Fluid Antenna Enabling Secret Communications

Boyi Tang, Hao Xu, *Member, IEEE,* Kai-Kit Wong, *Fellow, IEEE,* Kin-Fai Tong, *Fellow, IEEE,*
Yangyang Zhang, and Chan-Byoung Chae, *Fellow, IEEE*

***Abstract*—Recent researches have revealed that fluid antenna, a new position-switchable antenna technology, can make use of the spatial moments of deep fades of the interference signal occurred naturally due to multipath for multiple access. In this letter, this phenomenon is exploited in a physical layer security setup where a base station (BS) transmits an information-bearing signal to a legitimate user and an artificial noise (AN) signal to a potential eavesdropper while the user is equipped with a fluid antenna to overcome the AN signal. The proposed approach needs no effort from the base station (BS) to avoid the AN signal from harming the legitimate user. Trying to enhance the secrecy rate, we study the power allocation of the information-bearing and AN signals if the channel state information (CSI) is available at the BS. Both perfect and imperfect CSI scenarios are investigated. Simulation results demonstrate that the proposed system, with a single fluid antenna with one radio-frequency (RF) chain at the user, achieves the secrecy rate that is achievable by the user utilizing maximal ratio combining (MRC) with many antennas instead, and is the only approach robust to CSI uncertainties of the eavesdropper, requiring no power allocation nor beamforming at the BS.**

***Index Terms*—Artificial noise, Fluid antenna system, Physical layer security, Power allocation, Secrecy rate.**

I. Introduction

MANY technologies have been invented as wireless communications advances to deliver never-enough capacity and quality-of-experience under precious energy and spectral resources. In the physical layer, multiple-input multiple-output (MIMO) systems have been the core enabling technology that transforms mobile communications. For the fifth generation (5G), MIMO with huge numbers of antennas, widely referred to as massive MIMO, are relied upon to deliver the anticipated improvements [1]. Towards the sixth generation (6G), many predict that MIMO will shine [2] and there is already a notion of extra-large MIMO emerging to scale up the benefits even further [3]. It is worth mentioning that non-orthogonal multiple access (NOMA), e.g., [4] and reconfigurable intelligent surface (RIS), e.g., [5] are two other key technologies that are being pushed through in the 6G cycle. Nevertheless, like multiuser MIMO, NOMA and RIS are not simple solutions. They come with heavy computational efforts, not to mention the signaling overheads that acquire the channel state information (CSI).

On the other hand, wireless communications is regarded as a less secure medium because it exposes to eavesdroppers. In the physical layer, if we know the CSI of the eavesdropper, then base station zero-forcing (BSZF) will be absolutely effective; otherwise, artificial noise (AN) will be required [6]. Evidently, NOMA faces additional security threats as an untrusted user equipment (UE) may decode other users' data [7].

Motivated by the limitations of existing approaches, our goal is to develop a secure wireless communication system without the hassles of CSI acquisition[1] and beamforming optimization at the base station (BS) while also keeping the legitimate UE's receiver simple. Our approach is built upon the emerging fluid antenna technology that makes possible a position-switchable antenna to be deployed at the UE [8]. In the antenna community, fluid antenna including liquid-based antennas, e.g., [9]–[11] and reconfigurable pixel-based antennas, e.g., [12]–[14], has been around for decades. However, efforts using fluid antennas to improve wireless communications systems emerge only recently [15]–[23]. Of particular relevance to physical layer security is the merit of using fluid antennas for multiuser communication. Using a fluid antenna, the UE can access the deep fade of interference occurred naturally in the environment for multiuser communication, as illustrated in [20]–[23].

In this letter, this capability is exploited in the physical layer security setting where AN is utilized to secure the information from a potential eavesdropper with either no or uncertain CSI of the eavesdropper. The use of fluid antenna at the legitimate UE is highly motivated because it enables the UE to avoid the AN signal. The system becomes simple. The BS can now use one antenna to send the information-bearing signal to the UE and another antenna to transmit the AN signal to confuse the eavesdropper, without using BSZF nor the need of CSI.

Technically, we will investigate if the proposed system can match the secrecy rate performance of one that uses the CSI at the BS to optimize the BSZF or the power allocation between the information-bearing signal and the AN signal when BSZF is not adopted. Moreover, we will also compare the proposed system with one that uses maximal ratio combining (MRC) at the UE with many fixed antennas. In doing so, we will obtain the optimal power allocation for both scenarios of perfect and imperfect CSI. In the latter case, we consider bounded errors and use a lower bound of the secrecy rate for the optimization. Our key findings are summarized as follows:

- For typical signal-to-noise ratio (SNR) values, the power allocation over the information-bearing and AN signals only has a small gain in the secrecy rate for the proposed system though more gain appears if the SNR is extremely large. This indicates that the proposed system can work without the power allocation, hence no CSI at the BS.
- Optimal power allocation over the information-bearing and AN signals is important for the system with the UE

The work of Wong and Tong is supported by the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/W026813/1. For the purpose of open access, the authors will apply a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

The work of C. B. Chae is supported by the Institute of Information and Communication Technology Promotion (IITP) grant funded by the Ministry of Science and ICT (MSIT), Korea (No. 2021-0-02208, No. 2021-0-00486).

B. Tang, H. Xu, K. K. Wong and K. F. Tong are with the Department of Electronic and Electrical Engineering, University College London, Torrington Place, United Kingdom. *Corresponding author:* kai-kit.wong@ucl.ac.uk.

Y. Zhang is with Kuang-Chi Science Limited, Hong Kong SAR, China.

K. K. Wong and C. B. Chae are with School of Integrated Technology, Yonsei University, Seoul, Korea.

[1] CSI estimation at the UE is still needed for coherent reception but the aim is to eliminate the need of CSI feedback to the BS.

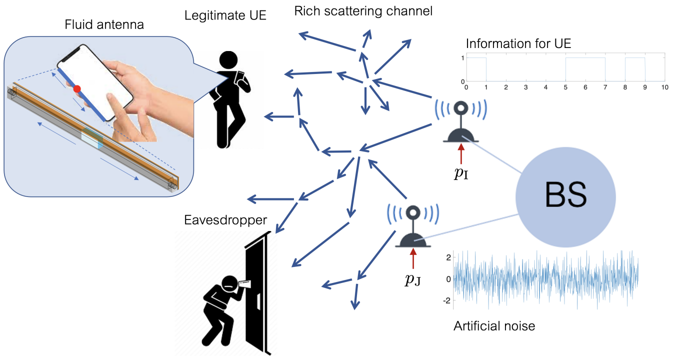

Fig. 1. A downlink communication system with a two-antenna BS sending the information signal to a fluid antenna assisted UE and an artificial noise signal to impair an eavesdropper. Except the UE, all antennas are fixed.

- using multi-antenna MRC. Our results demonstrate that the proposed system with the UE utilizing a single fluid antenna (not using CSI at the BS) can match the secrecy rate that is obtained by the system with the UE adopting many-antenna MRC under optimal power allocation.
- With perfect CSI at the BS, BSZF can greatly outperform the proposed system. However, as the CSI becomes more and more uncertain at the BS, BSZF degrades quickly and the proposed system obtains a much higher secrecy rate. In fact, the proposed system is perfectly robust since its performance is invariant to the quality of the CSI.

II. System Model

In this letter, we consider a downlink system with a BS, a UE and an eavesdropper, as shown in Fig. 1. The eavesdropper is equipped with a fixed antenna while the BS has two fixed antennas. The BS utilizes one antenna to transmit information to the UE and another antenna to transmit an AN signal for jamming the eavesdropper. The UE is assumed to have a fluid antenna whose location can be switched instantly to one of N preset locations evenly distributed over a linear dimension of length $W\lambda$, where λ denotes the wavelength.

The received signal at the k-th port of the UE is given by

$$y_{\rm U}^{(k)}=h_{\rm I,U}^{(k)}s_{\rm I}+h_{\rm J,U}^{(k)}s_{\rm J}+\eta_{\rm U}^{(k)}, \tag{1}$$

where $h_{\rm I,U}^{(k)}$ and $h_{\rm J,U}^{(k)}$ denote the respective complex channels from the BS antennas to the k-th port of the UE, $s_{\rm I}$ denotes the information-bearing symbol with ${\rm E}[|s_{\rm I}^2|]=p_{\rm I}$, $s_{\rm J}$ is the AN signal with ${\rm E}[|s_{\rm J}^2|]=p_{\rm J}$, and $\eta_{\rm U}^{(k)}$ represents the complex additive white Gaussian noise (AWGN) at the k-th port of the UE, i.e., $\eta_{\rm U}^{(k)}\sim\mathcal{CN}(0,\sigma_\eta^2)$. Similarly, at the eavesdropper,[2] we have the received signal given by

$$y_{\rm E}=h_{\rm I,E}s_{\rm I}+h_{\rm J,E}s_{\rm J}+\eta_{\rm E}, \tag{2}$$

where the variables are defined in a similar fashion.

All the channels are assumed to be independent and identically distributed (i.i.d.) and follow $\mathcal{CN}(0,\sigma^2)$. Nevertheless, within the UE, since the ports can be arbitrarily close to each other, the channels seen by different ports are correlated. As in [16], we model the cross correlation function of the channels between port k and ℓ as

$$\Sigma_{k,\ell}=\sigma^2J_0\left(\frac{2\pi(k-\ell)W}{N-1}\right), \tag{3}$$

where $J_0(\cdot)$ represents the zero-order Bessel function of the first kind. By eigenvalue decomposition, the covariance matrix $\mathbf{\Sigma}=[\Sigma_{k,\ell}]$ can be expressed as

$$\mathbf{\Sigma}=\mathbf{Q}\mathbf{\Lambda}\mathbf{Q}^\dagger, \tag{4}$$

in which the columns of $\mathbf{Q}$ are the eigenvectors of $\mathbf{\Sigma}$ and $\mathbf{\Lambda}$ is the diagonal matrix of eigenvalues. Then the channel vector $\mathbf{h}_{\rm I,U}=[h_{\rm I,U}^{(1)}\ \dots h_{\rm I,U}^{(N)}]^T$ is given by

$$\mathbf{h}_{\rm I,U}=\mathbf{Q}\mathbf{\Lambda}^{\frac{1}{2}}\boldsymbol{x}_{\rm I,U}, \tag{5}$$

where $\boldsymbol{x}_{\rm I,U}$ is a random vector containing i.i.d. entries each following $\mathcal{CN}(0,1)$. The channel vector $\mathbf{h}_{\rm J,U}$ is defined in a similar way but with an independent vector $\boldsymbol{x}_{\rm J,U}$.

Note that the above model differs from the one used in [18] but can be regarded as a special case of the accurate model in [21] where there is no direct line-of-sight (LoS) and it has many non-LoS paths. In other words, our model is an accurate one that represents the rich scattering environments.

III. Power Allocation

This section studies the optimzation of the power allocation over the information-bearing signal and the AN signal, i.e., $p_{\rm I}$ and $p_{\rm J}$ when a fixed power budget at the BS is given. Before we proceed, we first write down the rate at the UE as

$$R_{\rm UE}=\log_2\left(1+\frac{p_{\rm I}|h_{\rm I,U}^{(k^*)}|^2}{p_{\rm J}|h_{\rm J,U}^{(k^*)}|^2+\sigma_\eta^2}\right), \tag{6}$$

where

$$k^*=\arg\max_k\left\{\frac{\left|h_{\rm I,U}^{(1)}\right|}{\left|h_{\rm J,U}^{(1)}\right|},\dots,\frac{\left|h_{\rm I,U}^{(N)}\right|}{\left|h_{\rm J,U}^{(N)}\right|}\right\} \tag{7}$$

denotes the index of the best port at the UE. On the other hand, the rate of the wiretap channel can be found as

$$R_{\rm E}=\log_2\left(1+\frac{p_{\rm I}\left|h_{\rm I,E}\right|^2}{p_{\rm J}\left|h_{\rm J,E}\right|^2+\sigma_\eta^2}\right). \tag{8}$$

As such, the secrecy rate achievable by the UE is found as

$$R_s=(R_{\rm UE}-R_{\rm E})^+ \tag{9}$$

where $(x)^+=\max(0,x)$.

A. Perfect CSI

When the CSI is perfectly known at the BS, then R_s can be computed and we aim to solve

$$P_0:\max_{p_{\rm I}>0,p_{\rm J}\geq0}R_s\ \text{s.t.}\ p_{\rm I}+p_{\rm J}\leq P, \tag{10}$$

where P is the maximum power transmitted by the BS.

Lemma 1: At the optimum, the power constraint holds with equality, i.e., $p_{\rm I}+p_{\rm J}=P$.

[2] Even if multiple receive antennas or a fluid antenna are considered at the eavesdropper, it will not add to its capability in our model because the CSI is assumed not available at the eavesdropper.

Proof: See Appendix A. ■

According to Lemma 1, $p_{\rm J}^* = P - p_{\rm I}^*$ (the asterisk highlights optimality) and thus, the problem P_0 can be reformulated as

$$P_1 : \max_{0<p_{\rm I}\le P} R_s = R_{\rm UE} - R_{\rm E}, \tag{11}$$

where the operation $(\cdot)^+$ operation is omitted for brevity. We can check the sign of the objective function once the problem is solved. By investigating the value of $\frac{{\rm d}R_s(p_{\rm I})}{{\rm d}p_{\rm I}}$, we can find the optimal power allocation for maximizing R_s.

Theorem 1: Defining

$$\left\{\begin{aligned} A &\triangleq \frac{\left|h_{\rm I,U}^{(k^*)}\right|^2 - \left|h_{\rm J,U}^{(k^*)}\right|^2}{P\left|h_{\rm J,U}^{(k^*)}\right|^2 + \sigma_\eta^2},\\ B &\triangleq -\frac{\left|h_{\rm J,U}^{(k^*)}\right|^2}{P\left|h_{\rm J,U}^{(k^*)}\right|^2 + \sigma_\eta^2}, \end{aligned}\right. \quad \left\{\begin{aligned} C &\triangleq \frac{\left|h_{\rm I,E}\right|^2 - \left|h_{\rm J,E}\right|^2}{P\left|h_{\rm J,E}\right|^2 + \sigma_\eta^2},\\ D &\triangleq -\frac{\left|h_{\rm J,E}\right|^2}{P\left|h_{\rm J,E}\right|^2 + \sigma_\eta^2}, \end{aligned}\right. \tag{12}$$

and

$$\begin{cases} S \triangleq A - B - C + D,\\ T \triangleq ACD - BCD - ABC + ABD,\\ V \triangleq 2(AD - BC),\\ \Delta \triangleq V^2 - 4TS, \end{cases} \tag{13}$$

the optimal power allocation is given by

$$p_{\rm I}^* = \begin{cases} -\dfrac{S}{V} \text{ if } V < 0 \text{ and } 0 \le -\dfrac{S}{V} \le P,\\ \arg\max\limits_{p_{\rm I}\in\{0,P\}} R_s(p_{\rm I}) \text{ otherwise}, \end{cases} \tag{14}$$

if $T = 0$. In the case $T \ne 0$, $p_{\rm I}^*$ can be found as

$$p_{\rm I}^* = \begin{cases} \arg\max\limits_{p_{\rm I}\in\{0,p_1,P\}} R_s(p_{\rm I}) \text{ if } 0 \le p_1 \le P \text{ and } \Delta > 0,\\ \arg\max\limits_{p_{\rm I}\in\{0,P\}} R_s(p_{\rm I}) \text{ otherwise}, \end{cases} \tag{15}$$

where

$$p_1 = -\frac{V + \sqrt{\Delta}}{2T}. \tag{16}$$

According to Lemma 1, we have $p_{\rm J}^* = P - p_{\rm I}^*$.

Proof: See Appendix B. ■

B. Imperfect CSI

The CSI at the BS in the downlink, if available, is destined to be imperfect since it involves finite feedback. Knowing the CSI for the eavesdropper is even more challenging as it may be external to the system. For this reason, we model the CSI errors of the eavesdropper by

$$\begin{cases} h_{\rm I,E} = \hat{h}_{\rm I,E} + \Delta h_{\rm I,E},\\ h_{\rm J,E} = \hat{h}_{\rm J,E} + \Delta h_{\rm J,E}, \end{cases} \tag{17}$$

where $\hat{h}_{\rm I,E}$ and $\hat{h}_{\rm J,E}$ are the estimated channels at the BS, and $\Delta h_{\rm I,E}$ and $\Delta h_{\rm I,E}$ denote the CSI errors. Considering a worst-case model, we assume that the CSI errors are bounded by an uncertainty limit ε, i.e.,

$$\begin{cases} |\Delta h_{\rm I,E}| \le \varepsilon,\\ |\Delta h_{\rm J,E}| \le \varepsilon. \end{cases} \tag{18}$$

In what follows, one can optimize the power allocation for maximizing a worst-case secrecy rate bound. We start by

$$P_2 : \begin{cases} \max\limits_{p_{\rm I},p_{\rm J}} \min\limits_{\Delta h_{\rm I,E},\Delta h_{\rm J,E}} \left[\begin{aligned} &\log_2\left(1 + \frac{p_{\rm I}\left|h_{\rm I,U}^{(k^*)}\right|^2}{p_{\rm J}\left|h_{\rm J,U}^{(k^*)}\right|^2 + \sigma_\eta^2}\right)\\ &-\log_2\left(1 + \frac{p_{\rm I}\left|\hat{h}_{\rm I,E}+\Delta h_{\rm I,E}\right|^2}{p_{\rm J}\left|\hat{h}_{\rm J,E}+\Delta h_{\rm J,E}\right|^2 + \sigma_\eta^2}\right) \end{aligned}\right]^+\\ \text{s.t.} \quad p_{\rm I} + p_{\rm J} \le P. \end{cases} \tag{19}$$

Now, using triangle inequality, we have

$$|\hat{h}_{\rm I,E} + \Delta h_{\rm I,E}| \le |\hat{h}_{\rm I,E}| + |\Delta h_{\rm I,E}| \le |\hat{h}_{\rm I,E}| + \varepsilon, \tag{20}$$

and

$$|\hat{h}_{\rm J,E} + \Delta h_{\rm J,E}| \ge |\hat{h}_{\rm J,E}| + |\Delta h_{\rm J,E}| \ge \left(|\hat{h}_{\rm J,E}| - \varepsilon\right)^+. \tag{21}$$

Thus, a robust power allocation approach can be obtained by

$$P_3 : \begin{cases} \max\limits_{p_{\rm I},p_{\rm J}} \left[\begin{aligned} &\log_2\left(1 + \frac{p_{\rm I}\left|h_{\rm I,U}^{(k^*)}\right|^2}{p_{\rm J}\left|h_{\rm J,U}^{(k^*)}\right|^2 + \sigma_\eta^2}\right)\\ &-\log_2\left(1 + \frac{p_{\rm I}|w_{\rm I,E}|^2}{p_{\rm J}|w_{\rm J,E}|^2 + \sigma_\eta^2}\right) \end{aligned}\right]^+\\ \text{s.t. } p_{\rm I} + p_{\rm J} \le P, \end{cases} \tag{22}$$

where $w_{\rm I,E} = |\hat{h}_{\rm I,E}| + \varepsilon$, $w_{\rm J,E} = \left(|\hat{h}_{\rm J,E}| - \varepsilon\right)^+$.

Similar to Problem P_0 in (10), the power constraint always holds with equality at the optimum. As the worst-case secrecy rate bound is only a function of a single variable $p_{\rm I}$, we can obtain the optimal power allocation to Problem P_3 using the similar method as stated in Theorem 1.

IV. Simulation Results

In this section, we present our simulation results to evaluate the proposed system which we refer to as FAS (fluid antenna system). Several benchmarks are also provided for comparison. For the perfect CSI case, we have the schemes:

- BSZF–This scheme requires CSI at the BS to ensure the information-bearing signal is zero at the eavesdropper and no AN signal is needed. Thus, $p_{\rm I} = P$ and $p_{\rm J} = 0$.
- FAS-OPA–This is the proposed fluid antenna system with optimal power allocation. CSI at the BS is required.
- FAS-EPA–This is the proposed fluid antenna with equal power allocation, i.e., $p_{\rm I} = p_{\rm J} = P/2$, using no CSI.
- N_R-antenna MRC (OPA)—This scheme adopts N_R fixed antennas at the UE for MRC. Optimal power allocation over $(p_{\rm I}, p_{\rm J})$ requiring CSI at the BS is considered. Note that zero-forcing receiver at the UE is not suitable as it will reveal to the UE the CSI of the BS antenna dedicated for sending a different user's signal, a security breach.
- N_R-antenna MRC (EPA)—This scheme is same as above except using $p_{\rm I} = p_{\rm J} = P/2$ (no CSI at the BS required).
- One fixed antenna (OPA)—This is same as N_R-antenna MRC (OPA) when $N_R = 1$. CSI at the BS is needed.
- One fixed antenna (EPA)—This scheme adopts one fixed antenna at the UE and with $p_{\rm I} = p_{\rm J} = P/2$.

In the imperfect CSI case, the CSI from the BS to the UE is still assumed perfect but that to the eavesdropper is not. All the

This article has been accepted for publication in IEEE Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2023.3264634

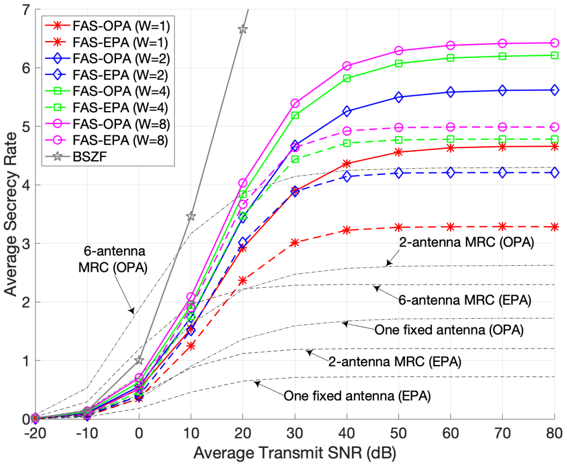

Fig. 2. Secrecy rate against the average SNR, $\sigma^2 P/\sigma_\eta^2$, with $N = 50$.

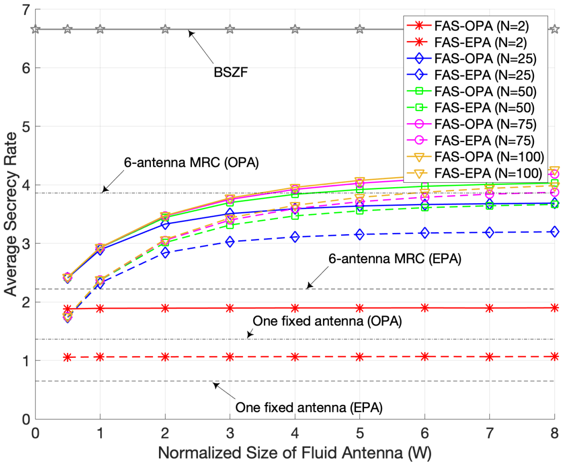

Fig. 3. Secrecy rate against the size of fluid antenna with SNR at 20dB.

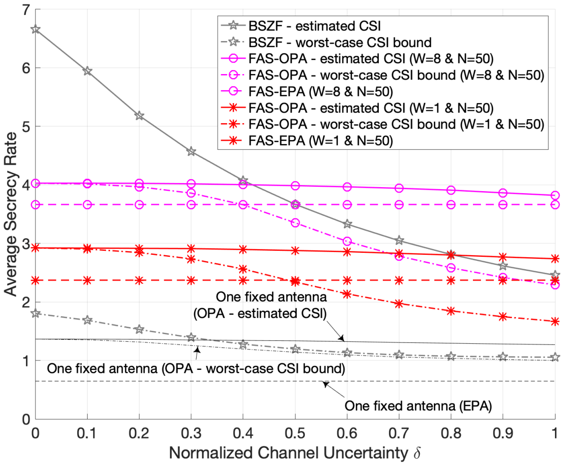

Fig. 4. Secrecy rate against the CSI uncertainty with SNR at 20dB.

considered schemes are similar as before except that when CSI is needed, the BS uses the estimated CSI for optimization. We define the normalized channel uncertainty as $\delta \triangleq \frac{\varepsilon}{\mathrm{E}[|h_{\mathrm{I,E}}|]} = \frac{\varepsilon}{\mathrm{E}[|h_{\mathrm{J,E}}|]}$. The channel errors $\Delta h_{\mathrm{I,E}}$ and $\Delta h_{\mathrm{J,E}}$ were generated uniformly and randomly in a circle centered at zero with radius ε. A scheme, which is referred to as 'BSZF using the worst-case CSI error bound', which knows only $|\hat{h}_{\mathrm{I,E}}|$ and $|\hat{h}_{\mathrm{J,E}}|$ to perform zero-forcing at the BS is also provided. The 'robust' versions of the optimal power allocation solution utilizing the worst-case CSI error bound as formulated in Section III-B are also given. For convenience, the power of all the channels is set to be equal in all of the simulations.

Finally, here, we consider $W = 1, 2, 4, 8$, which corresponds to a physical size of 15cm long fluid antenna at the UE for carrier frequency $f = 2, 4, 8, 16$GHz, respectively.

A. Perfect CSI

Focusing on the results in Figs. 2–3, we first note that BSZF outperforms significantly all the other methods. This should not be surprising because this is the only approach that uses all its power for transmitting the information to the UE, yet being completely secret to the eavesdropper. All the other methods have to handle the AN signal at the UE in exchange of secrecy. Additionally, the proposed FAS improves as the SNR or N or W increases. Remarkably, for FAS, OPA is only important if SNR is extremely high, as shown in Fig. 2. Moreover, we can observe in Fig. 3 that if N or W is large, then OPA is also less impactful for FAS. These observations indicate that FAS can work without OPA. By contrast, OPA is absolutely important for MRC systems. The results also illustrate that the proposed FAS can match or even exceed MRC with many fixed antennas, even without OPA if W and N are large enough.

B. Imperfect CSI

In Fig. 4, we study the secrecy performance of the different systems under imperfect CSI. An obvious change is that BSZF begins to perform very poorly as the CSI errors seem to affect very much the accuracy of zero-forcing. In particular, as the normalized CSI uncertainty δ increases, BSZF degrades fairly rapidly. On the other hand, FAS is absolutely robust as no CSI at the BS is utilized. FAS can even outperform greatly BSZF if δ is large. The impressive performance of FAS also comes with EPA. The results indicate that OPA using CSI at the BS only brings minor gain in the secrecy rate. Rather surprisingly, however, the supposed 'robust' OPA appears to perform badly. A close inspection of the worst-case OPA solution reveals that this is reasonable because the solution based on the CSI error bound is very conservative and will not perform well as far as the average secrecy rate is concerned. Furthermore, it is clear that BSZF using the worst-case CSI fails as expected because in this case, zero-forcing cannot be achieved with reasonably accuracy. Note that even if $\delta = 0$, 'robust' BSZF fails because it only uses the magnitudes of the CSI to attempt zero-forcing. Last but not least, the proposed FAS outperforms massively the conventional system with one fixed antenna.

V. Conclusion

In this paper, we proposed to employ a fluid antenna at the UE to resolve the AN signal for the BS to facilitate secrecy communication in the presence of an eavesdropper. The power allocation optimization over the information-bearing and AN signals was also addressed to understand the impact of power allocation. Our results left an optimistic taste of fluid antenna suggesting that without the need of CSI at the BS, the proposed fluid antenna system could exceed conventional systems with many fixed antennas using MRC at the UE, and even surpass BSZF when considerable CSI errors were present.

Appendices

A. Proof of Lemma 1

The first-order derivative of R_s over $p_{\rm I}$ is given by

$$\frac{\partial R_s}{\partial p_{\rm I}} = \frac{a-b}{(1+ap_{\rm I})(1+bp_{\rm I})\ln 2}, \tag{23}$$

where $a = \frac{|h_{\rm I,E}^{(k)}|^2}{p_{\rm J}|h_{\rm J,E}^{(k)}|^2+\sigma_\eta^2}$ and $b = \frac{|h_{\rm I,E}|^2}{p_{\rm J}|h_{\rm J,E}|^2+\sigma_\eta^2}$. For $a \leq b$, $\frac{\partial R_s}{\partial p_{\rm I}} \leq 0$, so R_s is monotonically decreasing as $p_{\rm I}$ increases. Therefore, the optimal value of $p_{\rm I}$ is 0. For $a > b$, $\frac{\partial R_s}{\partial p_{\rm I}} > 0$ and R_s is monotonically increasing as $p_{\rm I}$ increases. Thus, $p_{\rm I}$ should be at maximum to maximize R_s. For a given $p_{\rm J}$, the maximum power is $p_{\rm I} = P - p_{\rm J}$, which completes the proof.

B. Proof of Theorem 1

With $p_{\rm J} = P - p_{\rm I}$, the secrecy rate can be expressed as

$$R_s(p_{\rm I}) = \log_2(Ap_{\rm I}+1) - \log_2(Bp_{\rm I}+1) \\ - \log_2(Cp_{\rm I}+1) + \log_2(Dp_{\rm I}+1), \tag{24}$$

where A, B, C and D have been defined in (12). Hence,

$$\frac{{\rm d}R_s(p_{\rm I})}{{\rm d}p_{\rm I}} = \frac{Tp_{\rm I}^2 + Vp_{\rm I} + S}{\ln 2(Ap_{\rm I}+1)(Bp_{\rm I}+1)(Cp_{\rm I}+1)(Dp_{\rm I}+1)}, \tag{25}$$

where S, T, V are given in (13). Since $Ap_{\rm I}+1, Bp_{\rm I}+1, Cp_{\rm I}+1, Dp_{\rm I}+1 > 0$, the trend of $R_s(p_{\rm I})$ depends on the value of $Tp_{\rm I}^2 + Vp_{\rm I} + S$. The monotonicity of $R_s(p_{\rm I})$ is analyzed in TABLE I in which Δ is defined in (13), $p_1 = \frac{-V-\sqrt{\Delta}}{2T}$ and $p_2 = \frac{-V+\sqrt{\Delta}}{2T}$. The analysis gives the solution in Theorem 1.

TABLE I
MONOTONICITY OF THE SECRECY RATE FUNCTION

		$\frac{{\rm d}R_s(p_{\rm I})}{{\rm d}p_{\rm I}}$	Monotonicity of $R_s(p_{\rm I})$	Range of $p_{\rm I}$
$T>0$	$\Delta>0$	≥ 0	Increasing	$-\infty < p_{\rm I} \leq p_1$
		≤ 0	Decreasing	$p_1 \leq p_{\rm I} \leq p_2$
		≥ 0	Increasing	$p_2 \leq p_{\rm I} < \infty$
	$\Delta \leq 0$	≥ 0	Increasing	$-\infty < p_{\rm I} < \infty$
$T<0$	$\Delta>0$	≤ 0	Decreasing	$-\infty < p_{\rm I} \leq p_2$
		≥ 0	Increasing	$p_2 \leq p_{\rm I} \leq p_1$
		≤ 0	Decreasing	$p_1 \leq p_{\rm I} < \infty$
	$\Delta \leq 0$	≤ 0	Decreasing	$-\infty < p_{\rm I} < \infty$
$T=0$	$V=0$ $S \geq 0$	≥ 0	Increasing	$-\infty < p_{\rm I} < \infty$
	$V=0$ $S \leq 0$	≤ 0	Decreasing	
	$V>0$	≤ 0	Decreasing	$-\infty < p_{\rm I} \leq -\frac{S}{V}$
		≥ 0	Increasing	$-\frac{S}{V} \leq p_{\rm I} < \infty$
	$V<0$	≥ 0	Increasing	$-\infty < p_{\rm I} \leq -\frac{S}{V}$
		≤ 0	Decreasing	$-\frac{S}{V} \leq p_{\rm I} < \infty$

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, Feb. 2014.

[2] F. Tariq *et al.*, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[3] Z. Wang *et al.*, "Extremely large-scale MIMO: Fundamentals, challenges, solutions, and future directions," [Online] arXiv preprint arXiv:2209.12131, 2022.

[4] Y. Saito *et al.*, "Non-orthogonal multiple access (NOMA) for cellular future radio access," *IEEE Veh. Technol. Conf. Spring (VTC-Spring)*, 2-5 Jun. 2013, Dresden, Germany.

[5] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Select. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tut.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 9-13 Dec. 2018, Abu Dhabi, United Arab Emirates.

[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 Commun. and Netw., section Wireless Commun.*, 3:853416, Mar. 2022.

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

[10] X. Yan, L. Li, H. C. Zhang and J. Y. Han, "Broadband polarization-reconfigurable liquid dielectric resonator antenna controlled by gravity," *IEEE Antennas & Wireless Propag. Letters*, vol. 21, no. 10, pp. 2105–2109, Oct. 2022.

[11] X. Geng *et al.*, "Pattern-reconfigurable liquid metal magneto-electric dipole antenna," *IEEE Antennas & Wireless Propag. Letters*, vol. 21, no. 8, pp. 1683–1687, Aug. 2022.

[12] B. A. Cetiner, H. Jafarkhani, J.-Y. Qian, H. J. Yoo, A. Grau and F. De Flaviis, "Multifunctional reconfigurable MEMS integrated antennas for adaptive MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 12, pp. 62–70, Dec. 2004.

[13] A. Grau Besoli and F. De Flaviis, "A multifunctional reconfigurable pixeled antenna using MEMS technology on printed circuit board," *IEEE Trans. Antennas & Propag.*, vol. 59, no. 12, pp. 4413–4424, Dec. 2011.

[14] S. Song and R. D. Murch, "An efficient approach for optimizing frequency reconfigurable pixel antennas using genetic algorithms," *IEEE Trans. Antennas & Propag.*, vol. 62, no. 2, pp. 609–620, Feb. 2014.

[15] K. K. Wong, A. Shojaeifard, K. F. Tong, and Y. Zhang, "Fluid antenna systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1950–1962, Mar. 2021.

[16] M. Khammassi, A. Kammoun, and M.-S. Alouini, "A new analytical approximation of the fluid antenna system channel," [Online] arXiv preprint arXiv:2203.09318, 2022.

[17] L. Tlebaldiyeva, G. Nauryzbayev, S. Arzykulov, A. Eltawil, and T. Tsiftsis, "Enhancing QoS through fluid antenna systems over correlated Nakagami-m fading channels," in Proc. *IEEE Wireless Commun. & Netw. Conf. (WCNC)*, pp. 78–83, 10-13 Apr. 2022, Austin, TX, USA.

[18] K. K. Wong, K. F. Tong, Y. Chen and Y. Zhang, "Closed-form expressions for spatial correlation parameters for performance analysis of fluid antenna systems," *Elect. Letters*, vol. 58, no. 11, pp. 454–457, Apr. 2022.

[19] C. Skouroumounis and I. Krikidis, "Fluid antenna with linear MMSE channel estimation for large-scale cellular networks," *IEEE Trans. Commun.*, vol. 71, no. 2, pp. 1112–1125, Feb. 2023.

[20] K. K. Wong, and K. F. Tong, "Fluid antenna multiple access," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 4801–4815, Jul. 2022.

[21] K. K. Wong, K. F. Tong, Y. Chen, and Y. Zhang, "Extra-large MIMO enabling slow fluid antenna massive access for millimeter-wave bands," *Elect. Letters*, vol. 58, no. 25, pp. 1016–1018, Dec. 2022.

[22] K. K. Wong, K. F. Tong, Y. Chen, and Y. Zhang, "Fast fluid antenna multiple access enabling massive connectivity," *IEEE Commun. Letters*, vol. 27, no. 2, pp. 711–715, Feb. 2023.

[23] N. Waqar, K. K. Wong, K. F. Tong, A. Sharples, and Y. Zhang, "Deep learning enabled slow fluid antenna multiple access," *IEEE Commun. Letters*, vol. 27, no. 2, pp. 711–715, Feb. 2023.