Secure UAV Communications By STEEP Against Full-Duplex Active Eavesdropper

Md Saydur Rahman and Yingbo Hua
Department of Electrical and Computer Engineering
University of California at Riverside
Riverside, CA, 92521 USA
mrahm054@ucr.edu and yhua@ucr.edu

***Abstract*—Unmanned Aerial Vehicle (UAV) assisted wireless communication has emerged as a highly promising element in the landscape of future wireless networks. This paper investigates the application of "Secret-message Transmission by Echoing Encrypted Probes (STEEP)" to secure UAV communications between a ground station (Alice) and a UAV (Bob). Even with the presence of strong jamming from a full-duplex eavesdropper (Eve), STEEP shows resilience and maintains a strong positive secrecy rate in bits per channel use in every channel coherence period as long as Eve's observations during the probing phase of STEEP are not noiseless. STEEP is a novel round-trip transmission scheme for secure communications, overcoming limitations where prior schemes fail to achieve a positive secrecy rate when Eve's receive channel is stronger than users'.**

***Index Terms*—Physical layer security, UAV communications, secrecy outage probability.**

I. Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones, have altered industries, revolutionized civilian applications, and opened up new fronts in military communications. These versatile low-altitude platforms have been used for different purposes from aerial cinematography and mapping to precision agriculture, infrastructure inspection, rescue missions, and military expeditions. Wireless communications serve as a lifeline for UAVs, enabling real-time data exchanges and navigation updates. Moreover, lower-altitude UAV deployment reduces shadowing effects, ensuring high Line of Sight (LoS) communication probability with the ground. However, its ubiquity and openness make UAV communications vulnerable to wiretapping, jamming and cyber attacks, risking mission success, data confidentiality and public safety.

A. Related Works

Recently there have been a lot of research activities on physical layer security (PLS) for UAV communications. The authors of [1] explored the PLS of UAV communication systems, where a ground sender, Alice, transmits confidential messages to a hovering UAV, while eavesdroppers are randomly positioned around the ground source. The authors of [2] studied a UAV system with a linear trajectory, where a UAV performs inspection tasks along a straight path and communicates with a ground receiver while an eavesdropping UAV attempts to intercept the signal. The authors of [3] investigated energy-efficient and secure transmission in a downlink Air-2-Ground wiretap system with consideration of UAV's jitter effects. They also optimized the beamforming for confidential signal and artificial noise (AN) to minimize total transmission power from a UAV-mounted base station, and also addressed jamming from a full-duplex eavesdropper aimed at damaging the legitimate channel. The authors of [4] looked into a UAV-2-Vehicle system, where a UAV serves as a temporary aerial station exchanging information with a legitimate ground vehicle, subject to interception by an eavesdropping vehicle. Utilizing stochastic geometry theory, they examined the impact of UAV's 3D spatial randomness, and ground vehicles' positioning along highway, on the downlink and uplink secrecy outage performance. Furthermore, authors of [5] examined the ergodic secrecy outage rate while considering an aerial eavesdropper flying along a random trajectory with smooth turns in 3D spherical spaces. The authors of [6] applied a similar scheme as shown in the above references but considered secrecy outage for transmission from a multi-antenna ground station to a UAV subject to jamming from a multi-antenna full-duplex active Eve. The authors of [13] addresses security and reliability challenges in the integration of UAVs and NOMA for ultra-reliable low-latency communication (uRLLC) by proposing physical layer security (PLS) mechanisms, optimizing secrecy rates, and analyzing the impact of UAV mobility on enhancing communication security. The paper by Chen et al. [14] develops a UAV network architecture that enhances physical layer security by incorporating John Boyd's OODA loop decision-making framework, modeling risks from hybrid wireless attacks, and implementing adaptive cooperative jamming control schemes to optimize security, energy consumption, and resilience against threats. The study by Diao et al. [15] addresses secure wireless-powered NOMA communications in multi-UAV systems by proposing a joint energy transfer and artificial noise (ETAN) scheme that combines physical layer security (PLS) and artificial noise (AN) to protect against eavesdropping, while optimizing energy efficiency and enhancing the system's secrecy rate.

For the prior UAV works, it is widely assumed that Alice or Bob has more antennas than Eve does, and/or that the legitimate channel is stronger than Eve's channel with a significant probability. This is clearly not always practical. But the above assumption has been necessitated by the fact that the secrecy capacity of the classic wiretap channel transmission schemes would be zero otherwise.

Recently, a novel scheme called "Secret-message Transmission by Echoing Encrypted Probes (STEEP)" is proposed and studied in [8], [9] and [10]. STEEP is a hybrid of the notions for secret key generation and wiretap channel transmission, evolved from an earlier work shown in [7] on generalized channel probing and generalized preprocessing for secret key generation. It also turns out that the scheme shown in [12] for a binary symmetric channel is a special case of STEEP. A unique property of STEEP is that it enables a positive secrecy capacity even if Eve's channel is always stronger than the (legitimate) users' channel. The key contributions of this paper (a substantial extension of [11]) include the following:

- We present STEEP for a UAV based system subject to jamming from a full-duplex active Eve. We choose a system setup almost identical to that in [6]. It is shown that STEEP is far more resilient than conventional schemes as STEEP achieves a positive secrecy capacity under constant jamming from Eve. This unique feature of STEEP sets it apart from previous wiretap channel schemes and/or reciprocal-channel-based key generation schemes.
- We extend to our work in multiple users NOMA network against a single full-duplex eavesdropper. We show that our steep model can still have positive secrecy in NOMA access network where AP has imperfect channel information.
- We finally show numerical results that prove STEEP has much stronger robustness in achieving positive secrecy rates and/or low probabilities of secrecy outage than the conventional scheme. This is consistent with a STEEP's property that its secrecy capacity in bits per round-trip channel use is positive as long as Eve's channel strength during the probing phase is finite. Furthermore, the influence of jamming and channel fading on STEEP's performance is demonstrated, comparing it to a conventional half-duplex two-way scheme under identical power allocations.

II. Principle of STEEP

The principle of STEEP as shown in [8], [9] and [10] is a round-trip transmission scheme with a probing phase (phase 1) and an echoing phase (phase 2) showed in Fig. 1. Specifically, before node B transmits a secret message to node A, node A initiates the probing phase by transmitting probing (random) symbols to node B. Then node B obtains an estimate of each (effective) probing symbol. The estimated probes are subsequently encrypted with a secret message (meant for node A) and echoed back to node A in the echoing phase. Since node A knows the exact probing symbols and Eve can only has a noisy version of the probing symbols, node A has an advantage over Eve in detecting the secret message from node B provided that the effective noise or error rate in the echoing phase from node B to node A is kept small. Consequently, this results in a positive secrecy rate as long as Eve's receive channel strength during the probing phase is not infinitely stronger than that from node A to node B.

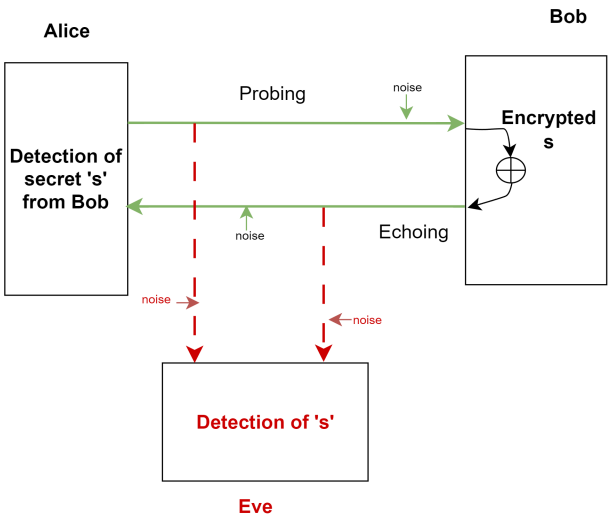


Fig. 1: Principle of STEEP

III. Network Model

In this paper, we first consider a network as illustrated in Fig. 2, which is similar to that in [6]. Here Alice and Eve are ground stations with n_A and n_E antennas respectively. Eve is capable of jamming and receiving in full-duplex. Bob is the UAV with a single antenna. The 3D Cartesian coordinates of Alice, Bob and Eve are respectively $\zeta_A = (0,0,0), \zeta_B = (\mu_u, \nu_u, \mathcal{A}_u)$, and $\zeta_E = (\mu_E, \nu_E, 0)$. We assume that the height of UAV, $\mathcal{A}_u$, satisfies $0 \leq \mathcal{A}_u \leq \mathcal{A}_u^{\max}$.

The channel vectors from Alice to Bob and from Bob to Alice are respectively $\mathbf{h}_{B,A} \in \mathcal{C}^{n_A \times 1}$ and $\mathbf{h}_{A,B} \in \mathcal{C}^{n_A \times 1}$. The channel matrix from Alice to Eve and the channel vector from Bob to Eve are respectively $\sqrt{\gamma_{E,A}}\mathbf{H}_{E,A} \in \mathcal{C}^{n_E \times n_A}$ and $\sqrt{\gamma_{E,B}}\mathbf{h}_{E,B} \in \mathcal{C}^{n_E \times 1}$. Here $\gamma_{E,A}$ and $\gamma_{E,B}$ are used to model the large scale fading gains at Eve (relative to the link between Alice and Bob). For channels between air and ground, we consider both line-of-sight (LoS) and non-line-of-sight (NLoS) components, i.e.,

$$\mathbf{h}_{B,A} = \sqrt{\frac{K_{\mathrm{B,A}}}{1+K_{\mathrm{B,A}}}}\mathbf{h}_{B,A}^{L} + \sqrt{\frac{1}{1+K_{\mathrm{B,A}}}}\mathbf{h}_{B,A}^{N}, \quad (1)$$

$$\mathbf{h}_{A,B} = \sqrt{\frac{K_{\mathrm{A,B}}}{1+K_{\mathrm{A,B}}}}\mathbf{h}_{A,B}^{L} + \sqrt{\frac{1}{1+K_{\mathrm{A,B}}}}\mathbf{h}_{A,B}^{N}, \quad (2)$$

$$\mathbf{h}_{E,B} = \sqrt{\frac{K_{\mathrm{E}}}{1+K_{\mathrm{E}}}}\mathbf{h}_{E,B}^{L} + \sqrt{\frac{1}{1+K_{\mathrm{E}}}}\mathbf{h}_{E,B}^{N} \quad (3)$$

Here $K_{\mathrm{B,A}}$, $K_{\mathrm{A,B}}$ and K_{E} are the Rician K-factors. The first terms are the LoS components, and the second terms are the NLoS components. The entries of $\mathbf{h}_{B,A}^{N}, \mathbf{h}_{A,B}^{N}, \mathbf{h}_{E,B}^{N}$, due to NLoS, are independent and identically distributed (i.i.d.) variables with the circularly symmetric complex Gaussian distribution with zero mean and unit variance, i.e., $\mathcal{CN}(0,1)$. The entries of $\mathbf{h}_{B,A}^{L}, \mathbf{h}_{A,B}^{L}, \mathbf{h}_{E,B}^{L}$ follow the far-field planar wave model without multipath. For example, assuming a

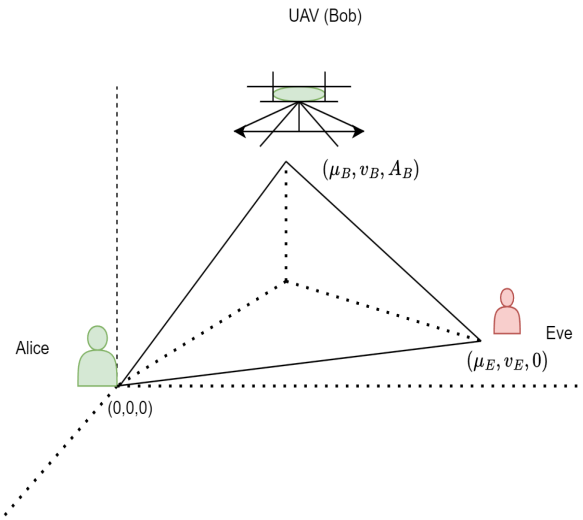


Fig. 2: A UAV wireless network with multi-antenna Alice and multi-antenna Eve

uniform linear array of antennas at Alice, the ith entry of $\mathbf{h}_{B,A}^L$ can be expressed as

$$(\mathbf{h}_{B,A}^L)_i = e^{-j2\pi\delta_{B,A}(i-1)\sin\phi_{B,A}\cos\theta_{B,A}} \tag{4}$$

where $\delta_{B,A}$ is the antenna spacing divided by wavelength, $\phi_{B,A}$ is the azimuth angle between Alice and Bob relative to the broadside of the antenna array (parallel to the ground), and $\theta_{B,A}$ is the elevation angle between Alice and Bob, i.e.,

$$\theta_{B,A} = \arcsin\left(\frac{\mathcal{A}_B}{d_{B,A}}\right) \tag{5}$$

with

$$d_{B,A} = \sqrt{\mu_B^2 + \nu_B^2 + \mathcal{A}_B^2}. \tag{6}$$

The structures of $\mathbf{h}_{A,B}^L$ and $\mathbf{h}_{E,B}^L$ can be similarly determined.

The channel matrix from Alice to Eve is $\sqrt{\gamma_{E,A}}\mathbf{H}_{E,A} \in \mathcal{C}^{n_E \times n_A}$, the elements of which are typically only due to NLoS and hence modelled as i.i.d. $\mathcal{CN}(0, \gamma_{E,A})$.

We will assume that all line-of-sight components are reciprocal (e.g., $\mathbf{h}_{A,B}^L = \mathbf{h}_{B,A}^L$), all γ gains are reciprocal (e.g., $\gamma_{E,A} = \gamma_{A,E}$), but the NLoS channel parameters are all statistically independent (e.g., $\mathbf{H}_{E,A}$ is independent of $\mathbf{H}_{A,E}$).

IV. Conventional Two-way UAV communication

We now formulate a conventional scheme to compare with STEEP. This scheme is based on that in [6] where a full-duplex Eve who knows $\mathbf{h}_{B,E}$ transmits a beamformed jamming signal to degrade the reception at UAV. Since STEEP requires both Alice and Bob to consume powers for transmission, for comparison purpose, we consider a conventional two-way half-duplex scheme between Alice and Bob. In the conventional scheme, Alice transmits a secret message to Bob in phase 1, and Bob sends an independent secret message to Alice in phase 2, which is detailed below.

A. Phase 1

In phase 1, Alice applies optimal beamforming and artificial noise. Specifically, for each sample interval, Alice transmits $\sqrt{p_A}(\mathbf{w_s}s_A + \mathbf{W}_{an}\mathbf{s}_{an})$ where s_A is a secret-carrying symbol assumed to be $\mathcal{CN}(0, \alpha_s)$, and $\mathbf{s}_{an}$ is an artificial noise symbol assumed to be $\mathcal{CN}(0, \beta_s\mathbf{I}_{n_A-1})$. Also $\mathbf{w}_s = \frac{\mathbf{h}_{BA}^*}{\|\mathbf{h}_{BA}\|}$, and $[\mathbf{W}_{\text{an}}, \mathbf{w}_s]$ is a unitary matrix with $\mathbf{w}_s^H\mathbf{W}_{\text{an}} = 0$. Moreover, $\beta_s = \frac{1-\alpha_s}{n_A-1}$ so that p_A is the effective transmit power consumed by Alice.

Following the transmission from Alice, the signals received by Bob and Eve are respectively

$$y_{B,1} = \sqrt{p_A}\mathbf{h}_{B,A}^T\mathbf{w}_s s_A + \sqrt{p_E\gamma_{B,E}}\mathbf{h}_{B,E}^T\mathbf{x}_{\text{B,E}} + w_B, \tag{7}$$

$$\begin{aligned}\mathbf{y}_{E,1} = &\sqrt{p_A\gamma_{E,A}}\mathbf{H}_{E,A}\left(\mathbf{w}_s s_A + \mathbf{W}_{an}\mathbf{s}_{an}\right)\\ &+ \sqrt{\rho p_E}\mathbf{H}_{E,E}\mathbf{x}_{B,E} + \mathbf{w}_{E,A},\end{aligned} \tag{8}$$

where $\mathbf{x}_{B,E}$ is the jamming signal from Eve to Bob, $\sqrt{\gamma_{B,E}}\mathbf{h}_{B,E}$ is the channel vector from Eve to Bob, $\mathbf{H}_{E,E}$ is the (residual[1]) self-interference matrix at Eve, and ρ denotes the (residual) self-interference coefficient. To maximally degrade the reception at Bob, Eve chooses the following beamformed jamming signal:

$$\mathbf{x}_{B,E} = \bar{\mathbf{h}}_{B,E}^* n_{B,E} \tag{9}$$

with $\bar{\mathbf{h}}_{B,E}^* = \frac{\mathbf{h}_{B,E}^*}{\|\mathbf{h}_{B,E}\|}$ and $n_{B,E}$ being $\mathcal{CN}(0,1)$.

We will assume that all noise elements such as w_B and elements in $\mathbf{w}_{E,A}$ are i.i.d. $\mathcal{CN}(0,1)$.

In this case, the effective signal-to-noise ratio (SNR), or equivalently the signal-to-noise-and-interference ratio, in $y_{B,1}$ at Bob is

$$\text{SNR}_{B,1} = \frac{\alpha_s p_A\|\mathbf{h}_{B,A}\|^2}{p_E\gamma_{B,E}\|\mathbf{h}_{B,E}\|^2 + 1}. \tag{10}$$

To determine the effective SNR in $\mathbf{y}_{E,1}$ at Eve, we consider a (scalar) sufficient statistic of $\mathbf{y}_{E,1}$ for s_A, which is

$$y_{E,1} \doteq \mathbf{w}_{G,s}^H\mathbf{y}_{E,1} \tag{11}$$

with $\mathbf{w}_{G,s} = \frac{\mathbf{H}_{E,A}\mathbf{w}_s}{\|\mathbf{H}_{E,A}\mathbf{w}_s\|}$. It is easy to verify that the effective SNR in $y_{E,1}$ is

$$\text{SNR}_{E,1} = \frac{\alpha_s p_A\gamma_{E,A}\|\mathbf{H}_{E,A}\mathbf{w}_s\|^2}{T_1 + T_2 + 1} \tag{12}$$

with $T_1 = \beta_s p_A\gamma_{E,A}\|\mathbf{w}_{G,s}^H\mathbf{H}_{E,A}\mathbf{W}_{an}\|^2$ and $T_2 = \rho p_E|\mathbf{w}_{G,s}^H\mathbf{H}_{E,E}\bar{\mathbf{h}}_{B,E}^*|^2$.

So, the secrecy capacity from Alice to Bob (in bits per complex channel use) is $\bar{C}_1 = C_1^+ \doteq \max(0, C_1)$ with

$$C_1 = \log(1 + \text{SNR}_{B,1}) - \log(1 + \text{SNR}_{E,1}). \tag{13}$$

Here the first term is the capacity from Alice to Bob while the second term is the capacity from Alice to Eve.

[1] After the best possible self-interference cancellation.

B. Phase 2

Unlike Alice, Bob with a single antenna is unable to apply artificial noise. Let a random symbol transmitted by Bob be $\sqrt{p_B}s_B$ with the distribution $\mathcal{CN}(0, p_B)$. The signals received by Alice and Eve are respectively

$$\mathbf{y}_{A,2} = \sqrt{p_B}\mathbf{h}_{A,B}s_{\mathrm{B}} + \sqrt{\frac{p_E\gamma_{A,E}}{n_E}}\mathbf{H}_{A,E}\mathbf{x}_{\mathrm{A,E}} + \mathbf{w}_A, \quad (14)$$

$$\mathbf{y}_{E,2} = \sqrt{p_B\gamma_{E,B}}\mathbf{h}_{E,B}s_B + \sqrt{\frac{\rho p_E}{n_E}}\mathbf{H}_{E,E}\mathbf{x}_{A,E} + \mathbf{w}_{E,B}. \quad (15)$$

In this case, we assume that the jamming signal $\mathbf{x}_{A,E}$ from Eve to Alice is independent of the channel matrix $\mathbf{H}_{A,E}$ from Eve to Alice. Furthermore, $\mathbf{x}_{A,E}$ is $\mathcal{CN}(0, \mathbf{I}_{n_E})$, and $\mathbf{x}_{A,E}$ is also independent of $\mathbf{x}_{B,E}$.

The effective SNR at Alice is the SNR in $\bar{\mathbf{h}}_{A,B}^H\mathbf{y}_{A,2}$ with $\bar{\mathbf{h}}_{A,B} = \frac{\mathbf{h}_{A,B}}{\|\mathbf{h}_{A,B}\|}$, which is

$$\mathtt{SNR}_{A,2} = \frac{p_B\|\mathbf{h}_{A,B}\|^2}{\frac{p_E\gamma_{A,E}}{n_E}\|\bar{\mathbf{h}}_{A,B}^H\mathbf{H}_{A,E}\|^2 + 1}. \quad (16)$$

Similarly, the effective SNR at Eve is

$$\mathtt{SNR}_{E,2} = \frac{p_B\gamma_{E,B}\|\mathbf{h}_{E,B}\|^2}{\frac{\rho p_E}{n_E}\|\bar{\mathbf{h}}_{E,B}^H\mathbf{H}_{E,E}\|^2 + 1} \quad (17)$$

with $\bar{\mathbf{h}}_{E,B} = \frac{\mathbf{h}_{E,B}}{\|\mathbf{h}_{E,B}\|}$.

Then the secrecy capacity from Bob to Alice is $\bar{C}_2 = C_2^+$ with

$$C_2 = \log(1 + \mathtt{SNR}_{A,2}) - \log(1 + \mathtt{SNR}_{E,2}). \quad (18)$$

C. Total secrecy capacity

The total secrecy capacity (in bits per round-trip complex channel use) of the conventional scheme is

$$\bar{C}_{conv} = \bar{C}_1 + \bar{C}_2. \quad (19)$$

For a target secrecy rate R_s, the secrecy outage probability of the conventional scheme is

$$O_{\text{conv}}\ (R_s) \doteq \mathrm{Prob}\left(\bar{C}_{\text{conv}}\ \le R_s\right). \quad (20)$$

V. Application of STEEP

We now consider a secret-message transmission from Bob to Alice using STEEP.

A. Phase 1

In phase 1 of STEEP, Alice sends a sequence of random probing vectors. Such a vector is denoted by $\sqrt{p_A/n_A}\mathbf{x}_A$ where $\mathbf{x}_A$ is $\mathcal{CN}(0, \mathbf{I}_{n_A})$. The signals received by Bob and Eve in this phase are

$$y_B = \sqrt{\frac{p_A}{n_A}}\mathbf{h}_{B,A}^T\mathbf{x}_A + \sqrt{p_E\gamma_{B,E}}\mathbf{h}_{B,E}^T\mathbf{x}_{B,E} + w_B, \quad (21)$$

$$\mathbf{y}_{E,Am} = \sqrt{\frac{p_A\gamma_{E,A}}{n_A}}\mathbf{H}_{E,A}\mathbf{x}_A + \sqrt{\rho p_E}\mathbf{H}_{E,E}\mathbf{x}_{B,E} + \mathbf{w}_{E,A}, \quad (22)$$

where $\mathbf{x}_{B,E}$ is the jamming noise from Eve as discussed before, i.e., $\mathbf{x}_{B,E} = \bar{\mathbf{h}}_{B,E}^* n_{B,E}$.

We will call the following an "effective probe" arriving at Bob:

$$p_0 = e^{-j\theta_B}\bar{\mathbf{h}}_{B,A}^T\mathbf{x}_A \quad (23)$$

with $\bar{\mathbf{h}}_{B,A} = \frac{1}{\|\mathbf{h}_{B,A}\|}\mathbf{h}_{B,A}$ and $\theta_B = 0$ for $n_A \ge 2$. If $n_A = 1$, we can choose θ_B to be the phase of $\bar{\mathbf{h}}_{B,A}$ so that no channel feedback from Bob to Alice would be necessary.

B. Phase 2

In phase 2 of STEEP, Bob transmits a sequence of virtually[2] independent symbols, and such a symbol is structured as

$$\sqrt{p_B}x_B = \sqrt{\frac{p_B}{2}}\left(\hat{p}_0 + s\right). \quad (24)$$

where s is a symbol in a secret message from Bob, and $\hat{p}_0$ is the MMSE estimate of p_0 by Bob from y_B. We will also let s be $\mathcal{CN}(0, 1)$. Here x_B is called an "encrypted probe".

Now the signals received by Alice and Eve are respectively

$$\mathbf{y}_A = \sqrt{p_B}\mathbf{h}_{A,B}x_B + \sqrt{\frac{p_E\gamma_{A,E}}{n_E}}\mathbf{H}_{A,E}\mathbf{x}_{A,E} + \mathbf{w}_A, \quad (25)$$

$$\mathbf{y}_{E,B} = \sqrt{p_B\gamma_{E,B}}\mathbf{h}_{E,B}x_B + \sqrt{\frac{\rho p_E}{n_E}}\mathbf{H}_{E,E}\mathbf{x}_{A,E} + \mathbf{w}_{E,B}, \quad (26)$$

where $\mathbf{x}_{A,E}$ is the jamming noise from Eve to Alice (as discussed before). As assumed before, $\mathbf{w}_A$ is $\mathcal{CN}(0, \mathbf{I})$, and $\mathbf{w}_{E,B}$ is $\mathcal{CN}(0, \mathbf{I})$.

Alice now needs to detect the information in s using her knowledge of $\mathbf{x}_A$ and $\mathbf{y}_A$ while Eve could try to detect the information in s based on $\mathbf{y}_{E,Am}$ and $\mathbf{y}_{E,B}$.

C. Secrecy Analysis of STEEP

1) Optimal estimation at Bob: Since $\hat{p}_0$ is the MMSE estimate of p_0 from y_B, it follows from (21) that

$$\begin{aligned}\hat{p}_0 &= \mathbb{E}\left\{p_0 y_B^H\right\}\left(\mathbb{E}\left\{y_B y_B^H\right\}\right)^{-1} y_B \\ &= \frac{\sqrt{\frac{p_A}{n_A}}\|\mathbf{h}_{B,A}\|\, y_B}{\frac{p_A}{n_A}\|\mathbf{h}_{B,A}\|^2 + p_E\gamma_{B,E}\|\mathbf{h}_{B,E}\|^2 + 1}.\end{aligned} \quad (27)$$

Furthermore, the MSE of $\hat{p}_0$ is

$$\begin{aligned}\sigma_{\Delta p_0}^2 &\doteq \mathbb{E}\left\{|\Delta p_0|^2\right\} = \mathbb{E}\left\{|\hat{p}_0 - p_0|^2\right\} \\ &= \frac{S_{B,E} + 1}{S_{B,A} + S_{B,E} + 1}\end{aligned} \quad (28)$$

with $S_{B,A} = \frac{p_A}{n_A}\|\mathbf{h}_{B,A}\|^2$ and $S_{B,E} = p_E\gamma_{B,E}\|\mathbf{h}_{B,E}\|^2$. Also

$$\sigma_{\hat{p}_0}^2 \doteq \mathbb{E}\left\{|\hat{p}_0|^2\right\} = \frac{S_{B,A}}{S_{B,A} + S_{B,E} + 1}. \quad (29)$$

[2]Due to forward-error-correction channel coding, they are not exactly independent.

2) Optimal estimation at Alice: It follows from (25), (27) and (21) that

$$\Delta \mathbf{y}_A \doteq \mathbf{y}_A - \mathbb{E}(\mathbf{y}_A|\mathbf{x}_A) = \mathbf{y}_A - \sqrt{\frac{p_B}{2}}\mathbf{h}_{A,B}\sigma^2_{\hat{p}_0}p_0. \quad (30)$$

and the MMSE estimate of s by Alice is given by

$$\begin{aligned}\hat{s}_A &= \mathbb{E}\left\{s\Delta\mathbf{y}_A^H\right\}\left(\mathbb{E}\left\{\Delta\mathbf{y}_A\Delta\mathbf{y}_A^H\right\}\right)^{-1}\Delta\mathbf{y}_A \\ &= \sqrt{\frac{p_B}{2}}\mathbf{h}_{AB}^H\left(\frac{p_B}{2}\left(\sigma^2_{\hat{p}_0}\sigma^2_{\Delta p_0}+1\right)\mathbf{h}_{A,B}\mathbf{h}_{A,B}^H\right. \\ &\left.+\frac{p_E\gamma_{A,E}}{n_E}\mathbf{H}_{A,E}\mathbf{H}_{A,E}^H+\mathbf{I}_{n_A}\right)^{-1}\Delta\mathbf{y}_A. \quad (31)\end{aligned}$$

Furthermore, the MSE of $\hat{s}_A$ is

$$\begin{aligned}\sigma^2_{\Delta s_A} &= 1-\frac{p_B}{2}\mathbf{h}_{AB}^H\left(\frac{p_B}{2}(\sigma^2_{\hat{p}_0}\sigma^2_{\Delta p_0}+1)\mathbf{h}_{A,B}\mathbf{h}_{A,B}^H+\right. \\ &\left.\frac{p_E\gamma_{A,E}}{n_E}\mathbf{H}_{A,E}\mathbf{H}_{A,E}^H+\mathbf{I}_{n_A}\right)^{-1}\mathbf{h}_{AB} \quad (32)\end{aligned}$$

So, the capacity of the effective return channel from Bob to Alice (relative to s) is

$$C_{A|B} = \log\frac{1}{\sigma^2_{\Delta s_A}}. \quad (33)$$

3) Optimal estimation at Eve: Recall that the signals received by Eve are $\mathbf{y}_{E,Am}$ in (22) and $\mathbf{y}_{E,B}$ in (26). Let $\mathbf{y}_E = \left[\mathbf{y}_{EA}^T, \mathbf{y}_{EB}^T\right]^T$. Then the MMSE estimate of s by Eve is

$$\hat{s}_E = \mathbb{E}\left\{s\mathbf{y}_E^H\right\}\left(\mathbb{E}\left\{\mathbf{y}_E\mathbf{y}_E^H\right\}\right)^{-1}\mathbf{y}_E \quad (34)$$

and its MSE is

$$\begin{aligned}\sigma^2_{\Delta s_E} &\doteq \mathbb{E}\left\{|\hat{s}_E - s|^2\right\} \\ &= 1-\mathbb{E}\left\{s\mathbf{y}_E^H\right\}\left(\mathbb{E}\left\{\mathbf{y}_E\mathbf{y}_E^H\right\}\right)^{-1}\left(\mathbb{E}\left\{s\mathbf{y}_E^H\right\}\right)^H. \quad (35)\end{aligned}$$

Here

$$\mathbb{E}\left\{s\mathbf{y}_E^H\right\} = \left[\mathbf{0}^T, \sqrt{\frac{p_B\gamma_{E,B}}{2}}\mathbf{h}_{E,B}^H\right], \quad (36)$$

$$\mathbb{E}\left\{\mathbf{y}_E\mathbf{y}_E^H\right\} = \begin{bmatrix}\mathbf{A} & \mathbf{C}\\ \mathbf{C}^H & \mathbf{B}\end{bmatrix}. \quad (37)$$

with

$$\mathbf{A} = \frac{p_A\gamma_{E,A}}{n_A}\mathbf{H}_{E,A}\mathbf{H}_{E,A}^H + \rho p_E\mathbf{H}_{E,E}\bar{\mathbf{h}}_{B,E}^*\bar{\mathbf{h}}_{B,E}^T\mathbf{H}_{E,E}^H + \mathbf{I}_{n_E} \quad (38)$$

$$\mathbf{B} = t_1\frac{p_B\gamma_{E,B}}{2}\mathbf{h}_{E,B}\mathbf{h}_{E,B}^H + \frac{\rho p_E}{n_E}\mathbf{H}_{E,E}\mathbf{H}_{E,E}^H + \mathbf{I}_{n_E} \quad (39)$$

$$\mathbf{C} = \sqrt{\frac{p_Ap_B\gamma_{E,A}\gamma_{E,B}}{2n_A}}\mathbf{H}_{E,A}\mathbf{r}\mathbf{h}_{E,B}^H, \quad (40)$$

where $t_1 = \sigma^2_{\hat{p}_0}+1$ and $\mathbf{r} = \mathbb{E}\{\mathbf{x}_A\hat{p}_0^*\}$. We have also used the independence between $\mathbf{x}_{A,E}$ and $\mathbf{x}_{B,E}$.

Let $\mathbf{Q} = [\mathbf{q}_1, \mathbf{Q}_1]$ be an $n_A \times n_A$ unitary matrix with $\mathbf{q}_1 = \bar{\mathbf{h}}_{B,A}^*$. Then

$$\begin{aligned}\mathbf{r} &= \mathbb{E}\left\{\mathbf{Q}\mathbf{Q}^H\mathbf{x}_A\hat{p}_0^*\right\} = \mathbf{Q}\begin{bmatrix}\sigma^2_{\hat{p}_0}\\ \mathbf{Q}_1^H\mathbf{r}\end{bmatrix} \\ &= \mathbf{Q}\begin{bmatrix}\sigma^2_{\hat{p}_0}\\ \mathbf{0}\end{bmatrix} = \sigma^2_{\hat{p}_0}\mathbf{q}_1. \quad (41)\end{aligned}$$

Therefore, it follows from (35) that

$$\sigma^2_{\Delta s_E} = 1-\frac{1}{2}p_B\gamma_{E,B}\mathbf{h}_{E,B}^H\left(\mathbf{B}-\mathbf{C}^H\mathbf{A}^{-1}\mathbf{C}\right)^{-1}\mathbf{h}_{E,B}. \quad (42)$$

Furthermore, $\mathbf{C}^H\mathbf{A}^{-1}\mathbf{C} = \frac{1}{2}t_2p_B\gamma_{E,B}\mathbf{h}_{E,B}\mathbf{h}_{E,B}^H$ with $t_2 = \frac{p_A\gamma_{E,A}}{n_A}\mathbf{r}^H\mathbf{H}_{E,A}^H\mathbf{A}^{-1}\mathbf{H}_{E,A}\mathbf{r}$. So,

$$\begin{aligned}\sigma^2_{\Delta s_E} =& 1-\frac{1}{2}p_B\gamma_{E,B}\mathbf{h}_{E,B}^H\left((t_1-t_2)\frac{p_B\gamma_{E,B}}{2}\mathbf{h}_{E,B}\mathbf{h}_{E,B}^H\right. \\ &\left.+\frac{\rho p_E}{n_E}\mathbf{H}_{E,E}\mathbf{H}_{E,E}^H+\mathbf{I}_{n_E}\right)^{-1}\mathbf{h}_{E,B}. \quad (43)\end{aligned}$$

The capacity of the effective return channel from Bob to Alice (relative to s) is

$$C_{E|B} = \log\frac{1}{\sigma^2_{\Delta s_E}}. \quad (44)$$

D. Secrecy Capacity of STEEP

Based on the classic wiretap channel theory and the above analysis of the effective channels with respect to the secret message transmitted from Bob, the secrecy capacity of STEEP (in bits per round-trip complex channel use) from (34) and (46) is $\bar{C}_{\texttt{STEEP}}$ with

$$C_{\texttt{STEEP}} = C_{A|B} - C_{E|B}. \quad (45)$$

Considering random channel realizations, especially when Eve's channels are unknown to users, we can use the secrecy outage probability of STEEP, relative to a target secrecy rate R_s, as defined below:

$$O_{\texttt{STEEP}}(R_s) = \texttt{Prob}(\bar{C}_{\texttt{STEEP}} \le R_s). \quad (46)$$

VI. Multiple UAVs against Full-duplex Eve

Now we consider M legitimate UAVs, and one full-duplex eavesdropper. We will examine the role of steep for multiple access with imperfect channels state information. in this case we assume that alice does not have the perfect channel state information but has a line of sight (LOS) between them. Based on the line-of-sight information alice can estimate the partial line of sight channel and formed a unit norm vector $\mathbf{v} \in \mathbb{C}^{n_A\times 1}$. $\gamma_{i,E}$ and $\gamma_{A,E}$ is the large scale fading gain for eve to i-the user and Alice respectively. According to phase -1 of STEEP [1], Alice sends random probing vector which can be denoted by $\sqrt{p_A/n_A}\mathbf{x}_A$. The signal received by i-th user and Eve in the first phase from Alice.

A. First Phase

$$y_i = \sqrt{\frac{p_A}{n_A}}\mathbf{h}_{i,A}^T\mathbf{x}_A + \sqrt{p_E\gamma_{i,E}}\mathbf{h}_{i,E}^T\mathbf{x}_{i,E} + w_i \quad (47)$$

$$= \sqrt{\frac{p_A}{n_A}}\mathbf{h}_{i,A}^T\mathbf{v}p + \sqrt{p_E\gamma_{i,E}}\mathbf{h}_{i,E}^T\mathbf{x}_{i,E} + w_i \quad (48)$$

where, $\mathbf{h}_{i,A} = e^{j\theta_i^d}(\frac{\alpha}{1+\alpha}\mathbf{h}_{u,0} + \frac{1}{1+\alpha}\Delta\mathbf{h}_{u,0})$ and from (47) Alice have the knowledge of only $\mathbf{h}_{u,0}$ so it can design the vector $\mathbf{v} = \frac{\mathbf{h}_{u,0}^*}{||\mathbf{h}_{u,0}||}$ based on the line-of-sight channel vector from AP to user-i. User knows the channel $\mathbf{h}_{i,A}$ but does not

know the p. so it can estimate p from the equation (47) where $p \sim \mathcal{CN}(0,1)$, $E\{|w_i|^2\} = \sigma_i^2$ and θ_i^d is uniformly distributed between [0,π] for probing phase. In this case, we assume that the jamming signal $\mathbf{x}_{i,E}$ from Eve to user-i is $\mathcal{CN}(0, \mathbf{I}_{n_E})$, . So we get from (47),

$$y_i = \sqrt{\frac{p_A}{n_A}} h_i p + \sqrt{p_E \gamma_{i,E}} \mathbf{h}_{i,E}^T \mathbf{x}_{i,E} + w_i \tag{49}$$

where, $h_i = \mathbf{h}_{i,A}^T \frac{\mathbf{h}_{u,0}^*}{||\mathbf{h}_{u,0}||}$, similarly eavesdropper will receive from Alice,

$$\mathbf{y}_{E,Am} = \sqrt{\frac{p_A}{n_A}} \mathbf{H}_{E,A} \mathbf{x}_A + \sqrt{\rho p_E} \mathbf{H}_{E,E} \mathbf{x}_{i,E} + \mathbf{w}_{E,A} \tag{50}$$

$$= \sqrt{\frac{p_A}{n_A}} \mathbf{H}_{E,A} \frac{\mathbf{h}_{u,0}^*}{||\mathbf{h}_{u,0}||} p + \sqrt{\rho p_E} \mathbf{H}_{E,E} \mathbf{x}_{i,E} + \mathbf{w}_{E,A} \tag{51}$$

$$= \sqrt{\frac{p_A}{n_A}} \bar{\mathbf{h}}_{E,A} p + \sqrt{\rho p_E} \mathbf{H}_{E,E} \mathbf{x}_{i,E} + \mathbf{w}_{E,A} \tag{52}$$

where, $\bar{\mathbf{h}}_{E,A} = \mathbf{H}_{E,A} \frac{\mathbf{h}_{u,0}^*}{||\mathbf{h}_{u,0}||}$. Now in phase-2 , multi user steep, M Users transmit their return signal concurrently using the same frequency band. where,$\sqrt{\frac{p_B}{2}}\,(\hat{p}_i + s)$

B. Second Phase

Alice has received,

$$\mathbf{y}_{Am} = \sum_{i=1}^{M} \sqrt{\frac{p_B}{2}} \mathbf{h}_{A,i} \left(\hat{p}_i + s_i\right) + \sqrt{\frac{p_E \gamma_{A,E}}{n_E}} \mathbf{H}_{A,E} \mathbf{x}_{A,E} + \mathbf{w}_A \tag{53}$$

$$= \sqrt{\frac{p_B}{2}} \mathbf{H}_A (\hat{\mathbf{p}} + \mathbf{s}) + \sqrt{\frac{p_E \gamma_{A,E}}{n_E}} \mathbf{H}_{A,E} \mathbf{x}_{A,E} + \mathbf{w}_A \tag{54}$$

where from (47), Alice knows $\mathbf{h}_{A,i}$ for all i and $\mathbf{H}_A \in \mathbb{C}^{n_A \times M} = [\mathbf{h}_{A,1}, \cdots, \mathbf{h}_{A,M}]$, and, $\mathbf{h}_{A,i} = e^{j\theta_i^u} (\frac{\alpha}{1+\alpha} \mathbf{h}_{A,i,0} + \frac{1}{1+\alpha} \Delta \mathbf{h}_{A,i})$, $\hat{\mathbf{p}} \in \mathbb{C}^{M \times 1} = [\hat{p}_1, \cdots, \hat{p}_M]^T$ and $\mathbf{s} \in \mathbb{C}^{M \times 1} = [s_1, \cdots, s_M]^T$. $\mathbf{w}_A$ is i.i.d $\sim \mathcal{CN}(0, \sigma_A^2 I)$ and θ_i^u is also uniformly distributed between [0,π] for echoing phase. and jamming signal $\mathbf{x}_{A,E}$ from Eve to Alice is $\mathcal{CN}(0, \mathbf{I}_{n_E})$. Moreover $\mathbf{x}_{A,E}$ is also independent of $\mathbf{x}_{i,E}$. similarly, eve will receive from the users in second phase,

$$\mathbf{y}_{E,U} = \sum_{i=1}^{M} \sqrt{p_B} \mathbf{h}_{E,i} \left(\hat{p}_i + s_i\right) + \sqrt{\frac{\rho p_E}{n_E}} \mathbf{H}_{E,E} \mathbf{x}_{A,E} + \mathbf{w}_{E,U} \tag{55}$$

$$= \sqrt{\frac{p_B}{2}} \bar{\mathbf{H}}_{E,U} (\hat{\mathbf{p}} + \mathbf{s}) + \sqrt{\frac{\rho p_E}{n_E}} \mathbf{H}_{E,E} \mathbf{x}_{A,E} + \mathbf{w}_{E,U} \tag{56}$$

where $\bar{\mathbf{H}}_{E,U} \in \mathbb{C}^{n_E \times M} = [\mathbf{h}_{E,1}, \cdots, \mathbf{h}_{E,M}]$,

C. Secrecy Analysis

1) Optimal estimation at user: From (47), first phase, since $\hat{p}$ is the MMSE estimate of p. it follows

$$\hat{p}_i = \frac{\sqrt{\frac{p_A}{n_A}} h_i^* y_i}{\frac{p_A}{n_A} |h_i|^2 + S_{i,E} + \sigma_i^2} \tag{57}$$

where, $S_{i,E} = p_E \gamma_{i,E} \mathbf{h}_{i,E}^T \mathbf{x}_{i,E} \mathbf{x}_{i,E}^H \mathbf{h}_{i,E}^*$ Also

$$\sigma_{\hat{p}_i}^2 \doteq \mathbb{E}\left\{|\hat{p}_i|^2\right\} = \frac{\frac{p_A}{n_A} |h_i|^2}{\frac{p_A}{n_A} |h_i|^2 + S_{i,E} + \sigma_i^2} \tag{58}$$

Furthermore, the MSE of $\hat{p}_i$ is

$$\sigma_{\Delta p_i}^2 = \mathbb{E}\left\{|\Delta p|^2\right\} = 1 - \frac{p_A}{n_A} h_i^* \left[\frac{p_A}{n_A} |h_i|^2 + S_{i,E} + \sigma_i^2\right]^{-1} h_i \tag{59}$$

$$= 1 - \sigma_{\hat{p}_i}^2 \tag{60}$$

2) Estimation at Alice: In phase 2 of NOMA multi-user STEEP, M-UEs transmit their return signals concurrently using the same frequency band from (53) The mean of $\mathbf{y}_{Am}$ given $\mathbf{x}_A$ and $\mathbf{H}_A$ is

$$\mathbb{E}\left\{\mathbf{y}_{Am} \mid \mathbf{x}_A, \mathbf{H}_A\right\} = \sum_{i=1}^{M} \sqrt{\frac{p_B}{2}} \mathbf{h}_{A,i} \sigma_{\hat{p}_s}^2 p_i \tag{61}$$

$$= \sqrt{\frac{p_B}{2}} \mathbf{H}_A \operatorname{diag}\left(\sigma_{\hat{p}_1}^2, \cdots, \sigma_{\hat{p}_M}^2\right) \mathbf{p} \tag{62}$$

$$= \sqrt{\frac{p_B}{2}} \mathbf{H}_A \mathbf{C} \mathbf{p} \tag{63}$$

with $\mathbf{C} = \operatorname{diag}\left(\sigma_{\hat{p}_1}^2, \cdots, \sigma_{\hat{p}_M}^2\right)$ and $\mathbf{p} = [p_1, \cdots, p_M]^T$.

$$\Delta \mathbf{y}_{Am} = \mathbf{y}_{Am} - \mathbb{E}\left\{\mathbf{y}_{Am} \mid \mathbf{x}_A, \mathbf{H}_A\right\} \tag{64}$$

$$= \sqrt{\frac{p_B}{2}} \mathbf{H}_A (\hat{\mathbf{p}} - \mathbf{C}\mathbf{p}) + \sqrt{\frac{p_B}{2}} \mathbf{H}_A \mathbf{s} + \sqrt{\frac{p_E \gamma_{A,E}}{n_E}} \mathbf{H}_{A,E} \mathbf{x}_{A,E} + \mathbf{w}_A \tag{65}$$

$$\Delta \mathbf{y}_{Am} = \sqrt{\frac{p_B}{2}} \mathbf{H}_A (\mathbf{I} - \mathbf{C}) \hat{\mathbf{p}} + \sqrt{\frac{p_B}{2}} \mathbf{H}_A \mathbf{C} \Delta \mathbf{p} + \sqrt{\frac{p_B}{2}} \mathbf{H}_A \mathbf{s} + \sqrt{\frac{p_E \gamma_{A,E}}{n_E}} \mathbf{H}_{A,E} \mathbf{x}_{A,E} + \mathbf{w}_A \tag{66}$$

Then, the MMSE estimate of s_1 by AP from $\mathbf{y}_{Am}$ is

$$\hat{s}_1 = \mathbb{E}\left\{s_1 \Delta \mathbf{y}_{Am}^H\right\} \left(\mathbb{E}\left\{\Delta \mathbf{y}_{Am} \Delta \mathbf{y}_{Am}^H\right\}\right)^{-1} \Delta \mathbf{y}_{Am}, \tag{67}$$

with

$$\mathbb{E}\left\{s_1 \Delta \mathbf{y}_{Am}^H\right\} = \sqrt{\frac{p_B}{2}} \mathbf{h}_{A,1}^H \tag{68}$$

$$\mathbb{E}\left\{\Delta \mathbf{y}_{Am} \Delta \mathbf{y}_{Am}^H\right\} = \frac{p_B}{2} \mathbf{H}_A (\mathbf{I} - \mathbf{C}) \mathbf{C} (\mathbf{I} - \mathbf{C}) \mathbf{H}_A^H + \frac{p_B}{2} \mathbf{H}_A \mathbf{C} (\mathbf{I} - \mathbf{C}) \mathbf{C} \mathbf{H}_A^H + \frac{p_B}{2} \mathbf{H}_A \mathbf{H}_A^H + \frac{p_E \gamma_{A,E}}{n_E} \mathbf{H}_{A,E} \mathbf{H}_{A,E}^H + \sigma_A^2 \mathbf{I}, \tag{69}$$

$$\mathbb{E}\left\{\Delta \mathbf{y}_{Am} \Delta \mathbf{y}_{Am}^H\right\} = \frac{p_B}{2} \mathbf{H}_A \mathbf{C}' \mathbf{H}_A^H + \frac{p_B}{2} \mathbf{H}_A \mathbf{H}_A^H + \frac{p_E \gamma_{A,E}}{n_E} \mathbf{H}_{A,E} \mathbf{H}_{A,E}^H + \sigma_A^2 \mathbf{I} \tag{70}$$

where $\mathbf{C}' = (\mathbf{I} - \mathbf{C}) \mathbf{C} (\mathbf{I} - \mathbf{C}) + \mathbf{C} (\mathbf{I} - \mathbf{C}) \mathbf{C} = (\mathbf{I} - \mathbf{C}) \mathbf{C}$

The MSE of $\hat{s}_1$ is

$$\sigma^2_{\Delta s_1} = 1 - \mathbb{E}\left\{s_1 \Delta \mathbf{y}^H_{Am}\right\} \left(\mathbb{E}\left\{\Delta \mathbf{y}_{Am} \Delta \mathbf{y}^H_{Am}\right\}\right)^{-1} \mathbb{E}\left\{s_1 \mathbf{y}^H_{Am}\right\}^H \tag{71}$$

$$= 1 - \frac{p_B}{2} \mathbf{h}^H_{A,1} \left(\frac{p_B}{2} \mathbf{H}_A \mathbf{C}' \mathbf{H}^H_A + \frac{p_B}{2} \mathbf{H}_A \mathbf{H}^H_A + \frac{p_E \gamma_{A,E}}{n_E} \mathbf{H}_{A,E} \mathbf{H}^H_{A,E} + \sigma^2_A \mathbf{I}\right)^{-1} \tag{72}$$

$$\mathbf{h}_{A,1}$$

The effective capacity from UE_1 to AP relative to s_1 is now

$$C_{A|1} = \log \frac{1}{\sigma^2_{\Delta s_1}} \tag{73}$$

Similarly, we have

$$C_{A|i} = \log \frac{1}{\sigma^2_{\Delta s_i}} \tag{74}$$

3) Estimation at Eve: The corresponding signals received by an ordinary Eve in phases 1 and 2 of STEEP are respectively and combine the both $\mathbf{y}_{E,Am}, \mathbf{y}_{E,U}$ from (73) and (74) as $\bar{\mathbf{y}}_E = \left[\mathbf{y}^T_{E,Am}, \mathbf{y}^T_{EU}\right]^T$. The MMSE estimate of s_1 by Eve is

$$\hat{s}_1 = \mathbb{E}\left\{s_1 \bar{\mathbf{y}}^H_E\right\} \left(\mathbb{E}\left\{\bar{\mathbf{y}}_E \bar{\mathbf{y}}^H_E\right\}\right)^{-1} \bar{\mathbf{y}}_E \tag{75}$$

and its MSE is

$$\begin{aligned} \sigma^2_{\Delta \bar{s}_E} &\doteq \mathbb{E}\left\{\left|\hat{s}_1 - s_1\right|^2\right\} \\ &= 1 - \mathbb{E}\left\{s_1 \bar{\mathbf{y}}^H_E\right\} \left(\mathbb{E}\left\{\bar{\mathbf{y}}_E \bar{\mathbf{y}}^H_E\right\}\right)^{-1} \left(\mathbb{E}\left\{s_1 \bar{\mathbf{y}}^H_E\right\}\right)^H \end{aligned} \tag{76}$$

Furthermore,

$$\mathbb{E}\left\{s_1 \bar{\mathbf{y}}^H_E\right\} = \left[\mathbf{0}^T, \sqrt{\frac{p_B}{2}} \mathbf{h}^H_{E,1}\right], \tag{77}$$

$$\mathbb{E}\left\{\bar{\mathbf{y}}_E \bar{\mathbf{y}}^H_E\right\} = \begin{bmatrix} \mathbf{R}_{AA} & \mathbf{R}_{AB} \\ \mathbf{R}^H_{AB} & \mathbf{R}_{BB} \end{bmatrix} \tag{78}$$

$$\mathbf{R}_{AA} = \frac{p_A}{n_A} \bar{\mathbf{h}}_{E,A} \bar{\mathbf{h}}^H_{E,A} + \rho p_E \mathbf{H}_{E,E} \mathbf{H}^H_{E,E} + \sigma^2_{E,A} \mathbf{I} \tag{79}$$

$$\mathbf{R}_{BB} = \frac{p_B}{2} \bar{\mathbf{H}}_{E,U} (\bar{\mathbf{R}} + \mathbf{I}) \bar{\mathbf{H}}^H_{E,U} + \frac{\rho p_E}{n_E} \mathbf{H}_{E,E} \mathbf{H}^H_{E,E} + \sigma^2_{EU} \mathbf{I} \tag{80}$$

$$\mathbf{R}_{AB} = \sqrt{\frac{p_A p_B}{2 n_A}} \bar{\mathbf{h}}_{E,A} \mathbf{r}^H_p \bar{\mathbf{H}}^H_{E,U} \tag{81}$$

and,

$$\mathbf{r}^H_p = \mathbb{E}\left\{p \hat{\mathbf{p}}^H\right\} = \left[\sigma^2_{\hat{p}_1}, \sigma^2_{\hat{p}_2}, \cdots, \sigma^2_{\hat{p}_M}\right]^T \tag{82}$$

where in (81),

$$\bar{\mathbf{R}} = \begin{bmatrix} \mathrm{r}_{1,1} & \mathrm{r}_{1,2} & \cdots & \mathrm{r}_{1,M} \\ \cdots & \cdots & \cdots & \cdots \\ \mathrm{r}_{M,1} & \mathrm{r}_{M,2} & \cdots & \mathrm{r}_{M,M} \end{bmatrix}.$$

for all i and j. For $1 \le i \le M, 1 \le j \le M$.

$$r_{i,i} = \sigma^2_{\hat{p}_i} \tag{83}$$

$$r_{i,j} = \frac{\left(\frac{P_A}{n_A}\right)^2 |h_i|^2 |h_j|^2}{\left(\frac{p_A}{n_A}|h_i|^2 + \sigma^2_i\right)\left(\frac{p_A}{n_A}|h_j|^2 + \sigma^2_j\right)} \tag{84}$$

finally from (76) we get,

$$\sigma^2_{\Delta \bar{s}_{E,1}} = 1 - \frac{p_B}{2} \mathbf{h}^H_{E,1} \left(\mathbf{R}_{BB} - \mathbf{R}^H_{AB} \mathbf{R}^{-1}_{AA} \mathbf{R}_{AB}\right)^{-1} \mathbf{h}_{E,1} \tag{85}$$

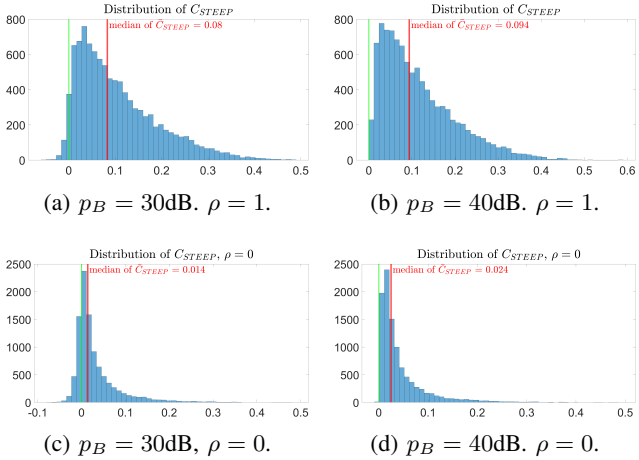
So, the capacity of the effective return channel from user-1 to Alice is

$$C_{E|1} = \log \frac{1}{\sigma^2_{\Delta \bar{s}_{E,1}}} \tag{86}$$

now (86) and (73), total secrecy capacity = $C_{A|1} - C_{E|1}$

VII. Numerical Results

In this section, we consider the scenario where Eve is directly below Bob (UAV), i.e., $\theta_{E,B} = \frac{\pi}{2}$. Hence we can choose $\gamma_{E,A} = \frac{1}{\cos^2 \theta_{B,A}}$ and $\gamma_{E,B} = \frac{1}{\sin^2 \theta_{B,A}}$ to reflect the relative channel gains. Furthermore, we assume that Bob is in the broadside of the antenna arrays at Alice and Eve, i.e., $\phi_{A,B} = \phi_{E,B} = 0$. Hence, $\mathbf{h}^L_{A,B} = \mathbf{h}^L_{E,B} = [1, \cdots, 1]^T$. We also assume that $K_{A,B} = K_{E,B} = 20$dB and $\alpha_s = 0.5$. The statistical results shown below are based on 10^4 independent realizations of all channel parameters.



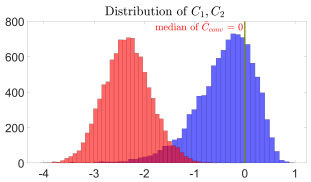
(a) $p_B = 30$dB. $\rho = 1$. (b) $p_B = 40$dB. $\rho = 1$.

(c) $p_B = 30$dB, $\rho = 0$. (d) $p_B = 40$dB. $\rho = 0$.

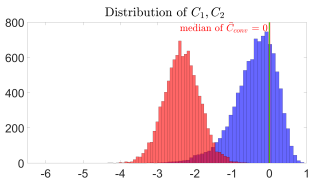
Fig. 3: Distributions of C_{STEEP} where $p_A = 20$dB, $p_E = 10$dB, $n_A = n_E = 4$ and $\theta_{B,A} = \frac{\pi}{6}$.

In Fig. 3, we show the distributions of C_{STEEP} for four combinations of $p_B = 30$dB or 40dB and $\rho = 1$ or 0. The principle of STEEP requires the channel quality in the echoing phase to be relatively strong to ensure a positive secrecy. So, here p_B is chosen to be 10dB and 20dB larger than p_A. We see indeed that C_{STEEP} is larger than zero with a high probability for the case of $p_B = 40$dB.

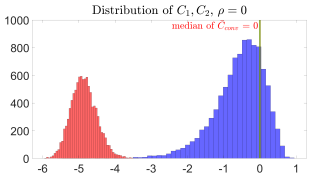
In contrast to Fig. 3, Fig. 4 shows the distributions of C_1 and C_2 for the conventional scheme where $p_B = 30, 40$dB and $\rho = 1, 0$. We see that in all cases, C_2 is less than zero (i.e., $\bar{C}_2 = 0$) with probability equal to one. A nonzero probability for $\bar{C}_{\mathrm{conv}} > 0$ comes from that of $C_1 > 0$, which is considerably smaller than the probability of $\bar{C}_{\mathrm{STEEP}} > 0$. Also note that



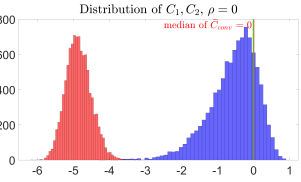
(a) $p_B = 30$dB. $\rho = 1$. C_1 (blue) is on the right, and C_2 (red) is on the left.



(b) $p_B = 40$dB. $\rho = 1$. C_1 is on the right, and C_2 is on the left.



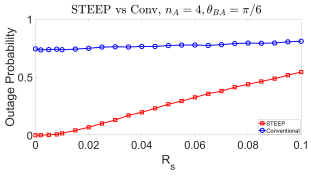
(c) $p_B = 30$dB. $\rho = 0$. C_1 is on the right, and C_2 is on the left.



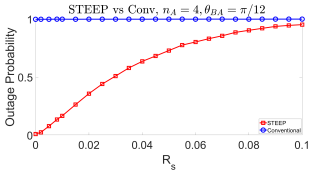
(d) $p_B = 40$dB. $\rho = 0$. C_1 is on the right, and C_2 is on the left.

Fig. 4: Distributions of C_1 and C_2 of the conventional scheme where $p_A = 20$dB, $p_E = 10$dB, $n_A = n_E = 4$, and $\theta_{B,A} = \frac{\pi}{6}$.

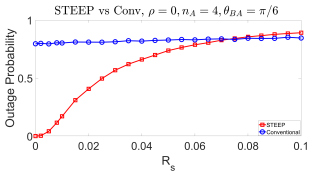
C_1 is invariant to p_B while C_2 is invariant to p_A. We also see that C_1 is not sensitive to ρ. This is because the noise at Eve is mostly due to the artificial noise from Alice, not due to self-interference. But C_2 reduces significantly as ρ decreases.



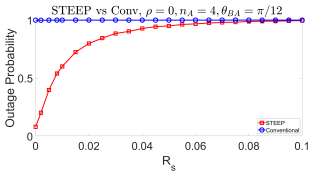
(a) $\theta_{B,A} = \frac{\pi}{6}$. $\rho = 1$.



(b) $\theta_{B,A} = \frac{\pi}{12}$. $\rho = 1$.



(c) $\theta_{B,A} = \frac{\pi}{6}$. $\rho = 0$.



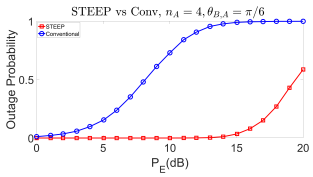
(d) $\theta_{B,A} = \frac{\pi}{12}$. $\rho = 0$.

Fig. 5: Secrecy outage probabilities versus R_s where $p_A = 20$dB, $p_B = 40$dB, $p_E = 10$dB and $n_A = n_E = 4$.

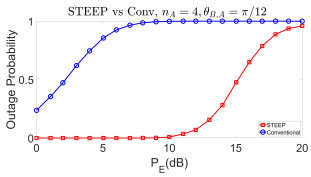
Fig. 5 compares the secrecy outage probabilities of the STEEP and conventional schemes (see (46) and (20)) versus a range of small but positive R_s for $\theta_{B,A} = \frac{\pi}{6}, \frac{\pi}{12}$ and $\rho = 1, 0$. As expected, for a small positive R_s, the outage rate of STEEP is small with a sufficiently large p_B.

Fig. 6 compares the secrecy outage probabilities of both schemes versus p_E. In all cases of $\theta_{B,A} = \frac{\pi}{6}$ or $\frac{\pi}{12}$ and $\rho = 1$ or 0, STEEP shows a much greater robustness against secrecy outage than the conventional scheme. As explained earlier, the performance of the conventional scheme is not sensitive to ρ.

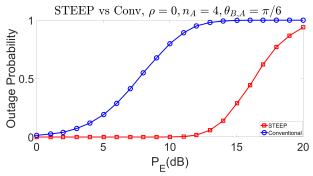
In Fig. 7, we compare the secrecy outage probabilities of both schemes versus the elevation angle $\theta_{B,A}$. We see that



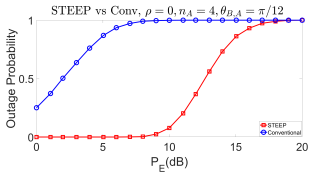
(a) $\theta_{B,A} = \frac{\pi}{6}$. $\rho = 1$.



(b) $\theta_{B,A} = \frac{\pi}{12}$. $\rho = 1$.

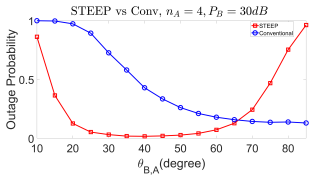


(c) $\theta_{B,A} = \frac{\pi}{6}$. $\rho = 0$.

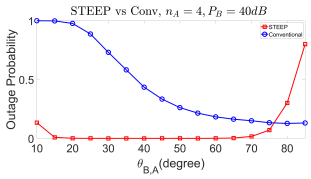


(d) $\theta_{B,A} = \frac{\pi}{12}$. $\rho = 0$.

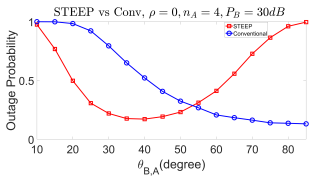
Fig. 6: Secrecy outage probabilities versus p_E where $R_s = 0$, $p_A = 20$dB, $p_B = 40$dB and $n_A = n_E = 4$.



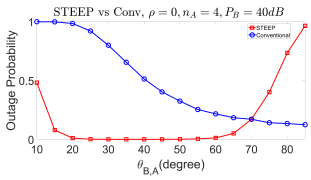
(a) $p_B = 30$dB. $\rho = 1$.



(b) $p_B = 40$dB. $\rho = 1$.



(c) $p_B = 30$dB. $\rho = 0$.



(d) $p_B = 40$dB. $\rho = 0$.

Fig. 7: Secrecy outage probabilities versus $\theta_{B,A}$ where $R_s = 0$, $p_A = 20$dB, $p_E = 10$dB and $n_A = n_E = 4$.

the conventional scheme always performs very poorly when $\theta_{B,A}$ is small but its performance improves as $\theta_{B,A}$ increases. Note that as $\theta_{B,A}$ reduces within $(0, \frac{\pi}{2})$, the channel gain between Bob and Eve (relative to the channel gain between Alice and Bob) increases, and as $\theta_{B,A}$ increases, the channel gain between Alice and Eve increases. When Eve is close to Alice, the artificial noise from Alice with multiple antennas is effective. But when Eve is close to Bob, the reception quality at Bob suffers significantly due to the jamming noise from the full-duplex Eve. However, for STEEP, we see that there is a wide range of $\theta_{B,A}$ within which the secrecy outage rate is virtually zero. We also see that as p_B increases, this range increases. In fact, it can be shown that for any $0 < \theta_{B,A} < \frac{\pi}{2}$ (and given all other parameters), there is a finite threshold of p_B beyond which $\bar{C}_{\text{STEEP}} > 0$.

VIII. Conclusion

In this paper, we have examined a novel application of STEEP for UAV communications subject to both jamming and eavesdropping from a full-duplex multi-antenna active

adversary (Eve). The legitimate nodes in this applications are a single-antenna UAV (Bob) and a multi-antenna ground station (Alice). We have analyzed the secrecy capacity of STEEP for this application as well as the secrecy capacity of a widely adopted conventional scheme using artificial noise from Alice. We have provided numerical illustrations of these secrecy capacities and their corresponding secrecy outage probabilities.

REFERENCES

[1] H. Lei, et al., "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1230-1244, Feb. 2020.

[2] G. Pan, H. Lei, J. An, S. Zhang and M.-S. Alouini, "On the secrecy of UAV systems with linear trajectory," IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6277-6288, Oct. 2020.

[3] H. Wu, Y. Wen, J. Zhang, Z. Wei, N. Zhang and X. Tao, "Energy-efficient and secure air-to-ground communication with jittering UAV," IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 3954-3967, April 2020.

[4] T. Li et al., "Secure UAV-to-vehicle communications," in IEEE Transactions on Communications, vol. 69, no. 8, pp. 5381-5393, Aug. 2021, doi: 10.1109/TCOMM.2021.3074969.

[5] X. Yuan, Z. Feng, W. Ni, Z. Wei, R. P. Liu and J. A. Zhang, "Secrecy rate analysis against aerial eavesdropper," IEEE Transactions on Communications, vol. 67, no. 10, pp. 7027-7042, Oct. 2019, doi: 10.1109/TCOMM.2019.2927449.

[6] C. Liu, J. Lee and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," IEEE Transactions on Wireless Communications, vol. 18, no. 6, pp. 2919-2931, June 2019,

[7] Y. Hua, "Generalized channel probing and generalized pre-processing for secret key generation," IEEE Transactions on Signal Processing, vol. 71, pp. 1067-1082, March 2023, doi: 10.1109/TSP.2023.3259142.

[8] Y. Hua, "Secret-message transmission by echoing encrypted probes — STEEP", 2309.14529.pdf (arxiv.org), Sept 2023.

[9] Y. Hua and M. S. Rahman, "Unification of secret key generation and wiretap channel transmission," arXiv:2403.06438 (preprint), to appear in IEEE ICC'2024, June 2024.

[10] Y. Hua, M. S. Rahman and A. Swami, "A Method for Low-Latency Secure Multiple Access," 2024 IEEE 30th International Symposium on Local and Metropolitan Area Networks (LANMAN), Boston, MA, USA, 2024, pp. 9-14, doi: 10.1109/LANMAN61958.2024.10621876.

[11] M. S. Rahman and Y. Hua"Secure UAV Communications By STEEP Against Full-Duplex Active Eavesdropper," to appear in asilomar, Oct 2024

[12] M. Hayashi and Á. Vázquez-Castro, "Two-way physical layer security protocol for Gaussian channels," IEEE Transactions on Communications, vol. 68, no. 5, pp. 3068-3078, May 2020, doi: 10.1109/TCOMM.2020.2973618.

[13] X. Zhao, K. Yu, D. Li, X. Liu and C. Luo, "Secure Ultra-reliable and Low Latency Communication in NOMA-UAV Networks," 2023 19th International Conference on Mobility, Sensing and Networking (MSN), Nanjing, China, 2023, pp. 127-134, doi: 10.1109/MSN60784.2023.00031.

[14] Y. Chen, G. Liu, Z. Zhang, L. He and S. He, "Improving Physical Layer Security for multi-UAV Systems Against Hybrid Wireless Attacks," in IEEE Transactions on Vehicular Technology, vol. 73, no. 5, pp. 7034-7048, May 2024, doi: 10.1109/TVT.2023.3337154.

[15] D. Diao, B. Wang, K. Cao, J. Weng, R. Dong and T. Cheng, "Secure Wireless-Powered NOMA Communications in Multi-UAV Systems," in IEEE Transactions on Green Communications and Network- ing, vol. 7, no. 3, pp. 1205-1216, Sept. 2023, doi: 10.1109/TGCN.2023.3283608.