Computer Networks 257 (2025) 110972

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Optimal obfuscation of awareness messages: Improving users' unlinkability in Intelligent Transport Systems☆

Yevhen Zolotavkin [a,*], Yurii Baryshev [b], Jannik Mähn [a], Vitalii Lukichov [b], Stefan Köpsell [a]

[a] Trustworthy Data Processing Group, Barkhausen Institut gGmbH, Schweriner Straße 1, Dresden 01067, Saxony, Germany
[b] Department of Information Protection, Vinnytsia National Technical University, Khmelnytske Shose 95, Vinnytsia 21021, Ukraine

ARTICLE INFO

Keywords:
Privacy
Unlinkability
ITS
V2X
Awareness messages
Obfuscation
Entropy

ABSTRACT

This paper introduces a novel methodology to enhance privacy in Cooperative Intelligent Transport Systems (C-ITS) by improving unlinkability in vehicle-to-everything (V2X) communication. Focusing on the Cooperative Awareness Basic Service, we employ a Hidden Markov Model (HMM) to model the unlinkability of Cooperative Awareness Messages (CAMs) exchanged between vehicles and roadside units (RSUs) under the surveillance of a Global Passive Adversary (GPA). Implementing a joint obfuscation approach maximizes unlinkability by transforming the CAMs' original data within a distortion threshold, preserving data utility while confounding the GPA's ability to reliably link messages to specific vehicles. The experimental evaluation confirms the superiority of our method when compared with multivariate independent noise models, including Gaussian and Laplace. Our approach also incorporates an authentication protocol, ensuring the secure and collaborative execution of the obfuscation algorithm by the vehicles involved.

1. Introduction

Current transport systems are evolving with a significant focus on automation, embodied in Cooperative Intelligent Transport Systems (C-ITS). These systems leverage real-time information sharing across diverse network entities, including vehicles and infrastructure, to enhance service delivery based on the current state of the transport environment [1]. C-ITS harnesses advanced communication, sensor, and control technologies, aiming to improve road safety, efficiency, sustainability, and user comfort. A key technology within this ecosystem is Vehicle-to-Everything (V2X), which enables various applications, such as collaborative forward collision warnings and electronic brake light alerts during emergencies [2,3]. Despite its benefits, V2X *raises critical privacy concerns*. For instance, Cooperative Awareness Messages (CAMs), which transmit *unencrypted geospatial data* at high frequencies (1–10 Hz) to boost traffic safety and flow, *can be intercepted* by a Global Passive Adversary (GPA). This growing dependence on V2X and CAMs, therefore, highlights a pressing **question**: What techniques can enhance the privacy of V2X communications?

The question above is complex due to the inherent tension between data utility and privacy. Our work focuses on developing a privacy model grounded in *unlinkability* as defined in ISO/IEC 15408-2 [4]. Unlinkability ensures that an adversary cannot determine whether multiple observed data points are related to the same user. Achieving unlinkability in V2X is particularly challenging because it is not attainable by a single user acting alone; it requires the cooperation of multiple users. Consequently, our approach involves a *joint obfuscation* methodology where two users (*Alice* and *Bob*) – driving their vehicles – collaborate to unlink their CAM data, thereby enhancing privacy without significantly compromising the utility of the information shared with the roadside unit (RSU).

The effectiveness of privacy-preserving techniques in V2X is heavily influenced by *assumptions* about potential adversaries' capabilities. Experts are divided on this front. Some assume that the GPA is weak, lacking access to actual identities and precise locations of vehicles or individuals [5,6]. Under this assumption, the GPA relies on heuristics such as multiple target tracking to infer information, making it difficult to quantify private information leakage with confidence due to the reliance on uncertain adversarial strategies [7].

☆ This research is co-financed based on the budget passed by the Saxonian State Parliament in Germany, and by the Federal Ministry of Education and Research, Germany, project KOMSENS-6G (funding label 16KISK122).

* Corresponding author.
E-mail addresses: yevhen.zolotavkin@barkhauseninstitut.org (Y. Zolotavkin), yuriy.baryshev@vntu.edu.ua (Y. Baryshev), jannik.maehn@barkhauseninstitut.org (J. Mähn), lukichov.vitalyi@vntu.edu.ua (V. Lukichov), stefan.koepsell@barkhauseninstitut.org (S. Köpsell).
URL: https://www.barkhauseninstitut.org (S. Köpsell).

https://doi.org/10.1016/j.comnet.2024.110972
Received 20 March 2024; Received in revised form 4 November 2024; Accepted 29 November 2024
Available online 6 December 2024

Conversely, other experts, including ourselves, assume a strong GPA, possess comprehensive knowledge of real vehicle identities, and can observe all communications within the network [8,9]. However, if effective privacy measures are in place, this adversary may still be uncertain about how to link obfuscated CAMs to specific identities. Adopting the strong GPA assumption allows us to utilize information-theoretic approaches to quantify the leakage of personally identifiable information (PII) [10]. This facilitates the development of privacy-preserving strategies with higher assurance levels, as the adversary's capabilities are more clear in that case.

Our obfuscation methodology aims to *optimize* certain parameters within our privacy model to maximize uncertainty for the adversary while adhering to distortion constraints. These constraints ensure that the obfuscated data remains within acceptable limits of accuracy and utility for V2X applications. Striking this balance is crucial; excessive obfuscation can degrade the quality of information necessary for safety-critical functions, whereas insufficient obfuscation may fail to adequately protect user privacy. By defining optimal obfuscation under distortion constraints, we provide a framework that enhances privacy without undermining the fundamental benefits of V2X communications.

Based on the above considerations, the **contribution** of this paper is as follows.

- We propose a model based on Hidden Markov Model (HMM) describing transitions between the joint states of *Alice* and *Bob*. We then introduce an assumption about a strong GPA who knows the original locations of the users and demonstrate how it simplifies reasoning about a lower bound on unlinkability;
- We develop a new methodology for optimal joint obfuscation where unlinkability is expressed using a Shannon entropy, which is maximized by modifying the original data under the constraint on distortion;
- We propose an algorithm implementing the developed obfuscation methodology and an authentication protocol, improving security assurances for the proposed obfuscation algorithm.

This paper has the following structure. In Section 2, we briefly systematize the works on obfuscation dealing with different types of GPAs. In Section 3, we set the grounds for our study: we provide initial definitions and assumptions. This is followed by Section 4, where we commence with a simplified model for obfuscation. We extend the model to include possible dependencies between CAMs produced at consecutive times; as a result, we obtain a Hidden Markov Model (HMM) to study the unlinkability of CAMs. In Section 5, we refine and formalize assumptions, define unlinkability through entropy, and optimize joint obfuscation, capable of producing observable states in HMM. Next, Section 6 describes a compact and efficient algorithm calculating the unlinkability in C-ITS and implementing previous findings to improve privacy. In Section 7, we experimentally evaluate the developed joint obfuscation approach and compare it with Gaussian and Laplacian obfuscation models. In Section 8, we develop a protocol for mutual authentication of users using Public Key Infrastructure (PKI) facilitating the use of the newly proposed obfuscation approach. Finally, we discuss our results, their novelty, advantages, and limitations in Section 9.

2. Existing works

We survey some existing approaches for privacy evaluation and improvement in the context of location-based services (LBS) utilizing V2X communication. The prevailing view of the role and capability of adversaries in the literature dealing with LBS privacy in V2X is as follows. All types of passive adversaries observe users' attributes in the intercepted (and often unencrypted) V2X communication (e.g., CAMs') content. The original attributes of the intercepted content are altered (obfuscated) by the users (prior to message transmission) to improve their privacy. Conditioned by these altered attributes in the intercepted messages, the adversary infers the *id*s (or actual locations) of the users who produced these messages. Such a non-consensual interception and inference may cause the linking of the messages. We further classify the privacy approaches in the literature based on the information that is available to the passive adversary for inference. First, we will survey papers dealing with weak Global Passive Adversary (GPA). Second, we will examine papers dealing with strong GPA. Third, we will review papers adopting the strong GPA concept and executing jointly optimized simultaneous obfuscation of multiple data items.

2.1. Weak GPA

Here, we consider literature where an adversary infers the links between modified (obfuscated) data items and *id*s (or ground truth data) of the users. The probabilities for the links are defined based on the distribution available to the adversary. This general distribution can be further refined if the actual subset realization of the original (e.g., ground truth) data at time step i is also known to the adversary. However, such a subset is usually hidden and must be first estimated based on the modified data observed at time steps preceding i. The need to estimate the hidden subset for a refined inference makes the adversary weaker.

In [5], the authors analyze the privacy of Location-Based Services (LBSs) using Hidden Markov Models (HMMs). Among other attacks, the authors consider De-Anonymization and Tracking attacks on the location information of mobile users. According to the authors' convention, an adversary knows the probability distribution of users' pseudonyms over a set of modified (obfuscated) geographic positions conditioned by their actual *id*s and actual locations. Because actual locations are unknown, they need to be estimated: these estimations are improved if previously reported locations and transition probabilities are known and taken into account by the adversary. To incorporate the latter, the authors use several techniques, including Forward-Backward and Viterbi algorithms. Finally, the authors use the Hungarian algorithm to find the most likely assignment of users' pseudonyms to the original *id*s.

In [11], the authors extend on their previous results considering privacy in LBS: they propose a new location-privacy protection mechanism (LPPM) which is based on Stackelberg Bayesian game where various privacy objectives may be admitted. Among other objectives, the authors aim at protecting the correlation between past, current, and future locations. The relations between the actual locations (e.g., hidden from the adversary) and pseudo locations (e.g., observable) can be modeled using HMM or any other suitable methodology. In the game, the defender maximizes the expected error that the optimal adversary incurs in reconstructing the user's actual trace. In turn, the adversary produces inference (e.g., best response), minimizing such an error after the defender completes their move in the game. To find equilibrium, the authors perform a linear optimization: as a result, they define a conditional distribution dubbed 'defensive mechanism encoding function'. Nevertheless, such an optimization relies on other parameters that need to be estimated: the optimality of the existing estimation methodologies is questionable. For example, an adversary is using prior probability distribution on the inference target location at time step i, given the adversary's prior knowledge derived from previous time steps, while the details of obtaining (e.g., estimating) such a distribution are not discussed.

The authors of Khodaei and Papadimitratos [6] present a novel scheme to exchange vehicular pseudonyms in cooperative and cryptographically protected mix zones. Thanks to disseminating decoy traffic (e.g., CAM messages), the authors report an improved unlinkability: for this, a special group of relaying vehicles emulate nonexisting vehicles. The vehicles participating in the scheme can filter these decoy messages out. This is done using a specially designed Cuckoo Filter, whose parameters are known to the legitimate vehicles and part of the C-ITS infrastructure, including RSU. The unlinkability of the scheme is

tested against GPA, and a tracking algorithm is used before and after mix zones to infer the users' *id*s. The tracking algorithm considers information in CAMs (timing, velocity, and location) and the road layout. The authors neither reason about the optimality of the tracking algorithm nor constrain its design. Instead, they propose a heuristic algorithm achieving some tangible results in tracking. As a result, inference about the links between the observable data items and users' *id*s can be improved if a more efficient tracking algorithm is discovered.

The hidden state estimation is one of the most significant limitations of the weak GPA models. The methodology for such an estimation is often sub-optimal, which causes additional uncertainties for the adversary. These additional uncertainties are difficult to quantify: the confidence in quantitative privacy statements is low, resulting in a low assurance level for corresponding claims. The level of privacy assurance can be strengthened for situations assuming a strong GPA.

2.2. Strong GPA

Similarly to the convention about the adversary in Section 2.1, here we analyze the literature where an adversary infers the links between modified (obfuscated) data items and *id*s of the users. However, in contrast to Section 2.1, at any time step i, the probabilities for such links are derived from a known distribution and do not need to be refined. As a result, adversarial inference cannot be further strengthened based on the estimation of additional parameters. The latter brings a higher confidence in the quantitative assessment of unlinkability and privacy in general.

To improve unlinkability in the V2X communication scenario, the authors of Li et al. [8] develop a new method to swap vehicles' pseudonyms. For reasoning about adversarial inference, the authors utilize generalized differential privacy: the vehicles swap their pseudonyms based on the exponential mechanism satisfying the pseudonym indistinguishability condition. These settings imply that the probability distribution for the links between the modified (swapped) pseudonyms and actual *id*s of the vehicles is available to the adversary. The authors assure that no further improvement of the adversarial inference (e.g., through additional parameter estimation) is possible: the swaps are only conducted between the small subsets of the vehicles whose driving states are similar and cannot be easily distinguished. The similarity criterion is a weighted sum of individual speed, direction, and position similarities for different vehicles.

In [12], the authors develop a new framework protecting the privacy of the users in a variety of location-based services (LBS) where users submit (and may also query) location-related data to a distrusted server, which further processes and manages it. The framework helps users protect their privacy (prior to the submission) through a perturbation-based obfuscation technique: it combines the concept of Local Differential Privacy (LDP) with the Staircase Randomized Response (SRR). The authors claim that such an L-SRR framework optimizes an LBS-oriented utility while guaranteeing strict ϵ-LDP privacy. Only parameters of the randomized obfuscation are known to the adversary who may control the server. Therefore, the knowledge of the adversary cannot exceed the knowledge about the probability distribution for the links between the modified data and the actual *id*s of the users. As such, the authors maintain that further improvement of the adversarial inference based on estimating additional (e.g., latent) parameters is impossible.

The authors of Takbiri et al. [9] develop a model for the use cases where n users change their pseudonyms once after every $m(n)$ steps. The authors introduce the obfuscation and anonymization steps to avoid pseudonym linking. During the obfuscation, some of the m data items of every user are altered: the number of the altered items may differ among the users. During the anonymization, the order of representing m-tupled data collections of all n users is randomized: based on the order of a collection, it is no longer possible to tell the *id* of the corresponding user with certainty. At every time step i, an adversary knows the probabilities of the states producing data items for every user, parameters of obfuscation, and anonymization algorithms. However, the exact realizations of random obfuscation and anonymization outcomes are unknown to the adversary. Also, the adversary has no other auxiliary or side information about users' data.

In situations involving a strong GPA, it is essential to provide the best level of privacy protection, which is still an open question. For example, among the existing publications, very few implement obfuscation methodologies that provide the optimal balance between unlinkability and the distortion introduced during the obfuscation.

2.3. Optimal obfuscation under strong GPA

Differential privacy (DP) is a popular methodology that can be adopted for obfuscation in C-ITS assuming a strong GPA. However, in such a context, multiple data items (e.g., CAMs produced by different vehicles) must be obfuscated simultaneously at every time step i. Here, we question the adequacy of the DP for the task of joint data modification in ITS.

The authors of Geng and Viswanath [13] propose an optimal data-independent staircase additive noise to protect the privacy of scalar query function (QF). Unfortunately, the scalar nature of the proposed mechanism for QF is a substantial limitation for joint obfuscation in ITS, where simultaneous processing of multiple entries is required. The authors of Sun et al. [14] aim at protecting the privacy of multi-dimensional and correlated queries. For the obfuscation task, the authors utilize a new criterion of ϵ-proximity under a constraint on additive noise variance. However, their results suffer from the following limitations: (i) the usage of a new criterion of ϵ-proximity remains unjustified; (ii) the reasoning about optimality is limited by the popular types of additive multi-variate noise only (e.g., uniform vs. Gaussian and Laplacian). The authors of both [15,16] maintain that adding i.i.d. noise to each matrix element (of a matrix-valued QF) typically leads to sub-optimal solutions. To address this issue, the authors of Chanyaswad et al. [15] introduce a new Matrix Variate Gaussian (MVG) mechanism: parameters sufficient to satisfy (ϵ, δ)-DP exist for the additive MVG noise. In [16], the authors address the non-optimality of the multivariate obfuscation caused by the full-rank covariance matrices in the Gaussian noise model: they propose a new Rank-1 Singular Multivariate Gaussian Mechanism (R1SMG) and provide parameters sufficient for (ϵ, δ)-DP. Nevertheless, the authors of Chanyaswad et al. [15], Ji and Li [16] consider specific additive noise models (e.g., multivariate Gaussian) only. Furthermore, a global optimum requires that the obfuscation conditions sufficient for (ϵ, δ)-DP are also necessary, which has not been demonstrated. Paper [17] elaborates on universal optimality for the d-DP criterion, which was first introduced in [18]. In deriving optimal obfuscation conditions, the authors of the former source utilize the Quantitative Information Flow (QIF) technique, which does not restrict the dimensionality of the QF and its arguments. Nevertheless, the practicality of Fernandes et al. [17] is limited: the d-DP criterion incorporates a distance metric whose application has not been sufficiently justified and is hardly generalizable.

The analysis of the literature sources provided above indicates numerous gaps in the methodology dealing with the optimal DP-based obfuscation of multivariate data records, which is required for joint data modification in C-ITS. The results of this paper are meant to fill these gaps partially.

3. Preliminaries

We introduce contextual information supporting our aim, settings, and privacy assumptions to justify the subsequent modeling steps.

3.1. Aim of the study

In specifying our aim, we follow privacy definitions derived from popular international standards and C-ITS domain-specific recommendations [4,19]. These sources emphasize the importance of *pseudonymity*

and *unlinkability* while producing, exchanging, and processing basic ITS safety messages (such as CAM).

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 messages broadcast by the vehicles should have the property of Definition 1 [19,20]. Unfortunately, usage of this definition is intricate as it describes an exclusively qualitative characteristic: *'...unable to determine...'* clause is either false or true. The latter implies that the privacy of the whole C-ITS (with many vehicles and observable during many hours) is expressed through a binary value. This issue has been recognized by practitioners and researchers alike resulting in extended set of instructions for privacy impact assessment [21]. For example, impact rating criteria for privacy can be expressed using severity degrees (e.g., negligible, moderate, major, and severe) for the privacy impact rating indicator. The degrees can be defined based on two aspects: (a) the level of sensitivity of the information about road users and (b) *how easily* it can be linked to a PII (Personally Identifiable Information) principal. Based on this, we incorporate the *easiness of linking* into Definition 1 to obtain a more versatile definition:

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 compare privacy indicators in C-ITS, we use Shannon entropy: it is an integral criterion of uncertainty in a system that expresses the *'...degree of inability to determine...'* [10]. Henceforth, the ***main aim*** of our paper is to develop a methodology maximizing entropy as a criterion of unlinkability in C-ITS.

3.2. Settings for the study

A general setup for our study is provided in Fig. 1. In Fig. 1(a), two vehicles are driven by *Alice* and *Bob*, respectively. Both vehicles transmit CAMs with the same frequency (synchronously), and the roadside unit (RSU) receives them without losses. The role of the *adversary* is played by the RSU, who tries to separate CAMs of *Alice* from CAMs of *Bob*: this allows the adversary to *link* CAMs received at different times but belonging to the same entity. The separation is done based on the content of CAMs and the order of their arrival within each time interval – see Fig. 1(b). We consider the ordering of CAMs' arrivals within the same time interval i to be either (A, B) or (B, A). For example, in an extreme case, the order is (A, B) on any time interval i. If an adversary knows about such a unique property, she can link messages without analyzing their payload. However, such extreme cases are unlikely, meaning that an adversary should also 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 [22]. In particular, we maintain that geo-position, velocity, and acceleration are essential: these parameters are mandatory in CAMs.

In this study, we exclude from further consideration the following types of CAM payload: *(1)* cryptographically produced proofs of authenticity (e.g., signatures); *(2)* categorical data (e.g., vehicle role). The exclusion of '*(1)*' is due to substantial attention to this issue from the members of the cryptographic community. For example, pseudonym unlinking solutions were proposed in [20,23]. The exclusion of '*(2)*' is due to categorical data is `OPTIONAL` in CAMs [22]. We also exclude `VehicleLength` and `VehicleWidth`, which otherwise are likely to be of great use in discriminating different vehicles [24]. This information can be omitted in CAMs if the codes 1023 and 62 are used in place of the vehicle's length and width, respectively [25].

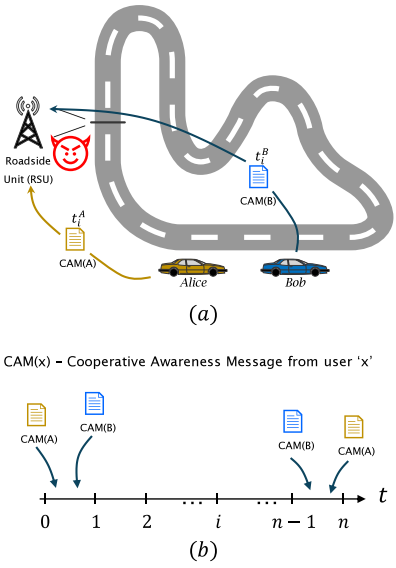

Fig. 1. Simplified diagram for awareness communication in C-ITS: (a) RSU receives message from *Alice* at t_i^A and from *Bob* at t_i^B; (b) Messages from both cars arrive within time interval i.

Because of the above arrangements, we further model CAM as a vector in $\mathbb{R}^z$ where $z \geq 1$. The latter allows us to apply commonly used distortion measures such as, for example, Squared Error (SE): this is a simple and straightforward way to express quality degradation of essential location services [11]. Further discussions about the advantages and disadvantages of such a distortion metric are beyond the scope of our paper.

3.3. Privacy assumptions and threats

Here, we briefly outline the rationale behind position obfuscation, adversarial inference, and the major factors affecting unlinkability provided by our approach. Subsequent sections introduce additional details.

Obfuscation: users *Alice* and *Bob* coordinate their efforts. They split the total distortion (e.g., 'budget') of obfuscation among $N-1$ time steps: as a result, the users know the distortion limit for every time step i. At the beginning of every time step i, *Alice* and *Bob* know the true measurements (including position, speed, acceleration, etc.) of each other. To obfuscate the data in their CAMs at every time step i, they agree on a random order of arrival (at RSU) for their CAMs. The users *define a joint distribution* according to which they change (obfuscate) their actual measurements in CAMs: the expected distortion does not exceed the limits.

Adversary: is strong GPA (as per Section 2.2). In addition, the adversary may know other information, such as the original geo-positions of the users at every time step i and the probabilities for the order of CAMs' arrivals. We, however, stress that the links between the obfuscated CAMs and the original data/identifiers are *unknown* to the adversary. She attempts to infer the source of every pair of CAMs observed at time i: entropy is calculated for such a statistical inference, which aligns with Definition 2. Specifically, the adversary uses the *joint distribution* utilized by *Alice* and *Bob* during the obfuscation.

Unlinkability factors: include (*i*) statistics for the order of CAMs' arrival, (*ii*) the limit for the obfuscation distortion, and (*iii*) the distance between the actual measurements of *Alice* and *Bob* at every time step i.

4. Mathematical model

The following systematization applies to the theoretical results in this paper.

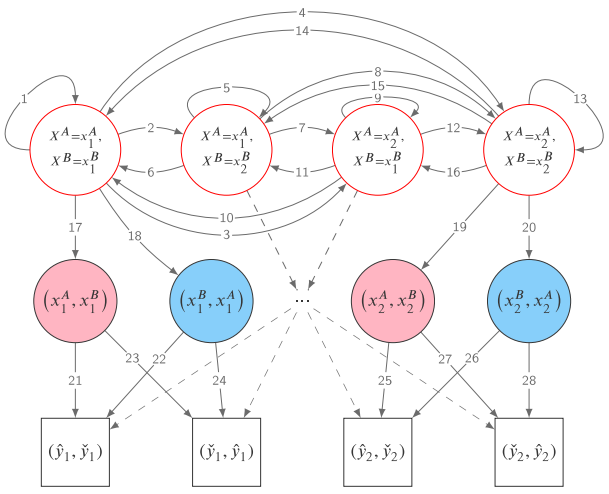

Fig. 2. Hidden Markov Model for 2 users sending CAMs. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

The purpose of the model is to *(i)* describe obfuscation in terms of random joint distribution utilized by *Alice* and *Bob*; *(ii)* provide inference expressions to calculate entropy.

The kind of model is HMM since it is the most generalizable and flexible in the context of C-ITS. Such an HMM-based description is suitable for situations dealing with weak and strong GPAs alike. In this paper, however, we do not explore the full depth of the weak GPA implications.

The meaning of the components of the model is the following. *Hidden states* describe original data and *ids* directly identifying vehicles and/or users driving them. *Colored states* describe the obfuscation algorithm's inner workings (e.g., concatenation order of users' data) and must not be revealed to the adversary. *Observable states* are the results of obfuscation and are known to the adversary. Using HMM terms, the main difference between weak and strong GPAs is that a strong GPA knows hidden states while a weak GPA tries to estimate them. The end goal of both GPAs is to infer the colored states.

The structure: this section starts with a simplified model where an adversary is strong and there is no need to estimate additional parameters for linking. We then consider an HMM to model unlinkability for situations that include other kinds of adversaries and contexts. The latter comes at the cost of increased computational demands and an overall lower level of confidence in the obtained results. To address this issue, in Section 5, we demonstrate how certain assumptions about adversaries can simplify reasoning about unlinkability using HMM.

4.1. Simplified model for unlinkability

Here, we provide a preliminary description of the unlinkability problem in C-ITS using common sets and operations. A generic information system with a GPA *Eve* includes sets of users' indices (e.g., unique identifiers) **U**, data (e.g., CAMs) **D**, and algorithms **P**. We consider subsets $\mathcal{U} \subset \mathbf{U}$ and $\mathcal{D} \subset \mathbf{D}$, where $\mathcal{U} = \{u_1, \dots, u_t, \dots, u_{|\mathcal{U}|}\}$ and $\mathcal{D} = \{d_1, \dots, d_t, \dots, d_{|\mathcal{D}|}\}$, respectively, $|\mathcal{U}| = |\mathcal{D}|$. There is a one-to-one mapping (which may be known to GPA) between $\mathcal{U}$ and $\mathcal{D}$ such that corresponding tuples (u_1, d_1), ..., (u_t, d_t), ..., $(u_{|\mathcal{U}|}, d_{|\mathcal{D}|})$ can be obtained and a set $\mathcal{T} = \{(u_t, d_t)\}_{1 \le t \le |\mathcal{U}|}$ can be formed. We then define an algorithm for joint obfuscation $\mathtt{O} \in \mathbf{P}$ and a permutation algorithm $\mathtt{M} \in \mathbf{P}$ (the both are known to *Eve*). We obtain an obfuscated set $\mathcal{D}^* = \mathtt{O}[\mathcal{D}]$, where $|\mathcal{D}^*| = |\mathcal{D}|$, but in general $\mathcal{D}^* \neq \mathcal{D}$. Algorithm $\mathtt{M}$ is probabilistic: the instruction on permuting indices $1, \dots, |\mathcal{U}|$ is a random vector (which particular realization is not known to *Eve*) $\mathbf{m} = \mathtt{M}[|\mathcal{U}|]$, $\mathbf{m} \in \mathbb{N}^{|\mathcal{U}|}$, such that $\{m_1, \dots, m_{|\mathcal{U}|}\} = \{1, \dots, |\mathcal{U}|\}$, but $\Pr(\mathbf{m} = (1, \dots, |\mathcal{U}|)) <$ 1. The released (obfuscated) set with improved unlinkability is then $\mathcal{T}^* = \{(u_t, d^*_{m_t})\}_{1 \le t \le |\mathcal{U}|}$, and the expected distortion of obfuscation is $\mathbb{E}(\hbar_{\mathcal{T},\mathcal{T}^*}) = \sum_{\mathbf{m} \in \mathbb{N}^{|\mathcal{U}|}} \varsigma(\mathbf{m}) \hbar_{\mathcal{T},\mathcal{T}^*}$, $\hbar_{\mathcal{T},\mathcal{T}^*} = \sum_t \hbar(d_t, d^*_{m_t})$, where $\hbar(\cdot,\cdot)$ is some suitable distortion measure, and $\varsigma(\mathbf{m})$ is a discrete probability density function for a random vector $\mathbf{m}$. Adversarial inference (linking) is typically done by *Eve* using algorithm $\mathtt{L} \in \mathbf{P}$ producing $\hat{\mathcal{T}} = \mathtt{L}[\mathcal{T}^*]$, where $\hat{\mathcal{T}} = \{(u_{\hat{m}_t}, d^*_{m_t})\}_{1 \le t \le |\mathcal{U}|}$ such that $\hat{\mathbf{m}} = \arg\max_{\mathbf{m} \in \mathbb{N}^{|\mathcal{U}|}} \Pr(\mathbf{m})$. Entropy $\mathcal{H}(\varsigma(\mathbf{m}))$ is a widely used indicator expressing uncertainty of inference [10]. Hence, the goal of optimization is to define algorithms $\mathtt{O}$ and $\mathtt{M}$ maximizing $\mathcal{H}(\varsigma(\mathbf{m}))$ under the constraint on the expected $\mathbb{E}(\hbar_{\mathcal{T},\mathcal{T}^*})$.

The above model assumes that *Eve* is a strong adversary who knows both $\mathcal{T}$ and $\varsigma(\mathbf{m})$. Next, we will consider a model where data $\mathcal{D}$ is hidden from *Eve*, and instead of $\varsigma(\mathbf{m})$ she only knows a mixture $\mathcal{E}(\mathbf{m})$ of multiple possible $\varsigma^{(1)}(\mathbf{m}), \dots, \varsigma^{(J)}(\mathbf{m})$. However, to reduce uncertainty, *Eve* may use the dependency between cooperative awareness data $\mathcal{D}_i$ and $\mathcal{D}_{i+1}$ produced at time steps i and $i+1$, respectively: based on the observable $\mathcal{D}^*_i$, $\mathcal{D}^*_{i+1}$, she may obtain (e.g., Forward-Backward algorithm) estimations $\hat{\mathcal{D}}_{i+1}$, $\hat{\varsigma}_{i+1}(\mathbf{m})$ for the actual data $\mathcal{D}_{i+1}$ and density $\varsigma_{i+1}(\mathbf{m})$, respectively.

4.2. Markov model for unlinkability

We use the Hidden Markov Model to model unlinkability in V2X with dependent states: it is graphically represented on Fig. 2. The following sets describe the model.[1] The set of all users is $\mathbb{P} = \{Alice, Bob, \dots\}$. For each user, there exists a set of hidden states for their vehicle, e.g., for *Alice* there is $\mathbb{X}^A = \left\{x^A_1, x^A_2, \dots, x^A_k, \dots, x^A_\mu\right\}$ and for *Bob* there is $\mathbb{X}^B = \left\{x^B_1, x^B_2, \dots, x^B_j, \dots, x^B_\omega\right\}$. Each state, for example,

Table 1
Notations.

Notation	Description
ITS	Intelligent Transport Systems
C-ITS	Cooperative Intelligent Transport Systems
V2X	Vehicle-to-Everything
CAM	Cooperative Awareness Message
RSU	Roadside Unit
HMM	Hidden Markov Model
$\mathbf{D}$	Set of user-and-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 users including *Alice* and *Bob*
$x^A_k,\ 1 \le k \le \mu$	A hidden state for *Alice*
$\mathbb{X}^A = \{x^A_k\}$	Set of hidden states for *Alice*
$x^B_j,\ 1 \le j \le \omega$	A hidden state for *Bob*
$\mathbb{X}^B = \{x^B_j\}$	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*
$i \in \{1, 2, \dots, N-1\}$	Time-step in discrete HMM
X^A_i	Variable on $\mathbb{X}^A$ at i
X^B_i	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 $i+1$
n	Length of keys used for cryptographic transformations

[1] To ease the reading, Table 1 contains our main notations.

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 $|\mathbb{P}|$ users 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 $\Pr(X_{i+1}^A = x_2^A, X_{i+1}^B = x_2^B \mid X_i^A = x_1^A, X_i^B = x_1^B)$. In practice, these probabilities can be obtained based on the well-studied physical models for vehicles [26].

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 adversary 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 colored 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 colored 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 $\Pr\left(\mathbf{X}_{i,\mathcal{R}} | \mathbf{X}_i\right) = \varphi \le 0.5$, and $\Pr\left(\mathbf{X}_{i,\mathcal{B}} | \mathbf{X}_i\right) = 1 - \varphi$.

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 $|\mathbb{X}_{\mathcal{R}}| \le |\mathbb{X}_{\{\mathcal{R},\mathcal{B}\}}| \le 2|\mathbb{X}_{\mathcal{R}}|$. For every $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$ there are transitions to observable joint states $\mathbf{Y}_i \in \mathbb{Y}$, $\mathbb{Y} = \{ (\hat{y}_1, \check{y}_1), (\check{y}_1, \hat{y}_1), \ldots, (\hat{y}_q, \check{y}_q), (\check{y}_q, \hat{y}_q), \ldots, (\hat{y}_\xi, \check{y}_\xi), (\check{y}_\xi, \hat{y}_\xi) \}$. 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.

5. Model properties

We follow Definition 2 to formally express unlinkability using conditional entropy $H\left(\ell_1, \ell_2, \ldots | \mathbf{Y}_1, \mathbf{Y}_2, \ldots\right)$ for the sequence of labels $\ell_1, \ell_2, \ldots, \ell_{N-1}$, given that an adversary observes $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_{N-1}$ [10]. In addition, we demonstrate how certain assumptions can simplify our reasoning and improve confidence for privacy assurance in C-ITS.

5.1. General expression for unlinkability

For the described HMM, probability of any hidden state at any time step can be specified using multivariate discrete distribution $\rho : \mathbb{X}^{(A,B)} \times \{0, 1, \ldots, N-1\} \to [0,1]^{N\left|\mathbb{X}^{(A,B)}\right|}$. We will further use ρ_i slices of ρ such that $\rho = \bigcup_{i=0}^{N-1} \rho_i$, where each slice represents a distribution over hidden states at time 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 adversary observes $\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_{N-1}$ and knows ρ analysis of $H\left(\ell_1, \ell_2, \ldots \mid \mathbf{Y}_1, \mathbf{Y}_2, \ldots, \rho\right)$ is central to our reasoning about unlinkability. We state the following.

Lemma 1. *Unlinkability in V2X system (as per Fig. 2) is expressed as (for details see Appendix A):*

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

5.2. 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* $\mathcal{H}_\mathrm{r}$ for $H\left(\ell_1, \ell_2, \ldots | \mathbf{Y}_1, \mathbf{Y}_2, \ldots, \rho\right)$. The concept of the rational lower bound is explained through the following assumptions [27].

Assumption 1 (*Worst-case Unlinkability*)**.** Requires that an adversary knows sets for the hidden, labeled and observable states. He knows all the transitions and the order mixing probability φ. For each observable state at time step 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 adversary does not know the labeled state ℓ_i (and cannot force its selection) at time step 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 labeled states considered by the adversary.

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 ρ); (2) probabilities for transitions from the hidden states to the labeled states (e.g., φ, $1-\varphi$), and from the labeled states to the observable states. Further, we consider a situation where the worst case ρ (*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:

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

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

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

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

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

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

We then point out that

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

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

where

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

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 (for details see Appendix A).*

Based on the result of Lemma 2, for every $\mathbf{Y}_i$ there is one and only one 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 one 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 labeled states to the observable states)?

5.3. 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 $\tilde{\mathbf{X}}_{i,\mathcal{R}}\to\mathbf{Y}_i$ and $\tilde{\mathbf{X}}_{i,\mathcal{B}}\to\mathbf{Y}_i$ imply that a non-zero distortion $\mathbb{E}\left[D_i\right]$ takes place:

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

where

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

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 step 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 $\mathcal{H}_{\mathrm{r},i}$ is maximized under constraint $\tilde{D}_i\geq\mathbb{E}\left[D_i\right]$? (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 $\tilde{D}\geq\sum_i\mathbb{E}\left[D_i\right]$ 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, labeled 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 labeled 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 adversarial uncertainty $\mathcal{H}_{\mathrm{r},i,j}$ as well as the distortion $D_{i,j}$.

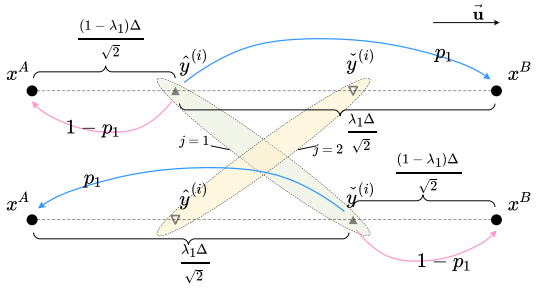

Fig. 3. Scheme for the obfuscation principle.

To maximize $\mathcal{H}_{\mathrm{r},i}$ under $\tilde{D}_i\geq\mathbb{E}\left[D_i\right]$ 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:

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

We then establish the following:

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

Corollary 2. *Minimal distortion is $D_{i,j}=\Delta_i^2p_j(1-p_j)\leq\frac{\Delta_i^2}{4}$, 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 time step i, the highest lower bound (maxmin entropy) is (for details see Appendix A):*

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

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 realization $\mathbf{y}_1^{(i)}$, and $\lambda_2^{(i)}=1-\lambda_1^{(i)}$ is used for $\mathbf{y}_2^{(i)}$. Second, maximum allowed distortion should be used at time step i meaning that $\mathbb{E}\left[D_i\right]=\tilde{D}_i$. Third, probabilities for transitions from labeled states to observable states are

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

5.4. Optimal obfuscation for $N-1$ time steps

For every time step 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 labeled states) for all the time steps. From the proof of 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

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

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 $\nu_i = \min\left\{\varphi,\ 0.5 - \sqrt{0.25 - 0.25\kappa_i}\right\}$.

6. Obfuscation algorithm

In this section, we design an obfuscation algorithm (see algorithm 1) using our earlier findings. The algorithm is practical and can be implemented in real settings: its complexity (excluding the complexity of `solve` procedure) is only $O(N)$. For input, the algorithm accepts arrays (of size N) $\mathbf{X}^A$, $\mathbf{X}^B$, users' IDs (id_A, id_B are for *Alice* and *Bob*, respectively), and scalars n, $\tilde{D}$, φ. Elements of the arrays are scalar/vector instances for X_i^A and X_i^B representing geo-positions of the users at time step 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 instances for obfuscated state $\mathbf{Y}_i$. The algorithm also calculates the unlinkability criterion (entropy) $\mathcal{H}_{\mathrm{r},i}$.

Algorithm 1: Obfuscation algorithm

input : $\mathbf{X}^A$, $\mathbf{X}^B$, id_A, id_B, n, $\tilde{D}$, φ ;
output: $\mathbf{Y}$, $\mathcal{H}_\mathrm{r}$;

begin
  $\mathcal{H}_\mathrm{r} \leftarrow 0$, $\mathbf{Y} \leftarrow \emptyset$, $\boldsymbol{\kappa} \leftarrow \mathtt{solve}\left(\tilde{D}, \mathbf{X}^A, \mathbf{X}^B\right)$;
  for $i \leftarrow 1$ **to** $N-1$ **do**
    $\nu_i \leftarrow \min\left\{\varphi,\ 0.5 - \sqrt{0.25 - 0.25\kappa_i}\right\}$,
    $\alpha \leftarrow (\varphi + \nu_i - 1)/(2\nu_i - 1)$,
    $\mathcal{H}_{\mathrm{r},i} \leftarrow -\nu_i \log(\nu_i) - (1-\nu_i)\log(1-\nu_i)$, $\mathcal{H}_\mathrm{r} \leftarrow \mathcal{H}_\mathrm{r} + \mathcal{H}_{\mathrm{r},i}$,
    $P_{1,\mathcal{R}} \leftarrow \alpha(1-\nu_i)/\varphi$, $P_{1,\mathcal{B}} \leftarrow \alpha\nu_i/(1-\varphi)$,
    $seed_A \leftarrow \mathtt{uniRand}_A\left([0, 2^n - 1]\right)$,
    $seed_B \leftarrow \mathtt{uniRand}_B\left([0, 2^n - 1]\right)$,
    $seed \leftarrow \mathtt{keySharing}(seed_A, seed_B)$, $r_1 \leftarrow \mathtt{hash}_n(seed)$,
    $r_2 \leftarrow \mathtt{hash}_n(\mathtt{concat}(id_A, id_B, seed))$,
    $\Lambda_\mathcal{R} \leftarrow 0.5 + (0.5 - \nu_i)\ \mathtt{sign}_{\pm}\left(P_{1,\mathcal{R}} - \frac{r_2}{2^n - 1}\right)$,
    $\Lambda_\mathcal{B} \leftarrow 0.5 + (0.5 - \nu_i)\ \mathtt{sign}_{\pm}\left(P_{1,\mathcal{B}} - \frac{r_2}{2^n - 1}\right)$;
    if $r_1 \leq \mathtt{round}(\varphi \cdot (2^n - 1))$ **then**
      $\hat{y}^{(i)} \leftarrow X_i^A + \Lambda_\mathcal{R}\left(X_i^B - X_i^A\right)$, $\check{y}^{(i)} \leftarrow X_i^B + \Lambda_\mathcal{R}\left(X_i^A - X_i^B\right)$,
      $\mathbf{Y}_i \leftarrow \mathtt{concat}(\hat{y}^{(i)}, \check{y}^{(i)})$;
    else $\hat{y}^{(i)} \leftarrow X_i^A + \Lambda_\mathcal{B}\left(X_i^B - X_i^A\right)$,
      $\check{y}^{(i)} \leftarrow X_i^B + \Lambda_\mathcal{B}\left(X_i^A - X_i^B\right)$, $\mathbf{Y}_i \leftarrow \mathtt{concat}(\check{y}^{(i)}, \hat{y}^{(i)})$;
    $\mathtt{send\_RSU}\left(\mathbf{Y}_i\right)$, $\mathbf{Y} \leftarrow \mathtt{concat}(\mathbf{Y}, \mathbf{Y}_i)$;

Obfuscation requires a joint effort from *Alice* and *Bob*: correctness of this joint effort can be questioned by each of the participants. Specifically, a consensus must be reached by *Alice* and *Bob* about random numbers r_1 and r_2 without revealing their values to a third-party (e.g., adversary *Eve*). For this, we first derive the common *seed* based on the procedure `keySharing`: the inputs are random seeds $seed_A$ and $seed_B$ generated by *Alice* and *Bob*, respectively. Next, the random number derivation is based on the keyless hash function `hash` (with the output of size n) along with the concatenation procedure `concat`. Below we describe some of the procedures and functions used in the algorithm:

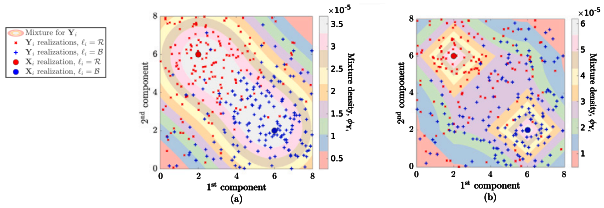

Fig. 4. Mixtures $\phi_{\mathbf{Y}_i}$ resulting from addition of bi-variate independent noise to $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$: (a) Gaussian noise, $\sigma = 2.5$; (b) Laplacian noise, $b = 2.5$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

- `uniRand` – generates uniformly distributed random numbers. For example, true random generators or cryptographically secure random numbers generating algorithms such as Fortuna can be used [28,29].
- `keySharing` – securely shares secret *seed* between *Alice* and *Bob*. It may implement a key agreement protocol such as Elliptic Curve Cryptography Cofactor Diffie–Hellman or another secure protocol [30].
- `hash` – unidirectionally maps its input (e.g., *seed*) into $\{0,1\}^n$ space. We suggest to use thoroughly researched hashing algorithms such as SHA-3 [31] to implement `hash`.
- `concat` – links inputs together into a single output data set: this is a basic programming operation performing mapping $\{0,1\}^n \times \{0,1\}^m \to \{0,1\}^{n+m}$.
- `send_RSU` – encapsulates data obfuscated at time step i in accordance with CAM format [22], and sends it to the nearest Roadside Unit (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, $\mathcal{H}_\mathrm{r}$. However, some steps in algorithm 1 require further explanation. For example, the authenticity of the claims of an entity with identity id_A (e.g., *Alice*) about the value $seed_A$ needs to be assured. Similarly, the claim's authenticity about $seed_B$ from id_B must also be provided. To satisfy these essential preconditions for the secure execution of algorithm 1, we develop a protocol for mutual authentication.

7. Experimental evaluation

The experiment aims to evaluate the proposed joint obfuscation's efficiency and compare it with other commonly used obfuscation techniques. The latter benchmarking techniques include bi-variate Gaussian and Laplacian noise models popular, for example, in the domain of Differential Privacy (DP) [14,15]. The evaluation is structured as follows. First, for original $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$ representing hidden states on Fig. 2, we synthesize random noisy (obfuscated) samples $\mathbf{Y}_i$ representing observable states. Second, for the generated $\mathbf{Y}_i$, we compare uncertainties of inference about the hidden state's label (which is either $\mathcal{R}$ or $\mathcal{B}$), and the distortion, D_i, caused by the obfuscation. Third, we define distribution of $\mathbf{Y}_i$ on the line segment $\mathbf{X}_{i,\mathcal{R}}\mathbf{X}_{i,\mathcal{B}}$: this allows to increase uncertainty of inference $H\left(\ell_i|\mathbf{Y}_i\right)$ and reduce D_i. Finally, we compare these obfuscation results with the results of the joint obfuscation method proposed by us.

To simulate hidden states, we append numerical components – realizations for X_i^A and X_i^B – of *Alice* and *Bob* together: the appending order specifies whether the resulting tuple is $\mathbf{X}_{i,\mathcal{R}}$ or $\mathbf{X}_{i,\mathcal{B}}$. The realizations above might be vectors (e.g., 3 dimensions specifying the vehicle's position and 3 dimensions specifying its velocity). However, for simplicity and without loss of generality we assume that realizations are scalars. As an example, the hidden state of *Alice* at step i is characterized by value 2, the hidden state of *Bob* at step i is characterized by value 6: we obtain $\mathbf{X}_{i,\mathcal{R}} = (2,6)$ and $\mathbf{X}_{i,\mathcal{B}} = (6,2)$. Marginal probabilities of having either $\mathbf{X}_{i,\mathcal{R}}$ or $\mathbf{X}_{i,\mathcal{B}}$ are equal, $\varphi = 0.5$.

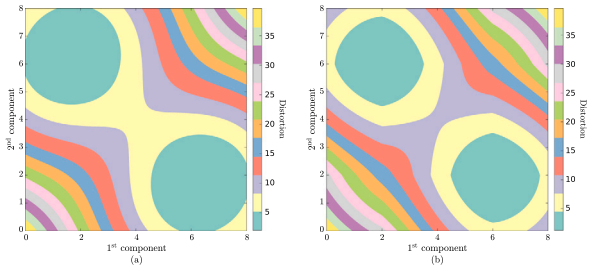

Fig. 5. For every $\mathbf{y}^{(i)}$ on the plane, distortion is $D_i(\mathbf{y}^{(i)}) = d(\mathbf{y}^{(i)}, \mathbf{X}_{i,\mathcal{R}})\Pr(\ell_i = \mathcal{R}|\mathbf{y}^{(i)}) + d(\mathbf{y}^{(i)}, \mathbf{X}_{i,\mathcal{B}})\Pr(\ell_i = \mathcal{B}|\mathbf{y}^{(i)})$: (a) Gaussian noise, $\sigma = 2.5$; (b) Laplacian noise, $b = 2.5$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

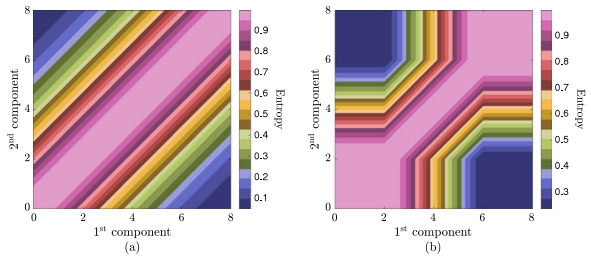

Fig. 6. Entropy of inference, $H(\ell_i|\mathbf{Y}_i = \mathbf{y}^{(i)})$, for different realizations of $\mathbf{Y}_i$: (a) Gaussian noise, $\sigma = 2.5$, $H(\ell_i|\mathbf{Y}_i) \approx 0.6$; (b) Laplacian noise, $b = 2.5$, $H(\ell_i|\mathbf{Y}_i) \approx 0.6$.

7.1. Bi-variate noise models

To obtain bi-variate noise models, we extend univariate Gaussian and Laplacian with $(0, \sigma)$ and $(0, b)$, respectively, for both components in 2D space independently and in a way that variances along each direction are equal [15,16]. Expected distortions for the obtained in such way bi-variate Gaussian and Laplacian (non-isotropic) are $\mathbb{E}[D_i^{\{\mathcal{N}\}}] = 2\sigma^2$ and $\mathbb{E}[D_i^{\{\mathcal{L}\}}] = 2b^2$, respectively.

By adding noise to $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$, we obtain juxtapositions of red and blue observable (obfuscated) samples, respectively (see Fig. 4). This produces a mixture which density, $\phi_{\mathbf{Y}_i}$, is depicted with a color map[2]: the probability $\Pr(\mathbf{Y}_i)$ of obtaining particular observable state is determined by that density.

For the random outcome $\mathbf{Y}_i$, an adversary attempts to infer[3] the label (e.g., color $\mathcal{R}$ or $\mathcal{B}$) of the original $\mathbf{X}_i$. An efficient obfuscation technique should maximize such an inference's uncertainty (e.g., entropy) while keeping distortion below the constraint. Color maps in Fig. 5 depict distortions caused by the noise-adding obfuscation: every realization $\mathbf{y}^{(i)}$ of $\mathbf{Y}_i$ on 2D plane is either the result of distorting $\mathbf{X}_{i,\mathcal{R}}$ by the amount $d(\mathbf{y}^{(i)}, \mathbf{X}_{i,\mathcal{R}})$, or the result of distorting $\mathbf{X}_{i,\mathcal{B}}$ by $d(\mathbf{y}^{(i)}, \mathbf{X}_{i,\mathcal{B}})$, where $d(\cdot,\cdot)$ is the squared l^2-norm. Density $\phi_{\mathbf{Y}_i}$ affects the total distortion of the obfuscation scheme. For example, if we take expectations over the corresponding mixtures in Fig. 4, we obtain distortion values 7.94 and 8.21 for Gaussian and Laplacian models, respectively.[4]

For every realization $\mathbf{y}^{(i)}$, uncertainty of inference is due to probability $\Pr(\ell_i = \mathcal{R}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ that $\mathbf{y}^{(i)}$ originates from $\mathbf{X}_{i,\mathcal{R}}$, and probability $\Pr(\ell_i = \mathcal{B}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ that $\mathbf{y}^{(i)}$ originates from $\mathbf{X}_{i,\mathcal{B}}$. Corresponding entropy maps are depicted in Fig. 6. As can be seen, entropy is the highest in the middle part of the heat map. However, mixture $\phi_{\mathbf{Y}_i}$ influences entropic

[2] For Gaussian, $\phi_{\mathbf{Y}_i} = \varphi\mathcal{N}(\mathbf{X}_{i,\mathcal{R}}, \mathbf{\Sigma}) + (1-\varphi)\mathcal{N}(\mathbf{X}_{i,\mathcal{B}}, \mathbf{\Sigma})$. For Laplacian, $\phi_{\mathbf{Y}_i} = \varphi\mathcal{L}(\mathbf{X}_{i,\mathcal{R}}, \mathbf{\Sigma}) + (1-\varphi)\mathcal{L}(\mathbf{X}_{i,\mathcal{B}}, \mathbf{\Sigma})$.

[3] Adversary tries to match a pair of components (observable states) at once: this is a *joint* inference.

[4] Only area visible in Figs. 4 and 5 is considered for such calculation.

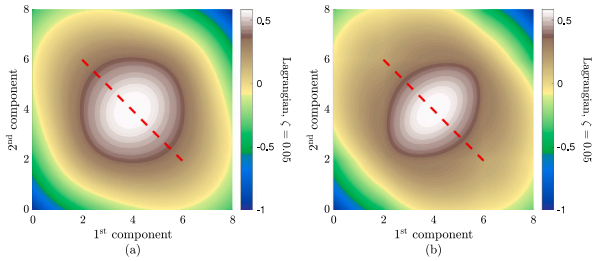

Fig. 7. Modified Lagrangian, $\mathcal{J}^*(\mathbf{y}^{(i)}, \zeta)$, $\zeta = 0.05$: (a) Gaussian noise, $\sigma = 2.5$; (b) Laplacian noise, $b = 2.5$.

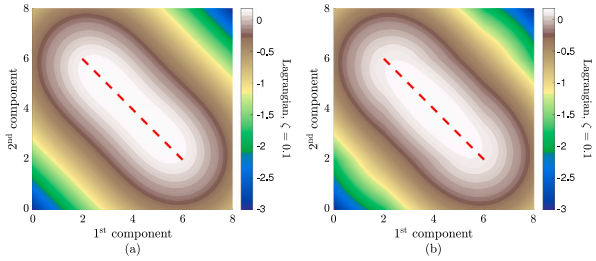

Fig. 8. Modified Lagrangian, $\mathcal{J}^*(\mathbf{y}^{(i)}, \zeta)$, $\zeta = 0.1$: (a) Gaussian noise, $\sigma = 2.5$; (b) Laplacian noise, $b = 2.5$.

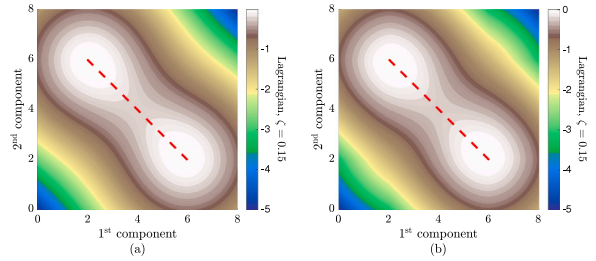

Fig. 9. Modified Lagrangian, $\mathcal{J}^*(\mathbf{y}^{(i)}, \zeta)$, $\zeta = 0.15$: (a) Gaussian noise, $\sigma = 2.5$; (b) Laplacian noise, $b = 2.5$.

expectation (e.g., conditional entropy): the effect of larger $H(\ell_i|\mathbf{Y}_i = \mathbf{y}^{(i)})$ values can be reduced. For example, if we take expectations over the corresponding mixtures in Fig. 4, we obtain $H(\ell_i|\mathbf{Y}_i)$ values 0.597 and 0.599 for Gaussian and Laplacian models, respectively.

The following rationale will help us improve 2D Gaussian and Laplacian models and compare them with our obfuscation method. Improvements in obfuscation efficiency can be due to: *(a)* modifications (e.g., optimizations) of mixture $\phi_{\mathbf{Y}_i}$ that keep $\Pr(\ell_i = \mathcal{R}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ and $\Pr(\ell_i = \mathcal{B}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ unchanged; *(b)* modifications of $\Pr(\ell_i = \mathcal{R}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ and $\Pr(\ell_i = \mathcal{B}|\mathbf{Y}_i = \mathbf{y}^{(i)})$ that keep $\phi_{\mathbf{Y}_i}$ unchanged; and *(c)* modifications of all the mentioned aspects. Intuitively, options *(a)* and *(b)* are sub-optimal, however, *(a)* has illustrative potential to explain why and how independent bi-variate Gaussian and Laplacian models can be improved to better serve the needs of joint obfuscation.

We demonstrate that the optimal mixture for Gaussian and Laplacian should be defined on a line segment connecting $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$. Due to the constrained entropy maximization, we use the Lagrangian function for our demonstration. We change the canonical expression $\mathcal{J}(\mathbf{y}^{(i)}, \zeta) = H(\ell_i|\mathbf{Y}_i = \mathbf{y}^{(i)}) - \zeta\left(D_i(\mathbf{y}^{(i)}) - \tilde{D}_i\right)$ into $\mathcal{J}^*(\mathbf{y}^{(i)}, \zeta) = H(\ell_i|\mathbf{Y}_i = \mathbf{y}^{(i)}) - \zeta D_i(\mathbf{y}^{(i)})$. Such $\mathcal{J}^*$ is suitable for a visual inspection allowing to spot maxima: it can be shown that if optimal $\dot{\zeta}$ is known, the remaining optimization of $\dot{\mathbf{y}}^{(i)}$ is indifferent to the value of term $\dot{\zeta}\tilde{D}_i$ which is omitted in $\mathcal{J}^*$. As the first step of optimization, it can be shown that a domain smaller than the entire 2D plane contains samples $\dot{\mathbf{y}}^{(i)}$ that maximize $\mathcal{J}^*$ under any ζ.

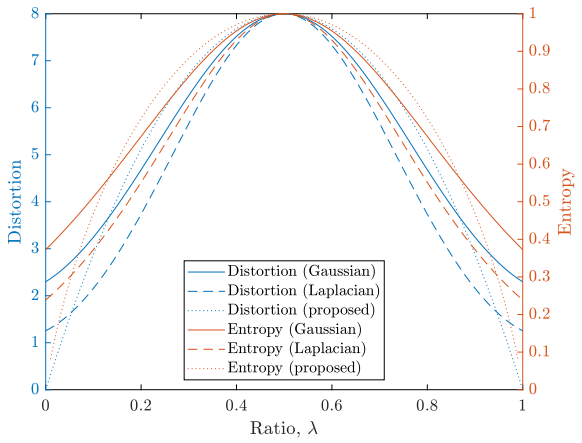

Fig. 10. Distortion and entropy plots for Gaussian, Laplacian, and the proposed obfuscation models defined for the line segment $\mathbf{X}_{i,\mathcal{R}}\mathbf{X}_{i,\mathcal{B}}$.

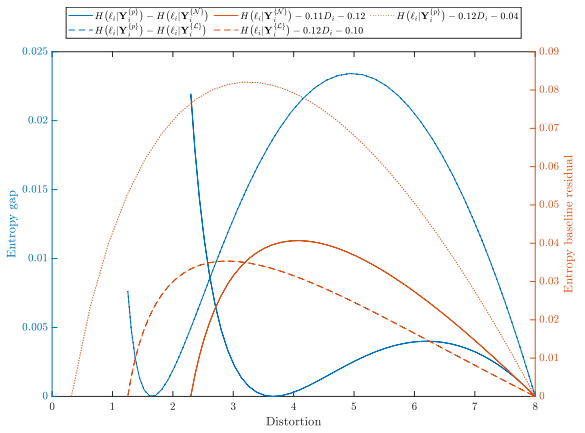

Fig. 11. Residual performance plots for Gaussian, Laplacian, and the proposed obfuscation models defined for the line segment $\mathbf{X}_{i,\mathcal{R}}\mathbf{X}_{i,\mathcal{B}}$.

We observe Figs. 7–9 to visually confirm a simple property that the line segment between $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$ contains $\dot{\mathbf{y}}^{(i)}$ maximizing $\mathcal{J}^*$. This property holds irrespective of ζ while the exact position of optimal $\dot{\mathbf{y}}^{(i)}$ on the line still depends on ζ. For example, for small ζ (e.g., see Fig. 7) entropic expression dominates in $\mathcal{J}^*$ while the distortion component is suppressed. As a result, $\dot{\mathbf{y}}^{(i)}$ is close to the middle of the line segment. In contrast, for larger ζ, optimal $\dot{\mathbf{y}}^{(i)}$ moves closer to the endpoints of the segment: assuring small distortions becomes more important than tracking for the highest entropy. The $\mathcal{J}^*$-based demonstrations confirm that further improvement of independent bi-variate Gauss/Laplace obfuscation is possible. Next, we will investigate whether redefining these obfuscation techniques for a line segment allows them to outperform our proposed method.

7.2. Adding noise on the line

We replace the 2D independent noise models used earlier with a random linear model for $\mathbf{Y}_i$ using $\lambda \in [0,1]$: any point $\mathbf{Y}_i$ on the line segment can be expressed as $\mathbf{Y}_i = \lambda\mathbf{X}_{i,\mathcal{R}} + (1-\lambda)\mathbf{X}_{i,\mathcal{B}}$. We then substitute these redefined samples $\mathbf{Y}_i$ into the Gaussian and Laplacian models to calculate the probabilities of inference $\Pr(\ell_i = \mathcal{R}|\mathbf{Y}_i = \mathbf{y}^{(i)})$, $\Pr(\ell_i = \mathcal{B}|\mathbf{Y}_i = \mathbf{y}^{(i)})$, and the resulting normalized density of the mixture $\phi^l_{\mathbf{Y}_i}$ (specific for the line segment).

For ratio λ of the line segment, we plot (see Fig. 10) distortions (left ordinate) and entropy of inference (right ordinate). Both distortion and entropy depend on the probability $\Pr(\ell_i|\mathbf{Y}_i)$ of inference. For the proposed obfuscation method, this probability is obtained based on Lemma 3. As can be seen from Fig. 10, all the distortion and entropy plots are symmetric about $\lambda = 0.5$ where they all peak. For all λ values, the distortion and entropy of Laplacian are below the distortion and entropy of Gaussian, respectively. However, distortion and entropy plots for the proposed method cross corresponding plots for Gaussian and Laplacian models.

To better demonstrate the advantages of the proposed obfuscation methodology, we plot the performance gap (left ordinate) between our method and each of the Gaussian and Laplacian line models, respectively. From Fig. 11, it can be seen that our method outperforms the models above: under the same distortion, entropy gaps are non-negative for our method. The gap plots approach zero on Fig. 11 at the points where the distortion plot (for our method) crosses corresponding Gaussian and Laplacian plots on Fig. 10. We also establish that Gaussian and Laplacian line mixtures $\phi^l_{\mathbf{Y}_i}$ can be further optimized: the resulting mixtures are unique and discrete. To show this, we build the following plots for the right ordinate on Fig. 11. The plots are residuals between entropy plots and their special linear models (baselines) defined using the first and the last points of the corresponding distortion-entropy plots (not shown here). Residual values on the plots are non-negative, implying that the dependences between distortions and entropies are concave for all three methods. The latter observation – combined with the fact that entropy grows monotonically with distortions – allows us to conclude that the entropic maximum is unique (one and only) for any given distortion constraint. In addition to reconfirming Corollary 3, such a demonstration is also beneficial for Gaussian and Laplacian models.

Mixtures for the random line-based obfuscation models are presented in Fig. 12. The left ordinate is used for the normalized continuous densities, $\phi^l_{\mathbf{Y}_i}$, defined for the Gaussian mixtures and Laplacian mixtures on the line segment. Expected distortions for these mixtures are $\mathbb{E}\big[D_i^{\{\mathcal{N}\}}\big] = 5.326$ and $\mathbb{E}\big[D_i^{\{\mathcal{L}\}}\big] = 3.992$, respectively. The values of expected conditional entropy are $H(\ell_i|\mathbf{Y}_i) = 0.728$ and $H(\ell_i|\mathbf{Y}_i) = 0.568$ for Gaussian and Laplacian, respectively. Comparing these indicators with the indicators for 2D independent noise models (see Section 7.1) already reveals the superiority of the line-based models for joint obfuscation.

The right ordinate in Fig. 12 is used to define discrete distributions maximizing entropy under the constraint on distortions. As an example, we plot optimal discrete mixtures for Gaussian and Laplacian under the constraints of 5.326 and 3.992, respectively. For the proposed method, we use the Gaussian constraint, 5.326. All three distributions are discrete but symmetric (the latter is due to unimodal and symmetric dependence between λ and entropy). All the three discrete distributions are 'close' to each other: roughly speaking, there are only two optimal realizations $\mathbf{y}_1^{(i)} \approx 0.78\mathbf{X}_{i,\mathcal{R}} + 0.22\mathbf{X}_{i,\mathcal{B}} = (2.88, 5.12)$, $\mathbf{y}_2^{(i)} \approx 0.22\mathbf{X}_{i,\mathcal{R}} + 0.78\mathbf{X}_{i,\mathcal{B}} = (5.12, 2.88)$, and $\Pr\big(\mathbf{Y}_i = \mathbf{y}_1^{(i)}\big) = \Pr\big(\mathbf{Y}_i = \mathbf{y}_2^{(i)}\big) = 0.5$.

We compare our joint obfuscation method with the Gaussian and Laplacian obfuscation for a larger range of σ and b values, respectively: we gradually increase both parameters from 1 to 10 (see Fig. 13). As a result, we plot conditional entropy $H(\ell_i|\mathbf{Y}_i)$ versus expected distortion $\mathbb{E}[D_i]$. Mixture densities for $\mathbf{Y}_i$ (e.g., $\phi_{\mathbf{Y}_i}$ or $\phi^l_{\mathbf{Y}_i}$) strongly affect the resulting efficiency of obfuscation. For instance, we contrast obfuscations using traditional independent noise models producing 2D mixtures, and the noise along the line segment $\mathbf{X}_{i,\mathcal{R}}$ and $\mathbf{X}_{i,\mathcal{B}}$. Calculations of entropy and distortion were only performed for the point in the area visible on Fig. 4. The latter implies that distortions caused by 2D noise models are underrepresented (e.g., less than actual) on the plot, while distortions of the points on the line segment are fully accounted.

As can be seen from Fig. 13, adding noise on the line provides a significant advantage over 2D noise models. Our joint obfuscation is the first approach exploiting this idea, and due to its optimal design, it outperforms Gaussian and Laplacian noise models defined for the line. It must be noted that the gain of our method over the Gaussian and

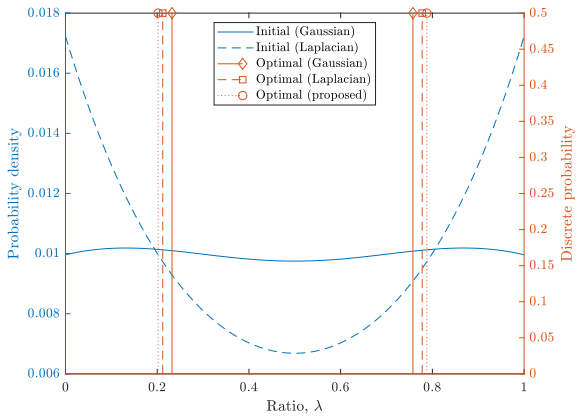

Fig. 12. Continuous and discrete densities, $\phi^{l}_{\mathbf{Y}_i}$, for mixtures produced by obfuscation methods on $\mathbf{X}_{i,\mathcal{R}}\mathbf{X}_{i,\mathcal{B}}$.

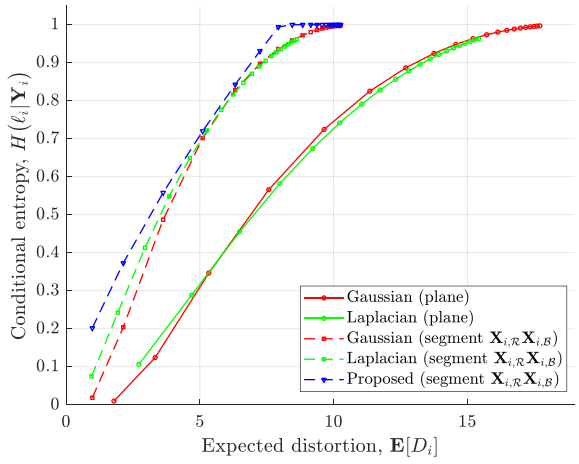

Fig. 13. Plots for obfuscation efficiency.

Laplacian noise on the line is not as vivid as the advantage over the 2D independent noise models on the plane [14,16]. For instance, the entropic gain for our method compared to the latter is up to 103%.

8. User authentication protocol

In this section, we define the requirements for authentication, technical means available in C-ITS, and propose our design of the authentication protocol (for analysis using BAN logic [32,33], see Appendix B). This protocol should be executed prior to the execution of algorithm 1.

For every user involved in the scheme, authentication must demonstrate exclusive control over a unique authenticator (e.g., based on an identifier). In addition, to protect from the replay attack, the authentication must be fresh and invoked at time step i of the current joint obfuscation session between *Alice* and *Bob*. To satisfy these requirements, we rely on the technical means that already exist in C-ITS.

Public Key Infrastructure (PKI) is essential for creating and managing digital certificates in transport systems: it supports public-key encryption and authentication. PKI is a part of the C-ITS ecosystem [2,3,34], including trustworthy V2X communication, since it provides an immutable record of all publicly accessible authenticators for which corresponding credentials are securely controlled by the legitimate entities registered with the PKI authority. Reliability and security of the PKI are central for the proper functioning of V2X and C-ITS in general: in our paper, we do not question these properties and assume that PKI functions correctly, and *Alice* and *Bob* are legitimate owners of the corresponding PKI credentials and use them securely.

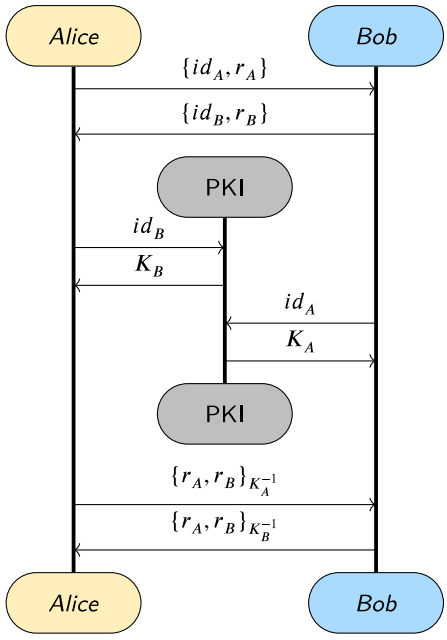

Fig. 14. Protocol for mutual authentication of *Alice* and *Bob*.

Cooperative Awareness Basic Service relies on numerous technical means, including individual On-board Units (OBU) installed in every vehicle [35,36]. Among other components, OBU includes a Hardware Security Module (HSM) implementing Elliptic Curves Digital Signature Algorithm (ECDSA) [37,38]. In the proposed authentication protocol, we assume that ECDSA is used for signing.

For our protocol (see Fig. 14), we make an assumption that *Alice* is incentivized to demand freshness from the authenticator used by *Bob*: a unique part of that authenticator, r_A, is randomly generated by *Alice* at time t and first submitted (with id_A of *Alice*) to *Bob* for signing. With a similar incentive, *Bob* generates unique random r_B at time $t+\Delta$ (we assume $\Delta \to 0$) and sends it with his id_B to Alice. A public key K_B corresponding to id_B can be retrieved from the PKI by *Alice*. As such, at time $t+2\Delta$, *Alice* expects *Bob* to send signed $\{r_A, r_B\}_{K_B^{-1}}$: this assertion from *Bob* now contains sufficient evidence about freshness and authenticity which can be verified by *Alice*. Finally, a public key K_A corresponding to id_A can be retrieved from the PKI by *Bob*. He then receives $\{r_A, r_B\}_{K_A^{-1}}$ from *Alice* at time $t+3\Delta$ and verifies freshness and authenticity of such an assertion.

By setting $seed_A \leftarrow r_A$, $seed_B \leftarrow r_B$ in the obfuscation algorithm 1, we achieve an authenticated key exchange (sharing). To protect confidentiality of $seed_A$, $seed_B$ (from *Eve*), r_A and r_B can be initially encrypted with the public keys of *Bob* and *Alice*, respectively. For the analysis of the proposed protocol using BAN logic, see Appendix B.

9. Discussion

In this paper, we combine: *(i)* a classical definition of unlinkability and strong GPA assumption to *(ii)* measure and improve privacy in C-ITS by developing a new optimal joint obfuscation technique implemented by *(iii)* an algorithm and supported by a two-party authentication protocol.

First, we use a classical definition of *unlinkability*, which is dictated by the standards governing the domain of C-ITS applications [1,19]. Based on the definition of unlinkability in Definition 2, we aim at creating uncertainty for the adversary: this uncertainty is expressed using Shannon entropy. We assume a strong GPA who knows the actual locations of *Alice* and *Bob* at every moment i. He also knows the probabilistic obfuscation and order-mixing algorithms used by the

users. The only aspects he does not know are the outputs of these probabilistic algorithms. His goal is then to infer the origin of the obfuscated messages. As a result of applying Assumption 1, the adversarial inference is very much simplified compared to the weak GPA situations [5]: information about HMM's hidden states (e.g., actual locations, velocities, etc.) and transition probabilities are not required for such reasoning. The latter detail is beneficial for privacy assurance since establishing probabilities for transitions in HMM is a laborious procedure whose outcome is often imprecise [26,39].

Second, the assumption about strong GPA helps us to *specify* the lower bound of messages' unlinkability in C-ITS. For every time step i unlinkability is defined through entropy $\mathcal{H}_{\mathrm{r},i}$: this lower bound of unlinkability corresponds to the worst-case adversarial inference (see Assumption 1). Components $\mathcal{H}_{\mathrm{r},i}$ are then summed over $N-1$ steps to obtain $\mathcal{H}_{\mathrm{r}}$ (see Lemma 1). Such summation is a simple and intuitive step. It is, nevertheless, justified because for any $i \in \{1, 2, \dots, N-1\}$, inference about the source (origin) of arrived CAM is independent of such inference at $i-1$. There is a similarity between entropy (unlinkability) values $\mathcal{H}_{\mathrm{r},i}$ and $\mathcal{H}_{\mathrm{r}}$, and the concepts of microscopic and macroscopic privacy, respectively [40]. Better protection of macroscopic privacy (e.g., trajectories) requires higher uncertainty about labels ℓ_i for the locations reported on the microscopic level. Higher uncertainty about labels of the users, ℓ_i, can only be achieved at the cost of higher expected distortion $\mathbb{E}[D_i]$ of their CAMs. To maximize uncertainty about labels, $\mathcal{H}_{\mathrm{r},i}$, under the constraint on distortions, $\mathbb{E}[D_i]$, we propose a new methodology. It allows defining a *joint distribution* for the obfuscation producing modified CAMs: the obfuscation must be conducted cooperatively by *Alice* and *Bob*. Optimality of (multivariate) noise parameters under distortion constraints has been researched by many authors in the past [14,16,17]. Our approach, however, differs: to improve microscopic privacy at i we apply data-dependent *joint probabilistic obfuscation* of the actual CAM-data from *different* users (see proof of Corollary 3). The superiority of our method over random Gaussian and Laplacian obfuscation models is also confirmed experimentally: the corresponding entropic gain reaches up to 103% (see Section 7). In addition, for the case when the corresponding total distortion cap is specified for the whole duration of observing *Alice* and *Bob* in C-ITS, we optimally allocate distortions over $N-1$ time steps (see Eq. (14)).

Third, all the findings of this paper are compactly represented in algorithm 1. Procedure `solve` is one of the major factors increasing the algorithm's time complexity. This, nevertheless, can be addressed if the obfuscation optimality is slightly sacrificed. For example, `solve` can be pre-computed for several cases only: each case would produce a distinct kind of distribution for a random variable $\frac{\Delta_i^2}{D}$. Then, the actual input data should be approximated by the best-matching distribution, and the corresponding pre-computed outputs of `solve` should be used for the obfuscation. Such a workaround can also turn our algorithm into a 'real-time algorithm': if *Alice* and *Bob* believe that their future data will align well with one of the pre-computed distributions (e.g., because of habitual daily commutes) they can obfuscate it 'on-the-fly'. Hence, the pre-computed cases for `solve` can be treated as *profiles* that pairs of users agree to use.

Among other properties, integrity and confidentiality of the algorithm's operations are paramount for privacy assurance attainable through obfuscation. Upon the algorithm invocation, *Alice* and *Bob* should be mutually authenticated: this assures the parties can be trusted to process privacy-sensitive data jointly. For instance, peers may be selected based on their reputation derived from previous events (such a reputation-based approach is a promising direction for further research). In Section 8, we provide the protocol for user authentication and a semi-formal analysis of its correctness (including authenticity and freshness of assertions) using BAN logic. Procedure `keySharing` allows *Alice* and *Bob* to securely share a seed used to produce a pair of pseudo-random numbers $\{r_1, r_2\}$, which they mutually agree on. This random pair is then used to simulate the outcomes of the probabilistic obfuscation producing $\mathbf{Y}_i$.

Finally, we plan to address some of this paper's limitations in our further studies. For example, only a strong GPA is considered in our paper to produce an assurance about minimally achievable unlinkability (e.g., rational lower bound, see Assumptions 1 and 2). However, in some situations, the assumption about a weaker GPA may be closer to the reality: in the future, we will use techniques from the domain of Multiple-Target Tracking to address this issue [26]. Only two users are considered for the obfuscation model proposed in Section 4. This is because constrained optimization tasks for cases involving more participants are nontrivial and may become computationally challenging. In the future, we plan to address this using methodologies (including heuristics) commonly applied to the optimization problem of maximum entropy [41,42]. Only limited in scope security assurance is conducted for the mutual authentication protocol in Section 8. In the future, we plan to extend this activity through a more detailed protocol analysis and formal analysis of the procedures in the obfuscation algorithm [43].

CRediT authorship contribution statement

Yevhen Zolotavkin: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Conceptualization. **Yurii Baryshev:** Writing – review & editing, Validation, Methodology, Investigation, Formal analysis. **Jannik Mähn:** Writing – review & editing, Methodology, Formal analysis. **Vitalii Lukichov:** Writing – review & editing, Visualization, Validation, Investigation. **Stefan Köpsell:** Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Proofs

Lemma 1. Unlinkability in V2X system (as per Fig. 2) is expressed as (for details see Appendix A):

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

Proof. For simplicity, we consider $N = 3$ only. First, it should be noted that

$$H\left(\ell_1, \ell_2 | \mathbf{Y}_1, \mathbf{Y}_2, \boldsymbol{\rho}\right) = H\left(\ell_1, \ell_2, \mathbf{Y}_1, \mathbf{Y}_2 | \boldsymbol{\rho}\right) - H\left(\mathbf{Y}_1, \mathbf{Y}_2 | \boldsymbol{\rho}\right) . \tag{15}$$

We then ponder at the right-hand side of Eq. (15). Each of these terms can be expressed as:

$$H\left(\ell_1, \ell_2, \mathbf{Y}_1, \mathbf{Y}_2 | \boldsymbol{\rho}\right) = H\left(\ell_2, \mathbf{Y}_2 | \ell_1, \mathbf{Y}_1, \boldsymbol{\rho}\right) + H\left(\ell_1, \mathbf{Y}_1 | \boldsymbol{\rho}\right) , \tag{16}$$

and

$$H\left(\mathbf{Y}_1, \mathbf{Y}_2 | \boldsymbol{\rho}\right) = H\left(\mathbf{Y}_2 | \mathbf{Y}_1, \boldsymbol{\rho}\right) + H\left(\mathbf{Y}_1 | \boldsymbol{\rho}\right) , \tag{17}$$

respectively. We point out that $H\left(\ell_2, \mathbf{Y}_2 | \ell_1, \mathbf{Y}_1, \boldsymbol{\rho}\right) = H\left(\ell_2, \mathbf{Y}_2 | \boldsymbol{\rho}\right)$ and $H\left(\mathbf{Y}_2 | \mathbf{Y}_1, \boldsymbol{\rho}\right) = H\left(\mathbf{Y}_2 | \boldsymbol{\rho}\right)$ in Eqs. (15) and (16), respectively. This follows from the fact that realizations of $\ell_i, \mathbf{Y}_i$ do not affect $\ell_{i+1}, \mathbf{Y}_{i+1}$. We finally stress that $\boldsymbol{\rho}$ is redundant for determining $\ell_{i+1}, \mathbf{Y}_{i+1}$ since only $\rho_{i+1} | \rho_i$ has relevance: $H\left(\mathbf{Y}_1 | \boldsymbol{\rho}\right) = H\left(\mathbf{Y}_1 | \{\rho_1 | \rho_0\}\right)$, $H\left(\ell_1, \mathbf{Y}_1 | \boldsymbol{\rho}\right) =$

$H(\ell_1, \mathbf{Y}_1|\{\rho_1|\rho_0\})$, $H(\mathbf{Y}_2|\boldsymbol{\rho}) = H(\mathbf{Y}_2|\{\rho_2|\rho_1\})$, $H(\ell_2, \mathbf{Y}_2|\boldsymbol{\rho}) = H(\ell_2, \mathbf{Y}_2|\{\rho_2|\rho_1\})$. Hence, Eq. (15) can be rewritten as

$$H(\ell_1, \ell_2|\mathbf{Y}_1, \mathbf{Y}_2, \boldsymbol{\rho}) = H(\ell_1, \mathbf{Y}_1|\{\rho_1|\rho_0\}) + H(\ell_2, \mathbf{Y}_2|\{\rho_2|\rho_1\}) - \left(H(\mathbf{Y}_1|\{\rho_1|\rho_0\}) + H(\mathbf{Y}_2|\{\rho_2|\rho_1\})\right). \quad (18)$$

The latter Eq. (18) can be regrouped

$$H(\ell_1, \ell_2|\mathbf{Y}_1, \mathbf{Y}_2, \boldsymbol{\rho}) = \left(H(\ell_1, \mathbf{Y}_1|\{\rho_1|\rho_0\}) - H(\mathbf{Y}_1|\{\rho_1|\rho_0\})\right) + \left(H(\ell_2, \mathbf{Y}_2|\{\rho_2|\rho_1\}) - H(\mathbf{Y}_2|\{\rho_2|\rho_1\})\right) = H(\ell_1|\mathbf{Y}_1, \{\rho_1|\rho_0\}) + H(\ell_2|\mathbf{Y}_2, \{\rho_2|\rho_1\}). \quad (19)$$ □

Lemma 2. For all $i \in [1, N-1]$ distribution $\rho_{\min,i}$ is degenerate (for details see Appendix A).

Proof. We presume that $\rho_{\min,i}$ is non-degenerate. For simplicity and without loss of generality we consider two-point distribution $\rho^*_{\min,i} : \{\mathbf{x}_1, \mathbf{x}_2\} \to [0,1]^2$. For instance, realizations $\mathbf{x}_1 = (x_1^A, x_1^B)$, $\mathbf{x}_2 = (x_2^A, x_2^B)$ can be used. Here $\Pr(\mathbf{X}_i = \mathbf{x}_1) = \xi$, and $\Pr(\mathbf{X}_i = \mathbf{x}_2) = 1 - \xi$.

Minimization of conditional entropy in Eq. (3) is equivalent to the minimization of $p_{\ell_i,\min}$ where

$$p_{\ell_i,\min} = \min\left\{\Pr(\ell_i = \mathcal{R} \mid \mathbf{Y}_i), \Pr(\ell_i = \mathcal{B} \mid \mathbf{Y}_i)\right\}, \quad (20)$$

and without loss of generality, we assume that $p_{\ell_i,\min} = \Pr(\ell_i = \mathcal{R} \mid \mathbf{Y}_i)$. To express $p_{\ell_i,\min}$ we then use Eqs. (4)–(6) and (8) with the following substitutions (simplifying expressions): $\alpha_1 = \varphi\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{R}} = (x_1^A, x_1^B))$, $\beta_1 = \varphi\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{R}} = (x_1^A, x_1^B)) + (1-\varphi)\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{B}} = (x_1^B, x_1^A))$, $\alpha_2 = \varphi\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{R}} = (x_2^A, x_2^B))$, $\beta_2 = \varphi\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{R}} = (x_2^A, x_2^B)) + (1-\varphi)\Pr(\mathbf{Y}_i \mid \mathbf{X}_{i,\mathcal{B}} = (x_2^B, x_2^A))$. The minimization task is then

$$\min_{\xi} p_{\ell_i,\min} = \min_{\xi} \frac{\xi\alpha_1 + (1-\xi)\alpha_2}{\xi\beta_1 + (1-\xi)\beta_2}. \quad (21)$$

By analyzing $\frac{\partial}{\partial\xi} p_{\ell_i,\min}$, we conclude that there are no local extrema for $\xi \in (0,1)$ and, hence, minimum is obtained in one of the end points, e.g., $\xi \in \{0,1\}$. □

Lemma 3. To minimize $D_{i,j}$ it is required that $\lambda_j = 1 - \Pr(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)})$ (for details see Appendix A).

Proof. From Eqs. (10) and (11) we derive that

$$D_{i,j} = p_j\Delta_i^2\lambda_j^2 + (1-p_j)\Delta_i^2(1-\lambda_j)^2,$$

where $p_j = \Pr(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_j^{(i)}) \le 0.5$, and $\Delta_i^2 = d(\tilde{\mathbf{X}}_{i,\mathcal{R}}, \tilde{\mathbf{X}}_{i,\mathcal{B}}) = \left\|\overline{\tilde{\mathbf{X}}_{i,\mathcal{R}}\tilde{\mathbf{X}}_{i,\mathcal{B}}}\right\|^2$. We next analyze $\frac{\partial}{\partial\lambda_j} D_{i,j}$ and find that $\lambda_j = 1 - p_j$ is the extremum (minimum) of $D_{i,j}$. □

Corollary 3. For every time step i, the highest lower bound (maxmin entropy) is (for details see Appendix A):

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

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

Proof. It is required: (1) to determine $\mathbb{Y}^{(i)}$ and probability distribution over it; (2) to determine $\Pr(\ell_i \mid \mathbf{Y}_i)$ for every element in $\mathbb{Y}^{(i)}$. For this, we demonstrate that maximum entropy under distortion constraint on $\mathbb{E}[D_i]$ is achieved for $|\mathbb{Y}^{(i)}| \le 2$: we analyze the case for $\mathbb{Y}^{(i)} = \left\{\mathbf{y}_1^{(i)}, \mathbf{y}_2^{(i)}\right\}$ where

$$\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right) = \Pr\left(\ell_i = \mathcal{B} \mid \mathbf{Y}_i = \mathbf{y}_2^{(i)}\right). \quad (22)$$

To prove the optimality of such settings, we consider several alternative cases where $\mathbb{E}[D_i] = \tilde{D}_i$ is fixed. Let us first consider an alternative case where $|\mathbb{Y}^{(i)}| = 2$ but

$$\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right) \ne \Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_2^{(i)}\right); \quad \Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right) \ne \Pr\left(\ell_i = \mathcal{B} \mid \mathbf{Y}_i = \mathbf{y}_2^{(i)}\right). \quad (23)$$

For simplicity, we use the following notations: $\Pr\left(\mathbf{Y}_i = \mathbf{y}_1^{(i)} \mid \tilde{\mathbf{X}}_i\right) = \alpha$, and $\Pr\left(\mathbf{Y}_i = \mathbf{y}_2^{(i)} \mid \tilde{\mathbf{X}}_i\right) = 1 - \alpha$; $\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right) = p_1 \le 0.5$, and $\Pr\left(\ell_i = \mathcal{R} \mid \mathbf{Y}_i = \mathbf{y}_2^{(i)}\right) = p_2 \ge 0.5$. Taking into account the expression for conditional entropy, we then require:

$$\begin{cases} \max[\mathcal{H}_{\mathrm{r},i}] = \max[\alpha H_1 + (1-\alpha)H_2]; \\ \tilde{D}_i = \alpha D_{i,1} + (1-\alpha)D_{i,2}, \end{cases} \quad (24)$$

where $H_1 = H\left(\ell_i \mid \mathbf{Y}_i = \mathbf{y}_1^{(i)}\right)$, $H_2 = H\left(\ell_i \mid \mathbf{Y}_i = \mathbf{y}_2^{(i)}\right)$. Based on Eq. (23) $D_{i,1} \ne D_{i,2}$. We now show that H_1 and H_2 are functions of $D_{i,1}$ and $D_{i,2}$, respectively. For this, we only point out that p_1 (similar results can be obtained for p_2) is a monotonically increasing function of $D_{i,1}$: it follows from Corollary 2 that $p_1 = \frac{\Delta_i - \sqrt{\Delta_i^2 - 4D_{i,1}}}{2\Delta_i}$. To demonstrate the fallacy of attaining both Eqs. (23) and (24) it is sufficient to show the following (concavity):

$$\alpha F(x) + (1-\alpha)F\left(\frac{\tilde{D}_i - \alpha x}{1-\alpha}\right) \le F(\tilde{D}_i), \quad (25)$$

where $x = D_{i,1}$, and $F(x) = -p_1(x)\log(p_1(x)) - (1-p_1(x))\log(1-p_1(x))$. The validity of Eq. (25) follows from

$$\frac{\partial}{\partial x}F(x) = \frac{1}{\Delta_i\theta}\log\left(\frac{\Delta_i+\theta}{\Delta_i-\theta}\right) \ge 0;$$

$$\frac{\partial^2}{\partial x^2}F(x) = -\frac{2}{\Delta_i\theta^2}\left(\frac{1}{\Delta_i+\theta} + \frac{1}{\Delta_i-\theta} - \frac{1}{\theta}\log\left(\frac{\Delta_i+\theta}{\Delta_i-\theta}\right)\right) \le 0,$$

where $\theta = \sqrt{\Delta_i^2 - 4x}$, and $x \in \left[0, \frac{\Delta_i^2}{4}\right]$.

Next, we point out a different case where $|\mathbb{Y}^{(i)}| > 2$ and demonstrate that it is non-optimal. For this we consider $|\mathbb{Y}^{(i)}| = 3$ while the conclusions for $|\mathbb{Y}^{(i)}| > 3$ can be derived inductively then. Similarly to Eq. (24) we demand

$$\begin{cases} \max[\mathcal{H}_{\mathrm{r},i}] = \max\left[\alpha H_1 + \beta H_2 + (1-\alpha-\beta)H_3\right]; \\ \tilde{D}_i = \alpha D_{i,1} + \beta D_{i,2} + (1-\alpha-\beta)D_{i,3}. \end{cases}$$

The task is then to show that there is $\mathbf{y}_4^{(i)}$ for which $D_{i,4} = \frac{\alpha D_{i,1} + \beta D_{i,2}}{\alpha+\beta}$, and $\max H_4 \ge \max\left[\frac{\alpha}{\alpha+\beta}H_1 + \frac{\beta}{\alpha+\beta}H_2\right]$. We henceforth maintain that $|\mathbb{Y}^{(i)}| \le 2$ represents optimal settings.

To obtain $\max[\alpha H_1 + (1-\alpha)H_2]$ in Eq. (24) it is sufficient that $H_1 = H_2$ and $D_{i,1} = D_{i,2} = \tilde{D}_i$. The latter requires that either $\lambda_1 = \lambda_2$ or $\lambda_1 = (1-\lambda_2)$: the first condition implies $p_1 = p_2 = 0.5$ and leads to a trivial situation where $\mathbf{y}_1^{(i)} = \mathbf{y}_2^{(i)} = 0.5(\tilde{\mathbf{X}}_{i,\mathcal{R}} + \tilde{\mathbf{X}}_{i,\mathcal{B}})$ meaning that $|\mathbb{Y}^{(i)}| = 1$. The second condition implies $p_1 = 1 - p_2$ and leads to $\mathbf{y}_1^{(i)} \ne \mathbf{y}_2^{(i)}$ if $\tilde{D}_i < 0.25\Delta_i^2$.

Requirement $\alpha \in [0,1]$ must be consistent with the order mixing probability φ:

$$\alpha p_1 + (1-\alpha)p_2 = \varphi, \quad (26)$$

from which we derive $\alpha = \frac{\varphi + p_1 - 1}{2p_1 - 1}$ demanding $\varphi \ge p_1$. Alternatively, this demand can be understood based on the fact $H(\ell_i) \ge H(\ell_i \mid \mathbf{Y}_i)$: setting $p_1 > \varphi$ results in a greater distortion, but this does not increase entropy. □

Appendix B. Protocol analysis

BAN logic is a convenient tool for developing a medium level assurance for authentication protocols [33]. For the analysis, we represent the protocol in the idealized form. Based on the previous sub-section, we use the following premises:

- *Alice* (*A* for short) and *Bob* (*B* for short) possess corresponding public and private keys. As such, in terms of BAN logic we have: (i) $\boxed{\overset{K_A}{\longmapsto} A}$, (ii) $\boxed{A \Rightarrow {K_A}^{-1}}$, (iii) $\boxed{\overset{K_B}{\longmapsto} B}$, (iv) $\boxed{B \Rightarrow {K_B}^{-1}}$;
- PKI functions properly and propagates information about credentials, meaning that: (v) $\boxed{\overset{K_B}{\longmapsto} A}$, (vi) $\boxed{A \mid\equiv \left(B \Rightarrow {K_B}^{-1}\right)}$, (vii) $\boxed{\overset{K_A}{\longmapsto} B}$, (viii) $\boxed{B \mid\equiv \left(A \Rightarrow {K_A}^{-1}\right)}$;
- *Alice* and *Bob* generate random numbers r_A and r_B, respectively. Therefore, they have confidence that the numbers are fresh: (ix) $\boxed{A \mid\equiv \left(\#(r_A)\right)}$, (x) $\boxed{B \mid\equiv \left(\#(r_B)\right)}$;
- *Alice* and *Bob* send to each other the generated random numbers, and we have: (xi) $\boxed{A \triangleleft r_B}$, (xii) $\boxed{B \triangleleft r_A}$;
- *Alice* and *Bob* privately compose tuples (r_A, r_B) (we ignore id_A and id_B for simplicity), sign them, and send these signed tuples to each other: (xiii) $\boxed{A \triangleleft \{r_A, r_B\}_{{K_B}^{-1}}}$, (xiv) $\boxed{B \triangleleft \{r_A, r_B\}_{{K_A}^{-1}}}$.

According to BAN logic, we now demonstrate that the assertion sent to *Alice* by *Bob* in (xiii) is sufficient to **believe** that *Bob* **said** (r_A, r_B), and this statement is **fresh**. First, we use (v) and (xiii) to infer that private key of *Bob*, ${K_B}^{-1}$, was used on (r_A, r_B):

$$\frac{A \triangleleft \{r_A, r_B\}_{{K_B}^{-1}},\ \overset{K_B}{\longmapsto} A}{A \mid\equiv \langle r_A, r_B\rangle_{{K_B}^{-1}}}. \tag{27}$$

Second, we use (vi) and the result of Eq. (27) to infer that *Bob* said (r_A, r_B):

$$\frac{A \mid\equiv \langle r_A, r_B\rangle_{{K_B}^{-1}},\ A \mid\equiv \left(B \Rightarrow {K_B}^{-1}\right)}{A \mid\equiv \left(B \mid\sim (r_A, r_B)\right)}. \tag{28}$$

Third, we use (ix) and the result of Eq. (28) to demonstrate freshness of the *Bob*'s assertion:

$$\frac{A \mid\equiv \left(B \mid\sim (r_A, r_B)\right),\ A \mid\equiv \left(\#(r_A)\right)}{A \mid\equiv \left(B \mid\sim \left(\#(r_A, r_B)\right)\right)}. \tag{29}$$

Based on the above inference, *Alice* develops an assurance that assertion $\{r_A, r_B\}_{{K_B}^{-1}}$ is authentic (received from *Bob*) and supports fresh claim (r_A, r_B). Similar results can be demonstrated for the assertion $\{r_A, r_B\}_{{K_A}^{-1}}$ received by *Bob*. Hence, at the end of the protocol on Fig. 14, *Alice* and *Bob* are authenticated to each other.

Data availability

No data was used for the research described in the article.

References

[1] ISO 24102-1, ITS Station Management — Part 1: Local Management, International Standard, International Organization for Standardization, Geneva, CH, 2018, p. 44.

[2] C-ITS Platform, Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS); Release 1.1, Technical Specification, European Commission, EU, 2018, p. 81.

[3] M. Hasan, S. Mohan, T. Shimizu, H. Lu, Securing vehicle-to-everything (V2X) communication platforms, IEEE Trans. Intell. Veh. 5 (4) (2020) 693–713, http://dx.doi.org/10.1109/TIV.2020.2987430.

[4] ISO/IEC 15408-2, Evaluation Criteria for IT Security — Part 2: Security Functional Components, International Standard, International Organization for Standardization, Geneva, CH, 2022, p. 273.

[5] R. Shokri, Quantifying and Protecting Location Privacy (Ph.D. thesis), EPFL, Lausanne, 2012.

[6] M. Khodaei, P. Papadimitratos, Cooperative location privacy in vehicular networks: Why simple mix zones are not enough, IEEE Internet Things J. 8 (10) (2021) 7985–8004, http://dx.doi.org/10.1109/JIOT.2020.3043640.

[7] S. Blackman, Multiple hypothesis tracking for multiple target tracking, IEEE Aerosp. Electron. Syst. Mag. 19 (1) (2004) 5–18, http://dx.doi.org/10.1109/MAES.2004.1263228.

[8] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, X. Huang, PAPU: Pseudonym swap with provable unlinkability based on differential privacy in VANETs, IEEE Internet Things J. 7 (12) (2020) 11789–11802, http://dx.doi.org/10.1109/JIOT.2020.3001381.

[9] N. Takbiri, A. Houmansadr, D.L. Goeckel, H. Pishro-Nik, Privacy of dependent users against statistical matching, IEEE Trans. Inform. Theory 66 (9) (2020) 5842–5865–5842–5865, http://dx.doi.org/10.1109/TIT.2020.2985059.

[10] I. Wagner, D. Eckhoff, Technical privacy metrics: A systematic survey, ACM Comput. Surv. 51 (3) (2018) http://dx.doi.org/10.1002/dac.4678, 1–38–1–38.

[11] R. Shokri, G. Theodorakopoulos, C. Troncoso, Privacy games along location traces: A game-theoretic framework for optimizing location privacy, ACM Trans. Priv. Secur. 19 (4) (2016) 11:1–11:31, http://dx.doi.org/10.1145/3009908.

[12] H. Wang, H. Hong, L. Xiong, Z. Qin, Y. Hong, L-SRR: Local differential privacy for location-based services with staircase randomized response, in: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, in: CCS '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 2809–2823, http://dx.doi.org/10.1145/3548606.3560636.

[13] Q. Geng, P. Viswanath, The optimal mechanism in differential privacy, in: 2014 IEEE International Symposium on Information Theory, IEEE, Honolulu, HI, USA, 2014, pp. 2371–2375, http://dx.doi.org/10.1109/ISIT.2014.6875258.

[14] M. Sun, C. Zhao, J. He, P. Cheng, D.E. Quevedo, Privacy-preserving correlated data publication: Privacy analysis and optimal noise design, IEEE Trans. Netw. Sci. Eng. 8 (3) (2021) 2014–2024, http://dx.doi.org/10.1109/TNSE.2020.3044590.

[15] T. Chanyaswad, A. Dytso, H.V. Poor, P. Mittal, MVG mechanism: differential privacy under matrix-valued query, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, in: CCS '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 230–246, http://dx.doi.org/10.1145/3243734.3243750.

[16] T. Ji, P. Li, Less is more: Revisiting Gaussian mechanism for differential privacy, 2023, http://dx.doi.org/10.48550/arXiv.2306.02256, arXiv:2306.02256.

[17] N. Fernandes, A. McIver, C. Palamidessi, M. Ding, Universal optimality and robust utility bounds for metric differential privacy, in: 2022 IEEE 35th Computer Security Foundations Symposium, CSF, IEEE, Haifa, Israel, 2022, pp. 348–363, http://dx.doi.org/10.1109/CSF54842.2022.9919647.

[18] K. Chatzikokolakis, M.E. Andrés, N.E. Bordenabe, C. Palamidessi, Broadening the scope of differential privacy using metrics, in: D. Hutchison, T. Kanade, J. Kittler, J.M. Kleinberg, F. Mattern, J.C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M.Y. Vardi, G. Weikum, E. De Cristofaro, M. Wright (Eds.), Privacy Enhancing Technologies, vol. 7981, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 82–102, http://dx.doi.org/10.1007/978-3-642-39077-7_5.

[19] ETSI TS 102 941, Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2, Technical Specification, European Telecommunications Standards Institute, Sophia Antipolis, France, 2021, p. 59.

[20] C. Hicks, F.D. Garcia, A vehicular DAA scheme for unlinkable ECDSA pseudonyms in V2X, in: 2020 IEEE European Symposium on Security and Privacy, EuroS&P, IEEE, Genoa, Italy, 2020, pp. 460–473, http://dx.doi.org/10.1109/EuroSP48549.2020.00036.

[21] ISO/SAE 21434, Road Vehicles — Cybersecurity Engineering, International Standard, International Organization for Standardization, Geneva, CH, 2021, p. 81.

[22] ETSI EN 302 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, Technical Specification, European Telecommunications Standards Institute, Sophia Antipolis, France, 2019, p. 23.

[23] J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, P. Towa, Zone encryption with anonymous authentication for V2V communication, in: 2020 IEEE European Symposium on Security and Privacy, EuroS&P, IEEE, Genoa, Italy, 2020, pp. 405–424, http://dx.doi.org/10.1109/EuroSP48549.2020.00033.

[24] S. Escher, M. Sontowski, K. Berling, S. Köpsell, T. Strufe, How well can your car be tracked: Analysis of the European C-ITS pseudonym scheme, in: 2021 IEEE 93rd Vehicular Technology Conference, VTC2021-Spring, 2021, pp. 1–6, http://dx.doi.org/10.1109/VTC2021-Spring51267.2021.9449078.

[25] ETSI TS 102 894-2, Intelligent Transport Systems (ITS); Users and Applications Requirements; Part 2: Applications and Facilities Layer Common Data Dictionary, Technical Specification, European Telecommunications Standards Institute, Sophia Antipolis, France, 2018, p. 14.

[26] S.S. Blackman, Multiple-target tracking with radar applications, 1986.

[27] M. Sniedovich, Wald's mighty maximin: A tutorial, Int. Trans. Oper. Res. 23 (4) (2016) 625–653, http://dx.doi.org/10.1111/itor.12248.

[28] Y. Cao, W. Liu, L. Qin, B. Liu, S. Chen, J. Ye, X. Xia, C. Wang, Entropy sources based on silicon chips: True random number generator and physical unclonable function, Entropy 24 (11) (2022) http://dx.doi.org/10.3390/e24111566.
[29] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, Inc, Indianapolis, Indiana, 2010.
[30] Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, Richard Davis, NIST special publication 800-56A. Revision 3. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography, 2018.
[31] NIST FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, International Standard, National Institute of Standards and Technology, Gaithersburg, MD, 2015.
[32] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36, http://dx.doi.org/10.1145/77648.77649.
[33] A. Rubin, P. Honeyman, Formal methods for the analysis of authentication protocols, 1993.
[34] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, R. Goudy, A security credential management system for V2X communications, IEEE Trans. Intell. Transp. Syst. 19 (12) (2018) 3850–3871, http://dx.doi.org/10.1109/TITS.2018.2797529.
[35] Unex, V2X mPCIe system-on-module, 2023, URL: https://unex.com.tw/pdf/SOM-352.pdf.
[36] Commsignia, Commsignia ITS-OB4: powerful V2X onboard unit, 2020, URL: https://www.commsignia.com/wp-content/uploads/2020/11/Commsignia_ITS_OB4_ProductBrief_v0.9.5_22062020_web.pdf.
[37] Don Johnson, Alfred Menezes, Scott Vanstone, The Elliptic Curve Digital Signature Algorithm (ECDSA), Technical Report, 1999, p. 55.
[38] NIST FIPS 186-5, Digital Signature Standard (DSS), International Standard, National Institute of Standards and Technology, Gaithersburg, MD, 2023.
[39] F. Lehmann, W. Pieczynski, Suboptimal Kalman filtering in triplet Markov models using model order reduction, IEEE Signal Process. Lett. 27 (2020) 1100–1104, http://dx.doi.org/10.1109/LSP.2020.3002420.
[40] R. Shokri, J. Freudiger, J.-P. Hubaux, A unified framework for location privacy, in: The 3rd Workshop on Hot Topics in Privacy Enhancing Technologies, HotPETS 2010, Berlin, Germany, 2010, pp. 74–94.
[41] D. Dowson, A. Wragg, Maximum-entropy distributions having prescribed first and second moments (Corresp.), IEEE Trans. Inform. Theory 19 (5) (1973) 689–693, http://dx.doi.org/10.1109/TIT.1973.1055060.
[42] P.J. Coles, M. Berta, M. Tomamichel, S. Wehner, Entropic uncertainty relations and their applications, Rev. Modern Phys. 89 (1) (2017) 015002, http://dx.doi.org/10.1103/RevModPhys.89.015002.
[43] S. Meier, B. Schmidt, C. Cremers, D. Basin, The TAMARIN prover for the symbolic analysis of security protocols, in: N. Sharygina, H. Veith (Eds.), Computer Aided Verification, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 696–701.

Zolotavkin, Yevhen received a B.S. degree in computerized automation and control systems in 2003 and an M.S. degree in control and automation systems in 2004 from Vinnytsia National Technical University (VNTU), Ukraine. In 2010, he received his Candidate of Science degree in information protection systems from National Aviation University, Kyiv, Ukraine. In 2015, he defended his PhD in information and systems from the University of Tampere, Finland. During 2016 – 2019 worked as a postdoctoral fellow at Monash University, Australia. During 2019 – 2021 worked as a postdoctoral fellow at Deakin University, Australia. Since 2022, he has been a senior researcher at Barkhausen Institut, Trustworthy Data Processing (TDP) group, Dresden, Germany. Interests include system privacy (unlinkability), security, and trustworthiness.

Yurii Baryshev received the B.S. degree in information protection of computer systems and networks and M.S. degree in information security from Vinnytsia National Technical University (VNTU), Vinnytsia, Ukraine, in 2007 and 2008, respectively, and the Ph.D. degree in computer systems and components with thesis on the topic "Methods and means of rapid multi-piped data hashing in computer systems" from VNTU, Vinnytsia, Ukraine, in 2012. In 2008 he joined academic staff of VNTU, where he is currently employed as the associate professor of the Information Protection department. His research interests include cryptography, distributed systems security, software development security, databases.

Vitalii Lukichov received the B.S. degree in computerized automation and control systems in 2003 and the M.S. degree in control and automation systems in 2004 from Vinnytsia National Technical University (VNTU), Vinnytsia, Ukraine, and in 2010 received his Ph.D. degree in information protection systems with thesis on the topic "Methods and means of steganographic information protection in computer systems and networks based on wavelet transforms" from National Aviation University, Kyiv, Ukraine. In 2011, he joined the academic staff of VNTU, where he currently works as the associate professor of the Information Protection department. His research interests include steganography, modeling, unlinkability, privacy.