Fundamental Limits of Activity-Based Covert Channels

Ke Li
Dept. Electrical and Computer Engineering
University of Massachusetts Amherst
kli0@umass.edu

Majid Ghaderi
Dept. Computer Science
University of Calgary
mghaderi@ucalgary.ca

Dennis Goeckel
Dept. Electrical and Computer Engineering
University of Massachusetts Amherst
goeckel@ecs.umass.edu

GLOBECOM 2021 - 2021 IEEE Global Communications Conference | 978-1-7281-8104-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GLOBECOM46510.2021.9686016

***Abstract*—Covert communication considers the ability of transmitter Alice to communicate reliably to intended receiver Bob without being detected by adversary warden Willie. One collection of approaches to covert signaling is for Alice to alter the state of a system in such a way that the altered state conveys information to Bob. Motivated by recent work on the foundations of covert communications that has largely considered the physical layer, we provide a fundamental characterization of one approach to covert signaling via activity: employing a codebook pre-shared with Bob, Alice encodes a message by selecting from the codebook the appropriate pattern of slots to insert innocuous packets into a slotted ALOHA system in the presence of other users. The intended recipient Bob detects patterns in the activity of the slotted ALOHA system to determine which codeword was sent. We provide a fundamental analysis of the performance of such a system under a covertness constraint. First, we consider signaling schemes derived specifically for the proposed channel when Bob or Willie has various abilities to discern the number of packets in a given slot. Given the challenges in such design, we next recognize that techniques from optical communications, although designed for a different channel, can potentially be employed and thus yield a large class of schemes that provide lower bounds on the achievable rate. Numerical results are provided to support the analytical development and to demonstrate the potential of covert signaling through such an approach.**

I. Introduction

Security is a major concern of modern communication networks, where it is often obtained by encryption. However, this is not sufficient in applications where the very existence of transmission arouses suspicion. For example, in military communications, the detection of a transmission may reveal activity in the region. This motivates the study of covert communication: a transmitter Alice reliably sending messages to a legitimate receiver Bob without that communication being detected by an attentive warden Willie. In practice, spread spectrum techniques have been traditionally employed at the physical layer to achieve covert communications. More recently, there has been an active line of research exploring the fundamental limits of covert communications. Bash *et al.* in [1] proved that Alice can transmit at most $\mathcal{O}(\sqrt{n})$ covert bits to Bob in n channel uses of an AWGN channel. Performance limits with scaling constants for covert communications were established in successive work [2]–[4]. Communication schemes to achieve n covert bits in n channel uses are then provided in [5], where an uninformed jammer is added to the system. Further work has begun to consider covert communications with a continuous-time model that corresponds to true physical channels [6]–[8]. In many of these systems, the transmitter Alice is not allowed to transmit at all and must hide in the background noise or jamming (e.g. [1]), but, more generally, Alice is allowed some innocuous behavior, but is not allowed to deviate from such.

In analogy with spread spectrum work at the physical layer, practical covert communications have been studied in higher layers. Of interest here are a number of efforts that aim to perform covert signaling by altering the state of a system in such a way that it can be detected by the intended recipient. For example, in [9] and [10], the behavior of TCP flows is modeled by a Markov chain composed of the states of TCP packets, and covert transmissions are achieved if deviations from the expected state cannot be detected. Our interest here is extending the line of fundamental analyses of covert communications [1]–[8] to consider a system that conveys information by altering the state of a system. However, it is challenging to perform fundamental analysis of the performance of such systems under a covertness constraint since even simple examples can lead to intractable analytic problems. For example, considering Alice altering the state of a general Markov chain which is then observed by Bob through a noisy channel requires the entropy of a hidden Markov model (HMM), which is hard to obtain [11]. Instead, we turn to a slotted ALOHA system, as described below.

In [12], we considered a scenario in which covert communication is achieved by carefully hiding covert messages among the legitimate (i.e., overt) messages transmitted by Alice to Bob. Specifically, the covert messages are inserted in the sequence of Alice's legitimate messages such that their effect on the system state is undetectable by the observer Willie. To receive covert messages, Bob decodes all messages received from Alice, some of which are covert messages. Such a model relies on a strong assumption that Willie does not look inside the transmitted messages; rather, Willie is constrained to be only an observer of the state of the system, e.g., how many messages are on the channel. Thus, as long as Alice's covert messages do not cause the state of the system to deviate

Ke Li and Dennis Goeckel were supported by the National Science Foundation under grant ECCS-2029323. Majid Ghaderi was supported by Natural Sciences and Engineering Research Council of Canada and Alberta Innovates.

appreciably from its expected state, Willie will not be able to detect covert messages.

In this work, we consider a more capable adversary than that in [12]: Willie not only observes the state of the system to detect unexpected deviations, but also looks inside the messages to ensure messages do not convey any information covertly. Thus, the actual messages cannot be used for covert communication between Alice and Bob anymore, as this would be detected by Willie. Instead, Alice tries to covertly communicate with Bob by altering her pattern of activity: inserting packets to modulate the state of the system itself. Then, by coding information in her activity patterns, Alice can covertly communicate with Bob without directly sending any observable message to Bob. The communication is accomplished through a shared resource, which is the state of the system. However, since Willie observes the state of the system, any manipulation of the system state has to be done carefully to avoid detection by Willie.

The contributions of the paper are:

- *Fundamental Characterization of Activity-Based Covert Channels:* To our knowledge, we provide the first fundamental characterization of a covert system that conveys information by activity patterns that alter channel state.
- *Derivation of Achievable Schemes:* We derive and characterize covert schemes specifically fitted to conveying information through activity in a slotted ALOHA system.
- *Leveraging Optical Communication Approaches:* Given the challenges faced, we demonstrate that optical communication methods can be adopted to the proposed framework and hence a large class of schemes can be employed. These achievable schemes provide a lower bound on the potential rate of covert approaches.

Section II presents the system model and metrics. Section III provides constructions fitted to the proposed framework, and Section IV discusses lower bounds on achievability derived from optical communications. Numerical results are presented in Section V, and conclusions are presented in Section VI.

II. System Model and Metrics

A. System Model

Consider a slotted random access channel with multiple system users, among whom is a transmitter Alice who wishes to convey covert information to intended recipient Bob without detection by an attentive warden Willie. Fig. 1 illustrates the system model. Each of the system users, other than Alice, randomly and independently transmits a packet in each slot with some probability. It is well-known that in such a random access system, the number of packets transmitted by the users during "standard" operation (i.e., the number of non-covert packets) can be approximated by a Poisson random variable with a suitable rate λ [12]. Each of Bob and Willie can observe the state of the system, perhaps with some limitations as described below, and, in contrast to [12], the adversary Willie is able to observe packet contents, hence preventing Alice from sending covert information explicitly or in encrypted form within the packet contents to Bob. Thus, the user-of-interest Alice, while trying to avoid detection by the warden Willie, is restricted to communicating with the intended recipient Bob by adding some number of packets to successive slots and conveying information through such activity.

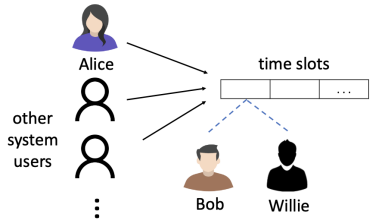


Fig. 1: Slotted ALOHA System: by modulating her activity pattern, the transmitter Alice attempts to communicate with the receiver Bob without being detected by warden Willie.

Traditionally, packets involved in a collision would simply be discarded and retransmission would be required. However, it is possible for an advanced receiver to recover some packets from a collision through multi-packet reception [13]. Likewise, the ability to detect multiple simultaneous transmissions is denoted as Multi-Packet Detection (MPD), and a receiver is called a K-MPD detector if it can detect up to K packet transmissions in a time slot on a channel. As in [12], we will consider scenarios where Bob and Willie have various abilities to perform multi-packet detection.

B. Metrics

1) Willie: Willie's goal is to determine whether Alice is conveying covert information in a time slot or not. Willie will observe a state of the system that will depend on the number of packets on the channel and his ability to observe such. We define the null hypothesis (H_0) to be that Alice is not conveying covert information, and the alternative hypothesis (H_1) to be that Alice is conveying covert information. Let Willie's probability of false alarm be denoted by $\mathbb{P}_{FA}$, and his probability of missed detection be denoted by $\mathbb{P}_{MD}$. We say that the transmission is covert if, for a given $\epsilon > 0$, we have $\mathbb{P}_{FA} + \mathbb{P}_{MD} \geq 1 - \epsilon$.

The optimal hypothesis test performed by Willie can be characterized by the total variation distance between the distribution $\mathbb{P}_0$ of observed channel states given H_0 and the distribution $\mathbb{P}_1$ of observed channel states given H_1 [1]:

$$\mathbb{P}_{FA} + \mathbb{P}_{MD} = 1 - d_{TV}(\mathbb{P}_0, \mathbb{P}_1),$$

where,

$$d_{TV}(\mathbb{P}_0, \mathbb{P}_1) = \frac{1}{2} \sum_{s \in \mathcal{S}} |\mathbb{P}_0(s) - \mathbb{P}_1(s)|\,, \tag{1}$$

and $\mathcal{S}$ denotes the set of possible channel states. Hence, covertness is achieved if:

$$d_{TV}(\mathbb{P}_0, \mathbb{P}_1) < \epsilon\,. \tag{2}$$

2) Bob: We will say communication between Alice and Bob is reliable if the probability of decoding error is less than or equal to δ for any $\delta > 0$ as the length of the codeword used by Alice and Bob approaches infinity. Since the effective channels built throughout this work will be discrete memory-

less channels (DMCs), the achievable rate with vanishing error probability in the limit of long block length is the maximum mutual information between the effective channel's input and output, and hence optimizing the mutual information will be the focus of succeeding sections.

III. Achievable Covert Schemes

In this section, we derive and characterize covert schemes specifically fitted to conveying covert information through activity in a slotted ALOHA system. Specifically, we establish constructions such that Alice can covertly transmit binary codewords to Bob in such a system. We will analyze the achievable rate in various scenarios.

A. Construction

We employ random coding and generate M codewords, each of length n, by independently drawing symbols from a Bernoulli distribution such that the symbol takes the value 1 with probability p_1, and 0 with probability $p_0 = 1 - p_1$. As in [1], this codebook is shared between Alice and Bob, and thus is unknown to Willie. The shared codebook in the covert context plays a role similar to that of a shared *secret* in cryptography. If Alice decides to transmit, she selects the codeword corresponding to her message, and adds the number of packets on the channel in the i'th time slot according to the i'th symbol of the codeword. She adds no packets for symbol 0, and one packet for symbol 1. Thus, the channel input $X \sim \text{Bernoulli}(p_1)$ is the number of packets sent by Alice in each time slot. As mentioned earlier, the number of non-covert packets in the background follows a Poisson distribution with parameter λ. This model corresponds to a discrete-time Poisson (DTP) channel with X being the channel input and Y being the output.

B. Achievable Rate

Here we analyze the achievable rate of the covert scheme when Bob has different detection capabilities.

1) 0-MPD at Bob: When Bob employs 0-MPD, he can only distinguish an idle channel and a busy channel. Hence, he either observes no packets (state $s = 0$) , or observes one or more packets (state $s = 1$). Given the distribution of p_0 and p_1, the entropy of Bob's observed state Y is given by:

$$\begin{aligned} H(Y) &= -\sum_{s=0}^{1} P(Y=s)\log P(Y=s) \\ &= -p_0e^{-\lambda}\log p_0e^{-\lambda} - (1-p_0e^{-\lambda})\log(1-p_0e^{-\lambda}) \end{aligned}$$

and the entropy of Y given Alice's transmission X is:

$$\begin{aligned} H(Y|X) &= E_X\left[H(Y|X=x)\right] = p_0 \cdot H(Y|X=0) \\ &= -p_0e^{-\lambda}\log e^{-\lambda} - p_0(1-e^{-\lambda})\log(1-e^{-\lambda})\,. \end{aligned}$$

The mutual information between X and Y is then given by:

$$\begin{aligned} I(X;Y) =& H(Y) - H(Y|X) \\ =& -p_0e^{-\lambda}\log p_0 - (1-p_0e^{-\lambda})\log(1-p_0e^{-\lambda}) \\ &+ p_0(1-e^{-\lambda})\log(1-e^{-\lambda})\,. \end{aligned}$$

In order to find the p_0 that maximizes the mutual information $I(X;Y)$, we take the derivative of $I(X;Y)$:

$$\frac{dI(X;Y)}{dp_0} = e^{-\lambda}\log(\frac{1}{p_0} - e^{-\lambda}) + (1-e^{-\lambda})\log(1-e^{-\lambda}).$$

Setting the above to zero results in:

$$p_0 = \frac{1}{2^{g(\lambda)} + e^{-\lambda}}, \tag{3}$$

where, $g(\lambda) = -(1-e^{-\lambda})\log(1-e^{-\lambda})$. Thus, when Alice employs the probability $p_1 = 1 - p_0$ to send a packet in a time slot on the channel, we achieve the maximum mutual information.

2) ∞-MPD at Bob: When Bob employs ∞-MPD, he can determine the exact number of packets on the channel (state $s = 1, \ldots, \infty$). Hence, this is the most capable Bob. Given the distribution of p_0 and p_1, the entropy of Bob's observation Y is given by:

$$\begin{aligned} H(Y) =& -\sum_{s=0}^{\infty} P(Y=s)\log P(Y=s) \\ =& -p_0e^{-\lambda}\log p_0e^{-\lambda} \\ &- \sum_{k=0}^{\infty}\left(p_0\frac{\lambda^{k+1}e^{-\lambda}}{(k+1)!} + p_1\frac{\lambda^k e^{-\lambda}}{k!}\right) \\ &\cdot \log\left(p_0\frac{\lambda^{k+1}e^{-\lambda}}{(k+1)!} + p_1\frac{\lambda^k e^{-\lambda}}{k!}\right), \end{aligned}$$

and the entropy of Y given Alice's transmission X is:

$$\begin{aligned} H(Y|X) =& -p_0\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\log\frac{\lambda^k e^{-\lambda}}{k!} \\ &- p_1\sum_{k=1}^{\infty}\frac{\lambda^{k+1}e^{-\lambda}}{(k+1)!}\log\frac{\lambda^{k+1}e^{-\lambda}}{(k+1)!}. \end{aligned}$$

Given the effective DMC, we know that rates approaching $\max_{p_0} I(X;Y) = \max_{p_0}\left(H(Y) - H(Y|X)\right)$ are achievable.

Since the analytic expression for the achievable rate does not appear to have a simple form, we provide numerical results in Section V. In addition, we will show in Section IV that a randomization step added after the codebook will yield an optical communication model, for which previous schemes from optical communications can be applied to provide suboptimal, but achievable rates, for our problem of covert communications over the slotted ALOHA channel.

C. Covertness Constraints

Here we provide the covertness constraints when Willie has different capabilities in detecting the number of packets on the channel in each time slot.

1) 0-MPD at Willie: When Willie employs 0-MPD, the total variation distance between the distribution $\mathbb{P}_0$ and $\mathbb{P}_1$ of the observed channel states conditioned on H_0 and H_1, respectively, is given by:

$$\begin{aligned} d_{TV}(\mathbb{P}_0, \mathbb{P}_1) &= \frac{1}{2}\sum_{s=0}^{1}|\mathbb{P}_0(s) - \mathbb{P}_1(s)| \\ &= \frac{1}{2}|e^{-\lambda} - p_0e^{-\lambda}| + \frac{1}{2}|1 - e^{-\lambda} - 1 + p_0e^{-\lambda}| = p_1e^{-\lambda}\,. \end{aligned}$$

Thus, according to (2), covertness is achieved if:

$$p_1 < \min(1, \epsilon \cdot e^{\lambda}), \tag{4}$$

for any given $\epsilon > 0$.

2) 1-MPD at Willie: When Willie employs 1-MPD, he can distinguish between an idle channel ($s = 0$) and one packet transmission ($s = 1$), but when more than one packet is transmitted over the channel, he only knows that more than one packet was on the channel ($s = 2$). The total variation distance between $\mathbb{P}_0$ and $\mathbb{P}_1$ is given by:

$$\begin{aligned} d_{TV}(\mathbb{P}_0, \mathbb{P}_1) &= \frac{1}{2}\sum_{s=0}^{2} |\mathbb{P}_0(s) - \mathbb{P}_1(s)| \\ &= \frac{1}{2}|e^{-\lambda} - p_0 e^{-\lambda}| + \frac{1}{2}|\lambda e^{-\lambda} - p_0 \lambda e^{-\lambda} - (1-p_0)e^{-\lambda}| \\ &\quad + \frac{1}{2}|(p_0\lambda + 1)e^{-\lambda} - (1+\lambda)e^{-\lambda}| \\ &= \frac{1}{2}(1-p_0)(1+\lambda+|\lambda-1|)e^{-\lambda}\,. \end{aligned}$$

Thus, according to (2), covertness is achieved if:

$$p_1 < \min\left(1, \frac{2\epsilon}{(1+\lambda+|\lambda-1|)e^{-\lambda}}\right), \tag{5}$$

for any given $\epsilon > 0$.

IV. Leveraging Optical Communication Approaches

As mentioned in Section III-B, it is difficult to derive a simple (e.g., closed-form) analytic expression for the achievable rate with our proposed covert scheme when Bob employs ∞-MPD. Given the challenges faced, in this section we demonstrate that our covert communication model based on a slotted ALOHA system, with a small randomization step after the codebook, is equivalent to an oft-studied optical communication model. This allows us to apply previous studies in optical communications to this problem to find achievable rates and hence lower bound the potential rate of covert approaches.

A. Background on Optical Communications

In optical communications, at the transmitter, a laser emits a stream of discrete photons with a time-varying rate which is proportional to the amplitude of the input current. The receiver consists of a photon detector which can determine the arrival times of individual photons. The stream of photons is typically modeled as an inhomogeneous Poisson point process with time-varying intensity proportional to the input current. The stream of photons generated in the laser on the background is modeled as an additive Poisson process with some fixed rate. With a randomization step after our codebook as described in the construction below, we have the standard discrete-time Poisson (DTP) model for optical communications, which is first studied in [15]. A DTP channel with *dark current* λ is a memoryless channel which takes input $X \in \mathbb{R}^+$, and outputs $Y \in \mathbb{Z}^+$. Conditional on input x, the output is Poisson distributed with mean $x+\lambda$. Thus, the conditional channel law:

$$W(y|x) = e^{-(x+\lambda)}\frac{(x+\lambda)^y}{y!}, \quad x \in \mathbb{R}^+, y \in \mathbb{Z}^+ \tag{6}$$

where the input x corresponds to the intensity of a photon-emitting source at the transmitter; the dark current λ models the background interference; and the output y corresponds to the number of photons arriving at the receiver.

B. Construction Using Optical Communication Approaches

We extend signaling schemes from optical communications to our framework of a slotted ALOHA system. As before, we employ random coding and generate M codewords, each of length n, independently drawing symbols from a Bernoulli distribution such that the symbol takes the value 1 with probability p_1, and 0 with probability $p_0 = 1 - p_1$. The codebook is shared between Alice and Bob but not Willie [1]. If Alice decides to transmit, she selects the codeword corresponding to her message, and adds a number of packets in the i'th slot according to the i'th symbol of the codeword. Different from our previous proposed scheme where Alice adds either no packets or just one packet, here she adds no packets for symbol 0, and adds a Poisson number of packets with mean $\lambda_a > 0$ for symbol 1. Thus, the channel input X is the rate of packets added by Alice, and X is either 0 or λ_a depending on the symbol transmitted. As long as λ_a is bounded by the covert limits established in [12], e.g., $\lambda_a \leq \ln \frac{1}{1-\epsilon e^{\lambda}}$ if $\lambda \leq \ln \frac{1}{\epsilon}$ and Willie employs 0-MPD, covertness can be achieved.

C. Achievable Rate

In order to analyze the performance of the covert scheme in Section IV-B, we analyze the capacity of the DTP channel. Previous studies have provided asymptotic lower bounds on the capacity with average-power and peak-power constraints. In [14], Lapidoth *et al.* study the asymptotic capacity of a DTP channel with an average-power constraint

$$E[X] \leq \mathcal{E}, \tag{7}$$

and a peak-power constraint

$$Pr(X > A) = 0. \tag{8}$$

Note that (7) corresponds to the constraint on the average rate of packets added by Alice in each time slot for our covert scheme, i.e.,

$$p_1\lambda_a \leq \mathcal{E}. \tag{9}$$

The peak-power constraint in (8) corresponds to a constraint on the peak rate of packets added by Alice in each time slot. Let C denote the capacity of the channel. Lapidoth *et al.* show that when λ scales with $\mathcal{E}$, we have

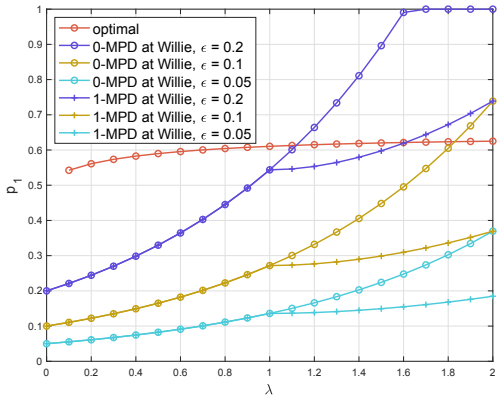
$$\lim_{\mathcal{E}\to 0} \frac{C}{\mathcal{E}\log\frac{1}{\mathcal{E}}} = 1, \tag{10}$$

and when λ is held constant and does not scale with $\mathcal{E}$:

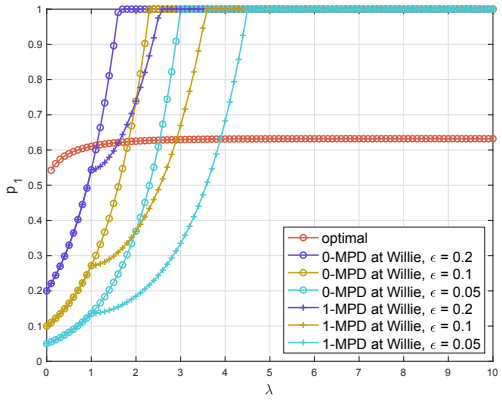
$$\liminf_{\mathcal{E}\to 0} \frac{C}{\mathcal{E}\log\log\frac{1}{\mathcal{E}}} \geq \frac{1}{2}. \tag{11}$$

The constraint in (9) can be combined with the covertness constraints established in [12]. For example, when Willie employs 0-MPD, which requires $\lambda_a \leq \ln \frac{1}{1-\epsilon e^{\lambda}}$ to be covert if $\lambda \leq \ln \frac{1}{\epsilon}$ for any given $\epsilon > 0$, we have the combined constraint

$$p_1 \ln \frac{1}{1-\epsilon e^{\lambda}} \leq \mathcal{E}. \tag{12}$$

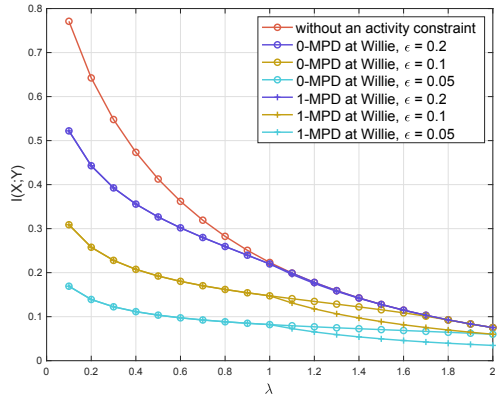


(a) When λ is around 1.

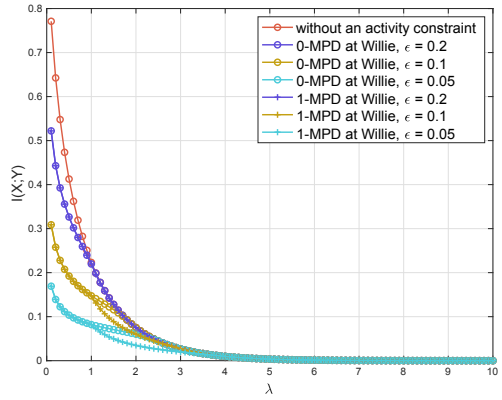


(b) When λ has a large range.

Fig. 2: The optimal probability p_1 that maximize $I(X;Y)$ when Bob employs 0-MPD and the upper bounds of p_1 that achieve covertness when Willie employs either 0-MPD or 1-MPD.



(a) When λ is around 1.



(b) When λ has a large range.

Fig. 3: The achievable mutual information $I(X;Y)$ under different activity constraints when Bob employs 0-MPD.

Letting $\mathcal{E} = p_1 \ln \frac{1}{1-\epsilon e^{\lambda}}$, which is a very small number for small λ, we can further derive from (10) when $\lambda \to 0$:

$$C = p_1 \ln \frac{1}{1-\epsilon e^{\lambda}} \log \left(\frac{1}{p_1 \ln \frac{1}{1-\epsilon e^{\lambda}}} \right),$$

and in (11) when λ is a small constant:

$$C \geq \frac{1}{2} p_1 \ln \frac{1}{1-\epsilon e^{\lambda}} \log \log \left(\frac{1}{p_1 \ln \frac{1}{1-\epsilon e^{\lambda}}} \right). \tag{13}$$

We provide numerical results for (13) in the next section.

V. Numerical Results

In this section, we provide numerical results when Bob and Willie have various detection capabilities.

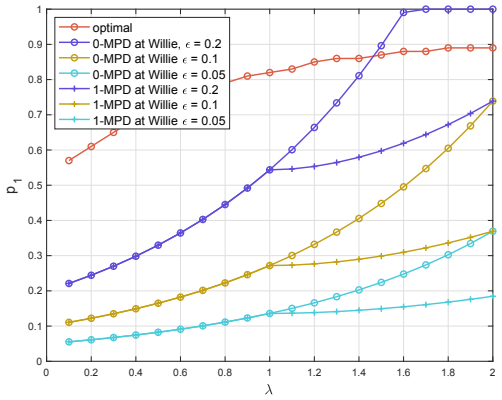
A. 0-MPD at Bob

Fig. 2 shows the optimal p_1 that maximizes $I(X;Y)$ when Bob employs 0-MPD and the upper bounds of p_1 by the covertness constraints when Willie employs 0-MPD, respectively. The parameter ϵ for the covertness constraint is set to be 0.2, 0.1 and 0.05. In realistic scenarios, the operating regime of the system is around $\lambda = 1$, which is depicted in Fig. 2(a). However, to better observe the trends in the behavior of the system, we have also plotted our results for a large range of λ, which is depicted in Fig. 2(b). An interesting observation is that, while higher background traffic (i.e., larger λ) provides Alice with increased opportunities to hide her covert messages, it does not necessarily lead to an increased covert throughput as it also increases the error rate at Bob. Indeed, we observe that as λ increases, the optimal p_1 that maximize $I(X;Y)$ approaches a constant. Thus, when Bob employs 0-MPD, from (3) and (4), we see that Alice should employ:

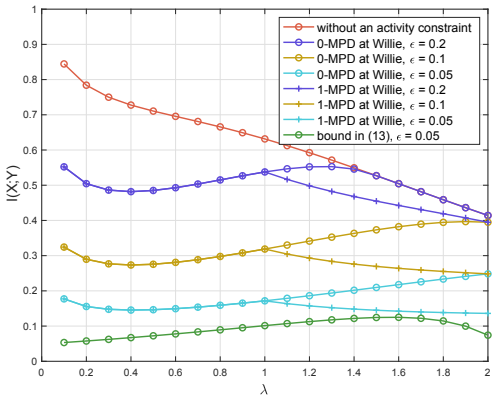
$$p_1 = \min \left(1, 1 - \frac{1}{e^{g(\lambda)} - e^{-\lambda}}, \epsilon \cdot e^{\lambda} \right),$$

in order to maximize her transmission rate while maintaining covertness. When Bob employs 1-MPD, from (3) and (5), we see that Alice should employ:

$$p_1 = \min \left(1, 1 - \frac{1}{e^{g(\lambda)} - e^{-\lambda}}, \frac{2\epsilon}{(1 + \lambda + |\lambda - 1|)e^{-\lambda}} \right),$$



(a) The optimal probability p_1 that maximize $I(X;Y)$ when Bob employs ∞-MPD and the upper bounds of p_1 that achieve covertness when Willie employs either 0-MPD or 1-MPD.



(b) The achievable mutual information and the capacity bound in (13) under different activity constraints when Bob employs ∞-MPD.

Fig. 4: The probability p_1 and the corresponding mutual information $I(X;Y)$ when Bob employs ∞-MPD.

in order to maximize her transmission rate while maintaining covertness. The associated mutual information $I(X;Y)$ is shown in Fig. 3. In particular, the case when λ is around 1 is depicted in Fig. 3(a), and the case when λ has a large range is depicted in Fig. 3(b). From these figures, we can see that, as the background traffic increases, the mutual information approaches zero regardless of any activity constraint on Alice.

B. ∞-MPD at Bob

Fig. 4(a) shows the optimal p_1 that maximizes $I(X;Y)$ when Bob employs an ∞-MPD receiver and the upper bounds of p_1 by different covertness constraints in the case of 0-MPD and 1-MPD at Willie. Fig. 4(b) shows the achievable mutual information with and without an activity constraint. Again, to maximize her covert transmission rate, Alice should employ a probability p_1 that is the minimum between the optimal p_1 that maximize $I(X;Y)$ and the p_1 that satisfies either (4) or (5) for covertness when Willie employs 0-MPD and 1-MPD, respectively. Comparing Fig. 4(b) with Fig. 3(a), we see that the achievable rate is significantly higher in the latter since Bob employs ∞-MPD, which is more capable in determining the exact number of packets on the channel.

Section IV allows us to adopt constructions from optical communication, which gives achievable (but suboptimal) covert schemes. As an example, in Fig. 4(b), we plot the bound of capacity in (13) which is obtained under the covert scheme from optical communications when Willie employs 0-MPD and $\epsilon = 0.05$. As expected, it is lower compared with the achievable rate of the scheme given in Section III but this alternate construction technique will allow us to consider a larger set of scenarios.

VI. Conclusion

In this paper, we studied covert communication via activity modulation in a slotted ALOHA system. Alice transmits legitimate packets in a pattern of slots determined by the codeword corresponding to the message to be sent to intended recipient Bob. We first considered achievable covert schemes and derived fundamental limits on the system parameters and performances when Bob or Willie have different detection capabilities. We then showed that optical communication approaches can be applied to the considered system, which provide a lower bound on the potential rate of our covert communication system.

References

[1] B. A. Bash, D. Goeckel and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Comm.*, vol. 31, no. 9, 2013.

[2] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE ISIT*, 2013.

[3] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," in *Proc. IEEE ISIT*, 2016.

[4] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," in *Proc. IEEE ISIT*, 2016.

[5] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Comm.*, vol. 16, no. 9, 2017.

[6] L. Wang, "The continuous-time Poisson channel has infinite covert communication capacity," in *Proc. IEEE ISIT*, 2018.

[7] Q. E. Zhang, M. R. Bloch, M. Bakshi and S. Jaggi, "Undetectable radios: Covert communication under spectral mask constraints," in *Proc. IEEE ISIT*, 2019.

[8] K. Li, T. V. Sobers, D. Towsley and D. Goeckel, PhD thesis, *Covert communications in continuous-time systems*, University of Massachusetts Amherst, May 2021.

[9] J. Zhai, G. Liu and Y. Dai, "A covert channel detection algorithm based on TCP Markov model," in *Proc. MINES*, 2010.

[10] J. Zhai, G. Liu and Y. Dai, "Detection of TCP covert channel based on Markov model," *Telecomm. Syst.*, 2013.

[11] P. Jacquet, G. Seroussi and W. Szpankowski, "On the entropy of a hidden Markov process," *The. Cmp. Sci.*, vol. 395(2-3), 2008.

[12] A. Sheikholeslami, M. Ghaderi and D. Goeckel, "Covert communications in multi-channel slotted ALOHA systems," in *IEEE Trans. Mobile Computing*, 2020.

[13] L Tong, Q. Zhao, and G. Mergen, "Multipacket reception in random access wireless networks: From signal processing to optimal medium access control," *IEEE Comm. Mag.*, vol. 39, no. 11, 2001.

[14] A. Lapidoth, J. H. Shapiro, V. Venkatesan and L. Wang, "The discrete-time Poisson channel at low input powers," in *Proc. IEEE ISIT*, 2011.

[15] S. Shamai (Shitz), "Capacity of a pulse amplitude modulated direct detection photon channel," in *Proc. IEE, Part I (Comm., Speech and Vision)*, vol. 137, no. 6, 1990.