세션키 및 공개키를 이용한 RFID 보안 인증 프로토콜의 안전성 검증

배우식*, 이종연**

Verification of Safety in a RFID Security Authentication Protocol Using Session and Public Keys

Woo Sik BAE*, Jong Yun LEE**

요 약 RFID 시스템은 무선 구간의 통신 취약성으로 공격자의 공격 목표가 되며 도청, 정보노출, 트래픽분석, 스푸핑 등 보안상 다양한 문제점을 가지고 있다. 따라서 많은 연구자에 의해 여러 가지 방식의 프로토콜이 제안되고 있으나 구현부분이 까다로워 정리증명이나 검증의 수준에서 제안되고 있는 실정이다. 따라서 본 논문에서는 공개키, 세션키, 해시, XOR 및 난수 개념을 사용하여 각각 태그와 리더구간, 리더와 서버 구간에 안전한 RFID 보안 프로토콜을 제안한다. 보안상 가장 취약한 리더와 태그 구간에 타임스탬프와 해시를 적용하여 시간차가 있는 공격신호에 대하여 공격을 탐지하며, 마지막 세션에서도 태그 정보를 노출시키지 않기 위해 해시 연산 후 통신하고 있다. 끝으로 본 논문의 학문적 기여도는 실제 시스템에서 사용가능한 프로토콜을 설계하고 차별화된 Casper 정형검증기법을 도입하여 제안프로토콜의 보안성을 검증하는데 있다.

주제어 : RFID 보안, 인증프로토콜, 해시함수, RFID 인증, 정형검증

Abstract Due to its communication vulnerability resulting in a range of problems, e.g. eavesdropping, information exposure, traffic analysis and spoofing, RFID system becomes the target of attackers. Accordingly, many investigators have proposed various protocols to the extent of theorem proving or verification as the implementation is challenging. This paper thus proposes a safe RFID security protocol using public keys, session keys, hashes, XORs, and random numbers. Timestamps and hashes are applied to the most vulnerable section between readers and tags to detect attacks in attack signals with time difference. Also, to prevent tag information from being exposed in the last session, hash operation is adopted before communication. Finally, in this paper, we designed a RFID security protocol using public and session keys applicable to real systems and verified the security of the proposed protocol with a differentiated formal verification technique.

Key Words : RFID security, authentication protocol, hash function, RFID authentication, Model Checking

1. 서론

RFID(Radio Frequency Identification)는 무선주파수를 통해 사물의 정보를 읽고 관리 할 수 있는 인식기술이다. 최근에 바코드를 대체하여 자재관리, 유통, 물류, 의료, 환경, 보안 등의 다양한 산업에 도입되어 지고 있다[3][15][16]. 그러나 태그의 반도체 칩에 내장된 정보를 무선주파수를 이용하여 읽어내기 때문에 도청, 정보노출, 트래픽 분석, 스푸핑 공격, 서비스거부 공격, 메시지유실 및 트래킹 공격 등 많은 취약점 들을 지니고 있어서 보안 부분에 심각한 문제를 야기할 수 있다[1][14][17]. RFID 시스템의 보안 취약성을 해결하고자 기존에 제안된 해시

본 과제(결과물)는 교육과학기술부의 재원으로 지원을 받아 수행된 산학협력 선도대학(LINC) 육성사업의 연구결과입니다(2012.)
*아주자동차대학 전산실
**충북대학교 디지털정보융합학과 교수(교신저자)
논문접수: 2012년 10월 23일, 1차 수정을 거쳐, 심사완료: 2012년 11월 20일

락기법[2][8][10], 해시기반 ID 변형기법[11] 등의 제안 프로토콜이 보안상으로 취약한 문제가 연구자에 의해 발견되고 있다. 또는 기존의 RFID 보안 프로토콜은 보안상 안전하지만 대부분 너무 복잡하여 현장에서 직접 적용할 수 없는 상태이다[5][9][18].

따라서 본 논문에서는 RFID 보안 취약점을 해결하고 실제 현장 시스템에서 적용 가능한 보안 프로토콜의 설계를 목적으로 한다. 제안 방식은 보안성은 충족하면서 계산을 간소화하고 실제 시스템에서 사용 가능성에 초점을 두고 실험하였으며 다음과 같은 연구결과를 얻었다. 첫째, 정형 검증기법으로 프로토콜을 검증하여 기존 연구자들이 제안하는 정리증명에 비해 신뢰성을 높였다. 둘째, 제안 프로토콜은 무선구간 세션에서 공개키, 세션키, 해시락, XOR 및 난수를 사용하여 보안성을 높였다. 셋째, 세션에서 최종 데이터 전송을 해시와 XOR방식을 사용하여 보안을 강화하고, 전송 데이터를 줄임으로 RFID 시스템의 효율을 높였다. 아울러 제안 프로토콜을 CasperFDR로 정형 검증하여 여러 가지 취약점 확인에 안전함을 확인하였다. 따라서 제안 방식으로 RFID 보안 프로토콜에 적용하면 각 구간에 대하여 보안상 안전한 시스템의 구축이 가능하다.

2. 관련연구

2.1 Casper

Caster(A Compiler for the Analysis of Security Protocols)[7][12]는 보안 속성을 순차적으로 표현하고 프로토콜을 명세하기 쉽게 Gavin Lowe에 의해 개발되어진 컴파일러이다. Casper에서 프로토콜의 동작과 검증해야 할 시스템을 두 부분으로 나뉘어 명세 한다. 첫째, 호스트들 간의 전달되는 메시지, 데이터타입, 함수, 변수, 및 동작순서 등을 정의한다. 둘째, 실 시스템에서 동작하는 각각 호스트의 역할, 함수선언, 공격자의 상태정보 등 검증해야 할 실제 시스템을 정의한다.

Casper에서 검증하기 위해 8개의 세부 항목으로 명세 및 분류하는데 각 항목의 헤더 부분은 #으로 시작하며 다음과 같다.

#Free variables : 변수 타입 및 함수 선언
#Process : 통신 에이전트의 초기상태
#Protocol description : 에이전트 간의 메시지 교환 순서
#Specification : 검증하고자 하는 보안 속성 선언
#Actual Variables : 실제 데이터 타입 및 이름선언
#Functions : 프로토콜에서 사용하는 함수선언
#System : 에이전트의 초기상태 표현
#Intruder Information : 공격자의 최초 상태정보

2.2 FDR(Failure Divergence Refinements)

FDR 도구는 CSP(Communicating Sequential Processes)[13]를 입력 언어로 받아 모델이 속성을 만족하는지 검사하는 모델 검사도구 이다. 만일 만족하지 않을 경우에는 반례(counterexample)을 보여주어 각종 보안 취약점을 분석하기에 용이하다. 보안프로토콜의 요구사항인 비밀성, 무결성, 인증, 부인방지 등의 속성을 만족하는지 검사하는 도구이며 안전성(safety) 검증, 교착상태(deadlock) 검증, 라이브락(livelock)검증 의 3가지 검증 방법을 지원한다. 아울러 추적모델(trace model), 실패모델(failure model), 실패/분기모델(failure/divergence model)을 지원한다[4].

가) 추적모델(trace model)

프로세스는 그 프로세스가 갖는 행위에 의해 유한 순서 집합으로 표현되며, P 프로세스가 Q 프로세스의 모든 행위를 포함할 때 $P \sqsubseteq TQ$ 라고 표기한다.

$$P \sqsubseteq TQ \triangleq traces(Q) \subseteq traces(P)$$

나) 실패모델(failure model)

실패(failure)는 (s, X)의 쌍으로, s는 추적(P)에서의 추적을 말하고 X는 s 이후에 프로세스가 거부하는 모든 이벤트의 집합을 말한다. 즉 교착상태를 의미하며, 다음과 같이 표기한다.

$$P \sqsubseteq FQ \triangleq failures(Q) \subseteq failures(P)$$

다) 실패/분기 모델(failure/divergence model)

프로세스의 분기는 라이브락(livelock)을 의미한다. 즉 실패/분기 모델은 교착(deadlock)상태이면서 라이브락 상태를 의미하며, 다음과 같이 표기한다.

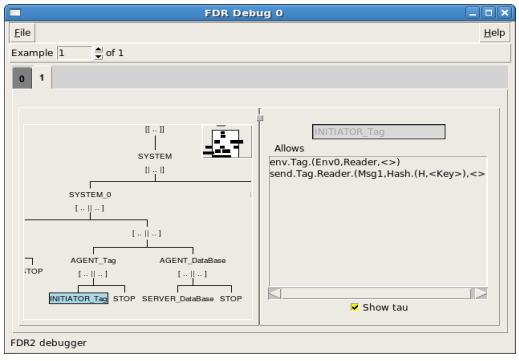
$$P \sqsubseteq FDQ \triangleq failures(Q) \subseteq failures(P) \wedge divergences(Q) \subseteq divergences(P)$$

2.3 기존 프로토콜

2.3.1 해시락 프로토콜

해시락 프로토콜은 항상 같은 metaID를 세션에서 사

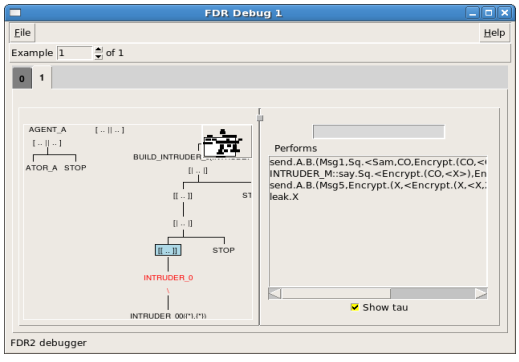
용함으로 공격자가 태그데이터를 식별하여 공격에 사용할 수 있는 문제가 있다. FDR 검증결과 [그림 1] 과 같은 디버그 상태 결과가 나왔으며 공격자에 의해 재전송 공격, 스푸핑 공격 및 추적이 가능한 문제점이 있다.



[그림 1] 해시락의 FDR 디버그 결과

2.3.2 Kenji et al. 프로토콜

Kenji *et al.* 프로토콜은 정보를 처음 보내는 세션에서 데이터를 암호화 하지 않고 전송하기 때문에 공격자가 데이터를 수집할 경우 위조할 수 있는 문제가 있다[6]. 공격자가 메시지를 임의로 작성하여 공격할 경우 시스템의 무결성에 문제가 생기며 취약성이 나타난다. [그림 2]는 FDR 검증결과 관련된 취약성을 확인할 수 있는 상태창을 보여주었다.



[그림 2] *Kenji et al.* 의 FDR 디버그 결과

3. 제안하는 프로토콜과 검증

3.1 제안하는 보안 프로토콜

본 논문에서 제안한 프로토콜에서 사용되는 기호에 대한 정의는 <표 1>과 같이 표기한다.

〈표 1〉 기호 정의

기호	설명
T	태그를 의미한다.
R	리더를 의미한다.
DB	데이터베이스 서버
Query	리더의 질의신호
pkd	PublicKey
skd	SecretKey
Ta, Tb	Timestamp로써 서버 기준
a1, a2	SessionKey
public	PublicKey
$\oplus$	Exclusive OR 연산자
H( )	HashFunction

본 절에서는 RFID 시스템의 보안 요구조건을 만족하는 프로토콜을 제안한다. 제안하는 프로토콜은 데이터베이스에서 태그에 대한 인증과 리더에 대한 인증이 동시에 이루어지며 기본적으로 타임스탬프 값인 Ta, Tb 값을 태그, 리더, 서버 구간에 확인할 수 있도록 하였다. 이는 공격자가 공격시 시간차이를 조작할 수 없도록 하기 위함이다. 아울러 서버의 값을 해시 연산된 값을 포함하며 난수와 세션키를 공개키로 암호화 하고 리더에게 전송하게 된다. 리더는 서버와의 통신에서 비교적 안전한 유선망 이지만 리더가 공격자로 위장가능 했을 때 시스템에 문제가 커지므로 서버와의 비밀키를 포함하여 전송하며 이때 세션키 a2와 타임스탬프 값 Tb를 포함해 줌으로써 서버와 리더구간의 보안을 더욱 강화하였다. 서버에서 리더로 보낼 때 새로운 서버의 H(S) 값을 포함하여 인증을 위해 공개키 암호화 하여 세션키와 함께 전송한다. 리더는 서버에서 받은 $H(S)\oplus(T,x,ka1_{public})(a2)$를 확인후 $ka1_{public},((x,k)(x))(k)\oplus H(S)$ 값을 생성하여 태그에게 보낸다. 태그는 리더에게서 받은 값을 비교한 후 새로운 H(S) 값을 저장한 후 인증하여 $H(T)\oplus(x)(k),pkd$ 값을 전송하여 완료한다.

제안 프로토콜은 전체적으로 [그림 3]과 같은 단계로 동작된다. 무선 구간에서 데이터의 전송을 최소화하여 전송효율을 효과적으로 높였다. 아울러 태그에서의 연산량을 줄이기 위하여 복잡한 계산은 데이터베이스와 리더에서 이루어지며 5단계로 인증을 완료하는 방식이다.

[그림 3]은 다음과 같은 단계로 동작한다.

◎ [Step 1] 태그 → 리더

태그 T는 리더로부터 Query를 수신한 후 응답 메시지를 생성하고 리더에게 전송한다.

태그 → 리더 : $Ta,pkd,H(S),xa1_{public}$

◎ [Step 2] 리더 → 데이터베이스

태그에서 전송한 $Ta,pkd,H(S),xa1_{public}$ 값과 리더가 가지고 있는 값을 계산하여 $Tb,skd,(xa1_{publics},a2,k)(a2)$를 생성후 데이터베이스로 전송한다.

리더 → 데이터베이스 : $Tb,skd,(xa1_{publics},a2,k)(a2)$

◎ [Step 3] 데이터베이스 → 리더

데이터베이스에서 확인하고 생성한 인증 값을 리더에게 전송한다.

데이터베이스 → 리더 : $H(S)\oplus(T,x,ka1_{public})(a2)$

◎ [Step 4] 리더 → 태그

리더는 데이터베이스에서 수신한 값을 이용하여 $ka1_{public},((x,k)(x))(k)\oplus H(S)$를 생성후 태그에게 메시지를 전송한다.

리더 → 태그 : $ka1_{public},((x,k)(x))(k)\oplus H(S)$

◎ [Step 5] 태그 → 리더

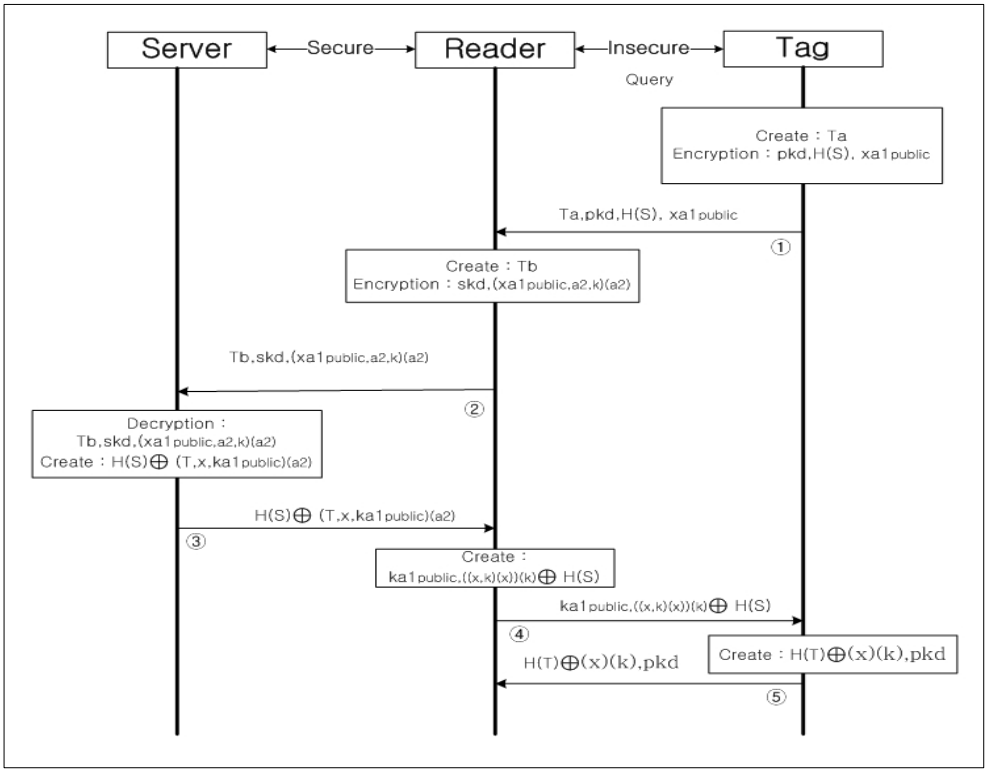
마지막으로 태그는 리더에게 자신의 정보를 암호화하여 리더에게 전송한다.

태그 → 리더 : $H(T)\oplus(x)(k),pkd$

3.2 Casper 코드 명세

제안하는 보안 프로토콜은 각종 변수유형선언, 초기상태, 동작절차, 보안속성, 데이터 타입, 함수선언, 에이전트 상태, 공격자 모델 등 총 8개 영역을 명세 한다. 제안 보안 프로토콜에서 중요한 변수유형선언, 초기상태, 동작절차, 보안속성의 주요 3개의 영역을 <부록>으로 첨부하였으며 간단한 설명은 다음과 같다[7][12].

변수들과 함수타입은 <#Free variables> 부분에 정의된다. T, R은 에이전트로써 태그와 리더이며 S는 데이터베이스 서버를 정의하는 에이전트를 나타낸다. 변수 x, k는 Nonce 타입이다. pkd, skd 는 공개키를 나타내고, a1, a2는 통신 스텝의 세션키를 나타내며, H는 해시함수연산을 나타낸다. Ta, Tb 타임스탬프를 나타낸다. Casper 스크립트에서 사용되는 해시함수는 <#Free variables>부



[그림 3] 제안 프로토콜 동작 순서도

분에서 해시함수 형식으로 선언되며, H(m)은 메시지 m에 대한 H의 함수 값으로 계산됨을 나타낸다. 또한 송신자와 수신자는 모두 H(m)을 생성할 수 있어야 된다. 수신자는 자신이 계산한 값과 받은 값이 같다면 정상인증을 하게 된다. InverseKeys = (pkd,skd),(k,k),(a1,a1),(a2,a2),(x,x)는 각 함수별 서로의 역의 키들을 반환한다는 의미로 선언되었다.

<#Processes> 부분은 호스트의 역할, 변수, 함수들을 정의한다. 본 논문에서는 INITIATOR와 RESPONDER 등 이름들은 에이전트를 나타내는 CSP에서 프로세스의 이름으로 사용된다. 이는 프로토콜 명세에서 R로 표현되는 에이전트는 인자 R은 매개변수 화된 CSP 프로세스 INITIATOR로 표현된다. R은 송신자 역할을 하고 S와 통신을 한다.

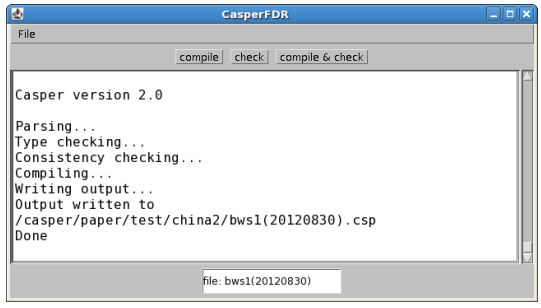
#Protocol description에는 프로토콜에서의 주요부분으로 메시지 전송순서에 대한 정의이다. 정수 0. 1. 2. 3. 등은 상호 전달되는 메시지의 순서를 나타낸다. 0번 메시지는 통신을 시작하는 R 호스트가 어떤 상대와 통신해야 하는지 알려주기 위해 사용되어진다. 표현식 m%enc에서 m은 전달하고자 하는 메시지를 의미하고, enc는 메시지를 저장하기 위한 변수로 사용된다. 즉 T는 메시지 1의 컴포넌트를 변수 enc에 저장하여 메시지 2의 두 번째 컴포넌트에게 전달한다. 이는 에이전트들이 자신이 받은 메시지가 어떤 형식의 메시지인지 분간할 수 없게 된다. 또한 메시지를 수신한 호스트가 메시지 m을 복호화 할 수 없고, 단지 다른 호스트에 전달만하는 기능을 표현하기 위해 사용된다. 타임스탬프와 공개키를 적용하여 통신과 상호 인증을 하며 이때 구간별로 해시함수를 사용함으로 데이터 전송량을 줄인 것이 특징이다.

<#Specification> 부분 명세코드로써 검증하고자하는 프로토콜의 보안속성을 정의한다.

- Secret(T, x, [R])는 호스트 T는 변수 x를 R 호스트만 알고 있는 비밀성을 공유한다고 정의한다.
- Secret(T, k, [R])는 호스트 T는 변수 k를 R 호스트만 알고 있는 비밀성을 공유한다고 정의한다.
- Agreement(R, T, [k])는 호스트 T는 변수 k를 이용하여 호스트 R로부터 인증을 받는다.
- Agreement(R, T, [x])는 호스트 T는 변수 x를 이용하여 호스트 R로부터 인증을 받는다.

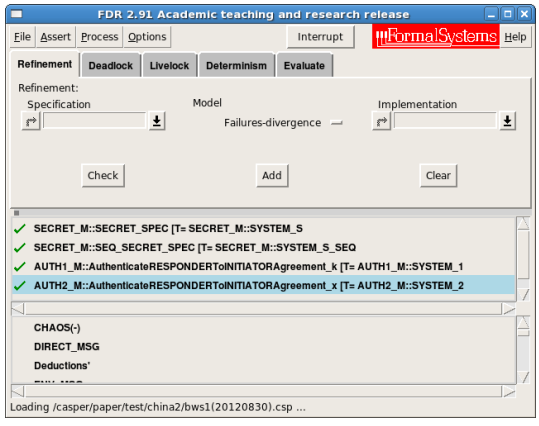
3.3 검증결과

[그림 4]와 같이 정상적인 Casper 언어로 오류 없이 명세 되어야 컴파일이 실행되며 제안한 프로토콜을 컴파일 한 결과 정상적인 CSP 파일의 변환이 이루어진다. 이때 컴파일 실행도중 오류가 발생하면 소스파일에서 오류를 수정한 후 다시 처음부터 컴파일 작업을 해야 한다.



[그림 4] FDR 검증결과

FDR 2.91 버전의 모델검증 도구를 이용하여 본 논문에서 설계한 프로토콜의 안전성(safety), 교착상태(deadlock), 라이브락(livelock) 등의 동작을 검증하기위해 FDR을 실행한다. 제안하는 프로토콜을 FDR 도구를 이용한 프로토콜 검증하기 위해 각각 항목을 순차적으로 실행해본 결과 [그림 5]와 같이 '√'표기로 프로토콜이 안전함이 표기된다. 제안 프로토콜은 모든 항목에서 안전함이 확인되었다.



[그림 5] FDR 검증결과

[그림 5]에는 4가지 검증 결과가 제시되며 각 결과의 표현은 다음과 같이 분석된다.

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

프로토콜의 보안성 확보로 메시지 앞의 체크표시는 프로토콜이 공격자에게 노출되지 않았음을 표현한다.

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

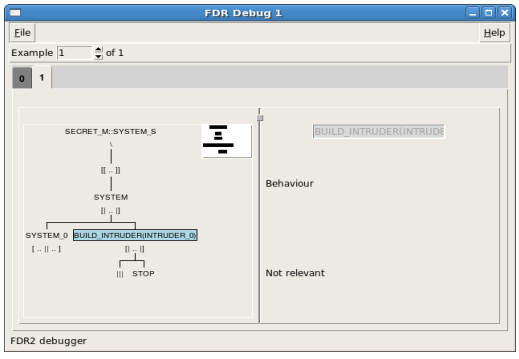
이 항목은 프로토콜이 시스템에서 정상적인 프로세스로 동작하는지를 확인 한 결과이며 제안한 프로토콜은 안전한 프로세스로 동작함을 확인하였다.

3) AUTH1_M::AuthenticateRESPONDERToINITIATOR Agreement_k[T=AUTH1_M::SYSTEM_1

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

3,4는 k, x를 통해서 Responder와 Initiator가 서로 인증할 수 있는지 검증한다는 의미로 서로 안전하게 인증함이 확인되었다.

[그림 6]에는 FDR이 제공하는 디버그 상태이다. 프로토콜에 취약성이나 문제가 발생하면 단계별로 확인하여 프로토콜의 취약점을 제거 할 수 있도록 지원된다. 제안 프로토콜은 오류 없이 검증됨을 확인할 수 있었다.



[그림 6] FDR 디버그 상태창

3.4 기존 프로토콜과의 비교 검토

본 논문에서 제안한 프로토콜은 <표 2>와 같이 보안요구사항을 만족함으로써 보안에 안전함을 알 수 있다. 해시락 기법은 공격자가 정당한 리더로 가장하여 태그로부터 metaID를 수신하고 이 metaID를 악의적 태그에 입력했을 때 악의적 태그는 정당한 태그로 가장한다. 이후 리더로부터 Query 의 응답에 키를 획득하게 된다.

〈표 2〉 프로토콜의 안전성비교

	해시락 기법 [2,8,10]	Kenji *et al.*기법[6]	제안 프로토콜
스푸핑 공격	취약	중간	안전
재전송 공격	취약	취약	안전
트래픽분석 공격	취약	안전	안전
위치추적 공격	취약	중간	안전
도청 공격	취약	취약	안전

마지막 세션에서 태그의 ID가 직접 전달되기 때문에 결국 metaID, key, ID를 모두 노출하게 되어 [그림 1]의 FDR 검증결과와 같이 스푸핑, 재전송, 트래픽분석, 위치추적, 도청 공격이 가능한 문제가 있다. Kenji *et al.* 기법[6]은 초기에 암호화하지 않은 형태의 데이터로 위조가 가능하여 [그림 2]의 Kenji *et al.* 프로토콜의 FDR 검증결과와 같이 재전송 공격, 도청 공격 등에 취약하며 스푸핑 공격, 위치추적에 중간 정도의 취약성이 있다. 반면 제안 프로토콜은 공격자가 정당한 리더로 가장하여 Query를 전송한다면, 태그로부터 $Ta, pkd, H(S), xa1_{public}$를 획득할 수 있다. 그러나 이 정보를 악의적인 태그에 넣어 리더에 대한 응답으로 전송하게 되면, 공격자는 다음 세션의 타임스탬프 Ta 값을 알아내기는 이론적으로 불가능하다. 아울러 각 세션별 모든 단계를 암호화 전송함으로써 동일한 값이 전달되는 경우는 없다. 따라서 제안 프로토콜의 안전성이 정리증명으로 입증되며 모델검증 실험에서도 동작에 안전함이 확인되었다.

4. 결론

본 논문에서 제안한 프로토콜은 타임스탬프, 세션키, 난수, 해시락 및 XOR를 이용하여 설계하였으며 정형검증 기법으로 보안속성을 만족하는지 검증을 실험하였다. 제안 프로토콜을 Casper, FDR 프로그램을 사용하여 검증결과 보안 안전성(safety), 교착상태(deadlock),라이브락(Livelock)등 보안적인 측면에서 안전함을 보였다. 제안 프로토콜을 실제 RFID 시스템에 적용할시 다음과 같은 기대효과가 예상된다. 첫째, RFID 및 무선 통신보안 분야에 까지 적용하여 사용할 수 있으며 현 시점에서 안전한 무선시스템을 구축할 수 있다. 둘째, 정리증명에 비하여 검증된 프로그램을 이용하는 방식으로 실 시스템에 적용할시 설계오류를 최소화 할 수 있다. 셋째, 최근 제안

되는 프로토콜에 비해 복잡하거나 계산 량이 많지 않아 효율적인 시스템을 구성할 수 있다. 끝으로 향후 태그의 종류별로 최적화된 프로토콜 설계로 좀 더 세분화된 연구를 진행할 계획이다.

참 고 문 헌

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

[2] C.A.R Hoare. Communicating Sequential Processes. Prentice-Hall. 1985

[3] Deborah Platt Majoras, “Radio Frequency Identification: Applications and Implications for Consumers,” *Workshop Report from the Staff of the Federal Trade Commission, Federal Trade Commission*, March 2005.

[4] Formal Systems(Europe) Ltd, Oxford University Computing Laboratory, "Failures-Divergence Renement," FDR2 User Manual, 19th October 2010.

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

[6] Gene Tsudik, “YA-TRAP: Yet Another Trivial RFID Authentication Protocol,” *Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, pp. 640-643, March 2006.

[7] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", *Financial Cryptography*, March 2005.

[8] I. Syamsuddin, T. Dillon, E. Chang, and S. Han, "A survey of RFID authentication protocols Based on Hash-Chain method," *ICCIT*, pp. 559-564, November 2008.

[9] J. Aragones, A. Martinez-Balleste, and A. Solanas, “A brief survey on rfid privacy and security,” *In World Congress on Engineering, vol II*, July 2007.

[10] Jihwan Lim, Heekuck Oh, SangJin Kim, A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection, *ISPEC 2008, LNCS*, vol. 4991, pp. 278 - 289 , April 2008.

[11] Kenji Imamoto and Kouichi Sakurai, "Design and Analysis of Diffie-Hellman Based Key Exchange Using ID by SVO Logic," *Proc. Electronic Notes in Theoretical Computer Science*, pp. 79-94, June 2005.

[12] Lee Y.C, Hsieh Y.C, You P.S, Chen T.C, "An improvement on RFID authentication protocol with privacy protection," *ICCIT*, pp. 569-573, November 2008.

[13] Mala Mitra. "Privacy for RFID Systems to Prevent Tracking and Cloning", *International Journal of Computer Science and Network Security*, Vol 8 No 1, pp. 1-5, January 2008.

[14] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *In Security in Pervasive Computing, LNCS*2802, pp. 201-202, 2005

[15] 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, 164 - 177, February 2012.

[16] Yeha, T. C, Wua, C. H, Tsengb, Y. M, “Improvement of the RFID authentication scheme based on quadratic residues”, Computer Communications, vol 34, pp. 337 - 341, March 2011.

[17] Yu Shucheng, Ren Kui, Lou, Wenjing, "A privacy-preserving lightweight authentication protocol for low-cost RFID tags," *IEEE MILCOM*, pp. 1-7, October 2007.

[18] Yu Tian-tian, Feng Quan-yuan, "A Security RFID Authentication Protocol Based on Hash Function," *ieec*, pp.804-807, 2009 International Symposium on Information Engineering and Electronic Commerce, 2009

〈부록〉 제안 프로토콜의 Casper 소스코드(3개영역)

```
#Free variables
T, R : Agent
S : Server
x, k : Nonce
H : HashFunction
pkd : PublicKey
skd : SecretKey
a1, a2 : SessionKey
Ta, Tb : TimeStamp
InverseKeys = (pkd,skd),(k,k),(a1,a1),(a2,a2),(x,x)

#Processes
INITIATOR(T, R, S, x, a1, pkd, skd)
RESPONDER(R, S, k, a2, pkd, skd)
SERVER(S, T, R, a1, a2, pkd, skd)

#Protocol description
0.   -> T : R
1. T -> R : Ta,pkd,H(S), {x}{a1}%enc1
[R !=T]
2. R -> S : Tb,skd,{enc1%{x}{a1},a2,k}{a2}
3. S -> R : H(S)(+){T,x,{k}{a1}%enc2}{a2}
4. R -> T : enc2%{k}{a1},{{x,k}{x}}{k}(+)H(S)
5. T -> R : H(T)(+){x}{k},pkd

#Specification
Secret(T,x,[R])
Secret(T,k,[R])
Agreement(R,T,[k])
Agreement(R,T,[x])
```


배 우 식

- 1997년 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2012년 2월 : 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 2009년 ~ 2010년 : 한국산학기술학회 이사 역임
- 2010년 ~ 현재 : 한국융합학회 상임총무이사
- 2010년 ~ 현재 : 중소기업정보기술융합학회 연구이사
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템
- E-Mail : bws@motor.ac.kr

이 종 연

- 1987년 2월 : 충북대학교 대학원 전자계산기공학과(공학석사)
- 1999년 2월 : 충북대학교 대학원 전자계산학과(이학박사)
- 1990년 ~1 996년 : 현대전자산업(주) 소프트웨어연구소와 현대정보기술(주) CIM사업부 책임연구원
- 1999년 ~ 2003년 : 강원대학교 삼척캠퍼스 정보통신공학과 조교수
- 2003년 ~ 현재 : 충북대학교 디지털정보융합학과 교수
- 2001년 ~ 2009년 : IEEE member
- 2003년 ~ 2004년 : 한국정보처리학회 논문지편집위원 데이터베이스분과 이사 역임.
- 2010년 ~ 현재 : 한국컴퓨터교육학회 이사(현)
- 2010년 ~ 현재 : 한국융합학회장(현)
- 관심분야 : 질의처리 및 최적화, 근사질의응답(AQA), 데이터베이스시스템, 데이터 마이닝, 유통물류, GIS, e-Learning과 평가방법, 정보영재교육.
- E-Mail : jongyun@chungbuk.ac.kr