http://dx.doi.org/10.14400/JDC.2015.13.9.297

# 차량간 보안 통신에서 융합 해시함수를 이용하여 공격에 안전한 통신방법 검증

이상준*, 배우식**
아주자동차대학 자동차디지털튜닝전공*, 아주자동차대학**

# Verification of a Communication Method Secure against Attacks Using Convergence Hash Functions in Inter-vehicular Secure Communication

**Sang-Jun Lee*, Woo-Sik Bae****
**Dept. of Automobile Digital Tuning, Ajou Motor College***
**Dept. of AIS Center, Ajou Motor College****

**요 약** 자동차에 정보기술 도입비율이 높아짐에 따라서 최근 스마트 카, 커넥티드 카로 일컬어지기 시작했다. 스마트자동차 시스템이 적용되어 외부 네트워크에서 차량과 접속하게 되면서 통신보안 위협 또한 증가하고 있다. 차량에 다양한 보안 위협에 대한 모의시험 결과로 관련된 취약성이 사회적 이슈와 기사화 되고 있으며, 자동차 융합 보안통신에 대한 연구가 활발히 진행되고 있다. 자동차 해킹이 일반적인 해킹보다 위험한 것은 운전자의 생명위협 및 사회적인 혼란을 야기할 수 있기 때문이다. 본 논문에서는 차량 대 차량, 차 내부 통신 등에 안전한 통신을 위해 해시함수, 난수, 공개키, 타임스탬프 및 Password 등을 이용하여 융합 프로토콜을 설계하였다. 정형검증 도구인 Casper/FDR을 이용하여 검증하였으며 제안한 프로토콜이 보안적으로 양호하게 동작되며 외부 공격자의 공격에 안전함을 확인하였다.

**주제어** : 차대차 보안프로토콜, 차량융합보안시스템, 차량인증프로토콜, Casper/FDR, 보안통신인증, 융합모델검증

**Abstract** The increase in applying IT to vehicles has given birth to smart cars or connected cars. As smarts cars become connected with external network systems, threats to communication security are on the rise. With simulation test results supporting such threats to Convergence security in vehicular communication, concerns are raised over relevant vulnerabilities, while an increasing number of studies on secure vehicular communication are published. Hacking attacks against vehicles are more dangerous than other types of hacking attempts because such attacks may threaten drivers' lives and cause social instability. This paper designed a Convergence security protocol for inter-vehicle and intra-vehicle communication using a hash function, nonce, public keys, time stamps and passwords. The proposed protocol was tested with a formal verification tool, Casper/FDR, and found secure and safe against external attacks.

**Key Words :** v2v Security protocol, Vehicular Convergence Security System, Vehicular Authentication protocol, Casper, Security authentication, Convergence Model Checking

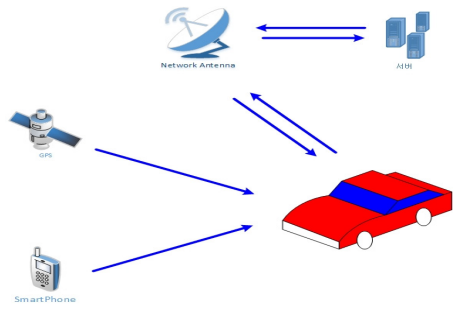
Received 25 July 2015, Revised 28 August 2015
Accepted 20 September 2015
Corresponding Author: WooSik Bae(Ajou Motor College)
First Author : SangJun Lee(Ajou Motor College)
Email: drbws@daum.net

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1. 서론

지능형 자동차(Intelligent Vehicle)가 최근 자동차 분야에서 많은 관심을 받고 있다. 자동차에 적용된 전기, 전자, 컴퓨터 제어기술이 발전하고 있고 자동차의 안전성과 효율성을 높이는 기술에 정보통신기술의 발전으로 현실화 되고 있다[1,2,3]. 아울러 정보통신과 시스템 및 네트워크가 결합한 자동차를 스마트 자동차, 커넥티드 자동차로 불리기도 한다. 스마트 자동차의 주요 기술으로는 자율주행기술, 안전기술 및 편의기술로 요약된다. 자율주행기술은 자동차 스스로 위험을 판단하고 주행 경로를 계획해 주행 조작을 최소화해서 스스로 안전주행이 가능한 자동차기술이다. 안전기술에는 사고 예방적인 측면의 안전기술과, 사고회피 기술, 충돌에 대한 피해 최소화 기술 등이다. 편의 기술로는 여러 가지 편의장치가 있겠지만 무엇보다 자동차가 움직이는 사무실이 되도록 하는 기술로 차내에서 전자우편 송수신, 화상회의 등의 업무를 처리하는 기술이라 할 수 있다[4,5]. 이러한 정보통신 기술과 자동차기술이 융합된 형태의 자동차가 미래 성장 동력으로 매우 주목받고 있는 상황이다[6,7]. 그러나 정보 플랫폼적인 스마트 자동차는 유, 무선 통신으로 자동차를 운영하게 되는데 통신구간에서의 보안 문제가 심각한 요소로 작용하고 있다[8]. 공격자의 해킹으로 인해 자동차를 제어함으로 탑승자의 프라이버시를 침해 할 수 있다. 또한 제동계통이나 속도제어 등으로 탑승자 및 주변에 생명의 위협까지도 가능하여 매우 위험한 상태에 놓이기도 한다. 최근 차량의 기능 안전성관련 국제규격인 ISO 26262가 제정되었으나 발전하는 정보기술개발에 적용하기에 미진한 상태이다[9].




[Fig. 1] Smart Car System

[Fig. 1]은 스마트 자동차의 개념으로 스마트폰으로 자동차의 상태를 확인 하거나 제어한다. 운행중 위치파악 등으로 GPS 신호를 받아 운행하며 차량의 정보를 수합하는 네트워크 기지국으로 나눠질 수 있다.

본 논문에서는 프로토콜 검증을 위해 정형검증 분야에서 사용하는 Casper/FDR[10,11,12,13,14] 도구를 실행하여 프로토콜을 검증 하였으며 자동차 통신시스템에서 안전한 프로토콜임이 증명되었다. 본 논문의 전체적인 구성은 다음과 같다. 2장에서는 관련된 연구로 자동차 보안 위협과 Casper/FDR 및 기 제안된 프로토콜에 대하여 알아본다. 3장에서는 상호 인증프로토콜을 제안하고 동작에 대한 상세한 이론적 확인을 하고, Casper/FDR을 이용하여 정형적인 실험 및 검증한다. 4장은 실험 결과 및 프로토콜의 안전성을 검증하고 최종적으로 5장에서 결론을 맺는다.

## 2. 관련연구

### 2.1 무선통신 보안위협

무선통신에서 일반적인 보안 위협은 차량 통신 보안 요구사항과 비슷하며 다음과 같다[15].

1) 인증 및 무결성 : 통신에서 디바이스가 정당한 소유자임이 확인되어야 하는데 이를 충족하기 위해 모든 디바이스는 유일한 ID를 가져야 한다.
2) 비밀성 : 무선 전송 통신에서 통신 디바이스 간 송·수신되는 데이터는 인증되지 않은 디바이스에 대하여 안정적으로 비밀성이 유지되어야 한다.
3) 익명 및 프라이버시 : 무선 통신에서 익명성이 만족되지 않으면 프라이버시 침해의 위험이 발생한다. 공격자가 차량의 정보를 확인할 경우 안전 등 심각한 문제가 발생할 수 있다.
4) 부인방지 : 데이터를 송신한 디바이스는 데이터 송수신 결과를 부인할 수 없도록 부인방지 기술이 적용 되어야 한다.

### 2.2 해시락 프로토콜

태그의 식별 값인 metaID가 고정되어있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송되었는지

확인할 수 있다. 그리고 리더와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 키를 획득한 후, 해시연산하고 metaID를 산출하여 인증을 받을 수 있다. 또한 제 3자가 고정된 metaID를 재전송함으로써 인증 받을 수 있으며, metaID가 식별자처럼 사용되기 때문에 스푸핑 공격 및 사용자 추적이 가능한 취약성이 있다[16].

## 3. 제안 프로토콜

본 논문에서는 보안성을 강화하기 위해 계산량을 증가 시켜 매 세션 바뀌는 난수와 변수 값을 이용하고 실시간과 패스워드 에이전트, 불 에이전트 값 및 해시함수를 적용하여 설계하였다. 데이터베이스에 적용되는 데이터 타입은 VARCHAR2 타입으로 보안적으로 안전하게 암호화 하여 저장되며, 데이터는 가변길이 최대 4000byte의 공간으로 사용한다. 본 실험은 실제 자동차에서 실험하지 않고 검증용으로 사용하는 프로그램을 이용함으로써 실제 적용 시 좀 더 많은 공격과 실험이 필요한 제약이 있다.

본 논문에서 사용하는 기호는 <Table 1>과 같다.

〈Table 1〉 Symbols and definition

| Symbols | Definition |
|---|---|
| Alice | Agent |
| BOB | Agent |
| DB | Database Server |
| H | Hash Function |
| i, j | Nonce |
| keyR, keyT | Session Key |
| pkdb | PublicKey |
| skdb | SecretKey |
| realAgent | Agent -> Bool |
| passwd | Agent x Agent -> password |

### 3.1 동작설명

단계별 자세한 설명은 다음과 같다.

◎ Step 1 : Alice → BOB

Alice는 BOB으로 부터 Query를 수신한 후 Alice에서 타임스탬프 Ta, 난수 i, 디바이스 BOB, 세션키 keyT 및 공개키 pkdb 값을 생성하고 변수 %enc에 각 값을 연접(concatenation)하여 BOB에게 전송한다. 이후 모든 세션에서 생성 값은 고유한 값이다. 타임스탬프의 사용으로 공격자가 공격할 시간을 만들어 주지 않는다.

◎ Step 2 : BOB → Server

Alice에서 수신한 BOB : Ta,i,{BOB,keyT}{pkdb} 값을 수신하여 리더가 가지고 있는 데이터와 Alice에서 수신한 값으로 BOB 값을 비교하여 확인한다. 상호 인증을 위한 기반데이터로 저장하며 정당한 BOB 인지 인증을 완료한다. 이후 다음의 값을 계산해 낸다. BOB이 계산한 Tb,i,{Alice,keyR}{pkdb},enc%{BOB,keyT}{pkdb},{passwd(Alice,BOB)}값을 데이터베이스서버로 전송한다.

◎ Step 3 : DB → BOB

BOB이 타임스탬프 값과 공개키 및 패스워드를 생성하여 연접후 전송한 Tb,i,{Alice,keyR}{pkdb},enc%{BOB,keyT}{pkdb},{passwd(Alice,BOB)} 값을 이용하여 BOB이 정상적으로 인증되었는지 그리고 Alice에 대하여 정당한 디바이스인지 확인후 데이터베이스 서버에서 계산한 j,keyT(+)keyR(+)H(BOB), Tb값을 생성한다 이때 해시연산은 $h_a(BOB) = h\int((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 형태로 연산되며 유일한 값이다. 타임스탬프의 확인 및 최종 연산된 j,keyT(+)keyR(+)H(BOB), Tb값을 BOB에게 전송한다.

◎ Step 4 : BOB → Alice

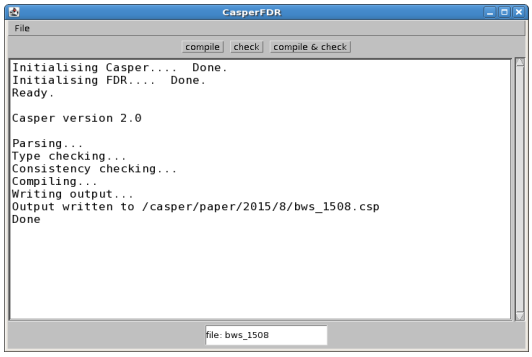
BOB은 데이터베이스서버에서 수신한 j,keyT(+)keyR(+)H(BOB), Tb 값을 상호인증하고 Alice : j,{BOB}{keyT}(+)H(BOB),Ta,{passwd(Alice,BOB)} 값을 생성한다. 데이터의 값을 해쉬 연산하는 방식은 다음과 같다. BOB, Alice 의 문자열에 대입하면 $h_a(BOB, Alice) = h\int((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 으로 j,{BOB}{keyT}(+)$h_a(BOB, x) = h\int((\sum_{i=0}^{k} x_i . a^i) \bmod p)$, Ta,{passwd(Alice,BOB)} 으로 계산되어 Alice에게 전송된다.

◎ Step 5 : Alice → BOB

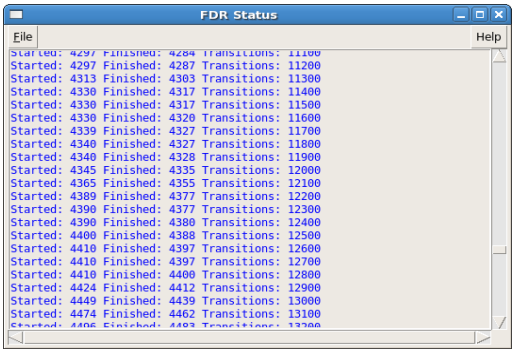
마지막으로 Alice는 BOB에게 Alice : j,{BOB}{keyT}(+)H(BOB),Ta,{passwd(Alice,BOB)} 값을 전송 받은 다음 Alice에서 계산한 값과 비교하여 확인되면 $h_a(keyT) = h((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ ,Ta,j로 해시연산 암호화한다. 타임스탬프와 난수를 연접하여 BOB에게 전송하여 태그의 인증 세션을 완료한다.

## 4. 실험결과

본 논문에서는 제안한 프로토콜의 검증을 위해 FDR 2.91 버전의 검증 도구를 사용하여 프로토콜의 교착상태, 안전성, 라이브락 등의 동작을 검증하였다. [Fig. 2]는 설계한 프로토콜을 CasperFDR 프로그램에 로딩 하여 오류 없이 CSP 형태로 변환이 완료된 상태이다.

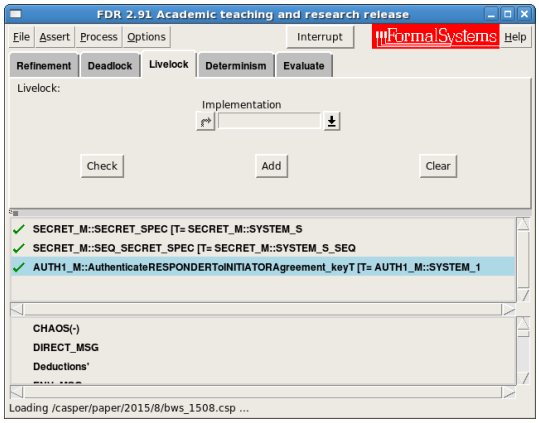



[Fig. 2] Verification setup and running




[Fig. 3] Status window displaying the verification is in progress

[Fig. 3] 은 제안한 프로토콜이 안전한지 각종 공격과 교착상태, 안전성 등의 상태를 단계별로 시험하는 상태창이다. 프로토콜에 취약점 또는 오류가 있을 경우 상태창의 내용을 확인하여 프로토콜을 수정할 수 있도록 메시지를 출력하여 준다. FDR 프로그램으로 프로토콜의 검증을 실행하여 검증한 결과 보안성이나 프로세스에 문제가 없으면 [Fig. 4]와 같이 좌측에 녹색 체크 아이콘이 출력되며 실험한 프로토콜이 안전함을 확인 할 수 있다.




[Fig. 4] Security verification results of the protocol

[Fig. 4]에는 3가지 검증결과를 나타내며 각각의 내용은 다음과 같다.

1)SECRET_M::SECRET_SPEC[T=SECRET_M::SYSTEM_S

제안한 프로토콜의 보안성 검증항목으로 프로토콜이 공격자의 공격에 안전함을 표기한다. 검증한 Agent간 전송되는 데이터 값과 난수, 암호, 해시락 및 세션키를 확인했으며 본 제안프로토콜은 안전하게 1번 항목을 완료하였다.

2)SECRET_M::SEQ_SECRET_SPEC[T=SECRET_M:: SYSTEM - S_SEQ

제안 프로토콜이 각 단계별로 문제없이 정상적인 프로세스로 동작했는지 검증한 결과이다. 본 논문에서 제안된 프로토콜은 각 단계별 암호화 인증 및 안전한 상태로 동작함이 검증되었다.

3)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_1

3)은 Responder와 Initiator가 서로 안전한 데이터 전송으로 상호 인증함에 문제가 없는지 검증하는 부분이다. 최종 결과 값과 같이 에이전트 간 보안적으로 안전하게 상호 인증됨을 검증하였다.

## 5. 결론

자동차 기술 동향이 스마트 자동차, 커넥티드 자동차 등으로 정보통신기술이 자동차에 도입되는 비중이 높아지고 있다. 그러나 통신구간에서의 취약성을 이용하여 해킹하거나 자동차를 임의로 조작하는 공격이 가능하여 심각한 문제로 인식되고 있다. 현재 자동차 소프트웨어 개발보안 표준, 자동차 소프트웨어 보안 인증 체계 구축, 자동차 보안 인력 양성 등이 부족하여 관련하여 보완이 무엇보다 중요하다고 할 수 있다.

본 논문에서는 자동차통신에서 보안 문제를 해결하기 위해 보안적으로 안전하고 효율적인 통신 프로토콜을 제안하였다. 정형검증 결과 보안 분야에서 안전한 통신 환경이 되도록 설계되었음이 검증되었다. 향후 교통 및 군사 분야에서 안전하게 통신할 수 있는 확장연구를 진행할 계획이다.

## REFERENCES


[1] Atallah, R.F.,Khabbaz, M.J.,Assi, C.M., Vehicular networking: A survey on spectrum access technologies and persisting challenges. Vehicular Communications, Vol. 2, Issue. 3, pp. 125-149, 2015.

[2] Zhu, X., Lu, Y., Zhu, X., Qiu, S., Lightweight and scalable secure communication in VANET. International Journal of Electronics, Vol. 102, Issue. 5, pp. 765-780, 2015.

[3] Hoque, M.A.,Hong, X.,Dixon, B., Efficient multi-hop connectivity analysis in urban vehicular networks. Vehicular Communications, Vol. 1, Issue. 2, pp. 78-90, 2014.

[4] Aiash M, Mapp G, Lasebae A, Phan R., A survey on authentication and key agreement protocols in heterogeneous networks. International Journal of Network Security & Its Applications, Vol. 4, No. 4, pp. 199-214, 2012.

[5] Keun-Ho Lee, A Security Threats in Wireless Charger Systems in M2M. Journal of the Korea Convergence Society, Vol. 4, No. 1, pp. 27-31, 2013.

[6] Seung-Hwan Kim, Keun-Ho Lee, User Authentication Risk and Countermeasure in Intelligent Vehicles. Journal of the Korea Convergence Society, Vol. 3, No. 1, pp. 7-11, 2012.

[7] WooSik Bae, Inter-device Mutual authentication and Formal Verification in M2M Environment. The Journal of Digital Convergence, Vol. 12, No. 9, pp. 219-224, 2014.

[8] Qi X., A new authenticated key agreement for session initiation protocol. International Journal of Communication Systems 2011; 25:47 - 54. DOI: 10.1002/dac.1286.

[9] ISO 26262, Road vehicles - Functional safety, Management of functional safety & Concept phase

[10] Aiash M, Mapp G, Lasebae A, Phan R, Loo J., A formally verified AKA protocol for vertical handover in heterogeneous environments using Casper/FDR. EURASIP Journal on Wireless Communications and Networking, Vol. 57, pp. 1-23, 2012.

[11] M. S. Han, W. S. Bae, Security Verification of a Communication Authentication Protocol in Vehicular Security System. Journal of Digital Convergence, Vol. 12, No. 8, pp. 229-234, 2014.

[12] W. S. Bae, Formal Verification of an RFID Authentication Protocol Based on Hash Function and Secret Code. Wireless Personal Communications An International Journal, Vol. 79, No. 4, pp. 2295-1609, 2014.

[13] G. Lowe. Casper: A compiler for the analysis of security protocols. User Manual and Tutorial. Version 1.12, 2009.

[14] Formal systems (Europe) Ltd.: Failures-Divergence Refinement. FDR2 User Manual, 2011.

[15] PRESERVE(PREparing SEcuRe VEhicle-to-X Communication Systems)Deliverable 1.1, Security

Requirements of Vehicle Security Architecture, 2011.

[16] Weis, S. et al., Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Security in Pervasive Computing, Vol. 2802, pp. 201-212, 2003.

**이 상 준(Lee, Sang Jun)**

- 1985년 2월 : 부산대학교 생산기계공학과(공학사)
- 1987년 2월 : 부산대학교 기계공학과(공학석사)
- 2000년 8월 : 충북대학교 기계공학과(공학박사)
- 1987년 2월 : 국방과학연구소(ADD) 연구원
- 1995년 3월 : 아주자동차대학 자동차계열 교수(현)
- 관심분야 : 자동차섀시, 기계설계, 기계설비
- E-Mail : lsjune@motor.ac.kr

**배 우 식(Bae, Woo Sik)**

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2012년 2월 : 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템
- E-Mail : drbws@daum.ner