Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.795

VANET 기반 클라우드 환경에서 안전과 프라이버시를 고려한 경로추적 및 철회 기법*

후세인 라쉬드,† 오희국‡
한양대학교

A Secure and Privacy-Aware Route Tracing and Revocation Mechanism in VANET-based Clouds*

Rasheed Hussain,† Heekuck Oh‡
Hanyang University

요 약

많은 연구 끝에 VANET의 상용화를 눈앞에 두고 있다. VANET은 차량용 애드혹 네트워크의 약자로서, Cloud와 융합하는 방향으로 연구가 진행되고 있다. 하지만 놀랍게도 VANET 기반 클라우드로 진화한데 가장 큰 역할을 한 것은 차량과 통신기술의 발달이다. 이러한 기술이 확산되는 단계에서 연구자들은 항상 보안과 프라이버시에 대해 고민해 왔다. 게다가 VANET처럼 프라이버시, 익명철회, 경로추적 등 상반된 보안 이슈들이 서로 얽힌 상황은 연구자들을 더욱 고민에 빠지게 했다. 최근 Hussain 등은 VANET 기반 클라우드 프레임워크인 VuC (VANET using Clouds)를 제안하였다. VuC는 VANET과 클라우드가 VANET 사용자(서비스 가입자)에게 서비스를 제공하기 위해 협력하는 환경을 말한다. 본 논문은 Hussain 등이 제안한 VANET 기반 클라우드 프레임워크인 VuC에 초점을 두고 있으며, 특히 앞서 말한 프라이버시, 익명철회, 경로추적에 대한 문제를 다루고 있다. 제안하는 기법은 다중 익명화를 통해 프라이버시를 보호한다. 또한 비컨(Beacon)메시지를 클라우드에 저장하여 경로추적과 익명 철회에 활용한다. 익명철회 권한을 가진 기관들은 연합하여 사용자 노드가 선택한 경로를 특정 시간 동안 추적할 수 있으며, 필요한 경우 신원을 확인할 수 있다. 제안된 기법은 안전하고 조건부 익명성을 보장하며 기존의 기법에 비해 연산량이 적다

ABSTRACT

Vehicular Ad hoc Network (VANET) has gone through a rich amount of research and currently is making its way towards the deployment. However, surprisingly it evolved to rather more applications and services-rich breed referred to as VANET-based clouds due to the advancements in the automobile and communication technologies. Security and privacy have always been the challenges for the think tanks to deploy this technology on mass scale. It is even worse that some security issues are orthogonally related to each other such as privacy, revocation and route tracing. In this paper, we aim at a specific VANET-based clouds framework proposed by Hussain et al. namely VANET using Clouds (VuC) where VANET and cloud

접수일(2014년 8월 8일), 게재확정일(2014년 10월 6일)
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학ICT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1015).
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학ICT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1044).
* 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2012R1A2A2A01046986).
* 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2012R1A1A2009152).
† 주저자, rasheed@hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr(Corresponding author)

infrastructure cooperate with each other in order to provide VANET users (more precisely subscribers) with services. We specifically target the aforementioned conflicted privacy, route tracing, and revocation problem in VANET-based clouds environment. We propose a multiple pseudonymous approach for privacy reasons and leverage the beacons stored in the cloud infrastructure for both route tracing and revocation. In the proposed scheme, revocation authorities after colluding, can trace the path taken by the target node for a specified timespan and can also revoke the identity if needed. Our proposed scheme is secure, conditional privacy preserved, and is computationally less expensive than the previously proposed schemes.
Keywords: VANET, VANET Clouds, Security, Conditional Privacy, Revocation, Route Tracing

I. Introduction

The push for Vehicular Ad Hoc NETwork (VANET) (a specialized breed of MANET-Mobile Ad Hoc NETwork) has resulted in the possible deployment of the technology in the near future. Noteworthy results have already been produced by research community in the field of VANET ranging from design all the way to security issues. Nonetheless, deployment of this technology on a mass scale has been a real challenge to date [1,2]. The main reason for such delay in the deployment stage is the unique security and privacy problems. Moreover there are many conflicting requirements such as privacy and revocation. A concrete and full privacy mechanism is favorable for the users; however, it gives room to the adversaries to exploit it and penetrate from the other ends in the form of Sybil attacks and so forth. Therefore for liability reasons, these users must be subject to revocation and in some cases the route they take must be traced, in case of any dispute such as a deadly accident or a terrorist attack. The tradeoff solution for aforementioned phenomenon is conditional privacy. Academia and research institutions have spawned their resources to take out the very roots of the security and privacy challenges in VANET [3-5].

In order to fully utilize the resources of current and near-future high-end vehicles, traditional VANET evolved to VANET-based clouds as a result of the combination of two emerging fields; VANET and Cloud Computing (CC). The main driving force behind the VANET-based clouds is that practically our cars' resources are wasted for most of the time (for instance our cars are parked and remain idle for most part of the day, i.e. tens of hours a day). It would be ideal if the car would be capable of utilizing its processing, computing, storage, and communication resources [6]. The cars could rent out the resources and earn some revenue as well.

In this paper, we aim at a specific class of VANET-based clouds framework namely VuC (VANET using Clouds) [7], and propose a revocation and route tracing mechanism for VuC. For this purpose, we particularly select a cloud-based traffic information dissemination application of VuC where beacons are stored and processed in the cloud for information dissemination and also leveraged route tracing by law enforcement authorities in case of any investigation. Note that beacons messages contain current mobility information which is used by VANET application to construct traffic views. The contributions of this paper are given below:

Conditional Privacy: We propose a multiple pseudonymous approach to conditionally preserve the privacy of the users. Our proposed pseudonyms are trapdoor-based, where in the normal circumstances, it is very hard to extract the

real ID from pseudonym unless the keys are compromised, otherwise.

Route Tracing: We model a privacy-aware mechanism on the top of our pseudonym-based privacy preserving approach, where the route taken by the user can be traced by the revocation authorities with the consensus of law enforcement agencies:

Revocation: We provide a private yet trapdoor-based pseudonymous approach which on the one hand guarantees privacy for the user, and on the other hand enables revocation authorities to revoke the user in case of a dispute.

This paper is the extended version of our work in [21]. However, in this paper, our approach is different from [21]. Due to the security and brute force overhead of the revocation and route tracing in identityless privacy-preserving approach, we introduced trapdoor-based pseudonyms that guarantee privacy to the users and guarantee liability in case of a dispute as well. The pseudonyms approach is carefully designed in order to provide the same level of privacy and reduce the revocation overhead as well as keep the adversaries at the bay to launch attacks such as Sybil attacks. Moreover, we also rigorously analyze our proposed scheme with respect to the previously proposed schemes.

The rest of the paper is structured as follows. Section II discusses the design rationale and baseline of the proposed scheme. Section III presents our proposed revocation and route tracing mechanism, followed by evaluation of our proposed scheme in section IV. State of the art is discussed in section V followed by concluding remarks in section VI.

II. Design Rational and System Model

2.1 Design Rationale

Due to its ephemeral nature, VANET requires stringent security and privacy measures. VANET technology is going to have a huge social impact on the lives of the users because users will not put their privacy at stake as a result of using such technology. Therefore any message, and or action should not be linked back to the user. On the other hand, for liability reasons, in case of dispute, users must be able to be revoked by the authorities and their routes must be traced. These two requirements clearly contradict each other. A tradeoff solution that has benefits for the both requirements, is essential. A mechanism that protects the privacy of the users as long as they are benign, and revoke their status as soon as they act maliciously, can solve this problem. Such mechanism is called conditional privacy preservation.

Since our proposed scheme is based on the beacons stored at cloud, the design rationale for the VANET services through cloud is also appealing. This approach has twofold advantages: 1) Storing large number of beacons in cloud would let the cloud to process the beacons for more fine-grained optimum location-based services. 2) The stored beacons enable authorities to carry out revocation and route tracing without any additional overhead and/or infrastructure.

2.2 System Participants

Our system integrates two technologies; VANET and CC. In VANET the system participants include department of motor vehicles (DMV), regional certification

Table 1. Notations

Notation	Explaination
V	Vehicle with OBU and TRH
G	Cyclic group of prime order q
P	The generator of G
r	Random nonce
u_V	Secret counter for pseudonym generation
o_V	Incrementing factor for pseudonym generation
s	Private master key
Pub	Public key corresponding to s
PS_V^i	ith pseudonym of vehicle V
K_V	Individual secret key of V
K_Z	Zone level secret key
K_{RSU}	RSU level key used for geoclock
K_{geolcok}	Location-based encryption key
K_{x-y}	Shared secret key between entities x and y
$h:\{0,1\}^* \rightarrow \{0,1\}^l$	Collision resistant hash function of length l
$H()$	A MaptoPoint hash function as: $H: \{0,1\}^* \rightarrow G$
$h_k()$	Keyed hash function
$\oplus$	Exclusive OR operation
$\|$	Concatenation function

authorities (RCAs), revocation authorities (RAs), road-side units (RSUs), and OBU-equipped vehicles. DMV is at the top of the management hierarchy which manages all underlying VANET entities. RCAs are autonomous and control specific reasonable size of zone which has RSUs deployed in it. Each zone anticipates its own cloud infrastructure. RAs are a number of government departments (for instance law enforcement agencies, and judiciary) to collectively revoke a node when necessary.

CC infrastructure consists of Authenticator, Cloud Knowledge Base (CKB), Cloud Processing Module (CPM), and Cloud Decision Module (CDM). RSUs, and vehicles with 4G serve as virtualization layer between VANET and CC, and forwards messages between VANET and CC back and forth.

2.3 Assumptions

1. Vehicles are equipped with onboard units (OBUs) and tamper resistant hardware (TRH), and only VANET authority is able to initialize the OBU and TRH.
2. Due to seriousness of liability issues, the revocation functionality is distributed among several physical entities which then collaboratively revoke a node by the power vested in them collectively through colluding.
3. All Messages are assembled inside TRH and RSUs are sufficiently deployed in hot spots such as cross-roads and intersections.
4. A potential healthy functional contract is present between VANET and CC authorities for service exchange. On the basis of this assumption, cloud is considered to be partially trusted and the existing standard procedures for auditing can be used by VANET authorities to maintain the trust level between the two entities.
5. RSUs serve as primary GT and 4G-containted vehicles serve as secondary GT to the cloud infrastructure.

III. Proposed Route Tracing and Revocation Scheme

3.1 Network Model

We introduce a three-layer network model as shown in Figure 1. The lowest layer is part of VANET and composed of vehicles on the road and we assume that there is enough market penetration of the OBU-equipped vehicles. The middle layer is virtualization layer and composed of VANET as well and realized by GTs (RSUs

and 4G-connected vehicles). The upper layer is the cloud layer or services layer. The main function of virtualization layer is to forward cooperation (beacons) from vehicles to the cloud and forward fine-grained services from cloud to the vehicles through GTs. The by far best example of such scenario is traffic information as a service from clouds to vehicles [9].

3.2 System Setup

The notations throughout this paper are listed in Table 1.

3.2.1 System Initialization

We use ElGamal encryption algorithm [10] over the ECC (Elliptic Curve Cryptography) [11] to encrypt K_V and K_i. Let G be a cyclic group of prime order q where G is generated by P. DMV first chooses $s \in Z_q^*$ as its private key and computes $Pub = sP$ as its public key. DMV then uses threshold based secret share scheme [12] and divides s into j parts where j is the number of revocation authorities, each carries a share s_i and $s_i = (s_1, s_2, ..., s_j)$. In order to construct s from individual s_i, must elect one of them to be group leader and construct s from combination of individual s_i.

3.2.2 TRH Initialization

The owner of the vehicle physically visits DMV for TRH initialization. After confirming the credentials, DMV initializes the TRH and saves the system parameters including $\{G, q, P, Pub, u_V, o_V\}$. Additionally TRH is also preloaded with K_Z and K_{RSU} of the current zone and nearby RSU respectively. DMV also saves vehicle's individual secret key K_V and pseudonym generation key K_i.

3.2.3 Pseudonym Generation

DMV generates number of pseudonyms for each vehicle and saves it in the TRH. The pseudonyms are generated by taking vehicle's secret counter u_V and increments it by o_V as follows:

$$PS_V^i = ((\beta)_{K_i} \| (\beta \oplus VID)_{K_V} \| n_i)_{K_{DMV}^-}$$

$\beta = u_V + n_i o_V$, where n_i is the current count of the generated pseudonyms, and VID is the identity of the vehicle. DMV saves these pseudonyms in vehicle's TRH and sends the anonymous pseudonyms to RAs as well. TRH also encrypts K_i and K_V, and sends the encrypted text to RAs which serves as a trapdoor for the revocation. Encryption is carried out as follows:

$$c_1 = rP,\ c_2 = (K_i \| K_V) \oplus H(rPub)\ ,$$

r is a random number selected by TRH to the encryption. TRH sends (c_1, c_2) to DMV and RAs. However RAs can only decrypt the cipher text by colluding and can get K_i and

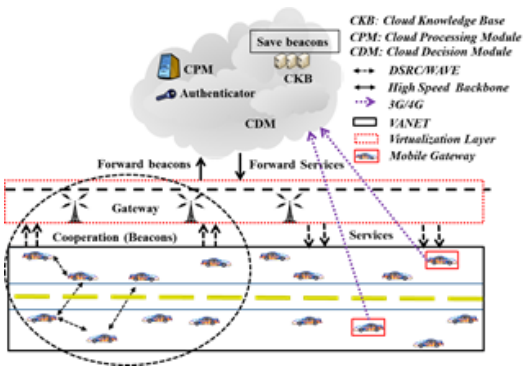

Fig. 1. Network Model

K_V when they agree upon constructing s from individual s_i. Additionally DMV also sends hashed credentials including K_i and K_V along with the pseudonyms to RAs which are in turn used to revoke the identity.

3.3 Privacy-Aware Beaconing

We extend Hussain et al.'s identityless beaconing mechanism [5] in our proposed scheme. The beacon format is given below:

$$B = (Payload, PS_V^i, \delta, h_{K_Z}(\delta \| Payload))_{K_{geolock}}$$
$$\delta = h_{K_V}(PS_V^i \| Payload)$$

Where B is the beacon broadcasted by vehicle V containing data $Payload$ which contains current time, location, velocity, and heading etc. Due to high frequency of the beacons, we use weak authentication in beacons by employing keyed HMAC. δ exhibits the functionality of both weak authentication and integrity of the data contained in beacons. In order to check the integrity of aforementioned value δ, another hash with zone key K_Z is calculated. It is worth noting that K_Z is distributed by RSUs among the vehicles of the same zone. However vehicles are subject to put request for new zone key while moving between zones. Vehicles use random pseudonyms from their pool with beacon messages. We assume that RCAs update these keys on regular basis.

To date, all previously proposed beaconing schemes send the contents of the beacons in plain text. Therefore, spatial and temporal correlation among beacon messages enables adversaries to construct movement profiles against specific users. To this end, we propose a geolock-based encryption and encrypt the entire beacon with $K_{geolock}$ (see next sub-section). GTs after receiving B, decrypt it with $K_{geolock}$, and then re-encrypt a part of B_i with $K_{RSU-DMV}$ and send the beacon (plaintext part $Payload$ and encrypted part $B-Payload_{K_{RSU-DMV}}$) to CKB. Since we are using fine-grained traffic information dissemination service from clouds, the data contained in beacons needs not to be encrypted in order for cloud to process the data. For that reason we only encrypt a part of beacon which contains the sensitive information and store it in the cloud for revocation and route tracing. is used by cloud to construct fine-grained traffic

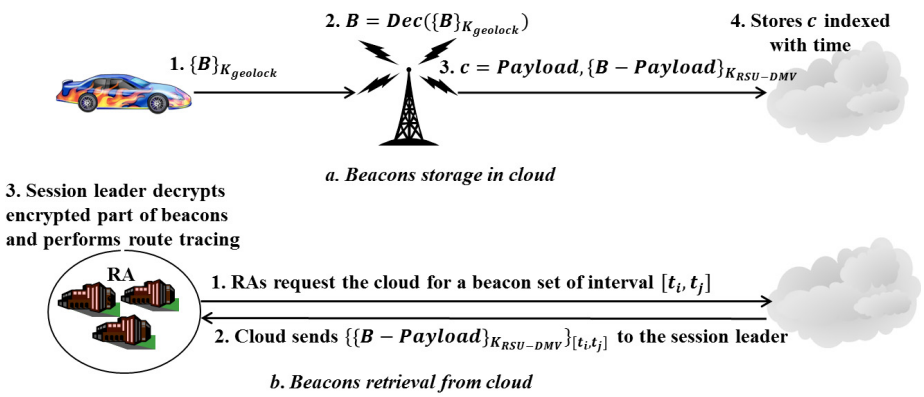

Fig. 2. Beacons storage and retrieval from cloud infrastructure

information based on physical sections of the road. CKB saves the beacon and indexes it with current time. The overall process is illustrated in Fig. 2.

3.4 Geolock-based Encryption

Traditionally in VANET, awareness information like speed, location, and heading information is sent in plaintext. Such scenario gives room to outsiders to generate movement profiles of the targets. Outsiders could also manipulate the location information in order to create illusions to launch Sybil attacks. It is somehow essential to provide location confidentiality against outsiders. However insiders are still a risk since they could manipulate the location information as well. Yan et al. proposed location-based encryption in order to achieve location confidentiality on the basis of assumption that the GPS information is private [13]. Their scheme uses only GPS information in order to construct a secure private value referred to as geolock. More precisely geolock-based encryption refers to an encryption scheme where location information is used to generate the key used for encryption and decryption. The purpose of such encryption is twofold: to provide location confidentiality against outsiders and to keep insiders from manipulating the contents of the message. Contrary to claim by Yan et al., we argue that GPS information is publicly available and their scheme may not be secure and virtually equivalent to plain text. All that would take attackers to decrypt the encrypted message would be to acquire GPS information. The fact that currently available hand-held GPS devices come handy and cheap, Yan et al.'s scheme is even more insecure.

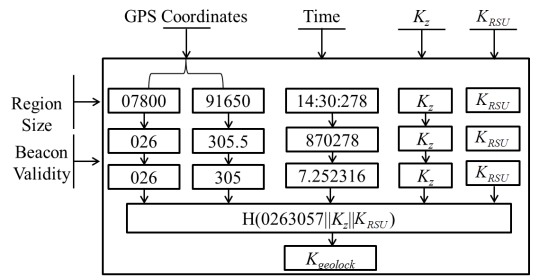

Fig. 3. Geolock-based encrytpion [9]

In order to diminish the effect of content manipulation, we use our extended and secure version [9] of Yan et al.'s location-based encryption [13].

Fig. 3 illustrates the construction process of K_{geolock}. The construction module takes as input, the effective region size, message lifetime, K_Z, K_{RSU}, and then multiplexes these values altogether in order to calculate hash value from the multiplexed content. The effective region size is used to define physical region where K_{geolock} is effective. Message lifetime helps to prevent the useless lingering around of stale messages in the network. K_{RSU} is the RSU-specific key issued to the legitimate vehicle whenever it comes under the RSU's transmission range. Our proposed location-based encryption mechanism uses different levels of confidentiality as follows: GPS coordinates are publically available, K_Z is known to the legitimate VANET users in a specific zone, and K_{RSU} is known to the vehicles currently present within the transmission range of the . Additionally it must be noted that some of no-RSU regions might exhibit a long distance with the same K_{RSU} but in that case, the time factor would limit the degree of content abuse. We assume that K_Z and K_{RSU} are subject to change on a regular or dynamic interval for security reasons; they have no contribution to security and privacy, otherwise.

3.5 Revocation and Route Tracing

In case of an investigation, for instance a deadly accident, the culprits must be brought to justice and their real identities must be revoked. In order to revoke a node, RAs agree upon constructing s from individual s_i. After that, current session leader decrypts from ciphertext as follows:

$$K_V = c_2 \oplus H(s \bullet c_1) = (K_i \| K_V) \oplus H(rPub) \oplus H(rsPub)$$

We assume that RAs already have got a warrant from DMV beforehand, and DMV also provides the session leader with $K_{RSU-DMV}$ since a portion of beacons is stored in encrypted form in the cloud. It is worth noting that any existing leader election mechanisms can be used to elect the leader of RAs which initiates the colluding mechanism to decrypt K_V and K_i. In order to revoke the vehicle in question, its beacons are retrieved from cloud with certain interval input. When the session leader decrypts K_i and K_V from c, it calculates δ for some of the beacons from the retrieved set of beacons, in order to verify the integrity of both keys and the beacon contents. Then with K_i and K_V in hand, the trapdoor inside the pseudonym in hand can be used to reveal the real VID of the vehicle. In this way, the real identity of the node is revoked.

For route tracing, DMV permits RAs to perform route tracing and RAs decrypt as aforementioned. Route tracing is performed as follows:

- RAs get a set of beacons from cloud infrastructure corresponding to any timespan $\triangle t$ (let say from time t_i to t_j), i.e. $\{b_{t_i}, b_{t_{i+1}}, ..., b_{t_{j-1}}, b_{t_j}\}$. Let the beacon set for route tracing is denoted by $B_{rt} = \{b_1, b_2, ..., b_k\}$.
- RAs check for the following condition.
  - For the first beacon when $t = t_i$ and $h_{K_V}(Payload)$, it is added to the route set which is denoted by B_{route} and $B_{route} = \{b_{t_i}\}$, t is the timestamp in the beacon and $b_{t_i} \in B_{rt}$.
  - For $t = t_{i+1}, ..., t_{j-1}, t_j$,

$$\forall b_i \in B_{rt} | t_{b_i} \in [t_i, t_j] \wedge h_{K_V}(Payload) = \delta$$
$$B_{route} = \left\{ b_{t_{i-1}} \right\} \cup b_{t_i}$$

t_{b_i} is the timestamp of beacon b_i and $B_{data_{[t_i, t_j]}}$ represents the beacon data whose timestamp is within interval $[t_i, t_j]$.

IV. Analysis and Evaluation

In this section we analyze our proposed scheme from security, conditional privacy, and computational overhead standpoint.

4.1 Security Analysis

The security requirements for beacons are *authentication*, *data integrity*, *user and location privacy*, and *confidentiality*. Due to high beacon frequency, we employ loose authentication through keyed HMAC. The hash value calculated with K_Z serves as both authentication and contents integrity verifier (including the integrity of δ). Apart from that, we also leverage location-based encryption where we encrypt the entire beacon with K_{geolock} in order to provide location confidentiality. It is worth noting that the plaintext beacons are prone to manipulation and movement profile generation from both insiders and outsiders [1]. To counter that issue and provide location privacy, we use geolock-based encryption. In order to manipulate the

contents, outsider must have obtained K_Z and K_{RSU} whereas for insiders, the contents of the message are meaningful only in the neighborhood with legitimate credentials (pair of K_Z and K_{RSU}).

4.2 Identity Preservation and Conditional Privacy

Our beacons include anonymous pseudonyms and are hard to link to each other and to the user, as long as K_Z and K_{RSU} are not compromised by outsiders. For insiders the window of linking would be too small. In our proposed scheme the compromise of K_Z alone does not affect the privacy until the current K_{RSU} is compromised as well. Even in such case, the consequences would be limited to the jurisdiction of the compromised RSU. K_V and K_i are saved by RAs in encrypted form, and without knowing s, RAs individually cannot abuse the user privacy. Moreover, even if RAs fail to confirm the value $h_{K_V}(Payload)$ to be from the target node, no additional information is exposed to RAs that could be abused. Moreover in case of $K_{RSU-DMV}$ compromise, the dire consequences would be limited to the jurisdiction of the concerned RSU, in the form of profilation. But the real identity of the nodes would still be preserved since from the pseudonyms in hand, it is not possible to link it to the user unless K_V and K_i are known.

Lemma 1*: It is very hard for adversaries to generate the real time profiles against the users.*

Proof: Since beacon is encrypted with K_{geolock}, in order for adversary to construct movement profiles of a specific target, the adversary must be in the transmission range and more precisely of the effective region of the K_{geolock} to decrypt the beacon and obtain the aforementioned value. By the characteristic of K_{geolock}, the adversary can only decrypt the message if it is physically present in the effective region where K_{geolock} can be constructed. In worst case, if the adversary is around the target all the times and holds legitimate K_Z and K_{RSU}, then the adversary can abuse the privacy of the target. However, the probability of such case is slim and equal to $\frac{1}{N_{RSU} \cdot N_Z \cdot \prod_{i=1}^{l} Cord_i \cdot \prod_{i=1}^{l} T_i}$, where $N_{RSU}, N_Z, Cord_i$ are the number of RSUs, number of zones, the coordinates of the area where current is valid at time. □

Lemma 2*: It takes universal brute force attack for K_{geolock} to compromise.*

Proof: In order to decrypt the message that is encrypted with current K_{geolock}, the decrypter must be physically present in the area where current K_{geolock} is valid and at the right time. Any insider legitimate user that is not currently present in the aforesaid area is considered as A_I. In order for A_I that is not physically present in the area where current K_{geolock} can be used for decryption, must construct all possible combinations of K_{geolock} for the decryption of the message. When A_I receives message encrypted with current K_{geolock} that is constructed with K_Z, K_{RSU}, t_{cur}, and loc_{cur}, it will be hard for A_I to figure out which K_Z and K_{RSU} are used to construct K_{geolock} and that is why A_I has to try all combinations of these two keys and the GPS locations in each zone, in other words try all zones and RSUs therein. Additionally even in the single zone and RSU, the GPS coordinates

are also important. If there are n zones, s RSUs in each zone and l locations under the jurisdiction of each RSU, then A_I must try the following number of keys to decrypt the message encrypted with current K_{geolock}.

$$\sum_{i=1}^{n}\sum_{j=1}^{s}\sum_{k=1}^{l}K_{ijk}$$

Moreover the time factor is an important issue in such brute force because after the expiry of the validity time denoted by which is also an input to the K_{geolock}, the key cannot be constructed and becomes stale. □

4.3 Computation and Communication Overhead Analysis

Revocation and route tracing functionalities are realized through computationally inexpensive HMACs. The size of beacon with security overhead denoted by is given below:

$$Size_B = Payload + 3H$$

According to [14], if we consider an optimistic size of the beacon payload, it will not exceed 50 bytes. So the size of the beacon becomes $50+3H$, however the real size will vary based on implementation. H denotes the size of the hash function used. The revocation cost for RA, denoted by T_{rev} is given by:

$$T_{rev} = 2T_{\text{mul}} + 3T_H + T_D + T_\lambda$$

T_{mul} is the time required for point multiplication, T_H is the time required to calculate hash, T_D is time required for symmetric decryption, and T_λ is the time required for table search. Route tracing cost, denoted by T_{rt} is given below:

$$T_{rt} = 2T_{\text{mul}} + 2T_H + nT_D + \prod_{i=1}^{|t_j|} T_{H_i}$$

RAs calculate j number of hash values, n is the number of beacons to be processed, and $|t_j|$ is the timespan for which route tracing is required. In [15], T_{mul} is found for a super-singular curve with embedding $k=6$ over $F_{3^{97}}$to be equal to 0.78 ms.

$$T_{rev} = 2(0.78) + 3T_H + T_E + \delta_{t_j}$$

$$T_{rt} = 2(0.78) + 2T_H + nT_D + \prod_{i=1}^{|t_j|} T_{H_i}$$

Let f_b be the beacon frequency, d be the traffic density at AoI (Area of Interest), and $\triangle_t$ be the timespan for tracing, then the number of beacons processed denoted by $b_{processed}$, is given by:

$$b_{processed} = d \times f_b \times \triangle_t$$

For revocation, the time required for node revocation denoted by T_α is bounded by the number of nodes whose credentials are saved in the RAs.

4.4 Comparison with Other Schemes

We compare our proposed scheme with Kim et al.'s [17] and Malandrino et al.'s [20] scheme. Table 2 outlines the comparison. The comparison is done from 'signatures with normal beacons', location privacy, profilation, and content security perspective. As it can be observed from the table that Kim et al. use signatures with the normal beacons, do not preserve location privacy, and profilation is possible

Table 2. Comparison with known schemes

Scheme	Signature with beacons	Location Privacy	Profilation	Content Security
Kim et al. [17]	Yes	No	Yes	No
Malandrino et al. [20]	No	Yes	Yes	No
Our Scheme	No	Yes	No	Yes

in their scheme. On the other hand, Malandrino et al. provides location verification, but their scheme still suffers from profilation and the content can easily be manipulated in their scheme. On the other hand, we use a modified location-based encryption scheme to provide location privacy, alleviate the content manipulation problem, and avoid profilation without shaking the normal structure of the beacons. Moreover the computational complexity incurred by our proposed scheme is less than Kim et al.'s scheme.

V. State of the Art

In this section we put light on the state of the art regarding standalone VANET and VANET-based clouds.

5.1 Standalone VANET

To date, a number of schemes have been proposed to preserve privacy and alleviate security threats in VANET [2,4]. In addition to user privacy, location privacy in VANET is essential at par. No matter, how ideal privacy preserving scheme is, location profiles might still be possible if the location information is exploited from regularly sent beacons. In order to provide location privacy and location confidentiality, a number of schemes were proposed. Mix zones were proposed by Huang et al. [18], where vehicles change their certificates and other keys when passing through mix zones. Yan et al. [13] proposed geolock-based encryption to provide location confidentiality. Hussain et al. proposed identityless beaconing mechanism, where beacons are broadcasts without any identity that could be traced back to the originator [5]. Although their scheme preserves conditional privacy, however, location privacy and content security is still a potential security hiccup in their scheme.

5.2 VANET-based Clouds

Olariu et al. for the first time envisioned paradigm shift by moving from traditional VANET to cloud-based VANET [6]. They came up with a new notion of VANET called AVC (Autonomous Vehicular Clouds). Yan et al. [16] outlined the security and privacy challenges in vehicular clouds. However Olariu et al. discussed vehicular clouds abstractly without mentioning particular framework architecture. Recently Hussain et al. [7] proposed three architectural frameworks for cloud-based VANETs namely VC, VuC, and HVC.

Qin et al. [19] proposed a cloud-based routing scheme in VANET named VehiCloud which provides routing services for VANET through cloud infrastructure. Vehicles share their current and future location information in the form of waypoints with cloud infrastructure and then cloud provides them with optimal

routing information. Recently Hussain et al. proposed a scheme referred to as TIaaS (Traffic Information as a Service) where they leverage cloud infrastructure to provide fine-grained traffic information to the moving vehicles on the road [9].

To date, at least to the best of our knowledge, there are only two schemes proposed for route tracing in VANET by Kim et al. [17] and Malandrino et al. [20]. Kim et al. included a tracker in their messages in order to trace back the route taken by the vehicles. However, apart from privacy preservation factor, their scheme includes signatures with normal messages which are questionable in VANET, and moreover they do not provide location privacy. The second scheme is proposed by Malandrino et al. namely A-VIP. However their scheme only provides location verification. They leverage anonymous position beacons and use Location Authority to confirm the locations announced by vehicles.

VI. Conclusion

Route tracing has not been given much attention in VANET (Vehicular Ad Hoc NETwork) and its successor VANET-based clouds. In this paper, we aimed at VANET-based clouds and proposed a pseudonymous beaconing paradigm where beacons are stored in cloud infrastructure in order to process them and provide VANET users with services. On top of that, we proposed a lightweight revocation and route tracing mechanism for privacy-preserved beacons in VANET-based clouds. Our proposed scheme guarantees conditional privacy, location confidentiality, and location privacy. Each beacon includes security parameters including trapdoor-based pseudonym, which are used in revocation and route tracing. The proposed scheme enables the law enforcement authorities to trace the route of a particular node within a stipulated timespan or revoke it.

References

[1] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, Vol. 15, pp. 39-68, 2007.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in Vehicular Ad Hoc Networks," IEEE Communications Magazine, Vol. 46, No. 4, pp. 88-95, 2008.

[3] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 21, No. 9, pp. 1227-1239, 2010.

[4] 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, pp. 1229-1237, 2008.

[5] R. Hussain, S. Kim, and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET," in Information Security Applications, Y. Heung Youl and Y. Moti, Eds., ed: Springer-Verlag, pp. 268-280, 2009.

[6] S. Olariu, M. Eltoweissy, and M. Younis, "Towards Autonomous Vehicular Clouds," ICST Transactions on Mobile Communications and Applications, Vol. 11, pp. 1-11, 2011.

[7] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing," in Proc. IEEE CloudCom 2012, pp. 606-609, 2012.

[8] L. Delgrossi and T. Zhang, "Dedicated short-range communications," Vehicle Safety Communications: Protocols, Security, and Privacy, pp. 44 - 51, 2009.

[9] R. Hussain, F. Abbas, J. Son, and H. Oh, "TIaaS: Secure Cloud-assisted Traffic Information Dissemination in Vehicular Ad Hoc NETworks," in Proc. 13thIEEE/ ACM CCGrid 2013, pp. 178-179, 2013.

〔10〕 T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.
〔11〕 V. S. Miller, "Use of elliptic curves in crytography," in Proceedings of Advance in Cryptology, pp. 417-426, Aug. 1985.
〔12〕 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, pp. 816-824, 2008.
〔13〕 Y. Gongjun, S. Olariu, and M. Weigle, "Providing location security in vehicular Ad Hoc networks," Wireless Communications, IEEE, Vol. 16, pp. 48-55, 2009.
〔14〕 J. Harri, F. Filali, and C. Bonnet, "Rethinking the Overhead of Geo-localization Information for Vehicular Communications," in Proc. IEEE 66th Vehicular Technology Conference (VTC-2007 Fall), pp. 2111-2115, 2007.
〔15〕 A. Wasef, J. Yixin, and S. Xuemin, "ECMV: Efficient Certificate Management Scheme for Vehicular Networks," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, pp. 1-5, 2008.
〔16〕 G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing," IEEE Transactions on Intelligent Transportation Systems, Vol. PP, No. 99, pp. 1-11, 2012.
〔17〕 S. Kim and H. Oh, "A Simple Privacy Preserving Route Tracing Mechanism for VANET," in Proc. IEEE 71stVehicularTechnologyConference (VTC2010-Spring), pp. 1-5, 2010.
〔18〕 L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in Proc. IEEE WCNC, pp. 1187 - 1192, Mar. 2005.
〔19〕 Y. Qin, H. Dijiang, and Z. Xinwen, "VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 1438-1445.
〔20〕 F. Malandrino, C. Casetti, C.F. Chiasserini, M. Fiore, R. S. Yokoyama, and C. Borgiattino, "A-VIP: Anonymous Verification and Inference of Positions in Vehicular Networks," to appear in IEEE Infocom, 2013.
〔21〕 R. Hussain, F. Abbas, J. Son, H. Eun, and H. Oh, "Privacy-Aware Route Tracing and Revocation Games in VANET-based Clouds," *IEEE WiMob 2013*, pp. 747-752, Oct. 2013.

〈저자소개〉

후세인 라쉬드 (Rasheed Hussain) 학생회원
2007년 5월: NWFP University of Engineering and Technology, Peshawar, Pakistan 학사
2010년 8월: 한양대학교 컴퓨터공학과 석사
2011년 9월~현재: 한양대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, VANET, Cloud computing, VANET-Cloud

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과 학사
1989년: 아이오와주립대학 전자계산학과 석사
1992년: 아이오와주립대학 전자계산학과 박사
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안