# Two High-performance Methods for Choosing the Transmit Antenna for Secure Spatial Modulation

**V MOUNIKA [1], T LAKSHMI KALA [2], A ANUSHA [3], SD SANA ANJUM [4], P. JULIAN [5]**

[1]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[2]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[3]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[4]UG Scholar, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.
[5]Associate Professor, Dept of ECE, Andhra Engineering College, Atmakur, AP, India.

**ABSTRACT**

This research investigates a safe spatial modulation (SM) system with the use of artificial noise (AN). Leakage-based and maximum secrecy rate (Max-SR) transmit antenna selection techniques and a generalised Euclidean distance-optimized antenna selection method (EDAS) are proposed and built to attain a greater secrecy rate (SR) in such a system. The four TAS systems are ranked in decreasing order of SR performance: Max-SR, leakage-based, generalised EDAS, and random (traditional). It's a lot more complicated than the Max-SR method since it involves an exhaustive search to obtain optimal SR performance, which is incredibly time-consuming as the number of antennas grows. In comparison to the Max-SR method, the proposed leakage-based method has a lower level of complexity. SR performance and complexity are thus well-aligned in this case. In terms of bit error rate (BER), random, leakage-based, Max-SR, and generalised EDAS are in ascending order.

## 1. INTRODUCTION

One of the most promising MIMO communication technologies, SPATIAL MODULATION (SM) makes use of both the index of an activated transmit antenna and an amplitude phase modulation (APM) signal to transport messages [1],[2]. SM technology can be used in energy-efficient applications because of the simplicity of the transmitter and receiver. Due to the broadcast nature of the wireless channel, it is possible that sensitive communications are received by unintentional recipients in an SM system. It's becoming an increasingly popular area of study in wireless networks to figure out how to secure transmission in SM systems. Physical layer security in MIMO systems, which exploits the uniqueness and time-varying properties of the channel [3]–[6] or the polarisation of antenna arrays [7]–[8] to secure transmission against eavesdropper, has recently been widely studied. A number of studies have examined the usage of secure messaging (SM) systems for transmission [9–14]. The secrecy mutual information (SMI) derived by the authors in [9] was used to suggest a precoding technique to improve the SM system's secrecy rate (SR) performance. In order to improve the SR performance of space shift keying (SSK) systems, the authors in [13] suggested an iterative approach for maximising SR. Artificial noise (AN) was used in both [10] and [14] to disrupt eavesdroppers on the desired channel. A high SR approaching the spectral efficiency (SE) was achieved by sending AN at transmitter [10] or full-duplex receiver [14]. In [11] and [12], the authors generalised precoding-aided spatial modulation (PSM) to secrecy PSM by creating time-varying precoder [11] or optimising the precoder of simultaneously lowering the receive power at eavesdropper while increasing the receive power at targeted user [12]. To reduce receiver complexity, PSM systems use antenna indices to carry bit information. Inter-channel interference (ICI) and inter-antenna synchronisation (IAS) are issues that arise when all transmit antennas are active in PSM systems (IAS). When it comes to upgrading SM systems, transmit antenna selection (TAS) was the first to be studied in [15]. Both the capacity-optimized antenna selection (COAS) and the Euclidean distance-optimized antenna selection (EDOAS) have been proposed by the authors of [15]. (EDAS). The EDAS scheme showed a superior bit error rate (BER) performance and more complexity than COAS scheme. As a result, several pieces of literature have been written to make the EDAS scheme's computations and searches easier [16]–[18]. According to our study, no one has attempted to develop TAS methods for a secure SM system yet. For the purposes of this study, we shall focus on the research component of the topic and make the following contributions: 1) A maximum secrecy rate (Max-SR) method with exhaustive search is presented to reach the SR bound. For a wide range of SNR, it can outperform existing approaches, according to simulation data. 2) A leakage-based TAS approach for a secure

SM system is proposed to limit the leakage power of confidential messages for intended users to eavesdroppers. In order to obtain the same SR performance with less complexity, a sorting-based approach is also described. The suggested leakage-based method delivers an SR performance comparable to that of the Max-SR method, but with significantly less complexity. Our final step is to convert the normal EDAS approach for non-secure Smart Meter (SM) systems into a secure version for use in Smart Meters that are secured. The complexity of the three TAS approaches is being examined and compared in the meantime. The rest of the material is arranged in this way. Second, in Section II, we present the secure SM system model and define the average SR for it. Leakage-based and Max-SR TAS approaches are then proposed, and the traditional EDAS scheme is extended to secure SM systems. The numerical simulation findings are discussed in Section IV of the report. In Section V, we draw our final conclusions. Throughout the study, we use capital letters to designate the three different types of variables: matrices, vectors, and scalars. To express inverse and conjugate transpose, we use the symbols () 1 and () H. The expectation operation is denoted by the E notation. tr() signifies the matrix trace for the N-by-N identity matrix IN.

## 2. LITERATURE SURVEY

Data traffic on wireless networks has grown at breakneck speed in recent years, thanks to the rising popularity of smart phones, electronic tablets, and video streaming, as well as the rapid expansion of service providers. Mobile broadband communications demand is increasing, which presents a problem for the design of 5G networks in the near future [2]. Due to the current environment, secure data transmission through next-generation wireless networks is critical. There has been a lot of interest recently in 5G wireless network physical layer security in order to develop dependable and secure transmission techniques [3], [4]. Physical layer security, as opposed to traditional methods that rely on cryptographic algorithms [5], ensures confidentiality by taking advantage of the intrinsic properties of wireless communications. Cryptographic techniques used in the top levels of networks protect processed data, but a possible solution through the transmission phase might be physical layer security. [6]

The wiretap channel is a basic model for physical layer security because it shows how an eavesdropper might listen in on messages being sent to a genuine recipient. It was shown by Wyner that confidentiality can be achieved in this situation if the genuine receiver uses a channel with a higher quality than the eavesdropper's [7] Several approaches for enhancing secrecy were presented on the basis of this paradigm, including artificial noise production [8], [9] and cooperative jamming [10]. Wyner's approach has also been extended to MIMO scenarios, which have showed promising performance in the presence of eavesdroppers [11]–[13]. With reality, in MIMO wiretap channels, also known as MIMOME channels, the Base Station (BS) can focus its main broadcast beam to legal terminals and thereby decrease information leakage to the eavesdroppers. To protect against passive eavesdropping, giant MIMO configurations [14] employ a mechanism that asymptotically cancels out passive malevolent terminals in the network. Massive MIMO systems have a lot of potential, but they come with a high cost and complexity in terms of radio frequency (RF). When it comes to huge MIMO systems, having a distinct RF chain for each antenna places a strain on the implementation. Other techniques, such as spatial modulation [18] and hybrid analog-digital precoding schemes [19, 20], have been devised as a result of this issue. During each coherence time, just a fraction of an antenna's settings are active. Selecting subsets based on certain performance metrics, such as feasible transmission rates, outage likelihood, or bit error rates [17], is common practise. However, the most effective methods of antenna selection rely on an extensive search that is computationally impractical in most situations. There have also been a number of less ideal, but more effective in terms of complexity, ideas put forth in the literature, such as those in [21]–[24]. Numerous studies have demonstrated that using suboptimal methods in MIMO systems does not significantly reduce throughput [23], [25], or even [26]. Recent research have shown that even basic antenna selection methods can retain the large-system features of massive MIMO systems [27, 28]. MIMO systems can benefit from antenna selection in terms of performance parameters including secrecy rate [29], energy efficiency [31], and effective rate [32] in some particular instances, as well as complexity reduction. To put it another way, in a standard MIMO arrangement, a single Transmit Antenna Selection (TAS) can offer high security levels, especially when the total number of transmit antennas increases. [33] demonstrated this. The research was then expanded in [34] to include scenarios involving eavesdroppers with several antennas, and the same findings were found. In [35], a single TAS was used to examine secure transmission in a generic MIMOME channel. In the literature, these results were extended to various MIMOME scenarios. When a

single TAS is used, the Nakagami-m fading channel is examined for secure transmission in [36]. [37] also looked into the effects of inaccurate channel estimation and antenna correlation. In addition, [38], [39] investigated the average secrecy rate and secrecy diversity analysis for a simple single TAS system. In [40], scenarios involving single-antenna receivers were examined using TAS and outdated Channel State Information (CSI). Additional research was done on the effect of a single TAS at the BS in the presence of eavesdroppers with a fullduplex receiver [41]. There hasn't been any research on the secrecy performance of MIMOME channels when using multiple TAS, i.e., activating multiple transmit antennas. In fact, the increase in the number of transmit antennas under multiple TAS benefits both the legal receiver and the eavesdropper, therefore its influence on the overall secrecy performance is unclear. Using huge MIMOME and numerous TAS, this work will investigate the effects. Involvement and the Workplace The performance of a MIMOME channel in which the BS uses a TAS algorithm to pick a fixed number of broadcast antennas is studied. As the number of transmit antennas increases, the distribution of the instantaneous secrecy rate in the large-system limit can be properly calculated. Scenario (A) in which the eavesdropper's CSI is available at the transmit side, and Scenario (B) in which the BS does not know the eavesdropper's CSI are examined using this approximation. Both scenarios have circumstances where the number of active antennas is less than the number of transmit antennas, resulting in optimal secrecy performance. If the number of active antennas is increased over a certain point, however, the secrecy performance degrades, as the number of selected antennas might sometimes improve until it reaches an optimal value. This best value can be derived analytically from our large-system results. To ensure the validity of our technique, we conduct numerical studies. The rest of the manuscript is arranged as follows: a Section II explains how the system model works. Section III focuses on large-scale analyses. Section IV examines the effects of TAS on secrecy performance and includes some numerical data and debates. Final remarks are contained in Section VI. The appendices also include the proofs of the important theorems. Notations: This paper uses non-bold, bold lower-case, and bold upper-case letters to designate all scalars, vectors, and matrices. As a point of reference, C stands for the complicated plain. N-by-N Identity Matrix IN indicates the Hermitian of H. It is shown by |H| and kxk that H's determinant and the Euclidean norm of x are the same. the number that is closest in Euclidean distance to x. The binary and natural logarithm are denoted by log (·) and ln (·), respectively, while 1{·} indicates the indicator function. E {·} is the mathematical expectation, while Q(x) and φ(x) are the standard Q-function and the zero-mean and unit-variance Gaussian distribution, respectively.

## 3. PROPOSED SYSTEM

PROPOSED TRANSMIT ANTENNA SELECTION METHODS

In this section, we propose two new TAS schemes: leakagebased and Max-SR, and generalize the conventional EDAS method to the secure SM scenario. Then, we analyze the complexity for the three TAS methods. A. Proposed Leakage-Based Antenna Selection Method

Problem formulation: Similar to multi-user MIMO systems in [19], we view the receive power of confidential messages at Eve as the so-called leakage. Thus, the signalto-leakage-and-noise ratio (SLNR) for the nth channel of the kth pattern is defined as

$$SLNR_n(\mathbf{T}_k) = \frac{\beta_1^2 P_S \parallel \mathbf{H}\mathbf{T}_k\mathbf{e}_n \parallel^2}{\beta_1^2 P_S \parallel \mathbf{G}\mathbf{T}_k\mathbf{e}_n \parallel^2 + N_b\sigma_b^2}$$

It is assumed that all Nt transmit antennas of the selected pattern are activated with equiprobability to transmit confidential messages, then the optimization problem of maximizing SLNR (Max-SLNR) is expressed as

$$\begin{aligned} \max \quad & \sum_{n=1}^{N_t} SLNR_n(\mathbf{T}_k) \\ \text{subject to} \quad & \mathbf{T}_k \in \{\mathbf{T}_1, \mathbf{T}_2, ..., \mathbf{T}_Q\} \end{aligned}$$

with Tk being the optimization variable. The above optimization problem can be solved by exhaustive search, which calculates Nt SLNRs for each pattern. There are total Q patterns, so the complexity is O (QNt) floating-point operations (FLOPs).

To lower its complexity, the low-complexity implementation is necessary. 2) Low-complexity sorting-based solution: Considering all transmit antennas are uncorrelated, that is, each transmit antenna results in different SLNR, the optimization problem in (17) is equivalent to choose the largest Nt values from all N SLNRs. Once we calculate the SLNR values per transmit antenna, we simply arrange them in descending order by sorting method as follows.

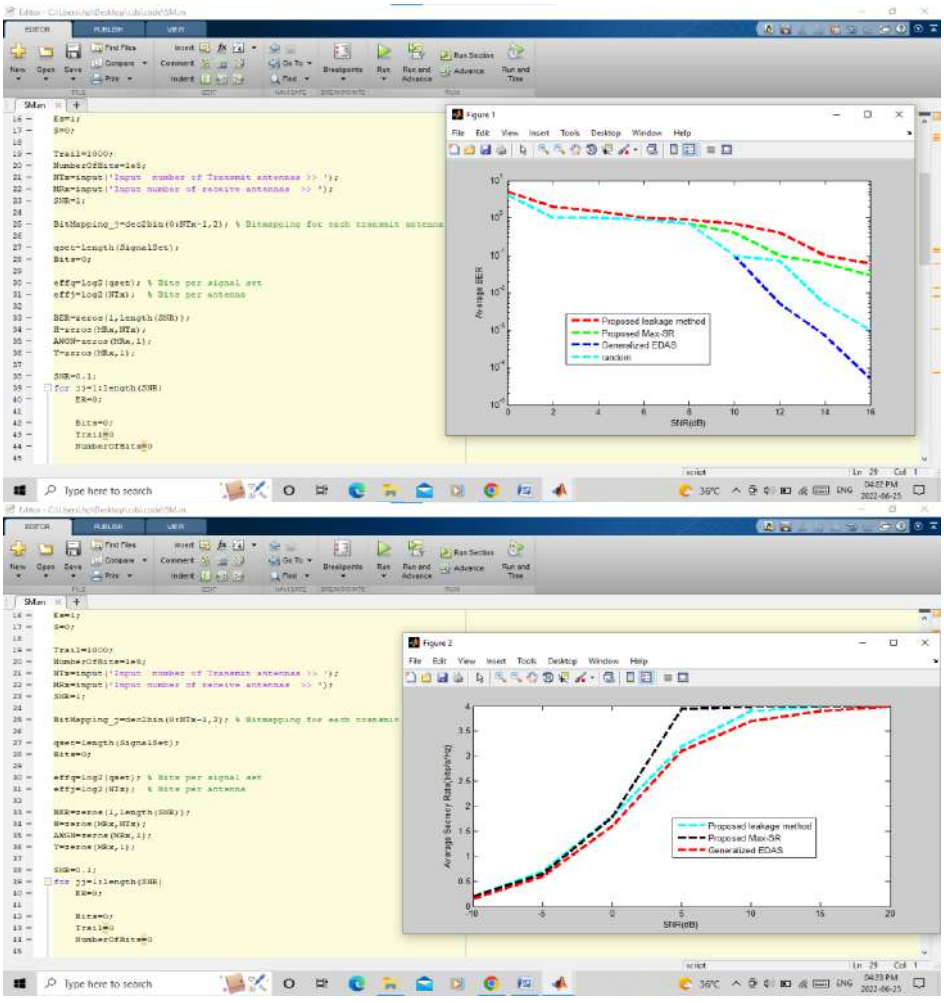
$$\underbrace{SLNR_{\pi_1} \geq SLNR_{\pi_2} \geq \cdots \geq SLNR_{\pi_{N_t}}}_{N_t \text{ selected antennas}} \geq \cdots \geq SLNR_{\pi_N} \tag{18}$$

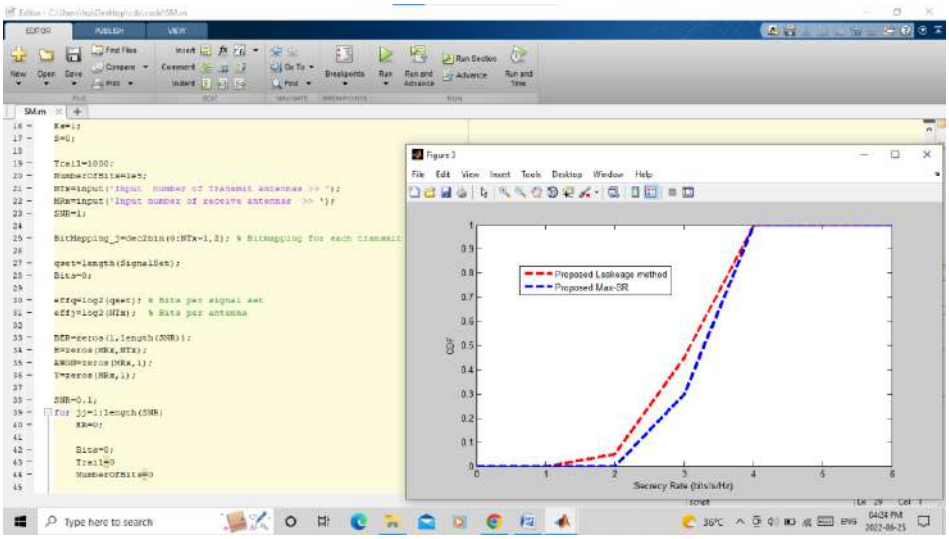
where {π1, π2, · · · , πN } is an ordered permutation of {1, 2, · · · , N} and SLNRπn is written as

$$SLNR_{\pi_n} = \frac{\beta_1^2 P_S \mathrm{tr}\left(\mathbf{h}_{\pi_n} \mathbf{h}_{\pi_n}{}^H\right)}{\beta_1^2 P_S \mathrm{tr}\left(\mathbf{g}_{\pi_n} \mathbf{g}_{\pi_n}{}^H\right) + N_b \sigma_b^2}$$

where hπn and gπn are the πnth column of H and G, respectively. The complexity is O (N) + O ( N logN 2 ) ≈ O ( N logN 2 ) , where O (N) and O ( N logN 2 ) are the complexities of calculating N SLNRs and sorting operation [20], respectively. Therefore, the sorting based solution is able to reduce the complexity without performance loss.

## 4. RESULTS AND DISCUSSION






## 5. CONCLUSION

TAS approaches in secure SM systems have been extensively studied in this work. Leakage-based and Max-SR TAS techniques were then suggested to increase SR performance, and the EDAS method was generalised to offer secure transmission. To attain an SR performance close to or equal to that of the suggested Max-SR approach while requiring significantly less complexity, the proposed leakage-based method was found to be superior in simulation results and complexity analysis to the other two TAS methods. The modified EDAS technique significantly beats the other two methods in terms of BER performance since it aims to maximise the minimal Euclidean distance, directly improving BER performance.

## REFERENCES

[1] R. Y. Mesleh, H. Haas, and S. Sinanovic, “Spatial modulation,” IEEE Trans. Veh. Technol., vol. 57, no. 4, pp. 2228–2241, 2008.

[2] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, “Spatial modulation: optimal detection and performance analysis,” IEEE Commun. Lett., vol. 12, no. 8, pp. 545–547, 2008.

[3] A. D. Wyner, “The wire-tap channel,” Bell System Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[4] J. Hu, F. Shu, and J. Li, “Robust synthesis method for secure directional modulation with imperfect direction angle,” IEEE Commun. Lett., vol. 20, no. 6, pp. 1084–1087, 2016.

[5] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, “Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems,” IEEE Access, vol. 4, no. 99, pp. 6614–6623, 2016.

[6] L. Liu, Y. Zhou, and V. Garcia, “Load aware joint comp clustering and inter-cell resource scheduling in heterogeneous ultra dense cellular networks,” IEEE Trans. Veh. Technol., vol. 67, no. 3, pp. 2741 – 2755, 2017.

[7] S. Gong, C. Xing, S. Chen, and Z. Fei, “Polarization sensitive array based physical-layer security,” IEEE Trans. Veh. Technol., vol. PP, no. 99, pp. 1–1, 2016.

[8] ——, “Secure communications for dual-polarized mimo systems,” IEEE Trans. Signal Process., vol. 65, no. 16, pp. 4177–4192, 2017.

[9] X. Guan, Y. Cai, and W. Yang, “On the secrecy mutual information of spatial modulation with finite alphabet,” International Conference on Wireless Communications and Signal Processing, pp. 1–4, 2013.

[10] L. Wang, S. Bashar, Y. Wei, and R. Li, “Secrecy enhancement analysis against unknown eavesdropping in spatial modulation,” IEEE Commun. Lett., vol. 19, no. 8, pp. 1351–1354, 2015.