적외선통신 암호화 연구

김민철*, 서태원**
*고려대학교 정보보호학과
**고려대학교 컴퓨터학과
e-mail: betamc@korea.ac.kr, suhtw@korea.ac.kr

A Study on Secure Infrared Communication

Minchul Kim*, and Taeweon Suh**
*Graduate School of Information Security, Korea University
**Dept of Computer Science and Engineering, Korea University

요 약

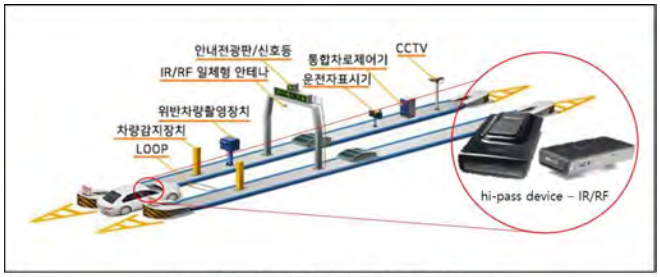
적외선통신은 리모컨이나 하이패스와 같이 주변에서 흔히 보이는 디바이스에서 사용하는 방법이다. 적외선통신을 이용하여 전송을 하게 되는 경우 전파를 이용한 통신에 비해 비용과 유지의 효율성 면에서 이점을 가진다. IoT환경에서 적외선통신은 민감하고 중요한 데이터까지 보내는 수단으로까지 사용되고 있다. 본 논문에서는 이러한 적외선통신을 IoT환경 하에서 안전하게 사용할 수 있도록 두 가지 관점을 제시한다. 적외선통신의 키를 사용하는 방법과 카운터를 사용하는 두 가지의 관점을 설명하고, 이에 대한 평가를 병행한다.

1. 서론

적외선통신은 TV, 에어컨, 오디오, 빔프로젝터 등 무선으로 기기를 조작하기 위해 사용되는 통신 방법이다. 적외선통신을 위해, 송신하는 쪽은 IRED로 수신하는 쪽은 Photodiode로 구성한다. 송신부와 수신부의 구성요소만 보아도 다른 통신 방법들에 비해 회로구성이 간결하고 저렴하며, 유지보수가 간편하다는 점을 알 수 있다. 소비전력이 낮으므로 상대적으로 긴 시간 사용도 가능하다. 빛 중에서도 적외선을 사용하기 때문에, 라디오 주파수를 이용하는 통신(예: Wi-Fi, Bluetooth, 5G와 같은 모바일 통신 등)과 충돌이 발생하지 않고, 전파 규제도 일어나지 않는다. 충돌되는 통신이 없고 전파 규제가 없으므로 적외선으로 통신을 할 경우 사용 가능한 채널의 대역폭이 넓고 채널을 자유롭게 이용할 수 있다. 널리 쓰는 방법임에도 불구하고 적외선통신에 있어 보안에 대한 연구는 찾아보기 매우 어려운데, 적외선통신은 한계를 확실하게 가지고 있는 통신 방법이기 때문이다. 자연광이나 인공광, 대기 중의 먼지에 민감하며 통신을 위해서는 송신기와 수신기가 마주 놓여야 한다. 통신거리도 짧고, 통신 시야각이 좁다는 제한점까지 가지고 있다[1-5]. 바로 이 점들 때문에 이제까지 적외선통신과 관련한 보안연구는 단 한 번도 이루어진 적이 없다. 일정반경 외에서는 통신을 할 수 없고, 송신기와 수신기의 각도가 일정수준을 벗어나면 통신이 되지 않는다. 따라서 제한된 환경 내에서 통신이 일어나는 것에 대해 보안이 필요하지 않다고 생각하여 적외선 통신의 보안 영역을 간과하게 된다. 과거에는 리모컨으로 디바이스의 단순한 기능만을 사용했다면, 지금에 와서는 리모컨 한 개로 결제사항이나 개인정보, 혹은 금융이나 기타 민감한 사항까지 입력하는 경우가 많아졌다. 이 때문에 보안을 위협하는 몇 가지 상황이 발생한다. 첫째는 동일한 공간에 존재하는 사람에 의한 위협이다. 동일한 공간 내에 여러 사람이 함께 있을 때는 송신기가 어디 있는지 알 수 없다. 중요한 회의가 열리고 있는 상황에서, 보조 장치인 빔프로젝터를 인가된 사람이 아닌 공격자가 마음대로 조작할 수 있다. 또한 공격자는 오디오 장치를 악의적으로 이용하여 회의를 방해할 수도 있다. 둘째는 적외선이 투명한 매질을 통과 할 수 있는 성질을 이용한 보안 위협이다. 이를테면 외부에서 창문이나 유리벽을 통해 집안에 있는 IPTV를 볼 수 있다. 사회 공학적 기법을 통해, 설정해놓은 비밀번호나 결제관련 정보를 유추할 수 있게 되면 금전적인 피해를 입을 확률이 커진다. 셋째는 첫 번째와 두 번째 항목과 연관하여, 적외선 레이저를 이용하여 다른 장소에서 디바이스를 마음대로 조작할 수 있다는 원거리 위협이다. 넷째는 공개된 공간에서 적외선 통신을 사용하는 경우에

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00533, 컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지대응)

서 발생하는 오픈 데이터에 의한 위협이다. 그림 1의 (a)와 같이, 고속화도로에서 상용화된 하이패스는 적외선을 사용하는 IR방식과 라디오 주파수를 사용하는 RF방식이 있다[6]. IR방식의 디바이스를 사용하는 사용자에게는 주차가 되어 있더라도 상시 배터리로 디바이스가 동작할 경우이거나 도로를 주행하는 경우 모두 공격에 노출되어있다. IR방식은 누구든 볼 수 있게 열려있기 때문에, 데이터 수집이 쉽기 때문이다. 본 논문에서는 이러한 공격이 가능하게 된 배경으로, 2장에서 적외선통신 프로토콜에 대해 살펴본다. 3장에서는 이러한 공격을 방지하기 위한 방어 방법에 대해 소개하면서, 공격 방법에 따른 취약점을 분석한다. 이를 토대로 4장에서는 적외선통신에 대한 보안을 총체적으로 분석하며 결론을 내린다.



(a) 국내 고속도로 자동결제 시스템 (hi-pass)

(b) IPTV

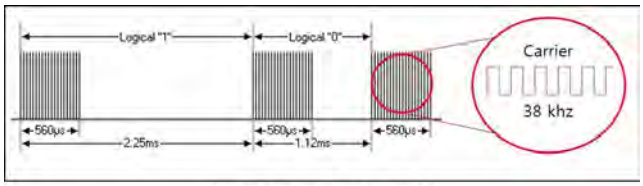
(그림 1) 실생활 적외선통신

2. 선행연구

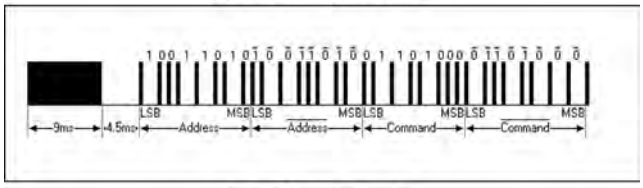
2.1. 적외선통신 프로토콜

적외선통신은 회사마다 다른 프로토콜을 사용한다. 본 논문에서는 대표적인 프로토콜인 NEC 방식[4]을 분석한다. 그림 2의 (a)에서와 같이 데이터 '1'과 데이터 '0'이 나타난다. 데이터 '1'은 560μs동안 38khz의 캐리어를 이용하여 신호를 보낸 뒤, 1690μs동안 아무 신호도 보내지 않는다. 데이터 '0'은 560μs동안 38khz의 캐리어를 이용하여 신호를 보내고 나서 560μs동안 아무 신호도 보내지 않는다. 이렇게 데이터 '1'과 '0'이 구분된다.

적외선통신은 비대칭통신이므로 데이터를 구분 짓기 위해 선행비트(Start bit)가 필요하다. NEC 프로토콜에서는 선행비트로 9ms동안 캐리어를 이용하여 신호를 보낸 후 4.5ms동안 아무 신호도 보내지 않는다. 데이터를 구분한 다음 데이터를 보낼 수 있다. 데이터는 기기를 식별할 수 있는 주소(address)와 명령(command) 부분으로 나뉜다. 두 부분의 데이터 사이즈는 각각 8bit으로, 주소와 명령 데이터는 수신이 잘 됐는지 판별하기 위해 데이터 '0'과 '1'을 서로 바꾸는 토글 과정을 거쳐 보낸다. 총 주소를 보내는데 16bit, 명령을 보내는데 16bit, 선행비트를 제외한 총 32bit의 데이터를 보낸다.



(a) 데이터 '1'과 '0'의 표현



(b) NEC 프로토콜 구조

(그림 2) NEC 프로토콜 적외선통신 방법

2.2. 적외선통신 도청방법

적외선통신은 그림 3의 (a)와 같이 적외선수신센서와 마이크로컨트롤러만 있으면 손쉽게 도청할 수 있다. 그림 3의 (b)는 LG 리모컨을 분석한 것이며, 데이터를 보낼 때 NEC 방식을 사용하는 것을 알 수 있다.

(a) 리모컨과 마이크로컨트롤러와 적외선센서 (b) 리모컨 데이터

(그림 3) 적외선통신 도청방법

3. 적외선통신 보안방법

적외선통신에서 보호하고자 하는 부분은 주소(address)부분이다. 명령(command)부분에 비밀번호와 같이 민감한 데이터가 들어 있음에도 불구하고 이를 보안하지는 않는다. 명령부분을 도청한다고 해

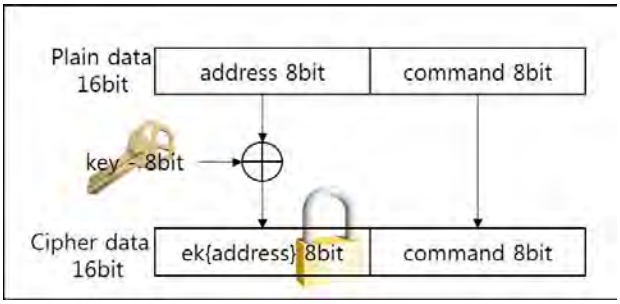
도 주소가 일치하지 않으면 적외선통신이 동작하지 않기 때문이다. 여기에서 더 고려해야 할 사항은 통신에 대한 보안을 기본으로 하되, 빠른 반응속도를 유지할 수 있도록 디자인해야 한다는 것이다. 과한 암호화는 사용자관점에서 작업을 저해하는 요인으로 작용하므로 업무 효율을 낮춘다.

3.1. 키를 사용한 보안

적외선통신에서 데이터 '1'과 '0'으로 인코딩되기 전 키를 이용하여 암호화하는 방법이다. 이를 위해 블록암호 전반을 사용할 수 있다. 블록암호 중 가장 간단한 데이터와 키를 XOR연산 하는 치환암호를 소개하면 다음과 같다.

8bit data ⊕ 8bit key = 8bit encrypted data (1)

(1)의 키를 이용한 보안은 고유한 주소를 숨기는데 도움이 된다. 그러나 주소와 동일한 키를 이용해 안전하게 사용하기 위해선 키 관리가 중요하다. 키가 항상 같다면 재전송 공격이 가능해지기 때문에 결국 문제가 발생할 수 있으므로 키를 주기적으로 바꾸어 주어야 한다. 어떠한 블록암호에서도 시간에 따라 값이 바뀌지 않으면 재전송 공격에 취약할 수밖에 없다. 그럼에도 불구하고 키를 이용한 보안을 사용하기 좋은 이유는 적외선통신이 도청하기 힘든, 홈 IoT 환경에서 사용할 수 있기 때문이다.

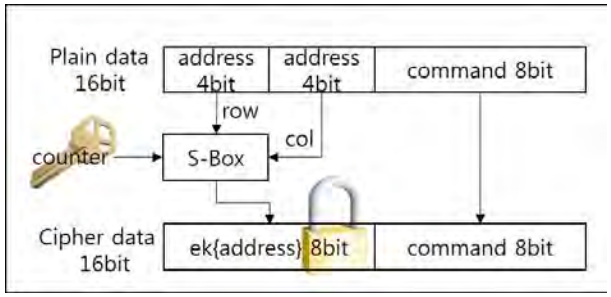


(그림 4) 키를 사용한 보안

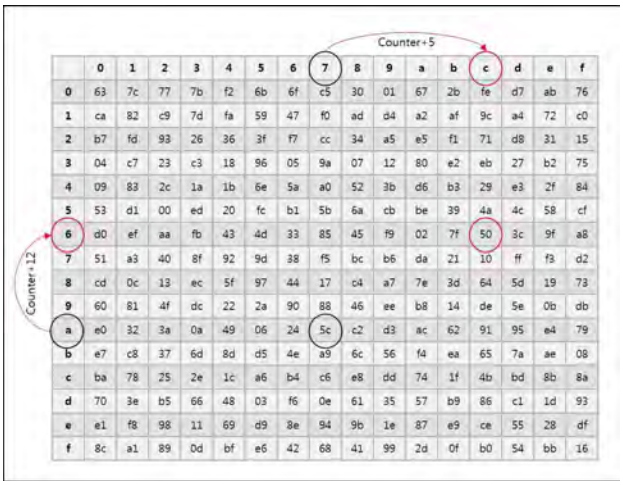
3.2. 카운터를 사용한 보안

카운터는 송신부와 수신부가 일치되었을 때만 정상적인 데이터로 판단하는 목적으로 사용한다. 따라서 카운터를 사용하는 보안은 사전에 카운터 동기화가 필요하다. 카운터를 위해 보안에 사용된 테이블은 미국의 NIST 표준인 AES(Advanced Encryption Standard) 암호[7]의 S-Box를 이용하였다. S-Box를 사용하는 이유는 전단사함수를 이용하여 복호화하는데 짧은 시간이 소요되기 때문이다. 또한 S-Box를 이용하면 선형분석(LC: Linear Cryptanalysis)에 대해 안전함을 보인다[8-10]. 그림 6의 표는 S-box이며 그림 5와 같이 행에 주소 4bit과 열에 주소 4bit을 이용한다. 카운터는 총 2개를 사용하며 행 카운터, 열 카운터를 사용한다. 초기에 카운터를 동기화하며 카운터의 시프트 연산을 통해 매번 입력할 때마다 값을 변경한다. 연산 후 최종 값을 주소로 사용한다. 그림 6을 보면 주소가 a7일 때, 카운터를 사용하지 않으면 5c로 고정된 출력을 가진다. 카운터를 사용할 때, 카운터에 의해 초기 주소가 6c가 되며 S-Box의 출력인 50을 주소로 사용한다. 또한, 카운터가 증가됨에 따라 출력이 바뀐다. 이전 카운터를 사용한 것과 다음에 사용한 카운터의 연관성은 S-Box에 의해 없으며 두 개의 카운터를 알지 못하면 복호화하기 어렵다. S-Box와 카운터 연산 후 결과인 50 (0101 0000)을 주소로 사용하여 IRED를 통해 데이터를 보낸다.

카운터를 이용한 보안의 경우 하드웨어와 소프트웨어가 오픈되어있다는 전제 하에서 카운터 값을 찾으면 공격자에게 기기의 주도권을 박탈당하게 된다. 이 때, 인가된 사용자의 리모컨은 더 이상 기능하지 못하게 된다. 따라서 카운터를 사용했을 때 일정 횟수 실패하면 카운터를 다시 동기화 할 수 있게 디자인해야 한다.



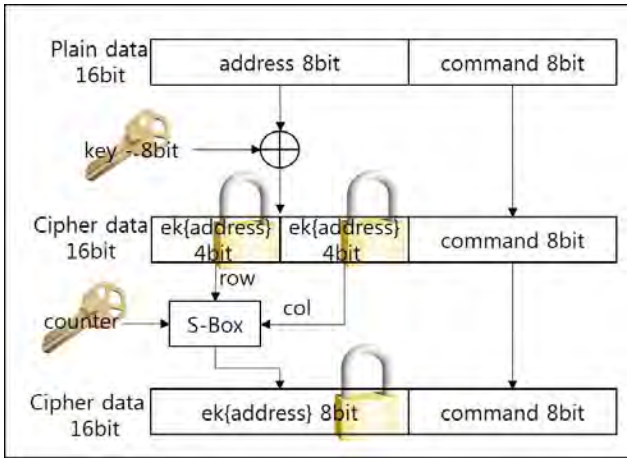
(그림 5) 카운터와 S-Box를 이용한 보안



(그림 6) S-Box와 카운터를 이용한 연산

3.3. 키와 카운터를 사용한 보안

3.1.키를 이용한 보안과 3.2.카운터를 이용한 보안을 믹스하여 둘의 단점을 보안한 것으로 주소값이 키에 의해 보호되며 키를 일정 시기마다 변경하게 되면 S-Box에 의해 전혀 다른 값이 나오게 되어 안전해진다. 그림 7은 그림 4와 그림 5의 융합된 형태로 구성되어 있으며 주소를 암호화한 후 S-Box와 카운터를 이용하여 암호화한다.



(그림 7) 키와 카운터, S-Box를 사용한 보안

4.결론

빛을 사용하는 적외선 통신은 라디오 주파수에 비해 혼선이 발생하지 않는다. 빛을 사용하는 방식으로 통신하기 때문에 채널을 제한 없이 사용할 수 있다. 통신에 필요한 송/수신 센서도 저렴하기 때문에 설계와 보수의 비용이 저렴하다. 또한 소비전력이 낮기 때문에 유지비용도 낮다는 장점까지 가지고 있다. 이러한 적외선통신은 우리가 의식하지 못하는 사이 리모컨이라는 이름으로 익숙하게 사용되고 있다. 그러나 이에 대한 보안 연구는 정작 이루어지지 않고 있다. 적외선통신으로 개인정보나 자산에 영향을 주는 데이터를 주고받는 상황이 늘어났으므로, 이를 효과적으로 보안할 수 있는 방법 또한 고안되어야 한다. 단순히 데이터를 암호화하는 것에 그칠 것이 아니라, 환경을 고려하여 보안 할 수 있는 방법을 찾는 것이 중요하다. 보안의 효율성과 사용자의 편리성은 반비례한다. 어느 쪽을 더 중요하게 여기는가에 따라 보안의 방향이 결정된다. 본 논문에서 제시한 보안 방법은 다소 보안에 치우친 것처럼 보이지만, 사용자의 편리성을 위해 하드웨어의 처리를 고려하여 최소의 보안으로 최대의 효과를 내기에 적합하다. 보안의 정도를 높이면서도 사용자에게 편리한 환경을 제공할 수 있는 보다 발전된 연구가 필요하다.

참고문헌

[1] H. Du and G. Xu, "Infrared indoor wireless MIMO communication system using 1.2GHz OOK modulation," in China Communications, vol. 16, no. 5, pp. 62-69, May 2019.

[2] M. Sugimoto, K. Aoyama and A. Kongoh, "Improvement of traffic control system by means of infrared beacon two-way communication," ITSC2000. 2000 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.00TH8493), Dearborn, MI, USA, 2000, pp. 258-263.

[3] F. Arvin, K. Samsudin and A. R. Ramli, "A Short-Range Infrared Communication for Swarm Mobile Robots," 2009 International Conference on Signal Processing Systems, Singapore, 2009, pp. 454-458.

[4] S. Ohtsuka, S. Hasegawa, N. Sasaki and T. Harakawa, "Communication System between Deaf-Blind People and Non-Disabled People Using Body-Braille and Infrared Communication," 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010, pp. 1-2.

[5] Wang Xianzhen, Yan Huan, Miao Changyun and Zhang Cheng, "The design of locomotive alarm and parking system based on infrared communication," 2010 Second Pacific-Asia Conference on Circuits, Communications and System, Beijing, 2010, pp. 5-8.

[6] 한국도로공사, Available: https://www.ex.co.kr/

[7] Standard, NIST-FIPS. "Announcing the advanced encryption standard (aes)." Federal Information Processing Standards Publication 197.1-51 (2001): 3-3.

[8] Keliher, Liam. "Refined analysis of bounds related to linear and differential cryptanalysis for the AES." International Conference on Advanced Encryption Standard. Springer, Berlin, Heidelberg, 2004.

[9] Musa, Mohammad A., Edward F. Schaefer, and Stephen Wedig. "A simplified AES algorithm and its linear and differential cryptanalyses." Cryptologia 27.2 (2003): 148-177.

[10] Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.