Improving Implantable Medical Device Security Through Cooperative Jamming

Kimberly M Lytle

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
In
Electrical Engineering

Timothy J. Talty, Chair
Alan Michaels
Jeff Reed

May 4, 2023
McLean, Virginia

Keywords: implantable biomedical devices, communication system security, array signal processing

Improving Implantable Medical Device Security Through Cooperative Jamming

Kimberly M Lytle

ABSTRACT

Implantable medical devices (IMDs) are medically necessary devices embedded in a human body that monitor chronic disorders or automatically deliver therapies, such as insulin pumps or pacemakers. Typically, they are small form-factor devices with limited battery and processing power. Most IMDs have wireless capabilities that allow them to share data with an offboard programming device, such as a smartphone application, that has more storage and processing power than the IMD itself. Additionally, the programming device can send commands back to the IMD to change its settings according to the treatment plan. As such, wirelessly sharing information between an IMD and offboard device can help medical providers monitor the patient's health remotely while giving the patient more insight into their condition, more autonomy, and fewer in-person appointments.

However, serious security concerns have arisen as researchers have demonstrated it is possible to hack these devices to obtain sensitive information or potentially harm the patient. This is particularly easy to do as most IMDs transmit their data in the clear to avoid allocating their limited resources to encrypting their packets. As these concerns and the percentage of the American population with IMDs grows, there is another fear that bad actors could exploit the link between the programming device and IMD. Theoretically, a hacker could launch a man in the middle attack to send the IMD unauthorized commands, reprogramming it to act as a radio, sniffing signals of interest in the environment. As such, the hacker could use the IMD as a software defined radio (SDR) that captures sensitive or even classified information without the patient's knowledge. If this were to happen, it is possible an unwitting person with an IMD who has access to classified or sensitive information could be used to exfiltrate data that, in the wrong hands, could be used for corporate espionage or to the detriment of national security. While governing bodies agree that cybersecurity risks are present in IMD systems, there are no requirements for IMD manufacturers to create their devices with security measures that mitigate these risks. Researchers have proposed physical, technical, and administrative security measures for IMDs, but other existing wireless security techniques may apply to the healthcare space and need to be explored.

Beamforming is an array signal processing technique that relies on individual elements of antenna arrays adjusting their phase and amplitude to create an overall effect of directing RF energy in a particular direction. Similarly, cooperative beamforming uses

several physically separate "friendly" beamforming-capable devices to collectively send artificial noise to eavesdroppers while ensuring the signal is successfully received by the intended receiver. Although there are several cooperative jamming algorithms, they share the underlying principles of minimizing SINR at potential eavesdroppers while maximizing the SINR at the intended receiver.

Researchers exploring cooperative jamming have largely used models to estimate its impact on channel secrecy. While RF propagation and communication system modeling provides valuable insight into system performance, many theoretical and empirical models are limited by the extent to which the operational environment matches that of the model itself. Ray tracing, alternatively, is more widely applicable as it accounts for a 3D environment and the objects a signal interacts with in that space. A ray is defined as an individual RF signal that travels in a straight line through a uniform medium; obeys the laws of reflection, refraction, and diffraction; and carries energy. As the ray interacts with objects in the environment, its energy will decrease by some amount that depends on the materials and geometry of the object.

While research has predominantly focused on applications like cellular communications, the same principles of minimizing SINR at potential eavesdroppers while maximizing the SINR at the intended receiver can be applied to IMDs. As IMD use cases assume the programmer is nearby, the friendly nodes will not need to act as relays and can instead focus all their power on jamming. The number of cooperative jammers will be low to simulate the number of devices an individual might have in a workspace or office setting, like a personal phone, smart watch, or laptop, and realistic power constraints will be observed. Further, ray tracing software will provide additional visual insights into how various building materials like drywall, concrete, brick, and glass impact cooperative jamming. Through these simulations, the trade-off between secrecy rate and physical separation and layout of friendly nodes can be determined, which in turn may inform how companies or individuals can protect their proprietary and personal information.

Improving Implantable Medical Device Security Through Cooperative Jamming

Kimberly M Lytle

GENERAL AUDIENCE ABSTRACT

Implantable medical devices (IMDs) are medically necessary devices embedded in a human body that monitor chronic disorders or automatically deliver therapies, such as insulin pumps or pacemakers. The data on IMDs need to be processed and their settings might need to be adjusted, but IMDs themselves usually cannot support direct user input, such as through screens or buttons, as they are inaccessible without surgery or generally too small to have space for displays. Further, they lack processing power and battery life due to their small form-factors, so relatively little data remains onboard. Instead, it is more convenient for the IMDs to wirelessly send their data to a more powerful external device like a smartphone. Since smartphones have more battery and processing resources available, and are easily recharged, they can store more data, monitor trends in the patient's health records, and upload the data to a server which the doctors can access. Additionally, these devices can send commands back to the IMD to change its settings according to the treatment plan. As such, wirelessly sharing information between an IMD and offboard programming device can help medical providers monitor the patient's health remotely while giving the patient more insight into their condition, more autonomy, and fewer in-person appointments.

However, serious security concerns have arisen as researchers have demonstrated it is possible to hack these devices to obtain sensitive information or potentially harm the patient. As these concerns and the percentage of the American population with IMDs grows, there is another fear that bad actors could exploit the link between the programming device and IMD. Theoretically, a hacker could send the IMD unauthorized commands that change the IMD's behavior so that they are reprogrammed to act as radios listening for signals in the environment in order to steal sensitive or even classified information. While governing bodies agree that cybersecurity risks are present in IMD systems, there are no requirements for IMD manufacturers to create their devices with security measures that mitigate these risks. Researchers have proposed physical, technical, and administrative security measures for IMDs, but other existing wireless security techniques may apply to the healthcare space and need to be explored.

Cooperative jamming is an existing defensive wireless technique that reduces the likelihood of an eavesdropper gaining access to unauthorized information. A known set of "friendly" transmitters each transmit noise to eavesdroppers while ensuring the signal

is successfully received by the intended receiver. Researchers exploring cooperative jamming have largely used models to estimate its impact on channel secrecy. While RF propagation and communication system modeling provides valuable insight into system performance, many theoretical and empirical models are limited by the extent to which the operational environment matches that of the model itself. Ray tracing, alternatively, is more widely applicable as it accounts for a 3D environment and the objects a signal interacts with in that space. A ray is defined as an individual RF signal that travels in a straight line through a uniform medium; obeys the laws of reflection, refraction, and diffraction; and carries energy. As the ray interacts with objects in the environment, its energy will decrease by some amount that depends on the materials and geometry of the object. Thus, using ray tracing to model cooperative jamming will provide new insights into the degree to which cooperative jamming could be used to protect an IMD from eavesdroppers, and how companies or individuals can protect their proprietary and personal information.

Acknowledgement

Thanks to The MITRE Corporation for the support and funding of my graduate degree.

The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1: Background on Implantable Medical Devices

Implantable medical devices (IMDs), such as pacemakers, insulin pumps, and cochlear implants, are small, electronic, battery-powered devices attached to or embedded in a human body that monitor chronic disorders or automatically deliver therapies. Many of these devices can communicate wirelessly over Wi-Fi, Bluetooth, or cellular to program the IMD, remotely monitor the patient, or transfer the patient's data to an external device [1] [2]. In 2021, roughly 10% of Americans had IMDs [3]. This number is expected to rise as technology advances, the population ages, and as cardiovascular ailments and obesity become more prevalent [4].

Although wireless communication systems are known to be vulnerable to cyber threats, IMDs historically have not been designed with security as a priority [2] [5] [6]. Further, IMDs are constrained by size, processing power, and battery life, and thus cannot support traditional cybersecurity practices and algorithms [2] [7] [8]. The Food and Drug Administration (FDA) regulates and creates standards for IMDs and has worked with the Federal Communications Commission (FCC) to properly regulate IMDs' wireless communications. The FCC is actively researching cybersecurity threats to IMDs through threat modelling to provide insights on how IMD manufacturers can make their devices more secure, as wireless capabilities are helpful if not necessary for both patient and medical providers [1] [9]. The ability for IMDs to offload their data to an external device or server with more computing resources allows patients and medical providers to have more insight into the treatment's effectiveness and device status through data analytics and, in some cases, artificial intelligence to predict trends [10] [11]. Wireless capabilities allow patients to have more autonomy in their daily lives, as a discrete sensor monitors their condition without the need for the user to be tethered to a medical bed, and the IMD can monitor their condition and perhaps administer medicine without user intervention. With predictive analytics, physicians can monitor patient status over time to note any abnormalities or potentially dangerous trends that can be precursors to more serious illness and act before the condition becomes more serious. Further, physicians can monitor their patients remotely, reducing the number of in-office visits needed and saving time and money. Thus, despite the security risks involved with wireless networks, it is impractical to suggest these threats be mitigated by migrating to wired solutions.

While there is more awareness about the need to secure communications systems involving IMDs, serious vulnerabilities still exist, and no general solution has been found that addresses IMDs as a whole. As devices become "smarter," there is inherently less

user control as the device is meant to be unobtrusive, removing or limiting the amount of work a patient must do to manage their condition.

1.2: Known Vulnerabilities

To date, there are no known hackers that have maliciously exploited IMDs to harm patients. However, ethical hackers have found serious vulnerabilities in both IMDs and other devices using common wireless protocols. Serious vulnerabilities in both IMDs and other devices using common wireless protocols. VxWorks is a common medical device operating system that powers roughly 2 billion industrial, medical, and enterprise devices [12] [13]. Researchers at Armis Labs found VxWorks to have 11 zero-day vulnerabilities in the TCP/IP stack, allowing attackers to take over devices without any user input [13]. If exploited, the attack would appear as legitimate network traffic, and could act as a worm, infecting other VxWorks-based devices on the network or targeting specific devices [13]. Notably, SweynTooth was a group of Bluetooth Low Energy (BLE) vulnerabilities affecting several kinds of Smart Home and medical devices [14]. Attackers in range could "trigger deadlocks, crashes, or partially bypass security depending on the circumstances" [15]. Major vendors such as Texas Instruments, Microchip, ON Semiconductor, Medtronic, and VivaCheck were affected [15].

In 2017, the FDA recalled roughly 500,000 pacemakers with critical vulnerabilities that would allow attackers to remotely control the devices, draining the battery or administering unauthorized pulses that could be fatal [16] [17]. Fortunately, no patients were harmed, and this event raised awareness among the public about cybersecurity vulnerabilities in IMDs [17]. One hobbyist, acting as an ethical hacker, explored whether he could reverse engineer the proprietary communications of his insulin pump and continuous glucose monitor to find any exploits [6] [18]. He successfully intercepted and decoded the signals and was able to inject fake data into the pump without the device indicating an unauthorized party had tampered with it [6]. In [19], Halperin et al. addresses the gap in IMD security studies and proposes security vulnerability mitigations with a focus on a specific Medtronic implantable cardioverter defibrillator (ICD). The team reverse engineered the devices using a software defined radio (SDR) and found they could directly get patient information and medical telemetry. They demonstrated a bad actor could use an SDR to change ICD information which could be fatal, such as adjusting therapy settings or administering a shock to the heart. Notably, they found ICD data is often unencrypted and can communicate with unauthorized devices, making it possible for attackers to launch a denial of service (DoS) attack, or send commands causing the ICD to continuously consume energy, thus draining the battery and "threatening availability." Halperin et. al. provide three defenses that would

require minimal design changes and do not require battery power in [19] and a general framework for evaluating IMD security and privacy, and discuss design trade-offs in [8].

In April of 2022, the FDA released a draft of cybersecurity guidance for IMDs, citing authenticity, authorization, availability, confidentiality, and secure and timely updatability as primary security objectives to consider in a dynamically evolving threat landscape [20]. Although the FDA is the governing authority over IMDs, requiring them to be reasonably safe, more responsibility is being shifted to patients and physicians to determine if the benefits of IMDs outweigh their risks [21]. Often, these devices provide a much higher quality of life to patients, rendering them necessary despite the known drawbacks.

1.3: Implications of IMDs in Secure Spaces

As concern over IMD vulnerabilities has grown over recent years, researchers have begun examining the implications of introducing these devices in spaces where privileged or even classified information is shared [22] [23]. In the United States, to perform work related to classified national security information, employees must obtain a security clearance and may be required to conduct this work in areas which limit or prohibit personal electronic devices (PEDs) such as cell phones, pagers, smart watches, and laptops [24] [25]. However, people with IMDs are protected under several laws including the Rehabilitation Act of 1973, Americans with Disabilities Act, and Health Insurance Portability and Accountability Act (HIPAA) and may not be discriminated against for their medical requirements [22] [26]. In 2010, roughly 2.3% of the 4.3 million people with security clearances were estimated to have IMDs, with insulin pumps being the most common [22] [23] [27]. The number of people with both active security clearances and IMDs is expected to continue rising over time [22] [23]. The Office of the Director of National Intelligence (ODNI) lists several specifications for sensitive compartmentalized information facilities (SCIFs), noting that PEDs and devices supporting two-way communications are particularly high-risk because unintended electromagnetic emissions (UEEs) can leak data [27] [28]. In unclassified areas where PEDs are allowed, privileged information may still be shared, such as trade secrets, intellectual property disclosures, personal or identifying information such as social security numbers or credit card information, or any other information not intended for competing companies or the general public. As such, it is important to understand the security implications of IMDs in secure spaces and conduct more research into techniques to mitigate data leaks.

Existing mitigations are either high risk to the person with the IMD, have low security benefit, or are impractical [22] [27]. For example, the primary security

mitigation is to leave devices outside the secure area, which is not always possible for IMD users, but other options are for the user to be subject to random physical inspections or be asked to wear RF shielding apparel [27]. Removing any data collected during the user's time in the secure area would require knowledge of each device, may present HIPAA concerns, and could unintentionally remove important device settings [27]. It is not practical to adjust the supply chain by requiring manufacturers to make SCIF-safe devices, especially as many IMDs are manufactured outside of the United States and the market for SCIF-safe devices is limited [27]. However, it may be practical for manufacturers to consider adding audible alarms to alert users when an external device is paired with their IMD or allow dual authentication through a third-party device before downloading data to an app [27]. The FDA could create more robust cybersecurity requirements, but this could complicate medical device design further and cause delays in getting the latest devices to consumers [27]. Further, encryption algorithms typically consume too much processing power and battery to be considered for IMD applications [2]. As such, the most practical solution may be to adjust the communication channel itself through RF jamming or beamforming. However, adding any wireless device, including countermeasures, to a secure space like a SCIF itself poses a security threat which may not outweigh its benefits. These mitigations and their shortcomings are summarized in Table 1. Focusing on mitigation techniques in spaces where privileged or confidential information is shared and PEDs are allowed makes the problem of securing IMD communications more tractable and may inform future solutions that center around secure areas.

Proposed Solution	**Counterargument**
FDA creates cybersecurity regulations	Medical device companies assert limited processing power and battery life inhibit cybersecurity practices
Manufacturers create IMDs that are hardened for use in SCIFs	Market is too small for private companies to allocate resources for development, testing, and certification
FDA mandates all IMDs must be made within the US and/or by US persons	Impractical, and does not assure backdoors are prevented
Administrative software installed on IMD programmer	Limiting IMD functions may impact patient health
Audible/visual alarms are triggered when a new or unauthorized connection is made to the IMD	Does not stop or prevent attacks
Physical signal attenuation	Could prevent health information from being processed at programmer, and could cause social pushback

Proposed Solution	Counterargument
Random inspections	Might violate HIPAA
Third-party authenticator	Additional hardware is cumbersome, and will only work when the patient has the authenticator nearby
Whitelisting	Does not stop or prevent attacks
Zeroization	Important health information will be lost

Table 1: A list of potential IMD mitigation strategies and their drawbacks.

Chapter 2: Alternatives Analysis

2.1: Security Concerns

To date, researchers have explored various ways of tackling the vulnerabilities associated with IMDs. As the population ages and develops more diseases, particularly diabetes and cardiac related ailments, the IMD market continues to grow. However, IMD integration with wireless technologies poses new threats, especially as they historically have not been designed from the outset with security in mind [5]. In 2012, NIST performed a cyber risk assessment of IMDs. The threats, vulnerabilities, and risks identified persist to this day, and are compounded as new issues come to light. These threats typically target authentication, authorization, availability, non-repudiation, or privacy [1] [2] [8] [19]. Since IMDs lack encryption to save on-board memory and power, data and commands are often sent in-the-clear and are relatively easy to reverse-engineer [18] [19]. Thus, bad actors could launch attacks that flood the IMD with commands, deny service, send unauthorized treatment updates, or steal personal information. Further, access to cyber-attack enabling technology (e.g., software defined radios (SDRs), network protocol analyzing software, and open-source resources) becomes more accessible as costs decrease and information about device operation is more widely accessible, such as through FCC filings or patent publications [18].

2.2: Proposed Solutions

Since the problems with IMD security are well-documented, it is reasonable to wonder why these issues persist, especially if the vulnerabilities could be exploited to cause harm to the user. As with any system, there are conflicting goals which must be prioritized. The FDA Center for Devices and Radiological Health regulates IMDs and focuses on safe, effective functioning and environmental conditions rather than cybersecurity, although the FDA does recommend some best practices [2] [20]. Implementing security measures, such as adding encryption or traffic verification mechanisms, would take up device resources that are used for necessary functions that enable the user to be treated with essential medical therapies. IMDs have limited board space, meaning the battery size and amount of memory is severely restricted. Further, batteries often must be surgically replaced, so conserving power is a priority. With limited processing capabilities and power, on-board protocols must be extremely simple. Often, this involves transmitting data in the clear rather than using encryption.

The National Security Agency (NSA) has a certification program that verifies equipment prevents electromagnetic information from being leaked from classified

spaces [29]. These certified systems are said to abide by "TEMPEST" standards. When considering secure spaces, the market for creating specialized IMDs, for example TEMPEST-certified IMDs which would abide by a standard related to the extent to which a classified signal is contained, is very small [22] [29]. Medical device companies therefore have little motivation to develop, test, certify, and market such specialized IMDs that would be unlikely to be a primary revenue source. Removing wireless capabilities altogether would be impractical, and thus mitigation techniques must be developed that account for these devices having limited resources.

Generally, IMDs rely on "security by obscurity;" that is, using proprietary protocols or obfuscating system processes [2]. Proposed threat mitigation strategies consider the technical benefit and impact on the individual. [2], [6], [22], and [30] enumerate the following options, although each have their own tradeoffs:

- **Administrative software**: software on the IMD's programmer, such as a smartphone, could allow the IMD to enter a sleep mode for a set period of time during which no new connections are allowed, and no data can be sent from the IMD to the programmer except in the case of a medical emergency. Limiting IMD functions may impact patient health.
- **Alarms**: A new or unauthorized connection to an IMD could trigger an audible or visual alert on the programming device so the patient knows there is an issue. However, this does not stop an attacker.
- **Physical signal attenuation**: requiring IMD users to shield their emissions, such as by wearing a Faraday cage or being near a noise generator, could mask the signal from attackers. However, it could prevent pertinent health data from being processed at the programmer. From a social perspective, people might be hesitant to use these devices as it could draw attention to their medical condition.
- **Random inspections**: mandating that employees who want to enter a secure space undergo random IMD inspections could identify which devices have been altered, but this may not be legal due to HIPAA protections.
- **Third-party authenticator**: systems like [31] and [32] propose using a separate device that acts as a relay between the IMD and programmer. However, if the authenticator is not close enough to the IMD, it will not be successful, and patients might find the additional hardware cumbersome.
- **Whitelisting**: maintaining a list of allowed devices against which to compare an IMD entering a secure facility would help prevent unwanted electronics but does not prevent the IMD from being attacked.

- **Zeroization**: deleting all data off of a device that was obtained while the IMD was in the secure space could prevent data from getting out if it was not already taken while in the secure area but might clear important health information.

Mitigation Strategy	**Threat Type**				
	Authentication	**Authorization**	**Availability**	**Non-repudiation**	**Privacy**
Administrative software	No	Yes	Yes	Yes	Yes
Alarms	Yes	Yes	No	No	No
Physical Signal Attenuation	No	No	No	No	Yes
Random Inspections	No	No	No	No	No
Third-Party Authenticator	Yes	Yes	No	Yes	Yes
Whitelisting	Yes	Yes	No	Yes	No
Zeroization	No	No	No	No	Yes

Table 2: A list of IMD mitigation strategies and whether they apply across various threat categories where "yes" indicates the threat is mitigated by the strategy

Chapter 3: Cooperative Jamming

3.1: Principles of Beamforming and Cooperative Jamming

In most wireless networks, upper layers in the protocol stack are responsible for encryption and security. However, adding encryption requires more processing and power resources, and the algorithm chosen may be reverse engineered so an eavesdropper can recover the information anyway [33] [34]. The physical layer is the lowest layer in the Open System Interconnect (OSI) model and defines the system's hardware specifications, transmission and reception methods, bit synchronization, encoding and signaling, and network topology [33]. Physical layer security is a critical component to consider when addressing secrecy and reliability concerns, especially for systems that do not have upper-layer encryption [34] [35] [36]. Namely, this is done by leveraging the channel's physical characteristics like randomness, time variation, reciprocity, and differences between the intended and unintended links rather than relying on an adversary lacking the computing resources to crack encryption algorithms [33] [34] [36].
In 1975, Wyner determined that perfect secrecy is achievable in a wire-tapped channel without the use of private keys [37]. This work demonstrated that successful encoding structure causes the maximum amount of uncertainty at the eavesdropper and has since been extended and generalized to other kinds of broadcast channels, such as Gaussian or fading channels [38] [39]. However, when the intended link, between the transmitter and intended receiver, is weaker than the unintended link, between the transmitter and eavesdropper, secrecy is unachievable [37]. Thus, while communication systems are typically averse to interference effects as they degrade signal quality at the receiver, creating artificial noise on the unintended link makes eavesdropping more difficult.
Beamforming is an array signal processing technique that relies on individual elements of antenna arrays adjusting their phase and amplitude to create an overall effect of directing RF energy in a particular direction. Similarly, cooperative beamforming uses several physically separate beamforming-capable devices to improve signal reception [35] [40] [41] [42]. Cooperative jamming is a defensive technique that uses several "friendly", beamforming-capable devices to collectively send artificial noise to eavesdroppers while ensuring the signal is successfully received by the intended receiver [42] [43].

3.2: Existing Cooperative Jamming Techniques and Uses

Existing cooperative jamming techniques propose using a subset of the friendly nodes as jammers while others act as relays by amplifying and forwarding the signal, or each node splitting its power between jamming and relaying [35] [36] [44] [41] [42] [43] [45].

[35] investigates how a two-phase relay system with multiple friendly nodes impacts the secrecy rate. Nodes either operate as relays or jammers under this system. This technique assumes channel state information (CSI) is available, assumes there are only the minimum number of friendly nodes needed to meet performance requirements in order to minimize overall complexity, and does not operate under an overall power constraint.

[36] discusses how friendly nodes may split their power to simultaneously transmit jamming and information-bearing signals under a time-varying channel. [36] concludes that secrecy rate loss is independent of power splitting factor, number of antennas, and eavesdroppers in areas with a high signal to interference and noise ratio (SINR). In areas with low SINR, the secrecy rate is impacted by these factors.

[44] extends existing research by introducing elements found in more realistic environments, such as moving nodes and reflecting objects. They assume the systems use frequency division duplexing (FDD) and channel information is available but assert that their results hold for time division duplexing (TDD) systems as "pilots in an uplink phase can be used for downlink channel estimation for beam design." These results corroborate those found in [36] where the secrecy rate in an environment with a high signal to noise ratio (SNR) is not impacted by the power splitting factor.

[41] focuses on multiple-input-single-output (MISO) systems when CSI is both available and unavailable. When CSI is available, [41] employs a strategy of minimizing the worst case SINR at eavesdroppers while ensuring a minimum quality of service at the intended receiver. Otherwise, the jamming power is maximized while guaranteeing a quality of service at the receiver.

[42] uses semidefinite relaxation techniques to show an optimal solution exists if CSI is available in a joint cooperative beamforming system with relay nodes. This paper assumes there is no direct link between the source and intended receiver and uses a multi-phased approach similar to that of [35].

Lastly, [45] proposes a scheme where one relay node is selected from a group of friendly jammers, and the process is broken into two phases. The jammer weights are derived such that there is no interference at the source or intended receiver, and the jamming signal is maximized at the eavesdropper. The paper shows the secrecy capacity grows with the number of helper nodes up to a point of diminishing returns.

3.3: Cooperative Jamming in Securing IMD Communications

In addition to the IMD threat mitigation strategies outlined previously, using an array of trusted transmitters that create nulls in the environment except where the IMD is located would secure the wireless channel without adding strain on the IMD's limited resources

by offloading the processing to existing devices nearby. Cooperative jamming has the benefit of securing the physical layer without requiring the IMD to implement encryption or to waste battery transmitting at a higher power to reach the programmer over an artificially inflated noise floor.

While research has predominantly focused on applications like cellular communications, the same principles of minimizing SINR at potential eavesdroppers while maximizing the SINR at the intended receiver can be applied to IMDs. By adopting and extending the existing techniques of [35], [36], [44], [41], [42], and [45], this paper will demonstrate how cooperative jamming can be extended to protect IMDs and their data. Because IMDs have limited power and range, this paper assumes the IMD, offboard programming device, cooperative jammers, and eavesdropper are in relatively close proximity with one another, but the eavesdropper CSI is not known. As IMD use cases assume the programmer is nearby, the friendly nodes will not need to act as relays and can instead focus all their power on jamming. The number of cooperative jammers will be low to simulate the number of Bluetooth-enabled devices an individual might have in a workspace or office setting, like a personal phone, smart watch, or laptop, and realistic power constraints will be observed. Further, ray tracing software will provide additional visual insights into how various building materials like drywall, concrete, brick, and glass impact cooperative jamming. Through these simulations, an understanding of how a few friendly nodes with narrow beamwidths impact IMD security in an office environment, which in turn may inform how companies or individuals can protect their proprietary and personal information. In the future, if more Bluetooth-enabled devices are allowed in secure spaces like SCIFs, this work could provide guidelines for how to use existing infrastructure to prevent unauthorized users from accessing privileged data.

Chapter 4: Methodologies Employed in Cooperative Beamforming Simulations

This chapter examines the difference between ray tracing and analytical models to motivate the use of ray tracing in this thesis. Remcom's Wireless InSite software is used to provide insights into wireless communication systems operating in complex environments through ray tracing. As it is a relatively uncommon, yet powerful, analysis tool, a discussion of its capabilities and example use cases are included. Wireless InSite is used in this work to understand how IMDs interact with an office environment and how cooperative beamforming can improve wireless security. Like any tool, there are limitations which are discussed as they pertain to this thesis. Further, openly available information about SCIF building material is synthesized for potential future research endeavors. Lastly, the proposed methodology for evaluating cooperative beamforming success for IMD use cases is introduced.

4.1: Ray Tracing

RF propagation and communication system modeling provides valuable insight into system performance, but many theoretical and empirical models are range-based and assume the operational environment matches that of the model itself. Ray tracing, alternatively, is more widely applicable as it accounts for a 3D environment and the objects a signal interacts with in that space. However, ray tracing is more computationally intensive as it often uses numerical techniques based on Maxwell's equations [46] [47] [48]. Under this model, a ray is defined as an individual RF signal that travels in a straight line through a homogeneous medium; obeys the laws of reflection, refraction, and diffraction; and carries energy. Specifically, the ray is considered to be a tube whose cross section increases as distance away from the propagation point increases such that the total power in the cross section is constant, which is accounted for in the spreading factor [46]. The energy density can also be reduced if the ray interacts with objects in the environment, such as through scattering.

Generally, ray tracing models predict the rays' paths from the transmitter to any given receiver and estimate the path loss for each ray. Each individual ray may interact with the environment in one of several ways. A ray may have direct line of sight (LoS) to the receiver, be reflected off one or more objects, be diffracted, or be scattered. Reflected rays, also known as transmitted rays, occur when the signal encounters an interface between two media. The reflected ray's magnitude is determined by Fresnel's equations [46]. Diffracted rays may occur when an incident ray encounters an edge, at which point many diffracted rays are generated. This becomes more complicated as a ray

encounters several edges. Scattering occurs when an EM wave encounters a rough surface.

The most common ray tracing algorithms include Fermat's principle of least time, the image method, the shooting and bouncing ray (SBR) method, and the hybrid method. As each of these methods are computationally and time intensive, acceleration methods have been developed to expedite the process [46].

The space divisions method separates the area of interest into smaller regions called "cells." Each cell has information about neighboring regions. Thus as a ray moves from one cell to the next, the neighboring cell's information reduces the number of object interactions to consider and consequently improves the computational efficiency [46] [49].

Reducing the problem from a 3D space to a 2D space is another way to increase computation speed [46] [50]. This can be done by using 2D triangulation and vector algebra, assuming building heights are known [50]. [50] demonstrated that the 2D simplification had excellent agreement with the 3D case while significantly reducing runtime.

While not an algorithmic change, graphics processing units (GPUs) and graphics cards have become more capable over time and can greatly reduce the runtime of numerical methods [46].

4.1.1: Remcom Wireless InSite Software

Remcom is a software company that "provides innovative electromagnetic simulation software and wireless propagation software for commercial users and U.S. government sponsors." [51] Their products enable high-fidelity design and analysis of complex systems in areas such as antenna design, cellular systems, wireless communications, electromagnetic (EM) field simulation, mobile device design, biomedical applications, and radar [51] [52].

Remcom's Wireless InSite software provides comprehensive assessments of EM propagation and communication systems in urban, rural, indoor, and mixed path environments [53]. It has the following features:

- **X3D propagation model**: a proprietary 3D propagation model that accounts for reflections, transmissions, diffractions, frequency-dependent atmospheric absorption, and diffuse scattering for frequencies up to 100GHz. It builds upon Remcom's depth-first and exact path algorithms to improve upon and correct limitations of traditional techniques like the shooting and bouncing rays (SBR) method. Further, there are no geometry restrictions, and the transmitters and receivers can be at any height. X3D propagation works for

built-in waveforms, and Remcom's Full 3D propagation mode must be used for user-defined waveforms [53] [54].

- **Antenna modeling**: common antenna types are built in, such as omnidirectional or half-wave dipole, but users can supply their own antenna patterns for single-input single-output (SISO), multiple-input multiple-output (MIMO), or massive MIMO systems. Further, users can design their own MIMO antenna with the MIMO array builder tool. An antenna's main beam direction, polarization, noise figure, total power, reflection efficiency factor, and cable loss can be specified [53] [55].
- **MIMO beamforming**: antenna diversity, spatial multiplexing, and beamforming are the common MIMO techniques supported by Wireless InSite . Receiver diversity approaches include selection combining, equal gain combining, and maximum ratio combining. Spatial multiplexing is performed using singular value decomposition (SVD) to generate orthogonal data streams. SINR and throughput are computed for each of the streams and summed to create a total throughput estimate. Beamforming is accomplished through either maximum ratio transmission (MRT) which adaptively maximizes the beam between transmitter and receiver points, or precoding tables wherein a user defines sets of beamforming weights, and the software chooses the strongest beam to each receiver point. An additional MIMO license is required [53] [56] [57].
- **Communication system analysis**: post-processing the ray-tracing results yields metrics including signal-to-interference-and-noise ratio (SINR), throughput, theoretical capacity, and bit error rate (BER). These results can be visualized with heat maps over the coverage area [53] [57].
    - Noise power is calculated using noise power density, signal bandwidth, and each receiver's noise figure and threshold while interference uses received power from each base station (transmitter) [57].
    - Throughput and capacity, defined as the theoretical maximum data rate, is calculated from the channel's bandwidth and signal to noise ratio (SNR) [57]. Built-in channel access methods include LTE, WiMax, 802.11n, and 802.11ac. Users can provide data to define additional access methods [57].
    - BER analysis can be done assuming an additive white Gaussian noise (AWGN) channel, Rayleigh or Rician fading channel, or by using the channel's complex impulse response [57]. BER is affected by the

modulation and coding scheme, SINR, bandwidth, and possibly channel characteristics given by the complex impulse response.

- **Materials**: the default material database contains common building or construction materials like wood, brick, concrete, drywall, glass, wet earth, metal, and sand [53] [58]. Additional material types include dielectric half-space, layered dielectric, perfect electrical conductor (PEC) backed layer, polarization-dependent constant coefficient, free space, and foliage. Users can define custom materials or edit existing material parameters in the database. Each feature, such as a wall or piece of furniture, is made of planar facets and assigned a material. Materials affect electromagnetic signals' reflections, transmissions, and diffractions, and these behaviors are frequency-dependent [58].
- **Engineered electromagnetic surfaces (EES)**: predominantly used in 6G research, EES are special materials classified as passive metasurfaces with conductive patterns printed on substrates that scatter high-frequency signals in a particular direction to enhance coverage [53] [59].
- **Diffuse scattering**: used primarily to improve scattering models for 5G applications, Wireless InSite's diffuse scattering model provides high-fidelity results for MIMO and massive MIMO systems through multipath interactions [53] [60]. Lambertian, directive, and directive with backscatter models are provided.
- **Feature import**: cities, objects, terrain, and foliage can be imported via a variety of file formats [53] [61].
- **Geometry caching**: avoids the need to re-process objects in the environment when running simulations using the same geometry, thus saving time [53] [62].
- **Fast ray-based methods**: for 2D geometries, particularly urban canyon, vertical plane ray, vertical plane urban, and triple path geodesic models [53] [63].
- **Empirical propagation models**: Hata, COST-Hata, Walfisch-Ikegami, OPNET path attenuation routine, and free space models can be used for both indoor and urban analysis. Wireless InSite's Wall Count model is specifically designed for indoor calculations, and accounts for every wall a ray intersects [64].
- **Outputs**: received power, path loss, propagation paths, time of arrival, direction of arrival, delay spread, and E-field magnitude and phase can be visualized on coverage maps. For communication systems, outputs may

include throughput, carrier to interferer ratio (C/I), strongest transmitter seen at each receiver, strongest transmitter power seen at each receiver, and total power. The Maximum Permissible Exposure (MPE) module provides hazard assessments against IEEE safety thresholds [65].

4.1.2: Remcom Wireless InSite Examples

In the figures below, Wireless InSite was used to model the received signal strength across the second floor of a simple office building. This building is comprised of drywall walls, concrete floors, and glass windows, and contains wooden desks, chairs, and a couch (not pictured). Some walls and the roof are invisible to showcase the layout. The transmitter (green cube) is acting as a wireless access point on the ceiling, and red cubes represent a receiver grid with a spacing of 0.45 feet for a total of 684 receivers. Outside the building, the green area is comprised of dry earth and the grey area is concrete, but it does not impact this example simulation.

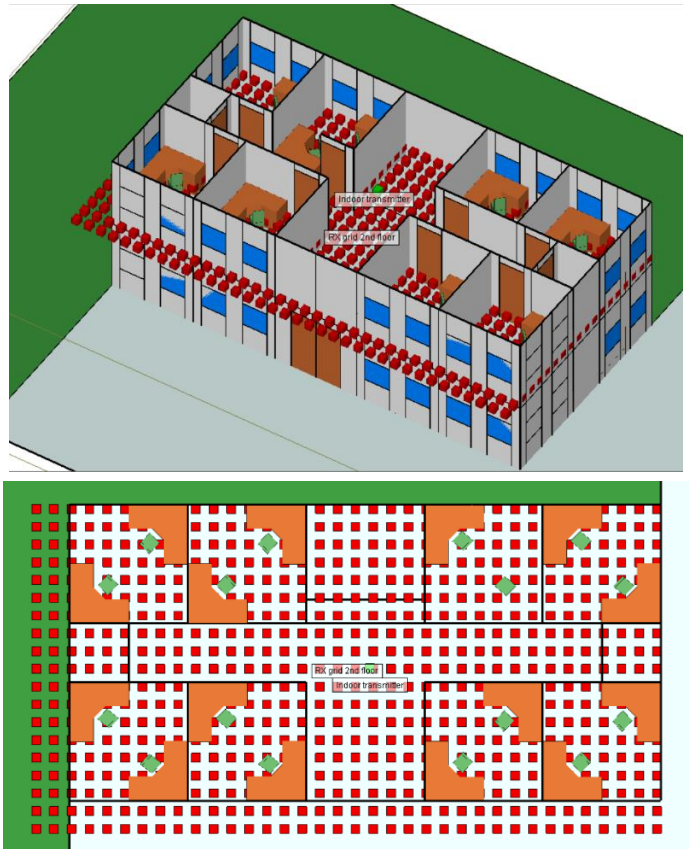

Figure 1: Example building, transmitter, and receiver layout as seen in a perspective view (top image) and from a bird's eye view (bottom image).

The following figures demonstrate how received signal strength can be visualized, and how individual rays can be traced between the transmitter and any given receiver.

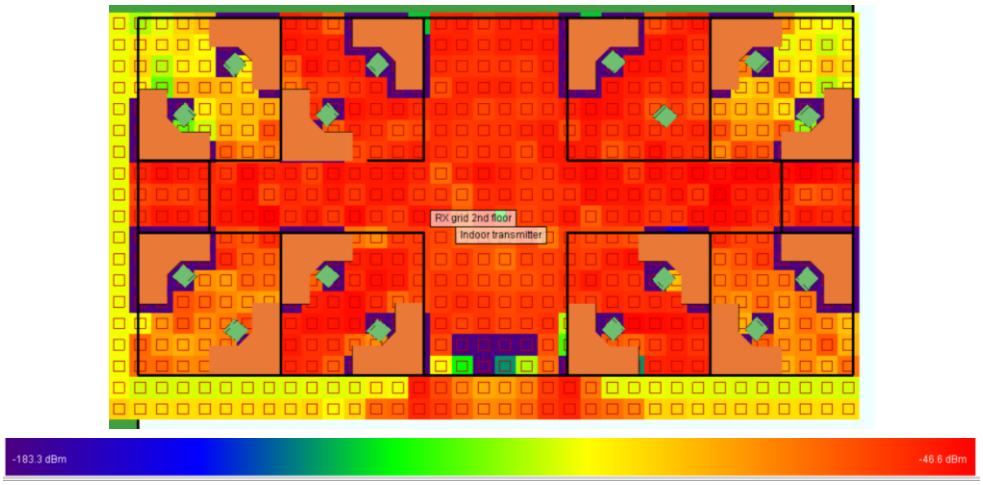

Figure 2: Received signal strength across the building's second floor. The highest received power was roughly -46.6dBm and the lowest was roughly -183.3dBm. The purple area toward the bottom middle of the image is where the couch was placed.

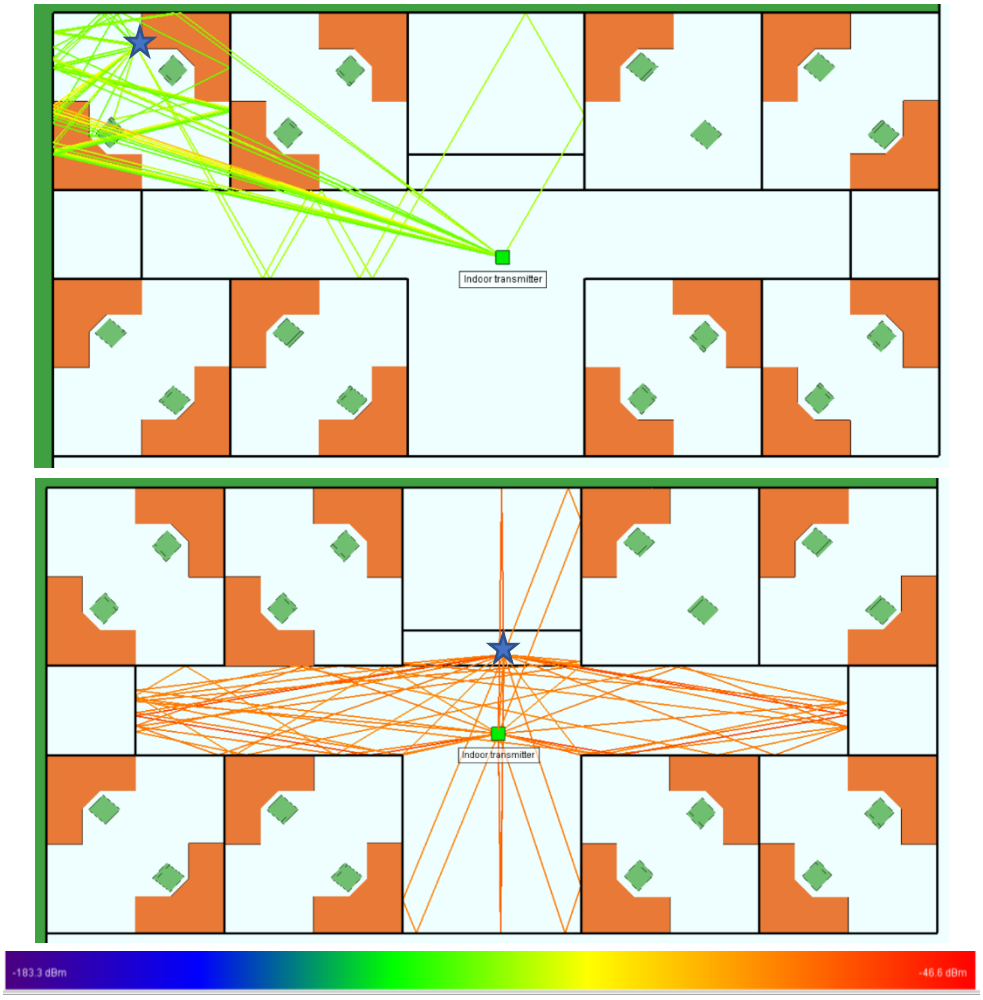

Figure 3: Example of ray tracing between a receiver, indicated with a star, and the transmitter. The top image with predominantly green lines indicates this receiver's total power was relatively low compared to that of the receiver in the bottom image with orange lines.

For more exact results at the expense of a longer runtime, the receivers could be spaced closer together, or the number of reflections, transmissions, and diffractions could be increased in the settings.

4.1.3: Limitations

While Wireless InSite provides valuable insight into communication environments through ray tracing, it is important to consider its limitations that impact the extent to which it accurately represents the real world. The built-in database contains a substantial number of materials and their impact on waveforms operating at different frequencies, but there is no human body model in Wireless InSite. As such, the impacts of the human body on IMD communication cannot be inherently modeled. Future researchers may create an antenna model that accounts for the body or add a material to the database that will impact signals as a body would. This would have to be performed for a specific IMD, as the different kinds of organs and tissues have unique impacts on signal propagation and impedance matching [66]. Alternatively, an assumption can be made about how much the signal will be attenuated to simplify the problem. Further, Wireless InSite cannot be used for moving transmitters or receivers. Perhaps additional research could work toward automating runs that incrementally move the transmitter relative to the receivers. This is not practical currently as it would have to be done manually, and each run may take close to an hour if the setup is similar to that of this paper, and the computer's processor is relatively powerful and not burdened with other computationally expensive tasks. Lastly, the building and objects within it are approximated with low polygon count renderings, causing ray interactions to be simplified.

4.1.4: Note on Materials Used in SCIFs

Limited information is openly available about specific SCIF construction criteria, but it is possible to find general parameters. Groups such as the National Counterintelligence and Security Center (NCSC) and United States General Service Administration publish reports on policies governing SCIF construction and assessment. While not every SCIF must be built to the same standard as the criteria varies by agency using the space, sources such as [67] [68] provide insight into what kind of construction a basic model should include. These models could then be updated by researchers at government organizations to fit their unique situation.

NCSC-approved SCIFs within the United States must abide by a set of physical and technical security requirements outlined in Intelligence Community Standards (ICDs) 705-01 and 705-02, and in Intelligence Community Directive (ICD) 705. ICD 705 and

ICS 705-01 lists criteria and best practices for physical and technical standards for SCIFs while ICS 705-02 are the standards for accrediting and using SCIFs [69]. [69] itself is the technical specification that provides details about how sensitive compartmented information (SCI) is protected against unauthorized collection. Its rules encapsulate perimeter walls, floors, ceilings, doors, and windows [67] [69]. Within these categories, the SCIF or room use case has further construction and material consideration. Generally, the guidance recommends perimeter walls be comprised of three layers of 5/8 inch-thick gypsum wallboard, acoustical sealant, acoustic fill material, 16 gauge continuous track, metal or wood studs, and grout [69]. In certain cases, concrete and steel may also be used [69]. [67] also lists RF protection should be used, and the number of windows should be minimized whenever possible.

The documents require RF protection be installed on perimeter walls if the other techniques do not provide enough attention on their own. In this case, the best practices for shielding RF emanations, as described in [70], must be observed. Information about the extent to which RF emanations within a SCIF must be attenuated to comply with the standards is not openly available.

4.2: Scope of Work

This thesis is focused on using ray tracing to model the use of cooperative beamforming in enhancing IMD security in a corporate environment, with the intent that these techniques could be extended to a SCIF provided additional material properties and construction requirements. The IMDs are assumed to be using Bluetooth Low Energy (BLE), as most do in actuality, at a 2.4GHz center frequency with a bandwidth of 2MHz, per the BLE standard [71]. It is assumed that the intended transmitters' locations are known information. Through ray tracing and experimenting with different layouts of cooperative jamming nodes, coverage profiles will be developed.

Success will be measured by the extent to which the intended transmitters are able to limit an unintended receiver from intercepting IMD information. The received signal strength outside of the intended link will be measured, and various architectures will be compared to determine the optimal layout. An iterative approach will be employed in creating the simulations wherein the system's complexity and building layout's detail will be increased with each pass.

Chapter 5: Results

5.1: Simulation Setup

These simulations were run in Remcom's Wireless InSite ray tracing tool, in which a model office building was created. Within the building, walls are made of drywall, windows are made of glass, the ground is made of concrete, desks are made of wood, and chairs are modelled using dry sand as dry sand's dielectric constant closely matched that of plastic, and plastic was not included in the given materials database. Transmitters were placed on the office desks to simulate where BLE devices might be within an actual office setting. Each transmitter was set to output a 2.4GHz signal with a 2MHz bandwidth and 0dBm transmit power per the BLE standard [71]. Each transmitter had a directional antenna that was set to point toward one of several locations for each test. A limited number of transmitters, beam directions, and layouts were tested due to time, resource, and Remcom license availability limitations. The beamwidths were chosen after testing a variety of options and configurations, and finding a narrow beamwidth was needed for these scenarios.

Figure 4 and Figure 5 show the setup for the two transmitter tests through a top-down view of the Wireless InSite office building. Figure 6 and Figure 7 show the setup for the three transmitter tests through a top-down view of the Wireless InSite office building.

The concrete floor is light blue, chairs are green, and wooden desks are brown. The doorways, walls, and windows are shown as black lines. The transmitters labeled Tx1 and Tx2 are on top of desks, which have a height of 0.9m to match a typical office desk height. Each transmitter's antenna points at one of five locations labeled A through E. Each plot's naming convention is the point at which Tx1 points, followed by the point at which Tx2 points. For example, if Tx1 was aimed at A while Tx2 was aimed at B, the plot would reference run AB.

This paper assumes the employee with an IMD is typically found in their office during the workday. As such, an "area of interest" is the floorspace over which the employee is expected to occupy, and thus over which cooperative jamming interactions were examined. Figure 5 shows the areas of interest: the smallest area comprising the two desk chairs, the next smallest area comprising the entire office, and the largest area that includes some of the hallway and nearby office. The largest area was included to see the potential impact on other building occupants. These are referred to as the primary, secondary, and tertiary areas of interest respectively.

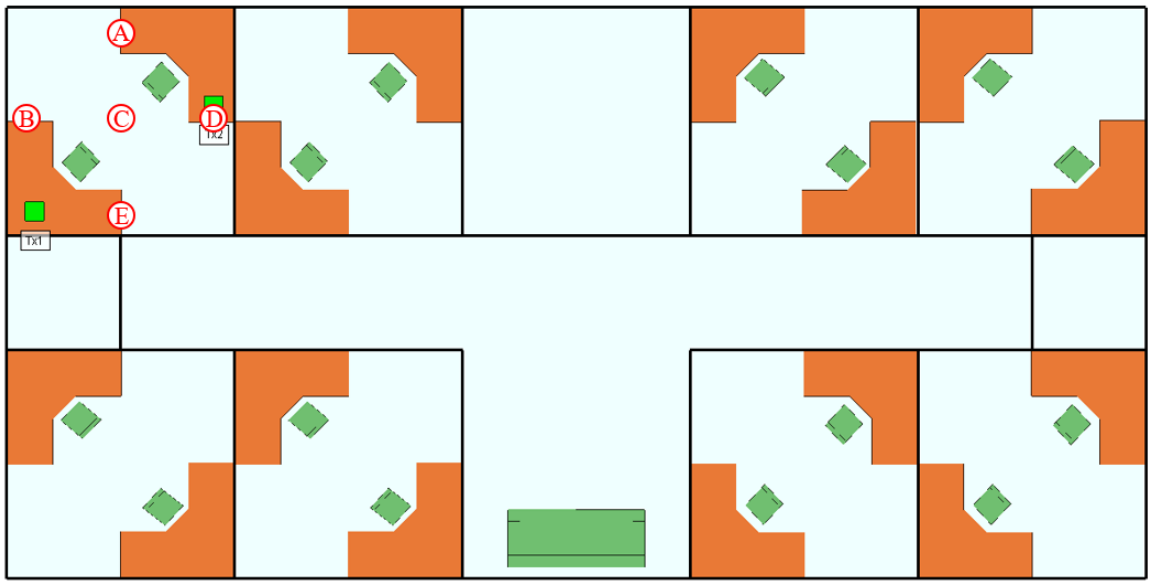

Figure 4: Two transmitter setup

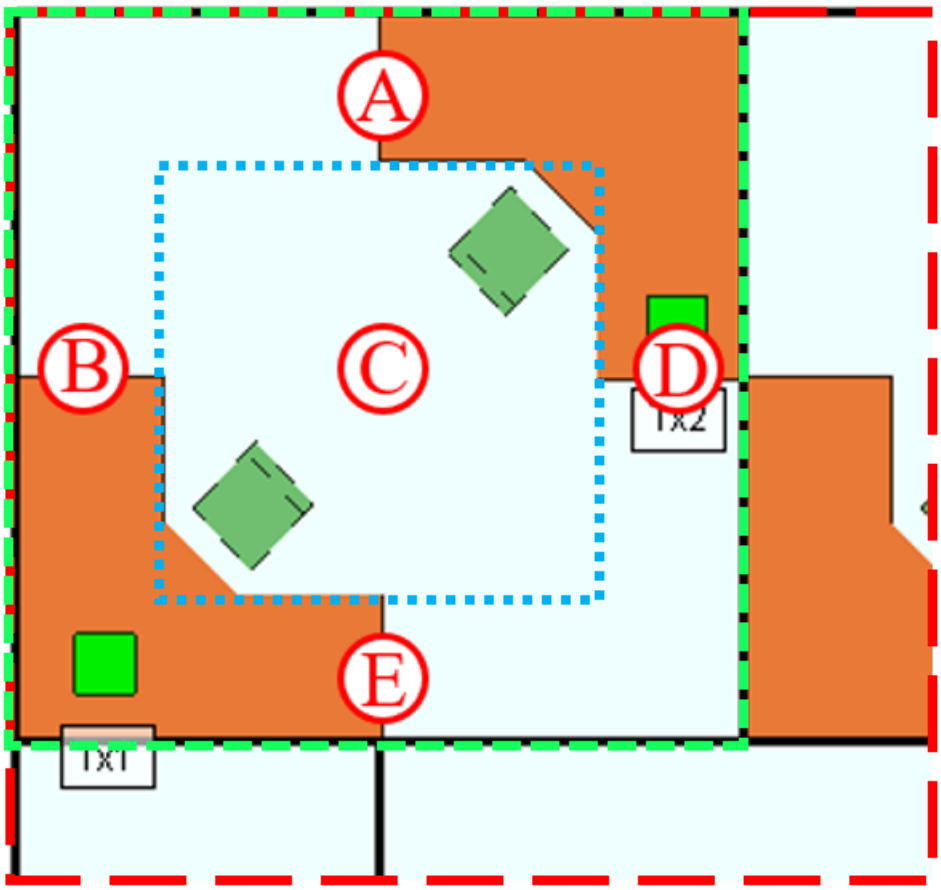

Figure 5: Closeup of the areas of interest for the two transmitter test. The blue line with short dashes shows the 1.8m x 1.8m area of interest, the green line with medium dashes shows the 3m x 3m area of interest, and the red line with long dashes shows the 7.5m x 6m area of interest.

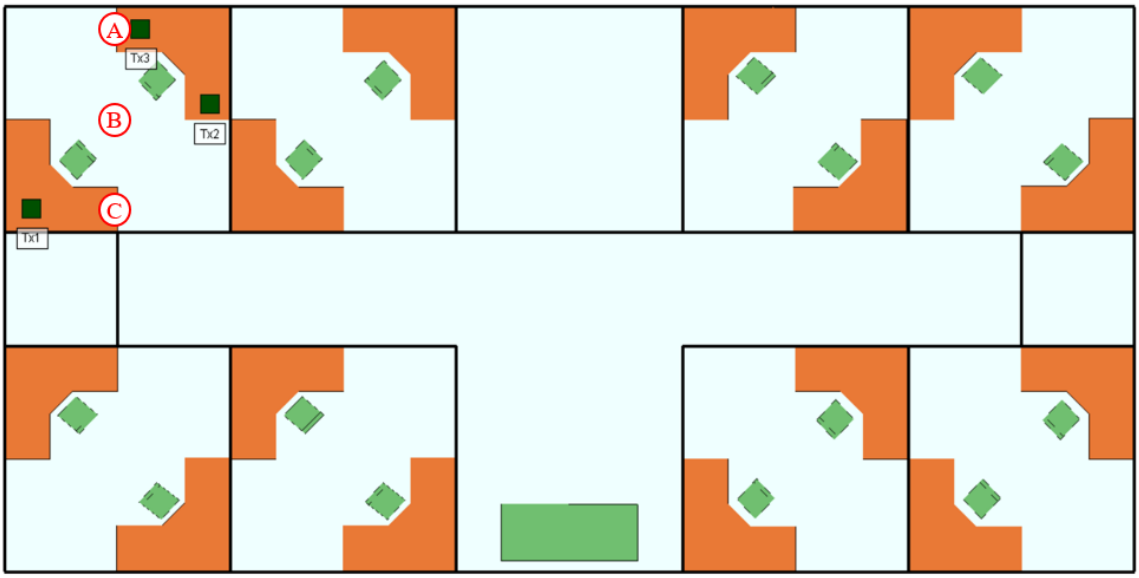

Figure 6: Three transmitter setup

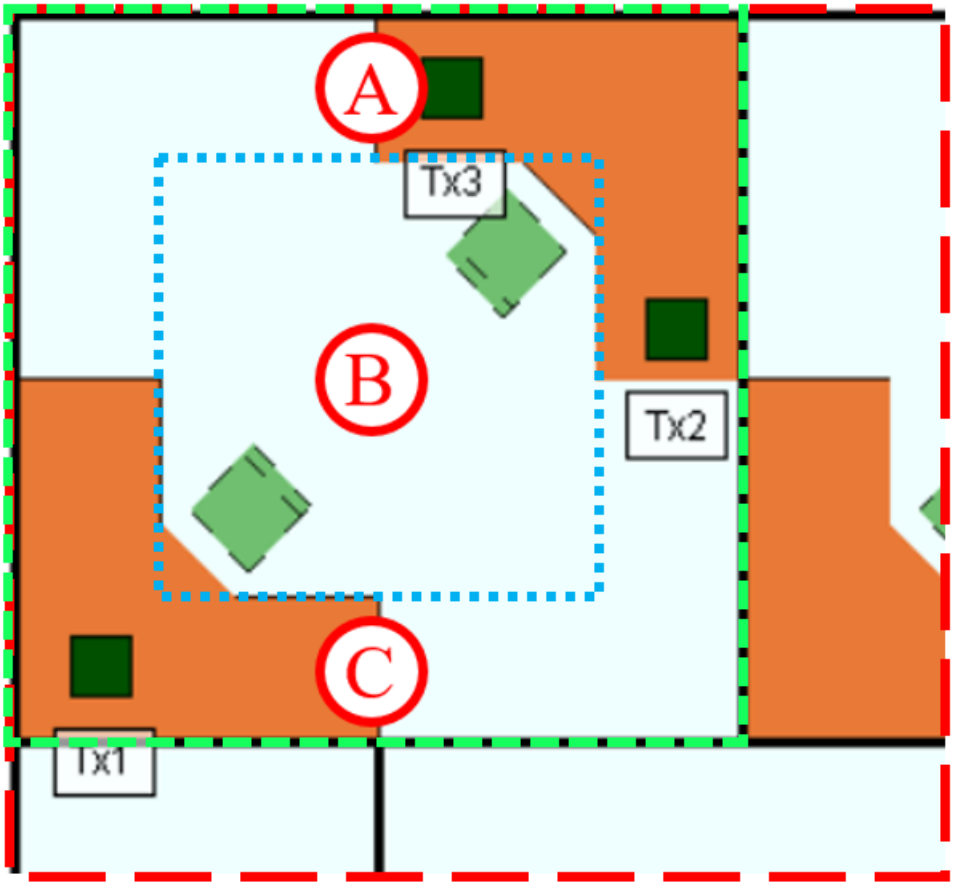

Figure 7: Closeup of the area of interest for the three transmitter test. The blue line with short dashes shows the 1.8m x 1.8m area of interest, the green line with medium dashes shows the 3m x 3m area of interest, and the red line with long dashes shows the 7.5m x 6m area of interest.

5.2: Primary Area of Interest

5.2.1: Two Transmitters, 0.5° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

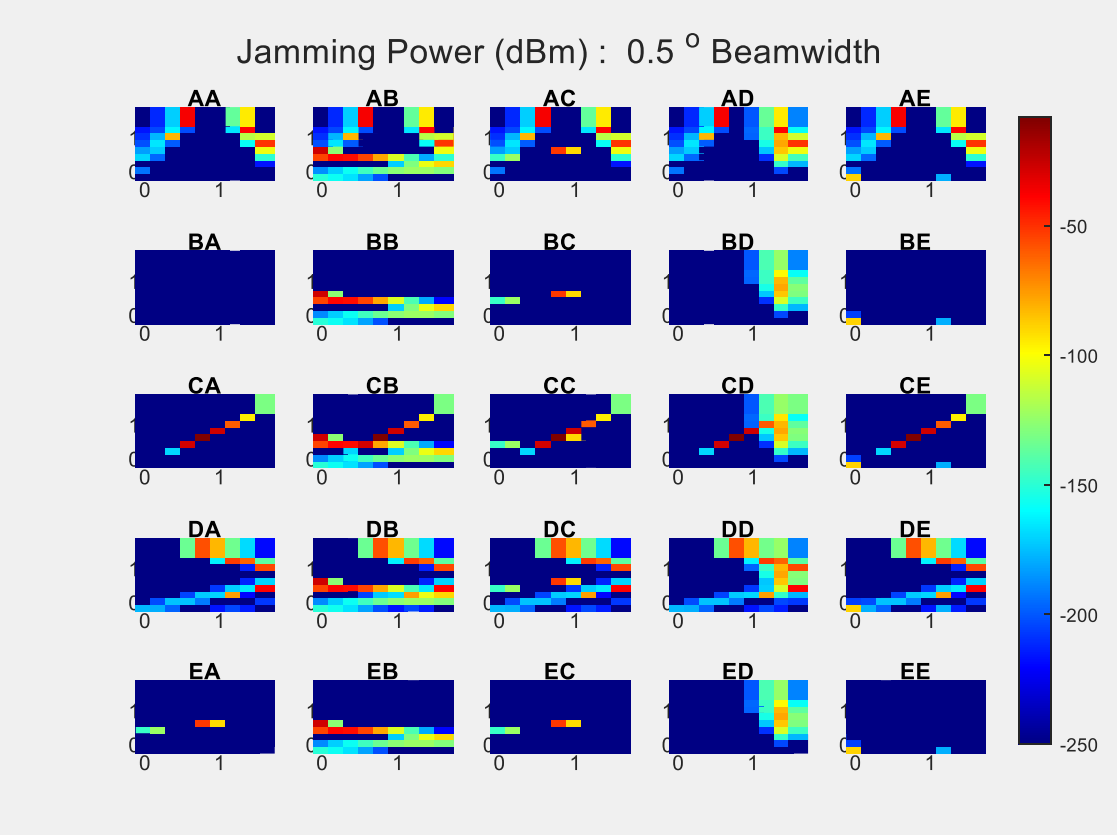

Figure 8: Total jamming power for the two transmitter, 0.5° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AA	95.06	4.94	0.00
AB	86.42	12.35	1.23
AC	93.83	6.17	0.00
AD	91.36	8.64	0.00
AE	93.83	6.17	0.00
BA	100.00	0.00	0.00
BB	91.36	7.41	1.23
BC	98.77	1.23	0.00
BD	96.30	3.70	0.00
BE	98.77	1.23	0.00
CA	95.06	1.23	3.70
CB	87.65	7.41	4.94
CC	95.06	1.23	3.70
CD	91.36	4.94	3.70
CE	93.83	2.47	3.70
DA	91.36	8.64	0.00
DB	82.72	16.05	1.23
DC	90.12	9.88	0.00
DD	87.65	12.35	0.00
DE	90.12	9.88	0.00
EA	98.77	1.23	0.00
EB	91.36	7.41	1.23
EC	98.77	1.23	0.00
ED	96.30	3.70	0.00
EE	98.77	1.23	0.00

Table 3: Floorspace covered by low, medium, and high amounts of jamming for the two transmitter, 0.5° beamwidth cases

5.2.2: Two Transmitters, 1 ° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

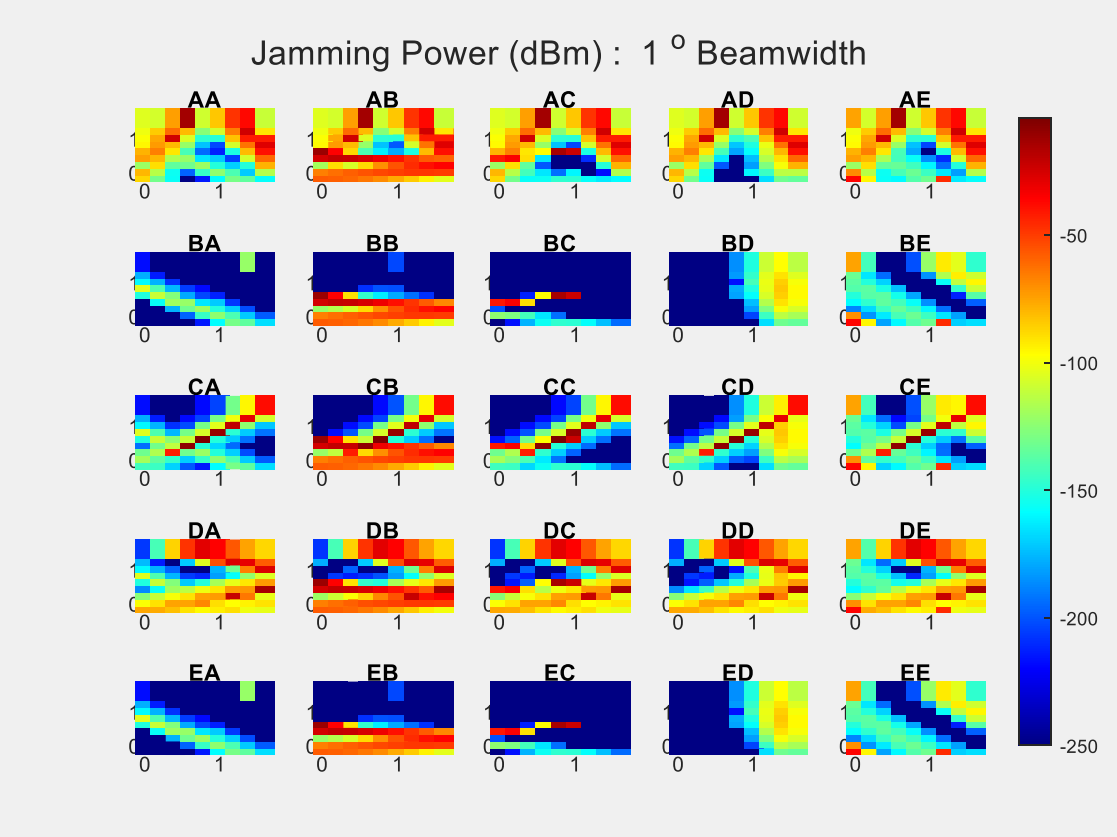

Figure 9: Total jamming power for the two transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AA	62.96	32.10	4.94
AB	32.10	56.79	11.11
AC	59.26	33.33	7.41
AD	62.96	32.10	4.94
AE	60.49	34.57	4.94
BA	100.00	0.00	0.00
BB	59.26	34.57	6.17
BC	93.83	3.70	2.47
BD	95.06	4.94	0.00
BE	95.06	4.94	0.00
CA	91.36	2.47	6.17
CB	51.85	37.04	11.11
CC	86.42	6.17	7.41
CD	87.65	6.17	6.17
CE	86.42	7.41	6.17
DA	62.96	29.63	7.41
DB	41.98	44.44	13.58
DC	56.79	33.33	9.88
DD	60.49	32.10	7.41
DE	60.49	32.10	7.41
EA	100.00	0.00	0.00
EB	59.26	34.57	6.17
EC	93.83	3.70	2.47
ED	95.06	4.94	0.00
EE	95.06	4.94	0.00

Table 4: Floorspace covered by low, medium, and high amounts of jamming for the two transmitter, 1° beamwidth cases

5.2.3: Three Transmitters

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

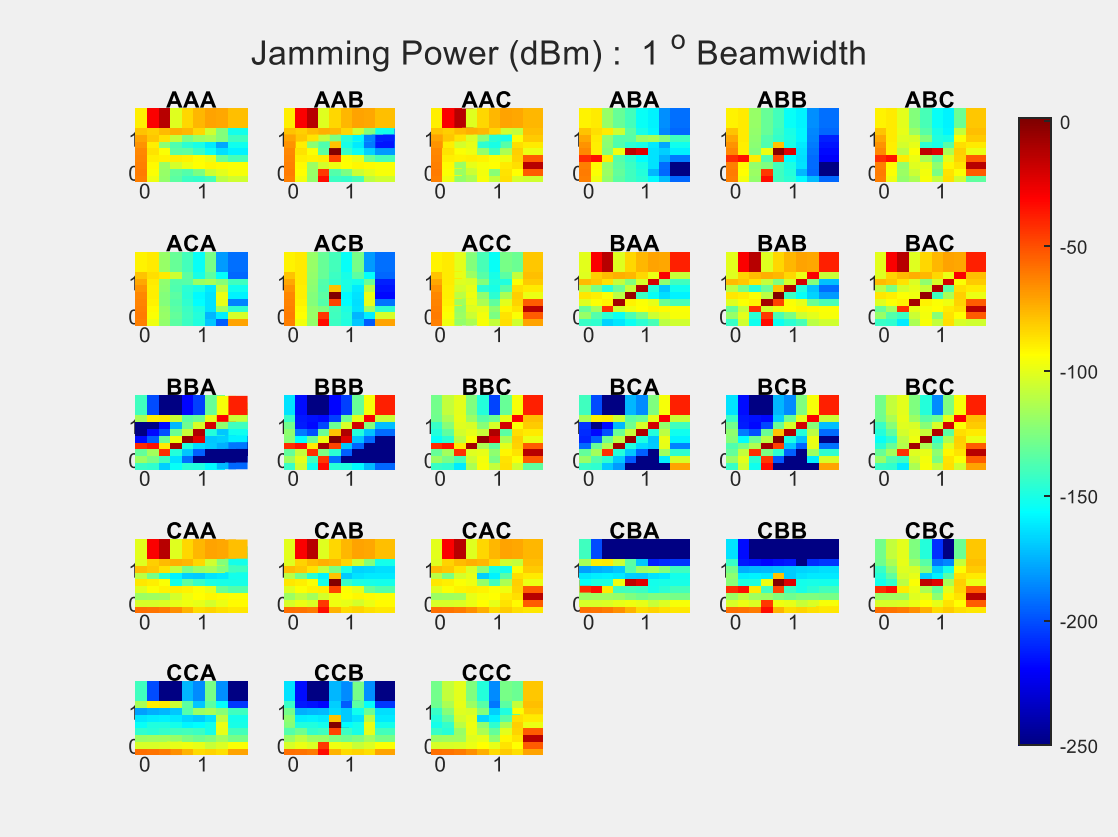

Figure 10: Total jamming power for the three transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AAA	66.67	30.86	2.47
AAB	60.49	35.80	3.70
AAC	50.62	45.68	3.70
ABA	77.78	19.75	2.47
ABB	74.07	23.46	2.47
ABC	62.96	33.33	3.70
ACA	81.48	18.52	0.00
ACB	76.54	22.22	1.23
ACC	66.67	32.10	1.23
BAA	71.60	19.75	8.64
BAB	66.67	24.69	8.64
BAC	55.56	34.57	9.88
BBA	83.95	8.64	7.41
BBB	81.48	11.11	7.41
BBC	71.60	19.75	8.64
BCA	87.65	6.17	6.17
BCB	85.19	8.64	6.17
BCC	75.31	17.28	7.41
CAA	66.67	30.86	2.47
CAB	61.73	34.57	3.70
CAC	51.85	44.44	3.70
CBA	80.25	17.28	2.47
CBB	79.01	18.52	2.47
CBC	67.90	28.40	3.70
CCA	86.42	13.58	0.00
CCB	83.95	14.81	1.23
CCC	74.07	24.69	1.23

Table 5: Floorspace covered by low, medium, and high amounts of jamming for the three transmitter experiments

5.2.4: Results Comparison

Table 6 compares the runs with two transmitters. The difference in coverage between the half and one degree beamwidth runs demonstrates that the cooperative jammers have stronger, more comprehensive coverage when the transmitters are set to have one degree beamwidths rather than half degree. On average, the one degree beamwidth runs had 19.45% less area categorized as low jamming coverage, 15.11% more area categorized as medium jamming coverage, and 4.35% less area categorized as high jamming coverage.

Table 7 compares the average percentage of low, medium, and high jamming coverage across all 25 runs for both the 1º and 0.5º two transmitter setups.

Run	Half Degree Beamwidth			One Degree Beamwidth			Difference		
	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	Low	Medium	High
AA	95.06	4.94	0.00	62.96	32.10	4.94	-32.10	27.16	4.94
AB	86.42	12.35	1.23	30.86	58.02	11.11	-55.56	45.68	9.88
AC	93.83	6.17	0.00	59.26	33.33	7.41	-34.57	27.16	7.41
AD	91.36	8.64	0.00	61.73	33.33	4.94	-29.63	24.69	4.94
AE	93.83	6.17	0.00	60.49	34.57	4.94	-33.33	28.40	4.94
BA	100.00	0.00	0.00	100.00	0.00	0.00	0.00	0.00	0.00
BB	91.36	7.41	1.23	59.26	34.57	6.17	-32.10	27.16	4.94
BC	98.77	1.23	0.00	93.83	3.70	2.47	-4.94	2.47	2.47
BD	96.30	3.70	0.00	95.06	4.94	0.00	-1.23	1.23	0.00
BE	98.77	1.23	0.00	95.06	4.94	0.00	-3.70	3.70	0.00
CA	95.06	1.23	3.70	91.36	2.47	6.17	-3.70	1.23	2.47
CB	87.65	7.41	4.94	51.85	37.04	11.11	-35.80	29.63	6.17
CC	95.06	1.23	3.70	86.42	6.17	7.41	-8.64	4.94	3.70
CD	91.36	4.94	3.70	87.65	6.17	6.17	-3.70	1.23	2.47
CE	93.83	2.47	3.70	86.42	7.41	6.17	-7.41	4.94	2.47
DA	91.36	8.64	0.00	62.96	29.63	7.41	-28.40	20.99	7.41
DB	82.72	16.05	1.23	41.98	44.44	13.58	-40.74	28.40	12.35
DC	90.12	9.88	0.00	56.79	33.33	9.88	-33.33	23.46	9.88
DD	87.65	12.35	0.00	60.49	32.10	7.41	-27.16	19.75	7.41
DE	90.12	9.88	0.00	60.49	32.10	7.41	-29.63	22.22	7.41
EA	98.77	1.23	0.00	100.00	0.00	0.00	1.23	-1.23	0.00
EB	91.36	7.41	1.23	59.26	34.57	6.17	-32.10	27.16	4.94
EC	98.77	1.23	0.00	93.83	3.70	2.47	-4.94	2.47	2.47
ED	96.30	3.70	0.00	95.06	4.94	0.00	-1.23	1.23	0.00
EE	98.77	1.23	0.00	95.06	4.94	0.00	-3.70	3.70	0.00

Table 6: Two transmitter results comparison

The comparison of the total amount of floorspace covered by all the possible transmitter pointing directions for the two-transmitter runs is summarized in Table 7 and shown visually in Figure 11. This explores the extent to which this setup could mitigate bad actors' interactions with IMDs in a dynamically changing environment. The difference row shows 50.62% less floorspace falls into the low jamming coverage category, 33.33% more floorspace falls into the medium coverage category, and 17.28% more floorspace falls into the high jamming coverage category when using 1° beamwidths rather than 0.5° beamwidths.

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 0.5°	70.37	24.69	4.94
Combined, 1°	19.75	58.02	22.22
Difference	-50.62	33.33	17.28

Table 7: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter setup

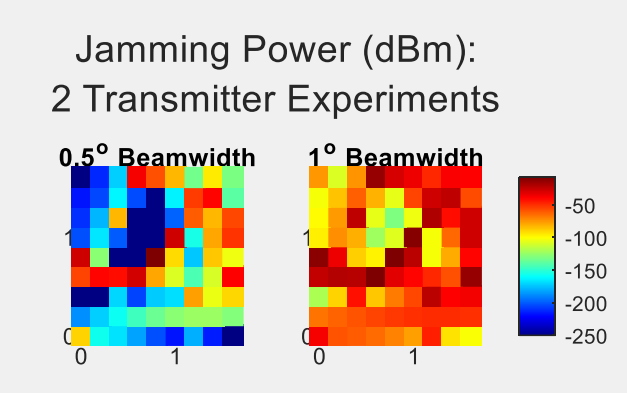

Figure 11: Combined received power statistics for the two transmitter experiments

The combined two transmitter, 1° beamwidth results are compared to that of the three transmitter setup in Table 8 to determine which setup performed best. The three transmitter experiments had only three possible beam pointing directions to keep the number of setup permutations tractable. The possible options were at the top center, middle, and bottom center of the room. Because there were three transmitters and three possible pointing directions, there were a total of 27 experiments. Thus, to compare the three transmitter and two transmitter experiments, only the two transmitter experiments with beam pointing directions in the same locations were considered. Because of this, the available data is reduced from 25 experiments (two transmitters with five possible pointing directions) to 9 experiments (two transmitters with three possible pointing directions). Figure 12 compares the combined coverage of 25 three transmitter experiments with the 9 comparable two transmitter experiments.

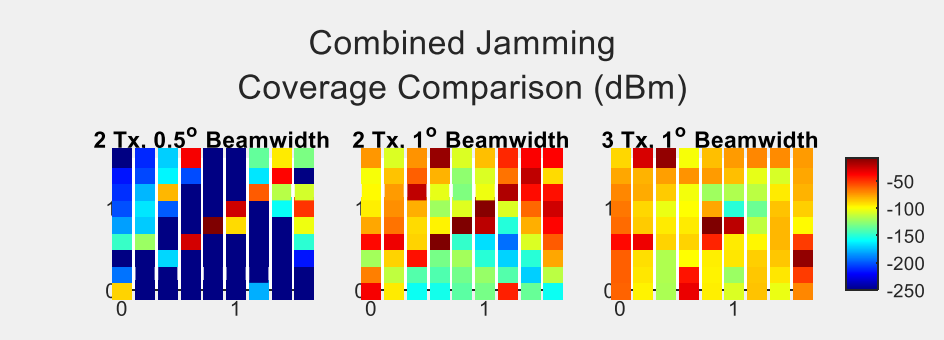

Figure 12: Combined floorspace covered by jamming in the two transmitter and 3 transmitter setups

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 2 TXs	51.85	37.04	11.11
Combined, 3 TXs	40.74	53.09	6.17
Difference	-11.11	16.05	-4.94

Table 8: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter, 1° beamwidth and 3 transmitter, 1° beamwidth setups

The three-transmitter setup has more overall coverage, but the two transmitter setup has more area covered by a higher jamming power.

5.3: Secondary Area of Interest

5.3.1: Two Transmitters, 0.5° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

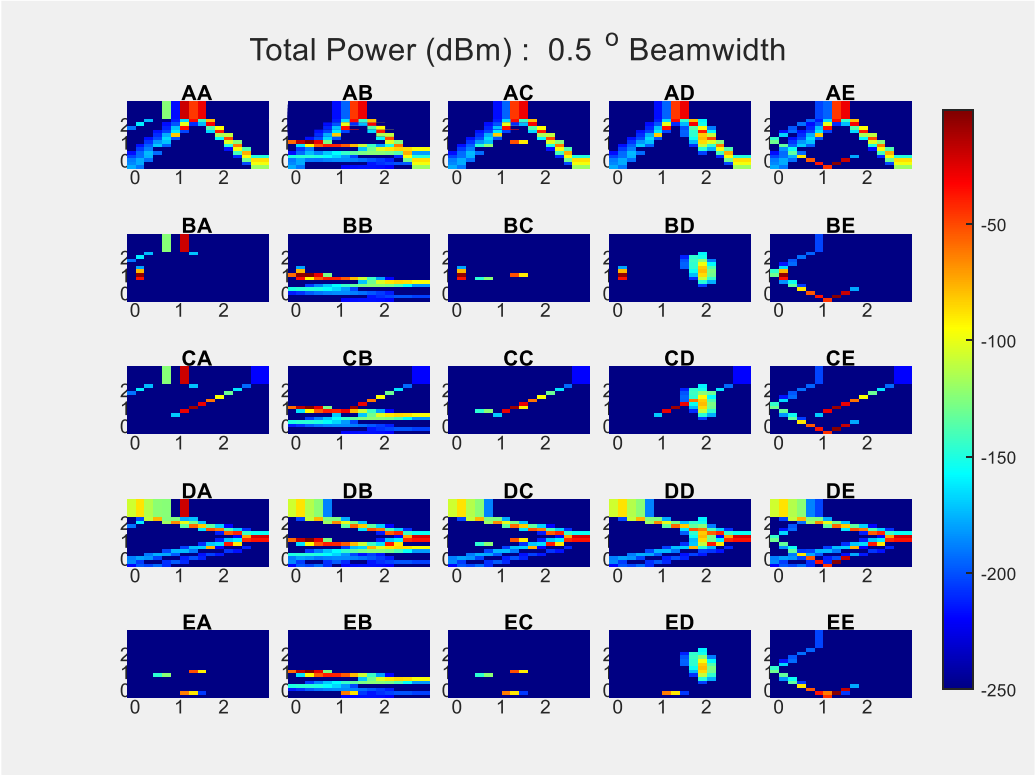

Figure 13: Total jamming power for the two transmitter, 0.5° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AA	94.22	4.89	0.89
AB	89.33	8.89	1.78
AC	94.22	5.33	0.44
AD	93.33	6.22	0.44
AE	92.00	6.67	1.33
BA	98.22	0.89	0.89
BB	93.78	4.89	1.33
BC	98.22	1.33	0.44
BD	97.33	2.22	0.44
BE	96.00	2.67	1.33
CA	97.78	0.44	1.78
CB	93.33	4.00	2.67
CC	98.22	0.44	1.33
CD	96.89	1.78	1.33
CE	95.56	2.22	2.22
DA	92.44	6.67	0.89
DB	87.56	10.67	1.78
DC	92.44	7.11	0.44
DD	91.56	8.00	0.44
DE	90.22	8.44	1.33
EA	98.67	1.33	0.00
EB	93.78	4.89	1.33
EC	98.67	1.33	0.00
ED	97.78	2.22	0.00
EE	96.89	2.22	0.89

Table 9: Floorspace covered by low, medium, and high amounts of jamming for the 0.5° beamwidth cases

5.3.2: Two Transmitters, 1 ° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

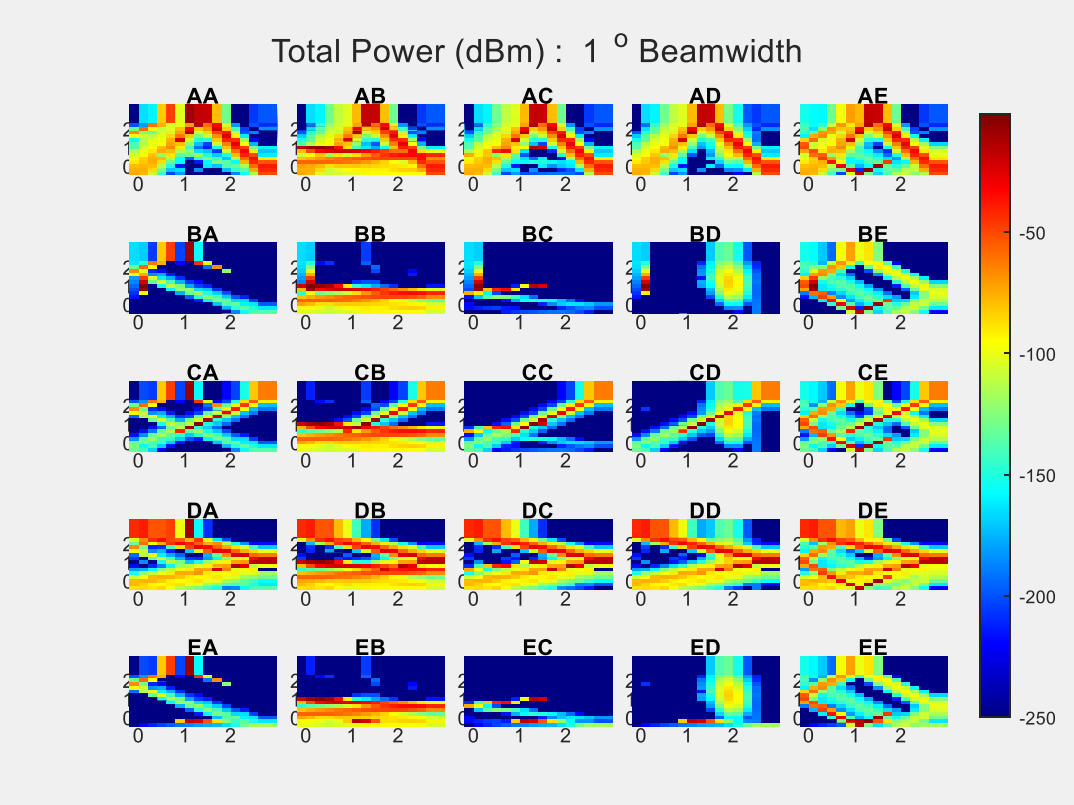

Figure 14: Total jamming power for the two transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AA	64.00	32.00	4.00
AB	47.11	45.78	7.11
AC	64.89	30.67	4.44
AD	66.22	30.22	3.56
AE	56.89	37.33	5.78
BA	93.78	4.44	1.78
BB	68.44	27.11	4.44
BC	94.67	3.11	2.22
BD	96.00	2.67	1.33
BE	87.56	8.89	3.56
CA	90.67	6.67	2.67
CB	64.89	29.78	5.33
CC	92.00	5.33	2.67
CD	93.33	4.44	2.22
CE	83.11	12.44	4.44
DA	66.22	28.44	5.33
DB	48.00	43.56	8.44
DC	64.89	29.33	5.78
DD	67.11	28.00	4.89
DE	59.11	33.78	7.11
EA	93.78	4.89	1.33
EB	67.56	28.00	4.44
EC	94.67	3.56	1.78
ED	96.00	3.11	0.89
EE	87.11	10.22	2.67

Table 10: Floorspace covered by low, medium, and high amounts of jamming for the 1° beamwidth cases

5.3.3: Three Transmitters, 1 ° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each

combination of transmitter pointing directions.

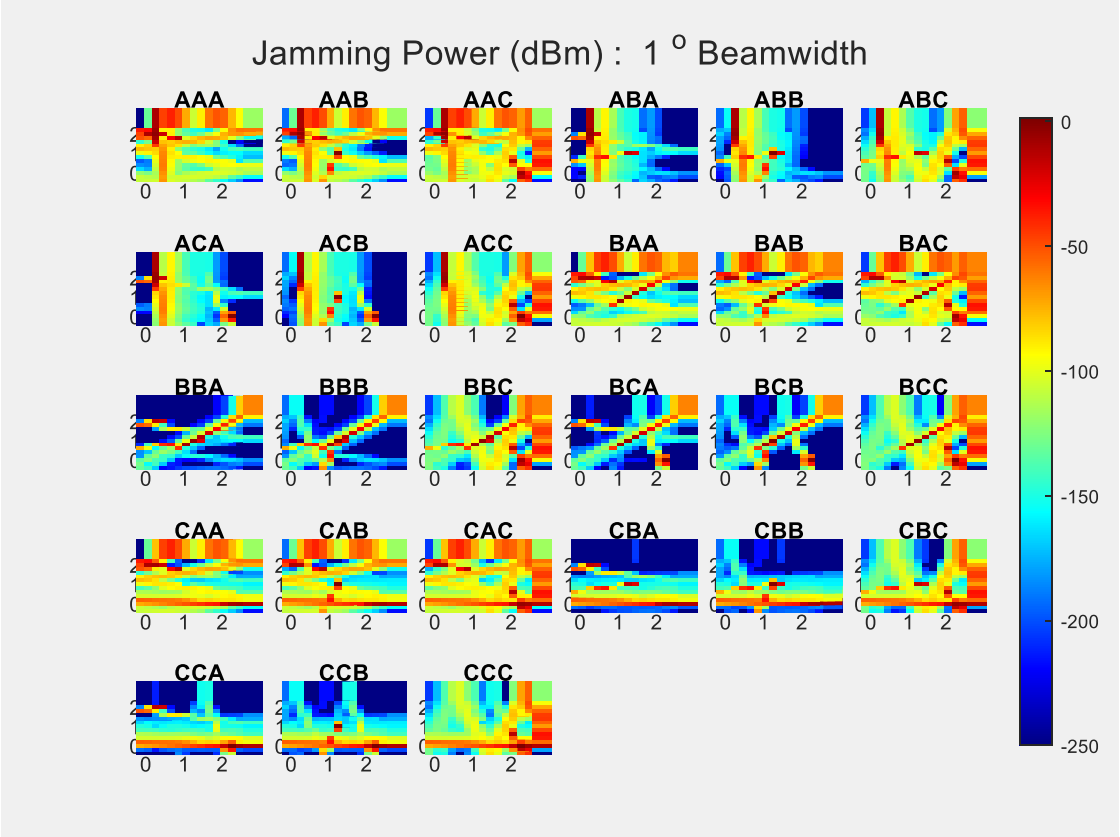

Figure 15: Total jamming power for the three transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
AAA	71.11	24.89	4.00
AAB	68.44	27.56	4.00
AAC	56.00	38.67	5.33
ABA	84.00	12.44	3.56
ABB	83.11	13.78	3.11
ABC	67.11	28.00	4.89
ACA	84.00	12.89	3.11
ACB	82.67	14.22	3.11
ACC	68.44	27.56	4.00
BAA	74.22	21.33	4.44
BAB	72.44	23.56	4.00
BAC	60.00	34.22	5.78
BBA	88.44	8.00	3.56
BBB	88.89	8.44	2.67
BBC	74.67	20.89	4.44
BCA	88.44	8.00	3.56
BCB	88.89	8.44	2.67
BCC	76.00	20.00	4.00
CAA	64.89	31.11	4.00
CAB	63.56	32.44	4.00
CAC	52.44	42.67	4.89
CBA	80.89	15.56	3.56
CBB	82.22	15.11	2.67
CBC	67.56	28.44	4.00
CCA	83.11	14.22	2.67
CCB	84.00	13.78	2.22
CCC	70.22	26.67	3.11

Table 11: Floorspace covered by low, medium, and high amounts of jamming for the three transmitter experiments

5.3.4: Results Comparison

Table 12 compares the runs with two transmitters. The difference in coverage between the half and one degree beamwidth runs demonstrates that the cooperative jammers have stronger, more comprehensive coverage when the transmitters are set to have one degree beamwidths rather than half degree. On average, the one degree beamwidth runs had 16.44% less area categorized as low jamming coverage, 14.63% more area categorized as medium jamming coverage, and 2.90% more area categorized as high jamming coverage. Table 13 compares the average percentage of low, medium, and high jamming coverage across all 25 runs for both the 1º and 0.5º two transmitter setups.

Run	Half Degree Beamwidth			One Degree Beamwidth			Difference		
	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	Low	Medium	High
AA	94.22	4.89	0.89	64.00	32.00	4.00	19.11	4.89	3.11
AB	89.33	8.89	1.78	47.11	45.78	7.11	-42.22	36.89	5.33
AC	94.22	5.33	0.44	64.89	30.67	4.44	-29.33	25.33	4.00
AD	93.33	6.22	0.44	66.22	30.22	3.56	-27.11	24.00	3.11
AE	92.00	6.67	1.33	56.89	37.33	5.78	-35.11	30.67	4.44
BA	98.22	0.89	0.89	93.78	4.44	1.78	-4.44	3.56	0.89
BB	93.78	4.89	1.33	68.44	27.11	4.44	-25.33	22.22	3.11
BC	98.22	1.33	0.44	94.67	3.11	2.22	-3.56	1.78	1.78
BD	97.33	2.22	0.44	96.00	2.67	1.33	-1.33	0.44	0.89
BE	96.00	2.67	1.33	87.56	8.89	3.56	-8.44	6.22	2.22
CA	97.78	0.44	1.78	90.67	6.67	2.67	-7.11	6.22	0.89
CB	93.33	4.00	2.67	64.89	29.78	5.33	-28.44	25.78	2.67
CC	98.22	0.44	1.33	92.00	5.33	2.67	-6.22	4.89	1.33
CD	96.89	1.78	1.33	93.33	4.44	2.22	-3.56	2.67	0.89
CE	95.56	2.22	2.22	83.11	12.44	4.44	-12.44	10.22	2.22
DA	92.44	6.67	0.89	66.22	28.44	5.33	-26.22	21.78	4.44
DB	87.56	10.67	1.78	48.00	43.56	8.44	-39.56	32.89	6.67
DC	92.44	7.11	0.44	64.89	29.33	5.78	-27.56	22.22	5.33
DD	91.56	8.00	0.44	67.11	28.00	4.89	-24.44	20.00	4.44
DE	90.22	8.44	1.33	59.11	33.78	7.11	-31.11	25.33	5.78
EA	98.67	1.33	0.00	93.78	4.89	1.33	-4.89	3.56	1.33
EB	93.78	4.89	1.33	67.56	28.00	4.44	-26.22	23.11	3.11
EC	98.67	1.33	0.00	94.67	3.56	1.78	-4.00	2.22	1.78
ED	97.78	2.22	0.00	96.00	3.11	0.89	-1.78	0.89	0.89
EE	96.89	2.22	0.89	87.11	10.22	2.67	-9.78	8.00	1.78

Table 12: Two transmitter results comparison

The comparison of the total amount of floorspace covered by all the possible transmitter pointing directions for the two-transmitter runs is summarized in Table 7. The difference row shows 53.33% less floorspace falls into the low jamming coverage category, 40.89% more floorspace falls into the medium coverage category, and 12.44% more floorspace falls into the high jamming coverage category when using 1° beamwidths rather than 0.5° beamwidths.

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 0.5°	76.00	19.11	4.89
Combined, 1°	22.67	60.00	17.33
Difference	-53.33	40.89	12.44

Table 13: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter setup

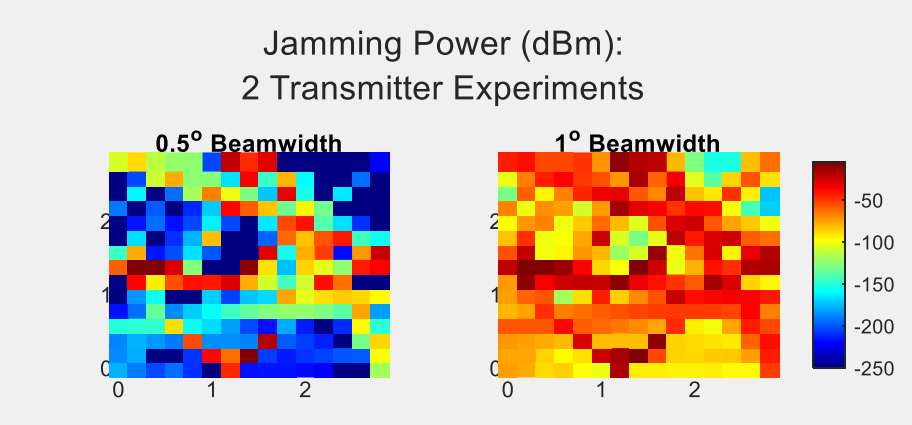

Figure 16: Combined received power statistics for the two transmitter experiments

The combined two transmitter, 1° beamwidth results are compared to that of the three transmitter setup in Table 13Table 8 to determine which setup performed best. The three transmitter experiments had only three possible beam pointing directions to keep the number of setup permutations tractable. The possible options were at the top center, middle, and bottom center of the room. Because there were three transmitters and three possible pointing directions, there were a total of 27 experiments. Thus, to compare the three transmitter and two transmitter experiments, only the two transmitter experiments with beam pointing directions in the same locations were considered. Because of this, the available data is reduced from 25 experiments (two transmitters with five possible pointing directions) to 9 experiments (two transmitters with three possible pointing directions). Figure 17Figure 12 compares the combined coverage of 25 three transmitter experiments with the 9 comparable two transmitter experiments.

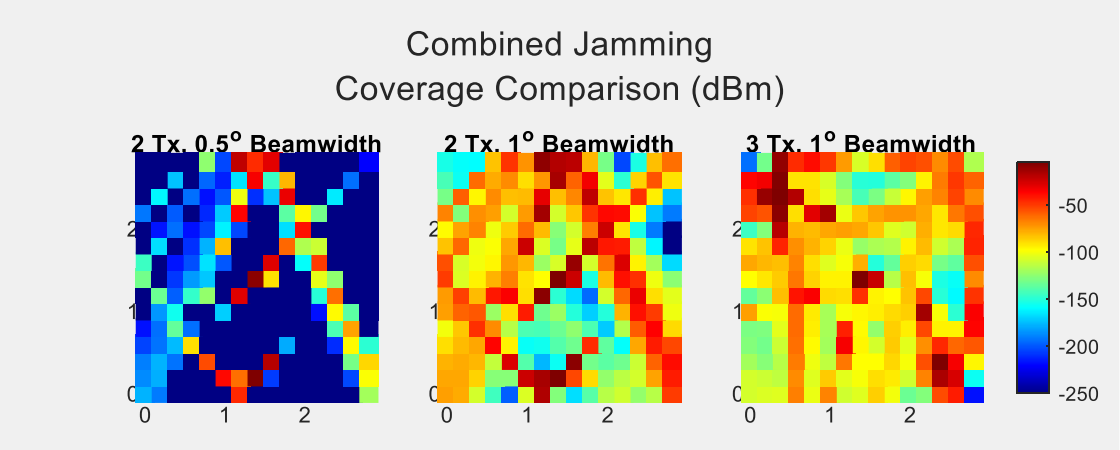

Figure 17: Combined floorspace covered by jamming in the two transmitter and 3 transmitter setups

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 2 TXs	47.11	44.00	8.89
Combined, 3 TXs	48.44	44.89	6.67
Difference	1.33	0.89	-2.22

Table 14: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter, 1° beamwidth and 3 transmitter, 1° beamwidth setups

5.4: Tertiary Area of Interest

5.4.1: Two Transmitters, 0.5° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

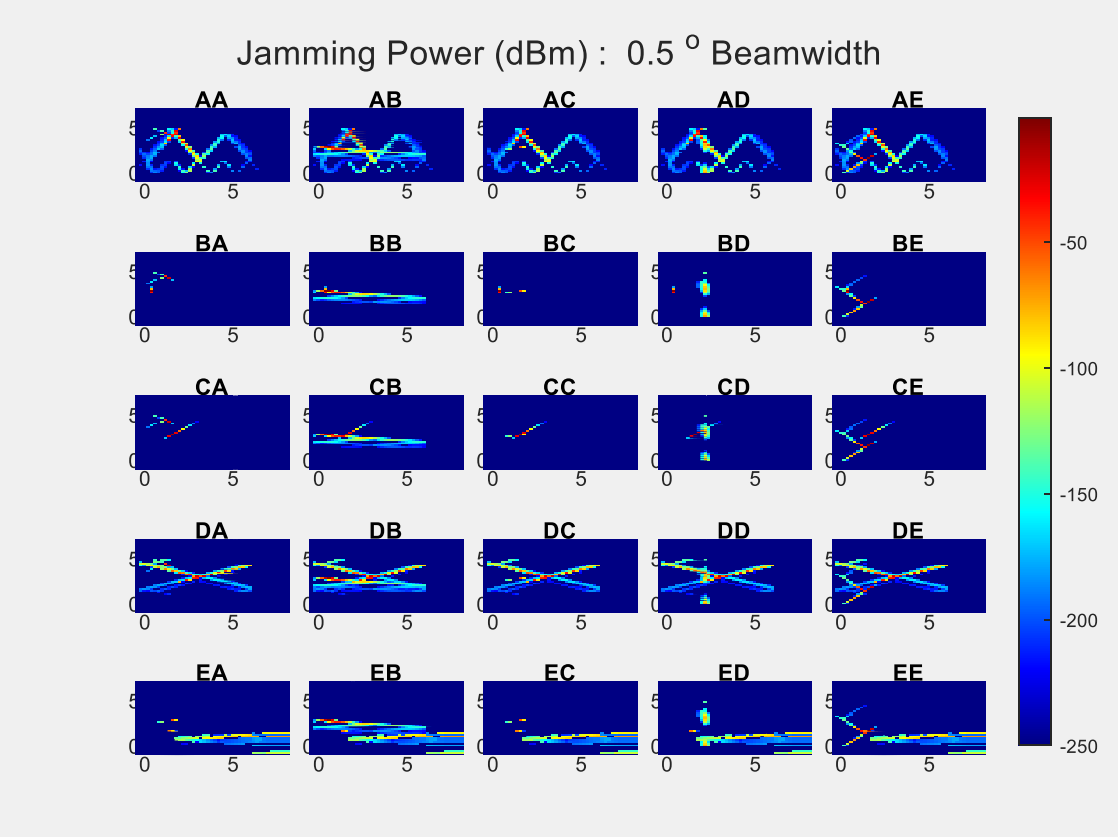

Figure 18: Total jamming power for the two transmitter, 0.5° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Coverage	% High Jamming Coverage
AA	98.59	1.16	0.25
AB	97.77	1.82	0.41
AC	98.68	1.16	0.17
AD	98.35	1.49	0.17
AE	98.01	1.65	0.33
BA	99.59	0.25	0.17
BB	98.84	0.91	0.25
BC	99.67	0.25	0.08
BD	99.34	0.58	0.08
BE	99.01	0.74	0.25
CA	99.50	0.17	0.33
CB	98.76	0.74	0.50
CC	99.67	0.08	0.25
CD	99.26	0.50	0.25
CE	98.92	0.66	0.41
DA	97.52	2.15	0.33
DB	96.69	2.81	0.50
DC	97.60	2.15	0.25
DD	97.27	2.48	0.25
DE	96.94	2.65	0.41
EA	98.43	1.57	0.00
EB	97.52	2.23	0.25
EC	98.43	1.57	0.00
ED	98.10	1.90	0.00
EE	97.85	1.99	0.17

Table 15: Floorspace covered by low, medium, and high amounts of jamming for the 0.5° beamwidth cases

5.4.2: Two Transmitters, 1 ° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

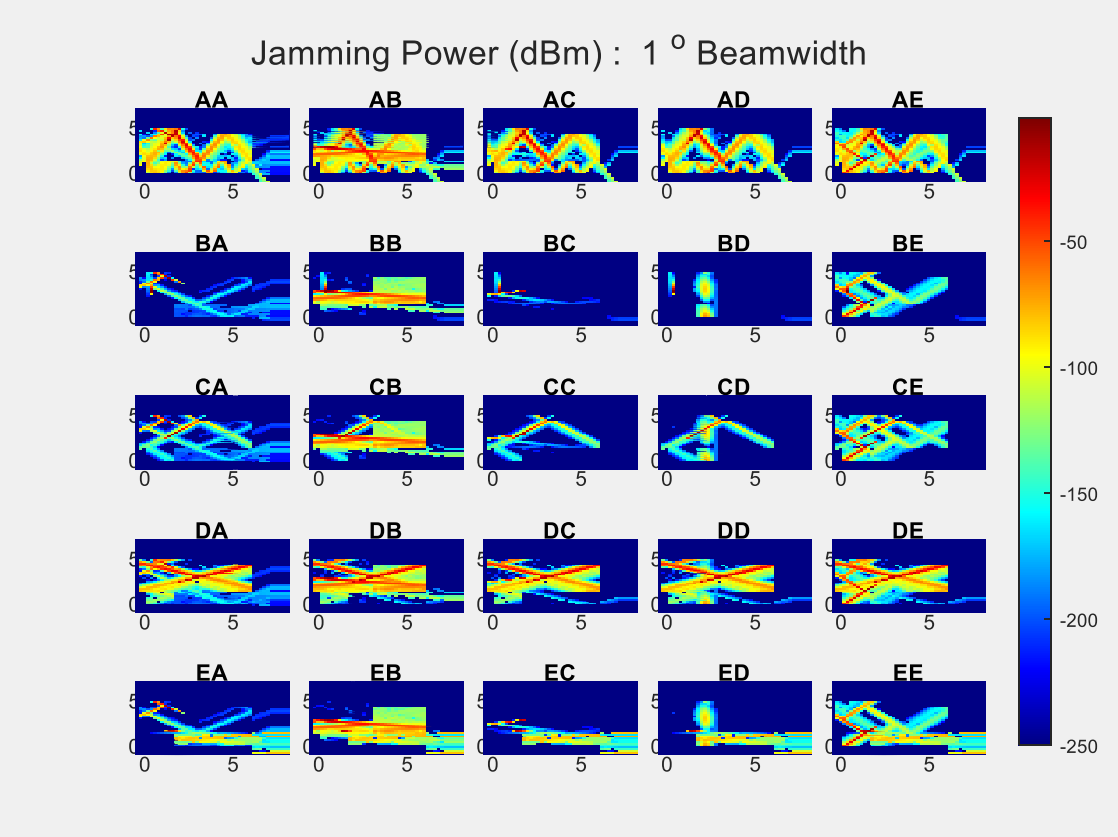

Figure 19: Total jamming power for the two transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Coverage	% High Jamming Coverage
AA	82.05	16.87	1.08
AB	73.70	24.73	1.57
AC	82.71	16.21	1.08
AD	82.96	16.13	0.91
AE	80.07	18.36	1.57
BA	98.26	1.32	0.41
BB	86.85	12.32	0.83
BC	98.92	0.66	0.41
BD	98.84	0.91	0.25
BE	95.78	3.31	0.91
CA	97.27	2.15	0.58

CB	85.77	13.23	0.99
CC	98.01	1.49	0.50
CD	97.93	1.65	0.41
CE	94.54	4.38	1.08
DA	84.53	13.81	1.65
DB	76.76	21.09	2.15
DC	84.62	13.73	1.65
DD	84.70	13.81	1.49
DE	81.80	16.05	2.15
EA	93.88	5.79	0.33
EB	82.30	16.87	0.83
EC	94.54	5.13	0.33
ED	94.46	5.38	0.17
EE	91.32	7.94	0.74

Table 16: Floorspace covered by low, medium, and high amounts of jamming for the 1° beamwidth cases

5.4.3: Three Transmitters, 1° Beamwidth

The following data shows the spatial relationship between transmitter pointing direction and jamming strength. The origin is at the bottom left of the area of interest. Both axes show meters away from the origin. The data shows the total jamming power for each combination of transmitter pointing directions.

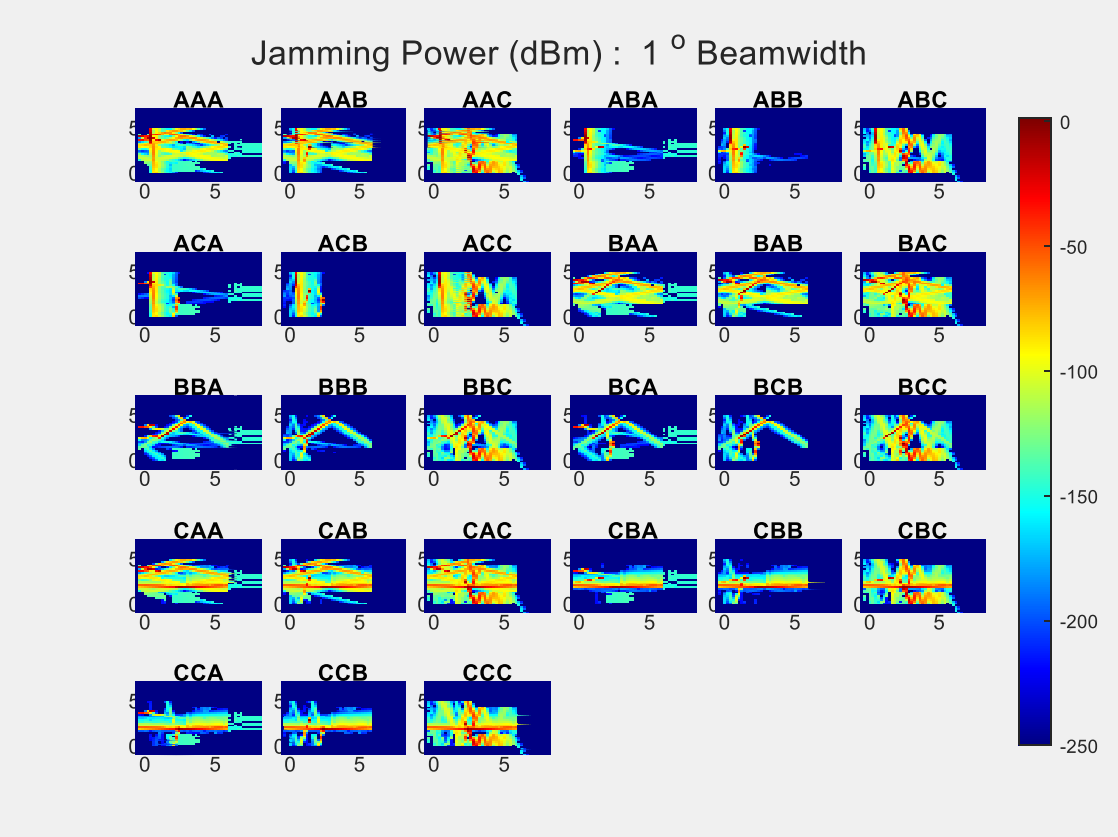

Figure 20: Total jamming power for the three transmitter, 1° beamwidth experiment

The percentage of floorspace covered by a relatively "low," "medium," and "high" amount of jamming for each transmitter's pointing direction contributes to the assessment of this setup's effectiveness. The Bluetooth standard's requirements for received power informed the thresholds used in this work. It is generally accepted that a strong connection is above -30dBm, and a device cannot be detected at -90dBm or less [72] [73] [74].

Run	% Low Jamming Coverage	% Medium Coverage	% High Jamming Coverage
AAA	88.42	10.42	1.16
AAB	88.01	10.84	1.16
AAC	79.65	18.53	1.82
ABA	95.62	3.47	0.91
ABB	95.53	3.64	0.83
ABC	86.10	12.32	1.57
ACA	95.29	3.89	0.83
ACB	95.12	4.05	0.83
ACC	86.02	12.57	1.41
BAA	89.91	9.10	0.99
BAB	89.66	9.43	0.91
BAC	81.47	16.87	1.65
BBA	97.19	2.15	0.66
BBB	97.35	2.15	0.50
BBC	88.50	10.26	1.24
BCA	96.86	2.48	0.66
BCB	97.02	2.48	0.50
BCC	88.42	10.42	1.16
CAA	84.53	14.14	1.32
CAB	84.37	14.31	1.32
CAC	76.26	21.84	1.90
CBA	92.22	6.70	1.08
CBB	92.56	6.53	0.91
CBC	83.37	15.05	1.57
CCA	92.31	6.78	0.91
CCB	92.56	6.62	0.83
CCC	83.54	15.05	1.41

Table 17: Floorspace covered by low, medium, and high amounts of jamming for the three transmitter experiments

5.4.4: Results Comparison

Table 6 compares the runs with two transmitters. The difference in coverage between the half and one degree beamwidth runs demonstrates that the cooperative jammers have stronger, more comprehensive coverage when the transmitters are set to have one degree beamwidths rather than half degree. On average, the one degree beamwidth runs had 9.51% less area categorized as a low jamming coverage, 8.79% more area categorized as medium coverage, and 0.72% more area categorized as high jamming coverage.

Run	Half Degree Beamwidth			One Degree Beamwidth			Difference		
	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage	Low	Medium	High
AA	98.59	1.16	0.25	82.05	16.87	1.08	-16.54	15.72	0.83
AB	97.77	1.82	0.41	73.70	24.73	1.57	-24.07	22.91	1.16
AC	98.68	1.16	0.17	82.71	16.21	1.08	-15.96	15.05	0.91
AD	98.35	1.49	0.17	82.96	16.13	0.91	-15.38	14.64	0.74
AE	98.01	1.65	0.33	80.07	18.36	1.57	-17.95	16.71	1.24
BA	99.59	0.25	0.17	98.26	1.32	0.41	-1.32	1.08	0.25
BB	98.84	0.91	0.25	86.85	12.32	0.83	-11.99	11.41	0.58
BC	99.67	0.25	0.08	98.92	0.66	0.41	-0.74	0.41	0.33
BD	99.34	0.58	0.08	98.84	0.91	0.25	-0.50	0.33	0.17
BE	99.01	0.74	0.25	95.78	3.31	0.91	-3.23	2.56	0.66
CA	99.50	0.17	0.33	97.27	2.15	0.58	-2.23	1.99	0.25
CB	98.76	0.74	0.50	85.77	13.23	0.99	-12.99	12.49	0.50
CC	99.67	0.08	0.25	98.01	1.49	0.50	-1.65	1.41	0.25
CD	99.26	0.50	0.25	97.93	1.65	0.41	-1.32	1.16	0.17
CE	98.92	0.66	0.41	94.54	4.38	1.08	-4.38	3.72	0.66
DA	97.52	2.15	0.33	84.53	13.81	1.65	-12.99	11.66	1.32
DB	96.69	2.81	0.50	76.76	21.09	2.15	-19.93	18.28	1.65
DC	97.60	2.15	0.25	84.62	13.73	1.65	-12.99	11.58	1.41
DD	97.27	2.48	0.25	84.70	13.81	1.49	-12.57	11.33	1.24
DE	96.94	2.65	0.41	81.80	16.05	2.15	-15.14	13.40	1.74
EA	98.43	1.57	0.00	93.88	5.79	0.33	-4.55	4.22	0.33
EB	97.52	2.23	0.25	82.30	16.87	0.83	-15.22	14.64	0.58
EC	98.43	1.57	0.00	94.54	5.13	0.33	-3.89	3.56	0.33
ED	98.10	1.90	0.00	94.46	5.38	0.17	-3.64	3.47	0.17
EE	97.85	1.99	0.17	91.32	7.94	0.74	-6.53	5.96	0.58

Table 18: Two transmitter results comparison

The comparison of the total amount of floorspace covered by all the possible transmitter pointing directions for the two-transmitter runs is summarized in Table 7. The difference row shows 33.33% less floorspace falls into the low jamming coverage category, 30.11% more floorspace falls into the medium coverage category, and 3.23% more floorspace falls into the high jamming coverage category when using 1° beamwidths rather than 0.5° beamwidths.

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 0.5°	92.47	6.37	1.16
Combined, 1°	59.14	36.48	4.38
Difference	-33.33	30.11	3.23

Table 19: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter setup

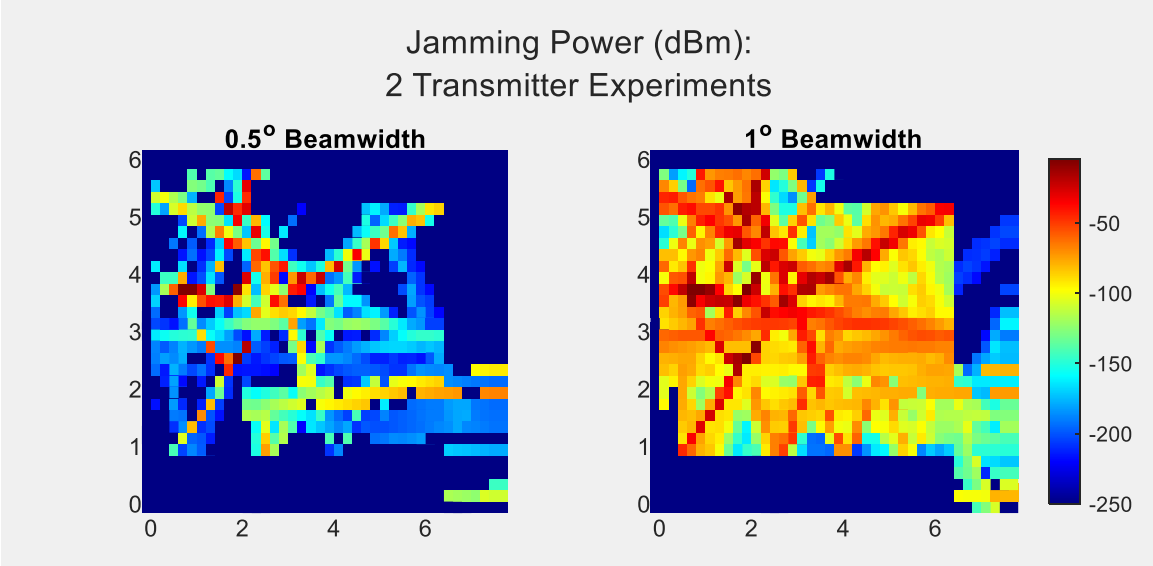

Figure 21: Combined received power statistics for the two transmitter experiments

The combined two transmitter, 1° beamwidth results are compared to that of the three transmitter setup in Table 20 to determine which setup performed best. The three transmitter experiments had only three possible beam pointing directions to keep the number of setup permutations tractable. The possible options were at the top center, middle, and bottom center of the room. Because there were three transmitters and three possible pointing directions, there were a total of 27 experiments. Thus, to compare the three transmitter and two transmitter experiments, only the two transmitter experiments with beam pointing directions in the same locations were considered. Because of this, the available data is reduced from 25 experiments (two transmitters with five possible pointing directions) to 9 experiments (two transmitters with three possible pointing directions). Figure 22 compares the combined coverage of 25 three transmitter experiments with the 9 comparable two transmitter experiments.

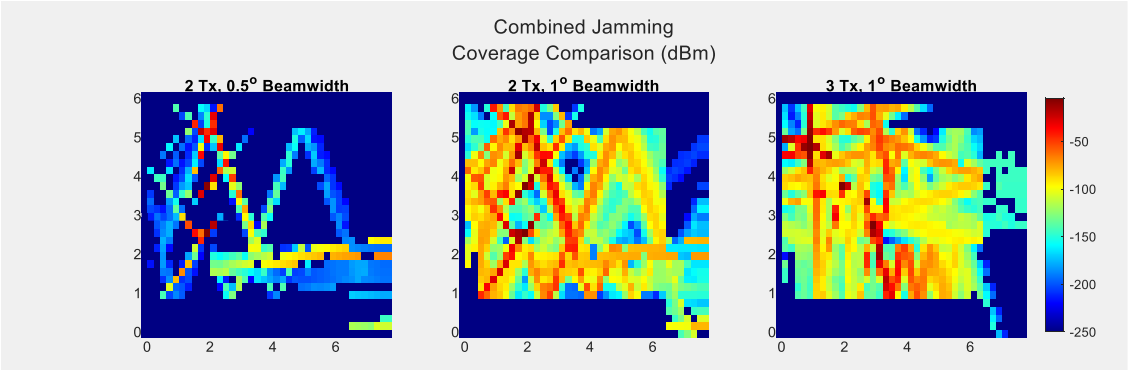

Figure 22: Combined floorspace covered by jamming in the two transmitter and three transmitter setups

Run	% Low Jamming Coverage	% Medium Jamming Coverage	% High Jamming Coverage
Combined, 2 TXs	73.95	23.82	2.23
Combined, 3 TXs	77.50	20.43	2.07
Difference	3.56	-3.39	-0.17

Table 20: Combined floorspace covered by low, medium, and high amounts of jamming in the two transmitter, 1° beamwidth and 3 transmitter, 1° beamwidth setups

5.5: Discussion of Results

Comparing the two transmitter runs demonstrates that the cooperative jammers have stronger, more comprehensive coverage when the transmitters are set to have one degree beamwidths rather than half degree. However, additional experimentation showed that wider beamwidths tend to flood the entire space, leaving no spaces free of jamming. Thus, more jammers would be needed to create an interference pattern allowing the IMD and programming device to communicate while blocking bad actors. However, as seen in the three transmitter results, adding transmitters may improve cooperative jamming efficacy, but additional coverage is not guaranteed. Adding transmitters may not be realistic in practice as more friendly jammers may improve coverage and have less stringent beamwidth requirements, but system costs will be significantly raised as each office would need numerous jamming nodes. Further, there may be concerns about the jamming nodes' security themselves and whether they could be targeted to make the environment advantageous to a hacker, or exploited so a hacker obtains unauthorized information.

Chapter 6: Summary and Future Work

This work discussed central issues with IMD security point to underlying, fundamental concerns that cooperative jamming can address. Chapter 1 provided background information on IMDs, their prevalence in the U.S. population, their security limitations which manufacturers attribute to limited onboard resources and battery power, and how the therapies they provide necessitates their use despite growing security concerns. Chapter 2 discussed proposed security solutions for IMDs, mainly in spaces that contain privileged or classified information. Some of the suggested techniques are unlikely to be put into practice due to potential HIPAA violations or the possibility of erasing important health information from the devices that was collected while the patient was in an area dealing with privileged information. Further, medical device companies are not incentivized to bolster their IMDs' security measures as their current models already abide by federal regulations, and making significant design changes would not only increase time to production but would incur substantial costs. Lastly, it is impractical to suggest removing IMD wireless capabilities altogether, thus this research focused on how mitigation techniques could be applied that account for IMDs having limited resources.

Chapter 3 introduced the principles of beamforming and cooperative jamming, citing studies that pointed to this technique's efficacy. This paper focused on how cooperative jamming applies to IMD communications, specifically in an office environment. Further, rather than using empirical models, the Remcom Wireless InSite ray tracing software was used to better understand how the environment impacts the cooperative jammers, which is discussed in Chapter 4. Because IMDs have limited power and range, this paper assumed the IMD, offboard programming device, cooperative jammers, and eavesdropper are in relatively close proximity with one another, but the eavesdropper CSI is not known. As IMD use cases assume the programmer is nearby, the friendly nodes will not need to act as relays and can instead focus all their power on jamming. The number of cooperative jammers will be low to simulate the number of Bluetooth-enabled devices an individual might have in a workspace or office setting, like a personal phone, smart watch, or laptop, and realistic power constraints will be observed.

The results in Chapter 5 provided an understanding of how a few friendly nodes with narrow beamwidths impact IMD security in an office environment. These results indicate cooperative jamming for IMD usage is possible and can be accomplished with a small number of friendly nodes over a given area. Further, introducing more jamming nodes may not improve system performance enough to warrant the additional device cost, or potential risk of adding another wireless device to the space.

Future work may consider the addition of several more nodes into the environment, perhaps upward of ten, for use cases where adding transmitters into the environment outweighs the risk of introducing new wireless devices, and perhaps in spaces whose protection warrants additional funding for jamming nodes. Higher jamming power levels could also be considered, although the jamming power should not exceed FCC transmitting regulations. Looking into dynamically changing environments with moving IMD users or other people of interest would present an interesting challenge, although this would be more realistic. Future work may also examine how similar protocols could be adapted for IMD users in classified spaces where introducing a wireless device is under more rigorous scrutiny. In turn, this body of information may inform how companies or individuals can protect their proprietary and personal information.

References

[1] Food and Drug Administration, "Wireless Medical Devices," 4 September 2018. [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/wireless-medical-devices. [Accessed 5 December 2022].

[2] S. Gupta, "Implantable Medical Devices -- Cyber Risks and Mitigation Approaches," in *NIST Cyber Physical Systems Workshop*, Gaithersburg, 2012.

[3] AMA Journal of Ethics , "Implantable Material and Device Regulation," September 2021. [Online]. Available: https://journalofethics.ama-assn.org/issue/implantable-material-and-device-regulation. [Accessed 5 December 2022].

[4] SkyQuest Technology Consulting Pvt. Ltd. , "Implantable Medical Devices Market to Reach $157.07 Billion by 2028," 27 June 2022. [Online]. Available: https://www.globenewswire.com/en/news-release/2022/06/27/2469658/0/en/Implantable-Medical-Devices-Market-to-Reach-157-07-Billion-by-2028-Competitive-Pricing-Aging-Population-and-Aggressive-Marketing-to-Play-Key-Role.html. [Accessed 5 December 2022].

[5] C. Brito, L. Pinto, V. Marinho, S. Paiva and P. Pinto, "A Review on Recent Advances in Implanted Medical Devices Security," in *16th Iberian Conference on Information Systems and Technologies (CISTI)*, Chaves, 2021.

[6] S. Anthony, "Black Hat hacker details lethal wireless attack on insulin pumps," ExtremeTech, 5 August 2011. [Online]. Available: https://www.extremetech.com/extreme/92054-black-hat-hacker-details-wireless-attack-on-insulin-pumps. [Accessed 5 December 2022].

[7] G. Haddow, S. H. E. Harmon and L. Bilman, "Implantable Smart Technologies (IST): Defining the 'Sting' in Data and Device," *Health Care Analysis,* vol. 24, no. 3, pp. 210-227, 2016.

[8] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30-39, 2008.

[9] The MITRE Corporation, "Playbook for Threat Modeling Medical Devices," The MITRE Corporation, McLean, 2021.

[10] S. S. Dutta, "Insight into Implantable Medical Devices," News-Medical.Net, 30 June 2022. [Online]. Available: https://www.news-medical.net/health/Insight-into-Implantable-Medical-Devices.aspx#:~:text=The%20most%20common%20examples%20of,implants%2C%20and%20intrauterine%20contraceptive%20devices.. [Accessed 5 December 2022].

[11] O. G. Vickers, P. R. Culmer, G. H. Isaac, R. W. Kay, M. P. Shuttleworth, T. Board and S. Williams, "Is in vivo sensing in a total hip replacement a possibility? A review on past systems and future challenges," *Progress in Biomedical Engineering*, vol. 3, no. 4, 2021.

[12] C. Campbell, "What You Should Do About the URGENT/11 VxWorks Vulnerabilities," Extreme Networks, 19 April 2021. [Online]. Available: https://www.extremenetworks.com/extreme-networks-blog/what-you-should-do-about-the-urgent-11-vxworks-vulnerabilities/. [Accessed 5 December 2022].

[13] Armis, "URGENT/11," 15 December 2020. [Online]. Available: https://www.armis.com/research/urgent11/. [Accessed 5 December 2022].

[14] Cybersecurity and Infrastructure Security Agency, "SweynTooth Vulnerabilities," 4 March 2020. [Online]. Available: https://www.cisa.gov/uscert/ics/alerts/ics-alert-20-063-01. [Accessed 5 December 2022].

[15] M. E. Garbelini, S. Chattopadhyay and C. Wang, "SweynTooth," 14 July 2020. [Online]. Available: https://asset-group.github.io/disclosures/sweyntooth/. [Accessed 5 December 2022].

[16] B. P. Dunleavy, "Pacemakers, insulin pumps can be hacked, experts say," United Press International, 1 June 2022. [Online]. Available: https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/7041653656330/. [Accessed 5 December 2022].

[17] B. M. Kuehn, "Pacemaker Recall Highlights Security Concerns for Implantable Devices," *Circulation,* vol. 138, no. 15, pp. 1597-1598, 2018.

[18] J. Radcliffe, "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System," in *Black Hat USA* , Caesars Palace , 2011.

[19] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *IEEE Symposium on Security and Privacy,* pp. 129-142, 2008.

[20] Food and Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," April 2022. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions. [Accessed 5 December 2022].

[21] D. Tillman, "What Should the Public Know About Implantable Material and Device Innovation in the US?," *AMA Journal of Ethics,* vol. 23, no. 9, pp. 697-705, 2021.

[22] Z. Chen, P. O'Donnell, E. Ottman, S. Trieu and A. Michaels, "An Invisible Insider Threat: The Risks of Implanted Medical Devices in Secure Spaces," National Intelligence University, Washington, D.C., 2020.

[23] C. Franklin, "A Most Personal Threat: Implantable Devices in Secure Spaces," Dark Reading, 8 July 2020. [Online]. Available: https://www.darkreading.com/iot/a-most-personal-threat-implantable-devices-in-secure-spaces. [Accessed 5 December 2022].

[24] U.S. Department of State, "Security Clearances," [Online]. Available: https://www.state.gov/security-clearances#:~:text=The%20purpose%20of%20a%20security%20clearance%20is%20to%20allow%20an,to%20classified%20national%20security%20information.. [Accessed 5 December 2022].

[25] Department of Defense, "Policy Memorandum 07-13," Doral, 2013.

[26] U.S. Equal Employment Opportunity Commission, "The Rehabilitation Act of 1973," [Online]. Available: https://www.eeoc.gov/statutes/rehabilitation-act-1973. [Accessed 5 December 2022].

[27] A. Michaels, *Carrying our Insecurities with Us: the Risks of Implanted Medical Devices in Secure Spaces,* Black Hat, 2020.

[28] Committee on National Security Systems, "Directive on the Use of Mobile Devices within Secure Spaces," Ft Meade, 2017.

[29] NIST, "TEMPEST certified equipment or system," 2015. [Online]. Available: https://csrc.nist.gov/glossary/term/tempest_certified_equipment_or_system. [Accessed 6 December 2022].

[30] M. A. Siddiqi, C. Doerr and C. Strydis, "IMDfence: Architecting a Secure Protocol for Implantable Medical Devices," *IEEE Access,* vol. 8, pp. pp. 147948-147964, 2020.

[31] T. A. Nesheim, *The BLE Cloaker: Securing Implantable Medical Device Communication over BlueTooth Low Energy Links,* San Luis Obispo , California, 2015.

[32] B. Lake, M. Karpovsky and M. A. Kinsv, "Bulwark: Securing implantable medical devices communication channels," *Computers and Security,* vol. 86, pp. 498-511, 2019.

[33] W. Shi, X. Jiang, J. Hu, A. Abdelgader, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu and J. Wang, "Physical layer security techniques for data transmission for future wireless networks," *Security and Safety,* vol. 1, 2022.

[34] R. Zhang, L. Song, Z. Han and B. Jiao, "Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers," *IEEE Transactions on Vehicular Technology,* vol. 61, no. 8, pp. 2693-3704, 2012.

[35] M. Hatami, M. Jahandideh and H. Behroozi, "Two-phase cooperative jamming and beamforming for physical layer secrecy," in *2015 23rd Iranian Conference on Electrical Engineering*, 2015.

[36] H. Yu, T. Kim and H. Jafarkhani, "Wireless Secure Communication With Beamforming and Jamming in Time-Varying Wiretap Channels," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 8, pp. 2087-2100, 2018.

[37] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal,* vol. 54, no. 8, 1975.

[38] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory,* Vols. IT-24, no. 4, pp. 451-456, 2978.

[39] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *IEEE Int. Symp. Inf. Theory,* pp. 356-360, 2006.

[40] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2735-2751, 2008.

[41] H. Ma, J. Cheng, X. Wang and P. Ma, "Robust MISO Beamforming With Cooperative Jamming for Secure Transmission From Perspectives of QoS and Secrecy Rate," *IEEE Transactions on Communications,* vol. 66, no. 2, pp. 767-780, 2018.

[42] E. R. Alotaibi and K. A. HAmdi, "Optimal Cooperative Relaying and Jamming for Secure Communication," *IEEE Wireless Communication Letters,* vol. 4, no. 6, pp. 689-692, 2015.

[43] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in IEEE Transactions on Wireless Communication," *IEEE Transactions on Wireless Communications,* vol. 7, no. 6, pp. 2180-2189, 2008.

[44] H. Yu and W. Khalid, "Secure communication with beamforming and jamming in time-varying channels," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, Vienna, 2016.

[45] M. Zhang, Y. Shang and Y. Zhao, "Strategy of Relay Selection and Cooperative Jammer Beamforming in Physical Layer Security," in *2020 IEEE 92nd Vehicular Technology Conference* , Victoria, BC, Canada, 2020.

[46] Z. Yun and M. F. Iskander, "Ray Tracing for Radio Propagation Modeling: Principles and Applications," *IEEE Access*, vol. 3, pp. 1089-1100, 2015.

[47] MathWorks, "Ray Tracing for Wireless Communications," 2022. [Online]. Available: https://www.mathworks.com/help/comm/ug/ray-tracing-for-wireless-communications.html. [Accessed 9 February 2023].

[48] N. Adhikari and S. Noghanian, "Understanding Wireless Propagation Through Ray-Tracing Simulation," in *ASEE North Midwest Section Conference*, Fargo, 2013.

[49] C. Takahashi, Z. Yun, M. F. Iskander, G. Poilasne, V. Pathak and J. Fabrega, "Propagation-prediction and site-planning software for wireless communication systems," *IEEE Antennas and Propagation Magazine*, vol. 49, no. 2, pp. 52-60, April 2007.

[50] Z. Yun, Z. Zhang and M. F. Iskander, "A ray-tracing method based on the triangular grid approach and application to propagation prediction in urban environments," *IEEE Transactions on Antennas and Propagation*, vol. 50, no. 5, pp. 750-758, 2002.

[51] Remcom, "Remcom - Electromagnetic Simulation Software," [Online]. Available: https://www.remcom.com/. [Accessed 7 February 2023].

[52] Remcom, "Applications," [Online]. Available: https://www.remcom.com/electromagnetic-applications. [Accessed 7 January 2023].

[53] Remcom, "Wireless InSite," [Online]. Available: https://www.remcom.com/wireless-insite-em-propagation-software. [Accessed 7 February 2023].

[54] Remcom, "High Fidelity Ray Tracing," [Online]. Available: https://www.remcom.com/wireless-insite-models/high-fidelity-ray-tracing. [Accessed 9 February 2023].

[55] Remcom, "Antenna Modeling Software," [Online]. Available: https://www.remcom.com/wireless-insite-antennas. [Accessed 9 February 2023].

[56] Remcom, "MIMO Beamforming, Spatial Multiplexing and Diversity in Wireless InSite," [Online]. Available: https://www.remcom.com/wireless-insite-mimo-beamforming-spatial-multiplexing-and-diversity. [Accessed 9 February 2023].

[57] Remcom, "Communication System Analysis," [Online]. Available: https://www.remcom.com/wireless-insite-communication-systems-analysis. [Accessed 9 February 2023].

[58] Remcom, "Materials," [Online]. Available: https://www.remcom.com/wireless-insite-materials. [Accessed 2 February 2023].

[59] Remcom, "Engineered Electromagnetic Surfaces (EES)," [Online]. Available: https://www.remcom.com/wireless-insite-engineered-electromagnetic-surfaces-ees. [Accessed 9 February 2023].

[60] Remcom, "Diffuse Scattering," [Online]. Available: https://www.remcom.com/wireless-insite-diffuse-scattering. [Accessed 2023 February 2023].

[61] Remcom, "Feature AImport," [Online]. Available: https://www.remcom.com/wireless-insite-feature-import. [Accessed 9 February 2023].

[62] Remcom, "Geometry Caching," [Online]. Available: https://www.remcom.com/wireless-insite-geometry-caching. [Accessed 9 February 2023].

[63] Remcom, "Fast Ray-Based Methods," [Online]. Available: https://www.remcom.com/wireless-insite-fast-ray-based-methods. [Accessed 9 February 2023].

[64] Remcom, "Empirical Propagation Models," [Online]. Available: https://www.remcom.com/wireless-insite-empirical-propagation-models. [Accessed February 9 2023].

[65] Remcom, "Outputs," [Online]. Available: https://www.remcom.com/wireless-insite-outputs. [Accessed 9 February 2023].

[66] M. M. Soliman, M. E. H. Chowdhury, A. Khandakar, M. T. Islam, Y. Qiblawey, F. Musharavati and E. Z. Nezhad, "Review on Medical Implantable Antenna Technology and Imminent Research Challenges," *Sensors,* vol. 21, no. 9, 2021.

[67] National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmentalized Information Facilities," National Counterintelligence and Security Center, 2017.

[68] U.S. General Service Administration, "1025.4 ADM Sensitive Compartmented Information Facility Use (SCIF) Policy," 14 December 2020. [Online]. Available: https://www.gsa.gov/directive/sensitive-compartmented-information--facility-use-%28scif%29-policy. [Accessed 14 February 2023].

[69] National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities: Version 1.5," NCSC, 2020.

[70] SAFECOM and National Council of Statewide Interoperability Coordinators, "Radio Frequency Interference Best Practices Guidebook," SAFECOM/NCSWIC, 2020.

[71] Bluetooth, "Bluetooth Technology Overview," 2023. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/. [Accessed 14 February 2023].

[72] M. Li, "Understanding the Measures of Bluetooth RSSI," Moko Blue, 21 January 2022. [Online]. Available: https://www.mokoblue.com/measures-of-bluetooth-rssi/#:~:text=Bluetooth%20RSSI%20(Received%20Signal%20Strength,device%20scans%20for%20Bluetooth%20devices.. [Accessed 2 April 2023].

[73] BeaconZone Blog, "Bluetooth LE Distance Determination Using RSSI," 5 May 2020. [Online]. Available: https://www.beaconzone.co.uk/blog/bluetooth-le-distance-determination-using-rssi/. [Accessed 2 April 2023].

[74] J. Marcel, "3 Key Factors That Determine," Bluetooth, 17 October 2019. [Online]. Available: https://www.bluetooth.com/blog/3-key-factors-that-determinethe-range-of-bluetooth/. [Accessed 2 April 2023].

[75] Bluetooth. [Online].

[76] B. D. Nelson, S. S. Karipott, Y. Wang and K. G. Ong, "Wireless Technologies for Implantable Devices," *Sensors,* vol. 20, no. 16, 2020.