한국정보전자통신기술학회논문지(jkiiect)'16-10, Vol.9 No.5
논문 16-09-05-451 http://dx.doi.org/10.17661/jkiiect.2016.9.5.451

동기화된 혼돈시스템을 이용한 RFID 통신 프로토콜 설계

임거수*

Design of an RFID Communication Protocol Using Synchronized Chaotic Systems

Geo-Su Yim*

요 약 최근 들어 데이터 전송 분야에서 안전성을 향상시킬 목적으로 통신의 암호화 방법에 혼돈 신호를 적용하는 연구가 많이 이루어지고 있다. 우리는 혼돈 신호의 초기치 민감성과 잡음 유사성을 RFID 통신 채널에 적용 시키는 새로운 보안 프로토콜을 설계하였다. 혼돈시스템은 각각 독립적으로 구동되는 시스템이라도 초깃값이 같으면 이후 같은 시간에 같은 신호를 발생하는 특성이 있으므로 예측할 수 없는 채널을 생성할 수 있는 장점이 있다. 그러나 보안 채널은 사전에 초깃값이 공유되어야만 생성될 수 있으므로 초깃값 전송 시에 무단으로 도용될 수 있는 문제점 또한 배제할 수 없다. 우리는 이런 문제점을 개선하기 위해 또 다른 혼돈 신호로 통신에 사용되는 두 혼돈 시스템을 동기화시키는 방법을 적용하여 초깃값을 은폐하는 새로운 통신 방법을 설계하였다. 그리고 설계된 방법을 검증하기 위해 이미지 암호화 및 복호화로 그 결과를 보였다. 우리가 제안한 방법은 기존 혼돈 신호를 이용한 통신방법의 문제점을 개선한 방법으로 보안에 취약한 RFID 통신 채널에 적용한다면 더욱 안전한 통신이 이루어 질 것으로 예측된다.

Abstract To improve security in the data communication field, many studies on the application of chaotic signals to encryption have been conducted in recent years. In this study, a new security protocol where the initial value sensitivity and noise similarity of chaotic signals have been applied to an RFID communication channel was designed. In the case of chaotic systems, if the initial values become identical, the same signals are generated at the same time after that point even though the two systems have been calculated independently. Therefore, an unpredictable security channel can be produced based on such characteristics. However, a security channel can be produced only when an initial value is shared in advance, and thus there is a potential problem of infringement during the transmission of the initial value. To resolve this problem, a method in which a certain proportion of new chaotic signals are applied to two chaotic systems for communication and are then synchronized after some time was proposed. This new method can conceal the initial value, and thus can resolve the problem of the existing communication method using chaotic signals. The designed method was verified with the encryption and decryption of images. It is expected that a more secure RFID system could be established by applying the communication protocol proposed in this study to insecure RFID communication channels.

Key Words : RFID, Chaos, Synchronization, Secure Communication

1. 서론

사회구조와 통신기술의 발달은 정보의 양과 질적인 변화를 가져왔고, 그중 가장 큰 변화를 보인 것은 USN(Ubiquitous Sensor-Network)과 RFID(Radio Frequency IDentification) 통신일 것이다. RFID는 기존의 근접 접촉식 인식장치인 바코드의 문제점을 해결하기 위해 개발된 것으로 현

*First & corresponding Author : Department of Electrical Engineering, Paichai University (lomac@pcu.ac.kr)
Received September 27, 2016 Revised October 26, 2016 Accepted October 28, 2016

재는 물류 유통뿐만 아니라 출입, 보안 카드 등에도 사용되고 있고 생체인식 분야까지 연구가 이루어지고 있다. RFID 시스템은 무선통신시스템으로 유선통신에서 발생 되었던 온습도, 진동, 먼지 등과 같은 환경제약 조건에 대응할 방법으로 그 활용 범위가 다양하다고 할 수 있다. 그러나 유선통신과 달리 무선통신은 통신 범위 내에 존재하는 인증되지 않은 송수신 장치가 무단으로 통신에 참여하여 데이터를 왜곡시킬 수 있는 문제점을 배제할 수 없어 보안에 대한 대책이 필요하고 관련 연구 또한 많이 이루어지고 있다 [1,2,3]. 특히 소형화가 요구되는 RFID 장치는 보안 프로그램을 탑재하기 위한 개발공간의 제약으로 기존의 대용량 암호화 방법을 탑재하기 어려운 특성이 있다. 우리는 이와 같은 RFID의 문제점을 해결하기 위해 비교적 간단한 수식으로 구동되는 혼돈시스템을 암호화에 적용하는 방법을 제시하고 관련 연구 결과를 보인다.

혼돈시스템에서 발생하는 신호는 시스템구동에 사용된 매개변수와 초깃값에 대해 민감한 특성이 있고[4,5], 발생하는 신호 또한 잡음 신호와 유사하여 예측이 불가능하다[6,7]. 이와 같은 신호를 RFID 통신에 적용한다면 개발공간의 문제점을 해결하고 강한 보안 특성을 갖는 RFID 통신프로토콜을 개발할 수 있을 것으로 예측된다[8]. 우리는 특히 혼돈시스템 암호화 방법의 취약점인 초깃값 분배의 위험성을 고려한 동기화 구조의 혼돈 신호를 이용한 RFID 프로토콜을 설계하고 연구를 진행했다.

2장에서는 기존 RFID에 대한 사전연구를 보이고, 3장에서는 초깃값 은폐를 위한 동기화 구조와 혼돈시스템의 특성을 보인다. 4장에서는 동기화 혼돈구조를 적용한 새로운 RFID 통신 프로토콜의 구조를 제시한다. 우리가 제시한 RFID 통신 방법은 아직 연구단계에 머물러 있는 방법이지만 계속된 적용연구가 이루어진다면 추후 RFID의 새로운 프로토콜로 자리 매김할 수 있을 것으로 예측한다.

2. RFID 인증 프로토콜

2.1 해쉬-락 인증 프로토콜

해쉬-락 인증 프로토콜은 RFID 인증의 초기모델로 2003년 S. A. Weis 등에 의해 발표된 인증 방법이다. [9] 해시 함수의 전 방향성을 이용한 방법으로 DataBase, Reader 그리고 Tag의 데이터 흐름을 그림 1 에 보인다. Reader의 요구에 따라 Tag의 ID 값을 Hash 함수로 암호화하여 Reader에게 전송하고 Reader는 전송받은 값이 DataBase에 존재하는지로 Tag를 인증 하게 된다. 이 방법은 H(ID)값을 참조하기 위해 DataBase의 모든 레코드를 검색해야 하고 전송되는 값이 고정되어 있어 무단 도청된 값이 재전송이나 위치추적 공격에 사용될 위험성을 가지고 있다.

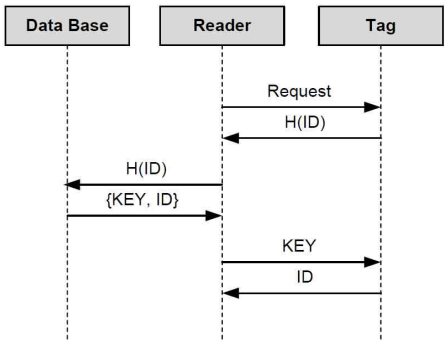

그림 1. 해쉬-락 인증 프로토콜
Fig. 1. Architecture of Hash-lock protocol

2.2 랜덤 해쉬-락 인증 프로토콜

랜덤 해시-락 인증 프로토콜은 해시-락 인증 프로토콜의 취약점을 개선한 방법으로 H(ID)값에 난수값을 포함하여 전송되는 값이 고정 되는 문제점을 해결한 방법이다[10]. 그러나 DataBase의 모든 레코드를 검색해야 하는 문제점과 서비스거부 공격에 취약한 문제점은 해결하지 못했다.

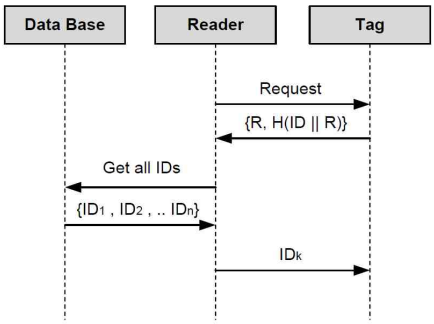

그림 2. 랜덤 해시-락 인증 프로토콜
Fig. 2. Architecture of Randomized Hash-lock protocol

3. 동기화 보안 채널

3.1 혼돈 시스템 특성

우리는 기존 RFID 인증 프로토콜의 문제점을 개선하기 위해 유사난수 신호를 발생하는 혼돈시스템을 인증 프로토콜에 적용하는 연구를 진행하였다.

보안통신에 사용되는 혼돈시스템은 계차 방정식 형태로 $x_{n+1} = F(\alpha , x_n)$ 형태를 가지고 있다.

계차 방정식 혼돈 시스템은 α 값과 x_n 값의 미세한 변화에 따라 예측할 수 없는 x_{n+1} 의 값이 계산되는 특징을 가지고 있고, 이와 같은 성질을 "초기치 민감성"이라고 한다. 이것은 시스템의 α 값을 모르면 x_{n+1} 을 계산할 수 없는 특성과 x_n 으로 x_{n-1}을 계산할 수 없는 단방향성 특성이 있어 보안 및 인증에 효과적으로 사용할 수 있는 특징이라고 할 수 있다. 혼돈 시스템에서 계산된 시계열값 $X = x_1, x_2, \ldots$는 잡음과 유사하여 전송하고자 하는 데이터를 $T_n = x_n \oplus Data$ 으로 암호화하여 전송하게 되면 T_n 역시 x_n 과 유사한 잡음 특성을 갖게 되기 때문에 무단도용이 불가능하게 된다. 그러나 수신측에서 같은 혼돈 시계열 X 를 갖고 있다면 전송된 데이터를 $Data = T_n \oplus x_n$ 으로 복호화할 수 있게 되어 보안 채널을 생성할 수 있게 된다.

3.2 혼돈신호를 이용한 동기화

혼돈 신호를 이용한 보안 채널 생성은 송·수신측이 모두 같은 초깃값에 의한 신호를 발생해야 하는 문제점을 갖고 있다. 기존은 방법들은 보안 채널 생성 전에 초깃값을 공유하는 초깃값 분배 과정을 거치 이후에 보안 채널을 생성한다. 그러나 우리는 이 방법의 위험성을 인지하고 동기화 현상을 초깃값 분배에 적용하는 연구를 진행하였다.

동기화 현상은 1673년 네덜란드의 물리학자 호이겐스의 진자시계 실험에서 처음 관측되었고, 이후 많은 관련 연구가 이루어졌다. 특히 혼돈시스템에서 동기화는 서로 다른 궤적을 보이는 시스템이 외부의 자극 신호 때문에 일정시간 이후 같은 궤적의 시스템이 되는 현상으로 보안 채널 생성에 효과적으로 사용될 수 있는 특징이라고 할 수 있다.

우리는 혼돈시스템의 동기화를 통신에 적용하기 위한 시스템을 구축하고 그 내용을 식 1 에 보인다.

식 1 은 생태계의 개체 수를 모델링한 Logistic Map을 변형한 시스템으로 RFID의 보안 채널 생성을 위한 만들어진 식이다 [11].

$$x_{n+1}^{(r)} = \lambda\, x_n^{(r)}(1-x_n^{(r)}) + \alpha x_n^{(s)} \qquad \text{(식 1)}$$
$$x_{n+1}^{(t)} = \lambda\, x_n^{(t)}(1-x_n^{(t)}) + \alpha x_n^{(s)}$$

$x^{(r)}$은 RFID 시스템에서 Reader에 탑재될 혼돈 시스템 신호이고, $x^{(t)}$는 Tag에 탑재될 혼돈시스템 신호이다. 그리고 $x^{(s)}$는 두 시스템의 초깃값을 은폐하기 위한 동기화용 혼돈 신호이다.

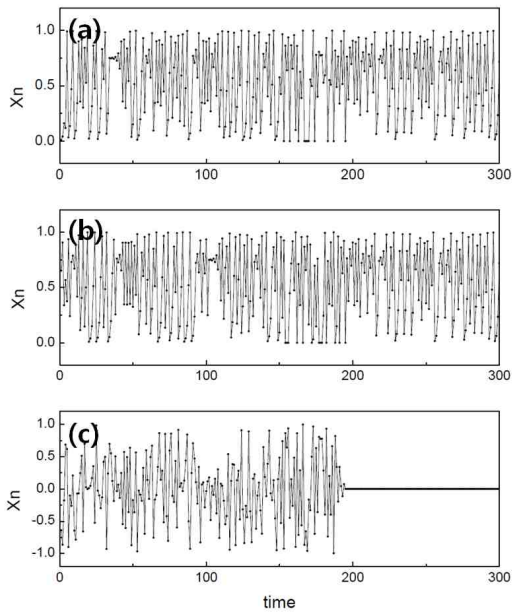

그림 3. 동기화된 혼돈신호 그래프

(a) $x_n^{(r)}$ (b) $x_n^{(t)}$ (c) $x_n^{(r)} - x_n^{(t)}$ 신호

Fig. 3. Graph of synchronized chaotic signal

(a) $x_n^{(r)}$, (b) $x_n^{(t)}$ (c) $x_n^{(r)} - x_n^{(t)}$ signal

식 1의 전산 시늉 시계열을 그림 3 에 보인다.

그림 3 의 (a), (b) 는 각각 $x_n^{(r)}$ 과 $x_n^{(t)}$ 의 혼돈신호이고, (c) 는 $x_n^{(r)} - x_n^{(t)}$ 값으로 동기화 유무를 확인하기 위한 차이 값이다. n 이 150 일 때 동기화 신호를 인가하였고 190 근처에서 동기화가 완료 된 것을 확인할 수 있다.

우리는 동기화 시작부터 동기화 완료까지의 시간이 동기화 신호 $\alpha x_n^{(s)}$의 가중치 α 값과 관계가 있는 것을 확인하고 α 값에 대한 동기화 지연시간 l_s 을 전산 시늉으로 계산하였다. α 값을 0.1 부터 0.6 까지 0.01 씩 증가시키면 100,000 반복 실험한 평균 결과를 그림 4 에 보인다.

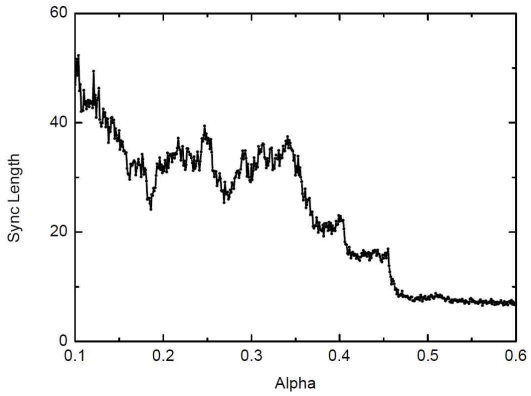

그림 4. 가중치에 따른 동기화 길이 그래프

Fig. 4. Graph of synchronized length with variable

전산시늉 결과 α 값이 0.5 이상에서 l_s 값이 일정한 것을 확인하였고, α 값이 0.2 부터 0.35 사이에서는 지연시간 l_s 를 40 이상으로 유지해야 동기화가 되는 것을 확인할 수 있다.

보안통신에 사용되는 채널 신호가 시스템의 매개변수, 초깃값, 전송되는 데이터 등과의 상관관계를 가지고 있으면 전송되는 데이터를 무단 복원시킬 때 데이터가 노출될 수 있는 위험 요소가될 수 있다.

우리 식 1에 제시된 시스템에서 동기화 신호와 동기화된 이후의 신호 사이에 존재하는 상관 관계 특성을 분석하기 위한 결과로 산포도를 그림 5 에 보인다.

x_n 값은 동기화 시작 지점의 값이고 x_{n+d} 는 d 시간 지연 이후 동기화되어 통신에 사용되는 신호이다. 전산 시늉 결과에서 x_{n+d} 값이 0.18 부근에 확률적으로 빈도수가 높은 걸 확인할 수 있다. 그러나 모든 x_n에 대해 같은 특성이므로 데이터가 무단 복원될 위험 요소로 작용하지는 않는다.

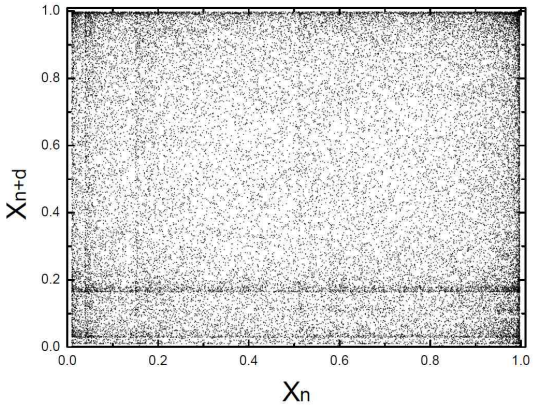

그림 5. 혼돈신호 x_n과 x_{n+d}의 그래프
Fig. 5. Graph of chaotic signal x_n and x_{n+d}

4. 제안된 RFID 프로토콜

4.1 RFID 인증 프로토콜

우리의 연구결과를 토대로 한 통신방법을 보안이 취약한 RFID 통신에 적용하고 그 데이터 흐름을 (a) 단계와 (b) 단계로 구분하여 그림 6 에 보인다.

단계 (a). 초기 Reader의 요구에 따라 Tag는 동기 화용 혼돈시스템 $F_1(S_n)$에서 계산된 혼돈 신호를 Reader에게 전송한다. Reader와 Tag는 $k\,S_n$ 값으로 동기화를 진행한다. 단방향 통신으로 Reader와 Tag의 동기화 유무를 확인 할 수 없으므로 그림 4 에 보인 바와 같이 α 값 0.5에 동기 지연시간 10을 기준으로 동기화 보장을 위해 15회 이상 (a) 구간을 반복하여 완전 동기화를 시킨다.

단계 (b). Reader와 Tag 사이의 동기화를 확인하기 위해 3-웨이 핸드쉐이킹(3-way handshaking) 방법과 혼돈 신호를 이용한 암호화 방법으로 Key 값을 전송하며 동기화 유무를 확인한다.

설명한 바와 같이 (a),(b) 단계를 거친 이후 Reader와 Tag 두 시스템의 각각 x_n 과 y_n의 값이 동일하게 되고, 이후 x_{n+1}과 y_{n+1} 또한 일치하게 되어 Reader와 Tag 사이에 난수 유사 신호로 암호화된 보안 통신 채널이 생성된다.

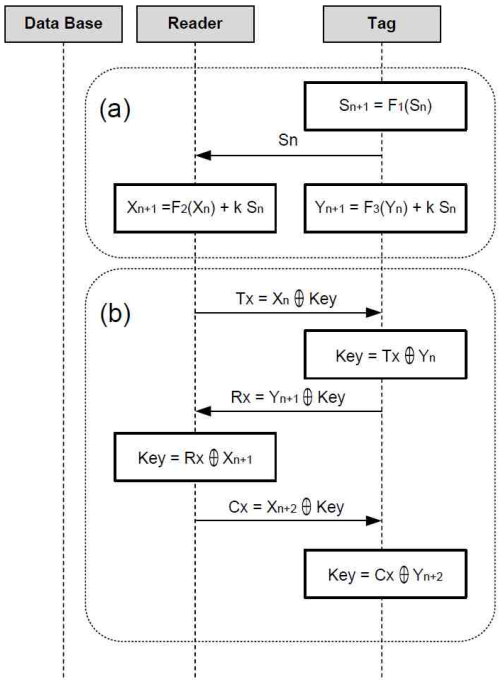

그림 6. 제안 프로토콜의 구조
Fig. 6. Structure of proposed protocol

4.3 이미지 암호화 및 복호화

우리는 본 논문에서 제안한 통신방법의 암호화 정도를 가시적으로 파악하기 위해 특정 이미지 데이터를 전송되는 통신 데이터 신호로 간주하고 암호화를 진행하였다. 전송되는 데이터와 무단 유출된 데이터에 대한 결과를 그림 7 에 보인다.

그림 7 의 (a)는 암호화 정도를 파악하기 위해 회색 256색으로 만들어진 원본 이미지이다. (b)는 원본 이미지의 히스토그램으로 색의 분포에 대한 정보를 확인할 수 있다. (c)는 우리가 제시한 프로토콜로 통신 되는 데이터를 무단 도용했을 때 이미지이고 (d)는 그것의 히스토그램이다. 결과적으로 (a),(b)는 전송되는 데이터의 기본정보와 분포

정보를 확인 할 수 있지만 (c),(d) 는 기본 정보뿐만 아니라 분포정보까지 파악하기 어려운 것을 확인할 수 있다.

통신 채널을 통해 전송되는 모든 데이터는 (c),(d) 형태로 전송되기 때문에 보안 통신 프로토콜에 효과적으로 적용 될 방법이라고 할 수 있다.

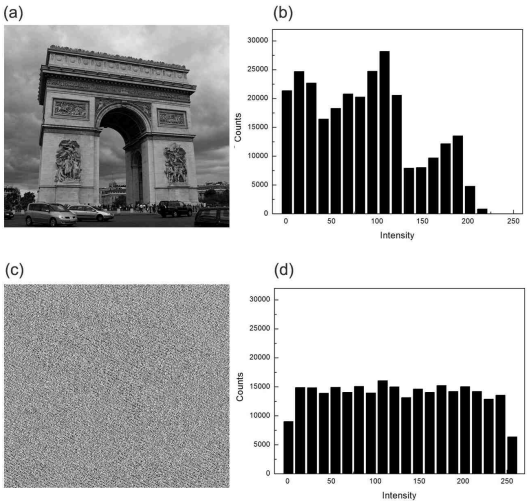

그림 7. 제안 프로토콜의 시뮬레이션
Fig. 7. Simulation of proposed protocol

5. 안정성 분석

혼돈 신호로 동기화된 혼돈시스템을 RFID 통신 프로토콜에 적용한 예를 4장 에서 보였다. 우리가 제시한 보안 프로토콜의 안정성을 위한 요구사항별 내용을 보인다.

5.1 기밀성(Confidentiality)

데이터 통신에서 기밀성이란 송수신되는 모든 데이터는 도청에 의한 무단 도용 시 사용할 수 없도록 암호화되어 있어야 한다는 것을 말한다. 본 논문에서 제안한 RFID 통신 프로토콜은 통신 되는 모든 데이터를 혼돈시스템에서 발생하는 유사난수 신호로 암호화하기 때문에 전송되는 데이터 또한 유사난수 특성을 가지게 되어 도청된 데이터는 무단 도용될 수 없게 되므로 기밀성이 유지된다.

5.2 무결성(Integrity)

혼돈 신호를 이용한 통신방법은 계차방정식 혼돈시스템인 $x_{n+1}=F(x_n)$ 구조를 같기 때문에 x_n 에 의한 x_{n+1} 의 단방향 인증이 가능하므로 전송되는 데이터에 대한 무단 변조 공격이나 재전송 공격 유무를 확인할 수 있어 이에 대한 즉각적인 대응이 가능하므로 무결성이 보장 된다고 할 수 있다.

5.3 가용성(Availability)

우리가 제안한 통신프로토콜은 혼돈시스템의 유사난수를 암호화에 이용하는 방법이고, 계차방정식 시스템의 특성으로 단방향 인증이 가능하여 보안 프로토콜 사용에 효과적이다. 시스템의 매개변수, 구동용 초깃값 등이 유출되어도 동기화된 초깃값은 송·수신 측에서 내부적으로 동기화 길이에 대응하여 발생하는 값이므로 유출이 불가능하다. 이런 특성으로 우리가 제안한 통신프로토콜의 가용성이 보장된다.

6. 결론 및 향후 과제

혼돈 신호를 이용한 통신방법은 혼돈시스템이 가지고 있는 비선형성을 이용하여 전송되는 데이터를 암호화하는 방법이다. 혼돈시스템의 신호는 계산 시 사용되는 매개변수와 초깃값에 따라 다른 신호가 발생되기 때문에 효과적인 암호화 통신방법으로 사용될 수 있다. 그러나 이 방법은 통신채널 생성 이전에 초깃값이 서로 공유되어야 하고, 이 초깃값을 공유하는 단계에서 발생할 수 있는 무단 도청공격은 치명적인 위험 요인으로 작용할 수 있다.

우리는 이 문제점을 해결하기 위해 초기에 공유된 초깃값으로 통신하는 것이 아니라 공유된 초깃값을 이용해 동기화 과정이 이루어지고 그 후 계산된 초깃값으로 통신하는 방법을 설계하였다. 그리고 이 방법에 대한 결과 값으로 통신방법의 안전성을 가시화하였다.

본 논문에서는 우리의 연구결과를 적용하기 위

해 보안이 취약한 RFID 통신을 선택하였고, RFID의 Reader와 Tag 사이의 인증 단계에 혼돈 시스템의 동기화 방법이 적용된 새로운 인증 프로토콜을 적용 하였다. 우리는 추후 지속적인 유사 연구로 동기화 혼돈신호를 이용한 통신방법을 RFID 뿐만 아니라 보안이 취약한 근거리 유무선 통신에도 적용시킬 계획이다.

REFERENCES

[1] H. Y. Kim, N. G. Kim, K. H. Kim, H. C. Bang, and S. J. Kim, "An Authentication Model for Sharing Logistic Information based on RFID System", The Korean Institute of Information Technology, Vol. 9, No. 3. pp. 155-161, March, 2011.

[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 Institude of Communications and Information Science, Vol. 35, No. 3, pp. 462-472, Mar, 2010.

[3] 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, July 2013.

[4] R. H. Abranham, and C. D. Shaw, "Dynamics - The Geometry of Behavior", Addison-Wesley, 1992.

[5] G. L. Baker, and J. P. Gollub, "Chaotic Dynamics 2nd", Cambridge University Press, 1996.

[6] G. P. Williams, "Chaos Theory Tamed", Taylor & Francis, 1977.

[7] A. H. Nayfeh, and B. Balachandran, "Applied Nonlinear Dynamics", Wiley-Interscience, 1995.

[8] M. H. Choi, and G. S. Yim, "Passive RFID Certification Protocol Design Using Digital Chaos System", Journal of KIIT, Vol. 12, No. 10, pp. 85-92, Oct 2014.

[9] 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. an Security in Pervasive Computing, Mar. 2003.

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

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

저자약력

임 거 수(Geo-Su Yim) **[정회원]**

- 1998년 2월 : 배재대학교 물리학과 대학원 (이학석사)
- 2004년 2월 : 서강대학교 물리학과 대학원 (이학박사)
- 2008년 3월 ~ 현재 : 배재대학교 전기공학과 교수

<관심분야> 시계열분석, 신호처리, 빅데이타 분석, FPGA 비젼 제어