**Contemporary Engineering Sciences, Vol. 9, 2016, no. 13, 619 - 625**
**HIKARI Ltd, www.m-hikari.com**
**http://dx.doi.org/10.12988/ces.2016.6449**

# Study on the Privacy-Preserving Vehicular PKI in Autonomous Driving Environments

**Jae Jung Kim**

Department of Computer Science
Sungshin University, Seongbuk-gu, Seoul, Korea

**Seng Phil Hong**

Department of Computer Science
Sungshin University, Seongbuk-gu, Seoul, Korea

## Abstract

Vehicle-to-Everything (V2X) communication for autonomous driving is currently a focus of research and standardization in the USA, Europe and Asia. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication has great potential to increase road and passenger safety, and has been considered a next important part of cooperative Intelligent Transportation Systems for the vision of accident-free driving. V2X communication have a lot of threats and vulnerabilities such as distribution of wrong or forged messages, tracking and profiling of vehicles or vehicle drivers, and disturbance or unavailability of communication system, etc. These risks have generated invasion of privacy and interference of autonomous driving. In particular, this paper analyzed the security services and public key infrastructure (PKI) defined in IEEE Wireless Access in Vehicular Environments (WAVE) 1609.2 and proposed the privacy preserving vehicular PKI that provides a trust and efficient V2X communication for autonomous driving environments.

**Keywords**: Vehicular PKI, Privacy, V2X, WAVE, Certificate

## 1. Introduction

One of the main requirements for a successful rollout of V2X communication technology is trustworthiness. Otherwise, if safety messages are not trustworthy, consumers will never adopt this new technology. Beside well-functioning sensors, communication devices and applications, security is a crucial requirement. The main security challenges for the exchange of Vehicle-to-Vehicle (V2V) messages are authenticity, integrity of messages as well as non-repudiation and privacy. [1]

In order to obtain an implementable system to enhance the trustworthiness of V2V communications in a large-scale Vehicle Ad hoc Network (VANET), we keep in mind the following main design goals: Liability, Anonymity, and Scalable Management.

The fundamental security functions in vehicular communications consist of ensuring liability for the originator of a data packet. There is anonymity if, by monitoring the communication in a VANET, message originators cannot be identified, except perhaps by designated parties. For a VANET deployed in a highly populated metropolitan area, managing up to (tens of) millions of vehicles is a substantial concern. [2]

To enable transportation safety, efficiency, and other applications, Intelligent Transport Systems (ITS) rely on V2X communication. V2X means V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) and/or V2N (Vehicle-to-Nomadic Devices). [3]

According to Dedicated Shot Range Communication (DSRC), vehicles broadcast traffic safety message every 100-300ms. In high traffic density scenario, verifying every message will bring great computation overhead. In addition to computational efficiency, privacy requirements are also essential as the safety packet contains privacy-related information about user's geographical location and personal predilection. To make VANETs practical in use, security and privacy requirements must be guaranteed first of all other issues. [4]

The Public Key Infrastructure (PKI) is a key element of the security and privacy concept of V2X communications. All stations (i.e. vehicles and roadside units) that are equipped with a V2X communication unit have to be registered with the PKI and certificates have to be stored in the security subsystem of an On-Board Unit (OBU). [5]

## 2. Problem Statement

We analyzed vehicular PKI requirements compared to the current accredited certification system and have suggestions for improvement.

First, it is widely agreed that anonymity and long-term unlinkability of broadcast messages is required for a successful WAVE deployment. Anonymity disallows any identifier in messages that can be linked to the vehicle, such as license plate number and vehicle identification number. Long-term unlinkability makes sure that two messages broadcast at time-intervals far apart (say, at different days) cannot be linked to avoid tracking of vehicles and to avoid that behavior patterns can be derived. The agreed approach is to regularly change pseudonyms. For instance, pseudonyms can be changed after a given time period (say, 8 hours), or during special events (e.g. each time a vehicle's engine is started). [6]

Second, Certificate Revocation List (CRL) in the classic PKI included the serial number of revoked certificate and verifiers check CRL whether the signer's serial number find or not. But, in vehicular PKI, the number of pseudonym certificates are a lot, if revoked these certificates and included all serial numbers into CRL. The CRL size is too large and the validation takes long time. We need a different mechanism to reduce the CRL size and validation time.

Third, accredited certificates in the classic PKI use many applications such as financial areas and e-government services for identification of users. So frequency of use is low and certificate size is doesn't matter. In vehicular PKI, each vehicle is broadcasting the signed basic safety messages (BSM) approximately ten times per second. So OBU calculates the public key internally instead of sending user's public key in order to reduce the certificate size. Misbehavior detection in vehicle should be critical process because vehicle's misbehavior is related to human life.

## 3. Related Research

IEEE WAVE 1609.2 describes the basic security protocol that secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages are defined in this standard. It also describes administrative functions necessary to support the core security functions.

IEEE WAVE 1609.2 has PKI hierarchy as follows; CA issues a certificate that is used to verify the signature on data other than a WAVE service advertisement. WSA CA issues a certificate used to verify a wireless access in WAVE Service Advertisement. [7]

## 4. Privacy Preserving Vehicular PKI

### 4.1 Vehicular-PKI Model

The proposed vehicular PKI model consist of Root CA, Enrollment CA, Pseudonym CA (PCA), CRL Signer, Misbehavior Authority (MA), and Registration Authority (RA). Root CA can issue CA certificate and an authority revocation list (ARL) to revoked CA certificates. Enrollment CA activates or initializes the OBU by issuing an enrollment certificate. Pseudonym CA issues the pseudonym certificates exchanged by OBU in V2V communication that support trust between users of the system. Pseudonym certificates issued by the PCA are the security credentials that allow the receiver of a message to validate the signature of the sender. CRL signer is the function that creates and publishes CRLs so that other system components can access and download them. Misbehavior Authority is responsible for detecting, tracking, and managing potential threats to connected vehicle system. The MA is also responsible for CRL creation, management, and publishing through the CRL signer activity.

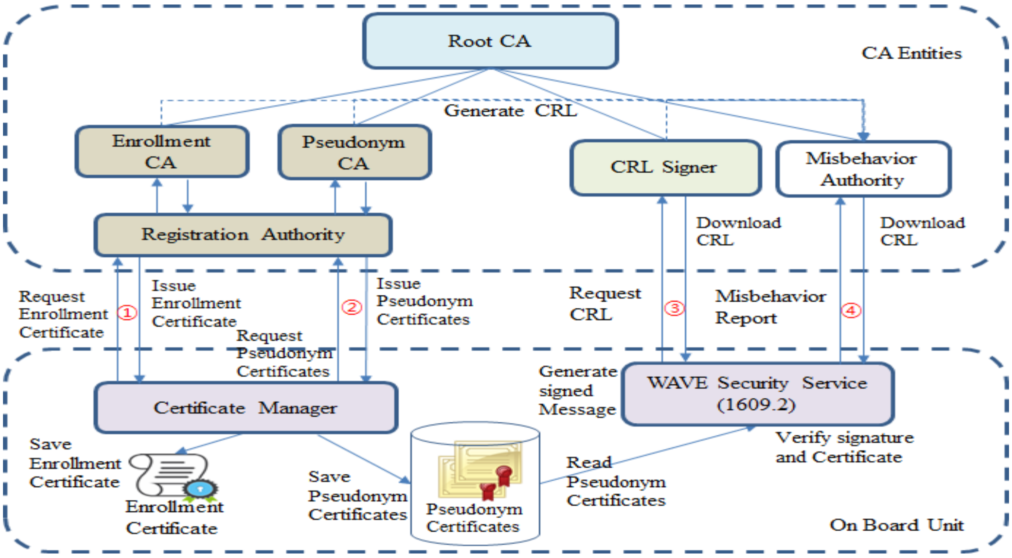


Fig.1 The Privacy Preserving Vehicular PKI Model

### 4.2 Certificate Issuance Process

There are two type of certificates, one is enrollment certificate and the other is pseudonym certificate. Enrollment certificate is like a passport for the OBU that it uses to request pseudonym certificates. It is provided to OBU during its bootstrap process. Pseudonym certificate is an authorization certificate that indicates its holder's permissions but not its holder's identity. It is used by an OBU primarily for basic safety message (BSM) authentication and misbehavior reporting. For privacy reasons, an OBU is given multiple certificates that are valid simultaneously, so that it can change them as often as necessary and possible. An OBU is given 3 years worth of certificates at a time, where validity period of each certificate is 1 week, and 20 certificates are valid simultaneously at any time.

### 4.3 Certificate Verification Process

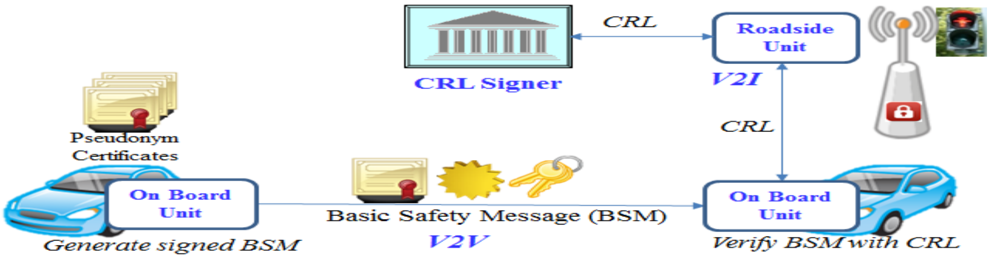


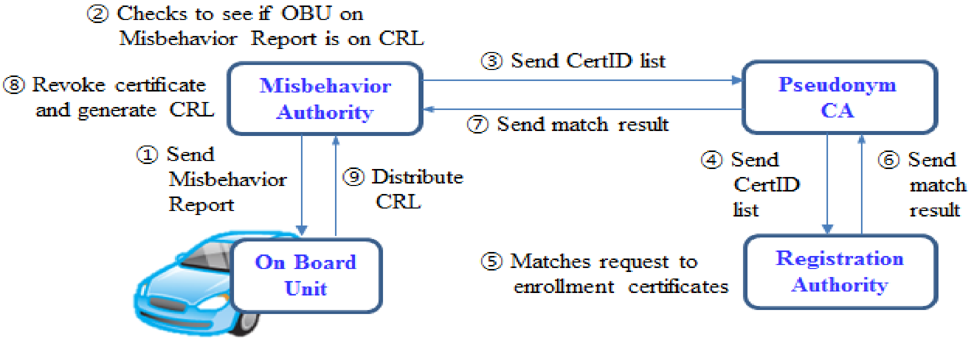
Fig.2 Certificate Verification Process

The basic safety message contains the core data elements such as vehicle size, position, speed, heading acceleration, brake system status, and so on. It transmitted approximately ten times per second. A sender generates the signed

BSM by own pseudonym certificate in order to protect privacy, the receiver will verify the signed BSM with CRL issued by CRL Signer. If verification failed, the receiver generate misbehavior report and follow misbehavior detection process.

### 4.4 Misbehavior Detection Process

The MA function is responsible for identifying potential misbehavior in the connected vehicle system. The OBU will send misbehavior reports to the MA, MA analyzes content from a misbehavior report to determine whether revocation of a specific enrollment certificate through placement on the CRL is necessary. If misbehavior is identified, the MA works with the PCA and RA to identify the OBU based on certificate identifiers, and then creates the CRL.

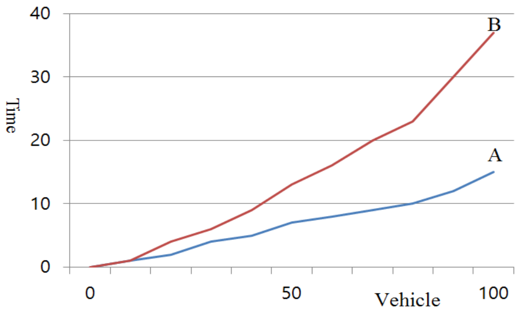

② Checks to see if OBU on Misbehavior Report is on CRL
⑧ Revoke certificate and generate CRL
Misbehavior Authority
③ Send CertID list
⑦ Send match result
Pseudonym CA
① Send Misbehavior Report
⑨ Distribute CRL
④ Send CertID list
⑥ Send match result
On Board Unit
⑤ Matches request to enrollment certificates
Registration Authority

[Fig.3] Misbehavior Detection Process

## 5. Comparison and Simulation

The proposed system is compared with the current classic PKI system as follow;

| Category | The classic PKI | V-PKI Model |
|---|---|---|
| Privacy against 3rd party entities | X | O |
| Privacy against authorities | X | O |
| Type of certificates | X.509 Certificate | Pseudonym Certificate |
| Misbehavior reporting | X | O |
| Non-Traceability | X | O |
| Contents of CRL | Serial number | Linkage values |



We have simulated the speed of certificate verification. Graph A shows the response time using pseudonym certificate with linkage values. Graph B is the result of response time X.509 certificate without linkage values. As a result of the simulation, verification time of A is faster than B because CRL size of A is smaller than B so that download time is reduced. Through this result, it is concluded that this system ensures not only privacy preserving but also speedy verification time.

## 6. Conclusion and Future Work

In this paper, we have suggested the privacy preserving vehicular PKI model that provides a trust and efficient V2X communication for autonomous driving environments. This system can be a solution to the problems caused by lack of security and reliability of the classic PKI. Vehicular PKI issues pseudonym certificates in order to avoid tracking of vehicles and to avoid that behavior patterns can be derived. If a vehicle detects misbehavior action among BSMs V-PKI adds that vehicle into blacklist and CRL. The future study will continue to focus applying this PKI model to actual autonomous vehicles.

**Acknowledgement.** This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-R0992-15-1011) supervised by the IITP(Institute for Information & communications Technology Promotion)

## References

[1] Stefan Kaufmann, Implementation and Adaptation of the Pseudonymous PKI for Ubiquitous Computing for Car-2-Car Communication, Chapter in *Automotive-Safety & Security* 2014 (*2015)*, 2014.

[2] Bo Qin, Qianhong Wu, Josep Domingo-Ferrer and Lei Zhang, Preserving Security and Privacy in Large-Scale VANETs, Chapter in *Information and Communications Security,* Volume 7043 of the series Lecture Notes in Computer Science, 2011, 121-135.
http://dx.doi.org/10.1007/978-3-642-25243-3_10

[3] Nikolaos Alexiou, Stylianos Gisdakis, et al., Towards a secure and privacy-preserving multi-service vehicular architecture, *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM),* (2013), 1-6.
http://dx.doi.org/10.1109/wowmom.2013.6583472

[4] Nayana P. Vaity, Surekha Janrao, Randeep Kaur, Efficient communication approach in Vehicular PKI, *International Journal of Engineering Trends and Technology (IJETT),* **18** (2014), no. 5, 2015-2020.
http://dx.doi.org/10.14445/22315381/ijett-v18p244

[5] Xuedan Jia, Xiaopeng Yuan, Lixia Meng, Liangmin Wang, EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication, *Journal of Software, **8** (2013) no. 8,* 1914-1922. http://dx.doi.org/10.4304/jsw.8.8.1914-1922

[6] Andre Weimerskirch, V2X security & privacy: the current state and its future, *ITS World Congress,* Orlando, FL, 2011.

[7] IEEE Standard for Wireless Access in Vehicular Environments, Security Services for Applications and Management Messages WAVE 1609.2- 2016. http://dx.doi.org/10.1109/ieeestd.2016.7426684

**Received: April 15, 2016; Published: June 2, 2016**