한국정보전자통신기술학회논문지(jkiiect)'20-10, Vol.13 No.5
논문 20-13-05-425 http://dx.doi.org/10.17661/jkiiect.2020.13.5.425

2차원 Tent-map을 이용한 RFID 인증 프로토콜 설계

임거수*

Design of RFID Authentication Protocol Using 2D Tent-map

Geo-su Yim*

요 약 산업과 기술이 고도화되면서 물류의 운송, 관리, 유통이 대량화되었고 이런 대량의 물류 정보를 효율적으로 관리하기 위해 RFID(Radio-Frequency Identification) 기술이 개발되었다. 관리를 목적으로 하는 RFID는 물류 산업뿐만 아니라 전력전송 및 에너지관리 분야까지 산업 전반에 응용되고 있는 상태이다. 그러나 RFID 장치는 프로그램 개발 용량의 제한으로 개발에 제약을 받고 있고, 이런 제약은 기존의 강인한 암호화 방법을 사용할 수 없어서 보안에 취약함을 가지고 있다. 우리는 이런 RFID의 제약적인 환경에 적용하기 쉬운 단순 연산으로 구현할 수 있는 보안용 혼돈 시스템을 설계하였다. 설계된 시스템은 2차원 Tent-map 혼돈 시스템으로 혼돈계의 매개변수에 따른 신호의 편중 분포 문제점을 해결하기 위해 암호용 매개변수(μ_1)와 분포용 매개변수(μ_2)그리고 키값으로 사용될 수 있는 상점 ID 값을 매개변수(θ)로 하는 시스템이다. 설계된 RFID 인증 시스템은 난수와 유사하며 초기값으로 재생산이 가능한 혼돈 신호의 특성이 있고 매개변수에 대한 편중 분포 문제를 해결하였기 때문에 기존의 혼돈 시스템을 이용한 암호화 방법보다 효과적이라고 할 수 있다.

Abstract Recent advancements in industries and technologies have resulted in an increase in the volume of transportation, management, and distribution of logistics. Radio-frequency identification (RFID) technologies have been developed to efficiently manage such a large amount of logistics information. The use of RFID for management is being applied not only to the logistics industry, but also to the power transmission and energy management field. However, due to the limitation of program development capacity, the RFID device is limited in development, and this limitation is vulnerable to security because the existing strong encryption method cannot be used. For this reason, we designed a chaotic system for security with simple operations that are easy to apply to such a restricted environment of RFID. The designed system is a two-dimensional tent map chaotic system. In order to solve the problem of a biased distribution of signals according to the parameters of the chaotic dynamical system, the system has a cryptographic parameter(μ_1), a distribution parameter(μ_2), and a parameter(θ), which is the constant point, ID value, that can be used as a key value. The designed RFID authentication system is similar to random numbers, and it has the characteristics of chaotic signals that can be reproduced with initial values. It can also solve the problem of a biased distribution of parameters, so it is deemed to be more effective than the existing encryption method using the chaotic system.

Key Words : RFID, Chaos, 2D Tent-map, Chaos-map, Authentication

1. 서론

사회발달과 더불어 산업구조가 복잡해지면서 물류의 이동량이 증가하고 관리 또한 대량화되고 있다. 기존의 물류관리 시스템인 바코드는 지향성 인식 시스템으로 동시에 여러 물류를 인식할 수 없는 특성으로 대

*Corresponding Author : Deportment of AI Electrical Engineering, Pai Chai University (lomac@pcu.ac.kr)
Received September 29, 2020 Revised October 05, 2020 Accepted October 12, 2020

량화에 적용하기 어려운 문제점을 가지고 있다. 이와 같이 동시에 여러 물류를 인식하고 인증하기 위한 요구에 의해 개발된 시스템이 RFID (Radio-Frequency Identification)시스템이다[1]. RFID는 무선을 사용하는 비 지향성 무 접촉 인식 기술로 동시에 여러 물류를 인식할 수 있는 특성으로 교통요금 지불부터 의료분야, 산업자동화, 전력제어, 에너지 관리까지 많은 부분에 적용 되고 있다. 최 점단 무선 인식 기술인 RFID 시스템은 Tag, Reader 그리고 DataBase로 구성되어 있고 Tag의 전원이 자체 배터리 또는 Reader에서 전자기파 형태로 공급되느냐에 따라 능동형 Tag와 수동형 Tag로 구분된다. Tag는 Reader의 요구에 따라 물품의 고유번호나 장치의 현재 상태를 ID값으로 전송하는 기능을 수행하고, Reader는 전송받은 ID값을 DataBase에 질의하여 Tag가 전송한 ID값을 확인하고 추가 정보를 제공한다. 그러나 Tag는 Reader의 요구에 따라 무조건 ID를 무선으로 전송하게 설계되어 있어 승인되지 않은 Reader에 의해 무단으로 정보가 유출 될 수 있고, 이것은 보안에 취약한 문제점으로 나타나고 있다[2-4]. 우리는 이와 같은 문제점을 해결하기 위해 선행 연구자들의 연구 결과들을 "2장. 관련연구"에 기술하였고, 문제점을 해결하기 위해 설계된 혼돈 시스템을 "3장. 2차원 Tent-map 설계"에 기술하였다. 그리고 최종적으로 3장에서 설계된 혼돈계를 RFID에 적용한 연구 결과를 "4장. 제안된 RFID 인증 프로토콜"에 제시하였다.

2. 관련연구

2.1 해쉬-락 RFID 인증 프로토콜

RFID 인증 방법 중 해쉬-락 인증 방법은 Tag의 정보를 Reader가 수신하여 DB Server에 그 값의 존재 유무로 질의하여 Tag를 인증하는 방법으로 그 구조를 그림 1 에 보인다. 해쉬-락 인증 방법은 Tag에서 전송되는 ID 값을 보호하기 위해 해쉬 함수를 사용한 Meta ID를 사용하고 있고, 이것은 DB Server의 모든 레코드를 검색해야 하는 부하와 통신 중간에 무단으로 획득된 Meta ID로 재 인증이 될 수 있는 문제점을 가지고 있다.

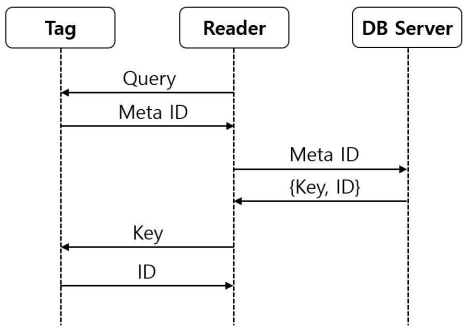

그림 1. 해쉬-락 인증 프로토콜
Fig. 1. Diagram of hash-lock protocol

2.2 랜덤 해쉬-락 RFID 인증 프로토콜

랜덤 해쉬-락 인증 방법은 해쉬-락 인증방법이 Meta ID 유출로 무단 인증이 될 수 있는 문제점을 해결하기 위해 제안되었고, Tag에서 Reader로 ID를 정송 할 때 난수 값을 같이 전송하여 ID값이 고정되는 문제점을 해결한 방법이다 [5]. 그러나 이 방법 또한 DB Server의 모든 레코드를 검색해야 하고 보안에서 노출된 ID_k값의 전송으로 재전송 공격이나 스푸핑 공격에 취약한 특성을 갖고 있다.

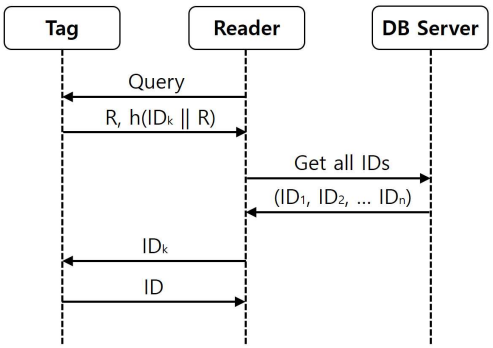

그림 2. 랜덤 해쉬-락 인증 프로토콜
Fig. 2. Diagram of randomized hash-lock protocol

2.3 해쉬-체인 RFID 인증 프로토콜

Ohkubo에 의해 2003년에 제안된 해쉬-체인 인증 방법은 두 개의 해쉬 함수 $H(s_i)$와 $G(s_i)$를 사용하여 체인 형태로 구성하여 보안을 강화한 인증 방법으

로 ID값과 통신 값을 각각 다른 단방향 해쉬 함수로 암호화하여 위치추적이나 재전송 공격에 강한 특성을 가지도록 구성하였다. 그러나 모든 ID값에 대한 해쉬 연산을 수행해야 하므로 DB Server의 연산이 과중되는 단점을 가지고 있다 [6].

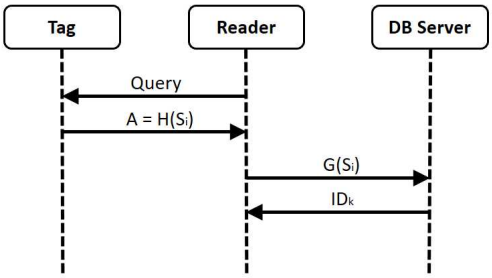

그림 3. 해쉬-체인 인증 프로토콜
Fig. 3. Diagram of hash-chain protocol

3. 2차원 Tent-map 설계

3.1 혼돈시스템의 특성

혼돈 시스템을 크게 시간영역으로 분류하면 이산적인(Discrete) 시스템과 연속적인(Continuous) 시스템으로 분류할 수 있다. 아날로그 신호 관련 암호화 방법에는 연속적인 혼돈 시스템이 사용되고 있고, RFID와 같은 디지털 통신에는 이산 혼돈 시스템이 암호화에 사용되고 있고 그 결과가 효과적이라고 할 수 있다.

이산 특성을 갖고 있는 혼돈 시스템은 계차 방정식 구조로 되어 있고, 그 발생 구조는 Return-map으로 설명되고 있다. 이산 특성을 갖는 맵 구조의 혼돈 시스템은 Logistic-map, Henon-map, Tent-map 등이 있고, 대표적으로 Tent-map의 지배방정식을 식 1에 보인다.

$$x_{n+1} = \begin{cases} \mu\, x_n & ;\ x_n < \frac{1}{2} \\ \mu\,(1-x_n) & ;\ \frac{1}{2} \le x \end{cases} \qquad \text{(식 1)}$$

식 1의 μ값의 변화에 따라 발생되는 x_n의 값을 그림 6의 (a)에서 보인다. 갈래질 도표 그림에서 μ값에 따라 신호의 분포가 편중되는 혼돈신호의 특징을 확인할 수 있다. 그리고 혼돈 시스템에서 발생하는 신호는 미세한 Δx_n의 차이 값이 이후 큰 x_{n+1}의 변화를 보이는 초기값 민감성의 특성을 가지고 있고, 매개변수 μ값에 따라 다른 결과를 보이는 특성과 방정식에서 계산된 신호는 난수와 유사하지만 x_n으로 x_{n+1}을 계산할 수 있는 재생산성을 가지고 있다 [7-9]. 이와 같은 혼돈 신호를 정보통신의 보안 강화용으로 적용하기 위해 송·수신측이 서로 같은 초기값 x_n과 매개변수 μ를 이용해 난수와 유사한 신호를 발생시켜 보안 채널을 생성한다면, 그 채널에 정보를 전송하여 보안이 강화된 통신을 구축할 수 있게 된다[10-12]. 우리는 이와 같은 혼돈 시스템의 암호화 특성을 강화하기 위해 Tent-map의 μ값이 변화하여도 일정한 분포를 갖는 2차원 혼돈 시스템을 새롭게 설계하고 그 내용을 RFID에 적용하는 연구를 진행하였다.

3.2 2차원 Tent-map 혼돈시스템

우리는 3.1절 혼돈 시스템의 특성에서 Tent-map의 편중 분포 특성을 보였다. 매개변수의 넓은 영역에서 효과적으로 암호화를 진행시키기 위해 μ값이 다른 2개의 서로 다른 Tent-map을 2차원 공간에서 θ값으로 투영되게 2차원 구조의 Tent-map을 설계하고 그 내용을 그림 5에 보인다.

그림 5의 S_1 평면과 S_2 평면은 각각 Tent-map의 발생구조를 나타내고 S_1에서 발생된 혼돈 신호는 θ로 투영되어 S_2에 y_n으로 입력된다. 그림에 보이는 z축은 S_1평면에서 혼돈 신호가 발생될 때는 x_{n+1}이고 S_2평면에서 발생될 때는 y_{n+1}로 계산된다.

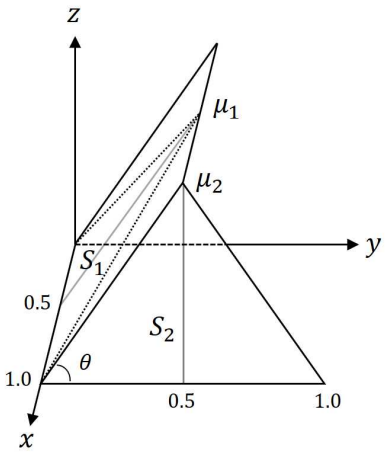

그림 5. 2차원 텐트-맵의 구조
Fig. 5. Structure of 2-Dimensional Tent-map

그림 5의 발생구조를 수식으로 표현하고 그 내용을 식 1에서 보인다. 식 1에서 보인 $x_n{}'$은 $x_n \sin(\theta)$값으로 θ값에 의해 S_2에 투영된 S_1의 신호 값이다.

$$x_{n+1} = \begin{cases} \mu_1 \, y_n & ; \, x_n < \frac{1}{2} \\ \mu_1 \, (1 - y_n) & ; \, \frac{1}{2} \leq x_n \end{cases} \qquad \text{(식 2)}$$

$$y_n = \begin{cases} \mu_2 \, x_n{}' & ; \, y_n < \frac{1}{2} \\ \mu_2 \, (1 - x_n{}') & ; \, \frac{1}{2} \leq y_n \end{cases}$$

식 1에 기술된 수식과 매개변수의 의미를 설명하기 위해 식 2로 정리하고 그 내용을 RFID 통신에 대하여 설명한다.

$$x_{n+1} = F(\mu_1 \, , \, \mu_2 \, , \, \theta \, , \, x_n) \qquad \text{(식 3)}$$

μ_1 : RFID에서 Key 값으로 사용되는 매개변수이다.

μ_2 : 2차원 Tent-map에서 발생되는 신호가 0과 1 사이에 분포하게 하여 편중 분포를 제거하기 위한 매개변수로 1.98로 고정하여 통신 프로토콜에 적용하였다.

θ : RFID에서 M_{ID} 값으로 상점 ID값을 위한 매개변수이다.

x_n : 계차방정식 구조의 혼돈 시스템에서 x_{n+1}을 발생시키기 위한 이전 혼돈 값을 나타낸다.

1차원 Tent-map과 2차원 Tent-map의 특성을 비교하기 위해 Julia 프로그램 언어를 이용하여 시뮬레이션한 결과를 그림 6에 보인다. (a)는 1차원 Tent-map의 매개변수 μ값은 1.2부터 2.0까지 0.001간격으로 증가 시키며 각각 100회씩 계산된 결과를 나타낸 갈래질 도표이고, (b)는 식 2에서 보인 2차원 Tent-map에서 μ_2 값을 2.0으로 고정시키고 μ_1값을 그림 6의 (a)와 동일한 방법으로 변화시키며 계산된 결과 값의 그림이다.

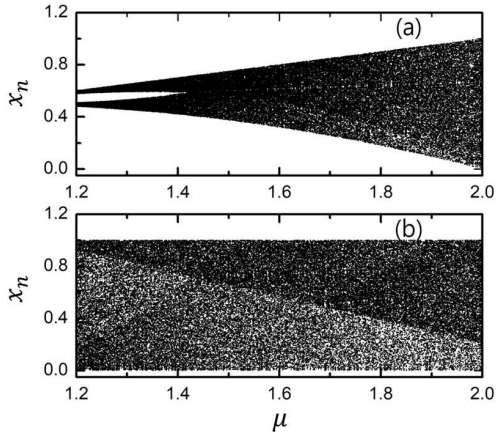

그림 6. 텐트-맵의 갈래질 도표
Fig. 6. Bifurcation diagram of Tent-map

그림 6의 갈래질 도표는 2차원 Tent-map의 μ_1의 변화에 따라 0.0과 1.0사이의 분포를 갖는 x_n신호가 발생되는 것을 확인할 수 있다. 이 결과는 보안채널 생성 시 키값으로 사용될 수 있는 μ값을 보다 넓은 영역에서 사용할 수 있어 보안통신에 효과적으로 적용될 수 있는 결과라고 할 수 있다.

우리는 설계된 2차원 Tent-map의 특성을 RFID에 적용시키기 위해 새로운 통신 프로토콜을 설계하고 그

내용을 다음에 보인다.

4. 제안된 RFID 인증 프로토콜

4.1 2D Tent-map으로 설계된 인증 프로토콜

RFID 인증을 위해 설계된 2차원 Tent-map을 적용한 RFID 인증 과정을 그림 7 에 보이고 각 단계별 진행 내용을 다음에 기술한다.

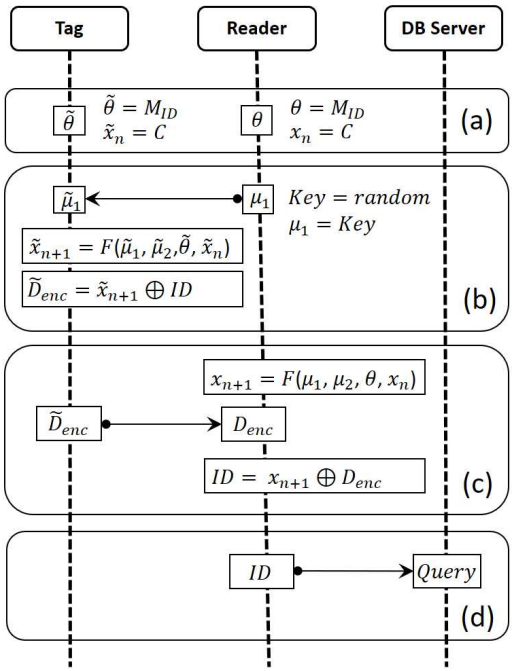

그림 7. 제안된 RFID 프로토콜의 인증 과정
Fig. 7. Authentication process of suggested RFID protocol

(a) 단계: Tag와 Reader에 시스템변수로 설정된 상점ID(M_{ID}) 값과 초기값 C를 각각 2차원 Tent-map의 혼돈신호 발생 매개변수인 θ와 x_n에 저장하고 μ_2는 시스템상수로 1.98로 고정하여 사용한다.

(b) 단계: Reader는 암호화 통신을 위한 혼돈신호의 발생구조를 은닉하기 위해 2차원 Tent-map의 매개변수로 사용되고 있는 μ_1을 Key값으로 지정하고 Tag에게 난수로 전송한다.

Tag는 (a)단계에서 설정된 $\tilde{\theta}$, $\tilde{\mu}_2$, $\tilde{x}_n$ 과 Reader로 부터 수신된 난수 값 $\tilde{\mu}_1$을 사용하여 Reader와 동일하게 2차원 Tent-map의 매개변수를 초기화 한다.

Tag는 2차원 Tent-map에서 발생된 혼돈신호 $\tilde{x}_{n+1}$ 과 Reader의 요청에 따라 전송되는 제품의 ID값을 배타논리(XOR)로 암호화 하여 $\tilde{D}_{enc}$를 계산한다.

(c) 단계: Reader는 (a)단계에서 설정된 매개변수와 Tag로 전송한 난수 값 μ_1으로 혼돈신호 x_{n+1}을 계산하고, Tag에서 전송 받은 D_{enc}와 계산된 x_{n+1}을 배타논리로 복호화 하여 제품 ID 값을 추출한다.

(d) 단계: 복호화 된 ID값을 DB Server 측에 질의하여 ID값의 유무를 확인하여 인증절차를 진행한다.

4.2 암호화 결과 분석

4.2.1 상관관계 분석

우리는 제안된 RFID 인증 프로토콜의 암호화 정도를 정량화하기 위해 Tag에서 Reader로 전송되는 정보를 난수로 가정하고 1차원 Tent-map과 2차원 Tent-map의 μ값을 변화시키며 상관관계를 계산하였다. 계산에 사용된 상관관계 식을 식 3에 보인다. 식에서 $cov(D_{enc}, D_{dec})$과 $\sigma_{D_{enc}}$,$\sigma_{D_{dec}}$는 각각 암호화 이전과 이후 정보의 공분산값과 표준편차를 나타낸다.

$$\rho = \frac{cov(D_{enc}, D_{dec})}{\sigma_{D_{enc}} \sigma_{D_{dec}}} \quad \text{(식 4)}$$

표 1. 암호화된 정보의 상관계수
Table 1. Correlation coefficient of encrypted information

Parameter(μ)	1D Tent-map	2D Tent-map
1.10	0.7021	0.5625
1.30	0.6255	0.4916
1.50	0.5667	0.4754
1.70	0.5568	0.5203
1.90	0.5574	0.5592

계산된 표 1의 결과 값으로 우리가 제안한 RFID 인증 프로토콜이 μ값의 변화에도 일정한 상관계수 값을 갖는 것을 확인할 수 있다.

4.2.2 이미지 암호화 분석

우리는 제안된 프로토콜의 암호화 정도를 가시화하기 위해 샘플 이미지를 8비트 흑백 이미지로 변환시키고, 2차원 Tent-map에서 계산된 x_n값을 8비트 정수형으로 변환하여 두 값을 배타 논리(XOR)로 계산하여 암호화 및 복호화를 진행하였다. 계산된 이미지와 각각의 히스토그램을 그림 8에 보인다.

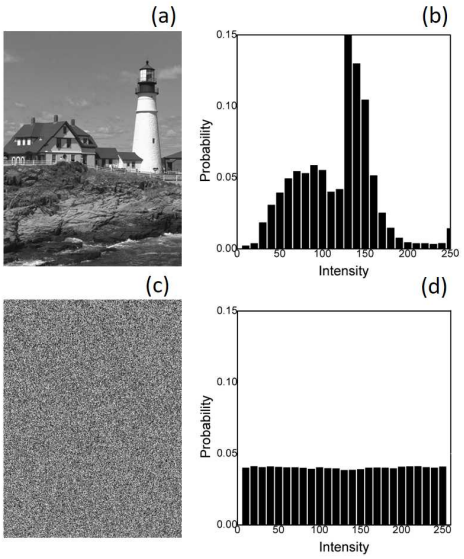

그림 8. 암호화된 이미지의 히스토그램
Fig. 8. Histogram of the cipher image

암호화된 이미지의 히스토그램이 모든 색에 대하여 일정한 분포를 갖는 결과를 그림 8의 (d)에서 확인할 수 있다.

4.2.3 기밀성(Confidentiality)

기밀성이란 전송되는 정보가 정보접근에 승인된 사람에게만 공개되는 것을 의미한다. 우리가 제안한 인증 프로토콜은 유산 난수로 보안 채널을 생성한 후 정보를 전송하기 때문에 보안 채널에 참여하지 못한 Reader는 난수와 같은 정보만 취득하게 되어 기밀성이 보장된다고 할 수 있다.

4.2.4 무결성(Integrity)

무결성이란 전송되는 정보가 정상적인 상태를 유지하고 무단으로 위·변조할 수 없도록 하는 것을 의미한다. 우리가 제안한 인증 프로토콜은 계차 방정식 형태로 되어 있고 x_n에 의해 x_{n+1}이 계산되는 구조로 무단 위·변조 시 확인이 가능하므로 무결성이 보장된다고 할 수 있다.

4.2.5 가용성(Availability)

가용성이란 정보 전송 시 시스템의 장애 없이 정상적으로 서비스를 수행할 수 있는 것을 의미한다. 우리가 제안한 인증 프로토콜은 초기에 μ_1과 θ가 분배되면 비교적 간단한 계차 방정식에 의해 암호화가 이루어지기 때문에 정보에 대한 접근과 사용이 적시에 이루어지므로 가용성이 보장된다고 할 수 있다.

5. 결론 및 향후 과제

사회와 정보통신 기술이 발달되면서 보다 효율적이고 효과적인 물류관리 방법이 필요하게 되었고 이런 요구에 따라 개발된 것이 RFID 통신 기술이다. 그러나 RFID 통신은 정보 전송을 위해 무선을 사용하고 있고, 이것은 보안에 취약한 특성을 나타내고 있다. 많은 연구자들은 이 문제점을 해결하기 위해 RFID 보안 강화에 대한 연구를 진행하고 있고, 특히 혼돈계와 같은 복잡계를 이용하여 정보를 암호화하는 인증 방법 또한 많은 연구가 이루어지고 있다. 그러나 혼돈계와 같은

복잡계에서 발생되는 신호 또한 매개변수에 따라 신호의 분포가 예측될 수 있는 문제점을 가지고 있어 보안에 취약함이 있다고 할 수 있다. 우리는 이와 같이 기존 혼돈계에서 보이는 매개변수에 따른 신호의 편중 분포 문제를 해결하기 위해 주 Tent-map 혼돈계가 부 Tent-map 혼돈계에 θ값으로 투영되어 움직이는 2D Tent-map 혼돈계를 설계하고, 그 결과를 RFID에 적용하여 새로운 RFID 인증 보안 프로토콜을 설계하였다. 우리가 설계한 암호화 인증 방법은 다소 이론적인 부분이 있을 수 있으나 추후 H/W에 직접 적용하는 후속 연구가 진행된다면 기존의 RFID 인증 프로토콜을 대체할 수 있는 새로운 인증방법이 될 것으로 생각된다.

REFERENCES

[1] K. Finkenzeller, "RFID Handbook - Second Edition," John wiley & Sons, pp. 2-9, 2003.

[2] K. H. Chung, K. Y. Kim, S. J. Oh, J. K. Lee, Y. S. Park, and K. S. Ahn, "A Mutual Authentication Protocol using Key Change Step by Step for RFID Systems," The Korean Institute of Communication and Information Science, Vol. 35, No. 3, pp. 462-472, Mar. 2010.

[3] S. J. Oh, K. H. Chung, T. J. Yun, and K. S. Ahn, "An RFID Mutual Authentication Protocol Using One-Time Random Number," The Korean Institute of Communication and Information Science, Vol. 36, No. 7, pp. 858-567, July 2011.

[4] H. S. Ahn, and K. D. Bu, "Robust RFID Distance-Bounding Protocol based on Mutual Authentication," The Journal of KIIT, Vol. 11, No. 7, pp. 47-55, March 2013.

[5] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System," Security in Pervasive Computation, LNCS 2802, pp. 201-212, Nov. 2004.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Enhanced Hash Chain based Scheme for Security and Privacy in RFID Systems," International Journal of Computer Applications, Vol. 28, No. 9, pp. 719-724, 2004.

[7] H. G. Schuster, "Deterministic Chaos: an Introduction 2nd(second) edition," VCH, pp 24-32, Dec. 1997.

[8] Ali. H. Nayfeh, "Applied Nonlinear Dynamics," A Wiley-Interscience Publication, pp. 6-15, Feb. 1995.

[9] E. Ott, "Chaos in Dynamical Systems Second Edition," Cambridge University Press, pp. 15-18, Sep. 2002.

[10] G. S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System," Korea Information Assurance Society, Vol. 8, No. 3, pp. 57-84, 2008.

[11] 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, pp. 201-206, 2011.

[12] G. S. Yim, "IoT MQTT Security Protocol Design Using Chaotic Signals," J. of Korea Institute of Information, Electronics, and Communication Technology, Vol. 11, No. 6, pp. 778-783. Oct. 2018.

저자약력

임 거 수(Geo-Su Yim) **[정회원]**

- 1998년 배재대학교 물리학과 대학원 (이학석사)
- 2004년 서강대학교 물리학과 대학원 (이학박사)
- 2008년 배재대학교 전기공학과 교수

〈관심분야〉 시계열분석, 빅데이터 분석, 머신러닝, 보안