Regular paper | Journal of the KIECS. pp. 981-986, vol. 15, no. 5, Oct. 31. 2020, t. 103, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2020.15.5.981

키값 동기된 혼돈계를 이용한 IoT의 보안채널 설계

임거수*

IoT Security Channel Design Using a Chaotic System Synchronized by Key Value

Geo-Su Yim*

요 약

사물인터넷은 장소나 시간에 제약 없이 센서와 통신 기능이 내장된 사물이 사람과 사물에 상호 작용이 가능하도록 구성된 사물 공간 연결망을 말한다. IoT는 인간의 편의를 위한 서비스 목적으로 개발된 연결망이지만 현재는 전력전송, 에너지관리, 공장자동화와 같은 산업 전반에 그 사용범위가 확대되고 있는 상태이다. 그러나 IoT의 통신프로토콜인 MQTT는 푸시 기술 기반의 경량 메시지 전송 프로토콜로 보안에 취약함을 갖고 있고 이것은 개인정보 침해나 산업정보 유출 같은 위험성이 내재되어 있다고 할 수 있다. 우리는 이런 문제점을 해결하기 위해 경량 메시지전송 MQTT 프로토콜에 서로 다른 혼돈계가 임의의 값으로 동기화되는 특성을 이용하여 보안 채널을 생성하는 동기화 MQTT 보안 채널을 설계하였다. 우리가 설계한 통신 채널은 혼돈 신호의 난수 유사성, 초기치 민감성, 신호의 재생산성과 같은 특성을 이용한 방법으로 잡음 채널에 정보를 전송하는 방법이라고 할 수 있다. 우리가 제시한 킷값으로 동기화된 암호화 방법은 경량 메시지 전송 프로토콜에 최적화된 방법으로 IoT의 MQTT에 적용된다면 보안 채널 생성에 효과적이라고 할 수 있다.

ABSTRACT

The Internet of Things refers to a space-of-things connection network configured to allow things with built-in sensors and communication functions to interact with people and other things, regardless of the restriction of place or time.IoT is a network developed for the purpose of services for human convenience, but the scope of its use is expanding across industries such as power transmission, energy management, and factory automation. However, the communication protocol of IoT, MQTT, is a lightweight message transmission protocol based on the push technology and has a security vulnerability, and this suggests that there are risks such as personal information infringement or industrial information leakage. To solve this problem, we designed a synchronous MQTT security channel that creates a secure channel by using the characteristic that different chaotic dynamical systems are synchronized with arbitrary values in the lightweight message transmission MQTT protocol. The communication channel we designed is a method of transmitting information to the noise channel by using characteristics such as random number similarity of chaotic signals, sensitivity to initial value, and reproducibility of signals. The encryption method synchronized with the proposed key value is a method optimized for the lightweight message transmission protocol, and if applied to the MQTT of IoT, it is believed to be effective in creating a secure channel.

키워드

IoT, MQTT, Security ProtocoL, Chaotic Signal, Chaotic Map
사물인터넷, MQTT, 보안 프로토콜, 혼돈신호, 혼돈 맵

* 배재대학교 AI·전기공학과 (lomac@pcu.ac.kr)
• 접 수 일 : 2020. 09. 20
• 수정완료일 : 2020. 10. 02
• 게재확정일 : 2020. 10. 15
• Received : Sep. 20, 2020, Revised : Oct. 02, 2020, Accepted : Oct. 15, 2020
• Corresponding Author : Geo-Su Yim
Dept. of AI·Electrical Engineering, PaiChai University,
Email : lomac@pcu.ac.kr

Ⅰ. 서 론

사회와 산업의 급속한 발달은 많은 정보를 생산하게 되었고 많은 정보로 인하여 새로운 서비스가 제공되고 있다. 그중 가장 대표적인 서비스를 위한 정보 생산 방법이 사물인터넷(IoT:Internet of Thing)일 것이다. 사물인터넷은 사람의 편의를 도모하기 위한 서비스를 제공하기 위하여 화분이나 도어락과 같은 사소한 물건에서부터 냉장고, 텔레비전과 같은 가전제품 그리고 산업체에서 사용되고 있는 전력, 에너지 제어 장치까지 그 적용 범위가 방대하다고 할 수 있다.

그러나 사물인터넷의 통신 방법은 푸시기술 기반의 경량화 통신을 사용하고 있기 때문에 보안에 대한 취약한 특성을 가지고 있다[1-3]. 우리는 이와 같은 사물인터넷의 보안을 강화하기 위해 혼돈계를 이용한 암호화 통신 연구를 진행하고 그 결과를 다음에 보인다. 논문의 2장 사전연구에서는 IoT의 통신 방법과 과 보안을 강화하기 위한 혼돈계의 특징과 새롭게 설계된 혼돈계에 대한 내용을 보인다. 3장에서는 설계된 혼돈계를 이용하여 IoT 통신의 보안을 강화하는 새로운 프로토콜을 제시한다. 4장에서는 새롭게 설계된 혼돈계를 이용한 IoT 통신의 안전성을 제시한다.

Ⅱ. 사전연구

2.1 IoT 통신

IoT(Internet of Things)는 사물인터넷으로 정보를 생성할 수 있는 모든 장치가 연결되어 상호협력으로 센싱, 네트워킹, 정보처리 등을 처리할 수 있는 관계를 형성하는 사물 공간 연결망이라고 할 수 있다. 사물인터넷의 통신 프로토콜은 MQTT와 CoAP등과 같은 종류가 있고, 그중 MQTT가 많이 사용되고 있는 추세이다. MQTT 통신 프로토콜의 데이터 흐름을 그림 1.에 보인다[4, 5].

MQTT(Message Queuing Telemetry Transport)의 구조는 정보를 중재하는 Broker를 기준으로 정보를 게시하는 Publisher와 정보를 구독하는 Subscriber가 Broker에 디렉토리 구조로 되어 있는 Topic을 참조하며 정보를 공유하는 구조로 되어있어 사용과 관리가 비교적 간단한 편이다. 그러나 사용상 편의를 제공하는 MQTT의 통신은 푸시 기반 경량 통신 프로토콜로 보안에 대한 취약함을 나타내고 있다.

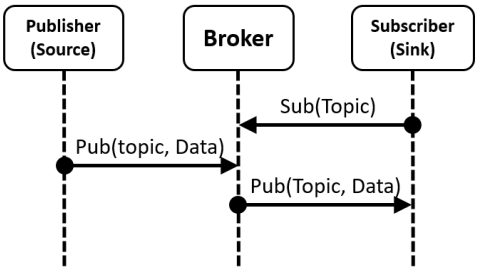

그림 1. IoT(MQTT) 전송 프로토콜
Fig. 1 Protocol of IoT(MQTT) Transport

2.2 혼돈계 설계

우리는 보안이 취약한 IoT의 MQTT통신에 새로운 암호화 통신 방법을 적용하기 위해 새로운 혼돈계를 설계하였다.

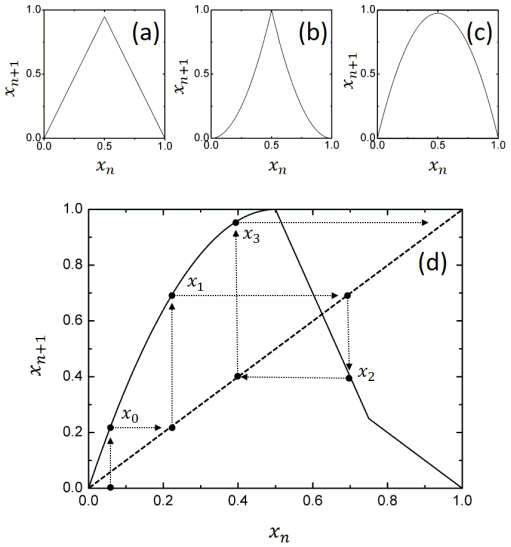

그림 2. 혼돈시스템의 리턴-맵
Fig. 2 Return-map of chaotic system

디지털 통신에 사용되는 혼돈계는 맵 구조의 혼돈계로 혼돈계에서 발생하는 신호는 초깃값의 미세한 변화에 대하여 이후 값에 큰 변화가 생기고 그 큰 변

화가 더 큰 변화를 만들어 예측할 수 없는 신호를 발생시킨다. 그리고 발생하는 신호는 난수와 유사하지만, 이전값에 의해 이후 값이 계산되어 재생산이 가능한 난수라고 할 수 있다. 이와 같은 특성을 통신을 하는 장치들에게 적용하기 위하여 초기단계에 동기화가 이루어져 같은 혼돈 신호를 발생시키게 된다면, 통신에 참여한 장치들은 난수 값으로 생성된 통신 채널을 통해 비밀통신이 가능하게 될 것이다[6-8].맵 구조의 혼돈계에서 혼돈 신호가 발생하는 구조를 이해하고 분석하기 위하여 사용되는 것이 리턴-맵이다. 우리는 기존의 대표적인 혼돈계의 맵과 우리가 설계한 맵의 구조를 그림 2.에 보인다.

그림 2.의 (a)는 Tent-map, (b)는 Quadratic-map, (c)는 Logistic-map 그리고 (d)는 우리가 설계한 새로운 맵이다. 그리고 모든 그림은 x_n과 x_{n+1}에 대한 관계를 나타낸 리턴-맵이다. 우리가 설계한 맵의 구조는 혼돈 신호의 복잡도를 높이기 위해 왼쪽 부분은 2차 함수로 구성하고, 오른쪽 직선 구간은 빠른 수렴과 0 부근에서 발산하도록 급한 계단 구조를 같도록 설계하였다. 설계 이후 모양이 상어의 지느러미 형상을 하고 있어서 이후 Shark-map으로 명명하기로 하고 내용을 수식으로 표현하여 식 1.에 보인다.

$$\begin{aligned} &\mathrm{if}(x_n \le 0.5) \\ &\quad x_{n+1} = 1.0 - 4.0(0.5 - x_n)^2 \\ &\mathrm{if}(0.5 < x_n \le 0.75) \\ &\quad x_{n+1} = 3.0(0.75 - x_n) + 0.25 \\ &\mathrm{if}(0.75 < x_n) \\ &\quad x_{n+1} = (1.0 - x_n) \end{aligned} \tag{1}$$

2.3 혼돈의 동기화

우리는 그림 1.에서 보인 IoT의 구조에서 Broker를 기준으로 Publisher와 Subscriber가 Shark-map에서 같은 x_n값을 갖기 위하여 동기화 방법을 선택하고 연구를 진행하였다[9, 10]. 보안을 위한 동기화 방법으로는 잡음을 이용한 방법이 많이 사용되었지만 잡음은 많은 정보가 필요하기 때문에 우리는 킷값을 반복적으로 인가하여 동기화되는 방법을 선택하였고 그 결과를 그림 3.에 보인다. 그림 3.의 (c)에 보인 동기화 비밀 킷값은 “CHARACTERS”라는 대문자 문자열을 사용하였고 각각의 문자는 식 2.를 이용하여 문자 ASCII 코드를 0과 1 사이에 분포하도록 계산하였고, 결합 세기(Coupling Strength)를 0.3으로 하여 반복적으로 인가하여 동기화시켰다.

$$Key = (Character - 65) \times (1/25) \tag{2}$$

그림의 (a)와 (b)는 서로 다른 초깃값으로 계산된 Shark-map의 $x(n)^p$와 $x(n)^s$의 시계열이고, (c)는 동기화를 위한 문자열 킷값이 반복적으로 인가되고 있는 $K(n)$의 시계열이다. (d)는 $x(n)^p$와 $x(n)^s$의 차이 값으로 n값이 110에서 완전 동기화된 것을 확인 할 수 있다.

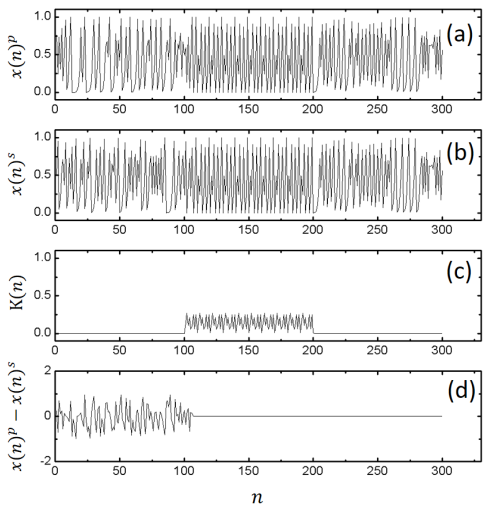

그림 3. 동기화의 시계열
Fig. 3 Temporal behavior of synchronization

III. 제안된 IoT 통신 프로토콜

우리는 보안을 위해 새롭게 설계한 Shark-map 혼돈계에 문자열 킷값을 반복적으로 인가하여 동기화되는 결과를 2장 3절에서 보였다. 보안이 취약한 IoT의 MQTT 통신을 강화하기 위해 Shark-map의 동기화를 이용한 보안 프로토콜의 설계하고 그 내용을 그림 4.에 보이고 각 단계별 과정을 아래에 보인다[11, 12].

(a) 단계는 동기화 단계로 Broker에서 동기화에 사용될 문자열 킷값을 Publisher와 Subscriber에게 전송하는 단계이다. 각각 창치들은 전송받은 킷값 K를 동기화 함수 F_{sync}로 계산하여 동일한 값의 $\tilde{x}_{n+1}$, $\hat{x}_{n+1}$ 그리고 x_{n+1}을 계산한다.

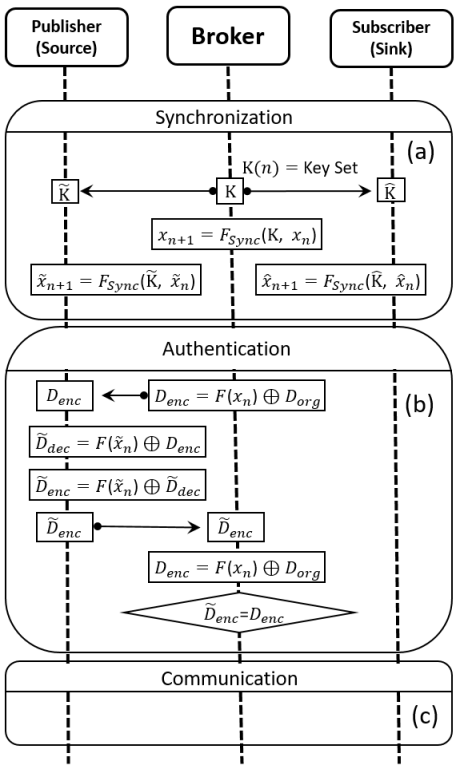

그림 4. 제안된 IoT 프로토콜의 구조
Fig. 4 Structure of proposed IoT protocol

(b) 단계는 인증 단계이다. 동기화 단계에서 계산된 동일한 x_n값을 이용하여 인증 코드를 XOR로 암호화하여 Publisher에게 전송한다. Publishers는 전송된 값을 $\tilde{x}_n$으로 복호화하고 이후 계산된 $\tilde{x}_{n+1}$으로 암호화하여 Broker에게 전송한다. Broker는 수신된 값을 이후 계산된 x_{n+1} 으로 복호화하여 계산된 값과 초기에 전송한 인증 코드를 비교하여 인증을 완료한다.

(c) 단계는 통신 단계로 데이터를 통신하는 방법은 인증단계와 동일하게 진행되고 인증 코드가 아닌 데이터를 전송하게 된다.

Ⅳ. 이미지 암호화 평가

우리는 본 논문에서 제안한 IoT 프로토콜의 암호화 정도를 가시화하기 위하여 임의의 컬러 이미지를 8비트 흑백 이미지로 변환시키고 Shark-map에서 발생되는 혼돈 신호를 이용하여 이미지의 암호화 및 복호화를 진행 하였다. 그림 5의 (a)와 (b)는 원본 이미지와 히스토그램을 나타내고, (c)와 (d)는 암호화된 이미지와 히스토그램을 나타낸다.

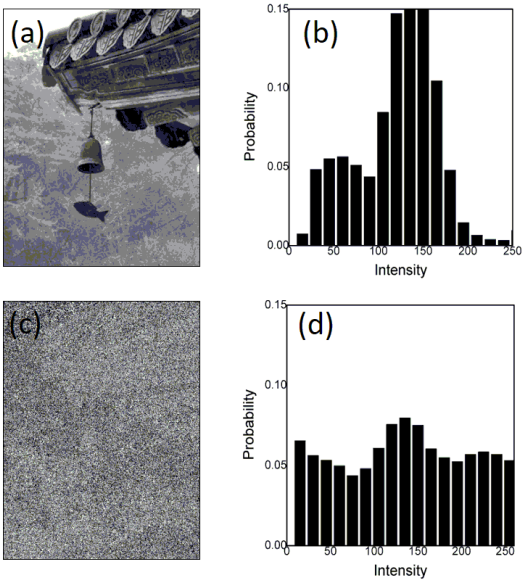

그림 5. 암호화된 이미지의 히스토그램
Fig. 5 Histogram of the encrypted image

Ⅴ. 안정성 평가

4.1 기밀성(Confidentiality)

IoT 보안 통신에서 기밀성이란 통신에 참여한 송·수신 장치인 Broker, Publisher, Subscriber에게만 정보가 공개되고 참여하지 않은 송·수신 장치는 정보를

열람할 수 없는 것을 의미한다. 우리가 제시한 통신은 혼돈 신호의 유사난수 신호를 채널로 하므로 승인되지 않은 장치에 의한 정보 열람은 난수와 같아서 정보를 파악할 수 없게 되어 기밀성이 보장된다.

4.2 무결성(Integrity)

IoT 통신에서 무결성이란 정보가 외부의 공격이나 악의에 의한 변조로 왜곡되지 않는 것을 의미한다. 우리가 제시한 Shark-map은 계차방정식으로 매번 통신이 이루어질 때 이전 값에 의해 이후 값이 계산되는 통신구조이기 때문에 자동으로 확인이 되고 무단으로 왜곡이나 변조가 되었을 때 바로 인지할 수 있어서 무결성이 보장된다.

4.3 가용성(Availiability)

가용성이란 IoT 통신에서 Publisher와 Subscriber가 장애 없이 Broker에 정상적으로 정보를 게시하고 열람할 수 있는 것을 의미한다. 우리가 제시한 Shark-map 혼돈계는 3구간으로 나누어져 구간별 각각 2차원과 1차원의 간단한 연산으로 계산되는 방정식으로 처리가 간단하여 정보에 대한 게시나 열람이 제한 없이 이루어질 수 있어서 가용성이 보장된다.

Ⅵ. 결 론

사회가 발달하고 정보량이 증가하면서 편의성을 고려한 초연결사회를 구성하기 위해 IoT의 필요성이 대두되고 있고 반면에 안전하게 사물 정보를 공유하기 위해 보안에 관한 관심 또한 급증하고 있다. 우리는 사물인터넷의 보안을 강화하기 위해 혼돈계를 적용하기로 하고 기존에 알려지지 않은 새로운 맵을 설계하였고, 그 이름을 Shark-map이라 정했다. 우리가 설계한 맵은 기존의 맵과 달리 3구간으로 구분된 맵으로 구조는 간단하지만 발생되는 신호가 복잡하여 맵의 구조를 파악하기 어려운 장점을 가지고 있다.

우리는 설계한 맵을 IoT에 적용하기 위해 킷값을 반복적으로 인가하는 동기화 방법을 선택하였고 그 내용을 IoT의 MQTT 통신에 적용하는 연구를 진행하였다. 우리가 제안한 방법은 혼돈 신호를 이용하여 보안 채널을 생성하고 그 채널을 이용하여 데이터를 전송하는 방법으로 혼돈 신호의 초기치 민감성과 난수 유사성 그리고 재 생산성을 이용하기 때문에 보안의 강도가 강하다고 할 수 있다. 또한 Shark-map의 구조가 간단하므로 저용량 저가격의 IoT장치에 암호화를 적용하기 용이할 것으로 생각된다.

References

[1] S. H. Oh, S. K. Ko, S. C. Son, B. T. Lee, and Y. S. Kim, “IoT Device Management Standard Protocol Trends in Mobile Communications,” *Electronics and Telecommunications Trends, Trans. Aerospace and Electronic Systems,* vol. 30, no. 1, 2015, pp. 94-101.

[2] Y. H. Jeon, “A Study on the Security Modeling of Internet of Things(IoT),” *J. of Korean Institute of Information Technology,* vol. 15, no. 12, December. 2017, pp. 17-27.

[3] J. Y. Ko. So. G. Lee, J. W. Kim, and C. H. Lee, “Technologies Analysis based on IoT Security Requirements and Secure Operation System,” *j. of The Korea Contents Association*, vol. 18, no. 4, March 2018, pp. 164-177.

[4] N. H. Kim, and C. S. Hong, “Lightweight Cryptography Algorithm basd Secure MQTT Protocol,” *j. of The Korean Institute of Information Scientists and Engineers*, vol. 16, no. 12, December 2016, pp. 757-759.

[5] N. H. Kim, and C. S. Hong, “Secure MQTT Protocol based on Attribute-Based Encryption Scheme,” *j. of The Korean Institute of Information Scientists and Engineers*, vol. 45, no. 3, December 2018, pp. 195-199.

[6] G. L. Baker, and J. P. Gollub, *Chaotic Dynamics an Introduction.* Cambridge University Press, 1996.

[7] H. G. Schuster, *Deterministic Chaos: An Introduction 2nd editionl.* Wiley-VCH, 1997.

[8] E. Ott, *Chaose in Dynamical Systems Second Edition.* Cambridge University Press, 2002.

[9] G. -S. Yim, and H. -S. Kim “Chaos-based

Image Encryption Scheme using Noise-induced Synchronizaiton," *j. of The Korea Society of Computer and Information*, vol. 13, no. 5, September 2008, pp. 155-162.

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

[11] G. -S. Yim "IoT MQTT Security Protocaol Design Using Chaotic Signals," *j. of The Korea Institute of Information & Electronic Communication Technology*, vol. 11, no. 6, December 2018, pp. 778-782.

[12] G. -S. Yim "RFID Security Protocol Design Using Noise Synchronization of Chaotic Signal," *j. of Korean Institute of Information Technology*, vol. 16, no. 10, October 2018, pp. 119-123.

저자 소개

임거수(Geo-Su Yim)

1996년 배재대학교 물리학과 졸업(이학사)
1999년 배재대학교 대학원 물리학과 졸업(이학석사)
2004년 서강대학교 대학원 물리학과 졸업(이학박사)
2008년 ~현재 배재대학교 전기공학과 교수
※ 관심분야 : 시계열분석, 머신러닝, 암호화