Journal of The Korea Society of Computer and Information
Vol. 22 No. 12, pp. 109-116, December 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.12.109

A Novel Certificate Revocation List Distribution for Vehicle Communications in Mobile Communication Networks

Du Anh Dan*, Hyun-Gon Kim**

Abstract

Short-lived pseudonym certificates as vehicle identities could satisfy both security and privacy requirements. However, to remove revoked certificates especially in vehicle communications, pseudonym certificate revocation list (CRL) should be distributed resource-efficiently from a practical deployment point of view and in a timely manner. In this paper, we propose a novel CRL distribution scheme capable of CRL multicast to only activated vehicles registered to the CRL multicast group using the group communication system enabler, namely, the GCSE which is being standardized. The scheme is resource efficient by using CRL distribution paths instead of paging processes to find out multicast vehicle(s) within a certain region. The analyzed results show that the proposed scheme outperforms in terms of paging cost, packets transmission cost, and the processing cost at the respective entities compared to the existing four schemes in the literature.

▸Keyword: Certificate Revocation List, Multicast, GCSE, GCS-AS, eMBMS

I. Introduction

차량통신에서는 차량의 익명성을 보장하기 위하여 공개키 방식의 단기 익명 인증서(pseudonyms)를 사용한다. 만약 차량이 고장나거나 오작동을 하거나 차량이 해킹을 당했거나 관리적 보안의 이유로 인증서를 취소해야 할 경우에는 인증서 취소목록(CRL; Certificate Revocation List)을 이용한다. CRL은 발급기관에 의해 서명되고 서명 결과 값이 부착되어 배포되며, 이를 수신한 차량들은 서명을 검증하여 성공했을 경우에만 CRL 정보를 신뢰한다. CRL에는 단기 익명 인증서의 체인번호를 넣어, 같은 시기에 생성된 단기 익명 인증서의 셋을 동시에 취소할 수 있다.

비교적 긴 주기를 가지고 CRL을 배포하는 유선과는 다르게, 차량통신에서는 CRL이 짧은 주기로 배포된다. 만약 차량이 어떠한 이유로 최신의 CRL을 수신하지 못하였다면 최근에 취소된 인증서들을 확인할 수 없게 된다. 예를 들어, 기지국(Road Side Unit)이 충분히 설치되지 않은 지역이나, 기지국 전파의 수신이 약한 지역에서는 차량이 최신의 CRL을 수신하기 어려워진다. 최신의 CRL을 수신하지 못하면, 차량은 주변 차량으로부터 수신된 메시지의 인증서와 첨부된 서명 값을 신뢰할 수 없기 때문에, 정상적인 차량으로부터 수신된 메시지인지, 아니면 악의적인 공격 차량으로부터 수신된 메시지인지에 대한 판단이 어려워진다. 만약 취소된 인증서를 가진 악의적인 공격 차량으로부터 수신된 메시지를 받아들이면 거짓 정보를 받아들일 수 있어 보안에 취약해진다. 예를 들어 앞차가 거짓으로 전방에 긴급 충돌했다는 정보를 뒤차에 전달하면 뒤차가 이를 믿고 급작스럽게 정지할 경우 추돌사고로 이어질 수 있다.

한편, 최근에는 차량통신 네트워크와 이동통신 네트워크가 연동되는 다양한 시나리오가 제시되고 있다. 특히, 이동통신 네트워크에서 차량 통신의 베어러를 제공하는 시나리오로서, 차량과 인프라간 통신(V2I)과 차량간 통신(V2)을 기본적으로 제공하고, 차량과 보행자간(V2P)통신도 도입 중에 있다[1]. 일예로, 테슬라 S 모델에서는 이동통신 단말 모듈인 LTE 모듈을 차량에 장착하여 통신에 활용하고 있다.

더불어, 이동통신 네트워크를 이용하여 CRL을 배포하는 기

• First Author: Du Anh Dan, Corresponding Author: Hyun-Gon Kim
*Du Anh Dan (duanhdan@gmail.com), Dept. of Information Security, Mokpo National University
**Hyun-Gon Kim (hyungon@mokpo.ac.kr), Dept. of Information Security, Mokpo National University
• Received: 2017. 10. 16, Revised: 2017. 10. 30, Accepted: 2017. 11. 28.

법들도 연구되고 있다[2~3]. 그러나 이동통신 네트워크를 이용하여 CRL을 배포하는 기법은 고가의 무선 자원을 사용하므로 효율성이 매우 중요해진다. 따라서, CRL을 배포하는데 있어서, 최소한의 유무선 자원을 사용하기 위해 유니캐스트 전송이 효율적인지 아니면 멀티캐스트 전송이 효율적인지에 대해 다양한 측면의 분석이 이루어져야 한다.

본 논문에서는 CRL을 이동통신 네트워크를 통해 배포하는데 있어서 유무선 자원을 효율적으로 사용할 수 있는 멀티캐스트 기법을 제안하고 기존 기법들과 성능을 비교 분석하였다. 제안한 기법은 기존에 활성화된 멀티캐스트 차량을 파악하기 위해 필요한 페이징 절차를 제거하고, 멀티캐스트 그룹의 차량이 있는 셀 단위로 CRL 배포 경로를 만들고, 멀티캐스트 차량들에게만 CRL을 배포하므로써 유무선 자원을 효율적으로 사용할 수 있다.

본 논문은 다음과 같이 구성된다. 서론에 이어 2장에서는 이동통신 네트워크를 이용해 CRL을 배포하는 기존 연구들과 eMBMS(evolved Multimedia Broadcast Multicast Services)를 간략히 소개한다. 3장에서는 본 연구에서 제안한 멀티캐스트 기반의 효율적인 CRL 배포 기법을 설계하였다. 4장에서는 제안한 기법과 기존의 CRL 배포 기법들의 비용을 비교분석하고, 5장에서 결론을 맺는다.

II. Related Works

1. CRL Distribution over UMTS

차량통신을 지원하기 위해 이동통신 표준화가 추진되고 있으며, 2017년 3월에 V2X 표준(R.14)이 완성되었다[1]. V2X는 기본적으로 차량과 다른 차량, 보행자, 도로 통신망 및 이동통신 네트워크와 통신하여 주행의 안전성과 효율성을 높이기 위한 기술이다. V2X는 좁은 의미로는 차량통신을 위해 LTE 네트워크를 활용하는 것이며, 넓은 의미로는 전송속도가 빠른 LTE 네트워크와 연동하여 다양하고 새로운 서비스를 창출하는 것이다.

한편, 차량통신에서 사용할 수 있는 지역별(regional) CRL을 이동통신 네트워크를 통해 배포하는 기법이 제안되었다[2]. Full CRL을 지역별 CRL로 만들고, 지역을 구성하는데 있어서 이동통신의 위치등록 기법을 이용하여 차량의 위치를 실시간으로 추적·관리하고, 그 지역에 위치한 차량들에게만 해당 지역별 CRL을 전달한다. 지역별 CRL 배포에 적합하나, point-to-point 통신을 하기 때문에 유무선 자원을 비효율적으로 사용하고, 모든 차량의 위치를 실시간으로 파악하기 위해 네트워크 측의 처리 부담이 있으며, 이동통신 시스템의 기능들을 많이 변경해야 된다는 단점이 있다.

지역별 CRL을 eMBMS를 이용해 CRL을 멀티캐스트 형태로 전송하는 기법도 제안되었다[3]. 멀티캐스트를 이용하여 유무선 자원을 효율적으로 사용하나, 활성화된 멀티캐스트 차량을 파악하기 위해 페이징을 수행해야 하고, 단위 셀내에 차량이 밀집될 경우에는 차량 수에 비례하여 유무선 자원이 집중적으로 사용된다는 단점이 있다. 또한, 이동통신 네트워크의 여러 엔티티들이 추가적인 기능을 제공해야 하고, 여러 엔티티들이 멀티캐스트 그룹 관리 등을 수행해야 하는 처리 부담이 있다.

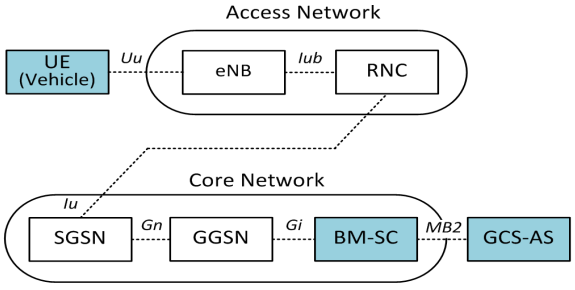
2. eMBMS

eMBMS는 이동통신 네트워크를 통해 동일한 데이터를 다수의 단말에게 동시에 point-to-multipoint로 전송하는 기술이다[4~5]. 특히, eMBMS의 MBSFN(Multimedia Broadcast multicast service over Single Frequency Network)은 다수의 기지국에서 같은 패킷을 같은 시간에 전송하는 브로트캐스트 전송 방식인 멀티 셀 전송방식을 이용하여 물리계층에서 다이버시티 이득을 얻어 전송효율을 최대화시킨다. 이 기술은 인접한 여러 셀에 걸쳐, 동시에 같은 멀티캐스트나 브로드캐스트 데이터를 더 효율적으로 전송할 수 있다. 그리고 본 논문에서 활용하고자하는 eMBMS Counting 기술은 네트워크측에서 단위 영역내에 eMBMS 서비스를 수신하는 활성화된 단말의 수를 파악하는데 사용된다[6].

한편, eMBMS에서는 패킷을 수신할 멀티캐스트 단말을 찾기 위해 제어국 단위의 페이징을 수행한다[4]. 페이징은 해당 제어국이 관할하는 모든 단말에 대해 이루어지므로, 단말로부터 페이징 응답을 받는데 지연이 생긴다. 만약 페이징을 하지 않고, 활성화된 멀티캐스트 단말들만을 미리 파악할 수 있다면 페이징으로 인한 지연을 없앨 수 있다.

3. Multicast Communications over UMTS

최근 이동통신 네트워크에서 그룹통신 기술인 GCSE(Group Communication System Enabler)에 대한 표준이 진행되고 있다[7]. GCSE는 이동통신 인프라에서 eMBMS를 활용하여 일정한 지역 안에 다수의 사람들에게 그룹 통신 내용을 전달해주는 기술이다. GCSE는 다양한 멀티캐스트 응용을 제공할 수 있는 틀을 제공하며, 대표적인 응용으로는 LTE 기반의 공공 안전 서비스를 들 수 있다[8]. 아래 Fig. 1에 GCSE를 반영한 UMTS 네트워크 참조 모델을 나타내었다.



eNB : evolved Node B
RNC : Radio Network Controller
SGSN : Serving GPRS Support Node
GGSN : Gateway GPRS Support Node
BM-SC : Broadcast Multicast Service Center
GCS-AS : Group Communication Service Application Server

Fig. 1. Network Reference Model of UMTS

GCS-AS는 이동통신 네트워크가 아닌 외부의 그룹통신 응용 서버이며, 특정 그룹에게 전송할 데이터와 그 데이터를 유니

케스트로 보낼지 아니면 멀티캐스트로 보낼지를 결정하고, 전송할 데이터의 지역정보 등을 이동통신 네트워크에게 전달하여 전송을 요청한다. BM-SC는 GCS-AS가 요청한 지역에 대해 멀티캐스트 베어러를 설정하고 eMBMS 세션을 설정하고 해제하는 역할을 한다. 본 논문에서는 GCS-AS를 CRL을 멀티캐스트로 차량들에게 배포하는 응용서버로 활용한다. 지역별로 서로 다른 지역별 CRL을 그 지역의 차량들에게 배포하기에 적합하다는 점에 착안한 것이다.

III. The Proposed Scheme

1. Design Principles

제안한 기법은 기존에 활성화된 멀티캐스트 차량을 파악하기 위해 필요한 페이징 절차를 제거하고, 멀티캐스트 그룹의 차량이 있는 셀 단위로 CRL 배포 경로를 만들고, 멀티캐스트 차량들에게만 CRL을 배포하므로써 유무선 자원을 효율적으로 사용한다.

이를 위해 첫째, 멀티캐스트 전송을 위해 eMBMS를 그대로 이용한다. 둘째, 멀티캐스트 차량의 위치를 파악하는데 필요한 페이징 절차를 제거한다. 대신에 활성화된 멀티캐스트 차량이 있는 셀 단위 또는 MBSFN 영역 단위의 CRL 배포 경로만을 파악하여 관리한다. 즉, CRL을 배포할 때, 페이징을 하는 대신에 미리 설정된 CRL 배포 경로로만 CRL 데이터를 전송하는 것이다. 셋째, 활성화된 멀티캐스트 차량이나 해당 영역을 파악하기 위해서 MBMS Counting 기법을 이용한다. 넷째, 멀티캐스트 그룹의 차량이 속한 셀 내에서는 CRL을 브로드캐스트 하여 무선자원을 효율적으로 사용한다. 다섯째, 이동통신 네트워크의 여러 엔티티들이 수행하는 멀티캐스트 그룹의 멤버 관리 기능을 외부 GCS-AS가 수행하도록 분리한다. 여섯째, CRL 배포 주기 사이에 wake-up 하는 멀티캐스트 차량이 최신의 CRL을 수신하지 못함으로 인해 보안이 취약해지는 점을 고려하여, 해당 차량에게 유니캐스트 형태로 CRL을 재전송한다. 일곱째, 이동통신 네트워크의 중간 엔티티들이 추가해야 할 기능들을 최소화 한다. 구체적인 실현 방안은 다음과 같다.

□ GCS-AS가 CRL 배포하는 응용서버 역할을 하며, CRL을 수신하고자 하는 차량들만을 멀티캐스트 그룹으로 관리한다.

□ CRL은 모든 셀에 배포하는 것이 아니라. 활성화된 멀티캐스트 차량이 속한 셀 또는 MBSFN 영역만 배포한다.

□ CRL은 외부의 GCS-AS에서 eNB까지는 멀티캐스트로 전달되고, eNB에서 차량까지는 브로드캐스트로 전달된다.

□ 모든 차량을 추적하지 않고, 활성화된 멀티캐스트 차량들만을 서빙하는 셀 또는 MBSFN 영역 단위의 추적을 하여 처리의 효율성을 기한다.

□ 활성화된 멀티캐스트 차량을 추적하기 위해 MBMS Counting 기법을 이용한다[5]. RNC가 eNB에게 일정한 주기로 MBMS Counting Request 메시지를 보내고 응답을 받아, 활성화된 멀티캐스트 차량이 속한 셀 또는 MBSFN 영역을 파악하여 GCS-AS로 전송한다.

□ GCS-AS는 이를 기준으로 CRL 배포 경로를 만든다. CRL 배포 경로란 외부의 GCS-AS에서부터 셀 또는 MBSFN 영역까지의 데이터 전송 경로를 말한다. 따라서 멀티캐스트 차량이 없는 셀의 경우에는 이 경로에 포함되지 않는다.

□ CRL 배포 경로는 일정한 주기로 업데이트 한다. 예를 들어 차량통신에서 정의한 CRL 배포 주기를 고려하여 CRL 배포 경로를 업데이트 하는 것도 한 가지 방법이다.

□ CRL 배포 주기 사이에 차량이 idle 상태에서 wake up하게 되면 이전에 수신한 CRL을 사용하여 보안에 취약해질 수 있다. 이를 위해 RNC는 최신의 CRL을 캐싱하고 있다가, 단말이 PMM-idle 상태에서 PMM-connected 상태로 전환될 때, 캐싱된 최신의 CRL을 해당 단말에게 유니캐스트 형태로 전달한다.

2. Functional Requirements

제안한 기법을 구현하기 위해 이동통신 네트워크의 각 엔티티들이 수행해야 할 주요 기능을 설계하였다. 기본적으로 각 엔티티들은 기존의 eMBMS 기능을 동일하게 수행하며, 추가적으로 아래의 기능들을 수행해야 한다.

□ GCS-AS
- 차량통신 네트워크의 CRL 배포 엔티티와 인터페이스
- 멀티캐스트 베어러 설정 요청 및 관리
- CRL을 수신하고자 하는 차량들을 멀티캐스트 그룹으로 구성하고 멤버십 관리
- RNC로부터 수신한 멀티케스트 차량이 속한 셀 또는 MBSFN 정보를 기반으로 CRL 배포 경로 관리
- 각 지역별 CRL을 셀 또는 MBSFN 영역으로 매핑
- CRL을 배포하고 최신의 CRL은 캐싱

□ BM-SC, GGSN, SGSN
- 기존의 eMBMS 기능을 transparent하게 수행
- 제안한 기법의 시그널링

□ RNC
- eNB에게 일정한 주기로 MBMS Counting Request 메시지를 보내고 응답을 받아, 활성화된 멀티캐스트 차량이 속한 셀 또는 MBSFN 영역을 파악하여 GCS-AS로 전달
- 최신의 CRL을 캐싱하고, 만약 캐싱하고 있지 않은 상태에서 멀티캐스트 차량으로부터 요청이 오면 GCS-AS로부터 받아 차량에게 재전송

□ eNB
- CRL 브로드캐스트

3. Protocol Design

3.1 Initial Operation

차량이 CRL을 수신하기 위해서는 초기에 멀티캐스트 베어

러를 설정하고 사용자를 등록하는 단계이다. 1) CRL을 멀티캐스트 형태로 전달하기 위해 eMBMS 베어러를 설정한다. GCS-AS가 멀티캐스트 베어러 설정을 요청하면 BM-SC, GGNS, SGSN, RNC를 거쳐 멀티캐스트 베어러가 설정된다. 2) 차량의 응용과 GCS-AS간에 멀티캐스트 그룹 세션을 설정한다. 3) GCS-AS는 CRL을 수신하고자 하는 차량들을 멀티캐스트 그룹으로 구성하고, 그룹의 멤버십을 관리한다.

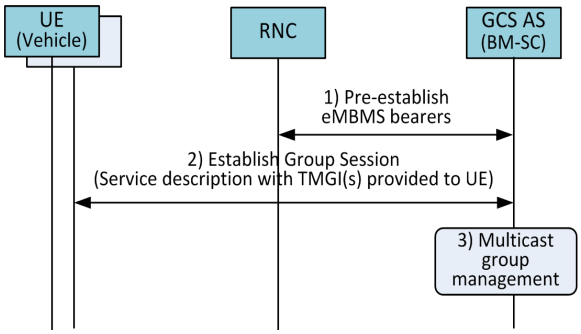


Fig. 2. Initial Operation

3.2 CRL Distribution Path Management

일정한 주기로 CRL 배포 경로를 관리하는 단계이다. 1) RNC는 일정한 주기로 MBMS Counting을 시작한다. 2) RNC가 MBMS Counting Request 메시지를 eNB에게 송신한다. 3) 셀 내에 속하고, 현재 활성화된 멀티캐스트 차량은 MBMS Counting Response 메시지로 응답한다. 4) 이를 수신한 RNC는 메시지에 포함된 셀 또는 MBSFN 영역을 파악한다. 5) RNC는 이 정보를 GCS-AS에게 전송한다. 6) GCS-AS는 이 정보를 기준으로 현재 활성화된 멀티캐스트 차량이 속한 eNB의 경로를 즉, CRL 배포 경로를 업데이트한다.

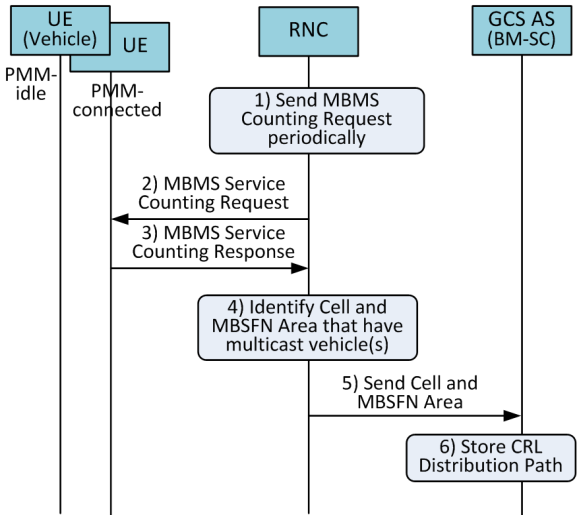


Fig. 3. CRL Distribution Path Management

3.3 CRL Distribution

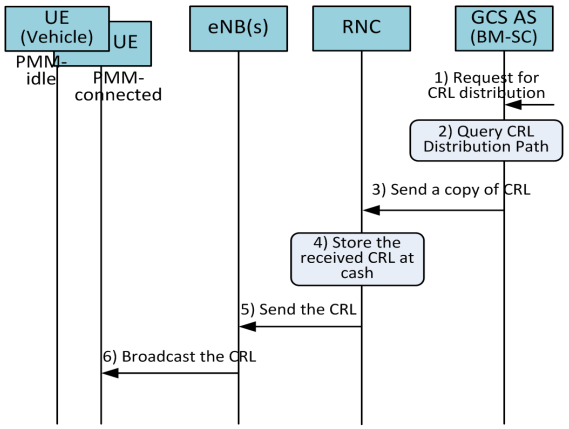


Fig. 4. CRL Distribution

차량통신 네트워크로 CRL 배포를 요청받고, 수신한 CRL을 멀티캐스트 차량들에게 배포하는 단계이다. 1) 차량통신 네트워크로부터 CRL 배포 요청을 받는다. 2) GCS-AS는 CRL 배포 경로를 조회한다. 3) GCS-AS는 CRL을 배포 경로에 있는 RNC에게 전달한다. 4) RNC는 수신한 CRL을 캐싱해 둔다. 5) RNC가 eNB에게 CRL을 전송한다. 6) 이를 수신한 eNB는 자신의 셀을 대상으로 CRL을 브로드캐스트 한다. CRL은 PMM-connected 상태인 차량들만 수신하고, PMM-idle 상태인 차량은 별도로 wake-up 시키지 않는다.

3.4 CRL Re-distribution

CRL을 배포하는 시점에 활성화되지 않았던 멀티캐스트 차량 즉, PMM-idle 상태의 멀티캐스트 차량은 CRL을 수신하지 못할 것이다. 이처럼 CRL 배포 주기 사이에 차량이 wake-up 하였다면 그 차량은 최신의 CRL을 보유하고 있지 않아 보안에 취약해지게 된다. RNC가 자신의 영역에 멀티캐스트 차량이 있는 경우에는 RNC가 최신의 CRL을 캐싱하고 있을 것이다. 따라서 RNC가 그 차량에게 CRL을 유니캐스트 형태로 재전송한다.

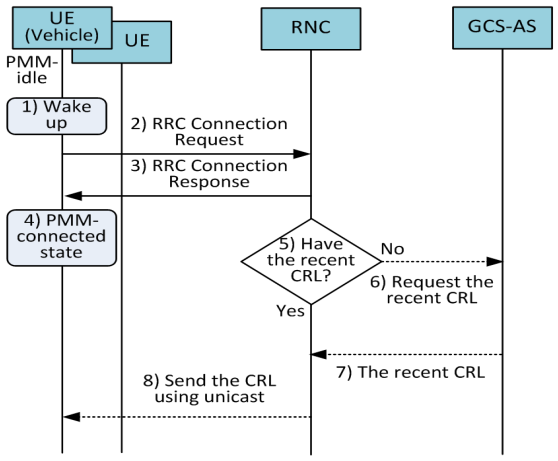


Fig. 5. CRL Redistribution for UE Wake-up

1) 멀티캐스트 서비스를 받는 차량이 Wake-up 한다. 2) 차량은 통신을 위해 RRC Connection Request 메시지를 RNC에

게 전송하여 베어러 설정을 요청한다. 3) RNC는 베어러를 설정한 후에 RRC Connection Response 메시지로 응답한다. 4) 차량은 PMM-connected 상태로 전환된다. 5) RNC는 자신이 CRL을 캐싱하고 있는지 체크한다. 6) 만약, RNC가 이전에 CRL 배포 경로에 속하지 않아 즉, 해당 RNC 영역에 이전에 멀티캐스트 서비스를 받는 차량이 없었다면 RNC도 최신의 CRL을 캐싱하고 있지 않을 것이다. 이를 위해 RNC는 GCS-AS에게 최신의 CRL을 요청한다. 7) GCS-AS는 RNC에게 최신의 CRL을 전달한다. 8) wake-up한 해당 차량에게 CRL을 유니캐스트 형태로 재전송한다.

IV. Cost Analysis

제안한 기법의 효용성을 판단하기 위해 멀티캐스트를 차량에게 CRL 배포하는데 소요되는 비용을 분석하고, 기존 기법들과 상대적인 비교를 하였다. 기존의 기법들과 비교를 위해서 참고문헌[9~10]의 비용분석 방법과 파라미터 그리고 수식을 참고하여 제안한 기법의 비용분석에 필요한 수식을 도출하였다.

1. Basic Cost Analysis Parameters

UMTS 네트워크에서 전송 비용과 처리 비용을 구하기 위해 필요한 파라미터를 Table 1과 Table 2에 나타내었다. 라우팅 영역의 전체 갯수(N_{RA})는 하나의 GGSN에 연결된 SGSN의 수($N_{S/G}$)와 하나의 SGSN에 연결된 RA의 수($N_{R/S}$)와의 곱이다. RNC의 전체 수(N_{RNC})는 N_{RA}와 하나의 라우팅 영역에 연결된 RNC의 수($N_{R/R}$)와의 곱이다. URA(UTRAN 등록 영역)의 전체 수(N_{URA})는 N_{RNC}와 하나의 RNC에 연결된 URA의 수($N_{U/R}$)와의 곱이다. eNB의 전체 수(N_B)는 N_{URA}와 하나의 URA에 연결된 eNB의 수와의 곱이다.

□ $N_{RA} = N_{S/G} \circ N_{R/S}$

□ $N_{RNC} = N_{S/G} \circ N_{R/S} \circ N_{R/R}$

□ $N_{URA} = N_{S/G} \circ N_{R/S} \circ N_{R/R} \circ N_{U/R}$

□ $N_B = N_{S/G} \circ N_{R/S} \circ N_{R/R} \circ N_{U/R} \circ N_{B/U}$

Table 1. Performance Analysis Parameters

Unit Transmission Costs					
h_{gs}	h_{sr}	h_{rb}	h_{bu}		
0.2	0.2	0.5	5		
Unit Processing Costs					
c_g	c_s	c_r	c_b		
0.5	0.5	0.75	1		
Weight Factors					
w_{dt}	w_{st}	w_{dp}	w_{sp}	w_t	w_p
0.6	0.2	0.1	0.1	1	1
Network Configuration Parameters					
$N_{S/G}$	$N_{R/S}$	$N_{R/R}$	$N_{U/R}$	$N_{B/U}$	
10	10	10	5	5	

Table 2. Cost Analysis Parameters

D_{gs}	Trans. cost of packet delivery between GGSN and SGSN
D_{sr}	Trans. cost of packet delivery between SGSN and RNC
D_{rb}	Trans. cost of packet delivery between RNC and Node B
D_{bu}	Trans. cost of packet delivery over the aire interface
S_{sr}	Trans. cost of paging between SGSN and RNC
S_{rb}	Trans. cost of paging between RNC and Node B
S_{bu}	Transmission cost of paging over the air interface
p_g	Processing cost of packet delivery at GGSN
p_s	Processing cost of packet delivery at SGSN
p_r	Processing cost of packet delivery at RNC
p_b	Processing cost of packet delivery at Node B
a_s	Processing cost of paging at SGSN
a_r	Processing cost of paging at RNC
a_b	Processing cost of paging at Node B

l_{gs}는 GGSN과 SGSN 사이의 평균 거리이고 l_{sr}은 SGSN과 RNC 사이의 평균 거리로 홉(hop) 수로 나타낸다. RNC와 eNB 사이는 1 홉으로 그리고 eNB와 차량 간에도 1 홉으로 가정하여 $l_{rb}=1$, 그리고 $l_{bu}=1$로 둔다. $h(\circ)$는 두 노드 사이의 링크상에 소요되는 단위 전송 비용이고, 패킷 전송을 위한 전송 비용 가중치(w_{dt})와 페이징 전송을 위한 전송 비용 가중치(w_{st})를 둔다. 그리고 분석의 용이성과 객관성을 고려해서, 전송 비용에 적용하는 전체 가중치(w_t)와 처리 비용에 적용하는 전체 가중치(w_p)를 둔다. 유선 링크에서의 패킷 전송 비용은 아래와 같다.

$$D(\circ) = w_t\, w_{dt}\, l(\circ)\, h(\circ)$$

위 식을 기준으로 하면 무선 링크의 전송 비용은 $l_{bu}=1$이므로 $D_{bu} = w_t w_{dt} h_{bu}$이다. 한편, GGSN, SGSN, RNC, eNB 등에서 소요되는 단위 처리 비용은 $c(\circ)$로 둔다. 패킷 전송과 유사하게, 패킷 전송을 위한 처리 비용에 가중치(w_{dp})와 페이징 전송을 위한 처리 비용에 가중치(w_{sp})를 둔다. 각 노드에서 데이터 트래픽을 위한 처리 비용과 페이징을 위한 처리 비용은 아래와 같이 각각 표현할 수 있다.

$$p(\circ) = w_p\, w_{dp}\, c(\circ)$$

$$a(\circ) = w_p\, w_{sp}\, c(\circ)$$

차량이 활성화 상태인지 휴지 상태인지를 반영하기 위해, 멀티캐스트를 이용하는 UE가 항상 네트워크에 연결될 수 있는 PMM-connected 상태와 PMM-idle 상태로 구분한다. 차량이 PMM-idle 상태에 들어갈 확률을 P_{RA}, 차량이 해당 셀에서 RNC에 의해 추적될 수 있는 확률을 P_{URA}, 차량이 URA 레벨에서 추적될 수 있는 확률을 P_{cell}이라 둔다. 따라서 차량이 PMM-connected 상태로 들어갈 확률은 $1-P_{RA} = P_{URA} + P_{cell}$이다. 그리고 데이터 세션 arrival rate은 λ_s로, 그리고 데이터 세션의 패킷 수를 N_p로 둔다.

2. Modeling of Multicast Vehicle Distribution

멀티캐스트 그룹의 활성화된 차량의 분포는 참고문헌 [9]를

참조하였다. 라우팅 영역(RA)의 전체 수를 다수의 l_{RA}로 구성한다. $1 < i < l_{RA}$의 경우에 클래스 i에 대한 RA의 수는 $N_i^{(RA)}$이다. 즉, $N_{RA} = \sum_{i=1}^{l_{RA}} = N_i^{(RA)}$ 이다. 따라서 멀티캐스트 차량을 가진 RA의 전체 수는 아래와 같이 표현할 수 있다. 여기서 $N_i^{(RA)}$는 클래스 i의 $N_i^{(RA)}$에 대해서 멀티캐스트 차량을 나타낸다.

$$n_{RA} = \sum_{i=1}^{l_{RA}} (1 - e^{-\theta_i^{(RA)}}) \circ N_i^{(RA)}$$

만약, 멀티캐스트 차량을 가진 n_{RA}개의 RA들이 있을 때, 하나의 SGSN이 멀티캐스트 차량을 가지지 않을 확률은 아래와 같다.

$$P_{S/G} = \begin{cases} \dfrac{(\dfrac{N_{RA} - N_{R/S}}{n_{RA}})}{(\dfrac{N_{RA}}{n_{RA}})} & \text{if } n_{RA} \le N_{RA} - N_{R/S} \\ 0 & otherwise \end{cases}$$

위 식을 토대로 멀티캐스트 서비스를 제공하는 SGSN의 전체 수 $n_{S/G} = N_{SG} \circ (1 - P_{S/G})$ 이다. 따라서 네트워크 내에 멀티캐스트 차량의 전체 수는 아래와 같다.

$$N_m = \sum_{i=0}^{l_{RA}} N_i^{(RA)} \ \theta_i$$

3. Cost Analysis for the Proposed Scheme

제안한 기법에서 특정 클래스 i에 속한 RA의 영역내에 있는 모든 RNC는 RA와 같이, 동일한 멀티캐스트 사용자 분포를 가진다고 가정한다. 하나의 RA내에는 균일밀도 분포(uniform density distribution)를 가진다고 했을 때, 클래스 i에 속하는 RA의 영역내에서 하나의 RNC의 멀티캐스트 분포는 아래와 같다.

$$\theta_i^{(RNC)} = \frac{\theta_i^{(RA)}}{N_{R/R}}$$

클래스 i에 속하는 RNC의 전체 수는 아래와 같다.

$N_i^{(RNC)} = N_i^{(RA)} \circ N_{R/R}$

$l_{RNC} = l_{RA}$로 두면, 멀티캐스트 사용자를 가진 RNC의 전체 수는 아래와 같다.

$$n_{RNC} = \sum_{i=1}^{l_{RNC}} (1 - e^{-\theta_i^{(RNC)}}) \circ N_i^{(RNC)}$$

이를 하나의 RNC의 영역내에 셀들에 동일하게 적용해보면 아래와 같다.

$$\theta_i^{(B)} = \frac{\theta_i^{(RNC)}}{N_{U/R} \circ N_{B/U}}$$

클래스 i에 속하는 eNB의 수는 아래와 같다.

$N_i^{(B)} = N_i^{(RNC)} \circ N_{U/R} \circ N_{B/U}$

$l_B = l_{RNC}$로 두면, 멀티캐스트 사용자를 가진 eNB의 전체 수는 아래와 같다.

$$n_B = \sum_{i=1}^{l_B} (1 - e^{-\theta_i^{(B)}}) \circ N_i^{(B)}$$

RNC가 하나의 멀티캐스트 패킷을 복사해서 멀티캐스트 차량들을 가진 모든 eNB에게 포워딩한다고 가정한다. eNB는 셀 상에서 CRL을 브로드캐스팅한다. 제안한 기법의 전체 비용은 아래와 같다.

$$D_{proposed} = [p_g + n_{S/G} \circ (D_{gs} + p_s) + n_{RNC} \circ (D_{sr} + p_r) + n_B \circ (D_{rb} + p_b + D_{bu})] \circ N_p \circ \lambda_s$$

4. Comparison of the Proposed Scheme with the Existing Schemes

비교분석을 위해 참고문헌 [9]에서 정의한 4개의 기법과 본 논문에서 제안한 기법의 비용을 상대적으로 비교하였다. 기법 I은 멀티캐스트 패킷을 차량에게 point-to-point로 전송한다. 기법 II는 멀티플 전송으로 멀티캐스트 그룹에 등록한 차량에게만 전송한다. 멀티캐스트 패킷을 복사하고, 멀티플 유니캐스트 터널을 설정한 다음에 패킷을 전송한다. 기법 III은 멀티캐스트 패킷을 멀티캐스트 사용자가 있는 특정 영역으로만 브로드캐스팅한다. 기법 IV는 네트워크 내에 있는 중간 노드들이 멀티캐스트 그룹을 관리하고, Fig. 1의 Gn과 Iu 인터페이스에 멀티캐스트 터널을 설정하여 사용한다. 본 논문에서 제안한 기법을 기법 V라 하였다.

이전 절에서 분석한 페이징 비용, 패킷 전송 비용과 각 노드들에서의 프로세싱 비용을 합하여 전체 비용으로 나타내었다. 참고문헌 [9]와 동일하게 l_{gs}=15, l_{sr}=10, l_{rb}=1, P_{RA}=0.7, P_{URA}=0.2, P_{cell}=0.1, λ_s=5로 두었다. RA는 2개의 클래스로 구분된다. 멀티캐스트 사용자의 분포가 $\theta_1 = 1/\delta$을 가진 RA가 클래스 1(i=1)이고, $\theta_2 = \delta$를 가진 RA가 클래스 2(i=2)이다. 만약 $\delta \gg 1$이면 클래스 1 RA는 멀티캐스트 사용자의 분포가 적어지고, 반대로 클래스 2 RA는 멀티캐스트 사용자의 분포가 커진다. 여기서 클래스 1 RA의 멀티캐스트 사용자 분포를 α로 두면 클래스 2 RA의 분포는 $1-\alpha$가 된다. 각 클래스들의 RA는 결국 $N_{R/R}$개의 RNC로 나누어지며, 각 클래스의 RNC는 다시 $N_{U/R} \circ N_{B/U}$로 나누어진다. 네트워크 토폴로지는 2개를 고려하였다. 토폴로지 I은 $N_{S/G}$=10, $N_{R/S}$=10, $N_{R/R}$=10, $N_{U/R}$=5, $N_{B/U}$=5이고, 토폴로지 II는 $N_{S/G}$=20, $N_{R/S}$=20, $N_{R/R}$=20, $N_{U/R}$=10, $N_{B/U}$=10이다.

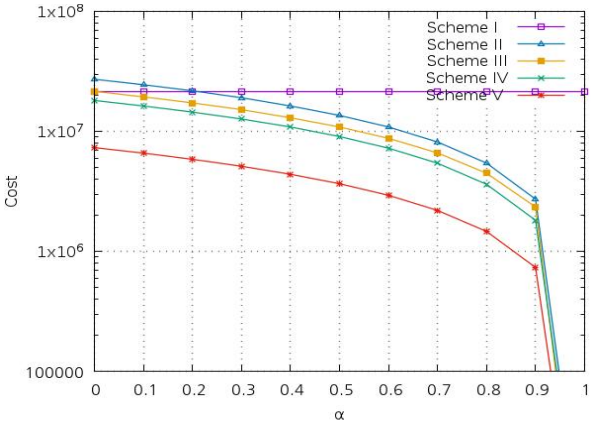


Fig. 6. Total cost of multicast packet delivery against α for topology I, with δ=100, N_p=50

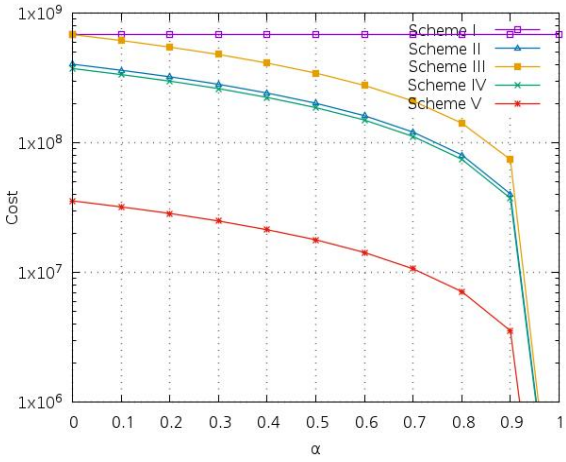


Fig. 7. Total cost of multicast packet delivery against α for topology I, with δ=100, N_p=5,000

Fig. 6과 Fig. 7은 네트워크 토폴로지 I에서 α의 변화에 따른 각 기법들의 비용을 나타내었다. 기법 I의 비용은 상수로 나타나고, 나머지 4개의 기법은 α가 증가함에 따라 비용이 줄어드는 것을 볼 수 있다. α가 증가한다는 의미는 클래스 1 RA의 멀티캐스트 사용자가 증가하고, 클래스 2 RA의 멀티캐스트 사용자는 감소한다는 뜻이다. Fig 6은 N_p 즉, 데이터 세션의 패킷의 수를 50으로 두었을 때의 결과이다. 기법 II, 기법 III, 기법 IV는 유사한 비용이 나타났으나 제안한 기법 V의 비용이 가장 낮게 나타났다. Fig 7은 N_p 즉, 데이터 세션의 패킷의 수를 5,000으로 두었을 때의 결과이다. 마찬가지로 기법 II와 기법 III가 유사한 비용을 나타내었으며, 제안한 기법 V의 비용이 가장 낮게 나타났다. N_p가 50에서 5,000으로 커지면 즉, 패킷의 수가 증가하면 제안한 기법 V는 기존 기법들에 비해 비용이 상대적으로 더 낮아진다. 즉, CRL 데이터의 용량이 커질수록 제안한 기법의 효용성이 높아지는 것이다.

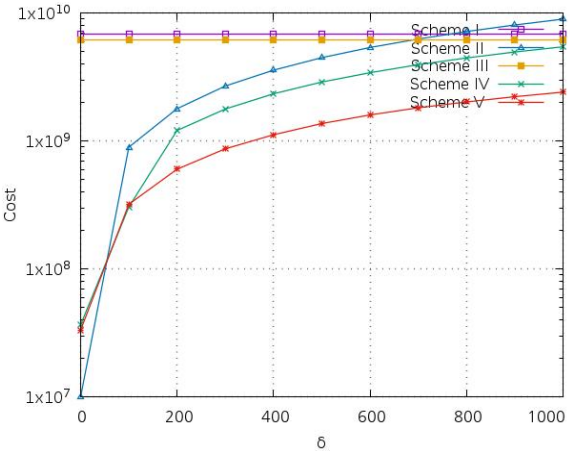


Fig. 8. Total cost of multicast packet delivery against δ for topology II, with N_p=500, α=0.1

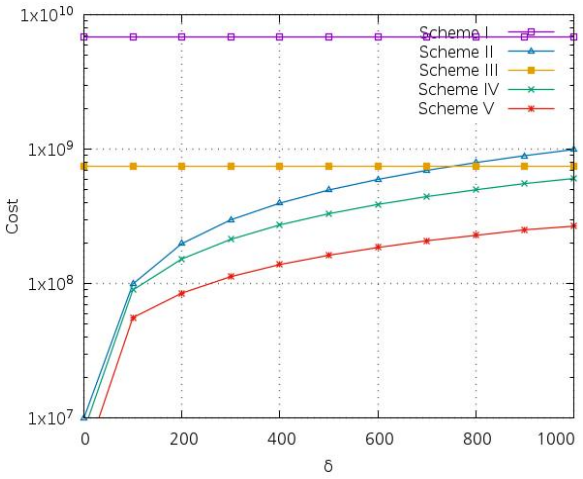


Fig. 9. Total cost of multicast packet delivery against δ for topology II, with N_p=500, α=0.9

Fig. 8과 Fig. 9는 네트워크 토폴로지 II에서 δ의 변화에 따른 각 기법들의 비용을 나타내었다. 기법 I과 기법 III의 비용은 상수로 나타났으며, 제안한 기법 V의 비용이 가장 낮게 나타났다.

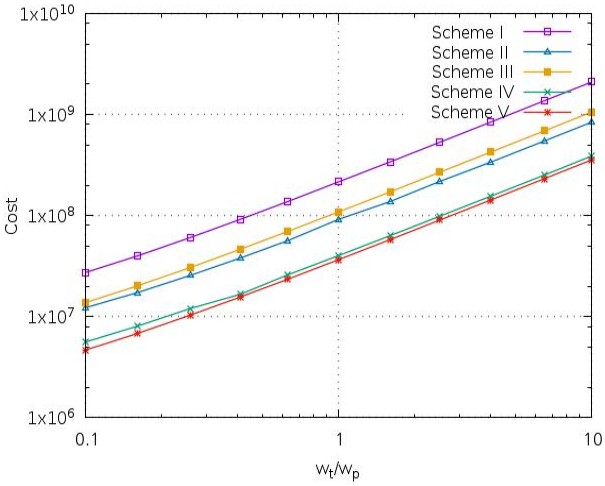


Fig. 10. Total cost of multicast packet delivery against w_t/w_p for topology I, with α=0.5, δ=100, N_p=500

Fig. 10과 Fig. 11은 네트워크 토폴로지 I에서 w_t/w_p와 w_{dt}/w_{st} 비율을 0.1에서 10까지 변화시켰을 때, 각 기법들의 비용을 나타내었다. 5가지 기법들이 모두 w_t/w_p와 w_{dt}/w_{st} 비율이 증가함에 따라 로그 스케일로 비용이 증가되는 것을 볼 수 있으며, 기법 IV와 제안한 기법 V의 비용이 동일하게 나타났다.

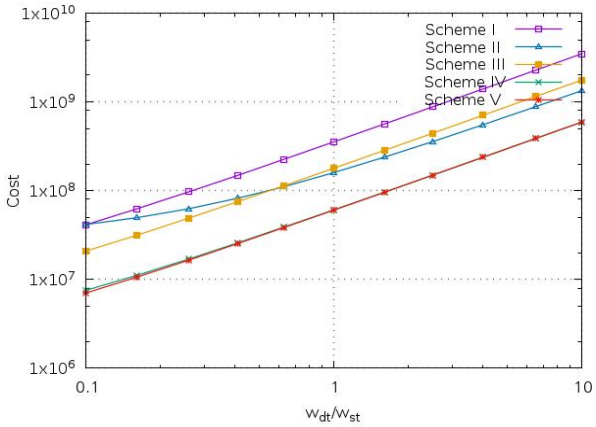


Fig. 11. Total cost of multicast packet delivery against w_{dt}/w_{st} for topology I, with α=0.5, δ=100, N_p=500

V. Conclusions

본 논문에서는 CRL을 이동통신 네트워크를 통해 배포하는데 있어서 유무선 자원을 효율적으로 사용할 수 있는 멀티캐스트 기법을 제안하고 기존 기법들과 비용을 비교 분석하였다. 제안한 기법은 기존에 활성화된 멀티캐스트 차량을 파악하기 위해 필요한 페이징 절차를 제거하고, 대신 멀티캐스트 그룹의 차량이 있는 셀 단위로 CRL 배포 경로를 만들고, 멀티캐스트 차량들에게만 CRL을 배포하므로써 유무선 자원을 효율적으로 사용함을 알 수 있었다.

제안한 기법을 구현하기 위해, 이동통신 네트워크의 각 엔티티들이 수행해야 할 주요 기능들과 프로토콜을 설계하였다. 그리고 효용성을 비교하기 위해 기존의 기법들과 페이징 비용, 패킷 전송 비용, 각 엔티티들의 프로세싱 비용 분석을 통해 전체 성능을 비교하였다. 분석 결과, 제안한 기법은 멀티캐스트 차량의 수가 많을수록 그리고 CRL 데이터의 사이즈가 커질수록 비용이 낮아져 효과적임을 알 수 있었다. 제안한 기법의 단점으로는 일정한 주기로 CRL 배포 경로를 관리해야 한다는 부담이 있다. 그러나 CRL 배포 경로를 파악하는 시점이 CRL을 실제 배포하는 시점과 무관해서 성능에 거의 영향을 주지 않는다.

REFERENCES

[1] 3GPP TR 36.885, "3GPP; Technical Specification Group Radio Access Network; Study on LTE-based V2X Services(R.14)," June 2016.

[2] Hwi Sung Hong etc., "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] HyunGon Kim, "A Certificate Revocation List Distribution Scheme over the eMBMS for Vehicular Networks," Journal of The Korea Society of Computer and Information, Vol. 21, No. 10, pp. 77-83, Oct. 2016.

[4] D. Lecompte etc., "Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: overview and Rel-11 enhancements," IEEE Commun. Mag., vol. 50, pp. 68-74, Nov. 2012.

[5] Robert Rummler etc., "Multicast in Third-Generation Mobile Networks," John Wiley & Sons, Ltd, 2009.

[6] ETSI TS 136 443, "Evolved Universal Terrestrial Radio Access Network(E-UTRAN); M2 Application Protocol (M2AP)(R. 10)," April 2011.

[7] ETSI TS 129 468, "Group Communication System Enablers for LTE(GCSE_LTE); MB2 reference point(R. 14)," April 2017.

[8] Rainer Liebhart etc., "LTE for Public Safety," Willey, March 2015.

[9] Robert Rummler etc., "Modeling and Analysis of an Efficient Multicast Mechanism for UMTS," IEEE Trans. on Vehicular Technology, Vol. 54, No. 1, Jan. 2005.

[10] Antonios Alexiou etc., "Multicast in UMTS: Evaluation and Recommendations," Wireless Communications and Mobile Computing, Vol. 1, pp. 463-481, Oct. 2006.

Authors

Du Anh Dan received the B.S. at the department of Computer Engineering of Hanoi University in Vietnam and he is a M.S. degree candidate at the department of Information Security of Mokpo National University in South Korea. His research interests include security of vehicular communications and security of mobile communications.

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.