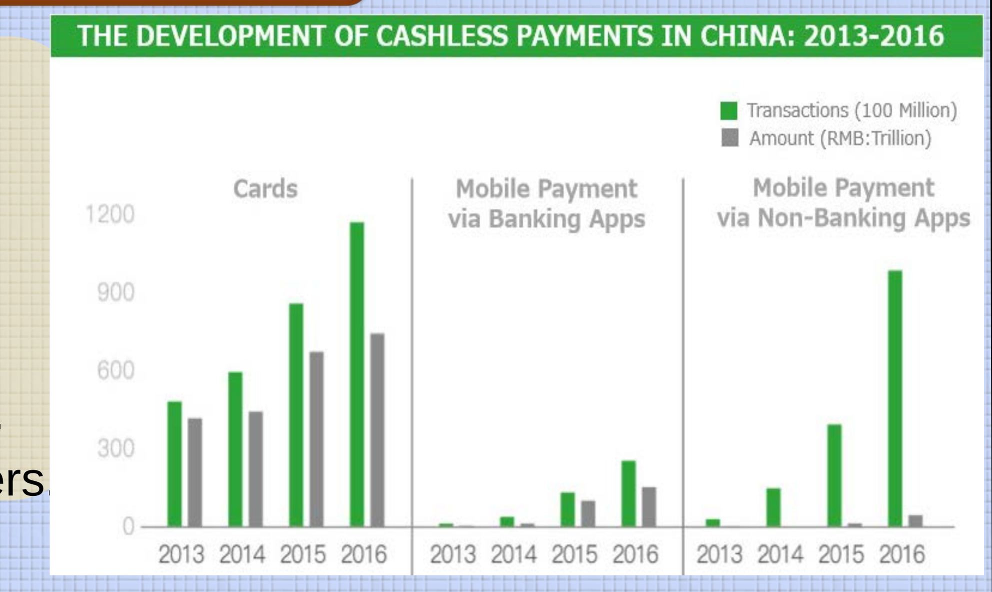
SHANGHAI JIAO TONG UNIVERSITY

Artificial Interference Aided Physical Layer Security in Cache-enabled Heterogeneous Networks

Zhao Wu, Zhiyong Chen, Kuikui Li，Bin Xia，Peng Chen

1 Background

- **Challenges:**
  - Increasing Security Rank
    - Mobile payment
    - Internet of things
  - Complex Network topology.
    - Heterogeneous BS deployment.
    - Randomly located Eavesdroppers



Physical Layer Solutions:
- Artificial noise
- Cooperative relays

Caching:
- Improve signal strength
- Cancel received interference

- **Questions:**
  How to utilize cache ability to improve transmission secrecy ?
  How to measure cache ability in secrecy improving?

2 System Model

- **Network and Caching Model**
  - A cache-enabled 3-tier HetNet : BSs Φ_b , users Φ_u, and Eves Φ_e.
  - A database: N files with equal length, $\boldsymbol{F}=\{f_1, f_2, \dots, f_N\}$.
    - Request probability: p_i, Zipf distribution.
  - BSs can access all the files in $\boldsymbol{F}$ without counting costs.
  - Only $\boldsymbol{\alpha}$ part of users have cached the files $\boldsymbol{M}=\{f_1, f_2, \dots, f_M\}$ from $\boldsymbol{F}$.
    - Cache hit ratio $\boldsymbol{\delta}=\sum_{i=1}^{M} p_i$.

- **File Access Protocol**
  - **Self-offloading: Cache-enabled user** u_o requests content from $\boldsymbol{M}$ which can be served by their local storage.
  - **Secure-transmission: Cache-enabled user** u_o requests content from $\boldsymbol{F}/\boldsymbol{M}$ which is served by the nearest BS in secure-transmission.

    Requested file ! $t_i=\sqrt{\boldsymbol{\theta} P}x_i+\sqrt{(1-\boldsymbol{\theta})P}x_m$ Cached file !
    - BSs served in this state are denoted as $\Phi_{b_1}(\lambda_{b_1})$
  - **Normal-transmission: Cache-untenabled user** u_o requests content from $\boldsymbol{F}$ which is served by the nearest BS in normal-transmission.

    $t_i=\sqrt{P}x_i$
    - BSs served in this state are divided by $x_i \in/\notin M$ as $\Phi_{b_2}(\lambda_{b_2})$, $\Phi_{b_3}(\lambda_{b_3})$

3 Transmission Scheme Analysis

- **Normal Transmission (NT)**
  - Consider a non-colluding wiretap scenario where each Eve individually overhears the data transmission from u_o to b_o.
  - The received SINR of u_o and an arbitrary Eve e_j can be write as (i=u_o, e_j)

$$\mathrm{SINR}_i=\frac{P\left|h_{i,b_0}\right|^2 d_{i,b_0}^{-\beta}}{\sum_{k\in\Phi_b\setminus\{b_0\}} P\left|h_{i,b_k}\right|^2 d_{i,b_k}^{-\beta}+\sigma^2}$$

Note that interference come from Φ_{b_1}, Φ_{b_2} and Φ_{b_3}.

- **Secure Transmission (ST)**
  - Since the pre-cached signal x_m is known perfectly at u_o. And assume that the perfect channel state information is fully available at cache-enabled users. The received SINR of u_o is

$$\mathrm{SINR}_{u_o}=\frac{\theta P\left|h_{u_0,b_0}\right|^2 d_{u_0,b_0}^{-\beta}}{\theta\sum_{k\in\Phi_{b_1}\setminus\{b_0\}} P\left|h_{u_0,b_k}\right|^2 d_{u_0,b_k}^{-\beta}+\sum_{k\in\Phi_{b_3}} P\left|h_{u_0,b_k}\right|^2 d_{u_0,b_k}^{-\beta}+\sigma^2}$$

The (1−θ) part of interference from Φ_{b_1} can be cancelled. ← Cached files M → The fully interference from Φ_{b_2} can be cancelled.

The transmitted signal x_m can introduce an extra interference to greatly restrict the e_j. The received SINR of an arbitrary Eve $e_j\in\Phi_e$ can be write as

$$\mathrm{SINR}_{e_j}=\frac{\theta P\left|h_{e_j,b_0}\right|^2 d_{e_j,b_0}^{-\beta}}{(1-\theta)P\left|h_{e_j,b_0}\right|^2 d_{e_j,b_0}^{-\beta}+\sum_{k\in\Phi_b\setminus\{b_0\}}\left|h_{e_j,b_k}\right|^2 d_{e_j,b_k}^{-\beta}+\sigma^2}$$

It has the form of $\frac{\theta X}{C+(1-\theta)X}$ → Upper bound !

- **Average Secrecy Rate**
  - The average secrecy rate is defined as $\mathbb{C}=[max\{C_u-C_e\},0]$.
  - When $\sigma^2\to 0$(interference−limited), the average secrecy rate of NT and ST are

$$C_{NT}=\frac{1}{ln2}\int_0^{\infty}\frac{e^{-\lambda_e/\left[\lambda_b\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)\gamma_{th}^{\frac{2}{\beta}}\right]}}{(1+\gamma_{th})[Z(\gamma_{th})+1]}d\gamma_{th}$$

→ Only depend on the ratio of $\frac{\lambda_e}{\lambda_b}$!

$$C_{ST}=\frac{1}{ln2}\int_0^{\gamma_{th_0}}\frac{\lambda_b e^{-\lambda_e/\left[\lambda_b\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)\left[\frac{\gamma_{th}}{\theta-(1-\theta)\gamma_{th}}\right]^{\frac{2}{\beta}}\right]}}{(1+\gamma_{th})[\lambda_{b_1}Z(\gamma_{th})+\lambda_{b_3}Z(\gamma_{th})+\lambda_b]}d\gamma_{th}+\frac{1}{ln2}\int_{\gamma_{th_0}}^{\infty}\frac{\lambda_b d\gamma_{th}}{(1+\gamma_{th})[\lambda_{b_1}Z(\gamma_{th})+\lambda_{b_3}Z(\gamma_{th})+\lambda_b]}$$

→ Depend on θ, the ratio of $\frac{\lambda_e}{\lambda_b}$ and $\left(\frac{\lambda_{b_1}}{\lambda_b},\frac{\lambda_{b_3}}{\lambda_b}\right)$ which are related to α and δ !

where $Z(\gamma_{th})\triangleq\frac{2\gamma_{th}}{\beta-2}\,{}_2F_1\left(1,1-\frac{2}{\beta},2-\frac{2}{\beta},-\gamma_{th}\right)$, ${}_2F_1[\cdot]$ is the Gauss hypergeometric function and $\Gamma[\cdot]$ is the Gamma function.

- **Secrecy Coverage Probability**
  - The secrecy coverage probability is defined as $\mathrm{P}=P_r(\mathbb{C}>R_S)$.
  - When $\sigma^2\to 0$, the secrecy coverage probability of NT and ST are

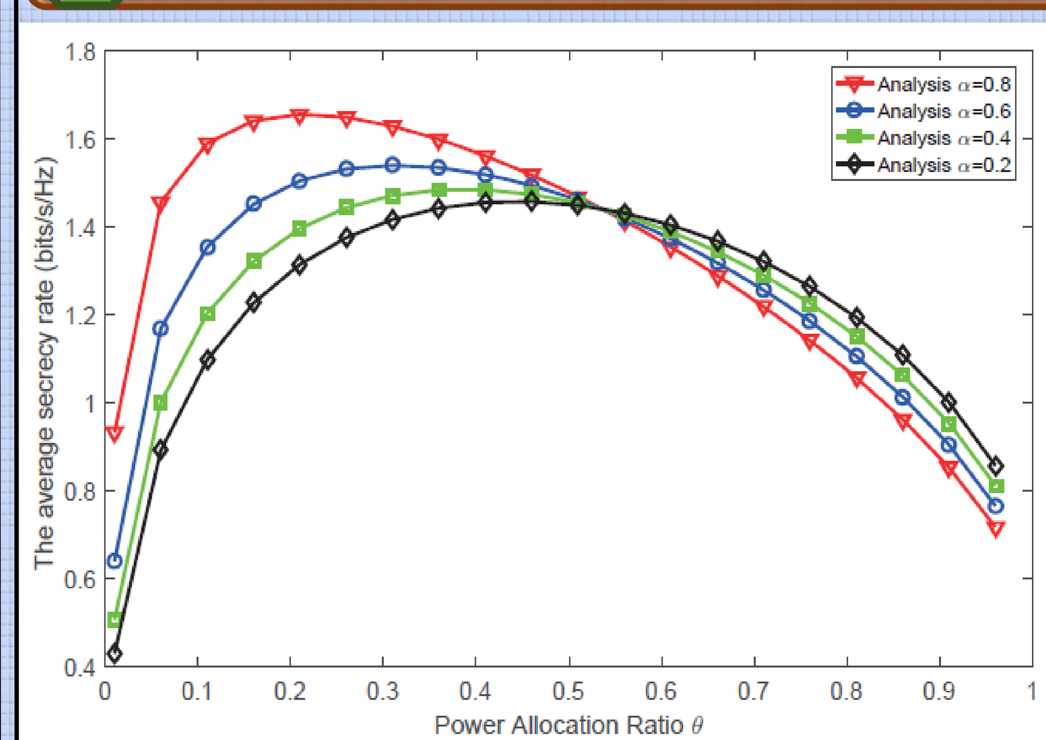
$$P_{NT}=\int_0^{\infty}\frac{2\lambda_e\gamma_{th}^{-\frac{\beta+2}{\beta}}e^{-\lambda_e/\left[\lambda_b\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)\gamma_{th}^{\frac{2}{\beta}}\right]}d\gamma_{th}}{\beta\lambda_b[G(R_S)+1]\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)}$$

→ Depend on θ, the ratio of $\frac{\lambda_e}{\lambda_b}$ and $\left(\frac{\lambda_{b_1}}{\lambda_b},\frac{\lambda_{b_3}}{\lambda_b}\right)$

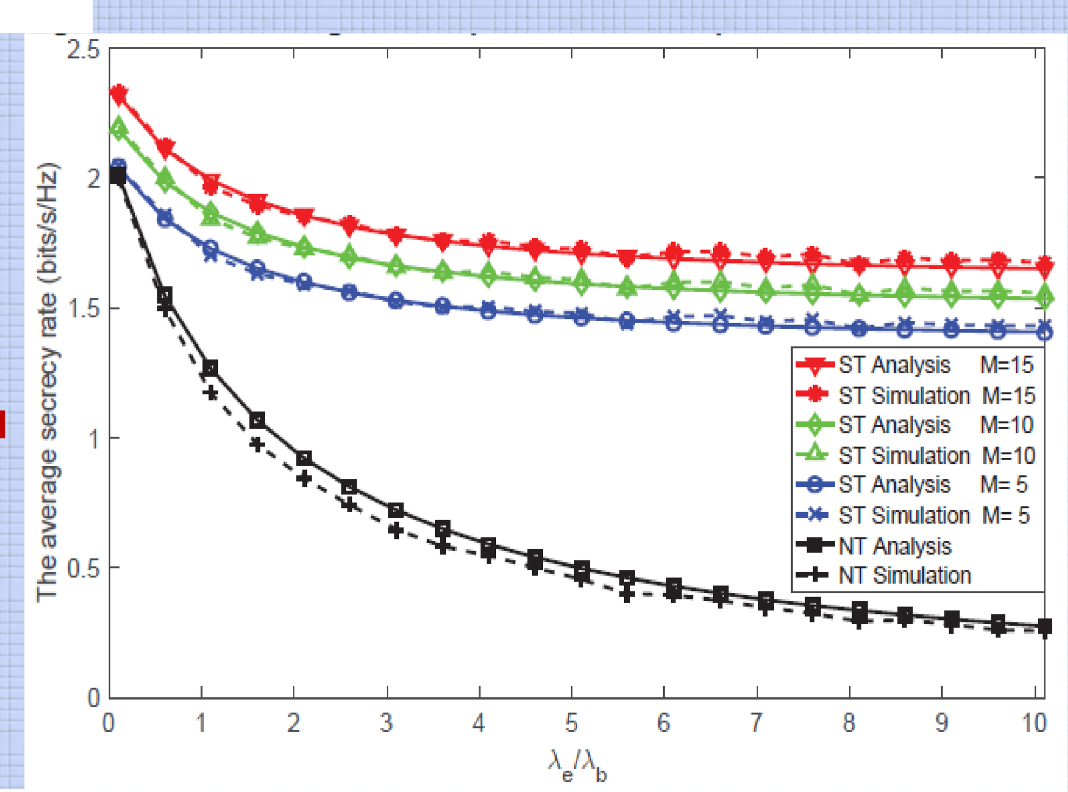
$$P_{ST}=\int_0^{\gamma_{th_0}}\frac{2\theta\lambda_e\gamma_{th}^{-\frac{\beta+2}{\beta}}e^{-\lambda_e/\left[\lambda_b\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)\left[\frac{\gamma_{th}}{\theta-(1-\theta)\gamma_{th}}\right]^{\frac{2}{\beta}}\right]}d\gamma_{th}}{\beta(1+\gamma_{th})[\lambda_{b_1}G(R_S)+\lambda_{b_3}G(R_S)+\lambda_b]\Gamma\left(1+\frac{2}{\beta}\right)\Gamma\left(1-\frac{2}{\beta}\right)\left[\frac{\gamma_{th}}{\theta-(1-\theta)\gamma_{th}}\right]^{\frac{\beta-2}{\beta}}}$$

where $G(R_S)\triangleq Z(2^{R_S}-1)$

4 Simulation & Numerical Results

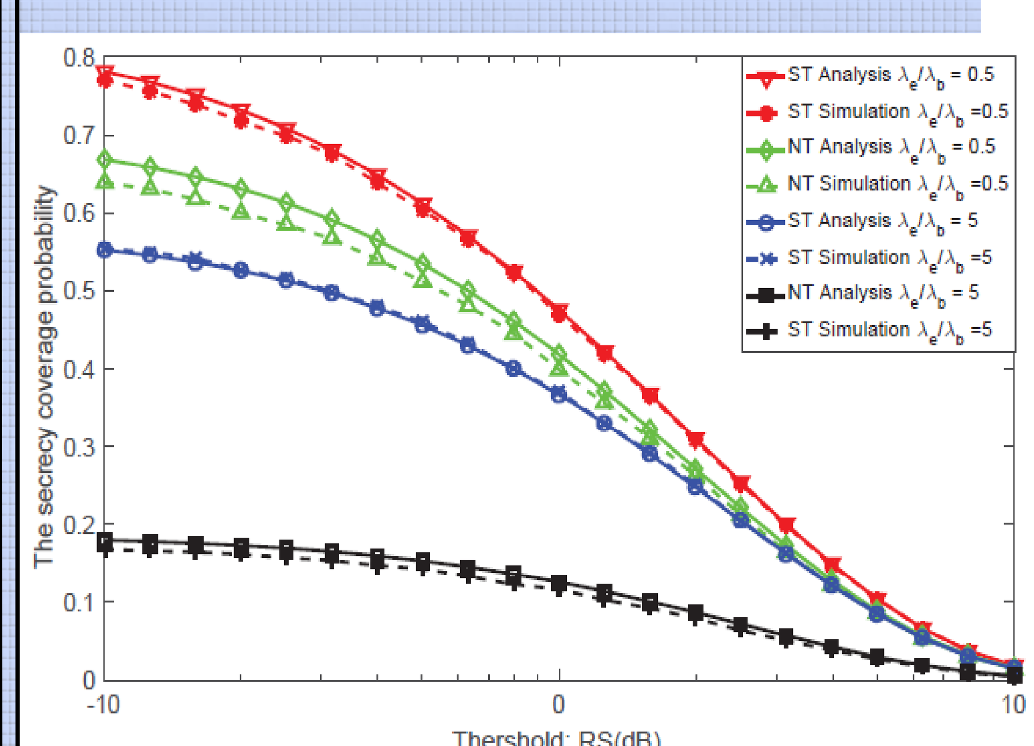


C_{ST} under different α and θ
It shows that there exists an optimal power allocation θ^* to achieve the maximal C_{ST} for a given cache user ratio α.



Compare of C_{ST} and C_{NT}
It shows that ST outperforms than NT in both Eve-dense scenario and Eve-sparse scenario.

It also shows that larger cache size achieves better secrecy rate.



Compare of P_{ST} and P_{NT}
It shows that ST outperforms than NT with larger secrecy coverage probability in both scenarios.

The 19th IEEE International Workshop on Signal Processing Advances in Wireless Communications, Session on Theoretical Network Bounds & Models

Email：zhiyongchen@sjtu.edu.cn