情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

차량통신에서 T-DMB 데이터 서비스에 기반한 인증서 취소 목록 배포 기법*

김 현 곤†
목포대학교 정보보호학과

CRL Distribution Method based on the T-DMB Data Service for Vehicular Networks*

HyunGon Kim†
Mokpo National University, Dept. of Information Security

요 약

차량통신에서는 안전한 통신을 제공하기 위해 공개키 방식을 적용하고 있다. 이를 위해 인증서 취소목록(CRL)은 공격자나 고장난 차량으로부터 보호하고, 차량 네트워크의 전반적인 보안과 안전을 증대시키키 위해 모든 차량에게 빠르게 전파되어야 한다. 즉, 인증서 취소목록을 어떻게 효율적으로 배포할 것인지가 매우 중요해진다. 이를 고려하여 본 논문에서는 T-DMB의 데이터 서비스를 이용한 CRL 분배 기법을 제안한다. 이 기법은 T-DMB 데이터 방송 채널을 이용하여 통신의 신뢰성 확대, 네트워크 커버리지 확대, CRL 실시간 전달을 가능하게 한다. 그리고 기지국(RSU)들이 성글게 설치되거나 설치되지 않은 지역에서도 차량들은 T-DMB 인프라를 통해 최신의 CRL들을 획득할 수 있다. 이 기법을 완성하기 위해 새로운 TPEG 응용 서비스를 설계하였다.

ABSTRACT

There is a consensus in the field of vehicular network security that public key cryptography should be used to secure communications. A certificate revocation list (CRL) should be distributed quickly to all the vehicles in the network 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 CRL distribution method aided by terrestrial digital multimedia broadcasting (T-DMB). By using T-DMB data broadcasting channels as alternative communication channels, the proposed method can broaden the network coverage, achieve real-time delivery, and enhance transmission reliability. Even if roadside units are not deployed or only sparsely deployed, vehicles can obtain recent CRLs from the T-DMB infrastructure. A new transport protocol expert group (TPEG) CRL application was also designed for the purpose of broadcasting CRLs over the T-DMB infrastructure.

Keywords: certificate, CRL, security for vehicular communications, T-DMB

접수일(2011년 5월 30일, 게재확정일(2011년 7월 13일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된것임 (NRF-2010-0024531)
† 주저자, hyungon@mokpo.ac.kr

I. Introduction

Vehicular ad hoc networks are an emerging research area. They are a promising means of facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. However, without the integration of strong, practical security and privacy-enhancing mechanisms, a vehicular communication system can be disrupted or disabled, even by relatively unsophisticated attackers.

The life-critical nature of vehicular networks highlights the need for careful assessment of the security design features of vehicular communication systems. The IEEE 1609.2 standard[1] and the European PRE-DRIVE C2X standard[2] both define security services for vehicular ad hoc networks. Their recommended secure message formats and techniques for processing secure messages are based on the public key infrastructure (PKI).

In traditional PKI architecture, the most commonly adopted certification revocation scheme uses a certificate revocation list (CRL), which is a list of revoked certificates stored in repositories prepared by certificate authorities (CAs). In a vehicular network, the CA supplements the CRL with identification details of any revoked certificate(s). The CA broadcasts 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 a network's operation. If the information is message faulty, compromised, or otherwise illegitimate, the situation becomes potentially dangerous and vehicles can be ignored.

The CA uses a set of road side units (RSUs) to broadcast CRLs to all passing vehicles. However, the RSU-based revocation may be challenging in certain areas (such as rural regions) where not enough RSUs are deployed or maintained. RSUs are likely to be sparsely placed in real environments, so vehicles may rarely encounter an RSU and spend a significant amount of time outside the radio range of an RSU[3]. In such cases, a vehicle has to wait a long time before receiving a recent CRL and the delay could be a threat to the security of the vehicular network. Even if a sufficient number of RSUs is eventually deployed, vehicular networks must be able to operate during stages of incremental deployment; that is, before a sufficient number of RSUs come online. CRLs should therefore be distributed quickly to every vehicle within the network.

On the other hand, several broadcasting techniques are used in vehicular networks. One example is narrow bandwidth solution such as FM radio; other examples include wider bandwidth digital services such as DAB, DVB, DVB-H, and T-DMB[2]. Broadcasting is an attractive solution because of its low cost, extensive coverage, and large potential volumes of data. Real-time traffic information is already available with services based on T-DMB broadcasting and the TPEG protocol. The T-DMB service is a free commercialized service; its infrastructure is widely deployed in Korea. The T-DMB data broadcasting service provides mobile users with various types of data such as web sites, graphic files, and traffic reports through its data channels.

To the best of our knowledge, all the solutions in the state of the art, including RSU-based distribution methods and vehicle-to-vehicle distribution methods, have problems with delays, availability, liability, limited transmission, and real-time delivery. Designing an effective system of distribution revocation information is the main problem at hand.

Our proposal focus on the fundamental problem of how to distribute CRLs in real time across wide regions including rural areas. The basic idea involves a subnet of vehicular network nodes. If a subnet can effectively receive CRLs via an alternative communication channel, an epidemic distribution method can be used to broadcast the CRLs. In this paper, we propose a T-DMB-aided method of distributing CRLs. By using an alternative communication media such as T-DMB data broadcasting channels, the proposed method can broaden the network coverage, achieve real-time delivery, and enhance transmission reliability. In addition, to broadcast CRLs via the T-DMB data broadcasting service, we designed a new TPEG CRL application conforms to TPEG standards.

The reminder of the paper is organized as follows: In section II, we discuss related works. In section III, we introduce the proposed CRL distribution method. In section IV, we describe a new TPEG CRL application designed for the T-DMB data broadcasting service. In section V, we present the comparative results of several CRL distribution methods and we draw some final conclusions.

II. Related Works

2.1 CRL Distribution

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. The CRLs are encoded into numerous self-verifiable pieces, so the information the vehicles get from the RSUs is limited to those encoded CRL pieces.

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 et al.[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

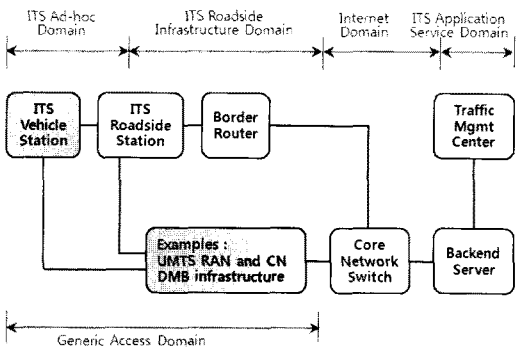
Most ongoing projects are based on the

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 et al.[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 methods, the UMTS bearer service is still needed.

2.3 ITS Networks 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.



[Figure 1] European ITS Network Reference Model

III. The Proposed CRL Distribution Method

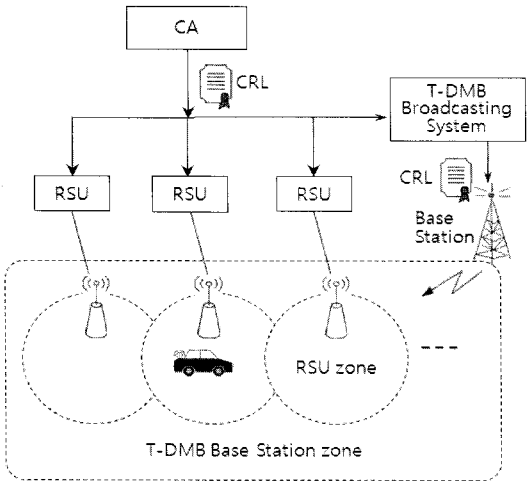
In this section, we describe the proposed T-DMB-aided distribution method. Every vehicle requires the most recent CRL for protection against malicious users and malfunctioning equipments. Up-to-date CRLs increase the overall security and safety of the vehicular networks. We use a T-DMB data broadcasting service 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.

3.1 T-DMB-aided CRL Distribution

T-DMB-aided CRL distribution 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, nonexistent. 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.

[Figure 2] shows a schematic of the proposed method. In addition to the RSU-based



[Figure 2] T-DMB-aided CRL Distribution

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.

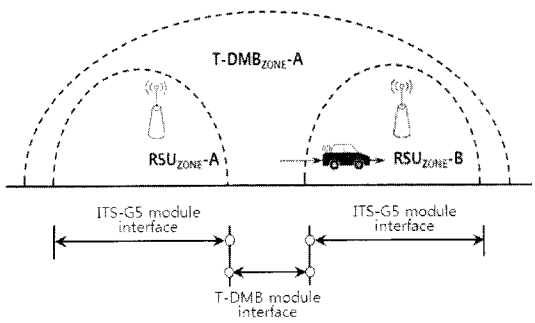
3.2 Handoff

The proposed method 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' ($T\text{-}DMB_{zone}$) consists of several RSU' zones ($RSUs_{zone}$). A single base station can therefore be expressed as follows:

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

The example in [Figure 3] shows how a vehicle that enters $RSU_{zone\text{-}A}$ 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



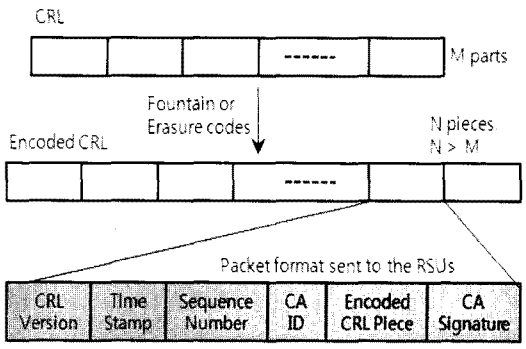
[Figure 3] Handoff between Vehicular Network and T-DMB Network

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 must 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.

3.3 The CRL Encoding Rule

The original CRLs should be encoded to ensure the CRL transmissions are efficient and reliable[13]. [Figure 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'. The new pieces are then sent to the RSUs and broadcast to vehicles.

Upon receiving one of the signed packets, 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 associated sequence number. When the vehicle receives enough pieces, it decodes the pieces and subsequently obtains the original CRL.



[Figure 4] CRL Encoding Rule

IV. Design of a New TPEG CRL Application

A standard TPEG protocol was used so that the proposed method could be used in conjunction with a T-DMB data broadcasting service. The TPEG is a bearer and language independent protocol that can be used for many data broadcasting channels such as DAB, DMB, DVB and others[14]. TPEG applications are data services that use the TPEG standards in their message structure. Our proposed CRL application also uses TPEG technology, it could be formalized as a new TPEG application that is could be called a new kind of TPEG application because it uses TPEG technology. The CRL application distributes CRLs in real-time via a T-DMB data broadcasting service. In this way a T-DMB base station can effectively distribute CRLs to vehicles.

4.1 Frame Structure of CRL Application

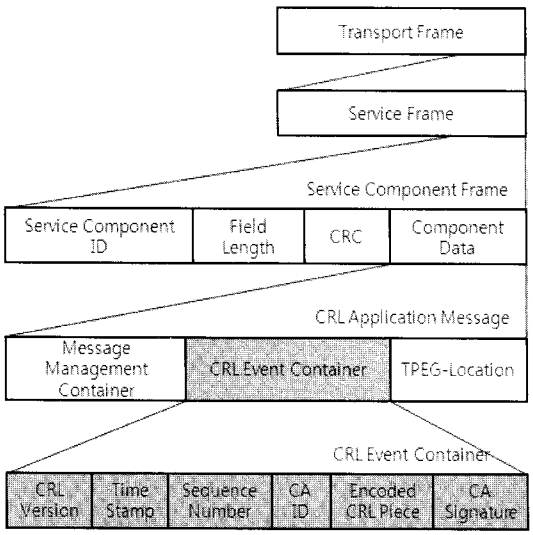
[Figure 5] shows the hierarchical transport frame structure, which includes a CRL application message. A transport frame, a service frame, and a service component frame are commonly used in TPEG applications. Details of theses frames are described in the TPEG standards[14].

The service component frame includes a service component identifier, the length of the component data, the component header's CRC, and the component data. The service component identifier has a reserved value of 0. The field length, which indicates the size of component data, is 2 bytes. The

calculation of the component header's CRC is based on the service component identifier, the field length, and the first 13 bytes of the component data.

We defined the CRL application message. The CRL application was designed to deliver a CRL application message. Thus, the CA issues CRLs in three containers: a message management container, an event container for transmitting CRLs, and a TPEG location container which includes information on the geographical location.

The way CRLs are received is facilitated by the message management container. This container includes a variety of information such as the following: date and time references, the generation time, the expiry time, the effect and reliability, and cross-reference information. The effect and reliability information provides a severity factor and unverified information so that judgments can be made about the effect on the travels of a vehicle. The cross-reference information enables each message to be cross-referenced with other messages of either, the CRL application or, other TPEG applications.



(Figure 5) Transport Frame Structure for CRL Application

4.2 Implementation Architecture for the CRL Application

For the implementation of the proposed method, the architecture and additional functionalities should be identified from the perspective of a T-DMB system. As shown in (Figure 6), the T-DMB data server is capable of processing a new CRL application. It collects large CRL packets through the CA interface and then converts them into a TPEG packet format. It also encodes the TPEG packet in the format of a CRL application message. Basically, a vehicle with a T-DMB terminal can interface with an OBU in the vehicle. Upon receiving a CRL application message, the T-DMB terminal processes the decoding and reassembly. Finally, the extracted CRLs are delivered to the vehicle's OBU.

V. Relative Comparison and Discuss

In this section, we summarize and compare the characteristics of the different revocation methods introduce in this paper. (Table 1) highlights the efficiency of T-DMB-aided 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 T-DMB-aided distribution method. However, the proposed T-DMB-aided distribution method has the disadvantage of requiring an additional T-DMB infrastructure and T-DMB module in the vehicle.

(Table 1) Relative Comparisons of CRL Distribution Methods

RSU-based distribution	UMTS-aided distribution	T-DMB-aided distribution
Throughput		
A few hundred 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	Yes	Yes

VI. Conclusions

We present basic ideas on a CRL distribution method for vehicular networks, with a focus on the use of an alternative communication media. The basic objectives of the proposed method 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 distribution method in which T-DMB data broadcasting channels are used to 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. In addition, to broadcast CRLs over T-DMB data broadcasting channels, we designed a new TPEG CRL application complies with TPEG standards.

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, July 2006.

[2] M. Bechler et al., "PRE-DRIVE Implementation and Evaluation of C2X Communication Technology, Deliverable D3.," PRE-DRIVE Std., Version 3.0, pp. 1-187, Mar. 2009.

[3] R. Resendes, "The New 'Grand Challenge' - Deploying Vehicle Communications, Keynote Address," *The Fifth ACM International Workshop on VehiculAr InterNETworing (VANET 2008)*, pp. 1-2, Sept. 2008.

[4] P. Papadimitratos et al., "Certificate Revocation List Distribution in Vehicular Communication Systems," *The Fifth ACM International Workshop on VehiculAr InterNETworing(VANET)*, pp. 1-2, Sept. 2008.

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

[6] Xiaodong Lin et al., "Security in Vehicular Ad Hoc Networks," *IEEE Communications Magazine*, Vol. 46, No. 4, pp.88-95, Apr. 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, Nov. 2008.

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

[9] M. Raya et al., "Certificate Revocation in Vehicular Networks", *Technical Report LCA-Report-2006- 006*, 2006.

[10] E. Uhlemann et al., "Cooperative Systems

for Traffic Safety: Will Existing Wireless Access Technologies Meet the Communication Requirements?," *ITS World Congress*, pp. 1-8, Sept. 2009.

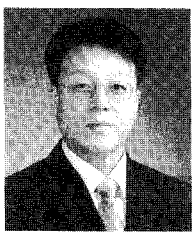
[11] Ivan Lequerica et al., "Efficient Certificate Revocation in Vehicular Networks using NGN Capabilities", *Vehicular Technology Conference 2010*, pp.1-5, Sept. 2010.

[12] Christoph Sommer et al., "Simulative Evaluation of a UMTS-based Car-to-Infrastructure Traffic Information System," *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1-8, Dec. 2008.

[13] Petra Ardelean, "Implementation and Evaluation of Certificate Revocation List Distribution for Vehicular Ad-hoc Networks," pp. 1-5, Jan. 2009.

[14] ISO/TS 18234-1, "Traffic and Travel Information (TTI) - TTI via Transport Protocol Expert Group (TPEG) data-streams - Part 1: Introduction, numbering and versions," pp. 1-258, June. 2006.

〈著者紹介〉



김 현 곤 (HyunGon Kim) 종신회원
1992년 2월: 금오공과대학교 전자공학과 졸업
1994년 2월: 금오공과대학교 전자공학과 석사
2003년 3월: 충남대학교 전자공학과 박사
1994~2005: 한국전자통신연구원 정보보호연구단 선임연구원
2005~현재: 목포대학교 정보보호학과 부교수
〈관심분야〉 차량통신 보안, 이동통신 보안