Design and Implementation of Certificate Revocation List Acquisition Method for Security of Vehicular Communications

Hyun Gon Kim◆

ABSTRACT

Distributing a Certificate Revocation List (CRL) quickly to all vehicles in the system requires a very large number of road side units (RSUs) to be deployed. In reality, initial deployment stage of vehicle networks would be characterized by limited infrastructure as a result in very limited vehicle to infrastructure communication. However, every vehicle wants the most recent CRLs to protect itself from malicious users and malfunctioning equipments, as well as to increase the overall security of the vehicle networks. To address this challenge, we design and implement a nomadic device based CRL acquisition method using nomadic device's communication capability with cellular networks. When a vehicle could not directly communicate with nearby RSUs, the nomadic device acts as a security mediator to perform vehicle's security functions continuously through cellular networks. Therefore, even if RSUs are not deployed or sparsely deployed, vehicle's security threats could be minimized by receiving the most recent CRLs in a reasonable time.

Key Words : Vehicular network, Secuiry threats, CRL, Nomadic device

Ⅰ. Introduction

Vehicular network has been one of the emerging research areas and promising way to facilitate road safety, traffic management, and infotainment dissemination of drivers and passengers. However, without the integration of strong and practical security and privacy enhancing mechanisms, vehicular communication system can be disrupted or disabled, even by relatively unsophisticated attackers.

Security and privacy are essential components for the successful deployment of vehicle networks. Those components need to be carefully assessed and addressed in the design of the vehicular communication system, especially because of the life-critical nature of the vehicular network operation. The IEEE 1609.2 standard[1] defines security services for vehicular networks. It defines secure message formats and techniques for processing these secure messages using the public key infrastructure (PKI). In traditional PKI architecture, the most commonly adopted certification revocation scheme is using certificate revocation lists (CRLs) method, which is a list of revoked certificates stored in repositories prepared by certificate authorities (CAs).

In vehicular networks, the CA adds the identification of the revoked certificate(s) to a CRL. The CA then publishes the updated CRL to all vehicular network participants, and instructing them not to trust the revoked certificate. Timely access to revocation information is important for the robustness of its operation: message faulty, compromised, or otherwise illegitimate, and overall potentially dangerous, vehicles can be ignored.

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2011-0027-006)
◆ 주저자 : Department of Information Security, Mokpo National University, hyungon@mokpo.ac.kr, 정회원
논문번호 : KICS2012-04-224, 접수일자 : 2012년 4월 29일, 최종논문접수일자 : 2012년 6월 18일

The CA employs a set of road side units (RSUs) to broadcast CRLs to all vehicles as they pass by. However, this RSU-based revocation may be challenging in certain areas (e.g., rural regions) where not enough RSUs are deployed or maintained. It is likely that RSUs will be sparsely placed in real environments, and thus, vehicles may spend significant time outside radio range of an RSU[2]. For example, RSUs are typically located along the highway and major roads in rural area. If the vehicle goes off major road and enters the less populated area or narrow and unpaved road, RSU may not be deployed in this area or road. In this case, a vehicle may rarely encounter an RSU as result in a long delay until the vehicle receives recent CRLs. The delay could create a potential threat to the security of vehicular networks. Even if RSUs are eventually deployed with sufficient density, vehicular networks must be able to operate during stages of incremental deployment, that is, before sufficient densities of RSUs come online.

The unavailability of CRL server and the lack of RSU connectivity would hinder the peer communication in verifying the certificate and would pose definite security threats of misusing certificates. Therefore, CRL distribution should distribute quickly to all vehicles within the networks and vehicles should receive the most recent CRLs as quickly as possible. Under these conditions, the problem is how to design functions that can achieve the most recent CRLs without interruption.

Our proposal has been concerned with the fundamental problem of how to achieve CRLs without interrupt across wide regions including rural regions. The basic idea is that if a vehicle can receive CRLs via an alternative communication media effectively, the epidemic distribution method can be used to achieve them. In this paper, we propose a nomadic device based CRL acquisition method using nomadic device's communication capability with cellular networks. When a vehicle could not directly communicate with nearby RSUs, the nomadic device will acts as a security mediator to perform security functions continuously through cellular networks. Therefore, even if RSUs are not deployed or sparsely deployed, vehicles can obtain the most recent CRLs using by nomadic device.

The reminder of the paper is organized as follows: Section II presents the related works, which focus on the different access technologies and the use of nomadic device; Section III introduces the proposed nomadic device based CRL acquisition method, which specifies design principles, network reference model, identified functional requirements, CRL acquisition procedure and algorithm; Section IV describes implementation results for security mediator on a android based smartphone; Section V summarizes results and end with some conclusions.

Ⅱ. Related Works

The problem of certificate revocation in vehicular networks has hardly attracted any attention in the literature. Papadimitratos et al.[3] aim at achieving scalable and efficient mechanism for the distribution of large CRLs across wide regions by utilizing a very low bandwidth at each RSU. CRLs are encoded into numerous self-verifiable pieces, so vehicles only get from the RSUs those pieces of the CRLs. Laberteaux et al.[4] proposed that revocation information is distributed in the form of a CRL in an epidemic mechanism through vehicle-to-vehicle communications. The mechanism provides significant advantages compare to the RSU-based distribution mechanism in terms of speed and breadth of network coverage. Lin et al.[5] present solution based on RSU-aided certificate revocation. Each RSU maintains the complete and updated base-CRL and continuously check the status of the certificates contained within all the messages broadcasted by passing vehicles. If a certificate has been revoked, the RSU broadcasts a warning message such that approaching vehicles can update their CRLs and avoiding communicating with the compromised vehicle.

2.1. Access Technologies for Vehicular Networks

The IEEE 802.11p/Wireless Access in Vehicular Environment (WAVE) standard is intended to provide wireless access to vehicles on the roads [1]. With respect to access technologies, one of the most significant efforts in combining wireless access technologies by ISO TC 204 WG16 is that different mobile communication networks could be used for access technologies like 3G cellular, 4G cellular, WiMax, or digital multimedia broadcasting (DMB), as well as short range communication systems like WiFi or, dedicated short-range communications (DSRC) as shown in Fig. 1. Radio cells of cellular networks and radio cells of vehicular networks will be overlaid independently according to maximum radio range of them. Lequerica et al.[6] proposed a use of the existing multimedia broadcast multicast service over 3G cellular networks, which improve the efficiency of the distribution of the CRL. Sommer et al.[7] present simulation results of a 3G cellular-based vehicle-to-infrastructure traffic information system.

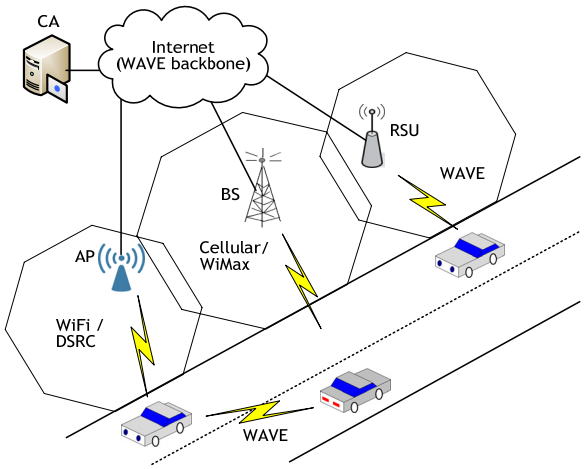

Fig. 1. Access technologies for vehicular networks

2.2. Use of Nomadic Devices in Vehicular Networks

External nomadic devices in a vehicle could include all types of information and communication as well as entertainment devices that can be brought into the vehicle by the driver to be used while driving in vehicular networks. Current examples are smartphones, mobile phones, portable computers, pocket PCs, PDAs, mobile navigation devices, iPods and future multi-functional smart phones.

Regarding the use of nomadic devices in vehicular networks, the ISO 13815 standard has been established to define the requirements of common software to a vehicle gateway to easily exchange vehicle information data among nomadic device, vehicle mobile gateway (VMG) and the vehicle's engine control units (ECUs)[8]. The standard also specifies the interface between VMG and nomadic device for provisioning and support of VANET service. Consequently, nomadic devices could be utilized as a communication mediator especially, in initial deployment stage of vehicular networks.

On the other hand, we can find some works that adopt nomadic devices, especially Android based smartphone, to support all sorts of VANET service. Hernandez et al.[9] developed a prototype of an on-board unit that allows the driver to communication with his vehicle, as well as with other available devices (PDAs, cellular, sensor networks, and so on) and with the road infrastructure in order to consume VANET service. Spelta et al.[10] implemented a system for vehicle-to-driver and vehicle-to-environment communication, based on a smart-phone core and Bluetooth communication. Jorge et al.[11] proposed combining existing vehicles with smartphones to achieve a solution able to improve security on the road. The smartphones are used as an alternative on-board unit within the vehicle.

Ⅲ. Design of a CRL Acquisition Method

A nomadic device could be used as alternative WAVE security functions of the vehicle, accessing the information in the vehicle's internal bus wirelessly. More specifically, it is possible to use the nomadic device with capability of the WAVE security functions when the vehicle is out of the communication range of nearby RSUs. In this

section, we present an example of how a nomadic device can be properly integrated with the VMG to achieve the security functions through wireless communication networks.

The security functions will provide the WAVE security services for applications and management messages defined in IEEE 1609.2[1]; those will ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust and so on. To integrate nomadic devices into vehicular networks, Fig. 2 shows the network reference model as a primary architectural model for interworking cellular networks. The nomadic device will act as a security mediator between CA and security-specific ECU for providing the WAVE security functions.

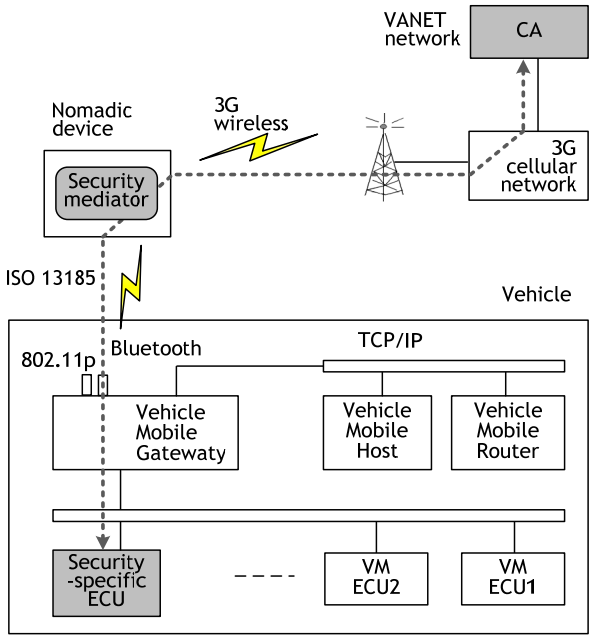

Fig. 2. Network reference model

Nomadic devices typically include different wireless interfaces such as Bluetooth, WiFi, and 3G, making them ideal for our purpose. The VMG is an interface device in the vehicle to act as the vehicle's mobile gateway between the vehicle's ECU(s) and the external nomadic device. The security-specific ECU would perform the WAVE security functions including cryptographic operations, as well as key and device management functions based on the IEEE 1609.2 standard. The main cryptographic operations provided by the hardware security module are digital signature generation and decryption of encrypted messages. The digital signature generation function is mainly used by the secure communication module for signing outgoing messages.

We assume that the security mediator in the nomadic device only performs CRL acquisition related functions, not providing full WAVE security functions in this paper. Thus, the nomadic device is utilized as a CRL acquisition device and an application capable of relaying CRLs to the security-specific ECU. Also, the nomadic device has a capability to communicate with CA through cellular networks, and the VMG through Bluetooth interface. The security mediator can be implemented as a smartphone application.

3.1. Functional Requirements of Nomadic Device

The basic function of a security mediator is to allow a nomadic device to receive CRLs from CA and to forward them to the internal security-specific ECU if vehicle-to-RSU connectivity is not available. The functional requirements for providing the proposed method are identified as follows:

- ○ The nomadic device has communication redundancy by using a WAVE network interface and a 3G cellular network interface.
- ○ The nomadic device has to have the ability to identify and use appropriate communication media for providing stable connectivity.
- ○ If vehicle-to-RSU connectivity is not available, the nomadic device has to have the ability to activate the security mediator automatically. In some cases, user can active the security mediator function manually.
- ○ To access the VMG, the nomadic device performs user or device authentication based

on the pre-shard secrets[8].

○ The nomadic device can receive CRLs from CA continuously through cellular networks.

○ Upon receiving CRLs, the nomadic device forwards them to the VMG

3.2. CRL Acquisition Procedure and Algorithm

The CRL acquisition procedure and algorithm are depicted in Fig. 3 and Fig. 4 respectively. This use case demonstrates that the security mediator application in the nomadic device gets the most recent CRLs from CA and forwards them to the VMG in the vehicle when user enters a vehicle and the nomadic device has been equipped with its holder without user interruption.

The CRL acquisition procedure involves the following steps: (1) the security mediator would be activated initially, (2) it requests user authentication, where user name and password for user or device authentication would be send to the VMG, (3) if authentication is successful, the VMG returns the user *Authentication succeed.* to the nomadic device, (4) if the security mediator supports full WAVE security functions, security operations would be performed between the CA and the security-specific ECU. However, this step will not be performed since the security mediator only performs CRLs acquisition, not providing full WAVE security functions, (5) the CA in the vehicular networks would distribute CRLs periodically. The nomadic device would receive the list from CA and relay it to the VMG, (6) the VMG also would relay it to the security-specific ECU, (7) the security-specific ECU would use them to provide secure communications and user privacy protection.

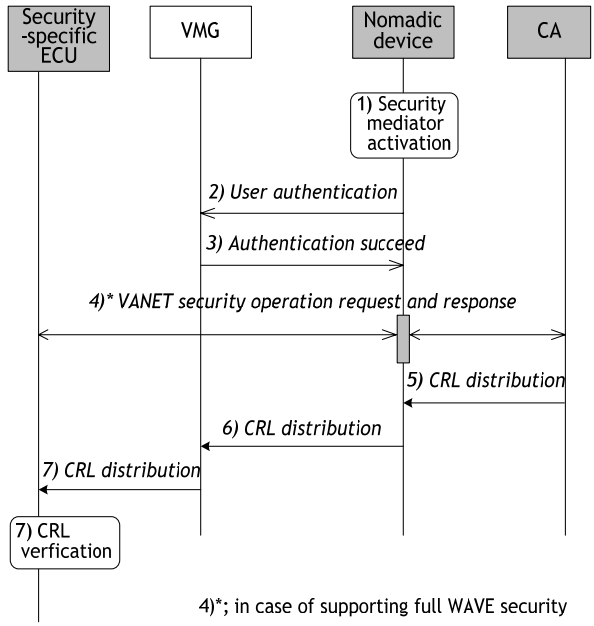

Fig. 3. CRL acquisition procedure

```
Algorithm for security mediator
1: In the WAVE network do:
2: Initialize security mediator process as a daemon;
3: Check VANET interface status;
4: if (WAVE interface is inactive) then
5:    Active cellular interface and set cellular_inf = ACTIVE;
6:    Authentication request to VMG
7:    if (authentication is success) then
8:       Auth = SUCC;
9:    else
10:      Auth = FAIL;
11:      Go to 2;
12:   endif
13: else
14:   Go to 2;
15: endif
16: loop CRL acquisition;
17:    if (receive a CRL from CA) then
18:      if (cellular_inf == ACTIVE and Auth == SUCC) then
19:        Forward the received CRL to VMG;
20:      endif
21:    else
22:      if (WAVE interface is active) then
23:        cellular_inf = INACTIVE;
24:      Go to 3;
25:    endif
26: end loop
```

Fig. 4. CRL acquisition algorithm

Ⅳ. Implementation and Test

In order to realize the security mediator, we implement a software of security mediator running on android-based smartphone, called CRLacq application, by using Android SDK(v.2.2) and Eclipse Galileo IDE(v.1.2.2) software tools[12]. The smartphone equipped with different wireless interface thus, IEEE 802.11p, Bluetooth, and 3G cellular. The CRL acquisition procedure and algorithm described in Fig. 3 and Fig. 4 have been implemented on the Pentium IV notebook with 1.73GHz and the Pentium IV desktop with 2.82GHz respectively.

To distribute CRLs, we utilize the Android Cloud to Device Messaging (C2DM) service that supports push service through 3G cellular network and helps developers send data from servers to their applications on Android devices[13]. In the C2DM service, three parties are involved as shown in Fig. 5; the CA server (e.g, application server) which wants to push messages to the nomadic device, the C2DM server, and the CRLacq application in the nomadic device. The C2DM service allows nomadic devices to register and receive push notifications from C2DM servers.

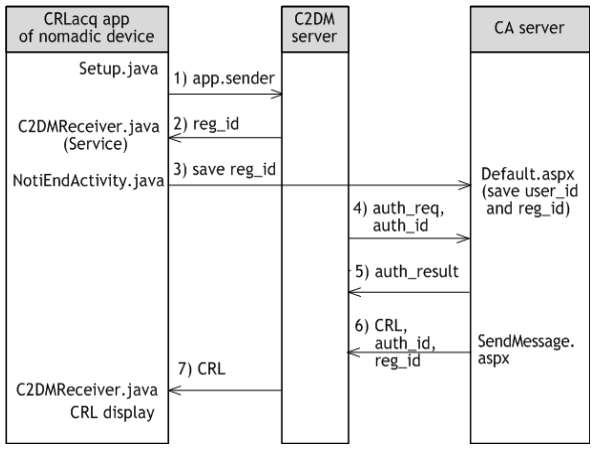

Fig. 5. CRL distribution procedure based on C2DM push service

The CA server creates CRLs as shown in Table 1 for test and sends them via an HTTP POST to the C2DM server as shown in Fig. 5. Upon receiving the CRLs, the C2DM server routes them to the nomadic device and then, the CRLacq application can receive them. Whenever the CRLacq application receives CRLs then, it relays them to the security-specific ECU through the VMG. Fig. 6 shows test configuration and results, which include the screen shot of the CRLacq application and the active window of the VMG.

Table 1. CRLs for test

Cert ID	Hashed certificate id	Expiry
64382	1, 101, 3, 15, -118, 11, 124, -71, -7, 5	2011-12-04 09:31:21
64381	22, 93, 110, 96, -104, 9, 99, 61, 48, 42	2011-12-04 09:20:38
64383	82, -33, -10, 32, -60, -57, -34, -84, -78, 78	2011-12-04 09:37:09
64384	56, -97, -35, 28, 127, 24, 113, -93, 55, -102	2011-12-04 09:42:19
64385	-32, -35, -109, 116, -44, 60, -23, -101, -82, 2	2011-12-04 09:46:58
38940	109, -54, -4, -113, -118, -95, 36, -61, 114, -95	2011-12-04 09:23:54
39068	1, -122, 85, 54, 105, -78, -26, 24, -68, -11	2011-12-04 09:31:36
39106	-14, 74, -105, -124, 117, -78, 100, 71, -53, -46	2011-12-04 09:36:05

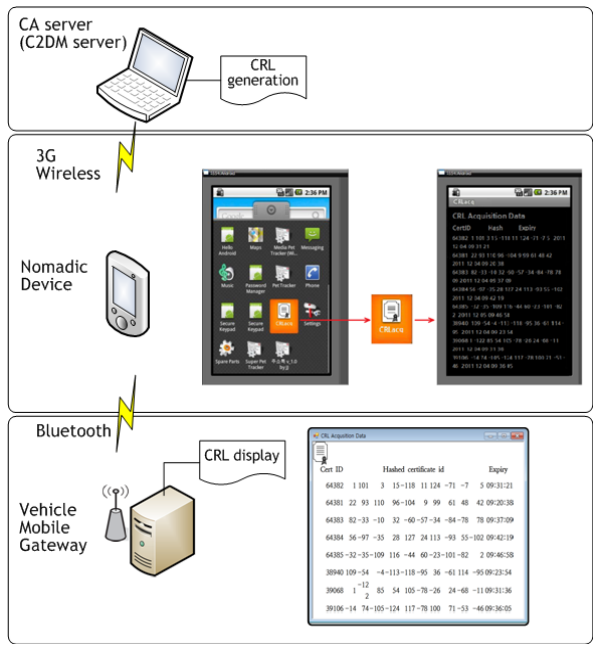

Fig. 6. Test results of implemented CRLacq application

Ⅴ. Conclusions

From a business point of view, utilizing smartphones for vehicular networks is very attractive. The presented results indicate that the utilization of smartphones for vehicular networks is feasible in specific circumstances especially, security of vehicular networks. In this paper, we have presented an example of how a nomadic device can be properly integrated with the vehicle to achieve the WAVE security functions through wireless communication networks. When a vehicle could not directly communicate with nearby RSUs, the nomadic device will acts as a security mediator to perform WAVE security functions continuously. Therefore, even if RSUs are not deployed or sparsely deployed, vehicle's security threats could be reduced by receiving the most recent CRLs in a reasonable time. The disadvantage of this approach is that additional resource allocations in wireless cellular networks are required for CRL distributions.

To complete the proposed method, we have discussed and presented design principles, network reference model, identified functional requirements, CRL acquisition procedure and algorithm, and implementation and test. As a part of further work, we have been planning to implement the full WAVE security functions on Android-based smartphone as a form of application.

References

[1] IEEE Std 1609.2, "Trial-use standard for wireless access in vehicular environments - Security services for applications and management message," *IEEE Standard 1609.2*, 2006.

[2] R. Resendes, "The new grand challenge - Deploying vehicle communications, keynote address," *15th ACM International Workshop on Vehicular Internetworking*, 2008.

[3] P. Papadimitratos, G. Mezzour, and J. P. Hubaux, "Certificate revolution list distribution in vehicular communication systems," *15th ACM International Workshop on Vehicular Internetworking*, pp. 1-10, 2008.

[4] K. P. Laberteaux, J. J. Haas, Y. C. Hu, "Security certificate revocation list distribution for VANET, *15th ACM International Workshop on Vehicular Internetworking*, pp. 88-89, 2008.

[5] X. Lin, R. Lu, C. Zhang, H. Zhe, P. H. Ho, X. Shen, "Security in vehicular ad hoc networks," IEEE Communications Magazine, Vol. 46, No. 4, pp. 88-95, 2008.

[6] I. Equerica, J. A. Martinez, P. M. Ruiz, "Efficient certificate revocation in vehicular networks using NGN capabilities," *Vehicular Technology Conference*, pp. 1-5, 2010.

[7] C. Sommer, A. Schmidt, R. German, W. Koch, F. Dressler, "Simulative evaluation of a UMTS-based car-to-Infrastructure traffic information system," Proc. *IEEE Global Telecommunications Conference (GLOBECOM)*, 2008.

[8] ISO/TC 204/SC, "Intelligent transport systems (ITS) – Vehicle interface for provisioning and support of ITS services – Part1: General information and use case definition," *ISO standard 13185-1.7*, 2010.

[9] U. Hernandez, A. Perallos, N. Sainz, and I. Angulo, "Vehicle on board platform: Communications test and prototyping," *Intelligent Vehicles Symposium (IV)*, pp. 967-972, 2010.

[10] C. Spelta, V. Manzoni, A. Corti, A. Goggi, and S. Savaresi, "Smartphone- based vehicle-to-drive/environment interaction system for moto cycles," Embedded Systems Letters, Vol. 2, No. 2, pp. 39-42, 2010.

[11] J. Zaldivar, C. T. Calafate, J. C. Cano, P. Manzoni, "Providing accident detection in vehicular networks through OBD-II devices and android-based smartphones," *5th IEEE Workshop on User Mobility and Vehicular Networks*, pp. 813-819, 2011.

[12] Shane Conder, Lauren Darcey, "Android Wireless *Application Development (2nd*

Edition)", Addison-Wesley, December 25, 2010.

[13] Android Cloud to Device Messaging Framework, https://developers.google.com/android/c2dm/

Hyun Gon Kim

He received a B.S. and a M.S. degrees at department of electrical engineering of Kumoh National Univ., and Ph. D degree at computer science of Chungnam National Univ. in 1992, 1994, and 2003 respectively. He worked at division of Information Security of ETRI from 1994 to 2005 as a senior engineer and a project manager. He is currently an associate professor at department of Information Security of Mokpo National University. His research interests include security of vehicle ad hoc network, security of mobile communications, and security of wireless Internet.