# A Survey on Privacy-preserving Electronic Toll Collection Schemes for Intelligent Transportation Systems

Amirhossein Adavoudi Jolfaei, Abdelwahab Boualouache, *Member*, *IEEE*, Andy Rupp, Stefan Schiffner, and Thomas Engel, *Member*, *IEEE*

**Abstract**—As part of Intelligent Transportation Systems (ITS), Electronic toll collection (ETC) is a type of toll collection system (TCS) which is getting more and more popular as it can not only help to finance the government's road infrastructure but also it can play a crucial role in pollution reduction and congestion management. As most of the traditional ETC schemes (ETCS) require identifying their users, they enable location tracking. This violates user privacy and poses challenges regarding the compliance of such systems with privacy regulations such as the EU General Data Protection Regulation (GDPR). So far, several privacy-preserving ETC schemes have been proposed. To the best of our knowledge, this is the first survey that systematically reviews and compares various characteristics of these schemes, including components, technologies, security properties, privacy properties, and attacks on ETCS. This survey first categorizes the ETCS based on two technologies, GNSS and DSRC. Then under these categories, the schemes are classified based on whether they provide formal proof of security and support security analysis. We also demonstrate which schemes specifically are/are not resistant to collusion and physical attacks. Then, based on these classifications, several limitations and shortcomings in privacy-preserving ETCS are revealed. Finally, we identify several directions for future research.

**Index Terms**—Intelligent Transportation Systems, Electronic Toll Collection Schemes, Privacy, Security.

## 1 Introduction

Intelligent Transportation Systems (ITS) have been designed to address several issues such as congestion, pollution, and accidents due to the significant increase in vehicular traffic, public transportation, fright, etc [1]. ITS data flow includes three main components: data collection, data analysis, and data dissemination [2]. The data collection component gathers information such as time, location, traffic flow, fuel consumption, etc. Later, such data can be analyzed for various applications: electronic toll collection (ETC), traffic statistic collection, road safety, automated traffic law enforcement, insurance pricing, and user convenience [3, 4]. ETC systems aim to improve road tolling by collecting tolls automatically, without slowing down the vehicles, as opposed to a manual toll collection system which drastically slows down the vehicles, thus causing delay and congestion. It is anticipated that the global electronic toll collection market, between 2019 and 2030, to have a compound annual growth rate (CAGR) of 8.3 percent, reaching around 18.5 billion U.S. dollars by 2030 [5].

Toll service providers (TSP) store various information, including times, locations, and vehicle identities, to bill drivers. The stored information could cause privacy issues in ETC systems, violating the EU General Data Protection Regulation (GDPR) articles[1]. The paper [6] summarizes the privacy issues associated with ETC systems. One of the key concerns is that the TSP may use drivers' data to learn their movement patterns, including where they go for work or recreation, creating individual travel profiles [7]. This practice would compromise the principle named "purpose limitation" stated in GDPR (Art. 5 GDPR). Another potential issue is that third parties, such as insurance companies, may find the data commercially valuable and wish to use it. In such a case, the usage of drivers' data by third parties should be subject to the customer's consent as specified in GDPR (Art. 7 GDPR). Data security is another aspect of privacy issues in ETC systems and is about ensuring that information is secured from external access and internal leakage. If security measures are not adequately considered, the external entities could learn about the data transmitted over the network, or the internal employees could infer information they are not supposed to. This is against the GDPR principle stating that data should be processed in a way that guarantees the security of the personal data appropriately (Art. 5 GDPR).

We give several examples demonstrating how toll data can violate privacy. According to an associated press survey, EZ-Pass records can provide courts with toll information as evidence in criminal and civil cases [8]. The New York civil liberties union states that wireless EZ-Pass transponders routinely gather private data, including the location data about drivers [9]. As another example, user profiling uses toll data, including time and location, to extract users' places of interest and movement patterns [6, 10, 11], and to monitor road traffic [12]. These examples show that more vehicles are becoming worried about their privacy in ETC systems. To handle this issue, researchers have presented privacy-preserving ETC schemes (ETCS). The objective of ETCS is to

*A. Jolfaei, A. Boualouache, A. Rupp, and T. Engel are with University of Luxembourg, Esch-sur-Alzette, AVE, 4365, Luxembourg e-mail: ({amirhossein.adavoudi,abdelwahab.boualouache,andy.rupp,thomas.engel}@uni.lu) S. Schiffner is with University of Münster, Germany, e-mail: ({stefan.schiffner}@uni-muenster.de).*

1. https://gdpr.eu/tag/chapter-2/

provide security and privacy for drivers.

An adversary in ETCS could perform various attacks violating security and privacy, which a malicious driver or a malicious toll service provider can do. The adversary, for example, can bene t from various tracking algorithms to track vehicles in an ETC system [13–17]. These algorithms typically get as input information such as drivers' locations, times, and toll fees and try to track vehicles, meaning to learn the locations visited by a driver [18].

The ETC schemes are based on different technologies and components, aiming to make ETC systems resistant to potential attacks. However, each of these schemes has its shortcomings. Some schemes, for example, lack formal security proof or lack implementation, thus making these schemes impractical in real-world scenarios. Or some of them focused only on a few attacks, and other potential attacks are not considered seriously. To the best of our knowledge, this survey is the  rst one that mainly focuses on the taxonomy of privacy-preserving ETCS. This survey collects and categorizes all potential security and privacy properties in such schemes. Additionally, based on our review, all potential attacks on ETCS are collected and grouped into various categories. Based on our categorizations and the analysis of the reviewed ETCS, several open directions are recommended, which pave the way for researchers to design privacy-preserving ETCS and guide toll engineers to deploy privacy-preserving ETC systems.

### Contributions

The main contributions of this survey can be summarized as follows:

- We discuss in detail the general aspects of ETC systems in Section 2, such as components of ETC systems and technologies of ETC systems. Then, we present the security aspects of ETCS in Section 3, including protection measures for ETCS, attacks on ETCS, and formal security de nitions in ETCS.
- We group ETCS, in Section 4, based on the technology used in them for operation: privacy-preserving GNSS-based schemes and privacy-preserving DSRC-based schemes. Afterward, under each group, we cluster them based on whether they support/do not support formal security proofs. Under each category, we discuss in detail the schemes.
- We analyze the discussed schemes under two categories, namely privacy-preserving GNSS-based schemes and privacy-preserving DSRC-based schemes (Sections 4.1.3 and 4.2.3). We discuss which schemes are/are not resistant to collusion and physical attacks and then discuss the other attacks to which these schemes are vulnerable and the performance of such schemes.
- We give some research direction to researchers concerning the design of privacy-preserving ETCS (Section 5).

### Search methodology

We have used the following relevant keywords and their combinations in search engines, which cover our research study: “privacy-preserving”, “toll collection”, “toll system”, “toll pricing”, “electronic traf c pricing”, “road pricing”, “Pay-as-you-drive”, “eCash”, “VANETs”, “security”, “blockchain”, “machine learning”, “deep learning”, “location-based services”, “Vehicular ad hoc network”, “survey”, and, we  nally found 650 papers. The year of publication of the resulting articles is between 2001 and 2022. The resulting papers fall into various publisher categories, including IEEE, ACM, Springer, and PETS. Then, we  ltered the collected papers by examining their titles and abstracts and excluded the unrelated and duplicated papers. In the end, 65 papers were studied and discussed in our survey.

Fig. 1 illustrates the road map of the paper. In Section 2, we discuss general aspects of ETC systems, and afterward, we elaborate on the security aspects of ETC systems in Section 3. The taxonomy of privacy-preserving ETCS is set out in Section 4. Sections 4.1.3 and 4.2.3 analyze the presented schemes. Section 5 gives some guidelines and proposes future research directions in ETCS. Finally, Section 6 concludes the survey.

TABLE 1
List of acronyms.

| Full name | Acronym |
|---|---|
| ANPR | Automated number plate recognition |
| AS | Aggregate signature |
| BC | Blockchain |
| BS | Blind signature |
| DL | Deep learning |
| DS | Digital signature |
| DSRC | Dedicated short-range communications |
| EC | Elliptic curve |
| ETC | Electronic toll collection |
| ETCS | ETC schemes |
| ETP | Electronic Toll pricing |
| FHE | Fully homomorphic encryption |
| GDPR | General Data Protection Regulation |
| GNSS | Global navigation satellite system |
| GPS | Global positioning system |
| GSM | global system for mobile communication |
| GSS | Group signature scheme |
| HC | Homomorphic commitment |
| HS | Homomorphic scheme |
| ITS | Intelligent Transportation Systems |
| LEZ | Low-Emission Zones |
| ML | Machine Learning |
| NIZK | Non-interactive zero-knowledge |
| OBU | On-board unit |
| OT | Oblivious transfer |
| PBFT | Practical Byzantine fault tolerance |
| PKES | Public key encryption scheme |
| POT | Priced oblivious transfer |
| PPT | Probabilistic polynomial time |
| PRF | Pseudo-random function |
| PRNG | pseudo-random number generator |
| RSU | Road-side unit |
| SE | Secure element |
| SMC | Secure multi-party computation |
| SRP | Smart road pricing systems |
| SS | Signature scheme |
| TC | Toll charger |
| TCR | threshold cryptography |
| TSP | Toll service provider |
| TTP | Trusted third party |
| ZKP | Zero-knowledge proof |

## 2 The general aspects of ETC systems

We give an overview of general aspects of ETC systems that seem necessary to understand privacy-preserving ETCS

Fig. 1. The road map of the paper

discussed in Sections 3 and 4. In the following, we elaborate on the aspects, including components of ETC systems, technologies in ETC systems, storage of private locations in ETC systems, payment methods, and charging schemes. The list of all acronyms used in this survey is presented in Table 1.

### 2.1 Components of ETC systems

We de ne the components typically used in an ETC system.

Toll service provider (TSP): This provider may be a private company that stores private location records to bill drivers, or in case of law enforcement, the TSP can provide the required private data to the related organization [19].

On-Board Unit (OBU): The OBU is a device that is installed on a vehicle to collect various information with the help of different sensors. This collected data can be processed and exchanged for different purposes, such as paying the toll fee [20].

Road-side Unit (RSU): This device communicates with the OBU and is generally managed by the TSP. It makes the routing of messages ef cient.

Enforcement system: This component handles various violations, i.e., when drivers do not honestly follow the protocol. For handling these violations, there are various mechanisms such as taking photos of license plates automatically via cameras or other mechanisms such as detecting a vehicle class to which a car belongs, a police control, or challenging the OBUs [21]. The enforcement can be done upon a request from the court or any authorized organization [19, 22].

Driver: This component typically must subscribe to a system such as TSP and reveal its identity, e.g., the passport. The driver uses the OBU to interact with other devices, such as RSU, to pay the toll fee.

Toll charger (TC): It is either a public or private organization that imposes tolls for road usage, and it de nes the correct use of the ETC system. In accordance with the TC, the TSP considers prices for the usage of the roads [21].

### 2.2 Technologies in ETC systems

For establishing an ETC, three types of technologies are typically used.

Dedicated short-range communications (DSRC): DSRC is widely used and falls into the radio frequency or microwave range of the electromagnetic spectrum. In this technology, antennas are installed on the toll gantries communicating with mounted transponders or tags in vehicles as they pass by [23]. Fig. 2 shows a DSRC-based ETC system. We brie y sketch the interactions between the components as follows. A driver submits their identity, such as a passport, to the TSP and receives an ID. When a vehicle passes a toll gantry, the OBU, located inside the vehicle, communicates with the RSU to compute the total toll fee. The RSU, from time to time, sends its information to the TSP for updating. Finally, the TSP issues an invoice for the driver at the end of the billing period, and accordingly, the driver pays the total toll fee, which s/he owes to the TSP.

Fig. 2. Components of a DSRC-based ETC system

Global navigation satellite system (GNSS): OBU, with the help of the Global Positioning System (GPS), receives the vehicle's location from the GPS satellite and measures its road usage. For communicating with the TSP, the GNSS and global system for mobile communication (GSM) are used together [19]. Fig. 3 shows a GNSS-based ETC system. As the gure shows, the vehicle autonomously obtains its locations and then calculates the nal total fee based on road usage or other parameters. In these systems, private locations are typically stored in the OBU, and the TSP is not aware of drivers' locations as opposed to DSRC-based systems where the RSU and TSP learn anonymous drivers' locations.

Fig. 3. Components of a GNSS-based ETC system [21]

Automated number plate recognition (ANPR): This technology bene ts from digital cameras and optical character recognition (OCR) to make photos of drivers. ANPR is typically used for enforcement purposes as it can provide evidence in case a driver behaves maliciously. It should be noted that ANPR inherently violates drivers' privacy [19, 23, 24].

### 2.3 Storage of private locations in ETC Systems

In [12, 25], the authors group ETC systems into two categories based on where the locations data is stored. Each approach has its own merits and disadvantages:

Location data stored on user devices: In this category, it is the user device, e.g., OBU, that manages and collects the locations and tolls, while servers are responsible for processing aggregated data. This approach reduces the issues of location privacy; however, the user bears the burden of storing travel history and the heavy computation, e.g., constructing zero-knowledge proofs (ZKP).
Location data stored on a central toll server: In this approach, the server stores and manages all the drivers' transactions. Applications such as traf c control and monitoring can bene t from this approach, while this might threaten the users' privacy.

### 2.4 Payment methods

There are two types of methods for paying toll fees.

Post-payment: in this type of payment, a driver will pay the total toll fee after a period, e.g., a month. The total toll fee is the summation of all the toll fees a driver owes to a toll provider [19].
Pre-payment: in this method, a driver will pay in advance a xed amount of toll fee [26].

### 2.5 Charging schemes

In ETCS, dynamic pricing is usually the ef cient type of pricing and the reasonable way to calculate the toll rate [27]. Dynamic pricing can be applied to control traf c and pollution based on various pricing schemes. Each ETC might use one or a mixture of the following pricing schemes based on its policies and regulations:

Class-based: Toll rate can be calculated based on different parameters related to a vehicle, including air pollution and noise caused by a car. Also, the number of axles and the vehicle's weight may be considered in this calculation [23]. Different classes could be de ned concerning the level of the toll rate; for example, [28] demonstrates six different classes from Euro1 to Euro6.
Distance-based: This pricing scheme encourages drivers to control their travel behaviors, such as the number of trips, mode of transport, etc. Even drivers might choose the place of their home and work to reduce the distance from home to work [23, 29].
Zone-based: This pricing scheme is typically used in urban areas to control not only traf c congestion but also air pollution in particular zones. A zone might include roads, bridges, tunnels, etc. These zones are called Low-Emission Zones (LEZ) in [23, 30–32]. Great cities try to control the number of vehicles entering areas with high levels of traf c jams and pollution. The vehicles must pay a toll when entering a zone.
Access/Facility-based: Toll can be imposed on a speci c facility, e.g., roads, tunnels, and bridges, or even levied on all or designated lanes of a facility [19, 23]. Access to a facility could be allowed based on the time of the day, e.g., rush hours [21].

# 3 THE SECURITY ASPECTS OF ETCS

We elaborate on the security aspects of ETCS, including protection measures for ETCS, attacks on ETCS, and formal security de nitions in ETCS.

## 3.1 Protection Measures for ETCS

In this subsection, we discuss two various protection measures for ETCS: security properties and privacy properties.

### 3.1.1 Security properties

Security properties of an ETC scheme, including authentication, con dentiality, availability, and integrity, are discussed here.

Con dentiality: In an ETC scheme, there can be different communication channels between the ETC's components, i.e., the channel between an RSU and a driver, a driver and a TSP, or an RSU and a TSP, etc. Based on the security policies of such a system, any of these channels can be con dential, which means no adversary should be able to eavesdrop on the channel [3, 19].
Integrity: This property guarantees that the content of a message sent or received by a driver in an ETCS is not modi ed by an adversary [33].
Availability: There should be mechanisms for the availability of the ETC's components which have to be accessible timely in the presence of malicious or faulty conditions. The cryptographic protocols used in an ETC scheme should be computationally and communicationally ef cient to provide data in a timely manner [3, 33, 34].
Authentication: In an ETC scheme, for communication between a driver and a server (e.g., a TSP), the driver has to register at the server [34, 35].
Non-repudiation: Using cryptographic signature schemes (SS), we can ensure that the sender or receiver of messages cannot falsely deny having been involved in a communication [33]. It is worth mentioning that using digital signature (DS) schemes should not sacri ce the anonymity property in case an ETC scheme requires such property.
Access control: By permitting authorized entities, they can access the services and the information which they are eligible for. For example, in an ETC scheme, only law enforcement authorities can access malicious drivers' private location records [35].
Physical security: To prevent drivers from manipulating the OBU, security measurements should be taken. For example, the scheme presented in [4] prevents a malicious driver from disabling the OBU.
Enforcement/Auditing: Misbehaving drivers can be detected using this property. A random spot check is an approach for the detection of such drivers. Typically, the random spot checks are used to check the correctness of the location or the fee calculation [21, 25]. In random spot locations, the time and the location where a vehicle has passed are recorded as proof. To record this data, e.g., an automatic license plate reader, a police control, or a camera can be used [21]. Tamper-resistant devices can force drivers to provide the correct data; however, a malicious driver might deactivate the OBU [25].
Accountability: Under certain conditions (e.g., a driver misbehaves), tracking of a malicious user should be possible. For example, the TSP should be able to disclose the misbehaved user's location records upon request from a law enforcement authority [3, 34, 36]. The papers [25, 37] used the term “traceability”, which implies the same notion as Accountability.
Blacklisting/Revocation: A TSP might need to blacklist a malicious driver to prevent his/her negative impact on an ETC scheme [3].

### 3.1.2 Privacy properties

Drivers in an ETC scheme wish to keep their private records con dential, including time and location. Drivers want to ensure that the ETC operators will not abuse the past, present, and future history of their transaction records. To this end, the following privacy features should be considered.

Anonymity: This privacy feature concerns the protection of a user's identity, which means the user can be authenticated and uses the available services and resources without revealing his/her identity [3]. The term anonymity in [38] is de ned as “the state of being not identi able within a set of subjects”. In an ETC scheme, the messages sent to the TSP by drivers should be anonymized so an attacker cannot associate the messages with the corresponding drivers. If a user is de-anonymized by an adversary due to a privacy attack, tracking a user can be done more easily. In fact, by combining the obtained identity with additional information, e.g., the mobility pro le of the user [39], the adversary can perform tracking and subsequently might commit crimes such as automobile thefts or abductions [40].
Pseudonymity: A pseudonym is an alternative name for a real identity used for authentication. A user can use his/her pseudonym without revealing the real identity to access services and resources. Although there are similarities between anonymity and pseudonymity, the latter provides accountability for the user. Accountability can be provided by associating the pseudonym with a reference, i.e., a pseudonym or an alias. The pseudonym of a malicious user can be linked with his/her real identity by the law enforcement authorities [3, 33]. The pseudonyms generated for a user are not linkable to obtain meaningful information [41].
Unlinkability: This feature means that the attacker cannot link the messages transmitted by the same driver together. As a result, the driver's actions are not traceable by a malicious user [18, 34, 36, 38]. In ETCS, the TSP or RSU should not be able to link the stored locations and times to the corresponding drivers; otherwise, drivers can be easily tracked.
Unobservability: If the messages broadcasted by a driver cannot be distinguished by others, particularly

the third parties, then the unobservability property is maintained during communication [42, 43]. As a result, the attacker should not be able to detect the legality of the communication [34].

Fig. 4 shows the protection measures, namely security and privacy properties, for ETCS.

Fig. 4. Protection measures for ETCS

### 3.2 Attacks on ETCS

In this subsection, we discuss various attacks which can be performed in ETCS. These attacks are grouped as follows: attacks by malicious drivers, attacks by malicious servers, and attacks by intermediate routers. Fig. 5 summarizes various types of attacks on ETCS.

Fig. 5. Types of attacks on ETCS

#### 3.2.1 Attacks by malicious drivers

Malicious drivers might use different methods to fool the ETC scheme to prevent billing. These methods are discussed as follows:

1) Collusion among dishonest drivers: Malicious drivers could submit incomplete or tampered toll transactions to get evidence proving that they have cheated. This evidence, then, will reveal the spot locations. Afterward, the malicious drivers can share this revealed information, i.e., spot locations to circumvent paying toll money [7].
2) Physical attacks: Malicious drivers can tamper with the OBU or transponder to avoid billing or to pay less. To do so, such drivers typically deactivate the OBU [4, 44]. The paper [4] mentions that a malicious driver can make a transponder generate incorrect tuples. These tuples will be used as the inputs for a function computing the total toll fee.
3) Message modi cation: A malicious driver might tamper with the messages sent and received in a protocol [21, 24].

   OBU with spoofed GPS data: A driver can spoof the GPS signal to simulate a cheaper route. To do so, such drivers might modify the record of transactions [4, 21].
   Invalid road prices: Drivers might assign an invalid fee to the roads on which they are moving [21].
   Reporting invalid total fee: Drivers might report an invalid total fee different from the nal valid fee calculated in the OBU [21].
   Changing the class of a vehicle: In transponder-based ETC, a driver whose vehicle's type falls into an expensive vehicle class, e.g., trucks, might maliciously use a transponder so that it belongs to a cheaper class such as taxis [24].

4) Double spending: A malicious driver might reuse a token two or more times when driving [8, 19].
5) Masquerade as another car: A malicious driver can eavesdrop on a message sent or received by a vehicle and then tries to pretend as that vehicle [4].

#### 3.2.2 Attacks by malicious servers

Malicious toll service providers or even third parties might perform the following attacks:

1) Tracking attack: In this attack, an adversary aims to reconstruct a driver's trajectories using tracking algorithms. A malicious TSP can use the collected information such as times, locations, total toll fee, and home addresses to track drivers, violating drivers' privacy in an ETC scheme [4]. Tracking can be done for various purposes. For example, a TSP wishes to know all the toll gantries a driver has passed through, or the TSP is interested in knowing the location sites (e.g., any workplace or supermarket) a driver has visited periodically [39]. In [45], a tracking algorithm is proposed based on the adversary's knowledge, including toll fees, total toll fees, the city's map, and other contextual information. The total fee is the summation of toll fees that a driver owes the TSP within a month. The algorithm's core idea is to solve the subset sum problem [46] in which

we nd the toll prices whose summation leads to a driver's total toll fee.

2) Identi cation attack: A malicious server might be interested in discovering a driver's identity corresponding to his/her trace in an ETC scheme. The server uses inference attacks to de-anonymize a speci c driver [39]. The inference attacks employ the linkability of users to sensitive locations such as their workplaces or homes.
3) Function modi cation: A malicious TSP could modify the result of a function, which it computes, to take advantage of drivers. For example, it may change the output of the pricing function to obtain nancial pro ts illegally. The work [4], for example, de nes some types of functions: the usage-base tolls function, which is used for the computation of tolling cost, and automated speeding tickets, which detects speed violations.
Note: this attack could fall into the category of "malicious drivers". If a driver's interaction is needed for the function computation, the driver impacts the function's output.

#### 3.2.3 Attacks by intermediate routers

The paper [4] explains that the malicious routers can create false packets, drop the packets and modify the packets sent and received between the car's transponder and the server. To prevent modi cation, drivers should encrypt data with the server's public key. To handle the dropped and forged packets, drivers should ensure that all their tuples (times and locations) exist in the downloaded tuples. If some tuples are dropped or forged, drivers can upload them to the server.

### 3.3 Methods of providing security and privacy

We discuss various methods used to provide security and privacy in ETCS. It should be noted that designers can harness various methods to design privacy-preserving ETCS. The methods are as follows.

Cryptographic primitive-based method: Designers use several cryptographic primitives to design such schemes. The commonly used methods include public key encryption, digital signatures, pseudo-random functions (PRF), non-interactive zero-knowledge (NIZK) proofs, and hash functions.
Secure multiparty computation-based method: Some privacy-preserving ETCS such as [4, 47] used this method. In this method, two or more parties jointly compute a function securely, and at the end of the protocol, no party learns more than its private input data and output [48]. This method itself might employ several cryptographic primitives.
Blockchain-based methods: Recently, several blockchain-based ETCS [49–52] and architectures [53–55] have been presented. Blockchain is a distributed decentralized ledger where data is recorded, and the data is always persistent [56, 57]. Blockchain has several fundamental properties, such as immutability: the data stored in blocks cannot be modi ed, integrity: changing a bit in a block is detectable, non-repudiation: it is provided by digital signatures, and transparency: since every recorded data stored in a block can be seen by all network nodes, and the stored data cannot be modi ed, this provides transparency.

### 3.4 Methods of formal security proof in ETCS

We de ne formal security de nitions employed by privacy-preserving ETCS. Both schemes "P4TC" [19] and "PrETP" [21] use a simulations-based security notion named "ideal-world/real-world paradigm" [58]. The ideal functionality $F$ is a trusted third party (TTP) that solves the problem in a perfectly secure and privacy-preserving manner. A protocol is as secure as the ideal functionality $F$ if no environment $Z$ can distinguish between two experiments, namely the real experiment and the ideal experiment. Note that the environment $Z$ is a probabilistic polynomial time (PPT) Turing machine. In the real experiment, the environment $Z$ communicates with the parties participating in the real protocol , and the experiment uses a real adversary $A$. In the ideal experiment, the parties send their input to the TTP $F$ and receive their output from $F$. In the ideal experiment, a simulator $S$ is employed in place of the real adversary $A$, and the simulator pretends to be the real adversary $A$ and simulates the network messages. Any attack on the real execution is also possible in the ideal one if no $Z$ can distinguish executions of the ideal and real experiment. In this case, we say that the protocol provides the same security level as the ideal functionality $F$. In terms of privacy, the parties just learn their output, which is sent to them by $F$. Hence, we can guarantee that no more information is revealed and thus, the achieved privacy level can be concluded from the ideal functionality's output.

Using the ProVerif tool is another approach for security proof used by the studies [25, 59]. This tool is for the automatic analysis of security protocols, which takes as input the protocol model. The model is obtained with the help of applied pi-calculus. The work [59] de nes location privacy for the VPriv scheme as follows. We denote the server's database $S$, including the tuples in the format $< tag; time; location >$. We de ne the set $S^0$, including the tuples $< location; time >$ that correspond to the tuple $< tag; time; location >$, where the item tag is removed. $C$ is an arbitrary vehicle. We consider the set $V$ denoting all information available to the server in VPriv. The information includes the data sent by $C$ to the server or any information computed or owned by the server during the calculation of $f$ (path of $C$), where $f$ computes the toll price corresponding to the path. The set $V^0$ represents all the information included in $S^0$, the output of $f$ (path of $C$), and other side channels in the raw database $S^0$. We say the calculation of $f$ preserves the $C$'s location privacy if what the server learns about $C$'s tuples is insigni cantly greater in $V$ than in $V^0$. Loosely speaking, from the server's view, the tags included in the tuples might just as well be random. Besides location privacy's de nition, the study [59] de nes privacy for list permutations and privacy for interactive zero-knowledge protocols using indistinguishability. Concerning the de nitions, they prepare a model upon which the ProVerif analyses VPriv.

The work [25] similar to [59] employs ProVerif to analyze the security. They de ne three security properties, namely correctness, accountability, and unlinkability. The rst property satis es that the server obtains the correct total toll fee and all users pay their toll fees. Accountability means that the scheme can detect the originator of malicious behavior. The last property guarantees that an adversary cannot link a user to its corresponding location records. After modeling the properties by the applied pi-calculus, they used ProVerif to analyze the protocol. Table 2 summarizes the methods applied by the ETCS to prove security and privacy formally.

The authors [60] analyze their scheme formally using a set of lemmas and one theorem. The theorem states that the ETC scheme meets the two design objectives de ned by the authors. Then, they use the lemmas to prove the theorem.

TABLE 2
Methods used for formal security proof in privacy-preserving ETCS.

| ETC scheme | Method for formal security proof |
|---|---|
| VPriv [4],[59] | ProVerif |
| PrETP [21] | Ideal-world/Real-world paradigm |
| [37], [25] | ProVerif |
| P4TC [19] | Ideal-world/Real-world paradigm |
| [60] | Lemmas and theorems |

## 4 Taxonomy of privacy-preserving ETCS

Over the past few years, several privacy-preserving ETC schemes have been proposed. In this section, we rst categorize these schemes under two technologies: GNSS and DSRC technology. The reason for such grouping is that the type of components and equipment used in these technologies are different (see 2.2). Different technologies inevitably lead to different privacy-preserving ETCS and accordingly cause different protection measurements to provide security and privacy. For example, based on the technology, there are differences in how the total fee is computed and in the type of information available to the TSP (see 2.2). Therefore, these differences justify our categorization into two groups. Then, we categorize each group into two groups: schemes supporting formal security proofs and schemes lacking formal security proofs. The reason for such grouping is that we are interested in determining the percentage of schemes supporting/not supporting formal proofs. This statistic can warn designers if there is a lack of formally proven ETCS, as they are more reliable to be deployed practically in real word scenarios. The taxonomy is shown in Fig. 6.

### 4.1 GNSS-based schemes

In this subsection, we discuss the schemes operating based on GNSS technology. We cluster the privacy-preserving GNSS-based schemes in two main groups: those supporting formal security and those lacking formal proofs. In the following, we explain the schemes supporting formal security proofs and then discuss those lacking formal proofs.

#### 4.1.1 Schemes supporting formal security proofs

Here, we elaborate on the schemes [4, 21, 25, 37, 59] which present formal proof. Almost all these studies consider various driver and server attacks (see 3.2). We should note that although the scheme [21] provides the formal proof, it does not consider the server attacks as opposed to the schemes [4, 25, 37, 59].

The authors in [4] presented VPriv, a system with two key components. The rst component aims to preserve the privacy of computing three different functions. These functions estimate the toll fee, speed, and delay with the help of secure multi-party computation (SMC). The second component is an enforcement method for the detection of malicious drivers. This method uses random check spots to prevent such drivers from physical attacks, such as turning off their OBUs. The threat model assumes that the server and drivers might misbehave as they have strong nancial motivation. VPriv includes three phases. In the registration phase, the client application, which is run by the driver, generates cryptographic commitments of the random tags (tags are random, so they cannot be linked with a car) and sends them to the server. Then the random tags will be bound to the driver's identity. In the driving phase, the car's transponder sends the tuples, i.e., random tag, location, and timestamp, to the server. In the last stage, reconciliation, the client computes the aforementioned functions at the end of the billing period. Then with the help of zero-knowledge proof, the client application proves to the server that the functions' output is correct. This phase is inef cient as the client downloads all the tuples from the server. For the implementation of these phases, various cryptographic tools are used: (1) homomorphic commitments (HC), (2) secure multiparty computation, (3) zero-knowledge proofs, and (4) a pseudo-random function. For verifying the total fee, the server uses homomorphic encryption over the encrypted data. Thus, the server only learns the total fee, not the private tuples. VPriv has several weaknesses, as mentioned in [21]. As drivers in VPriv have to send anonymous messages to the server, e.g., with the help of Tor [61], it imposes overhead on the system. Besides, although the server keeps anonymous tuples for each vehicle, the TSP can bene t from tracking algorithms such as [62–64] to obtain more information about the path that a vehicle has followed. Another weakness is that if the number of vehicles increases in the system, the computational and communicational complexity also increases. Finally, the authors analyzed their scheme's security against many attacks and demonstrated that it is resistant to malicious drivers and servers. Their analytical results show that their scheme can ef ciently run on stock hardware.

The authors in [59], introduced a framework for the formal analysis of privacy in ETCS and then applied it to the VPriv protocol [4]. They tried to create an abstract model of VPriv while keeping the features of the protocol. Then, the ProVerif tool analyzes the model with the assumption that attackers are honest-but-curious and merely follow the protocol speci cation. They demonstrated that VPriv preserves privacy properties in their abstract model.

The authors in [21] present PrETP, a privacy-preserving Electronic Toll pricing (ETP) system. This scheme uses a cryptographic construction, Optimistic Payment (OP), based on signature schemes and homomorphic commitments. The threat model in this work allows malicious users to manipulate the OBU and any of its interfaces. The system

Fig. 6. Taxonomy of privacy-preserving ETCS

model in which PrETP is de ned includes three entities: On-Board Unit, a Toll Service Provider (TSP), and a Toll Charger. The OBU locally computes the sub fees for the trajectories and then, at the end of the tolling period, adds up all the sub fees for calculating the total toll fee. This will preserve privacy as the OBU does not reveal any private data to TSP and TC. As opposed to VPriv, PrETP does not rely on anonymization techniques (i.e., Tor is not needed) since the drivers' private data are stored locally in the OBU. Afterward, the OBU proves to the TSP that it has performed valid computations. For protecting the OBU's data from malicious users, the data is encrypted inside the OBU with a method discussed in [65]. In contrast to VPriv, the computational complexity of the OBU is independent of the number of vehicles involved in the system, which is an advantage. Authors in [21] consider the driver's attacks, including drivers who inactive OBUs, drivers who cause OBUs to send false GPS location data, cause OBUs to use incorrect road prices, or cause OBUs to report total false fees. The TSP provides vehicles with OBUs. The TC imposes tolls for the roads and uses automatic license plate readers at random spot checks to detect malicious drivers. The authors in [21] mention several practical issues: although PrETP protects the drivers' privacy, the TSP has access to the users' identities and their home addresses. As the TSP accesses the total fee, decoding techniques [66] might be employed to obtain the possible sub fees from the total fee. The authors nally evaluated PrETP in terms of the OBU's and TSP's performance and demonstrated that PrETP can be run in an OBU in real time.

The paper [37] proposed an ETP system based on a group signature scheme (GSS). This scheme assures anonymity for the signers within a group. A message signed by a group member can be veri ed by the other member without revealing the signer's identity. The main aim of this study is to make a balance between the privacy of the users and the computational and communicational overhead. To do so, the users are divided into groups, and the corresponding toll fee is calculated in one round. This system has four phases: (1) based on a group division policy, a user will be assigned to a group, (2) the users anonymously transmit their collected locations along with the group name to a toll server. Besides, the hashes of the locations signed by the group signature scheme will be sent to the server, (3) the server sends the hashed locations and the associated toll fees, which are encrypted using a homomorphic cryptosystem, to the users. Then, the users add up their toll fees by multiplying them and sending the result to the server. The server nally decrypts the resulting ciphertext (4) in this phase, for the detection of a dishonest driver, the server sends the location signatures, the associated encrypted fees, and user payments to the authority. The presented protocol, however, has several challenges, e.g., nding a suitable group size that provides anonymity is dif cult. Additionally, although this scheme considers the attacks of a malicious server, it does not consider the drivers' attacks. Later, the authors in [25] veri ed the security and privacy of the presented system with the help of ProVerif.

#### 4.1.2 Schemes lacking formal security proofs

Here, we elaborate on the schemes [7, 12, 44, 47, 65, 67, 68] which lack the formal proofs; in fact, these schemes do not consider the driver and server attacks seriously, and each

scheme only focused on one or two types of attacks among all the driver and server attacks.

The work [65] provides a privacy-friendly architecture named “PriPAYD” to compute the premium for the pay-as-you-drive insurance systems. Although the work's application is for insurance companies, the proposed architecture idea can be applied to ETC applications. In both applications, drivers pay based on their road usage. The main part of the computation is carried out inside the OBU, and only the minimum information needed to bill users is sent to the insurance company. The data inside the OBU is encrypted to protect it from malicious users. Since no private data, including location data, is stored in the insurance company, the messages between the OBU and the insurance company do not need to be anonymous. The nal premium calculation is performed inside the OBU and will be encrypted by a public key encryption scheme (PKES) under the company's public key. Then it will be sent to the insurance company. Concerning this architecture, since the company does not check the correctness of the operations performed by the OBU, it jeopardizes its applicability to real-world scenarios [21]. The authors analyze the security of users and the company informally. The authors de ne three key security properties for the channel transferring the billing information: authenticity, con dentiality, and privacy. However, the presented architecture is not implemented in this work.

The authors in study [67] build the rst practical and functional road charging application which closely follows “PriPAYD” [65]. They show that their implementation is viable and the OBU's basic functionalities are possible by employing off-the-shelf hardware modules and free licensed software tools. Their implementation includes two steps. The rst step is to develop cryptographic modules, including authenticated encryption, public key encryption scheme, public key signature scheme, symmetric block cipher, pseudo-random number generator (PRNG), and hash function. The second step of the implementation deals with the normal mode of operation, including ve phases. (1) initialization: this phase initializes the OBU for the end user, e.g., storing parameters in the internal memory. (2) map-matching: this phase generates the mapped data in the form of strings, including time of the day, type of road (3) premium calculation: this function begins at the end of the user's journey. Each sub-fee of the journey is calculated based on the time of the day and the type of road. Then, all sub-fees are aggregated, resulting in the nal journey's premium. (4) GPS encryption: the full GPS data is rst encrypted by the authenticated encryption and then signed by the OBU using the RSA-PSS routine (5) send premium: This phase is performed at the end of the month when the vehicle needs to send the nal premium to the insurance company. Then, the authors evaluate the performance of the phases in terms of execution time. The results show that building a practical road charging system is feasible. However, the security of the scheme is not proved formally.

In the scheme [44], vehicles send the hash of their locations and the corresponding sub fees as commitments to a TSP. For con dentiality, these commitments will not reveal the drivers' road segments on which they have traveled. The presented scheme uses random spot checks to detect cheating drivers, providing auditing property. To do so, a very small percentage of the pre-images of the hash values, i.e., trajectories and fees, should be disclosed to the TSP. The spot checks in this scheme are applied to check the locations' correctness and the fee calculations [21]. This scheme discussed various methods for computing the total fee, one of which is homomorphic hashing. However, using this method, as the OBU can commit to a negative price, will let a malicious driver reduce the total fee, which is the drawback of this scheme [21]. More importantly, the authors did not mention to which attacks their model is resistant, and their work lacks formal proof and implementation.

In the paper [47], an ETC scheme named Milo, based on PrETP [21] is presented. The auditing protocol of Milo, as opposed to that of VPriv [4] and PrETP, does not disclose any information to the drivers even when drivers behave maliciously or collude with each other. The authors argue that the auditing component of both VPriv and PrETP reveals to the drivers the locations where they were observed. These locations are used for opening the requested cryptographic commitments, and the colluding drivers can share the location of the enforcement cameras. Hence, such drivers may refuse to pay for the camera-free locations. Milo utilizes an oblivious transfer (OT) protocol [69], which is based on blind identity-based encryption to hide the spot-checking locations from the drivers. In [47], the toll charger, i.e., the local government, is responsible for the spot checks compared to VPriv and PrETP in which the TSP performs the spot checks. This prevents the TSP from selling private information to gain pro t. However, Milo has not considered the physical attacks as compared to the papers [4, 21]. The papers [7, 19], also argue that Milo is not protected against mass-collusion of malicious drivers as when a dishonest driver is detected by the system, its associated spot check location is still revealed. Finally, the authors implemented Milo, but their work lacks formal proof.

The authors in [7], argue that even when the spot checks are kept secret, e.g., in Milo [47], collusion among dishonest users is still possible. The authors discuss that in mass surveillance, to prevent collusion, all transactions are required to be recorded, which contradicts privacy. The overall idea in this scheme is based on an authentication protocol, and it bene ts from a randomized OT, which is a cryptographic primitive. Using this protocol, it is possible to have mass surveillance without sacri cing the privacy of users. Only a fraction of the vehicles' data is collected, so this scheme has lower operating costs. This would discourage drivers from behaving maliciously. As opposed to other schemes [4, 21], this protocol does not rely on heavy computations such as zero-knowledge proof, and it is very ef cient. However, this scheme only discusses the collusion attack among all the drivers' attacks and does not consider the servers' attacks. This work also lacks formal proof and implementation.

The protocol presented in [68], uses the notion of cells, i.e., the road pricing area (i.e., a region, country) is divided into smaller segments called cells, each with its toll fee. The cells are used for the calculation of toll fees and the detection of fraud. When a driver enters a cell, she will be charged depending on the cell and possibly the time of day. The scheme uses a secure element (SE) that is tamper resistant

and embedded inside the car's OBU. As the SE is trusted, it adds up the toll fee of the cells a vehicle entered, stores the cumulative fee to its non-volatile memory, and nally sends the total fee to the TSP at the end of the billing period. By such a trusted device, this scheme does not require homomorphic encryption and proofs as opposed to [21]. In this scheme, a certain number of the cells are considered “check cells”. These cells are sent to the SE securely by the TSP and TC, which is a toll charger. The security of the proposed protocol is based on public key cryptography. The authors in this scheme consider the case in which some vehicles collude to avoid toll charges. However, this scheme only provides informal proof and does not consider server attacks.

The work [12] presents a secure and privacy-friendly scheme to address fraud detection in smart road pricing systems (SRP). Such schemes are the new generation of electronic road pricing systems and are relied on GNSS technology. SRP systems use satellites to bill drivers according to charging policy. The presented scheme employs vehicles' collaboration to detect a fraudulent driver aiming to evade tolling bills. For example, the scheme can detect a driver who disables his/her OBU. The scheme makes an overall comparison of the studies [4, 21, 32, 37, 47, 65] in terms of factors, including who collects location records, if spot check camera required. The proposed scheme works based on four components: bootstrapping, threshold-based control system, fraudulent evidence signature and veri cation, and tolling bill management. The scheme employs various cryptographic primitives to provide security and privacy for vehicles, namely digital signature, threshold cryptography (TCR), and elliptic curve (EC) cryptography. The work performs informal security analysis to ensure the scheme is resistant to impersonation and collusion attacks, besides to ensure the scheme provides privacy, accountability, con dentiality, and unforgeability. The authors performed simulations and demonstrated that their scheme outperforms the works [4, 21, 32, 37, 47, 65] in terms of storage and communication overhead.

The study [70] introduces “TollsOnly”, a fully homomorphic encryption (FHE) scheme. TollsOnly is a post-quantum privacy-preserving scheme that bene ts from blockchain so drivers can share their data with smart cities. Overall, the scheme includes three steps: (1) assess, (2) preserve, and (3) share. In the rst step, the authors de ne a model for risks to nd out the needed controls. In the second step, the scheme uses HE to encrypt toll data. In the last step, the scheme can share toll data if law enforcement requests it. To this end, the scheme locate the toll data in a blockchain to enable timed access to toll data. The authors build their model based on Gentry's fully homomorphic encryption [71]. They implemented their scheme using the Palisade framework, as it uses quantum-safe lattice operations, and showed their scheme can be applied in a real-world use case with speci c parameters. However, the scheme is not proved formally.

#### 4.1.3 Analysis of GNSS-based schemes

In Section 4.1, we discussed the GNSS-based privacy-preserving ETCS. We explained in detail the security and privacy properties these schemes provide and the security attacks to which these schemes are vulnerable. Table 3 summarizes various attributes of GNSS-based schemes. To visually demonstrate our categorization in the table, we make the column “Type of technology” bold, and the schemes supporting formal proof are shown in bolded “Yes”. In the following, the meaning of each attribute shown in Table 3 is explained:

ETC scheme: it denotes the scheme's reference and its name if it exists.
Year: it shows the year the paper is published.
Spot checks (cameras) are used: it means whether the misbehaving drivers are detected using spot checks.
Type of technology: it de nes the type of technology used in the ETC scheme: GNSS or DSRC.
Cryptographic method: it shows upon which cryptographic primitives an ETC scheme is built.
Supports blacklisting: it shows if the scheme considers blacklisting for malicious drivers.
Post-payments: it shows the type of toll payment which could be either post-payment or pre-paid.
Dynamic pricing: it shows if the calculation of the toll fee is dynamic or not
Formal proof: it means whether the discussed scheme or model is proved formally or not.
Implementation: it shows if the model is implemented.
Driver attacks: it shows if the reviewed paper fairly discusses the driver attacks, discussed in Subsection 3.2. If yes, the column is set to “Yes”, otherwise to “No”.
Server attacks: it shows if the server attacks (see Subsection 3.2) are discussed. If yes, the column is set to `Yes', otherwise to “No”.
Physical attacks: it shows if the scheme considers physical attacks. If yes, the column is set to `Yes', otherwise to “No”. Although this attack falls into drivers' attacks, we separate it as it is our focus.
Resistant to collusion attack: it shows if the scheme is resistant to collusion attack. If yes, the column is set to `Yes', otherwise to “No”. Like the physical attack, we consider it separately.

The analysis of the GNSS-based schemes is as follows:

Lack of formal security proof: Fig. 7 demonstrates the percentages of privacy-preserving GNSS-based ETCS supporting/lacking formal security proofs. It shows that only 27% of all the schemes provide formal security proofs, and the rest, i.e., 73%, do not. The percentages are based on the summarized information in Table 3.
Collusion attack: We can categorize these schemes into two groups: the schemes resistant to collusion attack and those not resistant to this attack. The schemes [7, 12, 25, 47, 68] are resistant to collusion attack, while the schemes [4, 21, 44, 65, 67] are vulnerable to this attack. The authors in [47] argue that the auditing component of [44], VPriv, and PrETP reveals to the drivers the locations where they were observed. These locations are used for opening the requested cryptographic commitments,

TABLE 3
Comparison of the GNSS-based privacy-preserving ETCS.

| ETC scheme | Year | Spot checks (cameras) are used | Type of technology | Cryptographic method | Supports Blacklisting | Post-payments | Dynamic pricing | Formal proof | Implementation | driver attacks | Server attacks | Physical attacks | Resistant to collusion attack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PriPAYD [65] | 2007 | No | GNSS | PK ES, DS, SE | No | Yes | Yes | No | No | Yes | Yes | Yes | No |
| [44] | 2008 | Yes | GNSS | Hash, HC | No | Yes | Yes | No | No | No | No | No | No |
| VPriv [4],[59] | 2009 | Yes | GNSS | SMC, ZKP, PRF, HC | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| [67] | 2010 | No | GNSS | PK ES, DS, SE, PRNG, Hash | No | Yes | Yes | No | Yes | Yes | Yes | Yes | No |
| PrETP [21] | 2010 | Yes | GNSS | RSA, ZKP | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Milo [47] | 2011 | Yes | GNSS | SMC, OT, RSA, ZKP | No | Yes | Yes | No | Yes | No[1] | No | No | Yes[2] |
| [68] | 2011 | Yes | GNSS | PK ES | No | Yes | No | No | No | No[3] | No | No | Yes |
| [37], [25] | 2012 | Yes[4] | GNSS | GSS, HS | No | Yes | Yes | Yes | No[5] | Yes | Yes | No | Yes |
| [7] | 2015 | Yes[6] | GNSS | OT, EC-ElGamal | No | Yes | Yes | No | No[7] | No[8] | No | No | Yes |
| [12] | 2018 | Yes | GNSS | DS, EC, TCR | No | No | Yes | No | Yes | Yes | No | Yes | Yes |
| TollsOnly [70] | 2021 | No | GNSS | FHE, BC | No | No | ND[9] | No | Yes | Yes | No | No | No |

[1] Only the Collusion attack is considered [2] Milo is not resistant to mass collusion of dishonest drivers [3] Only the Collusion attack is considered [4] Two solutions are considered: tamper-resistant devices and spot checks [5] Implementation is not considered, but the ef ciency is measured theoretically [6] Readers are used instead of cameras [7] Implementation is not considered, but the performance is assessed [8] Only the Collusion attack is considered [9] Not discussed.

and the colluding drivers can share the location of the enforcement cameras. Hence, such drivers may refuse to pay for the camera-free locations. It is worth mentioning that the papers [7, 19] argue that Milo is not protected against mass-collusion of malicious drivers as when a dishonest driver is detected by the system, its associated spot check location is still revealed.

Physical attack: Among all the GNSS-based schemes, only [4, 12, 21, 65, 67] take into account the physical attacks, and this type of attack is ignored by the other schemes.

Driver and server attack: As the table demonstrates, some papers do not consider the driver and server attacks. Only a few papers [4, 21, 25] formally proved the security and privacy and discussed the driver and server attacks explained in Section3.

Strong assumption: The security of the GNSS-based schemes [4, 21, 25, 37, 44, 47, 68] is based on a strong assumption, which is a key issue. The schemes assume that the locations of the spot checks (cameras) are random, and as soon as this assumption is valid, the cheating drivers can be detected and caught. Otherwise, the drivers can get rid of these spot checks and cheat.

Blacklisting: According to the table, none of the schemes support a blacklisting mechanism.

Implementation: Some of the schemes [7, 25, 37, 44, 65, 68] are not implemented, and this could cause concerns since such schemes might not be practical in terms of their performance and overhead.

Information leakage: The analysis of the privacy-preserving GNSS-based schemes shows that some information is inevitably revealed to the TSP. For example, the work [21] supporting formal security proof reveals the following information to the TSP: drivers' identities, home addresses, total toll fees, and all the commitments, which reveals the number of kilometers driven.

Gap of comprehensive privacy analysis: As Table 3 shows, the schemes [4, 21] formally prove the security and privacy of drivers. However, the authors in [21] argue that the TSP could learn more information than it is supposed to with the help of decoding techniques such as [66]. However, this study does not investigate the possibility of such decoding and its impact on drivers' privacy. Besides, the authors argue that the protocol VPrive [4] could be vulnerable to tracking algorithms such as [62–64]. However, the feasibility of the attack is not considered in [4].

### 4.2 DSRC-based schemes

This subsection elaborates on the privacy-preserving ETCS based on DSRC technology. Like the GNSS-based schemes, we group them into two categories: schemes supporting formal proofs and schemes lacking formal proofs.

#### 4.2.1 Schemes supporting formal security proofs

The framework P4TC [19] uses a payment system building block named BBA+ [72], which provides an unlinkable user wallet that is a core functionality. The authors in [19] improved BBA+ to deal with the real-world issues of an ETC use case. The authors elaborated on several security properties which a toll collection system typically provides, including double spending detection, unlinkability, and blacklisting. Then, with the help of these properties, an ideal functionality is de ned on which the formal security proof

of P4TC is based. P4TC is one of few studies that consider blacklisting to prevent fraud from illegal actions. The P4TC scheme includes several phases: wallet issuing, debt accumulation, and debt clearance. A driver first subscribes to a TSP and receives an ID. Then, in the wallet issuing phase, the driver sends its ID to the TSP and receives an anonymized wallet which will be stored in the OBU. In the debt accumulation phase, the driver sends an anonymized version of his/her wallet and receives a wallet with an updated balance amount. In the debt clearance step, at the end of the billing period, the driver sends his/her ID along with the claimed debt to the TSP, and then the TSP issues an invoice for the driver.

The study [60] presents a privacy-preserving ETC scheme where the toll fee is calculated by the entrance and exit points of each trip. Linkability among the trips made by a driver and between the entrance and exit transactions made for each trip is impossible. To this end, the scheme uses cryptographic primitives such as hash functions, RSA digital signature, and elliptic curve. The scheme uses a protocol named “priced oblivious transfer” (POT) [73], which is the scheme's core idea. In the protocol, a merchant offers different priced electronic items, among which a customer can buy an item after paying the amount. Using this protocol, the merchant neither learns the buyer's requested item nor the paid amount. Finally, the authors formally prove the scheme's security and privacy and evaluate its performance.

#### 4.2.2 Schemes lacking formal security proofs

The DSRC-based schemes which do not consider the formal proof are [8, 30–32, 49, 51, 52, 74–76] which are discussed below.

The SPEcTRe [8] is a suite of cryptographic primitives, including the RSA Full Domain Hash signature scheme, ecash, and a pairing to implement a blind signature (BS) scheme. SPEcTRe presented two schemes, namely the spot-record and no-record schemes. Both schemes depend on simple primitives rather than relatively computational intensive ones such as zero-knowledge proofs and secure multi-party computations, which are utilized in the previous works [4, 21, 47]. While the spot-record scheme provides the same level of privacy as prior schemes, it runs much faster. In this scheme, similar to [4, 21, 47], for the detection of cheating drivers, a small amount of information is recorded. The no-record scheme aims to detect dishonest drivers without collecting any information about honest drivers. However, these schemes have some shortcomings: in the spot-record scheme, tracking the users is possible using an exhaustive search on tokens [74], and also, both schemes have an important issue as they do not allow flexible prices [74]. Additionally, SPEcTRe does not consider the driver and server attacks; only the double spending attack is considered. This scheme also lacks formal proof of the model.

In [30–32], systems for low-emission zones are introduced, which depend on tamper-proof hardware. The main goal of the paper [30] is to protect the drivers' privacy and provide a mechanism for detecting fraud. In contrast to the studies [4, 21, 47], this scheme preserves the privacy of honest users, and only the fraudulent drivers are photographed by the checkpoints. Besides, the fraud detection in this scheme is not probabilistic as opposed to [4, 21, 47]. However, in this scheme, the pricing model is not dynamic. Later, the authors in [31] presented a similar system in which the toll fee is dynamically computed dependent on the traffic volume. In [32], the authors improved the system presented in [30], which supports more realistic scenarios. In the improved scheme, the LEZ is divided into different zones with different toll prices. However, these systems have shortcomings as they have not considered the driver and server attacks and lack formal proof and implementation.

In [74], an ETC scheme based on eCash is presented. The core of the system is built on a partially blind signature scheme. This scheme provides different presentations of the same signature so that the linkability of the signatures is impossible. In contrast to traditional eCash systems, in this system, each user holds just a single reusable token, and it can be reused a specified number of times in an unlinkable way, then the actual toll fee is computed at the exit RSU where the refund is received. With the help of the refund process, post-payments and dynamic pricing are possible in this scheme. Similar to [19], this scheme considers the blacklisting mechanism. Finally, they implemented their scheme, but it lacks formal proof as opposed to [19].

The work [75] presents a secure method to solve the consuming time in the e-payments systems such as SET and debit card models. Since vehicles have to complete their paying toll fee within a limited time in the communication range of toll stations, the scheme introduces a lightweight and security protocol to provide fast and secure payment. The protocol employs a blinded coin that includes the money designation, time stamp, and vehicle identity. The blinded digital coin ensures the preservation of users' privacy, authentication, and the payment's genuineness. The presented scheme consists of three phases: withdrawal, payment, and deposit. In the withdrawal phase, i.e., of line, the user buys coins from a bank. The bank signs the coin with a blind Schnorr signature to ensure the user's privacy. The ECC-based Schnorr signature by the user ensures the payment's Non-repudiation. In the payment phase, the user and the RSU are authenticated mutually, blinded coins are transferred to the RSU, and an invoice is issued to the user. In the deposit phase, the RSU transfers the coins to the bank, which checks the coins' and RSU's validity. The bank also checks if the coins are spent before to prevent double-spending. The authors perform simulations to evaluate the scheme's communication and computational delay performance. However, the proposed scheme does not consider the misbehaving users and does not analyze the users' security and privacy.

The work [52] design and implement a blockchain-based (Ethereum) scheme named “EdgeToll”, an open-source toll collection system. Using the method of payment channel, EdgeToll provides a quick, cost-efficient, and transparent solution to motivate edge service providers to participate in sharing their resources. Their scheme includes four main roles as follows. User: It uses the system to complement payments. Edge: It is an intermediate between a user and the cloud, which helps to facilitate computation. Proxy: It employs greedy algorithms to increase edge nodes' profit and decrease users' costs. The authors, finally, measure

transaction latency and gas fees in the Ethereum blockchain. The results show that the scheme reduces the gas fee cost and decreases the total time. However, the scheme is not proved formally.

The study [49] proposes two payment schemes based on blockchain, namely V-R transaction and V-Rs transaction. The authors present an electronic payment system model including two layers: the VANETs layer and the blockchain layer. In the rst layer, RSUs, vehicles, and the payment platform are involved in communications and transactions. In the latter layer, the entities within the blockchain (Ethereum) provide all transactions' security. All vehicles' and RSUs' accounts will be sent to the blockchain via the payment system. RSUs maintain all accounts stored in the blockchain with the help of a uni ed consensus mechanism. Vehicles have permission to obtain data in the blockchain through the RSU and to request a receipt from the RSU. The authors analyze the scheme's security informally and nally evaluate their scheme's performance.

The work [76] proposes a blockchain-based scheme for opportunistic autonomous vehicle platoon. The scheme's core idea is that several vehicles are put into a group or platoon with mutual trust, and then the platoon leader communicates with ETC as the representative. The vehicles following the platoon leader can pass through the ETC without further transaction with the ETC. By doing so, the ETC's operation time is exponentially reduced. To form a platoon, the authors employ the Ethereum blockchain in which the smart contract handles the creation of the platoon. The blockchain stores and veri es vehicles' driving history and credential information. To expedite the authentication process, an aggregate signature is employed. The authors evaluate their scheme's performance in terms of time consumption for DSRC, blockchain, and aggregate signature. Their results show that the scheme is ef cient and practical; however, they present no security proof.

The study [51] introduces a blockchain-based ECT scheme named “EdgeTC” which employs practical Byzantine fault tolerance (PBFT) to achieve faster performance. PBFT [77] is a consensus algorithm to reduce processing and bandwidth and to enhance network ef ciency and security. The scheme has four main critical steps as follows. Vehicle registration: every vehicle and toll gantry must get a key pair and a certi cate from the certi cate authority. Con rmation: the step ensures that a vehicle passes through a particular toll gantry. Transaction: after con rmation, the toll gantry sends the information to the PBFT blockchain. Validation: vehicles connect to the blockchain through RSUs and check the signature for validation. The fee calculation program is stored on the chain as a smart contract. This work, as opposed to [76], requires less computational power on the vehicle side, and as opposed to [49, 52], the work uses the Hyperledger Fabric platform to nish transactions faster. In the evaluation, the authors compare Ethereum-based and Hyperledger-based ETCS. The comparison shows that the latter scheme maintains stable performance if the chain grows. However, there is no formal security proof for the scheme.

#### 4.2.3 Analysis of DSRC-based schemes

In Section 4.2, we discussed the DSRC-based privacy-preserving ETCS. We explained in detail the security and privacy properties these schemes provide and the security attacks to which these schemes are vulnerable. Table 4 summarizes various aspects of DSRC-based schemes. To visually demonstrate our categorization in the table, we make the column “Type of technology” bold, and the schemes supporting formal proof are shown in bolded “Yes”.

The analysis of the DSRC-based schemes is as follows:

Lack of formal security proof: Fig. 7 shows the percentages of DSRC-based ETCS supporting/lacking formal security proof. It shows that a small percentage, i.e.,20% of all the schemes support formal security proof, and 80% do not consider it.
Collusion attack: Only the schemes [8, 19, 30–32, 60, 74] are resistant to collusion attacks.
Physical attack: All the DSRC-based schemes do not consider the physical attacks except [19].
Driver and server attack: Only the schemes [19, 60] considered the driver and server attacks, and the other DSRC-based schemes do not discuss such attacks. The scheme [8] only considered the double-spending attack, which falls into the drivers' attacks category.
Blacklisting: Only P4TC [19] and [74] schemes support blacklisting mechanism.
Implementation: All the DSRC-based ETCS are implemented except [30–32], and a prototype of the scheme [60] is developed in Java.
Information leakage: Analysis of the DSRC-based schemes demonstrates that various information is inevitably and inherently available to the service provider to charge drivers. The TSP must access drivers' identities as it should know with whom the total toll fee is associated. The TSP should know the total toll fee to bill drivers, and it needs the toll prices to compute the total toll fee. It should access drivers' home addresses to send their issued invoices. The TSP learns transactions (tuples of locations and times) from the RSU. Clearly, the TSP knows the city's map where toll stations are located. To summarize, the typical information unveiled to the TSP includes the total toll fee, transactions, driver's identities, toll prices, drivers' home addresses, and the city's map. The mentioned information impacts the privacy level of a driver in a privacy-preserving DSRC-based scheme.
Gap of comprehensive privacy analysis: The authors in [19] formally prove that their protocol “P4TC” provides security and privacy. It means the protocol does not leak more information than the protocol's leakage, including the total toll fee, driver's identities, and transactions. However, the privacy level of drivers should be considered along with other information, such as the city's map, toll prices, and home addresses. Apart from this, the concrete values of available information to the TSP in uence on drivers' privacy which is not investigated in [19].

TABLE 4
Comparison of the DSRC-based privacy-preserving ETCS.

| ETC scheme | Year | Spot checks (cameras) are used | Type of technology | Cryptographic method | Supports Blacklisting | Post-payments | Dynamic pricing | Formal proof | Implementation | driver attacks | Server attacks | Physical attacks | Resistant to collusion attack |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SPEcTRe [8] | 2011 | Yes | DSRC | RSA, BS | No | Yes | No | No | Yes | No[1] | No | No | Yes |
| [30],[31], [32][2] | 2014 | Yes | DSRC | PK ES, DS, Hash | No | No | Yes[3] | No | No | No | No | No | Yes |
| [75] | 2014 | No | DSRC | BS, EC, Hash | No | No | Yes | No | Yes | No | No | No | No |
| [74] | 2016 | No | DSRC | ZKP, BS | Yes | No | Yes | No | Yes | No | No | No | Yes |
| Edgetoll [52] | 2019 | No | DSRC | BC | No | ND[4] | ND | No | Yes | No | No | No | No |
| P4TC [19] | 2020 | Yes | DSRC | NIZK, PRF, DS, PK ES, HC | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| [49] | 2020 | No | DSRC | BC | No | ND | ND | No | Yes | No | No | No | No |
| BEHT [76] | 2020 | No | DSRC | EC DS, BC, AS | No | ND | ND | No | Yes | No | No | No | No |
| EdgeTC [51] | 2021 | No | DSRC | PBFT BC | No | ND | ND | No | Yes | No | No | No | No |
| [60] | 2022 | No | DSRC | Hash, RSA, BS, EC, POT | No | No | No | Yes | Yes[5] | Yes | Yes | No | Yes |

[1] Only a double spending attack is considered [2] The scheme [32] is published in 2016 [3] The scheme [30]is not dynamic [4] Not discussed [5] A prototype is developed in Java

Fig. 7. Percentages of ETCS supporting/lacking formal security proofs

## 5 Guidelines and Discussion

The survey findings have the potential to provide valuable insights into the development and design of secure and privacy-preserving ETCS. Additionally, guidelines can be proposed for the toll engineers to deploy ETC systems with appropriate security measures in place. To this end, the guidelines are presented in Section 5.1, while in Section 5.2, we discuss future works.

### 5.1 Guidelines

The overview of potential attacks and protection measures of privacy-preserving ETCS, such as confidentiality, integrity, and availability, guides researchers through designing ETC schemes ensuring privacy and security. Additionally, the overview provides a guideline for toll engineers deploying privacy-preserving ETC systems. This survey achieves this by introducing the security and privacy properties of such schemes and presenting types of attacks to which ETCS are vulnerable in Section 3. This survey provides designers of ETCS with a range of methods to provide security and privacy. These methods include cryptographic primitive-based, secure multiparty computation-based, and blockchain-based approaches. Moreover, this survey outlines different formal security proof methods that designers can use to validate the security and privacy of ETCS. Section 3 of this survey provides a detailed discussion of these methods.

Based on our analysis presented in Sections 4.1.3 and 4.2.3, we have found that researchers in designing ETCS have not widely considered the blacklisting mechanism. However, incorporating this mechanism could increase the practicality and feasibility of the schemes. By discouraging misbehaving drivers from committing illegal actions such as disabling the OBU or colluding with unauthorized parties, a blacklisting mechanism would contribute to the security and privacy of ETC systems.

Based on our analysis, we have found that certain ETCS, particularly the GNSS-based privacy-preserving ones, have not been implemented, and as a result, their performance is uncertain. This could potentially create practical issues in real-world scenarios. Cryptographic building blocks are integral components of these schemes and are typically computationally intensive, so they may cause delays. Such delays contradict the high speeds at which vehicles pass through toll gantries, where toll gantries must perform processing such as payments and other computations within a short period to bill drivers. Therefore, it is essential to implement

and validate the performance of privacy-preserving ETCS.

### 5.2 Discussion

The taxonomy of privacy-preserving ETCS reveals an important gap in such schemes: the lack of comprehensive privacy analysis. To the best of our knowledge, no studies investigate the impact of information available to the TSP on drivers' privacy. The studies [4, 21] argue that information stored in the TSP could potentially make an ETC scheme vulnerable to tracking attacks. Hence, given the information available to the TSP, the possibility of tracking attacks in privacy-preserving ETCS should be analyzed comprehensively. In addition, various factors would impact drivers' privacy, including the distribution of toll prices, the number of toll stations, and the distribution of total toll fees. Hence, a new line of research is required to investigate which parameters impact drivers' privacy and how the parameters' distribution affects privacy.

Until now, several studies present methods for types of attacks in VANET using machine learning (ML) [78–84] and deep learning (DL) algorithms [85, 86]. Our analysis in Sections 4.1.3 and 4.2.3 show that, to the best of our knowledge, no ETC schemes bene t from ML algorithms to detect security attacks. For example, given the information available to the TSP, one interesting question would be whether tracking drivers by pattern recognition using ML or DL methods is feasible. Hence, we recommend researchers investigate the possibility of applying such methods in ETCS to discover potential attacks.

Our analysis shows that the security of privacy-preserving schemes is based on a strong assumption, i.e., the positions of invisible spot checks should be at random locations within a billing period. This issue could be an open problem for researchers.

We discussed several blockchain-based ETCS in this survey. Blockchain enables transparency and trustworthiness of the toll records for heterogeneous ETC platforms. Blockchain helps such platforms interact with each other without any intermediate while providing transparency and trustworthiness. Blockchain is also used to record and verify every registered vehicle's driving history and credential information in ETC systems. However, the issues that blockchain-based ETC schemes face are as follows. Scalability is a research gap in these studies, which is essential for ETC systems as more and more vehicles join such systems. For example, the work [51] uses the PBFT algorithm to offer suitable performance; however, the algorithm is not proper for a large-scale network. Another issue is the lack of focus on the security analysis of such systems; the focus in these studies is much on the model and design of blockchain.

In future work, researchers can develop a framework for deploying privacy-preserving ETCS. This framework aims to balance two objectives: (1) ful lling a TSP's nancial and traf c policies and (2) protecting drivers' privacy. To maintain privacy, the system may suggest adjustments to the settings of an ETC system, such as setting toll prices within a certain range. The system will aim to balance these objectives against each other.

## 6 Conclusion

Privacy-preserving in ETCS, the focus of this research, is one of the major issues in such systems as drivers are concerned about their private data. This survey comprehensively reviews all privacy-preserving ETCS from various aspects, including protection measures for ETCS, attacks on ETC, and methods of formal security proofs in ETCS. Then, these schemes are categorized based on the technology they use and if they support formal security proof. Then, under each category, ETCS schemes are discussed, a comparison is made among the relevant ones, and the advantages and drawbacks of each scheme are discussed. This comparison reveals that a fairly large number of the schemes lack formal security proof and lack security analysis against potential attacks in ETCS. Additionally, implementation and, accordingly, performance are also ignored by some studies, which makes them impractical. Then, we give several research directions that help researchers design secure ETCS. This is achieved by discussing all relevant protection measures and all potential attacks in such systems.

## Acknowledgment

This was supported by the Faculty of Science, Technology, and Medicine (FSTM). This work was also supported by the 5G-INSIGHT bilateral project (ID: 14891397) / (ANR-20-CE25-0015-16), funded by the Luxembourg National Research Fund (FNR), and by the French National Research Agency (ANR).

## References

[1] M. N. Azadani and A. Boukerche, “Driving Behavior Analysis Guidelines for Intelligent Transportation Systems,” IEEE Transactions on Intelligent Transportation Systems, 2021.

[2] A. Sumalee and H. W. Ho, “Smarter and more connected: Future intelligent transportation system,” Iatss Research, vol. 42, no. 2, pp. 67–71, 2018.

[3] P. Asuquo, H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao, and Z. Sun, “Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4778–4802, 2018.

[4] R. A. Popa, H. Balakrishnan, and A. J. Blumberg, “VPriv: Protecting privacy in location-based vehicular services,” 2009.

[5] “Projections for the global electronic toll collection market size between 2019 and 2030,” https://www.statista.com/statistics/1254629/global-electronic-toll-collection-market-forecast/, accessed: 2021-12-20.

[6] K. Ogden, "Privacy issues in electronic toll collection," Transportation Research Part C: Emerging Technologies, vol. 9, no. 2, pp. 123–134, 2001.

[7] F. Kerschbaum and H. W. Lim, "Privacy-preserving observation in public spaces," in European Symposium on Research in Computer Security. Springer, 2015, pp. 81–100.

[8] J. Day, Y. Huang, E. Knapp, and I. Goldberg, "Spectre: spot-checked private ecash tolling at roadside," in Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, 2011, pp. 61–68.

[9] "Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York," https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass, accessed: 2021-12-20.

[10] F. Giannotti, M. Nanni, F. Pinelli, and D. Pedreschi, "Trajectory pattern mining," in Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, 2007, pp. 330–339.

[11] Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma, "Mining interesting locations and travel sequences from GPS trajectories," in Proceedings of the 18th international conference on World wide web, 2009, pp. 791–800.

[12] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1592–1603, 2018.

[13] S. Escher, M. Sontowski, K. Berling, S. Köpsell, and 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). IEEE, 2021, pp. 1–6.

[14] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in 2011 IEEE symposium on security and privacy. IEEE, 2011, pp. 247–262.

[15] C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for Vehicle-2-X communication," Computer Networks, vol. 55, no. 14, pp. 3199–3210, 2011.

[16] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in 2010 Seventh international conference on wireless on-demand network systems and services (WONS). IEEE, 2010, pp. 176–183.

[17] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in 2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM). IEEE, 2013, pp. 1–6.

[18] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770–790, 2017.

[19] V. Fetzer, M. Hoffmann, M. Nagel, A. Rupp, and R. Schwerdt, "P4TC—Provably-Secure yet Practical Privacy-Preserving Toll Collection," Proceedings on Privacy Enhancing Technologies, vol. 2020, no. 3, pp. 62–152, 2020.

[20] N. Ganeshkumar and S. Kumar, "Obu (on-board unit) wireless devices in vanet (s) for effective communication—A review," Computational Methods and Data Engineering, pp. 191–202, 2021.

[21] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "PrETP: Privacy-Preserving Electronic Toll Pricing." in USENIX Security Symposium, vol. 10, 2010, pp. 63–78.

[22] W.-H. Lee, S.-S. Tseng, and C.-H. Wang, "Design and implementation of electronic toll collection system based on vehicle positioning system techniques," Computer Communications, vol. 31, no. 12, pp. 2925–2933, 2008.

[23] A. de Palma and R. Lindsey, "Traffic congestion pricing methodologies and technologies," Transportation Research Part C: Emerging Technologies, vol. 19, no. 6, pp. 1377–1399, 2011.

[24] Z. J. Wong, V. T. Goh, T. T. V. Yap, and H. Ng, "Vehicle Classification using Convolutional Neural Network for Electronic Toll Collection," in Computational Science and Technology. Springer, 2020, pp. 169–177.

[25] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "Design and formal analysis of a group signature based electronic toll pricing system," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 4, no. 1, pp. 55–75, 2013.

[26] F. Baldimtsi, G. Hinterwalder, A. Rupp, A. Lysyanskaya, C. Paar, and W. P. Burleson, "Pay as you go," in Workshop on hot topics in privacy enhancing technologies, HotPETSs, vol. 2012. Citeseer, 2012.

[27] L. Yang, R. Saigal, and H. Zhou, "Distance-based dynamic pricing strategy for managed toll lanes," Transportation research record, vol. 2283, no. 1, pp. 90–99, 2012.

[28] Toll collect service on the road. [Online]. Available: https://www.toll-collect.de/en/toll_collect/bezahlen/maut_tarife/maut_tarife.html

[29] Z. Liu, S. Wang, B. Zhou, and Q. Cheng, "Robust optimization of distance-based tolls in a network considering stochastic day to day dynamics," Transportation Research Part C: Emerging Technologies, vol. 79, pp. 58–72, 2017.

[30] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras-Capellà, J. Castellà-Roca, and A. Viejo, "Electronic road pricing system for low emission zones to preserve driver privacy," in International Conference on Modeling Decisions for Artificial Intelligence. Springer, 2014, pp. 1–13.

[31] R. Jardí-Cedó, J. Castellà-Roca, and A. Viejo, "Privacy-preserving electronic toll system with dynamic pricing for low emission zones," in Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer, 2014, pp. 327–334.

[32] R. Jardí-Cedó, M. Mut-Puigserver, J. Castellà-Roca, M. Magdalena, and A. Viejo, "Privacy-preserving electronic road pricing system for multifare low emission zones," in Proceedings of the 9th International Conference on Security of Information and Networks, 2016, pp. 158–165.

[33] Z. Lu, G. Qu, and Z. Liu, "A survey on recent ad-

vances in vehicular network security, trust, and privacy," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760–776, 2018.
[34] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," IEEE Sensors Journal, vol. 21, no. 2, pp. 2422–2433, 2020.
[35] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Computer Communications, vol. 44, pp. 1–13, 2014.
[36] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19–30, 2017.
[37] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in 2012 Seventh International Conference on Availability, Reliability and Security. IEEE, 2012, pp. 85–93.
[38] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.
[39] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A unified framework for location privacy," Tech. Rep., 2010.
[40] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.
[41] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," Vehicular Communications, vol. 16, pp. 45–61, 2019.
[42] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "Vppcs: Vanet-based privacy-preserving communication scheme," IEEE Access, vol. 8, pp. 150 914–150 928, 2020.
[43] J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, and H. Treharne, "Privacy-enhanced capabilities for vanets using direct anonymous attestation," in 2017 IEEE Vehicular Networking Conference (VNC). IEEE, 2017, pp. 123–130.
[44] W. de Jonge and B. Jacobs, "Privacy-friendly electronic traffic pricing via commits," in International Workshop on Formal Aspects in Security and Trust. Springer, 2008, pp. 143–161.
[45] X. Chen, D. Fonkwe, and J. Pang, "Post-hoc analysis of user traceability in electronic toll collection systems," in Proc. 7th International Workshop on Data Privacy Management. Springer-Verlag, 2013, pp. 29–42.
[46] J. C. Lagarias and A. M. Odlyzko, "Solving low-density subset sum problems," Journal of the ACM (JACM), vol. 32, no. 1, pp. 229–246, 1985.
[47] S. Meiklejohn, K. Mowery, S. Checkoway, and H. Shacham, "The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion." in USENIX security symposium, vol. 201, no. 1, 2011.
[48] O. Goldreich, "Secure multi-party computation," Manuscript. Preliminary version, vol. 78, p. 110, 1998.
[49] X. Deng and T. Gao, "Electronic payment schemes based on blockchain in VANETs," IEEE Access, vol. 8, pp. 38 296–38 303, 2020.
[50] D. Das, S. Banerjee, P. Chatterjee, M. Biswas, U. Biswas, and W. Alnumay, "Design and development of an intelligent transportation management system using blockchain and smart contracts," Cluster Computing, vol. 25, no. 3, pp. 1899–1913, 2022.
[51] W.-Y. Chiu and W. Meng, "EdgeTC-a PBFT blockchain-based ETC scheme for smart cities," Peer-to-Peer Networking and Applications, vol. 14, no. 5, pp. 2874–2886, 2021.
[52] B. Xiao, X. Fan, S. Gao, and W. Cai, "EdgeToll: a blockchain-based toll collection system for public sharing of heterogeneous edges," in IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019, pp. 1–6.
[53] A. Didouh, A. B. Lopez, Y. El Hillali, A. Rivenq, and M. A. Al Faruque, "Eve, you shall not get access! A cyber-physical blockchain architecture for electronic toll collection security," in 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2020, pp. 1–7.
[54] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "Pay as you go: A generic crypto tolling architecture," IEEE Access, vol. 8, pp. 196 212–196 222, 2020.
[55] S. Huang, L. Yang, X. Yang, X. Li, and F. Gao, "A Decentralized ETC Architecture Based on Blockchain Technology," Journal of Advanced Transportation, vol. 2021, 2021.
[56] R. Jabbar, E. Dhib, A. ben Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review," IEEE Access, 2022.
[57] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1–34, 2019.
[58] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in Proceedings 42nd IEEE Symposium on Foundations of Computer Science. IEEE, 2001, pp. 136–145.
[59] M. Dahl, S. Delaune, and G. Steel, "Formal analysis of privacy for anonymous location based services," in Joint Workshop on Theory of Security and Applications. Springer, 2011, pp. 98–112.
[60] R. Borges, F. Sebé, and M. Valls, "An anonymous and unlinkable electronic toll collection system," International Journal of Information Security, vol. 21, no. 5, pp. 1151–1162, 2022.
[61] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.
[62] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in International Conference on Security in Pervasive Computing. Springer, 2005, pp. 179–192.
[63] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," IEEE Pervasive Computing, vol. 5, no. 4, pp. 38–46, 2006.
[64] J. Krumm, "Inference attacks on location tracks," in International Conference on Pervasive Computing.

Springer, 2007, pp. 127–143.
[65] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, "Pripayd: privacy friendly pay-as-you-drive insurance," in Proceedings of the 2007 ACM workshop on Privacy in electronic society, 2007, pp. 99–107.
[66] G. Danezis and C. Diaz, "Space-efficient private search with applications to rateless codes," in International Conference on Financial Cryptography and Data Security. Springer, 2007, pp. 148–162.
[67] J. Balasch, I. Verbauwhede, and B. Preneel, "An embedded platform for privacy-friendly road charging applications," in 2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010). IEEE, 2010, pp. 867–872.
[68] F. D. Garcia, E. R. Verheul, and B. Jacobs, "Cell-based roadpricing," in European Public Key Infrastructure Workshop. Springer, 2011, pp. 106–122.
[69] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2007, pp. 265–282.
[70] H. Karim and D. B. Rawat, "TollsOnly Please—Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2627–2636, 2021.
[71] C. Gentry, A fully homomorphic encryption scheme. Stanford university, 2009.
[72] G. Hartung, M. Hoffmann, M. Nagel, and A. Rupp, "BBA+ Improving the Security and Applicability of Privacy-Preserving Point Collection," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1925–1942.
[73] B. Aiello, Y. Ishai, and O. Reingold, "Priced oblivious transfer: How to sell digital goods," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2001, pp. 119–135.
[74] A. Barki, S. Brunet, N. Desmoulins, S. Gambs, S. Gharout, and J. Traoré, "Private eCash in practice (short paper)," in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 99–109.
[75] B. K. Chaurasia and S. Verma, "Secure pay while on move toll collection using VANET," computer Standards & interfaces, vol. 36, no. 2, pp. 403–411, 2014.
[76] Z. Ying, L. Yi, and M. Ma, "BEHT: blockchain-based efficient highway toll paradigm for opportunistic autonomous vehicle platoon," Wireless Communications and Mobile Computing, vol. 2020, 2020.
[77] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE, 2017, pp. 253–255.
[78] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," Computing, vol. 104, no. 3, pp. 503–531, 2022.
[79] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect DDoS attacks on VANET system: a survey," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). IEEE, 2019, pp. 1–6.
[80] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2018, pp. 564–571.
[81] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," in International conference on advances in computing and communications. Springer, 2011, pp. 644–653.
[82] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi, and S. Nandi, "Machine learning based approach to detect position falsification attack in VANETs," in International Conference on Security & Privacy. Springer, 2019, pp. 166–178.
[83] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," IEEE Access, vol. 10, pp. 1893–1904, 2021.
[84] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks," IEEE Communications Surveys & Tutorials, 2023.
[85] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "Deepvcm: a deep learning based intrusion detection method in vanet," in 2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing,(HPSC) and IEEE intl conference on intelligent data and security (IDS). IEEE, 2019, pp. 288–293.
[86] S. A. Almalki and F. T. Sheldon, "Deep Learning to Improve False Data Injection Attack Detection in Cooperative Intelligent Transportation Systems," in 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2021, pp. 1016–1021.

**Amirhossein Adavoudi Jolfaei** is currently doing his Ph.D. at the Department of Computer Science, University of Luxembourg. He received his M.S. degree at the University of Isfahan in 2017. His main research interests include lightweight security protocols, privacy-preserving in vehicular sensor networks, secure computation, and WSNs security.

**Abdelwahab Boualouache** is a research associate at the Faculty of Science, Technology and Medicine (FSTM), University of Luxembourg. He received a Ph.D. degree in computer science from USTHB University, Algiers, Algeria in 2016. His current research interests include security and privacy in connected vehicles and privacy-preserving collaborative learning solutions for 5G and Blockchain-based solutions for decentralized systems