International Journal of Wireless Information Networks (2020) 27:45–59
https://doi.org/10.1007/s10776-019-00473-4

Acoustic-Based Security: A Key Enabling Technology for Wireless Sensor Networks

S. Soderi[1]

Received: 31 January 2019 / Revised: 9 October 2019 / Accepted: 28 October 2019 / Published online: 13 November 2019

Abstract
Technological advances have proliferated in several sectors by developing additional capabilities in the field of systems engineering. These improvements enabled the deployment of new and smart products. Today, wireless body area networks (WBAN) are commonly used to collect humans' information, hence this evolution exposes wireless systems to new security threats. Recently, the interest by cyber-criminals in this information has increased. Many of these wireless devices are equipped with passive speakers and microphones that may be used to exchange data with each other. This paper describes the application of the watermark-based blind physical layer security (WBPLSec) to acoustic communications as unconventional wireless link. Since wireless sensors have a limited computation power the WBPLSec is a valuable physical layer standalone solution to save energy. Actually, this protocol does not need any additional radio frequency (RF) connection. Indeed, it combines watermarking and a jamming techniques over sound-waves to create secure region around the legitimate receiver. Due to their nature, wireless communications might experience eavesdropping attacks. The analysis proposed in this paper, addresses countermeasures against confidentiality attacks on short-range wireless communications. The experiments over the acoustic air-gap channel showed that WBPLSec can create a region two meters wide in which wireless nodes are able to communicate securely. Therefore, the results favor the use of this scheme as a key enabling technology to protect the confidentiality in wireless sensor networks.

Keywords Acoustic · Physical layer security · Watermarking · Ultrasonic · Jamming · Air-gap · Covert channel · WBAN · Secrecy capacity · IoT

1 Introduction

Nowadays, security companies report a massive amount of new security breaches every week. Names, email addresses, passwords, banking data and medical records are just few examples of the information stolen by hackers. Sometimes, the institution or company affected by security issues of this kind must notify their clients\customers to advise them to change their password or credit card number. Unfortunately, most of these incidents are not easily detectable, and furthermore, it is difficult to keep one's information perfectly safe, and practically impossible to avoid sharing data with the likes of governments, health insurers etc., and even at one's workplace. It is also true that many of these incidents do not even involve hackers. For instance, data might even be subjected to the wrong configuration by an IT server. Another aspect that makes this situation even worse is related to the timing of hackers and how they use the stolen data. Typically, data is stolen unnoticed by its owner, who is often unaware of the loss and must, sometimes, inevitably face the very serious repercussions only after some time has passed, thereby leading to more serious consequences.

Cybersecurity is now a fundamental fact of globalization. In the USA, the National Defense University (NDU) has defined the *cyberspace* as an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected information systems and their associated infrastructures [25].

Nowadays, we should consider that the global transformation of the industry to a renewed digital industry has given rise to other unexpected consequences. Many people, such as terrorist, hacktivist, and hackers are making life more

✉ S. Soderi
soderi@ieee.org

[1] Independent Cybersecurity Researcher and CPEH, Firenze, Italy

dangerous the life for those using digital products such as body sensors. Many data breach reports indicate that there are some industries that appear to be cyber-criminals favorites. In particular, health-care organizations and financial services are at the top of the list [1, 2]. Indeed, any data breach has a true cost, which may include not only a direct financial impact, but also a reputational damage. In any case, factors that affect this cost are

- The number of records stolen;
- The time to identify and fix the data breach;
- The cost to management.

In 2018, a very first analysis on how to apply a watermark-based physical layer security solution to acoustic communication was published [35]. In this paper, the author extends his previous publication with a deeper analysis of the acoustic channel model. Furthermore, the utilization of a different modulation scheme, that avoids phase gaps, has led to a wider security region around the legitimate receiver. The contribution of this paper is as follows:

- *Security attack scenario* The author of this paper has described herein a scenario in which the wide use of wireless sensors may be appealing for cyber-criminals. There is no doubt that these sort of people would be interested in the sensitive data exchanged between these sensors.
- *Acoustic communications* The author suggests the use of acoustic communications as an unconventional wireless link.
- *Physical layer security protocol* The author has developed a new transceiver to provide the architecture for acoustic communications. The innovative process to deploy a physical layer security protocol consists of three parts: spread-spectrum watermarking, a selective jamming receiver and a data decomposition method.
- *Analysis and evaluation* This paper describes the application of a blind physical layer security for wireless devices by exploiting audio communications. The author also discussed herein the effect of the distance between transmitter and receiver on the acoustic channel capacity.

The rest of this paper is organized as follows. Section 2 overviews the related work and the motivation behind this study. Section 3 describes the physical layer security system model applied to an acoustic communication scenario. Then, the paper continues with the analysis and results achieved in the test-bed. Finally, the conclusions are presented in Sect. 6.

2 Related Work

Since we live an hyper-connected society in which billions of data are exchanged wirelessly, this section provides the technical background necessary to understand the importance of having secure wireless communications among sensors. In the following subsections, the author describes the wireless sensors networks scenario and proposes an acoustic-based solution to overcame the security issues.

2.1 Data Breach

Over the last few years, many digital security firms have started to monitor data breaches. Today, the attacks on companies and governments have increased, impacting the data of millions of people. While this scenario is beginning to create new data protection and security processes, it will take significant time and money to fix these security deficiencies. The list of digital data breaches started many years ago, when in 1984 the Throwback [5] agency reported that one of its servers was hacked and millions of records were stolen. Most recently, in 2012, databases of LinkedIn [7] and Dropbox [3] were breached. Until last year, when the consumer credit report agency Equifax [4] realized that hackers were stealing credit card information, names, addresses and more [10].

Every year seems to have a unique trend its own in terms of data breaches. The digital security company, Gemalto [6], uses the breach level index (BLI) to monitor these events every year. Gemalto gathers this information by using the Internet, news articles and other sources [1]. Figure 1 shows data breaches classified by incident type and source over the last 5 years. It depicts an interesting trend. Since 2015, *health-care industry* have been more affected by security breaches than the financial institutions. In recent years, the health-care industry has been one of the prime targets for cyber-criminals. The reason behind cyber-attacks on health-care companies comes from the information stored into medical records. Usually, these data contain more identity detail than any other industry. Moreover, for the fact that health-care systems are widely regarded as having rather weak security and therefore makes them very attractive to hackers [9]. Cyber-attackers tend to capitalize on certain types of data, notably identity. Figure 1 also shows that malicious external attacks are the root cause of data breaches.

2.2 Our Hyper-Connected Society

We now live in a hyper-connected society where communications have infiltrated our lives. Technological progress has spread electronic devices everywhere, thereby creating

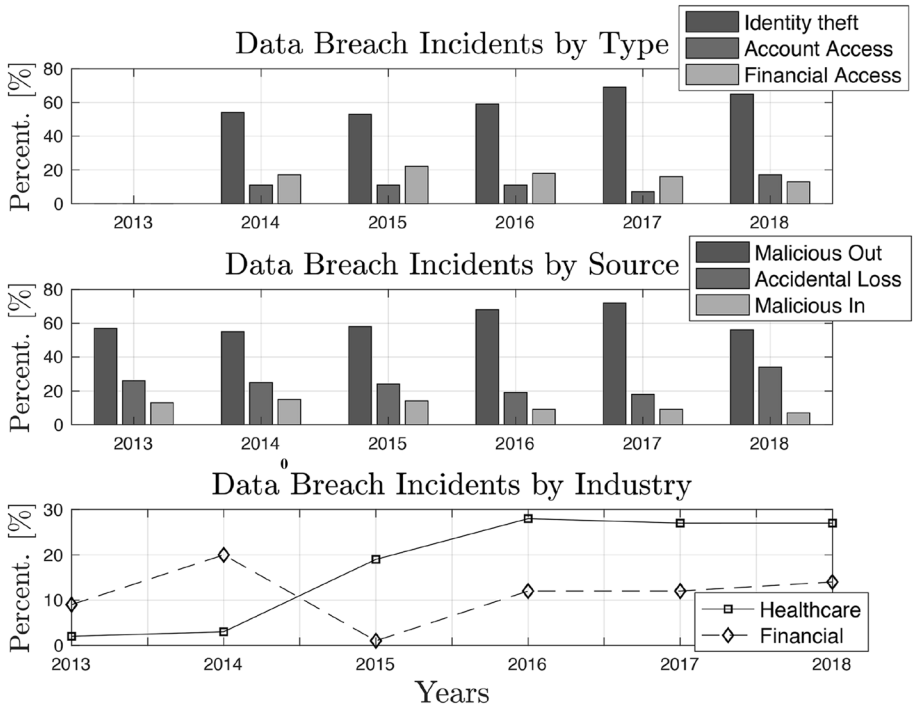


Fig. 1 Data breach incidents during the past 5 years [1]. In 2013, data were not classified by type

an augmented environment in which humans can interact with *smart objects*. We are living in the era of the Internet of things (IoT).

Wireless sensor networks (WSNs) can be classified by their application: intelligent buildings, precision agriculture, medical devices, machine surveillance and preventive maintenance [24]. Another important category is the wireless body area networks (WBAN). These networks are part of the cyberspace that not only give people support on their daily activities but also collect information on humans. In accordance with the *tier model*, WBAN and, more generally, wearable wireless networks (WWNs), include three levels of communication [13, 30].

Wearable sensors collect data within *tier 1* and convey this information to *tier 2* for aggregation purposes and data processing. Finally, data are transmitted to *tier 3* making them available for remote access. As shown in Fig. 2, the classical WBAN can be classified as an *on-body* communication. Instead, all the communications that occur in *tier 2* are *off-body* [13].

In this transmission chain, the security is one of the major concerns because an adversary, i.e. Eve, in Fig. 2 can perform several attacks. And the wireless link between nodes in the WBAN can also be attacked.

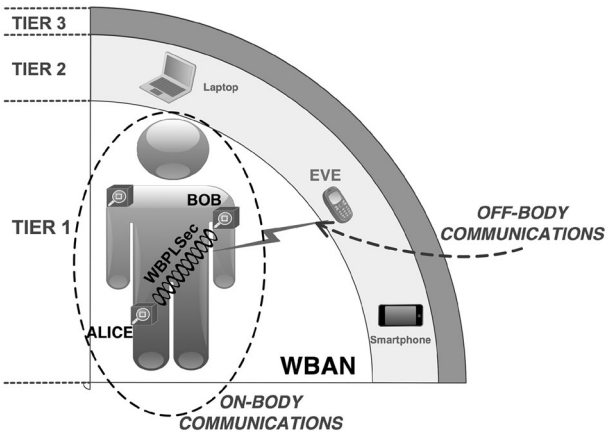


Fig. 2 Architecture of the WBAN: tier model and on-body/off-body communications

2.3 Motivation

The rapid development of IoT industry revealed the importance to have appropriate solutions to overcome security issues. In the next future, IoT devices, with limited resources and heterogeneous technologies, need to implement lightweight security protocols [17, 18]. IoT-based medical devices described in the tier model have changed the traditional ways for patients to get a health check-up in hospital. Smart WBANs will sense, process and communicate sensitive information of the patient to doctors. It is an outstanding improvement in medical treatment. However, at times, technical progress can—if not mastered well—present certain security risks. Nowadays, wireless medical devices create a border-less network in healthcare organizations. More generally, the wide use of WBAN

Fig. 3 Relationship between cryptography, steganography and watermarking

smart devices coupled with the evolution of malwares calls for a rethink on the security of WSNs.

The design of security solutions for WBANs will overcome the resource limitations in each wireless device. The balance between security, usability, and efficiency are aspects that will be taken into account.

The latest standardization of WBAN is the IEEE802.15.6 [11]. This standard aims to cover low-power, short-range wireless communication for both on-body and off-body networks. It provides the security structure for WBAN applications. This structures includes different states, procedures and protocols [37].

So far, although there are security solutions, in several applications security is implemented through cryptography at the upper layers in the open system interconnection (OSI) model [12]. However, in the past few years, several techniques that are based on signal processing have been used to secure communications at the physical layer, and have shown to be promising methods where a standalone security solution is needed. Undoubtedly, nodes of a WBAN fall into this category.

Since 1949, when Shannon developed the metric for the information theory for secrecy systems [33]. In the literature, there are several contributions that deal with the *physical layer security* in which secure communications are developed by exploiting wireless channel imperfections, multipath, and even interference. Furthermore, cryptography, steganography and watermarking are techniques that implement data secrecy using different paradigms. Figure 3 shows the relationship between them. Actually, cryptography deals with data secrecy by protecting the message encoding it. On the other hand, the watermarking technique embeds a message into another signal. In this case, the message might be visible. Instead, the steganography hides a message within another signal.

The author recently developed the watermark-based blind physical layer security (WBPLSec) protocol for wireless communications [36]. It combines the first paradigm for watermarking, as described by by Cox et al. (Appendix 1) with a jamming receiver to develop a standalone physical layer security solution.

In 1973, Lampson defined the *covert channel* as a communication channel which is not intended for information transfer at all [27]. Recently, the utilization of covert channels were proposed to circumvent network security policies by establishing new communication paths [20].

In this paper, the author extends the WBPLSec to *acoustic communications*. At the time of writing, there was no literature available to describe a similar technique whereby the watermark-based communication could exploit acoustic emanations to secure a wireless communication in WBANs.

3 Scenario

3.1 Understanding Acoustic Covert Channel

Two electronic devices in the same room, without any physical connection, between them, are separated by an *air-gap*. This scenario cannot guarantee the isolation between two computers [19]. Recently, *acoustic communications* became important in the field of short-range communications. Wang et al. developed an acoustic-based dual-channel communication, which uses a speaker and the microphones on off-the-shelf smart-phones to achieve concurrent audible and hidden communication [38]. Whereas, Mao et al. exploit inaudible sound to implement an high accurate objects motion tracking system [29].

Acoustic emanations produced by electronic devices can bridge the air-gap. The idea proposed in this paper addresses the countermeasures against confidentiality and integrity attacks by exploiting an acoustic covert channel. WBANs have high dynamics by nature. Nodes join and leave the network continuously. And in such a scenario, WBANs are subject to threats from network dynamics. Building new sensors with physical layer capability to secure a wireless communication through acoustic channel makes the entire WWN stronger.

Humans can perceive sound frequencies within the range of 20 Hz to 20 kHz. Whereas, ultrasounds are defined as those frequencies above 20 kHz. Sound-based covert channels can stealthily bypass many information flow control mechanisms. In scientific literature, there are contributions in which covert mesh networks are implemented over the air [20]. Ultrasonic communications are feasible with good accuracy by using standard microphones and loudspeakers [16, 22].

On the other hand, from the security point of view, ultrasonic sound does not require any permission and a computer can emit sounds to anything or anyone that hear them *bypassing* the network security restriction on policies. Indeed, in this mechanism was exploited by malware to infect other devices [19, 22]. Only military devices are able to mitigate this kind of security issue by disabling the sound-card driver when it is not needed.

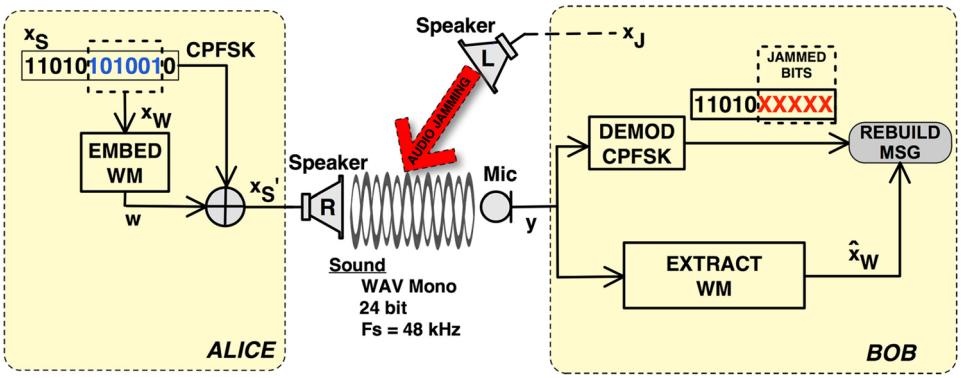


Fig. 4 WBPLSec system model in air-gap acoustic channel

In 2018, Zhang et al. introduced a plan that exploits a friendly jamming on the receiver to secure an acoustic communication between smart devices. They use frequencies in the audible band. In their plan, both sender and receiver share a random secret via an independent channel [40].

3.2 WBPLSec System Model in Acoustic Communications

This paper proposes the application of the WBPLSec over an acoustic channel by using an ultrasonic frequency range nearby. Figure 4 depicts the WBPLSec system model in acoustic communications. WBPLSec transmits the information via two independent paths implementing *data decomposition policy*. The information is sent via a narrow-band signal and through the SS watermarked signal. The narrow-band signal is partially jammed by Bob, but the watermark into the SS signal is used to re-compose the entire symbol [36]. Figure 5 illustrates the spectrum occupation when the WBPLSec is applied to the acoustic air-gap channel.

In accordance with the first rule of the framework presented by Cox et al. [14] (Appendix 1), a transmitter combines the original modulated signal with an SS watermark and an embedding rule defined as

$$x'_S(i) = x_S(i) + \mu w(i), \tag{1}$$

where $x_S(i)$ is the i-th sample of the continuous phase frequency shift keying (CPFSK) transmitted signal, μ is the scaling parameter and $w(i)$ is the SS watermark.

The direct sequence spread spectrum (DSSS) technique is selected for the signal watermarking implementation. The author selected a CPFSK instead of FSK to address the problem of audible clicks during the phase shift. Indeed, by using the FSK, each symbol is represented as a cosine wave but symbols do not connect seamlessly. These phase gaps cause *audible clicks* in the speakers. Clearly, the CPFSK does not have this problem.

The host CPFSK modulated signal x_S can be expressed as

$$x_S(i) = \begin{cases} A_a\sqrt{\frac{2}{T_{hs}}} \cdot cos(2\pi f_1 i + \theta(0)), & \text{for } 0 \le i \le T_{hs} \text{ (binary 1)}, \\ A_a\sqrt{\frac{2}{T_{hs}}} \cdot cos(2\pi f_2 i + \theta(0)), & \text{for } 0 \le i \le T_{hs} \text{ (binary 0)}, \end{cases} \tag{2}$$

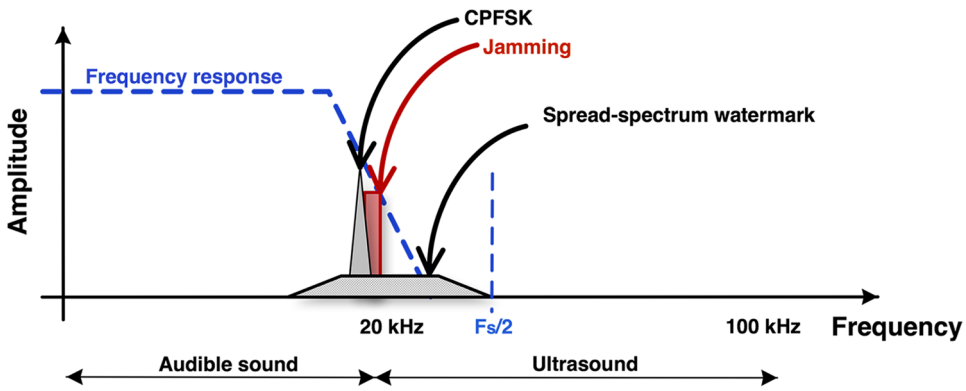


Fig. 5 Spectrum of the WBPLSec in acoustic air-gap channel

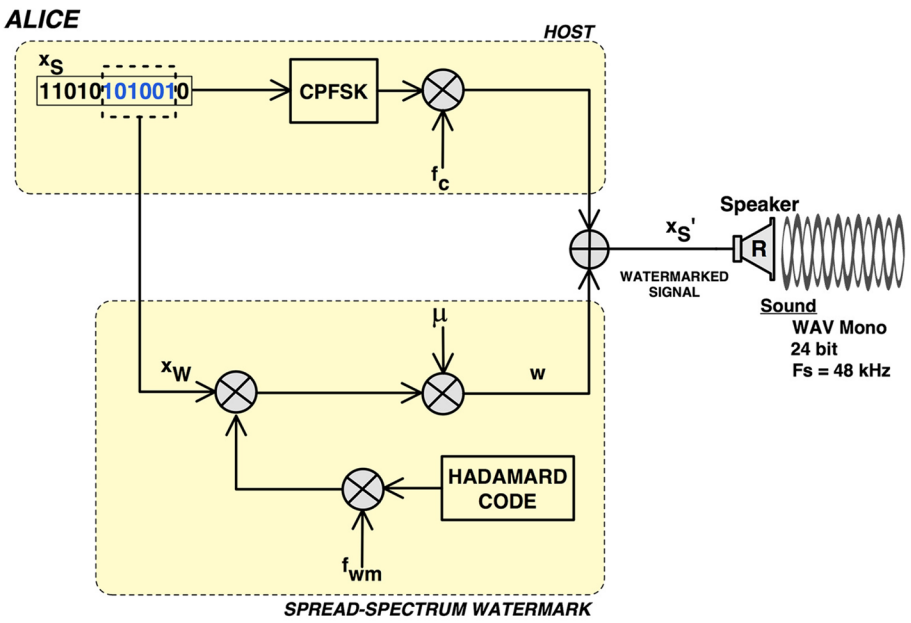


Fig. 6 Watermark embedding and modulation in the acoustic transmitter, i.e. Alice

where

$$f_1 = f_c + \frac{1}{2T_{hs}}$$
$$f_2 = f_c - \frac{1}{2T_{hs}}$$

where A_a is the amplitude, T_{hs} is the symbol time, f_c is the carrier frequency of the modulated signal, f_1 and f_2 are the two frequencies needed to transmit two binary digits. The $\theta(0)$ denotes the value of the phase at time $t = 0$. Author assumed $\theta(0) = 0$.

The DSSS watermark signal can be expressed as

$$w(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_W(i))_j (x_W(i))_k, \quad (3)$$

where $(x_W(i))_k$ is the k-th data bit of the watermark signal. $(c_W(i))_j$ represents the j-th chip of the orthogonal pseudo-noise (PN) sequence. $g(i)$ is the pulse waveform, T_c is the chip length and $T_b = N_c T_c$ is the bit length. Then, w modulates a carrier frequency close to the range of the f_c used by CPFSK.

Figure 6 shows the embedding stage of the watermark in CPFSK, where the information x_W is spread and then added to the host signal. In order to maintain the versatility, the watermarked signal x'_S is encoded into a waveform audio file format (WAV). Alice transmits the x'_S to Bob by playing the WAV file through her loudspeaker.

As shown in Fig. 7, while Bob is recording (i.e. receiving) the message, he jams it by playing the jamming signal encoded into another WAV file. In this diagram only Bob, who is the legitimate receiver, knows which part of the WAV file he jammed. Later, Bob is able to get a clean signal by replacing corrupted samples with the information he conveys via the SS watermark that is immune to any jamming interference. In contrast, the eavesdropper cannot remove the interference because he does not have any information on the jamming characteristics.

The physical layer security mechanism implemented by the WBPLSec consists of steps shown in Algorithm 1. In this model each sensor is equipped with a microphone and a loudspeaker, therefore nodes in the WBAN convey a human vital signal over the acoustic air-gap covert channel. Figure 2 shows the operating scenario of the WBPLSec inside the three-tier network model, in which the proposed solution can mitigate threats, such as the man-in-the-middle (MitM) and eavesdropping, within off-body communications.

4 Analysis and Evaluation

4.1 Channel Capacity

It is of interest to calculate the data rate of acoustic communications for different ranges and conditions. Since 1948, Shannon defined the *channel capacity* as the basic limit on communicating information. Based on his formulation, if the information rate is less than the channel capacity, then it is theoretically possible to achieve an error-free communication through the channel [31].

Algorithm 1 WBPLSec protocol in acoustic air-gap channel

1: **procedure** PHYSICAL LAYER SECURITY
2: *SS Watermarking* (*ALICE*):
A message is first modulated with DSSS and then embedded into the host CPFSK signal.
The CPFSK watermarked message is encoded in a WAV file, and then played, i.e. transmitted, through the loudspeaker.
3: *Jamming Receiver* (*BOB*):
The receiver jams N_W samples for each symbol transmitted by Alice.
The jamming signal is encoded into a WAV file and played through BOB's loudspeaker while he is recording ALICE's message with his microphone.
The received signal is then processed by the CPFSK demodulator to recover the data transmitted through the audio channel.
Due to the jamming, part of the signal is now corrupted and unusable.
4: *Watermark Extraction* (*BOB*):
The receiver extracts the watermark using a code matched filter.
5: *Symbol Rebuild* (*BOB*):
Knowing which samples are jammed the receiver, i.e. Bob, is able to rebuild a clean symbol using information contained in the watermark.
6: **end procedure**

Thus, the channel capacity (C) can be formulated as follows:

$$C = B \cdot log_2(1 + \gamma), \tag{4}$$

where B is the communication bandwidth, $\gamma = S/N$ is the signal-to-noise ratio (SNR) in which, S is the power of the acoustic signal received, and N is the additive white Gaussian noise (AWGN) interference.

To get good quality speech communication needs at least 2400 Hz [23]. Moreover, in speech a typical data rate is 50 bit/sec [32].

In wireless communications, the *efficiency* is defined as C/B. By comparing the efficiencies in mobile and acoustic communications it is evident how the latter uses the channel much less efficiently than typical electromagnetic communications systems. This is due to the low quality of the acoustic channel and how speakers and microphones are made [23].

The author of this paper has evaluated the channel capacity in acoustic communications between the JBL Bluetooth loudspeaker and the built-in microphone in the MacBook Pro, sweeping a sinusoid of 10 s in a range of 20 Hz to 22 kHz. Figure 8 shows the acoustic channel capacity for different ranges. As expected, the data rate close to ultrasound frequency range decreases to 100 bit/sec. Actually, the hardware used for these tests it is not designed for ultrasounds.

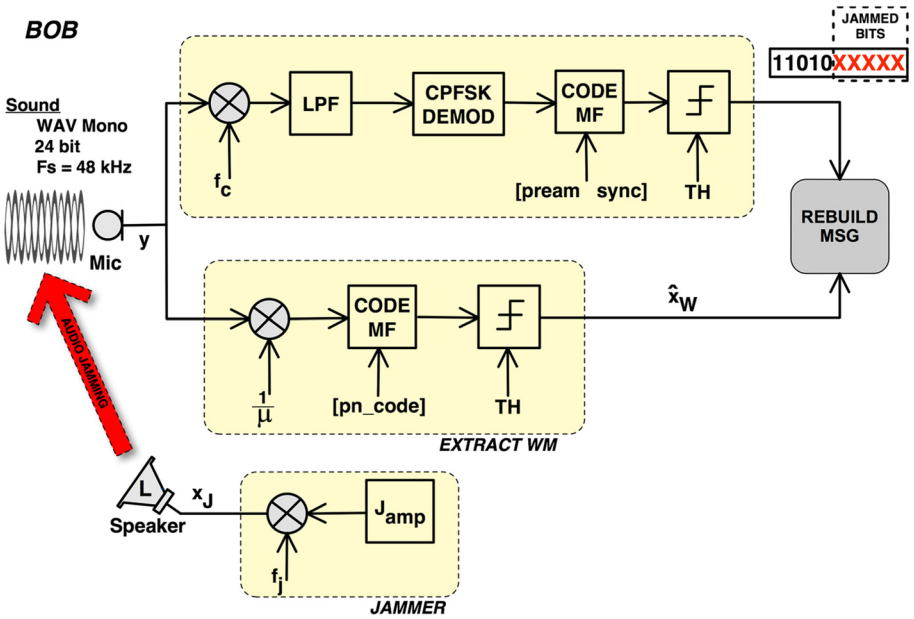


Fig. 7 Watermark extraction and demodulation in the acoustic receiver, i.e. Bob

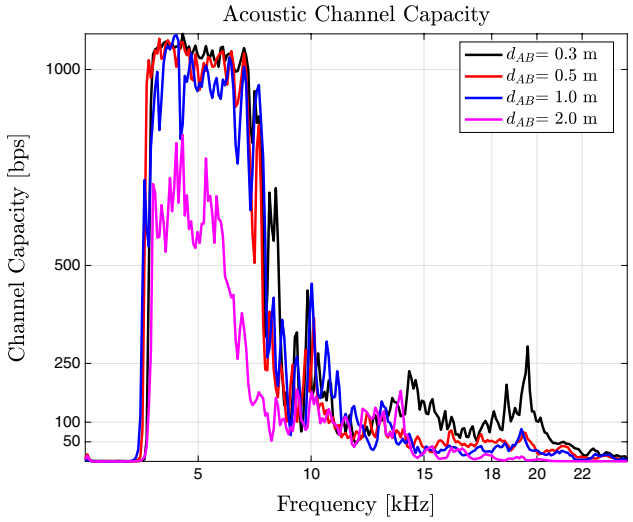


Fig. 8 Channel capacity of a speaker-to-microphone communication

On the other hand, this throughput it is enough to support a physical layer security protocol such as the WBPLSec.

4.2 Secrecy Capacity in Acoustic Channel

Sound is a wave phenomenon. The amount of energy which is transported in a given area of air per unit of time is known as the *intensity* of the sound wave. In acoustics there are many mechanisms that can reduce the sound levels. Incident sound waves are absorbed by material. Furthermore, sound power decreases as the square of the distance. Author assumed the *inverse distance law* as the primary attenuation mechanism in acoustic communications.

The instantaneous signal-to-interference-plus-noise ratio (SINR) at legitimate receiver, i.e. γ_M, is given by

$$\gamma_M \propto \frac{\frac{E'_S}{d_{AB}^2}}{N_0 + E_J}, \tag{5}$$

where both E'_S is the sound power of the watermarked signal, d_{AB} is the distance between Alice and Bob, N_0 is the additive Gaussian noise and E_J is the sound power of the jamming. Due to the proposed jamming receiver architecture, the E_J does not undergo any attenuation at the legitimate receiver.

The instantaneous SINR at the eavesdropper, i.e. γ_E, is given by

$$\gamma_E \propto \frac{\frac{E'_S}{d_{AE}^2}}{N_0 + \frac{E_J}{d_{BE}^2}} = \frac{\frac{E'_S}{d_{AE}^2}}{N_0 + \frac{E_J}{d_{AE}^2 + d_{AB}^2 - 2 \cdot d_{AE} \cdot d_{AB} \cdot cos\theta}}, \tag{6}$$

where both E'_S is the sound power of the watermarked signal, d_{AE} is the distance between Alice and Eve, N_0 is the additive Gaussian noise, E_J is the sound power of the jamming and d_{BE} is the distance between Bob and Eve. Using the *cosine law* (Appendix 2), d_{BE} is written in the expanded form.

The information theory for secrecy systems published by Shannon in 1949 defined the condition of *perfect secrecy* where the eavesdropper can not pull out or extract any information from the transmitted signal [33]. Subsequent studies extended the secrecy of communications by also defining new metrics. The *secrecy capacity* defined by Wyner is the maximum transmission rate achievable whenever the eavesdropper has a noisier channel than the legitimate user [39].

The secrecy capacity (C_s) of legitimate link is defined, similarly to the standard capacity, for the non-degraded Gaussian wiretap channel [15] as follows

$$\begin{aligned} C_s &= \max\{C_M - C_E, 0\}, \quad \text{where} \\ C_M &= \frac{1}{2}\log_2(1+\gamma_M) \quad \text{bit/transmission} \\ C_E &= \frac{1}{2}\log_2(1+\gamma_E) \quad \text{bit/transmission} \end{aligned} \tag{7}$$

where C_M is the channel capacity from Alice to Bob, i.e. the main acoustic channel, and C_E is the channel capacity

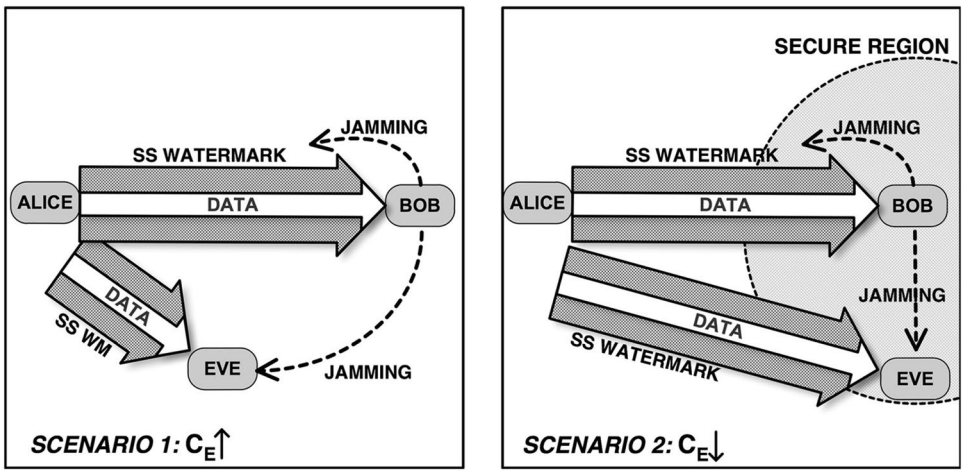


Fig. 9 Secure region around the legitimate receiver

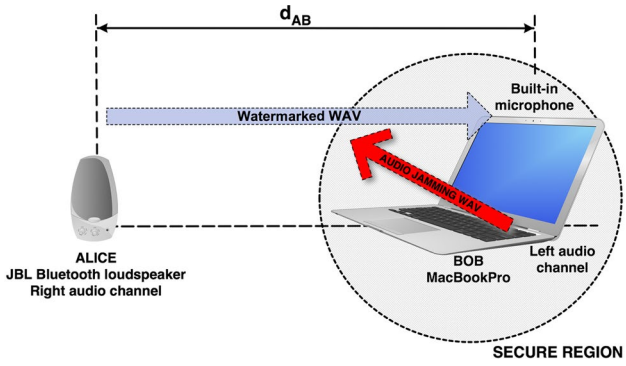


Fig. 10 Measurement setup

Table 1 Base-band CPFSK specifications

Parameter	Value
Modulation	CPFSK
Modulation order	2
Sample frequency[1]	2.4 kHz
Frequency separation	400 Hz
Samples per symbol	50

[1] Sample frequency at base-band. The signal is then re-sampled at 48 kHz before the up-conversion

from Alice to Eve, i.e. the acoustic channel exploited by the eavesdropper. When Bob has a better channel realization than Eve, C_S is given by the (7). Otherwise, if Eve has a better SINR than Bob, C_S is set to 0. In other words, Alice might decide not to transmit. From (5) and (6) is clear as SINRs decrease with increasing of distances. Whereas, (6) depicts how γ_E increases, and C_E increase accordingly, when d_{AE} gets closer to 0 for any value of θ. Thus, as shown in Fig. 9, the most advantageous position for Eve is close to the transmitter, i.e. scenario 1.

This theoretical analysis indicates that the WBPLSec seems to be a valuable technique for deploying physical layer security by creating a secure region around the legitimate receiver.

Figure 9 depicts two scenarios. The first in which Eve is far away from Bob. In this case the C_E increases, due not only to the limitation of Bob's jamming ability but also to the fact that Alice might suspend the data transmission. Instead in the second scenario, when Eve moves closer to the legitimate receiver, Bob jams all the acoustic communications near him. In this case, the eavesdropper's channel capacity decreases and Bob can establish a region around him with $C_S > 0$ where secure communication occurs. However, it is important to emphasize how Bob can rebuild the clean signal by exploiting the information set out in the watermark.

4.3 Measurement Setup

Experiments have been performed on a real test-bed to investigate the performance of the WBPLSec over the acoustic air-gap channel. The test-bed consisted of an Apple MacBook Pro and a JBL Flip Bluetooth speaker as shown in Fig. 10. In regard to the wireless speaker, it was necessary to vary the relative distance d_{AB} between Alice and Bob. The MacBook Pro was used as the main processing unit. Alice's is emulated with the Bluetooth speaker which plays the *right* audio channel only. Instead, Bob is emulated by the MacBook Pro that records by using the microphone and it plays the *left* side audio channel only. The decision to play WAV files as a mono channel, i.e. the right side only for Alice and only left side to jam, is done in order to split the communication and use only one main processing unit, i.e. the MacBook Pro.

As output devices, both MacBook Pro and JBL Flip have a frequency response that spans from 20 Hz to 24 kHz. Moreover, the internal speakers support a stereo data stream at bit depths of 24 bits per sample and at sample rate of 48 kHz. By the Nyquist-Shannon Sampling theorem [34], this means that the highest frequency signal that can be perfectly reconstructed without aliasing is a little below 24 kHz. On the other hand, as an input device, the internal microphone of the MacBook Pro supports recording at bit depths up to 24 bits per sample and a sample rate of 48 kHz (F_s).

4.4 Acoustic Communications Experiments

The CPFSK transmitter is a MATLAB [8] function that encodes binary 1's and 0's as two frequencies in the near range of ultrasound as shown in Fig. 5. This function first, creates the CPFSK base-band signal with the specifications in Table 1. Then, the base-band signal is up-converted to pass-band to be transmitted over the acoustic channel.

Figure 11 illustrates the transmitted signal in the acoustic air-gap covert channel, i.e. the watermarked CPFSK signal and the CW jamming as well.

The first part of the Alice's message consists of a preamble plus a synchronization sequence. The message payload consists of 128 bits. From this payload, only 40 bits (i.e., x_W) are utilized to create the SS watermark. The script creates a mono WAV right channel file (the left channel is silent) ready to be transmitted through the Bluetooth speaker. The amplitude of the watermarked signal is scaled up in order to maximize the volume of a 24 bit audio signal. The script also creates a continuous wave (CW) jamming signal. This signal uses a set amount of time to jam 40 bits over one frequency utilized by CPFSK. A second mono WAV left channel file is created with jamming information. The author assumed a perfect synchronization of these two WAV files.

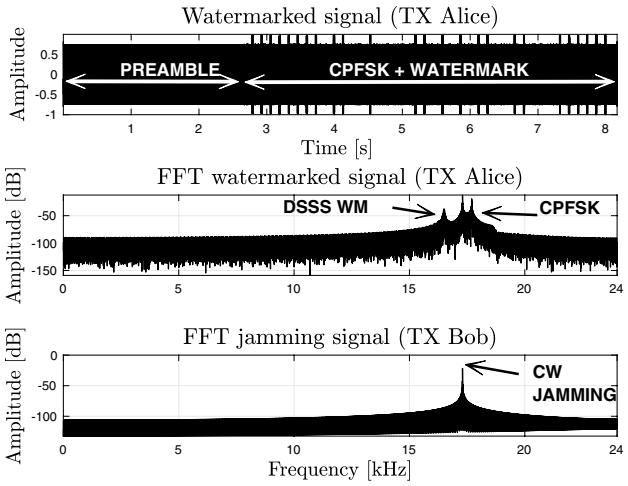


Fig. 11 Alice's watermarked signal and Bob's jamming signal

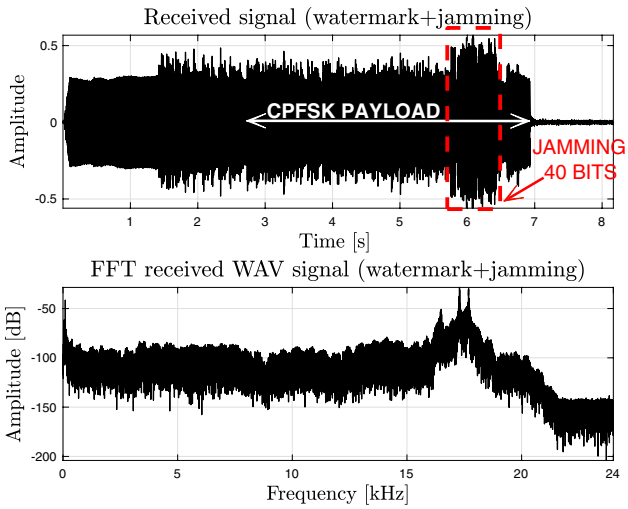


Fig. 12 Bob's received signal

Table 2 LPF specifications

Parameter	Value
Filter type	Low-pass Butterworth (IIR[1])
Pass-band	2.4 kHz
Stop-band	2.8 kHz
Attenuation[2]	80 dB

[1] Infinite impulse response (IIR).

[2] Minimum attenuation in the stop-band

Bob records the jammed WAV file through the MacBook Pro internal microphone as shown in Fig. 10. Figure 12 shows the received acoustic signal when Bob is 50 cm far from Alice.

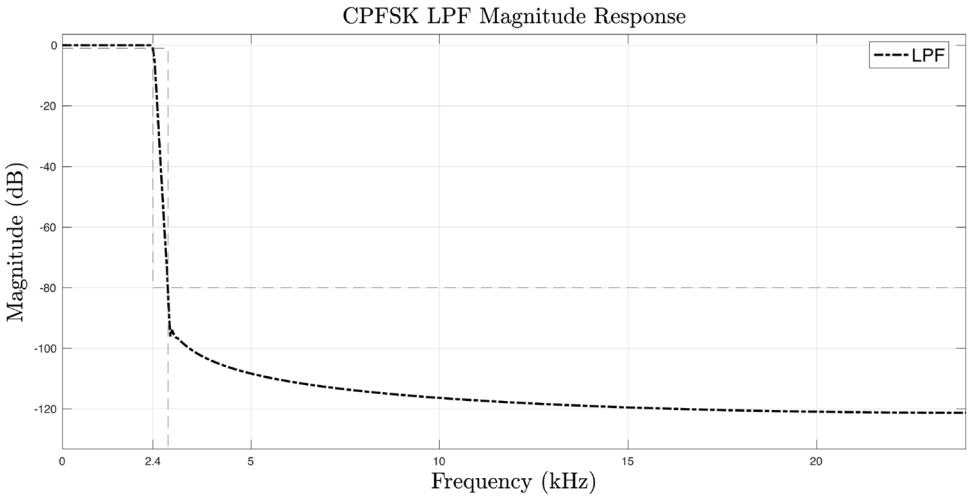
The received audio signal after the microphone is down-converted to the baseband by the carrier frequency f_c and then filtered with a low-pass filter (LPF). Figure 13 shows the magnitude response of the Butterworth LPF used by Bob before the CPFSK demodulation. Table 2 shows the LPF specifications. The author chose this type of filter because it has a flat frequency response in the pass-band and zero roll-off response in the stop-band.

In accordance with the WBPLSec Algorithm 1, the receiver demodulates the CPFSK. Then, it extracts the watermark to rebuild the original message. The watermark extraction is performed with the use of a code matched filter (CMF). This process is performed by computing the normalized statistics as [28, 36]

$$r \triangleq \frac{\langle \boldsymbol{y_M}, \boldsymbol{c_W} \rangle}{\langle \boldsymbol{c_W}, \boldsymbol{c_W} \rangle}, \tag{8}$$

where the $\boldsymbol{y_M}$ is the received signal by Bob as shown in Fig. 7, $\boldsymbol{c_W}$ represents the PN sequence. The author assumed $\langle \boldsymbol{c_W}, \boldsymbol{c_W} \rangle = 1$, i.e. PN sequences have unit energy. Figure 14

Fig. 13 Butterworth CPFSK low-pass filter



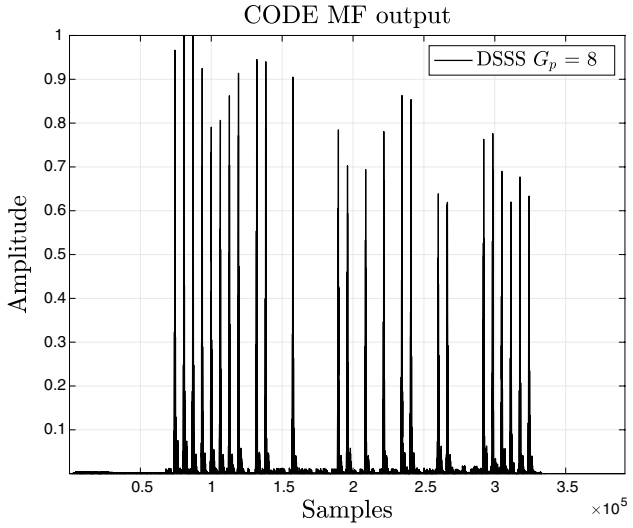


Fig. 14 Code matched filter output for the watermark extraction

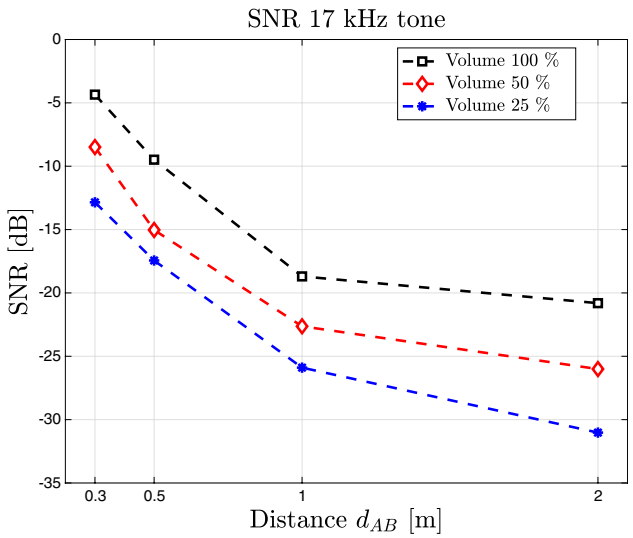


Fig. 15 SNR reduction with distance for different Bob's volume settings

shows the output of the CMF. It is known how the matched filter maximizes the SINR at the output of the detector.

The detector is the same one that was introduced with the traditional spread spectrum watermarking [28, 36], and the estimation of the embedded bit is given by

$$\hat{x}_W = sign(r). \tag{9}$$

The propagation phenomena in the acoustic channel affects the received signal. *Acoustic attenuation* represents the energy loss during the sound propagation in the air. The sound power decreases with doubling the distance by 6 dB. The author adopts a 17 kHz and 3 s length tone to measure the attenuation between the sender and the legitimate receiver. Figure 15 shows the decay in the test-bed between Alice and Bob for different volume settings.

A key feature of WBPLSec architecture is the jamming receiver. Bob transmits a jamming interference on the same frequencies utilized by Alice. With this technique, Bob destroys a specific part of the packet received. Acoustic communications are based on the sound level emitted by the sender. Bob receives the acoustic signal through the microphone. The microphone records a signal up to 24 kHz. In that frequency range, it has a linear system that utilizes an automatic gain control (AGC) to adjust the signal amplitude and use the internal analog to digital converter (ADC) in its whole range. In this architecture, Bob selected a 17.3 kHz CW jamming to suppress up to 40 bits of the payload transmitted by Alice. The jamming effectiveness depends on the distance between Alice and Bob. The idea utilized for the jamming is to increase its intensity by altering the dynamic of the microphone and weakening part of the wanted Alice's signal.

On the other hand, the jamming power shall be adjusted. The $\gamma_M|_{min}$ at the receiver imposes the theoretical lower bound on the bit error rate (BER). Figure 16 shows what occurs when the distance between Alice and Bob increases. For instance, when d_{AB}, doubles. The amplitude of the acoustic signal x'_S at receiver gets lower, instead the jamming intensity remains constant. This condition is acceptable until the SINR at receiver, i.e. γ_M, does not get lower than $\gamma_M|_{min}$. When it occurs, Bob shall reduce the jamming power, i.e. E_J, otherwise he might not demodulate the received signal.

4.5 Energy Cost to Evaluate WBPLSec

The author assumed that the efficiency of the proposed algorithm can be measured by using the energy cost metric. The WBPLSec is a promising technique for low-power sensor network. This algorithm secures the wireless communication utilizing lower energy than other jamming techniques [36]. Table 3 shows the evaluation of energy cost for each packet transmitted by Alice and jammed by Bob [35]. The implementation of WBPLSec requires more energy but author expects to save computation when compared to encryption [21]. This metric shows that the extra energy can be tuned changing the length of the watermark, i.e. N_W, and the number of jammed bits, i.e. M.

4.6 Results

Table 4 lists the parameters used for acoustic communications experiments described in the previous section. The main objective was to verify the reliability of the WBPLSec over an acoustic air-gap channel. The acoustic communication between Alice and Bob was evaluated using BER as metric. BER results show that by using the CPFSK and the jamming power adjustment, the secure region created by

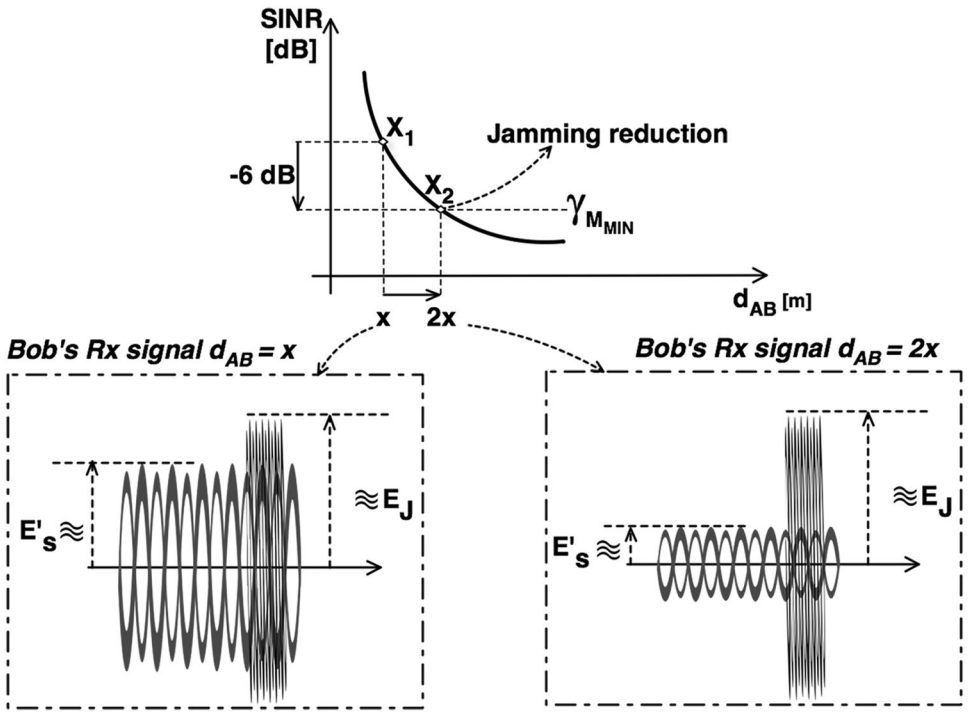


Fig. 16 Jamming power adjustment

WBPLSec around Bob gets wider up to 2 m and wider than previous results [35].

In acoustic communications, ambient noise and distance are the greatest limitations. Environmental noise usually creates audio clipping because the microphone is driven to its maximum excitation [22]. Typically, interference generated by music and speech is concentrated in frequencies lower than the ones chosen for these experiments [19]. The results confirmed these limitations and therefore, experiments occurred in a quiet room. In any case, the architecture proposed utilizes a Butterworth LPF to reduce the environmental noise effect.

During the measurement campaign, the author modified the distance between Alice and Bob, the DSSS processing gain (G_p) and the intensity of the watermark μ as defined in (1). Varying the distance between Alice and Bob, the higher the G_p, the lower the BER yields to increase the performance of the proposed protocol. Table 5 contains the description of the main parameters used in this study. Figure 17 illustrates the BER of the payload (i.e. 128 bits) at the legitimate receiver.

In literature, there are many contributions that deal with the maximum transmission rate achieved in acoustic communications [16, 19, 20]. The upper bound defined by the channel capacity of the acoustic covert channel analyzed in Sect. 4.2 represents a theoretical limit. Experiments show that at a distance of 2 m Alice and Bob can achieve a transmission rate of 48 bps. The bit-rate achieved is lower than the channel capacity represented in Fig. 8. This is due to the microphone and speakers used, as well as to the architecture selected. Actually, WBPLSec exploits a jamming receiver. This technique increases the CPFSK BER because for each packet exchanged, at least 40 bits are jammed. On the other hand, in WBPLSec it is important to evaluate the BER of the watermark, i.e. BER_{WM}. It is not higher than 5.5% at the distance of 2 m, as shown in Fig. 18. The results shown in Fig. 18 prove that an improvement in the BER_{WM} is achieved by increasing the watermark spreading factor.

5 Limitations and Further Research

The author investigated the acoustic channel. This medium has some limitations in the communication range on how even the maximum achievable bit-rate is. The actual bit rate is usually lower than the channel capacity and is determined

Table 3 Energy cost for each packet [35]

ALICE energy Tx	BOB energy Tx	WBPLSec total energy	$N = 128, N_W = 40, M = 40$
$E_{pkt}\left(1 + \frac{N_W}{N}\right)$	$\frac{M}{N}E_{pkt}$	$E_{pkt}\left(1 + \frac{N_W}{N} + \frac{M}{N}\right)$	$1.625 \cdot E_{pkt}$[1]

[1] E_{pkt} is the energy for each packet

Table 4 Scenario parameters for the acoustic WBPLSec experiments

Parameter	Value
d_{AB}	0.3 m, 0.5 m, 1 m , 2 m
CPFSK frequencies[1]	17.3 kHz, 17.7 kHz
DSSS carrier frequency	16.5 kHz
Samples per DSSS symbols	8
Jamming frequency	17.3 kHz
CPFSK bit-rate	48 bps
Number of bits CPFSK payload (N)	128
Number of bits CPFSK preamble[2]	256
Number of jammed bits (M)	40
Number of bits to create the watermark (N_W)	40
Watermarking scaling parameter (μ)	0.3, 0.5
DSSS Processing Gain (G_p)[3]	8, 16
Alice's WAV file[4]	Mono - Right channel
Bob's jamming WAV file[4]	Mono - Left channel
WAV file depth	24 bit
Input/output sampling frequency (F_s)	48 kHz
Temperature	20 °C

[1] Up-converted using 17.5 kHz carrier frequency.

[2] It consists of the preamble and a synchronization sequence.

[3] Using Hadamard PN code.

[4] Author assumed perfect synchronization between Alice and Bob

by the modulation scheme and the quality of the transmitter and receiver used. Other known limitations, that may affect the acoustic communications, are the effect of the environmental noise on the channel and the equipment's position as well [19]. Furthermore, author assumed the *inverse square law* as primary attenuation mechanism in acoustic communications. On the other hand, the absolute attenuation also increases with the *temperature*. In the literature there are contributions that deal with the impact of the temperature on acoustic communications [23, 26]. However, this paper describes experiments in acoustic channel at a temperature of 20 °C.

In order to overcome these limitations, author plans to compare different digital modulation schemes in acoustic channel medium, but also to test the proposed solution

Table 5 Description of the main parameters

Parameter	Description
d_{AB}	Distance between Alice and Bob
N	Number of bits in the CPFSK payload
M	Number of jammed bits
N_W	Number of bits to create the watermark
μ	Watermarking scaling parameter (Cox's framework)
G_p	DSSS processing gain obtained by using a Hadamard PN code

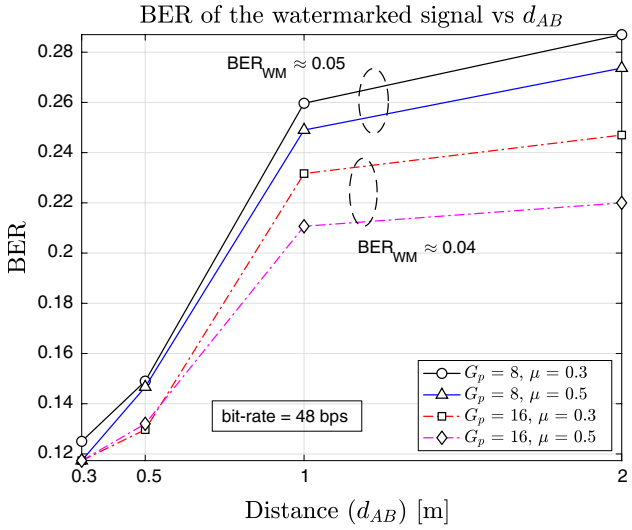


Fig. 17 BER watermarked signal

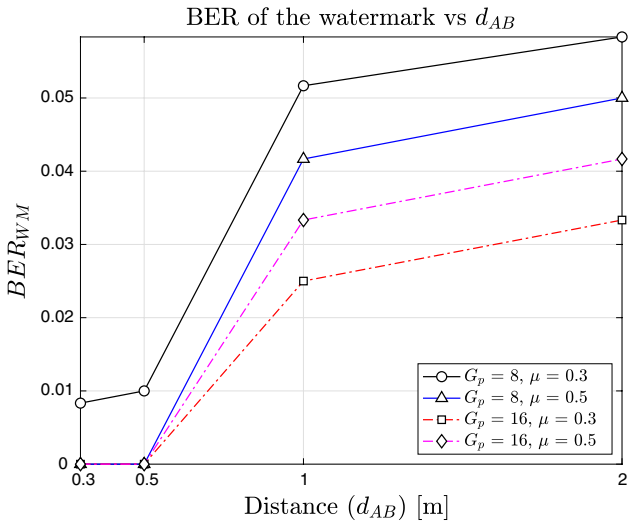


Fig. 18 BER watermark

across different devices. Furthermore, this extension proposal shall include the impact of temperature and different environmental noises on WBPLSec. The aim of these further investigations shall be to enhance the proposed physical layer security solution in a wider scenario.

6 Conclusions

We live in the era of IoT, in which people interact with countless smart objects. Smart wireless objects are presents in many scenarios such as health-care systems, automated houses and inside cars with in-vehicle communications.

This, plus the rapid evolution of malwares imposes a rethink of the security of WSNs. In this work, the author shows how an acoustic covert channel can be used to exchange data securely between wireless sensors.

The watermark-based communication with a jamming receiver needs multiple wireless interfaces. Today, wireless sensors are equipped with several air interfaces, e.g. audio inputs/outputs, BLE and WiFi. The author successfully demonstrated that the WBPLSec algorithm is applicable to acoustic air-gap covert channels to exchange a secret shared key of 128 bits. The sender and receiver communicate by means of speakers and microphones. The results demonstrated that this method is a valuable technique for deploying physical layer security by creating a *secure region* around the receiver up to 2 m.

Both theoretical analysis and acoustic communications experiments prove the robustness of the WBPLSec for acoustic communications. For the first time, this method applies a watermarking technique and a jamming receiver to ultrasonic waves. The WBPLSec technology analyzed herein, can be used to secure communications at physical layer, thereby ensuring data confidentiality against eavesdropping attacks.

WBPLSec is a blind full-rate protocol. A wireless sensor can use it over the acoustic channel to exchange a secret shared key with a neighboring device. Definitely, there are scenarios in which it might be convenient to exploit audio interfaces embedded instead of re-designing the whole wireless sensor. This study supports such strategy.

Appendix 1: Watermarking

Cox et al. [14] in 1997 defined the methodology for the digital watermarking. In accordance to his paradigm, three formulas can be utilized to compute the watermarked signal v'. These equations are

$$v'(i) = v(i) + \mu x(i), \tag{10}$$

$$v'(i) = v(i)(1 + \mu x(i)), \tag{11}$$

$$v'(i) = v(i)\left(e^{\mu x(i)}\right), \tag{12}$$

where $v(i)$ is the ith sample of the signal, μ is the scaling parameter and $x(i)$ is the watermark.

Appendix 2: Cosine Law

Alice, Bob and Eve form a triangle, as shown in Fig. 19.

Using the *cosine law*, the distance between the legitimate receiver and the eavesdropper, i.e. d_{BE}, is given by

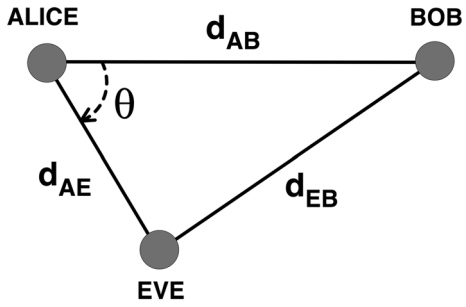


Fig. 19 Cosine law to calculate distances

$$d_{BE} = (d_{AE}^2 + d_{AB}^2 - 2 \cdot d_{AE} \cdot d_{AB} \cdot cos\theta)^{\frac{1}{2}}, \tag{13}$$

where d_{AE} is the distance between Alice and Eve, d_{AB} is the distance between Alice and Bob. θ denotes the angle between d_{AB} and d_{AE}.

References

1. Breach level index. https://breachlevelindex.com.
2. Cost of a Data Breach Study. https://www.ibm.com/security/data-breach.
3. Dropbox. https://www.dropbox.com.
4. Equifax. https://www.equifax.com/personal.
5. Experian. https://www.experian.com.
6. Gemalto. https://www.gemalto.com.
7. LinkedIn. https://www.linkedin.com.
8. MathWorks. http://www.mathworks.com.
9. Report: Healthcare Industry Workers Lack Basic Cybersecurity Awareness. https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-employees-are-low-hanging-fruit-social-engineering-attacks.
10. The Worst Data Breaches of the Last 10 Years. https://www.asecurelife.com/the-worst-data-breaches-of-the-last-10-years.
11. IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks, 2012. https://doi.org/10.1109/IEEESTD.2012.6161600.
12. R. J. Anderson, *Security Engineering—A Guide to Building Dependable Distributed Systems*, vol. 2nd, WileyNew York, 2008.
13. D. B. Arbia, M. M. Alam, Y. L. Moullec and E. B. Hamida, Communication challenges in on-body and body-to-body wearable wireless networks—a connectivity perspective, *Technologies*, Vol. 5, No. 3, p. 43, 2017. https://doi.org/10.3390/technologies5030043.
14. I. J. Cox, J. Kilian, F. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673–1687, 1997. https://doi.org/10.1109/83.650120.
15. I. Csiszar and J. Korner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339–348, 1978. https://doi.org/10.1109/TIT.1978.1055892.
16. L. Deshotels, Inaudible sound as a covert channel in mobile devices. In: 8th USENIX Workshop on Offensive Technologies (WOOT 14). USENIX Association. San Diego, CA, (2014). https

://www.usenix.org/conference/woot14/workshop-program/presentation/deshotels.
17. M. Frustaci, P. Pace, and G. Aloi, Securing the IoT world: Issues and perspectives. In: *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 246–251, (2017). https://doi.org/10.1109/CSCN.2017.8088629.
18. M. Frustaci, P. Pace, G. Aloi and G. Fortino, Evaluating critical security issues of the IoT world: present and future challenges, *IEEE Internet of Things Journal*, Vol. 5, No. 4, pp. 2483–2495, 2018. https://doi.org/10.1109/JIOT.2017.2767291.
19. M. Guri, Y. A. Solewicz, A. Daidakulov, and Y. Elovici, MOSQUITO: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication. CoRR abs/1803.03422, 2018. arxiv:1803.03422.
20. M. Hanspach, and M. Goetz, On covert acoustical mesh networks in air. CoRR abs/1406.1213, 2014. arxiv:1406.1213.
21. W. Harrison, J. Almeida, M. Bloch, S. McLaughlin and J. Barros, Coding for secrecy: an overview of error-control coding techniques for physical-layer security, *IEEE Signal Processing Magazine*, Vol. 30, No. 5, pp. 41–50, 2013. https://doi.org/10.1109/MSP.2013.2265141.
22. Z. Harvest, B. E. SqueakyChat, Ultrasonic communication using commercial notebook computers, 2014. https://github.com/bonniee/ultrasonic/blob/master/SqueakyChat.pdf.
23. S. Holm, O.B. Hovind, S. Rostad, and R. Holm. Indoors data communications using airborne ultrasound. In: *Proceedings (ICASSP '05) IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005*, vol. 3, pp. iii/957–iii/960 Vol. 3, (2005).
24. H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley-InterscienceNew York, NY, 2007.
25. F. D. Kramer and S. H. Starr, *Cyberpower and National Security*, Potomac BooksWashington, 2009.
26. F. Ladich. Acoustic communication in fishes: temperature plays a role. *Fish and Fisheries*, Vol. 19, No. 4, pp. 598–612. https://doi.org/10.1111/faf.12277. https://onlinelibrary.wiley.com/doi/abs/10.1111/faf.12277.
27. B.W. Lampson,. A note on the confinement problem. *Commun. ACM*, Vol. 16, No. 10, pp. 613–615, 1973. http://doi.acm.org/10.1145/362375.362389.
28. H. Malvar and D. Florencio, Improved spread spectrum: a new modulation technique for robust watermarking, *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, pp. 898–905, 2003. https://doi.org/10.1109/TSP.2003.809385.
29. W. Mao, J. He, H. Zheng, Z. Zhang, and L. Qiu, High-precision acoustic motion tracking: Demo. In: *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking, MobiCom '16*, pp. 491–492. ACM, New York, NY, USA (2016). http://doi.acm.org/10.1145/2973750.2985617.
30. C. Otto, A. Milenković, C. Sanders and E. Jovanov. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *J. Mob. Multimed.*, Vol. 1, No. 4, pp. 307–326, 2005. http://dl.acm.org/citation.cfm?id=2010498.2010502.
31. J. G. Proakis, *Digital Communications*, 4th ed. McGraw-HillBoston, Boston, 2000. http://www.loc.gov/catdir/description/mh021/00025305.html.
32. L. Rabiner and B. H. Juang, *Fundamentals of Speech Recognition*, Prentice-Hall IncUpper Saddle River, NJ, 1993.
33. C. Shannon, Communication theory of secrecy systems, *The Bell System Technical Journal*, Vol. 28, No. 4, pp. 656–715, 1949. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
34. C. E. Shannon, Communication in the presence of noise, *Proceedings of the IRE*, Vol. 37, No. 1, pp. 10–21, 1949. https://doi.org/10.1109/JRPROC.1949.232969.
35. S. Soderi, Security in body networks: watermark-based communications on air-gap acoustic channel. In: *13th EAI International Conference on Body Area Networks (Bodynets2018)*. Oulu, Finland, 2018.
36. S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J.H. Iinatti, Physical layer security based on spread-spectrum watermarking and jamming receiver. *Transactions on Emerging Telecommunications Technologies*, Vol. 28, No. 7, 2017. http://dblp.uni-trier.de/db/journals/ett/ett28.html#SoderiMHPI17.
37. M. Toorani, Security analysis of the IEEE 802.15.6 Standard, *International Journal of Communication Systems*, Vol. 29, No. 17, pp. 2471–2489, 2016. https://doi.org/10.1002/dac.3120.
38. Q. Wang, K. Ren, M. Zhou, T. Lei, D. Koutsonikolas, and L. Su, Messages behind the sound: real-time hidden acoustic signal capture with smartphones. In: *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking, MobiCom '16*, pp. 29–41. ACM, New York, NY (2016). 10.1145/2973750.2973765. http://doi.acm.org/10.1145/2973750.2973765.
39. A. Wyner, The wire-tap channel, *The Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x.
40. X. Zhang, J. Liu, S. Chen, Y. Kong, and K. Ren, PriWhisper+: An enhanced acoustic short-range communication system for smartphones. *IEEE Internet of Things Journal*, pp. 1–1, 2018. https://doi.org/10.1109/JIOT.2018.2850524.

Simone Soderi (SMIEEE) received his M.Sc. degree in 2002 from the University of Florence, Florence, Italy, and his Dr.Sc. degree in 2016, from the University of Oulu, Oulu, Finland. Dr. Soderi has more than fifteen years' experience in embedded systems and safety-related architectures. His skills range from cybersecurity and electromagnetic compatibility to software engineering. During 2010–2014 he was a member of the Steering Committee of a joint-research project between General Electric (GE), Florence, Italy and the Centre for Wireless Communications, University of Oulu, Finland. During 2011–2015 he contributed in ETSI for ultra-wideband (UWB) devices in road and rail vehicles. After, the Doctoral degree he was appointed as Italy Cybersecurity Manager at Alstom, Florence, Italy. Currently, he is an Independent Cybersecurity Researcher and Certified Professional Ethical Hacker (CPEH), while he continues to work for Alstom as System Designer. His research topics include cybersecurity for critical infrastructure systems, side-channel attacks, physical layer security, electromagnetic emissions security, and UWB. He has been TPC member of several conferences and served as a reviewer of IEEE Transaction on Intelligent Transport Systems (ITS). Dr. Soderi published Journal and Conference papers and, chapters in book. He holds five patents regarding wireless communications and positioning.