TEMPEST-LoRa: Cross-Technology Covert Communication

Xieyang Sun
Xi'an Jiaotong University
Xi'an, China
xieyangsun@stu.xjtu.edu.cn

Yuanqing Zheng
The Hong Kong Polytechnic University
Hong Kong, China
csyqzheng@comp.polyu.edu.hk

Wei Xi*
Xi'an Jiaotong University
Xi'an, China
xiwei@xjtu.edu.cn

Zuhao Chen
Xi'an Jiaotong University
Xi'an, China
czh869452912@gmail.com

Zhizhen Chen
Xi'an Jiaotong University
Xi'an, China
zhizhenc@stu.xjtu.edu.cn

Han Hao
Xi'an Jiaotong University
Xi'an, China
haohan9717@stu.xjtu.edu.cn

Zhiping Jiang
Xidian University
Xi'an, China
zpj@xidian.edu.cn

Sheng Zhong
Nanjing University
Nanjing, China
zhongsheng@nju.edu.cn

Abstract

Electromagnetic (EM) covert channels pose significant threats to computer and communications security in air-gapped networks. Previous works exploit EM radiation from various components (*e.g.*, video cables, memory buses, CPUs) to secretly send sensitive information. These approaches typically require the attacker to deploy highly specialized receivers near the victim, which limits their real-world impact. This paper reports a new EM covert channel, TEMPEST-LoRa, that builds on Cross-Technology Covert Communication (CTCC), which could allow attackers to covertly transmit EM-modulated secret data from air-gapped networks to widely deployed operational LoRa receivers from afar. We reveal the potential risk and demonstrate the feasibility of CTCC by tackling practical challenges involved in manipulating video cables to precisely generate the EM leakage that could readily be received by third-party commercial LoRa nodes/gateways. Experiment results show that attackers can reliably decode secret data modulated by the EM leakage from a video cable at a maximum distance of 87.5m or a rate of 21.6 kbps. We note that the secret data transmission can be performed with monitors turned off (therefore covertly).

CCS Concepts

• **Security and privacy → Side-channel analysis and countermeasures**.

*Wei Xi is the corresponding author.

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3744817

Keywords

TEMPEST, electromagnetic side channel, LoRa, covert communication, air-gapped systems, cross-technology communication

ACM Reference Format:
Xieyang Sun, Yuanqing Zheng, Wei Xi, Zuhao Chen, Zhizhen Chen, Han Hao, Zhiping Jiang, and Sheng Zhong. 2025. TEMPEST-LoRa: Cross-Technology Covert Communication. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3719027.3744817

1 Introduction

Physically isolated (air-gapped) networks are among the most effective ways of enhancing the computer and communications security against real-world attacks [33, 56] in industry, business, finance, and medical sectors. Electromagnetic (EM) covert channels, however, pose serious threats to the physically isolated networks [18, 35]. Previous research has demonstrated that implanted malware can manipulate electromagnetic radiation (EMR) of computer components (such as DRAM [19, 59], USB [22]), thereby covertly modulating and exfiltrating confidential data to covert receivers. The EM covert channels can bypass the air-gapped systems independently of traditional communication channels (*e.g.*, Internet, WiFi, Bluetooth, *etc*). Constrained by the emission characteristics (*e.g.*, ultra-low power of EMR, EM modulation fidelity and resolution, and data rate), existing covert channel attacks typically require very short communication ranges (*e.g.*, <10m) and necessitate the physical deployment of highly specialized bulky receivers (*e.g.*, high-end software defined radios) close to the isolated networks, which practically limit their risks and real-world implications so far.

In this paper, we reveal a new risk of EM covert channels, which could allow attackers to exploit existing operational LoRa (Long Range Radio [40]) nodes/gateways widely deployed worldwide to receive secret data leaked from air-gapped networks at much greater distances and higher data rates. Some third-party LoRa devices are freely accessible to attackers across the globe. To demonstrate the

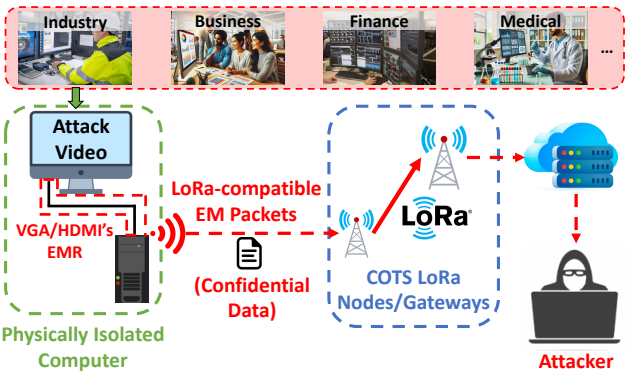


Figure 1: TEMPEST-LoRa reveals the risk of a new cross-technology covert communication attack, where attackers can manipulate video cables to generate LoRa-compatible EM packets, which can be received and processed by operational LoRa nodes/gateways widely deployed worldwide.

feasibility of such cross-technology (*i.e.*, EMR to LoRa) covert communication (CTCC), we develop TEMPEST-LoRa, which modulates EMR from video cables (VGA or HDMI) and thereby generates EMR-modulated LoRa packets. By doing so, attackers can leverage Commercial Off-The-Shelf (COTS) LoRa gateways as receivers to covertly receive secret data as depicted in Figure 1. Unlike previous work that necessitates close proximity from the EMR sources, the LoRa-like EMR signals can penetrate a few concrete walls and retain a sufficiently high signal strength over long propagation distances thanks to the unique noise-resilience feature of LoRa modulation and the high sensitivity of LoRa receivers [64].

We demonstrate that realizing this new type of covert communication, though challenging, is indeed possible for attackers at a very low attack launching cost and has a substantial security implication. To generate LoRa-compatible EMR signals with video cables, attackers must accurately modulate the EM leakage, which requires a new technical design. Although previous studies [20, 21, 30, 63] have investigated the problem of generating the EMR by manipulating video cables, the modulation fidelity and resolution of existing works fall short in supporting the cross-technology covert communication with commercial wireless protocols such as LoRa.

We revisit the EMR model of video cables and develop a novel fine-grained pixel-level EM modulation method. In particular, we repurpose a video cable as a direct radio-frequency (RF) sampling transmitter, enabling high-fidelity modulation up to the pixel clock (PC) frequency. With this new EMR control technology, a curated attack image can cause variations of electronic signals over the video cable to generate EMR at different frequencies. However, the PC frequency is typically much lower than the wireless frequency of LoRa gateways (*e.g.*, 915 MHz in US). To address this problem, we exploit the harmonics of EMR and shift the frequencies to the target LoRa band, making the EM packets readily decodable by operational LoRa nodes/gateways, widely deployed and freely accessible to attackers worldwide.

To ensure covertness during the secret data transmission, we also study how to achieve visual invisibility on the victim's monitor. We find that by modifying the power management interface of the monitor using DDCcontrol [4], attackers can deactivate the monitors while keeping the video cables active and continuously emitting EM packets. This could allow attackers to covertly send the secret data with a black display on the screen.

This paper makes the following key contributions:

- We develop a fine-grained pixel-level EMR modulation technique that transforms a video cable into a direct RF sampling transmitter, enabling attackers to generate protocol-compatible EMR signals for cross-technology covert communication with wireless protocols such as LoRa.
- We reveal the risk of a new type of covert channel from EMR to operational LoRa devices. Unlike previous works, this new covert channel poses a unique threat to air-gapped networks, since LoRa-compatible EM packets can penetrate thick concrete-walls over long attacking ranges and be directly received by LoRa nodes/gateways deployed worldwide.
- We prototype TEMPEST-LoRa and evaluate the performance in various practical settings. Our experiment results with both VGA and HDMI cables show that TEMPEST-LoRa can covertly transmit secret data to COTS LoRa nodes or gateways at a maximum rate of 21.6 bps or up to 87.5m away, and even further to low-cost software-defined radios (SDR) such as HackRF One with customized EM packets.

2 Related Work

TEMPEST (Transient ElectroMagnetic Pulse Emanation STandard [70]) was established by the NSA and NATO in response to the concerns about the acceptable level of EMR from computers. Van Eck [66] first demonstrated that attackers can recover the displayed content by analyzing the EMR of a TV. Such passive eavesdropping [23, 34, 45–47, 57] is collectively referred to as TEMPEST attacks. Soft-TEMPEST [30] extended this concept by actively generating controlled EM emissions through software-layer operation. For example, by displaying carefully crafted black-white images on a monitor, the video cable can emit signals at specific frequencies.

EM covert channels [18, 32] are designed to modulate the EMR emitted from electronic devices to exfiltrate confidential information, without relying on conventional communication media (WiFi, Bluetooth, Internet, *etc*). Previous works explored various manipulable leakage sources as summarized in Table 1. GSMem [19] manipulates the EM emission of the memory bus (DRAM) using specific memory-related CPU instructions, modulating secret data using Binary Amplitude Shift Keying (B-ASK) and sending it to a nearby (within 5.5m) spy phone with a rootkit implanted in its baseband firmware. BitJabber [75] improves the data rates of the DRAM-related EM covert channel, achieving a throughput of 100-300 kbps within a 3m distance (its modulation methods include Binary Frequency Shift Keying and Multiple Frequency Shift Keying). Noise-SDR [5] focuses on the customizability of DRAM's EMR using Radio-Frequency Pulse-Width Modulation (RF-PWM), and demonstrates receiving EM emission signals with multiple modulation modes on a USRP B210. Air-Fi [17] manipulates DRAM to emit binary data modulated with On-Off Keying (OOK modulation) on the 2.4 GHz band, requiring prior modifications for the WiFi adapter's

Table 1: TEMPEST-LoRa v.s. other works.

Method	Leak source	Range	Speed	Receiver
GSMem [19]	DRAM	1-5.5m	100-1kbps	Phone w/ modified firmware
BitJabber [75]	DRAM	<3m	100k-300kbps	SDR
NoiseSDR [5]	DRAM	<5m	11.2-2.56kbps	SDR
Air-Fi [17]	DRAM	2.1-8m	1-16bps	WiFi w/ modified firmware
TEMPEST for Eliza [63]	Video Cable	<5m	unknown	AM radio
AirHopper [20]	Video Cable	7-22m	100-480bps	Phone w/ FM radio
SideComm [11] (Cross-LoRa)	Processors	10-15m	1kbps	SDR
EMLoRa [59] (Cross-LoRa)	DRAM	40-137m	1.25-14bps	SDR
TEMPEST-LoRa (Cross-LoRa)	Video Cable	40-132m	180-21.6kbps	**COTS LoRa node/gateway or SDR**

driver and firmware. 'TEMPEST for Eliza' [63] demonstrated that crafted screen images can generate intentional EM emission from VGA cables. While initially designed to transmit AM-modulated music via VGA cable's EMR, it provided foundational insights into image-based EMR signal modulation. AirHopper [20] encodes data into Frequency-Modulation (FM) radio signals by manipulating VGA or HDMI cable's EMR via crafted screen images, using Audio Frequency-Shift Keying (A-FSK) or Dual-Tone Multiple-Frequency (DTMF) audio modulation to transmit data to nearby smartphones with FM receivers. SideComm [11] and EMLoRa [59] are recent advances in cross-LoRa side-channel communication. EMLoRa is the first study to integrate the DRAM's EMR with CSS modulation, significantly extending the attack range, albeit at the cost of low transmission speeds. SideComm focuses on using processors' EMR to provide additional wireless communication capabilities for low-power IoT devices. However, due to the limited EMR modulation capability (e.g., DRAM's EMR frequency cannot be modulated to the LoRa bands), the system implementations in all the above studies rely on specialized receivers such as SDRs.

Cross-technology communication (CTC) aims to achieve transparent transmission between incompatible wireless communication devices / protocols without the need for additional radio modules. Examples include WEBee [42] (WiFi to ZigBee), Bluebee [25] (BLE to ZigBee), BlueFi [6] (BLE to WiFi), L2X [65] and ZIMO [74], which achieve CTC between different IoT connectivity technologies. Similarly, cross-LoRa studies such as LoRaBee [60] (LoRa to ZigBee), BLE2LoRa [41] (BLE to LoRa), WiRa and Wi-Lo [15, 71] (WiFi to LoRa) facilitate interactions between LoRa and other wireless systems.

In contrast, TEMPEST-LoRa enables attackers to receive secret data through COTS LoRa nodes or gateways, outperforming most previous EM covert channels in both attack distance and data rates. To our knowledge, TEMPEST-LoRa is the first to integrate traditional CTC techniques with EM covert channels, achieving full compatibility of EMR with commercial wireless protocols.

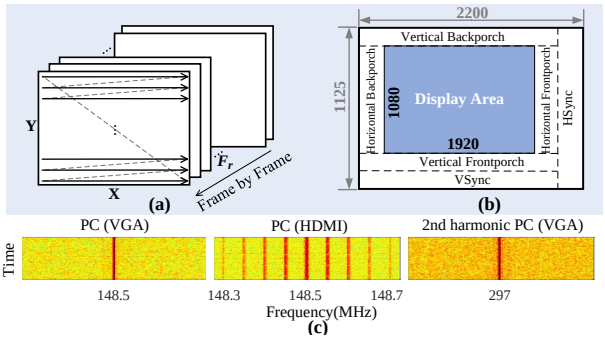


Figure 2: (a) Monitor's line-by-line scanning manner. (b) The screen consists of a display area and some 'hidden pixels'. (c) EMR of video cables at PC frequency and harmonics.

3 Overview

3.1 Background

EM leakage of video cable. Monitors display images through a process of scanning and refreshing pixels. As depicted in Figure 2 (a), when an image is transmitted to the monitor through a video cable, the monitor displays the pixels line-by-line from the top-left to the bottom-right corner and refreshes the entire screen at a frame rate F_r. Additionally, it includes a hidden display area at the edge of the screen, which is used for pixel synchronization and blanking [37], as shown in Figure 2 (b).

Suppose each frame contains Y scanlines, with each scanline consisting of X pixels. The duration of one pixel T_p is:

$$T_p = \frac{1}{X \cdot Y \cdot F_r} \tag{1}$$

While the monitor is in operation, the video cable will emit EMR at the Pixel Clock (PC) frequency and its harmonics as shown in Figure 2 (c) (these EMR spectra were captured while the monitor was displaying a black image). The value of PC can be calculated as:

$$PC = \frac{1}{T_p} \tag{2}$$

In this paper, we take the typical 1080X1920@60Hz display setting as a representative case for analysis. This setting corresponds to 1125 vertical lines and 2200 horizontal pixels per line, resulting in PC of 148.5 MHz [2]. In addition, because the HDMI employs Transition Minimize Differential Signaling (TMDS) [10] for pixel encoding, HDMI's leakage spectrum contains more frequency components [36].

LoRa physical layer. LoRa features long-range, low-power and high-sensitivity communication, which has been widely deployed all around the world to support various Internet of Things (IoT) applications [26] such as environment monitoring, pet tracking, logistics and so on [72, 73].

CSS modulation: LoRa's physical layer employs Chirp Spread Spectrum (CSS) modulation. A basic up-chirp (as shown in Figure 3 (a)) whose bandwidth spans from $-\frac{BW}{2}$ to $\frac{BW}{2}$ can be represented as:

$$Upchirp(t) = e^{j2\pi t(-\frac{BW}{2}+\frac{BW}{2T}t)} \tag{3}$$

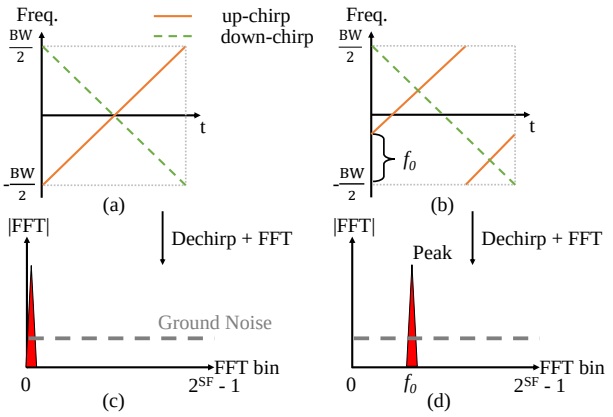


Figure 3: (a) Basic up-chirp and basic down-chirp. (b) An up-chirp with f_0 shifting. (c) Demodulation for the basic up-chirp. (d) Demodulation for the up-chirp with f_0 shifting.

where T denotes chirp duration. CSS modulates symbols by cyclically shifting the initial frequency f_0 as illustrated in Figure 3 (b):

$$y_e = Upchirp(t)e^{j2\pi f_0 t} \tag{4}$$

within the BW range, up-chirps that commence at distinct initial frequencies are mapped to unique symbols. In the LoRa standard, BW is partitioned into 2^{SF} distinct initial frequencies to encode SF-bits of data, where SF refers to the *spreading factor*. The most prevalent BW values for COTS LoRa are 125 kHz, 250 kHz, and 500 kHz, with SF varying from 6 to 12.

For demodulation, a LoRa receiver accumulates energy through coherent de-spreading. The coherent signal down-chirp can be expressed as $Downchirp(t) = e^{j2\pi t(\frac{BW}{2} - \frac{BW}{2T}t)}$. By utilizing the coherence of up-chirp and down-chirp, the result of multiplying the modulated up-chirp and the basic down-chirp is a single-frequency signal:

$$Dechirp(t) = y_e \cdot Downchirp(t) = e^{j2\pi f_0 t} \tag{5}$$

Next, the receiver performs a Fast Fourier Transform (FFT) on $Dechirp(t)$, producing a power peak at frequency f_0. The index of this peak corresponds to the initial frequency of the coded symbol, as shown in Figure 3 (d).

In this paper, similar to the Signal-to-Noise Ratio (SNR), we define the dechirp-to-noise ratio (DNR) to quantify the signal quality of the demodulated chirp signal:

$$DNR = 20 \cdot \lg \frac{Peak}{Noise} \tag{6}$$

where $Peak$ is the peak value of the dechirp + FFT, and $Noise$ is the noise level. A higher DNR indicates superior signal quality.

3.2 Attack Model

Victim: We assume that the target is a computer storing confidential data of interest to the attacker, typically located in high-security environments such as isolated internal networks. To protect against cyber-attacks, the victim's air-gapped computers have removed conventional communication modules (*e.g.*, Wi-Fi, Bluetooth, and Ethernet). The victim's computer only retains essential components, including the host and the monitor with a VGA or HDMI cable.

LoRa technology has been widely deployed in both indoor and outdoor IoT scenarios for data transmission [28], environmental sensing [9], industry control [39], *etc.* We assume the presence of LoRa nodes or gateways near the victim. This assumption is based on the fact that real-world standards for constructing air-gapped networks in various critical infrastructures, such as governments [3, 13, 53, 58], the European Union [49, 50, 67, 76], businesses [8, 31], industry [27, 38, 62], medical [1], and military sectors [7], primarily focus on strictly disconnecting the external communication interfaces on air-gapped computers. These air-gapped systems have not yet delineated essential procedures for the elimination or segregation of commercial wireless devices within their vicinity (*e.g.*, around 100m).

Attacker: Consistent with previous EM covert channels [18], we assume that an attacker has implanted malware carrying TEMPEST-LoRa on the victim's computer through supply-chain attacks [12, 33, 52, 56] or social engineering tactics [29, 68]. Once implanted, the malware scans the computer to locate confidential files and encrypts the secret data using the attacker's private key to ensure confidentiality. The attacker then covertly generates and plays an attack video when the computer is ensured to be unattended (such as in standby mode). The malware can obtain the resolution and refresh rate of the victim's monitor (*e.g.*, 'xrandr' command in Linux) and generate the corresponding attack video.

For the receiving end, TEMPEST-LoRa considers two possible approaches:

Approach 1: Receiving via operational COTS LoRa Gateways/Nodes. The attackers can deploy their own COTS LoRa nodes or gateways near the air-gapped systems, or leverage third-party operational LoRa gateways deployed worldwide to receive EM packets.

Subsequently, as shown in Figure 1, the EM packets carrying sensitive data are transmitted to nearby LoRa gateways. The (third-party) LoRa receivers can then forward the LoRa packet to the attacker's application server in the cloud. A unique feature of TEMPEST-LoRa is its fine-grained control of EMR signals, which allows TEMPEST-LoRa to generate EM packets compatible with all LoRa packet configurations (all combinations of BWs and SFs). Thus, all deployed COTS LoRa devices could potentially receive and relay the covert packets with suitable parameter configurations to attackers worldwide.

Approach 2: Receiving with SDR on Flexible Spectrum. Similarly to previous EM covert channels [59], attackers can also use low-cost SDRs (*e.g.*, HackRF) to receive EM packets. TEMPEST-LoRa has a strong frequency-modulation capability for EMR (within 10 MHz to 1000 MHz). We demonstrate that attackers can select less-crowded frequency bands and customize LoRa-like (but different) EM packets to achieve even longer attack distances at higher data rates than LoRa-compatible EM packets.

Visual covertness: To ensure visual covertness, we assume attackers can use DDCcontrol [4] to turn off the screen and keep the video cable continuously emitting EM packets. Specifically, attackers can first use *ddccontrol -p* command to obtain the device code of the monitor, such as *dev:/dev/i2c-3*. Subsequently, the attackers can modify the 0xe1 register address of the monitor to '1' to turn off

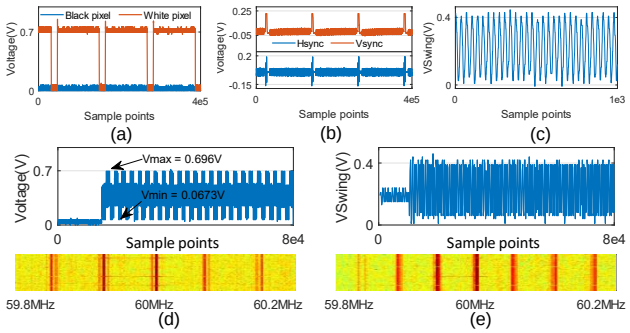


Figure 4: (a). Voltage of VGA's blue bus when transmitting black/white pixels. (b). Voltage of VGA's Hsync and Ysync buses. (c). The voltage swing of HDMI's clock bus. (d) and (e). Voltage of VGA's blue bus and Voltage swing of HDMI's DATA1+- buses when displaying a 60 MHz attack image and their EMR spectra.

the screen: *ddccontrol -r 0xe1 dev:/dev/i2c-3 -w 1*. The 0xe1 address corresponds to the power supply status. When the value of 0xe1 is modified to 1, it prevents the monitor from refreshing the screen and shows a black-screen, while keeping the video cable transmitting the pixel stream and emitting EM packets. This capability enables attackers to launch covert transmissions during periods of inactivity, such as after office hours or when the system is left unattended.

4 TEMPEST-LoRa

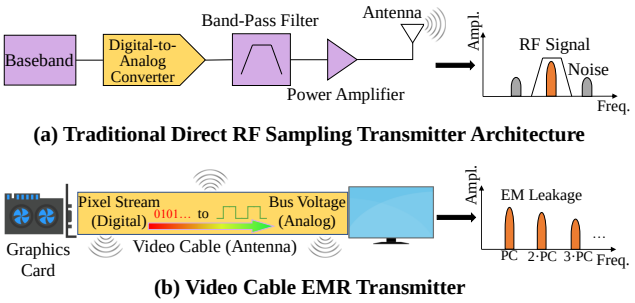
This section presents the technical details of TEMPEST-LoRa. First, we discuss the EMR model of video cables and how to manipulate the EMR through customized attack images. Second, we elaborate how to construct EM packets compatible with the LoRa protocol, which can be directly received by operational COTS LoRa devices; and then, we present an enhanced version with low-cost SDRs.

4.1 Video Cable EMR Transmitter

We focus on the EMR inherently caused by the voltage fluctuations on video cables (VGA and HDMI). These fluctuations mainly stem from the operation of data buses responsible for transmitting pixel information and the clock buses that ensure synchronization.

VGA uses [R,G,B] data buses to transmit red, green and blue pixels in the form of analog signals, and HDMI has three pairs of differential data buses (DATA0+-, DATA1+-, and DATA2+-) for pixel transmission with digital signals. For clock synchronization, VGA's VSync and HSync buses are used for vertical and horizontal pixel synchronization, respectively, while HDMI employs a pair of independent clock+- differential buses.

To visualize the relationship between EMR and various bus activities, we use an oscilloscope (RIGOL Oscilloscope MSO5000) to measure the voltage waveforms of the data buses and clock buses of VGA and HDMI. It should be noted that when transmitting black [0,0,0] or white [1,1,1] pixels, VGA's R, G, and B buses exhibit identical voltage waveforms; The same applies to HDMI's three pair of differential data buses (DATA0+-, DATA1+-, and DATA2+-). Figure 4 (a) illustrates the voltage waveforms on the Blue bus when



(a) Traditional Direct RF Sampling Transmitter Architecture

(b) Video Cable EMR Transmitter

Figure 5: Contrast of direct RF sampling transmitter architecture and video cable EMR transmitter.

transmitting 3 rows of black or white pixels, respectively. When scanning to the Porch and Sync areas, the voltage of the data bus is 0V (same as the voltage of the black pixel). Figure 4 (b) is the voltage waveforms of VGA's Vsync and Hsync buses, and Figure 4 (c) is the voltage waveform of the clock bus of HDMI. Since the bus speeds of the data buses and clock buses are both equal to the Pixel Clock (PC) frequency, the EMR frequencies of the VGA and HDMI cables are mainly concentrated at *PC and its harmonics* as shown in Figure 2 (c).

Modeling: We model the EMR according to their sources as follows:

$$S_{sum} = S_{color} + S_{sync} + S_{other} \tag{7}$$

where S_{color} is the aggregate EMR of all data buses that transmit pixel colors, S_{sync} is the sum of the EMR of clock buses, and S_{other} is the EMR collection of other sources (such as the GND bus). We further measure the voltage waveforms of other buses and confirm that the EMR signals come mainly from S_{color} and S_{sync}, so we ignore S_{other} in subsequent analysis.

Fine-grained control over the EMR source is essential to establish an EM covert channel. S_{sync} comes from the clock bus that cannot be manipulated and constantly appears at the PC and its harmonics. In contrast, S_{color}, which comes from the data bus that transmits image information, is adjustable. Next, we focus on designing the pixel stream of attack images to modulate the EMR of S_{color}.

Video cable EMR transmitter: From the radio-frequency (RF) transmitter perspective, the principle of EMR is similar to that of a 'direct RF sampling transmitter' (a typical RF hardware architecture that directly digitizes high-frequency RF signals [61]). Specifically, during the transmission of image data from the graphics card to the monitor via the video cable, the digital pixel stream is converted to the analog voltage, and the color of pixel determines the voltage level on the data bus (*i.e.*, the pixel stream corresponds to the baseband of the video cable). This conversion process from the pixel stream to the bus voltage largely fulfills the functionality of the Digital-to-Analog Converter (DAC) module in a direct RF sampling transmitter that converts the digital signal from the baseband to an analog signal, as shown in Figure 5 (a). The video cable EMR transmitter operates at a sampling rate of PC, and the emitted EMR is directly determined by the frequency components of the voltages on the cable's buses, with the cable itself serving as the antenna. The difference is that the band-pass filter in the direct RF sampling transmitter can filter out noise outside the desired frequency

Algorithm 1 Algorithm for designing attack image

```
1:  Input: Expected attack frequencies {f_1, f_2, ..., f_n}, pixel duration of each frequency {t_1, t_2, ..., t_n}, pixel clock PC
2:  Timer = 1;
3:  PixelStream = [];
4:  for k = 1 to n do
5:      for i = 1 to t_k do
6:          DownSampRate = mod(f_k, PC)/PC;
7:          Val = sin(2.0 · π · DownSampRate · Timer);
8:          if Val > 0 then
9:              PixelStream(Timer) = 1; // White pixel
10:         else
11:             PixelStream(Timer) = 0; // Black pixel
12:         end if
13:         Timer++;
14:     end for
15: end for
16: PixelStream = [PixelStream FramePadding];
17: Image = reshape(PixelStream, ScreenH, ScreenW);
18: Save2Image(Image[DisplayArea]);
```

band, and the power amplifier can boost the power of the RF signal. In contrast, the video cable EMR transmitter lacks such filtering, resulting in EMR at multiple harmonic frequencies of the PC, as illustrated in Figure 5 (b).

To actively manipulate the frequency of EMR, the key idea is to emulate down-sampling of the pixel rate S_{color} from PC to an expected frequency. Specifically, by carefully designing the pixel arrangement within the pixel stream to adjust the pixel frequency, the voltage frequency on the data bus can be indirectly modulated. When the frequency of bus voltage is the same as the expected EM leakage frequency, the video cable will emit EMR of the corresponding frequency. Algorithm 1 outlines the EMR frequency modulation process in the attack image.

Algorithm 1 is designed to generate an attack image that can manipulate the video cable sequentially to emit EMR at f_1 to f_n frequencies, with each frequency's emission lasting for $t_k \cdot T_p$. Lines 6 to 13 are the core of Algorithm 1. Line 6 calculates the ratio for downsampling S_{color} from the PC to f_k. The mod(f_k, PC) function serves to downsample the EMR harmonics when the expected frequency f_k exceeds PC. Lines 7 to 13 compute the pixel sequence required for the video cable to emit a single-frequency emission at f_k; here, white and black pixels are strategically utilized to alter the voltage waveform on the data buses. The benefit of using a black-white pattern is that it stimulates the cable to emit EM emission with maximum intensity. The sine function in Line 7 is an example of modulating the EMR into a sine wave (it can be modified to perform other modulation patterns). If the length of PixelStream is less than one frame, Line 16 fills the end with black pixels to make it a complete frame. Line 17 transforms the 1D PixelStream into a 2D attack image. For 1080x1920 resolution, the screen height *ScreenH* and width *ScreenW* equal 1125 pixels and 2220 pixels [2]. Line 18 selects the pixels of the Display Area (1080x1920) from the Image matrix (1125x2200) and saves as an attack image.

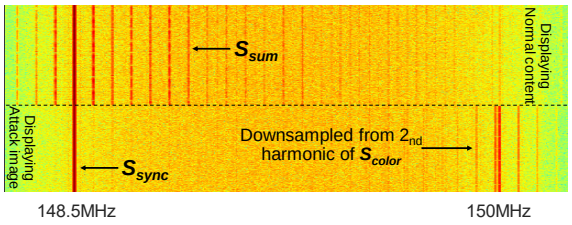


Figure 6: Comparison of HDMI's EMR spectrum: normal emission and 150 MHz intentional emission.

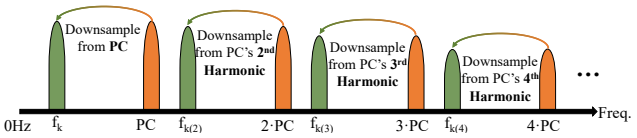


Figure 7: Emitting EMR at arbitrary frequency f_k by down-sampling PC or PC's $\lceil \frac{f_k}{PC} \rceil$-th harmonic.

Figures 4 (d) and (e) show examples of the voltage waveforms of the VGA and HDMI's data bus when the monitor displays a 60 MHz attack image. For the emission spectrum, since the waveform of the black-white pixel pattern is similar to a square wave, there are some frequency components near the expected frequency (the intensity of these components is always weaker than the expected frequency). These frequency components can be weakened by modifying Line 9 to Line 11 in Algorithm 1 to the grayscale value corresponding to *Val* (thus making the voltage waveform closer to a sine wave), but at the same time we find that the EMR intensity at the expected frequency f_k will also be weakened. Therefore, in practice, we still use the black-white pattern, focusing on the EMR at f_k and disregarding the lower intensity frequency components.

To illustrate how the attack image shifts the EMR's frequency, Figure 6 compares the HDMI leakage spectrum when no attack image is displayed and the 150 MHz attack image is displayed. The upper part is S_{sum} near the PC frequency (148.5 MHz), and the monitor displayed a web page at this time. When the 150 MHz attack image is displayed, only the S_{sync} leakage is left at the PC. The EMR that appears at 150 MHz is downsampled from the 2nd harmonic of S_{color} (297 MHz) to 150 MHz (at the same time, the fundamental band of S_{color} at 148.5 MHz is downsampled to 1.5 MHz). Building on this example, Figure 7 provides an abstract illustration of how EMR components at PC and its harmonics can be downsampled to an arbitrary target frequency f_k. When $f_k \in (0, \text{PC}]$, EMR is shifted from the PC frequency to f_k by a specially crafted pixel

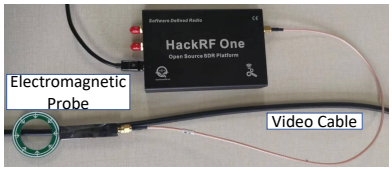


Figure 8: We use HackRF with an EM probe to measure the EMR intensity of VGA and HDMI.

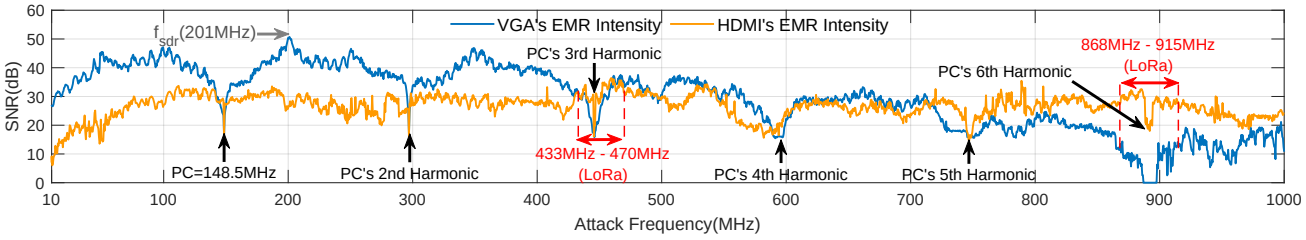


Figure 9: Actual EMR intensity of VGA and HDMI with attack frequencies from 10 MHz to 1000 MHz.

stream that forms a strong EM emission component at f_k. (from the perspective of the RF transmitter, it is equivalent to reducing the baseband rate from PC to f_k). When $f_k \in (\mathrm{PC}, +\infty)$, Algorithm 1 targets the manipulation of $\lceil \frac{f_k}{\mathrm{PC}} \rceil$-th harmonic of S_{color}.

Emission spectrum. The main operating frequency bands of LoRa include 433 MHz - 470 MHz and 868 MHz - 915 MHz, which are within the 3rd - 7th harmonic range of EMR. To verify that the video cable EMR transmitter has the capability to be frequency compatible with LoRa protocol, we measured the SNR of EMR from VGA and HDMI cables using a HackRF [14] with an electromagnetic probe as shown in Figure 8, and the probe was tightly attached to the video cable. In an electromagnetic darkroom, we create and display attack images on the monitor, configured at 1080x1920@60Hz, with attack frequencies sweeping from 10 MHz to 1000 MHz. Each attack image is designed to emit one single attack frequency, with a frequency interval of 0.5 MHz between adjacent attack images.

Figure 9 illustrates VGA and HDMI's EMR intensity at attack frequencies ranging from 10 MHz to 1000 MHz. It is evident that VGA demonstrates significantly higher leakage intensity than HDMI within the frequency band below the PC's 3rd harmonic (10 MHz - 445.5 MHz). In contrast, above the PC's 5th harmonic (742.5 MHz - 1000 MHz), HDMI shows a slightly higher intensity than VGA.

The disparity in EMR intensity between VGA and HDMI is due to their voltage ranges and pixel encoding methods. In the low-frequency band, the EMR intensity is mainly determined by the magnitude of cable voltage fluctuation. VGA operates within a voltage range of 0V to 0.7V, whereas HDMI has a voltage swing of 0.4V, hence VGA's EMR intensity is higher than that of HDMI below PC Hz. However, the black-white pixel stream drives the voltage waveform of VGA to approximate an ideal square wave, which more effectively concentrates the emission energy in the lower frequency band. Due to TMDS encoding, HDMI disperses part of its energy across frequencies other than the target attack frequency, resulting in a wider emission spectrum [51] and a more evenly distributed EMR intensity across the 10-1000 MHz range compared to VGA. In addition, we observed deviations between the actual bus voltage and the prescribed manufacturing standards. For example, when the monitor displays a 60 MHz attack image, the actual valley and peak voltages of the VGA are 0.0673V and 0.696V as illustrated in Figure 4 (d), which are not strictly equal to the specified 0V and 0.7V. We speculate that the alternating black-and-white pixel pattern leads to voltage overshoot and undershoot [44], which in turn results in fluctuations in emission intensity across various attack frequencies.

Although VGA and HDMI exhibit sufficient emission intensity to achieve frequency compatibility with LoRa bands (433-470 MHz and 868-915 MHz), the SNR significantly degrades near the PC frequency and its harmonics. This decline is mainly due to interference from the EMR of S_{sync}. Therefore, to maintain covert channel quality, attackers should avoid selecting frequencies close to the 3rd and 6th harmonics of the PC.

4.2 CTCC to LoRa

In this subsection, we present the methodology for constructing LoRa-compatible EM packets. Then, we explore strategies for performance enhancement that attackers could exploit with low-cost SDRs.

The core idea of modulating EMR into LoRa waveforms is to continuously shift the emission frequency in accordance with LoRa receiver's settings (SF and BW) at a selected LoRa frequency. This controlled frequency sweeping emulates the chirp signals used in LoRa modulation and enables the construction of LoRa-compatible EM packets.

Figure 10 (a) illustrates a standard LoRa packet configured with SF=8&BW=500kHz. The Preamble part comprises multiple consecutive basic up-chirps and helps the receiver detect the incoming signal and synchronize its timing; the SyncWord, made up of two up-chirps, serves to distinguish different LoRa networks; the Start Frame Delimiter (SFD) contains 2.25 basic down-chirps, which mark the beginning of the Payload part; finally, the Payload carries actual encoded data. To ensure that EM packets can be recognized and decoded by the COTS LoRa devices, the chirp duration and frequency band need to comply with LoRa standards.

Mapping chirp duration to pixel number. A LoRa chirp consists of 2^{SF} samples at a sampling rate of BW. Thus, the chirp duration can be calculated as follows:

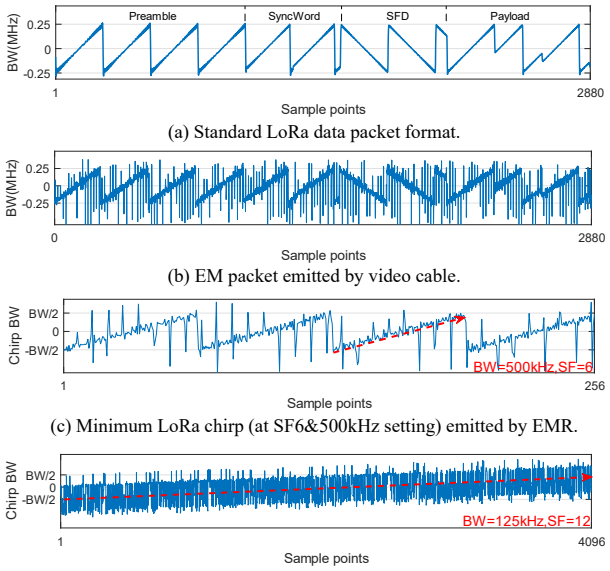
$$T_{chirp} = \frac{2^{SF}}{BW} \tag{8}$$

Given that the sampling rate of the video cable EMR transmitter is equal to PC (Hz), generating a LoRa-style EM chirp requires N_{pixel} consecutive pixels:

$$N_{pixel} = T_{chirp} \cdot PC \tag{9}$$

EM chirp modulation. We modified the input and modulation parts of Algorithm 1 to emit an EM chirp whose frequency varies linearly over the $[f_c - \frac{BW}{2}, f_c + \frac{BW}{2}]$ range.

In Algorithm 2, f_{low} and f_{high} define the frequency boundaries; N_{pixel} is the pixel length required for the video cable to emit an EM chirp; SF and BW are consistent with the LoRa receiver settings; K



(a) Standard LoRa data packet format.

(b) EM packet emitted by video cable.

(c) Minimum LoRa chirp (at SF6&500kHz setting) emitted by EMR.

(d) Maximum LoRa chirp (at SF12&125kHz setting) emitted by EMR.

Figure 10: COTS LoRa signal waveform and EM chirps.

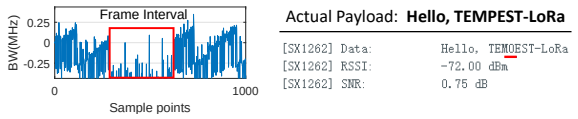
Algorithm 2 For emitting a modulated up-chirp EMR

1: **Input:** f_{low}=f_c - $\frac{BW}{2}$, f_{high}=f_c + $\frac{BW}{2}$, pixel duration N_{pixel}, spreading factor SF, chirp symbol offset K, PC
2: ...
3: $F1 = mod(f_{low}, PC)/PC$;
4: $F2 = mod(f_{high}, PC)/PC$;
5: $F_{step} = (F2 - F1)/N_{pixel}$;
6: $\text{Val} = \sin(2.0 \cdot \pi \cdot (F1 + F_{\text{step}} \cdot \text{mod}(N_{\text{pixel}} \cdot \frac{K}{2^{SF}} + \text{Timer} - 1, N_{\text{pixel}})) \cdot \text{Timer})$
7: ...

is the symbol offset corresponding to the chirp to be transmitted. Line 3 to line 5 calculate the downsampling ratios $F1$ and $F2$ to emit the EMR at f_{low} and f_{high} frequencies. Line 6 modulates an EM chirp with an initial frequency of $f_{low} + \frac{K}{2^{SF}} \cdot BW$ and K is an integer between [0, 2^{SF}-1]. For the SFD part, Algorithm 2 reverses f_{low} and f_{high} to emit the down-chirp.

To demonstrate the effectiveness of this approach, Figure 10 (b) shows a high-fidelity EM packet emitted by a VGA cable, which closely mirrors the chirp duration and frequency of the standard LoRa packet in Figure 10 (a). The noise within the EM packet is attributed to signal intervals when the monitor scans to the end of each scanline. Due to LoRa's high sensitivity and strong noise resilience, COTS LoRa receivers can still reliably identify and decode these LoRa-compatible EM packets.

Since LoRa's configuration encompasses a rich combination of BW and SF, each combination requires the video cable to emit EM chirp signals based on different EMR shifting speeds and transmission durations. Specifically, the combination of SF6&500 kHz requires the shortest chirp duration, while SF12&125 kHz corresponds to the longest chirp duration, which are the upper and lower



(a) Frame interval destroys part of chirps of the EM packet.

(b) COTS LoRa devices may decode incorrectly due to frame interval.

Figure 11: Frame interval and broken EM packet.

BW \ SF	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	1 frame / 130%	2 frame / 65.1%	3 frame / 32.6%	8 frame / 16.3%	18 frame / 8.1%	34 frame / 4%	44 frame / 2%
250kHz	1 frame / 260%	1 frame / 130%	2 frame / 65.1%	4 frame / 32.6%	9 frame / 16.3%	17 frame / 8.1%	22 frame / 4%
500kHz	1 frame / 520%	1 frame / 260%	1 frame / 130%	2 frame / 65.1%	5 frame / 32.6%	9 frame / 16.3%	11 frame / 8.1%

Figure 12: Minimum number of attack frames required assuming the payload size are 24 bits.

limits of all possible combinations. Fortunately, the video cable EMR transmitter's high sampling rate (148.5 MHz) provides sufficient resolution and timing precision to handle all such cases. Figures 10 (c) and (d) demonstrate these two extremes via HDMI cable.

Impact of frame interval: When the duration of a single EM packet exceeds the time span of one frame (approximately 16.7ms), TEMPEST-LoRa combines multiple attack frames into an attack video to emit a longer EM packet.However, the unavoidable frame interval (the time interval between the end of one frame and the start of the next) introduces an emission gap of approximately 0.673ms, which may disrupt the continuity of the EM signal and cause the resulting packet to be decoded incorrectly. Figure 11(a) illustrates a segment of an EM packet affected by such a frame interval. In this example, the chirp is configured with SF6&BW500 kHz. The intended LoRa-compatible EM packet carries the Payload of *Hello, TEMPEST-LoRa*. However, due to the emission gap caused by the frame interval, the decoded output is *Hello, TEMOEST-LoRa* as shown in Figure 11(b).

The settings of SF and BW, the number of frames, and the payload length jointly determine the effect of the frame interval on the EM packets. To provide an understanding of this trade-off, Figure 12 illustrates the number of frames required by TEMPEST-LoRa to construct an attack video under various combinations of SF (6 to 12) and BW (125, 250, and 500 kHz), assuming a fixed preamble of 4 up-chirps and a payload length of 24 bits (raw data length). Since the duration of the frame interval is fixed, Figure 12 also shows the ratio between the frame interval duration and the duration of the corresponding chirp. Increasing the chirp duration reduces the relative impact of frame intervals may corrupt EM packets, but at the cost of requiring more frames in the attack video. Note that since the LoRa physical layer uses error correction mechanisms such as the Hamming code, even EM packets containing frame intervals may be correctly decoded. We evaluated the packet reception rate under different parameter configurations in Section 5.4.

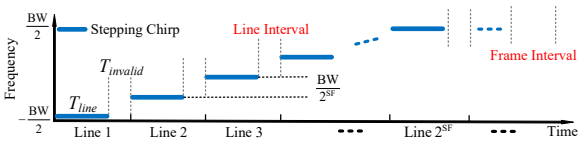


Figure 13: Stepping chirp for align signal intervals. Line interval and frame interval are aligned within each step and each frame respectively.

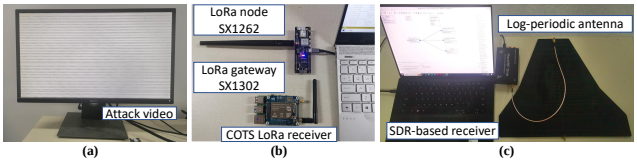


Figure 14: (a) The monitor displaying the attack image/video. (b) COTS LoRa node (SX1262) and gateway (SX1302) with LoRa antennas. (c) SDR-based receiver.

4.3 Low-cost SDR-based Enhancement

The above section showed that attackers could generate LoRa-compatible EM packets and receive them with operational LoRa devices deployed worldwide. To exploit LoRa nodes/gateways, attackers are limited to the parameter configurations (*e.g.*, SF, BW, central frequency, payload size, *etc*) of the LoRa standard. In the following, we present an SDR enhanced TEMPEST-LoRa, which could enable attackers the increased flexibility in generating EM packets not limited by the commercial LoRa standard.

Flexible frequency selection. Given the flexible frequency selection capabilities of the video cable EMR transmitter and SDR, attackers will be capable of selecting and generating an arbitrary attack frequency within 1000 MHz to evade potential detection mechanism or select frequencies with higher intensity to enhance attack distance. We selected f_{sdr} = 201 MHz as the representative frequency of this SDR-based version from Figure 9. f_{sdr} is away from the crowded ISM band, which can reduce interference from other coexisting wireless protocols (e.g. RFID [55], ZigBee [54], NB-IOT [48] and GSM [16]), and the risk of being detected by other COTS wireless receivers.

Align the signal interval: To overcome the damage to the continuity of EM packets caused by the signal intervals, we customized a stepping chirp to align the line interval and frame interval as shown in Figure 13. Within one frame image, each scanline emits one single-frequency EMR, and consecutive 2^{SF} scanlines together constitute a stepping chirp EMR. In this way, the line interval is aligned in each step, and the frame interval is aligned in each frame, thus ensuring the signal continuity of the EM packets. The frequency separation between two adjacent steps is $\frac{BW}{2^{SF}}$. Each line step T_{total} comprises the duration T_{line} of one scanline within display area and the line interval $T_{invalid}$, which can be expressed as:

$$\begin{aligned} T_{total} &= T_{line} + T_{invalid}, \\ T_{line} &= T_p \cdot X_{pixel}, \qquad T_{invalid} = T_p \cdot X_{invalid} \end{aligned} \tag{10}$$

here, X_{pixel} represents the horizontal pixel count (1920 pixels) within the display area, while $X_{invalid}$ denotes the aggregate pixel count of Porch and Sync regions with in a single scanline (2200 - 1920 pixels). Thus, one stepping up-chirp $UC_{step}(t)$ in Figure 13 can be expressed as:

$$UC_{\text{step}}(t) = \sum_{i=0}^{2^{SF}-1} \sin\left(2\pi\left(f_c - \frac{BW}{2} + i \cdot \frac{BW}{2^{SF}}\right)t\right) \cdot \text{rect}\left(\frac{t - i \cdot T_{\text{total}}}{T_{\text{line}}}\right) \tag{11}$$

where the rectangular window function is defined as

$$\text{rect}(\tau) = \begin{cases} 1, & -\frac{1}{2} \le \tau \le \frac{1}{2} \\ 0, & \text{otherwise} \end{cases}$$

where f_c is the chirp's center frequency, and $rect(\tau)$ is used to describe the transmission of the signal within a specific period of time. Specifically, for each step (T_{total}), the rect(τ) function acts as a switch only when t is 'on' (value 1) in the period of T_{line} and 'off' (value 0) in $T_{invalid}$. This ensures that the step frequency of each EMR is emitted only within the specified time slot, resulting in a stepping chirp signal. In the stepping dechirp calculation, the receiving end utilizes the basic stepping down-chirp $DC_{step}(t)$ to demodulate the received stepping up-chirp:

$$DC_{step}(t) = \sum_{i=0}^{2^{SF}-1} \sin\left(2\pi\left(f_c + \frac{BW}{2} - i \cdot \frac{BW}{2^{SF}}\right)t\right) \cdot \text{rect}\left(\frac{t - i \cdot T_{\text{total}}}{T_{\text{line}}}\right) \tag{12}$$

In this SDR-based version, we set the SF to 10, and the residual 56 scanlines (1080-2^{10}) and the frame interval serve as a guard interval. This stepping chirp's duration is approximately equal to the parameter configuration of SF = 12 and BW = 250 kHz in the standard LoRa protocol.

5 Experimental Evaluation

Experiment setup: Except for the cross-device evaluation in Section 5.1, we use a DELL P2317H monitor connected via a 1.5m VGA or HDMI1.4 cable (manufactured by UGREEN) to play the attack videos. The monitor is configured with a resolution of 1080x1920 and a refresh rate of 60 Hz, as illustrated in Figure 14 (a).

For COTS LoRa receivers, we use SX1262 LoRa nodes (for evaluation at 433 MHz) from LILYGO [43] and SX1302 LoRa gateways (for evaluation at 915 MHz) from WaveShare [69], equipped with standard circular antennas (2.2 dBi gain) as shown in Figure 14 (b). Upon detecting EM packets, these devices return data (Payload) and Received Signal Strength Indicator (RSSI). For SDR-based TEMPEST-LoRa, the chirp bandwidth is fixed at 500 kHz, and we employ a HackRF One [14] paired with a log-periodic antenna (6 dBi gain) to capture the physical layer samples for processing, as shown in Figure 14 (c).

5.1 Cross-device feasibility

To evaluate the cross-device feasibility of TEMPEST-LoRa, we use various commercially available display devices and video cables to emit EM packets at 433 MHz and 915 MHz. Then we record the RSSI values returned by the COTS LoRa devices.

Table 2: Testing of TEMPEST-LoRa on different cable specifications.

Cable Manuf.	Type	Length	Returned RSSI at 433MHz	Returned RSSI at 915MHz
SAMZHE	VGA/ HDMI1.4	1.5m	-76 dBm/ -79 dBm	-97 dBm/ -74 dBm
PHILIPS	VGA/ HDMI1.4	1.5m	-76 dBm/ -77 dBm	-96 dBm/ -74 dBm
CHOSEAL	VGA/ HDMI1.4	1.5m	-74 dBm/ -76 dBm	-93 dBm/ -76 dBm
HP	VGA/ HDMI1.4	1.5m	-73 dBm/ -75 dBm	-94 dBm/ -76 dBm
UGREEN	VGA/ HDMI1.4	0.5m	-78 dBm/ -78 dBm	-95 dBm/ -75 dBm
	VGA/ HDMI1.4/ HDMI2.0	1.5m	-78 dBm/ -77 dBm/ -77 dBm	-95 dBm/ -75 dBm/ -76 dBm
	VGA/ HDMI1.4	5m	-76 dBm/ -75 dBm	-94 dBm/ -75 dBm
	VGA/ HDMI1.4	10m	-73 dBm/ -73 dBm	-92 dBm/ -73 dBm
This test used Dell P2317H monitor.				

Table 3: Testing of TEMPEST-LoRa on different display devices.

Device Type	Device Manuf.	Model	Returned RSSI at 433MHz (VGA/HDMI)	Returned RSSI at 915MHz (VGA/HDMI)
Monitor	Dell	P2317H	-78 dBm/ -77 dBm	-95 dBm/ -75 dBm
	Dell	P2225H	-80 dBm/ -77 dBm	-96 dBm/ -76 dBm
	PHILIPS	275M7C	-77 dBm/ -75 dBm	-93 dBm/ -75 dBm
	HP	P24V G5	-78 dBm/ -78 dBm	-95 dBm/ -76 dBm
	Xiaomi	RMMNT27NF	-78 dBm/ -77 dBm	-97 dBm/ -77 dBm
Projector	SONY	VPL-U300WZ	-75 dBm/ -76 dBm	-93 dBm/ -74 dBm
	EPSON	CB-X05E	-80 dBm/ -77 dBm	-97 dBm/ -76 dBm
TV	Lenovo	Ideatv 55E31Y	-77 dBm/ -78 dBm	-93 dBm/ -74 dBm
This test used VGA (1.5m) and HDMI1.4 (1.5m) made by UGREEN.				

We first tested video cables from different manufacturers, with cable types and lengths as shown in Table 2. All cables have shielded metal layers (*i.e.*, aluminum foil wrapped around each bus) to minimize EM leakage. The results show that all video cables tested were able to be manipulated by TEMPEST-LoRa to emit EM packets. The reason for TEMPEST-LoRa's cross-device compatibility is that the electrical characteristics of commercially available display devices and video cables all follow the manufacturing standards defined by the Video Electronics Standards Association (VESA) [2], so their EM emission characteristics are also similar.

In general, there was no significant difference in the EMR intensity of the video cable of different manufacturers, and the corresponding RSSI values were similar. TEMPEST-LoRa is also compatible with VGA and two mainstream versions of HDMI (1.4 and 2.0). In the measurement of cable length, we tested VGA and HDMI1.4 from UGREEN with lengths of 0.5m, 1.5m, 5m, and 10m. We noticed that the RSSI value increased slightly with increasing cable length. For example, the RSSI corresponding to HDMI1.4 from 0.5m to 10m increased from -78 dBm to -73 dBm. We speculate that the actual power of the longer cable will increase slightly, resulting in an increase in EMR intensity.

Next, we test TEMPEST-LoRa on different display devices. Detailed manufacturers and models are shown in Table 3. The results show that TEMPEST-LoRa shows a wide range of feasibility on display devices from different manufacturers/models, and there is no significant difference in the RSSI values returned by COTS LoRa receivers. Additionally, although the main attack scenario of TEMPEST-LoRa is a monitor connected to a video cable, it can also work on projectors and TVs.

5.2 Attack Distance

We measure the maximum attack distance both indoors and outdoors. The attack video loops on the screen (*i.e.*, the video cable repeatedly emits EM packets), and the EM packet's payload length is fixed to 24 raw bits. In this section, the 'maximum attack distance' is defined as the farthest distance at which the receiver can reliably decode the EM packets. This distance is determined by moving Rx along the Measurement Path in Figure 15 (a) and (b) until the receiver is no longer able to receive and decode EM packets completely and correctly. Around the extreme attack distance, the receiver may detect LoRa packets, but the decoded Payload contains errors Due to signal attenuation. Therefore, the maximum attack distance we record is the farthest location where correctly decoded EM packets exist. For the evaluation of COTS LoRa, we ensure that the SF and BW of the EM packets match the settings of the LoRa receivers with SF ranging from 6 to 12 and BW options at 125 kHz, 250 kHz, and 500 kHz.

Indoor: The indoor testing is conducted in an office as shown in Figure 15 (a), where the distance between the two endpoints is 40m, a distance we deem sufficient to exceed the lengths of most real-world offices. The victim's computer (Tx) is placed on the far right side of the room. The receiver moves along the measurement path until the EM packet can no longer be decoded correctly. Table 4 shows the maximum attack distances in the office scene. As the

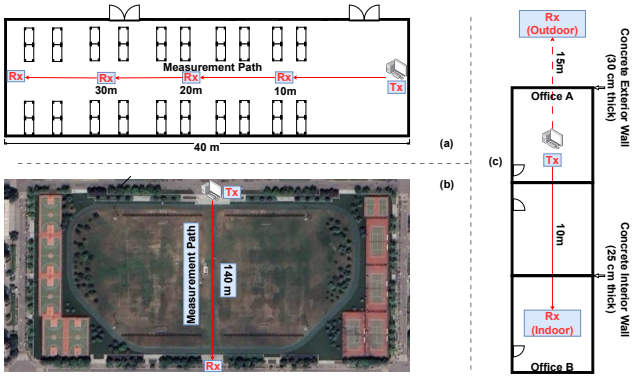


Figure 15: Indoor, outdoor, and through-wall scenes.

Table 4: Indoor attack distances on COTS LoRa.

433MHz&VGA	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	36.7m	40m	40m	40m	40m	8.8m	1.0m
250kHz	28.5m	32m	40m	40m	40m	35.2m	3.2m
500kHz	23.0m	17.9m	30.4m	40m	40m	40m	6.5m
433MHz&HDMI	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	30.4m	37.2m	40m	40m	40m	6.0m	1.0m
250kHz	28.7m	28.7m	37.5m	40m	40m	32m	3.5m
500kHz	17.2m	16.6m	30.9m	40m	40m	40m	6.0m
915MHz&VGA	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	25.0m	25.2m	26.5m	33.5m	30.5m	8.5m	1.0m
250kHz	22.0m	22.5m	26.2m	30.0m	27.4m	19.1m	3.4m
500kHz	17.2m	17.9m	22.5m	27.7m	26.5m	23.5m	5.3m
915MHz&HDMI	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	40m	40m	40m	40m	40m	6.0m	1.0m
250kHz	40m	40m	40m	40m	40m	19.5m	3.5m
500kHz	40m	40m	40m	40m	40m	40m	6.5m

Table 5: Outdoor attack distances on COTS LoRa.

433MHz&VGA	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	40.1m	46.0m	47.4m	**52.2m**	50.5m	8.5m	1.5m
250kHz	27.6m	38.5m	42.0m	47.5m	47.1m	26.0m	3.5m
500kHz	23.4m	30.6m	37.6m	43.5m	41.9m	43.0m	6.5m
433MHz&HDMI	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	36.6m	45.0m	46.2m	50.0m	**51.0m**	12.1m	1.0m
250kHz	31.9m	37.1m	42.0m	44.4m	47.5m	19.6m	3.0m
500kHz	23.4m	29.4m	36.5m	41.4m	42.1m	39.5m	4.0m
915MHz&VGA	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	23.1m	27.8m	32.0m	**39.5m**	36.5m	10.7m	1.0m
250kHz	20.1m	22.3m	29.5m	36.7m	34.2m	17.5m	3.3m
500kHz	15.4m	19.7m	24.0m	28.5m	30.5m	29.4m	6.0m
915MHz&HDMI	SF6	SF7	SF8	SF9	SF10	SF11	SF12
125kHz	64.2m	68.4m	73.5m	**87.5m**	87.2m	17.5m	3.5m
250kHz	61.9m	67.1m	70.5m	77.4m	83.5m	24.3m	7.5m
500kHz	53.1m	61.0m	66.1m	72.8m	69.2m	50.0m	10.0m

chirp duration (starting from SF6&500 kHz) increases, the attack distance gradually increases until it reaches 40m at the end of the room. This combination of SF&BW and the growth relationship of transmission distance are consistent with LoRa technology. At 433 MHz, between SF7 and SF11, both VGA and HDMI can support a transmission distance of up to 40m. At 915 MHz, VGA's maximum attack distance is 33.5m at SF8&125 kHz, while HDMI's maximum attack distance can be 40m. However, when the chirp duration surpasses the threshold of SF11&250 kHz, the attack distance drops sharply. This is because as the chirp duration increases, the number of frames required for the attack videos increases, resulting in increased errors due to the frame intervals. Figure 16 shows the maximum attack distance of SDR-based version. With the log-periodic antenna (higher receiving gain) and higher leakage intensity at f_{sdr} frequency, TEMPEST-LoRa can achieve the maximum attack distance of 40m.

Outdoor: For the outdoor scenario, we evaluate the maximum attack distance on a playground shown in Figure 15 (b). The receiver is moved along the measurement path from the Tx to determine the maximum attack distance. Table 5 shows the maximum attack distances supported by COTS LoRa in outdoor environments. The outdoor evaluation mirrors the indoor evaluation, with the attack distance incrementally extending as the chirp duration until SF11&250 kHz. Beyond this threshold, the attack distance decreases

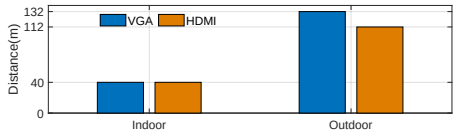


Figure 16: Maximum attack distances on SDR.

due to the frame interval. At 433 MHz, the maximum distance is 52.2m at SF9&125 kHz with the VGA cable, and 51.0m at SF10&125 kHz for HDMI. In the 915 MHz band, the HDMI cable performs better, and the attack distance that can be achieved at the SF9&125 kHz settings is 87.5m. While using VGA cable at SF9&125 kHz, the distance reaches 39.5m. When using an SDR-based receiver, the maximum distance is extended to 112m (HDMI) - 132m (VGA).

Comparing the results indoors and outdoors, the absence of obstacles outdoors typically results in longer attack distances compared to indoor environments. On the non-LoRa frequency bands, the higher emission intensity and higher antenna gain enable attackers to capture secret data from over hundred-meter away using the SDR. In addition, we notice that when the victim uses an HDMI cable, the attack distance at 915 MHz (87.5m) is longer than that at 433 MHz (51m), although the leakage intensity of 433 MHz (47.8 dB) is slightly higher than that of 915 MHz (43.1 dB) as shown in Figure 9. We speculate that the main reason for this difference is that the sensitivity of LoRa gateways is higher than that of individual LoRa nodes. From the attacker's perspective, the malware can initially identify the victim's cable type. If it is VGA, it could emit EM packets at 433 MHz; if it is HDMI, 915 MHz is more effective. Subsequently, the malware can select the appropriate settings (such as SF9&125 kHz, or use the SDR-based version of TEMPEST-LoRa) to decode secret data at a longer distance.

5.3 Through-wall Transmission

Next, we evaluate the through-wall transmission in the scenarios shown in Figure 15 (c). The Tx is located in Office A. The distance between Tx and the location of the outdoor receiver (Rx) is 15m, obstructed by a 30cm-thick concrete exterior wall; the distance between Tx and indoor Rx is 10m, separated by two concrete interior walls (25cm thick). To evaluate the receiving capability of COTS LoRa, Tx emits EM packets at 433 MHz via VGA cable and at 915 MHz via the HDMI cable with SF9&125 kHz settings (the combination for the optimal attack distance); we record the RSSI value returned by the LoRa node/gateway. For the SDR-based version, we compute the DNR of captured signals from VGA and HDMI.

Table 6: The EM packets' RSSI (for COTS LoRa) and DNR (for SDR) after through-wall transmission.

Through wall	433MHz	915MHz	SDR-based
One Exterior Wall	-108 dBm - -112 dBm	-108dBm - -111 dBm	18.7 (VGA) 14.7 (HDMI)
Two Interior Walls	-116 dBm - -120 dBm	-115 dBm - -118 dBm	11.6 (VGA) 7.4 (HDMI)

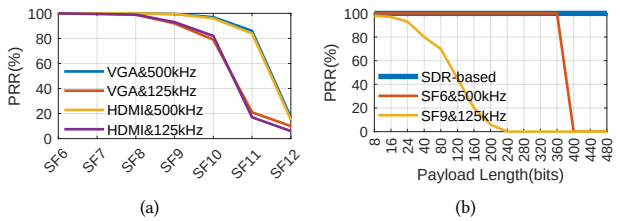


Figure 17: (a) PRR under various SF&BW. (b) PRR under various payload lengths.

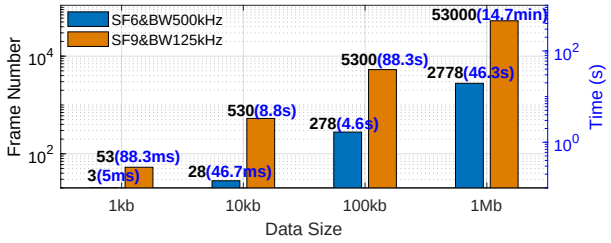


Figure 18: The frame number of attack video and the playback time for transmitting different amounts of secret data.

Table 6 shows the RSSI and DNR values for through-wall transmission using COTS LoRa devices and SDR. In the 'indoor to outdoor' scenario, the RSSI values reported range from -108 dBm to -112 dBm. While in 'indoor to indoor', transmissions experience more significant attenuation after passing through two interior walls, with RSSI decreasing from -115 dBm to -120 dBm. As a comparison, the minimum RSSI we observed in attack distance evaluation is between -120 dBm and -124 dBm. For the SDR-based version, we first measure the initial DNR of chirps at 1m away from Tx, which is 31.9 for VGA and 24.3 for HDMI. After penetrating one exterior wall, the DNR of VGA and HDMI drops to 18.7 and to 14.7, respectively; while after penetrating two interior walls, EM emission is further attenuated, with the DNR of VGA dropping to 11.6 and that of HDMI dropping to 7.4.

5.4 Packet Reception Rate

To quantify the impact of signal intervals on EM packets, we measure the packet reception rate (PRR) in the office scenarios shown in Figure 15 (a). The EM packets were emitted 1000 times; successful packet reception is defined as all bits in the EM packet being decoded correctly. We evaluate 433 MHz using VGA and 915 MHz using HDMI.

Combination of SF and BW: The settings include SF6 to SF12, paired with BWs of 125 kHz and 500 kHz, and the payload length is 24 raw bits. The COTS LoRa receivers are placed at half the maximum attack distance indoors as shown in Table 4 (*e.g.*, 16.75m from the monitor when at the HDMI&SF9&125 kHz setting).

As shown in Figure 17(a), the PRR exhibits a gradual decline from 100% to around 80% as the SF and BW increase and drop sharply when the SF is higher than 11 at BW of 500 kHz. In contrast, this turning point is at SF10 if the BW is 125 kHz. The reason is that the longer chirp duration requires more frames of attack video, which increases the possibility of EM packets being decoded incorrectly. Notably, under the same SF&BW settings, the cable type has little impact on the PRR.

Payload Length: Given the minimal impact of cable type on the PRR, in this evaluation, we use HDMI at 915 MHz to measure the PRR across payload lengths ranging from 8 raw bits to 480 raw bits. We select two representative combinations: SF6&500 kHz (with the minimum chirp duration) and SF9&125 kHz (with the longest attack distance). The COTS LoRa receiver/SDR is positioned 20m/40m from Tx.

As shown in Figure 17(b), under SF6&500 kHz, the PRR sustains at 100% when the payload length is less than or equal to 360 bits. However, it plummets to 0% when the payload length reaches 400 bits. This decline occurs because the 400-bit payload needs about 1.02 frames (that is, the attack video containing 2 frames), and one frame interval could destroy 5.2 chirps at SF6&500 kHz, such broken packets exceed LoRa's tolerance. Conversely, under the SF9&125 kHz setting, the PRR is 93% for 24-bit payload and begins to decline sharply beyond 40 bits. The duration of the frame interval is roughly 2% of a single chirp, which suggests a lower likelihood of EM packet corruption. Nonetheless, SF9&125 kHz requires more frames under the same payload length, and the PRR starts to drop at a shorter payload length. On the SDR, benefiting from the design of aligning signal interval, the EM packets with payload lengths ranging from 8 bits to 480 bits can be successfully decoded at a distance of 40m.

5.5 Data Rate

Data size: As shown in Figure 18, we selected the two most representative settings of SF6&BW500 kHz and SF9&BW125kHz to evaluate the number of attack video frames and the corresponding video time. For a short message of 1 kb (*e.g.*, access keys), TEMPEST-LoRa can complete the transmission in less than 1 second. For confidential information of 10 kb to 100 kb (e.g., log files), it only takes 46.7ms to 4.6s under the fastest setting SF6&BW500 kHz, and SF9&BW125 kHz takes between 8.8s and 88.3s.

Goodput: Next, we evaluate the actual throughput (goodput, the actual data rate after the error packets are removed) in indoors, including SF6&500 kHz, SF9&125 kHz, and SDR-based version, at frequencies 433 MHz (VGA), 915 MHz (HDMI), and f_{sdr}. The theoretical throughputs corresponding to these settings are 21.6 kbps, 1160 bps (which are equal to the standard LoRa's throughput), and 180 bps, respectively. The receiver is positioned at distances of 10m, 20m, and 40m from Tx. During each test, Tx emits 1000 EM packets, and we calculate the goodput.

Table 7 shows the goodput in the three settings at 10m to 40m. At 10m and 20m, TEMPEST-LoRa only has slight packet loss, and the goodput is equal to or close to the theoretical maximum throughput. As the distance increases to 30m to 40m, except for SF6&500kHz&VGA setting, which is not measured due to signal attenuation, the goodput of other settings decreases slightly. In general, in an office scenario, attackers can choose the SF6&BW500 kHz to transmit sensitive data at the fastest speed; if the receiver is far away from the victim, using SF9&BW125 kHz setting or the SDR-based version can capture secret data at a slightly lower rate but a longer distance.

Table 7: Goodput at 10m, 20, 30m, and 40m.

433MHz&VGA	SF6&500kHz	SF9&125kHz	SDR-based
10m	21.6 kbps	1160 bps	180 bps
20m	20.5 kbps	1156.5 bps	180 bps
30m	/	1153 bps	179.6 bps
40m	/	1148.4 bps	179.2 bps
915MHz&HDMI	SF6&500kHz	SF9&125kHz	SDR-based
10m	21.6 kbps	1160 bps	180 bps
20m	21.53 kbps	1160 bps	180 bps
30m	21.38 kbps	1154.2 bps	178.9 bps
40m	21.04 kbps	1151.9 bps	178.4 bps

5.6 Impact of Receiving Direction

We measure the emission intensity in various receiving directions for four potential cable placements: vertical, horizontal, circular, and curved. The Rx is placed at a distance of 10 meters from the monitor at different directions to record the RSSI values.

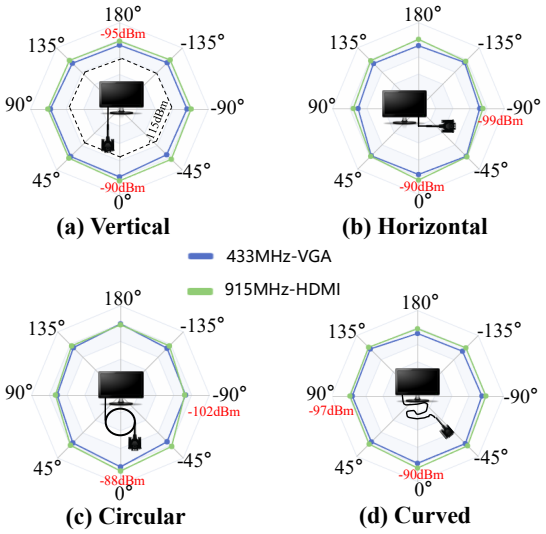


Figure 19: RSSI values in various directions.

As shown in Figure 19(a), overall, the RSSI of HDMI at the 915 MHz attack frequency is slightly higher than that of VGA at 433 MHz, and we marked the maximum and minimum RSSI of 915 MHz&HDMI in the corresponding direction. In all placement methods, the RSSI in front of the monitor (0°) is the highest (-88 dBm to -90 dBm). In the vertical placement, the position of minimum RSSI (-95 dBm) is behind the monitor (180°) because the monitor itself blocks part of the leakage. When placed horizontally, the RSSI on the sides of the monitor (90° and -90°) is the smallest (about -99 dBm). If the cable is placed casually, RSSIs range from -90 dBm to -97 dBm. Overall, the EMR intensity in different directions is relatively uniform, implying that attackers are not restricted to specific orientations when receiving the secret packets.

6 Discussion

In this section, we discuss considerations for practical deployment, TEMPEST-LoRa future work and countermeasures.

Multiple active monitors: The malware carrying TEMPEST-LoRa may infect multiple computers in proximity to the victim. If these active monitors simultaneously emit EM packets using the same LoRa settings, the receiving end may have difficulty distinguishing them. A straightforward solution is to embed a unique hardware identifier (*e.g.*, CPU ID or motherboard UUID, which is accessible at the software level) in each EM packet to enable source differentiation at the receiver. Furthermore, malware can utilize these hardware IDs to schedule transmission at randomized times, reducing the likelihood of packet collisions.

TEMPEST-LoRa and CTCC's future extension: Although this paper uses a common display setting of 1080x1920@60Hz for analysis and evaluation, TEMPEST-LoRa can be adapted to other resolutions and refresh rates by adjusting the input parameters (*ScreenH*, *ScreenW*, and *PC* under the corresponding display setting) in Algorithm 2, enabling COTS LoRa devices to decode the EM packets.

Additionally, on the basis of our experimental observations, we believe that the concept of CTCC can be extended to other commercial wireless technologies. First, we observe that the video cable can emit EMR beyond 1000 MHz as discussed in Figure 9. For example, HDMI cables still exhibit measurable EMR intensity at 2.4 GHz (WiFi and Bluetooth's frequency bands). Second, while generating waveforms compatible with other wireless protocols requires more sophisticated modulation techniques, it is feasible. For instance, EMR's amplitude can be more finely controlled by changing the grayscale value of the pixel (under the commonly used 8-bit RGB setting, this provides up to 256 levels of intensity control, allowing the video cable EMR transmitter to approximate 8-bit amplitude resolution). Furthermore, the EMR phase can also be manipulated by controlling the spatial arrangement of black-white pixels.

Countermeasures Analysis: Given the non-privilege, high flexibility of attack frequencies, and strong attenuation resistance of TEMPEST-LoRa, traditional countermeasures against physical covert channels need to be re-examined and improved:

(1) EM shielding. The video cables we experimented with in the evaluation are shielded with aluminum foil, copper braid, and twisted pair designs to reduce EMR. These shielding methods could protect against conventional EM covert channels, but fail to defend against attackers armed with TEMPEST-LoRa. The main reason is that the LoRa-compatible EM packets could benefit from strong noise resilience of LoRa wireless technology and high sensitivity of LoRa radios and be received at much greater distances even when the video cables are shielded and EM signals are minimized. We call for innovative shielding methods to mitigate the risks posed by CTCC techniques.

(2) RF jammers. RF jammers could overpower the leaked signal with high-power noise and obstruct CTCC's reception. This potential protection method would inevitably disrupt normal LoRa communications widely deployed worldwide as well as other coexisting wireless communications in the ISM bands such as WiFI and wireless radios for medical devices, which makes these countermeasures infeasible in practice. Moreover, attackers could adaptively

select different parameter configurations such as SF, BW and even central frequency to evade from RF jammers and covert channel detection.

(3) Covert packet detection. Unlike prior EM covert channels that rely on custom modulation schemes with distinctive spectral patterns (such as B-FSK), the LoRa-compatible waveforms making covert EM packets resemble legitimate LoRa transmissions on the spectrum. This similarity allows them to bypass conventional RF anomaly detection based on spectral signatures. However, subtle waveform differences still exist between LoRa-like EMR signals and genuine LoRa transmission. These differences do not affect packet decoding, but may serve as a basis for countermeasures. Future work could explore detection algorithms based on physical-layer fingerprints to differentiate covert EM packets from legitimate ones.

(4) Larger isolation area. Given TEMPEST-LoRa's over-hundred-meter attack range, the isolation areas for conventional air-gapped networks must be further expanded. Eliminating all COTS wireless devices from an entire building or creating a Faraday zoom is viable but incurs prohibitive implementation cost. Considering the high penetration of LoRa technologies supporting a variety of IoT applications worldwide, it is increasingly likely that attackers could self-deploy or leverage existing third-party LoRa infrastructure near a target to receive LoRa-compatible EM packets. Currently, only a few highly confidential scenarios (*e.g.*, military applications [24]) can afford and build large shielding areas while other sectors (*e.g.*, finance, business, medical, *etc*) remain vulnerable to the risk of this new type of covert channel attacks reported in this paper.

7 Conclusion

This paper reveals the risk of covertly leaking sensitive information from air-gapped computers by generating LoRa-compatible EM packets with video cables. The EM packets can be received from widely deployed COTS LoRa devices from afar, even when the video cables are protected behind concrete walls. Attackers also could go beyond and break the limit of the communication range of the LoRa protocol by crafting customized EM packets and receive with low-cost SDRs. The presented CTCC technologies with fine-grained control of EM leakage over a large wireless spectrum can potentially be applied to generate EM packets compatible with other wireless technologies such as WiFi and ZigBee [1]. We plan to comprehensively investigate such potential risks and possible countermeasures in the future.

8 Open Source

To promote reproducibility and further research, we have released the full implementation of TEMPEST-LoRa as open-source and permanently archived it on Zenodo: https://zenodo.org/records/15532223. We provide comprehensive reproduction materials, including the source code, detailed configuration settings for the monitor, the LoRa SX1262 node, and the SX1302 gateway, as well as some artifacts such as attack images generated under varying attack frequencies, spreading factors (SF), and bandwidths (BW).

[1]Preliminary results obtained but not reported in this paper due to page limit

Acknowledgments

We thank the anonymous reviewers for their insightful comments and constructive suggestions, which helped improve the quality of this paper. This work was supported by the National Key R&D Program of China 2023YFB2904000, the NSFC Grant No. 62302383, as well as the Hong Kong GRF Grant No. 15211924 and 15206123.

References

[1] Daniel Arendt. 2016. Medical-Grade Network Security-Air-Gap Isolation and PossibleWeak Points. *Journal of Applied Computer Science* 24, 3 (2016), 7–19.
[2] Video Electronics Standards Association. 2013. Video Electronics Standards Association, Display Monitor Timing 1.3. https://glenwing.github.io/docs/VESA-DMT-1.13.pdf.
[3] Elaine Barker and William Barker. 2018. *Recommendation for key management, part 2: best practices for key management organization.* Technical Report. National Institute of Standards and Technology.
[4] Nicolas Boichat. 2006. DDCcontrol documentation. *[Online] https://ddccontrol.sourceforge.net/doc/ddccontrol-0.4.pdf* (2006).
[5] Giovanni Camurati and Aurélien Francillon. 2022. Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1193–1210.
[6] Hsun-Wei Cho and Kang G Shin. 2021. BlueFi: bluetooth over WiFi. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 475–487.
[7] Chay Chua. 2005. *CyberCIEGE scenario illustrating software integrity issues and management of air-gapped networks in a military environment.* Ph. D. Dissertation. Monterey, California. Naval Postgraduate School.
[8] Google Cloud. 2024. *How Google protects the physical-to-logical space in a data center [online].* https://cloud.google.com/docs/security/physical-to-logical-space
[9] Fangming Deng, Pengqi Zuo, Kaiyun Wen, and Xiang Wu. 2020. Novel soil environment monitoring system based on RFID sensor and LoRa. *Computers and Electronics in Agriculture* 169 (2020), 105169.
[10] LLC et al. 2006. ,"High-Definition Multimedia Interface Specification Version 1.3 a: Supplement 1 Consumer Electronics Control (CEC)".
[11] Justin Feng, Timothy Jacques, Omid Abari, and Nader Sehatbakhsh. 2023. Everything has its Bad Side and Good Side: Turning Processors to Low Overhead Radios Using Side-Channels. In *Proceedings of the 22nd International Conference on Information Processing in Sensor Networks*. 288–301.
[12] FireEye. 2020. Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor. *FireEye Threat Research* (2020).
[13] Joint Task Force. 2017. *Security and privacy controls for information systems and organizations.* Technical Report. National Institute of Standards and Technology.
[14] Great Scott Gadgets. 2018. *Hackrf one Official Website [online].* https://greatscottgadgets.com/hackrf
[15] Piotr Gawłowicz, Anatolij Zubow, and Falko Dressler. 2022. Wi-Lo: Emulation of LoRa using Commodity 802.11 b WiFi Devices. In *ICC 2022-IEEE International Conference on Communications*. IEEE, 4414–4419.
[16] Guifen Gu and Guili Peng. 2010. The survey of GSM wireless communication system. In *2010 international conference on computer and information application*. IEEE, 121–124.
[17] Mordechai Guri. 2022. Air-fi: Leaking data from air-gapped computers using wi-fi frequencies. *IEEE Transactions on Dependable and Secure Computing* (2022).
[18] Mordechai Guri and Yuval Elovici. 2018. Bridgeware: The air-gap malware. *Commun. ACM* 61, 4 (2018), 74–82.
[19] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. {GSMem}: Data Exfiltration from {Air-Gapped} Computers over {GSM} Frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*. 849–864.
[20] Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval Elovici. 2014. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. IEEE, 58–67.
[21] Mordechai Guri and Matan Monitz. 2018. Lcd tempest air-gap attack reloaded. In *2018 IEEE International Conference on the Science of Electrical Engineering in Israel (ICSEE)*. IEEE, 1–5.
[22] Mordechai Guri, Matan Monitz, and Yuval Elovici. 2016. USBee: Air-gap covert-channel via electromagnetic emission from USB. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 264–268.
[23] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. 2014. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 954–965.

[24] Leland H. Hemming. 2000. *Architectural Electromagnetic Shielding Handbook: A Design and Specification Guide.* John Wiley & Sons.
[25] Wenchao Jiang, Zhimeng Yin, Ruofeng Liu, Zhijun Li, Song Min Kim, and Tian He. 2017. Bluebee: a 10,000 x faster cross-technology communication via phy emulation. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. 1–13.
[26] Mohammed Jouhari, Nasir Saeed, Mohamed-Slim Alouini, and El Mehdi Amhoud. 2023. A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges. *IEEE Communications Surveys & Tutorials* (2023).
[27] Eric D Knapp. 2024. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems.* Elsevier.
[28] Lone Kolobe, Boyce Sigweni, and Caspar K Lebekwe. 2020. Systematic literature survey: Applications of LoRa communications. (2020).
[29] Arif Koyun and Ehssan Al Janabi. 2017. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* 4, 6 (2017), 7533–7538.
[30] Markus G Kuhn and Ross J Anderson. 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*. Springer, 124–142.
[31] Yeu-Pong Lai and Ruan-Han Dai. 2009. The implementation guidance for practicing network isolation by referring to ISO-17799 standard. *Computer Standards & Interfaces* 31, 4 (2009), 748–756.
[32] Butler W Lampson. 1973. A note on the confinement problem. *Commun. ACM* 16, 10 (1973), 613–615.
[33] Ralph Langner. 2011. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy* 9, 3 (2011), 49–51.
[34] Federico Larroca, Pablo Bertrand, Felipe Carrau, and Victoria Severi. 2022. gr-tempest: an open-source GNU Radio implementation of TEMPEST. In *2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, 1–6.
[35] Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, and Stephane Molton. 2021. Whispering devices: A survey on how side-channels lead to compromised information. *Journal of Hardware and Systems Security* 5 (2021), 143–168.
[36] Euibum Lee, Dong-Hoon Choi, Taesik Nam, and Jong-Gwan Yook. 2022. A quantitative analysis of compromising emanation from TMDS interface and possibility of sensitive information leakage. *IEEE Access* 10 (2022), 73997–74011.
[37] Ho Seong Lee, Jong-Gwan Yook, and Kyuhong Sim. 2015. Measurement and analysis of the electromagnetic emanations from video display interface. In *2015 IEEE Electrical Design of Advanced Packaging and Systems Symposium (EDAPS)*. IEEE, 71–73.
[38] Ronald L Lendvay. 2016. *Shadows of Stuxnet: Recommendations for US policy on critical infrastructure cyber defense derived from the Stuxnet attack.* Ph. D. Dissertation. Monterey, California: Naval Postgraduate School.
[39] Luca Leonardi, Filippo Battaglia, and Lucia Lo Bello. 2019. RT-LoRa: A medium access strategy to support real-time flows over LoRa-based networks for industrial IoT applications. *IEEE Internet of Things Journal* 6, 6 (2019), 10812–10823.
[40] Chenning Li and Zhichao Cao. 2022. Lora networking techniques for large-scale and long-term iot: A down-to-top survey. *ACM Computing Surveys (CSUR)* 55, 3 (2022), 1–36.
[41] Zhijun Li and Yongrui Chen. 2020. BLE2LoRa: Cross-technology communication from bluetooth to LoRa via chirp emulation. In *2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 1–9.
[42] Zhijun Li and Tian He. 2017. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*. 2–14.
[43] Lilygo. 2024. *Official Website [online].* https://www.lilygo.cc
[44] Hui Lin, Liming Wu, Junxiu Liu, and Tengteng Wen. 2010. Overshoot and undershoot control for signal generator. In *2010 International Conference on Measuring Technology and Mechatronics Automation*, Vol. 2. IEEE, 864–867.
[45] Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejla Batina, and Martha Larson. 2020. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *arXiv preprint arXiv:2011.09877* (2020).
[46] Yan Long, Qinhong Jiang, Chen Yan, Tobias Alam, Xiaoyu Ji, Wenyuan Xu, and Kevin Fu. 2019. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. (2019).
[47] Martin Marinov. 2014. Remote video eavesdropping using a software-defined radio platform. *MS thesis, University of Cambridge* (2014).
[48] Emmanuel Migabo, Karim Djouani, and Anish Kurien. 2018. A modelling approach for the narrowband IoT (NB-IoT) physical (PHY) layer performance. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 5207–5214.
[49] European Cyber Security Organisation. 2021. *System security and certification considerations [online].* https://ecs-org.eu/ecso-uploads/2022/10/61ebc4a13b567.pdf
[50] European Cyber Security Organisation. 2022. *ECSO Technical Paper on Internet of Things (IoT) [online].* https://ecs-org.eu/ecso-uploads/2023/01/ECSO_WG6_IoT-Technical_paper_final.pdf
[51] Clayton R Paul, Robert C Scully, and Mark A Steffka. 2022. *Introduction to electromagnetic compatibility.* John Wiley & Sons.
[52] Sean Peisert, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benzel, Carl Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael. 2021. Perspectives on the SolarWinds incident. *IEEE Security & Privacy* 19, 2 (2021), 7–13.
[53] FIPS Pub. 1994. Security requirements for cryptographic modules. *FIPS PUB* 140 (1994), 140–2.
[54] C Muthu Ramya, Madasamy Shanmugaraj, and R Prabakaran. 2011. Study on ZigBee technology. In *2011 3rd international conference on electronics computer technology*, Vol. 6. IEEE, 297–301.
[55] Chris M Roberts. 2006. Radio frequency identification (RFID). *Computers & security* 25, 1 (2006), 18–26.
[56] Ignacio Sanmillan. 2020. Ramsay: A cyber-espionage toolkit tailored for air-gapped networks. *Retrieved October* 12 (2020), 2020.
[57] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Accuracy enhancement of electromagnetic side-channel attacks on computer monitors. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 1–9.
[58] Karen Scarfone, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh. 2008. Technical guide to information security testing and assessment. *NIST Special Publication* 800, 115 (2008), 2–25.
[59] Cheng Shen, Tian Liu, Jun Huang, and Rui Tan. 2021. When LoRa meets EMR: Electromagnetic covert channels can be super resilient. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1304–1317.
[60] Junyang Shi, Di Mu, and Mo Sha. 2019. Lorabee: Cross-technology communication from lora to zigbee via payload encoding. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*. IEEE, 1–11.
[61] Dimitrios Siafarikas and John L Volakis. 2020. Toward direct RF sampling: Implications for digital communications. *IEEE Microwave Magazine* 21, 9 (2020), 43–52.
[62] Keith Stouffer, Joe Falco, Karen Scarfone, et al. 2011. Guide to industrial control systems (ICS) security. *NIST special publication* 800, 82 (2011), 16–16.
[63] Erik Thiele. 2001. Tempest for Eliza. *[Online] http://www.erikyyy.de/tempest* (2001).
[64] Semtech LoRa Connect™ 137MHz to 1020MHz Long Range Low Power Transceiver. 2024. *SX1262 Official Website [online].* https://www.semtech.com/products/wireless-rf/lora-connect/sx1262
[65] Shuai Tong, Yangliang He, Yunhao Liu, and Jiliang Wang. 2022. De-spreading over the air: long-range ctc for diverse receivers with lora. In *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking*. 42–54.
[66] Wim Van Eck. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security* 4, 4 (1985), 269–286.
[67] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, 3152676 (2017), 10–5555.
[68] Zuoguang Wang, Limin Sun, and Hongsong Zhu. 2020. Defining social engineering in cybersecurity. *IEEE Access* 8 (2020), 85094–85115.
[69] WaveShare. 2024. *Official Website [online].* https://www.waveshare.com/
[70] Wikipedia. 2024. Tempest (codename) — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/Tempest_(codename)
[71] Dan Xia, Xiaolong Zheng, Fu Yu, Liang Liu, and Huadong Ma. 2022. WiRa: Enabling cross-technology communication from WiFi to LoRa with IEEE 802.11 ax. In *Proceedings of IEEE INFOCOM*.
[72] Xianjin Xia, Qianwu Chen, Ningning Hou, Yuanqing Zheng, and Mo Li. 2023. XCopy: Boosting Weak Links for Reliable LoRa Communication. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*. 1–15.
[73] Qiang Yang and Yuanqing Zheng. 2023. AquaHelper: Underwater sos transmission and detection in swimming pools. In *Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems*. 294–307.
[74] Yan Yubo, Yang Panlong, Li Xiangyang, Tao Yue, Zhang Lan, and You Lizhao. 2013. Zimo: Building cross-technology mimo to harmonize zigbee smog with wifi flash without intervention. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. 465–476.
[75] Zihao Zhan, Zhenkai Zhang, and Xenofon Koutsoukos. 2020. Bitjabber: The world's fastest electromagnetic covert channel. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 35–45.
[76] Anna ZYGIEREWICZ. 2020. Directive on security of network and information systems (NIS Directive). (2020).

A Artifact Appendix

This appendix provides a detailed description of the artifact accompanying our paper: "TEMPEST-LoRa: Cross-Technology Covert

Communication", accepted at ACM CCS 2025. The submitted artifact has been evaluated by the Artifact Evaluation Committee and has received the Artifacts Available badge.

A.1 Abstract

This artifact demonstrates a cross-technology electromagnetic (EM) covert communication technique that allows secret data to be transmitted via EM radiation (EMR) from a computer's video cable (VGA and HDMI) and received by commercial off-the-shelf (COTS) LoRa devices.

The artifact includes:

- Source code for generating specially attack images and videos that emit LoRa-compatible EMR signals when displayed.
- Instructions for setup and evaluation.
- Pre-generated demo attack images for quick testing.

The artifact is publicly on both GitHub and Zenodo, and runs on standard Linux/Windows systems (for transmission) and LoRa platforms (for reception). When an attack image or video is played in full-screen mode, it can manipulates the connected VGA or HDMI cable to emit EMR signals that conforms to the LoRa physical layer. These EMR packets can be directly received and decoded by nearby COTS LoRa nodes and gateways, verifying the feasibility of the covert channel.

The artifact is released under the MIT license.

A.2 Description & Requirements

The artifact is organized as a lightweight, self-contained package, and includes the following key components:

- **README.md**: A comprehensive guide to using the artifact. It contains setup instructions, hardware/software requirements, and step-by-step procedures for generating and testing the covert LoRa transmission.
- **EMR Tx/**: This folder contains the core source code written in MATLAB for generating attack images and videos. These media files are designed to modulate secret data onto electromagnetic radiation emitted via the VGA or HDMI cable when displayed on screen. Users can customize transmission parameters, data payloads, and modulation settings through the provided scripts.
- **AttackSamples/**: This folder includes a set of pre-generated images and videos that can be used directly for testing without requiring MATLAB or any code execution. These samples enable quick validation of the covert channel using only a media player and a COTS LoRa receiver.

A.2.1 Security, privacy, and ethical concerns. This artifact does not pose risks to system security, user privacy, or data integrity. However, as it involves the emission of electromagnetic signals that mimic LoRa transmissions, users must take precautions to avoid unintended interference with nearby legitimate LoRa networks.

Users are strongly advised to operate the artifact strictly in accordance with local radio frequency regulations and spectrum laws. The covert transmission should ideally be conducted in controlled, isolated environments (e.g., Faraday cages or shielded labs) to prevent accidental disruption of operational LoRaWAN infrastructure or licensed frequency bands. Alternatively, it may be safely tested in open environments only if it can be reasonably ensured that no operational LoRa networks exist within a 100-meter radius, and that testing does not interfere with nearby wireless services.

No security mechanisms are disabled or bypassed during the use of this artifact. All operations are software-controlled and non-destructive to the host system. Nonetheless, ethical use of this artifact is essential, especially in shared wireless environments.

A.2.2 How to access.

- **Zenodo**: https://doi.org/10.5281/zenodo.15779950
- **GitHub**: https://github.com/XieyangSun/TEMPEST-LoRa
- A **Demo Video** is available at: https://www.youtube.com/watch?v=HDbdAZd6cLw

A.2.3 Hardware dependencies. This artifact requires the following hardware:

- **Transmitter side (Tx)**: A computer with a monitor/projector/TV via VGA or HDMI cable. The display setting is 1080x1920@60Hz.
- **Receiver Side (Rx)**: Any COTS LoRa devices for reception. In our paper, we used (1) SX1262 LoRa node made by Lilygo. (2) SX1302 LoRa gateway made by Waveshare.

A.2.4 Software dependencies. The artifact has the following software dependencies:

MATLAB: Required for running the core transmission scripts in the EMR Tx/ directory, which generate the attack images and videos.

LoRa Receiver Software:

For SX1262 LoRa nodes, users can run a reception program on the Arduino development environments to detect and log incoming LoRa packets. We provide a reference Arduino sketch ('SX1262_Receive_Interrupt.ino' in our artifact) that demonstrates how to configure the node to receive and log packets.

For SX1302 LoRa gateways, the reception relies on standard LoRaWAN gateway software stacks, such as Semtech's packet forwarder, typically pre-installed.

Users do not need to compile any native code for transmission if using the pre-generated media in AttackSamples/, and standard media players (e.g., VLC) can be used for playback.

A.2.5 Benchmarks. None

A.3 Set Up

A.3.1 Installation. To install and verify the artifact, users should follow the steps below. A simple functionality test—generating a LoRa-modulated attack video and setting up a COTS LoRa receiver—can be completed after installation.

1. Install MATLAB and use it to run the most crucial MATLAB script for generating attack videos in the EMR TX/ folder.

2. To receive the LoRa packets emitted from the screen, users should configure COTS LoRa receivers:

- For **SX1262 LoRa Nodes**: We recommend using the RadioLib framework for convenient control of SX1262-based LoRa nodes. Refer to: https://www.ardu-badge.com/RadioLib. If using SX1262 boards from LilyGo, refer to their GitHub repository: https://github.com/Xinyuan-LilyGO/LilyGo-LoRa-Series.

- For **SX1302 LoRa Gateways**: We recommend using Semtech's official SX1302_hal framework to configure the gateway and capture LoRa packets. Refer to: https://github.com/Lora-net/sx1302_hal.

A.3.2 Basic test. First, users should use MATLAB to run the scripts in the EMR TX/ directory in the following order:

(1) **Config = CrossConfigFile.GetInstance**

This script is used to initialize and load global configuration parameters. Users can edit the CrossConfigFile.m script to customize transmission parameters such as frequency, spreading factor (SF), and bandwidth (BW).

(2) **PacketInfo = GetLoRaPacketInfo**

This script is used to load the symbol sequence of the LoRa packet's physical-layer.

(3) **GenerateAttackVideo(PacketInfo, Config)**

This script is used to generate an attack video (named 'Attack-Video.avi') in the current directory.

Then, users should continuously play the generated 'Attack-Video.avi' in full-screen mode on the monitor connected via VGA or HDMI. At the same time, a COTS LoRa node or gateway should be placed nearby and set to receive mode using the corresponding configuration and software.

If the transmission and reception parameters (e.g., frequency, spreading factor, and bandwidth) are correctly matched on both ends, the COTS LoRa device should be able to detect and decode the LoRa packets emitted through electromagnetic radiation from the video cable, confirming the functionality of the covert channel.

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20220926.