Optimization Schemes for Protective Jamming

Swaminathan Sankararaman[*]
Department of Computer Science
Duke University
swami@cs.duke.edu

Karim Abu-Affash
Department of Computer Science
Ben Gurion University
abuaffas@cs.bgu.ac.il

Alon Efrat
Department of Computer Science
The University of Arizona
alon@cs.arizona.edu

Sylvester David Eriksson-Bique
CS Department
University of Helsinki
sylvester.eriksson-bique@helsinki.fi

Valentin Polishchuk
CS Department
University of Helsinki
valentin.polishchuk@helsinki.fi

Srinivasan Ramasubramanian
Department of Electrical and Computer Engineering
The University of Arizona
srini@ece.arizona.edu

Michael Segal
Department of Communication Systems Engineering
Ben Gurion University
segal@cse.bgu.ac.il

ABSTRACT

In this paper, we study strategies for allocating and managing friendly jammers, so as to create virtual barriers that would prevent hostile eavesdroppers from tapping sensitive wireless communication. Our scheme precludes the use of any encryption technique. Applications include domains such as (i) protecting the privacy of storage locations where RFID tags are used for item identification, (ii) secure reading of RFID tags embedded in credit cards, (iii) protecting data transmitted through wireless networks, sensor networks, etc. By carefully managing jammers to produce noise, we show how to reduce the *SINR* of eavesdroppers to below a threshold for successful reception, without jeopardizing network performance.

We present algorithms targeted towards optimizing power allocation and number of jammers needed in several settings. Experimental simulations back up our results.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection (e.g., firewalls)*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

[*]This work was undertaken while S.S. was at the University of Arizona.

MobiHoc'12, June 11–14, 2012, Hilton Head Island, SC, USA.
Copyright 2012 ACM 978-1-4503-1281-3/12/06 ...$10.00.

General Terms

Algorithms, Theory

Keywords

Friendly jamming, RFID, wireless, security

1. INTRODUCTION

Wireless communicaton is especially susceptible to eavesdropping due to its broadcast nature. Ensuring private communication has typically been considered at higher layers of the network stack by using cryptographic techniques. However, in many types of communication, such as RFID communication and sensor networks, sophisticated cryptographic techniques are often impractical or impossible to implement, due to power or other hardware constraints. Therefore, it is of interest to consider physical layer-based techniques to secure the communication by exploiting the nature of the wireless channel. Such techniques rely on reducing the Signal-to-Interference-plus-Noise Ratio (*SINR*) of eavesdroppers to below a threshold required for successful reception, while taking care not to reduce the *SINR* at legitimate receivers too much so as to prevent reception.

Consider the following scenario motivating the application of such a technique. We have a warehouse where items are stored with RFID tags embedded on them for inventory management. These items are perpetually being transported in or out and can even be moved inside the warehouse. The RFID tags on them may contain private information such as the history of transactions on the item, which must be secured form eavesdroppers. We may ensure physical security of warehouses by building a fence around the warehouse such that potential eavesdroppers may not enter the fence. However, communication security is complicated by the fact that RFID devices are limited capability precluding the implementation of cryptographic techniques.

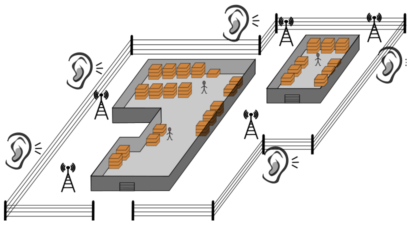


Figure 1: An example application scenario. Jammers secure communication in the warehouses gainst eavesdroppers outside the fence.

To complicate matters further, although we may be able to guess at the capabilities of eavesdroppers, we are unaware of their exact locations. Thus, to ensure the privacy of communication, friendly jammers which transmit artificial noise need to be deployed so that, (i) at *any* potential eavesdropper location, sufficient interference is caused to prevent reception, and (ii) *any* legitimate communication inside the warehouse is not disrupted; see Figure 1. Where should the jammers be placed and what should be their transmission powers such that the above requirements are satisfied?

RFID communication is an especially important application since, although the information stored may be especially sensitive, it is relatively easy to eavesdrop since the capabilities of tags are extremely limited. For example, in [7], the authors demonstrated the vulnerability of credit card RFID tags by successfully performing various attacks including eavesdropping using a device built at a cost of about \$150. Although there do exist RFID tags that possess cryptographic capabilities [21], these have been shown to be weak and vulnerable to even a brute-force attack (in [17], the authors showed the weakness of the algorithms in a widely used cryptographic RFID tag).

In general, friendly jamming may be applied in any scenario where cryptographic techniques are not preferred or where we desire additional security to cryptography. Physical methods such as insulation of the environment by some means of padding or physically ensuring that eavesdroppers cannot get near may oftentimes be cost-prohibitive and therefore, friendly jamming may provide a cheaper alternative. For example, it may not be cost-effective to use such methods in hospitals, warehouses or other large areas where important communication may take place.

This paper focuses on application scenarios where communication is geographically restricted, is of short range and we may ensure some minimal physical security. One additional form of wireless communication worth mentioning is the wireless sensor network, for example, in medical applications [14] and *Ambient Assisted Living* application [27, 16]. Sensor nodes have low power requirements and frequently operate in adverse environments where packet errors may make security schemes difficult. In general, although sensor hardware may be capable of cryptography, these schemes rely on either a trusted third party or secure key management schemes (see [26, 22]). Further, the exact network topology is hard to determine due to the large size and random deployment. These properties make the application of friendly jamming suitable. Placing jammers in such a manner creates a *"virtual Faraday cage"* preventing malicious nodes outside from eavesdropping.

The Environment Model. The model of the environment is termed as a *storage/fence* model. We assume that legitimate communication takes place in the *storage* which is a geographic region physically secured by a *fence* inside which eavesdroppers may not enter. The storage is not restricted in any way apart from the requirement that it is enclosed by the fence. In particular, a wireless network when the exact topology is known or multiple warehouses inside which the communication topology is difficult or impossible to determine are both encompassed by this model. The fence may not intersect the storage, i.e., we assume some minimum gap between the storage and fence. If this requirement is removed, eavesdroppers may move arbitrarily close to legitimate transmitters which makes the problem infeasible. Friendly jammers may be located inside the fence but not in the storage, termed as *jammer space*. Further, we assume that some estimate of eavesdroppers' capabilities or some desired protection level is known.

A similar model may be developed for the case when communication outside the fence should not be eavesdropped upon inside the storage or communication from inside the storage to outside the fence should be jammed. Such a model would be applicable in scenarios such as prisons where cellphone use is not permitted inside. The algorithms in this paper may be extended to this model as well.

Contributions. We present algorithms for placing and assigning power to jammers in the jammer space satisfying two objectives, as described above: (i) at *any* potential eavesdropper location, sufficient interference is caused to prevent reception, and (ii) *any* legitimate communication inside the warehouse is not disrupted. We consider two problems. The first problem is one of assigning transmission powers to a set of fixed jammers, referred to as *power assignment* and the second is one of locating a minimum number of *fixed-power* jammers. In addition, if we are given a set of candidate jammer locations, we show how to solve both problems simultaneously, i.e., locate a number of jammers and assign transmission powers to them so that a cost function which is a weighted sum of the number of jammers and the total transmission power is minimized. In all cases, we consider the setting where jammers may be co-operative as well as when the jammer are responsible for individually preventing eavesdropping.

Power Assignment. We present a linear programming formulation for optimally assigning power to the jammers when both the possible eavesdropper locations as well as possible storage locations (communication nodes) are discrete sets of points. In the more general case, where they may be continuous regions, we present an ε-approximation algorithm which solves a linear program with $O((n^2/\varepsilon^2)(\log^2(n/\varepsilon)+\log L))$ constraints in which, given a tunable parameter $0<\varepsilon<1/2$, the interference at a storage location is approximated within a factor of $(1-2\varepsilon)$, while the total power assigned is approximated within factor $(1+\varepsilon)$. Here, n is the total number of vertices, edges of storage/fence plus jammers and L is the distance between the two farthest points on the fence.

Jammer Placement. We present a linear programming formulation with $O((n|\mathfrak{J}|/\varepsilon^2)(\log(n/\varepsilon)\log(|\mathfrak{J}|/\varepsilon)+\log L))$ when the jammer space is a discrete set of points $\mathfrak{J}$ of size $|\mathfrak{J}|$. The solution to the linear program yields the minimum number of jammers so that, if each jammer is assigned factor $(1+\varepsilon)$ more power, the interference in the storage is ε-

approximated, similar to above. In addition, for the case when jammers are operativing individually, the storage and fence are convex polygons and the jammers' power is fixed at a specified value, we provide an almost-optimal algorithm for placing jammers anywhere in a continuous jammer space. This is interesting primarily as a theoretic contribution and serves to illustrate some of the difficulties of the problem.

We also show how to extend the algorithms to find a combined optimum solution for both power allocation and jammer location when the jammer space is discrete. In addition, when eavesdroppers use directional antennas to reduce the interference region, we show how to extend the linear programs to take this into account. Finally, we present the results of some preliminary simulations to compare individual jammers versus co-operating ones.

Prior Work. Several issues have been identified as being specific to RFID security [8, 18]. Although active jamming has been identified as a possible approach in previous works [10], to the best of our knowledge, this method has not been fully explored. This is partly because most works are interested in the security of a specific RFID tag. A similar approach to active jamming is explored in [10] where a single tag, placed in a container such as a bag, triggers a second *"blocker"* tag on the bag which sends interference to untrusted readers. This has also been extended to software approaches through *"soft blocking"* [9]. The drawback of these approaches are that they are special-purpose and require modification of RFID tags. In contrast with these approaches, we consider the region in which tags may be present for security purposes. To the best of our knowledge, such an approach is novel.

Sensor network security [19] has been mostly focused on cryptographic techniques. Asymmetric key cryptography is, in general, resource intensive and hence, the focus is on symmetric key cryptography where the primary problem is key management [22]. This still exposes vulnerabilities to eavesdropping or relay attacks during the key distribution phase.

In wireless networks, active jamming for security has been considered before, particularly in military applications. In [3], the authors formulate the problem of locating jammers with an integer program similar to the formulation in this paper. However, they do not consider the geometry of the region. In information-theoretic security, there exists a substantial number of works following the seminal work of [28], focusing on analysis of channel secrecy even when eavesdroppers have unlimited resources [12, 15, 23, 25]. Other works include game-theoretic approaches for power allocation to jammers [6] and also identifying "forbidden" regions where eavesdroppers must not be present. However, the geometry has not been fully explored and optimization schemes providing guarantees are not presented.

Outline of the paper. We begin, in Section 2, by describing the problem settings. In Section 3, we show that, under reasonable assumptions, it is sufficient to consider only the fence as possible eavesdropper locations irrespective of where eavesdroppers could lie. Section 4 describes our algorithms for power assignment and Section 5 for jammer placement. In Section 6, we show how to extend our algorithms for providing combined solutions as well as when eavesdroppers use directional antennas. Simulation results are presented in Section 7 followed by a few concluding remarks in Section 8.

2. SETTINGS

Let $\mathcal{S} \subset \mathbb{R}^2$ be the storage region which may be a discrete set of points or a collection of polygonal regions, inside which legitimate communication takes place and let $\mathcal{F}$ be the boundary of a polygon containing $\mathcal{S}$, representing the fence. Let this polygon be denoted by $P_{\mathcal{F}}$. Eavesdroppers may lie anywhere in the region $\mathbb{R}^2 \setminus P_{\mathcal{F}}$. Let $\mathcal{J}$ denote the jammer space which, typically, is the region between $\mathcal{S}$ and $\mathcal{F}$. We denote by n the *description complexity* of the problem. For the power assignment problem, n is the total number of vertices and edges of $\mathcal{S}$ and $\mathcal{F}$ plus the number of jammers and for the placement problem, n denotes the total number of vertices and edges of $\mathcal{S}$ and $\mathcal{F}$.

Slightly abusing notation, we refer to a node (eavesdropper, jammer or legitimate node in the storage) by its location, i.e., a jammer located at point j is referred to as j. For any two points $p_1, p_2 \in \mathbb{R}^2$, $\|p_1 - p_2\|$ indicates the Euclidean distance between them. For two sets of points (possibly infinite) $Q, Q' \subset \mathbb{R}^2$, we denote by $d(Q, Q')$, the minimum distance $\|q - q'\|$ over all points $q \in Q$ and $q' \in Q'$. Given a set of points Q and a point p, let $\mathrm{NN}(p, Q)$ denote the point in Q closest to p. Let $d(\mathcal{S}, \mathcal{F}) = 1$ and let L denote the distance between the two farthest points on $\mathcal{F}$. Our algorithms for power assignment run in time polynomial in n and $\log L$ and those for location depend only on n.

Communication Model. We use the *Signal to Interference plus Noise Ratio* (*SINR*) model (termed as physical model in [5]). Assuming all other factors are normalized and following the standard power dissipation model [20], for a transmission from p to q given a set of jammers J,

$$\mathit{SINR}_p(q) = \frac{P_p \|p - q\|^{-\gamma}}{\sum_{j \in J} P_j \|j - q\|^{-\gamma}}, \tag{1}$$

where P_p is the transmission power of p, P_j is the transmission power of jammer j, and γ is the path loss exponent (typically from 2 to 4). For clarity, we assume no ambient noise throughout the paper. All our results, with the exception of that of Section 5.2, can be extended to take this into account. A receiver q is able to successfully receive a transmission from p if $\mathit{SINR}_p(q)$ is at least a threshold depending on the node characteristics. We refer to the *SINR* at any eavesdropper location p of transmissions from its nearest point on $\mathcal{S}$ as $\mathit{SINR}(p)$. We assume that only jammer signals cause interference, since typically, we would have some collision resolution protocol for transmissions inside the storage.

Equation (1) assumes a model in which all jammers cooperate to interfere with a node. We term this the *Fully Cooperative* interference model, denoted by Full . In addition, we define the *Nearest Jammer* interference model, denoted by NJ , where a receiver only encounters interference from the closest jammer to it. Thus, in Equation (1), the denominator would now incorporate only the interference from the nearest jammer. The NJ model may be extended to include the k closest jammers yielding the k-NJ model. In practice, we expect that the NJ model may not too far from the Full interference model, due to the path loss exponent γ in the power dissipation equation: interference from the closest jammer is most important, while interference due to farther jammers fades away fast with distance.

For the purposes of clarity, we assume that legitimate communication inside $\mathcal{S}$ is of short enough range so as to experience insignificant path loss, but our algorithms can be extended to the cases where we know an upper bound on the range, or if, we know the exact topology of the communicating nodes. We also assume that all transmitters in $\mathcal{S}$ have the same transmitting power (normalized to 1). This assumption may be removed if the exact topology of legitimate nodes is known in advance. Let the *SINR* threshold for successful reception by legitimate receivers be normalized to 1 and the threshold for eavesdroppers be δ. The capabilities of eavesdropper nodes may be different from those of legitimate receivers due to possibly different hardware and therefore, we use different thresholds. We note that, for an eavesdropper, it is sufficient to jam possible transmissions from its nearest point on $\mathcal{S}$.

Finally, throughout, we make the assumption that jammers may be assigned a maximum power P_{max} (due to hardware constraints, a jammer may not be assigned an arbitrarily high power) and a minimum power of $(1/\delta)$. Roughly, the minimum power assumption implies that, if eavesdroppers and legitimate receivers have similar capabilities, then jammers must transmit at a power at least that of legitimate transmitters. The greater the capabilities of eavesdroppers, the higher the jammers' minimum transmission power. We show, in Section 3, that this assumption implies that it is sufficient to consider eavesdroppers on $\mathcal{F}$, i.e., *if an eavesdropper cannot eavesdrop from any location on $\mathcal{F}$, it cannot eavesdrop from any location in $\mathbb{R}^2\backslash\mathcal{F}$.* Although this does not look surprising, if the jammers may be assigned an arbitrarily low transmission power, it is easy to construct examples, where an eavesdropper may be able to successfully eavesdrop by moving away from $\mathcal{S}$ even though it could not eavesdrop from a closer location. We may remove the minimum power assumption if we instead assume that once an eavesdropper gets too far from any point in $\mathcal{S}$, it cannot eavesdrop (possibly due to ambient noise). In this case, our algorithms can be easily extended with running times which have an additional logarithmic dependence on this maximum distance.

Under the above communication model, assuming that eavesdroppers may lie only on $\mathcal{F}$, the following equations formalize the requirements of a set of jammers J where each jammer $j \in J$ has transmission power P_j: (i) at *any* potential eavesdropper location, sufficient interference is caused to prevent reception, and (ii) *any* legitimate communication inside the warehouse is not disrupted.

$$\frac{1}{\sum_{j\in J} P_j\|j-s\|^{-\gamma}} \geq 1, \qquad \forall s \in \mathcal{S} \qquad (2)$$

$$\frac{d(p,\mathcal{S})^{-\gamma}}{\sum_{j\in J} P_j\|j-p\|^{-\gamma}} < \delta. \qquad \forall p \in \mathcal{F} \qquad (3)$$

The above equations would be modified under the NJ model. We focus, in this paper, on the Full model and indicate the changes wherever we refer to the NJ model.

3. CONSIDERING THE BOUNDARIES IS SUFFICIENT

We show that under our communication model: (i) jamming the fence $\mathcal{F}$ is sufficient to ensure that eavesdroppers located outside the fence are also jammed successfully and (ii) ensuring that the any receiver on the boundary of $\mathcal{S}$ is not jammed is sufficient to ensure that receivers inside $\mathcal{S}$ are not jammed.

LEMMA 3.1. *Under any interference model, if SINR$(p) < \delta$ for all points p on $\mathcal{F}$, then for all points p' outside the region encapsulated by $\mathcal{F}$, SINR$(p') < \delta$.*

PROOF. We prove the lemma under the Full model. The proof for the NJ model is part of this proof. Let J be a set of jammers such that no eavesdropper on $\mathcal{F}$ is successfull and let P_j be the transmission power for any jammer $j \in J$. Let p' be a point outside $\mathcal{F}$ and let p be a point on $\mathcal{F}$ on the segment connecting p' to $\mathrm{NN}(p',\mathcal{S})$. Clearly, $\mathrm{NN}(p',\mathcal{S}) = \mathrm{NN}(p,\mathcal{S})$. Rearranging the *SINR* equation, we need to show that, to show that $(d(p,\mathcal{S}))^{-\gamma} < \delta\sum_{j\in J} P_j(\|j-p\|)^{-\gamma}$ implies that $(d(p',\mathcal{S}))^{-\gamma} < \delta\sum_{j\in J} P_j(\|j-p'\|)^{-\gamma}$.

We will show the proof by induction on the number of jammers. For any subset $X \subset J$, let a_X be a real number satisfying $a_X^{-\gamma} = \delta\sum_{j\in X} P_j(\|j-p\|)^{-\gamma}$. Consider a singleton jammer j and the corresponding a_j. Clearly, $(a_j+\|p-p'\|)^{-\gamma} < \delta P_j(\|j-p\|+\|p-p'\|)^{-\gamma}$ since $P_j \geq 1/\delta$. Thus, the base case is satisfied. This completes the proof for the NJ model.

Now, consider some subset $X \subset J$. The inductive hypothesis is that,

$$(a_X+\|p-p'\|)^{-\gamma} < \delta\sum_{j\in X} P_j(\|j-p\|+\|p-p'\|)^{-\gamma} \qquad (4)$$

Now, consider than a jammer j' is added to X and let $b_{X,j'}$ be a real number satisfying

$$b_{X,j'}^{-\gamma} = a_X^{-\gamma} + \delta P_{j'}\|j'-p\|'^{-\gamma} \qquad (5)$$

Clearly, $b_{X,j'} \leq a_x$ and $b_{X,j'} \leq \|j'-p\|$ since $\delta P_{j'} \geq 1$.

$$\begin{aligned}(b_{X,j'}+\|p-p'\|)^{-\gamma} &= b_{X,j'}^{-\gamma}(1+(\|p-p'\|/b_{X,j'}))^{-\gamma}\\ &= \frac{a_X^{-\gamma}) + \delta P_{j'}\|j'-p\|^{-\gamma}}{(1+(\|p-p'\|/b_{X,j'}))^{\gamma}},\end{aligned}$$

by Equation (5). Since $b_{X,j'} < a_X$ and $b_{X,j'} < \|j'-p\|$, this implies that,

$$\begin{aligned}(b_{X,j'}+\|p-p'\|)^{-\gamma} \leq &(a_X+\|p-p'\|)^{-\gamma}\\ &+\delta P_{j'}(\|j'-p\|+\|p-p'\|)^{-\gamma}.\end{aligned}$$

Hence, we know, for $X = J$, Equation (4) is satisfied. Now, since $a_X \leq d(p,\mathcal{S})$, the lemma is proved. □

LEMMA 3.2. *Under any interference model, if for all points p on the boundary of $\mathcal{S}$, SINR$(p) \geq 1$, then for all points p' inside $\mathcal{S}$, SINR$(p') > 1$.*

PROOF. For the NJ model, select an arbitrary point p' inside $\mathcal{S}$ whose closest jammer is $j(p')$. Let p be an intersection point of the segment joining p' and $j(p')$ with $\mathcal{S}$. Since $j(p') = j(p)$, we clearly have $1 \leq$ *SINR*$(p) <$ *SINR*(p').

For the Full model, the statement is equivalent to showing that the *SINR* attains it's minimum at the boundary of $\mathcal{S}$. This is the same as showing that the interference of the jammers attains its maximum on the boundary of $\mathcal{S}$. We do this by showing that the interference, as a function of position, is a sub-harmonic function and thus satisfies the Maximum principle known from complex analysis [1]. This is shown by differentiation:

$$\Delta_s I_s = (\partial_{s_1}+\partial_{s_2})\sum_{j\in J} P_j|s-j|^{-\gamma} = \sum_{j\in J}\gamma^2|s-j|^{-\gamma-2}.$$

Clearly, the Laplacian is positive. Hence, the function is sub-harmonic and the result follows. □

4. POWER ASSIGNMENT

In this section, we provide algorithms to assign powers to a set of fixed jammers J such that Equation (2) and Equation (3) are satisfied and the total power assigned is minimized. We may express the problem by means of the optimization program below, termed as Jamming-LP.

$$\text{Jamming-LP: } \textbf{Minimize } \sum_{j \in J} P_j$$

$$\textbf{s.t. } \forall s \in \mathcal{S} : \sum_{j \in J} P_j \|s - j\|^{-\gamma} \leq 1, \qquad \text{(I)}$$

$$\forall p \in \mathcal{F} : \sum_{i \in J} P_j \|i - p\|^{-\gamma} > \frac{1}{\delta d(p, \mathcal{S})^{\gamma}}, \qquad \text{(II)}$$

$$\forall j \in J : \qquad (1/\delta) \leq P_j \leq P_{max}. \qquad \text{(III)}$$

Constraints (I) and (II) are the equivalent of Equations (2) and (3). I_s and I_e are dependent on the variables P_j and are dictated by the interference models as described in Section 2. The number of constraints (I) and (II) is uncountably infinite if $\mathcal{S}$ and $\mathcal{E}$ are continuous regions in $\mathbb{R}^2$.

First note that when $\mathcal{S}$ and $\mathcal{E}$ are discrete sets of points, Jamming-LP becomes a linear program which may be solved in polynomial time since the number of constraints depends on the cardinalities of $\mathcal{S}$ and $\mathcal{F}$.

The continuous case is a more difficult since, as mentioned before, the number of constraints is uncountably infinite. To get around this difficulty, we provide an ε-approximation algorithm based on discretizations of $\mathcal{S}$ and $\mathcal{F}$. Given a parameter ε in the range $(0, 1)$, the algorithm proceeds according to the following steps:

(1) Compute a discrete set $\mathcal{S}' \subset \mathcal{S}$ such that if Equation (2) is satisfied for $\mathcal{S}'$, then Equation (2) is satisfied for $\mathcal{S}$ with threshold $1/(1 + 2\varepsilon) \geq (1 - 2\varepsilon)$.

(2) Compute a discrete set $\mathcal{F}' \subset \mathcal{F}$ such that if Equation (3) is satisfied for $\mathcal{F}'$ for some power assignment, then, by increasing the powers of the jammers by a factor $(1+\varepsilon)$, Equation (3) is satisfied for $\mathcal{F}$.

(3) Solve the linear program Jamming-LP with constraints corresponding to $\mathcal{S}'$ and $\mathcal{F}'$.

Theorem 1. *Given storage region(s) $\mathcal{S}$, fence $\mathcal{F}$, a set of jammer locations J and an interference model, by solving a linear program with $O((n^2/\varepsilon^2)(\log^2(n/\varepsilon) + \log L))$ constraints, we can compute a power assignment for J such that $\sum_{j \in J} P_j \leq (1 + \varepsilon) \sum_{j \in J} P_j^*$ where P_j^* is the optimal power assignment for j and (i) for each location $p \in \mathcal{F}$, SINR$(p) < \delta$, (ii) for each location $s \in \mathcal{S}$, SINR$(s) \geq (1 - 2\varepsilon)$.*

$\mathcal{S}'$ is constructed so that the interference at the point in $\mathcal{S}$ at which interference is maximum is approximated within factor $(1 - \varepsilon)$. Similarly, for the fence $\mathcal{F}$, the point p on $\mathcal{F}$ at which *SINR* is maximum for a transmission from $\mathrm{NN}(p, \mathcal{S})$, does not receive more than factor $(1 + \varepsilon)$ more *SINR* than the corresponding point in $\mathcal{F}'$. Now, if each jammer is actually assigned $(1 + \varepsilon)$ of the power assignment returned by Jamming-LP, we can jam every point on $\mathcal{F}$ and no point on $\mathcal{S}$ will reduce its *SINR* by more than a factor of $1/(1+\varepsilon)^2 > (1 - 2\varepsilon)$. Thus, Theorem 1 is proved. For the remainder of this section, we assume the Full interference model. However, all results may be applied to the NJ model with minimal modification. The schemes, particular the discretization of $\mathcal{S}$, use some of the ideas of Vigneron [24].

First, we briefly outline a couple of preliminary concepts which are essential for the rest of this section.

Voronoi Diagrams. The *Voronoi Diagram* (see [2] and [4, Chapter 7]) for a set of points Q, denoted by $\mathrm{VD}(Q)$ is a decomposition of the plane into cells such that all points in a cell are closest to the same point $q \in Q$. A cell is denoted by $\mathrm{Vor}(q)$ and edges of the Voronoi Diagram are straight-line segments (parts of bisectors between pairs of points of Q). The *generalized Voronoi Diagram* [11, 13] of a polygon P, is the generalization of the Voronoi Diagram to the vertices and edges of P. This is a decomposition of the plane into cells such that, in each cell, all points have the same closest vertex/edge. Both may be constructed in $O(|P| \log |P|)$ time where $|P|$ is the number of vertices/edges of P.

We are interested in the Voronoi Diagrams of the jammer set $\mathrm{VD}(J)$ and the generalized Voronoi diagram $\mathrm{VD}(\mathcal{S})$ of $\mathcal{S}$. Similar to our notation above, we denote by $\mathrm{Vor}((u, v))$ and $\mathrm{Vor}(u)$, the Voronoi cells of an edge (u, v) and vertex u of $\mathcal{S}$ respectively.

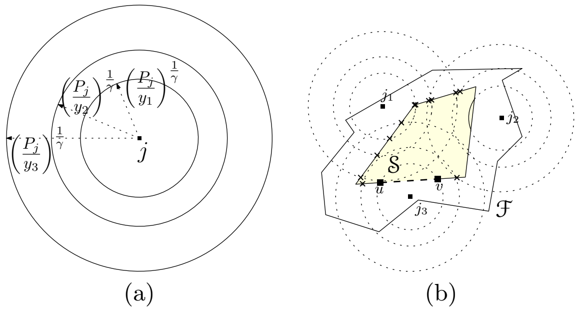

$\left(\frac{P_j}{y_2}\right)^{\frac{1}{\gamma}}$
$\left(\frac{P_j}{y_1}\right)^{\frac{1}{\gamma}}$
$\left(\frac{P_j}{y_3}\right)^{\frac{1}{\gamma}}$
j
(a)
j_1
j_2
$\mathcal{S}$
u
v
j_3
$\mathcal{F}$
(b)

Figure 2: (a) The disks corresponding to the superlevel sets for a jammer when $Y_j = \{y_1, y_2, y_3\}$. (b) The arrangement of the disks with respect to $\mathcal{S}$. Vertices are marked as ×.

Superlevel Sets and Arrangements. For a set of objects Γ and a polygon or collection of polygons P, the *arrangement* $\mathcal{A}_P(\Gamma)$ of Γ is the planar subdivision induced by Γ on the boundaries of polygons in P. Namely, its vertices are the intersection points of the boundaries of the disks and polygons in P together with original vertices of polygons in P and edges are the maximal connected portions of the boundaries of P not crossing a vertex; see Figure 2b. If the number of vertices in P is M, the objects in Γ are segments, rays or lines and the number of objects in Γ is N, the complexity, i.e., the number of vertices and intervals in $\mathcal{A}_P(\Gamma)$ is $O(MN)$.

For a jammer j, let $D[j; t]$ denote the disk of radius t centered at j. Note that at all points in $D[j; t]$, the interference due to j is atleast $P_j t^{-\gamma}$. In mathematics, $D[j; t]$ is known as a *superlevel set* of the function $f_j(x) = P_j \|j - x\|^{-\gamma}$.

Given three parameters $\rho > 0, \alpha > 0$ and $l \in \mathbb{Z}^+$, we define

$$Y(\rho, \alpha, l) = \{y_i = \rho/(1 + \alpha)^i \mid 0 \leq i \leq l\}.$$

Given a set of jammers J and $Y(\rho, \alpha, l)$ for a jammer j, let $\mathcal{D}_j = \{D[j; y_i] \mid 0 \leq i \leq l\}$; see Figure 2a for an example. Consider the arrangement $\mathcal{A}_P(\mathcal{D}_j)$ for some polygon or collection of polygons P. The intervals are all located between successive concentric disks centered at j. Clearly, the following lemma holds for $\mathcal{A}_P(\mathcal{D}_j)$

Lemma 4.1. *Let a, b be two points lying in the same interval of $\mathcal{A}_P(\mathcal{D}_j)$. If a, b lie outside all disks of $\mathcal{D}_j$, then $P_j\|j-a\|^{-\gamma} \le \rho/(1+\alpha)^s$ and $P_j\|j-b\|^{-\gamma} \le \rho/(1+\alpha)^s$. Otherwise, $P_j\|j-a\|^{-\gamma} \ge (1/(1+\alpha))P_j\|j-b\|^{-\gamma}$.*

Discretization of $\mathcal{S}$. We generate a discrete set $\mathcal{S}' \subset \mathcal{S}$ as follows. First, we set $\rho = P_j d(j,\mathcal{S})^{-\gamma}$, $\alpha = \varepsilon/9$ and $l = \lceil(1/\varepsilon)\log(n/\varepsilon)\rceil$. Next, setting $Y_j = Y(\rho, \alpha, l)$, we compute the set of disks $\mathcal{D}_{\mathcal{S}} = \cup_{j\in J}\mathcal{D}_{j,Y_j}$. Finally, we compute the arrangement $A_{\mathcal{S}} = \mathcal{A}_{\mathcal{S}}(\mathcal{D}_{\mathcal{S}})$ and select an arbitrary point in each interval of $\mathcal{A}_{\mathcal{S}}$ to add to the set $\mathcal{S}'$.

We choose $\rho = P_j d(j,\mathcal{S})^{-\gamma}$ because it is an upper bound on $P_j\|j-s\|^{-\gamma}$ for any point $s \in \mathcal{S}$, implying that there is no point of s in the smallest disk of $\mathcal{D}_{j,Y_j}$ for all jammers j. It is important to note that we do not know the values P_j to determine the value of ρ. However, we do not actually need it to compute the radii of the disks in $\mathcal{D}_{j,Y_j}$.

Correctness follows from the following two lemmas.

Lemma 4.2. *Let s be the point selected by our algorithm in some interval of $\mathcal{A}_{\mathcal{S}}$ and let s' be another point in the same interval. For any jammer $j \in J$, we have*

$$\|j-s\|^{-\gamma} \ge \begin{cases} \frac{1}{1+\alpha}\|j-s'\|^{-\gamma}, & \text{if } s \notin D[j; \frac{d(j,\mathcal{S})}{(1+\alpha)^l}], \\ \|j-s'\|^{-\gamma} - \frac{\alpha}{n}d(j,\mathcal{S})^{-\gamma}, & \text{otherwise.} \end{cases}$$

Proof. If $s \notin D[j; d(j,\mathcal{S})/(1+\alpha)^l]$, i.e., if it lies outside the outermost disk centered at j, then by the choice of l, the lemma follows. Otherwise, there exist two consecutive concentric disks centered at j such that interval containing s and s' lies in the region between these disks. By Lemma 4.1, the proof follows. □

Lemma 4.3. *Given a power assignment for the jammers, let s^* be the point maximizing $\sum_{j\in J} P_j\|j-s\|$ over all $s \in \mathcal{S}$ and let $\hat{s}$ be the point selected by our algorithm in the same interval in $\mathcal{A}_{\mathcal{S}}$ as s^*. Then,*

$$\sum_{j\in J} P_j\|j-s^*\|^{-\gamma} \le (1+\varepsilon/3)\sum_{j\in J} P_j\|j-\hat{s}\|^{-\gamma}.$$

Proof. Let J_{out} be the set of jammers such that s^* and $\hat{s}$ lie outside $D[j; d(j,\mathcal{S})/(1+\alpha)^l]$ for all $j \in J_{\text{out}}$ and let J_{in} be the remaining jammers. Lemma 4.2 implies that

$$\begin{aligned} \sum_{j\in J} P_j\|j-\hat{s}\|^{-\gamma} \ge & \sum_{j\in J_{\text{in}}} \frac{P_j}{1+\alpha}\|j-s^*\|^{-\gamma} \\ & + \sum_{j\in J_{\text{out}}} P_j\left(\|j-s^*\|^{-\gamma} - \frac{\alpha}{n}d(j,\mathcal{S})^{-\gamma}\right) \\ \ge & \frac{1}{1+\alpha}\sum_{j\in J} P_j\|j-s^*\|^{-\gamma} \\ & - \alpha\sum_{j\in J} P_j\|j-s^*\|^{-\gamma}, \end{aligned}$$

since s^* is the point maximizing $\sum_{j\in J} P_j\|j-s\|^{-\gamma}$ over all $s \in \mathcal{S}$. Since $\alpha = \varepsilon/9$, the lemma follows. □

Lemma 4.3 implies that if the point $\hat{s}$ does not receive too much interference from the jammers, no other point in $\mathcal{S}$ would have too much interference. Since we do not actually know which point is $\hat{s}$, we take care to ensure that the entire set $\mathcal{S}'$ is not jammed. If each jammer;s power is $P_j(1+\varepsilon)$, then the approximation factor would become $(1+2\varepsilon)$.

There are $O((n/\varepsilon)\log(n/\varepsilon))$ level sets in our arrangement. Thus, the cardinality of $\mathcal{S}'$ which is the number of vertices of $\mathcal{A}_{\mathcal{S}}$ is $O((n^2/\varepsilon^2)\log^2(n/\varepsilon))$ implying that the number of constraints (I) in Jamming-LP would be $O((n^2/\varepsilon^2)\log^2(n/\varepsilon))$ with an equal time required to generate them.

Discretization of $\mathcal{F}$. We generate a discrete set $\mathcal{F}' \subset \mathcal{F}$ as follows. Recall that L denotes the distance between the two farthest points in $\mathcal{F}$. First, we set $\rho = 1$, $\alpha = \varepsilon/3$ and let l be the largest integer such that $1/(1+\alpha)^l \le L^{-\gamma}$. Next, setting $Y_j = Y(\rho, \alpha, l)$, we compute the set of disks $\mathcal{D}_{\mathcal{F}} = \cup_{j\in J}\mathcal{D}_{j,Y_j}$. We compute the generalized Voronoi Diagram (see Section 3) VD($\mathcal{S}$) of $\mathcal{S}$ and let Γ denote the rays and lines constituting VD($\mathcal{S}$). Finally, we compute the arrangement $A_{\mathcal{F}} = \mathcal{A}_{\mathcal{F}}(\mathcal{D}_{\mathcal{F}} \cup \Gamma)$ and add the vertices of $\mathcal{A}_{\mathcal{F}}$ to $\mathcal{F}'$.

We note that on each interval ϕ of $\mathcal{A}_{\mathcal{F}}$, $d(p,\mathcal{S})$ for all points $p \in \phi$ is a linear function since there is a corresponding segment or point on $\mathcal{S}$ on which lie all the points closest to points in ϕ. Thus, the maximum and minimum distances are at the vertices of ϕ. Contrary to the discretization of $\mathcal{S}$ where we approximate the maximum interference received by points in $\mathcal{S}$, we approximate the maximum *SINR*. The choice of l based on the diameter L is to ensure that no point on $\mathcal{F}$ lies outside the disks for any j. Also, since $P_j \ge 1/\delta$ for all $j \in J$, eavesdroppers within distance 1 from any j are always jammed, i.e., their *SINR* is always too low. Note that we do not need to know the powers to compute the disks.

Correctness follows from the following two lemmas.

Lemma 4.4. *Let p be a point selected by our algorithm for any interval in $\mathcal{A}_{\mathcal{F}}$ and let p' be a point in the same interval. For any jammer $j \in J$, $\|j-p\|^{-\gamma} \le (1+\alpha)\|j-p'\|^{-\gamma}$.*

Proof. The distance from p_ϕ to j is between 1 and L. Thus, there exists two consecutive concentric disks in $\mathcal{D}_{j,Y_j}$ such that both p and p' lie between these disks. The proof follows from Lemma 4.1. □

Lemma 4.5. *Given a power assignment for the jammers, let p^* be the point on $\mathcal{F}$ at which SINR(p) is maximum over all $p \in \mathcal{F}$ and let $\hat{p}$ be the vertex in $\mathcal{F}'$ in the interval of p^* such that $d(\hat{p},\mathcal{S}) \le d(p^*,\mathcal{S})$. Then,*

$$\mathit{SINR}(p^*) < (1+\varepsilon)\mathit{SINR}(\hat{p}).$$

Proof. Let $\sum_{j\in J} P_j\|j-p^*\|^{-\gamma} \le \sum_{j\in J} P_j\|j-\hat{p}\|^{-\gamma}$ since otherwise, there is nothing to prove. By Lemma 4.4,

$$\sum_{j\in J} P_j\|j-\hat{p}\|^{-\gamma} \le (1+\alpha)\sum_{j\in J} P_j\|j-p^*\|^{-\gamma}.$$

Since $d(p^*,\mathcal{S})^{-\gamma} \ge d(\hat{p},\mathcal{S})^{-\gamma}$ and by our choice of $\alpha = \varepsilon/3$, the lemma follows. □

Lemma 4.5 implies that the *SINR*(p) $< (1+\varepsilon)\delta$ for any $p \in \mathcal{F}$. Thus, by assigning a power $(1+\varepsilon)P_j$ for all jammers $j \in J$, we can ensure that *SINR*(p) $< \delta$ for all $p \in \mathcal{F}$. The number of level sets corresponding to jammers is $O((n/\varepsilon)\log L)$. The number of vertices in their arrangement on $\mathcal{F}$ is $O((n^2/\varepsilon^2)\log^2 L)$ leading to as many constraints (II) in Jamming-LP, with an equal time required to generate $\mathcal{F}'$.

Remarks. We note that if all the jammers' powers are required to be the same, and we need to find the minimum power assignment, we may remove the dependency on the diameter L of $\mathcal{F}$. Briefly, this is due to the fact that, for the discretization of $\mathcal{F}$, we may develop an upper and lower bound on the power received at the eavesdropper with maximum *SINR* whose ratio is independent of L.

5. PLACEMENT OF JAMMERS

In this section, we consider the problem of placing a minimum number of jammers all of which have the same transmission power $\hat{P}$.

We first give some basic definitions. Note that for every point $s \in \mathcal{S}$, according to Equation 2, if a jammer j lies in the disk $\mathrm{D}[s; \hat{P}^{1/\gamma}]$, it will prevent reception at s. We define the *forbidden region* $\varphi(\mathcal{S}) = \cup_{s \in \mathcal{S}} \mathrm{D}[s; \hat{P}^{1/\gamma}]$. This is essentially the Minkowski sum [4] of a disk with radius $\hat{P}^{1/\gamma}$ and $\mathcal{S}$; see Figure 3. Next, for a point $p \in \mathcal{F}$, according to Equation 3, a jammer must lie in the disk $\mathrm{D}[p; (\delta\hat{P})^{1/\gamma}/d(p, \mathcal{S}))]$. We call this the *critical disk* and denote it by D_p and define the *visibility region* $\mathrm{Vis}(p)$ as $(P_{\mathcal{F}} \cap \mathcal{D}_p) \setminus \varphi(\mathcal{S})$. This is the region in which a jammer must lie in the jammer space to successfully jam p; see Figure 3. We call two visibility regions $\mathrm{Vis}(p_1)$ and $\mathrm{Vis}(p_2)$ *adjacent* if their intersection is exactly one point.

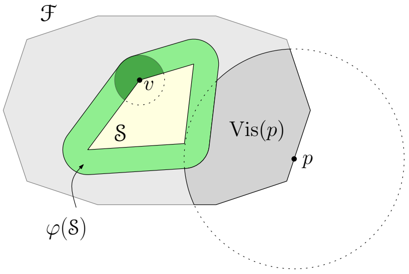
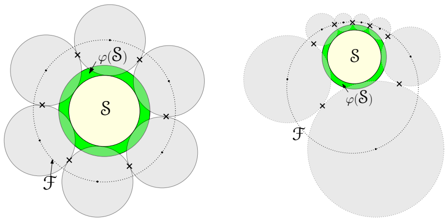


Figure 3: Forbidden region $\varphi(\mathcal{S})$ of $\mathcal{S}$ and visibility region $\mathrm{Vis}(p)$ for a point $p \in \mathcal{F}$.

Before we proceed with the algorithms, let us try and understand why this problem is challenging. Consider the simple examples in Figure 4. In both cases, we consider the NJ model. In Figure 4a, we have two disks which are concentric representing $\mathcal{S}$ and $\mathcal{F}$, while in Figure 4b, the disks are not concentric. Critical disks are also shown for various points on the fence. In both cases, an almost-optimal solution is to place the set of jammers at the points where two disks touch. In Figure 4a, since all critical disk are congruent, it is easy to characterize the optimal placement but in Figure 4b, it is not simple to characterize algebraically since the function of the distance between $\mathcal{S}$ and $\mathcal{F}$ is now more complicated. If, even in this simple example, the characterization of the problem is difficult, if we take into account all parameters such as jammer power, eavesdropper capability and possibly complicated shapes of $\mathcal{S}$ and $\mathcal{F}$, characterizing the solution seems to be particularly difficult.



(a) (b)

Figure 4: Two simple and similar examples where solutions differ significantly. The optimal placement of jammers is marked as ×.

With that in mind, we consider two basic settings: (i) when the jammer space $\mathcal{J}$ is a discrete set of points and (ii) when $\mathcal{J}$ is the entire region $P_{\mathcal{F}} \setminus \mathcal{S}$, where $P_{\mathcal{F}}$ is the polygon enclosed by $\mathcal{F}$. In the former, we give an ε-approximation algorithm and in the latter, we provide an optimal algorithm under a restricted setting.

5.1 ε-approximation given a discrete set of candidate locations

Given a discrete set of candidate locations $\mathcal{J}$ not in $\varphi(\mathcal{S})$, we discretize $\mathcal{F}$ and $\mathcal{S}$ using the scheme of Section 4. This gives us discrete sets $\mathcal{F}' \subset \mathcal{F}$ and $\mathcal{S}' \subset \mathcal{S}$. We can now design the following integer linear program JAMMING-ILP adapted from JAMMING-LP with binary variables c_i for each location $i \in \mathcal{J}$ indicating whether i is chosen or not.

$$\textsc{Jamming-ILP}: \textbf{Minimize} \sum_{i \in \mathcal{J}} c_i$$

$$\textbf{s.t. } \forall s \in \mathcal{S}' : \sum_{i \in \mathcal{J}} c_i \hat{P} \|s - i\|^{-\gamma} \leq 1, \qquad \text{(I)}$$

$$\forall p \in \mathcal{F}' : \sum_{i \in \mathcal{J}} c_i \hat{P} \|i - p\|^{-\gamma} > \frac{d(p, \mathcal{S})^{-\gamma}}{\delta}. \qquad \text{(II)}$$

Although JAMMING-ILPis formulated for the Full model of interference, it may easily be modified for the NJ model. This gives us the following theorem:

THEOREM 2. *Given storage region(s) $\mathcal{S}$, a fence $\mathcal{F}$, an interference model, a discrete set of candidate locations $\mathcal{J}$ for the jammers and a fixed power $\hat{P}$, we can find a minimum number of jammer locations from $\mathcal{J}$ such that Equation* (3) *is satisfied and for every point $s \in \mathcal{S}$, $SINR(s) > (1 - 2\varepsilon)$ by solving an Integer Linear Program with $O((n|\mathcal{J}|/\varepsilon)(\log(n/\varepsilon)$ $\log(|\mathcal{J}|/\varepsilon) + \log L))$ constraints.*

5.2 Near-optimal algorithm for a restricted setting

We consider the problem under the following restricted setting: **(i)** NJ interference model, **(ii)** $\mathcal{S}$ and $\mathcal{F}$ are convex, and **(iii)** each jammer is assigned a power $1/\delta$. Note that the assumption that each jammer has a power exactly $1/\delta$ implies that D_p for any $p \in \mathcal{F}$ will have radius exactly $d(p, \mathcal{S})$. Without this assumption, Lemma 5.1 does not hold and it is not possible to show almost-optimality for the algorithm.

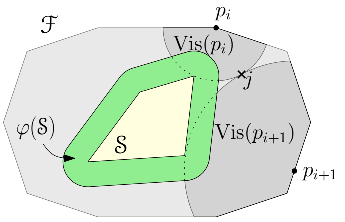


Figure 5: One step of the algorithm. p_{i+1} is selected such that $\mathrm{Vis}(p_i)$ and $\mathrm{Vis}(p_{i+1})$ are adjacent.

The algorithm proceeds as follows. We first pick an arbitrary point $p_0 \in \mathcal{F}$ as a starting point and keep finding adjacent regions by moving clockwise along the boundary until we reach a region which intersects $\mathrm{Vis}(p_0)$ again (see Figure 5). At the i^{th} step of the algorithm, we place a jammer

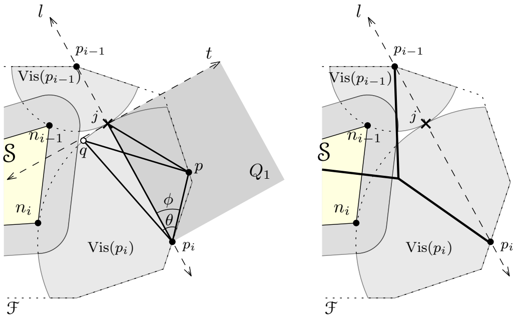
j_{i+1} at the point of intersection of $\text{Vis}(p_i)$ and $\text{Vis}(p_{i+1})$. Let p_k be the last point. We place a jammer j_{k+1} at the point in the intersection of $\text{Vis}(p_k)$ and $\text{Vis}(p_0)$ which is farthest from $\mathcal{S}$. Let J denote the set of jammers obtained.

The following lemma shows correctness as well as the fact that for each i, we need atleast one jammer.

Lemma 5.1. *Let p_{i-1}, p_i be two consecutive points selected and let j_i be the jammer placed at the point of intersection of* $\text{Vis}(p_{i-1})$ *and* $\text{Vis}(p_i)$. *The points jammed by j_i consists of the clockwise portion of $\mathcal{F}$ between p_{i-1} and p_i.*

Proof. First, we note that if $\text{D}_{p_{i-1}}$ and D_{p_i} are not tangential, j is placed at the their point of intersection away from $\mathcal{S}$. This is the single point of intersection of $\text{Vis}(p_{i-1})$ and $\text{Vis}(p_i)$. Let l denote the line passing through p_{i-1} and p_i and t denote the line passing through j perpendicular to l. l and t separate the plane into four quadrants. The portion of the fence in between p_{i-1} and p_i must clearly lie in the two quadrants which does not contain $\mathcal{S}$. Consider an eavesdropper location p between p_{i-1} and p_i on the quadrant Q_1 containing p_i; see Figure 6a. $\mathcal{S}$ must lie wholly in the sector Ψ_P formed by the lines through the points (p, p_i) and (p, j) of smaller angle. For a point $q \in \Psi_p$ which also lies on the boundary of $\mathcal{D}_{p_i}$, consider the angles $\theta = \angle p, p_i, q$ and $\phi = \angle p, p_i, j$ at p_i. It is easy to see that $\theta > \phi$ for every p. Hence, $\|p - j\| \leq \|p - q\|$. The proof for the other quadrant which contains p_{i-1} is similar.

Moving on to the second part, first, let $n_{i-1} = \text{NN}(p_{i-1}, \mathcal{S})$ and $n_i = \text{NN}(p_i, \mathcal{S})$. Clearly, $\|p_i - n_i\| = \|j - n_i\|$ and $\|p_{i-1} - n_{i-1}\| = \|j - n_{i-1}\|$, implying that the Voronoi diagram of $\{j, n_{i-1}, n_i\}$ (see Section 4 for a description of Voronoi diagrams) must pass through p_i and p_{i-1}, implying that the portion of $\mathcal{F}$ clockwise from p_i to p_{i-1} does not lie in the Voronoi cell of j as then, $\mathcal{F}$ would not be convex. Thus, all points of $\mathcal{F}$ in the portion clockwise from p_i to p_{i-1} are closer to either n_i or n_{i-1} than j, implying that they are not jammed. □



(a) (b)

Figure 6: Illustration of the proof of Lemma 5.1

We are now ready to bound the number of jammers in J.

Lemma 5.2. *Let* OPT *be the size of the optimal set of jammers. Then,* $|J| \leq \text{OPT} + 1$.

Proof. For each interval along the fence $[p_i, p_{i+1}]$, by Lemma 5.1, j_{i+1} is the only location where a jammer can jam every point on $[p_i, p_{i+1}]$ and does not jam any other point, implying that we need atleast one jammer for this interval. The proof follows. □

Putting it all together, we get the following theorem.

Theorem 3. *Given convex $\mathcal{S}$ and $\mathcal{F}$, when jammers have power $\hat{P} = 1/\delta$, we can find a set of jammer locations J in the jammer space such that Equation* (2) *and Equation* (3) *are satisfied under* NJ *model of interference and* $|J| \leq |OPT| + 1$. *The time required is polynomial in* $\max\{\text{OPT}, n\}$ *where* OPT *is the size of the optimal solution.*

Remarks. The solution guarantee does not hold when ambient noise is present. Further, the algorithm and its correctness proof outline the conditions under which guaranteed solutions may be obtained and serve to demonstrate the difficulty of the problem in general. Therefore, it is of primarily theoretical importance.

6. EXTENSIONS

We extend the algorithms of Sections 4 and 5 in two ways: (i) we show how to provide a solution to the combined problem of power assignment and placement of jammers while optimizing a linear combination of the total power and number of jammers, (ii) if eavesdroppers are equipped with directional antennas, we show how to extend Jamming-LP and Jamming-ILP to incorporate this fact while still maintaining a tractable number of constraints.

6.1 Combined Solution

We may develop a combined solution when given a discrete set of candidate locations $\mathcal{J}$ as follows. We set a weighting parameter μ, and define the cost functions $\sum_{j \in \mathcal{J}} c_j + \mu \sum_{j \in \mathcal{J}} P_j$, where $c_j \in \{0, 1\}$ and P_j is the power assigned to jammer j. If no jammer is located at j, this is simply indicated by a value of $P_j = 0$. Here, the weighting parameter μ specifies how we prefer one criteria versus the other. We substitute this in Jamming-ILP to get the desired program.

6.2 Directional eavesdroppers

Let eavesdroppers be equipped with *directional antennas* which may be orientable. Such an antenna would enable the eavesdropper to receive more powerful signals in one direction while other directions would have reduced power. If jammers are sparse enough, eavesdroppers could avoid interference. We model the beam of a directional antenna as a cone of opening angle θ, centered at the eavesdropper. Under this (simplified) model, the eavesdropper receives a signal, from a transmitter only if it lies in this cone.

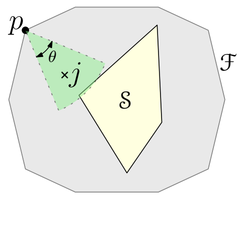


Figure 7: Jammer j needs to lie in the range of the directional antenna of eavesdropper p to affect p.

Given a discrete set of candidate locations $\mathcal{J}$, We need to find jammer locations and/or power assignment such that no such direction exists, so that for every cone orientation and location, there exists a jammer in this cone which would jam the signal from any point in $\mathcal{S}$ in the cone; see Figure 7. It is important to note that this is particularly applicable to RFID communication because, due to the low frequencies of RFID tags (13.56 Mhz), θ would be relatively large.

THEOREM 4. *Given θ, the opening angle of a directional antenna used by the eavesdropper, it is possible to find an ε-approximation to both power allocation and jammer placement problems by solving a linear program with polynomial number of constraints.*

PROOF SKETCH. First, we note that, for a point on $\mathcal{F}$, if there exists an orientation of the directional antenna where no jammer in $\mathcal{J}$ exists in the cone at this orientation, then it is not possible to jam this point. Thus, we assume that there does not exist any location on the fence with an orientation that contains no points in $\mathcal{J}$.

First, we obtain the set $\mathcal{F}'$ as in Section 4. However, to the set $\mathcal{F}'$, we add further points to obtain a new set $\mathcal{F}''$. Consider a point $p \in \mathcal{F}$. If we perform a circular sweep of a cone Ψ with p as apex, we have many "events" corresponding to some point $j \in \mathcal{J}$ or some vertex v of $\mathcal{S}$ added/deleted from Ψ. The number of such events is $O(n + |\mathcal{J}|)$. The set $\mathcal{F}''$ is constructed in such a manner that for each interval (u, v) on the fence obtained from consecutive points $u, v \in \mathcal{F}''$, two points in (u, v) have the same order of the sweep events.

For a location $p'' \in \mathcal{F}''$, we add a constraint for each "event" of the circular sweep. In between the events, the closest point in the storage is farther than at one of the events and the set of jammer candidates is the same. Since the number of events is $O(n+|\mathcal{J}|)$, we have only a polynomial number of constraints in total. □

7. SIMULATIONS

We conducted preliminary experiments to compare the NJ and Fullmodels. The setting we have chosen is the storage/fence shown in Figure 9. The fence is of dimensions 50x33 units and we placed a grid of 1x1 cells in the entire region. We simulated both JAMMING-LPand JAMMING-ILPin this setting. For the power assignment from JAMMING-LP, we investigated the difference in power and for JAMMING-ILP, we investigated the difference in number of jammers. Finally, we observed the variation in total power assigned with ε and δ and the number of jammers placed with ε, δ and $\hat{P}$. We chose the following values: (i) $\varepsilon = \{0.1, 0.2, 0.3, 0.4, 0.5\}$, (ii) $\delta = \{0.5, 0.6, \ldots, 1\}$, (iii) $\hat{P} = \{(1/\delta), (2/\delta), \ldots, (5/\delta)\}$. In both Full and NJ, we removed all grid points which were in the forbidden region.

For JAMMING-LP, we picked 10 random points from this set of grid points, repeated the simulation 50 times and calculated the mean and variance. Figure 8(a) shows the variation in total relative power with δ, which indicates how much more capable the eavesdropper is than legitimate receivers. As the eavesdropper gets more capable than storage receivers, the drop in the total relative power under NJ model is sharper than under Full model. The gap between them seems to be no more than constant-factor (approximately 2-3 times) but is definitely not negligible. However, the variance in NJ is also extremely high (ranging from aroung 60 to 100 vs 5 to 20 for the Full model). Possibly, the random selection of jammer locations leads to the large variance over different choices. The variance is likely to be much more in NJ model because each jammer contributes all the interference at a large number of nodes instead of only being a part of the entire jammer set. This emphasizes the importance of carefully locating the jammers. We conclude that, in practical scenarios, it would be of benefit to consider the combined problem of location and power assignment rather than computing an optimal power assignment for a naive placement of jammers. Further, the graph indicates that as the eavesdropper gets more and more capable, the effectiveness of the NJ model diminishes.

For JAMMING-ILP, the candidate jammer locations were all the points on the grid. In total, there are 1121 points. Figure 8(b) and Figure 8(c) show the variation of the number of jammers located with the power assigned and with δ, respectively. In this case, we note that NJ model and Full model are not far apart thus demonstrating the benefits of NJ model in this example setting. We noted that there was no significant variation in total relative power or number of jammers with ε indicating that even choosing large values of ε would yield results better than theoretical guarantees.

8. CONCLUSION

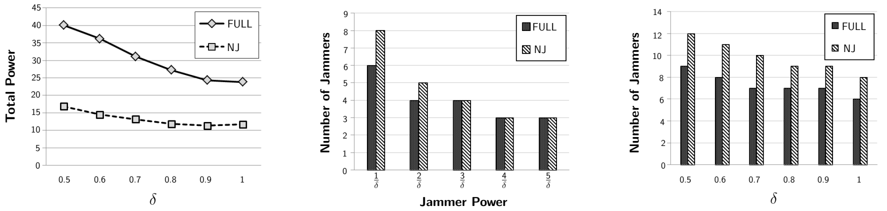
We considered the problem of friendly jamming under the storage/fence environment model when jammers are both cooperative and non-cooperative. We presented ε-approximation algorithms for the problem of assigning transmission powers to a set of fixed jammers as well as for selecting a minimum number of jammers from a discrete candidate set. We also presented an algorithm to place a near-optimal number of jammers when the jammers may be located anywhere between the storage and fence under a restricted setting. The former algorithms were extended to provide a combined solution where we are interested in achieving a tradeoff between number of jammers and power consumption, as well as to the setting where eavesdroppers may be equipped with directional antennas. Our preliminary simulations validated the theoretical results and show that the simpler non-cooperative model may not be significantly different than the cooperative model. Further, for the power assignment problem, the simulations also show that careful location of the jammers is paramount and further emphasizes the importance of the jammer placement problem.

Finally, we mention two directions in which this work may be extended: (i) When jammers use directional antennas, although the power of the jammers is now concentrated, it is not clear whether we may obtain better results. For example, if the storage and fence were convex regions, then using directional antennas could remove the jammers' effect on the storage but in general, it is not obvious whether this would be the case. Moreover, the region of influence of jammers is reduced leading to possibly a greater number of required jammers. (ii) It would also be constructive to see if battery-power jammers may be deployed and if we may schedule their transmissions so as to successfully protect the storage while maximizing their operating time.

Acknowledgments

The authors would like to thank Paz Carmi, Esther Ezra, Matya Katz, Anantha Raman Krishnan and Zvika Lotker for enlightening discussions. The authors would also like to thank the anonymous reviewers for their useful comments.

Valentin Polishchuk is supported by Academy of Finland grant 135280.



(a) JAMMING-LP*: Total Power vs eavesdroppers' capability (δ).*

(b) JAMMING-ILP*: Number vs power of jammers.*

(c) JAMMING-ILP*: Number of jammers vs eavesdroppers' capability (δ)*

Figure 8: Results of simulations with Jamming-LPand Jamming-ILP.

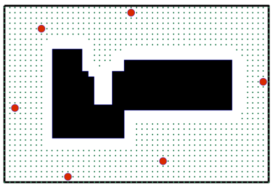


Figure 9: Storage/fence with candidate locations (small dots) and solution of Jamming-ILP(Large dots).

9. REFERENCES

[1] L. V. Ahlfors. *Complex analysis: an introduction to the theory of analytic functions of one complex variable*. International series in pure and applied mathematics. McGraw-Hill, 1979.

[2] F. Aurenhammer. Voronoi diagrams-a survey of a fundamental geometric data structure. *ACM Comput. Surv.*, 23(3):345–405, 1991.

[3] C. Commander, P. Pardalos, V. Ryabchenko, S. Uryasev, and G. Zrazhevsky. The wireless network jamming problem. *J. Comb. Optim.*, 14(4):481–498, 2007.

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

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

[6] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes. Physical layer security game: Interaction between source, eavesdropper, and friendly jammer. *EURASIP J. Wirel. Comm.*, pp. 11:1–11:10, Jun. 2009.

[7] T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O'Hare. Vulnerabilities in first-generation rfid-enabled credit cards. In *Financial Cryptography and Data Security*, vol. 4886 of *LNCS*, pp. 2–14. Springer, 2007.

[8] A. Juels. Rfid security and privacy: a research survey. *IEEE J. Sel. Area. Comm.*, 24(2):381–394, 2006.

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

[10] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In *Proc. 8th ACM Conf. on Computer and Communications Security*, pp. 103–111, 2003.

[11] D. G. Kirkpatrick. Efficient computation of continuous skeletons. In *Proc. 20th Annual Sympos. on Foundations of Comp. Sci.*, pp. 18–27, 1979.

[12] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE T. Inform. Theory*, 54(9):4005 –4019, 2008.

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

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

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

[16] J. Nehmer, M. Becker, A. Karshmer, and R. Lamm. Living assistance systems: an ambient intelligence approach. In *Proc. 28th Int. Conf. on Software Engineering*, pp. 43–50, 2006.

[17] K. Nohl, D. Evans, Starbug, and H. Plötz. Reverse-engineering a cryptographic rfid tag. In *Proc. USENIX Security Sympos.*, pp. 185–193, 2008.

[18] 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*, vol. 4217 of *LNCS*, pp. 159–170. Springer, 2006.

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

[20] T. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall PTR, 2001.

[21] N. X. P. Semiconductors. Mifare classic 1k. `http://www.nxp.com/documents/data_sheet/MF1S50YYX.pdf`.

[22] M. Simplício Jr., P. Barreto, C. Margi, and T. Carvalho. A survey on key management mechanisms for distributed wireless sensor networks. *Comp. Netw.*, 54(15):2591–2612, 2010.

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

[24] A. Vigneron. Geometric optimization and sums of algebraic functions. In *Proc. 21st Annual ACM-SIAM Sympos. on Discrete Algorithms*, pp. 906–917, 2010.

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

[26] Y. Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys Tutorials*, 8(2):2–23, 2006.

[27] W. Weber, J. M. Rabaey, and E. H. L. Aarts, editors. *Ambient intelligence*. Springer-Verlag, 2005.

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