Covert Communications on Continuous-Time Channels in the Presence of Jamming

Tamara V. Sobers‡, Boulat A. Bash†, Saikat Guha⊥, Don Towsley‡, Dennis Goeckel∗
‡The MITRE Corporation, Bedford, MA 01730
†Raytheon BBN Technologies, Cambridge, MA 02138
⊥The Univ. of Arizona, College of Optical Sciences, Tucson, AZ 85721
‡College of Info. and Comp. Sciences (CICS), Univ. of Massachusetts Amherst, Amherst, MA 01003
∗Dept. of Elec. and Comp. Engineering (ECE), Univ. of Massachusetts Amherst, Amherst, MA 01003

Abstract—Covert communication is achieved if the transmitter (Alice) sends messages to a legitimate receiver (Bob) without detection by an attentive warden (Willie). Recently, there has been significant work on establishing the limits of such covert communication, including our work demonstrating that a cooperative jammer can greatly improve the throughput of covert communication systems. However, this previous work has considered a discrete-time model, with the implicit implication that the results will be similar on the true continuous-time model of the physical channel. In this paper, we consider covert communication over the continuous-time channel model to understand the throughput scaling for large blocklengths. For the Alice-Bob-Willie scenario, the results from the discrete-time channel generally follow. However, when a jammer is added to the environment, we demonstrate that timing offsets between Alice’s signal and that of the jammer allow for the application of co-channel interference mitigation techniques at Willie’s detector, which call into question whether our previous results suggesting an improvement in the covert throughput with the help of the jammer will be obtained in practice. Finally, we consider initial approaches to thwart such a detector and achieve improved throughput scaling in the presence of the jammer.

I. INTRODUCTION

Security and privacy in wireless communication networks are topics of great research and societal interest. Most security research focuses on preventing an adversary from deciphering the content of a message, and hence the message content is encrypted. However, there are applications where keeping an adversary from even knowing that a transmission is taking place is critical. For example, wireless communications activity has often been used as a proxy for military activity [1], or an oppressive government might shut down any communication between certain parties, particularly if it is encrypted. Hence, the study of covert communications, where even the presence of the message is hidden from an adversary, is well motivated.

The limits of covert communication have been a topic of recent research interest. In the basic model, covert communications occurs if a transmitter, Alice, can reliably transmit messages to a legitimate receiver, Bob, without a watchful adversary, warden Willie, detecting her communications. The original work by Bash et al. in [2] demonstrates the square-root law (SRL): Alice can transmit $O(\sqrt{n})$ covert bits (and no more than $O(\sqrt{n})$ bits) in channel uses of a discrete-time channel with additive white Gaussian noise (AWGN) at both Bob and Willie. Successive work has considered in detail the discrete memoryless channel (DMC) and established the constants on the throughput for both the DMC and AWGN channels [3], [4]. Hence, the characterization of the Alice-Bob-Willie channel has proceeded rapidly for standard discrete-time channel models.

For the scenarios of most general interest, the aforementioned works largely establish the square-root law. However, recent work has shown that the SRL depends critically on assumptions made about adversary Willie. In particular, Lee and Baxley in [5], [6] demonstrate that if Willie’s channel estimation is such that he has uncertainty in his noise statistics and his receiver is restricted to a radiometer, then Alice can transmit $O(n)$ covert bits in $n$ channel uses. In contrast, work by Goeckel et al. [7] shows that if Willie’s channel estimator is instead not constrained, then under many conditions the covert throughput is not increased when Willie lacks knowledge of his noise statistics because these statistics can be readily estimated. To address such, Sobers et al. in [8], [9] prove that adding a jammer to the model can prevent such estimation and allow Alice to communicate $O(n)$ covert bits in $n$ channel uses without any assumption on Willie’s receiver. These results are obtained even when the jammer is uninformed in that it does not know at which time Alice might transmit. In the aforementioned results on the limits of covert communications, including [2], [5], [6], [8], [9], a discrete-time model is employed. However, as discussed in detail in Section IV-A below, this model only arises directly in the presence of the jammer in the unlikely event that Alice’s and the jammer’s transmissions have synchronous symbol boundaries at Willie’s receiver.

In this work, we consider covert communication based on a continuous-time model and consider the impact of potential
timing offsets between Alice and the jammer on the achievable covert throughput. Employing such timing offsets to separate users has been considered extensively in the mitigation of co-channel interference in narrowband systems (e.g. [10]). After presenting the system model in Section II, we briefly consider the extension of the results of [2], where the jammer is not present, to the continuous-time model in Section III. Then, in Section IV-A, we consider the natural continuous-time extension of the construction in [9] and demonstrate that Willie can exploit the timing offset between the signal of Alice and that of the jammer to restrict the covert throughput. Finally, we demonstrate in IV-C that, given ideal pulse shaping, there exists a construction that allows Alice to transmit $O(n)$ bits in $n$ channel uses against an optimal detector at Willie. Section V presents the conclusions.

II. SYSTEM MODEL AND METRICS

A. System Model

Consider the scenario presented in Fig. 1 where Alice would like to communicate as much information to Bob as possible per time interval of length $T$, $T \to \infty$, without warden Willie detecting her communications. A jammer is also present in the environment, and the jammer transmits his or her messages without any coordination with Alice. The jammer does not know if Alice transmits or at what time she does transmit if she chooses to do so. All channels are assumed to be additive white Gaussian noise (AWGN) channels with the appropriate pathloss based on the transmission distance.

Fig. 1: Scenario: Alice wishes to communicate information to Bob without detection by a capable and attentive adversary Willie. Also present in the environment is a friendly Jammer, who without knowledge of when Alice transmits (i.e. an “uninformed” jammer), seeks to aid with that transmission, as in [8], [9]. $d_{x,y}$ represents the distance from transmitter $x$ to receiver $y$, where $x$ is either Alice (“a”) or the jammer (“j”) and $y$ represents Willie (“w”) or Bob (“b”).

Here, we describe the natural continuous-time extension of the discrete-time system in [9] that achieves the transmission of $O(n)$ bits covertly and reliably in $n$ channel uses. Divide time into an infinite number of codeword “slots”, each of length $T$ seconds. If we assume, in analogy to [9], that the jammer uses a given average power in every slot of length $T$ and varies his power independently between slots, this allows us to focus on the single slot covering $t \in (0, T)$ to simplify the exposition. If Alice decides to transmit in this slot, she encodes her message into Gaussian symbols (see [2], [9]) and then scales the symbols by the square root of the power to form the transmitted sequence $f = \{f_1, f_2, \ldots, f_n\}$, which she transmits with the waveform:

$$x(t) = \sum_{k=1}^{n} f_k p(t - kT_b - \tau_a)$$  \hspace{1cm} (1)

where $E[|f_k|^2] = P_{max}$, $T_b$ is the symbol period, $P_{max}$ is her transmitted energy per symbol, $p(t)$ is a unit-energy square-root raised cosine (SRRC) pulse shape that results in zero intersymbol interference (ISI) after matched filtering at the receiver, and $\tau_a$ is the timing offset between Alice’s symbol boundary and a reference time zero at Willie’s receiver.

The jammer employs the same pulse shaping as Alice and, for $t \in (0, T)$, transmits $n$ independent and identically distributed (i.i.d.) Gaussian symbols $v = \{v_1, v_2, \ldots, v_n\}$ with average power $E[|v_k|^2] = P_{max}$. Hence, his signal is given by:

$$g(t) = \sum_{k=1}^{n} v_k p(t - kT_b - \tau_1)$$  \hspace{1cm} (2)

where $\tau_1$ is the constant timing offset between the jammer’s symbol boundary and time zero at Willie’s receiver.

Because the jammer varies his average power independently from time slot to time slot, Willie is unaware of the average power of the jammer on any given time slot and must try to detect Alice on $(0, T)$ in the presence of this uncertainty. Willie’s detection problem is a hypothesis test, as discussed in more detail below. Under $H_0$, which is the hypothesis that Alice did not transmit, his signal is given by:

$$z(t)|H_0 = \zeta \sum_{k=1}^{n} v_k p(t - kT_b - \tau_1) + N^{(w)}(t)$$  \hspace{1cm} (3)

where $\zeta = 1/d_{a,w}^{\alpha/2}$, $\alpha$ is the path-loss exponent, and $N^{(w)}(t)$ is the noise Willie observes at his receiver, which is a zero-mean Gaussian process with (two-sided) power spectral density $S_N^{(w)}(f) = \sigma_w^2$. Under $H_1$, which is the hypothesis that Alice did transmit, he observes:

$$z(t)|H_1 = \lambda \sum_{k=1}^{n} f_k p(t - kT_b - \tau_a)$$

$$+ \zeta \sum_{k=1}^{n} v_k p(t - kT_b - \tau_1) + N^{(w)}(t)$$  \hspace{1cm} (4)

where $\lambda = 1/d_{a,w}^{\alpha/2}$.

Bob receives the signal $y(t)$, which is analogous to $z(t)$ under each hypothesis, but with the substitutions of the distances $d_{a,b}$ and $d_{j,b}$ for $d_{a,w}$ and $d_{j,w}$, respectively, and with additive noise $N^{(b)}(t)$, which is a zero-mean Gaussian process with (two-sided) power spectral density $S_N^{(b)}(f) = \sigma_B^2$, instead of $N^{(w)}(t)$.

B. Metrics

Willie’s goal is to determine if Alice transmitted a message to Bob. Per above, the hypothesis test is given as:

$$H_0 : \text{Alice did not transmit a message in } (0, T)$$

$$H_1 : \text{Alice transmitted a message in } (0, T)$$  \hspace{1cm} (5)
Define $P_{MD}$ as Willie’s probability of missing Alice’s communication ($P(H_0|\text{Alice transmitted})$) and $P_{FA}$ as Willie’s probability of false alarm ($P(H_1|\text{Alice did not transmit})$). We assume equally likely hypotheses $P(H_0) = P(H_1) = \frac{1}{2}$. Following [2], Alice achieves covert communication if Willie’s probability of error, $P_e^{(W)}$, is upper bounded as follows: $\frac{P_{MD} + P_{FA}}{2} > \frac{1}{2} - \epsilon$ for any $\epsilon > 0$ as $T \to \infty$. In the case of hypotheses that are not equally likely, the probability of error is different, but the same criterion still applies, as explained in [9]. Reliable communication between Alice and Bob is also a requirement for covert communications. Therefore, for any $\delta > 0$, Bob’s probability of decoding Alice’s message should be less than $\delta$ for $T$ sufficiently large [2], [9].

III. THE ALICE-BOB-WILLIE SCENARIO

The case when a jammer is present in the environment is of most interest here. However, before considering the environment with a jammer, we briefly look at the extension of the work in [2] to the continuous-time model and sketch the appropriate arguments in this section. Willie’s hypothesis test is simplified to:

$$H_0 : z(t) = N^{(w)}(t)$$
$$H_1 : z(t) = \lambda \sum_{k=1}^{n} f_k p(t - kT_b - \tau_a) + N^{(w)}(t). \quad (6)$$

We consider both achievability and converse results. For achievability, Alice constructs a codebook as in Theorem 1.1 of [2], generates the symbol sequence $f_1, f_2, \ldots, f_n$ based on the information sequence, and maps the symbols to the waveform $x(t)$ as in (1). Now, because it is an achievability result, we make Willie more powerful by assuming that a genie informs Willie of the symbol timing $\tau_a$. Then, the set $\{p(t - kT_b - \tau_a), k = 1, 2, \ldots, n\}$ forms a complete orthonormal basis for $x(t)$ and thus Willie match filters to each of these waveforms to produce his received vector of length $n$, thus arriving at a model similar to that of Theorem 1.1 in [2], from which a throughput of $O(\sqrt{n})$ bits in $n$ symbol periods follows. Since the number of symbol periods, $n$, in a fixed bandwidth channel is proportional to the time duration $T$, $O(\sqrt{T})$ bits are sent in time $T$.

Conversely, assume that Willie employs a power detector over the interval $(0, T)$. Following analogous arguments to those in [2], this limits the total energy that Alice can employ to $\sqrt{T}$, from which a throughput of $\sqrt{T}$ bits in a time period of $T$ follows from the capacity of a bandlimited Gaussian channel by following analogous arguments to those in [2].

IV. THE ALICE-BOB-WILLIE-JAMMER SCENARIO

A. Mitigating the Jammer by Exploiting Timing Offsets

Consider now the general case described in Section II, where a jammer is present in the environment. Figure 2 shows a receiver for Willie motivated from work in co-channel interference mitigation [11]. Define $z_{mf}(t) = z(t) \ast p(-t)$ as the output of the matched filter, which is given by:

$$z_{mf}(t) = \sum_{k=1}^{n} f_k q(t - kT_b - \tau_a)$$
$$+ \sum_{k=1}^{n} q_k q(t - kT_b - \tau_a) + p(t) \ast N^{(w)}(t) \quad (7)$$

where $q(t) = p(t) \ast p(-t)$ is the zero-ISI raised cosine pulse and $\ast$ denotes convolution. In Figure 2, Branch A captures the signal sampled at Alice’s estimated offset, $\tilde{\tau}_a$, and Branch J captures the signal sampled at the jammer’s estimated offset, $\tilde{\tau}_J$. Following [9], the jammer varies his average power in each time slot of length $T$, but we assume the jammer does not vary his timing offset and thus Willie can estimate the jammer’s offset with minimal error by observing a large number of time slots. This assumption is validated in simulation results.

Assuming Willie observes $N$ samples on each branch, Willie’s observations $y^{(a)}$ and $y^{(j)}$ are:

$$\begin{bmatrix} y^{(a)} \\ y^{(j)} \end{bmatrix} = A \begin{bmatrix} f \end{bmatrix} + \begin{bmatrix} I^{(a)} \\ I^{(j)} \end{bmatrix}$$

where $A$ is a $2N \times 2N$ matrix:

$$A = \begin{bmatrix} I_{N \times N} & Q_{N \times N} \\ Q_{N \times N} & I_{N \times N} \end{bmatrix}. \quad (9)$$

$Q_{N \times N}$ is an $N$ by $N$ matrix with diagonal and off-diagonal terms described in [12] that reflects the interference from the jammer’s signal on Branch A and the interference from Alice’s signal on Branch J in terms of $q(t)$. The vectors $n^{(a)}$ and $n^{(j)}$ capture the sampled noise at Willie’s receiver on Branch A and Branch J, respectively.

If matrix $A$ is full rank, Willie can estimate the original symbols transmitted by Alice and the jammer by employing the inverse of $A$:

$$\begin{bmatrix} b^{(a)} \\ b^{(j)} \end{bmatrix} = A^{-1} \begin{bmatrix} y^{(a)} \\ y^{(j)} \end{bmatrix}$$

where $b^{(a)}$ is an $N \times 1$ vector representing Willie’s estimate of Alice’s symbols $Af$ and $b^{(j)}$ is an $N \times 1$ vector representing Willie’s estimate of Alice’s symbols $\zeta q$. Thus, if $A$ is full rank, Willie can measure the power observed in $b^{(a)}$, which has no components due to the jammer, to detect if Alice is transmitting for various estimates of $\tau_a$. Since the interferer is mitigated, the throughput returns to that of [2]. However, if $\tau_a = \tilde{\tau}_J$, $A$ is given by:

$$A = \begin{bmatrix} I_{N \times N} & I_{N \times N} \\ I_{N \times N} & I_{N \times N} \end{bmatrix}$$

which makes inversion impossible. In this case, the discrete-time model arises and the results of [9] apply. Numerical results are presented in the next section.

B. Numerical Results

We employ Monte Carlo simulation to evaluate Willie’s detection capabilities when he employs the proposed detector that exploits the timing offsets between Alice and the
A square-root raised cosine pulse shape set to 30 samples or roughly one-quarter of the symbol period. Timing offset between the jammer’s signal and Alice’s signal symbols that also have the symbol period 128 discrete-time periods. For the null hypothesis, Willie observes the jammer’s signal and AWGN. The jammer transmits Gaussian symbols, and she shares this codebook (secretly) with Bob per [2], [9]. If Alice decides to transmit, she sets $T_s = \frac{1}{2W}$, assigns the codeword can be ignored, and that Bob is able to recover excess bandwidth), that “edge effects” at the start and end of the codeword can be ignored, and that Bob is able to recover information from the key that he shares with Alice.

Assume a channel of bandwidth $W$ is available to Alice. She constructs a codebook by randomly drawing symbols from an i.i.d. Gaussian distribution for each element of each codeword, and she shares this codebook (secretly) with Bob per [2], [9]. If Alice decides to transmit, she sets $T_s = \frac{1}{2W}$, assigns

\[ x(t) = \sum_{k=1}^{n} f_k \cdot p(t - kT_s - \gamma_a) \]  

(12)

where $p(t) = 2W \text{sinc}(2Wt)$, and $\gamma_a$ is a random offset chosen uniformly from the interval $[0, T_s]$.

The jammer generates a sequence of $n$ i.i.d. Gaussian random variables $\{v_k, k = 1, 2, \ldots, n\}$ and transmits the signal:

\[ g(t) = \sum_{k=1}^{n} v_k \cdot p(t - kT_s - \gamma_j), \]  

(13)

again with $p(t) = 2W \text{sinc}(2Wt)$, where $\gamma_j$ is a random offset chosen uniformly from the interval $[0, T_s]$. The hypothesis test at Willie then becomes:

\[ H_0: \quad z(t) = \zeta \sum_{k=1}^{n} v_k p(t - kT_s - \tau_j) + N^{(w)}(t) \] 

(14)

\[ H_1: \quad z(t) = \zeta \sum_{k=1}^{n} v_k p(t - kT_s - \tau_j) + \lambda \sum_{k=1}^{n} f_k p(t - kT_s - \gamma_a) + N^{(w)}(t) \]
where $\tau_a$ and $\tau_j$, which incorporate the random offsets $\gamma_a$ and $\gamma_j$, respectively, and any propagation delays, can still be modeled as independent and each uniformly distributed on $[0,T_s]$.

Under $H_0$, the expectation of the signal part is given by: 

$$E[z(t)|H_0] = \sum_{k=1}^{\infty} E[v_k]p(t - k\tau_a - \tau_j) = 0.$$ 

Next, consider the autocorrelation function $R_z^{(0)}(t,t+\tau)$ of the signal portion of $z(t)$ under $H_0$. Taking the expectation over the uniformly distributed delay of the jammer and, per above, ignoring edge effects by assuming the signal continues infinitely, standard (but lengthy) arguments yield:

$$R_z^{(0)}(t,t+\tau) = \frac{\zeta^2 P_{\text{max}}}{T_s} \int_{-\infty}^{\infty} |P(f)|^2 e^{j2\pi f \tau} df$$

(15)

where $P(f)$ is the Fourier transform of $p(t)$. Thus, under $H_0$, the signal portion of $z(t)$ is wide-sense stationary with autocorrelation given by (15); hence, it has a well-defined power spectral density given by $S^{(0)}(f) = \frac{\zeta^2 P_{\text{max}}}{T_s} |P(f)|^2$. Under $H_1$, the independence of the random variables in $\{v_k\}$ and $\{\epsilon_k\}$ allows us to show that the signal portion of $z(t)$ is again wide-sense stationary with autocorrelation function:

$$R_z^{(1)}(t,t+\tau) = \frac{\zeta^2 + \lambda^2 P_{\text{max}}}{T_s} \int_{-\infty}^{\infty} |P(f)|^2 e^{j2\pi f \tau} df$$

(16)

and thus has power spectral density $S^{(1)}(f) = \frac{\zeta^2 + \lambda^2 P_{\text{max}}}{T_s} |P(f)|^2$.

By construction, $p(t) = 2W\text{sinc}(2Wt)$, and thus

$$P(f) = \begin{cases} 1, & |f| < W \\ 0, & \text{else} \end{cases}$$

(17)

and $|P(f)|^2 = P(f)$. Hence, the signal is bandlimited; by the sampling process for wide-sense stationary random processes, it is sufficient for Willie to sample the signal at frequency $2W$. Noting that $R_z^{(0)}(t,t+\tau) = c \cdot \text{sinc}(2W\tau)$, this implies that Willie observes an i.i.d. sequence of Gaussian random variables from the jammer’s signal in his samples, and hence the model of [9] applies. Hence, with ideal pulse shaping and a random timing offset between Alice and the jammer, Willie’s detector fails and covertness is maintained, without the need to decrease power as a function of blocklength. Simulations with parameters identical to those of Section IV-B are shown in Figure 4.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we considered the natural extension of recent work on covert communications over discrete-time channels to the continuous-time channels generally observed in practice. In the original scenario considered in [2], where Alice attempts to transmit to Bob without detection by an attentive adversary Willie in an AWGN environment, the throughput scaling with the continuous-time model is unchanged from that obtained from the discrete-time model. However, in the case where a jammer has been added to assist covert communications, as in [9], and promising covert throughput results were obtained, care must be exercised. In particular, if a straightforward extension of the work in [9] is implemented, the adversary can separate various transmitters through their timing offsets, hence mitigating the jammer and reducing the throughput back to that obtained in [2] without the jammer. If optimal pulse shaping can be assumed, we demonstrate an approach for Alice and the jammer that, under other mild assumptions, achieves the throughput of [9] even in the face of an optimal receiver at Willie. Currently, we are considering the important problem of providing provable non-zero rate covert communications while employing more practical pulse shapes.

REFERENCES