On Secret Key Generation with Massive MIMO Antennas using Time-Frequency-Space Dimensions

Elias Yaacoub
Faculty of Computer Studies, Arab Open University
Beirut, Lebanon
Email: eliasy@ieee.org

***Abstract*—Kerchoff's principle states that the security of encryption should be based on the key. Thus, increasing the encryption key length has been an essential approach in generating unbreakable ciphers. Recently, physical layer security has gained significant research attention. It allows secure communications between a source and destination without the need to resort to key-based encryption techniques. In this paper, secret key generation using massive multiple input multiple output (MIMO) techniques is investigated. The large number of subcarriers used in orthogonal frequency division multiple access (OFDMA) systems is also used to increase the key length. Several scenarios are investigated and corresponding key lengths are calculated. The combination of massive MIMO and OFDMA also allows to simultaneously implement physical layer security techniques while generating large keys for traditional key-based cryptography.**

I. Introduction

In cryptography, the well-known Kerchoff's principle, derived in the nineteenth century, states that the security in a cryptosystem should lie in the key, even if everything else about the system is publicly known. Hence, increasing the encryption key size is of primordial importance, especially with the advancements in processing power of modern computers, which could allow them to break keys that once were thought unbreakable. Quantum cryptography addresses this problem by using the properties of light photons to generate very long cryptographic keys [1].

With the advent of millimeter wave communications, Massive multiple input multiple output (MIMO) antenna deployments are becoming practically feasible [2]. This would allow the placement of a large number of antennas in a relatively small area. These large antenna arrays have their benefits in security applications. In fact, in [3], [4], methods to exchange secret keys with massive MIMO are investigated in the presence of pilot contamination attack (PCA), mostly common in time division duplex (TDD) systems.

They also have their role in physical layer security techniques, where communications are secured without relying on the overhead of traditional application layer encryption techniques. Instead, physical layer security relies on signal processing, channel coding, and other physical layer techniques [5]. However, the role of massive MIMO antennas in generating long secret encryption keys has not been sufficiently investigated in the literature.

In this paper, a frequency division duplex (FDD) system is considered. The presence of massive MIMO antennas, in conjunction with orthogonal frequency division multiple access (OFDMA), allows the generation of large secret keys with lengths comparable to those generated with quantum cryptography. In fact, key generation could benefit from several degrees of freedom in space, time, and frequency in order to generate large secret keys while misleading any potential eavesdropper. In addition, the presence of a large numbers of antenna elements could be used for transmitting the secret key and the encrypted messages to the receiver while simultaneously jamming an eavesdropper. A subset of the antenna elements could be used for each task. This allows combatting PCA and eavesdropping while still being able to transmit data securely. Thus, massive MIMO antenna arrays could be used for joint implementation of key-based cryptography in conjunction with physical layer security.

The rest of this paper is organized as follows. Section II presents the system model. Sections III and IV present the calculations for the scenarios where the antenna elements are used for multiplexing and diversity, respectively. In Section V, numerical results are presented and discussed. Section VI discusses methods to resist to eavesdropping while exchanging the secret keys. In Section VII, conclusions are drawn.

II. System Model

The system model is shown in Fig. 1. It consists of a source sending a message to a destination. Both are equipped with a massive MIMO antenna array. An eavesdropper could be present to attempt to intercept the exchanged secret keys and/or the encrypted messages.

In Fig. 1, the antenna array disposition is selected to be a planar one. Planar arrays allow obtaining directive beams that lead to high antenna gains in a desired direction while leading to low sidelobe levels in undesired directions. The antenna gain is closely related to the directivity of the antenna, which is calculated directly from the array factor [6]. Planar antenna arrays are obtained by placing linear arrays one parallel to the other such that the elements form a planar configuration, as depicted in Fig. 2. It was shown in [6] that the array factor of a planar array is equivalent to the multiplication of the array factors of two linear arrays in orthogonal directions.

This paper discusses secret key generation using planar arrays with a large number of antenna elements. With massive MIMO deployments being considered for future generation wireless networks, along with OFDMA, large secret keys can

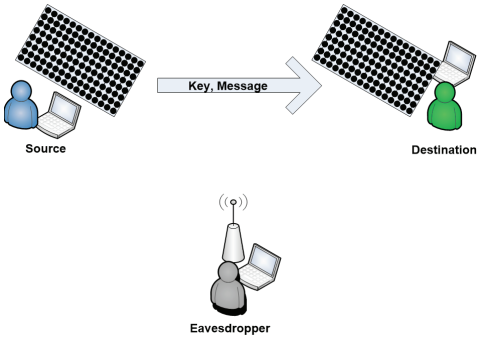

Fig. 1. System model.

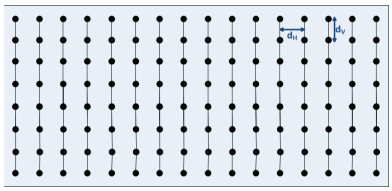

Fig. 2. Planar array.

TABLE I
DEFINITIONS.

Variable	Description
M	Number of antenna elements
F	Number of subcarriers
S_c	Number of symbols per channel use
B_s	Number of bits per symbol
T	Duration of transmission
T_c	Duration of one channel use

be exchanged between sender and receiver. Indeed, OFDMA relies on a large number of orthogonal subcarriers that can transmit data simultaneously benefiting from signal processing using Fast Fourier Transform (FFT) [7]. Large secret keys could be generated using this time-frequency-space combination as shown in the following sections, whether the antenna elements are used for multiplexing or for diversity. The definitions and notations used throughout the paper are shown in Table I.

Using the notations of Table I, the number N_c of channel uses during time T is given by:

$$N_c = \frac{T}{T_c} \tag{1}$$

III. MULTIPLEXING

In the multiplexing case, different bit sequences are transmitted over each (antenna, subcarrier) pair.

A. Best Case Scenario

When all antenna elements in the transmitter array can be differentiated at the receiver by their channel gains, then the MIMO matrix is full rank. Consequently, spatial diversity allows transmitting on all subcarriers from each antenna element while being able to recover the information at the receiver without interference. Hence, the number of bits that can be used in the secret key K is given by:

$$L_K = M \cdot F \cdot N_c \cdot S_c \cdot B_s \tag{2}$$

With each bit taking two possible values (0 or 1), the number of keys forming the search space for an attacker to find the right key is given by:

$$N_K = 2^{L_K} = 2^{M \cdot F \cdot N_c \cdot S_c \cdot B_s} \tag{3}$$

B. Worst Case Scenario

The previous scenario assumed a full rank MIMO matrix. This scenario requires significant feedback overhead to determine the channel state information (CSI) at each antenna element. Furthermore, it might lead to CSI leakage to an eavesdropper that might take advantage of the CSI information.

A simpler scenario consists of using beamforming to direct the main beam of the antenna array at the receiver towards the transmitting array. Then, at the transmitter, only one subcarrier can be used for transmission by each antenna element. Therefore, the number of independent parallel transmission streams would be $\min(M, F)$. In other words:

- When the number of subcarriers is equal to the number of antenna elements ($M = F$), one distinct subcarrier will be used at each antenna element.
- When the number of subcarriers is less than the number of antenna elements ($M > F$), F out of M antenna elements will be used for transmission, with one distinct subcarrier used at each of the F antenna elements.
- When the number of subcarriers is greater than the number of antenna elements ($M < F$), M out of F subcarriers will be used for transmission, with one distinct subcarrier used at each of the M antenna elements. It should be noted that, in this latter case, one can use $\lfloor F/M \rfloor$ subcarriers per antenna element (with $\lfloor \cdot \rfloor$ denoting the floor operation), which would provide longer keys. However, in this paper, we will present numerical examples only for the case of one subcarrier per antenna element.

In this scenario, the number of bits that can be used in the secret key K is given by:

$$L_K = \min(M, F) \cdot N_c \cdot S_c \cdot B_s \tag{4}$$

With each bit taking two possible values, the number of keys forming the search space for an attacker to find the right key is given by:

$$N_K = 2^{L_K} = 2^{\min(M,F) \cdot N_c \cdot S_c \cdot B_s} \tag{5}$$

IV. DIVERSITY

In the diversity case, the antennas and subcarriers are used to repeat the same data transmissions, i.e the same bit sequence is transmitted over a set of active (antenna, subcarrier) pairs. Hence, we have:

$$L_K = N_c \cdot S_c \cdot B_s \tag{6}$$

With each bit taking two possible values, the number of possible keys is given by:

$$N_K = 2^{L_K} = 2^{N_c \cdot S_c \cdot B_s} \tag{7}$$

However, the number of keys in (7) does not use the diversity information insured by transmissions on different (antenna, subcarrier) pairs. Therefore, we use $\delta_{i,j}$ as an indicator variable. It is set to $\delta_{i,j} = 1$ if subcarrier f_j is used for transmission over antenna element m_i, and set to $\delta_{i,j} = 0$ otherwise.

A. Best Case Scenario

When all antenna elements in the array can be differentiated by their channel gains, then the MIMO matrix is full rank. Consequently, spatial diversity allows distinguishing transmissions originating from all (antenna, subcarrier) pairs. There are $2^{M \cdot F}$ such possible combinations. Using this information to increase the key space, the number of keys forming the search space for an attacker to find the right key is given by:

$$N_K = 2^{N_c \cdot S_c \cdot B_s} \cdot 2^{M \cdot F} \tag{8}$$

B. Worst Case Scenario

The previous scenario assumed a full rank MIMO matrix. This scenario requires significant feedback overhead to determine the channel state information (CSI) at each antenna element. Furthermore, it might lead to CSI leakage to an eavesdropper that might take advantage of the CSI information.

A simpler scenario consists of using beamforming to direct the main beam of the antenna array at the receiver towards the transmitting array. Then, at the transmitter, only one subcarrier can be used for transmission by each antenna element. Therefore, the number of independent parallel transmission streams would be $\min(M, F)$. In other words:

- When the number of subcarriers is equal to the number of antenna elements ($M = F$), one distinct subcarrier will be used at each antenna element.
- When the number of subcarriers is less than the number of antenna elements ($M > F$), F out of M antenna elements will be used for transmission, with one distinct subcarrier used at each of the F antenna elements.
- When the number of subcarriers is greater than the number of antenna elements ($M < F$), M out of F subcarriers will be used for transmission, with one distinct subcarrier used at each of the M antenna elements.

In this scenario, the number of possibilities becomes $2^{\min(M,F)}$. In fact, only $\min(M, F)$ (antenna, subcarrier) pairs are allowed to participate in the key generation process. With two possible outcomes for each pair (either participating or not), there are $2^{\min(M,F)}$ possibilities. Hence, the number of keys in the key space becomes:

$$N_K = 2^{N_c \cdot S_c \cdot B_s} \cdot 2^{\min(M,F)} \tag{9}$$

TABLE II
KEY AND KEY SPACE LENGTHS.

Scenario	bits/ symbol	Key length (bits)	Number of keys
Multiplexing - Best Case	6	$11,010,048$	∞
Multiplexing - Worst Case	2	$3,584$	$7.79 \cdot 10^{1078}$
Diversity - Best Case	6	$131,156$	∞
Diversity - Best Case	2	$131,100$	∞
Diversity - Worst Case	6	212	$6.582 \cdot 10^{63}$
Diversity - Worst Case	2	156	$9.1344 \cdot 10^{46}$

TABLE III
TIME NEEDED FOR BRUTE FORCE ATTACK WITH 10^{12} KEY ATTEMPTS PER SECOND.

Scenario	bits/symbol	Time Needed (Years)
Multiplexing - Best Case	6	-
Multiplexing - Worst Case	2	$2.47 \cdot 10^{1059}$
Diversity - Best Case	6	-
Diversity - Best Case	2	-
Diversity - Worst Case	6	$2.0871 \cdot 10^{44}$
Diversity - Worst Case	2	$2.8965 \cdot 10^{27}$

V. NUMERICAL EXAMPLES

In LTE for example, one transmission time interval (TTI) has a duration of 1 ms, consisting of two 0.5 ms slots. Transmission in each slot consists of seven symbols over each subcarrier [8], [9]. Using quadrature phase shift keying (QPSK), then 2 bits/symbol are transmitted. Less bits per symbol can be transmitted, depending on the modulation and coding schemes combination. In this paper, with massive MIMO, considering 2bits/symbol as a worst case scenario is a reasonable assumption. If 64QAM (quadrature amplitude modulation) is used, up to 6 bits/symbol can be transmitted. Assuming $M = 128$ antenna elements and $F = 1024$ subcarriers, the results for the key length in bits and the number of keys in the key space for each of the investigated scenarios are shown in Table II. The duration of a brute force attack to determine the key used in each scenario is shown in Table III. However, an eavesdropper might use side channel information through signal leakage to determine the key instead of using a brute force attack. Techniques to mitigate this scenario are described in the following section.

VI. RESISTANCE TO EAVESDROPPING

The results presented consisted of the key lengths and the number of possible keys that can be generated and used for communication between the source and destination. In this section, we present methods for misleading an eavesdropper listening to the unsecure communication channel and attempting to learn the secret key exchanges between source and destination.

A. Data Permutation

The results presented in the previous sections, particularly for the multiplexing case, did not indicate the order of the

different sequences from the various (antenna, subcarrier) combinations. In fact, even if an eavesdropper detects all the communicated bits successfully, it cannot easily determine the order in which these bits are sorted at the source and destination in order to build the encryption key. Hence, in the best case scenario, there are $(M \cdot F)!$ possible permutations (with ! denoting the factorial operation), whereas in the worst case scenario with one subcarrier per antenna, there are $\min(M, F)!$ possibilities. With $M = 128$ and $F = 1024$, $(M \cdot F)!$ will lead to an infinite number of permutations whereas $\min(M, F)! = 128! = 3.8562 \cdot 10^{215}$ possibilities. Consequently, if the transmitter and receiver have a predefined method for ordering the key data, e.g., using a pseudorandom generator synchronized between source and destination to provide a pseudorandom order for the sequences of the different antennas, this technique can be used independently, or used in conjunction with the other methods described in the next sections to provide increased protection.

B. Beamforming

With a large number of antennas present at the transmitter, beamforming can be performed to place a null in the direction of the eavesdropper, thus eliminating, or significantly reducing its capability to detect the secret key transmission or later on the encrypted messages. In situations where the MIMO channel matrix is full rank and each antenna element is transmitting over all subcarriers, placing a null in the direction of an eavesdropper might not be feasible and thus some signal leakage might reach the eavesdropper. However, in the scenarios of Sections III-B and IV-B, the main beam can be directed towards the legitimate receiver, whereas sidelobes or nulls can be directed towards the eavesdropper thus minimizing the received data at the eavesdropper. Under these scenarios, the receiver can also steer its main beam in the direction of the transmitter, thus maximizing its received signal.

C. Jamming

Part of the antenna elements at the transmitter can be used to transmit a jamming signal in the direction of the eavesdropper. The remaining antenna elements can transmit the secret key information and then the encrypted data messages to the destination, as shown in Fig. 3. A relatively small number of elements can be sufficient to jam the eavesdropper by sinking the leaked signal in jamming noise. Even in a scenario when half of the antenna elements are used, the number of keys in the key space remains sufficiently large. When an eavesdropper is jammed, its ability to detect the useful signal becomes very limited. However, assuming the jammig is performed only during key transmission with half of the antenna elements, the results of key space size and duration of a brute force attack are shown in Table IV.

VII. Conclusions and Future Work

Secret key generation using massive MIMO techniques was investigated. The large number of antenna elements coupled with the large number of subcarriers in OFDMA systems were used to increase the key length. Several scenarios were investigated and corresponding key lengths were calculated. Even in worst-case scenarios, large key lengths were achieved.

The combination of massive MIMO and OFDMA allows for interesting future investigations, e.g. to simultaneously implement physical layer security techniques while generating large keys for traditional key-based cryptography.

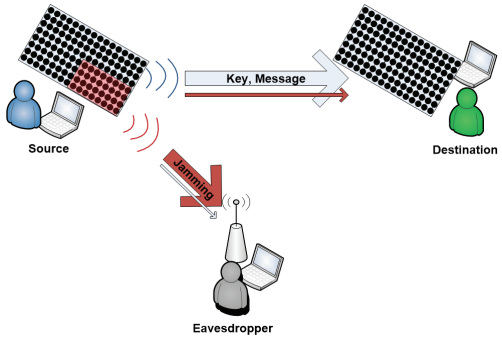

Fig. 3. Key exchange using massive MIMO with a subset of the antennas used for jamming the eavesdropper.

TABLE IV
Key Space Lengths and Brute Force attack Duration for the Diversity - Worst Case Scenario with 64 Antennas.

bits/sym.	Nb. of keys	Time Needed (Yrs)
6	$3.5681 \cdot 10^{44}$	$1.1314 \cdot 10^{25}$
2	$4.9518 \cdot 10^{27}$	$1.5702 \cdot 10^{8}$

References

[1] B.R. Auburn, "Quantum Encryption – A Means to Perfect Security?", SANS Institute, 2003.

[2] Z. Gao, L. Dai, D. Mi, Z. Wang, M. A. Imran, and M. Z. Shakir, "MmWave Massive-MIMO-based Wireless Backhaul for the 5G Ultra-Dense Network", *IEEE Wireless Communications*, vol. 22, no. 5, pp. 13–21, October 2015.

[3] S. Im, H. Jeon, J. Choi, and J. Ha, "Robustness of Secret Key Agreement Protocol with Massive MIMO under Pilot Contamination Attack", *International Conference on ICT Convergence (ICTC)*, pp. 1053–1058, Jeju, South Korea, October 2013.

[4] S. Im, J. Choi, and J. Ha, "Secret Key Agreement for Massive MIMO Systems with Two-Way Training under Pilot Contamination Attack", *IEEE Globecom Workshops*, pp. 1–6, San Diego, CA USA, December 2015.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication", *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, December 2015.

[6] C. A. Balanis, *"Antenna Theory, Analysis and Design"*, 4th edition, John Wiley and Sons, 2016.

[7] T. Keller and L. Hanzo, "Adaptive Multicarrier Modulation: A Convenient Framework for Time-Frequency Processing in Wireless Communications", *Proceedings of the IEEE*, vol. 88, no.5, pp. 611–640, 2000.

[8] 3rd Generation Partnership Project (3GPP), "3GPP TS 36.213 3GPP TSG RAN Evolved Universal Terrestrial Radio Access (E-UTRA) Physical layer procedures, version 13.1.1, Release 13," March 2016.

[9] 3rd Generation Partnership Project (3GPP), "3GPP TS 36.211 3GPP TSG RAN Evolved Universal Terrestrial Radio Access (E-UTRA) Physical Channels and Modulation, version 13.1.0, Release 13," March 2016.