SUBOPTIMAL FLUID ANTENNA SYSTEMS FOR MAXIMIZING THE SECRECY RATE WITH UNTRUSTED RELAYS

Tamer Mekkawy

Avionics Department, Military Technical College, Cairo, Egypt

ABSTRACT

This research examines the effectiveness of untrusted relays in fluid antenna-assisted communication systems subjected to arbitrary correlated fading channels. The transmitter is represented to share confidential information to a legitimate receiver,both utilizing a 1D Fluid Antenna System (FAS), while an untrusted relay, equipped with a fixed antenna, attempts to decrypt the intended message. In this case, cooperative jamming is adopted and we jointly optimize the power allocation of the transmitted jamming signal and the FAS beamforming weights to maximize the secrecy rate. Due to the non-convex nature of the optimization issue, we employ the Particle Swarm Optimization (PSO) approach to get the suboptimal secrecy rate. Ultimately, numerical results demonstrate that the use of FAS ensures more safe and reliable transmission, while an increase in FAS components produces more focused beams. This leads to improved alignment of the broadcast signal toward the legitimate receiver, increasing the necessary signal intensity while reducing leakage to unauthorized relays.

KEYWORDS

Beamforming, Cooperative jamming, Fluid Antenna System (FAS), Untrusted relay network.

1. INTRODUCTION

The market is elevated to unprecedented levels every decade by the emergence of a new generation of mobile communicators. The primary characteristics of Fifth Generation (5G) technology are the improvement of the experience quality. The objective is to enable universal connectivity with the emergence of 5G and the proliferation of Artificial Intelligence (AI). Concepts for the succeeding generation have been initiated beyond 5G and 6G [1]. Advanced technologies, such as AI-driven network optimization and quantum communication, will improve signal stability. 6G allows for unparalleled device density of over 10 million per square kilometer [2], allowing IoT deployments, smart cities, and real-time holographic communications.

The novel Reconfigurable Intelligent Surface (RIS) technology facilitates the 6G wireless air interface, anticipated to employ Multiple-Input Multiple-Output (MIMO) system [3]. Although, its brilliance, MIMO is a suitable solution, particularly regarding the challenges of acquiring the precoding matrix and the overhead due to Channel State Information (CSI). Notwithstanding the theoretical simplicity of massive MIMO [4], 5G utilizes a more intricate code book precoding technique that leverages quantized CSI [5].Recent recommendations in [6]– [12] suggested that this may be achievable through innovative fluid antenna technology.

Contemporary advancements in flexible antenna technology inspired the notion of FAS. These antennas are liquid based or reconfigurable pixel-based [6]. Other configurations of flexible antenna systems can also be constructed, including those utilizing meta-materials [7]. The authors

DOI:10.5121/ijwmn.2025.17101

of [8] described many types of fluid antennas that are frequently employed in mobile communications. FAS seems to have a bright future as a useful technology. FAS offers an innovative methodology that enhances and surpasses MIMO. Current FAS efforts are examining the potential of the switchable antenna for boosting the cellular communication network efficiency [9]. The rate of the received FAS at the level crossing was later calculated using a closed-form method [10]. The research detailed in [11] was expanded to include Nakagami fading channels.

The researchers contemplated activating several ports of a fluid antenna and amalgamating signals to enhance Terahertz communications and further augment performance. A jointly correlated channel model for the spatial correlation of FAS ports was developed in [12]. In [13], the authors built a model for the general multipath channel in the FAS design by integrating amplitude and phase from each of the various channel routes with farfield situations. The capacity of a FAS was explored in [14] by concurrently adjusting the positions of the FAS.

Recently, FAS was employed to increase the secrecy performance for wiretap channel. An analytical calculation for secrecy energy efficiency and secrecy outage probability (SOP) were described in [15]. Then, the antenna position for FAS was adopted to achieve higher security and covert communications [16].By jointly augmenting the transmitter beamforming with noise uncertainty for maximizing the sum covert rate was calculated in [17].In contrast, Wyner's original innovative research on wiretap channels attracted a lot of interest in physical layer security [18]. Therefore, with numerous cooperative nodes, Amplify and Forward (AF) relay approach has been devised in [19] to increase the secrecy rate, then the cooperative jamming has been utilized to weaken the wiretap channel [20]. In [21], the authors proved that, seeking collaboration with untrusted relay may increase the secrecy rate rather than only view it as a possible eavesdropper.

1.1. Motivation

Secure communication presents a significant challenge in wireless networks. Conventional MIMO systems are extensively utilized to improve secrecy rates through beamforming and diversity; however, they encounter limitations in highly dynamic or adversarial settings. FAS facilitates the dynamic selection of antenna positions (fluid elements) based on real-time channel conditions [16]. This adaptability can optimize the secrecy rate by diminishing the eavesdropper's channel quality while enhancing that of the legitimate user. Furthermore, in contrast to fixed MIMO configurations, FAS offers superior spatial diversity due to the continuous tunability of its fluid elements, allowing for better utilization of channel randomness, particularly in the presence of eavesdroppers. Additionally, FAS can be implemented in compact systems where traditional MIMO configurations are impractical due to size constraints, making it suitable for IoT devices or UAVs that require secure communication.

1.2. Contributions

In this paper, two users try to transmit information across an untrusted relay; each user is supplied with FAS to better orient the delivered signal toward the genuine receiver by enhancing the desired signal intensity while reducing leakage to the untrusted relay. In specifically, we presented a suboptimal combined FAS beamforming weight and power allocation for the jamming signal in order to improve the secrecy rate. Because the relay is regarded untrusted, there is no weight constraint to boost secure performance. The total secrecy rate is computed using non-convex logarithmic differences, since the secrecy rate involves logarithmic functions that are not linear. To handle this complex problem, Particle Swarm Optimization (PSO) is used, which resolves optimization challenges by progressively enhancing a candidate solution according to a specified fitness function. The suggested method aims to enhance the secure rate by broadcasting both the secret signal and the cooperative jamming signal.

The remainder of the paper is organized as follow: Section 2 describes the system model for FAS adopted for untrustedrelay network. In Section 3, the proposed beamforming weights and power allocation are calculated. In Section 4, the SOP is discussed for the suboptimal weights. Section 5 validates the accuracy and efficiency of the proposed approach and provides numerical data showing the effect of antenna arrangement. Finally, Section 6concludes the paper.

2. System Model

In this research, we take into consideration the transmission of cooperative jamming relay network, the system model of which is depicted in Figure 1. Alice (A), Bob (B), and an untrusted AF relay (R) are the components that make up the system. Ris equipped with a single antenna, whilst Aand Bare outfitted with a 1D FAS, N, preset places (i.e., ports), which are uniformly spread throughout a space of $W\lambda$, where λ denotes the wavelength of the carrier frequency. More precisely, a grid structure is proposed for the FAS ensuring that N ports are equally spaced over a linear region of length $W\lambda$, as shown in Figure 2. Apart from that, A and B can only change their FAS to one active port to optimize their beamforming weights in order to achieve the highest possible level of secrecy [15], by adjusting the positions of fluid antennas, which are connected to N radio frequency chains.

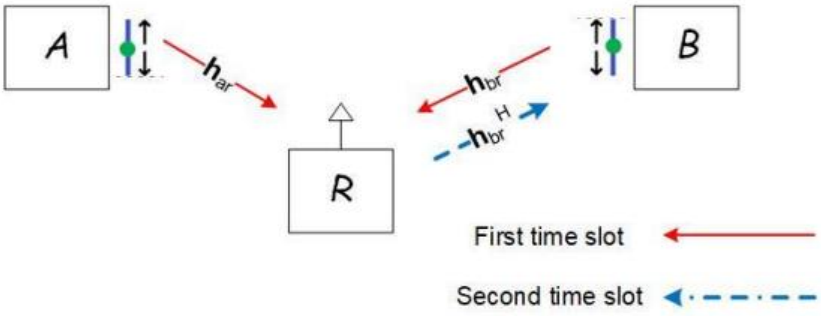


Figure 1.Secured transmission in a two-hop untrusted-relay network.

Because of the significant route loss or the impediments, there is no direct communication link between A and B. Thus, the transmission takes place in two different time slots to ensure that the communication is secured. Within the first phase, A is responsible for transmitting the confidential signals,x_a,to R. Simultaneously, Bis responsible for transmitting the jamming signal,x_j,to R. At the second phase, R transmits the combined signals that have been received to B. This occurs after the signals have been amplified using a constant amplification factor, $\sqrt{\beta}$. In addition, it is assumed that all of the wireless channels are time-varying Rayleigh fading. Furthermore, the noise that is received at every node is treated as an Additive White Gaussian Noise (AWGN) with zero mean and Power Spectrum Density (PSD) N_0. By assuming the channel vector gains from A to R, from B to R, and from Rto B, respectively, by the symbols $\boldsymbol{h}_{ar}$, $\boldsymbol{h}_{br}$, and $\boldsymbol{h}_{rb}^{\mathrm{T}}$. Furthermore,

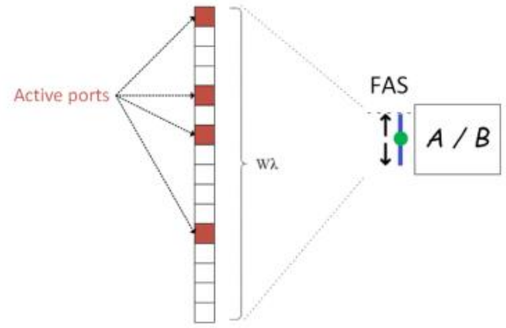


Figure 2.Schematic of a fluid antenna system.

we make the assumption that the channels are in accordance with the reciprocity theorem [20], which states that $\boldsymbol{h}_{br}$is equal to $\boldsymbol{h}_{rb}^{\mathrm{T}}$, where $\boldsymbol{h}_{br}$is a close approximation of$N(0, \sigma_{br}^2)$. During the first phase, the signal that is received at Ris denoted by the expression,y_r.

$$y_r = \sqrt{P_a}\boldsymbol{h}_{ar}\boldsymbol{w}_a x_a + \sqrt{P_j}\boldsymbol{h}_{br}\boldsymbol{w}_b x_j + n_r \tag{1}$$

where, $P_a$and P_j represent the transmitted power by Aand B, respectively; $\boldsymbol{w}_a$and $\boldsymbol{w}_b$are FAS beamforming weights at A and B, respectively; n_r signifies AWGN at R; x_a and $x_j$are independent variables, and each possessing unit power. Assume $\boldsymbol{w}_a = [a_1, a_2, \ldots., a_N]^{\mathrm{T}}$and $\boldsymbol{w}_b = [b_1, b_2, \ldots., b_N]^{\mathrm{T}}$such that $a_i = n_i e^{j\theta_i}$and $b_i = m_i e^{j\theta\varphi_i}$. We denote the total power transferred via Aand Bas P, with $\alpha \in [0,1]$representing the power allocation factor. In this scenario, Aconveys its confidential signal with power $P_a = \alpha P$, whereas Bemits its jamming signal with power $P_j = (1-\alpha)P$. Consequently, the instantaneous Signal-to-Interference-plus-Noise Ratio (SINR) at R, denoted as γ_r, may be expressed as

$$\gamma_r = \frac{\alpha P \|\boldsymbol{h}_{ar}\boldsymbol{w}_a\|^2}{(1-\alpha)P\|\boldsymbol{h}_{br}\boldsymbol{w}_b\|^2 + N_0} \tag{2}$$

During the second phase, the relay amplifies y_r by a factor of β prior to retransmission. Numerous studies have examined the amplification value of relays, demonstrating that the variable amplification gain, which depends on instantaneous channel gains, results in increased efficiency [19]. This aspect is not within our scope, as we regard the relay as an untrusted entity. The signal received at Bvia the untrusted relay,R,is

$$y_b = \sqrt{\beta} y_r \boldsymbol{h}_{br}\boldsymbol{w}_b + n_b \tag{3}$$

where $n_b$represents the AWGN received at B. Given that x_j represents the jamming signal transmitted by Bin the preceding phase, thus the self-interference termcan be completely eliminated when Bpossesses perfect CSI. Therefore, the instantaneous SINR at B, is defined as

$$\gamma_b = \frac{\beta\alpha P\, \|\boldsymbol{h}_{ar}\boldsymbol{w}_a\|^2 \|\boldsymbol{h}_{br}\boldsymbol{w}_b\|^2}{\beta N_0 \|\boldsymbol{h}_{br}\boldsymbol{w}_b\|^2 + N_0} \tag{4}$$

Thus, the instantaneous secrecy rate [19] is defined as

$$R_s = \frac{1}{2}[\log_2(1+\gamma_b) - \log_2(1+\gamma_r)]^+ \tag{5}$$

where the pre-log factor 0.5 because two stages are necessary to complete the transmission, and $[.]^+ = \max[.,0]$. In this paper, maximizing the secrecy rate is defined by jointly optimizing the FAS beamforming for both A and Band the power allocation factor, α. Based on (5), the objective problem can be mathematically formulated as:

$$\begin{aligned} &\max_{\boldsymbol{w}_a,\boldsymbol{w}_b,\alpha} \; R_s \\ \textbf{s.t.:}\quad &\alpha \in [0,1] \\ &\|\boldsymbol{w}_a\|^2 = 1 \\ &\|\boldsymbol{w}_b\|^2 = 1 \end{aligned} \tag{6}$$

As represented in (6), the secrecy rate incorporates logarithmic functions, which are non-linear. Despite the fact that logarithms are concave functions, the total secrecy rate is based on non-convex logarithmic discrepancies. The beamforming weight constraints are typically quadratic or nonconvex function. To find suboptimal solutions in this nonconvex setting, some specialized optimization techniques such as alternating optimization, convex relaxation, or metaheuristic algorithms are usually required.

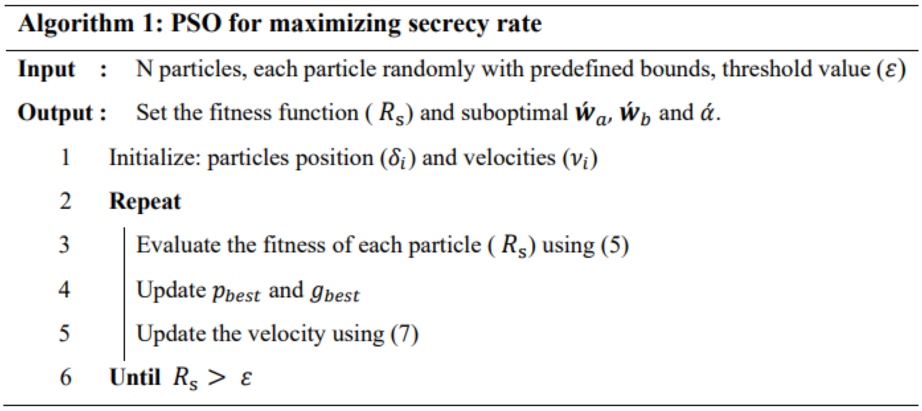
3. Partical Swarm Optimization for Maximizing the Secrecy Rate

A metaheuristic algorithm is employed to address the complex optimization problem presented. These metaheuristic algorithms represent advanced optimization methods aimed at effectively navigating extensive search spaces. Practically, metaheuristic algorithms are applicable to a diverse range of problems, particularly those that are non-convex, nonlinear, or possess multiple local optima. PSO is one of the metaheuristic optimization methods that utilizes a population-based approach, drawing inspiration from the collective behaviour observed in bird flocking and fish schooling. It is employed to address optimization problems through the iterative enhancement of a candidate solution based on a specified quality measure, referred to as a fitness function.

The PSO Algorithm consists of three primary steps: Initially, each particle serves as a candidate solution. The FAS weights, denoted as $[\boldsymbol{w}_a, \boldsymbol{w}_b, \alpha]$, are defined as random vectors subject to constraints on their amplitude and phase, with α assumed to be within valid power limits. Initial velocities for all particles in each dimension are assigned randomly. The secrecy rate, R_s, is calculated based on these initializations, serving as the fitness function in PSO for each particle.Secondly, the iterative optimization step involves comparing the current fitness (R_s) of each particle with its best-known fitness. Should the current $R_s$demonstrate improvement, theparticles best position, p_{best}, should be updated to reflect the current position. Identify the particle exhibiting the highest secrecy rate within the population and update the global best, denoted as g_{best}. The velocity is subsequently updated using:

$$v_i = \omega . v_{i-1} + c_1 . r_1 . (p_{best} - \delta_i) + c_2 . r_2 . (g_{best} - \delta_i) \tag{7}$$

where, $v_i$represents the velocity of the *i*-th particle, ωdenotes the inertia weight, and $\delta_i$indicates the current position of the *i*-th particle. The parameters $c_1$and $c_2$are the acceleration coefficients, while $r_1$and $r_2$are random values generated viaan uniform distribution. Subsequently, the positions of all particles, $\boldsymbol{w}_a, \boldsymbol{w}_b, \alpha$ are updated. The algorithm terminates if the convergence criteria are satisfied; otherwise, it proceeds to the next iteration. The third step involves determining the suboptimal solution for the positions of all particles, $\acute{\boldsymbol{w}}_a, \acute{\boldsymbol{w}}_b$ and $\acute{\alpha}$. Ultimately, the optimal secrecy rate is attained as represented in Algorithm 1.



Algorithm 1: PSO for maximizing secrecy rate

```
Input  :  N particles, each particle randomly with predefined bounds, threshold value ($\varepsilon$)
Output :  Set the fitness function ( $R_s$) and suboptimal $\acute{\boldsymbol{w}}_a$, $\acute{\boldsymbol{w}}_b$ and $\acute{\alpha}$.
Initialize: particles position ($\delta_i$) and velocities ($\nu_i$)
Repeat
    Evaluate the fitness of each particle ( $R_s$) using (5)
    Update $p_{best}$ and $g_{best}$
    Update the velocity using (7)
Until $R_s > \varepsilon$
```

4. SECRECY OUTAGE PROBABILITY

SOP is implemented by secure wireless communication systems to quantify the likelihood of failing to maintain a specified secrecy rate. In other words, it shows how likely it is that an untrusted relay will be able to decrypt data sent over a legal channel. Both the legal and eavesdropping channels' signal quality influences SOP. When the gap between the capacities of the legal and untrusted relay channels drops below a certain threshold, the SOP is defined as:

$$SOP = \mathbb{P}(R_s < \bar{R}) \tag{8}$$

Where $\mathbb{P}$ is the probability and $\bar{R}$ is the target secrecy rate. Utilizing statistical models of the channels allows for the evaluation of SOP. The channels' instantaneous SNRunder Rayleigh fading, for instance, has an exponential distribution. In order to determine the SOP, it is necessary to integrate over the probabilities of various untrusted relay channel circumstances, where the likelihood of the legal channel failing to preserve the necessary secrecy is weighted. Thus, SOP can be defined as:

$$\begin{aligned} SOP = {} & \mathbb{P}\left(\frac{1+\gamma_b}{1+\gamma_r} < 2^{\bar{R}}\right) \\ & = \mathbb{P}\left(\gamma_b < 2^{\bar{R}}(1+\gamma_r) - 1\right) \end{aligned} \tag{9}$$

Because we need to compute the probability that γ_b falls below the threshold $2^{\bar{R}}(1+\gamma_r) - 1$ for each value of γ_r, thus the Cumulative Distribution Function (CDF) of γ_b is $\mathrm{F}_{\gamma_b}(y) = \mathbb{P}(\gamma_b \leq y) = 1 - e^{y/\bar{\gamma}_b}$, where $\bar{\gamma}_b$denotes average SNR of the legitimate channel. Also, Probability Density Function (PDF) of $\gamma_r$as an exponential distribution as $f_{\gamma_r}(x) = \frac{1}{\bar{\gamma}_r} e^{x/\bar{\gamma}_r}$, where the average SNR of the untrusted relay channel is$\bar{\gamma}_r$. Based on the suboptimal values of $\acute{\boldsymbol{w}}_a$,$\acute{\boldsymbol{w}}_b$ and $\acute{\alpha}$ obtained using PSO in Section 3, and substituting them in (2) and (4),the SOP is calculated as:

$$SOP = \int_0^\infty \mathrm{F}_{\acute{\gamma}_b}\left(2^{\bar{R}}(1+x) - 1\right) f_{\acute{\gamma}_r}(x)\, dx \tag{10}$$

following a series of calculations and direct substitutions

$$SOP = \int_0^\infty \frac{1}{\bar{\gamma}_r} e^{x/\bar{\gamma}_r}\ dx - \int_0^\infty e^{-\left(2^{\bar{R}}(1+\gamma_r)-1\right)/\bar{\gamma}_b} \frac{1}{\bar{\gamma}_r} e^{x/\bar{\gamma}_r}\ dx \tag{11}$$

The first integral in (11) evaluates to 1, since it has the whole probability density, using standard integral $\int_0^\infty e^{Ax}\ dx = \frac{1}{A}\ \forall\ A > 0$, therefore SOP may be expressed as:

$$SOP = 1 - \frac{e^{-\left(2^{\bar{R}}-1\right)/\bar{\gamma}_b}}{\bar{\gamma}_r\left(\frac{2^{\bar{R}}}{\bar{\gamma}_b}+\frac{1}{\bar{\gamma}_r}\right)} \tag{12}$$

The SOP falls exponentially with an increase in the average SNR, $\bar{\gamma}_b$. Therefore, a greater SNR at B enhances secrecy performance. The denominator has $\bar{\gamma}_r$, suggesting that as the untrusted relay's SNR grows, SOP lowers, resulting in improved secrecy. The term$2^{\bar{R}}$inside the formula demonstrates that as $\bar{R}$increases, SOP degrades. This is because a greater secrecy rate need makes it more difficult to maintain secrecy.

5. Simulation Results and Discussions

This section presents numerical simulations of the proposed optimization algorithm, along with a comparative analysis. Let us assume that the components of $\mathbf{h}_{ar}$and $\mathbf{h}_{br}$are independent and distributed complex Gaussian characterized by a mean of zero and a variance of one. Each figure is based on 10^5independent realizations. We consider the total power transmitted from both users Aand Bto be P. Furthermore, the SNR is modified by the transmitted power P. The equivalent SNR is defined as $P/N_0$to assess system performance, the carrier frequency used is2.4 GHz, the convergence threshold for the proposed PSO is adjusted to be $10^{-4}$and the minimum inter-antenna distance for FAS is $D = \lambda/2$.

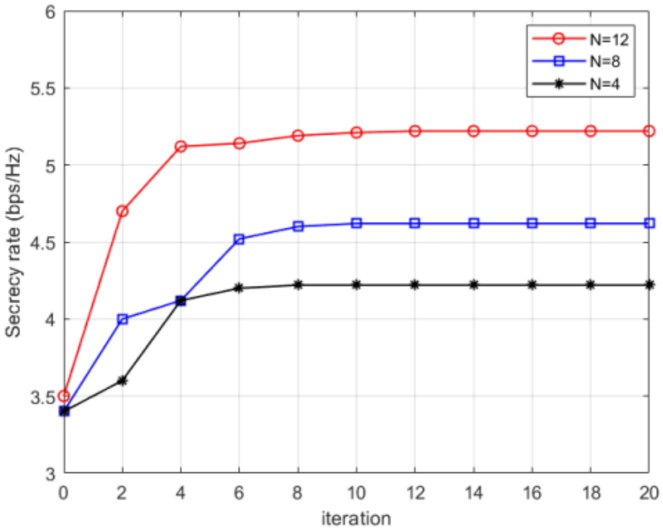


Figure 3.Convergence of proposed algorithm with different N at P =30 dBm.

Figure 3 represents the convergence of the proposed PSO with various FAS N elements when P = 30dBm. As previously anticipated, the secrecy rate rises as the numberof FAS components increases. This is because having a larger number of N enhances beamforming precision, resulting in greater interference suppression and signal amplification. As illustrated, the proposed algorithm converges in 10-15 iterations, indicating higher efficiency. Furthermore, convergence occurs faster with lower N. Moreover, upon convergence, the secrecy rate achieves a peak, suggesting that the algorithm has successfully found the optimal solution within the limitations.

Increasing the number of FAS components improves the secrecy rate through enhanced beamforming and geographic variety, as seen in Figure 3. However, this enhancement is at the expense of increasing computational complexity and hardware needs. Higher numbers need more processing power and circuitry, resulting in increased system delay and energy usage. Higher leads to significant performance increases, but beyond a certain point, the increase in secrecy rate becomes minimal relative to the growth in complexity. This emphasizes the trade-off between performance and cost, forcing a compromise based on system restrictions and application needs.

Figures 4 and 5 compare the secrecy rate of the proposed algorithm to other Position Antenna (PA) techniques for FAS, as a function of transmit power P for $N = 6$and $N = 8$, respectively. The suboptimal PA reflects our proposed algorithm's secrecy rate. This strategy uses suboptimal selection of $\boldsymbol{w}_a$,$\boldsymbol{w}_b$ and α, resulting in the maximum secrecy rate at all power levels. Equal PA [17] and Random PA depict FAS in which Ncomponents are weighted equally and randomly, respectively. While equal PA outperforms random selection, it does not completely harness since the random configuration is unlikely to match the ideal channel circumstances, resulting in diversity, resulting in a modest gain in secrecy rate. Random PA yields the lowest secrecy ratewasteful use of the FAS. The difference between the suboptimal PA and the others emphasizes the significance of optimizing weight selection and power distribution for higher secrecy rates.

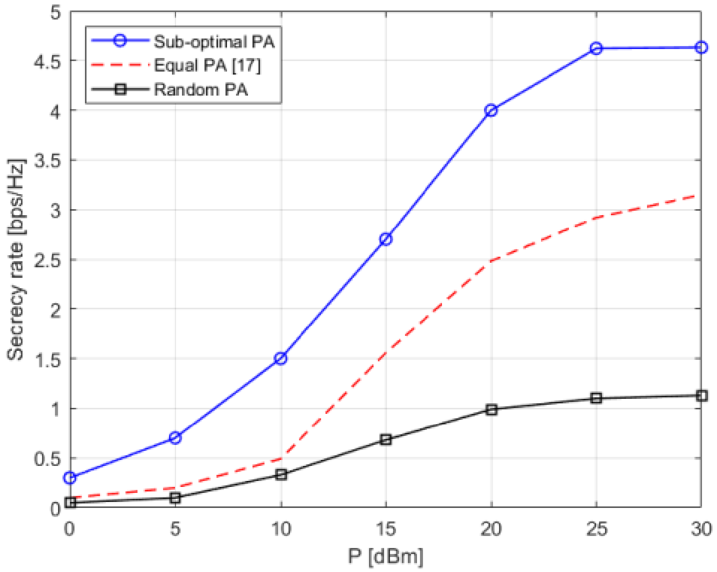


Figure 4.The maximum transmits power P versus the secrecy rate with N =8

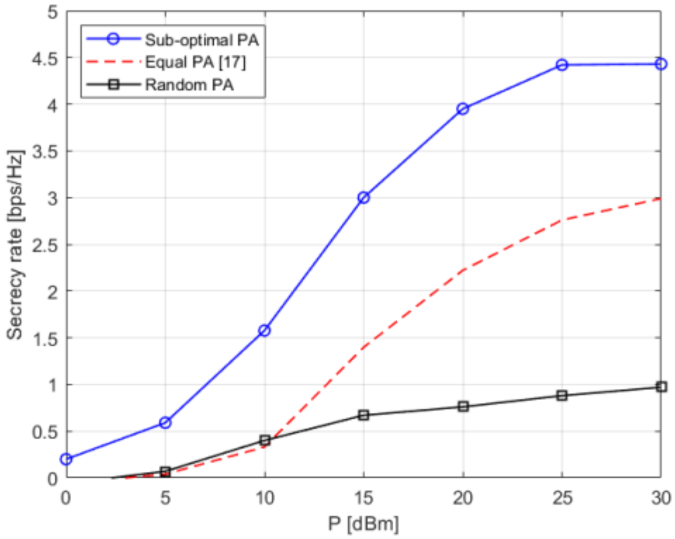


Figure 5.The maximum transmits power P versus the secrecy rate with N =6.

Ultimately, when the quantity of components in FAS escalates, the system is capable of generating smaller and more concentrated beams. This results in enhanced alignment of the broadcast signal towards the genuine receiver, augmenting the required signal strength while minimizing leakage to untrusted relays. It offers greater flexibility in modifying the amplitude and phase of the signal, leading to a more potent and focused beam. The FAS can more efficiently eliminate interference at untrusted relays with an increased number of components. This indicates that the system can direct energy to the authorized channel while suppressing the untrusted relay channel.

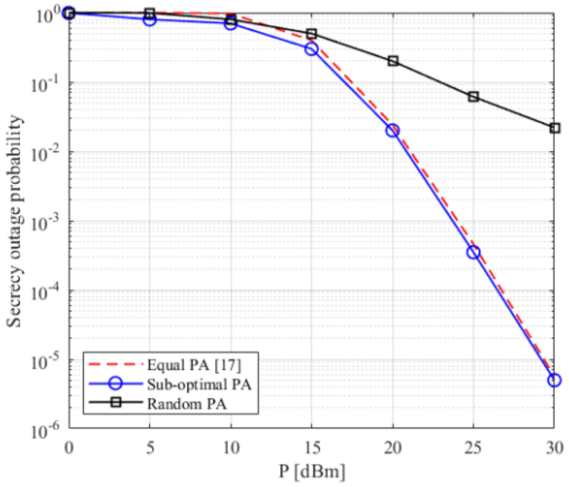


Figure 6.SOP versus P with $\bar{R}$ = 2 bps/Hz

To show how likely the untrusted relay will be able to decrypt data sent over a legal channel. Figure 6 discusses the secrecy outage probability versus P for different schemes, when target secrecy rate $\bar{R} = 2$ bps/Hz. At a reduced power level All schemes yield a high SOP (approximately 1). This suggests that the legitimate receiver's signal intensity is insufficient in comparison to that of the untrusted relay, making it challenging to maintain secrecy at low power.

The efficiency disparity between the schemes becomes apparent when P is set to 10 to 20 dBm. The suboptimal PA scheme begins to outperform the equal and random PA schemes by more effectively utilizing the available power. Despite the fact that the SOP for all schemes decreases at high P, the suboptimal PA maintains the greatest performance, approximating near-zero SOP. The random PA scheme continues to be subpar, indicating that it is unable to effectively leverage the increased transmit power for secrecy. The most effective PA is suboptimal. This strategy reduces the likelihood of secrecy outages across a broad spectrum of transmit powers by dynamically adjusting power allocation to optimize secrecy. Equal PA [17] provides a reasonable level of performance while maintaining simplicity: Although it is not as effective as suboptimal PA, it is simpler to implement and outperforms random PA.

6. CONCLUSIONS

Under arbitrarily correlated fading channels, this study examines the performance of untrusted relay in fluid antenna-aided communication systems. In this scenario, a trustworthy transmitter tries to send sensitive data to an authorized receiver using a 1D fluid antenna system (FAS), while an unreliable relay with a single fixed antenna tries to decipher the message. In this case, we optimize the secret rate by coordinating the transmission jamming signal's power distribution with the FAS beamforming weights. We apply the particle swarm optimization method to get a not ideal secrecy rate as the optimization issue is non-convex. Increasing the number of FAS elements results in more focused beams, and numerical findings show that FAS can ensure more secure and dependable transmission. This improves the broadcast signal's alignment towards the real receiver, which increases the needed signal intensity and reduces signal leakage to untrusted relays. As the number of components in the FAS increases, it becomes more efficient at eliminating interference at untrusted relays. This proves that the system is able to block the untrusted relay channel while directing power to the authorized one.

REFERENCES

[1] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[2] N. Docomo, "White paper: 5G evolution and 6G," *Accessed on*, vol. 1, 2020.

[3] Z. Wang, J. Zhang, H. Du, E. Wei, B. Ai, D. Niyato, and M. Debbah, "Extremely large-scale MIMO: Fundamentals, challenges, solutions, and future directions," *IEEE Wireless Communications*, 2023.

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

[5] D. A. Urquiza Villalonga, H. OdetAlla, M. J. Fernandez-Getino, and A. Flizikowski, "Spectral efficiency of precoded 5G-NR in single and multi-user scenarios under imperfect channel knowledge: A comprehensive guide for implementation," *Electronics*, vol. 11, no. 24, p. 4237, 2022.

[6] Y. Huang, L. Xing, C. Song, S. Wang, and F. Elhouni, "Liquid antennas: Past, present and future," *IEEE Open Journal of Antennas and Propagation*, vol. 2, pp. 473–487, 2021.

[7] M. C. Johnson, S. L. Brunton, N. B. Kundtz, and J. N. Kutz, "Sidelobe cancelling for reconfigurable holographic metamaterial antenna," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 4, pp. 1881– 1886, 2015.

[8] K.-K. Wong, K.-F. Tong, Y. Shen, Y. Chen, and Y. Zhang, "Bruce lee-inspired fluid antenna system: Six research topics and the potentials for 6G," *Frontiers in Communications and Networks*, vol. 3, p. 853416, 2022.

[9] K.-K. Wong, A. Shojaeifard, K.-F. Tong, and Y. Zhang, "Fluid antenna systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1950–1962, 2020.

[10] P. Mukherjee, C. Psomas, and I. Krikidis, "On the level crossing rate of fluid antenna systems," in *2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC)*. IEEE, 2022, pp. 1–5.

[11] L. Tlebaldiyeva, G. Nauryzbayev, S. Arzykulov, A. Eltawil, and T. Tsiftsis, “Enhancing QoS through fluid antenna systems over correlated Nakagami-m fading channels,” in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2022, pp. 78–83.

[12] M. Khammassi, A. Kammoun, and M.-S. Alouini, “A new analytical approximation of the fluid antenna system channel,” *IEEE Transactions on Wireless Communications*, vol. 22, no. 12, pp. 8843–8858, 2023.

[13] L. Zhu, W. Ma, and R. Zhang, “Modeling and performance analysis for movable antenna enabled wireless communications,” *IEEE Transactions on Wireless Communications*, 2023.

[14] W. Ma, L. Zhu, and R. Zhang, “MIMO capacity characterization for movable antenna systems,” *IEEE Transactions on Wireless Communications*, 2023.

[15] F. R. Ghadi, K.-K. Wong, F. J. Lopez-Martinez, W. K. New, H. Xu, and C.-B. Chae, “Physical layer security over fluid antenna systems: Secrecy performance analysis,” *IEEE Transactions on Wireless Communications*, 2024.

[16] J. Yao, L. Xin, T. Wu, M. Jin, K.-K. Wong, C. Yuen, and H. Shin, “FAS for secure and covert communications,” *arXiv preprint arXiv:2411.09235*, 2024.

[17] H. Mao, X. Pi, L. Zhu, Z. Xiao, X.-G. Xia, and R. Zhang, “Sum rate maximization for movable antenna enhanced multiuser covert communications,” *IEEE Wireless Communications Letters*, 2024.

[18] A. D. Wyner, “The wire-tap channel,” *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[20] R. Yao, T. Mekkawy, and F. Xu, “Optimal power allocation to increase secure energy efficiency in a two-way relay network,” in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1–5.

[21] C. Jeong, I.-M. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system,” *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2011.

AUTHOR

Tamer Mekkawy was born in Cairo, Egypt, in1983. He received the B.Sc. and M.Sc. degreesin electrical engineering from Military TechnicalCollege (MTC), Cairo, Egypt, in 2006,and 2014, respectively, and the Ph.D. degreefrom the School of Electronics and Information(SEI), Northwestern Polytechnical University,Xi’an, China in 2018. He is currentlya Lecture with the Department of Avionics, Military Technical College (MTC),Cairo, Egypt. His research interests include cooperative communication,physical layer security, wireless-powered communication systems, andlocalization in wireless networks.