물류 관리에 적용 가능한 패스워드 기반의 RF Tag 인증 프로토콜에 관한 연구

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

A Study on RF Tag Authentication Protocol of Based on Password applied Product Management

Dae-Hee Seo° 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 물류 관리에 적용을 고려하여 RF Tag 인증 프로토콜을 제안하고자 한다. 제안된 방식의 경우 기존 RF Tag 인증 연구에서 보다 하드웨어적 경량성을 제공할 뿐만 아니라 물류 적용을 위한 식별 회수에 제한둠으로 해서 보다 안전하고 효율적인 물류 관리 서비스를 적용할 수 있는 방식이다.

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[1].

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.

본 논문의 2장에서는 최근 많은 연구가 진행중에 있는 RFID기술의 개요에 대해 살펴본 뒤 3장에서는 RF Tag의 인증 연구와 관련된 기존 방식들을 분석한 뒤 4장에서는 RF Tag 인증 서비스에서 요구되는 보안 요구사항을 논하고자 한다. 5장에서는 물류 관리에 적용 가능한 패스워드 기반의 안전한 RF Tag 인증 프로토콜을 제안하고, 6장에서는 4장에서 제시한 보안 요구사항을 기반으로 기존 방식과의 비교를 통해 제안 방식을 분석한 후 7장에서 결론을 맺고자 한다.

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

2. RFID 기술의 개요

RFID는 판독 및 해독 기능을 하는 RF 판독기와 정보를 제공하는 RF Tag로 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 Tag를 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 Tag를 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 Tag가 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 Tag 및 무선 네트워크가 필요할 것이며 새로운 소프트웨어와 많은 아이

템을 다룰 수 있는 바코드 혹은 이와 비슷한 시스템이 요구될 수 있어 보다 다양한 형태의 어플리케이션을 지원할 수 있다.

3. 관련 연구

3장에서는 RF Tag의 인증과 관련된 기존 연구들을 분석하고자 한다.

① Hash Lock Scheme : MIT에 의해 제시된 방식으로 낮은 가격을 고려한 방식이다. 각각의 개체는 해쉬 함수를 가지고 있다고 고려되며 다음과 같은 방식으로 진행된다. 먼저 리더기는 키 K를 각각의 Tag에 전송하며 Tag는 Meta ID를 계산한다. (Meta ID = Hash(K)) Tag는 ID 엑세스를 위해 요청 메시지를 전송하고 이에 대한 응답 메시지로 Meta ID를 전송한다. 리더기는 사전 분배한 키와 Meta ID의 연계성을 고려하여 이를 검증하여 검증 결과가 올바른 경우 그에 대한 응답 메시지를 Tag에 전송한다. 이 방식의 경우 단지 전송 데이터에 대한 동의와 리더기가 가지고 있는 ID의 전송을 통해 인증 과정을 수행한다.
물론 본 방식에서는 낮은 가격과 고정된 Meta ID를 통해 낮은 가격에 적용 가능한 방식을 제한하였지만 공격자는 공개된 Meta ID를 통해 Tag에 대한 공격이 가능하다. 이외에도 Meta ID는 고정되어서는 안되지만 운영 시스템과 요구사항에 따라 약간의 차이가 존재하기도 한다.

② Randomized Hash Lock Scheme : MIT에서 제시된 방식으로 해쉬 락 방식의 확장된 형태이다. 이 방식의 경우 기존 방식과 달리 Tag가 안전한 해쉬 함수와 랜덤 생성기까지 가지고 있다고 가정한다. 각각의 Tag는 랜덤 수를 생성하여 이를 입력 값으로 안전한 해쉬 값을 생성한다. (r와 ID. C=H(id|r)), Tag는 C와 r을 리더기에 전송한다. 리더기는 전송된 데이터를 후방향 데이터 베이스에 전송한다. 데이터 베이스는 해쉬 함수를 이용해 전송된 r과 각각의 ID를 대응하여 저장한다. 데이터 베이스에서는 ID와의 연관성을 통해 C와 ID를 검증한다.
Tag의 output 정보가 엑세스 마다 매번 바뀌어 트래킹이 어려운 방식이다. 그러나 이와 같은 방식의 경우 RFID Tag의 위치 정보에 대해 추적 정보를 제공한다. 즉, Tag의 비밀정보와 관계됨을 의미한다. 이와 같은 방식은 전방향성 보안 사항에 만족할 수 없다. 추가적으로 해쉬 함수를 낮은 가격의 Tag에 적용될 수 있으나 의사난수 생성기와 같은 경우에는 사실적으로 불가능하다.

③ 해쉬 체인을 이용한 NTT Scheme : NTT에서 제안된 방식은 기존의 MIT에서 제안된 방식에서 익명성과 구분 불가능성에 목적을 두어 설계된 프로토콜이다. 이 방식의 경우 2개의 해쉬 함수를 이용하여 해쉬 체인을 형성하고 이를 기반으로 인증을 수행한다. NTT 방식은 초기 Tag의 초기 정보 s_1, i는 리더기에서 처리되는 횟수로 정의하고 RF Tag가 $a_i = G(s_i)$를 리더기에 전송한 후 사전 비밀값 s_i로부터 결정되는 갱신된 비밀정보 $s_{(i+1)} = H(s_i)$ 를 계산한다. 후방향 데이터베이스 서버의 경우 (ID, s_1)쌍을 리스트로 저장하여 유지한다. 데이터 베이스 서버는 Tag의 a_i를 리더기로부터 전송 받을 경우 ($a_i' = G(H^i(s_1))$)이며 각각의 s_1 리스트에 대해 계산을 수행한 후 $a_i = a_i'$과 같은지를 검증하고 같을 경우 a_i'에 해당되는 ID를 전송한다. 그러나 NTT 방식의 경우 2개의 해쉬 함수를 이용함으로 하드웨어적으로 한계성을 가질 수 있으며, 후방향 서버에서 저장된 데이터 s_i와 RF Tag의 정보가 상호 연관성이 있으므로, 후방향 서버의 안전성이 취약할 경우 적용의 한계성을 갖는다.

4. 보안적 요구사항 및 분석

RF 시스템에서는 일반적인 무선 환경의 보안 요구사항과는 별도의 요구사항이 요구된다. RF 시스템에서 요구되는 다양한 형태의 요구사항 중에서 본 논문에서는 다음과 같은 3가지의 보안 요구사항을 제시하고자 한다.
- 전방향성 보안 : RFID에서는 리더기를 기준으로 전방향(Tag-to-reader) 채널과 후방향(reader-to-Tag) 채널에 대한 보안이 요구된다. 그러나 현재의 RFID에서는 전방향/후방향 채널에 대한 보안 서비스를 제공하지 못해 사용자 프라이버시에 보호에 대한 취약성을 내포하고 있다. 따라서 전방향성 보안을 제공할 수 있는 인증 프로토콜이 요구된다.
- 비밀정보와의 연관성 : 초기 인증을 위해 전송되는 정보가 RF Tag의 인증 ID와의 연관성이 존재해서는 안된다. 만약 공격자가 피공격 대상의 RF Tag의 ID와 초기 인증 전송 메시지와의 연관성을 구분할 수 있다면, 이는 심각한 취약성을 가질 수 있다.
- 효율성 : RF Tag 인증 시스템을 구성하고자 할 경우 현재 RF Tag의 물리적 한계성 때문에 발생할 수 있는 적용의 문제점을 해결 할 수 있어야 한다. 여기에서 가장 중요한 점은 낮은 가격의 Tag에 적용이 가능한지의 여부이며, 이는 하드웨어적 구성에 초점이 맞추어지게 된다.

5. 물류 관리에 적용 가능한 패스워드 기반의 RF Tag 인증 프로토콜 제안

5장에서는 물류 관리에 적용 가능한 패스워드 기반의 RF Tag 인증 프로토콜을 제안하고자 한다.

5.1 가정사항

① RF Tag는 안전한 해쉬함수 H() 연산과 XOR 연산이 가능하다.
② 초기 RF Tag는 후방향 데이터 서버로부터 PW_1, t를 안전한 경로를 통해 할당받는다.
③ 후방향 서버는 RF Tag A에 할당된 PW_1과 대응되는 PW_2를 안전하게 저장한다.
④ PW_0는 H(PW_1) + H(PW_2)으로 구성된다.

5.2 시스템 계수

다음은 물류 관리에 적용 가능한 RF Tag 인증 프로토콜 제안을 위한 시스템 계수를 기술하고자 한다.

PW_1 : RF Tag에 등록된 초기 8bit 패스워드
PW_2 : 후방향 데이터 베이스 서버로부터 RF Tag가 초기 할당받은 패스워드

RFID, RID : RF Tag의 ID, 리더기의 ID
r : 리더기에서 생성된 의사난수
t : RF 리더기에서 설정한 RF Tag의 식별 회수
i : 식별 카운터 정보
$H()$: 안전한 해쉬 함수

5.3 프로토콜

패스워드 기반의 RFID인증 프로토콜은 다음과 같은 진행 과정으로 수행된다.

① RF 리더기는 초기 Query 메시지를 RF Tag에 전송한다.

Query

② RF Tag는 초기 등록된 8bit 패스워드인 PW_1을 다음과 같이 계산하여 RF 리더기에 전송한다.

$$W_a = H(PW_1)$$

③ RF 리더기는 RF Tag로부터 전송된 W_a와 후방향 데이터 베이스 서버로부터 RF Tag에 할당된 초기 패스워드 PW_2를 전송받은 후 PW_0를 다음과 같이 생성한 뒤 i를 1로 초기화 한뒤 RID와 r, PW_0를 RF Tag에 전송한다.

$$W_a + H(PW_2) = H(PW_1) + H(PW_2) = PW_0$$

④ RF Tag는 RF 리더기로부터 전송받은 RID, r, PW_0를 수신한 뒤 k를 계산하여 k, i, W_i를 RF 리더기에 전송한다.

$$k = (RFID \oplus r)$$
$$W_i = H^{t-i}(PW_0)$$

⑤ RF 리더기는 RF Tag로부터 전송된 k의 검증 과정을 수행한 뒤 W_i를 검증하여 올바른 경우 인증 과정을 종료한다.

6. 제안 방식 고찰

본 논문에서 제안된 방식은 4장의 보안 요구사항을 기반으로 기존 방식과의 비교 분석을 수행할 경우 다음과 같은 보안적 안전성을 갖는다.

- 전방향성 보안 : 초기 인증 메시지인 W_a의 경우 RF Tag에서 안전한 해쉬 함수로 생성된 값이며, RFID 인증을 위해 전송되는 값의 경우 카운터 값으로 해쉬 체인을 생성하여 전송함으로써 리더기와 RF Tag 사이의 안전성을 제공할 수 있다.
- 구분 불가능성 : 제안방식의 경우 RF Tag에서 전송되는 W_a와 $RFID$와는 연관성이 없이 전송된다. 또한 후방향 서버에 저장되어 있는 PW_2와 RF Tag에 저장된 PW_1을 기반으로 PW_0를 생성함으로 하나의 개체를 통해 획득된 정보를 기반으로 초기 PW를 보호할 수 있는 전방향성 보안을 제공한다.
- 효율성 : 제안된 방식은 기존의 MIT의 해쉬락 방식과 같이 하나의 해쉬함수만을 이용하여 구성된다. 따라서 하드웨어적 구성적으로는 MIT의 향상된 해쉬락 방식과 NTT에서 제안된 방식과 비교하였을 경우 보다 효율적인 하드웨어 구성이 가능하다.

7. 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 물류 관리에 적용이 가능한 RF Tag 인증 방식을 제안하였다.

제안된 방식은 기존의 유/무선 프로토콜과 비교해볼때 많은 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 제시하였다.

본 논문에서 제시된 방식은 기존의 방식보다 하드웨어적 안전성을 유지하면서 물류 관리에 적용을 위해 인증 회수의 제한을 두어 구성하였다. 향후 제안된 방식을 EPC 네트워크에 적용할 수 있도록 확장성을 제시하고자 하여 새로운 형태의 EPC 관리를 위한 연구를 지속적으로 수행하고자 한다.

참고문헌

[1] J.Hoffstenin, J.Pipher, and J.Silveman. NTRU : A ring based Public key cryptosystem. In ANTSⅢ (LNCS no.1423), pp.267-288, 1998

[2] A. Juels/ Privacy and authentication in low-cost RFID tags. In submission. Available at http://www.rsasecurity.com/rsalabs/staff/bios.ajuels/

[3] A.Juels and R.Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. in Proceedings of the 7th Financial Cryptography Conference, 2003.

[4] R. Rivest. The MD5 message-digest algorithm. Internet RFC 1321, April 1992.

[5] A.Perrig, R. Canetti, J.D. Tygar, and D. Song. The TESLA broadcast authentication protocol. CryptoBytes, 5(summer),2002.

[6] S. Sama, S. Weis, and D. Engels. Radio-frequency identifcation : Security risks and challenges. CryptoBytes, 6(1), 2003.

[7] J.Stern and J. Stern. Cryptanalysis of the OTM signature scheme from FC'02. In Proceedings of the 7th Financial Cryptography conference, 2003.

[8] Istvan Vajda and Levente Buttyan. Lightweight Authentication Protocols for Low-Cost RFID Tags (http://www.crsys.hu)

[9] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In Proceedings of the 1st International conference on Security in Pervasive Computing, 2003.