THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2024 August; 35(8), 622～626.

http://dx.doi.org/10.5515/KJKIEES.2024.35.8.622
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

전자기/회로 공동 시뮬레이션을 이용한 하드웨어 트로이목마 신호탈취 시스템의 모델링

Modeling of Hardware Trojan Signal Hijacking System Using EM/Circuit Co-Simulation

이 다 현 · 정 재 영

Dahyun Lee · Jae-Young Chung

요 약

전자기기에 악의적으로 하드웨어 트로이목마(HT, Hardware Trojan)를 삽입하고 외부로부터 전자파를 조사하여 정보를 탈취하는 기술이 보안 위협으로 대두되고 있다. 이와 관련된 연구들은 주로 반복적인 실험을 통해 이루어져 많은 시간과 공간이 소요된다. 본 논문에서는 전자기/회로 공동 시뮬레이션 기법을 이용하여 HT 기반 신호탈취 시스템을 모델링한 연구를 소개한다. 전자회로에 설치된 HT에 의해 전자회로 내의 신호가 변조되고 후방산란(backscattering)되어 외부에서 수신되는 시스템을 모델링하기 위해 전자기, 회로, 신호무결성 해석 등 3종의 시뮬레이션 소프트웨어를 연동하였다. 시뮬레이션 결과를 통해 고가의 실험 장비 없이 HT기반 정보탈취 시스템에 대한 이해를 높이고 추후 방어 기술 개발과 실험 시스템의 최적 구축에 활용할 수 있다.

Abstract

The hijacking of critical information by inserting Hardware Trojans (HT) into electronic devices is a significant security threat. Research on countermeasures against this threat has primarily relied on repeated experiments that require substantial time and resources. This letter introduces a simulation study that models an HT-based signal hijacking system by incorporating multiple simulation software packages. To model a system where signals are modulated and backscattered by an active HT inserted into an operating electronic circuit, three types of simulation software are used: full-wave electromagnetic analysis, circuit simulator, and signal integrity analysis tools. With this co-simulation strategy, the effects of the external electromagnetic wave frequency, HT location, distance, and polarization of the transmitting and receiving antennas on the backscattered signals can be examined. This is useful for understanding HT-based information hijacking systems and developing countermeasure technologies.

Key words: Electromagnetic Security, Hardware Trojan, Intentional Electromagnetic Leakage, EM/Circuit Co-Simulation

Ⅰ. 서 론

TEMPEST는 1960년대 후반 미국 정부의 작전명으로,

「이 논문은 2022년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-23-005).」

서울과학기술대학교 전기정보공학과(Department of Electrical and Information Engineering, Seoul National University of Science and Technology)

· Manuscript received July 23, 2024 ; Revised July 30, 2024 ; Accepted August 16, 2024. (ID No. 20240723-070)

· Corresponding Author: Jae-Yonung Chung (e-mail: jychung@seoultech.ac.kr)

전자기기로부터 누설된 전자파를 탐지, 수집, 분석하여 민감한 정보를 탈취하는 기술, 그리고 이를 방어하는 기술을 총칭한다. 최근 스피커폰, 모니터, 노트북 등으로부터 누설된 전자파를 복조하여 음성 및 영상을 복원한 연구들이 보고되고 있다[1],[2]. 이를 위해서는 짧은 시간에 급격하게 변화하는 디지털 클럭 신호에 의해 누설되는 고주파 신호들을 원거리에서 수집하는 것이 중요하다. 전파적합성 인증을 받은 전자기기의 경우 누설 전자파의 크기가 미약하여 최첨단 신호처리 기술로도 원신호의 복원이 불가능할 수 있다. 이렇게 전자기기의 내부에서 비의도적으로 누설된 미약 전자파가 아닌, 외부에서 의도적으로 전자파를 전자기기에 인가하여 정보누설을 꾀하는 기술(IEML, intentional electromagnetic leakage)이 보안 위협으로 대두되고 있다[3]. 악의를 가진 해커가 전자기기의 기획, 제조, 유통, 사후관리 등 다양한 과정 중에 몰래 하드웨어 트로이목마(HT, Hardware Trojan)를 설치하고 원하는 시간에 선택적으로 정보를 탈취할 수 있을 뿐 아니라 제어권 탈취, 급격한 전력소모 및 기능 불능 등을 꾀할 수 있다.

최근 HT를 칩 내부, 회로 기판, 케이블 등에 설치하여 정보를 탈취하거나 악의적으로 설치된 HT를 감지하는 연구가 보고되고 있다[4]~[6]. 이러한 연구는 주로 고가의 측정 시스템을 구축하고 반복적인 실험을 통해 이루어지고 있다. HT소자의 설계 및 HT 설치 위치 분석 등을 위해 전자파 또는 회로 시뮬레이션 소프트웨어를 부분적으로 이용한 경우는 있으나[7], HT기반 신호탈취 시스템 전반을 모델링하여 해석한 연구는 보고된 바가 없다. 그 이유는 능동소자인 HT가 전자회로에 실제로 설치된 상태에서 외부로부터 인가된 전자파에 의해 누설되는 신호의 시간응답(time response)을 단일 시뮬레이션 툴만으로 계산할 수 없기 때문이다.

본 논문에서는 전자기/회로 공동 시뮬레이션 (em-circuit co-simulation) 기법을 이용하여 외부에서 의도적으로 전자파를 인가하는 송신 안테나, HT가 설치된 인쇄회로기판(PCB, printed circuit board), HT에 의해 변조되고 후방산란(backscattering)하는 전자파를 수신하는 안테나를 포함한 전체 시스템을 전자기/회로 공동 시뮬레이션 기법을 이용하여 설계하였다.

Ⅱ. HT 기반 신호탈취 시스템의 모델링

그림 1은 전자회로에 HT를 설치하여 신호탈취를 꾀하는 시스템의 개요도이다. 별개의 송신 및 수신 안테나를 사용하는 bistatic 송수신 시스템으로, 외부로부터 PCB에 인가된 고주파 신호와 PCB 내의 선로를 통해 전송되고 있는 clock 신호가 HT에 의해 진폭변조(AM, amplitude modulation)되고 후방산란하여 수신 안테나에 이르는 원리로 신호를 탈취한다. 여기서 HT는 수동혼합기(passive mixer) 역할을 하며 전송선로의 중간에 매설되어 후방산란을 도모하는 비의도적 안테나(UA, unintentional antenna)를 구성한다.

수신단에서 탈취한 신호의 신호 대 잡음비(SNR, signal-to-noise ratio)를 높이기 위해서는 기본적으로 높은 파워의 송신기, 고이득 안테나 및 낮은 감도의 수신기를 사용해야 한다. 이 외에도 탈취 대상 신호를 효율적으로 변조 및 후방산란시킬 수 있는 HT와 UA를 선정하는 것이 중요하다. 이러한 과정을 반복적인 실험에만 의존하는 것은 많은 시간과 노력을 요구할 뿐 아니라, 결과 해석에 대한

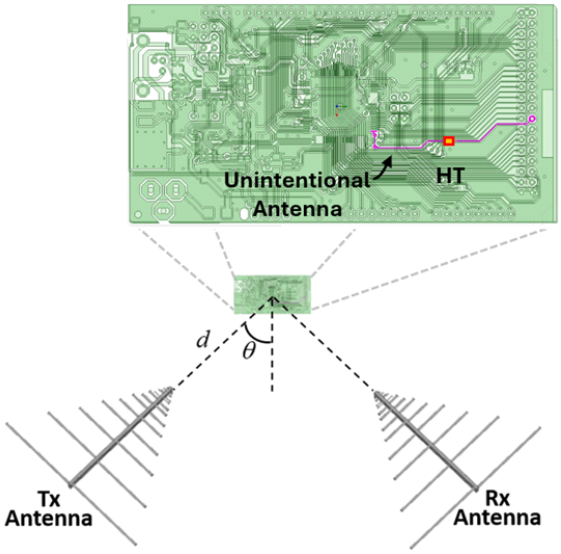

그림 1. 하드웨어 트로이목마(HT)가 매설된 전송선로를 안테나로 활용하여 신호를 탈취하는 bistatic 송수신 시스템

Fig. 1. A bistatic Tx/Rx system with an HT embedded in a transmission line in a printed circuit board.

제약이 크다. 그리하여 본 연구에서는 시뮬레이션 소프트웨어를 이용하여 HT 기반 신호탈취 시스템을 모델링하고 시스템 입출력 관계를 해석하고자 한다. 하지만 흔히 사용하는 3차원 전자파 시뮬레이션 툴(예: Ansys HFSS, Dassault systems CST 등)만으로는 해석이 불가하다. 구동 중인 전자회로에 능동소자인 HT에 의해 변조되고 후방산란된 신호의 주파수 응답 뿐 아니라, 시간응답을 관찰해야 하기 때문이다. 그리하여 본 논문에서는 전자파 해석, 회로 해석, 신호무결성 해석 등 3가지 시뮬레이션 툴을 연동하여 시스템을 모델링하였다.

그림 2는 회로 시뮬레이션 툴인 Ansys Circuit Simulator에 설계된 전체 시스템을 보여준다. 좌측의 clock signal은 탈취하고자 하는 신호로, 신호무결성 해석 툴인 Ansys SIwave를 이용하여 설계된 PCB에서 생성된 신호이다. 본 논문에서는 ATmega 마이크로컨트롤러가 탑재된 오픈소스 아두이노 메가 2560의 PCB를 설계하였다[8]. 공개된 IPC-2581 표준데이터와 IBIS(I/O buffer information specification) 모델 정보를 바탕으로 모델링하였다. 좌측 상단의 Tx Ant Input은 송신 안테나에 입력되는 정현파이다. 우측 하단의 Rx Ant output은 수신 안테나의 출력단으로, 송신 안테나에 의해 인가된 전파가 아두이노 PCB에 의해 후방산란되어 관찰되는 시스템의 최종단이다.

송수신 안테나와 아두이노 PCB는, 그림 1에서 볼 수 있듯이, 3차원 전자파 해석 툴인 Ansys HFSS에 모델링되어 각 입출력단 간의 산란계수(*S*-parameters)가 계산된다. 예를 들어, 송신 안테나와 UA 간 전송계수인 S_{21}, UA와 수신 안테나 간 전송계수인 S_{32} 등을 포함한 3×3 행렬이 계산된다. 송수신 안테나는 광대역 운용이 가능한 대수주기 안테나로 모델링하였다.

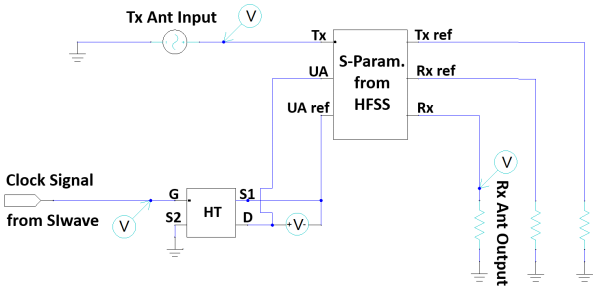

그림 2. SIwave, circuit simulator, HFSS를 연동하여 모델링한 HT기반 신호탈취 시스템
Fig. 2. The overall system modelled by incorporating SI wave, circuit simulator and HFSS.

SIwave로부터 제공된 저주파 clock 신호와 HFSS의 산란계수에 의해 보정된 고주파 신호가 HT에서 혼합되어 진폭변조 신호가 생성된다. 여기서 사용된 HT는 전계효과 트랜지스터(FET) 중 하나인 Avago ATE-54143으로 작은 게이트 전압 변화(~0.3 mV)에도 높은 임피던스 변화량(~600 Ω)을 보여 진폭변조용 수동혼합기에 적합한 제품이다[9]. 제작사에서 제공하는 FET 패키지의 회로도와 산란계수 정보를 바탕으로 ansys circuit simulator에서 모델링하였다. 그림 2의 HT블록에서 볼 수 있듯이 FET의 gate(*G*)단에 탈취하고자 하는 저주파 clock 신호가, source(S_1)와 drain(*D*)단에 병렬로 고주파 신호가 입력되도록 설정하였다. HT에 의해 진폭변조된 신호가 UA로 입력되고 후방산란하여 Rx Ant output에 이른다.

Ⅲ. 전자기/회로 공동 시뮬레이션 결과

본 절에서는 Ⅱ절에서 서술한 시뮬레이션 모델을 이용해 계산된 시뮬레이션 결과에 대해 논의한다. 그림 3은 HFSS를 통해 계산된 *S*-parameters이다. 더 구체적으로, 그림 1과 같은 설정으로 송신 안테나와 UA, UA와 수신 안테나 간의 *S*-parameters를 계산한 것이다. 여기서 송수신 안테나와 UA 간의 거리와 각도는 각각 d=1 m, θ=45°로

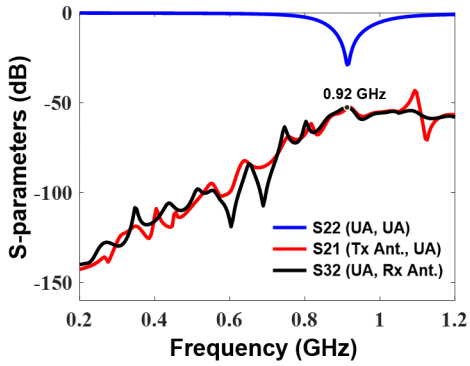

그림 3. 전파해석 툴인 HFSS를 이용해 계산된 *S*-parameters
Fig. 3. *S*-parameters calculated from the full-wave simulation tool HFSS.

설정하였다. UA는 그림 1과 같이 ATmega 2560 마이크로 컨트롤러 출력단과 연결된 43 mm 길이의 전송선로를 선정하였으며, 중간에 HT가 삽입되어 다이폴 안테나 형태를 이룬다. 그림 3에서 계산된 UA의 반사계수(S_{22})를 보면 0.92 GHz에서 공진함을 알 수 있다. 송신 안테나에서 UA로의 전송계수(S_{21})와 UA에서 수신 안테나로의 전송계수(S_{32})를 살펴보면 서로 유사한 경향성을 보임을 알 수 있다. UA의 공진주파수인 0.92 GHz에서의 전송계수값은 −52.5 dB로 송수신 안테나와 UA의 거리가 불과 1 m임에도 전파 감쇠가 상당함을 알 수 있다.

그림 4는 HT기반 신호탈취 시스템의 주요 단계에서의 시간응답 신호를 계산한 결과다. 즉, 그림 2의 시스템 블록도에 표기된 측정 프로브에서 계산된 시간응답으로, 송신 안테나에 입력되는 고주파 신호(Tx Ant input), HT에 입력되는 저주파 clock 신호(HT input), HT에 의해 진폭변조된 출력신호(HT output), 수신 안테나에서 관찰된 신호(Rx Ant output)가 그림 4의 위에서부터 아래 순으로 보여지고 있다. Tx Ant input은 주파수가 0.92 GHz(UA의 공진주파수)인 정현파로 진폭은 70 V이며, HT input의 clock 신호는 주기가 62.5 ns인 사각파이다. HT output 그래프를 보면 HT iutput의 사각파가 Tx Ant input의 정현파와 혼합되어 진폭변조된 것을 관찰할 수 있다. 이 진폭변조된 신호가 UA에 의해 후방산란되어 Rx Ant out에 관찰된 신호 역시 진폭변조된 형태를 유지한다. 하지만 0 state와 1 state가 각각 0.9 μV와 4 μV로 Tx Ant input의 진폭인 70 V에 비해 크게 낮음을 알 수 있다. 그럼에도 불구하고

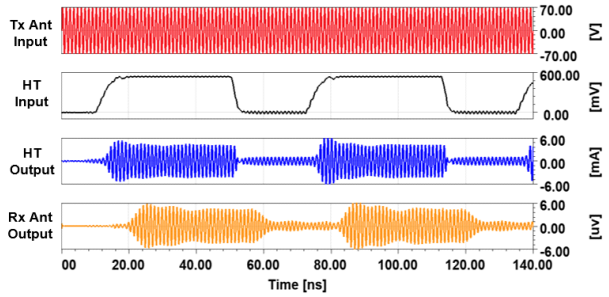

그림 4. 전자기/회로 연동 시뮬레이션을 통해 계산된 신호의 시간응답

Fig. 4. Time domain responses of input and output signals calculated by the EM/circuit co-simulations.

HT가 매설되지 않은 경우 거의 0에 가까운 후방산란 신호가 관찰된 것에 비해, HT 매설 후 pk-pk 8 μV의 변조된 신호를 수신할 수 있었다. 이는 −120 dBm이하의 수신감도를 갖는 수신기를 사용하면 감지할 수 있는 수준이다.

Ⅳ. 결 론

본 논문에서는 3가지 시뮬레이션 툴을 연동하여 HT기반 신호탈취 시스템을 모델링하였다. 모델링된 시스템을 검증하기 위해 오픈소스 아두이노 메가 2560을 victim PCB로 선정하고, 높은 임피던스 변화 특성을 갖는 FET를 HT로 선정하고 PCB에 설치하여 실제 구동되는 회로에 IEML이 인가됨에 따라 탈취되는 신호를 관찰하고자 노력하였다. 차기 논문에서는 여러 가지 시스템 파라미터를 조정함에 따라 탈취된 신호의 질이 어떻게 변화하는지 관찰한 결과 및 시뮬레이션 연구를 기반으로 구현한 실험 시스템을 이용해 측정한 결과들에 대해 논의하고자 한다.

References

[1] H. Lee, J. G. Yook, "Review of recent advances of TEMPEST," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, vol. 3, no. 2, pp. 29-38, Mar. 2020.

[2] D. H. Choi, E. Lee, T. Nam, and J. G. Yook, "Recent trends in image information recovery using leaked electromagnetic wave from electronic equipment," *IEEE Electromagnetic Compatibility Magazine*, vol. 11, no. 3, pp. 77-83, Dec. 2022.

[3] Y. S. Choi, S. S. Lee, Y. J. Choi, D. W. Kim, and B. C. Choi, "Trends of hardware-based Trojan detection technologies," *Electronics and Telecommunications Research Institute*, vol. 36, no. 6, pp. 78-87, 2021.

[4] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229-1247, Aug. 2014.

[5] D. Fujimoto, S. Nin, Y. I. Hayashi, N. Miura, M. Nagata, and T. Matsumoto, "A demonstration of a HT-detection method based on impedance measurements of the wiring around ICs," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 10, pp. 1320-1324, Oct. 2018.

[6] T. M. Supon, R. Rashidzadeh, "On-chip magnetic probes for hardware trojan prevention and detection," *IEEE Transactions on Electromagnetic Compatibility*, vol. 63, no. 2, pp. 353-364, Apr. 2021.

[7] M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Electromagnetic information extortion from electronic devices using interceptor and its countermeasure," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 4, pp. 62-90, Aug. 2019.

[8] Arduino, "Mega 2560 Rev3," 2020. Available: https://docs.arduino.cc/hardware/mega-2560

[9] Modelithics, "ATF-64143 data sheet." Available: https://www.modelithics.com/models/Vendor/Avago/ATF-54143.pdf

이 다 현 [서울과학기술대학교/석사과정]

https://orcid.org/0009-0005-3638-6907

2024년 2월: 서울과학기술대학교 전기정보공학과 (공학사)

2024년 3월～현재: 서울과학기술대학교 전기정보공학과 석사과정

[주 관심분야] EMI, EMC, 안테나 설계

정 재 영 [서울과학기술대학교/교수]

https://orcid.org/0000-0002-0982-6066

2002년 2월: 연세대학교 전기공학과 (공학사)

2002년 6월～2004년 6월: 모토로라 코리아 연구원

2007년 3월: 미국 오하이오주립대 전기 및 컴퓨터공학과 (공학석사)

2010년 6월: 미국 오하이오주립대 전기 및 컴퓨터공학과 (공학박사)

2010년 6월～2012년 8월: 삼성전자 책임연구원

2012년 9월～현재: 서울과학기술대학교 전기정보공학과 교수

[주 관심분야] 전자파 측정, 안테나 설계