Information Leakage Attacks on Air-Gapped Systems Using Inaudible-Band Multi-Element Encoding*

Ye-Rim Jeong, Yeon-Jin Kim and Il-Gu Lee†

Sungshin Women's University, Seoul, Korea
{220254016, 220246046, iglee}@sungshin.ac.kr

Abstract

Air-gapped systems are security architectures that protect sensitive data by physically isolating internal networks from external ones. To strengthen the security of air-gapped systems, systematic research into air-gap attack techniques is required so that diverse attack vectors can be understood and appropriate countermeasures developed. Conventional air-gap attacks that exploit electromagnetic emissions or optical channels tend to be relatively conspicuous, increasing the likelihood that users will detect the attack. In this paper, we propose an air-gap exfiltration technique that leverages the frequency and amplitude characteristics of signals in an inaudible frequency band. The proposed method employs frequencies outside the audible range to reduce perceptibility and exploits multiple signal attributes of frequency to increase the information throughput per unit time. Experimental results show that the proposed model can increase the data throughput per unit by up to approximately threefold compared with prior models. These findings provide a basis for developing future detection strategies against air-gap threats.

1 Introduction

Over the past few years, as dependence on the Internet has increased, cyberattacks have manifested in various forms such as viruses, worms, and ransomware[1]. Consequently, air-gapped systems have been employed as a primary security measure to protect classified information within states and industries by preventing cyberattacks in advance[2]. An air-gapped system is a security architecture that protects sensitive data by physically isolating an internal network from external networks; it is widely used in environments that require high levels of protection, such as national critical infrastructure and military systems[3]. However, recent research has demonstrated attack techniques that exploit peripheral components—such as computer hardware or IoT(Internet of Things) devices—to exfiltrate sensitive data from air-gapped environments via covert channels, suggesting that air-gapped systems are no longer intrinsically safe[4]. Indeed, in 2010 the Iranian nuclear facility was compromised by the Stuxnet malware[5]; in 2014 a South Korean hydroelectric research institute was hacked, and in

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec' 25), Article No. W6, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

† Corresponding author

2016 the Republic of Korea Ministry of National Defense suffered a breach[6]. Numerous cyber incidents against air-gapped systems in different countries have thus been reported. Covert-channel based data exfiltration is often difficult to detect using traditional network-based security solutions such as IDS(intrusion Detection Systems), IPS(intrusion Prevention Systems), and firewalls[7]. Therefore, to enhance the security of air-gapped systems, systematic research on air-gap attack techniques is required so that diverse attack vectors can be understood and appropriate countermeasures developed.

Conventional air-gap attacks that exploit physical channels such as optical or electromagnetic emissions suffer from the limitation of being conspicuous or readily detectable[8]. In this paper, we propose a data-exfiltration method that transmits binary information using frequency bands that are difficult for human hearing to perceive. The proposed technique encodes data in the frequency or amplitude of high-frequency signals outside the audible range, enabling efficient data transmission while reducing the likelihood of human detection.

The contributions of this paper are as follows.

- We propose a covert-channel air-gap attack mechanism that encodes binary data in an inaudible high-frequency band.
- We experimentally demonstrate the effectiveness and feasibility of a multi-element encoding scheme that concurrently exploits both the amplitude and frequency of high-frequency signals.

The remainder of this paper is organized as follows. Section 2 presents the proposed information-leakage method based on the frequency and amplitude of high-frequency signals. Section 3 analyzes the performance evaluation results. Section 4 concludes the paper and discusses directions for future work.

2 Proposed model

Figure 1 illustrates the overall workflow of the proposed method. First, the attacker injects malware into the air-gapped system. The malware selectively collects target data such as files, clipboard contents, and keystroke logs; the collected data are preprocessed and converted into a binary bitstream. The preprocessing stage inserts error-detection or correction information, such as checksums or forward error correction (FEC) codes.

To overcome the throughput limitations of conventional single-element encoding schemes, this study proposes a multi-element encoding technique that simultaneously exploits signal amplitude and symbol duration. The proposed method is designed to transmit more bits in parallel while operating in the same frequency band as single-element schemes. Each transmission symbol is composed of two independent attributes — the signal amplitude and the symbol duration — and each attribute is mapped to a single bit. The binary data collected by the malware are converted into a transmit waveform through amplitude-based encoding and symbol-based encoding stages. In the amplitude-encoding stage, amplitudes at or below a predefined threshold are mapped to bit ‘0’, and amplitudes above the threshold are mapped to bit ‘1’. In the symbol-encoding stage, symbol durations shorter than a threshold are mapped to bit ‘0’, and longer durations are mapped to bit ‘1’. If required, multi-level amplitude and duration encodings may be introduced to increase the number of bits conveyed per symbol. The choice of frequency band and the setting of thresholds are determined based on the characteristics of the real deployment environment, taking into account factors such as the background noise spectrum, the frequency response of the transmitter (speaker), and the microphone bandwidth and sensitivity of the receiver. Prior to transmission, the attacker performs a scanning phase to measure the ambient noise level and the signal-to-noise ratio (SNR) across frequencies in the target environment; these measurements are used to select a reliable high-frequency band and to determine appropriate thresholds and symbol-duration ranges.

When data transmission begins, the encoded signal is modulated into an inaudible high-frequency band (18–22 kHz) that is difficult for humans to perceive and emitted through the computer's speaker. The transmitted waveform includes a preamble and synchronization patterns so that the receiver can accurately detect the start of the data stream. From outside the air-gapped network, the attacker records the signal using a portable device such as a smartphone or smartwatch; the recorded audio file is then processed automatically and decoded to recover the original binary data. The decoding pipeline sequentially performs preamble-based synchronization, amplitude and symbol-duration discrimination, FEC decoding, and checksum verification.

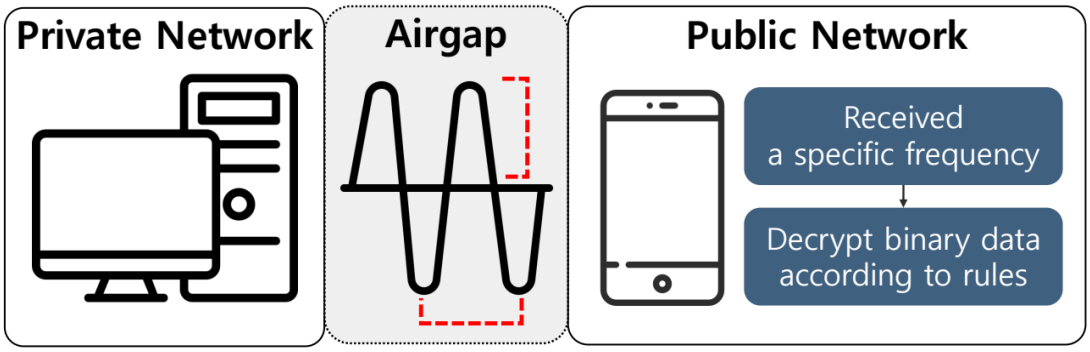

Figure 1: Attack Method Using Inaudible Frequency-Band Signals

The proposed method employs frequencies outside the human audible range, making the attack difficult for ordinary users to perceive. By simultaneously exploiting multiple signal attributes such as amplitude and symbol duration, the scheme increases the amount of information transmitted per unit time, enabling the exfiltration of large volumes of data in a single transmission.

3 Evaluation Result and Analysis

The experiments used a Samsung Galaxy Book Pro laptop as the transmitter system, with the laptop's built in speakers serving as the transmitter. A Samsung Galaxy S25 smartphone internal microphone was used to record the transmitted signal. The transmitter to receiver distance was increased from 1 m to 10 m in 1 m increments, and at each distance we measured the data transmission success rate and throughput. All experiments were conducted in an indoor environment with background noise levels of approximately 25 to 35dB. Recorded audio was initially saved in m4a format and then converted to wav files for analysis. We performed frequency analysis based on the Short Time Fourier Transform to extract frequency and symbol duration. Using these data, an automated decoding algorithm was applied to recover the transmitted bitstream.

The encoding parameters were as follows. For frequency based encoding, an 18 kHz signal represented bit 0 and a 22 kHz signal represented bit 1. For symbol based encoding, a symbol duration of 20ms or less was mapped to bit 0, and a duration greater than 20ms was mapped to bit 1. The transmitted payload consisted of the word "hello" repeated continuously, and a preamble pattern was inserted to enable accurate detection of the exact start of each data frame. To validate the performance of the proposed method, we compared it with a conventional single element encoding model that uses only the frequency element.

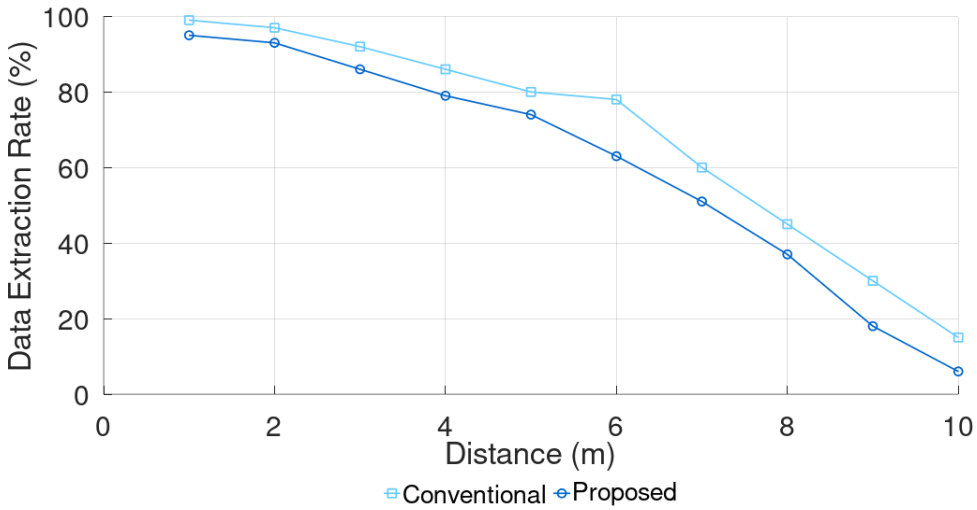

Figure 2: Data extraction success rate by distance

Figure 2 shows the data extraction success rate as a function of the distance between transmitter and receiver. The experimental results indicate that the proposed model exhibited, on average, an approximately 8% lower data extraction success rate than the conventional model. This reduction can be attributed to the need to recover multiple elements simultaneously; the proposed scheme is therefore more sensitive to background noise and signal distortion, which partially degrades recovery stability. However, this loss should be regarded as a trade-off for increased transmission efficiency rather than an overall performance degradation..

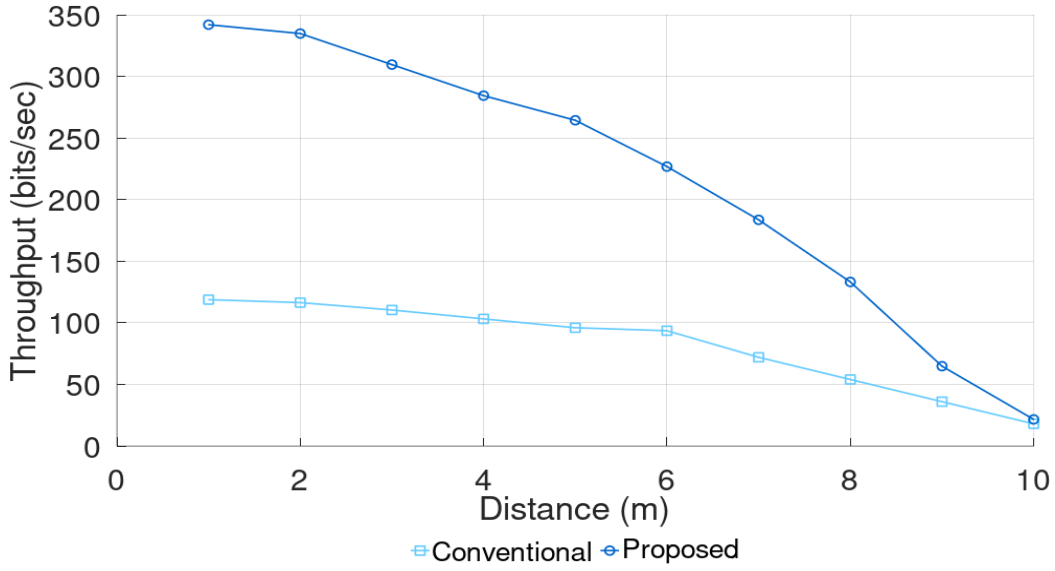

Figure 3: Throughput by distance

The variation in throughput with respect to distance is shown in Figure 3. Throughput was calculated using Equation (1).

$$Throughput = \frac{Number\ of\ Successfully\ Transmitted\ bits}{Transmission\ Time} \quad (1)$$

The experimental results indicate that, although the proposed model achieved a slightly lower data extraction success rate than the conventional model, it delivered significantly higher data throughput per unit time. The proposed model attained a maximum throughput improvement of 223.2 bits/s and an average improvement of approximately 134.66 bits/s. Unlike the conventional model, which relies on a single frequency element, the proposed scheme encodes data by exploiting multiple frequency- and signal-level elements concurrently, allowing more information to be transmitted in parallel within the same time interval. These findings demonstrate that the proposed technique can operate as an efficient and feasible data-exfiltration channel in real-world environments and reveal a novel security vulnerability in air-gapped systems..

4 Conclusion

Deploying air-gapped systems is recommended to protect critical data in government and industry and to resist the harms of cyberattacks. However, research exploiting various physical signals of air-gapped systems for data exfiltration has been actively advancing, undermining the presumed security of such systems. Because these covert-channel attacks are difficult to detect with traditional network-based security solutions, systematic study of air-gap attack techniques is needed to understand diverse attack vectors and to develop appropriate countermeasures.

Conventional air-gap attacks that exploit physical channels such as optical or vibration-based mechanisms are often visible or otherwise readily detectable, giving users a chance to notice the attack. To address this limitation, this paper proposes an air-gap exfiltration technique that leverages the frequency and amplitude of high-frequency signals. The proposed method uses frequencies outside the human audible range to reduce perceptibility and simultaneously exploits multiple signal attributes to increase the information transmitted per unit time, enabling the exfiltration of large volumes of data in a single transmission. Experimental results show that the proposed model increased the information throughput per unit time by up to 287.88% compared with the conventional model. In future work, we plan to apply error-correcting codes to develop a noise-robust, signal-based covert-channel technique.

Acknowledgments This work is supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry [grant number RS-2024-00415520] supervised by the Korea Institute for Advancement of Technology (KIAT), the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program [grant number IITP-2022-RS-2022-00156310] and National Research Foundation of Korea (NRF) grant [RS-2025-00518150], and the Information Security Core Technology Development program [grant number RS-2024-00437252] supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

References

[1] Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." Energy Reports 7 (2021): p. 8176-8186.

[2] Vähäkainu, Petri, Martti Lehto, and Antti Kariluoto. "Cyberattacks against critical infrastructure facilities and corresponding countermeasures." *Cyber Security: Critical Infrastructure Protection*. Cham: Springer International Publishing, 2022. pp.255-292.

[3] Na, Mohan Rajkumar, and K. B. Sundharakumar. "A study on air-gap networks." *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)*. IEEE, 2024. pp.1-6

[4] Kim, Yeon-Jin, Na-Eun Park, and Il-Gu Lee. "Air-Fuzz: Feasibility Analysis of Fuzzing-Based Side-Channel Information Leakage Attack in Air-Gapped Networks." *International Conference on Information Security Applications*. Singapore: Springer Nature Singapore, 2024. pp.231-242

[5] Abbas, Syed Qandil, and Hareem Fatima. "Cyber Security Threats to Iran and its Countermeasures: Defensive and Offensive Cyber Strategies." *Journal of Research in Social Sciences* 12.2 (2024): p. 1-21.

[6] Lee, Jieun, et al. "Optical air-gap attacks: analysis and IoT threat implications." *IEEE Network* 38.6 (2024): pp. 342-352.

[7] Naz, Mohammad Tazeem, and Ahmed M. Zeki. "A review of various attack methods on air-gapped systems." 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT). IEEE, 2020. pp. 1-6.

[8] Guri, Mordechai. "Air-gap electromagnetic covert channel." *IEEE Transactions on Dependable and Secure Computing* 21.4 (2023): pp. 2127-2144.