Improving Security for Future Wireless Networks Through Friendly Jamming

by

Mark. M. Adams

B. Eng., Royal Military College of Canada, 2015

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

May 2017

Abstract

As the number of connected devices and the importance of mobile communications continue to increase, a greater emphasis must be placed on security. Due to the broadcast nature of wireless communications, wireless networks are very exposed to eavesdropping. While this can be addressed above the physical layers using encryption, this still allows the attacker to receive the message and future work may allow decryption. Physical layer security is an approach to security which exploits the wireless channel to prevent the attacker from decoding the message. This thesis examines the use of friendly jamming, in which some nodes in a network broadcast white noise in order to degrade the channel between the legitimate transmitter and the eavesdropper. We address two problems related to the use of friendly jamming to improve physical layer security.

The first problem is routing a signal through a network while using the remaining nodes as jammers to secure the signal. This is solved as two convex problems of allocating power to the jammers and routing the signal using those jammers to secure the transmission. This is shown to be a feasible method to increase security in a network.

The second problem is estimating the self-interference channel (SIC) without using a calibration period for full-duplex jamming receivers. As the transmitter cannot transmit while the receiver estimates its SIC using a half duplex pilot signal, eliminating the calibration period can represent a significant capacity gain. Estimating the channel while receiving the desired signal causes it to act as an additional noise source, but this is shown to be overcome through the use of long estimation times. Our proposed scheme is able to increase the secrecy capacity of the system over that of calibration based estimation.

Lay Summary

As wireless devices broadcast a signal which can be received by any nearby devices, wireless networks are very exposed to eavesdropping. Physical layer security exploits the wireless channel to prevent the attacker from decoding the message. This thesis examines the use of friendly jamming, in which some nodes in a network act to impair the eavesdropper's ability to receive a message. We address two problems related to the use of friendly jamming to improve physical layer security. The first problem is routing a signal through a network while using the remaining nodes as jammers to secure the signal. This is shown to be a feasible method to increase security in a network. The second problem is estimating the self-interference channel (SIC) without using a calibration period for full-duplex jamming receivers. Our proposed scheme is able to increase the secrecy capacity of the system over that of calibration based estimation.

Preface

The following publications have resulted from the research presented in this thesis:

- M. Adams and V. K. Bhargava, "Using Friendly Jamming to Improve Route Security and Quality in Ad Hoc Networks," *2017 Canadian Conference on Electrical and Computer Engineering (CCECE)*, Windsor, ON, 2017, pp. 442-447 (Linked to Chapter 2)
- M. Adams and V. K. Bhargava, "Use of the Recursive Least Squares Filter for Online Self Interference Channel Estimation," *2016 IEEE Vehicular Technology Conf. (VTC)*, Montreal, QC, 2016, pp. 1-4. (Linked to Chapter 3)

Statement of Authorship

I am the primary author for both the publications listed above. I have been responsible to develop original ideas, derive mathematical solutions, and generate simulation results for these publications. Prof. Vijay K. Bhargava, who is my research supervisor, provided valuable guidance and directions in identifying the research problems, developing solution methodologies, and documenting the results. Some of the simulation results were obtained using the disciplined convex optimization software CVX developed by Grant, Boyd & Ye [1].

Table of Contents

List of Tables

List of Figures

Mathematical Notations

We represent matrices using boldface capital letters (e.g. $\mathbf{A}$), vectors using boldface small letters (e.g. $\mathbf{a}$), and scalars using small letters (e.g. a). The transpose of a matrix $\mathbf{A}$ is represented as $\mathbf{A}^T$. The Hermitian transpose of a matrix $\mathbf{A}$ is represented as $\mathbf{A}^H$. An $M \times M$ identity matrix is represented as $\mathbf{I}_M$ and sometimes I when the dimensions are clear from the context. If $\mathbf{a}$ is a circularly-symmetric complex Gaussian vector with mean μ and covariance matrix Π, we represent its probability distribution as $\mathbf{a} \sim \mathcal{CN}(\mu, \Pi)$. A function f in variables (x, y, z) is represented as $f(x, y, z)$. When the variables (y, z) in f are assigned with values (y_0, z_0), the resulting function is represented as $f(x; y_0, z_0)$. $\mathbb{E}\{.\}$ denotes expectation with respect to the random variable under context. The covariance of a vector $\mathbf{a}$ is represented by $\text{cov}(.)$ and the variance by $\text{var}(.)$. $|\mathbf{A}|$ and $||\mathbf{A}||$ respectively denote the determinant and the vector 2-norm of the square matrix $\mathbf{A}$.

List of Abbreviations

5G	:	Fifth Generation
ADC	:	Analog to Digital Converters
BS	:	Base Station
COP	:	Connection Outage Probability
CSI	:	Channel State Information
FDD	:	Frequency Division Duplexing
i.i.d	:	independent and identically distributed
LTE	:	Long Term Evolution
Mbps	:	Mega bits per second
MIMO	:	Multiple-input Multiple-output
ML	:	Maximum Likelihood
MMSE	:	Minimum Mean Squared Error
QoS	:	Quality of Service
RLS	:	Recursive Lease Squares
SIC	:	Self Interference Cancellation
SINR	:	Signal to Interference plus Noise Ratio
SIR	:	Signal to Interference Ratio
SOP	:	Secrecy Outage Probability
SNR	:	Signal to Noise Ratio
TDD	:	Time Division Duplexing

Acknowledgements

Firstly, I would like to thank my supervisor Professor Vijay K. Bhargava for his patience, knowledge, and generous financial support. I thank him for providing me with an excellent research atmosphere in his lab. This thesis would not have been possible without his support, guidance, and encouragement.

Secondly, I am very fortunate and grateful to have excellent colleagues at the Information Theory and Systems laboratory, who offered me genuine and friendly support to carry out my research. I particularly thank Dr. Shankanaad Mallick for his discussions, feedback and critical suggestions. I would also like to thank Surya Vara Prasad, Buddhika Nettasinghe, and Sudha Lohani for their friendship and support during my MASc research. I am also thankful to them for proofreading my thesis.

Dedication

To my friends and family

for all their help and support over the past years

Chapter 1

Introduction

1.1 Motivation

Current cellular networks are supporting billions of communication devices, and that number is only expected to increase in the coming years. With the increased use of applications such as mobile video and the internet of things, there will be greater importance placed on spectral efficiency in order to provide more services to more devices without requiring the expensive investment of increased bandwidth. The increased use of mobile devices also creates calls for increased security. With more information being available over wireless communications from the extra connectivity of IoT and the shift to conduct more business and banking on phones, it becomes an increasingly attractive target for malicious eavesdroppers. Securing against attackers will be increasingly important to effective development of wireless networks.

Due to the broadcast nature of wireless communications, wireless networks expose themselves to eavesdropping attacks. Traditionally, this is addressed through public key cryptography as proposed in [3] such as RSA or AES. While these are currently effective at stopping the attacker from reading the plain text message, they still allow the attacker to receive the message and future work could allow decryption. Another approach to security is physical layer security, in which the wireless medium is exploited in order to prevent the attacker from receiving enough information to decode the message [4].

In general, a transmitter and receiver are guaranteed secret communications if their channel is instantaneously better than the eavesdroppers channel. Due to fading, this means that in almost all scenarios some degree of secrecy can be achieved. The most common metrics for evaluating physical security are the ergodic secrecy capacity, which is analogous to channel capacity and the secrecy outage probability, which is the probability that the instantaneous secrecy capacity is below a fixed rate.

A problem with physical layer security in typical systems is that connection outage probability is a decreasing function of power, and secrecy outage probability is increasing. This often leads to a direct trade off where neither the security performance nor the service quality of a system is satisfactory. An approach to address this is friendly jamming. In friendly jamming, some nodes in a network will act as jammers, and broadcast noise to increase the interference at any eavesdroppers [5] [6]. This improves the secrecy outage probability of each link without raising the connection outage probability.

1.2 Objectives

The objective of this is thesis is to address two problems related to friendly jamming for physical layer security. In chapter 2 we examine the problem of routing a signal through a network, using friendly jamming to secure its transmission and a routing metric designed to maximize the probability that the route is both connected and secure. While similar work has been done for routing without friendly jamming [7][8], and for a jamming power allocation on a fixed route[9], the combination of routing and jamming is novel. In chapter 3, we examine the problem of self-interference channel cancellation for full-duplex jamming receivers. We propose the use of online estimation in the presence of the desired signal for self-interference channel (SIC) cancellation in jamming receivers. While these techniques have been studied for bidirectional communications and provide a modest gain [2], they can provide a more significant performance improvement in a security context as information cannot be transmitted during a half duplex calibration period. Full-duplex jamming receivers are proposed in [10] under the assumption of a fixed level of self-interference cancellation. [11] considers the effect of the SIC estimate, but does the channel estimate in a period of unsecured half duplex operation. We demonstrate improved system secrecy capacity through estimating the channel without the use of a half duplex calibration period. The remainder of this chapter provides background on physical layer security and challenges with self-interference cancellation for full-duplex communications.

1.3 Introduction to Physical Layer Security

Privacy and security are an increasing area of concern as growth in wireless networks continue and growing proportions of communications are carried out over wireless. In traditional approaches to security, all security concerns are approached from above the physical layer using cryptography with the physical layer providing only the link. Physical layer security instead approaches security as a link level concern, exploiting the randomness of the channel to provide security to the transmissions.

The theoretical basis for physical layer security is the information-theoretic approach of perfect secrecy, originally conceived by Shannon and improved by Wyner [12] [13]. Their papers created the field, proving that their exist coding techniques which can grant robustness to error as well as security in the wiretap channel. The downside of this original approach is that it required the legitimate channel to have a strictly better channel than the eavesdropper in order to guarantee a positive secrecy capacity. However, recent improvements have demonstrated that with fading present in the system, positive secrecy rates can be achieved even if the eavesdropper has a better channel than the legitimate receiver [14], without either the need for a feedback channel or sharing a secret between the transmitter and the receiver. However, even this approach suffers from the fact that practical codes for fading channels have not yet been achieved, and so the associated capacities are only theoretical and do not reflect the reality of the channel security.

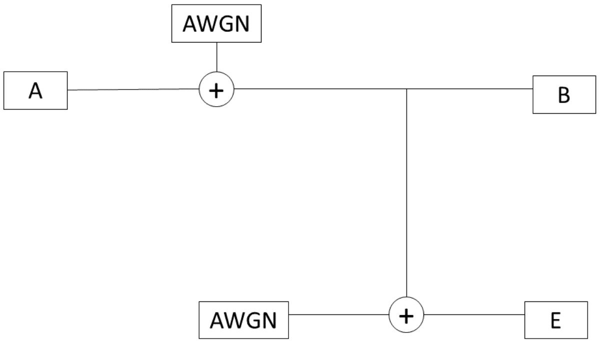

Figure 1.1: The Wiretap Channel model

1.3.1 The Wiretap Channel

The original consideration for physical layer security, and the foundation for most research is the Gaussian wiretap channel shown in Fig. 1.1.

This channel models the Alice Bob channel as an AWGN channel with noise power σ_1^2, with an additional AWGN source of noise power σ_2^2 between Alice and Eve. Alice (A) transmits at power P and Eve (E) and Bob (B) then receive the same transmission through different channels. The secure capacity of this channel is the difference in the capacity of the Alice-Bob channel and the Alice-Eve channel, as shown in [15].

$$\begin{aligned} C_{AB} &= \tfrac{1}{2}\log(1+\tfrac{P}{\sigma_1^2}) \\ C_{AE} &= \tfrac{1}{2}\log(1+\tfrac{P}{(\sigma_1^2+\sigma_2^2)}) \\ C_s &= C_{AB} - C_{AE} \end{aligned} \tag{1.1}$$

Note that this capacity is always positive in this model because the wiretap channel is a degraded copy of the main channel.

Another model to consider is the Rayleigh fading wiretap channel shown in Fig. 1.2. We assume that the main channel CSI is known to Alice and the eavesdropper channel CSI is known to Eve. Additionally, in order to achieve the secrecy capacity in (1.7) we must assume

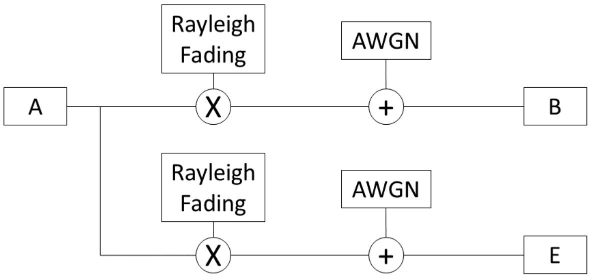

Figure 1.2: The Rayleigh Fading Wiretap Channel model

that Alice has statistical knowledge of Eve's CSI. This is a reasonable assumption for the case where Eve is another user in the network. With these assumptions, there is always some positive average capacity, even when the average SNR of the main channel is worse than the eavesdropper channel. This demonstrates the possibility of exploiting fading in order to secure communications, as shown in [14]. Alice transmits at power P. The fading coefficients of the Alice Bob and Alice Eve channel are given by H_b and H_e respectively, and their noise powers are N_b and N_e. Their corresponding channel gains are $G_b = |H_b|^2$ and $G_e = |H_e|^2$. Their instantaneous SNRs are given by

$$\begin{aligned} \gamma_b(i) &= \tfrac{PG_b(i)}{N_b} \\ \gamma_e(i) &= \tfrac{PG_e(i)}{N_e}. \end{aligned} \tag{1.2}$$

and their average values are

$$\begin{aligned} \bar{\gamma}_b(i) &= \tfrac{PE[G_b]}{N_b} \\ \bar{\gamma}_e(i) &= \tfrac{PE[G_e]}{N_e.} \end{aligned} \tag{1.3}$$

The secrecy capacity for a channel realization i is given as

$$C_s(\gamma_b, \gamma_e) = \begin{cases} \log(1+\gamma_b(i)) - \log(1+\gamma_e(i)) & \text{if } \gamma_b(i) > \gamma_e(i) \\ 0 & \text{otherwise.} \end{cases} \tag{1.4}$$

The average secrecy capacity is the integral of all possible combinations of γ_b and γ_e weighted by their probabilities of occurring

$$\bar{C_s} = \int_0^\infty \int_0^\infty C_s(\gamma_b, \gamma_e) p(\gamma_b) p(\gamma_e) d\gamma_b d\gamma_e. \tag{1.5}$$

Γ_b and Γ_e vary with $|H_b|^2$ and $|H_e|^2$, they follow exponential distributions

$$\begin{aligned} pr(\gamma_b) &= \tfrac{1}{\bar{\gamma_b}} e^{-\frac{\gamma_b}{\bar{\gamma_b}}} \\ pr(\gamma_e) &= \tfrac{1}{\bar{\gamma_e}} e^{-\frac{\gamma_e}{\bar{\gamma_e}}} \end{aligned} . \tag{1.6}$$

Therefore, (1.5) can be shown to be

$$\bar{C_s} = F(\bar{\gamma_b}) - F(\frac{\bar{\gamma_b}\bar{\gamma_e}}{\bar{\gamma_b} + \bar{\gamma_e}}) \tag{1.7}$$

where

$$F(x) = \int_0^\infty \log_2(1+u) \frac{1}{x} e^{\frac{-u}{x}} du.$$

This capacity is applicable in the case that Alice has full knowledge of the main channel CSI and statistical knowledge of the eavesdropper channel CSI. This is realistic for scenarios where Eve is an active wireless user, and Alice can estimate the channel while Eve transmits. The key difference between the Rayleigh and AWGN channel models is that the Rayleigh channel allows for a positive secrecy capacity even when the average channel quality of the

Alice Bob channel is lower than the Alice Eve channel. This allows secure communication by communicating only when there is an instantaneous positive secrecy capacity.

1.3.2 Secrecy Outage Probability

The secrecy performance of physical layer security schemes can also be evaluated using secrecy outage probability. Secrecy outage probability is used in two different ways, as it can refer to either the probability that the secrecy capacity falls below a certain threshold, or as the probability that there is a leakage of information to the eavesdropper while transmitting at a fixed rate. The first corresponds to the scenario where the transmitter is using a secrecy coding, and the latter corresponds to the situation where it is not. First we will consider the probability that the secrecy capacity falls below a threshold τ.

$$\begin{aligned} Pr(C_s < \tau) &= Pr(log(\tfrac{1+\Gamma_b}{1+\Gamma_e}) < \tau) \\ &= Pr(\Gamma_b > 2^{\tau}(1+\Gamma_e) - 1) \\ &= \textstyle\int_0^{\infty} Pr(\gamma_e)(\int_{2^{\tau}(1+\gamma_e)-1}^{\infty} Pr(\gamma_b)d\gamma_b)d\gamma_e \\ &= \tfrac{\bar{\gamma_b}}{\bar{\gamma_b}+\bar{\gamma_e}2^{\tau}} e^{-\frac{2^{\tau}-1}{\bar{\gamma_b}}} \end{aligned} \tag{1.8}$$

in the case where τ is 0, this is just

$$P(C_s < 0) = \frac{\bar{\gamma_b}}{\bar{\gamma_b} + \bar{\gamma_e}}. \tag{1.9}$$

This outage probability represents the probability that the channel fading realization can not support any rate of secure communication. This outage probability is applicable to the case where Alice has knowledge of Alice Bob and Alice Eve channels, and is using an appropriate variable coding to avoid leaking information. Therefore, this outage probability represents a stoppage of communication rather than a security leak. An alternative approach to secrecy outage probability is to consider the outage probability for the case of a fixed rate secrecy coding. In this case the SOP is represented by the probability that Eves received

SNR is greater than the threshold to decode the message.

$$\begin{aligned} SOP &= \Pr(\gamma_e > \gamma_{th}) \\ SOP_l &= e^{\frac{-\gamma_e}{\overline{\gamma_e}}} \end{aligned} \tag{1.10}$$

This is appropriate to the case with no knowledge of the Alice Bob or Alice Eve channel. In this scenario, Alice can do no better than setting her transmission rate to a constant level, and the secrecy outage probability represents the probability that Eves channel can decode information sent at that rate.

1.3.3 Friendly Jamming

Friendly jamming is a method used to degrade the quality of the eavesdropper's link in order to improve the physical secrecy performance. An FJ signal is essentially randomly generated noise broadcast from the jammers to the eavesdroppers. Either multiple antennas or multiple transmitters can be used to nullify the FJ signal at the legitimate receiver to avoid lowering the quality of the legitimate link. Friendly jamming can be done on many different scales. In multi hop communications, possible applications are choosing optimal positioning for jamming nodes, or optimal routes using jamming receivers. Chapter 2 examines the problem of routing a signal through a network using friendly jamming to secure the transmissions. In point to point communications, a full-duplex jamming receiver can be used to broadcast noise at the eavesdropper, while using self cancellation methods to avoid jamming itself [10]. Chapter 3 presents the use of online self-interference cancellation to provide a performance increase over calibration based estimation for full-duplex jamming receivers. The next section provides background on full-duplex communications.

1.4 Physical Layer Challenges for Full Duplex Communication

In-Band Full Duplex channel use has traditionally been considered impossible for communications due to the strong self-interference between the transmitted and received signals, and so radios have traditionally operated in half duplex or out of band full-duplex. However, recent research has been showing that with advances in self-interference cancellation technologies, IBFD communication can be achieved, and can offer many advantages to communication networks. In physical layer security, it is a key enabling technology for friendly jamming, as it will allow receivers to simultaneously jam any eavesdroppers. For device to device communication, or direct base station to user communication, IBFD has the potential to double the bidirectional data rate. When used for relaying, IBFD will be able to increase spectral efficiency to match that of the half duplex direct communication case.

The primary challenge involved with implementing IBFD stems from the self-interference in the terminal, as the receiver will receive both the signal of interest and the signal that it is transmitting. In [16] a conservative real world scenario with small cell base stations and mobile handsets was considered, and it was found that the self-interference must be suppressed by 106 dB to meet the SNR in a half-duplex link. Broadly speaking, this interference occurs in three domains: wireless propagation techniques, analog circuit techniques, and digital domain techniques.

Propagation layer suppression aims to eliminate the transmitted signal from impinging on the receive antennas. The methods to achieve this cancellation depend on the number of antennas in the system. If a single antenna is used for both transmission and reception, then a duplexer will be the only propagation layer SIC suppressor. While this is used effectively in applications such as continuous wave radar, and has been demonstrated to be usable in communications, it offers little to no performance benefits over multi-antenna systems [17]. The alternative is to use a separate transmit and receive antenna, and separate them through physical techniques such as polarization, distance, and shielding, or digital ones such as beam-forming. The disadvantage to this technique is that achieving high amounts of physical isolation will often suppress the transmitted signal by either directly requiring a lowered effective gain or through limiting the degrees of freedom in adaptive beam-forming [18]. Additionally, a large amount of space is required to achieve a significant amount of physical isolation, and so IBFD has yet to be achieved in small form factor devices [16] [19]. However, relay nodes are a great opportunity to employ full-duplex for the spectral efficiency gain. As they are part of the network infrastructure, size is much less of a concern as in user devices, so physical isolation will be much more attainable.

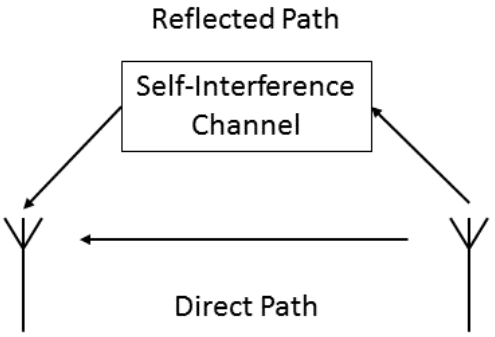

Figure 1.3: Direct and reflected self-interference paths

While physical domain self-interference cancellation can be effective, it is unable to eliminate the signal entirely. In order to achieve better isolation, it is typical to employ an analog interference cancellation circuit. Analog domain cancellation techniques function through taking a tapped copy of the transmitted signal, adjusting its phase, gain and delay as necessary, and subtracting it from the received signal. Single tap equalizers are typically used, which allows the receiver to account for the direct path interference, but is generally unable to handle environmental effects such as nearby reflectors as shown in Fig. 1.3. It is also possible to deal with reflections through the use of adaptive analog circuits, but this will increase the circuit complexity and require analog domain signal processing. In order to deal with the indirect SIC, it is most common to use digital domain cancellation techniques, through learning and exploiting the channel state information [16],[17].

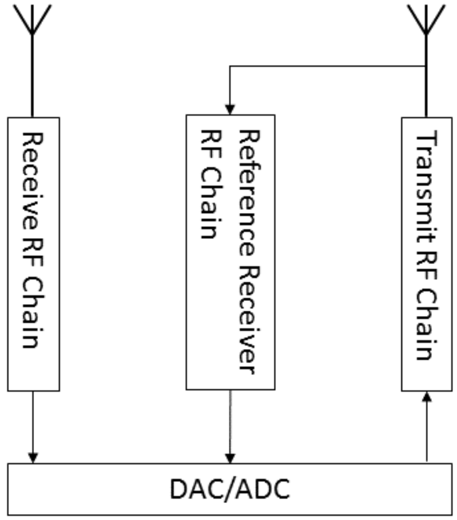

Figure 1.4: Self-interference cancellation with a reference receiver

Digital domain self-interference channel works through taking an estimate of the self-interference channel, filtering the transmitted signal through the estimated channel, and subtracting the result from the received signal. In general this is effective for reflections and other linear interference, but it cannot account for interference resulting from non-linearities in the transmit chain. In order to account for this, one option is to use a reference chain based canceler, where a tap of the transmitted signal is passed through a reference receiver, in order to capture non-linearities caused by power amplifiers, as shown in Fig. 1.4. Estimation can be done in several different ways. Traditionally, it is accomplished through the use of pilot signals in short periods of half duplex operation. While this is effective for channel cancellation, it lowers the total throughput of the system, particularly for low channel coherence times where the channel must be estimated frequently. An option which is currently being examined is estimating the channel during full-duplex operation. While the estimate length must be much longer, it is possible to achieve the same level of SIC cancellation as the pilot signals case without requiring periods of half duplex operation, increasing the total throughput [17].

While self-interference cancellation can work to dramatically lower the level of self-interference that is present in the transceiver, it is unable to eliminate it entirely [17]. This means that in practice, the efficiency gain of two is an upper bound, with real world communication links often operating far below that. In channels with poor self-interference cancellation communication in half duplex operation can actually be faster than full-duplex. When considering this effect, systems which can dynamically switch between half and full-duplex communication under different channel conditions will be faster over a long term average than those which operate only in full-duplex [2].

1.4.1 Related Research in Self Interference Cancellation

There is a significant amount of ongoing research for physical layer IBFD communication. The primary physical domain self-interference cancellation research focus is improving the analog SIC for small form factor devices. In [20], electrical balance duplexers which can be implemented on a chip are examined as a possibility to produce a duplexer which is effective enough for use in communications. Active analog RF cancellation circuits operating in frequency bins instead of delay taps are examined in [21] as a way to improve cancellation performance to compensate for the loss of separation between antennas.

Digital domain self-interference cancellation is also seeing a large amount of ongoing research. One of the primary research focuses is improving the bandwidth efficiency of the channel estimate. As the channel estimate accuracy is essential to the performance of IBFD, and there is a trade off between spending time estimating the channel versus constantly transmitting, improving the efficiency of the estimate can have significant performance improvements. In [22], an efficient expectation maximization estimator is proposed that can estimate the channel with less bandwidth costs than least squares estimates, at the cost of phase ambiguity. A set of constraints are also proposed under which the phase ambiguity can be resolved.

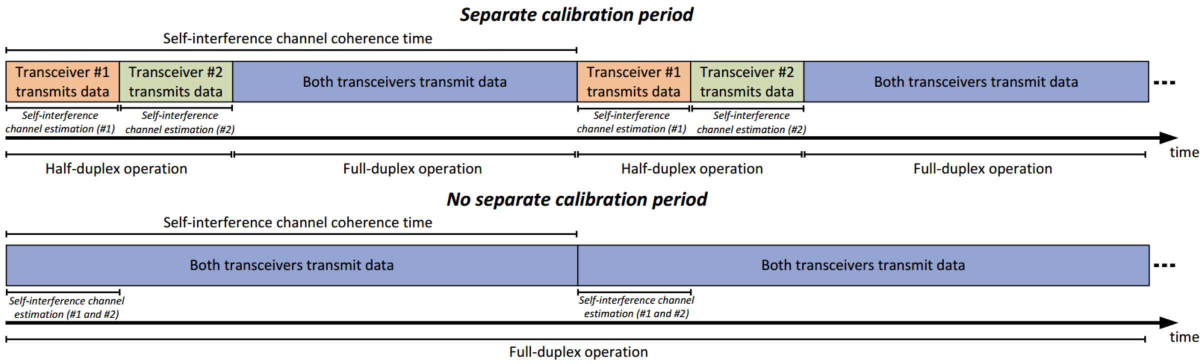
Separate calibration period
Self-interference channel coherence time
Transceiver #1 transmits data
Transceiver #2 transmits data
Both transceivers transmit data
Transceiver #1 transmits data
Transceiver #2 transmits data
Both transceivers transmit data
...
Self-interference channel estimation (#1)
Self-interference channel estimation (#2)
Self-interference channel estimation (#1)
Self-interference channel estimation (#2)
time
Half-duplex operation
Full-duplex operation
Half-duplex operation
Full-duplex operation
No separate calibration period
Self-interference channel coherence time
Both transceivers transmit data
Both transceivers transmit data
...
Self-interference channel estimation (#1 and #2)
Self-interference channel estimation (#1 and #2)
time
Full-duplex operation

Figure 1.5: Estimating the channel without a calibration period allows the system to operate more efficiently [2]

A second area of channel estimation is estimating the channel in the presence of the desired signal rather than during a half duplex calibration period. Such a method is proposed in [2], in which the estimate is carried out using least squares estimation during full-duplex communication. This scheme is illustrated in Fig. 1.5 They demonstrate that by using very long estimates the achievable SNR is in the same range as estimating during a short calibration period. This presents modest improvements when full-duplex is used for communications, as useful information is still transmitted during the calibration period. When full-duplex is instead used for jamming receivers, the gains are much more significant as the information sent during the calibration period is a noise signal which does not send any information. [10] examines the use of full-duplex receivers as jammers, but does not consider the use of online estimation for the self-interference cancellation. In chapter 3, we examine the use of online estimates for full-duplex jamming receivers rather than calibration periods, and demonstrate a significant performance gain.

1.5 Outline

In chapter 2 we address a problem in routing a signal through a network with friendly jamming. While friendly jamming in a network context and secrecy aware routing have both been studied, there is a lack of work which combines the routing and jamming. The problem is framed as a convex optimization problem, and simulated on random networks to analyze the performance. It is shown to be an effective measure to increase security in a network.

In chapter 3 we examine the use of self-interference channel estimation under the presence of the desired signal in the context of friendly jamming. SI channel estimation while concurrently receiving the desired signal has been studied in a full-duplex communication context, but has not been analyzed for the application of full-duplex jamming receivers. Unlike in previous works, this means that the SI estimation pilot signal is not transmitting useful information, so the potential performance gains by eliminating the pilot signals are greater for jamming receivers than for traditional applications.

Chapter 2

Routing and Jamming Power Allocation

In this chapter, we examine the problem of wireless routing with friendly jamming, using connection outage probability and secrecy outage probability as performance metrics. While the physical security is extensively studied for single links and single relay scenarios, only a few papers have considered physical layer security in multi link networks. The authors in [8] look at the problem of secure routing under a secrecy outage probability (SOP) constraint. They find the route that minimizes the use of network resources while meeting the SOP constraint. This is the simplest way to apply physical secrecy as it can be added as an additional constraint in current routing methods. In [7], the authors look at the problem of jointly minimizing the SOP and connection outage probability over the route. They use a flexible route metric that can trade off between SOP and connection outage probability (COP) based on the security needs of the user. The impact of friendly jamming is studied in [9] and [23] which consider placing jammers into a network. Through careful selection of the friendly jamming locations, they can jam the eavesdroppers while having a null at legitimate receivers, significantly increasing the capacity of the route. In [9] the authors study the problem of determining the most power efficient use of friendly jamming to meet a set secrecy constraint. In [24] the authors look at selecting jammers to increase the secrecy capacity along a given route, but do not examine how to select the route. In [25], the authors derive an optimal selection policy for both relays and jammers in a single hop relay network. The considered routing problem in [26] is similar to the one we consider in this chapter, however the authors did not use of friendly jamming to improve the security performance. We examine the problem of finding the best route through a wireless network under friendly jamming, jointly using SOP and COP as the route metric with friendly jamming to secure the transmissions.

2.1 System Model and Problem Formulation

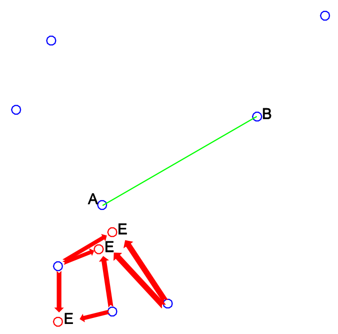

Figure 2.1: Unused nodes will be used to jam the eavesdroppers in each hop

The considered system consists of N nodes and E eavesdroppers (Eves) uniformly distributed over an area. At each message hop, the transmitter Alice will send the message to receiver Bob while the remaining nodes transmit noise to jam all Eves. The jamming nodes will act as a distributed multi-input multi-output system in order to maximize their jamming of the eavesdroppers while ensuring that they do not also jam the legitimate receiver. This system is illustrated in Fig. 2.1 with A as the transmitter, B as the receiver, and other nodes acting as jammers. The legitimate nodes are assumed to know the location of the eavesdroppers. This is applicable to the scenario where eavesdroppers and nodes are members of the same network, and the concern is data confidentiality between users. The system is considered to be under Rayleigh fading conditions, with the system limited by Signal to Interference and Noise ratios (SINR).

2.1.1 Link Secrecy Outage Probability

In this section, we derive the probability of a secrecy outage on the link l. The secrecy outage probability of a single link is the probability that one of the eavesdroppers will have a SINR above a threshold to decode the message.

$$SOP_l = \Pr(\max_e(\gamma_e) > \gamma_{th}) \tag{2.1}$$

$$\gamma_e = \frac{g_{le} f_{le} p_l}{N_0 + \sum\limits_{j \in J} g_{je} f_{je} p_j} \tag{2.2}$$

This is shown in (2.1) and (2.2), where g_{le} and f_{le} are the path loss and Rayleigh fading coefficient between the transmitter of link l and the eavesdropper e respectively, p_l is the link transmit power, and g_{je}, f_{je}, p_j representing the same for each jammer j in the set of all possible jammers J. In this representation, all nodes not part of the current link are being used to secure the transmission of the message, increasing message security at the cost of lowering network throughput. The eavesdroppers SINR can be safely assumed to be interference limited, so ignoring N_0 in the SINR (2.2), (2.1) can be rewritten as

$$SOP_l = \Pr(\max_e(\frac{g_{le} f_{le} p_l}{\sum\limits_{j \in J} g_j f_j p_j}) > \gamma_{th}) \tag{2.3}$$

The probability of a secrecy outage between link l and eavesdropper e in Rayleigh fading conditions is expressed in analytical form as shown in [27] as

$$SOP_{le} = \prod_{j \in J} \frac{1}{1 + \frac{\gamma_{th} g_{je} p_j}{g_{le} p_l}} \tag{2.4}$$

The link will have an outage if any of the eavesdroppers gets a signal. The probability of a secrecy outage on the link is then

$$SOP_l = 1 - \prod_{e \in E}(1 - \prod_{j \in J} \frac{1}{1 + \frac{\gamma_{th} g_{je} p_j}{g_{le} p_l}}) \tag{2.5}$$

Optimizing the link transmit power p_l is outside the scope of this analysis and so it is held as a fixed constant. Optimal jamming power p_j is determined in subsection 2.1.3. (2.5) can then be used to compute the SOP for all links prior to routing.

2.1.2 Route Secrecy Outage Probability

The route r will have a secrecy outage if any link in it has a secrecy outage. This is equivalent to the probability that the maximum eavesdropper γ_{le} between the link and any eavesdropper in the route is greater than than the security threshold γ_{th}

$$SOP_r = \Pr(\max_{l \in r}[\max_{e \in E}(\gamma_{le})] > \gamma_{th}) \tag{2.6}$$

or equivalently 1 minus the probability that all links are secure

$$SOP_r = 1 - \Pr(\max_{l \in r}[\max_{e \in E}(\gamma_{le})] < \gamma_{th}) \tag{2.7}$$

which can be written using the SOP_l which were computed in the previous section as

$$SOP_r = 1 - \prod_{l \in L}(1 - SOP_l)) \tag{2.8}$$

or

$$SOP_r = 1 - \prod_{l \in r}\prod_{e \in E}(1 - (\prod_{j \in J} \frac{1}{1 + \frac{\gamma_{th} g_{je} p_j}{g_{le} p_l}})) \tag{2.9}$$

in general. This probability is used to weight the cost of each route.

2.1.3 Jamming Power Allocation

In order to jam the eavesdroppers without interfering with the legitimate network, the jammers will act as a distributed MIMO system. By synchronizing their clocks, and calibrating for the varying delays between nodes, they will employ a cooperative friendly jamming protocol as in [3] in which they nullify their signals at the legitimate receiver. They can synchronize their clocks using a wireless synchronization protocol such as source sync [28]. This will account for varying transmission times and channel coefficients between Bob and the jamming nodes. This is possible as long as the number of jammers exceeds the number of legitimate receivers. The necessary condition for the jamming signal to be nullified is given by the following relation between the received signal $\mathbf{y}$, the jamming signal vector $\mathbf{w}$ and the channel vector $\mathbf{H_r}$ between the legitimate receiver at Bob and the jammers

$$y = \mathbf{H_r}\mathbf{w} = 0 \tag{2.10}$$

with m a random complex scalar with absolute value 1 sent in the sync header. Using the channel gain matrix between the eavesdroppers and jammers $\mathbf{H_e}$, the jamming weights w_j are determined to minimize the secrecy outage probability of the link l, subject to a total power constraint P_{max} and an individual jamming power constraint P_0. The optimal probability can be obtained by solving the following optimization problem with $p_j = w_j^2$ and $g_{je} = |h_{je}|^2$:

$$\underset{p_j}{minimize} \quad 1 - \prod_{e \in E}(1 - \prod_{j \in J} \frac{1}{1 + \frac{\gamma_{th} g_{je} p_j}{g_{le} p_l}}) \tag{2.11}$$

This objective is non-convex in the jamming power. In order to solve the problem, we instead consider the certainty equivalent margin (CEM),

$$\max_{e \in E}(\frac{g_{le} p_l}{\gamma_{th} \sum_{j \in J} |h_{ej} w_j|^2}) \tag{2.12}$$

which is the ratio of the best eavesdropper $SINR$ to the threshold for interception. This is a convex problem and varies closely with the optimization target in 2.11 [27] according to the bounds

$$\frac{1}{1+CEM} \leq 1 - SOP \leq 1 - e^{\frac{-1}{CEM}}. \tag{2.13}$$

These bounds are within approximately 10% of the actual value of $1 - SOP$ for desirable values of the SOP as shown in Fig. 2.2

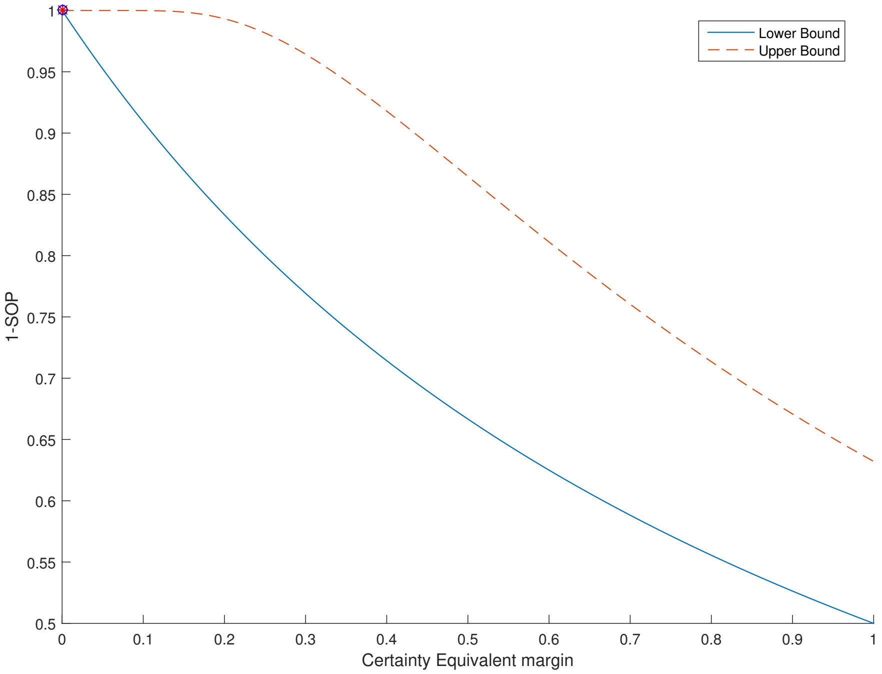

Figure 2.2: Minimizing the certainty equivalent margin corresponds well to minimizing the secrecy outage probability

Hence, we solve the following optimization problem instead:

$$\underset{w_j}{minimize} \quad \max_{e \in E}\left(\frac{g_{le}}{\sum\limits_{j \in J} |h_{ej} w_j|^2}\right) \tag{2.14}$$

subject to

$$\begin{array}{rcl} \mathbf{H_r w} & = & \mathbf{0} \\ \max\limits_{j} w_j^2 & \leq & P_0 \\ \sum\limits_{j \in J} w_j^2 & \leq & P_{max} \end{array} \tag{2.15}$$

This problem is convex and so can be solved through convex optimization techniques.

2.1.4 Link Connection Outage Probability

As shown in [9], the friendly jammers will synchronize their signals in order to nullify the signal at the legitimate receiver. Having done this, the signal to noise ratio in the link l will be only a function of p_l, g_l and the noise N_0.

$$COP_l = \Pr(\frac{g_l p_l}{N_0} < \gamma_{th}) \tag{2.16}$$

in Rayleigh fading conditions, this COP is determined as

$$COP_l = 1 - e^{-\frac{\gamma_{th} N_0}{p_l g_l}} \tag{2.17}$$

2.1.5 Route Connection Outage Probability

The route r will have a connection outage if any of the links $l \in r$ have an outage,

$$COP_r = \Pr(\min_{l \in r} \frac{g_l p_l}{N_0} < \gamma_{th}) \tag{2.18}$$

which can be rewritten as 1 minus the probability that all links are connected.

$$\begin{aligned} COP_r &= 1 - \prod_{l \in r} (1 - COP_l) \\ COP_r &= 1 - \prod_{l \in r} (1 - \Pr(\tfrac{g_l p_l}{N_0} < \gamma_{th})) \\ COP_r &= 1 - \prod_{l \in r} e^{-\frac{\gamma_{th} N_0}{p_l g_l}} \end{aligned} \tag{2.19}$$

2.2 Optimization problem

The optimization problem considered is the minimization of the probability of having either a route secrecy outage or a route connection outage. This can be equivalently written as the maximization of the probability that the route is both connected and secure, where r is a member of the set of all possible routes R

$$\underset{r \in R}{\text{maximize}} \quad (1 - COP_r)(1 - SOP_r) \tag{2.20}$$

which is given by

$$\underset{r \in R}{\text{maximize}} \quad \prod_{l \in L} (1 - COP_l) \prod_{l \in L} (1 - SOP_l) \tag{2.21}$$

or written in full

$$\underset{r \in R}{\text{maximize}} \quad \prod_{l \in L} e^{\frac{SNR_{th} N_0}{p_l g_l}} \prod_{l \in L} \prod_{e \in E} (1 - (\prod_{j \in J} \frac{1}{1 + \frac{\gamma_{th} g_{je} p_j w_j}{g_{le} p_l}})) \tag{2.22}$$

Using the link SOP and COP determined in (2.17) and (2.5), which are both positive constants less than 1 for any given l, this is the maximization of a monomial, and so is a geometric program. In many cases, connection and security will not be equally important. Therefore, the variable θ is introduced in order to trade off between the SOP and COP variables. Letting $P_{rconnected} = 1 - COP_r$ and $P_{rsecure} = 1 - SOP_r$, This new objective function is given as

$$\underset{r\in R}{\text{maximize}} \quad (P_{rconnected})^{\theta}(P_{rsecure})^{1-\theta} \tag{2.23}$$

As θ approaches 0 this problem is equivalent to maximizing the security of the route, and as θ goes to 1 it is equivalent to maximizing the connection probability. Taking the logarithm to convert this monomial into an LP gives

$$\begin{aligned}\underset{r\in R}{\text{maximize}} \quad & \theta\log(1-COP_r)+(1-\theta)\log(1-SOP_r)\\ &= \theta\sum_{l\in L}(\log(1-COP_l))+(1-\theta)(\sum_{l\in L}\log(1-SOP_l))\end{aligned} \tag{2.24}$$

which can be solved efficiently. This is a routing problem in the selection of the set L, with each link having an associated log secrecy outage probability and log connection outage probability as its weight. While only a single path is considered in the analysis, this is solved as a multipath routing problem. This is a product of the use of secrecy outage probabilities, in which a single bit being leaked is considered as a secrecy outage, and it cannot be mitigated by transmitting redundant copies. Due to this, the secrecy outage minimization will force the program to converge to a single path solution. While multipath routing is convenient for general communications, the security impacts are not well studied so we take advantage of this feature to more easily solve the single path routing problem. This greatly reduces computation time compared to running a mixed integer program for single path routing algorithms.

The considered optimization variable is the routing matrix R. Each element $r_{a,b}$ corresponds to the portion of the data flow routed on the link $l_{a,b}$ between node a and node b. Let $COP_{a,b}$ be the connection outage probability between a and b, similarly $SOP_{a,b}$. This optimization problem is expressed in full in (2.25).

The entire process for determining the network routing is then to first determine the jamming powers P_j for each link using (2.14), then to determine the link secrecy outage and connection outage probabilities $SOP_{a,b}$ in (2.5) and $COP_{a,b}$ in (2.17), then to use these probabilities to solve the final routing problem. The full optimization problem is expressed below:

$$\underset{R}{\text{maximize}} \quad \theta \sum_{a\in N} \sum_{b\in N} (r_{a,b} \log{(1 - COP_{a,b})}) + (1-\theta)(\sum_{a\in N} \sum_{b\in N} (r_{a,b} \log{(1 - SOP_{a,b})})) \tag{2.25}$$

subject to

$$\begin{array}{lcl} r_{a,b} & \leq & 1 \\ r_{a,b} & \geq & 0 \\ \sum\limits_{a\in N} r_{a,b} - \sum\limits_{c\in N} r_{b,c} & = & \begin{cases} 1, \text{ if } b \text{ is the destination} \\ -1, \text{ if } b \text{ is the source} \\ 0, \text{ otherwise.} \end{cases} \end{array} \tag{2.26}$$

2.3 Simulation Studies

This problem was simulated on a random network consisting of 30 nodes and 12 eavesdroppers. The nodes are uniformly distributed across the entire area of the 10 by 10 grid, while the eavesdroppers are normally distributed around the grids center. The message is sent from 0,0 to 10,10 to ensure it passes all eavesdroppers. The channel between each node is modeled by path loss and Rayleigh fading. The simulations show 3 separate comparisons. The first is the effect of changing the trade off variable θ, the second is the effect of changing the density of eavesdroppers, and the third is the impact of the friendly jamming.

Table 2.1: System Parameters

Network Parameter	**Value**
γ_{th}	1
Transmit Power	10 W
Noise Power	0.01 W
Total Jamming Power	120 W
Maximum Jammer Power	20 W
Number of nodes	12
Number of Eavesdroppers	4
θ	0.5
Network Size 10m x 10m	

2.3.1 Security and Service Quality Trade-off

The trade off variable θ is swept from 0.1 to 1, showing the differences in chosen routes. As θ is chosen to tend towards higher security, the route will move to a less direct path to increase the distance from transmitters to eavesdroppers, at the cost of longer hops increasing the connection outage probability. The impact of the jamming is to allow the routing to ignore eavesdroppers which are close to a large number of friendly nodes, as the jamming power will force Eves $SINR$ below the required threshold for interception.

Fig. 2.3 illustrates the effect of different values of θ on the chosen route. $\theta = 1$ shows the route for minimization of the connection outage probability, without regard for secrecy. The remaining routes are decided using θ to trade off between the secrecy and connection outage probabilities. Note how the route moves from an indirect route at the edge of the environment away from clusters of eavesdroppers, towards a more direct path with shorter hops as θ approaches 1. It is also visible that the jamming causes the route to avoid isolated eavesdroppers, while routing relatively close to eavesdroppers that are surrounded by friendly nodes. Fig. 2.4 and Fig. 2.5 show simulation results using the parameters in table 2.1 and 4 eavesdroppers, with θ swept from 0 to 0.95.

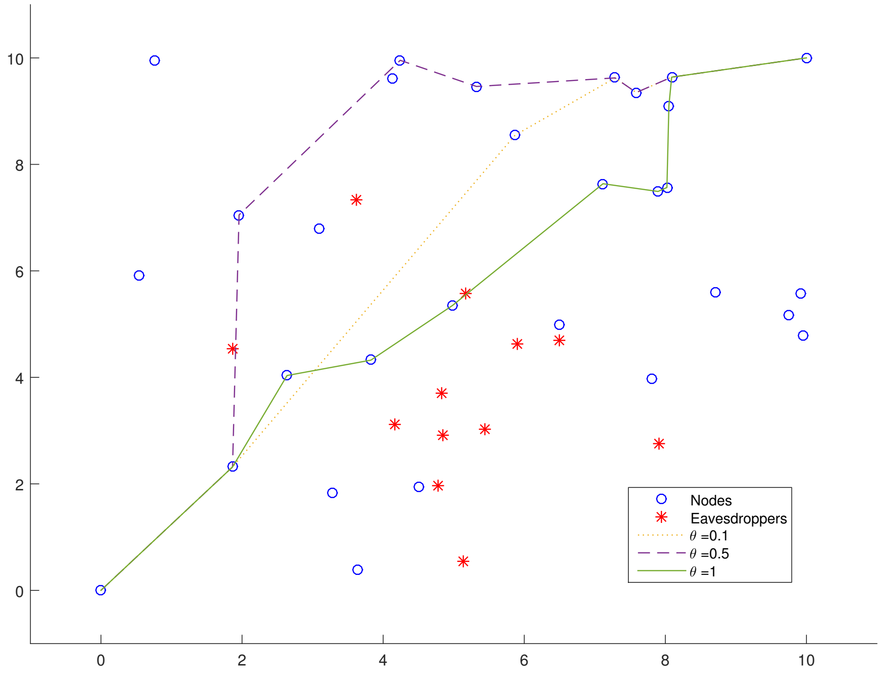

Figure 2.3: Emphasizing route quality forces a more direct route, while emphasizing security routes away from the eavesdroppers

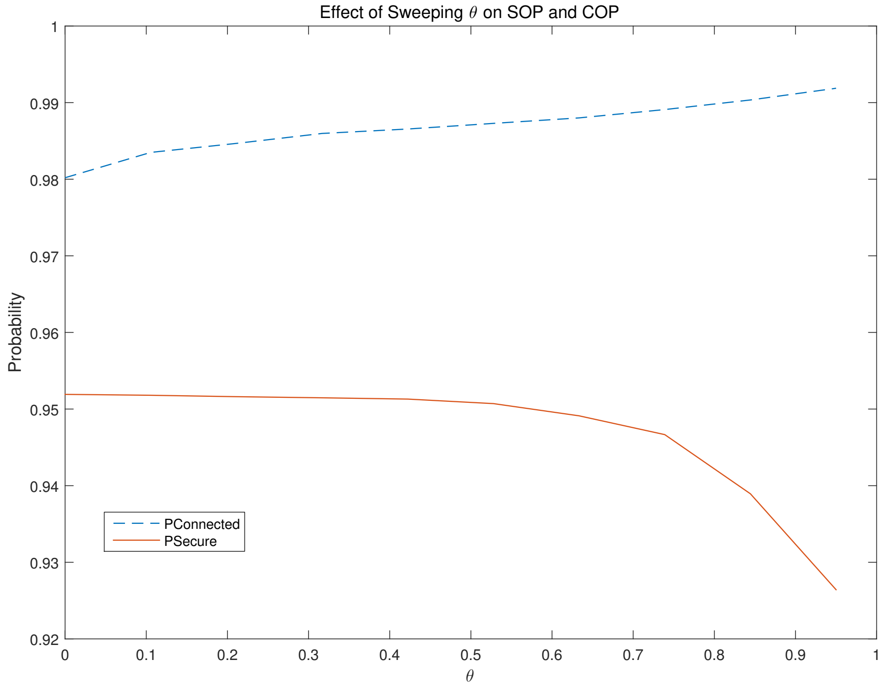

Figure 2.4: Route outage probabilities for different values of the trade-off variable. Increasing the focus on connection quality lowers the security performance

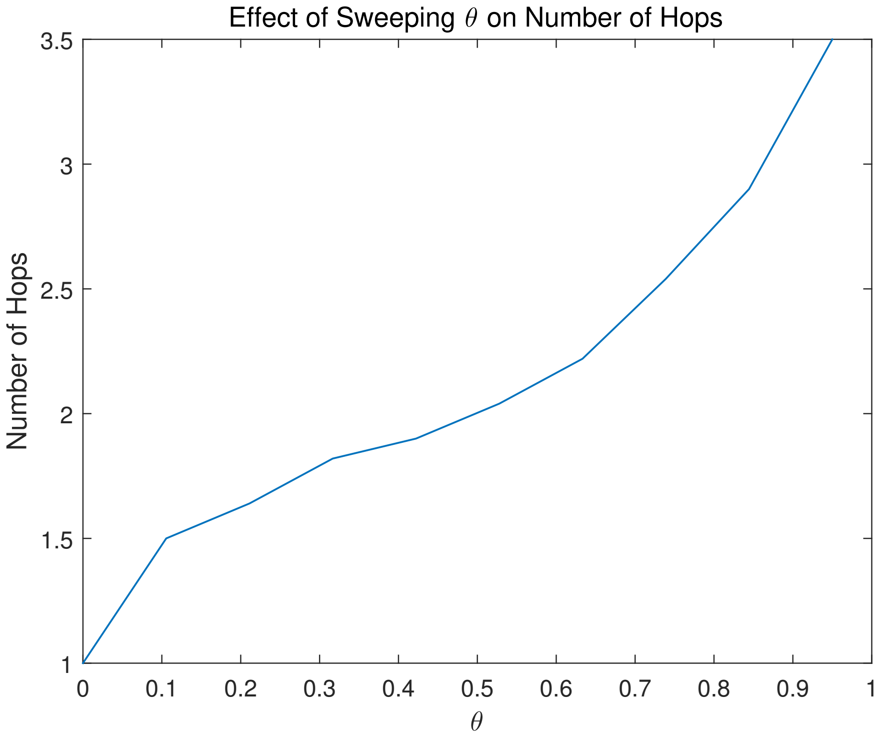

Figure 2.5: Emphasizing connection quality causes the number of links in the route to increase

2.3.2 Varying the number of eavesdroppers

Fig. 2.6 and Fig. 2.7 show the effect of adding additional eavesdroppers into the system. These simulations were done using the values in table 2.1, with θ set at 0.5 in each route. The number of eavesdroppers is swept from 1 to 12. As the number of eavesdroppers is increased, the SOP of each link increases. The routing algorithm compensates by routing to favour security. The effect is that the route SOP and COP both decrease as the number of eavesdroppers is increased as seen in Fig. 2.6. This means that the route moves to avoid clusters of eavesdroppers, and the hops become longer as demonstrated in Fig. 2.7.

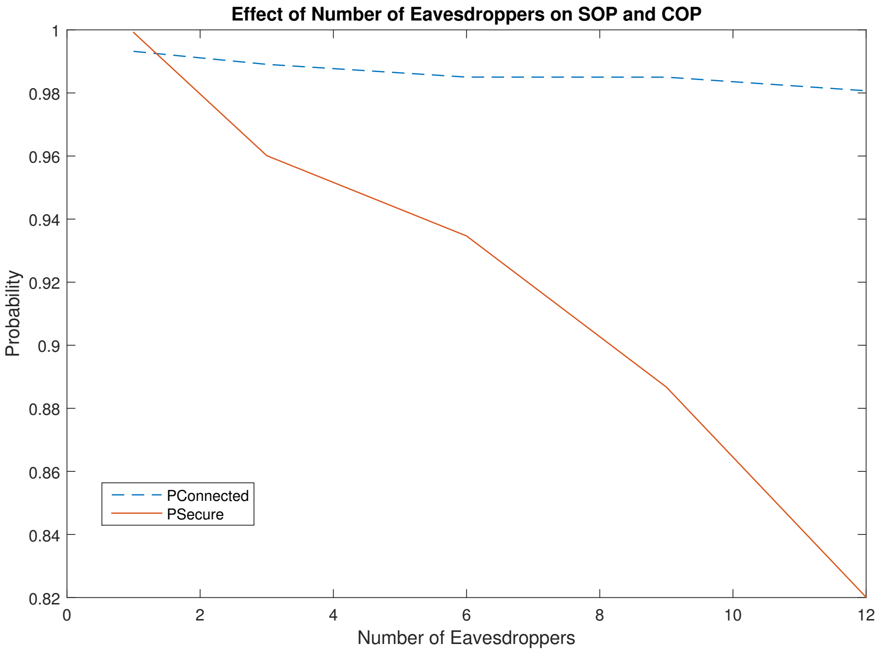

Figure 2.6: Route outage probabilities for different numbers of eavesdroppers. Increased eavesdropper density lowers both the security and service quality of the route.

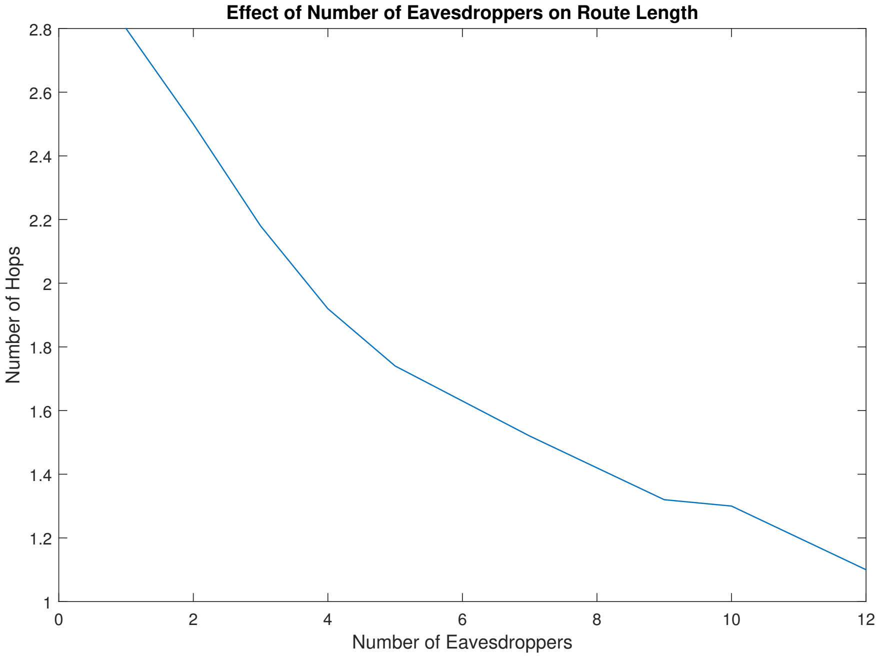

Figure 2.7: Increasing the eavesdropper density causes the route to favour longer hops.

2.3.3 Effect of friendly jamming

In this subsection, the same network is used to compare the generated routes with and without friendly jamming. Both routes are generated using the same routing metric, and differ only in their calculation of link SOPs. In all links, the SOP will be much higher without friendly jamming than with it. However, the effect is not uniform, as eavesdroppers which are located near nodes will be jammed much more effectively, while more isolated eavesdroppers will not have a high jamming power reducing their $SINR$. Fig. 2.8 shows the different route choices with and without using friendly jamming. The route without jamming leaves each link SOP as a function only of the difference to the nearest eavesdropper, as there is no way to lower their SINR. The lack of jamming causes the route to take a very indirect path in an effort to better avoid the eavesdroppers. Conversely, the route with friendly jamming is able to be much more direct, as any eavesdroppers which are located near a node can be easily jammed in order to greatly limit their ability to intercept a transmission. Additionally, the security performance of our scheme with friendly jamming is greatly improved over the proposed scheme in [26] without friendly jamming. Fig. 2.9 shows the effect of the total jamming power on the route SOP and COP. Increasing the jamming power improves both the SOP and COP, as the lowered SOP allows the signal to take a route that favours the connection quality. This is also seen in the increased route length shown in Fig. 2.10.

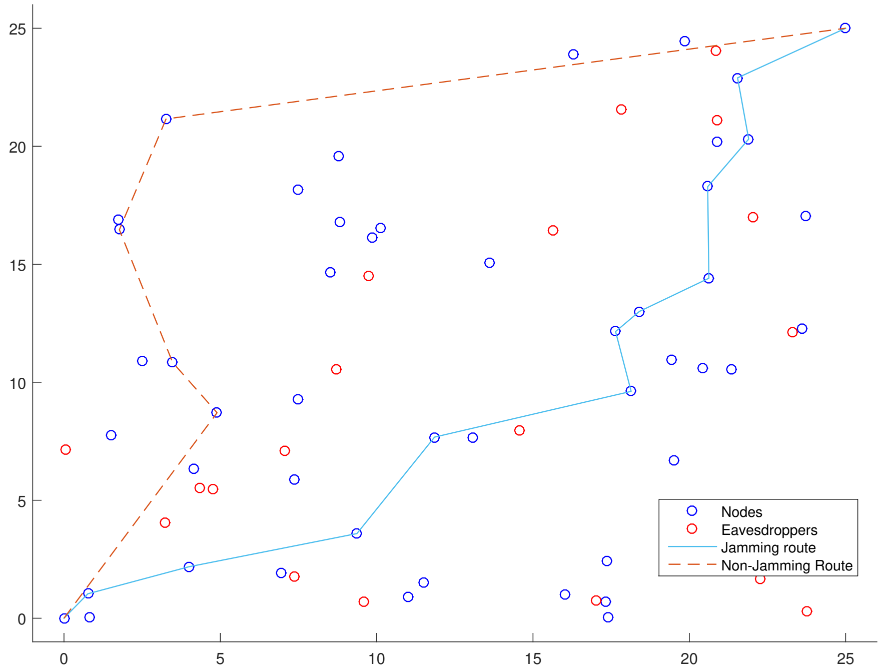

Figure 2.8: Application of friendly jamming allows for a much more direct route than using the same routing metric without jamming

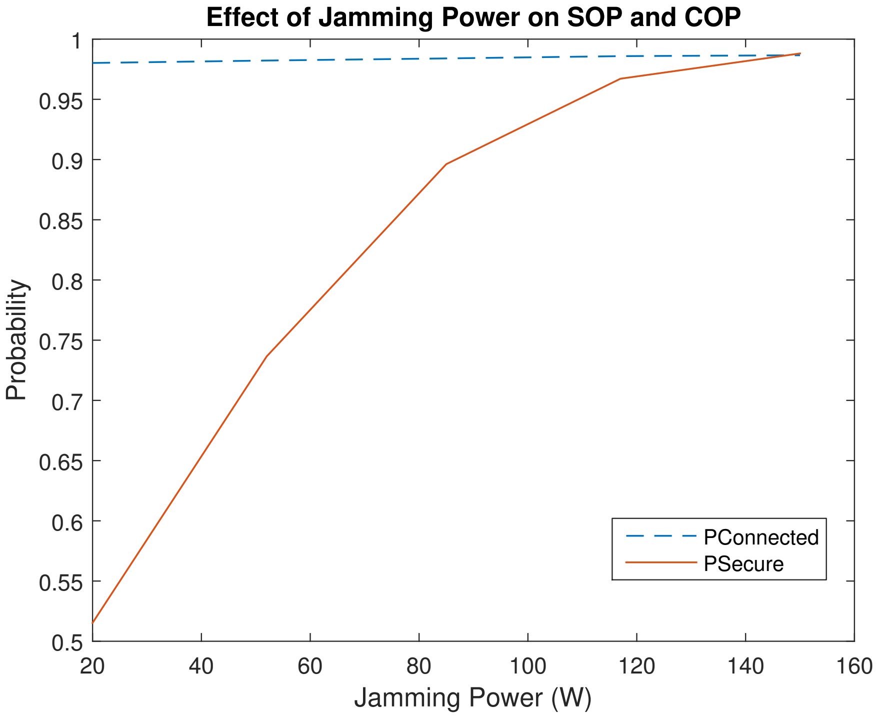

Figure 2.9: Increasing jamming power significantly improves the route security performance, and marginally improves the connection quality

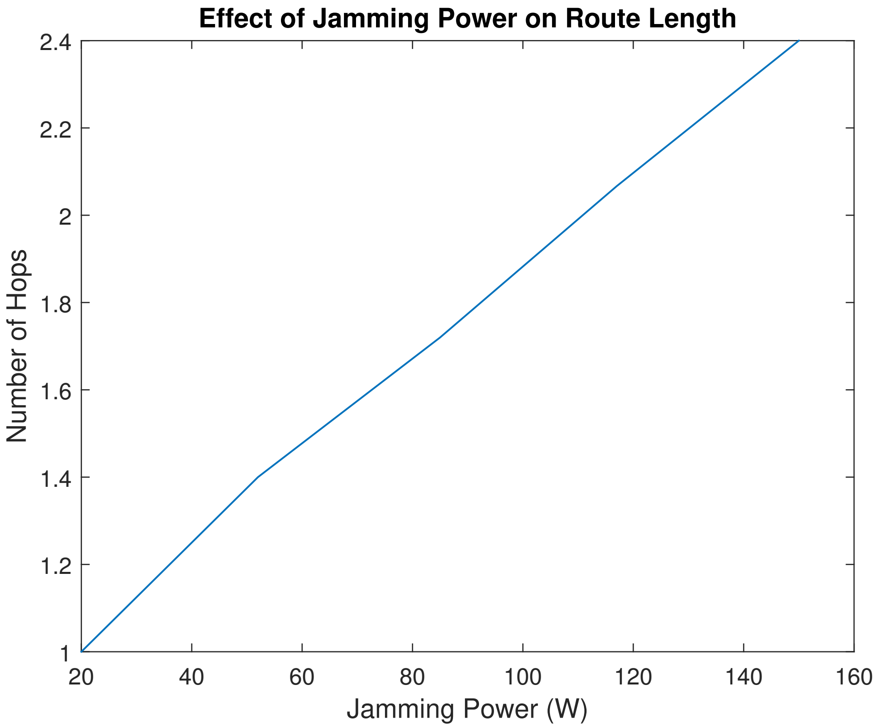

Figure 2.10: Increasing jamming power allows for a longer route

2.4 Conclusion

This chapter considered the problem of routing a signal through a wireless area network with concern for both SOP and COP of the route. The typical trade off is that increasing power to lower the COP will increase the SOP of the link. However, through the use of friendly jamming, we are able to lower the SOP of a route without raising its COP. This is desirable as it helps lower the need to compromise quality of service to improve security. We then considered the problem of routing through a wireless area network while jointly minimizing the secrecy outage probability and connection outage probability, a tuning variable θ to weight the COP and SOP to the needs of a user. The jamming powers are determined to place nulls at friendly receivers while maximizing the power to eavesdroppers. Using the jamming powers, the route metrics are derived, and the problem is framed as a convex optimization problem. The performance of the route is demonstrated under different densities of eavesdroppers, and different values of θ. It is also compared with the same routing problem without the assistance of friendly jamming, and achieves better security performance. The next chapter considers the problem of self-interference channel estimation for full-duplex jamming receivers.

Chapter 3

Adaptive Filtering for Self Interference Channel Cancellation

The objective of this chapter is to analyze the performance of estimating the self-interference channel (SIC) in the presence of the desired signal in the context of friendly jamming. This has the potential to significantly increase the secrecy capacity in systems containing full-duplex jamming receivers. Full-duplex jamming receivers are proposed in [10] which ignores the SIC estimate, and extended in [11] using half duplex estimation periods in which unsecured information is transmitted. In order to maximize the total system throughput, it is desirable to complete the SIC estimate without the use of a half duplex pilot signal. In [17] and [2], the authors examine schemes in which the SIC is estimated under interference from the desired signal through the use of very long sets of received data to achieve comparable results to pilot signal based estimation. In the context of in-band full-duplex communications this is able to provide only a slight performance gain, as the half duplex transmission periods still send information. When the receivers transmitted signal is a jamming signal, the half duplex period instead represents a period of no transmission as no information will be transmitted. In this context, eliminating the half duplex periods represents a more significant performance increase.

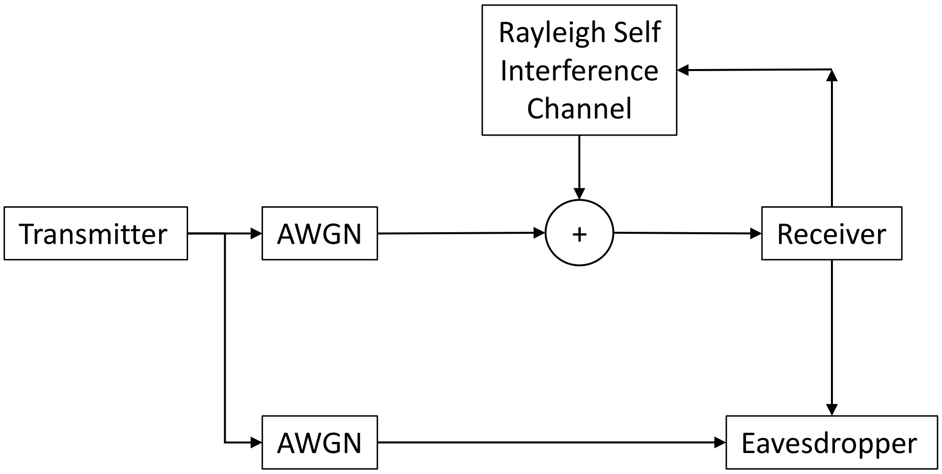

Figure 3.1: This system models a transmitter, and eavesdropper, and a single full-duplex jamming receiver

3.1 System Model and Problem Formulation

The objective of this chapter is to compare the use of RLS based continuous channel estimation under self-interference with the use of pilot signals for estimation in the context of friendly jamming. Our system model is shown in Fig. 3.1. It consists of a transmitter, an eavesdropper, and a full-duplex jamming receiver. The channels from the transmitter to both the receiver and the eavesdropper are modeled as AWGN channels for simplicity. The self-interference channel is modeled as a Rayleigh fading channel which is similar to previous work in this area [2] [29]. In most current writing on Self Interference Channel cancellation, the SIC estimate is completed through the use of a pilot signal and the off-line least squares estimation formula given by:

$$\Theta = (\Psi' W \Psi)^{-1} \Psi' W Y \tag{3.1}$$

where Ψ represents the LxN matrix of N transmissions of the known jamming signal into an L-tap channel, W the weighting factor matrix for each input, and Y the received signal holding N observations. $|Theta$ is then the estimated channel between the full-duplex jamming receiver and itself. This equation is the off-line version of the least squares estimator, and is computationally expensive as it requires a matrix inversion. Least squares estimation can instead be performed recursively, which is primarily used as it is less computationally expensive to compute than the standard least squares estimate. The recursive form of the least squares estimate is shown below, where ψ_n and ψ_{n+1} represent the current L previous transmitted signals and the previous set of signals, y_{n+1} the new received signal, and θ_n the current estimate.

$$\theta_{n+1} = \frac{\theta_n + P_n \Psi_{n+1}}{\lambda + \psi'_{n+1} P_n \psi_n}(y_{n+1}\theta_n) \tag{3.2}$$

$$P_{n+1} = \frac{P_n + P_n \Psi_{n+1} \Psi'_{n+1} P_n}{\lambda + \psi'_{n+1} P_n \psi_n} \tag{3.3}$$

An additional benefit of RLS is that it is able to be ran online to track a time varying channel, as long as the channel coherence time is longer than the effective asymptotic length of the algorithm, given by

$$L_{eff} = \frac{1}{1-\lambda} \tag{3.4}$$

This allows the algorithm to be ran constantly and track the channel continuously [30]

As shown in [29], the variance of the channel estimate will be given by

$$var(\hat{h}) = \frac{\sigma_n^2 + \sigma_r^2}{N_s P_{ref}} \tag{3.5}$$

where σ_n^2 is the noise power, σ_r^2 is the desired signal power and P_{ref} is the power of the transmitted signal. N_s is the number of samples in the estimate, or in the case of RLS, N_s will be the effective asymptotic length of the algorithm. When the signal is estimated in a separate calibration period, the residual power will be given by

$$var(\hat{h}) = \frac{\sigma_n^2}{N_c P_{ref}} \tag{3.6}$$

so the required number of samples for a given estimate quality is reduced by a factor of $1 + \frac{\sigma_r^2}{\sigma_n^2}$. However, the requirement for longer estimation lengths when estimating the channel without a calibration period is acceptable as data is still being transmitted. The associated SINRs are calculated under the assumption that the self-interference signal is Gaussian. This is a good assumption in the jamming receiver scenario, where the receiver is broadcasting white noise to the eavesdroppers, and is a common assumption and provides realistic results in the full-duplex communication scenario [17] [2]. The SINR is then

$$\gamma = \frac{\sigma_r^2}{\sigma_n^2 + var(\hat{h})P_{ref}} \tag{3.7}$$

The effective data rate for the bidirectional data stream under RLS cancellation can be expressed as

$$C_{rls} = \log_2(1 + \gamma_N) \tag{3.8}$$

where N represents the estimation length, and γ_N is the SNR achieved with that estimation length. Similarly, if pilot signals are used for calibration the capacity will be given by

$$C_c = (1 - \frac{N_c}{T_c F_s}) \log_2(1 + \gamma_{N_c}) \tag{3.9}$$

with N_c set to match the SINR for RLS case as

$$N_c = \frac{N}{1 + \frac{\sigma_r^2}{\sigma_n^2}}. \tag{3.10}$$

This equation models the fact that the receiver is not receiving any information while it is estimating its self-interference channel. $(1 - \frac{N_c}{T_c F_s})$ is the proportion of time that the receiver can receive, and $\log_2(1 + \gamma_{N_c})$ is its rate with an N_c sample estimate. As in chapter 1.3, the secrecy capacity will be the difference in capacity of the transmitter-eavesdropper channel and the legitimate channel. The channel capacity from the transmitter to the eavesdropper is given as

$$C_{te} = \log_2(1 + \frac{\sigma_{te}^2}{N_0 + \sigma_{je}^2}) \tag{3.11}$$

where σ_{te}^2 is the received signal power at the eavesdropper from the transmitter, and σ_{je}^2 is the received jamming power. Then,

$$SC_{rls} = C_{rls} - \log_2(1 + \frac{\sigma_{te}^2}{N_0 + \sigma_{je}^2}) \tag{3.12}$$

and

$$SC_c = C_c - \log_2(1 + \frac{\sigma_{te}^2}{N_0 + \sigma_{je}^2}) \tag{3.13}$$

3.2 Simulation

Numerical calculations were performed to compare the theoretical performance of online RLS channel estimation with pilot based estimation in a security context. These calculations were performed for 2 cases, the first representing SIC cancellation down to a fixed SINR, and the second representing SIC cancellation using a fixed estimation length. Finally, the two schemes are compared at different jamming powers. The metric to evaluate their performance is the secrecy capacity of the system.

Table 3.1: System Parameters

Network Parameter	**Value**
Noise power	0.01 mW
Received Desired Signal Power	1 mW
Transmitted Jamming Power	50 mW
Eavesdropper received signal power	1 mW
Eavesdropper path loss coefficient	0.01

As shown in Fig. 3.2, using RLS over pilot based estimation will provide a slight gain in data rate at a given desired SINR. In this simulation the RLS length is given by T_cF_s, and the equivalent length for the LS estimation is $\frac{T_cF_s}{1+\frac{\sigma_r^2}{\sigma_n^2}}$. The data rate gain for RLS estimation

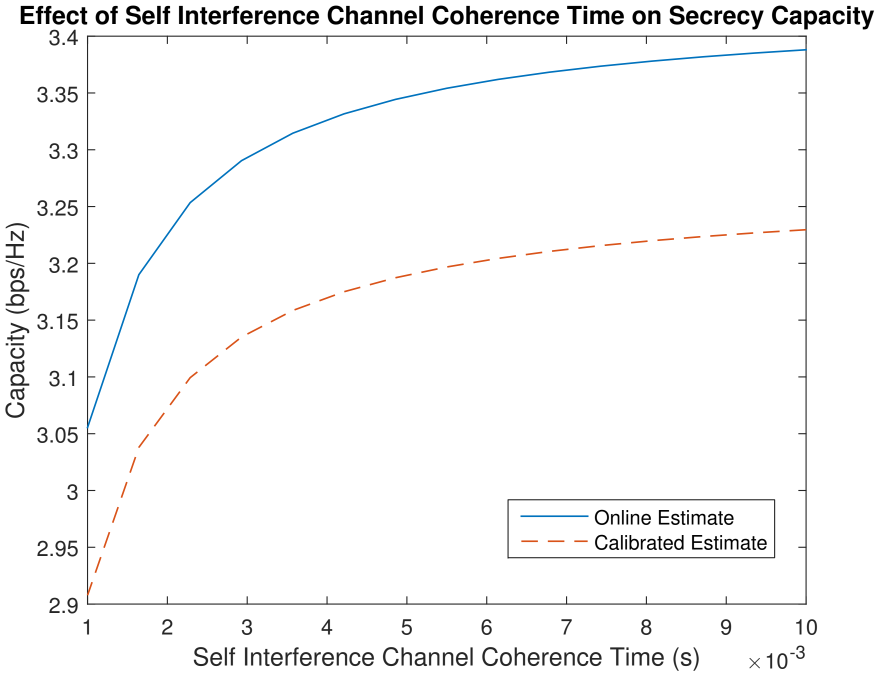

Figure 3.2: Estimating the self-interference channel without a calibration period allows for a significant increase in secrecy capacity

is caused by the need for the pilot based system to operate in half duplex mode during the channel estimation. It provides a constant rate gain expressed by

$$R_{RLS} = R_{pilot} \frac{1 + \gamma_d}{\gamma_d} \tag{3.14}$$

This demonstrates that estimation in full-duplex communication modes will not cause a loss of data rate in the system if the desired SNR is held constant.

In Fig. 3.3 both estimators are working with a fixed length of 50 samples. The RLS estimate does not vary with the channel coherence time, as the coherence time is longer than the estimator length in all cases. The calibrated estimate performs poorly at low coherence times, and increases in performance as the coherence time increases. In this scenario, the RLS estimation can be seen to have a significant data rate advantage with low channel coherence times. It's ability to track the channel constantly provides a significant gain over the LS estimator at low channel coherence times as the pilot signal transmission takes a larger proportion of the total channel time when the estimation must be performed frequently.

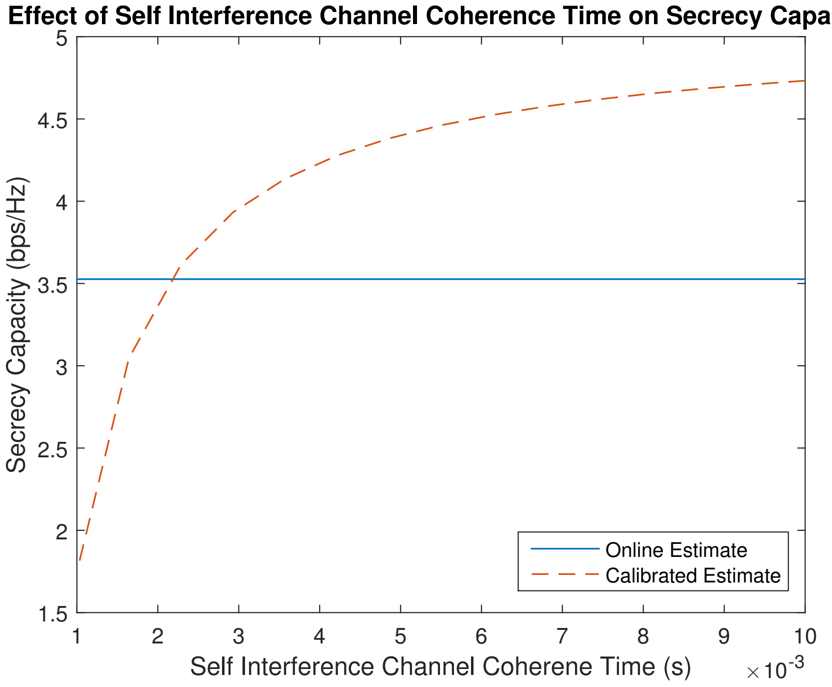

Figure 3.3: With both estimators using a fixed length, the online estimate is superior at shorter channel coherence times

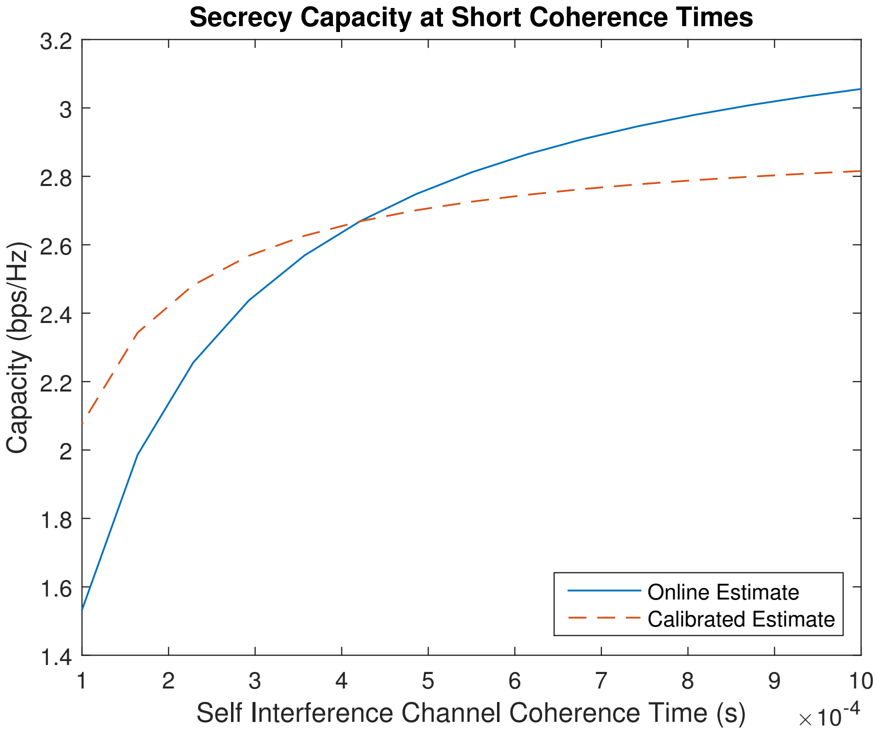

Figure 3.4: Online estimation outperforms calibration based estimation at all jamming signal powers

Fig. 3.4 shows the effect of short coherence times on the secrecy capacity. In this simulation, the calibration based estimate length is set to provide a fixed SINR. The online estimate matches this SINR if possible, and uses a length equal to the coherence time if it is not. When the coherence time is too short, the online estimate is unable to take enough samples to match the achieved SINR for the calibration based estimate. In these scenarios, estimating with a pilot signal can be more efficient even though there is no transmission during the estimate.

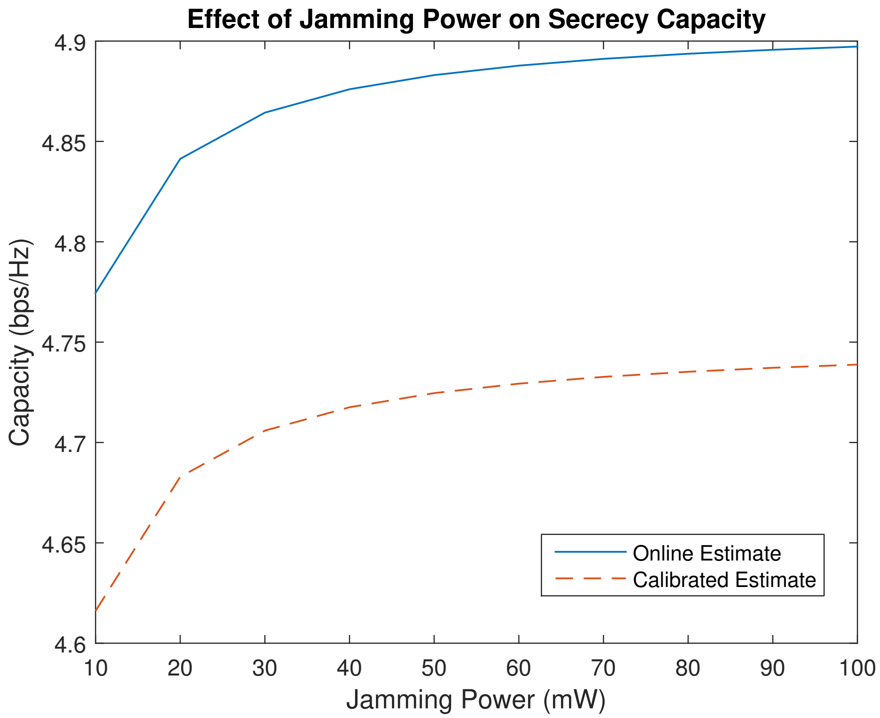

Figure 3.5: Online estimation outperforms calibration based estimation at all jamming signal powers

In Fig. 3.5, the online and calibrated estimator are compared at varying jamming powers. The increased jamming power lowers the SINR at the eavesdropper, while not affecting the SINR at the legitimate receiver. This is due to the fact that the estimation quality increases with the self-interference power. This assumption is reasonable only as long as the analog to digital converter is able to receive both the self-interference signal and the desired signal, so in practice there would be limits on the maximum jamming power.

3.2.1 Results

This analysis was able to demonstrate the performance advantage of online channel estimation over calibration based estimates for friendly jamming. The numerical simulations confirmed the ability of the online estimate to provide a significant gain over pilot based estimation in all channel conditions if the SINR of each estimate is matched, and over short channel coherence times if the estimation length is held constant. If the channel coherence time is too short to allow the achievable SINRs to be matched, then the calibration based estimate can outperform the online estimate. Additionally, as the online estimate does not require a calibration period it is simpler to implement for higher level protocols.

Chapter 4

Conclusions and Future Work

This thesis has addressed two problems relating to the use of friendly jamming for physical layer security: (1) an optimal power allocation and routing through a network, and (2) the use of online channel estimations for self-interference cancellation in full-duplex jamming receivers.

In Chapter 2, the use of friendly jamming to improve security performance was examined. An optimal jamming power allocation scheme was derived to determine the secrecy performance in each link. Using the determined secrecy and connection outage probabilities, and a tuning variable θ to weight the importance of connection outage probability and secrecy outage probability to the needs of a user, the signal was routed through the network to maximize the probability that the route was connected and secure. The performance of the route is demonstrated under different densities of eavesdroppers, and different values of the trade-off variable between security and connection outage probability. The routing and jamming problem was also compared with the same routing problem without the assistance of friendly jamming. It was found to have good performance when the number of nodes in the network is greater than the number of eavesdroppers, and acceptable performance when they are the same. Future work in this area should examine the routing and jamming problems at the network level rather than per signal, in order to increase power efficiency and reduce congestion.

In Chapter 3, the effectiveness of using recursive least squares (RLS) for continuous self-interference channel (SIC) estimation without pilot signals was analyzed. Results showed that RLS without a calibration period is able to increase the system's secrecy capacity in all jamming powers and channel coherence times if the estimate length is allowed to vary. If the estimate length is fixed, estimating the SIC without a calibration period still provides a higher secrecy capacity at short channel coherence times. The online estimate proved to be most accurate with a long effective filter length, and provides the greatest efficiency gain over current methods with a short channel coherence time. It provides a way to take advantage of having no fixed calibration period by continuously tracking the channel while consuming relatively few computational resources. Future work in this area should include the use of purpose built algorithms for SIC estimation over RLS.

Bibliography

[1] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[2] D. Korpi, T. Riihonen, and M. Valkama, "Achievable rate regions and self-interference channel estimation in hybrid full-duplex/half-duplex radio links," in *49th Annu. Conf. on Information Sciences and Systems (CISS)*, March 2015, pp. 1–6.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.

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

[5] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[6] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct 2012.

[7] Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/qos-aware route selection in multi-hop wireless ad hoc networks," in *IEEE Int. Conf. on Communications (ICC)*, May 2016, pp. 1–6.

[8] S. Tomasin, “Routing over multi-hop fading wiretap networks with secrecy outage probability constraint,” *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1811–1814, Oct 2014.

[9] R. Eletreby, H. Rahbari, and M. Krunz, “Supporting phy-layer security in multi-link wireless networks using friendly jamming,” in *IEEE Global Communications Conf. (GLOBECOM)*, Dec 2015, pp. 1–6.

[10] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[11] T. X. Zheng, Q. Yang, Y. Zhang, H. M. Wang, and P. Mu, “Physical layer security in distributed wireless networks using full-duplex receiver jamming,” in *IEEE Globecom Workshops*, Dec 2016, pp. 1–6.

[12] C. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1948.

[13] A. D. Wyner, “The wiretap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 3, pp. 1355–1367, 1978.

[14] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.

[15] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[16] A. Sabharwal *et al.*, “In-band full-duplex wireless: Challenges and opportunities,” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept 2014.

[17] K. Akcapinar and O. Gurbuz, “Full-duplex bidirectional communication under self-interference,” in *13th Int. Conf. on Telecommunications (ConTEL)*, July 2015, pp. 1–7.

[18] S. Venkatasubramanian, K. Haneda, and K. Yamamoto, “System-level performance of in-band full-duplex relaying on m2m systems at 920 mhz,” in *IEEE 81st Vehicular Technology Conf. (VTC Spring)*, May 2015, pp. 1–5.

[19] M. Duarte and A. Sabharwal, “Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results,” in *Conf. Rec. of the 44th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR)*, Nov 2010, pp. 1558–1562.

[20] L. Laughlin, M. Beach, K. Morris, and J. Haine, “Electrical balance duplexing for small form factor realization of in-band full duplex,” *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 102–110, May 2015.

[21] M. Ghoraishi, W. Jiang, P. Xiao, and R. Tafazolli, “Subband approach for wideband self-interference cancellation in full-duplex transceiver,” in *Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Aug 2015, pp. 1139–1143.

[22] A. Koohian, H. Mehrpouyan, M. Ahmadian, and M. Azarbad, “Bandwidth efficient channel estimation for full duplex communication systems,” in *Int. Conf. on Communications (ICC)*, June 2015, pp. 4710–4714.

[23] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[24] H. Huang, X. Zhang, X. Hu, P. Zhang, and Y. Li, “An optimal jammer selection for improving physical-layer security in wireless networks with multiple jammers,” in *2016 Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Sept 2016, pp. 719–724.

[25] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, “Secure relay and jammer selection for physical layer security,” *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug 2015.

[26] J. Yao, S. Feng, X. Zhou, and Y. Liu, “Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying,” *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 753–764, Feb 2016.

[27] S. Kandukuri and S. Boyd, “Optimal power control in interference-limited fading wireless channels with outage-probability specifications,” *IEEE Trans. Wireless Commun.*, vol. 1, no. 1, pp. 46–55, Jan 2002.

[28] H. H. H. Rahul and D. Katabi, “Sourcesync: A distributed wireless architecture for exploting sender diversity,” in *Proc. ACm SIGCOMM, New Delhi, India*, May 2010, pp. 171–182.

[29] D. Korpi, L. Anttila, and M. Valkama, “Impact of received signal on self-interference channel estimation and achievable rates in in-band full-duplex transceivers,” in *48th Asilomar Conf. on Signals, Systems and Computers*, Nov 2014, pp. 975–982.

[30] E. Eweda and O. Macchi, “Convergence of the RLS and LMS adaptive filters,” *IEEE Trans. Circuits Syst.*, vol. 34, no. 7, pp. 799–803, Jul 1987.