IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 29, 2017, accepted June 12, 2017, date of publication June 21, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2717999

A Hybrid Approach for Efficient Privacy-Preserving Authentication in VANET

UBAIDULLAH RAJPUT[1], (Student Member, IEEE), FIZZA ABBAS[2], (Member, IEEE), HASOO EUN[1], (Member, IEEE), and HEEKUCK OH[1], (Member, IEEE)

[1]Department of Computer Science and Engineering, Hanyang University, Ansan 15588, South Korea
[2]Department of Computer System Engineering, Quaid-e-Awam University of Engineering Science and Technology, Nawabshah 67480, Pakistan

Corresponding author: Heekuck Oh (hkoh@hanyang.ac.kr)

This work was supported in part by the Ministry of Science, ICT and Future Planning, South Korea, under the Information Technology Research Center Support Program, supervised by the Institute for Information & Communications Technology Promotion, under Grant IITP-2017-2014-0-00636 and in part by the National Research Foundation of Korea grant funded by the Korean government Department of Ministry of Education, Science and Technology under Grant NRF-2015R1D1A1A09058200.

ABSTRACT A vehicular ad hoc network (VANET) serves as an application of the intelligent transportation system that improves traffic safety as well as efficiency. Vehicles in a VANET broadcast traffic and safety-related information used by road safety applications, such as an emergency electronic brake light. The broadcast of these messages in an open-access environment makes security and privacy critical and challenging issues in the VANET. A misuse of this information may lead to a traffic accident and loss of human lives at worse and, therefore, vehicle authentication is a necessary requirement. During authentication, a vehicle's privacy-related data, such as identity and location information, must be kept private. This paper presents an approach for privacy-preserving authentication in a VANET. Our hybrid approach combines the useful features of both the pseudonym-based approaches and the group signature-based approaches to preclude their respective drawbacks. The proposed approach neither requires a vehicle to manage a certificate revocation list, nor indulges vehicles in any group management. The proposed approach utilizes efficient and lightweight pseudonyms that are not only used for message authentication, but also serve as a trapdoor in order to provide conditional anonymity. We present various attack scenarios that show the resilience of the proposed approach against various security and privacy threats. We also provide analysis of computational and communication overhead to show the efficiency of the proposed technique. In addition, we carry out extensive simulations in order to present a detailed network performance analysis. The results show the feasibility of our proposed approach in terms of end-to-end delay and packet delivery ratio.

INDEX TERMS Vehicular ad hoc network, security, privacy, authentication, pseudonym, conditional anonymity.

I. INTRODUCTION

According to the global status report[1] on road safety 2015, published by world health organization (WHO), the number of deaths caused by road traffic accidents have increased to 1.25 million per year. The leading factors of the increasing number of road traffic accidents include increasing population, traffic congestion, driver negligence, traffic rules violation, and insufficient information of roads. Vehicular Ad Hoc Network (VANET) is a new technology that aims to provide the road safety and comfort by reducing the road congestion [1]. VANET inherits many of the features of a Mobile Ad Hoc Network (MANET) with additional features such as the nodes (vehicles) moving with high speeds. Vehicles communicate with each other via vehicle-to-vehicle (V2V) communication and with an infrastructure called Road Side Unit (RSU) via Vehicle-to-Infrastructure (V2I) communication. Each Vehicle is equipped with an On Board Unit (OBU) with communication and processing capabilities. Vehicles communicate with each other and with the infrastructure through a Dedicated Short-Range Communication (DSRC) standard [2]. Fig. 1 shows a typical VANET environment composed of Vehicles and infrastructure.

In the context of road safety, each vehicle is required to broadcast traffic messages (or beacons) that contain information related to the vehicle and the traffic conditions.

[1]http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/

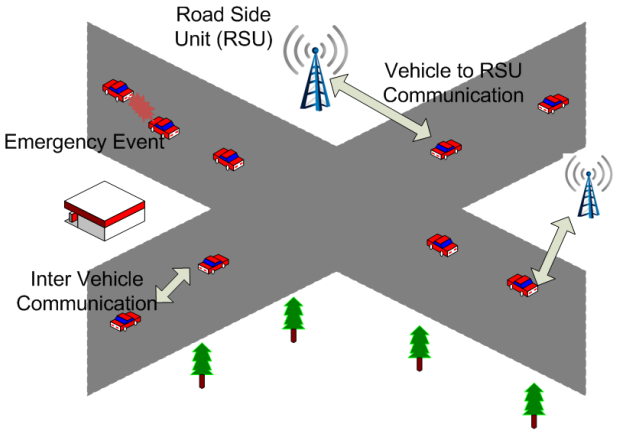

FIGURE 1. VANET overview.

This information is used by several applications such as Emergency Electronic Brake Light (EEBL), obstacle warning (to name a few). These applications help a driver in forming a contextual view of the surroundings that assists the driver in taking necessary action in case of a hazard. This information include vehicle's speed, direction, geo coordinates (to name a few) as well as traffic events. The open-access environment of VANET raises some serious security and privacy issues. The beacons contain the location and identification information of vehicles. The attackers can launch various types of attacks by intercepting, altering or forging this data. For example, an attacker may eavesdrop the communication in order to track a particular vehicle and later use this information to harass the driver. In the same way, an active attacker may spoof bogus beacons in the network to maliciously create the false impression of road congestion in order to take an unfair advantage or may cause an accident in the worst scenario. A solution to this problem is the authentication of vehicles, however, authentication requires some sort of identification information that may jeopardize the privacy of users. Therefore, we need privacy preserving authentication where a user's privacy is preserved during the authentication. However, the mechanism should only provide conditional anonymity i.e. a user's privacy is preserved until the user honestly follows the protocol. In case of a malicious activity, the culprit must be trackable. Parno and Perrig [3] and Raya, and Hubaux [4] identify various issues related to security and privacy in VANET. Authentication of vehicles plays a vital role in catering these issues. However, detection and revocation of malicious users while keeping the privacy of honest users makes authentication a challenging task in VANET. In this context, a number of privacy preserving schemes have been proposed which include pseudonymous based schemes [4]–[6] and group signature-based schemes [7], [43]. Furthermore, schemes such as presented in [39], [40], and [41], use mix zones to provide location blurring. However, these schemes propose pseudonym changing and distribution strategies and can be considered a subset of aforementioned broad categories. A broader taxonomy can be found in [10]. These schemes attempt to resolve most of the security and privacy issues in VANET, but each has some limitations. Most of the pseudonyms-based schemes use public key infrastructure (PKI) based signatures and corresponding certificates. One of the drawbacks is the computational overhead in verifying signatures and communication delays due to the large communication overhead. However, the biggest disadvantage comes with the Certificate Revocation List (CRL). In most of the pseudonym-based schemes, a Certification Authority (CA) creates and issues thousands of anonymous certificates to a vehicle, known as pseudonyms. The vehicle signs the beacon with the corresponding private key, attaches the certificate and broadcasts the beacon. The receiving vehicle verifies the beacon with the attached certificate. However, in case of a revocation, all the pseudonyms issued to the malicious vehicle are needed to be revoked. Therefore, vehicles in such schemes are needed to manage a large CRL that grows exponentially. This causes significant processing overhead on OBUs and consumes a large bandwidth during the CRL update and distribution. Additionally, it also causes transmission delays and packet loss due to the limited channel bandwidth.

In the group signature schemes, a vehicle acts as a group manager and other vehicles act as group members. The beacons are signed with individual vehicle's private key and verified with group public key. However, these schemes are not without disadvantages. According to [8], each operation required to check the signature involves two pairing calculations and therefore incurs significant processing overhead. Another major disadvantage is the group management and related trust issues. The group managers have complete information of group members and therefore, selecting a group manager is not trivial. In a dynamic group environment, vehicles continuously leave and join the group and the new manager has access to all the information. These trust related issues make group signature based schemes harder to implement.

This paper proposes a hybrid privacy preserving authentication approach with conditional anonymity. Our approach combines the benefits provided by pseudonyms-based schemes and group signature-based schemes and it efficiently eliminates the limitations of these schemes. We also propose modular architecture that acts as a Certification Authority (CA). The modular architecture is suitable to be implemented on cloud computing in order to assist the system to perform smoothly and efficiently. The CA is responsible for the tasks such as vehicle enrollment and distribution and verification of their credentials. However, we attempt to minimize the interaction between vehicles and the cloud for smooth operation. Moreover, our approach provides a novel concept of variable sized regions where vehicles communicate with each other under the same key. This paper is an extended version of our preliminary effort [9]. It covers state-of-the-art regarding pseudonymous authentication issues with a more rigorous computational and communication analysis of the approach as well as a detailed network

analysis with extensive simulation results. The main contributions of this paper are as follows:

1) We propose a privacy preserving authentication approach with a conditional privacy preservation for VANET. The real identity of a malicious user can be revealed at the detection of malicious activity.
2) Another significant contribution of this research is a simple, unique and light-weight pseudonym. The trapdoor inside the pseudonym provides a robust and efficient mechanism to provide conditional anonymity. Hence, it is very hard for an attacker to differentiate between two similar looking pseudonyms. However, the trapdoor mechanism guarantees the tracking of a malicious user that is subsequently identified and revoked from the system.
3) The proposed approach efficiently combines the concepts of two extensively used approaches in the literature, namely pseudonym-based approaches and group signature-based approaches. These two approaches are merged in such a way that their individual drawbacks (e.g., long CRL and group management overhead on vehicles) are efficiently eliminated.
4) We also propose a cloud-assisted modular architecture for the CA in our approach. The architecture is designed according to the current cloud-based computing paradigms. The modular architecture promises to play an efficient role in overall performance of the network.
5) Another novel contribution of this work is the region-based grouping of vehicles. We deviate from the traditional idea of vehicles-based grouping and introduce regional groups where a vehicle becomes the part of a group while entering in a particular area or road. These groups are managed by the CA and the use of similar credentials by vehicles makes it very hard for an attacker to distinguish a particular vehicle among other vehicles in the group.
6) We reduce the trust assumptions on the RSU as it works only as a relay in our scheme to assist vehicles getting the cryptographic credentials from the CA. In case of a non-pervasive deployment of RSU, vehicles do not need to contact the CA frequently and the light weight credentials make it possible for a vehicle to use data services to download the credentials from the CA directly.
7) Our approach provides an efficient prevention from various types of security threats on beacons such as attacks on message authentication, data integrity and non-repudiation.

The rest of the paper is organized as follows. Section II presents the related work. Section III explains preliminaries of the proposed approach. In Section IV, our proposed hybrid privacy preserving approach is presented that is followed by security, computational and communicational analysis in Section V. Section VI discusses the simulation results, while Section VII concludes the paper along with future work.

II. RELATED WORK

In the last decade, many privacy preserving authentication schemes have been proposed. These include pseudonym-based schemes, group signature-based schemes, ID-based schemes, symmetric cryptography-based schemes (to name a few) [10]. Since the publication of the landmark work by Raya and Hubaux [4], in which they highlighted the security and privacy requirements for VANET and propose one of the earliest pseudonym-based scheme, many authors have followed their work and proposed a number of pseudonym-based and group signature-based schemes.

The pseudonyms-based schemes are mostly implemented with the help of Public Key Infrastructure (PKI). PKI based certificates are attached with the beacons that are signed with the corresponding private keys. Each certificate contains a pseudo identity. The relation between the pseudo identity and the certificate is known to the issuing authority, called certification authority (CA). Raya and Hubaux [11] proposed a pseudonymous scheme in one of their pioneer works. In their scheme, the CA generates thousands of certificates that are subsequently distributed to a vehicle along with the corresponding private keys. The sender of the beacon selects one of the certificates, signs the beacon with the corresponding private key and broadcasts the beacon along with the certificate. The verifier is able to verify the beacon with the attached certificate. At the detection of a malicious beacon, the certificate is traced and the owner of the certificate is revealed by the CA. Raya *et al.* [12] come up with further improvements by introducing a hardware security module (HSM) or a Temper Proof Device (TPD) that is used to secure the cryptographic material stored in a vehicle's OBU. However, such schemes suffer from the storage and communicational overhead involved in the distribution and the storage of thousands of pseudonymous certificates. Another major drawback is the usage of a Certificate Revocation List (CRL). In case of revoking a vehicle, all the certificates issued to that vehicle needed to be included in the CRL whose size grows exponentially. Therefore, there is an additional overhead involved in the distribution, storage and checking of CRL. Zhang *et al.* [13] recently proposed an improved scheme that requires a realistic TPD instead of an ideal TPD. The scheme also provides conditional anonymity. Sun *et al.* [14] attempts to reduce the CRL by proposing hash chains and use a proxy re-signature scheme in order to improve the time required to update the CRL. Lu *et al.* [5] propose a conditional privacy preserving approach. A vehicle needs to acquire short-time pseudonym keys from RSU and therefore, this approach requires pervasive deployment of RSUs. However, the major drawback is that the trusted authority needs to frequently distribute the RSUs with updated CRL. Recently, Rajput *et al.* [19] proposed a hierarchical pseudonymous-based approach that requires vehicle to get primary pseudonym from the CA and secondary pseudonyms from the RSU. However, their scheme assumes the pervasive deployment of RSUs.

The approaches presented in [15] and [16] use identity-based cryptography [17] where the public key is a recognizable identity and the corresponding private key is generated by a Trusted Authority (TA). In order to provide privacy, the recognizable identity is concealed with the help of a pseudonym and therefore, these schemes suffer from the pseudonym management overhead. Zhang *et al.* [16] propose an identity based verification scheme that generates pseudo-identity based certificates and the corresponding private keys with the help of a TPD. However, this scheme is less efficient than a symmetric cryptography and also suffers from Denial-of-Service (DoS) attack.

In group signature based authentication schemes [7], [8], [18], a vehicle's real identity is concealed among a group of vehicles. The vehicles in a group sign beacons with individual private keys and the receiver verifies the beacon with the group's public key. In case of a malicious message, the group manager is able to trace the malicious member and subsequently revokes it. Calandriello *et al.* [8] proposed a technique that combines both the group signature-based and pseudonymous-based schemes. However, the scheme is computationally expensive as it requires to check a message against the revoked vehicles. The approach in [18] uses the RSUs to act as group managers in order to manage and maintain the vehicles. The vehicles form a group in a RSU's jurisdiction and broadcast beacons that are verifiable within the group as well as by the vehicles of the neighboring group. The scheme requires a pervasive deployment of the RSU that improves the overall system performance by load sharing. However, the pervasive RSU deployment can have a negative impact on the overall performance. Moreover, in case the RSU compromises, the security and privacy of the vehicles may be jeopardized. Xiong *et al.* [20] use revocable ring signatures proposed by Liu *et al.* [21]. The scheme provides conditional anonymity but suffers from the distribution of revocation information to all the vehicles.

The relevant literature reveals that the pseudonymous-based schemes mainly suffer from the communicational, computational and storage related overheads due to the CRLs. The CRL grows exponentially with the increasing number of revoked vehicles in the system. Identity-based schemes suffer from the pseudonym management tasks that are carried out in order to provide privacy. The group signature-based schemes incur overhead related to group management. Another disadvantage is the trust related issues with the vehicle acting as a group manager. Furthermore, use of a RSU endangers the privacy of the member vehicles. Finally, the group signature based schemes come with the computational overhead in terms of pairing-based calculations.

Our proposed hybrid approach neither requires the management and distribution of expensive CRL, nor involves vehicles or RSUs in group management issues. The modular architecture of CA is proposed keeping benefits of cloud computing in mind [35], [42]. We also propose a light-weight pseudonym that not only hides the identity of the sender of beacon message but also provides a trapdoor mechanism that enables the CA to detect a malicious group member and provides conditional anonymity. However, the pseudonym as well the beacons carrying the pseudonyms are very hard to distinguish among each other. The similar structure of the beacons makes it extremely hard for an attacker to identity a particular beacon broadcast by a vehicle. The receiver vehicle easily verifies the beacon with the common group certificate. Another advantage is the geographical region based grouping of vehicles that can make it easier to predict the number of vehicles in a particular region and subsequent resource allocation to handle the request.

III. PRELIMINARIES

This section describes attack model, security requirements, cryptographic tool, system model and assumptions of our proposed approach.

A. ATTACK MODEL

This section discusses various types of attackers and security attacks in a VANET environment. We can classify attackers based on their behaviors and capabilities in the network. An adversary vehicle injects or alters a beacon and therefore, disrupts the performance of the network for personal benefits. Raya and Hubaux [4], Zhou *et al.* [22], and Amer *et al.* [23] classify attackers with respect to their behavior and capabilities. Their classification includes (i) active vs passive attackers, (ii) insiders vs outsiders and (iii) malicious vs rational attackers. Active attackers inject bogus beacons while the passive attackers do not actively participate and only eavesdrop the communications. The stolen information is forwarded to other attackers. The insider attackers are to be considered very dangerous because of the detailed knowledge of the network. Insiders can launch a variety of complex attacks due to their knowledge about the network configuration. Outsiders are not the members of the network and are considered to be far less harmful then insiders. The malicious attackers' main objective is to disrupt and degrade the network performance without any personal benefits. These attackers are hard to detect and therefore, may severely damage the network. The motive of attacks of rational attackers is personal and they are easier to be detected.

Following are the various attacks against the security in VANET as described in [25] and [26].

1) Location tracking attack: where the location of a vehicle is tracked by attackers.
2) Modification attack: Attackers modify the content of the beacon messages.
3) Impersonation attack: Attackers uses a fake identity in order to pretend to be another vehicle.
4) Bogus information attack: where an attacker broadcasts fake or bogus information.
5) Sybil attack: Attackers forges fake identities of multiple vehicles.
6) Replay attack: Attackers replay the same message again.

7) Denial of Service (DoS) attack: Attackers degrade the performance of the network by injecting dummy messages.

In order to provide better security, a security scheme should provide prevention against such attacks. The section V-A analyzes the security of our proposed approach in the perspective of aforementioned security attacks.

B. SECURITY REQUIREMENTS

Following security requirements must be fulfilled in order to prevent various security attacks [11], [24].

- Vehicle authentication: The fundamental requirement of our approach is the privacy preserving authentication of a VANET user. This requirement assures the receiver of a beacon message about the legitimacy of the sender vehicle.
- Message Integrity: The proposed approach should also guarantee the message integrity, i. e., the content of the message should be delivered to a receiver unaltered.
- Privacy preservation: The content of a beacon should not reveal any information about the sending vehicle.
- Non-repudiation: The sender vehicle must not be able to deny the transmission of the beacon.
- Traceability: The approach must be able to track insider attackers.
- Low overhead: The security overhead should be kept to a minimum in terms of computation and communication.

C. CRYPTOGRAPHIC TOOL

We utilize Elliptic Curve Cryptography (ECC) as the cryptographic tool in our approach. For encryption, Elliptic Curve Integrated Encryption Scheme (ECIES) is used, whereas, for the signature we use Elliptic Curve Digital Signature Algorithm (ECDSA). ECIES comprises of Diffie-Hellman key exchange, a symmetric encryption scheme and a message authentication code (MAC). We adopt AES-128 bits as the encryption algorithm. It can be used with different modes such as CTR or CBC with PKCS#7 padding (where necessary) and SHA-1 HMAC for authenticity checks. The output is an encrypted message with padding, ephemeral public key and HMAC [27]–[29]. Following is the brief introduction of ECC.

The cubic equation of an elliptic curve has the form $y^2 + axy + by = x^3 + cx^2 + dx + e$, where a, b,c, d, and e are all real numbers. In an ECC system, the elliptic curve equation is defined as $E_p(a, b) : y^2 = x^3 + ax + b(modp)$, over a prime finite field F_p, where $a, b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0(modp)$ [38].

In general, the security of ECC depends on the difficulties of the following problems [38].

Definition 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)): Given two points P and Q over $E_p(a, b)$, the elliptic curve discrete logarithm problem (ECDLP) finds an integer $s \in F_p^*$ such that $Q = s \cdot P$.

Definition 2 (Computational Diffie-Hellman Problem (CDHP)): Given three points P, $s.P$ and $t.P$ over $E_p(a, b)$ for $s, t \in F_p^*$, the computational Diffie-Hellman problem finds the point $(s.t).P$ over $Ep(a, b)$.

D. SYSTEM MODEL

In this subsection, we discuss our system model.

1) VEHICLES

Each vehicle in a VANET is identified with a digital identity [34]. This digital identifier is issued and subsequently installed by some authority responsible to register the vehicles, such as Department of Motor Vehicles (DMV). We will subsequently refer this digital identity as *VID* in the rest of the paper. The *VID*, also known as electronic license plate (ELP), serves as a long term unique identity for the vehicle. Our approach utilizes *VID* in order to uniquely identity a vehicle and stores it in the CA's database at the time of registration of the vehicle with the CA. After the registration, the vehicle becomes a part of the network. However, in case of a malicious activity, a law enforcement agency provides the CA with the evidence of the malicious activity and requests the CA for malicious vehicle's revocation. The CA identifies the vehicle using our proposed trapdoor mechanism, revokes the vehicle and prevents the culprit from further taking part in the network. However, proposed approach does not consider the issuance and installation of *VID* in the vehicle. There are many possible ways to do this, such as the vehicle may require to physically visiting the DMV for issuance and installation of *VID*.

A vehicle in our system model assumes the role of sender as well as the receiver of beacons messages. We denote a sender vehicle with V_i and the receiver vehicle with V_r for simplicity. The V_i signs and broadcasts the beacon message and the V_r verifies the received beacon. In case of the detection of a malicious activity, such as a bogus beacon, the V_r reports the law enforcement authority with the recordings of the malicious act.

2) ROADSIDE UNIT (RSU)

RSUs assume a passive role in our proposed approach and serve as relays/gateway between the CA and the vehicles. The vehicles entering into a region detect the RSU's announcements and subsequently send region credential request to CA via RSU. The credential response is subsequently sent to the vehicle from CA via RSU. In case a vehicle is unable to receive the RSU announcement due to the absence of RSU or an obstruction, the vehicle uses its 3G/4G communication capabilities in order to communicate with the CA. In case the vehicle is not equipped with 3G/4G data communication capabilities, it uses 3G/4G capabilities of other vehicle to communicate with CA. Fig. 2 shows the system model of our proposed approach.

3) CLOUD-BASED CERTIFICATION AGENCY (CA)

The certification authority in our proposed approach comprises of many inter-related modules. These modules are responsible for various tasks related to the credential

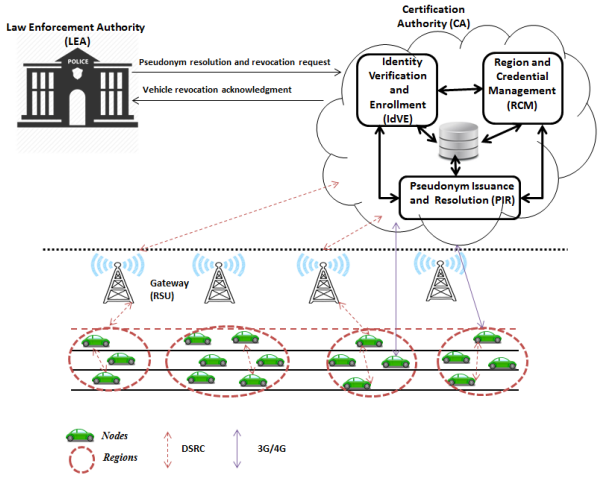

FIGURE 2. System model of proposed approach.

generation, management and verification. The vehicles request the CA for the appropriate action and the request is routed to the appropriate module. The modular architecture has been designed considering the benefits offered by cloud computing [35] such as faster processing, scalability and virtually unlimited storage capabilities and therefore, our proposed architecture is suitable for a cloud based implementation. However, the actual implementation is beyond the scope of this work. The CA is divided into three main modules named as identity verification and enrollment module (IdVE), pseudonym issuance and resolution module (PIR), and region and credential management module (RCM). The CA also contains a central database that is accessible to all the modules. The modules are responsible for various tasks such as identity verification of a vehicle, vehicle enrollment, pseudonym generation, issuance and resolution, region cryptographic credentials update and distribution. Following is the brief description of each module.

- Identity Verification and Enrollment (IdVE): is responsible for the identity verification of a vehicle. First a vehicle sends its vehicle identity (*VID*) to the CA. The IdVE first check the database for revoked vehicles and upon a positive response no further action is taken. In case of a negative response, user specific cryptographic credentials are generated and stored in the database against the *VID* and sent to the vehicle.
- Pseudonym Issuance and Resolution (PIR): is responsible for the issuance of a number of pseudonyms to a vehicle. Once a vehicle passes the check from IdVE, the PIR issues a number of pseudonyms to the requesting vehicle. It keeps the mapping of the issued pseudonyms and the associated vehicle cryptographic credentials. In case a malicious pseudonym is reported to the CA, the PIR resolves the relation between the culprit pseudonym and the associated vehicle's cryptographic credentials and forwards it to the IdVE. The malicious vehicle is identified and subsequently revoked by IdVE.
- Region and Credential Management (RCM): is mainly responsible for management tasks related to region credentials such as periodic generation of region cryptographic credentials and subsequent distribution of credentials (keys, certificates, expiration time) among vehicles upon arrival of incoming vehicles' requests.

4) LAW ENFORCEMENT AUTHORITY (LEA)

entertains complaints such as report of a malicious beacon or other malicious acts related to beacons. It provides the CA with the malicious beacon. The CA identifies and revokes the culprit's *VID* and also provides the *VID* to LEA for further proceedings.

5) REGIONS

We propose another unique concept of dividing the geographical map of the world into variable sized cloaking regions. Therefore, a region can be considered as a sub-division of entire world database. We borrow this idea from one of our earlier work presented in [33]. We divide the jurisdiction of CA into variable sized rectangular regions in order to form a grid. The size of the region is based on vehicles' population in such a way that the number of vehicles are evenly distributed. Therefore, regions of an urban area might be smaller but more populated then the regions of the rural (or sparse population) area. The regions are identified by a unique identifier on the grid (denoted by RegID in this approach). This unique identifier is denoted by the geo-coordinates of the upper-left corner of the region. However, a region may also be identified by the roads in the region. Therefore, once a vehicle joins a particular road during the journey, it identifies the region with the help of the GPS module installed in the vehicle. Fig. 3 illustrates this concept by dividing a portion of the map of South Korea into variable sized regions. The division of density based variable sized regions on a two dimensional map can be done by commonly used Miller cylindrical projection method [33].

E. ASSUMPTIONS

We have made the following assumptions in our approach.

1) Each vehicle's OBU is secured with a Hardware Security Module (HSM). The HSM is temper resistant in order to restrict the parallel usage of pseudonyms and cryptographic credentials.
2) The CA is a trusted entity.
3) The clocks of all the participants are synchronized.

IV. PROPOSED PROTOCOL

Our proposed approach is comprised of 5 phases, named as vehicle enrollment, pseudonyms issuance, region credentials issuance, message broadcast and pseudonym resolution and revocation. The working of the proposed approach is shown in Fig. 5. The notations are shown in Table 1. The network is initialized by the CA by setting the domain parameters p, a, b, G, n and h [28].

1) Let the field is defined by p.
2) G is the base point.
3) n is the order of G.

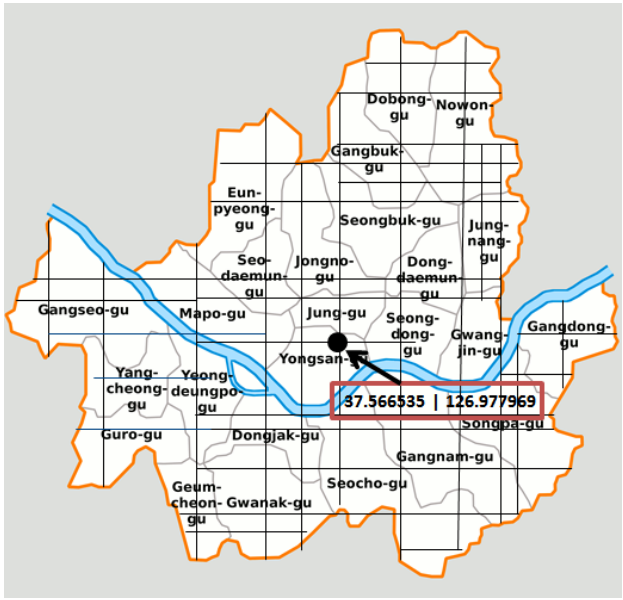

FIGURE 3. Regions representation.

TABLE 1. Notations.

Notations	Explanation
V_i	Initiator Vehicle
VID_i	Initiator's vehicle ID
PK_i, SK_i	Public/ private key pairs of V_i
PK_{CA}	CA Public key
PK_{Reg}/SK_{Reg}	Region's public/private key
T_{Reg}	Region's key certificate expiration time
$RegID$	Region identity
$p[i]$	i_{th} number of pseudonym
$Cert(PK_i, T)$	Long term certificate of V_i
beacon	Typical VANET message

4) a, b are curve constants.
5) cofactor $h = 1/n|E(E_p)|$.

The participants of the network are required to download these parameters from the CA. The CA randomly chooses $x \in Z_{p^*}$ as its private secret key. Similarly, all other participants also choose their respective keys in the same way.

A. VEHICLE ENROLLMENT

An initiator vehicle (V_i) needs to register itself with the CA. For this purpose, V_i generates a public/private ECC key pair PK_i/SK_i and prepares a Certificate Signing Request (CSR) that includes its VID_i and newly generated public key PK_i. V_i sends this CSR to the CA. This information is subsequently passed to the IdVE module of the CA.

1) $V_i \longrightarrow$ IdVE :$(VID_i||PK_i)_{Pk_{CA}}$

IdVE searches the VID_i in the database of revoked vehicles. If there is no match then it prepares a certificate containing the information provided by the vehicle such as the public key of V_i, a certificate expiration time T is also mentioned in the certificate that shows the validity period for the certificate. IdVE signs this certificate with the CA's private key and sends to the V_i. For simplicity we refer this certificate as

Pseudo code for Pseudonym Generation Algorithm

```
Begin
 t = timestamp      // the time for first pseudonym to be used
For i = 1 to k
    Begin
    Generate random n
    p = n || t
    pSigned = signCA (p) //where signCA is a function that signs p
    p[i] = pSigned || p   // stores i_th  p in an array
     t = t + 200   // increment time by 200 milliseconds for next p
     End
End
```

FIGURE 4. Pseudonym generation algorithm.

"long term certificate" in the rest of the paper. Note that this certificate will only be used for the confidential and authorized communication between user vehicle and the CA. The CA also keeps the long term certificates of the revoked vehicles in the database along with their hashes. An important requirement for a secure implementation is that a vehicle physically visits the CA for the first time in order to get the long term certificate and for subsequent expiration at T of long term certificate, may sends the expired long term certificate along with the CSR. Alternatively, a vehicle can be remotely verified by the CA using a PIN based authentication method. We propose that a vehicle remotely registers itself by securely providing the *VID*, a valid driver's identity such as driving license number and a cell phone number. Subsequently, after necessary verifications of user data, the CA authenticates the vehicle by sending a PIN code to the driver's registered cell number. This PIN code is then communicated to the CA securely for vehicle enrollment.

2) IdVE $\longrightarrow V_i : Cert(PK_i, T)$

B. PSEUDONYM ISSUANCE

The vehicle is now eligible for applying for the pseudonyms. In this regard, the vehicle prepares a request containing the acquired certificate and sends this to PIR.

3) $V_i \longrightarrow$ PIR: $(Cert(PK_i, T))_{Pk_{CA}}$

PIR module checks the database for revoked vehicles for the time period T mentioned in the long term certificate of V_i. If there is a match, PIR reports the malicious requester to IdVE. On a negative response, PIR issues a number of pseudonyms to V_i . PIR keeps a large pool of pseudonyms that are generated by executing the algorithm as shown in Fig. 4 and stored in CA's database. The issued pseudonyms and corresponding certificate of V_i are stored in the database (DB) as described in Table 2. As we can see, the certificate is not needed to be stored with every pseudonym as PIR uses two tables in the database, one for pseudonyms and one for the certificates with one-to-many relations. Therefore, the size of the PIR database is governed by the $n||t$ pair i.e., 20 bytes for each entry. In this way, the PIR module of CA requires 8.6 MB of storage for storing the pseudonyms issued to a vehicle per day and approximately 60 MB for a week. For storing this data for one million

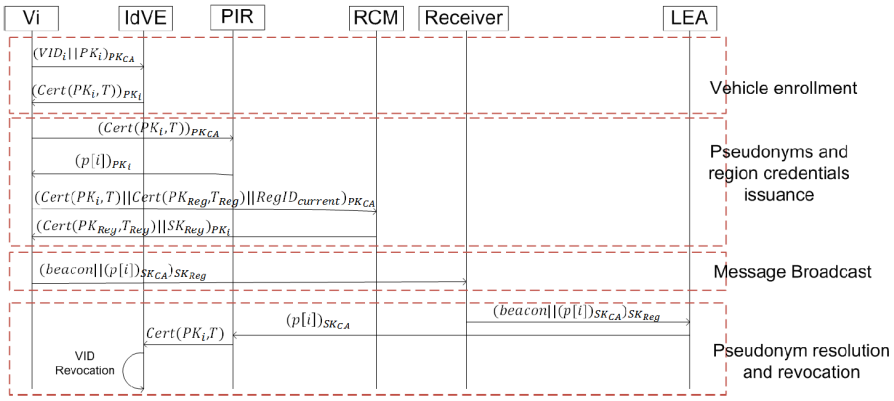

FIGURE 5. Working of proposed approach.

TABLE 2. A sample Database maintained by PIR.

$Timestamp$	n	$Certificate$
t_1	n_1	$(Cert(PK,T))_{Pk_{CA}}$
.	.	.
.	.	.
t_2	n_l	$(Cert(PK,T))_{Pk_{CA}}$
.	.	.
.	.	.
.	.	.
t_{n-1}	n_{m-1}	.
t_n	n_m	$(Cert(PK,T))_{Pk_{CA}}$

vehicles, CA only needs 60 TB of storage and additionally 177 MB for storing the certificates. By considering virtually unlimited storage capabilities of clouds, the CA can easily manage this amount of storage. The values $p[i]$ are then encrypted in public key of V_i and send back to the vehicle.

4) PIR $\longrightarrow V_i : (p[i])_{PK_i}$

C. REGION CREDENTIALS ISSUANCE

After getting certificate from IdVE and pseudonyms from PIR, a vehicle can request the current region's cryptographic credentials. The vehicle finds the current region identifier and then sends a request to the RCM in order to get the region specific cryptographic credentials. The request includes the long term certificate acquired by IdVE and the previous region certificate that has become invalid. The invalidation is either due to the expiration time mentioned in the region certificate or the vehicle has entered into a new region. In case the vehicle does not have the previously expired certificate due to recent inactivity or it is requesting region certificate for the first time, then V_i only sends its long term certificate, acquired from IdVE, along with the RegID to the RCM module of CA.

5) $V_i \longrightarrow$ RCM : $(Cert(PK_i, T)||(Cert(PK_{Reg}, T_{Reg})||RegID_{current})_{Pk_{CA}}$

A vehicle's request for the region specific cryptographic credentials is handled by the Region and Credential Management (RCM) module of CA. Upon receiving the request from V_i, the RCM takes the RegID from the certificate of the previous region and searches for a revocation in that region for time T mentioned in the certificate. In case the request does not contain a certificate for the previous region, the RCM takes the hash of the long term certificate provided by the V_i and searches this hash for the hashes of long term certificates of the revoked vehicles. On receiving a positive response no further action is taken, otherwise the RCM issues the cryptographic credentials to V_i including the region certificate and the signing key.

6) RCM $\longrightarrow V_i : (Cert(PK_{Reg}, T_{Reg})||SK_{Reg})_{Pk_i}$

Where PK_{Reg}, SK_{Reg} are the region's key pair and T_{Reg} is the credentials expiration time. Note that these credentials are common in a region at the same time instant.

D. MESSAGE BROADCAST

After acquiring region cryptographic credentials, V_i selects one of the pseudonyms that matches with the broadcast time of the beacon. It attaches pseudonym with the beacon, signs the pair with the region's private key and broadcasts the beacon. V_i does not need to attach the region certificate or CA certificate along with the beacon because every vehicle in the region already has these certificates. This procedure is repeated for every 200 ms until T_{Reg} or $Cert\ (PK_i, T)$ are expired or vehicle consumes all of the pseudonyms $p[i]$. In that case, the vehicle again needs to request for the new cryptographic credentials.

7) $V_i \longrightarrow$ Receivers (Beacon broadcast): $(beacon||(p[i])_{SK_{CA}})_{Sk_{Reg}}$

According to [4], the frequency of safety messages is 300 ms that drops to 100ms when the vehicles stop or move too slowly. Therefore, our proposed approach opts for an average beacons frequency of 200 ms.

E. PSEUDONYM RESOLUTION AND REVOCATION

The receiver of the beacon needs to perform two signature verifications. If any of the signature is not verified, the received beacon is dropped immediately. Otherwise the contents of the beacon are used to construct the traffic view.

A vehicle keeps the recent history of received beacons in such a way that it separately stores the hash of the attached pseudonym along with the beacon. Upon receiving a beacon, the vehicle checks for the hash of the pseudonym and if there is a match, the received duplicate beacon is discarded.

In case of detection of a malicious beacon, the receiving vehicle files a complaint to the law enforcement authority along with the recording of the malicious beacon.

8) Receiver $\longrightarrow$ LEA: $(beacon||(p[i])_{SK_{CA}})_{Sk_{Reg}}$

Law enforcement authority presents the pseudonym $p[i]$, contained in the message to the PIR of CA.

9) LEA $\longrightarrow$ PIR: $(p[i])_{sk_{CA}}$

PIR finds the corresponding $Cert(PK_i, T)$ associated with that pseudonym $p[i]$ and forwards it to the IdVE.

10) PIR $\longrightarrow$ IdVE: $Cert(PK_i, T)$

IdVE finds the corresponding long term certificate and subsequently the *VID* and revokes it.

11) IdVE $\longrightarrow$ Revokes: VID_i

It should be noted that until a region certificate expires, the revoked vehicle may continue to send messages. However, the damage related to this limitation can be significantly reduced by frequently changing the group credentials.

V. ANALYSIS OF THE PROPOSED APPROACH

This section discusses the proposed approach with respect to the security requirements. Additionally, we provide a thorough analysis against various security attacks, storage overhead, communication overhead, computational overhead and present a comparison of our proposed hybrid approach with the existing approaches.

A. SECURITY ANALYSIS

In this section, we analyze the proposed approach with respect to the security requirements.

1) VEHICLE AUTHENTICATION

All the vehicles in our proposed approach broadcast safety beacons. These beacons contain a pseudonym that consists of a random number and a timestamp $(n||t)$. The unique pair $(n||t)$ serves as a trapdoor. The 128 bit value of n also serves as a nonce. Moreover, the pseudonym contains the CA's signature and the entire beacon is signed with the region's private key. Only an authentic vehicle of the network poses a valid pseudonym and the region cryptographic credentials as it requires a valid long term certificate. Therefore, it is very hard for an attacker to acquire these credentials without the necessary valid information.

2) MESSAGE INTEGRITY

The content of the beacon message must contain a valid region signature. The region signature is easily verifiable through the region certificate and therefore, message integrity is guaranteed.

3) PRIVACY PRESERVATION

All the beacon broadcasts by vehicles in our proposed approach are similar. At a given time, all the beacons differ only by a random number. There is no relation between two consecutive beacon broadcasts. Additionally, the simple structure of a pseudonym does not contain any identity information. An attacker finds it very hard to establish any relation between consecutive beacons and therefore, our proposed approach preserves the privacy of the vehicle.

4) NON-REPUDIATION

The content of the beacon messages are signed by the region key. Besides, the beacons itself contains the unique pseudonym consisting of pair $(n||t)$. This pseudonym is only known to the message originator and therefore, the beacon broadcaster cannot repudiate.

5) REVOCATION/TRACEABILITY

Our proposed approach provides an efficient mechanism for a malicious vehicle's revocation. In case of receiving a malicious beacon, the receiver sends the recording of the malicious beacon to a law enforcement authority. The beacon contains the trapdoor i.e. user specific pseudonym. The LEA reports the malicious beacon to the PIR module that subsequently searches the CA's database for the pseudonym contained in the malicious beacon. Once matched, the corresponding long term certificate is reported to the IdVE that subsequently finds the associated *VID*. The *VID* is revoked as well as handed to LEA for further action.

Region credentials are essential for a vehicle to communicate with other vehicles. In case of a malicious activity, the CA revokes the $Cert\ (PK_i, T)$ and the malicious vehicle can no longer apply for the region credentials. However, until the current T_{Reg} expires, a malicious vehicle can send beacons. Therefore, the expiration time of T_{Reg} should not be set for a longer time period to prevent vehicle taking part in the network after revocation. However, this expiration time should not be too short to avoid possible burden on RCM.

6) CONDITIONAL ANONYMITY

Our proposed approach provides a conditional anonymity. All the beacons are identical in structure and therefore, individual vehicle's privacy is ensured until the vehicle does not involve in a malicious activity.

In the following, we discuss the prevention from various security attacks as mentioned in the attack model Section III-A.

1) Location tracking attack prevention:
   The beacons broadcast of vehicles contain the location information, however, a beacon does not contain any identity related information. Additionally, all the beacons in a region look similar. In the presence of more than one vehicle, an attacker who is eavesdropping, finds it hard to associate two beacons to a particular vehicle. Therefore, it is very hard for an attacker to launch a location tracking attack against a particular vehicle.

2) Modification attack prevention:
All the beacons in the network are signed using ECDSA and ECC based private key. The contents are easily verifiable with the help of region public key. In order to find the private key, the attacker needs to find the region private key. An insider attacker is easily traceable. However, an outsider attacker needs to compute the private key of the region. According to Diffie-Hellman Problem (DLP), given an element g and the value g^x, it is computationally infeasible for an adversary to compute the secret x. Therefore, it is computationally infeasible for an outsider attacker to launch a modification attack.
3) Impersonation attack prevention:
In order to launch an impersonation attack, an attacker needs a valid pseudonym and region credentials. The pseudonyms and the credentials are provided to a particular vehicle confidentially and stored in HSM of the vehicle. This makes an impersonation attack infeasible.
4) Bogus information attack prevention:
Our approach provides effective measures against a bogus information attack. All the vehicles are required to broadcast beacons with a valid pseudonym and signature. In case of a valid beacon containing bogus information, the tracing of the broadcaster is trivial in our approach. If the beacon containing the bogus information is not valid, then the receiving vehicle discards it.
5) Sybil attack prevention:
A Sybil attack requires an attacker to forges fake identities of multiple vehicles. The proposed approach requires every vehicle to be registered with the CA. The registration requires a valid VID_i or a valid long term certificates. These credentials are confidentially communicated and stored in vehicle's HSM. Therefore, it is very hard for an attacker to launch a Sybil attack.
6) Replay attack Prevention:
The proposed pseudonym is our approach provides an efficient way to cater a replay attack. Each of the pseudonyms contains the pair $(n||t)$. The timestamp t shows the time of the broadcasted beacon and therefore, makes a replay attack very hard. Additionally, the random value of n serves as a nonce and provides a second line of defense and therefore, upon detection of a repeated n, the receiver discards the replayed beacon.
7) Denial of Service (DoS) attack prevention:
DoS attacks are launched by injecting fake messages in the network. In case of such attack, a vehicle will experience an increased number of invalid beacons. Due to this abnormal behavior, a DoS attack will be detected early.
8) Physical attack on RSU prevention:
The RSUs in our proposed approach only serve as relays. All the communication between the vehicles and the CA is encrypted and therefore, it is useless for an attacker to compromise this communication.

B. STORAGE OVERHEAD ANALYSIS

Following are the storage requirements analysis of our approach.

1) SIZE OF THE PSEUDONYM

Each vehicle is pre-loaded with a set of pseudonym $P = p_1, p_2, p_3, ..., p_n$ in our approach. Each p_i consists of a 16 byte random number n, a 4 byte timestamp and a 64 bytes ECDSA (r, s) signature pair. The total size of the pseudonym is only 84 bytes.

2) SIZE OF THE CERTIFICATES

According to [36], an Elliptic Curve Qu-Vanstone (ECQV) X.509 certificate takes around 177 bytes with 224 bit ECC security [37]. For various certificate requirements in our proposed approach, we adopt the aforementioned certificate type.

3) STORAGE OVERHEAD ON OBU

Assuming a rate of 5 beacons per second, 432000 pseudonyms are required for a 24 hours travel and therefore, a vehicle needs only 36 MB of storage to store these pseudonyms. Similarly, for a nonstop traveling of one month, a vehicle only needs 1 GB of storage.Considering current hardware capabilities, the storage requirements of our approach are more than satisfactory.

Moreover, as soon as the timestamp t of a pseudonym expires (regardless of a vehicle use that pseudonym or not), the OBU deletes that pseudonym.

C. COMMUNICATION OVERHEAD ANALYSIS

Following is the communication cost of our approach.

1) VEHICLE TO CA COMMUNICATION

1) $V_i \longrightarrow$ RCM : $(Cert(PK_i, T)||(Cert(PK_{Reg}, T_{Reg})||RegID_{current})_{Pk_{CA}}$
Where $(Cert(PK_i, T) = 177$ bytes, $(Cert(PK_{Reg}, T_{Reg}) = 177$ bytes, 4 bytes RegID, 32 byte public key of CA for message encryption, 10 bytes of padding and 20 bytes of HMAC, and therefore, 420 bytes of message is communicated by the vehicle to the RCM module of CA in order to request region cryptographic credentials.
2) RCM$\longrightarrow V_i$: $(Cert(PK_{Reg}, T_{Reg})||SK_{Reg})_{Pk_i}$
where $(Cert(PK_i, T) = 177$ bytes, $SK_{Reg} = 32$ bytes, $PK_i = 32$ bytes for encrypting the message in the public key of vehicle, 15 bytes of padding and 20 bytes of HMAC, and therefore, 276 bytes response is communicated from CA to vehicle containing region cryptographic credentials.

2) VEHICLE TO VEHICLE COMMUNICATION

3) $Cert(PK_{Reg}, T_{Reg})||(beacon||p[i])_{SK_{Reg}}$

Where $Sig_{CA} = 64$ bytes, $p = 84$ bytes, beacon $=$ 200 bytes. The total size of beacon is 348 bytes with only 148 bytes of overhead.

D. COMPUTATIONAL OVERHEAD

In this subsection, we discuss the computational overhead of our proposed approach.

1) SEARCHING OVERHEAD ON CA

This subsection evaluates the computational overhead on the CA during real time operations such as search for revoked certificate during vehicle's request for regional credentials and searching for culprit pseudonyms during the revocation request. As mentioned in subsection 4-C-5, in case a vehicle's request includes the certificate of previous region, only few values are needed to be searched (assuming there will be only few revocations per region in time period T). However, in case the request does not contain region certificate of previous region, the RCM needs to check the certificate of the requesting vehicle against all the revoked certificates. Our proposed approach requires the CA to store the hashes of revoked certificates and therefore, the complexity can be computed as following:

Let there are n number of hashes of revoked certificates then total time needed to search will be:

$$log\ (n) \text{ or } O(log\ (n))$$

By considering today's hardware, the hashrate of some single ASIC units is over 1000GH/s.[2] In order to process a revocation request, the PIR module of the CA finds the culprit pseudonym by simply taking the hash of the pair $(n||t)$ of the malicious pseudonym p and compares the hashes of all values of $(n||t)$. However only those pair will be searched that have the matching t and therefore the searching time will be very small. We can formulate the complexity as shown below:

Let r be the number of pseudonyms with timestamp t needed to be searched. Let's assume that pseudonyms pair $(n||t)$ in the CA's database are sorted under time t. Let there are s such values of n associated with all those t. The searching complexity can then be calculated as:

$$log(r+s) \text{ or } O(log(r+s))$$

2) SIGNATURE VERIFICATION OVERHEAD ON VEHICLE

According to the proposed approach, a vehicle only needs a single ECDSA signature generation to sign a beacon with the region key and needs two ECDSA signature verifications for receiving beacon. Therefore, a vehicle can easily sign a beacon with 200ms frequency and verify enough beacons to form a broader traffic view. Moreover, if we consider existing batch verification schemes, the signature verification process can easily be made more efficient as all the beacons in a region carry same region signature.

E. COMPARISON WITH EXISTING APPROACHES

In order to better understand the advantages of our proposed approach, Table 3 provides a comparison of the proposed approach with both the pseudonym-based schemes and group signature-based schemes. The comparison table shows that the pseudonym-based schemes suffer from the problem of certificate revocation list. A vehicle needs to check the CRL upon receiving the beacon. Although the introduction of batch verification based schemes has reduced this problem, but CRL is still considered as a major drawback. The vehicles in group management approaches suffer with the group management related overhead. In order to provide traceability, the group manager needs to know the private information of the member vehicle that clearly violates the privacy preserving requirement. Additionally, most of the pseudonym-based and group signature-based schemes require the pervasive deployment of RSUs.

TABLE 3. Comparison with existing approaches.

Parameters	Pseudonym Based Approach	Group Based Approach	Proposed Approach
CRL Related Overhead	✓	×	×
Group Management Overhead	×	✓	×
Lack of Efficient Revocation	✓	✓	×
Requirement of Pervasive RSU Deployment	✓	✓	×

The proposed approach avoids all these limitations and provides an efficient solution for privacy preserving authentication in VANET. Our scheme efficiently caters the needs of a CRL by introducing a light-weight pseudonym containing the trapdoor for traceability. The vehicles or RSUs do not require managing any groups. Moreover, the proposed approach does not require the pervasive deployment of RSUs.

VI. NETWORK PERFORMANCE EVALUATION

In this Section, we evaluate the performance of our proposed privacy preserving authentication approach. We compare the performance of the traditional beacons that do not incur any cryptographic overhead and the secure beacons of our approach with respect to inter-vehicle beacon communication. For convenience, we will refer the beacons without any cryptographic overhead as unsecured beacons and our proposed beacons as secure beacons in the rest of the paper. We perform the comparison to show that there is no significant degradation in the performance; however, our proposed approach provides efficient security against various threats mentioned in attack model.

According to Raya and Hubaux [11], Raya *et al.* [12], the conventional beacon size is 200 bytes. Section V-C provides the details of the cryptographic overhead incurred by the secure beacons and other messages in our approach. We consider end-to-end delay, beacon reception rate, and packet loss as performance metrics for unsecured beacons and our proposed secure beacons. In the VANET environment, the speed of the vehicles as well as obstructions play an important role while in end-to-end delay, beacon reception

[2]https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison

rate, and packet loss. In order to perform realistic evaluation, we select three regions based on speed of the vehicles and the obstructions such as buildings. Our first region represents an area such as a downtown where the speed limit is low and there are higher number of obstacles. The length of the roads is smaller in comparison with other regions. The second region contain more open spaces, more longer sections with relatively more speed limit and relatively less number of obstacles in the path of the vehicles. The third region is highway with longest road sections and high speed vehicles. For convenience, we refer first region as a low speed region, second as a medium speed region, and third region as a high speed region in the rest of the paper. Our simulation evaluates the network performance of the beacons broadcast by the vehicles moving in low speed region, medium speed region and high speed region. Additionally, we simulate vehicles moving in all the regions simultaneously and traversing all three regions in such a way that some of the vehicles start from low speed region and then enter into medium and then high speed regions. Similarly the vehicles starting from medium and high speed regions also travel through the other two regions.

First we consider end-to-end delay incurred by both unsecured beacons and our proposed beacons. We analyze the end-to-end delay of the traffic with the above mentioned movement criteria. The simulation results are discussed in the next subsection. Next, the successful beacon delivery ratio is analyzed with respect to both the secure and unsecured beacons broadcast by vehicles and finally, we analyze the packet loss.

A. SIMULATION SETUP

VANET is mainly characterized by its unique topology and high speed mobility patterns exhibited by the vehicles. Traditionally VANET simulators consist of two components: a wireless network simulator and a road traffic simulator. We simulate our proposed approach with the help of Veins [30], an open source framework, to carry out vehicular based simulations. Veins consists of two simulators: OMNeT++ [31] and SUMO [32]. OMNeT++ is an event based simulator that is used to carry out wireless network based simulations and SUMO, a road traffic simulator, carries out realistic traffic simulations. Veins extends these two simulator to provide a comprehensive simulation model for vehicle based communications. We utilize the map of urban scenario provided by Veins and choose three regions based on the road speed limits and obstructions. The routes contain straight road sections where vehicles can attain maximum speed limits as well as turns where slow speed vehicles may form a small cluster. The straight road sections as well as road intersections allow a number of vehicles to be in the Line of Sight (LOS) of each other in order to receive a large number of beacons. Table 4 explains simulation setup.

To analyze our proposed approach, we simulated a number of scenarios with varying number of vehicles for all the regions including the mix regions scenario. In all the scenarios, we created two groups of vehicles starting their journey from the two opposite ends of a region and traveling towards other group's starting position. By doing so, we achieve the effects of one way traffic and two way traffic when the two groups pass by each other. The number of vehicles are ranging from 10 to 100 for the individual regions and from 30 to 150 for mix regions. The mean data for each group of vehicles is collected for each 10 vehicles interval in case of single region and 30 vehicles in case of mix regions. The length of the individual routes for each region is ranging from 1.5 km to 2.5 while the total route length of mix region is the sum of the routes' length of all three regions. In our scenarios, for single region, 10 vehicles' show sparse traffic that gradually becomes dense up to 100 vehicles with an increment of 10 vehicles. In case of mix regions, 30 vehicles show sparse traffic that becomes denser up to 150 vehicles with an increment of 30 vehicles. The maximum vehicle speed limit is set to 10 m/s to exhibit slow moving vehicle, 14 m/s to show medium speeds, and 28 m/s to show vehicle with high-speed. The minimum simulation run time observed is 121 simulation seconds for 10 vehicles running at a maximum speed of 28 m/s while the maximum simulation run time is observed as 707 simulation seconds for 150 vehicles running through all the regions with respective maximum speed limit per region.

TABLE 4. Simulation setup.

Parameters	Values
Frequency	5.9 GHz
Channel bandwidth	10 Mhz
IEEE 802.11p data rate	6 $Mbps$
Number of RSU	6
Total area	2.5 $km \times 2.5$ km
Number of Regions	3
Route Lengths	1.7 km, 1.9 km, 2.2 km, 5.8 km
Vehicular density	(10-150)
Simulation time	707 max
Vehicle speeds	10 m/s, 14 m/s, 28 m/s
Beacon frequency	200 Hz
Proposed secure beacon size	348 $bytes$
Unsecured beacon size (without cryptographic overhead)	200 $bytes$

A total number of six RSUs were placed at the locations such that maximum number of passing by vehicles can use RSUs as relay in order to get cryptographic credentials from the CA. The beacon size for the unsecured beacons is set to 200 bytes while the size of propose beacons is set to 348 bytes according to the section V-C.

B. PERFORMANCE MATRIX

The performance of our proposed approach is evaluated by comparing unsecured beacons with the secure beacons of our proposed approach with respect to mean end-to-end delay, successful beacon delivery ratio (or successful packet delivery ratio), and percent packet loss. The communication is single-hop broadcast.

It can be noted that the packet loss and end-to-end delay incurred by the beacons increase with the increase in traffic

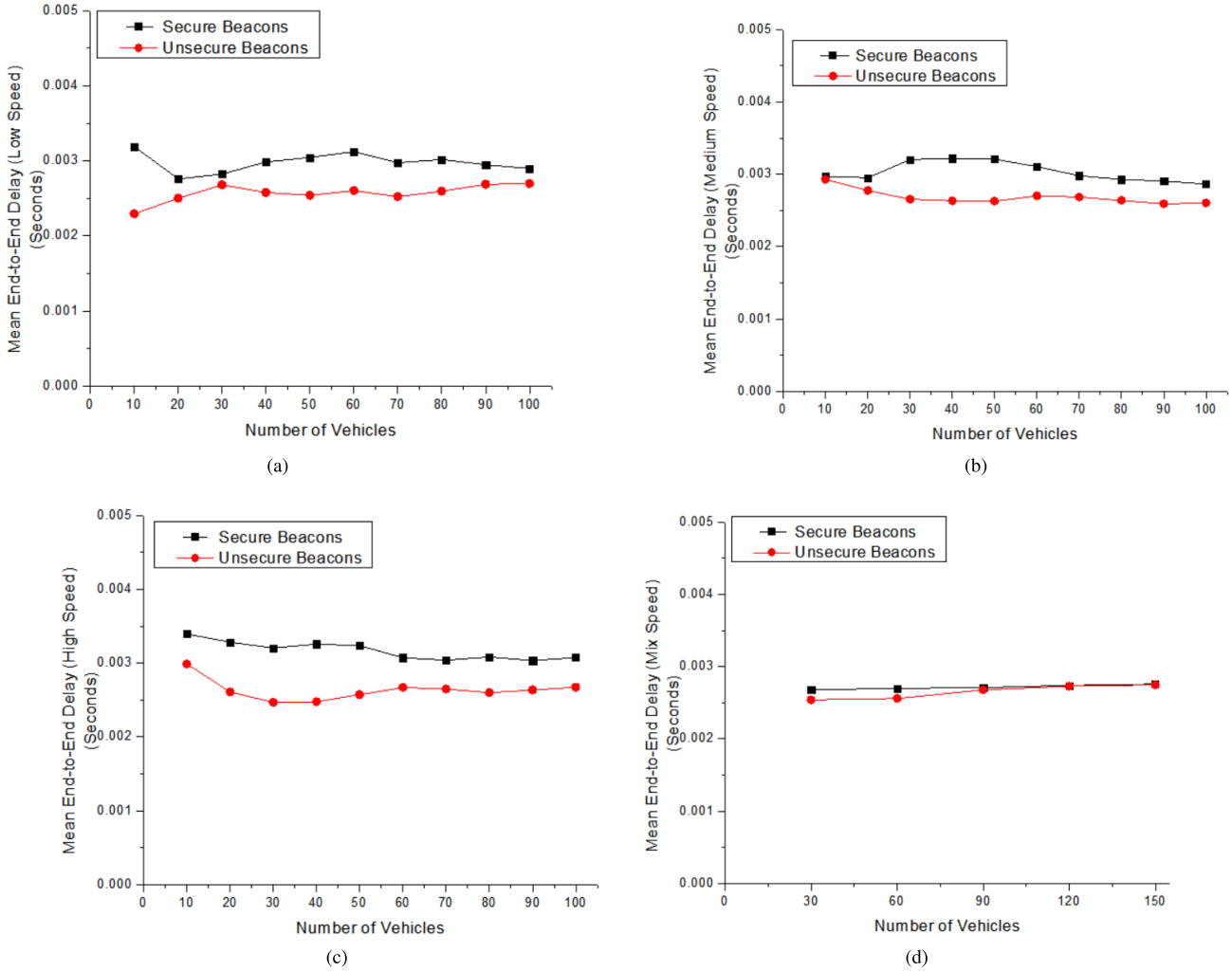

FIGURE 6. End-to-End delay w.r.t. speed. (a) End-to-end delay (low speed). (b) End-to-end delay (medium speed). (c) End-to-end delay (high speed). (d) End-to-end delay (mix speed).

density and vehicles' speed. The end-to-end delay mainly occurs due to the factors such as propagation delay, transmission delay, processing delay and queuing delay. Packet loss mainly occurs due to increased channel utilization. Therefore, we observe a performance degradation due to increasing vehicles' speed and channel utilization. The simulation results are discussed in the light of aforementioned simulation setup.

1) END-TO-END DELAY

It is important to discover the impact of cryptographic overhead on the end-to-end delay with increasing number of vehicles and speeds. The results obtained from the simulation are shown in Fig. 6. Fig. 6(a) corresponds to low speed region and it can be seen that there is no significant difference between end-to-end delay for unsecured beacons and our proposed beacons. We observe a small difference between both types of beacons till the number of vehicles increases to 40. As the number of vehicle increases beyond 40, the gap opens a little more. However, the maximum difference is very small (0.0008 seconds). This increase in end-to-end delay is due to the fact that slow moving vehicles become more and more congested, more beacons are being received and, therefore, our secure beacons occupy slightly more bandwidth and exhibits a slight increase in delay. However, after the traffic becomes more dense, (around 70-80 vehicles), the difference in the size of the beacons due to overhead start to become negligible. Fig. 6(b) and Fig. 6(c) follows the same pattern. In this case, the difference in end-to-end delay between unsecured beacons and proposed beacons increases slightly early, for around 30 vehicles and 20 vehicles in medium speed and high speed regions respectively. This is due to the added factor of higher speed of vehicles and therefore, beacons with cryptographic overhead experience slightly more but negligible end-to-end delay. Fig. 6(d) shows a more stable and average result for mix regions due to varying speeds and obstructions faced by vehicles in both cases. Moreover, it is observed that as the traffic density increases, the difference of end-to-end delay

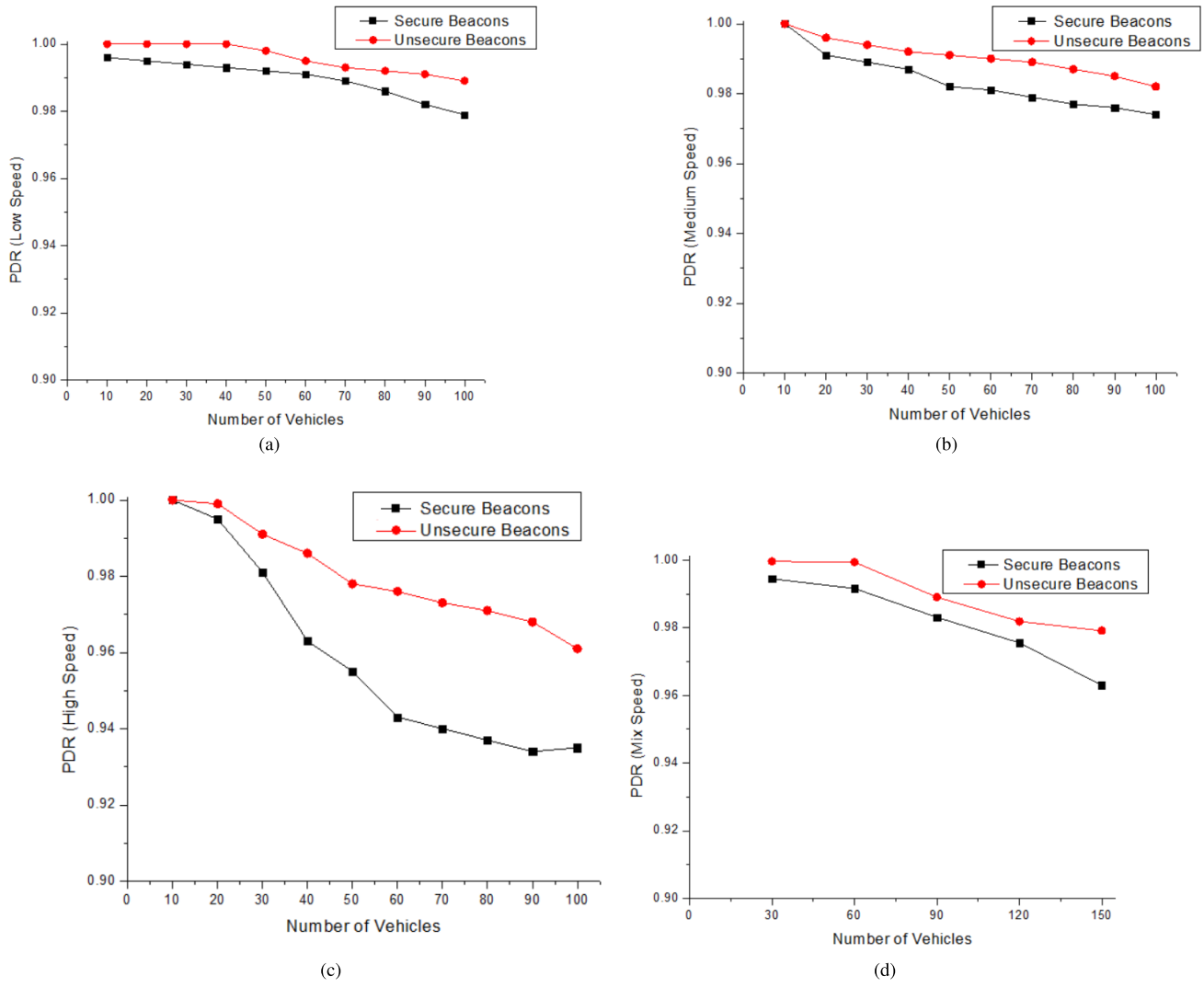

FIGURE 7. Packet delivery ratio (PDR) w.r.t. speed. (a) PDR (low speed). (b) PDR (medium speed). (c) PDR (high speed). (d) PDR (mix speed).

between both kinds of beacons becomes smaller and stable. Therefore, we can conclude that the difference of end-to-end delay between both types of beacons is very small and remains consistent.

2) PACKET DELIVERY RATIO (PDR)

Packet delivery ratio (PDR) is defined as the ratio of successful delivery of packets over the total number of sent packets. We randomly choose vehicles during multiple runs of the simulations for both the cases of secure and unsecured beacons and observed the surrounding number of vehicles in (or near) line-of sight of the observed vehicle in order to get the total number of sent beacons to that vehicle. The results obtained are shown in Fig. 7. Fig. 7(a) shows the PDR for slow speed region. We observe near 100% packet delivery ratio for up to 40 vehicles for unsecured beacons that gradually decreases to 99% for 100 vehicles. The secure beacons show a decrease in the PDR of 0.004 at the start that gradually degrades to a PDR of around 0.975 in case of 100 vehicles. Therefore, we observe a performance degradation of only 1-2% in case of slow moving vehicles. Fig. 7(b) shows a relatively decreased PDR in the start for both types of beacons. However, the difference in PDR increases to approximately 0.01 and remains stable after 50 vehicles. Fig. 7(c) shows the difference in PDR for both types of beacons in high speed region. Here, we observe relatively bigger difference in performance. The difference in PDR starts increasing after 50 vehicles and reaches to a maximum difference of around 0.03, where 100 high speed vehicles exhibit a PDR of 0.96 for unsecured beacons while vehicles broadcasting secure beacons show a PDR of 0.93. This is due to the reason that faster moving vehicles experience more signal-to-interference-plus-noise ratio as well as low Received Signal Strength Indication (RSSI). This loss affects the slightly large size packets of unsecured beacons a bit more. However, from 80 vehicles onwards, this difference observed to be remains consistent. In case of mix regions as shown in Fig. 7(d), we observe a difference in PDR of 0.02 for up to 150 vehicles.

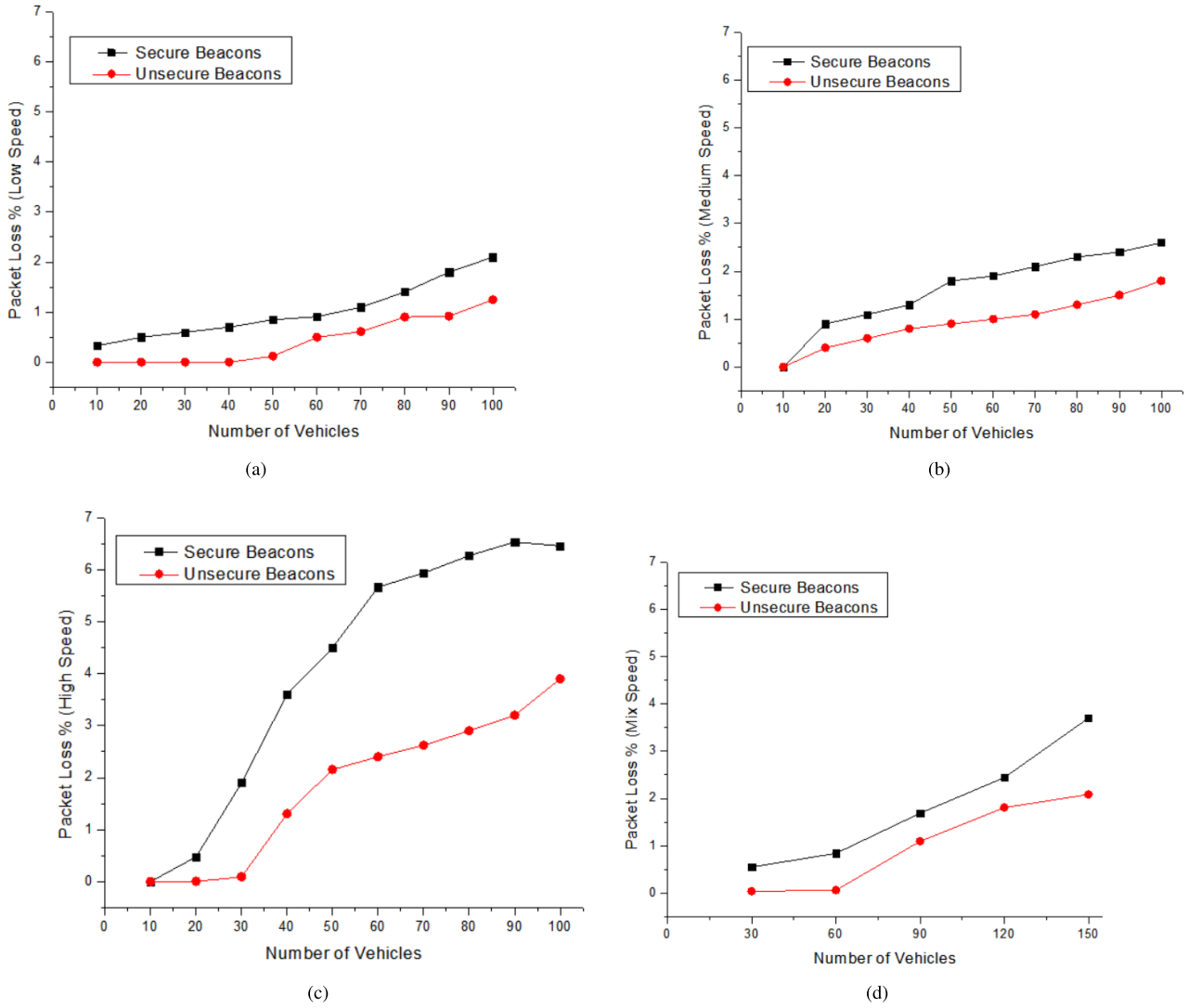

FIGURE 8. Packet loss w.r.t. speed. (a) Packet loss (low speed). (b) Packet loss (medium speed). (c) Packet loss (high speed). (d) Packet loss (mix speed).

3) PACKET LOSS

Another criterion to evaluate network performance is the mean packet loss that shows the average number of dropped packet by each vehicle. The results observed during the simulation are shown in Fig. 8. Fig. 8(a) shows the result for the vehicles of the low speed region. The effects of low speed congested traffic can be observed here. As the traffic becomes denser, there is slight increase in packet loss. The effect of slightly higher speeds results in a slightly higher packet loss in medium speed region as shown in Fig. 8(b). However, the difference between packet loss for both the unsecured and secure beacons does not exceed 2%. Fig. 8(c) shows packet loss for high speed vehicles that reaches to around 7% in case of our proposed beacons and 4% in case of unsecured beacons. In almost all the cases, the difference remains consistent after the traffic becomes denser. However, the difference does not become more than 3-4%. In case of mix regions, difference in packet loss can be observed as only 2% for up to 150 vehicles, as shown in Fig. 8(d).

In each of the case, i.e., end-to-end delay, PDR and packet loss, we observe that our proposed secure beacons are not showing any significant performance degradation. The maximum loss in all three parameters does not exceed 3-4% of loss and remains consistent in scaling traffic conditions. Therefore, we conclude that the network performance of our proposed approach does not degrade much while providing a desired level of security and privacy.

VII. CONCLUSION AND FUTURE WORK

This paper proposed an efficient approach for providing conditional privacy in VANET. The hybrid approach caters the individual flaws of pseudonym-based and group-signature based approaches. This research makes several contributions including proposing a light-weight pseudonym with trapdoor

mechanism that eliminates the need of CRL. The efficient mechanism of trapdoor provides traceability. The approach also proposes a modular architecture for the CA by keeping in view the scalability issues and deployment on a cloud computing platform. These modules efficiently handle the various requirements of the network such as vehicle registration, generation and distribution of pseudonyms and regional cryptographic credentials and vehicle revocation. Another significant contribution of this work is the proposed concept of geographical regions in a VANET environment where a number of vehicles anonymously communicate each other in the region. Moreover, we provide a detailed security analysis to show the robustness of the proposed approach while the communication and storage analysis shows that our approach is efficient and light-weight. The detailed network analysis of the proposed approach shows the feasibility of the proposed approach in terms of end-to-end delay, packet delivery ratio and average packet loss.

In the future work, we aim to reduce the cryptographic overhead on secure beacons and implement the proposed approach for more than two lanes in urban and highway scenarios.

REFERENCES

[1] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proc. 4th IEEE Int. Conf. Comput., Commun. Netw. Technol.*, Jul. 2013, pp. 1–6.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[3] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop Hot Topics Netw. (HotNets-IV)*, 2005, pp. 1–6.

[4] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1229–1237.

[6] B. Bellur, "Certificate assignment strategies for a PKI-based security architecture in a vehicular network," in *Proc. IEEE GLOBECOM*, Nov. 2008, pp. 1–6.

[7] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[8] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw.*, 2007, pp. 19–28.

[9] U. Rajput, F. Abbas, J. Wang, H. Eun, and H. Oh, "CACPPA: A cloud-assisted conditional privacy preserving authentication protocol for VANET," in *Proc. 16th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGrid)*, May 2016, pp. 434–442.

[10] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[11] M. Raya and J.-P. Hubaux, "The security of vehicular ad Hoc networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2005, pp. 11–21.

[12] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[13] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[14] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[15] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[16] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[17] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer, 1984, pp. 47–53.

[18] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

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

[20] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–6.

[21] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, "Revocable ring signature," *J. Comput. Sci. Technol.*, vol. 22, no. 6, pp. 785–794, Nov. 2007.

[22] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks," in *Proc. 4th Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services (MobiQuitous)*, Aug. 2007, pp. 1–8.

[23] A. Amer *et al.*, "Attacks on inter vehicle communication systems—An analysis," in *Proc. WIT*, 2006, pp. 189–194.

[24] Y. V. Singh, S. Misra, and M. Afaque, "Security in vehicular ad hoc networks," in *Security Self-Organizing Networks: MANET, WSN, WMN, VANET*. New York, NY, USA: Taylor & Francis, 2010, p. 227.

[25] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[26] J. M. de Fuentes, A. I. Gonzalez-Tablas, A. Ribagorda, "Overview of security issues in vehicular ad hoc networks," in *Handbook of Reseach on Mobility and Computing*, M. M. Cruz-Cunha, F. Moreira, Eds. Pennsylvania, PA, USA: IGI Global, 2010, pp. 1–17.

[27] *Certicom Research, Sec 1: Elliptic Curve Cryptography*, accessed on Jan. 15, 2017. [Online]. Available: http://www.secg.org/sec1-v2.pdf

[28] *Certicom Research, Sec 2: Recommended Elliptic Curve Domain Parameters*, accessed on Jan. 15, 2017. [Online]. Available: http://www.secg.org/sec2-v2.pdf

[29] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer-Verlag, 2006.

[30] *Veins*, accessed on Jan. 20, 2017. [Online]. Available: http://veins.car2x.org/

[31] *OMNeT++*, accessed on Jan. 20, 2017. [Online]. Available: https://omnetpp.org/

[32] *SUMO*, accessed on Jan. 20, 2017. [Online]. Available: http://sumo.dlr.de/wiki/Main_Page

[33] F. Abbas, R. Hussain, J. Son, and H. Oh, "Privacy preserving cloud-based computing platform (PPCCP) for using location based services," in *Proc. 6th IEEE/ACM Int. Conf. Utility Cloud Comput. (UCC)*, 2013, pp. 60–66.

[34] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, Mar. 2015.

[35] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014.

[36] *Elliptic Curve Qu-Vanstone (ECQV)*, accessed on Jan. 16, 2017. [Online]. Available: http://csrc.nist.gov/groups/ST/ecc-workshop-2015/presentations/session2-ford-warwick.pdf

[37] *Certicom Research, Sec 4*, accessed on Jan. 17, 2017. [Online]. Available: http://www.secg.org/sec4-1.0.pdf

[38] J.-H. Yang and C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Comput. Secur.*, vol. 28, nos. 3–4, pp. 138–143, May/Jun. 2009.

[39] Q. Arain *et al.*, "Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks," *China Commun.*, vol. 14, no. 4, pp. 89–100, Apr. 2017.

[40] Q. Arain *et al.*, "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Pers. Commun.*, pp. 1–17, 2017, doi:10.1007/s11277-016-3906-4.

[41] I. Memon, Q. Arain, M. H. Memon, F. A. Mangi, and R. Akhtar, "Search me if you can: Multiple mix zones with location privacy protection for mapping services," *Int. J. Commun. Syst.*, 2017, doi:10.1002/dac.3312.
[42] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[43] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. IEEE Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108.

UBAIDULLAH RAJPUT (S'14) received the bachelor's degree in computer system engineering from Quaid-e-Awam University of Engineering, Science and Technology (QUEST), Pakistan, in 2005 and the master's degree in computer system engineering from NUST, Islamabad, Pakistan, in 2011. He is currently working toward the Ph.D. degree in computer engineering with Hanyang University, South Korea. He has ten years of teaching and research experience and was an Assistant Professor with QUEST before taking study leave and coming to South Korea. His research interests include security and privacy issues in vehicle ad hoc networks, crypto-currency, Internet of Things, mobile social networks, and cloud computing.

FIZZA ABBAS (M'17) received the bachelor's degree in computer system engineering from Quaid-e-Awam University of Engineering, Science and Technology (QUEST), Pakistan, in 2007; the master's degree in communication system and networks from Mehran University, Pakistan, in 2011; and the Ph.D. degree in computer engineering from Hanyang University, South Korea, in 2017. She has nine years of teaching experience as an Assistant Professor with QUEST. Her research interests include security and privacy issues in social network services, mobile social networks, cloud computing, mobile cloud computing, and vehicle ad hoc networks.

HASOO EUN (M'11) received the B.S. and M.S. degrees in computer science and engineering from Hanyang University, South Korea, in 2010 and 2012, respectively, where he is currently working toward the Ph.D. degree in computer science and engineering. His research interests include information theory, network security, cryptographic protocols, homomorphic encryption, and functional encryption.

HEEKUCK OH (M'13) received the B.S. degree in electronics engineering from Hanyang University in 1983, and the M.S. and Ph.D. degrees in computer science from Iowa State University in 1989 and 1992, respectively. In 1994, he joined the Faculty of the Department of Computer Science and Engineering, Hanyang University, where he is currently a Professor. His research interests include network and system security. He is President Emeritus with Korea Institute of Information Security & Cryptology and is a member of the Advisory Committee for Digital Investigation in Supreme Prosecutors' Office of the Republic of Korea. He is also a member of the Advisory Committee on Government Policy under the Ministry of Government Administration and Home Affairs.