Journal of KIIT. Vol. 22, No. 12, pp. 227-233, Dec. 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.12.227

Big/Little Endian 방식을 적용하여 복잡도를 강화한 자가 재수정 유사 난수 생성기

문 상 국*

A Complexity-Enhanced Self-Reconfiguring Random Number Generator using Big/Little Endian Concept

Sangook Moon*

요 약

본 논문에서는 적외선 통신의 사실상 표준인 NEC 적외선 통신 프로토콜을 분석하고 16비트 주소 공간을 사용하도록 수정하여 목표 시스템에서 최대 216개의 센서 노드를 수용 가능하도록 한다. 간단하지만 효과적인 자가 재구성 유사 난수 주소 생성기를 고안하여 추가적인 암호학적 복잡성을 제고하였다. 이 생성기는 두 S-box의 이전 결과를 반복적으로 공급하는데, 이 이전 결과는 매번 S-box의 입력 시드로 작용하며 주소 암호화가 수행될 때마다 그 값들을 스스로 재구성한다. 제안된 자가 재구성 유사 난수 주소 생성기는 두 개의 16비트 256항목 S-박스 테이블과 하나의 8비트 XOR 논리 연산 쌍만을 필요로 하여 구조가 간단하다. 제안한 주소 생성기의 결과는 상용 라이브러리 기능에서 지원하는 것보다 우수한 암호학적 복잡도 특성을 나타낸다. rag_e3 버전은 2000개의 샘플 중 23개의 중복 값만을 보여주어, 상용 소프트웨어의 난수성에 비해 24.5% 감소된 우수한 결과를 나타낸다.

Abstract

In this paper, we analyze the de facto standard NEC infrared communication protocol and modify it to use a 16-bit address space, thereby allowing the target system to accommodate up to 216 sensor nodes. We have designed a simple yet effective self-reconfiguring pseudorandom address generator to increase cryptographic complexity. This generator repeatedly supplies the previous outcomes of two S-boxes, which act as a random seed and self-reconfigure their values each time address encryption is performed. The proposed self-reconfiguring pseudorandom address generator only requires two 16-bit 256-entry S-box tables and a pair of 8-bit XOR logic operations, making its structure straightforward. The results from the proposed address generator exhibit better statistical features than those supported by the commercial library function. The rag_e3 version displays only 23 redundant values out of 2000 samples, showing a 24.5% reduction compared to the randomness of the commercial software.

Keywords

infrared communication, self-reconfigurable, random number generator, edge-computing

* 목원대학교 전기전자공학과 교수
- ORCID: https://orcid.org/0000-0002-0290-1887

· Received: Nov. 11, 2024, Revised: Dec. 21, 2024, Accepted: Dec. 24, 2024
· Corresponding Author: Sangook Moon
Dept. of Electrical and Electronic Engineering
Tel.: 82+42-829-7637, Email: smoon@mokwon.ac.kr

Ⅰ. 서 론

적외선(IR, InfraRed)은 가시광선 스펙트럼의 붉은 대역의 끝과 마이크로파 사이의 파장을 가진 전자기파이다. 열을 전달하는 능력 덕분에 야간 시야, 온도 측정, 기상 분석, 통신, 센서, 분광학, 미사일 유도를 위한 추적, 의료 치료용 램프 등 다양한 응용 분야에서 널리 사용되고 있다[1]. IR 통신은 뛰어난 장점과 단점을 가지고 있다. 수신기와 송신기 간의 명확한 시야가 확보되어야 하며, 송수신기 사이의 장애물은 허용되지 않으며 통신 범위는 짧다. 이러한 제한에도 불구하고 특정 조건에서 IR 통신은 극히 낮은 전력을 활용하며, 실험적 센서의 비용이 낮다. 따라서 특정 환경에서 IR 통신은 저전력, 단거리 프로젝트에 이상적인 해결책이 될 수 있다[2]. 원자력 발전소, 특히 이차 계통에서 사물인터넷(IoT, Internet of Things) 센서를 사용하는 위험 감지 시스템은 수천 개의 센서에서 주기적인 데이터를 수집하는 데 가능한 한 최소한의 전력이 필요하다. 이러한 특이한 센서 네트워크 환경은 전기 보호를 위한 라디오 주파수 간섭(RFI, Radio Frequency Interference) 제한 및 전자기 간섭(EMI, Electo-Magnetic Interference) 규제가 필요하다[3]. 이러한 까다로운 조건을 만족시키는 IR 통신은 원자력 발전소 위험 방지 시스템과 같은 제한된 환경에서 재평가될 수 있는 특별한 방식이다. 그러나 원자력 발전소를 포함한 전력 시설에 대한 사이버 공격은 수십년 동안 발생해 왔다. 독일에서 2022년에 발생한 Nordex 풍력 터빈 시스템 공격, 2015년 우크라이나 전력망 해킹, 그리고 이란의 스턱스넷 웜과 같은 사이버 공격은 예기치 않은 공정의 중단, 악의적인 자원 도용, 전력 생성 기계에 심각한 피해를 초래할 수 있는 보안 위반의 잠재적 위협을 보여준다[4].

본 논문에서는 생물학적 위험으로 인해 사람이 직접 결함을 감지하기 어려운 원자로의 이차 계통을 타겟으로 가정한다. 또한 결함 감지를 위해 IR 센서 네트워크를 사용할 것이라고 가정한다. 수천 개의 센서 사이에서 IR 통신의 보안을 강화하기 위해 유사 난수 주소 생성기의 새로운 구조를 제안한다. 이 구조에서는 물리적 IR 센서 주소가 암호화가 수행될 때마다 무작위 시드로 반복적으로 재구성한다.

Ⅱ. 적외선 통신

IR 통신에서 가장 널리 사용되는 프로토콜은 NEC 프로토콜이다. NEC 프로토콜은 IR 데이터 거래에 대한 사실상의 표준으로 간주되고 있다. NEC 프로토콜은 펄스 거리로 비트 패턴 인코딩을 규정하는데, 각 비트 표현은 펄스와 공간의 쌍으로 구성된다. 펄스는 38kHz의 주파수로 전송되며, 이는 0.56ms의 주기로 나타난다. 논리적 "1" (참)은 그림 1에 표시된 바와 같이 Pulse-Space-Space-Space의 구조화된 패턴으로 표현되며, 총 0.56ms × 4 = 2.25ms의 시간을 차지한다. 반면에 논리적 "0" (거짓)은 Pulse-Space 패턴으로 표현되며, 총 기간은 1.125ms로, 그림 1에도 나타나 있다.

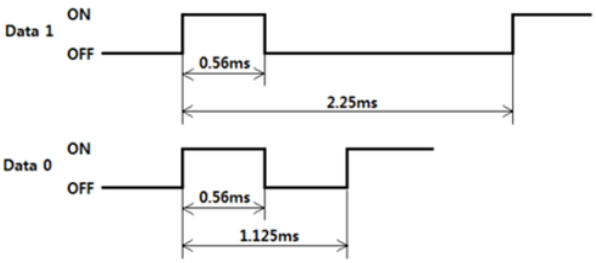


그림 1. NEC 통신 프로토콜의 참과 거짓 파형
Fig. 1. ON and OFF signals of NEC communication protocol and corresponding timing diagram

메시지 전송이 시작될 때, 그림 2에서 볼 수 있는 바와 같이 통신을 설정하기 위한 다음 프로토콜이 실행된다. 먼저, 9ms의 선도 펄스 버스트가 전송되고, 이어서 4.5ms의 스페이스가 따르며, 그 다음에는 27ms 동안의 8비트 슬레이브 장치 주소가 전송된다.

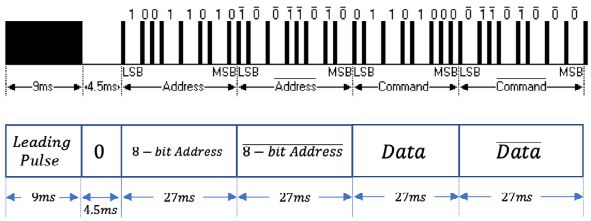


그림 2. NEC 데이터 프로토콜과 데이터 패킷의 지속 시간
Fig. 2. NEC data transmission protocol and corresponding time duration

그 후에는 해당하는 이진 보수값이 27ms 동안 전송되고, 그 다음에는 8비트 명령 (데이터)이 이진 보수 형태로 같은 길이 동안 27 밀리초에 걸쳐 전송된다. 통신은 최종 562.5ms 펄스로 종료된다. 그림 2에서 볼 수 있듯이 데이터는 LSB에서 MSB 순서로 전송된다.

III. 적외선 통신의 보안성 향상

3.1 적외선 통신 보안 이슈

IR 통신은 악의적인 행위자들에 의해 악용될 수 있는 보안 문제를 가지고 있다. IR 통신의 주요 보안 문제 중 하나는 도청이다. IR 신호는 방향성이 없으며, 신호 범위 내의 누구나 신호를 가로챌 수 있다. 이는 공격자가 IR 채널을 통해 전송되는 데이터를 쉽게 가로채고 해독할 수 있음을 의미한다[5]. 또 다른 보안 문제는 간섭이다. IR 신호가 빛 파동이기 때문에 다른 광원으로부터의 간섭을 받기 쉽다. 이는 데이터 전송 오류를 일으켜 데이터가 손상되거나 손실될 수 있다[6]. 게다가, IR 통신은 재전송 공격에도 취약할 수 있다. 재전송 공격은 공격자가 합법적인 IR 신호를 캡쳐한 후, 장치나 네트워크에 무단 접근을 얻기 위해 캡쳐한 데이터를 재전송하는 방식의 공격이다[7]. 이러한 보안 문제를 완화하기 위해 IR 채널을 통한 데이터 전송을 보호하기 위해 암호화를 사용하거나, 도청을 방지하고 신호 범위를 제한하기 위해 방향성 IR 신호를 사용하는 다양한 방법들이 제안되고 있다[8].

3.2 적외선 통신 프로토콜의 확장

본 연구의 목표 테스트 베드는 원자로의 이차 계통으로, 누출, 누설에 보호되어야 하는 파이프에 수천 개의 IR 센서를 배치하여 센서 데이터를 적외선 통신으로 수신 노드로 보내고, 이후에 유선으로 클라우드 서버로 전송할 예정이다. NEC 프로토콜에서는 주소 필드의 반전 비트 길이가 단 8비트로, 수천 개의 센서를 연결하기에는 부족하므로, 이론적으로 최대 2^16 (65536) 개의 센서를 관리할 수 있는 16비트 길이의 주소 필드를 제안한다. 주소 필드의 길이를 제외하고는 사실상 표준인 NEC 프로토콜을 따른다.

이로 인해 그림 3에 표시된 바와 같이 전송 시간의 지연을 121.5ms에서 175.5ms로 변경한다. NEC의 중복된 비트 반전 표현의 독특한 구조 덕분에 "1"과 "0"의 수가 동일해야 하므로, 프로토콜은 동기화 구현을 쉽게 할 수 있다.

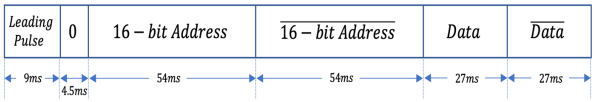


그림 3. 확장된 적외선 통신 프로토콜
Fig. 3. Proposed IR communication protocol expansion

3.3 자가 재구성 유사 난수 주소 생성기

독창적이고 암호학적 복잡도가 뛰어난 자가 재구성 유사 난수 주소를 개발하기 위해, 전체 메시지를 암호화하는 대신 일부 메시지만 부분적으로 암호화하여 연산 부담을 절약하고 데이터 전송 시간을 줄이는 아이디어를 채택했다[5]. 또한, Rijndael에 의해 제안된 비선형 S-box 테이블 쌍(순방향 및 역방향)을 채택했다. 두 테이블은 8비트 입력과 출력을 가지며, 이는 우리가 제안한 IR 프로토콜에 완벽하게 맞는 크기이다. 16비트 주소 필드 중 상위 8비트 주소는 순방향 S-box를 통과시키고, 하위 8비트는 역방향 S-box를 통과시킨다. S-box는 통계적으로 비선형적인 무작위 패턴을 생성하는 것으로 입증되었으며, AES 암호 시스템에 핵심 연산의 역할을 수행한다. 그러나 테이블 매핑 시드 값이 변동적인 무작위 특성을 가지지 않는 한 취약점이 여전히 존재한다.

암호화된 주소가 생성될 때마다 새로운 무작위 시드를 공급하기 위해, 그림 4에 표시한 바와 같이 간단하지만 까다로운 구조를 제안한다. AES S-box가 8비트 인터페이스를 가지고 있다는 점에 착안하여, 이를 통해 두 박스의 결과를 결합하여 16비트를 구성한다. 암호화가 시작될 때, 물리적 주소의 상위 8비트와 암호화된 주소의 상위 8비트(16'b0으로 초기화됨)를 XOR 연산하고, 그 결과를 순방향 S-box에 공급한다. 마찬가지로, 물리적 주소와 암호화된 주소의 하위 8비트를 XOR 연산하고, 그 결과를 역방향 S-box에 공급한다.

각 S-box는 선형 및 차분 암호 분석에 저항하도록 설계되었으며 무작위성을 나타낸다. 각 S-box의 8비트 출력은 신뢰할 수 있는 무작위 주소를 형성하기 위해 결합된다. 각각 새롭게 생성된 암호화된 주소는 다음 주소를 생성하기 위한 시드 값으로 사용되어, 무작위성의 지속적인 재구성을 보장하고 시간이 지남에 따라 보안 강도가 증가한다.

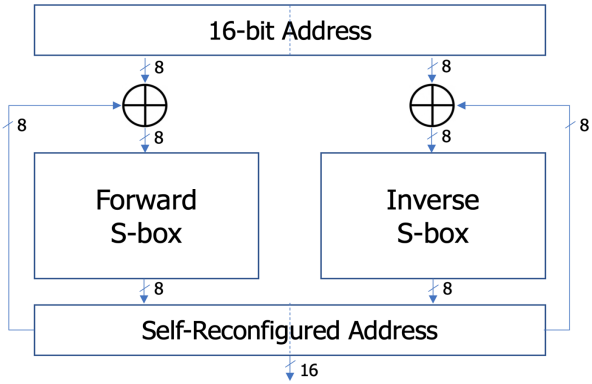


그림 4. 제안하는 자가 재구성 유사 난수 주소 생성기
Fig. 4. Proposed self-reconfiguring pseudo random address generator

3.4 구현

본 연구에서는 IR 통신을 위한 송수신 노드의 보안을 강화하기 위해 자가 재구성 설계를 적용하였다. 그림 5는 원자력 발전소의 이차 계통에서 데이터를 수집하고 암호화된 IR 데이터를 수신 노드로 전송하는 보안 강화 IR 센서 네트워크를 보여준다. CPU를 갖춘 송수신기 노드 쌍의 각 노드에는 자가 재구성 무작위 주소 생성기를 갖추었다. IR 통신은 해당 주소에 따라 송수신기 간에 수행되며, 데이터 전송이 이루어질 때마다 주소는 비선형적이고 무작위적인 방식으로 암호화되어 외부 침입자가 특정 노드를 식별하거나 어떤 노드의 제어권을 획득하지 못하게 한다. 하나의 IR 패킷 (주소 + 데이터)의 처리 시간이 175.5ms로 고정되어 있기 때문에 동기화는 자연스럽게 이루어진다. 이 기간은 송수신 노드에 내장된 CPU가 새로운 암호화된 주소를 재계산할 수 있을 만큼 충분히 길다.

시뮬레이션용 소프트웨어 도구로는 GNU Octave를 사용하였다[9]. 이는 오픈 소스 소프트웨어로, 상용 MATLAB과 유사한 작업을 수행하며 성능도 비슷하다. 수천 개의 주소 데이터를 고성능 행렬 연산을 사용하여 암호화된 데이터로 변환할 때 Octave의 기능을 활용하였다. Octave는 비트 조작 연산도 제공하며, dec2hex() 및 hex2dec() 함수를 행렬과 함께 사용하여 8비트 및 16비트 데이터에서 상위 또는 하위 바이트의 분리와 결합을 효과적으로 제어하여 자가 재구성 유사 난수 주소 발생기를 구현하였다.

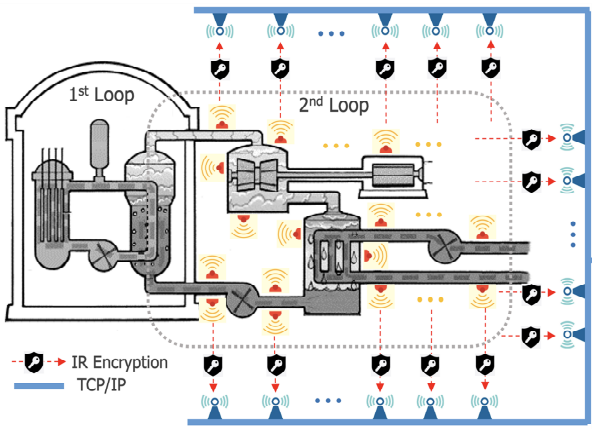


그림 5. 원자로 2차 계통에 부착될 센서들과 적외선 통신으로 연결된 보안 통신 개념도
Fig. 5. Concept diagram of a secure communication system connected with sensors through IR communication in a 2nd loop of a nuclear power plant

Ⅳ. 성능 평가

그림 6은 제안한 무작위 주소 생성기의 기대되는 결과를 보여준다. 이 그림에서는 Octave 도구 라이브러리의 randi() 함수를 사용하여 0에서 1999까지 선형적으로 증가하는 2000개의 테스트 주소 값을 적용하면서 무작위성을 얻었다. 그림 6의 왼쪽 그림은 선형 주소 값들을 나타내는 직선을 나타낸다. 오른쪽 그림은 명확성을 위해 선형 값들과 생성된 무작위 값들을 비교한다. 우리는 중복된 주소 값의 개수를 계산함으로써 무작위성의 강도를 측정했다. randi() 함수는 호출될 때마다 다른 무작위 숫자들을 생성하기 때문에 정확성과 일관성을 보장하기 위해 2000개의 무작위 주소를 2000번 생성하는 과정을 반복했다. 생성된 2000개의 주소 중 중복된 주소 값의 평균 개수는 30.492이였다.

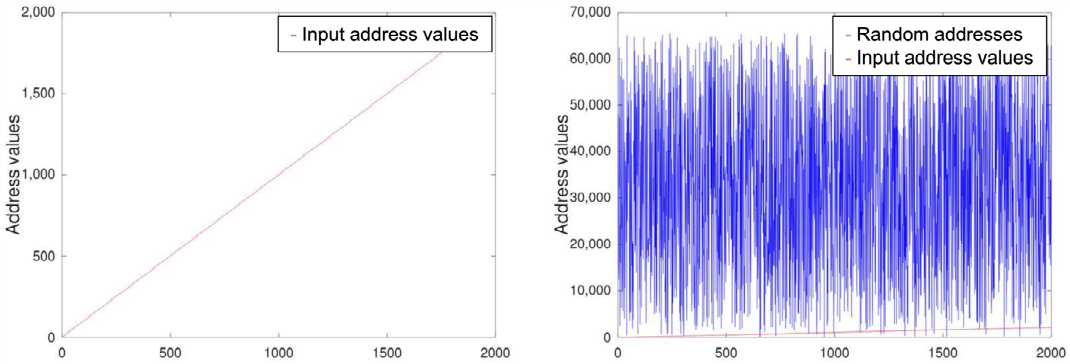


그림 6. randi( ) 함수를 사용한 무작위 주소 생성
Fig. 6. Random address generation using randi( ) function

제안한 구조로 난수 주소 생성기를 구현하였는데, 첫 번째 버전은 (rag) 256개의 샘플 주기를 가진 특이한 규칙성을 나타내며 무작위성이 부족하였다. 이후 S-box 테이블의 모든 단계를 검토하여 행과 열의 특정 교차점이 우연히 동일한 점으로 이어지는 것을 발견했다. 이는 입력 주소 값의 선형 특성 때문에 발생했다고 가설을 세웠다.

앞서 발생한 오류를 피하기 위해, big/little endian 개념을 적용하였다. big endian과 little endian은 메모리나 네트워크 통신에서 바이트가 배열되는 순서를 나타낸다[10]. 먼저 big endian의 순서대로 4개의 니블을 섞는다. 순서는 높은-높은 (Bit[15]-Bit[12])에서 시작하여 높은-낮은 (Bit[11]-Bit[8]), 낮은-높은 (Bit[7]-Bit[4]), 낮은-낮은 (Bit[3]-Bit[0]) 순으로 진행된다. 가장 중요한 두 니블은 순방향 S-box의 행과 열에 사용되고, 가장 덜 중요한 두 니블은 역방향 S-box에 사용된다. 제안한 4가지 방식에서 조합별 성능을 비교 평가한 내용을 표 1에 정리하였다.

표 1. U-Net3+기반 모델과 제안한 모델의 성능 비교
Table 1. Performance comparison between U-Net3+ based model and the proposed model

Category	Structure	Mean	Standard deviation	Duplicated
rag	1-2-3-4	32708	19365	109
rag_e0	4-3-2-1	33090	19033	76
rag_e1	4-2-3-1	31884	18530	31
rag_e2	4-1-2-3	32769	18826	27
rag_e3	4-1-3-2	32958	18962	23
Octave	N/A	32771.5	18910.7	30.492

엔디안 방식을 도입하여 니블 단위로 데이터를 셔플링 하여 초기 입력값으로 적용한 결과, 그림 7에 표시된 바와 같이 오류가 없는 랜덤 주소를 얻을 수 있었다. big-endian을 적용한 결과, 엔디안 개념을 추가하고 rag_e0을 제외한 나머지 구조가 대부분 우수했으며, 특별히 rag_e3에서 암호화된 2000개의 주소의 평균값은 32958, 표준편차는 18962으로 암호학적 랜덤성을 만족시키면서, 생성된 2000개의 주소 중 중복값은 23개로 라이브러리 소프트웨어로 생성한 값보다 우수하였다.

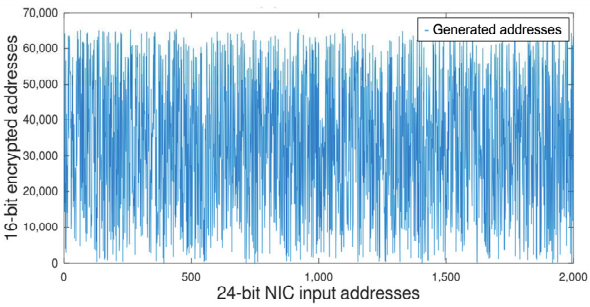


그림 7. 입력 데이터 셔플 적용 후 생성된 무작위 주소
Fig. 7. Generated random addresses after applying input data shuffle

V. 결론 및 향후 과제

본 논문에서는 원자력 발전소의 이차 계통에 설치가능한 센서보드의 적외선 송수신 노드용 자가 재구성 유사 난수 주소 생성기를 사용한 보안 강화 통신 아키텍처를 제안하였다. 또한, 송수신 노드 쌍

의 주소 식별 동기화 과정을 효율적으로 수행하기 위하여 NEC IR 프로토콜의 개선안도 제안하였다.

자가 재구성 주소 암호화 방법을 사용함으로써, 모든 센서의 물리적 주소는 IR 데이터 거래마다 다른 값의 16비트 표현으로 암호화되어 특히 rag_e3의 경우 매우 우수한 통계적 무작위성 특징을 보였다. 이는 외부 침입자가 오픈 채널의 IR 데이터 스트림을 얻을 수 있더라도 제어를 할 수 없는 것을 보장한다. 오버헤드는 256항목의 순방향 및 역방향 S-box 테이블 두 개와 8비트 2입력 XOR 논리연산뿐이며, 이는 기존 IR 통신의 극히 낮은 전력 소비 특성을 활용하면서 보안 강화에 충분히 감내할 수 있는 수준이다.

본 논문에서 제안한 내용은 진행 중인 프로젝트의 일부이며, 향후 작업에서 보안을 이중으로 강화하기 위해 그림 7의 유선 부분과 노드 부분에 더 많은 조치를 추가할 계획이다. 본 연구 결과가 IR 네트워크를 적용하는 모든 시스템에서 사이버 공격으로부터 무선 통신을 보호하는 데 도움이 될 것이라고 확신한다[11].

References

[1] C. E. Ngene, K. E. Adetunji, and T. Shongwe, "Development of an IR-based device for wireless communication in community health centres", 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, Dec. 2018. https://doi.org/10.1109/ICONIC.2018.8601088.

[2] S. Al-nassar, H. R. Hatem, and J. N. Shehab, "Design and implementation of infrared (IR) communication system", International Journal of Engineering Science, Vol. 11, pp. 29-33, Sep. 2018. https://doi.org/10.26367/DJES/VOL.11/NO.3/5.

[3] B. Elbert, "Radio Frequency Interference in Communications Systems", Artech House, USA, Feb. 2016.

[4] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, and L. Wu, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems", Journal of Modern Power Systems and Clean Energy, Vol. 11, No. 3, pp. 727-743, May 2023. https://doi.org/10.35833/MPCE.2021.000604.

[5] M. Kim and T. Suh, "Eavesdroppingvulnerability and countermeasure in infrared communication for IoT devices", Sensors, Vol. 21, No. 24, pp. 8207-8223, Dec. 2021. https://doi.org/10.3390/s21248207.

[6] H. B. Eldeeb, M. Hosney, H. M. Elsayed, R. I. Badr, M. Uysal, and H. A. I. Selmy, "Optimal resource allocation and interference management for multi-user uplink light communication systems with angular diversity technology", IEEE Access, Vol. 8, pp. 203224-203236, Nov. 2020. https://doi.org/10.1109/ACCESS.2020.3036616.

[7] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure secs/gem communications", Sustainability, Vol. 14, No. 23, pp. 15900, Nov. 2022. https://doi.org/10.3390/su142315900.

[8] Z. Chen and G. Srivastava, "A dual chaotic encryption method for lightweight infrared image", Mobile Networks and Applications, Vol. 27, pp. 767-774, Apr. 2022. https://doi.org/10.1007/s11036-021-01906-2.

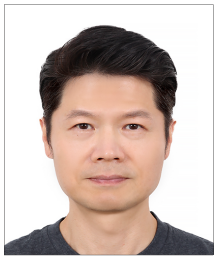
[9] J. T. Trejo, et al., "Experiences in the usage of octave on improving learning mathematics in an engineering faculty", 2021 IEEE World Conference on Engineering Education (EDUNINE), Guatemala City, Guatemala, Mar. 2021. https://doi.org/10.1109/EDUNINE51952.2021.9429162.

[10] D. V. James, "Multiplexed buses: the endian wars continue", IEEE Micro, Vol. 10, No. 3, pp. 9-21, Jun. 1990. https://doi.org/10.1109/40.56322.

[11] S. Suh, S. Lee, H. Moon, B. Kim, and J. Lee, "Utilization of Cyber Deception for Next-Generation Defense Digital Security", Journal of Korea Institute of Information Technology, Vol. 20, No. 1, pp. 1-11, Dec. 2022.

저자소개

문 상 국 (Sangook Moon)



1995년 2월 : 연세대학교 전자공학과(공학사)
1997년 2월 : 연세대학교 전자공학과(공학석사)
2002년 2월 : 연세대학교 전기전자공학부(공학박사)
2002년 2월 ~ 2004년 2월 : SK하이닉스 선임연구원
2004년 3월 ~ 현재 : 목원대학교 전기전자공학과 교수
관심분야 : 데이터 암호화, 마이크로프로세서, 디지털회로설계, IoT 임베디드시스템