Improving Unlinkability in C-ITS: A Methodology For Optimal Obfuscation

Yevhen Zolotavkin[1][a], Yurii Baryshev[2][b], Vitalii Lukichov[2][c], Jannik Mähn[1][d]
and Stefan Köpsell[1][e]

[1] *Barkhausen Institut gGmbH, Würzburger Straße 46, Dresden, Germany*

[2] *Department of Information Protection, Vinnytsia National Technical University,*
Khmelnytske Shosse 95, Vinnytsia, Ukraine

Keywords: Privacy, V2X, Unlinkability, Hidden Markov Model, Cybersecurity, Entropy, Obfuscation.

Abstract: In this paper, we develop a new methodology to provide high assurance about privacy in Cooperative Intelligent Transport Systems (C-ITS). Our focus lies on vehicle-to-everything (V2X) communications enabled by Cooperative Awareness Basic Service. Our research motivation is developed based on the analysis of unlinkability provision methods indicating a lack of such methods. To address this, we propose a Hidden Markov Model (HMM) to express unlinkability for the situation where two vehicles are communicating with a Roadside Unit (RSU) using Cooperative Awareness Messages (CAMs). Our HMM has labeled states specifying distinct origins of the CAMs observable by a passive attacker. We then establish that high assurance about the degree of uncertainty (e.g., entropy) about labeled states can be obtained for the attacker under the assumption that he knows actual positions of the vehicles (e.g., hidden states in HMM). We further demonstrate how unlinkability can be increased in C-ITS: we propose a joint probability distribution that both drivers must use to obfuscate their actual data jointly. This obfuscated data is then encapsulated in their CAMs. Finally, our findings are incorporated into an obfuscation algorithm whose complexity is linear in the number of discrete time steps in the HMM.

1 INTRODUCTION

Due to the intense development of *transport systems* over the recent decades, different modes of cooperative intelligence have been incorporated into their functionalities. *Intelligent transport systems* (ITS) are transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort. *Cooperative Intelligent Transport Systems* (C-ITS) are a group of ITS technologies where service provision is enabled by, or enhanced by, the usage of 'live', present situation related, dynamic data/information from other entities of similar functionality, and/or between different elements of the transport network, including vehicles and infrastructure (ISO/TC 204, 2015).

Technology allowing a vehicle to exchange additional information with infrastructure, other vehicles and other stakeholders in the context of C-ITS is called *vehicle-to-everything* (V2X). Multiple advances in modern C-ITS applications, such as collaborative forward collision warning and emergency electronic brake lights, are impossible without V2X. These advances, however, come at a cost: C-ITS applications rely on vehicles broadcasting signals to indicate their location, signals which are intended to be received and processed by a range of other devices. For example, vehicles may cooperatively broadcast (with the frequency of 1-10 Hz) geo-spatial information to nearby peers using short Cooperative Awareness Messages (CAMs). Hence, V2X raises essential *privacy questions*: ***i)*** to what degree can specific vehicles be located and tracked based on such information? ***ii)*** what are the techniques able to improve privacy of V2X? To answer these questions, we use the concept of *unlinkability* to reason about privacy.

[a] https://orcid.org/0000-0002-1875-122X
[b] https://orcid.org/0000-0001-8324-8869
[c] https://orcid.org/0000-0002-3423-5436
[d] https://orcid.org/0000-0003-0870-7193
[e] https://orcid.org/0000-0002-0466-562X

Zolotavkin, Y., Baryshev, Y., Lukichov, V., Mähn, J. and Köpsell, S.
Improving Unlinkability in C-ITS: A Methodology For Optimal Obfuscation.
DOI: 10.5220/0011786900003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 677-685
ISBN: 978-989-758-624-8; ISSN: 2184-4356

1.1 Research Motivation

Even though the problems of privacy in C-ITS were acknowledged in several relevant documents (having normative and informative character), satisfactory answers have yet to be provided to the privacy questions mentioned above. For example, the document (ISO/TC 204, 2018) recognizes the importance of unlinking private data from traceable address elements and identifiers in wireless messages sent by an ITS station unit (ITS-SU). However, relevant considerations in this document do not go beyond suggesting that "such unlinking can be done by means of pseudonyms": the sufficiency of these and many similar suggestions remain unaddressed. In contrast, limitations of pseudonym changes in CAMs have been recognized by academic authors (Wiedersheim et al., 2010; Karim Emara, 2013; Escher et al., 2021). In particular, vehicle tracking becomes possible due to CAM content being signed but *not encrypted*: this is demanded by the relevant standards in C-ITS (WG1, 2019). This is because full encryption of CAMs may impede C-ITS functionalities that are critical for safety. Nonetheless, recognition of privacy-affecting issues in C-ITS has yet to result in a solution where the degree of privacy is correctly measured, and privacy limitations are eliminated. In this paper, a methodology to address these challenges is developed: we provide an assurance for the procedure estimating the lower bound of unlinkability for CAMs and an algorithm maximizing this criterion under the overall constraint of location precision degradation.

1.2 Our Contribution

The unique contribution is due to combination of the study objective (guided by the criterion of unlinkability), robust assumptions, and the optimal obfuscation technique developed in the paper.

- First, the aim of this study is to protect C-ITS from the *threat of linking*: this is in contrast with the numerous obfuscation approaches which aim at impeding inferencing about the actual location of ITS-SU (Andrés et al., 2013; Bordenabe et al, 2014);
- Second, to obtain *high confidence* in the measured unlinkability, we assume that an attacker has complete knowledge about the system design, obfuscation algorithms, quality degradation (distortion) constraints, has access to CAMs, stored states vehicles' geo-positions, and the true states characterizing the geo-positions of the vehicles at any moment in time;
- Third, we develop an *optimal obfuscation* algorithm: for a given distortion constraint, it provides the highest level of uncertainty for the attacker trying to link obfuscated CAMs with their sources.

The rest of this paper is structured as follows. In section 2, we set the grounds for the study and provide basic definitions. It is followed by section 3, where we propose Hidden Markov Model (HMM), used to study unlinkability. In section 4, we formalize assumptions, define unlinkability through entropy and optimize joint obfuscation producing observable states in HMM. Next, section 5 describes a compact and efficient algorithm calculating the unlinkability in C-ITS and implementing previous findings to improve privacy. Finally, we conclude[1] the paper in section 6.

2 PRELIMINARIES

To justify subsequent modelling steps better, we introduce contextual information supporting our aim, settings and privacy assumptions.

2.1 Aim of the Study

To specify the aim, we analyze relevant cybersecurity requirements. Here, we use some of the classical definitions for privacy in complex systems to specify our aim with greater precision. Privacy requirements for C-ITS are often derived from ISO/IEC 15408-2. For example, (WG5, 2021) suggests that the combination of pseudonymity and unlinkability offers the appropriate sender privacy protection for basic ITS safety messages (such as CAM). In simple terms, *pseudonymity* requires that the identity of a user is never revealed or inferred. However, one of the major complications in dealing with pseudonymity is the following: an attacker may learn the user's identity composition based on multiple sessions, events, or traces. *Unlinkability* is the assurance about the ability to resist learning such a composition (ISO/IEC JTC 1/SC 27, 2022):

Definition 1 (Unlinkability of Operations). Requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system, or whether operations are related in some other manner.

In the context of V2X communication in C-ITS with many users, the cryptographically signed mes-

[1] For an in-depth discussion, see the full version of the paper (Zolotavkin et al., n.d.)

sages broadcasted by the ITS-SUs (controlled by these users) should have the property of definition 1 (WG5, 2021; Hicks eta al., 2020). Nonetheless, such interpretation has certain disadvantages, major of which is inflexibility. Indeed, *'...unable to determine...'* statement can either be false or true, meaning that the unlinkability of the whole C-ITS (with many vehicles and observable during many hours) is expressed using a binary value. This issue has been recognized by practitioners and researchers alike, which is reflected in comments and best practice recommendations to ITS engineers and managers. For example, (ISO/TC 22/SC 32, 2021) contains the table *'Example privacy impact rating criteria'*: it includes *Impact rating Criteria* interpreting the meaning for the severity degrees (e.g., Negligible, Moderate, Major, Severe) for *privacy impact rating* indicator. Importantly enough, interpretations in this table evolve around two aspects: a) the level of sensitivity of the information about road user; b) *how easily* it can be linked to a PII (Personally Identifiable Information) principal. Such emphasis on the *easiness of linking* motivates us to modify definition 1 in the following manner:

Definition 2 (Unlinkability of Operations*). Is the degree of inability to determine (by users and/or subjects) whether the same user caused certain specific operations in the system, or whether operations are related in some other manner.

To provide convenience in comparing unlinkability in C-ITS under different conditions, we use Shannon entropy: it is an integral criterion of uncertainty in a system that fully captures the *'...degree of inability to determine...'* (Wagner and Eckhoff, 2018).

Henceforth, the ***main aim*** of our paper is to develop a methodology providing high level of assurance that *entropy for CAMs' origins* is high in C-ITS.

2.2 Settings for the Study

In fig. 1, we introduce a general setup for our study. In fig. 1(a), two vehicles (ITS-SUs) are driven by *Alice* and *Bob*, respectively. Both ITS-SUs transmit CAMs with the same frequency, and the roadside unit (RSU) receives them without losses. The role of the *attacker* is played by the RSU, who tries to separate CAMs of *Alice* from CAMs of *Bob*: this allows the attacker to *link* CAMs belonging to the same entity. Although CAMs are signed, in our study we assume that a signature scheme providing unlinkability is used. Therefore, the separation is done based on the content of the CAMs (since the are transmitted unencrpyted) and the order of arrival of CAMs within each time interval – see fig. 1(b). We consider the ordering of CAMs' arrivals to be non-uniform in general: for example, in one extreme case, the CAM from *Alice* arrives first, and *Bob*'s CAM arrives second at any time interval *i*. If an attacker knows about such a unique property, he can link CAMs without considering their payload. However, these cases are unlikely, meaning that an attacker should also be able to infer the source (e.g., 'from *Alice*' or 'from *Bob*') of a CAM based on its content. The requirements for the content of CAMs can be found in (WG1, 2019). In particular, we consider that geo-position, velocity and acceleration are essential. On the one hand, these parameters are mandatory for the `HighFrequency` container in CAM. On the other hand, numerous techniques using these parameters have been developed for the domain of Multiple-Target Tracking (MTT): corresponding estimators can be of great use for reasoning about privacy in C-ITS (Blackman, 1986; Karim Emara, 2013).

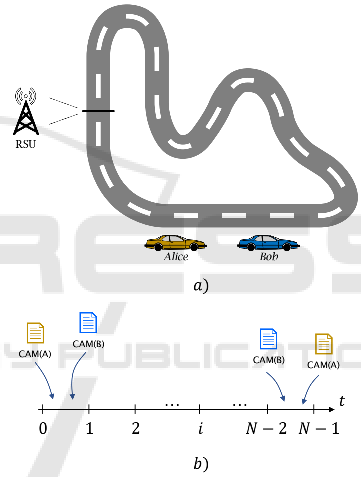

Figure 1: Setting for our study of unlinkability of CAMs.

In this study, CAMs' content unlinkability is the core of our attention. We exclude from further consideration the following CAM payload: *1)* cryptographically produced proofs of authenticity (e.g., signatures); *2)* categorical data (e.g., vehicle role). These exclusions are due to substantial attention to issue '*1)*' among the members of the cryptographic community. For example, pseudonym unlinking solutions were proposed in (Camenisch et al., 2020; Hicks eta al., 2020). Nevertheless, there is a need to complement these efforts by our study: the absence of encryption (due to safety reasons) in CAMs makes pseudonym unlinking necessary but *not sufficient* for CAMs' unlinkability. This is because other data, such as geographic positions, in CAMs may be used for linking. Issue '*2)*' can be omitted since categorical data is a part of `basicVehicleContainerLowFrequency` and is `OPTIONAL` in CAMs (WG1, 2019). We also exclude

`VehicleLength` and `VehicleWidth` (compulsory for the `HighFrequency` container), which otherwise are likely to be of great use in discriminating different vehicles (Escher et al., 2021). For such an exclusion we find justification in (WG1, 2018) which allows usage of the codes 1023 and 62 for the length and width, respectively, if the corresponding information is unavailable.

Because of the details described above, we will model CAM as a vector in $\mathbb{R}^z$ where $z \geq 1$. Such a step is beneficial: we can apply commonly used distortion measures such as, for example, Squared Error (SE). This is a clear and straightforward way to refer to the quality degradation of essential location services (Shokri et al., 2016). We, nevertheless, refrain from further discussions about the chosen distortion measure in this paper.

2.3 Privacy Assumptions and Threats

Here we provide a high-level intuition for the system and the threat of *linkability*, while the details will be introduced in the subsequent sections. *Alice* and *Bob* coordinate their efforts. They distribute the total allowed distortion among $N-1$ time steps: as a result, they know the distortion limit for every time step i. At the beginning of every time interval i, *Alice* and *Bob* know the true measurements (including position, speed, acceleration, etc.) of each other. To obfuscate data in their CAMs they randomly agree on the order of their arrival at RSU at every i. For every i they define a joint distribution according to which they change (obfuscate) their actual measurements: in expectation, they remain within the distortion limits.

An *attacker* who fully controls RSU statistically infers the source of every pair of CAMs which he observes during time i: this statistical inference is used to calculate entropy and aligns with definition 2. For this, the attacker refers to the joint distribution used by *Alice* and *Bob* during the obfuscation. He also knows other information, such as the original geo-positions of the players at every i, and the probabilities for the order of CAMs' arrivals. The resulting unlinkability in the system depends on: i) statistics for the order of arrival of CAMs from the players; ii) the level of allowed distortion; iii) how far apart actual measurements of *Alice* and *Bob* are at every i.

3 MATHEMATICAL MODEL

We explain our mathematical model in the following sections. To easy the reading, table 1 contains an overview about our notations.

Table 1: Notations.

Notation	**Description**
ITS	Intelligent Transport Systems
C-ITS	Cooperative Intelligent Transport Systems
ITS-SU	ITS Station Unit (including installed in vehicles)
V2X	Vehicle-to-Everything
CAM	Cooperative Awareness Message
RSU	Roadside Unit
HMM	Hidden Markov Model
$\mathbf{D}_u$	Set of user-related data
$\mathbf{D}_s$	Set of information system-related data
$\mathbf{U}$	Set of information system's users
$\mathbf{P}$	Set of data processing procedures at the information system
$\mathbb{P}$	Set of players including *Alice* and *Bob*
$x_k^A,\ 1 \leq k \leq \mu$	A hidden state for *Alice*
$\mathbb{X}^A = \{x_k^A\}$	Set of hidden states for *Alice*
$x_j^B,\ 1 \leq j \leq \omega$	A hidden state for *Bob*
$\mathbb{X}^B = \{x_j^B\}$	Set of hidden states for *Bob*
$\mathbb{X}^{(A,B)}$	Set of joint hidden states for $\langle Alice,\ Bob \rangle$
$\mathbb{X}^{(B,A)}$	Set of joint hidden states for $\langle Bob,\ Alice \rangle$
$\mathcal{R}$	Index (label) for rose nodes
$\mathbb{X}_{\mathcal{R}} = \mathbb{X}^{(A,B)}$	Set of all rose nodes
$\mathcal{B}$	Index (label) for blue nodes
$\mathbb{X}_{\mathcal{B}} = \mathbb{X}^{(B,A)}$	Set of all blue nodes
$\mathbb{L} = \{\mathcal{R}, \mathcal{B}\}$	Set of labels encoding $\lvert\mathbb{P}\rvert!$ combinations
$\mathbb{Y}$	Set of joint observable states for *Alice* and *Bob*
$i \in \{1, 2, ..., N-1\}$	Time-step in discrete HMM
X_i^A	Variable on $\mathbb{X}^A$ at i
X_i^B	Variable on $\mathbb{X}^B$ at i
$\mathbf{X}_i$	Variable for joint hidden state on step i
ℓ_i	Variable on $\mathbb{L}$ at i
$\mathbf{Y}_i$	Variable on $\mathbb{Y}$ on step i
$\Pr(\mathbf{X}_{i+1} \mid \mathbf{X}_i)$	Probability of transition between hidden states
$\Pr(\mathbf{Y}_i \mid \mathbf{X}_i)$	Conditional probability for observable states
φ	Order mixing (label permuting) probability
ρ_i	Distribution over hidden states on step i
$\rho_{i+1} \lvert \rho_i$	Conditional distribution over hidden states on step $i+1$

3.1 Markov Model for Unlinkability

To study unlinkability in V2X we use Hidden Markov Model which graphical representation is given on fig. 2. The following sets are needed to describe the model. The set of all players is $\mathbb{P} = \{Alice,\ Bob, ...\}$. For each player, there exists a set of hidden states for his vehicle, e.g., for *Alice* there is $\mathbb{X}^A = \left\{x_1^A, x_2^A, ..., x_k^A, ..., x_\mu^A\right\}$ and for *Bob* there is $\mathbb{X}^B = \left\{x_1^B, x_2^B, ..., x_j^B, ..., x_\omega^B\right\}$. Each state, for example, x_1^A can be a vector including specific position, velocity, acceleration and other characteristics applicable to *Alice's* vehicle at certain time. Throughout the paper we assume that $\mathbb{X}^A \cap \mathbb{X}^B$ is in general non-empty.

The system of $|\mathbb{P}|$ players is characterized by hidden and observable joint states. Transition happens between hidden states $\mathbf{X}_i$ and $\mathbf{X}_{i+1}$ when time step i proceeds to $i+1$, where joint state $\mathbf{X}_i = \left(X_i^A, X_i^B\right)$ is the composition (concatenation) of variables $X_i^A \in \mathbb{X}^A$ and $X_i^B \in \mathbb{X}^B$. As such, $\forall k, j (x_k^A, x_j^B) \in \mathbb{X}^{(A,B)}$, where $|\mathbb{X}^{(A,B)}| = |\mathbb{X}^A| \times |\mathbb{X}^B|$ (for simplicity of representation we further assume $|\mathbb{P}| = 2$, $|\mathbb{X}^A| = \mu = 2$, $|\mathbb{X}^B| = \omega = 2$).

Possible transitions from $\mathbf{X}_i$ to $\mathbf{X}_{i+1}$ are denoted using indices $1-16$ (see fig. 2): these transitions are governed by corresponding probabilities. For example, the transition from $\mathbf{X}_i = \left(X_i^A = x_1^A, X_i^B = x_1^B\right)$ to $\mathbf{X}_{i+1} = \left(X_{i+1}^A = x_2^A, X_{i+1}^B = x_2^B\right)$ is denoted by index 4. The probability of such a transition is $\Pr\left(X_{i+1}^A = x_2^A, X_{i+1}^B = x_2^B \mid X_i^A = x_1^A, X_i^B = x_1^B\right)$. In practice, these probabilities can be obtained based on the well-studied physical models for vehicles (Blackman, 1986).

For each $\mathbf{X}_i$ of the hidden joint states there are $|\mathbb{P}|!$ possible permutations for its concatenated components originating from the users. These permutations are the major cause of uncertainty when an attacker attempts to label combined CAMs of *Alice* and *Bob*. In practice, this is caused by the unpredictable arrangement of CAMs within each scan (or session) i. Hence, a permutation should be selected by randomly following one of the possible transitions. For example, while the system is in a joint state $\left(X_i^A = x_1^A, X_i^B = x_1^B\right)$ permutation $\left(x_1^A, x_1^B\right)$ (rose colored node) should be considered if transition with index 17 takes place, and $\left(x_1^B, x_1^A\right)$ (blue coloured node) should be considered if transition 18 happens (see fig. 2). We will use notations $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$ for rose and blue nodes, respectively, where $\mathbf{X}_{i,\mathcal{R}} \in \mathbb{X}_{\mathcal{R}}$, $\mathbf{X}_{i,\mathcal{B}} \in \mathbb{X}_{\mathcal{B}}$, and $\mathbb{X}_{\mathcal{R}} = \mathbb{X}^{(A,B)}$, $\mathbb{X}_{\mathcal{B}} = \mathbb{X}^{(B,A)}$. Further in the text, we will refer to the states represented by the coloured nodes as 'labelled states'. For the sake of simplicity and without loss of generality, for all realizations of hidden states $\mathbf{X}_i$, we consider $\Pr\left(\mathbf{X}_{i,\mathcal{R}} | \mathbf{X}_i\right) = \varphi \leq 0.5$, and $\Pr\left(\mathbf{X}_{i,\mathcal{B}} | \mathbf{X}_i\right) = 1 - \varphi$.

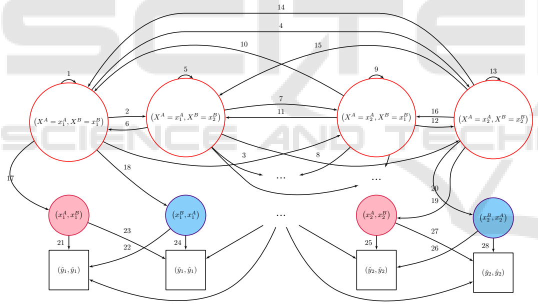
14
4
10
15
1
5
9
13
$(X^A = x_1^A, X^B = x_1^B)$
2
6
$(X^A = x_1^A, X^B = x_2^B)$
7
11
$(X^A = x_2^A, X^B = x_1^B)$
16
12
$(X^A = x_2^A, X^B = x_2^B)$
3
8
17
18
...
...
20
19
(x_1^A, x_1^B)
(x_1^B, x_1^A)
...
(x_2^A, x_2^B)
(x_2^B, x_2^A)
23
22
21
24
25
27
26
28
$(\hat{y}_1, \check{y}_1)$
$(\check{y}_1, \hat{y}_1)$
$(\hat{y}_2, \check{y}_2)$
$(\check{y}_2, \hat{y}_2)$

Figure 2: Hidden Markov Model for 2 players sending CAMs.

To denote the totality of hidden permuted joint states we use set $\mathbb{X}_{\{\mathcal{R},\mathcal{B}\}} = \mathbb{X}_{\mathcal{R}} \cup \mathbb{X}_{\mathcal{B}}$, where $|\mathbb{X}_{\mathcal{R}}| \leq |\mathbb{X}_{\{\mathcal{R},\mathcal{B}\}}| \leq 2|\mathbb{X}_{\mathcal{R}}|$. For every $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$ there are transitions to observable joint states $\mathbf{Y}_i \in \mathbb{Y}$, $\mathbb{Y} = \left\{(\hat{y}_1, \check{y}_1), (\check{y}_1, \hat{y}_1), ..., (\hat{y}_q, \check{y}_q), (\check{y}_q, \hat{y}_q), ..., (\hat{y}_\xi, \check{y}_\xi), (\check{y}_\xi, \hat{y}_\xi)\right\}$. Some of these transitions to observable states are denoted with indices $21 - 28$ on fig. 2. Until proven otherwise, the cardinality of $\mathbb{Y}$ is considered independent on $|\mathbb{X}_{\{\mathcal{R},\mathcal{B}\}}|$.

Measuring uncertainty about label $\ell \in \mathbb{L}$, $\mathbb{L} = \{\mathcal{R}, \mathcal{B}\}$, is of our main interest: this is done based on observable states.

4 MODEL PROPERTIES

To formally express unlinkability following definition 2 we will use conditional entropy $H\left(\ell_1, \ell_2, ... | \mathbf{Y}_1, \mathbf{Y}_2, ...\right)$ for the sequence of labels $\ell_1, \ell_2, ..., \ell_{N-1}$ given that an attacker observes $\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_{N-1}$ (Wagner and Eckhoff, 2018).

4.1 General Expression for Unlinkability

For the described HMM, probability of any hidden state at any time step can be specified using multivariate discrete distribution $\boldsymbol{\rho} : \mathbb{X}^{(A,B)} \times \{0, 1, ..., N-1\} \rightarrow [0,1]^{N|\mathbb{X}^{(A,B)}|}$. We will further use ρ_i slices of $\boldsymbol{\rho}$ such that $\boldsymbol{\rho} = \bigcup\limits_{i=0}^{N-1} \rho_i$, where each slice represents a distribution over hidden states at step i. Slice ρ_0 defines distribution over the hidden states before the start of the system. Because HMM has been previously defined (see fig. 2) using transitional probabilities that remain unchanged for all time steps, each slice can be fully determined in a conditioned sequential manner: $\rho_{i+1} | \rho_i$ means that ρ_{i+1} is trivially derived if ρ_i is given.

Since an attacker observes $\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_{N-1}$ and knows $\boldsymbol{\rho}$ analysis of $H\left(\ell_1, \ell_2, ... \mid \mathbf{Y}_1, \mathbf{Y}_2, ..., \boldsymbol{\rho}\right)$ is central to our reasoning about unlinkability. We state the following.

Lemma 1. Unlinkability in V2X system (as per fig. 2) is expressed as:[2]

$$H\left(\ell_1, \ell_2, ... \middle| \mathbf{Y}_1, \mathbf{Y}_2, ..., \boldsymbol{\rho}\right) = \sum_{i=0}^{N-2} H\left(\ell_{i+1} \middle| \mathbf{Y}_{i+1}, \{\rho_{i+1} | \rho_i\}\right) . \tag{1}$$

4.2 Worst-Case Unlinkability

We aim to obtain a computationally feasible estimation of unlinkability. Direct utilization of the results of lemma 1 presupposes computing $\{\rho_{i+1} | \rho_i\}$ which has several disadvantages: *a)* transition probabilities for hidden states need to be specified (which usually requires studying physical models of movement for the users); *b)* total computational complexity for defining distributions over the hidden states is therefore $O(N\mu^2\omega^2)$. To avoid these complications, we develop our unlinkability assurance based on a *rational lower bound* $\mathcal{H}_r$ for $H\left(\ell_1, \ell_2, ... \middle| \mathbf{Y}_1, \mathbf{Y}_2, ..., \boldsymbol{\rho}\right)$. The concept of the rational lower bound is explained through the following assumptions (Sniedovich, 2016).

[2] For proof, see the full version of the paper (Zolotavkin et al., n.d.)

Assumption 1 (Worst-Case Unlinkability). Requires that an attacker knows sets for the hidden, labelled and observable states. He knows all the transitions and the order mixing probability φ. For each observable state at time i he then defines the worst possible hidden state(s) which does not contradict his knowledge.

We nevertheless stress that despite assumption 1 might be viewed as excessive, the attacker does not know the labelled state ℓ_i (and can not force its selection) at time i.

Assumption 2 (Rational Lower Bound $\mathcal{H}_{\mathrm{r}}$). Requires that users are rational and maximize worst-case unlinkability: observable states are obtained through rational obfuscation of the worst labelled states considered by the attacker.

There are several aspects affecting the task of calculating such $\mathcal{H}_{\mathrm{r}}$: 1) probabilities for transitions between hidden states (e.g., the probabilities defining $\boldsymbol{\rho}$); 2) probabilities for transitions from the hidden states to the labelled states (e.g., φ, $1-\varphi$), and from the labelled states to the observable states. Further, we consider a situation where the worst case $\boldsymbol{\rho}$ (*minimizing entropy*) is defined for 1) while the most optimal probabilities (*maximizing entropy*) are then specified for 2) under constraint $\tilde{D}$ on the total distortion over $N-1$ steps.

We use the results of lemma 1 to require the following:

$$\mathcal{H}_{\mathrm{r}} = \min_{\boldsymbol{\rho}} \Big[H\left(\ell_1, \ell_2, ... \middle| \mathbf{Y}_1, \mathbf{Y}_2, ..., \boldsymbol{\rho}\right) \Big] = \sum_{i=0}^{N-2} \min_{\{\rho_{i+1}|\rho_i\}} \Big[H\left(\ell_{i+1} \middle| \mathbf{Y}_{i+1}, \{\rho_{i+1}|\rho_i\}\right) \Big] . \tag{2}$$

To obfuscate hidden states in the way maximizing $\mathcal{H}_{\mathrm{r}}$ we need to determine properties of

$$\rho_{\min,i+1} = \arg \min_{\{\rho_{i+1}|\rho_i\}} \Big[H\left(\ell_{i+1} \middle| \mathbf{Y}_{i+1}, \{\rho_{i+1}|\rho_i\}\right) \Big] . \tag{3}$$

Probabilities $\Pr\left(\ell_{i+1} = \mathcal{R}, \mathbf{Y}_{i+1} \middle| \{\rho_{i+1}|\rho_i\}\right)$, $\Pr\left(\ell_{i+1} = \mathcal{B}, \mathbf{Y}_{i+1} \middle| \{\rho_{i+1}|\rho_i\}\right)$ will be used in our further derivations. To simplify notations we will use $\Pr(\ell_{i+1} = \mathcal{R}, \mathbf{Y}_{i+1})$, $\Pr(\ell_{i+1} = \mathcal{B}, \mathbf{Y}_{i+1})$, respectively. The probabilities are defined as:

$$\begin{aligned} \Pr(\ell_{i+1} = \mathcal{R}, \mathbf{Y}_{i+1}) &= \\ \sum_{\mathbf{X}_{i+1,\mathcal{R}} \in \mathbb{X}_{\mathcal{R}}} &\Pr\left(\mathbf{Y}_{i+1} \mid \mathbf{X}_{i+1,\mathcal{R}}\right) \Pr\left(\mathbf{X}_{i+1,\mathcal{R}}\right) = \\ \sum_{\mathbf{X}_{i+1,\mathcal{R}} \in \mathbb{X}_{\mathcal{R}}} &\Pr\left(\mathbf{Y}_{i+1} \mid \mathbf{X}_{i+1,\mathcal{R}}\right) \varphi \Pr\left(\mathbf{X}_{i+1}\right) , \end{aligned} \tag{4}$$

$$\begin{aligned} \Pr(\ell_{i+1} = \mathcal{B}, \mathbf{Y}_{i+1}) &= \\ \sum_{\mathbf{X}_{i+1,\mathcal{B}} \in \mathbb{X}_{\mathcal{B}}} &\Pr\left(\mathbf{Y}_{i+1} \mid \mathbf{X}_{i+1,\mathcal{B}}\right) \Pr\left(\mathbf{X}_{i+1,\mathcal{B}}\right) = \\ \sum_{\mathbf{X}_{i+1,\mathcal{B}} \in \mathbb{X}_{\mathcal{B}}} &\Pr\left(\mathbf{Y}_{i+1} \mid \mathbf{X}_{i+1,\mathcal{B}}\right) (1-\varphi) \Pr\left(\mathbf{X}_{i+1}\right) . \end{aligned} \tag{5}$$

We then point out that

$$\Pr(\ell_{i+1} = \mathcal{R} \mid \mathbf{Y}_{i+1}) = \frac{\Pr(\ell_{i+1} = \mathcal{R}, \mathbf{Y}_{i+1})}{\Pr(\mathbf{Y}_{i+1})} , \tag{6}$$

$$\Pr(\ell_{i+1} = \mathcal{B} \mid \mathbf{Y}_{i+1}) = \frac{\Pr(\ell_{i+1} = \mathcal{B}, \mathbf{Y}_{i+1})}{\Pr(\mathbf{Y}_{i+1})} , \tag{7}$$

where

$$\Pr(\mathbf{Y}_{i+1}) = \Pr(\ell_{i+1} = \mathcal{R}, \mathbf{Y}_{i+1}) + \Pr(\ell_{i+1} = \mathcal{B}, \mathbf{Y}_{i+1}) . \tag{8}$$

The following result establishes an important property of $\rho_{\min,i+1}$.

Lemma 2. For all $i \in [1, N-1]$ distribution $\rho_{\min,i}$ is degenerate.[3]

Based on the result of lemma 2, for every $\mathbf{Y}_i$ there is one and only worst-case hidden state $\tilde{\mathbf{X}}_i$ (because $\Pr\left(\tilde{\mathbf{X}}_i \mid \rho_{\min,i}\right) = 1$). It implies the following:

Corollary 1. Design of HMM where for every state (realization) in $\mathbb{Y}$ there is one and only transition from $\mathbb{X}^{(A,B)}$ explicitly satisfies assumption 1.

Therefore, we will further adhere to such design principle and use $\tilde{\mathbf{X}}_i$ to denote hidden states. Next, we will elaborate on: *a)* what is the optimal number of different observable states $\mathbf{Y}_i$ for every $\tilde{\mathbf{X}}_i$? *b)* how should we define optimal observable states? *c)* what are the probabilities of transition (from the labelled states to the observable states)?

4.3 Requirements for the Observable States

Here we provide our analysis from the standpoints of the system that obfuscates hidden states (e.g., the system produces observable states) on behalf of *Alice* and *Bob*, and hence $\tilde{\mathbf{X}}_i$ is assumed to be known. The possibilities of transitions $\tilde{\mathbf{X}}_{i,\mathcal{R}} \rightarrow \mathbf{Y}_i$ and $\tilde{\mathbf{X}}_{i,\mathcal{B}} \rightarrow \mathbf{Y}_i$ imply that a non-zero distortion $\mathbb{E}[D_i]$ takes place:

$$\mathbb{E}[D_i] = \sum_{\mathbf{y}_j^{(i)} \in \mathbb{Y}^{(i)}} D_{i,j} \Pr\left(\mathbf{Y}_i = \mathbf{y}_j^{(i)} \mid \tilde{\mathbf{X}}_i\right) , \tag{9}$$

where

$$\begin{aligned} D_{i,j} = &\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right) d\left(\tilde{\mathbf{X}}_{i,\mathcal{R}}, \mathbf{y}_j^{(i)}\right) + \\ &\Pr\left(\ell_i = \mathcal{B} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right) d\left(\tilde{\mathbf{X}}_{i,\mathcal{B}}, \mathbf{y}_j^{(i)}\right) . \end{aligned} \tag{10}$$

Here $\mathbb{Y}^{(i)}$ is the set of all observable states to which transitions exist from the realizations of $\tilde{\mathbf{X}}_{i,\mathcal{R}}$ and $\tilde{\mathbf{X}}_{i,\mathcal{B}}$ at time i; $\mathbf{y}_j^{(i)}$ is an element in $\mathbb{Y}^{(i)}$; $d(\cdot,\cdot)$ is some distortion measure (e.g., SE).

The optimization effort is two-fold: *i)* how shall we obtain observable states $\mathbb{Y}^{(i)}$ in a way that $\mathcal{H}_{\mathrm{r},i}$

[3] For proof, see the full version of the paper (Zolotavkin et al., n.d.)

is maximized under constraint $\tilde{D}_i \geq \mathbb{E}[D_i]$? *ii)* how shall we define $\tilde{D}_i$ for every time step i such that $\mathcal{H}_{\mathrm{r}}$ is maximized and the total distortion constraint $\tilde{D} \geq \sum_i \mathbb{E}[D_i]$ is satisfied? We start with answering question *i)*, which will assist us in answering question *ii)*.

For the obfuscation, we utilize the following principles: every element $\mathbf{y}_j^{(i)}$ in $\mathbb{Y}^{(i)}$ can be fully specified by the realizations of $\tilde{\mathbf{X}}_{i,\mathcal{R}}$, $\tilde{\mathbf{X}}_{i,\mathcal{B}}$, and parameter λ_j. Probabilities $\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right)$, $\Pr\left(\ell_i = \mathcal{B} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right)$ then affect $\mathcal{H}_{\mathrm{r},i,j}$. All these parameters affect $D_{i,j}$. The diagram explaining relations between all the mentioned parameters is provided on fig. 3. In this example, labelled states are $\tilde{\mathbf{X}}_{i,\mathcal{R}} = \left(x^A, x^B\right)$, $\tilde{\mathbf{X}}_{i,\mathcal{B}} = \left(x^B, x^A\right)$; set $\mathbb{Y}^{(i)}$ contains only two elements $\mathbf{y}_1^{(i)} = \left(\hat{y}^{(i)}, \check{y}^{(i)}\right)$ and $\mathbf{y}_2^{(i)} = \left(\check{y}^{(i)}, \hat{y}^{(i)}\right)$. For example, to specify $\mathbf{y}_1^{(i)}$ we only need λ_1 in addition to the labelled states (Δ is the distance between them). To obtain $\mathbf{y}_2^{(i)}$ we should apply a similar procedure where λ_2 is known (in our particular example $\lambda_2 = 1 - \lambda_1$). Probability $\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right)$ is denoted as p_1: its value affects attacker's uncertainty $\mathcal{H}_{\mathrm{r},i,j}$ as well as the distortion $D_{i,j}$.

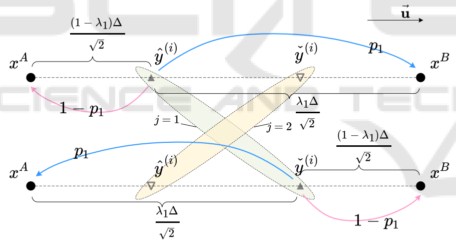
$\vec{\mathbf{u}}$
$\frac{(1-\lambda_1)\Delta}{\sqrt{2}}$
x^A
$\hat{y}^{(i)}$
$\check{y}^{(i)}$
p_1
x^B
$1 - p_1$
$j = 1$
$\frac{\lambda_1\Delta}{\sqrt{2}}$
$j = 2$
$\frac{(1-\lambda_1)\Delta}{\sqrt{2}}$
p_1
x^A
$\hat{y}^{(i)}$
$\check{y}^{(i)}$
x^B
$\frac{\lambda_1\Delta}{\sqrt{2}}$
$1 - p_1$

Figure 3: Scheme for obfuscation principle.

To maximize $\mathcal{H}_{\mathrm{r},i}$ under $\tilde{D}_i \geq \mathbb{E}[D_i]$ we consider realizations of $\mathbf{Y}_i$ and optimal adjustment of λ: such adjustment then allows us to increase p_1 and $1 - p_2$.

We note that $\mathbf{Y}_i$ shall belong to a line segment (in a multidimensional space) connecting $\tilde{\mathbf{X}}_{i,\mathcal{R}}$ and $\tilde{\mathbf{X}}_{i,\mathcal{B}}$. This property is trivial (goes without proof) and can be best understood if triangle $\triangle\, \tilde{\mathbf{X}}_{i,\mathcal{R}} \mathbf{Y}_i \tilde{\mathbf{X}}_{i,\mathcal{B}}$ is considered. As a result:

$$\forall \mathbf{Y}_i \left(\mathbf{Y}_i \in \mathbb{Y}^{(i)} \implies (\exists \lambda \in [0,1]) \wedge \left(\vec{\mathbf{Y}}_i = \overrightarrow{\tilde{\mathbf{X}}_{i,\mathcal{R}}} + \lambda \overrightarrow{\tilde{\mathbf{X}}_{i,\mathcal{R}} \tilde{\mathbf{X}}_{i,\mathcal{B}}}\right)\right). \quad (11)$$

We then establish the following:

Lemma 3. To minimize $D_{i,j}$ it is required that $\lambda_j = 1 - \Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right)$.[4]

Corollary 2. Minimal distortion is $D_{i,j} = \Delta_i^2 p_j (1 - p_j) \leq \frac{\Delta_i^2}{4}$, where $p_j = \Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}\right)$, $\Delta_i^2 = d\left(\tilde{\mathbf{X}}_{i,\mathcal{R}}, \tilde{\mathbf{X}}_{i,\mathcal{B}}\right)$.

Corollary 3. For every i, the highest lower bound (maxmin entropy) is:[4]

$$\mathcal{H}_{\mathrm{r},i} = -\nu_i \log_2 \nu_i - (1 - \nu_i) \log_2 (1 - \nu_i), \quad (12)$$

where $\nu_i = \min\left\{\varphi, \frac{\Delta_i - \sqrt{\Delta_i^2 - 4\mathbb{E}[D_i]}}{2\Delta_i}\right\}$.

There are several important takeaways from the proof of corollary 3. First, for every hidden state $\tilde{\mathbf{X}}_i$ there are two observable states that are obtained according to eq. (11) where $\lambda_1^{(i)} = 1 - \nu_i$ is used to define realisation $\mathbf{y}_1^{(i)}$, and $\lambda_2^{(i)} = 1 - \lambda_1^{(i)}$ is used for $\mathbf{y}_2^{(i)}$. Second, maximum allowed distortion should be used at step i meaning that $\mathbb{E}[D_i] = \tilde{D}_i$. Third, probabilities for transitions from labelled states to observable states are

$$\begin{aligned}
\Pr\left(\mathbf{Y}_i = \mathbf{y}_1^{(i)} \mid \ell_i = \mathcal{R}\right) &= \frac{1-\nu_i}{\varphi} \frac{\varphi+\nu_i-1}{2\nu_i-1}; \\
\Pr\left(\mathbf{Y}_i = \mathbf{y}_2^{(i)} \mid \ell_i = \mathcal{R}\right) &= 1 - \Pr\left(\mathbf{Y}_i = \mathbf{y}_1^{(i)} \mid \ell_i = \mathcal{R}\right); \\
\Pr\left(\mathbf{Y}_i = \mathbf{y}_1^{(i)} \mid \ell_i = \mathcal{B}\right) &= \frac{\nu_i}{1-\varphi} \frac{\varphi+\nu_i-1}{2\nu_i-1}; \\
\Pr\left(\mathbf{Y}_i = \mathbf{y}_2^{(i)} \mid \ell_i = \mathcal{B}\right) &= 1 - \Pr\left(\mathbf{Y}_i = \mathbf{y}_1^{(i)} \mid \ell_i = \mathcal{B}\right).
\end{aligned} \quad (13)$$

4.4 Optimal Obfuscation for $N - 1$ Time Steps

For every i we now define $\tilde{D}_i$ such that $\mathcal{H}_{\mathrm{r}} = \sum_i \mathcal{H}_{\mathrm{r},i}$ is maximized under the total distortion constraint $\tilde{D} \geq \sum_i \tilde{D}_i$. For this reason, we obtain optimal observable states and corresponding transition probabilities (from the labelled states) for all the time steps. From the proof of the corollary 3 we use that $\frac{\partial}{\partial \tilde{D}_i} \mathcal{H}_{\mathrm{r},i} \geq 0$ and $\frac{\partial^2}{\partial \tilde{D}_i^2} \mathcal{H}_{\mathrm{r},i} \leq 0$. To maximize $\mathcal{H}_{\mathrm{r}}$ we therefore require

$$\begin{cases}
\forall i \; \frac{\partial}{\partial \tilde{D}_i} \mathcal{H}_{\mathrm{r},i} = \frac{1}{\Delta_i^2 \sqrt{1-\kappa_i}} \log\left(\frac{1+\sqrt{1-\kappa_i}}{1-\sqrt{1-\kappa_i}}\right) = C; \\
\tilde{D} = \sum\limits_{i=1}^{N-1} \tilde{D}_i = \frac{1}{4} \sum\limits_{i=1}^{N-1} \kappa_i \Delta_i^2,
\end{cases} \quad (14)$$

where C is some constant, $\kappa_i = \frac{4\tilde{D}_i}{\Delta_i^2}$. We then solve the system eq. (14) for all κ_i, $i \in [1, N-1]$, and according to corollary 3 obtain $\nu_i = \min\left\{\varphi, 0.5 - \sqrt{0.25 - 0.25\kappa_i}\right\}$.

5 OBFUSCATION ALGORITHM

Here we represent our aforementioned findings in the form of obfuscation algorithm (see algorithm 1). It is practical and can be implemented in real settings: its

[4] For proof, see the full version of the paper (Zolotavkin et al., n.d.)

complexity (excluding the complexity of `solve` procedure) is only $O(N)$. For input, the algorithm accepts arrays (of size N) $\mathbf{X}^A$, $\mathbf{X}^B$, and scalars $\tilde{D}$, φ. Elements of these arrays are scalar/vector realizations for X_i^A and X_i^B characterizing geo-positions of *Alice* and *Bob*, respectively, at time i. In practice, these arrays may contain extrapolations based on historical data and repetitive patterns. For example, *Alice* and *Bob* may commute to work using the same routes and roughly at the same time every day. Procedure `solve` provides a solution to eq. (14): array $\boldsymbol{\kappa}$ contains elements κ_i needed to define realizations for obfuscated state $\mathbf{Y}_i$. It is also needed to calculate the unlinkability criterion (entropy) $\mathcal{H}_{r,i}$ dependent on the obfuscation process. Procedure `send_RSU` encapsulates data obfuscated at time i in accordance with one of the V2X communication formats and sends it to the nearest RSU. The output of the algorithm is, therefore, an array $\mathbf{Y}$ containing all the obfuscated records and the indicator of the total unlinkability in the system over $N-1$ steps, $\mathcal{H}_r$.

Algorithm 1: Obfuscation algorithm.

```
input  : $\mathbf{X}^A, \mathbf{X}^B, \tilde{D}, \varphi$ ;
output: $\mathbf{Y}, \mathcal{H}_r$ ;

begin
    $\mathcal{H}_r \leftarrow 0, \mathbf{Y} \leftarrow \varnothing, \boldsymbol{\kappa} \leftarrow \texttt{solve}\left(\tilde{D}, \mathbf{X}^A, \mathbf{X}^B\right)$ ;
    for $i \leftarrow 1$ to $N-1$ do
        $\nu_i \leftarrow \min\{\varphi,\ 0.5 - \sqrt{0.25 - 0.25\kappa_i}\}$,
          $\alpha \leftarrow (\varphi + \nu_i - 1)/(2\nu_i - 1)$,
          $\mathcal{H}_{r,i} \leftarrow -\nu_i \log(\nu_i) - (1-\nu_i)\log(1-\nu_i)$,
          $\mathcal{H}_r \leftarrow \mathcal{H}_r + \mathcal{H}_{r,i}, P_{1,\mathcal{R}} \leftarrow (1-\nu_i)\alpha/\varphi$,
          $P_{1,\mathcal{B}} \leftarrow \nu_i\alpha/(1-\varphi), r_1 \leftarrow \texttt{UniRand}([0,1])$,
          $r_2 \leftarrow \texttt{UniRand}([0,1])$,
          $\Lambda_{\mathcal{R}} \leftarrow 0.5 + (0.5-\nu_i)\,\texttt{sign}_{\pm}(P_{1,\mathcal{R}} - r_2)$,
          $\Lambda_{\mathcal{B}} \leftarrow 0.5 + (0.5-\nu_i)\,\texttt{sign}_{\pm}(P_{1,\mathcal{B}} - r_2)$ ;
        if $r_1 \leq \varphi$ then $\hat{y}^{(i)} \leftarrow X_i^A + \Lambda_{\mathcal{R}}\left(X_i^B - X_i^A\right)$,
          $\check{y}^{(i)} \leftarrow X_i^B + \Lambda_{\mathcal{R}}\left(X_i^A - X_i^B\right), \mathbf{Y}_i = \texttt{concat}(\hat{y}^{(i)}, \check{y}^{(i)})$;
        else $\hat{y}^{(i)} \leftarrow X_i^A + \Lambda_{\mathcal{B}}\left(X_i^B - X_i^A\right)$,
          $\check{y}^{(i)} \leftarrow X_i^B + \Lambda_{\mathcal{B}}\left(X_i^A - X_i^B\right), \mathbf{Y}_i = \texttt{concat}(\check{y}^{(i)}, \hat{y}^{(i)})$;
        send_RSU$(\mathbf{Y}_i), \mathbf{Y} = \texttt{concat}(\mathbf{Y}, \mathbf{Y}_i)$ ;
```

6 CONCLUSIONS[5]

In this paper, our research motivation aligns with other authors from the domain of C-ITS privacy protection: unlinkability of CAMs is an issue that needs to be addressed (Karim Emara, 2013; Escher et al., 2021). Our approach, however, differs in ***how*** we address our ***main aim*** (see section 2.1).

First, we use the classical definition of unlinkability. Despite being an apparent requirement based on standards and regulations, in many works, unlinkability is substituted by less demanding requirements such as geo-indistinguishability (Andrés et al., 2013; Bordenabe et al, 2014). We address unlinkability by adapting HMM to enable Bayesian inference about the labeled joint states (see fig. 2) in a system with two players, *Alice* and *Bob*. Based on such inference, we then calculate uncertainty about the labels: we use Shannon entropy to measure unlinkability.

Second, we assume a strong attacker who fully controls RSU and knows actual characteristics (e.g., positions, velocities, etc.) of the vehicles of *Alice* and *Bob* at any moment. The main benefit of such a worst-case assumption is that we obtain high confidence about the lower bound for the unlinkability of CAMs in C-ITS.

Third, we improve CAMs' unlinkability by developing the optimal joint obfuscation technique: we maximize the total entropy over $N-1$ time steps under the constraint on the distortion introduced to CAMs by *Alice* and *Bob*. This is complemented by an obfuscation algorithm whose complexity is only $O(N)$ (see algorithm 1).

Some of the application details of our findings are yet to be developed. For example, this may include the development of a secure and privacy-preserving protocol for joint obfuscation that is based on the proposed algorithm. Further developments will also focus on scaling the proposed obfuscation algorithm and conducting experiments, including simulations of different traffic situations.

ACKNOWLEDGMENT

This research is co-financed by public funding of the state of Saxony, Germany.

REFERENCES

Andrés, M. E., Bordenabe, N. E., Chatzikokolakis, K., & Palamidessi, C. (2013). Geoindistinguishability: Differential privacy for location-based systems. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 901–914.

Blackman, S. S. (1986, January 1). *Multiple-target tracking with radar applications*.

Bordenabe, N. E., Chatzikokolakis, K., & Palamidessi, C. (2014). Optimal Geo-Indistinguishable Mechanisms for Location Privacy. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 251–262.

Camenisch, J., Drijvers, M., Lehmann, A., Neven, G., & Towa, P. (2020). Zone Encryption with Anonymous

[5] For an in-depth discussion, see the full version of the paper (Zolotavkin et al., n.d.)

Authentication for V2V Communication. *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 405–424.

Escher, S., Sontowski, M., Berling, K., Köpsell, S., & Strufe, T. (2021). How well can your car be tracked: Analysis of the European C-ITS pseudonym scheme. 2021 *IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 1–6.

Hicks, C., & Garcia, F. D. (2020). A Vehicular DAA Scheme for Unlinkable ECDSA Pseudonyms in V2X. *2020 IEEE European Symposium on Security and Privacy (EuroS& P)*, 460–473.

ISO/IEC JTC 1/SC 27. (2022). *Evaluation criteria for IT security — Part 2: Security functional components* (International Standard No. ISO/IEC 15408-2:2022(E)). International Organization for Standardization. Geneva, CH.

ISO/TC 204. (2015). *Cooperative ITS — Part 7: Privacy aspects* (Technical Report (TR) No. ISO/TR 17427-7:2015(E)). International Organization for Standardization. Geneva, CH.

ISO/TC 204. (2018). *ITS station management — Part 1: Local management* (International Standard No. ISO 24102-1:2018(E)). International Organization for Standardization. Geneva, CH.

ISO/TC 22/SC 32. (2021). *Cybersecurity engineering* (International Standard No. ISO/SAE 21434:2021). International Organization for Standardization. Geneva, CH.

Karim Emara, W. W. (2013). *Beacon-based Vehicle Tracking in Vehicular Ad-hoc Networks* (Technical Report). TUM. Munich, Germany.

Shokri, R., Theodorakopoulos, G., & Troncoso, C. (2016). Privacy Games Along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy. *ACM Transactions on Privacy and Security*, 19(4), 11:1–11:31.

Sniedovich, M. (2016). Wald's mighty maximin: A tutorial. *International Transactions in Operational Research*, 23(4), 625–653.

Wagner, I., & Eckhoff, D. (2018). Technical privacy metrics: A systematic survey. *ACM Computing Surveys* (CSUR), 51(3), 1–38–1–38.

WG1, I. (2018). *Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary* (Technical Specification No. ETSI TS 102 894-2). European Telecommunications Standards Institute. Sophia Antipolis, France.

WG1, I. (2019). *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service* (European Standard No. DS/ETSI EN 302 637-2). European Telecommunications Standards Institute. Sophia Antipolis, France.

WG5, I. (2021). *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2* (Technical Specification No. TS 102 941). European Telecommunications Standards Institute. Sophia Antipolis, France.

Wiedersheim, B., Ma, Z., Kargl, F., & Papadimitratos, P. (2010). Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, 176–183.

Zolotavkin, Y., Baryshev, Y., Lukichov, V., Mähn, J., & Köpsell, S. (n.d.). *Improving unlinkability in C-ITS*. doi.org/10.6084/m9.figshare.21830418