모델체킹을 이용한 RFID 보안프로토콜 검증

김주배° 김현석 최진영
고려대학교 컴퓨터과
{jbkim°, hskim, choi}@formal.korea.ac.kr

Verification of RFID Security Protocol using Model Checking

Joobae Kim° Hyunseok Kim Jinyoung Choi
Dep. Of Computer Science & Engineering, Korea University

요 약

무선 네트워크를 사용하는 RFID 시스템은 정보 유출에 취약하다. 하지만 하드웨어적인 제약으로 인해 물리적인 방법을 통한 보안 안전성 확보가 용이하지 않으므로, 경량화된 보안 프로토콜을 필요로 한다. 이에 본 논문에서는 리더간 네트워크 기술을 이용한 RFID 시스템을 위해 제안된 보안 프로토콜을 정형 기법을 기반으로 하는 모델 체킹 방법을 통해 검증하였으며, 신뢰성 있는 보안 프로토콜을 적용한 RFID 시스템을 구축할 수 있도록 하였다.

1. 서 론

유비쿼터스 실현의 핵심기술인 RFID (Radio Frequency Identification)[1]와 이를 이용하여 주변의 데이터를 탐지, 인식하고 실시간으로 네트워크에 연결하여 정보를 관리하는 센서 네트워크 기술로 인해 모든 실체들이 무선 네트워크상에서 인식될 수 있는 존재가 되었다. 그러나 이러한 RFID 기술의 사용으로 개인의 프라이버시(위치정보)가 침해될 수 있고 RFID 태그의 ID가 식별이 용이하다는 점으로 인해 태그 정보가 사용자가 알지 못하는 사이에 모든 리더에게 전송될 수 있다는 문제점을 드러냈다. 산업적으로 많이 쓰이는 RFID 시스템은 배터리가 없어 가격이 낮은 Passive 태그를 사용하고 있고, 경제적이고 실제 사용 가능한 태그를 만들기 위한 노력이 지속되고 있어 하드웨어적인 제약이 많다. 따라서 전통적으로 사용되던 다양한 암호화 방법을 적용하지 못하게 되었다. 태그와 리더의 가격은 그들이 갖고 있는 메모리 용량과 데이터 처리 능력에 비례하기 때문에 이들의 기능을 최대한 보장하면서 보안성을 만족시켜줄 수 있는 경량화된 암호화 기술이 필요하게 되었다[2]. 또한 RFID 시스템은 태그와 리더간 통신이 무선으로 이루어지기 때문에 일정한 거리 내에 위치한 모든 시스템에서 데이터를 수신할 수 있어 보안에 매우 취약하다. 위와 같은 이유로 RFID 시스템은 보안적인 취약점을 보완하기 위해 각각의 시스템에 효율적인 보안프로토콜을 필요로 한다.

RFID 시스템의 보안문제를 해결하기 위해 많은 보안프로토콜이 제안되었으나, 안전하다고 여겨졌던 많은 보안프로토콜의 취약점들이 노출되고 있고, 설계 단계에서부터 보안프로토콜의 속성들을 검증하기 위해 정형기법이 활용되고 있다.

보안 프로토콜의 정형 검증 방법으로 크게 모델체킹 [3]과 정리증명이 사용된다. 모델체킹은 상태 전이 시스템과 특성이 주어지면, 주어진 상태전이 시스템이 검증하고자 하는 특성을 만족하는지 알아보기 위해 상태 전이 시스템의 모든 상태 공간을 검사하고 그 결과를 알려준다. 정리증명은 공리로부터 추론 규칙을 이용하여 보안 취약점을 추론하는 방식이다

본 논문에서는 FDR[4]이라는 모델체킹 도구를 이용하여 대량의 물류 관리를 위해 개발중인 RFID 리더 네트워크 시스템에 적용하기 위해 제안된 보안 프로토콜을 검증하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템을 위한 보안프로토콜의 요구사항에 대해 정리하였으며, 3장에서는 RFID 시스템 보안프로토콜의 연구현황에 대해 살펴보고, 4장에서는 프로토콜을 명세하고 검증하기 위한 Casper[5] 및 FDR 도구에 대해 소개하며, 5장에서는 대량 물류 관리 RFID 시스템을 위해 제안된 보안프로토콜을 명세 및 검증하고, 마지막으로 결론 및 향후 연구 방향을 제시하고자 한다.

2. RFID 시스템 보안 요구사항[6]

RFID 시스템의 보안 안정성을 높이기 위해 물리적 방법 외에 보안프로토콜과 같은 암호기술적 해결방안을 적용하기 위한 기준으로서 아래와 같은 4가지 기본적인

본 연구는 산업자원부의 성장동력사업 지원으로 수행되었음 (과제번호 10016756)

요구사항을 제시하였다.

A. 인증이 되지 않은 리더에게 정보유출이 되지 않아야 하며, 태그와 그 소유자 사이에 긴 시간 동안의 추적(long-term tracking)이 불가능해야 한다.

B. 태그의 내용은 근제한기법 (access control)에 의해 질의채널 (interrogation channel)이 안전하지 않다고 예상되면 암호화되어야 한다.

C. 태그와 리더 사이에는 상호인증(mutual authentication)이 제공되어야 한다.

D. 태그와 리더 모두 재생공격(replay attack) 및 공격자 중간공격(man-in-the-middle attack)에 대한 저항력을 갖춰야 한다.

3. RFID 시스템 보안프로토콜 연구 현황

RFID 시스템에 적용하기 위한 보안프로토콜 연구의 접근 방법은 아래와 같이 크게 세가지로 구분할 수 있다. RFID 시스템이 갖춰야 할 것으로 제시된 모든 보안 요구사항을 완벽하게 만족시키는 보안프로토콜은 아직 제안되지 못하고 있지만, 각각의 고유한 기술적 특성에 의한 단점을 다른 접근방법으로 보완하기 위한 연구들이 다양하게 진행되고 있다.

3.1 Public Key cryptography approach

RFID 태그와 서버가 상호 인증하는 과정에서 공개키 알고리즘을 사용하도록 프로토콜을 연구하는 방법이다. 하지만 공개키 알고리즘은 사용되는 비밀키를 찾아내는 것이 computationally infeasible하기 때문에 보안성이 강력한 만큼, 이 알고리즘을 사용하기 위해서는 고사양의 시스템이 필요하다.

3.2 Hash Function approach

해쉬 함수는 공유키 또는 공개키 알고리즘에 비해 복잡도가 낮고 구현이 쉬워, RFID 관련 보안 프로토콜을 설계하는데 각광받고 있는 알고리즘이다. 해쉬 함수는 비밀키 사용의 유·무에 따라서 MDC와 MAC 함수로 나뉘는데, RFID 보안 프로토콜을 설계하는데 사용이 가능하다. 이런 해쉬 함수를 사용하여 기존에 제안되었던 해쉬락 기법 및 Randomized 해쉬락 기법은 주고받는 값들 중 고정된 값이 있어, 이를 통한 태그 추적이 가능하고, 태그의 잠금상태를 해제하기 위한 Key가 노출될 수 있다는 단점이 있다. 또한 Randomized 해쉬락 기법은 리더가 서버가 보내온 ID들을 모두 비교하여 태그의 ID를 찾아야 하기 때문에 리더에 무리를 준다.

3.3 Message Authentication codes(MAC) approach

MAC 함수는 One-way 함수에 상호 공유하고 있는 비밀키를 사용하여 데이터를 암호화 하는 방법으로, 암호화 되지 않은 데이터와 MAC 데이터를 같이 보내어, 현재 보내는 데이터의 비밀성 및 인증성을 보장케하는 방법이다. 공유키 방식의 암호화 알고리즘에 비해 복잡도가 낮고, 구현도 용이하기 때문에 유·무선 통신에서 다양하게 사용되고 있는 함수이다. 태그와 리더가 주고받는 메시지들에 MAC 함수를 적용하여 사용한다는 방법으로, 태그의 위조에 비교적 취약하다.

3.4 SPINS(Security Protocols for Sensor Networks)[7]

버클리 대학의 SmartDust 프로젝트에서 채택하였으며, μTESLA와 SNEP으로 구성되어 있고, 메시지 인증, 무결성, 기밀성, 적시성 등의 서비스를 제공하고 있다. 랜덤키 사전 분배방식으로 키 DB을 선택하고 무작위로 키를 선택하여 센서 노드에 할당하며, 두 개의 노드는 자신의 키 DB를 탐색하여 상대방이 같은 공통키를 소유하고 있으면 이 키를 세션키로 사용한다.

4. CSP[8], Casper 와 FDR 도구

4.1 CSP(Communicating Sequential Process)

CSP 는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용되어졌으나, 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP 에서 제공하는 pure synchronization (|||)과 Interleaving parallelism(||) 개념을 사용하여 분산 시스템 환경에서 동작하는 클라이언트 서버와 공격자 모델을 정형적으로 표현할 수 있는 장점을 갖고 있다.

4.2 Casper (A Compiler for the Analysis of Security Protocols)

CSP(Communication Sequential Process) 언어를 이용하여 보안프로토콜 행위를 명세하고 FDR 정형검증 도구를 이용하여 보안속성을 검증하는 연구가 진행되었다. 하지만, CSP 언어를 이용한 정형명세과정은 정형적 설계 방법에 익숙지 않은 보안프로토콜 설계자에게는 매우 복잡한 명세언어라는 단점을 갖고 있었다. 이에 따라, 보안프로토콜의 행위를 간략히 명세할 수 있도록 Casper 도구가 개발되었다. Casper 도구로 보안프로토콜의 행위와 검증 속성을 명세하게 되며, 자동변환기능을 이용해 CSP 명세코드를 생성할 수 있다. 결국, 자동생성된 CSP 명세코드를 FDR 정형검증도구에 입력하여 보안프로토콜을 검증한다.

4.3 FDR (Failure Divergence Refinement)

FDR 도구는 CSP 를 입력으로 받아들이는 모델체커로서 옥스포드 대학에서 개발되었다. 이 도구는 CSP 명세언어로 기술된 보안프로토콜 모델이 보안속성들을 만족하는지 검증하고, 만일 만족하지 않을 경우에는 CSP 이벤트로 기술된 반례(counterexample)을 보여주어 보안상 취약점 분석을 용이하게 도와준다.

5. RFID 리더 네크워크 프로토콜 검증 및 분석

본 논문에서 다루고자 하는 RFID 리더 네트워크 시스템은 리더간의 통신을 위해 센서네트워크를 이용한다. 한 개의 리더는 서버로서의 역할을 담당하고, 나머지 여러 개의 리더가 클라이언트로서의 역할을 담당한다. 따라서, 서버와 클라이언트간 보안 프로토콜을 모델링 하기 위해 모든 클라이언트는 다른 클라이언트를 거치지 않고 서버와 직접 통신한다라고 가정하였다.

적용되는 RFID 환경에서 리더의 이동성과 크기는 덜 중요하게 고려되어 하드웨어적인 제약이 양호한 리더가 사용될 수 있으므로 비교적 보안 안전성이 강한 공개키 기반의 보안프로토콜[9]이 제안되었다.

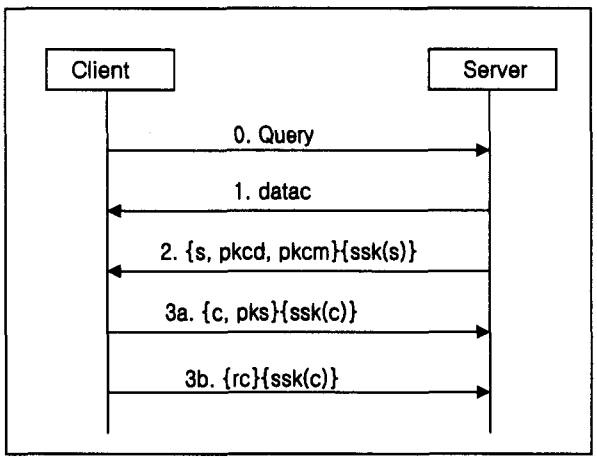

그림 1. RFID 리더 네트워크 보안 프로토콜

• **RFID 리더 네트워크 보안프로토콜 (그림 1. 참조)**

① 클라이언트가 서버에게 통신구성을 요청한다.
② 서버가 클라이언트에게 암호방식, 키 교환방식, 서명방식, 압축방식이 포함된 datac 를 제공한다.
③ 서버가 클라이언트에게 자신의 ID 와 함께 클라이언트의 Public Key 를 자신의 Secret Key 로 암호화하여 보낸다.
④ 클라이언트가 서버에게 자신의 ID 와 서버의 Public Key 를 자신의 Secret Key 로 암호화하여 보낸다.
⑤ 클라이언트가 서버에게 자신이 만들어낸 nonce 값을 자신의 Secret Key 로 암호화하여 보낸다.

5.1 Casper 를 이용한 프로토콜 명세

그림 2 는 RFID 리더 네트워크 시스템에 적용하기 위해 제안된 프로토콜을 Casper 도구를 이용하여 모델링한 것으로, 8 가지 명세 항목 중 자유변수 영역과 프로토콜 기술영역, 침입자 영역에 대한 표현이다.

```
#Free variables
c, s : Agent
pkcd, pkcm, pks : PublicKey
skcd, skcm, sks : SecretKey
SPK :  Agent -> AgentPublicKey
SSK :  Agent -> AgentSecretKey
datac : Nonce
rc : Nonce
InverseKeys = (pkcd, skcd), (pkcm, skcm),
(SPK, SSK), (rc, rc)

#Protocol description
0.      -> c : s
1.  s   -> c : datac
2.  s   -> c : {s, pkcd, pkcm}{SSK(s)}
3a. c   -> s : {c, pks}{SSK(c)}
3b. c   -> s : {rc}{SSK(c)}

#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Client, Sam, Mallory, Nm,
PKcd, PKcm, PKm, Pks, SKm, SPK(Sam), Rm}
```

그림 2 . Casper 를 이용한 프로토콜 명세

먼저 자유변수 영역에서 c 는 클라이언트, s 는 서버로서 프로토콜의 Agent 를 나타낸다. pkcd, pkcm, pks 는 Public 키이며, skcd, skcm, sks 는 Secret 키이다. SPK 와 SSK 는 공개키에 대한 암호화 및 복호화 방식이며, datac 와 rc 는 세션 구성을 통해 생성된 Nonce 이다. InverseKeys 는 Public 키와 Secret 키에 대한 암호화 복호화를 표현한다. 프로토콜 기술 영역은 프로토콜의 메시지 통신 절차를 나타낸다. 메시지 2 에서 s 는 자신의 Secret 키인 SSK(s)를 사용해서 암호화하며, 메시지 3 에서 c 는 자신의 Secret 키인 SSK(c)를 사용한

다. s 와 c 는 서로의 Secret 키에 대한 Public 키를 이미 공유한 상태이므로, 서로 상대방의 메시지를 복호화 할 수 있으며, 메시지 3b 에서 c 는 s 에게 자신이 생성한 nonce 를 전달한다. 마지막으로 침입자 영역에 대한 정보가 제시되어 있다.

5.2 FDR을 통한 프로토콜 검증 결과

FDR을 통하여 검증한 결과, RFID 리더 네트워크 프로토콜이 만족시켜야 할 보안 요구조건으로 제시했던 클라이언트와 서버의 ID 및 nonce에 대한 보안성을 만족하는 것으로 나타났다. 그림 3은 Casper를 이용하여 명세한 보안프로토콜을 FDR을 통해서 검증한 결과이다.

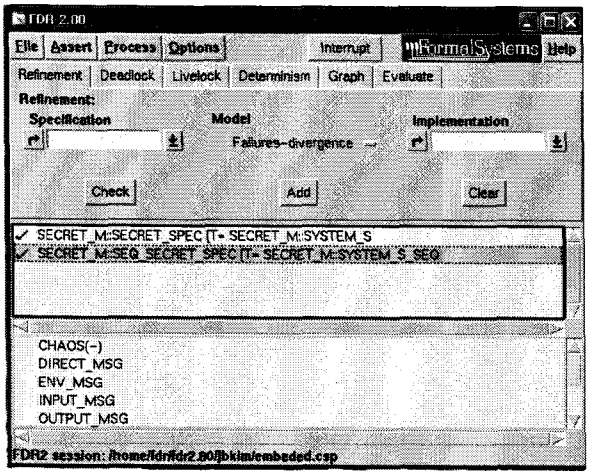

그림 3. FDR을 통한 RFID 리더 네트워크 보안 프로토콜 검증 결과

RFID 리더 네트워크의 보안 프로토콜에서 공격자가 통신을 구성하기 위해서는 반드시 s와 c의 ID와 nonce(rc)를 필요로 한다. 하지만, 검증 결과는 공격자가 이를 획득할 수 없음을 보여준다. 즉, s(서버)와 c(클라이언트)가 갖고 있는 Secret 키를 획득하지 못하므로, 이들 정보가 암호화되어 있는 메시지를 복호화 할 수 없음을 뜻한다. 따라서, 명세된 대로의 보안 프로토콜에 의해 구성된 시스템에서는 보안상 안전하다고 말할 수 있다.

6. 결론 및 향후 연구과제

RFID 시스템은 점차 활용범위가 확대되고 있고 기술적인 개발과 함께 보안성을 강화하기 위한 다양한 연구가 진행되고 있다. 무선 환경의 물리적인 제한사항을 고려하면서 보안성을 확보해야 하기 때문에 RFID 시스템은 보안 프로토콜에 의한 의존도가 특히 높다고 할 수 있다. 모델 체킹 방법을 적용한 보안 프로토콜의 검증을 통해 RFID 시스템은 보안 안전성을 확보할 수 있다. 본 논문에서는 리더간 네트워크 기반의 RFID 시스템에 적용하기 위해 제안된 보안 프로토콜을 검증하였으며 요구되는 조건이 만족됨을 확인하였다.

향후 연구에서는 프로토콜의 불필요한 암호화 기능을 최소화하고 단순화하여 RFID 환경에서의 실용화 될 수 있는 보안 프로토콜을 개발하여 제안하고자 한다.

참고문헌

[1] S. Sarma, S. Weis, and D. Engels, "RFID systems and security and privacy implications", In Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2002, LNCS No. 2523, pp. 454-469, 2003

[2] A. Juels, Privacy and authentication in low-cost RFID tags, In submission, Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

[3] A. Roscoe and M. Goldsmith, The Perfect Spy for Model-Checking Crypto-protocols, In Proceedings of the 1997 CIMACS Workshop on Design and Formal Verification of Security Protocols, 1997.

[4] Formal Systems Ltd. FDR2 User Manual, Aug. 1999.

[5] G. Lowe, Casper: A compiler for the analysis of security protocols, In Proceeding of the 1997 IEEE Computer Security Foundations Workshop X, IEEE Computer Society, Silver Spring, MD, pp. 18-30, 1997.

[6] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn Ted Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems", National Institute of Standards and Technology, April 2007.

[7] A. Perrig, et al., " SPINS : Security Protocols for Sensor Networks" , Mobile Computing and Networking 2001.

[8] C.A.R. Hoare, "*Communicating Sequential Processes*", Prentice-Hall, 1985.

[9] G. Gaubatz, J. Kaps, and B. Sunar, " Public Keys Cryptography in Sensor Networks Revisited", Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004).