JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 7, pp. 93-101, July 2020
https://doi.org/10.9708/jksci.2020.25.07.093

Certificate Revocation Scheme based on the Blockchain for Vehicular Communications

Hyun-Gon Kim*

*Professor, Dept. of Information Security, Mokpo National University, Mokpo, Korea

[Abstract]

Regional CRL(certificate revocation list) in vehicular communications is to partition Full CRL into several small CRLs according to geographic location to keep the size of individual CRLs with smaller. However, since a Regional CRL includes vehicle's revoked certificates within its administrative region, it has to know vehicle' location. For this, how to know vehicle' location effectively corresponding to every region represents a major challenge. This paper proposes a Regional CRL scheme which is envisioned to achieve vehicle's location and to make regional CRLs according to vehicles current location efficiently. The scheme is based on the short-lived pseudonyms defined by WAVE standard. It also acquires issued pseudonyms, vehicle's id and region information whenever a vehicle initiates pseudonyms refill after that, utilizes them to create and distribute the Regional CRL. To keep location privacy-preserving for vehicles, the scheme uses the blockchain technology in the network. The analysis results show that it reduces CRL size and database query time for finding revoked certificates sharply in the vehicle's on-board unit.

▸ **Key words**: Certificate Revocation, Regional CRL, Pseudonyms, Location Privacy, Blockchain

[요 약]

차량통신에서 지역별 CRL은 각 CRL의 사이즈를 최소화하기 위해 Full CRL을 다수의 지역별 CRL로 분할한다. 그러나 지역별 CRL은 해당 영역 내에 있는 차량의 취소된 인증서만을 포함해야 하므로 해당 영역에 있는 차량의 위치를 파악해야 한다. 따라서 분할된 영역에 속한 차량의 위치를 효율적으로 파악하는 것이 매우 중요해진다. 본 논문에서는 차량의 위치를 효율적으로 파악하고 차량의 현재 위치를 기준으로 지역별 CRL을 만드는 기법을 제안하였다. 이 기법은 WAVE 표준에 정의된 단기 익명인증서를 활용하며, 차량이 익명인증서를 리필할 때마다 생성된 단기 인증 익명인증서, 차량 ID, 지역 정보를 수집하고, 이 정보들을 활용하여 지역별 CRL을 생성하고 배포한다. 그리고 네트워크에서 차량의 위치정보를 보호하기 위해서 블록체인 기술을 사용한다. 분석 결과 제안한 기법은 CRL 사이즈를 줄이고, 차량 위치 프라이버시를 보호하며, 차량의 OBU에서 취소된 인증서를 조회하는 시간을 크게 줄일 수 있다.

▸ **주제어**: 인증서 취소, 지역별 CRL, 익명인증서, 위치 프라이버시, 블록체인

• 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: 2020. 06. 11, Revised: 2020. 07. 20, Accepted: 2020. 07. 20.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

국내의 차량통신 표준으로 미국 주도로 제정한 IEEE WAVE(Wireless Access for Vehicle Environment)를 적용할지 아니면, 이동통신 표준화 단체인 3GPP에서 제정한 C-V2X(Cellular Vehicle to everything)를 도입할지에 대한 이슈가 최근에 논의되고 있다[1][2].

WAVE에서는 차량의 익명성을 보장하기 위해 공개키 방식의 단기 익명인증서(pseudonyms)를 사용하며, 짧은 주기로 인증서를 바꿔가면서 사용해 차량의 위치를 추적하기 어렵게 한다. 또한, 네트워크에 배치된 하나의 노드가 가지고 있는 정보만으로 차량의 ID를 특정할 수 없고, 여러 노드가 가지고 있는 정보를 조합해도 차량의 ID를 특정할 수 없도록 설계되었다.

한편, 차량이 고장 나거나 오작동을 하거나 해킹을 당했거나 그 외에 관리적인 사유가 발생하면 해당 차량의 익명인증서는 취소된다. 만약 적시에 취소되지 않는다면 악의적인 공격자가 취소된 인증서를 사용해 가짜 긴급 정보를 주변에 전파하면 이를 수신한 차량은 위험에 빠질 수 있다. 차량통신에서는 익명인증서를 취소하는 방법으로, 불안정한 무선 연결을 고려하여 온라인 인증서 상태 프로토콜(OCSP)을 사용하지 않고, 인증서 취소목록(CRL; Certificate Revocation List)을 사용하며, CRL은 모든 차량에게 주기적으로 배포한다. 그러나 차량통신을 상용화하기 위해서는 CRL 사용에 따른 네트워크 자원의 효율적인 사용과 배치(deployment) 측면에서 아래의 문제들이 고려되어야 한다.

첫째, 차량통신에서 CRL은 유선과 다르게 짧은 주기로 배포되므로 네트워크 자원의 소모가 많고 특히, 고가의 무선자원이 소모되므로 CRL 데이터 사이즈는 최소화되어야 한다. 만약 CRL 사이즈가 커지면, 이에 비례해서 시스템과 차량의 처리 부하가 커지고 통신 지연이 길어진다. 이로 인해 차량은 공격에 취약해진다. 예를 들어, 정상 차량이 공격 차량으로부터 위변조된 공격 메시지를 수신하였다고 하자. 이때, 차량은 어떠한 이유로 공격 차량의 인증서가 포함된 CRL을 적시에 수신하지 못하거나 CRL 처리 지연이 발생할 수 있다. 이 상태에서 공격자의 위변조된 공격 메시지를 수신하면, 메시지의 인증서와 첨부된 서명 값을 신뢰할 수밖에 없으므로 공격자의 위협에 그대로 노출된다.

둘째, CRL의 배포 주기가 최적화되어야 하고 필요한 시점에 적시에 배포되어야 한다. 배포 주기가 짧으면 CRL을 처리하기 위한 네트워크 자원 소모가 커진다. 차량 OBU에서도 처리 부하가 커져서 지연에 민감한 응용(100ms 이내의 지연)이 정상적으로 동작하기 어렵다. 반대로 배포 주기가 길면 배포 주기 사이에 취소된 인증서를 이용한 고의적인 불법 통신이 이루어질 수 있어 보안에 취약해진다. 즉, 배포 주기는 트레이드 오프 관계에 있다. 이상적으로는 인증서가 취소되는 시점에 즉시 CRL을 배포하는 것이다. 그러나 이 경우 네트워크에 참여 차량이 많을수록 이에 비례하여 취소된 인증서가 자주 보고되고 그때마다 CRL을 배포해야 하므로 매우 비효율적이다.

이러한 점들을 고려하여 본 논문에서는 CRL 사이즈를 최소화하고, 인증서 취소가 보고되면 바로 CRL을 만들어 해당 인증서 취소 지역에만 즉시 배포할 수 있는 새로운 Regional CRL 기법을 제안한다. 제안한 기법은 WAVE 표준의 익명인증서를 그대로 사용하며 CRL 관리에 소요되는 네트워크 부하를 최소화한다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련 연구로 인증서 취소 기법과 차량통신에서 블록체인을 도입한 관련 연구를 소개한다. 3장에서는 제안한 Regional CRL 기법을 설계한다. 설계 원칙, 핵심 아이디어, 추가로 노드들이 수행해야 할 기능, 제안한 기법을 완성하기 위한 두 개의 프로토콜을 제시한다. 4장에서는 제안한 기법의 성능을 기존의 기법들과 비교 분석하고 5장에서 결론을 맺는다.

II. Related Works

1. Certificate Revocation Schemes

CRL 사이즈를 줄이기 위한 다양한 기법들이 제안되었다. 표준에서 정의한 Full CRL은 차량통신 네트워크 전체를 대상으로 CRL을 만들고 배포한다. 델타 CRL은 Full CRL의 네트워크 처리 부하를 경감시키고 통신 지연을 줄이기 위해 제안되었다. Full CRL을 시분할하여 배포하며, 이전에 전송한 델타 CRL에서 변경된 부분만을 보내 한번에 송신하는 CRL 사이즈를 줄인다. 블룸필터(Bloom filter)를 이용한 기법은 확률적 데이터 구조를 이용하여 CRL 사이즈를 줄인다.

Full CRL을 배포하는 대신에 지리적(geographic)으로 분할된 Regional CRL을 사용하는 기법도 제안되었다. 그러나 이 기법에서는 차량이 분할된 영역을 빈번히 이동하므로 차량이 현재 어느 영역에 있는지를 파악해야 한다. 그래야만 그 지역 내에서 취소된 인증서만을 묶어 Regional CRL을 만들어 그 지역 내에 배포할 수 있다. 차량의 이동을 고려한 Regional CRL을 적용하는 연구로서,

참고문헌 [3]은 이동통신 네트워크에서 사용하는 차량의 위치정보를 이용한다. 참고문헌 [4]에서는 이동통신의 멀티캐스트 채널을 이용하며, 영역별로 Regional CRL을 관리하고 배포한다.

위의 기존 연구들은 차량의 위치를 기반으로 영역을 구분하기 위해 복잡한 절차나 알고리즘이 요구되나, 본 연구에서는 WAVE의 익명인증서 리필 절차를 기반으로 영역별 차량을 효율적으로 구분하므로 차량의 익명성을 그대로 제공하고 CRL 처리 성능도 향상시킬 수 있다.

2. Blockchain for Vehicular Communications

차량통신에 블록체인을 도입하는 연구 사례가 늘고 있다. 참고문헌 [5]는 차량통신에 블록체인을 적용하여 네트워크 도메인이 서로 다른 환경에서 키를 효율적으로 관리한다. 참고문헌 [6]은 도메인 단위의 Security Manager들을 블록체인으로 연결하고, 배포된 익명인증서를 셔플링하여 재사용한다. 여기서는 채굴을 통해 작업증명을 한다. 참고문헌 [7]은 기지국(RSU)끼리 블록체인으로 연결하고, 블록체인을 통해 차량간 인증을 수행한다. 차량은 처리부하를 줄이기 위해 블록체인 연산은 하지 않으며 인접 RSU와 트랜잭션 데이터를 주고받는다. 참고문헌 [8]은 차량통신에서 발급되는 인증서와 인증서 취소목록을 블록체인에 기록하여 인증서 발급과 취소 정보를 투명하고 공개적으로 관리한다.

III. The Proposed Scheme

1. Design Principles

제안한 기법의 주요 아이디어는 어떤 영역에 차량이 진입하면 그 영역에서 유효한 익명인증서를 리필한다는 사실[9]에 착안하여 각 영역에 속하는 차량의 위치를 파악하고 활용하는 것이다. 이를 위해 익명인증서 리필 단계에서 발급된 익명인증서, 차량 ID, 지역별로 위치한 등록기관(RA; Registration Authority) ID를 획득한 후, 이 정보들을 기초로 Regional CRL을 생성하고 배포하는 데 활용한다.

한편, WAVE에서는 차량의 익명성을 제공하기 위해 차량의 ID를 사용하지 않고 짧은 기간에 유효한 익명인증서를 사용한다. 또한, 네트워크에 배치된 하나의 노드가 가지고 있는 정보만으로 차량의 ID를 특정할 수 없고, 여러 노드가 가지고 있는 정보를 조합해도 차량의 ID를 특정할 수 없도록 설계되었다. 제안한 기법은 위 두 가지 특징이 반영된 WAVE의 네트워크 구조와 기능을 그대로 유지한다. 추가로, 차량의 위치가 저장되는 AA(Accountability Authority) 노드들을 블록체인으로 연결하여 차량의 위치 데이터의 무결성과 기밀성을 제공한다. 그리고 구현의 용이성을 고려하여 기존의 WAVE 시스템과의 인터페이스 수와 인터렉션을 최소화한다.

2. Additional Functions for Nodes

제안한 기법을 완성하기 위해 네트워크 노드들이 추가로 수행해야 할 기능을 설계하였다. WAVE와 동일하게 모든 네트워크 노드는 X.509 기반의 인증서를 이용하여 암·복호화와 전자서명·검증을 수행한다. 그리고 아래의 기능을 추가로 수행한다.

- □ Vehicle: 익명인증서를 처리하며, Full CRL 대신에 Regional CRL을 처리한다. 익명인증서를 리필할 때마다, 익명인증서, 차량 ID, 영역 정보인 RA ID를 PCA와 AA에게 전달한다.
- □ PCA(Pseudonym Certificate Authority): 익명인증서를 생성하고 차량에 배포한 후, 차량으로부터 AA로 익명인증서를 전송하라는 요청을 받으면, 수신한 첫 번째 l_v값을 기준으로 동일 시점에 발행한 익명인증서인 l_v 시리즈를 자신의 DB에서 추출하여 AA에게 전송한다.
- □ AA(Accountability Authority): 교통사고 등으로 인한 책임소재를 판별하기 위해서 익명인증서에 해당하는 차량 ID를 추적한다. 이를 위해 AA는 차량의 익명인증서와 차량의 ID를 매핑하여 저장한다. 차량 ID가 해킹 등으로 노출되어 프라이버시가 침해당하지 않도록 블록체인을 활용한 강건한 보안을 제공한다.
- □ MA(Misbehavior Authority) : 차량에 대한 비정상 행위를 보고 받고, 비정상이라 판단되면 CRLG에게 Regional CRL 생성을 요청한다.
- □ CRLG(CRL Generator) : Regional CRL을 생성하고 최신화하여 배포한다. MA로부터 비정상 행위 차량의 익명인증서를 수신하면 AA에게 질의하여 취소된 익명인증서가 어느 영역에 있는지를 region_id를 통해 알아낸 다음, 이를 기준으로 해당 영역의 Regional CRL을 생성하고 즉시 그 영역에 배포한다.

3. Protocol Design

제안한 기법은 두 단계로 동작하며, 각 단계에서 필요한 필요한 프로토콜을 설계한다. 첫째, 차량이 익명인증서를 리필한 직후에 실행되는 '익명인증서 등록 프로토콜'이다. 이때 익명인증서-차량 ID-RA ID 튜플이 AA에 저장된다. 둘째, 비정상 행위 차량의 익명인증서를 수신하면 실행되

는 '인증서 취소 프로토콜'이다. 이때 Regional CRL을 생성하고 그 영역에 속한 차량들에게 배포한다. Table 1의 기호를 사용하여 두 프로토콜을 설명한다.

Table 1. Notation

Variable	Description
c	$c \leftarrow enc(node_{pk}, m)$ encrypt m using node's public key
m	$m \leftarrow dec(node_{sk}, c)$ decrypt c using node's private key
$sign$	$\sigma \leftarrow sign(node_{sk}, m)$ signing m using node's private key
$verify$	$true/false \leftarrow vefiry(node_{pk}, m, \sigma)$ verifying σ using node's public key
v_perm_id	vehicle's permanent ID
ra_id	Registration Authority(RA) ID
$lv(i,j)$	ith and jth linkage value
$region\_id$	partitioned geographic region ID
$ls_1(i), ls_2(i)$	ith linkage seed 1, 2
la_id_1, la_id_2	Linkage Authority(LA) ID 1, 2

1. 익명인증서 리필 절차가 완료되면, 차량은 수신한 i값, 첫 번째 $lv(i,0)$값, ra_id를 공개키 pca_{pk}로 암호화하여 c_1을 구한다. 그리고 차량의 ID(v_perm_id)와 i값, 첫 번째 $lv(i,0)$값, ra_id를 공개키 aa_{pk}로 암호화하여 c_2를 구한다.
2. 암호화된 c_1을 개인키 v_{sk}로 전자서명하여 σ_1을 구하고, c_2를 개인키 v_{sk}로 전자서명하여 σ_2을 구한다.
3. DB에 저장된 익명인증서를 AA로 전송하라는 메시지(pse_snd_req_to_aa)에 c_1, σ_1, 공개키 v_{pk}를 포함시켜 PCA에게 전송한다.
4. AA에게 차량의 ID-익명인증서-ra_id 튜플을 저장하라는 메시지(aa_tuple_sto_req)에 c_2, σ_2, 공개키 v_{pk}를 포함시켜 AA에게 전송한다.
5. PCA는 수신한 σ_1를 공개키 v_{pk}로 검증한다.
6. 검증에 성공하면 c_1을 복호화하여 i값, 첫 번째 링크값 $1st_lv(i,0)$를 구한다.
7. 자신의 DB에서 i값과 $1st_lv(i,0)$를 키로 하여 같은 시점에 발행한 익명인증서인 lv 시리즈를 모두 추출한다.
8. i값과 링크값 lv 시리즈를 aa_{pk} 로 암호화하여 c_3를 구한다.

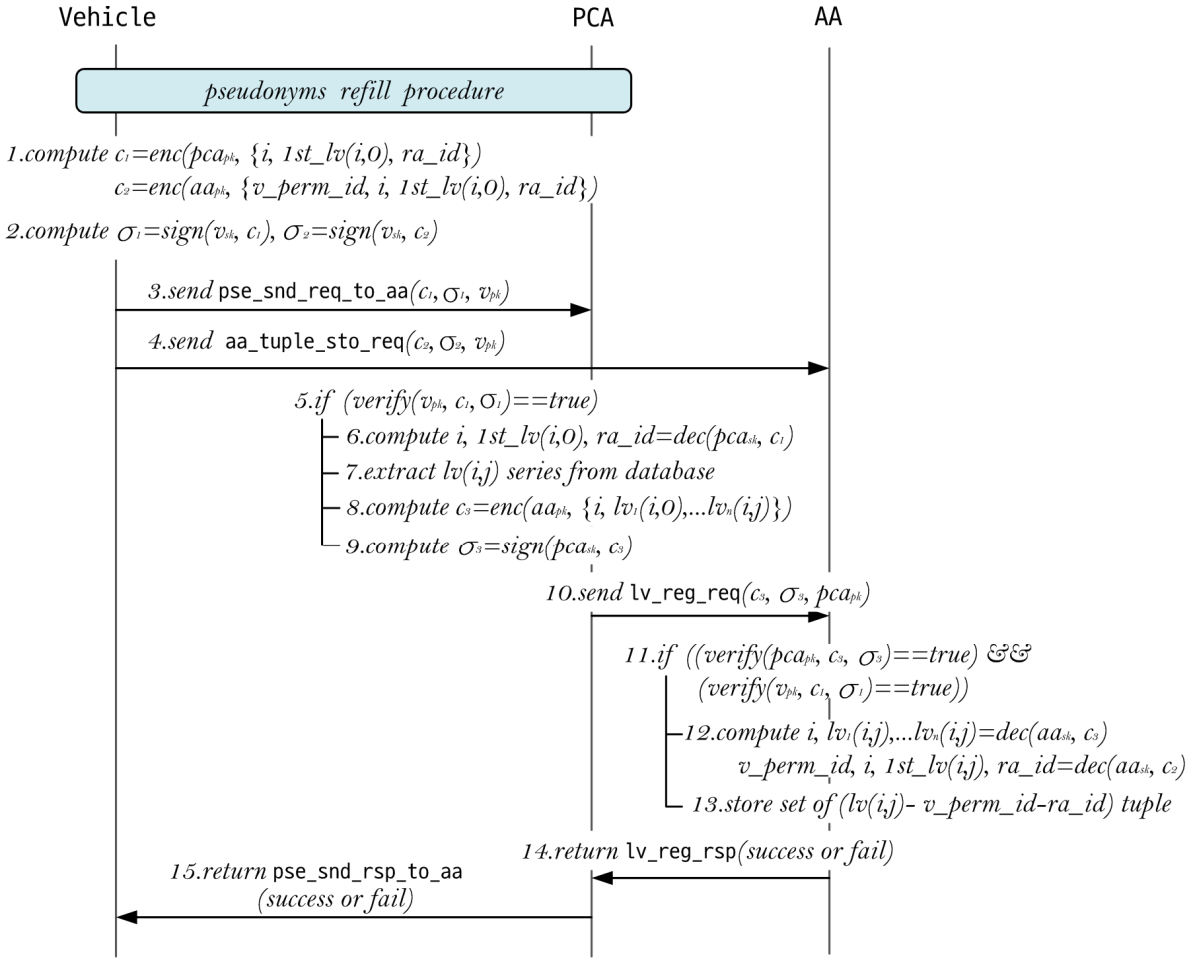

Fig. 1. Pseudonym Registration Protocol

9. c_3를 개인키 pca_{sk}로 전자서명하여 σ_3를 구한다.
10. c_3 σ_2, 공개키 pca_{pk}를 포함시킨 메시지(lv_reg_req)를 AA에게 전송하여 AA에게 lv를 저장하도록 요청한다.
11. 차량으로부터 수신한 σ_1와 PCA로부터 수신한 σ_3를 각각 검증하여 둘 다 성공하면 다음 절차를 진행한다.
12. c_2와 c_3를 복호화하여 차량 ID, i값, lv 시리즈를 구한다.
13. 익명인증서별로 익명인증서-차량 ID-RA ID($lv(i,j)$-v_perm_id-ra_id)튜플을 DB에 저장한다.
14. 성공 또는 실패를 포함시킨 메시지(lv-reg_rsp)를 PCA에게 리턴한다.
15. 성공 또는 실패를 포함시킨 메시지(pse_snd_rsp_to_aa)를 PCA에게 리턴한다. 차량은 이 메시지를 받으면 익명인증서 등록 절차를 종료한다.

인증서 취소가 발생하면 시작되는 인증서 취소 프로토콜을 Fig. 2에 나타내었다.

1. 주변 차량으로부터 특정 차량의 비정상 행위가 MA에게 보고되면 MA는 인증서 프로비저닝 절차를 수행한다.
2. MA는 해당 차량의 익명인증서에 대한 i값, 링크 값($lv(i,j)$), 링크 시드값($ls_1(i), ls_2(i)$), 두 LA(Linkage Authority) ID값(la_id_1, la_id_2)를 알아낸다. 이 정보들을 포함한 메시지(regi_crl_gen_req)를 CRLG에게 전달하여 Regional CRL을 생성하도록 요청한다.
3. CRLG는 해당 차량의 익명인증서가 어느 영역에 위치하는지를 알기 위해서 링크값 $lv(i,j)$에 해당하는 ra_id를 구해달라는 메시지(ra_id_req)를 AA에게 전송한다.
4. AA는 자신의 DB에서 $lv(i,j)$에 해당하는 ra_id를 조회한다.
5. 추출한 ra_id를 응답 메시지(ra_id_rsp)에 포함시켜 CRLG에게 리턴한다.
6. CRLG는 저장된 $lv(i,j)$-v_perm_id-ra_id 튜플로부터 해당하는 $region_id$를 추출한다. 이때 CRLG는 Regional CRL을 배포해야 할 영역을 구한 것이다.
7. CRLG는 그 영역에만 유효한 Regional CRL을 작성한다. Regional CRL에는 수신한 i값, 링크시드 값($ls_1(i), ls_2(i)$), LA ID값(la_id_1, la_id_2)을 포함시킨다. 그리고 CRL 헤더에 Regional CRL을 몇 개의 주변 영역에 중복해서 배포할지를 정책적으로 결정하여 $NumOverlay$의 수와 해당 RA_ID를 지정한다(Fig. 3 참조).
8. 성공 또는 실패를 포함한 메시지(regi_crl_gen_rsp)를 MA에게 리턴한다.
9. Regional CRL을 포함한 배포 메시지(regi_crl_dist_req)를 해당 영역에만 전송한다. Regional CRL이 해당 영역에만 배포되므로 다른 영역에는 영향을 주지 않아 네트워크 전체적으로 보면 처리 부하와 통신 지연이 줄어든다. 또한, 비정상 행위가 보고되면 바로 그 차량의 익명인증서가 Regional CRL에 포함되어 배포되므로 이를 수신한 그 영역 차량은 비정상 행위를 하는 차량과의 통신을 즉각 차단할 수 있어 더 안전하다 할 수 있다.

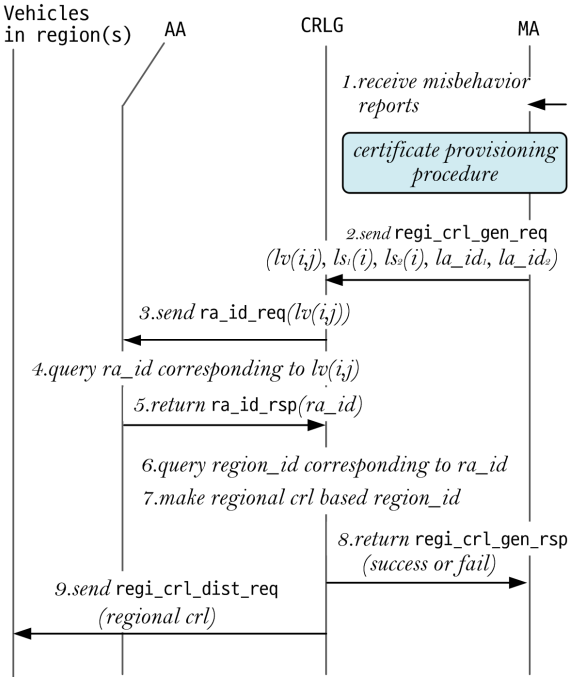

Fig. 2. Certificate Revocation Protocol

4. Regional CRL Message Format

Regional CRL 메시지는 WAVE 표준에서 정의한 CRL 메시지에 추가로 Regional CRL을 몇 개의 주변 영역에 중복해서 배포할지를 나타내는 $NumOverlay$와 해당 영역에 속하는 RA_ID 필드를 추가한다.

```
crlContents :: SEQUENCE {
    version             Uint8,                  1
    crlSeries           Uint16,                 2
    cracaID             Unit8,                  1
    issueDate           Uint32,                 4
    nextCrl             Uint32,                 1
    priorityInfo        Uint8,                  1
    NumOverlay          Unit8,                  1
    RA_ID1              Unit8,                  1
    RA_ID2              Unit8,                  1
    RA_ID3              Unit8,                  1
    fullLinkedCrl       ToBeSignedLinkageVelueCrl
}
```

Fig. 3. Regional CRL Message Format

5. Blockchain-base Privacy Protection

제안한 기법에서 AA는 익명인증서별로 익명인증서- 차량 ID-RA_ID 튜플을 저장하고 있다. 차량 ID는 위치가 추

적될 수 있는 중요한 프라이버시 정보이므로 노출되지 않아야 한다. 이를 고려하여 AA 노드들을 블록체인 네트워크로 연결하고, 차량 ID를 블록체인에 업로드하는 AA 노드 외에 다른 AA 노드들은 차량 ID를 읽지 못하도록 한다. 이후, 차량 ID는 오직 두 개의 인가된 노드 즉, CRLG 노드와 사고 등으로 인해 차량을 추적하는 노드만 읽을 수 있도록 한다. 그리고 두 노드가 차량 ID에 접근할 때에도 인증과 접근제어를 수행한다. 구현의 예를 들면, 프라이빗 블록체인의 하나인 하이퍼링크 레저 패브릭으로 구현한다면, 튜플을 생성하는 채널과 튜플을 읽는 채널을 분리하면 차량 ID 접근을 근본적으로 차단할 수 있다.

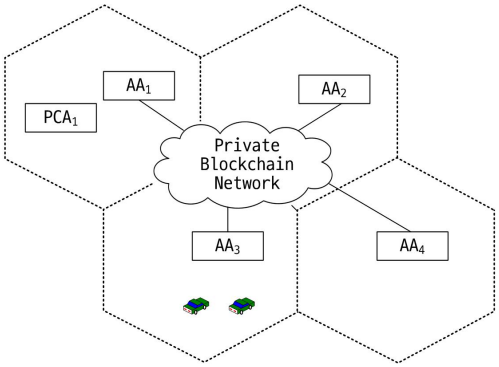

Fig. 4. Blockchain-based Vehicle Privacy Protection

IV. Performance Analysis

제안한 기법의 효율성과 성능을 분석하기 위해, CRL 사이즈와 차량 OBU에 저장된 CRL 엔트리 조회시간을 비교 분석하였다. 기존의 기법인 Full CRL 기법과 블룸필터 기반 Full CRL과 제안한 기법을 비교하였다.

1. Analysis for CRL Size

인증서 취소율에 따른 CRL 사이즈 비교와 Regional CRL 기법에 대하여 차량 대수나 익명인증서의 개수나 지역 분할의 수에 따른 CRL 사이즈를 비교 분석한다. 분석을 위한 파라메터와 Table 2의 기호는 참고문헌 [9][10]을 참조하였다.

전체 차량 대수 N은 국내 차량등록 대수를 고려하여 2,500만대를 적용한다. OBU의 인증서 생명주기 T는 1년을 적용한다. T 기간의 인증서 취소율 p는 0.025~1.5까지를 적용한다. p가 0.025이면 전체 차량 N의 OBU 인증서 중, 2.5%가 취소됨을 의미한다. 각 CRL 엔트리는 취소된 인증서의 SHA-1 해시값의 최상위 비트 10바이트(q)로 구성된다. WAVE[1]에 따른 Full CRL, 블룸필터 기반 Full CRL, Regional CRL 사이즈는 다음과 같이 각각 표현할 수 있다[9][10].

$$CRL_{Full} = N \circ p \circ T \circ q$$

$$CRL_{Bloom} = Header + K_r + K_v + m_v + m_r$$

$$CRL_{Regional} = M \circ \frac{N}{R} \circ p \circ T \circ q$$

Table 2. Notation for Performance Analysis

Variable	Description
N	number of vehicles
p	certificate revocation rate
q	each CRL entry(high order 10 bytes of the SHA-1)
M	average un-expired region-specific certificates
R	number of partitioned regions
T	lifetime of certificates
o	overlay number of Regional CRL
Nv	number of valid certificate
Nr	number of revoked certificate
Kv	number of hash functions of valid certificates for Bloom filter
Kr	number of hash functions of revoked certificates for Bloom filter
m_v	valid bit vector for Bloom filter
m_r	revoked bit vector for Bloom filter

Fig. 5에 인증서 취소율 p를 0.025에서 0.1까지 변화시키면서 CRL 사이즈를 비교하였다. Regional CRL 기법에서는 동일한 Regional CRL이 자신의 영역과 인접한 주변 영역 2개를 포함해 전체 3개의 영역에 중복으로 배포하는 것으로 계산하였다(o=3). 많은 논문에서 기준으로 삼는 p=0.1을 기준으로 하였을 때[9], 제안한 Regional CRL 기법의 CRL 사이즈는 블룸필터 기반 Full CRL에 비해 약 3배 그리고 full CRL에 비해 약 40배 정도 적은 것으로 나타났다.

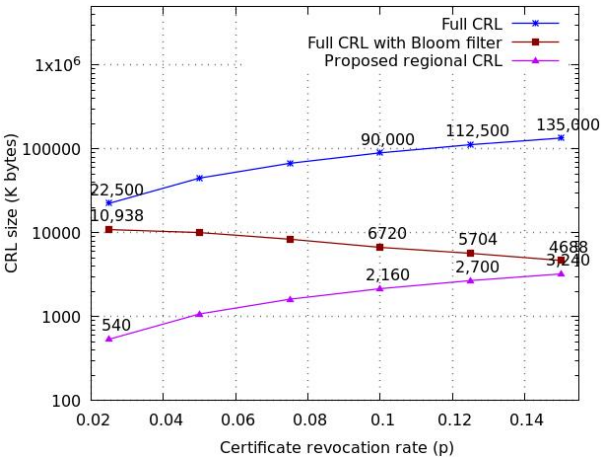

Fig. 5. CRL Size according to p

Fig. 6은 제안한 Regional CRL 기법에서 차량 대수를 변화시킬 때, Regional CRL의 크기를 비교하였다. p는 0.05, 0.1, 0.15를 각각 적용하였다. 그래프에서 차량이 증가하면 CRL 사이즈가 점진적으로 증가하는 것을 알 수 있다. 여기서는 상대적인 CRL 사이즈만 비교하므로 동일한 Regional CRL을 주변에 배포하는 중복 배포는 고려하지 않았다(o=1).

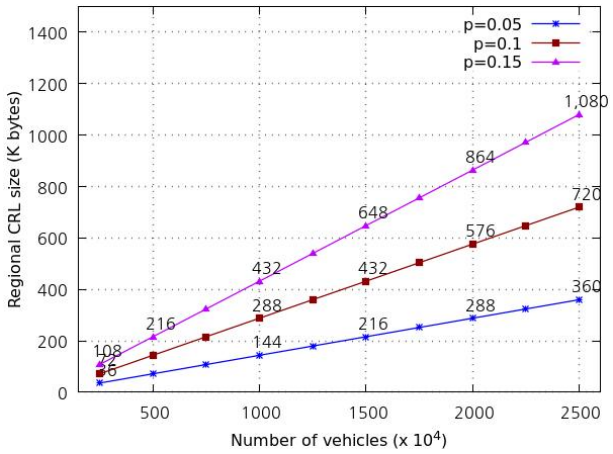

Fig. 6. Regional CRL Size according to number of vehicles

Fig. 7은 Regional CRL 기법에서 전체 영역을 지리적인 영역으로 나눌 때, CRL 사이즈의 변화를 나타내었다. 여기서 p는 0.1로 고정하고, Regional CRL 중복 배포를 나타내는 o는 3으로 고정하였다. 영역을 많이 나눌수록 CRL 사이즈는 급격하게 작아짐을 알 수 있다.

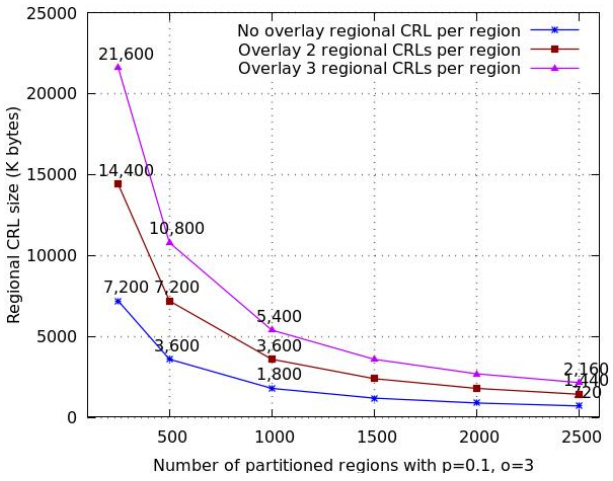

Fig. 7. Regional CRL Size according to R

2. Simulation for CRL Data Query

OBU가 취소된 익명인증서를 조회하는 데 소요되는 시간을 시뮬레이션해 측정하였다. 차량은 주변 차량으로부터 메시지를 수신하면, 메시지 발신 차량의 익명인증서가 DB 내 취소된 인증서 목록에 포함되어 있는지를 조회한다. 만약, 포함되어 있으며 그 차량으로부터 수신한 메시지를 취소하고 통신을 중지한다. 시뮬레이션 환경은 다음과 같다.

- CPU : Intel Core i5-6500 3.20GHz
- OS : Linux Debian 4.15.11-1 kali
- Language : Python 2.7.15
- Database : levelDB

Fig. 8은 차량의 수에 따라 DB에서 하나의 취소된 인증서를 조회하는데 걸리는 소요시간을 나타내었다. 여기서 취소된 인증서의 식별자인 링크값은 랜덤한 값으로 저장하고, 조회에 걸리는 시간은 10회 평균하였다. 익명인증서의 수 M은 20으로 고정하였다. Full CRL 기법과 블룸필터 기반의 Full CRL에 비해 제안한 Regional CRL 기법이 약 5배 정도 빠르게 조회하는 것으로 측정되었다.

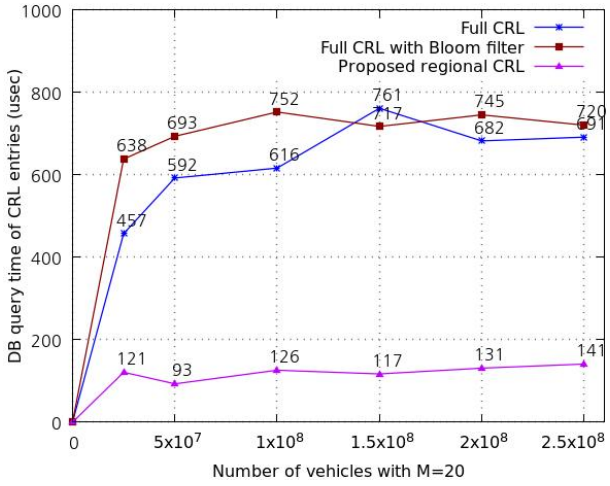

Fig. 8. Query Time for Finding a Revoked Certificate according to N

Fig. 9에 인증서 취소율 p에 따라 DB에서 하나의 취소된 인증서를 조회하는 데 걸리는 시간을 나타내었다. 인증서 식별자인 링크값은 랜덤한 값으로 저장하고, 조회에 걸리는 시간은 10회 평균하여 구했다. 익명인증서의 수 M은 20으로 고정하였다. Full CRL 기법은 차량 대수가 증가함에 따라 조회시간이 감소하나, 블룸필터 기반의 Full CRL 기법은 약간의 증가세를 보였다. 이에 비해 제안한 Regional CRL 기법은 차량 대수가 증가해도 거의 유사한 시간이 측정되었다.

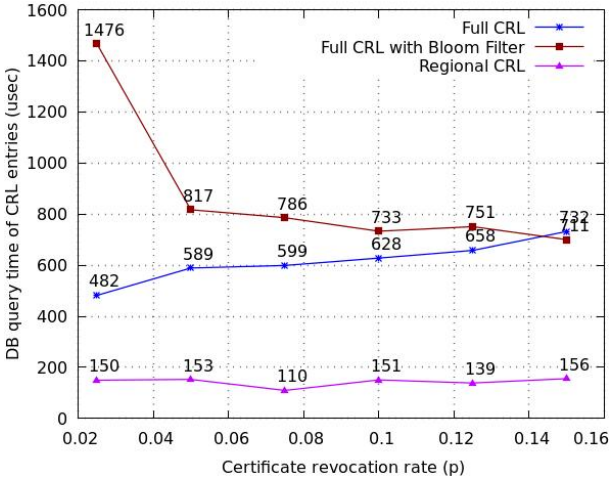

Fig. 9. Query Time for Finding a Revoked Certificate according to p

3. Discussion on CRL Size and Security

인증서 취소율이 10%일 때, CRL 사이즈는 Full CRL에 비해 Regional CRL이 약 40배 정도로 적은 것으로 나타났다. 인증서 취소율이 10%이고 차량 대수가 2,500만대일 때, Regional CRL 사이즈는 약 1MB이다. 인증서 취소율이 10%이고, 주변의 3개 영역에 중복 배포하고, 분할 영역이 500개 일 때, 전체 Regional CRL 사이즈는 약 10MB이다. 차량 대수에 따라 취소된 익명인증서 조회시간을 시뮬레이션한 결과, 차량 대수가 2,500만대일 때, Full CRL에 비해 Regional CRL의 인증서 조회시간이 약 5배 빠른 것으로 나타났다. 이 결과에 따르면 제안한 기법은 CRL 사이즈가 적어 네트워크에서 처리해야 처리 부하를 줄이고 성능을 향상하게 시키고 특히 차량 OBU가 취소된 인증서 조회시간을 크게 줄이는 것으로 나타났다.

제안한 기법은 WAVE에서 정의한 익명인증서를 그대로 사용하여 차량 익명성을 제공하며, 모든 메시지는 노드가 보유한 X.509 인증서를 활용하여 암·복호화와 전자서명·검증을 하여 기밀성과 무결성을 제공한다. 차량 ID에 대한 익명성을 보장하기 위하여 AA 노드들을 블록체인으로 연결하고, AA 노드들은 자신의 영역에서 생성한 튜플을 블록으로 생성할 수 있으나 타 AA 노드들은 읽을 수 없도록 한다. 블록체인을 통해 무결성과 기밀성, 송신자에 대한 인증, 차량 ID에 대한 익명성을 제공한다.

V. Conclusions

본 논문에서는 차량이 특정 영역에 진입했을 때 익명인증서 리필을 수행한다는 점에 착안하여 차량의 위치를 파악하고 그 위치를 활용한 Regional CRL 기법을 제안하였다. 제안한 기법을 완성하기 위해 기본 아이디어, 노드들이 수행해야 할 추가 기능, 익명인증서 등록 프로토콜과 인증서 취소 프로토콜을 설계하였다. 그리고 기존의 CRL 배포 기법과 제안한 기법의 CRL 사이즈를 분석하고 시뮬레이션을 통해 취소된 인증서 조회 시간을 비교 분석하였다.

제한한 기법의 장점은 기존 Full CRL이나 블룸필터 기반의 Full CRL 기법에 비해 CRL 사이즈를 줄임으로써 통신 부하와 지연 감소, 네트워크 자원 사용 감소, 차량 OBU의 CPU 부하 감소 등의 효과를 가진다. 그리고 인증서가 취소될 때마다 즉시 Regional CRL을 배포함으로써 차량의 보안 취약점을 더욱 감소시킬 수 있다. 추후 연구로 Regional CRL을 주변 영역에 중복으로 배포하는 방법의 효과를 상세히 분석하고자 한다.

ACKNOWLEDGEMENT

This Research was supported by Research Funds of Mokpo National University in 2019.

REFERENCES

[1] IEEE 1609.2-2016, "IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, "*IEEE Vehicular Technology Society*, Jan. 2016.

[2] H. Seo, etc., "LTE evolution for vehicle-to- everything services," IEEE Communication Magazine, Vol. 54, No. 6, Jun. 2016, pp.22-28.

[3] Hwi-Seung Hong, etc., "A Regional Certificate Revocation List Distribution Method based on the Local Vehicle Location Registration for Vehicular Communication," *Journal of The Korea Society of Computer and Information*, vol. 21, No. 1, pp.91-99, Jan. 2016.

[4] H.G. 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.

[5] LEI Ao, etc., "A Secure Key Management Scheme for Heterogenous Secure Vehicular Communication Systems," *ZTE Communications*, vol. 14, No. So, pp.21-31, June 2016.

[6] LEI Ao, etc., "A blockchain-based certificate revocation scheme for vehicular communication systems," *ELSEVIER Future*

Generation Computer Systems(online available), April 2019.

[7] Noureddint Lasla, etc., "Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS," *Conference Proc. for New Technologies, Mobility and Security(NTMS)*, pp.1-5, Feb. 2018.

[8] Ze Wang, etc., "Blockchain-based Certificate Transparency and Revocation Transparency," *Financial Cryptography and Data Security, Spring Berlin Heidelberg*, pp.144-162 March 2019.

[9] B. Bellur, "Certificate Assignment Strategies for a PKI-based Security Architecture in a Vehicular Network," in Proc. IEEE Globecom 2018, IEEE GLOBECOM 2008, pp.1-6, Nov. 2008.

[10] K. Kim, etc., "SSKM: Scalable and Secure Key Management Scheme for Group Signature Based Authentication and CRL in VANET, " *www.mdpi.com/electonics*, vol. 8, pp.1-21, 2019.

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 AI security.