Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.10.1145

비선형 Tent-Map을 이용한 RFID 인증 프로토콜 설계

한규광* · 임거수**

Design of an RFID Authentication Protocol Using Nonlinear Tent-Map

Kyu-Kwang Han* · Geo-Su Yim**

요 약

RFID(Radio-Frequency IDentification)시스템은 무선으로 사물을 식별하는 기술로 물류, 운송, 유통, 재고관리 등과 같은 물품관리를 획기적으로 개선할 수 있는 새로운 방법이다. 그러나 무선을 사용하고 있는 RFID는 통신구간에 대한 보안의 취약성 때문에 정보 누출 및 변조 같은 위험성을 가지고 있다. 우리는 이런 RFID 통신 시스템에 복잡계의 대표적인 계인 Tent-Map을 적용하여 새로운 인증 프로토콜을 설계하였다. 복잡계의 대표적인 특징인 초기치 민감성과 불규칙성을 RFID의 Reader 와 Tag에 적용하여 보다 견고하고 간략한 인증 시스템을 설계하였다. 본 논문에서 보인 복잡계를 이용한 RFID 인증 프로토콜 설계는 기존의 Hash 함수나 난수에 의존되었던 인증 시스템에 차별화된 새로운 방법으로 그 활용성을 검증하는데 그 목적이 있다.

ABSTRACT

The RFID (Radio-Frequency Identification) system is a technology to discern things by radio and an epoch-making new method to improve product management such as distribution, transport, mobilization, inventory control. However, RFID, which uses radio, is at risk for information leakage and falsification due to the vulnerability of security of the communication section. We designed the new authentication protocol by applying the tent map, which is the representative complex systems, to the RFID communication system. A more solid and simple authentication system was designed by applying the initial value sensitivity and irregularity, which are the representative characteristics of the complex system, to the reader and tag of RFID. The purpose of this paper is to verify the usability of the RFID authentication protocol design that uses the nonlinear system shown in this thesis by the new system differentiated from the authentication system that depends on the existing hash function or random numbers.

키워드

Encryption, RFID, Decryption, Secure Channel, Chaos, Pseudorandom Number
RFID, 암호화, 복호화, 보안채널, 혼돈, 유사난수

Ⅰ. 서 론

RFID(Radio Frequency IDentification)통신 시스템은 USN(Ubiquitous Sensor-Network) 환경 구축에 있어서 가장 중요한 기술이라 할 수 있다[1-2]. RFID 시스템은 기존의 바코드 시스템과 같은 접촉성의 문제를 해결한 무선 통신 인증 시스템으로 환경 요인에 제약을 받던 바코드와 달리 온도, 습도, 먼지 등에 관

* 배재대학교 전기공학과(khan@pcu.ac.kr)
** 교신저자(corresponding author) : 배재대학교 전기공학과(lomac@pcu.ac.kr)
접수일자 : 2014. 08. 29 심사(수정)일자 : 2014. 09. 25 게재확정일자 : 2014. 10. 17

계없이 인증할 수 있는 장점을 가지고 있다. 또한 무선 통신 방식을 사용하고 있어 동시에 여러 사물을 인증할 수 있는 특징을 가지고 있다. 현재 국내에서는 출입 카드, 보안 카드, 버스 카드 등에 이미 사용되고 있고 점차 물류유통과 자재관리 그리고 의료분야에서도 많은 연구가 이루어지고 있는 추세이다[3-4].

RFID 시스템은 무선채널을 사용하기 때문에 많은 연구자들의 관심의 대상이 되는 것이 보안에 대한 문제이다[5-6]. 기존의 다른 시스템들과 달리 RFID 시스템에서 사물에 부착되어 인증을 받는 Tag의 제약적인 개발 환경이 효율적인 암호화 방법의 적용에 있어서 가장 큰 문제점으로 대두되고 있다. 우리는 이런 20,000게이트 미만의 국한적인 개발 환경에 적용할 수 있는 보안방법을 기존의 해쉬-함수가 아닌 복잡계를 이용한 방법으로 제안하려 한다[7-9]. 복잡계는 자체적으로 비선형성을 가지고 있어 유사 난수를 발생하는 불규칙성과 초깃값에 민감한 결과를 보이는 특성을 가지고 있다[10-12]. 이런 복잡계의 특징을 RFID의 통신에서 Reader와 Tag 사이의 보안 인증 방법으로 사용하면 보다 효과적인 결과를 얻을 수 있을 것이다[13-15]. 또한 복잡계는 비교적 간단한 수식으로 구성되어 있기 때문에 하드웨어 구현 시 적은 게이트가 소요되므로 해쉬-함수 보다 효과적인 결과를 얻을 수 있을 것으로 예측된다.

II. 기존의 RFID 인증 프로토콜

RFID 인증 프로토콜의 대표적인 구현 방법은 해쉬-함수를 사용하는 방법이다. 이 방법은 Hash-Lock 방법이 알려지면서 많은 연구가 이루어지고 있고 현재도 관련된 새로운 방법들이 발표되고 있다. 구조적으로 해쉬-함수는 역함수가 존재하지 않는 단 방향성의 특징을 가지고 있어 특정 데이터의 위조 유무를 검증하는 용도로 사용되고 있다. RFID 분야에서도 인증을 위한 데이터 통신에 해쉬-함수를 사용하여 외부 공격으로부터 안전하게 시스템을 유지하고 있는 것이다. 이런 해쉬-함수 기반 방법으로는 HLP, RHLP, HCP 등이 있고 그 내용을 다음에 보인다.

2.1. 해쉬-락 인증 프로토콜

전 방향성을 갖는 해쉬-함수를 이용한 인증 방법으로 2003년 S. A. Weis 등에 의해 제안되었다[16]. Server 와 Reader 그리고 Tag의 데이터 흐름을 그림 1에 보인다. Tag 의 ID 값을 보호하기 위해 랜덤하게 선택된 Key를 해쉬-함수로 계산한 값을 metaID를 통해 Reader에게 전송하여 인증을 획득한 후 안전하게 ID를 전송하는 프로토콜이다. 그러나 고정된 metaID 값을 공격자가 무단 획득하여 Reader에게 전송하면 공격자를 Tag로 오인하고 Key 값을 전달하는 문제점을 가지고 있다.

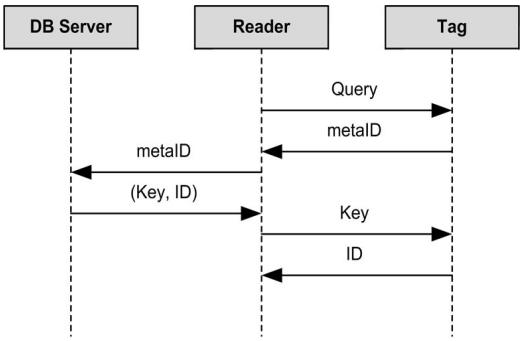

그림 1. 해쉬-락 인증 프로토콜
Fig. 1 HLP(Hash-Lock Protocol)

2.2. 랜덤 해쉬-락 인증 프로토콜

해쉬 락 인증 프로토콜의 고정된 metaID 유출에 따른 문제점을 해결하기 위한 방법으로 랜덤 해시 락 인증 프로토콜이 제안되었고, 그 내용을 그림 2에 보인다[17].

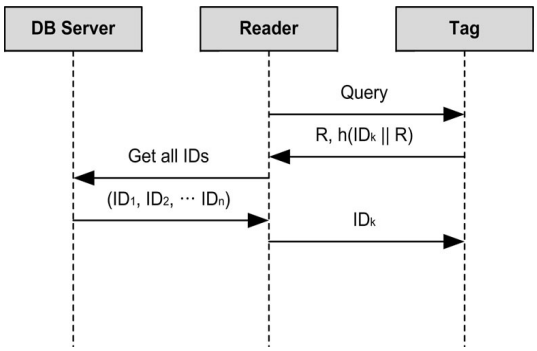

그림 2. 랜덤 해쉬-락 인증 프로토콜
Fig. 2 RHLP(Randomized Hash-Lock Protocol)

이 방법은 Reader의 요구에 따른 고정된 Tag의 응답을 난수를 사용하여 다르게 하여 metaID 유출에 따른 문제점을 해결하였다. 그러나 마지막 단계에서 ID_k 값이 안전하지 않은 채널로 전송되기 때문에 재전송 공격이나 스푸핑 공격이 있을 경우 ID_k 값이 유출될 가능성이 있다. 그리고 m개의 Tag가 있을 경우 해당되는 Tag를 찾기 위해 $m/2$ 의 해쉬 연산과 데이터베이스 검색이 필요하여 많은 시간과 연산량이 필요하게 되어 서비스 거부 공격에 취약하게 된다.

2.3. 해쉬-체인 인증 프로토콜

2004년 Ohkubo 등은 위치 추적 공격과 전 방향 안전성에 강한 해쉬 체인 인증 프로토콜을 그림 3과 같이 제안하였다[14]. 이 방법은 두 개의 해쉬-함수 $H(s_i)$와 $G(s_i)$를 사용하여 체인 형태로 구성하는 방식으로 H 해쉬-함수는 Tag 의 Key 값을 변화 시키는 역할을 하고 G 해쉬-함수는 통신에 사용되는 데이터를 암호화하는 역할을 한다. 이 방법은 위치 추적과 재전송 공격에는 강하지만 공격자가 Tag에게 Query를 보내면 H 해쉬-함수의 계산으로 Tag는 s_{i+1} 값으로 변경되지만 Reader는 s_i 값을 유지하고 있기 때문에 동기화가 되지 않아 서비스 거부 공격에 취약하게 된다.

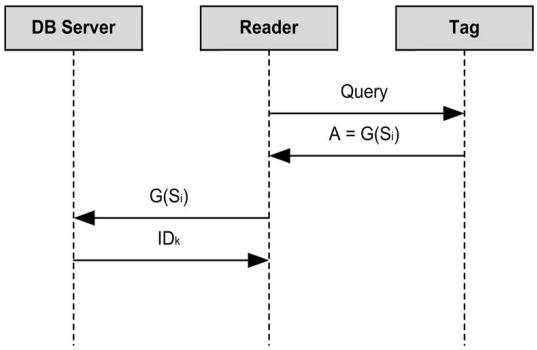

그림 3. 해쉬-체인 인증 프로토콜
Fig. 3 HCP(Hash-Chain Protocol)

기존의 해쉬-함수를 이용한 인증 방법은 구현은 용이하지만 취약한 보안 문제를 해결하기 위해서는 해쉬-함수를 중복 사용해야 하므로 시간과 자원의 효율성에 대한 문제점을 가지고 있다. 특히, SHA 계열의 해쉬-함수를 하드웨어로 구현하면 20,000개 이상의 게이트가 소요되므로 소형의 수동형 Tag에는 적합하지 않은 구현 방법이다. 우리는 이런 소형화의 문제점을 해결하기 위해 해쉬-함수와 유사한 기능을 수행할 수 있는 비교적 간단한 수식의 복잡계를 구성하고, 복잡계의 신호를 RFID 통신에 적용하여 그 결과를 보인다.

III. 제안 프로토콜

본 장에서는 암호화 방법의 새로운 연구 분야로 자리매김하고 있는 복잡계의 특징을 알아보고, 이 시스템을 RFID 통신 체계에 적용한 인증 프로토콜을 제안한다. 복잡계의 가장 큰 특징으로는 초기치 민감성과 불규칙성이 있다. 초기치 민감성은 작은 초기 값의 차이가 이후 서로 다른 결과 값으로 발산하는 특징으로 통신 체계의 킷값으로 사용하기 용이하고, 불규칙성은 출력 값이 난수와 유사하여 시스템을 알지 못하면 예측은 불가능하지만 재생산은 가능한 특징을 가지고 있어 통신의 시퀀스에 적용하면 스푸핑, 재전송, 서비스 거부 등의 공격에 대한 안전한 통신 체계 구축에 효율적이다.

3.1. 혼돈계 Tent-Map의 특성

비선형 복잡계에서 로지스틱-맵과 함께 가장 많이 알려진 맵이 텐트-맵이다[18]. 텐트-맵은 식 (1)에서 보인 바와 같이 간단한 수식으로 구성되어 있어 RFID Tag 와 같은 제약적인 개발 환경에서 효과적인 결과를 얻을 수 있다. 본 연구에서 텐트-맵을 선택한 이유도 이런 특징 때문이다.

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1-x_n) & \text{for } \frac{1}{2} \le x_n \end{cases} \quad (1)$$

기존의 텐트-맵을 RFID 통신 체계에 보다 효과적으로 적용하기 위해 식 (2) 와 같이 맵을 변형하였다. 외부의 공격에 강한 텐트-맵을 구성하기 위해 매개변수를 μ에서 $\mu_{[1..4]}$로 그리고 구간 값을 $r_{[1..4]}$로 구성하여 이 값들을 통신체계의 킷값으로 사용할 수 있게 하였다.

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu_1 x_n & \text{for } 0 < x_n \le r_1 \\ \mu_2 x_n & \text{for } r_1 < x_n \le r_2 \\ \mu_3 (1-x_n) & \text{for } r_2 < x_n \le r_3 \\ \mu_4 (1-x_n) & \text{for } r_3 < x_n \le r_4 \end{cases} \quad (2)$$

식(2)의 변형된 텐트-맵에서 $\mu_1 = 1.60$, $\mu_2 = 1.90$, $\mu_2 = 1.80$, $\mu_4 = 1.50$ 으로 설정하고, $r_1 = 0.20$, $r_2 = 0.50$, $r_3 = 0.80$ 그리고 $r_4 = 1.0$으로 설정하여 계산된 결과 값의 시계열을 그림 4에 보인다.

그림 4에 보이는 (a), (b), (c)는 각각 μ_2값을 1.95, μ_3값을 1.85, μ_4값을 1.55로 변경하여 계산된 시계열이다. (a), (b), (c) 모두 같은 초기 값으로 계산된 결과 값이지만 초기치 민감성으로 이후 값이 상이 하게 발산하는 것을 확인할 수 있고, 불규칙성 때문에 결과 값 또한 난수와 유사함을 확인할 수 있다.

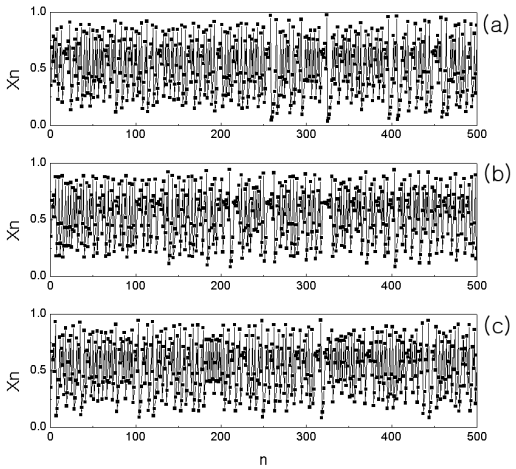

그림 4. 텐트-맵의 시계열 계산 값
그림 (a)는 μ_2=1.95, (b)는 μ_3=1.85, (c)는 μ_4=1.55
Fig. 4 Temporal behavior of Tent-Map
(a) μ_2=1.95, (b) μ_3=1.85, (c) μ_4=1.55

그림 4에 보인 결과 값을 RFID 통신 체계에 적용하기 위해 32비트 디지털 신호로 변화시킨 코드 값을 표 1에 보인다. 계산된 결과 값 x_{n+1}은 x_n과 $\mu_{[1..4]}$그리고 $r_{[1..4]}$ 에 의해 계산된 값으로 제시된 9개의 변수 값이 없으면 계산이 불가능하고, 특정 코드 값에 작은 변화를 주어 통신체계를 예측하려 시도 또한 초기치 민감성으로 계산 값이 즉시 발산해 버려 예측이 불가하게 된다.

표 1. 텐트-맵의 32비트 16진수 계산 값
Table 1. 32-Bit Hexadecimal value of Tent-Map

x_n	$\mu_1 = 1.60, \mu_2 = 1.90, \mu_3 = 1.80, \mu_4 = 1.50$			
	$\mu_1 \leftarrow 1.65$	$\mu_2 \leftarrow 1.95$	$\mu_3 \leftarrow 1.85$	$\mu_4 \leftarrow 1.55$
x_{n+0}	35C28F5C	35C28F5C	35C28F5C	35C28F5C
x_{n+1}	58B43958	56041893	56041893	56041893
x_{n+2}	ACF9096C	AB2BFDB5	A36E2EB2	A36E2EB2
	…	…	…	…
x_{n+10}	F3E97BEA	1F5DA8D8	74810D56	1A6DEDD7

3.2. 가정 사항 및 표기법

본 장에서는 텐트-맵을 이용한 RFID 인증 프로토콜 방법에 대한 제안에 있어서 가정 사항과 표기법을 나타낸다. 제안된 방법에 대한 표기법은 다음과 같다.

- M_{ID} 시스템의 비밀 식별값 (Marchant ID)
- T_{ID} Tag 의 비밀 식별값 (Tag ID)
- $nFun$ 텐트-맵 함수
- C 텐트-맵의 매개변수 값 (9개중 한 개)
- X_n 텐트-맵의 초기값
- R_C $C \oplus M_{ID}$
- R_X $X_n \oplus M_{ID}$
- K_n Tag 에서 계산된 n 번째 결과 값
- K_{n+1} Tag 에서 계산된 $n+1$ 번째 결과 값

제안된 인증방법은 다음과 같은 가정 사항을 갖는다.

① Server와 Reader 사이는 안전한 유선 통신 채널을 이용하고 있다고 가정한다.
② Reader와 Tag 사이는 무선 통신 채널을 사용하고 있고, 공격자의 공격에 노출되어 있다.
③ Reader와 Tag는 제시된 텐트-맵의 수식을 계산할 수 있는 기본 연산자를 포함하고 있다.
④ Reader는 난수를 계산할 수 있다.
⑤ Reader와 Tag는 필드에 적용 시 시스템(상점) 비밀 값 M_{ID} 값을 공유한다.
⑥ Reader와 Tag는 텐트-맵의 결과 값을 발산시

키기 위한 계산 반복 횟수 n 값을 공유한다.

3.3. Tent-Map을 이용한 RFID 인증 프로토콜

효율적인 RFID 통신체계를 제안하기 위해 본 논문에서는 변형된 텐트-맵을 구성하고 맵의 특징을 앞에서 보였다. 텐트-맵의 초기치 민감성과 불규칙성을 이용한 RFID 인증 프로토콜을 그림 5와 같이 제안하고 그 흐름을 아래에 보인다.

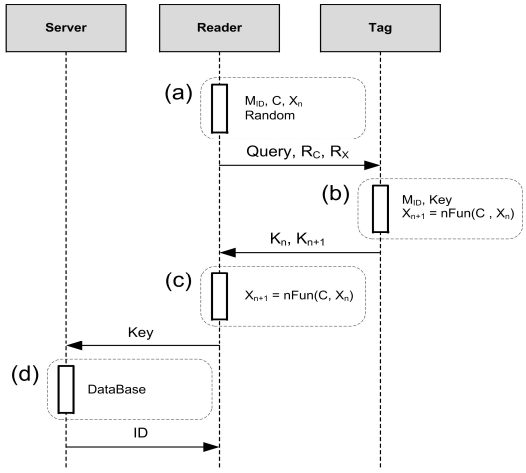

그림 5. 제안한 프로토콜의 인증 과정
Fig 5. Authentication process of suggested protocol

단계 (a). Reader는 난수 생성기를 이용하여 텐트-맵에 사용될 매개변수 C와 초깃값 X_n을 생성한다. 공유된 상점 ID 값 M_{ID}로 $R_C = C \oplus M_{ID}$, $R_X = X_n \oplus M_{ID}$를 계산하여 $Query$와 같이 Tag에 전송한다.

단계 (b). 전송 받은 값과 공유된 M_{ID}값으로 $C = R_C \oplus M_{ID}$, $X_n = R_X \oplus M_{ID}$를 계산하고, 그 결과 값으로 $X_{n+1} = nFun(C, X_n)$ 을 Reader와 공유된 값으로 n번 수행한다. 계산된 X_{n+1}값으로 $K_n = Key \oplus X_{n+1}$ 과 $K_{n+1} = nFun(C, K_n)$ 을 계산하고 K_n과 K_{n+1}을 Reader에게 전송 한다. 재전송 공격에 대한 보안 강도를 높이기 위해 전송되는 값을 K_n, K_{n+1}, ... , K_{n+i}으로 증가시키는 방법도 고려할 수 있다.

단계 (c). Reader는 전송 받은 K_n과 K_{n+1}값을 $K_{n+1} = nFun(C, K_n)$로 계산하여 전송 받은 값이 유효 한지 검증한다. 전송된 값이 검증 되면 $X_{n+1} = nFun(C, X_n)$ 을 발산을 위해 Tag 와 공유된 값으로 n번 수행하여 계산된 값으로 $Key = X_{n+1} \oplus K_n$ 을 계산하여 데이터베이스 Server에 전송한다.

단계 (d). 데이터베이스 Server는 전송 받은 값으로 질의하여 및 관련 정보를 Reader에 전송하여 이후 시퀀스가 이루어지도록 한다.

Ⅳ. 비교 분석

본 장에서는 텐트-맵을 이용한 RFID 통신체계와 기존의 방법들에 대한 보안성 및 효율성을 비교 분석하고 그 결과를 표 2에 보인다.

4.1. 도청 공격

Reader와 Tag는 공격자의 공격에 노출되어 있는 무선 채널을 사용하고 있다. 그러므로 RFID 시스템은 도청 공격에 대한 대응책을 가지고 있어야 한다. 본 논문에서 제시된 RFID 통신체계는 복잡계의 결과 값을 통신 데이터로 사용하기 때문에 기존의 해쉬-락 인증 프로토콜 방법과 달리 획득된 데이터는 난수와 유사하여 추후 공격의 자료로 사용될 수 없다.

4.2. 위치 추적

RFID시스템의 위치 추적은 초기 통신 단계에서 Reader에서 전송된 Query에 대한 Tag 의 응답이 고정된 값이라는 단점을 이용하여 Tag의 위치를 추적하는 공격 방법으로 해쉬-락 인증 프로토콜의 취약한 문제점이다. 우리가 앞에서 제시한 복잡계를 이용한 통신체계는 Query에 대한 응답이 복잡계의 결과 값과 XOR 하여 전송되고, 복잡계의 계산 값 또한 매번 다른 값이 전송되기 때문에 위치 추적을 할 수 없게 된다.

4.3. 스푸핑 공격

스푸핑 공격은 공격자가 Reader 와 Tag 사이에 전송되는 데이터를 무단 획득하여 인증된 장치처럼 통신에 참여하는 형태로 매우 위험한 공격 방법이다. 그

러나 우리가 제시한 통신체계는 매번 난수를 텐트-맵의 초기 값과 매개변수로 사용하기 때문에 어느 시점이든 중간에 획득한 데이터를 이용해서 인증된 장치로 통신에 참여할 수 없게 된다.

4.4. 재전송 공격

도청 공격으로 무단 획득한 통신 데이터를 이용하여 이후 같은 데이터가 통신될 때 미리 획득한 데이터를 사용하는 공격 방법으로 통신 데이터가 확률적으로 특정 값에 편중되어 있으면 위험 대상이 될 수 있는 공격 방법이다. 본 논문에서 제시한 텐트-맵을 이용한 통신방법은 계의 복잡성을 이용하고 K_n과 K_{n+i}의 연관된 데이터를 사용하기 때문에 도청 공격으로 유출된 통신 데이터가 반복되어 통신에 사용될 가능성이 극히 희박하여 재전송 공격이 이루어질 수 없게 된다.

4.5. 서비스 거부 공격

서비스 거부 공격은 데이터의 유출보다는 시스템을 마비시키는 공격으로 기존의 RFID 인증 프로토콜은 Tag 인증 시에 Reader 가 데이터베이스에 존재하는 모든 Key을 검색하는 방식으로 처리된다. 기존의 해쉬함수 관련 인증 프로토콜은 이때 전송되는 Tag ID에 대한 1차 검증이 이루어지지 않으면 요구 시 매번 검색해야 하므로 많은 시간과 연산량이 요구되어 치명적이 공격이 될 수 있다. 본 논문에서 제시한 비선형 텐트-맵을 이용한 인증 프로토콜은 Reader가 Tag에서 전송된 K_n, K_{n+1}을 1차 검증하기 때문에 서비스 거부 공격으로부터 안전하고 모든 Key 값을 검색하는 기존 방법과 달리 Reader 에서 Key 값을 계산하여 데이터베이스 서버에 질의하는 방식으로 구성되어 있어 보다 효율적이다.

표 2. 제안된 프로토콜의 효율성 비교
Table 2. Effectiveness comparison of proposed protocol

Attack \ Protocols	Hash-Lock Protocol	Random Hash-Lock Protocol	Hash-Chain Protocol	Proposed Protocol
Eavesdropping	×	×	○	○
Location Tracking	×	○	○	○
Spoofing	×	×	×	○
Replay	×	×	○	○
Dos	×	×	×	○

○: Safety, ×:Defect

V. 결 론

유비쿼터스 환경 구축에 있어서 가장 중요한 기술인 RFID는 그 효율성뿐만 아니라 보안의 취약성 때문에 많은 연구자들의 화두에 오르내리고 있다. 기존 RFID 인증 프로토콜에 대한 문제점을 II. 관련 연구에서 알아보고 문제점을 보완한 새로운 인증 프로토콜을 III. 제안 프로토콜에서 제안하였다. 우리가 제안한 인증 프로토콜은 유사 난수를 발생하는 복잡계를 사용하는 방법으로, Tag 의 제한적인 자원을 고려하여 수식이 비교적 간단한 텐트-맵을 사용하였다. RFID의 확장성을 고려하여 매개변수를 사용 할 수 있게 텐트-맵을 변형하였고, 그 시스템을 식 2.에 보였다. 본 논문에서 제안한 인증 프로토콜은 복잡계의 초기치 민감성과 불규칙성을 이용한 방법으로 대표적인 특징으로는 Tag에서 Reader로 전송되는 K_n, K_{n+1}값이 $K_{n+1} = nFun(C, K_n)$ 에 의한 계산으로 값이 유효한지 확인이 가능하므로 외부에서 무단 변조된 값에 대한 차제 검증이 가능하다는 것이다. 그리고 Reader 와 Tag에 구현된 텐트-맵이 서로 동기화되어 있어 Tag에서 유사 난수로 암호화된 Key 값을 Reader에서 복호화 하여 데이터베이스에 질의가 가능하기 때문에 기존 방식의 모든 Key 값을 질의하는 방법에 비해 시간과 자원을 절약할 수 있다는 장점이 있다. 우리가 제시한 복잡계를 이용한 방법은 아직 초기 단계이고 연구 과정에 머물러 있지만 보다 많은 연구와 구현이 이루어진다면 보안의 취약성으로 문제가 되고 있는 RFID 상호 인증 시스템에 있어서 새로운 방법으로 모색될 수 있을 것으로 생각된다.

참고 문헌

[1] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing," *Communications of the*

ACM, vol. 36, no. 7, 1993, pp. 75-84.

[2] K. Kim, K. Ban, S. Heo, and E. Kim, "Design and Implementation of System for Sensing Data Collection in RFID/USN," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 5, no. 2, 2010, pp. 221-226.

[3] J.-H. Shin and S.-S. Hwang, "Design of RFID Packaging for Construction Materials," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 8, no, 6, 2013, pp. 923-932.

[4] W.-S. Ryu, "A Simulation Technique for RFID Adoption in Hospital," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 1, 2014, pp. 61-66.

[5] A. Juels, "Strengthening EPC Tags Against Cloning," *ACM Workshop on Wireless Security*, Cologne, Germany, Sept. 2005, pp. 67-76.

[6] S.-J. Oh, K.-H. Chung, T.-J. Yun, and K.-S. Ahn, "An RFID Mutual Authentication Protocol Using One-Time Random Number," *The J. of Korea Information of Communications and Information Sciences*, vol. 36, no. 7, 2011, pp. 858-867.

[7] M. S. Masuda, "New Approach to Chaotic Encryption," *Physics Letters A*, vol. 263, 1999, pp. 373-375.

[8] J. Cheng and J.-I. Guo "A new chaotic key-based design for image encryption and decryption," *The 2000 IEEE Int. Symp. on Circuits and Systems*, Geneva, Switzerland, May 2000, pp. 49-52.

[9] H. E. Ahmed, H. M. Kalash, and O. S. Farag Allah, "An Efficient Chaos-Based Feedbacks Stream Cipher (ECBFSC) for Image Encryption and Decryption," *Informatica*, vol. 31, 2007, pp. 121-129.

[10] A. H. Nayfeh and B. Balachandran, *Applied Nonlinear Dynamics*, Toronto: Wiley-Interscience, 1995.

[11] R. H. Abraham, and C. D. Shaw, *Dynamics - The Geometry of Behavior*. California: Addison-Wesley, 1992.

[12] G. P. Williams, *Chaos Theory Tamed*. London: Taylor & Francis, 1997.

[13] G.-S. Yim and H.-S. Kim, "Chaos-based Image Encryption Scheme using Noise-induced Synchronization," *J. of the Korea Society of Computer and Information*, vol. 13, no. 5, 2008, pp. 155-162.

[14] G.-S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System," *Korea Information Assurance Society*, 2008, vol 8. no. 3, pp. 57-64.

[15] H.-S. Kim and G.-S. Yim, "Design of a digital photo frame for close-range security using the chaotic signals synchronization," *J. of the Korea Society of Computer and Information*, vol. 16, no. 2, 2011, pp. 201-206.

[16] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identifications Systems," *Int. Conf. on Security in Pervasive Computing*, Boppard, Germany, Mar. 2003.

[17] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Enhanced Hash Chain based Scheme for Security and Privacy in RFID Systems," *Int. J. of computer Applications*, vol. 28, no. 9, 2004, pp. 719-724.

[18] H. G. Schuster, *Deterministic Chaos an Introduction 2nd*, Weinheim: VCH, 1988.

저자 소개

한규광(Kyu-Kwang Han)

1983년 서울대학교 대학원 물리학과 졸업(이학석사)

1989년 미국 Univ. of Missouri Rolla 물리학과 졸업(이학박사)

1992년~현재 배재대학교 전기공학과 교수

※ 관심분야 : 시계열분석, 병렬컴퓨팅, 분자동역학

임거수(Geo-Su Yim)

1998년 배재대학교 대학원 물리학과 졸업(이학석사)
2004년 서강대학교 대학원 물리학과 졸업(이학박사)
2008년~현재 배재대학교 전기공학과 교수
※ 관심분야 : 시계열분석, 신호처리, 빅데이타 분석, FPGA 비전 제어