차량 보안 통신 알고리즘 적합성 분석

한선희*, 박민우*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:{shhan, mwpark}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

A Analysis on Suitability of the Security Algorithms in VANET

Sun-Hee Han*, Min-Woo Park*, Tai-Myoung Chung**
*Department of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information and Communication Engineering, Sungkyunkwan University

요 약

차량통신은 차량 내부 단말기 (OBU)를 통해 차량 간 (V2V) 통신을 제공하고, 노변 장치 (RSU)를 통해 차량과 인프라 간 (V2I) 통신을 제공하는 기술이다. 이를 통해 사용자는 교통사고 예방을 위한 서비스, 인터넷 연결 등을 통한 다양한 서비스를 제공받을 수 있다. 하지만 차량 주행 시 통신의 안전성이 보장되지 않는다면 위장공격 및 메시지 변조 공격 등으로 인해 사고를 발생 시킬 수 있다. 따라서 인증 및 무결성 제공 등 차량통신 메시지의 안전성이 보장 되어야 한다. 본 논문에서는 차량통신에서의 보안 서비스를 분석하였고, IEEE 1609.2에 정의된 보안 알고리즘의 요구조건을 만족하는지 분석하여 적합성을 판단하였다.

1. 서론

최근 무선통신과 위성 위치 확인 시스템 (GPS, Global Positioning System) 기술, 지능형 교통 시스템 (ITS, Intelligent Transportation System) 등 IT와 자동차산업의 융합이 가속화됨으로써 자동차 공간 내 스마트 서비스가 확대되고 있다. ATLAS의 조사에 따르면, 2015년에 약 1억대의 네트워크 접속이 탑재된 자동차가 출시될 것이며, 2020년에는 세계의 모든 자동차에 통신 단말이 탑재 될 것으로 예상된다[1]. 또한, 국내에서는 '스마트 하이웨이 사업단'이 차량통신을 위한 연구와 테스트를 수행함으로써 차량통신의 사업화를 추진하고 있다. '스마트 하이웨이 사업단'은 2014년에 기술을 도입할 것이며, 역시 2020년에는 모든 차량에 통신이 가능한 장비들이 설치될 것으로 전망하고 있다[2].

차량통신 (VANET, Vehicular Ad-hoc Networks)은 사고의 위험을 방지하고, 멀티미디어 등 인터넷을 통한 운행의 편의성을 제공하기 위한 기술로써 차량 간 (V2V, Vehicle to Vehicle) 통신, 차량과 인프라 간 (V2I, Vehicle to Infrastructure) 통신을 통해 서비스를 제공한다. 하지만 차량통신의 기술 도입을 위해서는 차량통신에서 주고받는 메시지의 안전성을 보장하기 위한 기술들이 필요하다. 본 논문에서는 차량통신에서의 보안 고려사항과 IEEE 1609.2에 정의된 보안 알고리즘이 차량통신 환경에서의 요구조건에 만족하는지에 대해 분석함으로써 현재 IEEE 1609.2에서 소개된 보안 알고리즘들의 적합성을 판단한다. 이를 통해 차량 통신에 적합한 보안 알고리즘 구현에 기여할 수 있을 것으로 기대된다.

본 논문의 구성은 다음과 같다. 2장에서는 차량통신의 구성요소 및 차량통신에 대한 전반적인 설명과 차량통신에서 발생 가능한 공격모델을 설명한다. 3장에서는 공격을 방지하기 위한 보안 요구사항을 정의하고, IEEE 1609.2에 정의된 보안 알고리즘들에 대해 차량통신 환경에서 만족해야 하는 요구 조건을 설명한다. 4장에서는 그 조건에 따라 적합성을 분석하고, 5장에서 분석 결과에 대한 결론을 맺고, 향후 연구 방향에 대해 설명한다.

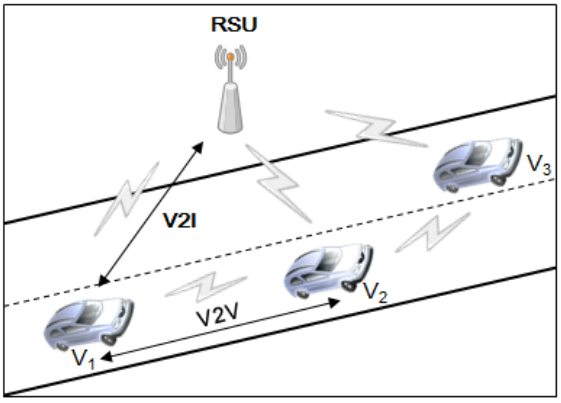
2. 관련연구

본 장에서는 차량통신의 시스템 구성 및 서비스에 대한 설명과 차량통신 환경에서 발생 가능한 공격 모델들을 설명하고, 그에 따른 보안 요구사항에 대해 설명한다.

2.1 차량통신 (VANET: Vehicular Ad-hoc Networks)

차량통신은 Mobile Ad-hoc Network (MANET), Mobile IPv6 (MIPv6), Proxy Mobile IPv6 (PMIPv6) 등을 차량의 특성에 맞도록 통합한 기술로써 사고발생 감소 및 차량 운행의 편의성을 제공한다. 차량통신 네트워크 기술은 차량과 인프라간 통신, 차량 간 통신으로 나눌 수 있다[4]. (그림 1)은 차량통신의 구성요소를 나타낸다. 차량 V_1과 노변장치 (RSU, Road Side Unit) 사이의 통신은 V2I 통신으로써 차량과 주변에 설치된 노변장치를 통해 기존의 인터넷 망과 연결되어 주로 사용자 편의 서비스를 제공한다. 차량 V_2와 V_3 사이의 통신은 V2V 통신으로써 차량 내부에 장착된 차량 단말기 (OBU, On-Board Unit)를 통해 주변의 차량과 통신할 수 있으며 주로 사고 예방

등과 관련된 응급 메시지를 교환할 때 사용된다.



(그림 1) 차량통신 구성요소

2.2 공격 모델

차량통신에서는 이웃 차량과의 협력통신, 전방 충돌 경고를 위한 긴급 메시지 전송, 실시간 교통 정보 전송 등 교통안전과 관련된 서비스 등 차량 운행의 편의성 제공과 관련된 서비스들을 제공한다. 차량통신에서 전송되는 메시지 중 안전 운행과 관련된 서비스를 위한 메시지가 거짓 정보를 나타내거나 위·변조된다면 사고가 유발될 가능성이 있기 때문에 차량통신 환경에 적절한 보안 메커니즘이 제공되어야 한다. <표 1>은 차량통신 환경에서 차량 정보 및 전송할 때 발생할 수 있는 보안 위협에 대한 설명이다[5,6,7,8].

<표 1> 차량통신의 보안 위협

공격 유형	설명
메시지 변조 공격	공격자가 송·수신자간에 전송되는 메시지에 변조된 메시지를 주입하는 공격 방식
Sybil 공격	공격노드가 다수의 식별자로 인식하도록 메시지 유입을 유도하여 지역적 정보를 이용하는 라우팅에 혼란을 주는 공격 방식
프라이버시 침해	시간, 위치, 차량 ID, 이동 정보 등 차량 관련 정보 및 개인 프라이버시 정보를 침해하는 공격
터널 공격	Group System for Mobile (GSM) 통신과 같이 분리된 통신 채널을 통해 전달되는 메시지들에 의한 공격 방식

메시지 변조 공격을 통해 자신의 차량을 응급 차량으로 위장함으로써 차량통신에 참여하는 차량들에게 혼란을 줄 수 있고, 사고의 위협까지 초래할 수 있다. Sybil 공격을 통해 실제 차량이 없더라도 공격 받는 측에서는 차량이 많은 것으로 나타날 수 있어 사용자들이 차량통신의 안전성을 제공받을 수 없다. 또한, 프라이버시 침해 공격을 통해 데이터, 신원, 위치 프라이버시의 침해를 당할 수 있고, 터널 공격을 통해 각 메시지에 인증된 지리적 위치를 포함함으로써 차량통신을 방해할 수 있다.

3. 차량통신 환경에서의 보안 요구사항

본 장에서는 차량통신 환경에서의 보안 서비스를 정의하고, 그에 따라 보안 알고리즘 요구사항 및 시스템 성능상의 요구사항을 정의한다.

3.1 차량통신 보안 서비스

네트워크 보안에서 기본적인 보안 서비스는 크게 6가지로써, 인증, 무결성, 기밀성, 부인방지, 가용성, 접근 권한으로 나눌 수 있다.

본 논문에서는 차량통신 환경에서의 보안 서비스를 인증, 데이터 무결성, 기밀성, 부인방지, 가용성, 프라이버시로 정의하였다. 차량통신에서는 차량의 움직임에 따라 차량이 어디로 움직이는지 추적할 수 있는 위협이 존재하기 때문에 프라이버시 보호 까지 차량통신을 위한 보안 서비스로 정의한다.

차량통신 환경에서의 보안 서비스는 다음과 같다[3,11].

- 인증 (Authentication)

식별은 유효한 사용자를 확인할 수 있는 것을 뜻하며, 인증은 사용자의 신분을 확인하는 과정을 의미한다. 차량통신 환경에서는 식별정보 추적으로 인해 프라이버시 침해의 문제가 있다. 따라서 프라이버시 보호를 위해 Silent period, Mix-zone 등의 기법을 통해 사용자의 신분 확인을 제공하면서 프라이버시도 보호하는 기술이 제안 되었다[9,10]. 신분 확인을 위한 디지털 서명 기술에는 ECC기반 디지털 서명 알고리즘 (ECDSA, Elliptic Curve Digital Signature Algorithm)이 사용된다[4].

- 데이터 무결성 (Data integrity)

데이터 무결성은 송신한 메시지의 수신된 메시지를 비교했을 때 변조되어서는 안 되는 것을 뜻한다. 메시지 수신자는 수신한 메시지가 전송 도중에 위·변조 되었는지 확인할 수 있어야 한다. 데이터 무결성을 제공하기 위해 차량통신에서는 SHA 알고리즘을 사용하여 해시 값을 비교한다.

- 기밀성 (Confidentiality)

기밀성은 메시지를 보낼 때 권한이 없는 제 3자에게 노출 되어서는 안 되는 것을 의미한다. 차량통신에서는 안전 메시지 (Safety message)와 비-안전 메시지 (Non-safety message)가 전송 되는데, 안전 메시지로 전송되는 정보는 사고를 알리는 응급 메시지로써 기밀성이 요구 되지는 않으며, 멀티미디어나 웹 서비스 등을 제공하는 비-안전 메시지 전송 시에는 기밀성이 요구된다.

- 부인 방지 (Non-repudiation)

부인방지는 송신자가 데이터의 전송을 부인할 수 없어야 하는 것을 의미한다. 안전 메시지의 기밀성은 제공하지

않아도 되지만 사고와 같은 상황에서 책임 회피를 방지하기 위해 송신한 메시지에 대해 부인할 수 없어야 하기 때문에 서명기술이 필요하다.

- 프라이버시 (Privacy)

프라이버시는 권한 없는 제 3자에게 사용자의 ID 및 사용자의 정보가 노출되는 것을 막는 것을 의미한다. 차량통신 환경에서는 사고와 같은 상황에서 신분 조회가 필요할 시에는 Trusted Group Manager (TGM)에 의해 정보를 제공받을 수 있다. 이처럼 그룹 서명을 이용하면 누가 서명하였는지는 알 수 없기 때문에 익명성을 보장받을 수 있고, 특정 상황에 신원을 제공하여 조건부 익명성을 제공해야 한다.

- 가용성 (Availability)

차량통신에서의 가용성은 시스템 가용성과 센싱 데이터의 가용성으로 나눌 수 있다. 하지만 이는 하드웨어 보안과 관련된 부분으로 본 논문에서는 고려하지 않는다.

3.2 보안 알고리즘 요구사항

보안 알고리즘 요구사항은 차량통신에서의 공격들을 방어하기 위해 보안 알고리즘이 만족해야 하는 조건을 의미한다. <표 2>는 차량통신에서 암호학적으로 요구되어지는 보안상의 요구사항을 나타낸다. 이는 Vehicle Safety Communications Application (VSC-A)에서 진행하는 프로젝트의 보고서에 정의된 요구사항이다[8].

<표 2> 보안 알고리즘 요구사항

분류	요구조건
R1	128-bit 보안 레벨의 요구사항을 만족해야 한다.
R2	메모리 공격을 막기 위해 모든 키는 적어도 80 bits 이어야 한다.

3.3 시스템 성능 요구사항

시스템 성능 요구사항은 네트워크나 하드웨어 플랫폼 한계에 의해 주어진다. <표 3>은 차량통신 시스템에서 보안 서비스가 만족해야 할 성능상의 요구사항을 나타내며 이 또한 VSC-A에서 진행하는 프로젝트의 보고서에 정의된 요구사항이다[8].

본 논문에서는 각 보안 서비스가 <표 2>와 <표 3>을 바탕으로 각 요구사항을 만족하는지를 분석하여 적합성을 판단한다.

<표 3> 인증 시 시스템 성능 요구사항

분류	요구조건
R3	인증을 위해 1초당 10개의 서명 값을 생성할 수 있어야 한다.
R4	인증을 위해 1초당 1000개의 서명 값을 확인할 수 있어야 한다.
R5	V2V 메시지의 서명을 생성하고 확인하는데 걸리는 시간은 총 20ms 이하를 만족해야 한다.

4. 적합성 분석

3장에서 설명한 보안 알고리즘 요구사항을 IEEE 1609.2에서 정의된 차량통신 알고리즘이 만족하는지에 대해 분석하여 적합성을 판단한다.

4.1 보안 서비스 별 알고리즘 적합성

본 논문에서는 보안 알고리즘의 적합성을 다음과 같이 보안 서비스 별로 분석하였다.

- 기밀성 (Confidentiality)

차량통신에서의 서비스는 안전 서비스 (Safety Application)와 비-안전 서비스 (Non-Safety Application)으로 나눌 수 있다. 3.1절에서 설명하였듯이 안전 서비스를 위한 메시지 전송 시에는 암호화를 하지 않으며, 비-안전 서비스를 위한 메시지 전송 시에는 암호화를 통해 기밀성을 제공해야 한다. 차량통신에서의 암호화는 ECIES를 통해 이루어진다[5].

- 데이터 무결성 (Data integrity)

차량통신에서 무결성 체크는 SHA-256의 해쉬 알고리즘을 사용한다[4]. SHA-1은 80-bit, SHA-256은 128-bit, SHA-384는 192-bit, SHA-512는 256-bit 수준의 보안 레벨을 만족한다. 따라서 데이터 무결성을 위한 메커니즘으로는 SHA-256을 사용하여 보안 요구사항 중 R1을 만족시킨다. SHA-256 알고리즘은 FIPS-2 standard에 정의되어 있다[12].

- 인증 (Authentication)

차량통신에서 인증을 위한 디지털 서명은 ECDSA를 사용한다. 차량통신과 같은 무선 환경에서는 RSA 방식대신 타원곡선 암호가 부각되고 있다. 타원곡선의 상수곱 연산은 바탕 유한체의 기본연산을 포함하고 있으므로 하드웨어와 소프트웨어상의 구현이 용이하다는 장점을 갖고 있다. 또한 추가 보안을 위해 주기적으로 곡선 E를 변경할 수 있다. 따라서 차량통신에서는 ECC 알고리즘 기반의 서명 알고리즘인 ECDSA를 사용한다[4]. ECDSA-256은 서명 생성 시 약 6ms, 확인 시 23ms가 소비되며, ECDSA-224는 서명 시 약 4ms, 확인 시 16ms가 소비된다[8]. <표 4>는 <표 3>의 시스템 요구사항을 만족하는지의 판단을 위한 처리 시간 결과이다.

<표 4> 시스템 요구사항 만족 여부 판단을 위한 연산

ECDSA -256	Generation: 6ms x 10 = 60ms = 0.06s Verification: 23ms x 1000 = 23000ms = 23s
ECDSA -224	Generation: 4ms x 10 = 40ms = 0.04s Verification: 16ms x 1000 = 16000ms = 16s

<표 4>에서와 같이 ECDSA-256은 0.06초 안에 10개의 서명 값을 생성할 수 있다. 또한, 서명 값 확인은 1초당 1000개의 서명 값을 확인하기 위해서는 23초가 소비되며 1초당 약 50개의 서명 값을 확인 할 수 있다. 따라서 R3

은 만족하지만, R4는 만족하지 못한다. 또한 R5의 요구사항인 서명 생성 및 확인 처리 시간은 20ms 이하에 대해 ECDSA-256은 29ms로 만족하지 못한다. 이에 비해 ECDSA-224는 총 20ms로 R5 요구사항을 만족한다. 따라서 R5의 요구사항에 따라 V2V 통신을 위한 메시지 전송 시에는 ECDSA-224를 통해 인증을 수행한다.

4.2 요구사항 만족 여부

본 절에서는 적합성 분석 결과 IEEE 1609.2 standard에 정의 되어 있는 알고리즘별로 요구사항을 만족하는 항목을 나타낸다. <표 5>는 SHA-256, ECDSA-224, ECDSA-256이 각각 어떤 요구사항을 만족하는지 나타낸다.

<표 5> 요구사항 만족 여부

보안 메커니즘	알고리즘	만족하는 요구사항
기밀성	ECIES	-
데이터 무결성	SHA-256	R1, R2
인증	ECDSA-224	R2, R3, R5
	ECDSA-256	R1, R2, R3

분석한 결과 데이터 무결성을 위한 SHA-256은 보안상의 요구조건을 모두 만족하였으며, 인증을 위한 ECDSA는 키 길이 224bits, 256bits 모두 <표 3>에서 R4로 명시된 서명 확인 시의 요구조건은 만족하지 못하였다.

5. 결론 및 향후 연구

차량통신 환경에서의 보안 위협을 줄이기 위해 차량 통신 환경에 적합한 보안 서비스를 제공해야 한다. 본 논문에서는 IEEE 1609.2에서 소개된 보안 알고리즘이 적합한지에 대해 요구사항의 만족 여부를 분석하였다. 그 결과 인증을 위한 ECDSA는 서명 확인 시 성능 상 부적합한 결과를 얻었다. 따라서 향후에는 차량 통신에 적합한 서명 기법을 연구하여 기존의 ECDSA보다 향상된 성능을 제공하는 서명기술을 제안 할 것이다.

ACKNOWLEDGEMENT

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소 지원 사업으로 수행된 연구임 (2011-0018397).

참고문헌

[1] ATLAS Research & Consulting, http://www.arg.co.kr/ (2012.03.01)

[2] SMART Highway, http://www.smarthighway.or.kr/ (2012.02.25)

[3] Sun-Hee Han, Hun-Jung Lim, Tai-Myoung Chung, “The Use Possibility of the LTE for Solving the Security Issues in Vehicular Ad-Hoc Networks,” International Conference on Electrical, Computer, Electronics and Communication Engineering, Apr. 2012.

[4] Steve M. Mills et al., “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Application and Management Messages,” IEEE Vehicular Technology Society, July. 2006.

[5] Hannes Hartenstein and Kenneth, P. Laberteaux, “VANET Vehicular Applications and Inter-Networking Technologies,” WILEY, pp. 299-363, Dec. 2009.

[6] Maxim Raya and Jean-Pierre Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security pp. 39-68, 2007.

[7] John R. Douceur, “The Sybil Attack,” Lecture Notes in Computer Science, LNCS 2429, pp. 251-260, 2002.

[8] Ahmed-Zaid, F. et. al., "Vehicle Safety Communications-Applications (VSC-A) Final Report: Appendix Volume 3 Security," National Highway Traffic Safety Administration, Sep. 2011.

[9] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: robust location privacy scheme for VANET,” IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1569-1589, 2007.

[10] J. Freudiger, M. Raya, “Mix-zones for location privacy in vehicular networks,” WiN-ITS, Aug. 2007.

[11] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications, pp. 8-15, Oct. 2006.

[12] National Institute of Standards and Technology, "FIPS 180-2, Secure Hash Standards, Federal Information Processing Standard (FIPS)", Publication 180-2, 2002.