Eavesdropping in Massive MIMO: New Vulnerabilities and Countermeasures

Chia-Yi Yeh, *Member, IEEE,* and Edward W. Knightly, *Fellow, IEEE*

***Abstract*—Massive multiple-input and multiple-output (massive MIMO) has the potential to thwart passive eavesdropping as the signals transmitted by large antenna arrays become highly focused. Indeed, the impact of passive eavesdropping has been shown to be negligible when the base station (BS) antenna size approaches infinity for Rayleigh channels. In this paper, we experimentally explore eavesdropping in massive MIMO incorporating real-world factors including a limited BS antenna array size, potential correlation in over-the-air channels, and adaptation of modulating and coding schemes (MCS) over a discrete and finite set. Using a 96-antenna ArgosV2 BS, we first explore scaling the array size and identify eavesdropper (Eve) advantages due to channel correlation. We next identify the ”MCS saturation regime” as a vulnerability even with high SNR due to limited MCS levels, and thereby demonstrating the need for power control as a counter-strategy, especially considering Eve's advantages in the over-the-air channels. We further demonstrate Eve's gain in optimizing her position, not only via being nomadic and searching for the most favorable position, but also via exploiting predictable line-of-sight (LoS) positional vulnerabilities. Specifically, we demonstrate Eve's advantage by simply sharing the elevation angle with Bob in the LoS scenario. Finally, we examine how Eve's advantage due to channel correlation scales with more eavesdropping antennas.**

I. INTRODUCTION

Wireless links are vulnerable to passive eavesdropping since wireless signals are broadcast into the air, and any device receiving a strong enough signal can overhear the message intended for the target user (Bob). When the transmitter (Alice) has multiple antennas, she can use beamforming to concentrate the signals to Bob attempting to avoid being intercepted by the eavesdropper (Eve). Indeed, in theory, massive MIMO systems [2], in which the base station (BS) is equipped with many antennas are immune to passive eavesdropping. Specifically, prior works have shown that as the BS antenna size approaches infinity, the secrecy rate approaches the channel capacity and therefore the threat of passive eavesdropping is negligible [3], [4], [5].

While the promising physical layer security improvement in massive MIMO has been widely accepted, most works are based on channel models and numerical results. In fact, the most common channel model in the massive MIMO security discussion is still the Rayleigh fading channels [6], [7], [8], [9]. However, practical channels are spatially correlated [10] and over-the-air (OTA) measurements are critical to reveal potential threats in practical systems.

In this paper, we present the extended *experimental* evaluation of eavesdropping in massive MIMO systems based on our earlier work [1], which employs the Rice Argos massive MIMO platform [11] with 96 antennas. In particular, we reevaluate the most fundamental single user scenario and examine whether the theoretical security enhancement applies to a practical system. To date, our work [1] remains the only work that provides experimental validation for massive MIMO passive attacks.

In contrast to prior theoretical studies [12], [13], [14], we necessarily incorporate several key factors for a practical system. First, OTA channel measurements can differ from idealized MIMO models with independent channels [15], [16], [17]. Second, the antenna array size in real massive MIMO systems is limited due to cost and space constraints. Lastly, practical systems are constrained by a discrete and limited set of modulation and coding schemes (MCS), instead of wiretap codes [18] designed for achieving information-theoretical secrecy. The combination of these factors offers us a unique perspective on the massive MIMO physical layer security when packets are sent with selected MCS via limited number of antennas over the air.

In our experiments, we first explore the role of scaling Alice's array size by sub-sampling measurements from the actual 96 element array. As our goal is to examine how the over-the-air channels differ from an idealized channel model without correlation, we also perform Monte Carlo simulations using independent Rayleigh channels as a baseline. First, we find that in the moderate-antenna regime, e.g., below 8 antennas, Bob's and Eve's measured signal-to-noise ratio (SNR) scales as predicted by the baseline channel models. However, in the many-antenna regime, Eve obtains a modest advantage over the idealized model due to channel correlation, with the gap between the measured channels and Rayleigh channels increasing with the number of BS antennas. We find that despite the rich multi-path environment of the indoor channels at 2.4 GHz, a significant line-of-sight (LoS) component nonetheless yields correlation that corresponds to a 4 dB advantage for Eve when the BS array size is 96.

Second, we examine how Eve's SNR advantage translates to higher packet delivery ratio at Eve and affects the BS's ability of using power adaptation as a countermeasure. We find that higher transmit power does not always lead to better secrecy.

A preliminary version of this paper was presented at IEEE CNS 2018 [1]. This extended version demonstrates a new security vulnerability of elevation angle sharing in the LoS scenario, adds mathematical formulation for Bob and Eve's SNR scaling, examine the threat of a multi-antenna Eve, and updates related works. (Corresponding author: Chia-Yi Yeh.)

C-Y. Yeh and E. W. Knightly are with the Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005 USA (e-mail: chia-yi.yeh@rice.edu; knightly@rice.edu).

We thank the editor and anonymous reviewers for their insightful feedback, which greatly improved the manuscript.

Instead, in the high SNR regime, *MCS saturation* occurs, where the channel from Alice to Bob is sufficiently strong that the BS could increase its MCS, yet it cannot because no higher order MCS is available. Once the MCS saturates, increasing transmit power only risks increasing Eve's SNR and reducing secrecy. Therefore, we consider that the BS employs power control in order to thwart Eve. We show that a larger BS antenna array offers better secrecy for a larger set of transmit powers. However, this advantage reduces in the real-world channels. When examining the secure packet deliver ratio (s-PDR), which we define as the fraction of packets decoded by Bob but not Eve, we find that 16 antennas yields s-PDR of only approximately 0.8 in the measured channels instead of almost 0.9 in Rayleigh channels under optimal power allocation. In addition, with 96 antennas at the BS, although an s-PDR of 0.95 can be reached in the measured channels, power control becomes much more stringent (spanning ∼10dB) compared to Rayleigh channels (spanning ∼20dB).

Next, we consider two passive eavesdropping positional strategies and their effectiveness in the over-the-air channels. We first consider a nomadic Eve who attempts to find a better location with increased channel gain to overhear the Alice-Bob transmission. We begin with Eve on the same radius as Bob, and find that having a low angular spread to Bob (Eve closer to Bob), does not help Eve, mainly because the separation distance in the measurements is beyond the order of the wavelength. Nonetheless, the positions on the radius have as much as 12 dB spread from worst to best, and if Eve checks all points, she will gain significantly. Likewise, Eve may position herself as close to Alice as possible to improve her channel gain.

The second positional strategy we consider is an Eve that exploits the knowledge of channel correlation in the LoS scenario to position herself at predictable favorable locations. While prior works demonstrated security vulnerability when Bob and Eve share the same path [19], [20], we further show Eve's advantage by sharing only the elevation angle with Bob when the BS is equipped with a rectangular antenna array. Specifically, we demonstrate that the theoretical LoS channel correlation for Bob and Eve located at the same elevation angle remains fixed with increasing rows of antennas at the BS, suggesting that adding new rows of antennas at the BS inevitably boosts Eve's SNR as the BS beamforms to Bob. The shared elevation angle vulnerability is then validated using Rician channel simulations, as well as channel measurements in both indoor and outdoor LoS scenario, revealing an increasing threat with stronger LoS.

Finally, we examine how Eve's advantage scales when she has multiple antennas. By applying maximum ratio combining, Eve's SNR is the summation of SNR of at each element, and her SNR advantage accumulates with increasing antennas. We show with over-the-air channel measurements in both indoor LoS and outdoor LoS scenarios that Eve's SNR advantage due to channel correlation persists with increasing Eve array size.

In summary, we find the physical layer security provided by the large antenna array alone does not prevent passive eavesdropping given practical factors and shrewd eavesdropping strategies. Therefore, additional security mechanisms such as sending orthogonal artificial noise to interfere with Eve [21], [22], [14], or applying optimum linear precoding given Eve's channel is known [23], [24] should be considered for massive MIMO systems.

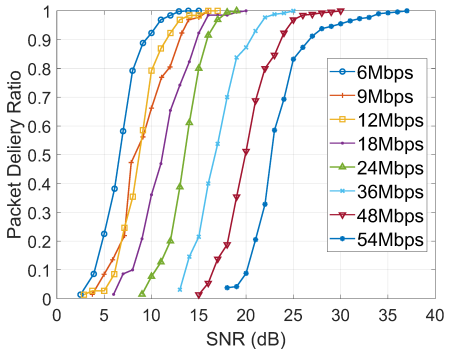


Fig. 1. PDR as a function of SNR. Adapted from [27].

II. System Model

A. Massive MIMO Downlink Transmission

We consider a multi-antenna BS (Alice) transmits to a single-antenna user Bob. The BS has M antennas, which can be as large as hundreds to explore the Massive MIMO regime.

In a downlink transmission, the BS first obtains Bob's CSI. In a time-division duplex (TDD) massive MIMO system for example, the BS estimates the uplink channel from Bob to the M antennas at the BS using the uplink pilot transmitted by Bob, and the downlink channel is obtained assuming channel reciprocity to avoid the high overhead caused by the downlink training scaling with M [2]. Specifically, the BS compares the received uplink pilot signals with the known pilot sequence and obtain a uplink channel coefficient for each of the M antennas, and the M channel coefficient constitutes the uplink channel vector $\boldsymbol{g}_{ul} \in \mathbb{C}^{M\times 1}$. The downlink channel vector to Bob $\boldsymbol{g}_b \in \mathbb{C}^{1\times M}$, assuming channel reciprocity, is the transpose of the uplink channel vector $\boldsymbol{g}_b = \boldsymbol{g}_{ul}^T$. We can further express the downlink channel as $\boldsymbol{g}_b = \sqrt{\beta_b}\boldsymbol{h}_b$, where $\sqrt{\beta_b}$ and $\boldsymbol{h} \in \mathbb{C}^{1\times M}$ represent the large-scale and the small-scale fading respectively, and the small-scale fading is normalized such that $\mathbf{E}\left[\|\boldsymbol{h}\|^2\right] = M$.

Based on the acquired CSI, the BS estimates Bob's SNR and selects the MCS level suitable for the transmission. Similar to the SNR-based rate adaptation strategies proposed in [25], [26], [27], the BS maximizes data rate by selecting the highest MCS that can support packet delivery ratio (PDR) of γ close to one. If Bob's SNR is too low for any MCS level, the lowest MCS is selected. Notice that PDR is a pre-defined function of the measured SNR. Although the SNR-PDR relationship is hardware dependent, the achievable MCS increases with SNR and has a sigmoidal transition period in which PDR rapidly increases. Fig. 1, adapted from [27], illustrates the general trend of the SNR-PDR relationship, and is used in our analysis.

With the selected MCS, the BS then transmits the packet using conjugate beamforming to maximize the receive signal strength at Bob. That is, the beamforming weights $\boldsymbol{w}$ =

The final version of record is available at http://dx.doi.org/10.1109/TWC.2021.3074941

$\frac{\sqrt{\beta_b}\boldsymbol{h}_b^H}{\left\|\sqrt{\beta_b}\boldsymbol{h}_b\right\|}$, where the superscript H denotes Hermitian transpose.

B. Threat Model

We consider a passive eavesdropper (Eve) in range of the BS, trying to intercept the downlink signals from the BS to Bob. To avoid being discovered, Eve passively monitors the channel without transmitting. In the following, we first focus on the effect of the propagation channels and isolate the beamforming gain due to scaling BS antenna size by investigating the case of symmetric passive eavesdropping, in which Eve has the same capability as Bob in terms of pathloss, antenna size, and decoding ability. We later extend the discussion to asymmetric Eve that has a different pathloss than Bob (§VII) or multiple antennas (§IX).

C. Secure Transmission in Practical System

The downlink transmission is secure if Eve is ignorant of the messages Alice sends to Bob. Since Eve can decode some of the packets, transmitting the confidential messages directly risks leakage to Eve. Therefore, we consider Alice to adopt an additional layer of secure coding across the messages before transmitting. Specifically, when the receiver fails to decode a packet, we consider it as a packet erasure. Hence, the packet delivery ratio (PDR) gap between Bob and Eve, $\text{PDR}_b - \text{PDR}_e$, represents the normalized secrecy rate, which can be realized by secure coding approaches on the messages before transmitting [28], [29].

Since high PDR at Bob and low PDR at Eve is desirable, BS's best strategy is to choose the highest supportable MCS for the predicted Bob's SNR as it forces Eve to have higher SNR to decode the signals for Bob. This strategy, fortunately, aligns with Alice and Bob's incentive to maximize throughput. Therefore, in the following, we examine the massive MIMO downlink secrecy as the BS chooses the highest MCS which can achieve PDR of a threshold γ close to 1.

III. Factors Affecting Passive Eavesdropping

In this section, we investigate the factors that affect passive eavesdropping, focusing on Bob and Eve's SNR. In the following, we first model the massive MIMO downlink transmission. We then study how Bob and Eve's SNR scales with each factor. Note that the exact scaling depends on the real propagation channels and will be studied in the later sections. Here we study a baseline case, independent Rayleigh channels, to gain the intuition on the scaling behavior.

A. Modeling Massive MIMO Downlink Transmission

In the massive MIMO downlink transmission, the received signal at Bob and Eve can be modeled as y_b and y_e respectively:

$$\begin{aligned} y_b &= \sqrt{p}\sqrt{\beta_b}\boldsymbol{h}_b\boldsymbol{w}s + n_b \\ y_e &= \sqrt{p}\sqrt{\beta_e}\boldsymbol{h}_e\boldsymbol{w}s + n_e, \end{aligned} \tag{1}$$

where $s \in \mathbb{C}$ denotes the transmit signal for Bob, and $\boldsymbol{w} \in \mathbb{C}^{M\times 1}$ is the beamforming weights for Bob and $\|\boldsymbol{w}\|^2 = 1$. Channels from the BS's M antennas to Bob and Eve are represented by large-scale fading β and small-scale fading $\boldsymbol{h} \in \mathbb{C}^{1\times M}$, $\mathbf{E}\left[\|\boldsymbol{h}\|^2\right] = M$. p is the BS transmit power. n_b and n_e are additive Gaussian noise $N(0, \sigma^2)$ at Bob and Eve.

The BS transmits using conjugate beamforming $\boldsymbol{w} = \frac{\boldsymbol{h}_b^H}{\|\boldsymbol{h}_b\|}$ to maximize the receive signal strength at the single user Bob. Therefore, the SNR at Bob and Eve are

$$\begin{aligned} \text{SNR}_{Bob} &= \frac{p\beta_b}{\sigma^2}\|\boldsymbol{h}_b\|^2 \\ \text{SNR}_{Eve} &= \frac{p\beta_e}{\sigma^2}\frac{\left|\boldsymbol{h}_e\boldsymbol{h}_b^H\right|^2}{\|\boldsymbol{h}_b\|^2}. \end{aligned} \tag{2}$$

Therefore, the SNR difference in dB between Bob and Eve is:

$$\text{SNR}_{Bob}^{dB} - \text{SNR}_{Eve}^{dB} = 10\log\frac{\beta_b}{\beta_e} - 10\log\frac{\left|\boldsymbol{h}_e\boldsymbol{h}_b^H\right|^2}{\|\boldsymbol{h}_b\|^4}. \tag{3}$$

We make two observations from Eq. (3). First, the BS transmission power and noise power are cancelled in the SNR difference. Therefore, the SNR difference between Bob and Eve in dB only depends on Bob and Eve's channels, not BS transmission power or noise power. Second, the SNR difference between Bob and Eve is the combination of channel gain difference and beamforming gain difference. Therefore, the two factors can be investigated separately by investigating the symmetric passive eavesdropping case, where Bob and Eve have the same channel gain.

B. Baseline: Independent Rayleigh Fading Channels

To gain insight into the scaling behavior, we study independent Rayleigh fading channels as a baseline, in which the channel coefficient is modeled as Gaussian process. That is, the channel coefficient follows standard complex normal distribution, where both the real and imaginary part of the channel coefficient are i.i.d. Gaussian random variables with mean 0 and variance $\frac{1}{2}$.

1) Bob's and Eve's SNR Distribution: We can derive Bob's and Eve's SNR distribution based on the independent Rayleigh channel. Applying independent Rayleigh channel to Equation (2), we find that Bob's SNR is the summation of $2M$ i.i.d. Gaussian random variable, and therefore follows **Erlang distribution** with shape M and scale $\frac{p\beta_b}{\sigma^2}$. The average of Bob's SNR is $M\frac{p\beta_b}{\sigma^2}$. That is, Bob's average SNR increases proportionally not only to the BS transmit power and Bob's channel gain, but also to the number of BS antennas M.

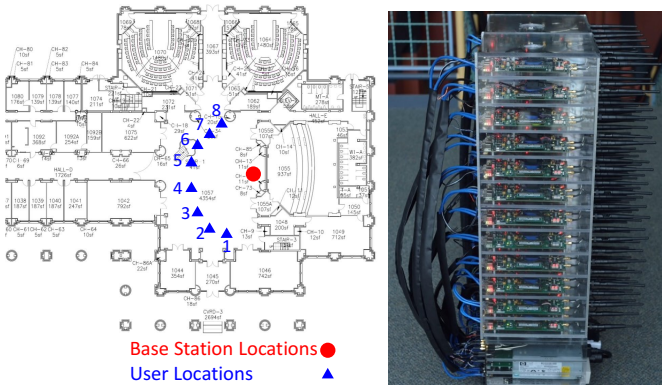
In comparison, Eve's SNR does not grow as the number of BS antennas M increases. From Eq. (2), we observe that Eve's SNR depends on her channel vector's projection on the direction of Bob's channel vector. Since the direction of Bob's channel vector distributes uniformly in independent Rayleigh fading, the projection is equivalent to projecting Eve's channel vector on any coordinate. Therefore, Eve's SNR is the summation of two squared Gaussian random variables, and therefore follows **exponential distribution** with rate $\frac{\sigma^2}{p\beta_e}$, making Eve's average SNR $\frac{p\beta_e}{\sigma^2}$. We observe that Eve's average SNR only

increases with higher transmit power and higher channel gain, but not increasing number of BS antennas.

2) SNR Difference Between Bob and Eve: From the above analysis, we see that Bob's SNR increases proportionally to the number of BS antennas M, while Eve's SNR remains the same in independent Rayleigh fading channels. As a result, the SNR difference between Bob and Eve also increases as the number of BS antennas M increases. However, we do not have a close form distribution for SNR difference between Bob and Eve.

IV. Methodology

In this section, we describe the Rice massive MIMO platform and channel measurement dataset we use to experimentally evaluate passive eavesdropping in a practical massive MIMO system. We describe post-processing methods to compute SNR and PDR at Bob and Eve and introduce a Monte Carlo simulation method to study Rayleigh channels as : two security



(a) Measurement topology (b) Argos BS

Fig. 2. Topology of the indoor channel measurement and the Argos BS

The channel measurement dataset we use is from [30]. The channel measurement are taken using the ArgosV2 BS (Fig. 2b) [11] with 96 antennas and 8 single-antenna WARP boards [31] in Duncan hall at Rice University in 2.4 GHz band with 20 MHz bandwidth. The 8 WARP boards are placed at the same distance from the ArgosV2 BS, all with a direct path to the ArgosV2 BS, as shown in Fig. 2a. The distance from the BS to each WARP boards is $\sim$ 13 meters, and the spacing between adjacent WARP boards is $\sim$ 3 meters. The 8 WARP boards are clients that can serve as Bob or Eve. The 96 antennas of the ArgosV2 BS are placed 8 in a row with total 12 rows on a plane, with spacing of 6.25 cm, which is half-wavelength of 2.4 GHz.

In each channel measurement, the 8 WARP boards send uplink pilots in the 52 subcarriers in a time-division manner, and ArgosV2 BS estimates the channels from the users to the BS. The reversed channels can be obtained assuming channel reciprocity. Therefore, a $96 \times 8 \times 52$ channel matrix is obtained in each measurement, capturing the channels from the 96 BS antennas to the 8 WARP boards across the 52 subcarriers. The channel measurements are taken every 2 ms for total 30 seconds, resulting total 15,000 snapshots. Since there is no device or environment mobility, CSI remains relatively static over the 30 seconds. Therefore, we treat the 15,000 measurement epochs as one channel state realization, and only use adjacent measurements for normalization.

B. CSI Processing and SNR Calculation

1) Subsampling: Now that we obtain a 96x8 channel measurement from the dataset, we describe how we extract different channel realizations from this channel matrix.

First, we can obtain channel realizations for different Bob-Eve Pairs. Since each of the 8 WARP boards can be viewed as Bob or Eve, there are total $8 \times 7 = 56$ different Bob-Eve combinations. Also, to explore different transmit array sizes at the BS, we subsample the 96 antennas. To preserve the physical structure of the array, we only subsample adjacent antenna elements to form linear arrays below 8 elements or rectangular array with 8 elements in a row.

2) SNR Calculation Using Measured CSI: Once the CSI measurements are subsampled, we obtain the channel vectors for Bob and Eve, for different numbers of BS antennas. With Bob and Eve's channel, the SNR at Bob and Eve can be calculated using Eq. (2).

C. MCS Selection and Packet Delivery Based on SNR-PDR Relationship

We assume the SNR-PDR relationship is known to the BS and the one used in our analysis is shown in Fig. 1, which is from [27]. Based on the predicted Bob's SNR, the BS selects the highest MCS which achieves PDR of γ, which is set to be 0.9 in our analysis. When Bob's SNR is so low that even the lowest MCS cannot be supported, the lowest MCS is selected. Once the MCS is chosen, the success of the transmission depends on the corresponding PDR via Bob and Eve's SNR. By tracing the delivery of each packet, we calculate the PDR at Bob and Eve.

D. Baseline: Independent Rayleigh Fading Channels

We use the widely-adopted independent Rayleigh channels as a baseline. While the analysis in §III-B provides Bob and Eve's SNR scaling behavior, to study the SNR difference between Bob and Eve, as well as Bob and Eve's PDR, we use Monte Carlo simulation with 100,000 instances for the independent Rayleigh fading channel, following the same procedure as above with randomly generated Rayleigh channels rather than the over-the-air channels.

E. Metrics for Evaluating Secure Transmission in Practical Systems

1) Secure Packet Delivery Ratio (s-PDR): As discussed in Sec. II-C, high PDR at Bob and low PDR at Eve is desirable

The final version of record is available at http://dx.doi.org/10.1109/TWC.2021.3074941

when considering passive eavesdropping in practical systems. Therefore, we define secure PDR (s-PDR) as

$$\text{s-PDR} = \frac{\text{Number of packets decoded by Bob but not Eve}}{\text{Total number of packets}}$$

When s-PDR is low, either Bob cannot decode packets, or both Bob and Eve can successfully decode the packet, which implies the transmission is either unsuccessful or insecure. In comparison, when the s-PDR is close to 1, Bob can decode most packets while Eve can hardly decode any, indicating a high achievable secure rate between Alice and Bob.

2) SNR Difference Between Bob and Eve: From the sigmoid behavior of the PDR with varying SNR, we know that no matter which MCS is chosen, the transmission can be secure once the difference between Bob's and Eve's SNR is large enough. In addition, from the analysis in §III, we learn that SNR difference is independent of the BS transmit power, making it a general metric for evaluating eavesdropping resilience of the system. Note that the conventional metric of secrecy capacity can be approximated as SNR difference with a scaling factor in the large SNR regime. Therefore, the scaling of SNR difference also represents the scaling of secrecy capacity in the large SNR regime.

V. Scaling BS Antenna Resources

Passive eavesdropping is affected by both BS array size and BS transmit power. To explore the factors separately, in this section, we explore the effect of scaling BS antennas by fixing the BS transmit power. We examine the SNR and PDR at Bob and Eve, as well as the selected MCS for the transmissions. In the following, we first examine the Rayleigh channels as a baseline and then study the measured channels.

A. Baseline: Independent Rayleigh Fading Channels

We first examine how Bob and Eve's SNR changes as the BS's antenna size increases for the baseline independent Rayleigh channels. This analysis quantifies Bob's SNR advantage over Eve under idealized channels as the BS devotes an increasing number of antenna resources to providing a beamforming gain to Bob, which will not benefit Eve. As described in §IV, we vary BS's array size from 1 to 96 and use Monte Carlo simulation with 100,000 instances.

Fig. 3a shows the median of Bob and Eve's SNR in dB vs. the number of transmit antennas for a fixed total transmit power. The 90% confidence interval is shown with the 5 and 95 percentiles. We choose the BS transmit power so that the median of Bob's SNR falls at 10 dB when the BS uses a single antenna, allowing Bob's SNR to fall in the MCS operating range, spanning from approximately 10 dB to 30 dB.

Fig. 3a indicates that Bob's SNR increases by approximately 3 dB when the size of BS antenna array doubles, which is a direct result of beamforming. In comparison, Eve's SNR remains the same no matter how many antennas are at the BS. This trend confirms the SNR analysis in §III-B. As a result, as the BS's antenna resources are increased, it can select a higher MCS to take advantage of Bob's SNR gain. However, since Eve's SNR remains the same, she may not be able to decode the higher order MCS.

As for the SNR variation, Bob's SNR variation decreases as the BS increases the array size thanks to the law of large numbers. The smaller SNR variation implies that Bob is less likely to encounters deep-fade events, and therefore avoids being forced to use lower MCS for transmissions. In contrast, Eve's SNR variation does not change with the scaling antenna resources as Bob and Eve's channels are independent. The consistent large SNR variation makes Eve encounter deep-fade events, but also gives Eve chances to have better channel conditions for eavesdropping.

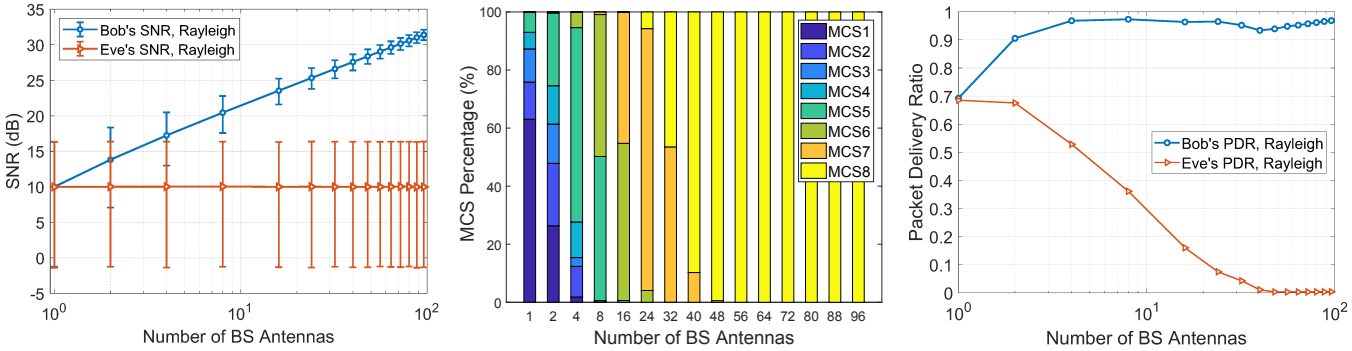
Next, we examine how the higher and more converged Bob's SNR affects the MCS selection. Fig. 3b shows the selected MCS when the BS chooses the highest MCS achieving over 90% PDR for transmission, as described in §IV-C. We observe that when the BS has only a small number of antennas, the beamforming gain is reduced and the BS must use a reduced MCS. As the BS antenna size increases, the BS can increase MCS. When the BS has more than 48 antennas, Bob's SNR is so large that the BS always chooses the highest MCS. We refer to this point as "MCS saturation" since while the channel can support a higher MCS, none is supported by the standard. Also, since the variation of Bob's SNR decreases as the number of antennas increases, the variety of the selected MCS decreases. For example, the BS chooses from MCS-1 to MCS-5 when it has 2 antennas, but only from MCS-6 to MCS-8 when it has 24 antennas.

Now we know the trend of Bob and Eve's SNR, as well as the selected MCS as the BS increases its antennas. Here we examine the resulting PDR at Bob and Eve, as shown in Fig. 3c. When the BS has only a single antenna, Bob and Eve have the same PDR, since they are at the same distance from the BS. We also observe that because of the large SNR variation, Bob sometimes fails to decode packets with even the lowest MCS, and therefore results in PDR lower than 90% (which would otherwise trigger MCS adaptation). As the BS has more antennas, Bob's PDR increases and remains above 90% given the higher SNR due to beamforming gains. In comparison, Eve's PDR drops with increasing BS antennas since Eve fails to decode packets transmitted with higher MCS. Eve's PDR drops below 10% at 24 antennas, and eventually drops to 0% when the BS has more than 40 antennas.

As the number of antennas and beamforming gains to Bob increase, the BS can utilize higher MCS due to Bob's increasing SNR; Eve eventually fails to decode the high-MCS packets, as her SNR (of Bob's packets) does not increase. Thus, with independent Rayleigh channels, a massive MIMO network becomes highly resistant to a single antenna passive eavesdropper when the BS has enough antennas, 24 in this same-radius eavesdropping scenario.

B. Measured Channels

Here, we apply the same methodology as above to over-the-air channels. As described in §IV, the following results are based on channel measurements from a 96-antenna BS to 8 same-radius users across 52 subcarriers. Specifically, Bob and Eve can locate at any 2 of the 8 locations, and the 96 antennas are subsampled to emulate different sizes



(a) Bob's and Eve's SNR (b) MCS proportion (c) Bob's and Eve's packet delivery ratio

Fig. 3. Independent Rayleigh channel

of antenna array. Therefore, the results include all Bob-Eve location combinations, all sub-array configurations, and 52 subcarriers.

Fig. 4a shows Bob and Eve's SNR with 5, 50, and 95 percentiles. Similar to Rayleigh channels, Bob's SNR increases by approximately 3 dB when the number of BS antennas doubles, with only a slight difference that the variation of Bob's SNR in the measurements is larger than that in the Rayleigh channels. However, in contrast to the Rayleigh case, Eve's SNR based on the measured channels does not remain the same when the BS increases its antennas. Instead, Eve's SNR starts to increase when the BS has more than 8 antennas. When the BS has 96 antennas, the 50 percentile of Eve's SNR has increased from 10 dB to 14 dB.

Both the larger variation of Bob's SNR and the increase of Eve's SNR are due to the LoS component of the channel. Since the LoS component causes correlation among the channels from the BS's antennas to Bob, it is more likely that Bob's channels experience good or bad channel conditions together, leading to more extreme SNR values and larger SNR variation. The LoS component also causes correlation between Bob's channel and Eve's channel (details in §VIII). As a result, Eve also receives part of the beamforming gain as the BS beamforms to Bob.

Next, we explore how the larger variation of Bob's SNR and the increase of Eve's SNR affect MCS and the PDR at Bob and Eve. We expect both factors to have a negative impact on resisting passive eavesdropping. Namely, the SNR at Bob can be particularly low in some cases due to the larger variation. As a result, the BS may be forced to choose a lower MCS, making decoding easier at Eve. The increase of Eve's SNR, albeit modest, also enhances Eve's probability of decoding Bob's packets. Therefore, indoor channels with a LoS component can be expected to be less resilient to passive-eavesdropping than in independent Rayleigh channels.

Fig. 4b shows the MCS selected for Bob's transmissions as a function of the number of transmit antennas. Similar to Rayleigh fading channels, the measurement data indicates that packets are transmitted with higher MCS as the BS has more antennas as a result of increasing Bob's SNR. However, when comparing the MCS chosen in measured channels (Fig. 4b) to Rayleigh channels (Fig. 3b), packets tend to be transmitted with more widely varying MCS in the measured channels as a reslut of Bob's larger SNR variation. For example, when the BS has 24 antennas, packets are transmitted with MCS 6, 7, and 8, in both measured and Rayleigh channels. However, in Rayleigh channels only few packets are transmitted with MCS-6 and MCS-8 (4% and 6%), whereas in measured channels, a larger portion of packets are transmitted with MCS-6 and MCS-8 (12% and 22%). Thus, larger portion of packets transmitted with lower MCS in the measured channel, indicating that more packets are vulnerable to passive eavesdropping.

Fig. 4c shows Bob and Eve's PDR in the measured channels and we can observe the negative impact of the LoS component. While the trends of Bob and Eve's PDR are similar to the case of Rayleigh channels, Eve's PDR decreases with a slower rate for measured channels. Furthermore, Eve's PDR does not drop to zero even when the BS has as many as 96 antennas; instead, Eve's PDR hovers around 7%. The slower drop of Eve's PDR is due to a higher percentage of lower-MCS packets and a higher SNR at Eve, making Eve's PDR above 0% even moving towards the many antenna regime.

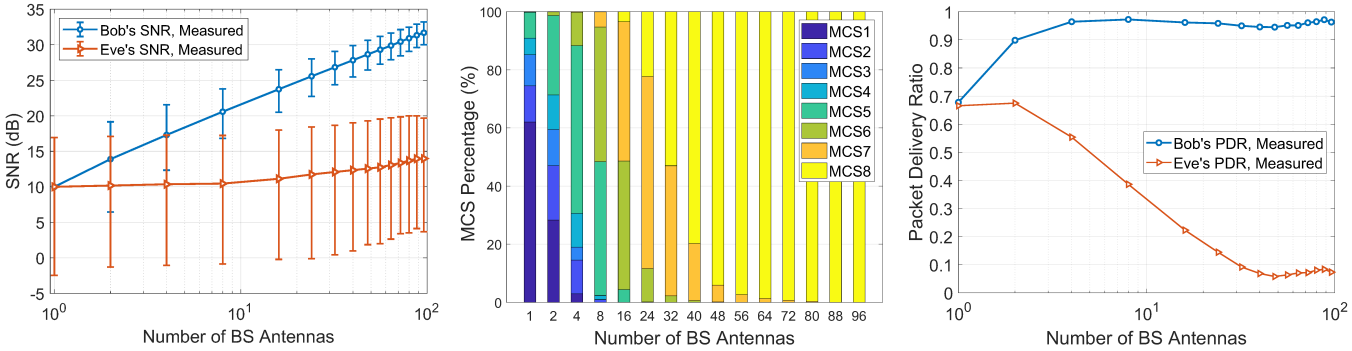
In summary, the over-the-air experiments indicate that the real system is less resistant to passive eavesdropping compared to Rayleigh channels. As a result, more antennas are needed so that Eve's PDR is suppressed below a target threshold in actual transmissions.

C. Scaling Beyond 100 Antennas

Although we only have channel measurements up to 96 antennas, we explore array size larger than 96 using linear regression in this subsection.

Fig. 5 shows the prediction of the median of SNR difference between Bob and Eve up to 200 antennas. The prediction is made using the last 6 data points, which corresponds to BS antennas range from 56 to 96. Note that this prediction can be too optimistic since it does not model the slower growth of SNR difference in the larger antenna regime for the over-the-air channels.

In Fig. 5, we observe that when the array size increases by 10 times, the SNR difference increases by 10.17 dB for Rayleigh channels, but only 4.45 dB for the measured channels, which is less than half of the increment in the Rayleigh channels. Under this prediction, 200 antennas in the



(a) Bob's and Eve's SNR (b) MCS proportion (c) Bob's and Eve's packet delivery ratio

Fig. 4. Indoor LOS

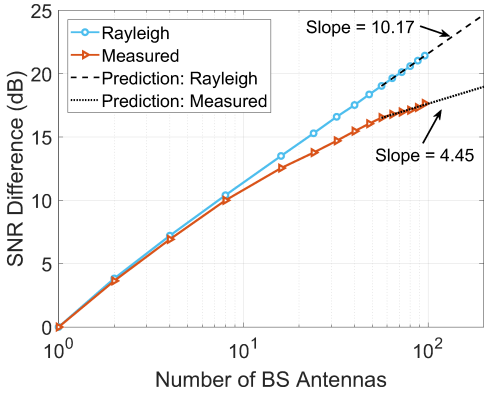


Fig. 5. SNR difference prediction.

measured channels will only have similar security level of 60 antennas in the Rayleigh channels. And about 700 antennas are required to match the performance of 96 antennas in the independent Rayleigh channel.

The result indicates that increasing security level in practical systems is a challenging problem. Since the growth of SNR difference slows down in the large-antenna regime for the over-the-air channels, the SNR difference growth predicted by Rayleigh channels will require another order of magnitude of antennas to achieve in the practical systems. Moreover, since the results of Rayleigh channels and the over-the-air channels diverge with scaling antennas, using Rayleigh channels to model the real channels becomes less applicable in the larger antenna regime.

VI. Transmit Power Adaptation as a Counter Measure

Thus far, we considered the BS to transmit with a fixed total power. Here, we consider the BS to use transmit power adaptation as a counter-strategy to enhance their resilience to Eve. We first define a normalized transmit power for fair comparison across different BS antenna sizes. We then analyze s-PDR for both Rayleigh and over-the-air channels under varying transmit power.

A. Receiver-Normalized Transmit Power

To compare BS transmit power across different BS array sizes and add context to the transmit power, we define the *receiver-normalized BS transmit power* in two steps. First, we normalize transmit power to the number of antennas such that the BS transmits to Bob with power $\frac{p}{M}$ when it has M antennas. This normalization allows Bob's SNR to remain consistent across varying BS antenna sizes. Second, we define the BS transmit power based on the median receive SNR at Bob. In this way, the BS's transmit power is translated to the SNR range Bob falls into.

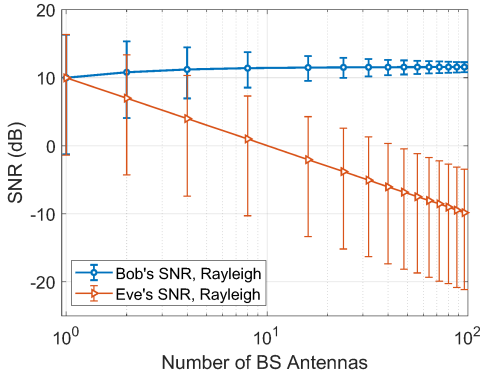


Fig. 6. Bob and Eve SNR in independent Rayleigh channels, BS transmit power is normalized to antenna size.

Fig. 6 shows an example of receiver-normalized BS transmit power of 10 dB for independent Rayleigh channels. In this example, all settings are the same as in §V except that the BS decreases its transmit power proportionally to its number of antennas. According to our definition, Bob's median SNR under single BS antenna (10 dB in Fig. 6) defines the receiver-normalized BS transmit power. Since the BS decreases its transmit power proportionally to its number of antennas, the beamforming gain is canceled out. Therefore, Bob's SNR remains approximately 10 dB as the BS array size increases. While Bob's SNR remains consistent, the variation reduces as array size increases due to the law of large numbers. In comparison, Eve's SNR is suppressed by the reduced transmit power as the BS has more antennas. In Fig. 6, Eve's SNR decreases by 3 dB when the array size doubles, with the same

variation. Using the receiver-normalized BS transmit power, we next compare passive eavesdropping across different BS array sizes.

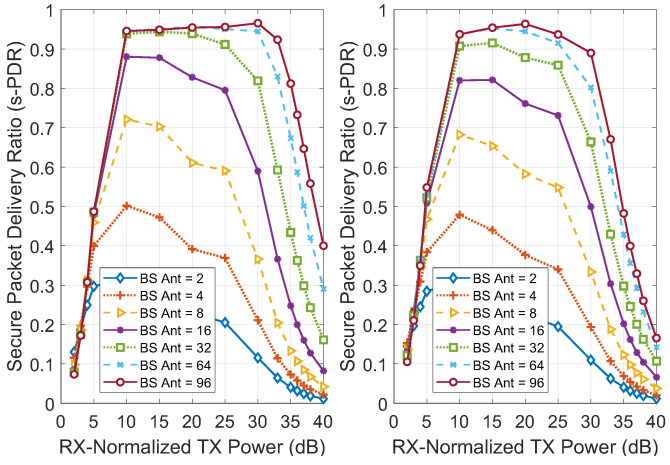
B. Independent Rayleigh Channels

Here, we study the power adaptation strategy that makes transmissions more resilient to Eve for Rayleigh channels. In particular, we use s-PDR, the percentage of packets received by Bob but not Eve, as the security performance metric. We vary the number of BS antennas from 2 to 96, and the receiver-normalized BS transmit power from 2 dB to 40 dB, which indicates Bob's SNR ranges. The results are based on Monte Carlo simulation with 100,000 instances.

Fig. 7a depicts s-PDR vs. receiver-normalized transmit power (defined in §VI-A), with a family of curves for different array sizes. For each array size, s-PDR first increases, and then decreases with increasing transmit power. To understand this behavior, we first consider the transmit power being so low that neither Bob nor Eve can receive the packets, making s-PDR close to zero. As the BS increases its transmit power, Bob starts to receive packets with the lowest MCS while Eve can barely decode packets for Bob due to a generally lower SNR when the BS has multiple antennas. Therefore, the s-PDR first grows as the BS increases its transmit power.

As the BS transmit power keep increasing, Eve's SNR also grows. If Bob's SNR is not significantly larger than Eve's, as occurs when the BS has few antennas, it is likely that some packets for Bob can also be decoded by Eve, and the s-PDR is hence reduced. In contrast, if Bob's SNR is significantly larger than Eve's, i.e., when the BS has many antennas, Eve cannot decode packets for Bob even with her improved SNR. Therefore, the s-PDR remains high, and we can observe a plateau when the BS has a large antenna array.

However, the s-PDR eventually decreases when the BS transmits with sufficiently high power, even when the BS has many antennas. In this case, Bob and Eve's SNR are both high enough to decode packets modulated with the highest MCS, resulting insecure transmissions. We term this regime *MCS saturation* as having increased MCS levels would defer this effect to higher powers. Nonetheless, MCS saturation cannot be avoided when MCS levels are limited. This result aligns with the theoretical prior works on finite alphabet inputs [32], [33], which suggested that higher power does not always result in better secrecy.



(a) Independent Rayleigh Channels (b) Measured Channels

Fig. 7. Secure packet delivery ratio (s-PDR) varies as BS increases its transmit power.

Fig. 7a also reveals the impact of scaling the array size by analyzing the family of curves: First, the highest achievable s-PDR grows as the number of antennas increases. For example, the highest achievable s-PDR is only 0.3 when the BS has 2 antennas, vs. 0.5 for 4 antennas, and 0.95 when the BS has more than 32 antennas. That is, more packets are decoded by Bob but not Eve as the BS has more antennas and chooses transmit power properly.

Second, when the BS has more antennas, the s-PDR remains high for a larger transmit power region. If we consider s-PDR above 0.9 as the desirable secrecy level, the normalized transmit power region which offers the desirable secrecy is 10-33 dB when the BS has 96 antennas. In comparison, the power region shrinks to 10-25 dB when the BS reduces its array size to 32. A larger antenna array at the BS increases the SNR difference between Bob and Eve, and thus relieves the precision of transmit power allocation.

In summary, a larger antenna array at the BS increases the achievable s-PDR, and also broadens the transmit power range that results in the desirable secrecy level. However, a large antenna array does not guarantee a high secrecy level, as the BS needs to be careful not to enter the MCS saturation regime, transmitting with power sufficiently high such that both Eve and Bob can decode the packets modulated with the highest MCS.

C. Measured Channels

Here, we explore the same factors using measurements between a 96-antenna BS and 8 same-radius single-antenna user in the indoor LoS setting as described in §IV-A. Fig. 7b shows that, similar to Rayleigh channels, s-PDR first increases, and then decreases, as the BS increases its transmit power, and the highest achievable s-PDR grows when the BS has more antennas.

However, the Argos system measurements requires more antennas at the BS to achieve the same s-PDR compared to Rayleigh channels. In Rayleigh channels, 16 antennas at the BS can achieve almost 0.9 s-PDR, whereas only 0.82 s-PDR is achieved in the measured channels. To achieve an s-PDR of 0.9, it requires only ∼20 antennas for Rayleigh channels, but ∼30 antennas for the measured channels. Furthermore, s-PDR drops at lower BS transmit power than for Rayleigh channels. For instance, when the BS has 96 antennas, s-PDR remains above 0.9 when receiver-normalized BS transmit power ranges from 10 to 33 dB for Rayleigh channels, but the s-PDR drops below 0.9 after 29 dB for the measured channels.

The lower secrecy level in the measured channels is a result of a smaller SNR difference between Bob and Eve in the measured channels. A large SNR difference between Bob and Eve makes Eve harder to decode packets for Bob, provided

The final version of record is available at http://dx.doi.org/10.1109/TWC.2021.3074941

that the system is not in the MCS saturation regime. In the measured channels, Eve also receives a small beamforming gain when the BS beamforms to Bob with a large antenna array. This advantage makes Eve attain the SNR required to decode packets for Bob at a lower BS transmit power.

In summary, achieving the same desirable secrecy level in the measured channels requires more transmit antennas compared to the Rayleigh channels. Also, the BS has to allocate its transmit power more carefully since s-PDR is more sensitive to BS transmit power in the measured channels than Rayleigh channels.

VII. Nomadic Eve

In the previous sections, we examine the overall passive eavesdropping behavior regardless of Bob and Eve's positions. However, there might exist some eavesdropping positions that are especially vulnerable to passive eavesdropping and will be exploited by a nomadic Eve. In addition, we consider a same-radius Eve so far, but a mobile Eve can move closer to the BS to increase her signal strength. Therefore, in this section, we first investigate the variation results from different Bob-Eve positions, in search of potential threatening location patterns. After that, we discuss the threat as Eve move closer to the BS.

A. Bob and Eve's Relative Position

Bob and Eve's position affects the resistance to passive eavesdropping. Therefore, our goal is to examine whether any position pattern exists for passive eavesdropping in the indoor environment with a LoS component. To this end, we examine the SNR difference of all Bob-Eve pairs from our 8 same-radius user dataset.

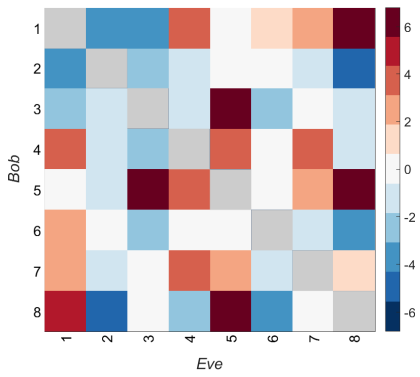


Fig. 8. Bob and Eve SNR difference of all Bob-Eve pairs when BS has 96 antennas. Values are relative to the average case.

Fig. 8 shows the median of SNR difference between Bob and Eve of each Bob-Eve pair when the BS has 96 antennas. The value shown in Fig. 8 is relative to the median of SNR difference of all pairs in dB. Color red, blue, and white represents a larger, lower, and similar SNR difference compared to the average case. As Bob and Eve cannot be at the same location, the diagonal elements are represented with gray and are excluded from the discussion.

Since (Bob,Eve)=(a,b) and (Bob,Eve)=(b,a) is simply swapping positions, we can observe Fig. 8 is nearly symmetric along the diagonal. Note that (Bob,Eve)=(a,b) and (Bob,Eve)=(b,a) do not result in exactly the same SNR difference due to variation of channel gain.

One natural expectation is that Eve receives higher SNR, or a smaller SNR difference, when Eve is closer to Bob. However, we do not observe this phenomenon. Fig. 8 depicts cases with a smaller angular separation between Bob and Eve as closer to the diagonal line. If being closer to Bob aided Eve, we would see mostly blue near the diagonal, followed by white and then red when moving further from the diagonal. However, we observe cases which are especially resistant to eavesdropping (red) even when Bob and Eve are adjacent nodes, namely (Bob,Eve) = {(4,5), (5,4)}. Similarly, we also observe cases which are especially vulnerable to eavesdropping (blue) when Bob and Eve have a large angular separation, such as (Bob,Eve) = {(2,8), (8,2)}.

To further explore the role of angular separation, we calculate the correlation between the two variables, SNR difference and angular separation, and find the correlation to be only 0.101. As a result, the transmissions do not become more secure when Bob and Eve have a large angular separation. Indeed, while correlation can exist when the distance between Bob and Eve is on the order of the wavelength (12 cm for of 2.4 GHz), the distance between Bob and Eve is at least $\sim$2 meters in our measured topology.

B. Eve Closer to the BS

So far, we consider Bob and Eve have similar pathloss. However, a nomadic and shrewd Eve would like to move closer to the BS for higher channel gain and a favorable SNR spread from Bob. In this case, achieving secure transmissions becomes even challenging.

The results of the measured channels are based on same-radius Bob and Eve, and therefore does not represent the near-far scenario. However, we still expect the near-far scenario performs no better than the Rayleigh channels considering the channel correlation in the real world.

When Eve has a higher channel gain than Bob, the SNR difference shown in Fig. 5 is reduced by the channel gain difference between Eve and Bob. As a result, the antenna size that achieves secure transmissions previously in the same-radius Eve case fails to prevent eavesdropping as Eve moves close to the BS. To achieve secure transmissions considering a close Eve, much larger antenna array, possibly a few more hundreds of antennas, is required at the BS. For example, if Eve's channel gain is 5 dB higher than Bob's, $\sim$70 and $\sim$350 antennas are required for Rayleigh channels and measured channels respectively. Similarly, the same issue happens when Bob locates far from the BS.

In summary, although a few dozens of antennas may be enough to prevent a same-radius Eve, the pathloss gap between Bob and Eve brings the required array size to another magnitude. In theory, keep increasing the BS antenna size solve the problem of passive eavesdropping. However, the order of antennas required may not be practical considering a close-Eve or far-Bob scenario and correlated channels in the real world.

VIII. 2-D Arrays and Elevation Angle Vulnerability

In the past sections, we examine the indoor LoS measured channels and find that the over-the-air channels do not offer as favorable security guarantees as predicted by the Rayleigh fading channels. In this section, we further explore the root of the secrecy degradation. Specifically, we show that with a 2D array at the BS, Eve gains an advantage by simply staying at the same elevation angle as Bob in the LoS scenario.

A. Eve's Advantages in LoS Scenario

1) Elevation Angle Sharing Vulnerability: In contrast to independent Rayleigh channels which result in asymptotic uncorrelated Bob and Eve channels with increasing number of antennas, prior works have shown that Bob's channel and Eve's channel remain correlated when they share a same path, leading to a degraded secrecy capacity [19], [20].

While prior works demonstrated Eve's advantage when she shares the same paths with Bob, we argue that Eve gains an advantage even when only the elevation angle is shared considering a 2D antenna array at the BS. To illustrate the idea, we consider a BS with a rectangular antenna array with n_R rows and n_C columns. The LoS channel for a given azimuth angle ϕ and elevation angle θ for the i-th BS antenna element at row n_r and column n_c is [34]

$$a_i\left(\phi,\theta\right) = e^{j2\pi\frac{d}{\lambda}|\sin\theta|\left[(n_c-1)\cos\phi+\frac{(n_r-1)}{\tan\theta}\right]}, \tag{4}$$

where d is the antenna spacing and λ is the wavelength of the carrier frequency. The LoS channel vector $\boldsymbol{a}\in\mathbb{C}^{1\times n_R n_C}$ for azimuth angle ϕ and elevation angle θ can be expressed using the channel vector of the first row of the antenna array $\boldsymbol{a}_R\in\mathbb{C}^{1\times n_C}$ as

$$\boldsymbol{a}\left(\phi,\theta\right) = \left[\boldsymbol{a}_R, e^{j\alpha}\boldsymbol{a}_R,\ldots,e^{j(n_R-1)\alpha}\boldsymbol{a}_R\right],$$

where $\alpha = 2\pi\frac{d}{\lambda}\frac{|\sin\theta|}{\tan\theta}$.

When Bob and Eve share the same elevation angle θ but locate at different azimuth angle ϕ_B and ϕ_E, we can express Bob and Eve's LoS channels using their LoS channel vectors of the first row of the antenna array, $\boldsymbol{a}_{R_B}$ and $\boldsymbol{a}_{R_E}$:

$$\boldsymbol{a}_B\left(\phi_B,\theta\right) = \left[\boldsymbol{a}_{R_B}, e^{j\alpha}\boldsymbol{a}_{R_B},\ldots,e^{j(n_R-1)\alpha}\boldsymbol{a}_{R_B}\right],$$
$$\boldsymbol{a}_E\left(\phi_E,\theta\right) = \left[\boldsymbol{a}_{R_E}, e^{j\alpha}\boldsymbol{a}_{R_E},\ldots,e^{j(n_R-1)\alpha}\boldsymbol{a}_{R_E}\right].$$

The correlation between the two LoS channel vectors can then be computed as

$$\begin{aligned}\frac{\left|\boldsymbol{a}_B\boldsymbol{a}_E^H\right|}{\|\boldsymbol{a}_B\|\,\|\boldsymbol{a}_E\|} &= \frac{\left|n_R\boldsymbol{a}_{R_B}\boldsymbol{a}_{R_E}^H\right|}{\sqrt{n_R\|\boldsymbol{a}_{R_B}\|^2}\sqrt{n_R\|\boldsymbol{a}_{R_E}\|^2}}\\ &= \frac{\left|\boldsymbol{a}_{R_B}\boldsymbol{a}_{R_E}^H\right|}{\|\boldsymbol{a}_{R_B}\|\,\|\boldsymbol{a}_{R_E}\|}\end{aligned} \tag{5}$$

From Equation (5), we observe that unlike the well-known zero-approaching user channel correlation in Rayleigh channels with increasing antennas [4], the LoS channel correlation between Bob and Eve at the same elevation angle remains fixed as the BS adds new rows of antennas.

In a strong LoS scenario, the LoS channel correlation largely represents the actual channel correlation, suggesting that Eve's SNR increases with Bob's SNR when they share the same elevation angle. In other words, when Bob and Eve shares the same elevation angle in a strong LoS scenario, increasing rows of antennas inevitably boosts Eve's SNR when the BS beamforms to Bob. Eve's advantage form the LoS channel correlation diminishes with weaker LoS component. In the extreme case of no LoS component, the channels fall back to Rayleigh fading channels discussed in previous sections.

While we demonstrate Eve's advantage when sharing only the elevation angle in the LoS scenario, this advantage, however, is not at the same level as the advantage Eve would get if she shares the exactly same LoS angle as Bob. As shown in [19], the average secrecy capacity does not increase with BS antenna size when Bob and Eve locate at the same angle. In contrast, when Bob and Eve share the same elevation angle, the secrecy capacity still scales with the BS antenna size, only slower due to the persistent channel correlation.

2) Azimuth Angle Sharing Not As Effective: After showing Eve's advantage when she shares the same elevation angle with Bob, one would expect a similar eavesdropping advantage when Bob and Eve share the same azimuth angle. However, we show in the following that the two statements are not equivalent and sharing azimuth angle is not an effective eavesdropping strategy in a LoS scenario.

Consider a scenario in which Bob and Eve share the same azimuth angle ϕ but are located at different elevation angles θ_B and θ_E. Using a similarly approach as before, their LoS channels can be expressed using Bob and Eve's LoS channel vector of the first column of the antenna array, $\boldsymbol{a}_{C_B}\in\mathbb{C}^{1\times n_R}$ and $\boldsymbol{a}_{C_E}\in\mathbb{C}^{1\times n_R}$:

$$\boldsymbol{a}_B\left(\phi,\theta_B\right) = \left[\boldsymbol{a}_{C_B}, e^{j\eta_B}\boldsymbol{a}_{C_B},\ldots,e^{j(n_C-1)\eta_B}\boldsymbol{a}_{C_B}\right],$$
$$\boldsymbol{a}_E\left(\phi,\theta_E\right) = \left[\boldsymbol{a}_{C_E}, e^{j\eta_E}\boldsymbol{a}_{C_E},\ldots,e^{j(n_C-1)\eta_E}\boldsymbol{a}_{E_E}\right],$$

where $\eta_B = 2\pi\frac{d}{\lambda}|\sin\theta_B|\cos\phi$ and $\eta_E = 2\pi\frac{d}{\lambda}|\sin\theta_E|\cos\phi$. Therefore, the correlation between the two LoS channels become

$$\begin{aligned}\frac{\left|\boldsymbol{a}_B\boldsymbol{a}_E^H\right|}{\|\boldsymbol{a}_B\|\,\|\boldsymbol{a}_E\|} &= \frac{\left|\rho\boldsymbol{a}_{C_B}\boldsymbol{a}_{C_E}^H\right|}{\sqrt{n_C\|\boldsymbol{a}_{C_B}\|^2}\sqrt{n_C\|\boldsymbol{a}_{C_E}\|^2}}\\ &= \frac{|\rho|}{n_C}\frac{\left|\boldsymbol{a}_{C_B}\boldsymbol{a}_{C_E}^H\right|}{\|\boldsymbol{a}_{C_B}\|\,\|\boldsymbol{a}_{C_E}\|},\end{aligned} \tag{6}$$

where $\rho = 1+e^{j(\eta_B-\eta_E)}+\ldots+e^{j(\eta_B-\eta_E)(n_C-1)}$. Since $|\rho|$ does not scale with n_C, the scaling factor $\frac{|\rho|}{n_C}$ approaches to 0 as number of columns n_C increases. That is, the LoS channel correlation between Bob and Eve decreases with increasing columns of antennas when Bob and Eve share the same azimuth angle, implying no eavesdropping advantage when Eve chooses to stay at the same azimuth angle as Bob.

While sharing the elevation angle and sharing the azimuth angle seem to be similar at the first sight, they actually represent different eavesdropping strategies. We can easily see the difference of the two strategies when visualize a specific azimuth angle or elevation angle. The locations with the same

elevation angle forms a cone shape, whereas the locations with the same azimuth angle forms a plane. Once we realize that sharing the azimuth angle is a strategy different from sharing the elevation angle, it is not surprising that sharing the azimuth angle does not result in the same eavesdropping advantage when sharing the elevation angle.

B. Simulation Validation of Elevation Angle Sharing

From the above LoS channel analysis, Eve is expected to obtain an eavesdropping advantage by simply staying at the same elevation angle as Bob in the LoS scenario. In this subsection, we further simulate the elevation angle sharing vulnerability using Rician fading channels, which capture a LoS path along with other scattered paths. Specifically, we demonstrate the scaling of Bob and Eve's SNR with increasing BS antennas in the LoS scenario. In addition, the simulation is based on parameters matching the massive MIMO measurements introduce in Section IV-A for a better comparison later.

1) LoS Eavesdropping Simulation with Rician Model: Rician fading channel models a scenario in which a LoS component is present as well as other scattered paths, making it suitable for examining the elevation angle sharing vulnerability in the LoS scenario. The parameter K in Rician fading captures the ratio between the power in the LoS path and the power in the other scattered paths. Specifically, $K = \frac{\nu^2}{2\xi^2}$, where ν^2 is the power in the LoS path and $2\xi^2$ is the power in the scattered paths. Since $\mathbf{E}\left[\|\boldsymbol{h}\|^2\right] = M$, the LoS power $\nu^2 = \frac{K}{1+K}$ and the scattered paths power $2\xi^2 = \frac{1}{1+K}$.

Monte Carlo simulation is used to explore Bob SNR and Eve SNR ranges as the size of BS antenna scales. Rician fading depends on the antenna array geometry and receiver locations. In the simulation, the antenna arrangement matches with the experiment, which is 8 antennas in a row, and new rows are added when the antenna size is larger than 8. Also, the antenna spacing is half-wavelength. Bob and Eve locations are set to be on the same height as the BS (elevation angle = 90°). Bob and Eve's azimuth angles falls within 30° to 150°, also reflecting the measurement scenario. In the over-the-air experiment, Bob and Eve always have an angular separation. Therefore, in the simulation, Eve is set to locate at least 10° apart from Bob. Bob and Eve locations are uniformly chosen in the area described above. In the simulation, K, the power ratio between the LoS path and other scattered paths, is set to an arbitrary number of 5, representing a scenario in which the LoS power is 5 times stronger than other scattered paths.

2) SNR Scaling under Shared Elevation Angle: Fig. 9 shows Bob's SNR and Eve's SNR when the BS employs a fixed total transmit power. As before, the figure shows the median SNR as well as 5 and 95 percentiles to demonstrate 90% of the SNR range.

We first observe that Bob's SNR scales with the BS antenna size, as in Rayleigh fading channels (Fig. 3a). However, Bob's SNR variation is smaller than in Rayleigh fading channels. Indeed, Bob's SNR variation comes from the multipath components. When the power of the multipath components decreases, the channel from the BS to Bob becomes more deterministic, resulting a less varying SNR. Furthermore, we

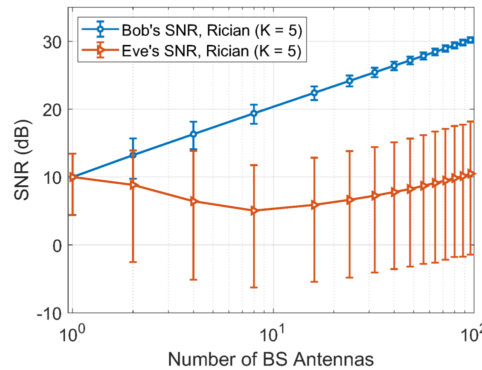


Fig. 9. Bob's and Eve's SNR in Rician fading channels with $K = 5$.

can mathematically show that the Bob's SNR follows the noncentral chi-squared distribution. Therefore, Bob's variance in the presence of a LoS path is scaled by a factor of $\frac{2K+1}{(K+1)^2}$ compared to Bob's SNR variance in Rayleigh channels, revealing a decreasing Bob SNR variance with increasing K. In summary, we observe that the existence of the LoS path does not degrade Bob's SNR. Instead, the LoS path can be interpreted as beneficial to eavesdropping resistance because the decreased multipath randomness prevents deep fade situation that can benefit Eve.

Next, we examine Eve's SNR in the presence of a LoS component. We observe that Eve's SNR scaling can be divided into two regions by antenna size equals to 8. When the BS antenna size is below 8, Eve's SNR decreases with increasing antenna. In contrast, Eve's SNR increases with the BS array size beyond antenna size of 8. Recall that in the simulation the BS array has 8 elements in a row. When BS antenna size is below 8, the antenna array is a horizontal linear array whose azimuth radiation pattern directivity increases with increasing number of antennas considering the LoS component. Therefore, for Eve who has at least 10° of azimuth angular resolution in the simulation, Eve's SNR decreases with increasing BS array size.

However, when more antennas are added to the BS for more rows, the directivity in the elevation angle increases but the azimuth directivity remains the same. For Bob and Eve locate at a same elevation angle, adding more antennas in new rows does not impair Eve's SNR. Instead, in the process of focusing the beam at Bob's elevation angle, Eve, despite being only at side lobes, also gain power simply be being at the same elevation angle as Bob. Here, we observe that Eve does not have to be at the exact same angle as Bob to gain an advantage in eavesdropping. Instead, Eve can also benefit by sharing only the elevation angle with Bob, as suggested by our analysis in the previous subsection.

C. Rician vs. Measurement

After examining the Rician fading channels, now we apply the insights we learn from the Rician model to the indoor LoS measurement results (Fig. 4a).

First, we observe that Bob's SNR in the indoor LoS scenario has the same scaling as the Rician channel prediction, despite

having a larger variation. Interestingly, the larger variation of Bob's SNR in the measurement is also related to the LoS component. Specifically, the LoS power can be varying, for example, across frequencies, in the real world. As a result, Bob's channels experience good or bad channel conditions together, leading to more extreme SNR values and larger variation in SNR. However, Rician fading channels assume a fixed LoS power, and therefore results in a smaller Bob SNR variation compared to the measured channels.

Next, we observe that Eve's SNR has a same turning point at antenna size of 8 in the measured channels as in the Rician channels. This reflects that Eve also benefits from the increasing BS antenna size by being at the same elevation angle as Bob when LoS component exists.

However, Eve's SNR in the measured channels does not decrease when antenna size is below 8, as predicted in the Rician fading channels. Instead, Eve's SNR remains relatively flat as in Rayleigh fading channels. This suggests that there are multiple paths from the BS to the user. Those paths have diverging azimuth angles but more focused elevation angles. As a result, the diverging azimuth paths alleviate the Eve SNR reduction predicted by a single LoS in Rician channel, resulting an Eve SNR trend closer to the Rayleigh fading channels.

In addition to the indoor LoS scenario, we further investigate in the outdoor LoS scenario, demonstrating an increasing eavesdropping advantage in a stronger LoS scenario predicted by the Rician model when Bob and Eve share the elevation angle.

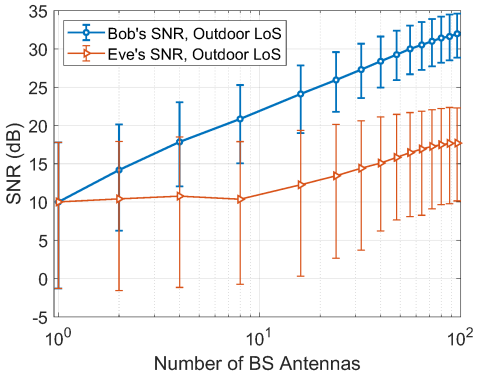


Fig. 10. Bob's and Eve's SNR in outdoor LoS scenario.

Fig. 10 shows Bob and Eve's SNR in an outdoor LoS scenario. The channels are measured using the same procedure and topology described in Section IV-A. In Fig. 10, we again see a clear turning point at antenna size of 8, the column size of the BS antenna array. Furthermore, Eve's SNR increases faster beyond antenna size of 8 as the BS increases more rows of antennas, showing a higher SNR correlation between Bob and Eve as predicted by the predicted by the Rician fading with a larger K.

From the Rician channel analysis to the measurements both in the indoor and outdoor LoS scenarios, we demonstrate an eavesdropping strategy in the LoS scenario unknown before. The elevation angle sharing strategy is a rather flexible requirement for the eavesdropper, and yet has shown to be effective in a LoS scenario. Due to the low requirement of the strategy, the threat is hard to detect or prevent. While limiting the row size of the antenna array at the BS can be a solution, it sacrifices the spatial resolution in the elevation domain at the same time. In the end, the physical layer security dream promised by the massive MIMO can not be taken as granted. In addition to the limited number of antenna and discretized MCS levels studied in the early sections, LoS, or more generally path sharing, adds to the imperfections in the practical world, resulting in eavesdropping vulnerabilities that cannot be ignored.

IX. Multi-Antenna Eve

In the previous sections, we study how Eve benefits from real-world factors when she has a single antenna. We further examine how the advantage scales as Eve increases her antenna size.

A. Multi-Antenna Eve Threat Model

We consider Eve with N_E antennas while the BS transmits to a single-antenna Bob. We can then rewrite Eve's receive signals in Eq. (1) as follows:

$$\boldsymbol{y}_e = \sqrt{p}\sqrt{\beta_e}\boldsymbol{H}_e\boldsymbol{w}s + \boldsymbol{n_e},$$

where $\boldsymbol{y}_e \in \mathbb{C}^{N_E\times 1}$ is Eve's receive signals across her N_E antennas, $\boldsymbol{H}_e \in \mathbb{C}^{N_E\times M}$ is the channel matrix from the M BS antennas to Eve's N_E antennas, and $\boldsymbol{n_e} \in \mathbb{C}^{N_E\times 1}$ is the additive Gaussian noise vector each with variance of σ^2. To maximize her SNR, the best Eve can do is to apply maximum ratio combining (MRC). Since the effective channel from the BS to Eve is $\boldsymbol{v}_e = \boldsymbol{H}_e\boldsymbol{w}$, Eve can apply MRC only if she knows both her own channel matrix $\boldsymbol{H}_e$ and the BS's beamforming weight $\boldsymbol{w}$. For the worst case analysis, we adapt these strong assumptions. Eve's SNR is thus

$$\begin{aligned}\text{SNR}_{Eve}^{\text{MRC}} &= \frac{p\beta_e}{\sigma^2}\frac{\left|\boldsymbol{v}_e^H\boldsymbol{v}_e\right|^2}{\|\boldsymbol{v}_e\|^2} = \frac{p\beta_e}{\sigma^2}\boldsymbol{v}_e^H\boldsymbol{v}_e = \frac{p\beta_e}{\sigma^2}\sum_{n=1}^{N_E}|v_n|^2 \\ &= \sum_{n=1}^{N_E}\text{SNR}_{Eve}^n,\end{aligned} \tag{7}$$

where SNR_{Eve}^n is the SNR obtained at the n-th antenna.

Eq. (7) shows the well known MRC result that the collective SNR is the summation of SNR at each element [35]. This result implies that the SNR advantage Eve gets due to channel correlation in a single antenna case accumulates in the multi-antenna scenario.

B. Experimental Results

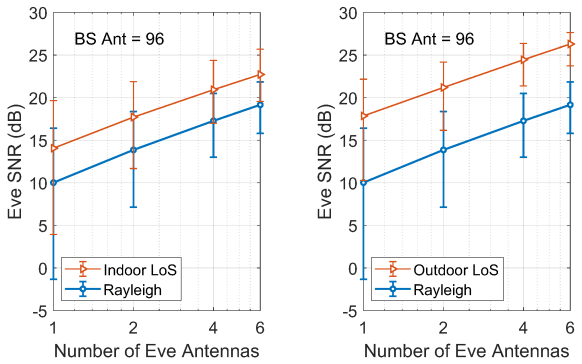
To investigate the multi-antenna Eve threat, we repurpose the same channel measurement datasets from a 96-antenna BS to 8 user locations in both indoor LoS and outdoor LoS scenario introduced in §IV-A and §VIII-C.

When using the dataset for multi-antenna Eve scenario, Bob is at one of the 8 user locations whereas Eve's N_E antennas are at N_E of the remaining 7 locations. That is, we consider Eve to have remote radio heads (RRH) at multiple separated

The final version of record is available at http://dx.doi.org/10.1109/TWC.2021.3074941

locations. While this setup is different from Eve having a co-located antenna array, it also captures the potential channel correlation in the real world. Since the RRH setup is more spread out in space and thus provides an averaging effect, we expect our results to have less extreme values than Eve having a co-located array. Nonetheless, we expect the RRH setup to capture the same trend.

In the multi-antenna Eve scenario, Alice's transmit strategy remains the same and results in the same Bob's SNR as in §V. Therefore, we focus on Eve's SNR in the following analysis. Specifically, we examine Eve's SNR scaling with increasing eavesdropping antenna size when the BS transmits to Bob with 96 antennas.



(a) Indoor LoS (b) Outdoor LoS

Fig. 11. Eve's SNR with increasing Eve antennas.

Fig. 11a and Fig. 11b show Eve's SNR as her antenna size increases from 1 to 6 in indoor LoS and outdoor LoS scenario respectively. Independent Rayleigh channel is shown as a baseline for comparison in both figures. First, we find that in all scenarios (indoor LoS, outdoor LoS, and Rayleigh) Eve's SNR increases by 3dB when her antenna size doubles. This result follows Eq. (7), which suggests that the collective SNR increases linearly with Eve's antenna size.

Next, we observe that Eve's SNR is larger in the measured channels than in independent Rayleigh channels, with Eve's SNR in the outdoor LoS being the highest. Recall we learn that Eve gets an SNR advantage due to channel correlation between Bob and Eve in the single-antenna Eve case (Fig. 4a and Fig. 10). In the multi-antenna Eve scenario, the SNR advantage is accumulated from all Eve's antennas and retains the same SNR advantage in the multi-antenna scenario. Therefore, higher channel correlation in the outdoor LoS scenario translates to a larger Eve SNR advantage compared to the indoor LoS scenario.

Eve's extra SNR gain due to channel correlation can be interpreted as a free multiplying effect on the Eve's antenna size. In the indoor LoS scenario, the 4 dB SNR advantage is effectively a $10^{4/10} \approx 2.5$ times larger array. That is, channel correlation in indoor LoS makes having only 2 antennas at Eve work as if having 5 antennas if there were no channel correlation. The multiplying factor is even larger for Eve in the outdoor LoS scenario. The 7 dB Eve SNR advantage in the outdoor LoS scenario effectively makes Eve's antenna array $10^{7/10} \approx 5$ times larger. While the cost of multiplying the actual array size scales exponentially with the array size, the effective array size multiplying due to channel correlation is always free, making channel correlation highly desirable for Eve but distasteful for Bob.

In this section, we discuss how channel correlation in the real world benefits Eve when she equips herself with more antennas. By using MRC, Eve accumulates SNR from all of her antennas. When channel correlation between Bob and Eve exists as in the real world, Eve's SNR advantages from different antennas are collected as well, resulting an extra SNR advantage in addition to the receive beamforming gain.

X. Related Works

Active eavesdropping. In TDD massive MIMO systems, Eve can actively contaminate the channel sounding pilot so that the BS obtains a faulty channel estimation for Bob and therefore unknowingly beamforms also to Eve when transmitting to Bob [36]. Many prior works investigated such pilot contamination attack [37] and its countermeasures [38]. In contrast, we examine an Eve passively monitoring the channels without sending any signals, showing a passive Eve can obtain advantages by better positioning considering channel correlation in the real world.

Theoretical Studies. Massive MIMO passive eavesdropping has been studied widely using theoretical approach. Under independent Rayleigh channels assumption, passive eavesdropping was shown to be negligible when the BS antenna size approaches infinity for single user [4] and multi-user scenarios [5]. Recent work also showed that selecting only a subset of antenna array enjoys the same favorable secrecy property [39]. In contrast, our work serves as the first effort to understand how the theoretical massive MIMO security prediction can be different in experimental settings. In addition, we examine the achievable secrecy on the existing physical layer by considering packet erasure at Bob and Eve, which reflects the achievable secrecy rate when secure network coding is applied before the transmissions.

Finite-Alphabet Input Wiretap Channel. While majority of the wiretap channel studies consider Gaussian input in which secrecy increases with transmit power, finite-alphabet input has been considered in the literature and was shown that higher transmit power does not always lead to better secrecy [32], countermeasures including power adaptation and null space jamming were thus investigated [33]. If Eve's channel is known, optimum precoding for finite alphabet inputs was also explored [23] and extended for large antenna arrays [24]. Compared to these theoretical prior works, we obtain similar results on power adaption based on an experimental setting. In addition, we examine the impact of the correlated over-the-air channels on the power adaptation countermeasure.

XI. Conclusion

Being the first experimental study of passive eavesdropping in massive MIMO, we consider practical factors including limited BS antenna array size, potential correlation in over-the-air channels, and adaptation of MCS over a discrete

and finite set. Based on channel measurements using a 96-antenna ArgosV2 BS, we have the following findings: *(i)* We find that Eve obtains a modest advantage due to channel correlation, and the gap between the measured channels and Rayleigh channels increases with the number of BS antennas. *(ii)* We identify the "MCS saturation regime" which happens when the high SNR saturates the predefined MCS levels and prevents the BS from utilizing potentially a better channel at Bob compared to Eve, suggesting the importance of transmit power adaptation. Yet, considering Eve's SNR advantage due to channel correlation, a more stringent power adaptation is required. *(iii)* We find that having a low angular spread to Bob does not help Eve. However, Eve can take advantage of the wide spread among different locations and search for the most favorable position. Also, Eve can move closer to the BS to improve her channel gain, which may force the BS to increase hundreds of antennas to counter. *(iv)* We demonstrate that Eve gains an advantage by simply sharing the elevation angle with Bob in the LoS scenario considering a rectangular antenna array at the BS. Moreover, this security vulnerability increases with stronger LoS. *(v)* We show that the SNR advantage obtained by a single-antenna Eve can be accumulated when she increases her antennas by applying MRC.

REFERENCES

[1] C.-Y. Yeh and E. W. Knightly, "Feasibility of Passive Eavesdropping in Massive MIMO: An Experimental Approach," in *Proceedings of 2018 IEEE Conference on Communications and Network Security (CNS)*.

[2] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for Next Generation Wireless Systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014.

[3] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[4] A. Al-Nahari, "Physical Layer Security Using Massive Multiple-Input and Multiple-Output: Passive and Active Eavesdroppers," *IET Communications*, vol. 10, no. 1, pp. 50–56, 2016.

[5] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical layer security in massive MIMO systems," in *Proceedings of 2017 51st Asilomar conference on signals, systems, and computers*. IEEE, 2017.

[6] Q. Li, C. Li, and J. Lin, "Constant Modulus Secure Beamforming for Multicast Massive MIMO Wiretap Channels," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 264–275, 2019.

[7] R. Zi, J. Liu, L. Gu, and X. Ge, "Enabling Security and High Energy Efficiency in the Internet of Things With Massive MIMO Hybrid Precoding," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8615–8625, 2019.

[8] J. Xu, P. Zhu, J. Li, X. Wang, and X. You, "Secrecy Energy Efficiency Optimization for Multi-User Distributed Massive MIMO Systems," *IEEE Transactions on Communications*, 2019.

[9] C. Song, "Leakage Rate Analysis for Artificial Noise Assisted Massive MIMO With Non-Coherent Passive Eavesdropper in Block-Fading," *IEEE Transactions on Wireless Communications*, vol. 18, no. 4, pp. 2111–2124, 2019.

[10] L. Sanguinetti, E. Björnson, and J. Hoydis, "Towards Massive MIMO 2.0: Understanding Spatial Correlation, Interference Suppression, and Pilot Contamination," *IEEE Transactions on Communications*, 2019.

[11] C. Shepard, H. Yu, and L. Zhong, "ArgosV2: A Flexible Many-Antenna Research Platform," in *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 2013.

[12] Y. Long, Z. Chen, L. Li, and J. Fang, "Non-asymptotic Analysis of Secrecy Capacity in Massive MIMO System," in *Proceedings of 2015 IEEE International Conference on Communications (ICC)*.

[13] J. Zhu, R. Schober, and V. K. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[14] ——, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.

[15] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading Correlation and Its Effect on the Capacity of Multielement Antenna Systems," *IEEE Transactions on communications*, vol. 48, no. 3, pp. 502–513, 2000.

[16] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky, "Correlation Analysis Based on MIMO Channel Measurements in an Indoor Environment," *IEEE Journal on Selected areas in communications*, vol. 21, no. 5, pp. 713–720, 2003.

[17] X. Gao, O. Edfors, F. Rusek, and F. Tufvesson, "Massive MIMO Performance Evaluation Based on Measured Propagation Data," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3899–3911, 2015.

[18] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, 2013.

[19] V. L. Q. Giang and T. T. Kiên, "Secret Capacity of Massive MIMO Systems with a Passive Eavesdropper," *Research and Development on Information and Communication Technology*, vol. 3, no. 40, 2018.

[20] X. Du and A. Sabharwal, "Shared Angles-of-Departure in Massive MIMO Channels: Correlation Analysis and Performance Impact," 2020.

[21] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, 2008.

[22] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively Securing Wireless Communications Using Zero-Forcing Beamforming," in *Proceedings of 2012 IEEE INFOCOM*.

[23] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear Precoding for Finite-Alphabet Signaling Over MIMOME Wiretap Channels," *IEEE transactions on vehicular technology*, vol. 61, no. 6, pp. 2599–2612, 2012.

[24] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure Transmission With Large Numbers of Antennas and Finite Alphabet Inputs," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3614–3628, 2017.

[25] G. Holland, N. Vaidya, and P. Bahl, "A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks," in *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001.

[26] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly, "Opportunistic Media Access for Multirate Ad Hoc Networks," in *Proceedings of the 8th annual international conference on Mobile computing and networking*. ACM, 2002.

[27] J. Zhang, K. Tan, J. Zhao, H. Wu, and Y. Zhang, "A Practical SNR-guided Rate Adaptation," in *Proceedings of the 27th Conference on Computer Communications (INFOCOM)*. IEEE, 2008.

[28] N. Cai and R. W. Yeung, "Secure Network Coding on a Wiretap Network," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 424–435, 2010.

[29] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," *IEEE Communications Letters*, vol. 18, no. 5, pp. 777–780, 2014.

[30] C. Shepard, J. Ding, R. E. Guerra, and L. Zhong, "Understanding Real Many-Antenna MU-MIMO Channels," in *Proceedings of the 50th Asilomar Conference on Signals, Systems and Computers*. IEEE, 2016.

[31] "WARP Project." [Online]. Available: http://warpproject.org

[32] M. R. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian Wiretap Channels with M-PAM Inputs," in *Proceedings of 2010 European Wireless Conference (EW)*. IEEE, 2010.

[33] S. Bashar, Z. Ding, and C. Xiao, "On the Secrecy Rate of Multi-Antenna Wiretap Channel under Finite-Alphabet Input," *IEEE communications letters*, vol. 15, no. 5, pp. 527–529, 2011.

[34] X. Zhang, L. Zhong, and A. Sabharwal, "Directional Training for FDD Massive MIMO," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5183–5197, 2018.

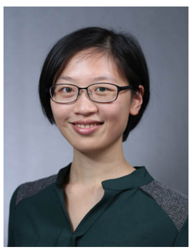
[35] A. Goldsmith, *Wireless Communications*. Cambridge university press, 2005.

[36] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

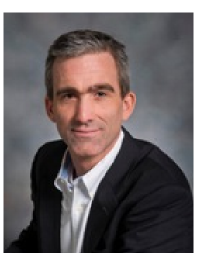
[37] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure Massive MIMO Transmission With an Active Eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[38] X. Zhang and E. W. Knightly, "Pilot Distortion Attack and Zero-Startup-Cost Detection in Massive MIMO Network: From Analysis to Experiments," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3094–3107, 2018.

[39] A. Bereyhi, S. Asaad, R. R. Muller, R. F. Schaefer, and A. M. Rabiei, "On Robustness of Massive MIMO Systems against Passive Eavesdropping under Antenna Selection," in *Proceedings of 2018 IEEE Global Communications Conference (GLOBECOM)*.



Chia-Yi Yeh received the B.S. degree in electrical engineering from National Taiwan University in 2014 and the M.S. degree in electrical and computer engineering from Rice University in 2017. She is pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering at Rice University. Her research interests are wireless security and cross-layer protocol design in new wireless systems including massive MIMO and terahertz communications.



Edward W. Knightly is the Sheafor-Lindsay Professor of Electrical and Computer Engineering and Computer Science at Rice University. He received his Ph.D. and M.S. from the University of California at Berkeley and his B.S. from Auburn University. He is an ACM Fellow, an IEEE Fellow, and a Sloan Fellow. He received the Dynamic Spectrum Alliance Award for Research on New Opportunities for Dynamic Spectrum Access and the National Science Foundation CAREER Award. His research interests are design and in-the-field demonstration of new mobile and wireless networks and systems, including mission-driven autonomous drone networks, wireless security, and millimeter wave and terahertz spectrum.