Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks

Berk Akgun, *Student Member, IEEE*, Marwan Krunz, *Fellow, IEEE*, and O. Ozan Koyluoglu, *Senior Member, IEEE*

***Abstract*— We consider a single-cell massive multiple-input multiple-output (MIMO) system in which a base station (BS) with a large number of antennas transmits simultaneously to several single-antenna users. The BS acquires the channel state information (CSI) for various receivers using uplink pilot transmissions. We demonstrate the vulnerability of the CSI estimation process to pilot-contamination (PC) attacks. In our attack model, the attacker aims at minimizing the sum rate of downlink transmissions by contaminating the uplink pilots. We first study these attacks for two downlink power allocation strategies under the assumption that the attacker knows the locations of the BS and its users. Later on, we relax this assumption and consider the case when such knowledge is probabilistic. The formulated problems are solved using stochastic optimization, Lagrangian minimization, and game-theoretic methods. A closed-form solution for a special case of the problem is obtained. Furthermore, we analyze the achievable individual secrecy rates under PC attacks and provide an upper bound on these rates. We also study this scenario without *a priori* knowledge of user locations at the attacker by introducing chance constraints. Our results indicate that such attacks can degrade the throughput of a massive MIMO system by more than 50%.**

***Index Terms*— Massive MIMO, pilot contamination, physical-layer security, jamming attack, stochastic optimization.**

I. Introduction

MASSIVE multiple-input multiple-output (MIMO) is one of the key technologies in the upcoming 5G systems. It is envisioned that a cellular 5G base station (BS) will be equipped with a very large antenna array, e.g., hundreds of antennas or more, boosting the spectral efficiency by orders of magnitude compared to a conventional MIMO system. Even though MIMO is a well-studied concept in wireless communications, massive MIMO requires novel techniques to overcome new design challenges, and as such it has received significant attention from researchers over the last few years (see, for example, [1]–[3], and the references therein).

Because of the large number of antennas at the BS and the relatively short channel coherence time, the channel state information (CSI) between the BS and individual users must be frequently estimated using uplink pilot transmissions. Assuming channel reciprocity, the BS utilizes these CSI estimates for downlink data transmissions. Due to the limited number of orthogonal pilot sequences (e.g., in the order of tens [4]), users in neighboring cells may share the same pilots. Interference among these pilots causes erroneous CSI estimates at the BS, leading to poor system performance. This is known as *pilot contamination* (PC). In addition to arising naturally due to reusing the same pilots, PC can be also caused by adversarial transmissions. Indeed, Zhou *et al.* [5] studied an attack that targets time division duplexing (TDD) systems. The key idea behind their attack is to contaminate uplink pilot transmissions and cause an erroneous uplink channel estimation. Typically, if the CSI is available, the BS would use MIMO beamforming techniques such as maximum-ratio transmission (MRT) to maximize the signal-to-noise-ratio (SNR) at various receivers. However, the benefits of these techniques vanish rapidly if the CSI estimates are erroneous. A self-contamination technique in which the user generates a random signal and superimposes it onto its uplink pilots was proposed in [6]. This random signal allows the BS to detect the attacker, but it also decreases the quality of channel estimation due to the introduced noise. An extension of this approach was provided in [7] to allow for the estimation of both legitimate receiver and attacker channels at the BS, and to enable secure communications in a single-user massive MIMO system. It is not clear how these attack detection methods can be applied in a multiuser scenario, as the introduced random signals from legitimate users would degrade the channel estimation at the BS even more. Kapetanovic *et al.* [8] proposed another approach in which the legitimate user transmits four random phase-shift keying symbols, and the BS checks the correlation matrix of the received signals. Based on the ratio of the two largest eigenvalues of this matrix, the BS detects the attack. In [9], an uncoordinated frequency shift scheme was proposed for detecting a PC attack. According to this scheme, the user applies random frequency shifts while transmitting the pilot sequence. However, this scheme requires joint estimation of the shift value and the channel between the BS and the user,

Manuscript received February 22, 2018; revised July 11, 2018 and September 18, 2018; accepted September 19, 2018. Date of publication October 22, 2018; date of current version January 23, 2019. This work was supported in part by the National Science Foundation under Grants CNS-1409172, CNS-1513649, IIP-1265960, and CNS-1748692, and in part by the Qatar Foundation under Grant NPRP 8-052-2-029. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Walid Saad. *(Corresponding author: Berk Akgun.)*

B. Akgun is with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721 USA (e-mail: berkakgun@email.arizona.edu).

M. Krunz is with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721 USA, and also with the Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: krunz@email.arizona.edu).

O. O. Koyluoglu is with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720 USA (e-mail: ozan.koyluoglu@berkeley.edu).

Digital Object Identifier 10.1109/TIFS.2018.2876750

hence incurring high computational complexity especially for a multiuser massive MIMO system. Tugnait [10] studied detection and mitigation of reused pilots (not necessarily due to an adversarial attack) in massive MIMO systems. However, their approach requires both training and information-bearing uplink data transmissions. Because a malicious attacker does not send uplink information messages to the BS, this method is not applicable to PC attacks. Secure transmissions for TDD-based massive MIMO systems was studied in [11] in the presence of an active eavesdropper. The authors derived the optimal power allocation for the information and artificial noise (AN) signals at the BS such that secrecy is asymptotically guaranteed as the number of BS antennas (M) tends to infinity. Secrecy performance of massive MIMO systems was studied in [12] and [13] in the presence of passive eavesdroppers. Zhu *et al.* [12] considered employing various linear data and AN precoding methods to secure downlink transmission, whereas Asaad *et al.* [13] studied the impacts of transmit antenna selection on the achievable ergodic secrecy rate and secrecy outage capacity. Basciftci *et al.* [14] proposed another method to provide secrecy against PC attacks by keeping pilot assignments hidden and using a pilot set that scales with M. However, there are two main problems with this scheme. First, it requires a longer pilot transmission phase, which increases the overhead and decreases the throughput. Second, computationally intensive cryptographic methods are required to keep pilot assignments hidden. A two-way training-based scheme against PC attacks was proposed in [15], which requires both downlink and uplink channel estimation. Such estimation can be prohibitively time-consuming to perform in massive MIMO systems if M is large. All of the above works consider an attacker that targets users, one at a time. Even when a multiuser system is considered, it is often assumed that the attacker randomly selects one user and contaminates its pilot sequence. Given that one of the key aspects of massive MIMO systems is to simultaneously serve tens of users, the vulnerabilities of these systems to a multiuser PC attack has not been investigated before.

As a side remark, Björnson *et al.* [16] [16] showed that as $M \to \infty$, massive MIMO systems can achieve unlimited capacity even under non-adversarial PC. However, the analysis in [16] was conducted assuming that the channel covariance matrices of various users are already known at the BS. Such an assumption cannot be made for the channel covariance matrix of an adversary, which makes the results of [16] inapplicable to our setup.

A. Motivation and Contributions

In this paper, we focus on a single-cell multiuser massive MIMO network in the presence of an external attacker. In general, non-adverserial PC has been extensively studied in the context of a multi-cell massive MIMO system [4]. Various PC mitigation schemes, including protocol-based methods and blind CSI estimation methods, have been proposed for such systems [3]. The main objective of these schemes is to separate the CSI estimation processes of adjacent cells so that inter-cell PC is mitigated. However, previously proposed schemes are not sufficient to mitigate PC from an intra-cell attacker. For example, protocol-based methods require coordination between adjacent BSs to avoid synchronized transmission of the same pilots. This will not work in the case of a non-cooperative adversary. On the other hand, blind CSI estimation methods rely on the fact that the distances between the BS and the interfering users in adjacent cells are much longer than the ones in its own cell. However, this is not the case for an intra-cell attacker, where the distance between the attacker and the BS can be very short. In our work, we consider a system where PC among multiple cells has been mitigated by employing one of the existing schemes, and we focus on the vulnerabilities of a single-cell massive MIMO network to an intra-cell attack. We do that based on an attack model that targets minimizing the sum-rate of downlink transmissions.

The contributions of this paper can be summarized as follows:

- In our attack model, the attacker contaminates the uplink pilot transmissions of multiple users, i.e., PC attack. The downlink transmission rates in the presence/absence of the attack are derived by exploiting the *channel hardening effect* of massive MIMO (effect of small-scale fading on channel gains vanishes as M tends to infinity).
- We investigate optimal PC attack strategies for two different cases: when the attacker knows the locations of the BS and its users, and when it does not have this information. Considering a fixed power allocation strategy for downlink data transmissions, convex problems are formulated to determine the optimal PC powers at the attacker that minimizes the downlink sum-rate. Unlike [17], a PC power constraint is introduced to take the attack detection probability into consideration. These problems are solved via the gradient descent and Lagrangian minimization methods.
- We obtain a closed-form solution for the optimal PC powers at the attacker when it has perfect information of the network. This solution represents a lower bound on the downlink sum-rate of massive MIMO systems under an optimal PC attack and a fixed BS transmission power. In the case of imperfect knowledge on the user locations, we first study the system for any arbitrary distribution. Then, a special case where the users are randomly and uniformly located on a ring around the BS is further analyzed to gain more insight into the interactions of various system parameters and to achieve faster convergence to the solution.
- We study the scenario where the BS optimizes its own power allocation scheme in the presence of a PC attack. For this case, a convex-concave game is formulated between the BS and the attacker. We present an iterative algorithm to obtain the Nash equilibrium (NE) of this game. This analysis provides an upper-bound on the downlink sum-rate of massive MIMO systems under an optimal PC attack.
- We extend our work in [17] and analyze the secrecy performance of a massive MIMO system under a PC attack. Note that although massive MIMO systems are robust against passive eavesdropping (as the CSI at a legitimate

receiver and an eavesdropper are near-orthogonal [8]), they are still vulnerable to an active attacker that contaminates the uplink pilot transmissions. Specifically, by using the PC attack, an attacker captures the downlink information signals with a much higher signal power. Here, we study a scenario where the attacker minimizes the maximum of the achievable individual secrecy rates at various users. The asymptotic behavior of the information leakage rate at the attacker is derived for a large number of antennas at the BS. Because the attacker simultaneously receives all information signals intended to various users, i.e., through a multiple-access channel, interference among these signals at the attacker leads to a non-convex problem. By deriving an upper-bound on the maximum interference power, we obtain a tractable problem that can be efficiently solved by our proposed iterative approach. Our analysis provides an upper-bound on the achievable individual secrecy rates in a given massive MIMO system under the PC attack. Moreover, by introducing chance constraints, we extend our analysis to the case when priori knowledge of user locations is not available to the attacker. Utilizing a similar bounding approach as in the previous case, we convert the non-convex problem to a tractable one under these constraints and solve it numerically. Our formulation for secrecy performance analysis in this paper can be applied to various other scenarios.

The rest of the paper is organized as follows. Section II describes the system model. In Section III, we compute the downlink transmission rates in the presence/absence of a PC attack. Our PC attack under a fixed and optimal BS transmission power is studied in Section IV. in Section V, we analyze the individual secrecy rates of users under this attack model. We provide numerical results in Section VI, and conclude the paper in Section VII.

Throughout the paper, we adopt the following notation. $\mathbb{E}[\cdot]$ indicates the expectation of a random variable. Row vectors and matrices are denoted by bold lower-case and upper-case letters, respectively. $(\cdot)^*$ and $(\cdot)^T$ represent the complex conjugate transpose and transpose of a vector/matrix, respectively. Frobenius norm and the absolute value of a real or complex number are denoted by $\|\cdot\|$ and $|\cdot|$, respectively. $\mathbf{A} \in \mathbb{C}^{M\times N}$ means that $\mathbf{A}$ is an $M \times N$ complex matrix, and $\mathbf{I}_M$ is an $M \times M$ identity matrix. $\mathcal{CN}(\mu, \sigma^2)$ denotes a complex circularly symmetric Gaussian random variable of mean μ and variance σ^2. $[x]^+$ is defined as $\max(x, 0)$. For simplicity, $\log_2(\cdot)$ is referred to as $\log(\cdot)$.

II. Preliminaries and Problem Statement

A. Link Model

Consider a massive MIMO system in which the BS (Alice) uses M antenna elements to transmit independent data streams to K single-antenna users (Bobs), where $M \gg K$. Because of the large M, the channel coherence time is too short to estimate the CSI for all M downlink channels at each user [3]. Therefore, TDD is used instead of FDD, in which the downlink and uplink channels are estimated separately (please refer to Fig. 1). In TDD, Alice estimates the CSI for uplink channels after receiving pilot sequences transmitted by various Bobs. If these pilot symbols are not perfectly orthogonal to each other, their mutual interference causes erroneous channel estimates at Alice. Assuming channel reciprocity, uplink CSI estimates are used in setting the precoding matrices for downlink data transmissions. There is no standardized way to ensure pilot orthogonality in massive MIMO systems. However, Marzetta [4] suggested assigning an orthogonal time-frequency pilot sequence to each Bob. Orthogonal space-time block codes can be also utilized, as in 802.11ac systems, to increase the number of orthogonal pilot sequences. In the following, the index k is used to refer to the kth Bob, $k \in \{1, \cdots, K\} \triangleq \mathcal{K}$. Let $\mathbf{p}_k \in \mathbb{C}^{1\times L}$ be the transmitted pilot sequence by Bob$_k$ (kth Bob), where L is the number of symbols in the pilot sequence. As these pilot sequences are orthogonal to each other, $\mathbf{p}_k\mathbf{p}_l^* = 0\ \forall\ k$ and $l \in \mathcal{K}$, $k \neq l$. We normalize the transmission powers of pilots such that $\mathbf{p}_k\mathbf{p}_k^* = L\ \forall k \in \mathcal{K}$. P_k is the pilot transmission power at Bob$_k$. The received signal at Alice during the pilot transmission phase is given by:

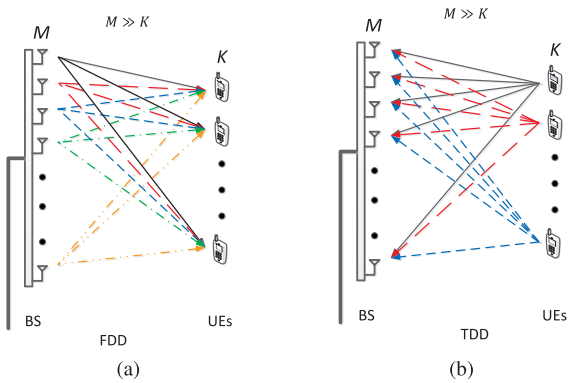


Fig. 1. (a) FDD massive MIMO requires M orthogonal pilots, (b) TDD massive MIMO requires K orthogonal pilots.

$$\mathbf{Y}_A = \sum_{i=1}^{K} \sqrt{P_k}\mathbf{h}_k^T\mathbf{p}_k + \mathbf{W} \tag{1}$$

where $\mathbf{h}_k^T \in \mathbb{C}^{M\times 1}$ is the uplink channel vector from Bob$_k$ to Alice. The mth entry of this vector is given by $h_k^{(m)} = \sqrt{\theta_k}g_k^{(m)}$, where θ_k and $g_k^{(m)} \sim \mathcal{CN}(0, 1)$ are the path-loss component (large-scale fading) and small-scale effects of the channel (Rayleigh fading), respectively. Note that θ_k is roughly the same for all antennas m, so $\mathbf{h}_k$ can be written as $\mathbf{h}_k = \sqrt{\theta_k}\mathbf{g}_k$, where $\mathbf{g}_k$ is a vector of all $g_k^{(m)}$, $m = 1, \cdots, M$. $\mathbf{W}$ is the additive white Gaussian noise (AWGN) matrix, whose entries are zero-mean, unit-variance normal random variables.

Without loss of generality, consider an arbitrary Bob$_i$, $i \in \mathcal{K}$. Let $\hat{\mathbf{h}}_i$ be Alice's estimate of the true $\mathbf{h}_i$. Under a priori knowledge of $\mathbf{p}_i$, Alice post-multiplies the received signal by $\mathbf{p}_i^*$ and divides it by $\sqrt{P_i}$ and L to obtain:

$$\begin{aligned}\hat{\mathbf{h}}_i^T &= \frac{\mathbf{Y}_A\mathbf{p}_i^*}{\sqrt{P_i}L} = \sum_{k=1}^{K}\frac{\sqrt{P_k}\mathbf{h}_k^T\mathbf{p}_k\mathbf{p}_i^*}{\sqrt{P_i}L} + \frac{\mathbf{W}\mathbf{p}_i^*}{\sqrt{P_i}L} \\ &= \mathbf{h}_i^T + \tilde{\mathbf{w}}_i^T\end{aligned} \tag{2}$$

where $\tilde{\mathbf{w}}_i^T \triangleq \frac{\mathbf{W}\mathbf{p}_i^*}{\sqrt{P_i}L} \sim \mathcal{CN}(0, \frac{1}{P_iL}\mathbf{I}_M)$.

B. Attack Model

Before describing our attack model, we provide background information on how synchronization between Alice and Bobs is achieved. Massive MIMO technology is expected to be deployed in 5G New Radio (NR) and LTE Advanced Pro (LTE-A) systems [2], [18]. The initial access and signaling procedures of both systems are very similar to each other. To add a new user to the network, both systems define two types of synchronization signals: primary synchronization signal (PSS) and secondary synchronization signal (SSS) [19], [20]. These signals are periodically broadcasted by the BS. A new user that wants to establish a connection with the BS tries to detect these signals, and uses the information embedded in them to synchronize itself with the BS (both in time and frequency). (There are various recently proposed methods that improve time and frequency synchronization of users with BSs [21], [22].) After the user and BS exchange control messages, the user joins the network. As stated before, TDD is envisioned to be employed in massive MIMO systems, where channel estimation is performed through uplink pilot transmissions. These pilots are called Sound Reference Signal (SRS), and their configuration is provided to the user after connection establishment via the Radio Resource Control (RRC) messages. SRSs are based on Zadoff-Chu sequences (whose cyclic shifts are orthogonal to each other), and generally, they are publicly known. A BS can schedule SRS transmissions from multiple users to the same physical radio resource.

Considering the initial access and pilot transmission mechanism in 5G NR and LTE-A, an attacker can contaminate uplink pilot transmissions by imposing its own signal. In particular, because of the periodic transmission of SRSs (pilots) and limited number of orthogonal sequences, the attacker can easily eavesdrop on the channel and learn various pilot assignments to various Bobs as well as their transmission time slots. Furthermore, an attacker may be an insider device, meaning that she can establish a legitimate connection with the BS and acquire the information of SRS transmission resources (as these resource are shared with multiple users). In another instance, this insider can convey the pilot transmission time and duration to an external colluding adversary, which can then contaminate the pilot transmissions. Let $\mathbf{x}_J \in \mathbb{C}^{1\times L}$ be the signal generated by the attacker, which will be explained shortly. After the attack, the received signal at Alice is modified as follows:

$$\mathbf{Y}_A = \sum_{k=1}^{K} \sqrt{P_k}\mathbf{h}_k^T \mathbf{p}_k + \mathbf{h}_J^T \mathbf{x}_J + \mathbf{W} \tag{3}$$

where $\mathbf{h}_J^T \in \mathbb{C}^{M\times 1}$ is the channel vector from the attacker to Alice. In the literature, $\mathbf{x}_J$ is often designed such that only a single arbitrarily selected user is targeted by the attacker [5], [14]. More specifically, $\mathbf{x}_J$ is often set to $\sqrt{P_J}\mathbf{p}_k$, where P_J is the average jamming power. In contrast, in our model (refer to Fig. 2), we set $\mathbf{x}_J$ to:

$$\mathbf{x}_J = \sqrt{P_J}\sum_{k=1}^{K} \sqrt{\alpha_k}\mathbf{p}_k \tag{4}$$

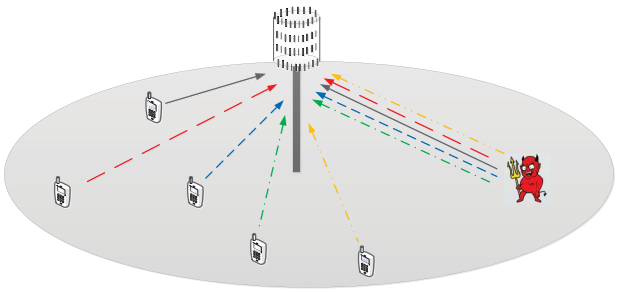


Fig. 2. Pilot contamination attack model in a multi-user massive MIMO system.

where α_k is the ratio between the power that the attacker allocates to contaminating pilot $\mathbf{p}_k$ and the average jamming power. Note that $\sum_{k=1}^{K} \alpha_k \leq 1$. Let R_k be the downlink transmission rate at Bob_k. The attacker's goal can be formulated as follows:

$$\underset{\{\alpha_k\ \forall k\in\mathcal{K}\}}{\text{minimize}} \sum_{k\in\mathcal{K}} R_k \tag{5}$$

$$s.t.\ \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1$$

where ρ is a given upper bound on the per-pilot jamming power. In the literature, it is noted that as the PC power increases, the attack detection probability at Alice also increases [6], [7]. As mentioned before, previous works studied only single-user scenarios, whereas here we consider a multiuser massive MIMO system. While it is not straightforward to apply previously proposed attack detection schemes to a multiuser setting, the attack detection probability certainly increases with the PC power in this case as well. Therefore, the attacker can try to hide herself from Alice (up to a predefined detection probability) by limiting her PC power. To account for this phenomenon, we introduce ρ.

III. Downlink Transmission Rates

In this section, we analyze the downlink sum-rate for the underlying massive MIMO system with/without the aforementioned PC attack.

A. Absence of PC Attack

For conventional MIMO systems, MRT gives rise to inter-user interference. However, as M tends to infinity, the channels between the BS and individual users become orthogonal to each other, and inter-user interference vanishes. In this case, MRT is the optimal precoder. For this reason, massive MIMO systems often apply MRT precoder at the BS [1]–[3], [23]. Let s_k be the downlink data transmission intended to Bob_k $\forall k \in \mathcal{K}$, and let $\mathbf{v}_k^T \in \mathbb{C}^{M\times 1}$ be its normalized precoder, with $\mathbf{v}_k\mathbf{v}_k^* = 1$. The received signal at Bob_k is given by:

$$y_k = \textstyle\sum_{i=1}^{K} \sqrt{P_i^{(d)}}\mathbf{h}_k\mathbf{v}_i^T s_i + w_k^{(d)} \tag{6}$$

where $P_k^{(d)}$ and $w_k^{(d)}$ are, respectively, the allocated power to s_k at Alice and the AWGN with zero-mean and unit-variance at

Bob_k. Under MRT precoding, $\mathbf{v}_k^T$ is given by $\mathbf{v}_k^T = (\hat{\mathbf{h}}_k^*/\|\hat{\mathbf{h}}_k\|)$. The achievable downlink rate at Bob_k becomes:

$$R_k = \log\left(1 + \frac{P_k^{(d)}|\mathbf{h}_k\mathbf{v}_k^T|^2}{\sum_{l\in\{\mathcal{K}\setminus k\}} P_l^{(d)}|\mathbf{h}_k\mathbf{v}_l^T|^2 + 1}\right), \quad k \in \mathcal{K}. \tag{7}$$

Note that the precoding vectors are computed based on channel estimates.

Next, we study the asymptotic behavior of R_k as $M \to \infty$. Such analysis is needed later on for comparison with the case under a PC attack. Consider the inter-user interference term $P_l^{(d)}|\mathbf{h}_k\mathbf{v}_l^T|^2$ in (7). Following the results in [3], [4], and [23], this term is scaled by M as follows:

$$\lim_{M\to\infty} \frac{P_l^{(d)}|\mathbf{h}_k\mathbf{v}_l^T|^2}{M} = 0 \tag{8}$$

$\forall k$ and $l \in \mathcal{K}$, where $k \neq l$. In other words, for a finite but sufficiently large M, with $M \gg K$, the channels are near-orthogonal, and hence, inter-user interference can be neglected. The underlying intuition behind this result is that entries of small-scale channel components of Bob_k and Bob_l are independent random variables of zero-mean and unit-variance. Hence, $\lim_{M\to\infty} \mathbf{g}_l\mathbf{g}_k^*/M = 0$ and $\lim_{M\to\infty} \mathbf{g}_l\tilde{\mathbf{w}}_k^*/M = 0$. Similarly, after some manipulations to the results in [23], the term in the numerator in (7) approaches:

$$\lim_{M\to\infty} \frac{P_k^{(d)}|\mathbf{h}_k\mathbf{v}_k^T|^2}{M} = \frac{P_k^{(d)}\theta_k^2}{\theta_k + \frac{1}{P_kL}} > 0 \tag{9}$$

Hence, the downlink rate at Bob_k behaves asymptotically as:

$$R_k \sim \log\left(1 + \frac{P_k^{(d)}\theta_k^2}{(\theta_k + \frac{1}{P_kL})\frac{1}{M}}\right). \tag{10}$$

In Section VI, we numerically verify these results. As explained before, θ_k is the large-scale channel components at Bob_k. (10) indicates that the SINR does not depend on the small-scale fading components, as these average out by the large antenna array (*channel hardening*). The term $(1/M)$ in (10) comes from the AWGN $w_k^{(d)}$ at Bob_k. As $M \to \infty$, the noise term vanishes and the SINR tends to infinity. Another noise term arises due to the channel estimation error $\tilde{\mathbf{w}}_i$. In particular, as the length of the pilots, L, increases, the second term in the denominator becomes smaller. This leads to an increase in the downlink rate. The same effect is also observed when the power allocated for pilots increases.

In this paper, we consider two different power allocation strategies for downlink transmissions: "fixed" and "optimal." Both strategies are subject to an average power constraint P_A. Under the fixed strategy, $P_k^{(d)}$ $\forall k \in \mathcal{K}$ is assumed to be known to the attacker. For example, based on some fairness criterion, these values may be determined by the BS before the pilot transmission phase and conveyed to various receivers through a feedback channel. If the attacker eavesdrops on this channel, it can obtain the power allocation values. In one instance of this strategy, the BS may simply allocate powers uniformly to information signals, i.e., $P_1^{(d)} = \cdots = P_K^{(d)} = P_A/K$. As for the "optimal" power allocation strategy, the BS relies on a water-filling technique to assign powers, using $(\theta_k + (P_kL)^{-1})/(M\theta_k^2)$ as the water levels [24].

B. Presence of PC Attack

Under the attack model in (4), the following channel estimation is performed at Alice for each Bob_k:

$$\hat{\mathbf{h}}_k = \mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k \tag{11}$$

where u_k is the ratio between the average power at the attacker and the pilot transmission power at Bob_k, i.e., $u_k = P_J/P_k$. In the rest of the paper, we assume that u_k is known to the attacker. Recall that we previously assumed that the attacker learns the pilot sequences by eavesdropping on uplink transmissions. The attacker can also learn the transmission powers of these pilots (which are typically fixed in current cellular systems). Because Alice is not aware of the presence of the attacker, she treats $\hat{\mathbf{h}}_k$ as the correct channel estimate. Employing MRT precoding based on $\hat{\mathbf{h}}_k$, Alice computes the precoder vector of s_k as:

$$\mathbf{v}_k^T = \frac{(\mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k)^*}{\|\mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k\|}. \tag{12}$$

Substituting $\mathbf{v}_k$ in (7), the attacker's optimization problem in (5) becomes non-convex in terms of α_k $\forall k \in \mathcal{K}$. To obtain a tractable model, we analyze the asymptotic behavior of R_k as $M \to \infty$. Following similar steps to the case of no attacker, the following expression can be obtained as $M \to \infty$:

$$R_k \sim \log\left(1 + \frac{P_k^{(d)}M\theta_k^2}{\theta_k + \alpha_k u_k\theta_J + \frac{1}{P_kL}}\right). \tag{13}$$

As M increases, the massive MIMO system expectedly becomes more resilient to PC attacks (in line with the conclusion in [16]). However, the vulnerability of the system against such an attack can be observed in (13), which shows that the SINR decreases with an increase in the jamming power $\alpha_k u_k$.

As in the previous section, we consider both a fixed and an "optimal" power allocation strategy to $P_k^{(d)}$'s. The fixed strategy is performed as before, whereas the "optimal" strategy is done as follows. Let $\phi_k \triangleq \theta_k + \alpha_k u_k\theta_J + \frac{1}{P_kL}$. Then, the "optimal" power allocation vector is given by:

$$\left[P_1^{(d)*} \cdots P_K^{(d)*}\right] = \underset{x_k,\forall k\in\mathcal{K}}{\text{argmax}} \sum_{k=1}^{K} R_{\text{sum}} \tag{14}$$

$$= \underset{x_k,\forall k\in\mathcal{K}}{\text{argmax}} \sum_{k=1}^{K} \log\left(1 + \frac{x_k M\theta_k^2}{\phi_k}\right) \tag{15}$$

subject to $\sum_{k=1}^{K} P_k^{(d)} \leq P_A$ and $P_k^{(d)} \geq 0$, $\forall k \in \mathcal{K}$. Note that in order to solve (14), Alice needs to be aware of the attack, which is not always possible. However, our goal here is to observe the effect of PC attack under the least favorable power allocation strategy from the perspective of the attacker. Essentially, this provides us with an upper-bound on the downlink sum-rate under any power allocation strategy.

IV. Analysis of Optimal PC Attack

A. Fixed Power Allocation Strategy

In this section, we study the optimal PC attack strategy under a fixed power allocation at Alice. We incorporate (13)

into problem (5), considering fixed power allocation for the information signals at Alice:

$$\mathbf{P1}: \quad \underset{\{\alpha_k,\ \forall k\in\mathcal{K}\}}{\text{minimize}} \sum_{k=1}^{K} \log\left(1+\frac{P_k^{(d)} M \theta_k^2}{\theta_k + \alpha_k u_k \theta_J + \frac{1}{P_k L}}\right)$$
$$s.t.\ \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1.$$

For a given $k \in \mathcal{K}$, we set $\theta_k = A z_k^{-\gamma}$, where A is a constant that depends on the operating frequency and transmit/receive antennas, while γ and z_k are the path-loss exponent and the distance between Alice and Bob$_k$, respectively. Similarly, z_J is the distance between Alice and the attacker. For simplicity, the antennas at Bobs and the attacker are assumed to be identical, so the same A is considered for all of them. As a result, the objective function in **P1** is converted to the following one:

$$R_{\text{sum}} = \sum_{k=1}^{K} \log\left(1+\frac{P_k^{(d)} M A z_k^{-2\gamma}}{\alpha_k u_k z_J^{-\gamma} + z_k^{-\gamma} + \frac{1}{A P_k L}}\right) \tag{16}$$

Next, we discuss two different scenarios based on the information available to the attacker.

1) Perfect Distance Information: Suppose that the attacker has perfect knowledge of the distances between Alice and individual Bobs as well as its own distance to Alice. Indeed, this is an idealized scenario (from the attacker's point of view), and is studied to provide a benchmark for comparison with the case of uncertainty in distances. **P1** is a convex programming problem. Its optimal solution is obtained as follows:

Theorem 1: **P1** has the following closed-form solution:

$$\alpha_k = \left[\min\left(\rho, \frac{\sqrt{A_k(A_k+4/\lambda)} - A_k - 2\ B_k}{2}\right)\right]^{+} \quad \forall k \in \mathcal{K} \tag{17}$$

where

$$A_k \triangleq \frac{P_k^{(d)} M A z_J^{\gamma}}{u_k z_k^{2\gamma}} \quad \text{and} \quad B_k \triangleq \frac{z_J^{\gamma}}{u_k z_k^{\gamma}} + \frac{z_J^{\gamma}}{u_k A P_k L}.$$

λ is the *Karush-Kuhn-Tucker* (KKT) multiplier and is chosen such that $\sum_{k=1}^{K} \alpha_k = 1$. It can be easily computed by the *bisection* method, given that $\sum_{k=1}^{K} \alpha_k$ is a decreasing function of λ.

Proof: See Appendix A. ∎

2) Uncertainty in Distances: Suppose that the attacker does not have exact knowledge of various distances, but has probabilistic information about such distances. Let Z_k and Z_J be random variables (rvs) that correspond to the Alice-Bob$_k$ and Alice-attacker distances, respectively. In this case, the attacker targets minimizing the expected value of R_{sum}, given by:

$$\mathbb{E}[\ R_{\text{sum}}\ ] = \mathbb{E}\left[\sum_{k=1}^{K} \log\left(1+\frac{P_k^{(d)} M A Z_k^{-2\gamma}}{\alpha_k u_k Z_J^{-\gamma} + Z_k^{-\gamma} + \frac{1}{A P_k L}}\right)\right]$$
$$= \sum_{k=1}^{K} \mathbb{E}\left[\log\left(1+\frac{P_k^{(d)} M A Z^{-2\gamma}}{\alpha_k u_k Z_J^{-\gamma} + Z^{-\gamma} + \frac{1}{A P_k L}}\right)\right] \tag{18}$$

where Z is a generic rv that has the same distribution as Z_k for all k. Let f_Z and f_{Z_J} be the PDF's of Z and Z_J, respectively, in the range $[D_{\min}, D_{\max}]$. In (18), the expectation is taken over Z and Z_J. The last equality follows from the assumption that the distributions of the distances between various Bobs and Alice are identical.

Let $\Phi_k \triangleq \alpha_k u_k Z_J^{-\gamma} + Z^{-\gamma} + \frac{1}{A P_k L}$. Under the fixed power allocation strategy, the optimal PC attack is the solution to the following stochastic programming problem:

$$\mathbf{P2}: \ \underset{\{\alpha_k\ \forall k\in\mathcal{K}\}}{\text{minimize}} \sum_{k=1}^{K} \mathbb{E}\left[\log\left(1+\frac{P_k^{(d)} M A Z^{-2\gamma}}{\Phi_k}\right)\right]$$
$$s.t.\ \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1.$$

The objective function in **P2** can be rewritten as:

$$\sum_{k=1}^{K} \int_{D_{\min}}^{D_{\max}} \int_{D_{\min}}^{D_{\max}} f_Z(x) f_{Z_J}(y) \log(\Psi_k(x,y))\, dx\, dy \tag{19}$$

where

$$\Psi_k(x,y) \triangleq 1 + \frac{P_k^{(d)} M A x^{-2\gamma}}{\alpha_k u_k y^{-\gamma} + x^{-\gamma} + \frac{1}{A P_k L}}.$$

This is a convex programming problem, as the objective function and inequality constraints are all convex functions. Notice that f_Z and f_{Z_J} can be any arbitrary distribution, as the integral operation in (19) preserves the convexity. The integral in (19) can be approximated by Simpson's Rule for double integrals, and can be solved efficiently by applying the interior-point method. We also note that **P2** need only be solved offline, so the time complexity of this solution method is not a concern.

To further analyze this scenario and gain more insight into the interactions of various system parameters, we consider a special case where Bobs are randomly and uniformly located on a ring around Alice. Hence, the PDF of Z is given by $f_Z(x) = 2x/(D_{\max}^2 - D_{\min}^2)$, for $x \in [D_{\min}, D_{\max}]$. Because Alice is a stationary BS, we assume that the attacker can acquire her distance information to Alice by overhearing messages such as already known preambles, i.e., z_J is known at the attacker. Therefore, the objective function in **P2** is converted to:

$$\sum_{k=1}^{K} \int_{D_{\min}}^{D_{\max}} \frac{2\ x}{(D_{\max}^2 - D_{\min}^2)} \log(\Psi_k(x, z_J))\, dx \tag{20}$$

The closed-form solution of this integral can be computed for any arbitrary integer valued γ. Here, we set γ to 2, and provide the result in (21) (at the top of the next page), where $C_k \triangleq P_k^{(d)} M A$ and $D_k \triangleq \alpha_k u_k z_J^{-2} + (A P_k L)^{-1}$. Note that the expression in (21) is a convex and differentiable function with respect to α_k, $\forall k \in \mathcal{K}$. Even though a closed-form solution does not exist for **P2**, a numerical solution can be obtained by applying the gradient-descent method, which leads to fast convergence.

$$\sum_{k=1}^{K} \frac{2}{(D_{\max}^2 - D_{\min}^2)} \left(\frac{x^2 \log\left(1+\frac{C_k}{D_k x^4+x^2}\right)}{2} + \frac{\log(1+D_k x^2)}{2\ D_k} - \frac{\log(D_k x^4+x^2+C_k)}{4\ D_k} + \frac{(4\ D_k C_k - 3)\arctan\left(\frac{1+2\ D_k x^2}{\sqrt{4\ D_k C_k - 1}}\right)}{2\ D_k \sqrt{4\ D_k C_k - 1}} \right) \Bigg|_{D_{\min}}^{D_{\max}} \tag{21}$$

3) Expected Value of Perfect Information (EVPI): Let $\mathbf{z} \triangleq [z_1, \cdots, z_K]$ be the vector of distances from Alice to various Bobs (known to the attacker). Let $\boldsymbol{\alpha}^*(\mathbf{z}, z_J) \triangleq [\alpha_1^*(\mathbf{z}, z_J), \cdots, \alpha_K^*(\mathbf{z}, z_J)]$ and $\boldsymbol{\alpha}^* \triangleq [\alpha_1^*, \cdots, \alpha_K^*]$ be the optimal solutions to **P1** and **P2**, respectively. The objective function of **P2** becomes $\mathbb{E}_{\mathbf{Z},Z_J}[R_{\text{sum}}(\boldsymbol{\alpha}^*)]$, and $\mathbb{E}_{\mathbf{Z},Z_J}[R_{\text{sum}}(\boldsymbol{\alpha}^*(\mathbf{Z}, Z_J))]$ becomes the expectation of the optimal solution of **P1** under perfect information, where $\mathbf{Z}$ is a vector of i.i.d. distances $Z_1, \cdots, Z_K$. The expectations are taken over the random distances, as previously explained. The EVPI is defined as follows:

$$\text{EVPI} \triangleq \mathbb{E}_{\mathbf{Z},Z_J}[R_{\text{sum}}(\boldsymbol{\alpha}^*)] - \mathbb{E}_{\mathbf{Z},Z_J}[R_{\text{sum}}(\boldsymbol{\alpha}^*(\mathbf{Z}, Z_J))]. \tag{22}$$

Note that EVPI is always greater than or equal to zero, as the case with perfect information outperforms the one with uncertainty. If EVPI is small, the attacker does not gain much by knowing the exact distances. It can perform attacks almost as powerful as when perfect information is available. On the other hand, if EVPI is high, the attacker may try to acquire distance information by estimating Bobs' locations relative to its own. For example, a group of colluding adversaries may employ localization techniques (e.g., RSSI and time-of-arrival) to estimate Alice-to-Bobs distances [25], [26]. This requires more complex and costly systems at the attacker. In Section VI, we study the behavior of EVPI.

B. Optimal Power Allocation

Next, we study the optimal PC attack strategy when Alice adopts "optimal" (the least favorable from the perspective of the attacker) power allocation strategy for downlink data transmissions. Our goal here is to provide an upper bound on the downlink sum-rate under ideal conditions from Alice's point of view. To do so, we investigate a scenario where the attacker tries to minimize that rate, while Alice maximizes it. This is a *min-max* problem, and its solution is found as follows.

As seen from (16), R_{sum} is a function of $\mathbf{P}^{(d)} \triangleq \left[P_1^{(d)} \cdots P_K^{(d)}\right]$ and $\boldsymbol{\alpha} \triangleq [\alpha_1, \cdots, \alpha_K]$. Thus, the problem can be formulated as a *convex-concave* game; for a fixed $\mathbf{P}^{(d)}$, $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$ is a convex function of $\boldsymbol{\alpha}$, and for a fixed $\boldsymbol{\alpha}$, $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$ is a concave function of $\mathbf{P}^{(d)}$. This means that the attacker needs to solve the following game:

$$\mathbf{P3}: \ \underset{\boldsymbol{\alpha}}{\text{minimize}} \left\{ \underset{\mathbf{P}^{(d)}}{\text{maximize}}\ R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha}) \right\}$$

$$s.t.\ \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1$$

$$P_k^{(d)} \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} P_k^{(d)} \leq P_A$$

Let $(\mathbf{P}^{(d)*}, \boldsymbol{\alpha}^*)$ be an optimal solution of this game, or a *saddle point*. That is, for any possible power allocation $\mathbf{P}^{(d)}$,

$$R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha}^*) \leq R_{\text{sum}}(\mathbf{P}^{(d)*}, \boldsymbol{\alpha}^*) \leq R_{\text{sum}}(\mathbf{P}^{(d)*}, \boldsymbol{\alpha}).$$

This relationship shows that an upper bound on $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha}^*)$ is obtained by solving **P3**, i.e., an upper bound on the downlink sum-rate in the presence of an optimal PC attack. For instance, when $\boldsymbol{\alpha} = \boldsymbol{\alpha}^*$, $\mathbf{P}^{(d)*}$ maximizes $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha}^*)$. This optimal solution is obtained by a well-known water-filling technique. Specifically,

$$P_k^{(d)*} = \left[\eta - \frac{\alpha_k^* u_k z_J^{-\gamma} + z_k^{-\gamma} + \frac{1}{AP_kL}}{MAz_k^{-2\gamma}} \right]^+ \tag{23}$$

where η is a water-filling level, chosen such that $\sum_{k=1}^{K} P_k^{(d)} = P_A$. It can be computed by the bisection method, as this summation is an increasing function of η. Similarly, when $\mathbf{P}^{(d)} = \mathbf{P}^{(d)*}$, $\boldsymbol{\alpha}^*$ minimizes $R_{\text{sum}}(\mathbf{P}^{(d)*}, \boldsymbol{\alpha})$. The optimal solution of this problem was previously given in Theorem 1. We propose to solve this game by using an iterative *Gauss-Seidel* method. To do that, we first solve $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$ for some initial values of α_k, e.g., $\alpha_k = 0\ \forall k \in \mathcal{K}$ (initially, there is no PC attack). Then, the obtained $P_k^{(d)}$ values are used in $R_{\text{sum}}(\mathbf{P}^{(d)*}, \boldsymbol{\alpha})$, and this problem is solved with respect to $\alpha_k\ \forall k \in \mathcal{K}$, as explained in Theorem 1. After this step, the second iteration starts by solving $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha}^*)$ using the new values of α_k's. As the number of iterations increases, a better approximation for the saddle point is obtained. We evaluated the number of iterations required to reach the Nash equilibrium of this game, and observed that the algorithm almost always converges after 10 iterations.

Theorem 2: Gauss-Seidel iterations converge when used to solve **P3**.

Proof: See Appendix B. ∎

Note that the above analysis applies to the case of perfect information where distances are known to the attacker. It can be easily extended to the case where only the probability distribution of distances is known. The same steps in Section IV-A.2 are applied to account for the uncertainty. In particular, the expectation of $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$ over Z_J and Z_k's would be used in the objective function of **P3**. The resulting problem is still a convex-concave game that can be solved by the Gauss-Seidel method. We skip this analysis here due to space limitations.

V. Secrecy Rate Under PC Attack

As stated before, the channels between Bobs and Alice are near-orthogonal as long as $M \gg K$. Indeed, as $M \to \infty$, inter-user interference vanishes in massive MIMO systems. The same reason also makes massive MIMO systems well-protected against a passive eavesdropper (Eve). For example,

channels of Eve and Bobs are near-orthogonal as well, so the mutual information leakage at Eve is negligible. However, we showed the vulnerability of massive MIMO systems against an active attacker that contaminates the pilot transmissions. So far, we only considered the case where the attacker's objective is to minimize the downlink sum-rate. A PC attack also makes Alice transmit information signals towards the attacker, as the precoding vectors are designed based on erroneous channel estimates, which are linear combinations of CSI at Bobs as well as at the attacker. As a result, the attacker may also receive information intended to Bobs in the data transmission phase. That is, instead of just reducing the transmission rates of legitimate users, the attacker may also aim at obtaining as much information as possible from the messages intended to these users.

To study this malicious eavesdropping scenario, we consider as a secrecy metric the individual secrecy rates of Bobs [27], [28]. Specifically, we study a problem in which the attacker, Eve, aims at minimizing the maximum of the "achievable individual secrecy rates" at given Bobs by adjusting its PC attack. By doing so, we aim at deriving an upper bound on the achievable individual secrecy rate that can be achieved by any Bob in a given massive MIMO system under an optimal PC attack. Notice that as Alice is not aware of such an attack, she may not achieve this upper bound. However, the analysis in this section gives some insightful results regarding how to design wiretap code to improve the secrecy outage probability or ergodic secrecy rate in massive MIMO systems. Considering MRT precoding at Alice and the same attack model in Sections II and III, the received signal at the attacker in the downlink data transmission phase is given by:

$$y_{\text{eve}} = \sum_{i=1}^{K} \sqrt{P_i^{(d)}} \mathbf{h}_J \mathbf{v}_i^T s_i + w_J \tag{24}$$

where w_J is the AWGN at Eve, and $\mathbf{v}_k^T = (\mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k)^*/\|\mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k\|$ is the precoder vector of s_k. The leakage rate of s_k to Eve is given by:

$$R_k^e = \log\left(1 + \frac{P_k^{(d)}|\mathbf{h}_J \mathbf{v}_k^T|^2}{\sum_{l\in\{\mathcal{K}\setminus k\}} P_l^{(d)}|\mathbf{h}_J \mathbf{v}_l^T|^2 + 1}\right), \quad \forall k \in \mathcal{K} \tag{25}$$

Note that R_k^e is obtained from the mutual information between s_k and y_{eve}, with the all other information signals are interpreted as noise. We analyze the asymptotic behavior of R_k^e as $M \to \infty$. Based on this analysis, the following limit is obtained:

$$\lim_{M\to\infty} \frac{P_k^{(d)}|\mathbf{h}_J \mathbf{v}_k^T|^2}{M} = \frac{P_k^{(d)}\alpha_k u_k \theta_J^2}{\theta_k + \alpha_k u_k \theta_J + \frac{1}{P_k L}} \tag{26}$$

(see Appendix C for the derivation of (26)). Therefore:

$$\lim_{M\to\infty} R_k^e = \log\left(1 + \frac{\frac{P_k^{(d)}\alpha_k u_k \theta_J^2}{\theta_k + \alpha_k u_k \theta_J + \frac{1}{P_k L}}}{\sum_{l\in\{\mathcal{K}\setminus k\}} \frac{P_l^{(d)}\alpha_l u_l \theta_J^2}{\theta_l + \alpha_l u_l \theta_J + \frac{1}{P_l L}}}\right). \tag{27}$$

Note that $\lim_{M\to\infty} R_k^e$ is independent of M. In addition, the case where $\alpha_k = 0$, $\forall k \in \mathcal{K}$ corresponds to a purely passive eavesdropper scenario. In that case, R_k^e asymptotically goes to zero. This result is indeed in line with (8), where the inter-user interference is proved to be negligible. In Section VI, we numerically compare two scenarios, with passive and active adversary. As we analyze the asymptotic behavior of the system, $\lim_{M\to\infty} R_k^e$ is simply referred to as R_k^e in the rest of the paper.

A. Known Distances at Attacker

The achievable individual secrecy rate for Bob_k is defined by $[R_k - R_k^e]^+$ [28]. Under the fixed power allocation strategy for the downlink transmissions and perfect distance information at Eve, the optimal PC attack that minimizes the maximum of individual secrecy rates is formulated as follows:

$$\begin{aligned} &\underset{\{\alpha_k,\ \forall k\in\mathcal{K}\}}{\text{minimize}} \quad \max\{R_1 - R_1^e, \cdots, R_K - R_K^e, 0\} \\ &s.t.\ \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1. \end{aligned}$$

We reformulate this problem by introducing a new decision variable ν, such that $\nu \geq \max\{R_1 - R_1^e, \cdots, R_K - R_K^e, 0\}$. This is equivalent to $\nu \geq 0$ and $\nu \geq R_k - R_k^e\ \forall k \in \mathcal{K}$. The problem is now converted to the following one:

$$\begin{aligned} \mathbf{P4}: \ &\underset{\{\nu,\alpha_k,\ \forall k\in\mathcal{K}\}}{\text{minimize}} \quad \nu \\ &s.t.\ R_k - R_k^e - \nu \leq 0\ \forall k \in \mathcal{K} \\ &\qquad \nu \geq 0, \quad \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1 \end{aligned}$$

Note that the solution of **P4** provides the tightest upper-bound on the achievable individual secrecy rate. However, due to the interference of the information signals at Eve, the first constraint in **P4** is not convex. This makes the problem intractable. Let $G_k \triangleq P_k^{(d)}\theta_J$. Therefore, R_k and R_k^e are given as follows:

$$R_k = \log\left(1 + \frac{A_k}{\alpha_k + B_k}\right) \tag{28}$$

$$R_k^e = \log\left(1 + \frac{\frac{G_k\alpha_k}{\alpha_k + B_k}}{\sum_{l\neq k}^{K} \frac{G_l\alpha_l}{\alpha_l + B_l}}\right). \tag{29}$$

Lemma 3: Let $I_k \triangleq \sum_{l\neq k}^{K} G_l\alpha_l/(\alpha_l + B_l)$ where $\alpha_l = [\sqrt{G_l B_l/\vartheta} - B_l]^+\ \forall l \in \mathcal{K}$, $l \neq k$ and ϑ is chosen such that $\sum_{l\neq k}^{K} \alpha_l = 1$. Let

$$U_k \triangleq R_k - \log\left(1 + \frac{G_k\alpha_k}{(\alpha_k + B_k)I_k}\right). \tag{30}$$

Then, U_k is an upper bound on $R_k - R_k^e$.

Proof: An upper bound on $R_k - R_k^e$ can be obtained by maximizing the term $\sum_{l\neq k}^{K} G_l\alpha_l/(\alpha_l + B_l)$ in R_k^e. This term is a concave function with respect to $\alpha_l\ \forall l \in \mathcal{K}$, $l \neq k$. We also know that $\sum_{l\neq k}^{K} \alpha_l \leq 1$ and $\alpha_l \geq 0\ \forall l \in \mathcal{K}$, $l \neq k$. By applying the Lagrangian maximization method to solve this

constrained optimization problem, one can easily show that the above term is maximized when $\alpha_l = [\sqrt{G_l B_l/\vartheta} - B_l]^+$ $\forall l \in \mathcal{K}$, $l \neq k$. ϑ is chosen such that $\sum_{l\neq k}^{K} \alpha_l = 1$ and computed by the bisection method as $\sum_{l\neq k}^{K} \alpha_l$ is a decreasing function of ϑ. ∎

Replacing the first constraint in **P4** by $U_k - \nu \leq 0$ $\forall k \in \mathcal{K}$ makes the problem tractable, and its solution still provides an upper bound on the achievable individual secrecy rate for any Bob. Furthermore, the logarithm function can be removed by defining $\hat{\nu} \triangleq 2^{\nu}$. Then, **P4** becomes:

$$\mathbf{P5}: \underset{\{\hat{\nu},\alpha_k,\ \forall k\in\mathcal{K}\}}{\text{minimize}}\ \hat{\nu}$$
$$s.t.\ \frac{I_k(\alpha_k + A_k + B_k)}{\alpha_k(I_k + G_k) + B_k I_k} - \hat{\nu} \leq 0\ \forall k \in \mathcal{K}$$
$$\hat{\nu} \geq 1, \quad \rho \geq \alpha_k \geq 0\ \forall k \in \mathcal{K}, \quad \sum_{k=1}^{K} \alpha_k \leq 1$$

Let $f_k(\alpha_k) \triangleq I_k(\alpha_k + A_k + B_k)/(\alpha_k(I_k + G_k) + B_k I_k)$. Then, f_k is a monotonically decreasing function of α_k. We propose the following iterative method to numerically solve **P5**. Initially, $\max\{f_1(\alpha_1), \cdots, f_K(\alpha_K)\}$ is found for $\alpha_k = 0$ $\forall k \in \mathcal{K}$. Without loss of generality, let f_i^* be this maximum. Then, α_i is updated as $\alpha_i \leftarrow \alpha_i + \delta$, where δ is a positive real number. After that, the same process is repeated with the new values of α_k's as long as $\sum_{k=1}^{K} \alpha_k \leq 1$, $\hat{\nu} \geq 1$, and $\alpha_k \leq \rho$ $\forall k \in \mathcal{K}$. In Section VI, we numerically compare the two upper bounds obtained by solving **P4** and **P5**.

B. Unknown Distances at Attacker

If the exact locations of Bobs are not available to the attacker, then it is not possible for the attacker to deterministically guarantee an upper bound on the individual secrecy rates. Indeed, we consider an attack model in which the attacker seeks a *soft bound* on secrecy rate. Specifically, we replace the first constraint of **P4** by the following chance constraint:

$$\Pr\{R_k - R_k^e \geq \nu\} \leq \epsilon\ \forall k \in \mathcal{K} \tag{31}$$

where $\epsilon \in [0, 1]$ is a given parameter. Note that the randomness in (31) comes from the distances between Bobs and Alice, Z_k $\forall k \in \mathcal{K}$. (We assume that the attacker knows her distance to Alice, which is a stationary massive MIMO BS.) This constraint guarantees that the probability of achieving an individual secrecy rate that is higher than or equal to ν is less than or equal to ϵ at Bobs. That is, only ϵ fraction of Bobs can achieve an individual secrecy rate above ν. As (31) does not have a closed-form expression, **P4** is intractable for this case as well. Therefore, we use a similar bounding method as in the previous case to make the problem tractable.

Lemma 4: Let $\hat{B}_l$ denote B_l when $z_l = D_{\max}$ $\forall l \in \mathcal{K}$. Further, let $\hat{I}_k \triangleq \sum_{l\neq k}^{K} G_l\alpha_l/(\alpha_l + \hat{B}_l)$ where $\alpha_l = [\sqrt{G_l\hat{B}_l/\vartheta} - \hat{B}_l]^+$ $\forall l \in \mathcal{K}$, $l \neq k$ and ϑ is chosen such that $\sum_{l\neq k}^{K} \alpha_l = 1$. Let

$$\hat{U}_k \triangleq R_k - \log\left(1 + \frac{G_k\alpha_k}{(\alpha_k + B_k)\hat{I}_k}\right). \tag{32}$$

Then, $\hat{U}_k$ is an upper-bound on $R_k - R_k^e$.

Proof: The function $R_k - R_k^e$ is monotonically increasing with respect to both α_l and z_l $\forall l \in \mathcal{K}$, $l \neq k$. Therefore, an upper-bound of this function is obtained when $z_l = D_{\max}$ $\forall l \in \mathcal{K}, l \neq k$. Also, by applying the Lagrangian maximization method as in Lemma 3, the term $\sum_{l\neq k}^{K} G_l\alpha_l/(\alpha_l + \hat{B}_l)$ is upper-bounded when $\alpha_l = [\sqrt{G_l\hat{B}_l/\vartheta} - \hat{B}_l]^+$ $\forall l \in \mathcal{K}$, $l \neq k$ and ϑ is chosen such that $\sum_{l\neq k}^{K} \alpha_l = 1$. ∎

Using Lemma 4, we have:

$$\Pr\{R_k - R_k^e \geq \nu\} \leq \Pr\{\hat{U}_k \geq \nu\} \tag{33}$$
$$= \Pr\{P_k^{(d)} MA\hat{I}_k Z_k^{-2\gamma} - (\hat{\nu} - 1)\hat{I}_k Z_k^{-\gamma}$$
$$\geq \hat{\nu} P_k^{(d)}\alpha_k u_k A z_J^{-2\gamma} + (\hat{\nu} - 1)\hat{I}_k(\alpha_k u_k z_J^{-\gamma} + (AP_kL)^{-1})\} \tag{34}$$
$$\leq \Pr\{P_k^{(d)} MA\hat{I}_k Z_k^{-2\gamma} - (\hat{\nu} - 1)\hat{I}_k Z_k^{-2\gamma}$$
$$\geq \hat{\nu} P_k^{(d)}\alpha_k u_k A z_J^{-2\gamma} + (\hat{\nu} - 1)\hat{I}_k(\alpha_k u_k z_J^{-\gamma} + (AP_kL)^{-1})\} \tag{35}$$
$$= \Pr\left\{Z_k \leq \sqrt[2\gamma]{\frac{P_k^{(d)} MA\hat{I}_k - (\hat{\nu} - 1)\hat{I}_k}{J_k}}\right\} \tag{36}$$

where $J_k \triangleq \hat{\nu} P_k^{(d)}\alpha_k u_k A z_J^{-2\gamma} + (\hat{\nu} - 1)\hat{I}_k(\alpha_k u_k z_J^{-\gamma} + (AP_kL)^{-1})$. To further analyze this chance constraint, we exploit (36), which is the CDF of Z_k. Assume that Bobs are randomly and uniformly located in a circular ring around Alice. Hence, the PDF of Z is given by $f_Z(x) = 2x/(D_{\max}^2 - D_{\min}^2)$, for $x \in [D_{\min}, D_{\max}]$. The chance constraint (31) is converted to:

$$\frac{P_k^{(d)} MA\hat{I}_k - (\hat{\nu} - 1)\hat{I}_k}{J_k} \leq (\epsilon(D_{\max}^2 - D_{\min}^2) + D_{\min}^2)^{\gamma} \tag{37}$$

$\forall k \in \mathcal{K}$. This is equivalent to:

$$\frac{\hat{I}_k(P_k^{(d)} MA + 1 + Q(\alpha_k u_k z_J^{-\gamma} + (AP_kL)^{-1}))}{\hat{I}_k + Q(P_k^{(d)}\alpha_k u_k A z_J^{-2\gamma} + \hat{I}_k(\alpha_k u_k z_J^{-\gamma} + (AP_kL)^{-1}))} \leq \hat{\nu} \tag{38}$$

$\forall k \in \mathcal{K}$ where $Q = (\epsilon(D_{\max}^2 - D_{\min}^2) + D_{\min}^2)^{\gamma}$. To find the minimum $\hat{\nu}$ for a given ϵ, the same problem as **P5** is considered at the attacker after replacing the first constraint by (38). Note that the constraint function in (38) is a monotonically decreasing function with respect to α_k. Therefore, the method that we propose for solving **P5** in the previous subsection can be used here as well.

In this paper, we study the scenario where the attacker aims at minimizing the maximum of individual secrecy rates. The problem in which the attacker tries to minimize the sum of the individual secrecy rates could be also solved by following similar steps. Particularly, the problem would be similarly reformulated, and the new problem would be a convex optimization problem as well. Due to space limitations, we omit the details here.

VI. Numerical Results and Discussion

We model the channel gain from each transmit antenna to each receive antenna as $h = g\sqrt{Ad^{-3.522}}$, where $g \sim$

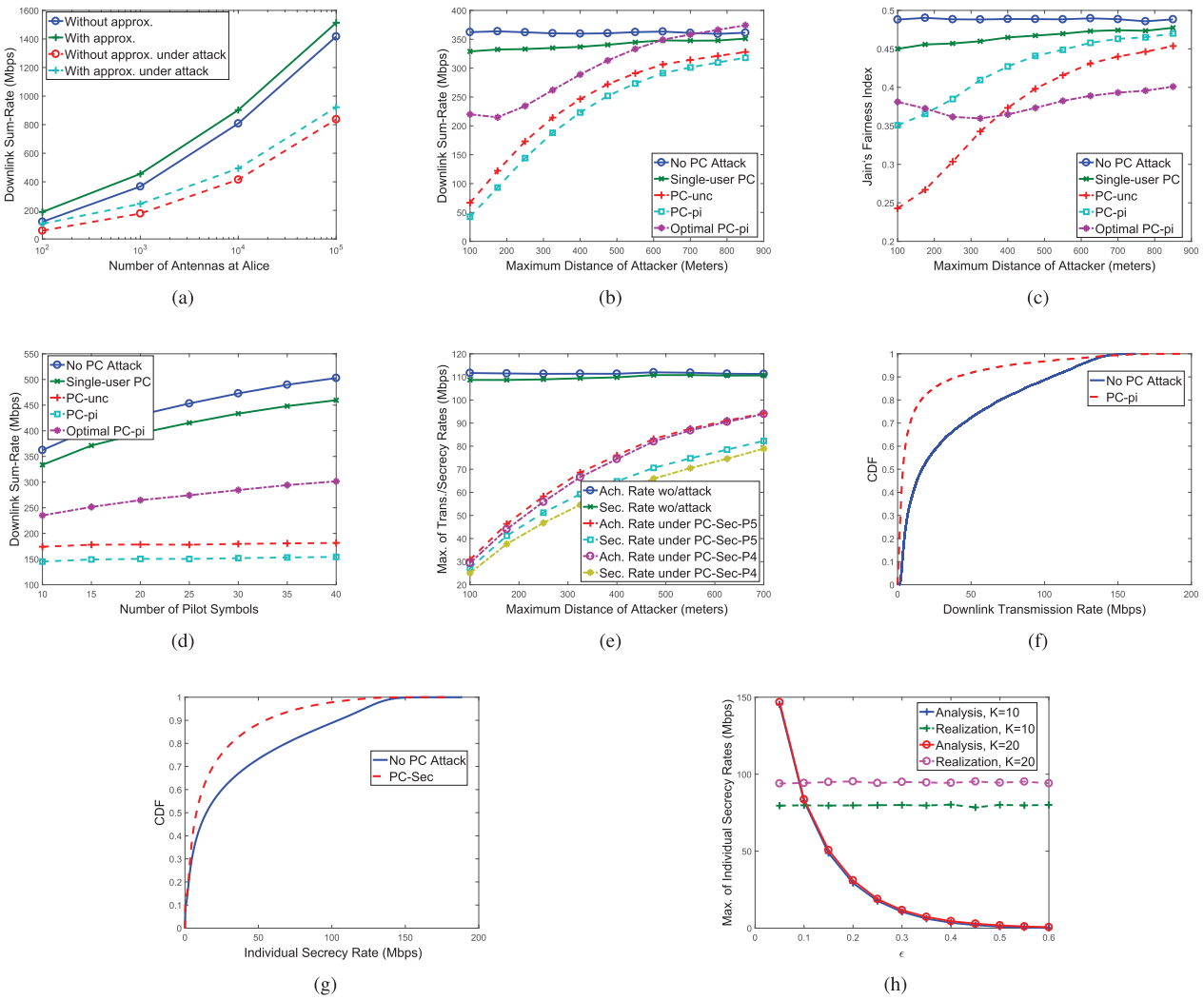


Fig. 3. (a) Downlink sum-rate vs. M under uniform power allocation at both Alice and the attacker, (b) downlink sum-rate vs. $D_{\max,\mathrm{J}}$, (c) Jain's fairness index vs. $D_{\max,\mathrm{J}}$, (d) downlink sum-rate vs. number of pilot symbols, (e) maximum of individual secrecy rates vs. $D_{\max,\mathrm{J}}$, (f) CDF vs. downlink transmission rate, (g) CDF vs. individual secrecy rate, (h) maximum of individual secrecy rates vs. ϵ.

$\mathcal{CN}(0,1)$ and $A = 3.0682 \times 10^{-5}$. The path-loss is modeled using the COST-Hata Model with center frequency is 2 GHz [29]. The average transmit powers at Alice, Bob_k, and the attacker are 46, 20, and 30 dBm, respectively. The durations of the pilot and data transmission phases are set to be equal [4]. We consider a 20 MHz channel with noise floor of -101 dBm. Bobs and the attacker are uniformly and randomly distributed within a circular ring whose center is Alice and whose outer radius is $D_{\max}$ and $D_{\max,\mathrm{J}}$, respectively. We set $D_{\max}$ to 750 meters and $D_{\min}$ to 10 meters. Our results are averaged over 10^5 different network realizations. As the purpose of this paper is to show the vulnerabilities of massive MIMO systems to PC attacks, we omit ρ in the numerical results. Also note that none of the previous works studied the PC attack detection for a scenario where the attacker aims at multiple Bobs.

We set the number of users $K = 10$. In Fig. 3(a), we consider uniform power allocation for both the information signals at Alice and the jamming signals at the attacker. The figure depicts the downlink sum-rate vs. M. It shows that (10) and (13) are good approximations for the downlink rates in (7). Note that the approximation-based sum-rate is slightly higher than the exact values, as the inter-user interference does not perfectly vanish at a finite M. In our subsequent results, we set M to 1000.

We observe the effect of the maximum distance between Alice and the attacker ($D_{\max,\mathrm{J}}$) in Figs. 3(b) and 3(c). In the case of a single-user PC attack, only one randomly selected Bob is targeted by the attacker. This attack can also be interpreted as an unintentional interference from a user in an adjacent cell. It does not have a big impact on the sum-rate. PC with uncertainty (PC-unc) and PC with perfect information (PC-pi) were explained in Section IV-A, and optimal PC-pi was studied in Section IV-B. Note that optimal PC-pi gives an upper-bound on the sum-rate of a massive MIMO system under an optimal PC attack. As the attacker moves farther from Alice, the sum-rate increases in all attack schemes. In Fig. 3(b), EVPI is around 20 Mbps. This says that when the attacker knows the distribution of

Bobs, it can launch attacks that are almost as powerful as when the attacker has complete CSI. We also observe that the downlink sum-rate without an attack (no PC attack case) is less than the one with the optimal PC-pi if $D_{\max,\mathrm{J}}$ is higher than 700 meters. The reason is that Alice uniformly allocates downlink transmission powers in no PC attack scheme, whereas she employs optimal power allocation in the optimal PC-pi. In Fig. 3(c), we depict Jain's fairness index for different schemes. Jain's fairness index ranges from $1/K$ to 1 for the worst and best cases, respectively (if all users have the same downlink rate, the fairness index is 1). The figure shows that fairness among Bobs is significantly reduced when PC attacks take place. PC-unc decreases the fairness more than PC-pi. The reason behind this phenomena is that when the attacker is close to Alice and knows the distances, Bobs with higher downlink rates are targeted. Therefore, Bobs are forced to have closer downlink rates, which increases the fairness index. Note that even though PC-pi makes the fairness higher compared to PC-unc, the sum-rate is lower in PC-pi.

In Fig 3(d), we set $D_{\max,\mathrm{J}}$ to 250 meters, and study the effect of the number of pilot symbols L. As L increases, the sum-rate increases as well in no PC, single-user PC, and optimal PC-pi attacks. The reason is that the error in MRT precoding vectors due to erroneous channel estimates decreases, and the signal strength at Bobs increases. On the other hand, the sum-rate does not increase under the PC-unc and PC-pi attacks. Note that in these cases, a fixed power is allocated for the information signals at Alice, and she does not exploit the decrease in channel estimation errors.

We evaluate the effect of PC attack on individual secrecy rates in Fig. 3(e). Specifically, we compare the schemes where there is no PC attack and PC attacks whose objective is to minimize the maximum of the individual secrecy rates (PC-Sec). PC-Sec-P4 and PC-Sec-P5 denote the results of the problems **P4** and **P5**, respectively, with known distances. Note that even though **P4** is not a tractable problem, we obtain its results with a brute force method. For each scheme, we show the results of both individual secrecy rates and transmission rates between Alice and Bobs. It is observed that the massive MIMO systems are resilient to passive eavesdroppers, as the maximum of transmission/secrecy rates are almost the same without a PC attack. On the other hand, PC attack decreases the maximum of individual secrecy rates from nearly 110 Mbps to 55 Mbps when $D_{\max,\mathrm{J}}$ is 325 meters. Moreover, we observe that when the attacker moves farther from Alice, PC attack still reduces the maximum of individual secrecy rates by almost 30%. It is also noted that the solution of **P5** is very close to the solution of **P4**, which provides the tightest upper-bound.

The empirical CDF of downlink transmission rate and individual secrecy rate under various schemes are shown in Figs. 3(f) and 3(g), respectively. 90% of Bobs achieve a transmission rate less than 40 Mbps under PC-pi. In the absence of a PC attack, nearly 33% of Bobs achieve a transmission rate higher than 40 Mbps. In Fig. 3(g), we observe that 13% of Bobs have a zero individual secrecy rate under PC-Sec, whereas only 7% fraction of Bobs have a zero individual secrecy rate when there is no PC attack. Moreover, only 5% of Bobs have a secrecy rate above 75 Mbps.

In Fig. 3(h), we evaluate our secrecy analysis with unknown distances at the attacker. We observe the effect of the designed parameter ϵ on the maximum of individual secrecy rates for both cases where $K = 10$ and $K = 20$. Based on our analysis, 0.1 fraction of Bobs may achieve an individual secrecy rate higher than 83 Mbps. When $K = 10$, the maximum of individual secrecy rates is just below this threshold value on average. On the other hand, when $K = 20$, this threshold value is exceeded almost always as expected. Note that when $\epsilon = 0.6$, the attacker guarantees that at least 0.4 fraction of Bobs have zero individual secrecy rate, which emphasizes the vulnerability of a massive MIMO system against a PC attack.

VII. Conclusion and Future Directions

We considered a single-cell massive MIMO system with several mobile users, and demonstrated vulnerabilities of uplink pilot transmissions to jamming attacks. Specifically, the attacker generates pilot sequences similar to those of users and contaminates the pilot transmissions to distort channel estimation at the BS. This PC attack reduces the downlink transmission rates, as the beamforming techniques utilized by the BS heavily depend on accurate CSI estimates. We formulated an optimization problem from the standpoint of the attacker to minimize the downlink sum-rate. Both cases when the attacker knows or does not know the distances between the BS and users were considered. Using (stochastic) optimization and game theory, we derived the optimal attacking strategies when the BS employs either fixed or optimal power allocation for downlink transmissions. We also analyzed the secrecy rates of the users in massive MIMO systems. In particular, we showed that even though such systems are robust against a passive eavesdropper, the PC attack significantly reduces the maximum of the individual secrecy rates. Our numerical results showed that the downlink sum-rate decreases significantly under a PC attack. Particularly, when the attacker is close to the BS, the downlink sum-rate of all users is reduced by more than 50%. Another important result of our work is that an attacker without perfect information about user locations is almost as devastating as one with perfect information. This fact emphasizes the vulnerability of massive MIMO systems to PC attacks. Further, we observed that even if the attacker moves farther from the BS, the maximum per-user secrecy rate is reduced by almost 30%.

We assumed that the attacker operates during a single transmission resource (e.g., frequency-time block). If she realizes that there is no transmission over that resource, she can switch to another one. Analysis of an attack model that includes multiple frequencies and time slots is left as future work. Furthermore, we considered single-antenna users throughout this paper for tractability. Our results can be easily extended to multi-antenna user scenarios under various setups. In one of these setups, each user may send a single pilot from all of its antennas, as the number of pilots is limited in massive MIMO systems. The BS estimates only the effective channels to users, so the system model reduces to multi-user multiple-input single-input (MISO) as we considered in this paper. In

another setup, multiplexing gain may be desired at users. In that case, users can transmit a different orthogonal pilot from each antenna so that the BS can estimate CSI to each one of them. To analyze the PC attack for this setup, the downlink transmission rates given in Section III need to be modified accordingly.

APPENDIX A
PROOF OF THEOREM 2

Let us define

$$A_k = \frac{P_k^{(d)} M A z_J^{\gamma}}{u_k z_k^{2\gamma}} \text{ and } B_k = \frac{z_J^{\gamma}}{u_k z_k^{\gamma}} + \frac{z_J^{\gamma}}{u_k A P_k L}$$

$\forall k \in \mathcal{K}$. Therefore, the objective of **P1** can be written by

$$R_{\text{sum}} = \sum_{k=1}^{K} \log\left(1 + \frac{A_k}{\alpha_k + B_k}\right) \tag{39}$$

Hence, the Lagrangian function of this problem is given by

$$L(\boldsymbol{\alpha}) = \sum_{k=1}^{K} \log(1 + \frac{A_k}{\alpha_k + B_k}) + \lambda(\sum_{k=1}^{K} \alpha_k - 1). \tag{40}$$

Its first derivative with respect to α_k becomes

$$\frac{\partial L(\boldsymbol{\alpha})}{\partial \alpha_k} = \frac{-A_k}{(\alpha_k + B_k)(\alpha_k + A_k + B_k)} + \lambda. \tag{41}$$

Let $\alpha_k^* \ \forall k \in \mathcal{K}$ be the optimal value that minimizes the objective function of **P1**. These values are also the roots of the polynomial functions where the equation (41) is equal to zero. Also, note that $\alpha_k^* \ \forall k \in \mathcal{K}$ is a nonnegative number, and their summation is equal to 1 due to the complementary slackness. Therefore,

$$\alpha_k^* = \left[\frac{\sqrt{A_k(A_k + 4/\lambda)} - A_k - 2B_k}{2}\right]^+ \tag{42}$$

where λ is chosen such that $\sum_{k=1}^{K} \alpha_k^* = 1$.

APPENDIX B
PROOF OF THEOREM 3

The players of the game described in **P3** are Alice and the attacker. In this game, the utility function of Alice is $R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$, and her strategy is to choose the optimal power allocation for the downlink transmissions. Similarly, $-R_{\text{sum}}(\mathbf{P}^{(d)}, \boldsymbol{\alpha})$ is the attacker's utility, and her strategy is to find the optimal $\boldsymbol{\alpha}$ to maximize this utility. The strategy sets of both players are non-empty, compact, and convex subsets of real numbers (the constraints in **P3** are linear functions). Furthermore, their utility functions are continuous and diagonally strictly concave. As a result, the existence and uniqueness of NE is proved for this game, and Gauss-Seidel method converges to this point [30].

APPENDIX C
PROOF OF EQUATION (26)

$$\lim_{M\to\infty} \frac{P_k^{(d)} |\mathbf{h}_J \mathbf{v}_k^T|^2}{M} = \lim_{M\to\infty} \frac{P_k^{(d)} |\frac{\mathbf{h}_J \hat{\mathbf{h}}_k^*}{M}|^2}{\frac{\|\hat{\mathbf{h}}_k\|^2}{M}} \tag{43}$$

Let us evaluate the limit of the numerator and denominator separately. The limit of the denominator is given by:

$$\lim_{M\to\infty} \frac{\|\hat{\mathbf{h}}_k\|^2}{M} = \theta_k + \alpha_k u_k \theta_J + \frac{1}{P_k L} \tag{44}$$

The equality is due to the fact that given a vector $\mathbf{x} \in \mathbb{C}^{1\times M}$ with a distribution $\mathcal{CN}(\mathbf{0}, c\mathbf{I})$, $\lim_{M\to\infty} \mathbf{x}\mathbf{x}^*/M = c$ [23, Lemma 1]. We analyze the limit of the numerator as follows:

$$\begin{aligned}\lim_{M\to\infty} \frac{\mathbf{h}_J \hat{\mathbf{h}}_k^*}{M} &= \lim_{M\to\infty} \frac{\mathbf{h}_J (\mathbf{h}_k + \sqrt{\alpha_k u_k}\mathbf{h}_J + \tilde{\mathbf{w}}_k)^*}{M} \\ &= \lim_{M\to\infty} \frac{\sqrt{\alpha_k u_k}\|\mathbf{h}_J\|^2}{M} = \sqrt{\alpha_k u_k}\theta_k. \end{aligned} \tag{45}$$

$\mathbf{g}_k$, $\mathbf{g}_J$, and $\tilde{\mathbf{w}}_k$ are independent vectors, and the result follows from [23, Lemma 1]. The expression in the numerator of (43) is a continuous function of $\mathbf{h}_J \hat{\mathbf{h}}_k^*/M$. Therefore, using the Continuous Mapping Theorem, we conclude that:

$$\lim_{M\to\infty} \frac{P_k^{(d)} |\mathbf{h}_J \mathbf{v}_k^T|^2}{M} = \frac{P_k^{(d)} \alpha_k u_k \theta_J^2}{\theta_k + \alpha_k u_k \theta_J + \frac{1}{P_k L}}. \tag{46}$$

It proves the equation (26).

ACKNOWLEDGMENT

Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF and QF.

REFERENCES

[1] E. Björnson, E. G. Larsson, and T. L. Marzetta, "Massive MIMO: Ten myths and one critical question," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 114–123, Feb. 2016.

[2] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[3] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct. 2014.

[4] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[5] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[6] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[7] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.

[8] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[9] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2658–2670, Jun. 2018.

[10] J. K. Tugnait, "On detection and mitigation of reused pilots in massive MIMO systems," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 688–699, Feb. 2018.

[11] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in *Proc. IEEE ICC Conf.*, London, U.K., Jun. 2015, pp. 1434–1440.

[12] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[13] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Müller, and R. F. Schaefer, "Optimal transmit antenna selection for massive MIMO wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 817–828, Apr. 2018.

[14] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin. (Mar. 2015). "Physical layer security in massive MIMO." [Online]. Available: https://arxiv.org/abs/1505.00396

[15] Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Han, "Secure transmission against pilot spoofing attack: A two-way training-based scheme," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1017–1026, May 2016.

[16] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO has unlimited capacity," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 574–590, Jan. 2018.

[17] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Pilot contamination attacks in massive MIMO systems," in *Proc. IEEE CNS Conf.*, Las Vegas, NV, USA, Oct. 2017, pp. 1–9.

[18] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, Jun. 2015.

[19] 3GPP, "NR and NG-RAN overall description," 3GPP, Sophia Antipolis, France, Tech. Rep. TR 38.300 v15.1.0, Mar. 2018.

[20] 3GPP, "Study on new radio access technology physical layer aspects," 3GPP, Sophia Antipolis, France, Tech. Rep. TR 38.802 v14.2.0, Sep. 2017.

[21] W. Zhang, F. Gao, S. Jin, and H. Lin, "Frequency synchronization for uplink massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 235–249, Jan. 2018.

[22] H. Minn, Q. Zhan, N. Al-Dhahir, and H. Huang, "In-phase and quadrature timing mismatch estimation and compensation in millimeter-wave communication systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4317–4331, Jul. 2017.

[23] F. Fernandes, A. Ashikhmin, and T. L. Marzetta, "Inter-cell interference in noncooperative TDD large scale antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 192–201, Feb. 2013.

[24] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[25] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, "Range-free localization and its impact on large scale sensor networks," *ACM Trans. Embedded Comput. Syst.*, vol. 4, no. 4, pp. 877–906, Nov. 2005.

[26] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: Challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Process. Mag.*, vol. 22, no. 4, pp. 24–40, Jul. 2005.

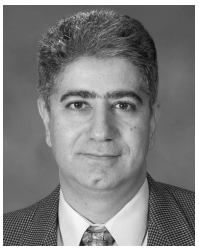
[27] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 956–968, Feb. 2017.

[28] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for broadcast channels with receiver side information," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4687–4708, Jul. 2017.

[29] V. S. Abhayawardhana, I. J. Wassell, D. Crosby, M. P. Sellars, and M. G. Brown, "Comparison of empirical propagation path loss models for fixed wireless access systems," in *Proc. IEEE VTC*, Stockholm, Sweden, May/Jun. 2005, pp. 73–77.

[30] R. Cominetti, F. Facchinei, and J. B. Lasserre, *Modern Optimization Modelling Techniques*. Basel, Switzerland: Springer, 2012.

Berk Akgun received the B.S. and M.S. degrees in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, in 2012 and 2014, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ, USA. From 2012 to 2014, he was a Software Design Engineer with the Communication and Information Technologies Division, Aselsan, Ankara. His current research interests lie in the areas of wireless communications and networking, with emphasis on secure multiuser multiple-input multiple-output (MIMO) systems (including massive MIMO, millimeter wave, LTE-A, and 802.11ac/ax).



Marwan Krunz (F'10) served as the UA Site Director for Connection One, an NSF IUCRC that focuses on wireless communication circuits and systems. In 2010, he was a Visiting Chair of Excellence at the University of Carlos III de Madrid. He held visiting research positions at UTS, INRIA-Sophia Antipolis, HP Labs, University of Paris VI, University of Paris V, University of Jordan, and US West Advanced Technologies. He is currently the Kenneth VonBehren Endowed Professor with the Electrical and Computer Engineering Department, The University of Arizona. He is also a Faculty Member of the University of Technology Sydney (UTS). He directs the Broadband Wireless Access and Applications Center, a multi-university industry-focused NSF center that includes affiliates from industry and government labs. He has authored over 270 journal articles and peer-reviewed conference papers. He is a Co-Inventor of several U.S. patents. His research interests lie in the areas of wireless communications and networking, with emphasis on resource management, adaptive protocols, and security issues. He was an Arizona Engineering Faculty Fellow from 2011 to 2014 and an IEEE Communications Society Distinguished Lecturer in 2013 and 2014. He was a recipient of the 2012 IEEE TCCC Outstanding Service Award and the NSF CAREER Award in 1998. He currently serves as the Editor-in-Chief for IEEE TRANSACTIONS ON MOBILE COMPUTING. He served on the editorial boards for IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKS, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TMC, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Computer Communications Journal*, and *IEEE Communications Interactive Magazine*. He was a General Vice-Chair of WiOpt 2016 and a General Co-Chair of WiSec'12. He was the TPC Chair of WCNC 2016 (Networking Track), INFOCOM'04, SECON'05, WoWMoM'06, and Hot Interconnects 9. He has served and continues to serve on the steering and advisory committees of numerous conferences and on the panels of several funding agencies. He was a keynote speaker, an invited panelist, and a tutorial presenter at numerous international conferences.

O. Ozan Koyluoglu received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2005, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2007 and 2010, respectively. From 2010 to 2011, he was with the Wireless Communication Theory Research Group, Nokia Bell Labs. From 2011 to 2013, he was a Post-Doctoral Fellow with The University of Texas at Austin. From 2013 to 2017, he was an Assistant Professor with the Department of Electrical and Computer Engineering, The University of Arizona. Since 2017, he has been with the University of California, Berkeley. His current research interests are in the areas of information theory, machine learning, distributed storage/computing, networks, and computational neuroscience.