Journal of The Korea Society of Computer and Information
Vol. 21 No. 1, pp. 91-99, January 2016
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.1.091

A Regional Certificate Revocation List Distribution Method based on the Local Vehicle Location Registration for Vehicular Communications

Hwi-Seung Hong*, Hyun-Gon Kim**

Abstract

A certificate revocation list(CRL) should be distributed quickly to all the vehicles in the network to protect them from malicious users and malfunctioning equipments as well as to increase the overall security and safety of vehicular networks. However, a major challenge is how to distribute CRLs efficiently. In this paper, we propose a novel Regional CRL distribution method based on the vehicle location registration locally to manage vehicle mobility. The method makes Regional CRLs based on the vehicles' location and distributes them, which can reduce CRL size and distribution time efficiently. According to the simulation results, the proposed method's signaling performance of vehicle's registration is enhanced from 22% to 37% compared to the existing Regional CRL distribution method. It's CRL distribution time is also decreased from 37% to 67% compared to the existing Full CRL distribution method.

▸ Keyword : Certificate Revocation List, Vehicle Location Registration, Vehicular Communications

I. Introduction

차량통신 시스템은 교통 시설의 전자, 제어 및 첨단 교통기술과 교통 정보를 융합하여 교통 체계의 운영과 관리를 과학화하고 자동화하고 있다. 이는 교통의 효율성과 운전자의 안전성을 향상시키는 교통 체계를 의미하는 지능형 교통 시스템(ITS)의 형태로 진화하고 있으며 특히, 차량통신 기술은 지능형 교통 시스템을 구축하기 위한 필수 요소이다. 차량통신 기술을 기반으로 구글은 자율운전 차량을 개발하여 실제 주행 시험을 하고 있으며, 우버와 애플 역시 자율운전 차량 개발에 주력하고 있다. 자동차와 IT간 융합이 가속화되면서 “스마트 카” 의 시대가 열리고 있는 것이다.

스마트 카는 자동차와 IT의 융합기술을 이용하여 자동차의 주행 안전성과 운전자의 편의성을 획기적으로 증대시키는 자동차를 의미한다. 스마트 카를 실현할 수 있는 다양한 센서 기술과 차량간 통신 기술은 기존의 센서에만 의존한 차량에 비하여 교통사고를 크게 감소시킬 것으로 기대된다. 한편, 연결성을 강조하여 차량간 통신 및 차량과 인프라간 통신이 구축된 차량을 ‘커넥티드 카’로 정의하고 있다[1].

그러나 최근 미국에서 지프 체로키가 다운타운 주변을 운행하던 중 원거리에서 해킹을 당해 통제력을 잃고 구덩이에 빠지는 동영상이 공개되었다[2]. 지프 체로키에 장착된 ‘유커넥트’라는 첨단 시스템이 해킹을 당한 것이다. 해커는 차량의 고유 IP를 찾아내고 ‘유커넥트’에 접근하여 악성코드를 심고 강제로 명령어를 하달하여 차량을 제어한 것이다. 이와 같이 차량 통신은 기존의 유무선 통신과 달리, 보안 기술이 완벽하게 지원되지 않으면 운전자와 탑승자의 생명을 위협할 수 있는 잠재성을 가지고 있어 매우 위험하다.

차량통신의 보안 위협으로는 개인식별 정보 전송이나 통신 오류, 바이러스 감염, 인가되지 않은 설정이나 사용, 인가되지 않은 정보 접근, 스니핑, 서비스 거부 공격, 메시지 변조, 로그 삭제, 무단 릴레이, 위치 추적 등을 들 수 있다[3].

차량통신의 보안 기술을 Fig. 1에 개념적으로 나타내었다. 기존의 차량통신 네트워크와 비교해보면 추가적으로 인프라측에 인증서 관리를 위한 인증기관(CA; Certificate Authority)이 연결된다. 그리고 기지국(RSU; Road Side Unit)과 CA 사이에는 안전한 채널이 구성된다. 차량에는 하드웨어 보안 모듈이 탑재되어 암호 키와 인증서가 관리되고 암호 오퍼레이션이 수행된다. 이 모듈을 이용하여 비콘 메시지를 포함하여 차량간 통신

• First Author: Hwi-Seung Hong, Corresponding Author: Hyun-Gon Kim
*Hwi-Seung Hong (wisehhs06@gmail.com), Dept. of IT System, Chosunilbo
**Hyun-Gon Kim (hyungon@mokpo.ac.kr), Dept. of Information Security, Mokpo National University
• Received: 2015. 12. 10, Revised: 2016. 01. 14, Accepted: 2016. 01. 20.

과 차량과 인프라간 통신에 안전성을 제공한다.

대표적인 차량통신 보안 표준인 IEEE 1609.2에서는 차량 인증, 메시지 인증, 그리고 차량의 위치 익명성을 보장하기 위해 차량통신 전용의 공개키 방식의 단기 익명 인증서(short term pseudonyms)를 적용한다[4]. 또한, 고장난 차량이나 공격자로부터 보호하고, 차량 네트워크의 전반적인 보안과 안전을 증대시키기 위해 취소된 인증서에 대한 차량통신 전용의 인증서 취소목록(CRL; Certificate Revocation List)을 주기적으로 배포한다.

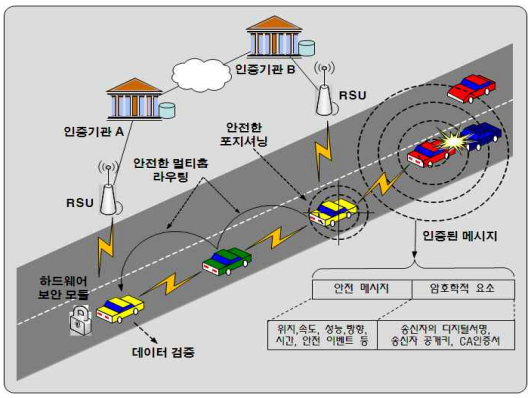

Fig. 1. Concept of Secure Vehicular Communications

한편, X.509에서 사용하는 유선환경의 CRL은 배포 주기가 하루 이상으로 빈번하지 않기 때문에 CRL 크기가 커도 네트워크에 큰 부하를 주지 않는다. 그러나 차량통신에서는 차량의 고장이나 짧은 주기 동안에만 사용할 수 있는 차량통신 전용의 단기 익명 인증서를 사용하기 때문에 이에 맞추어 CRL 배포 주기가 짧아지고 특히, CRL 크기가 커지면 고가의 무선 대역의 점유율이 높아져 정상적인 차량통신을 방해할 수 있는 요인으로 작용하게 된다. 따라서 차량통신 네트워크에서는 CRL을 어떻게 신속하고 효율적으로 배포할 것인지가 매우 중요해진다.

이와 관련하여 기존의 Regional CRL 배포 방법은 차량이 빠르게 그리고 자주 이동하는 실제 환경에 적합하지 않다. 이유는 차량이 등록해야 하는 마스터 HLR(Home Location Register)이 멀리 떨어져 있어도 반드시 마스터 HLR에게만 위치 등록을 해야 하므로 시그널링 지연시간이 매우 커지기 때문이다. 본 논문에서는 이 문제점을 개선하여 모든 차량이 지리적으로 근접한 HLR을 통해 빠른 위치등록을 가능하도록 하여 지연 시간을 최소화하는 새로운 Regional CRL 배포 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 서론에 이어 제 2장에서는 차량통신용 CRL을 소개하고 CRL 배포에 관련된 기존의 연구 결과들을 분석하였다. 제 3장에서는 기존의 Regional CRL 배포 방법의 비효율성을 분석한 다음, 이를 바탕으로 본 논문에서 제안하는 효율적인 Regional CRL 배포 방법을 설계하였다. 제 4장에서는 기존의 방법들과 제안한 방법의 이론적인 성능을 비교·분석하였다. 제 5장에서는 시뮬레이션을 통해 성능을 비교·평가하고 이어 제 6장에서 결론을 맺는다.

II. Related Works

2.1 CRL for Vehicular Communications

차량통신에서 차량은 정기적으로 비콘 메시지, 안전 메시지, 기타 어플리케이션 메시지를 브로드캐스트 한다. 전파 도달 범위 내의 모든 차량들은 무선의 브로드캐스트 특성 때문에 주변의 전파(메시지)를 수신한다. 따라서 비콘 및 안전 메시지는 차량통신을 하는 구성원을 인증해야 하고 구성원을 증명하기 위해 메시지 암호화와 전자 서명이 필요하다. 인증서는 서명된 메시지로 송신자를 식별하고, 같은 차량에 의해 전송된 메시지를 링크한다. 또한 인증서는 상대 노드를 인증하는 수단으로 사용하고, 동일한 인증서를 계속 사용하는 경우에는 인증서의 유효성 여부와 인증서 취소에 대한 목록을 구성하기 위해 CRL을 사용한다.

노드의 인증서가 취소되었다는 사실을 인지하면 현재 사용되고 있는 인증서는 해당 OBU(On-Board Unit)에 저장된 모든 내용과 함께 취소되어야 한다. 예를 들어, 인증서가 취소된 노드로부터 경고 메시지를 받으면 이를 비정상적으로 간주하여 폐기하여야 한다. 이 때 OBU에 저장된 모든 내용을 해지하면 그 노드로부터의 공격을 피할 수 있다. 더 이상 유효하지 않은 인증서의 정보는 CRL을 통해 모든 차량들에게 전달된다.

IEEE 1609.2 표준에서는 차량 전용의 CRL을 WAVE(Wireless Access in Vehicular Environments) CRL이라고 정의하였다[4]. WAVE CRL은 유선에서 주로 사용하는 X.509의 CRL에 비해 무선 환경을 고려하여 데이터 크기를 최대 230바이트로 줄이고, 취소된 인증서당 14 바이트씩을 추가하여 목록을 만든다. 하나의 CRL에는 최대 2^{64}-1개의 취소된 인증서를 포함시킬 수 있다. CRL 원본을 수정하여 불법으로 사용하는 것을 막기 위해 전자서명과 검증 절차가 이루어진다.

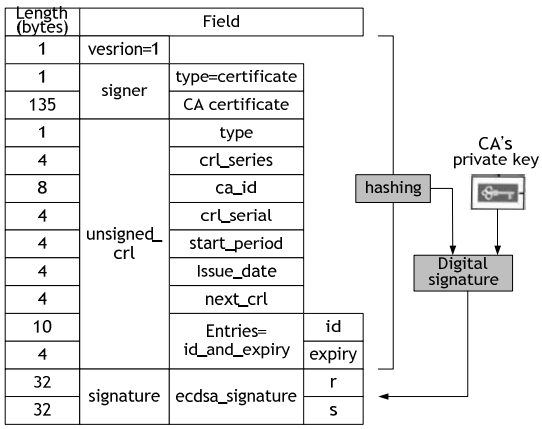

Fig. 2. WAVE CRL Architecture

2.2 Researches for CRL Distribution

차량통신에서 CA가 CRL을 생성하고 차량까지 배포하는 절

차를 Fig. 3에 나타내었다. 여기서는 CRL 사이즈가 매우 커서 여러 세그먼트로 분할하여 배포하는 것을 가정한다. (1)CA가 인증서 취소에 필요한 OBU의 인증서 목록을 생성한다. (2)CA는 차량 사양에 따라 CRL을 암호화하고 서명한 다음, 인코딩 과정에서 여러 조각의 CRL로 분할한다. 그리고 분할된 CRL 조각에 다시 서명한다. (3)RSU는 CA로부터 CRL 조각들을 모두 수신한 다음, 각 조각에 대해 서명을 검증한다. (4)모든 조각들이 검증되면 RSU는 자신이 관할하는 모든 차량들에게 브로드캐스팅 한다. 이 때 차량들간에도 V2V 통신을 이용해 CRL을 주변 차량에게 전달한다. 마지막으로 차량내의 OBU는 CA가 서명한 CRL 조각들을 검증하여 내부적으로 메모리에 저장하고 이를 기반으로 안전한 통신을 이룬다.

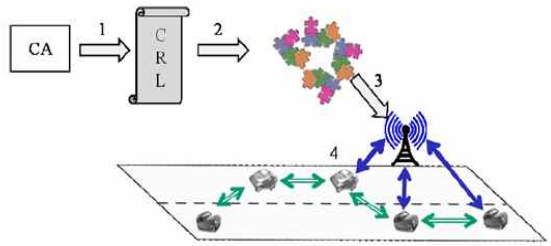

Fig. 3. CRL Distribution in Vehicular Communications

CRL은 CA나 인증개체에 의해 서명된다. 만약 통신 채널 및 저장 매체를 통해 전송 중, 임의 노드에서 CRL을 수정하면 수신자측에서 서명 검증에 실패하기 때문에 안전하다고 할 수 있다. CRL은 특정 해지 정책에 의해 지정된 시간 간격으로 배포된다. 각 사용자는 CRL을 유지하고 메시지 검증 프로세스의 일부로서 목록을 확인한다. 만약, 해지의 비율이 매우 낮은 상황이라면 전체 CRL은 자주 변경되지 않고 크기가 작게 될 것이다. 반대로 해지의 비율이 높은 상황에서는 전체 CRL의 크기가 커지고 변경이 자주 일어날 것이다. CRL 정보의 크기를 감소시키는 방법 대신 전체 CRL을 주기적으로 업데이트하여 전송하는 방법도 있다.

차량통신용 CRL 배포에 관한 연구 결과들을 조사하였다. 스위스의 연방 공과대학교(EPFL)에서는 차량통신에 대한 연구를 활발히 하고 있다. 연구 결과 중, CRL 배포와 관련된 대표적인 논문[6]에서는 스케일이 크고 멀티 도메인을 갖는 환경에서 CRL을 배포하는 방법을 제안하였다. 첫째, CRL에 지역내의 인증서 취소 정보만을 포함시키기 위해 CA들간에 상호 협력을 이룬다. 둘째, 악의적인 메시지 인젝션, 무선 신호 끊김, 통신 중단 등을 대비하기 위해서 암호학적으로 자체 검증이 가능한 다수의 CRL 조각들로 나누고 엔코딩한다. 셋째, 멀티 도메인 CA 구조를 통해 CRL 사이즈를 줄이고 다른 지역에서 방문하는 차량들의 인증서를 검증하기 위해 해당 지역에서 인증서 취소 정보를 가져온다. 이 경우 통신비용이 올라가기 때문에 짧은 라이프 타임을 갖는 인증서를 사용한다.

전파방식(epidemic)의 CRL 업데이트 방법도 제안되었다[7]. CRL 업데이트는 차량간 통신환경을 이용하였으며, 구체적인 시뮬레이션 방법과 수준을 정하기 어려워 간단한 감염모델을 사용하였다. 시뮬레이션에서 차량들이 2초마다 그리고 다른 차량의 100m 이내마다 CRL 업데이트를 받는 것으로 가정하고 실험하였다. 시뮬레이션에서는 약 26만대의 차량과 스위스 취리히 주변 지역의 354km x 263km 의 면적을 대상으로 하였다. 시뮬레이션 결과, 단일 RSU와 차량간 통신 환경에서 9,000초의 시뮬레이션 동안 99% 이상의 CRL을 업데이트 하였다. 차량간 통신만 고려한 경우에는 0.1초 주기와 RSU 325개를 사용하여 92%의 CRL을 업데이트 하였다.

인증서 수명 및 인증서 해지 방법에 대한 연구도 이루어졌다[8]. 차량통신의 참여 개체가 가능한 한 빨리 CRL을 배포하여 적시에 인증서 취소 정보를 수신하게 되면 차량통신의 보안성이 그 만큼 높아진다. CRL 배포 시간을 줄이기 위해 대부분의 해결책은 작은 크기의 파일이 더 빨리 배포되므로 CRL의 크기를 줄이는 것이고 더불어 해지가 필요한 경우를 제한하는 것이다.

한편, 이동통신의 위치등록 방법을 적용하여 Full CRL을 Regional CRL로 만들어 사이즈를 줄인 방법이 제안되었다[9]. 차량의 위치를 데이터베이스에 실시간으로 등록하고, 차량의 현재 위치를 기준으로 Regional CRL을 만들어 배포하는 방법이다. 즉, Full CRL을 몇 개의 RA(Regional Area) 영역으로 분할해서 해당 영역에서만 사용하는 Regional CRL을 만들고 배포한다. 그러나 지역별로 Regional CRL을 배포하기 위해서는 그 지역에 위치한 차량을 파악해야만 가능하다는 단점이 있다. 네트워크 측에서는 모든 차량의 위치를 실시간으로 파악할 수 있어야 한다. 이를 해결하기 위해서 이동통신에서 사용하는 단말의 위치관리 방법을 사용하였다. 차량의 위치를 실시간으로 등록하고, 등록된 차량의 위치정보를 기준으로 RA 영역별로 Regional CRL을 만들어 각 RA 영역에 배포한다. 이 방법의 장점은 데이터 크기가 큰 Full CRL을 지역별로 분할하므로 CRL의 크기를 최소화시킬 수 있다. 단점으로는 차량의 위치를 파악하기 위한 위치 등록 절차가 추가로 수행되어야 하므로 위치등록으로 인한 부하 부담이 어느 정도 생긴다는 것이다.

선행되었던 여러 연구들에서는 차량통신의 주변 환경, 네트워크 환경, 차량 인프라 등 많은 요소들을 고려하여 CRL 배포 방법들을 다루었다. 기존의 무선통신망을 그대로 이용하면서 CRL을 효율적으로 배포하기 위한 방법들은 차량과 인증기관 등을 액세스하는 비용이 낮고 효율적이라고 알려져 있다.

III. The Proposed Scheme

3.1 Inefficiency of the Existing Regional CRL Distribution

먼저 기존 이동통신의 위치등록 기법을 이용한 Regional CRL 배포 방법[9]의 위치등록 절차를 구체화해 보고 비효율성을 분석하였다. 차량통신 네트워크에서는 이동통신과 유사하게

몇 개의 HLR로 구성되며, 차량을 처음 등록한 HLR이 마스터 HLR로 동작한다. 즉, 마스터 HLR이란 차량을 처음 등록하고 그 차량의 정보를 가지고 있는 HLR을 말하기 때문에 각 차량마다 마스터 HLR이 다르다. 다수의 지역별로 분류된 하나의 RA는 하나의 VLR(Visited Location Register)과 1:1로 매핑된다. 하나의 RA 영역은 다수의 RSU들로 구성된다. HLR은 자신이 관할하는 모든 차량의 현재의 위치정보를 알고 있으므로 현재 어느 VLR (어느 RA) 영역에 위치하고 있는지를 파악할 수 있다.

기존의 Regional CRL 배포 방법의 비효율성을 설명하기 위해 차량이 이동할 때의 위치등록 절차를 Fig. 4에 구체화하였다. 차량 A가 RA1 영역에서 RA2 영역으로 이동하여 핸드오프하는 시나리오에서의 위치등록 절차이다.

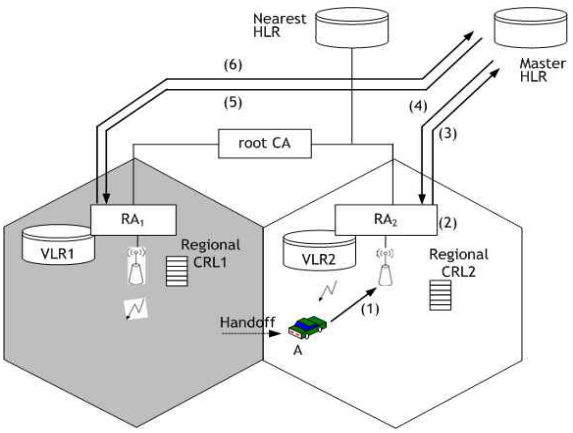

Fig. 4. The Existing Regional CRL Distribution Method

(1) 차량 A가 RA1 영역에서 RA2 영역으로 이동한다. 주변 RSU의 파일럿 신호 세기를 비교하여 자신이 새로운 RA2 영역으로 이동하였음을 인지한 후, RSU에게 핸드오프 트리거링 요청을 하고 그 지역을 담당하는 VLR2에게 위치등록을 요청한다.

(2) VLR2는 차량 A의 위치등록을 결정한다.

(3) VLR2는 해당 차량의 마스터 HLR에게 차량 A의 위치등록을 요청한다. 이 때 지리적으로 근접한 HLR 즉, Nearest HLR이 있음에도 불구하고, 멀리 떨어진 차량 A의 마스터 HLR에게 위치등록을 한다. 만약 차량의 속도가 빠르고 이동이 빈번하다면 여러 RA 영역에 걸쳐 위치등록이 발생하게 된다.

(4) 마스터 HLR은 차량 A의 위치를 등록한 후, 위치등록이 완료되었음을 VLR2에게 통보한다.

(5) 마스터 HLR은 이후에 차량 A의 이전 위치정보를 가지고 있는 VLR1에게 통보하여 VLR1이 가지고 있는 차량 A의 위치정보를 삭제하도록 요청한다.

(6) VLR1은 자신의 데이터베이스 내에서 차량 A의 위치정보를 삭제하고 마스터 HLR에게 이를 알린다. 이 절차가 끝나면 VLR1에는 차량 A의 위치정보가 삭제되고, 차량 A가 새로 진입한 영역의 VLR2에는 차량A의 위치정보가 새로이 등록된다. 그리고 마스터 HLR은 차량A의 현재 위치가 VLR2 즉, RA2 영역에 위치하고 있음을 안다. 이후에 차량 A는 Regional CRL2를 수신할 수 있다.

그러나 차량이 빠르게 그리고 자주 이동하는 실제 환경을 고려해보면 기존의 Regional CRL 배포 방법은 차량이 지리적으로 떨어진 그 차량의 마스터 HLR에게 반드시 위치등록을 해야 하기 때문에 지연시간이 매우 커지는 문제점을 가지고 있다. 이 문제점을 하나의 차량이 아니라 네트워크에 존재하는 모든 차량으로 확대해 보면, 모든 차량의 위치등록 시그널링들이 네트워크 전반에 걸쳐 횡단하므로 전체 지연시간은 더욱 커지게 될 것이다.

3.2 Proposed the Regional CRL Distribution

제안한 Regional CRL 배포 방법의 핵심적인 아이디어는 각 차량들이 자신의 마스터 HLR을 통해 위치등록을 함으로써 발생하는 긴 지연을 줄이기 위해서, 각 차량들은 현재 자신이 위치에서 지리적으로 가장 가까운 근접 HLR에 위치등록을 하도록 한다. 제안한 CRL 배포 방법은 다음과 같이 동작한다.

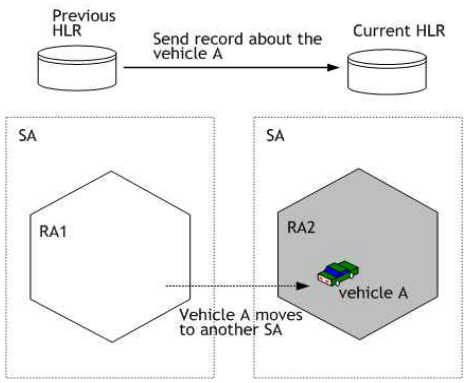

Fig. 5. Exchange of Vehicle Information between HLRs

첫째, 기존의 Regional CRL 배포 방법과 동일하게 HLR과 VLR을 활용하여 차량의 위치를 실시간으로 파악한다. 둘째, 각 차량들이 자신의 마스터 HLR에게 위치등록하기 위해 발생하는 지연을 최소화하기 위해서 각 차량들이 현재 자신이 위치에서 지리적으로 가장 가까운 근접 HLR에 위치등록을 하도록 한다. 셋째, 차량이 근접 HLR의 서비스 영역(SA; Service Area)을 벗어나 새로운 HLR 서비스 영역으로 진입하면 Fig. 5와 같이 HLR간에 차량의 정보를 상호 교환한다. 넷째, CA는 Full CRL을 모든 HLR에게 배포한다. 각 HLR은 자신의 서비스 영역에 위치하는 모든 차량을 기준으로 Regional CRL로 만들어 자신이 관리하는 서비스 영역에 배포한다.

제안한 Regional CRL 배포 방법에서의 위치등록 절차를 Fig. 6에 나타내었다. 차량 A가 SA2 영역내에서 이동하는 경우와 차량A가 SA1에서 SA2로 이동하는 두 가지 시나리오를

가정하여 설명한다. 여기에서는 이전 HLR이 차량 A의 마스터 HLR이라고 가정한다.

(1) 차량 A가 RA1 영역에서 RA2 영역으로 이동한다. 주변 RSU의 파일럿 신호 세기를 비교하여 자신이 RA2 영역에 진입하였음을 인지한 후, RSU에게 핸드오프 트리거링 요청을 하고 그 지역을 담당하는 VLR2에게 위치등록을 요청한다.

(2) VLR2는 차량A의 위치등록을 결정한다.

(3) VLR2는 근접한 HLR에게 차량A의 위치등록을 요청한다. 즉, 이전과 다르게 멀리 떨어져 있는 마스터 HLR에게 위치등록을 요청하지 않고 근접 HLR에게 위치등록을 요청하는 것이다.

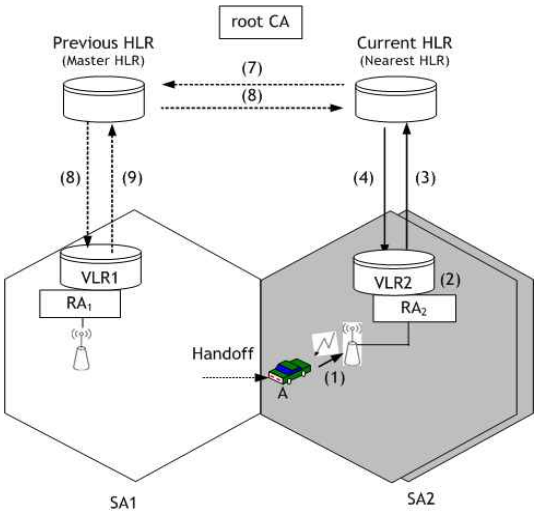

Fig. 6. Location Registration in the Proposed CRL Distribution Method

(4) 근접 HLR은 차량A의 위치를 등록한 후, 위치등록이 완료되었음을 VLR2에게 통보한다. 만약 차량이 동일한 서비스 영역인 SA2내에서 이동한다면 아래 (5)~(6)번 단계에서 위치등록이 완성되고, 만약 SA1에서 SA2로 이동하는 경우라면 아래 (7)~(10)의 단계를 모두 거쳐 위치등록이 완료된다.

(5) 만약 차량이 근접 HLR의 서비스 영역인 SA2내에서 이동하였다면, 이전에 머물렀던 VLR에게 위치등록 취소를 요청한다.

(6) 이를 수신한 VLR은 자신의 데이터베이스에서 차량 A의 위치를 삭제한 후, 응답 메시지를 근접 HLR에게 보낸다. 이 단계까지 진행되면 차량 A의 위치등록은 완료된 것이다. 즉, 기존의 차량 위치등록에서는 동일한 서비스 영역 내에서 이동하더라도 무조건 마스터 HLR에게 위치등록을 해야 한다. 반면에 제안한 방법은 차량이 동일한 서비스 영역 내에서 이동하였다면 마스터 HLR을 통해 위치등록을 하지 않고, 로컬에서 위치등록을 완료하는 것이다.

(7) 이 단계는 차량 A가 SA1 영역에서 SA2 영역으로 진입했을 때에 수행된다. 근접 HLR은 이전 HLR에게 차량이 이동하였음을 알리고 차량 A의 위치등록 정보를 삭제할 것을 요청한다.

(8) 이전 HLR은 차량A가 이전에 머물었던 VLR1에게 위치등록 취소를 요청한다.

(9) VLR1은 자신의 데이터베이스에서 차량A의 위치를 삭제한 후, 응답 메시지를 이전 HLR에게 보낸다.

(10) 이전 HLR은 차량 A의 위치등록 정보가 삭제되었음을 근접 HLR에게 통보한다.

이 방법은 대부분의 경우에 차량이 동일한 서비스 영역 내에서 위치등록((6)번 단계까지)을 완료하기 때문에 전체적으로 지연시간이 매우 적어진다. 서로 다른 서비스 영역 간에 위치등록이 발생하면 (10)번 단계까지 수행된다. 그러나 이 경우에도 (7)~(10) 단계는 실시간으로 처리할 필요가 없다. 예를 들어 (7)번을 수행하기 바로 전에 CA로부터 Full CRL을 받으면 근접 HLR은 차량A가 자신의 서비스 영역에 머물고 있다는 사실을 알기 때문에 이를 고려하여 Regional CRL을 만들어 방송을 하면 된다. 즉, 근접 HLR은 Full CRL을 Regional CRL로 분할하기 위해 필요한 자신의 서비스 영역내에 위치하는 차량들을 모두 파악하고 있기 때문에 효율적으로 위치등록을 수행할 수 있는 것이다.

결과적으로 제안한 방법은 지역별로 CRL을 만들어 배포하여 CRL 크기를 줄이고 배포 시간을 줄이는 장점을 그대로 활용한다. 그리고 차량의 빠르고 잦은 이동으로 인해 차량들이 지리적으로 떨어진 자신의 마스터 HLR에게 위치등록을 하여 지연시간이 매우 커지는 문제점을 개선하여 차량이 자신과 근접한 HLR에게 로컬 위치등록 하도록 하여 위치등록 지연 시간을 최소화 하였다.

IV. Performance Analysis

기존의 이동통신을 이용한 Regional CRL 배포 방법에서의 위치등록과 본 논문에서 제안한 Regional CRL 배포 방법에서의 위치등록 성능을 이론적으로 비교·분석한다. 이를 위해 단위 시간당 총 성능의 비율을 C'/C으로 정의하고, 서비스 영역 체류 시간에 따른 통화 수신 비율을 고려한 수신 대 이동 비율(CMR; Call-to-Mobility-Ratio)을 사용하여 차량위치 등록을 위한 시그널링 성능을 수치화 하였다.

4.1 Parameters for Analysis

차량이 동일한 SA 내에서 이동하였을 때 통화비율과 다른 SA로 이동하였을 때 통화비율(arrival rate)을 각각 λ_l과 λ_a로 그리고 $\lambda_c = \lambda_l + \lambda_a$로 정의한다. 차량이 RA내에 체류하는 평균 시간은 $1/\lambda_m$이고 SA간 이동확률은 p라고 정의한다.

$1/\lambda_m$과 p의 값은 차량의 이동 횟수와 이동하는 위치를 결정한다. 데이터베이스 액세스 비용은 데이터베이스 업데이트와 쿼리를 완성하는데 요구되는 지연시간을, 그리고 위치등록을 위한 시그널링 성능은 신호 전송을 위해 요구되는 지연시간으로 계산한다. 데이터베이스 쿼리와 업데이트는 동일한 비용으로 고려하였고, 통신 성능에 비해 매우 적다고 가정한다. HLR과 VLR의 위치등록 성능을 각각 C_h와 C_v로 정의한다. 그리고 동일한 SA 영역내에서 이루어지는 시그널링 성능을 C_{l1}, 서로 다른 SA 영역 간에 이루어지는 시그널링 성능을 C_{l2}이라 정의한다. 차량통신 네트워크 전체로는 N개의 SA가 존재한다고 가정하면 차량이 임의의 SA에 위치할 확률은 동등하게 $1/N$이다. 성능 분석을 위한 파라미터는 [10]을 참조하여 아래 Table 1과 같이 설정하였다.

Table 1. Parameters for Analysis

파라미터	설명
λ_l	이동 차량이 동일한 SA내에서 도착하는 경우의 차량 통화비율(arrival rate)
λ_a	이동 차량이 다른 SA로부터 도착하는 경우의 차량 통화비율(arrival rate)
$1/\lambda_m$	SA에서 차량의 평균 체류시간
p	SA간 차량이 이동할 확률
C_h	HLR에 대한 업데이트 및 질의에 대한 비용
C_v	VLR에 대한 업데이트 및 질의에 대한 비용
C_{l1}	차량이 동일 SA 영역내 이동 시 시그널링 비용
C_{l2}	차량이 다른 SA 영역간 이동 시 시그널링 비용

4.2 Performance of Vehicle Location Registration for the Existing CRL Dist.

기존 Regional CRL 배포 방법에서의 위치등록 성능을 계산하기 위해 Fig. 7과 같이 4가지 경우를 고려하였다. Case 1은 차량이 동일한 SA 내에서 위치등록하고 마스터 HLR도 동일한 SA 내에 위치하는 경우이다. Case 2는 차량이 동일한 SA 내에서 이동하여 위치등록하고 마스터 HLR은 다른 SA에 위치하고 있는 경우이다. Case 3은 차량이 다른 SA로 이동하여 위치등록하고 원래의 SA 또는 다른 SA 중 하나가 마스터 HLR인 경우이다. Case 4는 차량이 다른 SA로 이동하여 위치등록하고 기존의 SA와 새로운 SA 모두가 마스터 HLR의 영역이 아닌 경우이다.

Case 1에 대한 차량의 위치등록은 4개의 시그널링 성능이 계산되어져야 한다. 새로운 VLR과 HLR간 차량 위치등록 요청과 응답이 2개가 있고, 이전의 VLR과 HLR간 위치등록 취소 요청과 응답이 2개가 있다. 따라서 위치등록 시그널링 성능은 $4C_{l1}$이 된다. 이와 같이 계산하면 Case 2, Case 3, Case 4의 위치등록 시그널링 성능은 각각 $4C_{l2}$, $2(C_{l1}+C_{l2})$, $4C_{l2}$가 된다. 여기서 차량이 다른 SA으로 이동하지 않는 확률은 $(1-p)$이다. 그리고 Case 1과 같이 마스터 HLR 영역에서 체류할 확률은 $(1-p)/N$가 되며, Case 2, Case 3, Case 4는 각각 $(1-p)(N-1)/N$, $2p/N$, $(N-2)p/N$이 된다.

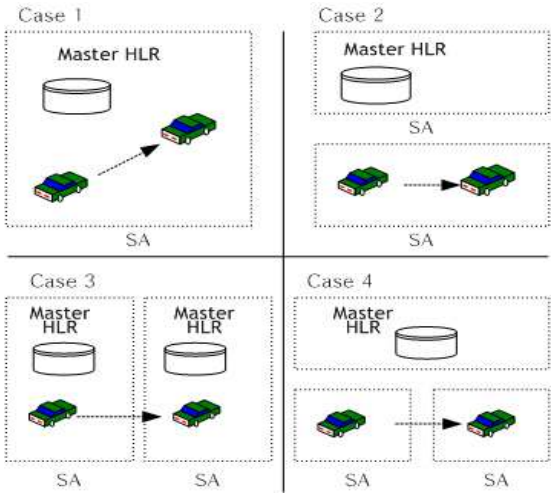

Fig. 7. Scenarios for the Existing Location Registration

기존의 위치등록 성능은 차량이 체류한 이전 VLR의 위치등록 취소, 차량이 진입한 현재의 VLR의 위치등록 요청, HLR의 위치등록을 고려하면 $2C_v$와 C_h가 된다. 계산된 값들을 모두 조합하여 위치등록을 위한 단위 시간당 전체 성능을 수식으로 나타내면 아래와 같다.

$$C_{LR} = \lambda_m[\frac{(1-p)}{N}4C_{l1} + \frac{(1-p)(N-1)}{N}4C_{l2}$$
$$\frac{2p}{N}2(+C_{l1}+C_{l2)} + \frac{(N-2)p}{N}4C_{l2} + 2C_v + C_h]$$
$$= \lambda_m[\frac{4}{N}C_{l1} + (N-1)C_{l2} + 2C_v + C_h].$$

4.3 Performance of Vehicle Location Registration for the Proposed CRL Dist.

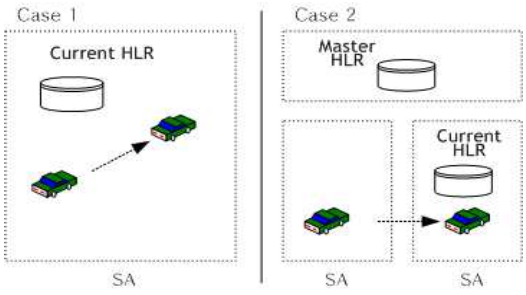

Fig. 8. Scenarios for the Proposed Location Registration

제안한 차량 위치등록 방법의 성능을 산출하기 위해 Fig. 8과 같이 2가지 경우를 고려하였다. Case 1은 차량이 $(1-p)$의 확률을 가지고 동일한 SA내에서 이동하는 것이다. Case 2는 이동 차량이 p의 확률을 가지고 서로 다른 SA을 이동하는 것

이다. 기존의 차량 위치등록과 같이 계산하면 Case1에 대한 위치등록 시그널링 성능은 $4C_{l1}$으로 나타낼 수 있다. 그리고 두 번의 VLR 데이터베이스 업데이트와 한 번의 HLR 데이터베이스 업데이트가 있으므로 총 데이터베이스 업데이트는 $2C_v + C_h$ 이다.

Case 2의 위치등록 시그널링은 새로운 VLR과 현재 HLR간 시그널링으로 $2C_{l1}$이 된다((3)~(4)단계). 그리고 이전의 VLR과 이전의 HLR간 시그널링 성능도 동일하게 $2C_{l1}$이다((8)~(9)단계). 그리고 이전의 HLR과 현재의 HLR간 두 번의 시그널링은 $2C_{l2}$이 된다. 덧붙여 두 번의 VLR 업데이트는 $2C_v$이, 두 번의 HLR 업데이트는 $2C_h$이 된다. 여기서 Case 1과 Case 2의 확률은 상호 $(1-p)$와 p의 관계이다. 모두 조합하여 위치등록을 위한 단위 시간당 전체 성능을 수식으로 나타내면 아래와 같다.

$$C'_{LR} = \lambda_m(1-p)(4C_{l1} + 2C_v + C_h) + p(4C_{l1} + 2C_{l2} + 2C_v + 2C_h).$$

4.4 Performance Comparison of Vehicle Location Registration

위치등록 시그널링 성능을 비교하기 위해 단위 시간당 총 성능의 비율인 C'/C 을, 그리고 서비스 영역에서의 차량의 통화비율과 차량의 이동성을 고려한 비율인 $CMR = \lambda_c/\lambda_m$을 사용하였다. 차량의 이동확률은 성능 비교에 큰 변수로 작용할 수 있다. 여기서 p = 0.5% 즉, p = 0.005로 그리고 HLR과 VLR의 업데이트 비용은 각각 $C_v = 0.1$, $C_h = 0.2$로 설정하였다. 상대적인 비율을 고려하기 위해 동일한 SA 사이의 위치등록 시그널링 성능인 $C_{l1} = 1$ 로, 서로 다른 두 개의 SA 사이의 위치등록 시그널링 성능인 $C_{l2} = 2, 3, 4$로 변경하면서 분석하였다.

SA의 전체 차량의 통화비율은 $\lambda_c = \lambda_l + \lambda_a$로 Case 1 $(\lambda_l = 1, \lambda_a = 9)$과 Case 2$(\lambda_m = 4, \lambda_a = 6)$를 고려하였다. 위치등록 시그널링 성능을 간략히 계산하기 위해 $\lambda_c = 10$ 으로 동일하게 설정하였다. 그리고 λ_m의 값을 변경시키며 시뮬레이션 하였다.

차량의 SA 간 이동확률 $p = 0.5\%$로 동일하다고 가정한다. 동일한 SA 사이의 위치등록 시그널링 비용인 $C_{l1} = 1$, 서로 다른 두 SA 사이의 위치등록 시그널링 비용인 $C_{l2} = 2$ 의 경우에 기존의 위치등록 방법(C_{LR})과 제안한 위치등록 방법(C'_{LR})의 성능을 수치화하여 Fig. 8에 나타내었다. Table2에서와 같이 기존의 위치등록보다 제안한 위치등록이 전체적으로 37.1%의 더 나은 성능을 나타내었다.

$C_{l1} = 1$, $C_{l2} = 3$인 경우는 기존의 위치등록 방법(C_{LR})의 성능에 비해 제안한 위치등록 방법(C'_{LR})이 약 26.7%의 더 나은 성능을, 그리고 $C_{l1} = 1, C_{l2} = 4$ 인 경우는 약 22.1%의 더 나은 성능을 나타내었다. 제안한 방법은 차량이 항상 근접 HLR에 위치등록을 하기 때문에 3가지 분석 결과, 모두 성능 면에서 더 나은 수치를 나타내었으며 약 20~40%의 비용을 절감할 수 있는 것으로 나타났다.

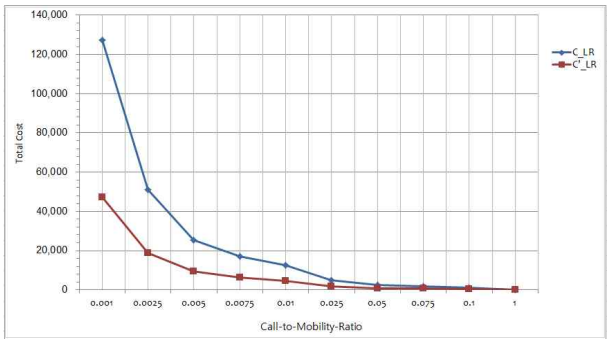

Fig. 9. Signaling Performance According to the CMR in the Case of $C_{l1} = 1, C_{l2} = 2$ and $p = 0.005$

Table 2. Comparison of C_{LR} and C'_{LR}

CMR	0.001	0.0025	0.005	0.0075	0.01	0.025	0.05	0.075	0.1	1
C_{LR}	127,400	50,960	25,480	16,982	12,740	5,096	2,548	1,698	1,274	127
C'_{LR}	47,320	18,928	9,464	6,307	4,732	1,892	946	630	473	47

특히, $CMR \leq 0.1$ 인 경우에는 차량이 SA에 평균 체류시간이 적어지는 것을 의미하므로 상대적으로 차량의 이동성이 높다는 것을 보여주며, 반대로 $CMR > 0.1$ 인 경우에는 차량이 SA에 평균 체류시간이 길어지는 것을 의미하므로, 상대적으로 차량의 이동성이 낮은 확률임을 분석 결과에서 확인할 수 있다. 만약, 차량의 이동성과 관련하여 SA의 크기가 작은 경우에 이동확률을 가정해 본다면 차량이 이동할 확률이 낮아지기 때문에 위치등록을 수행하는 성능도 낮아지게 됨을 알 수 있다.

V. Simulation Results

Full CRL 배포 방법과 제안한 Regional CRL 배포 방법의 성능을 비교하기 위해 ns-3를 이용하여 시뮬레이션을 수행하였다. 시뮬레이션은 CRL 데이터 크기를 변화시키면서 CA부터 OBU까지의 CRL 배포 시간을 측정하여 성능을 분석하였다.

5.1 Simulation Environment and Method

실험 환경을 Table 3에 나타내었다. ns-3에는 차량통신 전용의 통신 모듈이 개발되어있지 않기 때문에 대신에 다른 연구와 동일하게 ns-3에서 제공하는 이동통신 LTE lena 모듈을 적용하였다[11]. 시뮬레이션에서 차량과 RSU 수는 차량의 밀도와 밀접한 연관이 있는 요소로서 많은 샘플을 확보할수록 더 정확한 시뮬레이션이 가능하다. 본 시뮬레이션에서는 차량과 RSU의 개수를 각각 16개, 4개로 설정하고 차량의 이동과

이동 방향을 고려해서 “Random and Mobility Model"을 적용하였다. 시뮬레이션 수행시간 내에 CA에서 각 차량까지 CRL을 배포하고, CRL을 송수신 하는지 여부, 송수신 패킷의 수, 지연시간, CRL 배포에 걸리는 전체 시간을 측정하였다.

Table 3. Simulation Environment

라이브러리	운영체제	컴파일러 버전	추가모듈
ns-allinone-3.16.tar.bz2	Ubuntu 12.04 LTS (32bit)	g++-4.6.3 gcc-4.6.3	lena (LTE Module)

Table 4. Simulation Parameters

파라미터	내용
Model	Random and Mobility
No. of OBU/RSU	16 / 4
Packet Size	1,024 (bytes)
Simulation Time	10~2,100 (s)
Data Rate	256bps, 512bps
File Size	256K, 512K, 1,024K, 2,048K, 4,096K, 8,192K, 16,384K, 32,768K, 65,536K (bytes)

5.2 Performance of Full CRL Distribution

Full CRL 배포 방법의 성능 시뮬레이션 결과를 Fig. 10에 나타내었다. CRL 데이터의 크기가 증가함에 따라 CA에서 OBU에 CRL을 배포하는 지연시간이 급격하게 증가함을 알 수 있다. 각 OBU마다 지연시간이 다른 이유는 실험에서 CA와 OBU 간 링크가 16개가 사용되는데, 각 링크마다 전송 에러와 송수신 지연으로 인해 패킷 수신율이 52~100%로 달라지기 때문이다. 이로 인해 CA에서 OBU까지 CRL을 배포하는 총 지연시간이 다르게 나타났다.

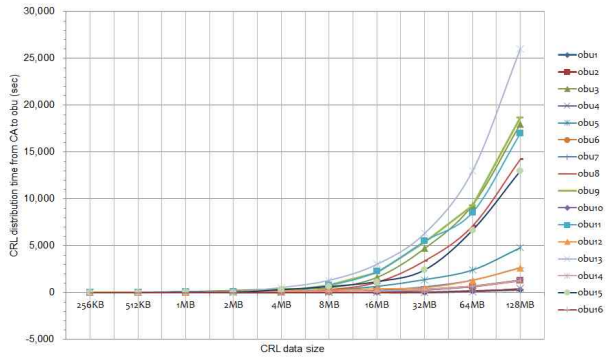

Fig. 10. Performance of the Full CRL Distribution

5.3 Performance of Proposed Regional CRL Distribution

제안한 Regional CRL 배포 방법의 성능 시뮬레이션 결과를 Fig. 11에 나타내었다. 동일하게 CRL 데이터의 크기가 증가함에 따라 CA에서 OBU에 CRL을 배포하는 지연시간이 급격하게 증가함을 알 수 있다. Full CRL 배포와 마찬가지로 링크마다 전송 에러와 송수신 지연으로 인해 CA에서 OBU까지 CRL을 배포하는 총 지연시간이 다르게 나타났다.

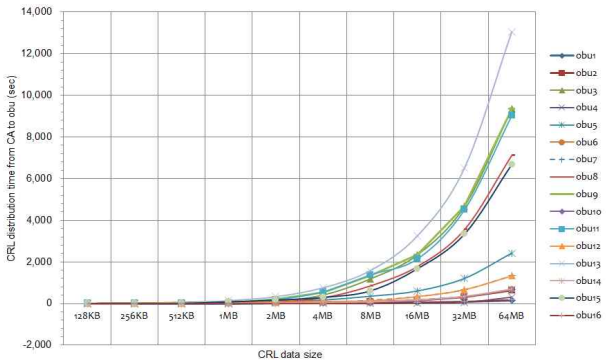

Fig. 11. Performance of the Proposed Regional CRL Distribution

5.4 Performance Comparison of Two Methods

CRL을 Full CRL 형태로 배포하는 것과 지역적으로 분할하여 Regional CRL 형태로 배포할 때의 성능을 최종적으로 비교하여 Fig. 12에 나타내었다. CRL 데이터 크기를 증가시키면서 CA부터 OBU까지 전체 지연시간을 측정했을 때, 제안한 Regional CRL 배포 방법의 지연시간이 월등히 적음을 알 수 있다. Table 6에 그 비율을 자세하게 나타내었다. CRL 데이터 크기가 구간 별로 증가함에 따라 지연시간이 약 37%~67% 적게 나타났다.

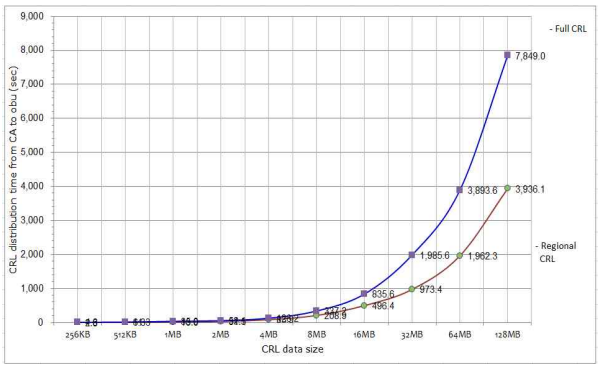

Fig. 12. Performance Comparison

Table 5. Performance Comparison(sec)

SIZE	256K	512K	1MB	2MB	4BM	8MB	16MB	32MB	64MB	128MB
Full CRL Dist.	4.63	11.29	35.04	52.08	126.17	337.17	835.58	1,985	3,894	7,849
Reg. CRL Dist.	2.82	6.30	13.00	31.54	83.93	208.90	496.40	973.41	1,962	3,936
Efficiency	61%	56%	37%	61%	67%	62%	55%	49%	50%	50%

VI. Conclusions

본 논문에서는 기존의 Regional CRL 배포 방법에서 차량의 빠르고 잦은 이동으로 인해 차량들이 지리적으로 떨어진 자신의 마스터 HLR에게 위치등록을 함으로써 지연시간이 매우 커지는 문제점을 개선하여, 차량이 자신과 근접한 HLR을 통해 로컬 위치등록을 하도록 하여 위치등록 지연 시간을 최소화하는 새로운 Regional CRL 배포 방법을 제안하였다. 제안한 방법의 효율성을 검증하기 위해 시그널링 성능을 이론적으로 분석하였으며, CRL 배포 시간을 측정하기 위해 ns-3를 이용하여 시뮬레이션을 수행하였다. 실험 결과, 제안한 방법의 시그널링 처리 성능이 기존의 Regional CRL 배포 방법에 비해 22%~37% 향상되었으며, CRL 배포 시간 또한 기존의 Full CRL 배포 방법에 비해 약 37~67% 줄일 수 있었다. 추후 연구 방향으로는 차량위치 등록 시그널링과 CRL 배포 시간을 합한 통합된 성능을 분석하고 HLR의 수를 최적화하는 문제를 연구할 예정이다.

REFERENCE

[1] The ng Connect Program(http://www.ngconnect.org)

[2] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] Taehyung Kim, "The Anti-war is being against Security Threats of Smart Car," BOANNEWS, 2015.11.25.

[4] IEEE 1609.2-2013, "IEEE Standard for Wireless Access in Vehicular Environments Security for Applications and Management Message," July 2012.

[5] P. Papadimitratos et. al,. "Certificate Revocation List Distribution in Vehicular Communication Systems," Proc. of VANET'08, pp. 86-87, Sep. 2008.

[6] T. Leinmueller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, "SEVECOM - Secure Vehicle Communication," 2006.

[7] Kenneth P. Laberteaux, Jason J. Haas, Yih-Chun Hu, "Security Certificate Revocation List Distribution for VANET," Proc. of VANET '08, 86-87, Sep 2008.

[8] A. Wasef, J. Yixin, and S. Xuemin, "ECMV: efficient certificate management scheme for vehicular networks," IEEE Global Telecommunications Conference New Orleans, LA, pp. 1-5, 2008,

[9] GangJu Cha et. al., "Method and System for Distribution Certificate Revocation List for Vehicular Communications," Korea Patent, Reg. No., 10-1509866, April 2015.

[10] Jie Li, Yi Pan, Yang Xiao, "A Dynamic HLR Location Management Scheme for PCS Networks," IEEE INFOCOM 2004.

[11] http://networks.cttc.es/mobile-networks/software-tools/lena/

Authors

Hyun-Gon Kim received the B.S. and M.S. degrees at the department of Electrical Engineering of Kumoh National University and the Ph.D degree at the department of Computer Science of Chungnam National University, Korea, in 1992, 1994, and 2003 respectively. He worked at the division of Information Security of ETRI from 1994 to 2005 as a senior engineer. He has been a visiting professor at the department of Computer and Information Sciences, University of Delaware, United States from 2011 to 2013. He is an associate professor at the department of Information Security of Mokpo National University currently. His research interests include security of vehicular communications and security of mobile communications.

Hwi-Seung Hong received the B.S. and M.S. degrees at the department of Information Security of Mokpo National University, Korea, in 2014 and 2015 respectively.

He is a faculty of the department of IT System of Chosunilbo, Korea, in 2015 currently. His research interests include Web&broadcast application of information security, and security of vehicular communications.