

Beyond TEMPEST: Workload-Modulated Power-Quality Covert Channels in Air-Gapped Systems

Vitor Hugo Silva

vitorhg20080@gmail.com

Universidade do Porto Faculdade de Ciencias <https://orcid.org/0000-0002-1055-5662>

Rolando Martins

Faculdade de Ciências da Universidade do Porto <https://orcid.org/0000-0002-1838-1417>

Research Article

Keywords: air-gapped systems, covert channels, data exfiltration, harmonic distortion, power factor, power quality, switched-mode power supplies

Posted Date: September 23rd, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11095329/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Beyond TEMPEST: Workload-Modulated Power-Quality Covert Channels in Air-Gapped Systems

Vítor Hugo Silva ^[ORCID]^{1*} and Rolando Martins ^[ORCID]¹

^{1*}Department of Computer Science, Faculty of Sciences, University of Porto, Porto, Portugal.

*Corresponding author(s). E-mail(s): up201402657@up.pt;

Abstract

Air-gapped computers remain connected to electrical infrastructure, where workload changes can alter the input current of switched-mode power supplies. This study evaluates true power factor and low-order current harmonics as information-bearing observables for a conducted covert channel. A desktop computer encoded data through binary on-off keying of processor load. Synchronized voltage and current were recorded near the power-supply unit and at an upstream office-level point. Three supply topologies were tested: no power-factor correction, passive correction, and active correction. Text, 128-bit example-key, and 256-bit elliptic-curve payloads were transmitted at nominal raw rates of 0.5 and 1 bit/s. Complete payload recovery with valid Reed–Solomon verification was reported in selected feature/configuration combinations. Active correction produced the smallest useful harmonic feature set, especially at the office-level receiver. Recoverable patterns nevertheless persisted in selected shared-infrastructure captures. The findings extend the receiver feature space of power-line covert channels to derived power-quality metrics and describe their dependence on the tested supply topology and receiver position.

Keywords: air-gapped systems, covert channels, data exfiltration, harmonic distortion, power factor, power quality, switched-mode power supplies

1 Introduction

Air-gapped systems remove conventional network paths. They are used when disclosure would have severe consequences. Isolation does not remove physical interaction with the environment. A compromised computer still emits heat, sound, light, vibration, magnetic fields, electromagnetic radiation, and electrical disturbances. Malware can modulate these effects and create covert channels [6, 9, 13, 14, 33].

The power supply is a persistent connection to external infrastructure. A switched-mode power supply (SMPS) converts the mains input into regulated direct-current rails. Its input current depends on its front-end topology and the downstream workload. A rectifier-capacitor front end draws narrow current pulses. These pulses contain low-order harmonics. Passive power-factor correction (PFC) reshapes the current. Active PFC uses a controlled converter to make the current follow the mains voltage more closely. This reduces low-order distortion and improves power factor. IEC 61000-3-2 specifies harmonic-current limits for equipment connected to public low-voltage networks [26]. IEEE 1459-2025 defines power quantities under nonsinusoidal conditions [25].

The closest electrical channels reviewed in Section 2 decode raw current, switching ripple, radiated emissions, or meter outputs. They do not jointly evaluate true power factor and individual low-order current harmonics across no-PFC, passive-PFC, and active-PFC supplies as done here. This study addresses that receiver-observable gap.

The paper makes four contributions. First, it provides proof-of-concept evidence that true power factor and low-order current-harmonic amplitudes can carry information in a conducted covert channel. Second, it compares these variables in recorded transmissions across three PFC topologies. Third, it evaluates a near-PSU receiver and an upstream office-level receiver. Fourth, it reports end-to-end payload recovery, nominal raw rate, protocol payload goodput, reported bit-error rate (BER), and Reed-Solomon validity. Repository information is given in the data and code availability statements.

2 Related work

Air-gap covert channels span several physical media. Electromagnetic channels turn ordinary computer components and cables into unintended transmitters. AirHopper uses video-cable emissions in the FM band [12]. GSMem uses memory activity in cellular bands [13]. USBee uses emissions from USB data transfers [16]. AIR-FI and BitJabber exploit memory-system activity [9, 34]. LANTENNA uses Ethernet cables as radiating elements [5]. LCD TEMPEST and TEMPEST-LoRa exploit display interfaces [11, 32]. COVID-bit instead uses workload-dependent low-frequency electromagnetic radiation [7]. Magnetic channels such as MAGNETO and ODINI use CPU-generated fields and smartphone magnetometers [6, 24].

Acoustic and mechanical channels use both dedicated audio hardware and incidental component noise. MOSQUITO establishes ultrasonic speaker-to-speaker communication [19]. Fansmitter, DiskFiltration, POWER-SUPPLaY, and CD-LEAK use cooling fans, hard-drive actuators, power-supply components, and optical drives, respectively [2, 8, 17, 22]. GAIRSCOPE couples ultrasonic tones into a smartphone

gyroscope [4]. ViBrAtIoNs uses fan-induced mechanical vibration [3]. BitWhisper uses thermal coupling between adjacent computers and provides very low-rate bidirectional communication [14].

Optical channels encode data in displays, indicator LEDs, or infrared light. VisiS-ploit modulates imperceptible screen content [15]. LED-it-GO, CTRL-ALT-LED, and xLED use storage, keyboard, and network-equipment LEDs [18, 20, 21]. aIR-Jumper uses infrared-capable surveillance cameras for exfiltration and infiltration [10]. These free-space channels differ in bandwidth, line-of-sight requirements, receiver hardware, proximity, and sensitivity to shielding or environmental noise.

A smaller body of work focuses on power components and electrical infrastructure. Powermitter changes CPU load to modulate electromagnetic emissions from a switching power adapter [35]. PowerHammer conducts workload-dependent current changes through building power lines and decodes raw current amplitude [23]. NoDE observes high-frequency voltage ripple produced by active-PFC switching at another outlet [29]. Bit Sufi-Dance converts load oscillations into observable motion or LED activity at an electricity meter [27]. PowerBridge uses a modified smart plug for outbound power measurement and inbound supply switching [28]. BREAKING TEMPEST combines workload-controlled outbound current modulation with inbound line-voltage modulation and PMBus sensing [1]. The present study is distinct. It derives true power factor and individual low-order harmonic amplitudes from synchronized voltage and current. It then evaluates these features across PFC topologies and receiver positions.

Table 1 compares the closest power-supply and power-infrastructure channels. The comparison focuses on signal generation and receiver observables. Rates from different hardware and electrical environments are not treated as direct benchmarks.

Table 1 Closest power-supply and power-infrastructure covert channels

Study	Transmitter action	Receiver observable	Scope
Powermitter [35]	CPU load	Radiated EM from power adapter	Outbound; nearby coil and oscilloscope
COVID-bit [7]	CPU load	Low-frequency radiated EM	Outbound; nearby antenna
PowerHammer [23]	CPU load	Raw line-current amplitude	Outbound; line and phase taps
NoDE [29]	Active-PFC switching	High-frequency voltage ripple	Outbound; another outlet
Bit Sufi-Dance [27]	CPU load	Electricity-meter disc or LED	Outbound; optical receiver
PowerBridge [28]	CPU load; plug switching	Smart-plug power/current; AC state	Bidirectional; modified smart plug
BREAKING TEMPEST [1]	Target load; line voltage	External line current; PMBus voltage	Bidirectional; building wiring and TEMPEST filters
This study	CPU load	True power factor; low-order current harmonics	Outbound; three PFC topologies and two receiver points

3 Channel model and threat assumptions

3.1 Power-quality observables

For synchronized voltage and current waveforms, active power is

$$P = \frac{1}{T} \int_0^T v(t)i(t) dt, \quad (1)$$

where T is the observation interval. Apparent power is

$$S = V_{\text{rms}} I_{\text{rms}}, \quad (2)$$

and true power factor is

$$\text{PF} = \frac{P}{S}. \quad (3)$$

For a nearly sinusoidal supply voltage and a distorted current,

$$\text{PF} \approx \cos \phi_1 \frac{I_1}{I_{\text{rms}}} = \frac{\cos \phi_1}{\sqrt{1 + \text{THD}_I^2}}, \quad (4)$$

where ϕ_1 is the fundamental voltage-current phase displacement. The term I_1 is the fundamental current RMS value. The term THD_I is current total harmonic distortion. This expression separates displacement from waveform distortion [25].

A periodic input current can be written as

$$i(t) = \sum_{n=1}^{\infty} I_n \sqrt{2} \sin(n\omega t + \phi_n), \quad (5)$$

where I_n is the RMS amplitude of harmonic order n . The receiver evaluates the 3rd, 5th, 7th, and 11th current harmonics. It retains both absolute RMS amplitude and amplitude relative to the fundamental:

$$H_{n,\text{dBc}} = 20 \log_{10} \left(\frac{I_n}{I_1} \right). \quad (6)$$

Absolute amplitude preserves workload-dependent scaling. Relative amplitude describes changes in spectral shape.

The physical mechanism follows the SMPS input stage. A non-PFC rectifier draws current near the voltage peaks. Workload changes modify pulse amplitude and conduction interval. Passive PFC reduces this distortion but does not regulate the input current continuously. Active PFC suppresses low-order distortion through current shaping. It should therefore reduce the observability of this specific harmonic channel.

3.2 Threat assumptions

The attacker has already compromised an isolated computer and can change CPU activity. No conventional network path is available. Malware maps data to low and high workload states. The intended payload is small. Examples include credentials, cryptographic material, commands, or beacons.

The receiver measures synchronized line voltage and current on the same electrical infrastructure. The near-PSU receiver observes the target branch directly. The office-level receiver observes the target together with concurrent office loads. Figure 1 summarizes both positions.

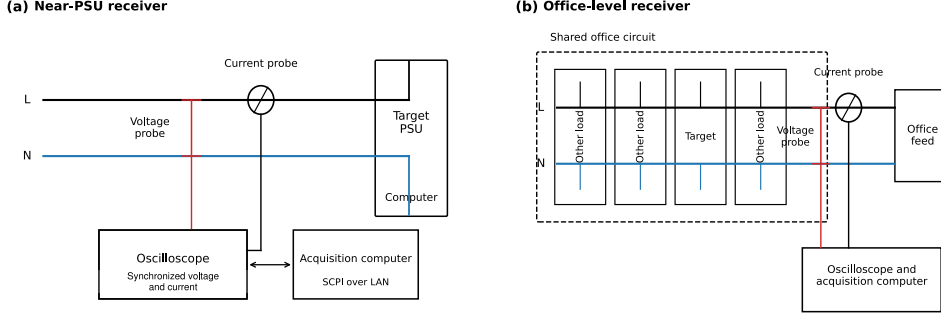


Fig. 1 Measurement configuration. Panel (a) shows synchronized voltage and current acquisition at the PSU input. Panel (b) shows the upstream office-level receiver. The office-level current contains the target contribution and other loads on the shared circuit.

The upstream current can be represented as

$$i_{\text{obs}}(t) = h_{\text{path}}(t) * i_{\text{target}}(t) + \sum_{k=1}^K i_{\text{load},k}(t) + \eta(t), \quad (7)$$

where h_{path} represents the electrical path. The terms $i_{\text{load},k}$ represent other loads. The term η represents measurement noise and external disturbance. Receiver separation is therefore a property of the conducted path. Cable impedance, branching, filtering, grounding, and background loads can all change the signal.

4 Methods

4.1 Study design

The experiments were originally documented in a master’s dissertation [30]. This article condenses that exploratory proof-of-concept study; it does not report an additional campaign of independent acquisitions.

The on-off-keying (OOK) matrix covered three PFC topologies and two receiver positions. At each topology/position pair, four payload/duration settings were evaluated: American Standard Code for Information Interchange (ASCII) text at $T_s = 2$ s, an Advanced Encryption Standard (AES-128) key at $T_s = 2$ s and $T_s = 1$ s, and Elliptic Curve Digital Signature Algorithm (ECDSA) material at $T_s = 2$ s. Each of the 24 resulting configurations was transmitted and acquired once ($N = 1$ per configuration). A run comprised one complete workload execution and synchronized voltage-current acquisition, followed by offline feature extraction and decoding.

The same processing procedure was applied to the captures. The primary receiver feature set comprised true power factor and the 3rd, 5th, 7th, and 11th current harmonics in absolute RMS and relative dBc form. Each feature was decoded separately. Different features from one capture are alternative analyses of the same transmission, not independent experimental repetitions. BER and decoding outcomes are descriptive results for those captures; no across-run variance, confidence interval, or expected packet-success probability was estimated.

4.2 Experimental platform and acquisition

The target was a desktop computer with an AMD Ryzen 5 3600 processor and 8 GB of memory. It ran Windows 11 Education 25H2. The same target and workload software were used for all supplies. Table 2 lists the electrical hardware and acquisition parameters.

Table 2 Experimental hardware and acquisition parameters

Item	Configuration
No-PFC PSU	500 W ATX SMPS (UNYKAch ATX 500W)
Passive-PFC PSU	600 W ATX SMPS (1Life PS:JET 600W)
Active-PFC PSU	650 W ATX SMPS (MSI MAG A650BN)
Oscilloscope	SIGLENT SDS1202X-E digital storage oscilloscope
Voltage probe	SIGLENT PP215, connected in parallel
Current probe	Hantek CC-650, applied to the phase conductor
Short captures	100 kSa/s, 70 s, 7,000,000 samples per channel
Payload captures	10 kSa/s, 700 s, 7,000,000 samples per channel
Receiver points	PSU input and upstream office supply
Mains supply	230 V RMS, 50 Hz

Voltage and current were recorded concurrently. The oscilloscope transferred each complete waveform to an acquisition computer. Baseline, load-sweep, and pulse-ramp tests used 100 kSa/s. Payload tests used 10 kSa/s to extend the record duration. Feature extraction was performed offline.

The office-level receiver was approximately 3.5 m from the target in the tested layout. This value describes the room geometry. It does not define channel range. The conducted path also included building wiring and the distribution panel.

4.3 Workload modulation and framing

A Python transmitter controlled CPU activity through worker threads and duty cycle. Three workload profiles were used. The baseline recorded normal idle behaviour. The load sweep increased CPU use from idle to full load over about 30 s. The pulse ramp alternated between idle and full load while increasing pulse duration from about 1 ms to 500 ms.

The communication test used binary on-off keying (OOK). One CPU-load state represented 0. The other represented 1. The main symbol duration was $T_s = 2$ s. An additional AES-128 configuration used $T_s = 1$ s. Each frame contained a preamble, a one-byte size field, the payload, and four Reed–Solomon parity bytes. The AES frame repeated the 16-bit alternating preamble. The other frames used it once.

The two symbol durations were conservative engineering choices, not optimized channel limits. On a 50 Hz supply, 2-s and 1-s symbols span approximately 100 and 50 mains cycles, respectively. The longer setting allowed the workload state to persist across multiple electrical cycles and was compatible with the oscilloscope memory constraint and the 10 kSa/s, 700-s acquisition. The shorter AES-128 setting tested a less conservative operating point. No systematic sweep over symbol duration was performed.

Three test payloads were transmitted. They were an 18-byte ASCII string, a 16-byte AES-128 example value, and 32 bytes of ECDSA-related key material. All cryptographic values were synthetic.

For one bit per symbol,

$$R_{\text{raw}} = \frac{1}{T_s}. \quad (8)$$

Payload goodput is

$$G_{\text{payload}} = \frac{N_{\text{payload}}}{N_{\text{frame}} T_s}, \quad (9)$$

where both N terms are measured in bits. Table 3 reports nominal protocol rates during the encoded frame, conditional on complete payload recovery. They exclude the idle portions of the 700-s capture and are not measurements of sustained goodput across repeated transmissions.

Table 3 OOK frame rates and payload goodput

Payload	Bytes	T_s (s)	Frame bits	Raw bit/s	Payload bit/s
ASCII string	18	2	200	0.5	0.360
AES-128 example	16	2	200	0.5	0.320
AES-128 example	16	1	200	1.0	0.640
ECDSA material	32	2	312	0.5	0.410

4.4 Feature extraction and decoding

Temporal segmentation was performed after acquisition of the complete waveform. The analysis-window length T_w controlled averaging, whereas the hop Δ controlled

the time spacing of the extracted features. Neither parameter is the transmitter symbol duration T_s . Longer windows can smooth symbol transitions; shorter windows retain less averaging. Each window produced RMS voltage, RMS current, active power, apparent power, true power factor, displacement power factor, and current-harmonic amplitudes. A discrete Fourier transform produced the harmonic features.

The decoder processed one scalar feature at a time. It removed invalid samples, merged duplicate timestamps, interpolated the series to a uniform grid, and applied moving-average smoothing. It then searched candidate symbol durations and timing offsets near the nominal values. The source dissertation does not specify all numerical values for T_w , Δ , the interpolation interval, moving-average length, and timing-search grids. These settings cannot be inferred from T_s alone. The procedure below follows the documented processing chain, without introducing unverified parameter values.

For each candidate timing, the decoder calculated the mean feature value $\bar{z}_m$ within each symbol. The automatic threshold was

$$\tau = \frac{q_{0.2} + q_{0.8}}{2}, \quad (10)$$

where $q_{0.2}$ and $q_{0.8}$ are the 20th and 80th percentiles of the symbol means. The bit decision was

$$\hat{b}_m = \begin{cases} 1, & \bar{z}_m \geq \tau, \\ 0, & \bar{z}_m < \tau. \end{cases} \quad (11)$$

The decoder also evaluated inverted feature polarity. It selected the candidate with the highest preamble score. Ties favoured the duration nearest the nominal value and then the earliest alignment.

A reported decode was counted as valid when the source table recorded complete payload recovery with successful Reed–Solomon verification (“Yes”). Candidates marked “No” or “RS invalid” were excluded. The known transmitted payload was used for pre-correction BER evaluation, not to set the threshold or symbol values.

For a compared bit interval, BER is the number of differing bits divided by the number of compared bits. The source tables do not identify that denominator for every candidate, and some reported BER/error-count pairs remain inconsistent. Additional file 1 preserves these values and marks unresolved entries rather than assigning a corrected count or assuming a full-payload denominator. The valid-decode counts below are re-counted from the reported outcome labels, not inferred from BER. A reported BER of zero means no differences in the compared interval; it does not establish a zero expected channel BER.

A large language model assisted with language editing, structural revision, and consistency checks between the manuscript and the dissertation tables, including re-counting the tabulated decoding outcomes. It did not generate experimental measurements or replace unresolved BER values. The authors remain responsible for verifying the final text, numerical values, citations, and interpretations.

5 Results

5.1 Workload-dependent electrical response

The idle captures showed stable but topology-dependent spectra. The no-PFC supply produced the strongest low-order harmonics. Passive PFC reduced and redistributed the harmonic content. Active PFC produced the weakest low-order signature. No deliberate temporal pattern appeared during the baseline period.

The load sweep produced ordered changes in the harmonic amplitudes. Figure 2 shows the absolute RMS response. The no-PFC and passive-PFC panels contain clear load-dependent bands. The active-PFC panel shows lower harmonic contrast. These measurements confirm that computational demand can modify low-order current harmonics at the mains interface.

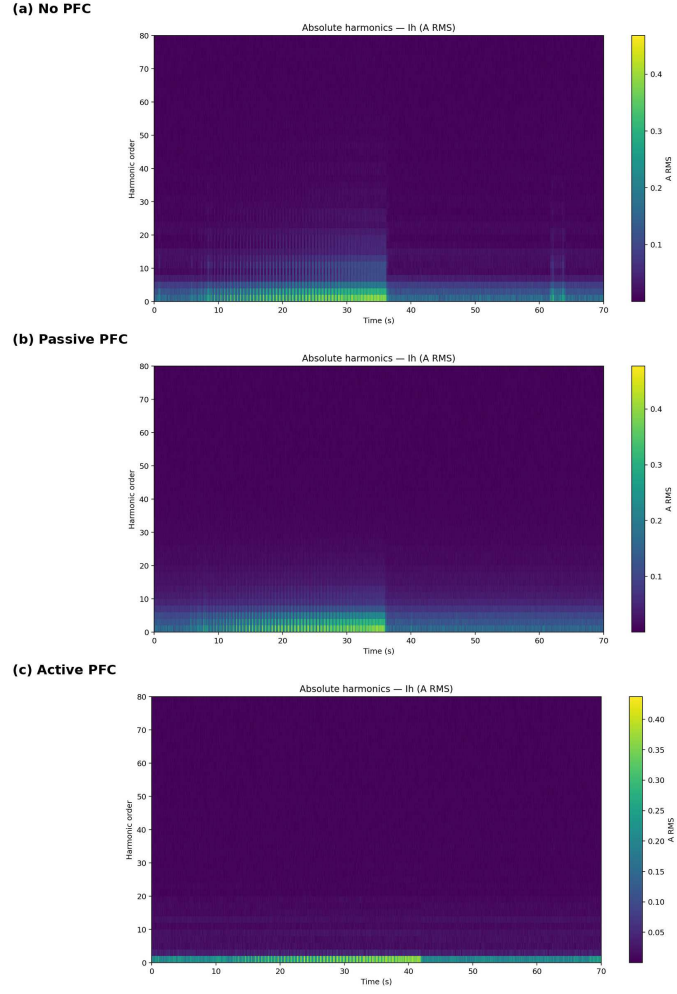


Fig. 2 Load-sweep harmonic response. Absolute RMS current harmonics are shown for (a) no PFC, (b) passive PFC, and (c) active PFC. CPU load increased during the first part of each 70-s capture.

The pulse ramp tested faster workload transitions. Figure 3 compares the no-PFC and active-PFC supplies. The power-factor envelope and harmonic amplitudes follow the increasing pulse duty cycle. The harmonic response is stronger without active PFC.

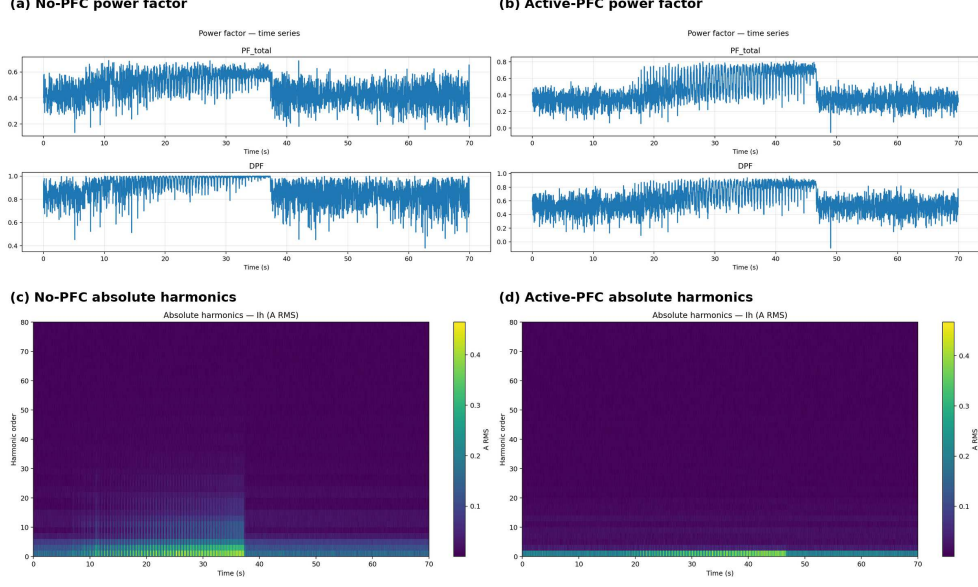


Fig. 3 Pulse-ramp response. Panels (a) and (b) show true and displacement power factor. Panels (c) and (d) show absolute RMS current harmonics. Pulse duty cycle increased during the first part of the capture.

Together, the recorded load-sweep and pulse-ramp tests provide evidence of a workload-dependent relation in the selected electrical observables.

5.2 End-to-end payload recovery

The OOK transmissions produced two electrical states. Figure 4 shows one AES-128 example transmission with a no-PFC supply. The pattern is visible at both receiver points. The office-level signal is mixed with other loads, but it retains a decodable structure. The decoder uses one scalar feature at a time. It does not classify the complete heatmap.

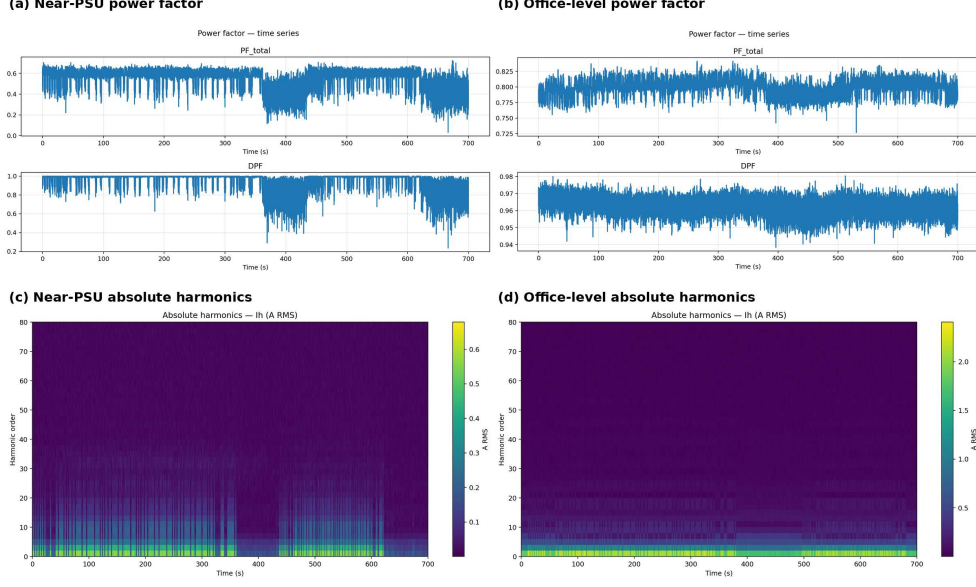


Fig. 4 Representative OOK transmission. Panels (a) and (b) show power-factor series near the PSU and at the office-level receiver. Panels (c) and (d) show absolute RMS current harmonics for the same AES-128 frame.

All three payload classes were recovered in selected configurations. The successful feature depended on PSU topology, receiver position, payload, and symbol duration. Table 4 summarizes reported valid decodes for the power-factor and harmonic feature set. The fractions count feature/configuration combinations within the recorded captures, not repeated independent trials.

Table 4 Valid power-quality decodes by configuration

PSU	Receiver	RMS valid	dBc valid	PF valid	Recovered A/K/E
No PFC	Near PSU	9/16	3/16	0/4	N/Y/Y
No PFC	Office level	9/16	6/16	0/4	Y/Y/Y
Passive PFC	Near PSU	14/16	3/16	2/4	Y/Y/Y
Passive PFC	Office level	7/16	5/16	0/4	Y/Y/Y
Active PFC	Near PSU	2/16	3/16	3/4	N/Y/Y
Active PFC	Office level	0/16	1/16	1/4	N/Y/N

RMS and dBc denominators are 16: four harmonic orders evaluated over four payload/duration settings (ASCII at 2 s, AES-128 at 1 s and 2 s, and ECDSA at 2 s). PF has one feature over the same four settings. These are not independent repetitions. A/K/E denotes recovery through at least one PF/harmonic feature for each payload. Active and apparent power are excluded. Counts use “Yes” outcomes in Additional file 1; RS-invalid candidates are excluded.

Complete per-feature and per-payload decoding outcomes are provided in Additional file 1.

Table 5 reports the lowest reported pre-correction BER among valid, unflagged PF/harmonic decodes in each row. The only non-zero best valid BER was 0.0069, for the passive-PFC, near-PSU ASCII transmission. At 0.5 bit/s, multiplication gives approximately 0.00345 erroneous bits per second over the compared symbols. This is a descriptive conversion for that recorded interval, not a long-term error-rate estimate.

Table 5 Best reported pre-correction bit-error rates

PSU	Receiver	Best BER A/K/E
No PFC	Near PSU	–/0/0
No PFC	Office level	0/0/0
Passive PFC	Near PSU	0.0069/0/0
Passive PFC	Office level	0/0/0
Active PFC	Near PSU	–/0/0
Active PFC	Office level	–/0/–

A zero denotes no reported bit difference in the compared interval. A dash denotes no valid payload recovery through the summarized PF/harmonic feature set. Entries flagged as unresolved in Additional file 1 are not used to select these minima. None of these entries estimates the expected channel BER.

5.3 Effect of PFC topology and receiver position

Within the recorded dataset, active PFC produced the fewest valid harmonic decodes at both receiver points. The near-PSU active-PFC row produced five valid harmonic combinations: two RMS and three dBc. The office-level row produced one. No-PFC and passive-PFC supplies retained larger harmonic feature sets, although the successful orders differed.

The successful feature set differed between receiver positions. The office-level capture did not always yield worse outcomes than the near-PSU capture. In particular, the no-PFC office-level receiver recovered all payload classes through at least one power-quality feature. These observations are not consistent with treating geometric separation alone as a predictor of decoding performance. Branching, concurrent loads, phase relations, and feature selection can affect separation. Because the positions were acquired separately without repetitions, this comparison does not isolate electrical-path effects from run-to-run variation.

The active-PFC office-level result was more restrictive. No absolute harmonic feature produced a valid decode in the summary. Only one relative-harmonic condition and one power-factor condition remained valid. This result is consistent with current shaping at the source and aggregation at the upstream receiver.

6 Discussion

The recorded experiments support three proof-of-concept findings. First, controlled CPU load changes can alter true power factor and low-order current harmonics. Second, these changes can carry complete low-volume payloads in selected configurations.

Third, the useful feature set differed across the tested PFC topologies and receiver positions.

The tested nominal rates are low. A 2-s symbol provides 0.5 bit/s raw, and a 1-s symbol provides 1 bit/s raw. Protocol overhead reduces payload goodput. These operating points are unsuitable for bulk transfer but remain relevant to compact secrets, commands, and beacons.

Rate and capacity scope. The tested rates are not a measured channel capacity or a maximum symbol rate. The receiver observes the grid-side response after PSU dynamics and finite-window feature estimation, rather than the CPU command directly. Shorter symbols may be smoothed by the measurement window or obscured by transients and background loads. The conservative 1-s and 2-s settings do not establish a minimum viable duration. Moreover, the tabulated signal-to-noise ratio (SNR) values do not specify an independently validated signal/noise estimator or a usable channel bandwidth, so they are not used to derive a Shannon-capacity estimate. Establishing a rate limit or sustained goodput would require the original processing settings, a symbol-duration sweep, and repeated independent transmissions.

6.1 Relation to prior power-line channels

The outbound transmitter is closest to PowerHammer because both systems encode symbols through CPU-load changes. The receiver is different. PowerHammer decodes raw current amplitude and emphasizes achievable rate [23]. This study converts synchronized voltage and current into true power factor and individual harmonic amplitudes. These derived quantities are standard outputs of power-quality analysis and expose both waveform shape and load-dependent scaling.

NoDE uses a complementary frequency range and physical mechanism. It exploits high-frequency switching ripple from active-PFC circuits [29]. The channel studied here relies on low-order distortion and becomes less observable with active PFC. Current shaping can therefore suppress the present feature space while leaving switching-frequency leakage available to a NoDE-style receiver.

PowerBridge also uses workload-driven power variation for outbound communication, but its receiver is a modified smart-plug power meter [28]. Its inbound path switches the target supply. The present study does not switch the supply and does not require a smart-plug receiver. It evaluates synchronized waveform-derived metrics at two points in the shared electrical path.

BREAKING TEMPEST overlaps with this study in the conducted medium and in workload-controlled outbound signaling. The experimental question is different. BREAKING TEMPEST decodes outbound symbols from line-current variation. It adds an inbound path by modulating line voltage, which the target reads through a PMBus interface. Its main contributions are bidirectionality, building-scale operation, and operation across TEMPEST-grade filters [1]. The present work is unidirectional. It does not inject line voltage, depend on PMBus, or test TEMPEST filters. Its contribution is the receiver feature space: true power factor and individual low-order current harmonics, evaluated across PFC topologies and receiver positions. The two studies therefore share the power line and the outbound workload source, but they measure different observables and answer different engineering questions.

6.2 Security implications

The electrical supply should be included in the threat model of high-assurance systems. Network isolation does not constrain conducted emissions.

Active PFC is a plausible mitigation factor for the tested low-order harmonic mechanism. Its smaller successful harmonic feature set is consistent with input-current shaping. The observations do not establish a category-wide reduction in attack success probability or make PFC a standalone security guarantee.

Power-quality monitoring may also provide a defensive sensor. A detector could search for sustained binary-like transitions in active power, apparent power, true power factor, or selected harmonic amplitudes. The main challenge is discrimination from legitimate workload variation.

Hardware integrity also matters. A defective or modified PFC stage may increase low-order distortion. Secure procurement and periodic electrical characterization can therefore complement software controls. Deliberate PFC degradation was outside this experiment.

6.3 Scope and future work

The central limitation is the single acquisition per configuration ($N = 1$). Multiple harmonics or many symbols within one capture do not replace independent transmissions. The study does not estimate expected BER, packet-success probability, confidence intervals, or statistical significance between configurations.

The evaluation used one target platform and one supply from each PFC category. It also used one office environment and two receiver points. PSU control laws, wiring topology, supply impedance, grounding, filters, temperature, and concurrent loads can change feature separability. The results therefore characterize the evaluated hardware and electrical path rather than every implementation in a PFC category.

The decoder uses one feature at a time. It uses a known preamble and searches timing, offset, and polarity. The expected payload is used only after decoding to calculate BER. False-alarm and missed-detection rates were outside the present evaluation. A deployment-oriented receiver should use blind packet handling and explicit detection thresholds.

Stealth was not measured. Full CPU-load transitions are visible to host telemetry. Lower-amplitude modulation may reduce host-level visibility, but it will also reduce electrical separation.

Full numerical reproduction also requires recovery of the original processing settings and resolution of the BER/count ambiguities documented in Additional file 1. These reporting limits are distinct from the absence of repeated runs.

Future work should first repeat configurations independently and evaluate a systematic range of symbol durations and background loads. Broader computing platforms, electrical paths, filtering arrangements, multifeature detectors, adaptive thresholds, error-control schemes, and defensive classification are relevant extensions.

7 Conclusions

Controlled CPU workload produced structured changes in true power factor and low-order current harmonics. Selected OOK configurations recovered complete test payloads at nominal raw rates of 0.5 and 1 bit/s. Recovery was possible near the PSU and at an upstream office-level point. With one acquisition per configuration, these results demonstrate feasibility in the evaluated captures, not run-to-run reliability.

Active PFC reduced the useful low-order harmonic feature set. No-PFC and passive-PFC supplies retained more valid harmonic decodes. Receiver position also changed which feature supported recovery. These results extend power-line covert-channel research from raw current and switching noise to derived power-quality metrics.

The study extends the receiver feature space for infrastructure-level covert channels to derived power-quality metrics. Its contribution is exploratory end-to-end feasibility and physical interpretation, rather than an optimized rate, a measured channel capacity, or a statistical characterization of reliability.

List of abbreviations

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BER	Bit-error rate
CPU	Central processing unit
DPF	Displacement power factor
ECDSA	Elliptic Curve Digital Signature Algorithm
OOK	On-off keying
PF	Power factor
PFC	Power-factor correction
PSU	Power-supply unit
RMS	Root mean square
RS	Reed–Solomon
SMPS	Switched-mode power supply
SNR	Signal-to-noise ratio
THD	Total harmonic distortion
dBc	Decibels relative to the fundamental component

Declarations

Ethics approval and consent to participate

Not applicable. The study did not involve human participants, human data, or animals.

Consent for publication

Not applicable.

Availability of data and materials

The dataset supporting the conclusions of this article is available in the Zenodo repository, <https://doi.org/10.5281/zenodo.21791997> [31]. The record contains experimental data, metadata, and processed outputs.

Code availability

Project name: Beyond TEMPEST reproduction scripts. Archived version: <https://doi.org/10.5281/zenodo.21791997>. Programming language: Python. Operating system: any platform supported by the documented dependencies. Execution instructions, dependency versions, licence, and applicable use conditions are included in the archive.

Competing interests

The authors declare that they have no competing interests.

Funding

The authors received no specific research grant for this work.

Authors' contributions

VHS conceptualized the study as part of his MSc research. He implemented the experimental and software pipeline, collected and analysed the data, curated the repository, and drafted the manuscript. RM supervised the research, refined the study design, interpreted the findings, and critically revised the manuscript. Both authors read and approved the final manuscript.

Acknowledgements

Not applicable.

Additional file

Additional file 1. PDF. *Complete decoding outcomes*. Reported results by payload, symbol duration, PSU topology, receiver position, and receiver feature, with single-run scope, corrected aggregation notes, and explicit markers for unresolved BER/error-count entries.

References

- [1] Balsdon TD, Grisel-Davy A, Fischmeister S (2026) Breaking tempest: Low-frequency bidirectional covert channel on power lines. In: Proceedings of the 12th International Conference on Information Systems Security and Privacy. SCITEPRESS - Science and Technology Publications, pp 422–433, <https://doi.org/10.5281/zenodo.21791997>.

org/10.5220/0014331000004061, URL <https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0014331000004061>

- [2] Guri M (2020) Cd-leak: Leaking secrets from audioless air-gapped computers using covert acoustic signals from cd/dvd drives. In: Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020. Institute of Electrical and Electronics Engineers Inc., pp 808–816, <https://doi.org/10.1109/COMPSAC48688.2020.0-163>
- [3] Guri M (2021) Exfiltrating data from air-gapped computers via vibrations. *Future Generation Computer Systems* 122:69–81. <https://doi.org/10.1016/j.future.2021.03.025>
- [4] Guri M (2021) Gairoscope: Leaking data from air-gapped computers to nearby smartphones using speakers-to-gyro communication. In: 2021 18th International Conference on Privacy, Security and Trust, PST 2021. Institute of Electrical and Electronics Engineers Inc., <https://doi.org/10.1109/PST52912.2021.9647842>
- [5] Guri M (2021) LANTENNA: Exfiltrating data from air-gapped networks via ethernet cables emission. In: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp 745–754, <https://doi.org/10.1109/COMPSAC51774.2021.00106>
- [6] Guri M (2021) Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields. *Future Generation Computer Systems* 115:115–125. <https://doi.org/10.1016/j.future.2020.08.045>
- [7] Guri M (2022) COVID-bit: Keep a distance of (at least) 2m from my air-gap computer! <https://doi.org/10.48550/arXiv.2212.03520>, arXiv:2212.03520
- [8] Guri M (2022) POWER-SUPPLaY: Leaking sensitive data from air-gapped, audio-gapped systems by turning the power supplies into speakers. *IEEE Transactions on Dependable and Secure Computing* <https://doi.org/10.1109/TDSC.2021.3133406>
- [9] Guri M (2023) Air-fi: Leaking data from air-gapped computers using wi-fi frequencies. *IEEE Transactions on Dependable and Secure Computing* 20:2547–2564. <https://doi.org/10.1109/TDSC.2022.3186627>
- [10] Guri M, Bykhovsky D (2019) air-jumper: Covert air-gap exfiltration/infiltration via security cameras and infrared (ir). *Computers and Security* 82:15–29. <https://doi.org/10.1016/j.cose.2018.11.004>
- [11] Guri M, Monitz M (2018) Lcd tempest air-gap attack reloaded. In: 2018 IEEE International Conference on the Science of Electrical Engineering in Israel (ICSEE). IEEE, pp 1–5, <https://doi.org/10.1109/ICSEE.2018.8646277>

- [12] Guri M, Kedma G, Kachlon A, et al (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, pp 58–67, <https://doi.org/10.1109/MALWARE.2014.6999418>
- [13] Guri M, Kachlon A, Hasson O, et al (2015) GSMem: Data exfiltration from air-gapped computers over gsm frequencies. In: 24th USENIX Security Symposium (USENIX Security 15). USENIX Association, Washington, D.C., pp 849–864, URL <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri>
- [14] Guri M, Monitz M, Mirski Y, et al (2015) Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In: 2015 IEEE 28th Computer Security Foundations Symposium. IEEE, pp 276–289, <https://doi.org/10.1109/CSF.2015.26>
- [15] Guri M, Hasson O, Kedma G, et al (2016) VisiSploit: An optical covert-channel to leak data through an air-gap. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp 642–649, <https://doi.org/10.1109/PST.2016.7906933>, URL <https://arxiv.org/abs/1607.03946>
- [16] Guri M, Monitz M, Elovici Y (2016) Usbee: Air-gap covert-channel via electromagnetic emission from usb. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp 264–268, <https://doi.org/10.1109/PST.2016.7906972>
- [17] Guri M, Solewicz Y, Daidakulov A, et al (2016) Diskfiltration: Data exfiltration from speakerless air-gapped computers via covert hard drive noise. arXiv:1608.03431
- [18] Guri M, Zadov B, Elovici Y (2017) LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led. In: Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2017), Lecture Notes in Computer Science, vol 10327. Springer, pp 161–184, https://doi.org/10.1007/978-3-319-60876-1_8, URL <https://arxiv.org/abs/1702.06715>
- [19] Guri M, Solewicz Y, Elovici Y (2018) Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication. In: 2018 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, pp 1–8, <https://doi.org/10.1109/DESEC.2018.8625124>
- [20] Guri M, Zadov B, Daidakulov A, et al (2018) xled: Covert data exfiltration from air-gapped networks via switch and router leds. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp 1–12, <https://doi.org/10.1109/PST.2018.8514196>

- [21] Guri M, Zadov B, Bykhovsky D, et al (2019) CTRL-ALT-LED: Leaking data from air-gapped computers via keyboard leds. In: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), vol 1. IEEE, pp 801–810, <https://doi.org/10.1109/COMPSAC.2019.00118>
- [22] Guri M, Solewicz Y, Elovici Y (2020) Fansmitter: Acoustic data exfiltration from air-gapped computers via fans noise. *Computers and Security* 91. <https://doi.org/10.1016/j.cose.2020.101721>
- [23] Guri M, Zadov B, Bykhovsky D, et al (2020) PowerHammer: Exfiltrating data from air-gapped computers through power lines. *IEEE Transactions on Information Forensics and Security* 15:1879–1890. <https://doi.org/10.1109/TIFS.2019.2952257>
- [24] Guri M, Zadov B, Elovici Y (2020) Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security* 15:1190–1203. <https://doi.org/10.1109/TIFS.2019.2938404>
- [25] IEEE (2025) IEEE Standard Definitions for the Measurement of Electric Power Quantities Under Sinusoidal, Nonsinusoidal, Balanced, or Unbalanced Conditions. IEEE Std 1459-2025, <https://doi.org/10.1109/IEEESTD.2025.11004570>
- [26] International Electrotechnical Commission (2024) Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for harmonic current emissions (equipment input current up to and including 16 A per phase). IEC 61000-3-2:2018+AMD1:2020+AMD2:2024 CSV
- [27] Liang Y, Shan H, Liu Z, et al (2024) Bit sufi-dance: Covert data exfiltration from air-gapped networks via electricity meter. *Electronics (Switzerland)* 13. <https://doi.org/10.3390/electronics13214198>
- [28] Liang Y, Shan H, Luo Z, et al (2024) Powerbridge: Covert air-gap exfiltration/infiltration via smart plug. *Applied Sciences* 14(14):6321. <https://doi.org/10.3390/app14146321>, URL <https://doi.org/10.3390/app14146321>
- [29] Shao Z, Islam MA, Ren S (2020) Your noise, my signal: Exploiting switching noise for stealthy data exfiltration from desktop computers. *arXiv preprint arXiv:200106729* URL <https://arxiv.org/abs/2001.06729>
- [30] Silva VH (2026) Data exfiltration. Msc dissertation in information security, Faculty of Sciences, University of Porto
- [31] Silva VH, Martins R (2026) Workload-modulated power-quality covert channels in air-gapped systems: Dataset and reproduction scripts. Zenodo research data repository, <https://doi.org/10.5281/zenodo.21791997>, URL <https://doi.org/10.5281/zenodo.21791997>, dataset and reproduction scripts

- [32] Sun X, Zheng Y, Xi W, et al (2025) TEMPEST-LoRa: Cross-technology covert communication. <https://doi.org/10.1145/3719027.3744817>, arXiv:2506.21069
- [33] Ullah F, Edwards M, Ramdhany R, et al (2018) Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications* 101:18–54. <https://doi.org/10.1016/j.jnca.2017.10.016>
- [34] Zhan Z, Zhang Z, Koutsoukos X (2020) Bitjabber: The world’s fastest electromagnetic covert channel. In: 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, pp 35–45, <https://doi.org/10.1109/HOST45689.2020.9300268>
- [35] Zhao B, Ni M, Fan P (2018) Powermitter: Data exfiltration from air-gapped computer through switching power supply. *China Communications* 15(2):170–189. <https://doi.org/10.1109/CC.2018.8300280>

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [supplementarytable.pdf](#)