THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2025 October; 36(10), 962～965.

http://dx.doi.org/10.5515/KJKIEES.2025.36.10.962
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

24 GHz FMCW Radar 기반 하드웨어 트로이목마 탐지 연구

Hardware Trojan Detection Using 24 GHz FMCW Radar

주경덕[1] · 임문철[2*] · 김용명[3] · 정영규[4**] · 권구형[5***] · 정영배[6]

Gyeong-Deok Ju[1] · Mun-Cheol Lim[2*] · Yong-Myeong Kim[3] · Young-Giu Jung[4**] · Koo-Hyung Kwon[5***] · Young-Bae Jung[6]

요 약

본 논문은 24 GHz FMCW 레이다를 활용하여 FPGA 내부의 하드웨어 트로이목마(HT)를 원격 탐지하는 비접촉식 기법을 제안한다. 제안 방법은 기존의 근접 EM 프로브 방식과 달리, FPGA 동작 시 발생하는 clock 신호와 레이다 신호의 혼변조 성분을 분석하여 정상 모델과 HT 삽입 모델 간의 스펙트럼 차이를 구분한다. 미약 신호 검출을 위해 8개 chirp 기반 코히런트 집적을 활용하여 SNR을 향상시켰으며, FFT를 통해 특징 벡터로 변환한 후 RBF 커널 SVM 분류기를 이용하여 분류하였다. 실험 결과, 평균 탐지율 98.5 %과 오탐율 1.2 %의 높은 성능을 달성하였다.

Abstract

This paper proposes a non-contact technique for remotely detecting hardware Trojans (HTs) in field-programmable gate arrays (FPGAs) using a 24 GHz FMCW radar. Unlike conventional proximity EM-probe methods, the approach analyzes intermodulation components between the FPGA clock signal and the radar signal to identify spectral differences between the normal (Golden) model and HT-inserted models. To enhance weak-signal detection, coherent integration across eight chirps is employed to improve signal-to-noise ratio, after which the received signals are transformed into feature vectors via FFT and classified using an RBF-kernel SVM. Experimental results demonstrate high performance, achieving an average detection rate of 98.5 % with a false positive rate of 1.2 %.

Key words: FMCW Radar, Hardware Trojan, FPGA Security, Coherent Integration, SVM Classifier

Ⅰ. 서 론

최근 사물인터넷(IoT) 기술의 급속한 발전은 스마트 홈, 산업 자동화, 헬스케어 등 다양한 분야에 혁신을 가져오고 있다. 특히 FPGA(field programmable gate array)는 재구성이 가능한 하드웨어 특성으로 인해 IoT 시스템의 핵

「본 연구는 국방과학연구소의 지원을 받아 수행된 연구임(UG233015TD).」

국립한밭대학교 전자공학과(Department of Electronic Engineering, Hanbat National University)
*국립한밭대학교 지능형나노반도체학과(Department of Intelligent Nano Semiconductor, Hanbat National University)
**YM 나을텍(Y.M. NaeulTech)
***국방과학연구소(Agency for Defense Development, ADD)
1: 석사과정(https://orcid.org/0009-0002-8902-7236), 2: 석사과정(https://orcid.org/0009-0008-3765-2818)
3: 석사과정(https://orcid.org/0009-0001-5945-0079), 4: 최고기술경영자(https://orcid.org/0009-0001-6062-7417),
5: 책임연구원(https://orcid.org/0009-0000-5158-8703), 6: 지도교수(https://orcid.org/0000-0002-7244-9187)

· Manuscript received July 2, 2025 ; Revised July 30, 2025 ; Accepted September 5, 2025. (ID No. 20250702-016S)

· Corresponding Author: Young-bae Jung(e-mail: ybjung@hanbat.ac.kr)

심 구성요소로 자리 잡았다[1]. 그러나 글로벌 공급망의 복잡성으로 인해 설계, 제조, 패키징 과정에서 악의적으로 하드웨어 트로이목마(HT, hardware Trojan)가 삽입될 가능성이 증가하고 있다[2].

HT는 특정 조건에서만 활성화되어 시스템 정보를 유출하거나 오작동을 일으키는 특성으로 인해 탐지가 매우 어렵다. 특히 IoT 환경에서는 수백만 개의 기기들이 연결되어 있어, 전체 네트워크의 보안을 위협할 수 있다.

본 논문에서는 24 GHz FMCW(frequency modulated continuous wave) radar를 활용하여 다양한 HT를 비접촉식 기법으로 탐지하는 새로운 방식을 제안한다. 기존의 전자계 프로브 방식은 회로에 프로브를 밀착시켜야만 측정이 가능하여 동작 중인 시스템에 적용이 어렵고, 프로브 위치 변화에 측정값이 크게 달라지는 한계가 있다. 반면, 본 연구 방식은 비접촉 기법으로 회로의 이상 신호를 감지할 수 있기에 적용 유연성과 측정의 재현성이 높아 회로의 보안 상태를 안정적으로 확인이 가능하다[3].

본 방식에 따르면, radar로부터 출력된 신호(f_0)가 FPGA 회로의 CPU와 같은 중앙 연산 모듈에 입력되어 CPU의 clock 주파수(f_c)와 혼변조(mf_0+nf_c)된 미약한 전자기 신호를 비접촉식으로 수신하여 분석함으로써 다양한 통신기기를 포함한 서버 등에 존재할 수 있는 HT를 검출할 수 있다.

Ⅱ. FMCW Radar를 이용한 HT 탐지

본 연구에서는 24 GHz 주파수 대역에서 동작하는 FMCW radar를 활용하였다. 해당 주파수는 60, 77 GHz 등 고주파에 비해 파장이 길어 전파 감쇠가 적고, 실내외 환경에서 안정적인 탐지가 가능하다. 또한, 관련 모듈이 상용화되어 실험 시스템 구성 및 하드웨어 구현이 용이하다.

Radar로는 FPGA 회로로부터 수신된 미약한 혼변조 신호를 탐지하는 데 한계가 있기에 이를 극복하기 위하여 기존의 단일 chirp를 활용한 방식이 아닌 다중 chirp 기반 코히런트 집적(multi-chirp coherent integration) 기법을 활용하여 수신 신호의 신호 대 잡음비를 높였다. HT에 의한 신호 변화 특성을 분석하고, 탐지 성능 분석을 위한 지도학습인 SVM(support vector machine) 분류 모델을 적용하여 HT가 존재하지 않는 정상적인 회로인 GM 모델(golden model)과 HT가 동작하는 회로(HT 모델)를 구분하였다.

제안된 HT의 탐지 방식은 그림 1에 도식된 바와 같이, 신호 전송 및 수신, 다중 chirp 기반의 신호 위상 정합 처리, 신호 전처리 및 주파수 도메인 변환, 특징 벡터 추출, SVM 분류, 최종 라벨링 단계로 구성된다. 특히, 다중 chirp 기반 코히런트 집적 기법을 통해 신호 대 잡음비를 높이고, 추출된 주파수 영역의 특징 벡터를 SVM 분류기에 입력하여 GM 모델과 HT 모델을 구분한다.

HT의 탐지는 FPGA 회로에서 동작하는 알고리즘에 따라 정상적인 프로세스와 HT가 동작 시 발생하는 미세한 Clock 주파수의 특성 변화를 분석한다. Clock 주파수나 혼변조 신호의 주파수 천이와 시간에 따른 신호전력의 세기 변화가 발생하나 미약 신호를 수신 한계로 인하여 탐지 성능이 크게 제한받는다.

이를 극복하기 위하여 본 연구에서는 다중 chirp 신호를 동일 위치에서 수신한 후 각 신호의 위상을 정렬하고 합산하는 코히런트 집적을 적용하여 잡음을 상쇄시키고 탐지 신호의 세기를 증가시켰다[4].

그림 2는 상단의 단일 chirp 수신 신호와 하단의 8개 chirp에 대한 집적 결과를 나타내며, 집적된 신호를 통하여 수신된 신호를 확인할 수 있다.

$$S_{coh}(t) = \sum_{n=1}^{N} s_n(t) = N \times s(t) + \sum_{n=1}^{N} n(t) \quad (1)$$

$$SNR_{coh} = N \times SNR_{\text{single}} \quad (2)$$

식 (1) 및 식 (2)와 같이, N개의 chirp 신호를 코히런트 집적하는 경우, 신호 성분 s(*t*)는 chirp의 개수에 비례하여 증가하지만 잡음 n(*t*)은 전력의 비상관(non-coherent) 특성

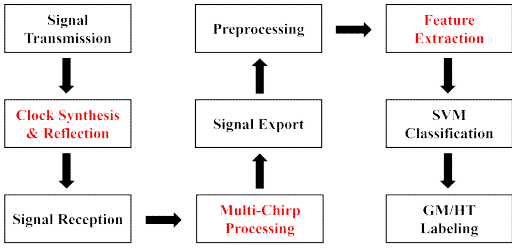

그림 1. HT 탐지를 위한 신호 처리 흐름도
Fig. 1. Signal processing flow for hardware Trojan detection.

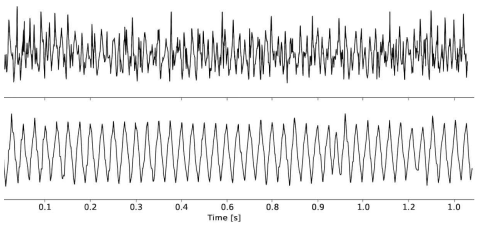

그림 2. Chirp의 수에 따른 코히런트 집적 향상 비교 결과 (8개 chirp(상)), 단일 chirp(하)
Fig. 2. Comparison of coherent integration gain according to the number of chirps (8 chirps (up)), single chirp (down).

으로 인해 상호 상쇄되어, 결과적으로 신호 대 잡음비가 N배만큼 향상된다[5].

제안된 방식의 효용성 검증하기 위한 시험은 건물 내의 복도를 포함한 다양한 실내 환경에서 수행되었으며, 본 시험환경과 장비 구성은 그림 3에 제시된 바와 같다. HT 탐지에 필요한 신호 수집을 위해 Digilent 사의 Arty-A7-100T FPGA 회로를 사용하여 두 가지 상태로 동작하도록 설정하였다. 첫 번째 상태는 정상적인 clock 주파수를 갖는 GM 모델이며, 두 번째 상태는 HT가 삽입되어 clock 주파수 패턴이 변형된 HT 모델로서 동작 상태를 구현하였다. 추가로, 삽입된 HT의 trigger 크기를 조정하여 미약한 신호의 세기 변화를 확인하였다.

GM과 HT 모델 간의 미세한 수신 신호의 변화를 분석하기 위하여, radar와 FPGA 회로 간의 거리는 약 1.5 m 간격으로 위치하였다. 각각의 동작 상태에 따라 동일한 조건에서 반복 측정을 진행하였으며, 주파수 도메인에서 측정된 신호는 CSV 형식으로 저장하였다. 저장된 데이터를 전처리하여 특징 벡터를 추출하고, GM 모델과 HT 모델

그림 3. Radar를 이용한 비접촉식 HT 탐지 시험 환경
Fig. 3. Radar-based remote HT detection setup.

간의 복잡하고 미약한 신호 패턴을 명확하게 구분하기 위해 SVM 분류기를 사용하였다. SVM은 고차원 특성 공간에서도 과적합 없이 안정적인 성능을 보이며, 모델 크기가 작고 예측 속도가 빠르기에 GM과 HT 모델 간의 분류에 적합하다. 추가로, 미약한 신호 패턴과 비선형 분포를 효과적으로 구분하기 위해 RBF(radial basis function) 커널을 적용하였으며, 이는 신호 간 유사도를 기반으로 데이터를 고차원 공간으로 매핑하여 GM과 HT 모델 간의 복잡한 분포를 명확하게 분리가 가능하다[6].

$$K(x_i,x_j) = \exp(-\gamma|x_i - x_j|^2) \tag{3}$$

식 (3)과 같이 x_i, x_j는 두 특성 벡터, γ는 커널의 폭을 조절하는 하이퍼파라미터이다. 이 함수는 각 벡터 간의 거리를 계산해 데이터를 고차원 공간으로 옮겨 분리하기에 어려운 데이터를 선형적으로 구분할 수 있도록 변환한다.

$$F1\,Score = 2 \times \frac{\mathrm{Precision} \cdot Recall}{\mathrm{Precision} + Recall} \tag{4}$$

식 (4)와 같이 GM 모델과 HT 모델에 해당하는 다양한 수신 신호를 수집한 뒤, 이를 주파수 영역에서 주요 성분으로 변환하여 특징 벡터를 추출하고, 이를 기반으로 SVM 분류기를 통해 두 클래스 간의 분류를 수행하였다. 분류 성능 평가는 SVM의 예측 결과를 실제 정답과 비교하여 precision(정밀도)과 recall(재현율)의 조화 평균인 F1 score를 계산함으로써, HT 탐지 성능을 확인하였다[7].

그림 4의 혼동 행렬(confusion matrix)은 SVM 분류기가 GM 모델과 HT 모델을 효과적으로 구분함을 보여주고 있다. 대각선의 진한 색상은 높은 분류 정확도를 나타내며, 각각의 모델별로 200, 1,000개 이상의 데이터 분류 성능 평균 98.5 % 달성하여 HT의 동작 여부를 판단할 수 있음을 알 수 있다.

그림 5는 특징 벡터를 3차원으로 축소하여 클러스터링을 진행한 PCA 시각화 결과이다. 본 결과를 통해 코히런트 집적 기법을 이용한 신호 처리 방식과 SVM 분류기를 활용하여 GM 모델과 HT 모델의 클러스터가 명확히 분리되어 있음을 알 수 있다. 이는 FPGA 회로의 정상적인 clock 신호와 HT에 의해 변조된 clock 신호가 radar chirp 신호와 혼변조 되어 생성된 혼변조 주파수 성분들이 서

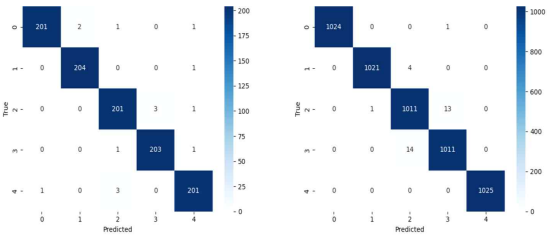

그림 4. SVM 분류기 혼동 행렬 결과
Fig. 4. Confusion matrix of SVM classifier results.

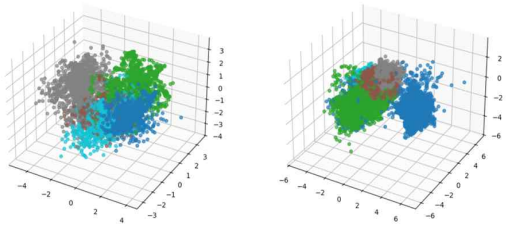

그림 5. PCA 3D 시각화 결과
Fig. 5. 3D visualization of feature vectors using PCA.

로 다른 스펙트럼 특성을 가짐을 의미한다.

특히, FPGA 회로에서 HT가 활성화되는 경우, 추가적인 회로 동작으로 인해 clock 주파수의 위상 잡음이 증가하고, 이는 혼변조 신호의 전력 스펙트럼상에서의 밀도 변화로 나타난다. SVM 분류기는 이러한 미세한 스펙트럼 변화를 RBF 커널을 통해 고차원 공간에서 효과적으로 구분하여, 1.5 m 거리에서도 HT 동작 여부를 높은 신뢰도로 탐지할 수 있음을 입증하였다.

Ⅲ. 결 론

본 논문에서는 FPGA 회로에 삽입된 HT를 비접촉 방식으로 탐지하기 위하여, 24 GHz FMCW radar를 활용한 비접촉식 탐지 기법을 제안하였다. 고가의 장비와 정밀한 위치 고정이 요구되는 기존 전자기 프로브 방식의 한계를 보완하고자, FPGA 동작 중 방출되는 전자기 신호를 비접촉식으로 수집하여 분석하는 방식을 활용하였다. 단일 chirp 신호로는 잡음으로 인해 식별이 어려운 주파수 성분을 효과적으로 검출하기 위해 다중 chirp 기반의 코히런트 집적 기법을 활용하여 신호 대 잡음비를 향상하였다. 수신된 신호를 주파수 도메인의 특징 벡터로 변환하고, 이를 SVM 분류기를 사용하여 정상 상태와 HT가 삽입된 상태를 구분하였다. 실험 결과, 평균 F1 score 98.5 %의 높은 분류 정확도를 보였으며, 혼동 행렬 결과와 시각화를 통해 두 상태 간의 구분이 가능함을 확인하여 FMCW radar 기반의 비접촉식 탐지 기법과 SVM 분류기를 통한 FPGA 내 HT 탐지에 유효함을 확인하였다.

향후 탐지 거리 확장을 위해 고이득 지향성 안테나의 적용, 다중 채널 신호 융합 기술 등을 통해 원거리에서도 안정적인 탐지가 가능할 것이라고 기대된다. 이를 통해 본 기술은 보안이 중요한 다양한 시스템에서 하드웨어 보안 위협 탐지에 효과적으로 활용될 수 있을 것으로 기대된다.

References

[1] C. Rooney, A. Seeam, and X. Bellekens, "Creation and detection of hardware trojans using non-invasive off-the-shelf technologies," *Electronics*, vol. 7, no. 7, p. 124, Jul. 2018.

[2] M. Tehranipoor, F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.

[3] O. Söll, T. Korak, M. Muehlberghuber, and M. Hutter, "EM-based detection of hardware trojans on FPGAs," in *IEEE International Symposium on Hardware-Oriented Security and Trust(HOST)*, Arlington, VA, May 2014, pp. 84-87.

[4] K. Jin, T. Lai, Y. Wang, G. Li, and Y. Zhao, "Coherent integration for radar high-speed maneuvering target based on frequency-domain second-order phase difference," *Electronics*, vol. 8, no. 3, p. 287, Mar. 2019.

[5] W. A. Lies, L. Narula, P. A. Iannucci, and T. E. Humphreys, "Long range, low swap-C FMCW radar," *IEEE Journal of Selected Topics in Signal Processing*, vol. 15, no. 4, pp. 1030-1040, Jun. 2021.

[6] K. L. Du, B. Jiang, J. Lu, J. Hua, and M. N. S. Swamy, "Exploring kernel machines and support vector machines: Principles, techniques, and future directions," *Mathematics*, vol. 12, no. 24, p. 3935, Dec. 2024.

[7] M. Sokolova, G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing & Management*, vol. 45, no. 4, pp. 427-437, Jul. 2009.