AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계

이남기*, 장태민, 전병찬, 전진오, 유수봉, 강민섭
*안양대학교 컴퓨터공학과
e-mail: southat@gmail.com

Design of Robust RFID Authentication Protocol Using AES Cipher Processor

Nam-Ki Lee*, Tae-Min Chang, Byung-Chan Jeon, Jin-Oh Jeon,
Su-Bong Ryu, Min-Sup Kang
*Dept of Computer Science, Anyang University

요 약

본 논문에서는 RFID 시스템의 Tag와 Reader 사이의 보안상의 문제점을 해결하기 위하여 공격에 강인한 AES 암호 프로세서 기반 인증 프로토콜을 제안한다. 제안한 인증 프로토콜은 Reader에서 난수를 생성하고 Tag와 Reader 그리고 Back-End Server의 인증과 통신 데이터를 암호화 하여 기존의 보안상의 문제점을 개선하고, ISO/IEC 18000-3 표준 프로토콜을 기반으로하여 확장된 패킷 구조를 사용한다.

제안한 시스템은 Xilinx ISE 9.1i 환경에서 Verilog HDL을 사용하여 설계하였으며, 설계 검증은 Mentor 사의 Modelsim 6.2c를 사용하여 제안된 시스템이 정확히 동작함을 확인하였다.

1. 서론

RFID(Radio Frequency IDentification) 기술은 IC칩과 무선을 통해 식품, 동물, 사물 등 다양한 개체의 정보를 식별하는 대표적인 근거리 자동 인식 기술로써 기존의 바코드 및 스마트카드 인식기술과 비교해 볼 때 한층 진보된 차세대 인식 기술이며, USN(Ubiquitous Sensor Network)의 핵심 기술 분야이다[1].

RFID 시스템은 최근 수많은 분야에서 각광을 받고 있는 기술이지만, 무선으로 전송되는 정보에 대한 보안과 프라이버시 보호는 문제로 지적되어왔다. 이를 해결하기 위해서는 강도 높은 수준의 암호화 알고리듬을 이용한 정보의 암호화가 필수적이다[2,3].

RFID Tag의 프로토콜을 정의하고 있는 ISO/IEC 18000-3 standard는 Reader와 Tag 사이에 양방향 통신에 사용된다[6]. 그러나 이 두 장치사에서의 데이터 교환은 안전하지 못한다. 즉 이 프로토콜이 Challenge-response 절차로 사용될 때 Man-in-the-middle attack에 취약하며, 제 3자로부터 공격에 취약하다[7].

기존의 해쉬 함수를 이용한 인증 프로토콜 방식은 ID가 노출되는 문제점과 Tag에 난수 생성부를 추가적으로 가져야 하는 단점이 있다. 이와 같은 RFID 시스템의 보안문제를 해결하기 위해서 Tag와 Reader간의 통신은 모두 암호화하는 방법이 제안되었다[4].

본 논문에서는 AES 암호 프로세서를 이용한 공격에 강인한 RFID 인증프로토콜을 제안한다. 제안한 방법은 보안성 강화를 위해 기존의 ISO/IEC 18000-3 표준 프로토콜의 패킷 구조를 수정·확장하여 사용한다. 제안한 시스템은 Xilinx ISE 9.1i 환경에서 Verilog HDL을 사용하여 설계하였으며, Xilinx Vertex XCV400E 디바이스를 Target으로 시스템을 구현하였다. 시스템의 검증은 Mentor Graphics 사의 Modelsim 6.2c 시뮬레이터를 사용하였으며, 시뮬레이션 결과를 통하여 설계된 시스템이 정확히 동작함을 확인하였다.

† 본 연구는 중소기업청 "2007 년도 산학연 공동기술개발 컨소시엄사업"과 IDEC 지원으로 수행되었음.

2. 관련 연구

2.1 RFID 시스템

RFID 시스템은 크게 Tag, Reader, Back-End Server로 구성된다. Tag는 고유 ID를 가지는 IC칩과 무선통신을 위한 안테나로 구성되어 있으며, Reader로부터 Query를 받아 Reader로 정보를 전송하는 역할을 담당한다.

Reader는 Tag로부터 정보를 받아들이는 역할을 하며 RF 신호의 발신, 수신과 데이터 디코딩을 하는 부분을 포함하고 있으며 Back-End Server 와의 통신을 수행하며, 읽기와 쓰기 기능이 모두 가능한 장치이다. 이때 Tag와 Reader의 통신구간은 Insecure channel로 보안에 취약하다.

Back-End Server는 Reader를 통하여 얻어진 Tag의 정보를 응용하는 부분으로 Database 서버와 네트워크, 응용프로그램을 총칭한다[1,6].

2.2 표준 통신 인터페이스

표준 통신 인터페이스는 변조, 프레이밍, 충돌방지 메커니즘, 프로토콜 파라미터, 기타 정보의 제공 등으로 구성되어 있다.

표준 통신 인터페이스에 따르면, 변조 방식은 ASK (Amplitude Shift Keying)방식을 많이 사용하며, 데이터 전송은 SOF(Start-of-frame)와 EOF(End-of-frame)의 구분자 사이에 데이터를 첨부하여 전송한다.

데이터 전송은 "Reader talks first"를 기본 개념으로, Reader가 Tag에게 요청 데이터를 전송하고, Tag는 이 요청 데이터를 분석하여 응답 데이터를 재전송하는 형태이다. 데이터는 크게 네 부분으로 구성되는데 각 각은 다음과 같다[6].

• Flags : 데이터의 전송 타입, Tag의 접근 방식, 데이터 rate 등의 정보를 기술하며, Tag는 이 정보를 기반으로 에러유무를 체크한다.

• Command code : Tag의 동작을 나타냄. 크게 3가지의 그룹으로 구성되어지며, Mandatory Command는 반드시 구현되어야 한다.

• Parameters and data fields : Command code의 데이터로 Command code의 동작에 필요한 데이터를 나타낸다.

• CRC : 통신상의 에러 체크영역으로, CRC알고리듬을 통하여 SOF와 EOF 데이터는 포함되지 않는다.

통신에 사용되는 Command code는 Inventory와 Select이며, 이 Command code의 통신 format을 변경하여 동작을 수행한다[6,7]. (그림 1)은 General request format 이고, (그림 2)는 General response format 이다.

SOF	Flags	Command code	Parameters	Data	CRC16	EOF

(그림 1) General request format

SOF	Flags	Parameters	Data	CRC16	EOF

(그림 2) General response format

표준 통신 인터페이스는 이 외에도 Custom Command에 대한 기술 방법 등에 대하여도 기술하고 있는데, 인증이나 보안을 위한 부분은 기술이 되어 있지 않다. 즉, 인증이나 보안을 행하기 위해서는 Custom Command를 이용하여 구현하여야 한다.

3. 강인한 인증 프로토콜

3.1 개선된 인증 프로토콜

RFID 시스템에서 무선으로 전송되는 Tag의 정보를 보호하기 위해 기존에 사용되는 해쉬 함수를 이용한 인증 프로토콜 방식은 ID 노출과 Tag에 난수 생성부를 추가적으로 가져야 하는 단점이 있다[2,3].

본 논문은 Reader에서 난수를 생성하고 Tag, Reader, 그리고 Back-End Server의 통신 데이터를 암호화 하여 보안에 강인한 인증 프로토콜을 제안한다. 또한, Replay-attack을 방지하기 위하여 Back-End Server와 Tag의 CD(Change Data)를 변경하는 기법을 제안한다. 제안하는 프로토콜은 <표 1>와 같은 표기를 통하여 기술한다.

<표 1> 용어 설명

용 어	설 명
Back-End Server	데이터베이스를 가진 Server, Tag의 정보를 기억
Reader	암/복호화 기능이 추가된 RFID Reader
Tag	암호화 기능이 추가된 RFID Tag
ID	Tag 고유 ID, UID(Unique identification number)
CID	Reader에서 ID와 CD를 Exclusive OR 연산한 변경 ID
k	Back-End Server, Reader, Tag가 공통으로 가지는 비밀 키
RN	Reader의 난수 생성기에 의해서 생성되는 난수
RN_1	Server의 난수 생성기에 의해서 생성되는 난수
CD	Changed 데이터로써 Server와 Tag간의 인증에 사용
Ek()	암/복호화 키 k로 데이터()를 암호화
⊕	Exclusive OR 연산

(그림 3)은 개선된 인증 RFID 프로토콜로서 프로토콜의 암호화 및 인증과정은 다음과 같다.

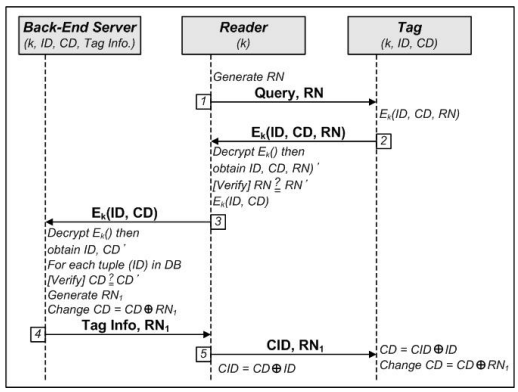
Step 1) Reader는 Query와 생성된 RN을 Tag로 전송

Step 2) Tag는 메모리에 있는 ID, CD와 전송된 RN값을 암호화하여 Reader로 전송

Step 3) Reader는 Tag로부터 전송받은 데이터를 복호화 하여 얻은 RN′과 처음에 생성했던 RN을 비교하여 Tag 인증, 인증이 되면 ID와 CD를 암호화하여 Back-End Server로 전송

Step 4) Back-End Server는 Reader로부터 전송된 데이터를 복호화 후 DB에서 ID를 검색하여 대응되는 CD를 비교, 일치하면 난수 RN_1을 생성하여 해당 ID의 CD와 XOR 하여 CD를 변경, Tag 정보와 RN_1을 Reader로 전송

Step 5) Reader는 Tag 정보 확인 후 CID 생성하여 Tag에 RN_1과 함께 전송, Tag는 전송받은 CID와 ID를 XOR하여 생성된 CD와 기존의 CD를 비교 후 인증이 되면, Reader로부터 받은 RN_1을 XOR 연산하여 CD를 변경



(그림 3) 개선된 인증 RFID 프로토콜

제안하는 프로토콜은 강인한 보안을 위해 AES 알고리듬을 사용하여 시스템에 적용 하였다.

3.2 확장된 패킷 구조

제안하는 인증 프로토콜에 따라, Reader에서 생성된 RN 데이터를 추가하였다. RN은 데이터 전송 시 많은 부하를 가지지 않도록 16 bit를 가지도록 구성하였다.

제안하는 인증 메커니즘에 따라 Tag는 Reader의 Inventory request 에 반응하여 (그림 5)와 같이 UID를 포함한 Ek(AES Encrypt) 데이터를 전송하게 된다. 이 UID 데이터는 Tag의 고유 ID이며, 이 ID는 세계적으로 유일한 코드로 구성된다 Ek(AES Encrypt)는 암호프로세서에 의해 생성된 암호화 데이터이다.

(그림 4)는 제안하는 Modified Inventory request format 이고, (그림 5)는 제안하는 Modified Inventory response format 이다.

SOF	Flags (8bits)	Inventory (8bits)	Optional AFI (8bits)	Mask length (8bits)	Mask value (0-64bits)	RN (16bits)	CRC (16bits)	EOF
	0x27	0x01	null	0x00	0x00	0xABCD	0x61CF	

(그림 4) Modified Inventory request format

SOF	Ek(AES Encrypt) = "0xD3E2F30ADE47D80D03808B99DF00580"						EOF
	Flags	DSFID	UID	CD	RN	CRC	
	8bits	8bits	64bits	16bits	16bits	16bits	

(그림 5) Modified Inventory response format

Select Command는 선택된 Tag를 식별할 수 있도록 Tag의 CID를 함께 전송한다. Select Command는 Inventory Command를 통하여 식별된 Tag의 ID 정보를 사용한다. 이 CID를 통하여 여러 개의 Tag를 구분하여 원하는 Tag를 작동시킨다. (그림 6)은 제안하는 Modified Select request format 이다.

SOF	Flags (8bits)	Select (8bits)	CID (64bits)	RN_1 (16bits)	CRC (16bits)	EOF
	0x23	0x25	0xE2B5F5F8FFFFF81F	0xEF12	0xE8B5	

(그림 6) Modified Select request format

CID는 UID와 CD 데이터를 XOR 연산하여 Back-End Server에서 생성한 RN_1 데이터를 함께 전송한다. RN_1 데이터는 replay-attack을 방지하기 위하여 Tag의 CD 데이터를 변경하는 데이터이다. 이를 통하여 다음 통신 시에는 Tag가 다른 CD 데이터를 가짐으로써 replay-attack을 방지가 가능하다.

3.3 안전성 분석

일반적으로 통신상에서 나타날 수 있는 문제는 다음과 같다[4].

• Man in the middle attack : 통신을 하는 두 개체의 통신 내용을 가로챈다.

• replay attack : 통신상에 발생한 데이터를 보관하고 이를 다음 통신에 사용한다.

• forgery : 통신상의 데이터를 위·변조한다.

• 데이터 loss : 통신상의 데이터가 외부의 공격에 의하여 사라지거나 일부를 잃어버린다.

RFID시스템을 사용한 통신상에서는 이 뿐만이 아니라 Tag의 복사까지도 발생할 수 있다. 보안의 관점에서 다음의 특징들을 만족하여야 하며, 제안하는 프로토콜은 다음과 같은 특징을 만족한다.

• 데이터 confidentiality : 데이터의 전송 시 데이터의 비밀성을 만족하여야 한다. 이는 전송하는 데이터를 man in the middle attack이나 replay attack을 방지하기 위함이다. 이를 위하여 제안하는 프로토콜은 AES 암호프로세서를 사용하여 보안 강인된 암호화데이터를 전송한다.

• Tag Anonymity : 데이터의 전송 시 데이터의 공급자 및 수요자에 대하여 익명성을 제공하여야 한다. RFID의 특성상 이는 만족하기 어렵지만, Tag로부터 받은 정보를 통하여 Reader가 여러 Tag들에 대하여 ID를 바로 알 수 없다는 점을 통하여 이를 만족시키고 있다.

• 데이터 Integrity : 데이터의 전송이 데이터가 위·변조되지 않도록 해야 한다. 이를 위하여 Reader에서 생성된 난수 RN과 Tag와 Reader에 암호화된 데이터를 전송하도록 하여 위·변조 되지 않도록 하였다.

<표 2>는 기존 프로토콜과 제안하는 프로토콜을 비교 분석 하였다. Tag와 Back-End Server의 상호 인증 통신이 가능하며 암호화 데이터로서 도청 및 통신 내용분석이 안전하다. 또한 위치트래킹과 스푸핑에 대해 안전하며, Tag와 Back-End Server에 가지고 있는 CD 값은 RN_1을 연산하여 CD 값을 변경함으로써 다음 통신에서 같은 데이터가 전송되지 않도록 하여 replay-attack을 방지가 가능하다.

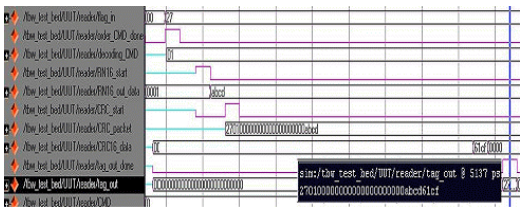
<표 2> 기존 프로톨과의 비교 분석

구분	Randomized Hash Lock	Hash Chain	ID 가변 정보화	제안프로토콜
상호 인증	불가능	가능	불가능	가능
도청 및 통신내용분석	안전	안전	안정	안전
위치트래킹	안전	불안전	안전	안전
스푸핑 (위조여부)	불안전	안전	불안전	안전
Replay-attack 방지	가능	가능	불가능	가능
Tag 계산량	해쉬 1번, 난수 생성 1번	해쉬 2번	곱셈 4번, n회마다 해쉬 1번	암호화 1회, XOR 연산 1회

4. 프로토콜 검증

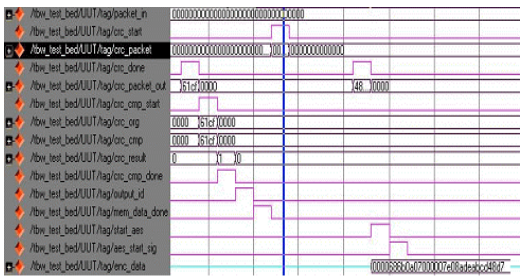
제안한 AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜은 Xilinx ISE 9.1i 환경에서 Verilog HDL을 사용하여 설계하였으며, Xilinx Virtex XCV400E 디바이스를 Target으로 시스템을 설계하였다. 시스템의 검증은

Mentor Graphics 사의 ModelSim 6.2c 시뮬레이터를 사용하였고 설계된 시스템이 시뮬레이션 결과를 통하여 정확히 동작함을 확인하였다. 테스트에 사용한 입력 패킷의 UID는 "0x686B0A07000007E0", CD는 "0x8ADE" 그리고 AES Key값은 "0x2B28AB097EAEF7CF15D2154F16A6883C"이 사용되었다[8].



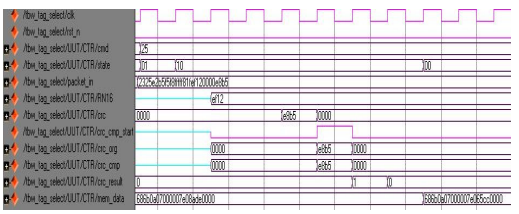
(그림 7) Reader에서 Inventory packet값을 만드는 과정

(그림 7)은 Reader에서 inventory packet 값을 만드는 과정을 나타낸다. order_CMD_done 신호가 입력되면 명령어 해석을 통해 inventory 명령어가 생성된다. 명령어 생성 과정이 끝나면 랜덤 발생기를 통해 Reader에서 생성된 RN과 flag, command code로 이루어진 Packet이 생성 된다. Packet 데이터는 Flags, Inventory, Mask length, Mask value, RN, CRC로 "0x270100000000000000000abcd61cf" 이며, (그림 4)와 같다.



(그림 8) Tag의 packet을 생성하는 과정

(그림 8)은 CRC 검증을 한 후 Tag의 packet을 생성하는 과정을 나타낸다. 암호화 할 데이터는 Flags, DSFID, UID, CD, RN, CRC로 이루어진 "0000686b0a07000007e08adeabcd48d7"이며 암호화 데이터는 "0xD3E2F30ADE47D80D03808B99DF00580"로, (그림 5)와 같다.



(그림 9) Tag를 Select하는 과정

(그림 9)는 Reader에서 생성된 데이터로 Tag를 Select 하는 과정을 나타낸다. 데이터 "2325e2b5f5f8fffff81fef120000e8b5"는 Tag로 전송된 Select packet으로 (그림 6)과 같다. Tag은 전송된 데이터의 CRC 검증과 CID 검증을 하게 된다. CID가 검증되면 CD값을 RN_1인 "ef12"와 xor 연산하여 새로운 CD값을 생성하게 된다. 데이터 "686b0a07000007e065cc" 는 Tag의 64bits ID와 갱신된 CD를 나타내며 메모리에 저장된다.

5. 결론

RFID Tag의 프로토콜을 정의하고 있는 ISO/IEC 18000-3 standard는 Reader와 Tag 사이에 양방향 통신에 사용되며, 이프로토콜이 Challenge-response 절차로 사용될때 Man-in-the-middle attack에 취약하며, 제 3자로부터 공격에 취약하다.

본 논문에서는 AES 암호 프로세서를 이용하여 공격에 강인한 RFID 인증프로토콜을 제안하였다. 제안한 방법은 보안성 강화를 위해 기존의 ISO/IEC 18000-3 표준 프로토콜의 패킷 구조를 수정·확장하여 사용한다. 제안한 프로톨의 검증을 위해 Mentor Graphics 사의 ModelSim 6.2c 시뮬레이터가 사용되었고, 시뮬레이션 결과를 통하여 제안한 프로토콜의 강인성이 입증되었다.

참고문헌

[1] 무선인식(RFID) 산업 활성화 지원센터, http://rfidepc.or.kr

[2] 서운석, 신순자, 구자동, 임진수, "유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구", 한국전산원, 2004.

[3] 전진오, 유수봉, 박상조, 강민섭, "Strong Authentication Protocol for RFID Tag Using SHA-1 Hash Algorithm" IEEE ICCSA, 2007.

[4] 전진오, 유수봉, 최호영, 강민섭, "Digital Codec Design for RFID Tag Based on Cryptographic Authentication Protocol", IEEE FGCN, 2007.

[5] 주학수, "RFID System의 보안 및 프라이버시 보호를 위한 기술 분석", 전자정보센터, 2004.

[6] ISO/IEC 18000-3, "Information technology AIDC techniques－RFID for item management Air interface,－Part 3: Parameters for air interface communications at 13.56 MHz", ISO, 2003.

[7] 서영준, 이현록, 김광조, "A Lightweight Authentication Protocol based on Universal Re-encryption of RFID Tags", University of Kaiserslautern.

[8] Joan Daemen, Vincent Rijmen, "AES Proposal : Rijndael", (http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf)

[9] 호정일, 이강, 조윤석, "저비용 FPGA를 이용한 AES 암호 프로세서 설계 및 구현", 한국정보과학회 학술지, 2005.