Journal of Korea Multimedia Society Vol. 14, No. 12, December 2011(pp. 1583-1590)

Certificate Revocation Scheme using MOT Protocol over T-DMB Infrastructure

Hyun Gon Kim†, Min Soo Kim††, Seok Won Jung†††, Jae Hyun Seo††††

ABSTRACT

A Certificate Revocation List(CRL) should be distributed quickly to all the vehicles for vehicular communications to protect them from malicious users and malfunctioning equipment as well as to increase the overall security and safety of vehicular networks. Thus, a major challenge in vehicular networks is how to efficiently distribute CRLs. This paper proposes a Multimedia Object Transfer(MOT) protocol based on CRL distribution scheme over T-DMB infrastructure. To complete the proposed scheme, a handoff method, CRL encoding rules based on the MOT protocol, and relative comparison are presented. The scheme can broaden breadth of network coverage and can get real-time delivery with enhanced transmission reliability. Even if road side units are sparsely deployed or, even not deployed, vehicles can obtain recent CRLs from T-DMB infrastructure effectively.

Key words: Carousel, Anonymous Certificate, CRL

1. INTRODUCTION

Vehicular ad hoc networks are emerging research area and promising approach to facilitating 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 is an issue that needs 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] and the European PRE-DRIVE C2X standard [2] define security services for vehicular ad hoc networks. They define 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 through CRLs which is a list of revoked certificates stored in repositories prepared in 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, instructing them not to trust the revoked certificate. Timely access to revocation information is important for

※ Corresponding Author : Jae Hyun Seo, Address : 560 Muanno, Cheonggye-myeon, Jeonnam, 534-729, TEL : +82-61-450-2712, FAX : +82-61-450-6215, E-mail : jhseo@mokpo.ac.kr
Receipt date : Nov. 12, 2011, Revision date : Dec. 21, 2011
Approval date : Dec. 28, 2011
† Associate Professor, Dept. of Information Security, Mokpo National University, Korea (E-mail : hyungon@mokpo.ac.kr)
†† Associate Professor, Dept. of Information Security, Mokpo National University, Korea (E-mail : phoenix@mokpo.ac.kr)
††† Associate Professor, Dept. of Information Security, Mokpo National University, Korea (E-mail : jsw@mokpo.ac.kr)
†††† Professor, Dept. of Information Security, Mokpo National University, Korea
※ 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).

the robustness of its operation: message faulty, compromised, or otherwise illegitimate, and overall potentially dangerous, vehicles can be ignored.

The CA employs a set of Road Side Units(RSUs) to broadcast CRLs to all vehicles as they pass. 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[3]. In this area a vehicle may rarely encounter an RSU and thus, there may be a long delay until the vehicle receives recent CRLs, which may cause 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. Therefore, CRL distribution should spread quickly to every vehicle within the networks.

On the other hand, for vehicular networks several broadcasting techniques are taken into account. That includes some narrow bandwidth solution like FM radio, but also wider bandwidth digital services such as DAB, DVB, DVB-H, T-DMB etc[2]. Broadcasting appears to be an attractive solution due to its low cost, large coverage range, and large potential volumes of data. There is already some service available that based on T-DMB broadcasting and Transport Protocol Experts Group(TPEG) protocol, offer real-time traffic information. T-DMB service is already commercialized for free and infrastructures are widely deployed in Korea. T-DMB data broadcasting service provides mobile users with various data such as web sites, picture files, and traffic reports through its data channels.

To the best of our knowledge all the solutions in the state of the art, RSU-based distribution schemes as well as vehicle-to-vehicle distribution schemes are non-effective solutions in terms of delays, availability, liability, limited transmission ranges, and real-time delivery. Under these conditions, the problem at hand is how to design a system that can distribute revocation information effectively.

Our proposal has been concerned with the fundamental problem of how to distribute CRLs in a real-time manner across wide regions including rural regions. The basic idea is that if a subnet of vehicular network nodes can receive CRLs via an alternative communication media effectively, epidemic distribution schemes can be used to broadcast them. From point of this view, we utilize the advantage of T-DMB data broadcasting service based on the MOT protocol in terms of real-time delivery, wide network coverage, and enhanced transmission reliability using an alternative communication media thus, T-DMB data broadcasting channels.

The reminder of the paper is organized as follows. In section 2, we first review the related works in this area. In section 3, we then propose a MOT protocol based CRL distribution scheme including a handoff method and CRL encoding rules on the MOT protocol. Subsequently, we discuss relative comparison and finalize with some conclusions.

2. RELATED WORKS

2.1. CRL Distribution Schemes

The problem of revocation in vehicular networks has attracted scant attention in the literature. Papadimitratos[4] used a very low bandwidth at each RSU in an effort to achieve an efficient scalable mechanism for the distribution of large CRLs across a wide region. They propose the encoding of CRLs into numerous self-verifiable pieces, so vehicles only get from the RSUs those pieces of the CRL that are not on-board.

Laberteaux[5] proposed that revocation information be distributed in the form of a CRL via

an epidemic mechanism that relies on vehicle-to-vehicle communication. The mechanism has significant advantages over an RSU-based distribution mechanism, particularly in terms of the speed and breadth of the network coverage.

Lin[6] proposed the use of RSU-aided certificate revocation. Each RSU has a completely updated base-CRL and continuously checks the status of the certificates contained in all the messages broadcast by passing vehicles. If a certificate has been revoked, the RSU broadcasts a warning message so that approaching vehicles can update their CRLs and avoiding communicating with the compromised vehicle.

Reducing the size and computational cost of processing CRLs has been the focus of extensive research on vehicular networks. Bellur[7] proposed the segmentation of an administrative area into a number of geographic regions and the assignment of region-specific certificates to an On-Board-Unit(OBU) resident of a vehicle; these measures could significantly reduce the size of CRLs.

Raya[8,9] combined two protocols tailored for vehicular networks: Revocation of a Trusted Component(RTC) and Revocation using Compressed Certificate Revocation Lists(RC^2RL). The former reduces the number of certificates that need to be inserted in the CRL, but CA must be able to geographically localize any vehicle in the system. The RC^2RL protocol is a CRL compressed with Bloom filter compression to limit the size of the CRL. Because of the false positive characteristic of Bloom filter compression, some legitimate certificates may also be revoked.

2.2. UMTS aided Distribution Schemes

Most ongoing projects are based on the IEEE 802.11p and ITS-G5A standards. Nevertheless, other mobile access technologies such as UMTS, WiMax and DMB can be used to distribute CRLs [10]. Lequerica[11] used an existing multimedia broadcast multicast service over UMTS and improved the efficiency of the CRL distribution. Sommer[12] presented simulation results of a UMTS-aided vehicle-to-infrastructure traffic information system. However, in spite of the low usage of cellular channels in these schemes, the UMTS bearer service is still needed.

2.3. ITS Network Reference Model

Figure 1 shows the network reference model of the European ITS communication architecture [2]. An ITS vehicle station compromises a number of ITS-specific functions. An ITS rodeside station, such as an RSU, can act as a gateway between the ITS ad hoc network domain and the network domain of the ITS roadside infrastructure. A border router offers IP connectivity to an ITS vehicle station and a core network switch in an Internet domain.

Two of the main components of a generic access network domain are the UMTS system and the DMB infrastructure. IP packet transport is assured by means of a generic IP access network or by means of encapsulation and tunnelling over the ad hoc network for vehicle-to-vehicle and vehicle-to-infrastructure communication. The ITS application service domain contains a backend server and a traffic management center.

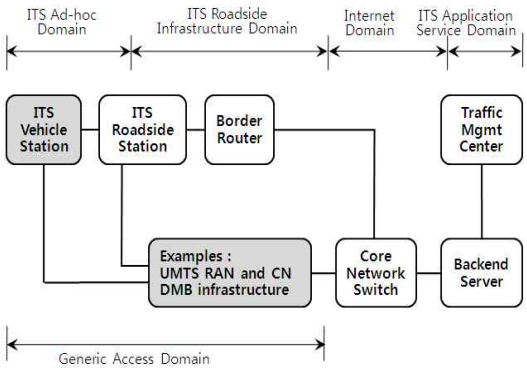

Fig. 1. European ITS Network Reference Model.

3. PROPOSED MOT PROTOCOL BASED CRL DISTRIBUTION SCHEME

In this session, we describe the proposed MOT protocol based CRL distribution scheme. Every vehicle requires the most recent CRL for protection against malicious users and malfunctioning equipments. Up-to-date CRLs increase the overall security and safety of the vehicular networks. We use a T-DMB data broadcasting service[13] to efficiently broadcast CRLs because the service has several advantages: besides being economical, it offers real-time delivery, wide network coverage, and enhanced transmission reliability.

The MOT protocol based CRL distribution scheme is based on the following design principles and assumptions:

- Besides the usual ETSI ITS-G5A module interface, a vehicle has a T-DMB terminal and another module interfaces.
- The T-DMB terminal interfaces with OBU in the vehicle.
- The deployment of RSUs can be sufficient, sparse or, in some areas, non-existent. Hence, sometimes vehicles may be unable to receive recent CRLs from an RSU or from neighboring vehicles.
- The CA periodically sends recent CRLs to a T-DMB base station that the CRLs can be broadcast over T-DMB data broadcasting channels.
- The coverage of T-DMB networks is wide and includes full coverage of vehicular networks.

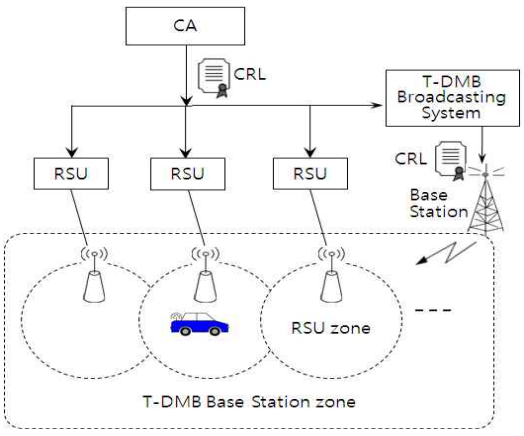

Fig. 2. MOT Protocol based CRL Distribution Scheme.

Fig. 2. shows a schematic of the proposed scheme. In addition to the RSU-based distribution, the CA uses T-DMB data broadcasting channels to distribute duplicated CRLs. The CA periodically sends recent CRLs to the RSU and the T-DMB base station over a fixed wireline in the same manner. Thus, at any given time the same CRLs are doubly distributed to vehicles through an RSU and a T-DMB base station. In an area where the RSU density is adequate, a vehicle can connect to the RSU directly; however, where the RSU density is low, a vehicle can switch over to the T-DMB base station. For this to happen, the interface of a vehicle must be changed from the IT-G5A module interface to the T-DMB module interface or vice versa. A vehicle that has no T-DMB module can use vehicle-to-vehicle communication to obtain CRLs broadcast from a neighboring vehicle.

3.1. A Handoff Method

The proposed scheme is based on the concept of an overlay zone, which occurs when the coverage of the RSU transmission overlaps with the coverage of a T-DMB base station transmission. In overlay zones, vehicles can directly obtain an RSU and a T-DMB base station. The standard[2] maximum cell coverage of ITS-G5A is approximately 500m for an RSU based on ITS-G5A, 1km for an RSU based on a Dedicated Short-Range Communication(DSRC) communication system, and 35km for a T-DMB base station. Therefore, as shown in Figure 3, the zone of a single base station′(T-DMB$_{zone}$) consists of several RSU′ zones(RSUs$_{zone}$). A single base station can therefore be expressed as follows:

$$T\text{-}DMB_{zone}\text{-}A \supseteq RSU_{zone}\text{-}A + RSU_{zone}\text{-}B + RSU_{zone}\text{-}C + \quad (1)$$

Fig. 3 shows how a vehicle that enters RSU_{zone-A} can receive CRLs from its ITS-G5A module interface namely, from RSU-A. If the vehicle travels beyond the transmission range of both RSU-A and RSU-B, it can still receive CRLs from its T-DMB module interface namely, the T-DMB base station.

Whenever the vehicle travels outside the RSU transmission range, the ITS-G5A module interface can be changed to the T-DMB module interface. The CA is responsible for the provision and maintenance of $T\text{-}DMB_{zone}$ to manage CRL distribution zones based on the T-DMB base station cell coverage. With $T\text{-}DMB_{zone}$, the CA can manage the CRL distribution zones on the basis if the cell coverage of the T-DMB base station. The logically designed RSU-based zones are assumed to be mapped to $T\text{-}DMB_{zone}$. The CA may collaborate with the T-DMB broadcasting system so that it can present $T\text{-}DMB_{zone}$ information and distribute CRLs through the T-DMB infrastructure.

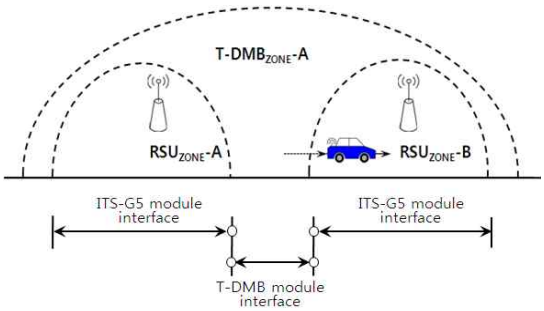

Fig. 3. Handoff between Vehicular Network and T-DMB Network.

3.2 CRL Encoding Rule based on the MOT Protocol

MOT is a transfer protocol used for data broadcasting providing a common interface for the transfer of objects and files respectively. The interface to MOT is an easy-to-use access point to T-DMB data channels and transmission modes. We adopt the MOT protocol to send CRLs efficiently. For this, the segmentation process from CRLs to MOT objects might need to be defined.

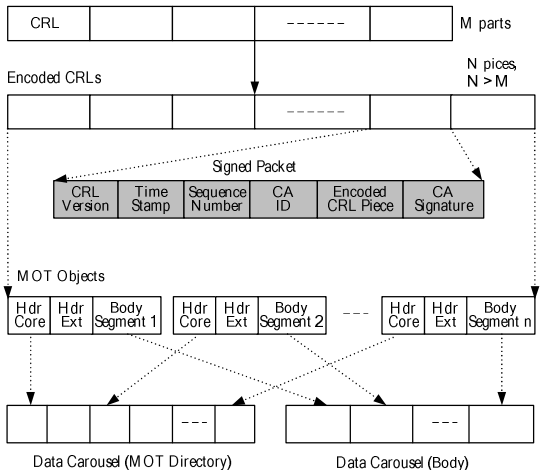

Fig. 4. CRL Encoding Rule based on MOT data carousels.

The original CRLs could be encoded to ensure that the CRL transmissions are efficient and reliable[14]. Fig. 4 shows a schematic of the CRL encoding. First, the CA generates a CRL and divides it into M pieces of equal length. The pieces are encoded with an erasure code and sorted into N redundant pieces. A header is added to each piece, and each peace is signed by the CA. The header contains the CRL version, a time stamp for avoiding a replay attack, the sequence number of the encoded piece, and ID number of the CA′. Then, MOT encoder generates the complete MOT objects including additional header information from all encoded CRLs. Each encoded CRL is divided into objects of equal length and then the objects are assigned to the data carousels as the form of MOT directory and body individually. Afterward, data carousels are broadcasted to the vehicles through RSUs and T-DMB base stations cyclically.

Upon receiving one of the signed packets from MOT decoder, a vehicle verifies the signature and time stamp of the message. To verify the signature, the vehicle searches its database for the public key associated with the CA ID extracted from the message. If the signature is valid, the vehicle checks whether this piece is already stored; if not, the vehicle stores the piece with the asso-

ciated sequence number. When the vehicle receives enough pieces, it decodes the pieces and subsequently obtains the original CRL.

4. RELATIVE COMPARISONS

In this session, we summarize and compare the characteristics of the different revocation schemes introduce in this paper. Table 1 highlights the efficiency of MOT protocol based CRL distribution. The UMTS-aided distribution is more efficient than the RSU-based distribution in terms of the throughput, guaranteed freshness and so on but not the CRL distribution cost. The high throughput, guaranteed freshness, and low CRL acquisition delay are key factors in determining the feasibility of the proposed MOT protocol based CRL distribution scheme. However, the proposed scheme has the disadvantage of requiring an additional T-DMB infrastructure and T-DMB module in the vehicle.

Table 1. Relative Comparison of CRL Distribution Schemes

RSU-based distribution	UMTS-aided distribution	MOT protocol based distribution
Throughput		
A few hund- red Kbps[4]	A few Mbps	A few Mbps
Freshness in rural areas		
Not guarantee	Guaranteed	Guaranteed
CRL acquisition delay in rural areas		
High[4]	Low	Low
CRL distribution cost		
Low	High	Low
CRL re-transmission		
Least efficient	Moderate	Most efficient
Transmission efficiency of large CRL		
Least efficient	Moderate	Most efficient
Communications		
Bi-directional	Bi-directional	Omni-directional
Interface with other access networks		
No need	Need	Need

5. CONCLUSIONS

We present basic ideas on a CRL distribution scheme for vehicular networks, with a focus on the use of an alternative communication media. The main objectives of the proposed scheme pertain to the fundamental problem of how to distribute CRLs in real-time across wide regions including rural areas. Our design approach is based on a T-DMB aided CRL distribution and utilizes the MOT protocol to distribute CRL efficiently. High throughput, guaranteed freshness, and low CRL acquisition delay are key factors in determining the feasibility of the proposed CRL distribution scheme. The proposed scheme can also broaden the network coverage, attain real-time delivery, and enhance transmission reliability. Even if RSUs are not deployed or only sparsely deployed, vehicles can obtain recent CRLs from the T-DMB infrastructure. However, it has the disadvantage of requiring an additional T-DMB infrastructure and T-DMB module in the vehicle.

REFERENCES

[1] IEEE Std 1609.2, “Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Message,” *IEEE Std 1609.2*, Vol.1. No.1, pp. 1-105, 2006.

[2] M. Bechler, “PRE-DRIVE Implementation and Evaluation of C2X Communication Technology, Deliverable D3.,” *PRE-DRIVE Std., Version 3.0*, pp. 1-187, 2009.

[3] R. Resendes, “The New 'Grand Challenge' - Deploying Vehicle Communications, Keynote Address,” *The Fifth ACM International Workshop on VehiculAr InterNETworing (VANET 2008)*, pp.1-20, 2008.

[4] P. Papadimitratos, G. Mezzour, and J. P. Hubaux, “Certificate Revocation List Distribution in Vehicular Communication Systems,”

The Fifth ACM International Workshop on VehiculAr InterNETworing (VANET), pp. 86-87, 2008.

[5] Kenneth P. Laberteaux, Jason J. Haas, and Yih-Chun Hu, "Security Certificate Revocation List Distribution for VANET," *The Fifth ACM International Workshop on VehiculAr InterNETworing (VANET)*, pp. 88-89, 2008.

[6] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, Xuemin Shen, "Security in Vehicular Ad Hoc Networks," *IEEE Communications Magazine*, Vol.46, No.4, pp.88-95, 2008.

[7] Bhargav Bellur, "Certificate Assignment Strategies for a PKI-based Security Architecture in a Vehicular Network," *Proc. IEEE GLOBECOM*, Vol.1, No.1, pp.1-6, 2008.

[8] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, pp. 1557-1568, 2007.

[9] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Certificate Revocation in Vehicular Networks," *Technical Report LCA-Report-2006-006*, 2006.

[10] E. Uhlemann and N. Nygren, "Cooperative Systems for Traffic Safety: Will Existing Wireless Access Technologies Meet the Communication Requirements?," *ITS World Congress*, pp. 1-8, 2009.

[11] Ivan Lequerica, J. A. Martinez, and P. M. Ruiz, "Efficient Certificate Revocation in Vehicular Networks using NGN Capabilities," *Vehicular Technology Conference 2010*, pp. 1-5, 2010.

[12] Christoph Sommer, Armin Schmidt, Reinhard German, Wolfgang Koch, and Falko Dressler, "Simulative Evaluation of a UMTS-based Car-to-Infrastructure Traffic Information System," *Proc. of IEEE GLOBECOM*, pp. 1-8, 2008.

[13] Gwang Soon Lee, Kwang Yong Kim, and Soo In Lee, "Development of Terristrial DMB Interactive Data Broadcasting System based on Middleware," *Journal of Korea Multimedia Society*, Vol.11, No.4 pp. 481-491, 2008.

[14] ETSI std, "Digital Audio Broadcasting (DAB); Multimedia Object Transfer (MOT) Protocol," *ETSI EN 301 234*, 2005.

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.

Min Soo Kim

He received a B.S., a M.S., and Ph. D degrees at department of computer science and statistics of Chonnam National Univ. in 1993, 1995, and 2000 respectively. He worked at KISA as a senior engineer from 2000 to 2001 as a senior engineer. He worked at System Security Research Center of Chonnam National Univ. as a reseach professor from 2001 to 2005. He is currently an associate professor at department of Information Security of Mokpo National University. His research interests include intrusion detection and response, computer forensics, secure OS, and data mining.

Seok Won Jung

He received a B.S., a M.S., and Ph.D. degrees at department of mathematics of Korea Univ. in 1991, 1993, and 1997 respectively. He worked at Center for Information Security Technology of Korea University from 2002 to 2004 as a research professor. He is currently an associate professor at department of Information Security of Mokpo National University. His research interests include designing cryptographic algorithms and protocols, smart card security, and broadcast security.

Jae Hyun Seo

He received a B.S., a M.S., and degrees at department of computer science and statistics of Chonnam National Univ. and at department of computer science and engineering of Chung-Ang Univ. in 1985 and 1988 respectively. He received a Ph. D degree at department of computer science and statistics of Chonnam National Univ. in 1996. He worked at Songwon Univ. as a professor from 1988 to 1996. He is currently a professor at department of Information Security of Mokpo National University. His research interests include information security, system and network security, and computer networks.