

Article

Physical Layer Security: Channel Sounding Results for the Multi-Antenna Wiretap Channel

Daniel Harman , Karl Knapp, Tyler Sweat, Philip Lundrigan , Michael Rice and Willie Harrison 

Department of Electrical and Computer Engineering, Brigham Young University, Provo, UT 84602, USA; knapp5@byu.edu (K.K.); tyler.sweat@byu.edu (T.S.); lundrigan@byu.edu (P.L.); mdr@byu.edu (M.R.)

* Correspondence: jdharman@byu.edu (D.H.); willie.harrison@byu.edu (W.H.)

Abstract: Many physical-layer security works in the literature rely on purely theoretical work or simulated results to establish the value of physical-layer security in securing communications. We consider the secrecy capacity of a wireless Gaussian wiretap channel using channel sounding measurements to analyze the potential for secure communication in a real-world scenario. A multi-input, multi-output, multi-eavesdropper (MIMOME) system is deployed using orthogonal frequency division multiplexing (OFDM) over an 802.11n wireless network. Channel state information (CSI) measurements were taken in an indoor environment to analyze time-varying scenarios and spatial variations. It is shown that secrecy capacity is highly affected by environmental changes, such as foot traffic, network congestion, and propagation characteristics of the physical environment. We also present a numerical method for calculating MIMOME secrecy capacity in general and comment on the use of OFDM with regard to calculating secrecy capacity.

Keywords: physical-layer security; MIMO wiretap channel; multiple antennas; channel sounding; secrecy capacity; channel coding



Citation: Harman, D.; Knapp, K.; Sweat, T.; Lundrigan, P.; Rice, M.; Harrison, W. Physical Layer Security: Channel Sounding Results for the Multi-Antenna Wiretap Channel. *Entropy* **2023**, *25*, 1397. <https://doi.org/10.3390/e25101397>

Academic Editors: Bill William Buchanan, Arslan Munir and Jawad Ahmad

Received: 24 August 2023

Revised: 19 September 2023

Accepted: 25 September 2023

Published: 29 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Over the last several decades, advancements in multiple antenna technology and multi-carrier waveforms have resulted in reliable wireless communications with increased bit rates. As advancements continue, the need for increased security has never been more important. Cryptography is the widely accepted method for secure transmission, relying on mathematical and computational complexity. As computation technology increases, such as with quantum computing, and subsequently time required to attack such systems decreases, additional security measures may need to be added [1]. In other situations, such as for Internet of Things (IoT) devices, high-level cryptography may be entirely unreasonable due to limited computational ability or power constraints.

Physical-layer security can offer additional security to that provided by cryptography with strong information-theoretic guarantees [2–4]. The additional security helps with situations such as key sharing while simultaneously increasing the eavesdropper's confusion about the message [5]. Physical-layer security operates through novel uses of signaling [6] and coding techniques [7].

Shannon introduced the idea of *perfect secrecy* [8], which is expounded upon within Wyner's wiretap model [9]. More recently, work with the multi-input multi-output multi-eavesdropper (MIMOME) Gaussian wiretap channel has been conducted by Khisti and Wornell [10], Oggier and Hassibi [11], and Liu and Shamai [12], yielding a model for the general case of multi-antenna secrecy capacity setups. Despite this information-theoretic foundation, very little work has been conducted in channel sounding to find realistic estimates for the MIMOME secrecy capacity in real-world environments [13]. Work in this area has been conducted with regards to single-input single-output (SISO) systems [14], and SISO vehicle-to-vehicle (V2V) systems [15].

We consider a three-node MIMOME system with two transmit antennas, two receiver antennas, and two eavesdropper antennas, deployed in a highly trafficked indoor environment. We assume a genie-aided system in which the channel state information (CSI) is known at all terminals, and no cryptography is employed. Over a period of time, we capture CSI using off-the-shelf hardware and calculate the secrecy capacity of the environment subject to both temporal and spatial variations to analyze the potential efficacy of physical-layer security in a real-world scenario. We discuss the impacts of the specific environment, such as foot and network traffic, and building construction. We show that these impacts can have significant effects on secrecy capacity over a wide range of SNRs. We also discuss the use of orthogonal frequency division multiplexing (OFDM) in the 802.11n WiFi standard with regard to calculating secrecy capacity. Finally, we provide a numerical method to optimize a brute force search to calculate MIMOME secrecy capacity in general, for any arbitrary SNR. Note that this work does not include a discussion or prescription for deploying channel coding in the case of the MIMOME channel, as no conclusive work yet exists as to what class of codes to use, and such a work would merit a number of publications of its own.

While many of the works listed previously rely on purely theoretical approaches to physical-layer security, this work analyzes actual channel sounding results captured in a real environment. Coupling the theoretical foundation with real experimental measurements, we demonstrate the potential efficacy of a MIMO physical-layer scheme in an indoor office-like environment using existing commercial hardware employing WiFi, an existing protocol. This is a vital next step in realizing the widespread use of physical-layer security, as it will hopefully inform future research and development efforts about the expected performance of any complete physical-layer security system. Additionally, there is little work on calculating MIMOME secrecy capacity in general, and this paper provides a simple, low-complexity algorithm to accomplish this.

The paper is organized as follows. Section 2 is a brief explanation of the notion used. Section 3 presents the wiretap channel model and assumptions used to calculate the secrecy capacity, including the details of our optimization algorithm for calculating MIMOME secrecy capacity. The procedure for acquiring the CSI, the physical environment and other variables are discussed in Section 4. We make concluding remarks in Section 5.

2. Notation

Bold font lower-case characters are reserved for vectors. Bold font capital letters represent either matrices or random variables, made clear by the context. Vector and matrix dimensions are either denoted as superscripts or made clear within the text. Vector dimensions also explicitly state whether each vector is a row or column vector by use of $1 \times n$ or $n \times 1$, respectively. Subscripts usually connect a variable to a user within the wiretap model, with a few exceptions. For example, C_s denotes secrecy capacity and k_i denotes an element, of index i , within a vector. $\mathbf{I}$ denotes the identity matrix and $\mathbf{0}$ denotes the zero matrix, where the respective dimensions are made clear by context. We let $\mathbb{C}^{m \times n}$ represent the set of all $m \times n$ dimensional complex matrices. Circularly symmetric complex Gaussian random variables with mean zero and covariance matrix $\mathbf{I}$ are denoted as $\mathcal{CN}(0, \mathbf{I})$. Also, we use $\text{range}(x, y, z)$ to denote a vector starting at x , ending at y and of length z . Where z is not denoted, it is left for the context to determine. Furthermore, all logarithms are assumed to be base 2.

Additionally, we use $\det(\cdot)$ and $\text{tr}(\cdot)$ to denote the determinant and trace of a matrix while $\text{diag}(\cdot)$ denotes a diagonal matrix whose argument determines the diagonal elements of the matrix. The superscripts T and † are used as the matrix transpose and the conjugate transpose operators, respectively. $\|\cdot\|$ denotes the Euclidean vector norm, and $\|\cdot\|_F$ denotes the Frobenius norm of a matrix. Finally, we use $\mathbf{A} \succeq 0$ to denote a positive semi-definite matrix $\mathbf{A}$.

3. Channel Model and System Setup

The framework for our experimental model is based on Wyner's 1975 work on the wiretap channel [9]. The model assumes three users: Alice, the legitimate transmitter; Bob, the legitimate receiver; and Eve, a passive eavesdropper. Alice transmits an encoded message as x to Bob over the main channel. Bob and Eve receive y_m and y_e , respectively, which are noisy versions of the input x ; see Figure 1. We assume that the main and eavesdropper's channels are time-varying, but are static for the duration of an individual transmission. Additionally, our setup features the use of multiple antennas for all nodes. As for the wiretap setup, we assume that Eve is capable of receiving and decoding messages sent from Alice. Finally, both Bob and Eve have an OFDM demodulator with cyclic prefix removal and FFT [16,17].

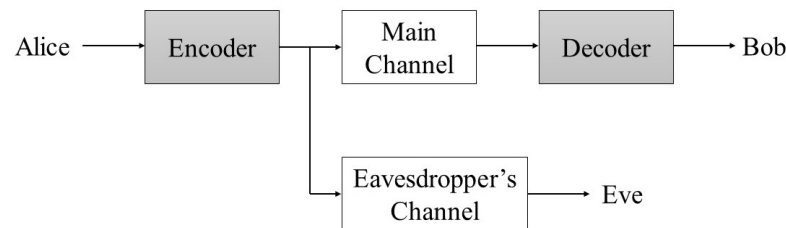


Figure 1. Wyner's wiretap model.

3.1. MIMOME Secrecy Capacity

The work in [10,11] independently developed the model for the MIMOME wiretap channel. In this work, we let the channel models for Bob and Eve be represented by

$$\begin{aligned} y_m(t) &= H_m(t)x(t) + z_m(t) \\ y_e(t) &= H_e(t)x(t) + z_e(t) \end{aligned} \quad (1)$$

respectively, where $x(t) \in \mathbb{C}^{n_t \times 1}$ is the OFDM transmitted signal vector at time t , and $H_m(t) \in \mathbb{C}^{n_m \times n_t}$ and $H_e(t) \in \mathbb{C}^{n_e \times n_t}$ are the channel gain matrices of the main and eavesdropper channels, respectively, at time t . We use n_t , n_m , and n_e to denote the number of transmitter, main receiver and eavesdropper antennas. The noise, at time t , is represented by $z_m(t) \in \mathbb{C}^{n_m \times 1}$ and $z_e(t) \in \mathbb{C}^{n_e \times 1}$, which are independent and identically distributed (i.i.d.) as $\mathcal{CN}(0, I)$.

The channel input is subject to the power constraint

$$E\{|x(t)|^2\} \leq P \quad (2)$$

where P is the total power constraint and the expectation is taken with regard to time. For brevity, the remainder of this work will omit function notation with regard to time, unless otherwise noted. The secrecy capacity is defined as the supremum of all achievable rates that satisfies the power constraint and the min-max optimization problem, i.e., maximizing the main channel capacity while minimizing the eavesdropper channel capacity. Secrecy capacity is expressed as

$$C_s = \max_{K_x} \left(\log \frac{\det\left(I + \frac{1}{\sigma_m^2} H_m K_x H_m^\dagger\right)}{\det\left(I + \frac{1}{\sigma_e^2} H_e K_x H_e^\dagger\right)} \right), \quad (3)$$

where the main and eavesdropper channels have noise variances σ_m^2 and σ_e^2 , respectively. We use K_x to denote the covariance matrix of x , i.e., $K_x = \mathbb{E}\{xx^\dagger\}$. The power constraint (2) can be written with K_x , such that

$$K_x \triangleq \{K_x : K_x \succeq 0, \quad \text{tr}(K_x) \leq P\}. \quad (4)$$

Note that all covariance matrices are positive-semi-definite by definition; however, we explicitly state this property for clarity. As noted in [18], the total power channel gain is defined as $\|\mathbf{H}\|_F$, where $\mathbf{H}$ is a channel gain matrix. This does, however, only apply in conditions where the total transmit power is equal for all transmit antennas. As the transmitter in general does not have equal power across all transmit antennas, and to maintain a consistent metric for both the main and eavesdropper channels, we define SNR for the MIMO case [19] to be

$$\text{SNR} = \frac{P}{\sigma_n^2} \quad (5)$$

where, $\sigma_n^2 = \sigma_m^2 = \sigma_e^2$.

3.2. High-SNR Asymptotic Results

We exploit the high-SNR asymptote from [10] in our analysis to check the accuracy of the brute force search described below. In the high-SNR regime, the secrecy capacity approaches a non-zero threshold for the maximum achievable secure rate. The generalized singular value decomposition (GSVD) is used to decompose the channel gain matrices into an equivalent parallel channel model. We define m_i and e_i to be the individual generalized singular values of the main and eavesdropper channels, respectively. We follow the convention of choosing the arbitrary indexing where singular values are ordered by ascending magnitude. Thus, we assign the generalized singular values as,

$$\sigma_i \triangleq \frac{m_i}{e_i}, i = 1, 2, \dots, s, \quad (6)$$

where s is the total number of singular value pairs. The high-SNR regime asymptote for secrecy capacity is then given as

$$\lim_{P \rightarrow \infty} C_s(P) = \sum_{j: \sigma_j \geq 1} \log \sigma_j^2, \quad (7)$$

because of the condition given in [10] that $\text{rank}(\mathbf{H}_e) = n_t$.

3.3. Note on Multi-Carrier Waveforms

A hallmark of the IEEE 802.11 standards for WiFi has been its use of OFDM, increasing both rates and reliability. Our approach to the MIMOME secrecy capacity includes the use of all 56 subcarriers available in the 802.11n standard. There has been some work conducted on the OFDM water-filling problem [20] for the MIMOME secrecy capacity with multi-carrier waveforms with a particular focus on energy efficiency; however, more work still remains to be conducted for an efficient solution that maximizes secrecy rate. Solutions designed around maximizing secrecy rate would begin with a total power constraint and then optimally allocate power to each of the main channel's subcarriers' eigenmodes while simultaneously minimizing the power transmitted to the eavesdropper, [16,21,22]. With a protocol such as any of the 802.11 standards and enough antennas, this can prove to be a daunting optimization problem, even when employing efficient iterative numerical methods designed for the non-convex, non-smooth nature of the optimization. If such solutions are to be deployed in real-world systems, it would be expected from previous work that the secrecy capacity would be significantly higher.

Thus, due to this constraint, we consider each subcarrier channel as having its own power constraint equal to the power constraints of the other subcarriers. The total secrecy capacity is then considered to be the sum of the secrecy capacity of all available subcarriers, defined below as,

$$C_s^{\text{OFDM}} = \sum_{i=1}^q C_s(i) \quad (8)$$

where i is the index of subcarrier, and q is the total number of subcarriers.

3.4. Brute-Force Optimization

This section outlines our technique for calculating MIMOME secrecy capacity based on a brute force algorithm. There exist other techniques in the literature that either focus on minimizing power [23] or gradient descent algorithms for specific cases [24]. The algorithm presented here is simple and based on constraining the search region under the assumption that the transmitter has a fixed power input as in (4). The algorithm presented here could be paired with the algorithm presented in [24] to better determine the starting criteria for the gradient descent method. This paper's novel contribution to this area lies mainly in its ability to constrain the search region using the method described below, which is an essential step whatever the final minimization technique.

As noted in [25], the objective function in the secrecy capacity expression (3) in general does not satisfy the Karush–Kuhn–Tucker (KKT) conditions; thus, a brute force search is used to identify the optimal input covariance matrix, K_x . During our analysis, we found that the most computationally expensive cases can be predetermined by the GSVD analysis proposed in [10] and eigenvalue analysis proposed in [11]. The work conducted in [11] considers two cases, which they refer to as the *definite* and *indefinite* cases. The *definite case* is defined by the following, which corresponds to a definite advantage for either the main or eavesdropper channels, respectively:

$$H_m^\dagger H_m \succ H_e^\dagger H_e, \quad (9)$$

$$H_e^\dagger H_e \succ H_m^\dagger H_m. \quad (10)$$

The definite case corresponds to the condition in (7), where all generalized singular values are greater than one. The *indefinite case* is where a clear advantage is not present for either the main or eavesdropper's channel. It is defined where both of the following expressions, (11) and (12), are true, i.e., $H_e^\dagger H_e - H_m^\dagger H_m$ has positive eigenvalues in addition to others that are zero or negative. Precisely,

$$H_e^\dagger H_e \not\geq H_m^\dagger H_m, \quad (11)$$

$$H_m^\dagger H_m \not\geq H_e^\dagger H_e. \quad (12)$$

The indefinite case corresponds to the condition in (7), where only some of the generalized singular values are greater than one.

The indefinite case is where we found the most difficulty with the brute force search. We found this analysis to be a natural starting point to determine the needed precision in the optimization, as checking for either the definite or indefinite case is computationally inexpensive relative to a high-precision search. In the definite case, lower precision is often sufficient to optimize to the desired level of accuracy. In the indefinite case, a substantially higher level of precision is required, as the gradient often has much more extreme changes around local and global extrema.

To simplify the brute force search, we restrict the search area to a region that satisfies all problem constraints; see (4). We assume that the optimal solution involves using all available power, which may not hold for all scenarios but it held true for our measurements and setup. This assumption makes the expression (4) solely an equality, restated below in (14). Given that our experimental data was gathered using NICs where $n_t = n_m = n_e = 2$, we define the following degrees of freedom in the search, such that

$$k \triangleq [k_1, k_2, k_3], \quad (13)$$

where

$$K_x \triangleq \{K_x : K_x \succeq 0, \quad \text{tr}(K_x) = P\} \quad (14)$$

and

$$0 \leq k_1 \leq P, \quad (15)$$

such that

$$\mathbf{K}_x = \begin{bmatrix} k_1 & k_2 - jk_3 \\ k_2 + jk_3 & P - k_1 \end{bmatrix}. \quad (16)$$

We begin by creating a set of nested for loops, iterating over each combination of all degrees of freedom with a hierarchy described by the order in (13). A closed-form expression can be found that restricts the search area for each iteration of k_1 by exploiting the quadratic formula during the process of finding the eigenvalues of $\mathbf{K}_x$, ensuring the positive-semi-definite condition in (14).

We begin with the identity of the eigendecomposition,

$$|\mathbf{K}_x - \lambda \mathbf{I}| = 0. \quad (17)$$

We let,

$$\mathbf{K}_\lambda = \begin{bmatrix} k_1 - \lambda & k_2 - jk_3 \\ k_2 + jk_3 & P - k_1 - \lambda \end{bmatrix} \quad (18)$$

Combining terms and simplifying yields

$$|\mathbf{K}_\lambda| = 0. \quad (19)$$

Next, we solve for the characteristic polynomial, i.e.,

$$\det \mathbf{K}_\lambda = \lambda^2 - \lambda P + k_1 P - k_1^2 - k_2^2 - k_3^2$$

and utilize the quadratic formula to solve for the roots of the characteristic polynomial, given as

$$\lambda = \frac{P \pm \sqrt{P^2 - 4(k_1 P - (k_1^2 + k_2^2 + k_3^2))}}{2}. \quad (20)$$

Analysis of (20) reveals that $\lambda \geq 0$ if

$$k_1 P \geq k_1^2 + k_2^2 + k_3^2, \quad (21)$$

thus ensuring a positive semi-definite condition.

With the search area constrained, it is advantageous to search the edge cases, as we found that the edges often contain local extrema. From the above expression, the maximum radius, $\tilde{r}$, is calculated as

$$\tilde{r} = \sqrt{k_1(P - k_1)}. \quad (22)$$

A radial or grid search is then employed, where k_2 and k_3 are constrained by (21) and (22). A grid search produces k_2 and k_3 in range $(-\tilde{r}, \tilde{r})$. A radial search produces r and θ in range $(0, \tilde{r})$ and range $(0, 2\pi)$, respectively. We then convert r and θ from polar to rectangular coordinate systems, producing the appropriate values of k_2 and k_3 . Iterating k_1 in range $(0, P)$ over a sufficiently large interval provides the required level of accuracy. The accuracy of the search can be checked against the high-SNR asymptotic approach (7).

This closed-form expression is usually computationally cheaper than the ill-conditioned problem of calculating eigenvalues to ensure the positive-semi-definite condition (14). In our experience, using this method and the radial search described previously was approximately 3600 times faster than an ill-targeted brute force search based on timers in our code. This method can be exploited for higher dimensional covariance matrices; however, it is limited by the closed-form solution to solving for the roots of a polynomial expression.

4. Channel Sounding

4.1. Environments

A temporal wiretap scenario simulating a passive eavesdropper attack was implemented in the step-down lounge study area of the Clyde Building at Brigham Young University (see Figure 2 for building layout). The area where data were gathered is open and the walls are cinder block with many windows on the west-facing wall. On the north end, there is an area partitioned by a glass wall in which Alice and Bob were set up about 10 m apart. Eve was set up outside the study area approximately 33.5 m from Alice to sufficiently disadvantage the eavesdropper while maintaining line of sight.

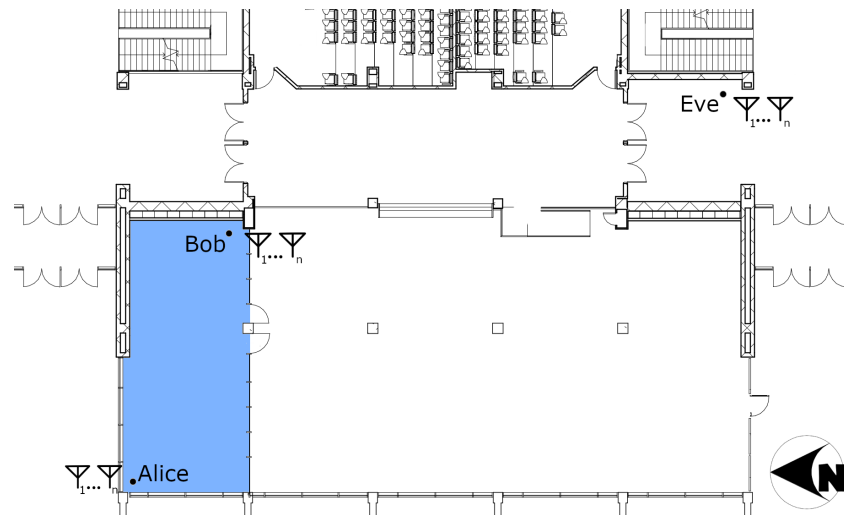


Figure 2. Indoor environment where the experiment was staged. The blue area is partitioned off from the main area by a glass wall and door.

A set of space-varying experiments were implemented in two parts on both the fourth floor of the Clyde Building and the fourth floor of the Engineering Building. The experimental area in the Clyde Building is a hallway with windows looking into student lab areas on either side. The hallway's primary material composition is that of reinforced glass windows, cinder block walls, and vinyl flooring tiles. The experimental area in the Engineering Building took place in the west electrical engineering faculty hallway. It consists of modern building materials, with metal framing, sheetrock covering, and carpeted flooring. Measurements were taken in a grid pattern with 12 cm spacing.

Measurements for the temporal experiment were taken between the hours of 11:30 a.m. and 3:30 p.m., during which time there were students utilizing the study space. Measurements for the spatial experiment were taken between the hours of 9:00 a.m. and 5:00 p.m. over the course of several weeks. Additionally, because the channel sounding measurements were taken in an indoor environment, we assume that the thermal noise for both the main and eavesdropper channels was equal.

4.2. Materials and Methods

The main goal of this paper was to use off-the-shelf radio equipment where possible to ensure realistic results. Thus, each node in the experiment runs Ubuntu 14.04 with a custom kernel developed by Xie [26] and network interface cards (NICs) based on the Qualcomm Atheros AR938X chipset. This design decision is based on using an existing, tested setup for measuring CSI on commercial off-the-shelf hardware to ensure results that are as realistic as possible. The standard 802.11n was employed due to the NICs and custom kernel support; however, extending our results to other WiFi or wireless standards was tied directly to the access of the internal channel sounding measurements taken by the hardware. Each node (a desktop computer running the modified Ubuntu kernel with the Atheros NIC) was deployed on a mobile cart for easy repositioning. The orientation

of the cart was kept the same for all the spatial experiments, preventing measurements immediately adjacent to the walls as evidenced in the 1st and 2nd figures in Section 4.3.2.

Alice is configured as a WiFi access point (AP) and sends out a user datagram protocol (UDP) packet every 30 s for the temporal experiment and every half second for the spatial experiment. For the spatial experiment, every location's secrecy capacity result is a time average of the individual secrecy capacity from 150 CSI measurements. Both Bob and Eve are configured as clients to the AP and upon receiving a packet, the kernel calculates and records the CSI for each antenna pair and every OFDM subcarrier.

Following data acquisition, a brute force optimization was run for each packet to calculate the secrecy capacity across all subcarriers as outlined in Section 3.4. Due to practical issues with off-the-shelf hardware and the environment, not all packets were received at either receive node, thus not triggering a CSI measurement in those situations. To account for this, we assume $\mathbf{0}$ to be the complex channel gain matrix for either Bob or Eve in these situations. This means that for situations when the eavesdropper fails to capture the packet, the secrecy capacity is considered to be simply the capacity of the main channel. In situations where the main channel fails to capture a packet, the secrecy capacity is simply zero because there is no main channel achievable rate to begin with.

4.3. Channel Sounding Results and Discussion

4.3.1. Temporal Experiment

The results of our temporal experiments are shown in Figure 3 for a single instance of a subcarrier, and for the whole experiment in Figure 4. The results in Figure 3 show a basic example where both receiver nodes have non-zero CSI data. The high-SNR asymptote is calculated using (7) to demonstrate the accuracy of the optimization.

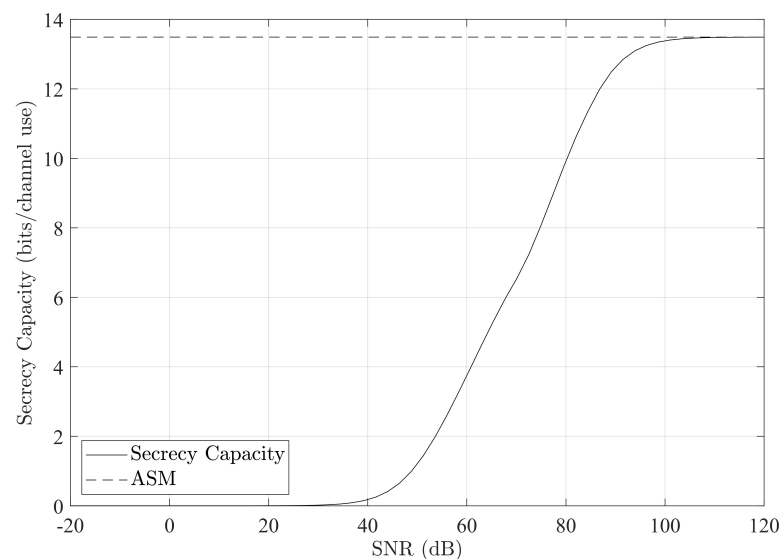


Figure 3. Secrecy capacity for a single subcarrier's set of measurements calculated over a range of transmit powers. ASM is the high-SNR asymptote for secrecy capacity as described in (7).

As can be seen, at high SNR it is possible to achieve significant bit rates comparable to normal usage. At very low SNR, it is much more difficult to get meaningful security. We note here that we assume the noise variance is unity and equal for the main and eavesdropper channels. We have chosen a unity noise variance to stay consistent with [10,11] and for numerical stability; however, as can be seen by inspection of (7), the noise power does not contribute to the secrecy capacity in the high-SNR regime.

The results in Figure 4 denote the total OFDM MIMOME secrecy capacity as a function of both time and SNR. An interesting observation is that during the first 3800 s of the capture, the secrecy capacity in the high-SNR regime is much lower (approximately an average of 500 bits per channel use) than afterward (approximately an average of 1500 bits

per channel use). In the beginning, the reduced secrecy capacity was likely caused by random environmental factors, e.g., a student was studying with a laptop connected to another WiFi AP, which would have influenced the main channel capacity. After the student left, the interference to the main channel presumably diminished. Thus, issues of security are not always a matter of disadvantaging the eavesdropper as they are increasing the advantage of the main channel. During the latter portion of the experiment, Eve was unable to receive approximately a fourth of the packets transmitted. This resulted in the zero-filled CSI condition mentioned previously. Thus, for the portions of the graph with the highest secrecy capacity, the values are equivalent to the Shannon capacity calculation for Bob. The graph shows high achievable secrecy rates for the majority of the experiment. These results suggest that environmental effects greatly influence security, especially in the MIMOME setup, for better or for worse.

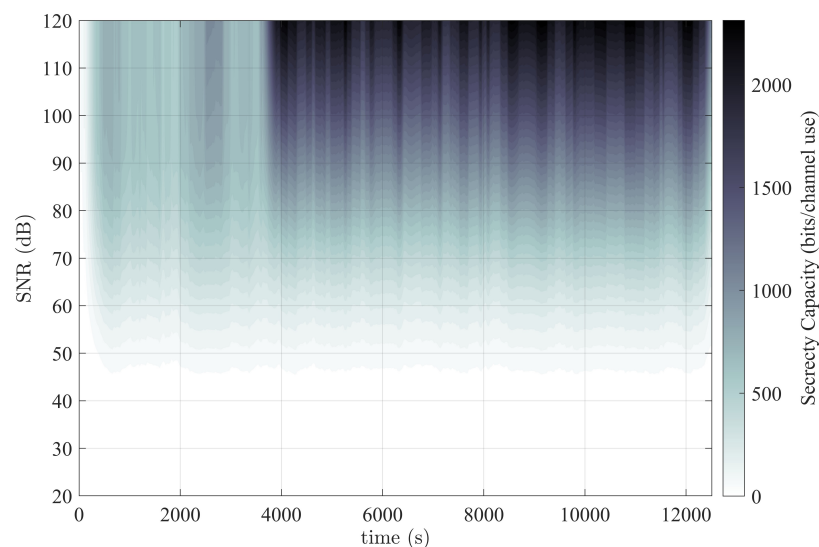


Figure 4. Experimental results over a period of 3.5 h as a function of time and SNR denoting the secrecy capacity in bits/channel use.

4.3.2. Spatial Experiment

The results for the Clyde Building secrecy capacity experiment are shown in Figure 5 and the results for the Engineering Building are shown in Figure 6. On each figure, Bob and Alice are fixed and each data point measures the secrecy capacity for the location as a potential position for Eve. These two experimental environments were chosen primarily for their differences. They both feature an unsecured hallway, which poses a large problem for any security scenario employing a wireless network due to RF signal propagation through walls and structures.

From our analysis of Figures 5 and 6, we note in instances of direct line-of-sight between the eavesdropper and the transmitter there are often substantial drops in the resulting secrecy capacity, a difference of approximately 500 bits per channel use in the most extreme cases. We also note that secrecy capacity tends to increase in proportion to the distance of Eve from the transmitter. The figures show that in instances of near equivalent channels between Bob and Eve, meaningful secrecy capacity can still be achieved (of approximately 100 to 200 bits per channel used in each building where the distances from Alice are roughly equal for Bob and Eve), which we note as a fundamental result of the measurement campaign.

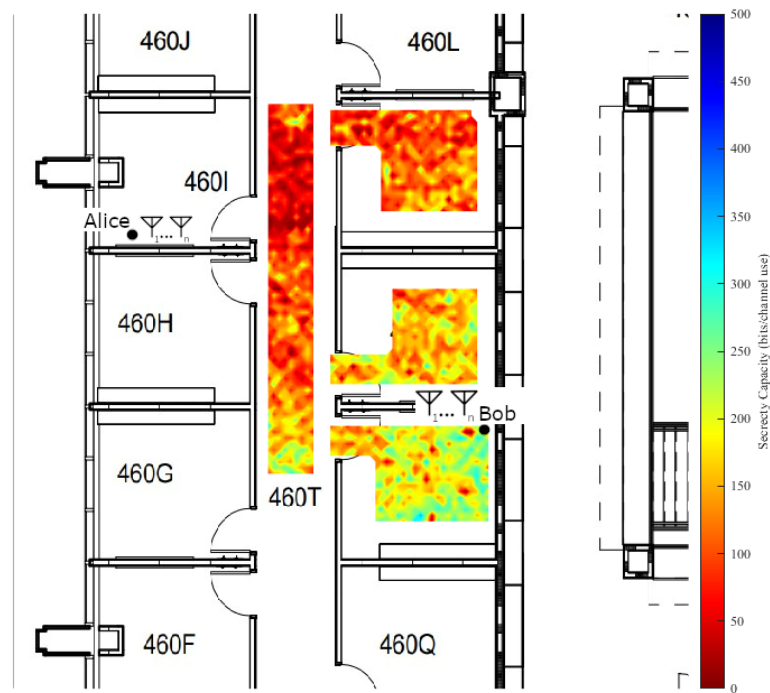


Figure 5. Spatial heatmap of average secrecy capacity in the Engineering Building.

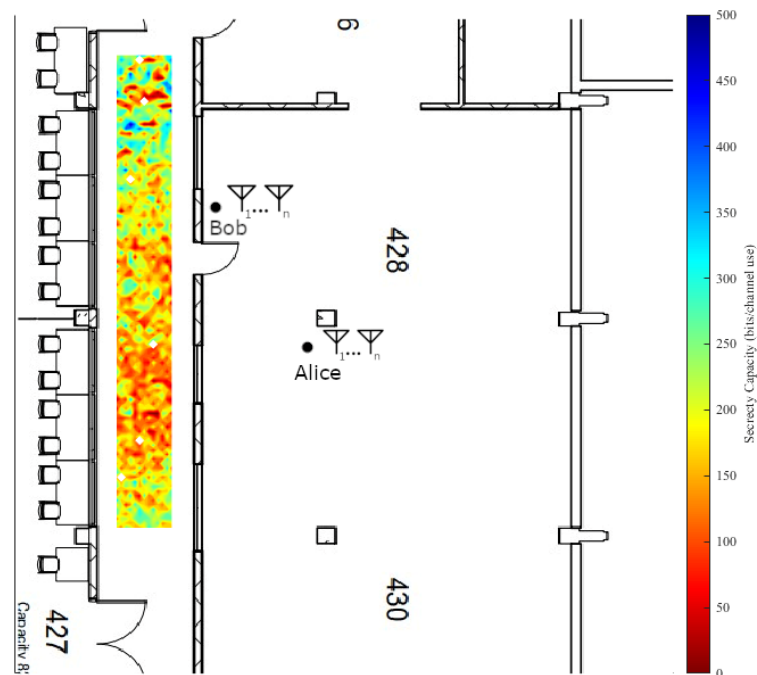


Figure 6. Spatial heatmap of average secrecy capacity in the Clyde Building.

Physical obstacles also play a fundamental role in the indoor scenario as they contribute to non-uniform or rapidly changing channel effects. Examples from the figures include office furniture, walls, doors, pillars, etc. These effects are both to the advantage and the detriment of the intended receiver in the measured environments, but could be placed strategically to increase secrecy capacity. As stated before, these two environments differ in the types of propagation characteristics that they exhibit due to their construction. The Clyde Building was opened in 1974 and the Engineering Building was opened in 2018. They have different material compositions and were built by employing different

construction methods. RF propagation in the WiFi bands is easier in buildings that use sheetrock walling rather than the more durable cinder block walls. Our analysis showed that building construction and materials are important security considerations, as can be noted by comparing the unsecured hallways between the two environments. Both instances have cases where Eve has a presumably superior channel; however, the secrecy capacity is generally higher for those cases in the Engineering Building, likely due to the cinder block construction.

Physical-layer security, and security in general, requires a specific understanding of the scenario, environment, network users and threat models. The variety of ways that malicious activity can be carried out requires security experts to be more conscious of the specifics of attacks. The spatial experiments carried out are an example of the utility that a measurement campaign can have in determining weaknesses.

5. Conclusions

In this paper, CSI was recorded over time and space in several indoor environments using real-world, off-the-shelf WiFi NICs. An experiment was conducted to determine the secrecy capacity for a range of SNR and plotted as a temporal heatmap. Two additional experiments were conducted to determine the secrecy capacity as a function of space, and plotted as a spatial heatmap against the layout of the environments in which the experiments took place. Our results show that environmental changes, such as foot and network traffic, physical obstacles, and relative positions to the transmitter affect the maximum achievable secure rate of communication significantly (an average of 1000 bits per channel use difference between the interference and non-interfered cases of the temporal experiment and by as many as 500 bits per channel use in the spatial experiments due to physical obstacles or relative positions to Alice). It is shown that meaningful and secure rates can theoretically be achieved in real and practical situations using commercially available hardware, as evidenced by the non-zero secrecy capacity in even non-ideal situations.

Author Contributions: Conceptualization, All; methodology, All; software, D.H.; validation, D.H., K.K., T.S. and W.H.; formal analysis, D.H. and W.H.; data curation, D.H., T.S. and K.K.; writing—original draft preparation, D.H. and T.S.; writing—review and editing, All; visualization, D.H., M.R. and W.H.; supervision, W.H., P.L. and M.R.; project administration, W.H.; funding acquisition, W.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially funded by the US National Science Foundation: Grant Award Number #1910812.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Channel sounding measurements and related code available upon email inquiry to the authors.

Acknowledgments: The authors thank A. Khisti for an insightful discussion regarding his work on MIMOME and MISOME secrecy capacity, and for his encouragement to augment the theoretical findings for these models with channel measurements.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
SISO	Single-Input, Single-Output
MIMO	Multi-Input, Multi-Output
MIMOME	Multi-Input, Multi-Output, Multi-Eavesdropper
CSI	Channel State Information
OFDM	Orthogonal Frequency Division Multiplexing

IOT	Internet of Things
V2V	Vehicle to Vehicle
SNR	Signal to Noise Ratio
IEEE	Institute of Electrical and Electronics Engineers
GSVD	Generalized Singular Value Decomposition
KKT	Karush Kuhn Tucker

References

- Shor, P. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [\[CrossRef\]](#)
- Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [\[CrossRef\]](#)
- Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
- Zhou, X.; Song, L.; Zhang, Y. *Physical Layer Security in Wireless Communications*; CRC Press: Boca Raton, FL, USA, 2016.
- Mucchi, L.; Nizzi, F.; Pecorella, T.; Fantacci, R.; Esposito, F. Benefits of Physical Layer Security to Cryptography: Tradeoff and Applications. In Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sochi, Russia, 3–6 June 2019; pp. 1–3. [\[CrossRef\]](#)
- Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [\[CrossRef\]](#)
- Harrison, W.K.; Almeida, J.; Bloch, M.R.; McLaughlin, S.W.; Barros, J. Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security. *IEEE Sign. Process. Mag.* **2013**, *30*, 41–50. [\[CrossRef\]](#)
- Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [\[CrossRef\]](#)
- Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [\[CrossRef\]](#)
- Khisti, A.; Wornell, G.W. Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 5515–5532. [\[CrossRef\]](#)
- Oggier, F.; Hassibi, B. The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 4961–4972. [\[CrossRef\]](#)
- Liu, T.; Shamai, S. A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel. *IEEE Trans. Inf. Theory* **2009**, *55*, 2547–2553. [\[CrossRef\]](#)
- Duong, T.Q.; Zhou, X.S.; Poor, H.V. *Trusted Communications with Physical Layer Security for 5G and Beyond*; The Institution of Engineering and Technology: London, UK, 2017; p. 439.
- Jensen, B.; Clark, B.; Flanary, D.; Norman, K.; Rice, M.; Harrison, W.K. Physical-Layer Security: Does it Work in a Real Environment? In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7. [\[CrossRef\]](#)
- Rice, M.; Clark, B.; Flanary, D.; Jensen, B.; Nelson, N.; Norman, K.; Perrins, E.; Harrison, W.K. Physical-Layer Security for Vehicle-to-Everything Networks: Increasing Security While Maintaining Reliable Communications. *IEEE Veh. Technol. Mag.* **2020**, *15*, 68–76. [\[CrossRef\]](#)
- Li, Z.; Yates, R.; Trappe, W. Secrecy Capacity of Independent Parallel Channels. In *Securing Wireless Communications at the Physical Layer*; Springer: Boston, MA, USA, 2010; pp. 1–18.
- Renna, F.; Laurenti, N.; Poor, H.V. Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1354–1367. [\[CrossRef\]](#)
- Tse, D.; Viswanath, P. *Fundamentals of Wireless Communication*; Cambridge University Press: Cambridge, UK, 2013.
- Brown, T.; DeCarvalho, E.; Kyritsi, P. *Practical Guide to the MIMO Radio Channel: With MATLAB Examples*; Wiley: Hoboken, NJ, USA, 2012.
- Yang, T.; Taghizadeh, O.; Mathar, R. SEE of Full-Duplex Multi-carrier Bidirectional Wiretap Channels with Multiple Eavesdroppers. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6. [\[CrossRef\]](#)
- Goldsmith, A.; Jafar, S.; Jindal, N.; Vishwanath, S. Capacity limits of MIMO channels. *IEEE J. Sel. Areas Commun.* **2003**, *21*, 684–702. [\[CrossRef\]](#)
- Cuan-Cortes, J.V.; Vargas-Rosales, C.; Munoz-Rodriguez, D. MIMO channel capacity using antenna selection and water pouring. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 288. [\[CrossRef\]](#)
- Mukherjee, A.; Ottersten, B.; Tran, L.N. On the Secrecy Capacity of MIMO Wiretap Channels: Convex Reformulation and Efficient Numerical Methods. *IEEE Trans. Commun.* **2021**, *69*, 6865–6878. [\[CrossRef\]](#)
- Mukherjee, A.; Kumar, V.; Jorswieck, E.; Ottersten, B.; Tran, L.N. On the Optimality of the Stationary Solution of Secrecy Rate Maximization for MIMO Wiretap Channel. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 357–361. [\[CrossRef\]](#)

25. Gursoy, M.C. Secure Communication in the Low-SNR Regime. *IEEE Trans. Commun.* **2012**, *60*, 1114–1123. [[CrossRef](#)]
26. Xie, Y.; Li, Z.; Li, M. Precise Power Delay Profiling with Commodity Wi-Fi. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1342–1355. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.