Legitimate Pilot Contamination Attack in Intelligent Multi-Access Networks

Wei Wang, Lingjie Duan, *Senior Member, IEEE,* Xin Liu, *Senior Member, IEEE,* and Nan Zhao, *Senior Member, IEEE*

***Abstract*—In this correspondence, we investigate the legitimate surveillance of a suspicious intelligent multi-access (MA) network via pilot contamination attack (PCA). Specifically, the base station (BS) can switch between orthogonal multiple access (OMA) and non-orthogonal multiple access (NOMA) to achieve the optimal sum rate for the paired two users. The monitor sends PCA signals to distort the channel estimation and misleads the mode selection at the BS, i.e., from OMA to NOMA. As thus, the monitor can replace the stronger user in the NOMA pair by itself and wiretap the information of both users, owing to the superimposed signals in NOMA. To this end, the PCA power is minimized subject to the sum-rate requirement and eavesdropping condition, which guarantees that the information can be successfully recovered by the monitor. Simulation results confirm the effectiveness of our PCA scheme in achieving the surveillance in intelligent MA networks.**

***Index Terms*—Legitimate surveillance, non-orthogonal multiple access, orthogonal multiple access, pilot contamination attack.**

I. Introduction

The explosive growth of wireless devices and continuous development of applications inevitably bring new challenges to the upcoming sixth generation (6G) networks [1]. It is expected that the 6G networks can achieve more intelligent connections and stronger security. On the one hand, one of the most important issues is to design more sophisticated multi-access (MA) scheme to cater to diverse demands of wireless devices [2]. On the basis of whether each user is assigned with the orthogonal resource or not, the mainstream MA schemes can be divided into orthogonal multiple access (OMA) and non-orthogonal multiple access (NOMA). As compared to OMA, NOMA can simultaneously serve multiple users in a single orthogonal resource, by bearing higher implementation complexity in both transmitter and receiver [3], [4]. Furthermore, the NOMA gain is greatly restricted when the channel difference among users is not distinctive [5]. Since each MA scheme has its own merits, intelligent MA was proposed as a promising solution to achieving the substantial rate capacity cost-effectively, in which the base station (BS) can adaptively switch between NOMA and OMA [6]. The basic switching rule is that the OMA mode is selected for transmission when applying NOMA has only negligible or limited gain.

On the other hand, security is another important issue worth attention [7]. Specifically, massive devices should be well surveiled by authorized parties to avoid being utilized for illegal communications of terrorists, spies or criminals [8]. As opposed to physical layer security (PLS) against illegal eavesdropping, the eavesdropper now becomes legitimate and acts as a monitor to overhear the suspicious links for surveillance. In turn, the attacks of illegal eavesdroppers in PLS can be utilized as surveillance methods, such as proactive eavesdropping and pilot contamination attack (PCA). Proactive eavesdropping can deteriorate the information reception at the suspicious user by injecting artificial jamming and overhear the suspicious links [9], while the PCA can contaminate the channel estimation and manipulate the downlink beams by sending the same pilot sequence as the legitimate user [10]. To our knowledge, the PCA has not been well investigated for legitimate surveillance of intelligent MA networks.

Motivated by this, we propose a novel PCA scheme for the legitimate surveillance of intelligent MA networks, where a legitimate monitor transmits the same pilot sequence as suspicious users to the BS. By utilizing PCA, the monitor can distort the channel estimation and induce the BS to serve users via NOMA, especially when the NOMA gain in term of sum rate is restricted compared with that of OMA. Thus, the monitor can gain the opportunity to fully replace the stronger user in the NOMA pair by itself and surveil both suspicious users. To this end, we investigate the PCA power minimization and propose an alternating optimization algorithm to solve it iteratively.

II. System Model and Preliminaries

As shown in Fig. 1, a legitimate monitor overhears two suspicious downlinks from the BS to two users [1]. Specifically, the BS is equipped with N antennas, the monitor and two users (i.e., near and far users) are single-antenna, denoted by

Manuscript received November 16, 2023; accepted December 14, 2023. The work of Nan Zhao was supported by the National Natural Science Foundation of China (NSFC) under Grant 62271099. The work of Lingjie Duan was supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 2 Grant (Award No. MOE-T2EP20121-0001), and the SUTD Kickstarter Initiative (SKI) Grant with no. SKI 2021_04_07. The associate editor coordinating the review of this paper and approving it for publication was A. Guerra. *(Corresponding author: Nan Zhao.)*

W. Wang, X. Liu and N. Zhao are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China (email: 21809066@mail.dlut.edu.cn, liuxinstar1984@dlut.edu.cn, zhaonan@dlut.edu.cn). L. Duan is with the Engineering Systems and Design Pillar, Singapore University of Technology and Design (SUTD), Singapore 487372 (e-mail:lingjie_duan@sutd.edu.sg).

[1]We present the two-user PCA scheme for ease of exposition, which can also be extended to the case of multiple users but more analysis is required.

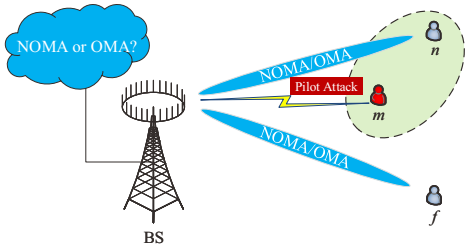

Fig. 1. A suspicious intelligent multiple access network includes two suspicious users, which is surveilled by a legitimate monitor.

U_m, U_n and U_f, respectively. The BS adopts the dynamic MA scheme to serve users in an intelligent manner, i.e., the BS can switch between NOMA and OMA in each downlink transmission depending on the achievable sum rate of its served users. Before downlink transmission, the BS first observes the superimposed pilot signals transmitted by users. The received signal $\mathbf{Y} \in \mathbb{C}^{N\times\tau}$ can be expressed as

$$\mathbf{Y} = \sum\nolimits_{i\in\{n,f\}} \mathbf{h}_i \mathbf{x}_i^H + \mathbf{N}, \tag{1}$$

where $\mathbf{x}_i \in \mathbb{C}^{\tau\times 1}$ and $\mathbf{h}_i \in \mathbb{C}^{N\times 1}$ are the transmitted pilot sequences with τ-length symbols and the corresponding channels of U_i to be estimated at the BS, respectively. $\mathbf{N} \in \mathbb{C}^{N\times\tau}$ is the additive Gaussian noise matrix. Accordingly, the BS can obtain the estimated channel vectors $\hat{\mathbf{h}}_i$, design the corresponding beams for each user and decide which mode is adopted according to the achievable sum rate.

A. NOMA Mode

In the NOMA mode, the BS transmits the superimposed signals of two users as $x = \sqrt{\rho P_B}s_n + \sqrt{(1-\rho)P_B}s_f$, where P_B denotes the maximum transmit power at the BS, $0 < \rho < 1$ is the power allocation ratio and s_i denotes the corresponding data symbol for user $i, i \in \{n, f\}$. As the optimal beamforming solution in NOMA mode is hard to obtain, we adopt the combined beamforming design which is low-complexity and can benefit the fairness of NOMA users. For simplicity, the estimated channels are combined to design the downlink NOMA beamforming vector, i.e.,$\mathbf{w} = \frac{\hat{\mathbf{h}}_n + \hat{\mathbf{h}}_f}{\|\hat{\mathbf{h}}_n + \hat{\mathbf{h}}_f\|}$, where $\hat{\mathbf{h}}_n$ and $\hat{\mathbf{h}}_f$ are the estimated channel vectors of U_n and U_f, respectively. Accordingly, the expected reception signal at U_i is given by $\hat{y}_i = \hat{\mathbf{h}}_i^H \mathbf{w}x + n$, where n denotes the additive Gaussian noise with variance σ^2. At the receivers, U_f directly decodes its own signal and the corresponding signal-to-interference-plus-noise ratio (SINR) can be expressed as

$$\hat{\gamma}_f^f = \frac{(1-\rho)P_B|\hat{\mathbf{h}}_f^H \mathbf{w}|^2}{\rho P_B|\hat{\mathbf{h}}_f^H \mathbf{w}|^2 + \sigma^2}. \tag{2}$$

U_n detects the signal of U_f, which is eliminated from the received signals via SIC. The related SINR/SNR at U_n can be rewritten as

$$\hat{\gamma}_n^f = \frac{(1-\rho)P_B|\hat{\mathbf{h}}_n^H \mathbf{w}|^2}{\rho P_B|\hat{\mathbf{h}}_n^H \mathbf{w}|^2 + \sigma^2}, \hat{\gamma}_n^n = \frac{\rho P_B|\hat{\mathbf{h}}_n^H \mathbf{w}|^2}{\sigma^2}. \tag{3}$$

Thus, the achievable rate of U_i in the NOMA mode is given by $\hat{R}_f^{\mathrm{NOMA}} = \log_2\left(1 + \min\{\hat{\gamma}_f^f, \hat{\gamma}_n^f\}\right)$ and $\hat{R}_n^{\mathrm{NOMA}} = \log_2\left(1 + \hat{\gamma}_n^n\right)$, and the sum rate maximization can be formulated as

$$\max_{\rho} \sum\nolimits_{i\in\{n,f\}} \hat{R}_i^{\mathrm{NOMA}} = \hat{R}_{sum}^{\mathrm{NOMA}} \tag{4a}$$

$$s.t. \quad \hat{R}_i^{\mathrm{NOMA}} \geq \Gamma_i, i \in \{n, f\}, \tag{4b}$$

where Γ_i is the predefined rate requirement at each U_i.

B. OMA Mode

In the OMA mode, the BS serves each user individually via two separate beams. Maximum ratio transmission (MRT) precoding is adopted, which can be designed as $\mathbf{w}_n = \frac{\hat{\mathbf{h}}_n}{\|\hat{\mathbf{h}}_n\|}, \mathbf{w}_f = \frac{\hat{\mathbf{h}}_f}{\|\hat{\mathbf{h}}_f\|}$. Accordingly, the achievable rate of U_k in the OMA mode can be expressed as $\hat{R}_n^{\mathrm{OMA}} = \frac{1}{2}\log_2\left(1 + \frac{\theta P_B|\hat{\mathbf{h}}_n \mathbf{w}_n|^2}{\frac{1}{2}\sigma^2}\right)$ and $\hat{R}_f^{\mathrm{OMA}} = \frac{1}{2}\log_2\left(1 + \frac{(1-\theta)P_B|\hat{\mathbf{h}}_f \mathbf{w}_f|^2}{\frac{1}{2}\sigma^2}\right)$, where $0 < \theta < 1$ is the power allocation ratio in the OMA mode. Note that the factor $\frac{1}{2}$ in $\hat{R}_i^{\mathrm{OMA}}$ is owing to the fact that each user is assigned with half of the resource block as compared to the case of NOMA. Thus, the sum rate maximization in the OMA mode can be formulated as

$$\max_{\theta} \sum\nolimits_{i\in\{n,f\}} \hat{R}_i^{\mathrm{OMA}} = \hat{R}_{sum}^{\mathrm{OMA}} \tag{5a}$$

$$s.t. \quad \hat{R}_i^{\mathrm{OMA}} \geq \Gamma_i, i \in \{n, f\}. \tag{5b}$$

With the estimated channel vectors $\hat{\mathbf{h}}_n$ and $\hat{\mathbf{h}}_f$, the BS can solve the sum rate maximization problems (4) and (5), and obtain the achievable sum rates in NOMA and OMA modes to compare, respectively. Consider that if the sum rate gap between NOMA and OMA is larger than the predefined threshold Δ, the BS chooses the NOMA mode. Otherwise, the OMA mode is adopted, i.e.,

$$\begin{cases} \text{NOMA is selected}, & \text{if } \hat{R}_{sum}^{\mathrm{NOMA}} - \hat{R}_{sum}^{\mathrm{OMA}} \geq \Delta, \\ \text{OMA is selected}, & \text{Otherwise.} \end{cases} \tag{6}$$

III. Pilot Contamination Attacking

During the pilot transmission, the monitor is able to masquerade as users by imitating its pilot sequence, and transmit the modified pilot sequence $\mathbf{x}_m \in \mathbb{C}^{\tau\times 1}$ together with the suspicious users [10]. In this way, the channel estimation results are contaminated and the superimposed pilot signal received at the BS is given by

$$\mathbf{Y} = \mathbf{h}_n \mathbf{x}_n^H + \mathbf{h}_f \mathbf{x}_f^H + \sqrt{P_m}\mathbf{h}_m \mathbf{x}_m^H + \mathbf{N}, \tag{7}$$

where $\mathbf{x}_m \in \{\mathbf{x}_n, \mathbf{x}_f\}$ [2] is the imitated pilot sequence transmitted by the monitor, with its corresponding PCA power P_m. For simplicity, we define $a = \sqrt{P_m}$ and assume that $\mathbf{x}_m = \mathbf{x}_n$. Thus, the noiseless estimated channel vectors at the BS can be expressed as

$$\hat{\mathbf{h}}_n = \mathbf{h}_n + a\mathbf{h}_m, \quad \hat{\mathbf{h}}_f = \mathbf{h}_f. \tag{8}$$

[2]Since the pilot sequence is usually fixed and reused over time, the monitor can readily obtain this sequence from the pilot observations.

It is worth noting that the estimated channel results and the achievable sum rate are strongly influenced by the PCA power at the monitor. Through PCA, the monitor can distort the channel estimation results, and further mislead the MA selection at the BS. Especially when the BS prefers OMA, the monitor can induce the BS to adopt the NOMA mode by carefully controlling the PCA power, which can be demonstrated by the following proposition.

Proposition 1: Under PCA, the estimated sum rate in NOMA mode of (4) can be superior to that in OMA mode of (5).

Proof: Though PCA, the estimated channel vectors are $\hat{\mathbf{h}}_n = \mathbf{h}_n + a\mathbf{h}_m, \quad \hat{\mathbf{h}}_f = \mathbf{h}_f$. Assume that the PCA power is sufficiently large and the estimated channel vector of U_n has been fully dominated by the monitor, i.e., $\hat{\mathbf{h}}_n = a\mathbf{h}_m$. For the OMA scheme, we introduce $\xi = \frac{P_B}{\sigma^2}$ and the sum rate of U_f and U_n can be approximated as

$$\begin{aligned}\hat{R}_{sum}^{\mathrm{OMA}} &= \frac{1}{2}\log_2\left(1+\xi|\hat{\mathbf{h}}_n|^2\right)+\frac{1}{2}\log_2\left(1+\xi|\hat{\mathbf{h}}_f|^2\right) \\ &\approx \log_2\left(a\sqrt{\xi}|\mathbf{h}_m|\right)+\log_2\left(\sqrt{\xi}|\mathbf{h}_f|\right) = \log_2\left(a\xi|\mathbf{h}_f||\mathbf{h}_m|\right).\end{aligned} \tag{9}$$

For the NOMA scheme, the combined beamforming vector is given by $\mathbf{w} = \frac{\hat{\mathbf{h}}_n+\hat{\mathbf{h}}_f}{\|\hat{\mathbf{h}}_n+\hat{\mathbf{h}}_f\|} \approx \frac{\mathbf{h}_m}{\|\mathbf{h}_m\|}$, the received SINR of U_f and U_n can be expressed as $\gamma_f = \min\left\{\frac{(1-\rho)P_B|\hat{\mathbf{h}}_n^H\mathbf{w}|^2}{\rho P_B|\hat{\mathbf{h}}_n^H\mathbf{w}|^2+\sigma^2}, \frac{(1-\rho)P_B|\hat{\mathbf{h}}_f^H\mathbf{w}|^2}{\rho P_B|\hat{\mathbf{h}}_f^H\mathbf{w}|^2+\sigma^2}\right\}$ and $\gamma_n = \frac{\rho P_B|\hat{\mathbf{h}}_n^H\mathbf{w}|^2}{\sigma^2}$, respectively. Then, the achievable rate of U_f can be given by

$$\hat{R}_f = \log_2\left(\min\left\{\frac{|\hat{\mathbf{h}}_n^H\mathbf{w}|^2+\frac{1}{\xi}}{\rho|\hat{\mathbf{h}}_n^H\mathbf{w}|^2+\frac{1}{\xi}}, \frac{|\hat{\mathbf{h}}_f^H\mathbf{w}|^2+\frac{1}{\xi}}{\rho|\hat{\mathbf{h}}_f^H\mathbf{w}|^2+\frac{1}{\xi}}\right\}\right) \xrightarrow{\xi\to\infty} \log_2\left(\frac{1}{\rho}\right). \tag{10}$$

Accordingly, for U_n, we have $\hat{R}_n = \log_2\left(1+\xi\rho|\hat{\mathbf{h}}_n^H\mathbf{w}|^2\right) = \log_2\left(1+a^2\xi\rho|\mathbf{h}_m|^2\right)$. The sum rate of NOMA mode satisfies

$$\hat{R}_{sum}^{\mathrm{NOMA}} = \log_2\left(1+a^2\xi\rho|\mathbf{h}_m|^2\right)+\log_2\left(\frac{1}{\rho}\right) \approx \log_2\left(a^2\xi|\mathbf{h}_m|^2\right). \tag{11}$$

Accordingly, the sum rate difference between NOMA and OMA modes can be expressed as

$$\begin{aligned}\hat{R}_{sum}^{\mathrm{NOMA}} - \hat{R}_{sum}^{\mathrm{OMA}} &= \log_2\left(a^2\xi|\mathbf{h}_m|^2\right) - \log_2\left(a\xi|\mathbf{h}_f||\mathbf{h}_m|\right) \\ &= \log_2\left(\frac{a|\mathbf{h}_m|}{|\mathbf{h}_f|}\right),\end{aligned} \tag{12}$$

which is a incremental function of a. Thus, the NOMA gain in sum rate can be guaranteed by carefully controlling the injected PCA power. The proof is completed. ■

Since the NOMA mode is adopted at the BS, the monitor can replace the stronger user in the NOMA pair by itself and also apply SIC for better surveillance performance. Thus, the corresponding SINR/SNR at U_m is given by

$$\gamma_m^f = \frac{(1-\rho)P_B|\mathbf{h}_m^H\mathbf{w}|^2}{\rho P_B|\mathbf{h}_m^H\mathbf{w}|^2+\sigma^2}, \qquad \gamma_m^n = \frac{\rho P_B|\mathbf{h}_m^H\mathbf{w}|^2}{\sigma^2}. \tag{13}$$

The eavesdropping rate of U_n and U_f are $R_m^i = \log_2(1+\gamma_m^i), i \in \{n, f\}$. The monitor can successfully decode the information of U_f and U_n when $\gamma_m^f \geq \min\{\gamma_f^f, \gamma_n^f\}$ and $\gamma_m^n \geq \gamma_n^n$ are satisfied, where $\{\gamma_f^f, \gamma_n^f, \gamma_n^n\}$ are the achievable SINR/SNRs with the actual channels $\mathbf{h}_f$ and $\mathbf{h}_n$.

IV. Problem Formulation and Optimization

To achieve the legitimate surveillance, the PCA power minimization problem can be formulated as

$$\min_{\rho,\theta,a} \ a^2 = P_m \tag{14a}$$

$$s.t. \ \ \hat{R}_{sum}^{\mathrm{NOMA}} - \hat{R}_{sum}^{\mathrm{OMA}} \geq \Delta, \tag{14b}$$

$$\gamma_m^f \geq \min\{\gamma_f^f, \gamma_n^f\}, \tag{14c}$$

$$\gamma_m^n \geq \gamma_n^n, \tag{14d}$$

where (14b) guarantees that the sum rate of NOMA mode with estimated channels is higher than that of OMA mode, and Δ is the expected NOMA gain compared with OMA. (14c) and (14d) show that the monitor can simultaneously eavesdrop the confidential information of both users.

Note that (14) with multiple coupled variables is non-convex and difficult to solve. Thus, we decompose it into two subproblems and solve them alternatively.

A. Power Allocation Optimization

With given $\bar{a}$, (14) can be regarded as the conventional sum rate maximization problem for NOMA and OMA, as illustrated in (4) and (5). Due to the non-convexity of (4) and (5), we can transform them into the second-order cone programming and solve them via CVX. We omit this part for simplicity, which can be refered to [11] for details.

B. PCA Power Minimization

With given $(\bar{\rho}, \bar{\theta})$, (14) is decomposed as the PCA power minimization problem subject to a. Thus, we introduce some auxiliary variables $(t_n, t_f, t, r, z) \in \mathbb{R}^+$ to transform the non-convex constraints. First for (14b), we let $\hat{R}_{sum}^{\mathrm{NOMA}} \geq r \geq \hat{R}_{sum}^{\mathrm{OMA}} + \Delta$, and construct the three inequalities as $1 + \min\{\hat{\gamma}_n^f, \hat{\gamma}_f^f\} \geq t_f$, $1 + \hat{\gamma}_n^n \geq t_n$ and $\log_2(t_n t_f) \geq \log_2(t^2)$ to handle the non-convexity of $\hat{R}_{sum}^{\mathrm{NOMA}}$. Then for (14c), we let z as the lower bound of $\min\{\gamma_n^f, \gamma_f^f\}$. Thus, the original problem (14) can be transformed as

$$\min_{a} \ a^2 = P_m \tag{15a}$$

$$s.t. \ \ 1 + \min\{\hat{\gamma}_n^f, \hat{\gamma}_f^f\} \geq t_f, \tag{15b}$$

$$1 + \hat{\gamma}_n^n \geq t_n, \tag{15c}$$

$$\left\|[2t, t_n - t_f]^H\right\| \leq t_n + t_f \tag{15d}$$

$$\log_2(t^2) \geq r, \tag{15e}$$

$$r \geq \hat{R}_{sum}^{\mathrm{OMA}} + \Delta, \tag{15f}$$

$$\gamma_m^f \geq z, \tag{15g}$$

$$\min\{\gamma_n^f, \gamma_f^f\} \geq z, \tag{15h}$$

$$\gamma_m^n \geq \gamma_n^n. \tag{15i}$$

As the modified constraints in (15) are still non-convex, we adopt successive convex approximation (SCA) to transform them into convex ones. First, for (15b), we have

$$\frac{(1-\theta)P_B|\hat{\mathbf{h}}_k^H\mathbf{w}|^2}{t_f - 1} \geq \theta P_B|\hat{\mathbf{h}}_k^H\mathbf{w}|^2 + \sigma^2, k \in \{n, f\}, \tag{16}$$

where $|\hat{\mathbf{h}}_k^H \mathbf{w}|^2 = \frac{|\hat{\mathbf{h}}_k^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2}{\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2}$, $\mathbf{h}_{nf} = \mathbf{h}_n + \mathbf{h}_f$. Then, we introduce a function as $\hat{F}_k(a,t_f) = \frac{\hat{f}_k(a)}{t_f - 1} = \frac{|\hat{\mathbf{h}}_k^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2}{t_f-1}$, $k \in \{n, f\}$. Accordingly, (16) can be transformed into

$$(1-\theta)P_B\hat{F}_k(a,t_f) \geq \theta P_B \hat{f}_k(a) + \sigma^2\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2. \quad (17)$$

Note that $\hat{F}_k(a,t_f)$ is a convex function subject to a and t_f, and the left-hand-side of (17) can be properly linearized via the Taylor-series approximation. The first-order Taylor expansion of $\hat{F}_k(a,t_f)$ around $(\bar{a},\bar{t}_f)$ can be given by

$$\hat{\mathcal{F}}_k(a,t_f,\bar{a},\bar{t}_f) = \hat{F}_k(\bar{a},\bar{t}_f) + \frac{\hat{f}_k'(\bar{a})(a-\bar{a})}{\bar{t}_f - 1} - \frac{\hat{f}_k(\bar{a})(t_f-\bar{t}_f)}{(\bar{t}_f-1)^2}, \quad (18)$$

where $\hat{f}_k'(a)$ is the first-order derivative of $\hat{f}_k(a) = |\widetilde{f}_k(a)|^2 = |\hat{\mathbf{h}}_k^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2, k \in \{n,f\}$. According to the equivalence of $\hat{f}_k(a) = \mathcal{R}\{\widetilde{f}_k(a)\}^2 + \mathcal{I}\{\widetilde{f}_k(a)\}^2$, $\hat{f}_k(a)$ can be easily reformulated as

$$\begin{aligned}
\hat{f}_n(a) =& a^4|\mathbf{h}_m|^4 + 2a^2\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_{nf}\}|\mathbf{h}_m|^2 \\
&+ 2a^3\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_m\}|\mathbf{h}_m|^2 + 2a^3\mathcal{R}\{\mathbf{h}_m^H\mathbf{h}_{nf}\}|\mathbf{h}_m|^2 \\
&+ 2a\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_m\}\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_{nf}\} + 2a\mathcal{I}\{\mathbf{h}_n^H\mathbf{h}_m\}\mathcal{I}\{\mathbf{h}_n^H\mathbf{h}_{nf}\} \\
&+ 2a\mathcal{R}\{\mathbf{h}_m^H\mathbf{h}_{nf}\}\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_{nf}\} + 2a\mathcal{I}\{\mathbf{h}_m^H\mathbf{h}_{nf}\}\mathcal{I}\{\mathbf{h}_n^H\mathbf{h}_{nf}\} \\
&+ 2a^2\mathcal{R}\{\mathbf{h}_n^H\mathbf{h}_m\}\mathcal{R}\{\mathbf{h}_m^H\mathbf{h}_{nf}\} + 2a^2\mathcal{I}\{\mathbf{h}_n^H\mathbf{h}_m\}\mathcal{I}\{\mathbf{h}_m^H\mathbf{h}_{nf}\} \\
&+ a^2|\mathbf{h}_n^H\mathbf{h}_m|^2 + a^2|\mathbf{h}_m^H\mathbf{h}_{nf}|^2 + |\mathbf{h}_n^H\mathbf{h}_{nf}|^2,
\end{aligned} \quad (19)$$

$$\begin{aligned}
\hat{f}_f(a) =& |\mathbf{h}_f^H\mathbf{h}_{nf}|^2 + 2a\mathcal{R}\{\mathbf{h}_f^H\mathbf{h}_{nf}\}\mathcal{R}\{\mathbf{h}_f^H\mathbf{h}_m\} \\
&+ 2a\mathcal{I}\{\mathbf{h}_f^H\mathbf{h}_{nf}\}\mathcal{I}\{\mathbf{h}_f^H\mathbf{h}_m\} + a^2|\mathbf{h}_f^H\mathbf{h}_m|^2.
\end{aligned} \quad (20)$$

Thus, the first-order derivative $\hat{f}_n'(a)$ and $\hat{f}_f'(a)$ can be readily obtained according to (19) and (20). We can substitute $\hat{f}_k(a)$ and $\hat{f}_k'(a)$ into (18) and finally obtain $\hat{\mathcal{F}}_k(a,t_f,\bar{a},\bar{t}_f)$. As thus, (17) has been transformed as a convex one as

$$(1-\theta)P_B\hat{\mathcal{F}}_k(a,t_f,\bar{a},\bar{t}_f) \geq \theta P_B\hat{f}_k(a) + \sigma^2\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2. \quad (21)$$

Similarly, (15c) can be converted to

$$\theta P_B\hat{\mathcal{F}}_n(a,t_n,\bar{a},\bar{t}_n) \geq \sigma^2\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2. \quad (22)$$

Then, we define $\Delta\hat{R}_f = \hat{R}_f^{\mathrm{OMA}} + \Delta$. (15f) can be rewritten as $\hat{R}_n^{\mathrm{OMA}} \leq r - \Delta\hat{R}_f$, which can be further approximated as

$$\frac{\theta P_B|\mathbf{h}_n + a\mathbf{h}_m|^2}{\frac{1}{2}\sigma^2} \leq 4^{\bar{r}-\Delta\hat{R}_f} + 4^{\bar{r}-\Delta\hat{R}_f}\ln 4(r-\bar{r}) - 1. \quad (23)$$

Then, (15g) and (15h) can be reformulated as

$$\frac{(1-\theta)P_B|\mathbf{h}_k^H\mathbf{w}|^2}{z} \geq \theta P_B|\mathbf{h}_k^H\mathbf{w}|^2 + \sigma^2, k \in \{m,n,f\}, \quad (24)$$

where $|\mathbf{h}_k^H\mathbf{w}|^2 = \frac{|\mathbf{h}_k^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2}{\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2}$, and we introduce $G_k(a,z) = \frac{g_k(a)}{z} = \frac{|\mathbf{h}_k^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2}{z}$. Accordingly, (24) can be modified as

$$(1-\theta)P_BG_k(a,z) \geq \theta P_Bg_k(a) + \sigma^2\|\mathbf{h}_{nf}+a\mathbf{h}_m\|^2. \quad (25)$$

To linearize the left-hand-side of (25), we take the first-order Taylor expansion of $G_k(a,z)$ as

$$\mathcal{G}_k(a,z,\bar{a},\bar{z}) = G_k(\bar{a},\bar{z}) + \frac{g_k'(\bar{a})}{\bar{z}}(a-\bar{a}) - \frac{g_k(\bar{a})}{\bar{z}^2}(z-\bar{z}), \quad (26)$$

where $g_k(a)$ can be expanded as

$$\begin{aligned}
g_k(a) =& a^2|\mathbf{h}_k^H\mathbf{h}_m|^2 + 2a\mathcal{R}\{\mathbf{h}_k^H\mathbf{h}_{nf}\}\mathcal{R}\{\mathbf{h}_k^H\mathbf{h}_m\} \\
&+ 2a\mathcal{I}\{\mathbf{h}_k^H\mathbf{h}_{nf}\}\mathcal{I}\{\mathbf{h}_k^H\mathbf{h}_m\} + |\mathbf{h}_k^H\mathbf{h}_{nf}|^2,
\end{aligned} \quad (27)$$

with its first-order derivative $g_k'(a)$ obtained according to (27). At last, (15g) and (15h) can be transformed into convex ones as

$$(1-\theta)P_B\mathcal{G}_k(a,z,\bar{a},\bar{z}) \geq \theta P_Bg_k(a) + \sigma^2|\mathbf{h}_{nf}+a\mathbf{h}_m|^2. \quad (28)$$

Similarly, (15i) can be approximated as

$$g_m(\bar{a}) + g_m'(\bar{a})(a-\bar{a}) \geq |\mathbf{h}_n^H(\mathbf{h}_{nf}+a\mathbf{h}_m)|^2. \quad (29)$$

Finally, the original problem (15) has been transformed into a convex one as

$$\begin{aligned}
\min_{a} \ & a^2 = P_m \\
s.t. \ & \sqrt{2^r} \leq t, \\
& \left\|[2t, t_n - t_f]^H\right\| \leq t_n + t_f, \\
& (21), (22), (23), (28), (29).
\end{aligned} \quad (30)$$

To solve (15), the proposed alternating optimization based method is summarized as Algorithm 1.

Algorithm 1 PCA Power Minimization Algorithm

1: **Initialize**: The channel vectors $\{\mathbf{h}_n, \mathbf{h}_f, \mathbf{h}_m\}$, the iteration index $j = 1$ and the PCA power $a^{(j)}$.
2: **Repeat**
3: For $a^{(j)}$, solve the sum rate maximization problem of NOMA in (4) and OMA in (5) via CVX, respectively. Obtain the optimal power allocation ratio $\theta^{(j)}$ and $\rho^{(j)}$.
4: Using $\theta^{(j)}$ and $\rho^{(j)}$, solve the PCA minimization in (30) via CVX and obtain the optimal $a^{(j+1)}$.
5: $j = j + 1$.
6: **Until** $|a^{(j)} - a^{(j-1)}|$ converges.

V. Simulation Results and Discussion

In this section, we present simulations to evaluate the performance of the proposed PCA scheme. With the worst-case consideration, we assume that the channel gains of two users are similar, i.e., the BS and the two users U_n and U_f are separated by the same distance $D_n = D_f = 200$ m, while the distance between the BS and monitor U_m is around 100 m. The Rayleigh fading channels are modeled as $\mathbf{h}_i = \sqrt{C_0 D_i^{-\alpha}}\mathbf{g}_i \in \mathbb{C}^{N\times 1}, i \in \{n,f,m\}$, where $\alpha = 2$, $C_0 = 10^{-3}$, $\mathbf{g}_i \sim \mathcal{CN}(\mathbf{0},\mathbf{I})$. The number of antennas is $N = 4$. $\Gamma_n = \Gamma_f = 1$ bit/s/Hz. The noise power is $\sigma^2 = -70$ dBm. The maximum transmit power at the BS is 5 mW. The predefined threshold of the sum-rate gain between NOMA and OMA modes is $\Delta = 0.5$ bit/s/Hz.

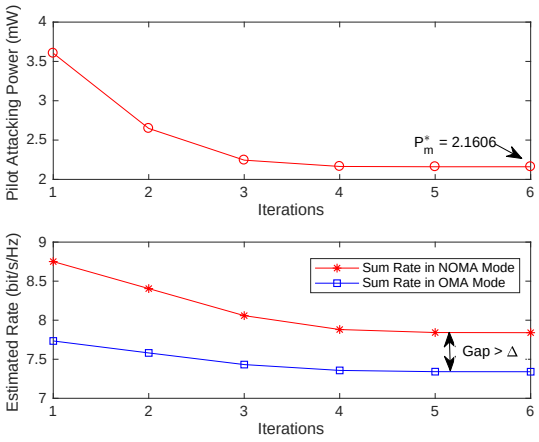

Fig. 2. Optimized PCA power and estimated sum rate in NOMA and OMA modes with iterations.

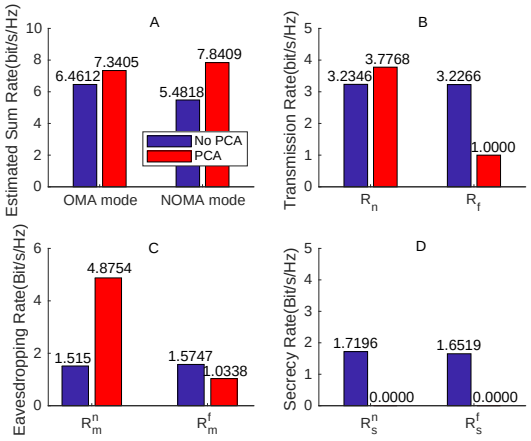

Fig. 3. Estimated sum rate, transmission rate, eavesdropping rate and secrecy rate of U_n and U_f.

In Fig. 2, we first verify the convergence of Algorithm 1 and present the estimated sum rate of NOMA and OMA modes with iterations. From the results, we can conclude that Algorithm 1 converges quickly and the optimal PCA power is $P_m^* = 2.1606$ mW. Accordingly, the estimated sum rate decreases with P_m, while the optimized sum rate of NOMA mode is always higher than that of OMA mode under the PCA. Furthermore, the NOMA gain is fully guaranteed in the perspective of BS, i.e., $\hat{R}_{sum}^{\mathrm{NOMA}} - \hat{R}_{sum}^{\mathrm{OMA}} \geq \Delta$. Thus, the BS adopts the NOMA mode to transmit the superimposed signals of U_f and U_n. In this way, the monitor gains the chance to replace the stronger user by itself and simultaneously overhear U_f and U_n.

To further illustrate it, we depict the estimated sum rate, transmission rate, eavesdropping rate and secrecy rate in Fig. 3. No PCA scheme and our PCA scheme are both taken into consideration. Fig. 3(A) shows that when the BS is not affected by PCA, the OMA mode is adopted as $\hat{R}_{sum}^{\mathrm{OMA}} > \hat{R}_{sum}^{\mathrm{NOMA}}$. While the monitor induces the BS to adopt the NOMA mode via PCA. Fig. 3(B) compares the transmission rate of U_n and U_f under the scenario without or with PCA. From Fig. 3(C), we can observe that the eavesdropping rates of both U_n and U_f in our PCA scheme are greater than that of their own transmission rates in Fig. 3(B), which indicates that the monitor can successfully overhear both users. In Fig. 3(D), the secrecy rates of both U_n and U_f in our PCA scheme are equal to 0, which means that the two suspicious links are fully surveilled.

VI. Conclusion

In this correspondence, we introduce PCA into the legitimate surveillance of a suspicious intelligent MA network, where the BS can switch between OMA and NOMA modes, according to the achievable sum rate of the paired two users. With PCA, the monitor can distort the channel estimation and mislead the MA selection at the BS, i.e., induce the BS to adopt NOMA when it prefers OMA. Owing to the fact that the users' signals are superimposed in the NOMA mode, the monitor can replace the stronger user by itself and overhear both users simultaneously. To this end, the PCA power is minimized to satisfied the sum-rate requirement and the eavesdropping condition. Accordingly, an alternating algorithm is proposed to solve this non-convex optimization iteratively. Simulation results indicate the feasibility and effectiveness of our PCA scheme.

References

[1] C.-X. Wang *et al.*, "On the road to 6G: Visions, requirements, key technologies, and testbeds," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 905–974, 2023.

[2] J. Mei, W. Han, X. Wang, and H. V. Poor, "Multi-dimensional multiple access with resource utilization cost awareness for individualized service provisioning in 6G," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1237–1252, Apr. 2022.

[3] Z. Liu, F. Yang, J. Song, and Z. Han, "Mulitple access for downlink multi-user VLC system: NOMA or OMA user pairing?," *IEEE Wireless Commun. Lett.*, to appear.

[4] Y. Ye, R. Q. Hu, G. Lu, and L. Shi, "Enhance latency-constrained computation in MEC networks using uplink NOMA," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2409–2425, Apr. 2020.

[5] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for IRS-aided secure NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.

[6] M. Baghani, S. Parsaeefard, M. Derakhshani, and W. Saad, "Dynamic non-orthogonal multiple access and orthogonal multiple access in 5G wireless networks," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6360–6373, Sept. 2019.

[7] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart. 2021.

[8] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[9] D. Xu, "Proactive eavesdropping of suspicious non-orthogonal multiple access networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13958–13963, Nov. 2020.

[10] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks," *IEEE Trans. Inf. Forens. Security*, vol. 15, pp. 1363–1378, 2020.

[11] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Trans. Signal Process.*, vol. 64, no. 1, pp. 76–88, Jan. 2016.