Wireless Secret Key Generation Versus Capable Adversaries

by

Masoud Ghoreshi Madiseh
B.Sc., Iran University of Science and Technology, 2005
M.Sc., Iran University of Science and Technology, 2007

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in Electrical and Computer Engineering Department

© Masoud G. Madiseh, 2011
University of Victoria

All rights reserved. This dissertation may not be reproduced in whole or in part, by photocopying or other means, without the permission of the author.
Wireless Secret Key Generation Versus Capable Adversaries

by

Masoud Ghoreishi Madiseh
B.Sc., Iran University of Science and Technology, 2005
M.Sc., Iran University of Science and Technology, 2007

Supervisory Committee

Dr. M.L. McGuire, Co-Supervisor
(Department Electrical and Computer Engineering)

Dr. S.W. Neville, Co-Supervisor
(Department Electrical and Computer Engineering)

Dr. T.A. Gulliver, Departmental Member
(Department Electrical and Computer Engineering)

Dr. B. Kapron, Outside Member
(Department of Computer Science)
Supervisory Committee

Dr. M.L. McGuire, Co-Supervisor
(Department Electrical and Computer Engineering)

Dr. S.W. Neville, Co-Supervisor
(Department Electrical and Computer Engineering)

Dr. T.A. Gulliver, Departmental Member
(Department Electrical and Computer Engineering)

Dr. B. Kapron, Outside Member
(Department of Computer Science)

ABSTRACT

This dissertation applies theories and concepts of wireless communications and signal processing to the security domain to assess the security of a Wireless secret Key Generation (WKG) system against capable eavesdroppers, who employ all the feasible tools to compromise the system’s security. The security of WKG is evaluated via real wireless measurements, where adversary knows and applies appropriate signal processing tools in order to predict the generated key with the communicating pair. It is shown that in a broadband stationary wireless communication channel, (e.g. commercial off-the-shelf 802.11 WLAN devices), a capable eavesdropper can recover a large portion of the secret key bits. However, in an Ultra-wideband (UWB) communication, at the same stationary environment, secret key rates of 128 bits per channel probe are achievable.
# Contents

Supervisory Committee ii  
Abstract iii  
Table of Contents iv  
List of Tables vii  
List of Figures viii  
Acknowledgements ix  
Dedication xi  

1 Introduction 1  
  1.1 Contributions ........................................ 6  
  1.2 Dissertation’s organization .............................. 7  

2 Literature Review 9  
  2.1 Theoretical work ........................................ 9  
  2.2 Practical work ........................................ 10  
  2.3 Taxonomy .............................................. 12  
  2.4 Comparison ............................................ 13  
  2.5 Summary .............................................. 17  

3 UWB Channel Measurements 18  
  3.1 UWB Signal Characteristics ............................ 18  
  3.2 Experimental Measurement Approach ................... 21  
  3.3 Testing for Alice-Bob Channel Reciprocity .............. 21  
  3.4 Testing for Spatial Correlations ....................... 23
3.5 Testing for Time Correlation ........................................ 25
3.6 Summary ............................................................. 29

4 Secret Key Rate .......................................................... 30
4.1 Bounds on Secret Key Rate .......................................... 31
4.2 Simplified Model for Eve with independent measurements .... 31
4.3 Nontrivial Upper-bound on Secret Key Rate ..................... 34
4.4 MIMO effect on secret key rate ..................................... 35
4.4.1 Calculate the non-trivial lower bound ......................... 36
4.5 Summary ............................................................. 38

5 Secret Key Generation Method ........................................ 39
5.1 Key Generation ........................................................ 39
5.2 Public Discussion to Ensure Key Consistency .................... 42
5.3 Performance .......................................................... 43
5.4 Summary ............................................................. 45

6 Removing Shadow Fading .............................................. 46
6.1 Proposed Prediction Approach ...................................... 49
6.2 Information theoretic analysis of the method ...................... 51
6.3 Simulation Results .................................................... 52
6.4 Summary ............................................................. 53

7 Random Beamforming .................................................. 55
7.1 Channel Prediction ...................................................... 57
7.2 Random Beamforming ................................................ 59
7.3 Analysis of Random Beamforming .................................. 61
7.3.1 Random Channel Matrix ....................................... 68
7.3.2 Random Beamforming .......................................... 71
7.4 Simulation results ...................................................... 72
7.5 Summary ............................................................. 73

8 Security Analysis ........................................................ 75
8.1 Passive Eavesdroppers ................................................. 76
8.2 Active Adversaries ..................................................... 78
8.3 Security tests versus capable eavesdroppers ...................... 81
8.4 Eve with an Array Antenna in Different Bandwidths ............ 82
<table>
<thead>
<tr>
<th>8.5 Ray-tracing test</th>
<th>88</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6 Concerns in reconciliation procedure</td>
<td>90</td>
</tr>
<tr>
<td>8.7 Summary</td>
<td>93</td>
</tr>
</tbody>
</table>

| 9 Conclusions | 95  |
| Bibliography | 98  |

<table>
<thead>
<tr>
<th>A Formulas</th>
<th>105</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1 Derivation of Eq. (7.18)</td>
<td>105</td>
</tr>
<tr>
<td>A.2 Derivation of Eq. (7.22)</td>
<td>106</td>
</tr>
</tbody>
</table>
List of Tables

Table 2.1 Comparison table of practical WKG solutions. . . . . . . . . . . 13
Table 3.1 Measurement apparatus. . . . . . . . . . . . . . . . . . . . . . . 19
Table 3.2 Reciprocity test LOS channel. . . . . . . . . . . . . . . . . . . 22
Table 3.3 Reciprocity test NLOS channel. . . . . . . . . . . . . . . . . . . 22
Table 8.1 Capable eavesdroppers with multiple antenna array. . . . . . . 88
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Test apparatus setup.</td>
<td>19</td>
</tr>
<tr>
<td>3.2</td>
<td>Transmitted pulse’s shape.</td>
<td>20</td>
</tr>
<tr>
<td>3.3</td>
<td>Spatial correlation test grid.</td>
<td>23</td>
</tr>
<tr>
<td>3.4</td>
<td>Spatial correlation prior to removing shadow fading effect.</td>
<td>26</td>
</tr>
<tr>
<td>3.5</td>
<td>Spatial correlation post shadow fading removal.</td>
<td>27</td>
</tr>
<tr>
<td>3.6</td>
<td>Time correlation test.</td>
<td>28</td>
</tr>
<tr>
<td>4.1</td>
<td>A typical UWB channel power profile.</td>
<td>33</td>
</tr>
<tr>
<td>4.2</td>
<td>Secret key rate versus SNR.</td>
<td>34</td>
</tr>
<tr>
<td>5.1</td>
<td>Block diagram of the key generation process.</td>
<td>41</td>
</tr>
<tr>
<td>5.2</td>
<td>Block diagram of key validation process.</td>
<td>42</td>
</tr>
<tr>
<td>5.3</td>
<td>The key generation’s performance versus quantization.</td>
<td>44</td>
</tr>
<tr>
<td>5.4</td>
<td>The key generation’s performance versus purification coefficient.</td>
<td>45</td>
</tr>
<tr>
<td>6.1</td>
<td>Ensemble of channel impulse responses.</td>
<td>48</td>
</tr>
<tr>
<td>6.2</td>
<td>Lag-lag plot of channel impulse response measurements.</td>
<td>50</td>
</tr>
<tr>
<td>7.1</td>
<td>Time correlation, NLOS channel.</td>
<td>58</td>
</tr>
<tr>
<td>7.2</td>
<td>Block diagram of random beamformers.</td>
<td>61</td>
</tr>
<tr>
<td>7.3</td>
<td>CDF of observed estimation error versus Gaussian.</td>
<td>65</td>
</tr>
<tr>
<td>7.4</td>
<td>CDF of observed estimation error versus Wrapped Stable.</td>
<td>66</td>
</tr>
<tr>
<td>7.5</td>
<td>Normalized estimation error of eavesdroppers, analytical.</td>
<td>70</td>
</tr>
<tr>
<td>7.6</td>
<td>Normalized estimation error of eavesdroppers, simulation.</td>
<td>72</td>
</tr>
<tr>
<td>8.1</td>
<td>Adversaries’ positioning.</td>
<td>83</td>
</tr>
<tr>
<td>8.2</td>
<td>Block diagram of eavesdropper’s predictor.</td>
<td>84</td>
</tr>
<tr>
<td>8.3</td>
<td>Integrated bandwidths and multiple antenna security test.</td>
<td>87</td>
</tr>
<tr>
<td>8.4</td>
<td>Capable adversaries with ray-tracing knowledge.</td>
<td>91</td>
</tr>
<tr>
<td>8.5</td>
<td>Reconciliation security concern; LDPC rate: 9/10.</td>
<td>92</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

I would like to thank:

Drs. Michael McGuire and Stephen Neville, for their support and invaluable advice.

My supervisory committee for the insight they shared with me.

Dr. Xiaodai Dong and her research team for their collaboration in this research by providing the UWB measurements.
ناگان و رخوان، از حوزه‌های مبارک
سوی تو گذارند، تا چنان چنان
ست خیار سندی، برهنگای پر زندی
ازدل خودرا آندی، آسان تو شجاعان
آه که زندیرون، از درون سپیدی جوان
من سرمایه ورودان مست قومی سرگان
تیم و جهاد از عمر زندی مرده را حمایت
که نفس تو و هم می‌شویم بنتی جان

پیشگاه ابنا (ه.الف.علی)
DEDICATION

In memory of the brave men and women who were martyred in the summer of 2009 in Iran, for a silent protest against an election result.
Chapter 1

Introduction

Recently, interest has grown in the theory, development, and application of wireless channel characterization-based key generation (WKG) methods [2, 5, 58, 38, 23, 49, 62]. These methods allow two communicating parties, nominally Alice and Bob, to exploit the channel (or process) noise and electromagnetic reciprocity characteristics innate to point-to-point wireless communications channels to effect a mutually observable random information source, which can then support key generation. Done correctly this enables Alice and Bob to independently generate identical information theoretically secure secret keys. More fundamentally, WKG techniques provide an alternative to standard key distribution solutions in that the key is independently generated as opposed to being transmitted. Additionally, WKG provides a physical layer alternative to techniques such as [28], thereby allowing the resulting security properties to be assessed directly in terms of the known physics of wireless channels.

WKG techniques are particularly attractive in scenarios, such as wireless sensors networks, where the desire for strong security must be balanced against low levels of available power and the obvious risk that adversaries will seek to actively collect and reverse engineer radio transceivers, so the adversaries have access to all algorithms and any configuration information such as preshared information and keys. As WKG systems exploit the hard to predict portions of the wireless channel for their key material, they can, when properly designed, produce on-demand spatially-temporally specific keys. Hence, sensor nodes lost to adversaries cannot be used to compromise the remaining in situ network even when the adversary’s reverse engineering processes are assumed perfect, under the obvious caveat that the network is designed to never engage in any key reuse.
As with classic Diffie-Hellman key exchange [14], WKG approaches innately cannot provide direct solutions to cryptographic authentication\(^1\), as is the case with any approach that begins by presuming that Alice and Bob start by holding no information about each other that is guaranteed to be true (\textit{i.e.} that was obtained from a trusted source over a known tamper proof channel)\(^2\). Unlike Diffie-Hellman, when properly structured, WKG systems can directly address man-in-the-middle attacks through the enforcement, by physical laws, of an upper bound on the mutual information measurable by any eavesdropping third party, Eve [39].

To achieve authentication, WKG solutions can be easily augmented, for example, by including a standard public-key authentication step, as per [15], or by a query-response process, as outlined in [38, 60]. The distinction over approaches such as [15] is that under WKG, authentication and securing the communications\(^3\) channel exist as two completely independent steps (\textit{i.e.} that share no common information). As per [23], a bootstrapping process can also be used for authentication such that when Alice and Bob first establish a secure channel and then authenticate, as per the methods outlined above, all subsequent authentications for all subsequently established secure Alice-Bob channels are then performed using information arising from a prior secure channel. This has the advantage that all Alice-Bob authentication processes, outside of the initial authentication, then fall under the same information theoretic security proofs as the WKG process itself.

Fundamentally, WKG methods exploit two physical properties of wireless channels, namely: a) channel reciprocity and b) channel (or process) noise\(^4\). Reciprocity guarantees that Alice and Bob will each see (or observe) the same channel when they independently make concurrent (simultaneous) measurements of their shared wireless channel (\textit{i.e.} wireless channels are identical, independent of which end they are measured from). Reciprocity in point-to-point wireless channels is guaranteed by the physical laws of electromagnetics [51]. Channel noise guarantees that portions of

\(^{1}\)The term \textit{cryptographic authentication} is used in this context to clearly denote Alice and Bob’s need to each prove who the other is (\textit{i.e.} their identify) and not just the more limited case whereby an assurance exists that a secure Alice-Bob communications link has been established, the latter having been denoted as \textit{authentication} within portions of the prior WKG literature [38].

\(^{2}\)By definition, to authenticate Alice and Bob \textit{must} know some testable information about the other that \textit{cannot} be known to any attacker or man-in-the-middle [44] (\textit{i.e.} as per the Station-to-Station protocol’s presumption that the \textit{correct} public keys are known [15]).

\(^{3}\)Here, secure communication means a communication that is unreadable to any third party.

\(^{4}\)Channel noise indicates the reciprocal none-predictable portion of the channel measurements and thermal or measurements noise indicates the independent asymmetrical additive noises in the system.
Alice and Bob’s channel characterization measurements will exist as random noise. Hence, by definition, these portion of Alice and Bob’s measurements are *unpredictable* by any known theory (*e.g.* physical laws, communications, signal processing, *etc.*). Combined with reciprocity, this means that Alice and Bob’s measured channel process noise innately exists as a mutually observable random information source (*i.e.* a true random source as opposed to the common computer-based pseudo-random sources). By well known theory [31, 35], such sources can be used to support secret key generation *provided* the source can also be shown not observable to any eavesdropper.

Pragmatically, Alice and Bob can, of course, never measure their shared channel simultaneously and their measurements will always also be contaminated by their own independent local measurement noise processes. Hence, real-world WKG solutions must be augmented with error reconciliation, privacy amplification, and public discussion steps [43, 11]. This leads to obvious questions as to how these additional required steps impact the security of WKG solutions and their achievable secrecy rates (*i.e.* can poor designs lead to WKG security failures or untenable low secrecy rates?).

The security of WKG solutions rests on developing a provable level of assurance that any eavesdropper or collaborating set of eavesdroppers, jointly denoted as Eve, cannot, by any means available to them, deduce Alice and Bob’s key or collapse the key space to one that can be tractably searched. Radio propagation and information theory indicates that if Eve’s antenna(s) are located outside of $\lambda/2$ neighborhoods\(^5\) of Alice and Bob’s antennas then an *upper bound* exists on the mutual information measurable by Eve about the Alice-Bob channel [1]. Hence, theory denotes that secure WKG is nearly always possible (*i.e.* a non-zero secret key rate nearly always exists) [43]. Theory though does not guarantee that any Eve located outside of $\lambda/2$ will be *incapable* of measuring *any* information about the Alice and Bob channel.

Obviously, well known wireless propagation issues, such as shadow fading[65], constructive interference[54], *etc.*, can produce significant measurement correlations for Eve even when her antenna(s) is located well outside of $\lambda/2$ neighborhoods of Alice or Bob’s antenna(s). Hence, WKG systems must be carefully designed to ensure that Alice and Bob’s key material is *only* ever sourced from the unpredictable portions of the Alice-Bob channel. If this is not the case, then the critical problem arises that

---

\(^5\)The communications wavelength $\lambda$ can be directly calculated as $\lambda = c/f$, where $c$ is the speed of light in $m/s$ and $f$ is the radio carrier frequency in Hertz.
Alice and Bob may use a WKG implementation to generate a key that they presume is secret but which is known, in whole or in part, by Eve.

Obviously, from a security perspective, it must be assumed that Eve will make every effort to deduce Alice and Bob’s key or gain information that their key space is collapsed into one that can be tractably searched. In general this means that, if it conveys an advantage, Eve will employ:

i) multiple antennas,

ii) ray tracing,

iii) pre-characterization of the communications environment,

iv) advanced communications and optimal signal processing theory,

v) reverse engineering, etc.

Eve could also actively inject signals into the Alice-Bob communications environment (i.e. to seek to gain control or influence over Alice and Bob’s generated key). It can be shown for properly structured WKG systems that successful passive attacks (i.e. eavesdropping) is a necessary precursor to successive active attacks (i.e. the information required for successful active attacks must be gained through passive eavesdropping) [27]. Hence, evaluating security solely from the passive eavesdropping perspective suffices for such WKG systems. This is also consistent with the nature of the WKG security assessments presented in the bulk of the WKG literature. Unfortunately, though, the current WKG literature has tended to focus on passive Eves who are quite limited in their capabilities. To our knowledge a rigorous assessment of WKG security against capable and knowledgeable passive Eves, as defined in terms of i-v above, has not been provided to date.

This PhD research consists of two parts that are outlined below:

(I) first part of this research focuses on detailing the theoretical considerations in performing non-line-of-sight (NLOS) UWB channel characterization-based key generation, inclusive of

a) proposing a key generation system and secure key agreement protocol,

b) assessing the achievable key rates,

c) the impact on key rates by introducing multiple-input multiple-output (MIMO) systems,
d) the impact of beamforming on the eavesdropper’s capability of estimating Alice and Bob’s channel.

e) assessing the provable security against both passive and active adversaries.

(II) the second part of this research seeks to remedy the security deficiency of previous WKG systems which presumed incapable eavesdroppers in the environment. Therefore, this research uses real-world measurements to highlight how and why WKG system design issues can lead to compromises in the WKG system’s presumed security. Fundamentally, the second part of this PhD research can be seen as developing pragmatic upper bounds on achievable secrecy rates. In particular, it is shown that channel bandwidth, error correction coding, and the filtering of the channel probe information all play critical roles in an implemented WKG system’s security, with improper design choices leading to WKG systems that are susceptible to capable Eves. More particularly, the security of the proposed WKG system is assessed against an Eve who has:

a) surrounded Alice or Bob with a 24 antenna array,

b) perfectly synchronized her channel measurements with Alice and Bob’s key generation process,

c) complete knowledge of Alice and Bob’s key generation process, save their actual channel measurements,

d) knowledge of optimal signal processing techniques allowing her to make the best possible estimates of the Alice-Bob channel based on her measurements of that channel.

e) knowledge of a ray-tracing algorithm that provide her an estimate of major reflectors in the environment with 3 dB estimation error.

Assessing the security of WKG solutions in light of such a capable Eve enables a number of critical design issues to be highlighted, which if mis-implemented can lead to the generation of keys known to more pragmatic real-world Eves. Innately, as security is the end-goal it is insufficient to show that a given WKG approach is secure against some Eves. Instead, it must be shown that security exists for all likely Eves. Moreover, in WKG systems the subset of Eves for which the system’s security also becomes a function of the claimed secrecy rate, as upper bounds innately exist on achievable WKG secrecy rates. WKG implementations can of course produce
more key bits than their upper bounds denote, the problem being that these extra bits will be known to Eve. Hence, it is critical in the design of WKG solution that pragmatic upper bounds on the achievable secrecy rates against capable Eves be developed and, moreover, that formal assurances exist in any WKG implementation that its produced key bits are indeed secure (i.e. unknowable and unpredictable to any reasonably capable Eve). The Eve explored in this research is fully implementable, given that the work analyses real measurement data. The limitation as to the need to be security against such a capable Eve is, therefore, only with respect to whether or not real Alices and Bobs would be guaranteed to observes such an Eve and, thereby elect to fail safely.

1.1 Contributions

This research pragmatically approaches wireless secret key generation methodologies. It verifies the conventional theory of WKG systems (reciprocity, low temporal-spatial correlation of the wireless channel’s fast fading characteristics) by performing real measurements in UWB communications. The UWB measurements are then filtered for security tests over lower bandwidths. The goals of this dissertation are as follows:

- To propose a WKG algorithm for UWB communications.
- To propose a secure key consistency check algorithm.
- To verify the performance of the proposed WKG system with real UWB channel measurements.
- To propose a method for removal of shadow fading of channel measurements that is a predictable portion of channel measurements.
- To introduce random beamforming as a solution to the undesirable effect of high temporal correlation in stationary environments.
- To assess the security of the proposed WKG system (bounds on secret key rate) against capable eavesdroppers who employ a multiple antenna array, full synchronization, and optimal signal processing tools to compromise the security of the system.
- To formally analyse the security of the proposed WKG system.
1.2 Dissertation’s organization

This dissertation is organized as follows:

Chapter 1 includes an introduction and provides a brief background on wireless key generation. This chapter also states the contributions of this research and abstractly reviews the methodology used for analysing the security of the proposed system.

Chapter 2 reviews the previous work published in this area and compares this dissertation’s contributions with previously published literature.

Chapter 3 presents the UWB measurements obtained to support the claims of this dissertation. This chapter starts with presenting the scenarios under which the measurements are taken (for reciprocity, spatial correlation, and temporal correlation tests). Furthermore, the application of shadow fading removal technique of Chapter 6 is verified by applying this algorithm on the real measurements. The results of this chapter are then used to support the dissertation’s claims and concerns for developing a secure WKG system.

Chapter 4 discusses the bounds on the secret key rate of the proposed WKG system. In other words, this chapter explores the maximum number of secret key bits that can ideally be generated per UWB channel probe. The chapter includes information theoretic lower and upper bounds. Furthermore, the bounds are analytically calculated for the special cases of a white Gaussian multipath channel and a MIMO channel with independent Gaussian transfer matrix.

Chapter 5 proposes a WKG system. The proposed method contains standard communication and signal processing units. This chapter also includes a secure protocol for checking the consistency of the generated keys at both ends of the communication channel.

Chapter 6 proposes a shadow fading removal technique that discards the predictable portion of the channel measurements prior to the key generation procedure. The method is an optimal technique that measures the noise level of the measurements with a wavelet optimized method, then distinguishes and removes all predictable samples by comparing the prediction error of samples versus the
noise level of the measurement samples (the samples that have a smaller prediction error than noise level in the environment are removed prior to the key generation procedure).

Chapter 7 addresses the issue of high temporal correlation of the channel measurements in our stationary test environment by a combination of MIMO communication and random beamforming. The time correlation results of Chapter 3 show a high probability that sequential keys generated at exactly the same spatial locations but different time instances are highly correlated. From the aspect of system security, eavesdroppers can leverage this to compromise the security of the system by profiling the communication environment. The analyses of this chapter shows that by employing MIMO communication combined with random beamformers at Alice’s and Bob’s ends, Eve can be bounded to a certain estimation error level that does not permit her to compromise Alice and Bob’s generated secret key’s security.

Chapter 8 presents a security analysis of the proposed WKG system introduced in Chapter 5. It is shown that, in theory, passive eavesdroppers located outside the $\lambda/2$ radii (20 cm radii in our measurement tests) around each member of the communicating pair, are not successful if the WKG system is accurately designed. Active adversaries are also unsuccessful and can only jam the communication (either during channel measurements or public discussion), which makes them detectable in the environment. This chapter also analyses the security of WKG system against capable eavesdroppers in different signal bandwidths. Eavesdroppers employ a multiple antenna array, optimum signal processing techniques, and ray-tracing equipment to predict the wireless channel between a communicating pair. Although the spatial correlation between Eve’s measurements and Alice and Bob’s measurements is low (non-zero), Eve, in low bandwidths (e.g. 20 MHz), is able to regenerate most of the key bits that Alice and Bob generate (i.e. upper-bound on secret key rate is almost zero). This chapter also discusses how applying the shadow fading removal technique is critical to the security of WKG (e.g. in low bandwidths, 20 MHz, WKG fails for measurements where shadow fading is not removed).

Chapter 9 concludes the dissertation and proposed the open problems as the future work of this research.
Chapter 2

Literature Review

This chapter reviews the previous related work published in the area of WKG. The publish literature are categorized into two sections of Theoretical and Practical works. Then Section 2.4 compares different WKG techniques.

2.1 Theoretical work

The problem of secret key generation originated in Wyner’s seminal work on the “wire-tap channel” [59], where the secrecy capacity of a channel is derived. The secrecy capacity of the channel between two users Alice and Bob with respect to a third user Eve is the maximum data rate that Alice and Bob can communicate over the channel while keeping their message undecipherable to Eve. The problem of secret key generation is defined as the use of shared observations of a single source of random signal source in the generation of a mutual secret key by two users Alice and Bob, so that the key is unknown, in an information theoretic sense, to an eavesdropping third party Eve.

In 1978 Csiszar et al. [12] determined the so-called secrecy capacity of the additive white Gaussian noise (AWGN) channel in terms of the signal-to-noise ratios (SNRs) of the legitimate communicating users and eavesdroppers. Csiszer et al. [12] demonstrated that the secrecy capacity is greater than zero if the SNRs of the legitimate users, Alice and Bob, are higher than that of Eve.

Maurer [43] analyzed a modified system where, in addition to the main communications channel, the legitimate users Alice and Bob can communicate over an error-free public channel which is also observable by Eve. Maurer demonstrated that
with this arrangement the Alice and Bob may have a non-zero secrecy capacity even if the SNR for Eve’s observations of the main channel is superior to theirs in certain circumstances. The key to this surprising result is that Alice and Bob can use the public channel to resolve the differences in the bit sequences they obtain from their measurements of the main channel. Hence, Alice and Bob can improve the matching of their bit sequences without aiding Eve. Thus a “virtual” channel is obtained in which Alice and Bob have a superior SNR to Eve, leading to a non-zero secrecy capacity. In [1], Ahlswede et al. calculates the secrecy capacity of Alice and Bob when the public channel is only used to communicate in one direction.

Within [13], a secure communication system is proposed that uses a trusted helper terminal to provide Alice and Bob with the secrecy rate constraints of their communications channel over a public channel. With this help, Alice and Bob may tune their communication processes to obtain the maximum secure communications rate. The disadvantage of this technique is it introduces the helper terminal as a trusted third party hence, it is vulnerable to the same attacks as trusted third party key distribution techniques [14].

More recently, Maurer considered the case when malicious third parties have the ability to both read and write to the communications channel. It was demonstrated that, in this case, the secrecy capacity of the channel is either unaffected or reduced to zero [39, 40, 41]. If the eavesdropper, using only their measurement of the channel and knowledge of the channel statistics, can produce a simulated measurement of the communications channel for either Alice or Bob that has the same joint probability density function as the true measurements, then the secrecy capacity of Alice and Bob’s channel becomes zero. In other words, if Eve can generate an artificial measurement for Alice (or Bob) which Alice (or Bob) cannot statistically indistinguishable from the real measurement, then the Eve can completely remove the ability of Alice and Bob to communicate secretly or generate a common secret key. Conversely, if there exists a statistical method for Alice and Bob to distinguish any injected artificial measurements from the true measurements, then Eve cannot reduce Alice and Bob’s ideal secrecy capacity.

### 2.2 Practical work

Hassan et al. introduced a practical key generation systems for the memoryless Rayleigh fading channel model in which the received signal amplitude was used as the
common observable source of random information [31]. Although the fading characteristics of narrowband radio channels can indeed be used as a random information source, such systems exhibit a limited number of distinguishable paths. Hence, Eve may only need to search a tractably small key space. Hassan et al.’s approach did not make use of the public discussion method introduced in [43] and instead relied solely on Alice and Bob employing standard decoders to extract their common bits, thereby leaving the approach susceptible to local measurement noise (e.g. thermal noise, etc.).

Key generation by wireless channel characterization has been extended to wireless LANs though the work of Aono et al. [2] where signal strength measurement profiles were used as the common source of random information and public discussion was employed to address local measurement noise. Through this work Aono et al. extended the prior works by adding beam forming techniques to intentionally fluctuate the channel characteristics, presuming of course that electronically steerable array radiator antennas are available. Aono et al.’s theoretical results were also supported through a set of feasibility experiments. In [38, 62, 33], the authors use the Received Signal Strength (RSS) of wireless LAN cards as the mutual source of random information for secret key generation, with a secret key rate of 10 bit/sec being obtained in [38].

In [63], secret key generation was extended to the domain of multi-path fading characteristics of cellular radio channels. An important issue brought forward in Ye et al.’s work was the identification of a significant gap between the achieved secret key rate and its theoretical upper bound. The postulated reason for this gap was that the public discussion algorithm that was used [61] sacrificed a significant portion of the potential key bits in favor of error correction capabilities (i.e. key bits are sacrificed in order to increase the probability of key agreement).

Within [8] Bloch et al. introduced a four step procedure to ensure that key generation over a quasi-static fading channel is secure when it was assumed that the eavesdropper observes all communications through a second independent quasi-static fading channel. The security of the communications is estimated in terms of the average secure communications rate and the outage probability. It is shown that secure communications requires: (i) a commonly observable source of randomness, (ii) message reconciliation, (iii) privacy amplification, and (iv) encryption. The introduced reconciliation method was based on multilevel coding and optimized LDPC codes.
Within [49], Patwari et al. identified the major challenges of wireless channel characterization-based key generation as: (i) the management of non-simultaneous channel measurements by the legitimate communicating parties, (ii) the existence of correlated measurements, and (iii) the low achievable secret key rates (i.e. the insufficiency in a cryptographic sense of the resulting secret key). Patwari et al. introduced a framework for interpolating, decorrelating, and encoding Alice and Bob’s channel measurements though multi-bit adaptive quantization to address issues (i) and (iii).

Within [47], key generation has been extended to sensor networks, where a set of secure protocols that rely on simple network coding coding approaches become the basis for the key generation process. Hence, this work is distinct from the other works in that network coding is used to give rise to the key generation approach, as opposed to using the observed wireless channel characteristics.

Within the domain of UWB communications, secret key generation for outdoor UWB has been proposed in [5], based on the deep fade portions of the received signal profiles. As with a number of the prior works, a reconciliation process was employed to ensure key agreement. Wilson et al. have proposed an approach to secret sharing within indoor wireless channels [58] based on electromagnetic reciprocity. Wilson et al. considered various secret key sharing strategies and provided a qualitative assessment of the vulnerability of their secret sharing approach against nearby passive eavesdroppers. Wilson's method differs from this dissertation method in terms of performance and security analysis.

2.3 Taxonomy

The idea of using wireless channel characteristics to generate secret keys was introduced by Hassan et al. in [31], in which a practical WKG system for a memoryless Rayleigh fading channels was proposed. The information theory foundations for WKG having been previously developed by Maurer’s work on secret key generation and agreement from partially shared mutual information sources (i.e. where the analysis includes the effects of local measurement noise) [43]. Table 2.1 lists and compares a number of recent WKG works according to their key characteristics namely: their bandwidth, whether they are based on impulse response or received signal strength (RSS) measurements, whether they address shadow fading, their reconciliation method, and their antenna use (e.g. single, multiple, or beamforming).
<table>
<thead>
<tr>
<th>Ref.</th>
<th>Alice/Bob Antenna Structure</th>
<th>Bandwidth</th>
<th>Channel Probe Info.</th>
<th>Reconciliation Approach</th>
<th>Removal of Shadow Fading</th>
</tr>
</thead>
<tbody>
<tr>
<td>[31]</td>
<td>Single BB Impulse</td>
<td>Linear Coding</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[2]</td>
<td>Beamforming Array BB RSS</td>
<td>BHC Coding</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[5]</td>
<td>Single UWB Impulse</td>
<td>Fuzzy Logic</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[58]</td>
<td>Single UWB Impulse</td>
<td>Linear &amp; BHC Coding</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[49]</td>
<td>Single BB RSS</td>
<td>Linear Coding</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[38]</td>
<td>Single BB Impulse &amp; RSS</td>
<td>Level Quant.</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[64]</td>
<td>Array BB RSS</td>
<td>Linear Coding &amp; Level Quant.</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[8]</td>
<td>Single BB RSS</td>
<td>Linear Coding</td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[25]</td>
<td>Single UWB Impulse</td>
<td>Linear Coding</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[23]</td>
<td>Single UWB Impulse</td>
<td>Linear Coding</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[36]</td>
<td>Single UWB Impulse</td>
<td>Linear Coding</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[27]</td>
<td>Array UWB Impulse</td>
<td>Linear Coding</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2.1: Comparison of proposed practical WKG solutions, where: BB denotes broadband (i.e. $W > 1$ MHz), UWB denotes ultra-wide band (i.e. $W > 0.5$ GHz), RSS denotes received signal strength, and Impulse denotes impulse response.

2.4 Comparison

These prior works, in general, all follow the two step WKG process first proposed in [43]. In this process Alice and Bob first make independent measurements of their common random information source (i.e. their shared radio channel). Alice and Bob then each seek to remove the local measurement noise that inevitably contaminates their channel measurements. This noise removal process, termed reconciliation (or purification), has generally been addressed through the use of linear error correction codes [31, 2, 58, 23, 62]. Though, in [5], a fuzzy logic based reconciliation method was proposed. Additionally, in [62, 38, 49], a level quantization technique was applied in which reconciliation was performed through transferring the quantizer’s indices not used in key generation over a public channel between Alice and Bob. To perform reconciliation with linear error correction coding [23, 62, 58, 8], the syndrome infor-
information produced from Alice and Bob’s independent error correction processes are shared over the public channel.

Post-reconciliation, Alice and Bob each hold a set of jointly known key bits, portions of which may also be known to Eve. As per [7], privacy amplification can then be used to generate a final secret key knowable only Alice and Bob (i.e. the $M$ bit potential key is reduced to an $N$ bit actual key via cryptographic hashing whereby $N < M$). In general, it is still possible, after all these processes have been completed, that Alice and Bob will not hold identical key sequences. Hence, simple public discussion processes, as per [27], are then also generally required as a final step before the generated key can be used to support cryptographic operations. As WKG systems use Alice and Bob’s mutually observable channel (or process) noise as the source of the key material and the prediction of this noise exists as a long standing open communications theory problem, there are strong guarantees that the produced key bits are indeed random, as required by cryptography\textsuperscript{1}. Hence, stronger arguments as to the randomness of WKG generated keys exist than are available for the empirical tests that are generally applied to pseudo-random number generators\textsuperscript{52}.

Several different radio systems have been used in prior experimental validations of WKG techniques. More specifically, WKG has been demonstrated with commercially available narrowband and broadband systems [2, 38, 49, 62], as well as with laboratory-grade ultrawideband (UWB) equipment [5, 58, 23]. WKG using consumer-grade equipment has generally been based on received signal strength (RSS) channel measurements whereas experiments using laboratory equipment have tended to be based on the measurement of the full channel impulse response (CIR). An obvious concern in a real-world WKG implementations is that Eve could elect to obtain CIR-based measurements in cases where Alice and Bob have elected to restricted themselves to RSS measurements. As the CIR innately provides more channel information than RSS\textsuperscript{2}, this may provide Eve with an advantage. Hence, for the purposes of this work, Alice, Bob, and Eve are all be assumed to use CIR measurements, with the understanding that the developed bounds on secrecy rates, therefore, exist as loose upper bounds on the secret key rates of any Alice-Bob RSS-based WKG techniques.

\textsuperscript{1}Fundamentally, the randomness of the WKG produced key bit sequences rests firmly on well known well established communications theory, provided the WKG systems is itself properly structured.

\textsuperscript{2}As is well known, RSS is proportional to the CIR signal power, where within implementations the associated received signal strength indicator (RSSI) is only measurable for signal that exceed the radio’s sensitivity. Exact RSSI computation methods vary across vendors.
To retain security, WKG must exploit the hard to predict portions of the wireless channels as the sources for any key material. In narrowband and broadband systems this hard to predict portion comes from fast fading, which innately requires that a non-zero relative velocity must exist between Alice and Bob’s antennas (i.e. if Alice and Bob are motionless in a static environment then, by definition, no fast fading can exist). Hence, there exists a direct relationship between achievable secret key rates and Alice and Bob’s Doppler frequency, which determines the bandwidth of any fast fading process. WKG in static environments can be addressed through transitioning to UWB systems as a direct result of UWB ability to resolve narrowly spaced CIR components (i.e. to independently resolve multi-path rays that are closely spaced in time). This is not possible within narrowband and broadband systems due to their receiver’s innately applying low pass filtering which renders such systems only capable of measuring aggregations of multi-path rays. Additionally, due to Eve’s ability to use ray tracing, WKG security depends on the existence of multipaths that carrying significant signal energy and that are not easily deducible by Eve. WKG is largely not applicable to LOS communications since LOS path characteristics are easily predicted by an Eve applying known communications theory.

At GigaHertz carrier frequencies and UWB signal bandwidths then, presuming a reasonably rich multipath environment exists (i.e. a standard office environment), numerous NLOS propagation paths will be produced by small sub-centimeter reflectors in the environment. Knowledge of the orientations, compositions, exact locations, etc. of all such signal reflectors is required if Eve is to be able to deduce the process noise of the Alice-Bob channel (i.e. compute the channel through means such as ray tracing). The ability of UWB receivers to resolve the details of these propagation paths in combination with channel reciprocity allows UWB WKG to possess non-zero secrecy rates even in static environments. Moreover, as per [36], UWB WKG systems can be structured to test the environment to ensure that Alice and Bob only make use of secrecy rates that the NLOS environment itself supports (i.e. such that in pathologically trivial environments WKG fails safely). A general trade-off exist in WKG systems between communications bandwidth, Doppler frequency, and secret key rates, with narrowband and broadband WKG systems generally producing secrecy rates on the order of 10 key bits per channel probe [2, 38, 49, 62] whereas UWB approaches have been shown to produce > 100 key bits per channel probe [5, 58, 27].

A core issue within WKG systems is to ensure that all of the resulting key bits are only taken from these unpredictable portions of Alice and Bob’s channel, as the
worst-case scenario would involve Alice and Bob making use of a key they believe is security but which Eve knows. The standard assumption used within

This thesis will present rigorous arguments on the security of the WKG systems. Prior work on WKG security have been based on the assumptions that if Eve’s antennas are outside of $\lambda/2$ neighborhoods around Alice and Bob then Eve cannot obtain any information about the Alice-Bob channel\(^3\) Within [62], an ad hoc moving average based filtering technique was proposed to ensure that only fast fading induced portions of a time sequence of Alice’s and Bob’s RSS measurements were used to generate secret key bits. Although the fast fading component does produce unpredictable high frequency components in such sequences, no formal arguments were provide that only fast fading can produce high frequency components in such sequences, nor was the exact frequency specification of the fast fading process derived. Hence, it is difficult to formally assess whether the proposed moving average filter will remove all predictable portions and all portions of the signal which are measurable by any set of capable and knowledgeable eavesdroppers. The proposed moving average based filtering of [62] is known to be non-optimal; hence, even if the generated key material is known to only Alice-Bob, the reported secrecy rate is not optimal.

Within WKG systems it is important to provide assurance that successive keys are independent (i.e. that the WKG is not merely just regenerating the same key with every application of the key generation process). In general, this temporal correlation between keys relates directly to the coherence time of the wireless channel (i.e. the time duration over which the channel can be accurately modeled as unchanging). Within CIR-based WKG, correlations also exist between CIR components for different propagation delays. Care must be taken to remove such correlations, as per [36], as these can give rise to statistical dependencies between different bits in the generated key.

WKG systems require Alice and Bob to engage in public discussions to assess whether they generated the same secret key [20, 57]. These public discussions are vulnerable to active attacks (e.g. jamming) that prevent these public discussions from completing [39, 40, 41]. However, jamming is an issue common to all wireless communication processes. WKG systems though can be designed to fail safely in

\(^3\)This source of this assumption is the standard propagation modeling and communications literature where this assumption is correct for the channel properties of interest to communication systems designers. It is expressly not correct for all channel characteristics of interest for WKG solutions, as WKG seeks to exploit the unpredictable portions of the wireless channel that are not generally used for communications processes.
such cases\cite{27, 23}. Although the existence of WKG solutions with appropriate security properties has been well established in both theory and practice, the pragmatic issues involved in designing security WKG solutions in the presence of capable Eves has not been well studied to date. This thesis’s contributes an analysis of these issues and the methods of managing the negative effects of these factors on actual WKG systems.

### 2.5 Summary

This chapter classifies the previous work related to this dissertation’s topic into Theoretical and Practical sections and then presents a comparison studies between various WKG techniques.
Chapter 3

UWB Channel Measurements

In this chapter, the equipment and processes used to perform the UWB channel measurement experiments analyzed in this work are discussed, as are the specific experiment scenarios that were conducted. UWB channel measurements were selected as standard filtering techniques allow narrowband and wideband channel measurements to be derived from UWB channel measurements.

3.1 UWB Signal Characteristics

Indoor UWB is defined by the American Federal Communications Commission (FCC) as communications in the 3.1 GHz to 10.6 GHz band, where the bandwidth of the communications channel is at least 0.5 GHz. The FCC requires that the effective isotropic radiated power (EIRP) must be kept to less than $-41.3$ dBm/MHz [22]. Within our measurements UWB signals were produced in an indoor research laboratory environment with a center frequency of 4.0 GHz and a bandwidth of 2.0 GHz (i.e. an UWB signal covering the 3.0GHz to 5.0GHz band).

In our tests, the radio transmitter and receiver are synchronized via a direct cable connection, alleviating the need to correct for lags between the measured signals. The transmitter sends a trigger pulse to the radio receiver over a cable connection at the same time that it sends UWB pulse through the wireless channel. The receiver-side measurement equipment starts signal sampling upon reception of this trigger signal. Measurements were performed for both Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) propagation conditions.
A radio connection is classified as LOS when 60% or more of the first Fresnel zone between the transmitter and receiver antennas is unobstructed, otherwise, the radio connection is classified as Non-Line-of-Sight [32]. For our carrier frequency of 4.0 GHz, an obstacle blocking at least the 40% of the first Fresnel zone of the LOS path must have a minimum radius of \( r = 49.18 \) cm to create a NLOS channel when it 10 m from either antenna.

Table 3.1 lists the test equipment used for all experiments. Figure 3.1 shows the block diagram of the measurement apparatus setup. The parameters of the measurement equipment are¹:

- A data sampling rate of \( f_s = 40 \) GS/sec.
- A carrier frequency of \( f_c = 4.0 \) GHz.
- A vector signal generator output that was set to have 10 dBm power for an EIRP of \(-41\) dBm/MHz.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oscilloscope</td>
<td>Agilent DSO81004A</td>
</tr>
<tr>
<td>2</td>
<td>Arbitrary Waveform Generator</td>
<td>Tektronix AWG7052</td>
</tr>
<tr>
<td>3</td>
<td>Vector Signal Generator</td>
<td>Agilent E8267D</td>
</tr>
<tr>
<td>4</td>
<td>Microwave System Amplifier</td>
<td>Agilent 83017A</td>
</tr>
<tr>
<td>5</td>
<td>UWB Antenna</td>
<td>EM-6865</td>
</tr>
</tbody>
</table>

Table 3.1: The UWB wireless channel measurement test apparatus.

Figure 3.1: Block diagram of measurement apparatus experiment setup² [23].

In the radio receiver, the frequency down-conversion to baseband is performed digitally by multiplying the received signal by an ideal 4.0 GHz cosine signal. This

¹More details are available in my technical report [24].
down-sampled signal is then filtered with a low-pass Chebyshev filter to remove all out-of-band measurement noise. The low-pass filter specifications are:

- Double side bandwidth: $W = 1.0 \text{ GHz}$.
- Normalized passband edge frequency: $\omega_p = \frac{W/2}{f_s} = 0.025$.
- Normalized stopband ripple: $\omega_a = 2 \times \omega_p$.
- Maximum bandpass ripple: $A_p = 0.1 \text{ dB}$.
- Minimum stopband attenuation: $A_a = 60 \text{ dB}$.
- Filter order: 9.

To obtain a clean benchmark signal, as shown in Figure 3.2, the experimental apparatus was placed in an electromagnetic anechoic chamber and the received signal measured for a single signal transmitted from one antenna to the other. This benchmark profile was then used within the receivers matched filtering processes during the actual measurement experiments.

![Transmitted Pulse Shape](image)

**Figure 3.2:** Transmitted pulse shape as obtained via testing within an anechoic chamber [23].
3.2 Experimental Measurement Approach

In this section, a description of all the performed measurements is provided and the correlation coefficients among the different channel measurements are calculated. As the measurement noise is assumed ergodic, the correlation coefficients between channel measurements, $X(n)$ and $Y(n)$ can be estimated as:

$$\hat{\rho}_{XY} = \frac{A[X(n)Y(n)] - \bar{X}\bar{Y}}{\sqrt{\sigma^2_X \sigma^2_Y}} \quad (3.1)$$

where $A[\cdot]$ calculates the time average of its operand over all samples $n$, $\bar{X} = A[X(n)]$, $\bar{Y} = A[Y(n)]$, $\sigma^2_X = A[X^2(n)] - \bar{X}^2$, and $\sigma^2_Y = A[Y^2(n)] - \bar{Y}^2$. For Eq. (3.1) to provide the statistical correlation, it is necessary for the channel impulse responses to be both correlation and mean ergodic. Ergodicity is not a property that can be confirmed with experimental measurements so, as is typical with experimental measurements, it is assumed without proof [50]. In general, for WKG system correlation measurements to be meaningful, maximal correlations must be reported. As the experimental setup includes direct cabled measurement synchronization, the additional step of removing signal lags is not needed (otherwise required).

Additionally, correlation is only a measure of the linear relationship between two random signals. Hence, restricting the security analysis to reporting correlations also requires showing that no non-linear relationship exists between the measured signals. For the experiments reported within this work, these additional test for non-linear relations can be found in [36], where the lack of structure within lag-lag plots confirms the low likelihood that any non-linear mappings exist.

3.3 Testing for Alice-Bob Channel Reciprocity

This test measures the extent to which the measurements made for signals transmitted from Alice’s antenna, denoted as $A$, to Bob’s antenna, denoted as $B$, match those for signals transmitted from antenna $B$ to antenna $A$. Standard electromagnetic the-

---

3In Chapter 6, lag-lag plot of the channel measurements for both LOS and NLOS channels are presented. According to these results, it is reasonable to assume that correlation of the measurements has a linear structure.

4In general, prior works have presumed that correlation measures suffice to assess security without checking for the existence of any non-linear mappings, which from a security perspective is expressly insufficient.
ory indicates that the match should be perfect for linear channels, but in real-world transmitter and receiver systems non-linearities innately exist and can cause mismatches between the measurements. A set of measurements were made to determine the extent that reciprocity can be presumed to exist in this real UWB system. For this experiment set, all the measurements for a given set of antenna positions are made within the coherence time of the radio channel (i.e. the channel can be modeled as being statistically invariant between measurements). To ensure a reasonable channel coherence time, object movement in the radio propagation environment was minimized as much as possible during the measurement processes.

The Table 3.3 shows the calculated correlation coefficient results for the LOS and NLOS channels at different $A$ to $B$ antenna separations. In the LOS case, the results are averaged over 16 measurement sets, whereas in the NLOS case, the average is calculated over 64 measurement sets. The reported signal-to-noise (SNR) values were measured as the output signal to power ratio of the vector signal generator which acted as the modulated signal carrier.

<table>
<thead>
<tr>
<th>Distance (meters)</th>
<th>No. Experiments</th>
<th>SNR (dBm)</th>
<th>Correlation Coefficient $0 \leq \rho \leq 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16</td>
<td>10</td>
<td>0.974</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>30</td>
<td>0.927</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>30</td>
<td>0.908</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>30</td>
<td>0.933</td>
</tr>
<tr>
<td>10</td>
<td>16</td>
<td>30</td>
<td>0.904</td>
</tr>
</tbody>
</table>

Table 3.2: Measured averaged correlation coefficients between Alice and Bob’s channel measurements for LOS channels.

<table>
<thead>
<tr>
<th>Distance (meters)</th>
<th>No. Experiments</th>
<th>SNR (dBm)</th>
<th>Correlation Coefficient $0 \leq \rho \leq 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>64</td>
<td>10</td>
<td>0.998</td>
</tr>
<tr>
<td>4</td>
<td>64</td>
<td>10</td>
<td>0.987</td>
</tr>
<tr>
<td>6</td>
<td>64</td>
<td>10</td>
<td>0.910</td>
</tr>
<tr>
<td>8</td>
<td>64</td>
<td>10</td>
<td>0.959</td>
</tr>
<tr>
<td>10</td>
<td>64</td>
<td>10</td>
<td>0.965</td>
</tr>
</tbody>
</table>

Table 3.3: Measured averaged correlation coefficients between Alice and Bob’s channel measurements for NLOS channels.

The tables show that in all the examined cases, Alice and Bob’s channel measurements are highly correlated. Hence, the real-world UWB channel can be assumed to
be sufficiently reciprocal to support WKG provided that Alice and Bob make their measurements within the channel’s coherence time.

### 3.4 Testing for Spatial Correlations

The security of WKG approaches hinges on low spatial correlations existing between the Alice-Bob channel measurements and any measurements available to Eve. Hence, a systematic set of tests were done to determine the nature of the spatial correlation of the UWB signals with respect to the particular research laboratory setting in which these tests were conducted, where these fundamentally mimicked a standard open floor office environment. For these tests, Bob’s antenna was kept stationary while Alice’s antenna was moved systematically through the 25 points of a 5 by 5 grid centered at Alice’s original position. Each grid point was separated by 20 cm along both the grid rows and columns, as shown in Figure 3.3, where for the tested 4 GHz UWB bandwidth signal’s wavelength ranges from 10 cm down to 6.0 cm. At each grid point an ensemble of 10 independent channel measurements were collected (i.e. 10 independent channel probes were sent and received). Ensemble averaging was then performed to reduce measurement noise. During all spatial correlation test measurements movement in the radio propagation environment was minimized so that the differences between channel measurements arose primarily through the antennas’ spatial offsets.

![Figure 3.3: Spatial correlation measurement test point grid.](image)

The spatial correlation coefficients were then calculated comparing the channel probe information received from each offset experiment with the base experiment in which Alice was located at the center point of her grid. Spatial correlation was computed both before and after the shadow-fading removal process of [36] was ap-
plied\(^5\). The results of unprocessed spatial correlation tests for both the LOS and NLOS channels are shown in Figure 3.4 as the ensemble averaged spatial offset correlations. The center grid point denotes the measured auto-correlation computed across the 10 received channel probes of the base experiment; hence, it provides a measure of the degree of per-experiment variability resulting from any unaccounted for per-experiment noise.

It is clear from these raw spatial correlation tests that significant correlations exist well outside of $\lambda/2$ neighborhoods of the Alice’s antenna. More particularly, all of the test grid points are well outside of $\lambda/2$ neighborhoods of Alice’s center grid point. Some prior WKG claims [49, 62], all spatial correlation measurements should denoted uncorrelated signals (i.e. near zero correlation). Spatial correlations in the range of 0.71 can be seen to occur at distances that are many multiple of the carrier wavelength from the reference point which is in contrast to the near-zero correlation that is assumed by many prior works on WKG. These high spatial correlations at long displacement distances are believed to result from shadow fading within the communications environment, where shadow fading is caused by the existence of significantly sized reflectors and obstructions within the environment giving rise to signal paths with low attenuation. For the carrier frequencies under consideration, such reflectors could be objects such as filing cabinets, window frames, thermal pane windows, whiteboards, etc. Obviously, exactly which multi-paths are the result of shadow fading depends on both the antenna locations and the specifics of the given communications environment. Hence the algorithm to remove shadow fading must be tuned on a per-environment basis and expressly cannot be removed simply by using fixed filters with prescribed passbands.

It should be clearly noted that the presented spatial correlation values are for perfectly stationary antennas (i.e. Alice and Bob are not moving). Hence, the correlations between iterative channel probes conducted between moving Alice and Bob’s can be inferred in terms of the distance offsets that would be produced from the center grid point due to Alice and Bob’s relative velocity during time interval between any two sequential channel probes. The existence of high shadow fading correlations at significant distance offsets implies that high correlations could also occur between successive channel probes in the case when Alice and Bob have non-zero velocities.

Prior works have sought to address shadow fading through the use of moving average filtering under the presumption that shadow fading must exist as a lower band-

\(^5\)The shadow-fading removal method is outlined in Chapter 6.
width process than fast fading [49, 62]. In particular, these works focus on removing shadow fading effects between successive channel probe events for moving Alice and Bob terminals. Within the standard outdoor communications shadow fading literature [30, 65] such assumptions are reasonable given that the shadow fading reflectors and obstructions are at sufficiently large distances from the antennas that from the antenna to the objects creating the shadow fading antenna is nearly constant during the time period between two successive channel probe transmission times. Within indoor environments with moving antennas, the closer proximity of the objects creating the shadow fading implies that the bearing angles can change more rapidly between channel probe events. For example, a small movement in Alice and Bob’s position can result in two different faces of a filing cabinet being the major signal reflector between two successive measurement which can give rise to large difference in the observed shadow fading effect for the two measurements. Hence, shadow fading can give rise to high frequency information within sequential channel probe events. As such, shadow fading effects, therefore, cannot be guaranteed to be removed in arbitrary environments by the moving average high-pass filtering approaches of [49, 62]. Moreover, shadow fading effects are reasonably easy to predict (e.g. via ray tracing). Hence, their removal is critical if the WKG solution is to be secure. Within [36], adaptive linear prediction was proposed as an alternate approach to remove shadow fading within arbitrary environments, where the linear predictor’s innovation sequence is then used as the source of the key material.

Figure 3.5 shows the spatial correlation results for an NLOS channel after application of the adaptive linear prediction process of [36]. It can be clearly seen that the shadow fading effects have been reduced and channel measurements are now less correlated (i.e. the highest correlation coefficient is reduced to 0.28). As Alice and Bob draw their key material from their resulting innovation sequences, their key material comes from the portion that they could not predict from their past measurements. The full description of the channel measurements can be found in [24].

3.5 Testing for Time Correlation

Obviously, if Alice and Bob are to use WKG to iteratively generate secret keys then it is important to assess the degree of similarity which may (or may not) exist between successively generated keys. Within these temporal correlation experiments Alice and Bob were kept stationary (immobile) and movement within the communications
Unprocessed measurements, Antennae distance= 3 (m) [LOS]

<table>
<thead>
<tr>
<th></th>
<th>0.23327</th>
<th>0.3509</th>
<th>0.50737</th>
<th>0.2667</th>
<th>0.27974</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.51474</td>
<td>0.54502</td>
<td>0.07844</td>
<td>0.18546</td>
<td>0.25778</td>
</tr>
<tr>
<td></td>
<td>0.17557</td>
<td>0.64773</td>
<td><strong>0.99118</strong></td>
<td>0.17388</td>
<td>0.71677</td>
</tr>
<tr>
<td></td>
<td>0.37351</td>
<td>0.19247</td>
<td>0.053255</td>
<td>0.26494</td>
<td>0.26524</td>
</tr>
<tr>
<td></td>
<td>0.27779</td>
<td>0.10979</td>
<td>0.36535</td>
<td>0.035595</td>
<td>0.17715</td>
</tr>
</tbody>
</table>

(a) LOS channels including shadow fading.

Unprocessed measurements, Antennae distance= 3 (m) [NLOS]

<table>
<thead>
<tr>
<th></th>
<th>0.23242</th>
<th>0.61288</th>
<th>0.15419</th>
<th>0.26707</th>
<th>0.038053</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.066535</td>
<td>0.52027</td>
<td>0.31882</td>
<td>0.36208</td>
<td>0.27174</td>
</tr>
<tr>
<td></td>
<td>0.35427</td>
<td>0.21817</td>
<td><strong>0.99711</strong></td>
<td>0.32237</td>
<td>0.18006</td>
</tr>
<tr>
<td></td>
<td>0.25811</td>
<td>0.29123</td>
<td>0.14862</td>
<td>0.238</td>
<td>0.40423</td>
</tr>
<tr>
<td></td>
<td>0.50607</td>
<td>0.37214</td>
<td>0.44652</td>
<td>0.64841</td>
<td>0.45618</td>
</tr>
</tbody>
</table>

(b) NLOS channels including shadow fading.

Figure 3.4: Measured ensemble averaged spatial correlation coefficient prior to removing shadow fading effects.

Environment was minimized. Alice transmitted a channel probe pulse every 500 msec and the channel impulse response was recorded by Bob for each pulse. Correlation coefficients were then computed comparing the first channel impulse response measured at \( \tau = 0 \) with all subsequent impulse responses measured at \( \tau = k \times 500 \) msec for \( k = 1, \ldots, 2000 \). This temporal correlation measurement test was conducted for both LOS and NLOS propagation conditions, as shown in Figure 3.6. The dips in the measured temporal correlations in both figures when a person’s movement obstructs one of the main propagation path of the radio channel, thereby, causing a significant signal attenuation.
Innovation of measurements, Antennae distance= 3 (m) [LOS]

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.041891</td>
<td>0.053515</td>
<td>0.014695</td>
<td>0.043993</td>
<td>0.066895</td>
</tr>
<tr>
<td>0.096712</td>
<td>0.026681</td>
<td>0.069857</td>
<td>0.025692</td>
<td>0.12577</td>
</tr>
<tr>
<td>0.062281</td>
<td>0.071193</td>
<td>0.85347</td>
<td>0.029113</td>
<td>0.33757</td>
</tr>
<tr>
<td>0.039825</td>
<td>0.076316</td>
<td>0.039451</td>
<td>0.018645</td>
<td>0.043802</td>
</tr>
<tr>
<td>0.018636</td>
<td>0.0061136</td>
<td>0.079554</td>
<td>0.0037544</td>
<td>0.0093613</td>
</tr>
</tbody>
</table>

(a) LOS channels without shadow fading.

Innovation of measurements, Antennae distance= 3 (m) [NLOS]

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.13804</td>
<td>0.18926</td>
<td>0.0033091</td>
<td>0.071209</td>
<td>0.092184</td>
</tr>
<tr>
<td>0.029346</td>
<td>0.20561</td>
<td>0.011879</td>
<td>0.12474</td>
<td>0.095167</td>
</tr>
<tr>
<td>0.066835</td>
<td>0.12515</td>
<td>0.83112</td>
<td>0.03136</td>
<td>0.047996</td>
</tr>
<tr>
<td>0.013853</td>
<td>0.11228</td>
<td>0.019748</td>
<td>0.054343</td>
<td>0.28549</td>
</tr>
<tr>
<td>0.056119</td>
<td>0.0091248</td>
<td>0.081025</td>
<td>0.24344</td>
<td>0.16853</td>
</tr>
</tbody>
</table>

(b) NLOS channels without shadow fading.

Figure 3.5: Measured ensemble averaged spatial correlation coefficient with shadow-fading effects removed via optimal prediction of Chapter 6.

These temporal correlation results show that channel probe events offset in time are highly correlated even at time offsets of up to tens of minutes. Additionally, it is noticeable that LOS channel time correlation values are significantly higher than NLOS channel time correlation values. Moreover, it should be noted that although the time periods of the “dips” produced by movement within the environment may appear to be attractive for key generation because of the low time correlation values. Unfortunately, they result from the movement of objects, in this case people, which are large enough to obstruct the radio channel’s Fresnel zone. The movement of these
Fundamentally, the temporal correlation measurements show that in nearly static environments a high probability exists that successive WKG processes will produce keys that are nearly identical unless special care is taken. The spatial correlation tests show that modest movements of Alice’s and/or Bob’s antennas (or movement of objects within the environment) can result in the production of independent keys.
by successive WKG processes. These results show the security benefits that NLOS channels have over LOS channels within WKG processes. Hence, WKG solutions should be structured to guarantee that only NLOS channel information is used for key material. In sufficiently complex environments this also helps protect against ray tracing solutions as the number of multi-path reflectors that must be accurately modeled (i.e. their composition, shape, orientation, etc.) becomes intractably large for Eve to both measure and ray trace. This is of course tied directly to both the bandwidth and frequency range of the WKG system’s utilized communication channel. For the tested UWB system, Eve would be required to accurately model the majority of sub-centimeter reflectors that may exist within the Alice-Bob communication environment. In most real-world environments, these would occur in sufficient numbers to preclude Eve’s ability to ray trace all the paths which contribute significantly to the WKG system’s measurements. Moreover, in general, Eve must also repeat this modeling processes any time objects are moved, added, and/or removed from the environment to estimate Alice and Bob’s wireless communication channel.

3.6 Summary

The results of UWB channel measurements are presented to validate the proposed WKG system’s security. The test scenarios include: (a) Reciprocity, (b) Spatial Correlation, and (c) Temporal Correlation tests. The reciprocity test results show, with high degree of confidence, that our WKG system, regarding all nonlinear (non-ideal) communication elements in the system, is reciprocal. The spatial correlation test results reveal that in distances farther than $\lambda/2$ from the communicating pair’s antennas, there still exists a significant correlation in the fast fading of the channel measurements between the communicating pair’s and the eavesdropper’s channels. It is also shown that after applying the shadow fading removal technique of the Chapter 6 the spatial correlation decreased, but remains non-zero. The temporal correlation test results show a high degree of time correlation in our test environment. The random beamforming technique proposed in Chapter 7 is applied as a solution to this security problem.
Chapter 4

Secret Key Rate

The section describes the information theoretical basis of secret key generation for wireless communications. The electromagnetic reciprocity theorem allows two parties to use a radio channel as a source of common information. This theorem states that the channel response at point $A$ (Alice) from the stimulus at point $B$ (Bob) is the same as the channel response at point $B$ if the same stimulus is applied at point $A$. Hence $h_{AB}(t) = h_{BA}(t)$ where $h_{AB}(t)$ represents the impulse response of the wireless channel measured at point $B$ when the stimulus pulse transmitted at point $A$.

In practice, the terminals at $A$ and $B$ will not measure exactly the same signals due to the independent measurement noises. Therefore, the received measurements at $A$ and $B$ are $y_A(t) = h(t) * s(t) + n_A(t)$ and $y_B(t) = h(t) * s(t) + n_B(t)$ where $h(t)$ is the mutual channel impulse response, $*$ denotes convolution, $s(t)$ is the transmitted pulse, and $n_A(t)$ and $n_B(t)$ are the measurement and thermal noise at $A$ and $B$ points, respectively. The signals measured at a third point $E$, the location of an eavesdropper, are denoted as $y_{EA}(t)$ and $y_{EB}(t)$ for the signals transmitted from $A$ and $B$. For brevity, the time index $t$ will be dropped in the equations below unless it is needed. In the discussion below, the two legitimate users Alice and Bob will be assumed to be located at points $A$ and $B$, respectively, with the Eve located at point $E$.

The maximum amount of secret information that can be shared between Alice and Bob when Eve is observing the channel is called secret key rate, $S(y_A, y_B | y_E)$ where $y_E = (y_{EA}, y_{EB})$, and $I$ represents the mutual information operator [43].
4.1 Bounds on Secret Key Rate

For secret key generation from mutual observations of a random process, such as the channel impulse response, it has been proven in [42] that the secret key rate, $S(y_A, y_B | y_E)$, available to A and B over an open broadcast channel with respect to an eavesdropper E is upper bounded by

$$S(A, B | E) \leq \min \left[ I(y_A ; y_B), I(y_A ; y_B | y_E) \right] ,$$

(4.1)

and lower bounded by

$$S(A, B | E) \geq \max \left[ I(y_A ; y_B) - I(y_A ; y_E) , I(y_A ; y_B) - I(y_B ; y_E) \right] .$$

(4.2)

This bound becomes tight when no mutual information exists between the channel measurements available to the eavesdropper E and those of A and B. As stated above, this case is realized when the eavesdropper is sufficiently far away from the legitimate users. Obviously, in such cases, the theoretic secret key rate is maximized.

4.2 Simplified Model for Eve with independent measurements

If measurements $y_E$ are independent of $y_A$ and $y_B$ then the secret key rate becomes $I(y_A ; y_B)$. This bound is achievable in practical communications systems when the channel measurements at point E are not correlated with the measurements at points A and B. For example, in Chapter 3, it has been shown that for indoor UWB radio channels, the radio channels for two points separated by more than 20 cm are almost uncorrelated.

The secret key rate available from UWB indoor channel measurements is derived. The UWB channel for indoor communications is modeled based on the contents of the IEEE 802.15.4a standard. This standard is based on the Saleh-Valenzuela model [53] with parameters based on extensive field measurements. The UWB channel impulse response is modeled as

$$h(t) = \sum_{l=0} a_{k,l} e^{j\phi_{k,l}} \delta(t - T_l - \tau_{k,l}) .$$

(4.3)
where parameters of the model are defined as follows:

- $\tau_{k,l}$ indicates the arrival time of the $k$-th ray within the $l$-th cluster with respect to the arrival time of the first ray of cluster $l$.
- $T_l$ indicates the arrival time of the first ray of the $l$-th cluster.
- $a_{k,l}$ shows the amplitude of the $k$-th ray within the $l$-th cluster.
- $\phi_{k,l}$ denotes the phase of the $k$-th ray within the $l$-th cluster.

The distributions for the parameters of the model Eq. (4.3) are selected to fit the type of environment (e.g. indoor office, industrial, etc.) being simulated. The following assumptions are made to facilitate calculations of the mutual information:

- The terminals at points A and B are synchronized.
- The random variables $a_{kl}$ are independently distributed Gaussian random variables with zero means and variances of $\sigma_{a_{kl}}^2$. The variances values depend on the type of the environment.
- The stimulus pulse is given by $s(t) = E_s sinc(\pi f_s t)$, where $f_s$ is the sampling frequency.
- The sample time, $T_s$, is selected so that all propagation paths are resolvable.
- The measurement noises at A, $n_A(t)$, and B, $n_B(t)$, are additive white Gaussian noise random processes with zero mean and spectral density $\sigma_0^2/2$.

Figure 4.1 illustrates a set of simulated UWB channel based on 802.15.4a for an NLOS channel.

After sampling, the received measurements of A and B are given by the vectors,

$$
Y_A = \begin{bmatrix} y_{A,1} & \cdots & y_{A,i} & \cdots & y_{A,N} \end{bmatrix},
$$

$$
Y_B = \begin{bmatrix} y_{B,1} & \cdots & y_{B,i} & \cdots & y_{B,N} \end{bmatrix},
$$

where

$$
y_{A,i} = E_s a_i + n_A(i),
$$

$$
y_{B,i} = E_s a_i + n_B(i).
$$
Figure 4.1: A typical UWB channel power profile for a NLOS channel where $\Lambda = 0.0667$, $\lambda = 2.1, \Gamma = 24$, and $\gamma = 12$. It is calculated based on IEEE 802.15.4a standard’s model\textsuperscript{2} [23].

To reduce the sensitivity of key generation process to mismatches of phase or frequency between the local oscillators in A and B, it is recommended that key generation is performed on the magnitudes of the measurements within $y_A$ and $y_B$. The absolute value calculation creates a loss of information so the following key rate calculations only provide an upper bound on the available secret key rate when this operation is performed.

The mutual information is given by

$$I(y_A; y_B) = \sum_i I(a_i + n_A(i); a_i + n_B(i)).$$ \hspace{1cm} (4.4)

The received signal processes, $y_A(i)$ and $y_B(i)$ are jointly Gaussian random variables with zero means, $\sigma_0^2 + \sigma_{a_i}^2$ variance, and a correlation coefficient of

$$\rho_i = \frac{E_{2}\sigma_{a_i}^2}{\sigma_0^2 + E_{2}\sigma_{a_i}^2}.$$ \hspace{1cm} (4.5)

\textsuperscript{2}The model assumes that the rays and clusters arrivals follow Poisson arrival rates. $\lambda$ denotes the interarrival time rate of the rays within the clusters and $\Lambda$ denotes the interarrival rate of the clusters. Since many rays exists per cluster $\lambda \gg \Lambda$ can be assumed. Furthermore, the model assumes that the mean square of rays amplitude, $\sigma_{a_i}^2$, decrease monotonically within the cluster arrival time and the rays interarrival time. $\Gamma$ and $\gamma$ are known as power decay factors for clusters and rays, respectively.
The mutual information of jointly Gaussian random variables is given by [21],

$$I(y_A(i); y_B(i)) = \frac{1}{2} \log_2 \left( \frac{1}{1 - \rho_i^2} \right). \quad (4.6)$$

The total mutual information is given by,

$$I(y_A; y_B) = \sum_i \frac{1}{2} \log_2 \left( \frac{1}{1 - \rho_i^2} \right), \quad (4.7)$$

where $\rho_i$ is a function of channel path gains, $\sigma_{ai}^2$.

By using the power profile of Figure 4.1 then $\rho_i$ parameter of Eq. (4.7) can be calculated for different Signal power to Noise power Ratio (SNR), $SNR = E_s^2/\sigma_0^2$. The SNR for secret key generation can be significantly different from the SNR of Alice and Bob communications receivers since $E_s^2$ may be larger than the communications symbol power. Figure 4.2 shows the secret key rate per use of the UWB channel for the power profile of Figure 4.1.

![Secret Key Rate per use of the channel](image)

Figure 4.2: Secret key rate per use of the channel versus SNR for the simulated power profile of Fig. 4.1. It is calculated based on Eq. (4.7) [27].

### 4.3 Nontrivial Upper-bound on Secret Key Rate

In [43], the upper-bound on secret key rate is calculated. For the case that $y_A$, $y_B$, and $y_E$ are Alice’s, Bob’s, and Eve’s observations from a mutual source of information (i.e. wireless communication channel), this upper-bound is $I(y_A; y_B | y_E)$. To
extract an analytical equation for the upper-bound of secret key rate, it is assumed that the random variables $y_A, y_B,$ and $y_E$ are jointly Gaussian random variables where $E[y_A y_B] = \rho_0, E[y_A y_E] = E[y_B y_E] = \rho, E[y_A^2] = E[y_B^2] = \sigma_0^2, E[y_E^2] = \sigma^2,$ and $E[y_A] = E[y_B] = E[y_E] = 0,$ where $E[\cdot]$ denotes the expectation operator.

According to mutual information definition,

$$I(y_A; y_B | y_E) = E\left[ \log_2 \left( \frac{f(y_A y_B | y_E)}{f(y_A | y_E) f(y_B | y_E)} \right) \right] = -\frac{1}{2} \log_2 (1 - \rho_{y_A y_B | y_E}^2), \quad (4.8)$$

where $f(.)$ represents the probability distribution function of its input random variables, and $\rho_{y_A y_B | y_E}$ denotes the correlation coefficients between random variables $y_A$ and $y_B$ given $y_E = y_E$.

In [48], the covariance matrix for $f(y_A, y_B | y_E = y_E)$ is given as

$$C_z = \sigma_0^2 \begin{bmatrix} 1 - \rho^2 & \rho_0 - \rho^2 \\ \rho_0 - \rho^2 & 1 - \rho^2 \end{bmatrix}. \quad (4.9)$$

Consequently, the correlation coefficient of $y_A$ and $y_B$ given $y_E = y_E$ will be

$$\rho_{y_A y_B | y_E} = \frac{\rho_0 - \rho^2}{1 - \rho^2}. \quad (4.10)$$

Substituting Eq. (4.10) in Eq. (4.8) gives the secret key rate as follows:

$$I(y_A; y_B | y_E) = \log_2 \left( \frac{1 - \rho^2}{\sqrt{(1 - \rho_0)(1 + \rho_0 - 2\rho^2)}} \right). \quad (4.11)$$

4.4 MIMO effect on secret key rate

To consider MIMO communications, we assume the legitimate pair of transceivers, Alice and Bob, each has an array consisting of $N$ antennas. Therefore, Alice and Bob transmit the length $N$ vector of functions $s(t)$ on their antennas where entry $i$ of $s(t)$, denoted $s_i(t)$, is the signal transmitted on antenna $i$. The multiple channels between Alice and Bob are characterized by the $N$ times $N$ matrix of functions $H_{AB}(t)$ where
the entry on row \(i\) of column \(j\) of \(H_{AB}(t)\), denoted \(H_{ij}^{AB}(t)\), is the impulse response of the channel from antenna \(j\) of A to antenna \(i\) of B. It is assumed that Eve measures the wiretap channel impulse response matrices \(H_{AE}(t)\) and \(H_{BE}(t)\) when Alice and Bob transmit, respectively. The following represent Alice, Bob, and Eve measurements during Alice and Bob communications:

\[
\begin{align*}
    x(t) &= H_{BA}(t) * s(t) + n_A(t) \quad (4.12) \\
    y(t) &= H_{AB}(t) * s(t) + n_B(t) \quad (4.13) \\
    z_1(t) &= H_{AE}(t) * s(t) + n_{E1}(t) \\
    z_2(t) &= H_{BE}(t) * s(t) + n_{E2}(t)
\end{align*}
\]

The vector functions \(n_A(t)\), \(n_B(t)\), \(n_{E1}(t)\), and \(n_{E2}(t)\) are measurement noise functions where all function entries are assumed to be independent additive white Gaussian noise processes. In the equations above, the \(*\) symbol denotes the ‘matrix-vector convolution’ operator which is analogous to matrix-vector multiplication with the multiplication operation replaced with time-domain convolution (\(i.e.\) if \(c(t) = A(t) * b(t)\) then \(c^k(t) = \sum_{i=1}^{N} A^{k,i}(t) * b^k(t)\) where \(N\) is the number of columns of \(A(t)\) and entries of \(b(t)\)). Electromagnetic reciprocity guarantees that \(H_{AB}(t)\) is the transpose of matrix \(H_{BA}(t)\) so the transfer function from transceiver from Alice to Bob is a deterministic function of the transfer function from Bob to Alice.

To simplify the calculations of common information, we can define the vector \(h_{AB}(t)\) as a reordering of the \(N \times N\) matrix \(H_{AB}(t)\) into an \(N^2 \times 1\) vector. The three vectors \(\hat{h}_{AB}^A(t)\), \(\hat{h}_{AB}^B(t)\), and \(\hat{h}_{AB}^E(t)\) are defined as the estimates of \(h_{AB}(t)\) by the terminals Alice, Bob, and Eve respectively.

### 4.4.1 Calculate the non-trivial lower bound

The secret key bits that can be generated by Alice and Bob with respect to eavesdropper Eve is bounded by

\[
S(A, B \mid E) = \max \left\{ I \left[ \hat{h}_{AB}^A(t), \hat{h}_{AB}^B(t) \right] - I \left[ \hat{h}_{AB}^A(t), \hat{h}_{AB}^E(t) \right], \right. \\
\left. I \left[ \hat{h}_{AB}^B(t), \hat{h}_{AB}^E(t) \right] - I \left[ \hat{h}_{AB}^B(t), \hat{h}_{AB}^E(t) \right] \right\}. \quad (4.14)
\]
Define $Q_A$ as the covariance of $\hat{h}_A^{AB}(t)$, $Q_B$ as the covariance of $\hat{h}_B^{AB}(t)$, $Q_E$ as the covariance of $\hat{h}_E^{AB}(t)$, $C_{AE}$ as the cross-covariance of $\hat{h}_A^{AB}(t)$ with $\hat{h}_E^{AB}(t)$, and $C_{BE}$ as the cross-covariance of $\hat{h}_B^{AB}(t)$ with $\hat{h}_E^{AB}(t)$. The mutual information between the two vectors is given by

$$I\left\{\hat{h}_A^{AB}(t), \hat{h}_B^{AB}(t)\right\} = \frac{1}{2} \log_2 |Q_A| - \frac{1}{2} \log_2 |Q_B - C_{AB} Q_B^{-1} C_{AB}^H|.$$

(4.15)

where it is assumed that all impulse responses are Gaussian random processes [21]. If we assume that $Q_A = Q_B = Q$ and the correlation between each entry of $\hat{h}_A^{AB}(t)$ and the corresponding entry of $\hat{h}_B^{AB}(t)$ is given by $\rho$, then $C_{AB} = \rho Q$. The mutual information given above is then calculated as

$$I\left\{\hat{h}_A^{AB}(t), \hat{h}_B^{AB}(t)\right\} = \frac{1}{2} \log_2 |Q| - \frac{1}{2} \log_2 |Q - \rho Q Q^{-1} Q^H\rho|$$

$$= \frac{1}{2} \log_2 |Q| - \frac{1}{2} \log_2 \left|(1 - \rho^2) Q\right|$$

$$= \frac{1}{2} \log_2 |Q| - \frac{1}{2} \log_2 \left[(1 - \rho^2)^N |Q|\right]$$

$$= \frac{N^2}{2} \log_2 \left(\frac{1}{1 - \rho^2}\right).$$

(4.16)

The identity that $|cD| = c^K |D|$ when $c$ is a constant and $D$ is a $K \times K$ matrix is used to simplify the result above. The $N^2$ factor in the number of secret key bits is independent of the form of the covariance matrix $Q$.

The expected number of secret key bits that terminals Alice and Bob may generate is the mutual information between $\hat{H}_A^{AB}(t)$ and $\hat{H}_B^{BA}(t)$ where $\hat{H}_A^{AB}$ is the estimate of $H_{AB}(t)$ by terminal B from $y(t)$ and $\hat{H}_B^{BA}(t)$ is the estimate of $H_{BA}(t)$ by terminal A from $x(t)$. If the pairwise antenna impulse responses in $H_{AB}(t)$ are independent Gaussian processes then the mutual information is calculated as the sum of the mutual information of the measured individual responses at each side. The independence assumption is applicable to practical systems since MIMO systems are designed so the impulse response for each antenna is subject to independent fast fading [29]. It can be seen from Eq. (4.16) that the number of secret key bits that can be generated per use of key generation protocol for a given pair of transceivers each with $N$ antennas is proportional to $N^2$. This is in contrast to MIMO secrecy capacity which is
proportional to $N$ [29] because the above calculation has been reported for each use of key generation protocol$^3$.

**Theorem 4.4.1.** Assume a MIMO WKG system, where Alice and Bob each using an array antenna of size $N$ to measure the MIMO communication channel with $H_{AB}$ transfer matrix of size $N \times N$. Also assume that

- Alice’s, Bob’s, and Eve’s estimations from $H_{AB}$ are $\hat{H}_{AB}^A$, $\hat{H}_{AB}^B$, and $\hat{H}_{AB}^E$, respectively.
- $a = \text{Reshape}(A)$ represent the operation of reshaping an $N \times N$ matrix $A$ to $N \times 1$ vector $a$.
- $\hat{h}_{AB}^A = \text{Reshape}(\hat{H}_{AB}^A)$, $\hat{h}_{AB}^B = \text{Reshape}(\hat{H}_{AB}^B)$, and $\hat{h}_{AB}^E = \text{Reshape}(\hat{H}_{AB}^E)$.
- $\hat{h}_{AB}^A$, $\hat{h}_{AB}^B$, and $\hat{h}_{AB}^E$ are zero mean Gaussian vectors, where $E\left[\hat{h}_{AB}^A (\hat{h}_{AB}^A)^T\right] = Q$, $E\left[\hat{h}_{AB}^B (\hat{h}_{AB}^B)^T\right] = Q$, and $E\left[\hat{h}_{AB}^E (\hat{h}_{AB}^E)^T\right] = Q_E$.
- $E\left[\hat{h}_{AB}^A (\hat{h}_{AB}^B)^T\right] = \rho Q$. 
- $E\left[\hat{h}_{AB}^A (\hat{h}_{AB}^E)^T\right] = \rho_{AE} Q_E$, and $E\left[\hat{h}_{AB}^B (\hat{h}_{AB}^E)^T\right] = \rho_{BE} Q_E$.

Then the lower bound on secret key rate is given by

$$S(A, B| E) = \frac{N^2}{2} \max \left\{ \log_2 \left( \frac{1 - \rho_{AE}^2}{1 - \rho^2} \right), \log_2 \left( \frac{1 - \rho_{BE}^2}{1 - \rho^2} \right) \right\}. \quad (4.17)$$

**Proof.** By expanding the result of Eq. (4.16) for wire-tap channel and substituting them in Eq. (4.14), Eq. (4.17) is deduced. \qed

### 4.5 Summary

The bounds of the secret key rate are extracted. The upper bound is derived analytically for a non-trivial Gaussian communication channel. The impact of MIMO communications on the secret key rate (lower bound) is also studied.

$^3$It should be noticed that in each key generation, the transmitter (or the receiver) independently probes the channel for each antenna of its array ($N$ probes for an array of size $N$).
Chapter 5

Secret Key Generation Method

In practice, channel measurements are contaminated with inevitable measurement noises that cause discrepancies at Alice’s and Bob’s generated bit streams. Therefore, a key generation algorithm must be employed to a) remove the discrepancies while b) preserving the security of the mutual source.

5.1 Key Generation

In this section, the step-by-step key generation process is introduced. In this system, amplitude of the received signal $r(t)$ is used as the source of mutually observable information of the communications pair. Figure 5.1 shows the block diagram of the key generation system. The procedures of this method are as follows:

1. Alice and Bob both independently transmit the publicly known pulse $s(t)$ over the wireless channel within the coherence time of the channel.

2. Alice and Bob sample their received signals after they are down-converted to the baseband and then processed by matched filters tuned to $s(t)$.

3. Alice and Bob digitize the output error pattern of their employed predictors by applying a $\Sigma - \Delta$ A/D converter\(^1\).

\(^1\)An ideal $\Sigma - \Delta$-A/D converter uses a linear predictor on an oversampled signal and then performs single bit quantization on the resulting prediction error. This has been shown to provide excellent quantization performance [9]. Additionally, the single bit quantization processes used by $\Sigma - \Delta$ converters are known to produce signal dependent quantization noise which, of course, is advantageous for key generation.
4. Alice runs a random interleaving algorithm over the bit stream created by the prior step and transmits the permutation order to Bob over the public channel. The permutation ensures that the bits common to both Alice and Bob are uniformly distributed over the generated bit stream.

5. Bob interleaves his received bit stream with the same order as was used by A.

6. Alice and Bob independently divide their generated bit string into $M$ blocks of length $n$ bits, where $n$ is the codeword length of the selected error correction code.

7. For each block of the bit stream of Step 5, both Alice and Bob perform decoding and one of them sends the correction vector for that block to the other side over the public channel [10]. In Figure 5.1, Bob sends correction information to Alice.

8. Alice and Bob then perform error correction on their own blocks and independently choose the maximum likelihood codeword associated with their generated block.

9. Alice and Bob independently compute the $k$-bit message associated with their computed maximum likelihood codeword and concatenate these $k$-bit blocks to form their available key bits.

Step 7 performs information reconciliation based on the sub-optimal proposed protocols in [10]. At the end of Step 9, Alice and Bob both hold sequences of $M$ code blocks. Due to the limits of the error correction code, there may exist a subset of blocks for which Alice and Bob disagree. These can be identified and discarded through a public discussion process of Section 5.2.

Post public discussion, Alice and Bob now each hold a common string of bits some of which may be known to the eavesdropper, Eve, due to the non-zero correlation of E’s channel measurements. As long as this correlation is sufficiently low, as in UWB when Eve is outside of the 20 cm radii, then Alice and Bob will be guaranteed to jointly hold a number of bits unknown to Eve.

The well known approach of privacy amplification can then be used to allow Alice and Bob to create a secret key that is unknown completely to Eve [7]. The goal of privacy amplification is to ensure that the only option left to Eve is a brute force searching of an infeasible large key space. This is done through Alice (or Bob)
choosing, at random, a hash function from a publicly known and sufficiently large set of universal hash functions. This function is then applied to the full set of known common bits held by Alice (or Bob). This hash is information lossy in that it results in a shorter key being produced. Alice (or Bob) then exchanges a description of the selected hash function over the public channel to Bob (or Alice) allowing the other to apply the same hash. Hence, Alice and Bob arrive at a commonly held secret key unknown to Eve. The appropriate hash can be easily selected by the knowledge of the length of the commonly held bits and, the presumed correlation of Eve’s channel measurements.
5.2 Public Discussion to Ensure Key Consistency

It is fully possible, depending on the nature of the local noise sources or active adversaries spoofing attack over the public discussion process (Step 7 of the Key Generation algorithm of Section 5.1), that Alice and Bob may decode their received blocks to different code words, which would then result in mismatches between their generated secret keys. Therefore, Alice and Bob need to engage in a public discussion process to ensure that $K_A = K_B$ prior to using the independently generated keys as a shared secret key.

As Figure 5.2 shows, this check can be performed via the following three step public discussion process, which has been validated through the AVISPA [3], automated validation of internet security protocols and applications.

![Figure 5.2: Block diagram of Key Validation (Public Discussion) Process [25]](image)

1. Bob selects a random real number $R$, encrypts it with its own key $K_B$, and sends the encrypted value $E_{K_B}[R]$ over the public channel to to Alice, where $E_K[.]$ is encryption operator with key $K$.

2. Alice decrypts the $E_{K_B}[R]$ signal received from Bob with the local $K_A$ key, then hashes the result with a secure one-way hash function $H(\cdot)$ producing $H(D_{K_A}[E_{K_B}[R]])$, where $D_K[.]$ denotes decryption with key $K$ and $H(\cdot)$ denotes...
a publicly known secure one-way hash function. Alice encrypts the result of the
hash function with its local key, $K_A$, and sends the resulting string over the
public channel to Bob.

3. Bob decrypts the received signal $H(D_{K_A}[E_{K_B}[R]])$, with the local key, $K_B$. If
the result is $H(R)$ then Bob sends an ‘OK’ acknowledgment message to Alice
confirming that $K_A = K_B$. Otherwise, if the result is not $H(R)$ then Bob knows
that $K_A \neq K_B$ and Bob then signals Alice that the key generation process has
failed and must be repeated.

The functions, $E_K[.]$, $D_K[.]$, and $H(.)$ are all assumed to be publicly known.
Additionally, the random seed $R$ must not be reused in order to preclude replay
attacks.

5.3 Performance

Section 5.1 presents algorithms for generating secret keys from channel measurements
in UWB systems [25]. This section applies these algorithms to the measurements
described in the Chapter 3 to see how many secret key bits are obtainable from these
channel measurements.

The simulation process is as follows: Each transceiver sends a pulse to the other
transceiver to be used for channel measurements. Each transceiver filters the received
signal with filter matched to the transmitted channel sounding pulse to reduce mea-
surement noise. The filtered signal on each side is then fed into a quantizer to convert
the signals into binary data vectors. This binary data is then reordered with pub-
lic permutation algorithm. In our observation, typically, we obtained 2000 samples
from a channel measurement so that the number of available bits for key generation
from a single channel measurement, using a 5 bit quantizer, approximately is 10000
bits. Finally, the public discussion is facilitated through as discussed by detail in
Section 5.1.

As reported in Figures 5.3 and 5.4, the disagreement probability, cost of key
generation process, increases monotonically along desired key length. For instance if
Hamming (7, 4) code is used at the decoder of Figure 5.1 then maximum available
key length is taken by $4 \times 10000/7$ where approximately is 5714. Generating such a
large key is not impossible but the probability of disagreement is almost one.
Using the public discussion method of Figure 5.1 with Hamming (7, 4) decoder, the probability of disagreement is calculated for different levels of quantization in Figure 5.3. Suppose that the output of the matched filter is $y_{m_i}$ where $i = a, b$. Here, the samples with the amplitude less than $C\sqrt{\text{Var}(y_{m_i})}$ are removed from the stream for both transceivers where $\text{Var}(\cdot)$ denotes the variance of input averaged over all samples. We call this signal purification and the coefficient $C$ is called the purification coefficient.

Figure 5.4 presents results for the use of different levels of purification for 5-bit quantization. Increasing the purification level means that the more samples in an observation are throwing out. Therefore, the number of available samples for the key generation process is reduced but the remaining samples (those are not eliminated during purification) are more likely to agree.

![Figure 5.3: probability of disagreement of LOS measurements for various key length values and different quantization levels; quantization levels are in bits. The purification coefficient is set to 0.5 in these results [23].](image)

Figure 5.4 shows that for larger values of the purification coefficient the probability of disagreement decreases.

The results verify that the algorithm proposed in Section 5.1 works with real data.
Figure 5.4: probability of disagreement of LOS measurements for various key length values and different purification coefficient. The signal is quantized with 5 bit quantizer [23].

5.4 Summary

A secret key generation algorithm for extracting secret keys via UWB channel characterization is proposed. A secure key consistency check algorithm is also proposed, through which the communicating pair can be certain that their generated keys are matched. Finally, the performance of the algorithm is evaluated with real UWB channel measurements.
Chapter 6

Removing Shadow Fading

In Chapter 5, it has been shown that UWB channel characterizations can be used as a source of common mutually observable random information by which a given pair of communicating parties, Alice and Bob, can generate a secret key in a manner that is secure versus eavesdropping.

The experimental measurements of Chapter 3, as is shown in Figures 3.5 and 7.1, clearly illustrate a high degree of time correlation occurs in both LOS and NLOS cases for indoor environments, such as a research laboratory setting, which are innately highly static environments (i.e. environments in which the majority of physical change involves people walking through the environment relatively sporadically). Hence, if ideal attackers is assumed to exist (i.e. one that is defined as having access to an oracle by which all past Alice to Bob channel characterization can be obtained perfectly), then this attacker will be able to either: (a) accurately predict the next key that Alice and Bob will generate or (b) when the issue of Alice’s and Bob’s local noise sources is included, only need to search a relatively small space to determine the key.

The relatively obvious approach to solve this innate problem is to introduce channel prediction into Alice’s and Bob’s key generation process. More particularly, Alice and Bob are assumed to hold all past channel characterizations and to implement a set of predictors that run across this ensemble to determine how predictable each time based sample of the next channel characterization process will be. If the given sample is highly predictable from past channel measurements (i.e. the sample arises primarily via the major static reflectors within the environment), then this sample is discarded and not used in the subsequent key generation process. Hence, the key bits are only extracted from the channel impulse response samples that have low predictability. Of course, it would be possible to replace the predictable portions of
the channel’s impulse response with the prediction filter’s innovation (\textit{i.e.} prediction error) sequence, but this presumes that the selected filter exists as the optimal prediction filter, whereas if this cannot be assured it can be argued that it is better to just discard predictable samples.

Three issues arise with respect to this proposed approach, namely: (a) the exact nature of the prediction filter must be selected (\textit{e.g.} linear, non-linear, \textit{etc.}), (b) the methodology by which the predictability threshold is set must be determined, and (c) it must be shown that the innate requirements of the approach are likely to exist within real-world settings. Sections 6.1 and 6.3 of this chapter will address questions (a) and (c). With respect to question (b) it can be observed that the required threshold can be constructed by calculating the distribution of prediction error variance. If the prediction error variance of the ensemble is larger than a set threshold then that ensemble will be kept for key generation otherwise the ensemble will be discarded. How this can be done is addressed in Section 6.1.

Hence, overall the following process can be applied to allow Alice and Bob to employ prediction to improve the temporal security of the key generation process.

(i) Alice and Bob retain a history of past impulse response measurements.

(ii) Alice and Bob engage in a new channel characterization process as per [27].

(iii) Alice and Bob independently apply the wavelet-based measurement noise estimation process, to be discussed in Section 6.1, to determine the measurement noise SNR and to denoise their received signals.

(iv) For each channel characterization, Alice and Bob independently apply an ensemble prediction filter across the store impulse response history to determine which samples from the current impulse response measurement are highly predictable (\textit{i.e.} in the sense that the variance of the ensemble prediction error is less than a certain threshold).

(v) Alice and Bob independently remove the samples from their current impulse response measurements that have been determined to have high predictability.

(vi) Alice and Bob proceed with key generation use the remaining impulse response samples, as per [27].
(vii) Should Alice or Bob have determined that all samples of the impulse response were predictable, then Alice or Bob can initiate a public discussion to either: (a) generate a new impulse response, hopefully that possesses less predictability, or (b) reduced the required threshold to preserve the ability to perform key generation but with a known weakening of the secrecy of the generated key.

It should be noted that the key generation process expressly focuses on the portion of the channel characterization that has the highest degree of non-stationarity and, hence, the portion that would expressly not be used for communications. Additionally, Alice and Bob do not necessarily communicate over this portion of the channel, they only perform channel characterization of this portion; instead, the fast fading portion of the channel exists as the “signal” of interest.

Figure 6.1: Set of linear least mean square predictors constructed for each impulse response time sample across the available ensemble [36].
6.1 Proposed Prediction Approach

Figure 6.1 illustrates the proposed channel prediction approach to be enacted independently by Alice and Bob based on the assumption that they retain the history of their past joint channel estimations. More particularly, as per the conducted real-world experiments, it is assumed that Alice and Bob have recorded a long history of channel impulse responses collected periodically. Assume that Alice and Bob have $k$ separate channel impulse responses taken at intervals of $m$ seconds apart and assume that the attacker (or eavesdropper) has perfect information regarding all but the last of these channel impulse responses (i.e. the attacker has exact information regarding all preceding $k - 1$ measurements but no information about measurement $k$).

Alice and Bob independently apply a set of adaptive linear least square error predictors to the $k-1$ ensemble to assess how much information the available impulse response history gives about each time domain sample within the currently measured impulse response. Linear prediction is a relatively easily applied process and, more importantly, adaptive least square error predictors do not require an a priori channel model which by the nature of the process is assumed unknown. More particularly, if a good channel model is a priori known then Alice and Bob cannot use the channel for key generation since the attacker can merely use the channel model itself to greatly reduce the required search space for the generated key. The physics of UWB channels preclude such a channel model from being available for the non-stationary portions of the channel. The lack of a sufficient channel model also precludes the use of predictors such the Kalman or extended Kalman filter (i.e. non-model based prediction innately must be employed).

Of course, the use of a linear predictor innately leads to the question, with respect to the security of the approach, as to where the attacker could employ a non-linear predictor and, thereby, gain an advantage over Alice and Bob. To confirm that non-linear prediction is unlikely to be advantageous lag-lag plots were constructed from the available set of 2000 experimentally collected impulse response traces taken every 500 msec for stationary antennae within a largely static environment. Typical examples of these lag-lag plots for both the LOS and NLOS channels are shown in Figure ??, where it can be seen that linear structure reasonably suffices the system correlation; hence, the data can be reasonably assumed not to possess any exploitable non-linear relationships. In particular, the experimental data that has been used can
Figure 6.2: Lag-lag plot of channel impulse response measurements [36].

be reasonably considered to be a worst-case scenario since the analysis measurements for the key generation obtained in highly static environment.

Finally, before applying the proposed prediction approach Alice and Bob must possess a method by which they can compute the measurement noise associate with the channel impulse response and where this measurement is applicable to non-stationary signals to denoise the received signals. As Alice’s and Bob’s independent measurement noise can be reasonably assumed to arise from standard effects such as thermal
noise, etc., then it is reasonable to assume that the Central Limit theorem will apply. Therefore, the well known approach of [16] can be applied to allow the standard deviation of the noise to be reasonably estimated as the standard deviation of the wavelet coefficients of the highest detail level available for in the wavelet decomposition of the measured time domain channel impulse response. More formally, \( \hat{\sigma} \) of the assumed \( N(0, \sigma) \) measurement noise process can be estimated as,

\[
\hat{\sigma} = \frac{1}{N/2 - 1} \sum_{k=1}^{N/2} [c_{j,k} - \bar{c}_j]^2, \tag{6.1}
\]

where \( c_j \) denotes the wavelet coefficients of the highest detail level of which there will be \( N/2 \) such coefficients is the time domain signal possesses \( N \) samples, and where \( \bar{c}_j \) denotes the statistical mean of the wavelet coefficients at this \( j \)th detail level. After calculating the noise power level, wavelet denoising can then be applied.

### 6.2 Information theoretic analysis of the method

The question to be answered with respect to the proposed method is whether the secret key rate remains positive (i.e. do non-predictable key bits exist).

To answer this question, we will calculate the lower bound on the secret key rate and show that this lower bound is strictly greater than zero. The secret key rate lower bound is given in [42] as

\[
\max \left[ I(y_A; y_B) - I(y_A; y_E) , I(y_A; y_B) - I(y_B; y_E) \right]
\]

where \( y_A, y_B, \) and \( y_E \) are the random variables indicate the observations of Alice, Bob, and Eve\(^1\), respectively.

Assume that Alice, A, and Bob, B, measure the channel characterization \( N \) times and for each channel characterization there are \( M \) time domain samples. Define matrix \( H \) as the composite of the channel characterizations where the \( j \)th element of \( i \)th row of \( H, h_{ij} \), denotes the amplitude of the channel sample \( j \) from the \( i \)th ensemble record.

If after wavelet denoising, the remained measurement noise contaminated the channel characterization at A, B, and E sides are denoted as \( n_A, n_B, \) and \( n_E, \) respectively, then observations of the \( N \)th ensemble's \( j \)th sample of channel characterization will be \( X = h_{Nj} + n_A \) for Alice, \( Y = h_{Nj} + n_B \) for Bob, and \( Z = \hat{h}_{Nj} + n_E \) for Eve,

\(^1\)Eve is the eavesdropper in the environment.
where $\hat{h}_{Nj} = h_{Nj} + e_{Nj}$ is Eve’s prediction of the $N$th ensemble’s $j$th sample obtained from Eve’s presumed perfect knowledge of the prior $N-1$ channel characterization events and $e_{Nj}$ is the prediction error.

Assume that the $h_{Nj}$ is a zero mean Gaussian random variable with variance $\sigma_h^2$. Additionally, assume that all measurement noises $n_A, n_B$ and $n_E$ are zero mean Gaussian with $\sigma_0^2$ variance. Further, ideally we can assume that $e_{Nj}$ is zero mean Gaussian with $\sigma_{e_j}^2$ variance (i.e. assume that the predictors are optimum so the output innovation sequence will be white Gaussian). In [21], the mutual information between two mutually Gaussian random variables $X$ and $Y$ is given by

$$I(X;Y) = \frac{1}{2} \log_2 \left( \frac{1}{1 - \rho_{xy}^2} \right),$$

where $\rho_{xy} = \frac{\mathbb{E}(XY)}{\sigma_X \sigma_Y}$.

To prove that the lower bound is strictly greater than zero, where $(y_A, y_B), (y_A, y_E)$, and $(y_B, y_E)$ are mutually Gaussian joint random variables, we need to show that

$$\rho_{y_A y_B} > \rho_{y_A y_E}.$$  

It can easily be shown that the inequality in Eq. (7.15) holds when the prediction error, $e_{Nj}$, has nonzero variance, $\sigma_{e_j}^2 > 0$. Consequently, information theoretic analysis validates that a secret key rate can be generated that provably Eve cannot know.

### 6.3 Simulation Results

The method is validated on the real measurements obtained from an experimental setup that are presented with details in Chapter 3.

The first step in the proposed algorithm is the wavelet denoising. In our test, we have obtained 2000 channel characterizations each of $4096 = 2^{12}$ samples. Denoising is then performed according to [16].

---

If $y_A$ and $y_B$ are statistically identical then $I(y_A; y_E) = I(y_B; y_E)$.
According to Donoho’s work in [16], after $6 = 12/2$ levels of wavelet filtering, the remained coefficient are noise with high estimation confidence. So, for wavelet denoising we wavelet the signal up to 6 levels and the clean constructed signal is the input of the predictors.

The predictors are linear adaptive least square predictors of order 20. To determine the threshold for removing the samples, across each ensemble $\bar{e}_j^2$, the average of the error pattern power, is calculated. The histogram of $\bar{e}_j^2$ illustrates that the prediction error power has the exponential distribution. Then the threshold is set to

$$ T = \sqrt{\frac{1}{4096} \sum_{j=1}^{4096} (\bar{e}_j^2)^2}, \quad (6.4) $$

which is the root mean square of $\bar{e}_j^2 = \frac{1}{N-1} \sum_{k=1}^{N-1} e_{kj}^2$. Therefore, only time samples from ensembles which have $\bar{e}_j^2 \geq T$ will be kept and used for key generation.

The simulation results for LOS channel shows that after applying the algorithm the number of samples available for key generation is reduced from 4096 samples to 405 samples (i.e. 90% of the measurement samples are highly predictable by the assumed ideal Eve). For NLOS channel the number of samples reduces from 4096 samples to 275 samples; hence, for NLOS and the ideal Eve 93.3% of the samples are highly predictable. This somewhat counter intuitive result arises due to the improved wavelet denoising that is available for the NLOS channel which results due to all of the received signal noise power coming from reflections in environment, whereas for LOS a significant portion of the received signal power follows the LOS path and, hence, is not contaminated by such environmental noise. Hence, the above prediction process for the NLOS path provides better results as the NLOS path has more noise and, hence, better noise estimation is possible via the wavelet approach.

### 6.4 Summary

Within this chapter a methodology based on a linear adaptive least square error prediction is developed to ensure that the predictable portions of UWB channel characterizations are not used as the basis for key generation processes. Furthermore, based on actual UWB channel measurements, it is shown that without applying such

---

3 Alice and Bob can of course choose to employ either a stronger or weaker threshold depending on their assumption regrading what Eve knows.
approaches, and where a rich past history of channel measurements is assumed and the physical environment is highly static, 90+% of the next channel characterization measurements are highly predictable. Hence, if the proposed approach is not applied, highly predictable keys would result. As the developed technique provides a mechanism by which Alice and Bob can independently arrive at the number of channel characterization samples available for key generation (i.e. unpredictable by Eve), the developed methodology can also be used by Alice and Bob as a decision mechanism whereby they can choose to only generate new secret keys when channel measurements indicate that sufficient degrees of non-stationarity have occurred (i.e. a fail safe mechanism is provided). It should be clearly noted that the provided analysis assumes a worst-case key generation scenario in which: (a) the physical environment is highly static, (b) Alice and Bob are absolutely stationary, and (c) Eve has full and perfect knowledge of all past channel characterization events. Even in this extreme case, it is shown that UWB based key generation remains feasible.
Chapter 7

Random Beamforming

In many practical situations it would be useful to have a WKG system that retains its ability to generated secret keys even in stationary environments (i.e. for point-of-sale systems, wireless keyboards, immobile sensors nodes, etc.). This can be accomplished by increasing the WKG system’s bandwidth up to ultra-wide bandwidth (UWB) scales. UWB systems possess the ability to resolve propagation paths that are closely spaced in terms of propagation time, whereas the innate low pass filtering processes of narrow and wide band receivers mean that they can only measure aggregations of propagation path with relative delays smaller than reciprocal of the radio signal bandwidth. This distinction within UWB WKG systems allows Alice and Bob to generate their keys material not from the fast fading portion of their shared channel but instead from measuring the individual characteristics of the each of the now resolvable multipaths channel coefficients.

At standard GigaHertz UWB carrier frequencies and GigaHertz bandwidths, these multiple propagation paths’ characteristics result from the orientation, composition, and location of numerous sub-centimetre reflectors within the Alice-Bob’s communication environment. Hence, the security of UWB WKG system in zero velocity scenarios rests on these reflectors occurring in sufficient numbers and with sufficient complexities that Eve is unable to accurately model (i.e. via ray tracing) the communications environment (i.e. as typically true in all but trivial environments) [58, 23].

As it is shown in Chapter 6, approaches exist whereby Alice and Bob can easily directly test for the appropriate environmental richness and, thereby, fail safely if it does not exist. Active adversaries could also exist, but, as the analysis of Chapter 8, it can be shown that active adversaries need to measure the same information about Alice and Bob’s channel as do successful passive Eve’s.
Hence, passive eavesdropping exists, within properly structured WKG systems, as the limiting case, thereby allowing WKG security to be assessed solely in terms of its security in the presence of passive eavesdroppers\(^1\).

For UWB WKG systems within stationary environments the critical secondary problem arises that successive key generation processes will, with highly likelihood, merely result in the production of identical (or nearly identical) keys. This, of course, is not the behavior that Alice and Bob desire. Alice and Bob expect that each successive WKG process produce a new secret key that is independent of all prior keys. The property of independence between successive keys is required if WKG is to be immune to certain forms of attack. For example, assume that WKG is being used in a standard office scenario to secure the connection between a computer and its wireless keyboard. Consider the scenario of Eve replacing the keyboard with a compromised keyboard which leaks information about any WKG process it participates in back to her. If after a single day the original keyboard is then placed back in the same position and nothing else changes in the office, then the next WKG process between the computer and the original keyboard will produce a key which the computer’s user believes is secure but which can be computed by Eve using the information logged by the compromised keyboard. The innate issue is that in stationary environments with an identically positioned keyboard, the radio multipath propagation characteristics will be identical even when the measurements are made at distinctly different times. Such attacks do not arise out of a failure of the WKG process, but occur when high temporal correlations exist within the environments in which they are used.

This chapter shows that one approach to addressing this problem is to transition Alice and Bob from using single antenna systems to using multiple-input multiple-output (MIMO) antenna systems in combination with random beamforming. This allows Alice and Bob to add directionality to their signal transmission and reception processes, where this directivity, due to its random nature, is unknowable to Eve. MIMO systems have been extensively proposed for wireless systems due to their potential to significantly increase communications capacity; hence, MIMO approaches are pragmatically feasible, as is the use of UWB communications for similar reasons.

The improved security of the resulting technique is assessed by analyzing the security achievable against a very capable Eve who is given perfect knowledge of

\(^1\)Of course, WKG is no more immune to broad spectrum signal jamming than any other known communications approach, but such jamming, by its definition, will also always lead to a safe failure with no secret information revealed to Eve.
Alice and Bob’s MIMO channel and the capability to accurately deduce their random beamformer coefficients down to a prescribed error. Such an Eve is not expected to exist in the real-world, but assessing such an Eve, who arguably exists at the supremum of the capability of any real-world Eve, is useful to assess the limits of security of the proposed technique.

It should be clearly noted that this chapter solely focuses on addressing the temporal correlation problem for WKG systems that arises in stationary environments. If sufficient movement exists between Alice and Bob (or within their communications environment) then the standard WKG security analysis suffices.

### 7.1 Channel Prediction

We have previously demonstrated that UWB channel measurements can be highly correlated in time (as is shown in Chapter 3), as illustrated in Figure 7.1 which plots the time correlations of radio channel coefficients during a 16 minute interval with a 3 m Alice-Bob antenna separation distance within a standard research laboratory environment. Sequentially applied WKG processes in such environments will, with high probability, tend to produce identical, or near identical, secret keys. This allows a knowledgeable Eve to apply all of the prior information she may have gleaned about any prior key (i.e. through her prior measurements, etc.) to deduce the current key or collapse its key space to a small, searchable space. This work considers an Eve that seeks to characterize the wireless environment through her own measurement processes for Alice’s and Bob’s antenna positions, such that when Alice and Bob generate their next key, Eve may also have some information about that key. As discussed in this chapter’s introduction, a pragmatic example can be easily constructed around the use of WKG to secure wireless keyboards. Obviously, this form of attack must be protected against if WKG approaches are to be usable in the real-world.

From Figure 7.1, it is obvious that Alice and Bob cannot address this problem by merely increasing the number of channel probes they use to produce each secret key, as each channel probe will merely reproduce the previously measured channel information. The technique of [36] ensures that on each successive channel probe Alice and Bob generate key bits not predictable from the ensemble of all of their prior channel characterization measurements, but the combination of high temporal correlation and local measurement noise will reduce the novel secret key material...
available from each successive channel probe to near zero in these nearly stationary environments.

The deep drops in the correlation visible in Figure 7.1 appear to be attractive times to generate independent keys, but these result from people moving within the research laboratory during the measurement interval. Hence, the problem arises that these drops may be predictable to an observant Eve, for example one who has placed cameras within the environment and who has access to reasonable wireless ray tracing solutions. Moreover, in [33], it was shown that Eve herself can, in some cases, effect a measure of control over the WKG process by being the one who moves within the Alice-Bob communications environment (i.e. being the one who causes the observed dips in the correlation to occur).

With respect to this chapter, it suffices to discuss security solely in terms of linear correlation, as prior tests discussed in Chapter 6, have shown that it is unlikely that non-linear relationships exist between the UWB channel measurements for Eve with the channel measurements of Alice and Bob. Without such assessments, there is the possibility that non-linear relationships may exist with Alice’s and Bob’s channel measurements that Eve could exploit, in which case solely assessing security in terms of linear correlations would be insufficient to determine security. Again, for the data
presented here, assessments have been made in Chapter 6 to confirm the low likelihood that any exploitable non-linear relationships exist\(^2\).

### 7.2 Random Beamforming

This work pre-supposes that, for stationary environments, Alice and Bob innately cannot solve the temporal correlation problem if they use single omni-directional antennas as they then have no control over how their radio signal energy radiates into the communications environment. Using multiple antennas allows Alice and Bob to enforce a directional sensitivity to their channel probe transmissions and receptions. If this directional sensitivity is structured to be random (i.e. through Alice and Bob independently employing random beamforming coefficients) then these transmission and reception directions will be unknown to Eve, thereby allowing a secure mechanism for producing independent keys even in stationary environments.

In order to maintain reciprocity, a necessary construct of WKG, Alice and Bob must hold their beamforming coefficients static during the full send and receive cycle for each channel probe event. But, to ensure independence of the generated key, Alice and Bob must change their beamforming coefficients between channel probe events. Moreover, Alice and Bob’s changes to their beamforming coefficients are done independently. These coefficients must not be picked deterministically, as the next coefficients would then become predictable by Eve.

The net effect of Alice and Bob both engaging in random beamforming is that, for each channel probe event for key generation, Alice and Bob’s WKG process is more sensitive to certain reflectors in the environment and less sensitive to others. To exploit this sensitivity, Eve must know which reflectors are the important reflectors for the current key generation event, which changes each time key generation is performed. It is Alice’s and Bob’s use of random beamforming coefficients that prevents Eve being able to easily exploit the introduced directional sensitivity for her gain since she must estimate the directivity of Alice’s and Bob’s beamforming coefficients. Alice and Bob do not need to know each other’s random beamforming coefficients for the approach to work, assuming they are seeking to perform WKG in a suitably rich multipath wireless environment. Moreover, for Eve to deduce Alice and Bob’s

\(^2\)To be clear, proving that no non-linear relationships exist is innately not possible. Hence, the best that can be done is to use processes such as lag-lag plots, as in Chapter 6, to demonstrate the low likelihood that any such relations exist within the given data.
resultant key she will need both perfect knowledge of Alice and Bob’s MIMO channel transfer function and all the beamforming coefficients.

It should be noted that the objective of random beamforming within this chapter is somewhat different than beamforming as it is standardly used within the communications literature[56]. In particular, beamforming techniques are generally used to algorithmically combine the signals received from a multiple antennas in order to maximize the signal-to-noise ratio (SNR) of the resultant point-to-point communications. From an electromagnetic perspective, beamforming creates directional antennas in point-to-point communications. Instead of seeking to maximize the SNR, random beamforming is used to randomly distribute the energy associated with Alice and Bob’s WKG channel probe events into the environment such that a non-stationary environment is mimicked when the true propagation environment is static (i.e. to allow random beamforming to mimic the same physical effects that would normally arise via movement induced fast fading). The goal of the random beamforming is to create independent secret keys for each of Alice and Bob’s key generation processes. The desired goal of the random beamforming as proposed in this chapter for WKG is, therefore, not the standard goal of maximizing the channel capacity between Alice and Bob over the beamformed channel.

In the proposed scheme, Alice and Bob both independently sample their beamforming coefficients from uniform distributions during each key generation event\(^3\) in order to maximize the key space that Eve must search even if she is given perfect knowledge of one (or more) of the prior keys. If Alice and Bob have some information about the other’s location, then the beamforming can be structured such that it minimizes the energy directed along the line-of-sight (LOS) path between Alice and Bob. This minimizes the SNR of the link between Alice and Bob but since the LOS path’s characteristics are easily predicted by Eve, the LOS path is not useful for secret key generation.

There is the problem that a lucky Eve could be located on one of the propagation paths favored by Alice and Bob’s directional gains and thus gain a large amount of information about the current key. This may be addressed by Alice and Bob performing an eXclusive OR (XOR) operation on the key material obtained from several consecutive random beamforming WKG events, with the number of events XORed together creating an upper bound on the probability that Eve will be located

\(^3\)This should not be confused with Alice and Bob seeking to produce an omni-directional (i.e. uniform) beam as this would not be beamforming.
on one of the primary propagation paths for each of the combined WKG events (i.e. if $p$ is the probability that Eve is on the favored paths then $p^n$ is the probability the Eve is on all paths used for $n$ randomly beamformed WKG events). By information theory, XORing ensures that Eve’s uncertainty about the final key is lower bounded by Eve’s uncertainty regarding any of the constituent per-event key material. The above arguments are analyzed in the next section.

### 7.3 Analysis of Random Beamforming

Figure 7.2 shows the block diagram of the proposed random beamforming signal reception process, as proposed in this chapter. During signal transmission, the signal flow is reversed.

The above system is a MIMO system with $N$ antennas per side. Therefore, assuming that Alice transmits a randomly beamformed channel probe event to Bob at time $t$, the transmitter antenna output vector will be $s(t) = s(t)w_{TM}^m$, where $s(t)$ is the output signal at Alice’s beamformer at time $t$, the vector $w_{TM}^m$ denotes Alice’s random beamformer’s coefficient in use the $m$th time Alice and Bob perform WKG, and the $T$ subscript denotes that channel gains vector is for the transmitter of the channel.
probe. Bob then receives the signal \( s(t) \) through his MIMO antennas as,

\[
y(t) = H(t)s(t),
\]

(7.1)

where \( H(t) \) is the \( N \times N \) matrix of the channel gains for the MIMO channel established between Alice to Bob at time \( t \) and where, for notational simplicity, the propagation time of the transmitted signals through the communications medium is neglected. To isolate the effects of random beamforming from other concerns, this chapter also assumes that Alice, Bob, and Eve have a perfect ability to remove their own measurement noise processes from all of their measurements. Hence, it is shown that even when Eve is capable of making perfect noise-free measurements under random beamforming she is still incapable of deducing Alice and Bob’s key.

The received signal at Bob’s \( k \)-th antenna, denoted as \( y_k(t) \), is multiplied by the current random beamforming weight for that antenna, \( w^m_k \), associated with the \( m \)th Alice-Bob WKG process. The resulting signal across the composite set of Bob’s \( N \) antennas is then \( r^m(t) = \sum_{k=1}^{N} w^m_k y_k(t) \) which then feeds a standard key generation process, such as that described in Chapter 5. Each of Alice and Bob’s antennas are assumed to have the standard \( \lambda/2 \) separations for antenna arrays. Hence, for the utilized UWB signals, each antenna receives a different distribution of the signal energy across the set of available propagation paths[37]. Alice and Bob’s random beamforming create different weighting on each of these paths, where neither Alice nor Bob, given just their own random beamforming coefficients, can deduce the nature of the weighting matrix of the other legitimate communicating partner.

The output of Bob’s receiver beamformer for key generation probe \( m \) with the random beamforming coefficient vector \( w^m_R \) can then be given by,

\[
r^m(t) = (w^m_T H(t) w^m_R s(t),
\]

(7.2)

where the \( R \) subscript denotes the reception of a channel probe. The transposition of a matrix \( C \) is denoted with the prime superscript as in \( C' \). Element-wise conjugation of a matrix \( C \) is denoted as \( C^* \), and complex transposition is denoted with a superscript dagger as in \( C^\dagger = (C')^* \).

If the \( w^m_R \) and \( w^m_T \) coefficients are time independent, white uniformly distributed, complex random vectors then \( \mathbb{E}[r^{m_1}(t) (r^{m_2}(t + \tau))^*] = 0 \) when \( \tau \) is greater than time period required for a single channel probe transmission and reception process.
to occur. The superscripts $m_1$ and $m_2$ represent successive channel probes event occurring respectively at times $t$ and $t + \tau > t$. Hence, as required, different randomly beamformed channel probes will generate uncorrelated measurements, presuming of course that the Alice-Bob communications environments is itself non-trivial. For the WKG process to be completed Alice and Bob must also then reverse their roles as transmitter and receiver of the channel probes. To maintain the reciprocity requirement, for each of Alice to Bob’s channel probe, the corresponding Bob to Alice’s channel probe event must be conducted within the coherence time of the channel and utilize the same random beamforming coefficient vectors.

To assess the worst-case scenario, it is assumed that Eve has perfect knowledge of the utilized Alice-Bob MIMO channel matrix, $\mathbf{H}(t)$. This approximates the situation where Eve makes perfect use of all of her prior channel measurements as well as any other information to model the Alice-Bob communications environment. Outside of trivial environments, real-world eavesdroppers would need to make use of an estimate of $\mathbf{H}(t)$ denoted as $\hat{\mathbf{H}}(t)$.

The analyzed case exists at the supremum of what would be possible for any real-world Eve. Therefore, showing that security is achieved for a Eve with $\hat{\mathbf{H}}(t) = \mathbf{H}(t)$ demonstrates that security is also achievable for any real-world Eves, assuming that trivial environments are addressed by appropriate testing, as per our work.

Even if Eve knows $\mathbf{H}(t)$, Eve must still estimate each of the $\mathbf{w}^m_T$ and $\mathbf{w}^m_R$ for $m = 1, \ldots, n$ if she is to deduce Alice and Bob’s key, assuming the final key is produced via the XORing of $n$ individual sets of channel probe produced key material. It is assumed that Eve, by some means, knows $\mathbf{w}^m_T$ and $\mathbf{w}^m_R$ to some non-zero degree of error. In this chapter, the normalized mean estimation error between Alice’s (or Bob’s) received signal $r^m(t)$ and Eve’s estimate of this signal $\hat{r}^m(t)$ is calculated. As the random beamforming coefficients are changed after each pair of Alice-to-Bob and Bob-to-Alice channel probe events and successively produced key material is XORed, the analysis can proceed by focusing on each $r^m(t)$ signal in isolation (i.e. the $m$ superscript can be dropped, as can the explicit denoting of time by $t$).

In this chapter, the random beamforming coefficients $\mathbf{w}_k$ are selected to be unit amplitude complex random variables (i.e. $\mathbf{w}_k = e^{j\theta_k}$ where $\theta_k$ is distributed uniformly over $[0, 2\pi]$). Eve’s estimates of the beamforming coefficient vectors can be denoted
by,
\[
\begin{align*}
\hat{\theta}_T &= \theta_T + z_T \quad (7.3) \\
\hat{\theta}_R &= \theta_R + z_R, \quad (7.4)
\end{align*}
\]
where \(z_T\) and \(z_R\) are independent white Gaussian vectors denoting Eve’s estimation error for both the transmitter and receiver side beamforming coefficients.

To verify the assumptions made on the distribution of Eve’s estimation errors, a set of simulations were performed. In the simulation scenario, it is assumed that Alice and Bob are employing random beamformers and measuring their MIMO channel with independent Gaussian measurements error vectors. An Eve who is able to measure Alice and Bob’s MIMO communication channel perfectly but does not know the random beamformers’ coefficients is overhearing Alice and Bob’s communication. Eve’s measurement vectors are given by

\[
\begin{align*}
y_{E,A} &= sH_{AE}w_T + v_{E,A}, \quad (7.5) \\
y_{E,B} &= sH_{BE}w_R + v_{E,B} \quad (7.6)
\end{align*}
\]

where \(y_{E,A}\) is the measurement vector for Eve from the signal transmitted by Alice, \(y_{E,B}\) is the measurement vector Eve from the signal transmitted by Bob. The matrices \(H_{AE}\) and \(H_{BE}\) denote the Alice to Eve and Bob to Eve channels, respectively. These matrices are \(N\) by \(N\) and each entry is sampled from an independent Gaussian distribution with mean zero and variance one. The Gaussian random vectors, \(v_{E,A}\) and \(v_{E,B}\) model the measurement noise and are assumed independent with zero mean and covariances given by \(\sigma_v^2I_N\) where \(I_N\) is the \(N \times N\) identity matrix. We make the pessimistic assumption that Eve has full knowledge of \(H_{E,A}\) and \(H_{B,A}\) when she is estimating \(w_T\) and \(w_R\).

Eve employs an optimum Wiener estimation for estimating \(w_T\) and \(w_R\):

\[
\begin{align*}
\hat{w}_T &= M_T^\dagger y_{E,A} \\
\text{with } M_T &= \left(H_{AE}H_{AE}^\dagger + \sigma_v^2I_N\right)^{-1}H_{AE}, \quad (7.7) \\
\hat{w}_R &= M_R^\dagger y_{E,B} \\
\text{with } M_R &= \left(H_{BE}H_{BE}^\dagger + \sigma_v^2I_N\right)^{-1}H_{BE}. \quad (7.8)
\end{align*}
\]
Since our beamforming vectors have an absolute value of one for each entry, we normalize to obtain $\tilde{w}_T$ and $\tilde{w}_R$ so that $\tilde{w}_T(k) = \hat{w}_T(k) / |\hat{w}_T(k)|$ and $\tilde{w}_R(k) = \hat{w}_R(k) / |\hat{w}_R(k)|$ for $k = 1, ..., N$. Our simulation results for SNR $\in [5, 10, 15 \text{ (dB)}]$ range shows that the estimation error of beamformers coefficients (i.e. $z_T = \hat{\theta}_T - \theta_T = \angle w_T - \tilde{w}_T$ and $z_R = \hat{\theta}_R - \theta_R = \angle w_R - \tilde{w}_R$) will not pass the Chi-square test for Gaussian random tests with a 95% degree of confidence. Figure 7.3 shows the cumulative distribution function (CDF) of the observed beamformers’ angle estimation error (i.e. $z_R$) versus a Gaussian random variable that has the same mean and variance as $\tilde{z}_R$. The number iteration for estimating a CDF for $z_R$ is $10^6$ times, where Alice’s, Bob’s, and Eve’s array antenna size is 4 and the SNR is assumed to be 10 dB. For comparison, the CDF of the simulated estimation error is also plotted in Figure 7.3, where the simulated CDF is calculated from an average over 20 trials. According to the Chi-Square test results, we are aware that Gaussian distribution for estimation error is an underestimation of eavesdroppers’ error (i.e. eavesdroppers in practice can estimate more accurately). However, for the sake of the analytical solution’s simplicity, we assumed that this error is Gaussian. More accurate estimation of eavesdroppers’ estimation error of $z_R$ or $z_T$ may be possible via wrapped Cauchy or wrapped Stable distributions [4] but this would significantly complicate the analysis.

![Estimated Error CDF, SNR=10](image)

Figure 7.3: CDF of the observed estimation error (at receiver side, $z_R$) versus CDF of a Gaussian random variable with the same mean and variance as the observed data [26].

Figure 7.4 shows the CDF of the observed beamformers’ angle estimation error versus the wrapped stable CDF with moment estimation parameters, $\hat{R}_1 = 0.9074$, $\hat{R}_2 =$
0.7538, \hat{\alpha} = 1.5406, \hat{\gamma} = 0.2202 \ [4], under similar simulation criteria to Figure 7.3. The wrapped stable modeling does not pass the chi-square test either, but from the observation aspect, Figure 7.4, has a better match with real data observation than the Gaussian model of Figure 7.3.

![Estimated Error CDF, SNR=10](image)

Figure 7.4: CDF of the observed estimation error (at receiver side, \( z_R \)) versus CDF of a wrapped stable distribution with moment estimation parameters: \( \bar{R}_1 = 0.9074, \bar{R}_2 = 0.7538, \hat{\alpha} = 1.5406, \hat{\gamma} = 0.2202 \).

The ability of Eve to deduce Alice and Bob’s generated key depends on the accuracy of Eve’s estimates of \( w_T \) and \( w_R \), denoted respectively as \( \tilde{w}_T \) and \( \tilde{w}_R \). The mean error power is given by

\[
\bar{\varepsilon}^2 = \mathbb{E} \left[ |r - \tilde{r}|^2 \right] \\
= |r|^2 + \mathbb{E} \left[ |\tilde{r}|^2 \right] - \mathbb{E} \left[ r\tilde{r}^\dagger \right] - \mathbb{E} \left[ r^\dagger \tilde{r} \right], \tag{7.9}
\]

where \( r \) represents Alice (or Bob’s) received signal, and \( \tilde{r} \) represents Eve’s estimate of \( r \), and \( \mathbb{E}[] \) denotes statistical expectation.

At this stage, it is assumed that the perfect knowledge of MIMO channel is provided so that the above expectation is performed over a deterministic \( H \). The cross correlation terms are given by

\[
\mathbb{E} \left[ r\tilde{r}^\dagger \right] = s^2 \mathbb{E} \left[ w_T^\dagger H w_R \tilde{w}_R^\dagger H^\dagger \tilde{w}_T^* \right]. \tag{7.10}
\]
Matrix vector quadratic forms can be rewritten using the matrix trace operator, \( \text{tr} \) as \( x^\dagger A x = \text{tr} \left( A x x^\dagger \right) \). Matrices within a trace operator can be circularly shifted as in \( \text{tr} (A B C) = \text{tr} (B C A) = \text{tr} (C A B) \). Using these properties the expected power of the received signal at a legitimate receiver is given by

\[
\mathbb{E} \left[ r \tilde{r}^\dagger \right] = s^2 \mathbb{E} \left[ \text{tr} \left( H w_R \tilde{w}_R^\dagger H^\dagger \tilde{w}_T^* w_T' \right) \right],
\]

(7.11)

The order of the trace and expectation operations are swapped to obtain

\[
\mathbb{E} \left[ r \tilde{r}^\dagger \right] = s^2 \text{tr} \left( H Q_T H^\dagger Q_R \right),
\]

(7.12)

where \( Q_R = \mathbb{E} \left[ w_R \tilde{w}_R^\dagger \right] \) and \( Q_T = \mathbb{E} \left[ \tilde{w}_T^* w_T' \right] \) are complex cross-covariance matrices denoting the beamforming vectors of Alice and Bob with Eve’s estimate of these vectors. The outer-product of \( w_R \), denoted as \( D_r \), is given by

\[
D_r = w_R w_R^\dagger = \begin{bmatrix}
1 & e^{j(\theta_{r1}-\theta_{r2})} & \cdots & e^{j(\theta_{r1}-\theta_{rN})} \\
e^{j(\theta_{r2}-\theta_{r1})} & 1 & \cdots & : \\
\vdots & \vdots & \ddots & \vdots \\
e^{j(\theta_{rN}-\theta_{r1})} & \cdots & \cdots & 1
\end{bmatrix}
\]

(7.13)

where \( \theta_{rk} \) is the \( k \)th entry of \( \theta_R \). From Eq. (7.13), the outer-product of the legitimate receiver beamforming vector \( w_R \) with the estimated receiver beamforming vector of Eve, \( \tilde{w}_R \) is given by

\[
Q_R = \rho^{1/2} D_r
\]

(7.14)

where \( \rho^{1/2} = \mathbb{E} \left[ e^{jz_k} \right] \) for all \( k = 1, \cdots, N \). The value of \( \rho \) is derived from the characteristic function of the Gaussian random variable \( Z \) with zero mean and variance \( \sigma^2_0 \), \( \Phi_Z (\omega) = \mathbb{E} \left[ e^{\omega Z} \right] = e^{-\sigma^2_0/2} \) with \( \omega = 1 \), allowing the correlation coefficient \( \rho \) to be found as

\[
\rho = e^{-\sigma^2_0}.
\]

(7.15)
A similar derivation shows that \( Q_T = \rho^{1/2} D_t \) where \( D_t \) has the same form as \( D_r \) using the directional vector \( \theta_T \). Consequently,

\[
\mathbb{E}[r\tilde{r}^\dagger] = s^2 \rho \text{tr} [H D_r H^\dagger D_t^*]. \tag{7.16}
\]

The rest of the Eq. (7.9)'s terms are given below:

\[
\begin{align*}
\mathbb{E}[|r|^2] & = s^2 \text{tr} [H D_r H^\dagger D_t^*], \tag{7.17} \\
\mathbb{E}[|\tilde{r}|^2] & = s^2 \text{tr} [H (\rho D_r + (1 - \rho) I_N) H^\dagger \\
& \quad (\rho D_t^* + (1 - \rho) I_N)], \tag{7.18} \\
\mathbb{E}[|r^*\tilde{r}|] & = s^2 \rho \left( \text{tr} [H D_r H^\dagger D_t^*] \right)^*, \tag{7.19}
\end{align*}
\]

where \( I_N \) denotes an identity matrix of \( N \) dimension. Full details of the derivation of Eq. (7.17) to Eq. (7.19) are provided in Appendices A.1 and A.2. The mean error power is, therefore, given by

\[
\varepsilon^2 = s^2 (1 - \rho)^2 \left\{ \text{tr} \left[ \mathbb{E} (H D_r H^\dagger D_t^*) \right] + \text{tr} \left[ \mathbb{E} (H H^\dagger) \right] \right\} \\
+ s^2 \rho (1 - \rho) \left\{ \text{tr} \left[ \mathbb{E} (D_r H^\dagger H) \right] + \text{tr} \left[ \mathbb{E} (H H^\dagger D_t^*) \right] \right\} \tag{7.20}
\]

Two cases, need to be considered. The first is when \( H \) is a random matrix and the beamforming vectors \( \mathbf{w}_R \) and \( \mathbf{w}_T \) are deterministic. The second is when \( H \) is deterministic and the beamforming vectors \( \mathbf{w}_R \) and \( \mathbf{w}_T \) are random.

### 7.3.1 Random Channel Matrix

In this section, it is assumed that \( \mathbf{w}_T \) and \( \mathbf{w}_R \) are deterministic and that eavesdropper can estimate these vectors with some measurement error. Also, in the this section we assume that MIMO channel matrix, \( H \), is random. Then to calculate the mean error power, the following theorem will be used.

**Theorem 7.3.1.** Assume we have a random matrix \( X \) with mean value of \( \mathbb{E}(X) = M \) and covariance given by \( \text{cov}[\text{vec}(X)] = U \otimes V \), where \( \text{vec}(X) \) denotes the vector formed by stacking the columns of \( X \) into a single column, and \( \otimes \) denotes the Kronecker product. For a deterministic matrix \( B \) of appropriate dimensions, we have

\[
\mathbb{E}[XBX'] = \text{tr}[BU] V + MBM' \tag{7.21}
\]
Proof. The proof is given in [46].

If $H$ is random Gaussian matrix with each entry of $H$ being independent of all other entries and having the normal distribution $N(0, \sigma_h^2)$, by applying Theorem 7.3.1, it can be derived that

$$
E_H [HD, H^* D^*] = N^2 \sigma_h^2, \quad (7.22)
$$

where $E_H[.]$ denotes expectation over random $H$ and $N$ is the array size of Alice’s and Bob’s beamformers. Eq. (7.22) is calculated in Appendix A.2. Similarly we have,

$$
E_H [\text{tr}(HH^* D^*)] = N^2 \sigma_h^2, \quad (7.23)
$$

$$
E_H [\text{tr}(D, H^* H)] = N^2 \sigma_h^2, \quad (7.24)
$$

$$
E_H [\text{tr}(HH^* H)] = N^2 \sigma_h^2. \quad (7.25)
$$

Consequently, Eq. (7.20), taking all expectations with respect to the distribution of the random matrix $H$, can be rewritten as

$$
\varepsilon^2 = 2s^2 \sigma_h^2 N^2 (1 - \rho). \quad (7.26)
$$

The normalized mean error then given by

$$
\bar{\varepsilon}^2 = \frac{\varepsilon^2}{\sigma_h^2 s^2} = 2N^2 (1 - \rho). \quad (7.27)
$$

The above equation denotes an upper bound on Eve’s knowledge of Alice’s (or Bob’s) received channel probe signal as a function of Eve’s error, through the averaged error $\bar{\varepsilon}^2$, in her estimates of Alice and Bob’s random beamforming coefficients, under the idealized assumption that Eve perfectly knows the MIMO channel $H$. This equation applies for each channel probe event. Hence, when Alice and Bob produce their final key by XORing the key material obtained from $n$ channel probe events, Eve’s estimation error becomes cumulative when Alice and Bob’s communications environment is a nontrivial multipath propagation environments and Alice and Bob pick their beamforming coefficients randomly from uniform distributions. Moreover, as Eq. (7.27) shows, Eve’s per-channel probe error increases exponentially with Eve’s
uncertainty in the directional sensitivity of Alice and Bob’s random beamformers. Hence, through random beamforming Alice and Bob have gained a strong measure of control that directly results in rapid increases in Eve’s channel estimation errors, assuming that for Eve $\bar{\epsilon}^2 > 0$. Figure 7.5 shows the normalized error $\bar{\epsilon}$ versus different array size, $N$, and variance of beamformers’ taps’ coefficients, $\sigma_0$.

![Gaussian MIMO channel](image)

Figure 7.5: Normalized estimation error of eavesdroppers, $\bar{\epsilon}$; $H$ is assumed to be independent Gaussian random matrix; $W_T$ and $W_R$ are deterministic [26].

It also becomes clear that Alice and Bob should select the number of channel probes, $n$, from which they XOR key material to produce their final key based on their belief as to Eve’s capabilities to accurately estimate their beamforming coefficients combined with their belief in the likelihood that a lucky Eve could be located exactly on all the primary propagation path(es) for any given channel probe event, where this is also a function of the number of antennas $N$ in Alice and Bob’s MIMO systems$^4$. In general, therefore, in selecting a given $n$, Alice and Bob effectively place an upper bound on Eve’s ability to estimate their per-channel probe beamforming coefficients and Eve’s luck in being located on all beamformed paths. As channel probes and the resultant WKG signal processing steps are of relatively low energy and computational cost, $n$’s large enough to address even quite capable Eves can be used even in pragmatic real-world settings (i.e. UWB WKG for $n > 10$ can still be performed within the period of a few seconds).

$^4$It is perfectly possible for Alice and Bob to make use of MIMO systems with differing antenna numbers as this merely complicates the resulting notation and not the discussed analysis process.
7.3.2 Random Beamforming

This section considers the case when the channel transfer matrix $H$ is fixed and the beamforming vectors are random. This case models the ability of Eve to estimate the legitimate receivers’ signal over several repetitions of the WKG process where randomly selected beamforming vectors are used in each case. In this case, the matrices $D_r$ and $D_t$ are random, being derived from the random vectors $w_R$ and $w_T$, respectively. It is assumed that the $w_R$ and $w_T$ are independent uniformly distributed.

Expectation taken over the distribution of the random beamforming vectors $w_T$ and $w_R$ will be denoted as $\mathbb{E}_W [\cdot]$.

Since the random angles within $\theta_T$ and $\theta_R$ are uniformly distributed from 0 to $2\pi$, it is easily seen that $\mathbb{E}_W [e^{j\theta_k}] = \mathbb{E}_W [e^{j\theta_m}] = 0$ for all receiver beamforming angles $k$ and transmitter beamforming angles $m$. It is then easily derived that $\mathbb{E}_W [D_t] = \mathbb{E}_W [D_r] = I_N$. The mean values of the components from Eq. (7.20) calculated over the probability distribution of the random beamforming angles is then calculated as

\[
\begin{align*}
\text{tr} \left[ \mathbb{E}_W (HD_rH^\dagger D_t^\dagger) \right] &= \text{tr} (HH^\dagger), \\
\text{tr} \left[ \mathbb{E}_W (HH^\dagger D_t^\dagger) \right] &= \text{tr} (HH^\dagger), \\
\text{tr} \left[ \mathbb{E}_W (D_rH^\dagger H) \right] &= \text{tr} (H^\dagger H), \text{ and} \\
\text{tr} \left[ \mathbb{E}_W (HH^\dagger) \right] &= \text{tr} (HH^\dagger).
\end{align*}
\]

Basic linear algebra shows that $\text{tr} (HH^\dagger) = \text{tr} (H^\dagger H) = \sum_{k=1}^{N} |\lambda_k|^2$ where $\lambda_k$ is the $k^{th}$ singular value of the channel transfer matrix $H$. It can then be seen that the mean error power averaged over beamforming vectors is given by

\[
\varepsilon^2 = 2 (1 - \rho) \sum_{k=1}^{N} |\lambda_k|^2.
\]

A comparison of Eq. (7.32) with Eq. (7.26) shows that neither a fixed channel coefficients nor fixed beamforming coefficients assist Eve in estimating the legitimate received signal.
7.4 Simulation results

Two critical questions remain. First, how does Eve’s ability to use multiple antennas affect her ability to deduce Alice and Bob’s key material? Second, how does the number of antennas \( N \) that Alice and Bob use in their MIMO systems affect Eve’s ability to deduce the generated key? The directional selectivity of a beamformed MIMO system increases with \( N \) (i.e. with \( N = 1 \) no direction selectivity exist, with \( N = 2 \) a modicum of selectivity is gained, and this continues to increase as \( N \) increases). Eve’s multiple antenna capability assists her to make a more accurate estimate of Alice’s and Bob’s beamformers’ coefficients (i.e. more accurate estimate results in lower \( \sigma_0 \)).

The theoretical response to the above questions are provided by the results of Eq. 7.27 and plotted in Figure 7.5. The normalized error of Eve quadratically increases with Alice’s and Bob’s antenna array size, \( N \). Eve’s normalized mean square error for Alice or Bob signal is proportional to the exponential of the variance of her estimation error of Alice and Bob’s beamforming angles. As Figure 7.5 shows, for array sizes, \( N \geq 4 \), the normalized mean error is greater than 0 dB, where the standard deviation of Eve’s estimation error for the angle of Alice’s and Bob’s beamformers’ coefficients is \( \pi/32 \) radians (i.e. about 5 degrees).

![Normalized estimation error of eavesdroppers, \( \bar{\epsilon} \); \( H \) is generated through UWB channel modeling of IEEE 802.15.3a [45]; \( W_T \) and \( W_R \) are deterministic [26].](image)

In practice, the elements of matrix \( H \) are not independent over time (i.e. the variance of the propagation path gains amplitude drops exponentially in each cluster
for time). Consequently, Eve’s normalized error will be less than the theoretical bounds given in Eq. (7.27). Figure 7.6 shows the normalized mean error power of Eve for a more realistic radio channel versus Alice’s and Bob’s antenna array size. The $H$ matrix is generated by the UWB channel simulator proposed in [45]. The UWB channel is a NLOS channel in which the separation distance between Alice’s and Bob’s transceivers is 4 to 10 meters. The generated UWB channel has 1296 samples per each channel probe and the number of trials for this test was set to 10000.

As results in Figure 7.6 show, in general, Eve’s normalized mean error is lower than the theoretical results. Unlike the theoretical results of Figure 7.5, for $\sigma_0 = \pi/32$, even using a large array of antennae (e.g. $N = 8$, the maximum array size in our test) does not help Alice and Bob to bound Eve’s normalized mean error to $\bar{\epsilon} > 0$ dB. Furthermore, for $\sigma_0 \geq \pi/16$ there are solutions within array size $N \leq 8$ to bound Eve’s normalized mean error to $\bar{\epsilon} > 0$ dB.

**Theorem 7.4.1.** Assume that Eve has estimated the MIMO channel $H_{AB}$ between Alice and Bob perfectly with no error (i.e. $\hat{H}_{AB} = H_{AB}$). Also assume that Alice and Bob employ random beamformers including $N$ antenna which are weighted by randomly picked complex coefficient vectors $w_T = e^{j\theta_T}$ and $w_R = e^{j\theta_R}$, respectively. Eve’s estimation error of $\theta_T$ and $\theta_R$ are $z_T$ and $z_R$, respectively. Let $z_T$ and $z_T$ be Gaussian white random vectors that each element has a zero mean and a $\sigma_0^2$ variance. Then the normalized mean estimation error of Eve from the beamformed signal will be given by

$$\epsilon^2 = 2 \left( 1 - e^{-\sigma_0^2} \right).$$

**Proof.** The proof is given in Subsection 7.3.1.

7.5 **Summary**

This chapter shows that by extending UWB WKG to MIMO systems and utilizing random beamforming, independent keys can be generated by each WKG event, even in near stationary environments.

It is then shown formally that this approach provides increased security even in the case of an highly idealized Eve who is assumed to have perfect knowledge of Alice and Bob’s MIMO channel, as well as an estimation of their utilized random beamforming
coefficients. Such information and particularly the NLOS MIMO channel information would be difficult for a real-world Eve to obtain with a high degree of accuracy, hence, the evaluated Eve can be viewed as existing at the supremum of any likely real-world Eve. This allows the results to be viewed as providing an upper bound on the likely capabilities of any real-world Eve, thereby confirming that the proposed technique would provide increased security under real-world scenarios.

Currently, implementing the solutions, as shown for the presented experimental results, requires relatively high grade UWB communications equipment. However, intensive research is being conducted on both MIMO and UWB communications, so the technique will be suitable for the next generation of consumer grade devices.

In future research, how to model the angle error of Eve with wrapped Stable distributions will be explored [4].
Chapter 8

Security Analysis

This chapter discusses the security of the described key generation approach of Chapter 5 against both passive eavesdroppers and active adversaries and shows that the limiting case for both arises from the $\lambda/2$ radius limit (20 cm radii in our measurement tests) for correlated channel measurements. Passive eavesdroppers and active adversaries are defined as follows:

**Passive Eavesdroppers:** passive eavesdroppers are a set of potentially collaborating terminals $E$ located within the communications environment of Alice and Bob who are only able to listen to Alice and Bob’s communications (i.e. the eavesdroppers are able to make and share their measurements of $h_{AE}(t)$ and $h_{BE}(t)$ where $|E| \geq 1$). Additionally, these eavesdroppers are assumed to have full knowledge of available wireless propagation models and theory, inclusive of having access to ray tracing software, as well as any measurement data sets they may have acquired through pre-characterising the wireless environment prior to Alice and Bob’s key generation process.

**Active Adversaries:** active adversaries $\tilde{E}$ have the same properties as the passive eavesdroppers $E$ except that they can also inject arbitrary signals $x(t)$ and $y(t)$ into the environment in order to disrupt or jam Alice and Bob’s key generation process or to seek to gain substantial influence over the generated key. The idealization will be made that $\tilde{E}$ can perfectly synchronize their $x(t)$ and $y(t)$ signal injections with Alice and Bob’s message transfers, where obviously such perfect synchronization is not feasible in the real world.

Given the above adversary model the security of the proposed technique can be detailed as follows.
8.1 Passive Eavesdroppers

The physical nature of NLOS UWB channels ensures that correlations in channel measurements decay rapidly as one moves away from the receiving antenna\[37\]. If shadow fading has been removed as per \[36\], then any channel measurements taken more than 20 cm from a receiving antenna are effectively uncorrelated with the receiving antenna’s measurements. Hence, all passive eavesdroppers located outside of the 20 cm radii neighborhoods of Alice and Bob will receive uncorrelated channel measurements. E’s measurements of the legitimate channel, namely $h_{AE}(t)$ and $h_{BE}(t)$, will therefore provide unusable estimates of $h_{AB}(t) = h_{BA}(t)$ (i.e. the physics of NLOS UWB channels guarantee that E’s measurement error will be large). This provides the guarantee that Alice and Bob will always have information that is unknowable to E. Hence, privacy amplification guarantees that Alice and Bob can always generate a secret key unknowable to E. The achievable secrecy rate will, of course, govern how many channel probes may be required to achieve a desired $k$-bit key.

Since eavesdroppers outside of 20 cm radii of Alice or Bob receive uncorrelated measurements, E gains no advantage by combining multiple $h_{AE}(t)$ and $h_{BE}(t)$ measurements taken at different locations (i.e. averaging across the composite of E’s measurements cannot be used to improve the estimates of $h_{AB}(t)$, as each of these measurements are uncorrelated with each other). Similarly combining measurements from multiple eavesdroppers at the same location is functionally equivalent to a single eavesdropper employing a higher gain antenna. But, increasing Eve’s antenna gain does not improve the correlation between $\{h_{AE}(t|s(t)), h_{BE}(t|s(t))\}$ and $h_{AB}(t|s(t)) = h_{BA}(t|s(t))$. Instead, Eve merely produces a better estimate of $h_{AE}(t)$ and $h_{BE}(t)$. As the correlation does not change, Alice and Bob still retain information in $h_{AB}(t)$ unknowable to the eavesdroppers.

Moreover, even if the eavesdroppers employs directional antennas, these antennas by definition would only measure some of the UWB propagation paths, while obtaining no information of propagation paths outside of the antennas directional windows. Hence, even if Eve was perfectly located on a NLOS path over which the $s(t)$ messages travel (i.e. with one directional antenna facing in the direction of the signal originating from Alice and another facing in the direction of the signal originating from Bob) the other NLOS paths would produce information in $h_{AB}(t)$ unknowable to Eve, thereby enabling privacy amplification to be used. Eavesdroppers would need to be located on all NLOS paths over which the $s(t)$ signals travel, if E is to fully know
Hence, passive eavesdropping can only work when $E$ is sufficiently dense in the wireless environment such that the probability tends to 1 that $E$ has directional antennae located on all NLOS paths through which the $s(t)$ messages pass. For reasonably rich environments, given the 20 cm restriction, such densities would need to be so high as to be both infeasible and clearly observable by Alice and Bob, even if one neglects the effects that such antennas densities would themselves have on the complexity of the wireless environment.

This leaves time averaging as Eve’s only remaining approach. If Alice and Bob perform multiple channel probes (i.e. send multiple $s(t)$ messages) within the coherence time of the channel, for example to improve their ensemble prediction process, then Eve can use time averaging to gain better estimates of $h_{AE}(t)$ and $h_{BE}(t)$. But, again, this does not address the lack of correlation between the $\{h_{AE}(t), h_{BE}(t)\}$ estimates and $h_{AB}(t)$. Moreover, via the ensemble prediction approach of [36], $A$ and $B$ can be innately structured to only use their least predictable portions of the $h_{AB}(t) = h_{BA}(t)$ channel for key generation (i.e. to use the portions of the channel that even they with a full set of channel probe histories cannot predict). These, by definition, are the areas for which averaging cannot improve Eve’s estimates (i.e. averaging filters out differences but Alice and Bob can be easily structured to use probe-to-probe differences as the sources for their key material).

By similar reasoning, if time averaging within the time coherence of the channel cannot help Eve, then pre-characterizing the wireless environment also cannot help, assuming the environment is non-trivial. Moreover, Alice and Bob can use the ensemble prediction process of [36] to test whether the environment is sufficiently rich to support key generation. Hence, they can fail safely in the event that the environment tests out to be trivial (i.e. they can chose not to perform key generation if the available key space proves via their independent measurements to be too small).

Moreover, Alice and Bob take the key bits from the unpredictable portions of the channel, where this unpredictability is based on Alice and Bob having full access to their measurements. Hence, ray tracing also cannot help Eve, given that ray tracing employs abstractions based on the assumed theoretical wireless propagation models and estimates of the environment’s random reflectors and, therefore, must produce worse estimates of $h_{AB}(t)$’s unpredictable portions than are available through Alice and Bob’s actual measurements. Again, the environment must be quite trivial for Eve to deduce the key through ray tracing and Alice and Bob can easily test for such trivial environments. Hence, if the WKG systems is designed correctly and predictable
portions of the measurement (predictable both in time and ensemble) are not used for the key generation, passive eavesdroppers can never do better than a single passive eavesdropper that is located within 20 cm of either Alice or Bob. Assuming the legitimate users can always detect an eavesdropper in such close proximity, then the key generation process is secure against passive eavesdropping.

8.2 Active Adversaries

Active adversaries $\tilde{E}$ seek to disrupt the key generation process or gain influence over the generated key by injecting signals $x(t)$ and $y(t)$ into the wireless environment when Alice and Bob are transmitting their $s(t)$ messages\textsuperscript{1}. For clarity, re-write $x(t)$ and $y(t)$ as the composite signals $x(t) = \hat{x}(t) + \tilde{x}(t)$ and $y(t) = \hat{y}(t) + \tilde{y}(t)$. Denote as $h_{XB}(t|z(t))$, the output of the linear impulse response estimation system for the channel from Alice (terminal A) to Bob (terminal B) at terminal B in response to the stimulus signal $z(t)$ sent from terminal X (where X may be A, B, or $\tilde{E}$). If $\tilde{E}$ is to influence the key bits then $\tilde{E}$ must deduce $x(t)$ and $y(t)$ such that,

\begin{align*}
    h_{AB}(t|s(t)) + h_{EB}(t|\hat{x}(t)) &= 0 \quad (8.1) \\
    h_{BA}(t|s(t)) + h_{EA}(t|\hat{y}(t)) &= 0 \quad (8.2) \\
    h_{EB}(t|\tilde{x}(t)) &= h_{EA}(t|\tilde{y}(t)) \neq 0 \quad (8.3)
\end{align*}

where: a) the active adversary $\tilde{E}$ sends the signal $\hat{x}(t)$ to terminal B over the channel $h_{EB}(t)$ in order to cancel out the channel characterization information contained in terminal A’s transmission of signal $s(t)$ at time $t$ to terminal B over channel $h_{AB}(t)$ (i.e. Eq. (8.1) must be satisfied for $A \xrightarrow{s(t)} B$ with $\tilde{E} \xrightarrow{\hat{x}(t)} B$ sent synchronously), similarly, b) Eq. (8.2) must be satisfied for $B \xrightarrow{s(t)} A$ with $\tilde{E} \xrightarrow{\hat{y}(t)} A$ also sent synchronously, and c) Eq. (8.3) then becomes the information used by A and B to produce their key bits, where these signals must also dominate both $n_A(t)$ or $n_B(t)$ for key generation to occur. It should be noted that, as the key generation process occurs in one step with the transmission of the $s(t)$ messages, $\tilde{E}$ must

\textsuperscript{1}Such active adversaries could also disrupt or corrupt the public discussion protocol messages but, in the worst-case, this can only ever lead to a fail safe operation (i.e. when Eve effectively performs a denial-of-service attack against the public discussion process). As no key bits are exchanged in the public discussion, Eve cannot influence any key arrived at by Alice and Bob in this manner. Hence, it is only the interference with the $s(t)$ messages that is of concern.
send the \( \{\hat{x}(t), \tilde{x}(t)\} \) and \( \{\hat{y}(t), \tilde{y}(t)\} \) signals concurrently with the given \( s(t) \) message transmission, which leads directly to the definitions of \( \tilde{E} \) needing to construct and send the appropriate \( x(t) = \hat{x}(t) + \tilde{x}(t) \) and \( y(t) = \hat{y}(t) + \tilde{y}(t) \) messages. Additionally, the above conditions are an idealization in that it is assumed that \( \tilde{E} \) also uses a directional antenna such that \( A \) cannot measure a response to the \( x(t) \) signal and \( B \) cannot measure a response to the \( y(t) \) signal.

To create these \( x(t) \) and \( y(t) \) signals \( \tilde{E} \) must innately: (a) possess a sufficiently good estimates of the \( A-B \) channel such that Eq (8.1) and Eq (8.2) can be satisfied \( (i.e. \text{such that the information in } h_{AB}(t|s(t)) = h_{BA}(t|s(t)) \text{ can be wiped out}) \) and (b) sufficiently good estimates of the \( E-A \) and \( E-B \) channels such that Eq (8.3) can be satisfied, assuming the idealization is made that the synchronization requirements can be achieved.

Estimating \( h_{AB}(t|s(t)) = h_{BA}(t|s(t)) \) is the same problem faced by the passive eavesdroppers \( E \). But, \( \tilde{E} \) must also simultaneously satisfy Eq. (8.3). In addition, \( \tilde{E} \) must know of the required \( x(t) \) and \( y(t) \) signals prior to \( s(t) \)'s transmissions. Hence, overall \( \tilde{E} \) has a significantly harder problem to solve than \( E \). Moreover, \( \tilde{E} \)'s use of directional antennae and/or multiple locales does not help \( \tilde{E} \) deduce what \( x(t) \) and \( y(t) \) signals should be produced, given that these approaches have also been shown not to aid \( E \). The passive eavesdropper case, therefore, places a lower bound on the effort required by active adversaries. But, if passive eavesdropping can be performed then active attacks are not required as Eve has full knowledge of the key\(^2\).

The only remaining approach available to active adversaries is to jam the entire UWB spectrum used by Alice and Bob. Narrowband jamming, of course, cannot be used as this can be addressed by privacy amplification. Broad spectrum jamming does not increase \( \tilde{E} \)'s knowledge about \( h_{AB}(t|s(t)) = h_{BA}(t|s(t)) \); hence, \( \tilde{E} \) can only use such jamming to overwhelm \( h_{AB}(t|s(t)) = h_{BA}(t|s(t)) \). But such jamming will be seen as non-reciprocal noise by Alice and Bob and, hence, will not enter into their agreed to key bits. Ensemble prediction also ensures that jamming with a non-noise signal cannot be used. Hence, in the presence of jamming, Alice and Bob’s key generation process will still either produce a sufficiently strong key, if the jamming signal is not sufficiently powerful, or fail safely.

Hence, overall the developed technique is susceptible to active or passive adversaries if and only if:

\(^2\)Moreover, active approaches would then not even be desired as they innately expose the attacker to detection, whereas passive eavesdropping does not.
(a) An eavesdropper is within 20 cm of $A$ or $B$,

(b) The eavesdroppers use directional antennae and are sufficiently dense in the environment such that the probability goes to 1 that all NLOS paths used by Alice and Bob are eavesdropped,

(c) An adversary actively jams the entire UWB channel with a noise signal, but this can only reduce the secrecy rate,

(d) Alice and Bob knowingly elect to engage in key generation in a trivial wireless environment.

All of these conditions are observable by Alice and/or Bob. Hence, the technique proposed either generates a sufficiently strong secret key or it fails safely.

It should be noted that the this security against passive eavesdropping and active adversaries directly exploits the high temporal resolution unique to UWB systems and signals (i.e. the ability to independently resolve numerous multi-paths). Hence, these properties do not necessarily translate to narrowband systems in which this high temporal resolution property is lost. Moreover, although the above discussion makes significant use of the lack of correlation in channel characterization measurements outside of Alice and Bob’s 20 cm neighborhoods, it does so only after shadow fading and other predictable effects have been removed. This is distinct from pre-supposing that correlations go to zero outside of 20 cm neighborhoods. Communication literature commonly uses this $\lambda/2$ assumption, but it should be noted this in communications the shadow fading and propagation loss effects are assumed to have been a priori removed. For the security of the key generation approaches it is critical that shadow fading in particular be formally removed from the measured signals prior to key generation.

The remainder of this chapter discusses how capable eavesdroppers leverage the low (but non-zero) spatial correlation of distances greater than $\lambda/2$ from either Alice’s or Bob’ antenna (20 cm in our measurement tests) and compromise the security of the WKG system.

---

$^3$It should be noted that in communications, the $\lambda/2$ antenna separation distances arise as this is the point where destructive interference occurs. Of course, at $\lambda$ separations, for example, constructive interference occurs; hence, correlations do not go to zero outside of $\lambda/2$ for real signals, except for the correlations due solely to fast fading.
8.3 Security tests versus capable eavesdroppers

The reported measurements and tests of Chapters 3 conclude that: a) the theoretical electromagnetic reciprocity exists, b) for distances further than 20 cm (i.e. almost 3\(\lambda\) with regards to our UWB measurement’s center frequency) from either Alice’s or Bob’s antenna an eavesdropper’s measurements have a low (but non-zero) correlation with the measurements of the communicating pair, once shadow fading effects have been removed, and c) channel measurements are likely to be highly correlated over long time offsets within static environments. It is important to assess the security of a given WKG system against capable eavesdroppers who have knowledge of the above properties. The following issues exist:

- Eve may elect to use an antenna array and not just a single antenna, as tested above. Although spatial correlation are low, as per the above test, they are still significant. The measurement advantage that Eve could obtain by using multiple antennas and combining measurements to estimate the radio channel between Alice and Bob must be determined.

- The above experiments do not distinguish how changing the communications channel bandwidth (i.e. from UWB down to narrowband) impacts the WKG systems secrecy rate, particularly against a capable Eve.

- Eve’s ability to exploit ray tracing is also not addressed within the above experiments, whereas it is well known that ray tracing of LOS paths can result in RSS propagation predictions within 3 dB of the actual Alice-Bob measurements [17, 34].

To address these concerns the following capable Eve scenario is constructed. Eve is assumed to have placed 24 antennas surrounding Alice’s antenna at the 20 cm separated 5 \(\times\) 5 grid points outlined above (i.e. Eve is given access to all of the prior experiment measurements except those of the baseline experiment). Eve is then utilizes optimal signal processing methods to make the best possible use of this information to predict the Alice-Bob channel measurements. Eve is also given full knowledge of the Alice-Bob WKG process, except for Alice and Bob’s actual CIR measurements. Finally, to assess the impact of ray tracing, Eve is also given access to the portions of the Alice-Bob channel that Alice and Bob themselves can predict offset by the expected 3 dB error introduced through ray tracing.
Results of the following extensive security tests are reported in terms of the upper-bound on secret key rate (bits / sample). In [43], the upper-bound on secret key rate is calculated. For the case that \(y_A, y_B, \) and \(y_E\) are Alice’s, Bob’s, and Eve’s observations, respectively, from a mutual source of information (i.e. wireless communication channel), this upper-bound is \(I(y_A; y_B | y_E)\).

### 8.4 Eve with an Array Antenna in Different Bandwidths

As Figures 3.5 show, the spatial correlations remain even after the shadow fading effects have been removed via the applied optimal filtering (i.e. the remaining spatial correlations are still \(> 0\)). In general, Eve gains an advantage by placing more antennas in close proximity to either Alice or Bob, where reciprocity entails that surrounding both provides no benefits over just surrounding one of the communicating pair. As described above, it is assumed that Eve has placed 24 antennas around Alice’s antenna, as per Figure 8.1. Eve uses a linear combination of these antenna measurements which to provide an optimal linear minimum mean square error estimate (MMSE) of Alice and Bob’s channel. Obviously, as correlations are reduced with distance it would be of greater benefit to Eve to place antennas near to either Alice and Bob than it would be to place them arbitrarily within the Alice-Bob communications environment. Additionally, the 24 antennas and 20 cm separation distances have been selected pragmatically due to experimental constraints, but it can be argued that any real-world Alice would be quite likely to notice 24 (or even fewer) antennas surrounding her, or antennas surrounding her in density exceeding the 20 cm distances (i.e. pragmatically, these numbers exist as upper bounds on what a real-world Eve (or Eves) should be able to achieve).

Eve then uses the Wiener filter to make the best linear MMSE estimation of the Alice-Bob channel from her available 24 antenna measurements, where it is assumed that Eve’s measurements are perfectly synchronized with Alice and Bob’s WKG process channel probe events. The calculation of the Wiener filter coefficients are described in more detail below. Figure 8.2 shows the block diagram of Eve’s Alice-Bob channel estimation process.

In a time analysis of the obtained measurements, extraordinary data samples are noticed. These are occurred due to non-ideal filtering of measurements. Theses sam-
Removing the outliers: in this test, the outliers of the channel’s fast fading measurements, $X$, which tend to bias the samples, are removed. Criteria under which the $i$-th element of $X$, $X_i$, is removed is determined based on the distance of that element from the median of the vector. In other words, if $|X_i - \text{MED}(X)| > 2 \text{STD}(X)$, the element $X_i$ will be removed, where MED(.) and STD(.) represent median and standard deviation of their input vector, respectively. The vectors with removed outliers are only used in the realization of the predictor’s impulse response, $h$. Removing the outliers eliminates the samples that bias the predictor, and reduces the average prediction error [6].

Weiner filter derivation: denote Eve’s measurements made at time $t$ from 24 antennas surrounding Alice’s antenna by the $x(t) = [x_1(t) \ldots x_k(t) \ldots x_{24}(t)]^T$. Denote the signal received by Alice from Bob’s channel probe event $y(t)$. Eve’s objective is to estimate $y(t)$ since if she has full knowledge of $y(t)$ then she can calculate the same key bits as Alice. The only information available to Alice to estimate $y(t)$ is the information from $x(t_1)$ for all $t_1 \leq t$ and the contents of the public discussions between Alice and Bob. The first step to performing this objective is to provide the optimal estimate of $y(t)$, $\hat{y}(t)$. If it assumed that the radio channel gains are jointly Gaussian random variables then the Wiener filter estimation procedure can
be used to provide optimal linear MMSE estimation which only needs to use the mean, variances and correlations of the random variables to be estimated as well as these same statistical parameters of the available measurements[55]. It is well established in the radio propagation literature that radio channel gains are well modeled as Gaussian
random variables, so the Wiener filter described below for calculating \( \hat{y}(t) \) from \( x(t) \) is optimal in terms of the MMSE.

The general radio channel assumption is made that all channel gains are jointly wide sense stationary (JWSS), so the correlation between \( x(t_1) \) and \( y(t_2) \), \( R_{xy}(t_1, t_2) \) is given by

\[
R_{xy}(t_1, t_2) = E \{ [x(t_1) - E[x(t_1)]] [y(t_2) - E[y(t_2)]] \} \\
= R_{xy}(\tau) \text{ with } \tau = t_2 - t_1.
\]

The (JWSS) properties shown in Eq. (8.4) indicates that it is only necessary to know the relative delay \( \tau \) to specify the correlation. To simplify the estimation equations, the time index \( t \) will not be denoted, so the estimation problem is stated as the calculation of \( \hat{y} \), the estimate of \( y(t_1) \), from the measurement vector of \( x \), where the \( k^{th} \) entry of \( x \) is the measurement from antenna \( k \) at time \( t_2 \), \( x_k(t_2) \), where \( t_2 \) is selected so that the correlation \( R_{xy}(t_2 - t_1) \) is maximized.

The Wiener filter solution for \( \hat{y} \) is given by \( \hat{y} = h^T x(n) \) where \( h \) is the so-called weight vector obtained by solving the Yule-Walker equation given as

\[
h = (R_{xx})^{-1} R_{xy}[55]. \tag{8.5}
\]

The matrix \( R_{xx} \) is the covariance matrix of the vector \( x \) given as

\[
R_{xx} = E \{ [x - E(x)] [x - E(x)]^T \}. \tag{8.6}
\]

\( R_{xy} \) is the cross-covariance of \( x \) and \( y \) which is defined as

\[
R_{xy} = E \{ [x - E(x)] [y - E(y)] \}. \tag{8.7}
\]

The Wiener filter provides an estimate \( \hat{y} \) which has the maximum correlation with Alice’s measurements.

Figure 8.3 shows the test results in different frequency bandwidths. In integrating antennae information in the test, the highest correlation ordering is used (i.e. the Wiener prediction test is performed for an array size of \( n = 1 \) to 24. For a nominal array size \( n = k \), \( k \) antennae that have the highest correlation with the central antenna are selected). Figure 8.3 compares the upper-bound (Eq. (4.11)) on secret key rate of unprocessed measurements (i.e. prior to shadow fading removal) versus innovation
measurements (*i.e.* after shadow fading is removed). In accordance with the reciprocity test’s results, Section 3.3, it is assumed that the cross correlation coefficient of Alice’s and Bob’s measurements, $\rho_{Y_A Y_B}$, equals 0.987 (*i.e.* $\rho_0$ of Eq. (4.11)).

The horizontal axis of Figure 8.3 represents the adjusted bandwidth of the LPFs in Figure 8.2. A general overview shows that the unprocessed measurements reveal more information to eavesdroppers than the innovation of measurements from which shadow-fading is removed. In other words, shadow fading, as theory states, includes a predictable portion of the signal that eavesdroppers can use as leverage for predicting Alice’s and Bob’s measurements.

An additional aspect of this test is the bandwidth effect on the mutual information. Results show that in lower bandwidths, eavesdroppers have more information about Alice and Bob’s channel measurements, and there exists a significant probability that Eve is able to generate the same key as the communicating pair if this high mutual information is not considered in designing the reconciliation process. For example, in the following scenario,

- employing one bit quantizers at Alice and Bob,
- narrowband communication $W = 20$ MHz,
- using unprocessed measurements for key generation (*i.e.* includes shadow-fading),

the secret key rate is zero and Eve is able to generate the same keys as Alice and Bob.

Table 8.1 shows the superiority of eavesdroppers with an array antenna (*i.e.* surrounding either Alice or Bob as Figure 8.1 shows) versus a single antenna eavesdropper, in different bandwidths. The numbers in row “array size” indicate the number of antennae involved in producing the optimum estimation for a specific bandwidth (*i.e.* the upper-bound on the secret key rate, Eq. (4.11), is calculated for antenna array size from $n = 1$ to $n = 24$ at a specific bandwidth, then the maximum value is reported in the table with the corresponding number of antennae created the maximum). A broad conclusion is that using multiple antennae is advantageous to eavesdroppers. A closer look shows that using multiple antennae works better in narrowband versus high frequency bandwidths. A reason for this is that in narrowband, it is more likely that the information of an extra antenna is useful to reduce the noise of the estimation (*i.e.* from the prediction aspect, correlated narrowband measurements of multiple antennae act as additional training samples, which can be
Figure 8.3: Integrated bandwidths and multiple-antenna test; comparing unprocessed and innovative measurements; NLOS channel, distance between Alice’s and Bob’s antennas is 3 m; cross correlation coefficient of Alice’s and Bob’s measurements, $\rho_{Y_A,Y_B} = 0.987$.

used for more accurate tuning the predictor filter coefficients and reducing the prediction error. However, in higher bandwidths the extra antenna information is more likely to be low correlated, and cannot help eavesdropper for a better estimation).

To show that the upper-bound on secret key rate in narrowband (e.g. bandwidths of 20 MHz) communication is independent of the center frequency of the frequency band, a frequency band slicing test is performed. In this test, the received signal
<table>
<thead>
<tr>
<th>BW (MHz)</th>
<th>2 G</th>
<th>1.5 G</th>
<th>1 G</th>
<th>750</th>
<th>500</th>
<th>400</th>
<th>300</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I (X;Y</td>
<td>Z)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>single antenna</td>
<td>2.63</td>
<td>2.56</td>
<td>2.52</td>
<td>2.42</td>
<td>2.54</td>
<td>2.56</td>
<td>2.38</td>
</tr>
<tr>
<td>$I (X;Y</td>
<td>Z)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>multi-antenna</td>
<td>2.54</td>
<td>2.54</td>
<td>2.52</td>
<td>2.34</td>
<td>2.48</td>
<td>2.53</td>
<td>2.38</td>
</tr>
<tr>
<td>array size</td>
<td>2</td>
<td>10</td>
<td>1</td>
<td>18</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 8.1: Eavesdroppers with multiple antennae versus eavesdroppers with single antenna. NLOS channel, Alice’s and Bob’s antenna distance is 3 m, shadow-fading is not removed; cross correlation coefficient of Alice’s and Bob’s measurements, $\rho_{YAYB} = 0.987$.

spectrum is being shifted by 20 MHz frequency steps, then passed through a lowpass filter with a 20 MHz bandwidth. For each frequency step, the upper-bound on the secret key rate of the corresponding frequency band is calculated. Our test confirms that the upper-bound is zero for all the 20 MHz bands in the received signal spectrum for the test environment.

## 8.5 Ray-tracing test

This test is conducted to discern the amount of information an eavesdropper can obtain from the communicating pair’s measurements by applying only a simple ray-tracing algorithm over a part of the channel characteristic (i.e. major reflectors in the environment which include the first impulse of each cluster in the received channel impulse response amplitude [53]). The test procedure is as follows:

a) The algorithm generates a partial channel impulse response, $\hat{y}$, from a set of full channel impulse measurements, $y$. 


b) The ray-tracing algorithm complements the partial impulse response, $\hat{y}$, by employing channel model information, thereby producing the simulated channel, $\tilde{y}$.

c) The algorithm repeats steps (a) and (b) for all eavesdropper’s antennae (i.e. the eavesdropper has an array antenna of size 24 as shown in Figure 8.1).

d) The algorithm removes outliers from $\tilde{y}_i$, where $i$ represents the index of antennae in the array, and produces $\tilde{y}_r$.

e) The algorithm calculates $h$ coefficients of Wiener filter given $\tilde{y}_r$ according to Eq. (8.5).

f) The algorithm filters $\tilde{y}$ with a linear filter realized by $h$.

Criteria of generating $\hat{y}$ from $y$, step (a): to produce a partial channel response, which includes the major reflectors in the environment, the algorithm presumes that only 10% of the received signal energy is coming from the major reflector, and that the eavesdropper measures the major reflector with 3 dB attenuation [17]. Furthermore, the algorithm determines the appropriate threshold that fulfills the criteria, then sets those impulses with power lower than the threshold to zero.

Ray-tracing, step (b): in $\hat{y}$, only the major reflectors are non-zero, all other impulses are set to zero. The ray-tracing algorithm estimates the zero elements of $\hat{y}$ according to UWB indoor channel model of [19]. The channel model shows that the power of rays’ amplitude within clusters have an exponential attenuation. Our rudimentary ray-tracing technique substitutes the zero elements of $\hat{y}$ with the equivalent estimated elements from the exponential modeling, and produces $\tilde{y}$.

Figure 8.4 shows the result of the above ray-tracing algorithm over an NLOS channel when the distance between Alice’s and Bob’s transceivers is 3 m. In this test, the shadow-fading is not removed. The horizontal axis indicates the bandwidth of the communication. Also, eavesdroppers use a combination of their array which maximize the upper-bound on secret key rate.

The results of Figure 8.4 show that in UWB ($W > 500$ MHz) and wideband ($W > 150$ MHz), ray-tracing over 24 channels works almost like a system that is given complete channel characterization over 24 channels (i.e. both ray-tracing and complete systems in Figure 8.4 are close to the solid line that indicates $I(Y_A;Y_B)$, which is equal to secret key rate if eavesdroppers receive independent measurements.
from Alice’s and Bob’s measurements.). Apparently, as it is better can be seen in lower bandwidths of Figure 8.4, eavesdroppers given complete channel characterization make a more accurate estimate of Alice and Bob’s channel than eavesdroppers with only ray-tracing information. Though, an interesting observation in lower bandwidths of Figure 8.4 is the decreasing in secret key rate by applying a ray-tracing algorithm over unprocessed measurements (e.g. in $W = 20$ MHz the upper-bound almost $50\%$ decreases regarding the case that eavesdroppers have no information from Alice and Bob’s channel, where the upper-bound is $I(Y_A; Y_B)$, by only applying a ray-tracing algorithm).

### 8.6 Concerns in reconciliation procedure

In this section, it is demonstrated that key generation must be carefully designed when the eavesdroppers’ measurements are correlated with those of the legitimate users. The simulation is performed as follows:

a) A random vector, $h$, consisting of $N$ independent and identically distributed Gaussian random values is generated where $N$ is the number of bits in the LDPC code’s codeword.

b) The legitimate users, Alice and Bob, as well as the eavesdropper, Eve, each measure the clean signal, $h$, with independent additive Gaussian white noise with mean signal-to-noise ratios (SNRs). The measurement vectors of Alice, Bob, and Eve are denoted as $y_A = h + z_A$, $y_B = h + z_B$, and $y_E = h + z_E$ with $z_A$, $z_B$, and $z_E$ are the zero mean measurement noise vectors for Alice, Bob, and Eve, respectively.

c) The SNRs for each user is denoted as $SNR_X = E\{h^2(n)/z_X^2(n)\}$ where $X$ is $A$, $B$, or $E$ for Alice, Bob, and Eve respectively. For the simulations described in this Appendix, $SNR_A = SNR_B$ and $SNR_E$ is $6$ dB less than the $SNR$ of Alice and Bob.

d) An rate $9/10$ LDPC code with a codeword length of $64800$ bits is employed. It is a standard LDPC code used in the digital video broadcast standards [18].

e) Alice feeds its received signal vector $y_A$ into a standard soft output BPSK detector with the log-likelihood ratio output, $LLR_A$, being fed into an LDPC decoder to
Figure 8.4: Ray-tracing test. NLOS channel, Alice’s and Bob’s antenna distance is 3 m, shadow-fading is not removed; cross correlation coefficient of Alice’s and Bob’s measurements, $\rho_{Y_A Y_B} = 0.987$.

obtain $\hat{LLR}_A$. The decoded bits are then fed into a BPSK modulator to obtain the signal $s$. The analog correction signal $c_A = y_A - s$ and binary correction signal $\tilde{c}_A = \text{sign} \left( \hat{LLR}_A \otimes LLR_A \right)$, where $\otimes$ denotes element-wise multiplication, are transmitted from Alice to Bob and can be intercepted by Eve.

f) Bob applies the analog correction to its input signal to calculate $\hat{y}_B = y_B - c_A$ which is then fed into a soft output BPSK detector to obtain the log-likelihood
ratio output, $LLR_B$. The binary correction from Alice is applied to the vector of log-likelihood values to obtain $\widehat{LLR}_B = LLR_B \otimes \tilde{c}_A$. Eve can apply the same detection and correction to its received vector to obtain $\widehat{y}_E$ and $\widehat{LLR}_E$.

\begin{itemize}
  \item[g)] Bob feeds its corrected LLR values, $\widehat{LLR}_B$, into a LDPC decoder to obtain $\widehat{\tilde{c}}_B$. Eve performs the same calculation to obtain $\widehat{\tilde{c}}_E$.
  \item[h)] Bob calculates its clean BPSK signal $s_B$ from a hard decision on $\widehat{\tilde{c}}_B$. Eve computes its clean BPSK signal as $s_E$.
  \item[i)] The Bit Error Rate for Alice and Bob is calculated as the number of differences between $s$ and $s_B$ divided by the length in bits $N$.
  \item[j)] The Bit Error Rate for Alice and Eve is calculated as the number of differences between $s$ and $s_E$ divided by the length in bits $N$.
\end{itemize}

![LDPC Reconciliation Method Performance](image)

Figure 8.5: Reconciliation process uses a rate 9/10 LDPC code; $(n = 64800, k = 58320)$. Eavesdropper measurement SNR is 6 dB lower than A and B’s measurements. Soft information is transferred over public channel.

Figure 8.6 shows that for SNRs less than 5 dB, Alice’s and Bob’s digital signals have significant probability of mismatch and key generation will likely fail. For $5 \text{dB} < SNR < 8 \text{dB}$, Alice and Bob will generate the same bit string with a very high probability and key generation will very likely succeed. However, for $SNR < 8 \text{dB}$, Eve’s generated binary string will have a significant probability of having a number of bits different from that of Alice and Bob. After key generation, Alice and Bob can
employ privacy amplification to ensure the bits of Alice and Bob’s common sequence known to Eve do not compromise the generated secret key.

When Eve has a SNR greater than 2 dB ($SNR_A > 8$ dB), the Eavesdropper can obtain Alice and Bob’s key with little or no error. Note that since Eve has access to the correction information sent from Alice to Bob, Eve has a 3 dB advantage over Alice and Bob. Consequently, the system designer must carefully consider the effect the choice of error-correction code used by Alice and Bob to ensure that it does not allow Eve to compromise the generated key.

In this test results, in terms of bits, it has been shown that how, bandwidth, Line-of-Sight information, and multiple antenna information can help eavesdropper to obtain correlated channel measurements with A and B (i.e. in some cases, over 75% of the bits are incommon).

### 8.7 Summary

The security of the proposed key generation system of Chapter 5 is analysed. It is shown that the system is secure against passive eavesdropping, where eavesdroppers are located farther than $\lambda/2$ from either member of the communicating pair engaged in the WKG process (i.e. eavesdroppers measure the fast fading independent from the communicating pair). In a smart active attack, where adversaries desire to forge a known key to be generated with the communicating pair, it is shown that active adversaries can not do better than passive eavesdroppers, where the active attackers are separated with distances larger than $\lambda/2$ from either member of the communicating pair. It is also shown that active attackers can only randomly jam the entire spectrum; this strategy is detectable and results in a safe failure in the proposed WKG process.

Moreover, the security of the WKG system is assessed against a capable eavesdropper who (a) surrounds either member of communicating pair with a multiple array antenna (size 24, spatial distance of array greater that $\lambda/2$), (b) is aware of perfect synchronization information, and (c) has optimal signal processing tools. It is shown that if shadow fading is not removed by optimal techniques then the upper bound of the secret key rate, particularly for broadband communication (e.g. bandwidth of 20 MHz), is zero or close to zero. It also shows how a multiple array antenna assists eavesdroppers in making a more accurate estimation. Furthermore, it is shown that ray-tracing of the major reflector in the environment (not a complex problem
for eavesdroppers) with accuracy of 3 dB of estimation error decreases the upper bound of the secret key rate (in lower bandwidths it drops to 50% in cases where no ray-tracing information is provided to eavesdroppers). Finally, it is shown that when capable eavesdroppers are present in the environment, $I(y_A, y_B | y_E) < I(y_A, y_B)$, there are security concerns that must be considered in designing the error correction code power of the reconciliation procedure (an example is provided for the case of LDPC code of the rate 9/10).
Chapter 9

Conclusions

This dissertation has pragmatically studied the security of WKG systems against capable eavesdroppers. The results of this research can be concluded as follows:

• The theoretical results are presented to develop a key generation process based on characterizations of NLOS UWB channels. More particularly, this technique focuses on addressing key generation within stationary environments, such as exists for point-of-sale devices and/or wireless keyboards (i.e. application domains not well addressed by key generation methods requiring significant Doppler spreading).

• The theoretical maximum secret key rate that can be achieved via idealized UWB channel models is derived.

• The MIMO advantage in increasing secret key rate is studied and new bounds for MIMO systems are extracted.

• The basic key generation method is developed inclusive of the required error correction, privacy amplification, and public discussion processes.

• The proposed key generation system is shown to be theoretically secure against both passive eavesdroppers and active adversaries.

• The security of the proposed WKG system is assessed against a capable eavesdropper who (a) surrounds either member of the communicating pair with a multiple array antenna (size 24, spatial distance of array greater than $\lambda/2$), (b) is aware of perfect synchronization information, and (c) possesses optimal signal processing tools.
• In the case of capable eavesdroppers, it is shown if shadow fading is not removed by optimal techniques then the upper bound of secret key rate, particularly for broadband communication (e.g. bandwidth of 20 MHz), is zero or close to zero.

• In the case of capable eavesdroppers, it is shown that, in practice, multiple array antenna assist eavesdroppers in achieving a more accurate estimation of the communicating pair’s channel (i.e. eavesdroppers are able to compromised the system security).

• Security is assessed against eavesdroppers who are provided with the ray-tracing information of the major reflector in the environment (i.e. this is not a computationally complex problem for eavesdroppers) with accuracy of 3 dB of estimation error. It has been shown that this information affects the upper bound of the secret key rate (in lower bandwidths almost 50% decrease) in contrast to having no ray-tracing information provided to eavesdroppers.

• It is shown that in the presence of capable eavesdroppers in the environment, where \( I(y_A, y_B | y_E) < I(y_A, y_B) \), there are security concerns that must be considered in designing the error correction code used in the reconciliation procedure (an example is provided for the case of LDPC code of rate 9/10).

• The methodology based on linear adaptive least square error prediction has been developed to ensure that predictable portions of UWB channel characterizations are not used as the basis for key generation processes. It is shown that without applying such approaches, if a rich past history of channel measurements is assumed and the physical environment is highly static, 90+% of the next channel characterization measurements are highly predictable.

• It is shown that extending the proposed key generation to MIMO systems and employing random beamformers solves the high temporal correlation of the stationary environments, where the two end users engaged in the key generation process are not moving. Independent random beamforming can provide increased the security even in the case of an highly idealized eavesdropper who is assumed to have prefect knowledge of the MIMO channel.

There are open issues that the future of this research can follow. These open problems are as follows:
• Translating the proposed approach into low-cost chip-level circuitry, where addressing the sampling rate required for GHz bandwidth signals becomes a significant issue. This same sampling rate question is being addressed in the research domains of compressive sampling for channel estimation and software defined radio; hence, as development in these areas mature, they will be directly applicable to UWB key generation.

• In applying random beamformers to solve the security issue of stationary environments, in this dissertation, it is ideally assumed that eavesdroppers estimation of random beamformers’ coefficients’ angles are Gaussian. An accurate modeling of theses angles’ estimation error with wrapped Stable distributions can be explored in the future of this research.

• For domains such as sensor networks it becomes attractive to leverage the point-to-point key generation approach available via UWB key generation into network-wide security (i.e. where one node can communicate securely with an arbitrary node of the network that is more than one hop away). Work is currently under way on developing such a network-level extension.

• Previous theoretical works have discussed how public information transmitted during reconciliation procedure can assist eavesdroppers to compromise the security of a WKG system. Our practical security tests against capable eavesdroppers verifies the theory and raises concerns about the reconciliation procedure’s design (e.g. the error correction power of the code used for reconciliation). In future research, there is the potential to formalize this limitation.
Bibliography


Appendix A

Formulas

A.1 Derivation of Eq. (7.18)

The steps for deriving Eq. (7.18) are as follows:

\[
\mathbb{E}[\tilde{r}^2] = s^2\mathbb{E}\left[ \text{tr}\left( \tilde{\mathbf{w}}_T^H \mathbf{R} \tilde{\mathbf{w}}_R^\dagger H^\dagger \tilde{\mathbf{w}}_T^* \right) \right] \\
= s^2\mathbb{E}\left[ \text{tr}\left( \mathbf{R} \tilde{\mathbf{w}}_R^\dagger H^\dagger \tilde{\mathbf{w}}_T^* \mathbf{R} \hat{\mathbf{w}}_T^* \right) \right] \\
= s^2\text{tr}\left[ \mathbb{E}\left( \hat{\mathbf{w}}_R^\dagger \mathbf{R} \hat{\mathbf{w}}_R^* \right) H^\dagger \mathbb{E}\left( \hat{\mathbf{w}}_T^* \tilde{\mathbf{w}}_T^* \right) \right].
\]

(A.1)

By definition of

\[
\rho^{1/2} = \mathbb{E}\left[ e^{jz_t^{(k)}} \right] \\
= \mathbb{E}\left[ e^{jz_t^{(k)}} \right],
\]

(A.2)

then we have,

\[
\mathbb{E}\left( \hat{\mathbf{w}}_R^\dagger \hat{\mathbf{w}}_R^\dagger \right) = [d_{mk}]; \quad d_{mk} = \begin{cases} 
1 & m = k \\
\rho & m \neq k
\end{cases}.
\]

(A.3)
According to the definition of $D_r$ in Eq. (7.14), the above equation can be rewritten as

\[
\mathbb{E}\left( \tilde{w}_R \tilde{w}_R^\dagger \right) = \rho D_r + (1 - \rho) I_N. \quad (A.4)
\]

With similar process we have,

\[
\mathbb{E}\left( \tilde{w}_T^* \tilde{w}_T^\prime \right) = \rho D_t^* + (1 - \rho) I_N. \quad (A.5)
\]

Consequently, Eq. (7.18) is deduced.

### A.2 Derivation of Eq. (7.22)

It is assumed that $H$ is a real random matrix that each member of $H$ is normally distributed with zero mean and $\sigma^2_h$ variance, and $\mathbb{E}[h_{ij}h_{mk}] = 0$ where $i \neq m$ or $j \neq k$. Also, full reciprocity is presumed $h_{ij} = h_{ji}$; therefore, $H^\dagger = H'$. With respect to our notation, the Theorem 7.3.1’s variables are redefined as follows: $U = \sigma^2_h$, $V = I_N$, $M = 0$, and $B = D_r$.

\[
\mathbb{E}[A] = \mathbb{E}_H \left[ \text{tr} \left( H D_r H^\dagger D_t^* \right) \right] \\
= \text{tr} \left[ \mathbb{E}_H \left( H D_r H' \right) D_t^* \right] \\
= \text{tr} \left[ \mathbb{E}_H \left( D_r \sigma^2_h I_N D_t^* \right) \right] \\
= N \sigma^2_h \text{tr} [D_t^*] \\
= N^2 \sigma^2_h. \quad (A.6)
\]