KIPS Trans. Comp. and Comm. Sys.
Vol.11, No.1 pp.35~42
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2022.11.1.35

A Study on Secure Encoding for Visible Light Communication Without Performance Degradation

Minchul Kim† · Taeweon Suh††

ABSTRACT

Visible light communication (VLC) is a method of transmitting data through LED blinking and is vulnerable to eavesdropping because the illumination affects the wide range of area. IEEE standard 802.15.7 defines On-Off Keying (OOK), Variable Pulse Position Modulation (VPPM), and Color Shift Keying (CSK) as modulation. In this paper, we propose an encryption method in VPPM for secure communication. The VPPM uses an encoding method called 4B6B where 16 different outputs are represented with 6-bit. This paper extends the number of outputs to 20, to add complexity while not violating the 4B6B generation conditions. Then each entry in the extended 4B6B table is scrambled using vigenère cipher. The probability of decrypting each 6-bit data is $\frac{1}{20}$. Eavesdropper should perform $\sum_{k=1}^{n} 20^k$ number of different trials to decrypt the message if the number of keys is n. The proposed method can be applied to OOK of PHY II and CSK of PHY III. We further discuss the secure encoding that can be used in OOK and CSK without performance degradation.

Keywords : Visible Light Communication, Secure Encoding, Secure Communication, On-off Keying, VPPM

가시광 통신에서 성능 저하 없는 보안 인코딩 연구

김 민 철† · 서 태 원††

요 약

가시광 통신은 LED의 빠른 점멸을 통해 데이터를 보내는 통신 방법이며, 조명이 영향을 미치는 범위가 넓어 도청에 취약하다. IEEE 표준 802.15.7에서는 가시광 통신을 위해 OOK(On-Off Keying), VPPM(Variable Pulse Position Modulation), CSK(Color Shift Keying)를 모듈레이션을 정의한다. 이 논문에서는 VPPM을 사용한 통신에서 보안을 위한 물리계층 암호화를 제안한다. VPPM은 4B6B를 사용하여 메시지를 인코딩하는데 16개의 출력을 6-bit를 사용해 표현한다. 제안하는 인코딩은 4B6B의 생성조건을 위배하지 않으며 복잡도를 높이기 위해 20개의 출력으로 확장한다. 그리고 확장된 4B6B 테이블의 각 출력을 vigenère cipher를 이용하여 암호화한다. 도청자가 암호화된 각 6-bit 데이터를 복호화할 확률은 $\frac{1}{20}$이다. 따라서 키의 개수가 n일 때 도청자는 메시지를 복호화하기 위해 최대 $\sum_{k=1}^{n} 20^k$ 만큼 전수조사해야 한다. PHY II의 OOK와 PHYIII의 CSK에서도 입력과 출력을 관리하는 테이블을 사용하기 때문에 제안하는 방식을 적용할 수 있다. 본 논문에서는 OOK와 CSK방식에서도 성능 저하 없이 사용할 수 있는 보안 인코딩에 대해 논의한다.

키워드 : 가시광 통신, 보안 인코딩, 통신 보안, On-Off Keying, Variable Pulse Position Modulation

1. 서 론

가시광 통신(Visible Light Communication: VLC)은 LED를 이용하여 데이터를 보내는 디지털 통신이다. Table 1은 가시광 통신의 IEEE 표준 802.15.7 [1]에서 분류한 운영 모드의 특징을 보여준다. PHY I과 II는 조명을 빠르게 켜고 끔을 이용하여 데이터를 생성한다. PHY I은 실외환경에 적합하게 설계되어 있으며 II는 실내 환경에 적합하게 설계되어 있다. 표1에서 보듯 PHY II는 I보다 데이터 전송속도가 빠르다. 실외환경의 경우, 외부의 빛에 영향을 많이 받기 때문에 상대적으로 저속으로 설정되어 안전하게 데이터를 전송하게 설계되어 있다. PHY III은 백색광의 원리를 이용하여 통신한다. 백색광은 빛의 구성성분인 빨강(R), 초록(G), 파란색(B)을 조합하여 만들 수 있다. 이를 이용하여 사람은 구분할 수 없는 색의 차이로 데이터를 만들어 보낸다.

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2019-0-00533, 컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지대응, IITP-2019-0-01343).
† 준 회 원 : 고려대학교 정보보호학과 박사과정
†† 종신회원 : 고려대학교 컴퓨터학과 교수
Manuscript Received : October 13, 2021
First Revision : December 7, 2021
Accepted : December 27, 2021
* Corresponding Author : Taeweon Suh(suhtw@korea.ac.kr)

Table 1. VLC Operating Modes

Operating mode	Modulation	RLL code	Data transfer rate
PHY I	OOK	Manchester	11.67-100 kb/s
	VPPM	4B6B	35.56-266.6 kb/s
PHY II	OOK	8B10B	6-96 Mb/s
	VPPM	4B6B	1.25-5 Mb/s
PHY III	CSK	-	12-96 Mb/s

가시광 통신은 빛을 이용한 통신이기 때문에 보안에 있어 두 가지 장점이 있다. 첫 번째 장점은 조명이 영향을 미치는 공간만 통신할 수 있으므로 물리적으로 통신이 되는 범위가 만들어진다는 것이다. 하나의 조명은 대략 2~3 m의 지름의 면적에 영향력을 가진다. 따라서 가시광 통신이 목표로 하는 통신은 PAN(personal area network)이다. PAN은 개인의 작업공간을 중심으로 디바이스들을 서로 연결하기 위한 네트워크로 가정이나 회사에서 사용하기 적합한 통신망이다. 조명의 영향이 미치는 범위 내에서 통신할 수 있으므로 도청자가 사용자의 공간에 함께하지 않는 이상 도청이 불가능하다. 두 번째 장점은 통신하는 빛 이외의 광원으로 도청에서 벗어날 수 있다는 것이다. 빛을 사용하는 통신의 특성상, 통신하는 빛 이외에도 자연광을 비롯하여 무수한 조명으로부터의 인공광이 존재한다. 이러한 광원은 통신에 방해를 유발할 수 있으나, 역설적으로 통신을 보호하는 역할을 하기도 한다. 후자의 원리를 이용하여 여러 조명을 사용하는 MIMO (Multiple-input Multiple-output) 연구가 활발히 진행 중이다 [2-6]. 이러한 연구는 사용자와 조명이 통신할 때, 도청자가 같은 공간에 있는 것을 가정한다. 통신에 사용되는 조명은 사용자에게 최단 거리에 위치하며, 개개의 통신 조명은 각기 다른 사용자를 위해 존재한다. 각각 다른 통신을 위한 조명은 사용자 한 명의 조명이 영향을 미치는 공간 안에 도청자가 있더라도 빛의 간섭을 통해 도청을 불가능하게 한다.

Fig. 1은 MIMO 환경에서 도청자가 존재할 수 있음을 보여준다. Fig. 1의 ① 도청자는 사용자가 통신을 할 때 사용자보다 더 가까운 위치에 존재할 수 있다. 이와 같은 상황은 오히려 사용자가 다른 빛의 간섭으로 도청자보다 통신에 좋지 않은 상황을 야기한다. Fig. 1의 ② 도청자는 통신을 하는 공간 밖에 존재할 수 있다. 빛은 창문과 같은 투명한 매질을 통과할 수 있으며, 문틈이나 열쇠 구멍과 같은 틈으로 빛이 새어 나올 수 있기 때문이다. Fig. 1의 ③ 도청자는 통신 중인 조명을 관측할 수 있는 장소에 존재할 수 있다. 가시광 통신은 포토다이오드를 이용해 데이터를 수신하는 연구도 있지만, 카메라를 이용하여 데이터를 수신하는 연구도 진행 중이다[7-9]. 이러한 방법은 비교적 먼 거리에서 데이터를 수신받을 수 있지만, 한편으로는 도청을 야기할 수 있다.

Fig. 2는 계속 켜져 있는 LED와 300 bits/s의 속도로 데이터를 보내는 LED를 CMOS 카메라를 이용해 촬영한 것이다. (a)와 다르게 (b)는 빛의 띠가 형성되어 있음을 알 수 있다. 이같이 통신하는 방법을 CMOS 카메라를 이용한 rolling shutter라고 한다. 이러한 방식은 센서를 사용하는 가시광 통신에 있어 부 채널 공격이 가능해지는 것을 의미한다. 가시광 통신의 기본 메커니즘은 조명을 켜고 끄는 것을 이용하는 디지털 통신이므로 카메라를 이용하여 조명이 꺼져있는 것과 켜지는 것이 촬영이 가능할 경우 데이터를 수집할 수 있는 것을 의미한다. 또한, 카메라의 성능은 계속 발전 중이다. 최근 개발된 카메라의 경우 1초에 70조 프레임을 찍을 수 있다 [10]. 시판 중인 스마트 폰의 경우 최대 초당 1,000 프레임까지 고속 촬영을 지원한다. 이 스마트 폰은 1 kHz의 샘플링을 가진 수신기가 될 수 있다. 1 kHz이하로 통신하는 경우 카메라로 도청할 수 있다.

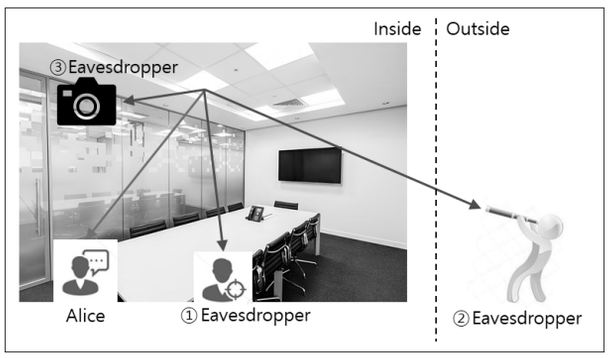
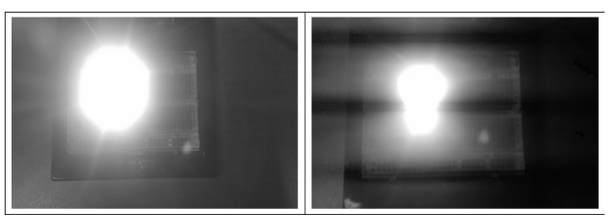


Fig. 1. Eavesdropper's Locations



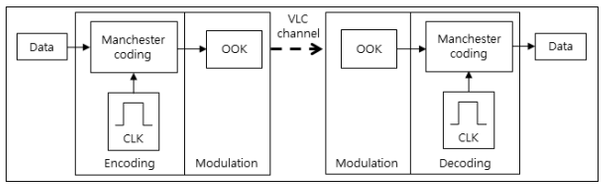
(a) (b)

Fig. 2. VLC Receiver using Camera (a) LED is Continuously Turned on (b) LED is Turned 300 Times on and off During 1s

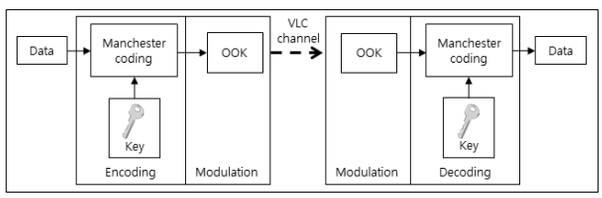
데이터를 주고받을 때 보안은 상위 계층에서도 가능하지만, 물리계층부터 보안을 제공하면 데이터 캡슐링을 통해서 보다 강력한 보안을 제공할 수 있다. 이를 구현하기 위해서는 추가적인 하드웨어가 필요하거나 소프트웨어의 도움이 필요하며, 암호를 처리하기 위한 동작 시간이 증가하는 것은 피할 수 없다. 본 논문에서는 IEEE 표준 802.15.7의 인코딩을 분석하여, 추가되는 하드웨어를 줄이고 처리속도를 최소화하는 보안 인코딩을 제안한다. 가시광 통신은 디지털 통신이기 때문에 모듈레이션 과정이 인코딩 과정과 통합하여 작동한다. 인코딩은 하드웨어로 설계되어 있으므로 이 과정에서 암호를 사용하면 하드웨어가 추가된다. 하드웨어 추가로 발생하는 비용을 절감하기 위해 최적화가 필요하다. 처리시간 또한 생각해 볼 문제이다. 통신 지연[11]은 프로세싱 지연, 큐잉 지

연, 전송 지연, 전파 지연으로 크게 네 가지로 분류된다. 프로세싱 지연은 제안하는 인코딩에서 발생 가능성이 있기는 하지만 통신에 지장을 줄 정도는 아니며, 다른 세 지연은 기존의 IEEE 표준 802.15.7에서 사용하는 것과 동일하다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 가시광 통신에서 도청 위협에 대한 연구와 PHY I의 OOK(On-Off Keying)방식에서 사용한 맨체스터 코딩을 대체하는 보안 인코딩을 소개한다. 3장에서는 PHY I과 II의 VPPM(Variable Pulse Position Modulation) 인코딩을 대체하는 보안 인코딩을 소개한다. 4장에서는 보안 인코딩에 대한 운용방법과 그에 대해 평가를 하며 5장에서는 PHY II의 OOK와 PHY III의 CSK(Color Shift Keying)에 대해 제안하는 보안 인코딩의 적용 가능성에 대해 논의한다. 마지막으로 6장은 본 논문에 대해 마무리한다.



(a) OOK using Manchester encoding [1]



(b) OOK using encryption [14]

Fig. 3. Difference between IEEE Standard 802.15.7 OOK[1] and OOK using Encryption[14]

2. 관련 연구

2.1 가시광 통신에서 도청 위협에 대한 연구

가시광 통신은 조명을 이용하여 통신하기 때문에 조명 아래에 있는 사용자만 데이터를 수신할 수 있다. 바닥과 천장을 제외한 사방이 투명하지 않은 벽에 막혀있어야 하며, 인가되지 않은 사용자(도청자)는 해당 공간에 존재하지 않는다는 점이 전제이다. 그러나 보안을 중요시하는 국가 단위 연구소나 큰 회사와 같은 곳이 아닌, 가정이나 일반 회사는 이러한 환경을 조성하기 어렵다. Jiska [12]는 실생활과 유사한 환경에서 가시광 통신에 대한 도청을 연구했다. 문틈으로 들어오는 빛과 열쇠 구멍을 통해 들어오는 빛, 그리고 유리창을 통해 새어 나가는 빛을 도청하여 데이터를 수집했다. 이 논문은 MIMO 환경을 고려하지 않은 단일 조명에 관해서만 연구되어 있다. 가시광 통신이 실용화된다면 하나의 조명만 사용하는 환경이 생기는 부분을 간과할 수 없기 때문이다. Mordechai [13]는 데이터를 훔치기 위해 악의적인 프로그램을 컴퓨터에 설치하고, 컴퓨터 하드의 LED를 이용하여 모스부호를 통해 데이터를 탈취하는 실험을 하였다. 이 과정에서 창문 밖에 드론을 이용하여 초당 천장의 사진을 찍는데, 악의적인 프로그램이 설치된 컴퓨터로부터 데이터를 수신했다. 외부에서 드론과 같은 비행물체에 매달린 카메라로 도청을 하면 가시광 통신의 장점인 공간의 한정성은 없어진다.

2.2 PHY I의 OOK 방식에서 적용된 보안 인코딩

Fig. 3은 IEEE 표준 802.15.7의 PHY I의 OOK 방식 [1]과 보안 인코딩 방식 [14]을 보여준다. IEEE 표준 802.15.7의 OOK 방식은 표1에서와같이 RLL code로 맨체스터 코딩을 사용하며, '0'일 때 끄고 '1'일 때 켜는 모듈레이션이다. 이 맨체스터 코딩은 2진(0/1) 데이터에 클록(CLK)을 XOR 연산하는 방식이다. 선행된 보안 인코딩은 클록을 대신하여 키와 XOR 연산을 하는 방식이다. 이 방식은 하드웨어 자원을 추가로 사용하지 않으며 처리속도가 기존과 동일하다.

보안 인코딩 방식에서는 사용할 수 없는 키가 존재한다. 맨체스터 코딩은 클록과 XOR 연산을 하므로 데이터가 '0'이나 '1'일 때 조명은 절반의 시간 동안 항상 켜져 있고, 절반의 시간 동안 항상 꺼져있다. 그러나 보안 인코딩은 키에 의존하기 때문에 키 선정이 중요하다. 키는 조명이 꺼질 수 있는 0000, 0011, 1100, 1111을 사용할 수 없다. 키와 데이터를 먼저 XOR하고 맨체스터 코딩으로 데이터를 보낼 수 있으나, 이 경우 XOR 연산을 두 번 수행해야 하며, 이는 하드웨어 비용이 추가되고, 처리속도 역시 두 배의 시간이 걸림을 의미한다. 키와 데이터를 먼저 XOR 하는 것은 데이터 1-bit와 키 1-bit가 연산 되지만, 제안된 보안 인코딩은 데이터 1-bit와 키 2-bit가 연산 되기 때문에 전자보다 보안 강도는 두 배 증가한다.

3. 가시광 통신에서 제안하는 보안 인코딩 방식

Fig. 4는 논문에서 제안하는 시스템의 구조이다. 사용자의 상태와 조명의 상태를 알려주기 위해 CSI(Channel State Information)를 사용하여 서로에게 적합한 통신이 이루어지도록 만든다. 상용화됐을 때를 고려하면 실내환경과 실외환경을 선택할 수 있어야 한다. 또한, 데이터 통신을 하기 전에 적합한 모듈레이션 방법을 선택할 수 있어야 최적의 통신을 할 수 있다. 이 과정에서 키를 전송한다.

Fig. 5는 IEEE 표준 802.15.7의 PHY I, II의 VPPM에서 사용하는 4B6B 방식과 제안하는 보안 인코딩 방식을 보여준다. 4B6B 방식은 세 가지를 고려하여 디자인되었다 [1]. 첫째로는 50% 듀티 사이클을 유지하여 균등하게 조명이 켜지는 것이다. 둘째로는 오류를 감지할 수 있는 기능이 있다는 점이며, 세 번째는 클록 복구가 가능하다는 점이다. Table 2

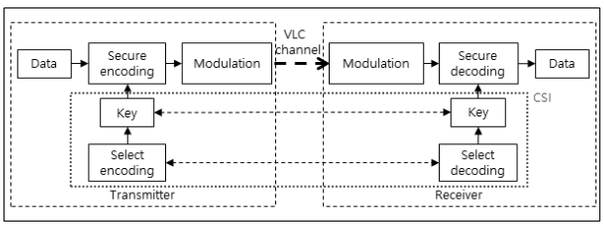
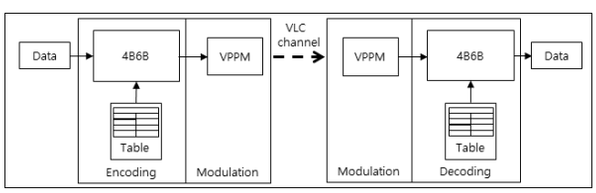
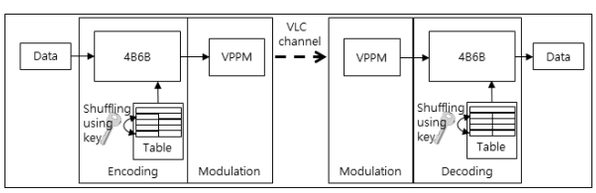


Fig. 4. Proposed Secure Encoding Scheme for VLC



(a) VPPM using 4B6B Table [1]



(b) Secure VPPM using the Proposed Table 3

Fig. 5. Difference between IEEE Standard 802.15.7 VPPM [1] and Proposed VPPM with Encryption

Table 2. Mapping Table from 4B Input to 6B Output [1]

4B(Input)	6B(Output)	Hex
0000	001110	0
0001	001101	1
0010	010011	2
0011	010110	3
0100	010101	4
0101	100011	5
0110	100110	6
0111	100101	7
1000	011001	8
1001	011010	9
1010	011100	A
1011	110001	B
1100	110010	C
1101	101001	D
1110	101010	E
1111	101100	F

를 보면 4B(Input)와 6B(Output)의 연관성은 없으며, IEEE 표준 802.15.7에서 4B6B 표의 생성원리는 기술되어 있지 않았다. 6B를 이용해 표현할 수 있는 수는 26으로 64가지이다. 4B6B의 생성원리인 50% 듀티 사이클을 만족하기 위해서는 6B에서 '0'을 3번 사용하고, '1'을 3번 사용하여야 한다.

Table 3. Proposed Mapping Table from 4B Input to 6B Output

4B(Input)	6B(Output)	Hex
0000	001110	0
0001	001101	1
0010	010011	2
0011	010110	3
0100	010101	4
0101	100011	5
0110	100110	6
0111	100101	7
1000	011001	8
1001	011010	9
1010	011100	A
1011	110001	B
1100	110010	C
1101	101001	D
1110	101010	E
1111	101100	F
-	110100	apparition 1
-	111000	apparition 2
-	001011	apparition 3
-	000111	apparition 4

4B6B 인코딩에서 출력의 경우의 수는'0'과 '1'의 개수에 따라 Equation (1)을 통해 계산할 수 있다.

$$\#of\,output\,combinations = \frac{\#of\,output\,bits!}{[\#of\,output\,bits/2]! \times [\#of\,output\,bits/2]!} = \frac{6!}{3! \times 3!} = 20 \quad (1)$$

6B에서 '0'과 '1'의 개수는 각각 3개이며, '0'과 '1'의 전체의 개수는 6개이다. Equation (1)을 이용하면 출력 6B에서 20가지를 가진다. Table 2를 보면 4B와 6B의 대응되는 가지 수는 16개이다. 이와 비교했을 때, 네 가지가 존재하지 않는다. Table 2에 존재하지 않는 000111, 001011, 111000, 110100 가 추가로 존재한다. 따라서 확장한 Table 3과 같이 디자인하여 복잡도를 올리고자 하였다.

본 논문에서 제안하는 방식은 4B6B 표를 뒤섞어 보안을 제공하는 것이다. 사용한 암호화 방식은 shift cipher [15]와 vigenère cipher [15]이다. 복잡한 암호화는 큰 하드웨어 비용을 야기하며 처리속도 또한 늘어나기 때문에 이를 줄일 수 있는 간단한 암호화 방식을 제안한다. Shift cipher를 적용한 암·복호화 식은 다음과 같다. Equation (2)에서 ek는 key를 사용한 암호화를 나타내며 m은 암호화되기 전 메시지

를 나타낸다. k는 키를 나타내며 Equation (3)에서 dk는 복호화를 나타낸다.

$$e_k(m) = (m+k) \bmod 20 \tag{2}$$

$$d_k[e_k(m)] = [e_k(m) - k] \bmod 20 \tag{3}$$

Shift cipher는 mod 연산이기 때문에 20의 배수를 사용할 수 없어 제약조건이 존재한다. 키가 20의 배수일 때, 연산은 Equation (4)와 같이 암호화되지 않기 때문이다. 데이터 통신을 할 때 키를 0이나 20의 배수를 사용하면 IEEE 표준 802.15.7의 인코딩을 그대로 사용할 수 있다.

$$e_{20n}(m) = (m+20n) \bmod 20 \tag{4}$$
$$= m \bmod 20 + 20n \bmod 20 = m \bmod 20$$

키는 랜덤하고 균등하게 생성되어야 동일한 확률을 제공할 수 있다. 그러나 shift cipher의 경우 키가 '0'을 포함한 20의 배수가 키로 사용될 수 없으므로 균등한 키 분배가 이루어지지 않는다. 이러한 키의 제약조건을 완화하기 위해 vigenère cipher를 제안한다. Vigenère cipher는 shift cipher의 확장형으로 shift cipher보다 복잡도가 높다. Equation (5)와 (6)은 vigenère cipher의 암·복호화 식을 보여준다.

$$e_k(m_1, m_2, \cdots, m_n) = (m_1 + k_1, m_2 + k_2, \cdots, m_n + k_n) \tag{5}$$

$$d_k[e_k(m_1, m_2, \cdots, m_n)] \tag{6}$$
$$= e_{k1}(m_1) - k_1, e_{k2}(m_2) - k_2, \cdots, e_{kn}(m_n) - k_n$$

shift cipher의 경우, 제안하는 VPPM에서 데이터 출력의 가지 수는 20개이기 때문에 기존의 4B6B에 비해 키를 저장하는데 5-bit가 필요하다. 암호화할 때, 하드웨어 비용은 추가되지 않는다. 테이블을 이용하여 암호화할 때, shift right 연산을 수행하고, 복호화할 때, shift left 연산을 수행하기 때문이다. mod 연산의 경우 Fig. 6과 같은 원형 큐(circular queue)로 맵핑 테이블을 관리하기 때문에 추가적인 하드웨어가 필요하지 않다. Vigenère cipher의 경우 키 여러 개를 저장해야 하므로 그에 따른 저장 공간이 필요하다.

4. 보안 인코딩 운용방법 및 평가

무선통신에서는 통신하기 전에 AP(Access Point)와 디바이스가 CSI를 공유한다. 채널 상태가 빠르게 변화하기 때문에 AP와 디바이스가 CSI를 공유해야 한다. CSI는 디바이스나 AP가 채널의 상태를 서로에게 보고하고 그에 맞는 서비스 제공을 목적으로 하고 있다. 가시광 통신 역시 디바이스에서

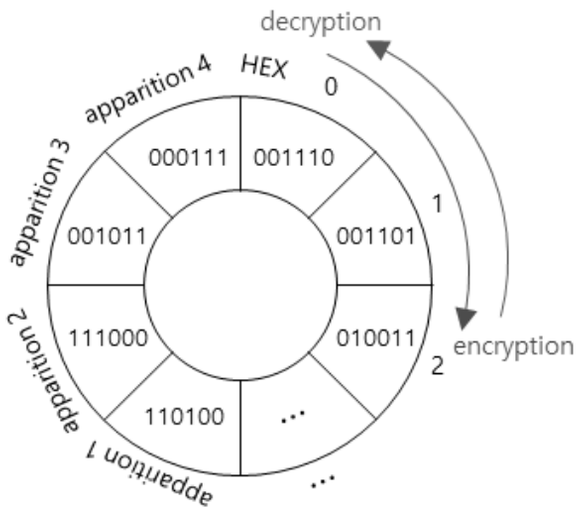


Fig. 6. Circular Queue for Implementing 4B6B Table

데이터를 인식하는 빛의 분해능에 따라 데이터 전송 속도가 달라지기 때문에 조명인 AP에 CSI를 보고해야 한다. CSI를 보고하는 과정에서 키를 함께 전송한다. 키의 전송속도는 모듈레이션의 데이터 전송속도에 따라 정해지며, 키의 전송으로 시간이 소요된다. 그러나 처음 CSI를 교환할 때만 키 전송 시간이 발생하고, 이후에는 통신 속도에 영향을 주지 않는다. Fig. 7과 8은 키의 길이가 늘어남에 따라 CSI에 키를 전송하는데 필요한 시간 그래프이다. Fig. 7은 OOK 방식의 최소와 최대 데이터 전송속도로 키를 보내는 시간을 보여준다. 키 1024 bits를 보낼 때 최대 87.75 ms와 최소 10.24 ms로, 평균 48.99 ms의 시간이 소요된다. Fig. 8은 VPPM에서 키를 전송할 때 소요되는 시간을 보여준다. VPPM의 경우 OOK 방식보다 속도가 빠르므로 키를 전송하는 시간이 짧다. 키 1024 bits를 보낼 때 최대 28.79 ms, 최소 0.02 ms의 시간이 소요되어, 평균 14.40 ms가 필요하다.

2.1의 PHY I의 OOK 방식에서 적용된 보안 인코딩은 사용자가 키를 알고 있기 때문에 2-bit씩 수신해도 데이터를 추출할 수 있다. Fig. 9는 암호화된 데이터를 받았을 때 요구되는 시간과 도청자에게 요구되는 시간을 보여준다. 도청자는 키의 길이만큼 데이터를 수집하는 동시에 키의 값도 추측해야 한다. 따라서 도청자는 Fig. 9처럼 키의 길이만큼 데이터를 수집하는 시간이 필요하다. 키가 4의 배수로 디자인되는 이유는 조명이 꺼지지 않게 하기 위함이다. 데이터 1-bit를 수신하는 시간이 t일 때, 데이터를 복호화하기위해 필요한 데이터의 수집시간은 키가 4의 배수로 디자인되었기 때문에 4t이다. 키의 개수가 n일 때 도청자는 메시지를 복호화하기 위해 최대 $\sum_{k=1}^{n} 2^k$ 만큼 전수조사해야 한다.

제안하는 VPPM에서의 보안 인코딩은 vigenère cipher를 사용한다. Shift cipher에서는 도청자도 복호화 툴을 가지고 있다면 4B6B 맵핑 표로부터 생성 메커니즘을 알 수 있다. 키

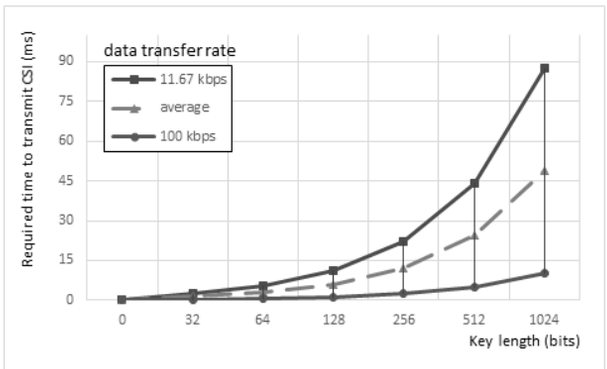


Fig. 7. Required Time to Transmit CSI in OOK

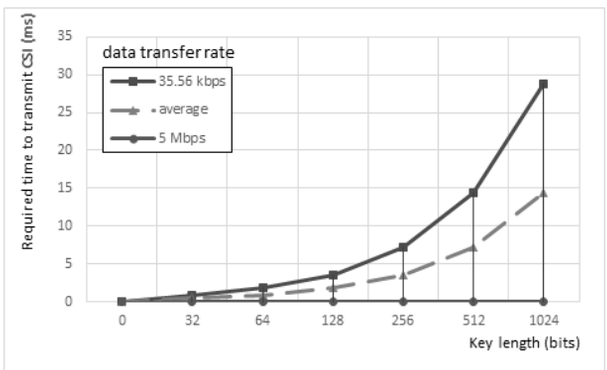


Fig. 8. Required Time to Transmit CSI in VPPM

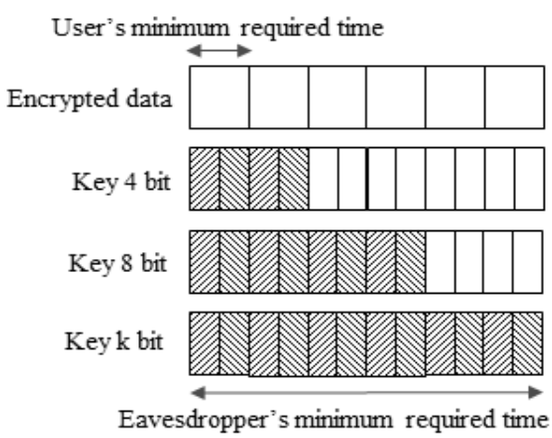


Fig. 9. Eavesdropper's Required Time

값을 모르더라도 미리 20번 shift 하여 만들어 둔 표를 가지고 복호화하면 빠른 해독이 가능하다. 그러나 최초로 표를 만들기 위한 시간이 들 뿐만 아니라, 20개의 표를 저장하기 위한 메모리가 필요하다. 이에 더해 데이터를 식별하기 위해서는 최소한 12 bits를 확인해야 한다. 6 bits가 하나의 문자로 맵핑되기 때문이다. Vigenère cipher는 shift cipher보다 상대적으로 강력한 암호이다. Shift cipher에서는 한 개의 키만 사용했으나, vigenère cipher에서는 여러 개의 키를 사용

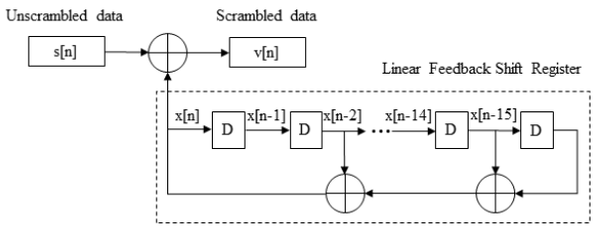


Fig. 10. Scrambler Block Diagram using LFSR

하기 때문에 암호화 강도가 증가한다. Vigenère cipher를 사용할 때, Table 3에서 출력인 6B로부터 데이터인 4B로 맵핑될 확률은 1/20이다. 키의 길이가 늘어날수록 보안 강도는 증가한다. 키의 길이는 무한히 길지 않으므로 일정 구간 이상이 되면 반복된다. 이를 대비하여 카운터모드 [16]와 같은 운용모드가 요구된다. 키를 유추할 수 없도록 키는 충분히 길어야 하며, 키를 매번 바꿔주는 운용모드가 필요하다. 제안된 vigenère cipher의 경우 도청자는 하나의 입력 값을 맞힐 확률 $\frac{1}{20}$에 키의 개수를 알아야 한다. 키가 n개일 때 도청자는 메시지를 복호화하기 위해 최대 $\sum_{k=1}^{n} 20^k$ 만큼 전수조사해야 한다. 6B의 1-bit를 수신할 때 t의 시간이 걸린다면, 6-bit를 수신해야 의미 있는 데이터가 되므로 6t의 시간이 필요하다.

5. 8B10B와 CSK에 대한 고찰

8B10B는 ANSI/INCITS 373에 명시된 라인 코딩이며 유선에서 사용하는 인코딩이다. 8B10B는 3B4B와 5B6B가 합쳐진 인코딩 방식으로 4B6B와 마찬가지로 전력이 균등하게 분포될 수 있는 기능이 내포되어 있다. 따라서 '0'또는 '1'이 최대 6번 이상 연속하여 발생하지 않는다 [17]. 8B10B 역시 입력과 출력의 맵핑 표를 사용하기 때문에 제안하는 암호화 방식을 적용하여 사용 수 있다.

PHY III의 CSK의 경우 IEEE 표준 802.15.7 [1]에서 보안을 제공하는 scrambler가 존재한다. 이 scrambler는 LFSR (Linear Feedback Shift Register)로 Fig. 10과 같이 디자인되어 있다. LFSR은 CSK에만 접목되어 사용되는 것이 아니라 모든 방식에 접목하여 사용 수 있다. 하지만 Fig. 10에서 LFSR과 연산된 값인 scrambled 데이터를 바로 인코딩에 사용할 수는 없다. 8B10B에 LFSR를 사용했을 때 출력은 0000 000000~1111 111111까지 출력되므로 조명이 꺼지는 경우가 발생한다. CSK에 LFSR이 사용했을 때에는 백색광이 아닌 특정한 색으로 표현될 수 있다. LFSR을 사용하기 위해서는 암호화, 복호화를 위해 수신측과 송신측이 동일한 LFSR로 디자인되어야 한다. 이는 두 가지 문제를 야기한다. 첫 번째는 LFSR의 구조를 바꾸지 않는 이상 결과가 동일하기 때문에 암호문과 평문의 쌍을 알게 되면 암호의 기능이 사라

지게 된다. 두 번째는 사용자의 디바이스에서 사용할 수 없다는 점이다. 그 이유는 사용자의 디바이스를 위해, 같은 LFSR를 모든 가시광 통신 시스템에서 동일하게 사용되어야 하기 때문이다. 동일한 LFSR을 도청자도 사용한다면 암호를 쓰는 의미가 없어진다. CSK에서는 사용자가 인지하지 못하는 색의 차이로 통신하기 때문에, 데이터를 보내기 위한 맵핑 표가 존재한다. 따라서 제안한 4B6B의 맵핑 표를 이용한 것과 같이 CSK 맵핑 표를 사용하여 제안하는 보안 인코딩처럼 vigenère cipher를 접목시켜 사용할 수 있다.

6. 결 론

물리계층에 암호화 모듈을 넣는 것은 전송속도와 하드웨어 비용에 영향을 미치므로, 복잡한 모듈을 넣기란 쉽지 않다. 또한, 가시광 통신의 특성 중 조명이 항상 켜져 있어야 한다는 전제 조건은 암호를 사용하는데 부정적인 요인으로 작용한다. 본 논문에서는 기존의 IEEE 표준 802.15.7의 인코딩을 분석하고, 맵핑 표를 사용한 인코딩에서 vigenère cipher로 암호화하는 것을 제안했다. 차세대 통신으로 각광 받는 가시광 통신은 아직 출발 선상에 있다. 이를 상용화하기에 앞서 보안에 관한 연구는 필수적이다.

References

[1] "IEEE Standard for Local and metropolitan area networks--Part 15.7: Short-Range Optical Wireless Communications," in *IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011)*, pp.1-407, 23 Apr. 2019.

[2] J.-Y. Wang, X.-T. Fu, J.-B. Wang, M. Lin, J. Cheng, and M.-S. Alouini, "Secrecy capacity bounds for visible light communications with signal-dependent noise," *arXiv preprint arXiv: 2109.11097*. 2021.

[3] A. Gupta, and X. Fernando, "Exploring secure visible light communication in next-generation (6G) internet-of-things," *2021 International Wireless Communications and Mobile Computing (IWCMC)*," 2021.

[4] T. V. Pham, and A. T. Pham, "Energy-Efficient Friendly Jamming for Physical Layer Security in Visible Light Communication," *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021.

[5] R. Shaaban, and S. Faruque, "An enhanced indoor visible light communication physical-layer security scheme for 5G networks: Survey, security challenges, and channel analysis secrecy performance," *International Journal of Communication Systems*, Vol.34, No.4, pp.e4726, 2021.

[6] N. Su, E. Panayirci, M. Koca, A. Yesilkaya, H. V. Poor, and H. Haas, "Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying," *IEEE Transactions on Communications*, Vol.69, No.4, pp.2585-2598, 2021.

[7] C.-W. Chow, Y. Liu, C.-H. Yeh, Y.-H. Chang, Y.-S. Lin, K.-L. Hsu, X.-L. Liao, and K.-H. Lin, "Display light panel and rolling shutter image sensor based optical camera communication (OCC) using frame-averaging background removal and neural network," *Journal of Lightwave Technology*, Vol.39, No.13, pp.4360-4366, 2021.

[8] J. He, and B. Zhou, "Vehicle positioning scheme based on visible light communication using a CMOS camera," *Optics Express*, Vol.29, No.17, pp.27278-27290, 2021.

[9] Y.-S. Lin, C.-W. Chow, Y. Liu, Y.-H. Chang, K.-H. Lin, Y.-C. Wang, and Y.-Y. Chen, "PAM4 rolling-shutter demodulation using a pixel-per-symbol labeling neural network for optical camera communications," *Optics Express*, Vol.29, No.20, pp.31680-31688, 2021.

[10] P. Wang, J. Liang, and L. V. Wang, "Single-shot ultrafast imaging attaining 70 trillion frames per second," *Nature Communications*, Vol.11, No.1, pp.1-9, 2020.

[11] J. F. Kurose, "Computer networking: A top-down approach featuring the internet," 7/E. Pearson Education India. 2017.

[12] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*, 2015.

[13] M. Guri, B. Zadov, and Y. Elovici, "LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive LED," *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2017.

[14] M. Kim and T. Suh, "A low-cost surveillance and information system for museum using visible light communication," *IEEE Sensors Journal*, Vol.19, No.4, pp.1533-1541, 2018.

[15] D. R. Stinson, "Cryptography: theory and practice," Chapman and Hall/CRC. 2005.

[16] H. Lipmaa, P. Rogaway, and D. Wagner, "CTR-mode encryption," First NIST Workshop on Modes of Operation, 2000.

[17] A. X. Widmer and P. A. Franaszek, "A DC-balanced, partitioned-block, 8B/10B transmission code," *IBM Journal of Research and Development*, Vol.27, No.5, pp.440-451, 1983.

김 민 철

https://orcid.org/0000-0003-0465-4223
e-mail : betamc@korea.ac.kr
2014년 ~ 현 재 고려대학교 정보보호학과 박사과정
관심분야 : 가시광통신, 적외선통신, 마이크로컨트롤러, 통신보안

서 태 원

https://orcid.org/0000-0002-6377-5482
e-mail : suhtw@korea.ac.kr
1993년 고려대학교 전기공학과(학사)
1995년 서울대학교 전자공학과(석사)
1995년 ~ 1998년 LG종합기술원 주임연구원
1998년 ~ 2001년 하이닉스반도체 선임연구원
2006년 Georgia Institute of Technology Computer Engineering (공학박사)
2007년 ~ 2008년 Intel Corporation System Engineer
2008년 ~ 현 재 고려대학교 컴퓨터학과 교수
관심분야 : 컴퓨터구조, 하드웨어 보안, AI accelerator, 블록체인 등