Journal of The Korea Society of Computer and Information
Vol. 21 No. 10, pp. 77-83, October 2016

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.10.077

A Certificate Revocation List Distribution Scheme over the eMBMS for Vehicular Networks

Hyun-Gon Kim*

Abstract

To verify the trustworthiness of messages, public key certificates and certificate revocation list(CRL) has been standardized for vehicular networks. However, timely distribution of large CRLs to vehicles should be more elaborated with low bandwidth utilization from a practical point of view. To address this concern, we propose a CRL distribution scheme using long term evolution(LTE) point-to-multicast transmission, namely the enhanced multimedia broadcast multicast service(eMBMS). The schem is much more resource efficient than the existing unicast CRL distribution schemes for vehicular networks and it allows realizing the regional CRL distribution schemes efficiently in LTE network. By means of ns-3 simulation, we analyze the performance, latency, and execution time of the scheme in terms of varying coverage of the multimedia broadcast multicast service over single frequency network (MBFSN).

▸ Keyword : Certificate Revocation List, Regional CRL, eMBMS, MBSFN

I. Introduction

IEEE에서 제정한 WAVE(Wireless Access for Vehicle Environment)는 고속으로 주행하는 차량에서 차량과 기지국간 그리고 차량들간 통신서비스를 제공받을 수 있는 차량통신 표준 기술이다[1]. 이 중 보안은 IEEE 1609.2에 정의되어 있으며, 공개키 방식의 단기 익명 인증서(pseudonyms)를 사용하여 통신 상대 인증, 메시지 인증, 그리고 차량의 위치 익명성 등을 지원한다. 또한 차량의 고장, 오작동, 차량 해킹, 관리적 보안 등의 이유로 해당 인증서를 취소할 수 있도록 인증서 취소목록(CRL; Certificate Revocation List)을 사용한다. CRL은 발행자에 의해 서명되고 서명 결과 값이 부착되어 배포되며, 이를 수신한 차량들은 검증 과정을 수행한다. 차량용 CRL은 배포 주기가 유선에 비해 매우 짧고 무선으로 전송된다는 특징이 있다.

한편, WAVE 네트워크를 구축하는 초기 단계에서는 기지국인 RSU(Road Side Unit)가 충분히 설치되지 않은 지역이나 RSU의 전파 수신이 약한 지역이 존재할 것이므로 차량이 제 시간에 갱신된 최신의 CRL을 수신하기 어려울 것이다. 만약 어떠한 사유로 갱신된 CRL을 다운로드 하지 못하게 되면, 차량은 주변 차량으로부터 수신된 메시지의 인증서와 첨부된 서명 값을 신뢰할 수 없기 때문에, 공격 차량인지 정상적인 차량인지에 대한 판단이 어려워진다. 따라서 정상적인 차량통신에 어려움을 겪게 된다.

이와 관련하여 이동통신 네트워크를 이용해 CRL을 배포하는 기법이 제안되었다[2]. 이 기법에서 차량은 테슬라 S모델의 예에서와 같이 LTE(Long Term Evolution) 모듈을 추가로 장착해야 한다. 이 기법의 단점은 유니캐스트 기반의 단대단(point-to-point) 전송 방식을 사용하기 때문에 유선 자원을 비효율적으로 사용한다. 그러나 CRL을 이동통신 네트워크를 통해 배포하기 위해, 어떠한 방식으로 배포할 것인지, 두 네트워크간 어떻게 인터페이스 할지, 이동통신 네트워크내에 있는 엔티티들은 어떠한 추가 기능을 가져야 할지 등의 구체적인 실현 방안에 대해서는 연구가 더 필요하다.

이러한 점들을 고려하여 본 논문에서는 eMBMS(enhanced Multimedia Broadcast Multicast Service)에서 제공하는 멀티캐스트 기반의 단대다(point-to-multicast) 전송 방식을 이용하여 유선자원을 효율적으로 이용할 수 있는 CRL 배포 기법을 제안하였다. 또한 두 네트워크간 인터페이스와 연동 시나리오를 설계하였으며, 지역별 CRL을 배포하는 방식이 실현 가능하도록 WAVE 네트워크에서 정의한 영역들을 이동통신 네트워크의 영역들로 매핑할 수 있는 방법을 설계하였다.

• First Author: Hyun-Gon Kim, Corresponding Author: Hyun-Gon Kim
*Hyun-Gon Kim (hyungon@mokpo.ac.kr), Dept. of Information Security, Mokpo National University
• Received: 2016. 08. 17, Revised: 2016. 09. 05, Accepted: 2016. 10. 05.

본 논문은 다음과 같이 구성된다. 서론에 이어 2장에서는 CRL 배포와 관련된 기존의 연구 결과들을 분석하고 3장에서는 본 연구에서 제안한 eMBMS를 이용한 지역별 CRL 배포 방법에 대해서 상세히 설명한다. 4장에서는 제안한 기법을 시뮬레이션을 통해 평가하고 5장에서는 결론과 향후 연구방향을 제시한다.

II. Related Works

1. CRL Distribution

차량통신에서는 장기 인증서뿐만 아니라 차량 자체의 인증, 송수신하는 메시지의 인증, 차량의 위치 프라이버시 보호를 위해 단기 익명 인증서를 사용한다. 그리고 차량의 고장이나 오동작, 차량 해킹, 관리적 보안 등의 이유로 해당 인증서를 취소할 수 있도록 CRL을 사용한다. 그러나 비교적 긴 주기를 가지고 CRL을 배포하는 유선과는 다르게, 차량통신에서의 CRL은 짧은 주기로 배포되므로 차량이 정확히 제 시간에 CRL을 수신하는 것이 매우 중요하고, 고가의 무선 대역을 사용하므로 효율성도 고려되어야 한다. 다음은 차량통신의 CRL과 관련된 기존 연구 결과들이다.

Rapadimitrator는 각 RSU가 매우 낮은 대역만으로 넓은 영역을 대상으로 큰 사이즈의 CRL을 배포할 수 있는 간단하고 스케일 가능한 기법을 제안하였다[3]. 이 기법에서는 CRL을 다수의 검증 가능한 조각들로 인코딩하고 배포해서 차량들은 자신이 가지고 있지 않은 조각들만을 RSU로부터 수신할 수 있도록 하였다. Laberteaux는 CRL을 다수의 조각들로 나눈다는 점은 유사하지만 CRL을 주변 차량들을 통해 점진적으로 배포하는 기법을 제안하였다[4]. 이 기법의 단점은 주변에 RSU나 차량들이 밀집하지 않은 지역에서는 낮은 성능을 나타낸다는 것이다. Lin은 RSU를 적극적으로 활용해서 CRL을 배포한다[5]. 각 RSU는 Full CRL과 업데이트된 base-CRL을 가지며, 지나가는 차량들이 브로드캐스트한 모든 메시지에 포함된 인증서들의 상태를 지속적으로 체크한다. 만약 RSU가 하나의 인증서가 취소되었다고 판단하면, 진입하는 차량들이 보유한 CRL을 업데이트 할 수 있도록 경고 메시지를 브로드캐스트 하여 인증되지 않는 차량들과 통신을 하지 않도록 한다. Rao는 신선도(freshness) 개념을 도입하고 송신자의 인증서를 RSU가 검증하도록 하는 기법을 제안하였다[6]. 즉, 수신자는 송신자의 인증서가 검증된 시간을 기준으로 메시지를 수신할 것인지 거절할 것인지를 결정한다. Hass는 계산 부하를 줄이기 위해 블룸필터를 사용하고, CRL내에 취소된 인증서를 검색할 때 확률에 기반한 데이터 구조를 사용할 것을 제안하였다[7]. Raya는 RC2RL(Revocation using Compressed Certificate Revocation List) 프로토콜을 설계하고 CRL 배포 오버헤드를 줄일 수 있는 블룸필터 기반의 압축 기법을 제안하였다[8].

한편, 유선의 경우에는 인증서 취소 상태를 확인하기 위해 CRL 배포 방식 이외에도 OCSP(Online Certificate Status Protocols)를 이용하여 인증서 취소 상태를 즉시 확인하는 방법을 사용한다. 그러나 차량통신 환경에서 OCSP를 적용할 경우, 인증서 취소 상태를 조회하기 위해 인증기관 또는 디렉토리 서버와 통신이 이루어져야 한다. 이 때 브로드캐스트 채널이 아닌 데이터 채널이 수시로 연결되어야 하므로 무선 자원이 사용된다. 만약 다수의 주변 차량으로부터 패킷을 수신할 경우, 다수의 무선 채널을 사용해야 하므로 무선 자원을 비효율적으로 사용하게 된다. 이러한 점을 고려하여 차량통신에서는 CRL을 서명하고 CA 인증서를 첨부해서 배포하고 이를 수신한 차량들은 CRL을 검증하도록 한다[1].

본 연구와 직접적으로 관련된 연구결과로서, Bellur는 전체 서비스 영역을 다수의 지리적 영역으로 분할하고, 그 지역으로 한정한 지역 인증서를 사용하며, 지역별로 CRL을 운영함으로써 CRL 사이즈를 크게 줄일 수 있는 기법을 제안하였다[9]. H. S. Hong은 Full CRL을 지역별 CRL로 만들어 배포하는 방식은 유사하나, 지역을 구성하는데 있어서 이동통신의 위치등록 기법을 이용하여 차량의 위치를 실시간으로 추적·관리하고, 그 지역에 위치한 차량들에게만 그 지역의 CRL을 전달하는 기법을 제안하였다[9]. 이 기법은 단대단 통신을 이용하기 때문에 유선 자원을 효율적으로 이용하기 어렵고, 모든 차량의 위치를 실시간으로 파악하기 위해 네트워크 측의 처리 부담이 있으며, 차량통신 네트워크와 이동통신 네트워크가 밀결합(tightly-coupled) 된다는 단점이 있다.

선행되었던 여러 연구들은 차량통신의 주변 환경, 네트워크 환경, 차량 인프라 등 많은 요소들을 고려하여 CRL 배포를 효율적으로 할 수 있도록 적절한 필터를 사용하여 CRL 사이즈를 줄이거나, 지역별 CRL을 운영하거나, 다른 통신 채널을 통해 CRL을 배포하는 기법들을 다루었다. 즉, CRL 사이즈를 줄이는 방법, 효율적으로 CRL을 배포하는 방법, 어떻게 CRL을 정확히 제 시간에 배포할 것인지 등이 주요 관심사 이다.

2. Introduction to eMBMS

이 절에서는 eMBMS에 대해 본 논문과 관련된 내용 위주로 살펴본다[10]. eMBMS는 LTE 네트워크를 통해 동일한 데이터를 다수의 단말에게 동시에 단대다 형태로 전송하는 기술이다. eMBMS는 멀티캐스트와 브로드캐스트 모드를 둘 다 지원한다. 브로드캐스트는 하나의 소스에서 특정 서비스 영역에 속한 모든 사용자에게 멀티미디어 데이터를 단방향으로 전송하는 서비스이다. 사용자는 자신의 단말에서 방송 서비스 수신 기능을 활성화 또는 비활성화 시킬 수 있다. 이 모드는 모든 사용자가 방송된 데이터를 동일하게 수신할 수 있기 때문에 서비스 가입절차가 필요 없으며, 사용자 과금 정보를 생성하거나 수집할 필요가 없다. 멀티캐스트 모드는 특정 멀티캐스트 그룹을 구성하고 그 그룹의 멤버들에게만 멀티미디어 데이터를 전송하는 서비스이다. 사용자가 특정 멀티캐스트 서비스를 수신하기 위해서는 해당 멀티캐스트 서비스 그룹에 가입되어 있어야 하고, 가입된 멀티캐스트 그룹에 조인된 상태에서만 멀티캐스트 데이터를 수신할 수 있다.

MBSFN(Multimedia Broadcast multicast service over Single Frequency Network)은 다수의 기지국에서 같은 패킷을 같은 시간에 전송하는 브로트캐스트 전송방식인 멀티 셀 전송방식을 이용하여 물리계층에서 다이버시티 이득을 얻어 전송효율을 최대화시킨다. 즉, 고가의 무선 주파수 자원을 효율적으로 활용하는데 유용한 네트워크 구축 기술로서, 서로 다른 전송단이 같은 주파수를 통해 같은 데이터를 동시에 전송하는 네트워크를 말한

다. 이를 이용하면 인접한 여러 셀에 걸쳐 동시에 같은 멀티캐스트나 브로드캐스트 데이터를 더 효율적으로 전송할 수 있다.

MBSFN의 셀 개념을 Fig. 1에 나타내었다[11]. 좌측은 7개의 기지국이 하나의 차량을 향해 동시에 데이터를 전송하는 경우를 보여주고 있다. 이동하는 차량은 우측과 같이 7개의 기지국으로부터 동일한 주파수로부터 동일한 데이터를 동시에 수신하게 되므로 7개의 작은 셀이 아니라 사이즈가 큰 하나의 셀에서 데이터를 수신하는 효과를 얻을 수 있다. MBSFN을 이용하면 넓은 지역에 분포하는 차량에 동일한 방송 서비스를 제공할 수 있다. 중요한 점은 각 셀의 경계지역은 기지국으로부터 거리가 멀고 인접 셀 기지국과 상대적으로 가까워 수신 신호의 품질이 악화되기 쉬우나, 인접 셀 기지국에서도 동일한 신호가 전송되므로 여러 기지국으로부터 수신한 신호를 중첩하여 수신 신호의 품질을 향상 시킬 수 있다. 그렇지만, 여러 전송단에서 동시에 전송한 데이터는 거리나 지형지물의 특성에 따라 서로 다른 거리와 방향으로부터 데이터가 도착하므로 심각한 다중경로 페이딩 문제가 발생할 수 있다. 이를 최소화하기 위해 eMBMS에서는 다양한 대응 기술들을 적용하고 있다.

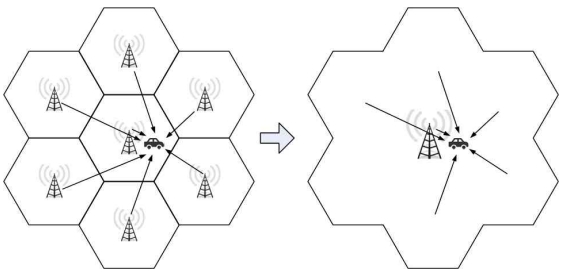

Fig. 1. Cell of MBSFN[11]

eMBMS는 전체 서비스 영역에 대해서 최대 256개의 MBSFN 영역을 구성할 수 있으며, 각 셀은 8개까지의 서로 다른 MBSFN 영역의 멤버가 될 수 있다. Fig. 2에 eMBMS 서비스 영역의 예를 나타냈다. MBSFN 영역 0은 셀 1~10을 포함하며, MBSFN 255 영역은 셀 8~16을 포함하며, MBSFN 영역 5는 셀 17~20을 포함한다. 셀들이 MBSFN 영역들간에 중첩되는 예로서, 셀 8, 9, 10은 MBSFN 영역 0과 255에 중첩된다.

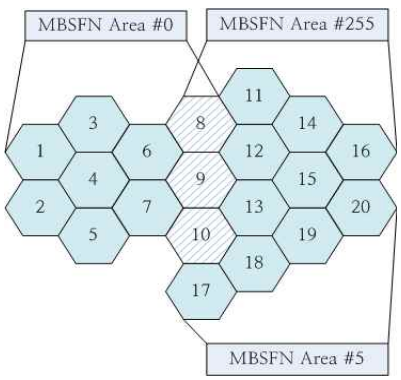

Fig. 2. An Example of MBSFN Area[11]

III. The Proposed Scheme

선술한 바와 같이 기존의 이동통신 네트워크를 이용하여 지역별 CRL을 배포하는 기법은 단대단 전송을 하기 때문에 유선 자원을 효율적으로 이용하기 어렵고, 모든 차량의 위치를 실시간으로 파악하기 위해 네트워크 측의 처리 부담이 있으며, 차량통신 네트워크와 이동통신 네트워크가 밀결합 된다는 단점이 있다[2].

본 논문에서는 이를 개선하기 위해 첫째, 단대다 통신인 LTE의 eMBMS를 이용하여 유선 구간의 자원을 효율적으로 사용한다. 둘째, 지역별 CRL 기법을 WAVE 네트워크에서도 가능하도록 WAVE 네트워크의 지역별 영역 정보를 eMBMS의 MBSFN 영역과 중첩하여 매핑시킨다. 이를 통해 부수적으로 차량의 CRL 수신율도 높일 수 있다. 셋째, 실시간 차량의 위치 정보를 이용하지 않고 지역별로 브로드캐스팅 하여 네트워크 측의 계산 부담을 감소시킨다. 넷째, 차량통신 네트워크와 이동통신 네트워크간의 결합을 최소화(loosely-coupled)하여 실현 가능성을 높인다.

본 논문에서는 지역별 CRL을 효율적으로 생성하고 배포할 수 있도록 eMBMS의 다음 특징들을 이용하였다.

- □ eMBMS 전체 서비스 영역을 다수의 MBSFN 영역으로 구성할 수 있음
- □ 하나의 기지국 eNB(evolved Node B)는 8개의 MBSFN 영역까지 속할 수 있음
- □ MBSFN 영역 내 eNB들은 모두 동기화(synchronize)됨
- □ MBSFN 영역 내에서는 동일한 콘텐츠를 방송하고, 이웃한 MBSFN 영역은 다른 콘텐츠를 방송할 수 있음
- □ MBSFN 영역 내에서 차량이 이동할 경우에 핸드오프가 필요 없음

1. CRL Distribution Strategies

제안한 기법에서 차량은 기본적으로 WAVE 차량통신을 하며, 차량은 테슬라 S모델의 예에서와 같이 LTE 모듈을 추가로 장착한다고 가정한다. 즉, LTE 네트워크를 통해 CRL을 배포함으로써, WAVE 통신이 원활하지 않거나 통신 인프라가 구축되지 않은 지역에서도 차량이 제 시간에 최신의 CRL을 획득할 수 있도록 한다.

이를 위해 먼저 LTE의 유니캐스트, 브로트캐스트, 멀티캐스트 중 어떠한 방법이 CRL을 효율적으로 배포할 수 있는지에 대해 고려가 필요하다. 유니캐스트는 임의의 시간에 동일한 CRL 데이터를 단대단 형태로 모든 차량에게 전달하므로 유선 자원을 비효율적으로 사용한다. 브로드캐스트와 멀티캐스트는 동일한 CRL 데이터를 다수의 차량에게 동시에 전송된다는 점에서 동일하다. 차이점은 브로드캐스트는 불특정 다수의 차량에 CRL을 전송하는 반면, 멀티캐스트는 특정된 다수의 차량에게 CRL을 전송한다는 점이다. 브로드캐스트는 어떤 차량이 이 데이터를 수신하는지 관심을 갖지 않으며, 브로드캐스트 한 CRL을 차량이 수신에 실패하더라도 신경 쓰지 않는다. 반면 멀티캐스트는 CRL을 수신하고자

하는 차량들을 그룹으로 구성하고, 그룹 내 모든 차량이 정상적으로 CRL을 수신할 수 있도록 관리한다. 이로 인해 별도의 그룹을 생성하고 관리해야 하는 부담이 있다.

차량통신 네트워크에 CRL을 배포하는 방법으로서 특정 지역에 동시에 CRL을 배포하는 브로드캐스트가 일견 적합해 보인다. 그러나 본 논문에서는 eMBMS 기반의 멀티캐스트를 사용할 것을 제안한다. 이유는 2.2절에서 설명한 바와 같이, 여러 셀에 걸쳐 동시에 같은 데이터를 관심 있는 차량들에게 효율적으로 전송할 수 있다. 그리고 WAVE 네트워크의 지역별 영역을 그대로 LTE 네트워크의 MBFSN 영역으로 중첩시켜 매핑함으로써 차량의 CRL 수신율을 높일 수 있다. 즉, MBSFN의 장점을 활용하면 해당 지역별로 특정 차량들에게만 효율적으로 CRL을 브로드캐스팅할 수 있는 것이다. 차량통신 도입 초기에는 일부 차량만 차량통신 기능을 가지고 있을 것이다. 통신을 희망하는 차량들만을 그룹핑하고 그 그룹에 속한 차량들에게만 CRL을 배포할 수 있다.

2. MBSFN Region Assignment

WAVE 네트워크에서 CRL을 배포하는 방법은 크게 두가지로 나눌 수 있다. 하나는 Full CRL을 전체 네트워크에 배포하는 방법이고, 다른 하나는 Full CRL을 다수의 지리적인 지역 영역(RA; Regional Area)으로 나누고 각 지역에 해당하는 지역별 CRL을 배포하는 방법이다. 전자는 Full CRL만 필요하지만, 후자는 다수의 RSU들이 하나의 RA에 속하는 형태의 RSU-to-RA 테이블과 지역별 CRLs이 필요하다.

차량통신에 사용하는 CRL을 LTE 네트워크를 통해 배포하기 위해서 먼저, WAVE 네트워크에서 정의한 RSU-to-RA 테이블을 정적으로 또는 동적으로 LTE 네트워크에 전달한다. 이를 수신한 LTE 네트워크에서는 RA-to-MBSFN 테이블을 만들어 두 네트워크 영역들을 매핑 한다. RA-to-MBFSN 테이블은 RA 영역에 해당하는 MBSFN 영역 내 eNB들의 목록이다. 실제로는 두 네트워크가 중첩되어 있고 두 네트워크의 영역 사이즈가 다르기 때문에 둘 간 매핑을 적절히 해야 한다.

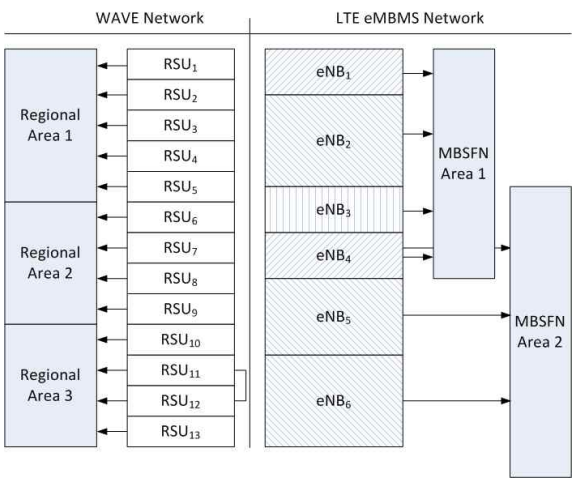

Fig. 3. An Example of MBSFN Region Assignment

두 네트워크의 영역간 매핑의 예를 Fig. 3에 나타내었다. MBSFN의 장점을 활용하기 위해서 다수의 RA 영역을 하나의 MBSFN 영역으로 매핑하도록 한다. 예를 들어 RA_1 영역과 RA_2 영역은 하나의 $MBSFN_1$ 영역에 속한다. 그리고 LTE 네트워크 자체적으로 보면 eNB_3와 eNB_4 영역은 $MBSFN_1$과 $MBSFN_2$ 영역에 중첩된다. 이를 WAVE 네트워크에 투영해보면 RSU_5의 일부영역, RSU_6~RSU_7 전체 영역, RSU_8의 일부 영역이 $MBSFN_1$과 $MBSFN_2$ 영역에 중첩된다.

3. Design of Functional Requirements and Interface

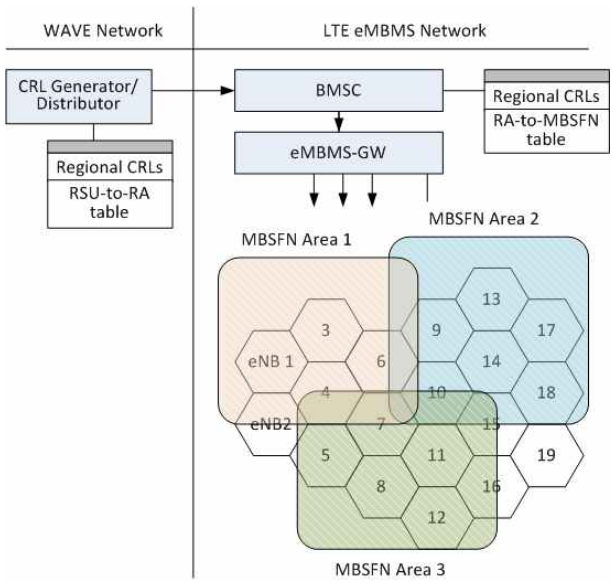

Fig. 4. Interface between Two Networks

지역별 CRLs과 RSU-to-RA 테이블을 LTE 네트워크로 전달하기 위해서는 두 네트워크가 상호 인터페이스 되어야 한다. 두 네트워크 사이의 종속성을 최소화시키기 위해서 각 네트워크에 속하는 엔티티들간의 연결을 최소화하고 각 엔티티들에 추가되는 기능들도 최소화시켰다.

□ 인터페이스 설계

CRL Generator/Distributor에서 BMSC(Broadcast Multicast Service Center) 방향으로 단방향 인터페이스를 새롭게 정의한다. BMSC에서 eMBMS-GW 방향으로는 기존의 인터페이스를 사용하며, 지역별 CRL을 포워딩하기 위한 단방향 메시지만을 추가한다.

□ 추가 기능 설계

CRL Generator/Distributor에 추가되는 기능은 기존에 사용하고 있던 지역별 CRLs과 RSU-to-RA 테이블을 BMSC에게 정적 또는 동적으로 전달하는 기능이다. RSU-to-RA 테이블을 수신한 BMSC는 이를 RA-to-MBSFN 테이블과 매핑한다. 그리고 이 테이블을 기준으로 지역별 CRL을 eMBMS-GW에게 전달한다. 따라서 BMSC는 MBSFN 영역을 RA로 매핑하고

관리하는 기능을 가져야 한다. eMBMS-GW는 멀티캐스트 세션을 제어하고, 지역별 CRLs을 해당 eNB들에게 IP 멀티캐스트 형태로 전송하는 기능을 가져야 한다. 차량의 LTE 모듈은 새로운 MBSFN 영역에 진입하였을 때에 이전 MBSFN 영역의 멀티캐스트 그룹에서 탈퇴하고, 새로운 MBSFN 영역의 멀티캐스트 그룹에 조인하는 절차를 수행해야 한다. 최종적으로 차량은 eMBMS를 통해 현재 위치한 지역의 지역별 CRL을 수신하여 사용한다.

IV. Performance Analysis

시뮬레이션을 통해 제안한 eMBMS의 MBSFN 영역을 이용한 지역별 CRL 배포 방법을 검증하였다. ns-3[12]를 이용하여 MBSFN 영역의 크기에 따라 성능과 지연시간 그리고 실행시간이 어떻게 변화하는지 분석하였다. 차량에는 LTE 모듈 즉, UE(User Equipment)가 장착되고, 지역별 CRL이 LTE의 eMBMS를 통해 배포되는 환경을 구성하고 실험하였다. LTE 모듈이 멀티캐스트 조인이나 탈퇴를 위한 동작은 새로운 MBSFN 영역에 진입할 경우에만 이루어지고 실제 CRL 배포 시점에는 영향을 주지 않으므로 성능 분석에서는 고려하지 않았다.

1. Simulation Environment and Method

실험은 리눅스 우분투 환경에서 ns-3가 기본적으로 제공하는 LTE 모듈을 사용하고, LTE EPC(Evolved Packet Core) Network Simulator(LENA) 모듈을 추가하였다[13]. LENA 모듈은 코어 네트워크 장치들을 설정하여 테스트 할 수 있는 환경을 제공한다. CRL 데이터는 BMSC에서 자체적으로 생성하여 배포하였다. 지역별 CRLs은 MBMS-GW와 eNB까지 유선으로 전송되고 eNB와 차량의 UE 사이는 무선으로 전달된다.

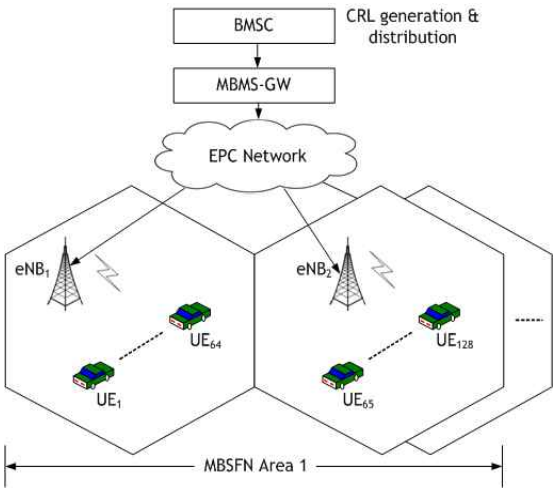

Fig. 5. Simulation with varying coverage of MBFSN

실험 환경과 사용된 파라미터들을 Table 1과 Table 2에 각각 나타내었다. eNB는 60m 간격으로 고정시켜 설치하고, UE는 'Random Walk 2d Mobility 모델'을 이용하여 UE가 랜덤하게 이동하면서 통신하도록 하였다. 그리고 하나의 MBSFN의 영역에 속한 eNB의 개수를 1개에서 128개까지 변화시키고, 더불어 하나의 eNB에 부착된 UE의 개수를 1개에서 256개까지 변화시켜서 두 조합에 따른 전체적인 성능(throughput), 지연(latency), 실행시간(execution time)을 측정하였다. 즉, MBSFN의 영역의 크기에 따라 성능, 지연, 실행시간이 어떻게 변화하는지를 분석하였다.

Table 1. Simulation Environment

ns-3	Processor	OS and compiler	ns-3 additional module
ns-allinone-3.22.tar.bz	Intel Core i5 with 2.5GHz	Ubuntu 14.04 LTS, gcc-4.6.3 g++-4.6.3	lena module (LTE+EPC)

Table 2. ns-3 Simulation Parameter

Parameter	Value
eNB mobility model	Constant Position Mobility
UE mobility model	Random Walk 2d Mobility
Number of UE	1 ~ 256
Number of eNB	1 ~ 128
Simulation time	5 (sec)
Uplink/down link between BM-SC and MBMS GW	1,024 (Mbps)
Max CRL data size	1,024 (bytes)
LteHelper::Scheduler	PfFfMacScheduler
LteHelper::PathlossModel	FriisSpectrumPropagationLossModel
LteEnbNetDevice	UlBandwidth & lBandwidth "25" / DlEarfcn & UlEarfcn 100"
LteUePhy	TxPower "10" & NoiseFigure "9"
LteEnbPhy	TxPower "30" & NoiseFigure "5"

2. Throughput vs Coverage of MBSFN

MBSFN의 영역 크기에 따른 성능 분석 결과를 Fig. 6에 나타내었다. 실험 결과, 영역 사이즈가 가장 큰 MBSFN(1)의 경우가 성능이 가장 높게 나타났으며, CRL 데이터 수신율이 가장 높다. 영역 사이즈가 크면 지역별 CRL이 BMSC에서 eNB로 전달될 때, 하나의 흐름(flow)으로만 전달되므로 유선 구간의 자원을 효율적으로 사용할 수 있다. 반대로 영역 사이즈가 작으면 그 영역의 개수만큼의 지역별 CRL들이 다수의 흐름으로 전달되므로 유선 구간의 자원이 비효율적으로 사용된다. 더불어 UE의 개수가 증가함에 따라서는 CRL 데이터 수신율이 떨어진다.

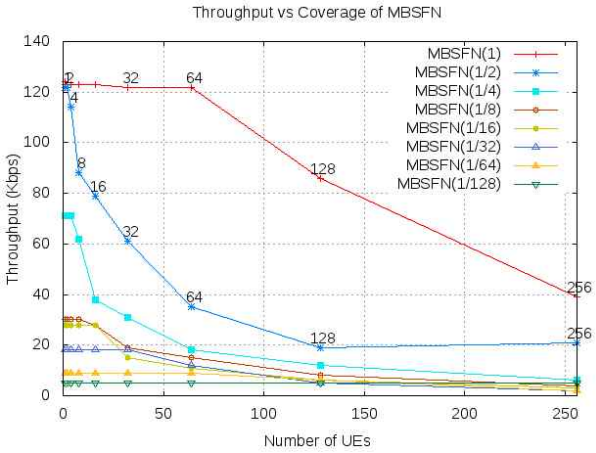

Fig. 6. Throughput vs Coverage of MBSFN

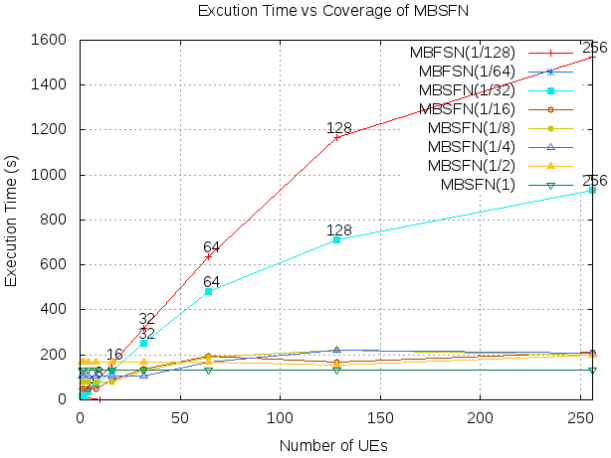

Fig. 8. Execution Time vs Coverage of MBSFN

3. Latency vs Coverage of MBSFN

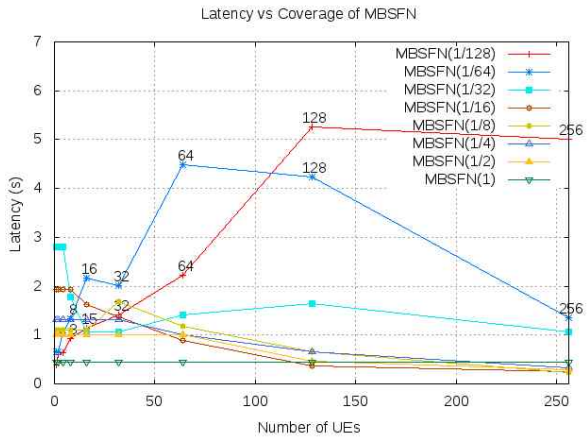

Fig. 7. Latency vs Coverage of MBSFN

MBSFN의 영역 크기에 따른 지연 시간 분석 결과를 Fig. 7에 나타내었다. 실험 결과, 영역 사이즈가 가장 작은 MBSFN(1/128)의 경우가 지연이 가장 긴 것으로 나타났다. 영역 사이즈가 작으면 처리해야 할 서로 다른 지역별 CRL이 많아짐으로 인해 지연시간도 길어지기 때문이다. 더불어 UE의 개수가 증가함에 따라서는 CRL 데이터 수신 지연이 길어짐을 알 수 있다.

4. Execution Time vs Coverage of MBSFN

MBSFN의 영역 크기에 따른 단위 노드의 실행 시간 분석 결과를 Fig. 8에 나타내었다. 실험 결과, 영역 사이즈가 가장 적은 MBSFN(1/128)의 경우가 실행시간이 가장 긴 것으로 나타났다. 더불어 UE의 개수의 증가에 따라서 실행시간이 길어짐을 알 수 있다. 마찬가지 이유로 영역 사이즈가 작으면 처리해야 할 서로 다른 지역별 CRL이 많아짐으로 인해 각 노드의 평균 실행시간도 길어지기 때문이다.

V. Conclusions

본 논문에서는 기존의 차량통신용 CRL을 이동통신 네트워크를 통해 배포하는 기법이 유니캐스트 기반의 단대단 전송방식을 사용함으로 인해 유선자원을 비효율적으로 사용하는 단점을 개선하였다. eMBMS에서 제공하는 멀티캐스트 기반의 단대다 전송 방식을 적용하여 유선자원을 효율적으로 이용하고, 차량 네트워크와 이동통신 네트워크간 인터페이스와 연동 시나리오를 설계하였으며, 지역별 CRL을 배포하는 방식이 실현 가능하도록 WAVE 네트워크에서 정의한 영역들을 이동통신 네트워크의 영역들로 매핑하는 방식을 설계하였다.

제안한 기법을 시뮬레이션을 통해 검증한 결과, 하나의 MBSFN 영역에 속하는 eNB의 수가 더 많을수록 CRL 배포 성능이 높게 나타나고 지연시간이 더 짧게 나타났다. 즉, eMBMS의 MBSFN을 활용하는 것이 기존 기법들에 비해 CRL을 더 효율적으로 배포할 수 있다. 제안한 기법의 단점으로는 LTE 모듈이 MBSFN 영역별로 멀티캐스트 조인이나 탈퇴를 추가로 수행해야 한다는 점이다. 그러나 이 기능들은 새로운 MBSFN 영역에 진입할 경우에만 이루어지므로 실제 CRL 배포 시점에는 영향을 주지 않는다. 추후 연구로 CRL 데이터 크기에 따라 MBSFN 영역을 최적화시키는 문제와 CRL 데이터 사이즈가 계속 증가하는 환경에서 CRL 배포방식에 따른 전송 효율을 높이는 문제를 다룰 예정이다.

REFERENCES

[1] IEEE 1609.2-2013, "IEEE Standard for Wireless Access in Vehicular Environments-Security Service

for Applications and Management Messages," IEEE Vehicular Technology Society, April 2013.
[2] Hwi Sung Hong et al, "Regional Certificate Revocation Method based on the Local Vehicle Location Registration for Vehicular Communications," Journal of The Korea Society of Computer and Information, Vol. 21, No. 1. pp. 91-99, Jan. 2016.
[3] P. Papadimitratos et al, "Certificate revocation list distribution in vehicular communication systems," Proc. Fifth ACM international workshop on Vehicular Inter-networking, pp. 86-87, 2008.
[4] K. Laberteaux et al, "Security certificate revocation list distribution for vanet," Proc. Fifth ACM international workshop on Vehicular Internetworking, pp. 88-89, Sept. 2008.
[5] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen. "Security in Vehicular Ad Hoc Networks." IEEE Communications Magazine, Vol. 46, No. 4, pp. 88-95, 2008.
[6] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey, "Secure V2V Communication With Certificate Revocations," IEEE Infocom 2007, Mobile Networking for Vehicular Environments workshop, pp. 127-132, 2007.
[7] J. Haas et al, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," Proc. Sixth ACM international workshop on Vehicular Inter-networking, pp. 89-98, Sept., 2009
[8] M. Raya et al, "Eviction of misbehaving and faulty nodes in vehicular networks," Selected Areas in Communications, IEEE Journal on, Vol. 25, pp. 1557 -1568, Oct. 2007.
[9] B. Bellur, "Certificate Assignment Strategies for a PKI-Based Security Architecture in a Vehicular Network," Proc. IEEE GLOBECOM 2008. pp. 1-6, Nov. 2008.
[10] ETSI TS 123 246(v13.3.0), "Universal Mobile Telecommunications System(UMTS); LTE Multimedia Broadcast/Multicast Service(MBMS); Architecture and functional description," March 2016.
[11] J. S Kim, S. H Kim, "Evolved-MBMS: Mobile IP TV Technology for 3GPP LTE," Information & communications magazine, Vol. 30 No. 2, pp. 66-74, 2013.
[12] https://www.nsnam.org
[13] 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 a 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.