

Received 25 October 2022, accepted 18 November 2022, date of publication 28 November 2022,  
date of current version 5 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3225452

## RESEARCH ARTICLE

# Attacker Detection in Massive MIMO Systems Over Spatially Uncorrelated Rician Fading Channels

GIANG QUYNH LE VU<sup>1</sup>, HUNG TRAN<sup>2</sup>, TRINH VAN CHIEN<sup>3</sup>, (Member, IEEE),  
LE NHAT THANG<sup>4</sup>, AND KIEN TRUNG TRUONG<sup>5</sup>, (Senior Member, IEEE)

<sup>1</sup>Faculty of Information Technology, National Academy of Education Management, Hanoi 100000, Vietnam

<sup>2</sup>Faculty of Computer Science, Phenikaa University, Hanoi 100000, Vietnam

<sup>3</sup>School of Information and Communication Technology (SoICT), Hanoi University of Science and Technology, Hanoi 100000, Vietnam

<sup>4</sup>Posts and Telecommunication Institute of Technology, Hanoi 100000, Vietnam

<sup>5</sup>Undergraduate Faculty, Fulbright University Vietnam, Ho Chi Minh City 700000, Vietnam


Corresponding author: Kien Trung Truong (kien.truong@fulbright.edu.vn)

**ABSTRACT** Physical layer security is a promising research direction for the fifth-generation and beyond networks. This paper investigates the physical layer security of massive multiple-input multiple-output (MIMO) systems over spatially-uncorrelated Rician fading channels in time-division duplex mode. In such systems, uplink training stage is required for the base station to estimate channel state information (CSI) for design downlink precoding matrices and for uplink data detection. Illegitimate users, or attackers, could intentionally send jamming signals during the training stage to degrade the quality of the CSI obtained at the base station, thus affecting the performance. In this paper, we propose a method for detecting the presence of an attacker. Based on the fundamental properties of Massive MIMO communication, the base station can treat the jamming signals as additive white Gaussian noise. A threshold to detect the existence of the attacker is, therefore, computed in closed-form expression with a sufficiently large number of antennas at the base station. The key merit of our proposed method is that it only requires statistical channel state information and two training time slots to detect the jamming activity. Numerical results show that our proposed attacker-detecting method is effective over various system parameter settings. Furthermore, the benefits of the dominant line-of-sight (LoS) components have been testified. In particular, the detection probability is improved by about 1.5 times with the presence of the LoS components, while the false-alarm probability gets improved by more than ten folds.

**INDEX TERMS** Massive MIMO, physical layer security, secrecy capacity, Rician fading, jammer/attacker detection, pilot contamination.

## I. INTRODUCTION

Massive multiple-input multiple-output (MIMO) has become one of the vital technologies in 5G networks [1], [2], [3], [4], [5], [6], [7]. The underlying idea of the technology is to equip the base station with a large number of antennas to provide extra degrees of freedom to simultaneously serve many users [1]. Theoretical results and practical implementation have proved that the massive MIMO technique has improved spectral efficiency, energy efficiency and transmission reliability of wireless networks significantly [8], [9], [10].

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Huo .

Nevertheless, due to the natural broadcast characteristics of wireless systems, illegitimate users could always be present and pose severe threats to the safe and secure communications between the base station and the legitimate user [11]. Such illegitimate users could perform two major types of attacking methods in wireless communications: passive attacks and proactive attacks [12]. In a passive attack, illegitimate users, often known as eavesdroppers, stay silent while overhearing the messages that legitimate users exchange with the base station. In a proactive attack, illegitimate users, often known as attackers or jammers, could generate jamming signals to contaminate the signals exchanged between the legitimate users and the base station, thus degrading their secure performance.

The study of the physical layer security under the deployment of massive MIMO technology has attracted many researchers to overcome the security threat in wireless networks [13], [14], [15], [16], [17], [18], [19]. Specifically, in [13], Zhu et al. have developed a method to protect the downlink transmission in a multicell massive MIMO system. The results illustrated that the protection of downlink transmission is possible by using matched-filter precoding and artificial noise (AN) generated at the base station. The achievable ergodic secrecy rate and the secrecy outage probability have been derived for these scenarios to examine the system performance. By considering the downlink transmission in a multi-cell massive MIMO system, four different data precoders, and three AN precoders have been studied when the number of antennas of the base station, mobile devices, and eavesdroppers are asymptotically large [14]. The ergodic capacity has been analyzed to examine the system performance. The results have illustrated that the proposed polynomial data and AN precoders closely approach the performance of selfish regularized channel inversion data and null-space-based AN precoders, respectively. Taking advantage of recent works, Wang et al. have provided an in-depth analysis of the AN-aided secure massive MIMO over i.i.d. Rician fading channel for massively distributed antennas [15]. The results revealed that as the number of transmit antennas increases to infinity, the secrecy outage in the Rician channels depends on the geometric locations of eavesdroppers.

Furthermore, in [16], the work has made an effort to improve security and optimize the power allocation under two secure constraints. The numerical results have reported that deploying several remote radio heads and autonomous power allocation can enhance the signal-to-interference-plus-noise ratio (SINR) significantly. Besides, in [17], Wu et al. studied the impact of large-scale multiple-antenna wiretap channel on the physical layer security problems. Results indicated two important results: 1) at the high signal-to-noise ratio (SNR) regime, a generalized singular value decomposition (GSVD) may show a severe performance loss for finite alphabet inputs. 2) a novel Per-Group-GSVD design has been proposed to effectively compensate the performance loss caused by the GSVD design.

For the attackers, in [20], Zhou et al. studied the attack strategies in the uplink training stage. These attacks directly influence the legitimate transmitter to alternate its precoder. By changing the precoding vectors, the network can enhance the received signal during the data transmission with the presence of an attacker. A new security attack has been discovered through the pilot contamination phenomenon. In [21], the authors studied a single-cell downlink massive MIMO system in the presence of an attacker with the jamming and eavesdropping capability. A novel beamforming strategy that establishes information-theoretic security without needing Wyner encoding has been proposed. In [22], Do et al. have proposed anti-jamming strategies to counter jamming attackers based on the pilot re-transmission. Numerical results

illustrated that the proposed strategies could improve the security performance significantly. Pilot reuse in the transmission is a matter of concern. In the future, we will study how to combine the method of detecting unauthorized device attacks with the reused pilot method for the channel model of the Rician fading channel. When so many devices are made from low cost components. Moreover, all practical implementations suffer from hardware impairments such as phase noise, quantization errors, amplification noises, and nonlinearities. These issues are of practice, which should be studied to evaluate and apply for the attacker detection. Because the advantage of our research method is that there is no need for knowledge channel information, it is also an advantage for systems under hardware impairments [23]. We stress that the previous works studied problems where the channels are subject to Rayleigh fading and users often have full channel state information. However, in practice, the channels contain the other features rather than the non-line-of-sight (NLoS) components only. Theoretically, the Rician fading channels are more general than the Rayleigh fading channels, because they include the LoS component [24], [25]. Nonetheless, a Rician channel model makes it difficult to analyze the secrecy capacity of the system [15], [26].

To the best of the authors' knowledge, this is the first investigation addressing the attack in the training stage over the Rician channels. In more detail, we focus on detecting the attacker's activity in a massive MIMO system with the prior information on the Rician fading channel coefficients. For the system analysis, we study the system model where the base station is equipped with many antennas and the attacks on the uplink training stage. The movement of the attacker affects the received signal direction. Let us suppose that when the attacker moves very close to the base station, it will affect the received signal and is more accessible than accepting the signal from the base station to decode. This can lead to two other problems: How can the network detect the attacker through energy leakage? How can the network evaluate the secrecy capacity with the presence of an attacker? In this paper, we assume that the intelligent attacker could choose the exact same location as the legitimate user. This means that the legitimate user and the attacker have the same distance to the base station and that they have the same angle of arrival (AoA) with regard to the bore-sight of the antenna array at the base station. This easily masquerades as a legitimate user.<sup>1</sup> Our main contributions are summarized as follows:

- We consider the physical layer security of massive MIMO systems with a possible presence of an attacker in the uplink training stage. The pilot contamination caused by the attacker is first analyzed for an arbitrary number of base station antennas. The effects of thermal noise and jamming attacks are then observed clearly as the number of base station antennas grow large.

<sup>1</sup>In the future, we should consider the impacts of the attacker mobility on the secure performance of the system.

- We propose a detection method to detect the attacker by pilot contamination without instantaneous channel state information. The detection process only needs two training symbols to detect the presence of the attacker.
- We analytically construct the detection region of the attacker. We further analyze the detection probability and the false-alarm probability. Our algorithm relies on only statistical channel state information.
- We propose a detection method to detect the attacker. Even when the AoAs are the same as each other, we still get a very high detection probability and low false alarm probability and can reach zero.

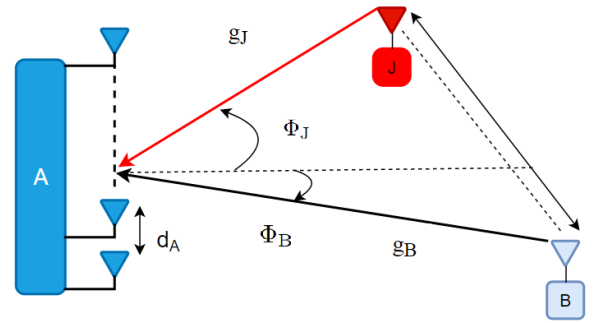
Numerical results disclose the detection performance of the proposed method over finite network dimensions. The numerical results also confirm the contributions of both the LoS and NLoS link to the detection and false-alarm probability. Parts of this paper were presented in [27]. This conference version, however, presented only the attacker detection method with pilot contamination in a radio frame. In contrast, this journal paper generalizes the attacker detection over one or more radio frames. Furthermore, the numerical results are extensively verified over both the Rician and Rayleigh fading channels to obtain insightful observations. Our study takes into account the impact of the AoA of the legitimate user and the attacker while estimating the detection probability and the false alarm probability.

The remaining of this paper is organized as follows. In Section II, we introduce our system model and the fading channel model. In Section III, we propose an attacker detection method. Numerical results are provided in Section IV. Finally, Section V concludes the paper and provides several topics for future work.

*Notation:* Lower letters are used for scalars. Upper and lower bold letters denote vectors and matrices, respectively. The  $(i, j)$ -the element of matrix  $\mathbf{A}$  is denoted as  $[\mathbf{A}]_{i,j}$ .  $\mathbf{I}_M$  is the identity matrix of size  $M \times M$ . The superscripts  $(\cdot)^T$  and  $(\cdot)^H$  represents regular and Hermitian transpose, respectively. The mean value of a random variable denotes as  $\mathbb{E}[\cdot]$ . The notation  $\xrightarrow{d}$  indicates the convergence in distribution. Finally,  $\mathcal{CN}(\cdot, \cdot)$  represents a circularly symmetric Gaussian distribution and  $\mathcal{N}(\cdot, \cdot)$  denotes a normal distribution.

## II. SYSTEM MODEL

We consider a single-cell massive MIMO system as illustrated in Fig. 1 where a base station A communicates with a legitimate user B under the presence of an attacker J. The base station is equipped with  $M$  antennas, while the legitimate user and the attacker are equipped with a single antenna. For convenience, let us define  $\mathcal{X} = \{B, J\}$ . We assume that the transmissions between the legitimate user and the base station are perfectly synchronized. Accordingly, the base station knows the positions of the training symbols in the uplink transmission. We denote  $\mathcal{K}_k$  as the index set of the training symbols in radio frame  $k$ . Let  $\mathcal{S}$  be the set of all possible training signals for uplink training. Similar to [12], we assume that  $\mathcal{S}$  is an  $N$ -PSK (phase-shift keying) alphabet



**FIGURE 1.** An illustration of the considered system model, where the single-antenna attacker J attacks the communication between the base station A, which is equipped with a large number of antennas, and the single-antenna legitimate user B.

with the set of  $N$  possible training signals defined as  $\mathcal{S} = \{e^{j2\pi m/N} : m \in \mathbb{Z}, 0 \leq m \leq N - 1\}$ . In the training symbol  $\ell \in \mathcal{K}_k$ , we assume that the legitimate user can transmit a random training signal  $s_{B,k,\ell} \in \mathcal{S}$  in order to make it unpredictable by the attacker. For most standardized wireless applications, the training signal set  $\mathcal{S}$  used by legitimate users is often explicitly specified in the technical specifications. Thus, it could be reasonably assumed that the attacker also has prior knowledge of  $\mathcal{S}$ . Nevertheless, it could not figure out exactly which training signal is sent by the legitimate user in a training symbol. One effective strategy that the attacker could apply is to transmit a random training signal selected from  $\mathcal{S}$ , denoted as  $s_{J,k,\ell} \in \mathcal{S}$ , to contaminate the uplink training transmission, hence reducing the accuracy of channel state information obtained at the base station. We can reformulate

$$s_{J,k,\ell} \stackrel{(a)}{=} s_{J,k,\ell} s_{B,k,\ell}^* s_{B,k,\ell} = s_{k,\ell} s_{B,k,\ell}, \quad (1)$$

where  $s_{k,\ell} = s_{J,k,\ell} s_{B,k,\ell}^* \in \mathcal{S}$  and  $s_{J,k,\ell}, s_{B,k,\ell} \in \mathcal{S}$ . In (1), (a) is obtained since  $|s_{B,k,\ell}|^2 = 1$ .

We introduce  $\alpha_{k,\ell}$  as the contaminating indicator parameter where  $\alpha_{k,\ell} = 1$  if the illegitimate user transmits a training signal in training symbol  $\ell \in \mathcal{K}_k$ , and  $\alpha_{k,\ell} = 0$  otherwise. In other words, pilot contamination occurs in training symbol  $\ell \in \mathcal{K}_k$  if and only if  $\alpha_{k,\ell} = 1$ . Let us denote  $p_X$  as the transmit power of user  $X \in \mathcal{X}$  during the uplink training stage. In this paper, we assume that  $p_X$  remains constant over many radio frames  $\mathcal{F}$ . Let us also denote  $\mathbf{n}_{k,\ell} \in \mathbb{C}^{M \times 1}$  as additive white Gaussian noise (AWGN) at the base station, which is distributed as  $\mathbf{n}_{k,\ell} \sim \mathcal{CN}(\mathbf{0}_{M \times 1}, \sigma^2 \mathbf{I}_M)$ , where  $\sigma^2$  as the variance of noise. The received training signal at the base station corresponding to training symbol  $\ell \in \mathcal{K}_k$ , denoted by  $\mathbf{y}_{k,\ell} \in \mathbb{C}^{M \times 1}$  is given as

$$\mathbf{y}_{k,\ell} = \sqrt{p_B} \mathbf{h}_{B,k} s_{B,k,\ell} + \alpha_{k,\ell} \sqrt{p_J} \mathbf{h}_{J,k} s_{J,k,\ell} + \mathbf{n}_{k,\ell}. \quad (2)$$

Let us denote the equivalent uplink channel coefficient vector as  $\mathbf{f}_{k,\ell} \in \mathbb{C}^{M \times 1}$ , which is given by

$$\mathbf{f}_{k,\ell} = \sqrt{p_B} \mathbf{h}_{B,k} + \alpha_{k,\ell} \sqrt{p_J} \mathbf{h}_{J,k} s_{k,\ell}. \quad (3)$$

Using (1), we could rewrite the received training signal  $\mathbf{y}_{k,\ell}$  in (2) as follows

$$\mathbf{y}_{k,\ell} = \mathbf{f}_{k,\ell} s_{B,k,\ell} + \mathbf{n}_{k,\ell}. \quad (4)$$

We assume that the locations of the base station and the users do not change over many radio frames. For analytical tractability, we assume that the antenna elements of base station A collectively form a uniformly-linear array (ULA). For such, we denote  $\bar{d}_A = \pi d_A/\lambda$  the normalized distance between adjacent antennas at the base station, where  $d_A$  is the distance between the adjacent antenna elements at the base station and  $\lambda$  is the wavelength corresponding to the carrier frequency. Furthermore, we denote  $d_X, \forall X \in \mathcal{X}$ , as the distance from the base station to user X. We also denote  $\Phi_X \in [-\pi, \pi], \forall X \in \mathcal{X}$ , as the angle between the line connecting the base station to user X and the bore-sight of the base station's antenna array. We believe this system model provides an initial mechanism for analytical tractability to obtain valuable insights. More complicated models, such as those with a large number of user terminals and/or with multiple-antenna users are left for future work. Under the ULA assumption at the base station, the array response  $\mathbf{g}_X \in \mathbb{C}^{M \times 1}$  of the channel vector  $\mathbf{h}_{X,k}$  is independent of radio frame  $k$  and is computed as

$$\mathbf{g}_X = \left[ 1, e^{j2\bar{d}_A \sin \Phi_X}, \dots, e^{j2\bar{d}_A(M-1) \sin \Phi_X} \right]^T. \quad (5)$$

By exploiting the fundamentals of massive MIMO antenna array [28], we obtain  $\mathbf{g}_X^H \mathbf{g}_X = M, \forall X \in \mathcal{X}$  and

$$\begin{aligned} \mathbf{g}_J^H \mathbf{g}_B &= \psi(\Phi_B, \Phi_J, M) \\ &= \frac{\sin(M\bar{d}_A(\sin \Phi_B - \sin \Phi_J))}{\sin(\bar{d}_A(\sin \Phi_B - \sin \Phi_J))} e^{j(M-1)\bar{d}_A(\sin \Phi_B - \sin \Phi_J)}. \end{aligned} \quad (6)$$

We can analytically observe the behavior of  $\psi(\Phi_B, \Phi_J)$  at the limiting regime, i.e.,  $M \rightarrow \infty$  as follows

$$\lim_{M \rightarrow \infty} \frac{|\psi(\Phi_B, \Phi_J, M)|}{M} = \begin{cases} 1, & \text{if } \sin \Phi_B = \sin \Phi_J, \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

In this paper, we assume spatially-uncorrelated Rician fading channels [26]. We denote  $\kappa_X$  as the Rician coefficient and  $\beta_X$  as the large-scale fading coefficient of  $\mathbf{h}_X$ . In general,  $\kappa_X$  and  $\beta_X$  remain constant in many radio frames. In other words, they are independent of the radio frame index. To initially gain insights, we assume that  $\kappa_X$  and  $\beta_X$  are known perfectly. Define the large-scale fading coefficients corresponding to the LoS part and the NLoS part of  $\mathbf{h}_{X,k}$  as

$$\beta_{X,L} = \frac{\kappa_X}{\kappa_X + 1} \beta_X; \quad \beta_{X,N} = \frac{1}{\kappa_X + 1} \beta_X. \quad (9)$$

The instantaneous channel coefficient vector  $\mathbf{h}_{X,k}$  can be decomposed in to the LoS and NLoS components as follows

$$\mathbf{h}_{X,k} = \beta_{X,L}^{1/2} \mathbf{g}_X + \beta_{X,N}^{1/2} \mathbf{w}_{X,k} \quad (10)$$

where  $\beta_{X,L}^{1/2} \mathbf{g}_X \in \mathbb{C}^{M \times 1}$  is the LoS component and  $\beta_{X,N}^{1/2} \mathbf{w}_{X,k} \in \mathbb{C}^{M \times 1}$  with  $\mathbf{w}_X \sim \mathcal{CN}(\mathbf{0}_{M \times 1}, \mathbf{I}_M)$  being the NLoS component. We emphasize that the Rayleigh fading model considered in much prior work is a special case of our model since it is only related to the NLoS component in the spatially-uncorrelated Rician fading channel model,

i.e.  $\kappa_X = 0$  and hence  $\beta_{X,L} = 0$  and  $\beta_{X,N} = \beta_X$  for all  $X \in \mathcal{X}$ . For notation convenience and comparison purpose, let us denote the following two subscripts  $(\cdot)_{\text{Ri}}$  and  $(\cdot)_{\text{Ra}}$  indicate the parameters regarding the Rician and Rayleigh fading channel model, respectively.

### III. PROPOSED ATTACKER DETECTION METHOD

In this section, we propose a new attacker detection method that takes into account the special characteristics of the spatially-uncorrelated Rician channel model. We first present how the detection regions are constructed and the detection algorithm. We then show that the proposed detection method is likely to take advantage of the features of this Rician channel model to provide a higher detection probability than much prior work considering the Rayleigh channel model. Similarly, let  $(\cdot)_J$  and  $(\cdot)_0$  indicate the parameters when the attacker transmits jamming signals and those when it does not transmit jamming signals, respectively.

#### A. PROPOSED METRIC

To avoid being detected as much as possible, the attacker may choose to transmit jamming signals randomly in time. Thus, to increase the detection probability, we propose a new scalar-valued metric that is defined as a scaled inner product of the received signal in training symbol  $l \in \mathcal{K}_k$  in radio frame  $k$  and that in training symbol  $u \in \mathcal{K}_q$  in radio frame  $q$  as follows:

$$z_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}_{k,l}^H \mathbf{y}_{q,u}. \quad (11)$$

Although the expression in (11) is seemingly the same as what was suggested in [29] for the Rayleigh fading channel model, our proposed metric is of significant extension since it does not require that the two training symbols be in the same radio frame or in two consecutive frames.

We first define  $s_B = s_{B,q,u}^* s_{B,k,\ell}$ , then  $s_B$  is a  $N$ -PSK symbol because both  $s_{B,q,u}^*$  and  $s_{B,k,\ell}$  are  $N$ -PSK symbols. For notation convenience, we define new variables as follows

$$a_{k,q} = \frac{1}{\sqrt{M}} \mathbf{f}_{q,u}^H \mathbf{f}_{k,\ell} \quad (12)$$

$$n_{k,q} = \frac{1}{\sqrt{M}} \left( \mathbf{f}_{q,u}^H \mathbf{n}_{k,\ell} + \mathbf{n}_{q,u}^H \mathbf{f}_{k,\ell} + \mathbf{n}_{q,u}^H \mathbf{n}_{k,\ell} \right). \quad (13)$$

By substituting (4) into (11) and using the new variables in (12) and (13), we obtain

$$z_{k,q} = a_{k,q} s_B + n_{k,q}. \quad (14)$$

Note that (14) can be treated as the input-output relationship of a single input single output (SISO) channel where  $s_B$  is the transmitted  $N$ -PSK symbol,  $a_{k,q}$  is the equivalent complex channel coefficient and  $n_{k,q}$  is equivalent noise.

Since it is very challenging to determine the exact distribution of  $n_{k,q}$ , we adopt the same approach as [29] in which we study its statistical property when  $M$  is sufficiently large. For a given realization of the channel vectors and the transmitted pilot symbols, both  $\mathbf{f}_{q,u}$  and  $\mathbf{f}_{k,\ell}$  are well defined.



Based on (11)–(14), one observes that

$$n_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}_{k,\ell}^H \mathbf{y}_{q,u} - a_{k,q} s_{\text{B}}, \quad (15)$$

where  $\mathbf{y}_{k,\ell}$  and  $\mathbf{y}_{q,u}$  are two independent Gaussian vectors of size  $M$  with the same variance  $\sigma^2 \mathbf{I}_M$ , while its means are  $\mathbf{f}_{k,\ell} s_{\text{B},k,\ell}$  and  $\mathbf{f}_{q,u} s_{\text{B},q,u}$ , respectively. It follows that  $\mathbf{E}[n_{k,q}] = 0$ . Since  $n_{k,q}$  is a sum of  $M$  complex-valued normal product Gaussian variables, we obtain the following result by applying the Lyapunov central limit theorem

$$\lim_{M \rightarrow \infty} \frac{n_{k,q}}{\sigma_M} \xrightarrow{d} \mathcal{CN}(0, 1). \quad (16)$$

where the variance  $\sigma_M^2$  is defined as below and will be proved later to be finite when  $M$  grows very large

$$\sigma_M^2 = \frac{\sigma^2}{M} (\|\mathbf{f}_{q,u}\|^2 + \|\mathbf{f}_{k,\ell}\|^2 + M\sigma^2). \quad (17)$$

In other words, when  $M$  grows large,  $n_{k,q}/\sigma_M$  converges to a complex-valued Gaussian random variable with mean 0 and variance  $\sigma_M^2$ . Numerical results in [29] showed that this approximation is relatively tight even for a small number of antennas at the base station, e.g.,  $M = 5$ . In general, the effective noise variance  $\sigma_M^2$  depends on a number of factors, including the presence of jamming signals, the channel model, and the positions of the two training symbols.

### B. ANALYSIS IN THE PRESENCE OF JAMMING SIGNALS

As jamming signals exist in both training symbols, i.e.  $\alpha_{k,\ell} = \alpha_{q,u} = 1$ , replacing these values into (17) leads to the following result:

$$\sigma_{\text{Ri},J,M}^2 = \frac{\sigma^2}{M} \left( \|\sqrt{p_{\text{B}}}\mathbf{h}_{\text{B},k} + \sqrt{p_{\text{J}}}\mathbf{h}_{\text{J},k} s_{k,\ell}\|^2 + \|\sqrt{p_{\text{B}}}\mathbf{h}_{\text{B},q} + \sqrt{p_{\text{J}}}\mathbf{h}_{\text{J},q} s_{q,u}\|^2 + M\sigma^2 \right). \quad (18)$$

We note that  $\sigma_{\text{Ri},J,M}^2$  in (18) is aligned with  $\sigma_M^2$  in (17), but the subscript  $(\text{Ri},J)$  indicates that we consider the Rician channel model and that the communication system suffers from the jamming attack. Since the expression of (18) contains the instantaneous channel coefficient vectors, it is nontrivial to observe the properties. Nonetheless, the insights are gained at the limiting regime. Specifically, as  $M$  grows large, i.e.,  $M \rightarrow \infty$ , we can compute its limiting value as follows

$$\begin{aligned} \bar{\sigma}_{\text{Ri},J}^2 &= \lim_{M \rightarrow \infty} \sigma_{\text{Ri},J,M}^2 \\ &= \sigma^2 \left( 2\bar{\beta}_{\text{B},k,k} + 2\bar{\beta}_{\text{J},k,k} + \sigma^2 \right. \\ &\quad \left. + 2\sqrt{\bar{\beta}_{\text{B},k,k}\bar{\beta}_{\text{J},k,k}} \psi(\Phi_{\text{B}}, \Phi_{\text{J}}) \text{Re}\{s_{k,\ell} + s_{q,u}\} \right), \quad (19) \end{aligned}$$

which is bounded from above thanks to the law of conservation of energy and a finite transmit power level. In (19), we define for all  $X \in \mathcal{X}$  as follows

$$\bar{\beta}_{X,k,q} = \begin{cases} p_X \beta_X, & \text{if } k = q, \\ p_X \beta_{X,L}, & \text{otherwise.} \end{cases} \quad (20)$$

Consequently, the equivalent channel coefficient is given as

$$\begin{aligned} a_{\text{Ri},J,k,q} &= \frac{1}{\sqrt{M}} (\sqrt{p_{\text{B}}}\mathbf{h}_{\text{B},q} + \sqrt{p_{\text{J}}}\mathbf{h}_{\text{J},q} s_{q,u})^H \\ &\quad \times (\sqrt{p_{\text{B}}}\mathbf{h}_{\text{B},k} + \sqrt{p_{\text{J}}}\mathbf{h}_{\text{J},k} s_{k,\ell}), \quad (21) \end{aligned}$$

which depends on whether or not the two training symbols are in the same radio frame. It also depends on if the training signals guessed by the attacker can match with those transmitted by B, i.e.,  $s_{q,u} = s_{k,\ell}$ . Let us define

$$\begin{aligned} \bar{a}_{\text{Ri},J,k,q} &= \lim_{M \rightarrow \infty} \frac{a_{\text{Ri},J,k,q}}{\sqrt{M}} \\ &= \bar{\beta}_{\text{B},k,q} + \bar{\beta}_{\text{J},k,q} s_{q,u}^* s_{k,\ell} \\ &\quad + \sqrt{\bar{\beta}_{\text{B},k,q}\bar{\beta}_{\text{J},k,q}} \psi(\Phi_{\text{B}}, \Phi_{\text{J}}) (s_{q,u}^* + s_{k,\ell}). \quad (22) \end{aligned}$$

Note that as  $s_{q,u} = s_{k,\ell}$ , which happens with the probability of  $1/N$ ,  $\bar{a}_{\text{Ri},J,k,q}$  is a real scalar regardless of the comparison of  $k$  and  $q$ . In this case, it has an overwhelming probability that the contaminated metric  $z_{k,q}$  is located within the circle of radius  $\bar{\sigma}_{\text{Ri},J}$  and centered at an  $N$ -PSK symbol scaled by  $\bar{a}_{\text{Ri},J,k,q}$ . In contrast, as  $s_{q,u} \neq s_{k,\ell}$ , appearing with the probability of  $(N-1)/N$ , then  $\bar{a}_{\text{Ri},J,k,q}$  is a complex scalar. It results in the contaminated metric  $z_{k,q}$  located within the circle of radius  $\bar{\sigma}_{\text{Ri},J}$  and centered at an  $N$ -PSK symbol scaled by  $|\bar{a}_{\text{Ri},J,k,q}|$  and rotated by a certain angle.

### C. ANALYSIS WITHOUT THE PRESENCE OF JAMMING SIGNALS

For completeness, we consider the case without an attack. When the attacker does not transmit signals in both the training symbols, we have  $\alpha_{k,\ell} = \alpha_{q,u} = 0$ . Let us denote  $\sigma_{0,M}^2$  the corresponding value of  $\sigma_M^2$ . By substituting  $\alpha_{k,\ell} = \alpha_{q,u} = 0$  into (17) and (12), we obtain

$$a_{\text{Ri},0,k,q} = \frac{1}{\sqrt{M}} \mathbf{h}_{\text{B},q}^H \mathbf{h}_{\text{B},k}, \quad (23)$$

$$\sigma_{\text{Ri},0,M}^2 = \frac{N_0}{M} \left( p_{\text{B}} \|\mathbf{h}_{\text{B},k}\|^2 + p_{\text{B}} \|\mathbf{h}_{\text{B},q}\|^2 + M\sigma^2 \right). \quad (24)$$

By using the properties of the Rician channel model provided in Section II and after performing some manipulations, we obtain the following asymptotic results

$$\bar{a}_{\text{Ri},0,k,q} = \lim_{M \rightarrow \infty} \frac{|a_{\text{Ri},0,k,q}|}{\sqrt{M}} = \bar{\beta}_{\text{B},k,q} \quad (25)$$

$$\bar{\sigma}_{\text{Ri},0}^2 = \lim_{M \rightarrow \infty} \sigma_{\text{Ri},0,M}^2 = N_0 \left( 2\bar{\beta}_{\text{B},k,k} + \sigma^2 \right). \quad (26)$$

While both the obtained results are bounded as  $M \rightarrow \infty$ , they indeed disclose a distinction. In particular,  $\bar{a}_{\text{Ri},0,k,q}$  is a function of the positions of the training symbols, but  $\bar{\sigma}_{\text{Ri},0}^2$  is not.

### D. PROPOSED METHOD

We recall that  $z_{k,q}$  can be treated as the equivalent received signal of the SISO channel with the input-output relationship given in (27). We now construct the detection region based

on the scalar metric  $z_{k,q}$  so that the base station could decide whether an attacker is contaminating the desired training symbols or not. Note that  $z_{k,q}$  is the sum of a  $N$ -PSK symbol scaled by  $a_{\text{Ri},0,k,q}$  and Gaussian noise with mean 0 and variance  $\sigma_{\text{Ri},0,M}^2$ . In general, the base station has not obtained accurate information of small-scale fading coefficients before the training periods. This means that it hasn't known exactly  $a_{\text{Ri},0,k,q}$  and  $\sigma_{\text{Ri},0,M}^2$  before making the decision on the presence of jamming signals. Nevertheless, as both the legitimate user and the attacker do not move in a long enough period, it is justifiable to assume that the base station could accurately estimate the large-scale fading coefficients  $\beta_B$  and  $\beta_{B,L}$ . Thus, for a given  $N$ -PSK modulation scheme and for a large-enough number of antennas  $M$ , we propose the detection regions as the circles of radius  $\bar{\sigma}_{\text{Ri},0}$  with the centers at the scaled  $N$ -PSK symbols with the common scaling factor of  $\sqrt{M}\bar{a}_{\text{Ri},0,k,q}$ . In order to reduce the effects of noise on detection accuracy, we also propose that  $K$ , where  $K \geq 2$ ,  $N$ -PSK training symbols are used for attacker detection purpose. Based on these detection regions and the use of  $K$  training symbols, we propose the following detection method:

- *Step 1:* The base station selects a set of  $K$  training symbols from one or more consecutive radio frames. The base station then forms a number of pairs of training symbols from the selected set. Note that the maximum number of pairs of training symbols is  $K(K - 1)/2$ .
- *Step 2:* For each formed pair of training symbols, for example, training symbol  $\ell$  in radio frame  $k$  and training symbol  $u$  in radio frame  $q$ , i.e.  $\ell \in \mathcal{K}_k$  and  $u \in \mathcal{K}_q$ , the base station performs the following steps:
  - 2.1. Compute the scalar-valued metric  $z_{k,q}$ .
  - 2.2. Compute  $d_m = |z_{k,q} - \sqrt{M}\bar{a}_{\text{Ri},0,k,q}e^{jm2\pi/N}|$  for each  $m \in 0, 1, \dots, N - 1$ . Note that  $d_m$  can be considered as the distance from the scalar-valued equivalent received signal to the  $m$ -th scaled  $N$ -PSK symbol.
  - 2.3. Compute the minimum distance, which is defined as  $d_{\min} = \min_{0 \leq m \leq (N-1)} d_m$ .
  - 2.4. If  $d_{\min} < \bar{\sigma}_{\text{Ri},0}$  then the base station decides that the training symbols are not contaminated; otherwise, it decides that they are contaminated, i.e., there exists an attacker.
- *Step 3:* Based on the majority of the detection results of the formed pairings, the base station determines the presence of the jamming signals.
- *Step 4:* The base station makes the decision on the presence of an attacker over the duration of the selected radio frames based largely on the results of attacker detection corresponding to the formed pairs.

We emphasize that the larger the number of formed pairs is, the more accurate the attacker detection decision is. The benefits, however, come at the cost of more overhead and more computational complexity. Note also that the use of more pairs of training symbols to take advantage of temporal diversity is one of the main differences between this paper in

relative comparison with prior work, including our own prior work [27].

### E. ASYMPTOTICAL ANALYSIS OF DETECTION PROBABILITY

In this section, we analyze the detection probability of the proposed method when the number of antennas  $M$  at the base station grows very large to obtain insights on the impacts of the channel model. Dividing both sides of (27) by  $a_{k,q}$ , which is non-zero, we get the following processed metric

$$\tilde{z}_{k,q} = s_B + \frac{n_{k,q}}{a_{k,q}}. \tag{27}$$

The radius of each proposed detection region is proportional to  $D_{\text{Ri},0,k,q} = \sigma_{\text{Ri},0,k,q}^2/|a_{\text{Ri},0,k,q}|^2$ . In addition, the radius of the circle, where the metric  $z_{k,q}$  appears with a high probability under the attacker, is proportional to  $D_{\text{Ri},J,k,q} = \sigma_{\text{Ri},J,k,q}^2/|a_{\text{Ri},J,k,q}|^2$ . In principle, the detection probability is close to zero when  $D_{\text{Ri},J,k,q} \leq D_{\text{Ri},0,k,q}$  and it increases with the ratio of  $D_{\text{Ri},J,k,q}/D_{\text{Ri},0,k,q}$  when  $D_{\text{Ri},J,k,q} > D_{\text{Ri},0,k,q}$ . Subsequently,  $D_{\text{Ri},J,k,q}/D_{\text{Ri},0,k,q}$  should be as large as possible. Notably, we can show  $D_{\text{Ri},J,k,q}/D_{\text{Ri},0,k,q} = D_{\text{Ri},J,k,k}/D_{\text{Ri},0,k,k}$  for all  $q$ . This means that the performance of the proposed approach allows the flexibility of checking the existence of jamming signals frequently.

### IV. NUMERICAL RESULTS

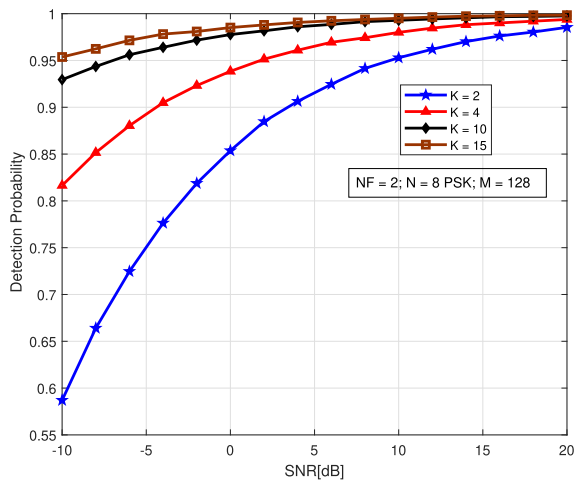
We perform the simulations based on the detection probability and the false-alarm probability to evaluate the performance of our detection method. The false-alarm probability is defined as the probability of detecting an attacker, given that this attacker is not present. We consider a system in which the base station is located at the center of the coverage area. The legitimated user and the attacker are randomly located. We assume that the effect of shadowing fading is ignored, so the large-scale fading coefficients are defined, similar to [30], [31], and [32], as follows

$$\beta_{X,Y} = -32.4 - 10n_Y \log_{10}(d_{3D,X}) - 20 \log_{10}(f_c).$$

where  $X \in \mathcal{X}$ ,  $Y \in \mathcal{Y} = \{L, N\}$ ,  $d_{3D,X}$  is the distance in meters from the base station to the user  $X$  in 3-D space, the carrier frequency  $f_c$  is set as  $f_c = 3.5$  GHz. Moreover,  $n_Y$  is the path-loss exponent. Moreover, the distance  $d_{3D,X}$  is given by

$$d_{3D,X} = \sqrt{d_{2D,X}^2 + (h_A - h_X)^2}, \tag{28}$$

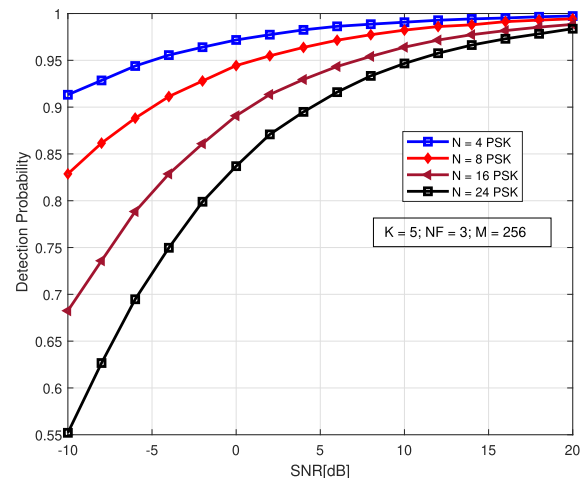
where  $d_{2D,X}$  is the distance from the base station to the user  $X$  in the 2-D space,  $h_A$  is the height of the base station  $A$ , and  $h_X$  is the height of the user  $X$  [30]. In the considered model, we suppose  $h_A = 10\text{m}$  and  $h_B = h_J = 1.5$  m. The paper investigates the urban cell environment (UMa: Urban Macro), then  $n_Y = 2$  for LOS and  $n_Y = 2.9$  for NLOS [31], [32]. Following [30], for the UMa environment,  $\kappa$  measured in dB is a normal random variable  $\mathcal{N}(9, 3.5)$ . For simplicity, we assume  $\kappa_B = \kappa_J = 9$  dB. The system works at bandwidth 10 MHz and the transmit power of the base station



**FIGURE 2.** Detection probability vs. SNR for the numbers of training symbols are 2, 4, 10, 15, the number of radio frames is 2, PSK number  $N = 8$ , the number of base station antennas  $M = 128$ ,  $P_B = 24$  dBm,  $P_J = 24$  dBm and  $\Phi_B = 0$  rad và  $\Phi_J = 0.1$  rad.

is  $p_d = 46$  dBm. The distance between adjacent antennas at the base station is half wavelength, that is  $d_A = 0.5$ . The noise density at the base station is 9 dB/Hz, while the noise density at the users B and J is 5 dB/Hz. We suppose  $\Phi_B = 0$  rad. We consider a simulation scenario where the attacker is close to the legitimate user with the parameter settings. First, the distance from either the legitimate user or the attacker to the base station is 300m. Second, the Rician factors are  $\kappa_B = \kappa_J = 9$  dB. Finally, numerical results are averaged over 200000 samples with the different number of training symbols  $K$  and the number of radio frames.

The SNR is defined as  $\text{SNR} = P_B/N_0$  dB. Fig 2 shows the detection probability value for different values of SNR when the base station is equipped with 128 antennas. The transmit powers are  $p_B = p_J = 24$  dBm. We consider different numbers of pilot signals  $K \in [2, 4, 10, 15]$ . The simulated modulation scheme is 8-PSK. As expected, the detection probability increases with the SNR value; in the high SNR regime, the detection probability approaches one. Notably, the larger the number of pilot signals, the larger the detection probability. Even with a low SNR = -10 dB and a number of training symbols  $K = 2$ , the detection probability is around 58%. When increasing the number of training symbols to  $K = 4$ , the detection probability increases greatly to 88% and gradually approaches 1 at a high SNR. If the number of pilot signals exceeds  $K = 10$ , the probability of detecting the attack is very high. It exceeds 93% and reaches almost one. Once the system exploits a sufficiently large number of pilot signals, the difficulty is increased for the attacker to collect channel information, simulate pilot training of licensed users and attack labor. Then the base station can easily detect the attacking device. The results show that in Massive MIMO communications with the Rician fading channels, the network can exploit a large number of antennas and an appropriate number of pilot symbols to successfully detect the illegitimate user with an overwhelming probability.

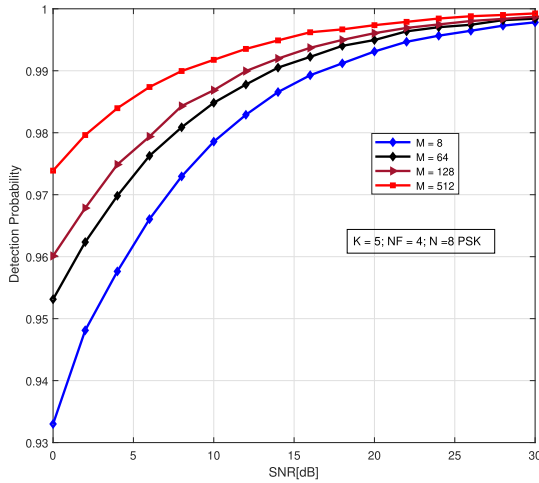


**FIGURE 3.** Detection probability vs. SNR for the number of training symbols is  $K = 5$ , the number of radio frames is 3, the number of base station antennas  $M = 256$ ,  $P_B = 24$  dBm,  $P_J = 24$  dBm and  $\Phi_B = 0$  rad and  $\Phi_J = 0.1$  rad.

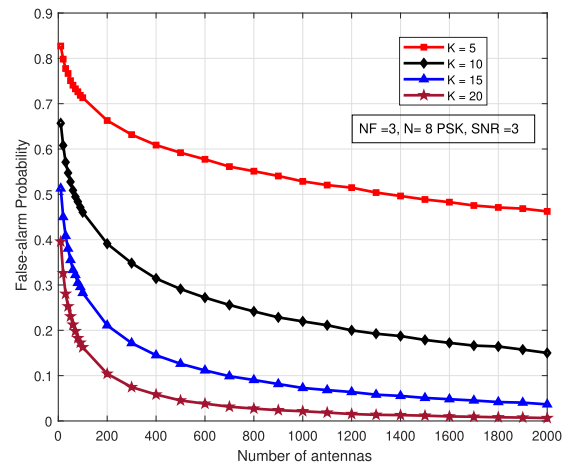
Fig 3 presents the detection probability as the function of SNR value in a scenario with 256 antennas at the base station. The transmit power values are  $p_B = p_J = 24$  dBm. The considered modulation levels are  $N = [4, 8, 16, 24]$ -PSK. Note that the detection probability increases with the SNR value and that in it is almost one in the high SNR regime. In addition, the detection probability decreases dramatically as the number of constellation points increases. For example, at the SNR value equal to 0 dB, the network using the 4-PSK modulation offers the detection probability of about 0.97. Nevertheless, the detection probability is only about 0.84 if the 24-PSK is used. A large number of constellation points have slower convergence rate. This issue can be improved by increasing the number of BS antennas or the SNR. The observation demonstrates the challenges to detect the attacker when a large number of constellation points is utilized.

Fig. 4 shows the detection probability vs. the different SNR values of our system for  $N = 8$  PSK and a different number of antennas at the BS. The detection probability increases with the SNR value. Although the detection probability has improved by roughly 0.93 with a few antennas at the BS and by utilizing the pilot training overhead  $K = 5$  in 4 frames only. When the BS is equipped with many antennas, e.g., with  $M = 128$  the detection probability can reach up to 0.96. According to the trend, the detection probability can be close to one when there are a sufficiently large number of antennas at the BS. Alternatively, the higher number of BS antennas offer better detection probability thanks to channel hardening and favorable propagation [33].

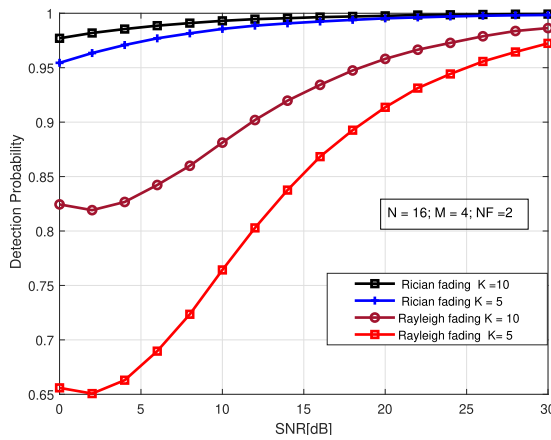
Meanwhile, Fig. 5 compares the detection probability between the Rayleigh and Rician fading channels as a function of the SNR with  $M = 4$ ,  $K \in [5, 10]$ , the number of radio frames is 2,  $N = 16$ ,  $p_B = 24$  dBm,  $p_J = 24$  dBm,  $\Phi_B = 0.1$  rad, and  $\Phi_J = 0.1$  rad. With  $K = 5$ , for a system over the Rayleigh fading channel model, the detection probability is lower bounded by 65% in the considered parameter settings



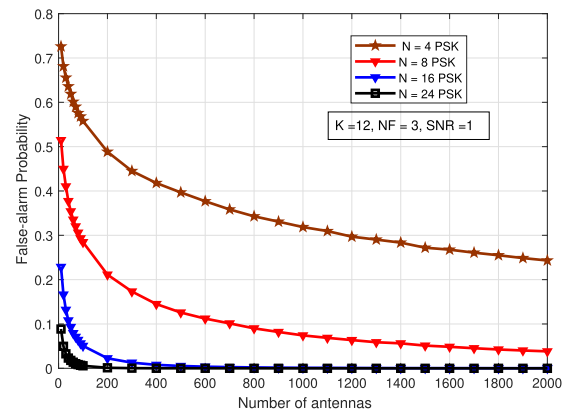
**FIGURE 4.** Detection probability vs. the SNR for the number of training symbols  $K = 5$ , the number of radio frames is 4, the PSK number  $N = 8$  PSK,  $P_B = 1$ ,  $P_J = 1$  and  $\Phi_B = 0$  rad, and  $\Phi_J = 0.1$  rad.



**FIGURE 6.** False-alarm probability vs. number of antennas  $M$  for the numbers of training symbols are  $[5, 10, 15, 20]$ ,  $SNR = 3$  dB, the number of radio frames is 3, PSK modulation level is  $N = 8$ ,  $\Phi_J = 0$  rad,  $\Phi_B = 0.1$  rad.



**FIGURE 5.** Detection probability of the Rayleigh fading and Rician fading channels vs. the SNR with the number of antennas  $M = 4$ , the number of training symbols  $K = [5, 10]$ , the number of radio frames is 2, PSK modulation level  $N = 16$ ,  $P_B = 24$  dBm,  $P_J = 24$  dBm and  $\Phi_B = 0.1$  rad and  $\Phi_J = 0.1$  rad.



**FIGURE 7.** False-alarm probability vs. the number of antennas for PSK modulation level are  $[4, 8, 16, 24]$ , number of training symbols is  $K = 12$ , the number of radio frames is 3,  $\Phi_J = 0$  rad,  $\Phi_B = 0.1$  rad,  $SNR = 1$  dB vs.  $M$ .

and gets better as the SNR increases. Meanwhile, with the same number of training symbols, in the Rician channel model, the detection probability is significantly improved with the lower bound of the detection probability 95%, increasing by 30% compared to the Rayleigh fading channel model and quickly reaching to one as the SNR increases. We observe that the detection probability of the system over the presence of LoS components is very high despite a few antennas equipped at the base station and even though the attacker has the same AoA as the user.

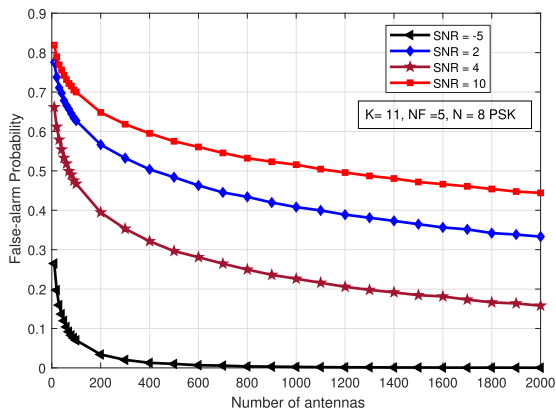
Fig. 6 shows the false-alarm probability vs. the number of base station antennas with PSK modulation level  $N = 8$ ,  $\Phi_J = 0$  rad, and  $\Phi_B = 0.1$  rad. The number of training symbols is selected in the set of  $[5, 10, 15, 20]$  in the three frames. As expected, the false-alarm probability decreases as the number of base station antennas increases. Moreover, all the results show that the false-alarm probability is relatively low with a sufficiently large number of training symbols.

Besides, the false-alarm probability approaches zero as the number of antennas is large enough. This means that the attacker can be detected effectively by a very high probability via utilizing a large number of training symbols as well as a large number of antennas.

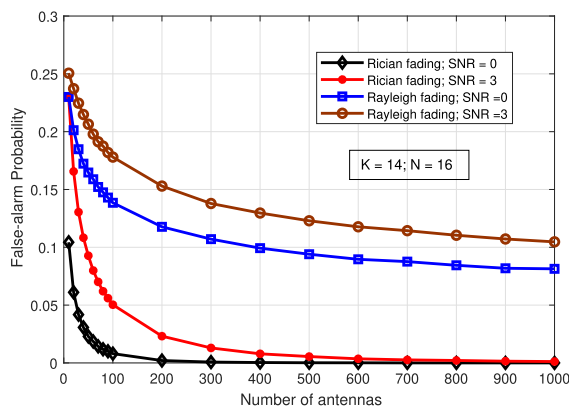
Fig. 7 presents the false-alarm probability for another setting of parameter including  $\Phi_J = 0$  rad,  $\Phi_B = 0.1$  rad with with number of PSK =  $[4, 8, 16, 24]$ , number of training symbols is  $K = 12$ , and in 3 frames when number of base station antennas increases. These results show the system get high values of PSK. The system has a lower probability of false alarm. Even if the probability of false alarm is very low, close to 0, it can be considered as a system with almost no false alarm.

Fig. 8 shows the false-alarm probability decreases even if  $\Phi_J = 0$  rad,  $\Phi_B = 0.1$  rad with the  $SNR = [-5, 2, 4, 10]$  dB, number of training symbols is  $K = 11$ , and in the number of radio frames is 2 when number of base station antennas increases. These results showed the system get less values of SNR, the system had the less false-alarm probabilities,





**FIGURE 8.** False-alarm probability of Rician fading channel vs. the number of base station antennas for the SNR are [-5, 2, 4, 10], the number of training symbols is  $K = 11$ , the number of radio frames is 5, PSK modulation level is  $N = 8$ ,  $\Phi_J = 0$  rad,  $\Phi_B = 0.1$  rad.



**FIGURE 9.** The false-alarm probability of Rician fading channels and the Rayleigh fading channels vs. the number of base station antennas with  $SNR \in [0, 3]$  [dB], the number of training symbols is 14, the number of radio frames is 8, PSK modulation level is  $N = 16$ ,  $\Phi_J = 0.1$  rad,  $\Phi_B = 0.1$  rad.

even the probability of false alarm is close to zero. Fig. 8 show the results of Rician fading channels. These results demonstrated that in the Rician fading channels false-alarm probabilities almost very close to zero while the number of antennas increased and the number of constellation points is sufficiently high.

Fig. 9 compares the false-alarm probability of the system over either the Rayleigh fading channels or the Rician fading channels with  $SNR = [0, 3]$  dB, the number of training symbols is 14, the number of radio frames is 8, PSK modulation level is  $N = 16$ ,  $p_B = 24$  dBm,  $p_J = 24$  dBm, and the AoA of legitimate user  $\Phi_B = 0.1$  rad and the AoA of the attacker  $\Phi_J = 0.1$  rad vs. the number of base station antennas. Even though the AoA of the attacker and that of the user are identical to each other, the considered benchmarks have, nonetheless, a very low false alarm probability. In our considered scenarios under the Rician fading channels, the false-alarm probability rapidly converges to zero when the number of base station antennas grows. In all the parameter settings, the system over the Rayleigh fading channels yields about 10% lower the false-alarm probability than that of the

system over the Rician fading channels. In particular, the results demonstrate that the false-alarm probability of our considered framework is significantly smaller than what was considered in [12]. The results manifest the benefits of a massive number of antennas in protecting legitimate users from jamming attacks.

## V. CONCLUSION AND FUTURE WORK

In this paper, we studied the detection scheme based on randomly transmitting the modulated pilot signals with the  $N$ -PSK modulation schemes. The detection scheme requested only the two training slots to execute detection at the base station without any the prior knowledge on the instantaneous channels. With a small number of the constellation points and the high SNR regime, we have explored that our proposed detection scheme achieves the detection probability one. Numerical results showed that the proposed detection scheme provided the high detection probability and lower false-alarm probability with many settings. As one potential direction for future work, we may investigate the affects of single or multiple attackers in massive MIMO communication systems with the spatially-correlated Rician channels.

## REFERENCES

- [1] 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.
- [2] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.
- [3] S. Jin, D. Yue, and H. H. Nguyen, "Spectral and energy efficiency in cell-free massive MIMO systems over correlated Rician fading," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2822–2833, Jun. 2020.
- [4] J. Zhang, J. Fan, B. Ai, and D. W. K. Ng, "NOMA-based cell-free massive MIMO over spatially correlated Rician fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
- [5] L. Sanguinetti, E. Björnson, and J. Hoydis, "Toward massive MIMO 2.0: Understanding spatial correlation, interference suppression, and pilot contamination," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 232–257, Jan. 2020.
- [6] *Study on New Radio (NR) Access Technology (Release 15)*, document 3GPP TR 38.912, Technical Report v.15.0.0, Jun. 2018.
- [7] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.
- [8] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.
- [9] 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.
- [10] T. Van Chien, H. Q. Ngo, S. Chatzinotas, B. Ottersten, and M. Debbah, "Uplink power control in massive MIMO with double scattering channels," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1989–2005, Mar. 2022.
- [11] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, May 2016.
- [12] 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.
- [13] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.
- [14] 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.

- [15] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.
- [16] K. Guo, Y. Guo, and G. Ascheid, "Security-constrained power allocation in MU-massive-MIMO with distributed antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8139–8153, Dec. 2016.
- [17] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3614–3628, Aug. 2017.
- [18] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.
- [19] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.
- [20] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
- [21] Y. O. Basciftci, C. E. Koksall, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 272–280.
- [22] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive MIMO pilot retransmission strategies for robustification against jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 58–61, Feb. 2017.
- [23] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 2001–2016, Jan. 2017.
- [24] O. Ozdogan, E. Bjornson, and E. G. Larsson, "Massive MIMO with spatially correlated Rician fading channels," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3234–3250, May 2019.
- [25] Y. Hu, Y. Hong, and J. Evans, "Angle-of-arrival-dependent interference modeling in Rician massive MIMO," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6171–6183, Jul. 2017.
- [26] L. Sanguinetti, A. Kammoun, and M. Debbah, "Theoretical performance limits of massive MIMO with uncorrelated rician fading channels," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1939–1955, Mar. 2019.
- [27] G. Q. L. Vu, H. Tran, and K. T. Truong, "Jammer detection by random pilots in massive MIMO spatially-uncorrelated rician channels," in *Proc. 8th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2021, pp. 440–445.
- [28] T. V. Chien, H. Q. Ngo, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surface-assisted massive MIMO: Favorable propagation, channel hardening, and rank deficiency," *IEEE Signal Process. Mag.*, vol. 39, no. 3, pp. 97–104, May 2022.
- [29] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. 24th PIMRC*, Sep. 2013, pp. 13–18.
- [30] *Study on Channel Model for Frequencies From 0.5 to 100 GHz*, document 3GPP TR 38.901, Technical Report v.15.0.0, Jun. 2018.
- [31] T. S. Rappaport, S. Sun, and M. Shafi, "Investigation and comparison of 3GPP and NYUSIM channel models for 5G wireless communications," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5.
- [32] S. Sun, T. S. Rappaport, T. A. Thomas, A. Ghosh, H. C. Nguyen, I. Z. Kovacs, I. Rodriguez, O. Koymen, and A. Partyka, "Investigation of prediction accuracy, sensitivity, and parameter stability of large-scale propagation path loss models for 5G wireless communications," *IEEE Trans. Veh. Tech.*, vol. 65, no. 5, pp. 2843–2860, May 2016.
- [33] C. V. Trinh, E. Björnson, and E. G. Larsson, "Joint pilot design and uplink power allocation in multi-cell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2000–2015, Mar. 2018.



**GIANG QUYNH LE VU** received the Bachelor of Science and master's degrees in computer science from Volgograd National Technical University, Russia, in 2005 and 2007, respectively. She is currently pursuing the Ph.D. degree with the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam. She is currently a Lecturer with the Information Technology, National Academy of Education Management, Hanoi. Her current research interest includes physical layer security

for very large MIMO systems.



**HUNG TRAN** received the B.S. and M.S. degrees in information technology from Vietnam National University, Hanoi, Vietnam, in 2002 and 2006, respectively, and the Ph.D. degree from the Blekinge Institute of Technology, Sweden, in March 2013. In 2014, he was with the Electrical Engineering Department, ETS, Montreal, Canada. From 2015 to 2020, he was a Researcher at Mälardalen University, Sweden. He is currently working as a Researcher at the Computer Science

Department, Phenikaa University, Vietnam. Besides doing research in the areas of wireless communication, he is also interested in topics of natural language processing and artificial intelligence, which have been applied to develop core engines for the academic gates platform.



**TRINH VAN CHIEN** (Member, IEEE) received the B.S. degree in electronics and telecommunications from the Hanoi University of Science and Technology (HUST), Vietnam, in 2012, the M.S. degree in electrical and computer engineering from Sungkyunkwan University (SKKU), South Korea, in 2014, and the Ph.D. degree in communication systems from Linköping University (LiU), Sweden, in 2020. He was a Research Associate at the University of Luxembourg. He is

currently with the School of Information and Communication Technology (SoICT), HUST. His research interests include convex optimization problems and machine learning applications for wireless communications and image and video processing. He received the Award of Scientific Excellence in the first year of the 5G wireless project funded by the European Union Horizon's 2020. He was an Exemplary Reviewer of IEEE WIRELESS COMMUNICATIONS LETTERS, in 2016, 2017, and 2021.



**LE NHAT THANG** received the B.Eng. degree in radio-electronics and communication from the Hanoi University of Science and Technology (HUST), Vietnam, in 1995, the M.Eng. degree in telecommunications from the Asian Institute of Technology (AIT), Bangkok, Thailand, in 2000, and the Ph.D. degree in information and communication technology (ICT) from the Department of Computer Science and Telecommunications (DIT), University of Trento, Italy, in 2006.

He is currently an Associate Professor and the Dean of the Postgraduate Studies Faculty, Posts and Telecommunications Institute of Technology (PTIT), Hanoi, Vietnam. His current research interests include performance analysis, modeling and simulations, wireless communications systems, physical layer security, queuing theory, and applications.



**KIEN TRUNG TRUONG** (Senior Member, IEEE) received the B.S. degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 2002, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Texas at Austin, Austin, TX, USA, in 2008 and 2012, respectively. He is currently a Lecturer of engineering at Fulbright University Vietnam, Ho Chi Minh City, Vietnam. His current research interests include

massive MIMO communications, millimeter-wave communications, the Industrial Internet of Things (IIoT), and engineering education. He was a fellow of the Vietnam Education Foundation, in 2006. He was a corecipient of the 2013 *EURASIP Journal on Wireless Communications and Networking* Best Paper Award and the 2014 IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS Best Paper Award.

• • •