# Optimal Placement of Protective Jammers for Securing Wireless Transmissions in a Geographic Domain


Esther 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 Systems
USA

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



## ABSTRACT

Wireless communication systems, such as RFIDs and wireless sensor networks, are increasingly being used in security-sensitive applications, e.g. credit card transactions or monitoring patient health in hospitals. Wireless jamming by transmitting artificial noise, which is traditionally used as an offensive technique for disrupting communication, has recently been explored as a means of protecting sensitive communication from eavesdroppers.

In this paper, we consider location optimization problems related to the placement and power consumption of such friendly jammers in order to protect the privacy of wireless communications constrained within a geographic region. Under our model, we show that the problem of placing a minimum number of fixed-power jammers is NP-Hard, and we provide a PTAS ($(1+\varepsilon)$-approximation scheme) for the same, where $\varepsilon$ is a tunable parameter between 0 and 1.


## 1. INTRODUCTION

Wireless communication is increasingly being employed to transfer highly sensitive information. Systems such as ambient living assistance systems [20], emergency response systems employing wireless networks [15], contactless smart cards [9] and military sensor networks [1] all employ wireless communication to transmit potentially sensitive information, such as patient health information, banking or financial data or military information. The shared nature of the wireless medium makes the protection of such information from eavesdropping an important problem.



*IPSN '15,* April 14 - 16, 2015, Seattle, WA, USA.



http://dx.doi.org/10.1145/2737095.2742142.


In many cases, the use of cryptographic techniques is impractical due to the limited capabilities of the communicating devices (e.g., low-cost sensors or RFID devices in smart cards) or due to application constraints (e.g., in emergency situations in which rescue personnel cannot spend time typing passwords or employing other authentication methods). Moreover, in many situations, there is a variety of communicating nodes on different frequencies and the nodes themselves may be dynamically changing, with mobile nodes or the addition/removal of nodes. It is, thus, advantageous for the security technique to be impervious to such variations in the system.

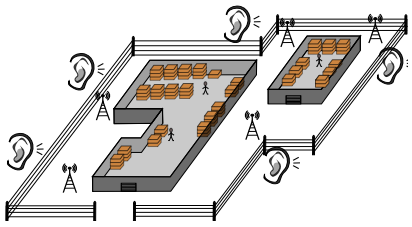

**Figure 1.** An example scenario in which the storage $\mathcal{S}$ consists of two warehouses containing the communicating nodes surrounded by a fence. Jammers placed within the fence prevent eavesdroppers outside the fence from listening.

Due to the inapplicability of cryptography in many scenarios, jamming has recently been explored as a defensive technique to achieve security from eavesdroppers [19, 27]. In contrast to its traditional offensive use, jamming for security must achieve the twin objectives of (i) reducing the *eavesdropper*'s channel quality to a level that is too low for successful reception, and (ii) doing so while maintaining sufficient channel quality for legitimate transmissions. We say that a set of jammers is *successful* if these two objectives are achieved.

Noting that the communication is often *geographically restricted*, Sankararaman *et al.* [23,24] present an environment model consisting of communication within a region, the *storage* $\mathcal{S}$, surrounded by

a *fence* $\mathcal{F}$, and the storage is to be protected from eavesdroppers lying outside the fence. In this context, they show how to configure friendly jammers placed within the fence that are to operate independently of the communicating network. This model is depicted in Figure 1 (from [23]).

The main advantages of this protection scheme are:

- The jammers need to know only minimal information about the communication taking place, such as the frequency of communication and bounds on receiver sensitivity and transmission powers.
- It supports dynamic behavior, such as mobility or addition/removal of nodes. As long as communication is restricted to the storage, the jammers do not need to know the exact locations of nodes within the region.
- It is proactive rather than reactive, requiring no overhead for the communicating nodes and requiring no synchronization amongst the jammers.

In this paper, we expand upon the results of [23, 24] in a number of important ways. We consider two models. The first model (the *Full-interference model*) takes into account the accumulative effect of all jammers on every point. The second model (the *Nearest-Jammers-interference model*, or *NJ-interference model*) assumes that all jammers use the same transmission power and that, for each point $p \in \mathbb{R}^2$, takes into account only those jammers that are nearest to $p$. (This model assumes that jammers are sparse enough that only the nearest jammer contributes interference; in many scenarios, this assumption is reasonable, due to the rapid decrease of a jammer's interference with distance.) Further details of these models are discussed below in Section 2.

Our specific contributions include the following:

1. Given a discrete set of potential eavesdropper locations and a geographic domain comprised of a discrete set of storage regions, we show that, in the NJ-model, it is NP-hard to minimize the number of jammers necessary to protect the domain.
2. 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. We present a "pruning" method of reducing the region where eavesdroppers can be placed so that the solution in the "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 [23,24] 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. The contribution of the pruning method is in showing that the the number of constraints required in the ILP/LP need not depend on the length of the fence.

Our approximation algorithms are bi-criteria approximations, i.e., we allow both some suboptimality (approximation) in the number/power of jammers and some relaxation of the channel quality requirement (measured using the signal-to-interference ratio) at the nodes.

**Related Work.** In the field of information theory, several papers [13, 19, 27, 29, 30] consider the wiretap channel [32], in which a single eavesdropper tries to listen to legitimate communication between a pair of nodes, and it is shown that perfect secrecy is possible when the eavesdropper's channel is worse than the legitimate channel. These works consider the use of jammers to degrade the eavesdroppers' channel and analyze the channel capacity under various scenarios, such as cooperating or independent jammers, multiple eavesdroppers, etc. Under the same model of eavesdroppers, there have also been game-theoretic approaches for optimizing power consumption of jammers [8, 17] and designating regions where eavesdroppers cannot be located [8]. However, most of these works do not explore the geometry of the problem sufficiently and are primarily of theoretical importance due to the simple scenarios under consideration.

Recent works [4,17] focus on the Multiple-Input-Multiple-Output (MIMO) wiretap channel where the transmitter, receiver, and eavesdropper, may possess multiple antennas. The authors of [4] obtain a closed-form relationship for the structure of the jammer's artificial noise covariance matrix that guarantees no decrease in the mutual information between the transmitter and the receiver. Under the model considered in [17], the eavesdropper can act either as a passive eavesdropper or as an active jammer, under half-duplex constraint. Consequently, the authors of [17] use a game-theoretic approach and examine conditions for the existence of Nash equilibria. In [2], the authors develop and implement a demodulator for a MIMO receiver. Via experiments, good performance is demonstrated in an environment containing two jammers.

Since RFID devices have extremely low power requirements, often making the use of cryptography difficult, jamming has been considered as a possible security measure [10, 11, 21], but most works address the security of only a single RFID tag. Another system with low capability devices is the wireless sensor network. Although, in many cases, cryptography is possible here [22], the focus is 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 [26], where eavesdropping is still possible. The authors of [25] propose to use an intelligent jammer that utilizes cryptography in order to avoid interfering with legitimate receivers. However, for the above mentioned reasons, such techniques are inappropriate for RFID and wireless sensor networks. It is, thus, viable to consider physical layer techniques in the context of sensor networks.

Gollakota *et al.* [6] have also used such a well-coordinated communication between source and jammers. These methods have significant advantages, but require reactive jammers (i.e., jammers synchronized with other jammers) and a flexible physical layer. None of these assumptions are required for our work.

Vilela and Barros ( [28]) showed that without any assumptions on jammers and eavesdroppers' location, one could still use other nodes as friendly jammers, as long as they avoid co-transmitting with the legitimate transmitter and in the vicinity of a common destination. The authors show how to abstract this setting as a graph, and how to find an optimal subset of nodes using ILP. In [31] the authors study asymptotic behaviour in a stochastic setting in which jammers and eavesdroppers are at randomly distributed locations. In particular they study the concept of *Secure Throughput*, which is based on the probability that a message is successfully received only by the legitimate receivers.

To the best of our knowledge, [23,24] is the only work that adapts jamming parameters to complex geometric positioning constraints. In this paper, we extend the results of [23, 24] in a number of ways.

## 2. PRELIMINARIES: THE MODEL

**Model of the Environment.** We consider a *Storage/Fence* environment model in which legitimate communication takes place within an enclosure specified by one or more polygonal regions,

$\mathcal{S} \subset \mathbb{R}^2$, called the *storage*. We let $\mathcal{L}_{\mathcal{S}}$ denote the total perimeter of $\mathcal{S}$. We do not assume any knowledge of the locations of nodes in $\mathcal{S}$, but we do assume some properties of legitimate communication (described below). In particular, legitimate receivers and transmitters can be located at any point $p_s \in \mathcal{S}$. Further, there exists a *controlled region*, $\mathcal{C} \subseteq \mathbb{R}^2$, that contains $\mathcal{S}$; no eavesdropper is able to be within the interior of $\mathcal{C}$. Outside of $\mathcal{C}$ is the *uncontrolled region*, $\mathcal{U}$. The boundary $\partial\mathcal{C}$ is referred to as the *fence* $\mathcal{F}$. We assume that $\mathcal{C}$ has no holes, but is not necessarily connected; it is a union of simply connected regions. We let $\mathcal{L}_{\mathcal{F}}$ denote the perimeter of $\mathcal{S}$ (i.e., the length of the fence $\mathcal{F}$). We are also given a region $\mathcal{P}$ where jammers can be placed at points of $\mathcal{A} \subseteq \mathcal{P}$. We refer to $\mathcal{A}$ as the *allowable region*. The allowable region permits us to model potential restrictions on locations of jammers, e.g., that they be within a minimum distance of $\mathcal{S}$, or that they be constrained to a specific subset of locations, e.g. near power outlets or in locations that are easily reached for maintenance purposes.

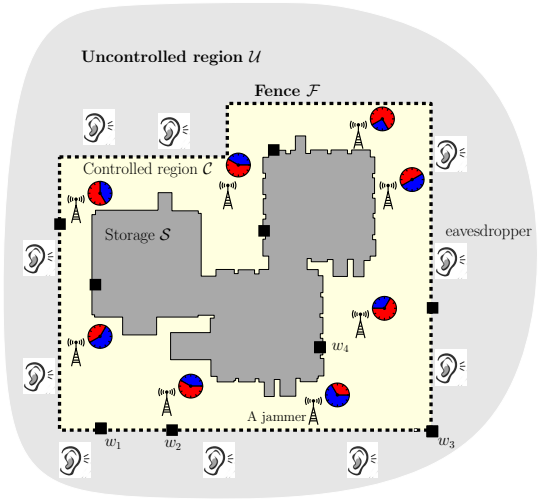


**Figure 2.** A "floorplan" of an example scenario, with storage $\mathcal{S}$ and the fence $\mathcal{F}$ enclosing the controlled region $\mathcal{C}$. Jammers marked as antenna towers are placed between the fence and the storage.

**Communication Model.** Our communication model is similar to that of [23, 24]. We assume that the transmission power $\tilde{P}$ is the same for all legitimate transmitters and that communication in $\mathcal{S}$ does not suffer significant path loss, i.e., for any transmission in $\mathcal{S}$, the received power is $\tilde{P}$. On the other hand, the signal at eavesdroppers does suffer path loss; formally, 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 $\gamma$ is the path-loss exponent, typically in the range $[2, 6]$, and $\|p - q\|$ is the Euclidean distance between $p$ and $q$.

The *Signal-to-Interference Ratio* ($\mathsf{SIR}$) is the ratio of the transmitted signal power to the total interference contributed by the jammers. Formally, for a legitimate receiver $p_s$ in $\mathcal{S}$,

$$\mathsf{SIR}(J, p_s) = \frac{\tilde{P}}{\sum_{j \in J} P_j \|j - p_s\|^{-\gamma}},$$

where $P_j$ is the transmission power of jammer $j$. For an eavesdropper $p_e$, since transmissions from the storage suffer path loss, we make the observation that the maximal signal power is received from a transmitter at the nearest location to $p_e$ on $\mathcal{S}$ (denoted by $\mathsf{s}(p_e)$) and define

$$\mathsf{SIR}(J, p_e) = \frac{\tilde{P}\|\mathsf{s}(p_e) - p_e\|^{-\gamma}}{\sum_{j \in J} P_j \|j - p_e\|^{-\gamma}}.$$

As in [23, 24], we note that the total interference at a location $p$ is usually dominated by the interference from the nearest jammer to $p$, if jammers $J$ are sufficiently spread out, due to the received power decreasing exponentially with distance.

In order that legitimate transmissions are adequately received, we require that $\mathsf{SIR}(J, p_s) > \delta_{\mathsf{s}}$, for points $p_s \in \mathcal{S}$ and some parameter $\delta_{\mathsf{s}}$ to be specified. Similarly, in order that eavesdroppers are unable to receive secure messages, we require that $\mathsf{SIR}(J, p_e) < \delta_{\mathsf{e}}$, for points $p_e \in \mathbb{R}^2 \setminus \mathcal{C}$ and some parameter $\delta_{\mathsf{e}}$. More formally, we make the following constraints on a set $J$ of jammers:

$$\mathsf{SIR}(J, p_s) > \delta_{\mathsf{s}}, \forall p_s \in \mathcal{S}, \text{ and} \tag{1}$$

$$\mathsf{SIR}(J, p_e) < \delta_{\mathsf{e}}, \forall p_e \in \mathbb{R}^2 \setminus \mathcal{C} \tag{2}$$

This model is the same as the widely accepted *Physical Model* described in [7].

Finally, as in [23, 24], we assume that the transmission power of every jammer is at least $(1/\delta_{\mathsf{e}})\tilde{P}$. This is a reasonable assumption, as long as eavesdroppers are not extremely sensitive, and guarantees that jamming $\mathcal{F}$ implies that all points in $\mathbb{R}^2 \setminus \mathcal{C}$ are also jammed, and that the signal from the storage does not "hop over" the fence to more remote locations. On the contrary, removing this assumption also implies that, with no assumptions on background noise, no placement of jammers can jam all possible eavesdropper locations. See [23, 24] for details.

**Remarks.** **(i)** Throughout the paper, for reasons of simplicity of exposition, we ignore the effects of background noise. However, this can be taken into account easily in the model, and all of our schemes carry over with no change to the guarantees provided. **(ii)** We can remove the assumption that legitimate communication is of fixed power if we have additional knowledge of node locations and transmitted distance, i.e., we know the topology of the communicating network.

Note that constraints (1) and (2) take into effect all jammers (weighted by distance$^{-\gamma}$). Thus, we refer to this model as the *Full-interference model*. We are now ready to formalize the problems discussed in this paper, under this model.

PROBLEM 1 (OPT-PLACEMENT). *Given*

1. *A set, $\mathcal{S}$, of storage region(s), each given as a polygonal region.*
2. *The controlled region, $\mathcal{C}$, such that $\mathcal{S} \subseteq \mathcal{C}$. The boundary $\partial\mathcal{C}$ is also called the* fence*, and is denoted $\mathcal{F} = \mathcal{C}$. We denote by $\mathcal{C}^c = \mathbb{R}^2 \setminus \mathcal{C}$ the region which is* outside *the controlled region.*
3. *An allowable region, $\mathcal{A}$, where jammers can be placed.*
4. *The transmission power, $\tilde{P}$, of legitimate transmitters (e.g. RFID tags).*
5. *The path loss exponent, $\gamma$.*
6. *A bound, $\delta_{\mathsf{s}}$, on the $\mathsf{SIR}$ for legitimate receivers in $\mathcal{S}$.*
7. *A bound, $\delta_{\mathsf{e}}$. If the $\mathsf{SIR}$ at $q \in \mathbb{R}^2$ is below $\delta_{\mathsf{e}}$, then tapping into transmissions from $\mathcal{S}$ is impossible.*
8. *The transmission power, $\hat{P}$, of each jammer.*

*The problem is to place a minimum number of fixed-power jammers in $\mathcal{A}$ to satisfy (1) and (2).*

The simulations in [23, 24] suggest that when all jammers have the same transmission power, the cumulative effect of the second, third, etc. nearest jammers to each point are negligible compared

to the effect of the nearest jammer. This is explained by the attenuation model, in which the received power decreases dramatically (exponentially) with distance. Hence, we study here a second model, called the *Nearest Jammers Interference Model*, or *NJ-interference model* for short, in which we assume that all jammers use the same transmission power and that, for each point $p \in \mathbb{R}^2$, we take into account only those jammers that are nearest to $p$.

PROBLEM 2. *Same as Problem 1, except that for any point $p$, in the storage $\mathcal{S}$ or in the uncontrolled region $\mathcal{U} = \mathbb{R}^2 \setminus \mathcal{C}$, only the effect of the nearest jammer to $p$ needs to be taken into account in constraints (1) and (2).*

# 3. HARDNESS OF OPTIMAL JAMMERS PLACEMENT

In this section, we show hardness results for Problem 2 in the case that $\mathcal{S} \subset \mathbb{R}^2$ is a discrete set of regions/points, eavesdropper can be placed only at points of 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 $|P| \leq k$.* [16] The reduction employed in the NP-completeness proof of HITTING-SET-FOR-PLANAR-UNIT-DISKS is from the problem PLANAR-3-SAT [5].

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 *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 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 $\delta$ (via Minkowski sum with a disk of radius $\delta$), then, with the appropriate choice of $\delta_e$, constraint (2) 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 (2) 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 $k$. □

# 4. JAMMER PLACEMENT

In this section, we present results for OPT-PLACEMENTin 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 4.2), 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 4.3). 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.

## 4.1 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 (1) and Equation (2) 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 3 for an illustration.

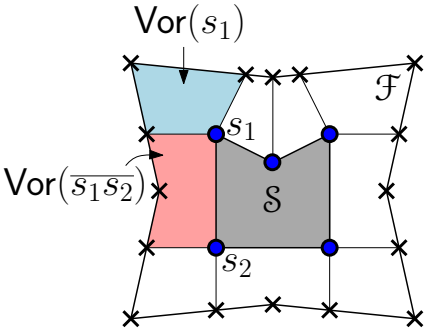


**Figure 3.** Generalized and Restricted Voronoi Diagrams.

The generalized Voronoi diagram is a well-studied structure in computational geometry [12,14] 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 4 illustrates two extreme yet

realistic scenarios, of a fence that is significantly larger than the storage (top of Figure 4), and a fence containing a sharp and long "spike" (bottom of Figure 4). 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.

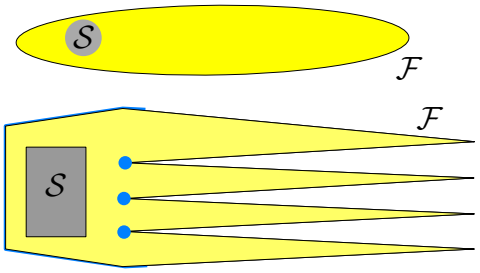


**Figure 4.** Two extreme cases: The yellow region represents the fence, while the grey area is the storage $\mathcal{S}$. The perimeter $\mathcal{L}_{\mathcal{S}}$ is arbitrarily smaller than the length of the fence. Theorem 2 states that, in order to jam all of $\mathcal{F}$, it suffices to jam a subportion of the fence (highlighted in blue) whose length is comparable to $\mathcal{L}_{\mathcal{S}}$.

The output of the pruning process is a set, $\Xi$, 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 $\Xi$ such that if a set $J$ of jammers (not necessarily using the same transmission power) satisfies constraint (2) at all locations $p_e \in \xi$ for $\xi \in \Xi$, then (2) is satisfied at all locations in $\mathcal{F}$. Further,*

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

## 4.2 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 $\alpha = (\delta_{\mathsf{e}}\hat{P}/\tilde{P})^{1/\gamma}$ and $\beta = (\delta_{\mathsf{s}}\hat{P})^{1/\gamma}$ 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 [3] of $\mathcal{S}$ with a disk with radius $\beta$. 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.)

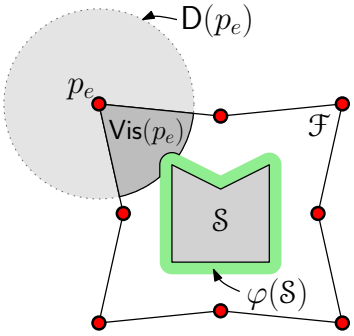


**Figure 5.** The forbidden region (marked in green) and visiblity regions for the case $\alpha = 1$

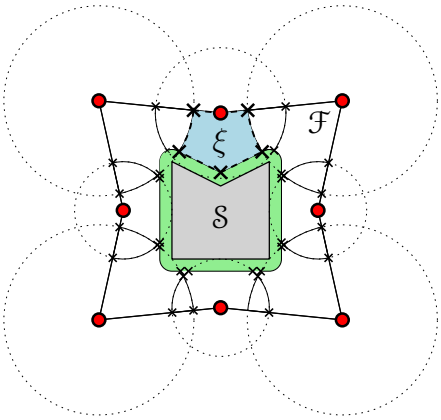


**Figure 6.** Arrangement of visibility regions

(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. 5

As is easily observed from the above discussion, successful jamming can be obtained by a set $J$ of jammers if and only if for every point $p_e \in \mathcal{F}$, there is a jammer of $J$ in $\mathsf{Vis}(p_e)$. Note that a successful jamming might not exist under the above constraints; for example, if $\beta$ is too large (e.g. if $\delta_{\mathsf{s}}$ 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 6.

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.

### 4.2.1 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 (1) and (2) are satisfied. Our algorithm is very similar to the algorithm presented in [23, 24] 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 4.2.2) 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 7 for an illustration of one step of the algorithm, and Figure 8 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 $\mathsf{OPT} + 1$.

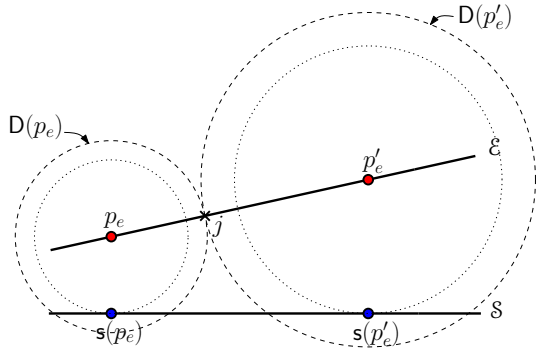


**Figure 7.** One step of the algorithm for disjoint segments, where $\alpha > 1$. The outer disks centered at $p_e$ and $p'_e$ are the critical disks of $p_e$ and $p'_e$, and their radii are $\alpha\|\mathsf{s}(p_e) - p_e\|$ and $\alpha\|\mathsf{s}(p'_e) - p'_e\|$, respectively. The algorithm places a jammer $j$ at the intersection point of these disks.

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 $J$ in time $O(\mathsf{OPT})$ such that (i) $\forall p \in \mathcal{E}$, $\mathsf{SIR}(J,p) < \delta_{\mathsf{e}}$ and (ii) $\forall p \in \mathcal{S}$, $\mathsf{SIR}(J,p) > \delta_{\mathsf{s}}$.*

PROOF. The proof follows from the arguments in [23, 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 4.2.2.

### 4.2.2 $(1+\varepsilon)$-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 $\mathsf{SIR}$ at each point on $\mathcal{E}$. The precise description of our result is given by the following theorem.

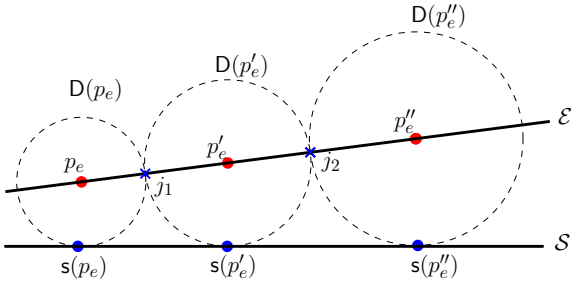


**Figure 8.** Two steps of the algorithm for disjoint segments, when $\alpha = 1$. Critical disks centred at $p_e$ (resp. $p'_e$,$p''_e$) has radius $\|\mathsf{s}(p_e) - p_e\|$, (resp. $\|\mathsf{s}(p'_e) - p'_e\|$, $\|\mathsf{s}(p''_e) - p''_e\|$). The witness point $p'_e$ is located such that $\mathsf{D}[p_e]$ 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 4. *Given storage region(s) $\mathcal{S}$, fence $\mathcal{F}$, thresholds $\delta_{\mathsf{s}}, \delta_{\mathsf{e}}$ and jammer power $\hat{P}$, under the NJ interference model, we can compute locations $J \subset \mathcal{A} \backslash \varphi(\mathcal{S})$ 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 $|J| \leq (1+\varepsilon)\mathsf{OPT}$, and if jammers of power $\hat{P}$ are placed at $J$, then*

*(i) For any point $p_e \in \mathcal{F}$, $\mathsf{SIR}(J, p_e) < (1+\varepsilon)\delta_{\mathsf{e}}$.*
*(ii) For any point $p_s \in \mathcal{S}$, $\mathsf{SIR}(J, p_s) > \delta_{\mathsf{s}}$.*

The overall idea of the algorithm is to compute a discrete set of *witness points* $\mathcal{E}' \subset \mathcal{E}$ such that the $\mathsf{SIR}$ at any point in $\mathcal{E} \setminus \mathcal{E}'$ is approximated by the $\mathsf{SIR}$ 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 $\Xi$ 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 $\Xi$, 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 [18] 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.

*Procedure* PLACE-WITNESSES($\Xi$). Let $\overline{p_e q_e}$ be a segment in $\Xi$ and without loss of generality, let $\|p_e - \mathsf{s}(p_e)\| < \|q_e - \mathsf{s}(q_e)\|$. We

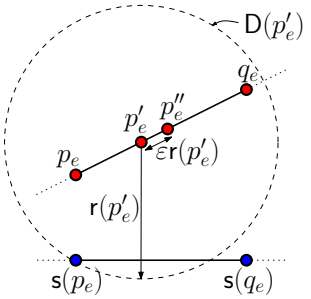


**Figure 9.** One step of procedure PLACE-WITNESSES

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 $\varepsilon'$ is chosen such that $(1+\varepsilon')^\gamma \leq (1+\varepsilon)$ and move to $p''_e$ (see Figure 9). 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 4.1. *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 $j \in \mathcal{J}$,*

$$\mathsf{SIR}(j, p''_e) \leq \delta_{\mathsf{e}} \Rightarrow \mathsf{SIR}(j, p'_e) \leq (1+\varepsilon)\delta_{\mathsf{e}}.$$

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 $j$, $\mathsf{SIR}(j, p''_e) \leq \delta_{\mathsf{e}}$, 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 $\varepsilon'$, the lemma is proved. □

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

*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 $\overline{p_e q_e}$, 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 7.3, we have that for any segment $\overline{p_e q_e} \in \Xi$ such that $\mathsf{s}(\overline{p_e q_e})$ 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 4.2. *For any segment $\overline{p_e q_e} \in \Xi \subseteq \mathcal{F}$ such that $\mathsf{s}(\overline{p_e q_e})$ is a single segment on $\mathcal{S}$,* PLACE-WITNESSES *places $O(\mathsf{OPT}/\varepsilon^{O(1)})$ witness points in $\overline{p_e q_e}$.*

PROOF. Let $\theta = \theta_c(\overline{p_e q_e})$ be the critical angle (see Definition 2 in the Appendix) of $\overline{p_e q_e}$. Consider any two points $p'_e, p''_e$ on $\overline{p_e q_e}$ 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 $\overline{p_e q_e}$.

Clearly, $p_{e,i}$ lies at the point of intersection of $\mathsf{D}(p_{e,i-1})$ and $\overline{p_e q_e}$. 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 $\Xi$.

We now use the algorithm from Section 4.2.1, 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 $\overline{p_e q_e}$.

For any disk in this set, PLACE-WITNESSES clearly places $O(1/\varepsilon^{O(1)})$ witness points. Thus, for a segment in $\Xi$, 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.

## 4.3 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 [23, 24] the authors show how, given a discrete set $\mathcal{J}$ of candidate locations of jammers, to compute a minimum cardinality set $J \subseteq \mathcal{J}$, such that Equations (1) and (2) are satisfied, up to a factor of at most $(1+\varepsilon)$.

Given $\mathcal{J}$, 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 4.1. Thus, we obtain the following theorem:

THEOREM 5. *Given storage region(s) $\mathcal{S}$, fence $\mathcal{F}$, discrete candidate jammer locations $\mathcal{J}$, thresholds $\delta_{\mathsf{s}}, \delta_{\mathsf{e}}$ 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 $p_e \in \mathcal{E}$, $\mathsf{SIR}(J, p_e) < (1+\varepsilon)\delta_{\mathsf{e}}$.*
*(ii) For any point $p_s \in \mathcal{S}$, $\mathsf{SIR}(J, p_s) > (1-\varepsilon)\delta_{\mathsf{s}}$.*

The paper [23, 24] 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.

# 5. CONCLUSION

In this paper, we have considered optimization problems in placement and power consumption of jammers designed to protect wireless communication within a specified region from eavesdroppers who are outside, physically isolated from this region. While we have shown that the general optimization problem is NP-Hard, we have also provided efficient $(1+\varepsilon)$-approximation schemes for the placement of a minimum number of jammers. Our schemes are proactive and require minimal knowledge of the communication system being protected.

## 6. ACKNOWLEDGMENT

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

## 7. REFERENCES

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

[2] D. W. Bliss. Robust MIMO wireless communication in the presence of interference using ad hoc antenna arrays. In *IEEE Military Communications Conference, MILCOM'03*, volume 2, pages 1382–1385. IEEE, 2003.

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

[4] S. A. Fakoorian and A. L. Swindlehurst. Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer. *IEEE Transactions on Signal Processing*, 59(10):5013–5022, 2011.

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

[6] 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.

[7] P. Gupta and P. R. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2):388–404, 2000.

[8] 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.

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

[10] 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.

[11] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *10th ACM Conference on Computer and Communications Security*, pages 103–111, 2003.

[12] D. G. Kirkpatrick. Efficient computation of continuous skeletons. In *20th Annual IEEE Symposium on Foundations of Computer Science (FOCS'79)*, pages 18–27, 1979.

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

[14] D. T. Lee and R. L. Drysdale. Generalization of Voronoi diagrams in the plane. *SIAM Journal on Computing*, 10(1):73–87, 1981.

[15] 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.

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

[17] A. Mukherjee and A. L. Swindlehurst. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Transactions on Signal Processing*, 61(1):82–91, 2013.

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

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

[20] J. Nehmer, M. Becker, A. Karshmer, and R. Lamm. Living assistance systems: An ambient intelligence approach. In *28th International Conference on Software Engineering*, pages 43–50, 2006.

[21] 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.

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

[23] S. Sankararaman, A. K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal. Optimization schemes for protective jamming. In *13th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc'12, Hilton Head, SC, USA, June 11-14, 2012*, pages 65–74, 2012.

[24] 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.

[25] 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 Symposium on Security and Privacy*, pages 174–188, 2013.

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

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

[28] 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.

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

[30] J. P. Vilela, M. R. Bloch, J. Barros, and S. W. McLaughlin. Friendly jamming for wireless secrecy. In *IEEE International Conference on Communications, ICC'10, Cape Town, South Africa, 23-27 May 2010*, pages 1–6, 2010.

[31] 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.

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

## Appendix: The 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 $\Xi_v$ 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 $\Xi_s$ 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 $\Xi_v$.

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

LEMMA 7.1. *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 $J \subset \mathcal{J}$,*

$$\mathsf{SIR}(J,p''_e) < \delta_{\mathsf{e}} \Rightarrow \mathsf{SIR}(J,p'_e) < \delta_{\mathsf{e}}.$$

PROOF. Clearly, (i) is true. The proof of (ii) follows from [23, cf. Lemma 3.1]. □

Lemma 7.1 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 $\Xi_s$ and $\Xi_v$ be replaced with the segments obtained through this shortening.

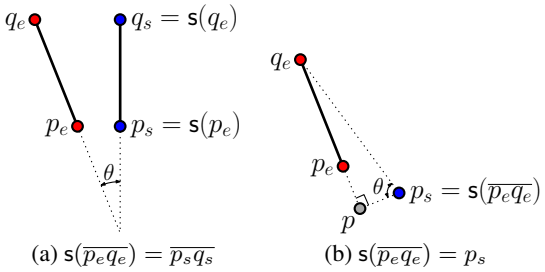


**Figure 10.** Critical angle $\theta = \theta_c(\overline{p_eq_e})$ for a segment $\overline{p_eq_e}$.

*Definition 2.* The ***critical angle*** $\theta_c(\overline{p_eq_e})$ (see Figure 10) 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 $\overline{p_eq_e}$.

We define the *grazing angle*

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

LEMMA 7.2. *For a segment $\overline{p_eq_e} \in \Xi_s$, if the critical angle $\theta_c(\overline{p_eq_e}) > \hat{\theta}$, 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 $\mathsf{SIR}(J,p_e) < \delta_{\mathsf{e}}$, then, for any $p'_e \in \overline{p_eq_e}$, $\mathsf{SIR}(J,p'_e) \leq (1+\varepsilon)\delta_{\mathsf{e}}$.*

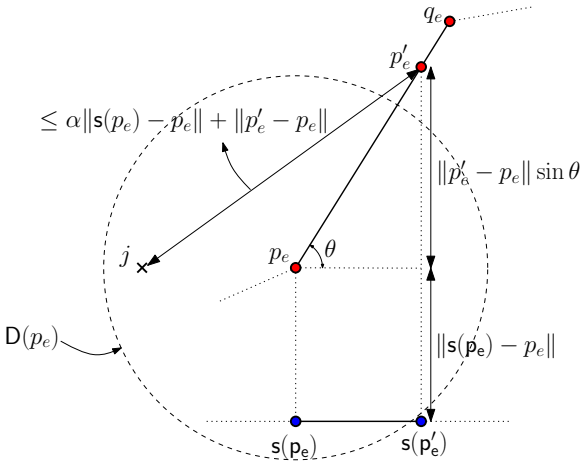


**Figure 11.** Illustration of proof of Lemma 7.2

PROOF. Let $\theta = \theta_c(\overline{p_eq_e})$. 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 [23, cf. Lemma 3.1]. Since $\mathsf{SIR}(j,p_e) \leq \delta_{\mathsf{e}}$, $j \in \mathsf{D}(p_e)$. For any $p'_e \in \overline{p_eq_e}$, we have

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

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 11 for an illustration. Further,

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

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 7.2, we then prune all segments of $\overline{p_eq_e}$ of $\Xi_s$ such that $\theta_c(\overline{p_eq_e}) > \hat{\theta}$. We remove all such segments from $\Xi_s$ and keep only their lower endpoint (as a degenerate segment).

LEMMA 7.3. *For a segment $\overline{p_eq_e} \in \Xi_v$, whose critical angle $\theta(\overline{p_eq_e}) > \hat{\theta}$ let $p_s = \mathsf{s}(\overline{p_eq_e})$ and $p''_e$ be the point on $\overline{p_eq_e}$ such that $\angle p''_ep_sp'_e = \hat{\theta}$ where $p'_e$ is the closest point to $p_s$ on the line containing $\overline{p_eq_e}$. 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 $\mathsf{SIR}(J,p''_e) < \delta_{\mathsf{e}}$, then, for any $p'''_e \in \overline{p''_eq_e}$, $\mathsf{SIR}(J,p'''_e) < (1+\varepsilon)\delta_{\mathsf{e}}$.*

PROOF. We have $\tan\angle p''_ep_sp'_e = \|p''_e - p'_e\|/\|p'_e - p_s\| = O(1/\varepsilon)$. 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 7.2. □

Lemma 7.3 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

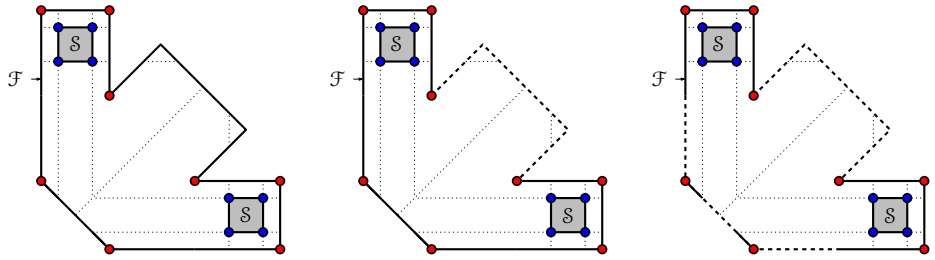


**Figure 12.** The solid lines represent the portion of the fence that needs to be considered, while the dashed lines represent portions that can be pruned and the thin dotted lines are the edges of the Voronoi diagram of $\mathcal{S}$ based on which the pruning is performed. (left) Original scenario, (middle) After pruning based on Lemma 7.1, (right) After pruning based on Lemmas 7.2 and 7.3.

such that, once shortened, the critical angle is exactly $\hat{\theta}$. The final set $\Xi$ is the resulting set of segments $\Xi_v \cup \Xi_s$.

Figure 12 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 12(a) shows the scenario where we have two storage regions in $\mathcal{S}$ inside a fence $\mathcal{F}$. Figure 12(b) shows the effects of pruning based on Lemma 7.1 while Figure 12(c) shows the pruned portions based on Lemmas 7.2 and 7.3. As can be seen, a significant portion of the fence need not be considered.

Combining Lemmas 7.1, 7.2 and 7.3, Theorem 2 is proved. **QED**.

We can actually prune further using the following lemma:

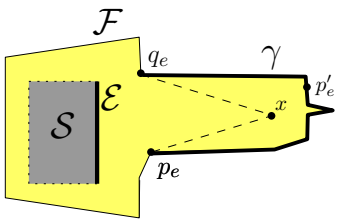


**Figure 13.** The settings of Lemma 7.4. Masking a connected portion of $\mathcal{F}$ by the two segments $\overline{p_e x}$ and $\overline{q_e x}$ (not on $\mathcal{F}$), in order to prune this portion.

LEMMA 7.4. *Assume next that $u$ and $v$ are points in $\mathcal{F}$. Let $\gamma$ 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 $\overline{p'_e s(p'_e)} \subset \mathcal{C}$. Refer to Fig. 13.*

*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 $\mathsf{SIR}(J, p_e) < \delta_\mathsf{e}$, and $\mathsf{SIR}(J, q_e) < \delta_\mathsf{e}$ then, for any $p'_e \in \gamma$, $\mathsf{SIR}(J, p'_e) \leq (1+\varepsilon)\delta_\mathsf{e}$.*