유동성을 지닌 RFID 시스템을 위한 인증 프로토콜 설계

김영진*

An Authentication Protocol Design in RFID System for Mobility

Young-jin Kim*

요 약

RFID는 무선통신을 사용하는 방법이다. 하지만 인증 및 보안성을 위한 메커니즘을 사용하고 있지 않다. 그러므로 다중인식 공격이나 도청공격과 같은 공격에는 매우 취약하다. 또한 RFID 시스템의 특성상 Tag의 제한된 환경적 요소 때문에 인증 프로토콜을 설계하는데 제약이 크다. 그렇다고 보안성이 없는 RFID를 사용할 경우 기업의 정보와 상품의 정보를 노출하게 되며, 공격자가 RFID 시스템에 침입하여 물류 시스템을 정지 시킬 수 있다. 그래서 본 논문은 Tag에 대한 무제한적인 접근이 아닌 유동성을 지닌 인증된 Reader만 접속만 가능하도록 Tag와 Reader간의 인증 메커니즘을 설계하고 또한 키 분배를 정의하여 새로운 인증 프로토콜을 제안하고자 한다.

ABSTRACT

RFID is method used on wireless system. However, this mechanism is not used for authentication and security. Therefore, it is very vulnerable to attacks such as dropping attacks and traffic attacks. the RFID Tags are of the limited nature due to environment factors and there is greater constraints in designing authentication protocol. If we do not RFID to secure corporate information and product all the information will be exposed. The attacker will break into the RFID system and stop the distribution system. So, this paper proposes a new authentication protocol which provides not only unlimited access to Tag&Reader of mobile and connection between Tag and Reader bet also provides authentication mechanism by defining the key distribution.

키워드

RFID, Tag, Reader, 인증

Key word

RFID, Tag, Reader, Authentication

* 조선이공대학교 메카트로닉스과 교수

접수일자 : 2009. 09. 28
심사완료일자 : 2009. 11. 13

Ⅰ. 서 론

물류 활동량이 증가하는 가운데 RFID기술의 필요성은 더욱 증대되고 있다. 하지만 RFID기술의 특성상 무선 네트워크이기 때문에 보안적 문제가 발생한다. 따라서 이런 보안적 문제를 해결하기 위해 현재 암호화 알고리즘을 사용하여 문제점을 해결하고자 하지만 태그가 가지고 있는 제한적 요소인 제한된 메모리와 전력 때문에 어렵다. 아무리 좋은 암호화알고리즘이라도 태그의 제한적 환경에 맞게 설계가 되어 있지 않다면 사용할 수 없다는 것이 현실이다. 전송하는 데이터 보다 암호화하는 과정에 더 많은 전력이 소모된다면 비효율적인 시스템이 되기 때문에 많은 기업에서도 태그에는 공개키 암호화 알고리즘을 사용하지 않는다[1].

또한 태그와 리더는 무선통신을 통해 정보를 전송하기 때문에 불법 리더에 의한 도청이 쉽게 가능하다. 하지만 이를 막는 기술은 미흡한 실정이며, RFID시스템을 사용하는 업체에서도 비용문제 때문에 보안적 기술을 사용하지 않는다[2]. 그래서 본 논문은 태그의 제한적 요소를 감안하며, 기존의 RFID 인증 시스템보다 높은 효율성과 안전성을 가진 RFID 인증 프로토콜을 설계하였다.

Ⅱ. RFID 인증 시스템

현재 많은 RFID 인증 시스템을 사용하고 있지만 가장 널리 사용하는 방식은 해쉬함수를 이용하는 방식이다. 그 이유는 태그의 제한적 환경 요소에 영향을 받지 않으며, 인증된 리더만이 태그에 접속이 가능하기 때문이다.

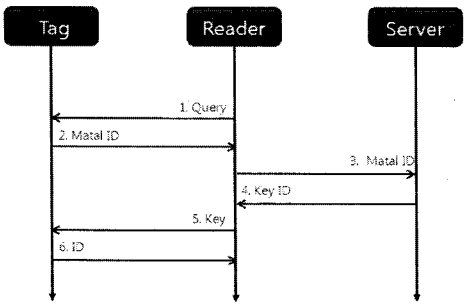

그림. 1 MIT 해쉬 함수
Fig. 1 MIT Hash Function

위 그림은 MIT 해쉬함수이며, 인증된 리더만이 태그의 정보를 수신할 수 있는 방법으로, Weis[3]가 제안하였다. 인증과정은 다음과 같다[4,5].

1. Query
   리더는 태그에게 정보전송을 요청한다.
2. Matal ID
   태그는 자신의 키에 대한 Hash 값인 Matal ID값을 계산한 뒤, 리더가 제시하는 Query에 대해 응답한다.
   Matal ID = Hash(kID)
3. Matal ID
   태그의 Lock 상태를 풀기 위해 리더는 Metal ID값을 서버에 Query로 제시한다.
4. Key ID
   서버는 저장된 ID에 대한 키를 찾아 리더에게 전달한다.
5. Key
   찾은 키를 리더가 태그에게 전송하면 태그는 그 키를 Hash 함수로 연산하여 Metal ID값과 일치한지 검사한다.
6. ID
   일치하면 Lock 상태가 풀고, 근처의 리더에게 자신의 ID 및 모든 기능을 제공한다.

Ⅲ. 취약점

RFID 시스템은 매우 효율적인 물류 시스템이다. 하지만 보안적 메커니즘이 확실하게 정의 되어있지 않는 상태이며, 사용자 및 기업이 필요성을 못 느끼고 있어 보안적 연구가 부진한 상황이다[6].

RFID 시스템에서 가장 취약한 부분은 태그이다. 태그는 무제한적 접근이 허용되므로 인증되지 않은 리더가 태그에 있는 정보를 쉽게 얻을 수 있다. 이런 문제점을 해결하기 위해 해쉬함수를 이용한 방법을 가장 많이 사용하고 있지만 해쉬함수도 보안적으로 매우 취약하다. 그림 1에서 설명한 것처럼 해쉬함수는 태그의 ID를 기반으로 하는 인증하는 방법이다. 하지만 이 방법 또한 ID가 유출된다는 문제점이 있다. 노출된 ID를 기반으로 태그의 복제가 가능할 뿐만 아니라 서버에 저장된 데이터

베이스도 ID를 기반으로 구축되어 있기 때문에 태그의 정보를 쉽게 얻을 수 있다[7~10].

표. 1 RFID 시스템의 취약점
Table 1. Weakness of RFID System

구분	특징
수집	• RFID정보주체의 인식여부에 관계없이 무제한 수집 가능
정보 변화	• RFID태그정보는 RFID태그가 부착된 물품이 사업자간의 교환 및 소비자에게 이동했을 경우 변화 가능
개인 정보화	• RFID태그정보와 개인정보의 융합시 개인 프라이버시 침해가 우려됨
발생 가능한 문제점	• RFID정보를 이용한 개인 신상정보 노출 • RFID정보를 활용한 개인의 물품 보유현황 노출 • RFID인식 기술을 이용한 위치정보 노출 • RFID가 상품에 활용될 때 개인의 구매 패턴 및 선호도 노출 • RFID정보를 원하는 기업이 있는 경우 개인의 의사와 무관하게 불법적인거래가 이뤄질 수 있음 • 타 정보와의 결합을 통한 개인 정보화
태그 정보의 침해 유형	• 부적절한 RFID정보의 접근과 수집 • 부적절한 RFID정보 분석 • 부적절한 RFID관련 정보의 이전 • RFID태그 정보를 활용하여 원하지 않는 영업 행위

Ⅳ. 제안하는 RFID 시스템

기존의 RFID 인증 시스템은 해쉬함수를 기반으로 하는 방식이며, 키 분배도 없다. 그렇기 때문에 태그의 정보가 쉽게 누출이 되며, 또한 태그의 복제가 가능하다[11]. 하지만 제안하는 RFID 시스템은 태그와 리더간의 인증 프로토콜과 키 분배를 정의하고, 리더와 서버간의 인증 프로토콜을 정의하여 보다 높은 보안성을 가지고 있다.

1. 태그와 리더간의 키 분배

기존의 RFID 시스템은 키 분배 과정이 없다. ID를 전송하고 ID를 기반으로 데이터베이스에서정보를 찾는 정도였다. 또한 네트워크가 성립되기 전에 같은 키를 분배라는 방식을 사용한다. 하지만 이 방법은 ID와 키가 유출되기 때문에 문제가 많다. 그래서 태그와 리더간의 키 분배를 정의하였다. 그 과정은 그림 2와 같다.

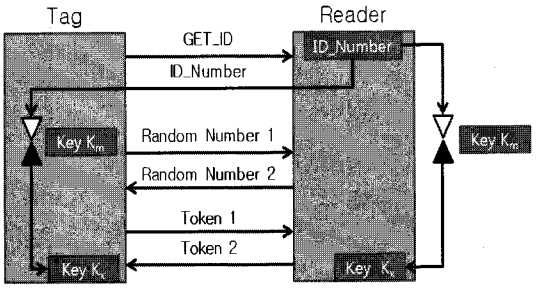

그림. 2 키 분배
Fig. 2 Key Distribution

1. GET_ID
태그는 ID를 리더에게 전송한다.
2. ID_Number
태그에서 전송받은 ID를 기반으로 데이터베이스에 저장된 정보를 태그에게 전송한다.
3. Random Number 1
태그는 전송받은 ID_Number를 기반으로 3자리 숫자를 추출하여 리더에게 전송한다.
4. Random Number 2
리더는 ID_Number를 기반으로 3자리 숫자를 추출하여 태그에게 전송한다.
5. Create Key
Key Km=
(Key kx ⊕ ID_Number)
리더와 태그는 전송받은 데이터를 가지고 새로운키를 생성한다.
6. Token 1
Token 1=
E_{km}(Random Number1 ‖ Tag's ID)
생성된 키를 기반으로 대칭키 암호화 방식을 사용하여 ID와 Random Number1을 암호화하여 리더에 전송한다. 이는 태그와 리더간의 인증과정에서 토큰 키로 사용된다.
7. Token 2
Token 2=
E_{km}(Random Number2 ‖ ID_Number ‖ Tag's ID)

생성된 키를 기반으로 대칭키 암호화 방식을 사용하여 Random Number2, ID_Number, ID를 암호화하여 태그에 전송하다. 이는 마찬가지로 태그와 리더간의 인증 과정에서 토큰 키로 사용된다.

2. 태그와 리더간의 인증 과정

태그와 리더간의 인증과정은 해쉬함수를 기초로 설계하였다. 하지만 해쉬함수는 태그와 리더간의 핸드쉐이크 과정이 총 4과정이지만 제안하는 방식은 총 2과정이다. 과정이 절반으로 줄었기 때문에 효율성 측면에서는 보다 높다는 것을 알 수 있으며, 또한 누출되는 과정을 줄였기 때문에 공격자에 공격받을 가능성도 줄어들게 되었다. 제안하는 인증과정은 그림 3과 같다. 제안하는 인증방식에서는 Query를 표시하지 않았다. 인증 과정을 시작하기 전에 먼저 리더의 요청이 있어야만 시작된다는 전제 조건이 있기 때문이다. 만약 Query부분까지 생각을 한다면 제안하는 인증방식은 총 3과정의 통신을 가지게 된다.

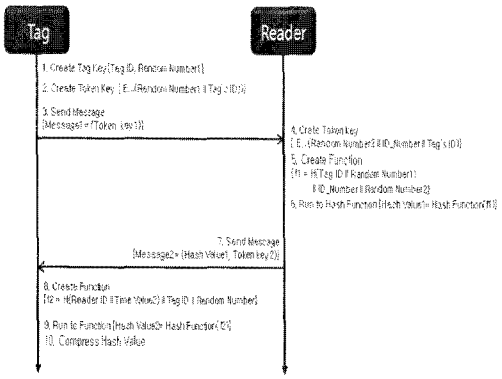

그림. 3 태그와 리더간의 인증 과정
Fig. 3 Authentication Mechanism between Tag and Reader

1. Create Tag Key(Tag ID, Random Number1)
   태그는 아이디와 Random Number1을 생성한다. 이 과정은 키 분배과정을 통해 이루어진다.
2. Create Token Key
   {Ekm(Random Number1 ‖ Tag ID}
   태그는 리더에 접근을 하기 위한 토큰키를 생성하며 이 과정 또한 키 분배과정에서 생성된 토큰키을 사용된다.
3. Send Message {Message1=(Token Key1)}
   생성된 토큰키를 전송하여 이를 기반으로 리더에 접근이 가능하게 된다. 새로 생성된 키로 암호화를 하였기 때문에 아이디는 유출되지 않는다.
4. Create Token Key
   E_{km}(Random Number2 ‖ ID_Number ‖ Tag ID)
   리더는 태그에 접근을 하기 위한 토큰키를 생성하며 이 과정 또한 키 분배과정에서 생성되는 토큰키를 사용한다.
5. Create Hash Function
   {f1 = H(Tag ID ‖ Random Number1) ‖ ID_Number ‖ Random Number2}
   태그의 ID와 태그에서 생성된 Random Number를 기반으로 해쉬함수를 연산하도록 하며 리더에 전송되는 ID_Number와 Random Number를 해쉬함수와 같이 연산하는 방정식을 생성한다.
6. Run to Hash Function
   {Hash Value1=Hash Function(f1)}
   5번 과정에서 생성된 해쉬함수를 연산을 한다.
7. Send Message
   {Message2=(Hash Value1, Token Key2)}
   연산되어 생성된 값과 리더에서 생성된 토큰키를 태그에게 전송한다.
8. Create Hash Function
   {f2 = H(ID_Number ‖ Random Number2)
   ‖ Tag ID ‖ Random Number1 }
   리더에서 전송한 ID_Number와 Random Number를 가지고 해쉬함수를 연산하도록 하며 태그에서 생성된 ID와 Random Number를 해쉬함수와 같이 연산하는 방정식을 생성한다.
9. Run to Hash Function
   {Hash Value1=Hash Function(f2)}
   8번 과정에서 생성된 해쉬함수를 연산을 한다.
10. Compress Hash Value
    6번 과정에서 생성된 해쉬값과 9번 과정에서 생성된 해쉬값을 비교하여 일치하면 인증이되며 접근이 가능하게 된다.

V. 시뮬레이션 환경

시뮬레이션은 OPNET14.5에서 구현하였다. 기본적인 RFID 시스템에서 하였으며, 태그 3개, 유동성 리더 1개, AP 1개, 서버 1개, 그리고 공격자 1개로 구성되었다. 태그는 Semi-passive방식의 태그를 사용하였다. Semi-passive방식은 능동형 방식과 수동형 방식을 결합해 놓은 Hybrid형 태그이다. 배터리는 내장되어 있으며 이 배터리는 내부적인 프로세싱에 사용된다.

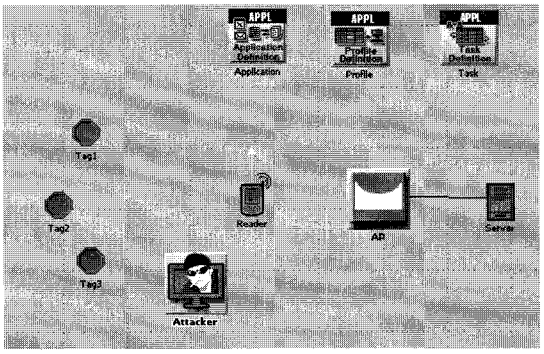

그림. 4 시뮬레이션 환경
Fig. 4 Simulation Environment

표. 2 시뮬레이션 파라미터
Table 2. Simulation Parameter

Statistics	Value
Scenario size	100m X 100m
Transmission Range	< 10 meter
Transmit Power	0.005W
Tag Type	Semi-passive
Tag Processer	54 bit
Simulation Time	1 hour

그림 4는 시뮬레이션 환경을 나타낸 것이다. 공격자는 태그와 리더간의 통신을 공격한다. 공격방법은 도청공격을 하며, 메시지를 도중에 가로채기공격도 하도록 설정하였다. 공격자가 사용하는 공격방법인 도청공격과 가로채기공격의 특성은 거의 똑같다. 도청공격은 인증되지 않은 리더가 태그에 접근하여 태그의 출력을 얻어 이를 기반으로 태그의 ID와 정보를 획득하는 공격방법이다. 가로채기공격은 리더와 태그사이의 인증과정에서 발생될 수 있는 공격방법으로, 인증된 정보를 가로채는 공격방법이다. 이 두 공격방법은 공격자가 공격을 통해 얻은 정보를 토대로 다시 리더나 태그에 접근할 수 있는 공격방법이다. 만약 제안하는 인증방법이 이 공격방법에 취약하다면 공격자가 보내는 인증되지 않은 정보를 처리하게 되며 이에 따라 통신량이 늘어나게 되는 현상이 발생하게 된다. 또한 공격자로 인해 태그와 리더사이에 원활한 통신을 할 수 없으며 응답시간의 지연현상이 생기며, 리더와 태그는 공격자가 보내는 변복조된 데이터를 받고 응답을 하거나 자신의 정보를 전송하게 된다.

VI. 시뮬레이션 결과

시뮬레이션에서 통신 환경은 기본적인 RFID시스템 환경이며 공격자가 통신에 간섭하는 가운데 MIT 해쉬함수 방법과 제안하는 해쉬함수 방법을 사용하여 전송량과 지연시간을 비교하였다.

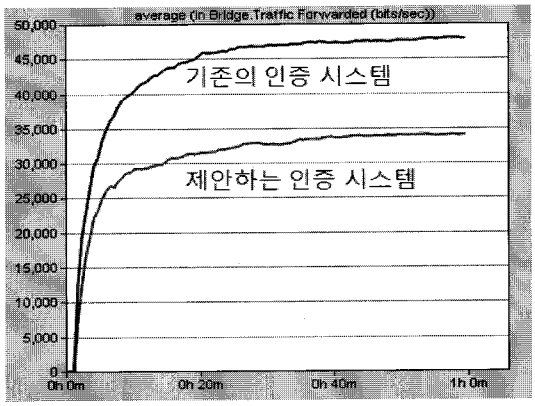

그림. 5 시뮬레이션에서 태그와 리더간의 전송량(bits/sec)
Fig. 5 Traffic between Tag and Reader in Simulation(bits/sec)

위 그림 5는 기존의 MIT 해쉬함수 인증방법과 제안하는 해쉬함수 인증방법의 전송량을 리더에서 측정하여 비교한 것이다. 그래프에서 볼 수 있듯이 제안하는 방식과 기존의 방식이 평균적으로 10,000bit/sec 정도 차이나

는 것을 알 수 있다. 이 차이는 공격자가 태그와 리더간의 정보를 수집하여 변복조하여 공격하는 방식을 막았다는 것을 보여준다. 변복조한 데이터에 대해서 인증이 되지 않았기 때문에 리더와 태그는 그에 대해 응답을 하지 않았으며, 그로인해 정보의 유출을 막았다고 볼 수 있다. 공격자가 보낸 데이터는 무시하고 태그와 리더는 원활한 전송을 할 수 있었다는 것을 그림 6의 지연시간 비교를 통해서도 알 수 있다.

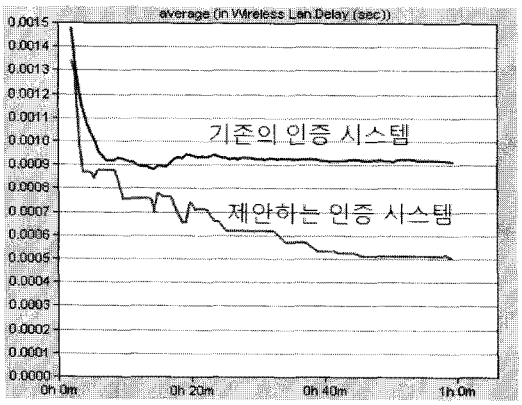

그림. 6 시뮬레이션에서 태그와 리더간의 지연시간(sec)
Fig. 6 Delay between Tag and Reader in Simulation(sec)

그림 6은 기존의 MIT 해쉬함수 인증방법과 제안하는 해쉬함수 인증방법의 지연시간을 리더에서 측정하여 비교한 것이다. 위 그래프에서 지연시간은 제안하는 방식이 약 0.0002sec 정도 이득을 보았다는 것을 알 수 있다. 공격자가 공격을 하는 도중 생기는 지연시간이 점점 줄어들어 가는 것을 보여주는 것이다.

두 개의 결과값으로 제안하는 방식이 기존의 인증 방식보다 보다 안전하다는 것을 입증하게 된다. 공격자가 전송하는 데이터는 인증이 되지 않는 데이터이므로 리더와 태그는 그에 대한 응답을 전혀 하지 않으며 그로 인해 공격자의 공격으로 인해 생기는 딜레이가 점점 줄어들어 태그와 리더간의 통신이 공격자의 간섭이 없이 통신을 할 수 있다는 것을 보여준다.

Ⅶ. 결론

기존의 MIT 해쉬함수를 이용한 인증 방식은 매우 유용한 방법이지만 아이디가 유출된다는 문제와 공격자에게 쉽게 공격을 받는다는 문제점을 가지고 있다. 제안하는 해쉬함수 방식은 키를 새로 생성하고, 생성된 키를 기반으로 접근을 할 수 있는 토큰키를 생성하게 하며, 마지막으로 토큰키안에 들어있는 ID, ID_Number, Random Number을 기반으로 해쉬함수를 만들어 인증하는 방식이다. 제안하는 인증 시스템은 키와 아이디가 유출되지 않으며, 접근방식이 암호화를 통한 토큰키로 Random Number가 들어가기 때문에 트래픽분석을 통한 복제를 방지할 수 있다.

하지만 태그의 제한적 환경 요소를 최대한으로 이용한 것이기 때문에 추가적인 데이터의 삽입의 공간이 적다는 문제점을 가지고 있다. 앞으로 태그의 제한적 환경 요소가 개선된 태그의 개발이 가능하다면 보다 높은 인증 시스템이 적용가능 할 것이며 그로 인해 물류시스템에 RFID를 적용하기가 보다 쉬워지며 RFID 시스템에 대한 신뢰성이 높아 질 것이다.

References

[1] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. "Sercurity and Privacy Aspects of Low-Cost Radio Frequency Identification System.", In Security in Pervasive Comp., Vol. 2802 of LNCS, pp. 201-212. 2004

[2] 김현. "Analysis of RFID Authentication Protocl", In KISA Report. 2006

[3] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. "Sercurity and Privacy Aspects of Low-Cost Radio Frequency Identification System.", In Security in Pervasive Comp., Vol. 2802 of LNCS, pp. 201-212. 2004

[4] 박규진, 한경헌, 성종엽, 유도경, 최동유, 한승조. "RFID Tag의 인증을 통한 보안성 향상", 정보보호학회 하계학술대회, 2009. 06

[5] H.Y. Chien, "Secure Access Control Schemes for RFID System with Anonymity", In Proceedings of 1005 national Workshop on Future Mobile and Ubiquitous Information Technologies. 2006

[6] G. Avoine, E. Dysli, and P. Oeschslin, "Reducing time Complexity in RFID systems", In The 12th Annual Workshop on Selected Areas in Cryptography. 2005

[7] M. Ohkuho, K. Suzki and S. Kinoshita, " Cryptographic Approach to 'Privacy- Triendly' Tags", In RFID Privacy Workshop. 2003

[8] D. Molnar and D. Wanger, "Privacy and Security in Library RFID: Issues, Pratices, and Archtiectures." In Conference on Computer and Communication Security. pp.210. 2004

[9] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-reponse based RFID Authentication Protocol for Distributed Database Environment", In International Conferences on Security in Pervasive Computing. pp.70. 2005

[10] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual Authentication Protocol for Low-Cost RFID", Handout of the Ecrypt Workshop on RFID and Lightweight Crypto. 2005

[11] J. Yang, J. Park, and K. Kim "Security and Privacy on Authentication Protocol for Low-Cost Radio", In The 2005 Symposium on Cryptography and Information Security. 2005

저자소개

김영진 (Young-Jin Kim)

1995년 ~ 2008년: 주) LG 데이콤
1998년 : 조선대학교 전자공학과 (공학 석사)
2003년 : 조선대학교 전자공학과 (공학 박사)

현재 조선이공대학 메카트로닉스과 교수
※ 관심분야 : 무선 네트워크, 네트워크 보안, 임베디드