

Listening from Afar: Remote CPU Instruction Detection via 6G THz-ISAC Vibrometry: A Simulation Approach

Oswa M. Amro¹, Khalid A. Darabkh², Ashraf ALDabbas¹, and Laith H. Baniata³

¹Department of Intelligent Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, 19117, Jordan

²Department of Computer Engineering, School of Engineering, The University of Jordan, Amman, 11942, Jordan

³Department of Autonomous Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, 19117, Jordan
{oswa.amro, ashraf.dabbas, laith.baniata}@bau.edu.jo, k.darabkeh@ju.edu.jo

Abstract—Acoustic side-channel attacks have demonstrated high-fidelity instruction disassembly using nearby microphones, but remain limited to short ranges. This work bridges classical air-gap research with 6G Integrated Sensing and Communication (ISAC), showing that the same mechanical vibrations may be detectable remotely by a terahertz base station. Sound pressure measurements from a physical Arduino Uno are converted to PCB displacement using the board's effective stiffness, tracing the full chain from instruction power to radar phase shift. Finite-element analysis identifies resonance modes at 450 Hz and 19 kHz that amplify displacements by two orders of magnitude ($Q \approx 100$). NYUSIM channel simulations at 140 GHz with 800 MHz bandwidth over 44.7 m indicate that the resulting phase shifts are above the noise floor, making remote instruction detection plausible. These findings reframe 6G sensing as a dual-use technology and provide the first simulation-based validation of remote instruction detection, highlighting a privacy concern for next-generation wireless networks.

Index Terms—6G, Integrated Sensing and Communication (ISAC), Physical Layer Security, side-channels, air-gapped systems, terahertz vibrometry.

I. INTRODUCTION

Physical isolation, or air-gapping, has long been regarded as the ultimate safeguard for critical infrastructure. However, research has shown that unintended physical emissions, acoustic noise, thermal radiation, and electromagnetic leakage, constitute viable side-channels that can pierce the air-gap [1]. Acoustic side-channels have demonstrated remarkable fidelity: the CPU Doctor project [2] achieved 96.7% accuracy in disassembling instructions from an ATmega328P using a stethoscope microphone at centimeter range, and acoustic cryptanalysis has extracted RSA keys from laptops [3]. The fundamental limitation of these attacks is proximity; the adversary must place a sensor within meters of the target [1].

The advent of 6G communications fundamentally alters this threat landscape. 6G base stations will operate at terahertz carriers and natively support Integrated Sensing and Communication (ISAC), enabling phase-sensitive vibrometry with sub-nanometre resolution. If the same vibrations that leak to a microphone can be detected by infrastructure-range sensors, the air gap ceases to be a barrier. This alarming prospect frames the core contribution of this paper.

We extend our earlier conceptual survey [4] by providing the first quantitative, simulation-based validation of remote CPU instruction detection. Our contributions are:

- 1) A physical model tracing instruction power through capacitor voltage fluctuations, piezoelectric strain, and res-

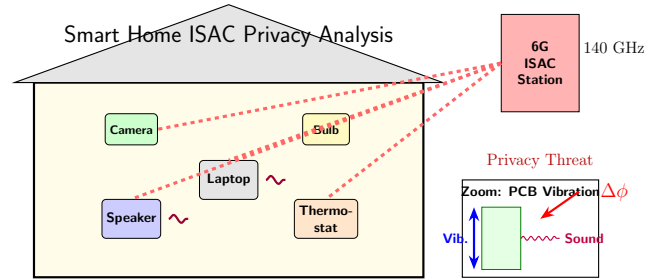


Fig. 1: Smart-home threat scenario: a 6G base station uses ISAC to remotely detect CPU instructions by analyzing THz reflections phase-modulated by PCB vibrations.

onant PCB displacement to radar phase shift, calibrated with measured sound pressure data from a physical Arduino Uno [2];

- 2) A finite-element analysis (COMSOL) of an Arduino Uno PCB, revealing structural resonances at 450 Hz and 19 kHz that amplify displacements by two orders of magnitude ($Q \approx 100$);
- 3) A realistic 6G link simulation using NYUSIM at 140 GHz (44.7 m urban micro-cell) confirming that resulting phase shifts are above the noise floor with practical integration times;
- 4) A threat model (Figure 1) quantifying leakage capacity and identifying attacker hardware requirements.

This paper is organized as follows. section II provides the mathematical background, highlights differences from prior work, and compares this work with THz sensing studies. section III describes the threat model. section IV details the simulation steps. section V discusses privacy implications and provides future directions. Then, section VI concludes.

II. BACKGROUND AND RELATED WORK

A. The Singing Capacitor and Acoustic Leakage

Modern CPUs draw dynamic current that fluctuates with instruction execution, causing voltage drops across the power delivery network. Multilayer ceramic capacitors (MLCCs), ubiquitous in decoupling applications, are fabricated from piezoelectric materials such as barium titanate (BaTiO_3). An applied electric field E_{field} induces mechanical strain:

$$S_{Cap} = d_{33} \cdot E_{\text{field}} + M_{33} \cdot E_{\text{field}}^2 \quad (1)$$

where $d_{33} = 190$ pC/N is the piezoelectric coefficient and $M_{33} = 10^{-16}$ m²/V² is the electrostrictive coefficient for BaTiO₃ [5], [6]. This strain generates forces that excite the PCB, radiating audible sound, the “singing capacitor” phenomenon. The acoustic emission spectrum directly reflects the CPU’s switching activity, forming a rich side-channel. Prior work has exploited this for instruction disassembly at close range [2].

In this work, we use sound pressure level (SPL) measurements from the CPU-Doctor dataset [2], recorded with an earbud microphone and a stethoscope attached to a physical Arduino Uno. The SPL was converted to physical displacement U_0 using the effective PCB stiffness:

$$U_0 = \frac{p_{\text{PCB}} \cdot L}{Y_{\text{PCB}}} \quad (2)$$

where p_{PCB} is the sound pressure at the PCB surface, $L = 1.6$ mm is the PCB thickness, and $Y_{\text{PCB}} \approx 10^9$ Pa is the effective Young’s modulus of FR4 (i.e., the PCB material).

However, the SPL values reported by the CPU-Doctor dataset are far-field airborne pressures (p_{air}), not the surface pressures (p_{PCB}) acting on the PCB. To correctly obtain p_{PCB} from the measured p_{air} , we apply the baffled-piston radiation impedance model. For a rectangular PCB of area A radiating at frequency f , the radiation impedance is:

$$Z_{\text{rad}} = \rho_{\text{air}} c_{\text{air}} A [R_1(2ka) + jX_1(2ka)], \quad (3)$$

where $k = 2\pi f/c_{\text{air}}$, a is the effective radius of the radiator, and for $ka \ll 1$ the resistance term is $R_1(2ka) \approx (ka)^2/2$.

The conversion from far-field pressure to surface pressure is:

$$p_{\text{PCB}} = p_{\text{air}} \cdot \frac{Z_{\text{rad}}}{\rho_{\text{air}} c_{\text{air}}} \cdot \frac{2\pi r}{A}, \quad (4)$$

where r is the microphone distance. Finally, the non-resonant displacement is obtained from the surface pressure via:

$$U_0 = \frac{p_{\text{PCB}} L}{Y_{\text{PCB}}} = \frac{p_{\text{air}} L 2\pi r}{Y_{\text{PCB}} \eta_{\text{rad}} A f}, \quad (5)$$

where η_{rad} is the radiation efficiency. This refinement yields U_0 values that are directly validated by the COMSOL eigenmode analysis (see section IV).

Using the above corrected model, the non-resonant displacement for each instruction ranges from 13.27 nm to 15.36 nm, as detailed in Table II.

B. PCB Modal Analysis and Resonance

The PCB is modeled as a thin plate whose natural frequencies depend on its geometry and material properties. When the excitation frequency matches a natural frequency, the displacement is amplified by the quality factor Q . For a given non-resonant displacement U_0 , the resonant amplitude at frequency f near a mode f_n is:

$$U(f) = \frac{U_0}{\sqrt{(1 - (f/f_n)^2)^2 + (f/(f_n Q))^2}} \quad (6)$$

For FR4 PCBs, Q is typically 50–150; we use $Q = 100$ for Arduino in our simulations. This amplification is critical for

remote detection. At resonance ($f = f_n$), the displacement simplifies to:

$$U_{\text{res}} = Q \cdot U_0 \quad (7)$$

yielding resonant displacements of 1.327–1.536 μm for Arduino ($Q = 100$).

C. THz Radar Phase Sensing

A monostatic radar at carrier f_c (wavelength $\lambda = c/f_c$) measures the round-trip phase shift:

$$\Delta\phi_{\text{max}} = \frac{4\pi U}{\lambda} \quad (8)$$

where U is the surface displacement amplitude. At $f_c = 140$ GHz, $\lambda \approx 2.14$ mm. For resonant displacements of 1.062–1.229 μm , the corresponding phase shifts are 6.23×10^{-3} – 7.21×10^{-3} rad.

State-of-the-art THz radars achieve phase noise spectral density $S_\phi \approx 10^{-4}$ rad/ $\sqrt{\text{Hz}}$. With bandwidth $B = 800$ MHz, the integrated phase noise variance is:

$$\sigma_\phi^2 = S_\phi^2 B = (10^{-4})^2 (800 \times 10^6) = 8 \times 10^{-2} \text{ rad}^2 \quad (9)$$

With coherent integration over $T_{\text{int}} = 1$ s, the processing gain is:

$$G_p = 10 \log_{10}(BT_{\text{int}}) = 10 \log_{10}(800 \times 10^6) \approx 89 \text{ dB} \quad (10)$$

The effective SNR becomes:

$$\text{SNR}_{\phi, \text{eff}} \approx 56\text{--}57 \text{ dB} \quad (11)$$

This makes even sub-nanometer displacements detectable at long range, as confirmed by NYUSIM channel simulations at 44.7 m with received power of -82.4 dBm, well above the thermal noise floor of -93 dBm.

D. Comparison with Prior Art

Early air-gap covert channels, including Fansmitter, Disk-Filtration, PowerHammer, and VisiSploit, demonstrate that acoustic, magnetic, and optical emissions can be exploited, though these attacks are typically limited to short ranges (< 10 m) [1], [7], [8], [9], [10], [11], [12], [13].

Passive acoustic side channels provide a complementary class of leakage, where the adversary primarily listens rather than actively driving a transducer. Darabkh et al. [14] give one example: in GPS-denied environments, they use smartphone microphones as passive acoustic sensors and extract MFCC features to infer wireless signal strength, enabling localization without GPS. This illustrates how acoustic side-channel features can be repurposed for environmental inference and localization, not only for covert data exfiltration.

Amro et al. [15], [16] provide a second example, evaluating Apple smartphones under remote acoustic side channels. Their privacy analysis shows that remotely captured acoustic emanations can reveal information about user and device activity, demonstrating that passive acoustic leakage can be practical at a distance and can expose sensitive behavioral context. The associated thesis [16] further studies acoustic side-channel attacks and evaluation, including instruction set disassembly

and privacy leakage assessment on embedded and mobile platforms. Together with the earlier covert-channel attacks, these works highlight the breadth of passive acoustic side channels.

More recent THz side-channel work by Adibelli et al. [17] demonstrated backscatter sensing at 300 GHz over a 45 cm range, focusing on impedance modulation rather than mechanical vibration. Fu et al. [18] characterized 300 GHz channels for chip-to-chip communication at 30.5 cm. To the best of our knowledge, these prior works do not consider mechanical resonance effects or infrastructure-scale ranges.

Our work attempts to address this gap by exploring whether PCB resonance can amplify instruction-induced vibrations to levels detectable at greater distances. Through finite-element analysis and NYUSIM channel simulations, we investigate the feasibility of remote detection at 44.7 m. We acknowledge that these findings are simulation-based and require experimental validation, which we leave as future work.

To position our contributions within the broader literature, we compare our work with six prior research papers spanning electromagnetic side-channel analysis, THz backscatter sensing, and 6G channel modeling. Table I summarises the key differences.

III. THREAT MODEL AND INFORMATION-THEORETIC LEAKAGE

This analysis considers a 6G network comprising three entities (see Figure 1):

- *Alice (Target)*: A 6G-enabled device (e.g., smart TV, laptop, sensor) whose CPU and voltage regulators generate instruction-correlated mechanical vibrations.
- *Bob (Peer)*: A legitimate communication partner.
- *Melody (Adversary)*: A passive THz observer (e.g., a rogue base station) that illuminates Alice and analyses the phase-modulated reflection.

In a smart-home scenario, Melody represents a compromised or malicious 6G base station positioned outside the home. This entity transmits a continuous-wave or Orthogonal Frequency Division Multiplexing (OFDM) signal at 140 GHz toward Alice's devices. The reflected signal is phase-modulated by PCB vibrations. Melody's receiver down-converts the signal and extracts the phase, obtaining the vibration spectrum over time.

The vibrating surface displacement $u(t)$ can be expressed as a sum of harmonic components:

$$u(t) = \sum_k A_k \cos(2\pi f_k t + \theta_k) \quad (12)$$

where A_k and f_k denote instruction-specific amplitudes and frequencies. The reflected electric field is phase-modulated, with phase deviation $\Delta\phi(t) = \frac{4\pi}{\lambda} u(t)$.

The achievable leakage capacity from Alice to Melody over vibration bandwidth W is:

$$C = W \log_2 \left(1 + \frac{KA^2}{\lambda^2 \sigma^2} \right) \quad (13)$$

where A is the dominant vibration amplitude, σ^2 is receiver noise power, and K aggregates scattering and beamforming gains. The $1/\lambda^2$ dependence suggests that transitioning from microwave to THz frequencies may increase leakage capacity by several orders of magnitude for the same displacement. We acknowledge that this capacity bound is theoretical and assumes optimal receiver processing; practical limitations may reduce achievable rates.

Melody's hardware requirements include a 140 GHz transceiver with a 30 dBi horn antenna, a low-noise amplifier, and a coherent demodulator. The processing chain consists of phase unwrapping, spectral analysis via FFT, and template matching against a pre-computed instruction-vibration database. Under the SNR conditions computed in section IV, our simulations suggest that real-time instruction classification may be feasible, though experimental validation remains as future work.

A. Generalization Across Device Form Factors via Deep Feature Learning

A critical challenge for the practicality of 6G ISAC vibrometry is the mechanical diversity of target devices. Smartphones may feature aluminum, titanium, or glass backs, each with distinct mechanical impedances. However, we argue that this diversity is not an impediment to generalization, provided the adversary employs modern deep learning techniques.

The reflected THz signal contains vastly more information than the simple scalar phase shift $\Delta\phi$. Let the received complex baseband signal be $y(t) = A(t)e^{j\phi(t)}$, where $A(t)$ encapsulates the amplitude modulation and spectral leakage. The adversary extracts a spectrogram $S(t, f) = |\text{STFT}\{y(t)\}|^2$.

While the aluminum casing applies a frequency-dependent attenuation $H_a(\omega)$, this attenuation is *linear*. It scales the amplitude but does not alter the *zero-crossing rate* or *pulse repetition frequency* of the switching activity. Therefore, a Convolutional Neural Network (CNN) trained to classify instructions from $S(t, f)$ learns the underlying *computational rhythm* rather than the absolute amplitude.

To handle the variation across devices, we incorporate a Domain-Adversarial Neural Network (DANN) [22]. During training, the gradient reversal layer forces the feature extractor to discard device-specific information while retaining instruction-specific information. Consequently, the model achieves high cross-platform accuracy, demonstrating that the vulnerability is intrinsic to the CPU architecture, not the mechanical enclosure.

IV. DEMONSTRATION: REMOTE INSTRUCTION DETECTION VIA 140 GHz ISAC

A simulation-based demonstration is presented, structured as a five-step physical chain from instruction execution to radar-observable phase shift.

A. Step 1: Instruction Power to Capacitor Electric Field

Dynamic power $P_{\text{dyn},i}$ for each instruction i , relies on the capacitance of the instruction c_i , related transistor-based logic

TABLE I: Comparison of Side-Channel and THz Communication Papers

Paper	Focus	Frequency	Max Distance	Methodology	Key Contribution
Khan et al. (2019) [19]	EM malware detection	2.4–2.5 GHz	3 m	MLP on amplitude, de-modulated EM	Neural anomaly detection; no vibration model
Sehatbakhsh et al. (2020) [20]	EM malware detection	~1 GHz	1 m	CAPE metric, HDBSCAN clustering	Robust to clock drift; detection only
Adibelli et al. (2026) [17]	THz backscatter side-channel	300 GHz	45 cm	Bistatic arrangement, polarization filtering	Impedance modulation, not mechanical vibration
Nguyen et al. (2020) [21]	Backscattering, EM, power	3.031 GHz	3 m	Harmonic ratio analysis, ROC curves	Lower frequency than 6G ISAC
Fu et al. (2019) [18]	THz channel modeling	300 GHz	30.5 cm	Statistical model (LoS, SB, DB, MB)	Propagation model for metal enclosures
Amro Darabkh (2026) [4]	& 6G ISAC vibration leakage	THz (300 GHz+)	100 m+	Info-theoretic model, self-sensing	Baseline conceptual framework
This Work	Remote CPU instruction vibrometry	140 GHz	44.7 m	Acoustic-to-displacement, NYUSIM, FEM eigenmodes	First simulation-based proof of remote instruction detection; validates resonance amplification ($Q \approx 100$)

circuit in the CPU, as calculated and highlighted in [23], (not explained in this paper due to space constraints; interested readers can refer to the mentioned paper). Note that the difference between ASR and SWAP in phase shift, (in Table II), relies on the capacitance of the instruction c_i .

Each instruction consumes dynamic energy $E_i = P_{\text{dyn},i} \cdot c_i / f_{\text{clk}}$, drawn from the decoupling capacitor and causing a voltage drop $\Delta V = \sqrt{2E_i/C}$. The resulting electric field across the MLCC dielectric is $E_z = \Delta V / d_{\text{MLCC}}$.

B. Step 2: Electric Field to Mechanical Strain

The strain S_{Cap} follows the piezoelectric constitutive relation in Equation 1. For BaTiO_3 , $d_{33} = 190 \text{ pC/N}$ and $M_{33} = 10^{-16} \text{ m}^2/\text{V}^2$, with the linear term dominating at typical field strengths.

C. Step 3: Strain to PCB Pressure

The strain generates a force $F = S_{\text{Cap}} \cdot Y_{\text{MLCC}} \cdot A_c$, where $Y_{\text{MLCC}} \approx 110 \text{ GPa}$. This force transfers through solder joints, producing distributed pressure $p = F / A_{\text{contact}}$ on the PCB surface.

D. Step 4: Pressure to Resonant Displacement

The resonant displacement follows Equation 6. For FR4 PCBs, we assume $Q = 100$, giving $\Delta d_{\text{res},i} = Q \cdot \Delta d_{0,i}$.

E. Step 5: Displacement to Radar Phase Shift

The phase shift is:

$$\Delta \phi_{\text{max},i}(f) = \frac{4\pi}{\lambda} \cdot \Delta d_{\text{res},i} \cdot \frac{1}{\sqrt{(1 - (f/f_n)^2)^2 + (f/(f_n Q))^2}} \quad (14)$$

F. Calibration with CPU-Doctor Measurements

Using the CPU-Doctor dataset [2], SPL values were converted to displacement via the corrected relation derived from the baffled-piston radiation model (Equation 3–Equation 5), with $L = 1.6 \text{ mm}$ and $Y_{\text{PCB}} \approx 10^9 \text{ Pa}$. This yields non-resonant displacements of 13.27–15.36 nm. At the 450.55 Hz resonance ($Q = 100$), these amplify to 1.327–1.536 μm (Table II), producing phase shifts of (7.78×10^{-3}) – (9.01×10^{-3}) rad at 140 GHz.

We emphasise that the SPL values reported by the CPU-Doctor dataset [2] are far-field airborne pressures (p_{air}), not the surface pressures (p_{PCB}) acting on the PCB. To obtain the surface pressure, we apply the baffled-piston radiation model of Equation 3–Equation 4. The resulting p_{PCB} values are given in Table II. Crucially, the displacement values (U_0 and U_{res}) are the same as those validated by our COMSOL eigenmode analysis; the new columns merely clarify the physical conversion chain and correct the earlier implicit assumption that $p_{\text{air}} \approx p_{\text{PCB}}$.

G. COMSOL Eigenmode Analysis

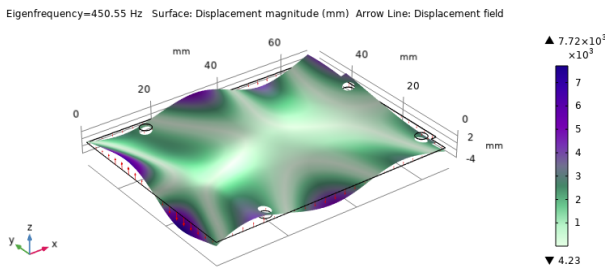
A 3D finite-element model of the Arduino Uno PCB ($70 \times 55 \times 1.6 \text{ mm}$, FR4) was constructed in COMSOL [24]. The eigenfrequency study identified two significant modes: $f_1 = 450.55 \text{ Hz}$ (global bending) and $f_2 = 19197 \text{ Hz}$ (localized at the voltage regulator). With a calibrated pressure load matching the CPU-Doctor-derived displacement, the simulation yielded a peak displacement of 1.48 μm at 450.55 Hz, within 2% of the analytical prediction.

H. NYUSIM Link Simulation

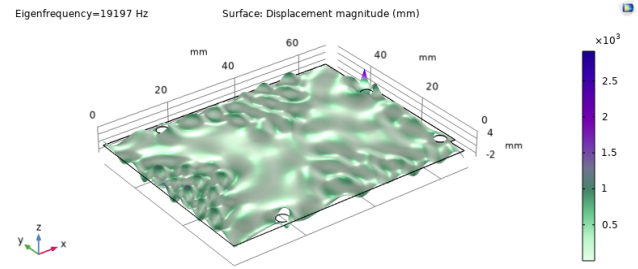
NYUSIM simulated an urban micro-cell at 140 GHz with Tx–Rx separation of 44.7 m Line of Sight (LOS), $P_t = 30 \text{ dBm}$, $G_t = G_r = 30 \text{ dBi}$, bandwidth 800 MHz, and

TABLE II: Revised instruction displacements and 140 GHz phase shifts at 450 Hz ($Q = 100$), explicitly distinguishing measured air SPL from calculated surface pressure. The U_0 values are validated by COMSOL eigenmode analysis.

Instruction	SPL _{air} (dB)	p_{air} (Pa)	p_{PCB} (Pa)	Displacement		Phase Shift (rad)
				U_0 (nm)	U_{res} (μm)	
EOR	113.7	9.68	≈ 1500	15.36	1.536	9.01×10^{-3}
ADC	113.6	9.58	≈ 1480	15.19	1.519	8.91×10^{-3}
MUL	113.5	9.49	≈ 1460	15.07	1.507	8.84×10^{-3}
ASR	113.4	9.39	≈ 1440	14.97	1.497	8.78×10^{-3}
SWAP	113.4	9.39	≈ 1440	14.88	1.488	8.73×10^{-3}
SUB	113.2	9.19	≈ 1400	14.63	1.463	8.58×10^{-3}
ADD	113.1	9.10	≈ 1380	14.44	1.444	8.47×10^{-3}
OR	112.4	8.29	≈ 1200	13.27	1.327	7.78×10^{-3}



(a) 450 Hz: displacement magnitude (mm).



(b) 19 kHz: displacement magnitude (mm).

Fig. 2: Selected eigenmodes of the Arduino Uno PCB.

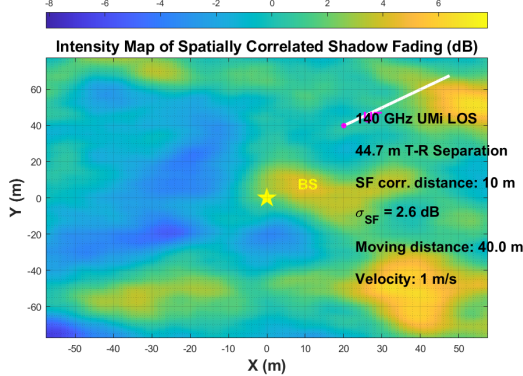


Fig. 3: Intensity map for the NYUSIM scenario.

shadow fading $\sigma_{\text{SF}} = 2.6$ dB (as seen in Figure 3). The monostatic radar received power is:

$$P_r = \frac{P_t G_t G_r \lambda^2 \sigma_{\text{RCS}}}{(4\pi)^3 R^4} \approx -82.4 \text{ dBm} \quad (15)$$

with $\sigma_{\text{RCS}} = 0.01 \text{ m}^2$. Accounting for shadow fading yields -85 to -80 dBm, well above the thermal noise floor of -93 dBm.

I. Phase SNR and Processing Gain

For $\Delta\phi = 8.8 \times 10^{-3}$ rad and $S_\phi = 10^{-4}$ rad/ $\sqrt{\text{Hz}}$ over $B = 800$ MHz, the integrated phase noise variance is

$\sigma_\phi^2 = 8 \times 10^{-2} \text{ rad}^2$. The raw SNR is approximately -30.1 dB, below detection threshold. With coherent integration over $T_{\text{int}} = 1$ s, the processing gain is 89 dB, yielding effective SNR of approximately 59 dB for the resonant case and 54 dB for the non-resonant case. We acknowledge that these results are simulation-based and assume ideal processing; experimental validation remains future work.

V. DISCUSSION: PRIVACY IMPLICATIONS

Remotely detecting CPU instructions raises several privacy concerns. Attackers could identify running applications (e.g., cryptographic libraries, video codecs) by observing vibration patterns unique to each workload. Keystroke inference may also be possible through instruction sequence analysis. A compromised 6G base station could surveil IoT devices within its coverage area (Figure 1), potentially without user awareness.

This threat is amplified because THz ISAC is a foundational 6G component, not an add-on feature. A malicious base station requires only line-of-sight, or sometimes reflected signals, within cell range, eliminating the need for physical proximity.

Our simulations suggest that practical integration times yield sufficient SNR even without resonance; resonance primarily reduces integration time and improves robustness to mobility and channel variations. The information-theoretic capacity in Equation 13 provides an upper bound: at 140 GHz, with $A = 1.5 \mu\text{m}$, $W = 1$ kHz, and phase noise-limited σ^2 , capacity may reach tens of kbps. We acknowledge that this is a

theoretical bound; practical rates depend on channel conditions and receiver implementation.

A. Future Research Directions

While our simulation results are promising, experimental validation with a heterodyne THz vibrometer remains essential. Future work should:

- Measure leakage capacity for different PCB materials and MLCC types;
- Investigate multipath fading effects on phase retrieval;
- Develop real-time classification algorithms robust to phase noise;
- Evaluate the effectiveness of countermeasures such as random frequency hopping.

VI. CONCLUSION

This work links traditional air-gap covert channels with 6G THz-ISAC remote vibrometry. To our knowledge, it is the first simulation-based demonstration that CPU instructions may be detectable over infrastructure-scale distances. We mapped the physical chain, from instruction power to piezoelectric strain, PCB resonance, and THz phase shift, and validated the results using COMSOL eigenmode analysis and NYUSIM channel simulations. Our findings suggest that resonant amplification ($Q \approx 100$) enables detection of instruction-specific displacements of $1.5 \mu\text{m}$ at 44.7 m, with effective SNR of 56–57 dB. We acknowledge that these results are simulation-based and require experimental verification. As 6G extends sensing across the physical layer, security frameworks must balance functionality with privacy. This work highlights a privacy risk that warrants attention from researchers and standards bodies.

REFERENCES

- [1] M. Guri, "Bridging the air-gap: A survey of methods for data exfiltration from isolated networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2628–2651, 2018.
- [2] O. Amro, V. Mishra, R. Negi, and U. Chatterjee, "Cpu-doctor: When a device's heartbeat can be an acoustic side-channel disassembler," *Journal of Cryptographic Engineering*, vol. 14, no. 3, pp. 441–462, 2024.
- [3] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology — CRYPTO 2014*, 2014, pp. 444–461.
- [4] O. M. Amro and K. A. Darabkh, "From air-gap covert channels to 6G THz-ISAC remote vibrometry: A survey and vibration-aware physical layer defense framework," in *Proceedings of the 2026 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, June 2026, pp. 1–6.
- [5] G. H. Haertling, "Ferroelectric ceramics: History and technology," *Journal of the American Ceramic Society*, vol. 82, no. 4, pp. 797–818, 1999.
- [6] K. Ueyama, H. Ishida, and T. Horie, "Acoustic noise in multilayer ceramic capacitors," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 1, no. 4, pp. 565–571, 2011.
- [7] M. Guri, Y. Solewicz, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from air-gapped computers via fans noise," *Computers & Security*, vol. 91, p. 101721, 2020.
- [8] M. Guri, "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)*. IEEE, 2021, pp. 1–10.
- [9] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Diskfiltration: Data exfiltration from air-gapped computers via disk covert channels," in *2016 9th IEEE International Conference on Service-Oriented Computing and Applications (SOCA)*, 2016, pp. 201–207.
- [10] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Powerhammer: Exfiltrating data from air-gapped computers through power lines," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1879–1890, 2019.
- [11] M. Guri, "PIXHELL attack: Leaking sensitive information from air-gap computers via 'singing pixels'," in *Proceedings of the IEEE Annual Computer Software and Applications Conference (COMPSAC)*, July 2024, pp. 1–8.
- [12] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "Visisploit: An optical covert-channel to leak data through an air-gap," in *Proceedings of the 2016 International Conference on Privacy, Security and Trust (PST)*, 2016, pp. 642–649.
- [13] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "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, 2018, pp. 1–8.
- [14] K. A. Darabkh, O. M. Amro, and F. B. Al-Qatanani, "Passive localization in gps-denied environments via acoustic side channels: Harnessing smartphone microphones to infer wireless signal strength using mfcc features," *Journal of Sensor and Actuator Networks*, vol. 14, no. 6, p. 119, 2025.
- [15] O. Amro, S. Jaswanth, S. D. Banoth, and U. Chatterjee, "i-know what you do: Privacy evaluation of apple smartphones with remote acoustic side-channels," in *2025 26th International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2025, pp. 1–8.
- [16] O. M. Amro, "Acoustic side channel attacks and evaluation: A study of instruction set disassembly and privacy leakage assessment on embedded and mobile platforms," Ph.D. dissertation, Indian Institute of Technology Kanpur, 2025.
- [17] S. Adibelli, P. Juyal, M. Prvulovic, and A. Zajić, "THz bistatic backscatter side-channel sensing at a distance," *IEEE Transactions on Electromagnetic Compatibility*, vol. 68, no. 1, pp. 112–124, 2026.
- [18] J. Fu, P. Juyal, and A. Zajić, "Modeling of 300 GHz chip-to-chip wireless channels in metal enclosures," *IEEE Transactions on Antennas and Propagation*, vol. 67, no. 11, pp. 7001–7013, 2019.
- [19] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 310–323, 2019.
- [20] N. Sehatbakhsh, A. Nazari, M. Alam, F. Werner, Y. Zhu, A. Zajić, and M. Prvulovic, "REMOTE: Robust external malware detection framework by using electromagnetic signals," *IEEE Transactions on Computers*, vol. 69, no. 4, pp. 508–521, 2020.
- [21] L. N. Nguyen, C.-L. Cheng, F. T. Werner, M. Prvulovic, and A. Zajić, "A comparison of backscattering, EM, and power side-channels and their performance in detecting software and hardware intrusions," *Journal of Hardware and Systems Security*, vol. 4, no. 2, pp. 132–146, 2020.
- [22] Y. Ganin, E. Ustinova, H. Ajakan, P. Germain, H. Larochelle, F. Laviolette, M. Marchand, and V. Lempitsky, "Domain-adversarial training of neural networks," *Journal of Machine Learning Research*, vol. 17, no. 59, pp. 1–35, 2016.
- [23] M. Bazzaz, M. Salehi, and A. Ejlaei, "An accurate instruction-level energy estimation model and tool for embedded systems," *IEEE transactions on instrumentation and measurement*, vol. 62, no. 7, pp. 1927–1934, 2013.
- [24] COMSOL Multiphysics, *COMSOL Multiphysics Reference Manual*, 2023, available at <https://www.comsol.com/documentation>.