WAVE 시스템 환경에서 CA와 차량간 보안통신 프로토콜

서동원*, 박승범*, 안재원*, 김은기*
*한밭대학교 정보통신공학과
e-mail:mpfive@nate.com

A Security Communication Protocol between CA and Vehicle for WAVE System

*Dong-Won Seo, *Seung-Peom Park, *Jae-Won Ahn, *Eun-Gi Kim
*Dept. of Information and Communication Engineering, Han-Bat National University

요 약

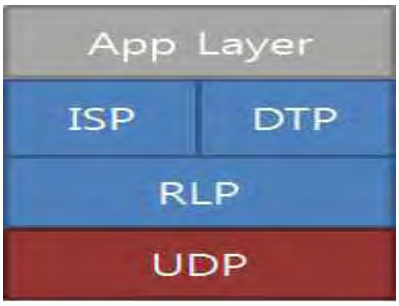
WAVE (Wireless Access in Vehicular Environments) 시스템 환경은 차량 간 무선통신을 가능하게 해주는 환경이다. 무선통신의 활용이 증가하면서 그에 따른 공격 방법도 증가하여, 통신 시 제3자에 의해 패킷이 변조될 수 있다. 제3자로부터 패킷을 보호하기 위해 통신 전 차량은 CA (Certificate Authority)로부터 자신이 적합한 호스트라는 것을 인증 받아야 한다. 본 논문에서는 차량과 CA의 통신 과정에서 Diffie-Hellman Key Exchange 알고리즘과 AES (Advanced Encryption Standard) 알고리즘 등을 이용하여 패킷의 기밀성과 무결성을 보장하는 프로토콜을 설계하였다.

1. 서론

최근 WAVE 시스템 환경이 각광을 받고 있다. 정부에서도 '국가 ITS (Intelligent Transport System) 기본계획'을 통해 차량 간 무선통신에 대한 활발한 지원을 계획한 상태이다[1]. WAVE 시스템 환경이란 차량이 고속으로 이동하고 있는 상황에서 기반시설 (Vehicle-to-Infrastructure)이나 다른 차량 (Vehicle-to-Vehicle) 과의 통신을 가능하게 해주는 환경이다. 이는 도로의 상황을 다른 차량에게 전달하여 인명사고 예방, 차량 추돌 방지, 실시간 교통 정보 제공 등 여러 방면에 활용될 수 있을 것으로 예상된다[2].

하지만 무선통신 기술 활용이 증가하면서 Man-in-the-Middle Attack, Eavesdroping, Replay Attack과 같은 공격들도 증가하여 보안상의 위험이 야기되었다[3]. 이러한 이유로 본 논문에서는 WAVE 시스템 환경에서 안전하게 통신하기 위해 Diffie-Hellman Key Exchange 알고리즘과 AES 알고리즘을 적용시킨 보안통신 프로토콜을 설계하였다. 속도 면에서 TCP는 오버헤드가 크기 때문에 WAVE 시스템 환경에서 사용하기에 적합하지 않다. 따라서 본 논문에서는 TCP보다 오버헤드가 적은 UDP 상에서 동작하도록 설계하였다. 그림 (1)은 프로토콜의 전체적인 구조를 나타낸다.

본 논문의 구성은 다음과 같다. 2장에서는 Diffie-Hellman Key Exchange 알고리즘, AES 알고리즘에 대하여 기술하였다. 3장에서는 프로토콜의 기본적인 설계에 대하여 기술하였다. 4장에서는 결론을 서술하였다.



(그림 1) 설계된 프로토콜 기본구조

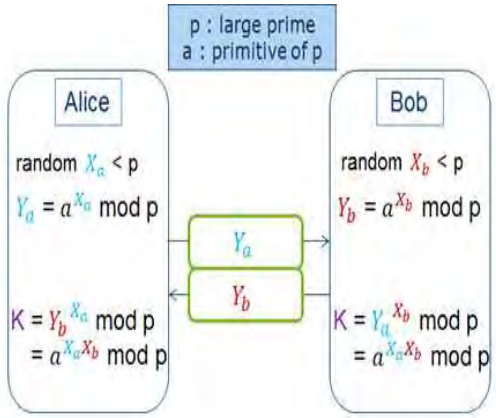
2. 관련 연구

일반적으로 패킷을 암호화하기 위해서는 키가 필요하다. 암호화에 사용된 키는 두 호스트만이 알 수 있도록 관리하는 것이 매우 중요하다.

2.1 Diffie-Hellman Key Exchange 알고리즘

Diffie-Hellman Key Exchange 알고리즘은 공개키를 교환하여, 두 호스트만이 알 수 있는 Session Key를 생성하는 알고리즘이다. 키 교환과정에서 공개키는 누구든 알 수 있지만 Session Key는 두 호스트만 알고 있기 때문에 Session Key로 데이터를 암호화하게 되면 제3자는 데이터의 내용을 알 수 없게 된다. 그림 (2)는 Session Key가 생성되는 과정을 나타낸다.

키를 교환하려는 두 호스트는 사전에 α, p를 공유한다. p는 Large Prime 이고 α는 p의 Primitive Root이다. 각 호

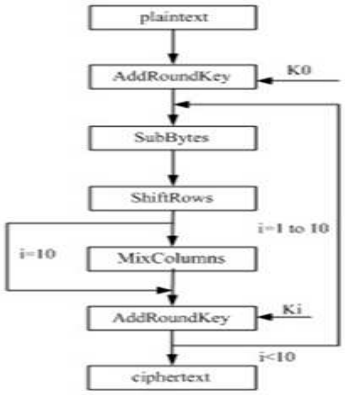


(그림 2) Diffie-Hellman Key Exchange Algorithm

스트는 p보다 작은 임의의 수로 자신의 개인키(Xa, Xb)를 생성하고 그 후 α, p, 개인키를 이용하여 공개키(Ya, Yb)를 생성한다. 각 호스트는 상대방에게 자신의 공개키를 보낸다. 상대방으로부터 받은 공개키, 자신의 개인키, α, p를 이용하여 K를 생성하는데 이 값이 Session Key이다[4]. 생성된 Session Key는 AES 알고리즘에 사용된다.

2.2 AES 알고리즘

AES 알고리즘은 대칭키 암호화 알고리즘으로 암호화와 복호화에 쓰이는 키가 동일하다. AES 알고리즘은 16바이트의 블록단위로 암호화하며 128, 192, 256비트 키를 사용한다[5]. 그림 (3)은 암호화가 이루어지는 과정을 나타낸다.

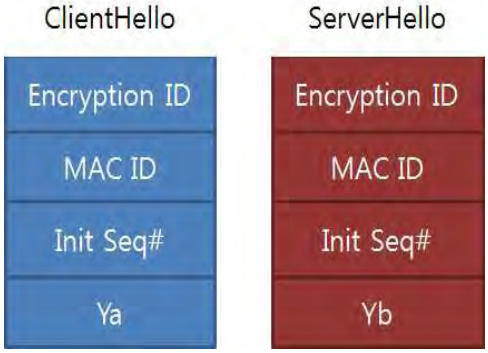


(그림 3) AES 알고리즘을 이용한 암호화 과정

3. 프로토콜의 기본적인 설계

차량과 CA는 통신하기 전에 ISP (Initial Setup Protocol)를 통해 초기 설정을 해야 한다. 차량은 ClientHello라는 ISP 패킷을 만들어 CA에게 보낸다. ClientHello에는 Diffie-Hellman Key Exchange 알고리즘으로 생성된 차량의 공개키와 초기 설정에 관련된 정보가 포함되어 있다. ISP 패킷은 전자서명을 통해 제3자의 공격으로부터 보호되도록 한다.

CA는 차량으로부터 받은 ClientHello의 내용을 확인하고 저장한 뒤 ServerHello라는 ISP 패킷을 만들어 차량에게 보낸다. ServerHello에는 Diffie-Hellman Key Exchange 알고리즘으로 생성된 CA의 공개키와 초기 설정에 관련된 정보가 포함되어 있다. 그림 (4)는 ISP 패킷의 구조를 나타낸다.



(그림 4) ISP Packet

ISP에서 생성된 패킷은 RLP (Record Layer Protocol)로 전송된다. 초기 설정이 이루어진 후 Application Data의 전송은 DTP (Data Transfer Protocol) 를 통해 시작된다. DTP는 Application Data를 AES 알고리즘을 이용하여 암호화하고 MAC (Message Authentication Code) 을 생성한다. 암호화된 Application Data는 MAC과 함께 RLP로 전송된다. RLP는 수신한 패킷을 Fragmentation하거나 에러를 제어하여 재전송하는 역할을 한다.

4. 결론

본 논문은 WAVE 시스템 환경에서 차량과 CA간 통신 시 패킷의 기밀성과 무결성을 보장해주는 프로토콜을 설계하였다. Application Data는 기밀성을 보장하기 위해 AES 알고리즘을 이용하여 암호화된다. 암호화에 사용될 키는 Diffie-Hellman Key Exchange 알고리즘을 이용하여 생성된다. RLP는 무결성을 보장하기 위해 에러를 제어하는 기능을 수행한다.

감사의 글

본 연구는 교육부와 한국연구재단의 지역혁신인력양성사업(No. 2013H1B8A2032154) 및 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0199293)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] 이상선, “차량통신 국제 표준화 동향”, 한국통신학회지(정보와통신) 제29권 제2호, 3-10, 2012

[2] 이세연, 정한균, 윤상훈, 임기택, “C-ITS 를 위한 WAVE 시스템 발전 동향”, 한국통신학회 학술대회논문집, 229-230, 2013

[3] 이연철, 서화정, 김호원, “WAVE 하드웨어 암호 라이브러리에 적합한 효율적인 AES-CCM 구조 설계”, 한국정

보통신학회논문지, 17(12), 2899-2905, 2013
[4] Behrouz A. Forouzan, Shphia Chung Fegan, “Data communications and Networking”, 4rd Ed., pp.943-945, 952-954, McGraw Hill, 2007
[5] 한국인터넷진흥원 암호이용활성화 공식사이트, http://seed.kisa.or.kr/