Journal of Network and Computer Applications 212 (2023) 103569

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A transparent distributed ledger-based certificate revocation scheme for VANETs☆

Andrea Tesei [a,b,*], Domenico Lattuca [a,b], Marco Luise [a], Paolo Pagano [b], Joaquim Ferreira [c], Paulo C. Bartolomeu [c]

[a] Department of Information Engineering, University of Pisa, Via G. Caruso 16, Pisa, 56122, Italy
[b] National Inter-university Consortium for Telecommunication (CNIT), Via Moruzzi 1, Pisa, 56122, Italy
[c] Instituto de Telecomunicações, Universidade de Aveiro, Campus Universitário de Santiago, Aveiro, 3810-193, Portugal

ARTICLE INFO

Keywords:
Certificate revocation scheme
Transparency
Privacy
Vehicular Public Key Infrastructure
Distributed Ledger Technology
Intelligent Transportation Systems
Vehicular *Ad-hoc* Networks

ABSTRACT

The widespread adoption of Cooperative, Connected, and Automated Mobility (CCAM) applications requires the implementation of stringent security mechanisms to minimize the surface of cyber attacks. Authentication is an effective process for validating user identity in vehicular networks. However, authentication alone is not enough to prevent dangerous attack situations. Existing security mechanisms are not able to promptly revoke the credentials of misbehaving vehicles, thus tolerate malicious actors to remain trusted in the system for a long time. The resulting vulnerability window allows the implementation of complex attacks, thus posing a substantial impairment to the security of the vehicular ecosystem. In this paper we propose a Distributed Ledger-based Vehicular Revocation Scheme that improves the state of the art by providing a *vulnerability window* lower than 1 s, reducing well-behaved vehicles exposure to sophisticated and potentially dangerous attacks. The proposed scheme harnesses the advantages of the underlying Distributed Ledger Technology (DLT) to implement a privacy-aware revocation process while being fully transparent to all participating entities. Furthermore, it meets the critical message processing times defined by EU and US standards, thus closing a critical gap in the current international standards. Theoretical analysis and experimental validation demonstrate the effectiveness and efficiency of the proposed scheme, where DLT streamlines the revocation operation overhead and delivers an economically viable yet scalable solution against cyber attacks on vehicular systems.

1. Introduction

In recent years, the symbiosis of Transportation Industry and Information and Communication Technology (ICT) has become real and created a new generation of vehicles with strong communication capabilities, intending to give people a better and safer driving experience. Besides the industrial growth of these technologies, Vehicular *Ad-hoc* Networks (VANETs) and, more broadly, Cooperative Intelligent Transportation System (C-ITS) have attracted much attention in academia also, where research and standardization efforts are focused on creating secure frameworks that enable a set of applications in the domain of road safety, traffic efficiency and driver assistance (Tesei et al., 2018).

There are two well-established types of communication in C-ITS, namely Vehicular-to-Infrastructure (V2I) communication and Vehicle-to-Vehicle (V2V) communication. Communication devices installed in vehicles are called On-Board Units (OBU), and the ones installed in road infrastructures are named Road-Side Unit (RSU). Using these standardized communication protocols, vehicles can exchange safety messages with each other and communicate directly with RSUs (Lu et al., 2019a).

The open and vulnerable nature of the C-ITS communication infrastructure requires sophisticated security mechanisms to ensure a safe, real-life deployment. Consequently, C-ITS industrial standards define stringent security requirements, considering all the technical, societal, legal, and economical concerns (e.g., privacy, unlinkability, anonymity, etc.) Tesei et al. (2018).

Authentication is essential to the security of C-ITS communications. Harmonization efforts from different stakeholders have reached

☆ This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957216, also referred as iNGENIOUS (Next-GENeration IoT sOlutions for the Universal Supply chain).

* Corresponding author at: Department of Information Engineering, University of Pisa, Via G. Caruso 16, Pisa, 56122, Italy.
E-mail addresses: andrea.tesei@phd.unipi.it, andrea.tesei@cnit.it (A. Tesei), domenico.lattuca@phd.unipi.it, domenico.lattuca@cnit.it (D. Lattuca), marco.luise@unipi.it (M. Luise), paolo.pagano@cnit.it (P. Pagano), jjcf@ua.pt (J. Ferreira), bartolomeu@ua.pt (P.C. Bartolomeu).

https://doi.org/10.1016/j.jnca.2022.103569
Received 27 June 2022; Received in revised form 29 November 2022; Accepted 24 December 2022
Available online 5 January 2023

a consensus on the use of Vehicular Public Key Infrastructure (VPKI) to manage credentials of vehicles. Among those stakeholders, it is worth mentioning the Car2Car Communication Consortium (C2C-CC), the Institute of Electrical and Electronics Engineers (IEEE) 1609.2 Work Group (WG) (IEEE, 2019a) and the European Telecommunication Standards Institute (ETSI) Technical Committee (TC) ITS WG 5 with TS 102 940 (ETSI, 2021a). With a number of Trusted Authorities (TAs), VPKI systems issue different certificates to vehicles: the Enrollment Credentials (ECs) are the long-term certificates used to enroll vehicles in the system; the Authorization Tickets (ATs) entitle the vehicle to access C-ITS specific applications and guarantee driver anonymity in the system.

However, to ensure the correct recognition of misbehaving and malicious drivers, the privacy of the driver is said to be *conditional*: the union of these two types of certificates (i.e., an EC and one or more ATs) can reveal the driver's identity. Indeed, the TAs are authorized to start the vehicle identity resolution process only if it is liable for any violation (Khodaei et al., 2018). In fact, in the recent years several researchers have demonstrated that Connected and Autonomous Vehicles (CAVs) are vulnerable to cyberattacks in real world (Parkinson et al., 2017; Xu and Guo, 2022). As discussed in Hasrouny et al. (2017), the attackers can be classified as *insider* when they are authenticated and authorized users, while they are defined as *outsider* representing all the malicious actors that do not own valid credentials. Leveraging the VPKI security architectures described above can potentially mitigate the risk of outsider attacks, but there can still be disruptive and dangerous insider attacks, as demonstrated by Amoozadeh et al. in Amoozadeh et al. (2015). In their work, the authors simulated an attack directed to a stream of cooperative driving CAVs assuming that the malicious actor is a compromised and trusted vehicle with a valid certificate. The attack consists of sending falsified messages containing wrong neighboring vehicles' positions and speed: this falsified information causes the gap between vehicles to dangerously change, increasing the risk of collision. Similar attack scenarios are reported in Sun et al. (2022), Chim et al. (2009), Rawat et al. (2012).

In these situation, *misbehavior detection* capabilities are mandatory to recognize these attacks, either based on the analysis of attacker behavior or on message data (Wang et al., 2020a). Finally, once a misbehavior is detected, a method is needed to promptly revoke valid certificates to the compromised vehicle, as well as a mechanism to disseminate revocation information securely.

Unfortunately, *misbehavior detection* and *revocation mechanisms* are not well covered by the latest US and EU industrial standard (IEEE, 2016, 2017, 2019b; ETSI, 2021a, 2020). Indeed, the current standards exploit the *revocation by expiry* method that exposes harmless vehicles to prolonged vulnerability windows in case of an attack (i.e., the exposure can last up to 3 months in the worst case with certificate preloading European Commission, 2018). This standard gap is limiting the deployment of Cooperative Intelligent Transportation Systems (C-ITS). In turn, research works related to vehicular revocation mechanisms lack a comprehensive method that matches the complex VANETs' requirements. Indeed, research endeavors aiming to evolve the current C-ITS security state of the art should be fully compatible with the existing standards and requirements to have a concrete chance to be effectively adopted in the real world.

In this paper, we present a novel transparent certificate revocation mechanism that encompasses the immutable archive of revocation information using Distributed Ledger Technology (DLT). The proposed DLT-backed Certificate Revocation List (CRL) can be exploited by vehicles to retrieve revocation information on the fly, directly accessing the distributed ledger every time a new secured message is received. This method eliminates the need to distribute CRL's content, lowering the *vulnerability window* period to underneath 1 s. The results obtained show a substantial improvement with respect to the vehicular security state of the art. Furthermore, this paper contributes to close a gap in current US and EU C-ITS standards, which do not provide any effective revocation mechanism for vehicles. To this end, we designed the proposed revocation scheme to be fully compatible with the current vehicular standards. This standard-focused research methodology assures that the proposed scheme can be accepted in the industry, thus enabling a wider base of adoption. Furthermore, this approach increases the possibility to apply research results in real-world use cases.

The capabilities of the revocation scheme are demonstrated in laboratory experiments, thanks to the integration with our Blockchain-based VPKI, named IOTA-VPKI, previously presented in Tesei et al. (2018) and Tesei et al. (2021a). To this end, we generalize the IOTA-VPKI customization for the logistics use case presented in Tesei et al. (2021a) to support the general C-ITS environment. Furthermore, in this paper we introduce a detailed theoretical analysis of the IOTA-VPKI security scheme proposed in Tesei et al. (2018) complemented with the new revocation scheme described herein. In addition, we present an extensive security analysis based on the security objectives presented in Section 4.2, particularly important to discuss the effectiveness of the IOTA-VPKI vehicular security scheme.

Experimental results show that the delay of revocation information distribution and the revocation checking time matches the requirements stated in the standards. Finally, we show that the delay of the revocation checking procedure is independent of the status of the certificate (i.e., valid or revoked), as well as of the number of revoked certificates, both critical requirements for a real usage of the proposed revocation scheme. We perform the validation in a pseudo-real environment composed of an OBU, a RSU, and an instance of the generalized IOTA-VPKI version equipped with our new revocation method.

To summarize, the key contributions of this article are the following:

- A novel DLT-based revocation scheme to transparently revoke misbehaving vehicles, fully compatible with current EU and US vehicular standards, thus closing a gap in the current industrial standards.
- A new generalized version of our previous work IOTA-VPKI (Tesei et al., 2021a), supporting the general vehicular environment.
- A detailed theoretical analysis of the generalized version of the IOTA-VPKI security scheme, including the details of the security objectives considered, allowing the reader to understand the whole picture of our research path.
- A complete security analysis of the proposed revocation scheme based on a detailed threat model that considers different threats for each security objective.
- Experimental results that demonstrate that the delay in checking the revocation status of the certificate, introduced by the proposed scheme, is independent of the status of the certificate and of the number of revoked vehicles.
- Experimental results demonstrating that the proposed scheme has a *vulnerability window* lower than 1 s, thus improving the prior art, and providing a security scheme fully compatible with the timeliness requirements of safety-related vehicular applications.

The rest of the paper is organized as follows: in Section 2 we introduce preliminary concepts to let the reader understand the problem addressed in this paper; in Section 3 we discuss relevant related works about vehicular security schemes and certificate revocation mechanisms; Section 4 presents the system overview, detailing the security objectives and threat model, whereas Section 5 provides a detailed description of the proposed revocation scheme with extended theoretical analysis; in Section 6 we discuss the security analysis of the IOTA-VPKI credential management system; in Section 7 the experimental setup and hypotheses are presented together with the discussion of the obtained results and the comparisons with other reference implementations; finally in Section 8 we further discuss our findings and conclude the paper with future works. All the acronyms used in the text are reported in Table 1.

Table 1
List of acronyms.

V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicular-to-Everything
ITS	Intelligent Transportation System
ITS-S	ITS Station
OBU	On-Board Unit
RSU	Road-Side Unit
VPKI	Vehicular Public Key Infrastructure
TA	Trusted Authority
AA	Authorization Authority
EA	Enrollment Authority
H-AA	Authorization Authority in *Home Domain*
H-EA	Enrollment Authority in *Home Domain*
F-AA	Authorization Authority in *Foreign Domain*
F-EA	Enrollment Authority in *Foreign Domain*
RA	Revocation Authority
MA	Misbehavior Authority
EC	Enrollment Credential
AT	Authorization Ticket
F-TKT	Ticket to move from *Home* to *Foreign* domain
DLT	Distributed Ledger Technology
CRL	Certificate Revocation List

2. Preliminaries

2.1. Proactive & reactive security

Considering the vulnerable communications and untrusted networks typical of VANETs, a privacy-preserving authentication scheme is required to protect vehicles from potential attacks. On the one hand, authentication prevents a malicious user from impersonating an authorized vehicle and broadcasting forged messages. On the other hand, the privacy-preserving characteristic of such an authentication scheme guarantees that the vehicles are protected against tracing.

Methods to protect vehicular systems can be broadly categorized as **proactive** or **reactive** (van der Heijden et al., 2019). Proactive security consists of the prevention of potential attackers from accessing the system (i.e., every mechanism that enforces a security policy, for example, a VPKI), while reactive security consists in the *detection* and the *reaction* steps that aim to identify and correct malicious activities within the system (i.e., misbehavior detection and revocation mechanisms). However, only the fusion of these two types of protection can ensure the high level of security required in C-ITS applications.

For example, considering the proactive security method provided by a VPKI, having valid credentials is not enough to ensure that each actor of the system behaves as stated in the standards and protocols. There are many cases in which an issued certificate should no longer be valid. For example, related cryptographic material could become compromised, or changing specific fields within the issued certificate is necessary for administrative reasons. Or even worse, when a vehicle becomes compromised and starts violating registration terms or obligations. Under these conditions, a reactive security mechanism is needed to identify misbehaving vehicles. Moreover, a method to revoke the certificates issued to the compromised vehicle must be enforced (that is, a vehicular revocation scheme). If a reactive security method such as the one described is missing, false and malicious messages can be potentially trusted by other vehicles, leading to serious accidents (Wang et al., 2020a). To avoid this situation, the security measures must consider a mix of proactive and reactive methods.

2.2. Standard vehicular revocation schemes: an overview

Revocation schemes mainly depend on the underlying authentication available in the vehicular security architecture. As described by Wang et al. in Wang et al. (2020a), a revocation mechanism is usually divided into three stages: *revocation information resolution*, *revocation information distribution*, and *revocation information usage*.

To succeed in permanently revoking a compromised vehicle, it is necessary to resolve its real identity. This is the *revocation information resolution* stage and it can be done by analyzing the malicious messages sent by the compromised vehicles and their corresponding anonymous certificates. Once the real identity of the compromised vehicle has been resolved, updated information on revoked certificates should be distributed to vehicles in the network as soon as possible, so that the vulnerability window can be minimized. This second stage is the *revocation information distribution* one. Finally, the revocation information is used by vehicles to determine whether a received message should be trusted. This final stage is the *revocation information usage* and it consists of the revocation check process performed every time a new secured message is received.

The sum of the duration of the first two steps described above, plus the *misbehavior detection time* corresponds to the *vulnerability window*, that is, the period in which a recognized misbehaving vehicle remains trusted by non-compromised vehicles. Furthermore, considering the delay-sensitive vehicular scenario, the *revocation information usage* should be as efficient as possible to minimize the impact on the processing latency of vehicular messages.

Generally speaking, each vehicular revocation mechanism should take into consideration the following requirements:

- The distribution of revocation information to non-revoked vehicles should be as fast as possible to minimize the vulnerability window (Rigazzi et al., 2017);
- The revocation process should be transparent, i.e., each entity should be able to check and track the whole revocation process for a specific certificate;
- The revocation check process should be as efficient as possible so that the message processing latency constraints can be matched (at most 25 ms, i.e., $\frac{1}{4}$ of the critical V2X messages latency time requirement defined by ETSI in ETSI (2019a) and ETSI (2019b) for the different basic set of vehicular applications).

As stated in Section 1, standardization bodies have reached a consensus on the use of a VPKI-based scheme to authenticate and authorize vehicles. However, an active revocation method is still missing for vehicles that meet the requirements described above. From the US standards point of view, IEEE 1609.0 (IEEE, 2019a) and IEEE 1609.2 (IEEE, 2016, 2017, 2019b) explicitly state that a method to distribute revocation information is still an open point that needs to be addressed. From the European perspective, neither ETSI standards (ETSI, 2021a,b, 2020), nor the European Commission (EC) certificate policy (European Commission, 2018, 2016; European Parliament, 2019) for C-ITS consider a revocation method for vehicle certificates (i.e., ATs, and ECs). They explicitly state that no revocation method is available for authorization tickets and enrollment credentials (ETSI, 2021b). Existing standards adopt a passive *revocation by expiry* mechanism to exclude malicious vehicles from the C-ITS system. With this passive revocation mechanism, when a vehicle is recognized to be misbehaving, the VPKI stops to issue new certificates to that vehicle. Once the issued certificates expire, the system definitely revokes the malicious actor. This method results in typically long vulnerability windows. Indeed, considering the current standards, the vulnerability window can reach 3 months in the worst case (i.e., in the case of certificate pre-loading European Commission, 2018). This severely limits the deployment of C-ITS applications in real-life scenarios. The evolution of security mechanisms (e.g., revocation checking) towards minimizing the communication overhead can be instrumental in scenarios that encompass emerging C-ITS technologies facing stringent timeliness requirements (e.g., EDGE computing) (Tesei et al., 2021b).

2.3. CRL-based revocation schemes limitations

The current standards define only a revocation method suitable for Trusted Authority (TA) revocation (i.e. the VPKI's certification authorities). This revocation mechanism is based on a Certificate Revocation

List (CRL), which is a blacklist containing the certificates that have been revoked by Trusted Authorities (TA).

In addition to the wider adoption of CRL-based revocation, this approach comes with several issues. First, as discussed earlier, vehicular networks are delay-sensitive. Hence, revocation information should be delivered to vehicles as quickly as possible to minimize the *vulnerability window*. To match these requirements, CRLs should be distributed frequently causing high bandwidth consumption. This problem can be alleviated by using compression techniques (e.g., Bloom Filter, Δ-CRL), or by doing selective broadcasting based on geographic regions. For example, in Khodaei and Papadimitratos (2020), Khodaei and Papadimitratos proposed a vehicle-centric efficient CRL distribution protocol. The proposed approach fuses the concept of Δ-CRL (i.e., partial and non-complete CRL updates) and Bloom Filter techniques, so that the vehicles receive only region and time-relevant revocation information.

The proposed distribution technique is very efficient with respect to the prior art in terms of the CRL size and vulnerability window (15 s to distribute CRL; up to 60 s to collect all the Δ-CRL). However, the size of the CRL is still dependent on the number of vehicles revoked as reported by the results, which affects the scalability of the solution. Furthermore, vehicle-centric approaches increase the complexity of the RSU/OBU side. In fact, considering the RSU case, a geographic-aware lookup on the CRL needs to be executed to broadcast the revocation list that applies to the covered region. This issue can be alleviated if the Trusted Authorities (TAs) directly publish the different Δ-CRL components with geographic information. As for the OBU, it needs to implement a Bloom Filter algorithm to retrieve the revocation information and use it once a new secured message is received.

Another issue of CRL-based revocation is related to the absence of transparency of TAs in the revocation process. It is well known that TAs are necessary for VANETs because they are responsible for vehicle registration, network maintenance, and dispute arbitration (Lu et al., 2019b). However, their operations should be transparent to all entities participating in the network. CRLs are published by the TA without any mechanism useful to check the whole certificate revocation process. If a TA becomes compromised, nobody can assure the correctness of the CRLs' content.

Finally, as the CRLs start growing with a large number of revoked certificates, the revocation checking delay will increase accordingly, and this may imperil the safety latency constraints defined in the standards.

2.4. The IOTA Distributed Ledger Technology

The IOTA Distributed Ledger Technology (DLT) (IOTA, 2022b) is a promising implementation of a Transaction-based Direct Acyclic Graph (TDAG) ledger. Unlike standard blockchain technologies (e.g., Bitcoin) characterized by a ledger structure made up of chain of blocks each of them containing a batch of valid transactions, in the DAG-based DLTs the blocks have been replaced directly by the transactions, which are linked with each other to create a DAG of transactions. This new ledger shape enables unprecedented scalability level, overcoming several standard blockchain's limitations (Kannengießer et al., 2020).

The IOTA ledger is a public and feeless DLT designed to support secure, transparent, and unmodifiable data flows for Internet-of-Things (IoT). The IOTA DLT is based on a special TDAG ledger structure, the *Tangle*, that was first presented in Popov (2018). In the Tangle every user is free to issue new transactions and attach them on the public TDAG, as long as they follow the basic rules of the protocol. Consequently, the Tangle is composed of a network of parallel processed transactions, the so-called Tips, which acts as multiple attach points for new transactions (Anon, 2022b).

The absence of a central entity that decides when and if the ledger can be updated, makes it possible for each user to create new transactions autonomously without paying fees. In this sense, IOTA is said to be a *leaderless* consensus mechanism. On the contrary, in nearly all blockchain-based DLT, a limited group of authorities (i.e., the miners) can decide which new transactions will be included in the next block based on the fee that the users are willing to pay: this will create a kind of oligarchy of miners which favors who pays higher fees and creates an unfair behavior of the ledger. Moreover, since only one miner will succeed in attaching a new block to the blockchain, only that single authority will earn the reward, while the others have wasted computational power and electricity that may have been used for other activities.

Considering the energy cost per transaction, the benchmark results reported in Anon (2022c,a) demonstrated that the IOTA network is designed to be lightweight and energy-efficient. Hence, the IOTA network is suitable to be used also by devices with limited computational resources, as the ones adopted in IoT and Cooperative, Connected, and Automated Mobility (CCAM) environments.

Finally, it is worth mentioning that the IOTA supports also no-value transactions containing pure data (i.e., the *zero-value* transactions), that is stored with immutable, unforgeable, and secure properties in the Tangle. This feature can be exploited in several use cases where IOTA DLT can be an enabler to unlock unprecedented functionalities in different environments (e.g., CCAM, IoT, etc.). We will discuss in details the *zero-value* transactions and other functionalities of the IOTA DLT in the subsequent Section 4.

3. Related work

The most widely used certificate revocation schemes in vehicular networks are based on Certificate Revocation Lists (CRL) and have been proposed in many previous contributions. Wang et al. (2020a) presents a systematic review on the available revocation methods, focused on CRL-based approaches. Different approaches are classified according to the location where the revocation information is placed. They considered revocation mechanisms implemented at the RSU side and the vehicle side, explaining the issues and limitations of different approaches. As previously discussed in Section 2, CRL-based revocation schemes have several drawbacks that affect the requirements of vehicular networks.

We report in this section several research works which aim to exploit Distributed Ledger Technology (DLT) and *Merkle Hash Trees* (MHTs) as an enabler to mitigate the aforementioned limitations. We focus our discussion on the way these technologies are employed, without exploring the details of the specific Blockchain technology used in each work. For further details about this topic, the interested reader can refer to the original works.

In Ali et al. (2019) Ali et al. designed an efficient Certificateless Public Key Signature (CL-PKS) scheme using bilinear pairing to provide conditional privacy-preserving authentication. In their proposed scheme, there are two Merkle Tree-based blockchains to which the different entities are connected: the *Blockchain for Pseudo-Identities*, which provides *Proof of Presence* of the pseudo-identity issued to the vehicles, and the *Blockchain for Revoked Pseudo-Identities*, which works as the *Proof of Absence* public database for all those pseudo-identities that have been revoked by the TA. Even if the proposed scheme is cryptographically cost-effective and eliminates the need to distribute revocation information, the numerical results showed that the communication delay grows with the number of vehicles, and thus the scheme does not apply to large-scale deployments.

The *Merkle Hash Tree* (MHT) is a fundamental component of blockchain and Distributed Ledger Technologies. For this reason, this data structure technology have attracted much attention to overcome the limitations of existing vehicular security mechanisms. In Lu et al. (2019b) Li et al. proposed a particular implementation of MHT data structure named the Merkle Patricia Tree (MPT). The authors proposed an authentication scheme that uses the MPT in conjunction with a Chronological Merkle Tree (CMT) to extend the conventional blockchain structure and provide a distributed authentication scheme

Table 2
Comparisons of revocation schemes available in research.

Scheme	Authentication method	Revocation method	Main limitations
Ali et al. (2019)	Blockchain-based Certificateless	*Active revocation*	High computation delay which grows with the number of signature/verification operations to be done in a single sign/verify batch (i.e., more than 100 ms for few messages)
Lu et al. (2019b)	Blockchain-based	*Active revocation*	Authentication delay grows with the number of vehicles (i.e., only feasible in less populated environments)
Ma et al. (2020)	Blockchain-based with smart contacts	*Active revocation*	Non-negligible smart contract fees (i.e., more than 40.000 USD per year for 1000 registered vehicles)
Yang et al. (2021)	Blockchain-based	*CRL-based active revocation*	CRL distribution algorithm not covered by the proposed scheme
Mendiboure et al. (2020)	Blockchain-based	*Active revocation*	Non-negligible vulnerability window in the case of cross-domain revocation (i.e., the vehicle to be revoked is registered to multiple domains)
Chulerttiyawong and Jamalipour (2021)	Blockchain-based with CRL	*passive revocation*	High revocation checking delay which grows with the size of the CRL
Noor et al. (2020)	Blockchain and notary system based	*Active revocation*	High vulnerability window depending on the validity of the notarized public-keys
Zhang et al. (2020)	Blockchain-based	*Active revocation*	Non-negligible transaction fees
Qi and Gao (2020)	CRL-based with Bloom Filter	*CRL-based active revocation*	Revocation checking delay dependent on the Bloom Filter algorithm efficiency
Wang et al. (2020b)	Trusted Party secret generation	*Secret-based active revocation*	Delay grows with the number of vehicles (i.e., only feasible in less populated environments)
Yang et al. (2020)	EDGE-based	*Active revocation*	Huge delay incompatible with VANETs (i.e., more than 600 ms authentication delay per vehicle in presence of only 10 entities)
Kumar et al. (2017)	Pre-issued Certificate	*Active revocation*	High vulnerability window and huge delay of certificate activation key distribution which grows with the number of revoked vehicles (i.e., more than 1 min for 1000 revoked certificates)
Verheul et al. (2019)	Pre-issued Certificate	*Active revocation*	High vulnerability window (i.e., 90 days)

without the need for a revocation list. The certificate revocation is obtained by broadcasting a revocation transaction containing the revoked certificate entity. The experimental results showed that the distributed authentication process is very fast, but the measurements are susceptible to the number of vehicles. Also, it is not clear if the scheme applies to blockchain implementations other than Hyperledger Fabric.

A promising approach to overcome the current vehicular security limitations consists in deploying multiple TAs that are entitled to authenticate and authorize a small subset of vehicles. In Yang et al. (2021) Yang et al. proposed a multi-domain vehicular authentication architecture that exploits blockchain technology to store and share cross-domain information among multiple administrative domains. In the proposed scheme, a dedicated pseudonym service stores certificates issued by TAs to vehicles on the blockchain. In turn, the pseudonym distribution is delegated to the RSU. However, the revocation mechanism is still based on CRL without enough details on the way this list is distributed to vehicles. Furthermore, there is no performance analysis about CRL distribution time, revocation checking delay, and other measurements needed to assess the vulnerability window of the proposed scheme.

A blockchain-based security scheme specifically designed for Software Defined Vehicular Networks (SDVN) is proposed in Mendiboure et al. (2020). In this paper the authors proposed a scalable architecture based on a set of interconnected Blockchain sub-networks to implement an efficient authentication and authorization scheme for all SDVN devices (vehicles, roadside equipment, SDN controllers). The proposed scheme exploits multiple blockchain technologies to distribute the vehicles' security management: each blockchain subnetwork is responsible of a specific geographical area and it manages authentication/authorization/revocation of a limited number of devices. However, the revocation checking delay is not reported in the performance analysis, thus it is very difficult to accurately estimate the vulnerability window of the proposed scheme.

Another interesting approach is presented by Zhang et al. in Zhang et al. (2020). The authors proposed a privacy-preserving authentication scheme for VANETs based on consortium blockchain. Instead of relying on standard certificate, the paper describes a novel data structure based on the unspent transaction output (UTXO) to let the authenticity of a vehicle or a road-side unit be represented by its transaction capability on blockchain. Consequently, authentication between two entities is accomplished by on-chain verification and corresponding communications. However, the proposed scheme has several limitations: on the one hand, it is based on the Bitcoin blockchain and thus subject to transaction price fluctuation; on the other hand, the reported evaluation is not mature enough to demonstrate its real and large-scale deployment feasibility.

Alternative blockchain-based schemes use smart contract techniques to implement certificate management. In Ma et al. (2020) Ma et al. proposed a decentralized key management mechanism (DB-KMM) that implements automatic registration, update, and revocation of user's public keys based on the smart contract technique. Performance measurements showed quite good computational overhead in terms of authentication and key management, but with non-negligible fees connected to smart contract functions. Another smart contract based approach was proposed in Chulerttiyawong and Jamalipour (2021). The authors exploited a permissioned consortium blockchain system to facilitate secure and conditional privacy-preserving vehicular pseudonym issuance and management in a multi-jurisdictional road network. The proposed scheme takes advantages of the wide availability of Roadside Units (RSU) that act as an interface between the blockchain network, trusted authorities' certificate services, and vehicles. However, the revocation scheme does not support any active revocation checking performed by vehicles upon new received messages. This is mitigated by issuing short-lived certificates, but still the vehicles are exposed to a non-negligible vulnerability window. Furthermore, the revocation mechanism is still based on CRL, and thus the revocation checking delay is dependent on the size of the CRL.

Other interesting approaches base the authentication and revocation schemes on third-party Trusted Authority (TA) clearance to authorize vehicles in the system. Wang et al. (2020b) proposed a tamper-proof device (TPD) based and privacy-preserving authentication scheme that

uses an RSU to generate up-to-date secrets needed by the vehicle to generate private signing keys. Whenever a vehicle is recognized to be misbehaving, the RSU stops generating secrets for that vehicle. However, the numerical results presented showed that the proposed scheme delay increases with the number of vehicles. Another interesting approach was proposed by Verheul et al. (2019), named *Issue First Activate Later* (IFAL). This scheme can pre-issue a set of pseudonym certificates, which are valid only in a configurable time epoch and are only usable upon receiving small activation codes by TAs. In this way, the need for a Certificate Revocation List (CRL) is eliminated, but a misbehaving vehicle remains trusted in the system for the entire epoch duration time (i.e., 90 days according to experimental results). Kumar et al. proposed a similar approach in Kumar et al. (2017), where vehicles are provisioned at the start of their lifetime with all the certificates they will need in encrypted format: vehicles can decrypt a certificate only after a trusted authority delivers the corresponding decryption key. The revocation, in turn, happens by avoiding the misbehaving vehicle from receiving the decryption keys. However, the experimental results reported high delays in distributing the decryption keys (up to 1 h) that are not compatible with delay sensitive VANETs applications.

Another activation-based security scheme was proposed by Noor et al. in Noor et al. (2020). The authors presented a Secure and Transparent Public Key Management System (ST-PKMS) based on blockchain and a notary system specifically designed for Vehicular Social Networks (VSNs). In ST-PKMS, each vehicle has multiple short-lived anonymous public keys, which are recorded on a blockchain platform. Those public keys are activated only when a notary system notarizes them. Other vehicles accept only notarized public keys during mutual authentication. Compromised vehicles can be effectively removed from the VSN by blocking the notarization of their public key. Even if the proposed scheme eliminates the need of CRL, thus decreasing dramatically the vulnerability window, the revocation mechanism is still based on a blacklist of misbehaving and compromised vehicles that can affect the scalability of the system. Furthermore, the performance evaluation showed that the communication overhead increases with the number of V2X communication handshakes, thus showing that the proposed scheme is not applicable in the presence of large numbers of vehicles.

Conversely, the certificate management is delegated to the EDGE in the authentication scheme presented in Yang et al. (2020). Unfortunately, the performance evaluation reported high delays, which do not match VANETs time requirements, especially in hazardous situations (i.e., more than 600 ms authentication delay per vehicle in presence of only 10 entities).

The Bloom Filter (BF) compression technique is a promising approach to limit the CRL size and mitigate the limitations of related revocation methods. An example of this technique is proposed by Qi and Gao in Qi and Gao (2020). The authors improved the existing Vehicular Public Key Infrastructure (VPKI) introducing BF to compress the CRL and support the batch revocation of pseudonyms, while keeping them unlinkable. Even if the proposed scheme can effectively reduce the CRL size, it is well known that BF is vulnerable to false positives: this exposes the system to the situation where revoked vehicles are considered trusted (and vice versa). This possibility is not well covered by the authors; thus, there are not enough elements to evaluate the vulnerability window of the proposed scheme. Furthermore, in addition to the CRL size reduction enabled by BF, the proposed scheme is still dependent on the size of the revocation list, reporting high certificate status checking in particular cases.

The aforementioned related works proposed several methods to manage authentication and revocation in vehicular networks, reporting performance results that put into question their suitability for specific dangerous and hazardous situations that may arise in vehicular environments. Even if some existing work already takes advantage of distributed ledger technology (DLT), the delay introduced by the proposed methods is mainly dependent of the number of vehicles, therefore only feasible in less populated environments. Considering the fundamental role of the security mechanism in the deployment of vehicular technologies, a comprehensive certificate management scheme that proposes an efficient revocation scheme must be studied and developed to increase vehicle safety. The considered research works and their limitations are summarized in Table 2.

The performance evaluation reported in this paper demonstrates that the proposed revocation scheme outperforms other related works with an unprecedented vulnerability window lower than 1 s, and a very fast and scalable revocation checking delay close to 10 ms, independent of the number of the message frequency, certificate status, and registered vehicles. Furthermore, the proposed scheme is fully compatible with US and EU standards, assuring a wide base of adoption in the real world. Moreover, the exploitation of IOTA Distributed Ledger Technology (DLT) assures feeless transactions and enables full transparency in the issuance and revocation process, as described in the Security Analysis reported in the next Section 6.

4. System overview

As introduced in Section 2, the current EU and US vehicular standards lack of an active revocation method for vehicles. This standard gap actually exposes well behaved vehicles to dangerous situations, thus impeding a real-life and large-scale deployment of ITS technologies. To close this gap, an evolution of the existing security infrastructure is needed to support vehicle misbehavior detection and to exclude malicious vehicles from the system. However, the compliance with international standards should be the starting point of each research work that aims to have broader adoption in the real world and that effectively envisages the state of the art evolution of ITS technologies.

For this reason, we have started our research work generalizing the previous IOTA-VPKI work (Tesei et al., 2021a) to support generic Intelligent Transportation System (ITS) environments. The resulting architecture encompasses two new authorities to meet ITS security requirements: the first named *Misbehavior Authority* (MA), which implements every method that can recognize misbehaving vehicles and mark them as malicious; the second named *Revocation Authority*, which actually implements the novel vehicle certificate revocation mechanism proposed in this article, thus being able to exclude malicious vehicles from the system. For the sake of self containment, in the following subsections we describe all the Trusted Authorities (TAs) that compose the new version of the IOTA-VPKI architecture. Furthermore, we provide a detailed discussion of the design concepts, threat model, and security objectives, which are the cornerstone of the new IOTA-VPKI architecture equipped with the proposed active certificate revocation scheme.

4.1. Blockchain-based vehicular PKI: IOTA-VPKI

We introduce IOTA-VPKI in Tesei et al. (2018) as an adaptation of the SECMACE credential management system (Khodaei et al., 2018). SECMACE was proposed by *Khodaei et al.* and it is fully compliant with the current US and EU standards described and analyzed in Section 2. We use the SECMACE reference architecture as our starting point, and we extend it with the introduction of IOTA DLT implementation as the transparent storage backend of each certificate issued to vehicles. As extensively described in Tesei et al. (2018), IOTA is a DAG-based DLT implementation well suited for the IoT domain. Devices with small resource capacity can issue a transaction by communicating with the nearest neighbor IOTA Reference Implementation node (IRI).

Our VPKI architecture is depicted in Fig. 1 and it is composed of the following entities with distinct roles:

- *Root Certification Authority (RootCA)*: is the highest-level authority and represents the trust anchor of the whole system;
- *Enrollment Authority (EA)*: is responsible for vehicle enrollment in the system and Enrollment Credential (EC) issuance;

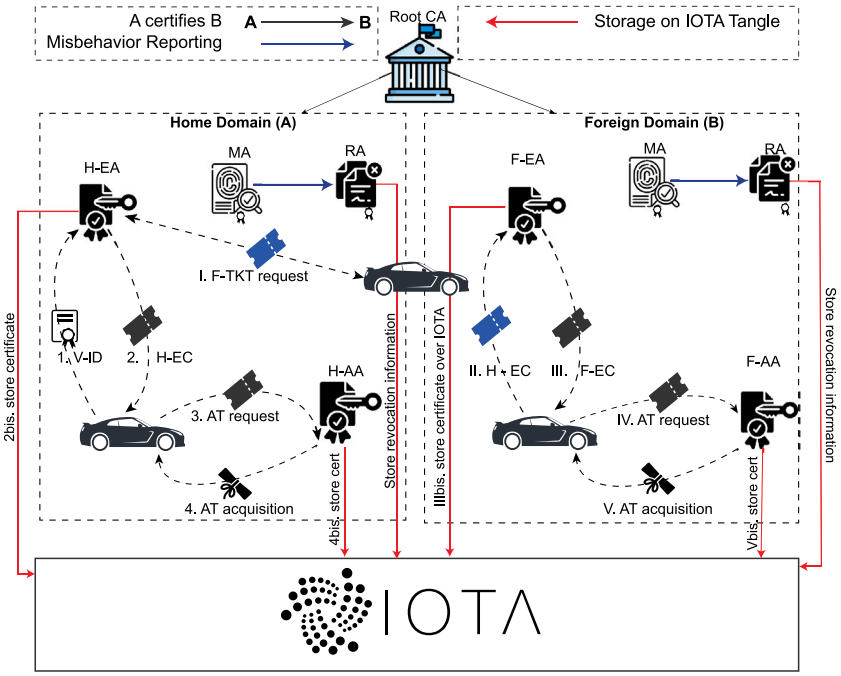

Fig. 1. IOTA-VPKI architecture: new version.

- *Authorization Authority (AA)*: is responsible for vehicle access authorization to system applications and facilities by issuing an Authorization Ticket (AT);
- *Misbehavior Authority (MA)*: is responsible for vehicle action and message checking to recognize eventually misbehaving entities to be excluded from the system;
- *Revocation Authority (RA)*: can revoke a misbehaving, malfunctioning or outdated vehicle resolving also its identity, thus avoiding it to obtain valid credentials anymore;
- *IOTA DLT*: is an instance of the IOTA Tangle which can be either the publicly available ledger or a private Tangle managed by the VPKI Manager.

Apart from the Root CA which is managed offline by the VPKI manager (e.g., the national authority), each of these entities are connected to the Internet and equipped with an IRI Node to have direct access to the IOTA DLT to read and write certificates, as well as to let the revocation information be available to vehicles.

We borrow also from SECMACE the concept of *home* and *foreign domains*: a *Home domain* is the one where the vehicle is registered from the beginning; while a *Foreign domain* is the one which a vehicle can reach after leaving its *Home domain*. Namely, a *domain* is defined as a set of vehicles, registered with their *Home*-EA (H-EA), subject to the same administrative regulations and policies (e.g. a country).

When an ITS station (i.e., a vehicle) δ wants to send a message, it must first acquire the rights to access C-ITS communications from the H-EA by sending its own pre-registration receipt (steps 1 and 2 in Fig. 1). Once issued, the H-EA immutably stores the certificate over IOTA Tangle (step 2bis). Then, it negotiates the rights to access the C-ITS services from H-AA (steps 3 and 4 in Fig. 1). Even in this case, the H-AA is responsible to immutably store the pseudonym certificate over the IOTA Tangle (step 4bis). Subsequently, it digitally signs V2X messages with its private signing key K_s^{δ} (corresponding to the currently valid AT_{δ}), and, finally, sends the message if and only if all the previous steps are successfully completed. Similarly, when the vehicle δ drives in a *Foreign* domain (e.g., after crossing the frontier of the home domain), it receives a Foreign EC from the F-EA after sending its own H-EC (Step I, II, and III in Fig. 1). Then, it can use the obtained F-EC to negotiate the rights to access the C-ITS services in the Foreign domain (Steps IV and V in Fig. 1). The same storage operations over IOTA Tangle apply in the *Foreign* domain (steps IIIbis, Vbis). When a misbehavior action is recognized by the MA (blue arrows in Fig. 1), the RA is notified to start vehicle certificate revocation process. Even in this case, the RA is responsible to store revocation information over the IOTA Tangle: in this way when a vehicle δ receives a digitally signed V2X message from another entity γ it can verify the validity of the sender's certificate directly accessing the IOTA Tangle without interacting with the authorities.

In particular, in our first IOTA-VPKI version (Tesei et al., 2018) we used the IOTA feature named *Masked Authenticated Message* (MAM) channels to implement the data flow between TAs and vehicles. MAM channels are always managed by a *channel owner* that publishes new data on such channels. In turn, devices can subscribe to the channel with read-only permissions and get the available data (IOTA, 2022c). There are three modes for MAM channels:

- *Public*: everyone can view the data;
- *Private*: only the owner can view the data;
- *Restricted*: the data are protected by a *sideKey*, and the owner gives this key only to authorized viewers.

In the first IOTA-VPKI architecture version, the TAs created a *restricted* MAM channel to establish a certificate data flow and spread the *sideKey* with pre-registered vehicles to allow them to decrypt the content of the messages (i.e., security management messages) that the TAs publish on the channel. The use of MAM restricted channels acts as a Group Signature (GS) based approach (Boneh and Shacham, 2004; Boneh et al., 2004), in which revocation can be obtained by changing *sideKey* whenever a new vehicle is revoked.

However, when we started implementing the customization of IOTA-VPKI for the logistics use case (Tesei et al., 2021a), we realized that MAMs have many limitations. Firstly of all, using the GS approach with a *restricted* MAM channel is not a scalable solution because the *sideKey* needs a distribution algorithm that extends the attack surface of the whole system (e.g., Man-in-the-middle attacks during the key distribution phase). Secondly, the only way to perform the revocation of a vehicle consists of changing *sideKey*. This creates a potentially unbounded vulnerability window that depends on the execution time

of the key distribution algorithm. Lastly, using a core feature of a specific DLT implementation would lock our architecture to this specific technology, becoming dependent on its future evolution.

For these reasons, in Tesei et al. (2021a) we abandoned the MAM-based approach and leveraged the concept of zero value IOTA transactions (IOTA, 2021c) as a means of immutably storing the revocation status of the seaport logistic vehicles and the position of the goods in the underlying DLT. Furthermore, we introduced for the first time a new authority named *Misbehavior Authority* (MA) responsible for the misbehavior detection process of malicious logistic vehicles.

The promising results obtained in the limited logistic scenario and reported in Tesei et al. (2021a) motivated us to evaluate whether the IOTA-VPKI logistics customization was eligible to be generalized to support generic vehicular environments. Indeed, the general vehicular scenario is more complex with respect to a "controlled" seaport environment. The vehicles need to be authenticated, authorized, and eventually revoked in a multi-domain scenario (i.e., home and foreign) without impairing the security level and performances of the vehicular system. This article addresses the new version of the IOTA-VPKI architecture that supports the general vehicular scenario. As shown in Fig. 1, we have replaced the MAM messages related to VPKI operations with general storage in IOTA Tangle that exploits zero-value transactions. In this way, we were able to overcome the scalability limitations of the MAM-based approach, and establish the transparent and immutable data flow between the Trusted Authorities (TAs) and the authorized vehicles. Furthermore, for the sake of completeness, we have also generalized the scope of misbehavior detection of the MA to recognize malicious actions in a vehicular environment, broader than the limited seaport area. However, the presence of this TA is only to let the reader understand where the revocation process actually starts: the way that the MA performs the detection of misbehaving vehicles is out of the scope of the present paper and is currently under investigation.

As previously discussed in Tesei et al. (2021a), the known limitation of zero-value transactions is related to the IOTA Snapshot process: when this process takes place, all zero-value transactions are reset. Hence, the stored information gets lost. To overcome this issue, an IOTA *permanent* node is required to store the IOTA-VPKI zero-value transactions and let them remain available even after a Snapshot process. This kind of permanent node is called *Chronicle*, which is a *permanode* solution that takes transactions from a node and stores them in a distributed database that is secure and scales well (IOTA, 2022a).

The new generalized IOTA-VPKI version was designed in such a way that it can be extended to support different available DLT technologies, thus avoiding the technology lock-in problem previously described. In fact, it exploits the basic transactions of the IOTA DLT implementation, i.e. *zero-value* transactions (IOTA, 2021c), which enable data storage over the IOTA Tangle. As a result, the proposed solution can be implemented using any DLT implementation that supports data storage over the distributed ledger. The IOTA-VPKI stores and distributes revocation information through DLT in a very short time, also supporting the inter-domain certificate revocation status checking (i.e., *home* and *foreign* domains).

4.2. Security objectives

The final goal of Vehicular Ad-hoc Networks (VANETs) and Intelligent Transportation Systems (ITS) technologies is to provide comfort and safety to drivers and passengers. To this end, an effective and comprehensive security mechanism should be designed to ensure the appropriate implementation of VANET services and operations. This means that the correct security objectives must be taken into account when evaluating a vehicular security scheme.

The VANET security and privacy requirements are well defined in industrial standards and discussed in the research literature. As Lu et al. presented in Lu et al. (2019a), every VANETs' security scheme must exhibit specific key security properties, which are confidentiality, data integrity, availability, non-repudiation & accountability, and authenticity. These requirements are the baseline to be covered by every security mechanism that aims to make the V2X communication channels secure, the core security problem of VANETs (Lu et al., 2019a).

From the industrial standards point of view, the ETSI Threat, Vulnerability and Risk Analysis (TVRA) report (ETSI, 2017) confirmed the security requirements discussed above. Furthermore, this report uses the TVRA method to identify VANETs and ITS-specific risks by isolating the vulnerabilities of the system. The report assesses the likelihood of malicious attacks on the recognized vulnerabilities, also determining the impact that such an attack will have on the whole system.

We briefly describe below the security objectives that we considered in our proposed security scheme:

- *SO1. Confidentiality*: all information sent to or from an authorized entity should not be revealed to any non authorized party. Furthermore, it should not be possible for an unauthorized party to deduce the location, identity, and route taken by a vehicle based on communication traffic analysis;
- *SO2. Integrity*: every information sent to or from an authorized entity should be protected from unauthorized modification, deletion, malicious modification, or manipulation during transmission;
- *SO3. Availability*: access to ITS services by authorized entities should not be prevented by malicious activity within the system;
- *SO4. Non-repudiation & Accountability*: all registered and authorized entities should be accountable for their actions and cannot deny having sent a message. In case of deviation from system policies, the misbehaving entity should be excluded from the system. Furthermore, it should be possible to audit all changes to security parameters and applications like updates, additions, and deletions;
- *SO5. Authenticity*: it should not be possible for an unauthorized user to impersonate an authorized entity when communicating with other authorized parties.

It is worth noting that the first security object SO1 is said to be *conditional*. That property guarantees the possibility to perform identity resolution of registered and authorized entities that are recognized to be misbehaving. In those cases, Trusted Authorities (TAs) are entitled to collaborate to reconstruct the real identity of the vehicle to effectively exclude it from the system. The exclusion of malicious entities also guarantees the safety of other well behaved vehicles.

4.3. Threat model

For each security objective, we considered a set of vulnerabilities that can be exploited by malicious actors to degrade the security level of the whole system. We selected threats from ETSI (2017) and Lu et al. (2019a) that may apply to our security scheme, with particular reference to the impact on the IOTA-VPKI architecture and the proposed revocation scheme.

- *Confidentiality*:
  - *Man-In-The-Middle attack*: a malicious actor can actively route packets to a controlled entity that impersonates a trusted actor (e.g. TA or harmless vehicle), thus gaining knowledge of identity, location and other confidential information;
  - *Eavesdropping attack*: an attacker can eavesdrop messages on the channel to gain knowledge of identity, location and other confidential information about well behaved vehicles;
  - *Traffic Analysis*: an attacker can analyze the message traffic to reveal which subscription services are being used by individual users, thus being able to launch direct attacks on a particular vehicle;

- *Integrity*:
  - *Manipulation attack*: malicious modification or manipulation of credential management information can severely limit the integrity security objective;
  - *Insertion of information attack*: insertion of crafted malicious information aims to degrade the integrity of the information available in the system. If the malicious information will be trusted by harmless vehicles to take decisions, the consequences can weaken the correctness of security operations and management, or worse, endanger the life of the passengers;
  - *Replay attack*: the attacker may continuously re-send previously received messages into the network, which will confuse other connected vehicles and traffic authorities while identifying vehicles in emergency incidents. The replay of messages could happen at a similar location but at different time, or at a different location and different time (i.e. wormhole attack);
- *Availability*:
  - *Denial of Service (DoS) attack*: this kind of attacks can substantially degrade the availability of the whole system with, for example, the intentional introduction of the high volume of messages that result in a limitation of access to ITS services by authorized and harmless vehicles;
  - *Spamming attack*: the attacker can inject a large number of spam messages in the VANETs system occupying the bandwidth to impede non-faulty vehicles to access ITS services;
  - *Broadcast Tampering attack*: fake warning messages may be broadcasted by malicious actors to conceal the correct safety messages to authorized and non-faulty vehicles;
- *Non-repudiation & Accountability*:
  - *Repudiation attack*: the attacker may deny having sent or receiving critical messages in case of dispute or liability. This happens because no proof exists that any particular message was ever sent by the specific ITS Station (ITS-S);
- *Authenticity*:
  - *Sybil attack*: a malicious actor may create a Sybil node to forge many fake identities to disrupt normal operations of VANETs and gain advantage on the road (e.g. simulate traffic jam to enforce well-behaved vehicles to change their routes and leave the road clear);

5. Proposed revocation scheme

Starting from the generalized version of the IOTA-VPKI architecture depicted in Fig. 1, we developed a novel certificate revocation mechanism fully compliant with EU and US standards as well as European Certificate Policy (European Commission, 2018). This certificate revocation method takes advantage of the DLT to store and distribute the revocation information to all participants in the network. The resulting active certificate revocation scheme overcomes the limitations described in previous Section 2.3, thus aiming at closing the gap in the current US and EU standards. In the following subsections, we will present the details of the proposed vehicular revocation scheme, describing also the way the DLT is integrated and used in the proposed scheme. All the algorithms reported in this section have linear time complexity if considered alone (i.e., without evaluating function calls). The time complexity evaluation of the IOTA functions is beyond the scope of this work. For the sake of clarity, we report in Table 3 the notations used in the presented algorithms.

5.1. Certificate Issuance Procedure

We introduce here the *Certificate Issuance Procedure* that allows a vehicle to access a secure Intelligent Transportation System (ITS). As introduced in Section 4.1, it is necessary for an ITS station δ to acquire rights (i.e., certificates) before accessing any secured ITS system. These rights are obtained in two steps: first, the vehicle δ requests an Enrollment Credential (EC_δ) to be enrolled in the system; then, it will ask for an Authorization Ticket (AT_δ) that entitles it to access the available services according to the granted permissions. To this end, once the vehicle δ has correctly obtained a valid EC (EC_δ), it will request a fresh AT as presented in Algorithm 1. For simplicity, we present only the AT issuance procedure since it shows to the reader the complete interaction between IOTA-VPKI's TAs. However, the EC issuance algorithm is very similar to the one presented here.

Algorithm 1 Authorization Ticket issuance in IOTA-VPKI

Input: $K_v^\delta,\ EC\_PoP_\delta,\ \pi,\ \sigma_{cr},\ m_{ko}$
if isValidECPoP($EC\_PoP_\delta,\ \pi$) **then**
  $AT_\delta \Leftarrow$ generateNewCertificate($\delta,\ K_v^\delta,\ \pi,\ AT$)
  $cur \Leftarrow$ wholeCertificateHash($AT_\delta|\}\}AT\varepsilon$)
  $iota\_address \Leftarrow$ tryte_encoder($HashedId8(cur)$)
  $\sigma_{ci} \Leftarrow$ sign(K_s^{AA}, AT_δ)
  $m_{ci} \Leftarrow (AT_\delta \mid \sigma_{ci})$
  $transaction \Leftarrow$ attachToTangle($iota\_address, m_{ci}$)
  if *transaction is attached* **then**
    $\sigma_{cir} \Leftarrow$ sign(K_s^{AA}, AT_δ)
    $m_{cir} \Leftarrow (AT_\delta \mid \sigma_{cir})$
  else
    $\sigma_{cir} \Leftarrow$ sign(K_s^{AA}, m_{ko})
    $m_{cir} \Leftarrow (m_{ko} \mid \sigma_{cir})$
  end if
else
  $\sigma_{cir} \Leftarrow$ sign(K_s^{AA}, m_{ko})
  $m_{cir} \Leftarrow (m_{ko} \mid \sigma_{cir})$
end if

To effectively perform an AT certificate issuance request, vehicle δ first generates a pair of asymmetric keys for signing operations, namely a signing key K_s^δ and a verification key K_v^δ. This step is done using the keygen$^{sign}(\lambda)$ cryptographic function, providing the security parameters λ as defined in IEEE 1609.2 standard (IEEE, 2019b). A fresh pair of asymmetric keys is generated for each certificate request to reduce the risk of using compromised keys in the communications. Then, the vehicle δ provides to the IOTA-VPKI the following inputs: the generated public verification key K_v^δ to be inserted by the IOTA-VPKI in the new certificate AT_δ; the *Proof of Possession* (EC_PoP_δ) of the valid EC (EC_δ) issued to the vehicle δ; the set of permissions π requested to the AA; the signature σ_{cr} of the certificate request message to be used by the IOTA-VPKI to verify the integrity of the provided inputs (i.e., matching the SO2 discussed earlier). With this information, IOTA-VPKI first contacts the EA to verify if the provided EC_PoP_δ is valid. This step is fundamental to check if the vehicle δ is entitled to request the received permissions π. To guarantee the separation of duties between the EA and the AA, the *Proof of Possession* can only be verified by the EA so that the AA cannot infer the real identity of the vehicle δ. If the EA responds negatively, a certificate issuance rejection message (m_{ko}) is returned to the vehicle δ. Conversely, if the EA confirms the validity of the provided EC_PoP_δ, the new AT_δ certificate is generated with the dedicated function (generateNewCertificate), including the provided verification key K_v^δ and the requested permissions π. Then, the certificate unique representation (cur) is obtained executing the *whole-certificate hash algorithm* (wholeCertificateHash) and then calculating the IOTA address ($iota\_address$) corresponding to the *tryte_encoded* representation of the certificate AT_δ *HashedId8* value. At this point, the AA prepares the IOTA certificate issuance transaction

Table 3
Primitive functions used in the algorithms.

Primitive function	Explanation
tryte_encoder(m)	Given an arbitrary string *m*, this function returns a unique string of 81 trytes as described in IOTA (2021b), that corresponds to the IOTA address representation of the provided string.
attachToTangle(addr, m)	Given a valid IOTA address *addr*, and an arbitrary message *m*, the function attaches a new zero-value transaction to the IOTA Tangle as described in IOTA (2021c).
existsTransactionAt(addr)	On input of a valid IOTA address *addr*, the function checks if a transaction exists on the given address and returns the content of the retrieved transaction.
wholeCertificateHash($Cert_\delta$)	Given a valid certificate $Cert_\delta$ issued to an authorized vehicle δ, the function calculates the *whole-certificate hash* as described in clause 6.4.3 of IEEE 1609.2 standard (IEEE, 2016).
Hashedld8(hash_value)	Given a valid hash binary value *hash_value*, the function returns the eight low-order bytes of the provided hash input, as defined in clause 6.3.27 of IEEE 1609.2 standard (IEEE, 2016).
keygen$^{sign}(\lambda)$	This function receives on input a set of security parameters λ and returns an asymmetric key pair to let the requesting entity δ executes the signing (i.e. K_s^δ) and verification (i.e. K_v^δ) operations.
sign(K_s^δ, m)	On input a signing key K_s^δ issued to an entity δ, and an arbitrary message *m*, the function calculates the signature σ over *m*.
verify(K_v^δ, σ, m)	On input a verification key K_v^δ issued to an entity δ, and an arbitrary message *m*, this function verifies if the provided σ is a valid signature for the message *m*.
notifyInvalidSignature(ρ_γ)	This function accepts on input an invalid signature event ρ_γ, and is used by any harmless entity γ to notify the Misbehavior Authority about some invalid actions made by a misbehaving vehicle.
deregisterVehicle(vehicle_id)	Upon an input of a vehicle identifier *vehicle_id*, this function removes the given identifier from the list of authorized vehicles in the Enrollment Authority.
isValidECPoP(EC_PoP_δ, π)	This function accepts on input the *Proof of Possession* (PoP) of EC_δ and the related set of permissions π requested by the vehicle δ and returns the value *True* when the PoP is valid and the entity δ is entitled to receive the requested permissions π.
generateNewCertificate(δ, K_v^δ, π, CertType)	On input a valid verification key K_v^δ, a vehicle identifier δ, and a set of permissions π, the function returns a new valid certificate of $CertType$ (i.e., EC or AT).

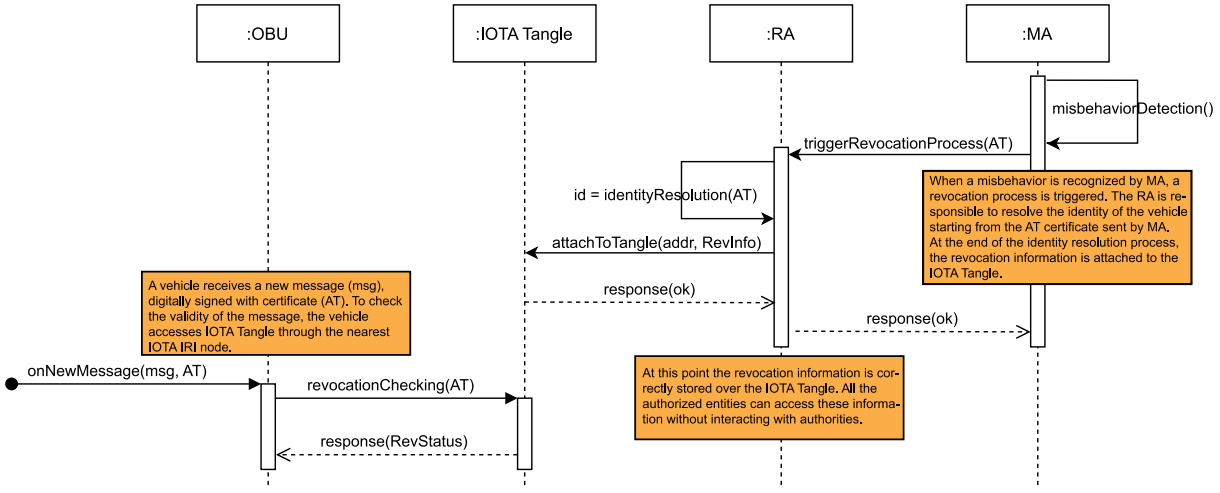

Fig. 2. Revocation process sequence diagram. Once misbehavior is recognized by the Misbehavior Authority (MA), the Revocation Authority (RA) is triggered to complete the revocation process. This last process is composed of two phases: the unique vehicle identifier resolution, and the storage and distribution of the revocation information over the IOTA Tangle.

(m_{ci}) containing the concatenation of the issued certificate (AT_δ) and the corresponding AA's digital signature (σ_{ci}) to guarantee the *integrity* (SO2) and the *authenticity* (SO5) of the issued certificate, as well as the *transparency* of the issuance procedure. Finally, if the transaction attachment (attachToTangle) succeeds, a certificate issuance response message (m_{cir}) containing the issued certificate AT_δ is digitally signed by the AA (σ_{cir}) and sent back to the vehicle δ. Otherwise, a certificate issuance rejection message (m_{ko}) is returned to the vehicle δ.

5.2. Vehicle certificate revocation mechanism

As described in Section 2.2, the revocation process starts when a vehicle δ is detected to be malfunctioning or misbehaving. Regardless of what the intent is (i.e., faulty or malicious node), the valid credentials (i.e. AT_δ and EC_δ) previously issued to the misbehaving vehicle need to be revoked, and all other participants need to be promptly informed.

The flow diagram of the revocation process that starts from a misbehavior detection event is depicted in Fig. 2. As discussed earlier, in each certificate revocation scheme there are two fundamental operations: the *Certificate Revocation* operation, which is executed by the Revocation Authority (RA), and the *Certificate Revocation Status Verification* operation, which is executed on the On-Board Unit (OBU) upon the reception of each new message.

The revocation information is stored in the underlying IOTA DLT by means of *zero-value* transactions, thus enabling each vehicle to retrieve the revocation information with direct access to the distributed ledger. To avoid clashes in revocation information transactions, we considered the unique certificate representation defined in IEEE 1609.2 (clause 6.4.3) (IEEE, 2016). This standard defines the so-called *whole-certificate*

hash algorithm, namely the way to encode the whole certificate with a secure hash function. In fact, this algorithm produces a unique hash value of 3, 8, or 10 bytes (i.e. ASN.1 definitions: *HashedId3*, *HashedId8*, and *HashedId10* respectively). Given this unique and standard hash representation of a generic certificate, we analyzed the current IOTA address format defined in IOTA (2021b), and used the official IOTA library to encode the certificate hash value into a valid *tryte* IOTA address format.

Algorithm 2 Certificate Revocation Process in IOTA-VPKI

Input: $AT_\delta,\ m_{ok},\ m_{ko}$
  $cur \Leftarrow$ HashedId8(wholeCertificateHash(AT_δ))
  $iota\_address \Leftarrow$ tryte_encoder(cur)
  $\sigma_{ri} \Leftarrow \text{sign}(K_s^{RA}, AT_\delta)$
  $m_{ri} \Leftarrow (AT_\delta \mid \sigma_{ri})$
  $transaction \Leftarrow$ attachToTangle($iota\_address, m_{ri}$)
  if *transaction is attached* **then**
    $\sigma_{rm} \Leftarrow \text{sign}(K_s^{RA}, m_{ok})$
    $m_{rm} \Leftarrow (m_{ok} \mid \sigma_{rm})$
  else
    $\sigma_{rm} \Leftarrow \text{sign}(K_s^{RA}, m_{ko})$
    $m_{rm} \Leftarrow (m_{ko} \mid \sigma_{rm})$
  end if

The *Certificate Revocation Process* is presented in Algorithm 2. For the sake of clarity, the reported algorithm describes the steps to revoke an Authorization Ticket (AT): the same operation is executed to revoke an Enrollment Credential (EC). Upon receiving a certificate (AT_δ) previously issued to a vehicle δ, the Revocation Authority (RA) executes the *whole-certificate hash algorithm* (wholeCertificateHash) compliant with IEEE 1609.2 to obtain the unique representation of the certificate *HashedId8* (cur). Then, the RA prepares an IOTA transaction to be issued at the address ($iota\_address$) representing the *tryte_encoded* representation of AT_δ. The message (m_{ri}) is created by concatenating the certificate (AT_δ) and the corresponding RA's digital signature (σ_{ri}) to guarantee the *integrity* (SO2) and the *authenticity* (SO5) of the revocation information. If the transaction attachment (attachToTangle) ends without errors, a success message (m_{ok}) is digitally signed by the RA (σ_{rm}) and correctly sent back to the Misbehavior Authority (MA). On the contrary, when an issue arises during IOTA transaction issuance, a certificate revocation rejection message (m_{ko}) is returned to MA.

Algorithm 3 Revocation Status Verification in OBU

Input: $m_\delta,\ \sigma_\delta,\ AT_\delta$
  if verify($K_v^\delta, \sigma_\delta, m_\delta$) **then**
    $cur \Leftarrow$ HashedId8(wholeCertificateHash(AT_δ))
    if existsTransactionAt(tryte_encoder(cur)) **then**
      if verify($K_v^{RA}, \sigma_{ri}, m_{ri}$) **then**
        ignore message m_δ
      else
        process message m_δ
      end if
    else
      process message m_δ
    end if
  else
    $\sigma_{mr} \Leftarrow \text{sign}(K_s^\gamma, (m_\delta \mid \sigma_\delta \mid AT_\delta))$
    $m_{mr} \Leftarrow ((m_\delta \mid \sigma_\delta \mid AT_\delta) \mid \sigma_{ecri})$
    notifyInvalidSignature(m_{mr})
    ignore message m_δ
  end if

Upon receiving a new secured message, the OBU executes the *Certificate Revocation Status Verification* operation to effectively check the validity of the sender's certificate. To this end, the OBU accesses the IOTA Tangle at the address obtained by *tryte-encoding* of the sender's certificate: if at least a transaction exists, the certificate was revoked, and the message cannot be trusted. Since the revocation checking consists only of the *tryte* value calculation of the sender's certificate hash value, the time needed to check revocation status is constant and it is independent of the number of the revoked certificates. We will discuss this finding later in Section 7, where we report the numerical results measured during the test sessions.

As reported in Algorithm 3, the OBU first verifies the signature (σ_δ) of the arrived message (m_δ): if the verification fails, the message is ignored. Furthermore, a digitally signed notification (m_{mr}) of this invalid signature event is sent by the OBU γ to the MA (notifyInvalidSignature) to let it know about this vehicle misbehavior δ. The notification contains all the information needed to replicate the signature error, namely the received message (m_δ), the received signature (σ_δ), and the sender's certificate (AT_δ). The details on the different misbehavior events that the OBU can notify, as well as the way MA treats those notifications are out of the scope of this work.

If the signature is correctly verified, the OBU calculates the unique *HashedId8* representation (cur) of the sender's certificate (AT_δ) executing the *whole-certificate hash algorithm* (wholeCertificateHash). Then, to effectively verify the revocation status of the provided certificate, the OBU checks the existence of a revocation transaction issued by the RA at the IOTA address corresponding to the *tryte-encoded* certificate representation (cur): if a transaction exists at the given address, and the RA's digital signature contained in the IOTA message is verified by the OBU, the AT_δ has been revoked and thus the received message (m_δ) shall be ignored by the OBU. If no IOTA transaction exists at the obtained address, the message m_δ is correctly processed by the OBU.

As described above, the revocation checking process happens directly by accessing the IOTA Tangle without V2I communication: this avoids increasing the traffic through VPKI elements. This implementation increases the availability of revocation information (SO3), which is in fact always accessible by vehicles and trust authorities, under the hypothesis that vehicles have always Internet access. When, for some reason, a vehicle has limited access to the network, fallback connectivity (e.g. satellite network) can be exploited to provide Internet access, thus allowing one to obtain updated revocation information. Another solution can benefit from Peer-to-Peer (P2P) communications enabling the delegation of the revocation check process to a neighboring vehicle. A similar P2P communication process is defined in IEEE 1609.2 (IEEE, 2016) as well as in ETSI 102 941 (ETSI, 2021b) for P2P Certificate Distribution (P2PCD) used when the end entity has limited access to the cellular network connection. However, even if current communication technologies make this assumption realistic, we have considered the worst-case scenario in which there is no Internet access at all. In this particular case, the revocation checking process cannot be performed. Therefore, to avoid taking into account messages from vehicles that may have been compromised, the received secured message is ignored.

5.3. Identity resolution of misbehaving vehicles

Apart from the RA and the MA that are responsible for misbehavior detection and the revocation process, other Trusted Authorities (TAs) are also important to resolve the identity of the misbehaving vehicle starting from anonymous certificates (i.e., AT). They are involved in the revocation process since the RA needs to resolve the misbehaving vehicle identity before effectively revoking all the certificates previously issued to such vehicles. Furthermore, once the malicious vehicle is revoked, all the TAs need to be promptly informed so that they can reject any new certificate requests received by the revoked entity.

In Fig. 3 is depicted the flow diagram that models the identity resolution of a misbehaving vehicle. Furthermore, we report its implementation in Algorithm 4. The *Vehicle Identity Resolution Process* is

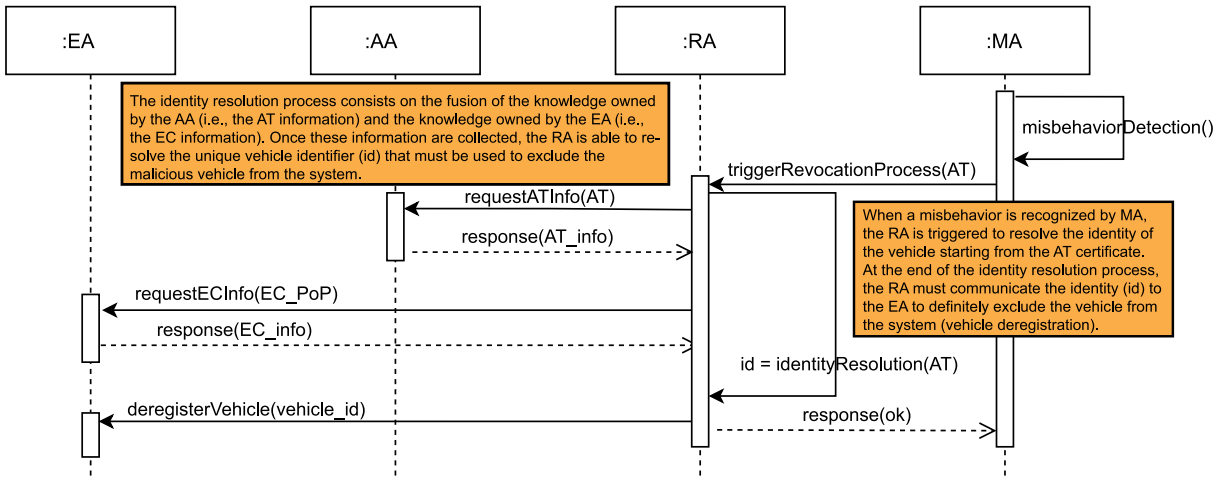

Fig. 3. Identity resolution of a misbehaving vehicle sequence diagram. The Revocation Authority (RA) needs to collect Authorization Ticket (AT) information and Enrollment Credential (EC) information in order to obtain the unique vehicle identifier (id). Once collected, the id is used to deregister the misbehaving vehicle, excluding it from the system.

Algorithm 4 Vehicle Identity Resolution in IOTA-VPKI

Input: AT_δ, m_{ok}, m_{ko}
Step 1 : AT_δ *information resolution*
$\sigma_{atri} \Leftarrow \mathsf{sign}(K_s^{RA}, AT_\delta)$
$m_{atri} \Leftarrow (AT_\delta \mid \sigma_{atri})$
$AT\_info \Leftarrow \mathsf{requestATInfo}(m_{atri})$
Step 2 : EC_δ *information resolution*
$\sigma_{ecri} \Leftarrow \mathsf{sign}(K_s^{RA}, AT\_info.EC\_PoP)$
$m_{ecri} \Leftarrow (AT\_info.EC\_PoP \mid \sigma_{ecri})$
$EC\_info \Leftarrow \mathsf{requestECInfo}(m_{ecri})$
Step 3 : Vehicle revocation in EC
$\sigma_{vr} \Leftarrow \mathsf{sign}(K_s^{RA}, EC\_info.vehicle\_id)$
$m_{vr} \Leftarrow (EC\_info.vehicle\_id \mid \sigma_{vr})$
$\mathsf{deregisterVehicle}(m_{vr})$

divided in three steps: the AT_δ information retrieving; the EC_δ details resolution; finally the vehicle δ full revocation in EA.

The first step starts once the MA sends a revocation request to the RA to effectively revoke the certificate AT_δ of the misbehaving vehicle δ. To this end, the RA digitally signs (σ_{atri}) a request for AT certificate information message (m_{atri}) to be sent to the AA (requestATInfo). The AA looks inside the list of issued certificates searching for the EC_δ *proof of possession* (EC_PoP) received from vehicle δ during the AT_δ issuance procedure (Algorithm 1). Using this *proof of possession* during the AT issuance avoids the AA to link the EC and the AT of the same vehicle, and helps to enforce the separation of duties between the EA and the AA. At this point, the RA begins the second step of determining the identity of the vehicle by contacting the EA. To do this, it digitally signs (σ_{ecri}) a EC certificate information request (m_{ecri}) containing the received $AT\_info.EC\_PoP$ and sends it to the EA (requestECInfo). In turn, the EA retrieves the EC_δ issued to the misbehaving vehicle δ and sends back to the RA the certificate details (EC_info).

At this point, the RA is able to match the information received from the two trust authorities in order to extract the so-called *canonical identifier* of the compromised vehicle (*EC_info.vehicle_id*). Hence, the identity resolution process is completed, and the RA needs to communicate to the EA that the retrieved vehicle identifier needs to be banned from the system and cannot obtain new valid certificates. To do this, the RA prepares a digitally signed (σ_{vr}) vehicle de-registration message (m_{vr}) containing the vehicle *canonical identifier* (*EC_info.vehicle_id*). Finally, the RA sends the message m_{vr} to the EA (deregisterVehicle) to effectively exclude the misbehaving vehicle from the system. This communication does not happen with the AA because, as stated in the standards (ETSI, 2021a,b), a vehicle can request an Authorization Ticket (AT) issuance if and only if it has already obtained a valid Enrollment Credential (EC) from the Enrollment Authority (EA). As a consequence, it is sufficient to de-register vehicle in EA to exclude the vehicle from the system. Furthermore, this requirements is enforced by the Authorization Authority (AA) that asks to EA the validation of the EC *proof of possession* received by the vehicle wishing to obtain a new AT.

Generally speaking, the proposed revocation scheme completely matches the requirements discussed in Section 2.2. Indeed, it realizes the distribution of the revocation information by exploiting the DLT underlying technology. Furthermore, it guarantees zero overhead on the vehicle during the revocation checking process. Finally, due to the underlying storage of DLT, it also provides *transparency* to the whole process.

6. Security analysis

In this section we analyze the new version of the IOTA-VPKI security scheme presented in Section 4.1 according to the security objectives presented in Section 4.2 and also against the threat model discussed in Section 4.3. To briefly recap, the considered security objectives are: *SO1. Confidentiality* to assure information sharing only between authorized entities; *SO2. Integrity* to protect information from unauthorized modification; *SO3. Availability* to let the ITS services being always accessible by authorized entities; *SO4. Non-repudiation & Accountability* to assure that authorized entities are accountable for their actions; and *SO5. Authenticity* to avoid unauthorized actors to impersonate an authorized entity. In particular, we analyze the implementation of the system, equipped with the proposed certificate revocation scheme to assess if it effectively matches the considered security objectives. Furthermore, we also measure the likelihood of exploiting the discussed threats against IOTA-VPKI architecture and the proposed revocation scheme.

V2I communication messages exchanged between vehicles and IOTA-VPKI entities are protected with symmetric and asymmetric encryption schemes that comply with the IEEE 1609.2 standard (IEEE, 2016). This is a mandatory requirement for each security scheme that complies with EU and US vehicular standards, which is, in fact, one of our research objectives. The exploitation of these encryption schemes in V2I communications guarantees the *confidentiality* (SO1) of all information exchanged by vehicles with the infrastructure. However, as discussed in Section 4.2, the security objective SO1 is guaranteed to any harmless and authorized vehicle until it is recognized to be misbehaving. In this case, the resolution of the vehicle identity is

obtained with cooperation between the Enrollment Authority (EA) and the Authorization Authority (AA) as described in Section 5.3. The vehicle identity resolution process is coordinated by the Revocation Authority (RA) that is entitled to resolve the identity of the misbehaving vehicle. In fact, the RA obtains the unique vehicle identifier by joining the AA and EA local information, thus retrieving the Authorization Tickets (ATs) and the Enrollment Credential (EC) issued to the vehicle. The encryption schemes also guarantee protection against *Main-In-The-Middle attack*, *Eavesdropping attack*, and *Traffic Analysis* since the attacker cannot access the content of the collected messages without the receiver's decryption key. Also, the IOTA-VPKI security scheme issues short-lived ATs to mandate vehicles to change pseudonym frequently. The supported pseudonym changing strategy is compliant with the one defined by the ETSI TS 102 940 (ETSI, 2021a) and IEEE 1609.2 (IEEE, 2016) standards, which are designed to prevent others from tracking vehicles.

Furthermore, the IOTA-VPKI security system and its integrated certificate revocation scheme digitally sign every information (e.g. credential request/response messages; revocation information stored on the IOTA Tangle). In this way, any harmless vehicle can check the signature and trust the content if and only if it was signed by the Trusted Authorities (TAs), thus guaranteeing the *Integrity* (SO2) and *Authenticity* (SO5) of each V2I message. The same security objectives are ensured for V2V messages. In fact, each authorized entity shall apply a digital signature to each message and send it along the content to let the receiver verify the authenticity and integrity of the message. Hence, by exploiting signature cryptography, the IOTA-VPKI prevents malicious actors from impersonating well behaved vehicles, as well as trusted security entities from IOTA-VPKI. Furthermore, the signature also guarantees the *Non-repudiation & Accountability* (SO4) security objective, since the sender cannot deny having sent a message that contains a valid signature calculated with its private key. Consequently, the security scheme is also robust against *Manipulation attack*, and *Insertion of information attack*: an attacker is not able to manipulate the content of the certificate request messages, or even alter revocation information stored in DLT, without the private signing key of the Revocation Authority (RA) or any other TA. Furthermore, the scheme is also protected against *Repudiation attack*s because the signature cannot be denied by the sender of the message. It is worth noting that the security scheme leverages the IOTA Distributed Ledger Technology (DLT) to enforce issuing and revoking certificate process transparency: the append-only log feature of IOTA DLT assures also a *proof of execution* for each issuance process made by IOTA-VPKI TAs. Additionally, since the AA issues only ATs with non-overlapping lifetimes, no vehicle can be provided with more than one valid AT at any time: thus an attacker cannot create a malicious Sybil node. Consequently, the security scheme is also robust against *Sybil attack*s. Finally, the *Replay attack* protection deserves a separate discussion. According to the standards, each message is bound with a sequence number (i.e. a timestamp) that is included in the calculation of the digital signature. To effectively implement a *Replay attack* the attacker should be able to calculate the new signature with an updated sequence number, and this is possible only with the sender's private signing key. Moreover, the AT certificate used to sign the messages that the attacker wants to re-send in the network should be still valid and not revoked at the time of the *Replay attack* implementation, and that may not hold due to the fact that the vehicles change pseudonym frequently as described earlier.

Finally, the system achieves the security objective *Availability* (SO3), as the IOTA-VPKI as well as the proposed revocation scheme store the results of the VPKI operation and the revocation information exploiting the DLT technology. If an attacker wants to degrade the certificate or revocation information availability the only way is to attack the underlying DLT technology directly which is challenging as discussed in Li et al. (2020). Consequently, the proposed security scheme is robust against *Denial of Service attack*. Furthermore, the proposed scheme guarantees protection against *Spamming attack* and *Broadcast Tampering attack* because any message that does not contain a valid signature is refused and considered untrusted by other non-faulty vehicles. The attacker can implement those types of attacks only by taking control of a trusted vehicle and use its valid credentials to send malicious messages. However, even in this condition, the Misbehavior Authority (MA) can be able to quickly identify false warning messages broadcasted in the network and promptly exclude the hacked vehicle from the system with certificate revocation.

7. Performance evaluation

As introduced in Section 2.2, the delay-sensitive characteristic of the vehicular environment imposes strict message processing latency requirements. Therefore, these time requirements must be taken into account to measure the feasibility of the implementation of any vehicular revocation scheme.

For this reason, we have concentrated our performance evaluation on the revocation checking delay and on the revocation process delay to demonstrate that the proposed revocation scheme performs well in different conditions, typical of the vehicular environment. In fact, these environments are characterized by a variable number of connected and autonomous cars continuously joining the system and exchanging messages at different frequencies depending on the road conditions (e.g., the message frequency is higher in hazardous situations). Consequently, each security system must not impact negatively the delay of communications to abide by the latency requirements typical of vehicular systems. Hence, the different types of experiments were been selected in a way that it would be possible to demonstrate the minimum impact on the communication delay introduced by the proposed security scheme. To this end, we defined the test sessions considering different message frequencies to mimic all the possible road conditions, and we simulated different numbers of revoked vehicles to evaluate the scalability of the system in presence of a huge number of entities.

In the following subsection, we present and discuss the numerical results of our experiments, providing the reader with the details of our experiment settings to assure the replicability of the test sessions. Finally, we provide a detailed comparative analysis with other implementations.

7.1. Experiment settings

To demonstrate the effectiveness of the proposed solution, a pseudo-real environment was created in our laboratory. Multiple test runs were conducted under different conditions to stress the revocation method and evaluate whether it meets the requirements discussed above.

The experimental environment architecture is depicted in Fig. 5. We used two workstations with 3.0-GHz Intel Core i5 CPU and 8-GB RAM to deploy an RSU instance and an IOTA-VPKI instance extended with the proposed certificate revocation scheme. Also, we equipped the RSU with the IOTA Reference Implementation (IRI) node that acted as a gateway towards the IOTA ledger for issuing transactions. The two workstations were connected to each other through a 1-Gb/s switch. We also used a Proof-of-Work (PoW) custom accelerator, encompassing an FPGA, to speedup the revocation process. To this end, we equipped the IRI node mentioned before with a Cyclone 10 LP FPGA, named PiDiver (Bartolomeu et al., 2020), connected through its GPIO pins to a Raspberry Pi 3B running an HTTP server, used by the IRI node to perform PoW computation offloading. Finally, to simulate the OBU we use our proprietary board equipped with SOM NXP i.MX 8M Quad-core (4 x Cortex™-A53 1.5 GHz) and 4 GB RAM, which simulated the revocation check procedure in different runs.

To avoid interference with public transactions, we have also deployed an instance of Private IOTA Tangle on the IOTA-VPKI instance (IOTA, 2022d). The main Tangle parameter is related to the Proof-of-Work (PoW) setup. One of the main functions of PoW is to reduce the ability of bad actors to spam the network with meaningless

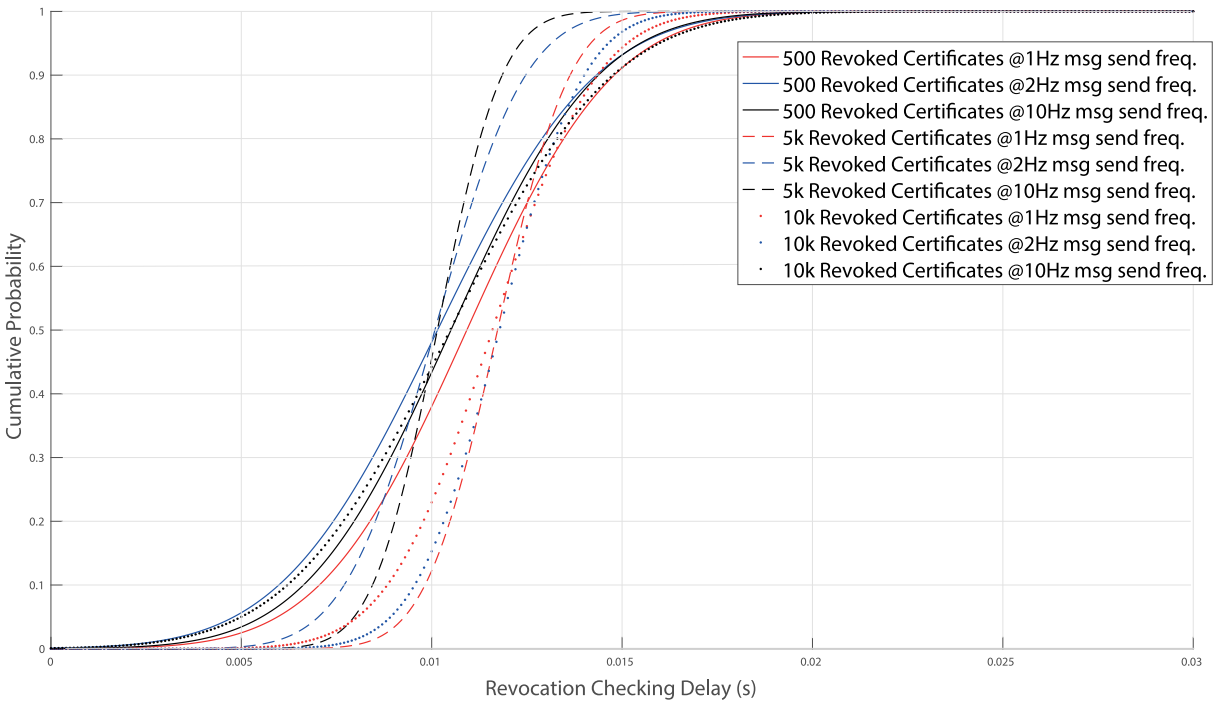

Fig. 4. Cumulative Distribution Function (CDF) of revocation checking delay for the different test runs. The tests were executed on the vehicle side by testing the different supported message frequencies in order to evaluate the performances in all the workload conditions supported by the standards. We replicate the same tests with different numbers of revoked certificates to check if the delay is dependent on the status of the certificates.

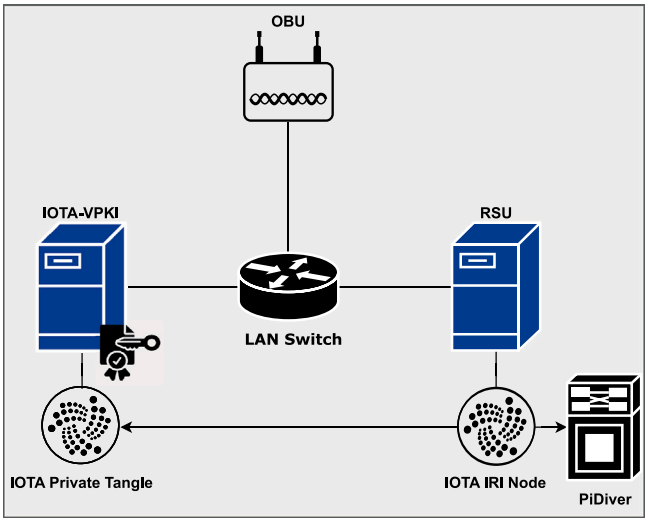

Fig. 5. Experimental environment architecture.

transactions/messages (Anon, 2022a). This avoids the allocation of a significant amount of wasted computational load for a long period of time. The Minimum Weight Magnitude (MWM) determines the computational load required for PoW calculation. In particular, The Private Tangle instance depicted in Fig. 5 was executed with an MWM equal to 9, similar to Devnet (IOTA, 2021a). However, the proposed method is perfectly compatible with the public IOTA Tangle instance which has a MWM equal to 14. To explain this compatibility, it is worth describing the concept of confirmed transaction and IOTA throughput (also known as, confirmed transactions per second (CTPS) Fan et al., 2021). As detailed in Silvano and Marcelino (2020), after attaching a new transaction to the Tangle, such transaction is considered an unapproved transaction and it is called *tip*. Each new *tip* waits for confirmation through direct or indirect approval until its accumulated weight reaches the predefined threshold (Silvano and Marcelino, 2020) at which point the *tip* becomes an *approved* and *confirmed* transaction. As detailed in the experiments reported in Fan et al. (2021), the transaction throughput (i.e., the CTPS) keeps a near-linear growth against the transaction arrival rate, while it is negatively affected by the network delay. However, our scheme does not depend on the *approval* process because vehicles can trust the content of a new transactions even when they are in the *tip* state thanks to the Trusted Authority (TA) cryptographic signature, which is applied on every content attached to the IOTA ledger (Tesei et al., 2021a). For this reason, in the experiments reported in the next section we measured the delay of attaching a new *tip* over the IOTA Tangle, which is much lower than the full approval time, and has greater throughput compatible with the proposed security scheme. Consequently, there is a full *delay* and *throughput* compatibility of the proposed security scheme with the IOTA private network performance reported in Fan et al. (2021), and we expect to experience comparable delays even using the public available IOTA Tangle thanks to the independency of our scheme on the transaction approval process.

7.2. Experimental results

In each run, we simulated that an OBU receives signed messages at different frequencies from different senders. Upon receiving a new message, the OBU first checks for the status of the sender's certificate by calculating the IOTA tryte address corresponding to the hash representation of the given certificate. If there exists at least one transaction on the obtained address, the OBU ignores the received message and goes on processing a new message. The revocation checking is done by exploiting the IRI node deployed on the RSU. This process was implemented in Python for both the revocation execution and revocation checking process.

In order to simulate real message frequencies, we have considered what is stated by ETSI in the Basic Set of Applications Definitions in ETSI (2009, 2019a,b). Considering the different message types (i.e. Cooperative Awareness Message (CAM), and Decentralized Environmental Notification Message (DENM)), and various conditions that

Table 4
Revocation check delay statistics.

Frequency 1 Hz			
# Revoked	Average	Maximum	Pr{t ≤ x} = 0.95
500	10.9 ms	31 ms	16.1 ms
5K	11.7 ms	24 ms	14.2 ms
10K	11.6 ms	29.8 ms	15.2 ms
Frequency 2 Hz			
500	10.2 ms	31.5 ms	15.6 ms
5K	10.1 ms	22.7 ms	13.2 ms
10K	11.8 ms	24.9 ms	14.7 ms
Frequency 10 Hz			
500	10.5 ms	25.2 ms	15.6 ms
5K	10.1 ms	25 ms	12.4 ms
10K	10.5 ms	26.4 ms	16.1 ms

Table 5
Revocation process delay statistics.

IOTA PoW	# Revoked	Average	Maximum	Pr{t ≤ x} = 0.95
Software	10 K	8 s	82.96 s	18.57 s
FPGA	10 K	0.512 s	3.091 s	1.093 s

Table 6
Revocation checking delay comparison.

	Revocation check	Vulnerability window
SEROSA (Gisdakis et al., 2013)	N/A	≥2 s
EADA (Yang et al., 2020)	≤0.200 s	N/A
SECMACE (Khodaei et al., 2018)	≤ 0.075 s	≈1.65 s
BPPA (Lu et al., 2019b)	≤0.015 s	≈2 s
Std. SCMS (Brecht et al., 2018)	≈0.123 s	≥7 days
IOTA-VPKI	≈0.010 s	≈0.50 s

may occur on the road, the possible message frequencies are: 1 Hz; 2 Hz; and 10 Hz. The use of multiple message frequencies was required to study the effectiveness of the proposed certificate revocation scheme under different road conditions (e.g. vehicles increase the frequency in hazardous situations). Furthermore, it allowed analyzing whether the latency of the revocation process check is independent of the available message frequency.

Finally, to demonstrate that the latency of revocation process checking is also independent of the certificate status (i.e. valid or revoked), we set up each run with half of the issued certificates in revoked status. We know that in a real situation this condition is not feasible because the number of valid certificates is typically much higher than those revoked. However, that setting was mandatory to guarantee that the OBU processes a message from a valid or revoked vehicle with equal probability.

Fig. 4 illustrates the Cumulative Distribution Function (CDF) of the revocation check procedure with different numbers of revoked certificates and different message frequencies. As summarized in Table 4, in the first run (500 revoked certificates) there is a 95% of probability that the delays are lower or equal to 16.1 ms when considering a 1 Hz message frequency. Increasing the message frequency has almost no impact on the delay for the 95% probability: 15.6 ms for the message frequencies 2 Hz and 10 Hz. The average delay value is slightly higher than 10 ms for all message frequencies in the first run, while the maximum delay value of 31.5 ms was measured at a message frequency of 2 Hz.

In the second and third runs, the measurements are very close to the first one. In fact, with 5 K revoked certificates, the delays are lower than or equal to 14.2 ms, 13.2 ms, and 12.4 ms in 95% of the cases regarding frequencies of 1, 2, and 10 Hz, respectively. Similarly, in the third run (10K revoked certificates) the $\Pr\{t \leq 15.2 \text{ ms}\} = 0.95$ for 1 Hz message frequency and remains close to this value with increased frequency values (i.e., 14.7 ms for 2 Hz and 16.1 ms for 10 Hz). The average values are still very close to the first run, namely around 11 ms (1 Hz), 10 ms (2 Hz and 10 Hz). Finally, the worst-case scenario in the second and third runs is equal to 29.8 ms and was measured at a 1 Hz message frequency with 10 K revoked certificates. The results confirm that the delay in revocation checking is independent of the number of issued and revoked certificates, as well as the frequency of the message. Furthermore, the majority of the measurements (95%) are significantly lower than 25 ms, which demonstrates that the proposed revocation method is compatible with the vehicular application requirements defined by ETSI in ETSI (2009, 2019a,b).

Furthermore, we randomly revoked 10k certificates to evaluate the delay of the revocation process. As described above, this delay corresponds to the *vulnerability window* of the proposed scheme. In the proposed scheme, this delay represents the time to attach a zero-transaction on the IOTA Tangle at the address derived by the hash value of the certificate to be revoked. Fig. 6 illustrates the CDF of the results obtained with a software implementation of the IOTA Proof-of-Work (PoW) algorithm. As shown in Table 5, with the IOTA PoW software implementation, the *vulnerability window* of the proposed scheme is lower than 18.57 s in 95% of the cases, a very short interval when compared to those in the *revocation by expiry* schemes. However, in the worst-case scenario, a misbehaving vehicle remains trusted in the system for 82.96 s, which means that at the maximum message frequency available (i.e., 10 Hz), an attacker can send a maximum of 829 messages before the revocation information arrives at the other harmless participants. However, this value is still much lower than what occurs in the *vulnerability window* exposed by the current standards (i.e., which is 3 months in the worst case with certificate pre-loading European Commission, 2018).

Executing the certificate revocation process with the PiDiver PoW accelerator provides significantly improved results, as comparatively documented in Fig. 7 and Table 5. In this case, the proposed scheme's *vulnerability window* is lower than 1.093 s in 95% of the cases, which corresponds to an 18-fold improvement with respect to the software implementation. Even the worst-case scenario outperforms the software implementation with a maximum delay of 3.091 s (27 times improvement compared to software implementation), which means that a misbehaving vehicle can send a maximum of 30 messages before the revocation information is effectively distributed to all system participants.

7.3. Comparison with other implementations

Several key implementations providing performance evaluation for the revocation mechanism were considered and compared with our solution. Furthermore, we considered the standard SCMS implemented by Crash Avoidance Metrics Partners LLC under a cooperative agreement with the U.S. Department of Transportation (USDOT) (Brecht et al., 2018), analyzing its performance analysis reported and discussed also in Khan et al. (2022). The addressed works encompass credential management systems and support active vehicle certificate revocation. Other proposals available in the literature such as (Förster et al., 2014), Bißmeyer et al. (2014), C2C-CC (2022), only support revocation by expiry, thus they are not directly comparable with our revocation mechanism proposal. The performance evaluation of the selected related work was carried out under conditions similar to those presented in Section 7.1. The key difference is that in the selected works vehicles (i.e. OBUs) are simulated using generic laptops (or desktop workstations), while we used specific vehicular hardware, which is compliant with EU and US standards and has lower computational power. Furthermore, we compare our results and the measurements reported by the other considered implementations exploiting a simple delay comparison. To this end, we compare our results with the delay

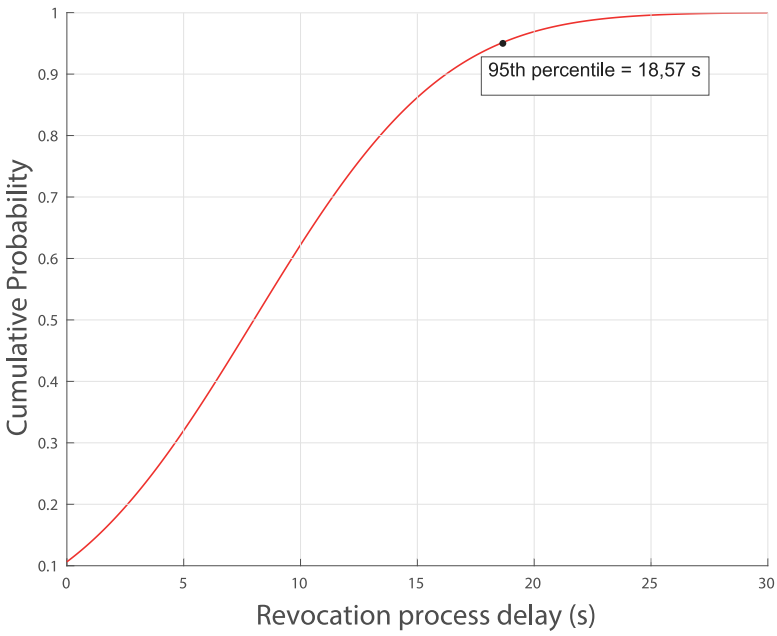

Fig. 6. Cumulative Distribution Function (CDF) of revocation process delay with the IOTA PoW algorithm software implementation. We executed 10k revocation processes for random certificates measuring the time needed to attach the revocation information over the IOTA Tangle.

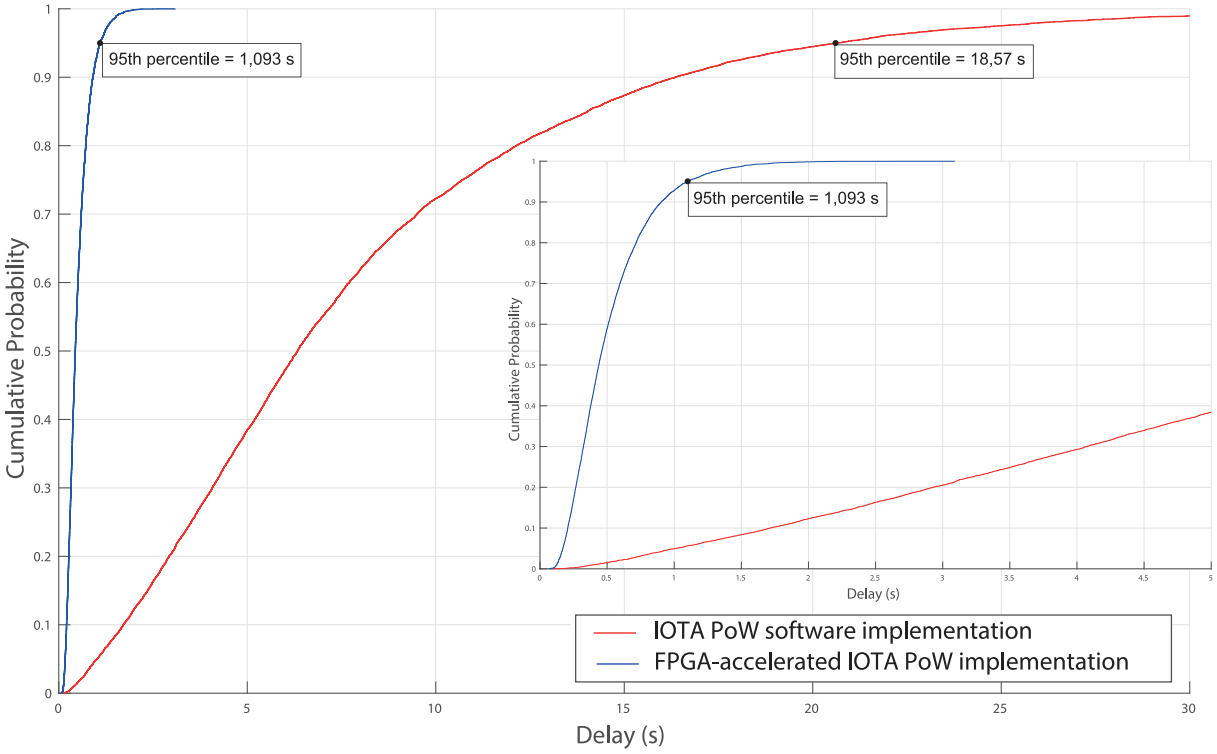

Fig. 7. Comparison between the CDFs obtained from the execution of the revocation process with hardware accelerated (PiDiver) and software implementation of the IOTA PoW algorithm.

in revocation checking and the size of the vulnerability window for each of the considered implementations. Table 6 shows the result of this comparison.

For what concerns revocation checking delay, the results confirm a significant performance improvement of our scheme over the standard US SCMS (Brecht et al., 2018) (12-fold improvement), as well as over SECMACE (Khodaei et al., 2018) (7-fold improvement) and EADA (Yang et al., 2020) (20-fold improvement). It is worth noting that the SECMACE solution takes advantage of the OCSP verification protocol (Santesson et al., 2013) but the verification is done after retrieving the CRL from the EA: the performance evaluation available (Khodaei et al., 2018) states that for a CRL with 100.000 pseudonyms the latency for obtaining a CRL is less than 1500 ms. The same considerations apply to the standard US SCMS (Brecht et al., 2018). In our solution, this delay is completely absent since the vehicle accesses revocation information directly on IOTA Tangle. Considering BPPA (Lu et al., 2019b), the best case out of the analyzed solutions, our scheme reports

a slight improvement of 5 ms. In turn, SEROSA (Gisdakis et al., 2013) does not provide measurements about the time needed by an OBU to check the revocation status of the sender's message (i.e. revocation checking delay). The authors reported only the pseudonym revocation process time (i.e. the vulnerability window) that encompasses the vehicle identity resolution (320 ms) plus the time needed by the other authorities to perform a certificate revocation list update and vehicle identity revocation (more than 1.6 s). Finally, the delay of our proposed scheme is independent of the number of revoked certificates and registered vehicles, which is not the case for EADA (Yang et al., 2020) and (Lu et al., 2019b). Similarly, the performance evaluation reported by SEROSA's authors demonstrates that the time needed to revoke a pseudonym is independent of the number of revoked certificates. However, since the certificate status checking is done by exploiting a CRL-based approach, the revocation checking delay is susceptible to the size of the whole CRL.

Similarly, our scheme outperforms the other considered implementations also in terms of *vulnerability window*. Considering the full revocation time as the vulnerability window size, the obtained results with hardware-accelerated IOTA PoW implementation confirm a significant improvement with respect to the other considered implementations, with a 3-fold improvement of the results reported for SECMACE (Khodaei et al., 2018), and a 4-fold improvement in both SEROSA (Gisdakis et al., 2013) and BPPA (Lu et al., 2019b) implementations. The comparison with the standard SCMS deserves a separate discussion. Considering the *revocation by expiry* approach defined by the standards, the vulnerability window strictly depends on two factors: the minimum validity period of the credentials issued to the vehicles; the exploited certificate changing strategy. The authors reported in Brecht et al. (2018) the following parameter values:

- Certificate validity time period: 7 days
- Number of certificates valid simultaneously: min 20
- Overall covered time-span: 1–3 years

Even if these parameters can be fully customized by the SCMS Manager, the absence of an active certificate revocation mechanism results in a vulnerability window that can vary from 7 days to several months. These values are very high compared with the ones measured with our scheme.

All in all, our scheme outperforms the other considered implementation with respect to revocation checking delay and vulnerability window size. As a result, our solution matches the VANETs time requirements and critical latency discussed in Section 2, while increasing the security level of the whole system. Furthermore, unlike all the considered research works' delays, which are highly dependent on the number of registered vehicles, the performance evaluation of the proposed scheme demonstrates that the delay introduced by the proposed scheme is completely independent of the message frequency and the number of issued and revoked certificates, thus independent of the number of registered and available vehicles.

8. Conclusion

In this article, we have presented a new VANET revocation method that closes a gap in the current US and EU standards implementing a transparent active vehicle revocation mechanism through IOTA Distributed Ledger Technology (DLT). The solution was a generalized version of our previous work IOTA-VPKI customized for the logistics use case (Tesei et al., 2021a). Starting on the first IOTA-VPKI architecture version presented in Tesei et al. (2018), we enhanced the Revocation Authority (RA) to support the proposed vehicular revocation mechanism taking advantage of the DLT technology to transparently save revocation information. Furthermore, we extended the IOTA-VPKI architecture with a *Misbehavior Authority* (MA) to allow the solution to be compatible with any method that aims to detect malicious or misbehaving vehicles on the road. Once the MA recognizes that a vehicle is compromised, the RA is activated to publish the revocation information on the IOTA Tangle ledger with a zero-value transaction. In parallel, the RA starts the identity resolution process to retrieve the vehicle identity and communicate it to other TAs, indicating that no more valid credentials can be issued to the compromised vehicle. In this way, once an On-Board Unit (OBU) receives a new secured message it retrieves revocation information about the sender's certificate with direct access to the IOTA Tangle: if at least one zero-value transaction signed by the RA exists at the address represented by the sender's certificate, the message must be ignored. To complement our proposal, we considered five well-known security objectives and discuss a threat model compatible with ETSI (2017) and Lu et al. (2019a). Furthermore, we reported a complete security analysis that discusses IOTA-VPKI robustness against common attacks in the scope of the security objectives considered.

Experimental results have documented that 95% of the revocation check delays are lower than or equal to 16 ms. These results demonstrate the effectiveness of the proposed revocation method and compatibility with the vehicular applications time constraints defined by ETSI in ETSI (2009, 2019a,b), enabling its use in realistic ITS environments. Furthermore, results confirm that the revocation checking delay is independent of the certificate status (i.e., issued or revoked) as well as independent of the total number of issued certificates. This, in turn, confirms also that the proposed scheme overcomes the issues found in CRL-based approaches available in current US and EU standards, characterized by low scalability and high revocation checking delays in presence of high number of revoked vehicles. Finally, the underlying IOTA DLT storage guarantees the transparency of the whole revocation process, as well as the permanent availability of revocation information that does not require complex distribution protocols.

The presented RA revocation process delay measurements demonstrate that the *vulnerability window* of the proposed revocation scheme is less than 1.093 s on the majority (95%) of the measurements. These results were obtained with a low-cost FPGA-accelerated implementation of the IOTA PoW algorithm. This is an important improvement with respect to the *vulnerability window* available in the current standards that can reach 3 months according to the latest European security policy (certificate pre-loading case European Commission, 2018). In addition, the proposed solution outperforms the other existing implementation in terms of *vulnerability window* (3 to 4 times improvements), thus advancing the state of the art in vehicle security.

Finally, the standard-focused research work approach that we exploited is mandatory for the proposed solution acceptance in the industry. This in turn fosters a wider base of adoption, as well as a real contribution to the evolution of the current C-ITS security standards. Last but not least, the approach also contributes to increase the security and safety offered to the drivers. In conclusion, we consider our solution to be an extension of current EU and US standards in order to close the current gap in the vehicle revocation mechanism. Furthermore, the proposed solution mitigates risks and reduces the *vulnerability window* of the current ITS security architecture. All in all, the proposed revocation scheme perfectly matches the requirements of VANETs, and it is ready to be used in a real and large-scale ITS deployment.

As future works, we plan to test the IOTA-VPKI system integrated with the proposed solution in two real testbeds: the first is available at the Livorno seaport and highway (Italy); the second is available in a Smart City context at Aveiro (Portugal). With these pilot sites, we will demonstrate the effectiveness of the proposed solution in a European large-scale testbed embodying a realistic ITS environment.

CRediT authorship contribution statement

Andrea Tesei: Writing – original draft, Writing – review & editing, Conceptualization, Methodology, Software, Validation, Investigation. **Domenico Lattuca:** Validation, Investigation, Data curation, Visualization. **Marco Luise:** Supervision. **Paolo Pagano:** Project administration, Supervision. **Joaquim Ferreira:** Writing – review & editing, Supervision. **Paulo C. Bartolomeu:** Writing – review & editing, Supervision.

Declaration of competing interest

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

Data availability

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

References

Ali, I., Gervais, M., Ahene, E., Li, F., 2019. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. J. Syst. Archit. 99, http://dx.doi.org/10.1016/j.sysarc.2019.101636.

Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H.M., Rowe, J., Levitt, K., 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Commun. Mag. 53 (6), 126–132.

Anon, 2022a. IOTA blog - Energy benchmarks for IOTA. URL https://blog.iota.org/internal-energy-benchmarks-for-iota/.

Anon, 2022b. IOTA Wiki - An introduction to IOTA. URL https://wiki.iota.org/learn/about-iota/an-introduction-to-iota.

Anon, 2022c. IOTA Wiki - Energy efficiency. URL https://wiki.iota.org/learn/about-iota/energy-efficiency.

Bartolomeu, P.C., Vieira, E., Ferreira, J., 2020. Pay as you go: A generic crypto tolling architecture. IEEE Access 8, 196212–196222. http://dx.doi.org/10.1109/ACCESS.2020.3034299.

Bißmeyer, N., Mauthofer, S., Petit, J., Lange, M., Moser, M., Estor, D., Sall, M., Feiri, M., Moalla, R., Lagana, M., et al., 2014. PRESERVE - preparing secure vehicle-to-X communication systems.

Boneh, D., Boyen, X., Shacham, H., 2004. Short group signatures. In: Annual International Cryptology Conference. Springer, pp. 41–55.

Boneh, D., Shacham, H., 2004. Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM Conference on Computer and Communications Security. pp. 168–177.

Brecht, B., Therriault, D., Weimerskirch, A., Whyte, W., Kumar, V., Hehn, T., Goudy, R., 2018. A security credential management system for V2X communications. IEEE Trans. Intell. Transp. Syst. 19 (12), 3850–3871. http://dx.doi.org/10.1109/TITS.2018.2797529.

C2C-CC, 2022. Car2Car communication consortium. URL https://www.car-2-car.org.

Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K., 2009. Security and privacy issues for inter-vehicle communications in VANETs. In: 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops. pp. 1–3. http://dx.doi.org/10.1109/SAHCNW.2009.5172962.

Chulerttiyawong, D., Jamalipour, A., 2021. A Blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement. IEEE Access 9, 127305–127319. http://dx.doi.org/10.1109/ACCESS.2021.3112013.

ETSI, 2009. ETSI, TR. 102 638 v1.1.1-Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Definitions. European Telecommunications Standards Institute (ETSI) Technical Report 102 638, Version 1.1.1.

ETSI, 2017. ETSI, TR. 102 893 v1.2.1-Intelligent transport systems (ITS);security; Threat, Vulnerability and Risk Analysis (TVRA). European Telecommunications Standards Institute (ETSI) Technical Report 102 893, Version 1.2.1.

ETSI, 2019a. ETSI, EN. 302 637-2 v1.4.1-Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. European Telecommunications Standards Institute (ETSI) European Norm 302 637-2, Version 1.4.1.

ETSI, 2019b. ETSI, EN. 302 637-3 v1.3.1-Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service. European Telecommunications Standards Institute (ETSI) European Norm 302 637-3, Version 1.3.1.

ETSI, 2020. ETSI, TS. 103 097 v1.4.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats. European Telecommunications Standards Institute (ETSI) Technical Specification 103 097, Version 1.4.1.

ETSI, 2021a. ETSI, TS. 102 940 v2.1.1-Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; Release 2. European Telecommunications Standards Institute (ETSI) Technical Specification 102 940, Version 2.1.1.

ETSI, 2021b. ETSI, TS. 102 941 v1.4.1-Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. European Telecommunications Standards Institute (ETSI) Technical Specification 102 941, Version 1.4.1.

European Commission, 2016. Security & Certification Final Report Annex II Revocation of Trust In Cooperative Intelligent Transport Systems (C-ITS). European Commission, C-ITS Platform WG5, Release 1.1.

European Commission, 2018. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). European Commission, C-ITS Platform Phase II, Release 1.1.

European Parliament, 2019. Commission Delegated Regulation (EU) of 13 Match 2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. Eur. Comm., Off. J..

Fan, C., Ghaemi, S., Khazaei, H., Chen, Y., Musilek, P., 2021. Performance analysis of the IOTA DAG-based distributed ledger. ACM Trans. Model. Perform. Eval. Comput. Syst. 6 (3), 1–20.

Förster, D., Kargl, F., Löhr, H., 2014. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In: 2014 IEEE Vehicular Networking Conference. VNC, IEEE, pp. 25–32.

Gisdakis, S., Laganà, M., Giannetsos, T., Papadimitratos, P., 2013. SEROSA: Service oriented security architecture for vehicular communications. In: 2013 IEEE Vehicular Networking Conference. IEEE, pp. 111–118.

Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A., 2017. Vanet security challenges and solutions: A survey. Veh. Commun. 7, 7–20. http://dx.doi.org/10.1016/j.vehcom.2017.01.002.

IEEE, 2016. IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1–240. http://dx.doi.org/10.1109/IEEESTD.2016.7426684.

IEEE, 2017. IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages - Amendment 1. IEEE Std 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016), pp. 1–123. http://dx.doi.org/10.1109/IEEESTD.2017.8065169.

IEEE, 2019a. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013), pp. 1–106. http://dx.doi.org/10.1109/IEEESTD.2019.8686445.

IEEE, 2019b. IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages - Amendment 2–PDU Functional Types and Encryption Key Management. IEEE Std 1609.2b-2019 (Amendment to IEEE Std 1609.2-2016), pp. 1–30. http://dx.doi.org/10.1109/IEEESTD.2019.8734860.

IOTA, 2021a. IOTA networks. URL https://legacy.docs.iota.works/docs/getting-started/1.1/networks/overview.

IOTA, 2021b. IOTA version 1 - Address format documentation. URL https://legacy.docs.iota.works/docs/getting-started/1.1/accounts/addresses.

IOTA, 2021c. IOTA version 1 - Transactions documentation. URL https://legacy.docs.iota.works/docs/getting-started/1.1/accounts/addresses.

IOTA, 2022a. IOTA Chronicle documentation. URL https://wiki.iota.org/chronicle.rs/welcome.

IOTA, 2022b. IOTA - Distributed ledger technology. URL https://www.iota.org.

IOTA, 2022c. IOTA masked authenticated messaging documentation. URL https://legacy.docs.iota.works/docs/mam/1.0/how-it-works.

IOTA, 2022d. IOTA: Set up a private tangle. URL https://legacy.docs.iota.works/docs/compass/1.0/overview.

Kannengießer, N., Lins, S., Dehling, T., Sunyaev, A., 2020. Trade-offs between distributed ledger technology characteristics. ACM Comput. Surv. 53 (2), 1–37.

Khan, S., Luo, F., Zhang, Z., Rahim, M.A., Khan, S., Qadri, S.F., Wu, K., 2022. A privacy-preserving and transparent identity management scheme for vehicular social networking. IEEE Trans. Veh. Technol..

Khodaei, M., Jin, H., Papadimitratos, P., 2018. SECMACE: Scalable and robust identity and credential management infrastructure in vehicular communication systems. IEEE Trans. Intell. Transp. Syst. 19 (5), 1430–1444.

Khodaei, M., Papadimitratos, P., 2020. Scalable & resilient vehicle-centric certificate revocation list distribution in vehicular communication systems. IEEE Trans. Mob. Comput..

Kumar, V., Petit, J., Whyte, W., 2017. Binary hash tree based certificate access management for connected vehicles. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks. WiSec '17, Association for Computing Machinery, New York, NY, USA, pp. 145–155. http://dx.doi.org/10.1145/3098243.3098257.

Li, Y., Cao, B., Peng, M., Zhang, L., Zhang, L., Feng, D., Yu, J., 2020. Direct acyclic graph-based ledger for internet of things: Performance and security analysis. IEEE/ACM Trans. Netw. 28 (4), 1643–1656. http://dx.doi.org/10.1109/TNET.2020.2991994.

Lu, Z., Qu, G., Liu, Z., 2019a. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transp. Syst. 20 (2), 760–776. http://dx.doi.org/10.1109/TITS.2018.2818888.

Lu, Z., Wang, Q., Qu, G., Zhang, H., Liu, Z., 2019b. A blockchain-based privacy-preserving authentication scheme for VANETs. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 27 (12), 2792–2801. http://dx.doi.org/10.1109/TVLSI.2019.2929420.

Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., He, W., 2020. An efficient decentralized key management mechanism for VANET with blockchain. IEEE Trans. Veh. Technol. 69 (6), 5836–5849. http://dx.doi.org/10.1109/TVT.2020.2972923.

Mendiboure, L., Chalouf, M.A., Krief, F., 2020. A scalable blockchain-based approach for authentication and access control in software defined vehicular networks. In: 2020 29th International Conference on Computer Communications and Networks. ICCCN, pp. 1–11. http://dx.doi.org/10.1109/ICCCN49398.2020.9209661.

Noor, A., Wu, Y., Khan, S., 2020. Secure and transparent public-key management system for vehicular social networks. In: 2020 IEEE 6th International Conference on Computer and Communications. ICCC, pp. 309–316. http://dx.doi.org/10.1109/ICCC51575.2020.9345086.

Parkinson, S., Ward, P., Wilson, K., Miller, J., 2017. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans. Intell. Transp. Syst. 18 (11), 2898–2915.

Popov, S., 2018. The tangle. White Pap. 1 (3).

Qi, J., Gao, T., 2020. A privacy-preserving authentication and pseudonym revocation scheme for VANETs. IEEE Access 8, 177693–177707. http://dx.doi.org/10.1109/ACCESS.2020.3027718.

Rawat, A., Sharma, S., Sushil, R., 2012. VANET: Security attacks and its possible solutions. J. Inf. Oper. Manag. 3 (1), 301–304.

Rigazzi, G., Tassi, A., Piechocki, R.J., Tryfonas, T., Nix, A., 2017. Optimized certificate revocation list distribution for secure V2X communications. In: 2017 IEEE 86th Vehicular Technology Conference. VTC-Fall, pp. 1–7. http://dx.doi.org/10.1109/VTCFall.2017.8288287.

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., 2013. X. 509 internet public key infrastructure online certificate status protocol-OCSP. RFC 6960, 1–41.

Silvano, W.F., Marcelino, R., 2020. Iota tangle: A cryptocurrency to communicate internet-of-things data. Future Gener. Comput. Syst. 112, 307–319.

Sun, Z., Liu, R., Hu, H., Liu, D., Yan, Z., 2022. Cyberattacks on connected automated vehicles: A traffic impact analysis. IET Intell. Transp. Syst..

Tesei, A., Di Mauro, L., Falcitelli, M., Noto, S., Pagano, P., 2018. IOTA-VPKI: A DLT-based and resource efficient vehicular public key infrastructure. In: 2018 IEEE 88th Vehicular Technology Conference. VTC-Fall, IEEE, pp. 1–6.

Tesei, A., Lattuca, D., Tardo, A., Mauro, L.D., Pagano, P., Luise, M., Bartolomeu, P.C., Ferreira, J., 2021a. Securing seaport logistic vehicles using a distributed ledger-based credential management system. IEEE Open J. Veh. Technol. 2, 162–179. http://dx.doi.org/10.1109/OJVT.2021.3067209.

Tesei, A., Luise, M., Pagano, P., Ferreira, J., 2021b. Secure multi-access edge computing assisted maneuver control for autonomous vehicles. In: 2021 IEEE 93rd Vehicular Technology Conference. VTC2021-Spring, pp. 1–6. http://dx.doi.org/10.1109/VTC2021-Spring51267.2021.9449087.

van der Heijden, R.W., Dietzel, S., Leinmüller, T., Kargl, F., 2019. Survey on misbehavior detection in cooperative intelligent transportation systems. IEEE Commun. Surv. Tutor. 21 (1), 779–811. http://dx.doi.org/10.1109/COMST.2018.2873088.

Verheul, E., Hicks, C., Garcia, F.D., 2019. IFAL: Issue first activate later certificates for V2X. In: 2019 IEEE European Symposium on Security and Privacy. EuroS&P, pp. 279–293. http://dx.doi.org/10.1109/EuroSP.2019.00029.

Wang, Q., Gao, D., Chen, D., 2020a. Certificate Revocation Schemes in Vehicular Networks: A Survey. IEEE Access 8, 26223–26234. http://dx.doi.org/10.1109/ACCESS.2020.2970460.

Wang, Y., Zhong, H., Xu, Y., Cui, J., Wu, G., 2020b. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs. IEEE Syst. J. 14 (4), 5373–5383. http://dx.doi.org/10.1109/JSYST.2020.2977670.

Xu, Y., Guo, G., 2022. Event triggered control of connected vehicles under multiple cyber attacks. Inform. Sci. 582, 778–796.

Yang, Y., Wei, L., Wu, J., Long, C., Li, B., 2021. A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular Ad-Hoc network. IEEE Internet Things J. 1. http://dx.doi.org/10.1109/JIOT.2021.3107443.

Yang, A., Weng, J., Yang, K., Huang, C., Shen, X., 2020. Delegating authentication to edge: A decentralized authentication architecture for vehicular networks. IEEE Trans. Intell. Transp. Syst. 1–15. http://dx.doi.org/10.1109/TITS.2020.3024000.

Zhang, Y., Tong, F., Xu, Y., Tao, J., Cheng, G., 2020. A privacy-preserving authentication scheme for VANETs based on consortium blockchain. In: 2020 IEEE 92nd Vehicular Technology Conference. VTC2020-Fall, pp. 1–6. http://dx.doi.org/10.1109/VTC2020-Fall49728.2020.9348497.

Andrea Tesei received his Master's degree in Computer Science and Networking jointly by Sant'Anna School of Advanced Studies and the University of Pisa, Italy in 2017. He is currently pursuing the Ph.D degree in the Department of Information Engineering at University of Pisa, Italy. His research interests include, vehicular public key infrastructure, security scheme for intelligent transportation system, vehicle revocation mechanisms, and misbehavior detection.

Domenico Lattuca received his master's degree in Telecommunications Engineer at the University of Palermo, Italy in 2018. From February 2019 he works at CNIT (National Interuniversity Consortium for Telecommunications) as researcher and Ph.D. student of Pisa University. His research interests include vehicular misbehavior detection, machine learning, and security mechanisms for intelligent transportation system.

Marco Luise is a Full Professor of Telecommunications at the University of Pisa, Italy. He has chaired a number of scientific conferences, including EUSIPCO 2006 and IEEE ICASSP in 2014. Formerly an Editor of IEEE Trans. Commun., he is the co-founder of the Int. Jou. of Navigation and Observation, a Division Editor of the Jou. of Commun. and Networks, and was the coordinator of the European Network of Excellence in Wireless Communications NEWCOM#. An IEEE Fellow, he's authored more than 300 publications, and his main research interests lie in the broad area of wireless/satellite communications and positioning.

Paolo Pagano received his Ph.D. degree in High Energy Physics from Trieste University having worked for the COMPASS collaboration at CERN. He holds a Master in IT from Scuola Superiore Sant'Anna in Pisa. From 2009 he is with the National Inter-University Consortium for Telecommunications (CNIT), leading the Networks of Embedded Systems area at the National Laboratory of Photonic Networks and Technologies in Pisa (http://pntlab.cnit.it/). From October 2015 he is the director of the joint (CNIT/Port Network Authority of the Northern Tyrrhenian Sea) laboratory on advanced sensing and networking in seaports (http://jlabports.cnit.it). His research activities have a specific focus on Intelligent Transportation Systems and Port of the Future. He is participating (on behalf of CNIT) to the ETSI standardization committees for Cooperative ITS and maritime communication. From September 2018 he is a member of the Working Group "Smart Roads", Technical Committee on Autonomous Driving at the World Road Association. He co-authored about 100 peer reviewed papers to international journals and conferences.

Joaquim Ferreira received a Ph.D. degree in Informatics Engineering from University of Aveiro, Portugal in 2005. Currently, he is an adjunct professor at School of Technology and Management from the University of Aveiro and researcher at Telecommunications Institute. He has been involved in several international and national research projects. His research interests include: dependable distributed systems, fault-tolerant real-time communications, wireless vehicular communications, cooperative ITS systems and medium access control protocols. He is the author of several scientific papers and book chapters in his areas of expertise. He is a senior member of IEEE and served on several scientific committees of conferences.

Paulo C. Bartolomeu received his Ph.D. in Informatics Engineering from the University of Aveiro, Portugal, in 2014. He has participated in several R&D projects both at the academia (ARMONIO, CAMBADA) and in the industry (CIRaF, DHT-Mesh, BikeEmotion, LUL, SheepIT). He is the author of two patents and more than 40 scientific publications including papers in conferences, journals and book chapters. His research interests include IoT, Real-Time Communications, Networked Embedded Systems, Decentralized Identity, and Blockchain.