논문 2005-42CI-6-4

유비쿼터스 환경에서 Pre-Distribution을 기반으로 한 안전한 RFID 시스템

(Approach of safe RFID system based on Pre-Distribution on Ubiquitous computing environment)

김 진 묵*, 유 황 빈*

(Jin Mook Kim and Hwang Bin Ryou)

요 약

다가올 유비쿼터스 컴퓨팅 환경에서 RFID(Radio Frequency IDentification)는 사물에 대한 인식과 차별화된 정보 제공의 수단으로 사용될 것이다. 하지만 RFID에 대한 보안서비스는 아직까지 미흡한 실정으로 이에 대한 대책 마련이 시급하다. 본 논문에서는 RFID 시스템에 대한 도청과 위조 및 변조 문제와 프라이버시 문제를 해결하기 위한 방안으로 RC5 암호 알고리즘과 Pre-Distribution 프로토콜을 사용해 이에 대한 해결책을 제시하고자 한다. 먼저 Pre-Distribution 프로토콜을 사용해 RFID 시스템에서의 2가지 주체인 태그와 리더에서 사용할 비밀키를 생성하여 분배한다. 이를 토대로 가변적이고 적은 자원 사용량을 갖는 RC5 암호 알고리즘을 이용해 RFID 시스템에 요구되는 보안 서비스를 제공할 수 있다. 제안한 안전한 RFID 시스템의 성능평가를 위해 ATmega128 환경에서의 시뮬레이션 결과를 나타내었다.

Abstract

RFID(Radio Frequency Identification) will be used for recognizing things and offering distinctive information in Ubiquitous environment. But we are not ready to provide security service to RFID. Therefore we propose the approach of safe RFID system which provides the solution for eavesdrop, forgery, and modification based on Pre-Distribution protocol and RC5 security algorithm. First We distributes the secret key to the Tag with the Reader that is major subject on RFID system using Pre-Distribution protocol. Then we will provide to various security services and privacy protection using RC5 security algorithm. The proposed safe RFID system simulated on ATmega128 evaluate environment.

Keywords: Privacy protection, RFID, Key distribution, Authentication.

I. 서 론

유비쿼터스 환경에서는 사물의 인식을 위해 기존의 바코드 시스템을 대체해 다량 인식 및 비-접촉 인식이 가능한 RFID 시스템이 적용될 것이다. 하지만 RFID 시스템 많은 보안상의 문제점들에 대한 해결책은 아직 미흡한 실정이다.

더욱이 모바일 환경의 통신 매체와 동일하게 RFID시스템의 태그는 이동성을 가지고 있으며 통신에 대한 응답 능력만을 가지고 있어 프라이버시 문제가 매우 심각할 것으로 예상된다.

이에 본 논문에서는 RFID 태그에 대한 프라이버시 보호를 위한 시스템을 제안하고 시뮬레이션을 수행해 향후 모바일 RFID 시스템이나 센서 네트워크 환경에 대한 프라이버시 보호 대책 마련 가능성을 가늠해 보려

* 정회원, 광운대학교 컴퓨터소프트웨어학과
(Dept. of Computer Science & Engineering, Kwang-Woon University)

※ 이 논문은 2005년도 광운대학교 교내연구비에 의해 연구되었음

접수일자: 2005년6월23일, 수정완료일:2005년11월4일

고 한다.

먼저 저-전력, 저-연산, 저-저장 능력을 갖는 RFID 시스템의 특징을 고려하여 Pre-Distribution 프로토콜을 사용해 암호화에 사용될 Key 분배 문제를 해결하고자 한다. 그리고 리더와 태그 사이의 통신에서 송.수신되는 데이터에 대해 RC5 암호 알고리즘을 적용하여 보안 서비스를 제공할 수 있도록 하는 방안을 제안한다. 추가적으로 RFID 시스템에 있어서 주요 보안 이슈중에 하나인 프라이버시 문제를 해결하기 위해 임시 태그 식별자를 부여하는 방안을 제안하여 개인의 프라이버시에 관한 문제를 해결할 수 있음을 보이고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 RFID 시스템에 관한 기존의 선행연구에 대해 기술한다. Ⅲ장에서는 제안하는 안전한 RFID 시스템의 구조에 대해 기술한다. Ⅳ장에서는 제안하는 시스템에 대한 설계 및 구현에 관한 내용을 다루고 Ⅴ장에서는 제안한 안전한 RFID 시스템에 대한 성능평가 결과에 대해 기술한다. 마지막으로 논문에 대한 결론에 대해 기술한다.

Ⅱ. 선행연구

RFID 시스템은 기존의 바코드로 대표되는 인식 시스템과 비교해 동시성과 대량성, 비-접촉성의 특징을 가지고 있다. 그리고 바코드 시스템과 비교해 볼 때 보다 많은 고급 정보를 수록할 수 있다는 장점을 갖는다. 하지만 하드웨어적인 제약 사항으로 인해 보안상의 위협요소들이 심각하게 많다. 이에 RFID 시스템의 환경에 대해 이해하고 적합한 해결책을 마련하는 것이 시급한 실정이다. 이를 인지한 많은 관련 분야의 학자들에 의해 선행 연구가 수행되고 있다.

본 논문에서는 선행된 관련 연구들을 2개 분야로 구분해 보안 프로토콜 분야와 프라이버시 관련기술 분야로 세분화해 살펴본다.

1. 보안 프로토콜에 관한 선행연구

첫 번째로 RFID 시스템에 보안 서비스를 제공하기 위해 선행 연구되어진 분야는 RFID 시스템의 하드웨어적인 특징을 고려한 새로운 암호 알고리즘과 이를 적용하기 위한 프로토콜 관련 분야이다. 새로운 암호 알고리즘에 관한 연구 분야는 암호 관련 학자들에 의해 활발하게 연구가 진행 중인 상태로 아직까지 공개된 암호 알고리즘이 없는 실정이다. 그리고 보안 프로토콜에 관한 분야에 대해 정리해 보면 아래의 표 1과 같다.

표 1. 보안 프로토콜에 관한 선행연구 목록
Table 1. List of related work about security protocols.

제안방법	특징
Kill 명령어	태그의 사용 목적이 소실되는 시점에서 Kill 명령을 사용해 정보를 소실하도록 하는 방법
Blocker Tag	태그의 정보를 필요에 따라 Blocking 할 수 있도록 하는 방법
Hash-Lock	리더와 태그가 사전에 Hash 값을 생성해 저장해 두고 Lock 상태로 설정하여 태그 정보의 위조 방지책
Random Hash-Lock	Hash-Lock 방식이 갖는 프라이버시 문제를 해결하기 위해 임의의 Hash 값 생성해 사용토록 하는 방식
재-암호화	인증기관에서만 추적이 가능하도록 인증기관의 공개키로 암호화하는 방식

2. 프라이버시에 관한 선행연구

두 번째로 RFID 시스템에 관한 선행 연구분야는 개인의 프라이버시 문제를 해결하기 위한 것이다. 다음에 나타내고 있는 표 2는 대표적인 프라이버시 보호에 관한 선행 연구 내용들을 정리해 나타내고 있다.

선행 연구들에 대해 살펴 본 결과, 대부분의 연구들이 해당하는 연구 목적에 편협한 분야에 대해 연구되고 있다. 그리고 공개키 기반의 보안 서비스를 제공하도록 연구가 진행 중에 있다.

하지만 RFID 시스템의 특성인 저-전력, 저-연산능력, 저-저장능력이라는 특징을 고려해 볼 때 이를 직접 수용하기에는 많은 어려움이 존재한다.

표 2. 프라이버시에 관한 선행연구 목록
Table 2. List of related work about privacy.

제안방법	특징
그룹서명	문제 발생시를 제외하고는 구성원의 서명을 밝힐 수 없도록 하는 방법
Blind 서명	전자화폐를 위한 서명 방식으로 메시지에 대한 내용에 대해 비밀성을 보장하는 서명 방법
Pseudonym	신뢰할 수 있는 인증기관이 해당하는 사용자에 대한 가명(Pseudonym)을 생성해 할당하는 방법
분산 암호	보안 서비스를 위해 사용하는 비밀키를 구성원들이 나누어 관리하도록 하는 방법

Ⅲ. 안전한 RFID 시스템에 관한 제안

1. 시스템 구성

기존의 선행연구들은 RFID 시스템의 하드웨어적인 제약조건이나 동작환경을 고려하지 않고 보안 알고리즘 자체에 대한 부분과 프로토콜 분야와 같이 단편적인 연구가 주요 골자를 이루고 있다.

하지만, 현재 현실 적용 단계에 이른 RFID 시스템을 위해서는 보다 현실적인 대책이 필요하다. 이에 본 논문에서는 RFID 시스템 동작 환경에 대한 이해를 바탕으로 Pre-Distribution 프로토콜과 가변적인 하드웨어 환경에 적용성이 높은 것으로 밝혀진 RC5 암호 알고리즘을 RFID 시스템에 적용하여 보안 서비스를 제공하고자 한다.

논문에서 제안하는 유비쿼터스 환경에서의 안전한 RFID 시스템에 대한 전체적인 구성은 위의 [그림 1] 과 같다. 제안한 시스템은 Pre-Distribution을 기반으로 하며 3개의 영역으로 구성된다.

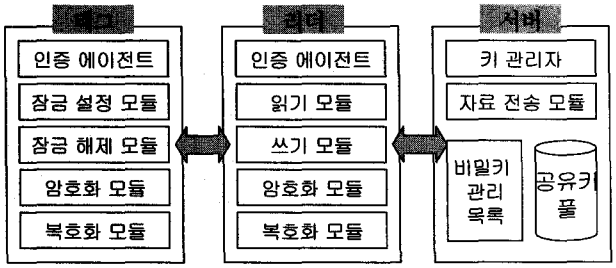

그림 1. 제안 시스템의 구성도
Fig. 1. Proposed Safe RFID system architecture.

가. 서버

서버는 리더가 요청한 태그에 대한 정보들을 제공하고 리더를 인증하며 리더와 태그 사이에 인증과 암호화를 위한 기초적인 작업들을 수행하기 위한 부분이다.

자료 전송 모듈, 키 관리자, 키 관리 목록, 공유키 풀로 구성된다. 키 관리자 모듈은 임의의 난수를 생성하여 공유키 풀에 할당해 두는 역할을 수행하고 리더와 태그 사이의 암호화에 사용할 공유키와 관련된 정보들을 관리하기 위해 키 관리자 목록을 관리하는 역할도 수행한다. 그리고 자료 전송 모듈은 리더의 요청에 대한 자료를 검색하여 전달하는 역할을 수행하는 모듈이다.

나. 리더

태그에 저장된 정보를 요청하기 위한 읽기 모듈과 태그에 새로운 정보를 저장하기 위한 쓰기 모듈을 갖는다. 추가로 리더와의 통신에 앞서 리더에 대한 인증여부를 확인할 수 있는 인증 에이전트를 갖는다.

그리고 태그와의 정보 전달을 위한 암호화 및 복호화에 관한 작업을 처리하는 모듈을 포함한다.

다. 태그

제안한 태그는 기본적으로 리더와의 통신을 통해 정보를 전달할 수 있다. 이때 상호 전달하는 정보에 대한 도청과 위조와 변조를 방지하기 위해서 전달하는 정보에 대한 암호화 및 복호화 모듈, 그리고 리더에 대한 인증 확인을 위한 인증 에이전트를 갖는다.

또한 태그에 대한 접근 제어 모듈도 포함한다. 리더에 대한 인증 작업을 수행하는 모듈은 자신의 임시 태그 식별자를 생성하는 모듈과 리더와 태그 사이의 통신에서 사용할 공유키를 검증하기 위한 모듈로 구성된다.

2. 시스템 동작과정

가. 기호 설명

제안한 시스템은 3 단계의 처리절차에 따라 동작한

기 호	설 명
‖	R‖T의 경우, R과 T를 연결하는 기호
EPC_Code	Tag 에 생산 단계에서 부여된 유일한 구분 기호(96 bits)
R_Serial	Reader에 생산 단계에서 부여된 유일한 구분 기호(8 or 13 bits)
T_ID	서버 등록과정에서 Tag에 부여된 임시 태그 식별기호(128 bits)
R_ID	서버 등록과정에서 Reader에 부여된 임시 리더 식별기호(128 bits)
K_R	사전 키 분배단계에서 생성되어 분배된 서버와 리더 사이의 비밀키(128 bits)
K_T	사전 키 분배단계에서 생성되어 분배된 서버와 태그 사이의 비밀키(128 bits)
RN_S	서버가 인증단계에서 생성해 전달하는 서버의 랜덤 값(128 bits)
RN_T	태그가 인증단계에서 생성해 전달하는 태그의 랜덤 값(128 bits)
RN_R	리더가 인증단계에서 생성해 전달하는 리더의 랜덤 값(128 bits)
K_{RT}	리더와 태그 사이에서 일반적으로 사용하는 비밀키(128 bits)
SK_{RT}	태그와 리더 사이에서 통신에 연결된 세션에 사용하는 비밀키(128 bits)
$AUTH_T$	태그와 리더 사이에서 인증확인을 위한 태그 인증값(512 bits)
$AUTH_R$	태그와 리더 사이에서 인증확인을 위한 리더 인증값(512 bits)

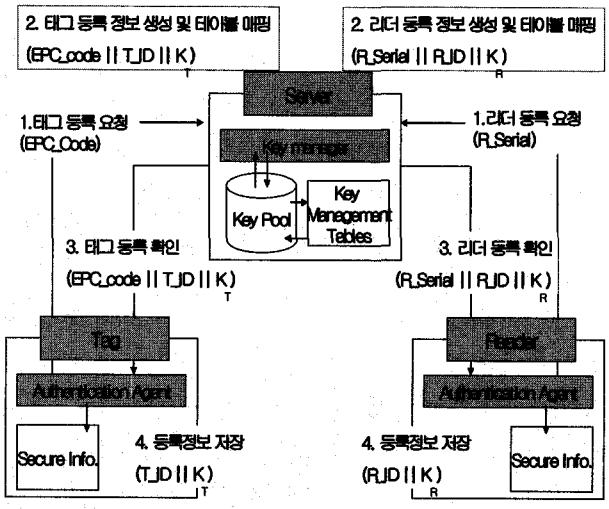

그림 2. 사전 키 분배 단계
Fig. 2. Phase 1 : Key pre-distribution.

다. 세부적인 동작과정을 나누어 살펴보면 아래의 [그림 2, 3, 4]에서 보이는 바와 같이 동작한다.

나. 사전 키 분배 단계

첫 번째로 사전의 키 분배 과정은 제안한 시스템에서 동작하는 태그와 리더를 등록하고 태그와 리더 사이에서 사용할 공유키를 분배하는 과정이다[2][3][4][5]. 이때 태그와 리더는 생산 시점에서 고유의 식별 정보를 부여받고 이를 각각 소유하고 있는 상태임을 가정한다.

① 태그 혹은 리더 등록 요청 : 태그와 리더 각각 독립적으로 서버에 등록요청을 위해 고유 식별 기호(EPC_Code 혹은 R_Serial)를 전달.
② 개체 등록정보 생성 및 테이블 매핑 : 태그나 리더의 등록 요청에 대해 고유 식별 기호에 대응하는 임시 식별자(R_ID 혹은 T_ID)를 생성하여 저장하고 각각에 비밀키(S_KEY_R 혹은 S_KEY_T)를 Key Pool로부터 선택하여 테이블에 매핑.
③ 태그 혹은 리더 등록 확인 : 태그나 리더의 등록을 수행하고 생성된 임시 식별자와 비밀키를 전달.
④ 등록정보 저장 : 리더와 태그는 각각 전달 받은 임시 식별자와 비밀키를 저장.

다. 인증 단계

사전 키 분배 단계에서 부여된 비밀키와 임시 식별자를 이용하여 통신을 요청한 리더와 태그 사이의 인증작업을 수행한다. 어를 위해 Tom Leighton에 의해 제안된 대칭키를 이용한 키 분배 알고리즘을 적용한다.

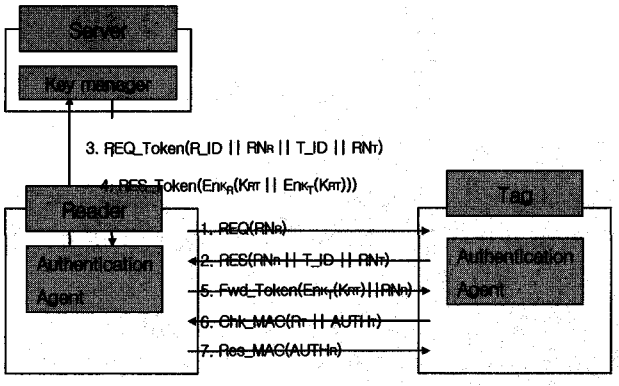

그림 3. 인증 단계
Fig. 3. Phase 2 : Authentication.

공개키 방식의 인증 알고리즘을 적용하기에는 RFID 시스템의 하드웨어적인 제약사항이 존재하는데 이처럼 Leighton의 제안을 적용함으로써 인증문제를 해결할 수 있을 것으로 보인다.

① 태그에게 토큰 생성을 위한 정보 요청 : 리더는 난수(RN_R)를 생성해 태그에게 토큰 생성을 위한 정보를 요청 하는 REQ(RN_R) 전달.
② 리더에게 태그가 응답 : 태그는 리더의 요청에 대한 응답으로 전달받은 리더의 난수, 자신의 임시 식별자와 난수를 포함하는 RES(RN_R||T_ID||RN_T) 전달.
③ 리더와 태그 사이의 공유 비밀키 요청 : 리더는 서버에게 리더와 태그 사이에서 사용할 공유 비밀키(K_{RT})를 요청하는 REQ_Token 수행.
④ 비밀 공유키를 리더에게 전달 : 리더와 태그 사이에서 사용할 공유 비밀키(K_{RT})를 태그의 비밀키(K_T)로 암호화 한 것과 공유 비밀키를 리더의 비밀키(K_R)로 암호화해 리더에게 전달하는 RES_Token 수행.
⑤ 태그에게 Token을 Fwd : 서버로부터 전달받은 Token을 해독한 후 리더가 새로 생성한 난수(RN_R)과 해독한 Token의 태그 전달 부분을 암호화해 전달.
⑥ 리더 인증을 요청하는 Chk_MAC 전달 : 태그가 리더의 인증을 요청하기 위해 새로운 난수(RN_T)를 생성하고 전송받은 리더의 새로운 난수(RN_R)와 함께 공유 비밀키(K_{RT})를 사용해 세션 비밀키(SK_{RT})를 생성한다. 그리고 생성한 세션 비밀키(SK_{RT})를 이용해 인증을 위한 메시지($AUTH_T$)를

생성하여 태그의 난수(RNT)와 함께 리더에게 Chk_MAC(R_T||$AUTH_T$)을 전달.

- SK_{RT} = Rand(RN_R, RN_T)
- $AUTH_T$ = CMAC(K_{RT}; T_ID||R_ID||RN_R||SK_{RT})

⑦ 리더 인증 확인 메시지 생성 : 태그로부터 전달받은 Chk_MAC(R_T||$AUTH_T$)를 검증하기 위해 리더도 세션 비밀키(SK_{RT})를 생성하고 이를 이용해 $AUTH_R$를 생성해 태그에게 전달.

- SK_{RT} = Rand(RN_T, RN_R)
- $AUTH_R$ = CMAC(K_{RT}; R_ID||T_ID||RN_T||SK_{RT})

위의 그림 3 과 같이 리더와 태그는 상대방이 생성해 전달한 $AUTH_R$과 $AUTH_T$를 자신이 직접 생성해 보고 동일성 여부를 비교해 인증성을 판별한다.

인증 여부에 따라 리더의 요청에 대한 태그에 대한 보다 자세한 정보의 제공 여부가 달라진다. 만약 인증되지 않은 리더라면 태그의 임시 식별자인 T_ID 이외에는 고급 정보를 제공 받을 수 없다. 하지만 인증된 리더라면 EPC_Code와 기타 고급 정보를 제공받게 될 것이다.

라. 암.복호화 단계

암.복호화 단계에서 수행할 작업은 태그와 리더 사이에 기초적인 정보인 임시 식별자를 제외한 고급 정보들을 전달하기 위해 암호화와 복호화하는 작업을 수행한다.

추가적으로 리더와 태그 사이에서의 통신 과정이 종료되면 리더는 서버에 요청하여 태그의 새로운 임시 식별자(New_T_ID)를 할당 받아 전달한다. 새로운 임시 식별자를 전달 받은 태그는 이를 저장하고 통신을 종료하게 된다.

① 리더가 태그에게 정보 요청 메시지 전달 : 리더가 태그에게 REQ_info(R_ID)를 전달함으로서 정보 전송을 요청.

② 리더의 요청에 태그가 응답 : 태그가 리더의 정보 전송 요청에 RES_info(T_ID||Opt_info)를 전송해 응답.

③ 정보 전송 종료 : 위의 2 개 절차를 리더와 태그가 원하는 동안 반복하다가 리더의 요청에 따라 정보 전송을 종료하고 새로운 태그 임시 식별자(New_T_ID)를 서버로부터 할당받아 전송하면 태그는 이를 저장하고 통신을 종료한다.

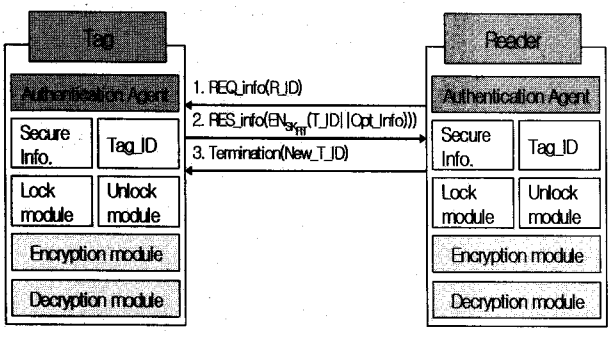

그림 4. 암.복호화 단계
Fig. 4. Phase 3: Encryption & Decryption.

서버와 리더, 태그의 구성 요소들로 구성된 RFID 시스템에서 3 단계로 나누어 사전 키 분배 단계, 인증 단계, 암.복호화 단계를 거쳐 리더와 태그 사이의 안전한 통신을 보장할 수 있도록 하였다.

이때 RFID 시스템의 하드웨어 자원의 제약 사항을 고려해 RC5와 같이 하드웨어적으로 구현하기 쉽고 그 적용 가능성이 높은 암호 알고리즘을 적용한다.

또한 리더와 태그 사이의 인증을 위해서 CBC_MAC을 사용하여 인증 서버를 가진 공개키 방식 보안 구조처럼 자원의 부담을 가지는 방식을 채택하지 않고서도 높은 효율성을 갖도록 하였다.

RC5는 알려진 바와 같이 빠른 연산 속도와 적은 하드웨어 자원 소모, 가변적인 적용 가능성을 가지고 있다. 제안한 시스템은 단순한 RC5 알고리즘의 3가지 처리 과정인 덧셈연산, XOR 연산, 순환 구조 Shift 연산을 사용해 암호화를 수행한다. 추가적으로 난수 발생기를 사용해 메시지와 객체에 대한 인증을 할 수 있도록 하였다.

태그와 리더 사이에서 전송되는 정보를 추적하여 태그를 소지하고 있는 사용자에 대한 정보나 태그의 위치 정보를 추적하는 프라이버시 문제를 해결하기 위해서 태그와 리더의 통신에 직접적인 태그의 정보인 EPC_Code를 사용하지 않고 태그에게 백-앤드 서버가 제공하는 임시 태그 식별자를 할당받아 사용함으로써 리더와 태그 사이의 새로운 통신 단위인 세션마다 새로운 임시 식별자를 사용하게 됨으로써 추적성을 회피할 수 있도록 하였다.

Ⅳ. 성능 평가

1. 실험환경

본 논문에서 제안한 시스템에 대해 전체적인 보안성

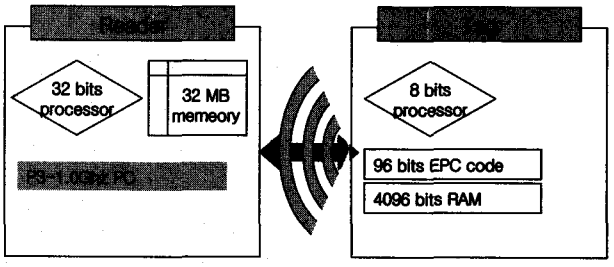

그림 5. 제안한 시스템의 실험환경
Fig. 5. Evaluate environment of safe RFID system.

을 증명하는 것은 매우 힘들다. 그러므로 본 논문에서는 RC5 암호 알고리즘과 난수 발생기를 적재 가능하고 8 bit 처리장치를 탑재한 환경에서의 성능에 대한 분석과 안전성 분석을 하고자 한다.

RC5와 같이 적용 가능성이 높고 처리 방식이 단순하며 적은 하드웨어 자원을 소비하는 암호 알고리즘이라 하더라도 RFID 시스템의 태그에 탑재하기에는 어려움이 많다. 현존하는 대표적인 low-cost RFID Tag는 대략 1달러 이하로 처리 장치를 가지고 있지 않고, 데이터의 저장 용량도 대체로 매우 적다. 이에 본 논문에서는 제안하는 semi-passive 태그로서 동작할 수 있는 실험 환경을 아래의 그림 5와 같이 제안한다.

위의 그림 5 에서 제안하는 바와 같이 안전한 RFID 시스템을 위해서 리더 역할을 하는 시스템은 일반적인 PC 환경이나 그 이상의 PDA와 같은 이동성이 있는 시스템을 가정한다.

리더가 가져야 하는 최소 처리 능력으로는 32 bit 처리장치와 32MB 이상의 메모리 영역을 가지고 있으면 충분하다. 제안하는 환경은 일반적인 PC나 Embedded system, 혹은 hand-held system으로 도 가능할 것으로 예상된다.

실험 환경을 설정하는데 있어서 주의해야 하는 부분은 태그의 환경이다. 태그 역할을 하는 시스템은 가격이 1 달러 이하로 저렴하고 제안하는 동작과정을 수행할 수 있어야 한다.

이러한 사항들을 만족하려면 먼저, 단순한 연산을 수행하기 위한 8 bit 처리 장치를 가지고 있어야 한다. 처리 장치를 가지고 있어야만 RC5 암호 알고리즘과 같이 덧셈, XOR, Shift 와 같은 연산을 처리할 수 있기 때문이다.

그리고, 기본 태그 식별정보인 EPC_Code와 고급 정보로 구성된 기초 정보들을 저장하기 위한 FLASH 메모리 영역과 연산을 수행하면서 임시적으로 사용되는 임시 식별자인 T_ID와 같은 정보들을 저장하기 위한 RAM 영역을 가지고 있어야 한다.

물론 일반적인 Passive 태그도 FLASH 메모리와 RAM 영역을 가지고 있다. 하지만 RFID 시스템에서 주로 사용되고 있는 1달러 미만의 Passive 태그들은 저장 용량이 FLASH 영역이 1 Kbits 이하, RAM 영역이 512 bits 이하로 구성되어 있다.

위와 같은 일반적인 Passive 태그 환경에서는 보안 서비스를 제공하기 위한 연산들에 필요한 정보나 처리 과정 중에 생성되는 정보들을 저장하기는 불가능하다. 그러므로 이를 확장한 환경은 최소 4 Kbits FLASH 메모리와 4 Kbits RAM 영역을 가질 것을 제안한다.

이러한 환경을 가진 RFID 태그를 구성하기는 현재로서는 매우 어렵다. 그러므로 본 논문에서는 실험을 위해 이와 유사한 환경으로 ATmel 사의 ATmega128 칩을 사용하여 실험을 진행한다.

제안한 ATmega128 칩은 8bit 처리장치를 가지고 있으며, 내부 64 Kbit FLASH 와 64 Kbit RAM을 가지고 있다. 그리고 외부로 128 Kbit까지 FLASH와 RAM을 확장할 수 있다.

그리고 이러한 칩은 SoC 구조로 칩 내부에 메모리와 처리장치를 모두 가지고 있어 처리속도가 빠르고 지연시간이 거의 없다. 제안한 실험 환경에서 사용될 칩의 현재 가격은 대략 1달러 이하로 RFID 시스템에서 제안한 태그의 가격과도 유사하다.

2. 실험 결과

가. 안전성 분석

제안한 안전한 RFID 시스템은 태그와 리더에서의 통신에서 발생할 것으로 예상되는 보안 취약성인 도청, 위조, 변조에 대한 문제를 해결하기 위해서 데이터를 암호화해 전달함으로써 문제를 해결하고자 한다.

먼저, 사전 키 분배 단계에서 리더와 태그는 각각 서버에 등록하는 과정을 통해 사전에 암호화에 사용할 비밀키(K_R, K_T)를 가지고 있다.

그리고 인증 단계에서 리더와 태그가 서로 인증을 하기 위해서 세션키와 인증 메시지를 생성하기 위해서도 믿을 수 있는 중재자 역할을 하는 서버가 반드시 필요하다. 그러므로 중간에 누군가가 악의적인 목적을 가지고 끼어들어 도청, 위조, 변조 등의 행위를 수행하려고 하여도 서버에서 각각의 리더와 태그에게 할당해 준 초기 비밀키와 세션키, 인증 메시지를 생성하기 위한 정보들을 알 수 없다면 이는 불가능하게 된다.

오랜 시간동안 Brute-force 공격을 통해 많은 데이터들을 수집해서 공격을 수행하고자 한다고 가정하더라도 리더와 태그 사이에서 사용하는 세션키나 임시 식별정보, 인증 메시지들은 난수를 사용해 생성되기 때문에 사전에 전달된 자료의 일부를 판독하게 된다 하더라도 그 효용성을 잃게 된다.

또한 사용자의 프라이버시를 침해하는 추적 문제에 대한 해결 방안으로 세션키와 함께 태그에 대한 임시 식별자를 서버에서 각각의 리더의 통신 요청마다 새로이 생성해서 사용하도록 한다.

그러므로 또 다른 리더가 태그와 통신을 시도하면 항상 새로운 임시 식별자와 세션키를 할당 받아 사용하고 보다 자세한 고급 정보들은 인증된 리더에 대해서만 전달하고 있다. 추가적으로 인증된 리더라 하더라도 항상 전달하는 정보들에 대해서는 서버와 태그 사이에서만 사용하도록 할당된 비밀키를 사용해 암호화해 전달함으로써 중간의 리더는 그 정보의 의미를 유추해 내는 것이 어렵다.

이와 같이 Leighton이 제안한 키 분배 프로토콜과 Rivest 에 의해 제안된 RC5 암호화 알고리즘들은 이미 그 안전성이 입증되었으며 이를 시스템에 적용함으로써 안전성에 대한 문제는 보장받을 수 있을 것이다.

하지만 제안한 시스템에서도 사전 키 분배와 인증을 위해 사용되는 서버의 Key Pool이나 Management Table 에 대한 공격을 통한 정보 획득과 같은 근본적인 문제에 대해서는 미흡한 점을 가진다.

나. 성능 분석

제안한 시스템의 성능 분석을 위해서 ATmega128 칩을 사용하고 WinAVR의 Programmers Notepad V2.0.5048을 이용해 ANSI-C 표준에 따라 8bit 처리 장치에 적용 가능하도록 소스 프로그램을 작성하였다.

컴파일러는 ANSI-C 컴파일러를 사용하며 디버거로는 AVRStudio V4.0.11을 사용한다. 시뮬레이터로는 8 bit 온 칩이 가능한 제품을 사용한다.

먼저 태그에서의 성능 분석을 위해 위에 제안된 환경에서 소스 프로그램을 작성하고 컴파일 작업을 수행한다. 다음으로 디버거에서 프로그램의 문법적인 오류들에 대해 점검 작업을 수행한 후 시뮬레이터에 하드웨어적으로 구현한다.

성능 분석을 위해 2가지 측면으로 나누어 실험을 진행하였다. 먼저 암호화와 복호화에 사용되는 RC5 암호 알고리즘은 가변적인 하드웨어 환경에 구현하기가 용이하다는 특징을 감안하여 시뮬레이터에 구현하였다. 비교 대상으로 AES와 같은 표준 대칭키 암호 알고리즘을 구현하여 처리 시간을 비교하고자 하였으나 하드웨어적으로 태그의 환경에 알맞게 변경하기가 어려웠다. 그러므로 태그에서의 수행시간은 RC5 알고리즘에 대한 처리 암호화와 복호화 시간만을 측정할 수 있었다.

표 3. 암호 알고리즘 처리시간(태그 환경)
Table 3. Performance of cryptography algorithm.

	처리 시간 (msec)	Round key 생성시간(msec)	Random 생성시간(msec)
RC5	1.22 / 0.90	1.40 / 1.10	0.90 / 0.48
CBC_MAC	0.80 / 0.57	0.92 / 0.64	0.74 / 0.50
H_MAC	X / 1.02	X / 1.06	X / 1.00
AES	X / 1.14	X / 1.20	X / 1.10

또한 태그에서 인증을 위해 필요한 MAC 처리 시간을 측정하고자 CBC_MAC에 대한 처리 시간을 측정하였다. 비교 대상으로 H_MAC에 대한 처리 시간을 측정하고자 하였으나 H_MAC은 하드웨어적인 제약사항으로 인해 태그환경에서는 동작할 수 없었다. 이에 태그 환경에서 동작 가능한 RC5 알고리즘을 암.복호화 처리 시간과 CBC_MAC에 대한 처리시간을 측정한 결과를 나타낸다.

추가로 위의 제안한 비교 대상과 태그 환경에서 구현한 각각의 알고리즘들에 대해 리더 환경에서 구현하여 처리 시간을 측정한 결과를 나타내었다.

리더 환경은 일반적인 저-사양의 데스크 탑과 유사하여 구현에 하드웨어적인 제약사항은 없다.

위의 표 3 과 같이 태그 환경에서 암호 알고리즘과 인증을 수행하는데 소요되는 처리 시간을 나타내었다.

실험에 적용된 환경변수는 태그의 처리장치가 8 bit 이고 그 저장 용량이 4 Kbits 이므로 RC5 알고리즘을 적용하기 위해 128 bits로 구성된 데이터 블록을 4개로 나누어 각각 32bit로 구성하였다. 작은 규모로 나눈 작은 블록을 다시 8 bit 단위로 처리할 수 있도록 하기 위함이다. 또한, RC5 알고리즘이 보안성을 보장 받기 위해 16 라운드 이상을 동작할 것을 권장하고 있다. 그러므로 bit 단위로 나뉜 16개의 작은 데이터 블록에 대응하는 8 bit 단위의 16개 비밀키 블록을 사용해 XOR 연산과 덧셈 연산, Shift 연산을 수행하도록 한다.

실험의 결과를 살펴보면 구분기호 '/' 의 좌측은 태그 환경에서의 처리시간을 msec 단위로 나타낸 것이고 구분기호 우측은 리더 환경에서의 처리시간을 각각 나타내고 있다.

H_MAC과 AES와 같이 낮은 사양의 환경에서는 동작하기 어려운 알고리즘들은 태그 환경에서는 그 처리 시간을 측정할 수 없었다. 하드웨어적인 제약 사항으로 인해 구현이 어렵기 때문이다.

제안한 시스템을 리더 환경에서 동작한 경우의 처리 성능을 살펴보면 인증을 수행하기 위해 H_MAC을 생성하는 것이 CBC_MAC을 생성하는 것과 비교하여 대략 2배 정도의 시간이 소요되는 것을 알 수 있다.

또한, RC5 암호 알고리즘에 비해 AES 알고리즘을 사용하는 것이 암호화와 라운드 키를 생성하는 경우에는 커다란 차이가 보이지 않지만 랜덤값을 구하는 경우에 대해서 큰 차이를 보이고 있다. 이는 AES 알고리즘이 RC5에 비해 내부적인 수행 연산이 복잡하고 처리 절차가 많기 때문으로 생각된다.

V. 결 론

유비쿼터스 환경에서는 다양한 사물의 인식을 위해 비-접촉방식과 대량 인식이 가능한 모바일 특성을 지닌 RFID 태그가 적용되어질 것이다.

하지만 RFID 태그가 모바일 매체로서 자주 이동하게 되고 하드웨어적인 자원을 매우 적게 가지고 있음을 고려한 프라이버시 보호 방안이 존재하지 못한 실정이다.

이에 본 논문에서는 센서 네트워크 환경에서 모바일 매체들에 대한 인증이나 보안 서비스를 제공하기 위해 제안한 Pre-Distribution을 기반으로 한 키 분배 방식을 적용해 RFID 시스템에 대한 프라이버시 보호 가능성을 제안하고 이에 대해 시뮬레이션을 통해 적용 가능성을 가늠해 보았다.

참 고 문 헌

[1] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Security and Pervasive Computing 2003, LNCS 2802, pp.201-212.

[2] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed Sensor Networks", ACM CCS'02, Nov. 2002, pp.41-47.

[3] H. Chan, A. Perrig and D. Song, "Random Key Pre-distribution Schemes For Sensor Network", IEEE Symposium on Security and Privcy, 2003.

[4] Tom Leighton and Silvio Micali, "Securet-Key Agreement without Public_Key Cryptography", Advaces in Cryptology CRYPTO 1993, 1994.

[5] Duncan S. Wong and Agnes H. Chan., "Efficient and mutually authenticated key exchange for low power computing devices", In Advances in Cryptology ASIACRYPT'2001.

저 자 소 개

김 진 묵(정회원)
1998년 배재대학교 컴퓨터과학과 이학사 졸업.
2000년 배재대학교 컴퓨터공학과 공학석사 졸업.
2000년~현재 광운대학교 컴퓨터과학과 박사과정.
<주관심분야 : 네트워크 보안, 유비쿼터스, RFID>

유 황 빈(정회원)
1975년 인하대학교 전자공학과 공학사 졸업.
1977년 연세대학교 대학원 공학석사 졸업.
1989년 경희대학교 대학원 공학박사 졸업.
1981년~현재 광운대학교 컴퓨터소프트웨어 교수
<주관심분야 : 멀티미디어 통신 및 응용, 네트워크 보안, RFID>