This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

Caching and UAV Friendly Jamming for Secure Communications With Active Eavesdropping Attacks

Yi Zhou, Phee Lep Yeoh, Cunhua Pan, Kezhi Wang, Zheng Ma, Branka Vucetic and Yonghui Li

***Abstract*—In this paper, we discuss the security and reliability performance of a communication system, where the base station (BS) transmits signals to multiple users and an unmanned aerial vehicle (UAV) jammer sends friendly jamming signals to protect against a full-duplex active eavesdropper with the aid of caching. We derive the closed-form expressions of outage probability (OP) and intercept probability (IP) for the legitimate users and active eavesdropper, respectively. Aimed at minimizing the sum of the IP and the maximum OP among all users, we jointly optimize the BS transmit power, UAV jammer location and jamming power. An efficient algorithm based on alternating optimization (AO) and successive convex approximation (SCA) methods is designed to solve the optimization problem. Numerical results show that compared to other benchmark strategies, the proposed solution improves the reliability and security performance with the aid of caching and UAV friendly jamming.**

***Index Terms*—Physical layer security, UAV communications, active eavesdropper, caching, jamming.**

I. Introduction

By exploiting the characteristics of high mobility, ubiquitous coverage and swift deployment, unmanned aerial vehicle (UAV) has been considered to be a promising technology supporter for the incoming sixth-generation (6G) wireless communications [1]–[5]. In [3], by jointly optimizing the communication and computing resources, the authors proposed a UAV-enabled latency minimization virtual reality delivery framework. In [4], a UAV-to-Everything (U2X) communication network was established and the key techniques of U2X communications including sensing protocol, UAV trajectory design and resource management were investigated. The authors in [5] developed a UAV-assisted ultra-reliable and low-latency communication framework with delay and packet loss probability considerations.

The work of Y. Zhou was supported by the Natural Science Foundation of Sichuan under Grant 2022NSFSC0887 and the Fundamental Research Funds for the Central Universities under Grant 2682021ZTPY117 and 2682022CX020. The work of P. L. Yeoh was supported by ARC under Grant DP190100770. The work of B. Vucetic was partially supported by ARC Laureate Fellowship under Grant FL160100032. The work of Y. Li was supported by ARC under Grant DP190101988 and DP210103410.

Y. Zhou and Z. Ma are with the Key Lab of Information Coding, and Transmission, Southwest Jiaotong University, Chengdu 610031, China. (e-mail:yizhou@swjtu.edu.cn;zma@home.swjtu.edu.cn).

P. L. Yeoh, B. Vucetic, and Y. Li are with the School of Electrical and Information Engineering, University of Sydney, NSW 2006, Australia (e-mail: phee.yeoh@sydney.edu.au; branka.vucetic@sydney.edu.au; yonghui.li@sydney.edu.au).

C. Pan is with the National Mobile Communications Research Laboratory, Southeast University, China. (e-mail:cpan@seu.edu.cn).

K. Wang is with the Department of Computer and Information Sciences, Northumbria University, Newcastle NE2 1XE, U.K. (e-mail: kezhi.wang@northumbria.ac.uk).

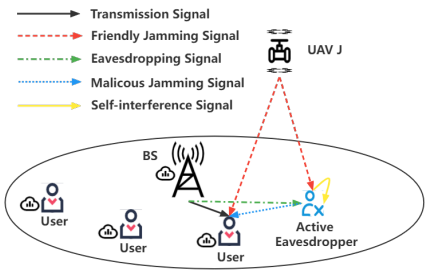

Fig. 1. A caching and UAV-enabled jamming communication system with an active eavesdropper.

However, due to the broadcast nature of wireless transmissions, the security of legitimate signals between BS and users could be compromised by nearby passive eavesdroppers intercepting the transmissions [6]–[9]. Unlike passive eavesdroppers, an active eavesdropper who operates in a full-duplex mode could perform malicious jamming and eavesdropping at the same time, resulting in a further degraded secrecy performance [10]–[14]. To tackle this issue, friendly jamming, an efficient physical layer security (PLS) technique has become a desirable solution to enhance the security in wireless communications by sending artificial noise. In [13], a two-fold zero-forcing jamming and beamforming scheme was proposed to prevent both active and passive eavesdroppers in terrestrial communications. In [14], based on jamming and beamforming, an effective secure transmission scheme was designed to protect the indoor visible light communication networks from being attacked by active and passive eavesdroppers.

Recently, the potential advantages of caching in improving security have been considered by exploiting the caching capabilities of legitimate users. In [15], by adopting different transmission schemes, the authors showed that the PLS performance can be improved significantly with the aid of caching. More recently, the security transmission algorithms of cache-enabled UAV communication systems were proposed in [16], [17] to protect the systems from passive eavesdropping attacks. However, we note that only limited research attention has been paid to prevent active eavesdropping attacks by employing the advantages of caching and UAV-enabled jamming.

Motivated by the above observations, in this paper, we propose a caching and UAV-enabled secure communication system where a symbol-level transmission strategy and a UAV friendly jammer are jointly adopted to against active eavesdropping attacks. Different from our previous work in [6] where only a UAV jammer is deployed to protect against passive eavesdropping attacks, this paper jointly considers the benefits of caching and jamming to prevent more advanced

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

attacks from a full-duplex active eavesdropper, thus resulting in a new system model and optimization framework for secure UAV communications.

We detail the main contributions of our paper as follows. We examine the reliability and security performance and derive the closed-form expressions of the outage probability (OP) and intercept probability (IP) for legitimate users and active eavesdropper, respectively. Next, we develop an efficient algorithm based on alternating optimization (AO) and successive convex approximation (SCA) methods to minimize the sum of the IP and the maximum OP among all users, where the BS transmit power, UAV jammer location and jamming power are jointly optimized. Our proposed algorithm is proven to quickly converge due to the iterative optimization of the BS and UAV design parameters. Finally, simulation results provide novel insights into the security and reliability advantages of caching and UAV friendly jamming.

II. System Model and Problem Formulation

Fig. 1 shows a caching and UAV-enabled secure communication system where one BS with caching capability is broadcasting signals to N ground users via frequency-division multiple access (FDMA) with one full-duplex active eavesdropper. The active eavesdropper is located at $\mathbf{v} = (x_e, y_e)^T \in \mathbb{R}^{2\times 1}$ and works on a full-duplex mode with two antennas to perform eavesdropping and malicious jamming attacks simultaneously. To further enhance security, a UAV J with caching capability is deployed as an aerial friendly jammer to send jamming signals to both the legitimate users and active eavesdropper, where the UAV jammer is fixed at altitude H with horizontal coordinate of $\mathbf{y} = (x_j, y_j)^T \in \mathbb{R}^{2\times 1}$.

A. Caching-Enabled Transmission Strategies

Denote $\mathcal{F} \triangleq \{f_1, f_2, \cdot\cdot, f_M\}$ as the file library with M same length files. We assume that each user has limited caching capacity while the BS with sufficient caching capability has stored all files in its large-size caching container during the off-peak time. Based on the caching status at each user, we consider the following caching-enabled transmission strategies.

1) Self Offloading: In this scenario, the file f_i requested by the i-th user has been cached at its cache container. Thus, the perfect secrecy can be guaranteed since the required file can be fetched locally without being overheard in the downlink transmissions.

2) Symbol-Level Transmission Strategy: In this case, the file f_i requested by the i-th user has not been cached at itself and needs to be transmitted from the BS. Aiming at improving the security and reliability performance, a symbol-level transmission strategy is adopted where the BS combines the file f_i requested by the i-th user with an additional file $f_k, f_k \neq f_i, \forall f_k \in \mathcal{F}$ by assigning different powers between the two signals to the i-th user. Without loss of generality, we assume that the probability of the i-th user to precache the file f_k follows the Zipf distribution, which is given by [19]

$$P_{i,k}^0 = \frac{1/k^\kappa}{\sum_k 1/k^\kappa}, k = 1, 2, \cdot\cdot\cdot, M, \forall i \in \mathcal{N}, \tag{1}$$

where κ denotes the skewness of the distribution. By doing so, the transmission signal s_i from the BS to the i-th user is expressed as

$$s_i = x_i\sqrt{\theta p_b} + x_k\sqrt{(1-\theta)p_b}, \forall i \in \mathcal{N}, \tag{2}$$

where x_i and x_k are the signals of the files f_i and f_k with $\mathbb{E}(|x_i|^2) = \mathbb{E}(|x_k|^2) = 1$, respectively. Moreover, p_b represents the BS transmit power and θ represents the power allocation ratio. With the aid of caching, we consider that the UAV friendly jammer transmits the file f_k to interfere both the legitimate users and active eavesdropper. Thus, the transmitted signal s_{uav} is given by

$$s_{uav} = x_k\sqrt{p_u}, \tag{3}$$

where p_u is the transmit power at the UAV frinedly jammer.

We note that if the file f_k has been cached at the i-th user, the corresponding interference signal x_k either from the BS or from the UAV jammer can thus be perfectly cancelled by applying the similar method of successive interference cancellation (SIC) as proposed in [15], [17], while the interference signal x_k cannot be eliminated if f_k has not been cached at the i-th user. Since the eavesdropper does not have the caching capability, the interference signal x_k cannot be eliminated at the active eavesdropper as well.

B. Communication Model

We consider a quasi-static Rayleigh fading model to capture the scattering and reflection effects for ground channels and define $g_{b,i}$, $g_{e,i}$ and $g_{b,e}$ as the small-scale fading variables for the channels from the BS to the i-th user, from the active eavesdropper to the i-user and from the BS to the active eavesdropper, respectively. Assume that the BS and ground users are located at $\mathbf{s} = (x_b, y_b)^T \in \mathbb{R}^{2\times 1}$ and $\mathbf{w}_i = (x_i, y_i)^T \in \mathbb{R}^{2\times 1}$, respectively. Thus, the corresponding large-scale path losses from the BS to the i-th user, from the active eavesdropper to the i-user and from the BS to the active eavesdropper can be defined as $h_{b,i} = \frac{\beta_1}{||\mathbf{s}-\mathbf{w}_i||^\alpha}$, $h_{e,i} = \frac{\beta_1}{||\mathbf{v}-\mathbf{w}_i||^\alpha}$ and $h_{b,e} = \frac{\beta_1}{||\mathbf{s}-\mathbf{v}||^\alpha}$, respectively, where β_1 is the reference channel power gain at $d_0 = 1$ m and $\alpha \geq 2$ is the path loss component.

Since UAV J is fixed at certain altitude, the corresponding air-to-ground (A2G) communication channels experience better line-of-sight (LoS) propagation and less shadowing. Thus, we consider a large-scale path loss-based pure LoS channel model and the channel gain from UAV J to the i-th ground user can be written as [7]

$$h_{u,i} = \frac{\beta_1}{H^2 + ||\mathbf{y} - \mathbf{w}_i||^2}, \forall i \in \mathcal{N}. \tag{4}$$

For the i-th user, the interference signal x_k can either be cancelled or not based on its caching status. Thus, the corresponding signal-to-interference-plus-noise ratio (SINR) is given by

$$\begin{cases} \gamma_i^0 = \dfrac{p_b\theta h_{b,i}g_{b,i}}{p_e h_{e,i}g_{e,i} + \sigma^2}, & \text{with } P_{i,k}^0 \\ \gamma_i^1 = \dfrac{p_b\theta h_{b,i}g_{b,i}}{p_u h_{u,i} + p_e h_{e,i}g_{e,i} + \sigma^2 + p_b(1-\theta)h_{b,i}g_{b,i}}, & \text{with } P_{i,k}^1, \end{cases} \tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

where σ^2 is the noise power at the receiver, p_e is the transmit power at the active eavesdropper. Moreover $P_{i,k}^1 = 1 - P_{i,k}^0$ represents the probability that the file f_k has not been cached at the i-th user.

Similarly, the channel gain for the A2G link transmitted from UAV J to the active eavesdropper is given by

$$h_{u,e} = \frac{\beta_1}{H^2 + ||\mathbf{y} - \mathbf{v}||^2}. \tag{6}$$

For the active eavesdropper, since the interference signal x_k cannot be eliminated, the SINR for eavesdropping each transmission is given by

$$\gamma_e = \frac{p_b \theta h_{b,e} g_{b,e}}{p_b(1-\theta)h_{b,e}g_{b,e} + p_u h_{u,e} + \xi p_e + \sigma^2}, \tag{7}$$

where ξp_e is the residual self-interference (SI) power at the active eavesdropper with ξ being the SI efficiency of the active eavesdropper who is operating in the full-duplex mode.

C. Reliability and Security Measurements

In this subsection, the OP for the legitimate users and IP for the active eavesdropper are derived to examine the reliability and security performance of our proposed communication systems. For legitimate transmissions, the outage occurs when the SINR of the legitimate user is less than a pre-defined positive threshold ϕ [20]. Therefore, the corresponding OP for the i-th user is given by

$$\begin{aligned} P_{out,i} =& P_{i,k}^0 P_r(\gamma_i^0 < \phi) + P_{i,k}^1 P_r(\gamma_i^1 < \phi) \\ =& P_{i,k}^0 \underbrace{\left(1 - \frac{1}{1 + \frac{\phi p_e h_{e,i}}{\mathcal{I}_{0,i}}} \exp\left(-\frac{\phi \sigma^2}{\mathcal{I}_{0,i}}\right)\right)}_{P_{out,i}^0} + \\ & P_{i,k}^1 \underbrace{\left(1 - \frac{1}{1 + \frac{\phi p_e h_{e,i}}{\mathcal{I}_{2,i}}} \exp\left(-\frac{\phi \mathcal{I}_{1,i}}{\mathcal{I}_{2,i}}\right)\right)}_{P_{out,i}^1}, \forall i \in \mathcal{N}, \end{aligned} \tag{8}$$

where $\mathcal{I}_{0,i} = p_b \theta h_{b,i}$, $\mathcal{I}_{1,i} = p_u h_{u,i} + \sigma^2$ and $\mathcal{I}_{2,i} = p_b h_{b,i}(\theta - \phi + \theta\phi)$.

Proof. Please refer to Appendix A. □

For the eavesdropping link, the interception occurs when the SINR of the active eavesdropper is larger than a positive threshold τ [6]. Thus, the corresponding IP can be given as

$$\begin{aligned} P_{int} &= P_r(\gamma_e > \tau) = P_r\left(g_{b,e} > \frac{\tau \mathcal{I}_4}{\mathcal{I}_5 - \tau \mathcal{I}_6}\right) \\ &\overset{(c)}{=} \exp\left(-\frac{\tau \mathcal{I}_4}{\mathcal{I}_5 - \tau \mathcal{I}_6}\right), \end{aligned} \tag{9}$$

where $\mathcal{I}_4 = p_u h_{u,e} + \xi p_e + \sigma^2$, $\mathcal{I}_5 = p_b \theta h_{b,e}$ and $\mathcal{I}_6 = p_b(1-\theta)h_{b,e}$. Moreover, (c) holds since the small-scale fading variable of $g_{b,e}$ follows the exponential distribution.

D. Problem Formulation

In this paper, with the aim of improving the reliability and security performance of our proposed system, we consider to minimize the sum of the IP and the maximum OP among all users. We jointly optimize the BS transmit power p_b, UAV jammer location $\mathbf{y} = (x_j, y_j)^T$ and jamming power p_u. As such, the optimization problem can be formulated as

$$\underset{p_b, \mathbf{y}, p_u}{\text{minimize}} \ \max_{i \in \mathcal{N}} P_{out,i} + P_{int} \tag{10a}$$

$$\text{s.t. } 0 \le p_u \le p_u^{max}, 0 \le p_b \le p_b^{max}. \tag{10b}$$

We note that due to the $\max(\cdot)$ operation in the objective function, it is challenging to derive the mathematically tractable expression of the objective function. To simplify the analysis, we introduce three variables q, x and z representing the $\max_{i \in \mathcal{N}} P_{i,k}^0 P_{out,i}^0$, $\max_{i \in \mathcal{N}} P_{i,k}^1 P_{out,i}^1$ and the upper bound of the IP, respectively, and reformulate the optimization problem as

$$\underset{p_b, \mathbf{y}, p_u, q, x, z}{\text{minimize}} \ q + x + z \tag{11a}$$

$$\text{s.t. } P_{i,k}^0 P_{out,i}^0 \le q, \forall i \in \mathcal{N} \tag{11b}$$

$$P_{i,k}^1 P_{out,i}^1 \le x, \forall i \in \mathcal{N} \tag{11c}$$

$$P_{int} \le z \tag{11d}$$

$$0 \le p_u \le p_u^{max}, 0 \le p_b \le p_b^{max}. \tag{11e}$$

We note that Problem (11) is non-convex and very challenging to solve due to the strong coupling effects between all variables. In the following, we adopt the AO method to solve the BS transmit power, UAV jammer location and jamming power in an iterative manner.

III. Proposed Solution

A. Solving BS Transmit Power

With fixed $\{\mathbf{y}, p_u\}$, the BS transmit power subproblem can be transformed as

$$\underset{p_b, q, x, z}{\text{minimize}} \ q + x + z \tag{12a}$$

$$\text{s.t. } 1 - \frac{q}{P_{i,k}^0} \le \frac{\exp(-\frac{c_{0,i}}{p_b})}{1 + \frac{c_{1,i}}{p_b}}, \forall i \in \mathcal{N} \tag{12b}$$

$$1 - \frac{x}{P_{i,k}^1} \le \frac{\exp(-\frac{c_{2,i}}{p_b})}{1 + \frac{c_{3,i}}{p_b}}, \forall i \in \mathcal{N} \tag{12c}$$

$$\frac{\tau \mathcal{I}_4}{p_b h_{b,e}(\theta - \tau + \tau\theta)} \ge -\ln(z) \tag{12d}$$

$$0 \le p_b \le p_b^{max}, \tag{12e}$$

where $c_{0,i} = \frac{\phi \sigma^2}{\theta h_{b,i}}$ and $c_{1,i} = \frac{\phi p_e h_{e,i}}{\theta h_{b,i}}$, $c_{2,i} = \frac{\phi(p_u h_{u,i} + \sigma^2)}{h_{b,i}(\theta - \phi + \theta\phi)}$ and $c_{3,i} = \frac{\phi p_e h_{e,i}}{h_{b,i}(\theta - \phi + \theta\phi)}$.

To solve Problem (12), we first analyze the monotonicity and convexity of the right-hand sides (RHSs) of (12b) and (12c) in the following Lemma.

Lemma 1. *The RHSs of* (12b) *and* (12c) *are decreasing and convex functions with respect to* $\frac{1}{p_b}$.

Proof. We note that the RHSs of (12b) and (12c) have the same structure in terms of $1/p_b$, therefore, we only prove Lemma 1 with the RHS of (12b) and the similar proof for (12c) is omitted for brevity. To show this, we denote $g(v) = \frac{\exp(-v c_{0,i})}{1 + v c_{1,i}}$, and we have

$$\frac{\partial g}{\partial v} = -\frac{\exp(-v c_{0,i})(c_{0,i} + c_{0,i} c_{1,i} v + c_{1,i})}{(1 + v c_{1,i})^2} < 0 \tag{13a}$$

$$\begin{aligned} \frac{\partial^2 g}{\partial v^2} =& \left(\frac{c_{0,i}^2}{(1 + v c_{1,i})} + \frac{2 c_{1,i}(c_{0,i} + c_{0,i} c_{1,i} v + c_{1,i})}{(1 + v c_{1,i})^3}\right) \\ & \times \exp(-v c_{0,i}) > 0, \end{aligned} \tag{13b}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

which indicates that $g(v)$ is a decreasing and convex function with respect to v. □

With Lemma 1, by introducing a slack variable v, we can rewrite the BS transmit power subproblem as

$$\underset{p_b,q,x,z,v}{\text{minimize}}\ q+x+z \tag{14a}$$

$$\text{s.t. } 1-\frac{q}{P^0_{i,k}} \le \frac{\exp(-vc_{0,i})}{1+vc_{1,i}}, \forall i \in \mathcal{N} \tag{14b}$$

$$1-\frac{x}{P^1_{i,k}} \le \frac{\exp(-vc_{2,i})}{1+vc_{3,i}}, \forall i \in \mathcal{N} \tag{14c}$$

$$v \ge \frac{1}{p_b},\ \text{(12d)},\ \text{(12e)}.$$

To convexify (14b), we apply the SCA solution to derive a lower bound of the RHS of (14b) based on the first-order Taylor expansion, which is given by

$$\mathcal{Y}_1(i) = \frac{\exp(-v^k c_{0,i})}{1+v^k c_{1,i}} - \frac{m_i \exp(-v^k c_{0,i})(v-v^k)}{(1+v^k c_{1,i})^2}, \tag{15}$$

where $m_i = c_{0,i}(1+v^k c_{1,i}) + c_{1,i}$ and v^k corresponds to the value of v in the k-th iteration. Similar approach can be used to transform the RHS of (14c) as follows

$$\mathcal{Y}_2(i) = \frac{\exp(-v^k c_{2,i})}{1+v^k c_{3,i}} - \frac{n_i \exp(-v^k c_{2,i})(v-v^k)}{(1+v^k c_{3,i})^2}, \tag{16}$$

where $n_i = c_{2,i}(1+v^k c_{3,i}) + c_{3,i}$.

Next, to convexify (12d), a concave lower bound of the left-hand side (LHS) of (12d) based on the first-order Taylor expansion is given by

$$\mathcal{Y}_3 = \frac{\tau \mathcal{I}_4}{p_b^k h_{b,e}(\theta-\tau+\tau\theta)} - \frac{\tau \mathcal{I}_4 (p_b - p_b^k)}{(p_b^k)^2 h_{b,e}(\theta-\tau+\tau\theta)}, \tag{17}$$

where p_b^k is the value of p_b in the k-th iteration.

With (15), (16) and (17), the BS transmit power subproblem can be approximated as

$$\underset{p_b,q,x,z,v}{\text{minimize}}\ q+x+z \tag{18a}$$

$$\text{s.t. } 1-\frac{q}{P^0_{i,k}} \le \mathcal{Y}_1(i), \forall i \in \mathcal{N} \tag{18b}$$

$$1-\frac{x}{P^1_{i,k}} \le \mathcal{Y}_2(i), \forall i \in \mathcal{N} \tag{18c}$$

$$\mathcal{Y}_3 \ge -\ln(z),\ v \ge \frac{1}{p_b},\ 0 \le p_b \le p_b^{max}. \tag{18d}$$

Due to its convexity, Problem (18) can be efficiently solved by using the convex optimization tool such as CVX.

B. Solving UAV Jammer Location

We note that $P^0_{out,i}$ is independent of $\mathbf{y}$ since the friendly jamming signal can be perfectly cancelled when the file f_k has been cached at the i-th user. Thus, with fixed $\{p_b, p_u\}$, by denoting one auxiliary variable η as the maximum OP among all users, the UAV jammer location can be derived by solving

$$\underset{\mathbf{y},\eta,z}{\text{minimize}}\ \eta+z \tag{19a}$$

$$\text{s.t. } P^0_{i,k}P^0_{out,i} + P^1_{i,k}\left(1-\mathcal{A}_i \exp\left(-\frac{\phi \mathcal{I}_{1,i}}{\mathcal{I}_{2,i}}\right)\right) \le \eta, \forall i \in \mathcal{N} \tag{19b}$$

$$\exp\left(-\frac{\tau \mathcal{I}_4}{\mathcal{I}_5 - \tau \mathcal{I}_6}\right) \le z, \tag{19c}$$

where $\mathcal{A}_i = 1/(1+\frac{\phi p_e h_{e,i}}{\mathcal{I}_{2,i}})$.

By introducing one set of auxiliary variables $\boldsymbol{t} = [t_1, t_2, \cdots, t_i], \forall i \in \mathcal{N}$ and a slack variable u and after taking several mathematical manipulations, we transform Problem (19) as follows

$$\underset{\mathbf{y},\eta,z,\boldsymbol{t},u}{\text{minimize}}\ \eta+z \tag{20a}$$

$$\text{s.t. } \frac{p_u \beta_1}{H^2+t_i} \le -\frac{\mathcal{I}_{2,i}}{\phi}\ln\left(\frac{1-(\eta - P^0_{i,k}P^0_{out,i})/P^1_{i,k}}{\mathcal{A}_i}\right) - \sigma^2, \forall i \in \mathcal{N} \tag{20b}$$

$$\frac{p_u \beta_1}{H^2+u} + \xi p_e + \sigma^2 \ge -\frac{\mathcal{I}_5 - \tau \mathcal{I}_6}{\tau}\ln z \tag{20c}$$

$$||\mathbf{y}-\mathbf{w}_i||^2 \ge t_i \tag{20d}$$

$$||\mathbf{y}-\mathbf{v}||^2 \le u. \tag{20e}$$

We note that constraints (20b) and (20c) are non-convex since both the LHSs and RHSs are convex. To convexify constraints (20b), we derive the concave lower bound of the RHS based on the first-order Taylor expansion as follows

$$\begin{aligned}\mathcal{W}_i = &-\frac{\mathcal{I}_{2,i}}{\phi}\ln\left(\frac{1-(\eta^k - P^0_{i,k}P^0_{out,i})/P^1_{i,k}}{\mathcal{A}_i}\right) - \sigma^2 \\ &+ \frac{\mathcal{I}_{2,i}(\eta-\eta^k)}{\phi(P^1_{i,k} - (\eta^k - P^0_{i,k}P^0_{out,i}))},\end{aligned} \tag{21}$$

where η^k corresponds to the value of η in the k-th iteration.

To convexity (20c), based on the first-order Taylor expansion, we adopt the SCA method to transform $\frac{p_u\beta_1}{H^2+u}$ as follows

$$\mathcal{S} = \frac{p_u \beta_1}{H^2+u^k} - \frac{p_u \beta_1 (u-u^k)}{(H^2+u^k)^2}, \tag{22}$$

where u^k corresponds to the value of u in the k-th iteration.

We also transform (20d) by applying the similar solution and approximate the UAV jammer location subproblem as

$$\underset{\mathbf{y},\eta,z,\boldsymbol{t},u}{\text{minimize}}\ \eta+z \tag{23a}$$

$$\text{s.t. } \frac{p_u \beta_1}{H^2+t_i} \le \mathcal{W}_i, \forall i \in \mathcal{N} \tag{23b}$$

$$\mathcal{S} + \xi p_e + \sigma^2 \ge -\frac{\mathcal{I}_5 - \tau \mathcal{I}_6}{\tau}\ln z \tag{23c}$$

$$t_i \le ||\mathbf{y}^k - \mathbf{w}_i||^2 + 2(\mathbf{y}^k - \mathbf{w}_i)^T(\mathbf{y}-\mathbf{y}^k), \forall i \in \mathcal{N} \tag{23d}$$

$$||\mathbf{y}-\mathbf{v}||^2 \le u, \tag{23e}$$

where $\mathbf{y}^k$ is the UAV jammer location in the k-th iteration. Due to the convexity of Problem (23), the UAV jammer location can be solved with standard convex optimization tool such as CVX.

C. UAV Jamming Power

With fixed $\{p_b, \mathbf{y}\}$, the UAV jamming power subproblem is transformed as

$$\underset{p_u,\eta,z}{\text{minimize}}\ \eta+z \tag{24a}$$

$$\text{s.t. } p_u h_{u,i} \le -\frac{\mathcal{I}_{2,i}}{\phi}\ln\left(\frac{1-(\eta - P^0_{i,k}P^0_{out,i})/P^1_{i,k}}{\mathcal{A}_i}\right) - \sigma^2, \forall i \in \mathcal{N} \tag{24b}$$

$$p_u h_{u,e} + \xi p_e + \sigma^2 \ge -\frac{\mathcal{I}_5 - \tau \mathcal{I}_6}{\tau}\ln z \tag{24c}$$

$$0 \le p_u \le p_u^{max}. \tag{24d}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

Similarly, we apply the SCA approach to convexify (24b) and approximate the UAV jamming power subproblem as

$$\underset{p_u,\eta,z}{\text{minimize}}\ \eta + z \tag{25a}$$
$$\text{s.t.}\ p_u h_{u,i} \leq \mathcal{W}_i, \forall i \in \mathcal{N} \tag{25b}$$
$$(24c),\ (24d).$$

Due to the convexity of Problem (25), it can be efficiently solved via convex optimization tool.

D. Proposed Iterative Algorithm

Algorithm 1 Proposed Solution.

1: Initialize $p_b^0 = 0.5$ W, $\mathbf{y}^0 = [50, 40]^T$, $p_u^0 = 0.1$ W and the number of iteration $k = 0$.
2: **repeat**
3: Obtain p_b^{k+1} with fixed $\{\mathbf{y}^k, p_u^k\}$ by solving (18);
4: Obtain $\mathbf{y}^{k+1}$ with fixed $\{p_b^{k+1}, p_u^k\}$ by solving (23);
5: Obtain p_u^{k+1} with fixed $\{p_b^{k+1}, \mathbf{y}^{k+1}\}$ by solving (25);
6: Update $k = k + 1$;
7: **until** convergence.

We summarize our proposed solution in Algorithm 1, where all variables are optimized alternately until convergence. To show the convergence, we set the value of the objective function generated in the k-th iteration as $P\left(p_b^k, \mathbf{y}^k, p_u^k\right)$, which follows

$$\begin{aligned} P\left(p_b^k, \mathbf{y}^k, p_u^k\right) &\geq P\left(p_b^{k+1}, \mathbf{y}^k, p_u^k\right) \geq P\left(p_b^{k+1}, \mathbf{y}^{k+1}, p_u^k\right) \\ &\geq P\left(p_b^{k+1}, \mathbf{y}^{k+1}, p_u^{k+1}\right), \end{aligned} \tag{26}$$

where the three inequalities hold due to the update of p_b^{k+1}, $\mathbf{y}^{k+1}$ and p_u^{k+1} by solving Problems (18), (23) and (25), respectively. We note that the objective value P has a lower bound at zero. Therefore, the proposed algorithm is guaranteed to converge. Moreover, we note that our proposed Algorithm 1 is of polynomial complexity since only convex optimization problems that need to be solved in Steps 3-5 of Algorithm 1.

IV. Simulation Results

In this section, the benefits of caching and jamming in improving the security and reliability performance have been evaluated via numerical results. We consider that the BS is located at the centre of a 30 m $\times$ 30 m square while $N = 4$ users are randomly distributed in this area. The active eavesdropper is located at $\mathbf{v} = [40, 40]^T$. We set the path-loss factor for the ground channels as $\alpha = 2.5$ and the noise power as $\sigma^2 = -110$ dBm. The reference channel power gain is set as $\beta_1 = 10^{-7}$. Moreover, the power allocation ratio of the BS is set as $\theta = 0.7$ and the transmit power at the active eavesdropper is $p_e = 0.05$ W. The SI efficiency of the active eavesdropper is set as $\xi = -110$ dB [7]. The IP and OP thresholds are $\phi = 0.8$ dB and $\tau = 0.8$ dB, respectively. For the sake of simplicity, we consider that the BS and the UAV jammer send the file $f_k, k = 5$ from a file library with $M = 6$ to all users as the additional signal and jamming signal, respectively. Moreover, we set $\kappa = 0.8$, $p_u^{max} = 0.3$ W and $p_b^{max} = 1$ W. For comparison purposes, we consider the following two benchmark schemes:

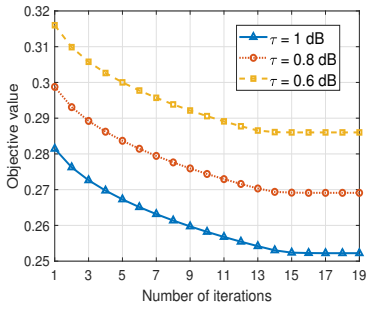

Fig. 2. Objective value versus number of iterations.

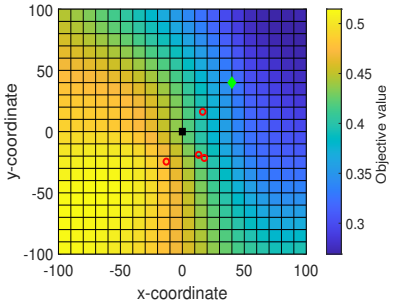

Fig. 3. Objective value of all possible UAV jammer horizontal locations.

- "Jamming only" scheme: We set $P_{i,k}^0 = 0$ and optimize the BS transmit power by solving the following problem

$$\underset{p_b,x,z,v}{\text{minimize}}\ x + z \tag{27a}$$
$$\text{s.t.}\ 1 - \frac{x}{P_{i,k}^1} \leq \mathcal{Y}_2(i), \forall i \in \mathcal{N} \tag{27b}$$
$$\mathcal{Y}_3 \geq -\ln(z) \tag{27c}$$
$$v \geq \frac{1}{p_b},\ 0 \leq p_b \leq p_b^{max}, \tag{27d}$$

  and optimize the UAV jammer location and jamming power by solving (23) and (25) with $P_{i,k}^0 = 0$, respectively.
- "Caching only" scheme: We set $p_u = 0$ W and optimize the BS transmit power by solving (18).

The convergence of our proposed solution is shown in Fig. 2 with three levels of τ ranging from 1 dB, 0.8 dB and 0.6 dB, respectively. It can be found that our proposed solution quickly converges to a minimum objective value within 20 iterations. Moreover, we notice that with a higher τ, the probability of the event that the SINR of the active eavesdropper is greater than the threshold τ reduces, which further leads to a lower objective value.

In Fig. 3, we plot the objective value of all possible UAV jammer horizontal locations with the optimized $p_b = 0.85$ W and $p_u = 0.3$ W. The locations of the users, BS and active eavesdropper are demonstrated as red circles, black square and green diamond, respectively. With the aim of minimizing the sum of the IP and the maximum OP among all users, the UAV jammer should be deployed far away from users to mitigate the jamming impact on reducing their SINRs while closer to the active eavesdropper. We obtain that by applying Algorithm 1, the optimal UAV jammer horizontal location is $[80.76, 81.18]$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TVT.2022.3186730 IEEE Transactions on Vehicular Technology

which can be accurately verified via Fig. 3.

The comparison between our proposed solution and benchmark strategies is shown in Fig. 4. It can be observed that our proposed Algorithm 1 achieves the minimum objective value over a wide range of p_u^{max}, which highlights the superiority of our proposed solution. Specifically, when $p_u^{max} = 0.1$ W, our proposed Algorithm 1 achieves an objective value of 0.299, which reduces 29.73% and 5.23% of that when comparing with the "Caching only" and "Jamming only" schemes, respectively. In addition, we observe that the objective value of "Caching only" scheme is independent of p_u^{max} since $p_u = 0$. Conversely, increasing the feasible range of UAV jamming power is helpful to reduce the objective value of Algorithm 1 until the optimal UAV jamming power $p_u = 0.44$ W reaches.

V. Conclusion

In this paper, we developed a secure communication system with caching and UAV-enabled jamming to protect against active eavesdropping attacks. Aimed at minimizing the sum of the IP and the maximum OP among all users, we jointly optimized the BS transmit power, UAV jammer location and jamming power. Numerical results show that the security and reliability performance was improved with the aid of caching and UAV friendly jamming.

Appendix A

To derive the OP, we first calculate $P_r(\gamma_i^0 < \phi)$ as follows

$$\begin{aligned} P_r(\gamma_i^0 < \phi) &= P_r\left(g_{b,i} < \frac{\phi\sigma^2}{\mathcal{I}_{0,i}} + \frac{\phi p_e h_{e,i} g_{e,i}}{\mathcal{I}_{0,i}}\right) \\ &\overset{(a)}{=} 1 - \exp\left(-\frac{\phi\sigma^2}{\mathcal{I}_{0,i}}\right) \mathbb{E}_{g_{e,i}}\left[\exp\left(-\frac{\phi p_e h_{e,i} g_{e,i}}{\mathcal{I}_{0,i}}\right)\right] \\ &\overset{(b)}{=} 1 - \exp\left(-\frac{\phi\sigma^2}{\mathcal{I}_{0,i}}\right) \times \int_0^\infty \exp\left(-\frac{\phi p_e h_{e,i} g_{e,i}}{\mathcal{I}_{0,i}}\right) e^{-g_{e,i}} d(g_{e,i}) \\ &= 1 - \frac{1}{1 + \frac{\phi p_e h_{e,i}}{\mathcal{I}_{0,i}}} \exp\left(-\frac{\phi\sigma^2}{\mathcal{I}_{0,i}}\right), \forall i \in \mathcal{N}, \end{aligned} \tag{28}$$

where $\mathcal{I}_{0,i} = p_b \theta h_{b,i}$. Moreover, (a) and (b) are derived due to the fact that the small-scale fading variables of $g_{b,i}$ and $g_{e,i}$ follow the exponential distributions. Similarly, we obtain $P_r(\gamma_i^1 < \phi)$ as follows

$$P_r(\gamma_i^1 < \phi) = 1 - \frac{1}{1 + \frac{\phi p_e h_{e,i}}{\mathcal{I}_{2,i}}} \exp\left(-\frac{\phi \mathcal{I}_{1,i}}{\mathcal{I}_{2,i}}\right), \forall i \in \mathcal{N}, \tag{29}$$

where $\mathcal{I}_{1,i} = p_u h_{u,i} + \sigma^2$ and $\mathcal{I}_{2,i} = p_b h_{b,i}(\theta - \phi + \theta\phi)$. Combining above results, (8) can be derived accordingly.

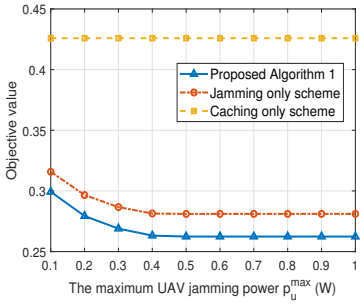

Fig. 4. Scheme comparison with the maximum UAV jamming power p_u^{max}.

References

[1] K. Wang, C. Pan, H. Ren, W. Xu, L. Zhang, and A. Nallanathan, "Packet Error Probability and Effective Throughput for Ultra-Reliable and Low-Latency UAV Communications," in *IEEE Trans. Commun.,* vol. 69, no. 1, pp. 73-84, Jan. 2021.

[2] M. Hua, L. Yang, C. Li, Q. Wu, and A. L. Swindlehurst, "Throughput Maximization for UAV-Aided Backscatter Communication Networks," in *IEEE Trans. Commun.,* vol. 68, no. 2, pp. 1254-1270, Feb. 2020,

[3] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Communication-and-Computing Latency Minimization for UAV-Enabled Virtual Reality Delivery Systems," in *IEEE Trans. Commun.,* vol. 69, no. 3, pp. 1723-1735, March 2021.

[4] S. Zhang, H. Zhang, and L. Song, "Beyond D2D: Full Dimension UAV-to-Everything Communications in 6G," in *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6592-6602, June 2020.

[5] C. She, C. Liu, T. Q. S. Quek, C. Yang, and Y. Li, "Ultra-Reliable and Low-Latency Communications in Unmanned Aerial Vehicle Communication Systems," in *IEEE Trans. Commun.,* vol. 67, no. 5, pp. 3768-3781, May 2019.

[6] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," in *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280-11284, Nov 2018.

[7] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Secure Communications for UAV-Enabled Mobile Edge Computing Systems," in *IEEE Trans. Commun.,* vol. 68, no. 1, pp. 376-388, Jan. 2020.

[8] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret Channel Training to Enhance Physical Layer Security With a Full-Duplex Receiver," in *IEEE Trans. Inf. Forensics Secur.,* vol. 13, no. 11, pp. 2788-2800, Nov. 2018.

[9] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three Artificial-Noise-Aided Secure Transmission Schemes in Wiretap Channels," in *IEEE Trans. Veh. Technol.* vol. 67, no. 4, pp. 3669-3673, April 2018.

[10] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-Free Massive MIMO Networks: Optimal Power Control Against Active Eavesdropping," in *IEEE Trans. Commun.,* vol. 66, no. 10, pp. 4724-4737, Oct. 2018.

[11] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV Communications Against Full-Duplex Active Eavesdropper," in *IEEE Trans. Wireless Commun.,* vol. 18, no. 6, pp. 2919-2931, June 2019.

[12] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust Resource Allocation to Enhance Physical Layer Security in Systems With Full-Duplex Receivers: Active Adversary," in *IEEE Trans. Wireless Commun.,* vol. 16, no. 2, pp. 885-899, Feb. 2017.

[13] J. Si, Z. Cheng, Z. Li, J. Cheng, H. -M. Wang, and N. Al-Dhahir, "Cooperative Jamming for Secure Transmission With Both Active and Passive Eavesdroppers," in *IEEE Trans. Commun.,* vol. 68, no. 9, pp. 5764-5777, Sept. 2020.

[14] S. Cho, G. Chen, and J. P. Coon, "Cooperative Beamforming and Jamming for Secure VLC System in the Presence of Active and Passive Eavesdroppers," accepted in *IEEE Trans. Green Commun. Netw.* 2021.

[15] W. Zhao, Z. Chen, K. Li, N. Liu, B. Xia, and L. Luo, "Caching-Aided Physical Layer Security in Wireless Cache-Enabled Heterogeneous Networks," in *IEEE Access,* vol. 6, pp. 68920-68931, 2018.

[16] N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV Assisted Secure Transmission in Hyper-Dense Networks Based on Interference Alignment," in *IEEE Trans. Commun.,* vol. 66, no. 5, pp. 2281-2294, May 2018.

[17] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-Relaying-Assisted Secure Transmission With Caching," in *IEEE Trans. Commun.,* vol. 67, no. 5, pp. 3140-3153, May 2019.

[18] A. Li, Q. Wu, and R. Zhang, "UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel," in *IEEE Wireless Commun. Lett.,* vol. 8, no. 1, pp. 181-184, Feb. 2019.

[19] X. Xu, Y. Zeng, Y. L. Guan, and R. Zhang, "Overcoming Endurance Issue: UAV-Enabled Communications With Proactive Caching," in *IEEE J. Sel. Areas Commun.,* vol. 36, no. 6, pp. 1231-1244, June 2018.

[20] Z. Zhang, Z. Ma, Z. Ding, M. Xiao, and G. K. Karagiannidis, "Full-Duplex Two-Way and One-Way Relaying: Average Rate, Outage Probability, and Tradeoffs," in *IEEE Trans. Wireless Commun.,* vol. 15, no. 6, pp. 3920-3933, June 2016.