Faculty of Science and Technology
Department of Informatics

Spread Spectrum and Jamming for Wireless Secrecy

João André Gomes de Sá Sousa

September 2, 2015

Faculty of Science and Technology
Department of Informatics

Spread Spectrum and Jamming for Wireless Secrecy

João André Gomes de Sá Sousa

Thesis submitted to the Faculty of Science and Technology (FCTUC) to bestow the Master's degree in Computer Science

Supervisor: Dr. João P. Vilela, University of Coimbra

Defense Committee: Dr. Jorge Granjal, University of Coimbra
Dr. Filipe Araujo, University of Coimbra

September 2, 2015

ABSTRACT

As Wireless Networks become increasingly popular, security is turning out to be something of the utmost importance to guarantee the confidentiality and robustness of communication under these systems. This thesis focuses on using physical-layer mechanisms to enhance confidentiality against eavesdroppers, more specifically, a recently published tweaked version of Frequency-Hopping - Uncoordinated Frequency Hopping - with the incorporation of defensive jammers for added security. For that, we characterize the secrecy level of this spread spectrum scheme, by devising a mathematical framework to assess the secure throughput (probability of secure communication) of devices operating under Uncoordinated Frequency Hopping. We then extend this mathematical model to accommodate the impact of defensive jammers and propagation effects on the legitimate communication, as well as, implement and evaluate this technique in a real-world test-bed. Results show that by exploiting frequency diversity, this method may be used for secret key-establishment, notably when eavesdroppers may appear in advantageous locations. Adding defensive jamming is also shown to be an effective solution for boosting the secrecy level against non-detectable adversaries like eavesdroppers.

SUMÁRIO

Com o crescimento exponencial das redes móveis, a segurança nestes ambientes tem ganho uma importância significativa de forma a garantir a proteção e confidencialidade da comunicação perpetrada neste tipo de sistemas. A nossa tese foca-se, sobretudo, na utilização da camada física da rede, em particular de alguns dos mecanismos a ela inerentes, para salvaguardar a informação partilhada entre utilizadores de ataques por parte de agentes escondidos, *eavesdroppers*, que procuram indevidamente escutar estas mensagens. Assim sendo, é utilizada uma versão alterada do *Frequency Hopping - Uncoordinated Frequency Hopping* - que incorpora um conjunto de agentes defensivos, *jammers*, para garantir a máxima segurança. Para atingir esse objetivo, nós caracterizamos o nível de segurança deste mecanismo de *spread spectrum* através do desenvolvimento de um modelo matemático para aferir a taxa segura de transferência de dados (probabilidade de comunicação segura) dos dispositivos legítimos que operam no sistema. De seguida, extendemos este modelo matemático de modo a incorporar o impacto negativo por parte dos *jammers* defensivos e dos efeitos de propagação no canal de comunicação legítimo, assim como, implementamos e avaliamos este conjunto de técnicas numa experiência/ensaio de um sistema real. Os resultados mostram que ao explorar a diversidade espectral, este método pode ser empregue em algoritmos de troca de chaves, em particular quando os *eavesdroppers* aparentam estar em situações vantajosas. Verificámos também que a utilização de *jamming* defensivo é uma solução eficaz para aumentar os níveis de segurança deste sistema, quando assolado por adversários indetetáveis como *eavesdroppers*.

To my parents, who have always been there for me, to my friends, who have put up with me for a long time, to Diana, who never gave up on me, and to professor João Vilela, Marco Gomes and Dinis Sarmento, who have made all this possible, I dedicate my ink and paper...

ACKNOWLEDGEMENTS

This work would not have been possible without the help of a great deal of people who have guided my throughout this journey, in particular, professor João Vilela who helped me a lot and was definitely an excellent supervisor and friend.

This path started many years ago, when I fortuitously decided to enroll in the Informatics Engineering course yet unaware of what was to come. Had I not made the friends and acquaintances, who are now so important to me, I would have not been successful in this *expedition* and I would, surely, not had written this thesis. Hence, I offer a big thanks to all of them, and I sincerely hope to continue to be part of their lives for a long time to come. I would like to particularly thank Adriana Ferrugento, Alexandre Jesus, André Maximino, Bruno Pedroso, Filipe Assunção, João Cerveira, João Claro, João Pedro, Mariana Lourenço, Pedro Matias, Tiago Mateus, for being the friends everyone would like to have.

In this last year, I had the opportunity to participate in new undertakings and to live different experiences, starting with my Erasmus in Switzerland during the first semester and ending with my cooperation with some research groups: the *Multimedia Signal Processing Lab*, from the Department of Electrical and Computer Engineering of the Faculty of Science and Technology of the University of Coimbra, and the *Laboratory of Communications and Telematics* (LCT), from the Department of Informatics Engineering of the Faculty of Science and Technology of the University of Coimbra.

I would also like to thank professor Marco Gomes and master student Dinis Sarmento, from the Department of Electrical and Computer Engineering, who have put up with my unceasing questions about electrical components, borrowed me some equipment and helped me execute the last stage of my work.

The final and most outstanding debt of gratitude is owed to my parents and to Diana whose encouragement and support where the key for my success, and whom I love very much!

This work was supported by Fundação para a Ciência e a Tecnologia (the Portuguese National Science Foundation) under grant EEI/UI326/2013, partially funded by the iCIS project under grant CENTRO-07-ST24-FEDER-002003, and the project PEst-OE/EEI /LA0008/2013 (WINCE - Wireless Interference and Coding for Secrecy) conducted at Instituto de Telecomunicações (IT), Portugal.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

a.v.n.	average node degree
BPSK	Binary Phase-Shift Keying
CA	Certificate Authority
cdf	cumulative distribution function
CDMA	Code Division Multiple Access
CSI	Channel State Information
CTS	Clear-to-send
DoS	Denial of Service
DS-CDMA	Direct Sequence - Code Division Multiple Access
DSP	Digital Signal Processors
DSSS	Direct Sequence Spread Spectrum
FCC	Federal Communications Commission
FH	Frequency Hopping
FPGA	Field Programmable Gate Arrays
GRC	Gnuradio Companion
GSM	Global System for Mobile Communications
HR/DS	High-Rate Direct Sequence
I/O	Input Output
IR	Infrared light
MIMO	Multiple-input Multiple-output
MISO	Multiple-input Single-output
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PCB	Printed Circuit Board
pdf	probability distribution function
PHY	Physical Layer

PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
RF	Radio Frequency
r.v.	random variable
s.d.o.f.	secure degrees of freedom
SDR	Software-defined Radio
SINR	Signal-to-interference-plus-Noise-Ratio
SMA	SubMiniature Version A
SNR	Signal-to-Noise-Ratio
SoA	State of the Art
SS	Spread Spectrum
TDMA	Time Division Multiple Access
UFH	Uncoordinated Frequency Hopping
UHD	USRP Hardware Driver
USRP	Universal Software Radio Peripheral
WPA	Wi-Fi Protected Access

1

INTRODUCTION

As somewhat expected, the last decade has seen the rise of Wireless Networks as the most popular way of communicating and sharing information. Moreover, we have also recorded an increase in the number of devices who inhabit this environment, which has necessarily meant a growing concern in terms of security. In fact, these systems are considered to be relatively prone to attacks from multiple sources and of different nature such as: phishing, spoofing, eavesdropping, denial-of-service (DoS), which interfere with the legitimate communication between nodes. Most researchers have pictured solutions based on cryptographic keys, as well as other techniques based on secret-key exchange, which have proven capable of guarantying, in most cases, the safe transmission of data between devices. However, these mechanisms are not without their limitations, and are sometimes considered inadequate when presented, for example, with spontaneous/ad-hoc networks, as key exchange might be too difficult to perform.

Spread-spectrum (SS) techniques such as Frequency Hopping (FH) SS and Direct-sequence SS have provided a new way of securing channels by allowing devices to jump between frequencies or to use different spreading patterns. Hence, by using the underlying characteristics of wireless networks, researchers have devised a new way of fending off attacks, mostly jammers, without depending on cryptography. Uncoordinated Frequency Hopping (UFH), first introduced by Strasser et al. [1], provided another SS alternative to escape these jamming attempts, this time without relying on a pre-shared secret hopping sequence. This technique accredited the idea that it is possible for nodes to securely communicate even when both of them do not agree upon a key sequence. Therefore, in this case, both transmitter and receiver randomly hop among frequencies and whenever, by chance, the nodes land in the same channel they briefly exchange data. Primarily intended as a key establishment protocol and although it meant a significant reduction of the average throughput, this scheme has proven to be effective against a jamming DoS attack. Originally thought out for protection against these DoS attacks, we consider employing this technique in a rather different way.

This thesis focuses in modelling and characterizing an UFH-based security scheme, but this time to resist eavesdropping by unauthorized users. In fact, the randomness associated with this SS protocol, and the fact that it does not entail any pre-established sequences, makes it a good choice for improving secrecy and reliability of wireless communications, especially when cryptography is deemed impracticable. Furthermore, most of current physical-layer security techniques rely on a degraded eavesdropper, thus warranting some sort of advantage that can be relied upon to achieve higher levels of security (e.g. Bob's better location). Under this challenging setup, it becomes hard to build robust schemes and new dimensions to establish advantageous periods of communication are needed. Without an advantageous setup we have to look for other ways of securing communication, for example, using the aforementioned spread spectrum technique (or other sources of spectral diversity). Finally, considering other works, part of the same field of study - *physical layer security* - we have also decided to include a set of defensive jammers to further disrupt any possible eavesdroppers' attacks, using their noise to degrade the assailants' channels.

1.1 Context and motivation

The need for security in wireless networks has led to an exponential increase in the number of schemes, mostly based on cryptography, that aim to provide reliable and safe communication of messages in these environments. However, in some situations, in particular for ad-hoc networks, where nodes are most of the times anonymous, these type of security schemes that rely on shared keys can be unsuitable and difficult to establish. First, there is the need for certificate authorities (CA) to guarantee authentication, and second, most of these strategies depend on mathematical problems whose complexity has not yet been proven. Even when relying on key-exchange mechanisms which do not leak any confidential data (e.g Diffie-Hellman), the presence of a degraded channel can compromise the transmission of this information. Nevertheless, physical layer security methods have to be regarded not has a substitute of cryptography but has a complementary technique, since it can add another layer of security.

Therefore, as part of my previous research work on spread spectrum and defensive jamming for wireless secrecy, in cooperation with professor João Vilela, we propose a new defensive scheme that combines both these techniques to provide a secure way of transmitting a particular sequence of data (e.g hopping sequence, secret key) to be used by other schemes (e.g. FH), which instead rely on shared information but offer higher throughput values.

This idea started has a research project held by professor João Vilela in early 2014 and soon became our undertaking. Hence, we decided to continue this work leading up to this moment.

This combination is significantly innovative and offers a successful way of avoiding eavesdroppers by exploiting the inherent randomness of these physical layer mechanisms, while guaranteeing the necessary spectral diversity, associated with SS to avoid potentially degraded channels that would, otherwise, disable the successful transmission of messages. Although the use of the physical layer to provide security is not by itself new, the combination of SS and defensive jamming to protect against non-degraded eavesdroppers, in a attempt to transmit confidential data, is significantly innovative with no prior work on this subject.

We point to the fact that our mechanism does not intend to replace common cryptographic tactics but rather tries to offer an added layer of security, which can be successfully employed in some situations, and does not rely on the computational restrictions of the attacker. Hence, our technique does not provide perfect secrecy but rather offers a sufficient secrecy level that makes it nearly impossible for the eavesdropper to listen to all data chunks, which can, with the right scheme (e.g. using a one-way hash function over all the message chunks to generate a shared secret), undermine its ability to decode the entire message.

Having started to conceive and mathematically characterize this security scheme in January 2014, we have already submitted some prior work that was accepted for the following conference proceedings:

- João Sá Sousa and João P. Vilela, "A Characterization of Uncoordinated Frequency Hopping for Wireless Secrecy", *IEEE 7th IFIP Wireless and Mobile Networking Conference*, Vilamoura, Algarve, Portugal, May 2014

Several of these contributions were developed during the following research projects:

- (Programa de Incentivo/EEI/UI326/2013) - *"A Characterization of Uncoordinated Frequency Hopping for Wireless Secrecy"*, January 2014 - March 2014
- WINCE (PEstOE/EEI/LA0008/2013) Project - *"Wireless Interference and Coding for Secrecy"*, September 2014 - September 2015.

This work was performed in cooperation with IT (*Portuguese Institute for Telecommunications*), in particular, with professor Marco Gomes and master student Dinis Sarmento from the Multimedia Signal Processing Lab, from the Department of Electrical and Computer Engineering of the Faculty of Science and Technology of the University of Coimbra. Their help has been valuable for the successful conception of our test-bed using software defined radios, with several tips on how to tune each device (e.g. antenna gain, amplitude, etc.), on what Gnuradio blocks and variables to use and on how certain physical layer mechanisms actually worked (e.g. modulation schemes).

1.2 Secrecy for Wireless Networks

Due to the paramount importance of security to guarantee reliable and confidential communication in wireless networks, throughout the years, researchers have continuously tried to bolster existent techniques, as well as develop new ones, with the intention of securing communication, by tackling the problems and liabilities of existent solutions. Although most current viable security techniques are based in cryptographic schemes such as Wi-Fi Protected Access (WPA), a different field of study emerged that no longer exclusively relies on the use of secret keys, but rather exploits the inherent randomness of the physical layer (PHY), for example by using noise interference from external helpers to disrupt the attackers' channels.

Methods such as Uncoordinated Frequency Hopping (UFH) [1], [4] and friendly jamming [5], [6] have been regarded as possible ways of improving secrecy and reliability of wireless communications without the need for a shared secret. Therefore, by combining these two mechanisms to prevent eavesdropping, our suggested security proposition is, thus, optimizing the joint operation of these techniques to harness the hidden power of PHY to offer secrecy.

1.2.1 *Uncoordinated Frequency Hopping*

Uncoordinated Frequency Hopping (UFH) implies the communication between transmitter and receiver through a randomly chosen frequency channel unknown for both agents. Therefore, both intervenients randomly and independently hop between a set of frequencies, briefly transmitting chunks of data when both of them land in the same channel. Since adversaries are unaware of the random hopping sequence, this enables adversary-free periods of communication whenever the transmitter and receiver lie in the same frequency without the adversary doing so.

This scheme acts, in some way, like regular FH, although it tries to offer a key-independent service (no previous hopping scheme is established between nodes). This leads to a significant reduction of the average throughput and, consequently, significantly decreases its performance at the benefit of adversarial-free information exchange. Originally thought out for protection against DoS jammers, these periods of adversary-free communication can then be used for exchanging a secret key or a hopping sequence for regular FH communication, with higher performance levels.

1.2.2 *Physical Layer Security*

Physical Layer Security had its debut with Shannon's first attempt [7] at perfect secrecy through information-theoretic security. In his work, Shannon demonstrated that to achieve information-theoretic security, the encrypted data had to be statistically independent from the original message, which, unsurprisingly could only be carried out if different keys, with the same length as the original message, were employed for each different transmission. Yet, it was not until Wyner's wiretap channel [8], that we got to know an alternative information-theoretic scheme, which revealed that secure communication was possible if the eavesdropper observed a noisy version of the legitimate message.

These conclusions, led to the emergence of a series of new techniques centered around the physical layer, which benefited from the randomness akin, for example, to signalling and coding processes. With its growing interest, an increasing number of new mechanisms were developed, which relied on different technologies related with PHY. These comprise, for example: *multiuser or cooperative diversity* using an optimized multiple-input multiple-output (MIMO) system, relay nodes to choose the best and secure path to transmit a signal [9]; *beamforming techniques*, to direct the message in a particular safe direction; *coding techniques* to arrange bits in a way that only the legitimate receiver can decode them [10]; *spatial probabilistic models* to arbitrarily disposition nodes in order to maximize secrecy [11]; or *cooperative jamming* and *noise interference* [5], [6] where a set of entities are tasked with creating noise to degrade the attacker's channel, similar to Wyner's wiretap channel model.

1.2.3 *Defensive Jamming*

The multitude of approaches previously listed paved the way for new forms of cooperation, in particular the use of cooperative helper nodes, or simply jammers, to generate noise and subsequently collisions to degrade eavesdroppers' channels. Therefore, this sparked an interest on the advantages of these schemes employing artificial noise to maximize secrecy. *Cooperative jamming* techniques have been proposed that for example: secure relaying by adding artificial noise [12]; make use of additional antennas at transmitter [6] or receiver [13], [14]; rely on a set of relay and jammer nodes to provide security in 1-D and 2-D networks [2] [15]; or try to set new jamming strategies based on the availability of channel state information (CSI) of both the eavesdropper and the receiver [16].

From a different perspective, Pinto et al. [17] and Vilela et al. [18] respectively use a probabilistic model to represent wireless networks, and provide a new cooperative defensive jamming scheme that tries to pin-point the best locations to place these defensive units in order to maximize their security level and at the same time reduce the impact their interference might have in the legitimate communication.

1.3 Contributions

This work aims to unveil a new way to use UFH for securing communication, in this case by denying eavesdroppers the chance to listen to messages. Furthermore, jammers are no longer seen as invasive, and are, otherwise, employed as a source of defensive interference capable of disrupting malicious eavesdroppers intents. As part of our preliminary analysis, we proposed [19] a mathematical representation of the secure throughput[1] of this setup, both with and without defensive jammers, as well as a way to optimize the secure throughput by adapting the number of frequencies to the number of eavesdroppers. Furthermore, we also extended this model to accommodate broadband communication [20], offering a more general equation to model our defensive mechanism. Results have shown that it is possible to use this scheme for securing legitimate communication from eavesdroppers, and unveiled the positive effect of using friendly jammers. Furthermore, we also proposed a new model which accommodates stochastic geometry [17] (probabilistic representation of nodes' locations), to better assess the impact of defensive jamming interference in both the eavesdroppers and the legitimate communication. In pursuit of these goals we made the following contributions:

- *State of the Art (SoA)* - provide a detailed review of related work and highlight interesting results;
- *UFH + defensive jamming* - employ UFH as a way of evading eavesdroppers, guaranteeing, with a certain probability, the secure transmission of messages between a transmitter and a receiver. Combine UFH with a set of jammers tasked with the defence of legitimate communication, and provide a mathematical representation for the secure throughput of this system;
- *Optimization* - propose and provide a characterization of this scheme, and tune up the number of available frequencies to optimize the secure throughput.
- *Path Loss* - incorporate the effect of path loss to the existent model to thoroughly assess its secrecy gains;
- *Spatial Analysis* - build up a stochastic model to probabilistically place jammers and eavesdroppers, and devise a series of metrics to capture the effect of jamming on the attained secrecy level according to the aforementioned UFH technique;
- *Validation* - implement and evaluate in a test-bed.

This work has led to the following publications in international conferences:

- João Sá Sousa and João P. Vilela, "Uncoordinated Frequency Hopping for Secrecy with Broadband Jammers and Eavesdroppers", *IEEE International Conference on Communications (ICC) Proceedings (accepted for publication)*, London, UK, June 2015
- João P. Vilela and João Sá Sousa , "Physical-layer Security Against Non-degraded Eavesdroppers", *IEEE Global Communications Conference (GLOBECOM) Proceedings (accepted for publication)*, San Diego, USA, December 2015

[1] Probability of secure communication.

1.4 Timeplan

The tasks, outcomes and time-line of this thesis were as follows:

Task Denomination	Start Date	Duration	Description/Outcome
Secrecy characterization of Narrowband UFH	Previous to the start of the thesis.	-	Characterize the the inherent level of security that UFH provides against eavesdroppers by calculating its secure throughput, i.e. the probability that transmitter and receiver land on the same frequency without the eavesdroppers doing so. Add friendly jammers whose goal is to cause interference to eavesdroppers without harming legitimate communication.
SoA Review	08-09-2014	3 months	Thoroughly analyze current methodologies associated with our thesis, in particular: SS Techniques; Physical Layer Security; Interference and Spatial Models; Defensive Jamming.
Secrecy characterization of Broadband UFH	08-09-2014	2 months	Extend previous mathematical narrowband model to accommodate broadband jammers and eavesdroppers (i.e. capable of simultaneously listening to more than one frequency channel).
Intermediate Report	1-12-2014	2 months	Write an intermediate version of our thesis and plan future work.
UFH Broadband Extended	02-02-2015	2 weeks	Estimate the maximum secure throughput for the broadband setup.
Mathematical Model for Network Interference	16-02-2015	3 weeks	Briefly review and devise a mathematical model which combines interference with the probabilistic disposition of nodes [21].
Aggregate SS System Model	09-03-2015	2 months	Combine the developed and analyzed mathematical model for network interference with the spread spectrum analytical framework previously developed.

Implementation and Evaluation	4-05-2015	3 months	Implement and evaluate the spread spectrum for secrecy methodologies in a real-world test-bed. In particular: • Definition of appropriate metrics to assess the secrecy and communication levels of networks under physical-layer security schemes; • Implementation of spread-spectrum and jamming mechanisms to enhance the frequency of favorable communication periods over the eavesdropper; • Explore both omnidirectional and directional jamming.
Thesis Final Version	27/07/2015	1 month	Write a final version of our thesis.

Table 1.: *Planning.*

Figures 1 and 2, in the next page, illustrate the start and finish dates of the aforementioned tasks that have been executed during our thesis. This schedule, introduced during the intermediate stage, add to be altered due to some constraints and difficulties, in particular, the considerable complexity of our extended mathematical model, the new programming software - Gnuradio - which took us some time to get adapted to and the number of lengthy runs that had to be executed to allow for an accurate statistical analysis of our test-bed.

1.5 Thesis Structure

The remainder of this thesis is divided into five other sections. In Section 2 we introduce the fundamental concepts behind our idea, as well as, related work, and briefly highlight relevant results. In Section 3 we present our preliminary results that focus on the first two methodology tasks, exploring the usefulness of *UFH + Jamming for secrecy* in narrowband and broadband setups. In Section 4 we extend our mathematical model to include the effect of jamming and propagation characteristics on all the different channels. In Section 5, we implement our test-bed and discuss the results. Finally, in Section 6, we highlight key issues and findings and include future directions for work.

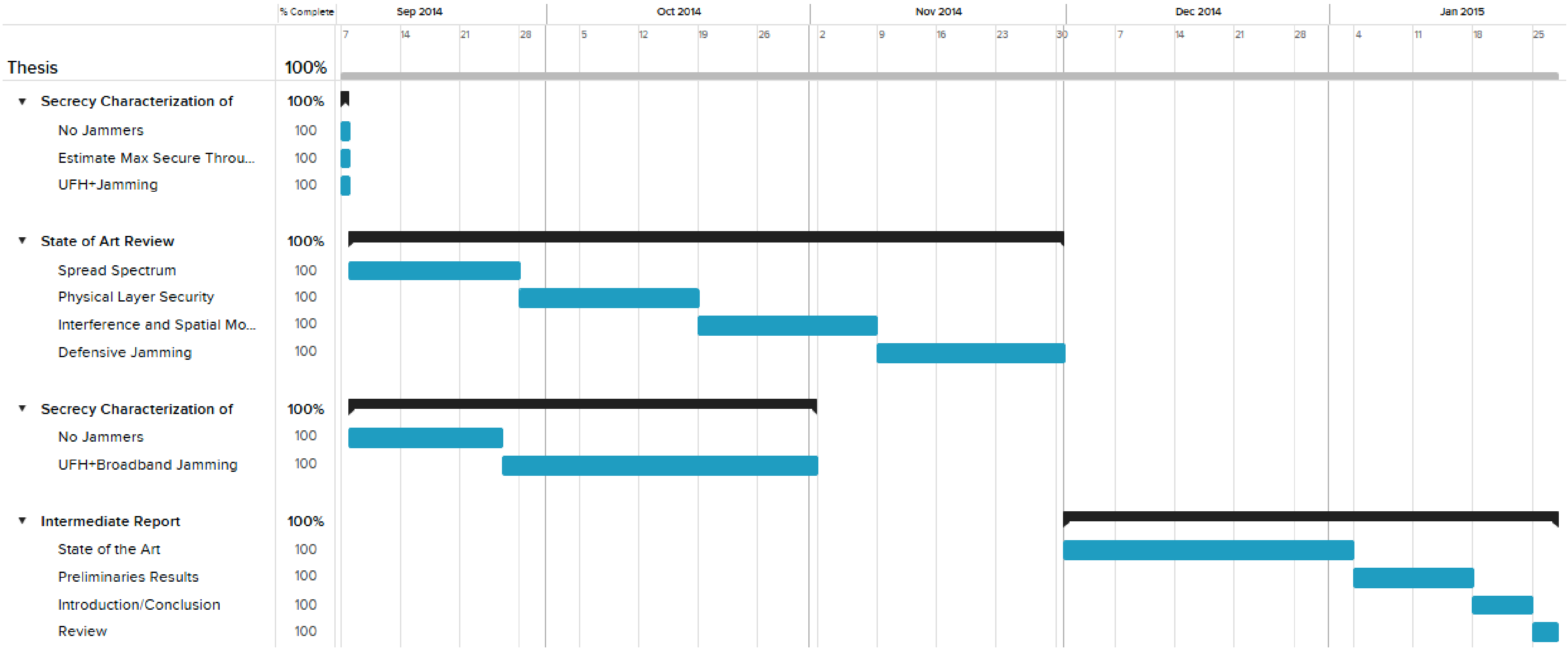
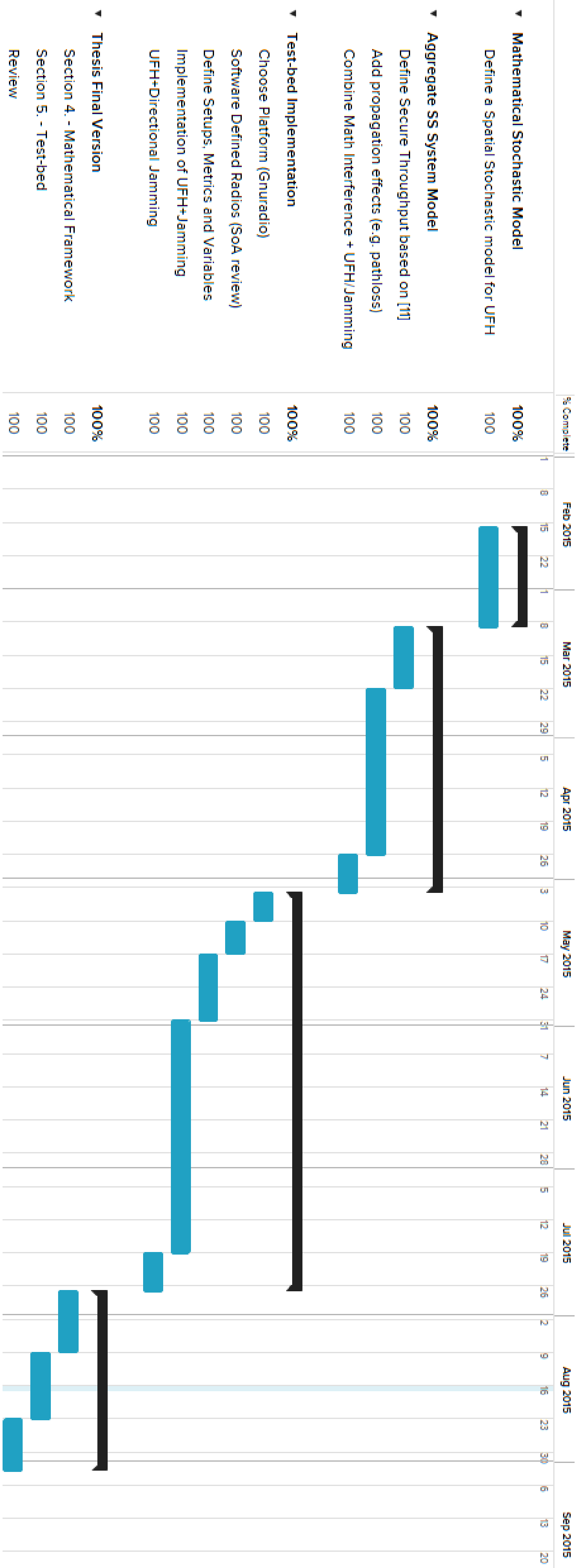


Figure 1.: *Gantt - 1st Stage*



	% Complete
Mathematical Stochastic Model	**100%**
Define a Spatial Stochastic model for UFH	100
Aggregate SS System Model	**100%**
Define Secure Throughput based on [11]	100
Add propagation effects (e.g. pathloss)	100
Combine Math Interference + UFH/Jamming	100
Test-bed Implementation	**100%**
Choose Platform (Gnuradio)	100
Software Defined Radios (SoA review)	100
Define Setups, Metrics and Variables	100
Implementation of UFH+Jamming	100
UFH+Directional Jamming	100
Thesis Final Version	**100%**
Section 4. - Mathematical Framework	100
Section 5. - Test-bed	100
Review	100

Figure 2.: *Gantt - 2nd Stage*

2

STATE OF THE ART

This chapter aims to provide the necessary background to back up our problem statement. The ensuing subsections describe the existent technologies, which represent the core of our idea, offering the readers a detailed insight on this subject. It is also our intention to contribute with a set of references that helped me develop our work, and how they relate to our approach to the problem of securing Wireless Networks. The first subsection covers some of the underlying physical aspects behind our security scheme: Spread Spectrum Techniques and Uncoordinated Frequency Hopping, followed by Wireless Communication concepts and Physical Layer security models. The last sections describe the currently employed Defensive Jamming techniques and consequent mathematical frameworks, as well as, the software and hardware contraptions used to implement our test-bed.

2.1 Spread Spectrum Techniques

Spread Spectrum (SS) Systems have been already around for quite some time, and have had a huge impact in Wireless Networks. The prospect of multiple access and ensuing spectral efficiency has made them invaluable to cope with the exponential growth in the number of users. Moreover, SS techniques have also provided a new way of ensuring the secure transmission of information, by spreading data over a large bandwidth. As a matter of fact, these mechanisms started as a elementary feature to avoid jamming attacks from narrowband devices during the Second World War, and have, since then, been used to increase the robustness of communication through wireless networks. Although there were many ways of spreading the spectrum, only two of them became widely accepted: *Frequency Hopping* (FH) and *Direct Sequence - Code Division Multiple Access* (DS-CMDA) [22], [23].

Albeit portraying different concepts, both these techniques have devised new ways of transmitting as much information as possible for a certain bandwidth, while maintaining communication stealthy, safe from intercept and capable of avoiding jamming efforts by hostile transmitters. The inlaid idea behind SS techniques is to use different spreading or hopping patterns for each user to mask and avoid interference, while allowing them to transmit in the same frequency band simultaneously.

2.1.1 *Direct Sequence Spread Spectrum*

Direct Sequence SS implies molding the transmitted signal in an unique and singular way. In essence DSSS spreads the signal into a larger frequency band by multiplying the initial signal with another with a very large bandwidth. Combining them actually adds up to the bandwidth of this final signal and reduces the *power-spectral density*[1], without changing its original transmit power. *Figure* 3 demonstrates how the original signal gets affected and what underlying advantages this might bring. In fact, depending on the spreading pattern, the resulting signal can lie just below the noise power-spectral density making it harder for unauthorized users to recognize any transmission attempts (for them it is just noise!). On the other hand, authorized users can simply invert this spreading operation, and thus recover the transmitted data.

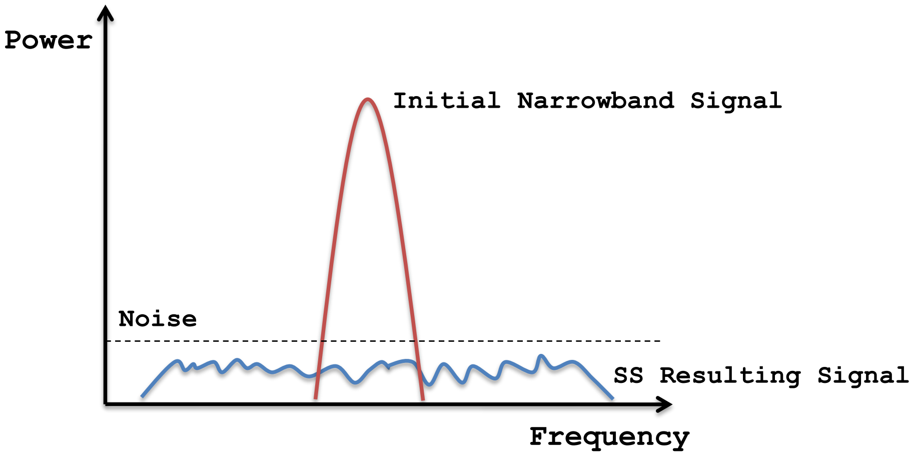


Figure 3.: *DSSS signal spreading.*

However, it is still not clear how can this modulation method for stealthy communications be used to achieve multi-access capability. In truth, for it to become accessible for multiple users, DSSS is used in conjunction with Code Division Multiple Access (CDMA), to provide each node with a different spreading code. Therefore, each transmitted signal is relatively different for each user, allowing for the desired signal to be obtained at the receiver by correlating it with its correspondent spreading sequence. Thus, many users can transmit simultaneously in a wide band. Yet, it is worth mentioning that in this technique, all other users are considered to be wideband interferers which can, in some cases, affect the quality of the retrieved signal. The choice of spreading sequences is thus an essential factor to ensure signal quality, to reduce the impact of *active* interference (other users) and for maintaining a robust CDMA system.

This SS technique requires the previous exchange, between users, of the underlying spreading pattern, which implies security risks and a considerable breaching point capable of being explored by attackers.

[1] Power-spectral density describes the signal power distribution over the frequency.

2.1.2 *Frequency Hopping Spread Spectrum*

Frequency Hopping (FH) is perhaps, conceptually speaking, the simplest SS technique. In fact, the basic thought behind this scheme is to change the carrier frequency of a narrowband transmitter over time and thus avoid cramped up frequencies and suppress narrowband interferers. Developed during the Second World War, this technique was primarily employed as a way of disrupting enemy jamming attacks by rapidly shifting frequencies, evading possible Denial of Service (DoS) incursions and dodging vulnerable channels. Furthermore, in addition to suppressing narrowband interferers, FH has also contributed to mitigate the effect of faded frequency bands by allowing nodes to use different frequencies throughout the transmission phase. Therefore, by interleaving[2] and coding packets the system is, sometimes, able to relay its data through "good" channels (low interference and attenuation) while avoiding the "bad" ones.

There are two different types of FH, *fast FH* and *slow FH*. The faster one implies changing the carrier frequency during the transmission of each symbol, effectively tackling interference issues at "*cellular*" level (for each symbol separately). However, this scheme is computationally inefficient and has long been replaced with Code Division Multiple Access (CDMA). On the other hand, *Slow FH*, employed in the Global System for Mobile communications (GSM), entails the transmission of one or more more symbols during each frequency hop. Frequently used in conjunction with Time Division Multiple Access (TDMA), this technique is further enhanced when the information is replicated among different timeslots, transmitted on different frequencies, which increases the chance of sending the data through a channel with low interference and attenuation.

Although sometimes coupled with other multiple access schemes, FH can act by its own while yielding both characteristics: interference suppression and spectral efficient multi-access. In this case, we have to consider two different scenarios: *synchronized* and *unsynchronized*, which deeply affect the underlying model and consequent system requirements. When synchronized, the transmitter can use different frequency channels to transmit its information to various receivers at the same time during a predetermined interval - ***hopping period***. Using *Figure* 4 as reference, we can notice that it is possible for a transmitter to use its different available bands to send its data to the correspondent receivers without changing the fundamental concept behind FH. As such, during the first hopping period: transmitter (*Tx*) can use frequencies 1 and 2 to send information to receivers R_A and R_B, respectively. Then, in the next timeframe, *Tx* can now transmit data to R_A in frequency 3 and to R_B in 1. Finally, in the third jump R_A is serviced through frequency 2, and R_B in frequency 3. Then, the whole sequence repeats. Therefore, by combining a series of hopping sequences associated with each different user, this SS scheme can avoid collision between devices and increase system capacity (e.g. adapting to the different interference levels of hopping patterns by assigning different bit rates for each slot) with the added benefit of frequency diversity. Nonetheless, it is worth mentioning that for this strategy to work, nodes have to guarantee that they are all synchronized by sharing runtime information among themselves,

[2] Interleaving is a method to make a system more reliable and efficient by arranging data in a non-contiguous manner.

as well as, prior agree and share the hopping sequence with the receiver. For more details, please refer to following books by Molisch [22] and Gast [23].

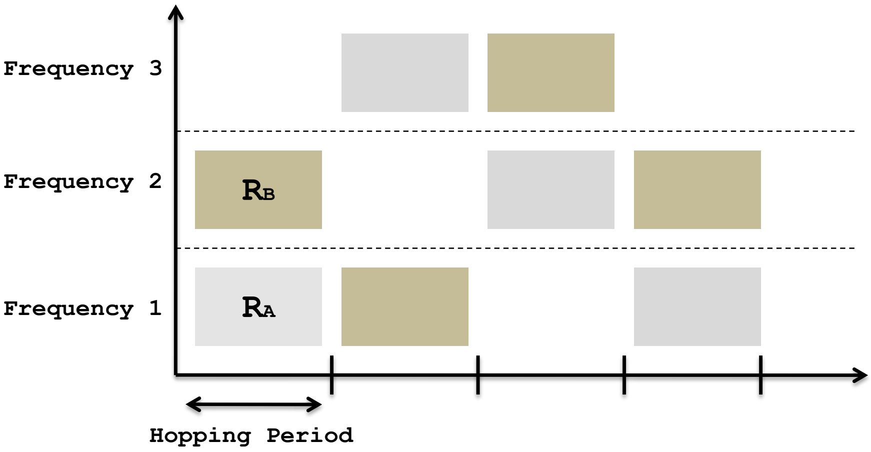


Figure 4.: *FH synchronized multi-access concept for two receivers (R_A and R_B).*

When not synchronized, for example for ad hoc networks, the use of these hopping patterns becomes slightly different and more prone to errors and collisions. Going back to the previous figure we can observe that any delay between signals can lead to collisions between transmissions. Therefore, it is necessary to use different hopping sequences and strategies that can sustain minor delays. For example, designing different hopping sequences which ensure that for each jumping cycle only one timeslot is disturbed, while the others remain collision-free (*Figure* 5).

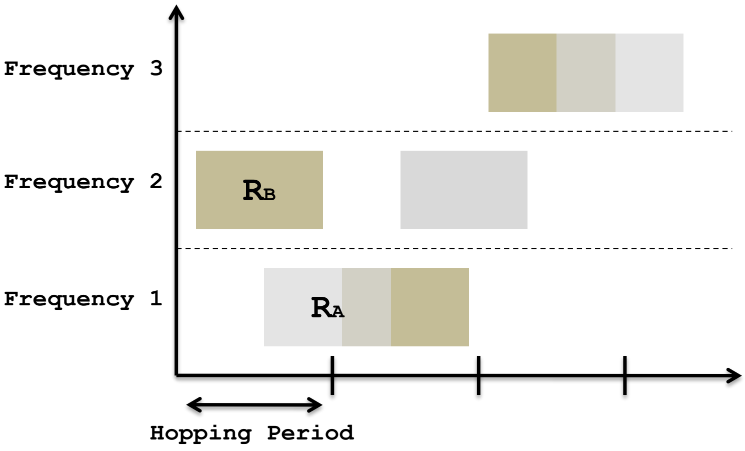


Figure 5.: *FH unsynchronized multi-access concept.*

Having detailed the most common SS techiques, one can quickly identify similarities and characteristics among them, as well as the fundamental security limitation behind these mechanisms - ***the need for a shared agreed hopping or spreading sequence***, as we can now elaborate.

2.2 Uncoordinated Frequency Hopping (UFH)

As previously remarked, the common SS techniques - *FH* and *DSSS*, have some intrinsic limitations which are usually tackled using supportive cryptographic algorithms for secret key exchange. Nonetheless, Strasser et al. [1] call the attention to the circular dependency of key establishment on a jamming-resistant communication: *how can devices share their secret (spreading or hopping) sequences without being targeted by jammers, as these anti-jamming algorithms require, themselves, shared secret keys?* Breaking down this dependency (*Figure* 6) we can easily claim that without a prior exchange of information, whether by out of band code pre-distribution or through key exchange protocols (e.g. Diffie-Hellman), the system is incapable of erecting a conceivable SS technique for preventing attacks. Strasser et al. [1] also offer a way out by building a different SS mechanism entitled ***Uncoordinated Frequency Hopping*** (UFH) intended to break this circular dependency.

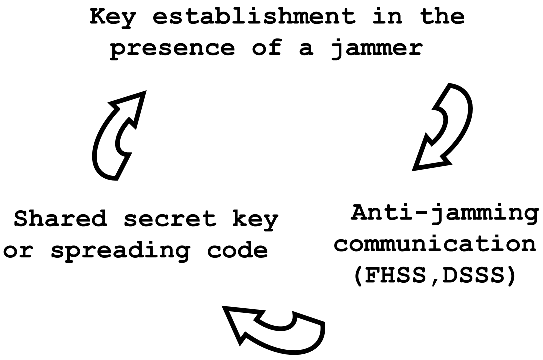

Key establishment in the presence of a jammer
Shared secret key or spreading code
Anti-jamming communication (FHSS,DSSS)

Figure 6.: *Circular dependency of FH: to communicate we need an anti-jamming mechanism which depends upon a key sequence, that requires a safe transmission method, and vice-versa [1].*

UFH is going to be the default SS communication scheme used for most of our work and, as the name entails, its behaviour closely resembles FH without the underlying circular dependency. This scheme implies the transmission of packets through different channels during fixed periods of time, by constantly hopping between frequencies. Therefore, it is based on the observation that, at some point in time, legitimate users will hop to the same frequency opening a brief transmission channel where they can send and receive messages, without an adversary jammer doing so, enabling them to communicate reliably. Whereas in FH the channel sequence is agreed beforehand, in this case, the jumping sequence is calculated randomly so there is no need to share it through the network. As expected, reliable communication comes at the cost of rather low throughput values for this scheme. In fact, given the randomness related with this mechanism, the transmitter will need numerous sending attempts to deliver a message. Nonetheless, it is important to notice that UFH is mainly proposed as a key-establishment secure protocol [1] and, as such, is mostly used for transmitting small chunks of data, more specifically, sequence keys. These keys can then be employed by conventional key-bounded SS techniques (FH or DSSS) for sharing messages with higher throughput.

Figure 7 represents the underlying communication model of UFH. As portrayed, communication nodes jump randomly among a set of finite frequencies and transmit data whenever they remain in the same channel. As anticipated, this scheme requires precisely synchronised transmission to avoid partially received message fragments. One other way to prevent this is to make the receiver permanently jumping between channels at a lower rate, thus reducing the number of partial reads.

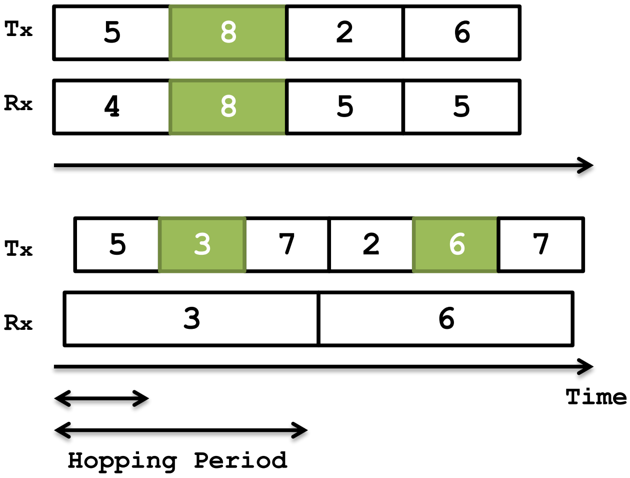


Figure 7.: *UFH communication model. Filled slots represent successful transmission of a message (both nodes land on same frequency) and blank slots the opposite. The top scenario represents loosely synchronized transmission, whereas the bottom scenario does not require synchronized transmission by permitting the receiver to jump slower than the transmitter, therefore reducing the number of partial reads.*

UFH also possess an innate message transfer protocol which allows for a reliable and secure transmission of messages under this scheme. As similar to coordinated FH, this message transfer model encompasses three distinct steps: *Fragmentation*, *Transmission* and *Reassembly*. First, the message is fragmented in small chunks of data, which are encapsulated in different packets, see *Figure* 8, and re-arranged to generate a linked packet chain. Each fragment has an *id*, a *fragment number*, the actual data itself, and a hash value for the next packet. Using this hash function guarantees a certain degree of safety and allows for an easier reassembly of the message. Before transmitting the data, the sender applies a generic coding scheme and interleaves packet bits to reduce the probability of bit errors. All different fragments are then transferred using UFH communication system, repeating the transmission of each packet an arbitrary high number of times. To conclude, in the last stage, the message is reassembled by rearranging the packet chain using the fragment number and the hash values of each received packet.

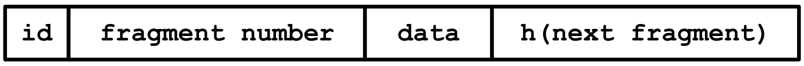


Figure 8.: *Packet structure after fragmenting message.* ***h*** *is a collision-resistant hash function.*

This message protocol further enhances the inherent UFH security level, by avoiding and limiting the insertion of arbitrary illegitimate packets (by an attacker) that could disrupt the efficient reconstruction of the message. Using hash functions to link fragments makes it near impossible to add new packets to the chain, since it would require finding $frag_i^{'}$ such that h($frag_i^{'}$) = h_{i+1}, where h_{i+1} is the previous legitimate message fragment hash value, which points to the next packet. Nonetheless, UFH can still be targeted by replay attacks (i.e. repeating complete packet chains), a problem that has to be tackled using timestamps and message buffering protocols. To conclude, UFH message transfer scheme does not initially intend to provide authentication, which can be achieved on the application layer, using the previously mentioned mechanisms.

2.2.1 *Enhancements to UFH*

Other message transfer protocols have already been proposed [4] that, for example, employ *erasure codes* [24] for a faster reassembly stage, efficient packet coding to make packets more resistant to bit error and consequently jamming attacks, and channel selection to reduce the probability of attacks.

In terms of enhanced packet coding, Strasser et al. [4] offer a detailed view on the performance of different coding schemes. In particular to UFH, these mechanisms have to bear in mind that shortening each packet, and corresponding hopping slot, offers a better protection against *reactive jammers*, which regularly perform wideband scans of the radio spectrum searching for ongoing transmissions before jamming a channel, but requires more packets to be successfully received. Longer slots, allow for an increasing redundancy and a consequent better bit-error protection and jamming defense. BCH block codes [25] have proven to be the effective for encoding UFH message chunks.

Finally, Strasser et al. [4] point out one last enhancement to the conventional UFH transmission scheme: introducing an optimal channel selection that strictly depends on the characteristics of the jamming. In fact, in contrast to FH, where the security is enhanced whenever we increase the number of frequencies, in UFH that does not necessarily happen. A big number of frequencies to choose from may irrevocably deem the communication almost impossible, as the associated throughput becomes too small. Results show that the optimal number of channels is, approximately, two times the number of blocked/jammed channels, $2C_b$. However, Strasser et al. warn to the fact that the number of jammed frequencies can be hard to detect without some other mechanism to help calculate the total number of affected channels. Nonetheless, the authors highlight that it is still possible to assume that UFH scheme operates better when adapting the available hopping frequencies to the average jamming strength (blocked channels) - $2C_b$.

Throughout this section, and related references, UFH was exclusively deployed in a single transmitter-receiver scenario, as a way of efficiently protecting communication between these two agents from jamming attempts. However, some extents have been added to this protocol [26], [27] to make it work under a multiple transmitter-receiver setup, allowing efficient and secure broadcast of messages using UFH. The aim of these articles was, mostly, to extend the inherent jamming-resistance capability of UFH, allowing it to work under a multiple-node setup, closely resembling real life situations, such as emergency alert broadcast or navigation signal-distribution. Pöpper et al. [26] provide the simplest extension protocol, where each of the many transmitter-receiver links work independently, employing UFH to send/receive messages. As such, each of the nodes hops randomly among frequencies and whenever the transmitter matches one of the arbitrary node's channel, communication occurs. However, this proposition does not account for the possibility of overlapping channels and consequent transmission failure. In fact, transmitters may happen to select the same channel to relay data, leading to the collision of packets, which can, depending on the number of occurrences, further reduce the UFH throughput rate. Xiao et al. [27] propose a different, more complex, approach, which, not only implies the broadcast of messages by transmitters, but also includes a relay protocol to be used by receiver nodes to send their data to other participants. Therefore, as depicted by *Figure* 9, the source node(s) employs UFH scheme to repeatedly and sequentially send the same fragmented message over multiple randomly selected frequency channels; whereas the nodes which have successfully received the whole message, help relay this same data to the remaining participants using a similar SS mechanism.

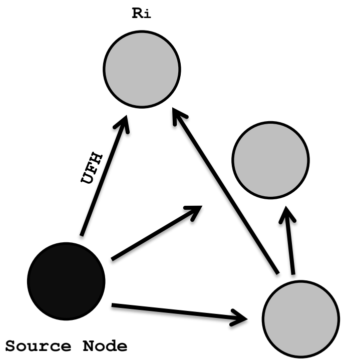


Figure 9.: *Collaborative jamming-resistant broadcast using UFH. In this protocol, source node broadcasts messages using simple UFH, whereas receiver nodes, R_i, relay this message to other nodes, whenever they have finished collecting data.*

To conclude, UFH has proved to be an effective solution for jamming-resistant communication, and recent work has further enhanced this protocol enabling its use in real life scenarios. Nonetheless, all previous work on UFH has solely used this scheme for protecting against jamming attacks. My thesis offers a new perspective on this SS technique, using it to deny eavesdroppers the chance to listen to messages. Furthermore, jammers are no longer seen as invasive, and are, otherwise, employed as a source of defensive interference capable of disrupting malicious eavesdroppers intents. Doing so opens new possibilities for UFH, which shifts from a jamming-resistant scheme to something more generalized and capable of securing communication against, for example, eavesdropping attacks. Our objective is to characterize the secrecy level of UFH when coupled with defensive interference, and also to maximize its secure throughput rate by tweaking protocols' variables such as number of channels, and number and location of jammers. We also develop an extended mathematical framework that incorporates the effect of jamming and propagation characteristics in this scheme, using spatial stochastic models to define the number of nodes and their locations.

2.3 Wireless Communication Models

Before continuing with the description of physical layer security techniques and in particular defensive jamming, we have decided to introduce and thoroughly describe a set of concepts (which have already been or will be mentioned) that play a decisively crucial role for fully understanding the next sections. Therefore, we will focus on: the *propagation effects* related with network traffic; the mathematical interpretation for *statistically and spatially* modelling wireless networks; and briefly illustrate how *random networks* work and how are they can be used to model and analyze our security scheme.

2.3.1 *Propagation Effects*

The performance of wireless channels is affected by three different phenomena which deteriorate and alter signal strength: *path loss*, *shadowing* and *multi-path fading*. The first two problems occur over relatively large distances and are grouped in what is sometimes referred as large-scale propagation effects. As for multipath fading is normally occurs over very short distances and is referred as a small-scale propagation effect. Goldsmith's book [28] provides a brief overview on how to accommodate these propagation characteristics in different channel models.

Path Loss is responsible for the reduction of power density associated with a transmitted signal (attenuation), which gets carried over a given channel. In other words, as referred in Goldsmith's book [28], path loss is defined as the difference in dB between the transmitted, P_T, and received, P_R, signal power.

$$P_{loss} = 10 \log_{10} \frac{P_t}{P_r} \tag{1}$$

Having in mind Shannon's famous formula for channel capacity and its correspondent simplification for a standard additive white Gaussian noise channel, $C = log_2(1 + \frac{P_T}{N_0})$[3], adding path loss, means changing this formula to

$$C = \log_2 \left(1 + \frac{P_T \cdot f(d_{tr})}{N_0} \right) \tag{2}$$

where d_{tr} is the distance between the transmitter and the receiver. Although there are many representations for $f(d_{tr})$, perhaps the most common one is $f(d_{tr}) = (\frac{d_0}{d_{tr}})^{\alpha}$, where d_0 is the close-in distance and α is the path loss exponent, which usually assumes values between 0.8 (e.g. hallways inside buildings) to 4 (e.g. dense urban environments) [29].

Shadowing, or shadow fading, corresponds to random variations of the received power at a given distance, which can occur thanks to the obstruction caused by objects lying in the transmission path, or by reflecting surfaces. As it happens with normal fading, this effect can vary with time and geographical position and is usually modelled as a ran-

[3] P_T is the average power constraint and N_0 is the noise power

dom process. The most common one is the *log-normal shadowing*, which is represented by a tweaked path loss equation.

$$P_{loss}(d_{tr}) = P_{loss}(d_0) + 10\alpha log_{10}\frac{d_{tr}}{d_0} + X_\sigma \tag{3}$$

where X_σ is a Gaussian distributed random variable with mean zero and variance σ, which can be represented in various ways.

Finally, *fading* or *multipath fading*, is a concept similar to shadowing, but in this case the variations in the signal are generated by multipath propagation, which results from the refraction and reflection of the transmitted signal in objects, as depicted by *Figure* 10.

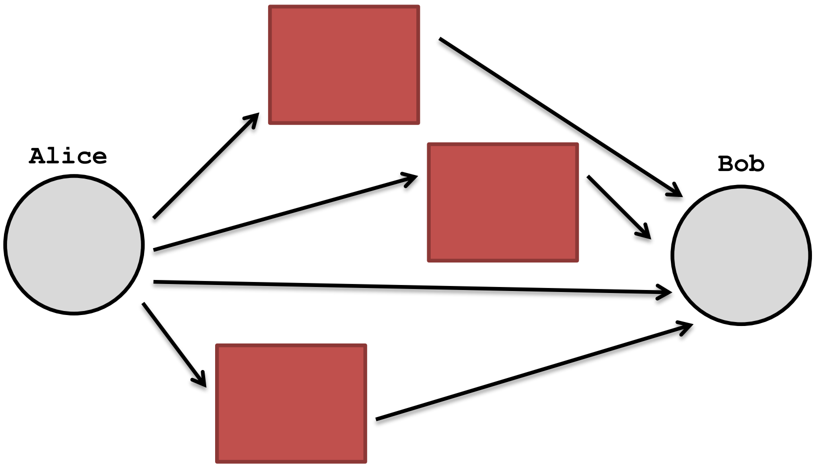


Figure 10.: *Multipath propagation.*

Similar to previous propagation effects, multipath fading can be accommodated using a variety of models [30]. Furthermore, we can discriminate two different fading types: *slow fading* - quasi static; and *fast fading*. The first one assumes that the channel holds the same fading coefficient during most of the transmission, whereas for the second type transmissions may experience several fading realizations and coefficients.

For slow fading and using Shannon's channel capacity formula, the effect of fading can be measured as the *outage probability* for communication rate, R.

$$P_{out}(R) = \mathbb{P}\left\{log_2\left(1 + \frac{P_T G_{tr}}{N_0}\right) < R\right\} \tag{4}$$

where G_{tr} is the function of the random fading gain. This probability corresponds to the receiver's ability to decode the transmission with a low chance of error. If not successful, the receiver node is said to be in *outage*. As for *fast fading*, channel capacity can be analyzed by averaging over many independent fading realizations.

2.3.2 *Stochastic Geometry*

As it has previously been mentioned, propagation effects and other channel network characteristics depend on, for example, the distance between transmitter and receiver or the disposition of the nodes in the network. There are two main methods for modelling the spatial distribution of nodes: *deterministically*, using fixed shapes (e.g line networks, triangle lattices); or *probabilistically* using stochastic geometry [31]. This last concept captures the randomness and the uncertainty of the location of the nodes, for example when deploying eavesdroppers and jammers, allowing for the development of a new set of performance metrics.

Stochastic geometry can employ several different distributions to model the location of nodes but the most common and widely employed, is the *Point Process* (PP), and more specifically the *Poisson Point Process* (PPP). A PP [32], Π, is a set of random points $\{x_1, x_2...x_n\}$ in a plane, which are mathematically mapped into $\mathbb{N}$ according a probability space, where $\mathbb{N}$ is the sequence of points in $\mathbb{R}^2$ that is locally finite, and independent, $x_i \neq x_j$ if $i \neq j$. Therefore, since this group of points is determined probabilistically, the realization of PP is a random choice of one of the sequences in $\mathbb{N}$. Thus, using this process we can, for example, probabilistically determine the number of points inside a certain region of $\mathbb{R}^2$. PPP, as the simplest spatial point process, accounts for two different distributions: *homogeneous*, and *inhomogeneous*, which are, respectively, used for generating regular or irregular distribution of points. The homogeneous PPP is prevalent when modelling wireless networks, and comprises a set of parameters such as the point density in a given region, λ. For this PP, the number of points, n, in a region $\mathcal{R} \in \mathbb{R}^2$ follows a Poisson distribution with parameter λ and this probability is given by [3]

$$\mathbb{P}\{n \text{ nodes in } \mathcal{R}\} = \frac{(\lambda \cdot \mathbb{A}\{\mathcal{R}\})^n}{n!} exp(-\lambda \cdot \mathbb{A}\{\mathcal{R}\}) \tag{5}$$

where $\mathbb{A}\{\mathcal{R}\}$ is the area of the region $\mathcal{R}$. For calculating the realization of the spatial location of points we simply have to draw the number of desired points, n, using Poisson distribution with parameter $\lambda \cdot \mathbb{A}\{\mathcal{R}\}$ and scatter them across the region. Hence, this process can be used to deploy network nodes uniformly at random in a specific region.

2.3.3 *Random Networks*

Random Networks rely on the use of probabilistic models to represent the location of nodes belonging to these particular environments. Therefore, by using a stochastic model to deploy our devices over the network, we can better generalize the connections between the nodes of a point process in space, and determine, for example, the impact of noise interference or propagation effects for different spatial distributions. Such as the location, the connectivity of nodes can also be represented according to several types of bonds, using the complementary concepts of stochastic geometry (e.g. Boolean Model, Collision model, etc. [33]).

Pinto et al. [17] introduce this subject by analysing connectivity and throughput of packet radio random networks, the same kind of networks that we will consider in our work proposal. This article provides information about the the spatial distribution of nodes, more specifically of jammers and eavesdroppers. One of the main reasons behind the disposition of these nodes probabilistically, using PPP, is the fact that the position of these terminals is most of times unknown to the transmitter and receiver. Mathematically speaking, the probability of n nodes to be inside a region, $\mathcal{R}$, with area, A, to be:

$$P\{n \text{ in } \mathcal{R}\} = \frac{(\lambda A)^n}{n!} e^{-\lambda A}, n \geq 0 \tag{6}$$

where λ is the spatial density of nodes per unit area. If we account for the propagation characteristics, we get that the following power, P_B, received at distance R from a transmitter is given by

$$P_B = \frac{P_T \Pi_{k=1}^{K} Z_k}{R^{2\alpha}} \tag{7}$$

where P_T transmitted power, α the amplitude loss exponent and $\{Z_k\}$ the independent random variables which represent the different propagation effects (e.g. path loss, fading, etc.).

Pinto et al. also propose a different connectivity property designated: *audible/inaudible nodes*, depicted in *Figure* 11. This property is rather important, since it enabled the development of a cooperative jamming technique [18], which we accommodate, in the extended mathematical model, to further assess the secrecy impact of jamming in our UFH setting.

Definition 1. *(Audible Node [17]) - A node is audible to another node if its received power, P_B, is higher than a given threshold (sensitivity of the receiver), otherwise is inaudible. In other words, $P_B \geq \theta$.*

This connectivity property allows for the characterization of the number of audible nodes, N_A, of a given terminal X, which, as expected, is a random variable (r.v.) determined by the channel propagation characteristics and the density of the nodes. Furthermore, given the nature of this variable, the authors concluded that N_A is no other than a discrete Poisson r.v. with the following mean:

$$\mathbb{E}\{N_A\} = \mathbb{E}_{\{Z_k\}}\{\mathbb{E}\{N_A|\{Z_k\}\}\} = \pi\lambda\left(\frac{P_I}{\theta}\right)^{\frac{1}{\alpha}} \Pi_{k=1}^{K} \mathbb{E}\{Z_k^{\frac{1}{\alpha}}\} \tag{8}$$

where P_I is the transmit power of each interferer. To make this derivation Pinto et al. used the fact that for a node to be audible it must be contained within a circle with radius $r_d = (\frac{P_I \Pi_{k=1}^{K} Z_k}{\theta})^{\frac{1}{2\alpha}}$ and area πr_d^2 (represented by the term $\mathbb{E}\{N_A|\{Z_K\}\}$) multiplied by the spatial density, λ, of nodes. Considering that a *probe node* is a transmitter node that is deterministically deployed so that it distantiates R_0 from the receiver placed at the origin, while all other nodes are interferers whose random distances to the origin is represented by R_i, the throughput, T, of the system is then:

$$T = \mathbb{P}\{\text{probe } \textit{transmits}\}\mathbb{P}\{\text{receiver } \textit{silent}\} \times \mathbb{P}\{\text{probe } \textit{audible}\}\mathbb{P}\{\text{no collision with audible } \textit{nodes}\} \tag{9}$$

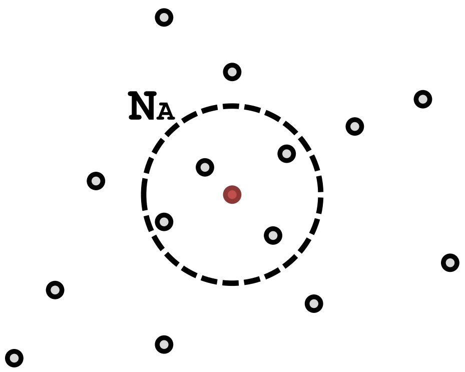


Figure 11.: *Audible Region (N_A).*

Win et al. [21] extend these results to account for the slow varying propagation effects - *quasi-static*. Moreover, it contrasts with the previous connectivity model because the authors no longer consider audible nodes as the only source of interference. In this approach, a node can hear the transmissions from all nodes in the network. As such, it was insightful to employ the SINR property and the outage probability to, subsequently, retrieve the throughput of the system.

$$SINR \equiv \frac{S}{I+N} \tag{10}$$

where S is the power of the received signal, I is the interference from the remaining active nodes in the network, and N is the constant noise power. Thus, I is the sum of the transmitted power of each interferer i, such that $I = \sum_{i=1}^{\infty} \frac{P_I \Pi_k Z_{i,k}}{R_i^{2\alpha}}$. As we no longer have an *audible* region, I can be determined by a *skewed stable distribution* that takes in consideration the randomness position of nodes and the propagation effects, in a similar way as the N_A r.v. from the previous model.

In this extended version, Win et al. no longer define the throughput as (9), but rather as

Definition 2. *(Throughput [21]) - The throughput, T, of a link is the probability of successfully receiving a packet, or in other words, the SINR must exceed an* ***audible threshold****, ξ.*

$$T = \mathbb{P}\{\text{probe } \mathit{transmits}\}\mathbb{P}\{\text{receiver } \mathit{silent}\}\mathbb{P}\{\text{no } \mathit{outage}\} \tag{11}$$

or

$$T = \mathbb{P}\{SINR \geq \xi\} = \mathbb{E}_{\{Z_k\}}\left\{F_I\left(\frac{S}{\xi} - N\right)\right\} \tag{12}$$

where, F_I is the cumulative distribution function (cdf) of the stable r.v I. Note that different propagation effects can change this probability.

It is important to mention that we plan to apply this stochastic model of network interference to mathematically represent jammers' impact on the eavesdropper and legitimate nodes.

2.4 Physical Layer Security

As hinted from previous sections, our work will focus on the characterization of a new physical layer security scheme using UFH and defensive jamming. Notwithstanding, in this section we provide an overview of physical layer security from its early stages to more recent advances and techniques [34], [35], including the use of jamming for secrecy.

2.4.1 *Physical Layer*

This paragraph is used to briefly describe 802.11 Physical Layer as presented in Gast's book [23]. The Physical Layer (PHY) is incorporated in the seven-layer OSI model of computer networking (see *Figure* 12) and integrates a series of basic networking hardware transmission technologies. As the first (lowest) layer it aims at transmitting information over a physical link connecting nodes. Most of times, transferred data is composed of bit streams or code words (groups of bit streams) that can be converted into signals and sent over hardware transmission mediums. PHY also combines a set of low-level parameters that identify for example: shapes and properties of the electrical connectors, transmission frequencies, modulation schemes, etc.

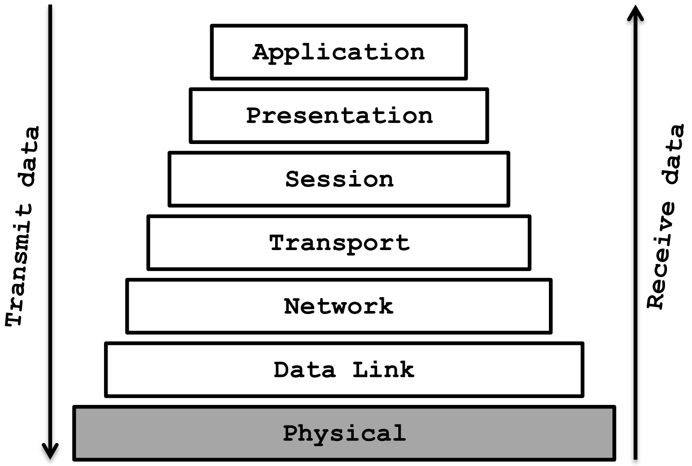


Figure 12.: *The seven layers of the OSI model.*

This Physical Layer is divided into two sublayers: *Physical Layer Convergence Procedure* (PLCP) and *Physical Medium Dependent* (PMD). The first one - PLCP - is responsible for communicating with the MAC protocol of the upper layer. The PMD is the layer in charge of transmitting any bits it receives using antennas or other transmission mediums. It is also defines transmission/reception details such as: bit timing, signal encoding, or properties concerning physical medium (e.g. Fast Ethernet).

PHY comprises a set of transmitting methods for radio signals like the aforementioned FH and DSSS. Others exist such as: Infrared light (IR), Orthogonal Frequency Division Multiplexing (OFDM), High-Rate Direct Sequence (HR/DS).

2.4.2 *Security at the Physical Layer - Early Stages*

Wireless communication systems are vulnerable to attacks, since their transmission medium is usually open and accessible to everyone. One of the most common types of attacks is eavesdropping, where unauthorized nodes try to intercept and read legitimate communication. In the past, researchers have focused most of their efforts in devising cryptographic schemes to cope with these security breaches, but recent approaches have tried new secure ways of transmitting information by harnessing the hidden power of the physical layer and ensuring some level of *information-theoretic security*.

Shannon's problem [7] was perhaps the first attempt at providing a information-theoretic security approach to address an eavesdropper attack. As illustrated by *Figure* 13, Alice (transmitter) and Bob (receiver) wish to communicate securely in a presence of Eve (eavesdropper). Shannon's model proposes the use of shared secret keys K_i, under a noiseless transmission medium (noiseless bit-pipes), to guarantee the safety transmission of a message M_i. Therefore, during each message broadcast, the data is encrypted, X, using a one-time pad approach - $X = M_i \oplus K_i$. Perfect secrecy is, thus, achieved whenever Eve cannot decipher M_i using X, or in other words, the mutual information, I, of M and X is:

$$I(M; X) = 0 \sim H(M|X) = H(M) \tag{13}$$

Therefore, M and X must be statistically independent in order to avoid providing any sort of information about each other to unauthorized users. $H(M|X)$, or *eavesdropper's equivocation*, measures the degree to which the eavesdropper is confused about the original message.

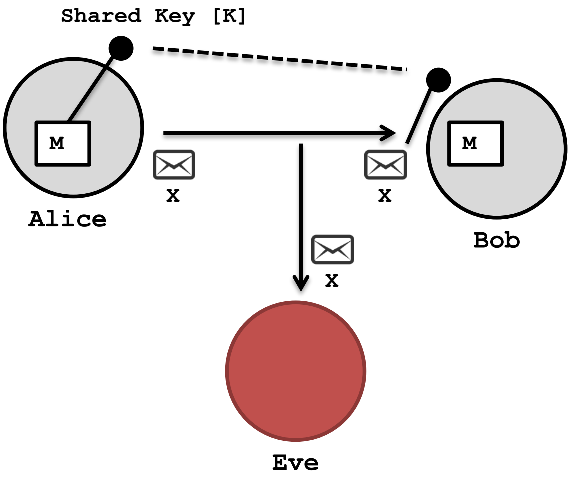


Figure 13.: *Wiretap Channel Model by Shannon.*

Unfortunately, Shannon proved that to achieve optimal secrecy, a different key is to be used to transmit each message, which, given its length (has to be as large as the message), is often too costly to implement efficiently. Therefore, to tackle this problem researchers shifted from information-theoretic security in lieu of computation-based security, employing public-key cryptography and subsequently, computationally hard problems (e.g. factoring integers into prime numbers) to encrypt/decrypt data.

Concurrently, Wyner [8] introduced a new concept to the conventional wiretap channel model - *noisy links*. In this case, as depicted in *Figure* 14, although Alice and Bob's channel and Eve's link are noisy, legitimate communication is still possible, whereas Eve's attempt to listen to the message is hampered by a degraded channel. Therefore, the main difference to the previous model lies on the existence of noisy channels which can be used to secure message transmission without needing a shared secret key. The goal is now twofold: to guarantee the maximum rate of secure transmission of data with a low probability of error to Bob; and to minimize the amount of information *fetched* by the eavesdropper.

Wyner also proposed a new secrecy condition entitled *secrecy capacity*, defined as the maximum rate at which a transmitter and receiver can communicate that guarantees reliability to Bob and security against the eavesdropper. Wyner's notion of security, also called *weak secrecy*, was relatively weaker and less strict, since this new definition did not required all bits to be successfully protected. As such, considering Z^n to be the degraded message received by Eve and M the original message, we have that in the limit of a large coding length n, there is a very small security leakage (a minimal amount of information can still be read by the eavesdropper):

$$\lim_{n\to\infty}\left[(\frac{1}{n})I(M;Z^n)\right] = 0 \tag{14}$$

Or, in other words, the *eavesdropper's equivocation* rate is very close to the message entropy rate for a large codeword length n:

$$\frac{1}{n}H(M|Z^n) \approx \frac{1}{n}H(M), n \to \infty \tag{15}$$

Yet, it is important to notice that this secrecy condition can still be strengthened (*strong secrecy*) [36] to maximize security, preventing any leakages. Nevertheless, as the secrecy capacity is the same [37], both definitions can result in security schemes that are more than capable of preventing messages to be successfully understood by Eve.

Wyner's results have demonstrated that it is possible to secure transmission of messages without using pre-shared secret keys if the eavesdroppers observation is a degraded version of the original legitimate message.

This last model gave us a clearer picture of what are the fundamental differences between cryptography and physical layer security. In a way, cryptography tends to be used (not exclusively) at higher layers of the protocol stack, whereas physical layer security is strictly bound to PHY, since it explores the inherent characteristics of this layer such as its randomness, signaling and channel coding properties.

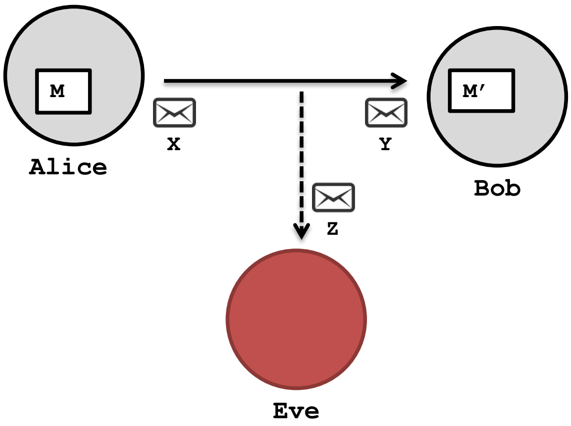


Figure 14.: *Wiretap Noisy Channel Model by Wyner.*

Picking up where we left off, Wyner's work led to some important conclusions about using the underlying randomness and channel characteristics to safeguard against eavesdropping. Later on, these results were further extended to a Gaussian wiretap model [38], where a different and more generic expression for the secrecy capacity was defined. Hence, secrecy capacity, C_S, turned out to be the difference between the channel capacity of Alice-Bob's link, C_B, and the that of the wiretap link, C_E.

$$C_S = C_B - C_E = \frac{1}{2}\log\left(1+\frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_E^2}\right), C_B \geq C_E \tag{16}$$

where P is the transmit power of the transmitter and σ is the correlated noise power. As expected, if this secrecy value falls below zero, the communication is deemed insecure, whereas for positive values secure communication can be obtained. The cost of secrecy can also be measured in terms of secure degrees of freedom (s.d.o.f.), which represents the secrecy capacity for a infinitely large P (i.e. $s.d.o.f = \lim_{P\to\infty} \frac{C_S}{\frac{1}{2}logP}$).

It is important to mention that some these calculations depend on the knowledge of Eve channel's statistics (e.g. probability distribution), and, as such, researchers tend to assume eavesdroppers follow normal protocols without attempting any jamming or tampering attacks. Still, values for this metric are hampered by degradation factors, such as fading, which can limit the secrecy capacity in wireless communications.

2.4.3 *Security at the Physical Layer - Recent Advances*

More recently, a set of new characteristics have been merged with the traditional artificial noise models to describe the nature of wireless networks, more specifically, channel qualities, e.g. fading channels.

Many fading models have been proposed to generalize the Gaussian wiretap model, and verify its usefulness for enhancing security. Bloch et al. [39] have successfully characterized quasi-static fading for these kind of systems and offered an outage for secrecy capacity. *Outage probability* for physical layer security measures the likelihood of the secrecy rate, R_S to be higher than the instantaneous secrecy capacity, C_S, for a particular fading distribution, which indicates the eavesdropper's channel is further degraded and secure communication is possible.

$$P_{out}(R_S) = \mathbb{P}\{R_S > C_S\}, R_S > 0 \tag{17}$$

Considering a setup similar to *Figure* 15, Bloch et al. proved that the secrecy capacity for quasi-static complex fading wiretap-channel was:

$$C_S = \begin{cases} log_2(1+\gamma_B) - log_2(1+\gamma_E), & \text{if } \gamma_B > \gamma_E \\ 0, & \text{if } \gamma_B \leq \gamma_E \end{cases} \tag{18}$$

where γ_B and γ_E are, respectively, the instantaneous realizations of the signal-to-noise ratio (SNR), which compares the level of a desired signal to the level of background noise, of the main and the wiretap channels.

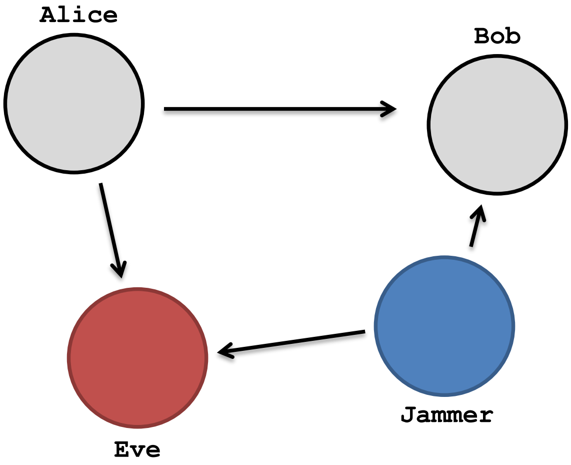


Figure 15.: *Wiretap Fading Model, an example of a wireless setup.*

Subsequently, the *outage probability* for a target secrecy rate, without CSI, is given by:

$$P_{out}(R_S) = \mathbb{P}\{R_S > C_S\} = 1 - \frac{\bar{\gamma_B}}{\bar{\gamma_B} + \bar{\gamma_E} 2^{R_S}} \exp\left(-\frac{2^{R_S}-1}{\gamma_B}\right) \tag{19}$$

where $\bar{\gamma_B}$ and $\bar{\gamma_E}$ are, respectively, the average SNR's of the main and the wiretap channels.

We pin-point the most relevant and recent models that now compose the repertoire of PHY security techniques. Withal, it is important to mention that defensive *jamming* mechanisms, as part of physical layer security and an indispensable element of our work, will have a section of its own later in the thesis (more detailed information there).

A multitude of new techniques have been proposed, relying on different methodologies, which can be used independently or grouped together, for example:

- *Multiuser Diversity* - determines the best possible way to use multiple-input multiple-output (MIMO), or multiplex data, to minimize wiretap channel capacity and maximize the main channel capacity;

- *Cooperative Diversity* - uses cooperative relay nodes to assist during a message transmission, to add diversity that helps legitimate users to better decode information;

- *Beamforming* - combines multiple antennas to transmit a single message in a particular safe direction (usually the eavesdropper lies in a different direction relative to the source node);

- *Channel or Network Coding* - interleaving message bits in a way that the receiver can securely and reliably read the data and the eavesdropper can not;

- *Directional Antennas/Sectorized Transmission* - uses nodes' possible disposition to offer new ways of avoiding eavesdroppers;

- *Jamming Defensive Interference* - employ jamming artificial noise to degrade eavesdroppers' channel.

The multiuser and cooperative diversity offer a new and interesting perspective for securing wireless transmissions which do not require the use of jammers to tamper the eavesdropper channel. Furthermore, they somehow mitigate the problem of some of the conventional artificial noise models, by reducing the need for additional power resources. Zou et al. [9], [40] have suggested three new security techniques which encompass most of these two concepts: using MIMO coupled with an *adaptive transmit process*; tweaking multiplexing mechanisms (i.e TDMA) in a multiuser environment to improve secrecy; and inserting relay nodes and cooperative beamforming.

For MIMO diversity, Zou et al. recommended combining the underlying increased capacity of this technique (multiple antennas at source and destination), which combats wireless fading, with three *adaptive transmit processes*: transmit beamforming, power allocation, and transmit antenna selection. The first method employs beamforming techniques by directing the desired signals to a particular direction, which can be significantly effective if the eavesdroppers are spatially separated. The second and third one rely, respectively, on allocating transmission power among certain antennas at source nodes or choosing a set of optimal antennas, that maximize security, to transmit data. Yet, as it happens with many of PHY security mechanisms, these techniques require channel state information (CSI) that is most of the times inaccessible (eavesdroppers remain silent).

In fact, the increasing interest in MIMO systems led to the *'arrival'* of an incredibly large number of physical security techniques related with this technology. It all begun with Hero's work [41] who tried to design a CSI-dependent transmission strategy using MIMO to reduce either the probability of interception, or the probability of detection by an eavesdropper.

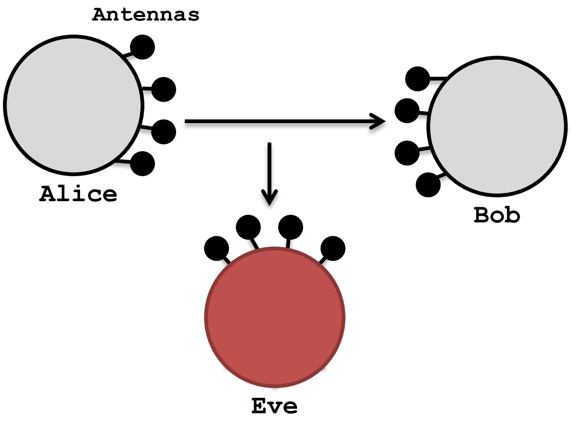


Figure 16.: *MIMO wiretap channel.*

These initial ideas were extended to design the MIMO wiretap channel model [42], represented by *Figure* 16. However determining the secrecy capacity under this setup is not straightforward, and most proposals still assume strong conditions such as accessibility to the eavesdropper's CSI.

Other contributions exist that involve the MIMO/MISO (multiple-input single-output), for example: a detection-theoretic method for exposing passive eavesdroppers based on their local oscillator leakage power [43]; a full-duplex eavesdropper model, which is capable of diving its antennas into two subsets to concurrently jam and eavesdrop a target communication channel [44]; or the MIMO secrecy capacity for OFDM-based channel selection [45].

A distinct way to provide security using multiuser diversity is to change the basic process behind multiplexer systems, such as TDMA or Orthogonal Frequency Division (OFDMA). Hence, in this case, Zou et al. [9] proposed the use of a different selection criteria where nodes were no longer chosen exclusively based on their throughput rate, for example, to access the given OFDM subcarrier, but also based on their channel's characteristics that could potentially enhance security.

Finally, for cooperative diversity, the authors attend to the security problems of basic relaying networks [40], which are prone to a higher number of eavesdropper's attacks - from transmitter to relay nodes and from relay nodes to source. For solving that, they came up with a cooperative beamforming scheme which uses the multiple relays to retrieve data from experience, to choose the optimal destination/direction.

Another way to secure communications using physical layer security is to consider the nonexistence of CSI and model a set of techniques using spatial deterministic models, for example Poisson Point Process (PPP), which work with random disposition of nodes with a λ density. As previously described, introducing spatial information allows for a more precise analysis of the underlying secrecy in a multitude of scenarios. Pinto et al. work on these kind of models gave us a clearer perspective of the power of eavesdroppers in a surrounding region, for example, for a large scale network [46] or when they are capable of cooperation (colluding attacks). [47].

For the first scenario, Pinto et al. explored some strategies for networks with a large number of nodes using: *sectorized transmission* and *eavesdropper neutralization*. To account for this large scale, Pinto et al. employed iS graphs [11], see *Figure* 17, or in other words, *secrecy graphs*, to represent local connections between participants. They have also opted for a different evaluation metric - *average node degree* (a.v.n.) - which measures the secure connectivity of each node in the graph. Results show that without enhancement $a.v.n. = \frac{\lambda_B}{\lambda_E}$, where λ_B is the density of the legitimate nodes and λ_E is the density of the eavesdroppers, according to a spatial stochastic model, as described in section 2.3.2. By limiting the transmissions to within L sectors of the plane, using a set of directional antennas, local connectivity is linearly increased according to the number of transmission sectors, $a.v.n. = L\frac{\lambda_B}{\lambda_E}$. Finally, considering that each node is able to neutralize eavesdroppers in a certain region, this value increases exponentially with the radius, p, of the neutral area, $a.v.n. = \frac{\lambda_B}{\lambda_E}(\pi\lambda_B p^2 + e^{\pi\lambda_E p^2})$.

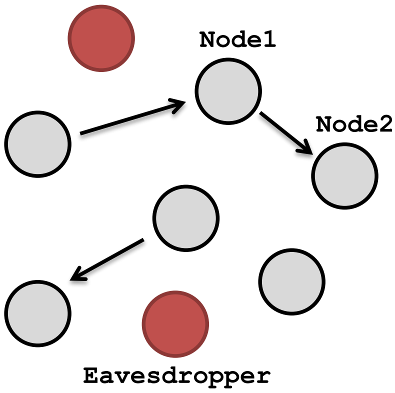


Figure 17.: *Example of an iS graph.*

For the second scenario, Pinto et al. proved that even a modest number of cooperative eavesdroppers, can highly reduce the security level of conventional PHY security techniques. For that they came with the secrecy capacity for a wiretap channel model with colluding eavesdroppers and a arbitrary spatial process and its corresponding characteristic statistical function (using homogeneous PPP to distribute the nodes).

$$C_S = \max\left\{ \log_2\left(1 + \frac{H_M P}{W_M}\right) - \log_2\left(1 + \frac{P_E}{W_E}\right), 0\right\}, \tag{20}$$

where P_E is the aggregate power received by eavesdroppers, W_E is the noise of eavesdroppers and W_M, H_M are, respectively, the noise and the gains of the main channel.

To conclude this section and complete our shortened list of PHY security mechanisms, we introduce some jamming defensive interference, more specifically a few cooperative jamming approaches [35] using: *Gaussian Noise*, *Alignment* and *Structured Codes* . It is important to add that there are more artificial noise techniques apart from these ones, and some of them will be fully described in the next section, as they convey important knowledge for our projected work.

Cooperative Jamming is used to describe the phenomenon of collaborative interference, which can, for example, be generated by independent transmitters who unintentionally interfere with both the eavesdroppers' channel and the legitimate receiver. Although it may look inconvenient, the truth is that this interference can yield security benefits and, subsequently, secrecy gains even when jamming the communication channel. As we can see from *Figure* 18, Alice and Amy wish to communicate with Bob, while Eve tries to overhear communication. In this particular scenario, both Alice and Amy interfere with each others transmission while disrupting Eve. As Amy possess the strongest channel (i.e. is closer to Eve) she can thus decide to forfeit her communication attempts and instead help Alice and Bob by injecting noise to the system, thus increasing Alice's secrecy capacity. The *Gaussian Cooperative Jamming* [5] recommends the use of independent identically distributed (i.i.d) Gaussian noise signals, while others (e.g. Structured Codes) propose a different kind of signal.

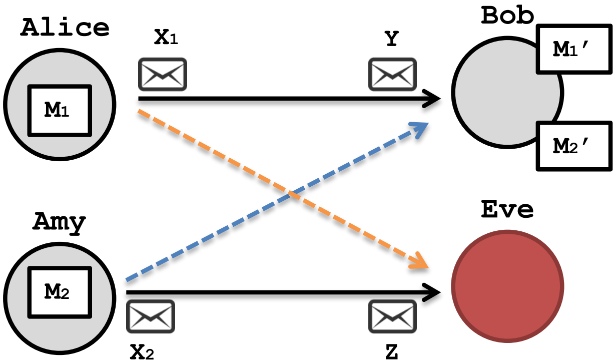


Figure 18.: *Two-user multiple access wiretap channel.*

This situation can be generalized for a set of K helpers who can work together to increase the *eavesdropper equivocation*. Tekin and Yener [5] described the overall secrecy capacity of the Cooperative Gaussian Model as:

$$C_S = \frac{1}{2}\log\left(1+\frac{h_1^2 P}{\sigma_B^2 + h^T Q h}\right) - \frac{1}{2}\log\left(1+\frac{g_1^2 P}{\sigma_E^2 + g^T Q g}\right) \tag{21}$$

where $h = (h_1, h_2, ..., h_K)$ is the vector of channel gains to the receiver node (Bob), $g = (g_1, g_2, ..., g_K)$ is the vector of channel gains to the eavesdropper (Eve), $x = (x_1, x_2, ..., x_K)$ is the vector of jamming signals from the K helpers and Q is the covariance matrix of x.

Given the underlying spatial requirements correlated with this technique (e.g. which node is closer to Eve?), many researchers have successfully improved the secrecy capacity of this scheme by introducing beamforming, coding and signaling mechanisms.

To mitigate the hazardous effect of artificial noise caused by helper nodes, working as jammers, on the legitimate communication, some different methods were developed. *Structured Codes*, *Interference Alignment* are some of the examples, although others exist.

Structured Codes [10] behave exactly like the Gaussian noise model but instead Alice and Amy send a set of signals with a specific structure, which can then be nulled out at the intended receiver. *Table* 1 provides a simplistic example of this technique. Because of the inherent code structure, interference and different propagation effects, Bob is able to extract most of the intended bits, whereas Eve gets a jumbled version of the message because both signals are completely aligned. He and Yener [10] were also able to prove that the ratio of secure communication, in this case, was $C_S > 0$ and $\lim_{L\to\infty}(\frac{C_S}{L}) = 0.5$, where L is the number of message bits.

Message [Alice]	Message [Amy]	Message [Bob]	Message [Eve]
$a_4 0 a_3 0 a_2 0 a_1 0 a_0$	$b_4 0 b_3 0 b_2 0 b_1 0 b_0$	$\begin{array}{r} a_4 \quad 0 \quad a_3 \quad 0 \quad a_2 \quad 0 \quad a_1 \quad 0 \quad a_0 \\ +b_4 0 \quad b_3 \quad 0 \quad b_2 \quad 0 \quad b_1 \quad 0 \quad b_0 \quad 0 \\ \hline b_4 a_4 b_3 a_3 b_2 a_2 b_1 a_1 b_0 a_0 \end{array}$	$\begin{array}{c} a_4 0 a_3 0 a_2 0 a_1 0 a_0 \\ +b_4 0 b_3 0 b_2 0 b_1 0 b_0 \\ \hline c_4 s_4 c_3 s_3 c_2 s_2 c_1 s_1 c_0 s_0 \end{array}$

Table 2.: *Cooperative Jamming using Structured Codes. a_i and b_i represent message bits.*

Although this secrecy level may look kind of low, recent work on coding for wiretap channel, such as explicit codes or polar codes, have enhanced this system secrecy capacity. Nonetheless, it is important to mention that the existent models for physical layer security do not yet guarantee complete secrecy without some strong assumptions (e.g. CSI).

Interference Alignment relies on signal adjustment [48] to improve secrecy capacity. More specifically, considering the K-helper case, the transmitter Alice divides her message in K parts, while each helper jammer transmits K interference signals. Using Bob's CSI, all of the submessages are aligned at Bob using the same dimension, whereas at Eve they are received at random dimensions (no real alignment). Therefore, Bob is able to separate the noise, with a probability of error, from the actual data and read the message, while Eve is incapable of doing so.

This section offered a quick look into different physical layer security techniques as well as some of their inherent advantages and limitations. Still, there is many things to be done to guarantee the complete safety of message transmission, and many of the satisfiable schemes still rely in strong assumptions. As part of our work, we will focus on defensive jamming interference coupled with the previously described UFH model, without using CSI knowledge and relying instead on spatial stochastic models [11]. This way, we can more realistically portray an ad-hoc scenario, where eavesdroppers usually remain hidden and there is only a statistical description of the location of nodes and possible density of attackers. Furthermore, our spatial model will also account for path loss for calculating the secrecy capacity and secure throughput of this system.

2.5 Jamming

Jamming is mostly seen by many as a way of disrupting wireless communications by interfering with the transmitted signals. In fact, DoS attacks are frequently caused by jamming, which consistently disables node's ability to communicate by generating high noise power, introducing fake packets or sending a overburdening amount of information which clogs up wireless channels. However, the increasing popularity of physical layer security mechanisms led to a substantial shift in the way we look at jammers. These devices are now being used as a way of defending against intruders, more specifically, as a way of combating eavesdroppers' attempts at listening to confidential information and, subsequently, increase the secrecy capacity of wireless networks.

This section aims to describe some important defensive jamming techniques, some of which will be employed to enhance the UFH security scheme, and to demonstrate the potential of using both mechanisms to defend against eavesdroppers. We will further explain the concept of cooperative jamming, briefly introduced in section 2.4.3, as well as, describe position-based jamming using stochastic spatial models. We will, however, start by presenting the other side of the coin - jamming for disrupting wireless communications - as well as, indicating some limitations of defensive jamming.

2.5.1 *Conventional Types of Jamming*

Traditionally jammers are used as a way of disrupting wireless networks by generating a high noise power close to the transmitter and/or receiver. *Offensive jamming*, as we will call it, as been used for multiple purposes, for example, during war efforts to bring down specific network nodes and shutdown any communication between soldiers, or for rattling sensor networks.

There are numerous types of jamming, [49] with different strategies and characteristics, for example:

Trivial	Generates continuous noise for a given duration of time.
Periodic	Generates a periodic noise pulse of defined length and transmission power, remaining silent between pulses.
Intelligent	Knows the underlying protocols, targeting specific signals/packets important during communication (e.g *Clear-to-Send* (CTS) packets at the MAC layer).
Static	Remains in the same channel or group of channels (frequency band).
Sweep	Tries to cover up the entire bandwidth by systematically updating jammed channels.
Random	Randomly jams a target frequency band for a brief period of time before switching to another one.
Responsive	Jams whenever it detects a signal transmission.
Hybrid	Combines different strategies (i.e. continuously jams but keeps looking for other signals in other frequency bands).

Table 3.: *Jammer classification.*

Hence, *Table* 2, provides us with a quick look on some jamming categories. However, it is worth mentioning that many more classes exist that relate to the duration of activity, the nature of traffic being targeted or the underlying communication protocols deployed in the network.

Thuente and Acharya [50] have revealed that using protocol knowledge, in a base station oriented network, makes jammers a much stronger assailant, requiring less energy and reducing the probability of detection (stealthiness). Furthermore, they prove that misbehaving nodes who can access the network (authenticated users) can provide a very strong source of intelligent jamming, nearly undetectable, which can dramatically reduce network throughput.

As previously stated, SS techniques can help reduce jamming probability through various mechanisms. For example, as depicted by *Figure* 19, using FH or UFH, which involves hopping among a set of known frequencies, enables nodes to partially avoid jammed frequency bands (at least whenever they land in a interference-free channel).

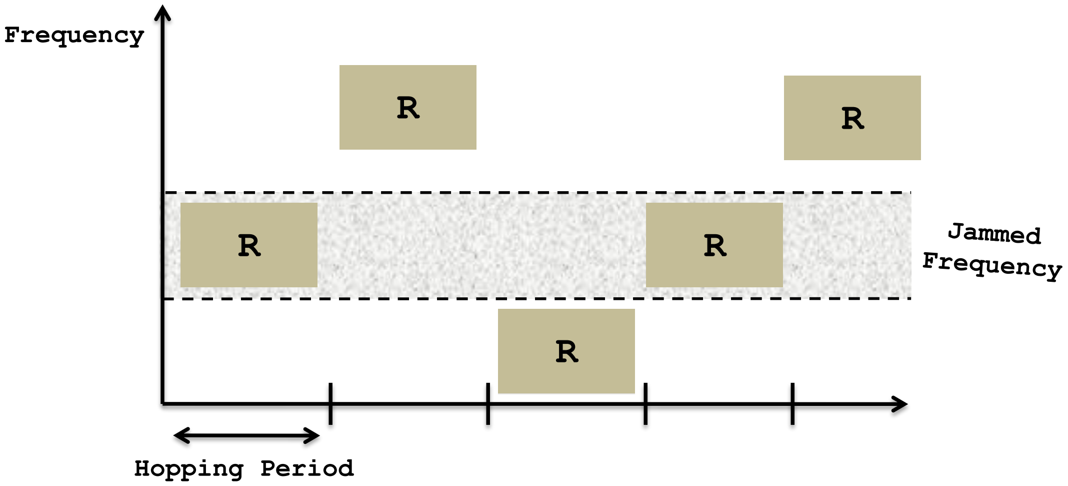


Figure 19.: *Avoiding Narrowband Jamming using FH. In this case node R continuously jumps among a set of pre-established frequencies trying to communicate with his homologous node.*

2.5.2 *Cooperative Defensive Jamming*

As we have seen in PHY security section, noise interference from jamming can be a used to enhance the secrecy capacity, therefore improving secure transmissions of data between nodes. Defensive noise interference has had an increase in popularity and many different schemes have been proposed. *Cooperative jamming*, introduced by Tekin [5] and Goel [6], has been one of them, but others exist, for example: secure relaying by adding artificial noise [12]; make use of additional antennas at transmitter [6] or receiver [13], [14] to introduce noise in the system and degrade eavesdropper's channel.

Nonetheless, substantial body of literature focus on what researchers call *cooperative jamming*. This security mechanism tries to prevent eavesdropper attacks by combining the efforts of external helpers, in order to enhance the system's security level.

Section 2.3 already introduces some of these techniques such as: cooperative jamming by *Gaussian noise*, *structure codes* or *signal alignment*. Common to all of these is the presence of external helpers, such as jammers or other nodes in space, who actively contribute to the overall system secrecy capacity.

Notwithstanding, several other similar schemes have been proposed. Sankararaman et al. [51] propose an optimization scheme in a storage/fence model, relying on: a cooperative scenario, where all the jammers's interference is combined at the receiver; and on a semi-cooperative approach, where only the K best jammers are chosen to attempt at degrading eavesdroppers' connection. They also present one complex algorithm for placing jammers inside the fence to optimize security, which was extended to provide a combined solution involving the number of necessary jammers and their required power levels, to prevent any attacks by an outsider.

Capar et al. [2], [15] presented some achievable scaling results for 1-D and 2-D large networks, defining two different algorithms to improve security levels, in the presence of eavesdroppers with unknown locations. In this case, instead of using secrecy capacity, authors opted to use two different metrics: the *secure throughput*, and the number of eavesdroppers that can be tolerated. The first one is particularly important for this thesis since it is going to be extensively used to evaluate all our different propositions.

Definition 3. *(Secure Throughput [18]) - The per-node* ***secure throughput*** *is the probability that a message transmitted by a transmitter is fully received by a receiver, and unsuccessfully received by every eavesdropper.*

For preventing attacks on 1-D networks, Capar et al. proposed a technique based on a routing algorithm, using legitimate nodes which relay the message and others that jam possible eavesdroppers. As depicted by *Figure* 20, the one dimensional network, composed of n legitimate nodes, is divided into multiple non-overlapping cells with a pre-determined length, and a couple of regions, which help secure the routing of the message. What happens is that the packets are first routed in single cell hops until they reach the neighborhood of a certain region, represented by the coloured rectangles. There the message is routed from a relay node A, in the beginning of the region, to a relay node B, in the end of the region, while a another node acts as jammer and transmits artificial noise. Coupled with TDMA and assuming that for an eavesdropper to read the message he has to collect all different transmitted packets, Capar et al. proved that with a density of $\lambda_E = \frac{1}{log(n)}$ eavesdroppers (placed according to a PP distribution) the per-node secure throughput of this cooperative approach is approximately $\frac{1}{n}$.

Similarly, for the 2-D network, although this time with different paths of cells, they were able to achieve a per-node secure throughput of $\frac{1}{\sqrt{nlog(n)}}$ under the same conditions (same density of eavesdroppers).

One important thing to consider for both Sankararaman and Capar works is that they consider path loss. Therefore, in this case, the received power at the destination, B, with

α as the path loss exponent, P_A as the transmit power and $\overline{AB}$ the distance from A to B, is modeled as:

$$P_B = \frac{P_A}{\overline{AB}^{\alpha}} \tag{22}$$

Hence, to successfully transmit a message under these conditions, the SINR of the receiver must exceed a certain threshold, τ_B, whereas the SINR of the eavesdropper must be lower than, τ_E, such that $\tau_B > \tau_E > 0$, or in other words:

$$SINR_B \equiv \frac{P_B}{N_0 + I_B} > \tau_B \tag{23}$$

where N_0 is the power of the additive Gaussian noise, and I is the interference received as artificial noise. From a information-theoretic perspective, the positive secrecy rate, R_S is given as:

$$R_S = \frac{1}{2}(log(1 + SINR_B) - log(1 + SINR_E)). \tag{24}$$

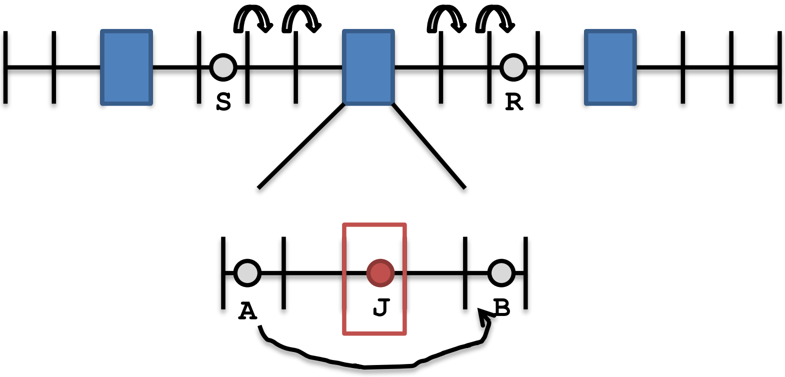


Figure 20.: *A cooperative jamming approach for 1-D network [2]*

Vilela et al. [16], [52] propose a different jamming scheme for proving the importance of cooperative jamming, which although similar in terms of objective, introduces some changes such as: new security metrics, different jamming strategies, and the inclusion of a fading + path loss model. Primarily focusing on a simple scenario with one transmitter A, one receiver B, one jammer J and one eavesdropper E, the authors evaluate secrecy performance in terms of outage probability, jamming coverage and efficiency, proving that the inclusion of a single jammer could be insufficient to provide a good security level. Closely resembling Bloch et al. [39] work on fading models, this time SINR at the receiver is represented as a random variable:

$$SINR_B = \frac{C_{AB}G_{AB}}{1 + C_{JB}G_{JB}}. \tag{25}$$

where, $C_{JB} = \frac{P_J C}{N_0 d_{JB}^{\alpha}}$, $C_{AB} = \frac{P_A c}{N_0 d_{AB}^{\alpha}}$ and G_{AB}, G_{JB} are independent exponential random variables with unit means and c is a normalization constant. The eavesdropper SINR follows the same reasoning and, since the presence of fading ensures a non-zero probability of not achieving a specific secure rate, R_S, this leads to the following secrecy outage probability:

$$P_{out}(R_S) = P\{C_S < R_S\} = P\{C_B - C_E < R_S\} = P\{log(1 + SINR_B) - log(1 + SINR_E) < R_S\}. \tag{26}$$

In terms of jamming strategy, Vilela et al. studied three different situations: *Blunt Jamming*, *Cautious* and *Adaptive*.

STRATEGY	CSI	ENERGY
Blunt	No CSI knowledge	Constant power: $P_{blunt} = P_J$
Cautious	Receiver and eavesdropper CSI	$P_{cautious} = \begin{cases} P_J, & \text{if } \frac{G_{JB}}{d_{JB}^{\alpha}} < \frac{G_{JE}}{d_{JE}^{\alpha}} \\ 0, & \text{otherwise} \end{cases}$
Adaptive	Receiver CSI	$P_{adaptive} = \begin{cases} P_J, & \text{if } G_{JB} < \theta \\ 0, & \text{otherwise} \end{cases}$

Table 4.: *Jammer classification.*

Table 3 highlights some of their characteristics, especially in terms of power consumption and CSI knowledge. In other words, *blunt jammer* keeps jamming all the time, *cautious* only jams whenever the channel to the eavesdropper is better than the channel to the receiver and *adaptive* defines a threshold of the channel quality, θ, above which will stop jamming as it might degrade the legitimate communication. Results pointed to the fact that, even though a single blunt jammer can provide with an average coverage and security efficiency, relying on cooperative multiple jammers or on CSI knowledge (different strategies) is mandatory to further improve the outage secrecy capacity, and the coverage/efficiency of jamming in wireless systems.

Vilela et al. following work [52] analyses this issue by including more than one defensive device and devised a new formula for the secrecy outage probability, $P_{out}(R_S)$. In this case, using all the available strategies previously described, results show a significant increase in the security level. In terms of coverage, multiple jammers offer a clear advantage over a single defensive device. Nonetheless, as expected, jammers too close to the receiver might negatively interfere with the communication. As for efficiency, if no power sum restrictions exist, the energy expenditure is much higher but leads to a significant improvement of secrecy levels. Therefore, the authors suggest a trade off between jammers' power levels and potential security benefits.

Following a different direction, Tekin and Yener [5] propose a cooperative jamming technique which uses the multiple-access nature of channels, of different nodes, to improve the secrecy of a system assailed by strong eavesdroppers, capable of accessing the message through the same type of channels. Authors were capable of mathematically characterizing this scenario, defining the achievable secrecy sum rate as metric for this multi-access system. This enabled them to conclude that this secrecy sum rate is maximized whenever the disadvantage users help disrupt the eavesdropper. The more degraded the transmitting user is, the more capable he is to jam nearby assailants. However, it is important to notice that this work relies on CSI knowledge about the eavesdroppers and fails to provide a generalized secrecy capacity for this multiterminal environment, something that is yet to be fully accomplished (without some strong assumptions).

2.5.3 *Position-Based Defensive Jamming*

Of all the different techniques based on artificial noise and/or cooperative jamming, we decided to focus on a smaller group of approaches based on the relative statistical position of nodes, which entails a set of different concepts to be described in this subsection. Therefore, we decided to mention a set of articles with the following main characteristics, which embody our plan on how to accommodate defensive jamming interference in a UFH security setting.

- *Spatial Stochastic Models* [31] - The spatial location of nodes is taken into consideration in order to calculate the underlying security of a given network system;
- *PP distribution of nodes* [32] - The location of interfering devices is modelled in a probabilistic manner (using concepts like distance and density of nodes);
- *Propagation effects* [30] - Considers the existence of fading channels and other propagation characteristics such as path loss or shadowing;

Making use of the concept of audible nodes presented in section 2.3.3 Vilela et al. [18] propose a new position-based security scheme where eavesdroppers are randomly placed in unknown positions, while jammers are deployed according to a set of strategies. This technique does not rely on eavesdroppers' CSI, but alternatively analyzes parameters such as the density and spatial distribution of eavesdroppers and jammers, as well as, the active interference region, and of audible nodes (*Definition 1*). The scheme comprises a transmitter, A, a receiver, B, and a set of jammers, J, and eavesdroppers, E. To assess the level of secrecy for communication, the authors decided to use the *secure throughput*, T_S, as presented in *Definition 3*.

This metric admits an outage interpretation as it considers a simple log-distance path loss model, which changes its interpretation and related mathematical formula. Hence, an approximate expression for the secure throughput is given by

$$\tilde{T_S} = exp(-\lambda_J \mathbb{A}\{\mathcal{B}_{x_B}(r_{J,B})\})exp(-\lambda_E \pi r^2_{A,E} p_{J,E}), \tag{27}$$

$$p_{J,E} = \frac{1}{\pi r^2_{A,E}} \iint_{\mathcal{B}_{x_A}(r_{A,E})} exp(-\lambda_J \mathbb{A}\{\mathcal{B}_{x_E}(r_{J,E})\}). \tag{28}$$

λ_J is the density of the eavesdroppers, $\mathbb{A}\{\mathcal{B}_{x_B}(r_{J,B})\}$ is the area of the ball inside which the jammers can interfere with the receiver, $\mathbb{A}\{\mathcal{B}_{x_E}(r_{J,E})\}$ is the area of the ball inside which the jammers can interfere with an eavesdropper at position x_E, $\mathbb{A}\{\mathcal{B}_{x_A}(r_{A,E})\}$ is the area of the ball inside which the eavesdroppers can hear the transmitter and $r_{k,y}$ is the radius between k and y such that $r_{k,y} \equiv \left(\frac{P_k}{\theta_y}^{\frac{1}{2\alpha}}\right)$ with θ as the *audible threshold* (check *Definition 2*).

To analyze the trade-off between the effect of jammer collisions on the eavesdroppers and on the receiver, Vilela et al. considered 4 different jamming disposition and selection strategies: *no jamming*, *global jamming*, *near-receiver contention* and *near-source jamming*. *Table* 4 encompasses some of their characteristics and correlated secure throughput, while *Figure* 21 show us how the last two new strategies work.

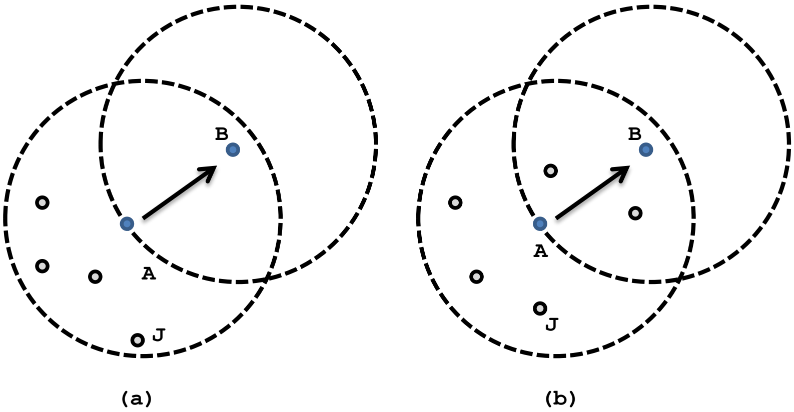


Figure 21.: *(a) represents near-receiver contention where jammers, J, are placed in the audible region of the transmitter, A, but outside of the receiver's reach, B. (b) represents near-source, where jammers can be arbitrarily deployed inside the A's audible region and can eventually interfere with B.*

Strategy	Harms B	Secure throughput
No Jamming	No	$\tilde{T}_S = exp(-\lambda_E \pi r^2_{A,E})$
Global	Yes	$\tilde{T}_S = exp(-\lambda_E \pi r^2_{J,B}) exp(-\lambda_E \pi r^2_{A,E} exp(-\lambda_E \pi r^2_{J,E}))$
Near-Receiver Contention	No	$\tilde{T}_S = exp(-\lambda_E \pi r^2_{A,E} p_{J,E})$
Near-Source	Yes	$\tilde{T}_S = exp(-\lambda_E \pi r^2_{A,E} p_{J,E}) exp(-\lambda_J \mathbb{A}\{\mathcal{B}_{x_B}(r_{J,B}) \cap \mathcal{B}_{x_A}(r_{A,E})\})$

Table 5.: *Jammer selection strategies.*

Results show that the use of jamming improves the secure throughput in a multi-terminal environment. However, the placement of the jammers must be adequate to minimize the negative impact on the legitimate communication. Therefore, jammers should not be deployed near the legitimate receiver, and their power should be controlled to allow for the maximization of their security benefits. Thus, as expected, the near-receiver contention strategy exhibits the best security gains, which scale well with the density of jammers, whereas near-source jamming worsens with increasing λ_J (due to a higher number of collisions over B). Finally to conclude this section, we would like to mention that friendly jamming models are still limited and much works needs to be done to safely guarantee perfect secrecy in wireless networks using these PHY security techniques. Tippenhauer et al. [53] disclose a series of disadvantages such as: the impracticability of friendly jamming near the message source; the need, in some cases, for eavesdroppers' CSI for maximum efficiency; or the inability to cope with very strong assailants or colluding attackers.

Our security scheme offers another alternative to improve defensive noise-interference techniques by adding a SS mechanism, UFH, to create more randomness and reduce the eavesdroppers' ability to decode the legitimate message. Hence, by using UFH, we can actually fabricate a way of communicating using a frequency channel which is not compromised by any attacker. Furthermore, since we will continue to include cooperative jamming, we are able to mitigate some of the eavesdroppers malicious intents whenever these devices, by chance, land on the same frequency band of the transmitter and receiver. Preliminary results show that UFH combined with jamming can provide benefits in terms of security efficiency even in a disadvantageous situation (e.g. high density of eavesdroppers). Finally, this scheme can also prove favorable when the eavesdropper is not degraded (e.g. located nearer to the source than the receiver), offering some protection by means of frequency diversity.

2.6 Software-Defined Radios

Software-defined radios (SDRs) are radio communication systems that operate in a similar way as actual hardware devices and usually include a set of components (e.g. filters, modulators/demodulators), which are implemented through software. These devices, such as the B210 (`http://www.ettus.com/product/details/UB210-KIT`) from National Instruments, employed in our test-bed, are equipped with analog-to-digital converters, as well as, radio frequency (RF) front ends that allow for the transmission and reception of different radio signals. The more traditional hardware based radio devices are considerably limited in terms of flexibility and can only be modified through physical intervention. On the other hand, SDRs encompass a series of elements powered by software making them *flexible* to changes, supporting a myriad of radio protocols, schemes, and mechanisms associated with signal transmission (e.g. physical layer protocols, multi-band) with significant utility and cost-efficient [54].

SDRs are, thus, seen as a collection of hardware and software components, where some or all of the radio's operating functions are implemented using software/firmware that can be altered on a whim. These devices include field programmable gate arrays (FPGA), digital signal processors (DSP) or other application specific processors, that can be programmed using specific toolkits such as Gnuradio, LabView or Matlab. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without needing to acquire new hardware. Recently, SDRs have become a very popular tool to experiment on since they accurately represent real hardware devices commonly used, and are geared up with an extended array of tools that allows them to easily adapt to different scenarios. Here are some of the benefits.

- New features and capabilities can be added without requiring major expenditures;

- A family of radio *products* can be implemented using a common platform architecture (e.g. Gnuradio);

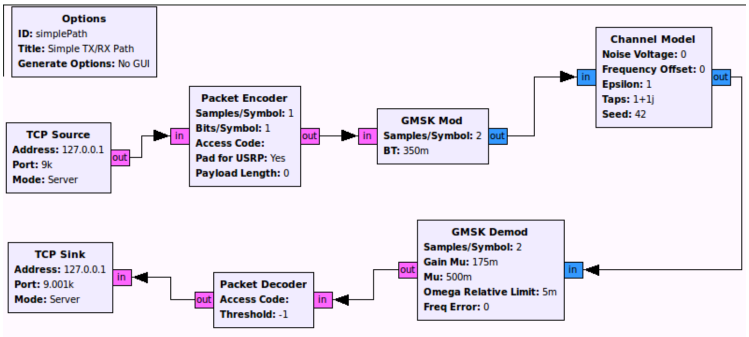
- Remote reprogramming, allowing variables to be changed while a radio is in service.

2.6.1 *Gnuradio*

Gnuradio is an open source toolkit designed to implement software radios that combines C++ and Python. It is organised in a simulation-like runtime environment and is divided into two different layers, one inner-layer (C++) where the computationally intensive processing blocks are implemented and an outer-layer (Python) that controls and coordinationates these blocks. Gnuradio introduces a series of core software modules, in particular, the *GR_block*, the *GR_top_block*, the *flowgraph*, the *sheduler* and the *GR_buffer*.

GR blocks are the key components of Gnuradio and encapsulate a series of data/signal processing functions, such as filters (*gr_iir_filter, gr_fir_filter*), decimators, modulators, etc. Each block may have one or multiple data/signal input stream(s) and/or output stream(s). Source/Start blocks only have input streams, whereas sink/end blocks only have output streams. Each of these objects has a work function that does the real computation, which usually involves gathering up input data, processing the items and dispatching them to the output stream(s). Different GR blocks vary depending on the implementation of the work function. Each block can be connected to another through GR buffers, which hold the data using a circular buffer, typically with the system page size, thus, providing adjacent blocks a way of exchanging information. GR blocks can be combined to form a *flowgraph*, which can be started using a GR top block, also responsible for executing the system scheduler. Gnuradio uses a scheduler that allocates a separate thread for each block's execution, allowing them to continuously loop until the program is terminated. In each loop, the threads begin by calling the block's executor (a function that checks buffers) and then the work function to start processing data. If buffers are empty or idle, the block waits for any changes to occur before calling the work function. Following the above mechanism, all the blocks in a *flowgraph* continuously process incoming data chunk by chunk.

Gnuradio also has a piece of software attached to it, *Gnuradio companion* (GRC), that eases out the task of combining blocks and tweaking variables. *Figure* 22 shows an example-code using the aforementioned layout, depicting a simple *flowgraph* intent on reproducing wireless communication (*gr_channel_model* block simulates a wireless channel). Finally, Gnuradio can easily be combined with SDRs using the UHD block library (i.e. *gr_usrp_source*, *gr_usrp_sink*), allowing the implementation of our test-bed.



Options
ID: simplePath
Title: Simple TX/RX Path
Generate Options: No GUI

TCP Source
Address: 127.0.0.1
Port: 9k
Mode: Server

Packet Encoder
Samples/Symbol: 1
Bits/Symbol: 1
Access Code:
Pad for USRP: Yes
Payload Length: 0

GMSK Mod
Samples/Symbol: 2
BT: 350m

Channel Model
Noise Voltage: 0
Frequency Offset: 0
Epsilon: 1
Taps: 1+1j
Seed: 42

GMSK Demod
Samples/Symbol: 2
Gain Mu: 175m
Mu: 500m
Omega Relative Limit: 5m
Freq Error: 0

Packet Decoder
Access Code:
Threshold: -1

TCP Sink
Address: 127.0.0.1
Port: 9.001k
Mode: Server

Figure 22.: *Simulating wireless communication using GRC.*

3

PRELIMINARY RESULTS

In this section we evaluate the combined usage of jamming with narrowband (single frequency) and broadband (multiple frequencies) UFH for secrecy against eavesdroppers by means of a simplified mathematical representation and corresponding simulation using Monte Carlo experiments. We show that the number of available frequencies can be adjusted so as to reduce the effect of adversary eavesdroppers; and jammers can greatly aid in providing higher levels of security by causing interference to eavesdroppers. We will, therefore, evaluate how narrowband and broadband jammers can hamper the ability of one or more eavesdroppers that are able to overhear in multiple frequencies at the same time. Doing this provides us with a greater insight into the impact that these defensive jammer agents can have in the secure throughput (i.e. probability of secure communication) of this system, according to different parameters, such as the number of receive/transmit channels, number of jammers and eavesdroppers, and number of hopping frequencies.

This section is divided in three other subsections: the first one describes the system notation and variables; the second one provides results for the secure throughput in a setup without jamming; while the last one adjoins this other defensive mechanism.

3.1 System Model

We consider a system comprised by one transmitter (Tx) and one receiver (Rx) deployed within reach of each other and capable of consistently communicating between themselves. Furthermore, it includes a set Π_e of E eavesdroppers, which, in the broadband setup, are able to listen to C_E different channels and J jammers, which analogously, are able to transmit in C_J different channels. Each node is capable of jumping through N possible frequencies following the Uncoordinated Frequency Hopping (UFH) scheme.

Let $\mathrm{x} \rightarrow \mathrm{y}$ denote the event of *successful reception* by device y of a message sent by x. Similarly, let $\mathrm{x} \not\rightarrow \mathrm{y}$ denote the event of *unsuccessful reception*, i.e. the complementary event of $\mathrm{x} \rightarrow \mathrm{y}$. Successful communication happens when Tx and Rx land on the same frequency channel.

3.1.1 *Assumptions*

We assume that all devices share the same physical characteristics (i.e. transmission power and rate), and jump synchronously between frequencies, using carrier sensing protocols to listen to packets being transmitted. Synchronization can be achieved in the same way as in frequency hopping by previously transmitting synchronization signals [55], or through other methods, which, for example, record temporal distances between transmissions allowing devices to coordinate their clocks [56]. All nodes belonging to this system are within reach of one another, meaning that all eavesdroppers can potentially listen to communication between *Tx* and *Rx*, while all jammers are capable of causing interference to those same eavesdroppers. We consider, for this preliminary model, that jammers coordinate with *Tx* and *Rx* to avoid harming legitimate communication, while causing interference to potential eavesdroppers. Although this is a strong assumption, it may be achieved through different mechanisms, such as steered/sectorized [57] transmission towards regions of potential eavesdroppers via directional antennas, or distributed beamforming schemes that have been recently incorporated into regular wireless networks [58], therefore allowing jammers' signals to add up coherently at an intended receiver, while causing interference to potential eavesdroppers.

However, this strong assumption is also something we aim to remove in our follow-up work, by employing spatial stochastic models of locations that will consider the harmful effect of jamming on legitimate communication.

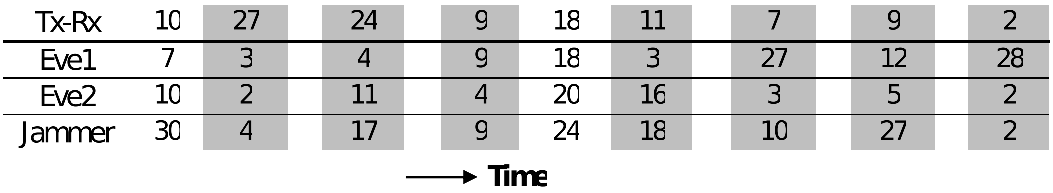
3.1.2 *Attacker Model*

For the attackers we consider a passive eavesdropper adversary, who lies silently within transmission range to overhear legitimate communication. The adversary eavesdroppers have the same characteristics as other agents and are able to detect and overhear communication in one or more frequencies, depending on their broadband capacity. The eavesdroppers also jump independently at random among the different frequencies searching for the legitimate communication channel. Eavesdroppers hop between frequencies at the same rate as the remaining devices. If eavesdroppers could hop between frequencies much faster than other devices, this would allow them to rapidly detect legitimate communication on a given frequency and remain on that frequency overhearing communication until *Tx* jumps to another frequency. However, the same kind of reasoning can be applied to jammers, in the sense that if jammers were able to hop between frequencies much faster this would allow them to affect eavesdroppers more frequently with corresponding security benefits. Whenever communication is possible (i.e. *Tx* and *Rx* are in the same frequency), we say that secure communication happens, *Figure* 23, if:

1. *Tx* and *Rx* are in the same frequency while no jammer or eavesdropper is present in that channel;

2. *Tx*, *Rx* and jammers are in the same frequency while there is no eavesdropper listening in that band;

3. *Tx*, *Rx* and jammers are in the same frequency, as well as eavesdroppers, with jammers avoiding interference on legitimate communication, while causing interference on eavesdroppers so as to limit their ability to overhear information.



Tx-Rx	10	27	24	9	18	11	7	9	2
Eve1	7	3	4	9	18	3	27	12	28
Eve2	10	2	11	4	20	16	3	5	2
Jammer	30	4	17	9	24	18	10	27	2

Figure 23.: *Example of secure communication under UFH. Numbers correspond to frequency channels, and only instances where communication occurs (Tx and Rx on the same channel) are depicted. Secure communication (shaded time-slots) happens when eavesdroppers (Eve) lie on a different frequency than Tx and Rx, or eavesdroppers lie on the frequency of Tx-Rx yet are obstructed by jammers on the same frequency. In all other cases communication is deemed insecure.*

3.2 UFH without Defensive Jamming

We consider a *secure throughput* security metric. The secure throughput measures the transmission rate at which *Tx* can communicate with *Rx* without eavesdroppers being able to acquire any information, as described in the previous three situations.

Definition 1 (Secure Throughput). *The secure throughput $\mathcal{T}_s$ from Tx to Rx is the probability that a message transmitted by Tx is* successfully *received by Rx, and* unsuccessfully *received by every eavesdropper in any frequency,*

$$\mathcal{T}_s \triangleq \mathbb{P}\left\{ Tx \rightarrow Rx \;\wedge \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i \right\}.$$

The secure throughput quantifies the probability of secure communication between *Tx* and *Rx*, depending on parameters such as the number of frequency channels, and the number of eavesdroppers and jammers in the system.

Proposition 1. The secure throughput for a setup with one *Tx-Rx* pair hopping uniformly at random through N frequencies, and E broadband eavesdroppers capable of simultaneously overhearing from C_E of those N frequencies is given by

$$\mathcal{T}_s^{broad} = \frac{N\binom{N-1}{C_E}^E}{N^2\binom{N}{C_E}^E}, \quad C_E < N, \tag{29}$$

where

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}, \quad n \geq r \wedge r > 0$$

represents the combination of r non-repeated elements selected from a group of n members, such that the order of selection does not matter.

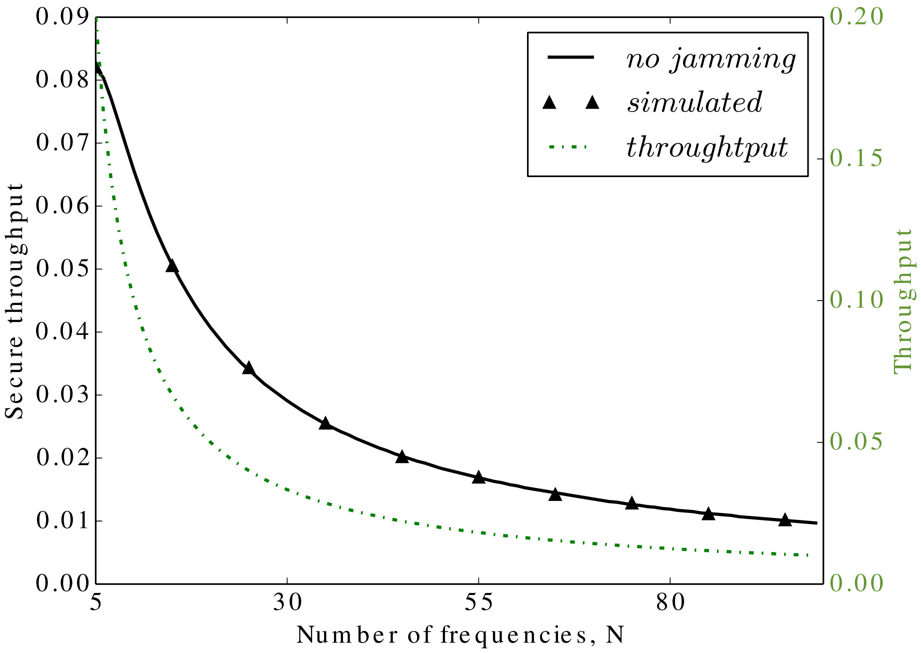


Figure 24.: *Secure throughput in the presence of $E = 4$ eavesdroppers for varying number of frequencies, N. The analytical secure throughput is based on (30) and the simulated secure throughput is also presented for comparison. The second y-axis and consequent curve represent the throughput associated with the Uncoordinated Frequency Hopping scheme.*

Proof. This formula, (29), results from the ratio of favorable cases over possible cases, where N represents the number of matching frequency channels between Tx and Rx, and $\binom{N-1}{C_E}^E$ the combination of the C_E frequencies being listened to by the eavesdroppers so that none of them is capable of overhearing legitimate communication.

As for $N^2\binom{N}{C_E}^E$, it encompasses all the possible permutations between all the devices currently selected for this setup (E eavesdroppers, plus Tx and Rx).

□

We can easily derive the secure throughput for a narrowband setup by considering $C_E = 0$.

$$\mathcal{T}_s^{narrow} = \frac{N(N-1)^E}{N^{2+E}}, \tag{30}$$

3.2.1 *Analysis - Narrowband Setup*

Figures 24 and 25 depict the behavior of the secure throughput with varying number of frequency channels N, for $E = 4$ and $E = 15$ eavesdroppers, respectively. Notice that the secure throughput assumes very low values, and those values decrease further with growing number of eavesdropper adversaries and number of frequencies. This happens because not only the underlying throughput is small, but also because the secure throughput is a demanding security metric, in the sense that one single eavesdropper being able to overhear communication deems that transmission insecure, even if other eavesdroppers are not able to do so.

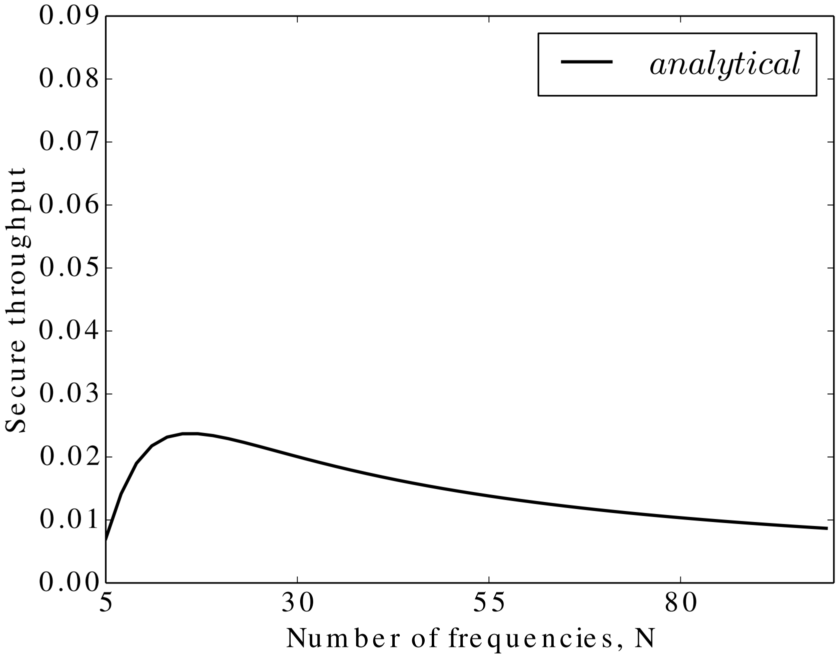


Figure 25.: *Secure throughput in the presence of $E = 15$ eavesdroppers for varying number of frequencies, N.*

Increasing the number of frequencies diminishes the probability of legitimate communication, with corresponding impact on the secure throughput. However, the behavior in *Figure 25* suggests that for larger numbers of eavesdroppers one can adapt the number of frequencies to maximize the secure throughput as follows.

Proposition 2. The maximum secure throughput as function of the number of eavesdroppers E is given by

$$\max_{N \in \mathbb{N}} \mathcal{T}_{\mathrm{s}}^{narrow} = E + 1$$

Proof. For fixed but arbitrary E, let

$$f(n) = \frac{n \times (n-1)^E}{n^{E+2}}, n \in [1, +\infty]$$

be the continuous function equivalent to $\mathcal{T}_{\mathrm{s}}^{narrow}$ in (30).

Let $f^{'}(n)$ and $f^{''}(n)$ respectively represent the first and second order derivative of $f(n)$. Since the first derivative of $f(n)$ is

$$f^{'}(n) = \frac{(E - n + 1) \times (n-1)^{E-1}}{n^{E+2}},$$

we get the following critical points where $f'(n) = 0$: $n = 1$ and $n = E + 1$, where $n = 1$ is discarded for being irrelevant from a practical standpoint.

By verifying the slope of the double derivative of $f(n)$,

$$f''(n) = (E^2 + E \times (3 - 4n) + 2 \times (n-1)^2) \times (n-1)^{E-2} \times n^{-E-3}$$

we observe that for $E \in \mathbb{R}^+$, $f''(E+1) < 0$, following that $E + 1$ is a local maximum.

Since the endpoint of $f(n)$ on the domain of n is $\lim_{n \to +\infty} \frac{(n-1)^E}{n^{E+1}} = 0$, the result follows. $\square$

3.2.2 *Analysis - Broadband Setup*

To carefully analyze the system's throughput and study the impact of broadband eavesdropping for Uncoordinated Frequency Hopping we started by elaborating a set of different situations using a varying number of adversary eavesdroppers and their capabilities. Both *Figure 26* and *Figure 27* depict a rather low secure throughput. This results from the negative effect of eavesdroppers on security, but also from the low throughput (i.e. probability that *Tx* and *Rx* land on the same frequency) between *Tx* and *Rx*, as depicted in *Figure 26*.

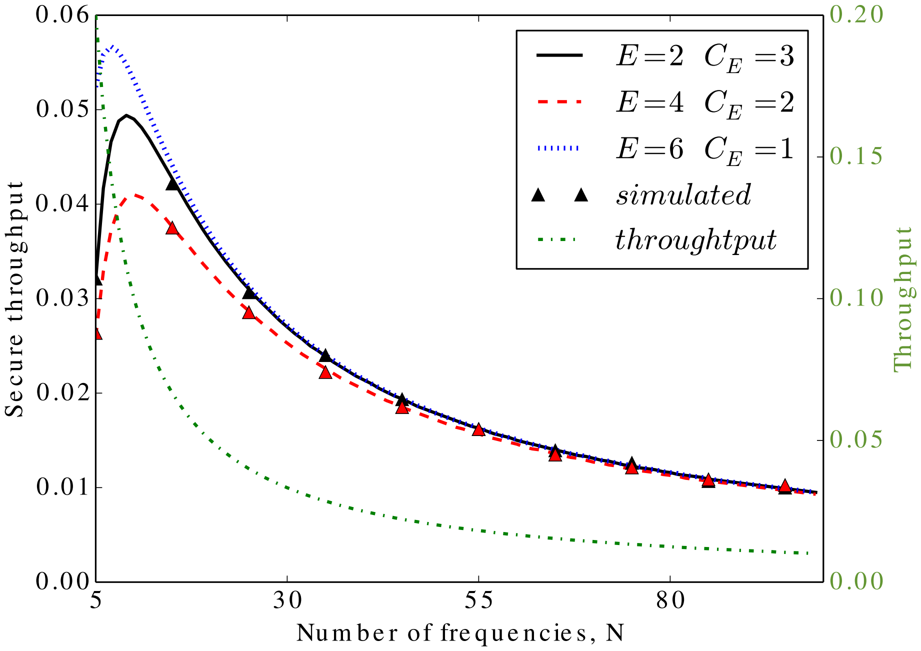


Figure 26.: *Secure throughput in the presence of $E = 2$, $E = 4$ and $E = 6$ eavesdroppers capable of, respectively, listening to $C_E = 3$, $C_E = 2$ and $C_E = 1$ frequencies at the same time for different number of possible frequency channels, N. Simulation results are also provided and validate the analytic results. The second y-axis and consequent curve represent the throughput associated with the Uncoordinated Frequency Hopping scheme.*

Figure 26 shows that there are two main factors limiting the secure throughput:

1. the increase in the number of frequencies N which, incidentally, reduces the throughput (probability of communication) between Tx and Rx;
2. the increase in the broadband capability (C_E) of eavesdroppers.

In particular, with respect to the second factor we can observe that the ability to overhear in more than one channel ($C_E = 3$ and 2) even for a lower number of eavesdroppers ($E = 2$ and 4), leads to a lower secure throughput when compared to the narrowband setup with more eavesdroppers ($E = 6$). This phenomenon is mostly due to the fact that, instead of having several eavesdroppers jumping independently through the N frequencies and possibly repeating some frequencies among them, these broadband devices are capable of eavesdropping while individually avoiding repetition among the C_E frequencies they listen to, therefore encompassing a larger number of independent frequencies under eavesdropping.

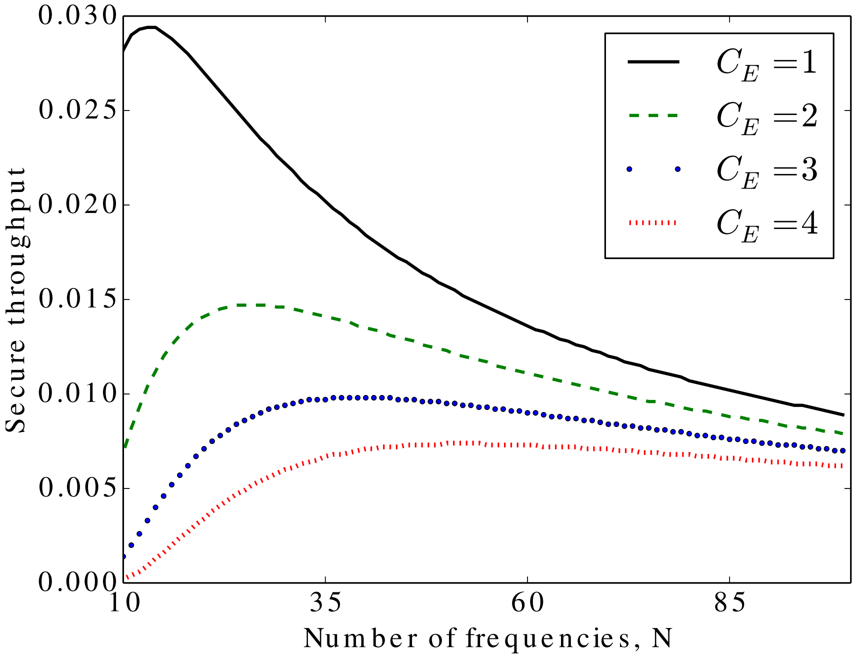


Figure 27.: *Secure throughput in the presence of* $E = 12$ *eavesdroppers listening between 1 and 4 different channels at the same time for a varying number of frequency channels, N.*

Figure 27 depicts the extreme low values of secure throughput obtained, resulting from a larger number of eavesdroppers (E =12). Again the secure throughput decreases with the number of frequencies N. More importantly, this graph illustrates the negative effect of increased broadband capabilities of eavesdroppers (C_E) on security. It is also important to mention that these very small values are also the result of the secure throughput being a very demanding metric, in the sense that it takes a single eavesdropper on a unique frequency to tamper the communication and deem the transmission of data insecure; even if other eavesdroppers are unable to overhear communication.

As suggested by *Figure 26* and *Figure 27* and already determined for the narrowband setup, it is possible to adapt the number of frequencies in order to maximize the secure throughput. In particular, for *Figure 27* the right shift in the maximum is quite noticeable when comparing broadband with narrowband ($C_E = 1$) eavesdropping. As the number of eavesdropped frequencies increases (due to the broadband characteristics of the devices) so does the amount of necessary hopping frequencies to obtain the maximum secure throughput.

Proposition 3. The maximum secure throughput as function of the number of eavesdroppers E and the number of channels C_E is given by

$$\max_{N \in \mathbb{N}} \mathcal{T}_s^{broad} = C_E(E+1)$$

Proof. For fixed but arbitrary E and C_E, let

$$f(n) = \frac{n\binom{n-1}{C_E}^E}{n^2\binom{n}{C_E}^E}, \quad C_E < n \wedge n \in [1, +\infty]$$

be the continuous function equivalent to $\mathcal{T}_s^{broad}$ in (29).

Let $f^{'}(n)$ and $f^{''}(n)$ respectively represent the first and second order derivative of $f(n)$. Since the first derivative of $f(n)$ is

$$f^{'}(n) = \frac{d}{dn}\left(\frac{n\left(\dfrac{(n-1)!}{C_E!(n-1-C_E)!}\right)^E}{n^2\left(\dfrac{n!}{C_E!(n-C_E)!}\right)^E}\right),$$

$$f^{'}(n) = \frac{d}{dn}\left(\frac{1}{n}\left(\frac{n-C_E}{n}\right)^E\right),$$

$$f^{'}(n) = -\frac{\left(\dfrac{n-C_E}{n}\right)^E(n - EC_E - C_E)}{n^2(n-C_E)}$$

we get the following critical points where $f'(n) = 0$: $n = C_E$ and $n = C_E(E+1)$, where $n = C_E(E+1)$ is discarded for being irrelevant from a practical standpoint.

By verifying the slope of the double derivative of $f(n)$,

$$f^{''}(n) = n^{-E-3}(n-C_E)^{E-2}(2n^2 - 4nEC_E - 4nC_E + C_E^2E^2 + 3C_E^2E + 2C_E^2)$$

we observe that for $E, C_E \in \mathbb{R}^+$, $f^{''}(C_E(E+1)) < 0$, following that $C_E(E+1)$ is a local maximum.

Since the endpoint of $f(n)$ on the domain of n is $\lim\limits_{n \to +\infty} f(n) = 0$, the result follows. □

3.3 Narrowband Jamming

We now consider a scenario where a set of J jammers is available to aid the *Tx* and *Rx* in securing communication by causing interference to eavesdroppers. These jammers may be devices specifically placed in the system with the purpose of helping legitimate devices to communicate securely, or devices that are silent due to some channel access mechanism to avoid collisions.

Proposition 4. The secure throughput for a setup with one *Tx-Rx* pair, E eavesdroppers and J jammers hopping uniformly at random through N frequency channels is given by

$$\mathcal{T}_\mathrm{s} = \frac{N\times(N-1)^E\times N^J + N\times(N^E-(N-1)^E)\times(N^J-(N-1)^J)}{N^{J+E+2}} \tag{31}$$

Proof. This results from counting the number of favorable and the number of possible cases as follows. Recall that we consider a transmission secure if

1. the *Tx-Rx* pair land on a given frequency without any eavesdropper doing so, or
2. the *Tx-Rx* pair land on a given frequency with one or more eavesdroppers, and one or more jammers are available at that frequency to cause interference to eavesdroppers.

$N \times (N-1)^E \times N^J$ represents the number of cases in which *Tx* and *Rx* land on one of the N frequencies, while all E eavesdroppers land on any of the remaining $N-1$ frequencies and jammers land on any frequency N, therefore representing case 1) above.

$N \times (N^E - (N-1)^E) \times (N^J - (N-1)^J)$ represents the number of cases in which *Tx* and *Rx* land on one of the N frequencies, while at least one eavesdropper lands on that frequency, i.e. $N^E - (N-1)^E$ (the complementary of $(N-1)^E$).

Similarly, $N^J - (N-1)^J$ corresponds to at least one jammer landing on that same frequency as *Tx*, *Rx* and eavesdropper(s).

Finally, N^{J+E+2} represents all possible cases for J jammers, E eavesdroppers, *Tx* and *Rx* hopping through N frequency channels. □

3.3.1 *Analysis*

Figure 28 depicts the secure throughput with varying number of frequency channels N, for $E = 4$ eavesdroppers and $J = 5$ jammers. Notice that the secure throughput compares favorably with similar results without jamming due to the positive effect of friendly jammers on secure communication. *Figure 29* shows the secure throughput for larger number of eavesdroppers $E = 15$ and different numbers of jammers. In this case, even with larger number of eavesdroppers, the secure throughput does not suffer much when compared to *Figure 28* because of the positive effect of jammers on security. Moreover, the secure throughput in *Figure 29* compares favorably with the same setup but without jammers, specially for lower values of of number of frequencies, where the secure throughput is not dominated by the low probability of legitimate communication.

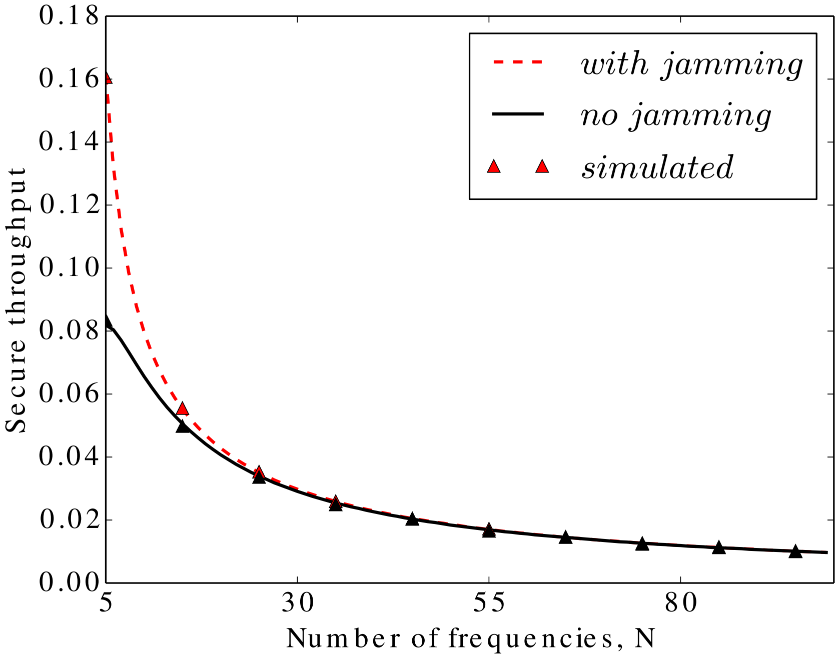


Figure 28.: *Secure throughput in the presence of $E = 4$ eavesdroppers and $J = 5$ jammers for varying number of frequencies, N. The analytical secure throughput is based on Proposition 4, and the simulated secure throughput is presented for comparison. These results are compared with a no jamming version of this setup.*

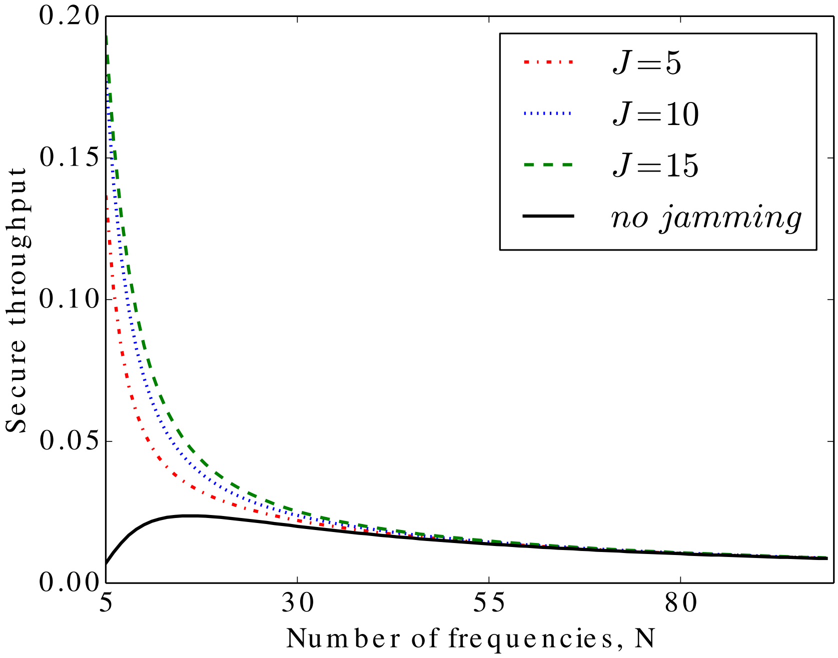


Figure 29.: *Secure throughput in the presence of $E = 15$ eavesdroppers for $J = 5$, $J = 10$, $J = 15$ jammers and No Jamming, for varying number of frequencies, N.*

3.4 Broadband Jamming

In this section we include an analysis of a scenario where we have added a number of J broadband jammers capable of transmitting on C_J frequency channels. The purpose of these defensive agents is to combat eavesdroppers by causing interference on the frequencies where they overhear communication.

Proposition 5. The secure throughput for a setup with one *Tx-Rx* pair, E broadband eavesdroppers listening in C_E frequencies and J broadband jammers transmitting in C_J frequencies, all of them hopping uniformly at random through N frequency channels is given by

$$\mathcal{T}_{\mathrm{s}} = \frac{N\left(\binom{N-1}{C_E}^E\binom{N-1}{C_J}^J+\binom{N-1}{C_E}^E\neg\binom{N-1}{C_J}^J+\neg\binom{E-1}{C_E}^E\neg\binom{N-1}{C_J}^J\right)}{N^2\binom{N}{C_E}^E\binom{N}{C_J}^J},\ C_E < N \wedge C_J < N,$$

where

$$\neg\binom{x-1}{y}^z = \binom{x}{y}^z - \binom{x-1}{y}^z$$

Proof. This formula is divided in three parts, each of which corresponds to one of the three situations described in Section 3.1.2. Again, N corresponds to the number of matching frequencies between the *Tx-Rx* pair, while:

$\binom{N-1}{C_E}^E\binom{N-1}{C_J}^J$ corresponds to the situation where none of these devices (eavesdroppers and jammers) lie in the communication channel;

$\binom{N-1}{C_E}^E\neg\binom{N-1}{C_J}^J$ represents the number of cases in which all E eavesdroppers are not listening to the communication channel, and at least one jammer lands on the frequency being used by the *Tx-Rx* pair (i.e. the complementary of $\binom{N-1}{C_J}^J$);

$\neg\binom{N-1}{C_E}^E\neg\binom{N-1}{C_J}^J$ refers to the number of cases in which at least one eavesdropper and one jammer land on the frequency currently being used by the *Tx-Rx* pair;

Finally $N^2\binom{N}{C_E}^E\binom{N}{C_J}^J$ represents, once more, all the possible permutations of all the devices present in the system (the *Tx-Rx* pair, J broadband jammers and E broadband eavesdroppers) hopping through N frequencies.

□

3.4.1 *Analysis*

By introducing jammers, we can assess the impact of these defensive agents on the secure throughput of the system. For *Figure 30* we have added one broadband jammer, so that we could highlight the secure throughput improvement of using these warding devices against harmful broadband eavesdroppers. As expected, the difference between both situations (jamming and no jamming) is quite significant for a lower number of frequencies N and fades away with increasing N due to the reduction in the throughput, as observed in *Figure 26*. It is noticeable the advantage of broadband jamming to secure these systems, especially for lower values of number of frequencies.

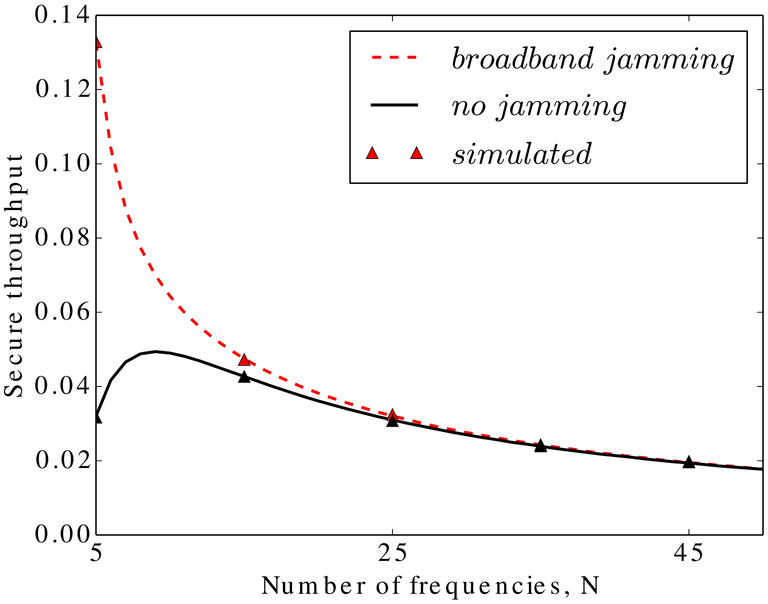


Figure 30.: *Secure throughput in the presence of $E = 2$ broadband eavesdroppers listening to $C_E = 3$ frequencies and $J = 1$ broadband jammer transmitting on $C_J = 3$ different channels at the same time for a varying number of frequency channels, N. These results are compared with a no jamming version of this setup.*

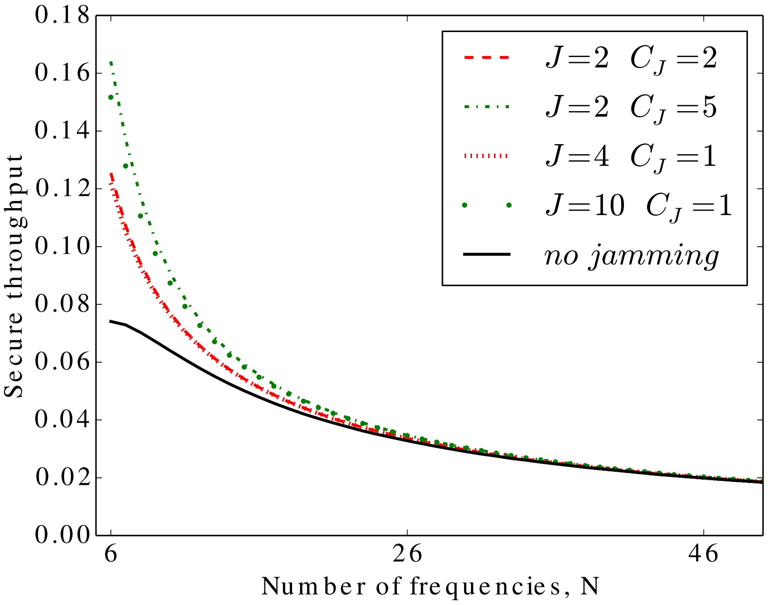


Figure 31.: *Secure throughput in the presence of $E = 2$ broadband eavesdroppers listening to $C_E = 2$ different channels at the same time, $J = 4$ and $J = 10$ narrowband eavesdroppers as well as $J = 2$ broadband jammers securing $C_J = 2$, $C_J = 5$ different frequencies, for a varying number of frequency channels, N. These results are compared with a no jamming version of this setup.*

In *Figure 31* we consider several jammer configurations to compare broadband jamming against narrowband jamming. We can again see that having jammers allows for a relevant gains in terms of secure throughput. We can also identify a slight increase in the secure throughput when using broadband jamming when compared with the equivalent narrowband version. For example, $J = 10$ jammers operating in $C_J = 1$ frequency leads to a somewhat lower secure throughput than $J = 2$ jammers operating in $C_J = 5$ frequencies, although the overall number of affected frequencies amounts to the same (10) in both cases. The same is noticeable for the cases $J = 4$, $C_J = 1$ and $J = 2$, $C_J = 2$. This happens because of the inherent characteristic of broadband jammers, as they do not repeat frequencies they operate on, allowing for a wider range of non-repeated frequencies to be covered. This suggests that it is more advantageous to have fewer broadband jammers operating in a larger number of frequencies other than several narrowband jammers. This also reduces the burden of cooperation/synchronization that would be needed among narrowband jammers if, for example, we wanted to avoid jammers lying in the same frequency.

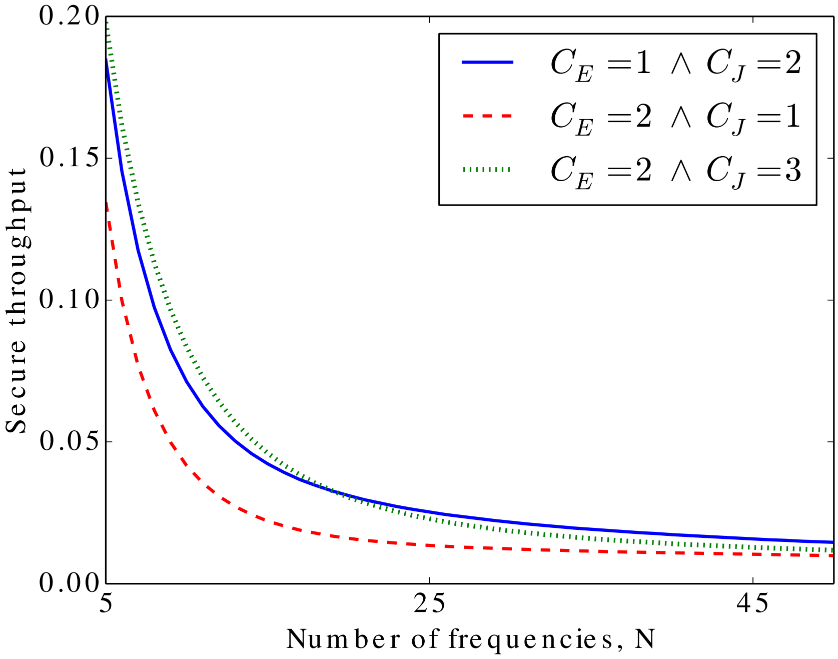


Figure 32.: *Secure throughput in the presence of $E = 20$ eavesdroppers and $J = 5$ jammers for different setups (mix of broadband and narrowband devices), for a varying number of frequency channels, N.*

Finally, *Figure 32* depicts the positive impact of jammers on the system in the presence of a larger number of eavesdroppers ($E = 20$). Even when presented with broadband adversaries, the negative effect of multiple eavesdroppers can be addressed by jammers by increasing the number of frequencies they operate on. In particular, note that 5 jammers alone operating in 3 frequencies each (dotted green line) are sufficient to ensure reasonable levels of secure throughput against 20 eavesdroppers.

4

MATHEMATICAL FRAMEWORK FOR WIRELESS SECRECY IN UFH

Our previous model provided preliminary results for the secrecy level of UFH coupled with friendly jamming, showing that the combination of these two schemes leads to improved secure throughput of wireless networks. Nonetheless, this mathematical framework included several strong assumptions, notably, the cancellation of interference caused by the jammers on legitimate receivers, and the nonexistence of propagation effects through an abstraction of node's locations by assuming that they are all within reach. These characteristics enabled a preliminary interpretation and evaluation of our security scheme but made this framework somewhat inaccurate. In fact, the specific location of the nodes has a strong impact on reception quality, and the number of eavesdroppers is most of the times unknown. Furthermore, interference cancellation is very difficult to achieve especially when originated from outer sources.

Therefore, we decided to include three major changes to our mathematical model that allow for a more precise analysis of this security scheme. First, we added stochastic geometry to account for the randomness of both eavesdroppers' and jammers' locations, as well as, their arbitrary number. Hence, we no longer have a specific set of devices, but rather a density of nodes in a particular region which are randomly positioned in space. We have also included interference models and propagation effects. For that, we resort to a unified framework that makes use of two relevant concepts: the SINR model [21], which encompasses some concepts from another model - audible nodes [18] - greatly extending its complexity.

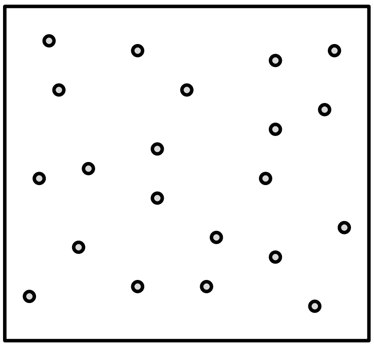


Figure 33.: *In the normal Poisson point process (PPP), commonly employed in stochastic geometry, the nodes are haphazardly distributed over a given surface, with no obvious regularity (statistically independent) [3].*

This *audible* model introduces the concept of *audible nodes*, briefly explained in section 2.3.4, where each device is given a particular bounded region, in which it can act, determined by its power and other propagation characteristics (e.g path loss). Naturally, this mathematical framework is much more complex and thorough than the one presented in the previous section. However, it is difficult to account for the degradation factor caused by nearby jammers on devices because any node inside an audible region is assumed to have the same impact, irrespectively of their specific location.

This other model - *SINR* - offers a more complete mathematical characterization that takes into account all the essential physical parameters that affect the aggregate interference. Therefore, this framework allows us to assess the impact of interference, given a particular node PPP disposition, and quantify its effect on all channels, whether legitimate or not, using the *signal-to-interference-plus-noise ratio* as a way of measuring it, as we will now detail.

The following chapter is divided into a single category that encompasses information on how does this scheme work, what changes have been made, its mathematical 'fingerprint' and an analysis of the results.

4.1 SINR Model

The SINR is a model for mathematically representing interference, whether originated from other devices (e.g. jammers) or from propagation effects (e.g. path loss), based on the following signal quality formula $SINR = \frac{S}{I+Nx}$, where I is the aggregate interference power, S is the power of the signal sent by the transmitter and Nx is the constant noise power. In this case, the impact from jammers anywhere in space is considered from the term I, which allows the accommodation of a very important feature to realistically portray a wireless network. This model can be used to determine the throughput, $\mathcal{T}$, of a network as follows [21]: $\mathcal{T} = \mathbb{P}\{SINR \geq \theta\}$.

The SINR model follows a different approach and adds unlimited jamming, not bounded to specific regions of space, which allows for a broader and complete analysis of our scheme. Therefore, interference is not only confined to nearby nodes, but instead, each one of the jammers present in space is due to affect the communication channels, one way or another. This framework measures the interference caused by each transmitting device and offers a way of quantifying it (e.g. nodes farther away will have less influence than the ones closer to the receiver).

Therefore, this framework successfully captures the **three essential physical parameters** that affect interference, allowing us to build a robust mathematical scheme for UFH+jamming.

- distribution of the interferers in space;
- transmission characteristics of the interferers (e.g. power);
- propagation characteristics of the medium (e.g. path loss).

The inlaid structure of this model was proposed by Moe Z. Win et al. [21], but multiple changes had to be made to fit our security scheme. Hence, our altered version of this framework takes into consideration the UFH communication paradigm, as well as, the coexistence of both receiver and eavesdroppers in the same network, that is, not only the throughput to the legitimate receiver, but also to all eavesdroppers..

Throughout this chapter we unveil some of this model's features, we obtain expressions for the secure throughput having in mind our forever present system model, and we analyze the effect of having a different number of frequency channels or different propagation characteristics. We consider that a packet is successfully received if the *signal-to-interference-plus-noise ratio* (SINR) exceeds a certain threshold. The notation and symbols used throughout this chapter are summarized in *Table* 6.

This sub-chapter is organized in the following way: the first section provides a representation and probabilistic characterization of the distribution of the interferers and eavesdroppers using a PPP to spatially model their location, as well as, a brief introduction to the system model; the second and third sections derive the distribution of the aggregate interference and define our secrecy metric - *secure throughput*; the last section analyzes the secure throughput of our scheme and reveals the innate connection of the secrecy to various important system parameters such as the number of available frequency channels, the transmitted power, path loss and the spatial density of the interferers.

Symbol	Usage
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
$F\{\cdot\}$	CDF operator
$\Gamma\{\cdot\}$	Gamma function operator
$b, 2b$	Amplitude/Power loss exponent
θ^*	SINR threshold
$\Pi_e = \{e_i\}, \Pi_j = \{j_i\}$	Poisson processes of eavesdroppers and jammers
λ_e, λ_j	Spatial densities of eavesdroppers and jammers
P_0, P_I	Transmit power of transmitter and jammers
r_0, r_e	Pair-wise distances between $Tx - Rx$ and $Tx - e_i$, respectively
$r_{tx,e}$	Radius of the circle around the transmitter
N_e	Expected number of jammers
N	Available number of frequencies
Nx	Constant noise power
$\mathcal{B}_x(\rho)$	Ball centered at x with radius ρ
$\mathcal{T}_s$	Secure throughput
$\mathcal{T}_{rx}, \mathcal{T}_e$	Throughput at Bob and Eve, respectively
$\mathcal{T}'_e$	Reverse throughput at Eve ($\mathcal{T}'_e = 1 - \mathcal{T}_e$)
μ_e	Average # of eavesdroppers inside a circle region centered on Tx

Table 6.: *Notation and Symbols.*

4.1.1 *Node Configuration*

The spatial location of the nodes is a mandatory feature in order to determine the exact impact of the interference, whether due to propagation effects or other transmitted signals. Just like in any stochastic model, the location and number of some of the nodes is deemed to be unknown. This particular setting closely resembles what actually happens in ad-hoc networks where only a statistical description of the location of the devices is available. Therefore, we consider that only the transmitter and receiver know their exact locations, whereas the attackers and defenders are placed in space according to a homogeneous Poisson point process.

Without a constrained structure on the nodes disposition a stochastic model is, thus, the best one available. Hence, we treat all these nodes' positions has completely random and the homogeneous PPP does just that, since it has maximum entropy among all homogeneous point processes [21].

We consider the following scenario depicted in *Figure* 34, where a legitimate user - transmitter (*Tx*) - deterministically placed anywhere on the two-dimensional plane, tries to communicate with another user - receiver (*Rx*) - located at the origin. We kept these positions as defined by Moe Z. Win et al. to allow for an easier accommodation of our own variables (without loss of generality). The system is also besieged by an arbitrary number of eavesdroppers, $\Pi_e = e_i \subset \mathbb{R}^2$, spatially distributed according to a homogeneous PPP on $\mathbb{R}^2$ with density λ_e. With the aim of improving secrecy, multiple jammers, $\Pi_j = j_i \subset \mathbb{R}^2$, transmit in cooperation with *Tx* and *Rx*, and are distributed following a similar random process with spatial density λ_j.

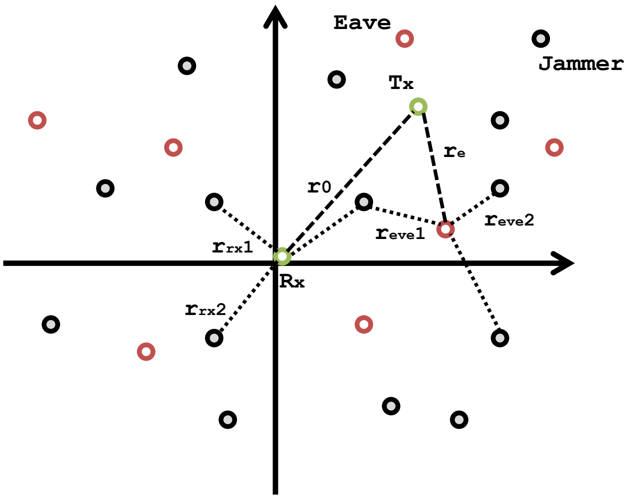


Figure 34.: *Transmitter and receiver try to communicate in the presence of both attackers (red nodes) and defenders (grey nodes), which are randomly distributed according to homogeneous Poisson point processes with different spatial densities. r_{rx} and r_{eve}, respectively, denote the distances from the receiver and each of the eavesdroppers to all different jammers.*

The transmitter and receiver employ UFH as their multiple-access technique, attempting to evade eavesdroppers' attacks by randomly jumping among frequencies. The remaining terminals jump as well, as they try to protect or overhear the communication. Nonetheless, for this framework to work nodes have to be loosely synchronized and with identical characteristics (e.g. same jumping rate) as to avoid any advantageous situation for any of the sides, and to ease out the task of mathematically characterizing our security scheme.

For analytical purposes, we assume that the transmitter is distanced r_0 from the receiver. Furthermore, the random distances from Rx to all the jammers are denoted by $\{r_{rx}\}_{rx=1}^{\infty}$, while the distances between a eavesdropper and all the interferers are represented by $\{r_{eve}\}_{eve=1}^{\infty}$.

4.1.2 *Wireless Propagation and Interference*

In order to analyze and mathematically characterize wireless propagation and interference, one needs to define and consider the *"power relationship between the transmitter and receiver"* [21] and account for the effect of other transmitted signals (noise), as well as, other 'environmental' effects (e.g path loss) on the communication channel.

Therefore, we use a model similar to [21], which considers that the power P_x received at distance R from the transmitter is given by

$$P_x = \frac{P_{tx} \prod_k Z_k}{r^{2b}} \tag{32}$$

where P_{tx} is the transmission power, b is the amplitude loss exponent, r is the distance between source and destination and Z_k is a random variable (r.v.) that represents the different propagation effects that influence communication, in particular, shadowing and multipath fading. Another important propagation characteristic, far-field path loss, is already modelled by means of the term $\frac{1}{r^{2b}}$. This accounts for the loss of signal-power as it travels through the medium and is closely related with the distance between source and destination, as well as, the other environmental dependent aspects hereby represented by the amplitude loss exponent b. This variable usually ranges from 0.8 (e.g. hallways) to 4 (e.g. urban environments) with 1 corresponding to free-space propagation [28].

Although this initial framework only accounted for one single receiver (located at the origin), the same kind of reasoning can be applied to all the eavesdroppers in the network as extra receivers. We decided that path loss was enough to have a general and accurate idea of the impact of propagation effects ($\prod_k Z_k = 1$), although many other propagation scenarios could also be considered [30] such as: *nakagami-m fading* or *log-normal shadowing*.

In order to relate this equation to the general model for interference, we start be defining another important concept: SINR.

Definition 2 (SINR)**.** *The SINR or signal-to-interference-plus-noise ratio quantifies the theoretical channel capacity (usually a upper-bound) and is commonly employed as a way to measure the quality of wireless connections. The SINR associated with a node positioned anywhere in space is defined as,*

$$SINR = \frac{S}{I + Nx} \tag{33}$$

where S is the power of the signal received from the transmitter, I is the aggregate interference power and Nx is the constant noise power. S and I are slow varying, or in other words, remain approximately the same over time and, as such, only depend on a given realization of the distances between nodes and the propagation effects, which can both be represented by random variables.

Using the power definition (32), S can be generally written as

$$S = \frac{P_0}{r^{2b}} \tag{34}$$

where P_0 is the transmitter power and r is the distance between source and destination. For Rx, r has a specific value (r_0 - see *Figure* 34), since the receiver is deterministically located. On the contrary, for the each eavesdropper, r is a random value (r_e) because of the stochastic distribution and location of these devices.

Similarly, I can be written as

$$I = \sum_{i=1}^{\infty} \frac{P_I}{r_i^{2b}} \tag{35}$$

where P_I is the interference power of each interferer/jammer and r_i accounts for the distance between interferer and receiver. Since jammers' positions are random (spatially distributed by a PPP), r_i is a r.v. and, consequently, so is I. This is valid for both receiver and eavesdroppers. For this to work, we have to assume each interferer has the same transmit power P_I. This suits our system model requirements, which regards all devices as having the same characteristics.

The simplicity of the SINR concept enables an extension such that what is thought for a legitimate receiver can also be applied to the eavesdroppers, however with the added difficulty that we may have multiple eavesdroppers in the system.

However, there is another important issue to bear in mind, which is the need for an aggregate **representation** that joins the propagation effects and the active interference from other transmitting devices - *a distribution for the I variable.* Although this representation is entirely proposed by Moe Z. Win et al., we shall briefly describe how it is obtained.

Let us begin by considering the simplest expression for representing the aggregate interference.

$$Y = \sum_{i=1}^{\infty} \frac{q_i}{r_i^{\eta}} \mathbb{1}_{\mathcal{A}}(Q_i, r_i) \tag{36}$$

where

$$\mathbb{1}_{\mathcal{A}}(q_i, r_i) = \begin{cases} 1, & (q, r) \in \mathcal{A} \\ 0, & \text{otherwise} \end{cases} \tag{37}$$

q_i accounts for the propagation characteristics in the same way as Z_k and is tightly connected to phenomenons like shadowing and multi-path fading, while r_i relates, once again, to the distances between receiver and interferers. η accommodates any environmental constraints (e.g. amplitude loss exponent - b) and the indicator function, $\mathbb{1}_{\mathcal{A}}(q_i, r_i)$, allows for the selection of the nodes which will interfere with the communication - *active interferers*. The selection can be based on multiple conditions but, in order to maximize the accuracy of this model, we consider all jammers in $\mathbb{R}^2$ to be active - $\mathcal{A} = \{(q, r) : r \in \mathbb{R}^2\}$.

From Theorem 3.1 in [21] we know that the characteristic function of Y can be expressed as

$$\phi_Y(w) = \exp(-2\pi\lambda_j \int_{\mathbb{R}^2} \Big[1 - \phi_q\Big(\frac{w}{r^{\eta}}\Big)\Big] r \, \mathrm{d}r) \tag{38}$$

where λ_j represents the spatial density of interferers for the two-dimensional PPP, and ϕ_q is the characteristic function of r.v. q. This equation can in turn be adapted to the r.v. I, for $b > 1$, as proven in the same article.

$$\phi_I(w) = \exp(-\gamma|w|^{\alpha} \Big[1 - j\beta sign(w) \tan\Big(\frac{\pi\alpha}{2}\Big)\Big]) \tag{39}$$

where

$$\begin{aligned} \alpha &= \frac{1}{b}, \\ \beta &= 1, \\ \gamma &= \frac{\pi\lambda_j \Gamma(2-\alpha)\cos\Big(\frac{\pi\alpha}{2}\Big) P_I^{\frac{1}{b}}}{1-\alpha} \end{aligned}$$

with Γ denoting the gamma function. ϕ_I resembles the characteristic function of a stable distribution (for $b > 1$) [59, 60], ϕ_{stlb}, with characteristic exponent $\alpha \in [0, 2]$, skewness $\beta \in [-1, 1]$ and dispersion $\gamma \in [0, \infty[$

$$\phi_{stlb}(w) = \begin{cases} \exp(-\gamma|w|^{\alpha} \Big[1 - j\beta sign(w) \tan\Big(\frac{\pi\alpha}{2}\Big)\Big]), & \alpha \neq 1 \\ \exp(-\gamma|w| \Big[1 + j\frac{2}{\pi}\beta sign(w) ln\Big(|w|\Big)\Big]), & \alpha = 1 \end{cases} \tag{40}$$

and can thus be represented as a **random variable following a** *skewed stable distribution* - $\mathcal{S}$ - with parameters α, β, γ.

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\pi\lambda_j\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right)P_I^{\frac{1}{b}}}{1-\alpha}\right) \tag{41}$$

However, we have to account for the fact that, due to UFH, jammers do not continuously disrupt the legitimate communication or any other of the eavesdroppers' channels. Therefore, only a set of these may actually be interfering with devices at a given time. To add this condition to the proposed interference representation we refer the *colouring theorem/ splitting property* [3] of the Poisson process.

Definition 3 (Colouring Theorem). *[3] "Let Π be a Poisson process on R with mean measure (density) λ. Let the points of Π be coloured randomly with k colours, the probability that a point receives the ith colour being p_i, and the colours of different points being independent (of one another and of the position of the points). Let Π_i be the set of points with the ith colour. Then the Π_i are independent Poisson processes with mean measures."*

$$\lambda_i = p_i\lambda \tag{42}$$

Hence, using (42), r.v. I can finally be succinctly expressed as

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\pi\lambda_j p_i\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right)P_I^{\frac{1}{b}}}{1-\alpha}\right) \tag{43}$$

where p_i is the probability of a jammer landing on the communication frequency and is given by $\frac{1}{N}$ where N is the number of available frequencies (e.g. if there are 10 possible frequencies to jump to, $p_i = \frac{1}{10}$)

4.2 Secure Throughput based on the SINR model

We now use the results from the previous sections to come up with a definition of secure throughput. Theoretically, this secrecy metric is once again the same as in any of the other models. However, the successful transmission of packets is no longer related with *relative probabilities* or *audible regions* but, instead, with the *SINR outage probability* [30].

Therefore, in this setup, a transmitted packet from *Tx* is successfully received by *Rx* if both these devices are using the same frequency channel and there is no outage - the $SINR$ exceeds some threshold. Furthermore, all eavesdroppers must be incapable of listening to the legitimate communication, which happens whenever they are positioned in the wrong frequency or their channel's SINR is bellow some threshold. The secure throughput is then greatly affected by the density and power of the jammers and eavesdroppers, as well as by the number of available frequencies.

The secure throughput, $\mathcal{T}_s$, is, thus, mathematically interpreted as

$$\mathcal{T}_\mathrm{s} = \mathcal{T}_{rx} \times \bigwedge_{e_i \in \Pi_\mathrm{e}} \mathcal{T}_{e_i}{}' \tag{44}$$

where $\mathcal{T}_{rx}$ is the throughput probability of the link between transmitter and receiver, $\mathcal{T}_{e_i}{}'$ is the complementary of the throughput probability for a specific eavesdropper i.

Proposition 6. The **secure throughput** for a setup with one *Tx-Rx* pair deterministically located in $\mathbb{R}^2$ hopping uniformly at random through N frequencies and with a set of eavesdroppers, $\Pi_e = e_i \subset \mathbb{R}^2$, and jammers, $\Pi_j = j_i \subset \mathbb{R}^2$ spatially distributed according to a PPP with densities λ_e and λ_j respectively, is given by

$$\mathcal{T}_\mathrm{s} = \frac{1}{N} F_I\left(\frac{P_0}{r_0^{2b}\theta^*} - Nx\right) \times \exp\left(-\frac{2\pi\lambda_e}{N}\int_0^{r_{tx,e}} F_I\left(\frac{P_0}{r_e^{2b}\theta^*} - Nx\right) r_e \, \mathrm{d}r_e\right) \tag{45}$$

with

$$I \sim \mathcal{S}\left(\alpha = \frac{1}{b}, \beta = 1, \gamma = \frac{\frac{\pi\lambda_j}{N}\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right)P_I^{\frac{1}{b}}}{1-\alpha}\right) \tag{46}$$

where, F_I represents the cumulative distribution function (cdf) of the stable variable I, r_e is the distance between the transmitter and each eavesdropper and $r_{tx,e}$ is the radius of a sphere centered over the transmitter, where the eavesdroppers are going to be 'weighted'.

Proof. From the definition of secure throughput, and considering N_e has the number of eavesdroppers, $\#\Pi_e$, we can write

$$\begin{aligned}
\mathcal{T}_\mathrm{s} &= \mathbb{P}\left\{Tx \to Rx \wedge \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \\
&\overset{1}{=} \mathbb{P}\left\{Tx \to Rx \,\middle|\, \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \times \mathbb{P}\left\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \\
&\overset{2}{=} \mathbb{P}\left\{Tx \to Rx \,\middle|\, \bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\right\} \times \sum_{n=0}^{\infty} \mathbb{P}\left\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i \,\middle|\, N_e = n\right\} \cdot \mathbb{P}\{N_e = n\},
\end{aligned} \tag{47}$$

To continue, we take into consideration the following premises/approximations, which we will later evaluate through simulations.

[1] Conditional probability: $\mathbb{P}\{A \wedge B\} = \mathbb{P}\{A|B\} \times \mathbb{P}\{B\}$

[2] Law of total probability: $\mathbb{P}\{A\} = \mathbb{E}_X\{\mathbb{P}\{A|X\}\} = \sum_x \mathbb{P}\{A|x\} \times \mathbb{P}(x)$.

1. event $\{Tx \rightarrow Rx\}$ is independent of $\{\bigwedge_{e_i \in \Pi_e} Tx \nrightarrow e_i\}$;
2. events $\{Tx \nrightarrow e_i | N_e = n\}$ are independent identically distributed (IID) for different i;
3. eavesdroppers are randomly distributed using a PPP inside a circle with radius $r_{tx,e}$ around the transmitter;
4. each distance from an eavesdropper to the transmitter, r_e, is independent from another.

Regarding (1.), we consider that the communication between transmitter and receiver does not in any way affect the eavesdroppers' channels, the same happening (2.) between each of the attackers' communication link. (3.) and (4.) are stronger approximations since they limit the area around which the eavesdroppers are placed, with each location being independent from one another.

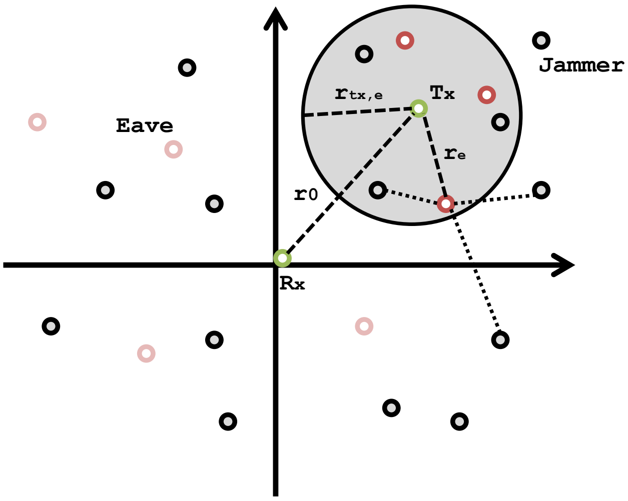


Figure 35.: *We make an approximation for the secure throughput by restricting eavesdroppers' influence around the grey circle. Due to their distance is almost impossible for any other eavesdroppers to overhear communication.*

With respect to point (3.), we restrict the spatial distribution of the **eavesdroppers** inside a specific region, a circle - $\mathcal{B}$ - around the transmitter - $\Pi_e \cap \mathcal{B}_{tx}(r_{tx,e})$ - *Figure* 35. In fact, if we consider a large enough area, we can have an almost perfect approximation for the secure throughput even if we have attackers placed outside this circle's borders. To do that, we adjust the radius of the circle to accommodate the assailants that can potentially overhear the communication. If we look at the throughput probability $\mathbb{P}\{SINR \geq \theta^*\}$ [21], which translates into $F_I(x)$[3], we can determine an upper-bound for the radius when $x = 0 \Rightarrow r_{tx,e} = \left(\frac{P_0}{Nx\theta^*}\right)^{\frac{1}{2b}}$.

[3] $\mathrm{F}_I(x) = CDF_I(x) = \begin{cases} 0 & x < 0 \\ y & 0 \leq x < 1 \\ 1 & x \geq 1 \end{cases}$, where y depends on the distribution of random variable I

Jammers are, otherwise, left exactly as planned, and are distributed in $\mathbb{R}^2$. Doing this allows for an accurate measure of the interference (a sum of all jammers's noise).

(47) then becomes

$$\mathcal{T}_s \approx \mathbb{P}\left\{Tx \rightarrow Rx\right\} \times \sum_{n=0}^{\infty} (1-\omega)^n \cdot \mathbb{P}\{N_e = n\} \tag{48}$$

where $\omega = \mathbb{P}\{Tx \rightarrow e_i | N_e = n\}$. To determine $\mathbb{P}\left\{Tx \rightarrow Rx\right\}$ we resort to the *SINR* concept and interference representation (43). Thus, we have

$$\begin{aligned} \mathbb{P}\{Tx \rightarrow Rx\} &= \mathbb{P}\left\{SINR_{rx} \geq \theta^*\right\} \\ &= \mathbb{P}\left\{\frac{S}{I+Nx} \geq \theta^*\right\} \\ &= \mathbb{P}\left\{\frac{P_0}{r_0^{2b}} \geq \theta^*(I+Nx)\right\} \\ &= \mathbb{P}\left\{\frac{P_0}{r_0^{2b}\theta^*} - Nx \geq I\right\} \\ &\overset{4}{=} F_I\left(\frac{P_0}{r_0^{2b}\theta^*} - Nx\right). \end{aligned} \tag{49}$$

We now determine the summation in (48), knowing that the number of eavesdroppers, N_e, in the circle region is a Poisson random variable with mean $\mu_e = \lambda_e \pi r_{tx,e}^2$ [17, 18].

$$\begin{aligned} \sum_{n=0}^{\infty} (1-\omega)^n \cdot \mathbb{P}\{N_e = n\} &\overset{5}{=} \sum_{n=0}^{\infty} (1-\omega)^n \cdot \frac{\mu_e^n e^{-\mu_e}}{n!} \\ &= e^{-\mu_e} e^{\mu_e(1-\omega)} \underbrace{\sum_{n=0}^{\infty} \frac{(\mu_e(1-\omega))^n e^{-\mu_e(1-\omega)}}{n!}}_{=1} \\ &= \exp\left(-\mu_e \cdot \omega\right). \end{aligned} \tag{50}$$

Finally, we conclude our proof by working out ω - *probability that an eavesdropper is not in outage*. Note that we have to take into account the possible position of each eavesdropper and correspondent distance to the transmitter. We know this distance, r_e, is a r.v. and, thus, we need to calculate its expected value, $\mathbb{E}$, (long-run average value).

[4] Cumulative Distribution Function (cdf): $F_X\{A\} = \mathbb{P}\{X \leq A\}$

[5] $\mathbb{P}\{n \ in \ \mathcal{R}\} = \frac{(\lambda A)^n}{n!} e^{-\lambda A}$

$$\begin{aligned}
\omega = \mathbb{P}\{Tx \rightarrow e_i | N_e = n\} &\overset{2}{=} \mathbb{E}_{r_e}\{\omega | r_e\} \\
&\overset{6}{=} \mathbb{E}_{r_e}\{\mathbb{P}\{SINR_e \geq \theta^*\}\} \\
&= \mathbb{E}_{r_e}\{F_I\Big(\frac{P_0}{r_e^{2b}\theta^*} - Nx\Big)\} \\
&\overset{7\ 8}{=} \frac{2}{r_{tx,e}^2}\int_0^{r_{tx,e}} F_I\Big(\frac{P_0}{r_e^{2b}\theta^*} - Nx\Big) r_e \, \mathrm{d}r_e)
\end{aligned} \tag{51}$$

□

[6] Property of PPP: for a fixed region and fixed number of nodes (in this case $N_e = n$), the location of the eavesdroppers is independent.

[7] Expectation value of a function: $\mathbb{E}_x(f(x)) = \iint f(x) pdf(x) \, \mathrm{d}x$.

[8] The probability density function (pdf) of the distances between the eavesdropper and the transmitter is given by: $pdf(x) = \frac{2r_e}{r_{tx,e}^2}$ (see appendix A).

4.2.1 *Evaluation*

In this subsection we will introduce our experiments and analyse the results. We will focus on a set of different scenarios, with different configurations and parameters. This will allow us to extract the necessary information to carefully assess the secrecy level of our security scheme, providing us an insight into the behaviour of the secure throughput as a function of important network parameters.

4.2.1.1 System Setup

We developed a series of matlab scripts for running *Monte Carlo* simulations matching our system model, *Figure* 36. We start by placing a transmitter and receiver distanced one unit/meter away from each other (i.e. $(x_{tx}, y_{tx}) = (0,0)$ and $(x_{rx}, y_{rx}) = (0,1)$) $\Rightarrow r_0 = 1m$, as well as, a random set of jammers and eavesdroppers on a circle region centered on the origin with a radius of $L = 4$ meters, which represents the boundaries of the space. The number of devices is, thus, determined using a Poisson random variable (mean $= \lambda \pi L^2$) and each of them is placed uniformly in the circle. Knowing that a node can successfully communicate if $\mathbb{P}\{SINR \geq \theta^*\}$ we determine the secure throughput. This procedure is repeated 10000 times, with different spatial realizations, to get an average approximation for this secrecy metric. We compare these results with our mathematical interpretation of secure throughput (45). Some of the remaining values are kept exactly the same throughout all the simulations, in particular, the transmitters' power $P_0 = P_I = 40\ mW$, the constant noise power $Nx = 4\ mW$ and the SINR threshold $\theta^* = 1$.

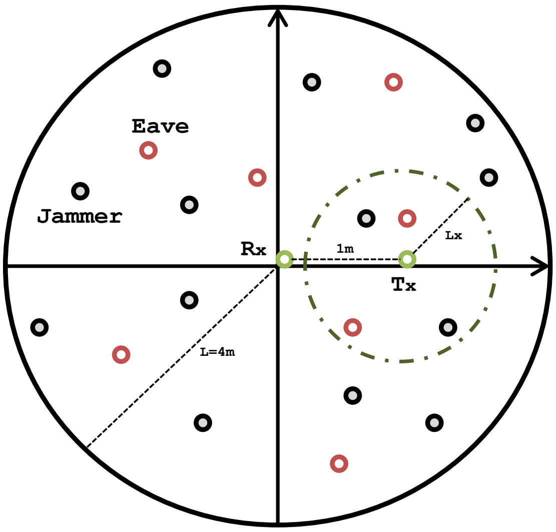


Figure 36.: *Setup for Monte Carlo experiments. The receiver* Rx *and transmitter* Tx *are respectively located at positions* $(0,0)$, $(0,1)$ *of an inner region of a circle centered on the origin and with radius* $L = 4m$. *The jammers and eavesdroppers are uniformly and independently distributed on this region. Both transmitter and jammers have a transmission power,* $P_0 = P_I$, *of 40 mW, and the SINR threshold,* $\theta^* = 1$, *is the same for all devices. The circle around* Tx, *with radius* $Lx = r_{tx,e}$, *is employed by (45) to approximate the value for the secure throughput.*

To simulate our $\mathcal{T}_s$ equation we need a closed form representation of the interference variable I. Stable distributions have a set of parametrizations that we can chose that allow us to clearly define this variable's density and distribution functions [59]. Given the proximity with our characteristic function (39), we chose one of Levy's stable distribution parametrizations with $\alpha = \frac{1}{2}$, $\beta = 1$, γ, as it fitted our own equation ($b > 1$). Analogously to Levy's case [60], we can represent our cumulative distribution function, F, as

$$F(x > 0) \sim \mathcal{S}(\alpha = 0.5, \beta = 1, \gamma) = \operatorname{erfc}\left(\frac{\gamma}{\sqrt{2x}}\right) \tag{52}$$

with *erfc* as the complementary error function. So, for our model,

$$F_I\left(\frac{P_0}{r_0^{2b}\theta^*} - Nx\right) = \operatorname{erfc}\left(\frac{\gamma}{\sqrt{\frac{2P_0}{r_0^{2\times b=2}\theta^*} - 2Nx}}\right) = \operatorname{erfc}\left(\frac{\pi\lambda 2\cos\left(\frac{\pi}{4}\right)\Gamma\left(\frac{3}{2}\right)\sqrt{P_I}}{N\sqrt{\frac{2P_0}{r_0^4\theta^*} - 2Nx}}\right) \tag{53}$$

Before analysing the results of our scheme, under the new model, we had to validate our analytical approximations, in particular, the independence between devices and the spatial restrictions to the eavesdroppers' area of influence (circle around Tx).

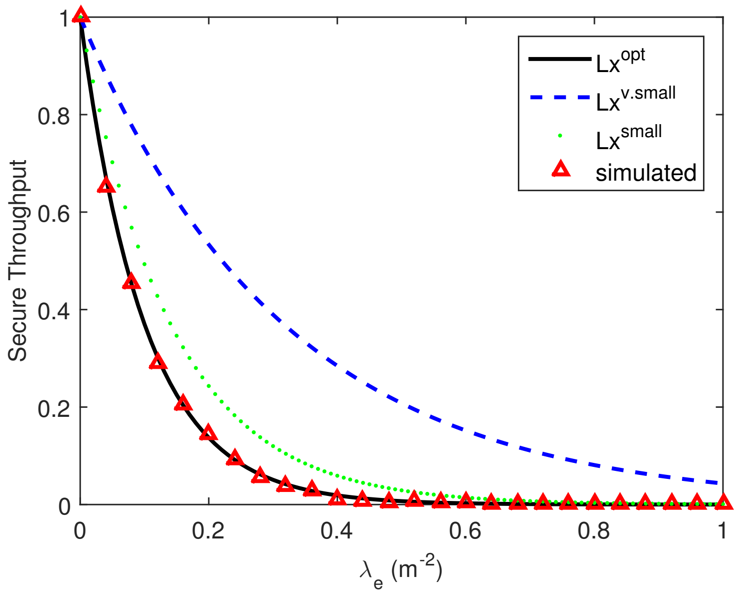


Figure 37.: *Secure throughput for a varying density of eavesdroppers with different analytical approximations (related with the radius - Lx - of the region around the transmitter) versus simulated results. This region is used to analytically determine the secure throughput defining the area in which eavesdropping is considered feasible. Three different values were chosen:* $Lx^{v.small} = 1$, $Lx^{small} = 1.5$, $Lx^{opt} \approx 1.77$.

Figure 37 displays the secure throughput (y-axis) for different Tx circle's radius, $Lx = r_{tx,e}$, with varying density of eavesdroppers by m^2 (x-axis). This plot provides a substantial evidence of our model's accuracy, showing that the probability of secure throughout approximates to the simulated scenario if we consider the optimal or a higher radius. Smaller regions, $Lx^{small} = 1.5$ or $Lx^{v.small} = 1$ do not necessarily portray the correct secure throughput and consequently our approximations do not hold in this case.

The inclusion of a threat-area, circle, around the transmitter, in which eavesdroppers are able to attack, was one of our strongest premises. This approximation was very important to determine the mathematical representation for the secure throughput and we analytically proved that it was possible to achieve an almost perfect approximation if this region was sufficiently wide - $r_{tx,e} = \left(\frac{P_0}{Nx\theta^*}\right)^{\frac{1}{2b}}$. Results from *Figure* 37 show exactly this ($Lx^{opt} \approx 1.77$), reinforcing our analytical findings.

This plot does not yet portray any of secrecy mechanisms (UFH or jamming), which explains the abrupt drop in the secure throughput that rapidly becomes impracticable ($\lambda_e \geq 0.4$). Nevertheless, results already support the fact that we no longer have a simple probabilistic model (30), where an eavesdropper in the communication channel could always overhear the information being transmitted, but rather a new one that takes into account the position of the attackers and the characteristics of the medium to better assess the probability and strenght of an attack. .

4.2.1.2 UFH

We now assess the secrecy impact of UFH with and without friendly jamming, using the optimal Lx to obtain the analytical results.Furthermore, we analyse the impact of a different set of parameters such as the number of available frequencies, the density of eavesdroppers and jammers, as well as, their interference power.

Figure 38 depicts the secure throughput (y-axis) for different attackers' density (x-axis) with a varying number of overhearing eavesdroppers close to the transmitter: without UFH vs UFH. This plot shows us that for densities of eavesdroppers, above 0.2, UFH can provide relevant protection in comparison with the *no ufh* scenario. This is associated with the availability of more non-besieged frequency channels which *Tx-Rx* can possibly use to communicate.

This advantage is particularly relevant for intermediate values of the number of eavesdroppers, where $\mathcal{T}_s^{no\ ufh}$ gets closer to 0, while UFH is still able to provide security. If an estimate of the number of eavesdroppers is available, the number of frequencies can be adjusted accordingly to maximize the secure throughput, as determined in section (3.2.1). This corresponds to the case $\mathcal{T}_s^{ufh}$-optimal-N, where the number of frequencies is adjusted to the optimal value of $\#\Pi_e + 1$. However, in the more likely case of not having information about the (silent) eavesdroppers, a non-optimal UFH still provides a secrecy advantage for a large range of number of eavesdroppers, as depicted in the curve for N = 10.

Figure 39 shows the secure throughput for the UFH scheme for varying number of frequencies, with three different densities of eavesdroppers. This graph once again highlights the fact that the number of frequencies, just like we have seen in our preliminary results (*Figure* 25) can be adjusted to significantly improve the secure throughput. Furthermore, we can see that the maximum can be obtained without abruptly changing the number of frequencies with increasing number of eavesdroppers. This happens because of the propagation effects (i.e. path loss) incorporated in this model that 'disables' some of the more distanced attackers.

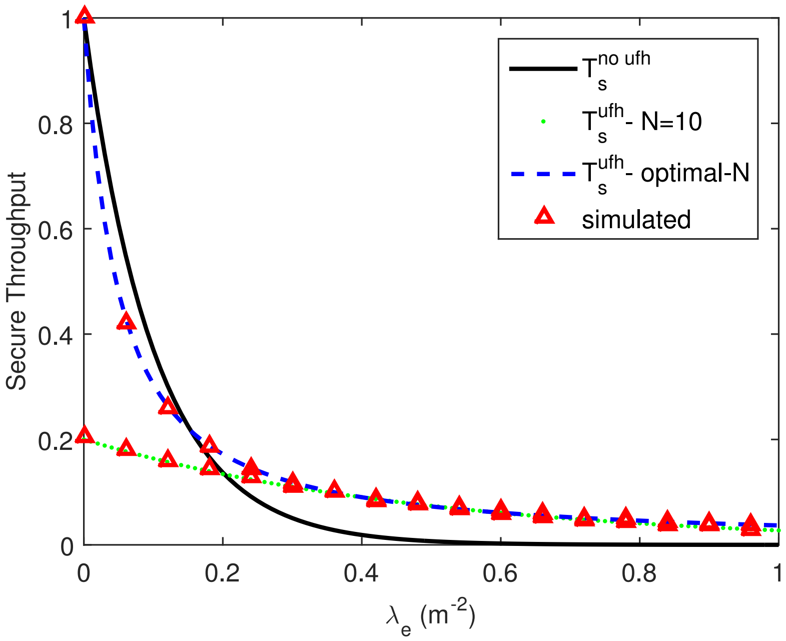


Figure 38.: *Comparison of strategies for varying λ_e (no UFH, optimal UFH, UFH with 10 frequency channels).*

4.2.1.3 UFH + Jamming analysis

Now that we have unveiled some of the positive effects of UFH, we add jamming to our system in an attempt to improve the secrecy level of this spread spectrum technique. With this extended model we no longer consider the possibility of the receiver completely eliminating the interference originated by these defensive devices, and, thus, we erase one of the strongest assumptions of the chapter 3. probabilistic model.

Figure 40 manages to keep the same characteristics has in the previous simulations but backs-up UFH ($N = 5$) with a new source of defense from jamming devices, which are randomly distributed in the system. This plot shows that jammers can improve the secure throughput after a certain density of eavesdroppers. This happens for different spatial densities of interferers, although it is clearly noticeable that high densities of jammers can have a negative effect on the secure throughput when we consider a low number of eavesdroppers.

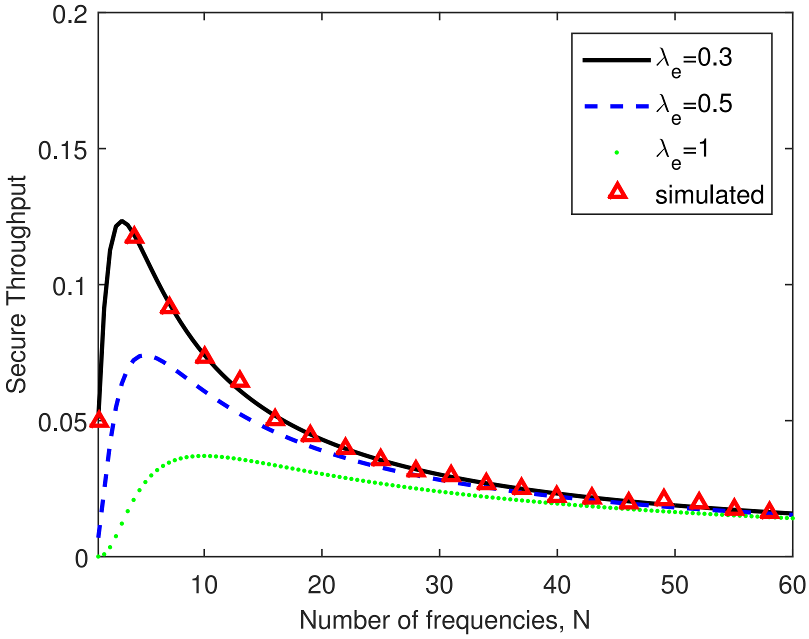


Figure 39.: *Secure throughput (T_s) with UFH versus the number of available frequencies, for various eavesdroppers' spatial densities, $\lambda_e = 0.3$, $\lambda_e = 0.5$ and $\lambda_e = 1$.*

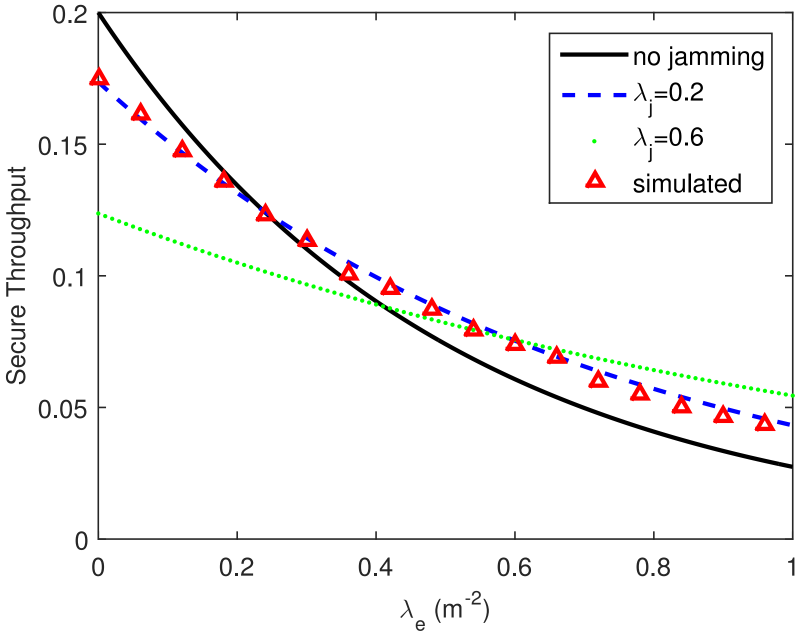


Figure 40.: *Secure throughput with UFH (5 available frequencies) and a varying number of jammers, for different λ_e. Notably, we consider three different situations, one with no jammers, another with a relatively small density of interferers, $\lambda_j = 0.2$, and another we high density of jammers, $\lambda_j = 0.6$.*

Another aspect to bear in mind is the secrecy gain provided by this mechanism. Comparing these results with the ones from the previous model (see *Figure* 31), we can verify that the $\mathcal{T}_s$ gains are lower, mainly due to the fact that this type of jamming can interfere with the communication channel and the eavesdroppers' channels. Furthermore, in this particular situation, defensive units are placed randomly in space which can hypothetically mean that some of them can be situated in rather troublesome locations (e.g very near *Rx*).

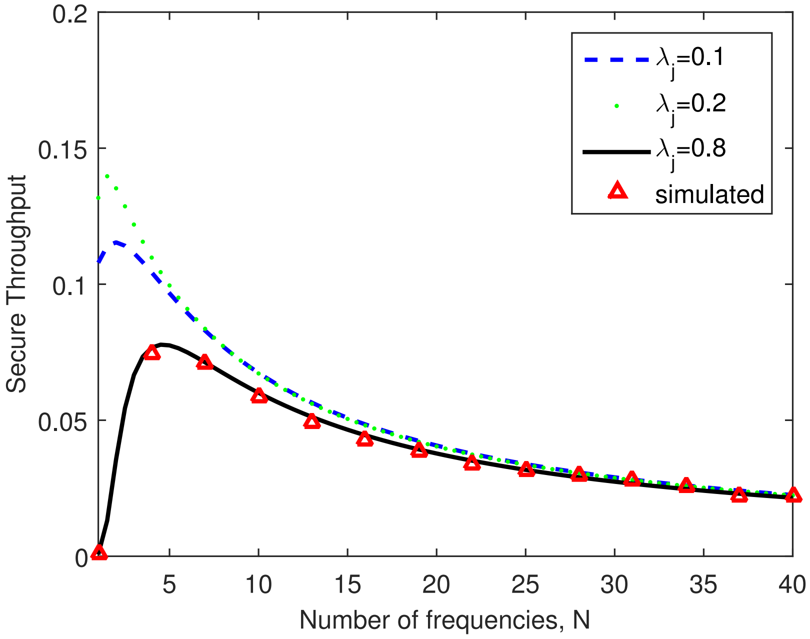


Figure 41.: *Secure throughput (T_s) with UFH and friendly jamming versus the number of available frequencies, for various jammers' spatial densities, $\lambda_j = 0.1$, $\lambda_e = 0.2$ and $\lambda_e = 0.8$.*

In *Figure* 41 we show the secure throughput with UFH and jamming for a varying number of available frequencies. We compare three different settings with dissimilar λ_j and a fixed $\lambda_e = 0.4$. This plot shows some interesting results, in particular, the existence of a maximum secure throughput as a function of the number of frequency channels also for the case with jamming. Our preliminary results from chapter 3 did not depict this situation because of the fact that jammers were solely seen has protectors and never interfered with the *Tx*-*Rx* channel. This shows that maximizing the secure throughput actually depends from both the density of eavesdroppers as well as jammers in the system.

This plot also shows that increasing the density of jammers does not necessarily mean an increase in the secure throughput for the overall system. Having many of these devices with a low set of frequencies and/or with a small number of eavesdroppers can compromise the beneficial effect of UFH, by degrading legitimate communication more often than it should. Yet one could adjust the number of jammers to the number of frequencies or eavesdroppers (if such information is available) or even add a spatial restriction to the jammers (e.g. at a minimum distance from *Rx*) to deny any unwanted strong interference to the communication channel.

To conclude, this new extended system model provides us with a more in-depth view on the secrecy level of our security scheme. Once more, we can observe an increase in the secure throughput whenever we add UFH and/or defensive jamming, and results show that the number of frequency channels available can also be adjusted to maximize secrecy. The secrecy gains are smaller when comparing with our preliminary model, which is explained by the way jammers also affect legitimate communication.

4.2.2 *UFH for secret key establishment*

Although the secure throughput associated with this scheme is relatively low, we argue that it can be useful for secret key establishment in adversarial setups without any added cost (nodes are only required to randomly hop through frequencies).

Let us consider, for example, that, on average, a user expects to get approximately 1 out of 10 secure packets ($\mathcal{T}_s$=0.1). Without knowing which packet is secure, this information may not be very useful. However, if we apply a one way hash function over all the message chunks n, and if we consider that one packet is secure from the eavesdropper, this is sufficient to generate a shared secret even if we do not know which of the message's chunk is actually protected. Furthermore, given a specific secure throughput value, one can increase the probability of having a shared secret key (at least one secure packet) by simply exchanging more packets as follows.

Lemma 1. *(Probability of having at least one secure packet):*

For a given secure throughout $\mathcal{T}_s$, the probability of having at least one secure packet for n transmitted packets is given by

$$\mathbb{P}\{\text{at least 1 secure packet}\} = 1 - (1 - \mathcal{T}_s)^n$$

and this can be made arbitrarily close to 1 with increasing number of transmissions n.

5

TEST–BED

This chapter introduces and describes our test-bed implementation using software defined radios (SDRs). These experiments are proposed as a way of verifying some of our previous analytical results, by comparing different setups and models, but mostly, as a tool for evaluating the performance of our security mechanisms when *realistically deployed*. We opted for a test-bed rather than a network simulation (e.g. NS-3) mainly because we wanted to have a clear and thorough overview of the impact of UFH and jamming in a real-life medium and with a set of hardware-bounded nodes. Although current simulation software allows for the development of a broader range of setups (i.e. with multiple nodes), a test-bed is the closest we have to a practical scenario.

The different setups displayed in the following sections were thought up having in mind our target system model, but most of all, the available hardware - five USRPs (Universal Software Radio Peripherals) and different antennas (e.g. omnidirectional, directional, etc.). Therefore, both prior to and during the project work, we accounted for the limitations and boundaries to make sure that the main goals would be tangible within the specified scope and time frame.

This chapter is organised in the following way: the first section describes each of the scenarios, introduces system variables and implementation details, whereas the second section displays and analyses the results obtained.

5.1 Settings

To build up our test-bed we resort to Gnuradio and SDRs (section 2.6), more specifically five USRPs B210, which can operate on a continuous frequency coverage from 70 MHz – 6 GHz. We consider a system setup identical to our mathematical model, but only comprising a maximum of two eavesdroppers and one jammer. We have devised four setups with different intervenients each representing a specific experiment.

Figure 42 portrays each of these scenarios, as well as, the disposition of the nodes and distances. Each of these devices corresponds to a single USRP and are hooked to a single computer, responsible for analysing the data. Hence, our **first setting** includes a transmitter, Tx, and a receiver, Rx, distanced $1.5\,m$ from each other and an eavesdropper, E, $2\,m$ away from Tx and approximately $1.75\,m$ from Rx. The reason for placing the destination nodes with dissimilar distances to the transmitter was to allow for the analysis of two different situations, by easily switching each node - one advantageous

(*Rx* is closer to the transmitter) and one disadvantageous (*Rx* farther away than the eavesdropper). These are obtained by simply swapping the roles of the eavesdropper and the legitimate receiver, without any other change to the system.

Our **second setting** adds another device, notably, an interferer which aims to defend the legitimate communication. This node is placed near the eavesdropper, $0.5\,m$, and $1\,m$ away from the receiver. Once again, we can easily switch the receiving devices, setting up a good and bad scenario. In this case, the jammer possess an omnidirectional antenna and therefore interferes with both *Rx* and *E*.

The **third setting** incorporates another assailant placed near the legitimate receiver, $0.2\,m$, and distanced $1.3\,m$ from the transmitter.

Finally, the **last setting** is similar to the second one but this time the jammer is deployed with a directional antenna which allows it to define a specific direction in which it will interfere (opposed to *Rx* and targeting an eavesdropper).

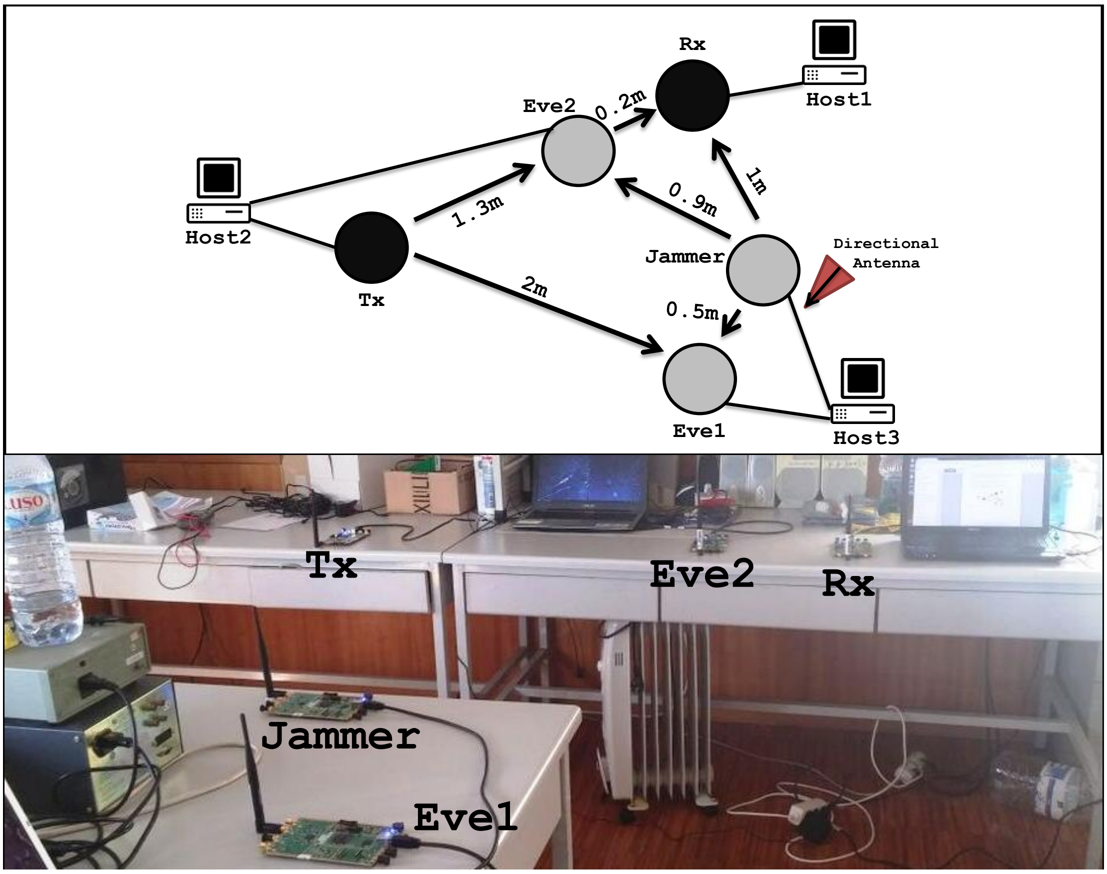


Figure 42.: *Test-bed setup. The scenarios are organised in the following way,* ***Scenario 1:*** *Tx, Rx and Eve1;* ***Scenario 2:*** *Tx, Rx, Eve1 and Jammer (omnidirectional antenna);* ***Scenario 3:*** *Tx, Rx, Eve1, Eve2 and Jammer;* ***Scenario 4:*** *Tx, Rx, Eve1 and Jammer (directional antenna).*

5.1.1 *Hardware*

The main system hardware is, for this *project*, limited to a maximum of five sets of B210 USRPs with Spartan6 FPGAs (Field-Programmable Gate Arrays) from National Instruments, and three different host computers. This implies that each host computer will control (through USB connection) between one to two USRPs (see *Figure* 42) each with their own omnidirectional or Log-Periodic/directional antenna (for the jammer in the last scenario). The purpose of the host computers is to capture data from the system, such as the transmitted/received signals, allowing us to control and monitor the different experiments. These host computers are also used to program the hardware of the controllers in the FPGA. *Table* 7 shows the specification of the different computers used in the test-bed.

Host PC 1	Host PC 2	Host PC 3
Ubuntu 14.0.4 LTS	Ubuntu 14.0.4 LTS	Ubuntu 14.0.4 LTS
Intel Core i5 - 2.40GHz× 4	Intel Core i7 - 2.00GHz× 2	Intel Core 2 Duo - 2.26GHz× 2
2 GB dual-channel 1067 MHz DDR3	4GB dual-channel 1600 MHz DDR3	2 GB dual-channel DDR3
Gnuradio 3.7.7	Gnuradio 3.7.7	Gnuradio 3.7.7
UBS 2.0	USB 3.0	USB 2.0

Table 7.: *Specification for all three host computers.*

The RF-Frontend modules (USRP model) used in these experiments are the five USRPs B210 (see *Figure* 43) that are responsible for converting all the digital signals, from the FPGA card, to analog form and transmit them over the air (transmitter and jammer) as radio-frequency (RF) signals within a specific frequency band with the help of antennas. The frontend modules can also receive analog radio signals with the help of antennas and then convert them to digital form (receiver and eavesdropper). These digital signals are then forwarded to the FPGA for signal processing and data analysis.

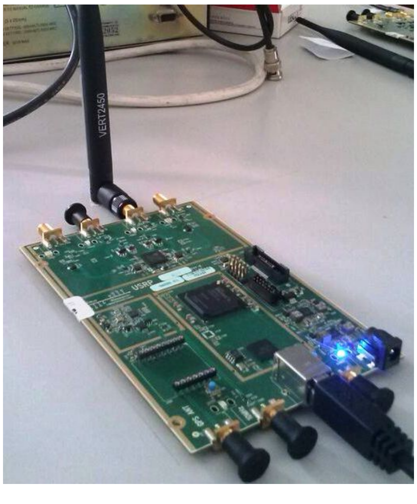


Figure 43.: *USRP B210.*

Each of these devices has two full-duplex outputs (Tx/Rx) and two receiving inputs (Rx), albeit only one of these *ports* is actually used. They operate within a frequency range from 70 MHz up to 6 GHz. The frontend modules are connected to the FPGAs through a custom Input Output (I/O) and the antennas are connected to the frontend modules through SubMiniature Version A (SMA) connectors. *Table* 8 shows the specifications of the USRP B210.

B210 USRP
Coverage: 0.07 – 6 GHz
Full duplex, MIMO (2Tx&2Rx)
Up to 56 MHz of real-time bandwidth
USB 2.0/3.0 connectivity
Spartan 6 XC6SLX150 FPGA
Full support for the USRP Hardware Driver (UHD) software

Table 8.: *Specification for the USRP B210.*

The antennas used in the test-bed, for transmitting and receiving the RF signals, are four omnidirectional vertical antennas and one Log-Periodic Printed Circuit Board (PCB) antenna. The first set is omnidirectional and operates over two different frequency bands, whereas the PCB antenna is directional and operates over a broader band of frequencies. The specific antennas used are, respectively, the VERT2450 and LP0965 PCB manufactured by Kent Electronics. *Table* 9 shows the specification for this equipment.

VERT2450	LP0965 PCB
2.4 – 2.5 and 4.9 – 5.9 GHz - Dualband	0.85 – 6.5 GHz
Forward Gain: 3 dBi	Forward Gain: 6 dBi
	Size: 13.4 × 14.2 cm
	120° horizontal and 160° vertical beam-width

Table 9.: *Specification for the antennas.*

5.1.2 *Software*

To have a complete overview of the system and its correspondent variables we present a GRC-style (Gnuradio companion) description of our program (see *Figures* 44 and 45). This information is particularly important to comprehend the inner-works of our test-bed.

Figure 44 shows the inlaid structure of the transmitter and receiver/eavesdropper programs. To build this software, we employed some of the available tools provided by

Gnuradio (e.g. *building* blocks), as well as, two example-codes, *benchmark_tx* and *benchmark_rx*. These two programs are accessible to the end-user to exemplify signal transmission and reception over the air, offering some added flexibility through a couple of input variables. Nevertheless, some changes had to be made in order to accommodate our system requisites and consequently fit our needs.

Both programs comprise the following modules: a *main class* responsible for continuously running the program during a specific time-frame, making the necessary changes in real-time (e.g. changing frequency, storing packets); a *top_block*, the outer class for any Gnuradio program, responsible for hooking up the lower layer blocks; and two *hier blocks* (classes that encapsulate other blocks), one for modulating/demodulating the information from in and out the USRPs, and another for setting up the USRPs as transmitters or receivers.

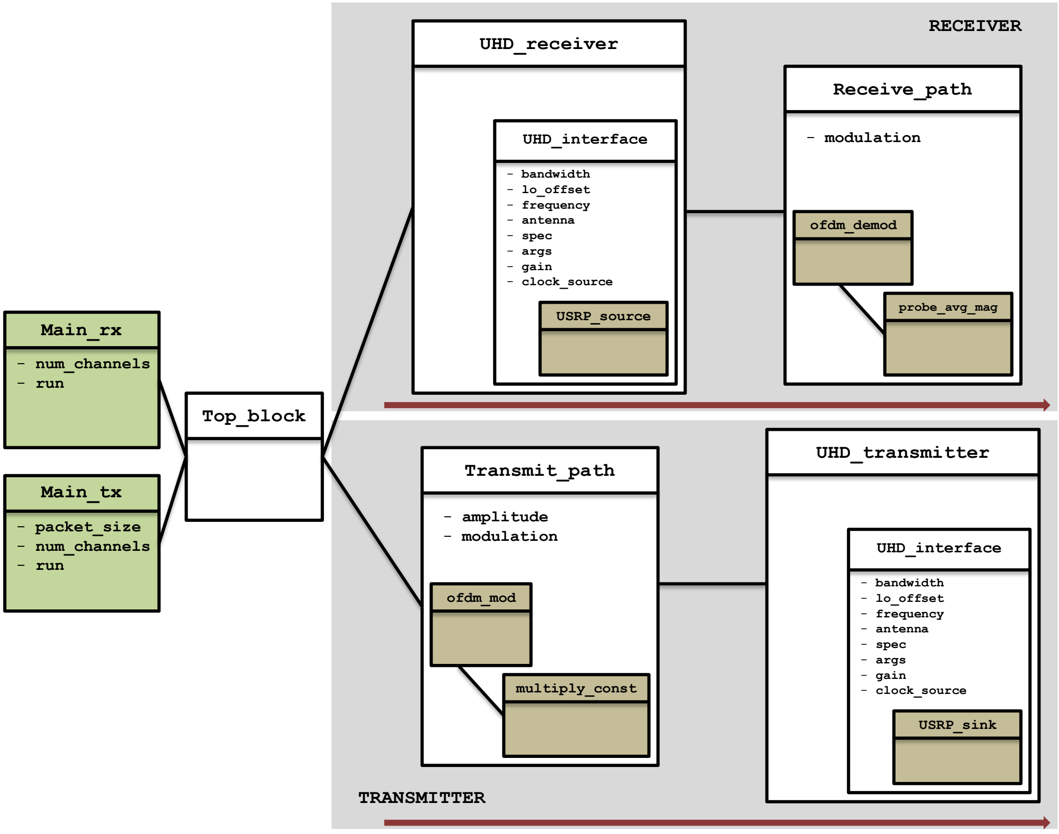


Figure 44.: *Schematic of the transmitter and receiver/eavesdropper code that allows the devices to, respectively, send and receive signals (packets) over the air. The arrow is the signal flow and the brown rectangles represent the in-built blocks (black box), which are already available in Gnuradio.*

A closer look at the *UHD_transmitter* and *UHD_receiver* reveals two in-built blocks (highlighted in brown), the *USRP_sink* and *USRP_source*. These particular blocks are Gnuradio components and are available for us to use, encompassing a series of variables (see *Table* 10) ready to be tuned up. This allows to us to easily define our transmitting/receiving front-ends.

Variable	Default	Definition
bandwidth (Hz)	$500 \times 10e3$	Symbol bandwidth or sample rate
lo_offset	0	Local oscillator offset in Hz
frequency	-	Transmit/receive frequency
antenna	-	Antenna (e.g. 'Rx')
spec	-	Subdevice of the USRP where appropriate
args	-	USRP device address
gain (dB)	midpoint	Transmit/receive gain in dB
clock_source	-	Clock source (e.g. 'external')

Table 10.: *Variables for the USRP source and sink blocks.*

Next, the *transmit_path* and *receive_path* also include a set of two Gnuradio blocks each, responsible for encoding/decoding and modulating/demodulating the 'information' travelling the medium. Hence, packets from the *main_tx* are encoded using orthogonal frequency-division multiplexing (OFDM), and each sub-carrier frequency is modulated with a conventional modulation scheme (the default is a binary phase-shift keying (BPSK) modulation) - *ofdm_mod*. The transmit amplitude of the signal sent to the USRP, which will then be forwarded to the air, is conveyed using the Gnuradio *multiply_const* block. In the opposite direction, the signal is received by the USRP and then demodulated, using *ofdm_demod*, filtered and its strength level compared with some threshold (for carrier sensing), *probe_avg_mag_sqrd*, to identify whether or not it is the intended signal. The transmitted packet is then propagated to *main_rx* through a callback function. All these blocks comprise a lot more operations and variables than the ones described here, which Gnuradio keeps hidden, for the sake of simplicity. *Table* 11 introduces some of the input variables.

Variable	Default	Definition
amplitude	0.1	Transmitter digital amplitude: $[0, 1[$
modulation	BPSK	Modulation type (bpsk, qpsk, 8psk, qam)

Table 11.: *Variables for the* transmit_path *and* receive_path *and correspondent blocks.*

Finally, the two *main* classes allow us to make some adjustments on the run, in particular, changing the device frequency periodically and/or setting up the packets to be sent. In order to account for UFH, devices switch frequencies randomly and between a predefined number of channels, *num_channels*, at a rate of 1 frequency/second. This hopping operation is asynchronous among devices, culminating in a small amount of lost packets, which is, nevertheless, insufficient to have any considerable impact on our results. Each packet transmitted encapsulates a specific sequential id number (2 bytes), as well as, some random data to fill in the remaining space, *packet_size* (by default 400-2 bytes). If there are any skipped id numbers at the receiver some packets are being lost.

The demodulator block also includes an in-built error-detection tool that informs the receiver of damaged packets.

All data is stored internally on the host computer and is later used to calculate the secure throughput - (# *packets received* - # *number of packets received that are compromised*) / # *packets sent*. The variable *run* in the *Tx* and *Rx* modules of *Figure* 44 keeps track of the number of executions to ease out the task of storing the information in files.

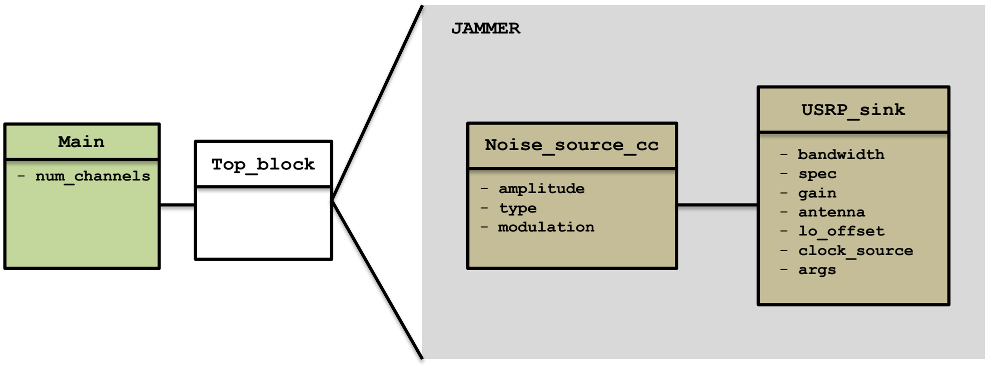


Figure 45.: *Schematic of the jammer code that allows the device to generate and propagate some noise (gaussian or uniform) over the medium.*

Figure 45 shows the structure of the jammer program. Although slightly different, this software yields a similar set of operations as the previous transmitter code, encapsulating some of the same blocks such as the *USRP_sink*. The block arrangement is based on another example-code provided by Gnuradio - *uhd_siggen* - and a couple of new functions and variables are added to account for UFH (i.e. *num_channels*).

The centerpiece for this application is the Gnuradio *noise_source* block, which intuitively allows us to generate different noise signal patterns that are continuously propagated to the medium and disrupt communication. As in any other transmitter program, we can set the signal amplitude and correspondent modulation technique to be employed (by default BPSK). Furthermore, this new block offers the possibility to choose from two different noise patterns (*type*) - Gaussian and uniform. Apart from this new block, the jammer code operates exactly as the previous transmitter, steadily jamming and switching frequencies every second.

To conclude, each one of these three programs is individually run at each USRP device depending on their role - transmit, receive/eavesdrop or jam. The results will heavily depend on the variables' values, as well as, on the disposition of the nodes (the setup).

5.1.3 *Device Configuration*

Setup	I	II	III	IV
Devices	Tx, Rx, Eve1	Tx, Rx, Eve1, J	Tx, Rx, Eve1,2, J	Tx, Rx, Eve1, J (PCB Antenna)
a)	Rx closer to Tx	Eve1 closer to J	No Jamming	Eve1 closer to J
b)	Eve1 closer to Tx	Rx closer to J	Jamming	Rx closer to J

Table 12.: *Setup's summary. Tx: Transmitter, Rx: Receiver, Eve: Eavesdropper and J: Jammer.*

To run each of our experiments (see *Table* 12), we designated a series of values for some of the correspondent input variables. The others were left unchanged, whether because we did not need them or were already correctly set by Gnuradio. Each device/program is tuned-up differently according to their role and spatial position. *Table* 13 lists all the values for the different variables.

Variable	Value		Variable	Value		Variable	Value
Transmitter			Receiver			Jammer	
args	*F5EAC0*		args	*F5EAE1*		args	*F5EABF*
antenna	Tx/Rx		antenna	Rx		antenna	Tx/Rx
bandwidth (Hz)	10e6		bandwidth (Hz)	10e6		bandwidth (Hz)	10e6
amplitude	0.6					amplitude	0.6
gain (dB)	60		gain (dB)	40		gain (dB)	50
modulation	BPSK		modulation	BPSK		modulation	BPSK
num_channels	[2, 9]		num_channels	[2, 9]		num_channels	[2, 9]
run	[1, 14]		run	[1, 14]		type	Gaussian
Eavesdropper 1			Eavesdropper 2				
args	*F5EAB8*		args	*F5EAB0*			
antenna	Rx		antenna	Rx			
bandwidth (Hz)	10e6		bandwidth (Hz)	10e6			
gain (dB)	40		gain (dB)	40			
modulation	BPSK		modulation	BPSK			
num_channels	[2, 9]		num_channels	[2, 9]			
run	[1, 14]		run	[1, 14]			

Table 13.: *System variables and their values.*

The *args* variable identifies the USRP by its id tag, while the *antenna* specifies which frontend will be used by the device (i.e. *Rx* and eavesdropper → *Rx*; *Tx* and Jammer → *Tx/Rx*). For *bandwidth*, or sample rate, we choose 10*e*6 Hz or samples/second, which, internally, allows for the transmitter to send 87 packets/second with 400 bytes each (default size). The jammer continuously emits Gaussian noise.

In terms of *amplitude*, we choose 0.6 for both transmitter and jammer. We adjusted the amplitude at the transmitter by slowly increasing its value, starting with 0.1 and stopping at 0.6. With lower values, transmitting packets resulted in significant distortion, whereas, beyond this point, we were generating far more power than was needed to get error-free reception. We did the same on the jammer, but this time we had in mind its effect on the communication (lower values → no impact; higher values → too much energy). We also kept the default BPSK modulation.

Although the Federal Communications Commission (FCC) mandates at least 50 different channels and at least a 2.5 Hz hop rate for narrowband frequency-hopping systems, we opted, because of time and hardware constraints, between 2 and up to 9 different frequency channels ranging from [2450 MHz, 2458 MHz], with a 1 Hz hop rate. Given the small number of devices, and the randomness associated with the communication paradigm, this number of channels was, thus, sufficient to allow for a rigorous portrayal of each setup. The range of frequencies is also adequate and works with both types of antennas, omnidirectional and directional.

The *gain* (in dB) relates to the frontend power gain and is a key performance figure which combines the URSP output power with the the antenna's direction and electrical efficiency. For a given frequency, the device's effective area is proportional to the power gain and thus, values throughout the different setups might sometimes change. Most of the times, the transmitter, receiver, jammer and eavesdroppers have a gain of 60, 40, 50, 40, 40 dB respectively, allowing for a smooth and error-free execution of our experiments. To get to these values we had to take into consideration hardware constraints and power loss due to fading and other propagation effects. USRPs B210 have a receiver frontend with 73 dB of available gain and a transmitter frontend with 89.5 dB of available gain. Although application-specific, Ettus Research recommends, in its manual, that users opt for at least half of the available gain to get a reasonable dynamic range. Therefore, we began by defining each frontend gain as half their maximum value and slowly increased it to account for power-loss. All receiving devices have the same gain in order to ensure similar receiving capabilities.

5.1.4 *Statistical Analysis*

Another aspect to take into consideration when running our test-bed is the number of repetitions, so that we can have an approximate and yet statistically accurate value for the secure throughput. In every setup, we execute a **2-minute** experiment **10 times** for each different number of available frequencies, ensuing no less than $10 \times 9 = 90$ tests. The relative small number of samples was mostly due to the high amount of time it took to execute each run but is still sufficient to provide valid statistical results. Despite the fact that a small number of samples tends to increase the margins of error of confidence intervals, we can still draw important conclusions if, for example, the differences are substantial. After collecting the data, we calculate the secure throughput - (*# packets received - # number of packets received that are compromised*) / *# packets sent* - and determine the mean value and correspondent confidence interval, which provides some indication of the reliability of the data.

The confidence intervals, represented in *Figure* 46 as the overlaying black lines, represent the range (interval) that symbolize the probability (relates to the confidence level) of observing the true mean. Whenever the number of samples is relatively small but independent and they do resemble a normal distribution and yet different from $\mathcal{N}(0,1)$, we use the *t-distribution* to determine the confidence interval [61]. Thus,

$$CL\% = \overline{X} + \frac{tS}{\sqrt{N_s}} \tag{54}$$

where CL is the confidence level or chosen probability (95%), $\overline{X}$ is the mean of the sample data, N_s is the size of the population, S is the standard deviation and t is the t statistic corresponding to the appropriate probability level and degree of freedom. The number of degrees of freedom depends on the number of samples ($N_s - 1$). There are three different values for the confidence level that are usually employed, 90%, 95% and 99%, which affects the overall size of the range (the higher CL is, the larger tends to be the confidence interval). The same happens with the number of samples, but this time, the confidence interval usually decreases as the sample size N_s increases. Whenever the confidence intervals do not overlap we can assume, with a certain degree of certainty, that the groups of samples are different [62], [63].

To ensure that the data extracted resembled a normal distribution (with unknown mean and standard deviation) and, hence, guarantee a correct statistical analysis, we ran for each collection of samples a *Shapiro Wilk test* [64]. This test computes a value (55), usually represented as W, using the observed samples, that indicates whether or not the data seems normally distributed - if W is higher than a certain threshold (depends on the confidence level being used) than it is normal, otherwise, it does not follow a normal distribution.

$$W = \frac{\left(\sum_{i=1}^{N_s} a_i x_{(i)}\right)^2}{\sum_{i=1}^{N_s} (x_i - \overline{x})^2} \tag{55}$$

where a_i are constants and $x_{(i)}$ is the ith order statistic (i.e. the ith-smallest number in the sample). Our results have shown that in fact each of our set of samples resembles a normal distribution and thus, we can use the *t-distribution* to determine our confidence interval.

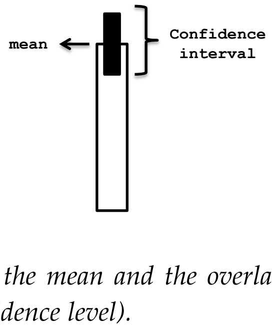


Figure 46.: *Bar plot. The top line is the mean and the overlapping black rectangle is the confidence interval (with a 95% confidence level).*

5.2 Results

This section introduces the four different setups and compares the results between them along with our mathematical analysis. To enact a precise and rigorous test-bed, we defined a clear and thorough set of values for our input variables and devised a statistical study to account for the inherent randomness associated with the tests.

5.2.1 *Setup I*

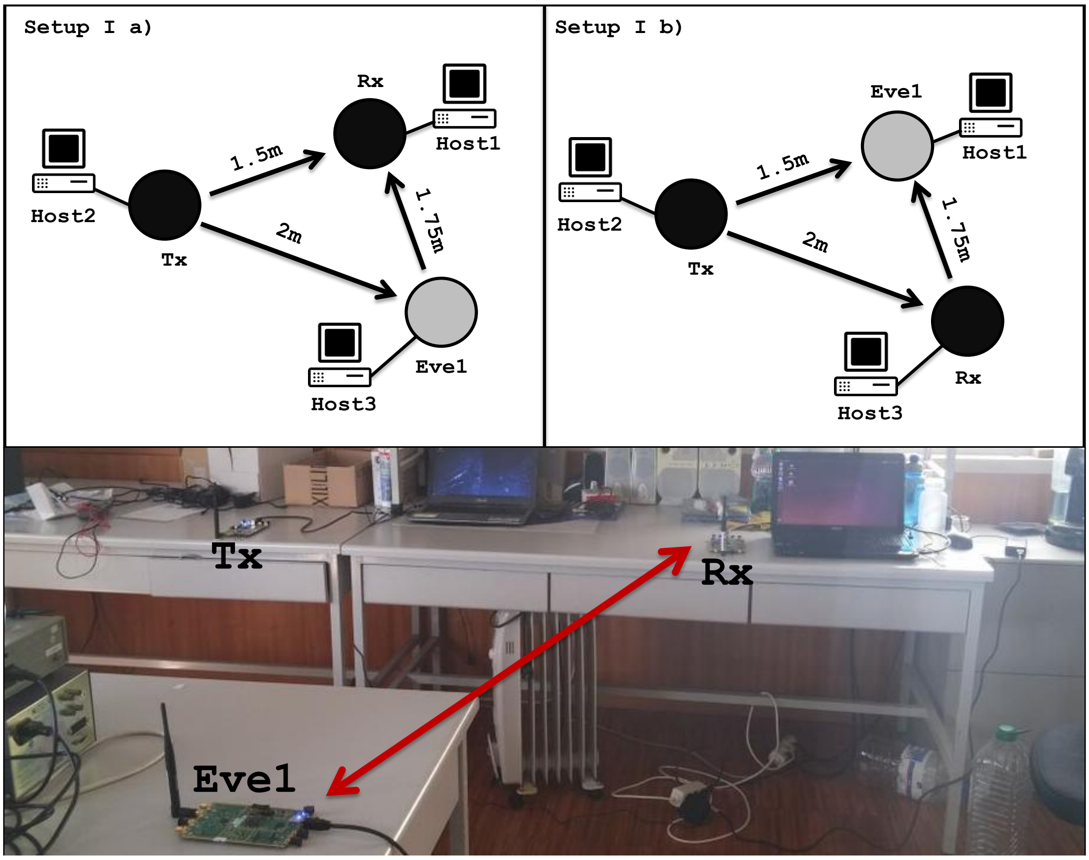


Figure 47.: *Setup I consists of one transmitter, one receiver and one eavesdropper spatially scattered. It comprises two scenarios: one advantageous, a), and another disadvantageous, b), whether the attacker is placed farther or closer to Tx.*

The **first setup**, *Figure* 47 attempts to recreate a simple scenario where one transmitter communicates with a receiver using UFH, while a silent assailant, eavesdropper, tries to overhear the communication. Each device is interpreted as an USRP board hooked up to a host computer. The transmitter is placed 1.5*m* directly away from the receiver and 2*m* from the eavesdropper. All devices asynchronously jump frequencies every second, using a predefined pool of available channels. *Table* 12 lists all system variables and values for the different agents, which are kept unaltered during this experiment.

This setup comprises two different settings, an *advantageous*, a), and a *disadvantageous*, b). They are exactly the same except for the fact that the receiver and eavesdropper

a)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.925	0.917	0.948	0.894	0.915	0.944	0.945	0.850
b)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.928	0.956	0.893	0.930	0.899	0.981	0.943	0.970

Table 14.: *Shapiro Wilk test (normality test) for setup I. The* ***threshold*** *for 95% confidence level is* ***0.842****.*

location is swapped, making it easier or harder for the attacker to miss any packets due to propagation effects. For both scenarios we calculate the secure throughput, or in other words, the ratio of uncompromising packets at the receiver versus the number of packets sent by the transmitter. Results are then compared with our previous mathematical model (29) using the distance between Tx and $Eve1$, $d = 2m$, to calculate a weak approximation for the number of participants. To do that, we determine the equivalent density (# $eves/m^2$) when there is only one eavesdropper inside a circle region with a $d = 2m$ radius (no jammers: $\lambda_j = 0$, $\lambda_e = \frac{1}{\pi d^2}$).

Table 14 lists the values for the Shapiro Wilk test for setup I (using SPSS software). This checks whether or not the data collected resembles a normal distribution. To do so we have to compare the test result, W, with a threshold - 0.842 - specific for our confidence level (95%). If this value is greater than the threshold the data seems normal and we can use the *t-distribution* to calculate our confidence interval.

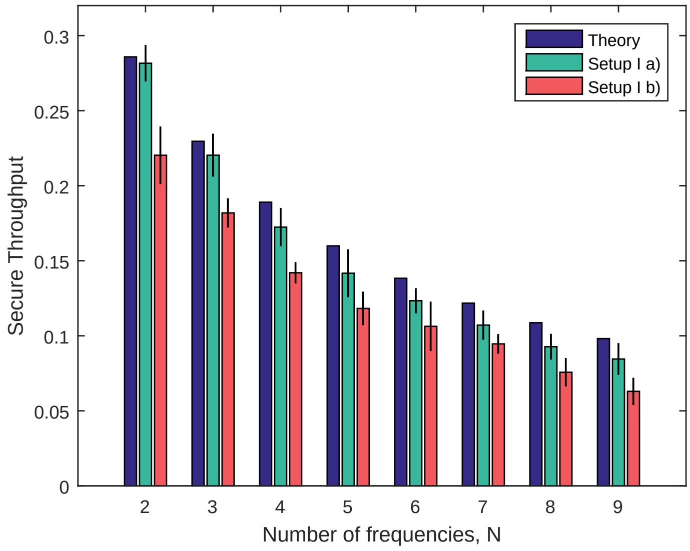


Figure 48.: *Setup I - mean and confidence interval (standard error of the mean).*

Figure 48 plots the mean of the secure throughput (y-axis) and its confidence interval (95%) with varying number of available frequencies (x-axis) for settings, a), b) and the theoretical results. We can see that the advantageous one, has a higher secure throughput than its counterpart, which can be explained due to a higher number of successfully received packets by the legitimate receiver, opposed to a lower number of correct packets overheard by the eavesdropper, as a result of the attacker being farther away.

In most cases the differences are quite significant since the confidence region for both groups does not overlap and we can assume with a 0.05 significance level (95% certainty) that the mean value for the first setting is relatively smaller than the second one. Nevertheless, both settings behave exactly the same way as we increase the number of available channels, and results follow the same behavior as our mathematical model. The discrepancy can be explained due to the inability to place the attacker at a specific location, since the theoretical model only considers random locations for the attackers. Other *environmental* characteristics (e.g. power of devices, fading levels, other propagation effects, etc.) can also increment the differences.

5.2.2 *Setup II*

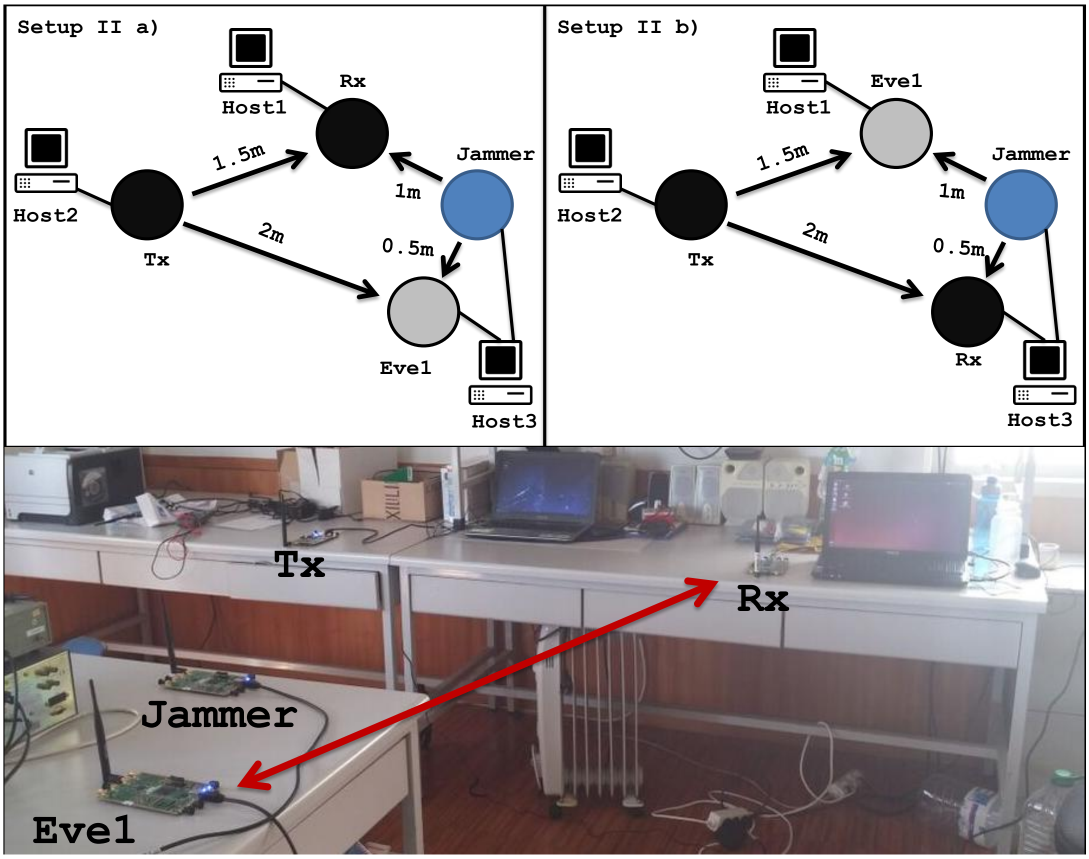


Figure 49.: *Setup II consists of one transmitter, one receiver, one eavesdropper and one jammer spatially scattered. It comprises two scenarios: an advantageous, a), and a disadvantageous, b), whether the jammer is placed farther or closer to the attacker.*

Figure 49 depicts our **second setup** which preserves the same structure as the previous one, but this time, with an added device, jammer, responsible for interfering with both the legitimate and eavesdropper channels. This new agent is placed $0.5m$ away from the eavesdropper and $1m$ from the receiver and has an omnidirectional antenna, capable of transmitting in all directions. It jumps frequency every second, and permanently emits Gaussian noise. For more information about its characteristics check *Table* 12.

a)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.959	0.950	0.957	0.937	0.979	0.893	0.936	0.985
b)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.873	0.930	0.889	0.918	0.903	0.964	0.907	0.905

Table 15.: *Shapiro Wilk test for setup II. The* ***threshold*** *for* 95% *confidence level is* ***0.842****.*

This setup also includes two different scenarios, where we, once again, swap the location of the eavesdropper and receiver to simulate two different settings: jammer is closer to *Rx*, b), or *Eve*, a). This allows for a *advantageous* and *disadvantageous* version of the system, unveiling the impact of jamming when it is differently positioned in space. Results from both settings are set side by side with *Setup I-a*. We do not compare our results with our mathematical model as it is almost impossible to exactly reproduce the same scenario, since (29) assumes both eavesdroppers' and jammers' locations to be random and unknown to the legitimate users.

Table 15 lists the values for the Shapiro Wilk test for setup II again showing the statistical validity of results.

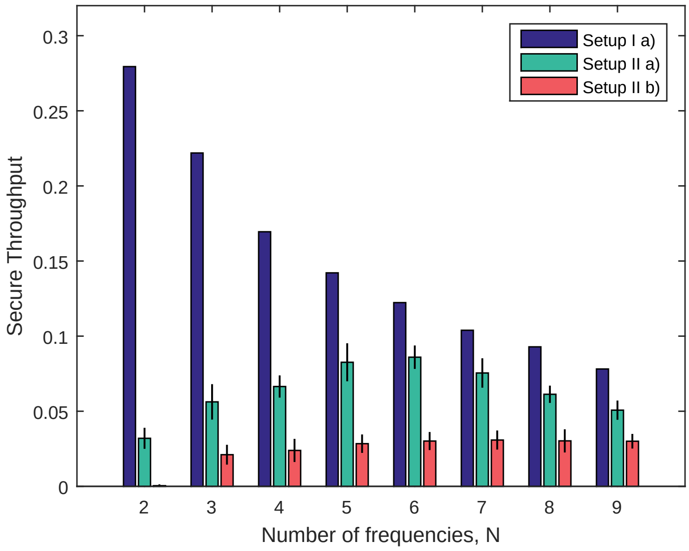


Figure 50.: *Setup II - mean and confidence interval (standard error of the mean).*

Figure 50 plots the mean of the secure throughput (y-axis) and its confidence interval (95%) with varying number of available frequencies (x-axis) for settings, a), b) and compares them with the previous advantageous setting (receiver closer to the transmitter). This figure shows that the secure throughput for both experimental settings can be maximized, depending on the number of available frequencies, a behaviour that we have also observed in our more evolved theoretical model of chapter 4. Our results also show the importance of the jammer closer to the eavesdropper (*Setup II-a*) to increases the secrecy level of our system. As such, developing a scheme for placing the jammers, [18], is fundamental to ensure maximum efficiency.

Yet, results from our jamming setup can be considered insufficient and are definitely lower when compared with our last UFH-only *environment*, *Setup II-a*. This particular behavior is in line with our theoretical model (see *Figure* 40), corroborating the fact that defensive jamming is more clearly beneficial, in the presence of multiple attackers.

5.2.3 *Setup III*

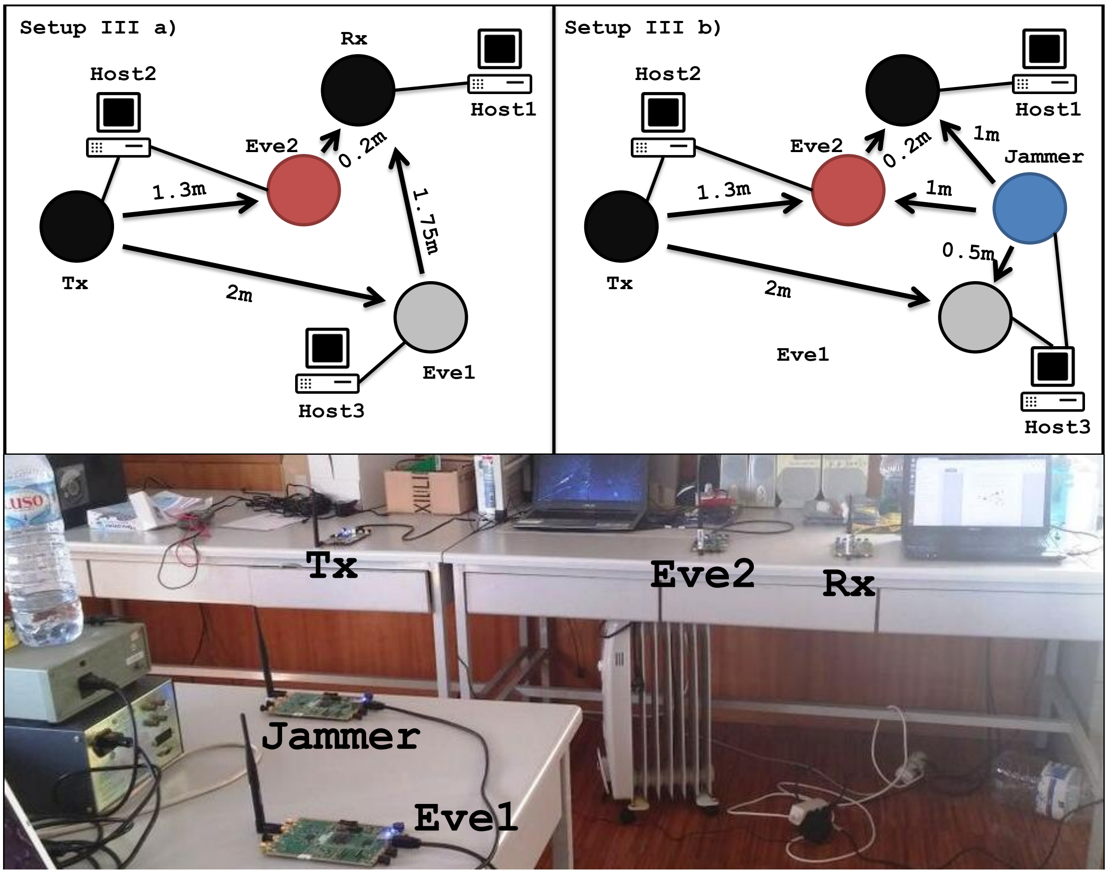


Figure 51.: *Setup III consists of one transmitter, one receiver, two eavesdroppers and one jammer spatially scattered. It comprises two scenarios: one with no jamming, a), and another with a single defender, b).*

The **third setup** of our installment, *Figure* 51, offers a more complex scenario by adding another assailant, *Eve2*, placed 1.3m away from the transmitter and 1m from the jammer. We have the same inlaid structure and values for our system variables (see *Table* 12), but this time, two of the devices try to overhear the packets being transmitted. The attackers are similar to each other and act independently with no collusion possible. Nevertheless, their location significantly impacts their potential threat, with *Eve1* being the least powerful attacker (farther away and near the jammer) and *Eve2* being the strongest one, a non-degraded version. For our first setting, a), we decided not to activate our omnidirectional jammer, while our second one, b), includes the fully operational defender.

a)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.959	0.949	0.952	0.897	0.946	0.940	0.920	0.879
b)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.916	0.969	0.955	0.956	0.939	0.911	0.911	0.885

Table 16.: *Shapiro Wilk test for setup III. The* ***threshold*** *for 95% confidence level is* ***0.842****.*

In this setup we compare results for both settings, with and without jamming, and confront them with our jamming experiment in a bid to demonstrate the positive impact defensive jamming has when the system is under attack by multiple devices.

As before, *Table* 16 lists the values for the Shapiro Wilk test for setup III.

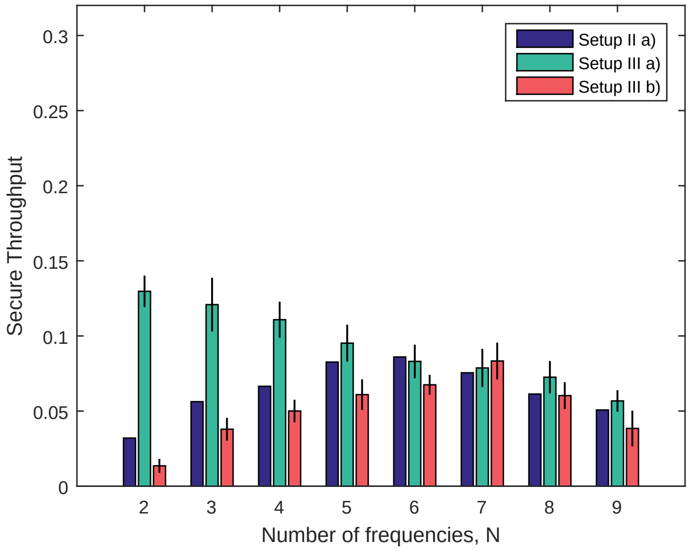


Figure 52.: *Setup III - mean and confidence interval (standard error of the mean).*

Figure 52 plots the mean of the secure throughput (y-axis) and its confidence interval (95%) with varying number of available frequencies (x-axis) for settings, a), b) and compares them with the previous jamming *Setup II-a*. This figure shows that, when the system is assailed by more than one attacker we can, with the right number of frequencies, increase the secure throughput if we add defensive omnidirectional jamming. Although visible, the gain is still not clearly significant but suggests that as we increase the number of attackers, jamming becomes more and more beneficial.

Furthermore, if we compare secure throughout values with one, *Setup I-a*, and two assailants, *Setup III-a*, we can notice that a higher number of attackers reduces the secrecy level of the system, even if they are operating independently (no collusion).

5.2.4 *Setup IV*

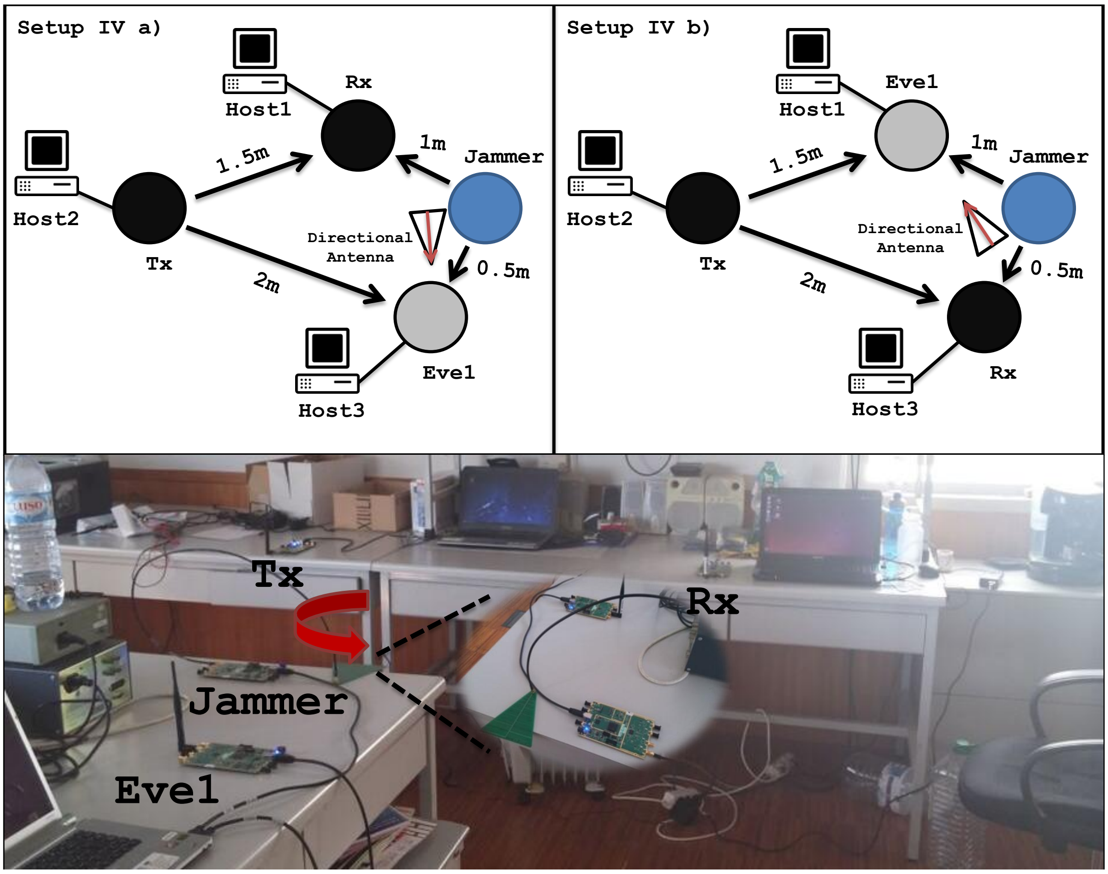


Figure 53.: *Setup IV consists of one transmitter, one receiver, one eavesdropper and one directional jammer spatially scattered. It comprises two scenarios: one where the jammer is placed farther away, b), and another, a), where it is closer to the attacker.*

Our **fourth**, and last, **setup**, *Figure* 53, is considerably similar to the second one but, this time, the jammer is geared up with a PCB antenna capable of transmitting signals in a particular direction. Therefore, we can shift the antenna towards the eavesdropper (or simply away from the receiver) to reduce the jammer's harmful effect on the legitimate communication, while still disrupting the eavesdropper channel. To corroborate this fact we devised two different scenarios, one where the jammer is closer to eavesdropper and relatively away from the receiver, and another where these devices swap positions. We also had to take into account the new PCB antenna by changing the gain value from 50dB to 60dB, in order to generate enough power for the Gaussian signal to disrupt the *Eve*'s channel.

In this setup we compare the results for both layouts to ascertain whether or not directional jamming can be advantageous and, thus, further increase the secure throughput of our UFH communication paradigm. We also invoke *Setup I-a* to correlate our results with a non-jamming setting to better assess these secrecy improvements.

2*a)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.936	0.846	0.889	0.891	0.972	0.941	0.939	0.907
2*b)	# Frequencies	2	3	4	5	6	7	8	9
	W	0.911	0.889	0.946	0.844	0.942	0.940	0.966	0.892

Table 17.: *Shapiro Wilk test for setup IV. The* ***threshold*** *for 95% confidence level is* ***0.842****.*

Table 17 lists the values for the Shapiro Wilk test for setup IV.

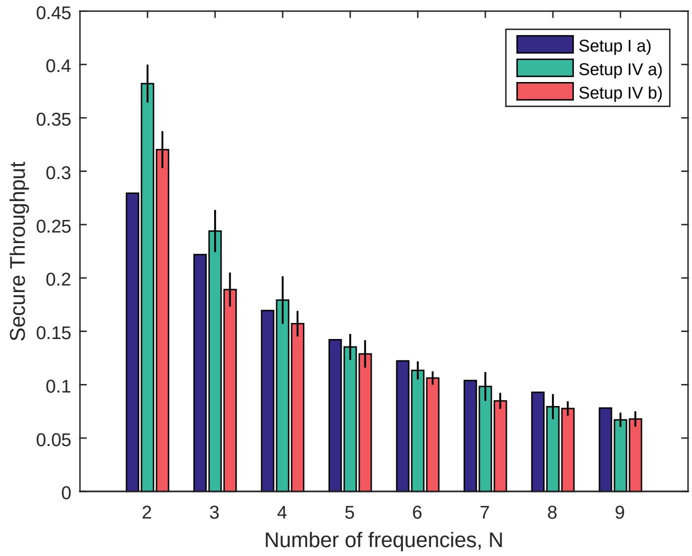


Figure 54.: *Setup IV - mean and confidence interval (standard error of the mean).*

Figure 54 plots the mean of the secure throughput (y-axis) and its confidence interval (95%) with varying number of available frequencies (x-axis) for settings, a), b) and compares them with the no-jamming setup (*Setup I-a*). This graph shows that directional jammers can improve secrecy levels, whether they are placed near or far from the receiver, if they are oriented away from this legitimate device and possibly targeting an attacker. In fact, most of the times, the difference between both settings is non-significant (the region delimited by the confidence line overlaps), and for a small number of channels, less than five, secure throughput is considerably higher than our no-jamming setup, even with only one eavesdropper and the jammer closer to the receiver.

These differences between the settings are due to the directionality of the noise which is propagated away from the receiver, significantly reducing its impact on this device.

We can envision the use of this jamming strategy to reduce the harmful effect of the jammer's noise on the legitimate channel, and perhaps create a jamming grid around the receiver to protect it from eavesdropping attacks that can come from multiple directions. For example, if we consider a factory building protected by a fence and using RFDI tags to track products, we can position a series of directional jammers near the fence pointing to the outside [51]. Thus, we reduce their harmful effect on the communication inside the factory floor and increase the secrecy level. However, this requires us to know some information about the possible location of the attackers and to actively build-up our defensive grid. On the other hand, omnidirectional jamming requires less concentrated effort since jammers can actually be other transmitting nodes already present in the network.

To conclude, results from our different setups, although limited by the small number of devices available, are coherent with our theoretical results and support our analytical findings.

6

CONCLUSION

We characterized the secure throughput (probability of secure communication) of a wireless system operating under Uncoordinated Frequency Hopping, a frequency hopping scheme in which devices hop uniformly at random between a set of frequencies. We considered the impact of narrowband and broadband eavesdropper adversaries that are capable of overhearing information in respectively one or multiple frequencies at a time, and narrowband and broadband friendly jammers that are available to combat those eavesdroppers by causing them interference.

We have seen that, in both scenarios it is possible to adapt the number of hopping frequencies to maximize the secure throughput and reduce the probability of eavesdropping. Therefore, by optimizing frequency hopping spread spectrum methodologies for secrecy, we expect to maximize the number of periods where the source and receiver land on the same frequency without the eavesdropper being able to listen to the information being transmitted. These periods may then be used to opportunistically exchange a key that can be used to protect subsequent communication (e.g. via exchanging a hopping pattern or key for the FH scheme or employing typical cryptographic mechanisms). We also unveiled the positive effect of friendly jammers on the secure throughput, in particular of broadband jammers that are capable of providing reasonable levels of secure throughput against a larger number of eavesdroppers in the system. The availability of broadband friendly jammers brings the additional benefit of allowing jammers to reduce the number of overlapping frequencies that may already be protected by other jammers, without the need for cooperation/synchronization between jammers.

We propose a new mathematical representation of the aforementioned UFH model plus jamming that takes into account the impact of path loss and features the degradation of legitimate communication by jammers. This aggregate interference model makes use of the signal-to-interference-plus-noise ratio concept and employs probabilistic methods, stochastic geometry, to position jammers and eavesdroppers randomly in space. Results showed that jamming coupled with UFH can provide secrecy gains when fending off multiple attackers. We have also seen that it is possible to adjust the number of frequencies to maximize the secure throughput whether or not we are using jamming. In fact, adapting the number of hopping frequencies while employing defensive jammers provides a way of reducing the negative impact their interference has on the legitimate channel. This extended characterization, thus, allowed us to better assess the secrecy level of our scheme, more closely mirroring a real life scenario.

Finally, we implemented a test-bed to validate and evaluate our theoretical results, comprising four different setups. We used software-defined radios and Gnuradio to build-up all of our different settings. Results support our previous analytical findings, showing that UFH and jamming are capable of providing a sufficient level of secure throughput to enable secret key exchange. We observed the beneficial impact that jamming has on legitimate communication when blend with UFH and when the system is under attack by multiple eavesdroppers. We tested different settings, with degraded and non-degraded eavesdroppers to ascertain the robustness of our scheme and included some other defensive strategies (e.g. jamming with directional antennas) that have proven advantageous.

6.1 Future Work

Future directions of this work include the extension our UFH security scheme so that we can account for the impact of other propagation effects (fading and shadowing), as well as, other types of jamming. More specifically, we want to ascertain the impact of having the receiver generate its own noise, being able to interfere with eavesdroppers while self cancelling its effect. Not only do we want to mathematically characterize such scheme, but we also want to test it using SDRs, something that has yet to be done in this field of study.

Appendices

A

PDF FOR RANDOM DISTANCES INSIDE A CIRCLE

Let (X, Y) be a random point in a circle C_R centered on (x_0, y_0) with radius R and pdf g. Let us also define $R_0 = \sqrt{(X - x_0)^2 (Y - y_0)^2}$ has the distance between (X, Y) and (x_0, y_0), and the cdf of R_0 as F.

$$\begin{aligned}
F_{R_0}(r_0) &= \mathbb{P}(R_0 \leq r_0), \forall_{r_0 \in \mathbb{R}} \\
&= \mathbb{P}(\sqrt{(X - x_0)^2 (Y - y_0)^2} \leq r_0) \\
&= \mathbb{P}((X, Y) \in C_{r_0}) \\
&= \iint_{C_{r_0}} g(x, y), \mathrm{d}x \, \mathrm{d}y \\
&\overset{1}{=} \frac{1}{\pi R^2} \iint_{C_{r_0}} \mathrm{d}x \, \mathrm{d}y \overset{2}{=} \frac{\pi r_0^2}{\pi R^2} \overset{3}{\Rightarrow} pdf(r_0) = \frac{2r_0}{R^2} \qquad (56)
\end{aligned}$$

[1] $(X, Y) \sim Uniform(C_R) \Rightarrow g(X, Y) = \begin{cases} (\pi R^2)^{-1} & \text{if } (x, y) \in C_R \\ 0 & \text{otherwise} \end{cases}$

[2] $\iint_{C_{r_0}} \mathrm{d}x \, \mathrm{d}y$: area of circle C_{r_0}

[3] $pdf(x) = \frac{\mathrm{d}F(x)}{\mathrm{d}x}$

BIBLIOGRAPHY

[1] M. Strasser, C. Pöpper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Symposium on Security and Privacy*, (Oakland, California, USA), pp. 64–78, 2008.

[2] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Cooperative jamming to improve the connectivity of the 1-d secrecy graph," in *45th Annual Conference on Information Sciences and Systems (CISS)*, (Baltimore, USA), pp. 1–6, March 2011.

[3] J. F. C. Kingman, *Poisson Processes*. Oxford University Press, 1993.

[4] M. Strasser, C. Pöpper, and S. Capkun, "Efficient uncoordinated fhss anti-jamming communication," in *MobiHoc '09 - 10th ACM International Symposium on Mobile ad hoc networking and computing*, (New Orleans, Louisiana, USA), pp. 207–218, 2009.

[5] 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, June 2008.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[8] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, January 1975.

[9] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network Magazine (accepted for publication)*, May 2014.

[10] X. He and A. Yener, "Secure degrees of freedom for gaussian channels with interference: Structured codes outperform gaussian signaling," in *IEEE Global Telecommunications Conference*, (Honolulu, Havai, USA), pp. 1–6, December 2009.

[11] P. C. Pinto, J. Barros, and M. Z. Win, "Physical layer security in stochastic wireless networks," in *IEEE International Conference on Communication Systems (ICCS)*, (Guangzhou, China), pp. 974–979, November 2008.

[12] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[13] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, October 2013.

[14] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proceedings IEEE INFOCOM*, (Shangai, China), pp. 1125–1133, April 2011.

[15] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proceedings IEEE INFOCOM*, (Orlando, Florida, USA), pp. 1152–1160, March 2012.

[16] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *IEEE International Conference on Communications (ICC)*, (Cape Town, South Africa), pp. 1–6, May 2010.

[17] P. C. Pinto and M. Z. Win, "A unified analysis of connectivity and throughput in packet radio networks," in *IEEE Military Communications Conference (MILCOM)*, (San Diego, California), pp. 1–7, November 2008.

[18] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based Jamming for Enhanced Wireless Secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, September 2011.

[19] J. S. Sousa and J. P. Vilela, "A characterization of uncoordinated frequency hopping for wireless secrecy," in *IEEE/IFIP Wireless and Mobile Networking Conference*, (Vilamoura, Portugal), May 2014.

[20] J. S. Sousa and J. P. Vilela, "Uncoordinated frequency hopping for secrecy with broadband jammers and eavesdroppers," in *IEEE ICC Conference Proceedings (accepted for publication)*, (London, UK), June 2015.

[21] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its application," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 205–230, February 2009.

[22] A. F. Molisch, *Wireless Communications, 2nd Edition*. A John Wiley and Sons Ltd., United Kingdom, 2011.

[23] M. Gast, *Wireless Networks: The Definitive Guide*. O'Reilly, United Kingdom, 2002.

[24] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. A. Spielman, and V. Stemann, "Pratical loss-resilient codes," in *29th annual ACM Symposium on Theory of computing (STOC)*, (New York, USA), pp. 150–159, 1997.

[25] S. G. Wilson, *Digital Modulation and Coding*. Prentice-Hall, 1996.

[26] C. Pöpper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, June 2010.

[27] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 297–309, February 2012.

[28] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[29] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 1996.

[30] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[31] F. Baccelli and B. Blaszczyszyn, *Stochastic Geometry and Wireless Networks*. INRIA & Ecole Normale Supérieure, 2005.

[32] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*. John Wiley & Sons, 1985.

[33] M. Franceschetti and R. Meester, *Random Networks for Communication*. Cambridge University Press, 2007.

[34] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1–24, January 2014.

[35] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, September 2013.

[36] I. Csiszar, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 48–57, January 1996.

[37] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology - EUROCRYPT 2000*, (Bruges, Belgium), pp. 351–368, May 2000.

[38] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no 4., pp. 451–456, July 1978.

[39] M. Bloch, J. Barros, M. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[40] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2011, October 2013.

[41] A. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, December 2003.

[42] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wiretap channel," in *Proc. IEEE International Symposium on Information Theory*, (Nice, France), pp. 2471–2475, June 2007.

[43] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the mimo wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, (Pacific Grove, California, USA), pp. 2809–2812, 2012.

[44] A. Mukherjee and A. L. Swindlehurst, “A full-duplex active eavesdropper in mimo wiretap channels,” in *Conference on Signals, Systems and Computers (ASILOMAR)*, (Pacific Grove, California, USA), pp. 265–269, November 2011.

[45] F. Renna, N. Laurenti, and H. V. Poor, “Physical layer secrecy for ofdm transmissions over fading channels,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, August 2012.

[46] P. C. Pinto, J. Barros, and M. Z. Win, “Techniques for enhanced physical-layer security,” in *IEEE Global Telecommunications Conference (GLOBECOM)*, (Miami, Florida, USA), pp. 1–5, December 2010.

[47] P. C. Pinto, J. Barros, and M. Z. Win, “Wireless physical-layer security: The case of colluding eavesdroppers,” in *IEEE International Symposium on Information Theory*, (Seoul, South Corea), pp. 2442–2446, July 2009.

[48] J. Xie and S. Ulukus, “Real interference aligment for k-user gaussian interference compound wiretap channel,” in *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, (Allerton, Iowa, United States), pp. 1252–1257, October 2010.

[49] R. A. Poisel, *Modern communications jamming principles and techniques*. Artech House, 2006.

[50] M. Acharya and D. J. Thuente, “Intelligent jamming in 802.11b wireless networks,” in *OPNETWORK Conference*, (Washington DC, USA), 2004.

[51] S. Sankararaman, K. Abu-Affash, and A. Efrat, “Optimization schemes for protective jamming,” in *Proceedings of the 13th ACM international Symposium on Mobile Ad Hoc Networking and Computing*, (Hilton Head, South Carolina, USA), pp. 65–74, 2012.

[52] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, “Wireless secrecy regions with friendly jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[53] N. O. Tippenhauer, L. Malisa, and S. Capkun, “On limitations of friendly jamming for confidentiality,” in *IEEE Symposium on Security and Privacy (SP)*, (Berkeley, California, USA), pp. 160–173, May 2013.

[54] J. Mitola, “Software radios: Survey, critical evaluation and future directions,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 8, no. 4, pp. 25–36, April 1993.

[55] J. Huovinen, T. Vanninen, and J. Iinatti, “Demonstration of synchronization method for frequency hopping ad hoc network,” in *IEEE Military Communications Conference, (MILCOM)*, (San Diego, USA), pp. 1–7, 2008.

[56] P. E. Atlamazoglou and N. K. Uzunoglu, “A passive synchronization method for frequency hopping systems,” *Journal of Applied Mathematics & Bioinformatics*, vol. 3, no. 1, pp. 151–161, March 2013.

[57] P. C. Pinto, J. Barros, and M. Z. Win, "Techniques for Enhanced Physical-Layer Security," in *IEEE Global Telecommunications Conference (GLOBECOM)*, (Miami, Florida, USA), pp. 1–5, December 2010.

[58] F. Quitin, M. M. U. Rahman, R. Mudumbai, and U. Madhow, "A scalable architecture for distributed transmit beamforming with commodity radios: Design and proof of concept," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1418–1428, 2013.

[59] J. P. Nolan, *Stable Distributions - Models for Heavy Tailed Data*. Boston, USA: Birkhauser, 2015.

[60] G. Samorodnistsky and M. Taqqu, *Stable Non Gaussian Processes - Stochastic Models with Infinite Variance*. London, UK: Chapman & HallCRC, 1994.

[61] D. Moore and G. McCabe, *Introduction to the practice of statistics*. Freeman, 4th edition, 2003.

[62] D. C. Montgomery, *Design and analysis of experiments*. Wiley, 7th edition, 2008.

[63] A. Field and G. Hole, *How to design and report experiments*. SAGE, 2003.

[64] S. S. Shapiro and M. B. Wilk, "An analysis of variance test for normality (complete samples)," *Biometrika 52*, vol. 3, no. 4, p. 591–611, 1965.