한국정보전자통신기술학회논문지(jkiiect)'18-12, Vol.11 No.6
논문 18-11-06-778 http://dx.doi.org/10.17661/jkiiect.2018.11.6.778

혼돈신호를 이용한 IoT의 MQTT 보안 프로토콜 설계

임 거 수*

IoT MQTT Security Protocol Design Using Chaotic Signals

Geo-Su Yim*

요 약 정보통신과 산업기술의 급속한 발전으로 인간과 모든 프로그램 그리고 사물들이 인터넷을 통해 연결되는 초연결사회(hyper-connected society)가 구현되고 있다. 초연결사회를 구현하기 위한 정보의 수집은 사물과 사물 그리고 사물과 인간을 연결하는 사물인터넷(IoT: Internet of Thing)이 그 역할을 담당하고 있다. (MQTT: Message Queuing Telemetry Transport)는 이런 사물인터넷의 제약된 통신환경에 최적화되어 개발된 푸시 기술(push technology) 기반의 경량 메시지 전송 프로토콜이다. 초연결사회를 지향하면서 IoT가 담고 있는 정보는 센서의 환경정보에서 이제는 사람의 질병과 건강관리까지 담당하는 광범위한 정보가 되었다. 이런 MQTT에 대한 보안 문제는 환경정보 유출뿐만 아니라 개인의 정보 침해에까지 이르게 되었다. 우리는 이런 MQTT의 보안의 문제점을 해결하기 위해 혼돈계의 초기치 민감성, 유사 난수성을 무결성과 기밀성에 적용하여 새로운 보안 MQTT통신방법을 설계하였다. 우리가 설계한 혼돈계를 이용한 암호화 방법은 구조가 간단하고 계산량이 적기 때문에 IoT와 같은 제한된 통신환경에 적합한 통신방법이라고 생각된다.

Abstract With the rapid advancement of information and communication technology and industrial technologies, a hyper-connected society is being realized to connect human beings, all programs and things via the Internet. IoT (Internet of Thing), which connects a thing and another thing, and things and human beings, gathers information to realize the hyper-connected society. MQTT (Message Queuing Telemetry Transport) is a push-technology-based light message transmission protocol that was developed to be optimized to the limited communication environment such as IoT. In pursuing the hyper-connected society, IoT's sensor environment information is now being used as a wide range of information on people's diseases and health management. Thus, security problems of such MQTT include not only the leak of environmental information but also the personal information infringement. To resolve such MQTT security problems, we have designed a new security MQTT communication by applying the initial-value sensitivity and pseudorandomness of the chaotic system to the integrity and confidentiality. The encryption method using our proposed chaotic system offers a simple structure and a small amount of calculation, and it is deemed to be suitable to the limited communication environment such as IoT.

Key Words : Iot, MQTT, Security Protocol, Chaotic signals, Tent-map

1. 서론

산업의 발전과 사회의 발전은 많은 종류의 정보가 필요하게 되고 네트워크는 컴퓨터 간의 통신에서 이제는 사물과의 사물의 통신까지 그 범위가 확대되고 있다. 사람의 편의를 도모하기 위한 텔레비전, 냉장고, 면도기 등과 같은 기기에서부터 화분이나 아기의 기저귀 같은 사소한 사물에 이르기까지 정보를 공유하기 위해 네트워크의 접속이 필요하게 되고 이런 필요에 의해 생성된 서비스 네트워크가 사물인터넷(IoT:Internet of Thing)이다. 사물과 사물, 사물과 사람을 연결하는 사물인터넷의 등장과 지속적인 발전으로 초연결사회가 현실화되고 있다. 이와 같은 사물인터넷의 발전은 기존의 편의를 도모하기 위한 용도의 센서 정보에

This work was supported by the research grant of Pai Chai University in 2018.
*Corresponding Author : Department of Electrical Engineering, Pai Chai University (lomac@pcu.ac.kr)
Received October 07, 2018 Revised October 15, 2018 Accepted December 20, 2018

서 이제는 사람의 신체정보와 개인정보까지 오가는 복잡한 네트워크로 발전되고 있다. 이와 같은 발전의 반면으로 보안에 대한 문제도 위험성이 부가되기 시작했다. 기존 통신에 대한 보안의 취약한 특성은 센서 정보의 유출이었으나 이제는 개인의 사생활 침해로 이어지고 있어 보안에 대한 문제가 심각해졌다[1, 2, 3].

우리는 이와 같은 사물인터넷의 대표 프로토콜인 MQTT를 분석하고 보안에 대한 문제점을 해결하기 위해 새로운 암호화 연구를 진행하였다.

우리는 혼돈계의 비선형 특성을 통신에 적용해 문제시되고 있던 MQTT의 보안 문제를 해결하고자 연구를 진행하였고, 2장에서는 IoT 통신과 혼돈계의 특성에 대하여 논하고, 3장에서 디지털 혼돈계를 적용한 MQTT통신 프로토콜의 구조와 통신방법에 대하여 기술한다.

2. 사전연구

2.1 MQTT 통신

사물인터넷(IoT)은 물리적 정보를 획득할 수 있는 주의의 모든 사물에 센서를 부착하여 획득한 환경정보를 가공하여 편의를 도모하기 위해 구성된 네트워크이다. 그러나 통신 밴드 폭에 의한 통신의 제약성이 있어 이것을 극복하기 위해 개발된 통신 프로토콜이 MQTT(Message Queuing Telemetry Transport)이다. MQTT의 구조를 그림 1에 보인다[4, 5].

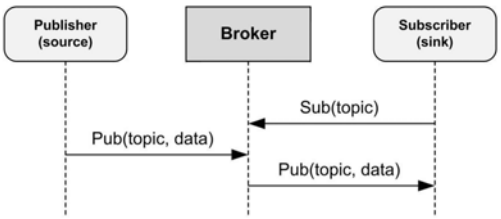

그림 1. MQTT 전송 프로토콜

Fig. 1. Protocol of MQTT Transport

통신 제약 문제를 해결하기 위해 MQTT에서는 통신 중간에 허브와 같은 역할을 하는 Broker를 두어 Publisher에서 보내온 topic에 해당하는 data값을 Broker의 저장 공간에 계층적 구조의 문자열로 저장했다가 Subscriber가 요구하는 topic에 해당하는 data를 전송하는 경량화 프로토콜이다. MQTT 프로토콜의 경량화에 대한 연구는 현재까지 많이 이루어지고 있지만 보안에 대한 연구는 아직 취약한 상태이다. 우리는 이런 MQTT의 보안을 강화할 목적으로 혼돈계를 선택하고 관련 연구를 진행하였다.

2.2 혼돈계의 특성

혼돈 신호를 발생시키는 혼돈계는 그 구조에 따라 크게 두 가지로 분류가 된다. 상미분 방정식 형태의 혼돈계인 Lorenz System, Rossler System, Chua System과 계차 방정식 형태인 Tent map, Logistic map, Henon map, Gauss map 등이 있다. 혼돈계에서 발생하는 신호는 지배 방정식에 주어지는 매개변수와 초기값의 미세한 차이로 인하여 전혀 다른 값을 발생시키는 초기치 민감성과 발생하는 신호를 재생성할 수 있는 특성, 그리고 발생된 신호가 난수와 유사한 특성이 있다. 이런 이유로 혼돈 신호를 재생산 가능한 난수라고 한다. 혼돈 신호의 특징 중 초기치 민감성을 통신에 적용하면 외부 변조 공격에 강한 특징을 구현할 수 있고, 난수와 유사한 특성은 통신의 기밀성을 유지할 수 있게 한다[6, 7, 8]. 우리는 혼돈계의 특성을 MQTT 프로토콜에 적용하기 위해 계차 방정식 혼돈계 중 16진수 출력을 할 수 있도록 변형된 디지털 혼돈계를 선택하였다[9].

2.3 디지털 혼돈신호 발생

본 논문에서 우리는 MQTT 통신 프로토콜에 혼돈계를 적용하기 위해 텐트 맵을 변형한 디지털 혼돈계를 선택하였다. 텐트 맵에서 발생하는 신호는 $x_n \in (0\ ,\ 1)$ 신호이지만 우리가 사용하려는 디지털 혼돈계의 출력 값은 $x_n \in (0000h, FFFFh)$로 발생하기 때문에 사용하기 용이하다[9, 10].

우리가 연구용으로 선택한 디지털 혼돈계의 지배 방정식을 아래에 보인다.

$$\text{if } (MSB(x_n) = 0)\ then \quad (1)$$
$$x_{n+1} = ((x_n \ll 1) - (x_n \gg 6))$$

$$\text{if } (MSB(x_n) = 1)\ then \quad (2)$$
$$y_n = FFFFh - x_n$$
$$x_{n+1} = ((y_n \ll 1) - (y_n \gg 1))$$

식 (1)과 식 (2)의 계산 결과를 그림 2에 보인다. 그림 2의 (a), (b) 그리고 (c)는 식 (1)의 시프트 연산 비트를 각각 3, 6, 9로 계산한 결과 값이다. 일반적인 혼돈계의 결과는 $0 \sim 1$ 사이에 분포하지만 디지털 혼돈계의 결과는 $2^0 \sim 2^{15}$사이에 분포되기 때문에 디지털 체계에 적용하기 용이하다.

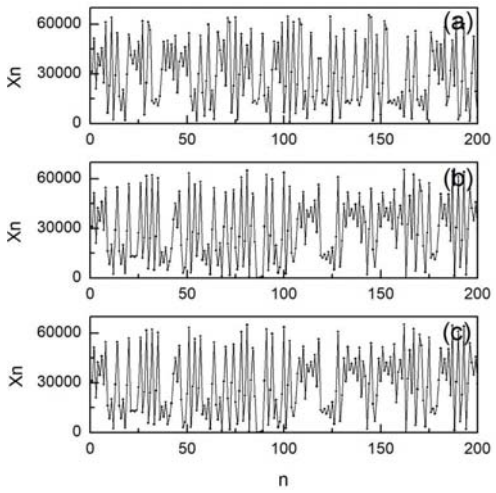

그림 2. 디지털혼돈계의 시계열 도표

Fig. 2. Temporal behavior of digital chaotic signals

3. 제안된 MQTT 통신 방법

3.1 암호화 및 복호화 방법

우리가 제안한 IoT의 MQTT 보안 통신 방법은 topic으로 분류되어 Broker에 저장되고 있는 data의 기밀성과 무결성을 보장하기 위한 방법으로 혼돈 신호로 암호화하여 기밀성을 유지하고 혼돈계의 연속성으로 무결성을 보장하는 방법이다. 제안된 암호화 방법을 그림 3에 보인다.

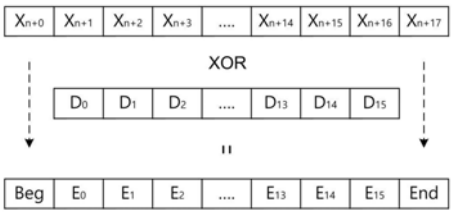

그림 3. 혼돈 신호를 이용한 암호화 구조

Fig. 3. Encryption scheme of chaotic signals

그림 3의 x_{n+0} 부터 x_{n+17} 신호는 혼돈계에서 발생한 신호이고 D_0에서 D_{15}는 전송 data이다. 암호화 방법은 두 데이터 세트를 XOR로 계산하였다. 암호화할 때 혼돈계의 시작 값과 끝 값은 data를 포함하고 있지 않아 이후 전송된 데이터를 복호화하거나 연결성을 확인할 수 있게 하였다. 데이터의 연결성 확인 방법을 그림 4에 보인다.

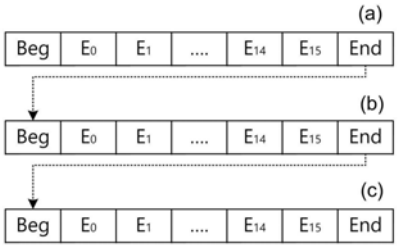

그림 4. 전송 데이터 암호화 구조

Fig. 4. Encryption scheme of transmission data

계차 방정식 형태의 혼돈계에서 발생하는 신호는 x_n에 의해 x_{n+1}이 계산되는 형태이므로 이전 데이터의 End는 x_n이고 이후 데이터의 Beg은 x_{n+1}이 되기 때문에 데이터의 연결성을 확인할 수 있어 무단으로 데이터를 삽입, 삭제하여 전송하는 위험 요소를 제거할 수 있다.

3.2 MQTT 보안 통신

지배 방정식에 의해 발생한 혼돈 신호는 난수와 유사하고 이전 값으로 이후 값을 계산할 수 있어 암호화에 적용하면 통신의 무결성과 기밀성 그리고 연결성을

보장할 수 있는 새로운 암호화 방법이라고 할 수 있다. 우리는 제안한 암호화 방법을 MQTT 통신 프로토콜에 적용하고 그 내용을 그림 5에 보인다.

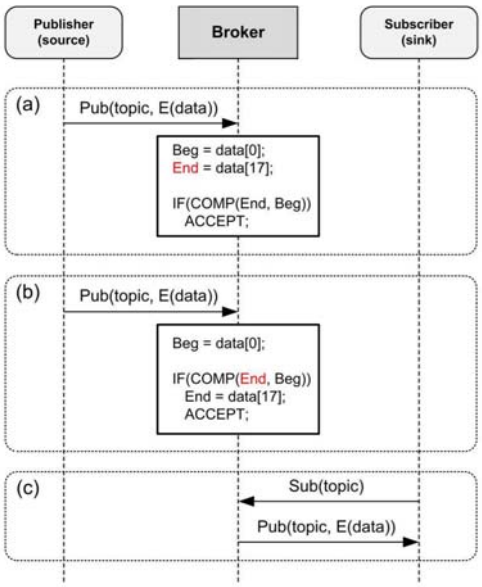

그림 5. 제안된 MQTT 프로토콜의 구조

Fig. 5. Structure of proposed MQTT protocol

그림 5의 (a) 단계는 Publisher가 topic에 해당하는 암호화된 data를 전송하는 단계로 Broker는 전송된 데이터의 data0 과 data17을 혼돈 신호 연결성 확인 함수 COMP()를 이용하여 검증하고 이상이 없으면 계산된 혼돈 신호와 수신된 데이터 data들을 XOR 연산으로 복호화한다. 그리고 data17 값을 End 변수에 저장한다.

(b) 단계는 이후에 전송된 data의 data0 값을 Beg 변수에 넣고 (a) 단계의 End 값과 연속적인 혼돈 신호인지 COMP()로 검증하여 전송된 데이터의 무결성을 검증한다.

(c) 단계는 Broker에 저장된 data들을 (a), (b)와 같은 방법으로 암호화하여 Subscriber에게 전송하게 된다.

우리는 그림 5에 제시된 MQTT 보안 통신의 암호화 정도를 가시화하기 위하여 Publisher에 의해 생성된 데이터를 암호화하여 Broker에 저장하고 Subscriber에 의해 복호화되는 과정의 모의실험을 진행하였다. 그림 6은 흑백 이미지를 이용한 모의실험의 결과이다.

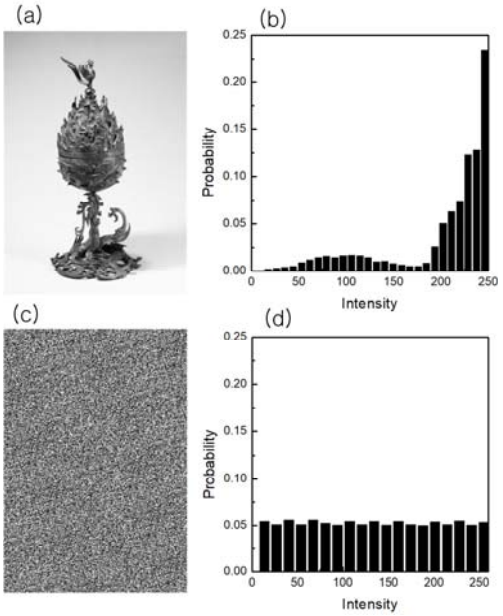

그림 6. 제안된 MQTT 프로토콜의 모의실험

Fig. 6. Simulation of proposed MQTT protocol

그림 6의 (a)는 원본 이미지 내용이고 (c)는 암호화된 이미지 내용이다. (b)와 (d) 각각 이미지 값의 히스토그램을 나타낸 것으로 암호화 이후 색의 분포가 일정하여 원본 이미지의 내용을 파악할 수 없는 것을 확인할 수 있다.

3.3 제안된 프로토콜 분석

우리가 제안한 혼돈 신호를 이용한 MQTT 보안 통신 방법은 난수와 유사한 혼돈 신호로 데이터를 암호화하므로 도청 공격, 스푸핑 공격, 서비스 거부 공격에 다음과 같은 특성을 갖게 된다[11].

1) 도청 공격으로 데이터가 유출되었어도 혼돈계에서 발생되는 신호는 혼돈계의 매개변수와 특성을 파악

하기 전에는 예측할 수 없는 난수와 같으므로 유출된 데이터에서 정보를 추출하기는 불가능하다고 할 수 있다.

2) 스푸핑 공격으로 데이터가 왜곡되어도 전송 데이터의 End와 Beg는 혼돈계에서 발생하는 신호로 연결되어 있어 혼돈계의 매개변수와 특성을 파악하기 전에는 데이터를 왜곡시킬 수 없게 된다.

3) 서비스거부 공격으로 무작위 데이터를 전송하여도 전송된 데이터의 Beg 값이 이전 데이터의 End 값과 연결성을 확인하여 수신 초기에 무시하기 때문에 공격에 강한 특성이 있다고 할 수 있다.

4) 제안된 프로토콜에서 보안의 목적으로 사용되고 있는 혼돈계의 신호는 초기치 민감성의 특성을 가지고 있어 초기값과 매개변수의 조합으로 구성된 암호가 공개되지 않으면 무단으로 데이터에 접근할 수 없어 강한 무결성을 갖고 있다고 할 수 있다.

표 1. 제안된 MQTT 프로토콜의 효율성
Table 1. Effectiveness of proposed MQTT protocol

공격기법	MQTT	제안된 프로토콜
도청공격	취약	안전
스푸핑공격	취약	안전
재전송공격	취약	안전
서비스거부공격	취약	안전
위치추적	취약	보통

제안된 MQTT 프로토콜은 혼돈계의 유사 난수성과 초기치 민감성과 같은 내재적인 특성을 가지고 있어 보안에 강한 특성을 나타내고 있고 그 내용을 표 1에 보인다.

4. 결론

초연결사회를 구현하기 위한 사물인터넷(IoT)은 사람을 포함한 사물과 공간 등 모든 것들을 인터넷으로 연결하여 모든 것들에 대한 정보를 수집 및 가공하고 사람의 편의를 도모하기 위해 활용하는 서비스 네트워크를 말한다. IoT의 대표적인 통신 프로토콜인 MQTT는 밴드폭의 제약으로 인하여 푸시 기술이 적용된 경량화 프로토콜을 사용하고 있다. MQTT는 프로토콜의 경량화로 보안에 대한 취약한 특성을 가지고 있고 우리는 MQTT 프로토콜의 보안을 강화하기 위해 혼돈 신호를 이용하여 암호화 연구를 진행하였다. 우리는 계차 방정식 Tent-map 혼돈계를 디지털화시킨 디지털 혼돈계를 이용하여 경량화에 적합한 MQTT 암호화 프로토콜을 설계하였고, 그 구조를 논문에서 보였다. 우리가 제시한 혼돈계를 이용한 보안 통신방법은 혼돈계에서 발생되는 유사 난수 신호와 초기값과 매개변수에 의존하는 초기치 민감성을 이용한 방법으로 난수와 유사한 신호에 숨겨진 정보는 난수와 유사한 특성을 보이기 때문에 외부 공격에 강인한 특성을 보이게 된다. 우리가 제안한 방법을 보안이 취약한 MQTT 통신에 적용한다면 무단 공격에 강인한 보안 통신을 구현할 수 있을 것으로 예측된다. 또한 계차 방정식 혼돈계의 간단한 수식을 이용한 작은 계산량의 IoT 프로그램을 개발할 수 있어 산업화에 효율성을 가져올 것으로 예측된다.

REFERENCES

[1] S. H. Oh, S. K. Ko, S. C. Son, B. T. Lee, Y. S. Kim, "IoT Device Management Standard Protocol Trends in Mobile Communications", Electronics and Telecommunications Trends, Vol.30, No.1, pp. 94-101, 2015.

[2] Y. H. Jeon, "A Study on the Security Modeling of Internet of Things(IoT)", Journal of KIIT, Vol.15, No.12, pp. 17-27, December, 2017.

[3] J. Y. Ko, S. G. Lee, J. W. Kim, C. H. Lee "Technologies Analysis based on IoT Security Requirements and Secure Operating System", Journal of KCA, Vol.18, No.4, pp. 164-177, March, 2018.

[4] N. H. Kim, C. S. Hong, "Secure MQTT Protocol based on Attribute-Based Encryption Scheme", Journal of KIISE, Vol.45, No.3, pp. 195-199, December, 2018.

[5] N. H. Kim, C. S. Hong, "Lightweight Cryptography Algorithm based Secure MQTT Protocol", Proc. of KIISE, Vol.2016, No.12, pp. 757-759, December, 2016.
[6] H. G. Schuster, "Deterministic Chaos: An Introduction: 2nd edition", VCH, pp. 24-32, December, 1997.
[7] E. Ott, "Chaos in Dynamical Systems Second Edition", Cambridge University Press, pp. 15-18, September, 2002.
[8] G. L. Baker, and J. P. Gollub, "Chaotic Dynamics an Introduction", Cambridge University Press, pp. 41-58, January, 1996.
[9] M. H. Choi, G. S. Yim, "Passive RFID Certification Protocol Design Using Digital Chaos System", Journal of KIIT. pp. 85-92, October, 2014.
[10] Lynch, Stephen, "Dynamical Systems with Applications Using Matlab", Birkhauser, pp. 35-47, 2004.
[11] G. S. Yim, "Design of USN Communication Protocol Using Individual Chaotic Systems, Journal of KIIECT, Vol.8, No.6, pp. 528-533, December, 2015 .
[12] Kitae Hwang, 'Design and Implementation of Dashboard Author and Viewer for IoT Systems based on MQTT', The Journal of The Institute of Internet, Broadcasting and Communication VOL. 18 No. 5, 2018

저자약력

임 거 수(Geo-Su Yim) **[정회원]**

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

〈관심분야〉 시계열분석, 신호처리, 빅데이터 분석, 머신러닝, 보안