Wei YANG, Jing MAO, Chen CHEN, et al., 2018. Resource allocation for physical-layer security in OFDMA downlink with imperfect CSI. *Frontiers of Information Technology & Electronic Engineering*, 19(3):398-408. https://doi.org/10.1631/FITEE.1700026

Resource allocation for physical-layer security in OFDMA downlink with imperfect CSI

Key words: Resource allocation; Orthogonal frequency-division multiple access (OFDMA); Imperfect channel state information (CSI); Physical layer security

Corresponding author: Chen Chen, c.chen@pku.edu.cn
ORCID: http://orcid.org/0000-0001-5058-6749

Motivation

- Secrecy or private message exchanges between mobile users and the base station are generally needed in present and future wireless systems. It is essential to integrate physical layer security which is an information-theoretic approach that achieves secrecy by using channel codes and advanced signal processing techniques into the resource allocation problem in multiuser OFDMA systems.
- Nearly none of existing works focused on the secrecy-based resource allocation problem under the imperfect channel state constraint, which is more practical.

Main idea

1. Modeling of imperfect channel state information

- ■ Noise and estimation errors
- ■ Feedback delay and LMMSE channel prediction
- ■ Limited feedback capacity --- the rate-distortion theory is used to find the relationship between quantization errors and feedback channel capacity

2. Maximizing the minimum secrecy rate among all users under the imperfect CSI constraint

- ■ Optimal power allocation algorithm for given subcarrier assignment
- ■ Low complexity subcarrier allocation based on a greedy algorithm

1. System model & problem formulation

Real CSI conditioned on partial CSI $f(\gamma_{n,k}|\hat{\gamma}_{n,k})$ is an NC_{χ^2} distribution.

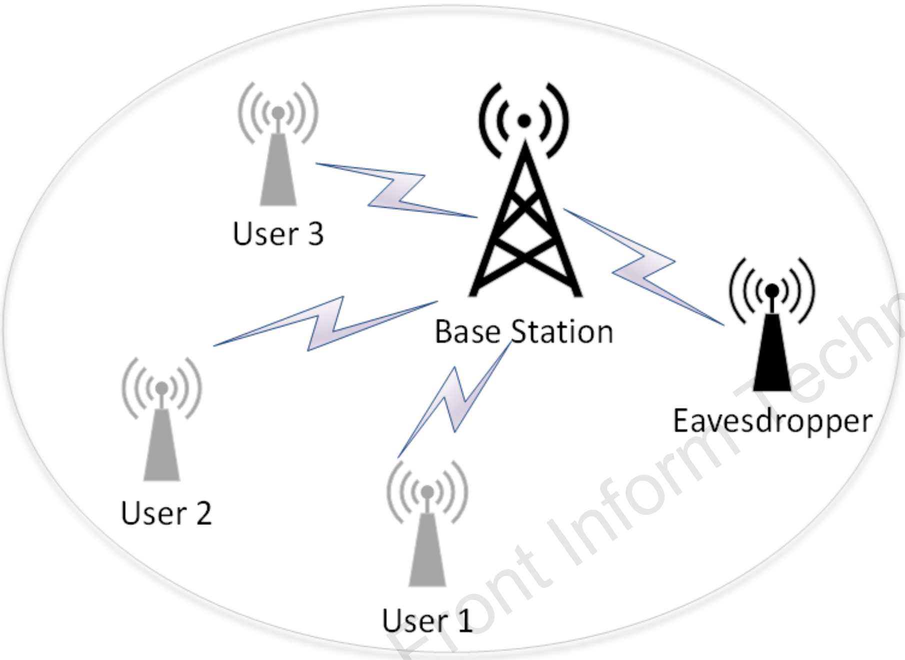


Fig. 1 System model

Problem formulation

$$\max_{\rho_{n.k},p_{n,k}} \min_{k} \sum_{n\in\mathbf{N}} \rho_{n.k} C_{n,k}(p_{n,k})$$

$$s.t. \sum_{k\in K,n\in N} \rho_{n.k} p_{n,k} \leq P_T, \tag{1a}$$

$$\sum_{k\in K} \rho_{k,n} = 1, n \in N, \tag{1b}$$

$$\rho_{k,n} \in \{1,0\},\ n \in N, k \in K, \tag{1c}$$

$$0 \leq p_{k,n} \leq P_T,\ n \in N, k \in K. \tag{1d}$$

Secrecy capacity, $C_{n,k}(p_{n,k}) = \{R_{n,k}(p_{n.k},\hat{\gamma}_{n,k}) - R_{n,e}(p_{n.k},\hat{\gamma}_{n,e})\}^{+}$

2. Power allocation for given subcarrier assignment

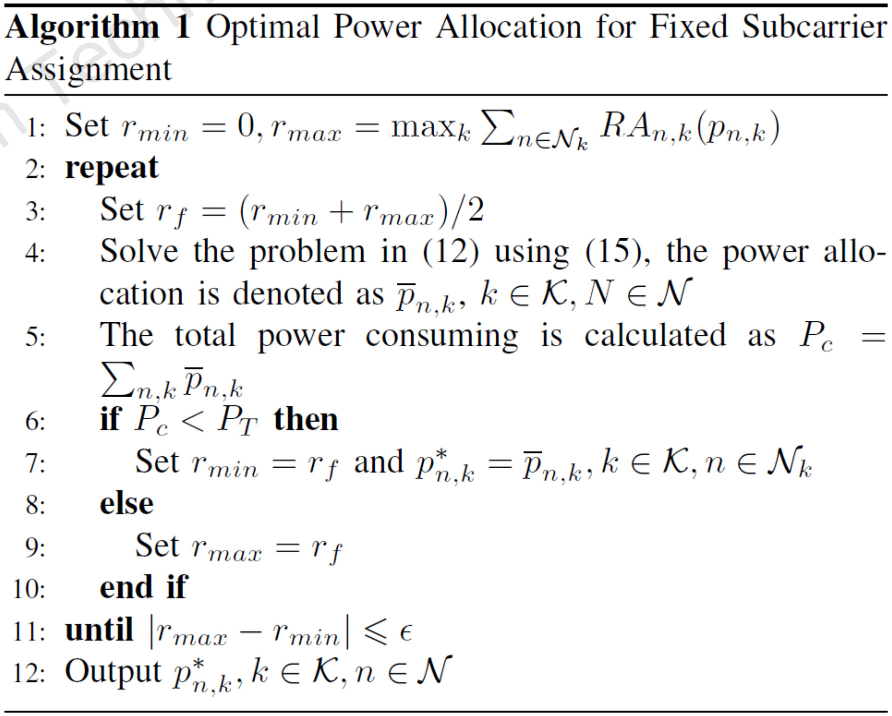
Problem conversion

$$\max_{p_{n,k},r} r$$

$$s.t.\ 0 \le r \le \sum_{n \in N_k} C_{n,k}(p_{n,k}), k \in K,$$

$$\sum_{k \in K, n \in N_k} p_{n,k} \le P_T.$$

Use the convex optimization tool to find the optimal solution.



Algorithm 1 Optimal Power Allocation for Fixed Subcarrier Assignment

```
Set $r_{min} = 0, r_{max} = \max_k \sum_{n \in \mathcal{N}_k} RA_{n,k}(p_{n,k})$
repeat
    Set $r_f = (r_{min} + r_{max})/2$
    Solve the problem in (12) using (15), the power allocation is denoted as $\overline{p}_{n,k}$, $k \in \mathcal{K}, N \in \mathcal{N}$
    The total power consuming is calculated as $P_c = \sum_{n,k} \overline{p}_{n,k}$
    if $P_c < P_T$ then
        Set $r_{min} = r_f$ and $p^*_{n,k} = \overline{p}_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}_k$
    else
        Set $r_{max} = r_f$
    end if
until $|r_{max} - r_{min}| \leqslant \epsilon$
Output $p^*_{n,k}, k \in \mathcal{K}, n \in \mathcal{N}$
```

3. Greedy algorithm based subcarrier allocation

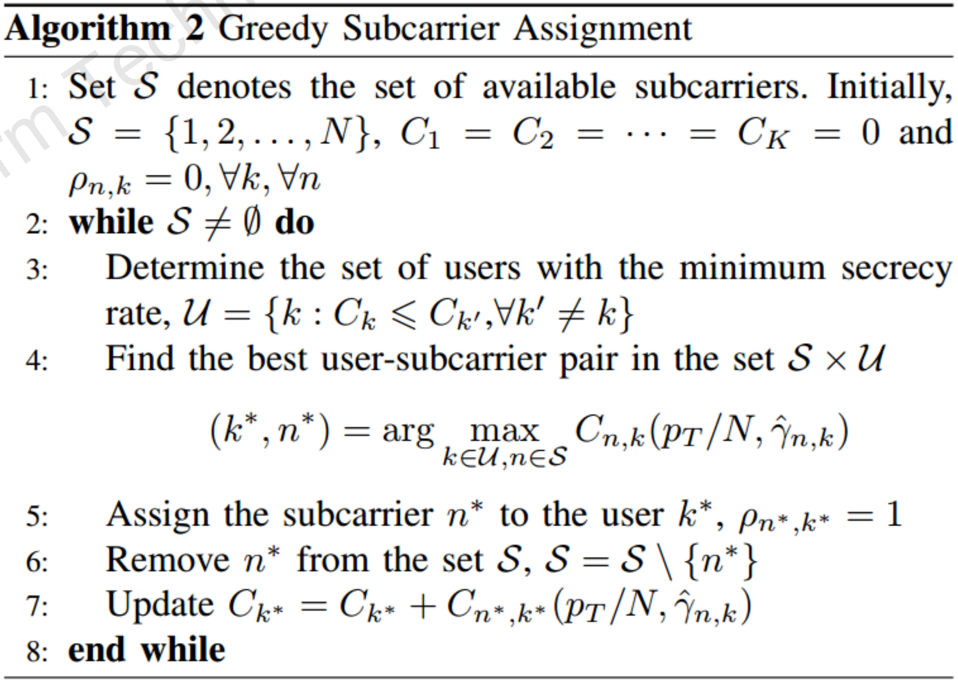
Assume that the power is equally split

$$\max_{\rho_{n,k},R} R$$

$$st.\ \sum_{n\in N}\rho_{n,k}C_{n,k}(p_{n.k})\geq R,\forall k;$$

$$\sum_{k\in K,n\in N}\rho_{n,k}p_{n.k}\leq P_T$$

The performance is limited by the lowest secrecy capacity



Algorithm 2 Greedy Subcarrier Assignment

```
Set $\mathcal{S}$ denotes the set of available subcarriers. Initially, $\mathcal{S}=\{1,2,\ldots,N\}$, $C_1=C_2=\cdots=C_K=0$ and $\rho_{n,k}=0,\forall k,\forall n$
while $\mathcal{S}\neq\emptyset$ do
    Determine the set of users with the minimum secrecy rate, $\mathcal{U}=\{k:C_k\leqslant C_{k'},\forall k'\neq k\}$
    Find the best user-subcarrier pair in the set $\mathcal{S}\times\mathcal{U}$
        $(k^*,n^*)=\arg\max_{k\in\mathcal{U},n\in\mathcal{S}} C_{n,k}(p_T/N,\hat{\gamma}_{n,k})$
    Assign the subcarrier $n^*$ to the user $k^*$, $\rho_{n^*,k^*}=1$
    Remove $n^*$ from the set $\mathcal{S}$, $\mathcal{S}=\mathcal{S}\setminus\{n^*\}$
    Update $C_{k^*}=C_{k^*}+C_{n^*,k^*}(p_T/N,\hat{\gamma}_{n,k})$
end while
```

Major results

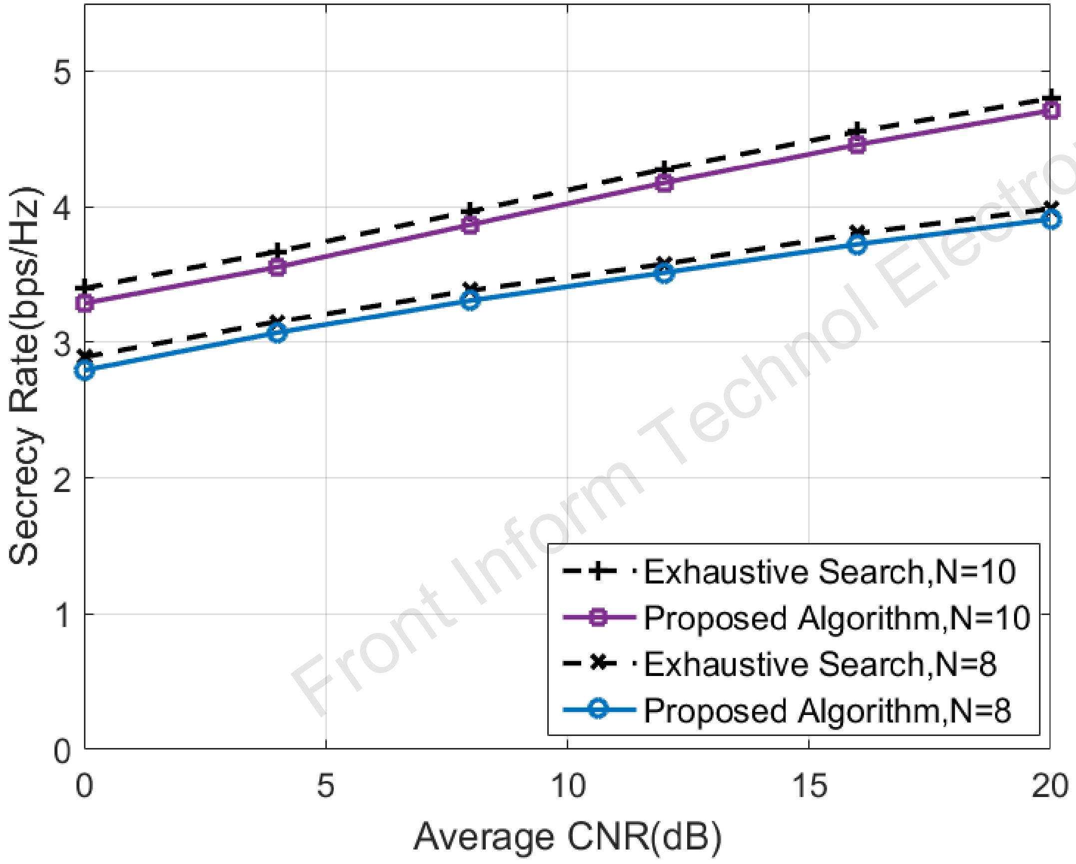


Fig. 2 Comparison of the proposed suboptimal algorithm and the optimal algorithm

Setup

1. $N = 8{,}10$
2. $K = 2$
3. $P_T = 20\ \mathrm{W}$
4. $v_k = 50km/h$
5. $Q = 5$
6. $\delta m_e = \delta m_k = 1$

Results

The performance of the proposed algorithm is very close to that of the optimal exhaustive search method.

Major results

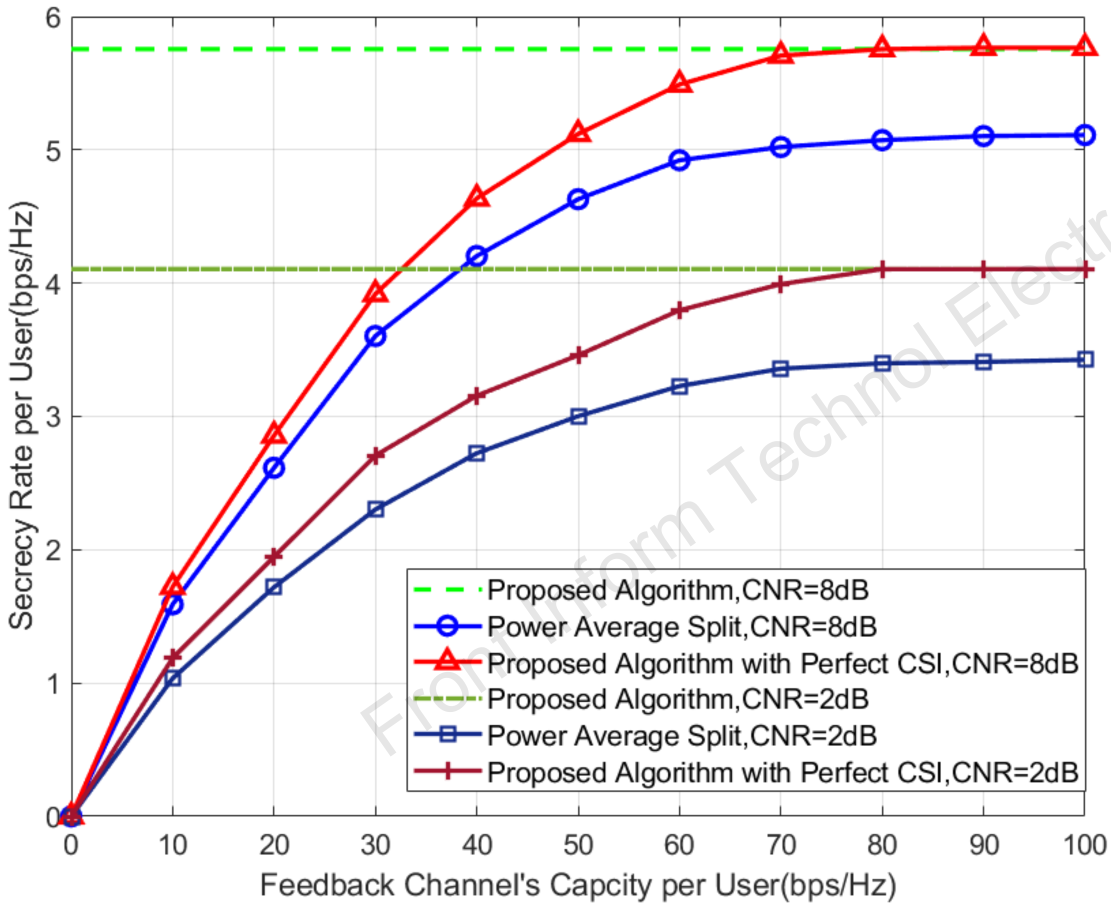


Fig. 3 Secrecy rate versus the capacity of the feedback channel

Setup

1. $N = 16$
2. $K = 4$
3. $P_T = 20\ \mathrm{W}$
4. $CNR = 8, 10\mathrm{dB}$

Results

The secrecy rate with imperfect CSI increases as the feedback channel capacity increases. Our proposed algorithm can achieve the secrecy rate with perfect CSI when the capacity of the feedback channel is high.

Conclusions

- To establish a unified mathematical model of imperfect CSI, three kinds of partial CSI scenarios were discussed, i.e., estimation errors, CSI feedback delay, and limited feedback capacity.
- Based on the imperfect CSI, we formulated the max-min secrecy rate problem and proposed a low computation complexity solution which includes power allocation and subcarrier allocation.
- Simulation results showed that the performance of the proposed algorithm is close to the optimal bound. The secrecy rate could catch up with the performance of perfect CSI when CSI feedback capacity is high.