다색 강도 조정 기반 광학신호 에어갭 공격

손우영, 권순홍*, 이종혁*

세종대학교 프로토콜공학연구실,

*세종대학교 정보보호학과 & 지능형드론 융합전공

wooyoung@pel.sejong.ac.kr, *soonhong@pel.sejong.ac.kr, *jonghyouk@sejong.ac.kr

Multicolor Intensity Modulation-Based Optical Signal Air-Gap attack

Wooyoung Son, Soonhong Kwon*, Jong-Hyouk Lee*

Protocol Engineering Lab., Sejong University,

*Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University

요 약

대부분의 국가핵심기반시설은 외부의 공격으로부터 시스템을 보호하기 위하여 에어갭 기술을 적용하여 내부망과 외부망이 분리된 형태로 존재하지만, 이러한 환경을 넘어 다양한 중간매체를 통해 내부망의 데이터를 탈취할 수 있음을 보이는 연구들이 지속적으로 수행되고 있는 실정이다. 이에 본 논문에서는 다색 강도의 조정을 통해 생성된 광학신호를 기반으로 내부망의 데이터를 외부망으로 전송함으로써 향상된 데이터 전송 속도를 달성함과 동시에 주변 환경 내 광원의 영향을 최소화하여 안정적인 데이터 전송을 수행할 수 있는 광학신호 에어갭 공격을 제안한다.

Ⅰ. 서 론

최근, 대부분의 국가핵심기반시설은 외부의 공격으로부터 시스템을 보호하기 위하여 내부망과 외부망을 분리한 에어갭 환경을 채택하지만, 이러한 환경에서도 내부망의 데이터를 외부망으로 탈취할 수 있다는 것을 보이는 에어갭 공격에 대한 연구/개발이 지속적으로 수행되고 있다.

광학신호, 전자기파, 음향신호 등과 같이 다양한 중간매체를 활용한 에어갭 기술이 제시되고 있으며, 그 중에서도 광학신호의 경우, 먼 거리까지 빠르게 도달할 수 있다는 특성으로 인해 탈취 데이터의 빠른 전송과 장거리 공격이 수행되어야 하는 에어갭 공격에서 주요한 요소로 활용되고 있다.

이에 따라 본 논문에서는 사용자가 스마트 전구의 색상 강도를 세밀하게 조정할 수 있다는 특성을 이용하여 RGB(Red, Green, Blue) 색상의 강도를 조정함으로써 공격을 수행하는 광학신호 에어갭 공격을 제안한다. 제안된 공격의 경우, 다색 강도를 조정함에 따라 다중 비트 데이터를 동시에 전송함으로써 빠른 데이터 전송을 수행하며, 기준이 되는 색상을 활용하여 수신된 광학신호를 구성하는 각 색상의 강도를 보정함으로써 주변 광원의 영향을 최소화한다는 장점을 지닌다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 연구/개발된 광학신호 기반 에어갭 공격에 대하여 활용된 인코딩 방식을 중점적으로 분석한다. 3장에서는 제안하는 다색 강도 광학 신호를 통한 에어갭 공격에 대하여 주요 프레임워크를 기반으로 설명하며, 4장에서는 본 논문의 결론을 맺는다.

Ⅱ. 광학신호 기반 에어갭 공격

광학신호 기반 에어갭 공격의 경우, 키보드의 Caps Lock, PC의 HDD LED(Light Emitting Diode), 모니터 등과 같이 광학신호를 발생할 수 있는 에어갭 송신기, 카메라, 빛 센서와 같이 해당 신호를 인식할 수 있는 에어갭 수신기로 구성되어 있다. 내부망에 위치한 PC 내 민감 데이터를 획득하고, 이를 비트열로 변환한 후, 비트열에 해당하는 광학신호를 에어갭 송신기를 기반으로 생성 및 방출함으로써 민감 데이터를 송신한다. 비트열에 해당하는 광학신호를 생성하기 위한 인코딩 방식으로는 깜빡임 제어, 밝기 변화, 색상 변화가 주로 사용된다. 먼저, 깜빡임 제어란, 광학신호를 방출하는 광원의 ON/OFF 여부에 따라 비트 0, 1을 표현하는 방식을 말한다. 즉, 비트 0을 인코딩하기 위해서는 특정 시간 동안 광원을 OFF 상태로 유지하여 광학신호가 발생하지 않도록 하며, 비트 1을 인코딩하기 위해서는 광원을 ON 상태로 유지하여 광학신호가 발생하도록 한다. 밝기 및 색상 변화의 경우, 비트 0과 1에 대하여 공격자가 사전에 설정한 밝기/색상의 값으로 변경함으로써 민감 데이터 비트열에 대응되는 광학신호를 생성 및 방출하는 인코딩 방식을 말한다.

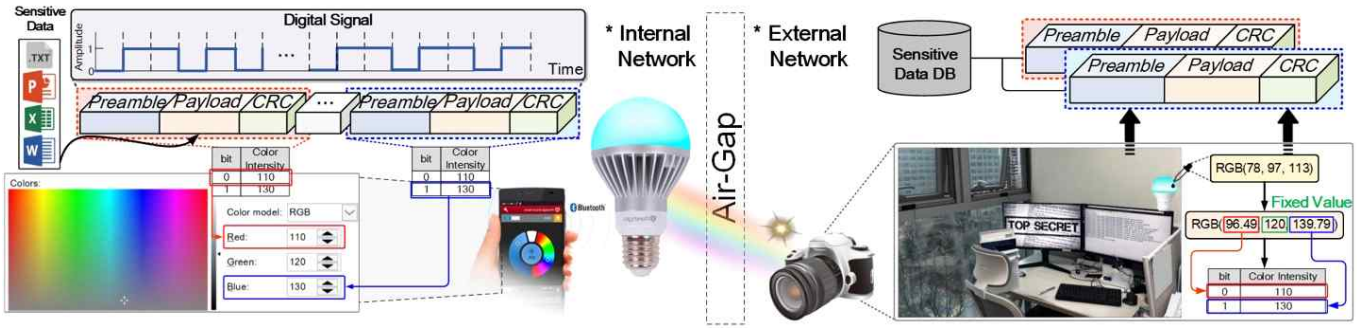
깜빡임 제어 방식은 가장 기본적인 광학신호 인코딩 방법으로 평가된다. 이 방식의 경우, 에어갭 수신기에서 광학신호에 해당하는 비트를 명확하게 판단할 수 있다는 장점이 있지만, 데이터 전송을 위해 LED 등의 광원을 명확하게 깜빡이게 함으로써 동작하기 때문에 눈에 띄는 깜빡임은 비교적 쉽게 감지될 가능성이 존재하여 에어갭 공격에서 중요한 스텔스 기능을 만족시키기 못한다는 한계점이 존재한다.

〔표 1〕 선행연구된 광학신호 기반 에어갭 공격 기술 비교

공격 기술	송수신 장비	인코딩 방식	심볼당 비트 수
J. Lee, et al. [1]	Smart Bulb / Camera	밝기 변화	1 bit
ETHERLED [2]	Network Interface Controller / Camera	깜빡임 제어 / 색상 변화	1 bit
BRIGHTNESS [3]	Monitor Display / Camera	밝기 변화	1 bit
xLED [4]	Swich, Router Status LED / Camera, Light Sensor	깜빡임 제어	1 bit

밝기 변화 방식의 경우, 예를 들어 밝기 수준이 80lm인 경우 비트 0, 240lm인 경우 비트 1을 나타내는 방식으로, 이는 광원의 주변에 있는 사람이 이를 인지하기 어려움에 따라 깜빡임 제어 방식에 비하여 스텔스 기능을 만족한다는 장점이 존재한다. 하지만, 에어갭 수신기에서도 해당 방식으로 인코딩된 광학신호에 해당하는 비트열을 판단하는 데에 어려움에 있으며, 에어갭 송신기가 위치한 환경의 명암에 큰 영향을 받는다는 한계점이 존재한다.

마지막으로, 색상 변화의 경우, RGB 색상 강도의 조합에 따라 변경되며,



(그림 1) 다색 강도 조정 기법을 활용한 광학신호 에어갭 공격 프레임워크

이러한 변화는 사람이 쉽게 인지하지 못함에 따라 스텔스 기능을 만족한다는 장점이 있다. 하지만, 이 또한 송신기 주변 환경 명암의 영향을 받는다는 한계점이 존재한다.

[표 1]의 경우, 선행 연구된 광학신호 기반 에어갭 공격에 대하여 하나의 송신기와 하나의 수신기로 구성된 상황임을 가정할 때의 송수신 장비, 인코딩 방식, 심볼당 비트 수에 초점을 맞추어 분석한 것이다. 심볼당 비트 수의 경우, 하나의 광학신호에 전달될 수 있는 비트 수를 말한다.

Ⅲ. 다색 강도 조정 기반 광학신호 에어갭 공격

본 장에서는 주변 환경의 명암에 영향을 받는다는 기존 색상 변화의 인코딩 방식을 활용한 광학신호 에어갭 공격의 한계점을 해결하고 데이터 전송 속도를 향상시킨 다색 강도 조정 기반 광학신호 에어갭 공격을 제안하며, 이에 대한 주요 흐름은 (그림 1)과 같다.

제안된 광학신호 에어갭 공격의 송신기는 별도의 컨트롤러를 사용하여 원하는 색상 강도를 세밀하게 조정할 수 있다는 특징을 가진 스마트 전구로 가정한다 [1]. 제안된 광학신호 에어갭 공격의 송신기는 내부망 PC로부터 획득한 민감 데이터를 비트열로 변환한 뒤, 이를 기반으로 에어갭 수신기에서 수신한 광학신호에 대한 동기화 및 오류 정정을 수행할 수 있도록 프리앰블, CRC(Cyclic Redundancy Check)를 추가한 패킷 단위로 생성한다. 이러한 과정을 통해 최종 생성된 비트열에 대응하여 색상 변화 인코딩 방식을 기반으로 광학신호가 생성된다. 색상 변화 방식의 경우, RGB의 색상 강도 조합에 따라 변화되며, 이는 세 가지 색상의 강도를 개별적으로 조정할 수 있다는 것을 의미한다. 이에 따라, 제안된 공격의 경우, R 색상의 강도만을 조정하여 심볼당 1 bit만을 전송한 BRIGHTNESS [3]와 달리, R, B, 두 가지 색상의 강도를 조정하여 인코딩함으로써 동시에 2 bits를 송신하고자 한다.

색상 강도가 조정되는 대상이 R, B인 이유는 R, G, B의 색상 중 두 색상이 가시광선 스펙트럼에서 가장 멀리 떨어져 있음에 따라 서로 간섭이 최소화되는 주파수 대역을 활용하기 때문이다. 최종적으로 전송하고자 하는 비트열을 두 개로 분할한 후, 첫번째 부분의 비트열에 대해서는 R 색상 강도를, 두 번째 부분의 비트열에 대해서는 B 색상 강도를 조정함으로써 광학신호를 생성하며, G 색상 강도의 경우, 고정된 특정 값을 갖는다. 이때, 비트 1에 대하여 광학신호로 인코딩을 수행하기 위해서는 높은 색상 강도로, 비트 0에 대해서는 낮은 색상 강도로 설정하며, 설정된 두 가지 색상 강도의 경우, 공격자가 사전에 결정한 값임에 따라 이 정보는 에어갭 송신기와 수신기 모두에게 알려져 있는 상태이다. 색상 강도를 통해 결정된 특정 색상을 갖는 광학신호는 특정 시간동안 발생됨으로써 내부망의 데이터를 외부망으로 전송한다.

광학신호 수신기의 경우, 내부망에서 발생하는 광학신호를 인식하고, 이에 대해 캡쳐를 수행한다. 이후, 캡쳐된 화면 내 광학신호 색상을 기반으로 RGB 각각의 색상 강도를 추출한다. 이후, 추출된 세가지 색상의 강도에 대하여 특정 고정 값의 색상 강도를 갖는 G를 기준으로 R과 B의 색상 강도를 조정하는 과정을 수행한다.

보정된 R, B 색상 강도를 기반으로 광학신호를 비트 문자열로 변환하며, 이때, 색상 강도의 값이 사전에 설정된 두가지 색상 강도 중 높은 값에 가까운 경우 비트 1, 그렇지 않은 경우 0으로 판단한다.

앞서 언급한 과정을 통해 수신기는 광학신호에 해당하는 민감 데이터 비트열을 도출할 수 있으며, 이를 패킷 단위로 분할한 후, ASCII 문자로 변환한다. 이러한 과정을 통해 수신된 민감 데이터가 출력되어 내부 네트워크 PC로부터 전송된 민감 데이터를 확인할 수 있다.

제안된 다색 강도 조정을 활용한 광학신호 에어갭 공격의 경우, 색상 변화의 인코딩 방식을 활용하여 생성된 광학신호를 기반으로 내부망의 데이터를 외부망으로 전송함에 따라 스텔스 기능을 가진다는 장점이 존재한다. 또한, R, G, B의 세 가지 색상 중 서로의 신호에 대한 간섭이 최소화될 수 있는 두 가지 색상의 강도를 동시에 조정함으로써 다중 데이터 스트림을 동시에 전송할 수 있게 함으로써 데이터 전송 속도를 높인다. 변화되지 않는 G의 색상 강도의 경우, 이를 기반으로 수신된 광학신호 내 R, B 색상 강도를 조정하도록 한다. 이를 통해, 에어갭 송신기가 존재하는 환경 내 광원으로 인하여 수신된 광학신호에 대한 정확한 분석이 어렵다는 기존 광학신호 에어갭 공격의 한계점을 해결하고, 다양한 환경에서도 광학신호를 기반으로 안정적인 데이터 전송을 가능하게 함으로써 높은 정확도의 공격의 수행될 수 있다는 장점을 지닌다.

Ⅳ. 결론

선행 연구된 광학신호 기반 에어갭 공격의 경우, 주변 환경의 명암에 큰 영향을 받는다는 한계점이 존재하는 실정이다. 이에 본 논문에서는 다색 강도 조정 기반 광학신호 에어갭 공격을 제안한다. 해당 공격의 경우, 두 가지 색상 강도를 조정하여 다중 데이터 스트림을 동시에 전송할 수 있게 함으로써 데이터 전송 속도를 높이고, 고정된 특정 색상 강도를 기반으로 수신된 광학신호 내 인코딩 시 변화된 색상 강도를 조정하는 과정을 수행함으로써 에어갭 송신기의 주변 광원에 대한 영향을 최소화한다. 향후 연구에서는 본 논문에서 제안한 광학신호 에어갭 공격에 대하여 Artificial Intelligence 및 Machine Learning 기술을 적용함으로써 실시간으로 높은 정확도의 색상 변화를 감지하고 해석할 수 있는 공격을 구현하고자 한다.

ACKNOWLEDGMENT

본 연구는 2023년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(2단계)(UD230020TD)의 지원을 받아 수행되었습니다.

참 고 문 헌

[1] J. Lee, et al., “Optical Air-Gap Attacks: Analysis and IoT Threat Implications,” *IEEE Network,* 2024.

[2] M. Guri, “ETHERLED: sending covert Morse signals from air-gapped devices via network card (NIC) LEDs,” in Proc. *IEEE Int. Conf. on Cyber Security and Resilience (CSR),* pp. 163-170, 2022.

[3] M. Guri, et al., “Brightness: Leaking sensitive data from air-gapped workstations via screen brightness,” in Proc. *12th CMI Conf. on Cybersecurity and Privacy (CMI),* pp. 1-6, 2019.

[4] M. Guri, et al., “xled: Covert data exfiltration from air-gapped networks via switch and router leds,” in Proc. *16th Annual Conf. on Privacy, Security and Trust (PST),* pp. 1-12, 2018.