http://dx.doi.org/10.14400/JDC.2015.13.4.205

자동차 보안시스템에서 장치간 상호인증 및 정형검증

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

Inter-device Mutual Authentication and Formal Verification in Vehicular Security System

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

요 약 자동차산업의 발전과 함께 M2M(Machine-to-Machine)통신이 자동차 산업분야에서 많은 관심이 되고 있다. M2M은 기상, 환경, 물류, 국방, 농.축산 등에서 사용하기 시작하여 장비들이 자동으로 상황에 맞추어 통신을 하고 상황에 맞는 동작을 함으로써 운영해가는 시스템이다. 자동차에서도 차량내부 장치 간, 차대 차, 차와 교통시설물, 차와 주변의 환경 등에 적용되고 있다. 그러나 통신시스템의 특성상 전송구간에서 공격자의 공격에 대한 문제가 있으며 자동차의 운행, 제어계통 및 엔진제어 등에 공격자의 공격이 진행되면 안전에 심각한 문제가 발생하게 된다. 따라서 디바이스 간 보안통신에 대한 연구가 활발히 진행되고 있다. 본 논문에서는 차량의 디바이스간 안전한 통신을 위해 해시함수 및 수학적 복잡한 공식을 이용하여 프로토콜을 설계하였으며 프로토콜 정형검증 도구인 Casper/FDR을 이용하여 실험하였으며 제안한 프로토콜이 각종 공격에 안전하게 동작되며 실제 적용할 때 효과적임을 확인하였다.

주제어 : M2M 보안 프로토콜, 차량보안시스템, 차량인증프로토콜, Casper, 보안통신인증, 모델검증

Abstract The auto industry has significantly evolved to the extent that much attention is paid to M2M (Machine-to-Machine) communication. In M2M communication which was first used in meteorology, environment, logistics, national defense, agriculture and stockbreeding, devices automatically communicate and operate in accordance with varying situations. M2M system is applied to vehicles, specifically to device-to-device communication inside cars, vehicle-to-vehicle communication, communication between vehicles and traffic facilities and that between vehicles and surroundings. However, communication systems are characterized by potential intruders' attacks in transmission sections, which may cause serious safety problems if vehicles' operating system, control system and engine control parts are attacked. Thus, device-to-device secure communication has been actively researched. With a view to secure communication between vehicular devices, the present study drew on hash functions and complex mathematical formulae to design a protocol, which was then tested with Casper/FDR, a tool for formal verification of protocols. In brief, the proposed protocol proved to operate safely against a range of attacks and be effective in practical application.

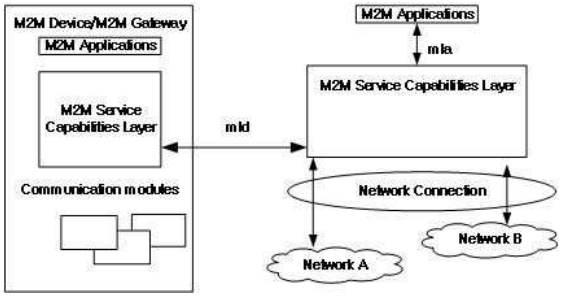
Key Words : M2M Security protocal, Vehicular Security System, Vehicular Authentication protocol, Casper, Security authentication, Model Checking

Received 6 February 2015, Revised 16 March 2015
Accepted 20 April 2015
Corresponding Author: WooSik Bae(Ajou Motor College)
First Author : SangJun Lee(Ajou Motor College)
Email: drbws@daum.net

ISSN: 1738-1916

1. 서론

디바이스와 디바이스간 자동 통신으로 M2M (Machine-to-Machine) 통신의 연구가 활발히 진행되고 있다[1,2]. 이는 대부분의 산업에 적용 되어 사람이 확인 및 조작하기 어려운 군사 감시 분야, 농·축산업, 기상관측, 안전, 환경, 자동차, 공업 등에 광범위 하게 사용되고 있다[3,4]. 차량에서도 차 대 차, 차와 장비, 차와 주변 사물, 차량 내부의 장비간 통신에 사람이 관여 하지 않고 자동으로 동작한다. 그러나 M2M 통신에서 무선구간의 통신의 경우 공격자의 공격에 취약한 문제가 있다[5]. 차량에서 볼 때 이는 생명을 위협할 수 있는 공격으로 보안성의 만족은 매우 중요한 문제가 되어있으며 많은 연구자에 의해 활발한 연구가 이루어지고 있다. 그러나 대부분의 연구가 정리증명(Theorem Proving) 단계에 머물러 있어 설계과정에서 생각지 못했던 문제가 발생하다. 실제 시스템에 적용할시 적용이 불가 하거나 관련된 많은 연구가 요구되고 있는 실정이다[6,7,8]. 차량의 기능 안전성의 국제규격인 ISO 26262가 제정되었으나 아직까지 장비간 보안위협에 대해서는 미진한 상태이다[9].



[Fig. 1] M2M system framework

[Fig. 1]은 M2M 서비스를 위한 시스템의 기본 구조를 나타낸다. M2M 서비스 기능(Service Capability)은 외부에서 다양한 방식으로 접근 가능한 인터페이스의 조합을 통해 코어 네트워크의 기능들을 사용하며 여러 개의 코어 네트워크와 인터페이스를 통해 접속할 할 수 있다[10]. M2M 애플리케이션은 각각 Device Application, Gateway Application, Network Application을 나타낸다.

M2M 통신에서는 디바이스·게이트웨이 도메인과 M2M 네트워크 도메인으로 구분된다. M2M 통신 참조 모델에서는 각각의 구성 요소 간의 통신을 위한 개방형 인터페이스를 제공해야 한다[11].

본 논문에서는 최근 정형검증 분야에서 많이 사용하는 Casper/FDR[12,13] 도구를 사용하여 제안한 프로토콜을 검증실험 하였으며 M2M 시스템에서 안전한 통신 프로토콜임이 증명되었다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 자동차 보안 위협과 CASPER/FDR 및 확장된 해시락 프로토콜에 대하여 알아본다. 3장에서는 인증프로토콜을 제안하고 동작에 대한 자세한 설명을 하고, Casper/FDR을 이용하여 실험 검증한다. 4장에서 실험 결과의 안전성을 확인하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 자동차 보안위협

차량 통신 보안요구사항은 다음과 같다[14].

1) 인증 및 데이터 무결성 : 차량 통신에서 개체가 자신이 정당한 소유자임이 확인되어야 하는데 이를 충족하기 위해 모든 개체는 유일한 ID를 가져야 한다.
2) 비밀성 : 차량통신에서 인증된 통신 개체 간 송·수신되는 데이터는 인증되지 않은 개체에 대하여 비밀성이 유지되어야 한다.
3) 익명 및 프라이버시 : 차량 통신에서 익명성이 결여되면 프라이버시 침해의 위험이 존재한다. 따라서 프라이버시 보호방안이 제공되지 않는다면, 공격자가 차량의 주행, 위치, 영상 등 정보를 확인하며 심각한 문제가 발생할 수 있다.
4) 부인방지 : 데이터를 송신한 개체는 데이터 송신 사실을 부인할 수 없어야 한다.

2.2 CASPER/FDR

Casper(a Compile for the Analysis of Security Protocols)는 CSP(Communication Sequential Process) 방식으로 프로토콜을 명세하기 쉽게 개발 되어진 컴파일러이다[15]. 명세 방법은 변수타입 및 함수선언, 통신 에이전트의 초기상태, 에이전트 간의 메시지교환 순서, 검증하고자 하는 보안 속성선언, 실제 데이터타입 및 이름

을 선언한다. 이어서 프로토콜에서 사용하는 함수선언, 통신 에이전트의 초기상태표현, 공격자의 초기상태정보 등을 명세 한다. 프로그램을 실행 시키면 자동으로 CSP 문서로 변환시켜 준다. 이렇게 변환된 CSP 문서를 FDR(Failure Divergence Refinements) 프로그램을 이용하여 보안성과 인증속성과 같은 보안속성을 만족하는지 검증하며 FDR 에서는 safety 검증, deadlock 검증, livelock 검증을 확인하며 보안상 취약점이 발견 되면 어떤 공격 시나리오가 가능한지 보여주어 취약점 분석이 쉽도록 되어있다. 아울러 FDR에서는 추적모델, 실패모델, 실패/분기모델을 지원한다[16].

2.3 확장된 해시락 프로토콜

해시락 기법에서 추적이 가능한 부분을 보완한 프로토콜이다. 태그는 사용자에 의한 질의에 대하여 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 식별 가능해야 하는 방식이다. 태그에 일방향 해시 함수연산이 가능해야 하며 난수발생 연산이 되어야 한다. 태그를 풀림 상태가 되기 위해서는 다음과 같은 프로토콜로 동작한다[17].

① 최초 리더 R은 태그 T에게 무선으로 질의를 보낸다.
② T는 자체적으로 랜덤 한 난수를 생성하여, hash(ID || R)값을 계산한다.
③ 계산된 값을 T는 R에게 (R, hash(ID || R))을 전송한다.
④ R은 알고 있는 IDi값에 대해 hash(IDi || R)을 연산한다.
⑤ 만약 hash(IDi || R) == hash(ID || R)을 만족하는 IDi 를 찾으면, R은 T에게 비로소 IDi를 전송한다.
⑥ IDi, ID가 일치하면, T는 잠긴 상태에서 풀림으로 된다. 난수를 사용하여 태그에서 리더로 전송되는 데이터가 매 세션마다 다른값으로 전송되므로 스푸핑 공격에는 강하지만 IDk 값이 노출되는 문제로 위치 추적이 가능하며 리더를 공격하는 공격자가 r,H(IDk || r)을 도청하여 재전송 할 경우 정당한 태그로 위장하여 재전송공격에도 취약한 문제가 있다.

3. 제안 프로토콜

본 논문에서는 매 세션 바뀌는 난수와 변수 값을 이용하고 실시간 에이전트 값 및 해시함수를 기반으로 설계하였다. 기호의 정의는 <Table 1>과 같다.

<Table 1> Symbols and definition

Symbols	Definition
Tag	Agent
Reader	Agent
Server	Server
H	Hash Function
x, k, y	Nonce
a1, a2	Session Key
PK	PublicKey
SK	SecretKey
realAgent	Agent -> Bool

3.1 동작설명

단계별 자세한 설명은 다음과 같다.

◎ Step 1 : Tag → Reader

디바이스 Tag는 리더로 부터 Query를 수신한 후 Tag에서 x, sk 및 Reader(+)y 값을 생성하고 변수 %m1에 각 값을 연접(concatenation)하여 Reader에게 전송한다. 이때 생성 값은 고유한 값으로 다른 디바이스에서는 생성할 수 없는 값이다.

◎ Step 2 : Reader → Server

Tag에서 수신한 Reader : {x}{sk1}%m1,Reader(+)(y) 값을 수신하여 리더가 계산한 (k)(+){m1%{x},sk1,k}{sk2},H(Reader,y) 값을 서버로 전송한다.

◎ Step 3 : Server → Reader

리더가 전송한 (k)(+){m1%{x},sk1,k}{sk2},H(Reader,y) 값을 이용하여 서버에서 계산한 H(Tag,x),{x,{k}{sk1}%m2}{sk2},H(S,Reader) 값을 생성한 후 리더에게 전송한다.

◎ Step 4 : Reader → Tag

Reader은 데이터베이스서버에서 수신한 H(Tag,x),{x,{k}{sk1}%m2}{sk2},H(S,Reader) 값을 인증하고 Tag : m2%{k}{sk1},{x}{k},H(Reader,Tag) 값을 생성하는데 이

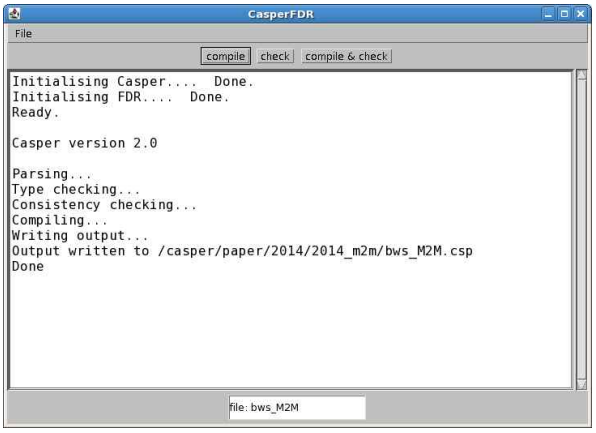
때 고정 길이의 데이터를 해쉬 하는 방식은 다음과 같다. Reader, Tag 의 문자열에 대입하면 $h_a(Reater, Tag) = h\int((\sum_{i=0}^{k} x_i.a^i) \bmod p)$ 으로 $h_a(Tag,x) = h\int((\sum_{i=0}^{k} x_i.a^i) \bmod p)$, {x,{k}{sk1}{k}{sk1}, {x}{k} $h_a(Reader, Tag) = h\int((\sum_{i=0}^{k} x_i.a^i) \bmod p)$ 으로 계산되어 Tag에게 전송된다.

◎ Step 5 : Tag → Reader

마지막으로 Tag는 Reader에게 Tag : m2%{k}{sk1}, {x}{k}, H(Reader,Tag)값을 전송 받은 다음 태그에서 계산한 값과 확인하여 확인되면 자신의 ID를 $h_a(tag,k) = h((\sum_{i=0}^{k} x_i.a^i) \bmod p)$ 로 해시연산 암호화하여 Reader에게 전송하여 태그의 인증 세션을 완료한다. 이후 세션을 완료하며 안정적으로 통신을 진행한다.

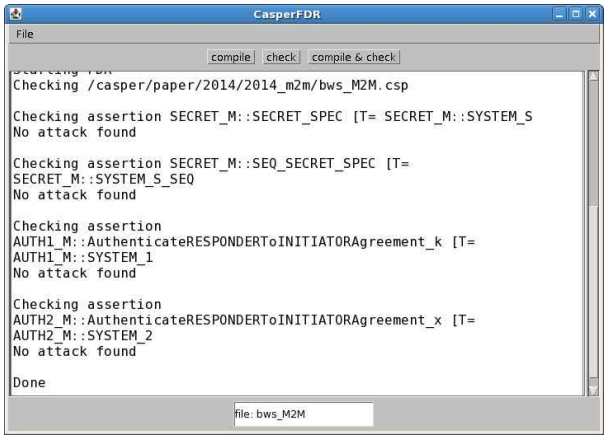
4. 실험결과

본 논문에서는 연구용 FDR 2.91 버전의 모델검증 프로그램을 사용하여 설계한 자동차 보안 M2M 프로토콜의 안전성, 교착상태, 라이브락 등의 동작을 검증하였다. [Fig. 2]는 소스 파일을 로딩하여 기본적인 오류 없이 CSP 소스로 변환진행이 완료된 상태이다.



[Fig. 2] Verification set-up and running

검증이 완료 되면 [Fig. 3]과 같이 각 공격에 대해 안전하다는 결과를 출력하였으며 안전하게 마무리 되었다. 본 논문에서 제안한 인증프로토콜을 Casper/FDR 프로그램을 실행하여 보안프로토콜의 보안성을 검증한 결과 [Fig. 3]와 같이 모든 보안속성에 대한 만족함이 확인되었다.



[Fig. 3] Security verification results of the protocol

[Fig. 3]에는 4가지 검증결과가 확인되며 각 결과의 내용은 다음과 같이 분석된다.

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

프로토콜의 보안성 확인 부분으로 제안한 프로토콜이 공격자에게 안전함을 나타낸다. 검증한 Agent간 통신과 데이터 값 과 세션키의 보안성이 안전한지 확인하였다.

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

시스템에서 각 스텝별로 정상적인 프로세스로 동작했는지 확인한 결과로써 본 논문에서 제안된 프로토콜을 확인한 결과 안전한 프로세스로 동작됨을 확인하였다.

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

4)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_x[T=AUTH2_M::SYSTEM_2

3), 4)는 k, x 의 Responder와 Initiator가 서로 정상적인 통신으로 상호 인증할 수 있는지 검증하는 부분으로

결과 값과 같이 에이전트 간 안전하게 상호 인증함을 확인하였다.

5. 결론

최근 자동차 통신시스템에서 디바이스간의 안전한 통신을 위해 뒤늦게 보안 분야에 많은 연구가 이루어지고 있다. 향후 각종 산업 분야에서 M2M 통신은 필연적으로 사용될 예정이다. 그러나 M2M 통신에서 무선으로 통신이 이루어지는 구간의 취약성을 이용하여 악의 적인 공격자의 공격에 심각한 문제가 발생할 수 있다. 이는 자동차 분야에서는 생명과도 직결된 문제로 중요한 분야이다. 본 논문에서는 자동차 M2M 통신에서 보안 문제를 해결하기 위해 보안적으로 안전하고 효율적인 통신 프로토콜을 제안하였다. 해시 연산과, 공개키 및 비밀키를 사용하였으며 $h_a(x) = h \int ((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 연산을 기본으로 설계하여 상호 인증을 제공하고 있다. Casper/FDR 정형검증 결과 각 항목에서 안전함이 확인되었으며 불필요한 계산을 하지 않고 효율적으로 동작을 종료하였다. 자동차 보안 분야에서 안전한 통신 환경이 되도록 설계되었음이 검증되었다. 향후 군사 및 의료장비 분야에서 안전하게 통신할 수 있는 확장연구를 진행할 계획이다.

REFERENCES

[1] V. Galetic et al., Basic principles of Machine-to-Machine communication and its impact on telecommunications industry. in Pro. of 34th International Convention on Information and Communication Technology, Electronics and Microelectronics, pp. 89-94, 2011.

[2] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, M2M: from mobile to embedded internet. IEEE Communications Magazine, Vol. 49, No. 4, pp. 36-43, 2011.

[3] G. Wu, S. Talwar, K. Johnsson, N. Himayat and K.D. Johnson, M2M: From mobile to embedded internet. IEEE Communications Magazine, Vol.49, No.4, pp. 36-43, 2011.

[4] ETSI, Machine-to-Machine communications (M2M); M2M service requirements. TS 102 689 V1.1.2., 2011.

[5] Huy Hoang Ngo, XianpingWu, Phu Dung Le and Bala Srinivasan, An individual and group authentication model for wireless network services. Journal of Convergence Information Technology, Vol.5, No.1, pp. 82-94, 2010.

[6] Chen C, He D, Chan S, Bu J, Gao Y, Fan R., Lightweight and provably secure user authentication with anonymity for the global mobility network. International Journal of Communication Systems 2010; 24:347 - 362. DOI:10.1002/dac.1158.

[7] 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.

[8] You I, Lee J-H, Kim B, Ilsun Y, Jong-Hyouk L, Bonam K. caTBUA: context-aware ticket-based binding update authentication protocol for trust-enabled mobile networks. International Journal of Communication Systems 2010;23:1382 - 1404. DOI: 10.1002/dac.1113

[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 2012.

[11] ETSI, Machine to Machine Communications (M2M); M2M functional architecture. ETSI, TS 102 690, DEC, 2011.

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

[13] Formal systems (Europe) Ltd.: Failures-Divergence Refinement. FDR2 User Manual. Available from:

http://www.fsel.com/documentation/fdr2/fdr2manual.pdf [Accessed 19 August 2011]

[14] PRESERVE(PREparing SEcuRe VEhicle-to-X Communication Systems)Deliverable 1.1, Security Requirements of Vehicle Security Architecture. June. 2011.

[15] Ryan P, Schneider S, Goldsmith M, Lowe G, Roscoe AW., The Modelling and Analysis of ecurity Protocols.PEARSON Ltd.: Edinburgh Gate. UK, 2010

[16] 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.

[17] Weis, S. et al., Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, 2003.

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.net

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 ~ 현재 : 아주자동차대학 자동차계열 교수
- 관심분야 : 자동차섀시, 기계설계, 기계설비
- E-Mail : lsjune@motor.ac.kr