On Characterizing and Measuring Out-of-Band Covert Channels

Brent Carrara and Carlisle Adams
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Ontario, Canada
bcarr092@uottawa.ca, cadams@uottawa.ca

ABSTRACT

A methodology for characterizing and measuring out-of-band covert channels (OOB-CCs) is proposed and used to evaluate covert-acoustic channels (i.e., covert channels established using speakers and microphones). OOB-CCs are low-probability of detection/low-probability of interception channels established using commodity devices that are not traditionally used for communication (e.g., speaker and microphone, display and FM radio, etc.). To date, OOB-CCs have been declared "covert" if the signals used to establish these channels could not be perceived by a human adversary. This work examines OOB-CCs from the perspective of a passive adversary and argues that a different methodology is required in order to effectively assess OOB-CCs.

Traditional communication systems are measured by their capacity and bit error rate; while important parameters, they do not capture the key measures of OOB-CCs: namely, the probability of an adversary detecting the channel and the amount of data that two covertly communicating parties can exchange without being detected. As a result, the adoption of the measure *steganographic capacity* is proposed and used to measure the amount of data (in bits) that can be transferred through an OOB-CC before a passive adversary's probability of detecting the channel reaches a given threshold. The theoretical steganographic capacity for discrete memoryless channels as well as additive white Gaussian noise channels is calculated in this paper and a case study is performed to measure the steganographic capacity of OOB covert-acoustic channels, when a passive adversary uses an energy detector to detect the covert communication. The case study reveals the conditions under which the covertly communicating parties can achieve *perfect steganography* (i.e., conditions under which data can be communicated without risk of detection).

Categories and Subject Descriptors

C.2.0 [**General**]: Security and Protection; D.4.6 [**Security and Protection**]: Invasive Software

IH&MMSec'15 June 17 - 19, 2015, Portland, OR, USA
ACM ISBN 978-1-4503-3587-4/15/06$15.00
DOI: http://dx.doi.org/10.1145/2756601.2756604

General Terms

Security, design

Keywords

Information hiding; covert channels; out-of-band covert channels; covert-acoustic channels; steganographic capacity; malware communication

1. INTRODUCTION

Formally, we define out-of-band covert channels (OOB-CCs) as a low-probability of intercept (LPI) / low-probability of detection (LPD) communication channel established between isolated processes (i.e., processes not able to communicate through traditional links) using existing commodity devices that are traditionally not used for communication. A literature review of the work on covert channels shows that OOB-CCs exist between a number of commodity device pairs: microphone and speaker [9, 17, 24, 25, 44], CPU and speaker [40, 50, 51], light source and ambient light sensor or camera [3, 4, 26, 36], speaker and accelerometer [26], vibration device and accelerometer [1, 17, 49], electromagnet and magnetometer [26], CPUs [43], as well as display and AM/FM radio [2, 23, 37]. OOB-CCs can be categorized as a separate class of covert channels as they differ from traditional network covert channels and steganographic channels because they do not require a cover protocol or object, respectively, to hide their communication within, i.e., where there is direct or indirect communication between the covertly communicating parties of network covert channels and steganographic channels, OOB-CCs establish a communication channel between parties that are not overtly communicating.

Additionally, OOB-CCs are relevant to a number of different contexts. Firstly, they could be used for malware communication between systems that are physically separated or isolated from one another, i.e., air-gapped systems [9,23,24,37]. Similarly, they could be used for malware communication between processes of secure operating systems that employ domain separation, i.e., "security by isolation" [17]. We also assume that OOB-CCs could be used for communication between entities not willing or allowed to use traditional communication links. These are common problems in applications supporting the expression of free speech in oppressive environments and during times of protest when traditional communication links are taken down, in whistleblower scenarios where sensitive information needs to be exfiltrated, and, in general, when the fact that communication is taking place needs to be kept hidden from detection by a third-party (e.g., governments, criminals, etc.). More generally, covert channels have also been discussed in the context of authentication [54]. Two parties that agree on both a medium and modulation scheme can use knowledge of the covert channel to authenticate each other. This type of authentication, however, is based on "security through obscurity" and is generally not recommended in direct application without some reliance on secret information [34]. Lastly, covert channels can be used to augment traditional communication links [54]. In general, we postulate that OOB-CCs provide a more deniable covert communication alternative to dedicated LPI/LPD communication systems since no additional hardware is required to establish communication.

OOB-CCs differ from both traditional and LPI/LPD communication systems in a number of different ways. Primarily, OOB-CCs are not necessarily concerned with general purpose communication. Often the main requirement of an OOB-CC, is to share a limited amount of high-value data (e.g., a password, an encryption key, or keystrokes in the case of malware, or a sensitive document in the whistle-blower scenario) and therefore their designers are concerned with the amount of data that can be transmitted before the channel is detectable by a passive adversary. Furthermore, OOB-CCs are constrained by the devices that are used for communication. Often the requirements for general-purpose communication in LPD systems call for communication at low signal-to-noise ratio (SNR) (e.g., below 0 dB), which might not be possible given that the commodity devices used in OOB-CCs were not designed for LPD communication and thus lack the necessary sensitivity to detect low SNR signals. Additionally, while the metrics used to measure traditional communication systems (e.g., data rate and bit error rate) and LPI/LPD communication systems (e.g., probability of detection) are useful measures for their respective systems, a more comprehensive metric is required for OOB-CCs that combines both their effectiveness (i.e., data rate) and efficiency (i.e., covertness) in order to characterize the covert channel. We point out, however, that despite the differences between OOB-CCs and general LPD communications systems, our analysis in this work from a passive adversary's perspective is similar to that of the analysis of LPD systems. We thus lean on the analysis of LPD communication systems in order to establish a framework for characterizing OOB-CCs.

The requirement for a measure to characterize OOB-CCs has led us to the *steganographic capacity* metric, which, in the context of steganography, is the largest payload which can be safely embedded in a cover object using a particular embedding method [33]. Previous researchers have measured the capacity of a number of steganographic systems and have empirically demonstrated or mathematically proven that their capacity is governed by a "square root law" (i.e., the maximum size of the embedded payload is proportional to the square root of the size of the cover) [20, 29, 30, 33]. Moreover, results in the low-probability of detection research community have also demonstrated a similar "square root law" governing their systems' capacity [5–7, 11–14, 27]. In both of these information hiding applications, the "square root law" demonstrates that the maximum amount of data that can be transmitted without detection is proportional to the square root of the size of the cover object or the number of channel uses, in the case of steganographic channels and low-probability of detection radar systems, respectively. Furthermore, the traditional rate used to measure communication systems is ineffective as the "rate" for information hiding systems tends to zero. Given these previous results, we measure the performance of the OOB-CCs studied in this work by calculating their *steganographic capacity.*

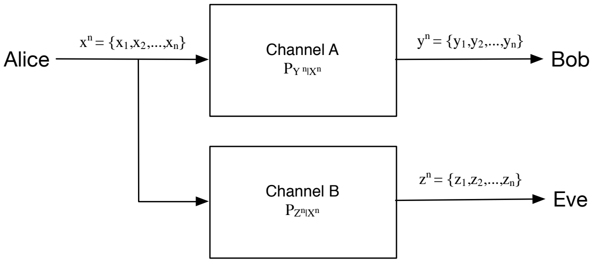
Alice
$x^n = \{x_1,x_2,...,x_n\}$
Channel A
$P_{Y^n|X^n}$
$y^n = \{y_1,y_2,...,y_n\}$
Bob
Channel B
$P_{Z^n|X^n}$
$z^n = \{z_1,z_2,...,z_n\}$
Eve

Figure 1: Our system model. Alice transmits a sequence of codewords $x^n = \{x_1, x_2, \ldots, x_n\} \in X^n$, $X^n \sim P_{X^n}$ through *Channel A* to Bob. Bob receives a sequence of codewords $y^n = \{y_1, y_2, \ldots, y_n\} \in Y^n$, $Y^n \sim P_{Y^n}$ where the sequence y^n is a possibly corrupted version of x^n and the distribution of Y^n is dependent on the channel transition probability distribution $P_{Y^n|X^n}$. Eve also receives a sequence of codewords $z^n = \{z_1, z_2, \ldots, z_n\} \in Z^n$, $Z^n \sim P_{Z^n}$ through *Channel B* where again the sequence z^n is a possibly corrupted version of x^n and Eve's distribution of codewords is dependent on $P_{Z^n|X^n}$. Once Eve observes z^n, she makes a decision and concludes whether or not Alice is communicating.

We measure the steganographic capacity of OOB-CCs, which we informally define as the maximum amount of data that can be communicated covertly before an adversary's probability of detection reaches a given threshold. We calculate the capacity by combining the communication rate achieved by two covertly communicating parties, Alice and Bob, and the probability of detection by an eavesdropper, Eve. Our analysis focusses on the passive adversary model shown in **Figure 1**. In our analysis, we assume that Eve is a passive adversary who is capable of monitoring the shared medium between Alice and Bob and is interested in answering the question: *is Alice communicating?* Previous research into OOB-CCs ([9, 17, 24, 25, 44]) has assumed that Eve is an unaware and unassuming adversary and an OOB-CC was deemed "covert" if the channel established between Alice and Bob was imperceptible to Eve's natural senses (e.g., sight, hearing). To evaluate the effectiveness of OOB-CCs in the presence of a passive adversary we make the reasonable assumption that Eve is able to deploy technical solutions to detect if Alice and Bob are communicating. We emphasize that this work deals with **detection** by a passive adversary and leaves the discussion of interception of Alice's codewords to later work. In this work, Alice is concerned with concealing the presence of her communication and not necessarily the confidentiality of the messages that she is sending. While confidentiality is an important requirement for secure communication systems, it is not the focus of this work.

As a result of our research, we make the following contributions to the covert channel literature. Using information theory and statistical hypothesis testing we determine the steganographic capacity of OOB-CCs when the channels between Alice and Bob as well as Alice and Eve are discrete memoryless channels (DMCs) (i.e., the input and output of the channel are modelled as discrete random variables and the output of the channel only depends on the current input). Moreover, we determine the steganographic capacity when both channels are corrupted by additive white Gaussian noise (AWGN) (i.e., the noise and information bearing signal are additive, the noise has constant power and the noise samples follow a Gaussian distribution), as well. Additionally, we perform a case study to measure the steganographic capacity of covert-acoustic channels (i.e., covert channels established using a speaker and microphone) when Eve deploys an energy detector to detect Alice's communications. Our case study allows us to determine the conditions under which Alice and Bob can communicate using *perfect steganography* (i.e., conditions under which data can be communicated without risk of detection) [8]. Lastly, we empirically determine the lowest SNR that commodity speakers and microphones can communicate at reliably in an effort to quantify the steganographic capacity of state-of-the-art covert-acoustic channels.

Our work impacts the evaluation of secure systems and has implications for the privacy-enhancing technologies community. Previously, the security risk associated with covert channels was measured by the bandwidth or channel capacity of the covert channel [38]. Both of these metrics on their own, however, do not adequately model the risk posed by covert channels that are only used to leak a fixed amount of data. In order to evaluate the security risk of these types of channels, a more comprehensive measure, i.e., steganographic capacity, is required. Furthermore, for the privacy-enhancing technologies community we show the conditions under which covert-acoustic OOB-CCs can be undetectable or require a passive adversary to capture a large number of samples in order to detect the channel.

This paper is organized as follows. In **Section 2**, we outline the background research in measuring steganographic channels, low probability of detection channels, and covert channels. In **Section 3**, we frame Eve's probability of detection problem in the context of statistical hypothesis testing to show that, on their own, probability of detect and channel capacity are not adequate measurements for OOB-CCs. We also examine how to measure the steganographic capacity and in **Section 4** we perform a case study to evaluate the steganographic capacity when Eve uses an energy detector to detect Alice's covert-acoustic communications. Lastly, in **Section 5** and **Section 6** we provide future work and conclude, respectively.

2. BACKGROUND

In [48], Shannon described a general mathematical theory for "secrecy systems" and broadly classified systems into *concealment systems*, *privacy systems*, and *"true" secrecy systems*. Shannon defined *concealment systems* as systems that ensured communication was hidden from the enemy and *"true" secrecy systems* as systems that ensured messages were unreadable by the enemy. Although Shannon's work defined the concept of *concealment systems*, it was Wyner in [53] that looked at the ability for two communicating parties to reliably communicate over a DMC while limiting the ability of a passive adversary to decode the originally transmitted message after observing it through a second DMC, i.e., the *wire-tap channel*. In Wyner's analysis, the goal of the authentic transmitter was to not only maximize channel throughput but also to maximize the equivocation rate of the eavesdropper, i.e., the entropy of the original message conditioned on the message output from the wire-tap channel. Both Shannon and Wyner's works were groundbreaking and paved the way for the analysis that led to the development of LPI communication systems.

LPI/LPD systems have been the focus of military researchers for a number of years. Much of this focus has been on time and frequency spread spectrum modulation schemes, i.e., direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) [45,46], respectively. Spread spectrum systems are difficult to detect because their transmitted signal's average power is lowered by spreading the signal's energy out over a much larger bandwidth than is required by the original signal. General detection of spread spectrum signals is performed using a radiometer [52], which is an energy detection device that filters, squares and sums a received signal before comparing it to a pre-determined threshold. If the signal's energy is above the threshold then the detector deems that communication has taken place; if it is below the threshold, the detector deems no communication occurred. The detection threshold is tuned by the detector to limit the probability of false alarm (false positive), α, and the probability of missed detection (false negative), β. In [52], Urkowitz showed that an energy detector is optimal when detecting a signal and only the signal's bandwidth, W, is known.

Recently, there have been a number of works outlining the theoretical limits of low-probability of detection communication for various channel models: the AWGN channel [5–7], the wire-tap channel [27], and the binary symmetric channel (BSC) (i.e., communication model where a bit is transmitted and received correctly with probability $1 - p$ and received incorrectly with probability p) [11–14]. In [5] and [6], Bash, et al., proved the "square root law" for LPD signals transmitted over an AWGN channel, which demonstrated that at most $O(\sqrt{n})$ and $o(\sqrt{n})$ bits can be communicated between Alice and Bob in n channel uses while lower bounding the sum of error probabilities $\alpha + \beta \geq 1 - \epsilon$ for some arbitrary $\epsilon > 0$ observed by Eve, when Eve's noise power is known by Alice and when it is not, respectively. The proof of their theorem showed that Alice's average transmit power is inversely proportional to the number of channel uses, n, and thus as $n \to \infty$ Alice's required transmit power $\to 0$. For practical systems, however, Bob must receive a signal from Alice with non-zero signal power in order to reliably communicate. Furthermore, their proof required that Alice and Bob had a shared secret that was at least equal in length to that of the messages transmitted by Alice to ensure confidentiality. In [7], Bash, et al., extended their result and showed that if Alice only transmitted in a single n-symbol slot out of a possible $T(n)$ slots, Alice could increase the amount of information she can transmit to Bob by a factor of $\sqrt{T(n)}$ at the cost of an extra $\log T(n)$ bits of shared secret between them.

In [11,13] and [14], Che, et al., examined the ability for Alice and Bob to communicate over a BSC while ensuring their communication is undetectable, which the authors referred to as being *deniable*. In their analysis, Eve observed Alice's transmissions through a noisier communication channel than Bob, i.e., the wire-tap channel, and were able to prove a similar "square root law" under this assumption. The difference between Che, et al.'s result and Bash, et al.'s result (other than the channel model) is that no secret information is required to be shared between Alice and Bob prior to communication under the authors' assumptions. In [12], Che, et al., extended their result to the situation where the noise observed by Bob and Eve was not deterministically known, but rather probabilistically distributed over a range. Their research showed that a "square root law" could still be observed under these conditions with the caveat that Eve's channel noise was still larger than Bob's. In [27], Hou and Kramer defined an information-theoretic measure "effective secrecy", which combined a measure for confidentiality and undetectability (or *confusion* and *stealth*, respectively, as defined by the authors). Their model relied again on the wire-tap channel to obtain confidentiality and to prove that an achievable rate does exist that satisfies constraints on both the confusion and stealth components of "effective security." While an important theoretical result, the work of Che, et al. and Hou and Kramer assume the wire-tap model, which is not a practical general assumption.

Prior to the works of Bash, et al., and Che, et al., a "square root law" was observed in information hiding systems by Ker while analyzing the capacity of batch steganography [30]. Since this seminal work was first published, other steganographic systems have also been found to respect this same law, namely Markov chain covers [20] and covers composed of i.i.d. elements [31]. In [33], a number of other covers were also empirically shown to follow the same law as well, but required the sender and receiver to share a secret "embedding key" at least linear in length to the payload in order to communicate without being detected. Additionally, under slightly different assumptions (i.e., the sender was able to combine more than one embedding location to convey one bit of information), Ker was able to show that no "embedding key" was required [32]. While no universal theory proving the "square root law" exists in general, the law is composed of a "collection of theories for different mathematical models" [33]. Given this collection of theories, more recent work has focussed on finding the "root rate", which is the proportionality constant in the calculation of steganographic capacity (i.e., capacity $\approx r\sqrt{n}$, where r is the "root rate"). The proportionality constant, r, is equivalent to the Kullback-Leibler (KL) divergence between stego object and cover object, however, estimating the KL divergence is difficult and instead the *Fisher information* of a stego-system is used to measure the system's performance given its relationship to the KL divergence (i.e., the Fisher information is the first term in the Taylor expansion of the KL divergence) [18, 19, 28]. Moreover, in [18], Filler and Fridrich show that under certain conditions (i.e., mutually independent embedding operations) Fisher information is equivalent to KL divergence. In this work, the mathematical models we analyze (e.g., DMC and AWGN) allow us to calculate the KL divergence directly.

Historically, covert channels, in general, have been measured by estimates on the channel's bandwidth. The Trusted Computer System Evaluation Criteria (TCSEC) [38], developed by the United States Department of Defense (DoD) to certify secure systems, classified covert channels in this way and laid out certification requirements for handling covert channels based on bandwidth limits [22]. It was Moskowitz and Kang in [42] who pointed out that both bandwidth and channel capacity alone were not appropriate measures to use when evaluating covert channels because of the fact that for short messages the capacity of the channel goes to zero while data is still effectively communicated through the covert channel. This conclusion is further supported by the square root laws presented in this section. Under the "square root law," a non-zero amount of data can be communicated through the channel undetected, but the capacity of the channel tends to zero as n gets large. Based on the observations of Moskowitz and Kang and the collection of "square root laws," it is clear that a more effective methodology is required to evaluate OOB-CCs.

3. MEASURING AN OOB-CC

For the remainder of this work, we use uppercase letters, X, to denote random variables and lowercase letters, x, $x \in X$, to denote a realization of a random variable. A random variable has a probability mass function, P_X, and we use the notation $X \sim P_X$ to indicate that X is distributed according to the distribution P_X. We denote sequences of random variables with the notation $X^n = X_1, X_2, \ldots, X_n$ and if each X is independent and identically distributed (i.i.d.) we write $P_{X^n} = P_X^n$.

In this section, we present the steganographic capacity for OOB-CCs when the channel between Alice and Bob as well as Alice and Eve is modelled by a DMC and we calculate the capacity by modelling Eve's problem of detecting Alice's communications as a statistical hypothesis test. Furthermore, we present the steganographic capacity under assumptions that are consistent with a large number of communication systems (e.g., the channels are DMCs as well as the channel noise model is AWGN and Alice is under an average power constraint). We present these results before studying the steganographic capacity of covert-acoustic signals in **Section 4**, where we assume that a passive adversary employs an energy detector to detect the covert signals.

3.1 Information-Theoretic Capacity

In this section, we quote generously from the discussion on statistical hypothesis testing in [39] and the discussion on information theory and statistical hypothesis testing in [15]. Using statistical hypothesis testing, Eve, upon making a sequence of observations, $\{z^n | z^n \in Z^n\}$ (where z^n is shown in **Figure 1**), decides whether to either accept the null hypothesis, H_0 (i.e., conclude "Alice is not communicating"), or reject the null hypothesis (i.e., conclude "Alice is communicating"). Eve constructs the distributions P_{H_0} and P_{H_1} in such a way that when H_0 is true the sequence $z^n \sim P_{H_0}$ and when H_1 is true the sequence $z^n \sim P_{H_1}$. In order to make a decision, Eve performs a *log-likelihood ratio test* (LLRT) and decides whether to accept or reject the null hypothesis.

As a result of performing the LLRT, Eve can make one of two types of errors: rejecting the null hypothesis when it is true (*Type I* error) or accepting the null hypothesis when it is false (*Type II* error). These two classes of errors are commonly referred to as false positive, whose probability is denoted by α, and false negative, whose probability is denoted by β, respectively. By the Neyman-Pearson Theorem, the LLRT is optimal in the sense that for a given false positive, α^*, β is minimized.

A common performance measure for statistical hypothesis tests is the *sum of probability errors*, $\alpha + \beta$, which we use throughout this discussion to evaluate Eve's performance when attempting to detect Alice's communications. Given that falsely accepting the alternate hypothesis represents falsely accusing Alice of covert communication, Eve would like to fix the level of significance to an arbitrarily low value and therefore minimize β for a set value of α. Using **Theorem 13.1.1** from [39], the sum of probability errors can be expressed as

$$\alpha + \beta = 1 - TV(P_{H_0}, P_{H_1}), \tag{1}$$

where $TV(P_{H_0}, P_{H_1})$ is the *total variational distance* between P_{H_0} and P_{H_1} and is expressed as

$$TV(P_{H_0}, P_{H_1}) = \sum_{x \in \mathcal{X}} |P_{H_0}(x) - P_{H_1}(x)|, \tag{2}$$

where $\mathcal{X}$ is the set of all possible n-length sequences of observations that Eve can observe. Using **Lemma 11.6.1** in [15], we can bound $TV(P_{H_0}, P_{H_1})$ using the following inequality

$$\sqrt{2 \ln 2 D(P_{H_0} \| P_{H_1})} \geq TV(P_{H_0}, P_{H_1}), \tag{3}$$

where $D(P_{H_0}, P_{H_1})$ is the KL divergence and is defined as $D(P\|Q) = \sum_x P(x) \log \frac{P(x)}{Q(x)}$ for two probability distributions P and Q. Given **Equation 3**, Eve's sum of probability errors is lower bounded by $1 - \epsilon_1$, where

$$\epsilon_1 = \sqrt{2 \ln 2 D(P_{H_0} \| P_{H_1})}. \tag{4}$$

Based on these preliminaries, we present **Theorem 1**:

THEOREM 1. *If the channel between Alice and Bob as well as Alice and Eve are DMCs and Alice generates sequences of codewords $\{x^n | x^n \in X^n\}$ such that each $X_i \sim P_X$ in $X^n = \{X_1, X_2, \ldots, X_n\}$, $1 \leq i \leq n$, is i.i.d.. then Alice can transmit L bits of information to Bob while ensuring the upper bound on Eve's probability of detection is $1 - \epsilon_2$, for some arbitrary $\epsilon_2 \in (0, 1-\alpha)$, where L is*

$$L = \begin{cases} \infty & \text{if } D(Q_Z \| P_Z) = 0, C > 0 \\ n^*TC & \text{if } D(Q_Z \| P_Z) > 0, C > 0 \\ 0 & \text{if } C = 0 \end{cases}, \tag{5}$$

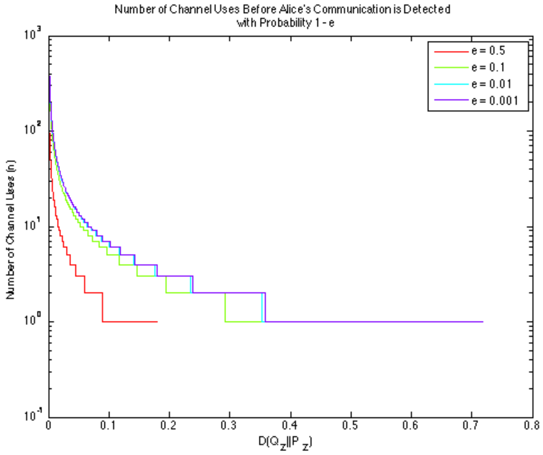

Figure 2: Plot of n versus $D(Q_Z \| P_Z)$ for various values of ϵ, where n is the number of channel uses that Alice can use to transmit data to Bob, while ensuring Eve's probability of detection, $P_D < 1 - \epsilon$ (*Note:* $n = 0$ *is not shown because the ordinate is plotted on a* log *scale*).

T is the duration of an observation, in seconds, C is the capacity of the channel between Alice and Bob, Q_Z is the probability distribution when Alice is not communicating, P_Z is the probability distribution when Alice is communicating and n^* is

$$n^* = \left\lfloor \frac{(1 - \alpha - \epsilon_2)^2}{2 \ln 2 D(Q_Z \| P_Z)} \right\rfloor \tag{6}$$

For a complete proof of **Theorem 1** see **Section 1** in [10].

Given **Theorem 1**, we take L to be the steganographic capacity and plot n^* versus $D(Q_Z \| P_Z)$ in **Figure 2**. From the plot in **Figure 2** and **Equation 6** it is clear that Alice's best strategy is to construct P_X such that P_Z matches Eve's model when Alice is not communicating, Q_Z, as closely as possible. Or, more formally,

$$\max_{P_X} C \tag{7}$$

$$\min_{P_X} D(Q_Z \| P_Z) \tag{8}$$

Conversely, Eve's strategy is to model the distributions when Alice is communicating and when she is not as closely as possible in order to maximize the distance, in the KL divergence sense, between P_Z and Q_Z.

3.2 Capacity for AWGN Channels

We now study the steganographic capacity assuming AWGN channel corruption for both *Channel A* and *Channel B* (shown in **Figure 1**) with noise variances, σ_B^2 and σ_E^2, respectively. Under the AWGN noise assumption, Eve's channel model when Alice is not transmitting can be expressed as $Z_1 =$

W_E, where $W_E \sim \mathcal{N}(0, \sigma_E^2)$. From [15], we know that when Alice's average transmit power is subject to an average power constraint (shown in **Equation 9**), Alice and Bob's channel capacity is maximized by distributing $X \sim \mathcal{N}(0, P_t)$, which can be achieved by Alice using random coding (e.g., encrypting the data stream, compressing the data stream).

$$\frac{1}{m}\sum_{i=1}^{m} x_i^2 = P_t \tag{9}$$

Assuming Alice generates symbols with a normal distribution and variance P_t, Eve's observation of the channel is $Z_2 = X + W_E$, $Z_2 \sim (0, \alpha_E^2 P_t + \sigma_E^2)$, where α_E is Eve's attenuation factor. Similarly, Bob's observation of the channel is $Y = X + W_B$, where $W_B \sim \mathcal{N}(0, \sigma_B^2)$ and $Y \sim \mathcal{N}(0, \alpha_B^2 P_t + \sigma_B^2)$, where α_B is Bob's attenuation factor. Eve's expected distributions, Q_Z and P_Z, are, therefore $\mathcal{N}(0, \sigma_E^2)$ and $\mathcal{N}(0, \alpha_E^2 P_t + \sigma_E^2)$ to model when Alice is communicating and when she is not, respectively.

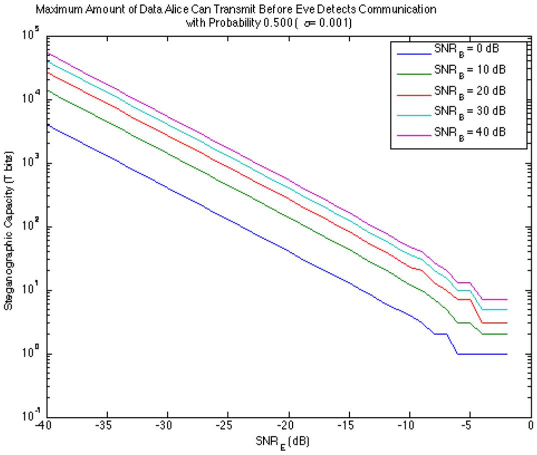

Figure 3: The steganographic capacity for the AWGN channel model is shown for a fixed false alarm rate, $\alpha = 0.001$ and threshold value, ϵ_2, of 0.5.

Given these preliminaries, we present **Theorem 2**:

THEOREM 2. *If*

1. *the channel between Alice and Bob as well as Alice and Ever are DMCs,*
2. *both channels are corrupted by AWGN with distributions $\mathcal{N}(0, \sigma_B^2)$ and $\mathcal{N}(0, \sigma_E^2)$, respectively,*
3. *Alice transmits symbols i.i.d. with distribution $\mathcal{N}(0, P_t)$,*
4. *and Alice is subject to the average power constraint shown in **Equation 9**, then*

Alice can transmit L bits of information to Bob while ensuring the upper bound on Eve's probability of detection is $1 - \epsilon_2$, for some arbitrary $\epsilon_2 \in (0, 1 - \alpha)$, where L is

$$L = \begin{cases} \infty & \text{if } D(Q_Z \| P_Z) = 0, C > 0 \\ n^* TC & \text{if } D(Q_Z \| P_Z) > 0, C > 0 \\ 0 & \text{if } C = 0 \end{cases},$$

T is the duration of an observation, in seconds, C is the capacity of the channel between Alice and Bob, Q_Z is the probability distribution when Alice is not communicating, P_Z is the probability distribution when Alice is communicating, n^* is

$$n^* = \left\lfloor \frac{(1 - \alpha - \epsilon_2)^2}{2 \ln 2 D(Q_Z \| P_Z)} \right\rfloor,$$

and $D(Q_Z \| P_Z)$ is

$$\frac{1}{2}\log\left(1 + \frac{\alpha_E^2 P_t}{\sigma_E^2}\right) + \frac{1}{2}\left(\frac{1}{1 + \frac{\alpha_E^2 P_t}{\sigma_E^2}} - 1\right).$$

For a complete proof of **Theorem 2** see **Section 2** in [10].

Denoting $\text{SNR}_E = \frac{\alpha_E^2 P_t}{\sigma_E^2}$ and $\text{SNR}_B = \frac{\alpha_B^2 P_t}{\sigma_B^2}$ for Eve and Bob's power signal-to-noise ratio, respectively, we plot the steganographic capacity versus SNR_E for various values of SNR_B in **Figure 3**. In the figure, the channel capacity between Alice and Bob is $C = \frac{1}{2}\log(1 + \text{SNR}_B)$ [15]. We show steganographic capacity curves for the case where $\epsilon_2 = 0.5$ to show the amount of data that Alice can transmit to Bob before Eve has a better than guessing chance of detecting her communication. The steganographic capacity plotted in **Figure 3** represents the absolute best case scenario for Eve since she knows the exact distribution of Alice's symbols and performs an optimal Neyman-Pearson test to detect Alice's communications for a fixed probability of false alarm. Conversely, this plot shows the worst case scenario for Alice; however, it is clear that Alice's strategy is to ensure that as little signal power, P_t, as possible gets to Eve in order to minimize her level of detection. Although this plot does paint a bleak picture for Alice (her capacity is at most 1 kilobyte at $\text{SNR}_E = -20$ dB) it makes generous assumptions about Eve's capabilities. As we will see in **Section 4**, Alice is able to communicate more data covertly when a simple energy detector is used for detection.

4. CASE STUDY

In [9, 17, 24, 25], and [44], various researchers showed covert-acoustic signals could be sent in the near ultrasonic, i.e., 17-20 kHz, and ultrasonic, i.e., > 20 kHz, ranges using commodity hardware from various vendors. In their respective works, the researchers used various modulation schemes (e.g., frequency-shift keying (FSK), orthogonal frequency-division multiplexing (OFDM)) to show that bit rates of over 100 bits per second (bps) could be achieved with low bit error rates (BERs). In all of these referenced works, the researchers assumed their adversary was unaware and unassuming and used only their natural ability to hear in order to detect the covert-audio communication. In this section, we evaluate the covertness of the scheme that was proposed in [9], which demonstrated that by using the OFDM modulation scheme, acoustic signals in the ultrasonic frequency range between 20 kHz and 20.5 kHz could be covertly communicated at data rates over 200 bps with a BER below 10%. Specifically, we calculate the steganographic capacity for covert-acoustic channels when Eve employs a radiometer, i.e., an energy detector. We build on the work in [9] because the researchers achieved the best results from a data throughput perspective when using truly ultrasonic ($>$ 20 kHz) signals, and by determining the steganographic capacity of their scheme we can set limits on how much data can be covertly communicated using ultrasonic audio signals when OFDM is used.

4.1 Acoustic Channel Model

Before proceeding with our analysis, we justify the application of the results from **Section 3** to the acoustic channel. In general, acoustic signals are corrupted by pink noise (i.e., the interfering noise power is inversely proportional to frequency) as opposed to white noise (i.e., the interfering noise power is spectrally flat for all frequencies) over the bandwidth supported by commodity microphones (i.e., 0 Hz to 22.050 kHz) [9, 21]. Furthermore, the source of noise in the acoustic spectrum is a combination of environmental noise (e.g., background conversations, electronic equipment) and imperfections in the receiver's audio equipment (i.e., microphone). The noise power, however, over the 20 kHz to 20.5 kHz bandwidth can be characterized as white noise, which we confirmed by performing a Kolmogorov-Smirnov test at a significance level of 0.001 [41].

Moreover, acoustic signals can suffer significant multi-path delay spreads (i.e., the receiver can continue to receive copies of a transmitted signal long after the signal is initially received) due to reflections of the transmitted signal off of objects in the environment. Carrara and Adams measured the multi-path delay spread for a common single desk closed-door office environment at upwards of 250 ms [9]. Therefore, if a transmitter sends signals with an inter-symbol time less than the multi-path delay spread of the channel, the channel cannot be considered a DMC as the receiver would receive a copy of the previously transmitted signal plus the currently transmitted symbol. However, if the multi-path delay spread is respected by the transmitter (often referred to as the transmitter inserting a "guard interval") the receiver would receive a copy of the transmitted symbol independent of the previously transmitted symbol. Under these circumstances the acoustic channel can be considered a DMC.

Lastly, one major factor to account for when dealing with acoustic signals is the attenuation of audio signals in air, especially if they contain high frequency components. The attenuation factor for acoustic signals depends on a number of elements: frequency of the transmitted signal, temperature of the air, relative humidity in the air, obstacles in the environment and distance between the sender and receiver [16, 35]. As an example, the attenuation rate of audio signals is roughly $0.5\frac{\text{dB}}{\text{m}}$, when the relative humidity in the air is 50 % and the ambient temperature is 20 ° C. The environmental factors and the distance between both Bob and Alice as well as Alice and Eve could have significant impact on SNR_E and SNR_B. We thus study the effect of distance on attenuation and the steganographic capacity at the end of this section.

Given our measurement of the noise in the 500 Hz bandwidth between 20 kHz and 20.5 kHz, the effect of attenuation on acoustic signals, and the characterization of the acoustic channel being modelled by a DMC, we proceed with applying the results of the previous section to covert-acoustic signals in our case study.

4.2 Analysis

In **Section 3.2**, we showed that for the AWGN channel model, the steganographic capacity of the channel is zero when $\text{SNR}_E \geq 0$ dB. As previously noted, this represents the best-case scenario for Eve and thus a lower bound on the steganographic capacity as Eve knows the exact statistical distribution both when Alice is communicating and when she is not and constructs an optimal test based on this information. In this section, we complement our previous result and evaluate the steganographic capacity in the best-case scenario for Alice when Alice is band-limited and Eve is attempting to passively detect her communications. In our analysis, we assume that Eve only knows the bandwidth of Alice's signal, W, and thus builds an optimal device based on simply knowledge of W and the fact that the channel model is AWGN.

Previous researchers, [52], have shown that the optimal device to detect signals in AWGN when only the signal's bandwidth is known is an energy detector. An energy detector is designed to distinguish between a received signal, $r(t)$, composed of either simply noise, i.e., $r(t) = n(t)$, or a signal plus noise, i.e., $r(t) = s(t) + n(t)$, and works as follows. First, the received signal, $r(t)$, is passed through a bandpass filter whose bandwidth matches the bandwidth of the signal being detected, $s(t)$. Once filtered, the signal is squared and integrated and the output is compared to a threshold, K. If the output of the integrator is above the detector's threshold it is concluded that the received signal contains $s(t)$, otherwise it is concluded that the received signal just contains noise, $n(t)$. The distribution at the output of the integrator when only $n(t)$ is received can be modelled by a central chi-squared distribution with $\eta = 2TW$ degrees of freedom, where T is the integrator's evaluation time, in seconds [45]. Moreover, when $s(t) + n(t)$ is received, the output from the integrator can be modelled by a non-central chi-squared distribution with $\eta = 2TW$ degrees of freedom and a non-centrality parameter, $\lambda = \frac{\eta \text{SNR}_E}{W}$, where $\text{SNR}_E = \frac{\alpha_E^2 P_t}{\sigma_E^2}$ represents the power SNR of the signal received by Eve [45].

When using a radiometer, a false alarm is raised if the output of the integrator, k, is above the threshold K, but the signal $s(t)$ was not present. Similarly, a missed detection error occurs when the output of the integrator, k, is below the threshold, K, but the signal $s(t)$ was present. The false alarm probability, α, is shown in **Equation 11** and the missed detection probability, β, is shown in **Equation**

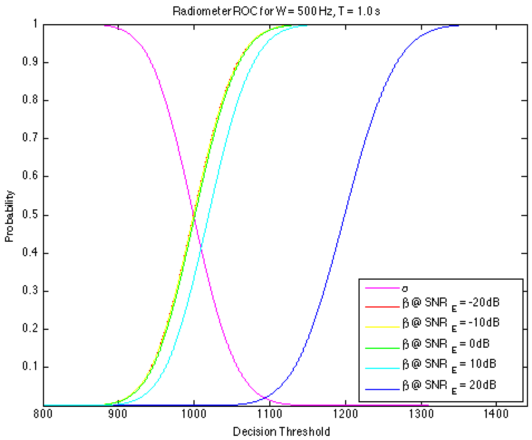

Figure 4: The receiver operating characteristics (ROC) for Eve's energy detector. We plot the probability of missed detection, β, for various values of SNR$_E$.

13, where $P_{\mathcal{X}^2_\eta}$ represents a central chi-squared distribution with η degrees of freedom and $P_{\mathcal{X}^2_{\eta,\lambda}}$ represents a non-central chi-squared distribution with η degrees of freedom and a non-centrality parameter, λ.

$$\begin{aligned}
\alpha &= Pr[k > K | s(t) \text{ not present}] && (10)\\
&= \int_K^\infty P_{\mathcal{X}^2_\eta}(x)dx && (11)\\
\beta &= Pr[k < K | s(t) \text{ present }] && (12)\\
&= \int_{-\infty}^K P_{\mathcal{X}^2_{\eta,\lambda}}(x)dx && (13)
\end{aligned}$$

We plot the receiver operating characteristics (ROC) for various values of SNR$_E$ in **Figure 4** and note that the equal error rate (EER) for the various β curves are 0.50, 0.50, 0.49, 0.41, and 0.02 for SNR$_E$ = -20 dB, -10 dB, 0 dB, 10 dB and 20 dB, respectively; thus as SNR$_E \to -\infty$, $\alpha + \beta \to 1$, and, therefore, Alice can communicate without being reliably detected, i.e., Alice has achieved *perfect steganography*. (*Note that we use the term perfect steganography when $\alpha + \beta = 1$ even though the original definition of perfect steganography was related to the condition that the KL divergence between stego object and covert object is zero [8]. A proof showing that if $\alpha + \beta = 1$, then perfect steganography is achieved is in **Section 3** of [10], which justifies our use of the term in this fashion*).

Given the energy detector's construction, in each observation Eve detects if Alice is communicating with probability $p = 1 - \beta$. The tradeoff between α and p is shown in **Figure 5**. This plot empirically confirms that as SNR$_E \to -\infty$, $p \to \alpha$ and thus $\alpha + \beta \to 1$. Similar to the analysis in the previous section, we assume that Eve performs multiple observations to increase her overall probability of detecting Alice's communications. From Alice's perspective, we assume she transmits data in intervals with a duration of T seconds

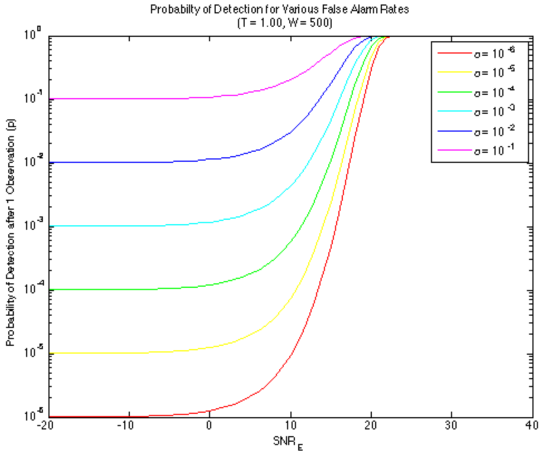

Figure 5: Plot of the single channel use probability of detection, p, versus SNR$_E$ for various false alarm rates α.

and that she wants to maximize the amount of data she can transmit to Bob. Furthermore, we point out that the value, T, is completely within Alice's control and we assume that Alice separates the intervals she transmits in with intervals of silence. Otherwise, Eve could use an integrator observation time greater than T (we analyze the effect of varying T at the end of this section). Given that Eve detects Alice's communications with probability p in each observation, we model the number of trials that Eve must perform before detecting Alice's communications for the first time using the geometric random variable, M, with parameter p and probability mass function $Pr[M = m] = (1-p)^{m-1}p$. The probability that Eve detects Alice's communications at least once after m observations is then $1-(1-p)^m$, i.e., one minus the probability of the event that Eve doesn't detect Alice's communications in any of the m observations. If we again define n^* to be the maximum number of observations such that Eve's upper bound on P_D is $1 - \epsilon$ for some arbitrary $\epsilon \in (0, 1 - \alpha)$ we get

$$\begin{aligned}
1 - (1-p)^{n^*} &= 1 - \epsilon && (14)\\
(1-p)^{n^*} &= \epsilon && (15)\\
n^* &= \left\lfloor \frac{\log \epsilon}{\log(1-p)} \right\rfloor && (16)
\end{aligned}$$

where we take the floor because we want to upper bound Eve's P_D. The steganographic capacity is then $L = n^*CT$, where T is the integrator's evaluation time, n^* is shown in **Equation 16** and C is the channel capacity of the channel between Alice and Bob and can be expressed as

$$C = W \log\left(1 + \frac{\alpha_B^2 P_t}{\sigma_B^2 W}\right) \frac{\text{bits}}{\text{second}}. \qquad (17)$$

In order to determine Eve's threshold, K, she first chooses an acceptable level for the false alarm rate, α^*, then solves

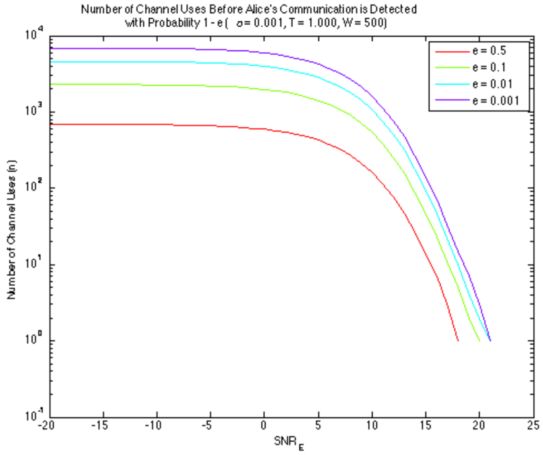

Figure 6: Plot of n versus SNR$_E$ for various values of ϵ. Eve determines her threshold value, K, based on the level of false alarm, $\alpha = 0.001$.

Equation 11 for K. Once the value for K is obtained, Eve's per-observation probability of detection, p, is calculated by applying **Equation 13** and subtracting the result from one. This procedure is the application of the Neyman Pearson criterion for detection [45]. We plot various curves for different values of ϵ to determine the maximum number of channel uses, n^*, that Alice can transmit on while upper bounding Eve's probability of detection in **Figure 6**. We remark that below approximately SNR$_E$ = -10 dB, the number of channel uses that Alice can use to transmit data plateaus. This again reflects the situation where $\alpha + \beta \to 1$.

The steganographic capacity when Eve uses a radiometer to detect Alice's communications is shown in **Figure 7**. Comparing this plot to the plot shown in **Figure 3**, we note that Alice has the potential to send much more data when Eve employs an energy detector than she does when Eve employs an optimal detector even though Alice is bandlimited to $W = 500$ Hz. We show independent SNR values for SNR$_E$ and SNR$_B$ to model the different attenuation factors, α_B and α_E, for Bob and Eve, respectively. We also show the effects of modifying the integrator evaluation time T in **Figure 8**. In **Figure 8**, the probability that Eve detects Alice's communication after one observation, p, and the effects of Alice varying her transmit time T when Bob's SNR is held constant at SNR$_B$ = 10 dB is shown. We see that as Eve increases her observation time, she is able to detect Alice's communication in just one observation (hence Alice can send no data covertly) at lower and lower values for SNR$_E$. It is clearly in Alice's best interest, therefore, to restrict how long she transmits for in order to limit Eve's observation time. This can be seen by examining the effect of lowering T in **Figure 8**. For fixed SNR, as $T \to 0$, the sum of probability errors, $\alpha + \beta \to 1$.

We end our case study with an analysis of the attenuation factors α_E and α_B as well as the BER at Bob at low received SNR, SNR$_B$. The effect of lowering Bob's received SNR on the BER is shown in **Figure 9**. From the plot it is clear that for Bob to communicate at a SNR of 10 dB and below, a sig-

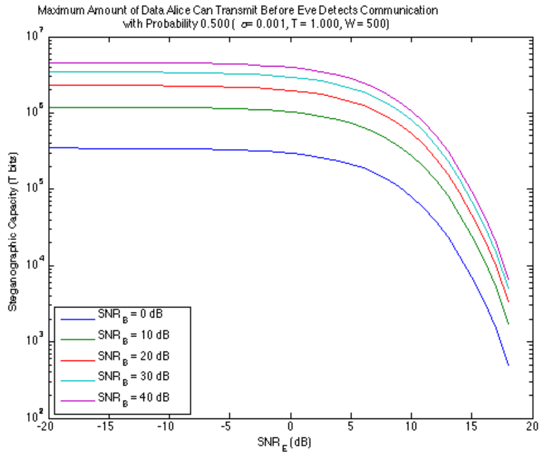

Figure 7: The steganographic capacity when Eve uses an energy detector to detect Alice's communication is shown for a fixed false alarm rate of 0.001 and a threshold value, ϵ, of 0.5.

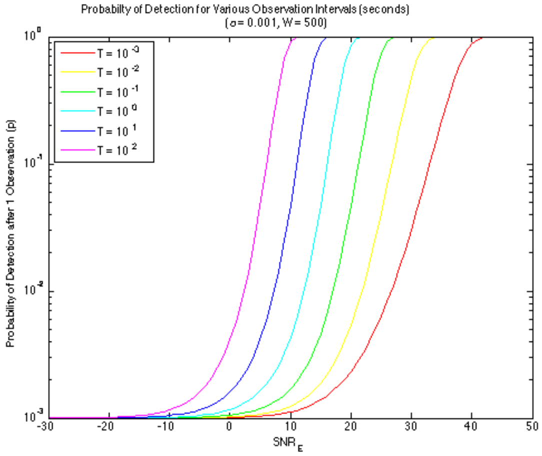

Figure 8: The tradeoff between the probability of detection, p, and the observation interval, T, is shown for a fixed probability of false alarm, α = 0.001. As T increases, p increases for a given SNR$_E$, however, as T decreases, the point where $\alpha = p$, i.e., $\alpha + \beta = 1$, for a given SNR$_E$, increases.

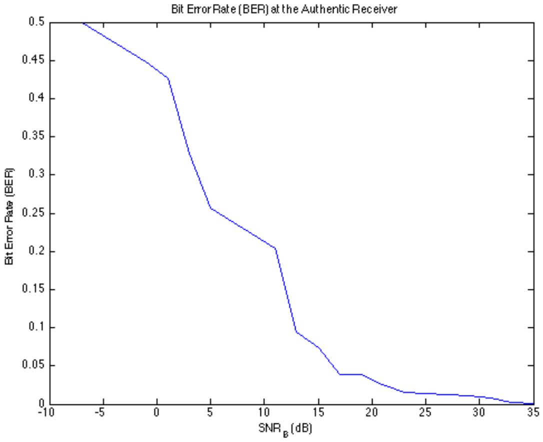

Figure 9: The effect of varying Bob's received SNR on the bit error rate is shown. Clearly, as Bob's received SNR drops below the noise threshold (i.e., ≤ 0 dB) Bob cannot reliably decode Alice's transmissions when commodity hardware is used and symbols are transmitted using OFDM.

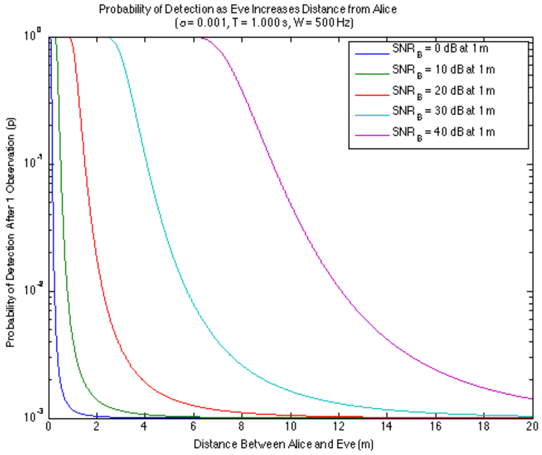

Figure 10: The relationship between Eve's probability of detection after one observation, p, is shown with respect to her distance from Alice. Multiple curves are shown, each of which correspond to a received SNR at Bob, SNR$_B$, at a distance of 1 m.

nificant number of errors need to be corrected. A plot of the probability of detection, p, versus distance is also shown in **Figure 10**. In the plot we show multiple curves corresponding to different received SNR values at Bob, SNR$_B$. For each curve, you can see the deleterious effect that distance has on Eve's probability of detection as her distance from Alice increases. This plot shows that if Alice can make assumptions about Eve's location and Alice knows Bob's location, then Alice has a better chance of approaching *perfect steganography*. Furthermore, given the physical properties of acoustic signals, it is clearly within Eve and Bob's best interest to be as close to Alice as possible when she is transmitting and within Alice's best interest to transmit signals to Bob at the lowest possible SNR value.

5. FUTURE WORK

To move this research forward, appropriate low SNR modulation and coding schemes need to be evaluated and the most error tolerant, high rate scheme needs to be implemented to increase the steganographic capacity between Alice and Bob while decreasing Bob's BER. The results presented in this work show that at an SNR$_B$ $= 5$ dB, an average BER of 0.25 can be expected when using commodity hardware and OFDM modulation. In order to reduce these error rates to acceptable levels, an $[n, k, d]$ forward error correcting code (where n is the block length, k is the message length, and d is the distance), capable of correcting $\lfloor \frac{d-1}{2} \rfloor$ random errors, such as $[n, k, n-k+1]$ Reed-Solomon Codes [47], would need to be used. To correct up to 25% bit errors using Reed-Solomon codes, an overheard of approximately 50% is required, thus reducing the effective bit rate by half.

From a detection perspective, more analysis is required to study the effects on the steganographic capacity when a detector is employed that takes more information into account than just the signal's bandwidth, W. While the energy detector we studied is optimal when only the signal's bandwidth is known, a motivated detector would try to employ a detection scheme that takes into account as much of the signal's information as possible to achieve the theoretical results we presented. A study where the detector, Eve, has knowledge of all the signal's properties except for some secret information that is shared between Alice and Bob, like we did in the analysis of AWGN, would be appropriate as a next step.

Furthermore, a study on the effects of the steganographic capacity when Eve is active is required to determine the effect of an active adversary. Certainly, if Eve has knowledge of the modulation scheme (e.g., OFDM) being used by Alice and Eve knows the bandwidth of Alice's signals, Eve can transmit noise on the same frequencies that Alice is using and jam Alice's signal, causing Bob's BER to increase. Lastly, now that the theoretical steganographic capacity has been calculated for DMCs when Alice transmits symbols i.i.d., as well as when the channel noise model is AWGN, research is required to study the steganographic capacity in other typical channel models (e.g., fading channel) that characterize OOB-CCs.

6. CONCLUSION

Previous researchers and certification bodies have relied on bandwidth and channel capacity to determine the security threat of covert channels. Our research shows that while these measures are useful, they do not evaluate how effective the channel is at communicating fixed amounts of data without being detected, nor do they capture the effect of the channel being monitored by a passive detector. We thus propose the adoption of the metric *steganographic capacity* to measure and characterize OOB-CCs. The steganographic capacity takes into account a passive detector and measures the maximum amount of data that can be transmitted through the covert channel while limiting a passive detector's ability to conclusively detect the channel by upper bounding its probability of detection.

By studying the theoretical steganographic capacity when the communication channel is a DMC, we showed that Alice, the transmitter, must maximize the channel capacity between her and her intended receiver, Bob, while minimizing Eve, the eavesdropper's, ability to calculate a difference between the probability distribution of symbols she detects when Alice is transmitting and when she is not. Furthermore, when the channel noise model is additive white Gaussian noise, we showed that the most important parameter in the system is Alice's transmit power, P_t. Lastly, we evaluated the ability for Eve to detect a covert-acoustic channel between Alice and Bob and determined that for Alice and Bob to maximize the data they can transmit between each other, Alice must send transmissions in short bursts and send signals to Bob at the lowest allowable SNR, while minimizing the SNR of the signal that Eve receives.

7. ACKNOWLEDGMENTS

Thanks are due to Dr. Rainer Böhme for advice and discussions as well as the anonymous reviewers of an earlier version of this paper for their suggestions.

8. REFERENCES

[1] A. Al-Haiqi, M. Ismail, and R. Nordin. A new sensors-based covert channel on Android. *The Scientific World Journal*, 2014, 2014.

[2] R. J. Anderson and M. G. Kuhn. Soft tempest–an opportunity for NATO. *Protecting NATO Information Systems in the 21st Century*, 1999.

[3] M. Backes, T. Chen, M. Duermuth, H. Lensch, and M. Welk. Tempest in a teapot: Compromising reflections revisited. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 315–327, May 2009.

[4] M. Backes, M. Durmuth, and D. Unruh. Compromising reflections-or-how to read LCD monitors around the corner. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 158–169, May 2008.

[5] B. Bash, D. Goeckel, and D. Towsley. Square root law for communication with low probability of detection on AWGN channels. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 448–452, July 2012.

[6] B. Bash, D. Goeckel, and D. Towsley. Limits of reliable communication with low probability of detection on AWGN channels. *Selected Areas in Communications, IEEE Journal on*, 31(9):1921–1930, September 2013.

[7] B. A. Bash, D. Goeckel, and D. Towsley. LPD communication when the warden does not know when. *CoRR*, abs/1403.1013, 2014.

[8] C. Cachin. An information-theoretic model for steganography. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 306–318. Springer Berlin Heidelberg, 1998.

[9] B. Carrara and C. Adams. On acoustic covert channels between air-gapped systems. In *Foundations and Practice of Security*, volume 8930 of *Lecture Notes in Computer Science*, pages 3–16. Springer, 2015.

[10] B. Carrara and C. Adams. Proofs for "On characterizing and measuring out-of-band covert channels". `http://www.site.uottawa.ca/~cadams/papers/Appendix.pdf`, 2015. Accessed: 2015-04-15.

[11] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi. Reliable, deniable and hidable communication. In *Information Theory and Applications Workshop (ITA), 2014*, pages 1–10, Feb 2014.

[12] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi. Reliable deniable communication with channel uncertainty. In *Information Theory Workshop (ITW), 2014 IEEE*, pages 30–34, Nov 2014.

[13] P. H. Che, M. Bakshi, and S. Jaggi. Reliable deniable communication: Hiding messages in noise. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2945–2949, July 2013.

[14] P. H. Che, M. Bakshi, and S. Jaggi. Reliable Deniable Communication: Hiding Messages in Noise. *ArXiv e-prints*, Apr. 2013.

[15] T. M. Cover and J. A. Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[16] M. J. Crocker. *Handbook of acoustics*. John Wiley & Sons, 1998.

[17] L. Deshotels. Inaudible sound as a covert channel in mobile devices. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, 2014.

[18] T. Filler and J. Fridrich. Complete characterization of perfectly secure stego-systems with mutually independent embedding operation. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pages 1429–1432, April 2009.

[19] T. Filler and J. Fridrich. Fisher information determines capacity of ε-secure steganography. In *Information Hiding*, Lecture Notes in Computer Science, pages 31–47. Springer Berlin Heidelberg, 2009.

[20] T. Filler, A. D. Ker, and J. Fridrich. The square root law of steganographic capacity for markov covers. In *Proc. SPIE*, volume 7254, pages 725408–725408–11, 2009.

[21] V. Gerasimov and W. Bender. Things that talk: using sound for device-to-device and device-to-human communication. *IBM Systems Journal*, 39(3.4):530–546, 2000.

[22] V. D. Gligor. *A guide to understanding covert channel analysis of trusted systems*. National Computer Security Center, 1994.

[23] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici. Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*, pages 58–67, Oct 2014.

[24] M. Hanspach and M. Goetz. On covert acoustical mesh networks in air. *CoRR*, abs/1406.1213, 2014.

[25] M. Hanspach and M. Goetz. Recent developments in covert acoustical communications. In *Sicherheit*, pages 243–254, 2014.

[26] R. Hasan, N. Saxena, T. Haleviz, S. Zawoad, and D. Rinehart. Sensing-enabled channels for hard-to-detect command and control of mobile devices. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 469–480, 2013.

[27] J. Hou and G. Kramer. Effective secrecy: Reliability, confusion and stealth. *CoRR*, abs/1311.1411, 2013.

[28] A. Ker. Estimating steganographic fisher information in real images. In *Information Hiding*, volume 5806 of *Lecture Notes in Computer Science*, pages 73–88. Springer Berlin Heidelberg, 2009.

[29] A. Ker. The square root law in stegosystems with imperfect information. In *Information Hiding*, volume 6387 of *Lecture Notes in Computer Science*, pages 145–160. Springer Berlin Heidelberg, 2010.

[30] A. D. Ker. A capacity result for batch steganography. *Signal Processing Letters, IEEE*, 14(8):525–528, 2007.

[31] A. D. Ker. The square root law requires a linear key. In *Proceedings of the 11th ACM Workshop on Multimedia and Security*, MM&Sec '09, pages 85–92. ACM, 2009.

[32] A. D. Ker. The square root law does not require a linear key. In *Proceedings of the 12th ACM Workshop on Multimedia and Security*, MM&Sec '10, pages 213–224. ACM, 2010.

[33] A. D. Ker, T. Pevný, J. Kodovský, and J. Fridrich. The square root law of steganographic capacity. In *Proceedings of the 10th ACM Workshop on Multimedia and Security*, pages 107–116, 2008.

[34] A. Kerckhoffs. *La cryptographie militaire*, volume 9. 1 1883.

[35] L. E. Kinsler, A. R. Frey, A. B. Coppens, and J. V. Sanders. Fundamentals of acoustics. *Fundamentals of Acoustics, 4th Edition, by Lawrence E. Kinsler, Austin R. Frey, Alan B. Coppens, James V. Sanders, pp. 560. ISBN 0-471-84789-5. Wiley-VCH, December 1999.*, 1, 1999.

[36] M. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pages 3–18, 2002.

[37] M. Kuhn and R. Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 124–142, 1998.

[38] D. C. Latham. Department of Defense trusted computer system evaluation criteria. *Department of Defense*, 1986.

[39] E. L. Lehmann and J. P. Romano. *Testing statistical hypotheses*. Springer, 2006.

[40] M. LeMay and J. Tan. Acoustic surveillance of physically unmodified PCs. In *Security and Management*, pages 328–334, 2006.

[41] F. J. Massey. The Kolmogorov-Smirnov test for goodness of fit. *Journal of the American Statistical Association*, 46(253):68–78, 1951.

[42] I. S. Moskowitz and M. H. Kang. Covert channels-here to stay? In *Computer Assurance, 1994. COMPASS'94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Proceedings of the Ninth Annual Conference on*, pages 235–243. IEEE, 1994.

[43] S. J. Murdoch. Hot or not: Revealing hidden services by their clock skew. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 27–36, 2006.

[44] S. J. O'Malley and K.-K. R. Choo. Bridging the air gap: Inaudible data exfiltration by insiders. In *20th Americas Conference on Information Systems (AMCIS 2014)*, 2014.

[45] R. L. Peterson, R. E. Ziemer, and D. E. Borth. *Introduction to spread-spectrum communications*, volume 995. Prentice Hall New Jersey, 1995.

[46] J. G. Proakis. *Digital communications*. McGraw-Hill, New York, 2008.

[47] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial & Applied Mathematics*, 8(2):300–304, 1960.

[48] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[49] V. Subramanian, S. Uluagac, H. Cam, and R. Beyah. Examining the characteristics and implications of sensor side channels. In *Communications (ICC), 2013 IEEE International Conference on*, pages 2205–2210, June 2013.

[50] E. Tromer. Acoustic cryptanalysis: on nosy people and noisy machines. *Eurocrypt2004 Rump Session, May*, 2004.

[51] E. Tromer. Hardware-based cryptanalysis. *Weizmann Institute of Science, Tese de Doutorado*, 2007.

[52] H. Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4):523–531, April 1967.

[53] A. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8):1355–1387, Oct 1975.

[54] S. Zander, G. J. Armitage, and P. Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys and Tutorials*, 9(1-4):44–57, 2007.