A study on physical layer security of massive MIMO in the Rician fading channel consideration

Le Vu Quynh Giang[1*], Truong Trung Kien[2], Hoang Trong Minh[3]

[1]National Institute of Education Management, Ha Noi, Vietnam;
[2]Fulbright University Vietnam, Ho Chi Minh City, Vietnam.
[3]Posts and Telecoms Institute of Technology, Ha Noi, Vietnam.
[*]Email: quynhgiang81@gmail.com
Received 09 June 2022; Revised 27 July 2022; Accepted 10 October 2022; Published 28 October 2022.
DOI: https://doi.org/10.54939/1859-1043.j.mst.82.2022.21-29

ABSTRACT

Massive MIMO is one of the fundamental technologies for 5G and beyond networks, which combines antennas at the transmitter and receiver to achieve significant efficiency. The technology provides a high spectral and energy yield with minimal manipulation, in the fact that this technology has enabled a wide range of IoT application solutions with apparent advantages in scenarios involving a vast amount of terminals. However, creating high-density networks of IoT applications brings a new challenging security problem for the system, which should be studied under a suitable deployment channel model assumption as the Rice channel model. This paper presents a novel security analytic method to identify and detect an eavesdropper over the physical layer of massive MIMO systems under Rican channel conditions. The numerical analysis results indicate that the proposal can detect attacks and estimate the probability of false alarms when attackers exist.

Keywords: Massive MIMO; Security; Eavesdropper; Analytic method; Rician channel model.

1. INTRODUCTION

MIMO is the most attractive wireless access method for meeting 5G and beyond network requirements. Massive MIMO is an extension of MIMO technology that enhances spectral efficiency and throughput by adding hundreds or thousands of antennas to a base station [1, 2]. This technology is a crucial enabler for 5G and future generations to solve the problem posed by significant data traffic, users of conventional cellular networks, and IoT devices [3]. Especially, emerging systems approach such as the free-cell massive MIMO system gives many benefits to the service users [4]. In these systems requiring such dense networks, practical channels can consist of a deterministic line of sight (LOS) path, and small-scale fading caused by multipath propagation led to recent research related to the Rice channel model [5-7].

Security is the most important aspect of wireless communication systems, particularly massive MIMO communications. In such a system, the physical layer security associated with massive MIMO systems has been the subject of numerous research since the possibility of eavesdropping attacks in IoT contexts is increasing exponentially [8]. Most researchers prefer the Rayleigh distribution model to study the physical layer security due to its simplicity and accuracy. However, from the requirements of the current application scenario, the Rican distribution model needs to be applied in both performance and security analysis models [9]. This study proposed an analytical method to detect the probability of an eavesdropper in a massive MIMO system with a Rician distribution model. The effectiveness of our proposal is proven by numerical simulation.

The structure of the paper is as follows. The following section briefs recently related works of other studies. The proposed system model is described in section III. Section IV presents our security validation through numerical results and insightful comments. The conclusion and our future work are summarized in the last section.

2. RELATED WORK

The massive MIMO with an independent Rayleigh distribution model brings to convenient propagation environment. The channels of different users are asymptotically orthogonal, and it favors highly directional LOS components. The primary motivation for using the Rayleight distribution model from the mathematical aspect is gained from the central limit theorem, which says that the sum of many independent and identically distributed random variables is approximately Gaussian. Hence, many studies consider this model to evaluate system performance or security issues [10, 11]. The above studies have yielded valuable results in detecting eavesdropping at the physical layer of the massive MIMO system. However, new communication channel conditions have led to a new approach to solving this problem.

The practical channels are combined with a deterministic LOS path and small-scale fading caused by multipath propagation in several real modern applications [4, 12]. To concentrate on the performance problem of massive MIMO systems using the Rician distribution model, several recent proposals have been presented in various considered technical features. To evaluate the uplink performance in massive MIMO with spatially correlated Rician fading channels. The author in [13] proposed an analytic model and used a phase-aware element based on the minimum mean squared error MMSE and a linear MMSE estimator (LMMSE) to improve the spectrum efficiency. Spectral and Energy Efficiency of the downlink in Cell-Free Massive MIMO Systems Over Correlated Rician Fading has been studied [9]. The authors derived the closed-form expressions of the sum spectral efficiency (SE) and total energy efficiency (EE) and then developed two successive approximation algorithms to improve the sum SE and total EE by optimizing the power control coefficients of DL data and pilot.

Considering the security aspects of massive MIMO with over Ricean fading channels, the authors in [14, 15] exploited that the eavesdropping attack causes anomalous effects and recognizable events. In [14], the authors proposed an angle aware user cooperation (AAUC) scheme, which avoids direct transmission to the attacked user and relies on other users for cooperative relaying. However, the proposed scheme requires the eavesdropper's angle information and adopts an angular secrecy model to represent the average secrecy rate of the attacked system. Based on all possible eavesdropping attacks in a typical massive MIMO system [15], The authors in [16] exploited that the eavesdropping attack causes signal-to-interference-plus-noise-ratios (SINRs) to change. However, the proposal is only focused on the Rayleigh fading channels of the massive MIMO system. Hence, in this paper, we propose a novel analytical model based on the characteristics of Rician fading channels to analyze and evaluate all possibilities of eavesdropping attacks on the system. Numerical simulation results will be given to verify our model.

3. SYSTEM ASSUMPTIONS

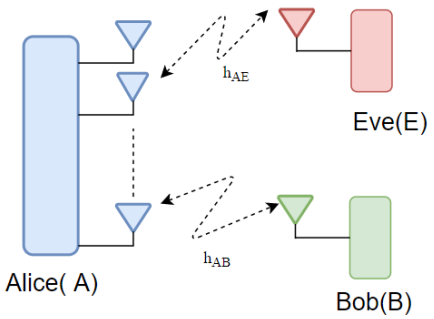

Figure 1. *A typical MIMO system.*

Consider a typical MIMO system is illustrated in figure 1. The number of antennas equipped in the base station is *Nt*. At the base station (BS) side, antennas are arranged as the uniform linear array (ULA). Denote β_X is the large-scale fading factor of a channel from BS to a user ($X \in \chi$, $X = \{B, E\}$, B is denoted as a normal user, and E is denoted as an eavesdropper). We have $\beta_{X,L} = \frac{k_x}{k_x + 1}\beta_X$ in case light of sight (LOS) and $\beta_{X,N} = \frac{1}{k_x + 1}\beta_X$ incase non-line-of-sight (NLOS). Where k_x is the Rician coefficient.

The channel vector coefficient of LOS from the base station to an anonymous user $X \in \chi$ is given by

$$g_x = \beta_{X,L}^{1/2}[1, e^{j2\pi d \sin\phi_X}, e^{j2\pi d(N-1)\sin\phi_X}]^T . \quad (1)$$

ϕ_X is the arrival angle from a user to BS; d is a function of antenna spacing and wavelength. We have,

$$g_X^H g_X = Nt\beta_{X,L}, \forall X \in \chi . \quad (2)$$

In which,

$$\psi(\phi_B, \phi_E) = \pi d(\sin\phi_B - \sin\phi_E),$$
$$\alpha(\phi_B, \phi_E, Nt) = \frac{\sin(Nt\psi(\phi_B, \phi_E))}{\sin(\psi(\phi_B, \phi_E))} .$$

Hence,

$$g_E^H g_B = \beta_{B,L}^{1/2}\beta_{E,L}^{1/2} e^{\psi(\phi_B, \phi_E)}\alpha(\phi_B, \phi_E, Nt) . \quad (3)$$

$h_B \in \mathbb{C}^{Ntx1}$ is the channel vector on the uplink from a user to the base station (BS).

$h_E \in \mathbb{C}^{Ntx1}$ is the channel vector on the uplink from Eve to BS.

Assume the channel model is perfect TDD reciprocity, we have $h_B^H, h_E^H \in \mathbb{C}^{1xNt}$.

With $W_x \sim CN(0, I_{Nt})$ is small-scale fading coefficient and the distribution of channel vector h_x is $\sim CN(g_X, \beta_{X,N} I_N)$, we have a channel factor h_x as below.

$$h_x = g_x + \beta_{X,N}^{1/2} w_x . \quad (4)$$

From (3) and $\psi(\phi_B, \phi_E) = \pi d(\sin\phi_B - \sin\phi_E)$, $\alpha(\phi_B, \phi_E, Nt) = \frac{\sin(Nt\psi(\phi_B, \phi_E))}{\sin(\psi(\phi_B, \phi_E))}$.

We have

$$g_E^H g_B = \beta_{B,L}^{1/2}\beta_{E,L}^{1/2} e^{\psi(\phi_B, \phi_E)}\alpha(\phi_B, \phi_E, Nt) . \quad (5)$$

In the uplink training phase, legitimate B has a transmit power P_B , and E has a transmit power (P_E). At the training time slot *j*, the pilot sent by B and E is $p_j^B, p_j^E \in A$ (A is all training symbols). Generally, pilot A emitted by Bob is public and standard.

In this case, Eve can transmit the same pilots as Bob.

An equation processes the received pilot signal at the BS.

$$y_j = \sqrt{P_B}\, p_j^B h_{AB} + \sqrt{P_E}\, p_j^E h_{AE} + nj\,. \tag{6}$$

Where $h_{AB} = g_B + \beta_{B,N}^{1/2} w_B; h_{AE} = g_E + \beta_{E,N}^{1/2} w_E, nj \sim CN(0, \delta_j^2 I_{Nt})$, and n_j is the additive white Gaussian noise.

Assume that the BS applies the linear minimum mean squared errors (MMSE) estimation method to obtain the following channel estimations. We have,

$$R_T^{11} = h_{AB}^H h_{AB} = Nt(\beta_{B,L} + \beta_{B,N}) = \beta_B Nt\,, \tag{7}$$

$$R_T^{12} = h_{AE}^H h_{AE} = \beta_{B,N}^{1/2} \beta_{B,N}^{1/2} e^{j\phi(\phi_B,\phi_E)} \alpha(\phi_B, \phi_E, Nt)\,, \tag{8}$$

$$R_T^{21} = [R_T^{12}]^H = \beta_{B,N}^{1/2} \beta_{B,N}^{1/2} e^{-j\phi(\phi_B,\phi_E)} \alpha(\phi_B, \phi_E, Nt)\,, \tag{9}$$

$$R_T^{22} = h_{AE}^H h_{AE} = Nt(\beta_{E,L} + \beta_{E,N}) = \beta_E Nt\,. \tag{10}$$

4. ATTACK DETECT CASES

Alice finds it very difficult to distinguish between the pilots deployed by Bob and Eve. Suppose Alice is aware of channel information $h_{AB,}$ h_{AE} and they are significantly different. Deviations in signal strength is shown, and the probability of detection increases. The information of Bob's pilots, however, works towards Eve's detection. Instead, the observed probability deviates from the anticipated signal gain if Bob broadcasts the pilots at random. This observation forms the basis for random pilot detection.

We discuss four cases to detect E to cover all possible eavesdropping attacks, and we discuss 4 cases to detect attacker (*E*). A sequence of random phase-shift keying (N-PSK) symbols forms the key to detecting at the base station side.

B transmits two pilot signals (p_1, p_2) that are independent of an N-PSK constellation. The base station recognizes Z as the phase of $y_1^H y_2$, where $(.)^H$ is a conjugate transpose. 4 scenarios can happen such as (1) *E* is absent in both time slots, (2) *E* is present in both time slots, (3) *E* is present in the first slot, and (4) *E* is present in the second slot.

4.1. The attacker is absent in both time slots

Assume that E is inactive at both times. Then, the signals are received in two training times, respectively:

$$\begin{cases} y_1 = \sqrt{\underline{P}_B}\, p_1^B h_{AB}^H + n_1 \\ y_2 = \sqrt{\underline{P}_B}\, p_2^B h_{AB} + n_2 \end{cases} \tag{11}$$

$$[Z_{12}^0] = [\frac{1}{Nt} y_1^H y_2] = \left\{ \frac{1}{Nt} \left[\sqrt{\underline{P}_B} v_1^B h_{AB} + n_1 \right]^H \left[\sqrt{\underline{P}_B} v_2^B \right] \right\}$$

$$= \frac{1}{Nt} \{ \underline{P}_B (p_1^B)^H p_2^B (h_{AH}^H h_{AB}) \} + \frac{1}{Nt} \sqrt{\underline{P}_B} (p_1^B)^H h_{AB}^H n_2 + \frac{1}{Nt} \underline{P}_B p_2^B h_{AB} n_1^H + n_1^H n_2$$

$$= \frac{1}{Nt} \underline{P}_B (p_1^B)^H (p_2^B) h_{AB}^H h_{AB} + N_{12}^0 = \frac{1}{Nt} \underline{P}_B (p_1^B)^H (p_2^B) R_T^{11} + N_{12}^0\,. \tag{12}$$

Where, $R_T^{11} = \beta[1\,1][1\,1]^T = 2\beta$, $E[Z_{12}^0] = \frac{2\beta \underline{P}_B}{Nt} (p_1^B)^H p_2^B \in N - PSK$.

$Z_{12}^0 \in N - PSK$ =>E is not present; Z_{12}^0 equals a scale PSK symbol disturbed by complex Gaussian noise with zero mean and variance $S_E^0 = \frac{1}{Nt} [2\underline{P}_B Nt \int_B^3 \sigma^2 + \sigma^4]$.

4.2. The attacker is present in both time slots

Assume that E is active at both times. Then, the signals are received in two training times, respectively:

$$\begin{cases} y_1 = \sqrt{\underline{P}_B}\, p_1^B h_{AB}^H + \sqrt{\underline{P}_E}\, p_1^E h_{AE}^H + n_1 \\ y_2 = \sqrt{\underline{P}_B}\, p_2^B h_{AB} + \sqrt{\underline{P}_E}\, p_2^E h_{AE}^H + n_2 \end{cases} \quad (13)$$

$$\begin{aligned} [Z_{12}^0] &= \frac{1}{Nt}(\sqrt{\underline{P}_B}\, p_1^B h_{AB} + \sqrt{\underline{P}_E}\, p_1^E h_{AE} + n_1)^H (\sqrt{\underline{P}_B}\, p_2^B h_{AB} + \sqrt{\underline{P}_E}\, p_2^E h_{AE} + n_2)\,. \\ &= \frac{1}{Nt}\{\underline{P}_B (p_1^B)^H\, p_2^B h_{AH}^H h_{AB} + \sqrt{\underline{P}_B \underline{P}_E}\,(p_1^B)^H (p_2^B) h_{AB}^H h_A \\ &+ \sqrt{\underline{P}_B \underline{P}_E}\,(p_1^E)^H (p_2^B) h_{AE}^H h_{AB} + \underline{P}_E (p_1^E)^H (p_2^E) h_{AE}^H h_{AE} + N_{12}^E\} \end{aligned} \quad (13)$$

Where $N_{12}^E = \sqrt{\underline{P}_E}\,(p_1^B)^H h_{AB}^H n_2 + \sqrt{\underline{P}_E}\left(p_1^E\right)^H h_{AE}^H n_2 + \sqrt{\underline{P}_B}\, p_2^B n_1^H h_{AB} + \sqrt{\underline{P}_E}\, p_2^E h_{AB} n_1^H + n_1^H n_2$.

N_{12}^E converges to a complex Gaussian variable with zero mean and variance S_E^M. Applying the same analysis in the previous section. We have,

If $p_1^E \left(p_1^B\right)^H = p_2^E \left(p_2^B\right)^H$ then $Z_{12}^E \sim N - PSK + N_{12}^E$

If $P_1^E \left(P_1^B\right)^H \neq P_2^E \left(P_2^B\right)^H$ then $Z_{12}^E \notin N - PSK$

4.3. The attacker is present in the first slot

Assume that E is active the first times. Then, the signals are received in two training times, respectively:

$$\begin{cases} y_1 = \sqrt{\underline{P}_B}\, p_1^B h_{AB}^H + \sqrt{\underline{P}_E}\, p_1^E h_{AE}^H + n_1 \\ y_2 = \sqrt{\underline{P}_B}\, p_2^B h_{AB} + n_2 \end{cases}, \quad (14)$$

$$Z_{12}^0 = \frac{1}{Nt}\left\{(\sqrt{\underline{P}_B}\, p_1^B h_{AB} + \sqrt{\underline{P}_E}\, p_1^E h_{AE} + n_1)^H (\sqrt{\underline{P}_B}\, p_2^B h_{AB} + n_2)\right\}$$

$$\begin{aligned} &= \frac{1}{Nt}\{\underline{P}_B (p_1^B)^H\, p_2^B h_{AH}^H h_{AB} + \sqrt{\underline{P}_B}\,(p_1^B)^H h_{AB}^H n_2 + \sqrt{\underline{P}_B \underline{P}_E}\,(p_1^E)^H (p_2^B) h_{AE}^H h_{AE} \\ &+ \sqrt{\underline{P}_E}\,(p_1^E h_{AE})^H n_2 + n_1^H \sqrt{\underline{P}_B}\, p_2^B h_{AB} + n_1^H n_2\} \end{aligned} \quad (15)$$

$$E\left[Z_{12}^E\right] = \frac{1}{Nt}\left\{\underline{P}_B (p_1^B)^H\, p_2^B R_T^{11} + \sqrt{\underline{P}_B \underline{P}_E}\,(p_1^E)^H\, p_2^B R_T^{22}\right\}$$

$$\begin{cases} E\left[Z_{12}^E\right] \in N - PSK \\ E\left[Z_{12}^E\right] \notin N - PSK \end{cases}$$

4.4. The attacker is present in the second slot

Assume that E is active the second times. Then, the signals are received in two training times, respectively:

$$\begin{cases} y_1 = \sqrt{\underline{P}_B}\, p_1^B h_{AB} + n_1 \\ y_2 = \sqrt{\underline{P}_B}\, p_2^B h_{AB} + \sqrt{\underline{P}_E}\, p_2^E h_{AE} + n_2 \end{cases}, \quad (16)$$

$$Z_{12}^{E}=\frac{1}{Nt}\left\{(\sqrt{p_B}\,p_1^B h_{AB}+n_1)^H(\sqrt{\underline{P}_B}\,p_2^B h_{AB}+\sqrt{\underline{P}_E}\,p_2^E h_{AE}+n_2)\right\}$$

$$=\frac{1}{Nt}\{\underline{P}_B(p_1^B)^H\,p_2^B h_{AH}^H h_{AB}+\sqrt{\underline{P}_B\underline{P}_E}(p_1^B)^H\,p_2^E h_{AB}^H h_{AE}+\sqrt{\underline{P}_B}(p_1^B h_{AB}^H)^H n_2+ \quad (17)$$

$$n_1^H\sqrt{\underline{P}_B}\,p_2^B h_{AB}+n_1^H\sqrt{\underline{P}_E}\,p_2^E h_{AE}+n_1^H n_2\}$$

$$E\left[Z_{12}^{E}\right]=\frac{1}{Nt}\left\{\underline{P}_B(p_1^B)^H\,p_2^B R_T^{11}+\sqrt{\underline{P}_B\underline{P}_E}(p_1^B)^H\,p_2^E R_T^{12}\right\}$$

$$\begin{bmatrix} E\left[Z_{12}^{E}\right]\in N-PSK \\ E\left[Z_{12}^{E}\right]\notin N-PSK \end{bmatrix}$$

There are 2 possibilities:

Scale product Z does not belong to the set of PSK signals. Alice then decides that E appears in this moment. Alice can decide to pause transmission or use another secure transmission method.

Z belongs to the set of PSK signals. That is, in order for Eve not to be discovered by Alice, at the second time Eve predicts and sends the pilot $p_2^E=p_1^E\left(p_1^B\right)^H p_2^B$.

We examined and determined the attack detection probability using this as our premise.

5. NUMERICAL RESULTS

To validate the effectiveness of our detection strategy, we simulate the detection probability and the false-alarm probability. The chance of a false- alarm is defined as the likelihood of detecting a jammer that does not exist. We looked at a network with only one cell, with the base station in the cell's center and the legitimate user Bob and the eavesdropper device dispersed across the cell.

If the shadowing effect is neglected, large-scale fading is calculated as [17], hence this study is investigated in the urban cell environment.

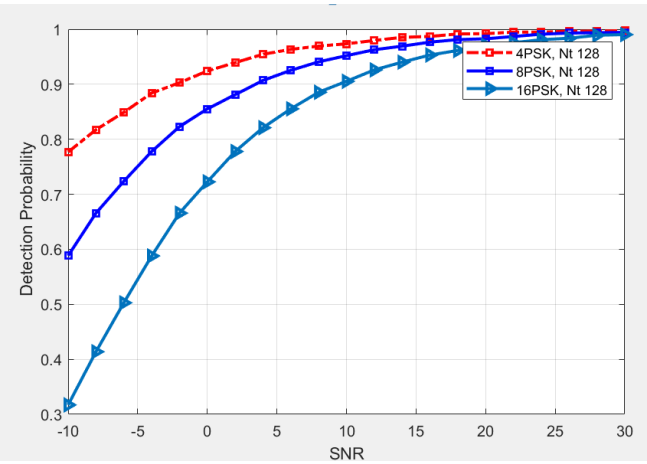

Figure 2. *Detection Probabilities vs PSK = 4, 8, 16, number of antennas N_t =128.*

The result shows the detection probability as a function of SNR when the base station has Nt =128 antennas and uses some PSK number. As expected, the probability of detection increases with SNR; in the high SNR domain, detection probability goes to 1. Notably, even with a small number of PSK, we have a very high probability of detecting jammers.

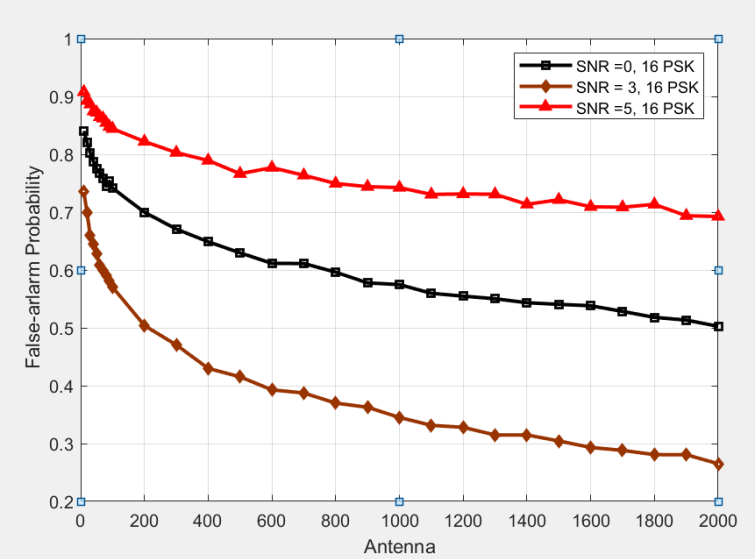

Figure 3. *False-alarm probabilities vs PSK =16, SNR =[0,3,5].*

Figure 3 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 used PSK number is big enough. These results is proven as tailored to theory.

To compare the detection probability between Rayleigh fading and Rician fading condition, we use lower PSK (8) and medium antenas to validate. In the figure 4 shows that our model can detect attacker better than Rayleigh fading case when the curve shows the apparent change of the detection probability with the change of SNR.

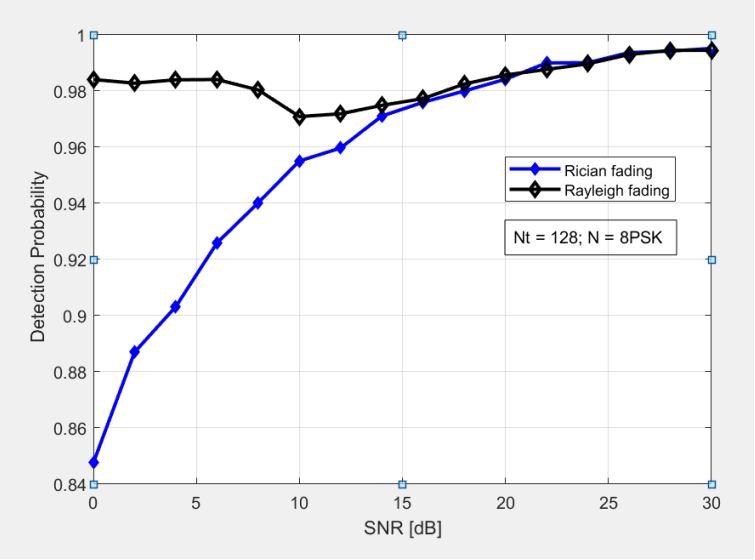

Figure 4. *Compare Detection Probabilities between Rayleigh fading and Rician fading.*

6. CONCLUSIONS

In this research, we present a model for the detection of attacks in massive MIMO systems with Rician fading. This approach is congruent with 5G's current deployment techniques for Internet of Things applications. On the basis of the proposed model, attack detection scenarios

were numerically simulated and matched with the conventional Rayleigh channel condition. Moreover, by using PSK and interference impacts from our proposed model, we can detect attacks without using channel information like traditional solutions. In the proposed model, we use random PSK pilots in a massive MIMO system then we devised a performance metric for detecting attack in two separate training symbols in convernience way. Our future work will be focused on the NOMA links of massive MIMO systems with Rician fading.

REFERENCES

[1]. 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, (2014).

[2]. Chataut, R., & Akl, R. *"Massive MIMO Systems for 5G and Beyond Networks-Overview, Recent Trends, Challenges, and Future Research Direction"*. Sensors (Basel, Switzerland), 20(10), 2753, (2020).

[3]. A.-S. Bana et al., *"Massive MIMO for Internet of Things (IoT) connectivity"*, Phys. Commun., vol. 37, (2019).

[4]. H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson and T. L. Marzetta, *"Cell-Free Massive MIMO Versus Small Cells,"* in IEEE Transactions on Wireless Communications, vol. 16, no. 3, pp. 1834-1850, (2017), doi: 10.1109/TWC.2017.2655515.

[5]. Wang Z, Zhang J, Bj¨ornson E, et al. *"Uplink performance of cell-free massive MIMO over spatially correlated Rician fading channels[J]"*. IEEE Communications Letters, 25(4): pp. 1348-1352, (2020).

[6]. Jin S N, Yue D W, Nguyen H H. *"Spectral and energy efficiency in cell-free massive MIMO systems over correlated Rician fading[J]"*. IEEE System Journal, 15(2): 1-12, (2020).

[7]. H. He, X. Yu, J. Zhang, S. Song and K. B. Letaief, *"Cell-Free Massive MIMO for 6G Wireless Communication Networks,"* in Journal of Communications and Information Networks, vol. 6, no. 4, pp. 321-335, (2021), doi: 10.23919/JCIN.2021.9663100.

[8]. Butun, P. Österberg and H. Song, *"Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,"* in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, (2020), doi: 10.1109/COMST.2019.2953364.

[9]. S. -N. Jin, D. -W. Yue and H. H. Nguyen, *"Spectral and Energy Efficiency in Cell-Free Massive MIMO Systems Over Correlated Rician Fading,"* in IEEE Systems Journal, vol. 15, no. 2, pp. 2822-2833, (2021), doi: 10.1109/JSYST.2020.2993048.

[10]. Pooja Singh, Aditya Trivedi, *"NOMA and massive MIMO assisted physical layer security using artificial noise precoding,"* Physical Communication, Volume 39, 100977, ISSN 1874-4907, (2020).

[11]. Singh, K.R., Trivedi, A. *"Physical Layer Security for Wireless Powered Massive MIMO Decode and Forward Relay Systems with Hardware Impairments: Performance Analysis"*. Wireless Pers Commun 112, pp. 1537–1547 (2020).

[12]. Kassaw, D. Hailemariam and A. M. Zoubirl, *"Performance Analysis of Uplink Massive MIMO System Over Rician Fading Channel,"* 2018 26th European Signal Processing Conference (EUSIPCO), Rome, pp. 1272-1276, (2018), doi: 10.23919/EUSIPCO.2018.8553192.

[13]. Z. Wang, J. Zhang, E. Björnson and B. Ai, *"Uplink Performance of Cell-Free Massive MIMO Over Spatially Correlated Rician Fading Channels,"* in IEEE Communications Letters, vol. 25, no. 4, pp. 1348-1352, (2021), doi: 10.1109/LCOMM.2020.3041899.

[14]. S. Wang, M. Wen, M. Xia, R. Wang, Q. Hao and Y. -C. Wu, *"Angle Aware User Cooperation for Secure Massive MIMO in Rician Fading Channel,"* in IEEE Journal on Selected Areas in Communications, vol. 38, no. 9, pp. 2182-2196, (2020), doi: 10.1109/JSAC.2020.3000837.

[15]. D. Kapetanovic, G. Zheng and F. Rusek, *"Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,"* in IEEE Communications Magazine, vol. 53, no. 6, pp. 21-27, (2015).

[16]. X. Zhang, D. Guo and K. Guo, *"Secure Performance Analysis for Multi-Pair AF Relaying Massive MIMO Systems in Ricean Channels,"* in IEEE Access, vol. 6, pp. 57708-57720, (2018).

[17]. 3GPP TR 38.901, *"Study on channel model for frequencies from 0.5 to 100 GHz,"* 3GPP, Technical Report v.15.0.0, (2018).

TÓM TẮT

Một nghiên cứu về bảo mật lớp vật lý cho hệ thống massive MIMO với điều kiện kênh Rician

Massive MIMO là một nền tảng cơ bản để phát triển mạng 5G nhờ kết hợp số lượng lớn các ăng ten tại cả phía thu và phía phát. Công nghệ này cung cấp giải pháp sử dụng phổ tần hiệu quả và tiết kiệm năng lượng truyền thông. Trên thực tế, hệ thống massive MIMO hỗ trợ hàng loạt các giải pháp ứng dụng IoT hiện nay khi xử lý được số lượng lớn các thiết bị đầu cuối. Tuy nhiên, mạng mật độ cao của các thiết bị IoT đem đến các thử thách mới về độ bảo mật của hệ thống. Nhất là mô hình kênh truyền thống không thực sự phù hợp với đặc tính kênh truyền mới của hệ thống như pha đinh theo kênh Rician. Vì vậy, bài báo này trình bày một phương pháp phân tích bảo mật mới để xác định và phát hiện kẻ nghe trộm trên lớp vật lý của các hệ thống massive MIMO theo điều kiện kênh Rican. Kết quả phân tích số chỉ ra rằng, mô hình đề xuất có thể phát hiện hiệu quả các cuộc tấn công vào lớp vật lý theo nhiều tình huống khác nhau và không cần đến thông tin cụ thể của kênh truyền.

Từ khoá: Massive MIMO; Bảo mật; Nghe lén; Phương pháp giải tích; Mô hình kênh Rician.