Journal of KIIT. Vol. 16, No. 10, pp. 119-123, Oct. 31, 2018. pISSN 1598-8619, eISSN 2093-7571 119
http://dx.doi.org/10.14801/jkiit.2018.16.10.119

혼돈 신호의 잡음 동기화를 이용한 RFID 보안 프로토콜 설계

임 거 수*

RFID Security Protocol Design Using Noise Synchronization of Chaotic Signal

Geo-Su Yim*

이 논문은 2018학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임.

요 약

RFID(Radio Frequency IDentification) 통신은 기존의 바코드와 같은 접촉식 인증 시스템의 문제점을 해결할 목적으로 개발된 근거리 인증 시스템이다. RFID는 무선통신을 이용한 인증 방식으로 환경 제약 조건에 강인한 특성이 있어 많은 분야에 응용되고 있다. 그러나 무선 통신을 사용하고 있어 항상 데이터의 기밀성이나 무결성이 위변조 공격에 노출되어 있다고 할 수 있다. 우리는 이 문제를 해결하기 위해 혼돈계의 동기화 방법 중 잡음을 이용한 방법으로 RFID 보안 프로토콜을 설계하였다. 잡음을 이용한 방법은 리더와 태그를 동기화시키는 정보가 잡음이기 때문에 도청 공격으로 정보가 노출되었어도 노출된 신호에서 혼돈계의 동기화에 관련된 정보를 추출할 수 없어 공격에 강인한 통신 방법이라고 할 수 있다.

Abstract

RFID (Radio Frequency Identification) communication is a local area authentication system developed for the purpose of solving the problems of the existing contact-type authentication systems such as bar codes. RFID is an authentication method using wireless communication, making it strong against environmental constraints, so it is applied in many fields. However, since RFID uses wireless communication, the confidentiality and integrity of data are always exposed to attacks for forgery. In order to solve this problem, we designed the RFID security protocol using noise among the chaotic system synchronization methods. Since the information that synchronizes the Reader and thetag is noise, the method using the noise is a strong communication method because the information related to the synchronization of the chaotic system cannot be extracted from the exposed signal even if the information is exposed by eavesdropping attacks.

Keywords
RFID, chaos, noise synchronization, security protocol, communication

* 배재대학교 전기공학과
- ORCID: https://orcid.org/0000-0002-2407-2768

· Received: Sep. 30, 2018, Revised: Oct. 12, 2018, Accepted: Oct. 15, 2018
· Corresponding Author: Geo-Su Yim
Dept. of Electrical Engineering, Paichai University, 155-40 Baejae-ro, Seo-gu, Daejeon, Korea,
Tel.: +82-42-520-5823, Email: lomac@pcu.ac.kr

Ⅰ. 서 론

본 논문에서 우리는 사회의 발달과 더불어 물류의 운송 및 유통과 재고관리 등의 인증 시스템으로 사용되고 있는 RFID의 통신에 관련된 연구 결과를 보인다. 기존의 바코드와 같은 접촉식 인증체계는 온도나 습도, 진동과 같은 환경 제약적인 요소로 인하여 사용에 제한이 있었으나, 무선을 사용하는 비접촉 인증체계인 RFID는 이런 문제를 해결할 수 있어 물류뿐만 아니라 출입 카드, 버스카드 등에 사용되고 있고 현재는 의료분야까지 그 영역을 확대하고 있다. RFID는 무선을 사용하기 때문에 다양한 분야에 사용되고 있고 그 응용 분야 또한 광범위하다고 할 수 있다. 그러나 무선통신으로 이루어지는 인증체계이기 때문에 보안의 취약성 또한 배제할 수 없는 위험요소이다[1]-[3]. 우리는 이와 같은 보안에 취약한 RFID의 인증 프로토콜을 혼돈계의 신호를 이용하여 보안을 개선하는 연구를 진행하였다.

혼돈계를 이용한 보안통신 방법은 난수와 유사한 혼돈 신호에 정보를 숨겨 전송시키는 방법으로 감청자에 의해 무단으로 유출된 데이터 역시 잡음과 유사하기 때문에 정보를 추출할 수 없어 보안에 강한 특성을 갖게 된다. 또한 혼돈 신호는 서로 같은 초깃값과 매개변수로 재생산할 수 있기 때문에 초깃값이 공유된다면 송신 측에서 혼돈 신호로 암호화된 데이터는 수신 측에서 발생한 같은 혼돈신호로 복호화 할 수 있게 된다. 또한 혼돈계의 동기화를 위해 전송되는 초깃값 정보를 보호하기 위하여 잡음을 동기화방법으로 선택하고 그 결과로 새로운 RFID 보안 프로토콜을 설계하였다.

Ⅱ. 관련 연구

2.1 혼돈계의 특성

혼돈계에 대한 연구는 현재 이학 분야에서 주로 이루어지고 있고 연구 내용 또한 혼돈계의 특성을 분석하는 내용이 주를 이루고 있다. 우리는 이런 연구결과를 공학적 관점에서 고찰하고 보안 통신에 응용하는 연구를 진행하였다. 혼돈계에서 발생하는 신호는 매개 변수에 의해 제어되고, 그 신호는 난수와 유사한 특성이 있다. 같은 매개변수와 같은 초깃값으로 계산된 혼돈 신호는 서로 같고 재생성할 수 있다. 초깃값의 미세한 차이는 같은 매개변수의 혼돈계라도 시간이 지날수록 전혀 다른 궤적을 그리면 신호를 발생시킨다. 위와 같은 특성을 초기치 민감성이라고 한다[4]-[6]. 위에 설명된 내용 중 매개변수 의존성, 유사난수 특성, 재생성의 특성은 혼돈계를 암호화에 적용하기 좋은 특징이고, 초기치 민감성은 외부 공격에 강인한 특징이라고 할 수 있다.

우리는 매개변수에 의한 혼돈계의 특성을 파악하기 위해 대표적인 1차원 계차방정식인 가우스-맵(Gauss-map)을 선택하고 시뮬레이션으로 특성을 분석하였다. 가우스-맵은 혼돈계 연구에 많이 사용되는 로지스틱-맵(Logistic-map)과 유사한 특성이 있어 응용 연구에 많이 사용되는 혼돈계이다.

$$x_{n+1} = \alpha\, x_n(1 - x_n) \tag{1}$$

$$x_{n+1} = \exp(-\alpha\, x_n^2) + \beta \tag{2}$$

로지스틱-맵과 가우스-맵의 형태를 식 (1)과 식 (2)에 보인다. 식 (2)에서 보인 가우스-맵을 사용하여 매개변수 값에 따른 혼돈 신호의 유사난수 특성을 검증하기 위하여 β 값을 -0.27145로 고정하고 α 값을 1.0부터 10.0까지 0.01 씩 변화시키면 계산하였고 계산된 x_{n+1}값을 α 축 위에 도식화하여 그 결과를 그림 1에 보인다.

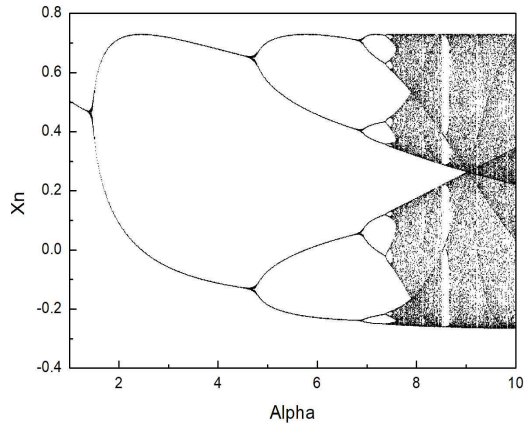

그림 1. 가우스-맵의 갈래질 도표
Fig. 1. Bifurcation diagram of gauss-map

2.2 혼돈계의 동기화

혼돈계의 동기화는 서로 다른 궤적으로 움직이고 있는 두 개의 혼돈계가 외부 신호의 영향으로 일정 시간 이후 같은 궤적으로 움직이는 현상을 말한다. 혼돈계의 동기화는 동기화 결과에 따라 크게 완전 동기화와 위상 동기화를 나누어지고 그 내용은 다음과 같다[7].

① 완전 동기화 (Identical Synchronization)
서로 다른 궤적을 나타내고 있는 두 개의 혼돈계가 외부 신호의 영향으로 점차 같은 궤적을 나타내는 동기화로 위상과 신호가 모두 일치한다.

② 위상 동기화 (Phase Synchronization)
서로 다른 궤적을 나타내고 있는 두 개의 혼돈계가 외부 신호의 영향으로 위상의 차는 일정하게 유지되지만, 신호는 일치 하지 않는 동기화를 말한다.

우리는 위의 동기화 방법 중 완전 동기화를 RFID 보안 통신에 적용하기 위해 리더와 태그에 혼돈계를 적용하여 보안 채널을 구축하는 연구를 진행하였다.

2.3 기존의 RFID 인증 프로토콜

기존의 대표적인 RFID 인증 프로토콜은 S. A. Weis등에 의해 개발된 해쉬-락 인증 프로토콜과 해쉬-락의 문제점을 해결하기 위해 개발된 랜덤 해쉬-락 인증 프로토콜 등이 있다[8].

해쉬-락 인증 방법은 데이터 센터에 사전에 저장되어 있는 {Key, ID} 값을 해쉬(Hash) 함수를 사용하여 태그에 저장된 값과 일치하는지를 확인하는 인증 방법으로 그 내용을 그림 2에 보인다.

랜덤 해쉬-락 인증 방법은 해쉬-락 인증 프로토콜에서 MetaID 값이 유출되었을 때 발생하는 보안 문제를 해결하기 위해 개발된 방법으로 인증 시 리더의 요구에 의한 태그의 전송 값에 난수를 포함하여 MetaID를 변형 시켜 보안을 강화한 방법이다. 그 내용을 그림 3에 보인다.

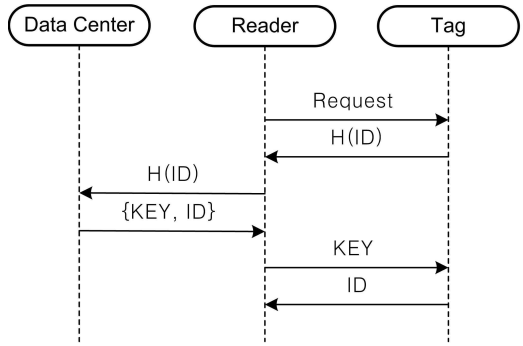

그림 2. 해쉬-락 인증 프로토콜 구조
Fig. 2. Architecture of hash-lock protocol

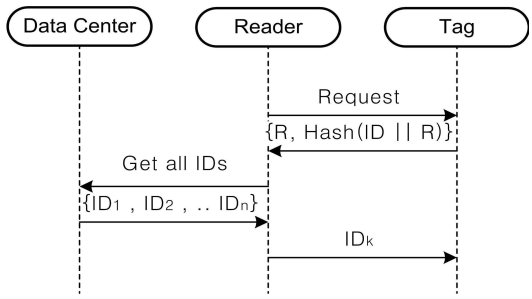

그림 3. 랜덤 해쉬-락 인증 프로토콜 구조
Fig. 3. Architecture of randomized hash-lock protocol

III. 제안된 RFID 보안 프로토콜

우리는 잡음을 이용한 혼돈계의 완전 동기화 현상을 RFID 통신에 적용하기 위해 잡음의 크기에 따른 동기화 현상을 실험하였고, 그 결과를 RFID에 적용하여 새로운 RFID 보안프로토콜을 설계하였다.

3.1 혼돈계의 잡음 동기화

우리는 리더와 태그의 보안 통신을 위해 혼돈계의 초깃값과 매개변수의 노출을 최소화할 수 있는 잡음 동기화 방법을 선택하였다.

$$\begin{cases} x_{n+1}^{(r)} = G(x_n^{(r)}) + \alpha\xi_n \\ x_{n+1}^{(t)} = G(x_n^{(t)}) + \alpha\xi_n \end{cases} \quad (3)$$

잡음 동기화 방법을 적용한 통신방법은 초기 인증 단계의 통신 내용이 잡음 신호이기 때문에 도청 공격에 강한 특성을 보이게 된다[9].

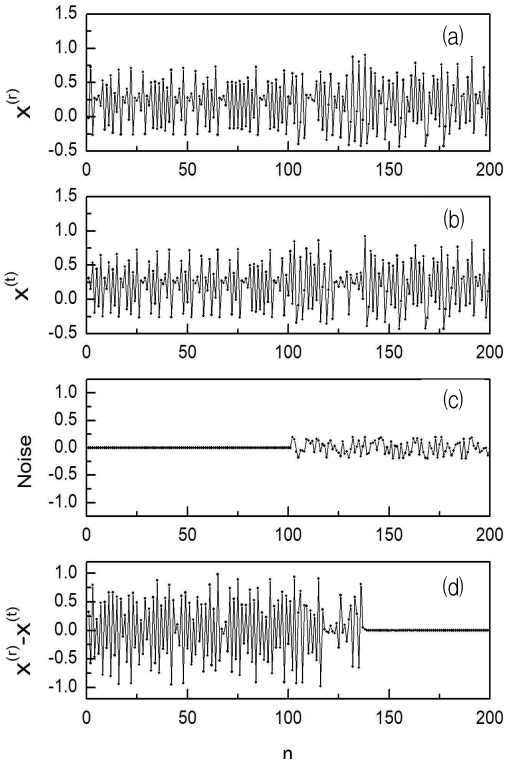

그림 4. 동기화 시계열 그래프
Fig. 4. Temporal behavior of synchronization

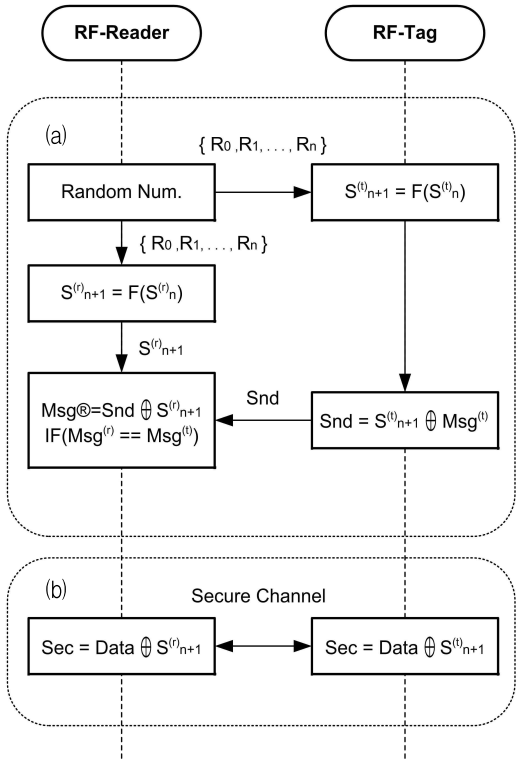

그림 5. 제안된 RFID 보안 프로토콜 구조
Fig. 5. Architecture of suggested RFID protocol

식 (3)에서 ξ_n은 잡음 신호이고 α 값은 가중치 값이다. 실험 결과 내용을 그림 4에 보인다.

(a)와 (b)는 각각 $x^{(r)}$과 $x^{(t)}$의 혼돈신호이고 (c)는 잡음의 가중치 α값을 0.4로 설정하고 발생시킨 신호이며 가중치의 크기는 동기화 시간을 결정한다. (c) 에서 n이 100인 지점부터 잡음을 인가시킨 것을 확인할 수 있다. (d)는 완전 동기화 확인을 위한 $x^{(r)}-x^{(t)}$ 값으로 n 값이 140 일 때부터 완전 동기화가 된 것을 확인할 수 있다. 우리는 잡음 인가 후 n 값을 50이전에 동기화를 시키기 위해 α값을 0.4로 설정했다.

3.2 동기화 RFID 프로토콜

서로 다른 궤적으로 움직이고 있는 두 개의 혼돈계에 같은 잡음을 인가했을 때 일정 시간 동안 동기화 과정을 거친 후 완전 동기화가 이루어지는 것을 실험으로 확인했다[10][11].

우리는 실험 결과를 RFID 통신에 적용하기 위하여 새로운 보안 프로토콜을 설계하였고, 그 내용을 그림 5에 보인다.

그림 5의 (a) 구간은 잡음 신호를 이용한 완전 동기화로 리더와 태그의 초기 인증 과정을 나타낸 도표이다. (b) 구간은 동기화 인증 이후 생성된 보안 채널로 통신이 이루어지는 내용을 나타낸 도표이다. (a) 구간을 살펴보면 리더와 태그의 초기 동기화 인증 과정에서 위험에 노출될 수 있는 내용은 난수 신호인 $R_0,R_1,\cdots,R_n$과 동기화 확인을 위해 $\oplus$로 암호화된 Snd 뿐 이므로 도청 공격으로 정보가 유출되어도 시스템의 정보를 파악할 수 없게 되어 강한 통신 방법이라고 할 수 있다.

Ⅳ. 결 론

RFID 통신은 물류 및 생산 관리에 사용하고 있던 바코드와 같은 접촉식 인증 방식을 비접촉식 인증 방식으로 변형시킨 대표적인 통신방법이라 할

수 있다. RFID는 비접촉 인증 특성 때문에 그 응용 범위가 넓어 점차 산업 분야 및 사회 전반에 자리 잡고 있다. 그러나 무선을 사용하고 있는 RFID는 통신내용이 항상 위험에 노출되어있어 보안에 취약한 특성이 있다. 연구자들은 이런 위험 요소를 제거하기 위하여 해쉬-락 인증 프로토콜, 랜덤 해쉬-락 인증 프로토콜들을 개발하였지만 공격 방법 또한 지능적으로 발전하고 있어 새로운 보안 방법이 필요하다고 생각된다. 우리는 이런 문제를 해결할 방법은 RFID통신 중 시스템에 관련된 정보를 최소화하는 것으로 생각한다. 우리는 먼저 동기화를 이용하여 암호화 채널을 생성하는 방법으로 RFID의 보안 통신을 설계하였고, 추후 통신내용에 시스템 정보를 최소화하기 위해 잡음으로 동기화되는 방법을 적용하였다. 설계된 내용은 시뮬레이션 결과와 프로토콜 설계이지만 추후 후속연구가 이루어진다면 기존의 통신 프로토콜을 대체할 수 있는 강인한 프로토콜이 될 것으로 예측된다.

References

[1] 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.

[2] 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. 858-867, Jul. 2011.

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

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

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

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

[7] X. S. Yang, "Concepts of synchronization in dynamical systems", Phys. Lett. A. 260, pp. 340-344, Sep. 1999.

[8] S. Weis, S. Sama, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System", Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Nov. 2004.

[9] G. S. Yim and H. S. Kim, "Chaos-based Image Encryption Scheme using Noise- induced Synchronization", Journal of the Korea Society of Computer and Information, Vol. 13, No. 5, pp. 155-162, May 2008.

[10] G. S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameter Chaotic System", Korea Information Assurance Society, Vol. 8, No. 3, pp. 57-64, Mar. 2008.

[11] H. S. Kim and G. S. Yim, "Design of digital photo frame for close-range security using the chaotic signals synchronization", Journal of the Korea Society of Computer and Information, Vol 16. No. 2, pp. 201-206, Feb. 2011.

저자소개

임 거 수 (Geo-Su Yim)

1997년 3월 : 배재대학교 물리학과(이학사)
1999년 3월 : 배재대학교 물리학과(이학석사)
2008년 3월 : 서강대학교 물리학과(이학박사)
2008년 3월 ~ 현재 : 배재대학교 전기공학과 교수
관심분야 : 시계열분석, 머신러닝, 보안통신