2025 Design, Automation & Test in Europe Conference (DATE 2025)

Comb Frequency Division Multiplexing: A Non-Binary Modulation For AirGap Covert Channel Transmission

Mohamed Alla Eddine BAHI
Univ Rennes, INSA Rennes
IETR - UMR 6164
Rennes, France
mbahi@insa-rennes.fr

Maria MENDEZ REAL
Univ Bretagne-Sud
Lab-STICC - UMR 6285
Lorient, France
maria.mendez-real@univ-ubs.fr

Maxime PELCAT
Univ Rennes, INSA Rennes
IETR - UMR CNRS 6164
Rennes, France
mpelcat@insa-rennes.fr

***Abstract*—Isolated networks ensure the confidentiality of sensitive data on a system by eliminating all physical connections to public networks or external devices, making the system *air-gapped*. However, previous work has shown that Electromagnetic (EM) emanations when correlated with secret data, can lead to side or covert channels. Specifically, EM emissions caused by clocks can modulate high-frequency signals, enabling unauthorized data transmission to cross the air-gap.**

This work focuses on covert channels where a software or hardware Trojan inserted in the victim system induces side channel emissions that the attacker can recover through the covert channel, producing an intentional transmission and leakage of sensitive information.

This paper introduces a novel encoding method for covert channels called Comb Frequency Division Multiplexing (CFDM). CFDM leverages modulated signals emitted by the victim system, which are evenly spaced across the frequency spectrum, creating a comb-like pattern. Moreover, the uncontrolled nature of the side channel modulation can make each subcarrier carry different information. Unlike traditional methods such as Frequency Shift Keying (FSK) and Amplitude Shift Keying (ASK), CFDM encodes information in both the frequency and amplitude dimensions of the covert channel harmonic sub-carriers.

***Index Terms*—Electromagnetic covert attack, hardware security, side-channel attack, signal processing, air-gap systems.**

I. Introduction

Hardware cybersecurity has recently garnered increasing attention, as most sensitive data is stored, manipulated, and transmitted by general purpose electronic devices, while cyber attacks are becoming more and more sophisticated [4]. In particular, covert channel attacks exploit the art of creating unauthorized communication between an infected victim and an outsider attacker to leak sensitive information [3].

In the context of EM covert channels, to covertly communicate, an attacker classically distinguishes two different EM emission patterns from the victim system, one corresponding to the victim in an idle state, and a second one corresponding to the victim in an altered state. In this scenario, the Trojan program or hardware Intellectual Property block (IP) executing within the victim can manipulate the state of the victim to alternately provoke the two different EM patterns. This approach allows for the use of 2-symbol methods to encode information.

CFDM is a novel modulation technique that encodes information on both the frequency and amplitude power peaks of unintended EM leakage signals as a variation of both ASK and FSK to increase the number of bits transmitted per symbol period. Unlike state-of-the-art covert channel modulation techniques, which use nuanced control of On-Off Keying (OOK), Binary-ASK or Binary-FSK to create, or approximate a well-known modulation waveforms [5], CFDM does not require fine-manipulation of the signal to achieve modulation. Instead, CFDM takes advantage of signals that are naturally (unintended) modulated within the system itself, which we refer to as *auto-modulated* signals.

II. CFDM and auto-modulation

Low-frequency signals associated with digital data in systems can be modulated by higher-frequency signals due to non-linear coupling [1]. This interaction leads to phenomena such as data-carrying clocks. A notable instance of this effect occurs in mixed-signal chips, where digital-induced signals coupled with the Radio Frequency (RF) signal [2], resulting in long distance emitted signals, which are correlated to data. These signals manifest as evenly spaced harmonics, which arise from the mixing of imperfect square-shaped digital signals with higher-frequency clock signals.

This phenomenon, referred to as auto-modulation, is explored in this paper as a means to create a multi-symbol covert channel as illustrated in Figure 1.

While the trojan controls the sub-carrier through state alternation with a period of τ_s, this control is reflected over time as power variations of certain harmonics.
These harmonics act as the information-carrying components, where the maximum Power Spectral Density (PSD) of each harmonic maps to a unique set of values associated with each state in the set of states S_{st}, as expressed in equation 1:

$$state_i = \{(f_{sc}, p_{i,1}), (2 \cdot f_{sc}, p_{i,2}), \ldots, (k \cdot f_{sc}, p_{i,k})\} \quad (1)$$

978-3-9826741-0-0/DATE25/© 2025 EDAA

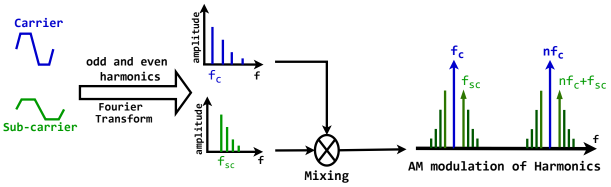

Fig. 1: Illustration of auto-modulation

with f_c: carrier fundamental harmonic frequency
f_{sc}: sub-carrier fundamental harmonic frequency
$n \in \mathbb{N}$: the order of the carrier harmonic

In equation 1:

- $state_i \in S_{st}$ represents the i-th state created by the trojan.
- f_{sc} is the fundamental frequency of the sub-carrier signal.
- $p_{i,k}$ denotes the maximum PSD of the k-th harmonic associated with the i-th state.

Additionally, each state is mapped to a unique symbol value s_i. As a result, for a generic N-symbol CFDM, S_{st} must have a cardinality that is a power of 2, expressed as:

$$N = \text{card}(S_{st}) = 2^m, \quad m \in \mathbf{N}^* \tag{2}$$

such that:

- $\text{card}(S_{st})$ denotes the cardinality of the set of states S_{st}.
- m is the number of transmitted bits in each symbol s_i.

In this scenario, the bit rate R_b is measured in bits per second (bit/s). is given by equation 3.

$$R_b = \frac{m}{\tau_s}\,\text{(bit/s)} \tag{3}$$

III. CFDM RECEIVER

Covert message transmission is achieved by sequentially executing a series of commands on the victim device, with each command corresponding to one of the states in S_{st} and also maps to a symbol value s_j.

$$s_j \Leftrightarrow \text{command}_j \tag{4}$$

The receiver captures the auto-modulated signal $S_{AM}(f)$, identifies the used commands through the state identification process, and reconstructs the message matrix $\mathcal{M}$ based on the alternating states as shown in equation 5. The time interval (or period) between two successive rows of the matrix corresponds to τ_s.

$$\begin{bmatrix} \text{command}_1 \\ \text{command}_2 \\ \vdots \\ \text{command}_j \end{bmatrix} \Leftrightarrow \mathcal{M} = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,k} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ q_{j,1} & q_{j,2} & \cdots & q_{j,k} \end{bmatrix} \tag{5}$$

In the message matrix $\mathcal{M}$:

- j represents the total number of commands used in the transmission process.
- k is the number of harmonics associated with each state in S_{st}.
- $q_{j,k}$ denotes the maximum PSD of the k-th harmonic for the j-th command.

Finally, $\mathcal{M}$ is mapped to the covert transmitted symbols as follows:

$$\mathcal{M} \Leftrightarrow \{s_1, s_2, \ldots, s_j\} \tag{6}$$

IV. CFDM FOR AUDIO INTEGRATED CIRCUIT (IC)

When recording audio on an air-gapped PC, the master clock of the audio IC auto-modulates the Analog-to-Digital Converter (ADC) clock, generating a CFDM harmonic signal of $f_{sc} = 48$ kHz. In this attack scenario, S_{st} consists of 4 states, determined by the combination of two distinct audio sampling rates and two different audio bit depths such that:

$$state_i = \{(f_{sc}, p_{i,1}), (3 \cdot f_{sc}, p_{i,3})\}, \quad i \leq 4 \in \mathbf{N}^* \tag{7}$$

V. RESULTS AND CONCLUSION

Experimental results demonstrate that CFDM can effectively establish a 2-bit-per-period covert channel between an audio processing chip in an air-gapped desktop computer and a Software Defined Radio (SDR) with an average Bit Error Rate (BER) that is 17.6% lower compared to conventional on/off encoding, and 25.8% lower relative to conventional Binary Amplitude Shift Keying (B-ASK) encoding.

REFERENCES

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, *The EM side-channel(s)*. In Cryptographic Hardware and Embedded Systems-CHES 2002. Springer Berlin Heidelberg, 2003.

[2] G. Camurati, A. Francillon, and F.-X. Standaert, *Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks*. In Cryptographic Hardware and Embedded Systems-CHES 2020; Springer, 2020.

[3] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues, et al., *Whispering devices: A survey on how side-channels lead to compromised information*. Journal Hardware and Systems Security, vol. 5, no. 2, pp. 143-168, 2021.

[4] J. van Woudenberg and C. O'Flynn, *The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks*, 2021.

[5] G. Camurati and A. Francillon, *Noise-SDR: Arbitrary modulation of electromagnetic noise from unprivileged software and its impact on emission security*. 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022.