JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 4 : 841~847 Apr. 2015

WAVE 통신 시스템을 위한 차량 보안 통신 프로토콜의 설계 및 구현

박승범 · 안재원 · 김은기*

Design and Implementation of Secure Vehicle Communication Protocols for WAVE Communication Systems

Seung-peom Park · Jae-won Ahn · Eun-gi Kim*

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

요 약

WAVE(Wireless Access in Vehicular Environments) 통신 시스템은 차량 간 무선통신을 가능하게 해주는 환경을 지원한다. 무선통신의 활용이 증가함에 따라 그에 따른 공격 방법도 다양해져, 패킷들은 통신 시 제3자에 의해 변조될 수 있다. 본 논문은 CA(Certificate Authority)와 차량이 통신 과정에서 ECIES(Elliptic Curve Integrated Encryption Scheme)를 이용하여 자신이 적합한 호스트임을 인증 받고, AES(Advanced Encryption Standard) 알고리즘을 이용하여 패킷의 기밀성과 무결성을 보장하는 프로토콜을 제안하였다.

ABSTRACT

The WAVE(Wireless Access in Vehicular Environments) communication system supports wireless communication environments between vehicles. As the utilization of wireless communication has been increased, attack methods have been varied. There is a high risk on packet manipulations conducted by third party. In this paper, we have designed a secure communication protocol between CA and vehicles. Our designed protocol uses a ECIES(Elliptic Curve Integrated Encryption Scheme) for vehicle authentication and AES(Advanced Encryption Standard) algorithm for protecting packet integrity and confidentiality.

키워드 : WAVE, 암호화, 무결성, 기밀성

Key word : WAVE, Encryption, Confidentiality, Integrity

Received 13 February 2015, **Revised** 05 March 2015, **Accepted** 18 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.2015.19.4.841 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

정부는 '국가 ITS(Intelligent Transport System) 기본계획'을 통해 차량 간 무선통신에 대한 활발한 지원을 계획하였다[1]. 국토해양부는 연중추돌사고와 같은 대형교통사고를 막기 위해, 앞 차량과의 추돌 예방 기능이 포함된 스마트 하이웨이를 구현하는 사업을 서울~수원 간에 시행하겠다고 밝혔다[2]. 이러한 추세에 따라 WAVE 통신 시스템이 각광을 받고 있다. WAVE 통신 시스템은 차량이 고속으로 이동하고 있는 상황에서 다른 차량(Vehicle-to-Vehicle)이나 기반시설(Vehicle-to-Infrastructure)과의 통신을 가능하게 해주는 환경을 지원한다. 이러한 기술은 도로의 상황을 다른 차량에게 전달하여 인명사고 예방, 차량 추돌 방지, 실시간 교통정보 제공 등 여러 방면에 활용될 수 있을 것으로 예상된다[3].

하지만 무선통신 기술 활용이 증가하면서 MITM (Man-in-the-Middle) 공격, 재전송 공격과 같은 공격들도 증가하여 보안상의 위험이 야기되었다[4]. 예를 들어 차량 추돌 사고를 알리는 데이터가 노출되어 제3자에 의해 변조되었을 때, 1차 충돌로 끝날 수 있는 사고가 더 큰 사고로 이어질 수 있다. 이러한 이유로 본 논문에서는 WAVE 통신 시스템에서 안전하게 통신하기 위한 보안통신 프로토콜을 제안하였다.

본 논문에서 제안하는 보안 통신 프로토콜은 WAVE 통신 시스템에서 필요로 하는 실시간 전송 기능을 지원하기 위하여 UDP 상위에서 동작하도록 하였는데, 기존의 UDP 상위에서 보안기능을 지원하는 DTLS (Datagram Transport Layer Security)는 오버헤드가 크고, 부분적인 에러 제어 기능만을 지원하는 단점이 있다. 이에 따라서, 본 연구에서는 모든 에러를 제어할 수 있는 기능을 지원하며, WAVE 통신 시스템에 최적화된 프로토콜을 제안하였다. 그림 (1)은 프로토콜의 전체적인 구조를 나타낸다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구를 위한 보안 알고리즘들에 대하여 기술하였고, 3장에서는 프로토콜을 설계 및 동작에 대하여 기술하였다. 4장에서는 성능 검증에 대하여 기술하였고, 마지막으로 5장에서는 결론을 서술하였다.

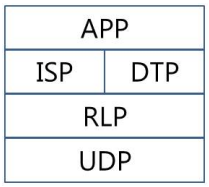

그림 1. 설계된 프로토콜 기본구조
Fig. 1 The Basic Structure of the Designed Protocol

Ⅱ. 본 연구를 위한 보안 알고리즘들

2.1. ECDSA 전자서명 알고리즘

ECC(Elliptic Curve Cryptography) 방식은 타원곡선이라 불리는 수식에 의해서 정의되는 특수한 가산법이다. ECDSA란 타원곡선을 활용한 전자서명을 말한다. 그림 (2)는 ECDSA(Elliptic Curve Digital Signature Algorithm)를 통한 전자 서명의 생성과 생성된 전자 서명을 확인하는 과정을 나타낸다.

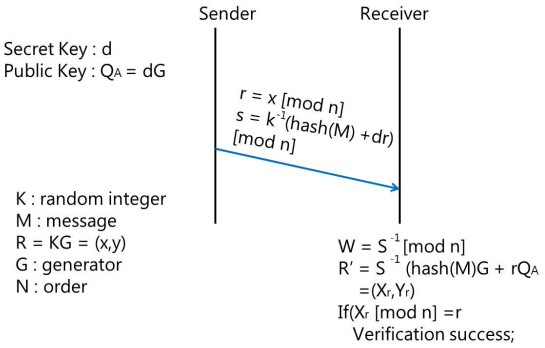

그림 2. ECDSA를 통한 전자 서명 생성과 확인 과정
Fig. 2 Digital Signature Generation and Verification Process through the ECDSA

2.2. ECIES 암호화 알고리즘

ECIES는 타원곡선을 활용한 암호화 방법이다. 데이터를 주고받으려는 두 호스트는 사전에 S_1, S_2를 공유한다. 데이터를 받을 호스트는 자신의 개인키 k_B에 G를 곱하여 공개키 K_B를 생성한다. 여기서 G는 앞서 ECDSA에서 사용한 G와 같은 파라미터다. 그리고 임의의 수 r을 G와 곱하여 R을 생성한다.

데이터를 보낼 호스트는 임의의 수 r을 상대방의 공

개키와 곱하여 P(P_x, P_y)를 생성한다. P_x와 S_1을 가지고 KDF(Key Derive Function)를 통하여 암호화에 쓰일 K_E, 메시지 인증에 쓰일 K_M를 얻어낸다. K_E로 메시지를 암호화하여 C를 생성한다.

암호화 결과 값 C에 S_2를 붙인 값과 K_M을 이용하여 MAC (Message Authentication Code) 을 생성하는데 이 값이 d가 된다. 암호화 된 데이터를 보낼 호스트는 R과 C와 d를 붙여서 상대방 호스트에게 보낸다. 이를 수신한 호스트는 수식 (1)과 같이 R 값을 통하여 S를 계산해낼 수 있다.

$$S = P_x = P(P_x, P_y) \\ = rK_B = rGK_B = RK_B \quad (1)$$

그 결과 호스트는 S와 사전에 공유한 S_1을 KDF를 통해 K_E, K_M를 계산하여 값을 구한다. C에 S_2를 붙인 값과 K_M를 이용하여 MAC을 생성한 후 수신한 d와 비교하여 메시지가 손실 없이 수신되었는지 확인하고, K_E를 가지고 C를 복호화 하여 메시지 내용을 인증한다. 그림 (3)은 ECIES를 통해 메시지를 암호화하고 복호화 하는 과정을 나타낸다.

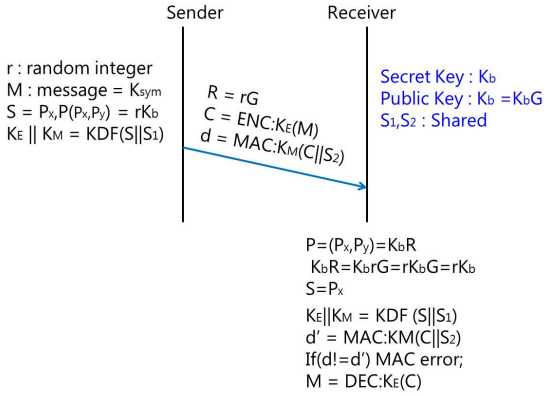

그림 3. ECIES를 통한 암호화, 복호화 과정
Fig. 3 Encryption and Decryption Process through ECIES

2.3. DH(Diffie-Hellman) 키 교환 알고리즘

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

DH 키 교환 알고리즘은 공개키를 교환하여, 두 호스트만 알 수 있는 세션키(Session Key)를 생성하는 알고리즘이다. 키 교환과정에서 공개키는 누구든 알 수 있지만 세션키는 두 호스트만 알고 있기 때문에 세션키로 데이터를 암호화하면 제 3자는 데이터의 내용을 복호화할 수 없게 된다. 그림 (4)는 세션키가 생성되는 과정을 나타낸다.

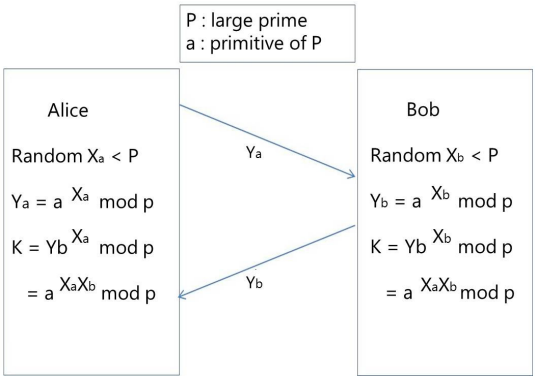

그림 4. DH 키 교환 알고리즘
Fig. 4 Diffie-Hellman Key Exchange Algorithm

키를 교환하려는 두 호스트는 사전에 α, p를 공유한다. p는 큰 소수(Large Prime)이고 α는 p의 원시근(Primitive Root)이다. 각 호스트는 p보다 작은 임의의 수를 생성하여 자신의 개인키(X_a, X_b)로 사용하고 그 후 α, p, 개인키를 이용하여 공개키(Y_a, Y_b)를 생성한다. 각 호스트는 상대방에게 자신의 공개키를 보낸다. 상대방으로부터 받은 공개키, 자신의 개인키, α, p를 이용하여 K를 생성하는데 이 값이 세션키다 [5]. 생성된 세션키는 AES 알고리즘과 HMAC-SHA에 사용된다.

2.4. AES 암호화 알고리즘

AES 알고리즘은 대칭키 암호화 알고리즘으로 암호화와 복호화에 쓰이는 키는 동일하여야 한다. AES 알고리즘은 16바이트의 블록단위로 암호화하며 128, 192, 256비트 키를 사용한다[6]. 그림 (5)는 암호화가 이루어지는 과정을 보여주고 있다.

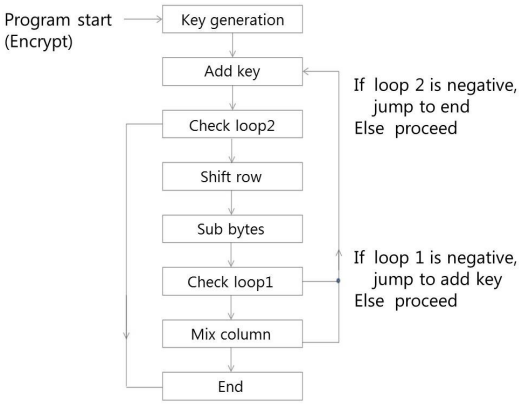

그림 5. AES 알고리즘을 이용한 암호화 과정
Fig. 5 The Encryption Process Using the AES Algorithm

2.5. HMAC-SHA

해시(Hash)란 어떤 데이터를 가지고 고정된 길이의 전자지문을 생성하는 것을 말한다. SHA란 암호학적 해시 함수들의 모음이다. 원래의 메시지를 해시하는 것은 가능하지만 해시한 메시지를 원래의 메시지로 돌리는 것은 불가능하다.

기본적으로 해시는 키가 필요 없지만 MAC은 키가 필요하다. HMAC은 해시와 개인키 암호화를 통한 MAC 생성 방식이 합쳐진 것을 말한다. RFC 2104에 나와 있는 HMAC에 대한 정의는 수식(2)와 같다.

$$HMAC(k,m) = H((K \oplus opad \,|\, H((K \oplus ipad)|M))) \quad (2)$$

- H: 암호화 해시 함수
- K: 해시 함수의 입력 블록사이즈만큼 0으로 패딩된 개인키
- m: 인증될 메시지
- | : 데이터 결합
- ⊕: Exclusive OR 연산
- opad: 외부 패딩
- ipad: 내부 패딩

Ⅲ. 보안 프로토콜 설계 및 동작

본 연구에서 제안한 프로토콜은 2장의 연구들을 바탕으로 그림 (1)과 같이 UDP와 응용 계층 사이에 ISP, DTP, RLP로 나누어 설계하였다.

3.1. ISP 부계층

차량과 CA는 통신하기 전 ISP(Initial Setup Protocol)를 통해 초기 설정을 해야 한다. 차량은 DH 키 교환 알고리즘(2.3)으로 생성된 차량의 공개키와 암호화 방법, 해시 알고리즘 선택, 순서번호가 포함되어 있는 ClientHello를 만든다. 그림 (6)은 ClientHello의 구조를 나타낸다.

하지만 DH 키 교환 알고리즘은 MITM 공격의 위험에 노출되어 있다는 치명적인 단점이 있다[7]. 이를 보완하기 위해 DH 키 교환 알고리즘으로 만들어진 세션키는 ECDSA(2.1)와 ECIES(2.2)를 활용하여 보호되도록 하였다[8].

ClientHello 뒤에 ECDSA로 생성한 전자서명 값 r과 s를 붙인다. 이 때 차량은 인증서를 발급받기 위해 사용했던 자신의 개인키로 전자 서명을 생성한다. 그리고 차량의 인증서를 ECIES 암호화 과정에서 생성된 값 R, C, d에 붙인다. 암호화에 사용된 키는 CA의 공개키이다[9]. 차량은 이러한 과정으로 ISP 데이터를 만들어 CA에게 전송한다.

CA는 차량으로부터 받은 ISP 데이터에서 R, C, d를 ECIES로 복호화한다. 복호화에 사용된 키는 CA의 개인키이다. 복호화한 결과 CA는 차량의 인증서를 얻게 된다. 그리고 CA는 차량의 인증서에서 공개키를 추출하여 수신한 전자 서명의 r과 s가 유효한지 확인한다. 전자 서명이 유효하다고 확인되면 CA는 차량의 ClientHello의 내용을 저장하고 ServerHello를 만든다. ServerHello에는 DH 키 교환 알고리즘으로 생성된 CA의 공개키와 CA의 초기 설정에 관련된 정보가 포함되어 있다.

그림 (6)은 ServerHello의 패킷의 구조를 나타낸다.

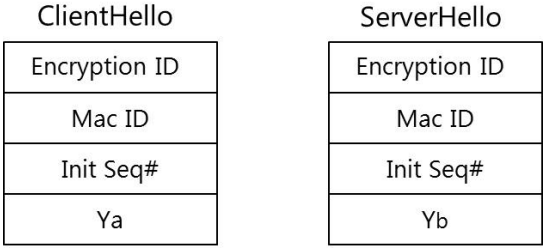

그림 6. ClientHello와 ServerHello 패킷의 구조
Fig. 6 Structure of ClientHello and ServerHello

CA는 ServerHello 뒤에 ECDSA로 생성한 전자 서명 값 r과 s를 붙인다. 이 때 CA는 자신의 개인키로 전자 서명을 생성한다. 차량은 CA의 공개키를 알고 있기 때문에 ServerHello에는 CA의 인증서를 붙이지 않는다. CA는 이러한 과정을 통해 ISP 패킷을 만들어 차량에게 보낸다. ServerHello를 수신한 차량은 CA의 전자 서명을 확인한다. 그림 (7)은 ECDSA, ECIES를 활용한 초기 설정 과정이다.

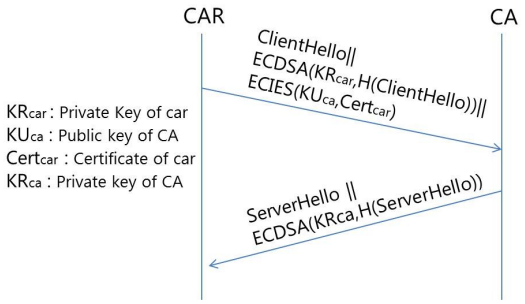

그림 7. ISP 초기 설정 과정
Fig. 7 ISP Initial Setup Process

3.2. DTP 부계층

차량과 CA는 ISP를 통해 초기 설정을 끝낸 후 DTP(Data Transfer Protocol)를 통해 데이터를 송수신한다. 차량은 DH 키 교환 알고리즘으로 생성된 차량의 공개키와 ServerHello를 통해 얻게 된 CA의 공개키를 이용하여 세션 키를 생성하고, 생성된 세션 키를 이용하여 데이터를 AES 알고리즘(2.4)으로 암호화한다.

암호화만 하여 데이터를 전송할 경우, 재전송 공격과 같은 공격에 취약해 지는데[10,11], 이를 보완하기 위해 암호화된 데이터와 순서 번호를 이용하여 MAC을 생성하여 데이터 뒤에 붙인 뒤 전송한다. 그림 (8)은 암호화된 데이터 와 MAC(2.5)을 붙인 데이터를 나타낸다.

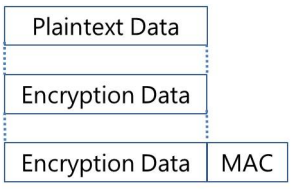

그림 8. 암호화된 데이터와 MAC
Fig. 8 Encryption Data and MAC

데이터를 수신한 CA는 데이터와 MAC 부분을 분리한다. 그리고 CA는 ClientHello에서 정해진 차량의 순서 번호와 암호화된 데이터를 이용하여 MAC을 생성한다. 수신측에서는 수신한 MAC과 생성한 MAC을 비교하여 재전송 공격이 방지되고[12] 무결성이 보장된 데이터임을 확인한다. 그 후 정해진 암호화 알고리즘을 이용하여 데이터를 복호화하여 상위 계층에 전송한다.

3.3. RLP 부계층

본 논문에서 제안한 프로토콜은 UDP 상위에서 동작하기 때문에 에러 제어 기능과 MTU(Maximum Transfer Unit)에 맞게 데이터를 나누어 주는 기능이 필요하다[13]. RLP(Record Layer Protocol)는 그림 (1)과 같이 ISP와 DTP의 하위 계층에 위치하여 이러한 기능을 지원한다.

기존의 UDP에서 보안기능을 지원하는 프로토콜인 DTLS는 타이머(Timer)를 이용한 부분적인 에러 제어 기능만을 지원하는 단점이 있다[13]. RLP는 이런 단점을 보완하기 위해 ARQ(Automatic Repeat Request) 기법 중 정지대기방식(Stop and Wait, Idle ARQ)[14]을 이용하여 에러를 제어하도록 하였다. ISP와 DTP에서 송신한 데이터는 하위 계층인 RLP에서 UDP의 MTU에 맞게 단편화하여 송신되고, 이렇게 나누어진 데이터를 수신측 RLP에서 재조립하여 수신측 ISP와 DTP로 전송하게 된다.

Ⅳ. 성능 검증

본 연구에서는 성능분석을 위하여, 본 연구에서 제안한 방식과 UDP 상에서 보안 기능을 지원하는 않는 단순 전송 응용과의 전송 속도를 비교하였다.

성능 분석에 필요한 서버와 클라이언트 간의 통신은 로컬 IPC(inter process communication) 방식을 이용하였다.

측정 내용은 데이터를 3, 5, 7, 10KB로 나누어 전송하고 전송시간을 측정하는 것이다. 측정은 단순 전송 응용을 측정한 후, 본 논문에서 제안한 프로토콜을 PER(Packet Error Rate)이 0%, 0.01%, 0.03%, 0.05%, 0.07% 인 순서로 측정하였다. 시간 측정은 clock_gettime() 시스템 콜을 사용하였으며 단위는 micro초로

제한하였다. 표 (1)과 (2), 그림 (10)은 측정한 내용을 각각 표와 그래프로 나타낸 것이다.

표 1. 단순 전송 응용의 성능측정 표 (단위 : msec)
Table. 1 Performance Measurement Table of Simple Transfer Application

PER \ Data	3kb	5kb	7kb	10kb
0.00%	2.89	4.34	5.92	8.49

표 2. 제안한 프로토콜의 성능측정 표 (단위 : msec)
Table. 2 Performance Measurement Table of Proposed Protocol

PER \ Data	3kb	5kb	7kb	10kb
0.00%	5.54	9.03	13.66	19.79
0.01%	5.68	9.13	13.97	20.65
0.03%	5.89	9.43	14.77	24.57
0.05%	5.91	9.63	16.50	29.53
0.07%	6.03	9.92	18.60	35.77

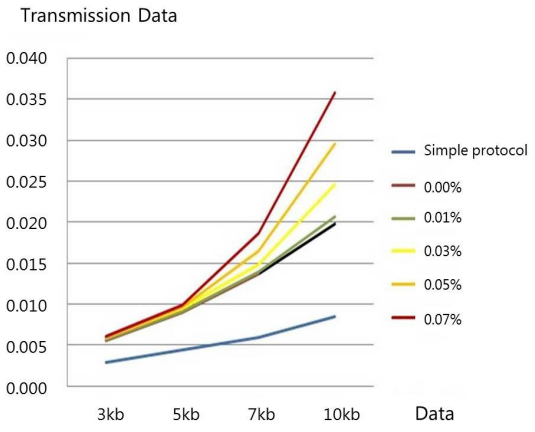

그림 9. 성능측정 그래프
Fig. 9 Performance Measurement Graph

분석 결과, 본 연구에서 제안한 프로토콜의 전송속도는 단순 전송 응용에 비해 느리다. 또한 PER이 높아지고 데이터양이 많아질수록 더 느려진다. 그 원인은 본 연구에서 제안한 프로토콜이 PER이 높아지고 데이터양이 많아질수록 에러 제어 메시지를 많이 전송하기 때문이다.

Ⅴ. 결 론

본 논문은 WAVE 통신 시스템 환경에서 차량과 CA 간 통신 시 패킷의 기밀성과 무결성을 보장해주는 프로토콜을 제안하였다. 제안한 프로토콜은 ISP에서 ECDSA와 ECIES를 활용하여 DH 키 교환 알고리즘이 MITM 공격에 취약한 점을 보완하였다.

또한, DTP에서 AES 알고리즘으로 데이터를 암호화하여 패킷의 기밀성을 보장하고[15], HMAC-SHA로 MAC을 생성하여 재전송 공격을 방지하였다[12]. 프로토콜은 보다 빠른 전송을 위해 UDP 상위에서 동작하도록 하였으며, RLP에서 Idle-RQ를 활용한 에러 제어를 통해 패킷의 에러를 제어하고 무결성을 보장하였다.

본 연구에서 제안한 프로토콜은 단순 전송 응용에 비해 전송속도가 느리지만, UDP 상위에서 패킷의 무결성과 기밀성, 에러 제어 기능을 지원하는 장점이 있다.

본 연구에서 제안된 프로토콜을 실제의 차량에 장착하여 차량 속도에 따른 성능을 분석하는 연구를 수행하여, 차량 속도에 최적화된 파라메타 값을 설정하는 연구를 추가로 수행할 예정이다. 또한 기존의 기술을 뛰어넘는 새로운 대안에 대한 지속적인 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] S.S. Lee, “Vehicle Communication International Standardization Trend”, *The Korean Institute of Communications and Information Sciences(Information & Communications Magazine)*, vol.29,no.2,pp. 3-10, 2012.

[2] M.Y. Bang, I.J. Jang. “"Act on the construction of a ubiquitous city" revised direction from the point of view of the traffic information business”, CEO Report 2008, No.13, pp.1-22.
[3] S.Y. Lee, H.G. Jeong, S.H. Yoon, and K.T. Lim, “Development Trend of WAVE System for the C-ITS Communication”, *Korea Electronics Technology Institute*.
[4] Y.C. Lee, H.J. Seo, H.W. Kim, “The Efficient AES-CCM Architecture for a hardware library in the WAVE”, *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 17, No. 12 : 2899~2905 Dec. 2013.
[5] Behrouz A. Forouzan, Shphia Chung Fegan, “Data communications and Networking”, 4rd Ed., pp.943-945, 952-954, McGraw Hill, 2007.
[6] National Internet Development Agency of Korea activation password using the official site. Available: http://seed.kisa.or.kr/.
[7] C. Krishana Kumar, G. Jai Arul Jose, C. Sajeev and C.Suyambulingom, “Safety measures against man-in-the-middle attack in key exchange” *ARPN Journal of Engineering and Applied Sciences*, Vol. 7, No. 2, Feb 2012.
[8] David J. Malan, Matt Welsh, Michael D. Smith, “A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography”, *IEEE 4-7*, pp.71-80, Oct. 2004,
[9] Dan Boneh and Igor E. Shparlinski “On the Unpredictability of Bits of the Elliptic Curve Diffie‐Hellman Scheme”, L*ecture Notes in Computer Science* Vol 2139, 2001, pp.201-212, Aug 2001.
[10] Gavin Lowe “An attack on the Needham-Schroeder public-key authentication protocol” *Information Processing Letters* 56 (1995) pp.131-133.
[11] K.C Shin, “A Robust and Secure Remote User Authentication Scheme Preserving User Anonymity”, *Journal of the Society of Korea e-commerce Aritcle* 18 No.2, Apr 2013.
[12] Junichiro Saito, Kouichi Sakurai, “Grouping proof for RFID tags”, *IEEE 28-30* , pp.621-624, Vol.2, Mar 2005.
[13] RFC 4347, *Datagram Transport Layer Security*, E.Rescorla, N. Modadugu, Apr 2006.
[14] R. J. Benice, A. H. Frey, “An Analysis of Retransmission Systems”, *IEEE*, Vol.12 pp.135-145, Jun 2003.
[15] Zilhaz Jalal Chowdhury, Davar Pishva, G. G. D. Nishantha “AES and Confidentiality from the Inside Out”, *IEEE 7-10*, pp.1587-1591, Vol.2, Feb 2010.

박승범(Seung-Peom Park)

2015년 2월 : 한밭대학교 정보통신공학과 (정보통신 학사)
2015년 3월 : 한밭대학교 정보통신전문 대학원 석사과정
※관심분야 : 네트워크, IOT, WAVE, Security, 무선랜

안재원(Jae-Won Ahn)

2014년 2월 : 한밭대학교 정보통신공학과 (정보통신공학 학사)
2014년 3월 ~ 현재 : 한밭대학교 정보통신전문 대학원 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