스마트폰 무음 소리 재생을 이용한 전자파 신호 은닉 채널 형성 방안

김용재*, 안현준**, 한동국***

*,**,***국민대학교 (학부생, 대학원생, 교수)

Construction of Electromagnetic Signal Covert Channel using Silent Sound Play on Smart Phone

Yong-Jae Kim*, Hyeon-Jun An**, Dong-Guk Han***

*,**,***Kookmin University(Undergraduate student, Graduate student, Professor)

요 약

은닉 채널은 특정 송신자와 수신자만 알고 있는 통신 기법을 통해 제삼자가 모르게 데이터를 은밀하게 통신하는 채널로써 스마트폰을 해킹해 사용자의 비밀 정보를 유출하는 등 다양하게 악용될 수 있다. 따라서 다양한 매체에서 형성될 수 있는 은닉 채널을 고려하고, 일상생활 속 많이 사용되는 스마트폰으로 형성될 수 있는 은닉 채널을 연구하여 사전에 대응할 필요가 있다. 본 논문에서는 2022년에 제안된 볼륨 0일 때 소리 재생을 이용한 은닉 채널이 최신 삼성 스마트폰 3종에서 적용할 수 없음을 보이고, 스마트폰 무음 소리 재생을 이용한 새로운 은닉 채널 형성 방안을 제안한다. 최신 삼성 스마트폰 3종을 대상으로 무음 소리 재생 시 스피커 부분에서 발생하는 0.1MHz~2.5MHz 전자파 신호에 대해서 분석하고, 전자파 신호의 특징을 고려하여 설계한 은닉 채널 형성 방안으로 데이터를 송/수신한 결과를 제시한다.

I. 서론

은닉 채널(Covert Channel)은 특정 송신자와 수신자만이 사전에 공유한 방법으로 데이터를 제삼자가 모르게 주고받을 수 있는 통신 채널이다. 스마트폰, 컴퓨터 등에 대한 접근 권한을 탈취한 공격자가 은닉 채널을 형성하여 사용자의 정보를 도청하거나 유출하는 등 악용할 수 있다. 은닉 채널은 5G, WIFI, 소리, 빛, 열, 전자파 등 다양한 매체를 이용하여 형성될 수 있고, 이러한 은닉 채널의 위험성을 경고하고 선제적으로 대응하기 위해 은닉 채널의 연구가 활발히 진행되고 있다.

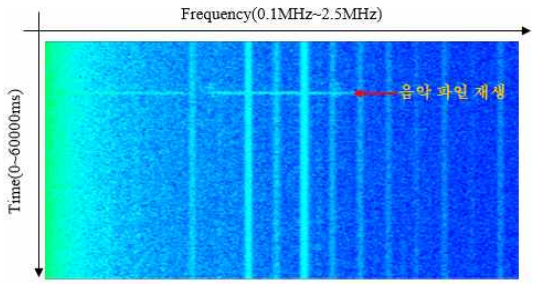
2022년, 스마트폰에서 볼륨이 0일 때 소리 재생을 이용한 은닉 채널[1]이 연구되었다. 하지만 최신 삼성 스마트폰 3종에서는 해당 은닉 채널 기법을 적용해도 은닉 채널을 형성할 수 없었다. 따라서 최신 스마트폰에서도 가능한 새로운 은닉 채널 형성 방안을 연구할 필요가 있다. 본 논문의 2절에서는 기존에 제안된 스마트폰에서 볼륨이 0일 때 소리 재생을 이용한 은닉 채널 형성 방안을 연구하고, 해당 방안을 최신 삼성 스마트폰에서 적용할 수 없음을 보인다. 3절에서는 새로운 은닉 채널 형성 방안 연구를 위해 최신 삼성 스마트폰 3종에서 무음 소리 재생 시 스피커 부분에서 발생하는 전자파 신호를 분석한다. 4절에서는 무음 소리 재생 시 발생하는 전자파 신호를 이용하여 은닉 채널을 형성하는 새로운 방안을 제안하고 은닉 채널을 형성하여 데이터를 송/수신한 결과를 제시한다.

[Contribution] 최신 삼성 스마트폰 3종에서 무음 소리 재생 시 스피커 부분에서 발생하는 전자파 신호를 분석하였다. 전자파 신호의 특징을 고려하여 설계한 무음 소리 재생을 이용한 새로운 은닉 채널 형성 방안을 제안하였다. 해당 은닉 채널을 통해 데이터를 송/수신한 결과를 제시하였다.

II. 관련 연구

2.1 스마트폰 볼륨이 0일 때 소리 재생 시 발생하는 전자파를 이용한 은닉 채널

2022년, 안성현 등은 스마트폰에서 볼륨이 0일 때 소리 재생 시 스피커 부분에서 발생하는 전자파를 이용한 은닉 채널[1]을 형성하였다. 대상 스마트폰인 Galaxy Note8는 소리가 재생되는 동안 1.65MHz에서 지속적인 전자파가 발생하였고, 소리가 꺼졌을 때는 3300ms가 지나고 해당 전자파가 사라졌다. 이러한 특성을 이용하여 소리가 재생될 때 발생하는 지속적인 전자파를 '1', 소리가 재생되지 않을 때 발생하지 않는 전자파를 '0'으로 변조하여 OOK(On-Off Keying)방식으로 은닉 채널을 형성하였다.



[그림 1] Galaxy S22에서 볼륨이 0일 때 소리 재생 시 발생하는 전자파 신호

2.2 기존 스마트폰 소리 재생을 이용한 은닉 채널의 한계점

[그림 1]의 ②는 Galaxy S22에서 볼륨이 0일 때 소리 재생 시 발생한 전자파 신호 파형이다. 소리가 재생되는 동안 지속적인 전자파가 발생하지 않고 재생 즉시 일시적인 전자파 신호만 발생하여 기존 OOK방식의 적용이 불가하였다. 따라서 해당 전자파 신호를 분석하여 새로운 은닉 채널 형성 방안을 연구할 필요가 있다.

III. 무음 소리 재생 시 발생하는 전자파 특징 분석

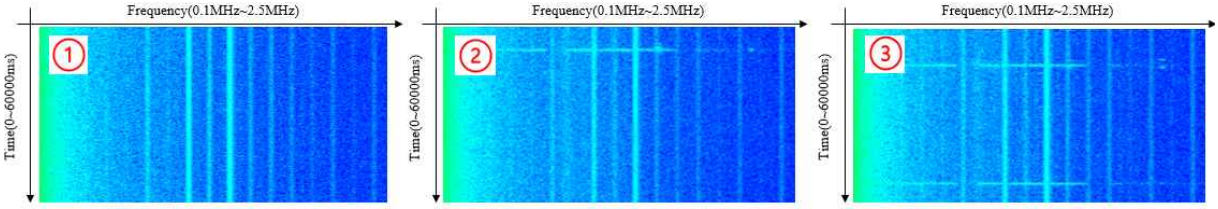
3.1 실험 환경

스마트폰 소리 재생 시 전자파 신호 특성 분석과 은닉 채널 신호를 수신받기 위한 실험 환경은 [그림 2]와 같다. [그림 2]의 ①은 Probe로 받은 신호를 10Hz~44GHz 사이의 원하는 주파수 대역별로 신호를 구분하여 표시하는 KeySight 사의 EXA N9010B 신호 분석기이다. [그림 2]의 ②는 스마트폰에서 방출되는 전자파를 탐지 및 수집을 하는 Probe이고, 100kHz에서 50MHz 사이의 주파수 대역을 탐지하는 Langer 사의 LF-R 400 H-Field Probe(2-A)이다. [그림 2]의 ③은 실험 대상 스마트폰인 Samsung 사의 2022년에 출시한 Galaxy S22이다. 전자파 측정 시 스마트폰 화면을 켠 상태에서 Probe의 위치는 스마트폰 뒷면 하단 스피커 부분으로 하였고, Probe와 대상 스마트폰 사이의 거리는 0.3cm이다. 신호 송신에 사용되는 소리 재생을 위해 Android Studio를 사용하여 SoundPool 클래스의 내장 함수인 play로 음성 파일을 재생하고, delay 함수로 재생 사이 시간을 지연시키는 애플리케이션을 구현하여 대상 스마트폰에서 실행하였다.

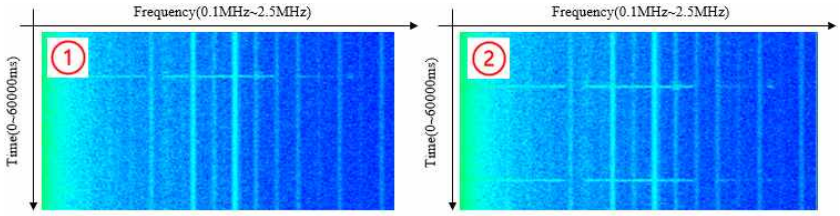
[그림 2] 실험 환경

3.2 실험 결과

파형의 가로축은 주파수 대역, 세로축은 시간, 색상은 흰색에 가까울수록 전자파의 세기가 강함을 나타낸다. [그림 3]은 모두 스마트폰 설정 볼륨이 0일 때 측정한 파형이다. [그림 3]의 ①은 아무 동작도 하지 않고 스피커 부분을 측정한 파형이다. [그림 3]의 ②는 음악 파일을 정지하지 않고 5초간 재생하였을 때 측정한 파형이다. 재생 즉시 0.02초 정도 전자파 신호가 발생하고 이후 다시 발생하지 않았다. [그림 3]의 ③은 음악 파일을 1초 재생한 후 3초 정도의 시간을 대기하였다가 재생했을 때 측정한 파형이다. 전자파 신호가 다시 발생하여 전자파 신호의 재발생에는 지연 시간이 필요함을 확인하였다. [그림 4]는 반복 재생할 때 전자파 신호가 재발생하는 최소 지연 시간을 측정하기 위해 재생 사이 지연 시간을 3000ms부터 100ms씩

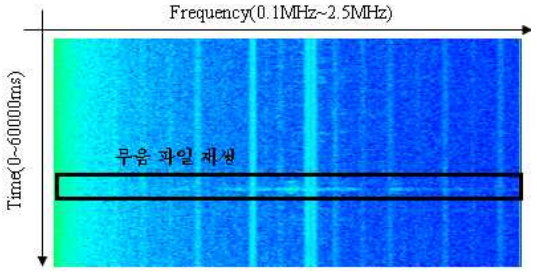


[그림 3] 볼륨이 0일 때 소리 재생 상황에 따른 전자파 신호 파형



[그림 4] 재생 사이 지연 시간이 3000ms, 3100ms일 때 전자파 신호 파형

증가시켜서 측정한 결과이다. [그림 4]의 ①인 3000ms의 지연 시간에서는 전자파 신호가 다시 발생하지 않았고, [그림 4]의 ②인 3100ms의 지연 시간일 때 전자파 신호가 다시 발생하여 최소 지연 시간은 3100ms로 측정하였다.



[그림 5] 볼륨이 켜진 상태에서 무음 파일을 재생했을 때 발생하는 전자파 신호 파형

[그림 5]는 스마트폰 설정 볼륨을 켠 상태에서 0Hz의 소리를 볼륨 0으로 녹음한 1초 길이의 파일을 재생해 측정한 파형이다. 볼륨이 0일 때 음악 파일을 재생한 [그림 3]의 ②와 같은 전자파 신호가 발생하였다. 이를 통해 스마트폰 설정 볼륨에 상관없이 소리 재생 시 스피커에서 소리가 나지 않으면 전자파 신호가 발생함을 확인하였다. 이러한 특징을 이용해 스마트폰의 볼륨 설정 권한이 없어도 무음인 은닉 채널을 형성할 수 있다. [그림 6]은 최신 삼성 스마트폰 3종의 전자파 신호 재발생에 필요한 최소 지연 시간을 측정한 파형이다. 3종 모두 무음 소리 재생 시 전자파 신호가 발생하였고, 반복 재생했을 때 전자파 신호가 발생하려면 지연 시간이 필요하였다. [그림 6]의 ①에서 Galaxy S21의 최소 지연 시간은 3900ms, [그림 6]의 ②에서 Galaxy S22의 최소 지연 시간은 3100ms, [그림 6]의 ③에서 Galaxy S23 Ultra의 최소 지연 시간은 2900ms로 측정하였다.

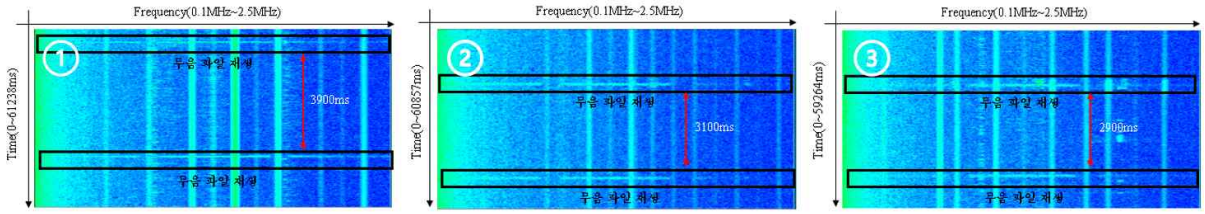
IV. 무음 소리 재생을 이용한 은닉 채널 형성

4.1 제안하는 은닉 채널 형성 방안

[표 1] 무음 소리 재생을 이용한 변조 방법

Algorithm 1. Modulation	
Input : bit_sequence, minimum_delay_time	
Output : modulated_signal	
1	**for** $i = 0$ **to** len(bit_sequence)
2	**if** bit_sequence[i] == 1 then
3	play(silent_sound)
4	delay(minimum_delay_time)
5	play(silent_sound)
6	delay(minimum_delay_time)
7	**else**
8	play(silent_sound)
9	delay(minimum_delay_time × 2)
10	play(silent_sound)

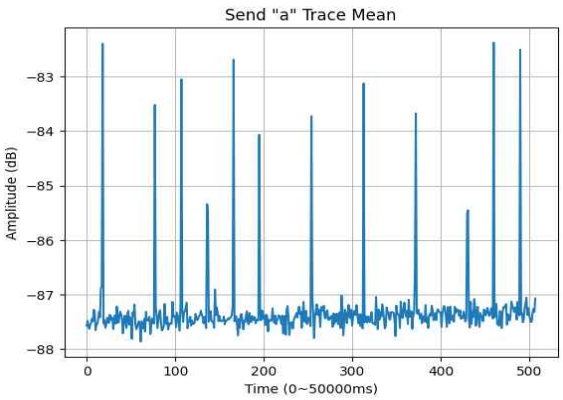
[표 1]은 무음 소리 재생 즉시 전자파 신호가 발생하고, 반복 재생 시 전자파 신호 재발생에는 최소 지연 시간이 필요하다는 특징을 이용하여 메시지를 변조한다. 비트열과 기기의 최소 지연 시간을 입력하면 비트값이 $1_{(2)}$인 경우 무음 소리 재생 후 최소 지연 시간으로 대기시키는 동작을 두 번 하고, $0_{(2)}$인 경우는 무음 소



[그림 6] 최신 삼성 스마트폰 3종의 전자파 신호 재발생에 필요한 최소 지연 시간 측정 파형

리 재생 후 최소 지연 시간의 두 배의 시간으로 대기시키는 동작을 한다. 비트열의 길이만큼 반복하고, 반복문이 종료되면 무음 소리 재생을 한 번 하여 마지막 신호를 발생시킨다. 복조 방법은 전자파 신호의 간격이 최소 지연 시간으로 두 번 발생하면 $1_{(2)}$로 복조하고, 신호의 간격이 최소 지연 시간의 두 배로 한 번 발생하면 $0_{(2)}$으로 복조한다. [표 1]은 비트당 변조에 같은 시간을 소요하여, 복조 시 시간에 따른 전자파 데이터를 최소 지연 시간의 두 배 간격으로 나눌 수 있다. 이를 통해 특정 비트를 변조하는 동안 잡음이 발생하여도, 몇 번째 비트인지 계산하여 해당 비트만 예외 처리할 수 있다.

4.2 제안하는 은닉 채널의 형성 결과



[그림 7] 무음 소리 재생을 이용한 은닉 채널을 통해 메시지 “a”를 보냈을 때, 시간에 따른 전자파 신호 변화의 0.1MHz~2.5MHz 대역의 평균

[그림 7]은 Galaxy S22에서 무음 소리 재생을 이용한 은닉 채널을 통해 “a” 문자를 아스키 코드로 인코딩하여 이진수로 변환한 비트열 $01100001_{(2)}$을 전송했을 때, 시간에 따른 전자파 신호 세기 변화의 0.1MHz~2.5MHz 주파수 대역의 평균이다. [그림 7]에서 $1_{(2)}$의 신호에 대응되는 전자파 신호 간격은 3100ms로 두 번 나타나고, $0_{(2)}$의 신호에 대응되는 전자파 신호 간격은 6200ms로 한 번 나타났다. 따라서, -86dB을 임곗값으로 삼아 파형을 전처리하고, 전자파 신호의 시간 간격에 따라 복조한다면 $01100001_{(2)}$을 에러 비트 없이 수신할 수 있다.

V. 결론

본 논문에서는 무음 소리 재생을 이용한 새로운 은닉 채널 형성 방안을 제안하였다. 3종의 최신 삼성 스마트폰을 대상으로 무음 소리 재생 시 스피커 부분에서 발생하는 전자파 신호를 분석하였고, 이를 통해 기존에 연구된 볼륨이 0일 때 소리 재생을 이용한 은닉 채널이 최신 삼성 스마트폰에 적용할 수 없음을 보였다. 또한, 스마트폰 기종별로 재생 사이에 다른 최소 지연 시간이 지나야 다시 전자파 신호가 발생함을 확인하였다. 분석한 전자파 신호의 특징을 바탕으로 비트값에 따라 다른 시간 간격으로 무음 소리를 재생하여 변조하고, 발생하는 전자파 신호의 간격을 측정하여 메시지를 복조하는 은닉 채널을 제안하였다. 이를 통해 은닉 채널을 성공적으로 형성하여 메시지를 송/수신한 결과를 제시하였다. 향후 연구로는 다른 제조사의 최신 스마트폰에도 제안한 은닉 채널을 적용하고, 스마트폰의 메모리 부분을 이용한 은닉 채널을 제안할 예정이다.

[사사] “이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00913, 무선 은닉 채널 위험성 검증 연구)”

[참고문헌]

[1] 안성현, “스마트폰 특성 전자기파를 이용한 은닉 채널 형성 방안”, 국내석사학위논문, 국민대학교 일반대학원, 2022.