한국정보전자통신기술학회논문지(jkiiect)'15-12, Vol.8 No.6
논문 15-08-06-528 http://dx.doi.org/10.17661/jkiiect.2015.8.6.528

개별 혼돈 시스템을 이용한 USN 통신 프로토콜 설계

임거수*

Design of USN Communication Protocol Using Individual Chaotic Systems

Geo-Su Yim*

요 약 USN 환경의 구축에 있어서 무선통신을 이용한 안전한 센서 네트워크 구현은 전체 시스템에 있어서 가장 중요한 요소라고 할 수 있다. USN 통신은 접근성, 비접촉성을 높이기 위해 무선통신을 사용하고 있으나 이것으로 인한 보안의 취약성은 시스템을 위험하게 하고 있다. 우리는 이런 다중센서 네트워크인 USN에 효율적으로 적용할 수 있는 보안 프로토콜을 제안한다. 우리가 제안한 프로토콜은 개별 혼돈 시스템을 이용한 방법으로 각각의 센서에 장착된 혼돈 시스템을 주 혼돈 시스템과 미리 준비된 킷값을 초깃값으로 동기화시키고, 동기화된 값을 대칭키로 하여 통신하는 보안 프로토콜이다. 본 논문에서 보인 통신 프로토콜은 USN의 취약한 보안 문제와 센서노드의 프로그램 용량 제한 문제점을 해결하기 위한 새로운 방법으로 계속적인 후속 연구가 이루어진다면 좋은 성과를 얻을 수 있을 것으로 생각된다.

Abstract In the construction of USN environment, the implementation of a safe sensor network using wireless communications can be said to be the most important factor in the entire system. Although USN communication uses wireless communications to enhance accessability and non-contact capability, this results in the security vulnerability, thus endangering the system. In this regard, we propose a security protocol that can be effectively applied to USN, a multi-sensor network. The proposed protocol is a method using an individual chaotic system, and it is a security protocol to synchronize the main chaotic system mounted on each sensor and prepared key values into the initial values, and to communicate with the use of the synchronized values as symmetric keys. The communication protocol proposed in this paper is expected to yield good results as a new method to resolve security problems of USN and program capacity limitations of sensor nodes if subsequent studies continue to be carried out.

Key Words : Ubiquitous, Sensor Network, Chaos, Secure Channel, multi-sensor network, chaotic system

1. 서 론

최근 들어 통신 및 인터넷의 발달로 사회는 계속 정보화되어 가고 있고 삶의 질적인 향상을 목적으로 한 USN(Ubiquitous Sensor Network)에 대한 연구는 다양화 측면에서 많은 발전을 가져왔다[1,2]. 그중 USN의 보안에 대한 연구는 최근 들어 많은 연구자들의 관심의 대상이 되고 있다. 연구자들은 USN의 보안을 위해 기존의 암호화 방법들인 DES, 3DES, RSA 같은 방법을 이용하여 암호화를 USN에 적용하는 연구를 진행하고 있다. 우리는 이런 고급 암호화 방법들은 구조가 많이 알려져 있어 무단 복호화의 목표가 되고 있다는 것을 인지하고 새로운 암호화 방법에 대한 연구도 기존의 암호화 방법을 견고하게 하는 연구와 더불어 병행되어야 한다고 생각한다. 이런 새로운 암호화 방법으로 우리가 선택한 것은 혼돈 시스템을 이용한 방법으로 혼돈 시스템에서

*Corresponding Author : Department of Electrical Engineering, PaiChai University (lomac@pcu.ac.kr)
Received December 01, 2015 Revised December 09, 2015 Accepted December 18, 2015

발생되는 신호는 잡음 신호와 통계적으로 유사하지만 신호를 생성하는 시스템의 초깃값과 매개변수를 알고 있으면 재생산할 수 있는 특성이 있어 데이터 암호화에 효율적으로 적용될 수 있다[3,4,5].

USN 통신에서 Sink 노드와 Sensor 노드가 혼돈시스템의 초깃값과 매개변수를 통신 초기에 공유하여 사용한다면 두 노드는 같은 시점에 같은 유사난수를 발생하게 되고 이것을 암호화와 복호화에 사용하면 견고한 암호화 채널을 구현할 수 있다.

우리는 혼돈 시스템을 이용한 USN 통신 프로토콜을 설계하기 위해 Sink 노드와 각각의 Sensor 노드에 초깃값과 매개변수를 갖는 개별 혼돈 시스템을 구성하고 발생되는 유사 난수를 Sensor 노드별로 다르게 설계하였다. 통신 프로토콜은 초기 인증 단계와 데이터 통신 단계로 구분하여 설계하였고, 이것은 초기 킷값 분배 시 외부의 도청 공격에 강하도록 설계된 것이다. 우리가 제시한 혼돈 시스템을 이용한 USN 통신 프로토콜은 선행된 연구가 없는 내용으로 초기에 안정화를 위한 연구가 필요하겠지만 후속 연구가 계속 이루어진다면 보다 효과적인 USN 통신 프로토콜로 사용될 수 있을 것으로 예측된다.

2. 관련연구

암호화 및 복호화를 위한 혼돈 시스템에 대한 연구는 네트워크의 속도와 전송되는 데이터양의 증가에 따라 그 필요성이 요구되고 있다. 혼돈 시스템의 신호를 이용한 대표적인 암호화 방법은 CKBA(Chaotic Key-based Algorithm), CBFSC(Chaos-Based Feedback Stream Cipher) 등이 있고, 이 방법들은 혼돈 시스템의 매개변수와 초깃값을 킷값으로 하여 발생되는 신호 값으로 암호화하는 방법이다[6,7,8]. 혼돈 시스템에서 발생되는 신호는 잡음과 유사하여 발생되는 신호로 데이터를 암호화하면 전송 되는 데이터 또한 잡음과 유사한 형태를 유지하는 특성을 가지고 있어 무단으로 복호화 할 수 없는 강한 암호화 특성을 가지고 있다.

혼돈 시스템은 크게 계차방정식 형태의 시스템과 미분방정식 형태의 시스템으로 구분된다. 이중 암호화 및 복호화에 주로 사용되는 혼돈 시스템은 계차방정식 형태의 시스템으로 1차원 시스템은 Circle map, Henon map, Logistic map 등이 있고, 2차원 시스템은 Ikeda map, Baker's map, Duffing map 등이 있다[9,10]. 우리는 이중 Logistic map을 이용하여 USN 통신프로토콜을 설계하였고 사용된 혼돈 시스템을 수식 (1)에 보인다.

$$X_{n+1} = \alpha X_n (1 - X_n) \tag{1}$$

식에 보인 X_n의 계산 구조를 혼돈 시스템 분석 방법 중 하나인 Return Map을 이용하여 그림 1에 보인다.

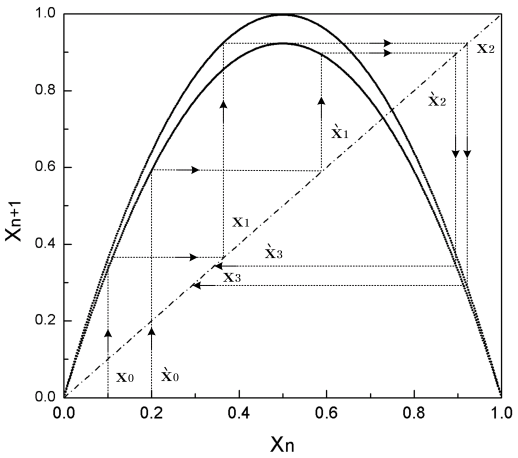

그림 1. 혼돈시스템의 리턴-맵
.Fig. 1. Return-map of chaotic system

그림에 보인 내용은 혼돈 신호의 발생 구조와 혼돈 시스템의 특징 중 하나인 초기치 민감성을 도식화 한 그래프이다. 혼돈 신호를 발생시키는 초깃값을 X_0과 $\acute{X_0} = X_0 + \delta$ 로 각각 인가하였을 때 두 신호가 서로 상관관계를 같지 않으면서 계산되는 내용을 보여 주고 있다[11,12].

3. 제안된 USN 프로토콜

3.1 결합 혼돈시스템

USN 통신에 사용되는 데이터를 암호화하기 위해 우리는 혼돈 시스템 중에서 가장 일반이고 복잡도가 높은 Logistic map을 사용하였다. 우리가 선택한 Logistic map은 1 차원 계차방정식의 형태를 가지고 있어 하드웨어적 시스템 구현이 용이하여 개발 용량 제한을 받고 있는 Sensor 노드에 탑재시키기 용이하다.

효율적인 USN을 위하여 결합 혼돈 시스템을 구성하여 전송되는 신호를 인증 신호 $C_n^{(id)}$와 데이터 신호 $D_n^{(id)}$로 구분하여 각각의 혼돈시스템의 매개변수를 달리하여 안전성을 증가시켰다.

$$\begin{cases} C_{n+1}^{(id)} = \alpha^{(id)} C_n^{(id)} (1 - C_n^{(id)}) \\ D_{n+1}^{(id)} = \beta^{(id)} D_n^{(id)} (1 - D_n^{(id)}) \end{cases} \quad (2)$$

그리고 $D_n^{(id)}$ 은 $C_n^{(id)}$이 인증된 후에 데이터를 전송하는 구조을 가지고 있어 데이터의 무결성을 보장해 주는 특징도 포함되어 있다.

3.2 혼돈시스템을 이용한 USN 프로토콜

3.2.1 USN 통신 프로토콜

우리가 제안한 USN 인증 프로토콜의 전체 흐름도를 그림 3에 보이고, 각각 (a) 와 (b) 처리 과정을 다음에 보인다.

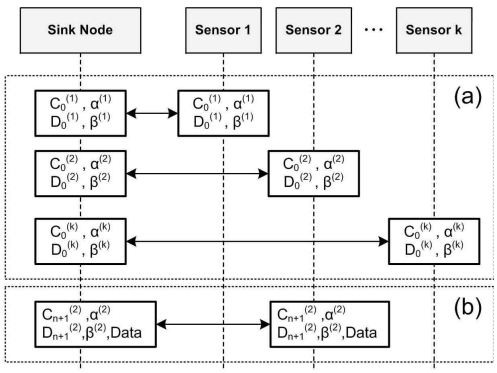

그림 2. 제안된 프로토콜의 구조
Fig. 2. Architecture of Proposed Protocol

단계(a) : 초기 인증 단계

Sink 노드와 Sensor에 구성된 혼돈 시스템의 초깃값과 매개변수를 공유하기 위한 단계이다. 초기 인증 단계가 이루어지면 Sink 노드는 각각 Sensor에 대한 매개변수 $\alpha^{(k)}$, $\beta^{(k)}$와 초깃값 $C_0^{(k)}$, $D_0^{(k)}$ 값을 공유하게 된다.

단계(b) : 데이터 통신 단계

초기 인증 단계를 거쳐 동기화된 매개변수와 초깃값으로 통신채널에 사용될 혼돈 신호를 생성한다. 생성된 혼돈 신호는 난수와 유사하므로 사용되는 통신채널은 무단 공격에 견고하다고 할 수 있다.

3.2.2 USN 인증 프로토콜

USN 통신을 위한 초기 인증 단계로 초깃값과 매개변수 공유 단계에 대한 프로토콜을 그림 4. 에 보이고 인증을 위한 단계별 통신 흐름은 다음과 같다.

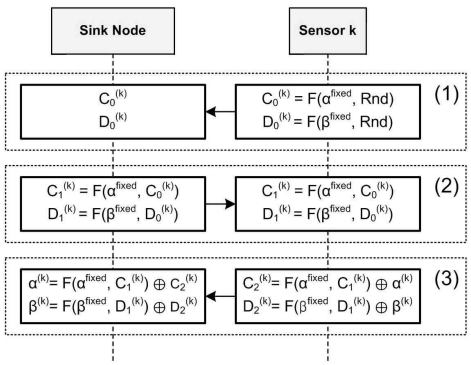

그림 3. 제안된 인증 프로토콜
Fig. 3. Proposed Authentication Protocol

단계(1) : 초기에 Sensor는 고정된 매개변수 α^{fixed},β^{fixed} 값과 난수를 초깃값으로 하여 계산된

혼돈신호 C_0과 D_0을 Sink 노드에 전송한다. C_0은 상호인증을 위한 혼돈 시스템의 초깃값이고, D_0은 데이터 통신을 위한 혼돈 시스템의 초깃값이다.

단계(2) : Sink 노드는 전송 받은 C_0와 D_0를 초깃값으로 하여 C_1과 D_1을 계산하여 Sensor 노드에 전송한다. Sensor는 전송받은 C_1과 D_1을 자체 계산된 값과 비교하여 Sink 노드를 인증한다.

단계(3) : Sensor에서 통신에 사용되는 혼돈 시스템의 매개변수 α^{fixed}와 β^{fixed}를 난수로 교체하여 Sink 노드와 Sensor 노드의 $\alpha^{(k)}$값과 $\beta^{(k)}$값을 분배하여 통신채널을 생성한다.

3.2.3 USN 데이터 통신 프로토콜

상호인증으로 통신채널이 생성된 Sink 노드와 Sensor의 초깃값을 이용하여 데이터를 전송하는 통신 프로토콜을 그림 5에 보이고 그 내용을 다음과 같이 보인다.

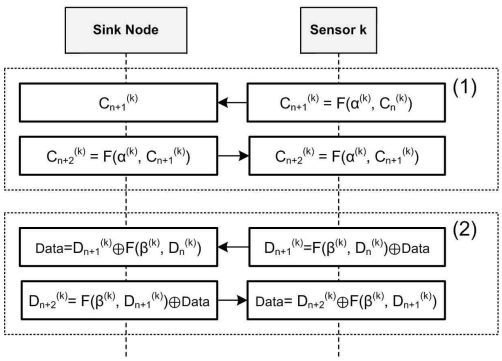

그림 4. 제안된 프로토콜의 구조
Fig. 4. Proposed Communication Protocol

단계(1) : 1단계는 인증 단계에서 분배된 매개변수 $\alpha^{(k)}$값과 초깃값을 이용해서 계산된 C_n을 전송하여 Sink 노드와 Sensor 노드가 서로 타당한 노드인지 검사하는 단계이다. 각각 노드에서 발생되는 혼돈 신호는 동기화되어 있기 때문에 잡음과 유사한 신호이지만 C_{n+1} 값을 계산할 수 있어 현재 통신 중인 노드의 진위를 검증할 수 있다.

단계(2) : 데이터 통신 인증단계에서 문제점이 발생되지 않으면 Sensor 노드에서는 현재 D_n 값으로 발생된 혼돈 신호와 데이터 신호를 XOR 연산하여 Sink 노드에 전송한다. Sink 노드 또한 내부 값 D_n으로 계산된 혼돈 신호와 수신된 데이터를 XOR 연산하여 Sensor 노드의 원 데이터를 복원한다. 복원된 데이터를 같은 처리 과정을 거치며 Sensor 노드에 전송해 원 데이터의 변조 유무를 검증한다.

4. 안정성 분석

본 장에서는 우리가 제시한 혼돈 시스템을 이용한 USN 통신 방법에 대한 안정성을 통신 프로토콜의 요구 사항 및 공격 방법별로 분석한다.

4.1 USN 인증 프로토콜의 요구사항

4.1.1 기밀성

USN 및 통신에 사용되는 데이터는 외부의 무단 도청 공격으로 유출되어도 식별이 불가능하도록 암호화되어 있어야 한다. 본 논문에서 제안된 프로토콜은 시스템에서 발생된 유사난수 신호를 통신 채널로 사용하므로 전송되는 데이터 역시 유사난수 특성을 지니고 있어 데이터에 대한 기밀성이 유지된다.

4.1.2 무결성

우리가 제안한 혼돈 시스템에서 발생되는 신호 X_{n+1}은 X_n에 의해 발생되는 계차 방정식 구조이므로 X_{n+1}이 외부에 의해 스푸핑 공격, 재전송 공격을 받았을 때 X_n에 의해 변조 유무를 확인할 수 있어 데이터의 무결성이 보장된다.

4.1.3 가용성

우리가 제시한 USN 통신은 Sink 노드와 Sensor 노드의 데이터 전송 시 유사 난수로 형성된 통신채널을 사용하고 있다. 그러나 각각 노드는 사용되는 유사 난수를 계산할 수 있기 때문에 원 데이터 대한 접근과 사용이 적시에 보장되어 가용성이 높다고 할 수 있다.

4.2 USN 공격별 안정성 분석

4.2.1 도청 공격

USN 환경에서 Sink 노드와 Sensor 노드는 유선과 무선을 혼용하여 사용되고 있다. 특히 무선통신은 무단 도청 공격에 노출되어 있어 보안에 취약한 특성을 가지고 있다. 우리가 제안한 방법은 유사 난수를 이용한 통신채널을 사용하고 있고 계산되는 유사난수는 X_n 에서 X_{n+1}로 매번 교체되어 대량으로 데이터가 도청 되었더라도 원 데이터를 복원할 수 없게 되어 도청 공격에 강한 특성을 가지고 있다.

4.2.2 스푸핑 공격

스푸핑 공격은 공격자가 Sink 노드나 Sensor 노드에게 자신을 정당한 상대 노드인 것처럼 속이고 거짓 정보로 시스템을 공격하는 방법이다. 우리는 이런 공격에 대처하기 위해 유사 난수 채널을 사용하였고 유사난수는 데이터 전송 시 매번 바뀌어 공격자는 중간에 도청된 데이터로 자신을 네트워크의 정당한 노드로 속일 수 없게 되어 스푸핑 공격에 강한 특성을 보인다.

4.2.3 서비스거부 공격

서비스 거부 공격은 네트워크에서 데이터 전송 시 거짓 정보를 대량으로 전송하여 노드가 마비되게 하는 공격 방법이다. 우리가 제시한 USN 통신 프로토콜은 X_n에 의해 X_{n+1}이 생성되는 통신채널을 사용하기 때문에 데이터 수신 초기가 데이터의 진위를 확인할 수 있어 서비스 거부 공격에 효율적으로 대처할 수 있다.

4.3 암호화 방법의 평가

USN 통신 프로토콜에 사용된 Logistic map 혼돈 시스템의 암호화 정도를 평가하기 위해 이미지를 암호화와 복호화하는 실험을 진행하였고, 그 결과와 각각의 히스토그램을 그림 5에 보인다.

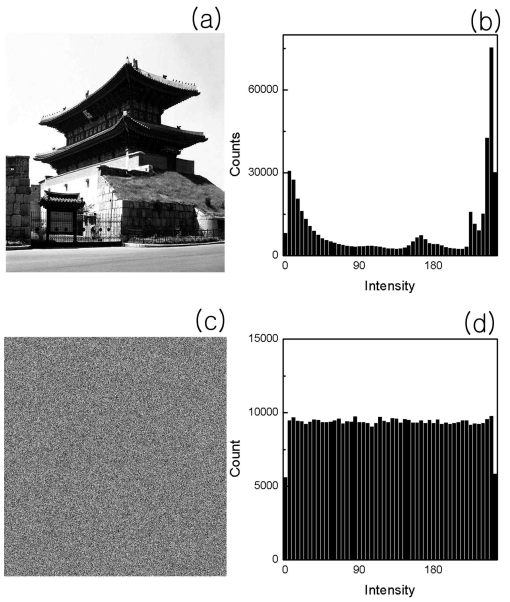

그림 5. 암호화된 이미지의 히스토그램
Fig. 5. Histogram of the cipherimage

5. 결론

USN 환경 구축에 있어서 Sink 노드와 Sensor 노드 간의 원활하고 안정적인 통신도 중요하지만 개인의 사적인 정보를 수집하는 Sensor 노드의 보안도 중요한 요소라고 할 수 있을 것이다.

제안된 USN 통신 프로토콜은 정보를 수집하는 Sensor 노드의 프로그램 메모리 영역 제한과 안전성을 고려하여 혼돈 시스템 중에서 계차방정식으로 구현이 용이하고 비교적 간단한 Logistic map 혼돈 시스템을 사용 하였다. 본 논문에서 제안한 프로토콜은 혼돈 시스템의 매개변수를 공유하는 초기 인증 단계와 데이터를 전송하는 데이

터 통신 단계로 구분되어 있으며 데이터 통신 시 전송되는 데이터는 혼돈 시스템에서 발생되는 유사 난수를 채널로 하여 보안이 강화된 통신이 이루어지기 때문에 기밀성, 무결성, 가용성에 위배되지 않는 효율적인 방법이라고 할 수 있다. 혼돈 시스템을 이용한 USN 환경 구축은 아직 선행연구가 이루어지지 않은 내용으로 이론적인 단계에 머물러 있지만 복잡도가 높거나 차원이 높은 혼돈 시스템을 USN 통신에 적용하는 후속 연구가 추후 계속 이루어진다면 불법적인 공격에 대응할 수 있는 새로운 USN통신 프로토콜로 발전 될 것으로 예측된다.

REFERENCES

[1] D. -H. Shin, “Design of Remote Health Monitoring System Based on USN”, Journal of Korean Institute of Information Technology, vol. 7, no. 4, pp. 183-187, Oct. 2009.

[2] C.-H. Lee, S.-C, Jeong, Y.-S. Ock, and M.-S, Kim, “Development of Water Quality Monitoring System using USN”, Journal of Korean Institute of Information Technology, vol. 10, no. 8, pp. 153-163, 2012.

[3] G.-S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System", Korea Information Assurance Society, vol. 8, no. 3, pp. 57-64, 2008.

[4] G.-S. Yim, and H.-S. Kim, "Chaos-based Image Encryption Scheme using Noise-induced Synchronization", J. of the Korea Society of Computer and Information, vol. 13, no. 5, pp. 155-162, 2008.

[5] G.-S. Yim, "Design and Implementation of Image Encryption Method for Multi-Parameters Chaotic System", Korea Information Assurance Society, vol. 8, no. 3, pp. 57-64, 2008.

[6] J. C. Yen, and J. I. Guo, "A new chaotic key-based design form image encryption and decryption", The 2000 IEEE international symposium on circuits and system, pp. 49-52, May. 2000.

[7] H. E. Ahmed, H. M. Kalash, and O. S. Farag Allah, "An Efficient Chaos-Based Feedbacks Stream Cipher for Image Encryption and Decryption", Information, vol. 31, pp. 121-129, 2007.

[8] F. Fu. Z. Zhang, Y. Chen, and X. Wang, "An Improved Chaos-Based Image Encryption Scheme", International Conference on Computer Science 2007, pp. 575-582, June, 2007.

[9] G. G. Schuster, “Deterministic Chaos: An Introduction: 2nd edition”, VCH, pp. 17-19, Dec. 1997.

[10] A. H. Nayfeh, and B. Blachandran, “Applied Nonlinear Dynamics” Wiley-Interscience, pp. 4-5, 1995.

[11] E. Ott, "Chaos in Dynamical Systems Second Edition", Cambridge University Press, pp. 15-18, Sept. 1996.

[12] G. P. Williams, “Chaos Theory Tamed”, Tayler&Francis, pp. 211-219, 1997.

저자약력

임 거 수(Geo-Su Yim) **[회원]**

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

<관심분야> 시계열분석, 신호처리, 빅데이터분석, FPGA 비전제어