# CRL DISTRIBUTION USING AN ALTERNATIVE COMMUNICATION MEDIA FOR VEHICULAR NETWORKS

HyunGon Kim
*Department of Information Security, Mokpo National University*
*560 Muanno Cheonggye-Mueon, Muan-Gun, 534-729, Jeonnam, Korea*

Keywords: VANET security, CRL, Overlay zone, T-DMB, TPEG application.

Abstract: Efforts on vehicular network security have been undertaken, with consensus on utilizing public key cryptography to secure communications. However, how to efficiently revoke node's certificates represents a major challenge in vehicular networks. Certificate revocation lists (CRLs) should be distributed quickly to every vehicle within the networks to protect them from malicious users and malfunctioning equipment as well as to increase the overall security and safety of the vehicular networks. In this paper, we propose a Terrestrial-Digital Multimedia Broadcasting (T-DMB) aided distribution method for CRL distribution. The method can broaden breadth of network coverage and can get real-time delivery and enhanced transmission reliability using an alternative communication media thus, T-DMB data broadcasting channels. Even if road side units are sparsely deployed or, even not deployed, vehicles can obtain recent CRLs from T-DMB infrastructure. In addition, to broadcast CRLs over T-DMB infrastructure, we design a new Transport Protocol Expert Group (TPEG) CRL application followed by TPEG standards.

## 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 (IEEE Std 1609.2, 2006) and the European PRE-DRIVE C2X standard (Bechler et al., 2009) 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 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 (Resendes, 2008). 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

Kim H..
CRL DISTRIBUTION USING AN ALTERNATIVE COMMUNICATION MEDIA FOR VEHICULAR NETWORKS.
DOI: 10.5220/0003497702170222
In *Proceedings of the 13th International Conference on Enterprise Information Systems* (ICEIS-2011), pages 217-222
ISBN: 978-989-8425-53-9

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 (Bechler et al., 2009). 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 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 stat of the art, RSU-based distribution methods as well as vehicle-to-vehicle distribution methods 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, the epidemic distribution method can be used to broadcast them. In this paper, we propose a T-DMB aided distribution method for CRL distribution. The method can broaden breadth of network coverage and can get real-time delivery and enhanced transmission reliability using an alternative communication media thus, T-DMB data broadcasting channels. In addition, to broadcast CRLs using T-DMB data broadcasting service, we design a new TPEG CRL application followed by TPEG standards.

The reminder of the paper is organized as follows. In section II, we present the related work. In section III, we introduce the proposed CRL distribution method. In section IV, to utilize T-DMB data broadcasting service, a new TPEG CRL application is designed and we finalize with some conclusions.

# 2 RELATED WORK

## 2.1 CRL Distribution Methods

The problem of revocation in vehicular networks has hardly attracted any attention in the literature. Papadimitratos et al. (Papadimitratos et al., 2008) 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. (Laberteaux, 2008) 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. (Lin et al., 2008) proposed the use of RSU-aided certificate revocation. Each RSU has the complete and updated base-CRL and it is continuously checking the status of the certificates contained in 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.

To reduce size and computational costs of processing the CRLs, extensive research efforts have been made in vehicular networks. Bellur (Bellur, 2008) proposed segmentation of an administrative area into a number of geographic regions and the assignment of region-specific certificates to an OBU resident on a vehicle, which could significantly reduce the size of CRLs.

Raya et al. (Raya et al 2007) propose the combination of two protocols specially tailored to the vehicular networks, the revocation of the trusted component (RTC) and revocation using compressed certificate revocation lists ($RC^2RL$). The RTC is intended to reduce the number of certificates that need to be inserted in the CRL. It requires the CA, however, to be able to geographically localize any vehicle in the system. The $RC^2RL$ is a CRL that is compressed using Bloom filter compression to limit the size of the CRL. Because of the false positive characteristic of Bloom filter compression, some legitimate certificates can get revoke as well.

## 2.2 CRL Distribution using an Alternative Communication Media

To distribute CRLs, while most of running projects are mainly based on the IEEE 802.11p and ITS-G5A, other mobile access technologies like UMTS, WiMax and DMB can be utilized (Bechler et al., 2009). Lequerica et al, (Lequerica et al., 2010) propose a use of the existing multimedia broadcast multicast service over UMTS, which improves the efficiency of the distribution of the CRL. Sommer et al, (Sommer, 2008) present simulation results of a UMTS-based vehicle-to-infrastructure traffic information system. However, even if the usage of the cellular channel is low in above two methods, there is need to use UMTS bearer service.

## 2.3 ITS Network Reference Model

The network reference model of European ITS communication architecture is depicted in Figure 1 (Bechler et al., 2009). The ITS Vehicle Station compromise a number of ITS-specific functions. The ITS Roadside Station such as RSU can act as gateway between the ITS ad-hoc network domain and the ITS roadside infrastructure network domain. The Border Router offers IP connectivity to ITS Vehicle Station and Core Network Switch in the Internet domain.

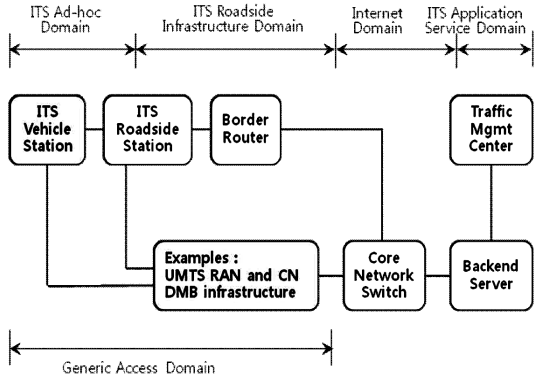


Figure 1: European ITS network reference model.

The main components for the generic access network domain can be UMTS system, DMB infrastructure etc. IP packet transport is assured either by means of encapsulation and tunnelling over the ad-hoc network for vehicle-to-vehicle and vehicle-to-infrastructure communication, or by using the generic IP access network. The ITS Application Service Domain contains Backend Server and Traffic Management Center.

# 3 NEW CRL DISTRIBUTION METHOD

In this section, we describe the proposed T-DMB aided distribution method. Every vehicle will want the most recent CRL to protect them from malicious users and malfunctioning equipment, as well as to increase the overall security and safety of the vehicular networks. We utilize the advantage of T-DMB data broadcasting service in terms of low cost, real-time delivery, wide network coverage, and enhanced transmission reliability.

## 3.1 T-DMB aided Distribution Method

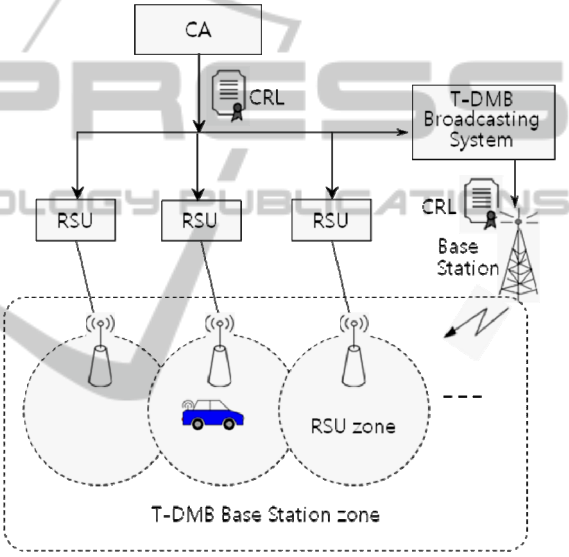


Figure 2: T-DMB aided distribution method.

Some design principles and assumptions are:

- In addition to the usual ETSI ITS-G5A module interface, basically vehicles have a T-DMB terminal and a module interface.
- T-DMB terminal has also an interface with on board unit (OBU) within a vehicle.
- RSUs can be deployed with sufficient density or, sparsely placed in certain areas or, even not placed. Therefore, in some areas, vehicles often cannot receive recent CRLs from RSU and even neighbouring vehicles.
- CA sends recent CRLs to the T-DMB base station periodically to broadcast CRLs over T-DMB data broadcasting channels.

The schematic diagram of the proposed method is depicted in Fig. 2. In addition to the RSU-based distribution, CA utilizes T-DMB data broadcasting channels to distribute duplicated CRLs additionally.

The CA sends recent CRLs to the RSU and T-DMB base station periodically over fixed wireline as the same fashion. Then, the same CRLs would be doubly distributed to the vehicles through a RSU and a T-DMB base station at any given time. In an area where RSU density is high enough, a vehicle can connect to the RSU directly. In contrast, in an area where RSU density is low, a vehicle can switch over to the T-DMB base station directly. To do this, vehicles has to change from IT-G5A module interface to T-DMB module interface or, in the opposite direction.

## 3.2 Overlay Zone

The proposed method is based on the concept of overlay zone, which is duplicated zone by RSU transmission coverage and T-DMB base station transmission coverage. Therefore, in that zone, vehicles can be able to obtain CRLs from a RSU as well as T-DMB base station directly. According to the standard (Bechler et al., 2009), maximum cell coverage of ITS-G5A based RSU, Dedicated Short Range Communication (DSRC) based RSU, T-DMB base station are approximately 500m, 1Km, and 35Km respectively. Therefore, as shown in Fig. 3, one base station's zone ($T\text{-}DMB_{zone}$) would be composed of several RSU's zones ($RSUs_{zone}$), which can be expressed as following:

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

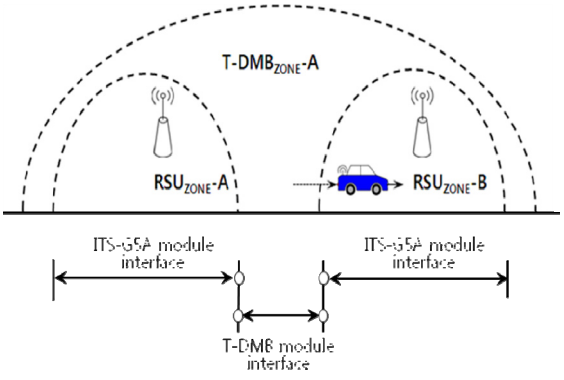


Figure 3: Overlay zone.

In our example of Fig. 3, when a vehicle enters the $RSU_{zone}$-A, it can receive CRLs from its ITS-G5A module interface (e.g., from the RSU-A). If the vehicle are beyond RSU-A's transmission range as well as RSU-B transmission range, then, it can also receive CRLs from its T-DMB module interface (e.g., T-DMB base station). Thus, as soon as the vehicle knows outside the range of its RSU transmission range, then the vehicle may change from the ITS-G5A module interface (or, WAVE module interface) to the T-DMB module interface.

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. We assume that logically designed RSU-based zones are mapped into $T\text{-}DMB_{zone}$. CA also has to collaborate with T-DMB broadcasting system to present $T\text{-}DMB_{zone}$ information and to distribute CRLs through T-DMB infrastructure.

## 3.3 CRL Encoding Rule

Original CRLs should be encoded to get transmission efficiency and credential (Ardelean, 2009). A schematic description of encoding the CRL is depicted in Fig. 4. First, the CA generates the CRL and divides into M equal length pieces. These pieces are encoded using an erasure code, into N redundant pieces. Each piece has a header added then, it is signed by the CA. The header contains the CRL version, time stamp for avoiding replay attack, the sequence number of the encoded piece, and the CA's ID. After this step the new pieces are sent to the RSUs and then, they are broadcasted to the vehicles.

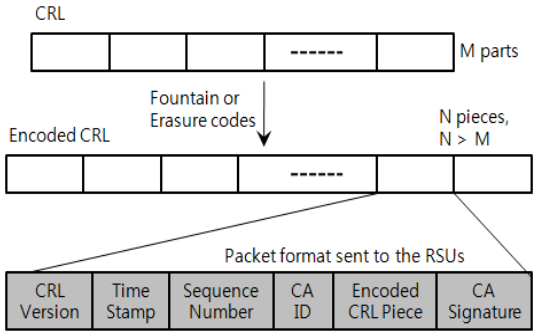


Figure 4: CRL encoding rule.

When receiving one of these signed packets, a vehicle first verifies the time stamp of the message, then the signature. The signature verification is done by searching in its database the public key associated to the CA ID extracted from the message. If the signature is valid then the vehicle verifies if it has already this piece stored, if not it store the piece with the associated sequence number. When it has enough pieces it will decode them and obtain the original CRL.

# 4 DESIGN OF TPEG CRL APPLICATION

To realize the proposed method using T-DMB data broadcasting service, standard TPEG protocol could be utilized. TPEG is a bearer and language independent protocol that can be used for many data broadcasting channels like DAB, DMB, DVB and others (ISO/TS 18234-1, 2006). TPEG applications are kinds of data services and its message structure is followed by TPEG standards. Since the proposed CRL application also uses TPEG technology, it could be formalized as a new TPEG application that is called the CRL application in this paper. The CRL application can distribute CRLs using T-DMB data broadcasting service as a real-time manner. It could allow T-DMB base station to distribute CRLs and allows vehicles to receive CRLs effectively.

## 4.1 Frame Structure of CRL Application

The hierarchical transport frame structure including CRL application message is shown Fig. 5. Transport Frame, Service Frame, Service Component Frame are commonly used like as other TPEG applications. Details of them are described in TPEG standards (ISO/TS 18234-1, 2006).

The Service Component Frame comprises the service component identifier, the length of the component data, the component header CRC, and component data. The service component identifier with the value 0 is reserved. The field length consists of 2 bytes and represents the number of bytes of the component data. The component header CRC is calculated from the service component identifier, the field length, and the first 13 bytes of the component data.

The CRL application message is what we defined. The CRL application is designed to deliver CRL application message; thus, CRLs issued by CAs, using three containers, which are the message management container, the event container for transmitting CRLs, and TPEG location container having the geographical location information.

To manage CRLs in the receiving side, the message management container includes information such as the date and time references, generation time, expiry time, the effect and reliability, the cross reference information etc. The effect and reliability information provide severity factor and unverified information to make a judgements about the effect on travel for a vehicle. The cross reference information would allow each message to be cross-referenced to other messages, either within the CRL application or, in other TPEG applications.

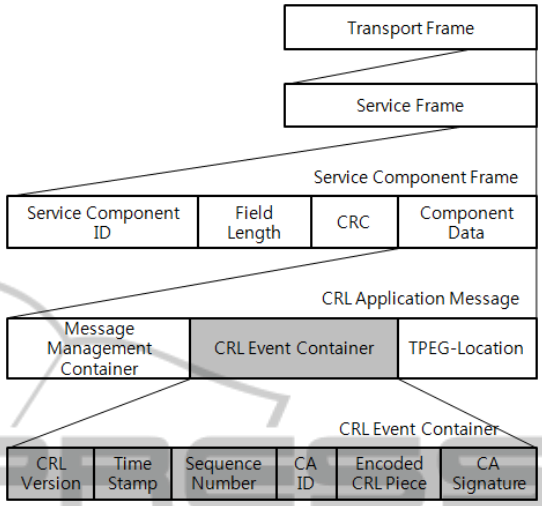


Figure 5: Transport frame structure for CRL application.

## 4.2 Architecture for CRL Application

To implement the proposed method, architecture and additional functionalities should be identified from a point of T-DMB system views. As shown in Fig. 6, T-DMB data server has capable of processing a new CRL application. It collects large size CRL packets through CA interface and then, converts into TPEG packet formats. And it also encodes TPEG packet to CRL application message formats.

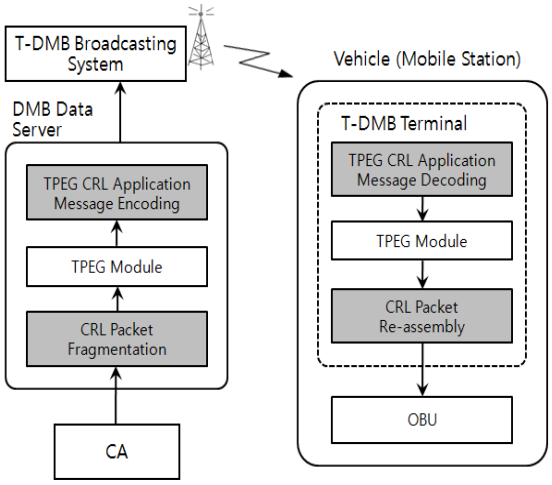


Figure 6: Implementation architecture for CRL application.

Basically a vehicle has a T-DMB terminal that may be interfaced with OBU within vehicle. Upon receiving CRL application messages, T-DMB terminal has to process decoding and re-assemble.

Finally extracted CRLs are delivered to the OBU within vehicle.

## 5 CONCLUSIONS

We present the basic ideas of a CRL distribution method for vehicular networks, with the focus on use of an alternative communication media. The basic objectives of the proposed method are concerned with the fundamental problem of how to distribute CRLs in a real-time manner across wide regions including rural regions. Our design approach seeks to use a T-DMB aided distribution method that can broaden breadth of network coverage and can get real-time delivery and enhanced transmission reliability using T-DMB data broadcasting channels. Even if road side units are sparsely deployed or, even not deployed, vehicles can obtain recent CRLs from T-DMB infrastructure. In addition, to broadcast CRLs over T-DMB data broadcasting channels, we design a new TPEG CRL application followed by TPEG standards.

## ACKNOWLEDGEMENTS

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-2010-0024531).

## REFERENCES

IEEE Std 1609.2. (2006). Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Message. *IEEE Std 1609.2*, 2006.

M. Bechler et al. (2009). PRE-DRIVE Implementation and Evaluation of C2X Communication Technology, Deliverable D1.4, *PRE-DRIVE Std.*, March 2009.

R. Resendes. (2008). The New 'Grand Challenge' - Deploying Vehicle Communications, Keynote Address, *The Fifth ACM International Workshop on VehiculAr InterNETworing(VANET 2008)*, Sept. 2008.

P. Papadimitratos et al. (2008). Certificate Revocation List Distribution in Vehicular Communication Systems, *The Fifth ACM International Workshop on VehiculAr InterNETworing(VANET)*, Sept. 2008.

Kenneth P. Laberteaux et al. (2008). Security Certificate Revocation List Distribution for VANET, *The Fifth ACM International Workshop on VehiculAr InterNETworing(VANET)*, pp.88-89, Sept. 2008.

Xiaodong Lin et al. (2008). Security in Vehicular Ad Hoc Networks, *IEEE Communications Magazine*, Vol. 46, No. 4, pp.88-95, April 2008.

Bhargav Bellur. (2008). Certificate Assignment Strategies for a PKI-based Security Architecture in a Vehicular Network, *Proc. IEEE GLOBECOM*, pp.1-6, Nov. 2008.

M. Raya et al. (2007). Eviction of Misbehaving and Faulty Nodes in Vehicular Networks, *IEEE Journal on Selected Areas in Communications*, pp.1557-1568, Oct. 2007.

M. Raya et al. (2006). Certificate Revocation in Vehicular Networks, *Technical Report LCA-Report-2006-006*, 2006.

E. Uhlemann et al. (2009). Cooperative Systems for Traffic Safety: Will Existing Wireless Access Technologies Meet the Communication Requirements?, *ITS World Congress*, Sept. 2009.

Ivan Lequerica et al. (2010). Efficient Certificate Revocation in Vehicular Networks using NGN Capabilities. *Vehicular Technology Conference 2010*, pp.1-5, Sept. 2010.

Christoph Sommer et al. (2008). Simulative Evaluation of a UMTS-based Car-to-Infrastructure Traffic Information System. *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2008.

Petra Ardelean. (2009). Implementation and Evaluation of Certificate Revocation List Distribution for Vehicular Ad-hoc Networks, 2009.

ISO/TS 18234-1 (2006). Traffic and Travel Information (TTI) – TTI via Transport Protocol Expert Group (TPEG) data-streams – Part 1: Introduction, numbering and versions. 2006.