A Study on Non-Invasive Malware Detection Using Electromagnetic Radiation Monitoring

Gyeong-Deok Ju
Department of Electronic Engineering
Hanbat National University
Daejeon, South Korea
kyoungduk99@naver.com

Patrick Danuor
Department of Electronic Engineering
Hanbat National University
Daejeon, South Korea
30211162@edu.hanbat.ac.kr

Yong-Myeong Kim
Department of Electronic Engineering
Hanbat National University
Daejeon, South Korea
kym8971@naver.com

Mun-Cheol Lim
Department of Intelligent Nano Semiconductor
Hanbat National University
Daejeon, South Korea
mclim6@naver.com

Young-Bae Jung [0]
Department of Electronic Engineering
Hanbat National University
Daejeon, South Korea
ybjung@hanbat.ac.kr

***Abstract*— Modern IoT environments face escalating security risks from sophisticated malware attacks that exploit resource constraints in embedded devices. This study presents an electromagnetic radiation monitoring approach for non-invasive malware detection. We develop a framework that leverages processor clock emissions to identify malicious activities through pattern analysis. Our approach achieves complete detection coverage while extending the operational range to 8cm and successfully distinguishes different malware behaviors through spectral signature analysis. (Electromagnetic radiation, malware, security, side-channel)**

I. Introduction

Malware targeting IoT ecosystems has evolved into a significant threat, capable of compromising entire network infrastructures. Traditional software-based security solutions are often inadequate for resource-constrained embedded systems because their computational overhead prevents the deployment of comprehensive protection mechanisms.

Electromagnetic radiation monitoring has emerged as a promising alternative that operates independently of device resources. In this study, we investigate a streamlined approach focusing on processor clock emissions—the strongest electromagnetic signature—to identify malware activities by exploiting the relationship between software execution patterns and electromagnetic emissions. This method enables real-time detection with an enhanced detection range and simplified signal analysis for malware identification.

II. Proposed Method

A. System Model

The system consists of:

1. The IoT device under test (an Arduino UNO with a 16 MHz ATmega328P),
2. An electromagnetic sensing chain composed of an H-field probe, a low-noise preamplifier, and a spectrum analyzer,
3. A detection algorithm that processes the acquired signal.

When malware executes, it causes variations in current draw, which modulate the amplitude of the EM emissions. The 16 MHz clock serves as a carrier, and the CPU activity amplitude-modulates this carrier. If malware triggers a periodic pattern of CPU usage, this results in corresponding periodic modulation of the clock signal's amplitude.

B. Detection Algorithm

The received EM signal is modeled as:

$$s(t) = [A_0 + \Delta A(t)]\sin(2\pi f_C t) + n(t) \quad (1)$$

where f_C is the clock frequency (16 MHz), A_0 is the nominal amplitude, $\Delta A(t)$ represents modulation due to program activity, and $n(t)$ is noise. Under normal conditions, $\Delta A(t) \approx 0$, but malware creates periodic $\Delta A(t)$.

The detection method analyzes the received signal power $P(t)$ through autocorrelation or FFT to identify dominant periodic components. A pronounced spectral peak at non-zero frequency indicates periodic modulation, suggesting malware presence.

III. Experimental Results

Seven bitcount algorithms from the MiBench benchmark suite were used as malware surrogates, with each algorithm running 20,000 repetitions to create distinct periodic patterns. The measurement setup included a 25 mm diameter H-field probe, Langer PA 2522 preamplifier with 25 dB gain, and an Anritsu MS2090A spectrum analyzer. The proposed method achieved 100% detection accuracy across all test cases. Each algorithm produced a unique side-channel pattern, allowing for both detection and coarse-grained classification. The system correctly identified malware presence in all 35 test runs. Detection effectiveness was evaluated at 3 cm, 5 cm, and 8 cm distances. While signal strength naturally decreased with distance, the method remained effective at 8 cm using longer-term integration (2–3 seconds), representing a 60% improvement over existing methods that typically operate in the 0–5 cm range.

Table I. Comparison With Existing EM Malware Detection Methods

Method	Target Device	Clock Freq.	Detection Range
REMOTE [1]	Arduino UNO	16 MHz	≤ 5 cm
ULTRA [2]	ARM/MIPS	700 MHz-1.2 GHz	Direct meas.
Proposed	**Arduino UNO**	**16 MHz**	**≤ 8 cm**

IV. Conclusion

This study demonstrates the effectiveness of electromagnetic radiation monitoring for malware detection through clock frequency analysis. Our framework achieves operational simplicity, non-invasive monitoring, 8 cm detection range, and behavioral classification. The approach successfully identified all malware variants with 100% accuracy, demonstrating viability for practical IoT security applications. Future research will explore multi-device monitoring scenarios.

Acknowledgment

This work was supported by the IITP (Institute of Information & Communications Technology Planning & Evaluation)-ITRC (Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT) (IITP2025-RS-2024-00437886). This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP- 2025-RS-2022-00156212) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

References

[1] N. Sehatbakhsh et al., "REMOTE: Robust external malware detection framework by using electromagnetic signals," *IEEE Trans. Computers*, vol. 69, no. 3, pp. 312–326, 2020.

[2] D.-P. Pham, D. Marion, and A. Heuser, "ULTRA: Ultimate rootkit detection over the air," in *Proc. 25th Int. Symp. Research in Attacks, Intrusions and Defenses (RAID)*, 2022.

[3] R. Guthaus et al., "MiBench: A free, commercially representative embedded benchmark suite," in *Proc. 4th Annu. IEEE Int. Workshop on Workload Characterization (WWC)*, 2001, pp. 3–14.

[4] H. A. Khan et al., "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," *J. Hardw. Syst. Secur.*, vol. 3, no. 4, pp. 305–318, 2019.