Journal of Korea Multimedia Society Vol. 19, No. 7, July 2016(pp. 1159-1165)
http://dx.doi.org/10.9717/kmms.2016.19.7.1159

Secure and Privacy Preserving Protocol for Traffic Violation Reporting in Vehicular Cloud Environment

Lewis Nkenyereye†, Kyung-Hyune Rhee††

ABSTRACT

Traffic violations such as moving while the traffic lights are red have come from a simple omission to a premeditated act. The traffic control center cannot timely monitor all the cameras installed on the roads to trace and pursue those traffic violators. Modern vehicles are equipped and controlled by several sensors in order to support monitoring and reporting those kind of behaviors which some time end up in severe causalities. However, such applications within the vehicle environment need to provide security guaranties. In this paper, we address the limitation of previous work and present a secure and privacy preserving protocol for traffic violation reporting system in vehicular cloud environment which enables the vehicles to report the traffic violators, thus the roadside clouds collect those information which can be used as evidence to pursue the traffic violators. Particularly, we provide the unlinkability security property within the proposed protocol which also offers lightweight computational overhead compared to previous protocol. We consider the concept of conditional privacy preserving authentication without pairing operations to provide security and privacy for the reporting vehicles.

Key words: Vehicular Cloud Computing, Traffic Violation Reporting, Authentication, Conditional Privacy Preservation

1. INTRODUCTION

Traffic violations are reported as one of the factors which cause accidents on the roads. The traffic violation can be classified into two categories: major or minor. Some known offenses can include driving under the influence of alcohol, reckless driving and driving while intoxicated [1]. Misbehaving drivers might continue and provoke major traffic violation if they are not properly handled. In general, a minor traffic offense will not result in the offender being arrested or sent to jail. The driver typically receives a citation that requires the payment of a fine, an appearance in court, or both. The major issue in court appearance is the evidence to convict the driver of his violations. Vehicular cloud computing (VCC) integrated with intelligent transportation system (ITS) sector avails suitable framework for reporting those acts of violations.

ITS was introduced to provide safer transportation environment through a variety of applications and has attracted attentions because of its direct effect on economic growth [2]. Vehicular ad hoc network (VANET) is a self-organized platform where the vehicles are assumed to possess

※ Corresponding Author : Kyung-Hyune Rhee, Address: (48513) 45 Yongso-ro, Nam-Gu. Busan, Republic of Korea, TEL : +82-629-6247, FAX : +82-626-4887, E-mail : khrhee@pknu.ac.kr
Receipt date : Feb. 1, 2016, Revision date : Apr. 28, 2016
Approval date : May 31, 2016

† Department of IT Convergence and Application Engineering, Pukyong National University (E-mail : nkenyele@pukyong.ac.kr)
†† Department of IT Convergence and Application Engineering, Pukyong National University
※ This work was supported by a Research Grant of Pukyong National University (2016 year).

wireless communication devices called on board unit (OBU) and road side units (RSUs) fixed along the roads to enable both vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [3]. A dedicated short range communications (DSRC) standardized by the IEEE is availed for the communication between vehicles and RSUs. The limited computational capabilities of VANETs are relieved by vehicular cloud computing (VCC) into which vehicle's devices are connected to cloud servers to perform complicated computational operations [4]. Based on a vehicular cloud computing architecture, we present a secure and privacy preserving protocol for traffic violation reporting in vehicular cloud environment and use conditional privacy preserving technique [5] to guarantee the security of reported messages.

Vehicular cloud computing is a new technological concept integrating cloud computing in a vehicular environment. In [6], the authors defined three types of architectures depending on the combination of VANETs and cloud computing. A classification for vehicular cloud-based services and their respective potential security threats were also presented. The authors pointed out the feasibility and practicability of vehicular cloud compared to VANETs. VANETs has received much attention on secure protocols for diversified applications [2,3,6,7,8,9]. The majority of the proposed protocols suggest security mechanisms which could be adopted in order for the vehicles to securely receive road services such as navigation services.

The traffic violation scenario in VANETs or VCC has not received much attention in the literature. One of the relevant work addressing the specific scenario was presented by Mallissery et al, [10]. The authors presented a transport and traffic rule violation monitoring services in ITS based on pseudo identity for guaranteeing vehicles anonymity. However, for their protocol, an attacker can link the pseudo identify of a reporting vehicle to trace its itinerary. Thus the protocol does not provide unlinkability of traffic violation messages. Furthermore, their protocol lacks security analysis and the used security primitive considerably affect the violation message overhead.

In this paper, to overcome the weakness of Mallissery et al.'s, we make use of ECC-based conditional privacy preserving authentication (CPPA) technique [5] to provide privacy and authentication of the reporting vehicles. The transmission overhead of the proposed protocol achieves better performance compared to Mallissery et al, [10].

2. SYSTEM MODEL

In this section, we present the system architecture, security objectives and the description of the main phases of the proposed protocol.

2.1 System Architecture

We describe the application model of our secure and privacy preserving protocol for traffic violation reporting in vehicular cloud environment. In figure 1, let assume that the red vehicle is moving on the highway and violates the speed limit. The surrounding vehicles record the violation through their in-built sensors and transmit the information to the traffic center (TC) through the roadside cluds (RSCs). Any vehicle within the violating vehicle's vicinity records the violation and transmits the report to the RSC. Later on, the RSC transmits the data to TC which could avail those information to the justice sector once requested. Our system model comprises of a trusted authority (TA), RSC, TC and vehicles equipped with OBU as described in Fig. 1.

• TA: It is in charge of the registration of all entities inside our system and issues cryptographic materials during the system initialization.

• RSCs: They are databases located along the roads and accessible by the vehicles. In this case, any recorded violation is transmitted to TC through RSC. We assume that RSC has sufficient compu-

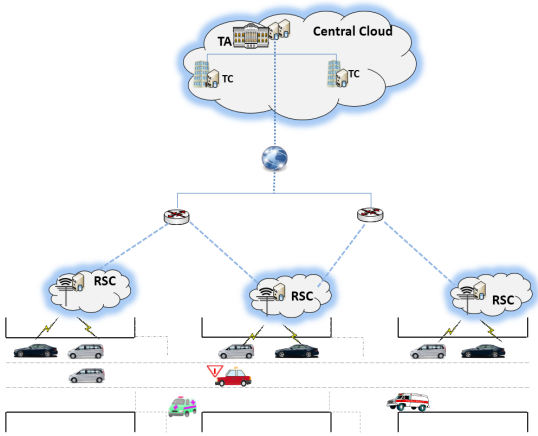

Fig. 1. System architecture.

tational capabilities to allow realtime communication with the TC.

• TC: It is a server located in the cloud controlled by the transportation authority. Beyond the routine activities, it is also in charge of keeping the file of traffic violators which could be used as evidence in court.

• Vehicle: Each vehicle is equipped with an OBU capable of performing cryptographic operations.

2.2 Security Objectives

Our proposed protocol should satisfy the following security requirements:

• Identity privacy preserving: The real identity of a vehicle transmitting a violation reporting message should be kept anonymous from other vehicle within the same RSC range. Otherwise, an attacker can use the real identity of the reporting vehicle to produce impersonation attacks.

• Authentication: Each vehicle should be authenticated before it transmits a violation reporting message.

• Unlinkability: RSC and malicious user should not be able to link two messages sent by the same reporting vehicle.

• Traceability: TA should be able to reveal the real identity of the vehicle in case of complaints.

2.3 Proposed Protocol description

From the above described architecture, our secure and privacy preserving protocol for traffic violation reporting is comprised of two phases: System initialization and Violation reporting.

• System Initialization: TA sets up its master secret key and its corresponding public key. TA assigns a real identity to each vehicle and forwards securely the vehicle real identity and the master secret key to the vehicle.

• Violation Reporting: When a vehicle sensor records any kind of violation, the vehicle first computes its pseudo-identity to be used during the violation reporting phase. The vehicle OBU further generates a ID-based signature on the violation reporting message which is sent to RSC. The communication between RSC and TC is not emphasized, rather adopt existing protocols such as [8]. Upon receiving the violation message from the vehicle, RSC verifies the vehicle's signature and stores the message in its database. In this paper we adopt CPPA in [5] as our building blocks.

3. PROTOCOL DESCRIPTION

The protocol description is made by the system initialization phase and the violation reporting phase as follows:

3.1 System Initialization

In initialization phase, TA generates system parameters and issues keys to the registering vehicles as follows:

• Chooses an additive group G with a prime order q and $P \in G$, where G consists of all points on a non-singular elliptic curve and P is a generator of G.

• Chooses $s \in Z_q^*$ as the private key of the system and computes the system public key $P_{TA} = sP$.

• Assigns an identity VID_i to each vehicle v_i.

• Provides v_i with (VID_i, s) securely. We assume that (VID_i,s) is pre-loaded into v_i's tamper-proof device.

• Publishes the system parameters $\{G,P,h_1,h_2,P_{TA},q\}$ where $h_1 : G \rightarrow Z_q$ and $h_2 : \{0,1\}^* \times G \rightarrow Z_q$ are two secure hash functions.

3.2 Violation Reporting

When detecting a traffic violation action through the sensors within the vehicle, the reporting vehicle v_i performs the following:

• Choose a random nonce $a \in Z_q^*$, compute $AID_{i,1} = aP$, $AID_{i,2} = VID_i \oplus h_1(aP_{TA})$, and sets its pseudo-identity as $AID_i = (AID_{i,1}, AID_{i,2})$

• Generate its signing key as $sk_i = a + \alpha_i s \mod q$ where $\alpha_i = h_2(AID_i \| T_i)$ and T_i is the time stamp.

To generate a signature on the traffic violation message M, we take the same reporting elements in [10] which are made of anonymous identity, Day, Date, Time, Latitude, Longitude, Vehicle Location, Sensor type and Sensor value for fair comparison. v_i performs the following:

• Choose a random nonce $w \in Z_q^*$ and compute $W_i = wP$, $\beta_i = h_2(AID_i \| T_i \| W_i \| M)$. The signature σ_i on the message is computed as $\sigma_i = sk_i + w\beta_i \mod q$.

• The vehicle sends $\{M, AID_i, T_i, W_i, \sigma_i\}$ to RSC_j

3.3 Violation message verification

To verify the message, RSC_j performs the following after checking the freshness of T_i:

• Compute $\alpha_i = h_2(AID_i \| T_i)$ and $\beta_i = h_2(AID_i \| T_i \| W_i \| M)$

• Then check if $\sigma_i P = AID_{i,1} + \alpha_i P_{TA} + \beta_i W_i$ is valid. The consistency can be proven as follows:

$$\begin{aligned} \sigma_i P &= (sk_i + w\beta_i)P \\ &= (a + \alpha_i s)P + (w\beta_i)P \\ &= aP + \alpha_i sP + w\beta_i P \\ &= AID_{i,1} + \alpha_i P_{TA} + \beta_i W_i \end{aligned}$$

After recovering the violation message, in non-rushing hours, RSC_j transmit the violation messages to TC. Thus, TC would be able to use those information to convince the drivers of their violations.

4. ANALYSIS

In this section, we give the evaluations of the proposed protocol in terms of security analysis, transmission overhead and average delay.

4.1 Security Analysis

We analyse the security of the proposed protocol based on the afore-mentioned security objectives.

• Identity privacy preserving: The real identity of a vehicle transmitting a violation reporting message cannot be obtained by an attacker since the used identity is $AID_i = (AID_{i,1}, AID_{i,2})$ with $AID_{i,1} = aP$ and $AID_{i,2} = VID \oplus h_1(aP_{TA})$. The attacker has to overcome the hardness of Computational Diffie-Hellman problem, thus the privacy of the reporting vehicles is guaranteed.

• Authentication: The authentication of the vehicle is assured by the signature generated by the violation reporting vehicle. The verifier checks if the equation $\sigma_1 P = AID_{i,1} + \alpha_i P_{TA} + \beta_i W_i$ is valid. Based on Discrete Logarithm problem, no adversary can forge a valid message.

• Unlinkability: Before a vehicle sends a violation reporting message, it first generates two random $a \in Z_q^*$ and $w \in Z_q^*$ to provide randomness on the pseudo-identity and signature for every message, thus no adversary can link two pseudo-identities of a same vehicle or its corresponding signatures.

• Traceability: Though the pseudo-identity of the vehicle is generated by the vehicle as $AID_i = (AID_{i,1}, AID_{i,2})$ with $AID_{i,1} = aP$ and $AID_{i,2} = VID \oplus h_1(aP_{TA})$. TA can recover the real identity of the vehicle by computing

$sAID_{i1} = asP = aP_{TA}$. The vehicle real identity is recovered as $VID_i = AID_{i,2} \oplus h_1(AID_{i,1} \| T_i)$.

4.2 Performance

In this section, we provide the performance of the proposed protocol in terms of transmission overhead. Let Tas−en, Tas−dec, Tmul, and Tsig be the time required to perform asymmetric encryption, asymmetric decryption, scalar point multiplication over an elliptic curve and signature generation respectively. We only consider the time taken by these operations and neglect all others such as addition or hash functions. To estimate the performance, we consider ECC-based ID-based CPPA of [5] with 160-bit prime q. The implementation was executed on a 3.5-GHz, core i-5, 16 GB RAM desktop computer. The obtained results are shown in Table 1.

The proposed protocol requires 6Tmul for pseudo-identity and signature generation and the signature verification requires 3Tmul. The total cost of the protocol is 9Tmul=0.78 × 9=7.02 milliseconds. In Mallissery et al [10], the PID generation phase and violation reporting requires each 5Tmul+Ts-enc+Ts-dec. The total cost is 10Tmul+2Ts-enc+2Ts-dec=9.92 milliseconds. In the same way, the vehicle uses, We further estimated the communication cost of the proposed protocol. Since the size of q is 160 bits (20 bytes), then the element size in G are 20 × 2=40 bytes. The vehicle in the proposed protocol broadcast $\{M, AID_i, T_i, W_i, \sigma_i\}$ which are 40 × 3=20=140 bytes. In [10], the message size of the message is 160 bytes along with the vehicle certificate which is 125 bytes. The total message size is 285 bytes. We further evaluate the transmission overhead of the proposed protocol compared to Mallissery et al. Fig. 2 shows the relationship between the number of received message and the transmission overhead. The proposed protocol performs better compared to Mallisery et al, [10].

Table 1. Measurement of cryptographic operations

Notation	Operation	time(ms)
Tmul	Point scalar multiplication	0.78
Tas-enc	Asymmetric encryption	1.17
Tas-dec	Asymmetric decryption	0.61
Ts-enc	Symmetric encryption	0.51
Ts-dec	Symmetric decryption	0.55
Tsig	Signature generation	1.56
Tver	Signature verification	3.12

Additionally, we evaluate the performance of the proposed protocol through simulation. We used VANET-SIM simulator for vehicle mobility coupled with ns-3 simulator for network simulation. We then set our scenario based on the IEEE 802.11p VANET platforms range which is 2.56 Mbps in highly populated street such as highways that use DSRC, to a maximum transmission range of 6 Mbps. We consider a city scenario with a map downloaded from OpenStreepMap database with a random speed for the vehicles ranging from 10 to 40 m/s (36-144 km/hr). The details of the simulation are shown in Table 2.

The average overall delay is computed as $AvD = \frac{1}{NVr}\sum_{i=1}^{NVr}\frac{1}{NRsc}\sum_{j=1}^{NRsc}(Tsend - Trec)$ where $NVr, NRsc, Tsend, Trec$ represent the number of violation report sent by v_i, the number of RSC, the time a violation report is sent and the time it is received by RSC respectively. As shown in figure 3, the proposed protocol has an average delay of 0.21 for 100 vehicles where as it is 0.67 for Mallissery et al. This is due to the package size

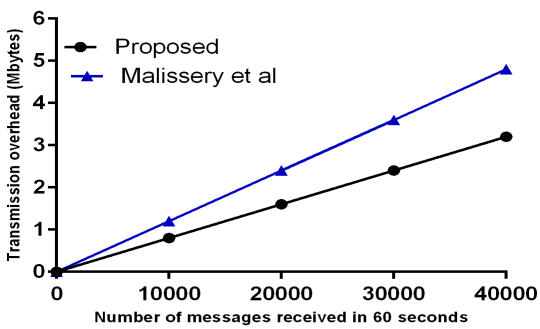

Fig. 2. Transmission overhead depending on the number messages.

Table 2. Simulation settings

Tools/Parameters	Value/Specification
Mobility generation tool	VANETSIM 2.02
Network simulation tool	ns-3
Transmission range	6 MBps
Number of vehicles	100
Simulation period	200 min
Wireless protocol	802.11a
Departure interval	20 sec
RSC radius	500m
Mobility model	Shortest path
Message size in [10]	140 bytes
Message size in proposed	285 bytes

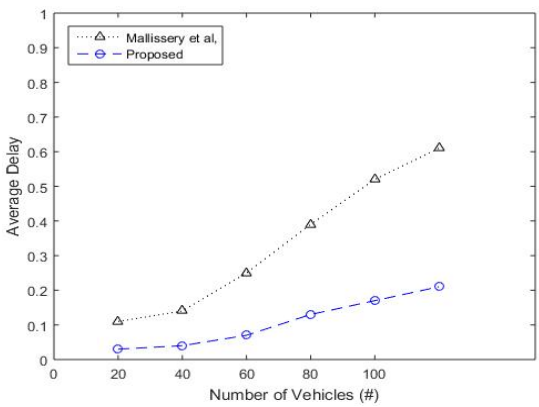

Fig. 3. Impact of vehicle density on average delay.

of the violating message between the proposed protocol and Mallisery et al, [10].

5. CONCLUSIONS

In this paper, we have proposed a secure and privacy preserving protocol for traffic violation reporting in vehicular cloud environment. The proposed protocol allows the vehicles to report the traffic violators, those information are collected by the RSC which forwards them to the transportation authority. The security analysis confirms that the proposed protocol preserve the identity of the reporting vehicles along with the unlinkabilitty of the reporting vehicles based on the sent messages. The performance evaluation of the proposed protocol based on the transmission overhead and average delay confirms its applicability.

REFERENCE

[1] S.H. Ahmed, M.A. Yaqub, S.H. Bouk, and D. Kim, "Towards Content-centric Traffic Ticketing in VANETs: An Application Perspective," *Proceeding of the Seventh IEEE International Conference on Ubiquitous and Future Networks*, pp. 237-239, 2015.

[2] T.W. Chim, S.M. Yiu, L.C. Hui, and V.O. Li, "VSPN: VANET-based Secure and Privacy-preserving Navigation," *IEEE Transactions on Computers*, Vol. 63, No. 2, pp. 510-524, 2014.

[3] W. Cho, Y. Park, C. Sur, and K. Rhee, "An Improved Privacy-preserving Navigation Protocol in VANETS," *Journal of Wireless Mobile Networks Ubiquitous Computer Dependable Applications,* Vol. 4, No. 4, pp. 80-92, 2013.

[4] S. Olariu, T. Hristov, and G. Yan, *The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds. Mobile ad Hoc Networking: Cutting Edge Directions*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2013.

[5] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 12, pp. 2681-2691, 2015.

[6] R. Hussain, "Cooperation-aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks," *Journal of Information Processing Systems,* Vol. 10, No. 1, pp. 103-118, 2014.

[7] L. Nkenyereye, B.A. Tama, Y. Park, and K. Rhee, "A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control

for VANETs," *Journal of Wireless Mobile Networks Ubiquitous Computer Dependable Applications*, Vol. 6, No. 2, pp. 98-112, 2015.

[8] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "A Novel Anonymous Mutual Authentication Protocol with Provable Link-layer Location Privacy," *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 3, pp. 1454-1466, 2009.

[9] Y. S. Park, C.D.Jung, Y. Park, K.H. Rhee, "An Efficient Anonymous Authentication and Vehicle Tracing Protocol for Secure Vehicular Communications," *Journal of Korea Multimedia Society,* Vol.13, No.6, pp.865-874, 2010.

[10] S. Mallissery, P.M.M. Manohara, N. Ajam, J. Mouzna, and P.M.J Mouzna, "Transport and Traffic Rule Violation Monitoring Service in ITS: A Secured VANET Cloud Application," *Proceeding of the 12th Annual IEEE Conference on Consumer Communications and Networking*, pp. 213-218, 2015.

Lewis Nkenyereye

Aug. 2009. Department of Computer Science, Light University of Bujumbura. (B.Sc)
Feb. 2013. Department of Information Technology, Uganda Christian University (M. Sc.)
Sept. 2013~Present. Doctor course student, Department of IT Convergence and Application Engineering, Pukyong National University
Field of Study: Cryptography, Vehicular cloud security

Kyung-Hyune Rhee

Feb. 1982. Department of Mathematical Education, Kyungpuk National University. (B.Sc)
Feb. 1985 Department of Applied Mathematics in Korea Advanced Institute of Science and Technology (M. Sc.)
Aug. 1992 Department of Mathematics in Korea Advanced Institute of Science and Technology (Ph.D.)
Mar. 1993~Present Professor at Department of IT Convergence and Application Engineering in Pukyong National University
Field of Study : Intelligence Security, Cryptographic Protocols, Applied Cryptography, Multimedia Security, IoT security