Rev. Roum. Sci. Techn.– Électrotechn. et Énerg.
Vol. **67**, 4*x*, pp. 479–482, Bucarest, 2022

ANALYSIS OF THE UNINTENDED PROPAGATION OF AUDIO SIGNAL EMITTED BY WIRELESS HEADPHONES

ALEXANDRU MADALIN VIZITIU[1,3], BOGDAN CATALIN TRIP[1,3], VLAD FLORIAN BUTNARIU[1,3], VALENTIN VELICU[2,3], LIDIA DOBRESCU[1], SIMONA HALUNGA[1]

Keywords: Audio signal; Electromagnetic compatibility; Wireless headphones; Transient electromagnetic pulse emanation standard (TEMPEST).

The information technology and communications (IT&C) market for audio devices has increased in supply and demand in recent years. Wi-Fi, Bluetooth, or DECT technologies involve connectivity that contains an encryption protocol scheme that assures resistance to third-party interception. However, when discussing a secured transmission, we must look at the communication link. The audio end devices generate unintended emissions, which may contain information that can be eavesdropped on, a phenomenon that researchers in the specialty literature have studied. This paper aims to emphasize the wireless headphones' vulnerability by analyzing their emission security breaches at several distances. Using specialized transient electromagnetic pulse emanation standard (TEMPEST) equipment, the vulnerability of two different headphone models is highlighted by successfully reconstructing pieces of information corresponding to three audio test patterns.

1. INTRODUCTION

The technology development, the variety, and the IT&C product's affordable prices continuously increase electronic device usage, including wireless headphones. Many devices are known to generate unintended emanations, leading to unwanted signals that can be reconstructed, a process referred to as eavesdropping. The unwanted signal is called compromising emanation (CE) because, if intercepted and analyzed, it would disclose the information transmitted and processed by the device. The literature presents a continuous concern of scientists regarding the study of different CE corresponding to the video signal from displays [1], the keyboard's keystroke signal [2], and the audio signal. The audio signal unintended propagation was studied only for wired devices [3,4] and in the proximity of audio end devices [5]. Therefore, studying the phenomena on wireless audio devices at a considerable distance can represent a new challenge.

Communication is a key element to succeed in most of our daily activities. Due to people's necessity to communicate at a distance while doing something else, such as working, jogging, handling goods, or driving, wireless headphones are a helpful instrument [6,7]. They substitute the wired headphones that hinder the user's mobility due to the cable and the implied necessity to have the source device nearby. The communication process involves 2 terminals: a host that initiates it, known as master, and a device that responds to the host when asked, known as slave.

There are two wireless communication standards used for headphones: Bluetooth [8] and Digital European Cordless Telecommunications [9] (DECT). The first one implies a direct connection between the master device and slave devices, a 1÷3 Mbps data rate, and ranges between 10 m and 100 m. DECT technology uses an intermediary device – a base station that must be used between the master device and the slave device. The data rate is lower than Bluetooth, with 32 kbps, 100 m range, but this standard is dedicated to audio communications. Network services engineers admit that Bluetooth technology uses 128-bit encryption, and DECT uses 64-bit encryption, eliminating the chance of eavesdropping. However, even though the communication standard is safe, a transmission is secure when the probability of a third party intercepting it is null from end to end. Therefore, this paper aims to present that the problem of intercepting the confidential message before encoding must be analyzed from the end-devices perspective, which applies to wireless headphones. No matter the applied standard to ensure connectivity, headphones should be analyzed to verify whether they generate unintended CE that can compromise the entire communication.

TEMPEST (transient electromagnetic pulse emanation standard) refers to investigations on electronic devices to ensure their protection against eavesdropping. National Security Agency (NSA) – the USA published the domain fundamentals in 1982, but Willem van Eck first emphasized the activity in 1950. According to the TEMPEST standard, devices are classified into three protection categories based on the CE levels. Moreover, to establish within TEMPEST how those devices are used with minimal vulnerability to be eavesdropping, the zoning activity must be considered – measuring the attenuation of rooms and buildings where devices are often used.

This article demonstrates a wireless headphones' vulnerability that an eventual interceptor can exploit. Studied devices under test (DUT) use Bluetooth standards to ensure connectivity between master and slave devices. The communication between them is secured by encryption schemes, as previously presented. It can be noticed that even though DUTs passed electromagnetic compatibility (EMC) requirements, unintended harmonics emitted by the headphones could represent the carrier wave for the audio signal which is transmitted to them. This unintended signal can be received using specialized receiving equipment.

During our measurements, the distance between antennas and DUT varies from 1 m to 3 m. The fact that the CE is present at those measurement distances should increase the users' awareness while headphones are widespread in today's IT&C market [10,11].

2. MEASUREMENT AND EQUIPMENT

The measurements were performed in a full anechoic room, with the DUT disposed on a table and connected to a laptop, as presented in Fig. 1. The master device was tested before to ensure the lack of influence during the measurements. The SAS-545 biconical antenna that is

[1] University Politehnica of Bucharest, Faculty of Electronics, Telecommunications and Information Technology, Bucharest, Romania
E-mail: vizitiuamadalin@gmail.com, {lidia.dobrescu, simona.halunga}@upb.ro, {bogdan.trip, vlad.butnariu}@stsnet.ro
[2] University Politehnica of Bucharest, Faculty of Electrical Engineering, Bucharest, Romania, Email: valentin.velicu91@gmail.com
[3] The Special Telecommunications Service, Bucharest, Romania

adequate to the measured emissions' frequency range was placed at different distances from DUT to determine the maximum distance at which the signal is received with an acceptable signal-to-noise ratio (SNR) higher than 3 dB. At the receiving point, a Rohde & Schwarz (R&S) FSWT Tempest Receiver was used to receive the signals emitted by the DUT, and an R&S MSO5204b oscilloscope displayed the receiver's intermediary frequency output to facilitate the CE detection and its analysis in the time domain.

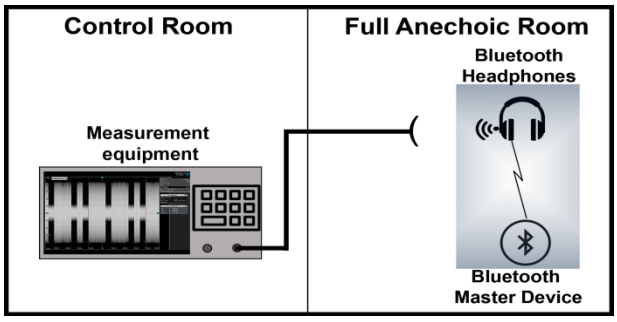


Fig. 1 – Measurements testbed.

To facilitate the CE illustration in the received signals, three different test signals were used. The frequency range for the tones that compose the test signals covers the narrowband frequency range considered in telephony: 300 Hz – 3400 kHz. The first test signal, presented in Fig. 2,a, consists of 3 sinus tones, corresponding to 2.3 kHz, 1.7 kHz, and 1.1 kHz, with the duration of 50 ms, 150 ms, and 150 ms and a silent 50 ms signal between tones.

The second test signal, presented in Fig. 2,b, is made up of 2 tones that correspond to 1.7 kHz and 900 Hz sinus signals. A 50 ms silent signal follows the first tone with a duration of 100 ms, and following them is the second tone with a duration of 150 ms. The test signal ended with a 100 ms silent part. During the measurement, the test signals play in a loop and are switched to validate the CE presence on the current frequency.

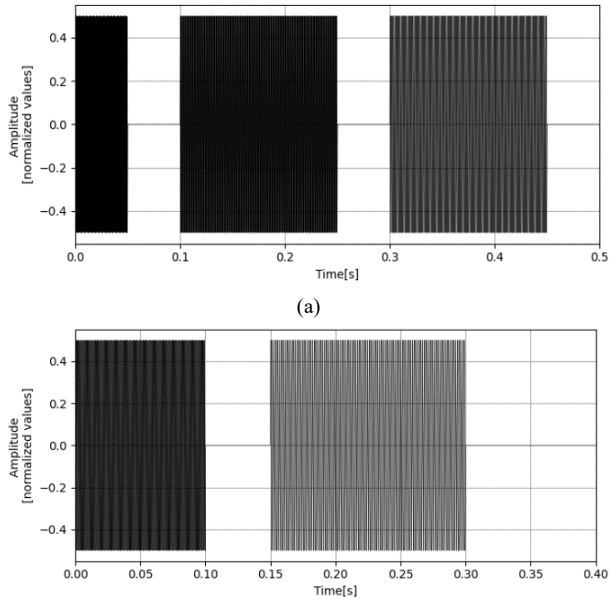


Fig. 2 – Test signals: a) first test signal (500 ms); b) second test signal (400 ms)

The phenomenon of generating unwanted CE during its normal functioning is present in different headphone types. This paper shows its presence on 2 different wireless headphone types of different brands. The first studied device is an overhead wireless headphone, and the second is an in-ear wireless headphone.

3. MEASUREMENT EXPERIMENT AND RESULTS

3.1. WORK PROCESS DESCRIPTION

To perform the measurement, a workflow must be followed by the test engineers. The flowchart presented in Fig. 3 describes the steps of the work process.

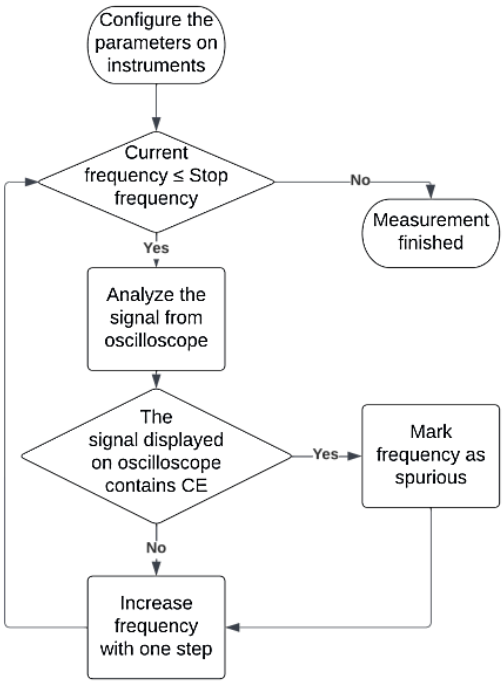


Fig. 3 – The work process flowchart.

The measurement begins by aligning the antenna with the headphones and setting the detection parameters on the receiver and oscilloscope. Starting from the first frequency in the analyzed band, the test engineers will check on the oscilloscope's display of the CE presence. In the case of spotting any similarities between the waveform displayed on the oscilloscope and the test signals highlighted in Fig. 2, they mark the current frequency as spurious. The process continues by increasing the receiver's frequency value. The measurement is finished when the current frequency equals the last frequency in the analyzed range.

3.2. RESULTS AND ANALYSIS

According to the measurements, unintended CE was found on both tested devices. Using a near-field probe, it is noted that the CE levels are higher around the headphones' microcontrollers and the speakers. The audio CE also is present along the wires between the headphones' controller and speakers. Still, the levels do not allow an illustration of the phenomenon due to the SNR drawbacks. During the measurements, the receiver's reference level does not change. Hence the signal level displayed on the oscilloscope is affected only by the distance between the antenna and the studied device.

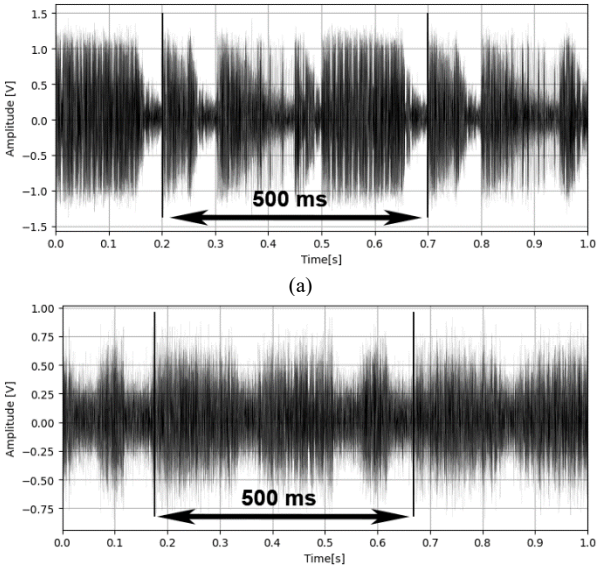
For the first DUT, the CE was found in the frequency range of 20 MHz ÷ 180 MHz. The representative frequencies are listed in Table 1.

Table 1

Frequency ranges where the CE is present for first DUT

Frequency ranges [MHz]		
22.49 ÷ 22.51	43.11 ÷ 43.14	117.20 ÷ 117.22
27.24 ÷ 27.28	44.12 ÷ 44.15	119.43 ÷ 119.45
28.81 ÷ 28.84	80.22 ÷ 80.25	185.04 ÷ 185.07
35.52 ÷ 35.55	82.13 ÷ 82.16	186.03 ÷ 186.06
37.08 ÷ 38.62	110.12 ÷ 110.15	187.58 ÷ 187.69

In the case of the first device, the audio test tones could be intelligibly recovered at distances up to 2 m. In Fig. 4, the signal captured from the oscilloscope for the first test signal is presented. The measurements illustrated in the figure were performed with the spectrum receiver tuned on the 44.14 MHz frequency.

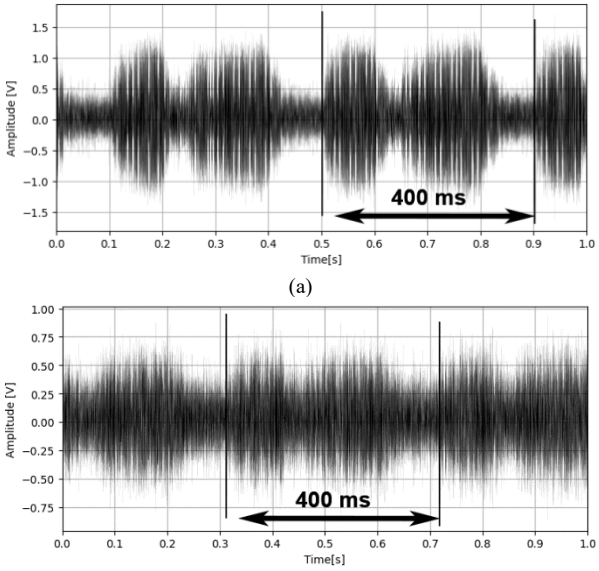


(a)

(b)

Fig. 4 – Second DUT (first test signal used) – received signal at distance of: a) 1 m; b) 3 m; frequency 115.992 MHz.

Due to the low SNR value, the 3 tones of the first test signal are sometimes difficult to be differentiated from the noise. It should be noted that noise is not so present once we move away from the DUT, and the signal is much easier to identify. For those headphones, it has been noted that the second test signal, consisting of only two tones, is easier to be detected on the oscilloscope's display (Fig. 5).



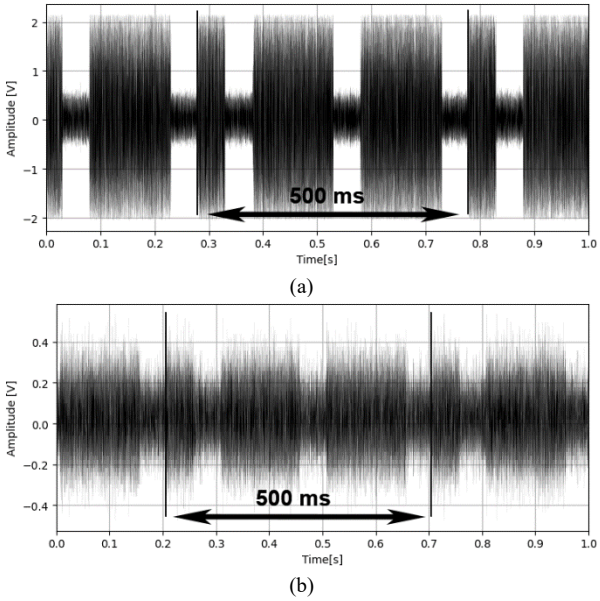
(a)

(b)

Fig. 5 – Second DUT (first test signal used) – received signal at distance of: a) 1 m; b) 3 m; frequency 115.992 MHz.

It should be noted that the SNR makes the CE hard to detect for higher distances.

The in-ear wireless headphones generate audio-compromising emanations only in a narrow frequency range: 115.975 MHz ÷ 116.025 MHz. Despite this, the SNR is more significant than in the previous device's case, and the CE is present up to 3 m from the DUT. The presented results are made with the spectrum receiver tuned on the 115.992 MHz central frequency. The results presented in Fig. 6 correspond to the captured waveform from the oscilloscope for the first test signal with a 500 ms length at 1 m and 3 m distances.

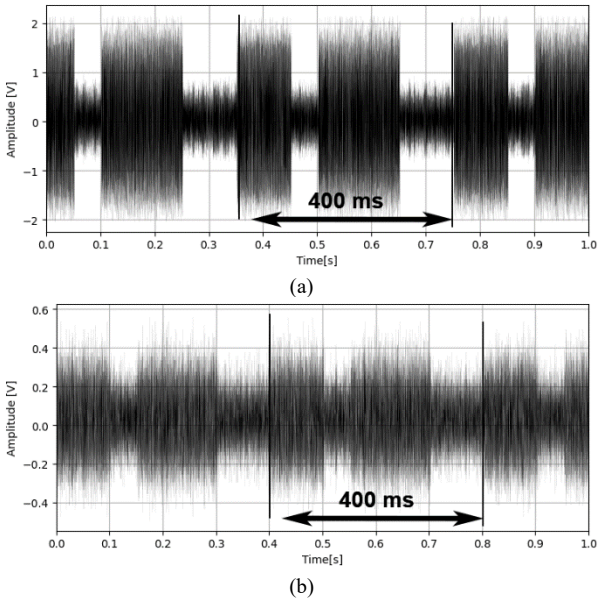


(a)

(b)

Fig. 6 – Second DUT (first test signal used) – received signal at distance of: a) 1 m; b) 3 m; frequency 115.992 MHz.

The results for the second studied DUT using the second test signal are presented in Fig. 7.



(a)

(b)

Fig. 7 – Second DUT (first test signal used) – received signal at distance of: a) 1 m; b) 3 m; frequency 115.992 MHz.

For the studied in-ear wireless headphones, we observed that both test signals are easily detected, and the captured waveforms from the oscilloscope for the 1 m distance (Figs. 6a, 7a) are like the test tones waveforms.

To further emphasize the wireless headphones' vulnerabilities, a third test signal was used. It corresponds

to a recorded waveform of a male voice saying a generic message: "Hello, John Smith" (Fig. 8), and it has a duration of 1.4 s. This sequence's simplicity will conduct easy CE detection. Given its content, it will likely be an ongoing phone call or a voice message. Hence, using one of the devices presented in this article, based on the previous measurements, the conversation could be compromised.

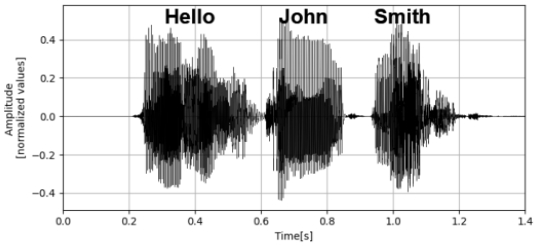


Fig. 8 – Test signal corresponding to a voice message saying "Hello, John Smith".

The third set of measurements was taken for both studied DUTs ensuring a 1 m distance between the antenna and headphones. The test signal was played in a loop during the measurements, as expected from the previous situations. For the overhead headphones, measurements were performed with the receiver tuned on the 44.14 MHz frequency, and in the case of the second analyzed device, the chosen frequency was 115.992 MHz. This also demonstrates the detecting audio CE technique's reliability using multi-tone patterns as test signals, although some harmonics belong to the vocal spectrum.

The captured waveforms from the oscilloscope (Fig. 9) contain 3 times the test signal, and the voice message's duration is highlighted. The first image corresponds to the overhead wireless headphones, and the second is for the in-ear ones.

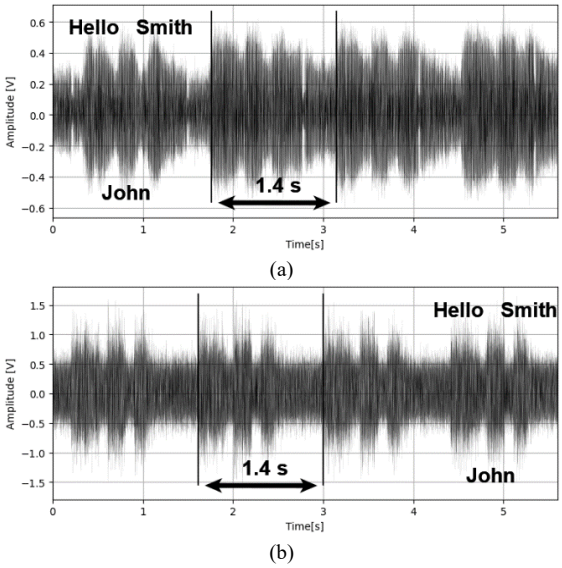


Fig. 9 – Captured waveform that contain CE corresponding to voice signal test signal: a) overhead headphones; b) in-ear headphones

As with the other two test messages, in-ear headphones leak in a more "accurate" manner the unintended audio CE, whilst for the first studied DUT, the test signal is harder to be detected due to the presence of high amplitude noise.

4. **CONCLUSIONS**

The unintended propagation of the audio CE phenomenon is present in the case of wireless headphones. This article depicts the audio CE presence in the 1 to 3 m from wireless headphones that use Bluetooth standards for connectivity. The study of audio CE represents a continuous concern for scientists. Up to this point, publications on this topic cover the subject of wired headphones and focus on the magnetic field of the audio end device, successfully revealing the presence of audio CE at distances up to 60 cm.

The connectivity standard to transmit the audio signal from master to slave devices should be further encrypted. This paper aims to increase the importance for end devices to pass both EMC and TEMPEST requirements, and to raise a degree of awareness among users, highlighting the fact that the connectivity protocol's encryption is not sufficient to secure the communication, as the end devices themselves may be vulnerable because of their unintended radiation pattern.

To illustrate that this phenomenon could occur for wireless headphones categories, the measurements could be performed utilizing wireless headphones with DECT standard to ensure the connectivity between master and slave devices.

The study on the compromising audio emanations could have a further direction focusing on new methods to facilitate the identification of this security breach.

Received on 19 September 2022

REFERENCES

1. P. De Meulemeester, B. Scheers A.E. Vandenbosch, *A quantitative approach to eavesdrop video display systems exploiting multiple electromagnetic leakage channels*, IEEE Transactions on Electromagnetic Compatibility, pp. 1-10 (2020).
2. R.I. Sokolov, R.R. Abdullin, D.A. Dolmatov, *Development of synchronization system for signal reception and recovery from USB-keyboard compromising emanations*, 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp. 1-4 (2016).
3. J. Choi, H.-Y. Yang, D.H. Cho, *TEMPEST comeback: a realistic audio eavesdropping threat on mixed-signal SoCs*, Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), Association for Computing Machinery, pp. 1085–1101, New York, USA (2020).
4. B. Trip, V. Butnariu, V. Velicu, S. Halunga, A. Boitan, *Analysis of the compromising audio signal from the emission security perspective*, 13th International Conference on Communications (COMM), pp. 363-366 Bucharest (2020).
5. Q. Liao, Y. Huang, Y. Zhong, H. Jin, K. Wu, *MagEar: eavesdropping via audio recovery using magnetic side channel*, Proceedings of the 20th Annual International Conference on Mobile Systems, Applications, and Services, pp. 371-383, Portland, USA (2022).
6. M. Nicolaescu, V. Croitoru, L. Tuță, *Radiation of a slot in a high-speed digital system*, Revue Roumaine des Sciences Techniques - Série Électrotechnique et Énergétique, **67**, *3*, pp.363-330 Bucharest (2020)
7. ***The state of play report 2019: A global look at the key drivers of consumer audio use cases,* Qualcomm Technologies, San Diego, USA (2019).
8. ***Advanced Audio Distribution Profile, Revision v.1.4* Bluetooth SIG (2022).
9. *Digital Enhanced Cordless Telecommunications (DECT); Advanced Audio Profile v1.1.1*, European Telecommunications Standards Institute (ETSI), France (2022).
10. I.C. Mustață, L. Bacali, M. Bucur, R.M. Ciureanu, A. Ioanid, A. Ștefan, *The evolution of industry 4.0 and its potential impact on industrial engineering and management education*, Revue Roumaine des Sciences Techniques - Série Électrotechnique et Énergétique, **67**, *1*, pp.73-78 Bucharest (2022)
11. ***Wireless Headphones Market - Global Industry Size, Share, Growth, Opportunity and Forecast, 2018-2028, Segmented by Product Type (In-Ear, Over-Ear Headphones, Others), Distribution Channel (Online, Offline), Application (Music & Entertainment, Gaming, Virtual Reality, Fitness, Others), Region (North America, Europe, Asia Pacific, Latin America, Middle East & Africa),* BlueWave Consulting, India (2022).