Wrocław University
of Science and Technology

Information hiding in chosen constrained network models

Doctoral dissertation

Mateusz Marciniak

Supervisor: **prof. dr hab. inż. Marek Klonowski**

Faculty of Information and
Communication Technology

Abstract

This thesis focuses on securing some protection aspects of communication in different network models. For the popular SINR model, different algorithms are presented for blocking the wireless signal at some chosen fragments of space, called *restricted areas*, using the *protective jamming*. This approach utilizes jamming stations, which generate interference that floods the restricted areas, blocking the signal of the network being protected. The algorithms are designed to maximize the *coverage* of the network - the value that allows measuring the negative impact of jamming on the network reception zones outside of restricted areas. Moreover, as the secondary goal, they target minimizing energy usage by the jamming networks. The solutions for this problem are presented for 1D and 2D versions of the network model.

In the 1D SINR part, the thesis presents multiple algorithms for the uniform network model, wherein all stations transmit with the same power. Two basic algorithms apply a positioning scheme for the restricted area represented by one or two barrier points but with some limited guarantees about the coverage effectiveness of the solution. The precise positioning algorithm is also described, which applies the procedure with a potentially high number of iterations to place the jamming stations but guarantees almost perfect coverage of the solution. For the 1D non-uniform model, there are two algorithms. One is based on single-side jamming with a high-power jamming station. The second one utilizes the noisy-dust strategy to position many jamming stations with relatively small power - effectively flooding the restricted area with interference. This algorithm has the property that with the decrease of jamming station power and increase of their number, the overall energy utilization converges to zero. A variant of the noisy algorithm is presented, which simplifies the positioning scheme but increases energy utilization.

The thesis defines particular types of restricted areas for the 2D SINR model, wherein the problem complexity increases substantially. For the uniform 2D networks, an algorithm is presented that allows for jamming the restricted areas surrounding the spaces shaped as convex polygons. It presents how to utilize this algorithm for the areas surrounding circular shapes and the experimental analysis of its effectiveness. The noisy-dust extension is presented for the non-uniform model, wherein stations with small powers are positioned inside the hexagonal grid, tiling the restricted areas. The algorithm shows its 1D version property of reducing the overall energy usage of the jamming network with a decrease in the jamming stations' powers, arbitrarily close to zero. Coverage, measured experimentally, also shows the high effectiveness of this algorithm.

The thesis investigates the problem of hiding the number of stations executing some types of protocols for the single-hop networks in the beeping model. The *size-hiding* property is defined, based on the popular *differential privacy*, along with the universal algorithm, which can be used as a pre-processing step for chosen types of protocols. The limitations of this universal algorithm are discussed and compared with the size-hiding properties of an algorithm from the literature.

The aforementioned problem is generalized in the last part of the thesis, wherein preliminary studies for hiding network details and executed algorithms facing an adversary observing the execution in a multi-hop network are presented. We present an extensive taxonomy of the considered model, including the capabilities of the adversary and network configurations. We also presented two general algorithms for chosen model settings.

Streszczenie

Rozprawa skupia się na zapewnianiu bezpieczeństwa pewnych aspektów komunikacji dla różnych modeli sieci. Dla popularnego modelu SINR zaprezentowane są różne algorytmy blokujące sygnał radiowy dla wybranych fragmentów przestrzeni, nazwanych *obszarem ograniczonym*, z wykorzystaniem techniki nazwanej *zagłuszaniem ochronnym*. To podejście wykorzystuje dodatkowe stacje, które generują zakłócenia, mające na celu pokryć cały obszar ograniczony i zablokować sygnał chronionej sieci na tym obszarze. Algorytmy są zaprojektowane tak, aby jednocześnie maksymalizować *pokrycie* sieci, czyli wartość, która pozwala mierzyć negatywny wpływ zagłuszania na sieć poza obszarami ograniczonymi. Ponadto, jako dodatkowy cel, algorytmy starają się minimalizować wykorzystanie energii przez sieć zakłócającą. Rozwiązania dla tego problemu są przedstawione dla modelu jedno oraz dwuwymiarowego sieci SINR.

Dla modelu SINR w 1D rozprawa prezentuje kilka algorytmów dla jednolitego modelu sieci, gdzie wszystkie stacje transmitują z identyczną mocą. Dwa podstawowe algorytmy wykorzystują specjalny schemat pozycjonowania stacji dla obszarów ograniczonych reprezentowanych przez jeden lub dwa punkty ograniczające, ale z pewną gwarancją dotyczącą wpływu ich rozwiązań na *pokrycie*. Opisany jest również precyzyjny algorytm pozycjonujący, który wykorzystując iteracyjną procedurę w celu ustawienia stacji zakłócających, gwarantuje niemal idealną wartość *pokrycia*. Dla modelu 1D z niejednolitymi stacjami przedstawione są dwa algorytmy. Jeden bazuje na wykorzystaniu jednej stacji o dużej mocy, aby zapewnić jednostronne zagłuszanie. Drugi algorytm wykorzystuje strategię *noisy-dust*, która zakłada wykorzystanie bardzo dużej liczby stacji zagłuszających o małej mocy — poprzez poprawne ich ustawienie, mogą efektywnie pokryć zakłóceniami wybrane obszary. Ten algorytm umożliwia również redukcję zużycia energii, która maleje razem z mocą pojedynczych stacji i wzrostem ich liczby w celu zagłuszania danego obszaru. Przedstawiony jest również wariant algorytmu, który kosztem większego zużycia energii umożliwia łatwiejsze pozycjonowanie stacji.

Dla modelu 2D zdefiniowane są specjalne typy obszarów ograniczonych, ze względu skomplikowanie problemu dla dowolnych kształtów. Dla jednolitych sieci 2D przedstawiony jest algorytm umożliwiający zagłuszanie obszarów ograniczonych zdefiniowanych jako strefy otaczające różne wypukłe wielokąty. Przedstawiona jest metoda, jak wykorzystać ten algorytm, gdy strefy bazują na kołach oraz przedstawiona jest eksperymentalna analiza efektywności tego algorytmu. Dla modelu niejednolitego przedstawiony jest algorytm *noisy dust*, który ponownie bazuje na stacjach o niewielkich mocach, ale tym razem układa je wewnątrz sześciokątów, które tworzą siatkę wypełniającą obszary ograniczone. Ten algorytm również dla modelu 2D wykazuje własność redukcji zużycia energii stacji zakłócających razem z ich mocą i wzrostem ilości stacji, umożliwiając uzyskanie niemal zerowego zużycia energii, oraz dużej efektywności względem wartości pokrycia.

W rozprawie analizowany jest również problem ukrywania liczby stacji dla sieci typu *single-hop* z wykorzystującej tzw. *beeping model*. Zdefiniowana jest własność ukrywania rozmiaru sieci (*size-hiding*) oparta o popularną koncepcję prywatności różnicowej. Przedstawiamy także uniwersalny algorytm, który może być wykorzystany jako wstępny krok dla wybranych typów protokołów w celu zapewnienia własności ukrywania rozmiaru. Przedstawione są ograniczenia tego algorytmu oraz jego efektywność jest porównana z własnościami ukrywania rozmiaru sieci wybranych, klasycznych algorytmów.

Podobny problem jest analizowany w kontekście sieci *multi-hop*. Przedstawiona jest wstępna analiza tego bardziej skomplikowanego modelu, razem z taksonomią możliwych modeli adwersarza i konfiguracji sieci. Przedstawione zostały dwa uniwersalne algorytmy dla wybranych założeń modelu oraz przeprowadzona została analiza ich własności.

Contents

Chapter 1

Introduction

In recent decades, network communication has been growing rapidly. Increasing demand for more stable and flexible connectivity resulted in the global spread of distributed and wireless communication systems. The Internet, which started as a project targeting the military and research usage [1], has grown steadily over the last years. With 4.95 billion users in 2022 (accounting for 62.5% of the world population), it more than doubled its users' number of 2.177 billion from 2012 [2]. Together with the Internet, the popularity of wireless technologies was increasing. The widespread of mobile cellular networks and Wi-Fi networks allows for convenient communication and access to the network even in very remote localizations - the 4G technology global population coverage surpassed 85% at the end of 2021 and is expected to reach 95% by 2028 [3].

Wireless communication impacts many industries [4]. For automotive, it allows for more comfortable user interactions with the vehicle and infrastructure - by providing navigation services, a possibility for better traffic management, automated toll collection systems, and even better recreational services access, like music streaming from the smartphone to the vehicle audio systems [5]. From the maintenance perspective, it allows easy access to diagnostic data through wireless sensors. It provides enhanced security services, like anti-theft systems or notifying emergency services about accidents. It is also crucial for autonomous vehicle development [6] or other related technologies, like VANET [7, 8].

In healthcare, the wireless networks can be used for medical sensors to monitor the patient's well-being, support large-scale medical studies by efficiently collecting data in non-laboratory environments, or enable communication with implants [9]. It might allow for better emergency support by better communication with the patient and acquiring the crucial data required for treatment earlier [10]. It can also give better access to telemedicine or support the rehabilitation process by enabling VR and AR devices [11]. Easy access to mobile technologies helped in the recent outbreak of COVID-19 to monitor the disease spread and target the help efforts in the places needing it the most [12, 13].

It is also utilized in manufacturing [14], military [15], agriculture [16], and many other fields. It impacts people in different life domains, like social life and recreation [17]. To comply with the population needs, many new technologies and concepts emerged in recent years, like *Internet of Things* (IoT) [18], 5G [19, 20] and even smart cities [21], among others.

All these technologies and uses of wireless networks have high requirements regarding the security and privacy of communication. Many threats exist, like intercepting the transferred data or interfering with the transmissions [22]. In some scenarios, even the knowledge that some wireless communication medium was used can expose the user to danger [23, 24]. It is crucial to analyze such threats and design solutions to prevent the potential adversary from overhearing the communication or manipulating its content.

This thesis presents a set of protocols for protecting some aspects of communication safety and privacy in different network models with limited resources. The first part is dedicated to the popular *Signal to Interference & Noise Ratio* model [25]. It imitates real wireless networks by decreasing the signal with distance and incorporating interference and

ambient noise to check if the signal reaches specific fragments of space. The protocols presented in this part focus on positioning special *jamming stations*, which block the signal in chosen fragments of space, preventing the adversary from receiving the signal. The model is defined for a D-dimensional space, but the presented protocols are dedicated to 1D and 2D spaces. Inside these two sub-groups, they are designed for uniform and non-uniform network configurations and employ a range of different positioning schemes, which might be optimal in different scenarios. One of the main requirements for designing these protocols was to reduce the unnecessary impact on the space where transmission is allowed - as jamming introduces additional interference, the inaccurately positioned and configured stations could prevent critical communication where they should not. Additionally, as the secondary goal, the energy required by the jamming network is analyzed and minimized. Notably, a group of *noisy dust* algorithms, introduced in this thesis, allows for a very effective reduction of energy usage by increasing the number of used jamming stations.

The second part of the thesis focuses on the single-hop radio networks and *beeping model*. The protocols there are focused on hiding the size of the network under the *size-hiding* property - defined in this thesis and based on popular *differential privacy* [26]. The significant contribution from this part is the pre-processing algorithm, which allows hiding the number of communicating stations by *faking* the existence of some additional, dummy stations.

Finally, the extended problem of hiding the parameters of a network and the executed algorithm is analyzed under the multi-hop radio network model. The *hiding property* is defined for this type of network along with a preliminary listing of possible network communication channel types, adversary types, and a taxonomy of other properties that can be used for analyzing the hiding properties of multi-hop networks. Two general algorithms with a formal analysis of their properties are also presented.

Thesis structure

This thesis is split into six chapters.

Chapter 1 (Introduction) introduces the motivation behind the analyzed topics, broadly presents the main contributions from the thesis, and describes its structure.

Chapter 2 (SINR network model) describes the SINR model and related notation. It defines the protective jamming problem in detail and presents the literature related to SINR networks and jamming.

Chapter 3 (Jamming in 1D SINR) presents protocols for 1D network. It starts with simple, uniform network positioning schemes, which do not have any extensive algorithmic requirements and provide protection without any considerable impact on protected stations' communication outside of restricted areas. Then, the precise jamming algorithm for a uniform network, which places stations arbitrarily close to their optimal positions, is presented. After that, two protocols dedicated to non-uniform networks are described. The second introduces the *noisy dust* scheme. Chapter is based on our paper [27]. Positioning schemes from this section are listed in the table below:

Section	Uniformity	# Jamm. stat.	Restricted area	Description
Sec. 3.1	uniform	1	(b, ∞)	Theorem 3
Sec. 3.2	uniform	2	$(-\infty, b_l) \cup (b_r, \infty)$	Theorem 4
Sec. 3.3	uniform	2	$(-\infty, b_l) \cup (b_r, \infty)$	Theorem 5
Sec. 3.4	non-uniform	1	(b, ∞)	Theorem 7
Sec. 3.5.2	non-uniform	multi	(b, ∞)	Theorem 9
Sec. 3.5.3	non-uniform	multi	(b_0, b_1)	Theorem 10

Chapter 4 (Jamming in 2D SINR) analyzes protocols in 2D space. The problem is refined for specific 2D configurations, and the solutions for uniform and non-uniform (using a noisy dust scheme) networks are presented. Chapter is based on our paper [28]. Positioning schemes from this section are listed in the table below:

Section	Uniformity	# Jamm. stat.	Restricted area	Description
Sec. 4.2.2	uniform	1 per polygon side	complement of a polygon	Theorem 12
Sec. 4.2.3	uniform	multi	complement of a disk	Fact 2
Sec. 4.3	non-uniform	multi	arbitrary 2D shape	Theorem 14

Chapter 5 (Size-hiding protocols in Beeping Model) introduces the formal model of size-hiding execution for the single-hop radio networks beeping model. It presents the universal protocol for hiding a count of its participants, which can be used as a pre-processing phase for other protocols. The Green Leader Election [29] is analyzed in relation to its size-hiding capabilities. Chapter is based on our paper [30].

Chapter 6 (Information hiding in multi-hop networks) presents the preliminary research of the hiding properties for multi-hop radio networks. Basic network configurations and adversary models are presented. Moreover, two universal algorithms are analyzed for their hiding properties. Chapter is based on our paper [31].

Chapter 7 (Conclusion) discusses the summary of presented algorithms and the possible research paths extending the analyzed problems.

Author contribution

The content of the thesis is largely based on the following publications:

- [27] *Exact and Efficient Protective Jamming in SINR-based Wireless Networks*, D. Bojko, M. Klonowski, D. R. Kowalski, M. Marciniak, *29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2021.
  Author contribution:
  - design of 1D algorithms for one-side jamming in the uniform model,
  - concept and design of the noisy dust algorithm in the non-uniform model,
  - simulations, testing, and experimental analysis of the uniform model one-side jamming, precise two-side jamming, and noisy dust algorithms.
- [28] *Efficient Protective Jamming in 2D SINR Networks*, D. Bojko, M. Klonowski, D. R. Kowalski, M. Marciniak, *29th International European Conference on Parallel and Distributed Computing (EuroPar)*, 2023.
  Author contribution:
  - defining the different 2D model configurations,
  - design and analysis of the uniform model algorithm for jamming in a 2D uniform network and simulations of this model for multiple configurations,
  - design and analysis of noisy-dust algorithm extension into 2D, with algorithm simulations and zero-energy property analysis.
- [30] *On Size Hiding Protocols in Beeping Model*, D. Bojko, M. Klonowski, M. Marciniak, P. Syga, *29th International European Conference on Parallel and Distributed Computing (EuroPar)*, 2023.
  Author contribution:

  - analysis of different approaches to hiding the size of the beeping model network under different algorithms,
  - Experimental analysis of the Universal Algorithm and the Green Leader Election algorithm.

- [31] *Preliminary Report: On Information Hiding in Multi-Hop Radio Networks*, M. Klonowski, M. Marciniak, *arXiv.org*, 2023. **Author contribution:**
  - literature research about different models, taxonomy, and algorithms for multi-hop networks,
  - construction of the first universal algorithm,
  - construction of the second algorithm and its initial analysis.

Chapter 2

SINR network model

The SINR (*Signal to Interference & Noise Ratio*) is a quantity that can be used to measure the quality of wireless communication. It considers both the decay of the signal power with an increase in distance from the transmitter and the interference of the other transmitters. It is believed to model the radio network reception zones realistically [32]. It can be generalized for any network dimension and allows configuring different parameters but still encapsulates it into a single equation, allowing for a precise analysis of algorithms. Although it has a simple form, the analysis can get very complicated even for a seemingly small number of stations and basic configuration parameters, as will be presented in the following thesis chapters. In this chapter, the basic geometric notation is introduced in Section 2.1, followed by a formal model of a SINR network in Section 2.2. The major problem analyzed in this thesis, concerning SINR, is presented in Section 2.3 and the SINR-related literature is analyzed in Section 2.4.

2.1 Basic notation

Consider the D-dimensional Euclidean space. A **point** is denoted as:

$$p = (p_1, \ldots, p_D) \in \mathbb{R}^D \ .$$

The point notation for $D = 1$ is simplified to just $p = p_1$ for readability. A D-dimensional Euclidean **metric** d is defined for points $x = (x_1, \ldots, x_D)$ and $y = (y_1, \ldots, y_D)$ as:

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_D - y_D)^2} \ .$$

A **vector** is denoted as:

$$\overrightarrow{v} = \overrightarrow{(v_1, \ldots, v_D)} \ .$$

A **line segment** between points $p_0 \in \mathbb{R}^D$ and $p_1 \in \mathbb{R}^D$ is denoted as:

$$\overline{(p_0, p_1)} \ .$$

A D**-ball** is defined for a radius r and a point $p \in \mathbb{R}^D$ as:

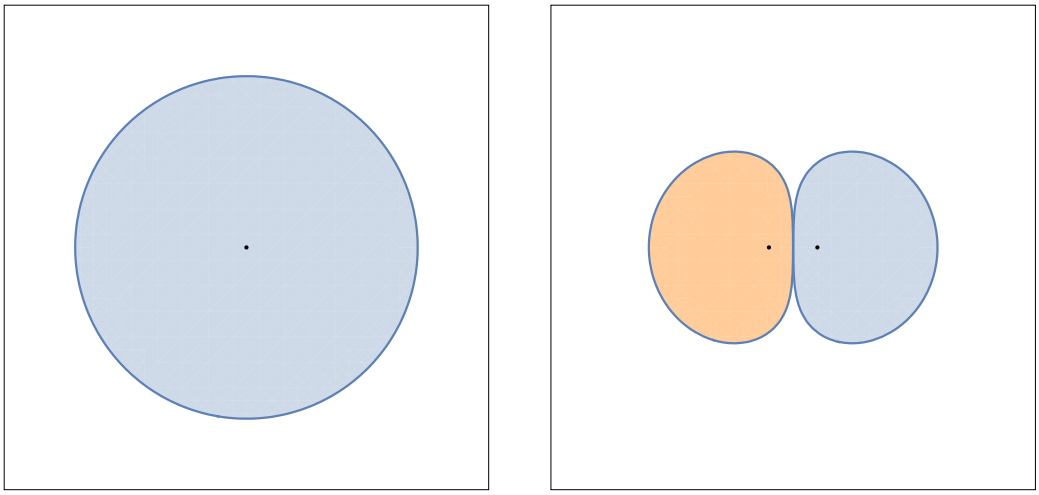
$$\mathcal{B}(r, p) = \{x \in \mathbb{R}^D : d(x, p) \leqslant r\} \ .$$

Moreover, the following notation is used:

$$[n] = \{1, \ldots, n\} \ .$$

2.2 Network model

The well-established definition of the **SINR (Signal to Interference & Noise Ratio)** network from literature ([25, 33]) is used.



(a) Single station's reception zone. (b) Two stations.

Figure 2.1: Comparison between a single station reception zone and how other station's interference impacts it.

Definition 1.1. *The **SINR network** is defined as a tuple $\mathcal{A} = \langle D, S, N, \beta, P, \alpha \rangle$, where:*

- $D \in \mathbb{N}$ *is the dimension of a network, in real-world scenarios limited to* $D \in \{1, 2, 3\}$,
- $S = \{s_1, \ldots, s_n\}$ *is a set of stations' positions in* $\mathbb{R}^D$,
- $N \geqslant 0$ *is a value of the ambient noise,*[1]
- $\beta \geqslant 1$ *is a value of the reception threshold,*
- $P : S \to \mathbb{R}$ *is the stations' power function;* $P_i = P(s_i)$ *denotes the power of station* s_i,
- $\alpha \geqslant 2$ *is the path-loss parameter.*

Definition 1.2. *For a* SINR *network* $\mathcal{A}$*, the **SINR function** is defined for a station* $s_i \in S$ *and a point* $x \in (\mathbb{R}^D \setminus S)$ *as:*

$$\mathrm{SINR}_{\mathcal{A}}(s_i, x) = \frac{P_i \cdot d(s_i, x)^{-\alpha}}{N + \sum\limits_{s_j \in S \setminus \{s_i\}} P_j \cdot d(s_j, x)^{-\alpha}} \ ,$$

where d is a D-dimensional Euclidean metric.

A point $x \in \mathbb{R}^D$ is able to receive the transmission from a station s only if:

$$\mathrm{SINR}_{\mathcal{A}}(s, x) \geq \beta \ .$$

That is, the s station's signal is received only if in position x it is equal to or exceeds the reception threshold β.

Definition 1.3. *The **reception zone** of a station s for a network $\mathcal{A}$ is defined as:*

$$H_s^{\mathcal{A}} = \{x \in \mathbb{R}^D : \mathrm{SINR}_{\mathcal{A}}(s, x) \geq \beta\} \ .$$

The visual example of the reception zone is presented in Figure 2.1a. The **energy** of a station s_i at a point x is expressed as:

$$E_{\mathcal{A}}(s_i, x) = P_i \cdot d(s_i, x)^{-\alpha} \ .$$

[1] The case of $N = 0$ is considered in literature as SIR model.

The cumulated **interference** (see Figure 2.1b for how stations interfere with each other) of stations different from s_i, generated at a point x, is denoted as:

$$I_{\mathcal{A}}(s_i, x) = \sum_{s_j \in S \setminus \{s_i\}} E_{\mathcal{A}}(s_j, x) = \sum_{s_j \in S \setminus \{s_i\}} P_j \cdot d(s_j, x)^{-\alpha} \ .$$

The corresponding definition of a SINR function can be rephrased as:

$$\mathrm{SINR}_{\mathcal{A}}(s_i, x) = \frac{E_{\mathcal{A}}(s_i, x)}{N + I_{\mathcal{A}}(s_i, x)} \ .$$

Similarly, the noiseless counterpart is defined as SIR.

Definition 1.4. *For a* SINR *network $\mathcal{A}$, the* ***SIR function*** *for a station $s_i \in S$ and a point $x \in (\mathbb{R}^D \setminus S)$ is defined as:*

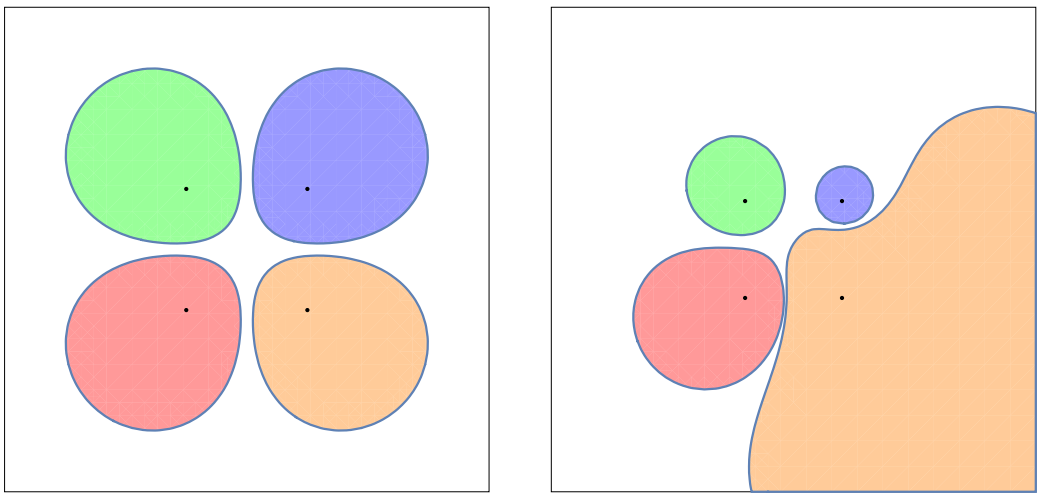
$$\mathrm{SIR}_{\mathcal{A}}(s_i, x) = \frac{E_{\mathcal{A}}(s_i, x)}{I_{\mathcal{A}}(s_i, x)} \ .$$

For networks with a non-zero value of noise[2], there is also the definition of a *range*, representing the theoretical maximal distance from a station, where any point can receive its signal after excluding interference from other stations.

Definition 1.5. *The* ***range*** *of a station s for a network $\mathcal{A}$ with a positive noise value ($N > 0$) is defined as:*

$$\mathrm{range}_{\mathcal{A}}(s) = \left(\sqrt[\alpha]{\frac{N\beta}{P}} \right)^{-1} \ .$$

Stations may transmit with different parameters. If all network stations use the same power level P, then the network is called uniform.



(a) Uniform network example. All stations transmit with identical power P.

(b) Non-uniform network example. Stations have different power levels $P_0 < P_1 < P_2 < P3$.

Figure 2.2: Different shapes of reception zones, depending on the uniformity of the network.

Definition 1.6. *The network $\mathcal{A} = \langle D, S, N, \beta, P, \alpha \rangle$ is* ***uniform****, if the power of all stations is identical, i.e. $(\forall s_i \in S)(P(s_i) = p)$, where $p \in \mathbb{R}$ is some constant value. Otherwise, the network is* ***non-uniform****.*

[2]With $N = 0$, the range definition would be ill-defined because infinite reception zones can appear.

The important properties of uniform networks, like the convexity and the connectivity, were analyzed in [25]. Avin et al. proved the Theorem 2, the basis for the $1D$ uniform network results presented in this thesis.

Theorem 2. *The reception zones in a* SINR *diagram of a uniform power network with path-loss parameter* $\alpha = 2$ *and reception threshold* $\beta > 1$ *are convex.*

However, it is important that due to the details of analyzed scenarios and algorithms, the restrictions related to path loss and reception threshold parameters do not apply to results in this thesis unless mentioned otherwise.

It can be assumed that $P = 1$ for any uniform station, which simplifies the calculations. Visualization of uniform and non-uniform networks are presented in Figure 2.2. One more variant of a SINR function, utilizing a constant interference value, is defined as:

$$\mathrm{SI_cNR}_{\mathcal{A}}(s, x, I_c) = \frac{E_{\mathcal{A}}(s, x)}{N + I_c} \ .$$

The auxiliary Fact 1 comes from the transformation of the equation:

$$\mathrm{SI_cNR}_{\mathcal{A}}(s, w, I_c) = \beta \ .$$

and the monotonicity of the $\mathrm{SI_cNR}$ function for one *side* of analyzed station.

Fact 1. *For a network* $\mathcal{A}$*, with* $S = \{s\}$*, for* $s \in \mathbb{R}^D$ *and* $P(s) = p$*, where* $p \in \mathbb{R}^+$*; and constant value of interference* $I_c \in \mathbb{R}^+$*, the distance* $w = d(s, x)$*, for values of* x *such that* $\mathrm{SI_cNR}_{\mathcal{A}}(s, x, I_c) = \beta$*, can be calculated as:*

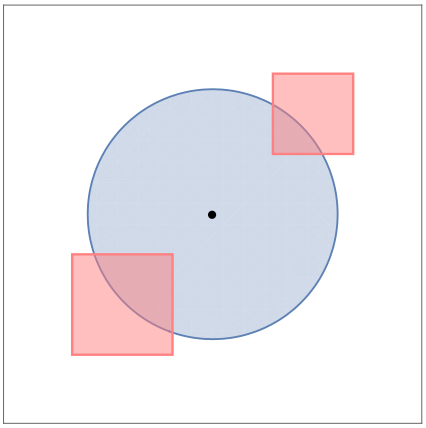
$$w = (\beta(N + I_c))^{-\frac{1}{\alpha}} p^{\frac{1}{\alpha}} \ .$$

If a network $\mathcal{A}$ is apparent from the context, it will be omitted from the notation symbols for the sake of readability (e.g., $\mathrm{SINR}_{\mathcal{A}}(s_i, x)$ will be replaced by $\mathrm{SINR}(s_i, x)$).

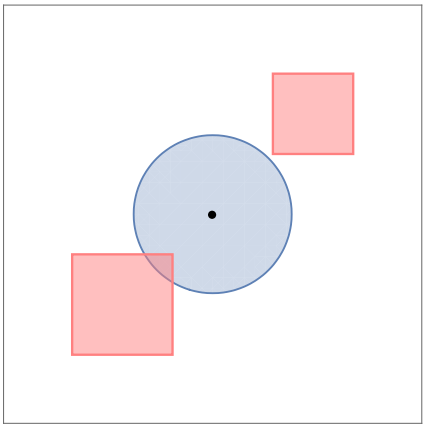
2.3 Protective jamming

For a network $\mathcal{A}$, there can be defined a **restricted area** $\mathcal{R}$, being the subset of a space, where no signal from any initial stations of $\mathcal{A}$ should be received. Assuming that this restricted area intersects the initial network's reception zone, the problem is how to modify the network to prevent the initial network's stations from being heard in these restricted areas while keeping the communication capabilities outside of them. Some techniques that can be used to achieve it might impact the reception zones outside of the restricted areas, limiting the network's capabilities, so part of the task is to limit this negative impact. The problem is depicted in Figure 2.3 with a two-dimensional network configuration, a single station, and a restricted area consisting of two rectangular fragments of space.

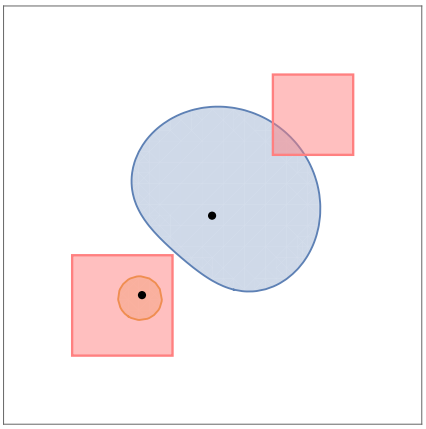
In Figure 2.3a, the reception zone intersects both restricted areas, exposing communication to a possible adversary. One action that can be taken is to reduce the power of a station, limiting its possible reception range - this is presented in Figure 2.3b. The problem with this approach is the impact, as mentioned earlier, on the communication range of a station outside of the restricted area. In the presented example, it might be possible to reduce the signal enough to remove the intersection with one of the restricted area patches. However, reducing it further would break critical communication, so the second restricted area patch still partially intersects with the reception zone. Another approach, presented in Figure 2.3c, is to take advantage of a station interference and add a special **jamming station**. Such a station does not have any requirements for its reception zone shape or size but only produces interference for a fine-grained limitation of the reception zones of the other stations. The problematic fragment of the restricted area was correctly protected using this approach - though the second patch problem remains. Finally, both techniques can be combined, as in Figure 2.3d, by positioning the jamming station and reducing the power of an initial station - achieving the goal of removing any intersections between the



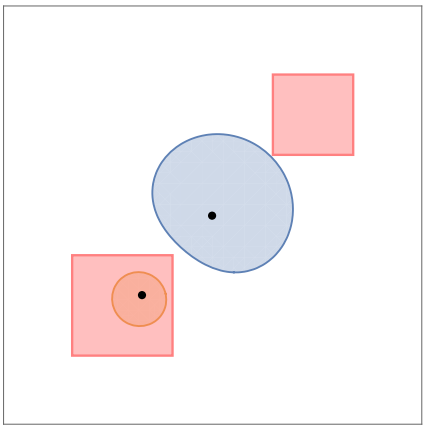
(a) Initial configuration - the reception zone of a station intersects the restricted areas.



(b) Reduced station power - the reception zone still intersects one of the restricted areas.



(c) Added a jamming station - it fixes the problem for one restricted area, but the reception zone still intersects the other one.



(d) The combined solution - reduced power of an initial station and added a jamming station - the reception area no longer intersects any restricted areas.

Figure 2.3: Example of the problem for a single broadcasting station (a blue color visualizes its reception zone) and multiple restricted areas (visualized by a red color).

restricted area and the reception zone of a station. In Figure 2.4, different scenarios are presented for configurations with multiple stations requiring protection.

While the original station power modification is feasible, this thesis focuses on using jamming stations to control the shapes and ranges of reception zones.

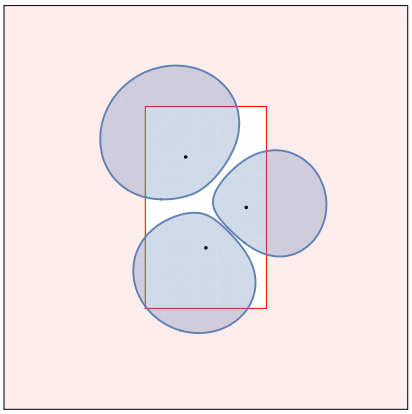
Definition 2.1. *For a set of jamming stations $S^{(J)}$ and the their power assignment functions $P^{(J)}$, the **jamming network** is defined as:*

$$\mathcal{J} = \left(S^{(J)}, P^{(J)}\right) .$$

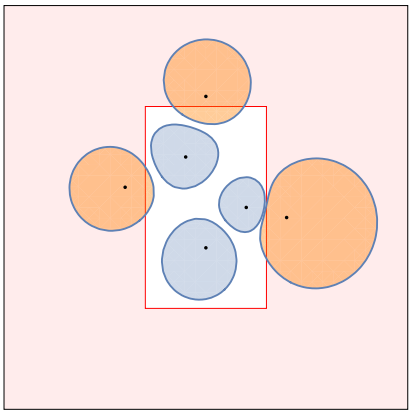
Jamming network can be combined with a network $\mathcal{A}$, creating the network $\mathcal{A}^{\mathcal{J}} = \langle D, S \cup S^{(J)}, N, \beta, P \cup P^{(J)}, \alpha \rangle$. The reception zones of stations from S should not intersect with the restricted area for the network $\mathcal{A}^{\mathcal{J}}$, as described in Definition 2.2.

Definition 2.2. *Jamming network $\mathcal{J} = \left(S^{(J)}, P^{(J)}\right)$ **correctly protects** the restricted area $\mathcal{R} \in \mathbb{R}^D$ for a network $\mathcal{A} = \langle D, S, N, \beta, P, \alpha \rangle$ if for a connected network $\mathcal{A}^{\mathcal{J}} = \langle D, S \cup S^{(J)}, N, \beta, P \cup P^{(J)}, \alpha \rangle$:*

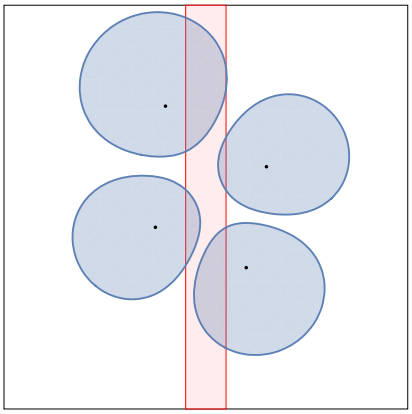
$$(\forall s \in S)(\forall x \in \mathcal{R})\ \mathrm{SINR}_{\mathcal{A}^{\mathcal{J}}}(s, x) < \beta .$$



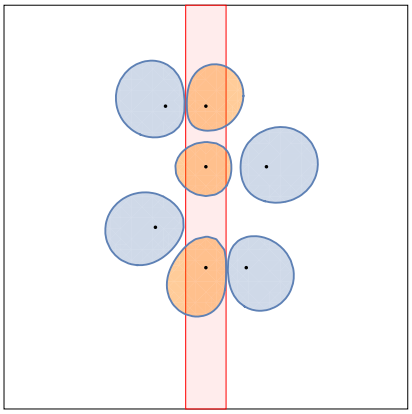
(a) Restricted area enclosing multiple stations.



(b) Jamming stations were added in a restricted area.



(c) Vertical restricted area (street) with stations surrounding it.



(d) Jamming stations were added to protect the street.

Figure 2.4: Different examples of the protective jamming problem.

While this definition is enough to provide the correctness of the results for jamming networks, more is needed to guarantee the quality of these results, namely, how significant its impact is on a network outside of the restricted area. One could, for example, decide to position numerous jamming stations with high power levels and just let their substantial interference break all communication in close vicinity, solving the described problem in a way that would not be accepted in a real-world scenario. Assuming a configuration similar to the one presented in Figure 2.4a, it can be imagined that the rectangle enclosed by the restricted area might be some military base or a research facility, where the wireless communication is critical for its operability. Thus, while the reception zone has to be limited to this rectangular area, the power and position of jamming stations must be carefully configured to not introduce too much interference and break internal communication.

The measure of the *coverage* is defined in Definition 2.3 to evaluate if the proposed algorithms are not producing too much interference. It is the fraction of a space covered by the reception zone *after jamming* within the maximal such space, but without any jamming.

Definition 2.3. *The* ***coverage*** *for some jamming network $\mathcal{J}$ and a network $\mathcal{A}$ is defined as:*

$$\mathrm{Cover}(\mathcal{J},\mathcal{A}) = \frac{\left|\bigcup_{s_i \in S}\left(H_i^{\mathcal{A}^{\mathcal{J}}} \cap (H_i^{\mathcal{A}} \setminus \mathcal{R})\right)\right|}{\left|\bigcup_{s_i \in S} H_i^{\mathcal{A}} \setminus \mathcal{R}\right|}.$$

In this definition, the restricted area is removed from the analyzed space, as this is where the original stations should not be operational. Note that the coverage is always correctly defined for positive values of a noise $N > 0$ and is bounded by:

$$0 \leq \text{Cover}(\mathcal{J}, \mathcal{A}) \leq 1 \ .$$

If the coverage value equals 1, the jamming does not impact the reception zones outside the restricted area. Finally, both Definition 2.2 and Definition 2.3 can be combined and formulate the problem analyzed in this thesis:

> ***For a network $\mathcal{A}$ and a restricted area $\mathcal{R}$, find the jamming network $\mathcal{J}$, such that, it correctly protects $\mathcal{R}$ and maximizes the value of*** $\text{Cover}(\mathcal{J}, \mathcal{A})$***.***

Coverage approximation The calculation of an exact value of coverage is a complex problem for the general case, so for the sake of presenting its value for the analyzed algorithms and scenarios, a simplified sampling approach is used. The space is split into a grid of uniform fragments (intervals in 1D, squares in 2D), densely spanning over the whole range of a station, for which the coverage will be calculated. Then, the center of each of such fragments is checked to see if this fragment should be able to receive a station's signal and if it receives it. The ratio between the number of fragments receiving the signal and fragments that should receive it is calculated as the approximation of the coverage. While the small enough size of these fragments is used to limit the precision loss, there might be some margin of error.

Because all stations consume energy, the secondary optimization goal is defined - the energy cost of the jamming network. The target is to minimize this value for the networks produced by different algorithms presented in this thesis.

Definition 2.4. *The energy cost of a jamming network $\mathcal{J} = \left(S^{(J)}, P^{(J)}\right)$ is defined as:*

$$\text{Cost}(\mathcal{J}) = \sum_{s \in S^{(J)}} P^{(J)}(s) \ .$$

2.4 Basic SINR literature and related work

The SINR is a well-established model in wireless networks research, including older and newer technologies, such as mobile networks, where it is usually used as the measurement of connection quality [34, 35], notably it is also used in relatively new 5G mobile networks [19].

SINR is also widely used in theoretical models of wireless communication. Its geometrical properties were studied by Avin et al. [25], who analyzed the properties of reception zones under a uniform SINR model, showing, among others, their convexity (the result heavily utilized in this thesis).

Non-uniform network properties were analyzed in [36], along with a new point location algorithm, and in [33], where non-uniform SINR network model, combined with Voronoi Diagrams, proved to retain some of the valuable properties of the uniform setting.

There is also a large amount of work considering the fundamental problems under the SINR model, such as *broadcasting* [37], *link scheduling* [38] or applying additional features to improve performance, such as *power control* [39].

Quickly evolving and growing wireless communication technology is prone to many security threats (ex. [40, 20]) and more than ever requires effective and efficient solutions to protect users' privacy. Most such protective measures are based on cryptographic solutions [41, 42]. The approach taken in this paper, using jamming stations as a part of the security mechanism, has been considered in [43, 44, 45] in the context of other models (i.e., non-SINR). Some of these approaches were proved to be practically feasible [46].

Regarding the SINR model, in [47], the authors considered settings similar to the one presented in this thesis but focusing on a specific 2D scenario, where the space is divided into a *storage*, in which the legitimate communication is supposed to take place, a *jamming*

space, where jammers can be placed, delimited by a *fence*, and the rest of the space, where the adversary can eavesdrop. In such settings, the optimization problems of jammers' positioning and power assignment were presented with approximation algorithms working for continuous space. This work has been further extended in [48], where SIR model is used as a connection quality measurement, and the solution is based on performing *temporal jamming*. The channel quality is modeled by the *bit-error probability*.

While the SINR is frequently utilized for wireless radio networks, like beam selection [49] or analysis of the network performance [50], it is worth mentioning that the general idea behind it can be utilized in less apparent scenarios, e.g., in VLC (*Visible Light Communication*) networks [51].

Chapter 3

Jamming in 1D SINR

This chapter considers the sub-class of one-dimensional networks ($D = 1$). This scenario, though seemingly over-simplified, can be used for modeling the networks on the streets, e.g., for VANET ([7]), where the width of the street can be negligible for jamming and the possible adversary is expected to be a part of the street traffic.

One of the advantages of the 1D networks is the relatively simple representation of reception zones, which can be, in practice, reduced to sets of intervals positioned on the line. It also highlights the first significant difference between uniform and non-uniform networks, where for the former, the reception zone of a station will always consist of a single interval due to the connectivity property of such networks [33]. The example is presented in Figure 3.1a. For the non-uniform network, the reception zone can get *split* into several components, like in Figure 3.1b, which makes their analysis much more involved.

(a) Example of a uniform network.

(b) Example of a non-uniform network.

Figure 3.1: Examples of 1D networks. The blue space is the reception zone of s_a, and the orange space is the reception zone of s_b.

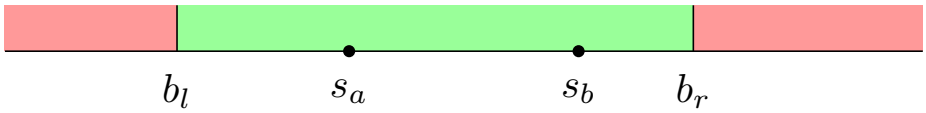
The analyzed problem can also be simplified in this model. As mentioned earlier, the generic notation of the restricted area $\mathcal{R}$ can be reduced to sets of intervals. For example, as presented in Figure 3.2a, the restricted area in the uniform model is a union of intervals $(-\infty, b_l)$ and (b_r, ∞), when for non-uniform example in Figure 3.2b, it consists of $\left(b_l^0, b_l^1\right)$ and (b_r, ∞). It is also worth noting that under the uniform stations' configuration, the segment $\left(b_l^0, b_l^1\right)$ in Figure 3.2b could be replaced by $\left(-\infty, b_l^1\right)$, due to convexity of reception zones.

In this chapter, unless mentioned otherwise, the following **initial network** is used:

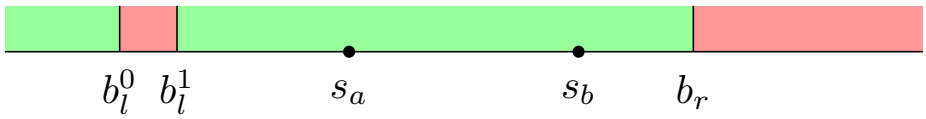
$$\mathcal{A} = \langle D = 1, S = \{s\}, N, \beta, P \equiv 1, \alpha \rangle \ .$$

Its single station is positioned at $s = 0$. The following restricted areas are defined for the network $\mathcal{A}$:

- $\mathcal{R}_b = (b, \infty)$, where $s < b < \text{range}_{\mathcal{A}}(s)$,



(a) Example of a jamming problem in a uniform network.



(b) Example of a jamming problem in a non-uniform network.

Figure 3.2: Examples of a 1D jamming problem instances (restricted areas are red).

- $\mathcal{R}_{b_l,b_r} = (-\infty, -b_l) \cup (b_r, \infty)$, where $b_l, b_r < \text{range}_{\mathcal{A}}(s)$,
- $\mathcal{R}_{\overline{b_l,b_r}} = (b_l, b_r)$, where $s < b_l < b_r < \text{range}_{\mathcal{A}}(s)$.

3.1 One side jamming in a uniform model

The uniform network model limits the power level of all stations to a single value. It can simplify analysis for some of the problems. Indeed, these networks have some important properties for chosen configurations, like connectivity or convexity of reception zones (see Theorem 2). On the other hand, such a model is still close to real-world scenarios. The single, fixed power level of all stations might be enforced by limited hardware capabilities or related constraints, which allow stations only to be positioned somewhere in space but not to change their power levels.

(a) The original reception zone.

(b) The reception zone with a one jamming station s_J.

Figure 3.3: Examples of a one-side jamming problem in 1D uniform model.

As mentioned before, all stations use the same power level $P = 1$ in uniform configurations. That also includes the added jamming stations - so the power is entirely excluded from calculations in this configuration. Without loss of generality, it can be assumed that a single analyzed station is positioned at $s = 0$ and the first analyzed variant of a restricted area is $\mathcal{R}_b$ (see Figure 3.3a). This problem can be solved by placing the jamming station at position $s_J = b + r$ for some $r > 0$, as presented in Figure 3.3b, forming the jamming network:

$$\mathcal{J} = \left(S^{(J)} = \{s_J\}, P^{(J)} \equiv 1\right) .$$

Nevertheless, the r must be carefully calculated to not unnecessarily decrease the coverage. An initial network, combined with a jamming network, has a form:

$$\mathcal{A}_{\mathcal{J}} = \langle D = 1, S = \{s, s_J\}, N, \beta, P \equiv 1, \alpha \rangle .$$

Unless mentioned otherwise, this section uses this network for all SINR related functions.

Theorem 3. *The jamming network $\mathcal{J}$ correctly protects $\mathcal{R}_b$ for the initial network $\mathcal{A}$, if:*

$$s_J = b + \sqrt[\alpha]{\frac{\beta}{b^{-\alpha} - \beta N}} \ .$$

Proof. The energy of a station s, generated at a point b, in this combined network is equal to:

$$E(s,b) = P \cdot d(s,b)^{-\alpha} = b^{-\alpha} \ .$$

To ensure that $\mathrm{SINR}(s,b) = \beta$, the interference generated by a jamming station has to be equal to:

$$I(s,b) = \frac{E(s,b)}{\beta} - N = \frac{b^{-\alpha}}{\beta} - N \ . \tag{3.1}$$

Assuming, that a single jamming station $s_J > b$ is used, the interference can be reduced to:

$$I(s,b) = P \cdot d(s_J,b)^{\alpha} = (s_J - b)^{-\alpha} \ . \tag{3.2}$$

From combining Equation 3.1 and Equation 3.2:

$$s_J = b + \sqrt[\alpha]{\frac{\beta}{b^{-\alpha} - \beta N}} \ .$$

The SINR energy function for the station s is monotonously decreasing for points $x > s$, particularly for $x > b$. Similarly, for the station s_J, its energy is monotonously increasing in the interval $(-\infty, s_J)$ and decreasing for (s_J, ∞). Based on that, $\mathrm{SINR}(s,x) < \beta$ for points $x \in (b, s_J)$, as they get closer to s_J and the interference at that interval will be higher than at the point b. For points $x > s_J$, because of the stations' uniformity, the $E(s,x) < E(s_J,x)$, thus the protection will be upheld for them.

□

Lemma 1. *The coverage of jamming network $\mathcal{J}$ protecting $\mathcal{R}_b$ for a network $\mathcal{A}$ is bounded:*

$$\mathrm{Cover}(\mathcal{J},\mathcal{A}) \in \left[\frac{b + (\beta(N + \mathrm{MaxI}))^{-\frac{1}{\alpha}}}{\mathrm{range}_{\mathcal{A}}(s) + b}, \frac{b + (\beta(N + \mathrm{MinI}))^{-\frac{1}{\alpha}}}{\mathrm{range}_{\mathcal{A}}(s) + b} \right] \ ,$$

where $\mathrm{MinI} := (s_J + \mathrm{range}_{\mathcal{A}}(s))^{-\alpha}$ *and* $\mathrm{MaxI} := (s_J + b)^{-\alpha}$.

Proof. The reception zone of a station s, after jamming, is equal to $H_s = [b_l, b]$, for a point $b_l < s$. Based on the connectivity of uniform networks, it holds that $\mathrm{SINR}(s, b_l) = \beta$ (see Figure 3.4). Calculating the exact position of b_l is challenging, so only an interval (x_l, x_r) bounding it is analyzed, and the coverage boundaries are derived from this interval.

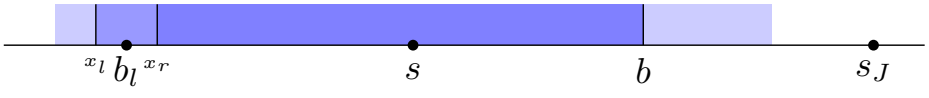


Figure 3.4: Boundaries of a reception zone.

Realize, that $b_l \in (-\mathrm{range}(s), -b)$. If the $b_l < -\mathrm{range}(s)$, it would be located outside of the initial reception zone of the station s. If $b_l = -\mathrm{range}(s)$, it would mean that no interference was added during jamming, which is not true. For the upper position bound, the $b_l < -b$ is based on the symmetrical properties of the SINR function. If $b_l > -b$, it would mean that the interference produced by s_J is greater for points $x < s$ than for $x \in (s,b)$, which is not possible due to monotonicity of SINR energy function for $x < s_J$ and s_J positioned according to Theorem 3. For the interval $(-\mathrm{range}(s), -b)$, the interference generated by s_J at its extreme points can be calculated:

- $\text{MinI} = I(s, -\text{range}(s)) = (s_J + \text{range}(s))^{-\alpha}$,
- $\text{MaxI} = I(s, -b) = (s_J + b)^{-\alpha}$.

The interference function is monotonic for $x \in (-\text{range}(s), -b)$, so the interference at this segment is also bounded by $[\text{MinI}, \text{MaxI}]$ and this fact is used to bound the possible position of b_l further. By using the $\text{SI}_\text{c}\text{NR}$ function, such points would have the distance from s matching the following equations (see Figure 3.4):

$$\text{SI}_\text{c}\text{NR}(s, x_l, \text{MinI}) = \beta \ , \qquad \text{SI}_\text{c}\text{NR}(s, x_r, \text{MaxI}) = \beta \ .$$

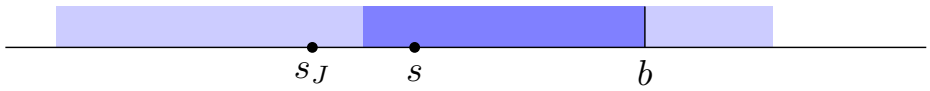
By applying Fact 1, the distance from these points to s can be calculated as:

$$d(s, x_l) = (\beta(N + \text{MinI}))^{-\frac{1}{\alpha}} \ , \qquad d(s, x_r) = (\beta(N + \text{MaxI}))^{-\frac{1}{\alpha}} \ .$$

By the construction, as both points $x_l, x_r < s$, it means that $x_l \leq b_l \leq x_r$, so the possible maximal reception zone can be $[x_l, b]$ and the minimal would be $[x_r, b]$. Combining it with the fact that the maximal initial reception zone of s before jamming, under the coverage definition, would be $[-\text{range}(s), b]$, it concludes the proof for the coverage boundaries. □

Note that the station s_J can be placed at three different positions. The one from the Theorem 3 is presented in Figure 3.3b and $s_J > b$ in this scenario. Two other possible positions are presented in Figure 3.5, with position $s < s_J < b$ in Figure 3.5a and $s_J < s$ in Figure 3.5b. While both locations are theoretically feasible to solve the problem, they are not optimal in terms of coverage as they generate the strongest interference outside the restricted area.

(a) The jamming station positioned between s and b.



(b) The jamming station positioned on the opposite side of s than b.

Figure 3.5: Alternative positions of the jamming station.

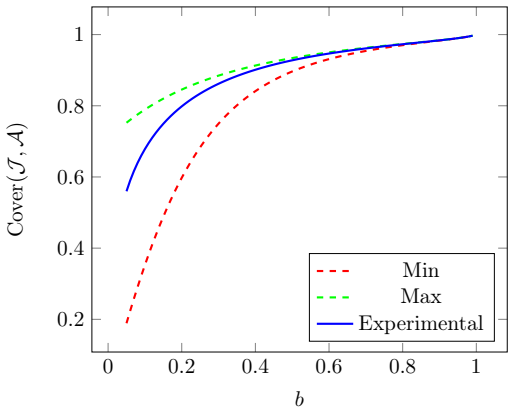
In this scenario, the direct consequence of the coverage bounding proof is an extension of a restricted area protected by a single jamming station.

Corollary 1. *The jamming network $\mathcal{J}$ defined in Theorem 3, for $x_l = (\beta(N + \text{MinI}))^{-\frac{1}{\alpha}}$, correctly protects the interval $(-\infty, x_l)$.*

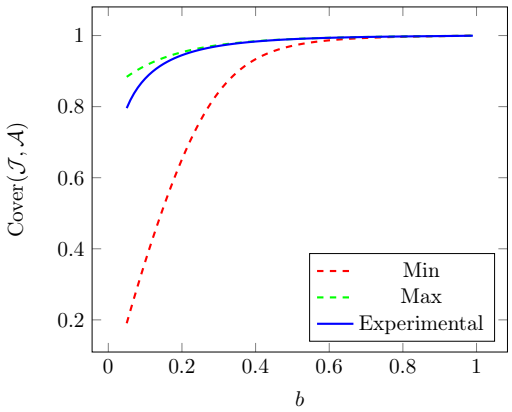
While the method has limited uses due to only one-side protection, it does not significantly impact the coverage. The experimental coverage measurements and its lower and upper bound visualization are presented in Figure 3.6. The bounds for the coverage are getting worse with the b point getting closer to the station s, but the overall coverage results tend to be greater than 0.8 for most configurations.

3.2 Two sides jamming in a uniform model

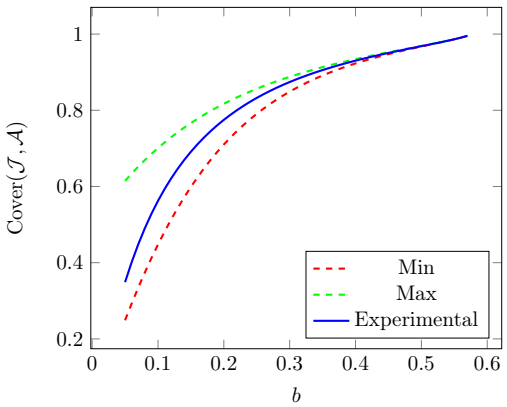
The natural augmentation of the method presented in Section 3.1 is to allow for jamming the station from two sides. While Corollary 1 presented how a one jamming station can achieve it, this approach is severely limited and has a big, unwanted influence on the coverage value.



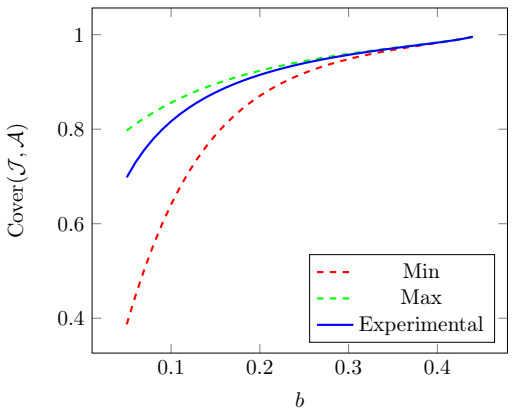
(a) Network using $N = 1, \beta = 1, \alpha = 2$.



(b) Network using $N = 1, \beta = 1, \alpha = 4$.



(c) Network using $N = 1, \beta = 3, \alpha = 2$.



(d) Network using $N = 5, \beta = 1, \alpha = 2$.

Figure 3.6: Measurement of a coverage for networks $\mathcal{A} = \langle D = 1, S, N, \beta, P \equiv 1, \alpha \rangle$ and the jamming network $\mathcal{J}$, created with the single station positioning scheme. *Experimental* is the coverage measurement based on sampling, the *Min*/*Max* are the bounds from Theorem 3.

With two border points present, one can also use the one-side method on each border point independently, but ignoring the other station's interference might also harm the coverage. In this section, the approach utilizing two jamming stations is presented. The initial network $\mathcal{A}$ remains the same as in the previous section, but the $\mathcal{R}_{b_l,b_r}$ restricted area is used. Two jamming stations are denoted as s_J^l, s_J^r, and:

$$s_J^l < b_l < s < b_r < s_J^r \ .$$

The jamming network is defined as:

$$\mathcal{J} = \left(S^{(J)} = \{s_J^l, s_J^r\}, P^{(J)} \equiv 1 \right) \ .$$

An initial network, combined with a jamming network, has a form:

$$\mathcal{A}_{\mathcal{J}} = \left\langle D = 1, S = \{s, s_J^l, s_J^r\}, N, \beta, P \equiv 1, \alpha \right\rangle \ .$$

This section uses this network for all SINR related functions unless mentioned otherwise.

Theorem 4. *The jamming network $\mathcal{J}$ correctly protects the initial network $\mathcal{A}$ for $\mathcal{R}_{b_l,b_r}$, if:*

$$s_J^l = -b_l - \beta^{\frac{1}{\alpha}} \left(b_l^{-\alpha} - \beta N - \beta \mathrm{MinI}_r \right)^{-\frac{1}{\alpha}} , \qquad s_J^r = b_r + \beta^{\frac{1}{\alpha}} \left(b_r^{-\alpha} - \beta N \right)^{-\frac{1}{\alpha}} \ ,$$

where:

$$\mathrm{MinI}_r := (s_J^r + b_l)^{-\alpha} \ .$$

Proof. The position of s_J^r comes directly from Theorem 3 by replacing b with b_r. Realize that:

$$\mathrm{MinI}_r = E(s_J^r, -b_l) \ .$$

This is the smallest interference value generated by s_J^r at any point inside of the range of station s. Because of that, it can be assumed that this interference is constant for the whole interval $(-b_l, s)$ during the calculation of the second station position. Its position can be acquired by solving the following equation for some $x = d(b_l, s_J^l)$ (slightly abusing notation):

$$\mathrm{SI_cNR}_{\mathcal{A}}(s, -b_l, \mathrm{MinI}_r + x^{-\alpha}) = \frac{E(s, -b_l)}{N + \mathrm{MinI}_r + x^{-\alpha}} = \beta \ .$$

As $E(s, -b_l) = b_l^{-\alpha}$, the equation can be transformed to:

$$x = \beta^{\frac{1}{\alpha}} \left(b_l^{-\alpha} - \beta N - \beta \mathrm{MinI}_r\right)^{-\frac{1}{\alpha}} \ .$$

Because the second station should be positioned on the opposite side of s than s_J^r, it results in $s_J^l = -b_l - x$. Protection correctness is ensured by the monotonicity of s_J^r and s_J^l energy functions for intervals (b_r, s_J^r) and $(s_J^l, -b_l)$ accordingly. Other points from $\mathcal{R}_{b_l,b_r}$ are protected because of the convexity of uniform network reception zones. □

Lemma 2. *The coverage of the jamming network $\mathcal{J}$ protecting $\mathcal{R}_{b_l,b_r}$ for a network $\mathcal{A}$ is bounded from below:*

$$\mathrm{Cover}(\mathcal{J}, \mathcal{A}) \geq \frac{\mathrm{MaxL} + \mathrm{MaxR}}{b_l + b_r} \ ,$$

where:

$$\mathrm{MaxL} = (\beta(N + \mathrm{MaxI}_l^L + \mathrm{MaxI}_r^L))^{-\frac{1}{\alpha}} \ , \qquad \mathrm{MaxR} = (\beta(N + \mathrm{MaxI}_l^R + \mathrm{MaxI}_r^R))^{-\frac{1}{\alpha}} \ ,$$

$$\mathrm{MaxI}_l^L = E(s_J^l, -b_l), \qquad \mathrm{MaxI}_l^R = E(s_J^l, s), \qquad \mathrm{MaxI}_r^L = E(s_J^r, s), \qquad \mathrm{MaxI}_r^R = E(s_J^r, b_r) \ .$$

Proof. The coverage lower bound is based on the interference approximation for both *sides* of the station s. Station s_J^l attains the maximal interference:

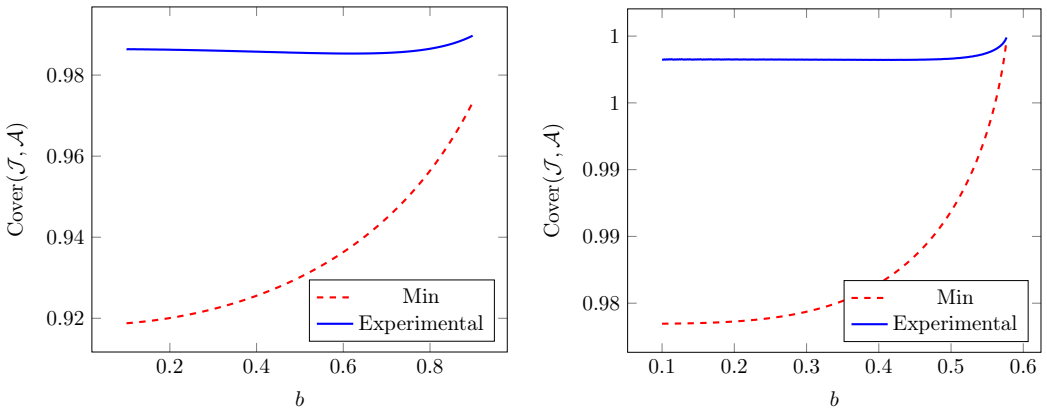
- for $x < s$, at point $-b_l$, denoted as MaxI_l^L,
- for $x > s$, at point s, denoted as MaxI_l^R .

Similarly, for station s_J^r, it attains the maximal interference:

- for $x < s$, at point s, denoted as MaxI_r^L,
- for $x > s$, at point b_r, denoted as MaxI_r^R .

Using these maximal interferences for both sides of the station, Fact 1 can be used to calculate the maximal distance where station s can be heard under such interference from both sides. These values are denoted as MaxL and MaxR for $x < s$ and $x > s$ accordingly. It means that the final reception zone is limited to $[-\mathrm{MaxL}, \mathrm{MaxR}]$. Moreover, this scenario's maximal possible reception zone is enclosed by $[-b_l, b_r]$, which finalizes the proof. □

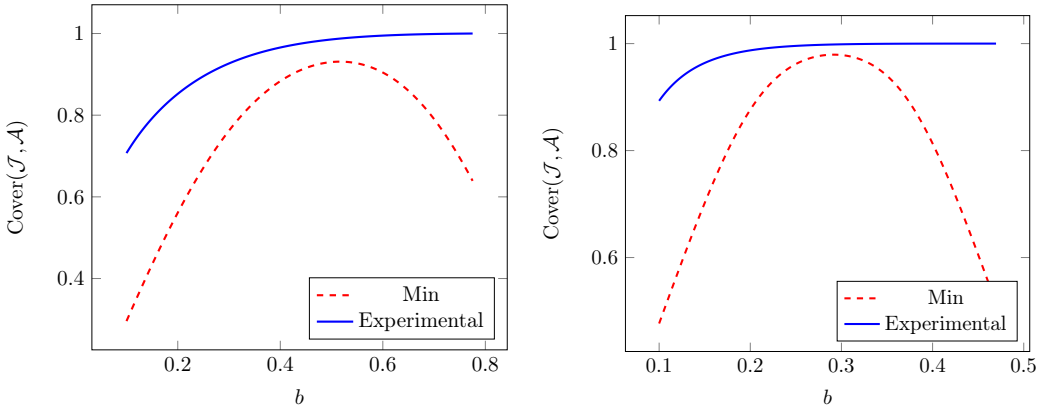
The experimental coverage measurements are presented in Figure 3.7 and Figure 3.8. The *Experimental* plot is the value of coverage acquired from the experimental sampling, and the *Min* plot represents the lower bound on coverage from Lemma 2. In Figure 3.7, the symmetrical change in b is checked, i.e. $b_l = b_r = b$. The results are, perhaps surprisingly, much better than presented in Section 3.1. It is because of uniform network properties, where station s is *sandwiched* between two jamming stations, and in this example, the distance between them and s is roughly similar. The asymmetrical configuration is presented in Figure 3.8. In this example, $b_l = b$ and $b_r = \mathrm{range}(s) - b$. These results are slightly worse, especially for b_l being closer to s than b_r. It shows that the order in which these points are calculated matters, i.e., assigning to b_r closer border point is better for the coverage. Overall, these results are quite close to the optimal coverage, but it is not guaranteed. In the next section, a more sophisticated method is fixing this issue.



(a) Network with parameters: $N = 1, \beta = 1, \alpha = 2$.

(b) Network with parameters: $N = 3, \beta = 3, \alpha = 4$.

Figure 3.7: Measurement of coverage for networks $\mathcal{A} = \langle D = 1, S, N, \beta, P \equiv 1, \alpha \rangle$ and jamming network $\mathcal{J}$, created according to Theorem 4. *Experimental* is the coverage measurement based on sampling, the *Min* is the lower bound from Theorem 3. Bounds are symmetrical, $b_l = b_r = b$.



(a) Network with parameters: $N = 1, \beta = 1, \alpha = 2$.

(b) Network with parameters: $N = 3, \beta = 3, \alpha = 4$.

Figure 3.8: Measurement of coverage for networks $\mathcal{A} = \langle D = 1, S, N, \beta, P \equiv 1, \alpha \rangle$ and jamming network $\mathcal{J}$, created according to Theorem 4. *Experimental* is the coverage measurement based on sampling, the *Min* is the lower bound from Theorem 3. Bounds are asymmetrical, $b_l = b$ and $b_r = \text{range}(s) - b$.

3.3 Precise stations positioning in a uniform model

In previous sections, the jamming station positioning schemes were burdened with an unwanted impact on the coverage due to little control over the generated interference. This nuisance can be rectified by the iterative method, which can control both the influence of interference and the size of a reception zone. In this section, such an approach, which should enlarge the coverage, is presented. The initial network has a form of:

$$\mathcal{A}_0 = \langle D = 1, S = \{s\}, N, \beta, P, \alpha \rangle \ .$$

Note that the value of P is not omitted from the calculations in this section. Moreover, the $\mathcal{R}_{b_l, b_r}$ restricted area type is analyzed (see Chapter 3 beginning). The primary goal is to find the positions of jamming stations $-x < -b_l$ and $y > b_r$ such that $H_s^{\mathcal{A}_0^{\mathcal{J}}} \subset [-b_l, b_r]$.

Definition 4.1. *If a pair of positions of jamming stations $s_l = -x^*$ and $s_r = y^*$ is the*

setup of the network $\mathcal{A}$ (with $S = \{s, s_l, s_r\}$) that guarantees $H_s^{\mathcal{A}} = [-b_l, b_r]$, then this setup of the network $\mathcal{A}$ is called ***optimal*** *and be denoted as $\mathcal{A}^*$.*

The $\mathcal{J}^* = \{-x^*, y^*\}$ is called the optimal arrangement (minimizing the coverage). The optimal positions of the jamming stations are denoted with an asterisk sign in the following subsections. Note that the optimal arrangement does not have to be unique.

Definition 4.2. *The network $\mathcal{A}$ is δ-**precise** if there exists an optimal arrangement $\mathcal{A}^*$ such that $|x - x^*| < \delta$ and $|y - y^*| < \delta$.*

The goal is to maximize the coverage of the demanded reception zone. Hence, the **secondary goal** is to arrange $\mathcal{A}$ in a finite number of steps so that it is δ-precise for a δ parameter given a priori. In practice, the δ parameter should be chosen smaller than the observational error of the distance measurement, so the admission of this kind of fault would be acceptable.

3.3.1 Description of the algorithm

Apart from parameters that describe the SINR model and the restricted area $\mathcal{R}_{b_l,b_r}$, the algorithm takes a precision parameter δ as an input. The following notation is used:

- $C_i = \frac{1}{\beta} - \frac{N}{P} b_i^{\alpha}$, for $i \in \{l, r\}$,
- for $b > 0$, let $f(a, b; x) = 1 + a\left(1 + (b - x^{-\alpha})^{-\frac{1}{\alpha}}\right)$ with a natural domain $x \in \left(b^{-\frac{1}{\alpha}}, \infty\right)$,
- $g(y) = f\left(\frac{b_r}{b_l}, C_r; f\left(\frac{b_l}{b_r}, C_l; y\right)\right)$ with a domain inherited from $\mathrm{dom}(f)$,
- $h(x) = f\left(\frac{b_l}{b_r}, C_l; f\left(\frac{b_r}{b_l}, C_r; x\right)\right)$ with a domain inherited from $\mathrm{dom}(f)$.

It can be easily concluded that the reception zone is convex (see [25]) and the $H_s^{\mathcal{A}^{\mathcal{J}}}$ is some interval included in $(-x, y)$. If the optimal positions x^*, y^* exist, then the optimal solution satisfies $-x^* < -b_l$ and $y^* > b_r$. The following four intervals are defined:

- $X = (b_l, \infty)$,
- $Y = (b_r, \infty)$,
- $\bar{X} = \left(1 + \frac{b_l}{b_r}, \infty\right)$,
- $\widehat{Y} = \left(1 + \frac{b_r}{b_l}, \infty\right)$.

Note that natural ranges of functions $f\left(\frac{b_l}{b_r}, C_l; y\right)$ and $f\left(\frac{b_r}{b_l}, C_r; x\right)$ are in $\bar{X}$ and $\widehat{Y}$ respectively. Moreover, if the optimal arrangement exists, then $x^* \in X$ and $y^* \in Y$. To transfer calculations from X and Y to their dual equivalents: $\bar{X}$ and $\widehat{Y}$, the auxiliary linear functionals are introduced that provide easy control over those transfers:

- an overbar, $\bar{\cdot} : X \to \bar{X}$, defined as $\bar{x} = 1 + \frac{x}{b_r}$,
- an underbar, $\underline{\cdot} : \bar{X} \to X$, defined as $\underline{x} = b_r(x - 1)$,
- an overhat, $\widehat{\cdot} : Y \to \widehat{Y}$, defined as $\widehat{y} = 1 + \frac{y}{b_l}$,
- an underhat, $\underset{\frown}{\cdot} : \widehat{Y} \to Y$, defined as $\underset{\frown}{y} = b_l(y - 1)$.

The notation of dual intervals is compatible with the symbols of the functionals. From now on, the elements from the intervals will be paired with the notation of appropriate functionals. For instance, points from $\bar{X}$ are denoted with overbar, like e.g. $\bar{z} \in \bar{X}$. However, this notation simultaneously entails that there exists $z \in X$ defined as $\underline{\bar{z}}$, which naturally fulfills $\bar{z} \in \bar{X}$ (since $\underline{\cdot}$ and $\widehat{\cdot}$ are inversions of $\bar{\cdot}$ and $\widehat{\cdot}$ respectively, so $\underline{\bar{x}} = x$ for $x \in X$ and $\widehat{y} = y$ for $y \in Y$). At first glance, the double notation seems redundant. However, out of the blue, it simplifies a brief description of reverse transformations without confusion. The choice of the definitions of the above functionals will significantly simplify the notation in the proof of Theorem 5.

The iterative algorithm that returns positions $-x, y$ of jamming stations that guarantee correct protection of the restricted area and are δ-close to optimal arrangement $-x^*, y^*$ (see the Theorem 5 for precise formulation) is presented in Algorithm 1.

Algorithm 1: AssingJammingStations(δ)

Algorithm `AssignJammingStations(`δ`)`
- $\bar{x}_0 = 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right)$
- $\bar{x} =$`AlignPosition(`$\bar{x}_0, \delta$`)`
- $D_f = \dfrac{\left|f'\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right| b_l}{b_r}$
- **if** $D_f \geqslant 1$ **then**
  - $\delta = \frac{\delta}{D_f}$
  - $\bar{x} =$`AlignPosition(`$\bar{x}, \delta$`)`
- $y = \left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right) - 1\right) b_l$ `// defined as` $\widehat{y}(\bar{x})$
- $x = (\bar{x} - 1) b_r$ `// defined as` $\underline{\bar{x}}$
- **return** $(-x, y)$

Procedure `AlignPosition(`$\bar{x}, \delta$`)`
- $\zeta = h'(\bar{x})$
- $k = \left\lceil \ln\left(\frac{\frac{\delta}{b_r}(1-\zeta)}{h(\bar{x}) - \bar{x}}\right) \Big/ \ln(\zeta) \right\rceil$
- **for** $i \in \{1, \ldots, k\}$ **do**
  - $\bar{x} = h(\bar{x})$
- **return** $\bar{x}$

The method for extracting the $\widehat{y}$ (corresponding to the position of the right jamming station) is presented in Section 3.3.2 and is based on the present value of $\bar{x}$ (which corresponds to the position of the left jamming station). With this information in mind, both positions of the stations can be controlled by focusing solely on $\bar{x}$. Therefore, the lion's share of the Algorithm 1 execution rectifies only $\bar{x}$. The Algorithm 1 initializes the positions of two jamming stations in such a way that they correctly protect $\mathcal{R}_{b_l,b_r}$, but allows the interference inside $[-b_l, b_r]$ to be higher than needed, resulting in smaller reception zone. A crucial idea of this algorithm is to adapt iteratively $\bar{x}$ to improve the efficiency of the broadcasting station at each step (without a loss of the protection of $\mathcal{R}_{b_l,b_r}$). As the number of iterations increases, the adaptations of x and y should tend to some optimal arrangement.

Now, to explain the run of the procedure in more detail - the Algorithm 1 consists of the initialization and two adaptation phases. During the initialization, a dual equivalent of the position of the left jamming station is established (note that $\bar{x}_0 \in \bar{X}$):

$$\bar{x}_0 = 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right) .$$

The first adapting phase iteratively sets the next dual equivalents of the left jamming station by applying the function h, i.e., $\bar{x}_{n+1} = h(\bar{x}_n)$. This phase ends when the requirement is met:

$$|x_n - x^*| = |\underline{\bar{x}}_n - \underline{\bar{x}}^*| \leqslant \delta .$$

Since the procedure stores values from $\bar{X}$, it is easier to consider the equivalent condition $|\bar{x}_n - \bar{x}^*| < \frac{\delta}{b_r}$ instead. One can check the requirement at each iteration step. Nevertheless, the appropriate number k of iterations is alternatively established in advance, and these steps are performed. As it was mentioned before, $f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)$ may be utilized to find the respective $\widehat{y}$ equivalent of the right jamming station. However, the appropriate setup of one jamming station does not imply the same for another one. Hence, if the condition $|\widehat{y} - \widehat{y}^*| < \frac{\delta}{b_l}$ is not fulfilled after the first adaptation phase, the analogous adaptation phase is needed for the second jamming station as well. Nevertheless, in order to reduce the number of calculations during the execution of Algorithm 1, the δ-precision of the second jamming station, transformed to $\bar{X}$, is verified - with the help of $\widehat{y} = f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)$ formula. The rest of the adaptation method remains the same. The detailed description of this mechanism is presented in proofs of Lemmas 10 and 11. Finally, the algorithm returns the positions of the jamming stations $-\underset{\sim}{x}$ and $\underset{\sim}{y}$.

3.3.2 Algorithm's analysis

Theorem 5. *Consider a uniform* SINR *network $\mathcal{A}_0$ with a single station $s = 0$ and parameters $N > 0, \alpha \geqslant 1$ and a restricted area $\mathcal{R}_{b_l,b_r}$ such that:*

1. $0 < b_l \leqslant b_r \leqslant \text{range}(s)$,
2. $C_r^{-\frac{1}{\alpha}} < \bar{x}_0 = 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right)$ *and* $C_l^{-\frac{1}{\alpha}} < 1 + \frac{b_r}{b_l}\left(1 + C_r^{-\frac{1}{\alpha}}\right)$.

Then:

1. *there exists a unique optimal arrangement $\mathcal{J}^* = \{-x^*, y^*\}$ for $\mathcal{A}_0$,*
2. `AssignJammingStations(`δ`)` *returns $\mathcal{J} = \{-x, y\}$ for $\mathcal{A}_0$, such that:*
   - *$\mathcal{J}$ correctly protects $\mathcal{R}_{b_l,b_r}$,*
   - *$|x - x^*| \leqslant \delta$ and $|y - y^*| \leqslant \delta$ (i.e. $\mathcal{J}$ is δ-precise).*

Note that if $b_l = b_r$, then the formulation of Theorem 5 simplifies a lot, as well, as its proof (there is no need to define functions g and h). First, the method how to derive the functions $h(\bar{x})$ and $g(\widehat{y})$ mentioned in Section 3.3.1 is presented in Lemma 3.

Lemma 3. *If the optimal arrangement $\mathcal{J}^*$ for $\mathcal{A}_0$ exists, then $\bar{x}^*$ and $\widehat{y}^*$ are fixed points of h and g respectively and*

$$\begin{aligned} \bar{x}^*(\widehat{y}^*) &:= 1 + \frac{b_l}{b_r}\left(1 + \left(C_l - (\widehat{y}^*)^{-\alpha}\right)^{-\frac{1}{\alpha}}\right) = f\left(\frac{b_l}{b_r}, C_l; \widehat{y}^*\right) \ , \\ \widehat{y}^*(\bar{x}^*) &:= 1 + \frac{b_r}{b_l}\left(1 + \left(C_r - (\bar{x}^*)^{-\alpha}\right)^{-\frac{1}{\alpha}}\right) = f\left(\frac{b_r}{b_l}, C_r; \bar{x}^*\right) \ . \end{aligned} \tag{3.3}$$

Proof. First, the method of deriving the function $f(a, b; \bar{x})$ is presented. It utilizes simple transformations of equations $\text{SINR}(s, b) = \beta$ for $b \in \{-b_l, b_r\}$ (note that these conditions guarantee the optimality of the solution). Starting with the case of $-b_l$:

$$\text{SINR}(s, -b_l) = \frac{b_l^{-\alpha}}{\frac{N}{P} + (x^* - b_l)^{-\alpha} + (y^* + b_l)^{-\alpha}} = \beta \ . \tag{3.4}$$

The considered SINR network is uniform, so $H_s^{\mathcal{A}}$ is convex (see [25]), so once $\text{SINR}(s, b) = \beta$ for both border points $b \in \{-b_l, b_r\}$, then $H_s^{\mathcal{A}^{\mathcal{J}^*}} = [-b_l, b_r]$. By rearrangement of Equation 3.4:

$$\frac{1}{\beta} - \frac{N}{P} b_l^{\alpha} = \frac{1}{(\frac{x^*}{b_l} - 1)^{\alpha}} + \frac{1}{(\frac{y^*}{b_l} + 1)^{\alpha}}. \tag{3.5}$$

Realize that the left-hand side of the above formula is constant (defined in Section 3.3.1):

$$C_l = \frac{1}{\beta} - \frac{N}{P} b_l^{\alpha} \ .$$

Let:

$$x_l^* = \frac{x^*}{b_l} \ , \qquad y_l^* = \frac{y^*}{b_l} \ .$$

The Equation 3.5 can be rewritten in two following forms:

$$C_l (x_l^* - 1)^{\alpha} (y_l^* + 1)^{\alpha} = (x_l^* - 1)^{\alpha} + (y_l^* + 1)^{\alpha},$$
$$x_l^* = 1 + \frac{y_l^* + 1}{(C_l (y_l^* + 1)^{\alpha} - 1)^{\frac{1}{\alpha}}} = 1 + (C_l - (y_l^* + 1)^{-\alpha})^{-\frac{1}{\alpha}}.$$

Analogically, the SINR equation for the latter border point b_r can be investigated:

$$y_r^* = 1 + \frac{x_r^* + 1}{(C_r (x_r^* + 1)^{\alpha} - 1)^{\frac{1}{\alpha}}} = 1 + \left(C_r - (x_r^* + 1)^{-\alpha}\right)^{-\frac{1}{\alpha}} \ .$$

To justify the usage of the overbar and the overhat functionals (defined in Section 3.3.1), realize that:

$$x_r^* + 1 = 1 + \frac{x^*}{b_r} = \bar{x}^* \ , \qquad y_l^* + 1 = 1 + \frac{y^*}{b_l} = \widehat{y}^* \ .$$

Instantly, these remarks can be utilized in order to provide the relations between $\bar{x}^*$ and $\widehat{y}^*$ in terms of the function f, given by equations (3.3). Realize that the combination of two equations (3.3) give either $h(\bar{x}^*) = \bar{x}^*$ or $g(\widehat{y}^*) = \widehat{y}^*$, what entails a fact that $\bar{x}^*$ and $\widehat{y}^*$ are fixed points of h and g respectively. □

Note that Lemma 3 shows that to obtain a δ-precise arrangement of the problem, it should be assumed that h and g have some fixed points. This observation causes the existence of some natural limits of such the setup (in fact — the constraint (2) from Theorem 5).

As mentioned before, both equations (3.3) allow calculating the position of the one jamming station when the position of the second one is given in such a way that the SINR value is equal to β in at least one of the border points. Nevertheless, rectifying the interference at one of the border points also alters the interference for the second one. The second SINR value may even be very far from β.

Next lemma shows that equations (3.3) are well defined:

Lemma 4. *If there exists an optimal arrangement $\mathcal{J}^*$ for a network $\mathcal{A}_0$, then*

$$C_l - (\widehat{y}^*)^{-\alpha} > 0 \qquad \textit{and} \qquad C_r - (\bar{x}^*)^{-\alpha} > 0 \ . \tag{3.6}$$

Proof. When the $(x^* - b_l)^{-\alpha}$ part is omitted in Equation 3.4, then it gives the inequality similar to Equation 3.5:

$$C_l = \frac{1}{\beta} - \frac{N}{P} b_l^{\alpha} > \frac{1}{(\frac{y^*}{b_l} + 1)^{\alpha}} = (\widehat{y}^*)^{-\alpha} \ .$$

An analogous calculation for $\mathrm{SINR}(s, b_r)$ gives the correct result for C_r, which ends the proof. □

Notice that the above conditions (3.6) means that $\bar{x}^*$ is in the natural domain of $\widehat{y}(\bar{x}) = f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)$ and $\widehat{y}^*$ is in the natural domain of $\bar{x}(\widehat{y}) = f\left(\frac{b_l}{b_r}, C_l; \widehat{y}\right)$. Then, the condition 2 from Theorem 5 can be fulfilled for some pair of points, which guarantees the existence of the solution. The following two lemmas are presented here for the convenience of a reader since they give an insight into the nature of transformations f, g, and h.

Lemma 5. *For $a, b > 0$, $f(a, b; z)$ is a descending and convex function in its whole domain.*

Proof. From the definition of f, its known that $z > b^{-\frac{1}{\alpha}}$. The derivatives of f can be easily calculated:

$$\frac{\partial f(a,b;z)}{\partial z} = -a(b - z^{-\alpha})^{-\frac{1}{\alpha}-1} \cdot z^{-\alpha-1} = -a(bz^{\alpha} - 1)^{-\frac{1}{\alpha}-1} , \tag{3.7}$$

so $f(a,b;z)$ is descending and:

$$\frac{\partial^2 f(a,b;z)}{\partial z^2} = a\,(1+\alpha)\,(bz^{\alpha} - 1)^{-\frac{1}{\alpha}-2} z^{\alpha-1} . \tag{3.8}$$

Therefore, $f(a,b;z)$ is convex. □

Lemma 6. *Functions $h(\bar{x})$ and $g(\widehat{y})$ are ascending and concave functions in their whole domains.*

Proof. The proof is presented only for $h(\bar{x})$. The proof for $g(\widehat{y})$ is analogous. From Lemma 5 comes:

$$\begin{aligned} h'(\bar{x}) &= \frac{\partial f}{\partial \bar{x}}\left(\frac{b_l}{b_r}, C_l; f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right) \cdot \frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}\right) \\ &\overset{(3.7)}{=} -\frac{b_l}{b_r}\left(C_l\left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right)^{\alpha} - 1\right)^{-\frac{1}{\alpha}-1} \cdot \left(-\frac{b_r}{b_l}\right)(C_r\bar{x}^{\alpha} - 1)^{-\frac{1}{\alpha}-1} \\ &= \left(\left(C_l\left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right)^{\alpha} - 1\right)(C_r\bar{x}^{\alpha} - 1)\right)^{-\frac{1}{\alpha}-1} , \end{aligned} \tag{3.9}$$

so $h(\bar{x})$ is ascending. Denote a natural, real domain of h by D_h. Realize that $h'(\bar{x}) > 0$ for $\bar{x} \in D_h$. The maximum of $h'(\bar{x})$ is to be found – or equivalently – a minimum of $H(\bar{x}) = \left(C_l\left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right)^{\alpha} - 1\right)(C_r\bar{x}^{\alpha} - 1)$, which is a way easier to investigate. By Lemma 4 and equations (3.3), the formulas in both parentheses are non-negative. Two auxiliary functions can be defined:

$$\mathcal{F}(\bar{x}) := \ln\left(C_l\left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right)^{\alpha}\right)$$

and:

$$\mathcal{X}(\bar{x}) := \ln\left(C_r\bar{x}^{\alpha}\right) .$$

Note that both are positive from Lemma 4. Thence the elegant equation can be provided:

$$H(\bar{x}) = (e^{\mathcal{F}(\bar{x})} - 1)(e^{\mathcal{X}(\bar{x})} - 1) .$$

And consequently:

$$\begin{aligned} H'(\bar{x}) &= \mathcal{F}'(\bar{x})e^{\mathcal{F}(\bar{x})}(e^{\mathcal{X}(\bar{x})} - 1) + \mathcal{X}'(\bar{x})e^{\mathcal{X}(\bar{x})}(e^{\mathcal{F}(\bar{x})} - 1) \\ &= e^{\mathcal{X}(\bar{x})+\mathcal{F}(\bar{x})}\left(\mathcal{X}'(\bar{x}) + \mathcal{F}'(\bar{x}) - \frac{\mathcal{X}'(\bar{x})}{e^{\mathcal{F}(\bar{x})}} - \frac{\mathcal{F}'(\bar{x})}{e^{\mathcal{X}(\bar{x})}}\right) . \end{aligned}$$

Realize that:

$$\mathcal{X}'(\bar{x}) = \frac{\alpha}{\bar{x}} , \qquad \mathcal{F}'(\bar{x}) = \frac{\alpha\frac{\partial}{\partial\bar{x}}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)}{f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)} .$$

So from equations (3.3) and conditions (3.6) for $\bar{x}$ and $\widehat{y}(\bar{x})$ (since $\bar{x}$ is in the domain of h):

$$\begin{aligned} \frac{H'(\bar{x})}{\alpha e^{\mathcal{X}(\bar{x})+\mathcal{F}(\bar{x})}} &= \frac{1}{\bar{x}} + \frac{\frac{\partial}{\partial\bar{x}}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)}{f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)} - \frac{1}{\bar{x}C_l\left(f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right)^{\alpha}} - \frac{\frac{\partial}{\partial\bar{x}}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)}{C_r\bar{x}^{\alpha}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)} \\ &> \frac{1}{\bar{x}} + \frac{\frac{\partial}{\partial\bar{x}}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)}{f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)} - \frac{1}{\bar{x}} - \frac{\frac{\partial}{\partial\bar{x}}f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)}{f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)} = 0 . \end{aligned}$$

Hence $H'(\bar{x}) > 0$ – or equivalently – $h''(\bar{x}) < 0$, so h is concave in its whole domain. Moreover, by Equation 3.9, it is also an increasing function. □

The following lemmas justify the correctness of the procedure `AlignPosition(`δ`)`.

Lemma 7. *If* $b_l \leqslant b_r$ *and* $C_l^{-\frac{1}{\alpha}} < 1 + \frac{b_r}{b_l}\left(1 + C_r^{-\frac{1}{\alpha}}\right)$, *then* $h'(\bar{x}) < 1$ *for* $\bar{x} > C_r^{-\frac{1}{\alpha}}$.

Proof. Note that $C_l^{-\frac{1}{\alpha}} < 1 + \frac{b_r}{b_l}\left(1 + C_r^{-\frac{1}{\alpha}}\right)$ guarantees that $\bar{x} > C_r^{-\frac{1}{\alpha}}$. In the proof of Lemma 6 it was defined:

$$\begin{aligned}
H(\bar{x}) &= (C_r\bar{x}^\alpha - 1)\left(C_l\left(1 + \frac{b_r}{b_l}\left(1 + \left(C_r - \bar{x}^{-\alpha}\right)^{-\frac{1}{\alpha}}\right)\right)^\alpha - 1\right) \\
&= (C_r\bar{x}^\alpha - 1)\left(c_1 + C_l\left(\frac{b_r}{b_l}\right)^\alpha\left(1 + \left(C_r - \bar{x}^{-\alpha}\right)^{-\frac{1}{\alpha}}\right)^\alpha\right) \\
&= (C_r\bar{x}^\alpha - 1)\left(c_2 + C_l\left(\frac{b_r}{b_l}\right)^\alpha\left(C_r - \bar{x}^{-\alpha}\right)^{-1}\right) \\
&= (C_r\bar{x}^\alpha - 1)\left(c_2 + C_l\left(\frac{b_r}{b_l}\right)^\alpha\bar{x}^\alpha\left(C_r\bar{x}^\alpha - 1\right)^{-1}\right) \\
&= C_l\left(\frac{b_r}{b_l}\right)^\alpha\bar{x}^\alpha + c_2\left(C_r\bar{x}^\alpha - 1\right) \ ,
\end{aligned}$$

where $c_1 = O(1)$ and $c_2 = O(1)$ as $\bar{x} \to \left(C_r^{-\frac{1}{\alpha}}\right)^+$. Therefore:

$$\lim_{\bar{x}\to\left(C_r^{-\frac{1}{\alpha}}\right)^+} H(\bar{x}) = \frac{C_l b_r^\alpha}{C_r b_l^\alpha},$$

which is at least 1 whenever $\frac{C_l}{b_l^\alpha} \geqslant \frac{C_r}{b_r^\alpha}$. Realize that from the definition:

$$\frac{C_i}{b_i^\alpha} = \frac{1}{\beta b_i^\alpha} - \frac{N}{P}$$

for $i \in \{l, r\}$, so $\frac{C_l b_r^\alpha}{C_r b_l^\alpha} \geqslant 1$ is equivalent to $b_l \leqslant b_r$. From the proof of Lemma 6 it is known that $H'(\bar{x}) > 0$, so $H(\bar{x}) > 1$ for $\bar{x} > C_r^{-\frac{1}{\alpha}}$. Thence for $\bar{x} > C_r^{-\frac{1}{\alpha}}$:

$$h'(\bar{x}) = H(\bar{x})^{-\frac{\alpha}{\alpha+1}} < 1 \ .$$

□

Remark that if $b_r < b_l$, then $h'(\bar{x}) \geqslant 1$ for $\bar{x}$ from some neighborhood of $C_r^{-\frac{1}{\alpha}}$. However $b_r < b_l$ does not forbid $h'(\bar{x})$ to be smaller than 1 for some $\bar{x}$. Notice that sometimes the assumption $C_l^{-\frac{1}{\alpha}} < 1 + \frac{b_r}{b_l}\left(1 + C_r^{-\frac{1}{\alpha}}\right)$ in the formulation of Theorem 5 may be weakened. In principle, it is only required to guarantee that the fixed point $\bar{x}^*$ of h exists by:

$$C_l^{-\frac{1}{\alpha}} < 1 + \frac{b_r}{b_l}\left(1 + \left(C_r - (\bar{x}^*)^{-\alpha}\right)^{-\frac{1}{\alpha}}\right) \ .$$

However, in such a case, it may not be clear how to choose the initial configuration for the algorithm, and it is needed to guarantee that $\bar{x}^*$ exists.

The Banach fixed point theorem [52], presented in Theorem 6, is necessary for the following lemmas and proofs.

Theorem 6 (Banach fixed point theorem)**.** *Let* $(\mathcal{X}, d)$ *be a non-empty complete metric space with mapping* $T : \mathcal{X} \to \mathcal{X}$ *with a contraction constant*

$$\Lambda := \sup\{\lambda \in \mathbb{R} : (\forall\, x, y \in \mathcal{X})\ d(T(x), T(y)) \leqslant \lambda d(x, y)\} \ .$$

Then T admits a unique fixed-point $x^* \in \mathcal{X}$. Furthermore, $x^* = \lim_{n\to\infty} x_n$ where x_0 is an arbitrary element of $\mathcal{X}$ and $x_n = T(x_{n-1})$ for $n \geqslant 1$. Then also:

$$d(x^*, x_n) \leqslant \frac{\Lambda^n}{1-\Lambda} d(x_1, x_0) \ .$$

Lemma 8. *For $n \in \mathbb{N}$, let:*

- $\bar{x}_0 = 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right)$,
- $\bar{x}_n = h(\bar{x}_{n-1})$.

Assume that:

- $b_l \leqslant b_r$,
- $C_r^{-\frac{1}{\alpha}} < 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right)$,
- $\bar{x}_0 \leqslant h(\bar{x}_0)$.

Then:

- *$(\bar{x}_n)_{n\in\mathbb{N}}$ is ascending and $(h'(\bar{x}_n))_{n\in\mathbb{N}}$ is descending,*
- *there exists a fixed point of h function given as the limit $\bar{x}^* = \lim_{n\to\infty} \bar{x}_n$,*
- *there exists an optimal arrangement $\mathcal{J}^*$ for a network $\mathcal{A}_0$ and $\mathcal{R}_{b_l,b_r}$ with jamming stations placed in $s_l = \underline{\bar{x}^*}$ and $s_r = \widehat{\bar{y}^*(\bar{x}^*)}$.*

Proof. By assumptions:

$$\bar{x}_0 > \max\left\{C_r^{-\frac{1}{\alpha}}, 1 + \frac{b_l}{b_r}(= \bar{b_l})\right\} \ .$$

By Equation 3.9, $h'(\bar{x}) > 0$, so $\bar{x}_k \leqslant h(\bar{x}_k)$ for any $k \in \mathbb{N}_0$. Moreover, the same argument, together with Lemma 7 and assumptions give:

$$\lim_{\bar{x}\to\left(C_r^{-\frac{1}{\alpha}}\right)^+} h(\bar{x}) = 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right) = \bar{x}_0 \ .$$

From Lemma 5, $f\left(\frac{b_l}{b_r}, C_l; \widehat{y}\right)$ and $f\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)$ are decreasing, so:

$$h(\bar{x}_0) = f\left(\frac{b_l}{b_r}, C_l; f\left(\frac{b_r}{b_l}, C_r; \bar{x}_0\right)\right) > \lim_{\widehat{y}\to\infty} f\left(\frac{b_l}{b_r}, C_l; \widehat{y}\right) = \bar{x}_0 \ .$$

Note that if $\bar{x} < h(\bar{x})$, then also $h(\bar{x}) < h(h(\bar{x}))$, because h is ascending from Lemma 6. From Lemma 7 and Lemma 6 once again it gets $0 < h'(\bar{x}) < 1$ and $h''(\bar{x}) < 0$, so:

$$h'(\bar{x}_1) = h'(h(\bar{x})) < h'(\bar{x}_0) < 1 \ .$$

Similarly, for any $n \in \mathbb{N}$:

$$h'(\bar{x}_n) < h'(\bar{x}_{n-1}) < 1 \ .$$

From Banach Theorem 6 comes that $h(\bar{x})$ is a contraction in $(\bar{x}_0, \infty)$, so $\lim_{n\to\infty} \bar{x}_n = \bar{x}^*$ is a fixed point of $h(\bar{x})$ and $\widehat{y}^* = f\left(\frac{b_r}{b_l}, C_r; \bar{x}^*\right)$ is then the fixed point of $g(\widehat{y})$. □

Remark that if the assumption:

$$C_r^{-\frac{1}{\alpha}} < 1 + \frac{b_l}{b_r}\left(1 + C_l^{-\frac{1}{\alpha}}\right)$$

is not met, then $h(\bar{x}) < \bar{x}$ for any $\bar{x} > C_r^{-\frac{1}{\alpha}}$, and hence there is no fixed point of h (compare with condition 2. from Theorem 5). With the assumptions from Lemma 8 in mind, it may give a sense to $-\underline{\bar{x}}_0$ as the initial position of the left jamming station. Then $-\underline{\bar{x}}_n$ may be interpreted as the n-th position of the left jamming station. According to equations (3.3), define:

$$\widehat{y}_n(\bar{x}_n) = f\left(\frac{b_r}{b_l}, C_r; \bar{x}_n\right) .$$

Then $\widehat{\underset{\sim}{y}}_n$ may be treated as the appropriate position of the right jamming station. Notice that $\widehat{\underset{\sim}{y}}_n = g(\widehat{\underset{\sim}{y}}_{n-1})$. Each application of h and g functions recursively *improves* the interference in border points.

Lemma 9. *Let $n \in \mathbb{N}$ and $N > 0$. With the assumptions from Lemma 8, the network $\mathcal{A}_0^{\mathcal{J}}$ with $\mathcal{J} = \left\{\underline{\bar{x}}_n, \widehat{\underset{\sim}{y}}_n\right\}$ satisfies $H_s^{\mathcal{A}_0^{\mathcal{J}}} \subset [-b_l, b_r]$. Moreover $\bar{x}_n \leqslant h(\bar{x}_n) \leqslant \bar{x}^*$.*

Proof. Let $\mathrm{SINR}(s, v; a, b)$ denotes the value of SINR in point v for the broadcasting station s, with $\mathcal{J} = \{a, b\}$. First of all, realize that from equations (3.3), if $\bar{x} > \max\left\{1 + \frac{b_l}{b_r}, C_r^{-\frac{1}{\alpha}}\right\}$, then:

$$\mathrm{SINR}\left(0, b_r; -\underline{\bar{x}}, \widehat{\underset{\sim}{y}}(\bar{x})\right) = \beta .$$

Clearly, $\bar{x}_0$ fulfills this condition. Similarly, from Lemma 8 there exists a fixed point $\bar{x}^*$ and if $\bar{x} \leqslant \bar{x}^*$, then:

$$\beta = \mathrm{SINR}\left(0, -b_l; -\underline{h(\bar{x})}, \widehat{\underset{\sim}{y}}(\bar{x})\right) \geqslant \mathrm{SINR}\left(0, -b_l; -\underline{\bar{x}}, \widehat{\underset{\sim}{y}}(\bar{x})\right),$$

since $\bar{x}^* \geqslant h(\bar{x}) \geqslant \bar{x}$. Similar reasoning gives:

$$\mathrm{SINR}\left(0, b_r; -\underline{h(\bar{x})}, \widehat{\underset{\sim}{y}}(\bar{x})\right) \geqslant \beta .$$

The convexity of the reception zone together with Lemma 8 gives the thesis. □

According to Lemma 9, it is required to find such the point $\bar{x}' < \bar{x}^*$ that $\underline{\bar{x}}'$ and $\widehat{\underset{\sim}{y}}'(\bar{x}')$ satisfy δ-precision property, or equivalently:

$$|\bar{x}^* - \bar{x}'| < \frac{\delta}{b_r} =: \xi_1 \qquad \text{and} \qquad \left|\widehat{\underset{\sim}{y}}'(\bar{x}') - \widehat{\underset{\sim}{y}}^*(\bar{x}^*)\right| < \frac{\delta}{b_l} . \tag{3.10}$$

Lemma 10. *If $\bar{x}^* - \bar{x} < \xi_1$, $\bar{x}' \in [\bar{x}, \bar{x}^*]$ and:*

$$|\bar{x}^* - \bar{x}'| \leqslant \frac{\delta}{b_l \left|\frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right|} =: \xi_2 , \tag{3.11}$$

then the conditions (3.10) are fulfilled.

Proof. From Lemma 5:

$$\left|\frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right| > \left|\frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}'\right)\right| .$$

Moreover:

$$|\widehat{\underset{\sim}{y}}(\bar{x}) - \widehat{\underset{\sim}{y}}^*(\bar{x}^*)| \leqslant \left|\frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}\right)\right| \cdot |\bar{x}^* - \bar{x}| . \tag{3.12}$$

If the right hand side of inequality (3.12) is smaller than $\frac{\delta}{b_l}$, then inequality (3.11) entails the second condition of (3.10) and the first one follows from $\bar{x} < \bar{x}'$. □

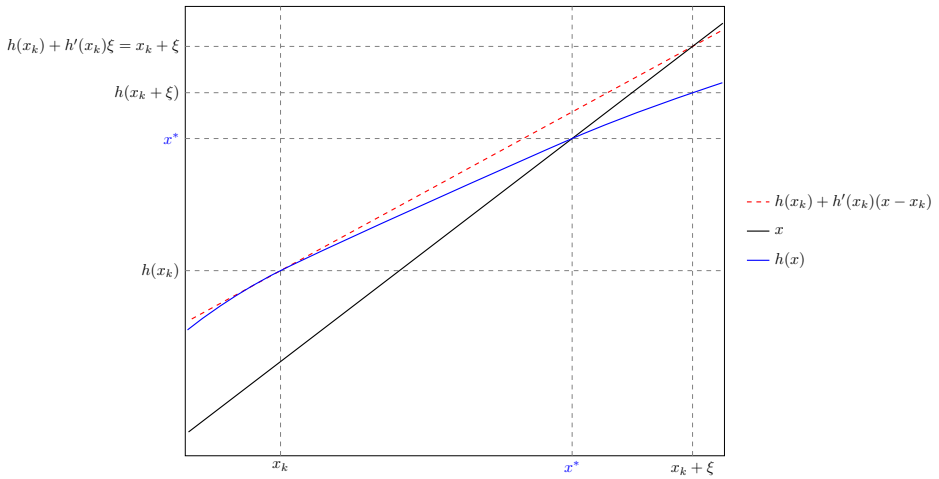


Figure 3.9: Graphical representation of the inequality $h(\bar{x}_k)+h'(\bar{x}_k)\cdot\xi = \bar{x}_k+\xi > h(\bar{x}_k+\xi)$.

Remark that if the first part of (3.10) is satisfied and $\left|\frac{\partial f}{\partial \bar{x}}\left(\frac{b_r}{b_l}, C_r; \bar{x}'\right)\right| < \frac{b_r}{b_l}$, then the second inequality from (3.10) follows from inequality (3.12). Note that, according to Lemma 10, the first adapting phase of Algorithm 1 should find such $\bar{x}$ that the first part of (3.10) is true for $\bar{x}$ and in the second phase it should find such the $\bar{x}' \in [\bar{x}, \bar{x}^*]$ that inequality (3.11) is fulfilled as well. It is possible to utilize the result of Banach Theorem 6 to verify the distance of the superpositions of h from the fixed point and the speed of convergence of the procedure. Hence, numbers $k(i) \in \mathbb{N}$, for $i \in \{1, 2\}$ are searched, such that the appropriate recursive superpositions of the function h applied to $\bar{x}_0$ guarantee that:

$$\left|\underset{\sim}{\bar{x}}_{k(1)} - \underset{\sim}{\bar{x}}^*\right| \leqslant \delta \qquad \text{and} \qquad \left|\underset{\sim}{\widehat{y}}_{k(1)+k(2)} - \underset{\sim}{\widehat{y}}^*\right| \leqslant \delta \ . \tag{3.13}$$

The next lemma shows how to set both parameters $k(i)$.

Lemma 11. *Let $\zeta(n) = h'(\bar{x}_n)$ and:*

$$k(i) \geqslant \left\lceil \ln\left(\frac{\xi_i(1-\zeta(n))}{|h(\bar{x}_n) - \bar{x}_n|}\right) \Big/ \ln(\zeta(n)) \right\rceil \tag{3.14}$$

for $i \in \{1, 2\}$. Then, the conditions (3.13) are fulfilled.

Proof. From Lemma 7 and Lemma 8 comes $h'(\bar{x}_k) < 1$, so from Lemma 6, there exists:

$$\xi > (\bar{x}^* - \bar{x}_k) \ ,$$

such that (see Figure 3.9):

$$h(\bar{x}_k) + h'(\bar{x}_k) \cdot \xi = \bar{x}_k + \xi > h(\bar{x}_k + \xi) \ .$$

Hence:

$$\xi = \frac{h(\bar{x}_k) - \bar{x}_k}{1 - h'(\bar{x}_k)} \ .$$

According to Lemma 10, in order to satisfy conditions (3.13), the $\xi < \xi_1$ and $\xi < \xi_2$ (defined in 3.10 and 3.11) respectively in the first and the second phase. Let $\zeta(n) := h'(\bar{x}_n)$. Then from Banach Theorem 6:

$$|\bar{x}^* - \bar{x}_{n+k}| \leqslant \zeta(n)^k \, |\bar{x}^* - \bar{x}_n| \leqslant \zeta(n)^k \frac{|h(\bar{x}_n) - \bar{x}_n|}{1 - \zeta(n)} < \xi \ .$$

Note that $((\bar{x}_0, \infty), |.|)$ is a complete metric space. The above can be transformed into condition (3.14) for both $i \in \{1, 2\}$. □

Proof of Theorem 5 Note that Lemma 8 shows that the optimal arrangement $\mathcal{J}^*$ for the network $\mathcal{A}_0$ exists. Lemma 9 shows that Algorithm 1 instantly achieves the correct protection of $\mathcal{R}_{b_l,b_r}$. Recall that Lemma 7 and Lemma 8 give $\zeta(n) < 1$ for any $n \in \mathbb{N}$. Note that these two lemmas utilize all the assumptions of Theorem 5 (the necessity of these assumptions is given by lemmas 3, 4 and 7). However, it is worth noting that one of them can be potentially weakened (for details, see a short discussion after the proof of Lemma 7). Therefore, according to Lemmas 10 and 11, it is only required to apply an appropriate $k(1)$ superpositions of h with $n = 0$ in the 1-st adapting phase of Algorithm 1 and $k(2)$ with $n = k(1)$ in the second one. Remark that D_f from Algorithm 1 is, in fact a ratio $\frac{\xi_1}{\xi_2}$, so it properly changes during the execution. Hence, Algorithm 1 also satisfies δ-precision property, what finishes the proof of Theorem 5. □

Remark that Algorithm 1 terminates in finite time and establishes two points of arrangement of jamming stations, so they do not need to be iteratively adjusted physically. In fact, Algorithm 1 is fast, what is presented in the next section.

3.3.3 Experimental results

The algorithm's two properties verified experimentally are the coverage and the number of its iterations. Due to the character of the algorithm, rather than present them on a plot for different configurations, minimal coverage and a maximal number of iterations are presented for selected scenarios. The *maximal iterations number* in results is the number of loop iterations in `AlignPosition(`δ`)` function. The experimental results were collected for the following networks:

- **N1** : $\alpha = 2, N = 1, \beta = 1$,
- **N2** : $\alpha = 4, N = 1, \beta = 1$,
- **N3** : $\alpha = 2, N = 1, \beta = 3$,
- **N4** : $\alpha = 2, N = 5, \beta = 1$,
- **N5** : $\alpha = 4, N = 3, \beta = 3$.

Symmetrical border points scenario: In this scenario, symmetrical border points of the form $b_l = b_r = b$ are used. The simulation assumed $b \in [0.1, 0.9]$, trimmed to the actual maximal range of stations s in a chosen network configuration and the algorithm restrictions.

Minimal coverage value

δ	**N1**	**N2**	**N3**	**N4**	**N5**
10^{-1}	0.985307	0.999152	0.97005	0.985297	0.998212
10^{-2}	0.986307	0.999152	0.99892	0.985946	0.998212
10^{-3}	0.999878	0.999213	0.999436	0.999819	0.998228
10^{-5}	1	1	1	1	1
10^{-10}	1	1	1	1	1

Figure 3.10: Experimental minimal coverage values for symmetrical border points scenario.

The coverage value in all scenarios is very high and usually close to the optimal one. For a higher precision parameter δ, the sampling precision does not allow for capturing any fragments where the reception zone is reduced, thence the 1s in the table.

Maximal iterations number

δ	**N1**	**N2**	**N3**	**N4**	**N5**
10^{-1}	1	0	108	829	1
10^{-2}	2	0	153	1103	2
10^{-3}	2	1	199	1376	2
10^{-5}	4	1	290	1924	4
10^{-10}	7	2	517	3292	8

Figure 3.11: Experimental maximal iteration numbers for symmetrical border points scenario.

For configurations **N0**, **N1** and **N5**, the run time of algorithm is negligible. It gets worse in **N3** and is the worst in **N4**, which suggests that it might be sensitive to the changing value of the noise and the reception threshold. It also tends to grow with parameter δ, which is expected. It is noteworthy that most of these long-running configurations used extreme b values - usually close to the range value. The iteration number was nominal for most of the other b values.

Asymmetrical border points scenario: In this scenario, asymmetrical border points of form: $b_l = b$ and $b_r = \text{range}(s) - b$, for $b_l \leqslant b_r$ are used. The simulation assumed $b \in [0.1, 0.9]$, trimmed to the actual maximal range of stations s in a chosen network configuration and the algorithm restrictions.

Minimal coverage value

δ	**N1**	**N2**	**N3**	**N4**	**N5**
10^{-1}	0.9855	0.99922	0.972201	0.985622	0.998303
10^{-2}	0.99582	0.99922	0.999342	0.991503	0.998303
10^{-3}	0.99995	0.99953	0.999602	0.999955	0.999307
10^{-5}	1	1	1	1	1
10^{-10}	1	1	1	1	1

Figure 3.12: Experimental minimal coverage values for asymmetrical border points scenario.

There are no significant changes in coverage values in this scenario. Similarly to the symmetrical one, these values are close to the optimal and show missing sampling precision for higher δ parameters.

Maximal iterations number

δ	**N1**	**N2**	**N3**	**N4**	**N5**
10^{-1}	0	0	1	0	0
10^{-2}	1	0	1	1	0
10^{-3}	1	1	2	1	1
10^{-5}	2	1	3	2	1
10^{-10}	4	2	7	4	2

Figure 3.13: Experimental maximal iteration numbers for asymmetrical border points scenario.

Compared to the symmetrical scenario, there are no high numbers of iterations, and the algorithm cost seems negligible. There is still the tendency to increase the number of iterations with the δ parameter, but even with high precision, this value seems relatively small.

3.4 Jamming in non-uniform networks

Non-uniform networks present more challenges than uniform ones, but there are also more opportunities to optimize the jamming network, especially regarding energy usage. The main issue is the lack of reception zone connectivity, so some of the methods presented in previous sections might give incorrect results when used directly in this model. For example, suppose a jamming station s_J is positioned close to the protected station s, but its power level is too low. In that case, it might result in correct protection for some segment $(s_J - x, s_J + y)$, but then the signal of s might be received at point $s_J + y + \epsilon$ (see Figure 3.1b). This section presents a method of jamming with a single station in a non-uniform model, with the correct positioning of the station and an alignment of its power. It can be treated as a non-uniform counterpart of Section 3.1. The restricted area $\mathcal{R}_b$ is used and the jamming network is denoted for jamming station power $P_J < P$ as:

$$\mathcal{J} = \left(S^{(J)} = \{s_J\}, P^{(J)} \equiv P_J\right) .$$

An initial network $\mathcal{A}$, combined with a jamming network, has a form:

$$\mathcal{A}_{\mathcal{J}} = \langle D = 1, S = \{s, s_J\}, N, \beta, P, \alpha\rangle ,$$

where $P(s) = P$ and $P(s_J) = P_J$. Unless mentioned otherwise, this section uses this network for all SINR related functions.

Theorem 7. *The jamming network $\mathcal{J}$ correctly protects the initial network $\mathcal{A}$ with $N > 0$ for $\mathcal{R}_b$ and:*

$$z(x) = \sqrt[\alpha]{\frac{\beta}{x^{-\alpha} - \beta N}} ,$$

if:

$$s_J = \left(\frac{\beta^{-\frac{1}{\alpha}} z(b) + b}{1 + \left(\frac{z(b)}{\beta^{\frac{1}{\alpha}} \operatorname{range}_{\mathcal{A}}(s)}\right)}\right) , \qquad P_J = \left(\frac{\operatorname{range}_{\mathcal{A}}(s) - s_J}{\operatorname{range}_{\mathcal{A}}(s)}\right)^{\alpha} \beta^{-1} .$$

Proof. For a jamming station, to correctly protect the interval (b, ∞), the following requirement must be fulfilled:

$$\mathrm{SINR}(s, b) = \frac{b^{-\alpha}}{N + P_J(s_J - b)^{-\alpha}} = \beta .$$

After transforming this equation, it gets:

$$s_J = b + \sqrt[\alpha]{\frac{P_J \beta}{b^{-\alpha} - \beta N}} = b + P_J^{\frac{1}{\alpha}} z(b) . \tag{3.15}$$

This position of s_J ensures the correct protection of the interval (b, s_J) due to the monotonicity of s and s_J energy functions. To ensure the same thing for $x \in (s_J, \operatorname{range}(s)]$, the following inequality must hold:

$$\mathrm{SINR}(s, x) \leqslant \beta .$$

Note that due to the requirement of $N > 0$:

$$\mathrm{SINR}(s, x) < \mathrm{SIR}(s, x) .$$

So, the problem can be solved by finding the following:

$$\mathrm{SIR}(s, x) = \frac{x^{-\alpha}}{P_J(x - s_J)^{-\alpha}} \leqslant \beta .$$

After simple transformations, it results in:

$$P_J \geqslant \left(\frac{x - s_J}{x}\right)^{\alpha} \beta^{-1} \ . \tag{3.16}$$

Realize that:

$$\lim_{x \to \infty} \left(\frac{x - s_J}{x}\right) = 1 \ .$$

But for the interval $(s_J, \text{range}(s)]$, it attains maximum at the maximal range of s:

$$\max_{x \in (s_J, \text{range}_{\mathcal{A}}(s)]} \left(\frac{x - s_J}{x}\right) = \frac{\text{range}_{\mathcal{A}}(s) - s_J}{\text{range}_{\mathcal{A}}(s)} \ .$$

This means, that Equation 3.16 is fulfilled for this value, i.e.:

$$P_J = \left(\frac{\text{range}(s) - s_J}{\text{range}(s)}\right)^{\alpha} \beta^{-1} \ . \tag{3.17}$$

Equation 3.15 and Equation 3.17 can be combined and solved for s_J and P_J. These solutions are the same as in the theorem. □

Lemma 12. *The coverage of jamming network $\mathcal{J}$ protecting $\mathcal{R}_{b_l,b_r}$ for a network $\mathcal{A}$ is bounded from below:*

$$\text{Cover}(\mathcal{J}, \mathcal{A}) \geqslant \frac{(\beta(N + \text{MaxI}^L))^{-\frac{1}{\alpha}} + (\beta(N + \text{MaxI}^R))^{-\frac{1}{\alpha}}}{\text{range}_{\mathcal{A}}(s) + b} \ ,$$

for:

$$\text{MaxI}^L = E(s_J, s) \ , \qquad \text{MaxI}^R = E(s_J, b) \ .$$

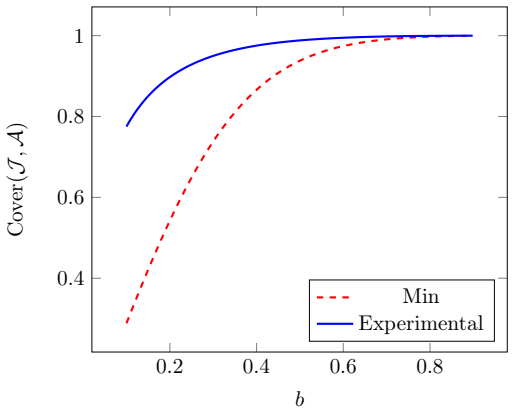
Proof. The coverage bounds come from similar arguments as in previous sections. The station s_J attains the maximal interference at s for $x < s$ and b for $x > s$. Thus, these points are used for calculating the constant interference and, later, the lower bound of the coverage value. □

Experimental results for this positioning scheme coverage are presented in Figure 3.14. Comparing these results with this algorithm's uniform counterpart (see Section 3.1), it is clear that coverage is better with non-uniform networks. Also, this scheme saves energy, as presented in Figure 3.15. Almost all results use $P_J < 0.5$, while the uniform model's power is fixed to 1.

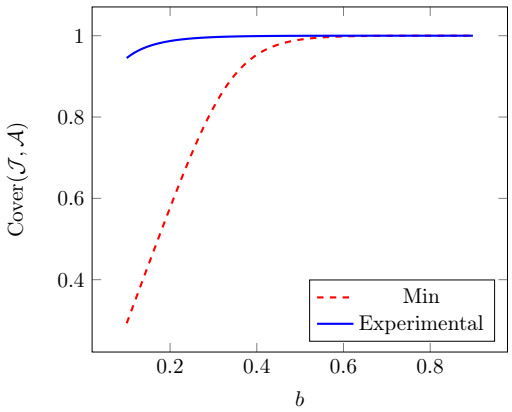
3.5 Noisy dust method

Up to this point, most of the presented methods focused on configuring one or two jamming stations, each with a power level equal to the protected station (uniform networks) or relatively similar (non-uniform networks). This approach simplified the algorithms and was usually based on a basic positioning scheme but with the caveat of having a high impact on the coverage values and high energy consumption. This section presents the idea of ***noisy dust***. It utilizes a high number of *small* jamming stations, with relatively small power levels, to *drown out* fragments of space for non-uniform networks. Limiting the power level of a single jamming station decreases overall energy usage compared to the previously analyzed algorithms, and the coverage value improves.

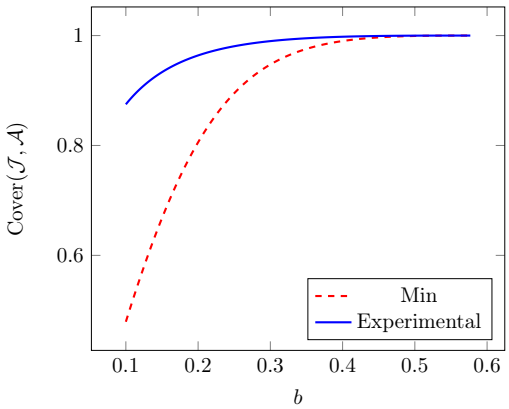
First, the description of what fragment of space a single station protects is presented in Section 3.5.1. Afterward, the adaptive noisy dust scheme, having the energy-efficiency related properties, is presented in Section 3.5.2, followed by a version of noisy dust scheme adjusted for more generic use-cases, utilizing the *stripes* of stations, is presented in Section 3.5.3. Finally, the coverage is analyzed for the generalized noisy dust in Section 3.5.4.



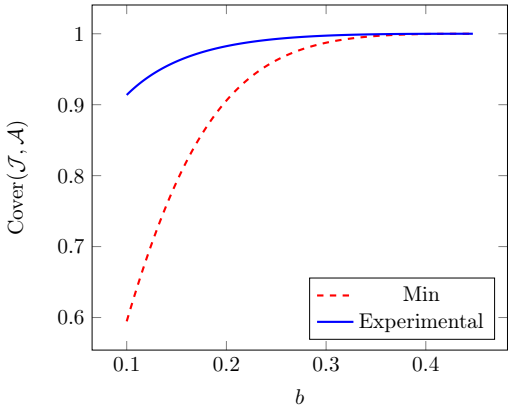
(a) Network using $N = 1, \beta = 1, \alpha = 2$.



(b) Network using $N = 1, \beta = 1, \alpha = 4$.



(c) Network using $N = 1, \beta = 3, \alpha = 2$.



(d) Network using $N = 5, \beta = 1, \alpha = 2$.

Figure 3.14: Measurements of coverage for the network $\mathcal{A}$ and the jamming network $\mathcal{J}$ defined in Theorem 7. *Experimental* is the coverage measurement based on sampling, the *Min* is the lower bound.

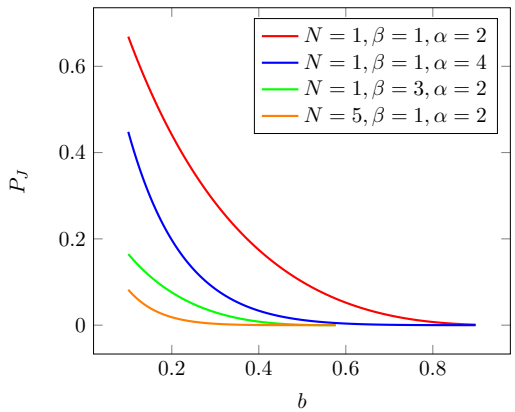


Figure 3.15: The value of P_J from Theorem 7, for different network configurations.

3.5.1 Effective jamming range

For a single station s with power $P \equiv 1$, without loss of generality, the **effective jamming range** of a station s_J can be defined as the convex fragment of space, which is correctly protected by this jamming station only. The construction of an effective jamming range is presented in Figure 3.16. For an initial network $\mathcal{A}$, some given point $b_l > s$ and power level $0 < p < P$, define:

- $F(p) = (p\beta)^{\frac{1}{\alpha}}$,
- $x_l = F(p) \cdot d(s, b_l)$,
- $x_r = x_l \left(\frac{1+F(p)}{1-F(p)}\right)$,
- $b_r = d(s, b_l) + x_l + x_r$.

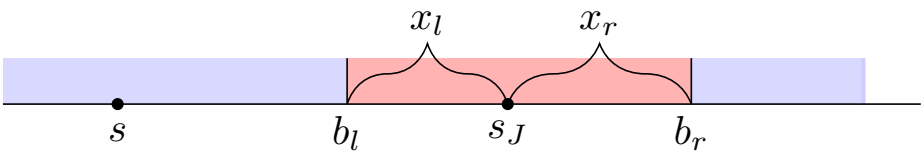


Figure 3.16: The effective jamming range of s_J is highlighted by a red color. The blue space represents the reception zone of s.

Theorem 8. *For an initial network $\mathcal{A}$, point b_l and power level p, construct a jamming network:*

$$\mathcal{J} = \left(S^{(J)} = \{s_J\}, P^{(J)} \equiv p\right) .$$

The $\mathcal{J}$ correctly protects $\mathcal{A}$ for $\mathcal{R}_{\overline{b_l,b_r}}$ if:

$$s_J = d(s, b_l) + x_l .$$

Proof. The position of the station s_J has to ensure that $\mathrm{SINR}(s, b_l) = \beta$. Because:

$$\mathrm{SINR}(s, b_l) \leq \mathrm{SIR}(s, b_l) ,$$

it is enough to analyze this requirement under the SIR model:

$$\mathrm{SIR}(s, b_l) = \frac{d(s, b_l)^{-\alpha}}{p \cdot x_l^{-\alpha}} = \beta .$$

From it, the value of $x_l = d(b_l, s_J)$ can be acquired, so $\mathrm{SIR}(s, x) < \beta$ for all points $x \in (b_l, s_J)$:

$$x_l = (p\beta)^{\frac{1}{\alpha}} \cdot d(s, b_l) \ = F(p) \cdot d(s, b_l) .$$

With the knowledge about the position of s_J, the extreme border point b_r, on the opposite side of the station s_J, can be calculated, a similar approach:

$$\mathrm{SIR}(s, b_r) = \frac{(d(s, b_l) + x_l + x_r)^{-\alpha}}{p \cdot x_r^{-\alpha}} = \beta .$$

From that, its distance from s_J is acquired:

$$x_r = \frac{F(p) \cdot (d(s, b_l) + x_l)}{1 - F(p)} = F(p) \cdot d(s, b_l) \left(\frac{1 + F(p)}{1 - F(p)}\right) = x_l \left(\frac{1 + F(p)}{1 - F(p)}\right) .$$

With $\mathrm{SIR}(s, b_l) = \mathrm{SIR}(s, b_r) = \beta$ and based on the monotonicity of the energy function in domains (b_l, s) and (s, b_r), all points $x \in (b_l, b_r)$ will attain $\mathrm{SIR}(s, x) < \beta$. It will also be true for $\mathrm{SINR}(s, x) < \beta$ because adding noise can only reduce the reception zone of s. □

This result can be utilized for positioning multiple jamming stations with the intention to *fill* the space with small effective jamming ranges. Other stations only add interference, so the size of the effective jamming range presented in the theorem would still hold.

3.5.2 Adaptive noisy dust

The first scheme, **adaptive noisy dust**, utilizing the idea of noisy dust, introduced in Section 3.5, is based on the iterative positioning of stations with some chosen low power level, one next to another - to tightly fill the restricted area with small effective jamming ranges. One of the significant advantages of this approach is the reduced energy usage, which converges to zero with the decrease of a single station's power and an increased number of stations for the fixed restricted area.

Algorithm 2: NoisyDust for $\mathcal{A}$.

Function `GetStationPosition` (b, p, i)
  return $b \cdot \frac{(1+F(p))^i}{(1-F(p))^{i-1}}$
Algorithm `NoisyDust` (b, p)
  $n = \left\lceil \frac{\ln\left(\frac{\text{range}(s)}{b}\right)}{\ln\left(\frac{1+F(p)}{1-F(p)}\right)} \right\rceil$
  $S^{(J)} \leftarrow \{\}$
  for $i \leftarrow \{1, \cdots, n\}$ **do**
    $s_i \leftarrow$ `GetStationPosition(`b, p, i`)`
    $S^{(J)} \leftarrow S^{(J)} \cup \{s_i\}$
  $\mathcal{J} \leftarrow \left(S^{(J)}, P^{(J)} \equiv p\right)$
  return $\mathcal{J}$

The algorithm is pretty straightforward. It starts by selecting the required number of jamming stations n, based on the network parameters, requested jamming station power level p, and the position of a border point b. It is designed to cover the whole segment $(b, \text{range}(s))$ with interference. Afterward, it iteratively positions each station s_i, assigning them with power p. Note that the n selection formula can be easily modified, so it will cover an arbitrary segment (b, b^*), for $b < b^* \leq \text{range}(s)$, but this thesis focuses on the worst-case scenario.

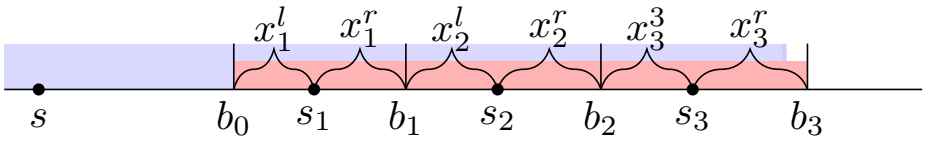


Figure 3.17: The Algorithm 2 example.

Theorem 9. *The jamming network* $\mathcal{J} =$ `NoisyDust`(b, p) *correctly protects* $\mathcal{A}$ *for* $\mathcal{R}_b$.

Proof. The procedure is depicted in Figure 3.17. The algorithm utilizes the properties from the Theorem 8, where the single station effective jamming range is calculated. This proof starts with extending it to positioning multiple stations, using the recursive dependency between them. Later, it is replaced by an iterative method, along with analyzing a network's required size and energy usage characteristics.

The first positioned station is denoted as s_1, and by following the theorem, its position is set based on the anchor point $b_0 = b$:

$$s_1 = d(s, b_0) + F(p) \cdot d(s, b_0) = d(s, b_0)(1 + F(p)) \ .$$

This position allows for covering an interval (b_0, b_1) with interference, for:

$$d(s, b_1) = d(s, b_0) + x_1^l + x_1^r \ ,$$

where:

$$x_1^l = F(p) \cdot d(s, b_0) \ , \qquad x_1^r = x_1^l \left(\frac{1 + F(p)}{1 - F(p)}\right) \ .$$

The value, being also the position, of the second border point b_1 can be simplified using these partial interval lengths:

$$\begin{aligned} d(s,b_1) &= d(s,b_0) + F(p)\cdot d(s,b_0) + (F(p)\cdot d(s,b_0))\left(\frac{1+F(p)}{1-F(p)}\right) \\ &= d(s,b_0)\left(1+F(p)+F(p)\left(\frac{1+F(p)}{1-F(p)}\right)\right) \\ &= d(s,b_0)\left(\frac{1+F(p)}{1-F(p)}\right) \ . \end{aligned}$$

The process can be repeated for the station s_2, which would take the b_1 as a base for positioning, which results in:

$$s_2 = d(s,s_2) = d(s,b_1)(1+F(p)) \ .$$

And a similar result for the next border point:

$$d(s,b_2) = d(s,b_1)\left(\frac{1+F(p)}{1-F(p)}\right) \ .$$

Based on it, the recursive dependency between consecutive border points b_i for $i \geq 0$ can be described as:

$$d(s,b_i) = d(s,b_{i-1})\left(\frac{1+F(p)}{1-F(p)}\right) = d(s,b_0)\left(\frac{1+F(p)}{1-F(p)}\right)^i \ .$$

It uses the point $b_0 = b$, provided as an input parameter to the whole algorithm. A similar recursive dependency exists between station positions for $i > 0$:

$$s_i = d(s,s_i) = d(s,b_{i-1})(1+F(p)) = d(s,b_0)(1+F(p))\left(\frac{1+F(p)}{1-F(p)}\right)^{i-1} = d(s,s_1)\left(\frac{1+F(p)}{1-F(p)}\right)^{i-1} \ .$$

The modified version of this equation is used in the algorithm positioning scheme:

$$d(s,s_1)\left(\frac{1+F(p)}{1-F(p)}\right)^{i-1} = d(s,b)\frac{(1+F(p))^i}{(1-F(p))^{i-1}} \ .$$

Any interval starting from b is correctly protected because stations are tightly positioned, one next to another, and they fill it in the whole range of a station s. To finalize the correctness of the algorithm, the required number of stations has to be found. The final border point in a chain should be outside of the maximal range of the station s, i.e., $d(s,b_n) > \text{range}(s)$:

$$d(s,b_0)\left(\frac{1+F(p)}{1-F(p)}\right)^n > \text{range}(s) \ .$$

After transforming the inequality, the result is:

$$n = \left\lceil \frac{\ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right)}{\ln\left(\frac{1+F(p)}{1-F(p)}\right)} \right\rceil \ .$$

It finalizes the proof of the algorithm's correctness. □

As mentioned earlier, the algorithm energy efficiency increases with the decrease of a single station's power usage and the increase of the number of stations.

Lemma 13. *The cost of the jamming network* $\mathcal{J} = \texttt{NoisyDust}(b,\ p)$ *protecting* $\mathcal{A}$ *for* $\mathcal{R}_b$ *converges:*

$$\lim_{p\to 0^+} \text{Cost}(\mathcal{J}) = 0 \ .$$

Proof. By using the just calculated number of stations, the overall energy used by the jamming stations is equal to:

$$\text{Cost}(\mathcal{J}) = np \ .$$

The original version of the n definition is numerically complex to analyze, so the version with the ceiling function removed is considered:

$$\tilde{n} = \frac{\ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right)}{\ln\left(\frac{1+F(p)}{1-F(p)}\right)} \ .$$

The aligned cost function:

$$\text{Cost}'(\mathcal{J}) = \tilde{n}p \ = \frac{p\ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right)}{\ln\left(\frac{1+F(p)}{1-F(p)}\right)}.$$

Lets split it into numerator, denoted as $\text{num}(p)$ and denominator, denoted as $\text{den}(p)$:

$$\text{num}(p) = p\ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right) \ , \qquad \text{den}(p) = \ln\left(\frac{1+F(p)}{1-F(p)}\right) \ .$$

Realize that $\text{range}(s)$ and position of b_0 does not depend on p (i.e., both are constants in this context), which means that the numerator of the Cost' converges to zero:

$$\lim_{p\to 0^+} \text{num}(p) = \lim_{p\to 0^+} p\ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right) = 0 \ .$$

As for $F(p) = (p\beta)^{\frac{1}{\alpha}}$, it converges to zero too:

$$\lim_{p\to 0^+} F(p) = 0 \ .$$

It is also true for the denominator of the cost equation:

$$\lim_{p\to 0^+} \text{den(p)} = \lim_{p\to 0^+} \ln\left(\frac{1+F(p)}{1-F(p)}\right) = ln\,(1) = 0 \ .$$

Because the numerator and denominator converge to zero, the L'Hôpital's rule can be used to find the cost function limit for p converging to zero. First, the derivative of $F(p)$ is calculated:

$$\frac{\partial\, F(p)}{\partial\, p} = \frac{(\beta p)^{\left(\frac{1}{\alpha}-1\right)}\beta}{\alpha} = \frac{F(p)}{\alpha p} \ .$$

In the next steps, the derivatives of the numerator and denominator have to be found:

$$\begin{aligned}
\frac{\partial\,\text{num}(p)}{\partial\, p} &= \ln\left(\frac{\text{range}(s)}{d(s,b_0)}\right) \\
\frac{\partial\,\text{den}(p)}{\partial\, p} &= \left(\frac{1-F(p)}{1+F(p)}\right)\frac{\frac{\partial\, F(p)}{\partial\, p}(1-F(p)) + \frac{\partial\, F(p)}{\partial\, p}(1+F(p))}{(1-F(p))^2} \\
&= \frac{\partial\, F(p)}{\partial\, p}\frac{2}{(1-F(p))(1+F(p))} = \frac{2F(p)}{\alpha p(1-F(p)^2)} \ .
\end{aligned}$$

Finally, from L'Hôpital's rule:

$$\begin{aligned}\lim_{p\to 0^+} \mathrm{Cost}'(\mathcal{J}) &= \lim_{p\to 0^+} \frac{\mathrm{num}(p)}{\mathrm{den}(p)} = \lim_{p\to 0^+} \frac{\frac{\partial\,\mathrm{num}(p)}{\partial\,p}}{\frac{\partial\,\mathrm{den}(p)}{\partial\,p}} \\ &= \lim_{p\to 0^+} \ln\left(\frac{\mathrm{range}(s)}{d(s,b_0)}\right) \frac{\alpha p(1-F(p)^2)}{2F(p)} \\ &= \alpha \ln\left(\frac{\mathrm{range}(s)}{d(s,b_0)}\right) \lim_{p\to 0^+} \frac{p\left(1-(\beta p)^{\frac{2}{\alpha}}\right)}{2\,(\beta p)^{\frac{1}{\alpha}}} \\ &= \alpha \ln\left(\frac{\mathrm{range}(s)}{d(s,b_0)}\right) \lim_{p\to 0^+} p^{1-\frac{1}{\alpha}} \frac{\left(1-(\beta p)^{\frac{2}{\alpha}}\right)}{2\,(\beta)^{\frac{1}{\alpha}}} = 0\ .\end{aligned}$$

Therefore, also $\mathrm{Cost}(\mathcal{J})$ tends to 0 as $p \to 0^+$, because:

$$|\mathrm{Cost}(\mathcal{J}) - (\mathrm{Cost}'(\mathcal{J}) + p)| < 2p\ ,$$

That concludes the proof. □

The details of the algorithm can be adjusted to match more specific configurations, e.g., for restricted areas of form $\mathcal{R}_{\overline{b_l,b_r}}$. Nonetheless, the zero-energy property and correctness should remain valid for such modifications. The coverage analysis of this algorithm will be presented in Section 3.5.4.

3.5.3 Noisy dust stripes

The adaptive noisy dust, presented in Section 3.5.2, provides an exact and effective method of jamming fragments of space with a small energy and coverage reduction footprint. The possible problem with it might be related to the positioning scheme, which is rather precise and, for some scenarios, might not be possible to achieve. To prevent it, the different flavor of the noisy dust is presented - **noisy dust stripes**. This approach is also focused on using many stations with low power levels. However, the positioning scheme will be simplified, and the distances between stations will depend only on their power levels and the initial border point, making them equal. It allows for deploying stations with less knowledge in the form of *stripes*. The idea is depicted in Figure 3.18. Note that the segment (b_0, b_1) represents the restricted area in this algorithm.

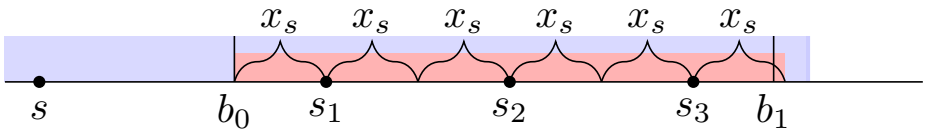


Figure 3.18: The noisy dust *stripe* example.

Theorem 10. *For initial network $\mathcal{A}$ and restricted area $\mathcal{R}_{\overline{b_0,b_1}}$ and some power level $0 < p < 1$, define:*

$$n = \left\lceil \frac{b_1 - b_0}{2F(p)b_0} \right\rceil\ , \qquad s_i = b_0(1 + F(p) + 2(i-1)F(p))\ .$$

The jamming network $\mathcal{J}_p = (\{s_i :\ i \in 1\ldots n\}, \{s_i \mapsto p :\ i \in 1\ldots n\})$ correctly protects $\mathcal{A}$ for $\mathcal{R}_{\overline{b_0,b_1}}$.

Proof. Take a look at the jamming station closest to b_0:

$$s_1 = b_0 + F(p)b_0\ .$$

Based on Theorem 8, it correctly protects the interval (b_0, s_1) and:

$$x_s = d(b_0, s_1) = F(p)b_0 \ .$$

On the other hand, due to the energy function of s being monotonously decreasing for $x > s$, it is known that any point $x > s_1$ requires less interference than point b_0 to be jammed. However, we have already generated enough interference at the range of x_s from s_1 to jam such points. Thus, the effective jamming interval of s_1 is $(b_0, b_0 + 2x_s)$. The next jamming station, positioned at some point $s_2 > s_1$, is also correctly protecting segment $(s_2 - x_s, s_2 + x_s)$ because of the energy of s decrease with distance. Note, as described in Theorem 8, these are not maximal possible protected intervals, but in this algorithm, the point is to keep stations equally spaced. By doing it, for $i > 1$ the station is positioned at:

$$s_i = b_0 + (2(i-1)+1)x_s \ = b_0 + (2(i-1)+1)F(p)b_0.$$

As each of the stations covers the interval of width $2x_s$, and the whole interval covered by all stations is of length $d(b_0, b_1)$, the number of required stations is equal to:

$$n = \left\lceil \frac{b_1 - b_0}{2x_s} \right\rceil \ .$$

□

The idea of Theorem 10 with single *stripe* set can be easily extended for jamming arbitrary networks — it only requires finding the closest points to protect (border points for each broadcasting station) and then configuring *stripes* accordingly. The coverage of this algorithm is analyzed in Section 3.5.4.

3.5.4 Noisy dust coverage

The lower bound on the coverage for the general noisy dust algorithms is presented in Theorem 11. It assumes that the analyzed restricted area is $\mathcal{R}_b$ and that a noisy dust algorithm was correctly configured.

Theorem 11. *For an initial network $\mathcal{A}$ and a jamming network $\mathcal{J} = \left(S^{(J)}, P^{(J)} \equiv p\right)$, generated by a noisy dust algorithm for a restricted area $\mathcal{R}_b$, the coverage is bounded from below:*

$$\mathrm{Cover}(\mathcal{J}, \mathcal{A}) \geq \frac{(\beta(N + \mathrm{MaxI}_l))^{-\frac{1}{\alpha}} + (\beta(N + \mathrm{MaxI}_r))^{-\frac{1}{\alpha}}}{\mathrm{range}(s) + b} \ ,$$

where:

$$\mathrm{MaxI}_l = \sum_{s_j \in S^J} p \cdot d(s_j, s)^{-\alpha} \ , \quad \mathrm{MaxI}_r = \sum_{s_j \in S^J} p \cdot d(s_j, b)^{-\alpha} \ .$$

Proof. The approach is similar to the proof of Lemma 1. The interference is approximated separately for the left and right sides of station s. On the right side, in the interval (s, b), the maximal interference generated by the noisy dust stations is attained at point b. It comes from the fact that stations are located in the interval (b, ∞), and their energy functions are monotonic for points in (s, b). Precisely, their energy decreases the closer it gets to station s. This value is MaxI_r. On the opposite side of station s, so for the interval $(-\mathrm{range}(s), s)$, the maximal interference of the noisy dust is attained at point s. Using a similar approach, this interference is denoted as MaxI_l. Finally, the Fact 1 can be applied to both interference limits:

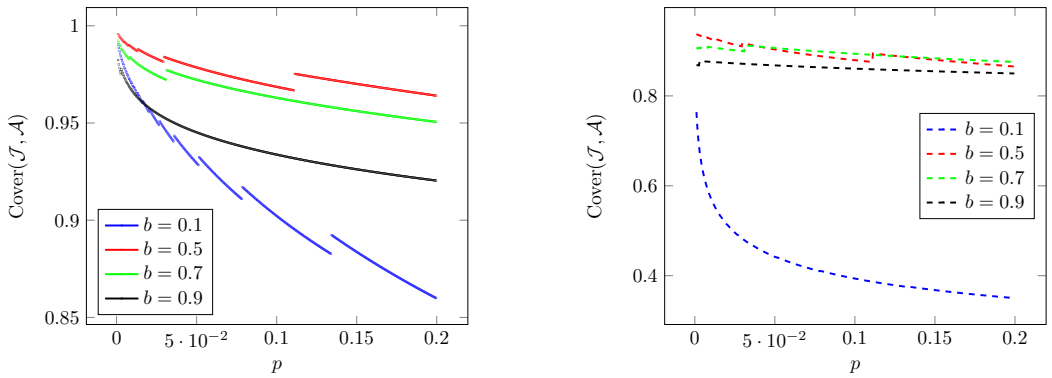
$$\mathrm{SI_cNR}_{\mathcal{A}}(s, x_l, \mathrm{MaxI}_l) = \beta \ , \qquad \mathrm{SI_cNR}_{\mathcal{A}}(s, x_l, \mathrm{MaxI}_l) = \beta \ .$$

It gets:

$$x_l = (\beta(N + \mathrm{MaxI}_l))^{-\frac{1}{\alpha}} \ , \qquad x_r = (\beta(N + \mathrm{MaxI}_r))^{-\frac{1}{\alpha}} \ .$$

It means that the size of a reception zone of s is bounded from below by $d(x_l, x_r)$. As the maximal possible reception zone is limited by a segment $(-\mathrm{s}, b)$, it finalizes the proof. □

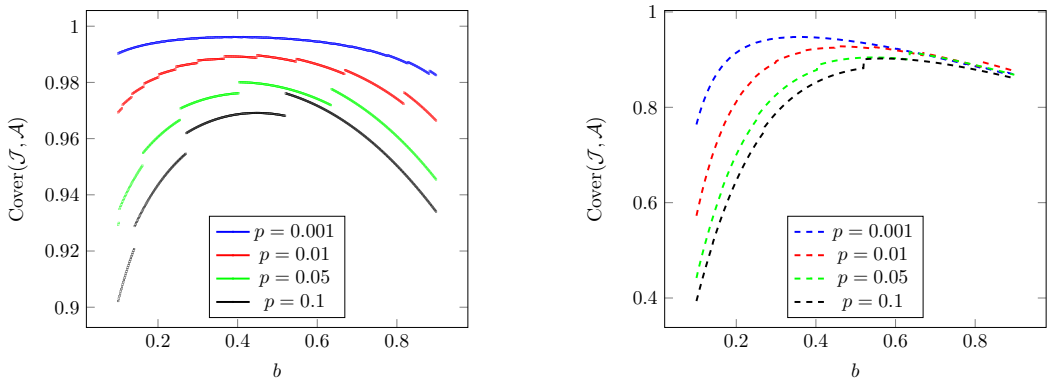
The coverage for both noisy dust algorithms was measured using the sampling method mentioned in Section 2.3. The adaptive noisy dust was analyzed for different values of p (see Figure 3.19) and b (see Figure 3.20) for a standard network configuration. The characteristic *steps* visible in the plot show when the algorithm adds or removes the stations, temporarily worsening or improving coverage. For the changing values of p, it is observable that experimental results tend to 1. It also shows that the lower bound presented in this subsection is not precise for all configurations. The results for changing values of b show that algorithm coverage efficiency worsens when applied on the extreme configurations - either too close to s or too far - it seems to work best for point b being positioned in the middle of a station s range.



(a) Experimental coverage.

(b) Coverage lower bound.

Figure 3.19: Adaptive noisy dust coverage for a network with $N = 1$, $\beta = 1$, $\alpha = 2$, for different values of p.

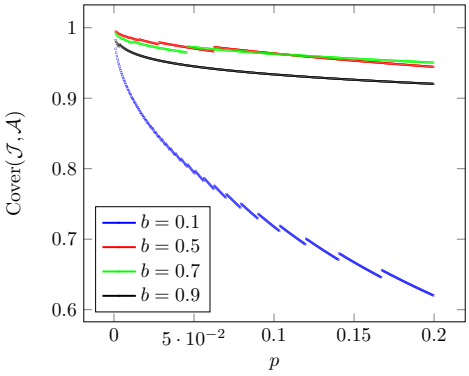


(a) Experimental coverage.

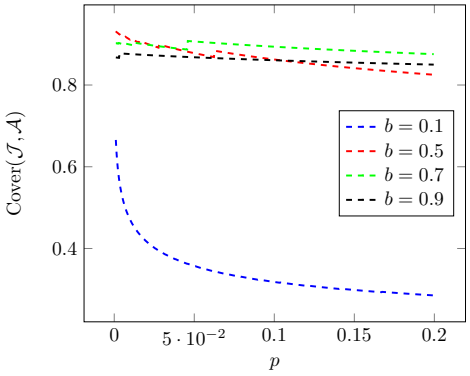
(b) Coverage lower bound.

Figure 3.20: Adaptive noisy dust coverage for a network with $N = 1$, $\beta = 1$, $\alpha = 2$, for different values of b.

The noisy dust stripes algorithm was also analyzed for p (see Figure 3.21) and b (see Figure 3.22). Its results are similar to the adaptive noisy dust, though much more frequent *steps* are visible, showing that more stations are being used for similar configurations. Its overall coverage also seems worse, but it is expected, given the gain in flexibility with fixed distances between stations. Other characteristics, like coverage converging to 0 with power level decrease and the better coverage results for points b focused in the range center, look similar.

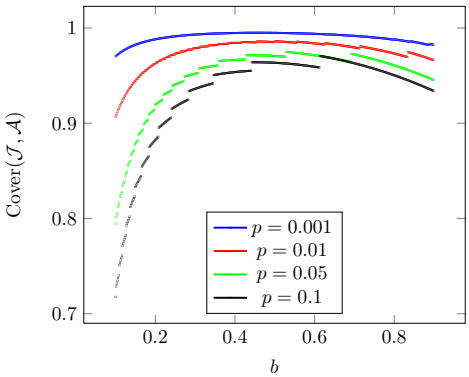


(a) Experimental coverage.

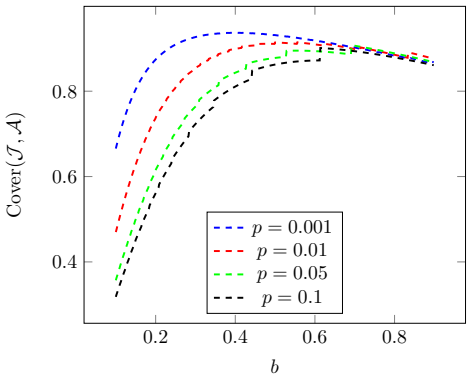


(b) Coverage lower bound.

Figure 3.21: Noisy dust stripes coverage for a network with $N = 1$, $\beta = 1$, $\alpha = 2$, for different values of p.



(a) Experimental coverage.



(b) Coverage lower bound.

Figure 3.22: Noisy dust stripes coverage for a network with $N = 1$, $\beta = 1$, $\alpha = 2$, for different values of b.

Chapter 4

Jamming in 2D SINR

In this chapter, networks positioned on a two-dimensional plane are considered. Reception zones are no longer reducible to sets of intervals, and more complex shapes are encountered in a two-dimensional case, making the analysis more complicated.

Due to the high complexity of possible configurations for the problem, the set of chosen restricted area models is defined in Section 4.1 - these are used for analyzing the effectiveness of algorithms presented later. Methods related to the uniform network model are described in Section 4.2, and for the non-uniform network, the *noisy dust* extension is presented in Section 4.3. This chapter uses an initial network of the following form:

$$\mathcal{A} = \langle D = 2, S = \{s\}, N, \beta, P, \alpha \rangle \ .$$

Similarly to the previous chapter, the single station is positioned at $s = (0, 0)$ and has a fixed power level, defined as $P(s) = 1$. The area of a 2D region is denoted by the $|.|$ operator, e.g. $|\mathcal{P}|$ is an area of polygon $\mathcal{P}$.

4.1 Restricted area types

The generic restricted area can have distinctive, complex shapes, including some unrealistic ones. For example, it can take a degenerated form of points scattered throughout the plane. Designing algorithms and analyzing their effectiveness for such restricted areas can be challenging. To prevent this issue, several restricted area types are selected and formally defined in this section. They are based on simple geometric shapes, which should remain close to the possible real-world scenarios and allow for effective algorithm creation and analysis.

The first type is an *enclosed* restricted area - defined by some bounding shape, inside which the communication is considered safe, but cannot leak outside of this shape. This space has a connected character, with protected stations inside the chosen shape. Within this type, two sub-types can be defined, based on the shape of enclosing figure - *circular*, as defined in Definition 11.1; and *polygonal* area, defined in Definition 11.2. Both sub-types are depicted in Figure 4.1 (red space is a restricted area, and black dots represent stations).

Definition 11.1. *The **enclosing circular area** is defined for $x, y, r \in \mathbb{R}$, as:*

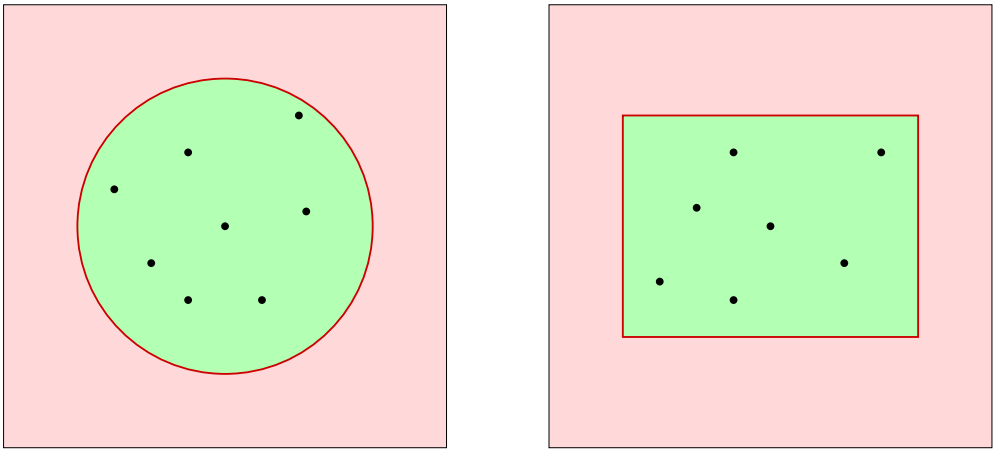
$$\mathcal{R}_r^{en}(x, y) = \mathbb{R}^2 \setminus \mathcal{B}(r, (x, y)) \ .$$

If the circular area central point is a point $g = (g_x, g_y)$, the notation is simplified to:

$$\mathcal{R}_r^{en}(g_x, g_y) = \mathcal{R}_r^{en}(g) \ .$$

Definition 11.2. *The **enclosing polygonal area** is defined for $\mathcal{P}$ being a convex polygon as:*

$$\mathcal{R}_{\mathcal{P}}^{en} = \mathbb{R}^2 \setminus \mathcal{P} \ .$$



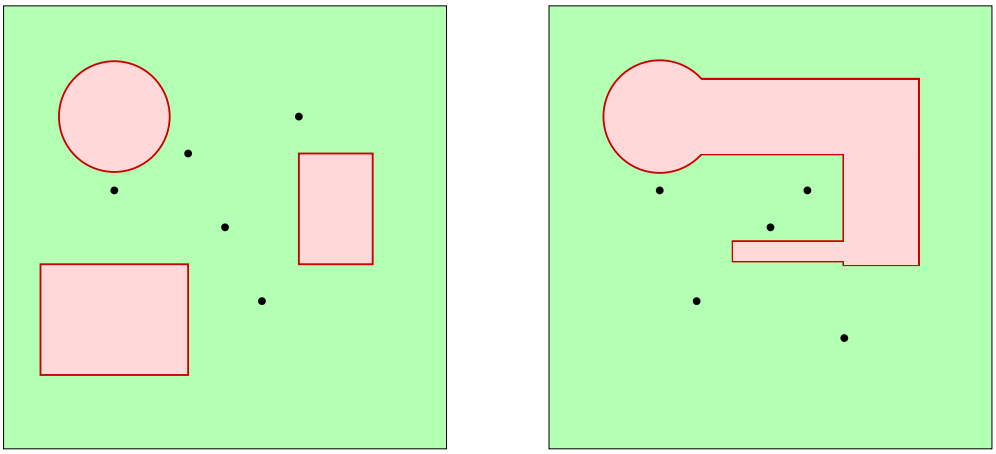
(a) A *circular enclosed* area.

(b) A *polygonal enclosed* area.

Figure 4.1: Examples of enclosing areas. Red space is a restricted area. Stations are denoted as black dots.

The second major type is a *detached* area, in which the restricted area consists of a union of polygons and balls scattered over the 2D plane and the protected stations in space between them. It is formally defined in Definition 11.3 and presented in Figure 4.2.

Definition 11.3. *The* ***detached area*** $\mathcal{R}^d_{\mathcal{G}}$ *is defined as a union of 2-balls* $\mathcal{B}(r,p)$ *for points* $p \in \mathbb{R}^2$ *and radii* $r > 0$*; and convex polygons* $\mathcal{P}$*.*



(a) A *detached* area with scattered figures.

(b) A *detached* area with a complex shape created from convex components.

Figure 4.2: Examples of detached areas. Red space is a restricted area. Stations are denoted as black dots.

4.2 Jamming in a uniform network

Similarly to the 1D model, the uniformity of a network in 2D comes with some nice properties of the reception zones and allows for a generic approach for positioning jamming stations. Interactions of two stations' reception zones, if positioned next to each other, are presented in Section 4.2.1. In Section 4.2.2, the generic algorithm is described for protecting the polygonal enclosing areas. Its extension for circular enclosing areas is presented in Section 4.2.3. Finally, the approach feasible for detached areas is discussed in Section 4.2.4.

4.2.1 Basic two stations model

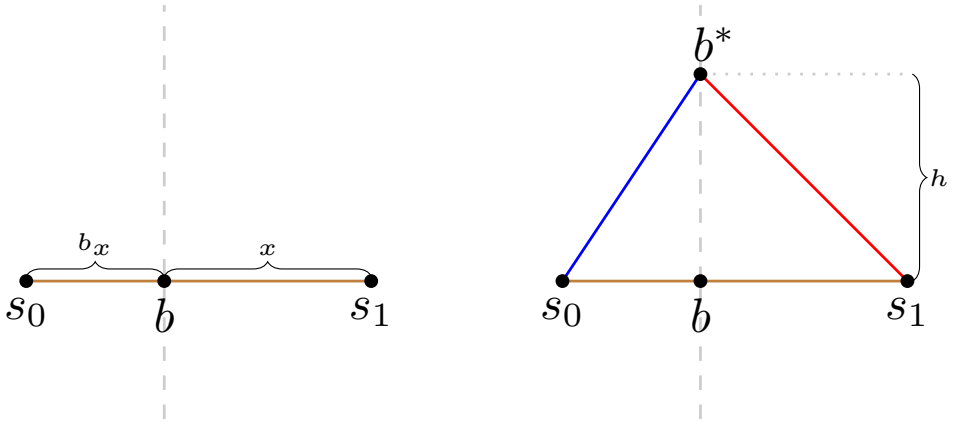
This section describes the interaction between two reception zones when only two stations with the same powers are positioned on the plane. The input configuration is a single station s_0, a border point b, and a line passing through that point. The line splits the plane into two half-planes, presenting how to position the other station s_1 so that the reception zone of station s_0 can be limited only to one of these half-planes. The positioning of the second station also limits the impact on the s_0 reception zone size, making it to *stick* to the line (ignoring the trivial scenarios, when the s_0 reception zone is already limited to the one half-plane). This method is presented in Lemma 14, with construction details depicted in Figure 4.3b.

Lemma 14. *Let $\mathcal{A} = \langle D = 2, S = \{s_0, s_1\}, N, \beta, P \equiv 1, \alpha \rangle$ be a network and define a border point $b = (b_x, 0)$. Position stations at:*

$$s_0 = (0, 0) \ , \qquad s_1 = \left(b_x \left(1 + \beta^{\frac{1}{\alpha}} \right), 0 \right) \ .$$

For any point $p \in \{(a, b) \in \mathbb{R}^2 : a \geqslant b_x\}$:

- $\mathrm{SIR}(s_0, p) \leqslant \beta$,
- $\mathrm{SINR}(s_0, p) < \beta$, *for* $N > 0$.



(a) Two stations' placing.

(b) A point on the line dividing two half-planes.

Figure 4.3: Positioning of the jamming station.

Proof. First step is to find the distance $x = d(s_1, b)$ (see Figure 4.3a), such that:

$$\mathrm{SIR}(s_0, b) = \frac{d(s_0, b)^{-\alpha}}{d(s_1, b)^{-\alpha}} = b_x^{-\alpha} x^{\alpha} = \beta \ .$$

The equation can be transformed to:

$$x = b_x \beta^{\frac{1}{\alpha}} \ .$$

Examine the point $b^* = (b_x, h)$ for $h = d(b, b^*)$, located on the line perpendicular to the segment $\overline{s_0 s_1}$ and crossing the point b (see Figure 4.3b). Distances from b^* to stations s_0 and s_1 are equal to:

$$d(s_0, b^*) = \sqrt{b_x^2 + h^2} \ , \qquad d(s_1, b^*) = \sqrt{x^2 + h^2} \ .$$

Value of SIR for s_0 and such points take the form of:

$$\mathrm{SIR}(s_0, b^*) = \frac{d(s_0, b^*)^{-\alpha}}{d(s_1, b^*)^{-\alpha}} = \left(\frac{x^2 + h^2}{b_x^2 + h^2} \right)^{\frac{\alpha}{2}} = \left(\frac{b_x^2 \beta^{\frac{2}{\alpha}} + h^2}{b_x^2 + h^2} \right)^{\frac{\alpha}{2}} \ .$$

For $h = 0$ it gets $b^* = b$ and $\mathrm{SIR}(s_0, b^*) = \beta$. For $h > 0$:

$$\frac{\mathrm{SIR}(s_0, b^*)}{\beta} = \left(\frac{b_x^2 \beta^{\frac{2}{\alpha}} + h^2}{b_x^2 \beta^{\frac{2}{\alpha}} + h^2 \beta^{\frac{2}{\alpha}}} \right)^{\frac{\alpha}{2}} \leqslant 1 \ ,$$

as $\beta \geqslant 1$; and strict inequality for $\beta > 1$. Replacing SIR with SINR, where $N > 0$, also produces strict inequality. Realize, that any point (x^*, y^*), such that $x^* > b_x$, is closer to s_1 and further away from s_0 than some point $b^* = (b_x, y^*)$. In consequence:

$$\mathrm{SINR}(s_0, (x^*, y^*)) < \mathrm{SIR}(s_0, (x^*, y^*)) < \mathrm{SIR}(s_0, (b_x, y^*)) \leqslant \beta \ .$$

□

From Lemma 14, it can be immediately concluded that one can configure the position of a jamming station s_1 for an arbitrary line and a given station s_0 in such a way that guarantees the limitation of s_0's reception zone to the one side of this line.

4.2.2 Algorithm for jamming enclosing polygonal areas

The enclosing polygonal areas jamming algorithm is based on a class of restricted areas defined as complements of convex polygons $\mathcal{P}$. Note that $\mathcal{P}$ can be represented as a set of sides of the polygon, namely:

$$F_{\mathcal{P}} := \{\overline{(x, y)} : x, y \in \mathbb{R}^2 \text{ are consecutive vertices of } \mathcal{P}\} \ .$$

This subsection focuses on the simplified version of the problem, where there is only a single station s to protect, located inside a polygon. For the uniform model, Lemma 14 is utilized to design Algorithm 3, which, for a given polygonal restricted area, places jamming stations in a way that provides the protection for the station s at any point in $\mathcal{R}^{\mathrm{en}}_{\mathcal{P}} = \mathbb{R}^2 \setminus \mathcal{P}$. The algorithm takes each segment from $F_{\mathcal{P}}$ and assigns a single jamming station. More precisely, for each such segment $\overline{(x_j, y_j)}$, Algorithm 3 initially provides two lines:

- l_j^d, which includes the segment $\overline{(x_j, y_j)}$,
- l_j^p, which is perpendicular to l_j^d and crosses the position of a station s.

The crossing point of these two lines is denoted as the border point b. Furthermore, for each created pair of lines, Algorithm 3 positions the station s_j somewhere on the line l_j^p in a way that s and s_j are on the opposite sides of the line l_j^d. Therefore, utilizing the distance between b and s and Lemma 14, the algorithm calculates the distance between s_j and b as:

$$x = d(s, b)\beta^{\frac{1}{\alpha}} \ ,$$

for $d(s_j, s) = d(s, b) + x$.
The correctness of the Algorithm 3 output is described in Theorem 12 and the internal functions it uses are defined as:

- `GetLine`(x, y) creates a line, which includes the segment $\overline{(x, y)}$,
- `GetPerpendicularLine`(l, s) creates a line passing through the point s and being perpendicular to the line l,
- `GetLinesCrossingPoint`(l_0, l_1) calculates the position of a crossing point for lines l_0 and l_1.

Theorem 12. *For an initial network $\mathcal{A}$, a restricted area $\mathcal{R}^{en}_{\mathcal{P}}$ such that $s \in \mathcal{P}$ for a convex polygon $\mathcal{P}$, Algorithm 3 returns the jamming network $\mathcal{J}$, which correctly protects restricted area $\mathcal{R}^{en}_{\mathcal{P}}$.*

Algorithm 3: Create 2D uniform jamming network for a polygon

Algorithm `AssignUniformJammingStations`$(\mathcal{P}, s)$

$S^{(J)} \leftarrow \{\}$

for $(x_j, y_j) \leftarrow \mathcal{P}$ **do**

$l_j^d \leftarrow$ `GetLine`(x_j, y_j)

$l_j^p \leftarrow$ `GetPerpendicularLine`(l_j^d, s)

$b \leftarrow$ `GetLinesCrossingPoint`(l_j^d, l_j^p)

$s_j \leftarrow s + \overrightarrow{(b-s)} \cdot \left(1 + \beta^{\frac{1}{\alpha}}\right)$

$S^{(J)} \leftarrow S^{(J)} \cup \{s_j\}$

$\mathcal{J} \leftarrow \left(S^{(J)}, P^{(J)} \equiv 1\right)$

return $\mathcal{J}$

Proof. The algorithm constructs a straight line for each polygon side, splitting space into two half-planes. Then, the station s_j is positioned for such a segment, according to the scheme presented in Lemma 14, which guarantees that all points on half-plane on the opposite side of a line to station s, are outside its reception zone. Since the operation is performed for all segments of a convex polygon, all of these half-planes could be united into the restricted area $\mathcal{R}^{\text{en}}_{\mathcal{P}}$. Additional interference from other stations can only reduce a reception zone, so the restricted area is correctly protected. □

4.2.3 Jamming for circular enclosing areas

The problem of jamming in uniform networks gets complicated when restricted areas become irregular shapes or contain some arcs or curves. The approach from Section 4.2.2 is no longer directly applicable to protect the restricted areas. In this subsection, the focus is put on enclosed circular restricted areas, which are of the form $\mathcal{R}^{\text{en}}_r(x) = \mathbb{R}^2 \setminus \mathcal{B}(r, x)$, where $x \in \mathbb{R}^2$. The idea behind the presented approach is to use regular polygons, approximating the shape of the disk around a station. This way, the problem can be reduced to jamming the polygonal restricted area.

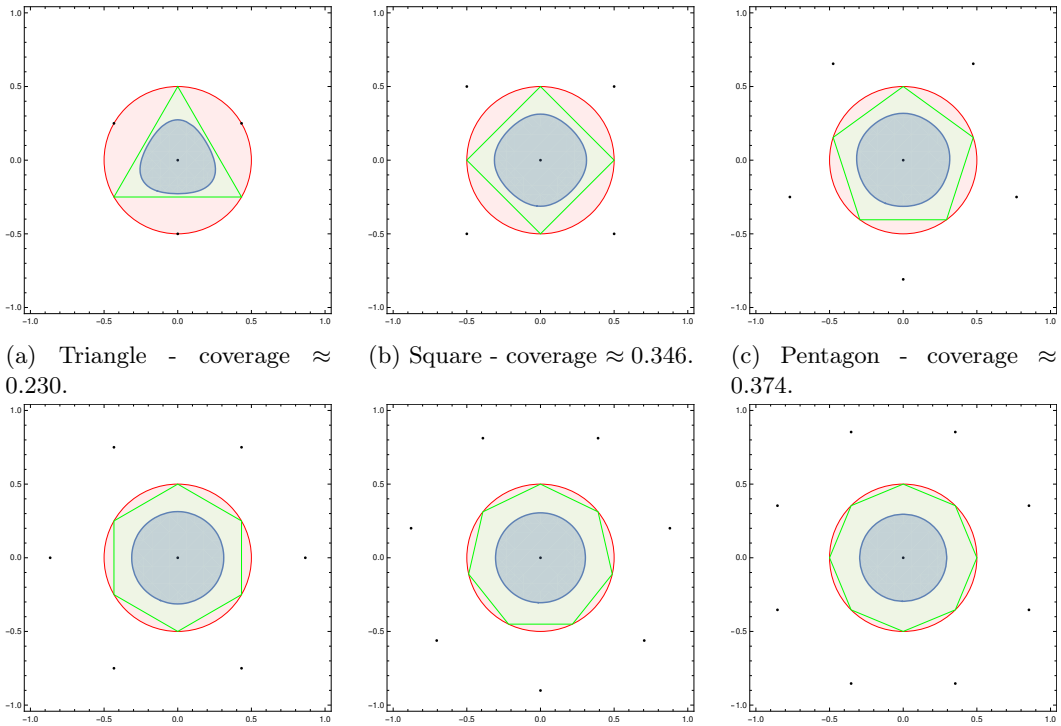
Fact 2. *For an initial network $\mathcal{A}$ and a restricted area $\mathcal{R}^{\text{en}}_r(s)$ for $r \in (0, \text{range}(s))$, Algorithm 3 for a regular polygon $\mathcal{P}$, inscribed into the disk $\mathcal{B}(r, s)$, as an input, returns a jamming network $\mathcal{J}$ correctly protecting the restricted area $\mathcal{R}^{\text{en}}_r(s)$.*

The reception zone of a single station can be restricted to any regular n-gon centered in the position of this protected station. A practical question is what n is ideal for such an arrangement of a task. Taking too small parameter n results in a smaller polygon (in terms of a measure), hence Algorithm 3 applies more potent interference outside the polygon, but still inside the original disk, which potentially can reduce the coverage. On the other hand, when n is too big, then Algorithm 3 arranges many stations, so their total interference may negatively affect the coverage, even when they are further from the center than in small n case. Moreover, it increases the cost of the jamming network. In Figure 4.4, different variants of polygons are presented, along with the experimental calculation of coverage for the initial network $\mathcal{A}$ and an enclosing area having a radius of length $r = 0.5$.

Besides the experimental coverage calculation, its value can be bounded for the algorithm using regular n-gons as presented in Lemma 15.

Lemma 15. *Let s be a single broadcasting station and $r \in (0, \text{range}(s))$. The restricted area is given by $\mathcal{R}^{en}_r(s)$, the jamming network $\mathcal{J}$ is created by Algorithm 3 for a regular n-gon $\mathcal{P}$ and b is the length of the polygon's apothem (the distance between s and sides of the polygon $\mathcal{P}$). The coverage of the combined network satisfies the following:*

$$\frac{(b(\beta b^{\alpha} N + n)^{-\frac{1}{\alpha}})^2}{r^2} \leqslant \text{Cover}(\mathcal{J}, \mathcal{A}) \leqslant \frac{|\mathcal{P}|}{\pi r^2} \ .$$



(a) Triangle - coverage ≈ 0.230.
(b) Square - coverage ≈ 0.346.
(c) Pentagon - coverage ≈ 0.374.
(d) Hexagon - coverage ≈ 0.367.
(e) Heptagon - coverage ≈ 0.349.
(f) Octagon - coverage ≈ 0.327.

Figure 4.4: Different circular shapes approximations. A red space represents the initial disk, a green space – the polygon – and blue space is the final reception zone. Black dots indicate stations.

Proof. The upper bound is obvious from Fact 2 — the maximal reception zone is limited by some polygon $\mathcal{P}$. The lower bound can be calculated by approximating the maximal range of station s in a direction to one of the jamming stations s_j. It is realized by a tricky modification of the resulting network, which assumes that all jamming stations are placed in the same point s_j (this trick effectively increases the power of s_j n times). The construction is presented in Figure 4.5. The radius of a disk inside the restricted area is denoted as r, b is the length of an apothem of the inscribed polygon (square in the example, given by the dotted lines), and x is the point placed at a maximal distance from s on the segment connecting s and one of the jamming stations, for which s is heard at x.

The unified jamming stations configuration (for which the following calculations are performed) is denoted as:

$$\mathcal{A}^J_{uni} = \langle D = 2, S = \{s, s_j\}, N, \beta, P, \alpha \rangle \ .$$

Station s_j simulates multiple stations from the jamming network, so $P(s_j) = n$. The point x is located on the segment $\overline{(s, s_j)}$, where $\mathrm{SINR}(s, x) = \beta$ and the interference at this point equals to some value $I(s, x)$. Realize that for the uniform algorithm example, with jamming stations located at their original positions, no point on the circle centered at s with radius $d(s, x)$ receives more interference than point x in the unified stations' scenario (due to the exponential decrease of jamming stations powers with a distance). Because of it, the value of $d(s, x)$ can be used as the lower bound of the radius of a reception zone of the station s. Represent this value in a form $d(s, x) = ab$, where $a \in (0, 1]$ and the inequality to satisfy it is of form:

$$\mathrm{SINR}_{\mathcal{A}^J_{uni}}(s, x) = \frac{(ab)^{-\alpha}}{N + n(d(s_j, s) - ab)^{-\alpha}} \geqslant \beta \ .$$

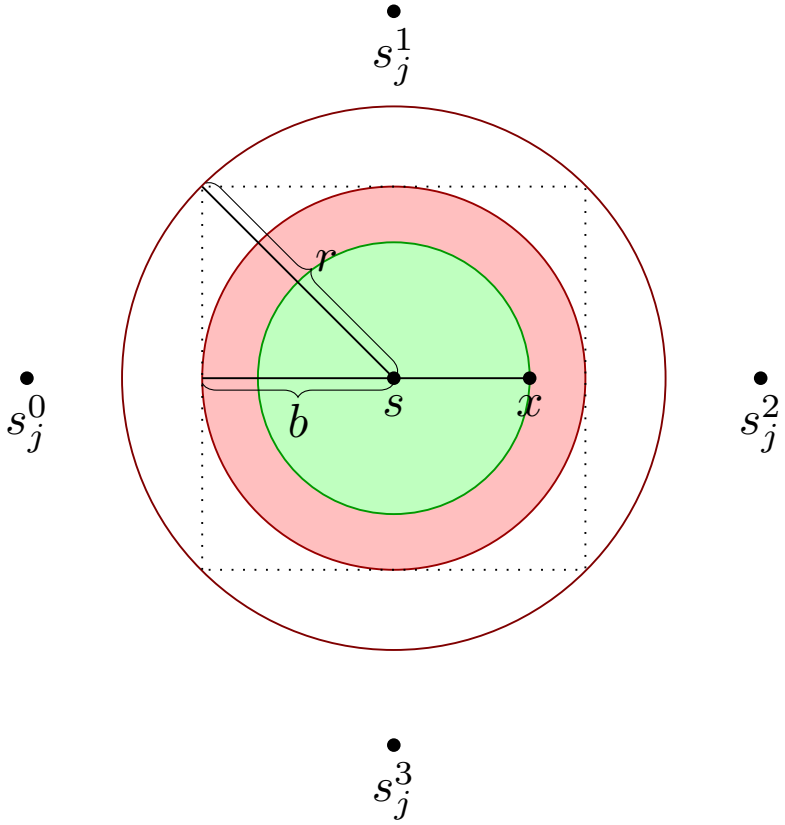


Figure 4.5: A single broadcasting station s surrounded by multiple jamming stations.

Since $d(s_j, s) = b\left(1 + \beta^{\frac{1}{\alpha}}\right)$ it can be transformed to:

$$(ab)^{-\alpha} \geqslant \beta N + \beta n \left(d(s_j, s) - ab\right)^{-\alpha} = \beta N + \beta n b^{-\alpha} \left(1 + \sqrt[\alpha]{\beta} - a\right)^{-\alpha} .$$

Realize that the maximal possible value of $a = 1$ maximizes the right-hand side of the inequality (with respect to a).Therefore, the component $(1 + \sqrt[\alpha]{\beta} - a)^{-\alpha}$ can be reduced, and the following inequality remains valid:

$$(ab)^{-\alpha} \geqslant \beta N + \beta n b^{-\alpha} (1 + \sqrt[\alpha]{\beta} - 1)^{-\alpha} = \beta N + n b^{-\alpha} .$$

Finally, the result is:

$$a \leqslant \sqrt[\alpha]{\beta N b^{\alpha} + n} .$$

By using the maximal possible value of a, the size of the maximal disk inscribed into the s reception zone can be calculated as $\pi(ab)^2$, finalizing the proof. □

4.2.4 Jamming for detached areas

Due to the complexity of the topic, it is only noted that methods presented in Section 4.2.1 can be adjusted for detached areas scenarios straightforwardly. For instance, for a circular detached restricted area, one might find the point closest to the protected station and tangent splitting the space into half-planes — one containing the whole restricted area — and use it for calculating the position of a jamming station similarly to Algorithm 3. A graphical example of this approach is presented in Figure 4.6, where points closest to s are found for three different detached areas. The described construction is performed, positioning one station per detached area. The detached areas jamming methods for non-uniform networks are presented in Section 4.3.

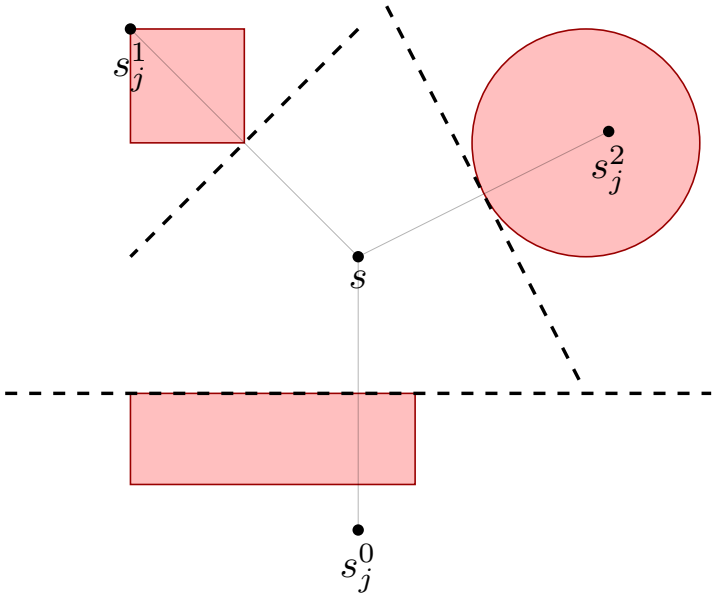


Figure 4.6: Detached model construction example with multiple restricted areas.

4.3 Extending noisy dust to 2D

This section analyzes non-uniform networks, wherein reception zones can be concave, increasing the analytic complexity. The main focus is on the arrangement of a network with a single station s with power $P(s) = P$ for which the *noisy dust* approach will be applied to protect the restricted area by *flooding* it, using numerous jamming stations with a small power $P_j \ll P$. The preliminary analysis of the space, where a single jamming station can effectively block another station's signal, is presented in Section 4.3.1. The approximation of this space by a hexagon is shown in Section 4.3.2, and a complete noisy dust algorithm is described in Section 4.3.3.

4.3.1 Effective jamming range of a single station

Consider a single station $s = (0, 0)$ with a power $P(s) = 1$ and a *border point* $b = (b_x, 0)$ such that $0 < b_x <$ range(s). Define a function:

$$F_j = (P_j\beta)^{\frac{1}{\alpha}} \ .$$

For $r = b_x F_j$, place a jamming station:

$$s_j = (b_x(1 + F_j), 0) \ .$$

From now on, it is tacitly assumed that $P(s_j) = P_j$. The present arrangement can be compared with Section 3.5 and is depicted in Figure 4.7. Note that $F_j < 1$ is required, so $\alpha \geqslant 2$ and $P_j < \beta^{-1}$. It also corresponds to the earlier mentioned property $P_j \ll P$. Clearly, like in the 1D case, the segment $\overline{(b_x, s_j)}$ is jammed. The disk $\mathcal{B}(s_j, r)$ could be used as an initial approximation of a space, where a single disturbing station can effectively jam the signal emitted by s. However, it would be imprecise if compared with the real effective jamming space (see Figure 4.8).

In the SIR model, the shape of a space, where s_j blocks the signal of s, would be expected to form an oval, irregular shape. Surprisingly, it forms a circle centered at:

$$c_j = \left(b_x + \frac{d(s, b)}{F_j^{-1} - 1}, 0\right) \ .$$

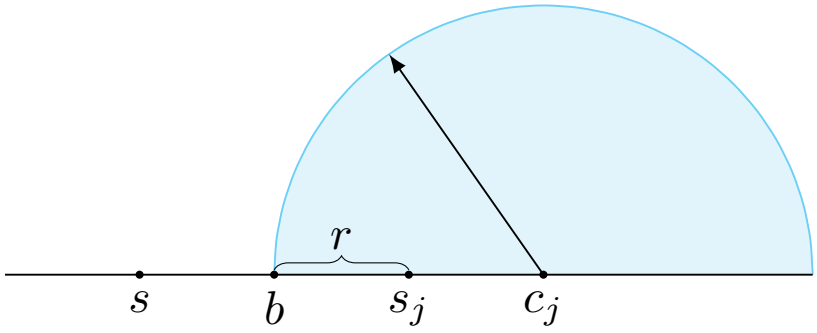


Figure 4.7: The top half of an area where a single jamming station can effectively block the signal of s (depicted as a half of a disk centered at c_j, positioned with an offset from s_j; the bottom half is symmetrical).

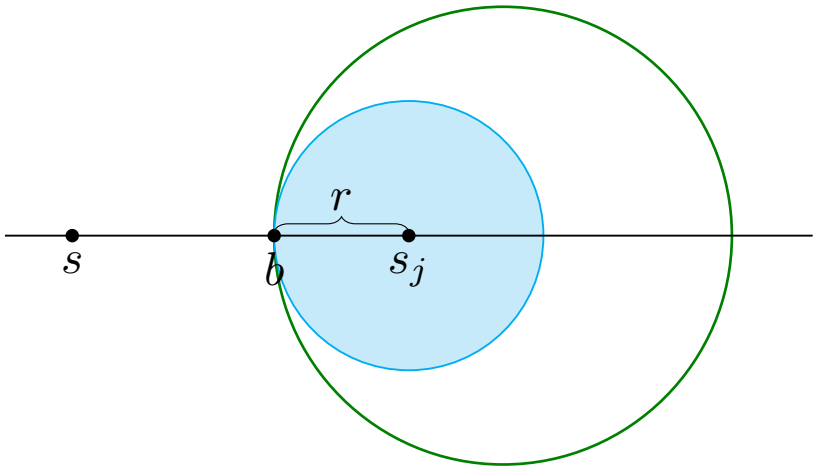


Figure 4.8: A single station's jamming range. A blue space denotes $\mathcal{B}(r, s_j)$. A green curve represents a boundary of the maximal region, where s_j correctly jams s.

Theorem 13. *For an initial network $\mathcal{A}$, the jamming network $\mathcal{J} = (S^{(J)} = \{s_j\}, P^{(J)} \equiv 1)$ correctly protects $\mathcal{R}_r^{en}(c_j)$, for:*

$$r = \frac{d(s,b)}{F_j^{-1} - 1} \ .$$

To the end of this subsection, the following combined network is assumed:

$$\mathcal{A}^{\mathcal{J}} = \langle D = 2, S = \{s, s_j\}, N, \beta, P, \alpha \rangle \ .$$

Points x forming the border of an area where the signal is blocked fulfill the equality $\mathrm{SIR}(s, x) = \beta$ (by continuity of SIR with respect to the tested position). The radial approach is used, i.e. create a vector $\overrightarrow{r_\gamma^*}$ ($\gamma \in [0, \pi]$ is an angle between the segment $\overline{ss_j}$ and the vector), such that:

$$x_\gamma^* = s_j + \overrightarrow{r_\gamma^*} \ , \qquad \mathrm{SIR}(s, x_\gamma^*) = \beta \ .$$

Note that SIR is monotonous in the direction of the vector, so there is precisely one appropriate x_γ^*. This method is presented in Lemma 16 with the construction depicted in Figure 4.9. Only half of the reception zone requires analysis, as the other half is symmetrical.

Lemma 16. *For a network $\mathcal{A}^{\mathcal{J}}$ and $\gamma \in [0, \pi]$, define a scalar:*

$$r_\gamma^* = d(s, s_j)((F_j^{-2} - \sin^2 \gamma)^{\frac{1}{2}} + \cos \gamma)^{-1} \ ,$$

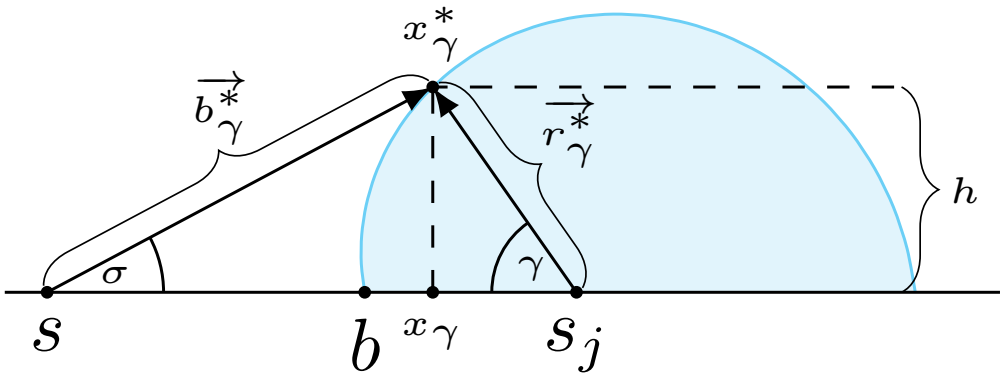


Figure 4.9: Construction of a radial based description of the $\mathcal{B}\left(\frac{d(s,b)}{F_j^{-1}-1}, c_j\right)$ space.

a vector:

$$\overrightarrow{r^*_\gamma} = \overrightarrow{(-r^*_\gamma \cos\gamma, r^*_\gamma \sin\gamma)}$$

and a point:

$$x^*_\gamma = s_j + \overrightarrow{r^*_\gamma} \ .$$

Then $\mathrm{SIR}(s, x^*_\gamma) = \beta$ *and* $\mathrm{SINR}(s, x^*_\gamma) \leqslant \beta$. *Moreover,* $\mathrm{SINR}(s, x) \leqslant \beta$ *for any point* $x \in \overline{s_j x^*_\gamma}$.

Proof. Define the base vector $\overrightarrow{r} = \overrightarrow{(b - s_j)}$. The vector $\overrightarrow{r^*_\gamma}$ is acquired by rotating $\overrightarrow{r}$ by an angle γ in a clockwise direction. Obviously, if $r^*_\gamma = \|\overrightarrow{r^*_\gamma}\|$, then:

$$\overrightarrow{r^*_\gamma} = \overrightarrow{(-r^*_\gamma \cos\gamma, r^*_\gamma \sin\gamma)} \ .$$

Define a new vector $\overrightarrow{b^*_\gamma} = \overrightarrow{x^*_\gamma - s}$ of a length b^*_γ and the angle between $\overrightarrow{b^*_\gamma}$ and $\overrightarrow{s_j - s}$ as σ (see Figure 4.9). Note that:

$$\sin\gamma = \frac{h}{r^*_\gamma} \ , \qquad \sin\sigma = \frac{h}{b^*_\gamma} \ , \qquad \frac{r^*_\gamma}{b^*_\gamma} = \frac{\sin\sigma}{\sin\gamma} \ .$$

The point x^*_γ has to keep the property $\mathrm{SIR}(s, x^*_\gamma) = \beta$, hence:

$$\frac{r^*_\gamma}{b^*_\gamma} = F_j = \frac{\sin\sigma}{\sin\gamma} \ . \tag{4.1}$$

By using the Pythagorean identity ($\sin^2\sigma = 1 - \cos^2\sigma$), it can be converted to:

$$\cos\sigma = \sqrt{1 - F_j^2 \sin^2\gamma} \ . \tag{4.2}$$

It can be easily obtained:

$$d(s, s_j) = b^*_\gamma \cos\sigma + r^*_\gamma \cos\gamma \ . \tag{4.3}$$

By applying Equation 4.1 and Equation 4.2 to Equation 4.3:

$$d(s, s_j) = \frac{r^*_\gamma \sqrt{1 - F_j^2 \sin^2\gamma}}{F_j} + r^*_\gamma \cos\gamma = r^*_\gamma \left(\sqrt{F_j^{-2} - \sin^2\gamma} + \cos\gamma\right) \ . \tag{4.4}$$

Finally, it results in the following:

$$r^*_\gamma = \frac{d(s, s_j)}{\sqrt{F_j^{-2} - \sin^2\gamma} + \cos\gamma} \ .$$

By properties of the construction it is guaranteed that $\mathrm{SIR}(s, x^*_\gamma) = \beta$ for any γ, so in particular $\mathrm{SINR}(s, x^*_\gamma) \leqslant \beta$. Since energy of s_j is decreasing, starting from the point s_j, in the direction of $\overrightarrow{r^*_\gamma}$, for any point $p \in \overline{x^*_\gamma s_j}$, it holds that $\mathrm{SINR}(s, x^*_\delta) \geqslant \mathrm{SINR}(s, p)$, making all such p correctly jammed. □

In the next step, the vector representation of $\overrightarrow{r^*_\gamma}$ has to be converted to a parametric one. In particular, the h component of $\overrightarrow{r^*_\gamma}$ can be based on the x_γ argument as $\overrightarrow{r^*_\gamma} = \overrightarrow{(x_\gamma, r^*(x))}$, via a function $r^*(x) = h$, where $x = d(b, x_\gamma) \in [0, d(b, x_\pi)]$. This transformation is presented in Lemma 17.

Lemma 17. *For every point x^*_γ ($\gamma \in [0, \pi]$), there exists x, such that:*

$$x^*_\gamma = (b_x + x, r^*(x)) \ ,$$

where:

$$r^*(x) = \left(-x^2 + \left(\frac{2d(s,b)}{F_j^{-1} - 1} \right) x \right)^{\frac{1}{2}}$$

and $b = (b_x, 0)$. Moreover, $\{x^*_\gamma : \gamma \in [0, \pi]\}$ forms a half of a circle.

Proof. Let $x^*_\gamma = (b_x + x, h)$, where $x \in [0, d(b, x_\pi)]$. The value of h from this formula depends on the γ angle as follows:

$$r^*_\gamma \cos\gamma = d(s_j, b) - x \ , \qquad r^*_\gamma \sin\gamma = \sqrt{\left(r^*_\gamma\right)^2 - (d(s_j, b) - x)^2} \ . \tag{4.5}$$

From Equation 4.4 it is known that:

$$d(s, s_j) = r^*_\gamma \sqrt{F_j^{-2} - \sin^2\gamma} + r^*_\gamma \cos\gamma \ .$$

Combining it with Equation 4.5 brings:

$$\begin{aligned} r^*_\gamma \sqrt{F_j^{-2} - \sin^2\gamma} = d(s, s_j) - d(s_j, b) + x = d(s, b) + x \ , \\ (d(s, b) + x)^2 = \left(r^*_\gamma\right)^2 (F_j^{-2} - 1) + (d(s_j, b) - x)^2 \ , \\ \left(r^*_\gamma\right)^2 = \frac{(d(s, b) + x)^2 - (d(s_j, b) - x)^2}{F_j^{-2} - 1} \ . \end{aligned}$$

The last of the above equations might have two real solutions for $\left(r^*_\gamma\right)^2$. However, only the positive one should be considered. Under assumptions $d(s, b) \geqslant d(s_j, b)$ and $F_j^{-2} - 1 > 0$, it satisfies:

$$r^*_\gamma = \sqrt{\frac{(d(s, b) + x)^2 - (d(s_j, b) - x)^2}{F_j^{-2} - 1}} \ .$$

Finally, this result can be used to calculate the parametrization $r^*(x) = r^*_\gamma \sin\gamma$ from the definition of $\overrightarrow{r^*_\gamma}$:

$$\begin{aligned} r^*(x) &= r^*_\gamma \sin\gamma \\ &= \sqrt{\left(r^*_\gamma\right)^2 - (d(s_j, b) - x)^2} \\ &= \sqrt{\frac{(b_x + x)^2 - (b_x F - x)^2 F_j^{-2}}{F_j^{-2} - 1}} \\ &= \sqrt{\frac{b_x^2 + 2xb_x + x - (b_x^2 - 2xb_x F_j^{-1} + x^2 F_j^{-2})}{F_j^{-2} - 1}} \\ &= \sqrt{-x^2 + \left(\frac{2b_x}{F_j^{-1} - 1} \right) x} \ . \end{aligned}$$

The last formula is a geometric mean of x and $\left(\frac{2b_x}{F_j^{-1}-1} - x\right)$, hence $\{x^*_\gamma : \gamma \in [0,\pi]\}$ is a half of a circle of diameter $\frac{2b_x}{F_j^{-1}-1}$. Therefore, the considered region is in fact $\mathcal{B}\left(\frac{d(s,b)}{F_j^{-1}-1}, c_j\right)$. □

Lemmas 16 and 17 conclude the proof of Theorem 13. Assume that the point b and radius of a circle $r = \frac{d(s,b)}{F_j^{-1}-1}$ are known in advance. Then the power level of station s_j can be calculated as:

$$P_j = \beta^{-1}\left(1 + \frac{d(s,b)}{r}\right)^{-\alpha} = \beta^{-1} r^\alpha d(s,c_j)^{-\alpha} \ . \tag{4.6}$$

In the following subsections, the predefined value of r is used, and each station has a fixed position, so Equation 4.6 can be utilized to assign power levels to these stations.

4.3.2 Space filling method

This part of the thesis is designated to fill the restricted area with small jammed regions. Assume that all regions are identical. The first candidate for a shape of such regions that comes to mind would be a disk. However, this idea does not allow the creation of an efficient and dense space tiling, so some of its approximations should be used. Therefore, a reasonable choice is a hexagonal tessellation. A regular hexagon is a neat approximation of a disk's shape. Theorem 13 reduces the jamming problem to filling the space with such hexagons. It is only required to decide on their sizes and position them densely. Then, for each cell formed by a hexagon, the position of a single jamming station has to be assigned, along with its power level, to guarantee that every hexagon's interior is correctly jammed. This arrangement is described in the form of Fact 3:

Fact 3. *Consider a network with a single station s and two points b, c_j such that:*

$$d(s,b) = (1-F_j)d(s,c_j), \qquad P_j = \beta^{-1} d(s,c_j)^{-\alpha} r^\alpha \ .$$

Let:

$$\overrightarrow{v} = \frac{\overrightarrow{(s-c_j)}}{\|\overrightarrow{s-c_j}\|}$$

and assume, that H is a hexagon inscribed into a circle centered at c_j with a circumradius r. Then, one can place a station s_j with a power P_j at the position:

$$s_j = c_j + (r - F_j d(s,b))\ \overrightarrow{v} \ .$$

For any point $x \in H$, the property $\mathrm{SINR}(s,x) \leqslant \beta$ *is satisfied, and in particular, for $N > 0$,* $\mathrm{SINR}(s,x) < \beta$.

Note that for $F_j < 1$:

$$d(s,c_j) = d(s,b) + \frac{d(s,b)}{F_j^{-1}-1} = \frac{d(s,b)}{1-F_j} \ .$$

Fact 3 directly follows from Theorem 13 and Equation 4.6, because the stated positioning and power assignment scheme of s_j guarantee that any point within the disk centered at c_j with a radius r is correctly jammed, and so are points from H. Details, how to fill a subset of space using hexagons heavily depends on the shape of such the set, so a generic algorithm is not presented in detail.

4.3.3 Noisy dust 2D algorithm

In this subsection, for a restricted area $\mathcal{R}$, the pre-constructed hexagonal grid $\mathcal{H}$ is present:

$$\mathcal{H} = \{h_0, h_1 \dots\} \ .$$

Its elements, h_i, are central points of equally sized, regular hexagons. Let $\mathrm{Hex}(h_i, r)$ be a hexagon with a center h_i and a circumradius r. For the sake of practicality, the grid $\mathcal{H}$ is assumed to be constructed from densely packed hexagons, and it fills the analyzed restricted area:

$$\mathcal{R} \subset \bigcup_i \mathrm{Hex}(h_i, r) \ .$$

Additionally, to reduce the complexity of the algorithm definition, it is assumed that all hexagons have an intersection point with a jammed station maximal reception zone (so there will be no hexagons without stations afterward). The main Algorithm 4 is defined for such a constructed hexagonal grid.

Algorithm 4: Create the noisy dust for $s = (0, 0)$, a restricted area $\mathcal{R}$ and a hexagonal grid $\mathcal{H}$ with a circumradii equal to r.

Algorithm `GenerateNoisyDust`$(s, \mathcal{H}, r)$
- $J \leftarrow \{\}$
- **for** $h \leftarrow \mathcal{H}$ **do**
  - $P_j \leftarrow \beta^{-1} d(s,h)^{-\alpha} r^{\alpha}$
  - $F_j \leftarrow (P_j \beta)^{1/\alpha}$
  - $s_j \leftarrow h + (r - F_j(d(s,h) - r)) \left(\frac{\overrightarrow{s-h}}{d(s,h)} \right)$
  - $J \leftarrow J \cup \{s_j, P_j\}$
- **return** J

Theorem 14. *For the network $\mathcal{A}$, the jamming network $\mathcal{J} =$* `GenerateNoisyDust`$(s, \mathcal{H}, r)$ *correctly protects the restricted area $\mathcal{R}$.*

Proof. Constructions from Section 4.3.1 and Section 4.3.2 correctly protect each hexagon from $\mathcal{H}$, in particular, that whole grid correctly protects $\mathcal{R}$. □

A schematic execution of Algorithm 4 is depicted in Figure 4.10. Figure 4.10a shows the initial problem — a single station with its range and a restricted area. In Figure 4.10b, a dense hexagonal grid is added to fill the entire restricted area within the range of the broadcasting station. Figure 4.10c presents a SINR range of the central station when jamming stations are arranged inside hexagons, and their powers are calculated according to Fact 3. The restricted area is correctly flooded with interference, and the impact on the original reception zone is limited, even when hexagons' radii are relatively big. Indeed, the coverage should improve considerably for smaller ones, which can be observed in Figure 4.10d.

Finally, the cost of Algorithm 4 can be analyzed. Let $A(r) = \frac{3\sqrt{3}r^2}{2}$ be the area of a hexagon with circumradius r.

Lemma 18. *For the network $\mathcal{A}$ let the jamming network $\mathcal{J} =$* `GenerateNoisyDust`$(s, \mathcal{H}, r)$*, use n jamming stations, approximately equal to:*

$$n \approx \frac{|\mathcal{R} \cap \mathcal{B}(\mathrm{range}(s), s)| + o(A(r))}{A(r)} \ .$$

Then the cost of this jamming network for $\alpha = 2$ is equal to:

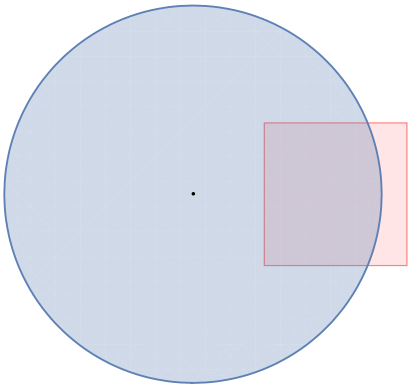
$$\mathrm{Cost}(\mathcal{J}) \equiv O(1) \ .$$

For $\alpha > 2$:

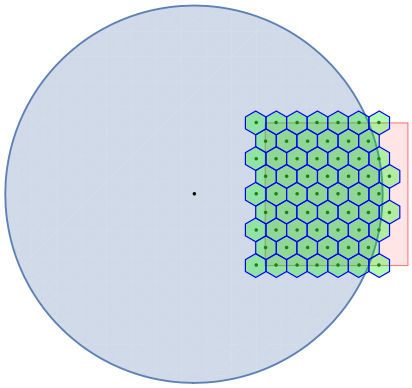
$$\mathrm{Cost}(\mathcal{J}) \xrightarrow{r \to 0^+} 0 \ .$$

Proof. Assume that parts of a restricted area located outside of the range of s are excluded, and the required number of hexagons of circumradii r, required to fill a restricted area $\mathcal{R}$, is defined as:

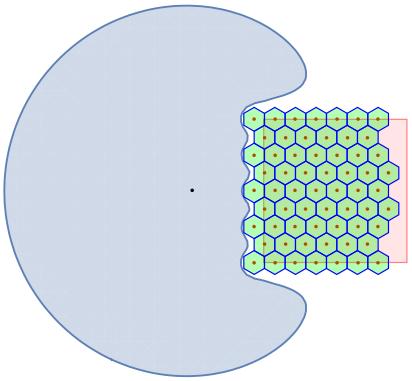
$$n = \frac{|\mathcal{R} \cap \mathcal{B}(\mathrm{range}(s), s)| + o(A(r))}{A(r)} \ .$$



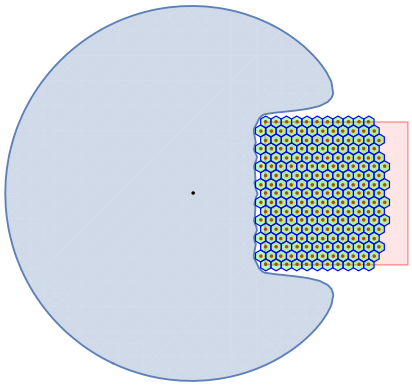
(a) An initial problem: the range of a broadcasting station is given as a blue disk, and the restricted area is depicted as a red rectangle.



(b) A hexagon grid is filling the restricted area.



(c) Jamming stations positioned with an offset from hex cells' centers.



(d) An example with reduced size of hexagons' cells. Notice, how reception zone *fits* better, reducing coverage.

Figure 4.10: An illustration of the 2D noisy dust algorithm. Black dot in the center is an initial station.

This assumption should be fulfilled in all realistic scenarios. The area of the restricted region $|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)|$ is a constant ($\mathcal{R}$ and s are given a priori). It is naturally bounded by the area of the initial disk around the broadcasting station in the SINR model:

$$|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)| \leqslant |\mathcal{B}(\text{range}(s), s)| \leqslant \pi \cdot \text{range}(s)^2 \ .$$

Cumulative energy required to set up jamming stations for an arbitrary $\mathcal{R}$ is given by:

$$\sum_{i=0}^{n-1} \beta^{-1} r^{\alpha} d(s, c_i)^{-\alpha} \ ,$$

where a circumradius of every single hexagon equals r, and each jamming station s_i is positioned in a unique hexagonal cell and vice versa. Each cell contains only one jamming station. Observe that one can limit the value of $d(s, c_i)$ by a distance between s and the closest single hexagon within the hexagonal grid — denote it by $d_s = \min\{d(s, c_j) : j =$

$1, 2, \ldots, n\}$. Since $d(s, c_i) \geqslant d_s$ for any hex cell:

$$\sum_{i=0}^{n-1} \beta^{-1} r^{\alpha} d(s, c_i)^{-\alpha} < \sum_{i=0}^{n-1} \beta^{-1} r^{\alpha} d_s^{-\alpha} = n\beta^{-1} r^{\alpha} d_s^{-\alpha} \approx \frac{|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)|}{A(r)} \beta^{-1} r^{\alpha} d_s^{-\alpha}$$
$$= \frac{2|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)|}{3\sqrt{3}\beta d_s^{\alpha}} r^{\alpha-2} ,$$

Remark that for $\alpha = 2$, this upper bound is constant:

$$\frac{2|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)|}{3\sqrt{3}\beta d_s^{\alpha}} .$$

Moreover, one can similarly find a lower bound of cumulative energy required to set up jamming stations by substitution of d_s by its antipodal counterpart $\max\{d(s, c_j) : j = 1, 2, \ldots, n\}$ (which is also bounded by $\text{range}(s) + r$) and realizing that:

$$n \geqslant \frac{|\mathcal{R} \cap \mathcal{B}(\text{range}(s), s)|}{A(r)} .$$

It shows that in this case (of $\alpha = 2$), the cumulative energy is $O(1)$ as $r \to 0^+$. On the other hand, for $\alpha > 2$, the upper bound converges to 0 as $r \to 0^+$, which upholds the zero-energy property from the 1D version of the noisy dust algorithm. When $\alpha < 2$, both upper and lower bounds are $O(r^{2-\alpha})$, as $r \to 0^+$, so in this case, the total energy usually rises along with the number of jamming stations. □

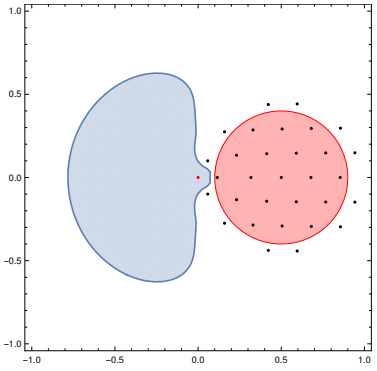
The actual coverage is checked experimentally. Four different scenarios are considered for the initial network configuration:

$$\mathcal{A} = \langle D = 2, S = \{s\}, N = 1.0, \beta = 1.0, P, \alpha = 3.0 \rangle .$$

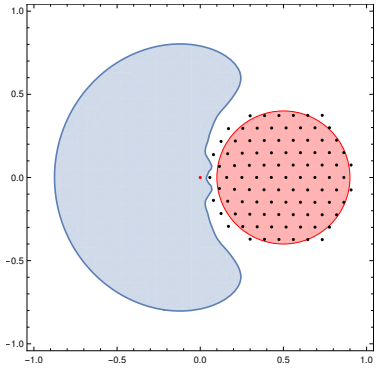
Each experiment is conducted for hexagons with radii:

$$r \in \{\ 0.125,\ 0.25,\ 0.5,\ 1\ \} .$$

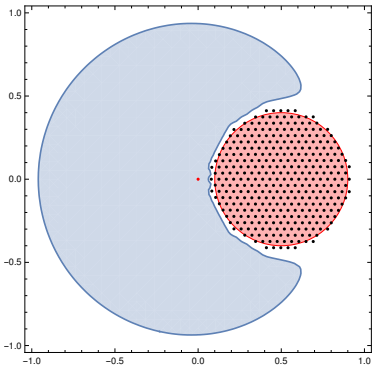
The first case, presented in Figure 4.11, shows the detached restricted area as a disk (s is red for distinction). In Figure 4.12, the detached restricted area forms a rectangle. In the third scenario (see Figure 4.13), the restricted area is represented by a half-plane, and finally, in Figure 4.14, we can find the enclosing restricted area with a disk shape. A summary of all the scenarios is presented in the coverage plot with respect to r in Figure 4.15. One can easily see that all cases hold the property that the coverage value increases as the sizes of hexagons decrease. The method might not work very well for smaller sizes of hexagons in some configurations (e.g., one presented in Figure 4.11), but generally, it is pretty efficient.



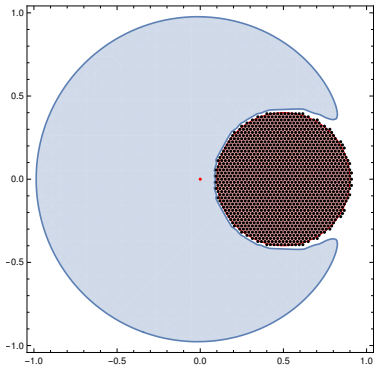
(a) $r = 0.1$



(b) $r = 0.05$

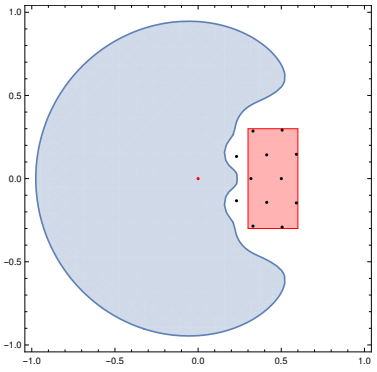


(c) $r = 0.025$

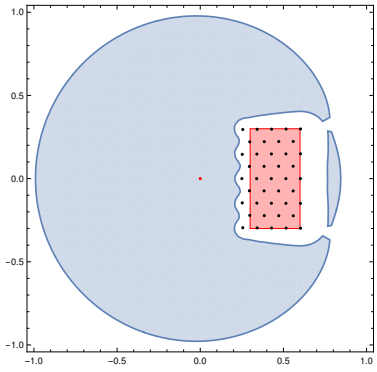


(d) $r = 0.0125$

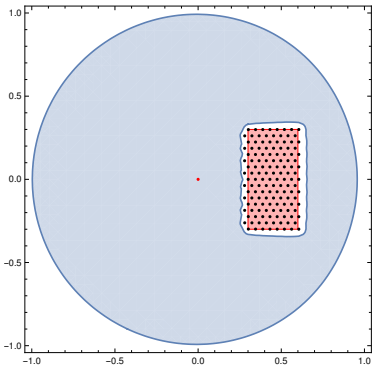
Figure 4.11: Example 1: detached disk restricted area.



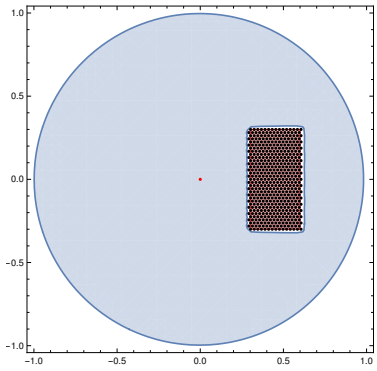
(a) $r = 0.1$



(b) $r = 0.05$

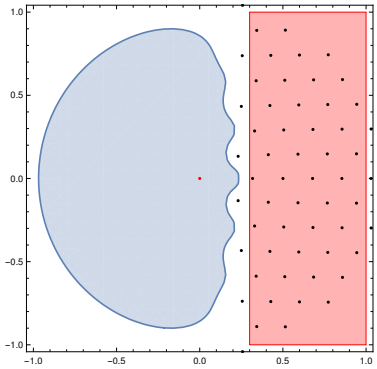


(c) $r = 0.025$

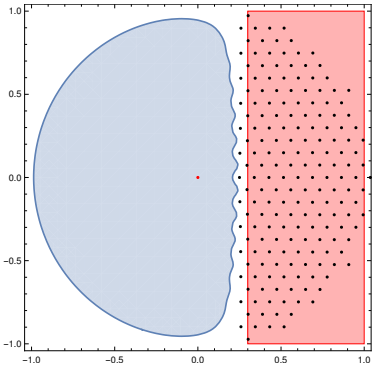


(d) $r = 0.0125$

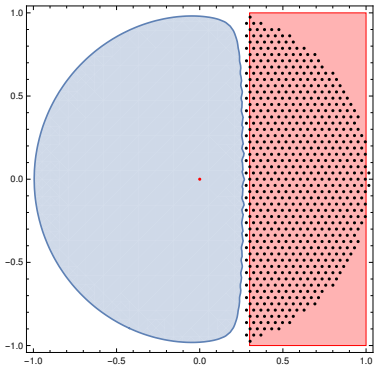
Figure 4.12: Example 2: detached rectangle.



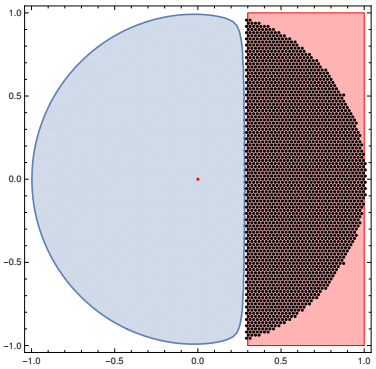
(a) $r = 0.1$



(b) $r = 0.05$

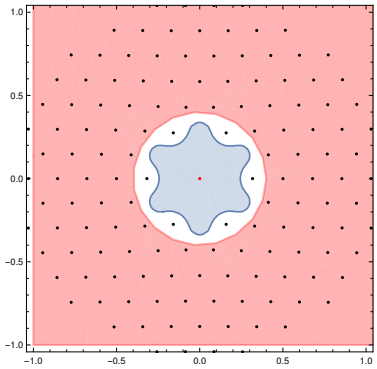


(c) $r = 0.025$

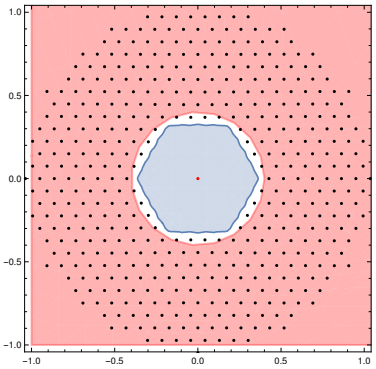


(d) $r = 0.0125$

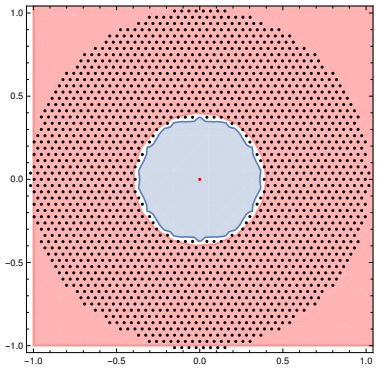
Figure 4.13: Example 3: half-plane detached restricted area.



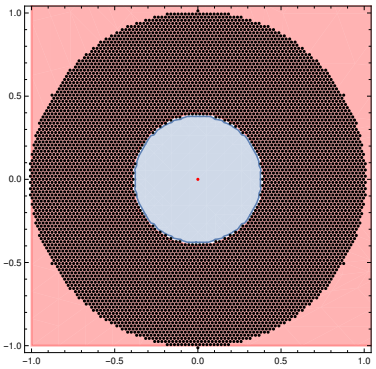
(a) $r = 0.1$



(b) $r = 0.05$



(c) $r = 0.025$



(d) $r = 0.0125$

Figure 4.14: Example 4: enclosing disk.

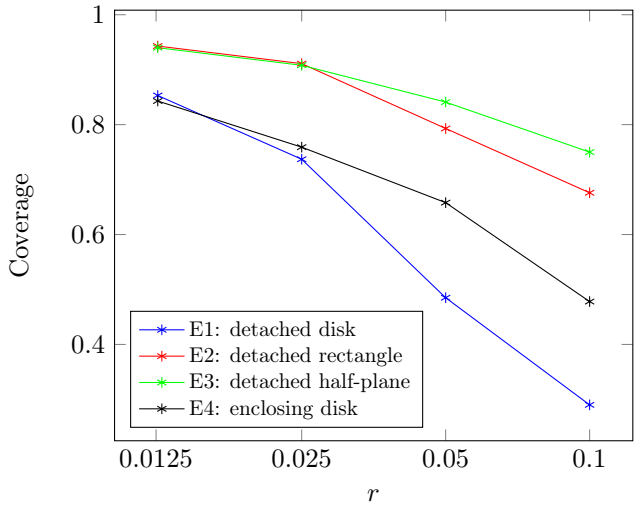


Figure 4.15: The coverage obtained for four considered examples with respect to the circumradius r of each hexagon in the grid.

Chapter 5

Size-hiding protocols in Beeping Model

This chapter will focus on different network models, namely the single-hop radio networks and the beeping model. The distinctive feature of the beeping model is its simplicity. It distinguishes only two channel states - no station is transmitting (silence), or at least one station is transmitting (beep). While it limits its capabilities in information sharing, it also allows straightforward and efficient implementations of this model. In wireless communication, it can be realized by simple bursts of a signal or energy, and the whole communication can be performed by carrier sensing [53, 54]. It can even be implemented by more primitive techniques, e.g., blinking lights. Additionally, algorithms implemented in a beeping model can usually be easily modified to work in more complex models, including ones with collision detection. In this model, the problems of counting [55], network size approximation [56], and minimal independent set [57] were analyzed, among others.

In Section 5.1, the formal model of the network will be presented, along with the definition of *size-hiding* property, which is based on the differential privacy and tries to formalize the property of keeping the size of the network hidden during the execution of algorithms. In Section 5.2, the universal algorithm will be presented, which allows hiding (to some extent) the size of the network of the underlying protocol. Finally, Section 5.3 demonstrates that some classic protocols are size-hiding by design and do not reveal much information about network size, even if a rigorous definition is used.

5.1 Formal Model

Consider a communication model with a single shared channel and n participating stations. The parameter n is unknown in advance to stations, or, possibly, some limited knowledge about n is available (e.g., a rough upper bound on n is given). Stations are anonymous, i.e., initially, they do not have any individual identifiers. Time is divided into separated and synchronized rounds, and all stations can determine the round of communication. In every round, stations can transmit or listen to the channel following the beeping model [54]. Depending on the number of transmitting stations in a given round, each station can recognize a present state amongst these in the set:

$$\mathcal{S} = \{Beep, Silence\} \ .$$

The state of the channel is as follows:

- *Beep* in a given round if and only if at least one station transmits,
- *Silence* otherwise.

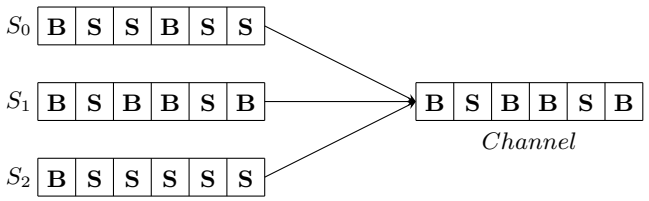


Figure 5.1: Beeping model example with three stations. *Beep* is denoted by **B** and *Silence* by **S**.

5.1.1 Adversary and security model

The outer *adversary* will be assumed, capable of observing the channel while some protocol $\mathcal{P}$ (e.g., initialization, leader election, or size approximation) is executed. Thus, its input can be described as some $\mathbf{s} \in \mathcal{S}^*$, i.e., a finite sequence of states of the channel[1]. Even if $\mathcal{P}$ is randomized, its distribution may depend on the number of participating stations n. The adversary is passive and is limited to eavesdropping on the communication channel. The adversary aims to gain additional knowledge about n, given the sequence of states $\bar{\mathbf{s}}$. In other words, the adversary may have some *a priori* knowledge about n before executing the protocol $\mathcal{P}$. However, his goal is to extend it by analyzing the observed execution. In contrast to previous work (e.g., [58, 59]), there is no assumption that the stations share any secret information, nor cryptographic key unknown to the adversary, that could be used to establish a secure communication channel inaccessible to the adversary. This assumption makes even passive adversaries very powerful, as they have the same information as any legitimate station. However, in the used model, the adversary has no access to local sources of the randomness of stations.

5.1.2 Size-hiding definition

Informally, the *size-hiding* property requires the protocols in similar-sized networks to result in (almost) indistinguishable channel states. Let $X_n^{\mathcal{P}} \in \mathcal{S}^*$ be a random variable denoting the states of the channel when executing the protocol $\mathcal{P}$ by exactly n stations. For the sake of clarity, a simplified notation will be used:

$$p_{n,\mathcal{P}}(x) := \Pr[X_n^{\mathcal{P}} = x] \ , \qquad p_{n,\mathcal{P}}(A) := \Pr[X_n^{\mathcal{P}} \in A] \ .$$

Moreover, whenever it is clear from the context, the name of the protocol will be skipped, using just $p_n(x)$.

Definition 14.1. *A protocol $\mathcal{P}$ is (d, ε, δ)-**size-hiding** when for any possible set of channel states $A \subset S^*$:*

$$p_{n,\mathcal{P}}(A) \leq \exp(\varepsilon) p_{m,\mathcal{P}}(A) + \delta \ , \tag{5.1}$$

for $n, m \in \mathbb{N}_+$ such that $|n - m| \leq d$.

This definition is extended by the auxiliary Lemma 19.

Lemma 19. *If there exist parameters ε, δ and a set A of channel states of protocol $\mathcal{P}$ that, for any n, m such that $|n - m| \leq d$:*

1. $\Pr[X_n^{\mathcal{P}} \notin A] \leq \delta$,
2. $(\forall\, x \in A)\ \Pr[X_n^{\mathcal{P}} = x] \leq \exp(\varepsilon) \Pr[X_m^{\mathcal{P}} = x]$,

then $\mathcal{P}$ is (d, ε, δ)-size-hiding.

[1] Note that $\mathcal{S}$ can represent different sets of states. It is not limited to a two-state beeping model.

The above lemma is analogous to the differential privacy property of probabilistic counters and can be found in [60]. Protocols with this property will yield similar results when performed by networks having similar sizes, resulting in the probability of distinguishing the network of size n from any network of size $[n-d, n+d]$ negligible if ε and δ are small. Sometimes, the definition is fulfilled only for n greater than some n_0. Informally, it can be said that it is more difficult to mask the difference between executions when comparing 2 with 22 stations than when comparing 102 with 122 stations.

Note that Definition 14.1 can be seen as a counterpart of the very popular *differential privacy* introduced in [26]. The main difference is that we use the parameter d instead of "neighboring" states. Also, one cannot directly apply methods for preserving privacy in a distributed system (e.g., like the Laplace mechanism in [61]) since we cannot "add" negative values while mimicking the nodes. Finally, the Fact 4 is presented to argue that only randomized protocols will be considered.

Fact 4. *For any non-trivial protocol to be size-hiding, it must be randomized.*

Clearly, if $\mathcal{P}$ is deterministic with respect to the size n, then $p_{n,\mathcal{P}}(x_n) = 1$ for a unique x_n. The deterministic protocol for a fixed network size generates a fixed sequence of channel states x_n. One can easily see that for any $\varepsilon \geq 0$, and any $n > 0$, the inequality 6.1 from the Definition 14.1 can be fulfilled for two consecutive sizes of networks n and $n+1$ only if $x_n = x_{n+1}$. Inductively, this reasoning can be extended for all $n > 0$. Thus, the Definition 14.1 can be fulfilled only if the algorithm returns trivially the same value for any size n.

5.1.3 Related literature

The beeping model is usually considered for single-hop networks [53, 62] and multi-hop networks [57, 54, 63, 64]. There is existing work on some common problems for different variants of the beeping model, like finding a maximal independent set [57], leader election [65] and broadcasting [66]. The problem related to this part of the thesis, approximating the network size, was studied in [62].

The *differential privacy*, which inspired the definition of *size-hiding* property, was described in [67]. Its application for the learning algorithms boosting method was analyzed in [68]. It was also considered for the protecting privacy of distributed systems scenarios in [69] and *Internet of Things* in [70, 71].

The problem of secure communication using the beeping model was studied in [72], along with the algorithm preserving the security. The privacy of communication in the single-hop MAC model for size approximating algorithms was analyzed in [73].

5.2 Universal Algorithm for Beeping Model

This section will present the universal algorithm, which can be used as a pre-processing for a broad class of algorithms. In a typical case, this approach moderately extends the execution time.

The presented approach is based on the following trick. Each station additionally mimics some random number of "virtual" stations (called *dummies*). This simple idea needs a precise calibration of parameters to be efficient. A careful analysis of security is presented below.

This approach is universal in that it can be applied to various algorithms as a separate subroutine[2]. In particular, the stations do not need any extra knowledge about the system and do not require any substantial changes in the executed code. A station "virtually" executes a code of a regular protocol for itself and in the name of dummies, so the number of mimicked stations is never zero. This approach does not require global knowledge and communication outside the shared channel.

[2]Note that it can be applied in many arrangements distinct from the beeping model as well.

On the other hand, one may need to notice some limitations of this approach: it can be applied only in the system, where a single station can imitate several stations. It can be realized in the *beeping model*, as described in Section 5.1. The station transmits if a given station or any dummy station is scheduled to be transmitted. Otherwise, it remains silent. Moreover, this approach can be applied to some restricted classes of problems.

Definition 14.2. *The randomized algorithm is* ***size determined*** *if its random output* Ξ *has the same distribution while executed for any network of size given a priori.*

Many fundamental problems considered in distributed systems are size determined, including size approximation, leader election, waking-up, and initialization/naming [74]. However, note that some natural problems are **not** size determined. One example is summing up all values kept by local stations.

Fact 5. *Let* $\mathcal{A}(n)$ *be a size-determined protocol executed by* n *stations. Moreover, let* T *be* (d, ε, δ)*-size-hiding protocol in values in* $\mathbb{N}$ *(independent of* $\mathcal{A}$*). Then* $\mathcal{A}(T)$ *is* (d, ε, δ)*-size-hiding.*

Proof. By the assumption about T, for any $n, m \in \mathbb{N}$ such that $|n - m| \leq d$, there is:

$$\Pr(T(n) \in \mathbb{N}) \leq \exp(\varepsilon) \Pr(T(m) \in \mathbb{N}) + \delta \ .$$

Thus, for any $l \in \mathbb{N}$, one can find values $\delta_{n,m,l} \geq 0$, such that:

$$\Pr(T(n) = l) \leq \exp(\varepsilon) \Pr(T(m) = l) + \delta_{n,m,l}$$

and:

$$\sum_{l \in \mathbb{N}} \delta_{n,m,l} = \delta \ .$$

Observe that:

$$\begin{aligned}
\Pr[\mathcal{A}(T)(n) \in S] &= \sum_{l \in \mathbb{N}} \Pr[\mathcal{A}(l) \in S] \Pr[T(n) = l] \\
&\leq \sum_{l \in \mathbb{N}} \Pr[\mathcal{A}(l) \in S] \left(\exp(\varepsilon) \Pr[T(m) = l] + \delta_{n,m,l}\right) \\
&\leq \exp(\varepsilon) \sum_{l \in \mathbb{N}} \Pr[\mathcal{A}(l) \in S] \Pr[T(m) = l] + \sum_{l \in \mathbb{N}} \delta_{n,m,l} \\
&= \exp(\varepsilon) \Pr[\mathcal{A}(T)(m) \in S] + \delta.
\end{aligned}$$

□

Note that this fact is a straightforward extension of the post-processing theorem for differential privacy (e.g., [67]) changed in two aspects. Technically, randomized algorithms $\mathcal{A}$ have to be considered, and the formulation has to be adapted to the modified definition.

How many dummy stations will a given real station mimic? As proved earlier, this number has to be randomized. There are n real stations. The i-th station mimics X_i virtual stations, wherein X_i, for all $i \in \{1, \ldots, n\}$, are independently and identically distributed according to some fixed distribution F. In result, the whole system mimics $T(n) = n + \sum_{i=1}^{n} X_i$ stations.

A crucial decision is to choose the distribution F. Intuitively, F with higher variance should have better size-hiding properties; however, it may extend the expected time of protocol execution compared to the original protocol and worsen the precision of size approximation.

Here, the *binomial strategy* BS is presented, depending on a parameter $p \in [0, 1)$, wherein each station chooses if it represents just itself (with probability $1-p$) or also mimics one extra station (plays two stations) with probability p[3]. In the case of BS Strategy, the total number of dummy stations has binomial distribution $\mathrm{Bin}(n, p)$.

[3]Note that many other natural strategies can be considered. Several of the most natural approaches have been considered, but surprisingly, they give similar results to BS, so the most elegant one has been picked.

5.2.1 Algorithm analysis

Before the main theorem presenting the algorithm size-hiding properties, the auxiliary Definition 14.3 and Lemma 20 will be presented:

Definition 14.3. *For $x \in \mathbb{R}$, $m \in \mathbb{N}$ and $h \in \mathbb{R}$, define a generalized shifted rising factorial*[4]*:*

$$[x]_m^{(h)} := \prod_{i=1}^{m}(x + ih) \ .$$

One can define a generalized shifted falling factorial as $(x)_m^{(h)} = [x]_m^{(-h)}$. We omit the upper index whenever $h = 1$.

Lemma 20. *If $|x - 1 \pm mh| < 1$, then:*

$$m(x-1) + h\binom{m+1}{2} - \frac{m(x-1)^2}{2} - h(x-1)\binom{m+1}{2} - \frac{h^2\binom{2m+2}{3}}{8} \leq \ln\left([x]_m^{(h)}\right) \leq m(x-1) + h\binom{m+1}{2} \ .$$

Proof. Note that:

$$\ln\left([x]_m^{(h)}\right) = \sum_{i=1}^{m} \ln(1 + (x-1) + ih) \ .$$

Moreover, for $|y| < 1$, by the application of Maclaurin series:

$$y - \frac{y^2}{2} \leq \ln(1+y) \leq y \ .$$

Therefore:

$$\sum_{i=1}^{m}(x-1) + ih - \frac{((x-1)+ih)^2}{2} \leq \ln\left([x]_m^{(h)}\right) \leq \sum_{i=1}^{m}(x-1) + ih \ .$$

Now, the thesis follows from two classical facts:

$$\sum_{i=1}^{m} i = \binom{m+1}{2} \ , \qquad \sum_{i=1}^{m} i^2 = \frac{m(m+1)(2m+1)}{6} = \frac{\binom{2m+2}{3}}{4} \ .$$

□

Theorem 15. *Let $T_{BS}(n)$ be the number of stations mimicked by n stations applying binomial strategy with parameter p. Let $\beta(n) < \frac{1}{2}$ be such that:*

$$[np(1-\beta(n)), np(1+\beta(n))] \cap \mathbb{N} \neq \emptyset$$

and:

$$d(n) \leq \min\left\{(1-\beta(n))np - 1, (1 - p(1+\beta(n)))\,\frac{n}{2} - \frac{1}{2}\right\}$$

for any considered size of the system n. Then $T_{BS}(n)$ is $(\varepsilon(n), \delta(n), d(n))$-size hiding, where

- $$\varepsilon(n) = \frac{d(n)(1+p)\beta(n)}{1-p} + d(n)\beta(n)^2 \max\left\{\frac{1}{2}, \frac{p^2}{(1-p)^2}\right\} + \frac{\binom{2d(n)+1}{2}}{n(1-p)}\left(1 + \frac{p\beta(n)}{1-p}\right) + \frac{\binom{d(n)+1}{2}}{np}(1 - p + \beta(n)) + \frac{d(n)\beta(n)}{n}\max\left\{\frac{1}{p}, \frac{2p}{(1-p)^2}\right\} + \frac{\binom{4d(n)+2}{3} + 8d(n)}{8n^2p^2(1-p)^2} \ ,$$

[4] An adjective "shifted" is due to a fact that product starts with $i = 1$ instead of $i = 0$ as it is usually defined (in both versions, the product has m factors). Also predominantly, $h > 0$, however we allow $h \leq 0$.

- $\delta(n) = 2e^{-2np^2\beta(n)^2}$.

Proof. Assume that $f(n)$ is a sequence in $\mathbb{N}^{\mathbb{N}}$ and $f(n) \leqslant d(n)$. Further, f will be used instead of $f(n)$ for convenience. One can see that:

$$\Pr(T_{BS}(n) = n + k) = \binom{n}{k} p^k (1-p)^{n-k} \ ,$$

so:

$$\Pr(T_{BS}(n \pm f) = n + k) = \binom{n \pm f}{k \mp f} p^{k \mp f} (1-p)^{n-k \pm 2f} \ .$$

The $u_{\pm}$ will be used as the following quotient of probabilities:

$$u_{\pm} := \frac{\Pr(T_{BS}(n) = n + k)}{\Pr(T_{BS}(n \pm f) = n + k)} = \frac{n!(k \mp f)!(n - k \pm 2f)! p^{\pm f}}{k!(n-k)!(n \pm f)!(1-p)^{\pm 2f}} \ . \tag{5.2}$$

Note that $\mathbb{E}\left(T_{BS}(n)\right) = n + np$. Therefore, the form of k of interest here is $np(1 + b(n))$, where $|b(n)| \leq \beta(n)$ (roughly speaking, consider the quotient only for the points in the vicinity of the mean). Analyze the "plus sign" case of (5.2) first, using generalized shifted factorials:

$$\begin{aligned} u_+ &= \frac{[n-k]_{2f} p^f}{[n]_f (k+1)_f (1-p)^{2f}} = \frac{[n - np(1+b(n))]_{2f} p^f}{[n]_f (np(1+b(n)) + 1)_f (1-p)^{2f}} \\ &= \frac{[1 - p(1+b(n))]_{2f}^{(\frac{1}{n})}}{[1]_f^{(\frac{1}{n})} [1 + b(n) + \frac{1}{np}]_f^{(-\frac{1}{np})} (1-p)^{2f}} = \frac{[1 - \frac{pb(n)}{1-p}]_{2f}^{(\frac{1}{n(1-p)})}}{[1]_f^{(\frac{1}{n})} [1 + b(n) + \frac{1}{np}]_f^{(-\frac{1}{np})}} \ . \end{aligned}$$

Dually, one can get similar:

$$u_- = \frac{(n+1)_f [k]_f (1-p)^{2f}}{(n-k+1)_{2f} p^f} = \frac{[1 + \frac{1}{n}]_f^{(-\frac{1}{n})} [1 + b(n)]_f^{(\frac{1}{np})}}{[1 - \frac{pb}{1-p} + \frac{1}{n(1-p)}]_{2f}^{(-\frac{1}{n(1-p)})}} \ .$$

By Lemma 19, realize that ε parameter is related to the upper bounds of $|\ln(u_{\pm})|$. Namely, if:

$$(\forall\, n \in \mathbb{N})(\exists\, A(n) \in \mathcal{P}(\mathbb{N}))(\forall\, k \in A)\ |\ln(u_{\pm}(n,k))| \leq \varepsilon(n) \ ,$$

then the 2nd condition of Lemma 19 is satisfied. Here is the discrete interval:

$$[np(1 - \beta(n)), np(1 + \beta(n))] \cap \mathbb{N}$$

plays a role of the set $A(n)$. At this point, realize that the need for constraint on $d(n)$ in the formulation of Theorem 15 is dictated by the assumptions of Lemma 20. The aforementioned upper bounds will be carefully analyzed by utilizing Lemma 20 as follows:

$$\begin{aligned} \ln(u_+) &\leq \left(-\frac{2fpb(n)}{1-p} + \frac{\binom{2f+1}{2}}{n(1-p)} \right) - \frac{\binom{f+1}{2}}{n} - \left(f\left(b(n) + \frac{1}{np} \right) - \frac{\binom{f+1}{2}}{np} \right) \\ &+ \frac{\binom{2f+2}{3}}{8n^2} + \left(\frac{f\left(b(n) + \frac{1}{np} \right)^2}{2} - \frac{\left(b(n) + \frac{1}{np} \right)\binom{f+1}{2}}{np} + \frac{\binom{2f+2}{3}}{8n^2p^2} \right) \\ &\leq \frac{d(n)(1+p)\beta(n)}{1-p} + \frac{d(n)\beta(n)^2}{2} + \frac{\binom{2d(n)+1}{2}}{n(1-p)} + \frac{\binom{d(n)+1}{2}(1-p)}{np} \\ &+ \frac{\binom{d(n)+1}{2}\beta(n)}{np} + \frac{d(n)\beta(n)}{np} + \frac{\binom{2d(n)+2}{3}(1+p^2) + 4d(n)}{8n^2p^2} \ . \end{aligned}$$

Remark that the inequalities $0 \leq f(n) \leq d(n)$ and $|b(n)| \leq \beta(n)$ were tacitly used in the latter transformation. Analogously, it can be attained:

$$\begin{aligned}
\ln(u_-) &\leq \left(\frac{f}{n} - \frac{\binom{f+1}{2}}{n}\right) + \left(fb(n) + \frac{\binom{f+1}{2}}{np}\right) \\
&- \left(2f\left(\frac{-pb(n)}{1-p} + \frac{1}{n(1-p)}\right) - \frac{\binom{2f+1}{2}}{n(1-p)}\right) \\
&+ \left(f\left(\frac{-pb(n)}{1-p} + \frac{1}{n(1-p)}\right)^2 - \frac{\binom{f+1}{2}\left(\frac{-pb(n)}{1-p} + \frac{1}{n(1-p)}\right)}{n(1-p)} + \frac{\binom{4f+2}{3}}{8n^2(1-p)^2}\right) \\
&\leq \frac{d(n)(1+p)\beta(n)}{1-p} + \frac{d(n)p^2\beta(n)^2}{(1-p)^2} + \frac{\binom{2d(n)+1}{2}}{n(1-p)} + \frac{\binom{d(n)+1}{2}(1-p)}{np} \\
&+ \frac{\binom{2d(n)+1}{2}p\beta(n)}{n(1-p)^2} + \frac{d(n)}{n} + \frac{2d(n)p\beta(n)}{n(1-p)^2} + \frac{\binom{4d(n)+2}{3} + 8d(n)}{8n^2(1-p)^2} \ ,
\end{aligned}$$

with a similar upper bound. However, the lower bounds are also of interest here, so one can carefully use the same tricks and obtain the following:

$$\begin{aligned}
\ln(u_+) &\geq \left(-\frac{2fpb(n)}{1-p} + \frac{\binom{2f+1}{2}}{n(1-p)}\right) - \frac{\binom{f+1}{2}}{n} - \left(f\left(b(n) + \frac{1}{np}\right) - \frac{\binom{f+1}{2}}{np}\right) \\
&- \left(\frac{fp^2b(n)^2}{(1-p)^2} - \frac{\binom{2f+1}{2}pb(n)}{n(1-p)^2} + \frac{\binom{4f+2}{3}}{8n^2(1-p)^2}\right) \\
&\geq -\frac{d(n)(1+p)\beta(n)}{1-p} - \frac{d(n)p^2\beta(n)^2}{(1-p)^2} - \frac{d(n)}{np} - \frac{\binom{2d(n)+1}{2}p\beta(n)}{n(1-p)^2} \\
&- \frac{\binom{4d(n)+2}{3}}{8n^2(1-p)^2} \ , \\
\ln(u_-) &\geq -\frac{d(n)(1+p)\beta(n)}{1-p} - \frac{d(n)\beta(n)^2}{2} - \frac{2d(n)}{n(1-p)} \\
&- \frac{\binom{d(n)+1}{2}\beta(n)}{np} - \frac{\binom{2d(n)+2}{3}(1+p^2) + 4d(n)p^2}{8n^2p^2} \ .
\end{aligned}$$

In the end, by Hoeffding's inequality:

$$\Pr\left[|T_{BS}(n) - n(1+p)| \geqslant \beta(n)np\right] \leq 2\exp\left\{-2\beta(n)^2np^2\right\} \ . \tag{5.3}$$

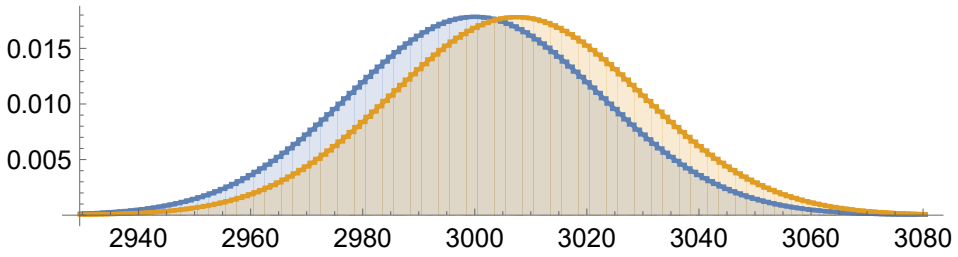
By Lemma 19, inequality (5.3) and the bunch of inequalities for $|\ln(u_\pm)|$, it emerges that:

$$\delta(n) = 2\exp\left\{-2\beta(n)^2np^2\right\}$$

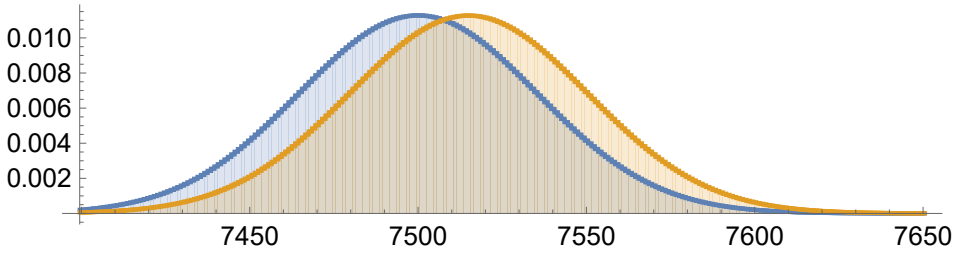
and:

$$\begin{aligned}
\varepsilon(n) &= \frac{d(n)(1+p)\beta(n)}{1-p} + d(n)\beta(n)\max\left\{\frac{1}{2}, \frac{p^2}{(1-p)^2}\right\} \\
&+ \frac{\binom{2d(n)+1}{2}}{n(1-p)}\left(1 + \frac{p\beta(n)}{1-p}\right) + \frac{\binom{d(n)+1}{2}}{np}(1-p+\beta(n)) \\
&+ \frac{d(n)\beta(n)}{n}\max\left\{\frac{1}{p}, \frac{2p}{(1-p)^2}\right\} + \frac{\binom{4d(n)+2}{3} + 8d(n)}{8n^2p^2(1-p)^2} \ ,
\end{aligned}$$

in order to attain $(\varepsilon(n), \delta(n), d(n))$-size-hiding property of the universal protocol. □



(a) $n = 2000$ and $n = 2006$ with $p = 1/2$.



(b) $n = 5000$ and $n = 5010$ with $p = 1/2$.

Figure 5.2: Examples of distributions for different stations with BS strategy. In the case of a relatively small difference in the number of stations (parameter n), the behaviors of networks are practically indistinguishable.

5.2.2 Algorithm applications

Theorem 15 is very general and can be used in various scenarios offering various trade-offs between the hiding range d and security hiding quality parameters (ϵ, δ) . Three of them are presented below.

Corollary 2. *Fix $p \in (0,1)$. Let:*

$$f_1(p) := \frac{1+p}{1-p} + \max\left\{\frac{1}{2}, \frac{p^2}{(1-p)^2}\right\}$$

and:

$$f_2(p) := \frac{2}{1-p} + \frac{1-p}{2p} \ .$$

Then there exists $n_0(p)$ such that, for any $n > n_0(p)$, $T_{BS}(n)$ is:

1. $\left(\varepsilon(n) = f_1(p) + \frac{f_2(p)}{(\ln(n))^2} + O\left(\frac{1}{\sqrt{n}\ln(n)}\right), \delta(n) = \frac{2}{n^{2p^2\ln(n)}}, d(n) = \frac{\sqrt{n}}{\ln(n)}\right)$*-size hiding,*
2. $\left(\varepsilon(n) = \frac{f_1(p)}{p\sqrt{\ln(n)}} + \frac{f_2(p)}{(\ln(n))^2} + O\left(\frac{1}{\sqrt{n}\ln(n)}\right), \delta(n) = 2n^{-2}, d(n) = \frac{\sqrt{n}}{\ln(n)}\right)$*-size hiding,*
3. $\left(\varepsilon(n) = \frac{f_1(p)}{p\sqrt[15]{n}} + \frac{f_2(p)}{\sqrt[3]{n}} + O\left(n^{-2/3}\right), \delta(n) = 2\exp(-2\sqrt[5]{n}), d(n) = \sqrt[3]{n}\right)$*-size hiding.*

These results are obtained from Theorem 15 by substituting the pointed $d(n)$ and $\beta(n)$ equal respectively $\frac{\ln(n)}{\sqrt{n}}$, $\frac{1}{p}\sqrt{\frac{\ln(n)}{n}}$ and $\frac{1}{pn^{2/5}}$. Note that the $n_0(p)$ should be chosen in such a way that the assumptions of Theorem 15 are true, concerning the chosen parameter $p \in (0,1)$ (for $n \leq n_0(p)$ one can modify $d(n)$ and $\beta(n)$ to satisfy the assumptions in order to apply the Theorem). Note that in the two latter cases of Corollary 2, both security parameters tend to 0. On the other hand, the bound $\varepsilon(n) = \Theta(1)$ is acceptable and commonly used in differential privacy literature. Therefore, the first mentioned system of parameters is appropriate, especially when p is relatively small (however, choosing very small p is not recommended because it occurs that then $f_2(p)$ may be uncomfortably big).

Remark that $\varepsilon(n) = \Theta(1)$ may be obtained from Theorem 15 whenever $d(n)\beta(n) = \Theta(1)$. Also, note that, if $\beta(n) = O\left(n^{-1/2}\right)$, then we can only attain $\delta(n) = \Omega(1)$ from Theorem 15.

The power of Theorem 15 is demonstrated under application for some classic results in the beeping model. The Binomial Strategy is applied as a pre-processing step before executing the algorithm.

Corollary 3. *There exists an explicit algorithm that returns $(1+\varepsilon)$ approximation of the network size in $O(\log\log n + \log f/\varepsilon^2)$ with probability at least $1 - 1/f$ that is*

$$\left(\varepsilon(n) = 1 + o(1), \delta(n) = O(\frac{1}{n^2}), d(n) = \frac{\sqrt{n}}{\log n}\right) \textit{-size hiding .}$$

This fact follows from [62] (Theorem 1). Note that in [56], the optimality for this class of protocols has been proved.

Corollary 4. *There exists an explicit algorithm that names n stations with running time $O(n \log n)$ that is correct with probability $1 - n^{-\alpha}$ and is*

$$\left(\varepsilon(n) = o(1), \delta(n) = o(1), d(n) = \sqrt[3]{n}\right) \textit{-size hiding .}$$

This fact follows from the analysis of the naming algorithm in [74]. From the energy-preserving perspective, a similar result appeared in [75].

In particular, the results listed below describe explicit algorithms as long as they extend explicit procedures. Note that the chosen decision about mimicking some extra station can be kept for any number of executions of any algorithm. This approach protects from information leakage and security decay when the adversary observes the system from a longer perspective. As a result, there is no need to apply any composition-like theorems (cf. [67]).

5.2.3 Limitations of the Universal Algorithm

The BS Strategy above can hide an exact number of stations with excellent security parameters and negligible execution overhead. The adversary cannot distinguish between n and $n \pm \sqrt{n}$ stations. It is a counterintuitive result since one may think that adding, say, a random number of virtual stations uniformly distributed from $\{1, 2, \ldots, n\}$ could improve the hiding effect and extend the approach for an arbitrary range of mimicked stations.

Fact 6. *Consider a strategy such that each station mimics independently X stations, where X has an expectation μ and variance σ. No such strategy can hide the number of stations for general n and $d = \omega(\sqrt{n})$.*

The sketch of the proof would be as follows. Consider two cases for n and N real stations ($N > n$). If, according to the algorithm, all stations mimic X other stations, the total number of mimicked stations would be close to $T_n \sim \mathcal{N}(n\mu, n\sigma^2)$ and $T_N \sim \mathcal{N}(N\mu, N\sigma^2)$ (Berry-Esseen-type theorem). One can easily see that $T(n)$ and $T(N)$ can be distinguished with probability greater than 0.97 if:

$$N\mu - 2\sqrt{N}\sigma > 2n\mu + \sqrt{n}\sigma \ .$$

The last relation is true even for n, N of moderate size.

5.3 Size Hiding in Regular Protocols

The approach presented in Section 5.2 has many merits - it is simple to implement and does not require any complex changes in the algorithm to which it is applied. However, it is limited with respect to the number of stations that can be hidden in networks of realistic sizes. Moreover, as demonstrated in the previous section, this type of approach cannot be

substantially improved when we insist on the assumption that the legitimate stations do not share any knowledge and execute the same code. One may suspect, however, that there are particular problems that can be solved using some size-hiding algorithm offering better properties, in particular higher d.

In this section, it will be demonstrated that the `GreenLeaderElection` protocol introduced in [29] by Jacquet et al. is size-hiding for parameter $d = \Theta(n)$ (comparing $d = O(\sqrt{n})$ for the universal algorithm) keeping parameters δ and ε reasonably small. Explaining in application terms, the adversary cannot distinguish between 1000 and 1300 stations, which is a substantial improvement compared to the previous approach. Moreover, it will be presented that there is no need to modify the original algorithm by Jacquet et al. to get the size-hiding property. Note that this is a similar case as *noiseless* privacy (cf. [76, 77]).

5.3.1 Green Leader Election algorithm description

The `GreenLeaderElection` algorithm consists of two phases. The aim of Phase I is to reduce the size of competing stations. In Phase I, stations transmit in consecutive slots with geometrically decreasing probability until there is silence on the channel. Only the stations transmitting in the last slot with a beep (i.e., *survivors*) participate in Phase II. Note that Phase II can be executed using any leader election protocol effectively since, with high probability, the number of survivors is minimal. This fact is proved in [78, 29]). Function $Geo(p)$ in Algorithm 5 generates random variable from a geometric distribution with parameter p.

Algorithm 5: Size-hiding leader election scheme for a single station.

```
Algorithm GreenLeaderElection(p)
    Phase I
        t ← Geo(p)
        for round ← 1, ..., t do
            Transmit()
        channel = GetChannelState()
        if channel ≡ Silence then
            status ← Candidate
        else
            status ← NotCandidate
    Phase II
        if status ≡ Candidate then
            LeaderElection()
```

5.3.2 Algorithm analysis

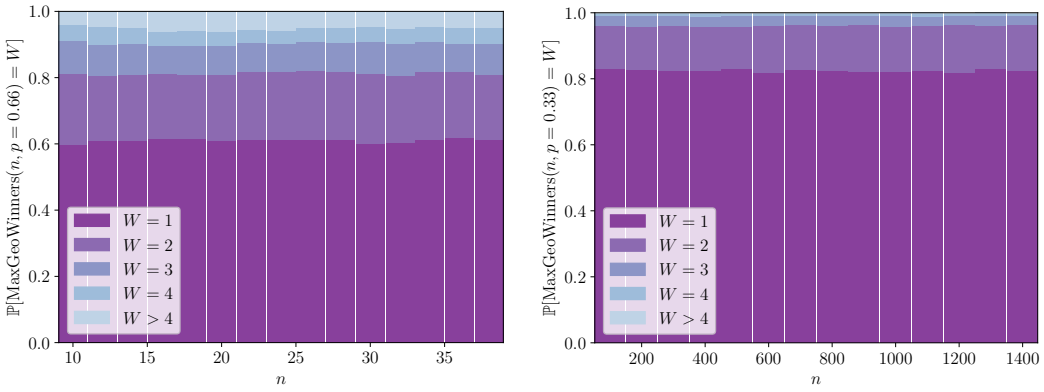
One can see that the information revealed to the adversary consists of the time of the Phase I execution T and the observable execution of the leader election for the limited subset of stations. The latter, however, is entirely determined by S, the number of stations that survived Phase I.

Let the pair (T_n, S_n) be the random variable observed by the adversary if the initial number of stations is n . The conclusion is based on two observations.

1. The expected length of the Phase I, T_n for n stations, is logarithmic with respect to the network size n, and it is difficult to distinguish even cases with n and $2n$ real stations.

2. Number of survivors S_n promoted to Phase II is almost independent of n and constant with a high probability.

While the first observation is relatively intuitive, the second is based on a careful analysis from [78, 29], wherein authors prove some other properties of this algorithm (mainly limited energy expenditure). This fact is depicted in Figure 5.3.



(a) $p = 2/3$, small networks.

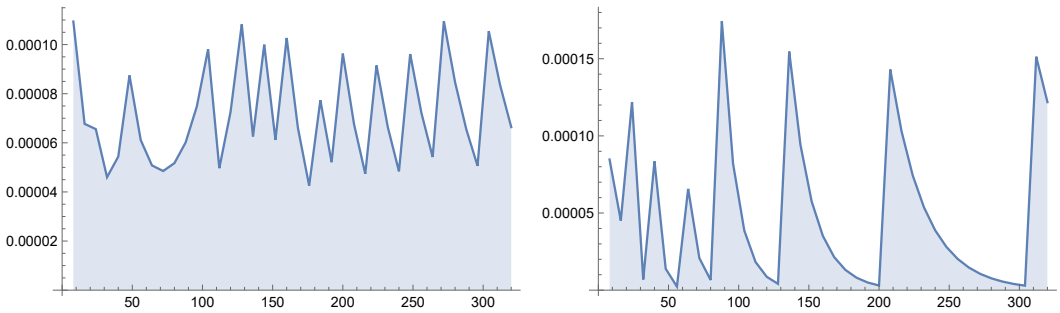
(b) $p = 1/3$, large networks.

Figure 5.3: Distribution of the number of stations participating in Phase II for various network sizes (parameter n). This distribution is almost independent of n (but depends on p).

Using the exact formulas from [78, 29] for distribution of S_n and a very straightforward analysis of T_n, it can be numerically checked that:

Fact 7. *`GreenLeaderElection` with paramer $p = 1/2$ with n devices guarantees $(\varepsilon, \delta, d(n))$-size hiding for $\varepsilon = 2, \delta = 0.0002$ and $d(n) = 0.25n$ and for $n > 10$.*

This presentation is limited to proving that the original algorithm hides a significant number of stations according to a rigorous definition. Note that its analysis can be subject to many extensions upon the needs of a particular scenario. In particular, accepting higher ε can make δ completely negligible. Moreover, one can easily prove that the same observable execution may occur for very different sizes exceeding 25% specified in Fact 7 with comparable probabilities. In effect, the adversary cannot be certain even about the order of magnitude of the network size.



(a) $p = 1/2, \varepsilon = 2$

(b) $p = 1/10, \varepsilon = 3$

Figure 5.4: Maximal parameter δ for n in the range $[5, 320]$ when $d = 0.25n$. Two examples with different parameters ε, p.

Chapter 6

Information hiding in multi-hop networks

In this chapter, similar to one presented in Chapter 5, the problem of hiding the properties of the network is analyzed, but from the perspective of synchronous multi-hop networks. The problem of a distributed algorithm execution is considered from the perspective of hiding some (meta) information from the curious observer (an adversary) who has access to some data sources related to the execution (feedback from the algorithm execution). The idea is presented in possibly high-level/abstract form, covering a wide range of distributed systems. The presentation will be focused on a multi-hop, synchronous ad hoc radio network, where an adversary can observe some transmissions and possibly partially know the network's topology. The motivation behind the information hiding for this type of system is straightforward: learning the details of the protocol execution may reveal some information about inputs for the executed distributed algorithm (e.g., the number of packets processed by individual stations), the type of algorithm that is executed or properties of the underlying network (e.g., number of stations in the network). Revealing such information can be highly undesirable, e.g., a group of robots collectively exploring some terrain shall not reveal too much about the algorithm they execute, e.g., in military applications.

We assume that the network is operating in a multi-hop model. There may be no direct communication between some pairs of devices, and communication between some pairs must be conducted by some relay. Such communication might also require some protection against eavesdropping - potential adversaries may infer some pieces of information about the topology of the network, having some details of protocol execution. For example, the total number of transmissions or the length of the execution of a given algorithm may be strongly correlated with the network's diameter. Moreover, in some cases, the details of the algorithm's execution allow the adversary to recover the exact topology. In the broad spectrum of considered adversarial-observer cases, we also consider the scenario wherein the adversary aims to learn the details of the executed algorithm (e.g., local inputs, type of algorithm) while the topology is known.

In contrast to previous work concentrated on single-hop radio networks, in multi-hop settings, we need to consider various network models and different capabilities of the adversary aiming at learning the details of the execution and the network itself. Moreover, the adversary's capabilities and possible countermeasures to hide some information strongly depend on the communication model. That is, replacing the plain beeping model from Chapter 6 with another communication channel (e.g. classic noCD) may result in dramatically different analysis and results even in the single-hop case.

This chapter presents only preliminary research pointing out how complicated and versatile are various cases of hiding information in multi-hop networks. Apart from the formal model, we present a taxonomy of different models from the perspective of information hiding and a few basic protocols for just a few models.

In the Section 6.1, some details of the formal model are presented. Section 6.2 is devoted

to the taxonomy of possible network settings and adversarial models. Section 6.3 presents some chosen algorithms.

6.1 Model

Describing a formal model for our problem is complex since we want to consider all essential details. First, the network needs to be described, including settings governing synchronization and the capabilities of nodes. Then, the communication model has to be described - how the information is transmitted using the communication channel. Finally, the security model has to be specified, in particular, the capabilities of the adversary. In particular, we need to specify the *feedback function*, i.e., what the adversary learns from the protocol's execution. Let us stress that the described systems can consider different feedback functions motivated by different real-life scenarios depending on the distributed system and the acting of the adversary.

6.1.1 Network model

The network is represented by undirected, connected graph $G = (V, E)$, where V will be a set of stations and $|V| = n$. Stations are connected by edges $\{v, u\} \in E$, where $u, v \in V$. When there is an edge between two stations, they can bidirectionally communicate with each other and receive/send some information through that links. Each station's $v \in V$ set of neighbors is denoted as $N(v) = \{u : \{u, v\} \in E\}$ and $N^+(v) = N(v) \cup \{v\}$. Let D be the diameter of the network.

6.1.2 Communication channel

Communication between stations will be synchronized by a global clock accessible for all stations and split into *slots*. In each slot, a station can transmit or listen. The transmission emitted by a station v reaches all neighbors of v, i.e., $N(v)$. The following communication channels are considered:

Beeping model (e.g. [54, 79, 80, 81]) - the signal is received by a station v if and only if at least one station from the set $N(v)$ is transmitting and v is in the listening mode. It is the simplest model, where each station v can recognize only two communication states: *Beep* if any station from $N^+(v)$ transmitted a message in this round and *Silence* when no station transmitted.

no-CD MAC (e.g. [82, 81]) In this model, each station v can detect two communication states: *Transmission* when exactly one station from $N^+(v)$ transmitted and *Noise* in any other case - including also the case when no station transmits - interfering signals cannot be discerned from an ambient noise.

CD MAC (e.g. [81]) This model allows station v to detect one of three states: *Transmission*, when precisely one station from $N^+(v)$ transmits, *Silence* if no station transmits and *Noise* in other cases. It is a model closer to modern wireless communication solutions, which allows differentiating between these states.

Direct Messaging (e.g. [83])

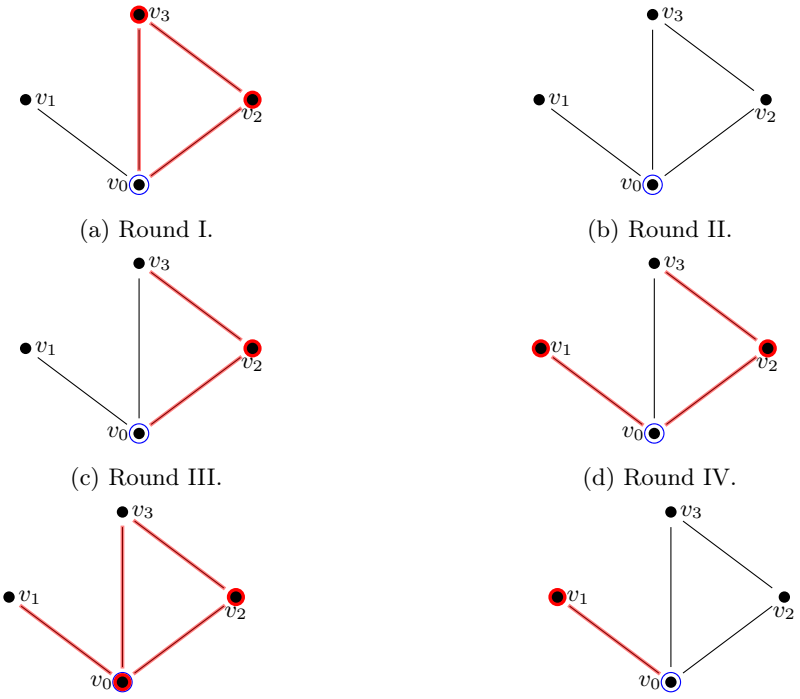
In this model, each station v can send direct messages to any station u if link $\{u, v\}$ exists in E, and each such station u can detect the message coming distinctively from node v. In particular, a station in a given round can receive a message from all its neighbors. No collisions occur in this model.

In the Beeping Model, the signal is assumed to represent a single bit (present or absent signal). In contrast, in the other models, one can assume that the messages are more

complex and contain many bits. That is, during a single slot with "Transmission," many bits can be transmitted [1].

Note that other, less popular models can also be possible and naturally motivated by some real-life networks (e.g., systems where the collision occurs starting from some threshold of the number of transmitting stations. Below this threshold, the channel capacity allows the correct delivery of all messages.

The example of several transmission rounds is presented in Figure 6.1. There are six rounds, and in each, different stations are transmitting. In Figure 6.2, the observable channel states from the station v_0 are presented for each of the described model types.



(a) Round I. (b) Round II.

(c) Round III. (d) Round IV.

(e) Round V. (f) Round VI.

Figure 6.1: Example of an algorithm execution in multi-hop network. Dots marked by red denote the transmitting stations, red lines mark *active* links, and the blue marked node v_0 is the analyzed receiver.

Round:	*I*	*II*	*III*	*IV*	*V*	*VI*
Beeping model	*Beep*	*Silence*	*Beep*	*Beep*	*None*	*Beep*
no-CD MAC	*Noise*	*Noise*	*Transmission*	*Noise*	*None*	*Transmission*
CD MAC	*Collision*	*Silence*	*Transmission*	*Collision*	*None*	*Transmission*
Direct Messaging	$m_{2,0}, m_{3,0}$	$\emptyset$	$m_{2,0}$	$m_{1,0}, m_{2,0}$	*None*	$m_{1,0}$

Figure 6.2: Description of channel states observable by station v_0 from Figure 6.1 at each round, for different channel types.

6.1.3 Adversary model

It can be imagined as some spying entity located close to the wireless network, capable of detecting limited information about the communication in the network. More precisely, in each round, the adversary gains some feedback from the network's communication. The

[1] Typically, it is assumed that the communication channel allows in a single slot to transmit at least a unique identifier of a station with $\Theta(\log n)$ bits, where n is the number of stations.

feedback is the value of a feedback function for a given state (transmissions of all stations) of the network in a given slot. A few types of adversaries will be analyzed, modeled as *feedback functions*.

1. **Beep detecting adversary** - in each round, the adversary can detect if at least one station is transmitting.
2. **Transmission counting adversary** - in each round, the adversary can detect how many stations are transmitting.
3. **Local adversary** - states of the local channels of a subset of stations are presented to the adversary.
4. **Full information adversary** - the adversary gains knowledge about all the communication (but does not know the content of the transmitted messages).

The information that the adversary received will be in the form of a stream $s \in \mathbb{N}^*$, e.g., stream $(1, 0, 2, 0, 1)$ will mean that in the first round, only one station transmitted, in second round none station transmitted, in third - two stations transmitted and so on. Obviously, in adversary model 1, it will be limited to $s \in \{0, 1\}^*$.

We present what different adversaries can see in Figure 6.3, given the algorithm's execution from Figure 6.1.

Round:	*I*	*II*	*III*	*IV*	*V*	*VI*
Beep detecting adversary	*Beep*	*Silence*	*Beep*	*Beep*	*Beep*	*Beep*
Transmission counting adversary	*2*	*0*	*1*	*2*	*2*	*1*

Figure 6.3: Different data acquired from rounds of execution presented in Figure 6.1 by different types of adversaries.

The **Full information adversary** detects the following information per each round of algorithm from Figure 6.1:

Round I: $m_{2,0}, m_{2,3}, m_{3,0}, m_{3,2}$.

Round II: $\emptyset$.

Round III: $m_{2,0}, m_{2,3}$.

Round IV: $m_{1,0}, m_{2,0}, m_{2,3}$.

Round V: $m_{0,1}, m_{0,2}, m_{0,3}, m_{2,0}, m_{2,3}$.

Round VI: $m_{1,0}$.

The model will be presented in a possibly general form. Thus, it is assumed that the adversary may have some prior knowledge about the executed protocol and the network itself. It can be modeled as a probability distribution. The adversary aims to enrich its knowledge using the feedback from the execution. Note the adversary may have no exact information about the network; however, given the feedback from the execution, some scenarios turned out to be significantly more probable. Indeed, the execution can make some scenarios (e.g., about the number of stations) a posteriori more or less probable, even without pointing to the exact one. This case can be a security threat and must be considered in the formal model.

6.1.4 Algorithm's evaluation

In analyzing the problem of information hiding, many fundamental issues with measuring the algorithm's quality and cost were encountered (understood as additional time and energy spent to obtain new properties). In some models, adding extra transmission rounds to hide the accurate execution is indefensible. Thus, completing the same task is more expensive in terms of communication as well as the total time of execution. Such an approach was presented in Chapter 5, where the universal algorithm for hiding the network size was introduced and was based on each station having a probability to simulate one additional station in the single-hop model. It was presented under the regime of *size-hiding* regime, which was based on the *differential privacy*, presented in [67].

Definition 15.1. *(hiding property) Let $f_{\mathcal{A}}$ be a feedback function with values in $\mathcal{Y}$ representing the knowledge of the adversary from all the slots of the algorithm's $\mathcal{A}$ execution. Let $\mathbb{A}$ be a set of possible algorithms (including their parameters), and let $\mathbb{N}$ be the set of all possible network parameters. Let $\Xi = \mathbb{A} \times \mathbb{N}$. Moreover, let (Ξ, d) be a metric space. We say that $\mathcal{A} \in \mathbb{A}$ is $(d, \Xi, l, \varepsilon, \delta)$-hiding when for any $S \subset \mathcal{Y}$:*

$$\Pr[f_{\mathcal{A}}(x) \in S] \leq \exp(\varepsilon) \Pr[f_{\mathcal{A}}(y) \in S] + \delta \tag{6.1}$$

for all $x, y \in \Xi$ such that $d(x, y) \leq l$.

Note that in the assumed model, the feedback function (possibly randomized) depends only on $x \in \Xi$. This definition is a generalized version of Definition 14.1, with $f_{\mathcal{A}}$ being the beeping function (1 if at least one station is transmitting, 0 otherwise), $\mathbb{N}$ being the set of all fully connected networks that can be identified with natural numbers. Moreover, the metric is $d = |n - m|$ for all $n, m \in \mathcal{N}$.

Except for the security (hiding) property, some other metrics need to be considered while evaluating the hiding method. Similarly to the bulk of previous papers on information hiding in distributed systems, in all suggested methods, our paper is somehow based on the redundancy of communication (adding some surplus actions to obfuscate the adversary's view). In effect, the obfuscated algorithm is somehow more expensive concerning the execution time and the energy necessary for completing the algorithm. The latter can be measured as a value proportional to the maximal number of transmissions over all stations participating in the protocol. This approach is motivated by two facts:

- listening is an order of magnitudes less energy consuming than transmitting;
- the system's lifetime is equal to the shortest life over all stations.

Let $\mathcal{E}(\mathcal{A}), \mathcal{T}(\mathcal{A})$ be an energy and a time of execution of an algorithm $\mathcal{A}$. By S_T, let us define all the algorithms completing a given task T. Moreover, let

$$\begin{aligned} e_T &= \inf_{\mathcal{A} \in S_T} \mathcal{E}(\mathcal{A}) \ . \\ t_T &= \inf_{\mathcal{A} \in S_T} \mathcal{T}(\mathcal{A}) \ , \end{aligned}$$

That is, e_T and t_T are optimal time and energy needed to complete a task T, respectively. Let $S_T^{*,\theta}$ be the set of algorithms for task T hiding the execution with respect to some model parameters θ (including $\delta, \varepsilon, d, l$) . Analogously we define

$$\begin{aligned} e_T^{*,\theta} &= \inf_{\mathcal{A} \in S_T^{*,\theta}} \mathcal{E}(\mathcal{A}) \ , \\ t_T^{*,\theta} &= \inf_{\mathcal{A} \in S_T^{*,\theta}} \mathcal{T}(\mathcal{A}) \ . \end{aligned}$$

As the *cost of hiding* w.r.t the time of execution is defined as $\frac{e_T^{*,\theta}}{e_T}$. Similarly $\frac{e_T^{*,\theta}}{e_T}$ is the *cost of hiding* w.r.t energy.

6.2 Taxonomy

Compared to the results from the paper Chapter 5, where a single-hop radio network was considered, the case of a multi-hop radio network (and similar distributed systems) is dramatically more complex. There are many substantially different (yet still natural) assumptions about the topology of the network and the way the stations communicate. Even more important is the power of the adversary modeled by the feedback function that describes what the adversary may observe in the run of the protocol. A full description of the adversary needs to cover the a priori knowledge of the adversary about the executed algorithm and topology. Moreover, we need to specify what the ultimate aim of the adversary is - what it wants to learn from the feedback function. In this section, we list the main categories for which the varying configurations can impact the algorithm design and evaluation.

Network topology
We assume that a graph with nodes representing stations describes the network topology. That is, the connection between any pair of nodes is symmetric. The signal transmitted by station x reacheches station y if and only if $\{x, y\}$ is an edge in the graph. Similarly, x gets the signal if y transmits. We assume that the graph is connected.

- Single-hop - the network is represented by a complete graph.
- Multi-hop - at least two nodes are not connected in the graph. That is, there are at least two non-connected stations x and y. In particular, to deliver a message between them, one needs to use a path of relay stations. In this case, delivering a message from x to y takes more than a single round.

Communication channel

- Beeping model.
- MAC with Collison Detection.
- MAC without Collison Detection.
- Direct messaging.

Local communication channels act as described in Section 6.1.2.

Station's topology awareness

- Stations know the topology of the network.
- Stations do not know the topology. It can be collectively recovered in the course of the algorithm.

Station's algorithm awareness

- Algorithm aware - stations know only its code executed locally.
- Algorithm knowledge restricted - stations know the code of all stations (in particular if it is the same for all stations). The local inputs, however, remain unknown.

Secret sharing

- Secret capable - from the beginning of the execution, all the stations share a secret unknown to the adversary. In particular, they can use a secret to encrypt the communication that the adversary cannot read.
- Open communication - at the beginning of the algorithm's execution, the stations do not share any secret.

Adversary's topology awareness

- Topology aware - the adversary knows the specified topology of the network.
- Topology knowledge restricted - the adversary has no or partial knowledge about the network's topology. In particular, the adversary may know that the network is a regular graph or contains, at most, some N nodes. We also allow to represent the knowledge of an adversary as a probability distribution over a set of graphs.

Adversary's algorithm awareness

- Algorithm aware - the adversary knows the exact algorithm executed by all stations; however, it does not know the inputs of the stations.
- The adversary has limited knowledge of the executed algorithm. In particular, the knowledge can be a distribution over a set of potential algorithms.

Adversary's feedback function
Different types of feedback functions are described in Section 6.1.3. We consider:

- beep detecting adversary,
- transmissions counting adversary,
- local adversary,
- full information adversary.

The preliminary research suggests that choosing the factors mentioned above leads to significantly different adversary capabilities. We also observed that, consequently, for each model, one needs to apply different defense strategies. One may consider some other factors influencing both the adversary's capabilities as well as possible countermeasures. We decided, however, to restrict our attention to the most important ones in order to keep the taxonomy practical.

6.3 Algorithms

This section presents a few elementary algorithms offering information-hiding properties for chosen models from the introduced taxonomy.

6.3.1 Naive Oblivious

This algorithm can be applied for a relatively weak **beeping model** of the feedback adversary and the strongest **direct messaging** as a communication model. Other parameters can be fixed arbitrarily. In particular, the algorithm does not assume any shared secret (**open communication** model). Moreover, the stations do not have to know topology and can have only local knowledge about the execution.

Description The Naive Oblivious algorithm $\mathcal{N}(\mathcal{A})$ is built on the top of any algorithm $\mathcal{A}$. We assume that messages sent by stations during the protocol are of equal size l, and stations know the upper bound on the execution length N. Naive Oblivious $\mathcal{N}(\mathcal{A})$ works as follows:

- If in the original protocol $\mathcal{A}$, in a round $1 \leq t \leq N$, station s_i sends a message $m^n_{s_i,s_j}$ to s_j, in the modified protocol in the round t in the protocol $\mathcal{N}(\mathcal{A})$ the station s_i sends to s_j a message $1 \| m^t_{s_i,s_j}$. That is, the same message is sent, however, with a prefix $'1'$.

- If in the round t the message is **not** sent in $\mathcal{A}$, in the $\mathcal{N}(\mathcal{A})$ the station s_i sends to s_j the *dummy* message of the length $l+1$ with zeros, only.

The original messages from $\mathcal{A}$ can be easily distinguished from dummies.

Analysis The analysis of security properties is obvious. One can see that the adversary can observe only a sequence of N beeps. That is, the protocol is totally oblivious. In effect, one gets $\varepsilon = \delta = 0$ as the security basic parameters for any properly defined d and Ξ. On the other hand, the stations taking advantage of the significantly more informative communication model can execute the $\mathcal{A}$.

Note that the assumption about the equal length of messages sent in the protocol can be easily bypassed using, e.g., standard padding.

6.3.2 Binomial Boxes Algorithm

The simplicity of the Naive, Oblivious algorithm was based on the fact that the adversary, having just beeping feedback, was much weaker compared to the regular stations in the network that could communicate simultaneously with all their neighbors. This section introduces the Binomial Boxes Algorithm (or BBA, for short) that can be applied to an adversary still having beeping feedback with constrained regular stations (beeping model or CD/no-CD MAC). The price of reducing the difference in capabilities of the adversary and the regular stations is the requirement that the stations need to share a common secret unknown to the adversary. Moreover, the execution of the algorithm is significantly larger in terms of time and energy and depends on the parameter determining the security level.

Descripion Each time slot of execution of a regular protocol $\mathcal{A}$ is represented by a box that consists of $n+1$ consecutive regular slots. In each box, a single *true slot* is chosen uniformly in a pseudo-random random manner. Other n slots are independently chosen as *beep dummy* or *silent dummy* with probability 1/2. The position of the true slot and decisions if the remaining slots are silent or beep dummies are to be determined by the shared secret[2]. Thus, the position of the true slot in a box and the kind of dummies are known for the stations sharing the secret but remain random for the adversary.

The execution of the protocol $\mathcal{BBA}(\mathcal{A})$ is as follows:

- In the true slot of the t-th box of $\mathcal{BBA}(\mathcal{A})$ all the stations execute the actions of the t-th slot of $\mathcal{A}$;
- In all beep dummy slots, all the stations transmit.
- In all silent dummy slots, all the stations remain silent.

Box	Box I			Box II			Box III			
Slot	0	1	**2**	**0**	1	2	0	**1**	2	Message
Station A	S	S	**S**	**S**	B	S	S	**S**	B	SSS
Station B	S	S	**S**	**B**	B	S	S	**B**	B	SBB
Station C	S	S	**B**	**S**	B	S	S	**S**	B	BSS
Station D	S	S	**B**	**B**	B	S	S	**S**	B	BBS

Figure 6.4: Example execution of $\mathcal{BBA}$ algorithm with three boxes and three slot each. The true slot is marked in bold. Notice how stations in other slots are using the same behavior.

[2]This can be done straightforwardly using a chain of one-way hash functions with the secret as a seed .

Analysis The correctness $\mathcal{BBA}(\mathcal{A})$ of the protocol is obvious. Since the stations neglect dummy slots, the execution of the true slots needs to give the same result[3] as $\mathcal{A}$.

More subtler analysis of information-hiding properties is needed. Let us observe that the adversary can only distinguish the slot with and without any transmitting station.

Let us call the box representing the slot with the transmission in the true slot a *beep box* and the remaining a *silent box*. Since the position of the true slot in each box is random from the perspective of the adversary, the only information the adversary can learn is the number of beep slots (including the true slot) in a given box. One can easily see that statistically, there is one more beep in the beep slot. Intuitively, the difference between the types of boxes vanishes with a growing parameter n. Formally, the number of beeping slots in the silent box is binomially distributed $T_S \sim \text{Bionmial}(n, 1/2)$, while in the case of beep box, we got $T_B \sim \text{Bionmial}(n, 1/2) + 1$. Let us recall the following version of the Chernoff bound.

Fact 8. *Let X be binomially distributed with parameters n and p. For any $\delta > 0$ and $\mu = np$ following holds:*

$$\Pr[|X - \mu| \geq \delta\mu] \leq 2\exp\left(-\frac{\delta^2\mu}{3}\right) .$$

This version of the Chernoff inequality is obtained by a simple union bound to unify cases with upper and lower bounds for binomial distribution (see, e.g., [84]). Let $\delta = 2\xi\frac{1}{\sqrt{n}}$ for some $\xi > 1$ being a security parameter. Applying directly δ to 8 to T_S we get:

$$\Pr\left[|T_S - \frac{n}{2}| > \xi\sqrt{n}\right] \leq 2\exp\left(-\frac{4}{6}\xi^2\right) < \exp\left(-\frac{\xi^2}{2}\right) .$$

It directly implies that:

$$\Pr\left[|T_B(-1) - \frac{n}{2}| > \xi\sqrt{n}\right] < \exp\left(-\frac{\xi^2}{2}\right) .$$

In effect values of T_B and T_S are in the interval $\mathbf{I} = \left[\frac{n}{2} - \xi\sqrt{n}, \frac{n}{2} + \xi\sqrt{n} + 1\right]$ with probability exceeding $1 - \exp\left(-\frac{\xi^2}{2}\right)$. For extreme values, it can be easy to distinguish if the result is from T_B or T_S. For example, having beeps in all $n + 1$ slots, it is evident that we deal with beep-box. We show, however, that all the values from $\mathbf{I}$ can appear in T_B or T_S almost with the same probabilities. Note that for any $2 \leq l \leq n$:

$$\frac{\Pr(T_S = l)}{\Pr(T_B = l)} = \frac{\Pr(T_S = l)}{\Pr(T_S = l - 1)} = \frac{\binom{n}{l}\frac{1}{2^n}}{\binom{n}{l-1}\frac{1}{2^n}} = \frac{n - l + 1}{l} := f(n, l) .$$

One can see that for $l \in \mathbf{I}$ we have:

$$f(n, l) \geq \frac{n - \left(\frac{n}{2} + \xi\sqrt{n} + 1\right) + 1}{\frac{n}{2} + \xi\sqrt{n} + 1} = 1 - \frac{2\xi\sqrt{n} + 1}{\frac{n}{2} + \xi\sqrt{n} + 1} \geq 1 - \frac{2\xi\sqrt{n} + 1}{\frac{n}{2}} \geq 1 - \frac{5\xi}{\sqrt{n}} .$$

In the same way, one can show that for $l \in \mathbf{I}$ we have:

$$f(n, l) \leq 1 + \frac{7\xi}{\sqrt{n}} .$$

Thus the ratio $|f(n, l)| \leq 1 + x$ for some $|x| = \Theta\left(\frac{\xi}{\sqrt{n}}\right)$ for all $l \in \mathbf{I}$. Since $\ln x = 1 + x + \Delta$ for some $|\Delta| < x^2$ if $x < 1$, we easily get that:

$$f(n, l) \leq \exp(\varepsilon)$$

[3]We do not formalize explicitly the results of the protocol, but it can be seen, for example, as the states of local memories of all stations.

for:

$$\varepsilon = \ln(|f(n,l)|) = \Theta\left(\frac{\xi}{\sqrt{n}}\right) .$$

Finally we need to recall that we proved that $l \in \mathbf{I}$ with probability at least $1 - \exp\left(\frac{\xi^2}{2}\right)$. As a consequence of the above considerations, one gets the following fact.

Fact 9. *Let $\mathbb{A}^{(k)}$ be a set of algorithms lasting exactly k rounds in the MAC communication channel[4]. For any $\mathcal{A} \in \mathbb{A}^{(k)}$ the algorithm $\mathcal{BBA}(\mathcal{A})$ with parameters $n > 0$ and $0 < \xi < 1$ is $(\Xi, d, l, \varepsilon, \delta)$-hiding for*

- $\varepsilon = \Theta\left(k \cdot \frac{\xi}{\sqrt{n}}\right)$,
- $\delta = \Theta\left(k \cdot \exp\left(-\frac{\xi^2}{2}\right)\right)$,
- $\Xi = \mathbb{A}^{(k)} \times \mathbf{N}$ *for any* $\mathbf{N}$,

any metric d and any number $l > 0$.

The parameters for $k = 1$ (a single-round algorithm) follow directly from the analysis described above. The case for $k > 1$ is a direct consequence of the composition theorem (see eg.[67]). Note that using $\xi = \ln n^\alpha$ for $\alpha > 1$ gives a reasonable trade-off between security parameters with $\delta, \varepsilon \xrightarrow{n} 0$, assuming that k is fixed. Let us also stress that $\mathcal{BBA}$ is a very general algorithm. Therefore, in the Fact 9, we can use any metric d and a very general class of cases Ξ. It means that the $\mathcal{BBA}$ algorithm hides all the details of the algorithm and the network but the length of the execution. Note that the above theorem can be optimized, and better results can be obtained (especially for limited types of $\mathcal{A}$ algorithm).

[4]with or without CD

Chapter 7

Conclusion

The thesis presented several protocols that allow for protecting network communication from adversaries. The work was focused on two distinct models, each of which will be concluded in a separate section. The algorithms presented in Chapters 2-4 were focused on the SINR model and entirely blocked the communication at fragments of space, where an adversary could receive it otherwise. These chapters are concluded in Section 7.1. Chapter 5 analyzed the single-hop network model, focusing on keeping the communication private from an adversary. This chapter is concluded in Section 7.2.

7.1 Jamming in SINR networks

The main objective of the SINR network-related algorithms was to entirely block the communication at fragments of space called restricted areas. The approach was based on using special jamming stations positioned in space and introducing enough interference that the secure network was not heard in any restricted areas. Another goal was for the jamming to be precise enough not to impact communication outside blocked areas. As a secondary goal, protocols target the reduction of the overall energy required for jamming. The thesis analyzed several scenarios - namely uniform and non-uniform networks considered under 1D and 2D environments.

The typical limitations of the uniformly powered networks regarding the analyzed task were discussed. In 1D, the simple positioning schemes with one or two stations were presented - with basic configuration came a constant energy cost and a mediocre coverage impact. The precise positioning scheme was also presented, which allows for configuring the jamming station positions arbitrarily close to their optimal placing with small runtime overhead. For the 2D model, the generic algorithms for protecting the enclosing restricted areas were presented, with a sketch of how to implement it for detached areas. In this model, the experimental calculation showed that the jamming network significantly impacted coverage due to uniformity limitations.

More effective algorithms were analyzed for non-uniform networks. Starting with the 1D basic positioning scheme for one jamming station, which reduced its power to accommodate the non-uniformity, it allowed for optimizing the power and coverage impact. Then, the noisy dust algorithm showed that the jamming network could decrease its energy footprint and coverage impact with many jamming stations with relatively small power levels. Two variants of this algorithm were presented - one for the precise configuration and one for simplified deployment of the jamming stations. In the 2D model, this algorithm was extended with a pre-initialized hexagonal grid. The size of a single hexagon impacted the jamming station's power. With a fine enough grid, the algorithm showed energy and coverage reduction properties similar to the 1D version in exchange for the increased number of stations.

All these results allow for quick and efficient protection of stations in a SINR model in a static environment. There are multiple directions in which these results can be extended.

- Analyze dynamic model extensions. It can include the movement of restricted areas and their dynamic shape and size changes, the movement of jamming stations, or the movement of protected stations. The 1D model could simulate the roads for vehicular network modeling, the 2D model could be used as a simulation for water ships communication, and the 3D model is good for a drone network environment.
- Extend the SINR model with a more complex notion of stations' signal reception capabilities - some stations, either from the initial or jamming network, might have different reception thresholds, or these thresholds might change with time (e.g., the adversary could have more sensitive receivers than the initial network). Adjusting and extending the algorithms to account for such scenarios seems challenging.
- Generalizing existing jamming algorithms to n dimensions. Currently, solutions are dedicated to $1D$ or $2D$. However, there are similarities between these variants, which can be utilized to generalize these solutions or at least extend them to realistic dimensions, like $3D$.

7.2 Privacy protection in single and multi-hop networks

In Chapter 5, the pre-processing algorithm for the beeping model was presented. It can be used as an enhancement for other algorithms, which will hide the actual size of the network from the adversary. It is simple to use and provides good hiding properties. Its only problem is a limited maximal size difference between the two networks it can hide. On the other hand, a green leader election algorithm was discussed, which provided much better capabilities in this regard. Both these results point to the possible extensions of this research. Similar schemes of mimicking dummy stations could be analyzed to search for better size-hiding properties. One could verify the size-hiding properties of already existing algorithms or combine them to get better parameters. The problem could be analyzed in similar models, e.g., MAC with and without collision detection. Alternatively, the problem could be considered under the multi-hop model, introducing an entirely different set of issues and privacy-protection capabilities.

Chapter 6 concerns the multi-hop variant of ad-hoc radio networks. The analogical model to Chapter 5 is presented in a generic form. Different types of communication channels and adversaries are described, and the high-level taxonomy of different configurations to consider in such a problem is presented. Finally, the preliminary analysis of two simple algorithms is described.

Bibliography

[1] J. Naughton, "The evolution of the internet: from military experiment to general purpose technology" in *Journal of Cyber Policy*, vol. 1, pp. 5–28, 2016.

[2] DataReportal, "Digital 2022 global digital overview", `https://datareportal.com/reports/digital-2022-global-overview-report`, 2022.

[3] Ericsson, "Ericsson mobility report", `https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2022`, 2022.

[4] M. Attaran, "The impact of 5g on the evolution of intelligent automation and industry digitization" in *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 5977–5993, 2023.

[5] Md. A. Rahim, Md. A. Rahman, M.M. Rahman, A. T. Asyhari, Md. Z. A. Bhuiyan, D. Ramasamy, "Evolution of IoT-enabled connectivity and applications in automotive industry: A review." in *Vehicular Communications*, vol. 27, pp. 100285, 2021.

[6] F. Jameel, Z. Chang, J. Huang, T. Ristaniemi, "nternet of autonomous vehicles: Architecture, features, and socio-technological challenges." in *IEEE Wireless Communications*, vol. 26, pp. 21–29, 2019.

[7] D. Zelikman, M. Segal, "Reducing interferences in VANETs" in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, pp. 1–6, 2014.

[8] M. Lee, T. Atkison, "VANET applications: Past, present, and future." in *Vehicular Communications*, vol. 28, pp. 100310, 2021.

[9] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, M. Welsh, "Wireless sensor networks for healthcare" in *Proceedings of the IEEE*, vol. 98, pp. 1947–1960, 2010.

[10] P. Manoharan, A. Sharma, M. Hamdi, M. Ma, N. Chilamkurti, "Smart healthcare in smart cities: wireless patient monitoring system using IoT" in *The Journal of Supercomputing*, vol. 77, 2021.

[11] D. Li, "5G and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare¿' in *Precision Clinical Medicine*, vol. 2, pp. 205–208, 2019.

[12] E. Aiken, S. Bellue, D. Karlan, C. Udry, J. Blumenstock, "Machine learning and phone data can improve targeting of humanitarian aid" in *Nature*, vol. 603, pp. 1–7, 2022.

[13] N. Saeed, A. Bader, T. Y. Al-Naffouri, M. S. Alouini, "When wireless communication responds to covid-19: Combating the pandemic and saving the economy" in *Frontiers in Communications and Networks*, vol. 1, 2020.

[14] J. Cheng, Y. Yang, X. Zou, Y. Zuo, "5G in manufacturing: a literature review and future research" in *The International Journal of Advanced Manufacturing Technology*, 2022.

[15] A. R. Sfar, Z. Chtourou, Y. Challal, “A systemic and cognitive vision for iot security: A case study of military live simulation and security challenges.“ in *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, pp. 101–105, 2017.

[16] Kh. E. Khujamatov, T K. Toshtemirov, “Wireless sensor networks based agriculture 4.0: challenges and apportions.“ in *2020 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–5, 2020.

[17] B. Nee, M. Tu, “The social economic, environmental, human health, and cybersecurity impacts of wireless and mobile computing“ in *Journal of Communications*, vol. 13, pp. 32–39, 2018.

[18] K. S. Yeo, M. Chian, T. Ng, D. Tuan, “Internet of things: Trends, challenges and applications.“ in *Proceedings of the 14th International Symposium on Integrated Circuits, ISIC 2014*, pp. 568–571, 2015.

[19] S. A. Busari, S. Mumtaz, S. Al-Rubaye, J. Rodriguez, “5G millimeter-wave mobile broadband: Performance and challenges.“ in *IEEE Communications Magazine*, vol .56, pp. 137–143, 2018.

[20] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, “Overview of 5G security challenges and solutions“ in *IEEE Communications Standards Magazine*, vol. 2, 2018.

[21] C. Yin, Z. Xiong, H. Chen, J. Wang, D. Cooper, B. David, “A literature survey on smart cities“ in *Science China Information Sciences*, vol. 58, 2015.

[22] M. Z. Gunduz, R. Das, “Cyber-security on smart grid: Threats and potential solutions.“ in *Computer Networks*, vol. 169, pp. 107094, 2020.

[23] S. D’Oro, F. Restuccia, T. Melodia, “Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying.“ in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 1585–1593, 2019.

[24] S. Yan, S. V. Hanly, I. B. Collings, D. L. Goeckel, “Hiding unmanned aerial vehicles for wireless transmissions by covert communications“ in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.

[25] C. Avin, Y. Emek, E. Kantor, Z. Lotker, D. Peleg, and L. Roditty, “SINR diagrams: towards algorithmically usable SINR models of wireless networks,” in *ACM PODC 2009,* pp. 200–209, 2009.

[26] C. Dwork, F. McSherry, K. Nissim, and A.D. Smith, “Calibrating noise to sensitivity in private data analysis“ in *Theory of Cryptography*, vol. 3876, pp. 265–284, 2006.

[27] D. Bojko, M. Klonowski, D.R. Kowalski, M. Marciniak, “Exact and Efficient Protective Jamming in SINR-based Wireless Networks” in *29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS 2021)* pp. 1-8, 2021.

[28] D. Bojko, M. Klonowski, D.R. Kowalski, M. Marciniak, “Efficient protective jamming in 2D SINR networks“ in *2023 29th International European Conference on Parallel and Distributed Computing (EuroPar23)*, 2023.

[29] P. Jacquet, D. Milioris, P. Mühlethaler, “A Novel Energy Efficient Broadcast Leader Election“ in *MASCOTS 2013*, pp. 495–504, 2013.

[30] D. Bojko, M. Klonowski, M. Marciniak, P. Syga, “On size hiding protocols in beeping model“ in *2023 29th International European Conference on Parallel and Distributed Computing (EuroPar23)*, 2023.

[31] M. Klonowski, M. Marciniak, "Preliminary report: On information hiding in multi-hop radio networks." in *arXiv. org*, 2023.

[32] R. Maheshwari, S. Jain, S. Das, "A measurement study of interference modeling and scheduling in low-power wireless networks" in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*, pp. 141–154, 2008.

[33] E. Kantor, Z. Lotker, M. Parter, D. Peleg, "Nonuniform SINR+Voroni diagrams are effectively uniform" in *Theoretical Computer Science*, vol. 878–879 pp. 53-66, 2021.

[34] A. Goldsmith, "Wireless Communications", *USA: Cambridge University Press*, 2005.

[35] K. Pahlavan, A. H. Levesque, "Wireless Information Networks (Wiley Series in Telecommunications and Signal Processing)", *John Wiley & Sons, Inc., Hoboken, NJ, USA*, 2005.

[36] E. Kantor, Z. Lotker, M. Parter, D. Peleg, "The topology of wireless communication" in *J. ACM*, vol. 62, 2015.

[37] T. Jurdzinski, D. R. Kowalski, G. Stachowiak, "Distributed deterministic broadcasting in wireless networks of weak devices" in *Automata, Languages, and Programming*, pp. 632–644, 2013.

[38] M .M. Halldórsson, P. Mitra, "Nearly optimal bounds for distributed wireless scheduling in the SINR model" in *Distributed Computing*, vol. 29, pp. 77–88, 2016.

[39] Z. Lotker, M. Parter, D. Peleg, and Y. A. Pignolet, "Distributed power control in the SINR model," in *IEEE INFOCOM 2011,* pp. 2525–2533, 2011.

[40] M. A. Burhanuddin, A. A. Mohammed, R. Ismail, M. Hameed, A. N. Kareem, H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective." in *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, pp. 17–21, 2018.

[41] A.H. Lashkari, M.M.S. Danesh, B. Samadi, "A survey on wireless security protocols (wep, wpa and wpa2/802.11i)," in *ICCSIT 2009*, pp. 48-52.

[42] N. Sklavos, X. Zhang, "Wireless Security and Cryptography: Specifications and Implementations", *CRC Press, Inc., USA, 1st edition*, 2007.

[43] I. Martinovic, P. Pichota, J.B. Schmitt, "Jamming for good: A fresh approach to authentic communication in wsns," in *WiSec 2009*, pp. 161-168, 2009.

[44] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "Rfid systems: A survey on security threats and proposed solutions." in *Personal Wireless Communications*, pp. 159–170, 2006.

[45] A. Juels, R. L. Rivest, M. Szydlo, "The blocker tag: Selective blocking of rfid tags for consumer privacy." in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 103–111, 2003.

[46] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "Carving secure wi-fi zones with defensive jamming" in *ACM ASIACCS 2012*, pp. 53–54, 2012.

[47] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming" in *MobiHoc 2012*, pp. 65–74, 2012.

[48] Y. Allouche, E. Arkin, Y. Cassuto, A. Efrat, G. Grebla, J. Mitchell, S. Sankararaman, and M. Segal, "Secure communication through jammers jointly optimized in geography and time" in *Pervasive and Mobile Computing*, vol. 41, pp. 83–105, 2017.

[49] I. Orikumhi, J. Kang, H. Jwa, J. H. Na, S. Kim, "SINR maximization beam selection for mmwave beamspace mimo systems" in *IEEE Access*, vol. 8, pp. 185688–185697, 2020.

[50] H.H. Yang, T.Q.S. Quek, H.V. Poor, "A Unified Framework for SINR Analysis in Poisson Networks With Traffic Dynamic" in *IEEE Transactions on Communications*, vol. 69, pp. 326-339, 2021.

[51] S.I. Mushfique, A. Alsharoa, M. Yuksel, "Optimization of SINR and Illumination Uniformity in Multi-LED Multi-Datastream VLC Networks" in *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, pp. 1108-1121, 2020.

[52] K. Ciesielski, "On Stefan Banach and some of his results" in *Banach J. Math. Anal*, vol. 1, pp. 1–10, 2007.

[53] S. Gilbert, C. Newport, "The computational power of beeps" in *Distributed Computing*, pp. 31–46, 2015.

[54] A. Cornejo, F. Kuhn, "Deploying Wireless Networks with Beeps" in *Distributed Computing*, vol. 6343, pp. 148–162, 2010.

[55] A. Casteigts, Y. Métivier, J. M. Robson, A. Zemmari, "Counting in one-hop beeping networks" in *Theoretical Computer Science*, vol. 780, pp. 20–28, 2019.

[56] P. Brandes, M. Kardas, M. Klonowski, D. Pajak, R. Wattenhofer, "Fast size approximation of a radio network in beeping model" in *Theoretical Computer Science*, vol. 810, pp. 15–25, 2020.

[57] Y. Afek, N. Alon, Z. Bar-Joseph, A. Cornejo, B. Haeupler, F. Kuhn, "Beeping a maximal independent set" in *Distributed Computing*, pp. 32–50, 2011.

[58] M. Klonowski, P. Syga, "Enhancing privacy for ad hoc systems with predeployment key distribution" in *Ad Hoc Networks*, vol. 59, pp. 35–47, 2017.

[59] M. Kardas, M. Klonowski, P. Syga, "How to obfuscate execution of protocols in an ad hoc radio network?" in *Ad Hoc Networks*, vol. 84, pp. 90–106, 2019.

[60] D. Bojko, K. Grining, M. Klonowski, "Probabilistic Counters for Privacy Preserving Data Aggregation" in *CoRR*, vol. 2003.11446, 2020.

[61] T.-H. Hubert Chan, E. Shi, D. Song, "Privacy-preserving stream aggregation with fault tolerance" in *Financial Cryptography and Data Security*, pp. 200–214, 2012.

[62] P. Brandes, M. Kardas, M. Klonowski, D. Pajak, R. Wattenhofer, "Approximating the size of a radio network in beeping model" in *SIROCCO 2016*, vol.9988, pp. 358–373, 2016.

[63] A. Casteigts, Y. Métivier, J. Robson, A. Zemmari, "in Design patterns in beeping algorithms: Examples, emulation, and analysis." in *Information and Computation*, vol. 264, 2018.

[64] B. Ghojogh, S. Salehkaleybar, "Distributed voting in beep model" in *Signal Processing*, vol. 177, pp. 107732, 2020.

[65] K. T. Förster, J. Seidel, R. Wattenhofer, "Deterministic leader election in multi-hop beeping networks" in *Distributed Computing*, pp. 212–226, 2014.

[66] A. Czumaj, P. Davies, "Communicating with beeps" in *Journal of Parallel and Distributed Computing*, vol. 130, pp. 98–109, 2019.

[67] C. Dwork, A. Roth, "The algorithmic foundations of differential privacy" in *Found. Trends Theor. Comput. Sci.*, vol. 9, pp. 211–407, 2014.

[68] C. Dwork, G.N. Rothblum, S. Vadhan, "Boosting and differential privacy" in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pp. 51–60, 2010.

[69] A. Cheu, A. Smith, J. Ullman, D. Zeber, M. Zhilyaev, "Distributed differential privacy via shuffling" in *Advances in Cryptology – EUROCRYPT 2019*, pp. 375–403, 2019.

[70] X. Zheng, Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots" in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[71] M. Ul-Hassan, M.H. Rehmani, J. Chen, "Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions" in *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[72] P. Błaśkiewicz, M. Klonowski, M. Kutyłowski, P. Syga, "Lightweight protocol for trusted spontaneous communication" in *Trusted Systems*, pp. 228–242, 2015.

[73] M. Klonowski, P. Syga, "Practical privacy preserving size approximation in distributed systems" in *2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pp. 1–6, 2016.

[74] B.S. Chlebus, G. De Marco, M. Talo, "Naming a channel with beeps" in *Fundamenta Informaticae*, vol. 153, pp. 199–219, 2017.

[75] N.A. Andriambolamalala, V. Ravelomanana, "Energy efficient naming in beeping networks" in *Ad-Hoc, Mobile, and Wireless Networks*, vol. 11803, pp. 355–369, 2019.

[76] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, A. Thakurta, "Noiseless Database Privacy" in *ASIACRYPT 2011*, vol. 7073, pp. 215–232, 2011.

[77] K. Grining, M. Klonowski, "Towards Extending Noiseless Privacy: Dependent Data and More Practical Approach" in *AsiaCCS 2017*, pp. 546–560, 2017.

[78] J. Cichon, R. Kapelko, D. Markiewicz, "On Leader Green Election" in *CoRR*, vol. 1605.00137, 2016.

[79] M. Ghaffari, B. Haeupler, "Near optimal leader election in multi-hop radio networks" in *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 748–766, 2013.

[80] J. Beauquier, J. Burman, P. Davies, F. Dufoulon, "Optimal multi-broadcast with beeps using group testing" in *Structural Information and Communication Complexity*, pp. 66–80, 2019.

[81] A. Czumaj, P. Davies, "Leader election in multi-hop radio networks" in *Theoretical Computer Science*, vol. 792, pp. 2–11, 2019.

[82] R. Bar-Yehuda, O. Goldreich, A. Itai, "Efficient emulation of single-hop radio network with collision detection on multi-hop radio network with no collision detection" in *Distributed Computing*, vol. 5, pp. 67–71, 1991.

[83] D. Peleg, "Distributed Computing: A Locality-Sensitive Approach" in *Society for Industrial and Applied Mathematics*, 2000.

[84] W. Mulzer, "Five proofs of chernoff's bound with applications" in *Bulletin of European Association for Theoretical Computer Science*, vol. 124, 2018.