http://dx.doi.org/10.14400/JDC.2015.13.5.213

M2M 통신환경에서 안전한 P2P 보안 프로토콜 검증

한군희*, 배우식**
백석대학교 정보통신학부*, 아주자동차대학**

Verifying a Safe P2P Security Protocol in M2M Communication Environment

Kun-Hee Han*, Woo-Sik Bae**
Dept. of Information and Communication, Baekseok University*
Dept. of AIS Center, Ajou Motor College**

요 약 최근 정보통신 기술의 발전과 함께 M2M(Machine-to-Machine) 산업분야의 시스템이 다기능 고성능화 되고 있으며 IoT(Internet of Things), IoE(Internet of Everything)기술 등과 함께 많은 발전해가고 있다. 통신상 보안적인 서비스를 제공하기 위해서는 인증, 기밀성, 익명성, 부인방지, 데이터신뢰성, 비연결성, 추적성 등이 충족 되어야 한다. 그러나 통신방식이 무선 전송구간에서는 공격자의 공격에 노출되어 있다. M2M 무선통신 프로토콜에서 보안상 문제가 생기면 시스템오류, 정보유출, 프라이버시문제 등의 심각한 상황이 발생할 수 있다. 따라서 프로토콜 설계는 상호인증과 보안이 필수적인 요소이며, 최근 보안통신프로토콜에 대한 분야가 매우 중요한 부분으로 연구되고 있다. 본 논문에서는 안전한 통신프로토콜을 위해 해시함수, 난수, 비밀키 및 세션키를 적용하여 설계하였다. 제안 프로토콜이 공격자의 각종공격에 안전함을 증명하기 위해 프로토콜 정형검증도구인 Casper/FDR 도구를 이용하여 실험하였다. 실험결과 제안프로토콜은 안전성을 충족했으며 문제없이 종료됨을 확인하였다.

주제어 : M2M 보안 프로토콜, 보안시스템, 인증프로토콜, Casper, 보안통신인증, 모델검증

Abstract In parallel with evolving information communication technology, M2M(Machine-to-Machine) industry has implemented multi-functional and high-performance systems, and made great strides with IoT(Internet of Things) and IoE(Internet of Everything). Authentication, confidentiality, anonymity, non-repudiation, data reliability, connectionless and traceability are prerequisites for communication security. Yet, the wireless transmission section in M2M communication is exposed to intruders' attacks. Any security issues attributable to M2M wireless communication protocols may lead to serious concerns including system faults, information leakage and privacy challenges. Therefore, mutual authentication and security are key components of protocol design. Recently, secure communication protocols have been regarded as highly important and explored as such. The present paper draws on hash function, random numbers, secret keys and session keys to design a secure communication protocol. Also, this paper tests the proposed protocol with a formal verification tool, Casper/FDR, to demonstrate its security against a range of intruders' attacks. In brief, the proposed protocol meets the security requirements, addressing the challenges without any problems.

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

* 이 논문은 2015학년도 백석대학교 대학연구비에 의하여 수행된 것임
Received 1 March 2015, Revised 13 April 2015
Accepted 20 May 2015
Corresponding Author: WooSik Bae(Ajou Motor College)
Email: drbws@daum.net

ISSN: 1738-1916

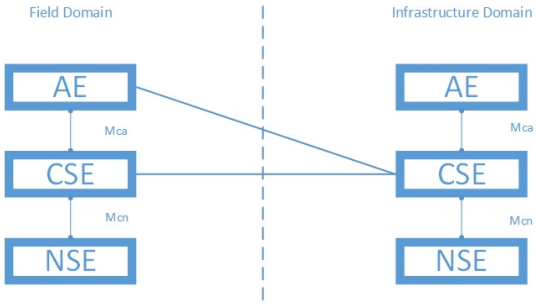
1. 서론

최근 각종 통신기기의 등장과 발전으로 M2M(Machine-to-Machine), IoT(Internat of Thing), IoE(Internet of Everything) 등의 개념으로 사물인터넷 기술이 차세대 기술로 각광받고 있다. 사물인터넷은 주변에 존재하는 사물들이 온도, 습도, 열, 가스, 조도, 초음파, 레이더, 위치, 모션, 영상 센서 등과 네트워크를 통해 인터넷연결 및 장비간 통신하여 각종 정보를 주고받는 개념이다[1,2,3,4]. 사물들끼리 통신하는 장비간 에서는 공통적으로 사용할 수 있는 언어가 있어야 하며 아울러 외부 공격자에게 전송데이터의 보안이 안전한 통신이 진행되어야 한다[5,6,7]. 그러나 장비간 무선통신에서는 공격자에 의한 정보누출 및 공격에 취약하게 된다[8,9,10]. 이와 관련하여 많은 연구자들이 무선네트워크의 통신프로토콜을 꾸준히 연구하고 있다. 본 논문에서는 모델체크 기법으로 효과성을 인정하고 있는 Casper[11,12] 와 FDR[13,14]을 이용하여 제안한 프로토콜이 보안적으로 안전한지 검증한다. 본 논문의 전체적 구성은 다음과 같다. 제 2장에서 관련연구로써 M2M 통신 및 보안 위협에 대하여 확인하고 이후 3장에서 제안 보안프로토콜을 명세한 후 단계별로 확인하며, 4장에서 보안적으로 안전한지 실험검증을 실시한다. 최종적으로 5장에서 결과에 대한 결론을 맺는다.

2. 관련연구

2.1 M2M 통신의 구조 및 보안위협

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, 편집, 처리하여 상호 전달하는 기술로써 RFID/USN 기술의 발전으로 응용영역을 확장 하고 있다.



[Fig. 1] oneM2M Architecture

[Fig. 1]은 oneM2M 의 기본적인 아키택처를 위한 기능구조를 나타내었으며 응용 엔티티(Application Entity), 공통서비스 엔티티(Common Services Entity), 네트워크 서비스 엔티티(Network Services Entity) 로 구성된다. 통신은 레퍼런스 포인트를 통해 통신하게 된다. M2M 통신 보안요구사항을 다음과 같이 정리하였다.

1) 인증 : M2M 통신환경에서 디바이스나 게이트웨이로부터 데이터를 송.수신하기 위해서 정당한 디바이스에서 전송된 데이터인지 검증해야한다. 인증을 하지 않을 경우 공격자가 M2M 디바이스의 정상 통신을 방해가능한 문제가 있다. 따라서 보안위협에 대응하기 위해 상호 인증을 하여 안전한 통신이 되도록 해야 한다.
2) 무결성 : 송신 데이터가 변경이 되지 않았음을 확인하는 것으로 송신한 메시지와 수신한 메시지가 같음을 보장하는 것이다. 이는 중간자 공격을 이용하여 전송되는 데이터를 위변조하는 공격자의 보안위협에 대응하기 위함이다.
3) 기밀성 : 데이터의 노출로부터 보호하는 것을 의미한다. 통신 데이터에 개인정보, 위치정보 등 민감한 정보들이 전송될 경우 공격자가 데이터를 확인할 수 없도록 데이터를 보호해야 한다.
4) 부인방지 : 데이터를 송신한 디바이스는 데이터 송신 사실을 증명함으로써 부인할 수 없도록 해야 한다. 일반적으로 송.수신 데이터 로그를 수집하거나, 디지털서명을 사용함으로써 부인방지를 제공할 수 있다.
5) 프라이버시 : 영상데이터 및 위치정보가 공격자에게 노출될 경우 공격자의 목표가 될 수 있어 프라

이버시를 보호하기 위한 요구사항이다.

6) 추적성 : M2M 통신에서 범죄, 사고 등과 같은 문제가 발생했을 경우 데이터를 추적 확인할 수 있어야 한다. 다만 추적정보는 철저한 보안이 유지되어야 한다[2,3,15].

2.2 해시락 프로토콜의 취약점

태그의 식별 값인 메타 아이디가 고정된 값으로 있으며, 전송되는 데이터가 같아 어떤 태그로부터 데이터가 전송되었는지 확인이 가능하다. 아울러 리더와 태그사이의 통신은 도청공격이 가능하여 공격자는 키를 획득한 후, 해시연산하고 메타ID를 연산하여 인증이 가능하다. 또한 공격자가 변함없는 메타ID를 재전송함으로써 인증받을 수 있다. 동일한 메타ID가 사용되어 스푸핑 공격 및 태그 추적이 가능하다.

해시락 프로토콜은 다음과 같이 표현된다.

(1) Tag → Reader : ID
(2) Reader → DB : ID
(3) DB → Reader : sKey
(4) Reader → Tag : sKey
(5) Tag → Reader : ID

```
#Free variables
R, T : Agent
DB : Server
skey : SessionKey
Id : Text
H : HashFunction
InverseKeys = (key, key)
#Protocol description
0. -> T : R
1. T -> R : (H(skey)) % metaID
2. R -> DB : metaID % (H(skey))
3. DB -> R : skey, Id
4. R -> T : skey
5. T -> R : Id
#Intruder Information
Intruder = Mallory
IntruderKnowledge =
{Tag, Reader, DataBase}
```

[Fig. 2] Specification of a hash-lock protocol

[Fig. 2]는 해시락 프로토콜을 Casper로 명세한 3개 영역이다. Free variables영역에서 R, T는 에이전트, DB는 서버이다. 키는 한 번의 세션에서만 사용하기 때문에 세션키 sKey로 명세했다. InverKey는 Session키에 대한 암호화를 표현하며, H는 해시함수연산을 표현한다. 해시락 프로토콜을 FDR 도구를 이용하여 검증한 결과 취약성이 발견되었다. ID의 값을 중간자공격 및 재생공격에 이용함에 따라 태그정보의 노출 및 위치 추적이 가능한 문제가 있었다[5,16].

3. 제안 프로토콜

M2M 통신은 사람이 확인하기 어려운 장소 등에 유.무선 통신을 이용하여 정보를 송.수신 한다. 통신 구간중 무선통신 구간에 보안위협이 있으며 공격자의 보안위협으로부터 안전한 통신환경을 제공하는 방법을 제안한다. 본 논문에서는 전송되는 매 세션에 바뀌는 세션키, 난수값을 적용하고 해시함수 연산을 하며 비밀키 및 공개키를 추가하여 통신을 한다. 본 논문에서 제안한 프로토콜 기호의 정의는 <Table 1>과 같다.

〈Table 1〉 Symbols and definition

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

3.1 동작설명

제안한 프로토콜의 동작은 단계별로 다음과 같이 동작한다.

◎ Step 1 : Tag → Reader

Tag는 Reader로 부터 Query를 수신한 후 Tag에서 Reader에게 보내질 H(R),{R, SkeyT}{pkdb}%enc 값을 생성한 후 변수 %emc에 저장한다. 이어서 각 값을 연접(concatenation)하여 Reader에게 전송한다. 이때 생성하여 전송되는 값은 고유한 값으로 세션 및 다른 장치에서

는 동일하게 생성할 수 없는 값이다.

◎ Step 2 : Reader → SERVER

Tag에서 수신한 Reader H(R),{R, SkeyT}{pkdb}%enc 값을 수신하여 확인 인증하고 수신된 값을 이용하여 Reader가 생성한 H(R)(+){T,SkeyR}{pkdb},enc%{R,SkeyT}{pkdb} 값을 데이터베이스서버로 전송한다.

◎ Step 3 : Server → Reader

Reader 에게서 송신된 H(R)(+){T,SkeyR}{pkdb},enc%{R,SkeyT}{pkdb} 값을 수신한 후 데이터베이스서버에서 계산한 SkeyT(+)SkeyR값을 생성한다. 이후 인증 진행을 위해 Reader에게 송신한다.

◎ Step 4 : Reader → Tag

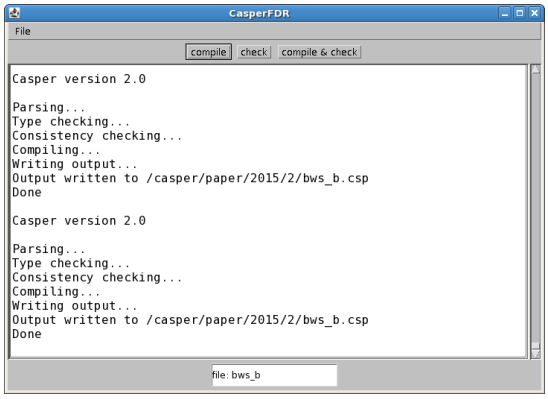
Reader는 데이터베이스서버에서 수신한 SkeyT(+)SkeyR 값을 확인한 후 인증하고 Tag 에 보낼 {x}{SkeyT}(+)H(R) 값을 생성하는데 이때 고정 길이의 데이터 값을 연산하여 해시 하는 방식은 다음과 같다. Reader의 문자열에 다음의 공식으로 대입하면 $h_a(Reader) = h\int((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 으로 연산되며 전송되는 데이터는 {x}{SkeyT}(+) $h_a(Reader, x) = h\int((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 으로 계산 및 생성되어 Tag에게 전송된다.

◎ Step 5 : Tag → Reader

마지막으로 Tag는 Reader에게 Tag 에서의 {x}{SkeyT}(+)H(R)값을 전송 받은 이후 태그에서 생성한 값과 확인 및 비교하여 참이면 자신의 ID를 $h_a(SkeyT, T) = h((\sum_{i=0}^{k} x_i . a^i) \bmod p)$ 로 해시연산 암호화하여 Reader에게 전송함으로 태그에서의 인증 세션을 완료한다. 이후 확인세션을 완료하며 안정적으로 통신을 진행한다.

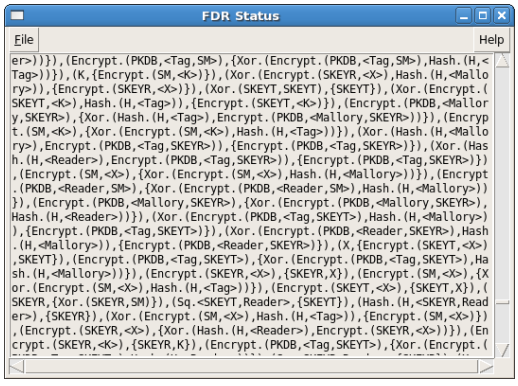
4. 실험결과

본 논문에서는 연구용 FDR 2.91 버전의 모델검증 도구를 사용하였다. 설계한 M2M 보안 프로토콜의 안전성, 교착상태, 라이브락 등의 동작오류를 검증하였다. [Fig. 3]는 소스 파일을 로딩하여 오류 없이 CSP 소스로 변환이 완료된 상태이다.



[Fig. 3] Verification set-up and running

제안 프로토콜의 검증 진행상태창은 [Fig. 4]와 같이 복잡한 여러 가지 공격을 대입하여 시도하고 취약점에 대한 검증을 하게 된다.



[Fig. 4] status of the proposed protocol

검증이 완료 되면 [Fig. 5]와 같이 검증결과가 확인되며 각 결과의 내용은 다음과 같이 분석된다.

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

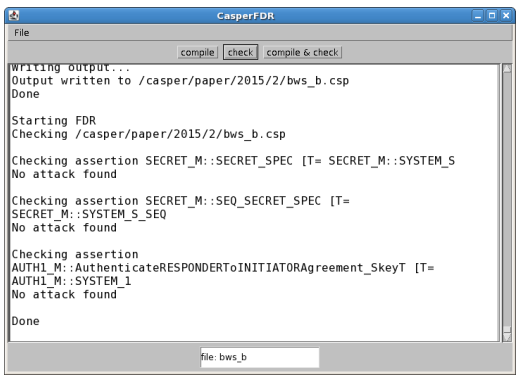
제안한 프로토콜이 보안적으로 안전한지 확인 부분으로 제안한 프로토콜이 공격자에게 노출되지 않았음을 나타낸다. 검증한 Agent간 통신이 안정적으로 진행 되었는지 와 전송 데이터 값 , 난수 및 세션키의 보안성이 적합하게 안전한지 확인되었다.

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

이 항목의 검증은 프로토콜이 시스템에서 안전한 프로세스로 동작했는지 실험한 결과로써 본 논문에서 제안한 M2M 프로토콜은 그림과 같이 안전한 프로세스로 실행됨을 실험하였다.

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

3)은 전송되는 데이터가 Responder와 Initiator가 서로 상호 인증함이 적합한지 실험하는 부분으로 통신 에이전트 구간에서 안전하게 상호 인증됨을 확인하였다. 따라서 각 공격에 대해 안전하다는 메시지를 출력하며 그림과 같이 안전하게 종료되었다.



[Fig. 5] Security verification results of the protocol

5. 결론

최근 이슈가 되고 있는 사물인터넷은 세계적으로 도입 초기 단계로 향후 모든 산업에서 활용될 것이다. 그러나 많은 디바이스가 네트워크로 연결되기 때문에 이를 악용하여 공격하는 문제점이 생긴다. 따라서 본 논문에서는 M2M 통신에서 안전한 통신을 위해 보안적으로 안전한 유 무선 통신 프로토콜을 제안하였다. 난수, 해시연산, 세션키, 공개키 및 비밀키를 이용하여 설계 하였으며 보안성을 최대한 높여 상호인증을 제공하고 있다. 정형검증 도구인 Casper/FDR 프로그램을 이용하여 정형검증 결과 각 분야에서 안전함을 확인하였다. 아울러 프로토콜이 효율적으로 동작을 종료함을 실험하였다. 따라서 M2M 보안 분야에서 안전한 통신환경이 되도록 설계 제안되었음을 검증하였다. 향후 의료, 군사, 귀중품 분야에서 안전하게 통신할 수 있는 확장연구를 진행할 계획이다.

ACKNOWLEDGMENTS

This work was supported by the research grant of Baeseok University in 2015.

REFERENCES

[1] Kyoung-nam Kim, Lee, Jae Moon, MyounJae Lee, Sunghyuck Hong, Convergent Secure Wireless Sensor Network Routing Algorithm. Journal of the Korea Convergence Society, Vol. 6, No. 1, pp. 65-70, 2015.

[2] Yang, M. H., and Hu, H. Y., Protocol for ownership transfer across authorities: with the ability to assign transfer target, Security and Communication Networks, vol .5, pp. 164 - 177, 2012.

[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] S. Y. Lien, K. C. Chen, and Y. Lin, Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. IEEE Communications Magazine, vol. 49, no. 4, pp. 66-74, 2011.

[5] 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.

[6] 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.

[7] W. S. Bae, Inter-device Mutual authentication and Formal Verification in M2M Environment. Journal of Digital Convergence, Vol. 12, No. 9, pp. 219-223, 2014.

[8] Bo-Kyung Lee, A Study on Security of Virtualization in Cloud Computing Environment for Convergence Services. Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 93-99, 2014.

[9] Keun-Ho Lee, A Study of Security Requirement in Wireless Charging. Journal of the Korea Convergence Society, Vol. 5, No. 3, pp. 23-27, 2014.

[10] Eui-Seok Nahm, Design of Computer Hardware Fault Detector using ROM BIOS. Journal of the Korea Convergence Society, Vol. 4, No. 3, pp. 21-26, 2013.

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

[12] C. Kraetzer, Modelling Watermark Communication Protocols using the CASPER Modelling Language. Proceedings of the 12th ACM workshop on Multimedia and security. pp. 107-116, 2010.

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

[14] Mihai-Lica Pura, Victor Valeriu Patriciu, Ion Bica, Formal Verification of G-PAKE Using Casper/FDR2-Securing a Group PAKE Protocol Using Casper/FDR2. SECRYPT 2010: pp. 299-303, 2010.

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

[16] Yu Tian-tian, Feng Quan-yuan, A Security RFID Authentication Protocol Based on Hash Function. IEEC09, pp. 804-807, 2009.

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

한 군 희(Han, Kun Hee)

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
- E-Mail : hankh@bu.ac.kr