Journal of KIIT. Vol. 24, No. 3, pp. 91-99, Mar. 31, 2026. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2026.24.3.91

구간별 선형 혼돈계를 이용한 스마트그리드 IoT 보안 통신 설계

임거수*, 송창후**

Smart Grid IoT Secure Communication Design using Piecewise Linear Chaotic Maps

Geo-Su Yim*, Chang-Hoo Song**

본 결과물은 2025년 교육부 및 대전광역시의 재원으로 대전RISE센터의 지원을 받아 수행된
지역혁신중심 대학지원체계(RISE)의 결과입니다.

요 약

스마트그리드 환경은 효율적인 에너지 관리를 위해 사물인터넷(IoT) 기반 통신 기술을 활용하여 전력 계통에서 발생하는 운영 데이터를 실시간으로 수집하고 이를 에너지 관리 및 운영 최적화에 활용하고 있다. 그러나 스마트그리드는 개방형 네트워크 기반에서 운영되기 때문에 무단 공격에 취약한 환경을 갖는다. 특히 MQTT 프로토콜은 기본적인 보안 기능이 미흡하여 전력 정보 유출뿐만 아니라 사용자 개인정보 침해로도 이어질 가능성이 높다고 할 수 있다. 본 논문에서는 이러한 보안의 취약성을 해결하기 위해 MQTT의 경량성을 유지하면서도 보안을 강화할 방법으로 PWLCM(Piecewise Linear Chaotic Map)을 적용한 보안 통신 방법을 제안한다. PWLCM은 균일한 분포 특성으로 통계적 공격에 강인하며, 낮은 연산 비용으로 경량 시스템에 적합하여 기존 혼돈맵 기반 방법보다 우수한 장점이 있다.

Abstract

Smart grid environments leverage Internet of Things (IoT)-based communication technologies to efficiently manage energy, collecting operational data generated from the power system in real time and utilizing this data for energy management and operational optimization. However, because smart grids operate over open networks, they are vulnerable to unauthorized attacks. In particular, the MQTT protocol lacks basic security features, making it highly susceptible to not only power data leaks but also user privacy breaches. To address these security vulnerabilities, this paper proposes a secure communication method that applies the Piecewise Linear Chaotic Map (PWLCM) to enhance security while preserving MQTT's lightweight characteristics. PWLCM offers advantages over existing chaotic map-based methods, including robustness against statistical attacks due to its uniform distribution and suitability for lightweight systems owing to its low computational cost.

Keywords

dSmart grid, IoT, MQTT, secure communication, chaotic map, synchronization

* 배재대학교 전기·전자공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-2407-2768
** 배재대학교 전기·전자공학과
- ORCID: https://orcid.org/0009-0009-5053-184X

· Received: Feb. 03, 2026, Revised: Mar. 10, 2026, Accepted: Mar. 13, 2026
· Corresponding Author: Geo-Su Yim
Dept. of Electrical and Electronic Engineering
Paichai University, Daejeon, Korea
Tel.: +82-42-520-5373, Email: lomac@pcu.ac.kr

Ⅰ. 서 론

사회의 발전과 산업의 고도화로 정보의 생산과 활용이 급격히 증가하고 있다. 이에 따라 정보의 흐름은 컴퓨터 중심의 통신에서 사물과 사물, 사물과 사람으로 그 범주가 확장되고 있고, 이와 같은 네트워크를 다변화할 수 있게 하는 기술이 사물인터넷(IoT, Internet of Things)이다.

IoT는 일상에서 쉽게 접할 수 있는 가전제품에서부터 산업용 장비까지 모든 사물에 각종 센서와 제어장치를 적용하여 초연결 사회가 구현될 수 있는 기반을 제공하고 있다. 특히, 스마트그리드 환경은 수많은 IoT 장치가 유기적으로 연결되어 안정적이고 효율적인 전력 계통을 운영할 수 있도록 정보를 제공하고 있다[1]. 스마트그리드에서 사용되는 IoT 통신은 저전력 및 경량화를 요구하고 있고, 대표적인 프로토콜은 MQTT, CoAP 등이 있다.

MQTT는 Publish와 Subscribe 구조를 기본으로 하여 다수의 장치와 효율적인 메시지 전송을 가능하게 하지만, 보안이 취약한 단점을 가지고 있어[2], 도청, 위변조, 재전송 등의 공격에 취약한 특성이 있다[3]. 이와 같은 위험은 전력을 스마트그리드로 운용하고 있는 국가 기반 시설에는 심각한 위험으로 작용할 수 있다.

본 논문에서는 이러한 문제를 해결하기 위해 균등분포 특성을 갖는 구간별 선형 혼돈계를 설계하고 스마트그리드 IoT의 MQTT 통신에 적용한 새로운 경량 보안 통신 프로토콜을 제시한다. 제안된 혼돈계는 선형 연산을 기반으로 설계되어 계산 복잡도를 최소화하고, 혼돈 시스템의 고유한 특성인 초기치 민감성과 난수 유사성을 활용하여 보안 강도를 강화한 경량 암호 기법이다.

그림 1의 스마트그리드는 기존의 단방향 전력망에 정보통신기술(ICT, Information and Communications Technology) 을 통합하여 전력 생산, 송전, 배전에 이르는 전력 계통 전 과정에서 양방향 정보 교환과 지능형 제어를 가능하게 한 차세대 전력 인프라를 의미한다[4]. 이러한 구조는 실시간 운영 데이터를 기반으로 전력 시스템의 효율성, 안정성, 지속 가능성을 향상하며, 소비자가 전력 수요관리 과정에 능동적으로 참여할 수 있는 기반을 제공한다[5].

전통적인 전력망은 발전소에서 생산된 전력을 소비자에게 일방적으로 공급하는 선형 구조로 되어 있어 부하 변동에 대한 대응, 분산 전원 연계, 설비 상태에 대한 예측 등에 한계를 가지고 있다. 그러나 스마트그리드는 실시간 전력 사용량, 분산 전원 발전량, 계통의 상태 등 다양한 정보를 양방향으로 수집 공유하는 지능형 전력 시스템으로 전통적인 전력망의 문제점을 해결할 수 있다.

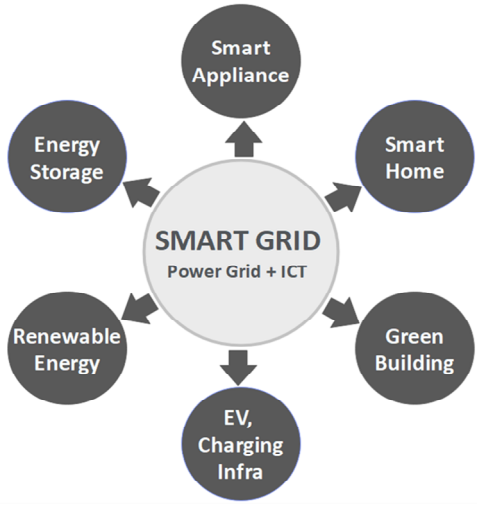

그림 1. 스마트그리드 흐름도
Fig. 1. Flow diagram of the smart grid

사물인터넷(IoT)은 센서, 내장형 소프트웨어, 네트워크 통신 기능을 갖춘 다양한 물리적 사물들이 인터넷을 통해 서로 연결되어 데이터를 실시간으로 수집하고 교환하는 기술이다. 기존의 정보처리 체계를 개별 장치 중심에서 네트워크 기반의 환경 전체로 확장하는 역할을 하고, 이를 통해 제조, 에너지, 의료, 교통 등 다양한 산업 분야에서 지능화된 서비스 제공과 운영 효율성 향상을 가능하게 한다.

스마트그리드에서 IoT는 전력 흐름, 전압·전류, 부하 상태, 재생에너지 발전량, 전력 품질, 설비 상태 등 전력 계통의 다양한 운영 데이터를 실시간으로 수집하고 전송하여 계통 운영자가 계통 상태를 정확하게 파악하고 자동 제어를 수행할 수 있도록 지원하는 핵심 요소이다. 또한 고급 계량 인프라[6], 감시제어 및 데이터 수집 시스템과 같은 첨단 감독 시스템 역시 동적 전력망의 안정적 운영과 관리 효율성 향상에 중요한 역할을 수행한다.

II. 혼돈계

2.1 혼돈계의 특징

혼돈계는 20세기 중반 이후 비선형 동역학의 특성을 연구하는 과정에서 발전된 비선형 복잡 시스템의 대표적인 형태로 비연속적인 결괏값을 생성하는 이산구조 혼돈계와 연속적인 결괏값 생성하는 미분방정식 형태의 혼돈계로 구분된다.

혼돈계는 결정론적 방정식에 의해 지배되지만, 생성되는 신호는 통계적으로 난수와 유사한 성질을 보이고 있으며[7], 초깃값에 대한 민감성과 결괏값에 대한 장기적인 예측이 불가능한 특성이 있기 때문에 암호화, 보안 통신, 난수발생기 등 다양한 분야에 적용할 수 있는 잠재력을 가지고 있다고 할 수 있다[8].

보안 통신 연구에 활용되는 대표적인 이산 혼돈계는 1차원 형태의 Logistic-map, Tent-map 등이 있고 2차원 형태의 혼돈계는 Henon-map, Ikeda-Map, Duffing-Map 등이 있다.

2.2 Logistic map 혼돈계

로지스틱맵은 생태학적 개체수 변동을 설명하기 위해 로버트 메이(Robert M. May)가 제안한 1차원 이산 비선형 동역학 모델이다. 단순한 형태의 모델이지만 다양한 혼돈계의 현상을 나타내는 대표적인 혼돈계로 널리 연구되고 있다. 로지스틱맵의 이산 방정식을 식 (1)에 보인다. 식 (1)에 매개변수 r값의 변화에 따라 다양한 혼돈 특성을 보이고 r값이 3.9에서 잡음과 유사한 혼돈 신호를 발생한다.

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

2.3 Henon map 혼돈계

해논맵은 프랑스의 수학자 미셸 해논(Michel Henon)이 1976년에 제안한 2차원 이산 비선형 동역한 시스템으로, 간단한 수식으로 복잡한 혼돈 현상과 자기 유사성 구조를 보여주는 대표적인 혼돈계이다. 해논맵의 이산 방정식을 식 (2)에 보인다. 해논맵은 매개변수 a, b에 따라 다양한 동역학적 특성을 보이는 혼돈계이다.

$$\begin{aligned} x_{n+1} &= 1 - a x_n^2 + y_n \\ y_{n+1} &= b x_n \end{aligned} \tag{2}$$

2.4 Tent map 혼돈계

텐트맵은 1차원 이산 비선형 동역학 시스템의 대표적인 혼돈계로 방정식의 형태가 삼각형 구조로 되어 있어 텐트맵이라고 한다. 단순한 구조에서 비선형성과 초깃값 민감성을 나타내며 암호연구에 많이 사용되는 혼돈계이다. 텐트맵의 이산 방정식을 식 (3)에 보인다. 매개변수 β값의 변화에 따라 다양한 혼돈 특성을 보이며, β값이 1.9일때 잡음과 유사한 혼돈 신호를 생성한다.

$$x_{n+1} = \begin{cases} \beta x_n & x_n < 0.5 \\ \beta(1 - x_n) & x_n \geq 0.5 \end{cases} \tag{3}$$

우리는 스마트그리드 보안 통신에 적용하기 위해 텐트맵을 변형한 구간별 선형 혼돈계를 설계하고 그 내용을 다음과 같이 제안한다.

III. 제안된 구간별 선형 혼돈계 모델

3.1 구간별 선형 혼돈계

암호화에 많이 사용되는 텐트맵은 생성되는 혼돈 신호의 분포가 로지스틱맵이나 해논맵에 비해 균등한 특성이 있어 암호화에 유리한 장점이 있다. 그러나 상대적으로 낮은 비선형성으로 보안 적용 시 한계가 존재한다. 본 연구에서는 텐트맵의 비선형을 강화한 구간별 선형 혼돈계(PWLCM, Piecewise Linear Chaotic Map)를 제안하고 보안이 취약한 스마트그리드의 사물인터넷에 적용하는 연구를 진행하였다.

구간별 선형 혼돈계는 입력구간을 여러 개의 구간으로 나누어 각 구간에 서로 다른 선형함수를 적용하여 출력값이 다른 형태를 보이는 변형 이산 혼돈 시스템이다. 제시된 구간별 선형 혼돈계는 구조

는 간단하지만 강한 비선형 동역학 특성과 넓은 혼돈영역을 나타내므로, 사물인터넷과 같은 자원 제약 환경의 통신 시스템에서 경량 암호화 적용에 효과적이라고 할 수 있다.

본 연구에서 사용된 4구간 선형 혼돈계의 방정식을 식 (4)에 보이고 혼돈 신호 발생 구조인 Return map을 그림 2에 보인다.

$$x_{n+1}=\begin{cases}\dfrac{x_n}{p_1}, & 0\le x_n<p_1\\ \dfrac{x_n-p_1}{p_2-p_1}, & p_1\le x_n<p_2\\ \dfrac{p_3-x_n}{p_3-p_2}, & p_2\le x_n<p_3\\ \dfrac{1-x_n}{1-p_3}, & p_3\le x_n<1\end{cases} \tag{4}$$

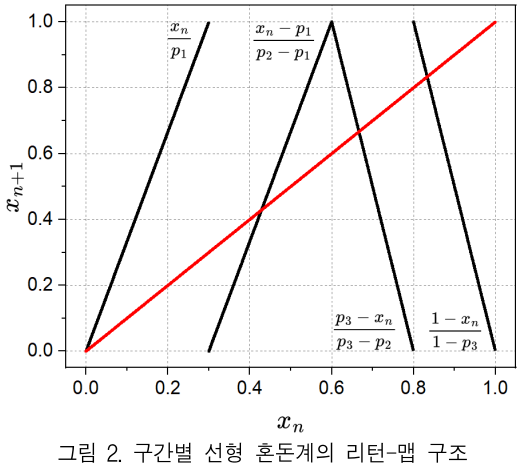

그림 2. 구간별 선형 혼돈계의 리턴-맵 구조
Fig. 2. Return map of the piecewise linear chaos system

Return map은 x_n과 x_{n+1}의 관계를 나타낸 그래프로, 혼돈 신호의 발생 구조를 분석하기 위해 사용된다. 그림 2의 적색 선은 대각선을 나타낸 것이다.

3.2 PWLCM 혼돈계의 특성 분석

혼돈 시스템은 지배방정식의 매개변수에 따라 안정 상태와 혼돈 상태로 전이하며, 다양한 혼돈 특성을 보인다. 보안 통신에서 이러한 매개변수는 공개키로 사용될 수 있으므로, 매개변수 공간 전반에서 일관된 혼돈 특성을 유지하는 것이 암호화 성능 향상에 효과적이라고 할 수 있다.

제시된 구간별 선형 혼돈계의 특성을 파악하기 위해 매개변수 변화에 따른 갈래 질 도표를 그림 3에 보인다.

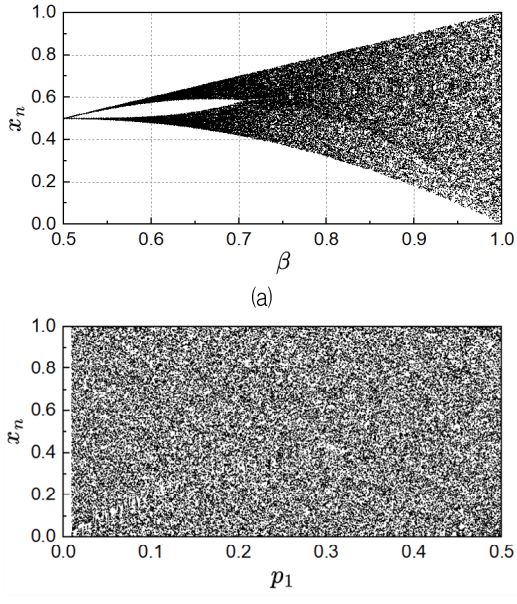

그림 3. 혼돈계의 갈래질 도표
(a) 텐트-맵, (b) 구간별 선형 혼돈계
Fig. 3. Bifurcation plot of the chaotic system
(a) Tent map, (b) Piecewise linear chaotic map

그림 3(a)는 텐트-맵의 갈래 질 도표를 나타낸다. 매개변수 β값이 1.0 근처에서만 x_n값이 $(0,1)$구간에 분포하는 혼돈 신호가 발생한다. 이와 같은 특성은 키 공간의 제약으로 안전성을 심각하게 저하할 수 있다.

구간별 선형 혼돈계 방정식에서 p_2와 p_3값을 각각 0.6과 0.8로 설정하고 p_1값을 0.0에서 0.5까지 변화시키며 계산된 신호의 갈래 질 도표를 그림 3(b)에 보인다. 그림에서 확인할 수 있듯이 발생하는 신호는 매개변수 변화에 따라 x_n값이 $(0,1)$구간 내에서 비교적 균등하게 분포되는 특성을 보인다.

혼돈계를 이용한 암호화 기법에 관한 선행 연구를 살펴보면, 디지털 혼돈계[9]는 자원제약이 큰 RFID 환경에서 경량 암호화를 구현하기 위해 곱셈 연산을 쉬프트 레지스터로 대체한 16비트 연산 기반 암호화 방법이다. 그러나 이 방식은 초깃값이 키

로 사용되기 때문에 키 공간이 제한적이라 보안 측면에서 잠재적인 위험성이 존재한다. 또한 동일한 혼돈계를 2차원으로 확장하여 연결한 혼돈계[10]의 경우 시스템 매개변수 μ에 따라 상태 공간의 모든 영역을 암호화에 활용하기 어렵고, 특정 매개변수 구간에서는 통계적 분포가 균일하지 않아 보안성이 저해될 수 있는 문제점을 가진다. 한편, 새로운 형태의 리턴맵을 갖는 혼돈계[11]는 기존에 알려지지 않은 혼돈 특성을 기반으로 예측이 어려운 장점이 있지만, 이 역시 초깃값에 의해 키 공간이 제안되는 문제점을 갖고 있다.

이와 같이 키 공간이 제한된 암호화 방식은 Brute Force 공격, Dictionary 공격, Key Reuse 공격 등에 취약해질 가능성이 있으며, 이는 전체 암호 시스템의 보안성에 위협이 될 수 있다.

본 연구에서 제안하는 구간별 선형 혼돈계는 기존 연구의 한계로 지적된 키 공간 제한 및 통계적 취약성을 개선하기 위해 여러 제어 변수와 초깃값을 통시에 활용하는 구조를 적용하였다. 이를 통해 보다 확장된 키 공간을 확보하고 통계적 특성을 향상해 기존 방식 대비 높은 보안성을 제공한다.

3.3 PWLCM 혼돈계의 잡음 동기화

본 연구에서 구간별 선형 혼돈계를 사물인터넷 MQTT통신에 적용하기 위해 서로 다른 혼돈계의 동기화 연구를 진행하였다.

동기화는 서로 다른 궤적으로 움직이고 있는 혼돈계를 같은 궤적으로 움직이게 하는 방법으로 우리는 잡음을 이용한 방법을 적용하였다[12].

식 (5)에서 x_n과 y_n은 서로 다른 구간별 선형 혼돈계의 신호 값이고 ξ_n은 두 혼돈계에 공통으로 인가되는 잡음신호이다.

$$\begin{aligned} x_{n+1} &= \lambda\xi_n + (1-\lambda) f_{chaos}(p_1, p_2, p_3, x_n) \\ y_{n+1} &= \lambda\xi_n + (1-\lambda) f_{chaos}(p_1, p_2, p_3, y_n) \end{aligned} \quad (5)$$

식 (5)에 의해 계산된 시계열을 그림 4에 제시한다. 그림 4(a)는 잡음 신호를 나타내며, 그림 4(b)와 그림 4(c)는 각각 혼돈계 x와 y에서 생성된 혼돈 신호를 나타낸다.

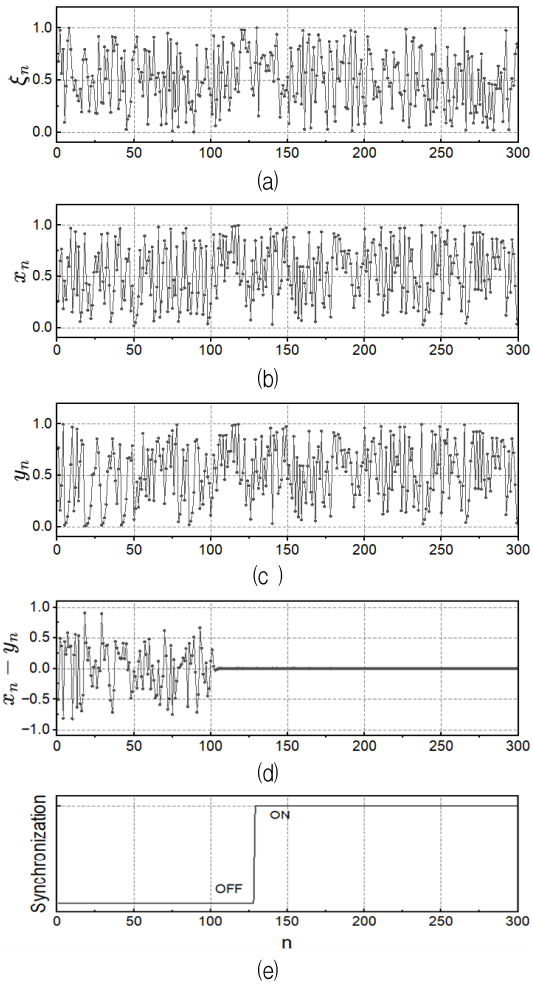

그림 4. 구간별 선형 혼돈계의 잡음 동기화 시계열
(a) 잡음신호, (b) 혼돈계 x_n, (c) 혼돈계 y_n,
(d) 두 혼돈계의 차이, (e) 동기화 여부

Fig. 4. Time-series analysis of noise-induced synchronization in the piecewise linear chaotic system (a) noise signal, (b) master chaotic system, (c) slave chaotic system, (d) difference between chaotic systems, and (e) synchronization state

그림 4(d)는 x, y혼돈계에서 발생한 혼돈 신호의 차이를 나타낸 것으로, 0으로 수렴할 때 두 혼돈계는 동기화되었다고 판단할 수 있다. 그림 4(e)는 동기화 상태를 나타내는 그래프로 그림 4(d)의 값이 정확하게 0으로 수렴한 것을 검증하기 위한 것이다. $n=100$에서 잡음신호가 인가되었고, $n \approx 130$ 부근에서 동기화가 이루어진 것을 확인할 수 있다. 잡음이 인가될 때 잡음 강도 λ는 0.85로 계산하였다. 잡음에 의한 유도된 두 혼돈계의 동기화 특성은

서로 떨어져 있는 두 혼돈계가 같은 궤적을 형성하도록 만드는 것으로, 보안 통신에서는 이러한 특성을 이용하여 공개 채널을 통해 동일한 비밀 키를 공유하는 방식으로 활용될 수 있다.

IV. 스마트그리드 MQTT 보안 통신 설계

4.1 MQTT 기반 보안 통신 구조 설계

우리는 스마트그리드의 사물인터넷 환경에서 보안 통신 프로토콜을 구현하기 위해, 그림 4에서 보인 결과를 기반으로 구간별 선형 혼돈계를 MQTT 프로토콜에 적용하는 연구를 수행하였다.

그림 5(a)는 Publisher 측에 공유된 킷값으로 구간별 선형 혼돈계의 초깃값을 계산하는 단계이고, 그림 5(b)는 Subscriber 측에서 공유된 킷값으로 초깃값을 계산하는 단계이다. 서로 다른 x_n^P와 x_n^S로 계산되기 때문에 결괏값인 x_{n+1}^P와 x_{n+1}^S는 서로 다른 신호가 생성된다. 이후 그림 5(c) 단계에서 Broker가 잡음신호 ξ_n을 Publisher와 Subscriber에 전송하여 그림 5(d)와 그림 5(e)와 같이 동기화를 진행한다. 동기화 이후 그림 5(f)와 같이 Data를 암호화하여 Broker를 통해 전송하면 그림 5(g)와 같이 복호화하여 Data를 획득하게 된다.

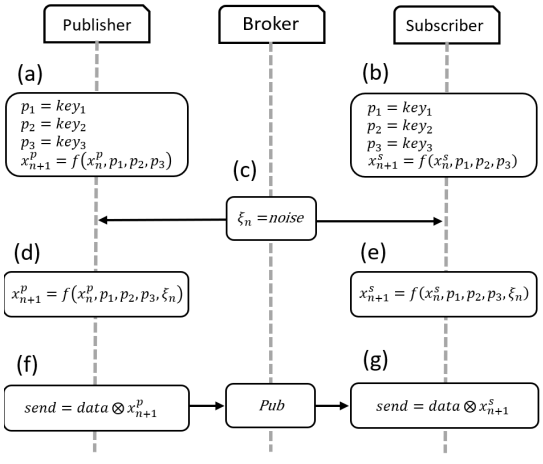

그림 5. 스마트그리드 MQTT 보안 통신 흐름도
Fig. 5. Secure MQTT communication flow for smart grids

4.2 히스토그램 분석

제안된 프로토콜의 보안 성능을 시각적으로 평가하기 위해 이미지에 암호화 및 복호화 실험을 진행하였다. 이미지 데이터는 시각적으로 암호화 정도를 분석이 쉬워 보안 성능 평가에 널리 활용되는 데이터 유형이다.

그림 6(a)는 스핑크스(Sphinx) 이미지를 8비트 흑백 이미지로 변환한 것이다. 동기화된 구간별 선형 혼돈계에서 발생한 실수값 x_n을 8비트 정수형으로 변환하여 흑백 이미지와 배타 논리(XOR, Exclusive OR)로 계산하여 암호화 및 복호화를 진행하였다. 그 결과를 그림 6에 보인다. 그림 6(c)는 암호화된 이미지를 나타내며, 그림 6(b)와 그림 6(d)는 각각 원본 이미지와 암호화된 이미지의 히스토그램으로 암호화 이후 균등분포를 유지하는 것을 확인할 수 있다.

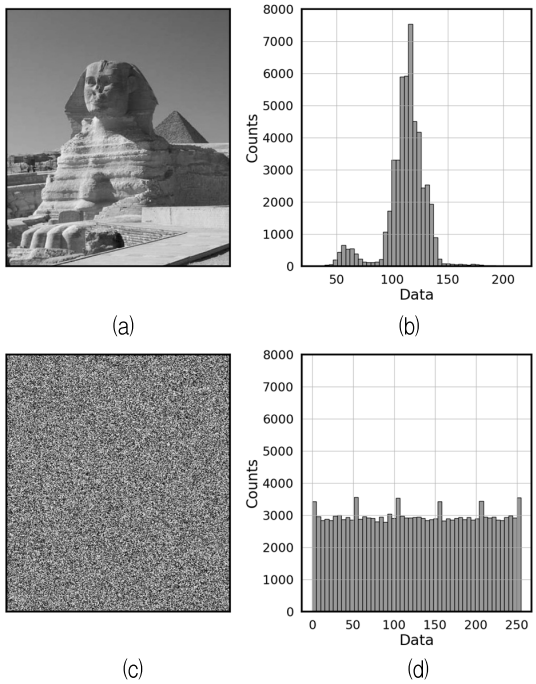

그림 6. 구간별 선형 혼돈계를 이용한 이미지 암호화 및 복호화 (a) 원본 이미지, (b) 원본 이미지의 히스토그램, (c) 암호화된 이미지, (d) 암호화된 이미지의 히스토그램
Fig. 6. Image encryption and decryption using a piecewise linear chaotic system (a) Original image, (b) Histogram of the original image, (c) Encrypted image, (d) Histogram of the encrypted image

4.3 인접 픽셀 상관관계 분석

제안된 프로토콜의 암호화 정도를 분석하기 위해 암호화된 이미지의 특정 픽셀과 인접한 픽셀에 대한 상관관계 분석을 다음과 같이 진행하였다.

$$r = \frac{Cov(x, y)}{\sigma_x \sigma_y} \tag{6}$$

식 (6)에서 $Cov(x, y)$는 공분산을 나타내고, σ_x와 σ_y는 각각 x와 y의 표준편차이다.

상관계수를 이용한 상관관계 분석은 이미지의 공간적 규칙성이 암호화 이후 얼마나 효과적으로 제거되었는지를 평가하는 대표적인 통계적 안정성 지표이다. 암호화가 효과적으로 처리된 경우, 상관계수는 0에 가까운 값을 나타낸다.

표 1. 암호화된 이미지의 상관관계 분석
Table 1. Correlation anslysis of the encrypted image

Direction of adjacent pixels	Original image Fig. 6(a)	Encrypted image Fig. 6(c)
Horizontal	0.9680	0.0382
Vertical	0.9306	0.0112
Diagonal	0.8992	0.0008

4.4 픽셀 변화율과 평균 변화 강도

픽셀 변화율(NPCR, Number of Pixel Change Rate)은 원본 이미지와 그 이미지의 한 픽셀을 변경시킨 이미지를 각각 암호화하고, 두 이미지의 픽셀 변화 정도를 정량적으로 평가하는 지표로 암호화 정도를 측정하는 대표적인 방법이다. 계산된 NPCR 값이 99% 이상일 때 이상적으로 암호화가 되었다고 판단한다. 우리가 제안한 구간별 선형구조 혼돈계의 NPCR 값은 99.57%로 통계적 공격에 대한 높은 민감도와 우수한 확산 특성을 갖는다고 할 수 있다. 식 (7)의 W과 H는 이미지의 가로, 세로 크기를 나타내고, $D(i, j)$는 두 이미지의 i행, j열 픽셀이 서로 같다면 0, 다르면 1을 나타내는 함수이다.

$$NPCR = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H} D(i, j) \times 100\% \tag{7}$$

평균 변화 강도(UACI, Unified Average Changing Intensity)는 암호화된 두 이미지 간 픽셀값 변화의 평균 강도를 나타내는 지표로 NPCR과 함께 암호화의 정도를 파악하는 대표적인 지표이다. UACI가 높으면 픽셀값이 크게 바뀌어 차분 공격에 강한 특성을 갖게 되고 UACI 값이 작으면 확산이 부족하여 공격에 취약한 특성을 갖게 된다. 이상적인 값은 33%이고, 우리가 제안한 방법은 33.67%의 특성을 나타내고 있다.

$$NPCR = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H} \frac{|C(i,j) - C'(i,j)|}{255} \times 100\% \tag{8}$$

식 (8)에서 $C(i, j)$와 $C'(i, j)$는 암호화 된 두 개의 이미지를 나타낸다.

Ⅴ. 결론 및 향후 과제

본 연구에서는 스마트그리드 사물인터넷 환경에서 가장 널리 사용되고 있는 MQTT 프로토콜의 구조적 보안 취약성을 보완하기 위해 경량 혼돈계 기반 보안 통신 방법을 제안하였다. MQTT는 경량 메시지 전달 프로토콜로서 IoT 환경에 적합하다는 장점을 가지고 있지만, 기본적인 암호화 및 인증 기능이 제한적이라서 다양한 사이버 공격에 노출될 가능성이 높다고 할 수 있다. 이러한 보안 취약성은 단순한 전력 정보 노출을 넘어 전력 공급의 연속성 저해와 국가 기반 시설 전반의 안전성에 심각한 영향을 미칠 수 있는 잠재적 위험 요소가 된다.

이와 같은 문제점을 해결하기 위해 본 논문에서는 연산 복잡도가 낮으면서 높은 비선형과 통계적 무작위성을 갖는 구간별 선형 혼돈계 기반 암호화 방법을 설계하였다. 제안된 방법은 기존의 혼돈계에 비해 매개변수 확장성과 키 공간 확보 측면에서 유연성을 가지면 넓은 매개변수 구간에서 혼돈 특성을 유지함을 갈래 질 도표를 통해 확인하였다.

보안 성능 검증을 위해 히스토그램 분석, 인접 픽셀 상관계수 분석, NPCR 및 UACI 평가를 수행하였다. 실험 결과, 암호화된 데이터는 균등 분포 특성을 나타내고 있으며, 인접 데이터와의 상관성이

제거되었고, NPCR 및 UACI 값 또한 이상적인 값 근처에 있는 것을 확인할 수 있었다.

비론 혼돈계 기반의 암호화 방식이 기존의 표준 블록 암호화 체계와 비교할 때 이론적 안전성 검증 측면에서 한계를 가질 수 있으나, 제한된 자원을 사용하는 스마트그리드 IoT 환경에서는 경량성과 보안성을 동시에 만족시킬 수 있는 대안으로 경쟁력을 가진다고 할 수 있다.

결론적으로, 본 연구에서 제안한 구간별 선형 혼돈계 기반 MQTT 보안 통신 구조는 스마트그리드 IoT 환경에서 경량성과 보안성을 고려한 현실적인 활용에 기여할 수 있을 것으로 기대된다.

References

[1] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, "A survey of smart grid architectures, application, benefits and standardization", J. Netw. Comput. Appl., Vol. 76, pp. 23-36, Dec. 2016. https://doi.org/10.1016/j.jnca.2016.10.003.

[2] A. Bashir and A. H. Mir, "Securing Publish-Subscribe Services with Dynamic Security Protocol in MQTT Enabled", Int. J. Secur. Appl., Vol. 11, No. 11, pp. 53-66, Nov. 2017. https://doi.org/10.14257/ijsia.2017.11.11.05.

[3] J. Roldan-Gomez, J. Carrillo-Mondejar, J. M. C. Gomez, and S. Ruiz-Villafranca, "Security Analysis of the MQTT-SN Protocol for the Internet of Things", Applied Sciences, Vol. 12, No. 21, pp. 1-24, Oct. 2022. https://doi.org/10.3390/app122110991.

[4] N. H. Kim and C. S. Hong, "Lightweight Cryptography Algorithm base Secure MQTT Protocol", Journal of KIISE, Vol. 16, No. 12, pp. 757-759, Dec. 2016. https://doi.org/10.5626/JOK.2016.16.12.757.

[5] N. H. Kim and C. S. Hong, "Secure MQTT Protocol based on Attributed-Based Encryption Scheme", Journal of KIISE, Vol. 45, No. 3, pp. 159-199, Dec. 2018. https://doi.org/10.5626/JOK.2018.45.3.195.

[6] M. A. Hafeez, K. H. Shakib, and A. Munir, "A Secure and Scalable Authentication and Communication Protocol for Smart Grids", J. Cybersecurity and Privacy, Vol. 5, No. 11, pp. 1-20, Dec. 2024. https://doi.org/10.3390/jcp5020011.

[7] H. G. Schuster, "Deterministic Chaos: An Introduction 2nd edition", Wiley-VCH, pp. 24-32, Dec. 1997.

[8] E. Ott, "Chaos in Dynamics Systems 2nd edition", Cambridge University Press, pp. 15-18, Sep. 2002.

[9] G.-S, Yim, "IoT MQTT Security Protocol Design Using Chaotic Signals", Journal of KIIECT, Vol. 11, No. 6, pp. 798-783, Oct. 2018. http://doi.org/10.17661/jkiiect.2018.11.6.778.

[10] G.-S, Yim, "Design of RFID Authentication Protocol Using 2D Tent-map", Journal of KIIECT, Vol. 13, No. 5, pp. 425-431, Oct. 2020. https://doi.org/10.17661/jkiiect.2020.13.5.425.

[11] G.-S, Yim, "IoT Security Channel Design Using a Chaotic System Synchronized by Key Value", Journal of KIECS, Vol. 15, No. 5, pp. 981-986, Oct. 2020. https://doi.org/10.13067/JKIECS.2020.15.5.981.

[12] G.-S, Yim and H.-S. Kim, "Chaos-based Image Encryption Scheme using Noise-induced Synchronization", Journal of KSCI, Vol. 13, No. 5, pp. 155-162, Sep. 2008.

저자소개

임 거 수 (Geo-Su Yim)

2004년 2월 : 서강대학교 물리학과(이학박사)
2006년 5월 : ㈜로콜넷 연구소장
2008년 3월 ~ 현재 : 배재대학교 전기·전자공학과 교수
관심분야 : PLC 자동제어, 인공지능, 디지털트윈

송 창 후 (Chang-Hoo Song)

2026년 2월 : 배재대학교
전기·전자공학과(공학사)
관심분야 : PLC 자동제어, IoT
보안통신