The Ultrasonic Jammer

Daniel Hoasov Cohen *, Coral Raz *, Raz Ben Yehuda, Nezer J. Zaidenberg

Posted Date: 7 April 2026

doi: 10.20944/preprints202604.0405.v1

Keywords: ultrasound; security; communication

 doi:10.20944/preprints202604.0405.v1

Article

The Ultrasonic Jammer

Daniel Hoasov Cohen [1,*], Coral Raz [1,*], Raz Ben Yehuda [1] and Nezer J. Zaidenberg [2]

[1] Department of Electronic Engineering, HIT, Holon
[2] Ariel University Israel
* Correspondence: hoasov@gmail.com (D.H.C.); coral8089@gmail.com (C.R.)

Abstract

Ultrasonic cyberattacks represent an emerging threat vector capable of exfiltrating information even from high-security systems. Modern computing devices equipped with integrated speakers and microphones can generate ultrasonic emissions that may be exploited for covert communication. Previous studies have demonstrated that malicious software can utilize ultrasonic audio channels to establish communication links between otherwise isolated systems, enabling data leakage from air-gapped environments by relaying information through acoustic signals. Experimental results have shown that data can be transmitted at rates of up to 20 bits per second over distances of approximately 18 meters (60 feet), facilitating the covert transfer of sensitive information. Moreover, networks of compromised devices can be chained together to bridge air-gapped systems and transmit data to external receivers. The work presents a real-time system that detects and disrupts covert ultrasonic communication used for hidden data transmission. The authors demonstrate the threat by building an ultrasonic Morse-code channel capable of transmitting data up to 20 meters. To counter this, they develop a mitigation framework using external acoustic hardware that detects ultrasonic signals and jams them with high-power interference. The system effectively prevents data exfiltration, showing strong performance at distances of 5, 10, and 15 meters across different environments.

Keywords: ultrasound; security; communication

1. Background

Ultrasonic communication has been widely studied for short- to medium-distance transmission [1]. Due to the relatively slow propagation speed of sound, ultrasonic signals are particularly effective in enclosed or indoor environments. Their primary applications are found in medicine, chemistry, and electronics. Ultrasonic devices operate by transmitting short sound waves at relatively high frequencies, typically above 20 kHz [5], which are beyond the range of human hearing. In noisy environments, these frequencies remain imperceptible to the human ear. This phenomenon is further influenced by sound masking, whereby louder audible sounds obscure weaker ones, rendering ultrasonic signals undetectable to human listeners.

Ultrasonic communication systems typically consist of a transmitter and a receiver, with data encoded through binary modulation. Despite their utility, these systems present several limitations [15] , including:

- limited transmission range,
- susceptibility to environmental disturbances
- sensitivity to temperature variations
- dependence on air density
- challenges in reliable encoding

Air-gapped networks are a well-established security measure designed to isolate a group of computers from external networks. An air-gapped computer is physically disconnected from the outside world—both wired and wireless [4]. Typically, data transfer into such environments is carried out

 doi:10.20944/preprints202604.0405.v1

manually using portable storage devices such as USB drives. Consequently, adversaries may attempt alternative attack vectors, including the exploitation of sonic devices. Indeed, air-gapped networks have previously been compromised through various methods, including infected USB drives, malicious code injection into OEM partitions [13], and insider threats. Moreover, recent research has demonstrated that ultrasonic transmissions can also be leveraged as a covert channel for data exfiltration.

Air gap research classified throughout the years four ways of communication:

1. Acoustics
2. Electromagnetic
3. Thermal
4. Optics

Acoustic techniques use a transmitter and a receiver. The transmitter has a speaker, and the receiver has a microphone. However, acoustic transmission is not latent from the human ear, which can hear frequencies up to 20 kHz. Therefore, to conceal the transmission, ultrasonic transmission is used. [2] 2013 noticed that a typical speaker and a microphone can produce sound waves up to 24Khz. Thanks to this observation, [2] successfully demonstrated a covert ultrasonic channel. To tackle this, an organization can remove speakers and microphones from the computers in the organization. This sort of security measure is referred to as an audio gap. Another example of a covert acoustic channel is ventilator noise [6]. A malicious program can control the ventilator's acoustic waves, sending them to an adjacent computer up to 8 meters away.

Electromagnetic radiation (EMR) is an energy that propagates through space. In many cases, it propagates from electric devices. [4] showed that it is possible to manipulate electric cables, displays, etc. For example, the software can manipulate a graphic display card to emit AM waves from the video cable by creating specific pixel patterns.

Controlling the heat to move data from two adjacent computers is another **thermal** technique to create a covert channel. Here, the air-gapped computer performs calculations that emit heat for a long time. The peer computer senses the heat changes through its heat sensors.

VisiSploit [14] is an **optic** method to leak information covertly. VisiSploit embeds picture frames undetectable to the human eye.

A sound wave is a disturbance in air density. Sound waves propagate through space, liquids, other gases, and solids. Through mediums such as gas, liquids, and plasma, the waves span in a longitudinal form or are compression waves. The speed of a sound wave is 1230 Kmph, or 343 meters a second. A sound wavelength is the distance between adjacent crests or identical points in the adjacent cycles of a waveform signal. For example, the low threshold of the human ear is 20 hz. Therefore, the wavelength is $343/20 = 17$ meters. The relatively high threshold is 20khz. Therefore, its wavelength is 17mm. A sound wave may act in various ways when it hits a barrier.

A **reflection** is when the sound is returned from the barrier. Reflection usually happens when the barrier is enormous compared to the wavelength or when the barrier is closed from three directions. The angle of return depends on the surface of the barrier it hits. Some of the wave power may propagate through the medium it hits and cause it to vibrate. This vibration is called broadcast. The wave traversing through the matter changes its speed. This change of speed is called **retraction**. A measure of the part of the sound absorbed in the barrier in the matter **absorption coefficient**. A **diffraction** of sound is when the sound passes the barrier. A **scattering** of the sound depends on the surface of the barrier. A toothed surface, a convex surface, a concave surface, or a wavy surface scatters the sound.

A sound **echo** several times in vast spaces. The phenomena of a wave retracted several times is called **reverberation**. A sound **interference** is when sound waves span in the same medium and create a third wave. Whether the interference is **constructive interference** and a **destructive interference** depends on the listener's position and the wavelength. If the two waves are in the phase, i.e. Both peaks are positive, the wavelength of the third wave is double the amplitude. However, the listener can change its position so that the peaks of the waves are 180 degrees opposing, the sum of the two

 doi:10.20944/preprints202604.0405.v1

waves is zero, and the waves cancel each other. This cancellation is called destructive interference or jamming.

As the electromagnetic spectrum becomes denser, researchers look for other technologies. Ultrasonic transmissions become more attractive since they have a thin spectrum, but suffer from disturbances, short distances, and the Dopler effect.

2. Ultrasonic Communication

Ultrasonic waves are shorter than regular sound waves. Therefore, it is subjected to interference; short waves weaken faster than long waves, are more error-prone to the structures of space, and are more sensitive to reflections.

Data over sound (DoS) is an emerging broadcasting technology in the IoT arena. Many devices have speakers. Therefore, DoS does not require special equipment. DoS technology is suitable for payment transactions, device-to-device, human-to-device, etc. Ultrasonic communication offers some advantages:

- Physical Positioning.
- Costs. Smartphones have speakers and microphones. Thus, no new hardware is required.
- Transmission models. Broadcast or unicast.

Morse code is a technique [3] to pass data using sound. Letters are encoded using dots and dashes. The dot signal differs from the dash signal by duration. The dash is three times longer. A silence of three dots separates the letters of each word, and a silence of seven dots separates words. Morse code can also be carried over electric, radio, light, and sound waves. This paper uses Morse code to transfer DoS.

3. Introduction

Most viruses today try to propagate sensitive information through standard network interfaces, such as Ethernet or Bluetooth, so most antivirus software is designed to detect these attacks. However, information leaked via air gap is not detected in the current technology. This paper aims to create an ultrasonic communication protocol as an attack vector and then demonstrate the techniques to detect and disturb it.

This paper describes a system composed of a speaker acting as a transmission device and a receiving microphone. The transmission is Morse-coded, binary-encoded, encoded, and de-modulated on the receiving part. A third device is the transmission detector, which jams the data. Ultratalk [kumarprashant] is software that provides peer-to-peer ultrasonic communication using the speaker of smartphones. Our devices use Ultratalk to communicate.

The jamming strength of our ultrasonic jamming device is a few meters. The jamming device scans the in search of an ultrasonic transmission. Since jamming devices jam the receivers (the microphone) and not the transmitters, a relatively high-power jamming wave must be directed to the speaker.

There are two ways to block a signal:

Spot jamming The full jamming power is focused on a single channel.

Barrage Jamming The jamming power spreads on all channels.

This paper aims to detect the broadcast traffic.

3.1. Jamming

Passing data through a covert channel is done in two ways:

- **Uni Directional**
  A single transmitter with one or more listeners. In this case, the listener never receives a transmis-

 doi:10.20944/preprints202604.0405.v1

sion. Therefore, the listeners require only a microphone, while the transmitters require only a speaker. Unidirectional transmission requires synchronization.

- **MultiDirectional**
  The two machines exchange data. Exchanging data requires both machines to have a speaker and a microphone for bidirectional transmission.

The communication efficiency is subjected to the signal-to-noise ratio (SNR). The following formula describes the SNR:

$$InBandSNR = 10log_{10}\frac{\int_{fc}^{(\frac{fc+1)}{2Tc}} S(f)^2\, df}{\int_{fc}^{(\frac{fc+1)}{2Tc}} N(f)^2\, df} \quad (1)$$

A signal's average frequency is referred to as the signal's spectrum. When S(f) is the clean spectrum signal, N(f) is the noise spectrum, and $\int_{fc}^{(\frac{fc+1)}{2Tc}}$ is the signal frequency integration dimensions.

An energy concentration in time units is the energy spectral density or the spectral power energy - PSD. Figure 1 depicts the PSD of disturbing music. It shows the signal's power spreads over all frequencies while a small amount of energy is over the 18 kHz band. Therefore, a channel over 18Khz is not disturbed by common noise, such as music or human talk. Moreover, in interior spaces, voice propagates from walls and objects, thereby increasing the wave's energy by 95% [8], creating many propagation paths. Knowledge may leak accidentally, for instance, when a person hears by mistake or actively when someone listens by some means. Therefore, in secured environments, it is expected to see sound masking technology [8]. Specifically, when the transmitter and the receiver are not positioned directly, the SNR reduces. The speaker direction determines the amount of the signal consistency.

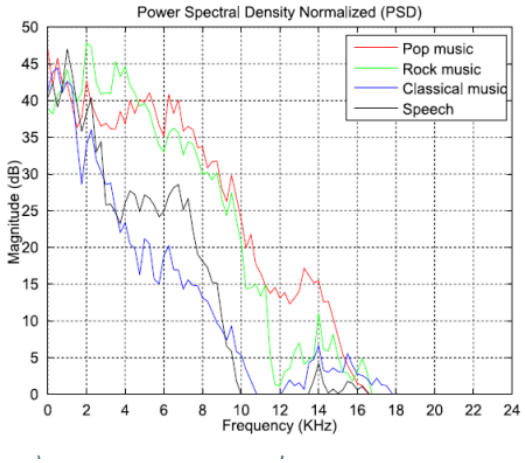

Figure 1. Spectral power density considering the types of interference

There is technology to conceal audio in random sound. This system is already available in some navigation devices. An ultrasonic signal is embedded in the music sound, which provides the speaker's position. However, most available techniques [9,10] spread spectrum, or low-bit programming, require intensive processing, which causes a delay between the hosting signal and the covert signal.

Another everyday use for ultrasonic signals is in smartphones. For example, a protocol called Nearby [11] by GOOGLE. Nearby detects nearby phones by sending a token on an ultrasonic signal. These days, smartphones use Wifi or Bluetooth. However, there are advantages to ultrasonic:

1. **Connection time**
   Creating a connection in Wifi or Bluetooth requires a few seconds. This is not the case in ultrasonic communication, where there is no delay.

 doi:10.20944/preprints202604.0405.v1

2. **Secured premisis**
   Unlike wifi or Bluetooth, relatively high-peak sounds usually do not pass walls. This is useful for creating a single common range of sound.
3. **Disconnections**
   Bluetooth suffers from many abrupt disconnections.

However, the disadvantages of sound are the wide number of propagation channels, echoing, disturbances and hardware limits. Additional disadvantages are in smartphones, where We also include the signal intensity, computation cost and retrieval time.

We now present a different technique to translate data. The Direct Sequence Spread Spectrum (DSSS) is used to reduce signal interference. In DSSS, the data is transmitted in a narrow microphone range. A DSSS signal regulates the data. Each period defines a single character frame, modulated by Multiple Frequency Shift keying (MFSK). DSSS is considered resistant to multiple channels. Compared to FSK (Frequency Shift Keying) or PSK (Phase Shift Keying), DSSS solves the signal arrival time with a much lower resolution than PSK or FSK. [11] (Figure 2) believe that they present the first sound communication implementation when the peers are smartphones.

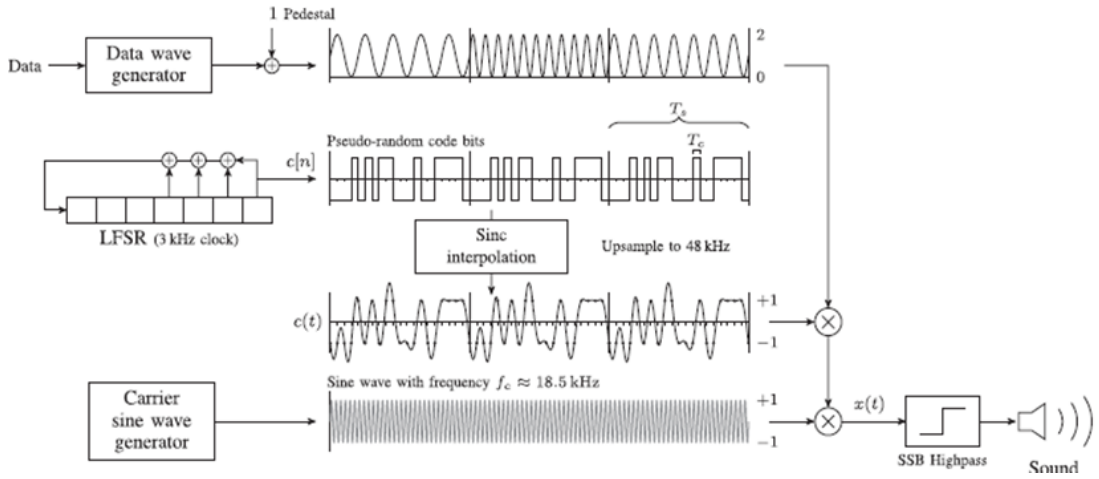

Figure 2. Signal Encoding scheme

Research in ultrasonic communication showed that OOK, BFSK, and BPSK are possible candidates for communication, when the signal carrier is ultrasound. Researchers [11], used 83Kbp/s bandwidth, when a sequence of 200 letters was presented by a time signal of 200 microns. The research showed that all three techniques are good communication candidates when BPSK is the best in BER (Bit Error Rate) and SNR measures. In short distance of 50 mm, showed that BPSK was the best, BFSK came second, and OOK was easily disturbed [12]. In longer distances (few meters), BPSK still proved to be the best choice.

To summarize, research showed that it is possible to perform air-gap communication in 8 meters distance using ultrasound.

Threat Model

In this work, we assume that an attacker has access to the speaker of the attacked computation device and has a computation unit with a microphone capable of receiving the sound from the leaked device within a few meters' radius in a noisy and closed environment. There is no requirement for connectivity other than an ultrasonic signal in a single direction. Also, there is no knowledge of the physical location of any of the two peers.

4. System Description

Our system is shown Figure 3, and the hardware shown in figure 4 comprises three computers. The first laptop is the transmitting device, which is a laptop that emits ultrasonic signals; the second

 doi:10.20944/preprints202604.0405.v1

laptop is the jamming device. The jamming device has an external microphone and an external speaker (Figure 4). It generates sound waves at an intensity greater than that of the transmitting computer, as it is required to jam the signal. The third device is the receiving laptop, which as an external receiver.

Figure 3. System

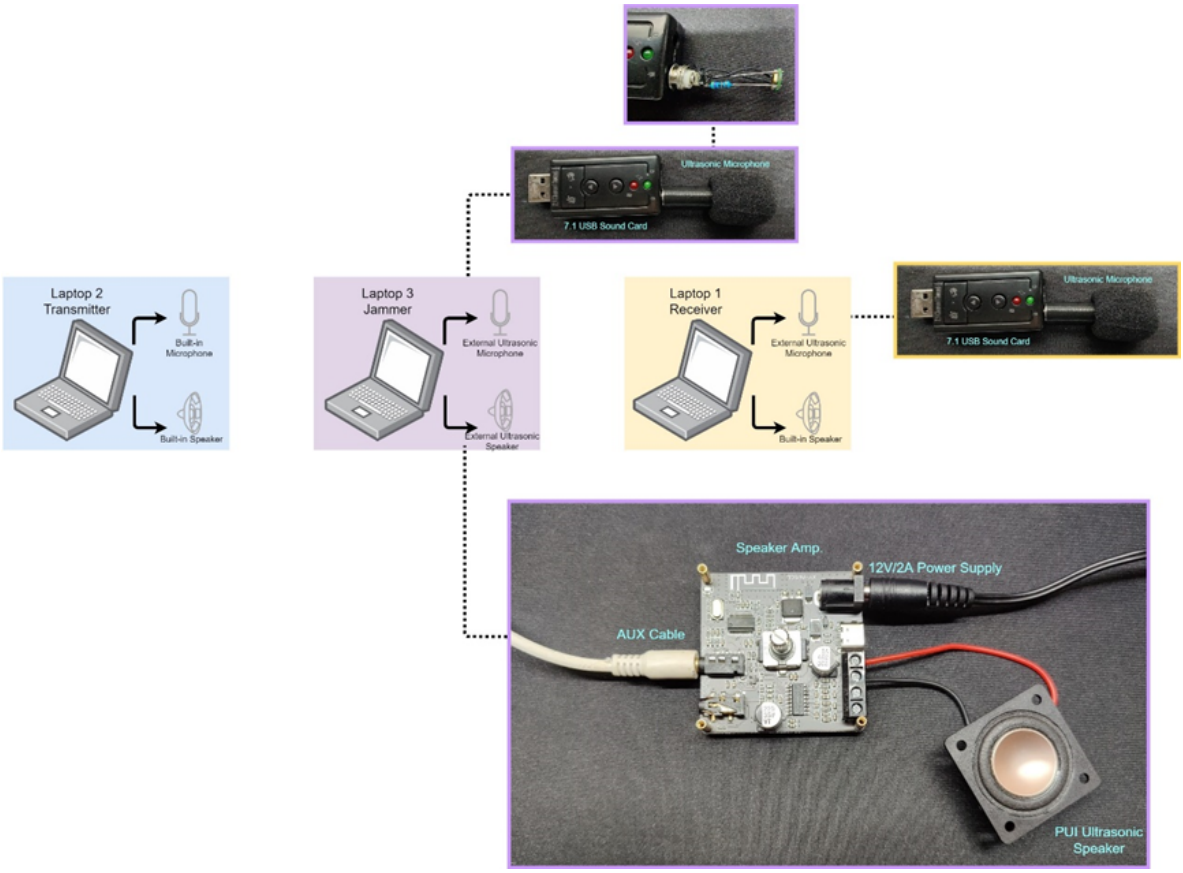

Figure 4. System Hardware

Figure 5 demonstrates the technique in which data are processed. We first convert the data to Morse code. Then, it is converted to WAV format. The WAV is transmitted by playing it and then received by a microphone. The receiving part does exactly thehe opposite. Converts the recorded WAV to Morse, and then converts it back to text. To transmit in relatively high frequencies, i.e. over 20Khz, we were required to use an external periphery for a microphone and a speaker. For a microphone, we used SPU0410LR5H−QB (Figure 6).

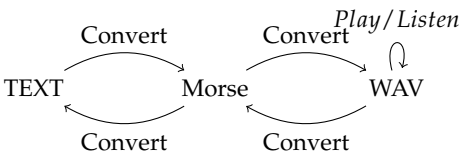

Figure 5. Text to Morse to WAV

 doi:10.20944/preprints202604.0405.v1

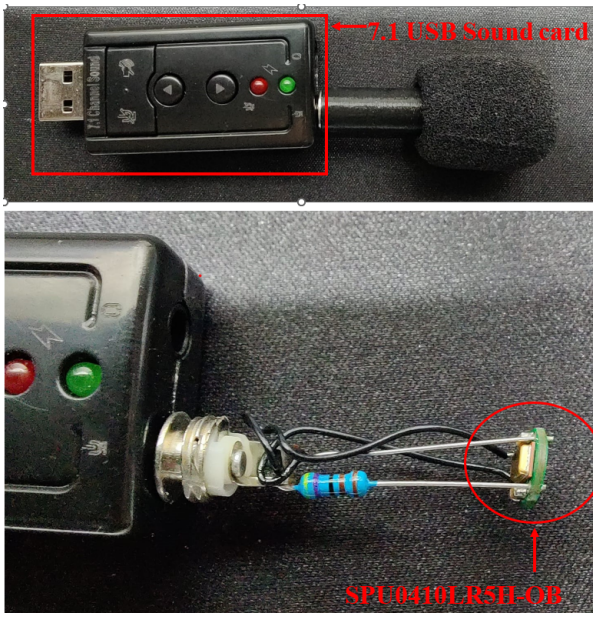

Figure 6. External Microphone acting as a reciever

We chose SPU0410LR5H−QB because it keeps relatively high sensitivity in a wide receiving spectrum, from 10kHz to 80kHz, as depicted Figure 7. This miniature device two 3.5mm separate sockets, a speaker and a reciver, and it features the following:

- A wide frequencies range, 10kHz - 80KHz
- A low noise ratio
- A flat frequency response (the difference between the signal enters a device in from out it comes out)
- A low current consumption
- Stable measures of ultrasonic frequencies

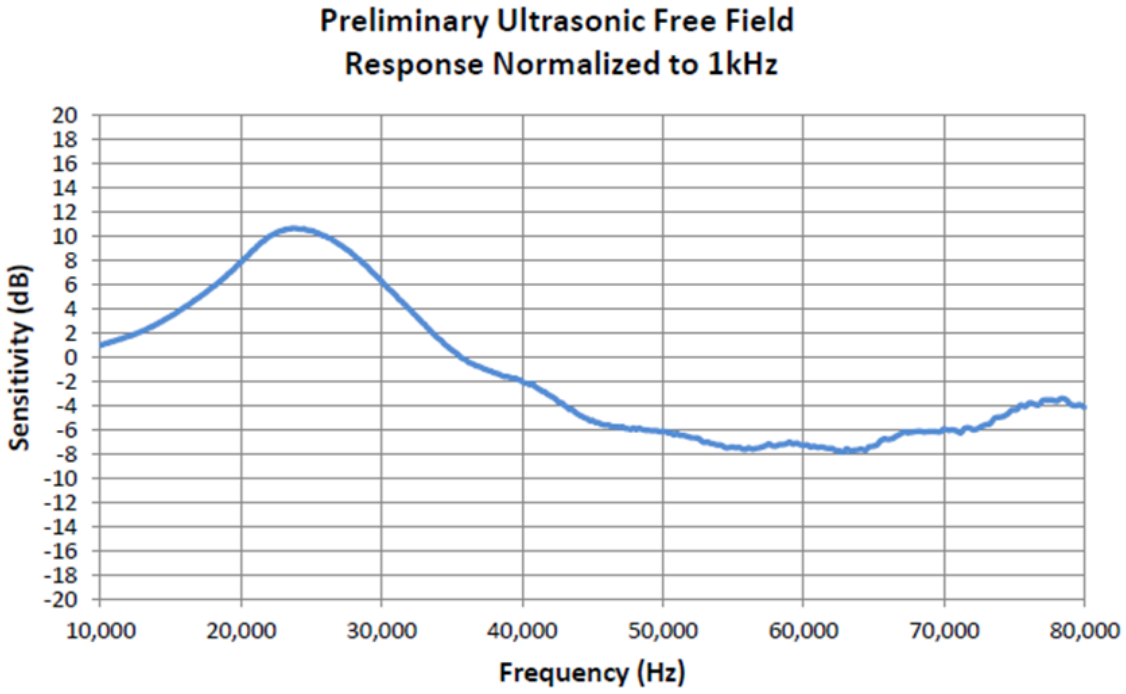

Figure 7. Sensitivity as a function of frequency

 doi:10.20944/preprints202604.0405.v1

In addition, the device's form factor is 3.76 cm in length, 3.00 cm in width, and 1.1 cm in height. Also, additional modifications (Figure 8 and Table 1) were required to the microphone to better its efficiency.

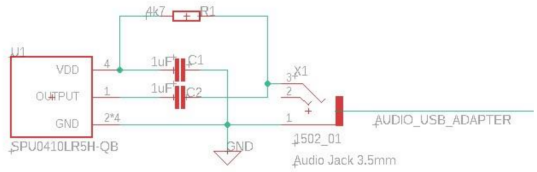

Figure 8. Voltage Supply: Mic modifications

Table 1. Microhopne adaption

Pin	Pin Name	Type	Description
1	GND	Signal	Output signal connected to 1uF (C2)
2	GND	Power	Ground
3	GND	Power	Ground
4	VDD	Power	Power supply, connected to 4uF (R1) and 1uF (C1)
5	GND	Power	Ground
6	GND	Power	Ground

We added a 3.5mm plug to connect it to the periphery (Figure 9), and packed it in a 3d model that We printed.

Figure 9. 3.5 Plug

4.1. Amplifier Specifications

The amplifier (Figure 10) is made up of three components:

1. USB sound card
2. - SPU0410LR5H
3. XY-AP50L Amplifier

We already discussed the sound card and the SPU0410LR5H. The amplifier is used to amplify the ultrasound signals that the scrambler emits. The component of the TPA3116D2 amplifier, developed by Texas Instruments, enables the amplification of ultrasonic signals in a range of up to 22 kHz. It is mounted on the XY-AP50L board, which includes all the necessary peripherals for efficient amplifier operation. We connected the amplifier via an AUX cable to a 7.1 USB sound card and supplied it with 12 V/2 A power through an external adapter.

 doi:10.20944/preprints202604.0405.v1

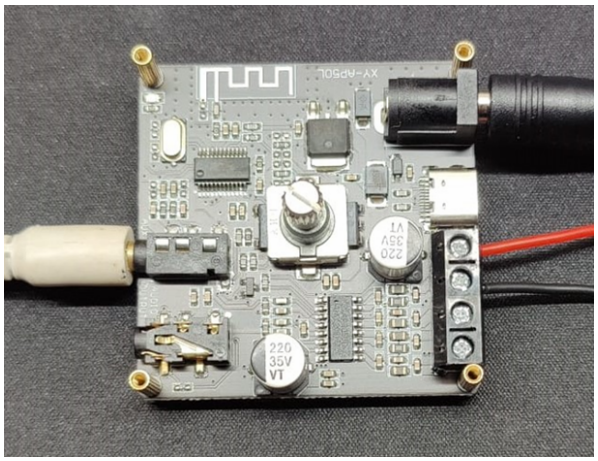

Figure 10. Amplifier

The speaker Figure 11 did not require any special modifications. It operates in the ultrasonic frequency range and has the following characteristics:

1. Wide frequency range: 150 Hz – 40 kHz
2. High sensitivity threshold: 78 dB
3. Convenient connectivity, compatible with the amplifier.

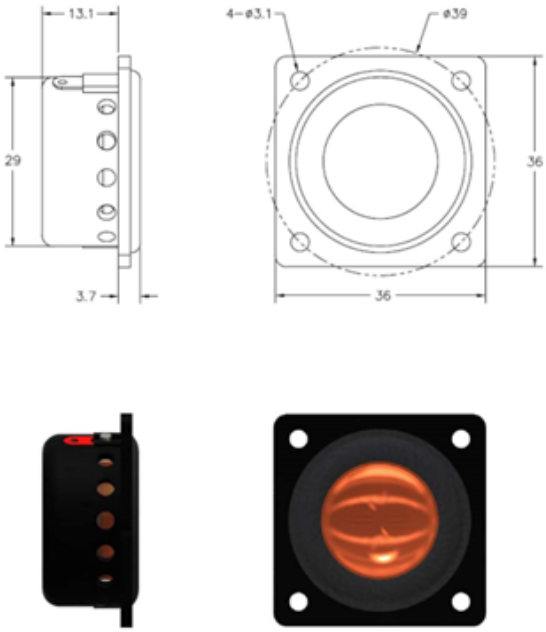

Figure 11. PUI Speaker AS03608AS

The TPA3116D2 component allows amplification up to 22kHz, and the PUI AS03608AS-R (Figure 11) was used due to its high sensitivity threshold and support for frequencies up to 40kHz.

5. Architecture

The ultrasonic communication system developed in this project enables data transmission between end devices using relatively high-frequency sound waves. The system consists of three main components:

- Transmitter – generates an ultrasonic signal containing encoded data.
- Receiver – records and processes the incoming ultrasonic signal.
- Jammer – detects ultrasonic communication and disrupts it in real time.

 doi:10.20944/preprints202604.0405.v1

The communication protocol converts textual information into Morse code, which is then modulated into ultrasonic frequencies and transmitted through the air. The system architecture includes the following stages:

1. Text input
2. Conversion to Morse code
3. Signal generation
4. Ultrasonic transmission
5. Audio capture
6. Signal processing and decoding

Each stage is implemented using MATLAB signal processing tools.

5.1. Signal Encoding

Text to Morse Code

The input message is first converted into Morse code symbols. Morse code represents characters using two symbols:

- Dot
- Dash

Each character is encoded as a sequence of dots and dashes according to the Morse coding standard. Example:

$$A = \cdot -$$

$$B = - \cdots$$

This encoding allows textual information to be represented as a sequence of short and long pulses.

Binary Representation

For digital transmission, the Morse symbols are mapped to binary signals:

- Dot $\rightarrow$ short ultrasonic pulse
- Dash $\rightarrow$ long ultrasonic pulse
- Space $\rightarrow$ silence

This representation allows the signal to be processed using digital signal processing methods.

5.2. Signal Generation

The Morse sequence is converted into an audio waveform at ultrasonic frequencies. Let the transmitted signal be defined as:

$$s(t) = A \sin(2\pi f_c t)$$

Where:

- A – signal amplitude
- f_c – carrier frequency (typically around 20 kHz)
- t – time

The frequency f_c is chosen above the human hearing threshold ($f > 20kHz$) to ensure that the communication remains inaudible.

5.3. Signal Transmission

The generated waveform is written into a WAV file and played through a speaker.

```
[y, Fs] = audioread('sound.wav');
```

Where:

- y – sampled audio signal

 doi:10.20944/preprints202604.0405.v1

- F_s – sampling frequency

  The sampling frequency used in the system is:

$$F_s = 48000\ Hz$$

  This ensures sufficient resolution for ultrasonic signals.

5.4. Signal Reception

The receiver captures the transmitted signal using a microphone. The captured audio is stored as a time-domain signal and then analyzed using spectral analysis techniques.

5.5. Spectrogram Analysis

To analyze the ultrasonic signal over time, a spectrogram is used. The spectrogram represents the signal power as a function of both time and frequency. The Short-Time Fourier Transform (STFT) is applied to compute the spectrogram:

$$STFT\{x(t)\} = X(t, f)$$

where:

- $x(t)$ – input signal
- $X(t, f)$ – time-frequency representation

In MATLAB, the spectrogram is computed as:

```
[S,F,T,P] = spectrogram(signal,window,
noverlap,nfft,Fs,'yaxis');
```

Where:

- S – complex STFT matrix
- F – frequency vector
- T – time vector
- P – power spectral density (PSD)

5.6. Window Function

A Hamming window is applied to reduce spectral leakage.

$$w(n) = 0.54 - 0.46\cos\left(\frac{2\pi n}{N-1}\right)$$

Where:

$$N = 512$$

5.7. Power Representation

The power spectrum is converted to decibels using:

$$P_{dB} = 10\log_{10}(P)$$

This representation makes it easier to visualize signal energy within the spectrogram.

5.8. Signal Detection

To detect ultrasonic transmissions, the system searches for maximum power values within the spectrogram matrix.

```
[Max,indexM] = max(P);
```

 doi:10.20944/preprints202604.0405.v1

Where:

- Max – maximum power value detected
- indexM – frequency index where the maximum occurs

The detected peaks correspond to the transmitted ultrasonic pulses.

5.9. Jamming Mechanism

Once an ultrasonic signal is detected, the jammer generates interfering signals in the same frequency band.

The interference introduces destructive interference that prevents the receiver from correctly decoding the signal.

The jamming signal can be represented as:

$$j(t) = A_j \sin(2\pi f_j t)$$

Where:

- A_j – jamming amplitude
- f_j – jamming frequency

If the jamming frequency overlaps the communication frequency band, the signal-to-noise ratio decreases significantly and communication becomes unreliable.

5.10. Summary

The proposed system demonstrates an ultrasonic communication protocol capable of transmitting encoded information between devices using audio hardware. The main contributions include:

- Morse-based ultrasonic communication protocol
- Real-time ultrasonic signal detection
- Spectrogram-based signal analysis
- Jamming mechanism to disrupt covert ultrasonic channels

This system provides a potential defensive mechanism against covert ultrasonic cyber-attacks.

6. Experiment

Our experimental evaluation is divided into two phases. The first phase focuses on transmission performance under controlled disturbances, including masking effects, varying propagation distances, and different reception angles.

The second phase evaluates the jammer under comparable distance conditions, considering multiple separations between the transmitter and receiver. Additionally, the jammer was assessed when positioned outside the classroom at a distance of 5 m, as well as under varying transmission angles.

phase 1

We start by transmitting the word "test" in lab conditions (. Figures 12. We conducted an experiment with nosie. as can be seen in Figure 13, this experiment was successful. Unlike the laboratory conditions, at lower frequencies the effect of environmental noise can be observed; however, it did not interfere with the reception of the ultrasonic signal.

 doi:10.20944/preprints202604.0405.v1

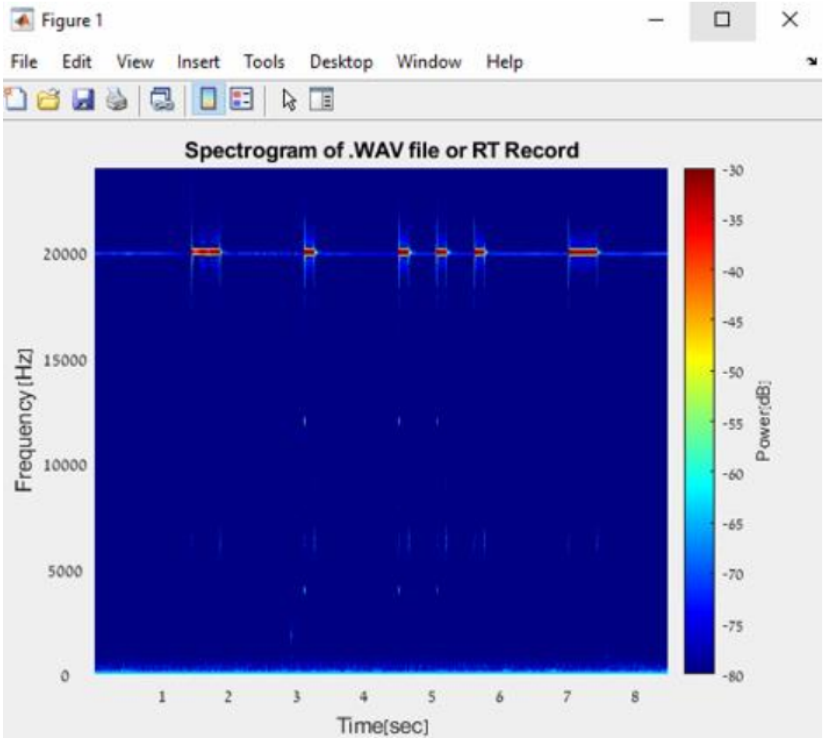

Figure 12. Lab Conditions

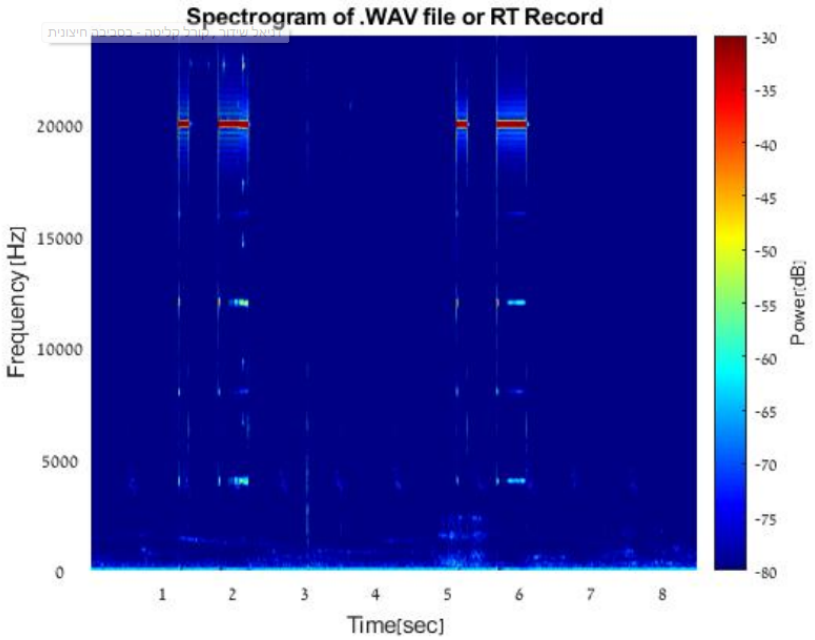

Figure 13. Noise Conditions

Figures 14, 15 and 16 illustrate that signal power decreases as distance increases. Additionally, it can be observed that the signal power gradually attenuates as the distance increases; however, signal reception is still possible at distances of approximately 20 meters. It should be noted that as the distance increases, so does the probability of errors in decoding the received word or sentence.

 doi:10.20944/preprints202604.0405.v1

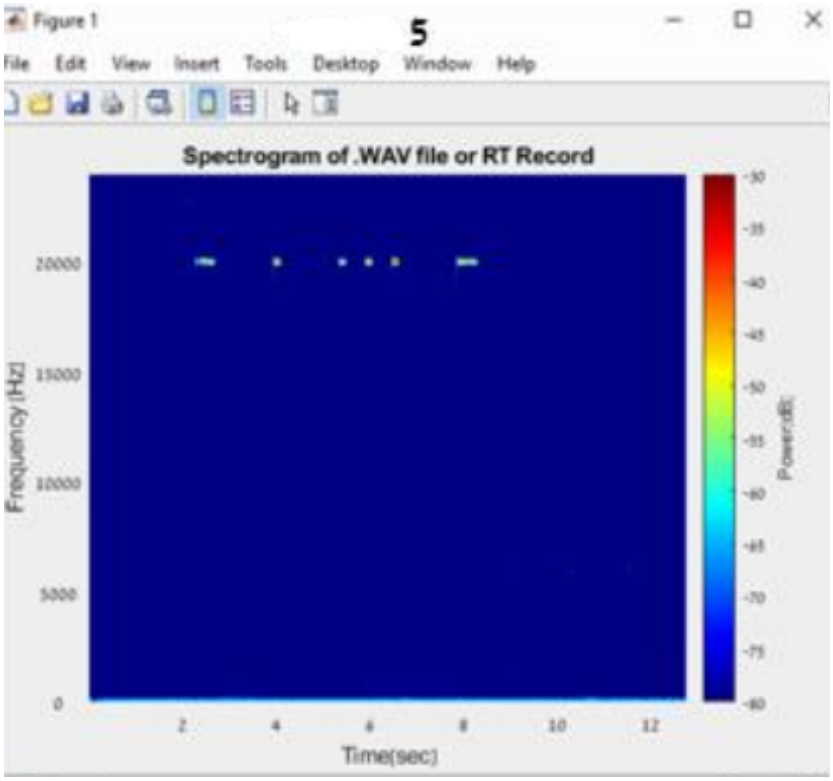

Figure 14. Spectogram 5 meters

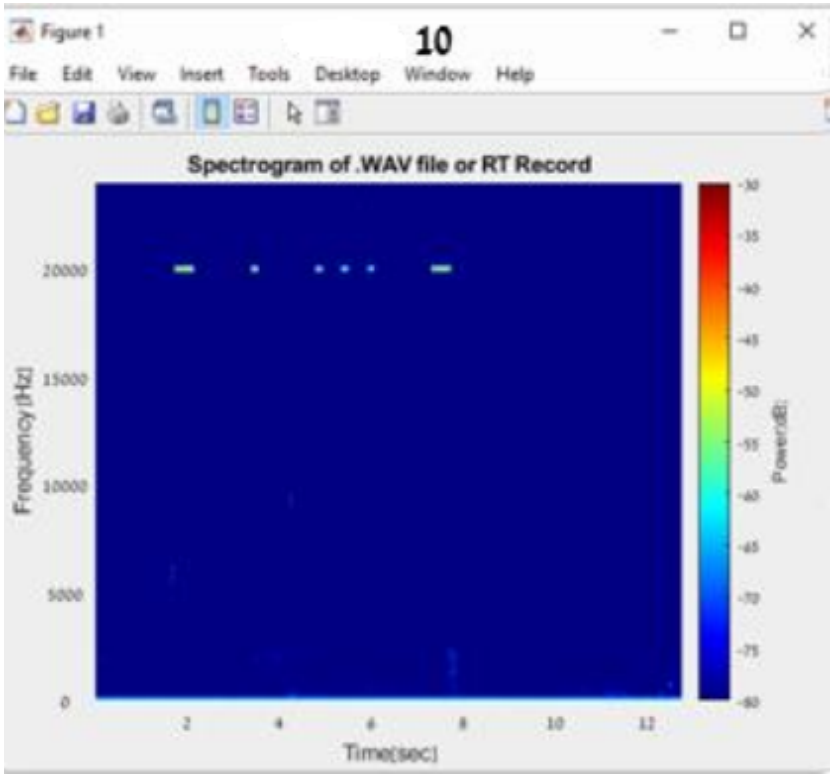

Figure 15. Spectogram 10 meters

 doi:10.20944/preprints202604.0405.v1

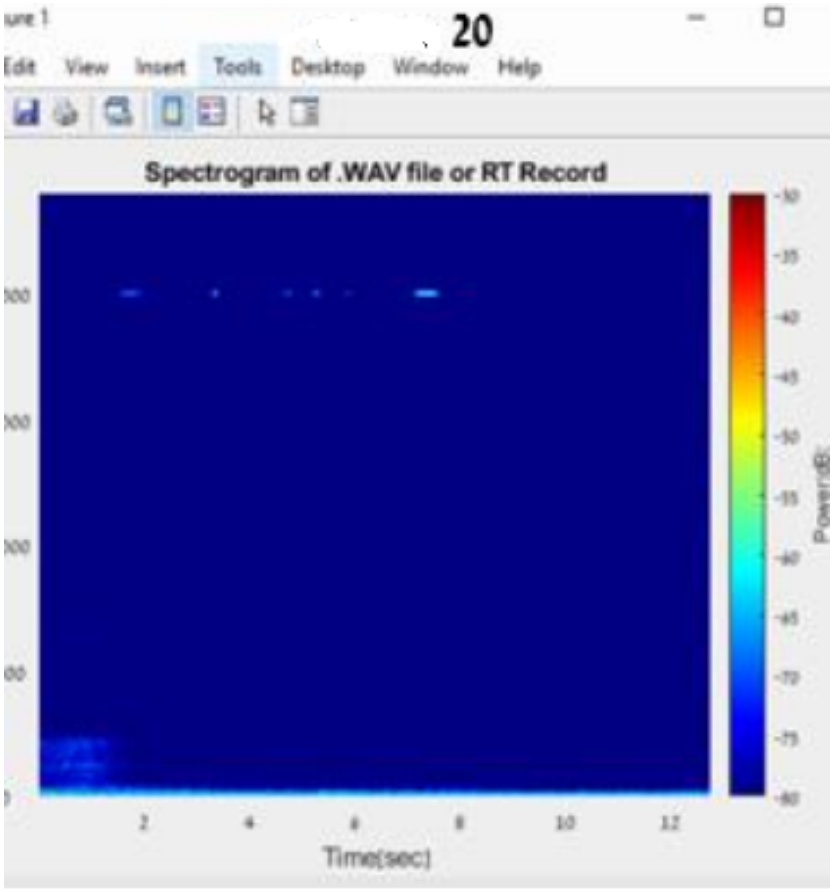

Figure 16. Spectogram 20 meters

Figure 17 reflect how music disturbs an ultrasonic wave. As can be observed, the ultrasonic signal was successfully received at a frequency of 20 kHz with relatively high power, as expected. However, interference is present across the entire frequency range of the spectrogram due to background music played in close proximity (0 m) to the receiver. In addition, reflections of the transmitted signal appear at lower frequencies as a result of the short transmission distance.

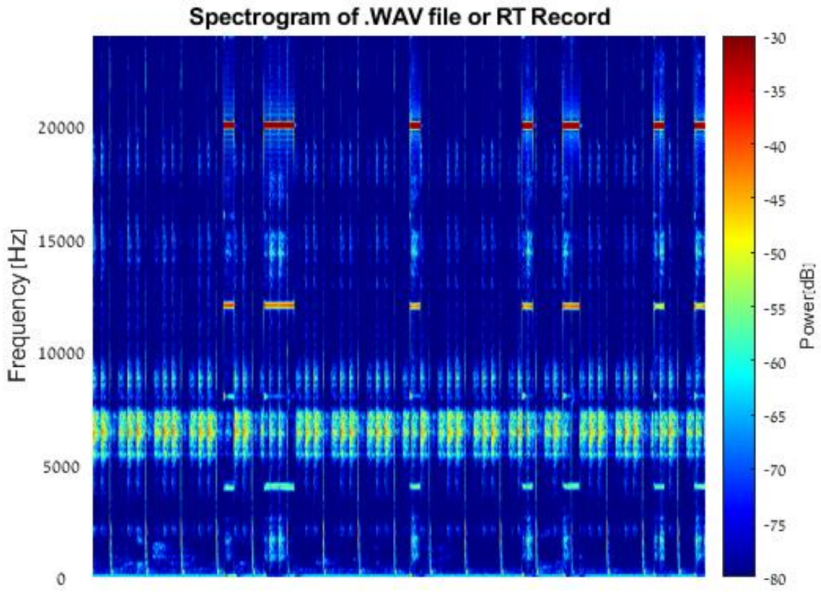

Figure 17. Music distrubance

 doi:10.20944/preprints202604.0405.v1

Figure 18 reflect how voice disturbs an ultrasonic wave. In this experiment, the transmitted signal was received at the receiver at a distance of 0 m. Unlike music, due to the non-monotonic nature of the audio sequence and the variability in frequency content of the sound waves, the resulting spectrogram appears irregular and random. Naturally, this behavior varies between different audio segments and depends on the intensity of the speech. Similar to the previous experiment, reflections of the transmitted signal appear at lower frequencies due to the short transmission distance.

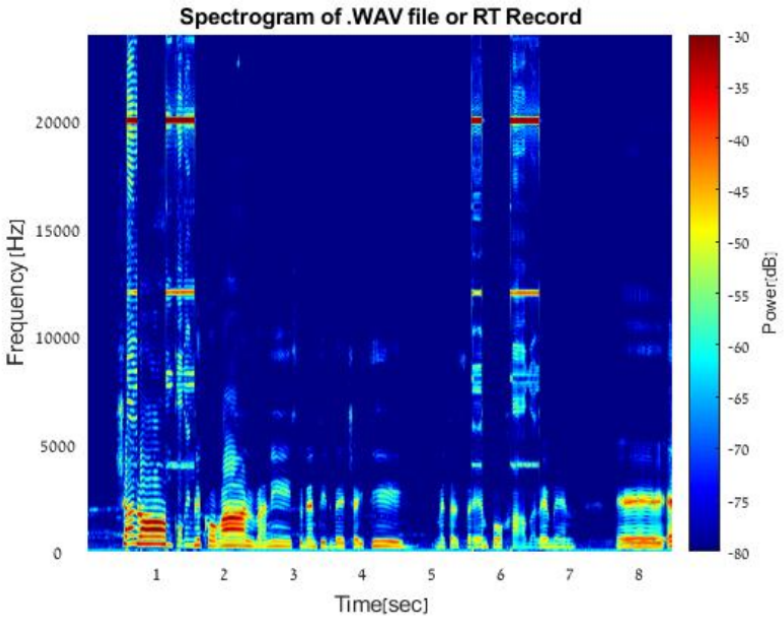

Figure 18. Music distrubance

Figure 19 represents a meeting-like scenario in which multiple participants are speaking, while the transmission is evaluated at extreme angles of 0° and 180°.

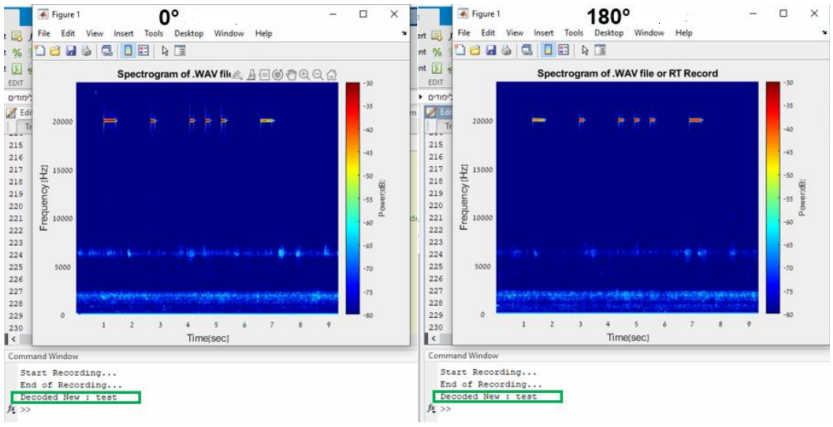

Figure 19. Spectogram many people

As can be observed, the experiment was successfully conducted. The transmitted word "test" was received and fully decoded without distortion or interference from background noise or the defined transmission distance. In addition, the received signal power is relatively relatively high, ranging between approximately $[-45 : -35]$ dB. It can also be seen that lower frequencies capture ambient noise present in the environment, while the reception angles do not significantly affect the received signals.

Additional tests were conducted to evaluate the effect of the human body on transmission efficiency. We observed that when a person was positioned at a distance of 0 meters Figure 20 from the

 doi:10.20944/preprints202604.0405.v1

receiver, and only part of the transmitted word was successfully received ("tes"). When the distance was increased to 0.5 meters Figure 21, the transmission still failed.

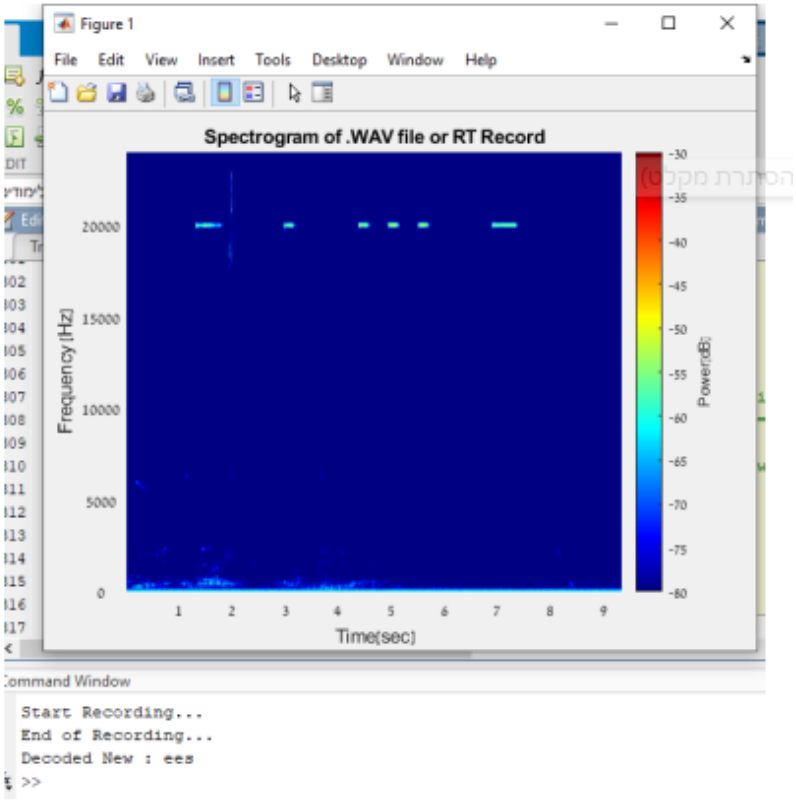

Figure 20. human 0 meter distance from receiver

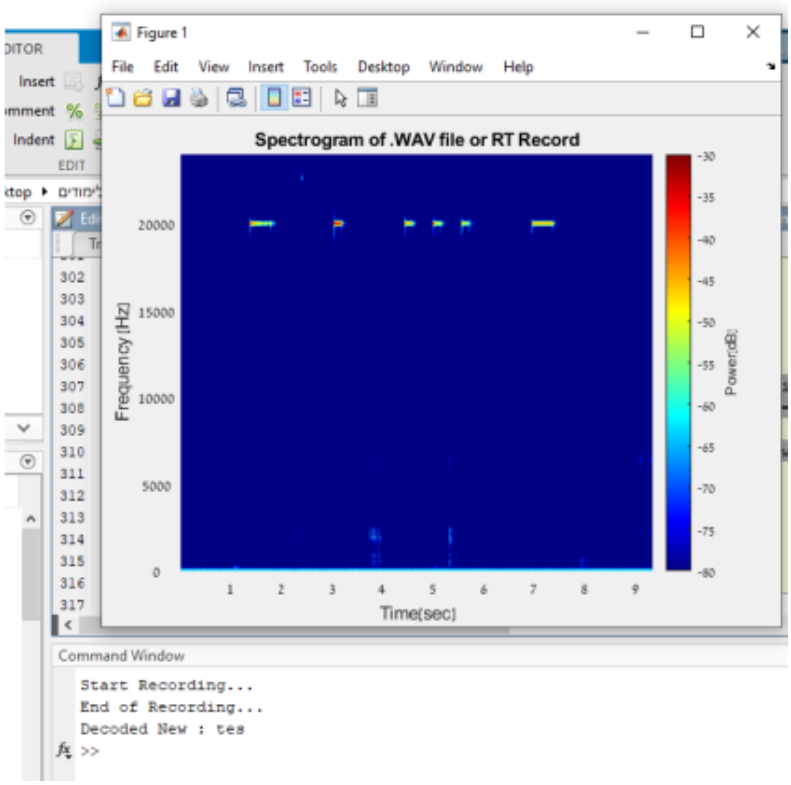

Figure 21. human 0.5 meter distance from receiver

 doi:10.20944/preprints202604.0405.v1

Other objects, such as wooden doors, also interfered with the transmission. However, reducing the detection threshold (i.e., increasing sensitivity) enabled successful reception. In contrast, metallic or glass objects completely blocked the transmission.

Transmission and Reception at Different Beam Angles:

The objective of This experiment was to evaluate the received signal power and decoding performance under different reception angles relative to the transmitter. The experiment was conducted in an enclosed environment, with a transmission distance of approximately 5 meters. The reception angles were varied between 0 and 180 degrees. Figure 22 presents the received signal power as a function of the angles. From Figure 22, the variation in the received signal power as a function of the reception angle can be observed. The maximum received power was obtained at reception angles of 20 and 80 , while the minimum power was observed at angles of 10 and 120. The maximum power difference between the received signals is approximately 11.8875 dB and does not affect the decoding of the received signal under the default parameters defined in the implementation.

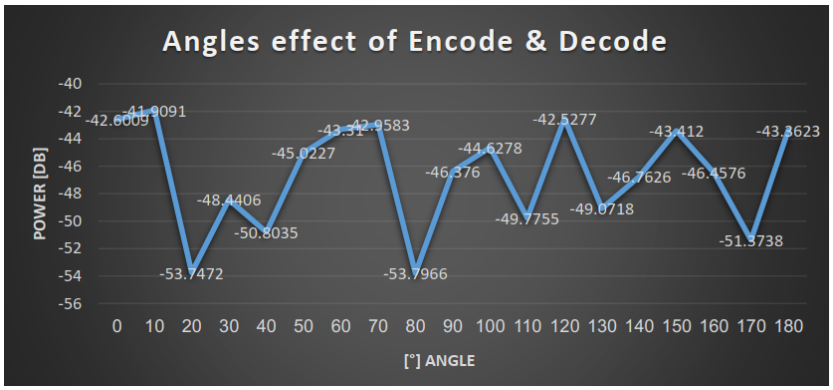

Figure 22. Angles effects of Encode and Decode

Jamming

Following the ultrasonic transmission experiment between a transmitter and a receiver, We developed a jammer as a third end device to disrupt the transmitted signal. The jammer detects ultrasonic transmissions and, upon detection, emits a relatively high-power ultrasonic signal in a predefined sequence of pulses. This effectively disrupts the communication between end devices A and B.

The experiment was divided into several main stages:

- **Stage 1:** Evaluation of transmission at distances of 5 m, 10 m, and 15 m, with the jammer positioned at the center of the communication path.
- **Stage 2:** Transmission and reception outside the classroom, while the jammer remained inside the classroom at a distance of approximately 5 meters.
- **Stage 3:** Evaluation of transmission and reception at different beam angles relative to the jammer.

Stage 1: Transmission Evaluation

at Different Distances (5 m, 10 m, and 15 m) with the Jammer Positioned at the Center of the Communication Path. The objective of This experiment was to evaluate the performance of the jammer at different transmission and reception distances, and to determine whether distance constitutes a limitation for effective signal disruption. It should be noted that the experiment was conducted in a closed classroom environment.

Figure 23 depicts the difference in decoding performance between the two experiments can be clearly observed. On the left—when the jammer is active—the transmitted word "test" is not correctly decoded, indicating successful disruption of the transmission. In contrast, on the right—without the jammer—the transmitted word is correctly decoded as expected.

 doi:10.20944/preprints202604.0405.v1

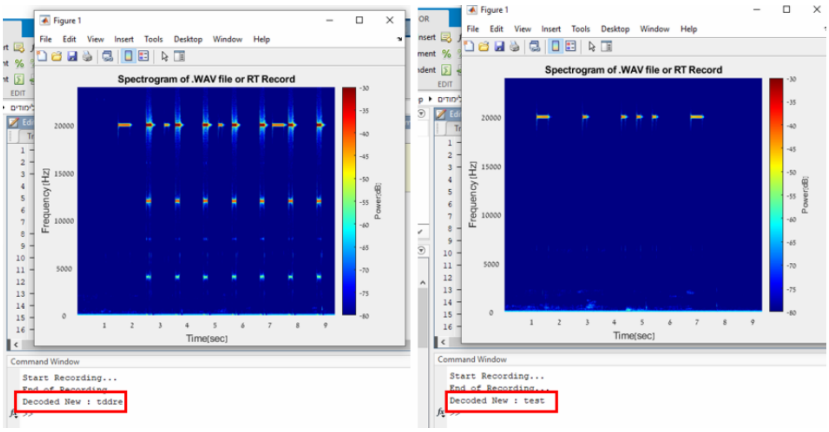

Figure 23. Spectrograms: left with a jammer, right without

Stage 2 – Transmission and Reception Outside the Test Classroom

In this phase, transmission and reception were performed outside the test classroom (Figure 24), while the jammer was located inside the classroom at a distance of 5–7 m. The objective of this experiment was to evaluate the jammer's performance when it is not positioned along the main communication path.

Experimental Conditions

1. The classroom door was open.
2. The transmission–reception distance between the two end devices was approximately 2 m.
3. The jammer was positioned at a distance of 5–7 m from the end devices and, unlike in the previous experiment, was not located along the direct communication path.

Test Configurations

1. Classroom door open
2. Classroom door closed

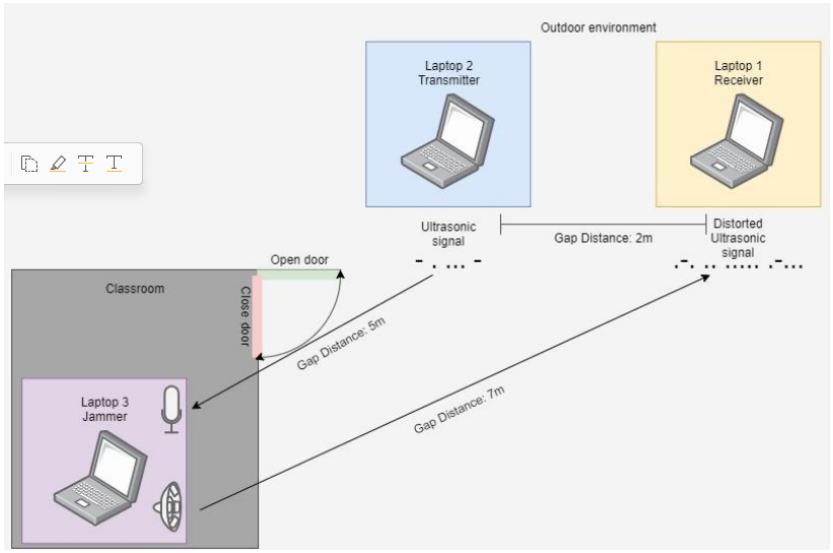

Figure 24. jammer outside the room

Figure 25 shows the spectrogram for the case where the door is open. It can be observed that the signal was successfully jammed, and the transmitted word "test" is not detected. Although the jammer effectively disrupts the transmitted signal, the spectrogram indicates that signal components are still present at relatively high power levels (approximately −40 dB to −30 dB). Following this experiment, the same conditions were repeated with the classroom door closed (Figure 26). In this configuration,

 doi:10.20944/preprints202604.0405.v1

the jammer remained inside the classroom, while the transmission between endpoint A and endpoint B was conducted outside the classroom.

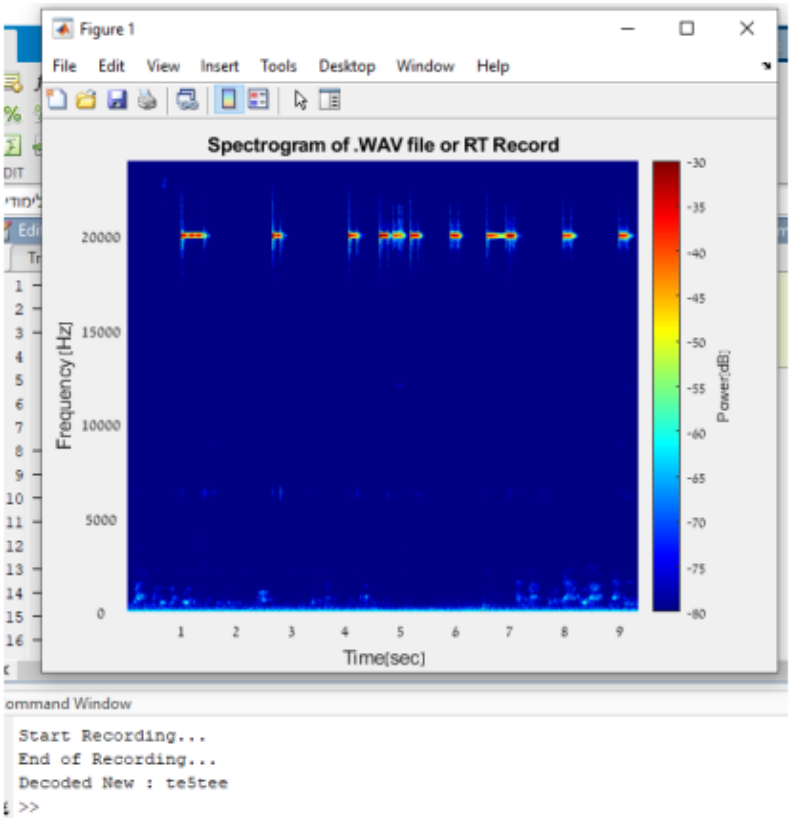

Figure 25. jammer with the door open

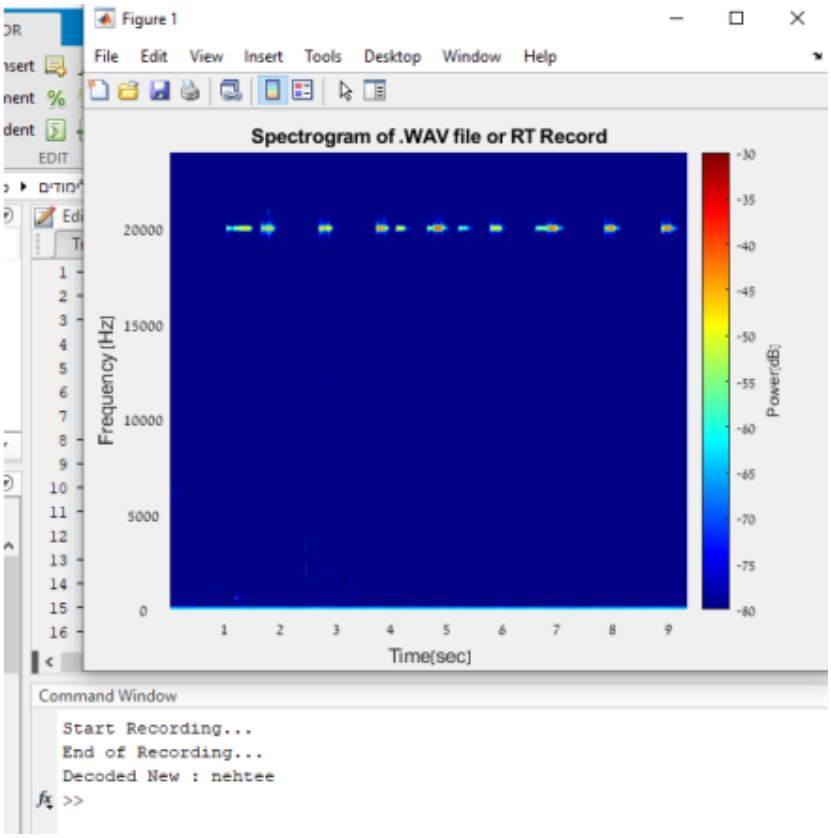

Figure 26. jammer with the door shut

 doi:10.20944/preprints202604.0405.v1

Stage 3: Transmission and Reception vs. Beam Angle (Jammer)

The objective of this experiment was to evaluate the decoding of received signals at the receiver under varying reception angles relative to the transmitter. The transmitter was positioned at a fixed distance of approximately 2.5 m from the jammer throughout the experiment. The variation in angles was achieved by repositioning the receiver, with angles of 0°, 45°, and 90° relative to the jammer. The distance between the jammer and the receiver was approximately 2.5 m. Figure 27 depicts the experiment. Variations in the reception angles did not affect the jammer's performance, which successfully disrupted the transmitted signal throughout the entire experiment. Therefore, the experiment was considered successful.

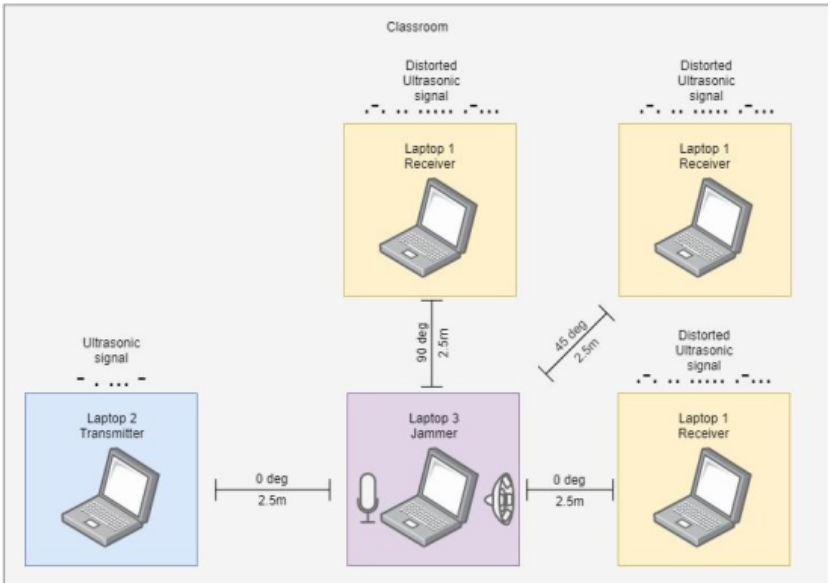

Figure 27. Scheme Experiment

7. Conclusions

We have successfully implemented the experiment of leaking information. We examined the medium of communication (ultrasonic) between edge equipment. We examined the transfer of communication between two laptops as well as one end of which was used a development board and transmitter on one end and computer on the other. The main conclusions and highlights from the first experimental section are detailed below:

- It is possible to receive a transmission of ultrasonic signals at a distance of about 20 meters. Of course, as the distance increases, so does the probability of an error in the decoding aspect, and this is about the loudspeaker of end B, which is used as a transmitter.
- The main masks that disrupt the ultrasonic transmission are physical masking (at a distance of 0 meters), a metal door, an elevator, a thin layer of aluminium and masking of a glass wall.
- The barriers that can be overcome with the help of an algorithm change are physical distance (A distance greater than 0 meters) and a thick wooden door.

In addition, we examined the effect of reception angles on data transmission at a distance of 5 meters. From the setup and the experimental conditions we used, it can be concluded that there is no effect on the transmission of the broadcast.

In the second experiment, we added a jammer to the experimental setup. The purpose of the jammer is to disrupt the ultrasonic communication transmitted between the two end devices and to test the effectiveness of the jammer in several different situations, such as:

- Changing transmission and reception distances (the jammer is in the center of communication traffic). The experiment met our expectations, while the distance was not a factor in the operation of the jammer.

 doi:10.20944/preprints202604.0405.v1

- A transmission and reception experiment at a distance of about 5 meters from the jammer. Here, too, the jammer was transmitted with high power and strength and succeeded in disrupting the ultrasonic transmission between the end devices.

Similar to the first experimental section, in this section, different reception angles did not constitute an obstacle to the operation of the jammer, which disrupted the ultrasonic transmission.

There are several main factors to secure information regarding ultrasonic signals and communications. First, the size of the building, the material from which the building is made and constructed, the number of windows, the ventilation openings, the types of doors, and the like may significantly influence the success or failure of the attacker/hostile party in stealing the desired information using this method. Therefore, our experiment was based on more than just the laboratory classroom area. Still, we tried to examine various areas and buildings in the institute to draw efficient and optimal conclusions from the experiments performed.

In conclusion, ultrasonic transmission can be a security breach for various security institutions and organizations, but as we have proven, correct use of the jamming operation can prevent and deter hacking and attacks by parties hostile.

8. Further Research

With the advancement of technology and its entry into all aspects of modern life, the world has become dynamic and complex regarding cyber attacks and information theft. Some of these technological advances have driven a significant shift in the issue of cyber-attacks and the planting of viruses and various offensives in classified and isolated networks from the Internet. Also, there has been an awakening and tremendous technological progress in information security in security and sensitive institutions and organizations. Over the past decades, tremendous progress has pushed the limits and importance of information security. Dedicated devices and software have been developed to safeguard sensitive and classified information on computers and networks. As part of an in-depth study carried out on the subject, these are sensitive points that can be suggestions for further research:

- Conducting research on ultrasonic transmission and reception through various communication and electrical channels (for example, PVC channels, metal channels, power lines and any wall passages used for other purposes).
- Research ultrasonic transmission in ventilation openings (central air conditioners, etc.).
- The effect of ultrasonic transmission in buildings with different raw materials (glass, metal, plaster, etc.).

As part of conducting the research and the lessons learned from the experiment, several recommendations can be listed that can be implemented when conducting experiments in this field:

- It is required to check the hardware restrictions on portable computers, whether the built-in speakers and microphones support the transmission of frequencies in the high range - and, if necessary, to limit and refine the use in sensitive areas.
- Using headphones to transmit ultrasonic communication is required to prohibit leaving headphones and audio equipment permanently connected to computers at a high classification level.
- Implementation of jammers in security institutions and organizations - which detect and disrupt ultrasonic transmission upon detection.
- Installation of metal doors and glass walls in rooms and buildings and attention to acoustic sealing of the room during compassionate discussions/meetings.

The dangers that arise in this area are not the top priority, and this is because of the many challenges, risks and obstacles in the electromagnetic medium. Of course, with the technological development and the misguided dangers in this progress, it is necessary to continue researching, developing and protecting the information transmitted in the air.

 doi:10.20944/preprints202604.0405.v1

References

1. Stojanovic, Milica and Beaujean, Pierre-Philippe J. (2016). *Acoustic communication*. Springer Handbook of Ocean Engineering.
2. Byres, Eric. (2013). *The air gap: SCADA's enduring security myth*. Communications of the ACM.
3. Lee, Chin-Tan and Wu, Chia-Chun and Su, Bo-Rui and Shen, Tung-Chun. (2016). *A novel electronic lock using ultrasound Morse code based on FIR filter*. 2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE).
4. Guri, Mordechai and Elovici, Yuval. (2018). *Bridgeware: The air-gap malware*. Communications of the ACM.
5. Szent-Gy (1933). Chemical and Biological Effects of Ultra-Sonic Radiation. Nature.
6. Mirsky, Yisroel and Guri, Mordechai and Elovici, Yuval. (2017). *Hvacker: Bridging the air-gap by attacking the air conditioning system*. arXiv preprint arXiv:1703.10454.

kumarprashant. Kumar, Ravi Ranjan and Rai, Manish. (). *PRASHANT KUMAR SINGH ANURAG ANAND NIKITA KHANDARE*. .

8. Ballou, Glen. (2013). *Handbook for sound engineers*. .
9. Kirovski, Darko and Malvar, Henrique S. (2003). *Spread-spectrum watermarking of audio signals*. IEEE transactions on signal processing.
10. Bassia, Paraskevi and Pitas, Ioannis and Nikolaidis, Nikos. (2001). *Robust audio watermarking in the time domain*. IEEE Transactions on multimedia.
11. Getreuer, Pascal and Gnegy, Chet and Lyon, Richard F and Saurous, Rif A. (2017). *Ultrasonic communication using consumer hardware*. IEEE Transactions on Multimedia.
12. Li, Chuan and Hutchins, David A and Green, Roger J. (2008). *Short-range ultrasonic digital communications in air*. IEEE transactions on ultrasonics, ferroelectrics, and frequency control.
13. Nissim, Nir and Yahalom, Ran and Elovici, Yuval. (2017). *USB-based attacks*. Computers and Security.
14. Guri, Mordechai and Hasson, Ofer and Kedma, Gabi and Elovici, Yuval. (2016). *VisiSploit: An optical covert-channel to leak data through an air-gap*. arXiv preprint arXiv:1607.03946.
15. Krautkr(2013). *Ultrasonic testing of materials*. .