Signal Processing 238 (2026) 110201

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Anomalous activity detection using RF emanations☆

Venkatesh Sathyanarayanan [a],*, Peter Gerstoft [b]

[a] Manipal Academy of Higher Education (MAHE), MIT Bengaluru, Bengaluru, Karnataka, 560064, India
[b] University of California San Diego, La Jolla, CA, 92093-0238, USA

ARTICLE INFO

Keywords:
Emanations
Side-channel attacks
RF anomaly
Data security and privacy
Unintended RF emission

ABSTRACT

Electronic activity in digital systems unintentionally emits radio frequency (RF) signals called emanations. These emanations compromise data security, which is important for corporate and military establishments. This work focuses on detecting anomalous activity that compromises data security through emanations. An example of such anomalous activity is emanations from damaged peripherals, such as a mouse or keyboard, which can be used to steal digital data. Prior work on emanation detection uses profiling on specific hardware (HW). However, this is not scalable across all types of HW. We propose a HW-agnostic solution for finding anomalous activity using emanations by scanning the signature of harmonics from leakages of clock signals. An algorithm for multi-harmonic pitch estimation is introduced for wireless applications. A preprocessing technique is developed that removes the effect of artifacts. Thorough mathematical derivations demonstrate the algorithm theoretically. In-phase and Quadrature-phase (IQ) data are collected from emanation sources placed in a shielded room from 0.1–1.1 GHz using software-defined radios (SDR). Results are presented for use cases emulating anomalous activity that compromises data security, such as damaged peripherals and unauthorized data copy onto external devices.

1. Introduction

The digitization of daily life activities has increased the volume of data and complicated the life cycle of data. This complexity has increased the challenges of data security. Data security is important for applications such as cellular wireless networks [1], RF space within sensitive civilian and military establishments [2]. Activities that compromise data security are termed anomalous. This work focuses on detecting anomalous activities using unintended RF emissions called emanations.

Activity within electronic systems results in emanations [3]. If a mapping is found between the emanations and data processed within the electronic system, it makes digital data vulnerable. Other types of emanation signals include power consumption patterns [4], acoustic signals [5], and optical signals [6].

Prior work on emanations [7–9] profiles a specific make and model of HW to learn emanation patterns. They assume knowledge of the specific device in question. The profiling uses classical signal processing and deep learning approaches to map specific types of software activities to received emanations.

We propose identifying anomalous activity that potentially compromises data security due to information leakages using emanations. The prior profiling-based approach is not scalable for anomalous activity detection. This is because it requires learning patterns from all types of HW, makes, and models, which is unfeasible. For example, Ref. [10] profiled a specific type of monitor to decode the data displayed on the screen by capturing emanations at a distance from a different room across walls. Similarly, emanations from keyboards [11] have been profiled to decode the key presses from those specific keyboard types from a distance.

To detect anomalous activity without HW profiling, we scan for a generic signature symptomatic of emanations using classical signal processing techniques. Intentionally transmitted signals such as Wi-Fi, Bluetooth, 4G, and 5G cellular signals, referred to as overt signals, are human-constructed with a regular structure. Spectrum sensing applications exploit this structure to detect and classify signals with known templates [12,13]. Motivated by this, a template of harmonics due to leakages from clock signals is scanned for as a signature of emanations. Clock signals are an essential component of electronic systems [11,14,15]. The generic HW-agnostic signature proposed is a harmonic series in the frequency domain, at pitch frequencies spread across wide bandwidths that are affected by artifacts.

Machine learning (ML) techniques have been used in prior work for finding anomalies [16]. Ref. [1] highlights how ML models can

☆ This work is supported by Intelligence Advanced Research Projects Activity (IARPA), United States, via 2021-2106240007.
* Corresponding author
E-mail address: vesathya@mahe.edu (V. Sathyanarayanan).

https://doi.org/10.1016/j.sigpro.2025.110201
Received 7 April 2025; Received in revised form 25 June 2025; Accepted 7 July 2025
Available online 18 July 2025

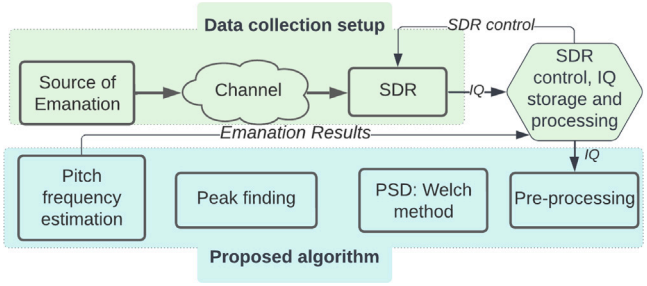


Fig. 1. System block diagram illustrating the high-level modules of data collection setup and proposed algorithm. The emanation is converted into IQ by the SDR and processed by the algorithm. The four steps of the algorithm are illustrated.

Table 1
Abbreviations used and their expansions.

Abbrev.	Expansion	Abbrev.	Expansion
RF	Radio Frequency	HW	Hardware
IQ	In-phase and Quadrature-phase	SDR	Software Defined Radio
PSD	Power Spectral Density	SNR	Signal to Noise Ratio
AWGN	Additive White Gaussian Noise	FFT	Fast Fourier Transform
HDMI	High-Definition Multimedia Interface	USB	Universal Serial Bus
SD	Secure Digital (Card)	CPU	Central Processing Unit
ML	Machine Learning		
$\circledast$	Convolution operator	$\odot$	Hadamard product

be used to detect non-conforming RF signals and thereby identify interference, jamming, and unexpected signal behavior. Ref. [17] uses the RF fingerprinting technique by learning HW fingerprints using semi-supervised ML models to detect anomalies. It achieves state-of-the-art performance with minimal labeled data by using data augmentation within the context of wireless communication signals and combines consistency-based regularization and pseudo-labeling. ML approaches for emanation detection [18,19] are currently not feasible due to the scale of HW and lack of training data. The algorithm in this work uses a classical signal processing techniques that help establish an interpretable baseline upon which we can build ML algorithms in the future.

In any RF environment, ambient emanations from numerous sources form the baseline of the emanation pattern. We detect and characterize all emanations in ambient RF environments across a wide bandwidth to build the baseline set of emanations. A change in the baseline set of emanations is identified as symptomatic of anomalous activity.

The system block diagram in Fig. 1 summarizes the emanation detection algorithm and data collection, an extension of our conference paper [20]. Emanations are transmitted from the source, where harmonic series at different pitches and center frequencies are obfuscated by random frequency shifts referred to as unintended modulation. They further undergo channel and HW artifacts and thermal noise, before being sensed by SDR and converted into IQ samples. This is the first work to showcase profiling-free emanation detection. Therefore, the objective is to showcase the performance of data collected in a controlled environment, such as a shielded room, for a limited set of real-time use cases, backing the theoretical exposition.

An important preprocessing technique is developed to deal with the unintended modulation, channel, and HW artifacts. Derivations describe the removal of artifacts, harmonic structure extraction, finding peaks, and estimating the pitch of harmonics. This is shown for single-harmonic and multi-harmonic cases in the presence of interferences.

The detection of anomalous activity is demonstrated in the following use cases. Due to the wear and tear of electronic equipment such as a mouse or keyboard, there could be leakages compromising data security [11]. This is emulated by exposing a portion of the cable from a mouse and keyboard connected to a laptop and collecting IQ data from the resulting emanations. Compromise of data security is emulated by copying data onto external storage peripherals. These data transfers result in emanations [21]. This is emulated by copying data from a laptop to a secure digital (SD) card and a pen drive, and IQ samples captured from resulting emanations.

The IQ data is captured across 0.1–1.1 GHz, split into 25 MHz slices and processed separately in each slice. The resulting emanation pattern across the entire frequency range consists of emanations detected from each slice. Emanation patterns for IQ from damaged peripherals are compared with the baseline of an idle laptop only to detect anomalous activity. An organization could use the proposed algorithm to detect anomalous activities. Note that the list of abbreviations used are in Table 1.

The major contributions of this paper are as follows:

- A profiling-free, HW agnostic emanation detection is achieved by scanning for a harmonic signature instead of profiling of specific HW make and model, as in prior work.
- Thorough mathematical derivations are provided, showcasing the theoretical basis of the proposed algorithms: removal of artifacts using the preprocessing technique, finding peaks, and estimating pitch frequency.
- A custom preprocessing technique is introduced that removes unintended modulation, channel, and HW artifacts while retaining harmonic structure.
- An algorithm is introduced for multi-harmonic pitch detection for wireless applications.
- Anomalous activity detection is showcased on wideband IQ data collected in a shielded room from 0.1–1.1 GHz. This is showcased for the use cases: wear and tear of electronic devices, leaking information, and unauthorized copying of data to external storage devices.

2. Method

To identify anomalous activity, emanations are detected by scanning for harmonic signatures in the frequency domain. The high-level details of the emanation detection algorithm are in the flow chart in Fig. 2. Models are presented for emanation signal, unintended modulation of emanation, and artifacts it undergoes in Sections 2.2, 2.3, and 2.4. The harmonic signature x_{sh} in the time domain [22, Eq. (1.1)] is:

$$x_{\text{sh}}[n] = \sum_{m=1}^{M} \alpha_m \exp(j w_h m n),\ n \in [0, \dots, N-1], \tag{1}$$

where $\alpha_m \in \mathbb{C}$ is the complex amplitude, w_h pitch frequency, M is the number of harmonics, and N is the number of samples. The Fourier transform of x_{sh} is:

$$X_{\text{sh}}(w) = \sum_{m=1}^{M} \alpha_m \delta(w - m w_h). \tag{2}$$

Frequency in radians w is used in equations for conciseness, and frequency in Hz f is used in plots for ease of interpretation. The pitch frequency in radians w is related to physical frequency in Hz f as [22, Eq. (1.4)] $w = 2\pi f / f_s$, where f_s is the sampling rate.

The harmonic signature x_{sh} undergoes unintentional modulation within the HW from where emanations are transmitted with unknown frequency shifts w_d characteristic of the physics of the HW [15]. This is modeled as x_{tx}:

$$x_{\text{tx}}[n] = x_{\text{sh}}[n] \sum_{d=1}^{D} \alpha_d \exp(j w_d n), \tag{3}$$

where w_d, α_d are the dth frequency and complex amplitude shifts applied due to unintended modulation, and D is the total number of frequency shifts. The emanation signal x_{tx} transmitted from HW undergoes channel h, HW artifacts β and thermal noise w, and received as IQ samples y ($\circledast$ is the convolution operator):

$$y[n] = (x_{\text{tx}} \circledast h)[n] \exp(j\beta[n]) + w[n]. \tag{4}$$

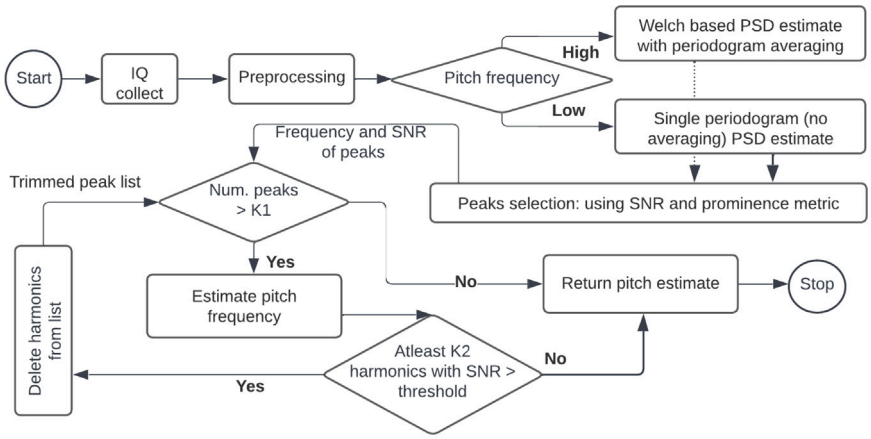


Fig. 2. Algorithmic flowchart of emanation detection.

2.1. Approach for pitch detection

The received IQ samples are a function g of complex amplitude and pitch frequency of harmonics α_m, w_h, complex amplitude and frequency shifts of unintentional modulation α_d, w_d, channel artifact h, HW artifact β, and thermal noise w:

$$\boldsymbol{y} = g\left(\alpha_m, w_h, \alpha_d, w_d, h, \beta, w\right), \tag{5}$$

where $\boldsymbol{y} = [y[0], \ldots, y[N-1]]^T$. The goal is to estimate w_h given the IQ samples y parameterized by the parameters:

$$w_h = g^{-1}\left(\boldsymbol{y}; \alpha_m, \alpha_d, w_d, h, \beta, w\right). \tag{6}$$

This amounts to the detection of an emanation.

To detect the emanation, we introduce multi-harmonic pitch detection for wireless applications, motivated by [23]. Our application requires detecting and characterizing emanations from multiple sources simultaneously, and there could be interference due to overt signals. The proposed algorithm addresses these requirements. It also handles the shortcomings in prior work, which are highlighted below. The function g^{-1} is thus approximated by the series of steps that are part of the proposed algorithm: preprocessing, Welch-based Power Spectral Density (PSD) estimate, peak detection, and pitch frequency estimation.

Pitch estimation is used in many applications such as source separation, enhancement of audio effects, biomedicine, and mechanics. Techniques such as cross-correlation [24] use a similarity measure to estimate the pitch frequency. Frequency domain techniques include cepstrum [25] using a dual transform for estimation. Techniques based on parametric estimation theory, as maximum likelihood [26] and maximum a posteriori [27], have been explored. Techniques using notch filters at frequencies of harmonics to suppress them and minimize the overall output power are in [22].

These approaches assume some of the following in their signal model that limits their application: assumption of white or colored Gaussian noise only and no consideration of channel and clock artifacts, knowledge of the number of sources and number of harmonics in each source, and an equal number of harmonics in each source. These techniques are built for audio and are computationally not feasible for wireless systems with high sample rates. Further, communication systems have reference signals to alleviate artifacts caused by the channel, HW, and thermal noise. Emanations are unintentionally generated signals with no reference signals. In addition, emanations are weak signals, unlike communication signals that are boosted by power amplifiers [28]. This makes it difficult to estimate the pitch frequency from the IQ samples received.

In this work, each IQ capture is processed with a 25 MHz bandwidth and a 100 ms duration, giving an IQ length of $N = 2.5 \times 10^6$. This is very high compared to the 44.1 kHz sample rate used in audio applications. In [22], techniques such as the non-linear square, subspace-based MUSIC, and filtering-based Capon method operate on matrices of dimension $O(N)$, where N is IQ length. In wireless applications where N is in the millions, these techniques are unfeasible.

The preprocessing introduced is an important contribution, since it removes artifacts and retains the harmonic structure in the frequency domain. The preprocessing on IQ samples results in s:

$$s[n] = \sum_m \gamma_m \exp(j w_h m n) + z[n], \tag{7}$$

where $\gamma_m \in \mathbb{C}$, z represents thermal noise and interferences due to cross-terms.

This is extended to a use case where multiple emanations are present, resulting in multi-harmonics in the received signal. In the multi-harmonic case, the y from (4) is extended to multiple receive emanations as follows. Each harmonic series undergoes unintentional modulation at the emanation source, channel, and HW artifacts. They are combined at the receiver with thermal noise $\boldsymbol{w}_{\text{mh}}$ resulting in received IQ signal $\boldsymbol{y}_{\text{mh}} = [y_{\text{mh}}[0], \ldots, y_{\text{mh}}[N-1]]^T$ as:

$$\boldsymbol{y}_{\text{mh}} = \sum_{k=1}^{K} \boldsymbol{y}_k + \boldsymbol{w}_{\text{mh}}, \tag{8}$$

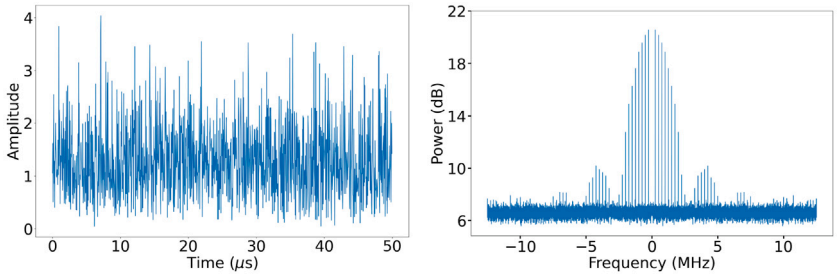
where K is the number of emanations. Derivations are introduced to show preprocessing removes artifacts for single and multi-harmonic use cases in Section 2.5. In Section 2.6, the algorithm deals with overt signals interfering with emanations.

Synthetically generated emanation signatures with AWGN noise added are in Fig. 3. The time domain signal has no visible signatures, but the frequency domain shows a harmonic signature. Thus, a PSD estimate is taken to move to the frequency domain to find emanations.

The Welch method is used to estimate the PSD of the preprocessed signal, see Section 2.7. Periodogram averaging reduces signal variance and improves the subsequent peak-finding. Dominant peaks are identified using SNR thresholding and prominence-based parameterless distance separation, see Section 2.8. SNR thresholds are computed based on the signal variance estimates of the IQ samples. The frequency and SNR of dominant peaks are used to estimate the pitch frequency of each emanation, see Section 2.9.

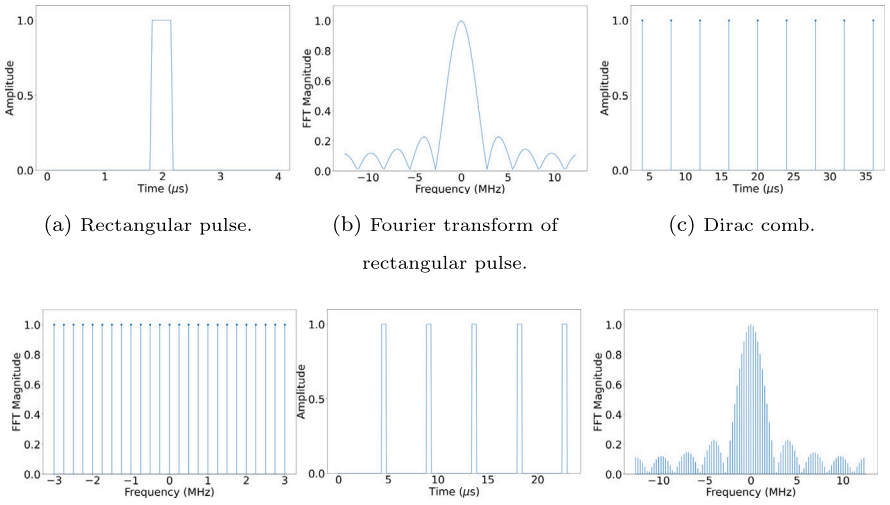
2.2. Harmonic signal model

Models for the harmonics are provided for the signal, modulation, and artifacts to derive algorithm performance. Devices with microprocessors generate periodic carrier and clock signals. These have sharp transitions and are approximated as a periodic pulse train [11,14,15].



(a) Time domain. (b) Frequency domain.

Fig. 3. Synthetically generated noisy emanation signature in time and frequency domain. AWGN noise is added. The harmonic signature is only visible in the frequency domain. This motivates the processing of the algorithm to estimate harmonics in the frequency domain.



(a) Rectangular pulse. (b) Fourier transform of rectangular pulse. (c) Dirac comb.

(d) Fourier transform of Dirac comb. (e) Pulse train. (f) Fourier transform of pulse train.

Fig. 4. A rectangular pulse with a duration of 0.5 μs in (a) and its Fourier transform in (b). The main lobe width is $1/T$, where T is the pulse duration. A Dirac comb in (c) at 250 kHz fundamental frequency. Its Fourier transform in (d) is also a Dirac comb. Convolution of a rectangular pulse with a Dirac comb is a pulse train in (e) at 250 kHz frequency, duty cycle T/T_h of 0.1, and its Fourier transform in (f) is a sampled sinc function. The magnitude of the Fourier transforms is normalized.

A rectangular pulse $p[n]$ with width T is

$$p[n] = \begin{cases} 1 & |n| < \frac{T}{2T_s} \\ 0 & \text{otherwise,} \end{cases} \tag{9}$$

where T_s is the sampling instant. Its Fourier transform is a sinc function:

$$P(w) = T\frac{\sin\left(\frac{wT}{2T_s}\right)}{\frac{wT}{2T_s}} = T\,\text{sinc}\left(\frac{wT}{2T_s}\right). \tag{10}$$

A Dirac comb or Shah function is:

$$\text{Ш}[n] = \sum_{m=-\infty}^{\infty} \delta(nT_s - mT_h), \tag{11}$$

where T_h is the periodicity, whose Fourier transform is:

$$\text{Ш}(w) = \sum_{m=-\infty}^{\infty} \delta(w - mw_h), \tag{12}$$

where $w_h = 2\pi/T_h$ is the pitch frequency. The time domain convolution of the rectangular pulse with the Dirac comb is a pulse train:

$$x[n] = p[n] \circledast \text{Ш}[n] = \sum_{m} \text{Ш}(nT_s - mT_h), \tag{13}$$

whose frequency transform is:

$$X(w) = P(w)\text{Ш}(w) = T\,\text{sinc}\left(\frac{wT}{2T_s}\right) \sum_{m=-\infty}^{\infty} \delta(w - mw_h). \tag{14}$$

Thus, we get a sampled sinc function in the frequency domain. The rectangular function $p[n]$ and its Fourier transform $P(f)$ from (9) (10) are illustrated in Figs. 4(a), 4(b). Further, Dirac comb $\text{Ш}[n]$ and its Fourier transform $\text{Ш}(f)$ from (11) and (12) are in Figs. 4(c), 4(d). The rectangular pulse $p[n]$ is convolved with the Dirac comb $\text{Ш}[n]$ to obtain a rectangular train $x[n]$. The rectangular train $x[n]$ and its Fourier transform $X(f)$ from (13) and (14) are in Figs. 4(e), 4(f).

A generic signal model for a single harmonic series x_{sh} (1) is used in this work, and it captures the harmonic pattern of the pulse train in (13).

2.3. Transmit emanation model

The harmonic signature undergoes unintended modulation that is characteristic of the physics of the HW and unknown to us. This is captured in the transmit emanation model in this section. In a digital communication system, signal modulation is defined as follows: the binary sequence to be transmitted is parsed into subsequences of length K_m, indexed by i. Each subsequence is mapped into a waveform x_i. In a frequency modulation scheme, a frequency shift w_i is applied to a carrier frequency w_c: [29, Eq. (4.8)]:

$$x_i[n] = \exp\left(j\left(w_c + w_i\right)n\right), \quad 1 \le i \le 2^{K_m}, \tag{15}$$

where 2^{K_m} is the number of waveforms, $n \in [0, \ldots, N-1]$. In contrast to modulation in a digital communication system, unintended modulation occurs on emanation signals. Signal generation circuits of a

processor generate periodic clock signals that act as a carrier. Due to space constraints, signal generation and data processing circuits are in proximity, leading to unintentional modulation of carrier signals [14]. Activities in desktops and laptops modulate the clock signals and apply specific frequency shifts unknown to the user [15,30]. Examples of activities are based on processor and memory activities. A program is run at an alternating period T_d to achieve a frequency modulation of w_d. Such unintentionally modulated emanation signal with unknown frequency shifts w_d of the harmonics x_{sh} is modeled as x_{tx}, see (3). The preprocessing operation in Section 2.5 is shown to remove the effect of frequency modulation w_d, see (B.6). Expanding x_{tx} by inserting (1) into (3) gives:

$$x_{\text{tx}}[n] = \sum_m \alpha_m \sum_d \alpha_d \exp(j(mw_h + w_d)n). \tag{16}$$

2.4. Receive emanation model

The transmitted emanation further undergoes HW, channel artifacts, and thermal noise. The transmit emanation source and receive HW are considered static, and the channel is time-invariant. Transmit emanation x_{tx} impacted by channel impulse response h becomes x_{ch}:

$$x_{\text{ch}}[n] = (x_{\text{tx}} \circledast h)[n], \tag{17}$$

Inserting (16) into (17) x_{ch} becomes:

$$x_{\text{ch}}[n] = \sum_m \sum_d h_{m,d}\alpha_m\alpha_d \exp(j(mw_h + w_d)n), \tag{18}$$

see derivations in Appendix A. This also describes how the channel artifacts are removed.

The channel artifacts, time-variant clock artifact, and thermal noise impact of transmit emanation, resulting in received IQ samples as follows:

$$\boldsymbol{y} = \boldsymbol{v} + \boldsymbol{w}. \tag{19}$$

where $\boldsymbol{y} = [y[0], \dots, y[N-1]]^T$ is emanations impacted by channel and clock artifacts $\boldsymbol{v} = [v[0], \dots, v[N-1]]^T$, and thermal noise $\boldsymbol{w} = [w[0], \dots, w[N-1]]^T$, such that $\boldsymbol{y}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^N$.

Emanation impacted by channel and clock artifacts $\boldsymbol{v}$ result in the Hadamard product ($\odot$) between clock artifacts $\boldsymbol{c}$ and emanation impacted by the channel $\boldsymbol{x}_{\text{ch}}$:

$$\begin{aligned} \boldsymbol{v} &= \boldsymbol{c} \odot \boldsymbol{x}_{\text{ch}}, \boldsymbol{x}_{\text{ch}} = [x_{\text{ch}}[0], \dots, x_{\text{ch}}[N-1]]^T, \\ \boldsymbol{c} &= [\exp(j\beta[0]), \dots, \exp(j\beta[N-1])]^T, \end{aligned} \tag{20}$$

where $\beta[n] = w_e[n]n + \theta_e[n]$ [31, pg. 360], w_e, θ_e frequency and phase errors due to imperfect time-variant clocks. Combining (18), (19), (20), receive IQ y is expanded as:

$$y[n] = \sum_m \sum_d h_{m,d}\alpha_m\alpha_d \exp(j(mw_h + w_d + w_e[n])n) \exp(j\theta_e[n]) + w[n]. \tag{21}$$

Expanding y_{mh} from (8) following (21):

$$y_{\text{mh}}[n] = \sum_k \sum_m \sum_d h^k_{m,d}\alpha^k_m\alpha^k_d \exp(j(mw^k_h + w^k_d + w^k_e[n])n + j\theta^k_e[n]) + w_{\text{mh}}[n]. \tag{22}$$

Note that the expression for both single and multi-harmonic cases y, y_{mh} contains the harmonics at pitch frequency w_h, w^k_h obfuscated by unintended modulation, channel, clock artifacts, and AWGN noise.

2.5. Preprocessing

A mathematical representation has been provided on how the harmonics undergo modulation and artifacts to result in received IQ samples y. The samples received y are processed to extract one or more harmonic series. This section shows that preprocessing removes the effect of modulation, channel, and clock artifacts and helps extract the harmonics.

Preprocessing takes the product of each IQ sample y with its complex conjugate y^*:

$$s[n] = y^*[n]y[n]. \tag{23}$$

This is equivalent to a matched filter [29, Eq. (3.56)] in the frequency domain:

$$\begin{aligned} S(w) &= Y^*(w) \circledast Y(w) = \sum_{w_1} Y^*(w_1)Y(w - w_1) \\ &= \sum_{w_1} Y^*(w_1)Y(-(w_1 - w)), \end{aligned} \tag{24}$$

where $Y(w)$ the Fourier transform of y is correlated against its frequency-reversed copy $Y(-w)$. This preprocessing operation is computationally simple. It is motivated by the time domain auto-correlation used in pitch estimation in audio.

The preprocessing operation on y results in the following, see Appendix B for derivations.

$$s[n] = \sum_m \gamma_m \exp(jw_h mn) + z[n], \tag{25}$$

where $\gamma_m \in \mathbb{C}$, z contains noise and interferences due to cross terms. Its Fourier transform is:

$$S(w) = \sum_m \gamma_m \delta\left(w - mw_h\right) + Z(w), \tag{26}$$

where Z is the Fourier transform of z. The expression of receive IQ y in (21) contains artifacts that obfuscate the harmonics. With preprocessing, the artifacts are removed, and harmonics at the pitch frequency w_h are extracted in (25). The PSD of y and s for real IQ data illustrate this, see Figs. 5(a), 5(b).

Further, preprocessing helps remove artifacts for the multi-harmonic use case. Following derivations similar to preprocessing for a single harmonic case, it is shown in Appendix C that preprocessing over y_{mh} gives s_{mh} as:

$$s_{\text{mh}}[n] = y^*_{\text{mh}}[n]y_{\text{mh}}[n] = \sum_k \sum_m \gamma^k_m \exp(jw^k_h mn) + z_{\text{mh}}[n], \tag{27}$$

where $\gamma^k_m = \sum_d \gamma^k_{m,d}$, z_{mh} contains noise and interferences due to cross-terms. Fourier transform of s_{mh} gives:

$$S_{\text{mh}}(w) = \sum_k \sum_m \gamma^k_m \delta(w - mw^k_h) + Z_{\text{mh}}(w), \tag{28}$$

where Z_{mh} is the Fourier transform of z_{mh}. The expression of receive IQ y_{mh} in (22) contains artifacts that obfuscate the harmonics. With preprocessing, the artifacts are removed, and harmonics at the pitch frequency w^k_h are extracted in (27).

2.6. Overt signals

Overt signals x_o are added to the multi-harmonic signal model in (8) to study the impact of overt on pitch estimation. Overt signal that undergoes channel and clock artifacts is expanded using (17), (19), and (20):

$$y_o[n] = \exp(j\beta[n])\left(x_o \circledast h\right)[n]. \tag{29}$$

Combining $\boldsymbol{y}_o = [y_o[0], \dots, y_o[N-1]]^T$ with received emanations $\boldsymbol{y}_k$ and thermal noise $\boldsymbol{w}_{\text{mh}}$, the received IQ $\boldsymbol{y}$ is:

$$\boldsymbol{y} = \sum_{k=1}^{K} \boldsymbol{y}_k + \boldsymbol{y}_o + \boldsymbol{w}_{\text{mh}}. \tag{30}$$

Applying preprocessing on receive IQ $\boldsymbol{y}$ following derivations of the multi-harmonic case, it can be shown that this term results in a harmonic pattern only if the overt signal has a harmonic pattern, see Appendix D for details. Typically, overt signals do not have a harmonic pattern as the signature in the frequency domain, except for the On-Off-Keying modulation signal that is not widely used in digital communication systems [29, pg. 175].

2.7. Power spectral density estimation

Dominant peaks are identified in the PSD of the preprocessed signal. The frequency and SNR of the dominant peaks are used to estimate the pitch in Section 2.9. Large signal variance results in picking false peaks and missing true peaks, which impacts pitch frequency estimation. PSD is estimated using the Welch method, that helps reduce the signal variance. The description follows the Welch method in [32, pg. 730]. The time series is divided into smaller segments, and their modified periodograms are averaged to reduce variance. The Welch PSD $P_s(w_l)$, with periodogram averaging over N_s segments, each of length L, such that total sample length $N = LN_s$, has variance reduced by the factor N_s:

$$Var(P(w_l)) = \frac{1}{N_s} Var(P_s(w_l)), \tag{31}$$

where $P_s(w_l)$ is the PSD of $s_{\text{mh}}[n]$ (27) without periodogram averaging.

For fixed-length IQ samples, there is a tradeoff between frequency resolution and signal variance. The frequency resolution is equal to the main lobe width of the Kaiser window $w_{\text{res}} = \frac{2\pi}{L}\sqrt{1+\beta/\pi^2}$, where β is the kaiser window parameter. Consider adjacent peaks that are part of a harmonic series as $(m+1)w_h$ and mw_h for $\forall m$, their separation is w_h. The condition to resolve adjacent peaks is:

$$w_h \geq w_{\text{res}} = \frac{2\pi}{L}\sqrt{1+(\beta/\pi)^2}. \tag{32}$$

Thus, the window length L restricts the detectability of the pitch frequency w_h. Periodogram averaging increases frequency resolution w_{res} by a factor $\frac{N}{L}$. To detect pitch frequency below w_{res}, a modified periodogram without averaging, is computed on s_{mh} at frequencies $w_n = \frac{2\pi n}{N}$, $n \in [0, N-1]$. Computing Welch PSD over s_{mh} from (27):

$$P(w_l) = \sum_k \sum_m \eta_m^k \delta(w_l - mw_h^k) + P_z(w_l), \tag{33}$$

where $P_z(w_l)$ represents non-harmonic terms, η_m^k is the power of the harmonic peaks.

2.8. Peak finding

This section describes the identification of peaks in the PSD of the preprocessed signal. Peak detection is extensively used in biomedical signal processing [33,34]. Peaks are commonly identified by searching for local maxima whose SNR exceeds a threshold. Biomedical signal peaks have specific patterns that are utilized to estimate the noise floor and SNR accurately [34]. In this work, a robust and generic percentile-based approach is used to estimate the noise floor and threshold which does not assume a specific model for signal peaks.

The frequency and SNR of the detected peaks are passed to the subsequent pitch frequency estimation block. The peaks with SNR exceeding a given threshold are picked. They are pruned further using the prominence metric. To handle a non-flat noise floor, the spectrum is split into N_f narrow frequency slices of length $L_f = L/N_f$, where L number of samples in PSD. The PSD in dB of ith frequency slice out of L slices is:

$$P^i_{\text{dB}}(w_l) = P_{\text{dB}}(w_{(i-1)L_f+l}), \quad l \in [0, L_f - 1], \tag{34}$$

where $P_{\text{dB}}(w_l) = 10\log_{10} P(w_l)$. The noise floor of ith slice NF_i is the median of $P^i_{\text{dB}}(w_l)$. The threshold is calculated based on the estimated standard deviation σ of signal power around the median. Assuming a Gaussian noise distribution, the estimated standard deviation for the ith frequency slice is calculated:

$$\sigma_i = (\text{PCT}(P^i_{\text{dB}}, 84\%) - \text{PCT}(P^i_{\text{dB}}, 16\%))/2, \tag{35}$$

where PCT is the percentile function. There could be parts of the spectrum with stronger interferences and overt signals. A median is taken for estimated standard deviations across frequency slices:

$$\sigma_t = \text{PCT}([\sigma_1, \ldots, \sigma_{N_f}], 50\%). \tag{36}$$

The presence of overt signals and interferences would bias the noise floor and standard deviation calculation. Preprocessing removes the effect of overt signals occupying large frequency bands and thus aids in an accurate estimate.

Points of local maxima are identified at frequencies w_p, and their SNR is:

$$\text{SNR}(w_p) = P_{\text{dB}}(w_p) - \text{NF}_i, \tag{37}$$

where i is the frequency slice containing w_p. These peaks at w_p are trimmed based on SNR exceeding the threshold as $\text{SNR}(w_p) > 2n_\sigma\sigma_t$, where n_σ is a hyper-parameter chosen empirically.

Peaks filtered by the SNR threshold might have false peaks close to a true peak. Explicitly specifying a distance separation is not robust, as the pitch frequency could vary across frequencies. The prominence metric is a parameterless minimum distance separation to filter false peaks close to a true peak. This metric is also popularly used in biomedical [35] and speech signal processing [36]. The peak prominence is its height relative to the lowest contour line:

$$\text{Prominence}(w_p) = P_{\text{dB}}(w_p) - P_{\text{dB}}(w_{\text{prom}}) \tag{38}$$

where w_{prom} is calculated as:

$$w_{\text{prom}} = \underset{w_m}{\text{argmax}}\{P_{\text{dB}}(w_m) : P_{\text{dB}}(w_m) \leq P_{\text{dB}}(w_p)\}, \tag{39}$$

and w belongs to a set of points of local minima:

$$w_m \in \{w : P_{\text{dB}}(w - w_l) \geq P_{\text{dB}}(w) \leq P_{\text{dB}}(w + w_l)\}\ . \tag{40}$$

2.9. Pitch frequency estimation

The frequency and SNR of dominant peaks are used to find the pitch frequency. There could be no harmonic series, single, or multiple. The pitch frequency estimation in [23] is generalized to detect multiple harmonic series.

The measured multiples are the peaks w_p identified in the PSD of preprocessed IQ in Section 2.8. PSD is assumed to contain peaks at harmonics that are integral multiples of the pitch at w_h^k of the kth emanation source, referred to as predicted multiples. The set of measured multiples $\mathcal{M} = w_p : \forall p$ is assumed to include K series of harmonics from K sources of emanations:

$$\mathcal{M} = F_1 \bigcup F_2 \bigcup \ldots \bigcup F_K \bigcup F_p, \tag{41}$$

where $F_k = mw_h^k : m \in [1, \ldots, M]$ is the set of harmonics for kth source, F_p is the set of false peaks due to noise, interferences, spectral leakage, etc.

An iterative process estimate pitch w_h^k of kth emanation source as:

$$w_h^k = \underset{w}{\text{argmin}}\ \mathcal{L}(w), \quad w \in \mathcal{S}_w. \tag{42}$$

where w is the frequency, $\mathcal{S}_w$ the frequency search space. The loss function $\mathcal{L}(w)$ considers the following factors: higher loss for a larger difference in frequency between predicted and measured multiple, higher loss for lower SNR valued measured multiple. A measured multiple is considered part of the harmonic series if within a threshold percentage error pt of the predicted multiple:

$$F_k = \{w_p : \left|w_p - mw_h^k\right| \leq \frac{\text{pt}}{100} w_h^k\}. \tag{43}$$

Set of measured multiples is updated as $\mathcal{M} \equiv \mathcal{M} - F_k \equiv \{w \in \mathcal{M} : w \notin F_k\}$. Pitch frequency estimation for a new harmonic series w_h^{k+1} is thus iteratively attempted on the updated set $\mathcal{M}$.

The list of multiples F_k is removed from $\mathcal{M}$ and pitch frequency estimation of w_h^{k+1} is again attempted on the set of peaks $\mathcal{M} - F_k \equiv \{w \in \mathcal{M} : w \notin F_k\}$. This process is recursive until the pitch corresponding to each of the K sources is estimated. The loss function is calculated as follows:

$$\mathcal{L}(w) = L_{\text{pm}}(w) + \alpha_w L_{\text{mp}}(w), \tag{44}$$

where L_{pm} is the cumulative error in matching predicted to measured multiples, L_{mp} measured to predicted multiples, α_w weight given to L_{mp}.

The loss L_{pm} is computed by iterating over predicted multiples, penalizing the mismatch to its closest measured multiple:

$$L_{\text{pm}}(w) = \sum_{n=1}^{N_f} \frac{\left|nw - w_{p_n}\right|}{(nw)^{q_1}} \left(1 + q_2 (A_{p_n})^{q_3}\right), \tag{45}$$

where q_1, q_2, q_3 are hyper-parameters chosen empirically, A_{p_n} is SNR of peak w_{p_n}, $N_f = \frac{max(\mathcal{M})}{w}$. The index of measured multiple p_n, closest to a predicted multiple at nw is:

$$p_n = \underset{p}{\text{argmin}} \left|nw - w_p\right|. \tag{46}$$

Since iteration is upon predicted multiples, there is no penalty for unaccounted measured multiples $\mathcal{M} - F_k \equiv F_{k+1} \bigcup \ldots \bigcup F_p$ in the loss function L_{pm}. These are instead considered in L_{mp}. The unaccounted measured multiples are due to the presence of multiple sources of emanations and false peaks. Similarly, L_{mp} does not penalize for unaccounted predicted multiples. The unaccounted predicted multiples occur due to the low SNR of the corresponding measured multiples. These measured multiples are not picked in the peak finding block described in Section 2.8 due to low SNR. The low SNR could be due to factors such as the nature of the emanation, high noise, and interferences. The loss functions are combined in (44) to estimate the pitch.

The loss function L_{mp} iterates over the measured multiple, penalizing the mismatch with the closest predicted multiple:

$$L_{\text{mp}}(w) = \sum_{p=1}^{P} \frac{\left|n_p w - w_p\right|}{(w_p)^{q_1}} \left(1 + q_2 (A_p)^{q_3}\right), \tag{47}$$

where A_p is SNR of peak w_p, the index of predicted multiple n_p closest to the measured multiple w_p is:

$$n_p = \underset{n}{\text{argmin}} \left|nw - w_p\right|. \tag{48}$$

The derivations demonstrate the theoretical performance of the algorithm. The computational complexity of the four steps of the algorithm is now discussed. The preprocessing step has time complexity $O(N)$, where N is the number of raw IQ samples. The second step of Welch PSD estimation is a standard operation with time complexity $O(L \log L)$, where L is the number of samples per periodogram. The PSD output of length L is split into slices of length L_f in the third step of peak finding. This step has a time complexity of $O({L_f}^2)$. The hyperparameter n_σ in Section 2.8 decides the number of peaks detected, which impacts the computational load of the pitch estimation. The prominence metric used in peak finding has $O(L_f)$ time complexity, helps filter false peaks, and reduces the computation of pitch estimation. The final step of pitch estimation has a time complexity of $O(P^2)$, where P is the length of points in the search space grid. A two-stage approach of coarse and fine grid search is introduced to reduce computation. The values L, L_f, n_σ, and P can be tuned to improve the computational performance with a tradeoff in performance.

3. Experimental setup

The Signal Hound SDR captures IQ samples from sources of emanation inside a shielded room. An antenna is placed inside the room about 2.5 m away from the emission source. To ensure no emanations due to the SDR, both the SDR and the laptop controlling the SDR are placed outside the room. The setup is sanitized by collecting IQ from an empty room and confirming no emanations were detected when passed through the algorithm.

Sources of emanation of interest are placed inside a shielded room, with parameters of IQ capture in Table 2. The 200 MHz is the maximum bandwidth capture for the Signal Hound SDR and is split into 25 MHz slices that are processed. The choice of 25 MHz processing bandwidth and 100 ms capture duration is a balance between computational load and algorithm performance: Fixing the capture duration, a larger processing bandwidth means more samples and computation but restricts the highest pitch frequency of the harmonics that can be estimated. Similarly, fixing processing bandwidth and increasing the duration of capture increases SNR gains obtained from periodogram averaging, see Section 2.7, but increases computational load.

Table 2
Parameters used.

Type	Details
IQ	Freq. captured: 0.1–1.1 GHz, Bandwidth and duration of IQ capture: 200 MHz (max bandwidth of SDR) and 100 ms, Bandwidth and duration of input to the algorithm: 25 MHz and 100 ms.
PSD	Ensemble duration: 1 ms, 75% overlap, Window: Kaiser with beta of 10.
Pitch freq. estimation	Error threshold: 10% for pitch freq. < 500 Hz and 2% otherwise, $q_1 = 0.5$, $q_2 = 1$, $q_3 = -1$, $\alpha_w = 10^{-3}$ for high pitch, 100 for low pitch, $n_\sigma = 2$.

4. Results

The focus is on finding anomalous activities by learning and tracking emanation patterns. Emanations identified from narrow frequency slices are grouped to build the emanation pattern. A change in the pattern from baseline is a potential anomalous activity. In this section, the algorithm from Section 2 is verified on real IQ data. The performance is demonstrated first on a single frequency slice for the case of a laptop connected to a monitor, highlighting algorithm performance in a step-by-step manner. This is followed by learning emanation patterns across a 1 GHz bandwidth for a laptop and a desktop connected to a monitor, and for IQ collected from cases emulating anomalous activity.

An emanation corresponds to a harmonic series with a pitch at f_1. There could be multiple emanations corresponding to multiple harmonic series with pitch at f_1, f_2, etc. Physical frequency f is more intuitive and used in illustrations, compared to the frequency in radians in Section 2.

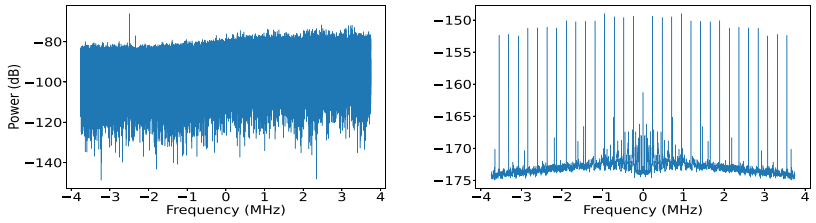
The algorithm is demonstrated step-by-step for a laptop connected to a monitor via a USB-C to HDMI adaptor. The PSD with and without preprocessing illustrates the effect of removing artifacts. The PSD of the raw IQ is in Fig. 5(a) with no visible signatures. In Section 2.5, preprocessing is shown to deal with artifacts. PSD on preprocessed signal is in Fig. 5(b). Notice the peaks with harmonic patterns after preprocessing, similar to the form in (28). There are one or more harmonic series in the PSD that can be estimated.

In the PSD, peaks are detected using the algorithm in Section 2.8, the challenge is to detect peaks in the presence of noise. This is done by finding local maxima in the PSD whose SNR exceeds a threshold, these are calculated from PSD using (36) and (37). Further prominence as a distance-based metric removes false peaks. Peaks thus identified are shown in Fig. 5(c).

The detected peak frequency and SNR are fed to the subsequent pitch frequency estimation block in Section 2.9. The loss function is computed for every candidate pitch frequency from the frequency search space, see (44), (45), and (47). Pitch is estimated as the frequency where the loss function is minimum. Harmonics of the estimated pitch are estimated using (43). The pitch is valid only if at least 5 harmonics are identified using (43). The pitches and corresponding harmonics are in Fig. 5(d). The IQ capture from 125 to 150 MHz contains pitch at frequencies 236 kHz and 365 kHz.

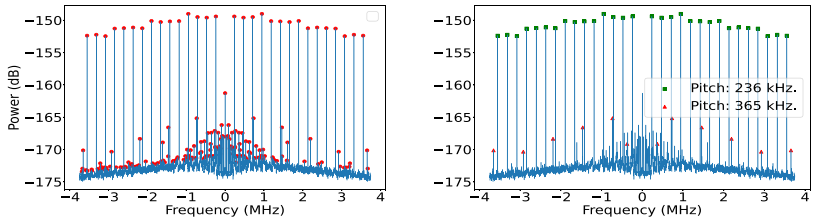
The algorithm is stress tested by synthetically adding AWGN noise w_s at various SNRs, to the received signal y:

$$\boldsymbol{y}_s = \boldsymbol{y} + \boldsymbol{w}_s. \tag{49}$$



(a) PSD of IQ without preprocessing. A noise-like signal is observed.

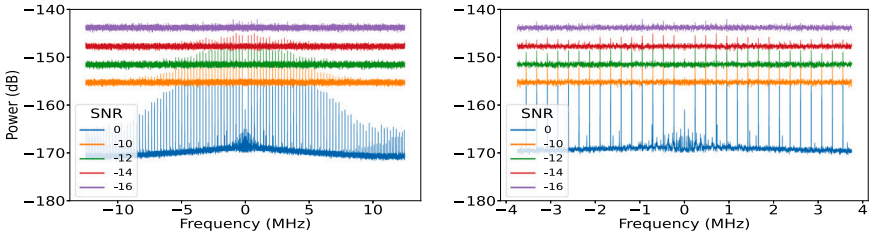
(b) PSD of IQ with preprocessing. A clear harmonic pattern with prominent peaks is observed.



(c) Peaks are identified and overlayed on PSD.

(d) Harmonics of estimated pitches at 236 and 365 kHz are overlayed on PSD.

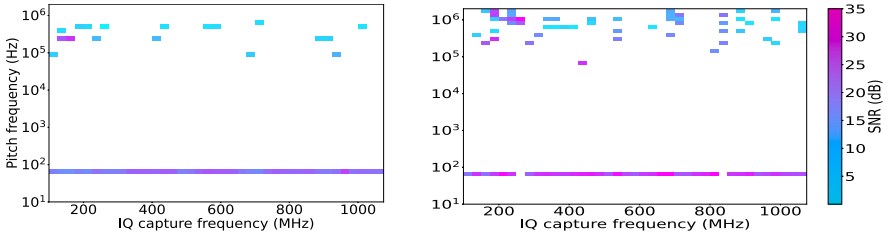
Fig. 5. Emanations from a laptop connected to a monitor via an HDMI to USB-C adaptor, the center frequency is 137.5 MHz. The bandwidth of IQ samples processed is 25 MHz. However, the plots are zoomed in x-axis for clarity of illustration.



(a) PSD at various SNRs.

(b) Zoomed at 30%.

Fig. 6. PSD of preprocessed IQ, highlighting the impact of noise on peaks. Thermal noise is synthetically added at specified SNR levels to IQ from emanations of a laptop connected to a Monitor. Emanations are detected up to SNR as low as −14 dB.



(a) Laptop to Monitor.

(b) Desktop connected to a monitor via an HDMI to USB-C adaptor

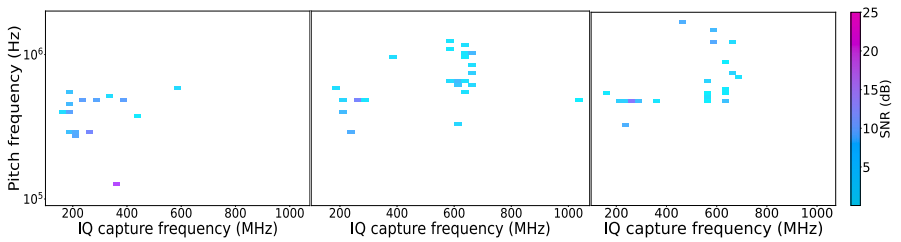
Fig. 7. Illustration of emanation patterns. Emanations detected in each of the 25 MHz slices of IQ data are plotted. The x-axis represents the center frequency at which IQ samples are captured, y-axis represents the pitch frequency of detected emanations. The colormap is the SNR of the pitch. The desktop has central-processing-unit (CPU) intensive processes running, resulting in more emanations with higher SNR spread across wider capture frequencies, compared to a laptop.

The SNR is defined as:

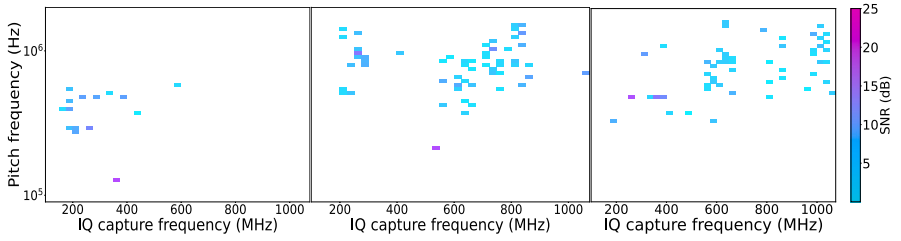
$$\text{SNR} = 10\log_{10}\left(\|\boldsymbol{y}\|^2/\|\boldsymbol{w}_s\|^2\right), \quad \|\boldsymbol{y}\|^2 = \frac{1}{N}\sum_i \left(y_I^2[i] + y_Q^2[i]\right), \tag{50}$$

where y_I and y_Q are the I and Q of the complex receive sample $y = y_I + jy_Q$. The AWGN noise w_s is a complex Gaussian distribution [37, A.1.3]: $w_s \sim \mathcal{CN}(0, \sigma_{w_s})$, where variance $\sigma_{w_s} = \|\boldsymbol{y}\|^2 10^{-\frac{\text{SNR}}{10}}$. Synthetic AWGN noise is added to IQ data of emanations of a laptop connected to a monitor. The PSD over preprocessed IQ is shown in Fig. 6, for various levels of SNR. The algorithm detects the pitch frequency at 236 kHz until around −14 dB SNR. This highlights the robustness of the algorithm. For detection of the pitch frequency at SNRs below −10 dB, $q_1 = 0.9$ instead of the default in Table 2.

Further emanation patterns are presented for a laptop, and a desktop connected to a monitor, see Figs. 7(a) and 7(b). The x-axis represents the center frequency at which IQ samples are captured, y-axis represents the pitch frequency of detected emanations. The laptop is



(a) Laptop idle state. (b) Laptop to mouse. (c) Laptop to keyboard.



(d) Laptop idle state. (e) Laptop to SD card. (f) Laptop to pen drive.

Fig. 8. Detection of anomalous activity. Emulating wear and tear of electronics: emanation pattern of Laptop (a) in idle state, (b) connected to a damaged mouse, (c) connected to a damaged keyboard. Emulating illegal copying of secure data: emanation pattern of Laptop (d) in idle state, (e) connected to SD card with active data transfer, (f) connected to pen drive with active data transfer. Emanations patterns in (b) and (c) differ from baseline (a), similarly for (e) and (f) over (d), indicating detection of anomalous activity.

in an idle state, desktop has CPU-intensive processes running. This causes crowded emanations in the plot with stronger SNR, compared to the emanation pattern of a laptop. The wideband pitch at 60 Hz corresponds to the leakage from the monitor with a 60 Hz refresh rate.

Detection of anomalous activity is illustrated using two use cases as described below. In the first use case, the wear and tear of a mouse and keyboard are emulated by exposing the copper wire by removing cable shielding in a small area. IQ data is collected from the damaged mouse and keyboard that are actively used. Emanation patterns detected on the data are in Fig. 8. In the baseline of an idle laptop only, the emanation pattern has pitches detected more in the lower IQ capture frequencies. For damaged peripherals, the plot has more emanations at higher frequency regions compared to the baseline, indicating potential anomalous activity.

For the second use case, IQ data is collected from an SD card and a pen drive with active data transfer to a laptop. The emanation patterns detected are in the bottom row of Fig. 8. Notice a larger number of emanations detected at higher IQ capture frequencies when there is active data transfer to external storage devices compared to an idle laptop, indicating anomalous activity. This work is the first effort towards a generic HW agnostic solution in detecting anomalous activity using emanations. Therefore, the focus is on detecting emanations and establishing that emanation patterns can be used to detect anomalous activity. The emanation pattern plots in Fig. 8 are a proof of concept demonstrating this.

The real world has interferences from overt signals, channels, HW artifacts, and thermal noise. The challenge in extending this work from a shielded room to an outdoor environment would involve dealing with these artifacts. Since this is a non-cooperative system, unlike a typical communication system, there are no reference signals to help alleviate the artifacts, which makes it a harder problem. It is shown theoretically that the algorithm is robust and generalizes to different channel and HW conditions, see Sections 2.4, 2.5, 2.6, and 4 and Appendix A, B, C, and D. However, there is an assumption of no relative movement between the source of emanations and the receiving HW. The effect of the fast fading channel and high-speed Doppler needs to be explored as future work. The algorithms alleviate the impact of artifacts but do not completely remove them, as shown in the derivations. Therefore, the performance of the pitch estimation algorithm remains to be studied in complex RF environments.

Conclusion

A profiling-free HW agnostic technique is presented to detect RF emanations. Harmonics from leakages of clock signals are identified as a generic signature symptomatic of emanations. A model for emanations as harmonics modulated by random frequency shifts is used. The important custom preprocessing helps remove unintended modulation, channel, and HW artifacts, while retaining the harmonic structure. Thorough mathematical derivations highlight the performance of the algorithm theoretically. Derivations are shown for single-harmonic and multi-harmonic cases with intentionally transmitted signals.

The algorithm performance is shown on IQ data collected in a shielded room. Emanations detected across the 1 GHz bandwidth are shown as emanation pattern plots of detected pitch frequencies vs. IQ capture frequency. Emanation detection is demonstrated using two use cases: (a) Anomalous activity of damaged electronic peripherals and (b) Illegal data transfer. Damaged electronic peripherals are emulated by exposing cables of a mouse and keyboard, and data transfer is emulated by active data transfer between an SD card and a pen drive with a laptop. Emanation patterns for both use cases showed different emanation patterns compared to the baseline of an idle laptop. Thus, we have demonstrated the HW-agnostic anomalous activity detection using emanations.

CRediT authorship contribution statement

Venkatesh Sathyanarayanan: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Peter Gerstoft:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Removal of channel artifacts

This Appendix shows that channel artifact has no impact on pitch estimation. Taking the Fourier transform upon inserting (16) into (17):

$$X_{\text{ch}}(w) = X_{\text{tx}}(w)H(w) = H(w)\sum_m\sum_d \alpha_m\alpha_d\delta(w - mw_h - w_d)$$
$$= \sum_m\sum_d h_{m,d}\alpha_m\alpha_d\delta(w - mw_h - w_d), \tag{A.1}$$

where $h_{m,d} = H(mw_h + w_d)$, $X_{\text{tx}}(w)$ is the Fourier transform of x_{tx} and contains pure tones, represented as Dirac delta functions at $mw_h + w_d$. The effect of the channel artifact is an amplitude and phase shift $h_{m,d}$ that does not impact the frequency of tones. Thus, the channel does not impact the pitch estimation with the assumption of a static channel. Inverse Fourier transform of $X_{\text{ch}}(w)$ (A.1) is taken to get $x_{\text{ch}}[n]$ as follows:

$$x_{\text{ch}}[n] = \sum_m\sum_d h_{m,d}\alpha_m\alpha_d \exp(j(mw_h + w_d)n). \tag{A.2}$$

Appendix B. Preprocessing for single harmonics

The preprocessing is introduced as the Hadamard product of the signal with its complex conjugate. This helps remove the artifacts, as shown below. Combining ((19), (23)), the feature sample vector $\boldsymbol{s} = [s[0], \dots, s[N-1]]^T$ is:

$$\boldsymbol{s} = \boldsymbol{y}^* \odot \boldsymbol{y} = \boldsymbol{v}^* \odot \boldsymbol{v} + \boldsymbol{z}_1, \quad \boldsymbol{z}_1 = 2\Re\mathfrak{e}\left\{\boldsymbol{v}^* \odot \boldsymbol{w}\right\} + \boldsymbol{w}^* \odot \boldsymbol{w}. \tag{B.1}$$

where reduction is due to the distributive property of the complex conjugate and the distributive property of the Hadamard product. Variants of notation z represent cross terms that do not contain harmonic patterns. Emanations impacted by channel and clock $\boldsymbol{v}$ from (20) is inserted into (B.1):

$$\boldsymbol{v}^* \odot \boldsymbol{v} = (\boldsymbol{c} \odot \boldsymbol{x}_{\text{ch}})^* \odot (\boldsymbol{c} \odot \boldsymbol{x}_{\text{ch}}) = \boldsymbol{x}^*_{\text{ch}} \odot ((\boldsymbol{c}^* \odot \boldsymbol{c}) \odot \boldsymbol{x}_{\text{ch}}) = \boldsymbol{x}^*_{\text{ch}} \odot \boldsymbol{x}_{\text{ch}}, \tag{B.2}$$

where the commutative and associative properties of Hadamard product, and the distributive property of complex conjugate operator over Hadamard product result in the second term of (B.2). Further, the properties $\boldsymbol{c}^* \odot \boldsymbol{c} = \boldsymbol{J}_N$ and $\boldsymbol{J}_N \odot \boldsymbol{x}_{\text{ch}} = \boldsymbol{x}_{\text{ch}}$, where $\boldsymbol{J}_N \in \mathbb{C}^N$ is an all ones vector, gives final reduced term $\boldsymbol{x}^*_{\text{ch}} \odot \boldsymbol{x}_{\text{ch}}$. This removes the time-varying clock artifacts and reduces signal variance.

Rewriting $\boldsymbol{x}_{\text{ch}}$ from (18) by grouping the summation over d gives:

$$\boldsymbol{x}_{\text{ch}} = \sum_d \boldsymbol{x}_d, \qquad x_d[n] = \alpha_d \sum_m h_{m,d}\alpha_m \exp(j(w_h + w_d)mn), \tag{B.3}$$

where $\boldsymbol{x}_d = [x_d[0], \dots, x_d[N-1]]^T$.

Inserting $\boldsymbol{x}_{\text{ch}}$ from (B.3) into (B.2):

$$\boldsymbol{x}^*_{\text{ch}} \odot \boldsymbol{x}_{\text{ch}} = \Big(\sum_{d_1} \boldsymbol{x}_{d_1}\Big)^* \odot \Big(\sum_{d_2} \boldsymbol{x}_{d_2}\Big) = \sum_{d=1} \boldsymbol{x}^*_d \odot \boldsymbol{x}_d + \boldsymbol{z}_2, \boldsymbol{z}_2 = \sum_{\substack{\forall d_1,d_2 \\ d_1 \neq d_2}} \boldsymbol{x}_{d_1} \odot \boldsymbol{x}_{d_2}, \tag{B.4}$$

where the distributive property of Hadamard product and complex conjugate operator over addition gives (B.4), and $\boldsymbol{z}_2$ contains cross terms. Combining (B.1), (B.2), (B.4), $\boldsymbol{s}$ becomes ($\boldsymbol{z} = \boldsymbol{z}_1 + \boldsymbol{z}_2$):

$$\boldsymbol{s} = \sum_d \boldsymbol{x}^*_d \odot \boldsymbol{x}_d + \boldsymbol{z} = \sum_d \boldsymbol{s}_d + \boldsymbol{z}. \tag{B.5}$$

$s_d[n]$ is computed using $x_d[n]$ from (B.3) as follows:

$$s_d[n] = \sum_{m=-M}^{M} \gamma_{m,d} \exp(jw_h mn), \tag{B.6}$$

where $s_d[n] \in \mathbb{R}$, $\gamma_{m,d} = |\alpha_d|^2 |h_{m,d}|^2 |\alpha_m|^2 (M - |m|)$ such that $\gamma_{m,d} \in \mathbb{C}$. Preprocessing removes the effect of unknown frequency modulation term $\exp(jw_d n)$ in x_d (B.3) and s_d. Inserting (B.6) into (B.5):

$$s[n] = \sum_m \exp(jw_h mn) \sum_d \gamma_{m,d} + z[n] = \sum_m \gamma_m \exp(jw_h mn) + z[n], \tag{B.7}$$

whose Fourier transform is:

$$S(w) = \sum_m \gamma_m \delta\left(w - mw_h\right) + Z(w), \tag{B.8}$$

where Z is the Fourier transform of z.

Appendix C. Preprocessing for multi-harmonics

This Appendix contains derivations for preprocessing for the multi-harmonics use case. An emanation from each of the K sources impacted by channel and clock artifacts is:

$$\boldsymbol{y}_k = \boldsymbol{c}_k \odot \boldsymbol{x}^k_{\text{ch}}, \tag{C.1}$$

where $\boldsymbol{x}^k_{\text{ch}}$ is transmit emanation impacted by channel, clock artifacts $\boldsymbol{c}_k = [\exp(j\beta_k[0]), \dots, \exp(j\beta_k[N-1])]^T$, $\beta_k[n] = w^k_e[n]n + \theta^k_e[n]$ such that $w^k_e[n]$, $\theta^k_e[n]$ represent frequency and phase errors of kth source due to imperfect clocks. Preprocessing is applied on receive IQ $\boldsymbol{y}_{\text{mh}}$, inserting (8) into (B.1) as follows:

$$\boldsymbol{s}_{\text{mh}} = \boldsymbol{y}^*_{\text{mh}} \odot \boldsymbol{y}_{\text{mh}} = \Big(\sum_{k_1} \boldsymbol{y}_{k_1} + \boldsymbol{w}\Big)^* \odot \Big(\sum_{k_2} \boldsymbol{y}_{k_2} + \boldsymbol{w}\Big). \tag{C.2}$$

The properties of commutative, distributive over-addition of the Hadamard product, distributive over-addition, and distributive over Hadamard product of the complex conjugate operator are used to reduce (C.2) into:

$$\boldsymbol{s}_{\text{mh}} = \sum_k \boldsymbol{y}^*_k \odot \boldsymbol{y}_k + \boldsymbol{z}_1, \boldsymbol{z}_1 = \boldsymbol{w}^* \odot \boldsymbol{w} + 2\sum_k \Re\mathfrak{e}\left\{\boldsymbol{y}^*_k \odot \boldsymbol{w}\right\} + \sum_{\substack{\forall k_1,k_2 \\ k_1 \neq k_2}} \boldsymbol{y}^*_{k_1} \odot \boldsymbol{y}_{k_2}, \tag{C.3}$$

where $\boldsymbol{z}_1$ represents cross-terms. Using (C.1), $\boldsymbol{y}^*_k \odot \boldsymbol{y}_k$ becomes:

$$\boldsymbol{y}^*_k \odot \boldsymbol{y}_k = \left(\boldsymbol{c}_k \odot \boldsymbol{x}^k_{\text{ch}}\right)^* \odot \left(\boldsymbol{c}_k \odot \boldsymbol{x}^k_{\text{ch}}\right) = \left(\boldsymbol{x}^k_{\text{ch}}\right)^* \odot \left(\boldsymbol{x}^k_{\text{ch}}\right) = \Big(\sum_{d_1} \boldsymbol{x}^k_{d1}\Big)^* \odot \Big(\sum_{d_2} \boldsymbol{x}^k_{d2}\Big), \tag{C.4}$$

where (B.2), and (B.4) are used. Further, using (B.4):

$$\boldsymbol{y}^*_k \odot \boldsymbol{y}_k = \sum_d \left(\boldsymbol{x}^k_d\right)^* \odot \left(\boldsymbol{x}^k_d\right) + \boldsymbol{z}_k, \quad \boldsymbol{z}_k = \sum_{\substack{\forall d_1,d_2 \\ d_1 \neq d_2}} (\boldsymbol{x}^k_{d_1})^* \odot (\boldsymbol{x}^k_{d_2}), \tag{C.5}$$

Using (C.3) and (C.5), $\boldsymbol{s}_{\text{mh}}$ becomes:

$$\boldsymbol{s}_{\text{mh}} = \sum_k\sum_d \boldsymbol{s}^k_d + \boldsymbol{z}_{\text{mh}}, \quad \boldsymbol{z}_{\text{mh}} = \sum_k \boldsymbol{z}_k + \boldsymbol{z}_1, \tag{C.6}$$

where $\boldsymbol{s}^k_d = \left(\boldsymbol{x}^k_d\right)^* \odot \left(\boldsymbol{x}^k_d\right)$, $\boldsymbol{z}_{\text{mh}} = [z_{\text{mh}}[0], \dots, z_{\text{mh}}[N-1]]^T$. Using (B.6), $\boldsymbol{s}^k_d = [s^k_d[0], \dots, s^k_d[N-1]]^T$ becomes:

$$s^k_d[n] = \sum_m \gamma^k_{m,d} \exp(jw^k_h mn), \tag{C.7}$$

Inserting (C.7) into (C.6), s_{mh} gives:

$$s_{\text{mh}}[n] = \sum_k\sum_m \exp(jw^k_h mn) \sum_d \gamma^k_{m,d} + z_{\text{mh}}[n] = \sum_k\sum_m \gamma^k_m \exp(jw^k_h mn) + z_{\text{mh}}[n], \tag{C.8}$$

where $\gamma^k_m = \sum_d \gamma^k_{m,d}$. Fourier transform of s_{mh} gives:

$$S_{\text{mh}}(w) = \sum_k\sum_m \gamma^k_m \delta(w - mw^k_h) + Z_{\text{mh}}(w), \tag{C.9}$$

where Z_{mh} is the Fourier transform of z_{mh}.

Appendix D. Preprocessing for overt signals

This Appendix contains the details of applying preprocessing for overt signals. Applying preprocessing on receive IQ $\boldsymbol{y}$ following (C.2):

$$\boldsymbol{s}_o = \boldsymbol{y}^* \odot \boldsymbol{y} = \boldsymbol{s}_{\text{mh}} + \boldsymbol{z}_o, \tag{D.1}$$

where $\boldsymbol{s}_{\text{mh}}$ is the preprocessing applied to the received signal from multiple emanation sources from (C.2), $\boldsymbol{z}_o$ containing additional terms is:

$$\boldsymbol{z}_o = 2\Re\mathfrak{e}\left\{\boldsymbol{y}^*_o \odot \boldsymbol{w}\right\} + 2\sum_k \Re\mathfrak{e}\left\{\boldsymbol{y}^*_k \odot \boldsymbol{y}_o\right\} + \boldsymbol{y}^*_o \odot \boldsymbol{y}_o. \tag{D.2}$$

The term $\boldsymbol{y}^*_o \odot \boldsymbol{w}$ represents cross-correlation between overt and thermal noise and $\boldsymbol{y}^*_k \odot \boldsymbol{y}_o$ between emanation source and overt, $\boldsymbol{y}^*_o \odot \boldsymbol{y}_o$ autocorrelation of overt. The first term is uncorrelated and does not result in a harmonic pattern. The second and third terms result in a harmonic pattern only if the overt signal has a harmonic pattern.

Data availability

The authors are unable or have chosen not to specify which data has been used.

References

[1] A. Shahid, A. Kliks, A. Al-Tahmeesschi, Large-scale AI in telecom: Charting the roadmap for innovation, scalability, and enhanced digital experiences, 2025, arXiv:2503.04184. https://arxiv.org/abs/2503.04184.

[2] IARPA program to detect RF anomalies. https://www.iarpa.gov/research-programs/scisrs.

[3] B.B. Yilmaz, E.M. Ugurlu, M. Prvulovic, Detecting cellphone camera status at distance by exploiting electromagnetic emanations, in: IEEE Mil. Commun. Conf., 2019, pp. 1–6.

[4] R. Spolaor, L. Abudahi, V. Moonsamy, No free charge theorem: A covert channel via USB charging cable on mobile devices, in: Appl. Crypto. Netw. Secur., 2017, pp. 83–102.

[5] S. Anand, N. Saxena, Keyboard emanations in remote voice calls: Password leakage and noise (less) masking defenses, in: ACM Conf. Data Appl. Secur. Privacy, 2018, pp. 103–110.

[6] M. Guri, B. Zadov, E. Atias, LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive LED, in: Detect. Intrusions Malware Vulnerability Assess., 2017, pp. 161–184.

[7] M. Dey, A. Nazari, A. Zajic, EMPROF: Memory profiling via EM-emanation in IoT and hand-held devices, in: IEEE Int. Symp. Microarchit., 2018, pp. 881–893.

[8] A. Nazari, N. Sehatbakhsh, M. Alam, EDDIE: EM-based detection of deviations in program execution, in: IEEE Int. Symp. Comput. Archit., 2017, pp. 333–346.

[9] M.F. Bari, M.R. Chowdhury, B. Chatterjee, Detection of rogue devices using unintended near and far-field emanations with spectral and temporal signatures, in: IEEE Int. Microw. Symp., 2022, pp. 591–594.

[10] A. Sayakkara, Le-Khac, Nhien-An, Accuracy enhancement of electromagnetic side-channel attacks on computer monitors, in: Proc. Int. Conf. Availability, Reliability, Secur., 2018.

[11] M. Vuagnoux, S. Pasini, Compromising electromagnetic emanations of wired and wireless keyboards, in: USENIX Secur. Symp., 2009, pp. 1–16.

[12] V. Sathyanarayanan, P. Gerstoft, A. El-Gamal, RML22: Realistic dataset generation for wireless modulation classification, IEEE Trans. Wirel. Commun. 22 (11) (2023) 7663–7675.

[13] H. Xia, K. Alshathri, V.B. Lawrence, Cellular signal identification using convolutional neural networks: AWGN and Rayleigh fading channels, in: IEEE Int. Symp. Dyn. Spectr. Access Netw., 2019, pp. 1–5.

[14] D. Agrawal, B. Archambeault, R.J. Rao, P. Rohatgi, The EM side-channel(s), in: Crypto. Hardw. Embed. Syst., 2003, pp. 29–45.

[15] M. Prvulovic, A. Zajić, R.L. Callan, A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems, IEEE Trans. Electromagn. Compat. 59 (1) (2017) 34–42.

[16] D. Romero, T.N. Ha, P. Gerstoft, Spoofing attack detection in the physical layer with robustness to user movement, in: IEEE Wirel. Commun. Netw. Conf., 2024, pp. 1–6.

[17] W. Wang, C. Luo, J. An, L. Gan, H. Liao, C. Yuen, Semisupervised RF fingerprinting with consistency-based regularization, IEEE Internet Things J. 11 (5) (2024) 8624–8636.

[18] G. Zaid, L. Bossuet, A. Habrard, Methodology for efficient CNN architectures in profiling attacks, IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020 (1) (2019) 1–36.

[19] D. Das, A. Golder, J. Danial, X-Deepsca: Cross-device deep learning side channel attack, in: Desig. Automat. Conf., 2019.

[20] V. Sathyanarayanan, P. Gerstoft, Detection and characterization of unintended RF emissions on wideband real data, in: Int. Conf. Signal Process. Commun., 2024, pp. 1–5.

[21] O.A. Ibrahim, S. Sciancalepore, G. Oligeri, R.D. Pietro, MAGNETO: Fingerprinting USB flash drives via unintentional magnetic emissions, ACM Trans. Embed. Comput. Syst. 20 (1) (2020) 26–50.

[22] M.G. Christensen, A. Jakobsson, Multi-Pitch Estimation, Springer, 2009.

[23] C.R. Maher, J.W. Beauchamp, Fundamental frequency estimation of musical signals using a two-way mismatch procedure, J. Acoust. Soc. Am. 95 (4) (1994) 2254–2263.

[24] E. Azarov, M. Vashkevich, A. Petrovsky, Instantaneous pitch estimation based on RAPT framework, in: Proc. Eur. Signal Process. Conf., 2012, pp. 2787–2791.

[25] S.S. Abeysekera, Multiple pitch estimation of polyphonic audio signals in a frequency-lag domain using the bispectrum, in: IEEE Int. Symp. Circuits Syst., 2004, pp. 469–472.

[26] M.G. Christensen, S.H. Jensen, Variable order harmonic sinusoidal parameter estimation for speech and audio signals, in: Proc. Asilomar Conf. Signals Syst. Comput., 2006, pp. 1126–1130.

[27] J. Tabrikian, S. Dubnov, Y. Dickalov, Maximum a-posteriori probability pitch tracking in noisy environments using harmonic model, IEEE Trans. Speech Audio Process. 12 (1) (2004) 76–87.

[28] M.F. Bari, M.R. Chowdhury, S. Sen, Long range detection of emanation from HDMI cables using CNN and transfer learning, in: Des. Autom. Test Conf., 2023, pp. 1–6.

[29] B. Sklar, Digital Communications: Fundamentals and Applications, Prentice Hall, 2001.

[30] R. Callan, A. Zajić, M. Prvulovic, FASE: Finding amplitude-modulated side-channel emanations, in: Int. Symp. Comput. Archit., 2015, pp. 592–603.

[31] M. Rice, Digital Communications: A Discrete-Time Approach, Pearson Education Inc, 2012.

[32] A.V. Oppenheim, R.W. Schafer, J.R. Buck, Discrete-Time Signal Processing, Prentice Hall Inc., 1998.

[33] C. Yang, Z. He, W. Yu, Comparison of public peak detection algorithms for MALDI mass spectrometry data analysis, BMC Bioinf. 10 (4) (2009) 1–4.

[34] P. Du, W.A. Kibbe, S.M. Lin, Improved peak detection in mass spectrum by incorporating continuous wavelet transform-based pattern matching, Bioinf. 22 (17) (2006) 2059–2065.

[35] B. Kashyap, M. Horne, P.N. Pathirana, Automated topographic prominence based quantitative assessment of speech timing in cerebellar ataxia, Biomed. Signal Process. Control. 57 (101759) (2020) 1–22.

[36] Y. Song, N. Madhu, Improved CEM for speech harmonic enhancement in single channel noise suppression, IEEE Trans. Audio Speech Lang. Process. 30 (1) (2022) 2492–2503.

[37] D. Tse, P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005.