가시광 통신 물리계층 암호화 연구

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

A Study on Physical Layer Security in Visible Light Communication

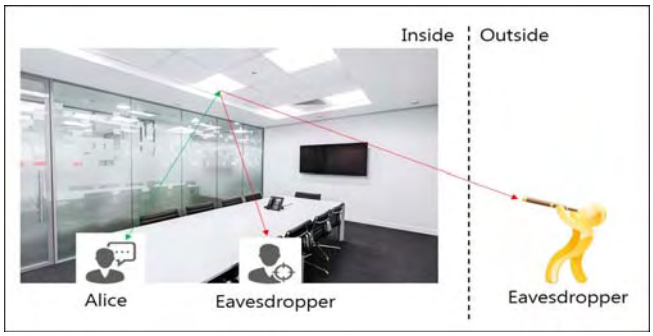
Minchul Kim*, and Taeweon Suh**
*Graduate School of Information Security, Korea University
**Dept of Computer Science and Engineering, Korea University

요 약

가시광 통신 환경 내에서 사용자가 데이터를 받을 때, 공격자가 도청하는 위치는 특정할 수 없다. 공격자는 특정되지 않은 위치에서 다양한 행위를 할 수 있다. 공격자는 조명 그 자체를 관측하여 유의미한 데이터를 얻을 수도 있고, 사용자의 근처에서 사용자와 같은 데이터를 얻을 수도 있다. 이와 같은 도청 행위를 방지하기 위해서 암호화가 필요하다. 본 연구에서는 사용자의 통신에 지장을 주지 않는 물리계층 암호화 방법을 제안한다.

1. 서론

가시광 통신은 조명을 이용하여 통신하기 때문에 조명 아래에 위치한 사용자만 데이터를 수신할 수 있다. 즉, 이 통신 방법은 사방이 투명하지 않은 벽에 막혀있고, 인가 받지 않은 사용자(도청자)가 공간에 침범해서는 안 된다는 전제를 가진다. 보안을 중요하게 생각하는 국가 단위의 연구소나 큰 회사와는 달리, 가정이나 일반적인 회사는 이러한 환경을 조성하기 어렵다. 따라서 가시광 통신을 상용화하기 위해서는 이러한 한계를 극복하기 위한 암호화 방법이 필요하다.



(그림 1) 내부 도청자와 외부 도청자

가시광 통신이 사용될 경우 (그림 1)과 같은 도청이 가능하다. 내부 도청의 경우 사용자의 정보를 손쉽게 도청할 수 있는데, 같은 조명으로부터 받아온 값이 사용자나 도청자가 다르지 않기 때문이다. 외부 도청의 경우 정보를 담고 있는 빛이 외부까지 도달하기는 힘들지만, 조명기구를 초고속 카메라를 이용하여 촬영함으로써 정보를 받을 수 있다.

지금까지 연구된 초고속 카메라의 경우 초당 5조 프레임까지 사진 촬영이 가능하며[1], 시판 중인 고속카메라 Phantom V2512의 경우 최대 초당 100만 프레임을 지원한다[2]. 따라서 이 카메라의 경우 1 MHz 샘플링을 갖는 센서라고 볼 수 있다.

가시광 통신 방법 중 OOK(On-off keying)는 LED의 꺼짐과 켜짐을 이용한 데이터 전송방법이다. 1 Mbps 이하의 전송속도를 사용하는 가시광 통신의 조명을 직접 관찰할 경우 데이터는 고속 카메라를 이용해 수집될 위험을 가지고 있다. 따라서 이를 방어하기 위한 가시광 통신 물리계층 암호화 방법을 제안한다.

2. 관련연구

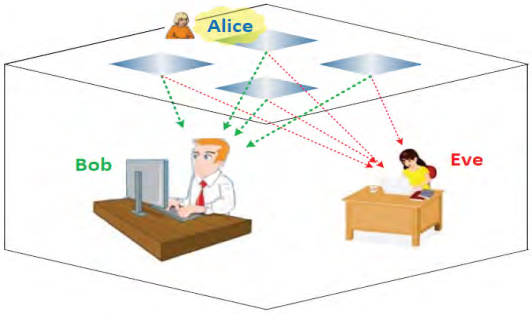
2.1.실내 가시광 통신에서 물리계층 보안

실내 가시광 통신에서의 물리계층 보안 중에서도 다중 안테나를 사용하는 방식이다. (그림 2)와 같이 조명등은 여러 개이며, 도청자가 같은 공간에 위치하더라도 사용자의 SNR(Signal-to-noise ratio)을 높게 설정하고 다른 위치의 도청자의 SNR을 낮게

본 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 기본연구지원사업 지원을 받아 수행되었음(NRF-2017R1D1A1B03028926)

설정하는 방식이다[3].

그러나 이 연구의 경우 조명에서 나오는 빛을 바탕으로만 SNR을 측정한다. 그러므로 조명 자체를 관측하여 도청하거나 정상 사용자 근처에서 데이터를 도청할 경우에는 취약함을 보인다.



(그림 2) 다중 안테나를 통한 물리적 보안

2.2.가시광 통신을 이용한 군용 차량 보안통신

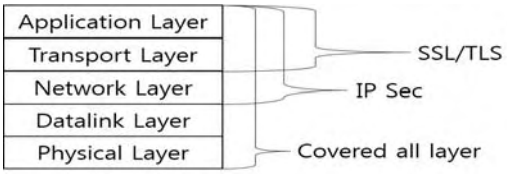
군 통신을 위해 민간인이나 악성 침입자가 도청을 하거나 통신에 방해를 하게 해서는 안 된다. 이를 방지하기 위해서 군용 통신의 신뢰성 있는 키 전송을 통해 군용 통신망을 구축했다. 신뢰성 있는 키 전송 방식으로 가시광 통신을 사용했으며, 암호화 방식은 AES이다[4].

(그림 3) 가시광 통신을 이용한 군용 보안 통신

이 논문에서 사용한 가시광 통신은 신뢰관계를 유지하기 위해, 멀티미디어 데이터와 같은 정보를 담은 데이터가 아니라 비밀키를 보낼 때만 사용하고 있다. 키 교환으로 이 방식을 사용하는 이유는 빛의 직진성 때문이며, 앞차와 뒤따르는 차량의 관계를 시각적으로 분별할 수 있기 때문에 안전한 키를 제공받을 수 있다.

3. 물리계층 보안 동작원리

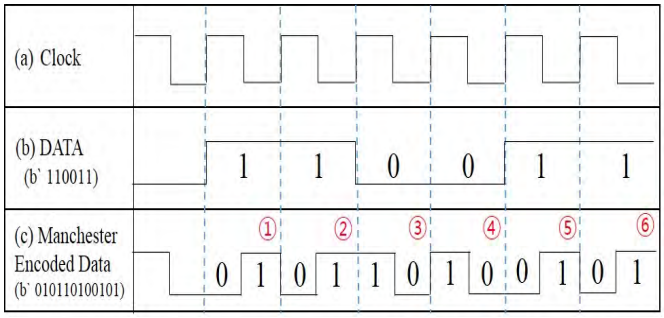
물리계층 보안은 상위 계층을 전부 방어할 수 있으며, 계층이 나눠져 있기 때문에 독립적으로 사용가능하여 상위 계층의 보안과도 함께 사용할 수 있다. 물리 계층에서는 회선을 어떻게 공유할지, 데이터의 전송을 단방향 혹은 양방향으로 보낼지, 데이터를 교대로 보낼지를 정해야 한다. 또한 어떤 네트워크 장치들이 상호 작용하는지에 대한 토폴로지를 설계해야 한다. 어떤 신호를 사용할 것인지, 인코딩은 어떻게 할 것인지, 두 장치 간에 정보를 공유하는 효과적인 방법은 무엇인지까지 고려해야한다. 단순해 보이는 물리계층이지만 많은 부분을 고려하여 디자인해야 한다.



(그림 4) 계층별 암호화되는 영역과 방식

이 중 인코딩은 데이터를 어떻게 신호로 표현할 것인지를 담당하는 부분이다. 가시광 통신의 기본적인 메커니즘은 LED의 깜빡임으로 비트를 구분하는 것이다. LED의 켜짐과 꺼짐의 표현인 '0'과 '1'을 나타내는 비트를 사용한 디지털 통신방법이라 볼 수 있다. 가시광 통신에서의 인코딩은 빛이 꺼지지 않게 디자인해야 하므로, 일정 간격 동안 지속적으로 꺼지는 상황을 피하기 위해 OOK나 VPPM(Variable Pulse Position Modulation)을 이용한다[5]. 이러한 인코딩 과정에 키를 더해, 조명의 기능을 하면서도 데이터 암호화도 가능케 하는 방식을 제안한다.

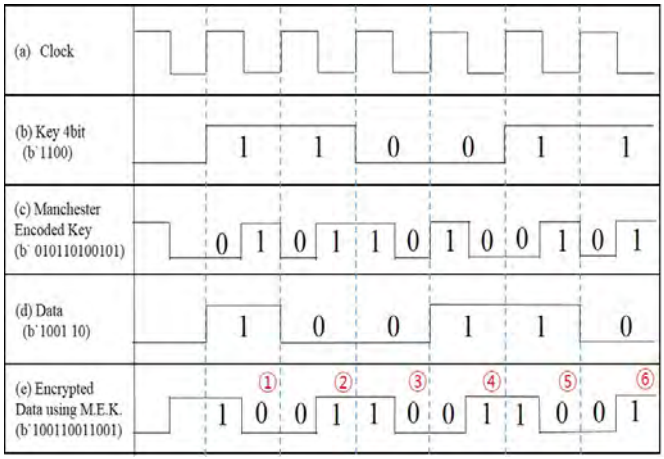
가시광 통신에서 사용하는 OOK(On-off keying) 방식을 살펴보면 (그림 5)와 같다.



(그림 5) 멘체스터코딩을 이용한 OOK방식

OOK 방식은 멘체스터코딩을 이용한 방식으로 클럭과 데이터를 XOR하여 보내는 신호를 생성한다. (그림 5)의 ①과 ②를 보면 데이터가 '1'값일 때 '01'값을 가지며, ③과 ④를 보면 데이터가 '0'값일 때 '10'값을 가진다. 따라서 데이터가 '1'값일 때와 '0'값일 때 값이 고정적이다. 하지만 키를 인가했을 때, (그림 6)의 ①과 ④번의 경우 데이터는 똑같은 '1'이지만 결과 값은 '10'과 '01'로 다르다. 이는 서로

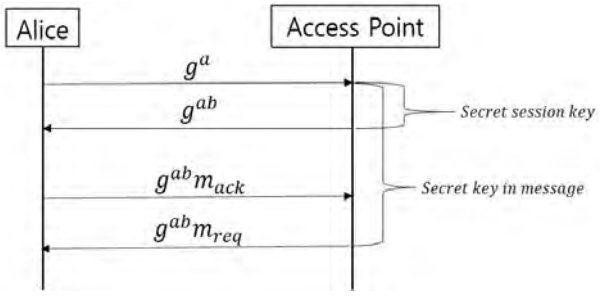
다른 표현형으로 나타나므로 비트의 표현형에 있어 '0'과 '1'을 결정지을 데이터의 확률은 동전을 던졌을 때의 확률과 같다.



(그림 6) 암호화된 OOK 방식

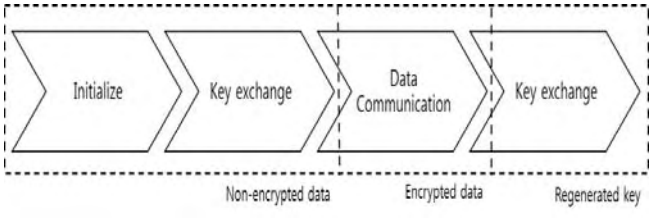
데이터 통신을 하기 위해 사용자와 조명과의 세션을 맺는 과정을 우선적으로 수행한다. 이 과정에서 사용자와 기지국인 조명 사이에 공유하는 비밀키를 설정하여 데이터를 주고받을 때 사용한다. 비밀키는 상위 단계에서 만들거나 직접 키를 지정하는 두 가지 방식으로 만들 수 있다. 키를 생성하는 메커니즘으로, (그림 7)과 같이 디피-헬만 키 교환 알고리즘을 사용한다.

세션키를 생성하는 과정은 물리계층에서 만들어지는 것이 아니라, 상위 단계인 전송계층(transport layer)에서 사용하는 키 교환 방식으로 만들어진다. 여기서 생성된 키를 물리계층에서 직접 사용하는 방법과 메시지에 물리계층에서 사용할 비밀키를 넣어 사용하는 방법이 있다.



(그림 7) 키 교환 메커니즘

이 두 가지 키 교환 방식은 각각 장단점이 존재한다. 세션키를 이용했을 때 키의 제약조건이 발생한다. 키의 제약조건은 소수여야 하며, 안전성을 위해서는 10진수로 백에서 천 자리의 큰 소수여야 한다. 많은 양의 데이터를 한 번에 연산할 때는 이와 같은 키를 사용하는 것이 안전하지만, 실시간으로 영상을 처리할 수 있는 스트리밍 서비스를 지원하기 위해서는 처리할 데이터의 사이즈가 작아야 한다. 이처럼 사이즈가 작은 키를 교환할 때는 메시지에 물리계층용 키를 새로 생성하여 넣는 것이 낫다. 메시지에 키를 넣어서 사용하는 경우에도 키의 크기에 제한 조건이 없으므로 키를 생성할 때 편리하다.



(그림 8) OTP(One Time Password) 적용

데이터는 외부에서 들어오는 것으로 인터넷에서 들어오는 값이나 설계자가 임의로 보내는 정보 값이다. 키의 값은 기지국인 조명과 사용자가 서로 주고받아 생성한 키이다. 따라서 외부로부터 생성하지 않고 서로간의 협약을 통해 만들어진다. 조명과 사용자가 세션을 맺는 과정에 키를 이용한 통신을 하며 일정 시간이 지난 후, 키의 값을 다시 배정받는 과정을 수행한다. (그림 8)과 같이 이렇게 키를 다시 배정 받는 이유는 두 가지로 첫 번째는 OTP(One Time Password)처럼 사용하기 위해서이다. OTP는 시간에 따라 다른 암호화된 키를 가지기 때문에 암호화를 더욱 강력하게 해준다. 인코딩에 사용한 키의 길이는 매우 짧다. 따라서 계속 사용하면 키가 노출될 위험이 있다. 이를 방지하기 위해 주기적으로 키를 바꿀 경우 도청자는 이전의 키를 가지고 현재의 데이터를 복호화 하면 다른 값을 갖기 때문에 기존에 키를 복호화해도 현재 통신하는 키가 아니면 불필요하다.

두 번째 이유는 사용자는 유동적이기 때문이다. 사용자가 다른 기지국 조명에서도 사용을 할 수 있어야 한다. 디바이스와 기지국인 조명사이에서 세션이 유지되는 시간이 존재한다. 다른 기지국 조명으로 갔을 때 똑같은 비밀키를 사용할 수 있겠지만 이미 그 키를 받은 사용자가 존재한다면 기존의 비밀키를 사용하는 것은 위험하다.

4.도청자와 보안의 상관관계

보안 수준이 높을수록 도청은 어려워진다. 도청자가 암호를 뚫는 비용과 사용자가 필요한 비용의 차이를 계산하여 보안 수준을 알아볼 수 있다.

$$Cost_{alice} = m\,bits\,data \times n\,bits\,key$$
$$= (known\,data\,size) \times (known\,key's\,probabilty) \quad (1)$$
$$= m \times 1$$

식 (1)은 사용자가 데이터를 알아보기 위해 들어가는 비용으로, 사용자가 이미 키를 가지고 있어 처리 시간이 들지 않는다. 키의 길이가 늘어나는 경우 메시지의 길이도 함께 늘어나기 때문에 데이터를 받는 사용자는 m 만큼의 시간을 기다려야한다.

$$Cost_{eve} = Guessing\,data\,size \times Guessing\,key\,value$$
$$= Guessing\,key \quad (2)$$
$$= \sum_{k=0}^{n} 2^k = 2^{k+1} + 1$$

식 (2)는 도청자가 사용자의 데이터를 알아내기 위해 발생하는 비용이다. 데이터의 길이와 키의 값을 알아내야 데이터 값을 도청할 수 있다. 데이터 길이는 키의 길이에 비례하기 때문에 궁극적인 공격 방식은 키를 찾는 것이다. 이 도청자이자 공격자가 키의 길이와 키의 값을 찾는 전수조사 과정은 키를 사용하지 않는 평문을 보내는 0의 길이부터 시작한다. 인코딩에 들어간 키이므로 0과 1의 두 가지 경우의 수인 2이며, 키의 길이만큼을 연산하는 k제곱을 하여 키의 값을 찾아낸다.

$$Security\,Capacity = Cost_{eve} - Cost_{alice}$$
$$= 2^{k+1} + 1 - m - 1 \quad (3)$$
$$= 2^{k+1} - k > 0$$

식 (1)과 식 (2)로부터, 식 (3)은 전체 보안정도를 나타내는 식이다. 도청자가 암호를 뚫는 비용과 사용자가 필요한 비용의 차로 보안정도를 알 수 있다. 키의 길이로 메시지의 길이를 반복적으로 암호화하기 때문에, 메시지의 길이는 키의 길이와 같다. 즉, 메시지 길이 m은 k와 같은 값을 가진다. 또한 데이터를 암호화 하지 않았을 때 도청자는 바로 알아 볼 수 있기 때문에 초기 값인 1을 빼주어야 한다.

이를 빅 오 계산으로 보면 사용자 입장에서는 데이터의 사이즈가 키의 길이와 같다는 것과 키가 k라는 것을 알기 때문에 Θ(k)이며, 도청자가 알아내기 위한 빅 오 연산은 $O(2^{k+1})$ 이다. k는 키의 길이로 메시지와 키를 이용하여 복잡도를 제공하기 때문에 키의 값에 따라 보안 정도가 결정된다. 키의 길이가 늘어나면 보안에는 좋지만, 사용자의 입장에서는 받아야할 메시지 길이가 길어져야 되기 때문에 적절한 길이의 키를 사용하는 것이 좋다.

이 방식은 고정키일 때 해당하는 값이며, OTP로 사용됐을 때는 키와 데이터의 길이를 시간에 따라 다시 추측해야하므로 짧은 키를 사용하더라도 도청자에게는 많은 시간이 소요된다.

5.결론

가시광 통신 물리계층 보안에 대한 연구는 빛의 매개체를 전파와 같은 성격으로 취급하고, 사용자와 도청자를 같은 측면에서 위치에 대한 안전성 연구가 많았다. 하지만 사용자와 같은 환경에서만 도청이 이루어지는 것은 아니다. 실제 사용하는 환경도 고려해야 하며, 시스템의 작동메커니즘을 완벽하게 알고 보안을 설계해야 한다.

IoT 디바이스가 급증함에 따라 라디오 주파수가 부족한 환경이 올 것이다. 현재 유무선 공유기를 사용해 다수의 기기들을 수용하는 것처럼 보이지만, 사람이 밀집한 지역에서는 와이파이 수신이 불안정하거나 통화가 잘 되지 않는 경우가 발생한다. 이는 라디오 주파수에 가용 채널수가 정해져 있기 때문이다. 와이파이의 경우 2.4GHz 대역에서 사용할 수 있는 채널수는 13개이며, 추가로 개방한 5GHz 대역도 대략 9개의 채널수를 가진다. 이러한 라디오 주파수를 대신할만한 통신망 기술이 필요하다.

또한 IoT는 가볍게 디자인되었기 때문에 보안이 힘들다. 따라서 통신망에서 보안을 고려하여 설계할 필요가 있다.

참고문헌

[1] Zhang, M. (2017). This World's Fastest Camera Shoots 5 Trillion Frames Per Second. [online] PetaPixel. Available at: https://petapixel.com/2017/05/01/worlds-fastest-camera-shoots-5-trillion-frames-per-second/.

[2] Phantomhighspeed.com. Phantom v2512 | World's Fastest Digital Ultrahigh-Speed Camera. [online] Available at: https://www.phantomhighspeed.com/products/ultrahigh-speed-cameras/v2512.

[3] Mostafa, A.(2014). Physical-layer security for indoor visible light communications. In Communications (ICC), 2014 IEEE International Conference on (pp. 3342-3347). IEEE.

[4] Ucar, S.(2016). SecVLC: Secure Visible Light Communication for Military Vehicular Networks. In Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access (pp. 123-129). ACM

[5] Rajagopal, S.(2012). IEEE 802.15. 7 visible light communication: modulation schemes and dimming support. IEEE Communications Magazine, 50(3).