IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 29, 2016, accepted October 17, 2016, date of publication October 25, 2016,
date of current version November 28, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2620999

A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET

UBAIDULLAH RAJPUT, (Student Member, IEEE), FIZZA ABBAS, (Student Member, IEEE), AND HEEKUCK OH, (Member, IEEE)
Department of Computer Science and Engineering, Hanyang University, Ansan 15588, South Korea

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

This work was supported in part by the National Research Foundation of Korea by the Korean Government Ministry of Education, Science and Technology under Grant NRF-2015R1D1A1A09058200 and in part by the Ministry of Science, ICT and Future Planning, Korea, under the Information Technology Research Center supervised by the Institute for Information & communications Technology Promotion (IITP) under Grant IITP-2016-H8501-16-1018.

ABSTRACT Vehicular ad hoc network (VANET) is a technology that enables smart vehicles to communicate with each other and form a mobile network. VANET facilitates users with improved traffic efficiency and safety. Authenticated communication becomes one of the prime requirements of VANET. However, authentication may reveal a user's personal information such as identity or location, and therefore, the privacy of an honest user must be protected. This paper proposes an efficient and practical pseudonymous authentication protocol with conditional privacy preservation. Our protocol proposes a hierarchy of pseudonyms based on the time period of their usage. We propose the idea of primary pseudonyms with relatively longer time periods that are used to communicate with semi-trusted authorities and secondary pseudonyms with a smaller life time that are used to communicate with other vehicles. Most of the current pseudonym-based approaches are based on certificate revocation list (CRL) that causes significant communication and storage overhead or group-based approaches that are computationally expensive and suffer from group-management issues. These schemes also suffer from trust issues related to certification authority. Our protocol only expects an honest-but-curious behavior from otherwise fully trusted authorities. Our proposed protocol protects a user's privacy until the user honestly follows the protocol. In case of a malicious activity, the true identity of the user is revealed to the appropriate authorities. Our protocol does not require maintaining a CRL and the inherent mechanism assures the receiver that the message and corresponding pseudonym are safe and authentic. We thoroughly examined our protocol to show its resilience against various attacks and provide computational as well as communicational overhead analysis to show its efficiency and robustness. Furthermore, we simulated our protocol in order to analyze the network performance and the results show the feasibility of our proposed protocol in terms of end-to-end delay and packet delivery ratio.

INDEX TERMS Vehicular adhoc network, authentication, privacy, pseudonyms.

I. INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network (MANET) where smart vehicles act as mobile nodes and their movement is governed by road topologies [1]. The aim to develop VANET is to provide drivers and passengers with a reliable and safe environment. A typical VANET environment is composed of vehicles and infrastructure as shown in Fig. 1. The vehicles communicate each other with the help of vehicle-to-vehicle (V-2-V) communication and with Road-Side Unit (RSU) with the help of vehicle-to-infrastructure (V-2-I) communication. Each vehicle is equipped with an On-Board Unit (OBU) that has computational and communication capabilities [2]. According to Dedicated Short Range Communication (DSRC) standard, a vehicle periodically broadcasts traffic and safety related messages known as beacons [3]. These beacons contain information such as vehicle's speed, location, direction and traffic events such as congestion or accident. This information helps drivers forming a contextual view of traffic conditions that enable them to avoid situations like congested routes or accidents. However, the privacy of such information is critical because it may reveal whereabouts of a traveler. For instance, starting and ending positions of a private vehicle can often be the address of home and office of a commuter.

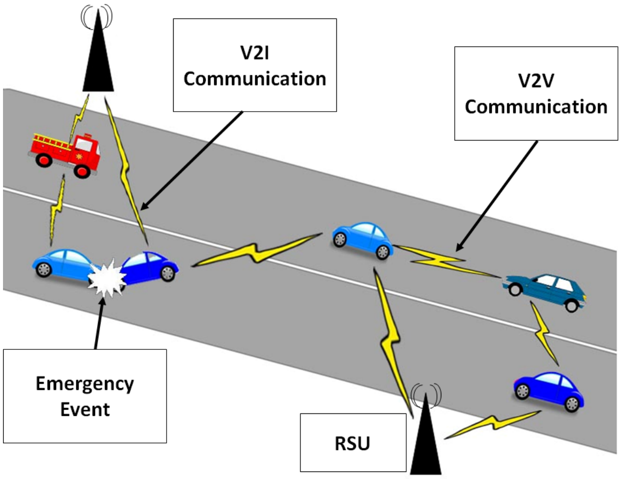


FIGURE 1. Typical VANET scenario.

Besides, there is a risk involved if attackers beacon the bogus information to gain an unfair advantage in case of road congestion, or at worse, cause an accident that may result in loss of human life. A legitimate user must be authenticated in order to take part in the VANET. However, authentication of a legitimate user in such an environment is challenging. This is mainly due to the fact that authentication often involves some identity information such as driving license or vehicle's number plate. Therefore, revealing such information may jeopardize the privacy of the user. It is desired to authenticate a user while keeping his/her privacy intact. In case a malicious activity is detected, the mechanism should be able to identify the malicious user. These scenarios make security and privacy a critical challenge in VANET and for a successful deployment these issues need to be resolved [4], [5].

A number of privacy preserving authentication schemes have been proposed recently. We can broadly categorize these schemes into pseudonymous-based schemes [5]–[7] and group signature-based schemes [8]. Additionally, there are other approaches namely RSU assisted approach [6], Mix-zones, and silent period [9]. However, these schemes propose pseudonym changing and distribution strategies and hence can be considered a subset of aforementioned broad categories. These schemes attempt to resolve many of the security and privacy related issues in VANET, but each has its own limitations. Most of the pseudonymous-based schemes implement public key infrastructure (PKI) by employing digital signatures to authenticate messages but this approach may involve significant delays [10]. As mentioned in [10], verification of a signature requires around 20 ms by an OBU equipped with a 400 MHz processor. This may not be an issue in a sparsely populated vehicular environment, but in a densely populated area, this may cause significant delays during message verification. Another significant disadvantage of most of the pseudonymous-based schemes is the certificate revocation list (CRL). A certification authority (CA) issues a number of pseudonymous public key certificates to a vehicle. The vehicle then signs the beacon with the private key, attaches the corresponding public key certificate and broadcasts the beacon. However, in case of a revocation, all certificates associated with the revoked vehicle are needed to be added in to the CRL. As the number of revoked vehicle grows, the CRL grows exponentially. Each time a vehicle receives a beacon message, the attached certificate is needed to be checked for an entry in CRL by the OBU. This causes significant processing and communication overhead for an OBU and therefore makes such schemes almost impractical. Pseudonymous-based schemes also suffer from trust issues, as these schemes require complete trust of CA and sometimes RSU as well. The CA has all the information of vehicles and in case of an attack on CA, or if the CA becomes malicious, the users' privacy may be jeopardized. The RSUs are located in open spaces and a side channel attack can compromise the RSU's security/privacy. The group signature-based schemes have certain disadvantages as well. As mentioned in [11], the pairing operation needed to check the association between the signature and the identity requires significant overhead on the processor of an OBU. Another disadvantage of group signature-based schemes is the group management issues. Group managers are able to track the members, as they have complete knowledge of group members. Therefore, the selection of group manager becomes tricky. Vehicle may join or leave the group at any time in a dynamic environment and the newly joined group manager may have all the knowledge of members.

In this paper, we propose a hierarchical pseudonymous-based protocol that authenticates a vehicle during the communication with other vehicles in network and provides conditional anonymity. Therefore, unless a vehicle involves in a malicious activity, it is hard to trace the vehicle. However, in case a malicious activity is detected, the culprit is tracked and subsequently revoked from the network. To the best of our knowledge, our proposed protocol is the first effort to present the idea of avoiding the CRL while using pseudonyms and presenting hierarchical pseudonyms that differ from each other with respect to their time to live. Our protocol also supports the sparse RSU deployment. The expiration time of pseudonyms can be adjusted according to the sparse/dense RSU distribution. This paper is the extended version of our preliminary effort [12] and it covers state of the art regarding pseudonymous authentication issues and more detailed analysis with extensive simulation results. After scrutinizing the previously proposed research efforts, the main contributions of this paper are as follows:

- We propose the idea of hierarchical pseudonyms. The primary pseudonyms are used to communicate with the CA, RSU and can be used for a relatively longer time period. The secondary pseudonyms are short lived and are used to authenticate the beacon broadcast.
- The CA keeps the association between the encrypted real identities of vehicles and primary pseudonyms. However, the identities are encrypted with the public key

of revocation authority (RA) and therefore CA cannot know the real identities of the vehicles.

- Once encrypted, RA does not have any access to the CA database.
- Only upon detecting a malicious activity, the Law Enforcement Agency (LEA) asks RA to provide the decryption key to the CA in order to reveal the real identity of the culprit primary pseudonym holder.
- The CA does not require distributing the ever-growing CRL to RSUs.
- The protocol only expects an honest-but-curious behavior from the CA, RA and RSU.
- RSU does not know the real identity of the vehicle and only knows the primary pseudonyms that are periodically changed by a vehicle.
- The beacons broadcasted by a vehicle are signed with the private key of associated public key inherent in the secondary pseudonym.
- In case the database of the CA is compromised, no valuable information is revealed to attackers.
- RSU does not hold information regarding the real identities of the user. In case of a side channel attack on RSU, no valuable information is revealed to the attackers.
- The protocol only provides conditional anonymity. In case a malicious activity is detected, the real identity can be revealed to the LEA. However, a legitimate user is provided with the privacy guarantees. Therefore, it is very hard for an attacker to get the real identity of a vehicle.
- With the help of security analysis and extensive simulations, we show the efficiency, robustness, feasibility, and applicability of our protocol.

The rest of the paper is organized as follows. Section II presents the related work. Section III explains the preliminaries of the protocol. In Section IV, we present the proposed pseudonymous authentication protocol that is followed by security and communicational analysis in Section V. Section VI presents the results obtained during the simulation, while the Section VII concludes the paper.

II. RELATED WORK

A number of researchers have put forward their efforts regarding privacy preserving authentication. We can categorize these research efforts into two broad categories. First is the pseudonymous-based authentication and the second is the group signature-based authentication. Most of the pseudonymous-based schemes are implemented with the help of Public Key Infrastructure (PKI). These schemes use PKI based certificates that are attached with the signed beacon messages with corresponding private keys. A pseudo identity is attached with a certificate and the relation between the actual identity and pseudonym is known to the provider of pseudonyms which normally is the Certification Authority (CA). In one of their pioneer work, Raya and Hubaux [13], distribute thousands of pseudonyms among vehicles with corresponding private keys. The sender of the beacon message selects any of the pseudonyms and signs the message with the corresponding private key. The receiver of the beacon message is able to verify the pseudonym with the corresponding certificate. In case of detection of a malicious activity, the real identity is revealed by the CA. Reference [14] proposes the concept of a Hardware Security Module (HSM) or Temper Proof Device (TPD) in order to enhance the security of the cryptographic material stored in a vehicle's OBU. However, these schemes have obvious drawbacks. First, there is considerable communicational and storage overhead involved during the distribution and storage of thousands of pseudonyms. Secondly, in case of a revocation, CA needs to revoke all the pseudonymous certificates issued to the vehicle and therefore, CRL grows exponentially. Sun et al. [15] propose to use the hash chains in order to reduce the size of the CRL. Moreover, they employ proxy re-signature scheme in order to improve the time to update the certificates. Authors of [16], use an identity-based batch verification scheme. They use TPD to generate random pseudo-identity based certificates and corresponding private keys. The scheme is prone to Denial-of-Service (DoS) attack and is less efficient than symmetric cryptography. Lu et al. [6] propose another conditional privacy preserving protocol where the short time pseudonym keys are acquired by OBU from RSU but the drawback is the assumption of pervasive deployment of RSUs. Another disadvantage is the use of trusted authority that needs to frequently update RSUs with the CRL.

In group signature-based authentication schemes [8], [17], [18], a group of vehicles is formed and the privacy preservation is provided by hiding the real identity of the message sender among the other group members. The message is signed by the individual group key and subsequently verified by the group public key certificate. Authors of [17], use identity-based signatures where the RSU signs and authorize each of the messages. Another advantage is the reduced size of CRL in group signatures as it grows linearly with the number of revoked vehicles. Calandriello et al. [19] propose a hybrid scheme that combines the features of pseudonymous-based and group signature-based schemes. However, this scheme is computationally infeasible as it requires to check that a message is from a revoked vehicle. The scheme presented in [18], introduces an interesting idea of using RSUs as group managers to maintain and manage the groups of vehicles. The vehicles entering into the jurisdiction of a RSU can send anonymous messages that are verifiable by the group members of the same group but also verifiable by the vehicles of the neighboring groups. The scheme assumes a pervasive deployment of RSU that share the system load and therefore, the overall performance of the system improves. However, the same assumption can also be regarded as a drawback of this scheme due to the requirement of pervasive deployment of RSUs acting as group managers. Xiong et al. [20] use revocable ring signature scheme, proposed by Liu et al. [21] in order to achieve conditional privacy. However, the revocation information must be distributed through revocation lists to all vehicles. Recently, Rajput et al. [22] proposed a hybrid scheme that avoids the disadvantages of both the pseudonymous-based and group signature-based schemes and provides the conditional anonymity. The authors proposed the idea of grouping vehicles and assign a common key pair to the group members. However, this scheme assumes the pervasive deployment of RSUs.

Upon reviewing the literature, we deduce the following limitations. Pseudonymous-based schemes incur significant computational, communicational and storage overhead due to the presence of ever growing CRL. As the number of vehicles grow in the network, the CRL grows exponentially. The group signature-based schemes suffer from the inherent requirement of group management tasks. The vehicles serving as group managers need to be trusted. There is group management overhead as well as computational overhead due to pairing based calculations. Another common problem is the need to have full trust on CA or other third parties.

This paper attempts to cater aforementioned issues by proposing the concept of hierarchical pseudonyms. Our proposed protocol neither involves any group management overhead nor does it require managing any CRL. Moreover, our proposed protocol does not require full trust of CA, RA and RSU but expects only an honest-but curious behavior from these authorities. The CA issues the primary pseudonym as well as keeps the association between the primary pseudonym and the real identity of a vehicle. However, the real identities in CA's database are encrypted by another entity knows as Revocation authority (RA) and therefore, CA is unable to decrypt these real identities. Once a vehicle is involved in a malicious activity, appropriate authority such as LEA allows RA to provide the decryption key in order to decrypt the real identity of the culprit in CA's database. Secondary pseudonyms are issued by RSU upon successful verification of the primary pseudonym. A vehicle then broadcasts a message signed by the associated private key of the secondary pseudonym and the receiving vehicle verifies the message with associated public key provided in the secondary pseudonym.

III. PRELIMINARIES

This Section describes system model, attack model, design goals, assumptions and the cryptographic tools used in this paper.

A. SYSTEM MODEL

According to [23], each vehicle is uniquely identified with some vehicle identity. We subsequently refer this identity as *VID* in the rest of the paper. The *VID*, sometimes referred as Electronic License Plate (ELP), is issued and installed in a vehicle's OBU by a vehicle registration authority such as Department of Motor Vehicles (DMV). The *VID* serves as the real identity of the vehicle in our protocol by considering the fact that a vehicle is usually driven by 3-4 persons at most. A vehicle in our protocol is required to provide the *VID* to the CA in order to get the first primary pseudonym. However, the issuance of *VID* from DMV has not been considered in this paper. We assume that, at the time of the registration of the vehicle with the DMV, *VID* is issued and installed in the vehicle's TPD. Our system model constitutes of the following participants.

1) *Certification Authority (CA):* The CA issues the primary pseudonyms and keeps the association between the primary pseudonyms and encrypted *VID* of a vehicles. We describe the details of *VID* encryption in the next subsection. Once the primary pseudonym expires, the vehicle needs to request for a fresh primary pseudonym from CA. This can be done in two ways. First is by requesting thorough RSU located in the area where the vehicle is currently traveling. The other way is by directly requesting the CA through 3G/4G communications. In case a malicious activity is detected, the Law Enforcement Agency (LEA) provides the culprit's primary pseudonym to CA. Furthermore, LEA instructs revocation authority (RA) to provide CA with the decryption key of the associated *VID* of the malicious primary pseudonym. The CA decrypts and reveals the real *VID* of the malicious vehicle to the LEA and the malicious vehicle is subsequently revoked from the network. The LEA can find the real identity of the owner of the malicious vehicle by providing the malicious *VID* to the DMV.
2) *Revocation Authority (RA):* During vehicle registration, the RA generates a public/private PKI key pair and encrypts the vehicle's *VID*. The plaintext *VID* is deleted by the CA. Once a vehicle is found to be involved in a malicious activity, the LEA instructs RA to provide the decryption key of the encrypted *VID* associated with the primary pseudonym of the malicious vehicle to the CA.
3) *Roadside Units (RSUs):* Secondary pseudonyms are issued by RSU upon request from a vehicle. The requesting vehicle needs to provide the primary pseudonym to the RSU. Upon successful verification of the primary pseudonym, the RSU provides the secondary pseudonym to the requesting vehicle, otherwise discards the request. The RSU keeps the association between primary and secondary pseudonyms. Once the secondary pseudonym expires, the vehicle needs to acquire a new secondary pseudonym from the RSU. Similarly, if the primary pseudonym is expired, the vehicle needs to acquire a new primary pseudonym from the CA. In case a bogus beacon is reported to the LEA, the RSU provides LEA with the primary pseudonym associated with the secondary pseudonym present in the bogus beacon.
4) *Sender Vehicle:* The sender vehicle (or initiator of the beacon message), denoted by V_i in the rest of the paper, signs the beacon message with the private key whose corresponding public key is mentioned in the secondary pseudonym. The initiator then broadcasts the signed beacon message along with the secondary pseudonym.

5) *Receiver Vehicle:* The receiving vehicle verifies the message with associated key provided in the secondary pseudonym. In case the message is bogus, the receiver reports this beacon along with the attached secondary pseudonym to the LEA. If any of the signatures is not verified, the message is simply discarded by the receiving vehicle.

B. ATTACK MODEL

The attack model considers various types of adversaries with different capabilities. First are the internal and external adversaries. Both the sender and the receiver of the message may assume the role of an authenticated internal adversary. They both may try to deviate from the protocol in order to reveal the real identity of the other. The external adversary acts as an intruder and his/her attacks may be limited to eavesdropping. There are active and passive attackers. In order to trace a vehicle, capabilities of passive attackers are limited to attacks such as eavesdropping. The active attacks may include injecting bogus or forged messages into the network. We have local and global adversaries whose eavesdropping capabilities range from a single RSU to many RSUs. We consider CA, RA and RSU as honest-but-curious. These entities may have interest tracking a vehicle while honestly following the protocol. We consider side-channel attacks on storage of an RSU but do not consider that the RSU remains functional after the compromise. Similarly, we also consider attacks on CA database.

C. DESIGN GOALS

The design goals of the proposed protocol are as under:

- **Privacy Preserving Authentication**
  First and the most important objective is to ensure the authenticity of a legitimate user without revealing his/her real identity. The receiver vehicle should be able to authenticate sender and the beacon without knowing sender's real identity.
- **Message Integrity**
  The protocol must also preserve the integrity of the message. The contents of the message sent by the sender vehicle should be delivered unaltered to the receiver vehicle.
- **Non-Repudiation**
  One of the very important requirements is non-repudiation. A sender vehicle must not be able to deny the ownership of the message. In other words, once a message is authenticated, it proves the ownership of the sender vehicle. If the message was altered or replayed by an attacker, the receiver must not be able to verify it.
- **Pseudonym Revocation**
  Once a pseudonym is revoked, an insider should not be able to use it again.
- **Vehicle Revocation**
  Once a vehicle is revoked, it should not be able to take part in the network.
- **Conditional Anonymity**
  The protocol should provide conditional anonymity. By conditional anonymity we mean that the privacy of a vehicle is preserved until it follows the protocol honestly. In case of a malicious activity, the real identity of the vehicle is revealed by the LEA.

D. ASSUMPTIONS

We have made following assumptions in our protocol.

1) We expect an honest-but-curious behavior from CA, RA, and RSU.
2) Any collusion between CA, RA and RSU is not considered.
3) We assume that the vehicles' OBUs can store received messages for a period of time. In case of detection of a malicious activity, these recordings are presented to the LEA.
4) All parties keep their cryptographic credentials safe.
5) All parties' clocks are synchronized.
6) The CA, RA, RSU and LEA use secure channel for communication with each other.

E. CRYPTOGRAPHIC TOOLS

Two separate cryptosystems have been used in this protocol. For simple public key infrastructure (PKI) operations the protocol utilizes Elliptic Curve Cryptography (ECC) [26]–[28], while for the homomorphic operations, Paillier homomorphic cryptosystem has been used [24]. It should be noted that only CA and RSU need to use Paillier cryptosystem while the rest of the participants use ECC. Following are the details of ECC and the variant of Paillier homomorphic cryptosystem that is used in our protocol [25]. This variant supports the negative inputs.

1) PAILLIER ENCRYPTION

A Paillier encryption is a non-deterministic cryptosystem [24]. In a non-deterministic cryptosystem, the encryption results are non-deterministic instead of deterministic. Therefore, the encryption of same plaintext may map to two different ciphertexts at two different encryptions processes.

$$C_1 = E_k(M), C_2 = E_k(M), C_3 = E_k(M), \ldots, C_n = E_k(M)$$

The Paillier cryptosystem significantly facilitates the provision of guaranteed security of the designed protocols. Paillier cryptosystem is an additive homomorphic cryptosystem; that implies, given only the public-key and the encryption of m_1 and m_2, one can compute the encryption of $m_1 + m_2$. As per the requirement of our proposed protocol, the negative inputs are realized by dividing the ring of n into two parts and considers any plaintext $m \geq \frac{n}{2}$ as negative. The variant of the Paillier cryptosystem have the following steps:

Key Generation: Generate two large prime numbers p and q each with half the specified modulus bit length for the cryptosystem.

- $gcd(pq, (p-1)(q-1) = 1$ and $p \neq q$.
- Modulus $n = pq$ and pre-compute n^2.

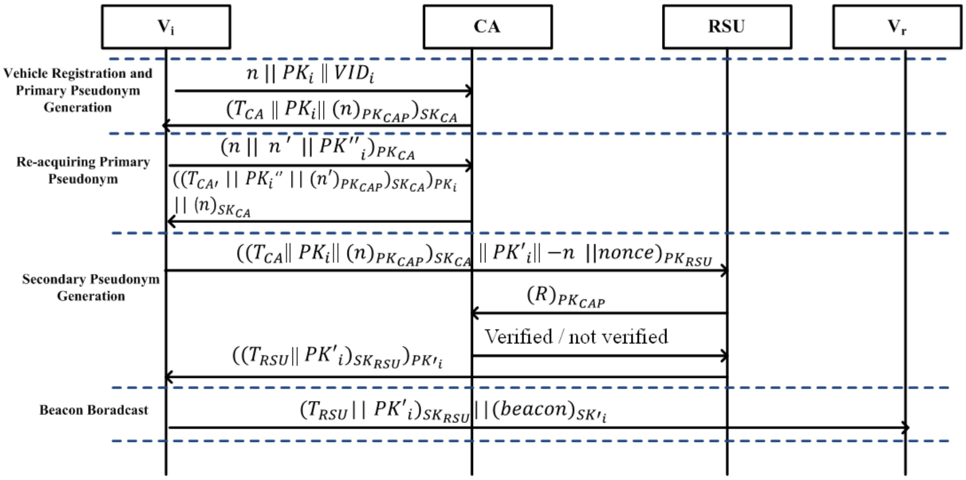

$\mathrm{V_i}$
CA
RSU
$\mathrm{V_r}$
Vehicle Registration and Primary Pseudonym Generation
$n \,||\, PK_i \,\|\, VID_i$
$(T_{CA} \,\|\, PK_i\| \,(n)_{PK_{CAP}})_{SK_{CA}}$
Re-acquiring Primary Pseudonym
$(n \,||\, n' \,||\, PK''_{i})_{PK_{CA}}$
$((T_{CA'} \,||\, PK_i'' \,||\, (n')_{PK_{CAP}})_{SK_{CA}})_{PK_i} \,||\, (n)_{SK_{CA}}$
Secondary Pseudonym Generation
$((T_{CA}\| \,PK_i\| \,(n)_{PK_{CAP}})_{SK_{CA}} \,\|\, PK'_i\| -n \,\|nonce)_{PK_{RSU}}$
$(R)_{PK_{CAP}}$
Verified / not verified
$((T_{RSU}\| \,PK'_{i})_{SK_{RSU}})_{PK'_i}$
Beacon Boradcast
$(T_{RSU} \,||\, PK'_{i})_{SK_{RSU}} \,||\, (beacon)_{SK'_i}$

FIGURE 2. Working of proposed protocol.

- Compute $\lambda = lcm(p-1), (q-1) = \dfrac{(p-1)(q-1)}{gcd(p-1, q-1)}$.
- $g \leftarrow (1+n)$. {optimized but originally selects random $g \epsilon Z^*_{n^2}$ such that n divides the order of g}.
- $gcd(L(g^\lambda \text{mod } n^2), n = 1$ where $L(u) = \frac{u-1}{n}$.{Optimization: g^λ mod $n^2 = (1 + n\lambda)$ mod n^2}.
- Pre-compute the modular multiplicative inverse $\mu = L(g^\lambda \text{mod } n^2)^{-1}$ mod n.
- **return** Public Key : (n, n^2, g) and Private Key : (λ, μ).

Encryption:

Require : Plaintext $m \epsilon Z_n$

- Choose random $r \epsilon Z^*_n$.
- **return**: Ciphertext $c \leftarrow (1+mn)\, r^n$ mod n^2. {Optimized here but originally: $c \leftarrow g^m r^n$ mod n^2}.

Decryption:

Require: Ciphertext $m \epsilon Z^*_{n^2}$.

- **return:** Plaintext $m \leftarrow L(c^\lambda$ mod $n^2)\mu$ mod n.

2) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

We have utilized Elliptic Curve Cryptography (ECC) as the cryptographic tool in our protocol. For encryption, Elliptic Curve Integrated Encryption Scheme (ECIES) has been used while for the signature we have used 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 the encrypted message with padding, ephemeral public key and HMAC. Following is the brief introduction of ECC.

TABLE 1. Notations.

Notations	Explanation
V_i	Initiator/Sender vehicle
V_r	Receiver vehicle
VID_i	Initiator's/Sender's vehicle ID
$PK_i, SK_i, PK'_i,$ SK'_i, PK''_i, SK''_i	ECC public/ private key pairs of V_i
PK_{CA}/SK_{CA}	ECC public/private key pairs of CA
PK_{CAP}	Paillier public key pair of CA
PK_{RSU}/SK_{RSU}	ECC public/ private key pair of RSU
$T_{CA}, T_{CA'}$	Expiration time of primary pseudonym set by CA
T_{RSU}	Expiration time of secondary pseudonym set by RSU
Beacon	Typical VANET message

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 the form of $E_p(a, b) : y^2 = x^3 + ax + b(modp)$, over a prime finite field F_p, where a, $b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0(modp)$ [30].

In general, the security of ECC depends on the difficulties of the following problems [26], [29], [30].

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 $s \cdot P = Q$.

Definition 2: *Computational Diffie-Hellman Problem (CDHP)*

Given three points P, sP and tP over $Eq(a, b)$ for $s, t \in F_p$, the computational Diffie-Hellman problem finds the point $(s.t).P$ over $Ep(a, b)$.

IV. PROPOSED PROTOCOL

In our proposed protocol, a user needs to register with the CA in order to get the primary pseudonym. The primary pseudonym has a life time and expires after that period of time. This period of time is denoted as T_{CA} in our protocol and set by CA at the time of primary pseudonym generation. Fig. 2 shows the working of the proposed protocol while Table I shows the notation used in our protocol. In the following we present our proposed protocol.

A. SYSTEM INITIALIZATION

CA initializes the system by establishing the domain parameters p, a, b, G, n and h.

1) Let the field is defined by p.
2) The cyclic group is defined by its base point G.
3) n is the order of G.
4) a, b are curve constant.
5) cofactor $h = 1/n|E(E_p)|$.

All of the participants of the protocol download these parameters from CA. CA randomly chooses $x \in Z_{p^*}$ as its private key. Similarly, other participants generate their credentials. Note that, RA generates a number of public/private ECC key pairs and provides CA the public keys, that are later used by CA for VID encryption. It is worth mentioning here that we have used two different n. One is used as the order of the group G and the other is used as a random number in the protocol.

B. VEHICLE REGISTRATION AND PRIMARY PSEUDONYM GENERATION

During the registration, sender/initiator vehicle (V_i) generates a random number n (This random value is later encrypted in CA's Paillier public key) and a public/private ECC key pair PK_i/SK_i. V_i sends this information along with the VID_i to CA.

Step 1: $V_i \rightarrow$ CA : $n||PK_i||VID_i$.

The V_i sends this information to the CA via some secure channel (for example vehicle visits the CA). Step 1 is required only once.

CA validates the VID_i. Upon verification it encrypts VID_i with one of the public keys generated by RA, encrypts n with its paillier public key PK_{CAP}, generates an expiration time T_{CA} and creates the following database (DB) entries as shown in Table II.

TABLE 2. Example of CA database.

User Serial	Data
...	...
n	$(VID)_{PK_{RA}}\|\|T_{CA}\|\|PK_i$
...	...

- CA → DB : $(VID_i)_{PK_{RA}}||T_{CA}||PK_i||n$
- CA signs $(T_{CA}||PK_i||(n)_{PK_{CAP}})$, and assigns it to V_i as its first primary pseudonym.

Step 2: CA→V_i : $(T_{CA}||PK_i||(n)_{PK_{CAP}})_{SK_{CA}}$

C. RE-ACQUIRING PRIMARY PSEUDONYM

Once the T_{CA} expires, V_i needs to acquire the primary pseudonym again. In this regard, V_i randomly select some n', generates a public/private ECC key pair PK_i''/SK_i'', encrypts this data in public key of CA along with n and sends it to CA using 3G/4G communication.

Step 3: $V_i \rightarrow$ CA: $(n||n'||PK_i'')_{PK_{CA}}$

In case, the vehicle requests the re-acquiring of primary pseudonym to CA via RSU then it sends this message to the nearby RSU that forwards this request to the CA. For such a request, some special purpose bits in the message can be used that enables the RSU to identify that a vehicle is requesting for primary pseudonym via RSU or the vehicle is requesting the RSU for a new secondary pseudonym.

Step 3': $V_i \rightarrow$ RSU→ CA: $(n||n'||PK_i'')_{PK_{CA}}$

CA verifies this message with correct n, generates new expiration time $T_{CA'}$, update its database with new values of n', PK_i'' and the $T_{CA'}$. CA repeats step 2, but encrypts the newly generated primary pseudonym in PK_i'' and sends back to V_i. In case, the request has come from RSU then CA sends this message to V_i through RSU along with the signed n. The signed value of n creates an association with the new value of n'. When the RSU broadcast this message, V_i identifies it with old n, verifies CA's signature, decrypt it and changes its primary pseudonym. Due to encryption, RSU is unable to relate the new primary pseudonym to the V_i.

Step 4: CA $\rightarrow$:$V_i((T_{CA'}||PK_i''||(n')_{PK_{CAP}})_{SK_{CA}})_{PK_i''}||(n)_{SK_{CA}}$

D. SECONDARY PSEUDONYM GENERATION

RSU periodically broadcasts a message announcing its presence. This message also contains the public key of the RSU. Once a vehicle receives this message it requests for the secondary pseudonym. The vehicle generates another public/private ECC key pair (PK_i', SK_i'). It encrypts this newly generated public key, its primary pseudonym, $-n$ and a nonce in RSU's public key and sends it to the RSU.

Step 5 : V_i $\rightarrow$ RSU $((T_{CA}||PK_i||(n)_{PK_{CAP}})_{SK_{CA}}||PK_i'||-n||nonce)_{PK_{RSU}}$.

RSU verifies CA's signature, encrypts $-n$ with paillier public key of CA. RSU takes homomorphic sum of both $(n)_{PK_{CAP}}$ and $(-n)_{PK_{CAP}}$, gets $(R)_{PK_{CAP}}$. Where $(R)_{PK_{CAP}}$ $=(n)_{PK_{CAP}} + (-n)_{PK_{CAP}}$

RSU sends $(R)_{PK_{CAP}}$ to CA for verification.

Step 6: RSU → CA: $(R)_{PK_{CAP}}$

CA decrypts R, finds 0 $(n + (-n) = 0)$ and sends *verified* message to RA otherwise sends *not verified*.

Step 7: CA → RSU: verified / not verified.

CA only gets a encrypted value that provides no hint about which vehicle is using this value. The value of $-n$ is used to prevent an impersonation attack as mentioned in Section V-A (Theorem 2).

Upon getting verification that the message came from V_i, RSU prepares a secondary pseudonym. It creates the expiration time T_{RSU}, embed it with newly generated PK_i', signs it, encrypts in PK_i' and sends it to V_i. Note that, PK_i' has to be generated by V_i every time a secondary pseudonym is requested. However, a vehicle can pre-compute a pool of ECC key pairs.

Step 8: RSU → V_i: $((T_{RSU}||PK_i')_{SK_{RSU}})_{PK_i'}$.

E. BEACON BROADCAST

V_i signs the beacon message with the private key whose associated public key is contained by the secondary pseudonym.

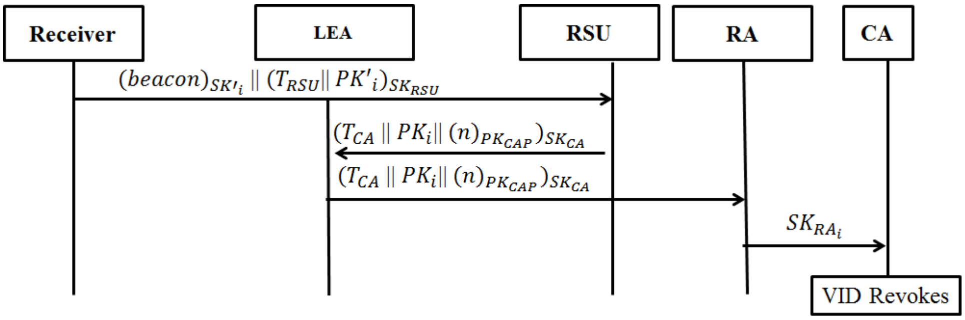

Receiver
LEA
RSU
RA
CA
$(beacon)_{SK'_i} \,||\, (T_{RSU}||\, PK'_i)_{SK_{RSU}}$
$(T_{CA} \,||\, PK_i||\, (n)_{PK_{CAP}})_{SK_{CA}}$
$(T_{CA} \,||\, PK_i||\, (n)_{PK_{CAP}})_{SK_{CA}}$
SK_{RA_i}
VID Revokes

FIGURE 3. Revocation procedure of a malicious vehicle in proposed protocol.

It attaches the secondary pseudonym with the beacon and broadcasts the message.

Step 9: V_i Broadcasts: $(beacon)_{SK'_i}||(T_{RSU}||PK'_i)_{SK_{RSU}}$

The receiver of the message verifies the pseudonym by checking the RSU's signature and then verifies the beacon by verifying the V_i's signature with the help of PK'_i contain in the secondary pseudonym.

F. VEHICLE REVOCATION

As shown in Fig. 3, if a user is found to be involved in broadcasting a bogus message then the culprit is traced and revoked by the following way.

- The receiver presents the recordings of the malicious message (step 9) to the LEA.
- LEA contacts the RSU that signed the secondary pseudonym attached with the bogus message.
- RSU provides LEA with the corresponding primary pseudonym.
- LEA instructs the RA to provide the decryption key of the encrypted *VID* whose associated primary pseudonym is found to be malicious.
- RA provides the corresponding decryption key to CA along with a revocation request.
- CA decrypt the *VID* of the malicious party and revokes it.

The contents of a beacon message are used to construct the traffic view. The typical transmission range of a vehicle is around 300 meters. Therefore, the contents of a bogus traffic report will be verifiable within minutes. The victim will immediately complain the LEA with the recordings of the bogus message. Therefore, the beacon messages needed to be recorded for a short time period with an upper bound of 30-60 minutes.

V. ANALYSIS OF THE PROPOSED PROTOCOL

This Section provides the analysis of our protocol with two perspectives. First is the security analysis, where we provide various attack scenarios and explain the resilience of our protocol against those attacks to show the effectiveness of the protocol in accordance with the design goals. Next, we provide the communicational overhead in form of excess bytes due to the encryption.

A. SECURITY ANALYSIS

1) *Privacy Preserving Authentication:*
In our protocol, only RA has the secret key of the encrypted real identity (*VID*). However, RA does not have access to the encrypted values in the database of CA. Moreover, our protocol requires that a user vehicle should acquire a new primary pseudonym after a certain time period that is set by CA, and therefore, the RSU will find it very hard to correlate a user because of his changing primary pseudonyms. At the RSU side, after every few message broadcast, a new secondary pseudonym is used. Therefore, it is very hard for an attacker to correlate the secondary pseudonyms of the vehicle.
2) *Message Integrity:* The beacon message broadcasted in step 9 is signed by the private key of the sender vehicle. The associated public key is contained in the secondary pseudonym for verification. Therefore, the message integrity is preserved.
3) *Non-Repudiation:* The beacon message broadcasted in step 9 is signed by the private key whose associated public key is contained by the secondary pseudonym. The beacon message itself contains the current time stamp as well as a nonce. No other vehicle can broadcast this message and therefore, not only non-repudiation is provided but the protocol also provides prevention against replay attacks.
4) *Vehicle Revocation:* Every beacons message contains the secondary pseudonym. The RSU keeps the association between primary and secondary pseudonyms. The RSU ensures the validity of the primary pseudonym during the secondary pseudonym generation. The secondary pseudonym doest not need to be revoked due to its very short expiration time. However, the primary pseudonym has a relatively longer life time. For that purpose, as soon as a vehicle is found to be involved in a malicious activity, the RSU and CA both mark corresponding primary pseudonym as revoked. In case, the malicious vehicle attempts to renew the primary pseudonym, or attempts to acquire the secondary pseudonym, the CA and the RSU immediately finds the status of the vehicle as revoked and denies

such attempt. However, in case, of a non-pervasive RSU deployment, a relatively longer life time T_{RSU} is set by an RSU for the secondary pseudonym depending upon how far the next RSU is located. In that case, a malicious vehicle may broadcast the beacon for that time period. Once expired, the secondary pseudonym will not be issued again. We argue that there is a tradeoff here. In a pervasive RSU environment, we face no problems at all; however, in case the RSU deployment is sparse then a revoked vehicle might be able to broadcast beacons until T_{RSU} expires.

5) *Conditional Anonymity:* On detection of a maliciously activity, the real identity of the culprit is traced and subsequently revoked from the system as mentioned in Section IV-F of the protocol. However, the system guarantees the anonymity of the honest vehicles.

B. ATTACK SCENARIOS

Theorem 1: Communication between all the participants is semantically secure.

Proof: All the communication in our protocol is encrypted using ECC cryptography. According to Diffie-Hellmen Problem (DLP) given an element g and the value g^x, it is computationally infeasible for an attacker to compute secret x. Therefore, the communication is secure.

Theorem 2: An attacker tries to impersonate the sender while sending request for secondary pseudonym.

Proof: If an attacker tries to impersonate the initiator, he/she needs to get the primary pseudonym of the initiator. This primary pseudonym is send to the RSU securely and therefore, the attacker needs to compromise the RSU. However, even the attacker gets the primary pseudonym, he/she needs to provide the correct value of n. This value is only known to the initiator or the CA. Therefore, an impersonation attack is not possible.

Theorem 3: If an attacker tries to replay the message in step 5.

Proof: In step 5, we have used nonce. Therefore, a replay attack will not be succeed.

Theorem 4: If the RSU tries to correlate the pseudonyms of the initiator.

Proof: RSUs only issue secondary pseudonyms on the basis of primary pseudonym. An initiator only uses a primary pseudonym for a short period of time and after that it securely gets another primary pseudonym from CA without the knowledge of RSU. It is, therefore, very hard for the RSU to establish any link between two primary pseudonyms.

Theorem 5: If the receiver of the beacon message tries to correlate the secondary pseudonyms of a user.

Proof: The sender vehicle changes the secondary pseudonyms after a few beacon broadcasts. After every few beacons the receiver vehicle receives the beacon containing a different secondary pseudonym. Therefore, it is very hard for a receiver to establish any correlation between rapidly changing secondary pseudonyms.

Theorem 6: If an attacker succeeds in compromising RSU.

Proof: RSU only has the mapping between current primary pseudonym and associated secondary pseudonym. The primary pseudonyms are subjected to change after a short period of time. Therefore, it is very hard for an attacker to get any useful information by compromising any of the RSUs.

Theorem 7: If an attacker succeeds in compromising CA database.

Proof: The database of CA contains encrypted *VIDs*. Therefore an attacker only gets encrypted *VIDs* and currently associated primary pseudonyms. Unless, the attacker has the private keys of the RA, he/she cannot get the real identities of the users. However, this prevention does not secure the system if the compromised CA continues to be operational.

C. COMMUNICATIONAL COST ANALYSIS

This subsection presents the communication cost of various messages that are communicated in our proposed protocol. Following is the message size for the primary and secondary pseudonyms as well as total message size including encryption overhead for the messages that are communicated between different participants of our proposed protocol. The primary pseudonym size is 354 bytes and the secondary pseudonym is of 98 bytes. The request for the secondary pseudonym by a vehicle requires a message size of 468 bytes. The response from RSU comprises of 164 bytes of encrypted secondary pseudonym. Finally, the broadcasted beacon's size is 362 bytes in total.

1) PRIMARY PSEUDONYM

$(T_{CA}||PK_i||(n)_{PK_{CAP}})_{SK_{CA}}$ where

- $T_{CA} = 2$ byte, $PK_i = 32$ byte (one point on ECC curve), $(n)_{PK_{CAP}} = 256$ bytes and ECDSA signature= 64 bytes.

The total size is 354 bytes

2) SECONDARY PSEUDONYM

- $T_{RSU} = 2$ bytes and $PK_i' = 32$ bytes, signature $= 64$ bytes.

The total size is 98 bytes.

3) REQUEST FOR SECONDARY PSEUDONYM

$V_i \longrightarrow$ RSU: $((T_{CA}||PK_i||(n)_{PK_{CAP}})_{SK_{CA}}||PK_i'|| - n||nonce)_{PK_{RSU}}$ where

- $(T_{CA}||PK_i||(n)_{PK_{CAP}})_{SK_{CA}} = 354$ bytes, $PK_i' = 32$ bytes, $-n = 10$ bytes, nonce $= 10$ bytes, $PK_{RSU} = 32$ bytes, padding $= 10$ bytes and HMAC 20 bytes.

The total size is 468 bytes.

4) RSU RESPONSE FOR SECONDARY PSEUDONYM REQUEST

- RSU $\longrightarrow V_i$: $T_{RSU} = 2$ bytes and $PK_i' = 32$ bytes (ephemeral key), PK_i' 32 bytes (vehicle's public key), signature $= 64$ bytes, padding $= 14$ bytes and HMAC $=$ 20 bytes.

The total size is 164 bytes.

5) RE-ACQUIRING OF PRIMARY PSEUDONYMS

$(n||n'||PK_i'')_{PK_{CA}}$

- $n = 10$ bytes, $n' = 10$ bytes, $PK_i'' = 32$ bytes, $PK_{CA} =$ 32 bytes, padding = 12 bytes and HMAC= 20 bytes.

Total size of message is 116 bytes.

6) BEACON BROADCAST

Secondary pseudonym = 98 bytes, beacon data = 200 bytes, signature = 64 bytes.

Total size of message is 362 bytes.

The beacon encryption overhead incurs only 162 bytes and shows that our protocol is light-weight.

D. COMPARISON WITH EXISTING APPROACHES

This subsection provides the comparison of our protocols with existing approaches such as pseudonymous authentication-based and group signature-based.

First of all, our protocol does not require the creation and distribution of a large number of pseudonyms. Due to this reason, our protocol does not need storage required for storing a large pool of pseudonyms. Not using a Certificate Revocation List (CRL) is another major advantage. Neither the protocol needs any CRL management requirements nor does it require computational and communicational overhead related to CRLs. The protocol also does not utilize any of the concept of group-based approaches. Hence, there is no need of group management and costly group signature computations.

Finally, our protocol does not require trusted entities like CA or RSU. If a server is compromised, no valuable information is leaked that reveals the real identity of the user. Table III shows the comparison of the protocol with existing approaches.

TABLE 3. Comparison with existing approaches.

Parameters	Pseudonym-based	Group-based	Proposed Protocol
Creation, distribution & storage requirement for large number of pseudonyms	✓	×	×
Management of Revocation list	✓	✓	×
Group management	×	✓	×
Valuable information leaked if server is compromised	✓	✓	×

VI. PERFORMANCE EVALUATION

In this Section we discuss performance evaluation of proposed protocol.

A. COMPUTATIONAL OVERHEAD

In this subsection, we evaluate the computational overhead incurred by the RSU during the secondary pseudonym generation. The RSU processes the secondary pseudonym request of a vehicle by executing various cryptographic primitives. Therefore, it is desired to know that the time taken by the RSU to process one request on average and subsequently, we measure the simultaneous requests by the vehicles that can be entertained by the RSU. We also evaluate the computational overhead incurred by a vehicle during the beacon generation and verification.

TABLE 4. Computational cost of proposed protocol.

	Encryption Overhead	Time
RSU processing overhead	1 ECC decryption 1 ECC signature verification 1 Paillier encryption 1 ECC Encryption 1 ECC Signature generation	0.025 seconds
Vehicle processing overhead	1 ECC Signature generation 2 ECC signature verification	0.0006 seconds 0.005 seconds

1) TEST BED AND RESULTS

Our test bed consists of an intel i7 processor with 16 GB of RAM in order to simulate the RSU. To calculate the execution time, we developed an application in JAVA due to its rich support for calculating cryptographic primitives. We calculated the execution time required by RSU during the secondary pseudonym generation that involves ECC encryption and decryption, Paillier encryption, and ECC signature generation and verification. The test was run for 100 times in order to get the average values. The results obtained are shown in Table IV. The total computational time taken by the RSU in order to serve the pseudonym change request is around 0.025 seconds, while the beacon verification by a vehicle requires only around 0.005 seconds. Therefore, if the pseudonym change request time interval of vehicles is set to 1.4 seconds then the RSU can simultaneously process around 55 vehicles in this time interval. Similarly, the time taken by a vehicle in signature generation and verification is observed to be sufficient enough such that, the vehicle generates beacons within recommended beacon frequency as well as verifies a large number of beacons (approximately 40 beacons) in order to construct a broader traffic view.

B. NETWORK SIMULATION RESULTS

In this subsection, we evaluate the performance of our proposed protocol in two major aspects. First is the performance of inter-vehicle beacon communication with respect to unsecure beacons that do not incur any encryption overhead, and the secured encrypted beacons of our protocol. For convenience, we will refer the beacon without any cryptographic overhead as conventional beacon in the rest of the paper. The second aspect is the performance evaluation of RSU, where vehicles frequently request the RSU for secondary pseudonym by providing primary pseudonym. In this case, RSU verifies the primary pseudonym contains in the request and then generates and sends the secondary pseudonym to the requesting vehicle. Therefore, it is important to verify that the RSU is able to perform this task on a consistent basis while serving a number of vehicles. We assume that conventional beacons are unencrypted and therefore, we compare them with the encrypted beacons of our protocol in order to show that there is no significant difference in the performance of our secure beacons and that of conventional beacons; however, our proposed protocol provides security against various threats mentioned in attack model.

According to Raya et al. [13], [14], the conventional beacon size is 200 bytes. We encrypt our beacons as detailed in subsection V-C and therefore, the size of encrypted beacons follows aforementioned section of this paper. We consider end-to-end delay, beacon reception rate, and packet loss as performance matrices for conventional beacons and our proposed encrypted beacons. In the VANET environment, the speed of the vehicles also plays an important part while considering end-to-end delay, beacon reception rate, and packet loss. Therefore, we also analyzed the performance matrices with different vehicle speeds as well. First we consider end-to-end delay incurred by both conventional and encrypted beacons.

For that purpose, we analyzed the end-to-end delay of the traffic at varying density and at various maximum speeds running on two single lane routes. The simulation results are discussed in the next subsection. Next, the successful beacon delivery ratio is analyzed with respect to both the encrypted and unencrypted beacons broadcasted by vehicles with varying maximum vehicle speeds and densities. Finally, we show mean packet loss. To analyze the performance of RSU, the encryption, decryption, signature generation and verification timings were calculated by developing a JAVA application and appropriate service time delay was introduced in RSU between secondary pseudonym request arrival and appropriate response (providing secondary pseudonym or denying the request otherwise). The performance matrix for the RSU is to successfully entertain a number of vehicles requesting at a time without dropping a significant number of requests.

1) *Simulation Setup:* In this subsection, we explain our simulation results and compare conventional beacons with our proposed encrypted beacons. The main characteristic of VANET is its unique topology and high-speed mobility patterns exhibited by moving vehicles. Traditionally VANET simulators consist of two components. One is the wireless network simulator and the other is the road traffic simulator. We simulate our protocol with the help of Veins [31] that is an open source framework for running vehicular network simulations. Veins is based on two simulators: One is OMNeT++ [32], an event-based network simulator that carries out wireless network based simulations and the other is SUMO [33], a road traffic simulator to perform realistic traffic simulations. Veins extends these two simulators in order to provide a comprehensive suite of models for inter-vehicle communication. We utilized the map of urban scenario provided by Veins and generated a number of vehicles moving along multiple routes in east-to-west direction in a city environment with varying maximum speeds. The routes contain straight road sections where vehicles can attain there maximum speeds as well as quick turns where slow speed vehicles may form a small cluster. The straight road sections also allow a number of vehicles to be in line of sight (LOS) of each other in order to receive a large number of beacons. The routes also contain relatively open spaces as well as those with more buildings. Table V explains simulation setup.

To analyze our proposed protocol, we simulated a number of scenarios with varying number of vehicles at different maximum speeds. The vehicles mostly follow each other during the simulation. The number of vehicles are ranging from 10 vehicles up to 70 vehicles and the mean data is collected for every 10 vehicles interval. In our scenarios, 10 vehicles show sparse traffic that gradually becomes dense up to 70 vehicles with an increment of 10 vehicles. The maximum vehicle speeds were set to 20 m/s to exhibit slow moving vehicle, 25 m/s to show medium speeds, and 30 m/s to show vehicle with high-speed. The minimum simulation run time observed was 230 simulation seconds for 10 vehicles running at a maximum speed of 30 m/s while the maximum simulation run time was observed as

TABLE 5. Simulation setup.

Parameters	Values
Frequency	5.9 GHz
Channel bandwidth	10 Mhz
IEEE 802.11p data rate	6 $Mbps$
Number of RSU	1
Total area	2.5 km × 2.5 km
Routes	3 km, 4 km
Vehicular density	(10-70)
Simulation time	498 max
Vehicle speed	20 m/s, 25 m/s, 30 m/s
Beacon frequency	200 Hz
Encrypted beacon size	364 $bytes$
Standard beacon size (without cryptographic overhead)	200 $bytes$

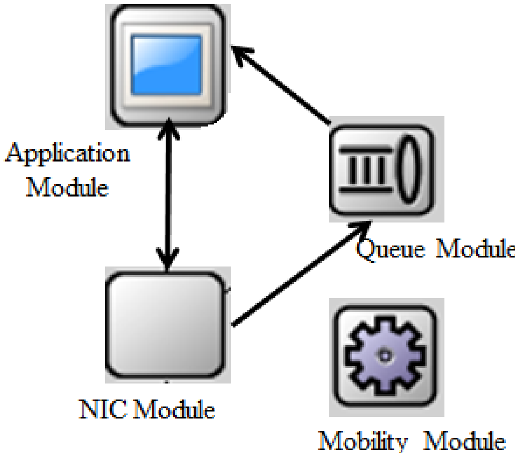
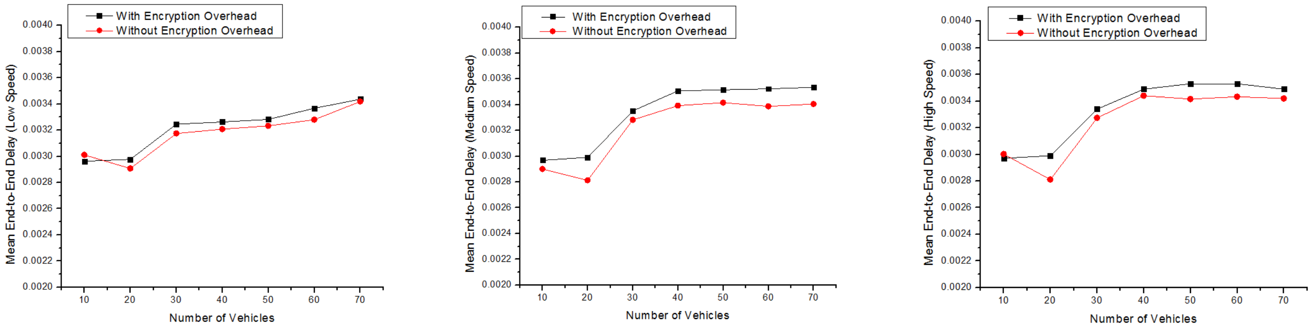


FIGURE 4. RSU implementation of our protocol in OMNeT++.



(a) (b) (c)

FIGURE 5. **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).**

498 simulation seconds for 70 vehicles running at a maximum speed of 20 m/s.

RSU was placed at a road intersection with maximum number of passing by vehicles requesting RSU for pseudonyms in order to evaluate its performance under increasing work load. Fig. 4 shows our RSU implementation in OMNeT++. We placed a small queue that can hold 10 messages between NIC module and application module of RSU. This queue keeps the incoming pseudonym requests while RSU is busy serving a request. The secondary pseudonym change frequency was set to 1.4 seconds which means every vehicle requests for pseudonym after approximately 7 beacons.

2) *Performance Matrix:* The performance of our proposed protocol is evaluated by comparing conventional beacons with the encrypted beacons of our proposed protocol with respect to mean end-to-end delay, successful beacon delivery ratio (or successful packet delivery ratio), and total packet loss. The communication is multi-hop broadcast. The RSU performance is measured by evaluating any loss of packets while receiving requests from vehicles and issuing secondary pseudonym. This evaluation shows the ability of RSU to consistently provide secondary pseudonym to the vehicles in time without dropping any significant number of requests.

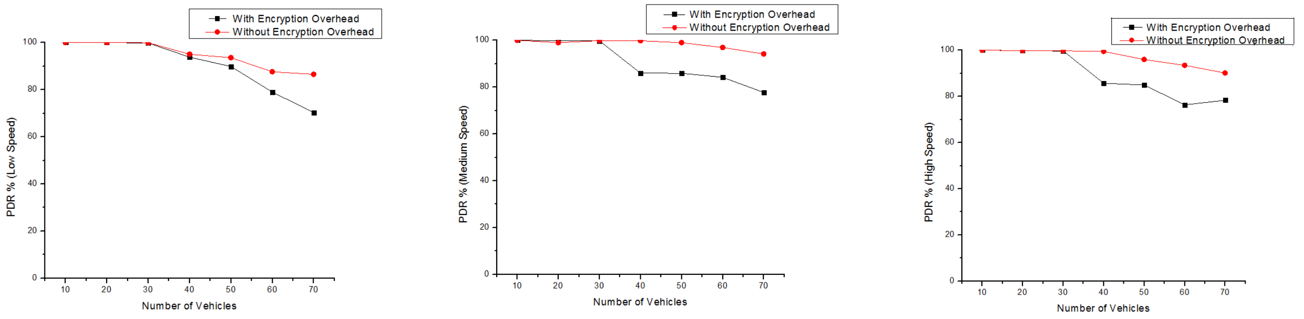
It can be noted that the packet loss and end-to-end delay incurred by the beacons increases with the increase in traffic density and vehicles' speed. This is due to the packet collisions due to high traffic density, increasing speed of vehicles and packet loss while transmitting due to high packet reception rate. 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 encryption overhead on the end-to-end delay with increasing number of vehicles and speeds. The results obtained from the simulation are shown in Fig. 5. Fig. 5(a) corresponds to low speed vehicles, and it can be seen that there is no significant difference between conventional beacons and our proposed encrypted beacons. We observe a similar increase for both types of beacons when the number of vehicles increases to 30 vehicles. This increase is due to the fact that slowly moving vehicles become more and more congested, more beacons are being received and, therefore, beacons occupies more bandwidth and exhibits a slight increase in delay. Fig. 5(b) and Fig. 5(c) follows the same pattern however, the difference between conventional beacons and encrypted beacons increases slightly. This is due to the higher speed of vehicles and therefore, beacons with encryption overhead experience slightly more end-to-end delay. However, this slightly more difference observed to be around 0.0001 of a seconds and therefore, we can conclude that the difference of end-to-end delay between both types of beacons is very small and remains consist.

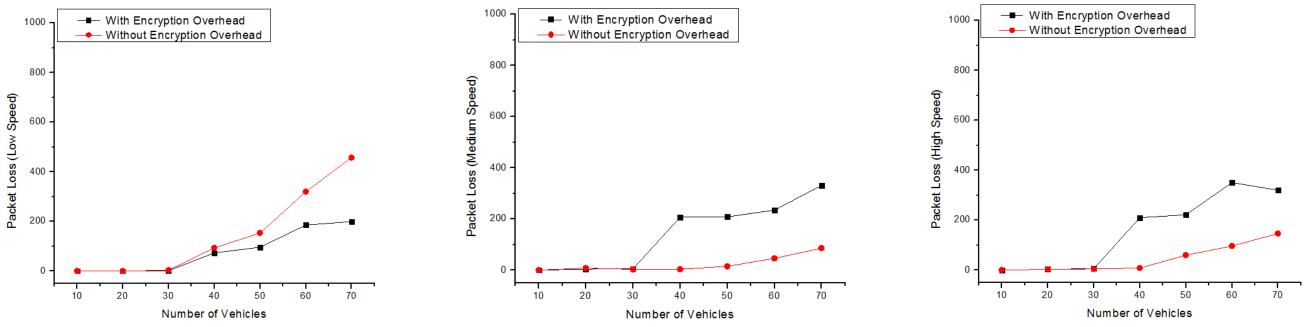
2) PACKET DELIVERY RATIO (PDR)

Packet delivery ratio is defined as the ratio of successful delivery of packets over the total number of sent packets. The results obtained are shown in Fig. 6. Fig. 6(a) shows the PDR for slow moving vehicles. We observe near 100 % packet delivery ratio for up to 30 vehicles and after that the gap gradually starts to expand. When the number of vehicles increases to 60, the difference in PDR starts to get significantly higher. This is due to the reason that, as the number of vehicles increases, the slow moving vehicles tend to get closer and the number of vehicles per unit area increases. The encrypted packets that occupy more bandwidth start to drop more than those without encryption. However, we observe that up to 60 vehicles, this difference is very small (up to 5%). We observe the PDR for medium and high speed vehicles in Fig. 6(b) and 6(c) respectively. When the number of vehicles reaches to 40, the difference between the encrypted beacons and the conventional beacons increases. 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 larger size



(a) (b) (c)

FIGURE 6. PDR (%) w.r.t. speed (a) PDR % (low speed). (b) PDR % (medium speed). (c) PDR % (high speed).



(a) (b) (c)

FIGURE 7. Packet loss w.r.t. speed. (a) Packet loss (low speed). (b) Packet loss (medium speed). (c) Packet loss (high speed).

encrypted packets more. However, from 50 vehicles upwards, this difference observed to be remains consistent.

3) MEAN 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. 7. Fig. 7(a) shows the result for low speed vehicles. We observe an increasing packet loss when number of vehicles receives more packets due to minimized gap between them and therefore, experience more packet loss due to collision. The difference between both types of beacons becomes significant when the number of vehicle reaches 70. However, we argue that 60 vehicles are a sufficient value to construct a traffic view for a vehicle. Fig. 7(b) and 7(c) shows the mean packet loss by medium and high speed vehicles. We observe a relatively high number of packet drop by encrypted beacons when the number of vehicles reaches 40. However, after that we observe a consistent difference between the two types of beacons that is around 150 packets. This makes around 10-12% of the total sent packets. We argue that this loss should be an acceptable cost for the added security provided by the encrypted beacons.

4) RSU PACKET LOSS

For RSU, we did not observe any loss of packets in application module. This was mainly due to the pseudonym change interval time that was set to 1.4 seconds. This time interval was set according to the time taken by the RSU in our implementation during the verification of primary pseudonyms and generation of secondary pseudonyms. The small queue was observed to be filled only up to 7 messages in case of 70 vehicles, and the average queuing wait time was around 0.005 seconds. However, we observed a negligible packet loss at MAC layer that was comparably much less than a vehicle due to the stationary nature of the RSU. We argue that the pseudonym change interval time can be set to a smaller value while setting an increasing queue length for the smooth operation of the RSU. This pseudonym change interval time is adjustable for sparse/dense RSU deployment or for the varying traffic load. During the rush hours as the number of vehicles grows, more RSUs are required to serve the increasing number of vehicles. In case of a sparse RSU deployment, the secondary pseudonym change interval time needs to be increased.

VII. CONCLUSION AND FUTURE WORK

This paper proposes a hierarchical pseudonymous authentication protocol with conditional privacy preservation. We proposed the novel idea of two levels hierarchy for the pseudonyms with different life time. Our protocol exhibits several advantages over current approaches such as less trust on CA, RA and RSU and no disclosure of valuable information in case of attacks on these entities. Moreover, the protocol provides conditional anonymity to the users of the network and only the involvement of a vehicle in a malicious activity reveals the real identity. The protocol incurs no overhead related to CRL and group management tasks that are otherwise used consistently by current approaches. The security analysis of our proposed protocol exhibits the resilience against various security threats. Furthermore, the performance evaluation of our proposed protocol not only shows the low computational and communication overhead, but also shows the applicability by showing little or acceptable difference in network performance in comparison with the beacons without any security. Our future work includes the implementation of the protocol with more number of RSUs in urban and highway scenarios.

REFERENCES

[1] 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 Trans. Mobile Comput.*, vol. 11, no. 1, pp. 33–46, Jan. 2012.

[2] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.

[3] DSRC Technology. *Intelligent Transportation Systems*. accessed on Feb. 15, 2016. [Online]. Available: http://www.its.dot.gov/dsrc/

[4] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. 4th Workshop Hot Topics Netw. (HotNets)*, 2005, pp. 1–6.

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

[6] 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.

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

[8] 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, Jun. 2007.

[9] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 93–105, Jan./Feb. 2016.

[10] H. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, and B. Bellur, "Flooding-resilient broadcast authentication for VANETs," in *Proc. 17th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, pp. 193–204, 2011.

[11] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *J. Comput.*, vol. 98, no. 7, pp. 1–24, 2014.

[12] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for VANET," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 643–650.

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

[14] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 13, no. 1, pp. 8–15, Oct. 2006.

[15] Y. Sun, R. Lu, X. Lin, and X. Shen, "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.

[16] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 246–250.

[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 F. J. Domingo, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[19] 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.

[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. (ICC)*, May 2010, pp. 1–6.

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

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

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

[24] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 1999, pp. 165–179.

[25] A. Basu, J. Vaidya, H. Kikuchi, T. Dimitrakos, and S. K. Nair, "Privacy preserving collaborative filtering for SaaS enabling PaaS clouds," *J. Cloud Comput.*, vol. 1, no. 1, pp. 1–14, 2012.

[26] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide To Elliptic Curve Cryptography*. Berlin, Germany: Springer, 2006.

[27] *Certicom Research, Sec 1: Elliptic Curve Cryptography*. accessed on Jun. 20, 2016. [Online]. Available: http://www.secg.org/sec1-v2.pdf

[28] *Certicom Research, Sec 2: Recommended Elliptic Curve Domain Parameters*. accessed on Jun. 20, 2016. [Online]. Available: http://www.secg.org/sec2-v2.pdf

[29] F. Li, X. Xin, and Y. Hu, "Identity-based broadcast signcryption," *Comput. Standard Interfaces*, vol. 30, nos. 1–2, pp. 89–94, Jan. 2008.

[30] 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, 2009.

[31] *Veins*. accessed on May 18, 2016. [Online]. Available: http://veins.car2x.org/

[32] *OMNeT++*. accessed on May 22, 2016. [Online]. Available: https://omnetpp.org/

[33] *SUMO*. accessed on May 22, 2016. [Online]. Available: http://sumo.dlr.de/wiki/Main_Page

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

FIZZA ABBAS (S'14) received the bachelor's degree in computer system engineering from the Quaid-e-Awam University of Engineering, Science and Technology (Quest), Pakistan, in 2007, and the master's degree in communication system and networks from Mehran University, Pakistan, in 2011. She is currently pursuing the Ph.D. degree in computer engineering with Hanyang University, South Korea. She has nine years of teaching experience and was working as an Assistant Professor with Quest before taking study leave and coming to Korea. Her research interests are security and privacy in social network services, mobile social networks, cloud computing, mobile cloud computing, and vehicle ad hoc networks.

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, ERICA campus, where he is currently a Professor. His current research interests include network and system security. He is a member of the Advisory Committee for Digital Investigation in Supreme Prosecutors' Office, Korea, and the Advisory Committee on Government Policy under the Ministry of Government Administration and Home Affairs. He is also a President Emeritus of the Korea Institute of Information Security and Cryptology.