The average secrecy rate is defined as

\[ C_{ST} = \frac{1}{2} \int_{\gamma_{th}}^\infty \lambda_b e^{-\lambda_b \gamma} \left( \frac{(1-2)^2}{(1-2)^2 + \beta} \right) \frac{\Gamma(\frac{\beta}{2})}{\Gamma(\frac{\beta}{2} + 1)} \frac{\gamma^{\frac{\beta}{2}}}{\gamma^{\frac{\beta}{2} + 1}} d\gamma_{th} \]

where \( \gamma_{th} \) is the threshold SNR. This shows that there exists an optimal power allocation \( \alpha \) to achieve the maximal \( C_{ST} \) for a given cache user ratio \( \beta \).

**Average Secrecy Rate**

- The average secrecy rate is defined as \( C = \max(C_u - C_e, 0) \).
- When \( \sigma^2 \to 0 \) (interference-limited), the average secrecy rate of NT and ST are

\[ C_{NT} = \frac{1}{2} \int_{\gamma_{th}}^\infty e^{-\lambda_b \gamma} \left( \frac{(1-2)^2}{(1-2)^2 + \beta} \right) \frac{\Gamma(\frac{\beta}{2})}{\Gamma(\frac{\beta}{2} + 1)} \frac{\gamma^{\frac{\beta}{2}}}{\gamma^{\frac{\beta}{2} + 1}} d\gamma_{th} \]

**Secrecy Coverage Probability**

The secrecy coverage probability is defined as \( P = P_c(\gamma > R_e) \). When \( \sigma^2 \to 0 \), the secrecy coverage probability of NT and ST are

\[ P_{NT} = \int_{\gamma_{th}}^\infty e^{-\lambda_b \gamma} \left( \frac{(1-2)^2}{(1-2)^2 + \beta} \right) \frac{\Gamma(\frac{\beta}{2})}{\Gamma(\frac{\beta}{2} + 1)} \frac{\gamma^{\frac{\beta}{2}}}{\gamma^{\frac{\beta}{2} + 1}} d\gamma_{th} \]

\[ P_{ST} = \int_{\gamma_{th}}^\infty e^{-\lambda_b \gamma} \left( \frac{(1-2)^2}{(1-2)^2 + \beta} \right) \frac{\Gamma(\frac{\beta}{2})}{\Gamma(\frac{\beta}{2} + 1)} \frac{\gamma^{\frac{\beta}{2}}}{\gamma^{\frac{\beta}{2} + 1}} d\gamma_{th} \]

where \( \gamma_{th} \) is the threshold SNR. This shows that there exists an optimal power allocation \( \alpha \) to achieve the maximal \( C_{ST} \) for a given cache user ratio \( \beta \).

**File Access Protocol**

- **Self-offloading:** Cache-enabled user \( u_0 \) requests content from \( M \) which can be served by their local storage.
- **Secure-transmission:** Cache-enabled user \( u_0 \) requests content from \( F/M \) which is served by the nearest BS in secure-transmission.
- **Normal-transmission:** Cache-untenabled user \( u_0 \) requests content from \( F \) which is served by the nearest BS in normal-transmission.

\[ t_i = \sqrt{\beta e X_i} \]

**Caching**

- Improve signal strength
- Cancel received interference

**Physical Layer Solutions**

- Artificial noise
- Cooperative relays

**Questions**

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

**System Model**

**Network and Caching Model**

- A cache-enabled 3-tier HetNet: BSs \( \Phi_b \), users \( \Phi_u \) and Eves \( \Phi_e \).
- A database: \( N \) files with equal length \( F = \{ f_1, f_2, \ldots, f_N \} \).
- Request probability: \( \nu_j \), Zipf distribution.
- BSs can access all the files in \( F \) without counting costs.
- Only \( \alpha \) part of users have cached the files \( M = \{ f_1, f_2, \ldots, f_M \} \) from \( F \).
- Cache hit ratio \( \delta = \sum_{i=1}^M \nu_i \).

\[ \lambda_b e^{-\lambda_b \gamma} \left( \frac{(1-2)^2}{(1-2)^2 + \beta} \right) \frac{\Gamma(\frac{\beta}{2})}{\Gamma(\frac{\beta}{2} + 1)} \frac{\gamma^{\frac{\beta}{2}}}{\gamma^{\frac{\beta}{2} + 1}} d\gamma_{th} \]

**Transmission Scheme Analysis**

**Normal Transmission (NT)**

- Consider a non-colluding wiretap scenario where each Eve individually overhears the data transmission from \( u_0 \) to \( b_j \).
- The received SINR of \( u_0 \) and an arbitrary Eve \( e_j \) can be written as \( (\nu_{u_0}, \nu_{e_j}) \).

\[ \text{SNIR}_i = \frac{P | h_{b_j} |^2 d^{\beta}}{\sum_{k \in \Phi_b \setminus \{b_j\}} | h_{k} |^2 d^{\beta} + \sigma^2} \]

**Secure Transmission (ST)**

- Since the pre-cached signal \( x_{u_0} \) is known perfectly at \( u_0 \). And assume that the perfect channel state information is fully available at cache-enabled users. The received SINR of \( u_0 \) is

\[ \text{SNIR}_i = \frac{\theta P | h_{b_j} |^2 d^{\beta}}{\sum_{k \in \Phi_b \setminus \{b_j\}} | h_{k} |^2 d^{\beta} + \sum_{k \in \Phi_e} | h_{k} |^2 d^{\beta} + \sigma^2} \]

The (1-\( \theta \)) part of interference from \( \Phi_u \) can be cancelled.

The transmitted signal \( x_{u_0} \) 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 written as

\[ \text{SNIR}_{e_j} = \frac{\theta P | h_{b_j} |^2 d^{\beta}}{(1-\theta) P | h_{b_j} |^2 d^{\beta} + \sum_{k \in \Phi_b \setminus \{b_j\}} | h_{k} |^2 d^{\beta} + \sum_{k \in \Phi_e} | h_{k} |^2 d^{\beta} + \sigma^2} \]

It has the form of \( \frac{\theta x}{x + (1-\theta) \sigma} \)