http://dx.doi.org/10.14400/JDC.2014.12.9.219

M2M 환경에서 장치간 상호 인증 및 정형검증

배우식
아주자동차대학

Inter-device Mutual authentication and Formal Verification in M2M Environment

WooSik Bae
Dept. of AIS Center, Ajou Motor College

요 약 최근 무선통신 시스템의 기술이 발전함으로 M2M(Machine-to-Machine)이 산업분야에서 관심이 되고 있다. 기기간 통신인 M2M은 재난, 안전, 건설, 보건복지, 기상, 환경, 물류, 문화, 국방, 의료, 농.축산 등 사람의 접근이 어려운 공간 등에 설치되어 운용된다. 이는 사람을 대신해 장비들이 자동으로 상황에 맞추어 통신을 하고 어느 정도의 조치는 자동으로 취해지도록 함으로써 사람을 대신한 정보 관리 및 장비 운영을 할 수 있다. M2M이 디바이스간 통신이 무선으로 이루어지는 경우 공격자의 공격에 노출되어 운영되는 보안적 문제로 정당한 장치인지 상호인증 등 적절한 보안이 필요하다. 관련하여 최근 보안적으로 안전한 많은 프로토콜이 연구 되고 있으며 본 논문에서는 M2M 보안문제를 해결하기 위하여 SessionKey, HashFunction, 및 Nonce 를 적용하였으며 보안취약성을 보완한 안전한 프로토콜을 제안한다. 제안프로토콜을 기존의 대부분의 연구처럼 수학적 정리증명으로 안전함을 주장하지 않고 Casper/FDR을 이용하여 정형검증 하였으며 실험결과 제안프로토콜이 안전함이 확인되었다.

주제어 : M2M 보안시스템, 인증프로토콜, Casper, 보안인증, 모델검증

Abstract In line with the advanced wireless communication technology, M2M (Machine-to-Machine) communication has drawn attention in industry. M2M communication features are installed and operated in the fields where human accessibility is highly limited such as disaster, safety, construction, health and welfare, climate, environment, logistics, culture, defense, medical care, agriculture and stockbreeding. In M2M communication, machine replaces people for automatic communication and countermeasures as part of unmanned information management and machine operation. Wireless M2M inter-device communication is likely to be exposed to intruders' attacks, causing security issues, which warrants proper security measures including cross-authentication of whether devices are legitimate. Therefore, research on multiple security protocols has been conducted. The present study applied SessionKey, HashFunction and Nonce to address security issues in M2M communication and proposed a safe protocol with reinforced security properties. Notably, unlike most previous studies arguing for the security of certain protocols based on mathematical theorem proving, the present study used the formal verification with Casper/FDR to prove the safety of the proposed protocol. In short, the proposed protocol was found to be safe and secure.

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

Received 10 July 2014, Revised 23 August 2014
Accepted 20 September 2014
Corresponding Author: WooSik Bae(Ajou Motor College)
Email: drbws@daum.net

ISSN: 1738-1916

1. 서론

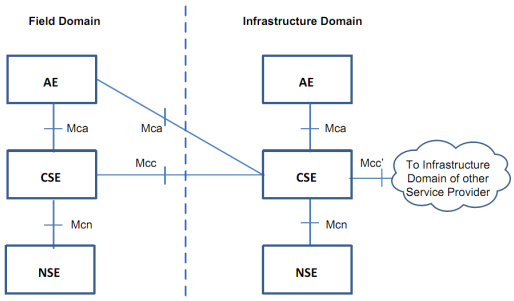
최근 장비와 장비간에 지능적으로 동작하는 사물지능통신에 많은 연구가 이루어지고 있다. M2M(Machine-to-Machine) 통신은 사람의 개입 없이 동작되며 사람이 직접 확인점검하기 어려운 분야 또는 단순반복적인 분야, 군사용 등 위험한 각종 산업분야에서 사용되고 있다. M2M 통신시스템은 정보를 전송하고 교환함으로 고장진단, 수리, 각종 모니터링, 정보의 수집 등 산업 전반에 광범위하게 이용할 수 있다[1,2,3,4,5]. 그러나 디바이스 간의 통신을 위해 무선통신을 하는 경우 공격자에 의해 전송데이터를 도청, 임의적 변경, 삭제, 프라이버시 등의 문제가 발생할 수 있으며 보안적으로 많은 위험이 존재할 수 있다. 이와 관련하여 많은 연구자들이 M2M 네트워크의 통신프로토콜을 활발히 연구하고 있다. 그러나 대부분의 연구가 수학적인 논리식을 사용하여 시스템과 시스템상의 요구되는 특성에 대하여 논리식으로 증명하는 방법으로 제안되고 있다. 이를 정리증명(Theorem Proving)이라 하는데 간혹 설계과정에서 생각하지 못했던 부분의 취약성이 생기며 실제 시스템에 적용시 많은 시간과 후속 실험이 요구된다[6,7,8].

본 논문에서는 기존의 프로토콜 제안의 문제를 보완하기 위해 정형기법을 사용하였으며 이는 수학적 또는 논리적으로 표현하는 정형명세(formal specification) 과정과 명세된 내용이 보안적 요구사항을 만족하는지 증명하는 과정으로 정형검증(formal verification)을 실시하여 제안 프로토콜을 검증한다. 본 논문에서는 모델검사기법으로써 효율성을 인정받고 있는 Casper[9]와 FDR[10]을 이용하여 제안한 프로토콜이 보안상으로 안전한지를 검증한다. 본 논문의 구성은 다음과 같다. 2장에서 관련 연구로 M2M 통신 등에 대하여 알아보고 이후 3장에서 제안보안프로토콜을 명세한 후 4장에서 보안적으로 안전한지 검증 실험한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 M2M 통신의 구조

M2M 통신 기술은 다양한 장치 및 장비에 유선이나 무선통신 모듈을 장착하여, 통신・방송・인터넷 인프라를 인간 대 인간 중심에서 인간 대 사물, 사물대 사물 간 영역으로 확대하는 기술이다. 이는 사람의 개입 없이 사물 간 통신을 통해 정보를 수집, 가공, 처리하여 상호 전달하는 기술로써 RFID/USN 기술의 발전으로 응용영역을 확장 하고 있다[3,4].



[Fig. 1] oneM2M Functional Architecture

[Fig. 1]은 oneM2M 의 기본적인 아키텍처를 위한 기능구조를 나타내었으며 응용 엔티티(Application Entity), 공통서비스 엔티티(Common Services Entity), 네트워크 서비스 엔티티(Network Services Entity) 로 구성된다[11].

2.2 CASPER/FDR

CSP(communication Sequential Process)로 프로토콜을 명세하기 쉽게 개발 되어진 컴파일러로써 Casper에서는 일정한 방식에 맞추어 자동으로 생성된다. Casper(a Compile for the Analysis of Security Protocols)[9]는 기존의 CSP[12] 언어를 이용한 정형명세 과정에서 정형적 설계방법에 서투른 보안프로토콜 설계자에게는 매우 복잡한 명세 언어이기 때문에 작은 실수가 있어도 오류가 생겨 설계 및 분석을 어렵게 진행하는 단점이 있었다. 이를 개선하기 위해 보안프로토콜의 행위를 간략히 설계할 수 있도록 개발된 프로그램이 Casper이다.

Casper에서 생성된 CSP 문서를 FDR(Failure Divergence Refinements) 프로그램을 이용하여 보안성과 인증속성과 같은 보안속성을 만족하는지 검증한다. FDR 에서는 safety 검증, deadlock 검증, livelock 검증을 확인하며 보안상 취약점이 발견되면 어떤 공격시나리오가 가능한지 보여주어 취약점 분석이 쉽도록 되어있다.

또한 추적모델(trace model), 실패모델(failure model), 실패/분기모델(failure/divergence model) 등을 지원한다.

1) 추적모델(trace model)
검증 프로세스는 행위에 의해 유한 순서 집합이며, P 프로세스가 Q 프로세스의 전체적 행위를 포함할 때 $P \sqsubseteq TQ$ 라고 표기한다.
$P \sqsubseteq TQ \triangleq traces(Q) \subseteq traces(P)$

2) 실패모델(failure model)
검증 값의 교착상태를 표현하며, 다음과 같이 나타낸다.
$P \sqsubseteq FQ \triangleq failures(Q) \subseteq failures(P)$

3) 실패/분기 모델(failure/divergence model)
실패/분기 모델은 교착 상태이고 라이브락 상태인 경우를 나타내며, 다음과 같이 표현한다.
$P \sqsubseteq FDQ \triangleq failures(Q) \subseteq failures(P) \wedge$ divergences(Q)$\subseteq$ divergences(P)

3. 제안 프로토콜

M2M 디바이스는 유선 및 무선 통신을 이용하여 게이트웨이 도메인과 네트워크 도메인 사이에 정보를 송.수신 한다. 이 통신 구간에 다양한 보안위협이 있으며 공격자의 공격 등 보안위협으로부터 안전한 통신환경을 제공하고자 본 논문에서는 키 인증과 해시함수를 기반으로 설계 및 실험하였다. 세션간 전송되는 데이터는 매 세션 암호화 및 복잡한 공식에 의해 바뀌어 전송데이터가 다르다. 아울러 세션키 및 난수를 적용하여 공격자가 도청한 정보를 가지고 다른 용도로 이용하거나 재생공격을 할 수 없으며 스푸핑공격, 재전송공격, 위치추적, 도청공격, 트래픽 분석 등에 안전하다. 제안 프로토콜에 사용할 기호의 정의는 <Table 1>과 같다.

〈Table 1〉 Symbols and definition

Symbols	Definition
Tag	Agent
Reader	Agent
S	Server
H	Hash Function
x, k, y	Nonce
sk1, sk2	Session Key
Vector1, Vector2	Vectors
||	Concatenation

3.1 동작설명

단계별 자세한 설명은 다음과 같다.

◎ Step 1 : Tag → Reader
디바이스 Tag는 애플리케이션 리더로부터 Query를 수신한 후 Tag에서 x, sk 및 Reader 값을 생성하고 변수 %Emc에 각 값을 연접(concatenation)하여 Reader에게 전송한다. 이때 생성 값은 고유한 값으로 다른 디바이스에서는 생성할 수 없는 값이다.

◎ Step 2 : Reader → SERVER
Tag에서 전송한 {x}{sk1}%m1,Reader 값을 수신하여 리더가 계산한 {m1%{x}{sk1},sk2,k}{sk2},H(Reader) 값을 데이터베이스서버로 전송한다.

◎ Step 3 : Server → Reader
리더에게서 전송된 {m1%{x}{sk1}, sk2,k}{sk2}, H(Reader) 값을 이용하여 데이터베이스서버에서 계산한 H(Tag),{x,{k}{sk1}%m2}{sk2},H(S) 값을 생성한 후 리더에게 전송한다.

◎ Step 4 : Reader → Tag
Reader은 데이터베이스서버에서 수신한 H(Tag), {x,{k}{sk1}%m2}{sk2},H(S) 값을 인증하고 m2%{k}{sk1}, {x}{k},H(Reader) 값을 생성하는데 이때 고정 길이의 데이터를 해쉬 하는 방식은 다음과 같다.

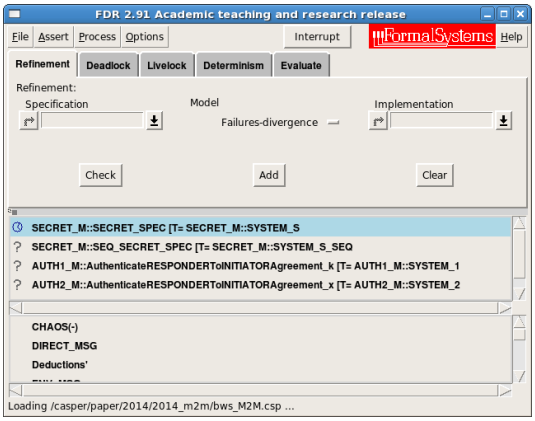
$h_a(\overline{x}) = h \int ((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 방식으로 계산되어 Tag에게 전송된다.

◎ Step 5 : Tag → Reader

마지막으로 Tag는 Reader에게 m2%{k}{sk1},{x}{k}, H(Reader)값을 전송 받은 이후 태그에서 생성한 값과 비교하여 확인되면 자신의 ID를 H(Tag, Reader)로 해시연산 암호화하여 Reader에게 전송함으로 태그에서의 인증 세션을 완료한다. 이후 Reader는 Tag에서 전송되어온 값을 데이터베이스서버에 전송하게 되면 저장되어 있는 Tag의 해쉬된 값을 확인 하게된다. 정상적인 확인이 완료되면 해쉬된 코드와 Tag코드를 확인 할 수 있음으로 확인세션을 완료하며 이후 안정적인 통신을 진행한다.

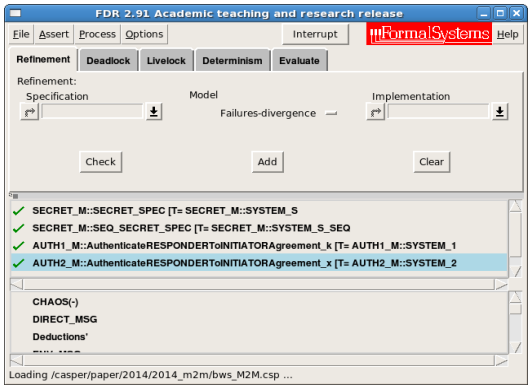
4. 실험결과

연구용 FDR 2.91 버전의 모델검증 프로그램을 사용하여 본 논문에서 설계한 M2M 프로토콜의 안전성, 교착상태, 라이브락 등의 동작을 검증하였다. [Fig. 2]는 소스 파일을 로딩하여 기본적인 오류없이 실행하고 있는 상태이다.



[Fig. 2] Verification set-up and running

검증이 완료 되면 녹색 √표시로 바뀌며 이는 검증결과 안전하다는 의미이다. 본 논문에서 제안한 인증프로토콜을 FDR 프로그램을 실행하여 보안프로토콜을 검증한 결과 [Fig. 3]와 같이 모든 보안속성에 대한 만족함이 확인되었다.



[Fig. 3] Security verification results of the protocol

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

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

프로토콜의 보안성 확인 부분으로 메시지 앞의 녹색 체크표시는 제안한 프로토콜이 공격자에게 노출되지 않았음을 나타낸다. 검증한 Agent간 통신과 데이터 값 과 세션키의 보안성이 안전한지 확인하였다.

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

이 항목은 프로토콜이 시스템에서 온전한 프로세스로 동작했는지 확인한 결과로써 본 논문에서 제안한 프로토콜은 안전한 프로세스로 실행함을 확인하였다.

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

3)은 k, x 의 Responder와 Initiator가 서로 상호 인증할 수 있는지 확인하는 부분으로 에이전트 간 안전하게 인증함을 확인하였다.

5. 결론

M2M은 USN 기술발전으로 무선 분야에서도 많은 연구와 적용이 되고 있다. 사용범위도 경비, 기상, 환경, 국

방, 의료 등 그 범위가 광범위하게 사용되고 있다. 그러나 M2M 시스템의 운용 및 제어에 외부의 공격자가 개입 된다면 보안적으로 심각한 문제를 일으킬 수 있다. 보안문제를 해결하기 위해서 암호프로토콜 등으로 보안적 안전성을 확보하는 다양한 연구가 많은 연주자에 의해 진행중이다. 본 논문에서는 해시함수, 난수, 세션키를 이용하여 설계 및 실험하였으며 해시락 연산의 방식과 함께 난수 및 세션키를 적용하여 각 세션마다 모두 다른 값을 전송하며 아울러 전송데이터를 암호화함으로 줄여 전송함으로써 전송 효율성을 높였다. 이를 Casper 언어로 명세한 후 제안 프로토콜이 FDR Tool의 보안속성을 만족하는지 검증을 실시하였다. 검증결과 재생공격, 중간자공격, 가장공격, safety 검증, Deadlock검증, livelock 검증 등 FDR에서 제공하는 모든 보안적인 측면에서 만족함을 보였다. 본 실험의 결과로 앞으로 더욱더 복잡하고 강력한 함수를 이용하여 M2M 디바이스에 적용할 수 있는 보안적으로 안전하고, 효과적인 프로토콜을 연구 및 검증함으로 의료, 국방용 등에 사용할 프로토콜의 설계를 진행할 예정이다.

REFERENCES

[1] J. S. Song, “M2M Standards and Technology Trends,” TTA Journal, Vol.150, pp.84-89, 2013. 11.

[2] C. S. Pyo, “M2M Techonolgy and Its Standardization Trends, oneM2M 2013 Seoul International Conference, 2013. 06

[3] G. Wu, S. TalwReader, 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] Huy Hoang Ngo, XianpingWu, Phu Dung Le and Bala Srinivasan, “An individual and group authentication model for wireless network services,” JCIT: Journal of Convergence Information Technology, vol.5, no.1, pp.82-94, 2010.

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

[6] K. Oh, T. Kim, and H. Kim, “Implementation of publickey-based key distribution in wireless sensor network,” in Proc. KOSBE, , pp. 95-98, Seoul, Korea, Feb. 2008

[7] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, “Towards viable certificate-based authentication for the Internet of Things,” in Proc, ACM HotWiSec ‘13, pp. 37-42, Budapest, Hungary, Apr. 2013

[8] P. Kalyani and C. Chellappan, “Heterogeneous wireless moobile sensor network mobile based routing adapted to dynamic topology,” European Journal of Scientific Research, vol. 50, no. 1, pp.143-150, 2011.

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

[10] Oxford University Computing Laboratory. FDR2 User Manual, 19th October 2010

[11] oneM2M-TR-0003. “ Analysis of Security Solutions for the oneM2M System.” Technical Specification. 2014. 08

[12] C.A.R HoReadere. Communicating Sequential Processes. Prentice-Hall. 1985

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 : bws@motor.ac.kr