Game-Guided Matching Theory-Based Resource Allocation for Secure Semantic Communications

Xingyu Yang, *Student Member, IEEE*, Helin Yang, *Senior Member, IEEE*, Yifu Jiang, Arokiaswami Alphones, *Senior Member, IEEE*, and Liang Xiao, *Senior Member, IEEE*

***Abstract*—Semantic communication (SemCom) has become one of the most promising techniques in breaking the performance bottleneck for sixth-generation wireless networks, but the SemCom performance is easily degraded under malicious jamming and eavesdropping attacks over open wireless links. Therefore, this paper designs a reliable and secure SemCom approach against a hybrid attacker based on resource allocation, with the objective to jointly optimize channel selection and the number of transmitted semantic symbols to maximize secrecy semantic transmission rate (SS-R) under different quality of service requirements. We adopt a hierarchical framework based on Stackelberg game to model the interactions between legitimate users and the hybrid attacker. Furthermore, we model the optimization problem as a many-to-one matching problem with externalities, and propose two swap-based resource allocation algorithms, aiming to maximize the overall SS-R and meet fairness awareness. The two proposed algorithms are able to guide the iteration properly based on the dynamic of attack behaviors, which improves the secure resource allocation efficiency. Simulation results show that the proposed approaches outperform the baselines and benchmarks under different scenarios.**

***Index Terms*—Semantic communications, physical layer security, resource allocation, semantic secrecy rate, hybrid attacker.**

I. Introduction

With the development of coding and multiplexing techniques, modern wireless communication systems have exploited conventional theories to optimize data-oriented performance like data rate and bit error, which has greatly benefited industries and our daily lives. However, with higher requirements of high transmission data rate, the conventional data-centric communication system is facing a performance limit. Thankfully, a new paradigm semantic communication (SemCom) has emerged [1]–[3]. Compared with traditional communication, SemCom aims at extracting and transferring the most important information for specific tasks rather than raw data, which has been viewed as a promising solution to break the bottleneck. Furthermore, SemCom also has the potential to be integrated with other new key techniques to achieve further performance enhancement, such as the reconfigurable intelligent surface (RIS) technique [4], [5], which can achieve fine-grained reflect beamforming and thus ameliorate the signal propagation environment.

Motivated by the potential of SemCom, relevant studies have been investigated in recent years. For example, utilizing the advanced techniques of natural language processing (NLP) and computer vision (CV), several deep learning (DL)-based SemCom architectures were developed, such as DeepSC [6], DeepSC-S [7] and DeepSC-VQA [8]. To provide theoretical guidelines, Bao *et al.* [9] provided a theory of SemCom, in which semantic entropy is adopted to quantify semantic information. To evaluate the semantic similarity for text transmission, Sentence-Bidirectional Encoder Representations from Transformers (BERT) was adopted [6]. Furthermore, DL-based feature capture is deemed as a potential method to evaluate semantic similarity for image transmission [3].

Though there has not been a unified semantic theory and common semantic metrics, researchers have blazed their trails on enhancing the performance of SemCom systems. Like any wireless system, how to efficiently utilize limited resources is a major challenge for SemCom. [10] and [11] are pioneering works in resource allocation for SemCom systems. [10] defined the semantic spectral efficiency (S-SE), and proposed to jointly optimize the channel allocation and transmitted semantic symbols, while [11] designed a semantic quality-of-experience (QoE) and optimized the power selection in addition to the former. Hu *et al.* [12] expanded the resource allocation to multi-UAV semantic networks and proposed a deep reinforcement learning (DRL)-based solution to optimize the long-average cost and quality of services (QoS) of users. In conventional communication, the secrecy rate is optimized to enhance the systems security against eavesdroppers [13], [14]. Ahuja *et al.* [15] investigated a subcarrier allocation problem against a full-duplex hybrid attacker and proposed graph theory based algorithms to minimize the maximal intercept probability of users. Zhang *et al.* [16] modeled the anti-jamming mechanism as a multi-leader one-follower Stackelberg game. For SemCom, Chen *et al.* [17] revealed the risk of privacy leaks in SemCom systems by introducing the model inversion eavesdropping attack (MIEA), and proposed a novel defense scheme from the perspective of encryption. Li *et al.* [18] considered eavesdroppers for every user, and proposed to optimize the total latency.

In this paper, we first design a reliable and secure multimodal semantic communication model against a hybrid attacker. To analyze the secure SemCom scenario, we propose

This work was supported by the National Natural Science Foundation of China under Grants No. 62371408 and U21A20444, Fujian Provincial Natural Science Foundation of China under Grant 2024J09002, and Xiaomi Young Talents Program. (Corresponding author: *Yifu Jiang*)

X. Yang, H. Yang, and L. Xiao are with the School of Informatics, Xiamen University, Xiamen 361005, China (e-mail: 23320231154427@stu.xmu.edu.cn, {helinyang066, lxiao}@xmu.edu.cn).

Y. Jiang is with the Department of Economics Analysis, University of Zaragoza, Zaragoza 50001, Spain (e-mail: 849201@unizar.es).

A. Alphones is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: ealphones@ntu.edu.sg).

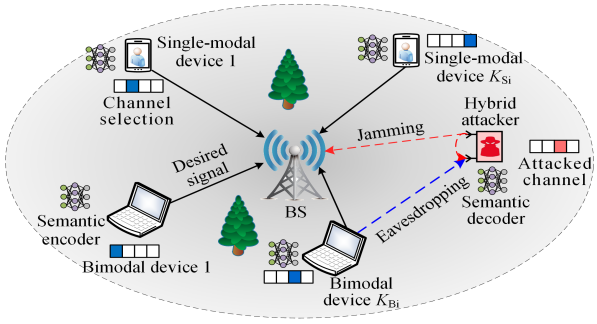


Fig. 1. Multi-user uplink semantic system with a hybrid attacker.

an anti-attack framework based on Stackelberg game, and propose to jointly optimize channel selection and the number of transmitted semantic symbols to maximize secrecy semantic transmission rate (SS-R) under QoS constraints. Then, we model the optimization problem as a many-to-one matching with externalities, and propose a low-complexity swap-based secure resource allocation algorithm. Subsequently, to address the shortcomings in fairness, we design another swap-based algorithm with fairness awareness. Simulation results show that the proposed algorithms achieve higher SS-R and fairness compared with benchmarks, demonstrating the effectiveness and superiority of our algorithms.

The rest of the paper is organized as follows. Section II introduces the system model and the optimization problem based on Stackelberg game. Section III presents two proposed resource allocation approaches. Section IV provides simulation results and analysis and Section V concludes the paper.

II. System Model

We consider a secure uplink communication scenario of a cellular network consisting of a base station (BS), a set of legitimate users denoted by $k \in \mathcal{K} = \{1, 2, ..., K\}$ and a hybrid attacker $\mathcal{A}$, as shown in Fig. 1. Similar to [10], BS, legitimate users and $\mathcal{A}$ are all equipped with semantic transmitters and receivers. Each user is allocated several channels to send semantic information to BS, while $\mathcal{A}$ issues hybrid attacks to the legitimate links over the available channels.

A. Semantic Source and Transmitter

In this paper, we consider the coexistence of single-modal and bimodal tasks to represent the difference among legitimate users, and divide $\mathcal{K}$ into K_{Si} single-modal users and K_{Bi} bimodal users, where $K_{\mathrm{Si}} + K_{\mathrm{Bi}} = K$. For convenience, we denote user k as a single-modal and a bimodal user for $k > K_{\mathrm{Bi}}$ and $k \leq K_{\mathrm{Bi}}$, respectively. Single-modal users are assumed to conduct text transmission with DeepSC [6] transmitter. For bimodal users, we consider the visual question answering (VQA) task, for which DeepSC-VQA is adopted [8]. Specifically, bimodal users are configured to sequentially transmit texts and images in pairs over the same channels.

The semantic entropy in [11] is adopted to quantify semantic information for different semantic sources. For single-modal users, the approximate semantic entropy is denoted as $\widetilde{H}_{\mathrm{Si}}$, while for bimodal users, $\widetilde{H}_{\mathrm{Bi,t}}$ and $\widetilde{H}_{\mathrm{Bi,i}}$ represent the approximate semantic entropy for text and image, respectively.

B. Uplink Transmission and Hybrid Attack

We assume there is a set of orthogonal channels denoted by $m \in \mathcal{M} = \{1, 2, ..., M\}$, and each occupies a bandwidth of B. We use a set of binary variables $\rho = \{\rho_{k,m}\}$ to represent the channel allocation, i.e., if channel m is allocated to user k, $\rho_{k,m} = 1$; otherwise, $\rho_{k,m} = 0$. Furthermore, we allow each legitimate user to occupy multiple channels but limit that one channel can only be allocated to one user,

$$\sum\nolimits_{m=1}^{M} \rho_{k,m} \leq M, \forall k; \sum\nolimits_{k=1}^{K} \rho_{k,m} \leq 1, \forall m. \tag{1}$$

Apart from the legitimate users, We consider a hybrid attacker $\mathcal{A}$ that possesses the capability of eavesdropping as well as jamming [15]. Ability to work in full-duplex (FD) mode enables $\mathcal{A}$ to perform both attacks at the same time, which means hybrid attacks. Moreover, $\mathcal{A}$ is able to perform multiple hybrid attacks to different channels simultaneously, and we also assume that $\mathcal{A}$ only chooses part of the available channels to attack. For a certain channel, $\mathcal{A}$ performs eavesdropping attack by tapping the legitimate transmissions over this channel. To enhance the validity of this eavesdropping model in SemCom system, we assume that $\mathcal{A}$ can reconstruct the original information from the eavesdropped semantic symbols through MIEA [17]. Besides, to impair the legitimate receptions at the base station (BS) and enhance the wiretap efficiency, $\mathcal{A}$ also executes jamming attacks by sending the interference with a certain power over channels.

Similarly, $\beta = \{\beta_m\}$ is used to indicate the attack decision of $\mathcal{A}$, i.e., if $\mathcal{A}$ chooses to attack channel m, $\beta_m = 1$; otherwise, $\beta_m = 0$. Moreover, since $\mathcal{A}$ only attacks part of the available channels, we have $\sum_{m=1}^{M} \beta_m = D, D < M$.

For user k, the signal-interference-to-noise ratio (SINR) of the uplink communication over channel m can be given as

$$\gamma_{k,m} = \frac{p_k g_k |h_{k,m}|^2}{BN_0 + \beta_m I_m^{jam}}, \tag{2}$$

where p_k is the transmit power of user k, g_k is the large-scale channel gain of user k including path loss and shadow effect, $h_{k,m} \sim \mathcal{CN}(0, 1)$ refers to the Rayleigh fading coefficient for k over channel m, and N_0 is the noise power spectral density. I_m^{jam} is the received jamming power at BS from $\mathcal{A}$ over channel m, expressed as $I_m^{jam} = p_{jam} g_e |h_{e,m}|^2$, where p_{jam} denotes the jamming power, g_e is the channel gain between $\mathcal{A}$ and BS, and $h_{e,m} \sim \mathcal{CN}(0, 1)$ refers to the Rayleigh fading.

For the hybrid attacker $\mathcal{A}$, the SINR of eavesdropping legitimate user k over channel m can be given as

$$\gamma_{k,m}^{e} = \frac{p_k g_k^{e} |h_{k,m}^{e}|^2}{BN_0 + \delta p_{jam}}, \tag{3}$$

where g_k^e is the large-scale channel gain from user k to $\mathcal{A}$, $h_{k,m}^e \sim \mathcal{CN}(0, 1)$ is the Rayleigh fading coefficient between them over channel m. Moreover, $\mathcal{A}$ suffers a residual self-interference (SI) of δp_{jam} where δ is the SI efficiency [14].

Moreover, as the central controller of the network, we assume the BS is equipped with sufficient servers and other hardware resources, which granted it with powerful capabilities in sensing and computation. And the user devices also

have the corresponding basic abilities though they are usually resource-constrained. Therefore, the instantaneous channel state information (CSI) of legitimate links and eavesdropped links are further assumed to be precisely obtained at BS.

C. Semantic Receiver

For single-modal users, i.e., $k > K_{\mathrm{Bi}}, k \in \mathcal{K}$, the received semantic symbols are recovered to the original text by the DeepSC receiver. To evaluate the ability to recover the original information, semantic similarity χ is adopted [10], which is a function of the number of transmitted semantic symbols n and SINR γ, i.e., between user k and BS, $\chi_{k,m} = f_{\mathrm{Si}}(n_{k,m}, \gamma_{k,m})$; for eavesdropping over channel m, $\chi^e_{k,m} = f_{\mathrm{Si}}(n_{k,m}, \gamma^e_{k,m})$.

For bimodal users, i.e., $k \leq K_{\mathrm{Bi}}, k \in \mathcal{K}$, the received semantic symbols include the parts of text and image. The DeepSC-VQA receiver decodes the two parts and fuses them to predict the answer. Similar to single-modal users, answer accuracy [11] is adopted to evaluate the task performance and is also denoted as χ for convenience. Specifically, χ is determined by the SINR γ and the numbers of transmitted semantic symbols of task and image transmission, i.e., n^t and n^i respectively. That is, between user k and BS, $\chi_{k,m} = f_{\mathrm{Bi}}(n^t_{k,m}, n^i_{k,m}, \gamma_{k,m})$; for eavesdropping over channel m, $\chi^e_{k,m} = f_{\mathrm{Bi}}(n^t_{k,m}, n^i_{k,m}, \gamma^e_{k,m})$.

D. Secrecy Semantic Transmission Rate

The average semantic transmission rate (S-R) is defined as the amount of successfully delivered semantic information per second, measured in $suts/s$ [10]. For single-modal users $k > K_{\mathrm{Bi}}, k \in \mathcal{K}$, $n_{k,m}$ semantic symbols are used to carry the amount of semantic information of $\widetilde{H}_{\mathrm{Si}}$ over channel m, therefore the corresponding S-R and eavesdropping S-R of $\mathcal{A}$ can be defined respectively as

$$\Phi_{k,m} = \frac{\widetilde{H}_{\mathrm{Si}}}{n_{k,m}/B}\chi_{k,m}, \Phi^e_{k,m} = \frac{\widetilde{H}_{\mathrm{Si}}}{n_{k,m}/B}\chi^e_{k,m}, \tag{4}$$

where the physical symbol rate is considered to be equal to the channel bandwidth B. For bimodal users $k \leq K_{\mathrm{Bi}}, k \in \mathcal{K}$, the S-R of text and image transmission are given as

$$\Phi^t_{k,m} = \frac{\widetilde{H}^t_{\mathrm{Bi}}}{n^t_{k,m}/B}\chi_{k,m}, \Phi^i_{k,m} = \frac{\widetilde{H}^i_{\mathrm{Bi}}}{n^i_{k,m}/B}\chi_{k,m}, \tag{5}$$

where $n_{k,m} = (n^t_{k,m}, n^i_{k,m})$, the corresponding S-R is defined as the average value of (5) as follows

$$\Phi_{k,m} = \frac{\Phi^t_{k,m} + \Phi^i_{k,m}}{2} = \left(\frac{\widetilde{H}^t_{\mathrm{Bi}}}{n^t_{k,m}} + \frac{\widetilde{H}^i_{\mathrm{Bi}}}{n^i_{k,m}}\right)\frac{B\chi_{k,m}}{2}, \tag{6}$$

and the eavesdropping S-R of $\mathcal{A}$ is given by

$$\Phi^e_{k,m} = \left(\frac{\widetilde{H}^t_{\mathrm{Bi}}}{n^t_{k,m}} + \frac{\widetilde{H}^i_{\mathrm{Bi}}}{n^i_{k,m}}\right)\frac{B\chi^e_{k,m}}{2}. \tag{7}$$

Furthermore, to depict the secure performance of our system considering the eavesdropping ability of $\mathcal{A}$, we define the average secrecy semantic transmission rate (SS-R), combining conventional secrecy rate [13] and S-R as follows

$$\Phi^{\mathrm{sec}}_{k,m} = \left[\Phi_{k,m} - \beta_m \Phi^e_{k,m}\right]^+, \tag{8}$$

where $[x]^+ \triangleq \max(0, x)$. And considering the orthogonality among channels, the SS-R of user k can be given by $\Phi^{\mathrm{sec}}_k = \sum_{m=1}^{M} \rho_{k,m}\Phi^{\mathrm{sec}}_{k,m}$.

E. Problem Formulation

In this paper, we focus on improving the secure performance of the semantic network. As stated before, the resource allocation and the attacks from $\mathcal{A}$ jointly determine the security performance of the entire system. To better analyze the interaction between them, we model it as a hierarchical framework based the two-stage Stackelberg game model [16], in which the system (i.e., the entity consisted of the BS and the legitimate users) is set as leader and $\mathcal{A}$ is set as follower. At stage 1, the leader first determines the resource allocation to maximize its security performance. Then at stage 2, reacting to the leader, the follower chooses D channels to attack. Moreover, we consider $\mathcal{A}$ as a rational and selfish player aiming at maximizing its overall eavesdropping S-R, which can be realized by sorting the channels in descending order according to their achievable eavesdropping S-R (i.e., $\Phi^e_{k,m}$) and then choosing the top D channels to attack.

Based on the above description, we seek to optimize the channel allocation $\rho = \{\rho_{k,m}\}$ and the average number of transmitted semantic symbols $n = \{n_{k,m}\}$, and the problem formulation can be given by

$$\max_{\rho,n} \Phi^{\mathrm{sec}} = \sum\nolimits_{k=1}^{K} \Phi^{\mathrm{sec}}_k \tag{9a}$$

$$s.t. C_1 : \rho_{k,m} \in \{0,1\}, \forall k \in \mathcal{K}, \forall m \in \mathcal{M}, \tag{9b}$$

$$C_2 : \sum\nolimits_{k=1}^{K} \rho_{k,m} \leq 1, \forall m \in \mathcal{M}, \tag{9c}$$

$$C_3 : \sum\nolimits_{m=1}^{M} \rho_{k,m} \leq M, \forall k \in \mathcal{K}, \tag{9d}$$

$$C_4 : n_{k,m} \in \mathcal{N}, \chi_{k,m} \geq \chi_{\mathrm{th}}, \forall k \in \mathcal{K}, \forall m \in \mathcal{M}, \tag{9e}$$

$$C_5 : \Phi^{\mathrm{sec}}_k \geq \Phi^{\mathrm{sec}}_{\mathrm{th}}, \forall k \in \mathcal{K}, \tag{9f}$$

$$C_6 : \beta = h(\rho, n), \tag{9g}$$

where C_1 refers to the range of $\rho_{k,m}$, C_2 and C_3 indicate the restrictions of channel assignment, C_4 specifies the available numbers of transmitted semantic symbols and the minimum required semantic similarity, in which $\mathcal{N} = \mathcal{N}_{\mathrm{Si}}$ when $k > K_{\mathrm{Bi}}$ and $\mathcal{N} = \mathcal{N}_{\mathrm{Bi}} = \{\mathcal{N}_{\mathrm{Bi,t}}, \mathcal{N}_{\mathrm{Bi,i}}\}$ when $k \leq K_{\mathrm{Bi}}$. C_5 restricts the minimum SS-R for users to access the network with security, and C_6 represents the attack strategy of $\mathcal{A}$ acting as the follower in the game-guided framework.

III. Swap-based Resource Allocation Approaches

In this section, we analyze the proposed optimization problem based on the matching theory [19] and then propose two swap-based approaches to solve the problem.

A. Game-Guided Matching Theory for Resource Allocation

Considering $\rho = \{\rho_{k,m}\}$ and $n = \{n_{k,m}\}$ are both sets of discrete variables, (9) is a three-sided many-to-one matching

problem [19] among legitimate users, channels, and numbers of transmitted semantic symbols under the established game-guided framework based on Stackelberg game. For better analysis, we form a transmitter set $\mathcal{R}$ by putting together all combinations of legitimate users and numbers of semantic symbols, i.e., $\mathcal{R} = \{(k,n), \forall k \in \mathcal{K}, \forall n \in \mathcal{N}\}$. The element of $\mathcal{R}$, i.e., $r = (k,n)$ is defined as a transmitter block. Then (9) becomes a two-sided matching problem between $\mathcal{M}$ and $\mathcal{R}$.

Definition 1. *In the proposed two-sided many-to-one matching model, a matching θ is a function from $\mathcal{R} \cup \mathcal{M}$ into all subsets of $\mathcal{R} \cup \mathcal{M}$ such that $\theta(m) = r$ if and only if $m \in \theta(r)$.*

To better analyze problem (9), we still focus on the utilities of channels and users. Accordingly, the utility of channel m under matching θ is defined as the SS-R of user k over it:

$$U_m(\theta) = \Phi^{\text{sec}}_{k,m}(\theta) = \left[\Phi_{k,m} - \beta_m \Phi^e_{k,m}\right]^+, \tag{10}$$

where $\theta(m) = r$ and $k \in r$.

For legitimate user k, we define the utility as its overall SS-R according to (9) in the following:

$$U_k(\theta) = \Phi^{\text{sec}}_k(\theta) = \begin{cases} \Phi^{acc}_k(\theta), & \text{if } \Phi^{acc}_k(\theta) \geq \Phi^{\text{sec}}_{\text{th}}; \\ 0, & otherwise, \end{cases} \tag{11}$$

where $\Phi^{acc}_k(\theta) = \sum_{r \in \mathcal{R}_k} \sum_{m \in \theta(r)} \Phi^{\text{sec}}_{k,m}(\theta)$, and we define the subset of $\mathcal{R}$ formed with user k as $\mathcal{R}_k = \{(k,n), \forall n \in \mathcal{N}\}$.

According to the game-guided framework where $\mathcal{A}$ issues attacks in reaction to the overall resource allocation, the utility of each channel is not only based on the transmitter block to be matched, but also on other channels' matching results. Specifically, (9) is a *matching problem with externalities* [19]. Therefore, we adopt the idea of swap matching [20] to get low-complexity algorithms.

Definition 2. *Swap Matching: Given a matching θ with $\theta(m) = r$, $\theta^{(r,r')}_m$ is a swap matching where channel m swap $r = (k,n)$ with $r' = (k',n')$, a channel m' currently matched with k' also swap (k',n'') with (k,n), and other channels matchings remain unchanged. Note that m' is optional to m, denote $\mathcal{M}^\theta_k$ as the channels matched with user k under θ.*

To enable the operation of adding channels to each user, we denote $\mathcal{M}_0 = \{m_{0,k}, \forall k \in \mathcal{K}\}$ as a set of virtual channels, and $m_{0,k}$ is for user k. As auxiliary indicators, $\mathcal{M}_0$ will not be matched, and the corresponding utilities are set as 0.

Moreover, the externalities in (9) where the utility of each channel depends on the overall matching results are more than peer effects [11], and cannot be tackled with classical iteration conditions [20]. Fortunately, from the perspective of $\Phi^e_{k,m}$, only m and m' will be affected after $\theta^{(r,r')}_m$. This enables us to propose our approaches based on the change of attack targets caused by $\theta^{(r,r')}_m$. Next, we give our modified definition of stable matching to ensure performance and convergence.

Definition 3. *Given the current matching θ, denote m' as the channel that swaps user with m in swap matching $\theta^{r,r'}_m$, $\mathcal{M}^*$ as the originally secure channels that are attacked due to $\theta^{r,r'}_m$, $\mathcal{M}^\circ$ as the originally attacked channels that are secure due to $\theta^{r,r'}_m$, $\mathcal{K}^*$ as the users that suffer more attacks after $\theta^{r,r'}_m$ than before, and $\mathcal{K}^\circ$ as the corresponding users that suffer fewer attacks. A matching θ is stable if and only if, for each player $m \in \mathcal{M}$ with $\theta(m) = r$, no swap matching $\theta^{r,r'}_m$ satisfies the following conditions, given $\mathcal{M}^+ = \{m, m'\} \setminus \{\{m, m'\} \cap \mathcal{M}^*\}$, $\mathcal{K}^+ = \{k, k'\} \setminus \{\{k, k'\} \cap \mathcal{K}^*\}$, $\exists r' \in \mathcal{R}$, $\exists m' \in \mathcal{M}^\theta_{k'} \cup m_{0,k'}$:*

$$\begin{aligned}
&1)\ \forall s \in \left\{\mathcal{M}^+, \mathcal{K}^+\right\}, U_s(\theta^{r,r'}_m) \geq U_s(\theta), \\
&\sum_{m^- \in \{\mathcal{M}^*, \mathcal{M}^\circ\}} U_{m^-}(\theta^{r,r'}_m) \geq \sum_{m^- \in \{\mathcal{M}^*, \mathcal{M}^\circ\}} U_{m^-}(\theta), \\
&\sum_{k^- \in \{\mathcal{K}^*, \mathcal{K}^\circ\}} U_{k^-}(\theta^{r,r'}_m) \geq \sum_{k^- \in \{\mathcal{K}^*, \mathcal{K}^\circ\}} U_{k^-}(\theta)\ \textit{and} \\
&2)\ \exists s \in \left\{\mathcal{M}^+, \mathcal{K}^+\right\}, U_s(\theta^{r,r'}_m) > U_s(\theta)\ \textit{or} \\
&\sum_{m^- \in \{\mathcal{M}^*, \mathcal{M}^\circ\}} U_{m^-}(\theta^{r,r'}_m) > \sum_{m^- \in \{\mathcal{M}^*, \mathcal{M}^\circ\}} U_{m^-}(\theta)\ \textit{or} \\
&\sum_{k^- \in \{\mathcal{K}^*, \mathcal{K}^\circ\}} U_{k^-}(\theta^{r,r'}_m) > \sum_{k^- \in \{\mathcal{K}^*, \mathcal{K}^\circ\}} U_{k^-}(\theta).
\end{aligned}$$

Based on [20], we add extra conditions to keep the sum of utilities of the players that suffer more attacks and those who gain a decrease in attacks to increase, respectively for channels and users. And we only force the utilities of players in the swap to increase if they have not suffered more attacks.

Remark 1: *In Definition 3, every approved swap matching will make the overall SS-R (i.e., Φ^{sec}) strictly increase and the iteration will finally converge to a sub-optimal solution of (9).*

Based on the above analysis, we develop a swap-based secure resource allocation (SSRA) algorithm to obtain a sub-optimal solution of (9). As shown in **Algorithm 1**, SSRA starts by a random matching, and then the swap matching process aiming at optimizing the overall SS-R follows.

Algorithm 1: The SSRA algorithm

```
Initialization: Obtain the initial matching θ_0 by randomly matching channels m with r, ∀m ∈ M, ∀r ∈ R. Denote the current matching as θ.
Swap-matching for a stable matching:
repeat
    for all m ∈ M do
        r = θ(m);
        for all r' ∈ R, r' ≠ r do
            for all m' ∈ M^θ_{k'} ∪ m_{0,k'}, k' ∈ r' do
                Generate a swap matching θ^{r,r'}_m;
                if θ^{r,r'}_m satisfies the conditions in Definition 3 then
                    Update the matching as θ = θ^{r,r'}_m;
                else
                    Keep the current matching state;
until θ is stable according to Definition 3;
```

Remark 2: The worst time complexity of the proposed SSRA is $O\left(V \times M \times (M+K) \times N_{\max} \times H\right)$ where V is the number of iterations, $N_{\max} = \max\left(|\mathcal{N}_{\text{Si}}|, |\mathcal{N}_{\text{Bi}}|\right)$ and $H = M \log\left(\min\left(M - D, D\right)\right)$ is the complexity of heap sort algorithm. However, the complexity of exhaustive searching method is $O((K \times N_{\max})^M \times H)$, which is unacceptable.

B. Complement with Fairness Awareness

The SSRA can efficiently maximize the overall SS-R, but shows defects in resource allocation fairness among different users since it is unconscious for users' accesses and the final matching is significantly affected by the initial matching.

In each swap operation, any user can only be allocated one more channel at most. Based on this, if a user k can not access the network even with one more channel based on the initial matching, it will be much less possible to gain more channels in the following iterations according to Definition 3, which results in unfairness. To address this, we propose to obtain an access-fair matching before finding a sub-optimal solution.

Definition 4. *Denote m' as the channel that swap user with m in swap matching $\theta_m^{r,r'}$, and $\mathcal{K}_s$ as the legitimate users affected by $\theta_m^{r,r'}$. Give $\mathcal{K}_+ \subseteq \mathcal{K}_s$, where $\forall s \in \mathcal{K}_+$, $U_s(\theta) \geq \Phi_{\text{th}}^{\text{sec}}$, and $\mathcal{K}_- = \mathcal{K}_s \backslash \mathcal{K}_+$. A matching θ is access-fair if $\forall s \in \mathcal{K}$, $U_s(\theta) \geq \Phi_{\text{th}}^{\text{sec}}$ or for each $m \in \mathcal{M}$ with $\theta(m) = r$, no swap matching $\theta_m^{r,r'}$ satisfies the following conditions:*

1) $\forall s \in \mathcal{K}_+$, $U_s(\theta_m^{r,r'}) \geq \Phi_{\text{th}}^{\text{sec}}$ *and*
2) $\forall s \in \mathcal{K}_-$, $\Phi_k^{acc}(\theta_m^{r,r'}) \geq \Phi_k^{acc}(\theta)$ *and*
3) $\exists s \in \mathcal{K}_-$, $\Phi_k^{acc}(\theta_m^{r,r'}) > \Phi_k^{acc}(\theta)$.

The conditions above ensure access for users that have accessed before and motivate other users to obtain increases in SS-R. Based on this, we propose a swap-based secure resource allocation algorithm with fairness awareness (SSRA-FA), as shown in **Algorithm 2**. Considering SSRA-FA may show differences from SSRA in SS-R and complexity due to the additional swap stage, we characterize it as an optional complement to SSRA with fairness awareness.

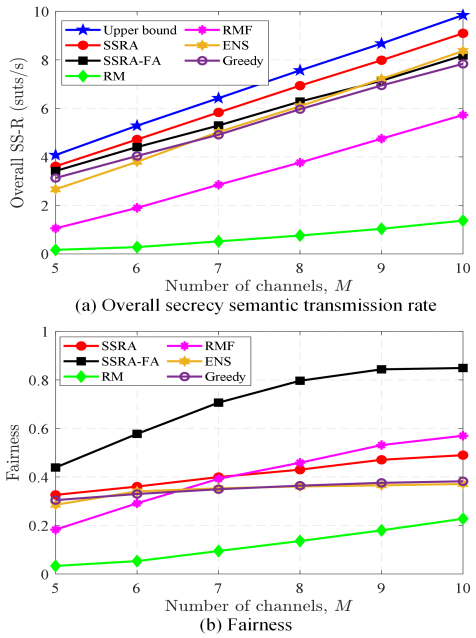
Algorithm 2: The SSRA-FA algorithm

1 **Initialization:** Same initialization as in Algorithm 1.
2 ***Stage 1: Swap-matching for an access-fair matching:***
3 Similar operations as in Algorithm 1 (lines 3-13) with Definition 4 substituting Definition 3;
4 ***Stage 2: Swap-matching for a stable matching:***
5 Same operations as those in Algorithm 1 (lines 3-13);

Remark 3: The worst time complexity of SSRA-FA is $O\left((V_1+V_2)\times M\times(M+K)\times N_{\max}\times H\right)$.

IV. Simulation Results

This section provides simulation results and analysis of the proposed secure resource allocation approaches. A cell with a radius of 500 m is considered, where legitimate users are randomly distributed. The attacker is also randomly distributed but is set to be away from the edge of the cell within 100 m. Similar to [10], the pathloss model is $128.1+37.6\lg[\mathrm{d(km)}]$ dB and the shadowing factor is set to 6 dB. The bandwidth of one channel is set as $B = 180$ kHz and the noise power spectral density is $N_0 = -174$ dBm/Hz. We set $p_k = p_{jam} = 10$ dBm. For the attacker, the SI coefficient is set as $\delta = 0.05$. The performance constraints are $\chi_{\text{th}} = 0.9$ and $\Phi_{\text{th}}^{\text{sec}} = 1.0 \times B$ suts/s. The semantic entropy and the mapping relations of χ are obtained from [11]. The ranges of numbers of transmitted semantic symbols are set as $\mathcal{N}_{\text{Si}} = \{1, 2, ..., 20\}$, $\mathcal{N}_{\text{Bi,t}} = \{2, 4, 6, 8, 10\}$ and $\mathcal{N}_{\text{Bi,i}} = \{394, 788, 1576, 2364, 3152\}$, respectively.



(a) Overall secrecy semantic transmission rate

(b) Fairness

Fig. 2. Performance of algorithms vs. number of available channels with $(K_{\text{Si}}, K_{\text{Bi}}) = (2, 2)$ and $D = 4$.

We compare the following approaches: (1) **SSRA**: Our proposed secure resource allocation algorithm; (2) **SSRA-FA**: Our proposed complement to SSRA with fairness awareness; (3) **Random matching algorithm (RM)**; (4) **Random matching with fixed symbol selection (RMF)**: Channels are randomly allocated, but the numbers of transmitted semantic symbols are selected exhaustively [11]; (5) **Exhaustive search without security awareness (ENS)**; (6) **Greedy search (Greedy)**: A heuristic algorithm that greedily enhances the overall SS-R by maximizing the individual SS-R over each channel, whose complexity is $O(M \times K \times N_{\max})$; (7) **The upper bound of exhaustive search (Upper bound)**.

We compare each algorithm in SS-R and resource allocation fairness calculated by Jain's fairness index as $\frac{\left(\sum_{k=1}^{K}\Phi_k^{\text{sec}}\right)^2}{K\sum_{k=1}^{K}\left(\Phi_k^{\text{sec}}\right)^2}$. Considering the fixed bandwidth of B, next we divide SS-R by B for better expression. Fig. 2 compares each algorithm with different numbers of channels. Fig. 2(a) shows the overall SS-R of each method increases with more channels. With proper iteration conditions, SSRA and SSRA-FA can efficiently utilize the resources, flexibly counteract the limited attacks under the proposed game-guided framework, and thus outperform RM and RMF, where SSRA achieves higher SS-R than ENS and Greedy, and is close to Upper bound. Specifically, there are improvements of 8% to 36% and 15% to 19% provided by SSRA over ENS and Greedy, respectively. Due to the additional swap stage, SSRA-FA shrank its search space before searching for a sub-optimal solution which results in lower SS-R than SSRA and ENS in some cases. Yet, SSRA-FA is still able to obtain improvements of 3% to 9% over Greedy. Fig. 2(b) presents the resource allocation fairness of each algorithm. With more channels, more users can access the network, which increases fairness. SSRA-FA

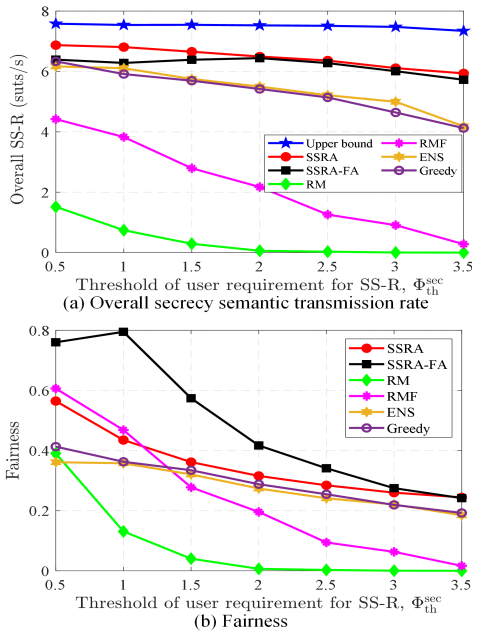


Fig. 3. Performance of algorithms vs. threshold of user requirement for SS-R with $(K_{\rm Si}, K_{\rm Bi}) = (2, 2)$ and $(M, D) = (8, 4)$.

outperforms other algorithms since the additional swap stage allows more users to access the network by fair allocation. More specifically, compared with SSRA, Greedy and ENS, SSRA-FA achieves fairness improvements of 35% to 85%, 44% to 125% and 54% to 130%, respectively.

Fig. 3 shows the metrics of each algorithm versus the threshold of user's SS-R, i.e., $\Phi_{\rm th}^{\rm sec}$. In Fig. 3(a), with higher $\Phi_{\rm th}^{\rm sec}$, the overall SS-R of each algorithm decreases, due to stronger user restrictions. Moreover, for SSRA-FA, since the swap stage for an access-fair matching becomes less effective with higher $\Phi_{\rm th}^{\rm sec}$, more search spaces are released to enhance the overall SS-R. As a result, SSRA-FA becomes closer to SSRA, which causes an upward trend before further decreases in SS-R. SSRA and SSRA-FA achieve higher overall SS-R than other approaches except Upper bound, which reflects their adaptabilities. Compared with Greedy and ENS, SSRA provides improvements of 8% to 44% and 11% to 42% in overall SS-R, respectively. And for SSRA-FA, the corresponding values are 3% to 37% and 2% to 39%. Fig. 3(b) depicts the fairness of different algorithms, where SSRA-FA outperforms other methods and achieves fairness higher than Greedy and ENS by 25% to 120% and 24% to 122%. Similar to SS-R, higher $\Phi_{\rm th}^{\rm sec}$ motivates more channels fairly assigned to each user, which results in the fairness increase of SSRA-FA before the downward trend. Other algorithms generally gain fairness decreases since fewer users can access the network.

V. Conclusion

This paper has investigated a security-aware resource allocation problem against a hybrid attacker for semantic communication networks. We proposed two swap-based algorithms to solve the problem by jointly optimizing the channel allocation and numbers of transmitted semantic symbols under the established framework guided by Stackelberg game. Comparative simulation results reveal the effectiveness and adaptability of our approaches. There are some possible future research directions we may consider in our future works. First, the formulated anti-attack scheme is based on complete CSI, whereas considering partial CSI is more practical in real-world scenarios. Second, more intelligent attacks and dynamic environments would provide the scheme with better applicability.

References

[1] G. Shi, Y. Xiao, Y. Li, and X. Xie, "From semantic communication to semantic-aware networking: Model, architecture, and open problems," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 44C50, Aug. 2021.

[2] W. Yang, H. Du, Z. Q. Liew, W. Y. B. Lim, Z. Xiong, D. Niyato, X. Chi, X. Shen, and C. Miao, "Semantic communications for future internet: Fundamentals, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 213C250, 1st Quart., 2023.

[3] Z. Qin, X. Tao, J. Lu, and G. Y. Li, "Semantic communications: Principles and challenges," Dec. 2021, *arXiv: 2201.01389*.

[4] Q. Li, M. El-Hajjar, I. Hemadeh, A. Shojaeifard, A. A. M. Mourad, B. Clerckx and L. Hanzo, "Reconfigurable Intelligent Surfaces Relying on Non-Diagonal Phase Shift Matrices," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 6367-6383, Jun. 2022.

[5] Q. Li, M. El-Hajjar, I. Hemadeh, D. Jagyasi, A. Shojaeifard and L. Hanzo, "Performance Analysis of Active RIS-Aided Systems in the Face of Imperfect CSI and Phase Shift Noise," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 8140-8145, Jun. 2023.

[6] H. Xie, Z. Qin, G. Y. Li, and B. H. Juang, "Deep learning enabled semantic communication systems," *IEEE Trans. Signal Process.*, vol. 69, pp. 2663C2675, Apr. 2021.

[7] Z. Weng and Z. Qin, "Semantic communication systems for speech transmission," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2434C2444, Aug. 2021.

[8] H. Xie, Z. Qin, X. Tao, and K. B. Letaief, "Task-oriented multi-user semantic communications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 9, pp. 2584-2597, Sep. 2022.

[9] J. Bao, P. Basu, M. Dean, C. Partridge, A. Swami, W. Leland, and J. A. Hendler, "Towards a theory of semantic communication," in *Proc. IEEE Netw. Sci. Workshop*, pp. 110C117, 2011.

[10] L. Yan, Z. Qin, R. Zhang, Y. Li, and G. Y. Li, "Resource allocation for text semantic communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1394-1398, Jul. 2022.

[11] L. Yan, Z. Qin, R. Zhang, Y. Li, and G. Ye Li, "QoE-aware resource allocation for semantic communication networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 3272C3277, 2022.

[12] H. Hu, X. Zhu, F. Zhou, W. Wu, and R. Q. Hu, "Semantic-oriented resource allocation for multi-modal UAV semantic communication networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 7213-7218, 2023.

[13] K. Zhang, M. Peng, P. Zhang and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Trans. Veh. Technol.*,vol. 66, no. 2, pp. 1822-1834, Feb. 2017.

[14] 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," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 376-388, Jan. 2020.

[15] B. Ahuja, D. Mishra and R. Bose, "Fair subcarrier allocation for securing OFDMA in IoT against full-duplex hybrid attacker," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2898-2911, Mar. 2021.

[16] Y. Zhang, Y. Zhang, Y. Xu, Y. Xu, Y. Yang, Y. Luo, Q. Wu, and X. Liu, "A multi-leader one-follower Stackelberg game approach for cooperative anti-jamming: No pains, no gains," *IEEE Wireless Commun. Lett.*, vol. 22, no. 8, pp. 1680-1683, Aug. 2018.

[17] Y. Chen, Q. Yang, Z. Shi and J. Chen, "The model inversion eavesdropping attack in semantic communication systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 5171-5177, 2023.

[18] Y. Li, X. Zhou, and J. Zhao, "Resource allocation for semantic communication under physical-layer security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 2063-2068, 2023.

[19] S. Bayat, Y. Li, L. Song, and Z. Han, "Matching theory: Applications in wireless communications," *IEEE Signal Process. Mag.*, vol. 33, no. 6, pp. 103C122, Nov. 2016.

[20] J. Zhao, Y. Liu, K. K. Chai, A. Nallanathan, Y. Chen, and Z. Han, "Spectrum allocation and power control for non-orthogonal multiple access in HetNets," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 5825-5837, Sep. 2017.