IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2018.DOI

SPATA: Strong Pseudonym based AuthenTicAtion in Intelligent Transport System

QAZI EJAZ ALI[1], NAVEED AHMAD[1], ABDUL HASEEB MALIK[1],GAUHAR ALI[1], MUHAMMAD ASIF[2], MUHAMMAD KHALID[3], YUE CAO[4,3]

[1]Department of Computer Science, University of Peshawar, Pakistan. (e-mail: qaziejazali; n.ahmad; haseeb; gauharstd@uop.edu.pk)
[4]Department of Computer Science, University of Peshawar. Pakistan. (e-mail: gauharstd@uop.edu.pk)
[2]Department of Electronics, University of Peshawar, Pakistan. (e-mail: m.asif@uop.edu.pk)
[3]Department of Computer & Information Sciences, Northumbria University, UK. (e-mail: m.khalid; yue.cao @northumbria.ac.uk)
[4]Transportation Science and Engineering, Beihang University, Beijing, China.

Corresponding Author: Yue Cao (e-mail: yue.cao@northumbria.ac.uk), Qazi Ejaz Ali (qajiejazali@uop.edu.pk).

ABSTRACT Intelligent Transport System (ITS) is generally deployed to improve road safety, comfort, security, and traffic efficiency. A robust mechanism of authentication and secure communication is required to protect privacy and conditional resolution of pseudonyms to revoke malicious vehicles. In a typical ITS framework, a station can be a vehicle, Road Side Unit (RSU), or a server that can participate in communication. During authentication, the real identity of an Intelligent Transport System-Station (ITS-S), referred to as a vehiclečň should not be revealed in order to preserve its privacy. In this paper, we propose a Strong Pseudonym based AutenTicAtion (SPATA) framework for preserving the real identity of vehicles. The distributed architecture of SPATA allows vehicles to generate pseudonyms in a very private and secure way. In the absence of a distributed architecture, the privacy cannot be preserved by storing information regarding vehicles in a single location. Therefore, the concept of linkability of certificates based on single authority is eliminated. This is done by keeping the real identity to pseudonym mappings distributed. Furthermore, the size of the Certificate Revocation List (CRL) is kept small, as only the most recent revoked communication pseudonyms are kept in the CRL. The privacy of the vehicle is preserved during the revocation and resolution phase through the distributed mechanism. Empirical results show that SPATA is a lightweight framework with low computational overhead, average latency, overhead ratio, and stable delivery ratio, in both sparse and dense network scenarios.

INDEX TERMS Intelligent Transport System, Pseudonym, Privacy, Authentication.

I. INTRODUCTION

INTELLIGENT Transport System (ITS) is an emerging area that embeds intelligence in vehicles making transportation efficient, comfortable, and safe. In the absence of intelligence, there may be issues of traffic jams, accidents, and congestion. Incorporating intelligence in transport system results in safe and efficient driving. In case of an accident on the road, broadcasting relevant messages enables Intelligent Transport System-Stations (ITS-Ss e.g. vehicles) to diverge among lanes. Such information dissemination avoids congestion and pile up accidents.

ITS communication architecture, as shown in Figure 1 consists of ITS-Ss such as vehicles, Road Side Units (RSUs), and servers. The vehicles are equipped with On Board Units (OBUs) that enable them to communicate with other ITS-Ss (vehicles or RSUs). ITS supports Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, known as V2X communication [1], [2]. Particularly, for V2V and V2I communications, the IEEE 802.11P standard is used. This standard is also known as Wireless Access in Vehicular Environment (WAVE)/Dedicated Short Range Communication (DSRC) [3], [4].

Each ITS-S (vehicle) broadcasts position messages known as Cooperative Awareness Messages (CAMs) in Europe [5] or Basic Safety Messages (BSMs) in the United States [6]. CAMs are broadcasted among vehicles and RSUs, to achieve road safety and traffic efficiency. The use of CAMs includes emergency vehicle warnings, traffic turn collision

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

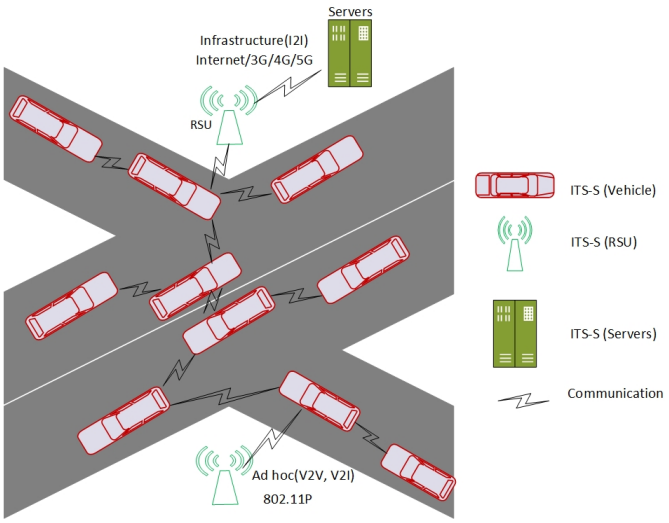


FIGURE 1: ITS communication architecture

warnings, slow vehicle indications, lane change messages, emergency brakes, traffic condition warning messages, on the road or roadside stationary vehicles (accident or vehicle problem), road work messages, hazardous locations, wind, and visibility warnings. ITS applications are mainly divided into road safety, traffic efficiency, and infotainment applications [7]. Infotainment or miscellaneous applications include advertised services such as public transport information, point of interest advertisements/notifications, parking facilities, media downloading, local electronic commerce, fleet management, financial services, real time traffic conditions, and insurance.

One of the building blocks of ITS is Vehicular Ad hoc Networks (VANETs) [8]. In VANETs, like other wireless networks, there exist attacks that jeopardize a vehicle's privacy. False information can be used by an attacker to collect users' private data and their location [9]. To protect legitimate users' in VANETs from attackers, privacy and security techniques must be in place.

The IEEE 1609.2 standard addresses security issues in VANETs [10]. According to this standard, a Certificate Authority (CA) issues digital certificates to each vehicle in ITS. In case of a malicious behavior, the vehicle's certificates may be revoked. In ITS, both location and identity privacy is needed to avoid unethical usage by malicious ITS-S. The author [11] demonstrated privacy in degree levels that is different for every application. Applications that use CAMs for communication need conditional anonymity. In the case of a malicious activity, the malicious vehicle should be revoked. Applications that use infotainment services require privacy from low to high degree. For instance, if an ITS user is getting public transport information, it requires low privacy.

Vehicles broadcast beacons (also known as safety messages) periodically, in order to inform other vehicles about its current speed, direction, and position. Unfortunately, eavesdroppers may use the status information of the vehicles for user tracking [12]. To provide secure and private communication in ITS, the typical security properties must be preserved, i.e., privacy, authentication, integrity, and non-repudiation [13], [14].

In order to protect the real identity of a vehicle, pseudonyms are used [13], [15]. Changing user pseudonyms at regular intervals is important to avoid linkability [16]. The pseudonym based techniques, discussed in [17], [18] used cryptography to protect the identity of a user. However, the techniques produce high computational and communication costs. Onion routing, multi-hop anonymization techniques are not feasible solutions for ITS [19], as its computational and communication overheads are high. The self generation pseudonyms are not encouraged in ITS due to Sybil attacks [20].

Schaub et al. [21] proposed that pseudonym resolution information should be incorporated in the pseudonym certificate instead of the pseudonym issuing authorities. However, the pseudonym to real identity mapping should not be directly incorporated into the pseudonym certificate, because it can be used to jeopardize the privacy of source vehicles.

Wang et al. [22] proposed that there should be two servers one for pseudonym and the second for reputation. However, this work produces a delay in the communication, due to extra overhead on the reputation server, in order to compute and check the reputation of vehicles each time. The authors [23] presented the idea of primary and secondary pseudonyms. The primary pseudonym is provided by the CA and is a single point of attack. Similarly, the secondary pseudonyms are generated through RSUs and are used for V2X communication. However, RSUs are located in an open infrastructure, and prone to side channel attacks [24].

The malicious vehicle should be banned from the ITS network by invalidating its certificates [25]. Schaub et al. [20] discussed that there should be minimum exposure of information of a vehicle to other ITS-Ss (vehicles or server). ITS communication [25] should be conditionally anonymous, in case of malicious activities, the malicious vehicle should be revoked.

To provide effective anonymity, two or more beacons related to the same vehicle should not be linked. If unauthorized vehicles are not revoked from ITS communication, then according to [26], syntactic linking and semantic linking attacks are possible. In a syntactic linking attack, if in a given time period only one vehicle changes its pseudonym among more than two vehicles, the attacker can easily link two pseudonyms. Similarly, in a semantic linking attack, the adversary can link different pseudonyms from beacons by predicting the next pseudonym change position of the vehicle.

Therefore, in order to consider the aforementioned issues in ITS, there is a need to develop privacy and security techniques, that not only preserve the real identity during the communication but also authorize only the legitimate vehicles to participate in communication. In this paper, we pro-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

pose a novel framework for ITS, namely Strong Pseudonym based AuthenTicAtion (SPATA) in ITS. The contributions of this paper are as follows:

- A new framework is proposed for pseudonyms generation based on multiple entities interaction. Thus, prior to the pseudonym certificate provided by pseudonym providers, identity to pseudonym and pseudonym to pseudonym mapping is deployed. To achieve unlinkability the mapping function is distributed and it is not possible for a single authority to reveal the real identity of an ITS-S (vehicle).
- A novel protocol is proposed for the revocation of malicious vehicles. It preserves the real identity of vehicles, which is revealed only to vehicle manufacturing company and to law enforcement organization, once the vehicle is found malicious. During the resolution of pseudonyms to a real identity, control anonymity is achieved. The proposed framework of SPATA not only preserve privacy among vehicles but also eliminate the concept of single authoritative behavior from certificate authority.

The rest of the paper is organized as: In section II related work is presented. In section III, the preliminaries of the proposed SPATA framework are discussed. In section IV, SPATA revocation process is presented. Section V consists of performance analysis. In section VI, security analysis is presented, while section VII presents conclusion and future work.

II. RELATED WORK

Due to the ad hoc nature of ITS, there is a problem of end to end connectivity. Therefore, the authentication and integrity of messages must be verified [27]. Onion based routing scheme is not encouraged in ITS due to real time constraints. In ITS, the privacy protection schemes are mainly categorized into Group Signature Based (GSB)/Ring Signature Based (RSB) schemes and Pseudonym Based (PB) approaches. Table 1 shows their comparative analysis.

TABLE 1: Existing ITS privacy schemes performance

Parameters	GSB/ RSB	PB
Scalability	Low	High
Computational cost	Medium	High
Privacy	Low	Medium
Average latency	High	High
Overhead ratio	High	High
Delivery ratio	Medium	Low

In GSB/RSB approaches [28]–[30], vehicles are grouped and authenticity is achieved through the public key certificate. In GSB/RSB approaches, the real identity of a vehicle is hidden from other members of the group through group keys. In these schemes, an individual key of the group/ring is used to sign the message for the group. However, these schemes are not scalable, because group size is limited. The work proposed in [29] allows RSUs to sign and verify messages. However, in order to avoid side channel attacks [23], RSU participation in pseudonym generation is not encouraged. Zhang et al. [30] proposed an approach where the RSUs can be used as a group manager for group management. However, RSUs may be compromised due to its nature of deployment. Revocable ring signature approach is presented by Liu et al. [31] for VANETs security. This scheme provides strong privacy, but it is limited to a particular ring/group and is not scalable. Xiong et al. [32] proposed that privacy of vehicles can be secured conditionally using revocable ring signature, as the CRL needs to be timely distributed among all ITS-Ss. This methodology leads to an increase in overhead as the CRL size grows exponentially.

Most pseudonym based approaches use public key cryptography. The private key is used for message signing, while the corresponding public key is used for signature verification. CA provides pseudonyms along with certificates, and the relationship between the real identity and pseudonym is known to the CA. In [13], the author proposed a generation of bulk pseudonyms and its distribution. The source of message selects any random pseudonym issued by the CA. The message is then signed with the corresponding private key. The message destination verifies the pseudonym through the corresponding public key certificate. Only the CA can map the actual identity if the malicious behavior is detected. In this scheme, CA may be a single point of attack having mapping information of all ITS-Ss (vehicles).

Raya et al. [33] proposed the idea of Tamper Proof Device (TPD) or Hardware Security Module (HSM) in the vehicle OBU. Due to the bulk of pseudonym certificates, the storage and communication overhead increases. The CRL size also grows exponentially to revoke more than a thousand pseudonyms. Similarly, another issue is that the CA should know the vehicle coordinates. The CA can send revocation messages directly to vehicles. In this case, the privacy of a vehicle is also affected. To reduce the size of CRL, Sun et al. [34] suggested the idea of hash chains. However, calculating crypto hashes of CRL may introduce computational overheads. Calandriello et al. [35] and Rajput et al. [36] use a hybrid approach of group signature schemes and pseudonym based schemes. In these approaches, there is an extra overhead of each time a message is checked whether it is from a revoked vehicle or not. Moreover, a common key pair is assigned to each member of the group, which may be compromised. RSUs take part in the generation of pseudonyms for communication and is a single point of attack.

Identity based verification techniques are introduced in [37], [38] in order to secure vehicular communication. These schemes use TPD for generation of pseudonym based identity certificates. These approaches are inefficient when compared with conventional cryptography, and are prone to Denial of Service (DoS) attacks. A conditional privacy preserving protocol is proposed by Lu et al. [39]. This approach demonstrates the idea of short time pseudonym keys that are acquired by the vehicle OBU from RSU. However, RSUs are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

located in open infrastructure and can easily be targeted.

The work proposed in [40] suggests anonymous credentials and Camenisch-Lysyanskaya (CL) signature for beacons authentication. This approach is not efficient due to computational overhead. The work proposed in [41] suggests that for collision avoidance in V2V and V2I there must be linkability between real identity and pseudonym. However, direct linkability between the real identity and pseudonym can jeopardize the privacy of vehicles. Shaub et al. [21] presented an approach to enable the vehicles to obtain anonymous pseudonym certificates through V tokens. Only Registration Authority (RA) can recover the real identity and is a single point of attack. The authors [42] proposed the idea of an intrusion detection system, to prevent ITS from external attacks. However, there is a lack of malicious vehicles revocation and identification, as there exists internal attacks in ITS. The protocol proposed in [43] is useful for non-safety applications because it contains the original identities.

Kamat et al. [44] proposed the approach of a Trusted Authority (TA) that can issue pseudonym certificates to vehicles. TA is the only assigned entity for certificate generation, CRL generation and is only a single point of attack. CRL is stored by base stations, located in nonsecure infrastructure that can be easily compromised. Wang et al. [45] presented a scheme in which Key Management Center (KMC) is introduced instead of CA. The KMC is responsible for the whole communication process. There may be colluding attack as KMC is the single point of attack.

To avoid the problem of long storage requirements, and to store PKI certificates in the vehicle OBU, a scheme presented in [46] suggests a certificate-less public key cryptography (CL-PKC). In the CL-PKC scheme, the key generation center (KGC) helps in generating the private key. However, the scheme incurs a high computational cost with low privacy. As the KGC is the only assigned entity that helps in the generation of the private key, and is exposed to colluding attack. Similarly, another certificate less scheme presented in [47] to reduce the computational cost, but lacks malicious vehicle revocation. Tso et al. [48] presented a certificate-less security model with low computational cost in signature generation. However, the scheme is exposed to active and passive attacks. In addition, there is no proper mechanism for revocation of malicious vehicles. Similarly, Horng et al. [49] presented a good certificate-less approach for V2I communication. However, the scheme [49] considers only V2I communication, and lacks support for malicious vehicle revocation. In addition, RSU can take part in the signature verification process, and is prone to side channel attacks, due to its nature of deployment.

In related work, it has been discussed that trust is not distributed with adequate privacy control. Similarly, there are issues of scalability, computational cost, latency, storage, and communication overhead. In the next section of this paper, we present the SPATA framework, which is a novel framework for distributed pseudonym generation protocol. This is coupled with privacy preserving resolution and revocation mechanism. In SPATA, the accountability of malicious vehicles is also considered, and thus can be revoked with privacy. Hence, privacy of vehicles is maintained efficiently.

III. PRELIMINARIES

In this section, the proposed SPATA framework, inferences, design objectives, security primitives, privacy metrics, SPATA proposed protocol, and the threat model is presented.

A. SPATA FRAMEWORK

Private communication in ITS requires hiding the real identity of ITS-Ss (vehicles). In the SPATA framework, it is not possible for a single entity to reveal the true identity of a vehicle. At the same time, the malicious vehicles should be held accountable for their misbehavior. The SPATA framework is based on pseudonym identities, and certificates in a distributed manner to avoid linkability.

The SPATA framework is composed of:

1) **Vehicular Manufacturing Company (VMC)**: The VMC assigns an initial pseudonym to the vehicle through a secure channel. The VMC is introduced in the proposed framework, to avoid the concept of the single authoritative role of the CA. In the proposed framework, the CA has no information regarding the real identity of the vehicle. In SPATA, the vehicle interacts with the VMC once or in case of ownership changes.
2) **Certification Authority (CA)**: The CA provides Long Term Certificates (LTC) to vehicles, which are successfully verified by the VMC. This has to be done through a secure channel. The lifetime of an LTC is one year, or it can be set by the CA in the timestamp field. In a normal situation, the vehicle interacts for the LTC with the CA once per year, or as set by the CA in the timestamp field.
3) **Long Term Certification Authority (LTCA)**: The LTCA provides a Pseudonym Certificate (PC) to the vehicle after a reliable verification process, through a secure channel. The lifetime of PC in normal situations is six months, or as set by the LTCA in the time stamp field. However, this should be less than the lifetime of the LTC. The vehicle contacts the LTCA for the PC every six months, or as specified by the LTCA in the timestamp field.
4) **Pseudonym Provider (PP)**: The PP or cascaded PPs provides Short time Communication Pseudonyms (SPCs) to the vehicle after a reliable verification process, by using a trustworthy channel. To acquire SPCs for communication, the vehicle frequently interacts with PP.
5) **Source Vehicle**: The originator of beacon/safety message (V_i), signs the beacon with its private key and transmits it. The sign beacon consists of the corresponding public key and SPC.
6) **Receiving Vehicle**: The recipient vehicle (V_j) authenticates the beacon, the signature is verified through

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

the corresponding public key and the SPC. In case of a bogus message, the V_i is reported to PP and LEO for revocation and accountability. If a signature from a beacon is not verified, the recipient vehicle simply discards the beacon.

The validity of SPCs does not depend on the type of vehicle. For all types of vehicles, the validity of SPCs range from 20 milliseconds to 60 milliseconds. If a vehicle is found malicious, SPCs cannot be issued and the vehicle can no longer participate in the communication. Furthermore, PP revokes all the issued SPCs of that particular vehicle. Only in the case of a malicious activity, the real identity can be revealed by the LEO of that particular country. If ownership of a vehicle changes, all the certificates need to be revoked. This revocation leads to unavailability of pseudonyms communication prior and afterwards. The new owner of the vehicle needs to repeat the steps from VMC to PP as shown in Figure 3, detailed in Section III-F.

B. INFERENCES

We assume that VMC discloses the real identity of the vehicle, to the Law Enforcement Organization (LEO) only on the basis of malicious activities. All the service providing authorities should have secure and reliable communication. In case if any PP is compromised, it will be isolated. A vehicle requests pseudonyms from VMC, CA, LTCA, and PP, through RSU or directly using 3G/4G/5G communication. In the proposed framework, RSU acts as a router between V2X communications. The RSU does not take part in the generation or verification of long or short time pseudonym certificates, in order to avoid the side channel attacks.

There will be several PPs to provide unlinkability by the attacker. As different pseudonyms are provided by different pseudonym providers. All the parties' clocks in the SPATA framework are synchronized to meet the essence of the ITS, as there are timestamps in the pseudonymous communication.

C. DESIGN OBJECTIVES

The proposed SPATA framework design objectives are as following:

- **Confidentiality and authentication**: All the communication should be encrypted. Authentication and authorization of a legitimate vehicle will be performed without revealing its true identity. The source vehicle and its beacon will be authenticated without revealing its true identity to the receiving vehicle.
- **Integrity of messages**: In case of alteration in beacons, the signature will not be verified. Then, unverified beacons will be rejected and discarded.
- **Non-repudiation**: Once a message is verified, it confirms the claim of source vehicle. A source vehicle then cannot deny the communication.
- **Revocation**: Once, a pseudonym or vehicle is revoked, it should not take part in the ITS network.
- **Restrictive obscurity**: The proposed framework is rendering restrictive obscurity. A vehicle that follows SPATA rules will have its privacy preserved. The true identity of a vehicle can be revealed, only in case of malicious behavior.

D. SECURITY PRIMITIVES

SPATA uses a combination of asymmetric and symmetric cryptographic schemes. Symmetric Key Cryptography (SKC) operations are faster than Asymmetric Key Cryptography (AKC) [50]. However, alone SKC does not provide the feature of non-repudiation. Therefore, we combine both techniques to enhance security and privacy performance. For asymmetric cryptography, Rivest, Shamir, and Adelman (RSA) scheme is used. While for the symmetric key system, Advanced Encryption Standard (AES) technique is used. The vehicle OBU generates a key pair of public and private keys. The private key is used for signature generation, while the public key is sent along with the beacon for verification of the signature at the receiving end. The key pairs are generated according to the following rules:

- Two random prime numbers are generated that is a and b, n is computed, where n is the product of a and b.

$$n = (a)(b) \tag{1}$$

- Public key (pb) is calculated such that Greatest Common Divisor (GCD) between pb and totient function $(\varphi(n))$ is 1.

$$GCD(pb, \varphi(n)) = 1 \tag{2}$$

Where,

$$\varphi(n) = (a-1)(b-1) \tag{3}$$

- Private key (pr) is calculated such that:

$$(pb)(pr) \equiv 1 mod(\varphi(n)) \tag{4}$$

Where the property of congruence is satisfied through the following equation:

$$((pb)(pr)) - 1) mod \varphi(n) = 0 \tag{5}$$

Public key is $\{pb,n\}$ and private key is $\{pr,n\}$. For AES we use 128 bits (16 bytes) data block and 128 bits symmetric key. When the message is larger than 128 bits, the Cipher Block Chaining (CBC) method is used [51]. Therefore, we break the message block into smaller blocks of 128 bits. If a data block size is less than 128 bits, padding is used, so that the size of the data block becomes 128 bits. A random number N, that is exclusive OR (XOR) with the first data block. Similarly, for the next plaintext block, the previous ciphertext block acts as a random number. The SPATA, CBC operation is shown in Figure 2. After ITS-S (server/vehicle) receives the secure message, it will be verified.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

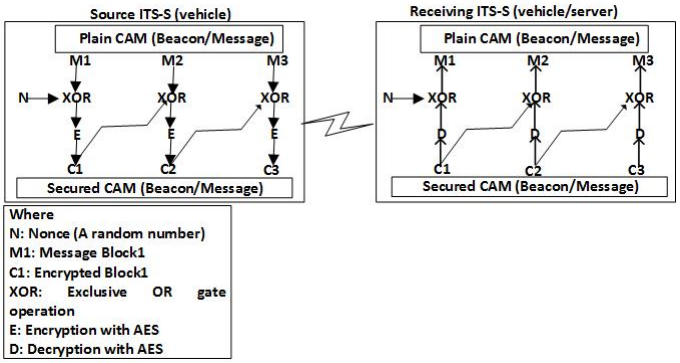


FIGURE 2: SPATA, CBC Operation

E. PRIVACY METRICS

A good security and privacy approach should provide a high degree of anonymity. In order to assess the privacy level through pseudonyms, a range of metrics is suggested. We discuss the following most considered metrics:

- **Anonymity Set Size**: In ITS, Anonymity Set (AS) is the set of vehicles that are identical with the target itself [52]. The AS size is the number of vehicles included in the anonymity set. The size of AS corresponds with the protection of privacy achieved, and in this case should be larger than one. However, this metric expects that all vehicles are fairly being the target. Therefore, the AS metric as debated in [53] cannot be used to describe what and how many vehicles can be targeted by the adversary. Therefore, entropy is proposed instead of AS [53].
- **Entropy of AS Size**: Entropy expresses distrust in a random variable. The entropy concept comes from information theory that provides uncertainty of a random variable. In case of ITS, random variable is the number of vehicles.

  Let N be a random variable with a probability such that:

$$y_j = p_{rob}(n = j) \tag{6}$$

  Where j defines a possible number that N can consider with probability $y_j > 0$. Each j corresponds to the AS i.e. y_j is the probability of the content that is linked to vehicles. However, using the following expression, entropy can be calculated [11] as:

$$H(N) = -\sum_{j=1}^{|AS|} y_j Log_2(y_j) \tag{7}$$

  In the above expression y_j is the probability of a vehicle, j being the target. If the probability of the target/attack vehicle is the same for all vehicles, there is a uniform distribution of the probabilities on the AS. The maximum value of entropy is then achieved by the following expression:

$$\forall_j : y_j = \frac{1}{|AS|}, H_{max} = -\sum_{j=1}^{|AS|} y_j Log_2(y_j) = Log_2|AS| \tag{8}$$

  For example, if there are 25 vehicles and we assume that all vehicles have the same probability to attack, then y_j=1/25 so (y_j=0.04) and the entropy is 4.64. A large value of entropy shows higher AS size, as the number of vehicles increases the entropy will increase.
- **Anonymity Level**: It is supposed that if the attacker has no past information of the vehicles anonymity set. The attacked information can be measured through the following difference: $(H_{max} - H(N))$. Where $H(N)$ is the effective anonymity set size and H_{max} is the maximum entropy. Diaz [11] suggested d as the level of anonymity which is a normalized quantity in the range of [0,1] and the anonymity level is then measured by the following expression:

$$d = 1 - \frac{H_{max} - H(N)}{H_{max}} = \frac{H(N)}{H_{max}} \tag{9}$$

In the proposed framework of SPATA, we try to maintain a high degree of anonymity, through a distributed framework.

F. SPATA PROPOSED PROTOCOL

ITS-S (vehicle) is pre-loaded with a secret key issued by the VMC, further, it requests an LTC from CA. The CA checks the identity of the vehicle in CRL, if it is not found then Algorithm 1 is executed. The SPATA framework is shown in Figure 3, while the notations used in the proposed protocol are shown in Table 2.

Algorithm 1 SPATA Process

1: V → VMC: $K_{VVMC}[ID_{VMC} \parallel \text{N} \parallel ID_V]$
2: VMC→ V: K_{VVMC}[P1 $\parallel ID_{VMC} \parallel ID_{CA} \parallel$N$\parallel K_V]$
3: V→ CA: $Pk_{CA}[P_1 \parallel ID_{VMC} \parallel K_V]$
4: CA→VMC: $Pk_{VMC}[P_1 \| ID_{VMC} \| K_V]$
5: VMC → CA: Pk_{CA}[ok or decline] if ok then
6: CA→V: $K_V[Sk_1 \| P_2 \| TS_1 \| LT_1 \| ID_{LTCA} \| Token_{LTCA}]$
7: CA→LTCA: $Pk_{LTCA}[P_2 \| SK_1 \| TS_1 \| LT_1 \| ID_{LTCA}]$ or $Token_{LTCA}$
8: V→LTCA: $Sk_1[P_2 \| ID_{LTCA} \| Token_{LTCA}]$ where $Token_{LTCA}$: $K_{LTCA}[P_2 \| ID_{LTCA} \| TS_1 \| LT_1]$
9: LTCA→V: $Sk_1[P_3 \| Sk_2 \| LT_2 \| TS_2 \| Token_{PP} \| ID_{PP}]$
10: LTCA→PP: $Pk_{PP}[P_3 \| Sk_2 \| ID_{PP} \| TS_2 \| LT_2]$ / $Token_{PP}$
11: V→PP: $Sk_2[P_3 \| ID_{PP} \| Token_{PP}]$ where $Token_{PP}$: $K_{PP}[P_3 \| ID_{PP} \| TS_2 \| LT_2]$
12: PP→V: $Sk_2[P_4 \| P_5 \| P_6 \| P_7 \| TS_3 \| LT_3]$

The SPATA protocol shows that:

- Step 1: The vehicle requests the VMC for initial pseudonym using a secure channel.
- Step 2: The VMC issues an initial pseudonym to the vehicle through a secure channel.
- Step 3: The vehicle requests CA for LTC, using a secure channel.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

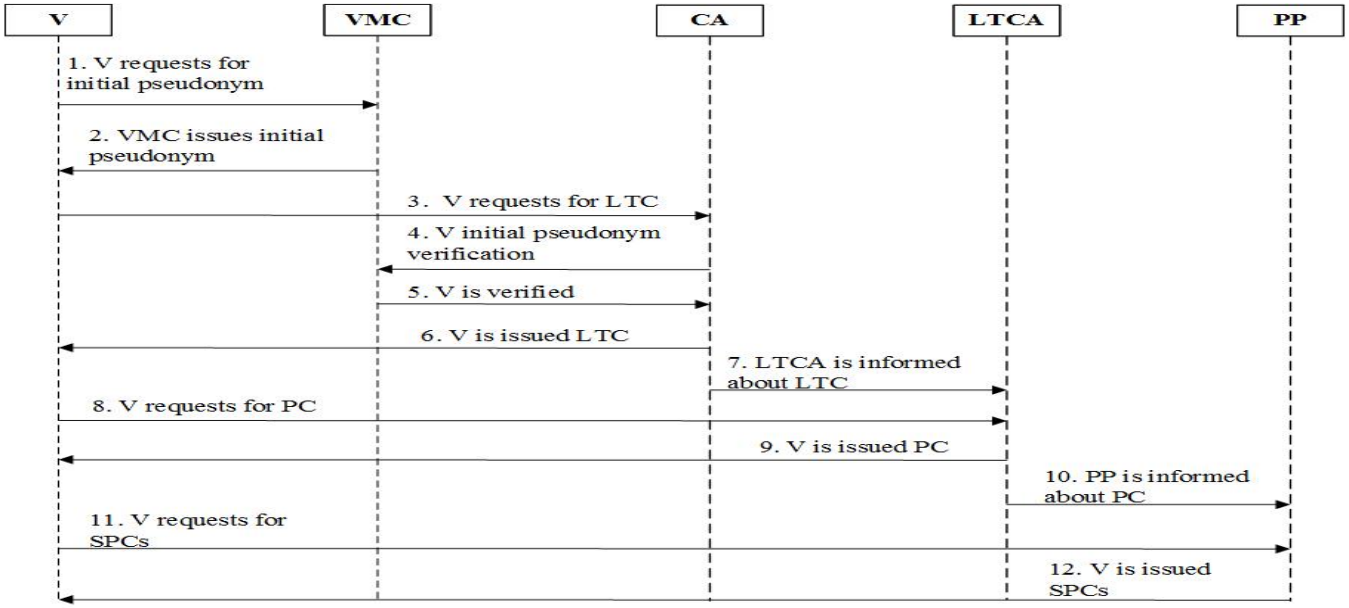


FIGURE 3: SPATA Framework

TABLE 2: Description of notations used in SPATA

Notations	Description
V	ITS-S (vehicle)
PP	Short Time Pseudonym Provider for vehicular communication
S_k	Session key
K_{VVMC}	Secret key shared by V and VMC
V_i	Source vehicle
V_j	Receiving/affected vehicle
SPCs	Short Time Pseudonyms
P_1	Pseudonym 1
P_2	Pseudonym 2
P_3	Pseudonym 3
Pk_{LTCA}	Public key of LTCA
Sk_1	Session key for V and LTCA
Sk_2	Session key for V and PP
K_V	Secret session key for CA and V
Pk_{VMC}	Public Key of VMC
Pk_{CA}	Public Key of CA
Pk_{PP}	Public Key of PP
LT	Life Time of pseudonym
TS	Time Stamp
$\|\|$	Concatination
N	Nonce a random number
Token	Only for the authorized vehicle / server
K_{LTCA}	Secret key shared by CA and LTCA
K_{PP}	Secret key shared by LTCA and PP
K_{Vi}	Secret key of V_i
Pk_{Vi}	Public key of V_i
/	or

- Step 4: The CA verifies the vehicle from the VMC, using a secure channel.
- Step 5: The VMC verifies or declines the vehicle.
- Step 6: The CA issues LTC to the vehicle, after a successful verification from the VMC. If CA finds a vehicle that is malicious, it will be reported to LEO for further accountability.
- Step 7: The CA informs the LTCA about the LTC of the vehicle through a secure channel.
- Step 8: The vehicle requests LTCA for PC, through a secure channel. The LTCA verifies the vehicle credentials through matching tokens as forwarded by the CA and also provided by the vehicle.
- Step 9: The LTCA issues a long term certificate as PC to the vehicle, through a secure channel.
- Step 10: The LTCA informs PP or cascaded PP about the PC of the vehicle, through a secure channel.
- Step 11: The vehicle requests PP for SPCs, on the basis of the PC through a secure channel.
- Step 12: The PP after verification issues SPCs to the vehicle for communication among V2X, through a secure channel.

The pseudo code of a vehicle registration in the SPATA framework is shown in Algorithm 2. Once the vehicle obtains SPCs from PP or cascaded PPs, that vehicle can communicate with other ITS-Ss (vehicles) and RSUs through SPCs as shown in Figure 4. In case of bogus beacons from the source vehicle (V_i), V_i can be reported to LEO for revocation. The vehicle revocation process is presented in the next section of this paper.

G. THREAT MODEL

Different types of attacks are considered in the threat model. The insider or internal attacker cannot obtain the real identity of a vehicle from the CA, LTCA or PP. This is because the initial pseudonym is provided by VMC through a secure channel. Similarly, the VMC cannot obtain the real identity of a vehicle during communication, as CA, LTCA, and PP provide communication pseudonyms.

The external attacker role is limited in the SPATA frame-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

Algorithm 2 SPATA Vehicle Registration

```
if V requests CA then
    V is cross checked with VMC
    V is authorized by VMC
end if
if V is authenticated then
    CA issues LTC to V
    V requests LTCA for PC
end if
if V is authenticated then
    LTCA issues PC
    V requests PP for SPCs
end if
if V is authenticated then
    PP issues SPCs for communication
end if
```

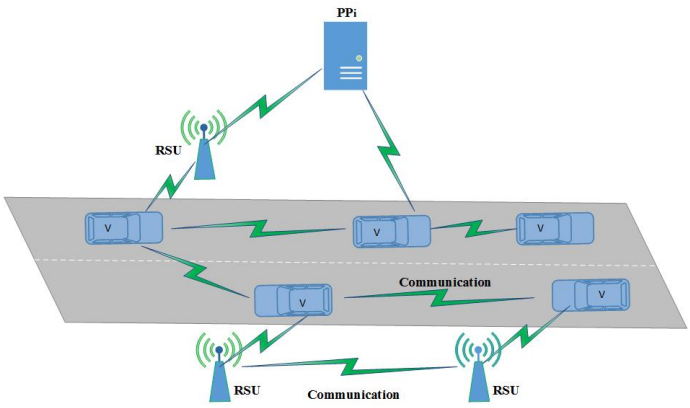


FIGURE 4: SPATA, communication scenario

work, as all the communication is pseudonymized and encrypted. Similarly, the role of passive and active attackers are limited in the SPATA framework, because all communication is encrypted, and in case of injecting bogus beacons or alteration in the beacons, the signature cannot be verified.

Theorem: The SPATA framework is semantically secured against passive and active attacks. Proof: Let an attacker get a secure message during the communication between a vehicle and a server. The attacker has to try 2^n (where n is the key size). As the key size in the proposed framework of SPATA is 128 bits, so the attacker needs to try 2^{128} (3.4×10^{38}) keys to find the actual key. In the worst case scenario, if an attacker has a very powerful computer, which can calculate 10^6 decryptions per microsecond, the total time needed is 5.4×10^{18} years that is impractical for an attacker in ITS.

Without the key, it is impossible for an attacker to know the communication. Besides, the key, the nonce N is also used in the SPATA framework that further enhances the security of messages. Therefore, an attacker has to know both the key and the nonce that is impossible in the proposed framework of SPATA, due to the strong SKC, AKC techniques, and the distributed mechanism.

Similarly, if an attacker gets a secure message and tries to alter the beacon contents or insert a bogus beacon, the signature cannot be verified, and unverified messages are simply discarded. To launch an active attack, the attacker needs to generate the key pairs in a real time. However, without prior knowledge of a and b as discussed in Section III-D, it is impossible to generate the key pairs, which eliminates the concept of active attacks. The proposed framework of SPATA uses strong security and privacy measures between the vehicles and service providers, and this provides a high degree of anonymity.

To evaluate the proposed theorem, we use entropy. Entropy shows the amount of secure information in a message to be sent across the network and is expressed in terms of a discrete set of probabilities p_i, such that:

$$H(X) = -\sum_{i=1}^{n} p(x_i) log_2\ p(x_i) \tag{10}$$

And:

$$H_{max} = log_2|n| \tag{11}$$

Further to evaluate the probabilities, the Shannon entropy equation provides a way to estimate the average minimum number of bits needed to encode a string of symbols, based on the frequency of the symbols. The average minimum number of bits per symbol is $numBits$=$[H(X)]$ where, $H(X)$ shows the secure information.

A large value of entropy shows that the information being transmitted is highly secure. Therefore, it is impractical for an attacker to launch passive or active attacks. In order to provide a higher degree of security and privacy, information theory suggests that for the neighboring vehicles, the local neighborhood probabilities are as follows:

$$\Omega(x,y) = \{(x+1,y),(x-1,y),(x,y+1),(x,y-1)\} \tag{12}$$

where, x and y are the coordinates of the communicating vehicles.

The probabilities related to the total weights of the private keys of the vehicles are as follows:

$$Z(x,y) = \sum_{(i,j)\varepsilon\Omega(x,y)} H(X) \times W((x,y),(i,j)) \tag{13}$$

The normal values of the key security at an iteration $t+1$ is given by the weighted average of its neighboring normal values at previous iteration t:

$$n^{(t+1)}(x,y) = \frac{\mu^{(t+1)}(x,y)}{|\mu^{(t+1)}(x,y)|^2} \tag{14}$$

where,

$$\mu^{(t+1)}(x,y) = \sum_{(i,j)\varepsilon\Omega(x,y)} n^t(i,j)\frac{W((x,y),(i,j))}{Z(x,y)} \tag{15}$$

The security primitives used in the proposed framework of SPATA guarantee a higher degree of anonymity i.e.:

$$d = \frac{H(X)}{H_{max}} \tag{16}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

where $H(X)$ is the amount of information being secured and H_{max} is the maximum entropy. Therefore, d shows the degree of secured information in the communication system. Hence, honest vehicles can communicate freely with a higher degree of security and privacy, that guarantee full trust on the SPATA framework.

IV. REVOCATION IN SPATA

The SPATA revocation and resolution process of a malicious vehicle is shown in Figure 5. It has the following steps:

- **Step 1**: The affected vehicle V_j (receiving vehicle of spurious beacons) informs PP to revoke the SPCs of the malicious vehicle (V_i). The PP revokes the SPCs of V_i through broadcasting. Revoked SPCs then cannot be verified and thus other honest vehicles cannot be attacked.
- **Step 2**: The affected vehicle informs LEO for the revocation of the malicious vehicle (V_i) from ITS network and accountability.
- **Step 3**: LEO asks CA for revocation of V_i and real identity mapping.
- **Step 4**: CA informs PP not to issue more SPCs. The CA also directs PP or cascaded PP to send the pseudonym information of V_i to LTCA.
- **Step 5**: CA revokes LTC. The CA informs LTCA to revoke the PC of V_i and reports back after PP replies.
- **Step 6**: PP sends the pseudonym information to LTCA.
- **Step 7**: LTCA sends the pseudonym information to CA after revoking the PC of V_i.
- **Step 8**: CA forwards the pseudonym information of V_i to LEO.
- **Step 9**: LEO sends the information to VMC for the real identity mapping.

In this way, the real identity of V_i can be revealed. The LEO can take action as per the laws of that particular country. The protocol steps are subsequently elaborated in Algorithm 3.

Algorithm 3 SPATA Revocation and Resolution

1: Vj → PP: [(beacon message)K_{Vi} || Pk_{Vi} || Pseudonym]
2: Vj → LEO: [(beacon message)K_{Vi} || Pk_{Vi} || Pseudonym]
3: LEO → CA: [(beacon message)K_{Vi} || Pk_{Vi} || Pseudonym]
4: CA→PP: Pk_{PP}[(beacon message)K_{Vi} || Pk_{Vi} || Pseudonym]
5: CA→LTCA: Pk_{LTCA}[(beacon message)K_{Vi} || Pk_{Vi} || Pseudonym]
6: PP→LTCA: $Pk_{LTCA}[P_3]$
7: LTCA→CA: $Pk_{CA}[P_2]$
8: CA→LEO: $[P_1]$
9: LEO→VMC: $[P_1]$

The beacons consist of pseudonyms and are stored for a short period of time. The beacon contents are verified quickly through the public key and pseudonyms. The beacons are signed by the private key of the vehicle (V_i). The corresponding public key of V_i is attached with the beacon. In the SPATA framework, the vehicle cannot deny communication as it is signed through the vehicle's private key. The pseudonyms as provided by PP are attached with beacon messages to ensure integrity and non-repudiation. The pseudo code of the SPATA revocation and identity mapping process is shown in Algorithm 4.

In SPATA, the CRL size does not grow exponentially as recent communication pseudonyms of the malicious vehicle are revoked and broadcasted. Thus revoked pseudonyms cannot be verified.

Algorithm 4 SPATA Revocation and Identity Mapping

1: **if** Vj reports to LEO **then**
2: F Vj reports to PP
3: PP revokes the valid SPCs of Vi
4: LEO requests CA for mapping the factual identity of Vi
5: CA revokes LTC and LTCA revokes PC
6: PP sends the available information of Vi to LTCA
7: LTCA sends the available information to CA
8: CA reports back to LEO regarding Vi
9: LEO requests VMC to reveal the original identity of Vi
10: **end if**

V. PERFORMANCE ANALYSIS

The SPATA framework has been evaluated using Opportunistic Network Environment (ONE) simulator [54]. The system used for evaluation of the SPATA framework is a core i7 laptop with 8 GB RAM. The experiments were executed 200 times. The speed of vehicles was kept variable to accurately evaluate the behavior of SPATA framework. The real map of Helsinki city was used with random way point model. The simulation parameters that were used during the experiments are shown in Table 3.

TABLE 3: Parameter Guidelines for SPATA Modeling

Parameter name	Description
Duration	3600 seconds
Interface type	Simple broadcast interface IEEE 802.11P
Transmit speed	10 Mbps
Number of PP	1
Number of vehicles	5 - 100
Slow speed range	10 km/h to 50 km/h
Medium speed range	51 km/h to 80 km/h
High speed range	81 km/h to 120 km/h
Mobility model	Map based mobility
Routing protocol	Epidemic(EP)
Routing protocol	Spary and Wait(SW)
Map of city	Helsinki
Transmit range	1000 meters
Area	10 km^2

Epidemic (EP) and Spray and Wait (SW) [55] as underlying routing protocols have been used in the simulations. The primary goal of EP and SW routing is to render beacons with high probability even in the intermittent communication channel. The EP routing incurs high overhead due to its flooding nature. In SPATA, the vehicle periodically sends beacon messages to other vehicles. The SW routing nature is not an inundation. There is a number associated with the new beacon showing the limit of admissible copies. The two routing protocols are considered during simulations to perfectly analyze the behavior of the SPATA framework. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

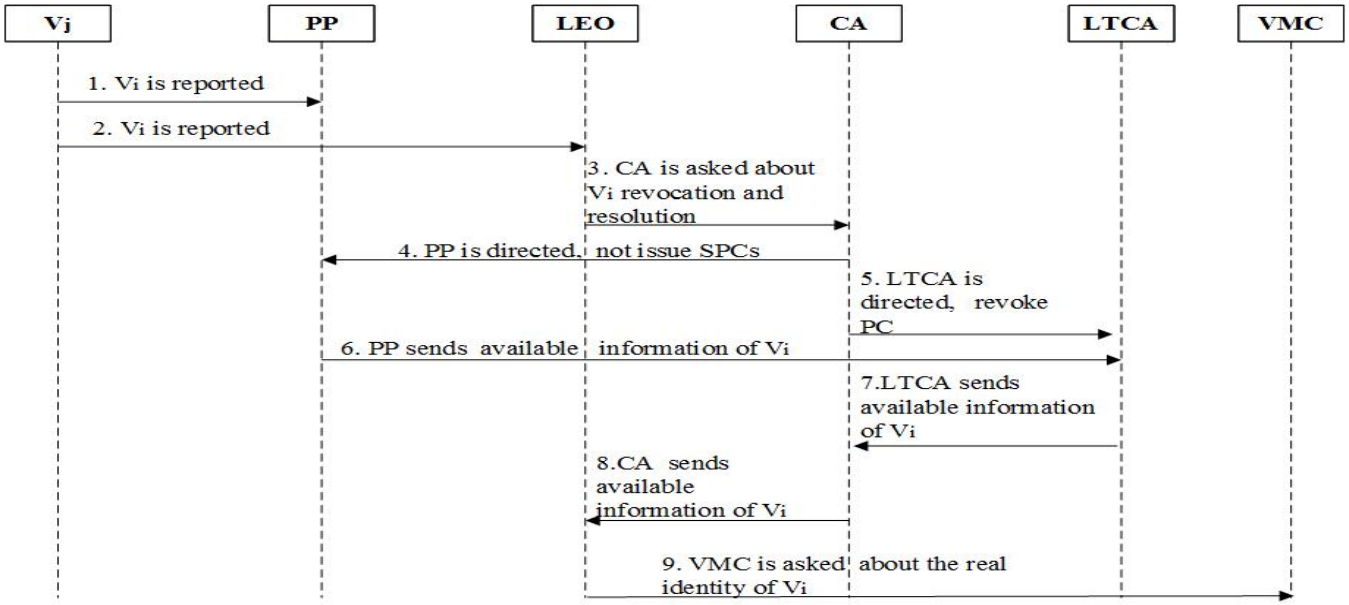


FIGURE 5: SPATA Revocation and Resolution Process of Malicious Vehicle

following network performance parameters are considered for analyzing the performance of the SPATA framework.

- Average latency = Average (Message delivered time – Message created time)
- Overhead ratio = (Relayed messages – Delivered messages) / Delivered messages
- Delivery ratio = Delivered messages / Relayed messages

A. AVERAGE LATENCY

It is required to show the effect of the SPATA framework on average latency in sparse and dense scenarios with different speeds. The results obtained during the simulations are shown in Figure 6. The results show that there is no significant difference between SPATA and without SPATA scenarios. We noticed similar trends in sparse and dense scenarios with both forms of beacons. The reason for the increase in the average latency in Figure 6 (a), is due to slow speed vehicles are moving slowly and become congested. Therefore, the number of beacons received are more and more bandwidth is occupied. The average latency is less than 1 milliseconds in both cases of encrypted (with SPATA) and unencrypted (without SPATA) beacons. The average latency is 0.9 milliseconds only in that scenario where the number of vehicles is less (up to 30 vehicles). In summary, deployment of SPATA in a sparse network leads to an increase in latency while in the dense network the latency is either stable or decreasing. Moreover, the extra layer of security and privacy does not hinder communication.

B. OVERHEAD RATIO

The results shown in Figure 7 depict similar trends in case of with and without SPATA implementation. The results carried both encrypted and plain text form of beacons for sparse and dense network scenarios. We noticed that overhead ratio/communication overhead is high only in those scenarios where vehicles received more beacons. The reason is a minimum gap among vehicles and sense more collision. The maximum overhead is less than 2% in all type of scenarios between with and without SPATA, that is negligible as a tradeoff with privacy and security.

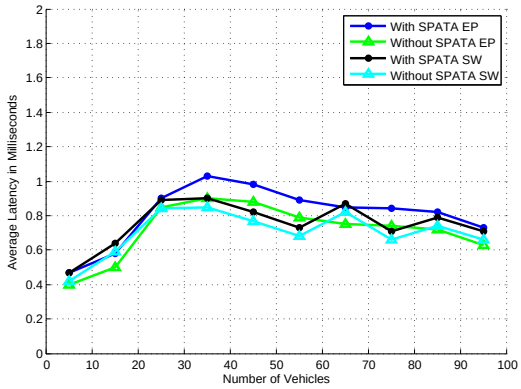
C. DELIVERY RATIO

The delivery ratio is another parameter to show the suitability of SPATA. The results retrieved during simulations as shown in Figure 8 reflects no decrease in the delivery ratio with the deployment of SPATA. The delivery ratio is increasing in sparse as well as in dense scenarios. However, in the case of slow speed vehicles, the delivery ratio is decreasing after the number of vehicles reach 85. This is because slow speed vehicles become closer and receive more beacons. More beacons require more bandwidth and start to drop beacons. While in Figure 8 (b) and Figure 8 (c) the delivery ratio is increasing or stable with increasing number of vehicles. The reason is that distances between vehicles are increasing and occupy less bandwidth. Thus the cryptographic primitives used in the SPATA framework do not affect the messages delivery ratio.

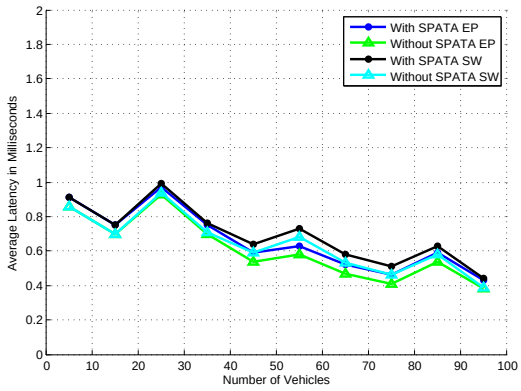
D. COMPUTATIONAL COST ANALYSIS

The computational cost of SPATA has been evaluated as shown in Table 4. The total time taken in the generation of the beacon, including signature is 3.70 milliseconds. The beacon verification time is 0.58 milliseconds. The vehicle can easily and efficiently generate and verify a large number of beacons simultaneously. The average values for vehicle LTC and PC

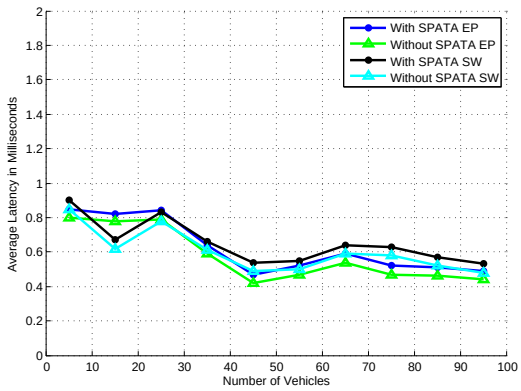
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access



(a) Slow speed

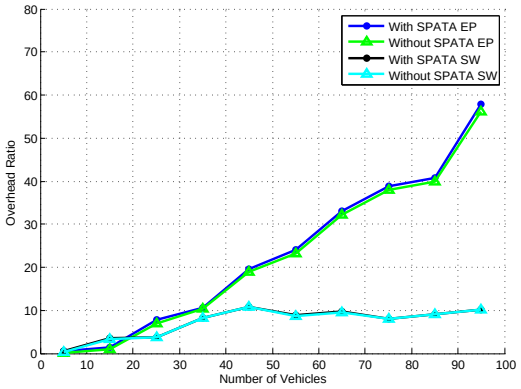


(b) Medium speed

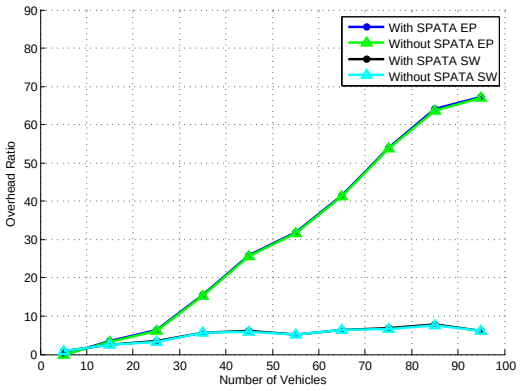


(c) High speed

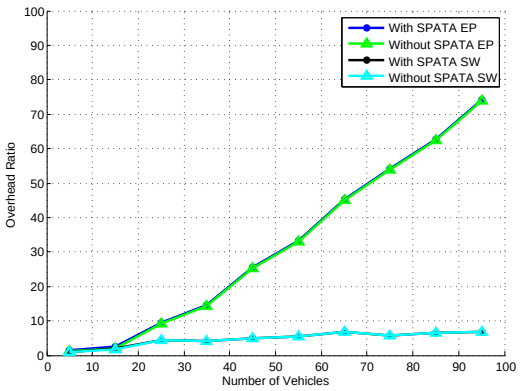
FIGURE 6: Average latency



(a) Slow speed



(b) Medium speed



(c) High speed

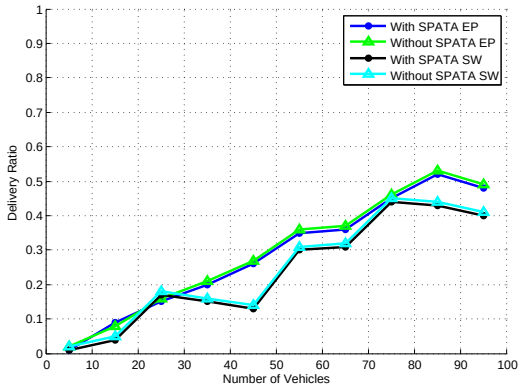
FIGURE 7: Overhead ratio

registration are 4 milliseconds respectively. While for SPCs the average time taken is 5 milliseconds. The time required to generate and verify beacon message is less than 5 milliseconds. Therefore, the lightweight implementation framework of SPATA allows certificate authorities and service providers to process a large number of requests efficiently.

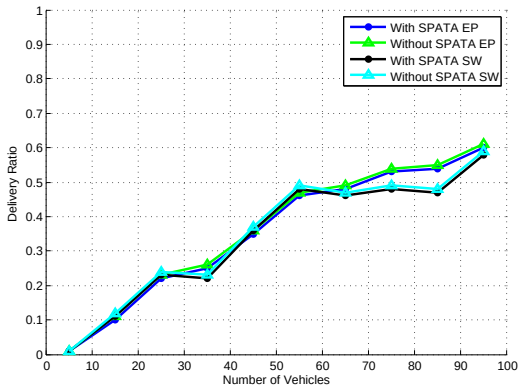
E. MESSAGE SIZES ANALYSIS

The security primitives used in pseudonym generation and revocation with their field sizes are listed in Table 5. The message sizes in the SPATA framework between vehicle and authorities during the registration phase are: In step 1, the total size of the message is 112 bytes. In step 2, the message size is 144 bytes. In step 3, the total size of the message is 80 bytes. In step 4, the message size is 80 bytes. In step 5, the total size of the message is 2 bytes. In step 6, the message size is 180 bytes. In step 7, the message size is 90 bytes. In step 8, the message size is 154 bytes. In step 9, the message size is 180 bytes. In step 10, the total size of the message is 90 bytes. In step 11, the message size is 154 bytes. In step 12, the message size can be up to 74 bytes per second, as communication pseudonyms are changing frequently.

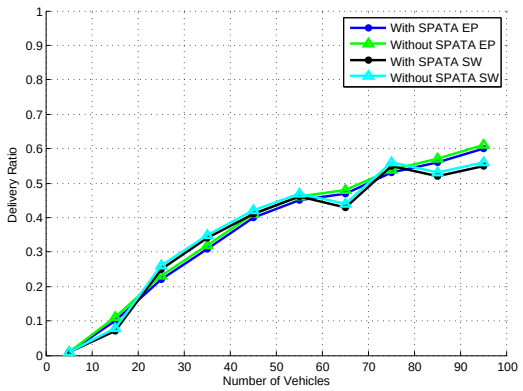
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access



(a) Slow speed



(b) Medium speed



(c) High speed

FIGURE 8: Delivery ratio

The message sizes in the SPATA framework between vehicle and authorities for revocation and real identity mapping are: In step 1, the total message size is 100 bytes. In step 2, the message size is 100 bytes. Step 3, the message size is 100 bytes. In step 4, the message size is 100 bytes. Step 5, the message size is 100 bytes. Step 6, the total message size is 16 bytes. Step 7, the message size is 16 bytes. Step 8 and step 9 the total message sizes are 16 bytes respectively.

From the results, it can be concluded that there are no substantial differences in scenarios with SPATA and without SPATA. This shows the literal setup and ideal point of the

TABLE 4: SPATA computational cost in milliseconds

SPATA	Average computational time (ms)	Standard deviation (ms)
Message encryption	0.18	0.03
Signature generation	3.52	0.13
Message decryption	0.21	0.03
Signature verification	0.37	0.13

TABLE 5: Individual Field Size of SPATA

Field name	Size in bytes
ID_{VMC}	48
N	16
ID_V	48
P_1	16
K_V	16
Sk_1	16
TS_1	5
LT_1	5
ID_{LTCA}	48
ID_{PP}	48
Beacon message	34
Signature	34
Pk_{Vi}	16
Pseudonym	16

SPATA performance. In order to further check the adaptability of SPATA, we implemented SPATA in sparse and dense scenarios. We also checked the SPATA framework using slow, medium, and high speed scenarios. In all scenarios, we found no significant change with or without SPATA. SPATA is a lightweight approach and does not require to maintain a long pool of pseudonymous chatty communication.

F. COMPARISON WITH LITERATURE

In this subsection, a comparison of SPATA with existing GSB/RSB and PB schemes is presented. In SPATA, there is no need to maintain a long pool of on-board pseudonyms and large size of CRL. Once a malicious vehicle is revoked, it cannot take part in communication. There is no need for large storage in the OBU of the vehicle.

There are multiple authorities and even CA, LTCA, and PP have no information about the real identity of the vehicle. In SPATA, if any of the CA, LTCA or PP servers are compromised, the real identity of the vehicle cannot be revealed due to distributed mapping. A comparison of SPATA with existing schemes is presented in Table 6 and 7, respectively. The computational and communication overheads of SPATA are negligible, making it scalable. On the basis of results, it can be concluded that the SPATA framework is an efficient, distributed, secure, and robust framework.

VI. SECURITY ANALYSIS

This section analyzes security and privacy services in the SPATA framework. Further, various threat scenarios are discussed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

TABLE 6: SPATA Comparison with Existing ITS Privacy Schemes

Parameters	GSB/ RSB	PB	SPATA
Scalability	Low	High	High
Computational cost	Medium	High	Low
Privacy	Low	Medium	High
Average latency	High	High	Low
Overhead ratio	High	High	Low
Delivery ratio	Medium	Low	High

A. SECURITY AND PRIVACY SERVICES

The proposed SPATA framework is trustworthy and lightweight with conditional anonymity. There is no single authority that can reveal the real identity of the vehicle. The SPATA framework offers the following security and privacy services:

1) **Confidentiality**: Vehicle acquires its pseudonyms in a secure manner. Thus only the service providers have access to the respective mapping data but not full mapping. Here, a combination of symmetric and asymmetric encryption is used for robustness and security.
2) **Anonymity**: Vehicle uses restrictive obscurity through pseudonymized identity for communication, after registration with VMC. This pseudonymized identity provides anonymous communication among ITS-Ss (vehicles) and service providers. The real identity of the vehicle is preserved in a controlled way.
3) **Integrity**: The communication is controlled and monitored by trusted authorities that are VMC, CA, LTCA, and PP. In case of any alteration in beacons, the signature can not be verified.
4) **Authentication**: Vehicle achieves anonymous authentication by verifying the beacons without revealing source vehicle real identity.
5) **Non-repudiation**: The communication consists of messages along with signature and pseudonyms. If a vehicle is found malicious, the vehicle cannot deny the communication. As the beacons consist of pseudonyms provided by the authorities.

B. THREAT SCENARIOS

In order to achieve maximum conditional anonymity and privacy, the following different types of threat scenarios are considered in the SPATA framework.

1) All the communication between vehicles and the authorities are encrypted. Therefore, it is impossible for an adversary to eavesdrop on the communication.
2) It is impossible for an attacker to get SPCsâĂŹ without PC. Similarly, it is impossible for an adversary, to obtain the PC without LTC. It is also impractical for an adversary to obtain the LTC without the authorization of VMC.
3) If the PP is compromised the attacker cannot obtain any useful information regarding the real identity of the vehicle. The PP contains only the PC information that is pseudonymized and encrypted.
4) If the LTCA is compromised the attacker cannot obtain any useful information regarding the real identity of the vehicle. The LTCA contains the LTC information that is pseudonymized and encrypted.
5) Similarly, the CA database contains encrypted and pseudonymized information. In case, if the CA database is compromised, no useful information can be leaked.
6) Once a vehicle is registered in the SPATA framework, the attacker cannot get any useful information regarding the real identity of a vehicle, in case if the VMC database is compromised. The vehicle is using pseudonymized communication among V2X and all the information in the VMC is encrypted.
7) In case, if an attacker tries to modify a beacon or inject bogus beacon. The signature cannot be verified.

VII. CONCLUSION AND FUTURE WORK

Privacy and security are always a deep concern in ITS, because of its loosely coupled network topology. In the proposed SPATA framework, the pseudonym generation involves multiple certificate authorities to avoid linkability between the real identity and pseudonym. In the revocation phase, privacy of a vehicle is preserved even from the service providers and certificate authorities. The results show a stable decrease in the average latency, overhead ratio, and increase in the delivery ratio for various scenarios and speeds. The computational cost of all cryptographic primitives implemented in the SPATA framework are negligible and do not hinder the communication efficiency. In future, we will use other security techniques for the implementation of the SPATA framework. We will try to make SPATA more robust by further reducing the computational overhead, which enable it to work efficiently in more complex scenarios with large number of vehicles.

REFERENCES

[1] Q. E. Ali, N. Ahmad, A. Malik, G. Ali, W. Rehman, et al., "Issues, challenges, and research opportunities in intelligent transport system for security and privacy," Applied Sciences, vol. 8, no. 10, p. 1964, 2018.
[2] C. Bila, F. Sivrikaya, M. A. Khan, and S. Albayrak, "Vehicles of the future: A survey of research on safety issues," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 5, pp. 1046–1065, 2017.
[3] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for vanet," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, pp. 643–650, IEEE, 2015.
[4] DSRC, "Intelligent transportation systems," Nov. 19, 2016.
[5] T. ETSI, "Etsi ts 103 097 v1. 1.1-intelligent transport systems (its); security; security header and certificate formats," Standard, TC ITS, 2013.
[6] D. Committee et al., "Dedicated short range communications (dsrc) message set dictionary," SAE Standard J, vol. 2735, p. 2015, 2009.
[7] E. ETSI, "302 665 v1. 1.1: Intelligent transport systems (its)," Communications architecture, 2010.
[8] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228–255, 2015.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

TABLE 7: The Comparison on Computational Cost, Communication Overhead, Storage Requirements, Group Management, and Security Attacks in ITS

Research Papers	Computational Cost	Communication Overhead	Storage Requirements	Group Management	Replay Attack	Sybil Attack	Side channel Attack
[13]	High	High	High	No	Yes	Yes	No
[21]	High	High	High	No	No	Yes	No
[29]	Medium	Medium	Medium	Yes	Yes	No	Yes
[30]	Medium	High	Medium	Yes	Yes	No	Yes
[33]	High	High	High	No	Yes	Yes	No
[35]	High	High	High	No	Yes	Yes	Yes
[36]	High	High	High	No	Yes	Yes	Yes
[39]	Low	High	High	No	No	Yes	Yes
[44]	High	High	High	No	Yes	Yes	Yes
[45]	High	Medium	High	No	Yes	Yes	No
SPATA	Low	Low	Low	No	No	No	No

[9] C. Gañán, J. L. Munoz, O. Esparza, J. Mata-Díaz, and J. Alins, "Epa: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," Pervasive and Mobile Computing, vol. 21, pp. 75–91, 2015.

[10] I. T. S. Committee et al., "Ieee trial-use standard for wireless access in vehicular environments-security services for applications and management messages," IEEE Vehicular Technology Society Standard, vol. 1609, p. 2006, 2006.

[11] C. Diaz, "Anonymity metrics revisited," in Dagstuhl Seminar Proceedings, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.

[12] A. M. Carianha, L. P. Barreto, and G. Lima, "Improving location privacy in mix-zones for vanets," in Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International, pp. 1–6, IEEE, 2011.

[13] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[14] M. Thiago, H. O. Almeida, A. Perkusich, L. de Sales, and M. de Sales, "A privacy-preserving authentication and sybil detection protocol for vehicular ad hoc networks," in Consumer Electronics (ICCE), 2014 IEEE International Conference on, pp. 426–427, IEEE, 2014.

[15] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th, pp. 2521–2525, IEEE, 2007.

[16] J. Freudiger, M. H. Manshaei, J.-Y. Le Boudec, and J.-P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in INFOCOM, 2010 Proceedings IEEE, pp. 1–9, IEEE, 2010.

[17] D. Förster, F. Kargl, and H. Löhr, "Puca: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (vanet)," in Vehicular Networking Conference (VNC), 2014 IEEE, pp. 25–32, IEEE, 2014.

[18] D. Förster, F. Kargl, and H. Löhr, "Puca: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," Ad Hoc Networks, vol. 37, pp. 122–132, 2016.

[19] K. Sakai, M.-T. Sun, W.-S. Ku, J. Wu, and F. S. Alanazi, "Performance and security analyses of onion-based anonymous routing for delay tolerant networks," IEEE Transactions on Mobile Computing, vol. 16, no. 12, pp. 3473–3487, 2017.

[20] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in Computational Science and Engineering, 2009. CSE'09. International Conference on, vol. 3, pp. 139–145, IEEE, 2009.

[21] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in vanets," in Wireless Communications and Networking Conference (WCNC), 2010 IEEE, pp. 1–6, IEEE, 2010.

[22] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "Rprep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled vanets," International Journal of Distributed Sensor Networks, vol. 12, no. 3, p. 6138251, 2016.

[23] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for vanet," IEEE Access, vol. 4, pp. 7770–7784, 2016.

[24] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2017.

[25] J. Whitefield, L. Chen, F. Kargl, A. Paverd, S. Schneider, H. Treharne, and S. Wesemeyer, "Formal analysis of v2x revocation protocols," in International Workshop on Security and Trust Management, pp. 147–163, Springer, 2017.

[26] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in Vehicular Networking Conference (VNC), 2009 IEEE, pp. 1–8, IEEE, 2009.

[27] M. N. M. Bhutta, H. S. Cruickshank, and Z. Sun, "An efficient, scalable key transport scheme (eskts) for delay/disruption tolerant networks," Wireless networks, vol. 20, no. 6, pp. 1597–1609, 2014.

[28] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: a secure and privacy-preserving protocol for vehicular communications," IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442–3456, 2007.

[29] A. Shamir, "Identity-based cryptosystems and signature schemes," in Workshop on the Theory and Application of Cryptographic Techniques, pp. 47–53, Springer, 1984.

[30] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010.

[31] D. Y. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, "Revocable ring signature," Journal of Computer Science and Technology, vol. 22, no. 6, pp. 785–794, 2007.

[32] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in Communications (ICC), 2010 IEEE International Conference on, pp. 1–6, IEEE, 2010.

[33] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, 2006.

[34] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3589–3603, 2010.

[35] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19–28, ACM, 2007.

[36] U. Rajput, F. Abbas, J. Wang, H. Eun, and H. Oh, "Cacppa: A cloud-assisted conditional privacy preserving authentication protocol for vanet," in Cluster, Cloud and Grid Computing (CCGrid), 2016 16th IEEE/ACM International Symposium on, pp. 434–442, IEEE, 2016.

[37] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM journal on computing, vol. 32, no. 3, pp. 586–615, 2003.

[38] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 246–250, IEEE, 2008.

[39] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 1229–1237, IEEE, 2008.

[40] A. Singh, M. Wagner, J. Schäfer, H. Simo-Fhom, and N. Bißmeyer, "Restricted usage of anonymous credentials in vanet for misbehavior detection," Master's thesis, University of Applied Sciences, Frankfurt am Main, 2012.

[41] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in

Vehicular Networking Conference (VNC), 2013 IEEE, pp. 71–78, IEEE, 2013.

[42] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," Digital Communications and Networks, vol. 3, no. 3, pp. 180–187, 2017.

[43] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 33–46, 2012.

[44] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for vanets," in Proceedings of the 3rd international workshop on Vehicular ad hoc networks, pp. 94–95, ACM, 2006.

[45] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "Lespp: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication," Computing, vol. 98, no. 7, pp. 685–708, 2016.

[46] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in International Conference on the Theory and Application of Cryptology and Information Security, pp. 452–473, Springer, 2003.

[47] D. H. Yum and P. J. Lee, "Generic construction of certificateless signature," in Australasian Conference on Information Security and Privacy, pp. 200–211, Springer, 2004.

[48] R. Tso, X. Huang, and W. Susilo, "Strongly secure certificateless short signatures," Journal of Systems and Software, vol. 85, no. 6, pp. 1409–1417, 2012.

[49] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," Information Sciences, vol. 317, pp. 48–66, 2015.

[50] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," Vehicular Communications, 2017.

[51] S. B. Venkata, P. Yellai, G. D. Verma, A. Lokesh, K. Adithya, and S. S. S. Sanagapati, "A new light weight transport method for secured transmission of data for iot," in Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on, pp. 1–6, IEEE, 2016.

[52] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," IEEE Journal on Selected Areas in communications, vol. 25, no. 8, 2007.

[53] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in International Workshop on Privacy Enhancing Technologies, pp. 41–53, Springer, 2002.

[54] J. Herrera-Tapia, E. Hernández-Orallo, A. Tomás, C. T. Calafate, J.-C. Cano, M. Zennaro, and P. Manzoni, "Evaluating the use of sub-gigahertz wireless technologies to improve message delivery in opportunistic networks," 2017.

[55] T. Abdelkader, K. Naik, A. Nayak, N. Goel, and V. Srivastava, "A performance comparison of delay-tolerant network routing protocols," IEEE Network, vol. 30, no. 2, pp. 46–53, 2016.

QAZI EJAZ ALI did his MS (Computer Science) degree in 2008 from IBMS, Agricultural University Peshawar, Pakistan. He is working towards his Ph.D. Degree in Computer Science from Department of Computer Science, University of Peshawar and in addition, he is working as an Assistant Professor in Department of Computer Science, University of Peshawar, Pakistan. His research interests are network security, intelligent transport system security and privacy, and its efficiency.

NAVEED AHMAD received his BS(Computer Science) degree from University of Peshawar, Pakistan in 2007 and PhD in Computer Science from University of Surrey, UK in 2013. He is currently working as an Assistant Professor in Department of Computer Science, University of Peshawar, Pakistan. His research interests include security and privacy in emerging networks such as VANETs, DTN, and Internet of Things (IoT).

ABDUL HASEEB MALIK received his Ph.D. degree in Computer Science from the University of York in 2012. Since then he has been working as Assistant Professor in the Department of Computer Science, University of Peshawar. His research interests include Real-Time Systems, High Performance Computing, Concurrency and Programming Platforms. Presently, his research is focused on increasing predictability in platforms for Real-Time Big Data Analytics.

GAUHAR ALI received his MS (Computer Science) degree from Institute of Management Sciences, Peshawar, in 2012. He is a PhD scholar at University of Peshawar. His research interests include internet of things, access control, blockchain, intelligent transport system, formal verification, and model checking.

MUHAMMAD ASIF is working as an assistant professor in Department of Electronics, University of Peshawar. He did his PhD in Electronics Engineering from University of Surrey, UK. His research interests include MANETs, sensor networks, signal processing, and renewable energy.

MUHAMMAD KHALID completed his MS in computer science form Institute of Management Sciences, Peshawar, Pakistan. He is working towards his PhD degree from Northumbria University, Newcastle Upon Tyne, UK. His research interests include EV charging and scheduling, Internet of Things, Wireless Sensor Network, and Autonomous Valet Parking.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2883134, IEEE Access

YUE CAO received the PhD degree from the Institute for Communication Systems (ICS), 5G Innovation Centre (5GIC), at University of Surrey, Guildford, UK in 2013. He was a Research Fellow at the ICS until September 2016, and Lecturer in Department of Computer and Information Sciences, at Northumbria University, Newcastle upon Tyne, UK until July 2017, and currently the Senior Lecturer since August 2017. His research interests focus on Intelligent Mobility. He is the Associate Editor of IEEE Access, KSII Transactions on Internet and Information Systems.