RFID 기반의 안전한 네트워크 관리 방식에 관한 연구

서대희*, 이임영*, 남기효**, 강창구**
순천향대학교 정보기술공학부*
프롬투정보통신(주)**

A Study on Secure Network Management Scheme based on RFID

Dae-Hee Seo*, Im-Yeong Lee*, Ki-Hyo Nam**, Chang-Goo Kang**
Division of Information Technology Engineering. SoonChunHyang University*
From2 Information & Communication Co. Ltd**

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 필수적으로 요구된다.

본 논문에서는 RF Tag 기반의 안전한 네트워크 방식을 제안하고자 한다. 제안된 방식은 안전한 네트워크를 형성한 뒤 불법적 Tag에 대한 보안 서비스와 다양한 서비스를 제공한다.

1. 서 론[1)]

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 네트워크에 활용 가능한 기술이 RFID이다. RFID는 무선 통신을 이용해 원격으로 감지 및 정보를 인식하여 정보의 교환을 가능케 하는 기술로써 기존의 오프라인에서 대표적으로 활용되고 있는 바코드 체계를 대체할 수 있어 개인생활은 물론 산업 전반에 많은 응용 서비스가 가능하여 최근 많은 연구 개발이 이루어지고 있다[2][5].

2. RFID의 개요와 보안 요구사항 분석

다음은 기존의 RFID의 개요와 보안 요구사항에 대해 분석하고자 한다.

2.1 RFID의 개요

RFID의 국제 표준화 작업은 현재 5개 주파수대역을 중심으로 총 14종의 표준안이 논의되고 있어 2003년 후반부터 국제표준으로 제정될 전망이다. RFID 시스템의 표준화 프레임워크는 각 SG 및 ARP 그룹의 표준화 영역으로 구분된다. 이중 가장 중요한 부분이 리더기와 태그간의 통신을 위한 Air Interface 분야로서 6종의 표준안이 현재 논의중에 있다. JTC1/SC31의 WG4에서는 현재 진행중인 총 12개의 표준안에 관련하여 2003년에 5종, 2004년 5종, 2005년 2종을 제정하는 것을 목표로 하고 있다[4].

2.2 RFID의 보안 요구사항 분석

경제성과 효율성을 고루갖춘 시스템인 RFID 시스템의 경우 다양한 환경의 적용성을 갖고 있다. 그러나 실제 ACIN (Authentication, Confidentiality, Integrity, Non-repudiation)과 관련된 공격 방법 뿐만 아니라 다양한 취약성이 Tag 기반의 RFID 시스템에서 실제적으로 발생할 수 있으며, 이는 다음과 같다[3].

- 채널 보안 : RFID에서는 리더기를 기준으로 전방향(태그-to-리더기) 채널과 후방향 (리더기-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.

1) 본 과제(결과물)는 산업자원부와 한국산업기술재단에서 시행한 지역혁신인력양성사업(지역전략산업 석박사 연구인력 양성사업)의 연구결과 입니다.

- 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 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.

2.3 Tag 기반 네트워크의 보안 요구사항

RFID 시스템과는 별도로 하여 RF Tag기반으로 네트워크를 형성하였을 경우 다음과 같은 추가적인 보안 요구사항을 제시할 수 있다[2].

- 불법 Tag에 대한 보안 서비스 : Tag 기반 네트워크 형성시 불법 Tag가 접근 시도를 수행할 경우 이를 차단할 수 있는 보안 서비스가 요구된다.
- 그룹 서비스 : 다양한 Tag들이 이동되면서 임시적인 그룹으로 설정하고 이에 해당되는 서비스를 제공함으로써 리더기의 효율성을 높일 수 있는 서비스가 요구된다.

3. 기존 관련 연구 분석

Tag기반의 RFID와 관련된 연구는 최근 유비쿼터스 컴퓨팅과 관련하여 많은 주목을 받고 있으며, 이와 관련된 기존 연구로 대표적인 방식이 MIT Auto-ID 센터 방식이다.

MIT Auto-ID 센터에서는 RF Tag와 관련한 다양한 보안 연구를 수행중에 있다. 이와 관련해 Stephen A. Weis(외3명)이 저가격의 RFID의 보안에 관련한 연구를 수행하였다. 본 방식의 경우 저가격의 RFID에서 요구되는 최소한의 보안 서비스를 위해 해쉬 함수를 이용한 방식을 제안하였다. 그러나 제안된 방식으로 Tag 기반의 네트워크를 형성하였을 경우 다음과 같은 문제점을 지적할 수 있다[2][4][5].

- 채널 보안 : 제안된 방식의 경우 전방향성 채널의 보안을 중심으로 설계되어 후방향성 채널에 대한 보안이 요구된다. 이는 초기 쿼리에 대한 수정 공격이나 전송 데이터와의 무결성 뿐만 아니라 기밀성을 위한 서비스가 추가적으로 연관된다.
- 프로토콜 보안 : 본 방식의 경우 프로토콜의 보안을 위해 해쉬 함수만을 이용함으로써 프로토콜상에서 발생할 수 있는 서비스 거부 공격이나 프로토콜 수정 공격에 취약하다.
- 불법 Tag에 대한 취약성 : 본 방식의 네트워크를 형성하였을 경우 불법 Tag에 대한 접근이 허용되어 Tag 기반의 네트워크에 취약성을 내포할 수 있다. 따라서 이를 보완할 수 있는 보안 서비스가 필수적으료 요구된다.
- 그룹 서비스 : 본 방식은 단일한 Tag에 대한 서비스만을 고려함으로써 Tag 개수가 증가함에 따라 리더기의 효율성이 저하되어 Tag 기반의 네트워크 구성시 전체 네트워크 효율성을 저하 시킬 수 있는 요인이 된다.

4. Tag기반의 안전한 네트워크 구성 제안

본 논문에서는 RF Tag 기반의 안전한 네트워크 관리 방식을 제안하고자 한다. 제안된 방식의 경우 초기 등록 과정을 수행한 뒤 RF Tag의 현재 위치 및 서비스 등록 과정을 수행한다. 또한 불법적인 RF Tag에 대한 보안 서비스와 단일 서비스와 그룹 서비스를 위한 안전한 프로토콜을 제안한다.

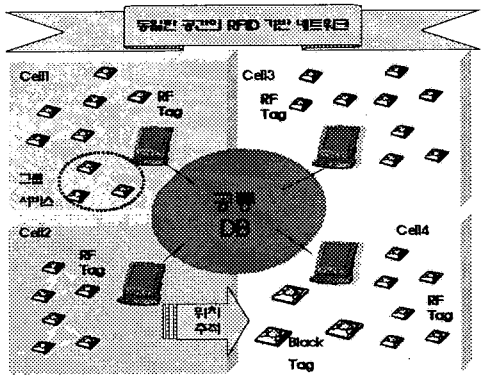
4.1 시스템 계수

Tag 기반의 안전한 네트워크 관리 방식 제안을 위한 시스템 계수는 다음과 같다.

* (r :리더기, t : RF Tag)
Metal ID : RF Tag의 물리적 주소
RFID, RID : RF Tag와 리더기의 ID
R, r : 의사난수
MKey : 초기 마스터 키
H : 안전한 해쉬 함수
Trace : RF Tag의 이동 경로 정보
M* : 각 개체의 서비스 메시지
T : 타임스탬프
E : 암호화 알고리즘
L_* : RF Tag의 위치정보(초기 등록된 RID, 타임스탬프)

4.2 Tag 기반의 안전한 네트워크 관리 방식 시나리오

제안 방식의 적용은 다음 (그림 1)과 같이 고려될 수 있다.



(그림 1) 제안방식 시나리오

4.3 세부 프로토콜

다음은 각 단계별 세부 프로토콜 과정을 기술한다.

[단계 1] 초기 등록 및 키 분배 단계

초기 등록 및 키 분배 단계는 RF Tag를 RF 리더기에 초기 등록 과정을 수행하고 각각의 Tag에 키를 분배하는 과정이다.

① RF Tag는 접속을 위한 초기 Query를 RF 리더기에 전송한다.

Query

② 초기 접속 Query를 전송한 RF Tag는 Metal ID를 RF 리더기에 전송한다.

Metal ID

③ RF Tag로부터 Metal ID를 수신한 RF 리더기는 다음을 계산한 뒤 RFID와 초기 Mkey를 RF Tag에 전송한 후 Metal ID와 RFID를 대응시켜 테이블로 저장한다.

$RFID = H(Metal\ ID \| r_R)$, Mkey

이상의 과정을 통해 RF Tag는 RF 리더기에 초기 등록과 키 분배 과정이 이루어진다.

[단계 2] 위치 및 서비스 등록 단계

RF 리더기는 현재 RF Tag의 위치를 확인하기 위하여 RF 리더기는 위치 정보를 생성하고 이에 대한 서비스를 등록하는 단계이다.

① RF 리더기는 RF Tag에 대한 현재 위치에 대한 요청 메시지를 전송한다.

Get_Challenge

② RF Tag는 RF 리더기로부터 전송된 Get_Challenge 메시지를 수신한 후 임의의 난수 R_t를 생성하고 다음을 계산하여 RF 리더기에 L_t, M_t, h_t를 전송한다.

$h_t = H(RFID \| R_t)$, R_t, L_t

③ L_t, h_t와 R_t를 수신한 RF 리더기는 Trace 정보와 Metal ID를 이용해 X_m을 계산한 후 X_m을 기반으로 Z_m을 계산하여 임의의 난수 R_r과 함께 RF Tag에 X_m, Z_m을 전송한다. 전송 후 RFID와 L_t에 대한 정보를 대응 테이블로 저장한다.

Trace = H(L_t)

$X_m = (Trace \| MetalID)$

$Z_m = H(RFID, L_t, X_m)$

④ RF Tag는 새로운 Key인 NKey를 RF 리더기에 전송된 R_r을 기반으로 생성한다.

NKey = $(MKey \square R_r)$

[단계 3] 불법 Tag에 대한 보안 서비스

불법적인 Tag를 본 논문에서는 Black Tag라하며, Black Tag가 위치 및 서비스 단계에서 RF 리더기에 확인 될 경우 다음의 과정을 수행한다.

① Black Tag는 접속 요청 메시지를 RF 리더기에 전송한다.

Service_Challenge_Message

② RF Tag로부터 Service_Challenge Message 메시지를 수신한 RF 리더기는 [단계 1]의 ③에서 설정한 RFID인지 검증한 후 RF 리더기의 RFID 리스트에 등록되지 않는 ID일 경우 메시지 요청 메시지에 대한 응답 메시지를 다음과 같이 송신한다.

Black Tag_Sevice_Request

③ Black Tag는 RFID와 L_{BT}, X_m, Z_m을 RF 리더기에 송신한다.

④ RF 리더기는 Black Tag의 RF ID와 메시지 L_{BT}를 전송 받고 Black Tag의 Z_m을 검증한다. 검증이 올바른 경우 Black Tag에 대한 정보(Metal ID, L_{BT})를 브로드캐스팅하고 Black Tag 리스트에 해당 Tag에 대한 내용을 등록한다.

[단계 4] 인증된 단일 Tag의 서비스 제공

인증된 Tag가 서비스를 요구할 경우 RF 리더기는 SToken을 생성하여 이를 RF Tag에 전송하여, 서비스를 제공한다.

① RF Tag는 접속 요청 메시지를 RF 리더기에 전송한다.

Service_Challenge_Message

② RF Tag로부터 Service_Challenge Message 메시지를 수신한 RF 리더기는 서비스 정보 요청 메시지를 송신한다.

Service_information_reponce_message

③ RF Tag는 RF 리더기로부터 전송된 서비스 정보 요청 메시지를 수신한 뒤 임의의 난수 R_{t_1}과 타임 스탬프 T_t, NKey를 RF 리더기에 전송한다.

NKey, R_{t_1}, T_t

④ NKey, R_{t_1}, T_t를 수신한 RF 리더기는 서비스 정보 요청 메시지에 대한 단일 서비스

토큰을 생성하여 이를 RF Tag에 전송한다.

$$\text{SToken} = E_{NKey}(R_t \| R_r \| RID)$$

[단계 5] 그룹 서비스 제공

단일 서비스를 제공하는 SToken이 일정 개수 이상 RF 리더기에 전송되어 서비스를 제공 받고자 할 경우 다음과 같은 그룹 서비스를 제공한다.

① RF Tag는 서비스 요청 메시지와 SToken을 RF리더기에 전송한다.

RFID, Service_Request, SToken

② SToken을 전송받은 RF 리더기는 일정 개수 이상의 동일한 Service_Request 메시지가 리더기에 전송될 경우 다음과 같이 그룹 서비스 토큰을 생성하여 각각의 RF Tag에 전송함으로써 동일한 서비스를 요구하는 RF Tag들을 위한 임시 그룹 서비스를 제공한다.

$\text{GToken} = E_{Mkey}(H(SToken_i) \| R_r \| RID_i)$

(i는 동일한 서비스를 요구하는 Tag의 개수)

이상의 과정을 거쳐 RF Tag 기반의 안전한 형태의 네트워크 관리 방식이 수행된다.

5. 제안방식 분석

본 논문에서는 Tag 기반의 안전한 네트워크 구성 방식에 대한 연구를 수행하였으며, 기존 방식과 다음과 같은 차별화된 특징을 제시할 수 있다.

- ACIN(Authentication, Confidentiality, Integrity, Non-repudiation) : 제안된 방식의 경우 기존 방식과 비교 분석해 볼 때 기존방식과 동일한 ID기반의 인증 및 부인봉쇄 서비스와 안전한 해쉬 함수를 이용한 무결성 서비스가 제공된다. 그러나 기존 방식에서 고려되지 못했던 기밀성과 부인봉쇄를 위해 리더기에서 암호화된 서비스 토큰인 Token (단일서비스 토큰 $E_{Nkey}(R_t \| R_r \| RID)$, 그룹서비스토큰 $E_{Mkey}(H(SToken_i) \| R_r \| RID)$)을 이용해 어플리케이션 서비스를 위한 데이터의 기밀저장과 더불어 Trace정보를 이용 불법 Tag에 대한 추적 서비스를 제공할 수 있다.

- 채널 및 프로토콜 보안

제안된 방식은 리더기에서의 암호화를 통해 Tag에 전송되는 정보의 기밀성을 보장하였다. 따라서 기존 방식의 전방향 채널에서의 기밀성 서비스를 제공할 수 있도록 하였으며, 프로토콜상에서 전송되는 정보에 대한 기밀성과 무결성 제공을 위해 암호 알고리즘과 해쉬 함수를 이용한 방식을 제시하였다.

- 그룹 서비스

제안 방식의 경우 기존 방식에서 고려되지 않았던 Tag 기반의 네트워크 형성시 효율성을 높이기 위한 단일 및 그룹 서비스 토큰을 이용한 방식을 제안하였다. 서비스 토큰은 ID 기반의 인증 수행후 임시적인 그룹 서비스를 위해 제공할 수 있어 리더기에 대한 효율성과 임시적인 그룹을 위한 서비스 방식을 제시하였다.

- 불법 Tag에 대한 보안

제안된 방식은 기존 방식에서 고려되지 않았던 Trac 정보인 $X_m = (Trace \| MetalID)$을 이용해 불법 Tag가 접근시 불법 Tag에 대한 이동 경로를 추적할 수 있을 뿐 아니라 이에 대한 접근 제한 서비스를 위해 블록 Tag에 대한 내용을 주변 리더기에 브로드캐스팅하고 이에 대한 정보를 유지하도록 하였다.

6. 결론

본 논문에서는 차세대 IT 기반 환경인 유비컴퓨팅 기술의 적용을 위해 다양한 연구와 상용화가 추진중에 있는 무선 통신기술중에서 RFID를 기반으로 한 Tag 기술로 네트워크가 형성되었을 경우 발생할 수 있는 보안 취약성을 분석하고 이를 보완할 수 있는 네트워크 구성 방식에 대해 제안하였다.

제안된 방식의 경우 Tag에 대한 연산량과 메모리에 대한 고려는 거의 이루어지지 않았다. 따라서 제안된 방식은 저가격의 Tag 보다는 고가의 Tag를 이용한 네트워크 형성시 적용이 가능하다. 따라서 보다 현실적인 연구를 위해 저가격 Tag에서 고효율을 제공할 수 있는 네트워크 구성 및 관리 방식에 대한 지속적인 연구가 필요하다.

7. 참고 문헌

[1] Stephen Wolfram. Cryptography with Cellualr Autonoma. In Advances in Cryptology - CRYPTO, volume 218 of LNCS, pp429-432, Springer-Verlag, 1985.

[2] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Raido Frequescy Identification Systems. In Security in Pervasive Computing, 2003

[3] Frank Stajano and Ross Anderson. The Resurrecting Duckling : Security Issues for Ad-hoc Wireless Networks. In 7th International Workshop on Security Protocols, volume 1796, page 172-194, Leture Notes in Computer Science, 1999.

[4] MIT Auto-ID Center. http://www.autoidcenter.org

[5] RFID Journal. Gillette to Phurchase 500 Millin EPC Tags http://www.rfidjournal.com