Secure Communication through Jammers Jointly Optimized in Geography and Time[1]

Yair Allouche

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

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

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, 150 Broadway, Cambridge, MA 02142, USA

Michael Segal

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

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.

1. Introduction

More and more, highly sensitive and private information is being transferred via wireless communication. Example systems include contactless smart cards [11], military sensor networks [1], emergency response systems employing wireless networks [19], and ambient living-assistance systems [24]; these systems use wireless communication to

[1] Extended abstracts of this paper appeared as parts in [2] and [3].

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 [23, 34]. 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 [27]. 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. For example, in a hospital, one might desire to protect sensors' data, at least from tapping from outside the patient's room, while assuming that tapping from within the same room is much more noticeable and daring. 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 [27].

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

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

Problems 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.

We consider different aspects of the optimization problem that addresses how to optimize (temporal or fixed-duration) jammers effectiveness via improving their placements. We believe that this would pave the way to global all-parameters optimizations.

Contributions.

1. We consider two communication models in this paper for complete-duration and temporal jammers respectively: (i) a static model in which channel quality is measured using the *signal-to-interference ratio* (*SIR*), and (ii) a model which measures the temporal 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. The latter 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 7.
2. Given a discrete set of potential eavesdropper locations and a geographic domain comprised of a discrete set of communication regions (such as buildings in a warehouse complex), we highlight the hardness of the placement problem. Specifically, even if all jammers have equal power and characteristics, and each point is effected only by nearest jammer (*NJ-model*), it is NP-hard to minimize the number of jammers necessary to protect the domain. However, given similar assumptions, we present, for any fixed $\varepsilon > 0$, a polynomial-time $(1+\varepsilon)$-approximation algorithm (i.e., a *polynomial-time approximation scheme* (PTAS)) for placing a minimum cardinality set of fixed-power jammers in the NJ-interference model.
3. Given a continuous geographic domain where eavesdroppers may be located, we present a "pruning" method which reduces this to a discrete set of potential eavesdropper locations so that the solution to this "reduced" problem closely approximates the solution to the original problem. This allows us to obtain more efficient solutions, by decreasing the number of constraints needed in integer linear programming (ILP) solutions to optimal jammer placement problems. For example, in the Full-interference model, it is shown in [28, 29] that the problem of either **(i)** finding a subset of equal-power jammers (taken from a discrete subsets $\mathcal{A}$ of possible locations), or **(ii)** assigning powers to each jammer for a given set of jammer locations, can be solved using ILP for the former problem and LP for the latter one. With the "pruning" approach, we show that the number of constraints in these is independent of the area of the geographic domain.

Related Work. The wire-tap channel [41] has been considered within information theory [17, 23, 34, 39]: 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 [10], 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 [25, 14, 13], 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 [26], 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 [12], 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, [20] 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 [28], 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. Deca *et al.* [6] showed how to use friendly jamming to guaranty reliable vehicle-basestation communication. Sheth *et al.* [32] 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 [36] 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.* [15] present an experimental study on how to create a secure zone around an access point using multiple friendly jammers. Tippenhauer *et al.* [35] show that the impact of friendly jamming can be eliminated using (carefully placed) multiple antennae; a potential advantage of our approach is to make such countermeasures less effective. Gollakota *et al.* [8] 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. We mention here that none of these assumptions are required for our work. Vilela and Barros [38] 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 [40] the authors study asymptotic behavior 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. The paper [31] 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. Finally, recently Siyari et al. [33] considered joint optimization of artificial noise (AN) and information signals in a MIMO wiretap interference network, wherein the transmission of each link may be overheard by several MIMO-capable eavesdroppers and tackled the problem by game theory concepts.

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 [28], 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 [28]. 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.

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 $\mathbb{R}^2$. Consider 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. The closer the transmitter q is to the eavesdropper is at p, the the 'louder' is transmissions are received at p. Let us denote by $\mathsf{s}(p)$ the closest point of $\mathcal{S}$. See illustation in Fig. 1 Right. That is,

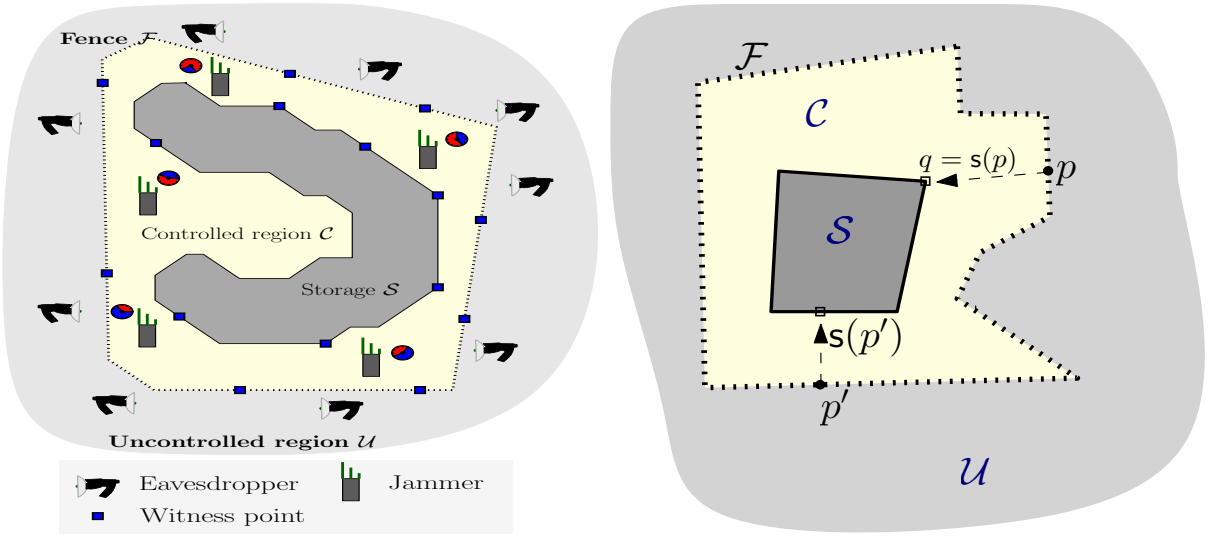

Figure 1. Left: *An example scenario with a storage (dark gray) containing the communicating nodes, and surrounded by a fence (dotted). Jammers are placed within the controlled regions prevent eavesdroppers outside the fence from listening.*[1]. **Right:** *A illustrations showing two possible locations p and p' (resp.) of eavesdroppers, and the nearest storage points $\mathsf{s}(p)$ and $\mathsf{s}(p')$ (resp.)*

$\|p-\mathsf{s}(p)\| \leq \|p-q\|, \forall q \in \mathcal{S}$, 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 the allowable region $\mathcal{A}$ (between the storage $\mathcal{S}$ and the fence $\mathcal{F}$).

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 their nearest legitimate transmitters 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 [28], 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. Communication 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 $\gamma > 0$ 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 [9]. Formally, any set of complete-duration jammers $\mathcal{J}$ needs to satisfy the following constraints

$$SIR(\mathcal{J}, p_e) \leq \delta_1, \forall p_e \in \mathcal{U} \text{ and} \tag{1}$$
$$SIR(\mathcal{J}, p_s) \geq \delta_2, \forall p_s \in \mathcal{S}. \tag{2}$$

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*[2]. 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 eavesdropper 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 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.

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

3.1. 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.

3.2. A Single Jammer

Here we assume that each point q is influenced by at most a single jammer which is active at q, while the effect of other jammers are neglectable at q.

During active times for a jammer at location p_j, its jamming signal 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 $f(0; d)$.

3.3. 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.

3.4. 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)

$$\mathsf{BEP}_{\text{jam}}(p_e) = f_I(\|p_j - p_e\|), \tag{7}$$

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

$$\mathsf{BEP}(p_e) = f_F(1 - f_I) + f_I(1 - f_F) = f_F + f_I - 2f_F f_I, \tag{8}$$

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

$$\mathsf{BEP}(p_e) \geq \max\left[f_F(\|\mathsf{s}(p_e) - p_e\|), f_I(\|p_j - p_e\|)\right]. \tag{9}$$

In addition to its simplicity, the max lower bound of (9) has the advantage that it is not specific to the independent bit flipping error model assumed in (8), 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

$$\mathsf{BEP}_{\text{jam}}(p_e) \geq \max_{j \in J} f_I(\|p_j - p_e\|). \tag{10}$$

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

$$\mathsf{BEP}(p_e) \geq \max\left[f_F(\|\mathsf{s}(p_e) - p_e\|), \max_{j \in J} f_I(\|p_j - p_e\|)\right]. \tag{11}$$

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 (11) 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

$$\mathsf{BEP}(p_s) = \mathsf{BEP}_{\text{jam}}(p_s) \leq \sum_{j \in J} f_I(\|p_j - p_s\|). \tag{12}$$

Here the right-hand side of (12) can replace, without loss of correctness, the true bit-error probability requirement for legitimate receivers.

3.5. 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 Fig. 2, 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.

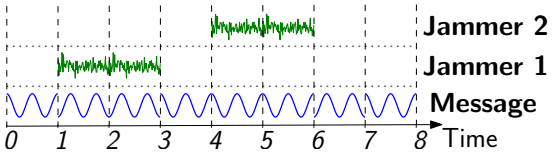

Figure 2. Jammers 1 and 2 actively transmit for the duration of two bits at different times during the transmission of a message. The transmissions of both jammers help to achieve the required bit-error probabilities.

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. Let $d_s(p) \triangleq \|\mathsf{s}(p) - p\|$, 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

$$\begin{aligned}
&\mathsf{TBEP}(p, j_1, j_2) = \\
&\qquad (1-\eta_{j_1})(1-\eta_{j_2}) \cdot f_F(d_s(p)) && (13)\\
&\qquad +\eta_{j_1}(1-\eta_{j_2}) \cdot f(d_s(p); \|p_{j_1} - p\|) && (14)\\
&\qquad +\eta_{j_2}(1-\eta_{j_1}) \cdot f(d_s(p); \|p_{j_2} - p\|) && (15)\\
&\qquad +\eta_{j_1}\eta_{j_2} \cdot f(d_s(p); \|p_{j_1} - p\|, \|p_{j_2} - p\|). && (16)
\end{aligned}$$

Note that the expressions in (13)–(16) 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 (14)–(16) is not applied while (13) 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

$$\mathsf{TBEP}(p_e, j1(p_e), j2(p_e)) \geq \tau_1, \ \forall p_e \in \mathcal{U}, \quad (17)$$
$$\mathsf{TBEP}(p_s, j1(p_s), j2(p_s)) \leq \tau_2, \ \forall p_s \in \mathcal{S}, \quad (18)$$

where $j1(p), j2(p)$ are the two nearest jammers to p, and τ_1 (resp. τ_2) is the lower threshold (resp. upper bound) 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 (17)–(18), 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 (17)–(18). 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 (17)–(18). 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 [30] 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* [41]. It is well known [37] 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

$$\Delta = \text{Capacity}(\mathsf{TBEP}(p_s)) - \text{Capacity}(\mathsf{TBEP}(p_e)). \tag{19}$$

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 (19) 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. 3. The distance between s and j is d_1, and the distance between

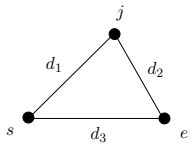

Figure 3. *The geometric layout of the legitimate node (s), the jammer (j), and the eavesdropper (e) in the example.*

j and e is d_2. Suppose the f functions governing the bit-error probabilities are given as follows. Bit error-probability due to signal decay at distance x from the source is given by

$$f_F(x) = \frac{1}{2}\left[1 - e^{-\alpha_F x^{\gamma_F}}\right]. \tag{20}$$

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 (9). 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

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

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. 4 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

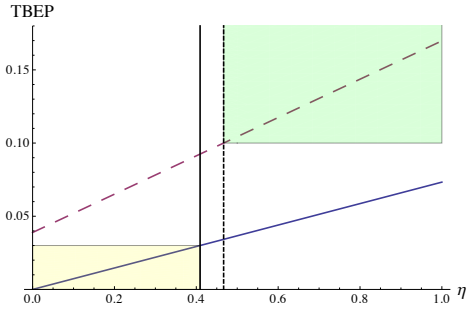

Figure 4. $\mathsf{TBEP}(s,j)$ *(solid) and* $\mathsf{TBEP}(e,j)$ *(dashed) as a function of* η*. Shaded regions represent* η *values that satisfy* $\mathsf{TBEP}(s,j) \le \tau_2$ *(bottom-left) and* $\mathsf{TBEP}(e,j) \ge \tau_1$ *(top right). The intersection between allowed* η *values is empty.*

Fig. 4 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 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. 5 the same TBEP functions from Fig. 4, only this time marking the allowed regions specified by τ_1' and τ_2'. It can be observed in Fig. 5

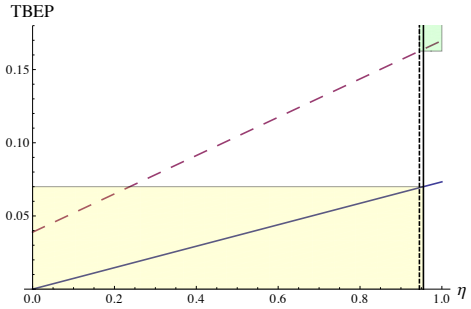

Figure 5. *The same* $\mathsf{TBEP}(s,j)$ *and* $\mathsf{TBEP}(e,j)$ *functions, now with shaded regions marking* η *values allowed by the shifted thresholds* τ_1' *and* τ_2'*. The intersection between allowed* η *values is non-empty.*

that now the 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 7.

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

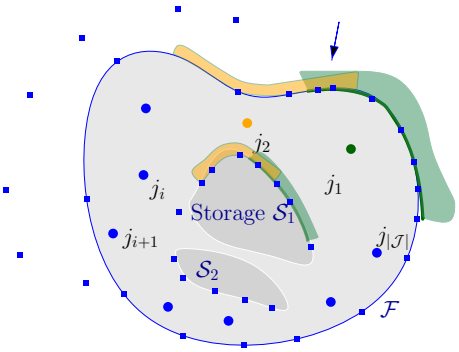

Figure 6. (a) An example of a setting in which the circular assumption holds. Squares indicate the witness points of $\mathcal{W}$. Jammers are indicated by disks. The portion of the fence and (boundary of) storage influenced by the orange jammer j_2 (resp., green jammer j_1) are highlighted in orange (resp., green). The arrow indicates a fence point influenced by both jammers.

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 [5]) .
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 TBEP $\geq \tau_1$ 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 TBEP $\leq \tau_2$ threshold for all $p \in W_j \cap \mathcal{S}$.
6. If for every $j \in \mathcal{J}$, $L_j \leq U_j$ 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

$$\mathsf{TBEP}(p_e, j1(p_e), j2(p_e)) \geq \tau_1, \ \forall p_e \in \mathcal{W} \bigcap \mathcal{U}, \tag{21}$$

$$\mathsf{TBEP}(p_s, j1(p_s), j2(p_s)) \leq \tau_2, \ \forall p_s \in \mathcal{W} \bigcap \mathcal{S}. \tag{22}$$

We need to find an assignment to $\eta_1, \ldots, \eta_{|\mathcal{J}|}$ satisfying (21)–(22), 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 6): 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 $I_{ij}(\eta', \eta'') = TRUE$ 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. Hardness of Optimal Jammers Placement

Next, we address the jammer placement problem, and assume other parameters of jammers (e.g. power or burst duration) are fixed and identical for all jammers.

To fully understand the difficulty of the problem, let us assume further that the nearest jammer models is used, and that $\tilde{P} = \hat{P}$ where $\tilde{P}$ is the transmitter's signal power. Substituting $\delta_1 = \delta_2 = 1$ in Equations (1) and (2) leads to the following formalization:

Opt-Placement Problem. Find a smallest cardinality set $\mathcal{J}$ of jammers, satisfying
1. $\|p_e - NJ_{\mathcal{J}}(p_e)\| \leq \|p_e - s(p)\|$ for every $p_e \in \mathcal{U}$, where $NJ_{\mathcal{J}}(p_e)$ is the jammer of OPT which is closest to p_e.
2. $OPT \subseteq \mathcal{A}$

The first condition implies that for any eavesdropper positioned in $\mathcal{U}$, and for every nodes in $\mathcal{S}$ that he tries to tap to, there is a jammer of OPT that jams this nodes *SIR*-wise. The second condition implies that jammers could be placed only on an allowable region $\mathcal{A} \subseteq \mathbb{R}^2$ (for example, not too close to $\mathcal{S}$, but still in the controlled region $\mathcal{U}$.)

We now show hardness of Opt-Placement Problem even in the case that the storage $\mathcal{S} \subset \mathbb{R}^2$ consists of multiple disconnected regions. It is sufficient to show this for the case when $\mathcal{S}$ is a set of points, eavesdroppers can be located only at a discrete set $\mathcal{E} \subset \mathbb{R}^2$ of points distinct from $\mathcal{S}$, and jammers can be placed anywhere in the plane (i.e., the allowable region $\mathcal{A} = \mathbb{R}^2$). Our reduction uses ideas from the NP-completeness proof of the problem Hitting-Set-for-Planar-Unit-Disks: *Given a set $\mathcal{D}$ of disks of equal radii in the plane and an integer k, compute whether there is a set $P \subseteq \mathbb{R}^2$ such that $D \cap P \neq \emptyset$ for all $D \in \mathcal{D}$ and $|P| \leq k$.* [21] The reduction employed in the NP-completeness proof of Hitting-Set-for-Planar-Unit-Disks is from the problem Planar-3-SAT [7].

Theorem 1. *Assume that the allowable region where jammers can be placed is $\mathcal{A} = \mathbb{R}^2$. Then, given a discrete set, $\mathcal{S}$, of storage regions and a discrete set, $\mathcal{E}$, of potential eavesdropper locations, disjoint from the regions $\mathcal{S}$,* Opt-Placement Problem *is* NP*-hard.*

Proof. For a given instance of Planar-3-SAT, the construction used in the proof of NP-completeness of Hitting-Set-for-Planar-Unit-Disks considers a specific set $\mathcal{D} = \{D_1, \ldots, D_m\}$ of unit disks in the plane, and these disks have the following property: Each disk appears as an arc of positive length on the boundary of the union, U, of the disks in $\mathcal{D}$. To compute a hitting set for $\mathcal{D}$, we can select one representative point per face of the arrangement of the m disks; therefore, it suffices for a hitting set to be selected as a subset of points on the faces of this arrangement.

From $\mathcal{D}$, we construct an instance of the problem Opt-Placement Problem as follows. First, we let $\mathcal{E}$ be the set of m centerpoints of the disks $\mathcal{D}$. Let U' denote the union of disks of radius $1 + \delta$, with $\delta > 0$ chosen small enough that U' has exactly the same combinatorial structure as U (the exact same arcs on each component of the boundary of the union). Within each connected component of the set $\mathbb{R}^2 \setminus U'$ (which consists of the "holes" in the union U' of disks, as well as the unbounded face outside U') we construct a simple polygon, which is one of the storage regions of the set $\mathcal{S}$, that touches each of the circular arcs bounding the face. (It is easy to see that such a polygon can be constructed having its number of vertices linear in the complexity of the face.) The set, $\mathcal{P}$, of such polygons has the property that if each member polygon is grown by δ (via Minkowski sum with a disk of radius δ), then, with the appropriate choice of δ_1, constraint (1) requires that there must be a jammer within each of the unit disks D_i centered at the points $\mathcal{E}$ in order to satisfy (1) at these points $\mathcal{E}$. In particular, each unit disk is in contact with the (up to 5) regions grown from polygons $\mathcal{P}$ corresponding to the faces to which the corresponding unit disk contributes an arc to the boundary of U. A minimum-cardinality set of jammers, then, corresponds precisely to an optimal hitting set for the disks $\mathcal{D}$. Thus, there exists a jamming set of size k if and only if there exists a hitting set for $\mathcal{D}$ of size k. □

6. Jammer Placement under the Nearest-Jammer Model – Positive Results

In this section, we present results for Opt-Placement Problem in both interference models. We are given a set, $\mathcal{S}$, of storage regions and a polygonal fence $\mathcal{F}$ enclosing $\mathcal{S}$. All jammers have fixed transmission power $\hat{P}$. We consider two possible cases for the allowable region, $\mathcal{A}$: **(i)** the continuous case, in which $\mathcal{A} = \mathcal{C} \setminus \mathcal{S}$ and we use the NJ-interference model (Section 6.2), and **(ii)** the discrete case, in which $\mathcal{A} \subset \mathcal{C} \setminus \mathcal{S}$ is a discrete set of candidate locations and we use the Full-interference model (Section 6.3). In both cases, we provide $(1 + \varepsilon)$-approximation schemes.

In the above settings, we first describe how to prune significant portions of $\mathcal{F}$. This will aid in bounding the running times of our algorithms. Following this, we describe our approximation schemes.

6.1. Pruning the Fence

In this section, we show how to discard portions of $\mathcal{F}$ (thereby reducing the controlled region $\mathcal{C}$) so that, at any point in the discarded portions, the *SIR* (under any interference model) is approximated by the *SIR* at some remaining location. Thus, if eavesdroppers located in the remaining portions are successfully jammed, any eavesdropper on $\mathcal{F}$, or anywhere outside $\mathcal{C}$ is also approximately successfully jammed. As stated, the *approximation* here means that Equation (2) and Equation (1) hold, after possibly multiplying one of the sides by a factor of $(1+\varepsilon)$.

We first give a few definitions. Let $\partial\mathcal{S}$ be the boundary of $\mathcal{S}$. For two points $p_s, q_s \in \partial\mathcal{S}$ that belong to the same polygon in $\mathcal{S}$, let $\overline{p_s q_s}$ denote the portion of $\partial\mathcal{S}$ obtained by walking counterclockwise from p_s to q_s. We define $\overline{p_e q_e}$ analogously for two points $p_e, q_e \in \mathcal{F}$. Let $\overline{p_i p_{i+1}} \subset \partial\mathcal{S}$ be a straight line edge on $\partial\mathcal{S}$ (that is, p_i, p_{i+1} are consecutive vertices of $\partial\mathcal{S}$) . The ***generalized Voronoi region***, denoted by $\mathsf{Vor}(\overline{p_i p_{i+1}})$ is the set $\{p \in \mathbb{R}^2 \mid \mathsf{s}(p) \in \overline{p_i p_{i+1}}\}$, where $\mathsf{s}(p)$ is the nearest point to p on $\mathcal{S}$. Similarly define the Voronoi region of each vertex p_i. The ***generalized Voronoi diagram*** $\mathsf{VD}(\mathcal{S})$ is the subdivision of $\mathbb{R}^2$ induced by the Voronoi regions of edges and vertices of $\mathcal{S}$. The ***restricted Voronoi Diagram*** $\mathsf{RVD}(\mathcal{S}, \mathcal{F})$ of $\mathcal{S}$ on $\mathcal{F}$ is the subdivision of $\mathcal{F}$ into segments induced by $\mathsf{VD}(\mathcal{S})$ together with the vertices of $\mathcal{F}$; see Figure 7 for an illustration.

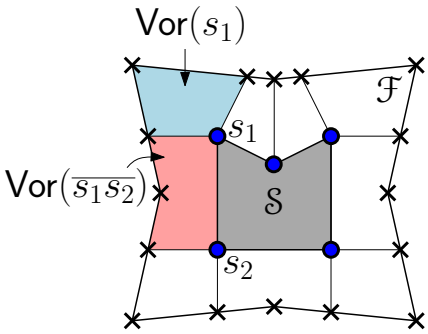

Figure 7. Generalized and Restricted Voronoi Diagrams.

The generalized Voronoi diagram is a well-studied structure in computational geometry [16, 18] and can be computed in $O(n \log n)$ time. Consequently, the restricted Voronoi diagram $\mathsf{RVD}(\mathcal{S}, \mathcal{F})$ can be computed in time $O(n^2)$.

Before describing the pruning process, let us emphasize the intuition behind its importance. Figure 8 illustrates two extreme yet realistic scenarios, of a fence that is significantly larger than the storage (Figure 8(a)), and a fence containing a sharp and long "spike" (Figure 8(b)). Theorem 2 (below) implies that in both cases we can solve the optimization problem while considering a much smaller fence, whose perimeter is proportional only to the perimeter of the storage, and does not contain such sharp angles.

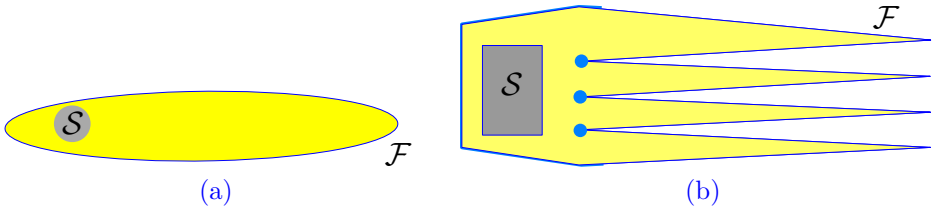

Figure 8. The solid lines represent the portion of the fence that needs to be considered, while the dashed lines represent portions that can be pruned and the thin dotted lines are the edges of the Voronoi diagram of $\mathcal{S}$ based on which the pruning is performed. (left) Original scenario, (middle) After pruning based on Lemma A.1, (right) After pruning based on Lemmas A.2 and A.3.

The output of the pruning process is a set, Ξ, of segments, which are edges of $\mathcal{F}$. The main result is the following theorem, whose proof is based on a series of lemmas associated with different stages of the process; see the Appendix for the lemmas and proofs. In specifying the bounds below, we assume, for simplicity, that distances are scaled so that the distance between the closest pair of points $p \in \mathcal{S}$ and $q \in \mathcal{F}$ is 1.

Theorem 2. *Given a set, $\mathcal{S}$, of storage regions, a fence $\mathcal{F}$ enclosing $\mathcal{S}$ such that eavesdroppers may lie on $\mathcal{F}$, we can generate a set of segments Ξ such that if a set $\mathcal{J}$ of jammers (not necessarily using the same transmission power) satisfies constraint (1) at all locations $p_e \in \xi$ for $\xi \in \Xi$, then (1) is satisfied at all locations in $\mathcal{F}$. Further,*

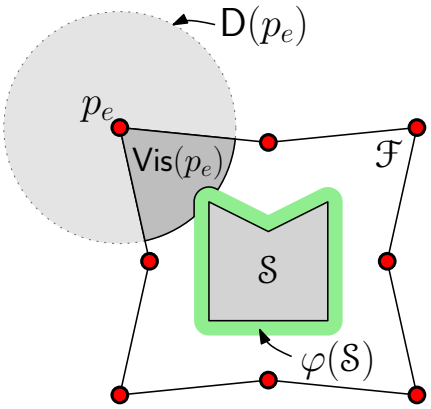

Figure 9. The forbidden region (marked in green) and visiblity regions for the case $\alpha = 1$

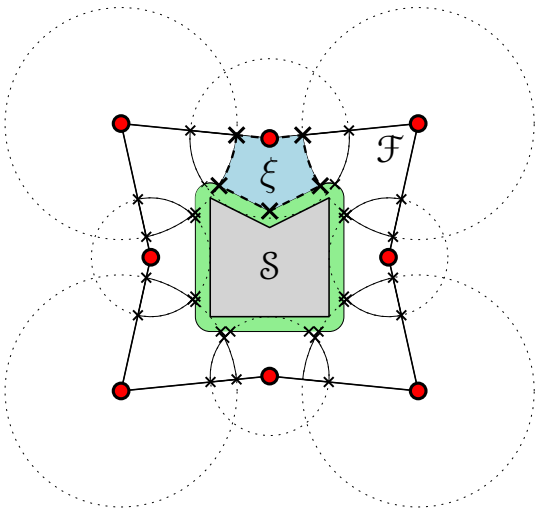

Figure 10. Arrangement of visibility regions

(i) Each segment $\xi \in \Xi$ is a subset of $\mathcal{F}$;
(ii) Any pair of segments in Ξ is disjoint; and,
(iii) $\sum_{\xi\in\Xi} |\xi| = O((\mathcal{L}_{\mathcal{S}} + n)/\varepsilon)$, where $|\xi|$ is the length of ξ, and n is the total complexity of $\mathcal{S}$ and $\mathcal{F}$.

6.2. Placement Within a Continuous Allowable Region

In this section, we present a $(1+\varepsilon)$-approximation bi-criteria approximation scheme under the NJ-interference model when the allowable region $\mathcal{A}$ is a continuous (but not necessarily connected) domain consisting of all the points in the controlled region $\mathcal{C}$ that are not too close to the storage $\mathcal{S}$, as formalized below.

We first present a few necessary definitions. Let $\hat{P}$ be the transmission power of a jammer and let $\tilde{P}$ be transmission power of the legitimate communication nodes. Let $\mathsf{D}[p;r]$ denote a disk of radius r centered at a point p. Also, let $\alpha = (\delta_1\hat{P}/\tilde{P})^{1/\gamma}$ and $\beta = (\delta_2\hat{P})^{1/\gamma}$ be two parameters useful in simplifying the exposition.

Definition 1. (i) The ***forbidden region*** $\varphi(\mathcal{S})$ is the region $\cup_{p_s\in\mathcal{S}}\mathsf{D}[p_s;\beta]$. This is essentially the Minkowski sum [4] of $\mathcal{S}$ with a disk with radius β. No jammer can lie in $\varphi(\mathcal{S})$ since it would cause too much interference to possible legitimate transmissions within $\mathcal{S}$.
(ii) The ***allowable region*** is $\mathcal{A} = \mathcal{C}\setminus\varphi(\mathcal{S})$. (Our algorithm straightforwardly generalizes to accommodate various other assumptions on the allowable and forbidden regions.)
(iii) For a point $p_e \in \mathcal{E}$, the ***critical disk*** is the disk $\mathsf{D}(p_e) = \mathsf{D}[p_e; \alpha\|\mathsf{s}(p_e) - p_e\|]$. Under the NJ-interference model, this disk must contain a jammer in order to prevent an eavesdropper at p_e from listening to transmissions within $\mathcal{S}$, and, in particular, to a transmitter placed in $\mathsf{s}(p_e)$.
(iv) For a point in $p_e \in \mathcal{F}$, the ***visibility region*** $\mathsf{Vis}(p_e)$ is the region $\mathsf{D}(p_e)\bigcup\mathcal{A}$. The *vertices* of $\mathsf{Vis}(p_e)$ are the non-differentiable points of $\mathsf{Vis}(p_e)$. Refer to Fig. 9

As is easily observed from the above discussion, successful jamming can be obtained by a set $\mathcal{J}$ of jammers if and only if for every point $p_e \in \mathcal{F}$, there is a jammer of $\mathcal{J}$ in $\mathsf{Vis}(p_e)$. Note that a successful jamming might not exist under the above constraints; for example, if β is too large (e.g. if δ_2 is too small) the forbidden region might contain essential portions of $\mathcal{F}$.

Arrangements. Given a discrete set, $\mathcal{E}'$, of points outside $\mathcal{C}$, let the ***arrangement*** $\mathbf{A}(\mathcal{E}', \mathcal{S}, \mathcal{F})$ denote the subdivision of $\mathbb{R}^2$ induced by the set of regions $\mathsf{Vis}(\mathcal{E}') = \{\mathsf{Vis}(p_e) \mid p_e \in \mathcal{E}'\}$. The *vertices* of $\mathbf{A}(\mathcal{E}', \mathcal{S}, \mathcal{F})$ are the intersection points of the visibility regions of points in $\mathcal{E}'$, together with the vertices of the visibility regions. An *edge* of $\mathbf{A}(\mathcal{E}', \mathcal{S}, \mathcal{F})$ is a portion of a visibility region between two vertices, and a *face* is a connected component of $\mathbb{R}^2\setminus\mathsf{Vis}(\mathcal{E}')$. The *complexity* of an arrangement is the total number of vertices, edges and faces; see Figure 10.

We first present an optimal algorithm for a restricted case that is useful in the analysis of the $(1+\varepsilon)$-approximation scheme for the general case.

6.2.1. An Optimal Algorithm for a Special Case

When $\mathcal{S}$ is a (straight-line) segment and $\mathcal{E}$ is another (straight-line) segment disjoint from $\mathcal{S}$, we can find an optimal set of jammers, i.e., one of minimum cardinality such that (2) and (1) are satisfied. Our algorithm is very similar to the algorithm presented in [28, 29] for the case of convex $\mathcal{S}$ and convex $\mathcal{F}$ enclosing $\mathcal{S}$, with $\alpha = 1$.

Apart from being an interesting case in which optimal results can be achieved, this algorithm is used in the analysis of our approximation algorithm for the general case (see Section 6.2.2) to bound the running time.

Let $\mathcal{E} = \overline{p_e q_e}$ and $\mathcal{S} = \overline{p_s q_s}$. The steps of the algorithm are as follows:

1. Initialize point $p = p_e \in \mathcal{E}$.
2. For the current point p, compute the next point, $p' \in \mathcal{E}$, to the right of p, such that $\mathsf{D}(p)$ and $\mathsf{D}(p')$ are tangential.
3. If $p' \in \mathcal{E}$, place a jammer at $\mathsf{D}(p) \bigcap \mathsf{D}(p')$, set p to p' and repeat steps 2 and 3.
4. If $p' \notin \mathcal{E}$, stop.

See Figure 11 for an illustration of one step of the algorithm, and Figure 12 for an illustration and the following step. Essentially, we compute a sequence of disks, covering $\mathcal{E}$, such that any two consecutive disks are tangential and the number of disks is at most $\mathsf{OPT} + 1$, where OPT is optimal number.

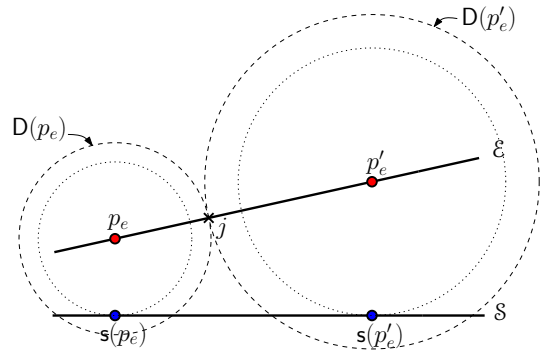

Figure 11. One step of the algorithm for disjoint segments, where $\alpha > 1$. The outer disks centered at p_e and p'_e are the critical disks of p_e and p'_e, and their radii are $\alpha\|\mathsf{s}(p_e) - p_e\|$ and $\alpha\|\mathsf{s}(p'_e) - p'_e\|$, respectively. The algorithm places a jammer j at the intersection point of these disks.

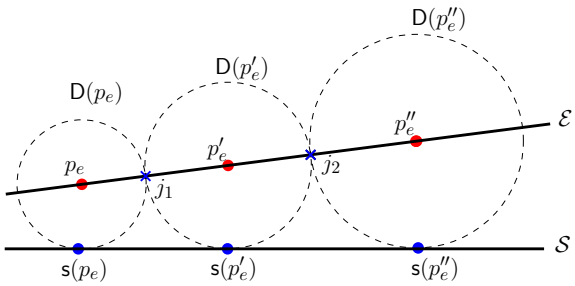

Figure 12. Two steps of the algorithm for disjoint segments, when $\alpha = 1$. Critical disks centred at p_e (resp. p'_e,p''_e) has radius $\|\mathsf{s}(p_e) - p_e\|$, (resp. $\|\mathsf{s}(p'_e) - p'_e\|, \|\mathsf{s}(p''_e) - p''_e\|$). The witness point p'_e is located such that $\mathsf{D}[p_e]$ and $\mathsf{D}[p'_e]$ are tangential, and the algorithm places the first jammer j_1 at $\mathsf{D}[p'_e] \cap \mathsf{D}[p''_e]$. The process then repeats for locating the second jammers j_2 and so on.

Theorem 3. *Given disjoint segments $\mathcal{S} = \overline{p_s q_s}$ and $\mathcal{E} = \overline{p_e q_e}$, we can place a set of at most $\mathsf{OPT} + 1$ jammers $\mathcal{J}$ in time $O(\mathsf{OPT})$ such that (i) $\forall p \in \mathcal{E}$, $SIR(\mathcal{J}, p) < \delta_1$ and (ii) $\forall p \in \mathcal{S}$, $SIR(\mathcal{J}, p) > \delta_2$.*

Proof. The proof follows from the arguments in [28, cf. Section 5]. □

We use the property that there are at most $\mathsf{OPT} + 1$ disks constructed during the course of the algorithm in the analysis of the approximation scheme in Section 6.2.2.

6.2.2. $(1 + \varepsilon)$-Approximation for the General Case

In this section, we present a bi-criteria polynomial-time approximation scheme where we allow some leeway in both the number of jammers as well as the *SIR* at each point on $\mathcal{E}$. The precise description of our result is given by the following theorem.

Theorem 4. *Given storage region(s) $\mathcal{S}$, fence $\mathcal{F}$, thresholds δ_2, δ_1 and jammer power $\hat{P}$, under the NJ interference model, we can compute locations $\mathcal{J} \subset \mathcal{A} \setminus \varphi(\mathcal{S})$ in time $O((T/\varepsilon^{O(1)})^{O(1/\varepsilon^2)})$, where $T = \min\{\mathcal{L}_{\mathcal{F}}^2, \mathcal{L}_{\mathcal{S}}^2, n^2\mathsf{OPT}^2\}$, such that $|\mathcal{J}| \leq (1+\varepsilon)\mathsf{OPT}$, and if jammers of power $\hat{P}$ are placed at $\mathcal{J}$, then*

(i) For any point $p_e \in \mathcal{F}$, $SIR(\mathcal{J}, p_e) < (1+\varepsilon)\delta_1$.

(ii) For any point $p_s \in \mathcal{S}$, $SIR(\mathcal{J}, p_s) > \delta_2$.

The overall idea of the algorithm is to compute a discrete set of *witness points* $\mathcal{E}' \subset \mathcal{E}$ such that the SIR at any point in $\mathcal{E} \setminus \mathcal{E}'$ is approximated by the SIR at some point in $\mathcal{E}'$. Thus, if we ensure that any point in $\mathcal{E}'$ is successfully jammed, we ensure that any point in $\mathcal{E}$ is "almost" successfully jammed, i.e., we are off the threshold by only a factor $(1+\varepsilon)$.

Algorithm Description. The algorithm consists of the following stages.

Stage (i). Generate witness points. The set $\mathcal{E}'$ of witness points is constructed in two steps. First, we obtain a set of segments Ξ from $\mathcal{F} = \partial\mathcal{C}$ according to Theorem 2 and add their endpoints to $\mathcal{E}'$. For each segment $\overline{p_e q_e}$ in Ξ, we then place witness points as described below in PLACE-WITNESSES. Let $\mathcal{E}'$ be the set of these points.

Stage (ii). Generate Candidate Jammer Locations: We now compute a discrete set of candidate jammer locations $\mathcal{J}'$ as follows: compute $\mathsf{Vis}(p_e)$ for each $p_e \in \mathcal{E}'$ and compute the arrangement $\mathcal{A}(\mathcal{E}', \mathcal{S}, \mathcal{F})$. For each face of the arrangement we pick an arbitrary point and add it to $\mathcal{J}'$.

Stage (iii). Find an almost-optimal set of jammers: Given discrete sets $\mathcal{E}'$ and $\mathcal{J}'$, the problem now transforms into the following discrete hitting set problem: *Given a discrete set of critical disks centered at points of $\mathcal{E}'$ and a discrete set of points $\mathcal{J}'$, compute a minimum cardinality subset $J \subset \mathcal{J}'$ such that every critical disk contains at least one point in J.* Although the minimum hitting set problem for disks is NP-Hard, we can obtain a $(1+\varepsilon)$-approximate solution using the method of Mustafa and Ray[22] in time $O(|\mathcal{E}'||J'|^{O(1/\varepsilon^2)})$. If there is no feasible solution to the hitting set problem, there is no feasible placement of jammers.

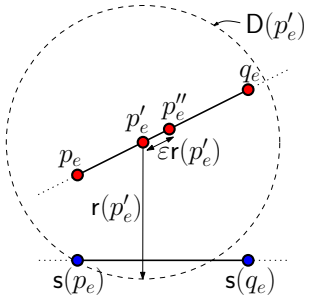

Figure 13. One step of procedure PLACE-WITNESSES

Procedure PLACE-WITNESSES(Ξ). Let $\overline{p_e q_e}$ be a segment in Ξ and without loss of generality, let $\|p_e - \mathsf{s}(p_e)\| < \|q_e - \mathsf{s}(q_e)\|$. We place witness points along $\overline{p_e q_e}$, starting at p_e, until we reach q_e. At an intermediate step, assume we are located at an already placed witness point $p'_e \in \overline{p_e q_e}$. Let $\mathsf{r}(p'_e)$ be the radius of the critical disk $\mathsf{D}(p'_e)$. We place a witness point p''_e on the portion $\overline{p'_e q_e}$ such that $\|p'_e - p''_e\| = \varepsilon'\mathsf{r}(p'_e)$, where ε' is chosen such that $(1+\varepsilon')^\gamma \leq (1+\varepsilon)$ and move to p''_e (see Figure 13). If $\|q_e - p'_e\| < \varepsilon'\mathsf{r}(p'_e)$, we terminate the procedure. Let the set of witness points placed for a segment $\overline{p_e q_e}$ be denoted by $\mathcal{E}'_{\overline{p_e q_e}}$.

Lemma 6.1. *For any segment $\overline{p_e q_e}$ and any point $p'_e \in \overline{p_e q_e}$, there exists a point $p''_e \in \mathcal{E}'_{\overline{p_e q_e}}$ such that, for any jammer $j \in \mathcal{J}$,*

$$SIR(j, p''_e) \leq \delta_1 \Rightarrow SIR(j, p'_e) \leq (1+\varepsilon)\delta_1.$$

Proof. Assuming without loss of generality that $\|p_e - \mathsf{s}(p_e)\| \leq \|q_e - \mathsf{s}(q_e)\|$, let p''_e be the point closest to p'_e on $\overline{p_e p'_e}$ implying that $\|p''_e - p'_e\| \leq \varepsilon'\alpha\|p''_e - \mathsf{s}(p''_e)\|$. If, for a jammer j, $SIR(j, p''_e) \leq \delta_1$, then $j \in \mathsf{D}[p''_e; \alpha\|p''_e - \mathsf{s}(p''_e)\|]$. Therefore,

$$\begin{aligned}\|p'_e - j\| &\leq \|p'_e - p''_e\| + \alpha\|p''_e - \mathsf{s}(p''_e)\| \\ &\leq (1+\varepsilon')\alpha\|p'_e - \mathsf{s}(p'_e)\|,\end{aligned}$$

since $\|p'_e - \mathsf{s}(p'_e)\| \leq \|p''_e - \mathsf{s}(p''_e)\|$. Now, since $(1+\varepsilon')^\gamma \leq (1+\varepsilon)$, by the choice of ε', the lemma is proved. □

We add to $\mathcal{E}'$ all points in $\mathcal{E}'_{\overline{p_eq_e}}$ for all $\overline{p_eq_e} \in \Xi$.

Analysis. It remains to bound the number of points in $\mathcal{E}'$. Clearly, since the minimum distance between $\mathcal{S}$ and $\mathcal{F}$ is 1, for each segment $\overline{p_eq_e}$, procedure PLACE-WITNESSES places $O(\|p_e - q_e\|/\varepsilon^{O(1)})$ witness points in $\mathcal{E}'$. Thus, a simple bound is $O(\mathcal{L}_\mathcal{F}/\varepsilon^{O(1)})$.

However, from Lemma A.3, we have that for any segment $\overline{p_eq_e} \in \Xi$ such that $\mathsf{s}(\overline{p_eq_e})$ is a vertex of $\mathcal{S}$, PLACE-WITNESSES places $O(1/\varepsilon^{O(1)})$ witness points in $\mathcal{E}'$. Combined with Theorem 2, we clearly have $O(\mathcal{L}_\mathcal{S}/\varepsilon^{O(1)})$ witness points placed by PLACE-WITNESSES.

We can also obtain a different bound independent of perimeters of $\mathcal{S}$ or $\mathcal{F}$ by a more complicated analysis.

Lemma 6.2. *For any segment $\overline{p_eq_e} \in \Xi \subseteq \mathcal{F}$ such that $\mathsf{s}(\overline{p_eq_e})$ is a single segment on $\mathcal{S}$,* PLACE-WITNESSES *places $O(\mathsf{OPT}/\varepsilon^{O(1)})$ witness points in $\overline{p_eq_e}$.*

Proof. Let $\theta = \theta_c(\overline{p_eq_e})$ be the critical angle (see Definition 2 in the Appendix) of $\overline{p_eq_e}$. Consider any two points p'_e, p''_e on $\overline{p_eq_e}$ such that $\mathsf{D}(p'_e)$ and $\mathsf{D}(p''_e)$ are tangential to each other and $\|p'_e - \mathsf{s}(p'_e)\| \leq \|p''_e - \mathsf{s}(p''_e)\|$. Then,

$$\alpha\|p''_e - \mathsf{s}(p''_e)\| = \alpha\|p'_e - \mathsf{s}(p'_e)\|(1+\sin\theta)/(1-\sin\theta).$$

Now, consider the set of points $\{p_{e,0}, p_{e,1}, \ldots, p_{e,k}\}$ such that $p_{e,0} = p'_e$ and

$$\alpha\|p_{e,i} - \mathsf{s}(p_{e,i})\| = \alpha\|p_{e,i-1} - \mathsf{s}(p_{e,i-1})\|(1+\sin\theta),$$

and k is the largest integer such that $p_{e,k}$ lies in between p'_e and p''_e on $\overline{p_eq_e}$.

Clearly, $p_{e,i}$ lies at the point of intersection of $\mathsf{D}(p_{e,i-1})$ and $\overline{p_eq_e}$. We can now see that $k = O(1/\varepsilon)$ from the fact that $\alpha\|p''_e - \mathsf{s}(p''_e)\| = \alpha\|p'_e - \mathsf{s}(p'_e)\|(1+\sin\theta)/(1-\sin\theta)$ and that $\sin\theta < 1/(1+\varepsilon)^{1/\gamma}$ for all segments in Ξ.

We now use the algorithm from Section 6.2.1, which computes a sequence of disks such that any two consecutive disks are tangential. From Theorem 3, it is clear that we can compute such a sequence of at most $O(\mathsf{OPT})$ disks to cover $\overline{p_eq_e}$.

For any disk in this set, PLACE-WITNESSES clearly places $O(1/\varepsilon^{O(1)})$ witness points. Thus, for a segment in Ξ, the total number of witness points in $\mathcal{E}'$ is $O(\mathsf{OPT}/\varepsilon^{O(1)})$. □

Putting it all together, we have $|\mathcal{E}'| = O(\sqrt{T}/\varepsilon^{O(1)})$ and $|\mathcal{J}'| = O(T/\varepsilon^{O(1)})$, where $T = \min\{\mathcal{L}_\mathcal{F}^2, \mathcal{L}_\mathcal{S}^2, n^2\mathsf{OPT}^2\}$ thus completing the proof of Theorem 4.

6.3. Discrete Candidate Locations

In this subsection we study the usefulness of the pruning technique for jammer location under the Full-interference model as well. Given storage region(s) $\mathcal{S}$, a polygonal fence $\mathcal{F}$ enclosing $\mathcal{S}$ such that eavesdroppers may lie on $\mathcal{F}$, in [28, 29] the authors show how, given a discrete set $\mathbf{J}$ of candidate locations of jammers, to compute a minimum cardinality set $\mathcal{J} \subseteq \mathbf{J}$, such that Equations (2) and (1) are satisfied, up to a factor of at most $(1+\varepsilon)$.

Given $\mathbf{J}$, the algorithm first identifies two sets, $\mathcal{S}' \subset \mathcal{S}$ and $\mathcal{E}' \subset \mathbb{R}^2 \setminus \mathcal{S}$, of witness points. From these sets, an Integer Linear Program (ILP) is determined in which each witness point yields one constraint, yielding overall $O(|\mathcal{E}'| + |\mathcal{S}'|)$ constraints. The solution provides a bi-criteria approximation similar to our results above, which hold for any point in $\mathcal{S}$ or outside of $\mathcal{C}$. However, it is important to reduce the number of constraints as much as possible, especially for the ILP whose computation cost can be very high; in this case, a decrease in the number of constraints is achieved through a reduction in the number of witness points. Specifically, we apply our pruning techniques from Section 6.1. Thus, we obtain the following theorem:

Theorem 5. *Given storage region(s) $\mathcal{S}$, fence $\mathcal{F}$, discrete candidate jammer locations $\mathcal{J}$, thresholds δ_2, δ_1 and jammer power $\hat{P}$, under the Full interference model, we can compute a set of locations $J \subset \mathcal{E}$ by solving an integer linear program with at most $O(k(n^2/\varepsilon^{O(1)})(\log^2(n/\varepsilon^{O(1)}) + \log T))$ constrains, where $T = \min\{\mathcal{L}_\mathcal{F}, \mathcal{L}_\mathcal{F}\}$ such that $|J| \leq (1+\varepsilon)\mathsf{OPT}$ and if jammers of power $\hat{P}$ are placed at J,*

(i) For any point $p_e \in \mathcal{E}$, $SIR(J, p_e) < (1+\varepsilon)\delta_1$.

(ii) For any point $p_s \in \mathcal{S}$, $SIR(J, p_s) > (1-\varepsilon)\delta_2$.

The paper [28, 29] discusses a similar algorithm for assigning power to the jammers, while having their locations fixed. A result analogous to Theorem 5 holds for this case as well.

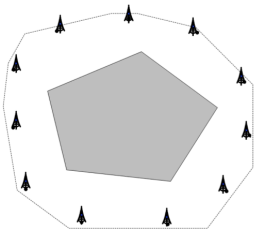

Figure 14. The Storage/Fence environment used in the simulations. Jammers $\mathcal{J}$ are indicated by up-arrows.

7. 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 14. 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. 15(a), where, given an upper threshold τ_2, a higher lower threshold τ_1 is achieved as α_F grows. Fig. 15(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. 15(c) and Fig. 15(d) shows the correlations between prescribed τ_2 value and the corresponding η values assigned by the optimal algorithm. Fig. 15(c) shows the maximum of the η_j values among the jammer set $\mathcal{J}$, and Fig. 15(d) shows the average over $\mathcal{J}$. These plots explain why Figs. 15(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.

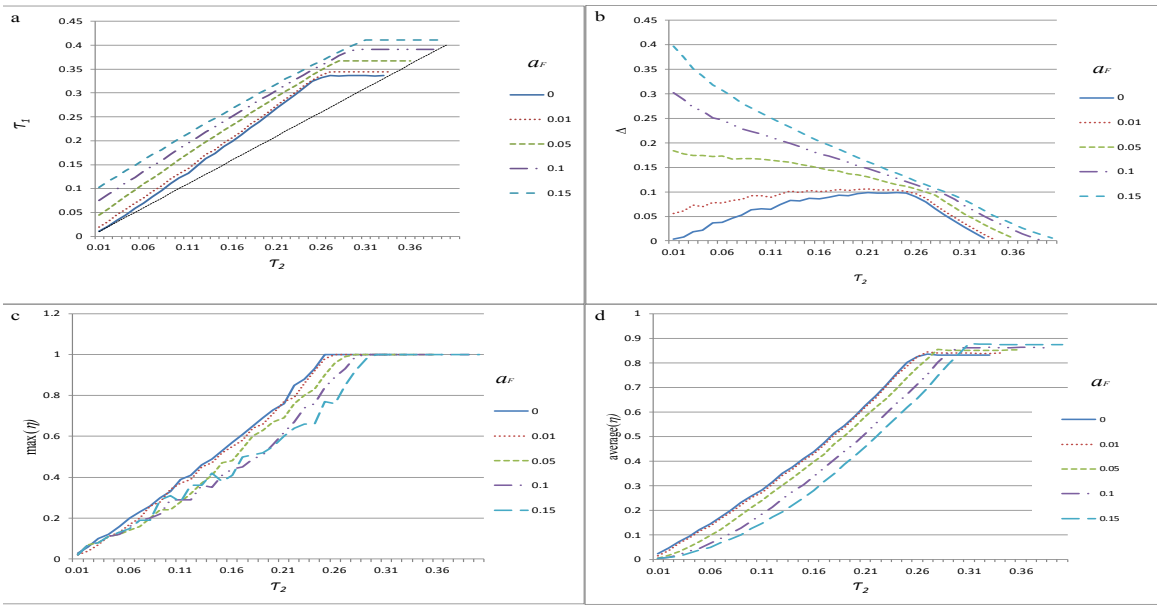

Figure 15. *Simulation results. For different α_F values, (a) presents the maximum achieved τ_1 threshold given τ_2. (b) presents the delta capacity, which is equivalent to the achievable communication rate. (c-d) present the maximum jammer activity and the average jammer activity versus τ_2, respectively.*

8. 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). M. Segal was partially supported by Israel Science Foundation (grant No. 317/15), IBM Corporation and the Israeli Ministry of Economy and Industry.

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] Y. Allouche, Y. Cassuto, A. Efrat, M. Segal, E. Arkin, G. Grebla, and J. S. Mitchell. Secure communication through jammers jointly optimized in geography and time. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc*. ACM, 2015.

[3] E. Arkin, Y. Cassuto, A. Efrat, G. Grebla, J. S. Mitchell, S. Sankararaman, and M. Segal. Optimal placement of protective jammers for securing wireless transmissions in a geographic domain. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, pages 37–46. ACM, 2015.

[4] M. de Berg, M. van Kreveld, M. Overmars, and O. Schwarzkopf. *Computational Geometry: Algorithms and Applications*. Springer-Verlag, 2000.

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

[6] B. Deka, R. M. Gerdes, M. Li, and K. Heaslip. Friendly jamming for secure localization in vehicular transportation. In *International Conference on Security and Privacy in Communication Systems*, pages 212–221. Springer, 2014.

[7] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.

[8] 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.

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

[10] 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.

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

[12] M. A. S. 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.

[13] 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.

[14] 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.

[15] 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, pages 53–54. ACM, 2012.

[16] D. G. Kirkpatrick. Efficient computation of continuous skeletons. In *Proc. 20th IEEE FOCS*, pages 18–27, 1979.

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

[18] D. T. Lee and R. L. Drysdale. Generalization of voronoi diagrams in the plane. *SIAM J. Comput.*, 10(1):73–87, 1981.

[19] 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.

[20] 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, pages 161–168, 2009.

[21] N. Megiddo and K. Supowit. On the complexity of some common geometric location problems. *SIAM J. Comput.*, 13(1):182–196, 1984.

[22] N. H. Mustafa and S. Ray. Improved results on geometric hitting set problems. *Discrete Comput. Geom.*, 44:883–895, 2010.

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

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

[25] 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.

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

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

[28] 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.

[29] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal. Optimization schemes for protective jamming. *Mobile Networks and Applications*, 19(1):45–60, 2014.

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

[31] 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.

[32] 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.

[33] P. Siyari, M. Krunz, and D. N. Nguyen. Friendly jamming in a mimo wiretap interference network: A nonconvex game approach. *IEEE Journal on Selected Areas in Communications*, 2017.

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

[35] 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.

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

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

[38] J. P. Vilela and J. Barros. Collision-free jamming for enhanced wireless secrecy. In *IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks", WoWMoM 2013, Madrid, Spain, June 4-7, 2013*, pages 1–6, 2013.

[39] 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.

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

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

Appendix: Proof of Theorem 2

The pruning process employs the following steps. Initially, we compute $\mathsf{RVD}(\mathcal{S},\mathcal{F})$. For any fence segment $\overline{p_eq_e}$ in $\mathsf{RVD}(\mathcal{S},\mathcal{F})$, let $\mathsf{s}(\overline{p_eq_e})$ be the set $\{p_s \in \mathcal{S} \mid \exists p'_e \in \overline{p_eq_e}, \mathsf{s}(p'_e) = p_s\}$. Let Ξ_v be the segments $\overline{p_eq_e} \in \mathsf{RVD}(\mathcal{S},\mathcal{F})$ such that $\mathsf{s}(\overline{p_eq_e})$ is a single vertex of $\mathcal{S}$ and let Ξ_s be the remaining segments. For each segment $\overline{p_eq_e} \in \Xi_v$ such that p'_e is the closest point to $\mathsf{s}(\overline{p_eq_e})$ on the line through p_e and q_e, if $p'_e \in \overline{p_eq_e}$, we replace $\overline{p_eq_e}$ with $\overline{p_ep'_e}$ and $\overline{p'_eq_e}$ in Ξ_v.

With the sets of segments Ξ_v and Ξ_s, we further shorten or remove segments according to the following lemmas. The proofs hold under both interference models.

Lemma A.1. *For any segment $\overline{p_eq_e} \in \Xi_s$, (i) $\mathsf{s}(\overline{p_eq_e})$ is either a segment $\overline{s_es_{e'}}$ along the boundary of some region in $\mathcal{S}$, and (ii) for some $p'_e \in \mathcal{E}$, if the segment connecting p'_e to $\mathsf{s}(p'_e)$ intersects $\mathcal{E}$ at some point p''_e, then, for any $J \subset \mathcal{J}$,*

$$SIR(J,p''_e) < \delta_1 \Rightarrow SIR(J,p'_e) < \delta_1.$$

Proof. Clearly, (i) is true. The proof of (ii) follows from [28, cf. Lemma 3.1]. □

Lemma A.1 implies that we can shorten all segments in $\mathsf{RVD}(\mathcal{S},\mathcal{F})$ to portions such that for any point p_e in the remaining portions, the segment connecting p_e and $\mathsf{s}(p_e)$ does not intersect $\mathcal{F}$. Let Ξ_s and Ξ_v be replaced with the segments obtained through this shortening.

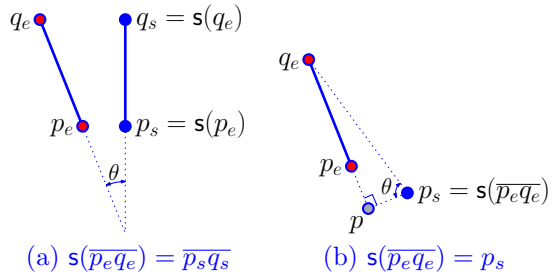

Figure 16. Critical angle $\theta = \theta_c(\overline{p_eq_e})$ for a segment $\overline{p_eq_e}$.

Definition 2. The ***critical angle*** $\theta_c(\overline{p_eq_e})$ (see Figure 16) for a segment $\overline{p_eq_e} \in \Xi$ is defined as follows (assuming without loss of generality $\|q_e - \mathsf{s}(q_e)\| \geq \|p_e - \mathsf{s}(p_e)\|$):

(i) If $\mathsf{s}(\overline{p_eq_e})$ is a segment $\overline{p_sq_s}$, then $\theta(\overline{p_eq_e})$ is the angle between the lines containing $\overline{p_eq_e}$ and $\overline{p_sq_s}$

(ii) If $\mathsf{s}(\overline{p_eq_e})$ is a vertex $p_s \in \mathcal{S}$, then $\theta(\overline{p_eq_e})$ is the angle $\angle q_ep_sp$ where p is the closest point to p_s on the line containing $\overline{p_eq_e}$.

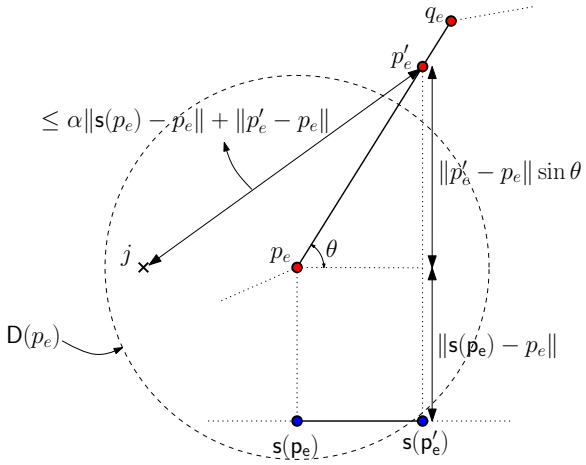

Figure 17. Illustration of proof of Lemma A.2

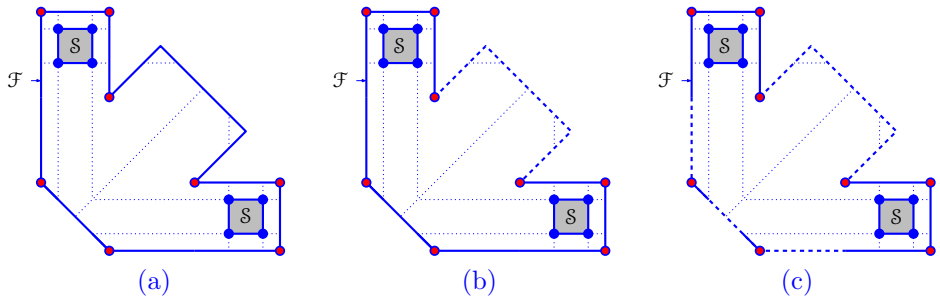

Figure 18. The solid lines represent the portion of the fence that needs to be considered, while the dashed lines represent portions that can be pruned and the thin dotted lines are the edges of the Voronoi diagram of $\mathcal{S}$ based on which the pruning is performed. (left) Original scenario, (middle) After pruning based on Lemma A.1, (right) After pruning based on Lemmas A.2 and A.3.

We define the *grazing angle*

$$\hat{\theta} = \sin^{-1}\left(\frac{1}{(1+\varepsilon)^{1/\gamma}}\right).$$

Lemma A.2. *For a segment $\overline{p_e q_e} \in \Xi_s$, if the critical angle $\theta_c(\overline{p_e q_e}) > \hat{\theta}$, then,*
(i) $\|p_e - q_e\| = O(\frac{1}{\varepsilon})\|\mathsf{s}(p_e) - \mathsf{s}(q_e)\|$.
(ii) For any $J \subset \mathcal{J}$, if $SIR(J, p_e) < \delta_1$, then, for any $p'_e \in \overline{p_e q_e}$, $SIR(J, p'_e) \leq (1+\varepsilon)\delta_1$.

Proof. Let $\theta = \theta_c(\overline{p_e q_e})$. The proof of part (i) follows from the fact that $\|p_e - q_e\| = \|\mathsf{s}(p_e) - \mathsf{s}(q_e)\|/\cos\theta$. We prove part (ii) under the NJ-interference model as follows. The proof under the Full-interference models follows from combining this with [28, cf. Lemma 3.1]. Since $SIR(j, p_e) \leq \delta_1$, $j \in \mathsf{D}(p_e)$. For any $p'_e \in \overline{p_e q_e}$, we have

$$\begin{aligned} SIR(j, p'_e) &\leq \frac{\tilde{P}\|\mathsf{s}(p'_e) - p'_e\|^{-\gamma}}{\hat{P}\|j - p'_e\|^{-\gamma}} \\ &\leq \frac{\tilde{P}}{\hat{P}}\left(\frac{\|p'_e - p_e\| + \|j - p_e\|}{\|p'_e - p_e\|\sin\theta + \|\mathsf{s}(p_e) - p_e\|}\right)^{\gamma}, \end{aligned}$$

since $\|\mathsf{s}(p'_e) - p'_e\| = \|p'_e - p_e\|\sin\theta + \|\mathsf{s}(p_e) - p_e\|$ and by triangle inequality, $\|j - p'_e\| \leq \|p'_e - p_e\| + \|j - p_e\|$. See Figure 17 for an illustration. Further,

$$\begin{aligned} SIR(j, p'_e) &\leq \frac{\tilde{P}}{\hat{P}}\left(\frac{\|p'_e - p_e\| + \alpha\|\mathsf{s}(p_e) - p_e\|}{\|p'_e - p_e\|(\frac{1}{1+\varepsilon})^{1/\gamma} + \|\mathsf{s}(p_e) - p_e\|}\right)^{\gamma} \\ &\leq (1+\varepsilon)\alpha^{\gamma}\frac{\tilde{P}}{\hat{P}} \leq (1+\varepsilon)\delta_1, \end{aligned}$$

since $\|j - p_e\| \leq \alpha\|\mathsf{s}(p_e) - p_e\|$, $\alpha \geq 1$ and $(1+\varepsilon)^{1/\gamma} \geq 1$. Thus, the lemma is proved. □

Based on Lemma A.2, we then prune all segments of $\overline{p_e q_e}$ of Ξ_s such that $\theta_c(\overline{p_e q_e}) > \hat{\theta}$. We remove all such segments from Ξ_s and keep only their lower endpoint (as a degenerate segment).

Lemma A.3. *For a segment $\overline{p_e q_e} \in \Xi_v$, whose critical angle $\theta(\overline{p_e q_e}) > \hat{\theta}$ let $p_s = \mathsf{s}(\overline{p_e q_e})$ and p''_e be the point on $\overline{p_e q_e}$ such that $\angle p''_e p_s p'_e = \hat{\theta}$ where p'_e is the closest point to p_s on the line containing $\overline{p_e q_e}$. We now have,*
(i) $\|p_e - p''_e\| = O(\frac{1}{\varepsilon})\|p_s - p_e\|$.
(ii) For any set of jammers $J \subset \mathcal{J}$, if $SIR(J, p''_e) < \delta_1$, then, for any $p'''_e \in \overline{p''_e q_e}$, $SIR(J, p'''_e) < (1+\varepsilon)\delta_1$.

Proof. We have $\tan\angle p''_e p_s p'_e = \|p''_e - p'_e\|/\|p'_e - p_s\| = O(1/\varepsilon)$. Since $\|p''_e - p'_e\| \geq \|p''_e - p_e\|$ and $\|p'_e - p_s\| \leq \|p_e - p_s\|$, part (i) is proved. Part (ii) can be proved in a manner similar to the proof of part (ii) of Lemma A.2. □

Lemma A.3 implies that we can shorten all segments that lie in the Voronoi region of a vertex of $\mathcal{S}$ and have a high critical angle such that, once shortened, the critical angle is exactly $\hat{\theta}$. The final set Ξ is the resulting set of segments $\Xi_v \cup \Xi_s$.

Figure 18 shows the effects of this pruning process through an example. In each case, the dashed edges are the portions of the fence that are pruned. Figure 18(a) shows the scenario where we have two storage regions in $\mathcal{S}$ inside a fence $\mathcal{F}$. Figure 18(b) shows the effects of pruning based on Lemma A.1 while Figure 18(c) shows the pruned portions based on Lemmas A.2 and A.3. As can be seen, a significant portion of the fence need not be considered.

Combining Lemmas A.1, A.2 and A.3, Theorem 2 is proved. **QED**.

We can actually prune further using the following lemma:

Lemma A.4. *Assume next that u and v are points in $\mathcal{F}$. Let γ be the portion of $\partial\mathcal{F}$ between p_e and q_e, and $\mathcal{E} \subset \partial\mathcal{S}$ be a straight-line segment such that for every $p'_e \in \gamma, \mathsf{s}(p'_e) \in \mathcal{E}$, and $\overline{p'_e \mathsf{s}(p'_e)} \subset \mathcal{C}$. Refer to Fig. 19.*

Assume that in addition there is a point $x \in \mathcal{C}$ such that

- $\overline{p_e x} \subset \mathcal{C} \setminus \mathcal{S}$.
- $\overline{q_e x} \subset \mathcal{C} \setminus \mathcal{S}$.
- $s(\overline{p_e x}) \subset \mathcal{E}$ *and* $s(\overline{q_e x}) \subset \mathcal{E}$ *and*
- $\theta_c(\overline{p_e x}) > \hat{\theta}$ *and* $\theta_c(\overline{q_e x}) > \hat{\theta}$

Then for any $J \subset \mathcal{J}$ if $SIR(J, p_e) < \delta_1$, and $SIR(J, q_e) < \delta_1$ then, for any $p'_e \in \gamma$, $SIR(J, p'_e) \leq (1+\varepsilon)\delta_1$.

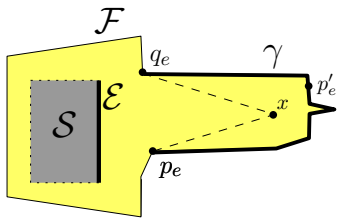

Figure 19. The settings of Lemma A.4. Masking a connected portion of $\mathcal{F}$ by the two segments $\overline{p_e x}$ and $\overline{q_e x}$ (not on $\mathcal{F}$), in order to prune this portion.