" in *Proc. of the 3rd ACM Workshop on Cloud Computing Security Workshop*, 2011, pp. 113–124.

[19] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doröz *et al.*, "Practical Homomorphic Encryption: A Survey," in *Proc. of the Xth International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2014, pp. 2792–2795.

[20] X. Zhao, D. Pi, and J. Chen, "Novel Trajectory Privacy-Preserving Method Based on Clustering Using Differential Privacy," *Expert Systems with Applications*, vol. 149, p. 113241, Jul. 2020.

[21] T. Feng, Z. Zhang, W.-C. Wong, S. Sun *et al.*, "A Privacy-Preserving Pedestrian Dead Reckoning Framework Based on Differential Privacy," in *Proc. of the 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Helsinki, Finland, Sep. 2021, pp. 1487–1492.

[22] A. Paverd, A. Martin, and I. Brown, "Modelling and Automatically Analysing Privacy Properties for Honest-But-Curious Adversaries," *Tech. Rep*, 2014.

[23] D. Reinhardt and I. Manyugin, "OP4: An OPPortunistic Privacy-Preserving Scheme for Crowdsensing Applications," in *Proc. of the 41st Conference on Local Computer Networks (LCN)*, 2016, pp. 460–468.

[24] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci *et al.*, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervasive and mobile Computing (PMC)*, vol. 9, no. 3, pp. 353–371, 2013.

[25] M. Bachmann, M. Morold, and K. David, "On the Required Movement Recognition Accuracy in Cooperative VRU Collision Avoidance Systems," *IEEE Trans. Intell. Transp. Syst*, vol. 22, no. 3, pp. 1708–1717, Mar. 2021.

[26] M. Bachmann, M. Morold, and K. David, "Improving Smartphone Based Collision Avoidance by Using Pedestrian Context Information," in *Proc. 2017 IEEE Int. Conf. on Pervasive Computing and Communications Work in Progress (PerCom WiP 2017)*, Kona, USA, Mar. 2017, pp. 2–5.