논문 2011-48IE-2-9

토큰키와 해쉬함수를 이용한 RFID 인증 프로토콜 설계

(Design of an RFID Authentication Protocol Using Token Key and Hash Function)

나 영 남*, 한 재 균**

(Young-Nam Na and Jae-Kyun Han)

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 태그의 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 태그에 대한 무제한적인 접근이 아닌 인증된 리더만 접속 가능하도록 태그와 리더간의 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 and connection between Tag and Reader bet also provides authentication mechanism by defining the key distribution.

Keywords : RFID, Hash, Authentication

Ⅰ. 서 론

근래 각종 매체를 통해 빈번히 보도되고 있는 유비쿼터스 기술은 또 한 번 정보통신 기술의 대혁신을 예고하고 있다. RFID(Radio Frequency Identification) 및 USN(Ubiquitous Sensor Network)기술은 이러한 유비쿼터스 환경의 가장 핵심적인 요소라고 할 수 있으며 지식경제부에서도 미래의 정보통신 기술 구현을 위한 핵심 인프라로 선정된 바 있다. 실제로 RFID기술은 물류, 운송, 유통, 내부 재고관리 등에 획기적인 개선을 가져올 것으로 예상되며 이미 여러 분야에 적용되어 사용되고 있다.

RFID기술은 사물의 식별정보 등을 극소형 태그에 저장하여 사물에 부착하고 해당 사물 및 주변 환경 정보를 무선주파수를 통하여 안테나가 장착된 리더 및 네트워크로 전송하여 필요한 정보처리를 하는 비접촉식 자동식별 기술을 말한다. 그러나 RFID기술은 인간생활에 편리함을 주는 동시에 '언제·어디서나' 개인정보가 누출될 수 있는 환경을 제공하여 프라이버시 침해의 역기능 문제도 동시에 안겨주고 있다.

RFID는 무선네트워크를 기반으로 하는 소규모 네트

* 정회원, 조선이공대학 정보통신과
(Dept. of Information Communications, Chosun University College of Science & Technology)
** 정회원-교신저자, 한국방송통신대학교
(Korea National Open University)
접수일자: 2011년5월26일, 수정완료일: 2011년6월15일

워크로 이루어지기 때문에 보안적인 문제가 많이 발생한다. 이런 보안적인 문제를 해결하기 위해 현재 사용중인 높은 보안성을 가지는 알고리즘을 사용하여 문제점을 해결하고자 하지만 RFID 태그의 특성인 제한된 메모리와 제한된 전력 때문에 크기가 큰 암호화 알고리즘을 사용하지 못한다. 매우 좋은 암호화 알고리즘이라도 태그의 제한적 환경에 알맞게 설계가 되어 있지 않다면 사용할 수 없다는 것이 현실이다. 전송하는 데이터 보다 암호화하는 과정에 더 많은 전력이 소모된다면 비효율적인 시스템이 되기 때문에 사용하지 못한다. 좋은 암호화 알고리즘을 사용하기 위해서 좋은 태그를 사용하면 되지만 태그의 단가가 높아지기 때문에 많은 기업에서도 태그에는 암호화 알고리즘을 사용하지 않는다.

태그와 리더는 무선 통신을 통해 정보를 교환하기 때문에 불법적인 리더에 의한 도청 및 정보의 변복조가 쉽게 가능하다. 하지만 이를 막는 기술은 매우 미흡한 상태이며, 사용하는 기술도 많은 문제점을 가지고 있다. 그래서 본 논문은 태그의 제한적 요소를 감안하여 기존의 인터페이스를 계속 사용하는 가운데 기존의 RFID 인증 시스템보다 높은 효율성과 안전성을 가진 RFID 인증 프로토콜을 설계하고, 시뮬레이션을 통해 기존의 보안 방식과 비교·검토함으로서 그 실용성과 타당성을 검증하고자 한다.

Ⅱ. RFID 시스템 특징

RFID 시스템은 물품과 같이 관리할 사물에 태그를 부착하고 신호를 이용하여 사물의 ID 정보 및 주변 환경 정보를 인식하여 각 사물의 정보를 수집, 저장, 가공 및 추적함으로써 사물에 대한 원격처리, 관리 및 정보 교환 등 다양한 서비스를 제공한다. 기본적인 동작원리는 리더가 무선통신을 이용하여 태그에게 질의를 보내면 태그 안에 내장된 안테나가 전파를 수신한다. 태그 안에 내장된 IC칩이 정보를 신호화하여 안테나를 통해 신호를 전송함으로써 리더는 전송된 신호를 유무선 방식으로 종단 시스템으로 전달한다. 그리고 리더의 종단 시스템은 태그가 전송한 정보와 종단 시스템의 정보를 비교하여 매치된 정보를 리더에게 전송하며, 리더는 이를 디스플레이 장치를 통해 사용자에게 보여준다.

RFID 시스템의 효율성과 정확성은 바코드 시스템과 비슷한 수준이지만 RFID의 경우에는 바코드에 비해 더 많은 장점을 가지고 있다[1].

① 태그 내부에 저장되어 있는 정보를 효과적으로 실시간 갱신이 가능

② 비금속 물질을 투과해서 읽을 수 있으며, 비접촉 인식이 가능

③ 태그 설치의 제한을 받지 않아 보이지 않은 곳에 설치 가능

④ 불법 사용자가 특정 상품에 관한 데이터를 변경할 수 없도록 보호가 가능

⑤ 바코드보다 판독시간이 40% 빠름

Ⅲ. 기존의 해쉬 인증방법

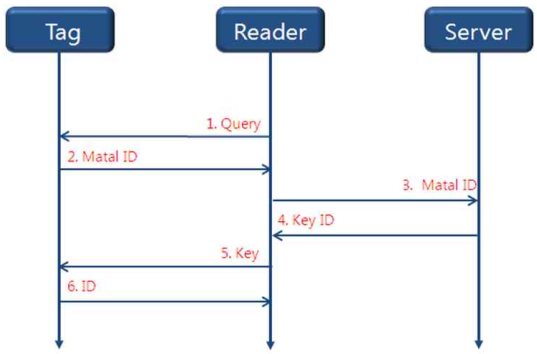

그림 1. MIT 해쉬 함수
Fig. 1. MIT Hash Function.

그림 1은 MIT 해쉬함수이며, 인증된 리더만이 태그의 정보를 수신할 수 있는 방법으로, Weis[11]가 제안하였다. 인증과정은 다음과 같다[8~9].

① **Query**

리더는 태그에게 정보전송을 요청한다.

② **Matal ID**

태그는 자신의 키에 대한 Hash 값인 Metal ID값을 계산한 뒤, 리더가 제시하는 Query에 대해 응답한다.

Metal ID = Hash(key)

③ **Matal ID**

태그의 Lock 상태를 풀기 위해 리더는 Metal ID값을 서버에 Query로 제시한다.

④ **Key ID**

서버는 저장된 ID에 대한 키를 찾아 리더에게 전달

⑤ **Key**

찾은 키를 리더가 태그에게 전송하면 태그는 그 키를

Hash 함수로 연산하여 Metal ID값과 일치여부 검사

⑥ **ID**

일치하면 Lock 상태가 풀고, 근처의 리더에게 자신의 ID 및 모든 기능을 제공한다.

해쉬락 기법에서는 리더와 태그가 모두 동일한 해쉬 함수를 미리 가지고 있으며, 인증 정보를 생성하고 태그를 잠금 상태로 만드는 과정과 실제 태그-리더간 인증을 수행하는 풀림 과정으로 구성된다. 해쉬락 기법의 경우 스푸핑 공격에 대해 안전하지 않다. 스푸핑 공격은 공격자가 태그에게는 리더로 가장하고, 리더에게는 태그로 가장하는 공격 기법으로, 공격자는 메타 ID와 키를 모두 알아낼 수 있다. 스푸핑 공격을 방지하기 위해 태그가 잠금을 풀기 전에 한 번 더 ID를 서버에서 검색하는 방법이 제안되었다. 그러나, 이 방법은 마지막에 보내는 ID가 여전히 식별자의 역할을 수행하기 때문에 사용자에 대한 추적이 가능하다.

Ⅳ. 제안하는 인증방법

1. 키 분배

제안하는 인증 방법은 좀 더 높은 연산능력을 가지는 태그를 위해 설계를 하였다. 제안하는 인증 방법은 좀 더 많은 연산이 가능하므로 랜덤 함수를 추출할 수 있는 기능을 가진 인증 방법을 설계하였다. 랜덤 함수는 리더에서 전송받은 태그의 ID_Number를 기초로 추출하며, 이는 매번 접속할 때 사용하는 토큰키의 일회성 성질을 부여하게 된다. 토큰키 생성과정은 다음과 같은 절차에 의해 이루어진다.

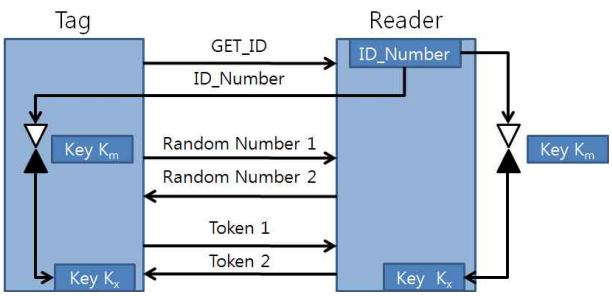

그림 2. 난수 발생 키 분배
Fig. 2. Distribution of Random Number.

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 새로운 키를 생성한다.

⑥ **Token 1**

Token 1 = Ekm(Random Number1 ‖ Tag's ID)

생성된 키를 기반으로 대칭키 암호화 방식을 사용하여 ID와 Random Number1을 암호화하여 리더에 전송한다. 이는 태그와 리더간의 인증과정에서 토큰키로 사용된다.

⑦ **Token 2**

Token 2 =

Ekm(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 인증과정에서 토큰키로 사용된다.

제안하는 인증 방법의 토큰키 생성과정 첫 번째 인증방법의 토큰키 생성과정과 비슷하다. 5번 과정에서 생성되는 키 Km은 분배된 키 Kx와 ID_Number를 쉬프트 연산을 통해 얻어지며 이 키는 외부에 노출되지 않는다. 3번 과정과 4번 과정에서 얻어지는 Random Number는 태그의 ID_Number에서 무작위로 순서에 관계없이 추출되는 방법을 사용하였다. 그리고 6번 과정과 7번 과정에서 생성되는 토큰키는 5번 과정에 생성된 키를 기반으로 암호화 하였으며, 안에 랜덤함수를 첨부하였기 때문에 매번 접속할 때 토큰키가 변하는 성질을 가지게 된다. 공격자가 토큰키를 복사해 그대로 사용하더라도 매번 토큰키가 변하기 때문에 공격자는 통신에 참여를 할 수 없게 된다. 그러므로 인증과정에서 사용되는 해쉬함수도 안전하게 된다.

2. 인증 기법

인증 방법은 첫 번째 제안하는 인증 방법과 같이 2차 해쉬함수를 기반으로 설계하였다. 첫 번째 제안한 인증 방법과 다른 점이 있다면 해쉬함수에 들어가는 변수가 랜덤함수가 들어가므로 매번 인증할 때 사용되는 해쉬함수의 결과 값이 일회성의 성질을 가지고 있다. 그러므로 인증 값을 도중에 가로채서 공격하는 공격방법에도 취약하지 않게 될 것이다.

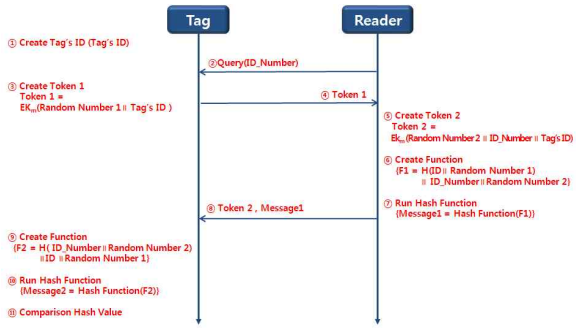

그림 3. 태그와 리더 인증과정
Fig. 3. Tag and Reader's Certification Process.

① **Create Tag Key**(Tag's ID, Random Number1)

태그는 아이디와 Random Number1을 생성한다. 이 과정은 키 분배과정을 통해 이루어진다.

② **Create Token Key**

{Ekm(Random Number1 ‖ Tag's ID}

태그는 리더에 접근을 하기 위한 토큰키를 생성하며 이 과정 또한 키 분배과정에서 생성된 토큰키를 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**

Ekm(Random Number2 ‖ ID_Number ‖ Tag's ID)

리더는 태그에 접근을 하기 위한 토큰키를 생성하며 이 과정 또한 키 분배과정에서 생성되는 토큰키를 사용한다.

⑤ **Create Hash Function**

{f1 = H(Tag's 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's 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 인증이 되며 접근이 가능하게 된다.

V. 실험 및 고찰

제안하는 인증 방법과 기존의 해쉬-락 인증을 재생공격, 서비스 거부 공격, 그리고 도청 공격과 같은 3가지 형태의 공격을 통해 인증 방법의 안정성 측면에서 비교 분석을 한다. 또한 RFID 시스템의 전송 특성상 무선이라는 점을 감안하여 높은 보안성을 가진 인증 방법이라고 해도 전송 효율성이 떨어진다면 사용자 입장에서는 사용을 할 수 없기 때문에 전송 효율성 측면에서도 비교 분석을 하였다.

시뮬레이션은 OPNET 14.5에서 구현하였다. 기본적인 RFID 시스템에서 하였으며, 태그 3개, 유동성 리더 1개, AP 1개, 서버 1개, 그리고 공격자 1개로 구성되었다. 태그는 능-수동방식의 태그를 사용하였으며, 능-수동방식은 능동형 방식과 수동형 방식을 결합해 놓은 하이브리드형 태그이다. 배터리는 내장되어 있으며 이 배터리는 내부적인 프로세싱에 사용된다.

그림 4는 시뮬레이션을 OPENT 14.5에서 구현한 화

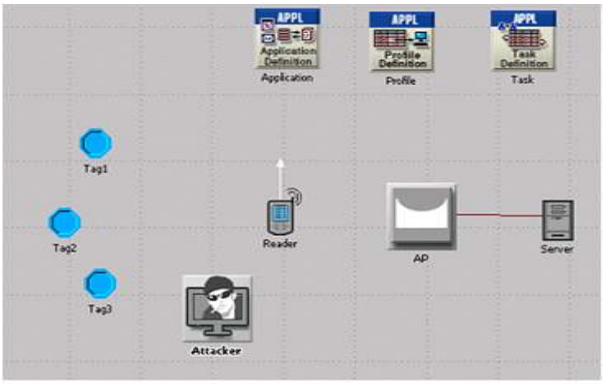

그림 4. 시뮬레이션 환경
Fig. 4. Simulation Environment.

표 1. 시뮬레이션 파라미터
Table 1. Simulation Parameter.

Statistics	Value
Scenario Size	100m X 100m
Transmission Range (Tag → Reader)	< 5 meter
Transmission Range (Reader → Server)	< 100 meter
Tag Transmit Power	0.001W
Reader Transmit Power	0.005W
Tag Type	Semi-passive
Tag Processer	54 bit
Tag Date Rate	1 Mbps
Reader Data Rate	11 Mbps
Simulation Time	1 hour

면이다. 공격자는 태그와 리더간의 통신을 공격하며 이 경우 포핸드 인증 방식이 공격을 받게 된다. 공격방법은 서비스 거부 공격, 도청공격, 재생공격으로 총 3가지의 방법으로 하였다. 서비스 거부 공격은 RFID 시스템을 악의적으로 공격하여 태그와 리더의 자원을 부족하게 하여 원활한 통신을 하지 못하게 하는 공격이다. 리더에게 수많은 접속 신호를 만들어 태그가 정상적으로 접속을 하지 못하게 하거나, 리더의 TCP 연결을 바닥내는 등의 공격을 한다. 공격자가 사용하는 공격방법들 중 도청 공격과 재생 공격의 특성은 거의 똑같다. 도청 공격은 인증되지 않은 리더가 태그에 접근하여 태그의 출력을 얻어 이를 기반으로 태그의 ID와 정보를 획득하는 공격방법이다. 재생공격은 리더와 태그사이의 인증 과정에서도 발생될 수 있는 공격방법으로 통신과정에서 발생하는 신호를 그대로 재생하여 보내는 공격방법이다. 재생 공격과 도청 공격은 리더와 태그사이의 통신을 획득한 정보를 토대로 이루어지는 공격방법이다.

만약 제안하는 인증 방법이 3가지 공격에 취약하다면 공격자 리더나 태그에 전송하는 정보를 처리하게 된다. 이에 따라 리더와 태그가 처리해야하는 정보가 증가하게 되는 현상이 발생하게 되며, 이 현상은 리더와 태그사이에 원활한 통신을 할 수 없게 만들며 그로 인해 응답시간이 지연되게 된다. 또한 공격에 취약한 인증방법일 경우 공격자가 전송한 데이터를 응답하게 되어 태그와 리더가 가진 정보를 공격자에게 전송하게 되는 문제점을 발생하게 될 것이다.

VI. 결과 분석

1. 재생 공격(Replay Attack)에 대한 반응

재생 공격은 첫 번째 제안하는 인증과 같이 리더와 태그사이에 발생하는 통신 정보를 획득하여 그대로 다시 전송하는 공격방법이다. 그림 5에서 재생 공격에 대한 응답을 보면 기존의 해쉬-락 인증 방법은 37[Sec]로 재생 공격에 취약하다는 것을 보여준다. 하지만 두 번째로 제안하는 인증 방법의 응답은 3[Sec]로 재생 공격에 강하다는 것을 보여준다.

다시 정리하면 재생공격에 대한 응답은 기존의 해쉬-락 인증 방법이 37[Sec], 첫 번째 제안하는 인증 방법이 27[Sec], 두 번째 로 제안하는 인증 방법이 3[Sec]이다. 기존의 해쉬-락 인증 방법의 경우 리더와 태그사이에 발생하는 통신 정보는 아무런 암호화 과정도 없고, 이를 다시 전송하더라도 리더나 태그는 공격자라는 것을 확인할 방법이 없다. 그리고 첫 번째로 제안하는 인증 방법은 매번 접속할 때 사용되는 토큰키가 똑같기 때문에 공격자 토큰키를 그대로 재생하여 사용한다면 기존의 해쉬-락 인증 방법과 같이 리더나 태그는 공격자라는 것을 확인할 방법이 없다. 하지만 두 번째로 제안하는 인증 방법은 랜덤함수를 사용한다는 특성을 가지고 있다. 랜덤함수는 매번 접속할 때 사용되는 토큰키가 변한다는 성질을 부여한다. 이는 토큰키가 일회성

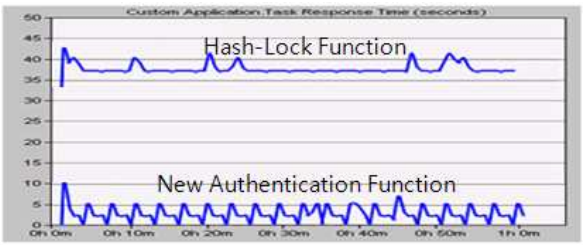

그림 5. 재생 공격에 대한 결과
Fig. 5. Result of Replay Attack.

표 2. 재생 공격에 대한 결과
Table 2. Result of Replay Attack.

	해쉬-락 기법	제안하는 인증기법	차이
응답시간	37Sec	3Sec	34Sec

의 특성을 가지고 있기 때문에 한번 사용된 키는 재생하여 다시 사용할 수 없게 된다. 그러므로 다른 인증방법과 달리 재생 공격에 응답을 하지 않게 되는 장점을 가지고 있다.

2. 서비스 거부 공격(Denial of Service Attack)에 대한 반응

서비스 거부 공격은 첫 번째 제안하는 인증 방법과 같은 공격방법이다. 그림 6에서 서비스 거부 공격에 대한 응답을 보면 기존의 해쉬-락 인증 방법은 37[Sec]로 서비스 거부 공격에 취약하다는 것을 보여준다. 하지만 두 번째로 제안하는 인증 방법의 응답은 3[Sec]로 서비스 거부 공격에 강하다는 것을 보여준다. 이는 두 번째로 제안하는 인증 방법이 첫 번째와 동일하게 토큰키를 사용하기 때문에 토큰키가 없는 공격자가 접근 요청을 하더라도 리더나 태그는 그 요청을 받아들이지 않게 된다. 그러므로 공격자의 접속요청에 의해 태그의 제한적 환경요소는 소모되지 않게 되어 공격에 의한 유지 보수 비용이 증가하지 않게 된다.

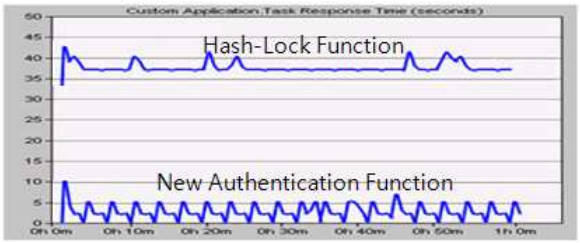

그림 6. 서비스 거부 공격에 대한 결과
Fig. 6. Result of DoS.

표 3. 서비스 거부 공격에 대한 결과
Table 3. Result of DoS.

	해쉬-락 기법	제안하는 인증기법	차이
응답시간	37Sec	3Sec	34Sec

3. 도청 공격(Eavesdropping Attack)에 대한 반응

도청 공격은 첫 번째 제안하는 인증과 같이 리더와 태그사이에서 발생하는 통신 정보를 해석하여 그 정보

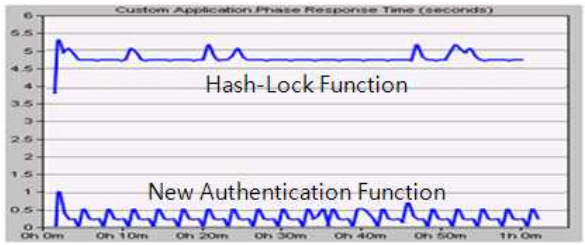

그림 7 도청 공격에 대한 결과
Fig. 7. Result of Eavesdropping Attack.

표 4. 도청 공격에 대한 결과
Table 4 Result of Eavesdropping Attack.

	해쉬-락 기법	제안하는 인증기법	차이
응답시간	4.7Sec	0.2Sec	4.5Sec

를 획득하는 공격방법이다. 도청 공격은 리더와 태그사이의 정보를 습득하는 것으로 시작 한다. 그리고 습득한 정보를 기반으로 태그나 리더로 둔갑하여 네트워크에 참여하는 공격방법이기 때문에 다른 공격방법 보다 응답시간이 짧다. 그림 7에서 기존의 해쉬-락 인증 방법의 재생공격에 대한 응답은 4.7[Sec]이며 이 결과는 도청공격에 취약하다는 것을 보여준다. 하지만 두 번째로 제안하는 인증 방법의 응답은 0.2[Sec]로 도청 공격에 강하다는 것을 보여준다. 두 번째 인증 방법은 첫 번째 인증 방법과 같이 내부에서 생성되는 키를 가지고 암호화한 토큰키를 사용한다. 이 키를 알지 못하는 공격자는 통신 정보를 획득 할 수 없기 때문에 도청 공격에 강하다.

4. 효율성 분석

시뮬레이션에서 통신 환경은 기본적인 RFID시스템 환경이며 공격자가 통신에 간섭하는 가운데 기존의 해

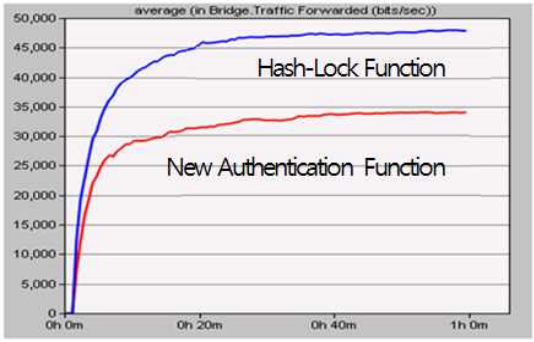

그림 8. 도청 공격 중 태그와 리더 전송량[bits/sec]
Fig. 8. Tag and Reader's Throughput during Eavesdropping Attack.

쉬-락 인증 방법과 제안하는 인증 방법을 사용하여 전송량과 지연시간을 비교하였다.

그림 8은 기존의 해쉬-락 인증 방법과 제안하는 인증 방법의 전송량을 비교한 것이다. 기존의 해쉬-락의 평균 전송량은 45,000[bit/sec]이고, 제안하는 인증 방법은 30,000[bit/sec]로 차이가 15,000[bit/sec]가 나는 것으로 측정되었다.

공격자가 도청공격을 할 경우 기존의 해쉬-락 인증 방법은 공격자를 태그나 리더로 인식하여 공격자가 전송한 정보에 응답을 하기 때문에 리더와 태그 사이의 전송량이 높게 측정되었다. 하지만 기존의 인증방법은 리더나 태그는 공격자가 전송한 정보에 대한 인증이 이루어지지 않았기 때문에 공격자가 리더와 태그사이의 통신에 참여 할 수 없게 된 것이다. 다시 말하면 제안한 인증 방법은 공격자를 제외한 인증을 받은 리더와 태그 사이에 이루어진 통신량이 측정이 된 것이며, 기존의 해쉬-락 인증 방법은 인증을 받은 리더와 태그 그리고 공격자의 통신량이 모두 측정이 된 것이다. 이 차이는 공격자가 통신에 참여를 못하였다는 것을 의미하며, 그 의미는 태그나 리더의 정보 유출을 막았다고 볼 수 있다. 공격자가 보낸 정보를 처리하지 않아 태그와 리더는 원활한 통신을 할 수 있다는 것을 그림 5.9의 지연시간 비교를 통해서도 알 수 있다.

그림 9는 기존의 해쉬-락 인증 방법과 제안하는 인증 방법의 지연시간을 비교한 것이다. 기존의 해쉬-락 인증 방법의 평균 지연시간은 0.009[Sec]이고, 제안하는 인증 방법의 평균 지연시간은 0.006[Sec]이다. 지연시간의 차이가 생기는 이유는 공격 정보를 전송하여 생기는 통신 지연시간으로 기존의 해쉬-락 인증 방법보다 제안하는 인증 방법이 공격에 취약하지 않기 때문에 통신의 지연시간이 감소한 것을 알 수 있다. 또한 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.

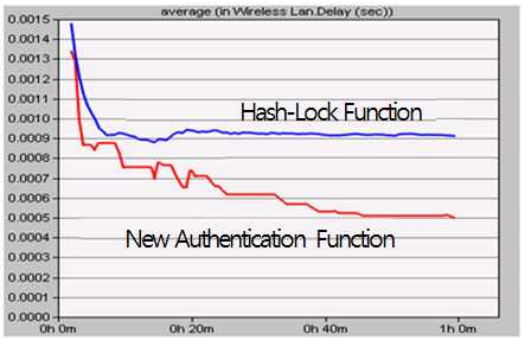

그림 9. 도청 공격 중 태그와 리더간의 지연시간[sec]
Fig. 9. Tag and Reader's Delay during Eavesdropping Attack.

Ⅶ. 결 론

RFID는 매우 유용한 시스템이지만 리더의 제한된 환경적 요소로 인해 보안이 매우 취약하다. 보안적인 문제를 해결하기 위해 해쉬-락 인증 방법이 많이 사용되고 있지만 이 방법은 아이디 및 패스워드 유출이라는 문제점을 가지고 있다. 그래서 본 논문에서는 해쉬-락 인증 방법을 변형시킨 인증 방법을 제안하고 있다.

본 논문에서는 제안하는 인증 방법의 특성 분석을 통해 다음과 같은 결론을 얻었다.

- 키 분배를 통해 새로운 키를 얻어내는 과정을 추가하여 키 유출을 막았으며, 난수를 이용하여 토큰키의 일회성 성질을 부여하였다.
- 2차 해쉬함수 연산을 통해 보다 안정적인 해쉬 인증 방법을 구현하였으며, 해쉬함수에 들어가는 정수는 매번 달라져 패턴인식 공격에 강한 방어력을 가진다.
- 기존의 해쉬 함수에 비해 적은 핸드쉐이크 과정으로 외부 유출을 최소화 하였다.
- 서비스 거부 공격, 도청 공격, 재생 공격에 강한 방어력을 가진다.
- 랜덤 함수 알고리즘으로 인해 기존의 저가형 태그보다 더 많은 연산능력이 필요한 태그에만 적용이 가능하다.

앞으로 연구되어야 할 방향은 모든 공격에 강한 방어력을 가진 저가형 태그를 위한 인증 방법이 연구되어야 할 것이다. 이는 제한된 환경에서 보다 우수한 인증 및 암호화를 통해 강한 보안성을 지니는 보안 기술이 매우 절실히 필요로 하는 연구 분야이다. 이 기술이 연구되어 발전되어진다면 기존의 인터페이스를 그대로 사용하면서 강한 보안성을 지닌 물류 시스템의 구축이 가능해질 것이다. 또한 다른 연구 방향은 태그의 제한된 환경

요소의 확장이다. 지금 현재 사용 중인 저가형 태그보다 더 많은 연산 능력과 저장 능력이 가능한 태그가 개발이 되어 같은 가격에 시장에 나온다면 물류 시스템에서 RFID 기술을 사용하는 시점을 앞당길 수 있으리라 예상한다.

현재 RFID 기술의 사용은 미미하다. 하지만 앞으로 소프트웨어적으로나 하드웨어적으로 더욱 연구되어 나간다면 RFID 기술은 우리 일상생활에서 없어서는 안되는 기술이 될 것이다. 또한 RFID 기술이 발전해 나가면서 보안적인 기술도 같이 접목하여 나가야 할 것이다.

참 고 문 헌

[1] 나종민, “트리-워킹 방식 기반의 RFID 시스템 스푸핑 방어 알고리즘.”, 광운대학교 대학원 컴퓨터과학과, 2007.

[2] Miyako Ohkudo. Koutatou Suzuki and Shingo Kinoshita, “Cryptographic Approach to Privacy-Friendly Tags.”, Submitted 2003.

[3] CRYPTOREC reports, published 2002 in Japen

[4] David J. Wheeler and Robert M. Needham. TEA, a Tiny Encryption Algorithm. Technical report. Computer Laboratory. University of Cambridge. 1995.

[5] NTRU. GenuID. http://www.ntru.com/products,com

[6] 주학수, “RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석”, 전자정보센터 IT리포트

[7] ISO 18185-4, “Freight containers - Identification and Communication, Electronic seals - part 4: Data Protection”, ISO Working Draft, 2004.

[8] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호 기술.”, *한국정보보호학회 학회지 제 14권 6호*, pp.28-36, 2004.

[9] Ari Juels and Ravikanth Pappu, “Squealing Euros; Privacy Protection in RFID Enalbed Banknotes”, Financial Cryptography 2003 Springer Verlag 2003.

[10] Juels, A et al. “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy”, *10th ACM Conference on Computer and Communication Security*, 2003.

[11] 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.

[12] 박규진, 한경헌, 성종엽, 유도경, 최동유, 한승조. “RFID Tag의 인증을 통한 보안성 향상”, *정보보호학회 하계학술대회*, 2009.

[13] 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.

[14] 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.

[15] K. Yuksel, “Universal Hashing for Ultra-Low-Power Cryptograaphic Hardware Applications”, Master's Thesis, Dept, of Electroniacal Engineering, WPI, 2004.

저 자 소 개

나 영 남(정회원)

1991년 조선대학교 전자계산학과 학사 졸업(이학사)
1993년 조선대학교 전자계산학과 석사 졸업(이학석사)
1998년 조선대학교 전산통계학과 박사 졸업(이학박사)
1998년 3월~ 현재 : 조선이공대학 교수
<주관심분야 : RFID/USN, 인공지능, 네트워크>

한 재 균(정회원)-교신저자

1997년 한국방송통신대학교 정보통계학과 학사 졸업(이학사).
1999년 조선대학교 전자공학과 석사 졸업(공학석사).
2005년 조선대학교 전자공학과 박사 졸업(공학박사).
<주관심분야 : RFID/USN, 네트워크, 보안>