Secure Communication through Jammers Jointly Optimized in Geography and Time

Yair Allouche
Dept. of Communication Systems Engineering
Ben-Gurion University
Beer-Sheva, Israel

Yuval Cassuto
Dept. Electrical Engineering
Technion – Israel Institute of Technology
Haifa 32000, Israel

Alon Efrat
Dept. of Computer Science
The University of Arizona
Tucson, AZ 85721, USA

Michael Segal
Dept. of Communication Systems Engineering
Ben-Gurion University
Beer-Sheva, Israel

Esther M. Arkin
Dept. Applied Mathematics and Statistics
Stony Brook University
Stony Brook, NY 11794, USA

Guy Grebla
Dept. Electrical Engineering
Columbia University
New York, NY 10027, USA

Joseph S. B. Mitchell
Dept. of Applied Mathematics and Statistics
Stony Brook University
Stony Brook, NY 11794, USA

Swaminathan Sankararaman
Akamai Technologies
Cambridge, MA 02142, USA

ABSTRACT

Security-sensitive applications, such as patient health monitoring and credit card transactions, are increasingly utilizing wireless communication systems, RFIDs, wireless sensor networks, and other wireless communication systems. The use of interference-emitting jammers to protect these sensitive communications has been recently explored in the literature, and has shown high potential. In this paper we consider optimization problems relating to the temporal distributions of jammers' activity, and the suitable coding regimes used for communication. Solving the joint problem optimally enables comprehensive security in space, at a low power consumption and low communication overhead. The joint optimization of jamming in space and time is driven by a new framework that uses the *bit-error probability* as a measure of communication quality. Under this framework, we show how to guarantee information-theoretic security within a geographic region, and with increased flexibility to tailor the coding regime to the problem's geometry. We present efficient algorithms for different settings, and provide simulations for various scenarios using the bit-error probability functions. These simulations demonstrate the efficiency of the scheme. We believe that our scheme can lead to practical, economical and scalable solutions for providing another layer of protection of sensitive data, in cases where encryption schemes are limited or impractical.

MobiHoc'15, June 22–25, 2015, Hangzhou, China.

DOI: http://dx.doi.org/10.1145/2746285.2746322.

1. INTRODUCTION

More and more, highly sensitive and private information is being transfered via wireless communication. Example systems include contactless smart cards [7], military sensor networks [1], emergency response systems employing wireless networks [12], and ambient living-assistance systems [15]; these systems use wireless communication to transmit banking/financial data, military intelligence, sensory patient health data, and other private information. The open nature of the wireless medium mandates that precautions be taken to protect the privacy of information, e.g., from potential eavesdropping. Unprotected communication, e.g. within sensor networks, also opens the door for various types of attacks on the network, such as sensor impersonation, sybil attacks and wormhole attacks.

Communication devices, such as RFID devices in smart cards, have limited computational capabilities, making cryptographic techniques impossible. Further limitations may come from application constraints, in which, e.g., emergency personnel are unable to enter passwords or use authentication methods to secure data transfer. To make the situation more complex, there may be multiple types of communication nodes, utilizing different frequencies, and the nodes may be changing over time, as nodes are removed or added or become mobile; thus, we are motivated to pursue security techniques that are impervious to variations in the structure of the system or the network.

Wireless jamming has been explored as a means of achieving security from eavesdroppers through the selective introduction of artificial noise [14,24]. In addition to making sure the eavesdropper's channel quality is degraded sufficiently, the quality of legitimate channels must not be compromised. This additional constraint marks a contrast between friendly jamming and traditional offensive jamming.

Sensitive communication may be on single or multiple frequencies and it is often imperative to secure all frequencies. In such scenarios, channel degradation at eavesdroppers may

be achieved through several jamming techniques [18]. Some examples are *barrage jamming*, which transmits noise on all frequencies continuously, *narrowband jamming*, which is restricted to a single frequency, and *pulse jamming*, which sends periodic bursts of noise.

In many cases, legitimate communication is restricted to within a geographic region such as a warehouse, hospital or bank and must be protected from eavesdroppers outside this region. The communication inside the region may be highly dynamic, i.e., nodes may be mobile or may be added/removed and thus, jammers may only use minimal information about the communication taking place in order to intelligently configure themselves. In addition, the existence of only minimal information implies that jammers must be proactive rather than reactive, i.e., they cannot synchronize themselves with legitimate transmissions, nor with each other. Moreover, jammers do not need to have a (common) clock, and synchronization is not required. These assumptions render a collections of such jammers highly dynamic and easily adaptable to changes in the environment they protect. However, we do assume (and actually take advantage of) that jammers could produce noise for some portion of the time (affecting only a subset of the bits in a transmitted message), and burst distributions could be controlled by the user. These temporal jammers fall under the category of pulse jammers in [18].

We argue that temporal jamming has multiple advantages over continuous jamming in eavesdropping mitigation:

1. *Energy savings*: Guaranteed jamming can be achieved with low operation duty cycles.
2. *Simplicity*: Jammers can be fixed-power, and flexibly placed in space.
3. *Spatial separation:* A single-radio jammer can be active on different frequencies at different times, thus being able to secure multi-frequency communications.
4. *Robustness*: Temporal jamming is significantly more difficult to cancel at the eavesdropper's receiver, due to their bursty nature.
5. *Feasibility* There are examples where successful jamming that provides full privacy (in the formal meaning defined below) does not exist with a given set of continuous jammers, yet random temporal jamming is possible.

A central benefit of temporal jamming we explore in this paper is the possibility to employ advanced unconditionally secure coding techniques. Operating the jammers in the time domain allows us to reason about their effect on the most fundamental information unit: a single bit. Therefore, existing jamming optimization techniques can be complemented by coding performed on the transmitted information. When designed together, coding and geometric jammer layout can simultaneously provide reliable communication for legitimate nodes and unconditional privacy from eavesdropping.

Problem Statement. In this paper, we adopt the above approach and consider the combined problem: How should one select the fractions of time in which temporal jammers are active sending noise to secure the communication, and at which coding regime information needs to be communicated. The solution to this problem relies upon three important elements: a new framework for modeling temporal jamming using bit-error probabilities, a geometric optimization algorithm, and information theoretic definitions of reliable and secure communication. The geometric optimization problem aims at minimizing the total jamming power required to achieve reliability and secrecy constraints given the problem's geometry. It is important to note that the output of this optimization is some set of minimal activity fractions for all jammers, whose deployment does *not* require coordination between jammers on when to transmit.

Related Work. The wire-tap channel [31] has been considered within information theory [11, 14, 24, 29]: a single eavesdropper attempts to listen in on a legitimate communication between a pair of nodes. It is shown that perfect secrecy is possible when the eavesdropper's channel is worse than the legitimate channel. Prior work has considered the use of jammers to degrade the eavesdroppers' channel and has analyzed the channel capacity under various scenarios, such as cooperating or independent jammers, multiple eavesdroppers, etc. Within this same model of eavesdroppers, game-theoretic approaches for optimizing power consumption of jammers have been studied [6], as has the problem of designating regions where eavesdroppers cannot be located. Most of these prior works do not explore the geometry of the problem and are primarily of theoretical interest because of the simple scenarios considered.

Jamming has been considered as a possible security measure [8, 9, 16], designed to address the fact that RFID devices are extremely limited in power, making the use of cryptography difficult. Most works address the security of only a single RFID tag. Wireless sensor networks are another example of systems with low-capability devices; while, in many cases, cryptography is possible here [17], the focus has been on symmetric key cryptography due to the more resource-intensive nature of asymmetric key cryptography. Here, the primary problem occurs during the key distribution phase [23], where eavesdropping is still possible. It is, thus, viable to consider physical layer techniques in the context of sensor networks. On an interesting side note, [13] presents a method for securing against impersonation attacks in sensor networks by jamming nodes that are sent impersonated packets, in order to prevent receipt of the packets.

Only a few works consider the geography/geometry of the environment for security purposes. The model upon which this paper is based is presented in [19], where the authors present primarily theoretical results on power optimization and jammer placement. In addition, several other related works where the objective is to protect geographically restricted communication exist. Sheth *et al.* [22] present a method using directional antennas together with coding packets across multiple transmitters in order to define a secure region of coverage. Here, the region of coverage is restricted to the intersection of the ranges of the antennas. Tiwari holds a patent [26] for a method in which jammers are placed around a wireless network to secure it. However, security is achieved through active jamming and, thus, requires coordination between transmitters and jammers. In contrast, our methods do not require any coordination between jammers and legitimate nodes. Finally, using a model very similar to the one in this paper, Kim *et al.* [10] present an experimental study on how to create a secure zone around an access point using multiple friendly jammers. Tippenhauer *et al.* [25] show that the impact of friendly jamming can be eliminated using (carefully placed) multiple antennae; a potential ad-

vantage of our approach is to make such countermeasures less effective.

Gollakota *et al.* [4] have also used such a well-coordinated communication between source and jammers. These methods have significant advantages, but require reactive jammers (i.e., jammers synchronized with other jammers) and a flexible physical layer. None of these assumptions are required for our work.

Vilela and Barros [28] showed that without any assumptions on jammers and eavesdroppers' location, one could still use other nodes as friendly jammers, as long as they avoid co-transmitting with the legitimate transmitter and in the vicinity of a common destination. The authors show how to abstract this setting as a graph, and how to find an optimal subset of nodes using ILP. In [30] the authors study asymptotic behaviour in a stochastic setting in which jammers and eavesdroppers are at randomly distributed locations. In particular they study the concept of *Secure Throughput*, which is based on the probability that a message is successfully received only by the legitimate receivers.

Recently [21] suggested an elegant method for establishing friendly jamming where friendly nodes are able to communicate while enemy nodes are prevented from doing so. The idea is that a signal generated according to a secret key could appear as noise when key is not known. Gollakota *et al.* [4] have also used such a well-coordinated communication between source and jammers. These methods have significant advantages, but requires reactive jammers (that is, jammers synchronized with other jammers) and a flexible physical layer. None of theses assumptions are required for our work.

Finally, [2] studied schemes similar to our assumptions. They showed that allocating (optimally) equal-power jammers is an NP-hard problem and provided a PTAS for this problem. They have also provided an efficient scheme for pruning significant portions of the fence (see definitions below) so that various optimization problems can be addressed more efficiently.

Contributions. We measure the effect of jamming by modeling channel quality using the *bit-error probability* (BEP), which is a fundamental measure able to capture any specific scenario governing the physical layer. This new characterization of the jamming signals allows to improve the jamming quality via information-security codes tailored for the specific geometric setup. In particular, we present an algorithm that given a geometric and physical-layer setup finds the coding parameters that guarantee private reliable communication. To the best of our knowledge, this is the first time in jammer optimization where the optimal code parameters are found jointly with the assignment of the jammers' activity. The BEP framework is introduced in Section 2, and further developed in Section 3. In Section 4 we show that given the problem geometry it is possible to translate infeasible jamming specifications to a feasible specification by changing the coding parameters, without loss of security, reliability or communication rate. We then translate this possibility to efficient polynomial-time algorithms for computing optimal jammer parameters to meet the specifications, while minimizing energy requirements. The validity and efficiency of our scheme is shown through simulations in Section 5.

2. MODELS AND TOOLS

In this section we detail the settings within which the paper's results are obtained. We first introduce the models and tools pertaining to the *geometric* setup, then the *communications* model that drives the new temporal-jamming framework. The geometric model we use is essentially the same as considered in [19], with some adaptations. Using an established geometric model is a convenient choice, given that the key novelty of this paper lies in the tailoring of a wieldy communications model to practical geometric settings.

2.1 Geometric model and tools

Modeling communication in geographically restricted locations, we consider a *Storage/Fence* environment model, similar to the one in [19]. A depiction of this model is given in Fig. 1:

- We partition the region of interest into two (not necessarily connected) regions: the *controlled region*, $\mathcal{C}$, and its complement, the *uncontrolled region*, $\mathcal{U}$. Eavesdroppers may exist in $\mathcal{U}$ but not in $\mathcal{C}$. A polygonal fence $\mathcal{F}$ separates $\mathcal{U}$ from $\mathcal{C}$.
- Legitimate communication is enclosed within a polygonal region, or a set of polygonal regions, $\mathcal{S} \subset \mathcal{C}$, called the *storage*. The reader may wish to think of the storage as a warehouse containing items emitting sensitive information, e.g. RFID tags, sensors etc. Legitimate receivers and transmitters may be located at any point within $\mathcal{S}$. Note that $\mathcal{S}$ is in the controlled region.
- A set $\mathcal{J}$ of friendly jammers are placed in the region $\mathcal{A} = \mathcal{C} \setminus \mathcal{S}$, termed the *allowable region*. Note that jammers are not placed outside of the controlled area, since they could be destroyed physically, and they cannot be placed inside the storage $\mathcal{S}$, since they might interfere with legitimate communications.

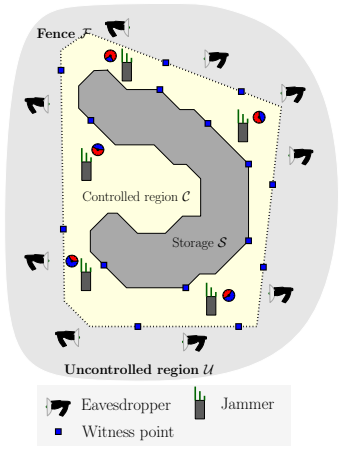


Figure 1. *An example scenario with a storage (dark gray) containing the communicating nodes, and surrounded by a fence (dotted). Jammers are placed within the controlled regions prevent eavesdroppers outside the fence from listening.*[1]

We believe that this model is applicable to multiple scenarios at which some geographic buffer zone separates the transmitting nodes from the potential eavesdroppers.

With a slight abuse of notation, we identify a node (receiver/jammer/eavesdropper) by its location p in $\mathbb{R}^2$. Con-

sider a potential eavesdropper located at a point p in the uncontrolled region $\mathcal{U}$. Note that if any point $q \in \mathcal{S}$ may contain a transmitter, then for any communication model where reception quality is inversely proportional to distance, the highest risk of information leak heard by p is from the transmitter located at the nearest point to p from all storage point. Let us denote this point as $\mathsf{s}(p)$. That is, $\|p-\mathsf{s}(p)\| \leq \|p-q\|, \forall q \in \mathcal{S}$, where $\|a-b\|$ is the Euclidean distance between the two points a, b. Also assume that a set of jammers $\mathcal{J}$ is placed in $\mathcal{A}$.

Witness points. A major component in our toolbox is the *discretization* obtained by assigning only a polynomial relatively small number of *witness points* with the property that if required lower (resp. upper) bounds on jamming intensity are satisfied at these points, then the required conditions also hold for any point inside the storage (resp. outside the fence). It is clear that the number of these witness points we consider in lieu of the entire regions of interest affects the performance of the optimization algorithms dramatically. The operator can specify a tuning parameter $\varepsilon > 0$ trading accuracy vs. number of witness points and algorithmic efficiency. Given a parameter ε, we seek a set $\mathcal{W} = \{w_1 \dots w_m\}$ of witness points in $\mathcal{U}$ such that for every point $p \in \mathcal{U}$, there is a witness point $w_i \in \mathcal{W}$ satisfying $\|p - \mathsf{s}(p)\| \leq (1+\varepsilon)\|w_i - \mathsf{s}(w_i)\|$. Moreover, $\|p-j\| \leq (1+\varepsilon)\|w_i-j\|$ for every jammer location $j \in \mathcal{J}$. In other words, for every potential eavesdropper $p \in \mathcal{U}$ (within the continuous domain), there is a witness point $w \in \mathcal{W}$ such that the distances from either p or w to the nearest legitimate transmitter are nearly equal. An analogous condition holds for a set of witness points within the storage, whose distances to the jammers are nearly equal to the distances between the legitimate receivers and the jammers. As shown in [19], such sets of witness points can be found with sizes equal to $\{(n+|\mathcal{J}|)\log(d)\}^2$ where d is the ration between $diam(\mathcal{F})$ and the minimum distance between storage and fence. Such polynomial-size sets of witness points imply the possibility to run jammer optimization algorithms on these sets with jamming guarantees on the true locations of receivers and eavesdroppers, for any jamming function that is "well behaved", e.g. inverse proportional to a polynomial of distance r) in small intervals $(r, r(1+\varepsilon))$. We note that all the jamming functions we consider in this paper indeed have this smoothness property.

2.2 Comm. model: temporal jamming

In this sub-section we introduce the *temporal jamming* model driving the jamming optimization results that follow. Temporal jamming refers to the ability of jammers to transmit the jamming signal intermittently, in fine time resolution of a single bit. This is in contrast with the more common *complete-duration* jammers, whose signals are set to be constant in time. We note from the outset that the benefits of temporal jamming shown later in the paper do *not* assume coordination between jammers, neither between jammers and transmitters. Rather, we only assume that each jammer is able to set its activity in time to a static value that is determined by the environment's geometry. To link the temporal-jamming model with the main thread of existing work, we first review the complete-duration jamming model.

Complete-Duration Jamming. When a jammer transmits a continuous signal at a certain power, it is convenient to formulate the jamming optimization in terms of *Signal to Interference Ratios* (*SIR*) at locations within the environment's geometry. Successful jamming is achieved if the *SIR* observed at all potential eavesdropper locations are below some specified threshold.

Formally, we express the signal decay due to path loss as follows: for an eavesdropper p_e listening to a transmitter $p_s \in \mathcal{S}$, the received power is $\tilde{P}\|p_s - p_e\|^{-\gamma}$, where $\tilde{P}$ is the transmitter's signal power and γ is the path-loss exponent. A similar formulation can be made for the received power at legitimate nodes, and for received jamming signal power. Recalling that for an eavesdropper p_e the nearest point on the storage is denoted $\mathsf{s}(p_e)$, we have

$$SIR(\mathcal{J}, p_e) = \frac{\tilde{P}\|\mathsf{s}(p_e) - p_e\|^{-\gamma}}{\max_{j\in\mathcal{J}} \hat{P}\|j - p_e\|^{-\gamma}},$$

where $\hat{P}$ is the jammer transmit power, and neglecting noise and the interference from the non-nearest jammers. An analogous (but slightly different) expression can be given for the *SIR* at legitimate-receiver locations.

The natural way to identify successful jamming is through an upper threshold, δ_1, on *SIR* for eavesdroppers, and a lower threshold, δ_2, on *SIR* for legitimate receivers. Thresholds on *SIR* are the widely accepted *"physical model"* described in [5]. Formally, any set of complete-duration jammers $\mathcal{J}$ needs to satisfy the following constraints

$$SIR(\mathcal{J}, p_e) \leq \delta_1, \forall p_e \in \mathcal{U} \text{ and} \quad (1)$$

$$SIR(\mathcal{J}, p_s) \geq \delta_2, \forall p_s \in \mathcal{S}. \quad (2)$$

Temporal Jamming. Moving from complete-duration to temporal jammers, it is clear that we can no longer use the *SIR* measure, as it carries no notion of temporal activity. To capture the temporal activity, we will work with the most fundamental communication unit: a *bit*, and its corresponding measure of equivocation: the *bit-error probability*[1]. Since jammers' activity is characterized as being on/off at a single-bit resolution, it is natural to measure the jamming quality by the bit-error probability induced upon an eavesdropper. Given a jammer active at some bit instant, the probability that it flips a bit at an eavsdropper location will be calculated based on a physical model considering signal and propagation characteristics. Later, this error probability will also include the randomness of whether a jammer is on or off at a given bit instant, assuming jammer activity epochs are drawn at random by each jammer independently. Formally, we denote by $\mathsf{BEP}(p)$ the bit-error probability at point p induced by a set of active jammers. We emphasize that the $\mathsf{BEP}(p)$ function captures the raw physical errors observed by the receivers, before any coding is considered, but after factoring in *all the assumptions* on the physical layer (modulation, antenna type, receiver sensitivity, etc). Clearly the function $\mathsf{BEP}(p)$ will depend on the number of active jammers and their position with respect to p. A detailed discussion of the functions $\mathsf{BEP}(p)$ is given in Section 3. When the bit-error probability considers random jammer activity in addition to the randomness of the communication medium, we denote it by $\mathsf{TBEP}(p)$. As an example, consider a single jammer that induces a bit-error probability of $\mathsf{BEP}(p)$ at point p when it is active. If this

[1]The same model extends readily from a bit to a higher-order symbol without fundamental changes.

jammer is active at bit instants i.i.d. with probability η, then the effective bit-error probability at point p will be $\mathsf{TBEP}(p) = \eta\mathsf{BEP}(p)$. In a similar way we can incorporate random partial-activity jamming into more involved scenarios with more than one jammer.

3. BIT-ERROR PROBABILITY

In the temporal jamming communications model that we described above, we wish to induce a high bit-error probability at eavesdropper locations, while keeping a low enough bit-error probability within the storage. To this end we defined the bit-error probability at point p using the abstract function $\mathsf{BEP}(p)$. In this section we further develop the model to discuss the properties of $\mathsf{BEP}(p)$ functions. The properties of a $\mathsf{BEP}(p)$ function will depend on whether p is in $\mathcal{S}$ or in $\mathcal{U}$, and on the number of jammers affecting the bit reception at p. Bit errors result from both the decay of the signal in space, and from the incidence of the jamming signal at the receiver. For points in $\mathcal{S}$ we assume below that signal decay is negligible, but this assumption is for convenience rather than necessity. For points in $\mathcal{U}$, which have larger distance from the transmitters in $\mathcal{S}$, the $\mathsf{BEP}(p)$ functions will incorporate both jamming and signal decay.

We now describe the $\mathsf{BEP}(p)$ functions from the simplest scenario of no jammers (only signal decay), followed by the single-jammer and multiple-jammers scenarios.

No Jammers. In the absence of jamming activity, bit errors are caused by the decay of communication signals in space. For legitimate receivers within $\mathcal{S}$, since we assume that the decay is negligible, the bit-error probability without jamming is identically zero. (We reemphasize that this assumption is only for ease of exposition, and not an essential one for the schemes to work.) For an eavesdropper at location $p_e \in \mathcal{U}$, a message is received with bit-error probability that depends on its distance to the transmitter. For the transmitter location we take the point in $\mathcal{S}$ closest to p_e, which is denoted $\mathsf{s}(p_e)$. Then we write the jamming-free bit-error probability at p_e as

$$\mathsf{BEP}_{\text{free}}(p_e) = f_F(\|\mathsf{s}(p_e) - p_e\|), \tag{3}$$

where $f_F(\cdot)$ is a monotone non-decreasing function. $f_F(\cdot)$, as all the bit-error probability functions in the paper, admits values in $[0, 0.5]$. Bit-error probabilities above 0.5 are clearly not practically interesting.

A Single Jammer. At times when a jammer is active in location p_j, the noise it emits introduces bit-error events in addition to errors due to signal decay. The bit-error probability at location $p_e \in \mathcal{U}$ is in this case a function combining the two sources of bit errors

$$\mathsf{BEP}(p_e) = f(\|\mathsf{s}(p_e) - p_e\|; \|p_j - p_e\|), \tag{4}$$

where $f(\cdot;\cdot)$ is monotone non-decreasing in its left argument and monotone non-increasing in its right argument.
For legitimate receivers within $\mathcal{S}$ we assume negligible signal decay, so for these locations the bit-error probability is a function of jamming interference only

$$\mathsf{BEP}(p_s) = f_I(\|p_j - p_s\|), \tag{5}$$

where $f_I(d)$ can be regarded as a special case taking $f(0; d)$.

Multiple Jammers. For the case of multiple jammers *active at the same bit instant*, a bit-error event may be caused by any of the jammers, as well as by signal decay. To accommodate for multiple jammers, we extend the function $f(\cdot;\cdot)$ in (4) to have multiple right arguments

$$\mathsf{BEP}(p_e) = f(\|\mathsf{s}(p_e) - p_e\|; \|p_{j_1} - p_e\|, \|p_{j_2} - p_e\|, \ldots). \tag{6}$$

We mainly consider in this paper the case where f is symmetric in its right arguments, i.e., the bit-error probability depends on the jammers only through their distances to p_e (or p_s). This assumption is equivalent to equal-power jammers in the *SIR* model. At this point it is instructive to explain how the functions f_F, f_I, f are obtained in practice. There are different ways to do it, and the choice depends on the design stage at which the functions are needed. For the initial design of the system, one may use common communications models (power-decay with AWGN noise, fading etc.) to come up with estimates on these functions given some reasonable assumptions on the physical layer and communication medium. At a later stage when jammer activity assignments actually need to be decided, the exact system specifications are known, and so real measurements can yield f_F, f_I and f with good precision. In both cases we get an accurate characterization of the fundamental communication reliability that is better than known coarse characterizations such as SIRs. In Section 4.1 we give an example of natural parameterized functions for f_F, f_I, for which the modelling and measurement techniques mentioned above could be used to find the values of a small number of parameters per each system.

3.1 Decompositions and bounds for the BEP functions

For some optimization tasks, we would want to decompose the function f from (6) to separable functions in f's arguments. The main advantage of separability is in making f easier to measure and estimate in a deployed system. It is much easier to obtain the bit-error probability as a function of a single variable (e.g. distance to a single jammer) than as a complex function of multiple distances. When it is too complex to separate the effects of the multiple arguments, we use separable functions that give upper and lower bounds on f. The upper bounds allow to guarantee low enough error probabilities for legitimate receivers, and the lower bounds guarantee high enough error probabilities at eavesdropper locations.

When the bit-error probability is caused by a single active jammer, we use the interference-only function from (5)

$$\mathsf{BEP}_{\text{jam}}(p_e) = f_I(\|p_j - p_e\|),$$

where we recall that $f_I(\cdot)$ is a monotone non-increasing function admitting values in $[0, 0.5]$. Now we wish to combine the single-jammer interference-only bit-error probability with that from signal decay given in (3). In order for a bit to be received in error, it needs to be flipped by either signal decay or by jamming interference, but not both. Assuming independence between the two error mechanisms, the resulting bit-error probability is

$$\mathsf{BEP}(p_e) = f_F(1 - f_I) + f_I(1 - f_F) = f_F + f_I - 2f_F f_I, \tag{7}$$

where f_F and f_I are short notations for $f_F(\|\mathsf{s}(p_e) - p_e\|)$ and $f_I(\|p_j - p_e\|)$, respectively. Since for any $f_F, f_I \leq 0.5$

we have $f_F + f_I - 2f_F f_I \geq \max[f_F, f_I]$, we get the following lower bound on the error probability

$$\mathsf{BEP}(p_e) \geq \max\left[f_F(\|\mathsf{s}(p_e) - p_e\|), f_I(\|p_j - p_e\|)\right]. \quad (8)$$

In addition to its simplicity, the max lower bound of (8) has the advantage that it is not specific to the independent bit flipping error model assumed in (7), but can rather be justified for other physical error sources.

Similarly, we can use the max function to combine the bit-error probabilities from multiple jammers, yielding the lower bound

$$\mathsf{BEP}_{\text{jam}}(p_e) \geq \max_{j\in J} f_I(\|p_j - p_e\|). \quad (9)$$

The multi-jammer error probability can again be combined with the decay error probability, obtaining the lower bound

$$\mathsf{BEP}(p_e) \geq \max\left[f_F(\|\mathsf{s}(p_e) - p_e\|), \max_{j\in J} f_I(\|p_j - p_e\|)\right]. \quad (10)$$

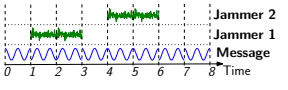
For eavesdropper locations we are interested in bounding the combined error probability from below, such that a jammer assignment guarantees no less than a certain amount of equivocation. Hence the right-hand side of (10) can replace the true bit-error probability requirement without loss of correctness. In contrast, for legitimate-receiver locations we look to bound the error probability from *above*, such that the actual error probability observed by legitimate clients is not worse than some guaranteed value. Consequently, for a legitimate-receiver location $p_s \in \mathcal{S}$ we may choose the sum combining, which is an obvious upper bound on the true combined error probability

$$\mathsf{BEP}(p_s) = \mathsf{BEP}_{\text{jam}}(p_s) \leq \sum_{j\in J} f_I(\|p_j - p_s\|). \quad (11)$$

Here the right-hand side of (11) can replace, without loss of correctness, the true bit-error probability requirement for legitimate receivers.

3.2 Partial-activity jammers

Now that we have set the basic formal infrastructure for calculating and bounding bit-error probabilities given a jammer setup, we move to treat partial-activity jammers, which are the key component of the temporal-jamming framework. A partial-activity jammer j transmits its jamming signal for an $\eta_j \in [0,1]$ fraction of the time. In the remaining $1-\eta_j$ fraction of time, the jammer is idle and does not contribute to the equivocation of the eavesdroppers and legitimate receivers. In the simplest case we assume that the jammer's activity on bit instants is drawn as i.i.d Bernoulli random variables with probability η_j. Consequently, a jammer is added as a right-argument to $f(\cdot;\cdot)$ at bit instants when it is drawn active, and excluded at other time instants. An example of activity instants of two jammers is given in the figure on the right, where Jammers 1 and 2 actively transmit for the duration of two bits at different times during the transmission of a message.



The design problem at hand is to set the activity fractions η_j of the deployed jammers to meet the privacy requirements induced by the system's geometry. Note that the random selection of activity instants simplifies the system operation, and in particular, no coordination is required between jammers.

The Two Nearest Jammer (2NJ) model. For solving various optimization problems addressed in this paper, we use either the NJ model (*nearest jammer*) or the 2NJ model (*two nearest jammers*). In 2NJ, the jamming impact of the third jammer and beyond on a point p could be neglected. This assumption is justified by the rapid decay of power with distance. Define $d_s(p) \triangleq \|\mathsf{s}(p) - p\|$, i.e., the distance from p to the nearest point on $\mathcal{S}$. The combined bit-error probability from two partial-activity jammers j_1, j_2 affecting p is calculated as

$$\begin{aligned}
&\mathsf{TBEP}(p, j_1, j_2) = \\
&\qquad (1-\eta_{j_1})(1-\eta_{j_2}) \cdot f_F(d_s(p)) && (12)\\
&\qquad +\eta_{j_1}(1-\eta_{j_2}) \cdot f(d_s(p); \|p_{j_1} - p\|) && (13)\\
&\qquad +\eta_{j_2}(1-\eta_{j_1}) \cdot f(d_s(p); \|p_{j_2} - p\|) && (14)\\
&\qquad +\eta_{j_1}\eta_{j_2} \cdot f(d_s(p); \|p_{j_1} - p\|, \|p_{j_2} - p\|). && (15)
\end{aligned}$$

Note that the expressions in (12)–(15) correspond to *disjoint* time instants within the transmission block. Hence combining with a sum is without loss of correctness. When $p = p_s$ is a location in the storage, we have $d_s(p_s) = 0$, and the left argument of each of the f functions in (13)–(15) is not applied while (12) is identically zero.

The motivation to stop at two nearest jammers, besides the decay of received power, is the decreasing probability $\eta_{j_1}\eta_{j_2}\eta_{j_3}\cdots$ to have a large number of simultaneous active jammers.

To achieve successful jamming, we need to satisfy the following constraints simultaneously

$$\mathsf{TBEP}(p_e, j1(p_e), j2(p_e)) \geq \tau_1, \ \forall p_e \in \mathcal{U}, \quad (16)$$

$$\mathsf{TBEP}(p_s, j1(p_s), j2(p_s)) \leq \tau_2, \ \forall p_s \in \mathcal{S}, \quad (17)$$

where $j1(p), j2(p)$ are the two nearest jammers to p, and τ_1 (resp. τ_2) is the lower (resp. upper) threshold of bit-error probability in $\mathcal{U}$ (resp. $\mathcal{S}$) locations. The solution should be given as an assignment to $\eta_1, \ldots, \eta_{|\mathcal{J}|}$ satisfying (16)–(17), with minimal total activity $\sum_{j=1}^{|\mathcal{J}|} \eta_j$.

4. ALGORITHMS FOR JAMMER ACTIVITY ASSIGNMENT

The purpose of this section is to provide constructive tools to find jammer activity assignments that satisfy the requirements of (16)–(17). The first such tool is called *threshold shifting*, which allows choosing "the best" pair of thresholds τ_1, τ_2 from all pairs that are equivalent in terms of the communication rate. The second tool are algorithms to solve the activity assignment problem for the NJ and the 2NJ models.

4.1 Threshold shifting through information-theoretic security

The principal benefit of working with the bit-error probability measure is its fundamental relations with *information theory*. These relations allow to cleverly employ information *coding* to aid the feasibility and efficiency of friendly jamming in a given geometric setup. In the sequel we show that geometric setups that do not admit a feasible assignment of η_j activity values to jammers, may be solved by shifting the lower and upper thresholds τ_1, τ_2 to values that are more favorable in terms of the geometric setup. Building on coding techniques, we are able to perform such a shift while allowing the same communication rate between legitimate nodes in the storage.

To see how coding fits in the solution, we examine the bit-error probability constraints in (16)–(17). While the left-hand side TBEP functions in the constraint inequalities are governed by the geometric setup of the problem, the right-hand side thresholds τ_1, τ_2 originate from informational – and not physical – features of reliable communication. In other words, the claim that τ_1 and τ_2 are sufficient thresholds must be backed by a code that provably guarantees that legitimate nodes can communicate reliably, while eavesdroppers gain no information from their received signals. As a corollary to that, it is possible to change the thresholds τ_1, τ_2 by changing the code used for communications. We call this operation threshold shifting. Suppose we have a code that gives the correct guarantees given a threshold pair τ_1, τ_2. Then we run an optimization algorithm to find η_j's that satisfy these thresholds. It may be the case that there is no feasible assignment to η_j's given τ_1, τ_2. Then we may look for an alternate pair τ_1', τ_2', for which a different code with the same rate exists, and solve a different optimization problem, with better success this time.

We briefly sketch the information-theoretic principles underlying threshold shifting and the associated code design problem. A detailed constructive treatment is deferred to future work. In information-theoretic terminology, communication between a transmitter and a legitimate receiver in location p_s in the storage is done over a *binary symmetric channel* (BSC) with parameter $\mathsf{TBEP}(p_s)$ given in (5). A BSC with parameter γ flips any bit i.i.d. with probability γ. Similarly, the communication between a transmitter and an eavesdropper in location p_e is done over a BSC with parameter $\mathsf{TBEP}(p_e)$ given in (6). The BSC is the most fundamental channel model, and a heavily studied one in information theory. For a BSC with parameter γ, it is known [20] that a communication rate of $1 - h(\gamma)$ is achievable using coding, and also optimal, where $h(\cdot)$ is the binary entropy function. This limiting rate $1 - h(\gamma)$ is called the *capacity* of the BSC. The scenario of a legitimate receiver communicating over one BSC with an eavesdropper communicating over another (worse) BSC is also a well studied problem in information theory called the *wire-tap channel* [31]. It is well known [27] that it is possible to communicate reliably with a legitimate receiver, while leaving the eavesdropper in complete equivocation, at a rate that is at most the difference

$$\Delta = \text{Capacity}(\mathsf{TBEP}(p_s)) - \text{Capacity}(\mathsf{TBEP}(p_e)). \quad (18)$$

In other words, we can change the bit-error probabilities of the legitimate receiver and the eavesdropper, and maintain the same communication rate so long as the difference between the respective channel capacities is maintained. Since both bit-error probabilities go in the same direction (either both upward or both downward), we refer to this operation as threshold shifting. To fit this into the jammer-activity optimization problem, we replace the individual TBEP values in (18) with the thresholds τ_1 (for p_e), and τ_2 (for p_s). The following example shows the potential of threshold shifting.

Example. Assume a simple configuration of a single legitimate node (denoted s), a single jammer (denoted j), and a single eavesdropper (denoted e) given in the Fig. 2. The distance between s and j is d_1, and the distance between j and e is d_2. Suppose the f functions governing the bit-error probabilities are given as follows. Bit error-probability due

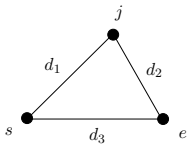


Figure 2. *The geometric layout of the legitimate node (s), the jammer (j), and the eavesdropper (e) in the example.*

to signal decay at distance x from the source is given by

$$f_F(x) = \frac{1}{2}\left[1 - e^{-\alpha_F x^{\gamma_F}}\right].$$

Bit error-probability due to interference at distance y from the jammer is given by $f_I(y) = \frac{1}{2}e^{-\alpha_I y^{\gamma_I}}$. The constants α_F, γ_F, α_I, γ_I allow fitting the functions to measured values in the particular system. For any choice of these parameters we have the desired properties that $f_F(0) = 0$, $f_I(0) = 0.5$, reflecting, respectively, no errors at the source and complete equivocation at the jammer. At the limit of distances going to infinity the behaviors are inverted, where f_F is tending to 0.5 and f_I is tending to 0. For the legitimate receiver s we assume to only have bit-error probability contribution from f_I (recall that s is located in a relatively small storage, hence very proximate to the transmitter). For the eavesdropper location e we have contributions from both functions, which we combine with the max function, as shown in (8). Altogether, assuming a jamming signal active at a η fraction of time, we have

$$\mathsf{TBEP}(s,j) = \eta f_I(d_1) = \frac{1}{2}\eta e^{-\alpha_I d_1^{\gamma_I}}$$

and

$$\begin{aligned}\mathsf{TBEP}(e,j) &= (1-\eta)f_F(d_3) + \eta \max\left[f_F(d_3), f_I(d_2)\right] \\ &= f_F(d_3) + \eta \max\left[f_I(d_2) - f_F(d_3), 0\right] \\ = \frac{1}{2}\left[1 - e^{-\alpha_F d_3^{\gamma_F}}\right. &+ \left.\eta \max\left[e^{-\alpha_I d_2^{\gamma_I}} + e^{-\alpha_F d_3^{\gamma_F}} - 1, 0\right]\right].\end{aligned}$$

Now with the closed-form expressions for $\mathsf{TBEP}(s,j)$ and $\mathsf{TBEP}(e,j)$ above, the jammer needs to set the activity factor η to guarantee that $\mathsf{TBEP}(e,j)$ is *above* some specified threshold τ_1 and $\mathsf{TBEP}(s,j)$ is *below* some specified threshold τ_2. The jammer's selection of η is best explained with a concrete numerical example. Suppose the measured parameters for propagation and jamming are found to be $\alpha_F = 0.1$, $\gamma_F = 2$, $\alpha_I = 3$, $\gamma_I = 2$. In addition, the distances of the problem are $d_1 = 0.8$, $d_2 = 0.6$, $d_3 = 0.9$. Then we can substitute these values into the f_I and f_F functions, and obtain in Fig. 3 the values of $\mathsf{TBEP}(s,j)$ (solid diagonal line) and $\mathsf{TBEP}(e,j)$ (dashed diagonal line) as a function of η. Given specified TBEP thresholds

$$\tau_1 = 0.1,\ \tau_2 = 0.03,$$

the solid vertical line in Fig. 3 marks the upper boundary of η values that satisfy $\mathsf{TBEP}(s,j) \le \tau_2$ (these values are marked by the shaded region on the bottom left). Similarly, the dashed vertical line marks the lower boundary of η values that satisfy $\mathsf{TBEP}(e,j) \ge \tau_1$ (these values are marked by the shaded region on the top right). It is clear from the figure that the intersection between the η values of the left and right regions is empty, hence there is no η that can satisfy both constraints, and jamming is impossible with these

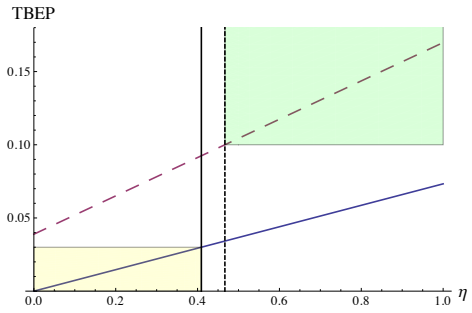


Figure 3. $\mathsf{TBEP}(s,j)$ *(solid) and* $\mathsf{TBEP}(e,j)$ *(dashed) as a function of* η*. Shaded regions represent* η *values that satisfy* $\mathsf{TBEP}(s,j) \le \tau_2$ *(bottom-left) and* $\mathsf{TBEP}(e,j) \ge \tau_1$ *(top right). The intersection between allowed* η *values is empty.*

parameters. Now we show that using the threshold shifting technique, jamming will become possible *without any loss in information rate*. We choose the alternative thresholds $\tau_1' = 0.163,\ \tau_2' = 0.07$ which satisfy

$$\text{Capacity}(\tau_2') - \text{Capacity}(\tau_1') = h(\tau_1') - h(\tau_2') = 0.275.$$

This difference is identical to

$$\text{Capacity}(\tau_2) - \text{Capacity}(\tau_1) = h(\tau_1) - h(\tau_2) = 0.275.$$

Therefore, the same rate of communication (between legitimate nodes) can be maintained with the alternative thresholds, only changing the code used for communication. As a result, we repeat in Fig. 4 the same TBEP functions from Fig. 3, only this time marking the allowed regions specified by τ_1' and τ_2'. It can be observed in Fig. 4 that now the

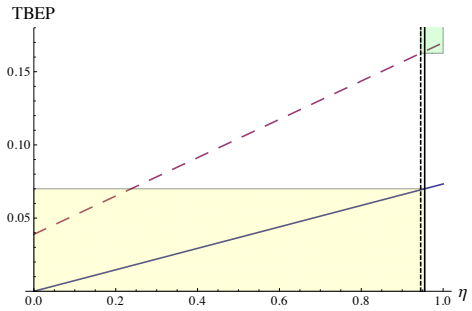


Figure 4. *The same* $\mathsf{TBEP}(s,j)$ *and* $\mathsf{TBEP}(e,j)$ *functions, now with shaded regions marking* η *values allowed by the shifted thresholds* τ_1' *and* τ_2'*. The intersection between allowed* η *values is non-empty.*

bottom-left and top-right shaded regions do intersect on η values between 0 and 1; hence, jamming is possible with these shifted thresholds.

This example can, of course, be generalized to much more complex jamming scenarios, as we see later in Section 5.

4.2 Computing $(\eta_1, \ldots, \eta_{|\mathcal{J}|})$ under the nearest-jammer model

Given a set of jammers $\mathcal{J}$ in specified locations, and a pair of threshold values τ_1, τ_2, we wish to set the activity fractions $\eta_1, \ldots, \eta_{|\mathcal{J}|}$ of the jammers to guarantee bit-error probability of at least τ_1 at eavesdropper locations, and at most τ_2 at locations in the storage. In addition to satisfying the bit-error probability thresholds, to save power we wish to achieve that with the lowest possible total activity sum $\sum_{j=1}^{|\mathcal{J}|} \eta_j$.

First we handle the nearest jammer model. That is, each point, on the storage or outside the fence, is influenced by the nearest jammer to the point, while more remote jammers' impact is neglected. The problem is, as above, to determine the values η_j for each jammer $j \in \mathcal{J}$.

1. Compute the set of witness points $\mathcal{W}$ as explained in Section 2.
2. Compute the Voronoi Diagram of $\mathcal{J}$, in $O|\mathcal{J}|\log|\mathcal{J}|)$ time (see [3]) .
3. Using the Voronoi Diagram, for each point in $\mathcal{W}$ find the nearest jammer in $\log|\mathcal{J}|$ time. Denote by $\mathcal{W}_j \subseteq \mathcal{W}$ the set of witness points whose nearest jammer is $j \in \mathcal{J}$.
4. For each $j \in \mathcal{J}$, compute L_j, the minimal η_j value that meets the $\mathsf{TBEP} \ge \tau_1$ threshold for all $p \in W_j \cap \mathcal{U}$.
5. For each $j \in \mathcal{J}$, compute U_j, the maximal η_j value that meets the $\mathsf{TBEP} \le \tau_2$ threshold for all $p \in W_j \cap \mathcal{S}$.
6. If for every $j \in \mathcal{J}$, $L_j \le U_j$ output $\eta_j = L_j$. If not, output "failure".

4.3 Computing $(\eta_1, \ldots, \eta_{|\mathcal{J}|})$ under the 2-nearest jammer model

Let $j1(p)$ (resp., $j2(p)$) be the first (resp., second) closest jammer to point p. Hence, $\{j1(p), j2(p)\} = 2NJ(p)$. Now we need to satisfy the constraints

$$\mathsf{TBEP}(p_e, j1(p_e), j2(p_e)) \ge \tau_1,\ \forall p_e \in \mathcal{W} \bigcap \mathcal{U}, \qquad (19)$$

$$\mathsf{TBEP}(p_s, j1(p_s), j2(p_s)) \le \tau_2,\ \forall p_s \in \mathcal{W} \bigcap \mathcal{S}. \qquad (20)$$

We need to find an assignment to $\eta_1, \ldots, \eta_{|\mathcal{J}|}$ satisfying (19)–(20), with minimum total activity $\sum_{j=1}^{|\mathcal{J}|} \eta_j$. Note that this model is more involved than the single nearest jammer model, since the values η_j depend on each other. To overcome the computational difficulty, we use the geometric structure of the problem as follows. We assume the problem layout satisfies the *circular order assumption* (Figure 5): the jammers can be ordered $\mathcal{J} = (j_1, j_2, \ldots)$ such that each TBEP constraint involves either a single jammer j_i or a pair of jammers j_i, j_k, and furthermore, if a witness point $w \in \mathcal{W}$ is influenced by j_i (together with possibly another jammer), then no witness point w' is influenced by j_{i_1}, j_{i_2}, where $i_1 < i < i_2$. (Jammer indices wrap around, from $|\mathcal{J}|$ back to 1.) The implication is that once the values of η_i, η_k are fixed, then the values of $\eta_{i+1}, \ldots \eta_{k-1}$ (within the $[i,k]$ interval of indices) can be computed independently from the values of $\eta_{k+1}, \eta_{k+2} \ldots \eta_{i-1}$ (outside the $[i,k]$ interval of indices).

In the 2NJ model, the circular assumption amounts to some very natural topological assumptions on the shapes of the storage and warehouse, e.g. being simply connected. With this assumption, the region of influence of j_i on $\mathcal{S}$ and $\mathcal{U}$ may overlap with the regions of influence of j_{i-1} and j_{i+1}, but no other jammers.

Under the circular assumption, the solution can be simplified greatly with the following dynamic program. Let the η values be taken from a finite set D. For fixed value of η_i, η_j let $I_{i,j}(\eta', \eta'')$ be defined as *TRUE* if for $\eta_i = \eta', \eta_j = \eta''$ there is an assignment of $\eta_{i+1}, \eta_{i+2} \ldots \eta_{j-1}$ from D such that all inequalities that involve these indices are satisfied. (Recall that indices wrap from $|J|$ back to 1.) Note that

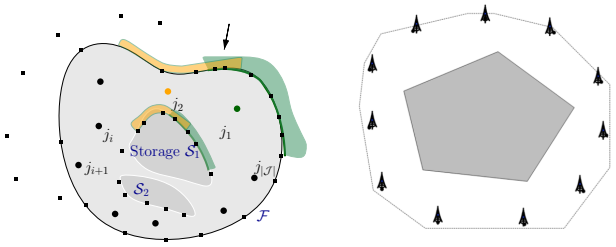


Figure 5. **Left** *An example of a setting in which the circular assumption holds. Squares indicate the witness points of $\mathcal{W}$. Jammers are indicated by disks. The portion of the fence and (boundary of) storage influenced by the orange jammer j_2 (resp., green jammer j_1) are highlighted in orange (resp., green). The arrow indicates a fence point influenced by both jammers.* **Right** *The Storage/Fence environment used in the simulations.*

$I_{ij}(\eta', \eta'') = TRUE$ and $I_{jk}(\eta'', \eta''') = TRUE$ imply that $I_{ik}(\eta', \eta''') = TRUE$.

The algorithm first computes $I_{i,i+1}(\eta', \eta'')$ for all $\eta', \eta'' \in D$ and $i = 1, 2, 3 \ldots$, then merges this data to compute $I_{i,i+2}(\eta', \eta'')$ for $i = 1, 3, 5 \ldots$ and so on. In each iteration the number of pairs considered is halved compared to the preceding iteration. Therefore, the time complexity is $O(|\mathcal{J}||D|^2 \log |\mathcal{J}|)$. Note that the storage $\mathcal{S}$ does not have to be connected, and could contain several components ($\mathcal{S}_1, \mathcal{S}_2$ in this example),

5. SIMULATION RESULTS

The goal of the following simulation study is to evaluate the new temporal-jamming framework in complex realistic jamming scenarios. The results build strongly on the tools developed in Section 4: they use the efficient algorithms for finding optimal jamming-activity assignments, and they reveal the benefits of the threshold-shifting technique. The Storage/Fence environment model used in the study is depicted in Figure 5. In this model, eleven friendly jammers are located along the fence (dotted) to protect the communications of nodes within the storage (gray). In the following, we use the 2NJ model with the f_F and f_I functions given in the example of Section 4.1. We fix three of the propagation and jamming parameters to $\gamma_F = \gamma_I = 2$ and $\alpha_I = 0.4$. The fourth parameter, α_F, is varied to model different scenarios. A small α_F implies slow decay of the information signals, and thus corresponds to poor separation between the storage and the fence, while a large α_F corresponds to better separation and an "easier" jamming problem. This can be seen in Fig. 6(a), where, given an upper threshold τ_2, a higher lower threshold τ_1 is achieved as α_F grows. Fig. 6(b) shows the delta capacity, which amounts to the achievable communication rate, as a function of the prescribed τ_2 value. This plot shows that for low α_F parameters, it is beneficial to raise (shift) τ_2 sufficiently in order to reach the maximum rate. Hence, it is seen that threshold shifting may be beneficial to overcome more challenging jamming scenarios. Fig. 6(c) and Fig. 6(d) provide information on the η values assigned by the optimal algorithm for each prescribed τ_2 value. Fig. 6(c) shows the maximum of the η_j values among the jammer set $\mathcal{J}$, and Fig. 6(d) shows the average over $\mathcal{J}$. These plots explain why Figs. 6(a,b) flatten out for large τ_2 values: due to saturation of jammer activity values, it becomes impossible to increase τ_1 further, regardless of the allowable τ_2.

6. CONCLUSION

In this paper, we considered the joint optimization problems arising out of the usage of friendly jammers for securing communication in a flexible manner, i.e., choosing jamming parameters optimally based on space as well as time. Our results are based on a new communication framework using the bit-error probability as a quality metric.

We first showed the benefits of temporal jamming where jammers' activity on individual bit instants are drawn as i.i.d Bernoulli random variables independent of other jammers. This scheme can be easily extended to the domain of multiple jamming frequencies. Next, we showed how to transform infeasible jamming specifications to feasible ones without any impact to security, reliability and communication rate by changing the coding parameters. Based on this, we presented two polynomial time approximation algorithms for computing jammers' activity parameters with a $(1+\varepsilon)$-approximation of the best achievable energy consumption. Our results demonstrate the benefits of choosing coding parameters in conjunction with assigning jammers' activity to efficiently manage secure reliable communication.

Acknowledgment A. Efrat was partially supported by the National Science Foundation (CNS-1017114). G. Grebla was partially supported by the Defense Threat Reduction Agency grant HDTRA 1-13-1-0021. E. Arkin and J. Mitchell were partially supported by the National Science Foundation (CCF-1018388) and by the US-Israel Binational Science Foundation (Grant 2010074).

7. REFERENCES

[1] D. S. Alberts, J. J. Garstka, and F. P. Stein. Network centric warfare: Developing and leveraging information superiority. Technical report, DTIC Document, 2000.

[2] E. Arkin, Y. Cassuto, A. Efrat, G. Grebla, J. S. B. Mitchell, S. Sankararaman, and M. Segal. Optimal placement of protective jammers for securing wireless transmissions in a geographic domain. In *ACM IPSN*, 2015.

[3] M. de Berg, M. Van Kreveld, M. Overmars, and O. C. Schwarzkopf. *Computational geometry*. Springer, 2000.

[4] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. *ACM SIGCOMM Computer Communication Review*, 41(4):2–13, 2011.

[5] P. Gupta and P. R. Kumar. The capacity of wireless networks. *IEEE Trans. Inf. Theory*, 46(2):388–404, 2000.

[6] Z. Han, N. Marina, M. Debbah, and A. H. rungnes. Physical layer security game: Interaction between source, eavesdropper, and friendly jammer. *EURASIP Journal on Wireless Communications and Networking*, 2009(1):452907, 2009.

[7] M. Hendry. *Multi-application Smart Cards: Technology and Applications*. Cambridge University Press, 2007.

[8] A. Juels and J. Brainard. Soft blocking: flexible blocker tags on the cheap. In *Proc. 2004 ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 1–7, 2004.

[9] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *Proc. 8th ACM CCS*, pages 103–111, 2003.

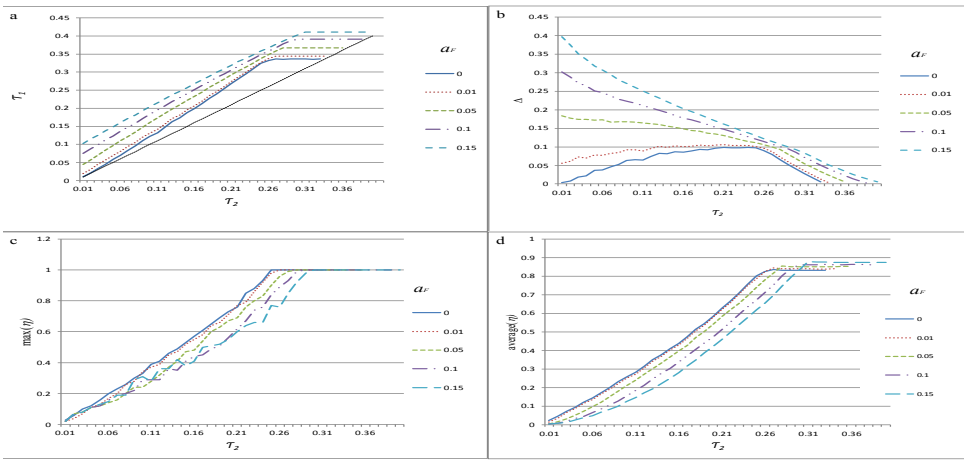


Figure 6. *Simulation results. For different α_F values, (a) presents the maximum achieved τ_1 threshold given τ_2. (b) presents the delta capacity, which is equivalent to the achievable communication rate. (c-d) present the maximum jammer activity and the average jammer activity versus τ_2, respectively.*

[10] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In *ACM Symposium on Information, Computer and Communications Security*, ASIACCS '12, 2012.

[11] L. Lai and H. E. Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, 2008.

[12] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. In *Proc. 1st International Workshop on Wearable and Implantable Body Sensor Networks*, pages 55–58, 2004.

[13] I. Martinovic, P. Pichota, and J. B. Schmitt. Jamming for good: a fresh approach to authentic communication in wsns. In *Proc. ACM conference on Wireless network security*, WiSec, 2009.

[14] R. Negi and S. Goel. Secret communication using artificial noise. In *Proc. IEEE 62nd VTC*, pages 1906–1910, 2005.

[15] J. Nehmer, M. Becker, A. Karshmer, and R. Lamm. Living assistance systems: an ambient intelligence approach. In *Proc. 28th ICSE*, pages 43–50, 2006.

[16] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. RFID systems: A survey on security threats and proposed solutions. In *Personal Wireless Communications*, volume 4217 of *LNCS*, pages 159–170. Springer, 2006.

[17] A. Perrig, J. A. Stankovic, and D. Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.

[18] R. A. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House, 2011.

[19] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal. Optimization schemes for protective jamming. In *Proc. 13th ACM MobiHoc*, pages 65–74, 2012.

[20] C. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(9):379–423, Oct. 1948.

[21] W. Shen, P. Ning, X. He, and H. Dai. Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *IEEE Symp. on Security and Privacy*, 2013.

[22] A. Sheth, S. Seshan, and D. Wetherall. Geo-fencing: Confining wi-fi coverage to physical boundaries. In H. Tokuda, M. Beigl, A. Friday, A. Brush, and Y. Tobe, editors, *Pervasive Computing*, volume 5538 of *Lecture Notes in Computer Science*, pages 274–290. Springer Berlin Heidelberg, 2009.

[23] M. A. Simplício Jr., P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho. A survey on key management mechanisms for distributed wireless sensor networks. *Computer Networks*, 54(15):2591–2612, 2010.

[24] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference assisted secret communication. *IEEE Trans. Inf. Theory*, 57(5):3153–3167, 2011.

[25] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. On limitations of friendly jamming for confidentiality. In *IEEE Security and Privacy (SP)*, pages 160–173, 2013.

[26] S. Tiwari. Wireless perimeter security device and network using same. US Patent 7917945, 2011.

[27] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. Information Theory*, 43(2):712–714, 1997.

[28] J. P. Vilela and J. Barros. Collision-free jamming for enhanced wireless secrecy. In *IEEE (WoWMoM)*, pages 1–6, 2013.

[29] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Wireless secrecy regions with friendly jamming. *IEEE Trans. Inf. Forensics Security*, 6(2):256–266, 2011.

[30] J. P. Vilela, P. C. Pinto, and J. Barros. Jammer selection policies for secure wireless networks. In *IEEE Communications (ICC)*, pages 1–6, 2011.

[31] A. D. Wyner. The Wire-tap Channel. *Bell Systems Technical Journal*, 54(8):1355–1387, 1975.