유비쿼터스 컴퓨팅 시스템이 생성하는 전자기장 신호의 응용 동향 연구

이의제, 김효수*

중앙대학교

exitfill1234@cau.ac.kr, *hskimhello@cau.ac.kr

A Survey Study on the Applications of Electromagnetic Signal Induced by Ubiquitous Computing Systems: 'Potential Threat or Opportunity'

Lee Eui Je, Kim Hyo Su*

Chung-Ang Univ.

요 약

본 논문은 유비쿼터스 컴퓨팅 시스템 (예, 스마트폰, 무선 이어폰, 전기자동차)이 발생시키는 전자기장을 응용 및 활용하는 연구 동향에 대해 살펴본다. 연구를 스피커 위협 모델, 기타 전자 모듈 모델, 상호작용 기기 응용 그리고 인증 응용으로 분류하고 차세대 유비쿼터스 컴퓨팅 환경 실현을 위해 전자기장의 하드웨어/소프트웨어적 특성의 탐구를 역설한다.

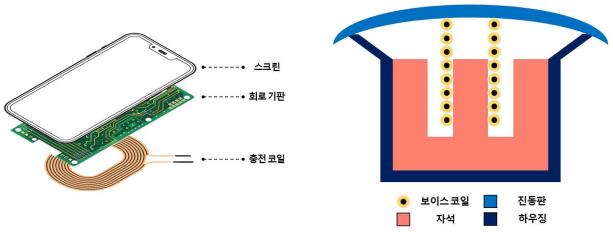

그림 1. 스마트폰 무선 충전 모듈과 스피커 구조

Ⅰ. 서 론

본 논문에서는 유비쿼터스 컴퓨팅 시스템 (예, 스마트폰, 무선 이어폰, 전기자동차)이 발생시키는 전자기장을 응용 및 활용하는 연구 동향에 대해 탐구한다. PC의 발명 이후, 우리는 여러 전자제품과 일상생활을 함께하고 있다. 이러한 전자제품은 전류가 흐르는 회로와 센서로 인해 전자기장(electromagnetic field)을 발생시킨다. 예를 들어, 그림 1과 같이 스마트폰 무선 충전을 지원하기 위한 코일 그리고 음성을 재생하기 위한 스피커의 보이스 코일이 비교적 큰 세기의 전자기장을 발생시킬 수 있다 [11, 2]. 사용자와의 상호작용이 일어날 시, 전자기장은 관련된 특성을 반영하여 전파한다. 이러한 독특한 전자기장의 특성을 활용한 연구가 최근 활발히 진행되고 있다. 한편, 사용자 또는 시스템을 공격하는 위협 모델 (threat model)이 연구되어 민감한 정보를 탈취하는데 활용되고 [1, 2, 4, 5, 6], 다른 한편으로는 새로운 상호작용을 제시하여 사용자-입력 인터페이스의 표현력을 증대시키고 있다 [3, 7, 8, 9, 10, 11]. 이러한 기술 동향을 살펴보고 향후 연구 방향을 제시하고자 한다.

Ⅱ. 본론

해당 문단에서는 전자기기에서 발생하는 전자기장을 활용한 위협 모델와 응용 연구들을 분류하고 살펴본다. (표 1)

스피커 위협 모델: 스마트폰과 무선 이어폰에 탑재되어 있는 스피커는 보이스코일, 자석, 진동판으로 구성되어 있다. 요구되는 음성을 출력하기 위해 전자 모듈이 음성 신호에 맞는 전기 신호를 보이스코일에 보내면, 전기 신호로 생성된 자기장이 진동판을 밀어내어 공기중에 상응하는 소리를 전달하게 되는 원리이다. 정리하자면, 스피커는 코일로 이루어진 자석이다. 이러한 구조를 이용하면, 외부에서 자기장을 생성하여 공격자(adversary)가 의도한 음성을 '삽입'할 수 있다 [1]. 또한, 사용자가 무선 이어폰이나 헤드폰을 통해 재생하고 있는 소리를 실제 마이크 없이 수십 cm 거리에서 도청할 수 있다 [2, 4]. 이는 스피커의 보이스코일로부터 유출되는 전자기장이 재생 중인 소리 신호와 큰 상관관계를 띄기 때문이다. 이러한 공격 기술은 Apple Siri와 같은 Voice Assistant 기술을 공격하여 사용자로 위장하는데 사용될 수 있다. 스피커와 같은 하드웨어 제조사들은 이와 같은 공격을 방어할 수 있는 새로운 구조를 연구할 필요가 있다.

기타 전자 모듈 위협 모델: 공격 음성 삽입 및 전자기장 유출 위험은 스피커에게만 존재하는 것이 아니다. 전자제품을 구성하는 부품 중, 공기 중에 진동을 만들어낼 수 있는 스피커와 유사한 구조를 가지거나 측정할 수 있는 크기의 전자기파를 유출할 수 있는 부품이 존재하면 위험이 존재할 수 있다. 예를 들어, LED 램프에 존재하는 축전기(capacitor)는 스피커와 유사한 구조를 지니고 있어 piezoelectric effect를 통해 음성 노이즈를 발생시킬 수 있다 [5]. 이러한 특성과 신호 처리 기술을 활용하여 스마트폰으로부터 최대 10.5 cm 되는 거리에서 '문을 열어줘'라는 음성 명령을 입력할 수 있다. 반면, 삼성페이에 사용되는 MST 코일과 같은 특수한 모듈에서도 위험이 존재한다. 철과 같은 강자성 물질이 삼성페이 자기 신호와 같이 '강한' 외부 자기장을 만나면, 물질의 모양과 크기가 빠르게 변화하는 magnetostriction 현상이 발생한다. 이 때, 현상으로 인해 고주파의 소리가 발생하는데, 해당 소리를 통해 삼성페이 결제 토큰을 복원할 수도 있다 [6]. 이 외에도 주변을 구성하는 전자기기에 숨겨진 위험이 존재할 수 있다 [9]. 이를 사전에 탐구하고 방어 수단을 구축하는 것이 해결해야 할 과제이다.

상호작용 기기 응용: 유출된 전자기장은 위험만 되는 것은 아니다. 사용자의 입력 인터페이스 표현력 증대에 중요한 역할을 할 수 있다. 일례로, 무선 이어폰의 스피커가 자석이라는 점에 착안하여 스마트폰으로부터 무선 이어폰의 위치를 mm 단위의 정확도로 파악할 수 있다 [8]. MagSound [8]의 연구진은 자석은 거리가 가까울수록 (mm 수준), 소리

는 거리가 비교적 먼거리에서 (1cm ~ 1m) 정확도가 높다는 점을 활용하여 두 센서 모달리티를 조화롭게 융합하였다. 한편, EVLeSen [10] 및 MagPie [11]은 각각 전기자동차의 모터 및 자율주행을 위한 센서 그리고 무선 충전 코일에 강자성 금속을 놓았을 때 변화하는 전자기장의 특성을 활용하였다. EVLeSen는 차 내부에서 수행할 수 있는 10가지 동작과 MagPie는 커스텀이 가능한 스마트폰 뒤편의 엑세서리를 통해 사용성이 높은 새로운 상호작용 방식을 제안하고 있다. 이처럼 다양한 폼펙터 및 기기에서 새로운 상호작용을 제시하는 연구가 더욱 진행될 수 있을 것이다.

인증(Authentication) 응용: 전자기장의 특성은 사용하기에 따라 앞서 살펴본 공격 위험이 될 수도, 또는 공격을 막는 방패의 역할을 할 수도 있다. 입력한 정보에 대한 특성을 남기고 있는 유출된 전자기장을 인증에 활용할 수 있기 때문이다. MagLive [3]은 사람 음성과 스피커 음성이 전자기장에 남기는 서로 다른 특성을 통해 음성 생체 인식(liveness detection) 명령이 실제 사람의 것인지 가짜로 생성된 음성인지를 판별하는 연구이다. iSTELAN [7] 연구는 사용자가 스마트폰 어플리케이션들을 사용하기 위해 터치할 때 발생하는 전자기장을 분석한다. 어플리케이션의 종류와 사용자 주변 환경에 따라 특성이 다르기 때문에 인증에 충분히 활용 가능한 연구이다. 이러한 연구에서 알 수 있듯이, 전자기장의 특성을 분석하는 데 대부분 스마트폰에 내장되어 있는 Magnetometer 센서가 앞으로 중요한 역할을 할 것이다.

이처럼 우리 주변의 전자기장은 유해할 수도 또는 유익할 수도 있다. 제조사는 하드웨어를 설계할 때 여러 시뮬레이션 방식을 통해 잠재적 위험을 도출할 필요가 있다. 반면에, 새로운 컴퓨터 시스템을 도입하여 사용성, 범용성의 새로운 지평선을 열 수도 있다. 두 가지 측면을 상호적으로 고려한 연구가 진행되어야 할 것이다.

연구	기술	대상	성능
Magbackdoor [1]	공격 음성 삽입	스마트폰 스피커	Success Rate 95%
MagEar [2]	음성 도청	무선 이어폰	Similarity 90%
Periscope [4]	음성 도청	유선 헤드셋	WER 7.44%
CapSpeaker [5]	공격 음성 삽입	LED 램프	최대 10.5 cm
MagSnoop [6]	MST 토큰 도청	MST 토큰	Accuracy 93.6%
MagHacker [9]	필기 도청	스타일러스 펜	Accuracy 80%. 거리 10cm
MagSound [8]	2D tracking	무선 이어폰	Accuracy 95.43%
EVLeSen [10]	모션 인식	전기자동차	Accuracy 90%
MagPie [11]	입력 인터페이스	스마트폰 무선 충전 모듈	Accuracy 97.1%
MagLive [3]	음성 샘플링 방어	스마트폰 마이크	EER 0.77%
iSTELAN [7]	터치 이벤트 추론	Magnetometer	Accuracy 90%

표 1. 위협 모델 및 응용 연구 요약

Ⅲ. 결론

본 논문에서는 스마트폰, 무선 이어폰, 전기자동차과 같은 유비쿼터스 컴퓨팅 시스템에서 유출되는 전자기장의 활용 연구 동향에 대해 살펴보았다. 최근 연구는 스피커 위협 모델, 기타 전자 모듈 모델, 상호작용 기기 응용 그리고 인증 응용으로 나눌 수 있다. 이러한 연구들은 정교화되고, 정확도가 높아지고 있으며 다양한 기기에서 탐구되고 있다. 위협을 막기 위해서 하드웨어 제조사의 잠재적 위험 평가가 필요하고, 새로운 시스템의 연구를 위해선 전자기장에 대한 깊은 탐구가 필요하다. 상호 보완적으로 연구가 진행된다면 보안성과 사용성을 동시에 충족하는 차세대 유비쿼터스 컴퓨팅 환경을 실현할 수 있을 것이다.

참 고 문 헌

[1] Liu, Tiantian, et al. "Magbackdoor: Beware of your loudspeaker as a backdoor for magnetic injection attacks." 2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023.

[2] Liao, Qianru, et al. "MagEar: eavesdropping via audio recovery using magnetic side channel." MobiSys. 2022.

[3] Sun, Xiping, et al. "MagLive: Robust Voice Liveness Detection on Smartphones Using Magnetic Pattern Changes." arXiv preprint arXiv:2404.01106. 2024.

[4] Chen, Huiling, et al. "Eavesdropping on Black-box Mobile Devices via Audio Amplifier's EMR." Proceedings of the 2018 Annual International Conference on Network and Distributed System Security (NDSS). 2024.

[5] Ji, Xiaoyu, et al. "Capspeaker: Injecting voices to microphones via capacitors." Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021.

[6] Choi, Myeongwon, et al. "Extracting Payment Tokens Out of Sounds Produced by Magnetic Field Fluctuations." IEEE Transactions on Mobile Computing 23.9 (2024): 8803-8821.

[7] Mohamed, Reham, et al. "Istelan: Disclosing sensitive user information by mobile magnetometer from finger touches." Proceedings on Privacy Enhancing Technologies (2023).

[8] Wang, Lihao, et al. "Magsound: Magnetic field assisted wireless earphone tracking." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 7.1 (2023): 1-32.

[9] Liu, Yihao, et al. "Maghacker: eavesdropping on stylus pen writing via magnetic sensing from commodity mobile devices." Proceedings of the 18th international conference on mobile systems, applications, and services. 2020.

[10] Cui, Minhao, et al. "EVLeSen: In-Vehicle Sensing with EV-Leaked Signal." Proceedings of the 30th Annual International Conference on Mobile Computing and Networking. 2024.

[11] Kim, Insu, et al. "MagPie: Extending a Smartphone's Interaction Space via a Customizable Magnetic Back-of-Device Input Accessory." Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. 2025.