태그 기반의 센서 네트워크 관리에 관한 연구

서대희⁰, 이임영
*순천향 대학교 정보기술공학부
e-mail : patima@sch.ac.kr

A Sensor Network Management based on Tag

Dae-Hee Seo⁰ Im-Yeong Lee
Soonchunhyang Univ. Division of Information Technology Eng.

요약

휴대 단말기 보유율의 급격한 증가는 새롭고 다양한 형태의 무선 통신 기술의 개발을 촉진시키는 계기가 되었으며, 특히 국내의 경우 이동통신 시장의 경제적이나 양적으로 급속한 성장을 이루어 사회 전반에 걸쳐서 새로운 가치를 생산해 내어 생활 모습을 크게 바꾸어 놓고 있다. 따라서 이러한 환경의 변화는 사용자 중심의 다양한 서비스를 제공할 수 있는 차세대 무선 통신 기술의 연구가 필요한 실정이다.

따라서 본 논문에서는 RF 태그 기반의 네트워크 형성과 더불어 유비컴퓨팅 환경에서 요구되는 서비스 생성에 따른 인증 및 동일한 서비스에 대한 관리 방식을 제안하고자 한다. 제안된 방식의 경우 RF 태그를 기반으로 이루어지는 네트워크에서 태그가 생성하는 서비스에 따라 인증 레벨을 설정하고 동일한 서비스와 인증 레벨을 갖는 서비스가 발생할 경우 이를 관리할 수 있는 그룹 아이디와 키를 생성해 관리하는 방식을 제안하고자 한다.

1. 서 론

인터넷 및 이동전화로 대표되는 정보통신 기술의 발전은 생활 패턴 자체를 변화 시켜 가정, 학교 사무실을 비롯한 모든 환경에서 정보를 습득 및 서비스를 제공받는 환경으로의 변화를 가져왔다. 특히 정보통신의 기술은 새로운 서비스 제공을 위해 지속적인 연구와 발전을 지속하고 있으며, 이러한 발전의 특징은 다양한 무선 통신 기술의 개발과 의존성에 있다.

최근 주목받고 있는 무선 기술중 차세대 무선 통신기술로써 인정받고 있으면서, 유비쿼터스 컴퓨팅과 같은 사용자 중심의 차세대 네트워크 구조에 적용 가능한 기술로 RFID에 대한 연구가 주목을 받고 있다.

따라서 본 논문에서 태그 기반의 센서 네트워크 구성 및 서비스 생성의 효율성과 안전성을 제공하기 위한 방식을 제안하고자 한다.

본 논문의 2장에서는 최근 많은 연구가 진행중에 있는 RFID기술의 개요에 대해 살펴본 뒤 3장에서는 태그 기반으로 센서 네트워크가 구성되었을 경우 요구되는 보안적인 서비스에 대해서 논하고자 한다. 4장에서는 안전성과 효율성을 갖는 태그 기반의 센서 네트워크 구성 및 서비스 생성 방안을 제안하고 5장에서는 3장에서 제시된 보안 요구사항을 기반으로 제안 방식을 분석한 후 6장에서는 결론을 맺고자 한다.

2. 관련 연구

RFID는 판독 및 해독 기능을 하는 RF 판독기와 정보를 제공하는 RF 태그로 구성된 무선통신 시스템이다. RFID는 사람, 자동차, 화물등에 개체를 식별하는 정보를 부가하는 시스템으로 그 부가 정보를 무선 통신 매체를 이용하여 비접촉으로 해독함으로써 기존에 오프라인으로 이루어지는 다양한 어플리케이션을 자동화할 수 있으며 그 특징은 다음과 같다.

- 편리한 사용과 여러 태그를 동시에 인식이 가능
- 고속 인식이 가능하여 시간적인 효율성이 가능
- 시스템 특성이나 환경 여건에 따라 손쉬운 적용
- 비접촉식의 특성에 따른 반영구적 사용과 유지보수에 대한 경제성이 우수
- OTP(One Time Programming)로 태그를 프로그램하여 데이터 위조 및 변조에 대한 보안성 제공
- 시스템 확장이 용이
- 양방향 인식이 가능

RFID에서는 'The Internet of Things'란 개념이 활용된 시스템이다. 'The Internet of Things'란 MIT Auto-ID 센터에서 제시된 개념이다. 이는 인터넷과 인터넷 비슷한 네트워크를 통하여 무선 태그가 부착된 아이템을 원거리에서 실시간으로 감지하는 서비스 개념이다. 따라서 The Internet of Things는 인터넷의 새로운 사용을 가능할 것을 예측할 수 있다.

따라서 연간 수십억개 이상의 보다 효율적인 RFID 태그 및 무선 네트워크가 필요할 것이며 새로운 소프트웨어와 많은 아이템을 다룰 수 있는 바코드 혹은 이와 비슷한 시스템이 요구될 수 있어 보다 다양한 형태의 어플리케이션을 지원할 수 있다.

3. 보안적 요구사항 및 분석

RFID를 기반으로하여 센서 네트워크를 구성할 경우 일반적인 무선 시스템에서의 보안 취약성 뿐만 아니라 RF 시스템만이 갖는 보안 취약성은 다음과 같이 정리할 수 있다.

3.1 일반적인 무선 시스템의 일반적인 보안 취약성

보안 서비스인 ACIN(Authentication Confidentiality Integrity Non-repudiation)과 관련한 공격방법은 다음과 같이 요약할 수

있다.
- 인증 : 통신과정에서 반드시 요구되는 보안 서비스가 인증이다. 그러나 일반적인 무선 통신상에서는 PIN(Personal Identification Number)에 근거한 묵시적 사용자 인증과정을 수행한다. 이는 사용자의 인증 보다는 단말기 인증을 의미하며, 묵시적으로 사용자의 모바일 디바이스를 PTD(Personal Trust Device)라는 가정하에 이루어진다. 따라서 사용자의 모바일 디바이스가 PTD가 아닐찌라도 단말기 인증과 더불어 사용자 인증을 위한 보안 서비스가 요구된다.
- 기밀성 : 무선 통신을 이용하는 단말기의 특성상 암호 통신을 위한 키의 길이가 매우 짧거나, PIN의 불법 누출에 따른 취약성과 더불어 저장된 데이터에 대한 기밀 저장 서비스가 제공되지 않는다.
- 무결성 : 무결성과 관련해서는 일반적으로 CRC(Cyclic Redundancy Check) 체크를 기반으로 이루어진다. 그러나 WLAN(Wireless Local Area Network)에서와 같이 CRC를 통해 전송 데이터에 대한 무결성 서비스를 제공하지 못할 뿐 아니라 모바일 단말기의 불법적 데이터 수정에 대한 보안 서비스를 제공해주지 못하고 있다.
- 부인봉쇄 : 단말기 인증만을 수행하는 형태의 인증이 수행된다면, 불법적인 데이터 송신 및 수신에 대한 부인봉쇄 서비스를 제공해 줄 수 없으며, 이는 모바일 전자상거래와 같은 금융권에 반드시 요구되는 보안 서비스이다.

3.2 RF 시스템에서의 보안 취약성 분석
RF 시스템에서는 ACIN과는 별도의 보안 사항이 요구된다. 그러나 다음과 같은 보안 요구사항에 대해 RF 시스템은 취약성을 내포하고 있다.
- 채널 보안 : RFID에서는 리더기를 기준으로 전방향(태그-to-reader) 채널과 후방향(reader-to-태그) 채널에 대한 보안이 요구된다. 그러나 현재의 RFID에서는 전방향/후방향 채널에 대한 보안 서비스를 제공하지 못해 사용자 프라이버시에 보호에 대한 취약성을 내포하고 있다.
- 물리적 공격 : RF 태그에 대한 기판 파괴 공격, 에너지 공격과 같은 물리적인 공격에 안전성을 제공할 수 있는 보안 서비스가 요구된다.
- 프로토콜 보안 : 태그와 리더기 사이에서 이루어지는 쿼리의 수정 공격으로 인한 전송 데이터 보안이 이루어지지 않고 있다. 따라서 이를 보완할 수 있는 서비스가 요구된다.
- 도청 : RF 통신과정에서 제한적인 도청이나 로지컬한 메시지에 대한 도청이 수행될 경우 전송 데이터에 대한 무결성에 대한 보안 서비스가 필수적으로 요구되나, 현재 서비스에서는 이를 위한 보안 서비스가 제공되지 않고 있다.
- 서비스 거부 공격 : 메시지에 대한 존재만 확인이 가능한 공격자가 1:n 통신을 위한 브로드캐스트 메시지의 차단이나 서비스 거부 공격을 통해 전송 데이터에 대한 고의적인 정보 차단이 가능하다.

4. 태그 기반의 센서 네트워크 구성 및 서비스 생성에 관한 연구

제안방식은 태그 기반의 센서 네트워크 구성 및 서비스 생성의 효율성과 안전성을 제공하고자 한다.

4.1 시스템 계수
다음은 태그 기반의 센서 네트워크 구성 및 서비스 생성에 관한 시스템 계수를 기술하고자 한다.
* (데이터베이스 서버 : D, RF 리더기 : R, RF 태그 : T)
*ID : 각 구성 객체의 ID
r : 랜덤 수
H : 안전한 해쉬 함수
a : 랜덤 인덱스 ($a \in \{0, 1\}^k$)
Cnt : 카운트 정보
x : 태그의 초기 정보
$F()$: 의사 랜덤 함수
M : 서비스 메시지
T : 타임 스탬프
AL(Authenticition Level) : 인증 레벨

4.2 제안방식 프로토콜
태그 기반의 센서 네트워크 구성 및 서비스 생성은 다음과 같은 가정사항을 기반으로 수행된다.

가) 가정사항
① 모든 RF 태그는 Active 태그로써 사전에 데이터베이스 서버에 MID를 등록한다.
② RF 리더기와 데이터베이스 서버와는 유선으로 연결되어 있으며, 신뢰된 객체이다.
③ RF 태그는 MID에 대응되는 RID를 RF 리더기에 사전 등록한다.

나) 초기화 프로토콜
① RF 리더기는 RF 태그에 통신 Query를 전송한다.
② RF 태그는 MID와 x를 RF 리더기에 전송한다.

$$MID,\ x$$

③ RF 리더기는 RF 태그로부터 전송된 MID, x를 임시 저장하고, RF 태그로부터 사전 등록된 RID와 랜덤 수 r을 생성하여 다음과 같은 안전한 해쉬값 R_h를 계산한 후 R_h, RID, r을 데이터베이스 서버에 전송한다.

$$R_h = H(RID \| r)$$

④ 데이터베이스 서버는 RF 리더기로부터 전송된 R_h, RID, r을 기반으로 다음과 같은 검증 과정을 수행한다.
- RF 리더기로부터 전송되어온 RID, r을 기반으로 R_h'를 생성하여 전송되어온 R_h와 비교하여 전송 데이터에 대한 무결성을 검증
RF 리더기에 전송된 RID에 대응되는 MID와 랜덤 수 r_D를 기반으로 Key를 생성한다.

$$Key = H(MID \| r_D)$$

데이터베이스 서버는 Key와 RFID를 RF 리더기에 전송한다.

$$(Key,\ \text{RFID})$$

⑤ RF 리더기는 데이터 베이스 서버로부터 전송된 (Key, RFID)를 임시 저장하고 α를 계산 한 뒤 이를 태그에 전송한다.

$$\alpha = (RFID, F_a(Key \| Cnt) \oplus h(x))$$

⑥ 태그는 α를 수신한 뒤 이벤트 종결 메시지를 전송함으로써 초기화 프로토콜을 종료한다.

다) 서비스 생성에 따른 인증 레벨 프로토콜
서비스 생성에 따른 인증 레벨 프로토콜은 초기화 프로토콜을 진행한 뒤 태그 정보에 대한 인증 레벨을 설정하는 과정이다.
① 태그는 가)의 α정보에서 RFID를 추출하여 서비스 생성 메시지 M과 함께 RF 리더기에 전송한다.

$$M,\ \text{RFID}$$

② RF 리더기는 가)의 ⑤에서 생성된 α와 RFID, x, Cnt를 데이터 베이스 서버에 전송한다.

$$\text{RFID},\ \alpha,\ x,\ Cnt$$

③ RFID, α, x, Cnt를 전송받은 데이터 베이스 서버는 전송 정보에 대한 검증과정을 수행한 뒤 올바른 정보일 경우 RFID에 해당되는 태그의 인증 레벨 정보를 다음과 같이 생성한다.
- 검증 과정 : $\alpha' = (RFID, F_a(Key \| Cnt) \oplus h(x))$, $\alpha' = \alpha$ 인지 검증
- 인증 레벨 정보 AL(Authentication Level) 생성 : 데이터 베이스 서버는 랜덤 수 r을 생성한 후 A를 생성한다.

생성된 A로부터 인증 레벨 정보 AL을 계산 한 뒤 T_D와 함께 RF 리더기에 이를 전송한다.

$$A_{1or\ 2or\ 3} = (MID_* \oplus r \mid x_*)$$
$$AL_{1or\ 2or\ 3} = H(A_{1or\ 2or\ 3})$$

- AL_1 : 초기화 과정이 수행된 RF 태그에 대해서만 자동 접근이 허용된다. 비신뢰 태그의 경우 초기화 과정이 요구된다.
- AL_2 : 초기화 과정이 수행된 RF 태그라 할찌라도 초기화 과정이 재수행된다.
- AL_3 : 모든 장비에 대해 개방적이다. 인증이 필요하지 않으며, 개체에 대한 접근이 자동적으로 허용된다.

④ RF 리더기는 서비스 생성 메시지 M에 대한 응답 메시지 M_{res}를 생성하고 태그에 대한 인증 레벨 정보 AL_*과 Key_1을 태그에 전송한다.

$$Key_1 = F_a(Key)$$
$$M_{res},\ AL_{1or\ 2or\ 3}$$

라) 동일한 서비스에 대한 관리

동일한 서비스와 AL_*을 갖는 태그의 서비스 요청이 있을 경우 다음과 같은 수행과정을 거쳐 동일한 서비스에 대한 관리를 데이터 베이스 서버를 수행한다.

① 태그는 서비스를 요청하는 Service Request와 $RFID$, Key_1을 RF 리더기에 전송한다.

② RF 태그로부터 전송된 Service Request, $RFID$, Key_*에서 동일한 Service Request를 요구하는 태그가 일정 개수 이상일 경우 해당되는 태그들의 AL_*, $RFID$, Cnt를 데이터 베이스 서버에 전송한다.

$$AL_*,\ (RFID_1, \ldots, RFID_n),\ (Cnt_1, Cnt_2, \ldots, Cnt_n)$$

③ 동일한 태그들의 서비스 요청에 따른 AL_*, $RFID$, Cnt를 전송받은 데이터 베이스 서버는 임시그룹서비스 TGS, 임시 그룹 ID, 임시 그룹키 G_{key}를 생성한다.

$$TGS = H((Key_1 \oplus Cnt_1) \mid\mid, \ldots, \mid\mid (Key_n \oplus Cnt_n))$$
$$GID = (MID_1 \mid\mid MID_2 \mid\mid, \ldots, \mid\mid MID_n)$$
$$G_{key} = H(r_{D_1} \oplus r_{D_2} \oplus, \ldots, r_{D_n})$$

생성된 그룹 정보에서 GID, G_{key}를 RF 리더기에 전송한다.

④ RF 리더기는 데이터 베이스 서버로부터 전송된 GID, G_{key}를 임시 저장하고, GID에 해당되는 태그에 G_{key}를 전송함으로써 임시 그룹키를 할당한다.

5. 제안 방식 고찰

본 논문에서 제안된 태그 기반의 센서 네트워크 구성 및 서비스 생성 방식은 3장에서 제시된 보안 요구사항을 기반으로 다음과 같은 특징을 가지고 있다.

- 채널 보안 : 제안된 방식은 전방향과 후방향 채널에 대한 보안 사항을 α=$(RFID, F_a(Key \mid Cnt) \oplus h(x))$를 검증한 뒤 인증 레벨 AL_*을 기반으로한 안전한 해쉬 함수를 이용한 채널 보안을 제공한다.
- 물리적 공격 : 물리적 공격의 경우 본 논문에서서 제안된 방식은 안전성을 제공하지 못한다.
- 프로토콜 보안 : 태그와 리더기 사이에 전송되는 정보 수정 공격에 대해 랜덤 수 r과 안전한 해쉬값 R_h와 랜덤 함수 F_a를 이용해 태그와 리더기 사이에 전송되는 정보에 대한 정보 수정 공격을 보완해 안전성을 유지하고자 하였다.
- 도청 : 제안방식의 경우 기존의 도청 공격에 취약하다 할 수 있다. 그러나 RF 시스템의 특징적인 형태를 볼때 높은 상태의 보안 서비스보다 경제성과 효율성을 갖춘 보안 서비스를 제공하고자 하였다.
- 서비스 거부 공격 : 제안 방식의 경우 기존의 서비스 공격에 대해 안전성을 제공할 수 없다.
- ACIN : 기밀성 측면에서는 지속적으로 Cnt정보에 대한 변화를 통해 인증 권한을 설정함으로써 불법 사용되는 Key에 대한 안전성을 유지하고자 하였으나, 부인봉쇄 측면에서는 여전히 문제성을 지니고 있다.

6. 결론

유비컴퓨팅 환경과 같은 사용자 중심의 네트워크 형성을 위해서는 근거리 무선 통신 기술이 반드시 요구되고 이와 더불어 사용자의 프라이버시를 보호할 수 있는 보안 기술이 반드시 요구되는 시점에서 RF 시스템을 이용한 센서 네트워크 형성과 관리 방안에 대한 연구를 제안하였다.

기존 네트워크 관리 방식과 비교해볼때 많은 보안적 취약성을 가질 수 있으나, RF 시스템의 특성상 경제성을 고려하면서 사용자의 프라이버시를 보완할 수 있는 방식은 매우 한정적이고 제약될 수 밖에 없다.

따라서 본 논문에서 제안된 방식이 모든 조건을 만족하는 안전성을 제공할 수 없다. 그러나 현재 연구중이면서 개발중인 RF 시스템에서 고려되어야 하는 보안 사항을 어떻게 적용하고 활용할 것인지에 대한 방안과 더불어 불법 공격자로부터 최소한의 안전성을 유지할 수 있는 방법을 제시하고자 한다.

본 논문에서 제시된 방식은 한정적인 형태의 적용을 위해 제안되었으며, 향후 제안된 방식을 보다 다양한 형태로 적용 시켜 프로토콜의 안전성을 향상 시킬 수 있는 새로운 형태의 관리 방식에 대한 연구가 지속적으로 필요할 것으로 사료된다.

참고문헌

[1]http://www-903.ibm.com/kr/solutions/wireless/eb2sm/rfid.html
[2]http://kdaq.empas.com/dbdic/db_view.jsp?ps=src&num=3752184
[3]http://kdaq.empas.com/dbdic/db_view.jsp?ps=src&num=3752185
[4]http://blog.empas.com/harnie/print.php?a=666858
[5]http://www.smart1.co.kr/biz/biz_product_rfid_1.htm
[6]http://www.rapa.or.kr/korean/data/2002/6/2002_6_06.htm
[7] http://www.irda.org
[8] http://www.tta.or.kr
[9] http://www.irda.co.kr
[10] http://www.kepf.org
[11]http://eagle.kisa.or.kr/edu/edu2002/edu_20020819/edu_20020823_013.pdf