JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 4 : 800~806 Apr. 2015

WAVE 시스템 지원을 위한 CRL 다운로드 프로토콜의 설계 및 구현

유권정 · 선설희 · 최범진 · 김은기*

Design and Implementation of CRL download protocol for supporting of WAVE systems

Kwon-jeong Yoo · Seol-hee Seon · Beom-jin Choi · Eun-gi Kim*

Department of Information and Communication Engineering, Hanbat National University, Daejeon 305-719, Korea

요 약

WAVE(Wireless Access in Vehicular Environments) 시스템은 차량이 고속 이동 환경에서 차량 간 또는 차량과 인프라 간 패킷을 주고받을 수 있는 무선 통신 기술이다. 본 연구에서는 차량이 WAVE 시스템에서 통신 할 때 상대방의 인증서가 폐기 되었는지 확인하기 위한 CRL(Certificate Revocation List) 다운로드 프로토콜을 설계하고 구현하였다. WAVE 시스템은 UDP 상에서 동작하도록 하였으며, 보안기능을 지원하기 위해 ECDSA(Elliptic Curve Digital Signature Algorithm)를 사용하여 상호 인증을 하고 ECIES(Elliptic Curve Integrated Encryption Scheme)를 사용하여 기밀성을 보장한다. 또한 CRL 데이터에 MAC(Message Authentication Code)을 추가하여 데이터의 무결성을 보장하고, 선택적 재전송 방식(Selective Repeat Automatic Repeat Request)을 이용하여 데이터의 에러 및 흐름 제어를 수행한다.

ABSTRACT

WAVE(Wireless Access in Vehicular Environments) system is wireless communication technology that vehicle sends and receives packets between vehicles or between vehicles and infrastructure in a high-speed mobile environment. In this study, we have designed and implemented a CRL(Certificate Revocation List) download protocol that is used to verify certificate revocation status of the other party when the vehicles communicate with WAVE system. This protocol operates over UDP. And to support security features, also, ECDSA(Elliptic Curve Digital Signature Algorithm) is used for mutual authentication and ECIES(Elliptic Curve Integrated Encryption Scheme) is used to ensure the confidentiality. Moreover, this protocol ensures the integrity of data by adding MAC(Message Authentication Code) to the end of packet and support the error and flow control mechanisms.

키워드 : WAVE, CRL, 자동차 통신, 보안

Key word : WAVE, CRL, vehicular communication, security

Received 13 February 2015, **Revised** 02 March 2015, **Accepted** 17 March 2015

*** Corresponding Author** Eun-Gi Kim(E-mail:egkim@hanbat.ac.kr, Tel:+82-42-821-1215)
Department of Information and Communication Engineering, Hanbat National University, Daejeon 305-719, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.4.800 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 주행 중인 차량 정보와 주변 교통 정보를 수집하여 차량 안전 운행을 지원하기 위해 IEEE에서 제정한 WAVE(Wireless Access in Vehicular Environments) 시스템의 개발이 활발해지고 있다. IEEE P1609.2는 어플리케이션 및 관리 메시지를 위한 보안 서비스에 관한 표준으로 보안 메시지 형식과 보안 메시지 교환 기능 지원을 위한 환경을 정의한다[1]. IEEE P1609.3은 네트워킹 서비스(Networking Services)를 위한 표준으로 보안된 WAVE 데이터 교환 시 필요한 어드레싱 및 라우팅을 포함하는 네트워크 계층과 트랜스포트 계층을 정의하고 있다. 이 표준은 어플리케이션에 의해 바로 사용될 수 있는 IPv6뿐만 아니라 WAVE에 특화된 프로토콜인 WSMP(WAVE Short Message Protocol)도 정의하고 있다[2]. WAVE는 차량이 최대 200km/h의 고속으로 이동하는 환경에서 V2V(Vehicle to Vehicle) 또는 V2I(Vehicle to Infrastructure) 간 통신 서비스를 지원한다. 또한 유니캐스트(unicast) 및 방송 모드(broadcast)의 통신 방식과 반경 1Km이내에서 1Mbps의 속도를 지원한다[3].

UDP는 TCP와 달리 3 단계 패킷 교환(3-way-handshake)을 수행하지 않으므로 TCP보다 더 빠르게 CRL을 다운로드 할 수 있다. 본 논문에서 제안한 CRL 다운로드 프로토콜은 고속으로 이동하는 자동차 환경에서 보안 패킷들의 신속한 전송을 위하여 UDP 상위에서 동작하도록 설계하였다[4, 5].

본 연구에서는 WAVE 시스템에서 차량이 CA (Certificate Authority)로부터 CRL을 다운받을 때 기밀성과 무결성을 보장하는 프로토콜을 설계하였다. CRL (Certificate Revocation List) 다운로드 프로토콜은 ISP (Initial Setup Protocol), DTP(Data Transfer Protocol), RLP(Record Layers Protocol) 등으로 구성되었다.

ISP에서는 DH(Diffie-Hellman) 키 교환 알고리즘을 이용하여 공유된 비밀 키를 생성하고, ECDSA(Elliptic Curve Digital Signature Algorithm)를 사용하여 상호인증을 하고 ECIES(Elliptic Curve Integrated Encryption Scheme)를 사용하여 기밀성을 보장한다.

DTP는 CRL을 전송하는 프로토콜로서, 데이터 무결성을 보장하기 위하여 CRL 뒤에 MAC(Message Authentication Code)을 추가하여 RLP로 전송한다.

RLP는 ISP나 DTP에서 수신한 데이터를 정해진 길이로 단편화(Fragmentation) 시킨 후, 각 단편(Fragment)에 RLP 헤더를 붙여 하위 계층으로 전송한다. 그리고 전송 과정에서 송수신된 패킷들에 대해 선택적 재전송 방식(Selective Repeat Automatic Repeat Request)과 슬라이딩 윈도(Sliding Window)를 이용하여 에러 제어 및 흐름 제어를 지원한다.

본 논문의 2장에서는 ISP, DTP, RLP의 동작을 자세히 설명하고 3장에서는 성능 검증, 4장에서는 결론을 다룬다.

Ⅱ. 본 론

2.1. ISP

본 프로토콜에서는 서버와 클라이언트 간의 안전하고 신뢰도 높은 통신을 지원하기 위해 상호 인증을 수행한다. ISP는 Client_Hello와 Server_Hello 패킷을 이용하여 상호인증을 수행하며, 이때 이러한 패킷들의 무결성을 확인할 수 있도록 인증 코드(Authentication Code)를 추가한다. 이러한 패킷들은 순서번호(sequence number) 와 클라이언트와 서버간의 비밀 키를 공유하기 위한 DH 공개 키로 구성되어 있다. 다음 (그림 1)은 ISP data에 인증 코드가 추가되는 것을 나타낸 그림이다.

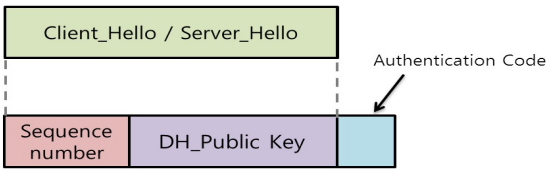

그림 1. ISP : Hello 패킷에 인증 코드 추가
Fig. 1 ISP : Authentication code addition in Hello packet

2.1.1. DH 키 교환 방식

본 연구에서는 두 종단이 공유된 비밀 키를 생성하기 위해서 DH 키 교환 방식을 사용한다. 이 방식에서 두 종단은 p와 α를 먼저 공유해야 하는데, p는 큰 소수이고 α는 p의 원시 근이다.

각 종단에서는 p보다 작은 임의의 개인키를 생성한다. 그리고 p, α, 개인키를 이용하여 각자의 공개키를 생성한다. 이 공개키를 서로에게 전송한 후, 수신한 상대

방의 공개키와 자신의 개인키, p를 이용함으로써 비밀키를 생성하게 된다[6]. DH 키 교환의 과정은 (그림 2)와 같다.

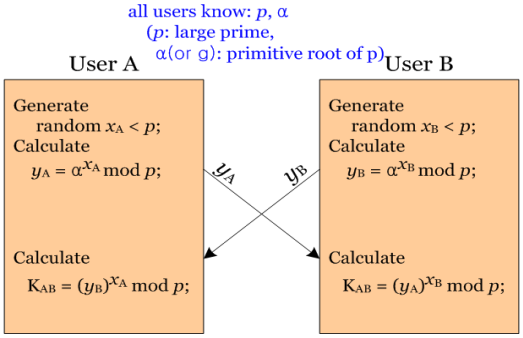

그림 2. Diffie-Hellman 키 교환 알고리즘
Fig. 2 Diffie-Hellman key exchange algorithm

2.1.2. ECDSA 와 ECIES

차량과 CA는 전자서명을 통해 서로에게 본인임을 증명함으로써 신뢰도를 높인다. 본 논문의 CRL 다운로드 프로토콜에서는 타원곡선 암호(Elliptic curve cryptosystem)를 이용한 전자서명 방식인 ECDSA를 이용한다. 타원곡선 암호 방식은 다른 암호 방식에 비해 키의 길이가 짧기 때문에 암호화, 복호화 속도가 빠르다. 그리고 보다 강력한 보안성을 가지는 특징이 있다.

메시지에 서명을 하기 위해 서명자가 임의의 개인키를 생성한 후, ECDSA 파라메타를 이용하여 공개키를 생성한다. 그리고 임의의 수 k, ECDSA 파라메타, 메시지의 해시 값과 개인키를 이용하여 메시지의 서명인 r, s를 생성한다[7]. 이 r과 s는 ISP 데이터의 인증 코드에 포함된다. 다음 (그림 3)은 ECDSA의 서명이 계산되는 과정을 나타낸다.

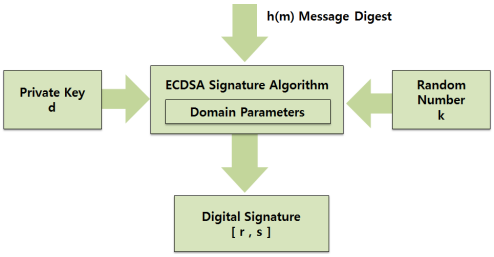

그림 3. ECSDSA 서명 계산 과정
Fig. 3 ECDSA signature calculation

ECDSA의 서명 검증과정에서 증명자는 동일한 해시 알고리즘을 사용하여 생성된 해시 값, 서명자의 공개키와 s를 계산하여 수신된 r과 비교한다[7]. ECDSA의 서명 값으로 서명을 검증하는 과정은 (그림 4)와 같다.

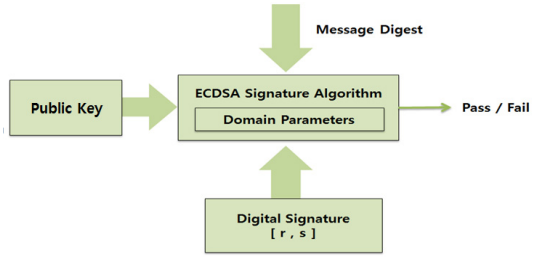

그림 4. ECDSA 서명 검증 과정
Fig. 4 ECDSA signature verification process

본 논문에서는 상호 인증 과정에서 차량이 CA의 공개키를 알고 있다고 가정한다. 차량이 CA로부터 인증을 받기 위해서는 CA에게 자신의 인증서를 보내 주어 CA가 차량의 공개키를 알 수 있게 해야 한다. 또한 ECIES를 사용하여 인증서의 무결성을 위해 인증서의 MAC 값을 계산한다. 이 값과 ECIES의 매개 변수, 인증서는 Client_Hello 패킷의 인증 코드에 포함된다.

2.2. DTP

DTP는 CRL을 전송하는 프로토콜로서 데이터의 무결성을 보장하기 위해 CRL 뒤에 MAC을 추가한다. 이때, MAC 키는 ISP에서 공유한 비밀키의 일부를 이용한다. 그리고 재전송(Replay) 공격을 방지하기 위하여 MAC에 사용되는 메시지에 순서 번호를 추가한다. 다음 (그림 5)는 DTP data에 MAC이 추가되는 것을 나타낸 그림이다.

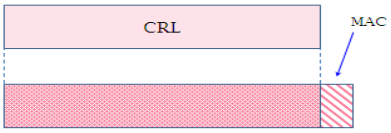

그림 5. DTP: CRL 데이터에 MAC 추가
Fig. 5 DTP : MAC addition in CRL data

2.3. RLP

RLP는 상위 계층에서 수신한 데이터를 송수신하는 프로토콜로 상위계층으로부터 전달받은 데이터를 (그

림 6)과 같이 단편화 하여 RLP 헤더를 덧붙인다.

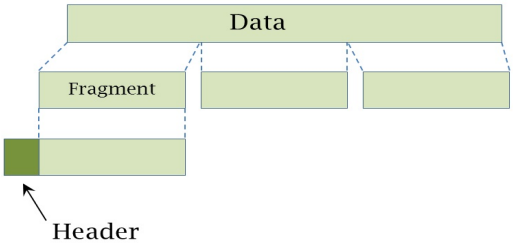

그림 6. RLP 부계층에서 데이터 단편화의 예
Fig. 6 Examples of data fragmentation in RLP sublayer

RLP는 MTU(Maximum Transmission Unit)에 따라 단편화 한 후, 각 데이터 단편에 RLP 헤더를 덧붙여 하위 계층으로 전송한다. 이때 RLP MTU의 값은 IP계층의 MTU에서 IP 헤더, UDP 헤더, RLP 헤더의 크기를 제외한 값을 갖는다[4]. (그림 7)은 RLP 헤더의 구조를 나타낸다.

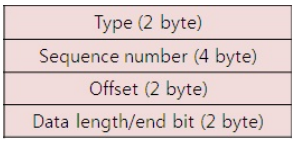

그림 7. RLP 헤더 구조
Fig. 7 RLP header structure

2.3.1. RLP의 동작 과정

본 연구에서 CRL 다운로드 프로토콜은 차량이 고속으로 이동하는 WAVE 환경에 맞게 UDP 상위에서 구현되었다. 하지만 UDP에서는 별도의 에러 제어와 흐름 제어를 하지 않기 때문에[7] RLP에서 선택적 재전송 방식과 슬라이딩 윈도를 이용하여 흐름 제어 및 에러 제어 기능을 지원하도록 하였다[4, 5, 8].

선택적 재전송 방식은 패킷 당 개별 타이머를 설정하여 타임아웃이 발생하기 전에 수신자의 응답에 따라 윈도를 슬라이딩하거나 재전송하는 방식이다. 만일 타임아웃이 발생하기 전에 응답이 오지 않으면 타임아웃 카운트를 증가시킨다. 임의의 패킷에 대한 타임아웃 카운트 값이 3일 때 송신자는 데이터의 전송을 포기하고 수신자에게 연결 종료 패킷을 전송한다.

슬라이딩 윈도는 윈도의 가장 앞에 있는 패킷의 ACK를 수신하면 윈도를 슬라이딩 하여 다음 순서의 패킷을 전송하고 마지막으로 전송한 패킷을 윈도의 가장 마지막에 위치하게 하는 방식이다. 단, NACK가 오면 윈도를 슬라이딩 하지 않는다[4, 5, 8]. 본 연구에서는, 이를 이용하여 흐름제어를 하였다. (그림 8)은 전송측 RLP 알고리즘이다.

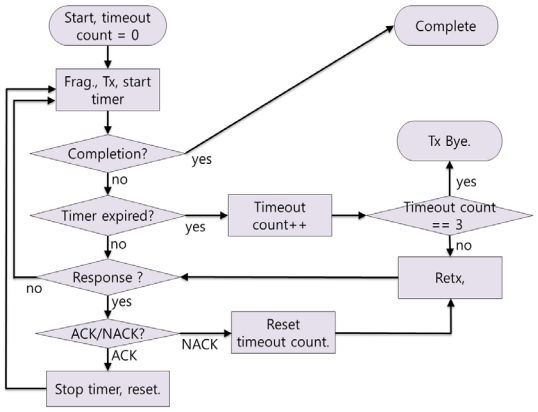

그림 8. 전송측 RLP 알고리즘
Fig. 8 Sender RLP algorithm

수신자는 수신한 패킷의 RLP 헤더를 통해 에러 유무를 확인 할 수 있다. 에러가 발견되면 송신자에게 해당 패킷의 재전송을 요청하거나 연결 종료 패킷을 전송한다. 수신자는 패킷들을 모두 수신하면 각 패킷의 RLP 헤더를 이용하여 수신한 단편들을 재조립한다. (그림 9)은 수신측 RLP의 동작 알고리즘이다.

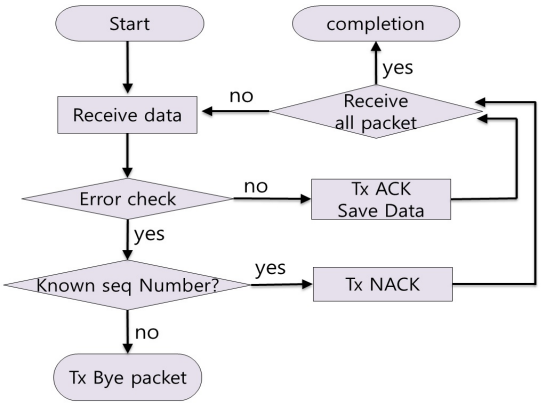

그림 9. 수신측 RLP 알고리즘
Fig. 9 Receiver RLP algorithm

Ⅲ. 성능 검증

성능분석의 조건으로는 서버와 클라이언트는 같은 IP 대역이고 1개의 라우터를 통과하는 것이다. 성능검증은 PER(Packet Error Rate)과 데이터 크기에 따른 전송시간을 측정하는 방식으로 진행하였다. 기존 UDP에서 에러가 발생하지 않는 경우의 측정 결과는 (표 1)에 나타내었으며, 본 논문에서 제안한 프로토콜에 에러율을 적용한 측정 결과는 (표 2)에 나타내었다. (그림 10)은 (표 1)과 (표 2)를 도식화 한 것을 보여주고 있다.

표 1. 기존 UDP 상위에서의 CRL 다운로드 성능 측정 표 (시간 단위 : msec)
Table. 1 CRL download performance measurement table on the existing UDP

Layer \ Data size (kB)	1	3	5	10
UDP	7.081	9.978	12.147	17.631

표 2. 본 연구의 CRL다운로드를 이용한 CRL 다운로드 성능 측정 표 (시간 단위 : msec)
Table. 2 CRL download Performance Measurement table using the CRL download protocol of this study

Error rate(%) \ Data size (kB)	1	3	5	10
0.00	85.248	86.820	121.032	197.624
0.01	89.075	91.188	135.567	212.519
0.03	107.287	131.243	158.247	251.041
0.05	111.357	144.624	176.750	325.208
0.10	135.435	187.296	247.009	411.076

(표 1)과 (표 2)의 에러율이 0.00%인 경우의 측정 결과를 비교하면, 같은 크기의 데이터를 다운로드할 때 기존 UDP 상위에서의 측정 시간보다는 본 논문에서 제안한 프로토콜에서의 측정 시간이 큰 값을 갖는다. 이는 본 논문에서 제안한 프로토콜이 UDP에서는 지원하지 않는 에러제어, 흐름제어, 그리고 보안 기능 등을 지원하기 때문인 것으로 생각된다. (표 2)를 분석하면 에러율과 데이터의 크기가 커짐에 따라 에러 제어를 위한 처리 시간이 늘어나 CRL을 다운받는 시간이 지연되는 것을 알 수 있다.

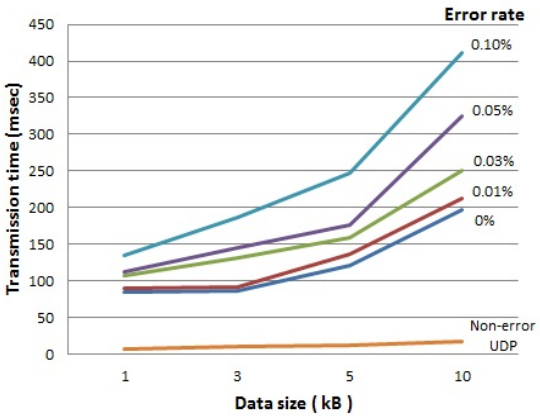

그림 10. 전체 성능 측정 그래프
Fig. 10 Total performance measurement graph

Ⅳ. 결 론

본 연구에서는 WAVE 시스템에서 차량이 CA로부터 CRL을 다운로드 하는 프로토콜을 UDP 상에서 구현하였다.

본 연구에서 제안한 CRL 다운로드 프로토콜은 ISP에서 ECDSA로 상호인증을 수행하고, ECIES 방식의 암호화 기능을 지원한다. 또한 DH 키 교환 방식으로 공개키를 공유하고, 생성된 비밀키의 일부를 DTP에서 MAC 키로 사용함으로써 데이터의 무결성을 보장할 수 있다.

본 연구에서 제안한 프로토콜은 UDP 상에서 CRL을 단순히 다운받는 것에 비해 전송속도가 느리다. 하지만 본 연구의 프로토콜은 다운받은 데이터의 무결성을 보장할 수 있고, 에러 및 흐름 제어 기능을 제공하기 때문에 안전하고 신뢰도가 높은 통신을 할 수 있다는 장점을 갖는다.

추후에는 본 논문의 CRL 다운로드 프로토콜을 임베디드 보드에 포팅하고, 실제 차량이 이동하는 환경에서 동작 및 성능을 확인하는 연구를 수행할 예정이다.

감사의 글

이 논문은 2013년 교육부와 한국연구재단의 지역혁신인력양성사업의 지원을 받아 수행된 연구(NRF-2013H1B8A2032154) 및 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0199293)의 연구수행으로 인한 결과물임을 밝힙니다.

REFERENCES

[1] IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Std 1609.2, 2013.

[2] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, 1609.3, 2010.

[3] John B. Kenney, Member IEEE, “Dedicated Short-Range Communications (DSRC) Standards in the United States” in *Proceedings of the IEEE*, vol.99, No.7, July 2011.

[4] Behrouz A. Forouzan “TCP/IP Protocol Suite, Fourth Edition”, McGRAW HILL INTERNATIONAL EDITION, 2010.

[5] Behrouz A. Forouzan “Data Communications and Networking”, McGRAW HILL FIFTH EDITION

[6] Pravir Chandra, Matt Messier, John Viega “Network Security with OpenSSL”, June 2002.

[7] S. Blake-Wilson, G. Karlinger, T. Kobayashi, Y. Wang “Using the Elliptic Curve Signature Algorithm (ECDSA) for XML Digital Signatures”, RFC 4050, IETF, April 2005.

[8] UNIVERSITAT PADERBORN. Simulation of Selective Repeat / Go Back N. Available:http://www.ccs-labs.org/teaching/rn/animations/gbn_sr/

유권정(Kwon-Jeong Yoo)

2015년 2월 : 한밭대학교 정보통신공학과 (정보통신공학 학사)
2015년 3월 ~ 현재 : 한밭대학교 정보통신전문대학원 석사과정
※관심분야 : 네트워크, WAVE, Security

선설희(Seol-Hee Sun)

2015년 2월 : 한밭대학교 정보통신공학과 (정보통신공학 학사)
2015년 3월 ~ 현재 : 한밭대학교 정보통신전문대학원 석사과정
※관심분야 : 네트워크, WAVE, Security

최범진(Bum-Jin Choi)

2014년 2월 : 한밭대학교 정보통신공학과 (정보통신공학 학사)
2014년 3월 ~ 현재 : 한밭대학교 정보통신전문대학원 석사과정
※관심분야 : 컴퓨터 네트워크 , 암호화, 네트워크 보안

김은기(Eun-Gi Kim)

1989년 2월 : 고려대학교 대학원 전자공학과(전자공학 석사)
1994년 2월 : 고려대학교 대학원 전자공학과(전자공학 박사)
1995년 2월 ~ 현재 : 한밭대학교 정보통신공학과 교수
※관심분야 : 컴퓨터 네트워크, 임베디드 S/W, 암호화, 네트워크 보안