Physical Layer Security for Two-Way Untrusted Relaying with Friendly Jammers

Rongqing Zhang and Lingyang Song
School of Electrical Engineering and Computer Science
Peking University, China
Aug 24, 2010

Outline

- Introduction
- System Model
- Analysis of Two-Way Untrusted Relaying with Friendly Jammers
- Simulation Results
- Conclusion

Outline

- **Introduction**
- System Model
- Analysis of Two-Way Untrusted Relaying with Friendly Jammers
- Simulation Results
- Conclusion

Introduction

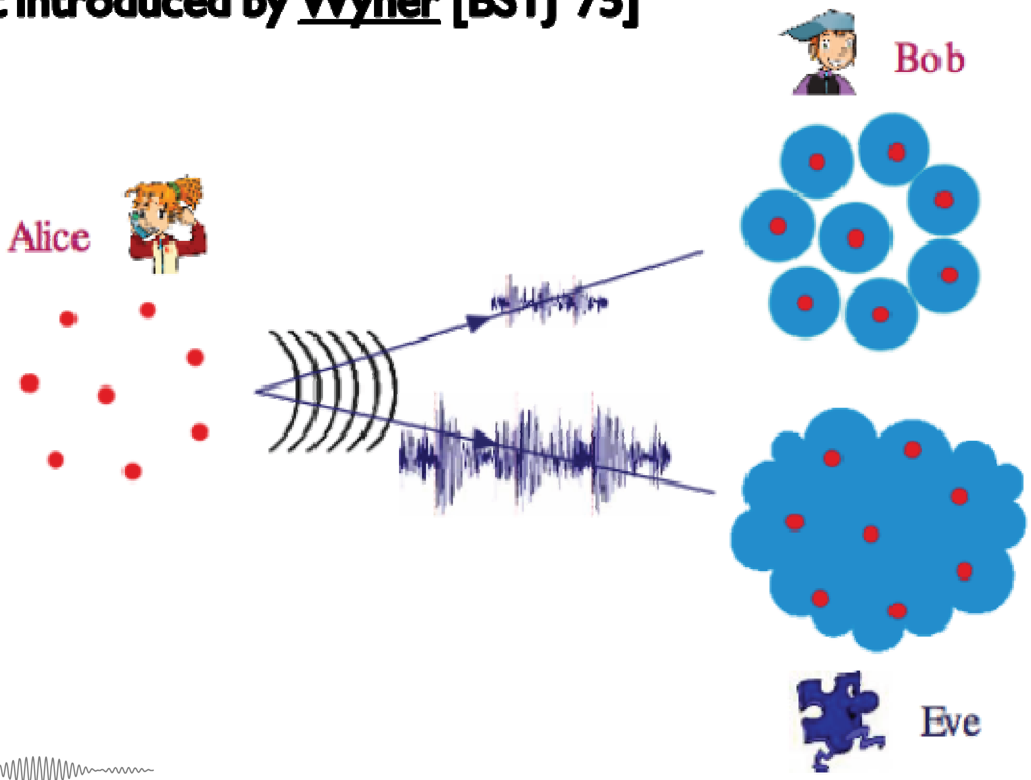
◆ **Physical Layer Security**

- **Wire-tap Channel**
- **Secrecy Capacity (Secrecy Rate)**
- **Approaches to Improve Secrecy Capacity**

Introduction

◆ Physical Layer Security

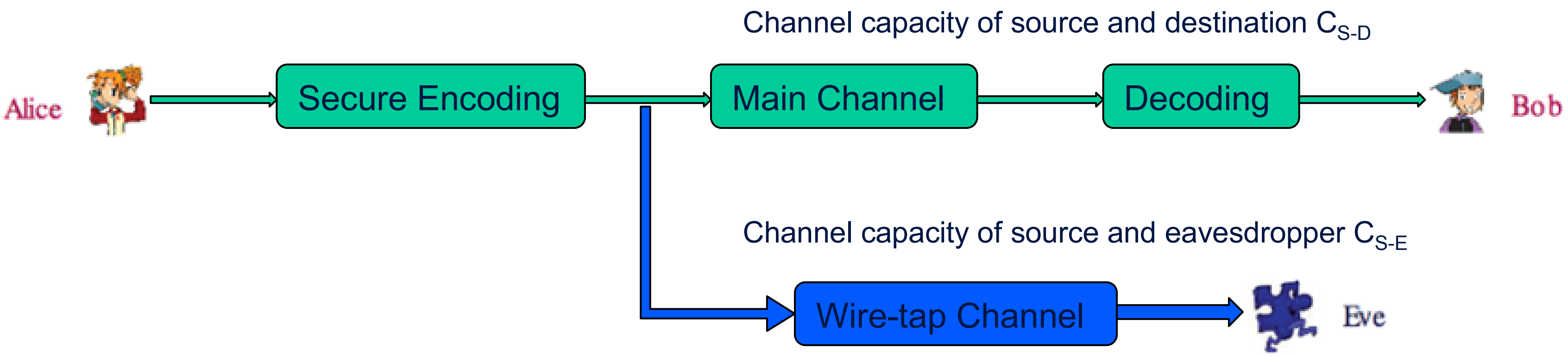
- Wire-tap Channel
  - First introduced by Wyner [BSTJ'75]



Introduction

◆ Physical Layer Security

● Wire-tap Channel



Channel capacity of source and destination $C_{S\text{-}D}$

Alice

Secure Encoding

Main Channel

Decoding

Bob

Channel capacity of source and eavesdropper $C_{S\text{-}E}$

Wire-tap Channel

Eve

- The eavesdropper knows well the encoding scheme at the source and the decoding scheme at the destination.
- However, it is still available that there exists a positive rate of reliable communication between Alice and Bob if the wire-tap channel is worse than the main channel, for the eavesdropper can be kept ignorant solely by the greater noise present in its received signal.

Introduction

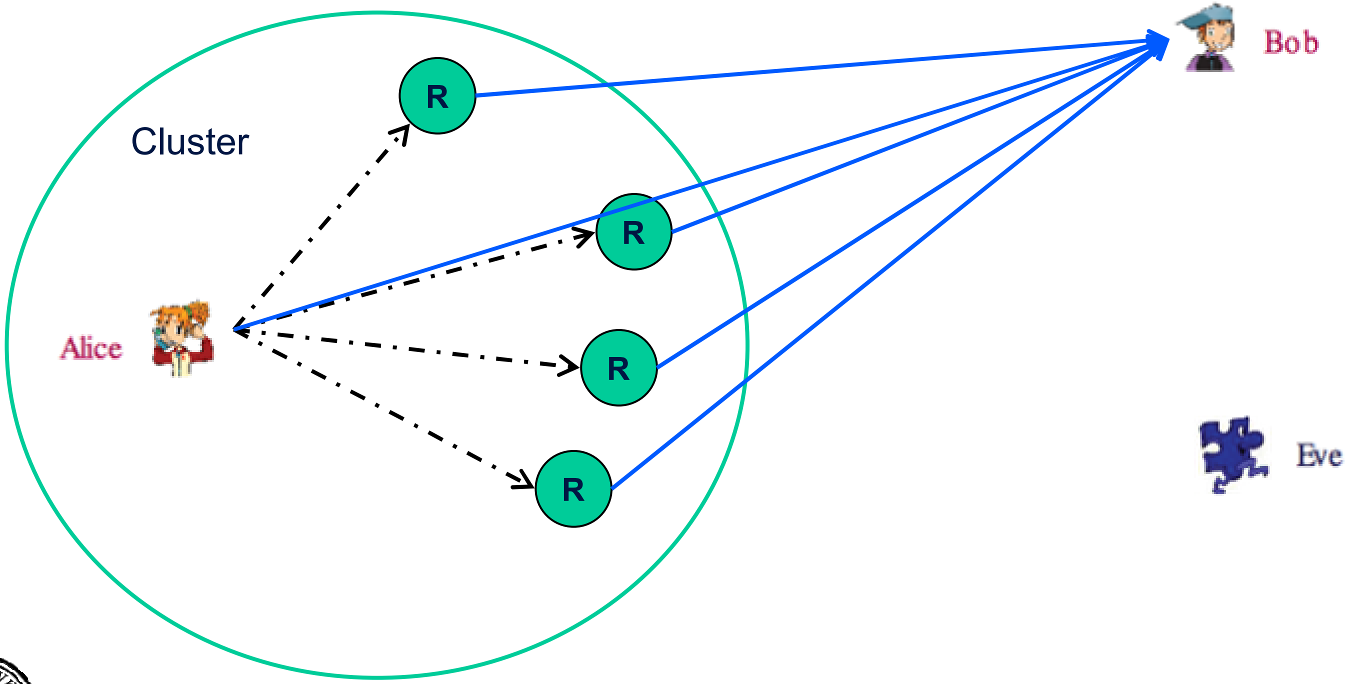
◆ Physical Layer Security

- Secrecy Capacity
  - The *secrecy capacity* is define as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers.
  - The *secrecy rate* is an achievable rate that is smaller than the secrecy capacity.
  - Note that if the source-eavesdropper channel is less noisy than the source-destination channel, the perfect secrecy capacity will be zero. Thus, Some recent work has been proposed to overcome this limitation using relay cooperation.

Introduction

◆ Physical Layer Security

- Approaches to Improve Secrecy Capacity
  - Cooperative Relaying

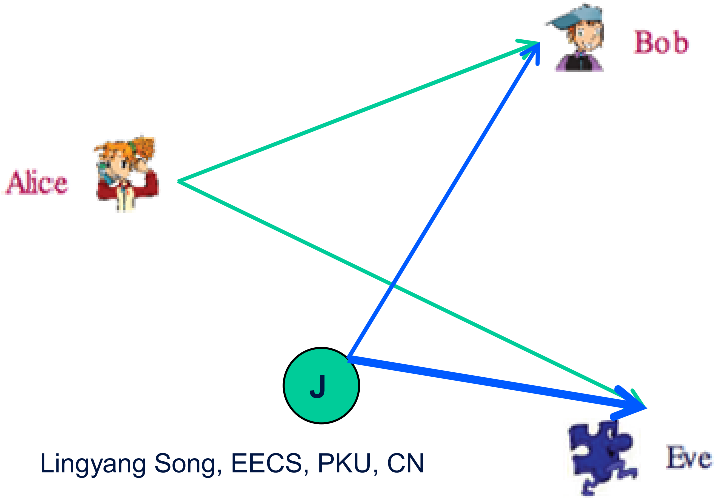


Introduction

◆ Physical Layer Security

- Approaches to Improve Secrecy Capacity
  - Cooperative Jamming

➢ The jamming signal can be as interference to both destination and eavesdropper, which makes both the wire-tap channel and the main channel getting worse. But if the interference effect on Bob is less than that on Eve, the secrecy rate will be improved.

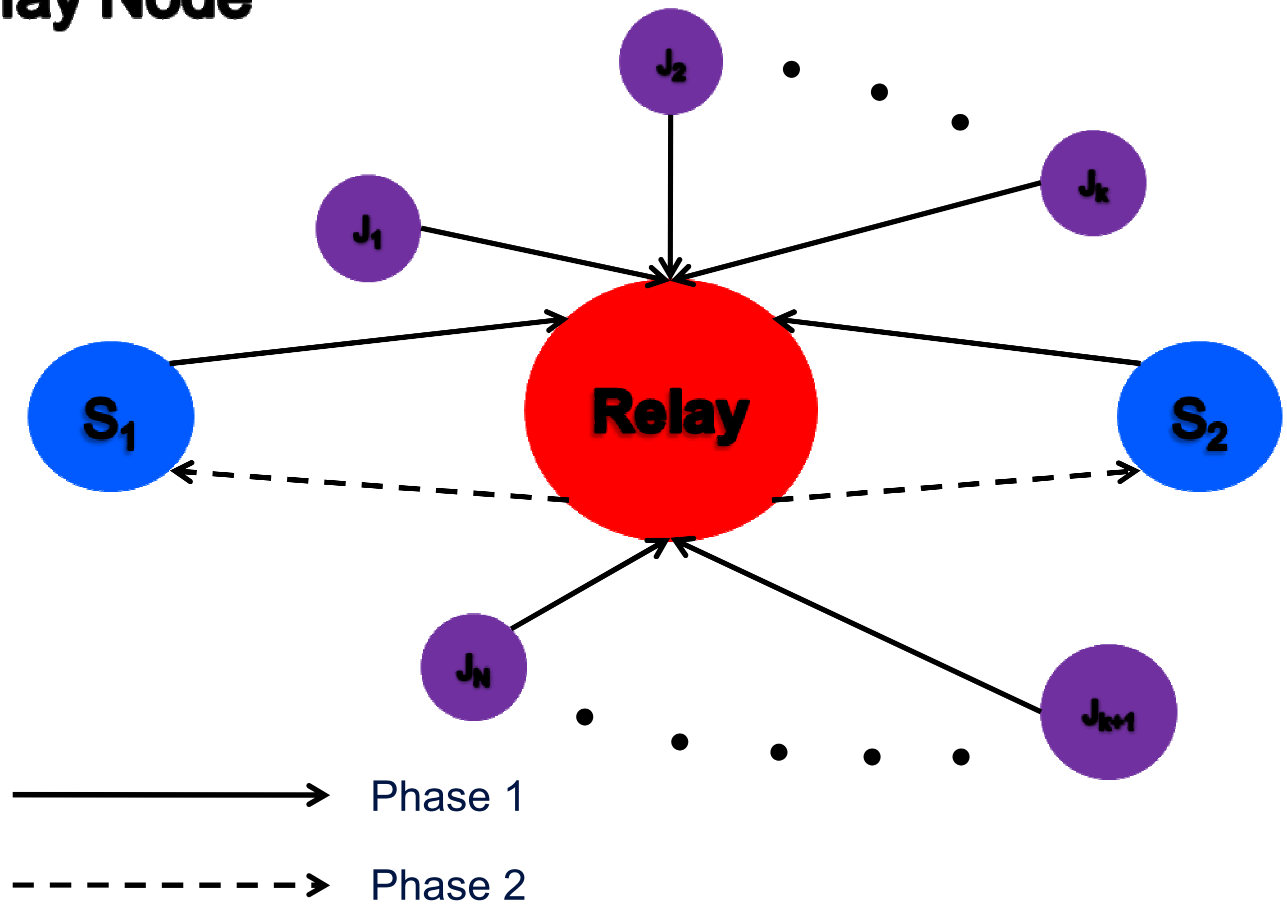


Outline

- Introduction
- **System Model**
- Analysis of Two-Way Untrusted Relaying with Friendly Jammers
- Simulation Results
- Conclusion

System Model

- **Two-Way Relay Communication through an Untrusted Relay Node**



System Model

- **Key Assumptions:**
  - All the nodes are equipped with only a single omni-directional antenna and operating in a half-duplex way.
  - No direct communication link between the two source nodes.
  - The untrusted relay node, working in Amplify-and-Forward protocol, acts both as an essential relay and a malicious eavesdropper who also wants to eavesdrop the transmitted data coming from the sources.
  - The source nodes have perfect knowledge of the jamming signals transmitted by the friendly jammers, for they have paid for the service.

System Model

- **Secrecy Rate for S_1 and S_2:**

$$C_1^s = \frac{W}{2}\left[\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2 + K_1 + \sum_i \frac{\sigma^2 g_{J_i,R}}{p_r g_{S_2,R}} p_i^J}\right) - \log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2 + p_2 g_{S_2,R} + \sum_i g_{J_i,R} p_i^J}\right)\right]^+$$

$$C_2^s = \frac{W}{2}\left[\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2 + K_2 + \sum_i \frac{\sigma^2 g_{J_i,R}}{p_r g_{S_1,R}} p_i^J}\right) - \log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2 + p_1 g_{S_1,R} + \sum_i g_{J_i,R} p_i^J}\right)\right]^+$$

System Model

- $(x)^+$ represents max{x, 0} .
- p_1, p_2, p_i^J denote the transmitting power of the sources S_1, S_2, and the friendly jammer J_i, respectively.
- In addition,

$$K_1 = \frac{\sigma^2\left(p_1 g_{S_1,R} + p_2 g_{S_2,R} + \sigma^2\right)}{p_r g_{S_2,R}} \qquad K_2 = \frac{\sigma^2\left(p_1 g_{S_1,R} + p_2 g_{S_2,R} + \sigma^2\right)}{p_r g_{S_1,R}}$$

Outline

- Introduction
- System Model
- **Analysis of Two-Way Untrusted Relaying with Friendly Jammers**
- Simulation Results
- Conclusion

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ A Special Case without Jammers

◆ Game between Sources and Friendly Jammers

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ A Special Case without Jammers

- Secrecy Rate for S_1 and S_2 in This Special Case:

$$\tilde{C}_1^s = \frac{W}{2}\left[\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+K_1}\right)-\log\left(1+\frac{p_1 g_{S_1,R}}{\sigma^2+p_2 g_{S_2,R}}\right)\right]^+$$

$$\tilde{C}_2^s = \frac{W}{2}\left[\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+K_2}\right)-\log\left(1+\frac{p_2 g_{S_2,R}}{\sigma^2+p_1 g_{S_1,R}}\right)\right]^+$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆A Special Case without Jammers

● Existence of Non-zero Secrecy Rate

- ➢ **We can prove that under the power constraints** $\begin{cases} p_1 \le p_{\max} \\ p_2 \le p_{\max} \\ p_r \le p_{\max} \end{cases}$**, there exists at least one pair of** (p_r, p_1, p_2) **that satisfies**

$$\mathrm{P}\left(\tilde{C}_1^s > 0, \tilde{C}_2^s > 0\right) = \mathrm{P}\left(K_1 < p_2 g_{S_2,R}, K_2 < p_1 g_{S_1,R}\right)$$

$$= \mathrm{P}\left(p_r > \max\left\{\frac{K}{p_2 g^2_{S_2,R}}, \frac{K}{p_1 g^2_{S_1,R}}\right\}\right) > 0$$

$$K = (p_1 g_{S_1,R} + p_2 g_{S_2,R} + \sigma^2)\sigma^2$$

which actually indicates that a non-zero secrecy rate in the two-way relay channel is indeed available.

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆A Special Case without Jammers

- **Optimal Transmitting Power Allocation to Maximize the Secrecy Rate**
  - **We formulate the problem subject to the individual secrecy rate constraints and power constraints as**

$$\max \tilde{C}^s = \max \sum_{k=1}^{2} \tilde{C}_k^s$$

$$\text{s.t.} \begin{cases} \tilde{C}_1^s > 0, \tilde{C}_2^s > 0 \\ p_1 \le p_{\max},\ p_2 \le p_{\max},\ p_r \le p_{\max} \end{cases}$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ A Special Case without Jammers

- Optimal Transmitting Power Allocation to Maximize the Secrecy Rate
  - ➢ After further calculation, we can get the following results:
  - When maximizing the secrecy rate, the relay should always transmit with the maximum power, i.e., $p_{r\_opt} = p_{\max}$
  - We define

$$\tilde{F}\left(p_r, p_1, p_2\right) \triangleq \frac{\left(1+\dfrac{p_1 g_{S_1,R}}{\sigma^2+K_1}\right)\left(1+\dfrac{p_2 g_{S_2,R}}{\sigma^2+K_2}\right)}{\left(1+\dfrac{p_1 g_{S_1,R}}{\sigma^2+p_2 g_{S_2,R}}\right)\left(1+\dfrac{p_2 g_{S_2,R}}{\sigma^2+p_1 g_{S_1,R}}\right)}$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆A Special Case without Jammers

- **Optimal Transmitting Power Allocation to Maximize the Secrecy Rate**
  - **If** $g_{S_1,R} > g_{S_2,R}$**, we have that** $$\begin{cases} p_{1\_opt} = \begin{cases} p_1^*, & if\ p_1^* \in (0, p_{\max}) \\ p_{\max}, & otherwise \end{cases} \\ p_{2\_opt} = p_{\max} \end{cases}$$ $$where\ p_1^*\ is\ the\ solution\ of\ \frac{\partial \tilde{F}(p_{\max}, p_1, p_{\max})}{\partial p_1} = 0.$$
  - **If** $g_{S_1,R} < g_{S_2,R}$**, we have that** $$\begin{cases} p_{1\_opt} = p_{\max} \\ p_{2\_opt} = \begin{cases} p_2^*, & if\ p_2^* \in (0, p_{\max}) \\ p_{\max}, & otherwise \end{cases} \end{cases}$$ $$where\ p_2^*\ is\ the\ solution\ of\ \frac{\partial \tilde{F}(p_{\max}, p_{\max}, p_2)}{\partial p_2} = 0.$$
  - **If** $g_{S_1,R} = g_{S_2,R}$**, we have that** $$\begin{cases} p_{1\_opt} = p_{\max} \\ p_{2\_opt} = p_{\max} \end{cases}$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

- Stackelberg type of game between Sources and Jammers
  - Here we consider the two sources as two buyers who want to optimize their secrecy rates, while the cost paid for the "service", i.e., jamming power p_i^J, $i \in \mathrm{N}$, should also be taken into consideration.
  - Also we employ the pricing scheme to the payment of the two sources. For simplicity, here we mainly consider linear pricing scheme.

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

- Source Side Game
  - For the source side, we define the utility function as

$$U_s = a\left(C_1^s + C_2^s\right) - M$$

where a is a positive constant representing the gain per unit rate, and M is the cost to pay for the friendly jammers.

  - Here we have $M = \sum m_i p_i^J$, where m_i is the price per unit power paid for the friendly jammer i by the sources.

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

- **Source Side Game**
  - The source side game can be expressed as

$$\max U_s = \max\left(a\left(C_1^s + C_2^s\right) - M\right)$$

$$\text{s.t.}\begin{cases} C_1^s > 0,\, C_2^s > 0 \\ 0 \le p_i^J \le p_{\max},\, p_r = p_{\max},\, fixed\ p_1, p_2 \end{cases}$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

- Friendly Jammer Side Game
  - For the friendly jammer side, we define the utility function of each friendly jammer as $U_i = m_i \left(p_i^J \right)^{c_i}, i \in \mathrm{N}$

    where $c_i > 1$ is a constant to balance the payment from the sources and the transmission of the jammer itself. With different values of c_i, the jammers have different strategies for asking the price m_i.
  - Here the jamming power p_i^J is also a function of the vector of prices $\left(m_1, m_2, \ldots, m_N \right)$,as the amount of jamming power that the sources will buy also depends on the prices that the friendly jammers ask.

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

● Friendly Jammer Side Game

- The friendly jammer side game can be expressed as

$$\max_{m_i} U_i,\ \ i \in \mathrm{N}$$

- The optimal asking price for jammer i can be given as

$$m_{i\_opt} = m_i^* \left\{ \sigma^2, g_{S_1,R}, g_{S_2,R}, \left\{ g_{J_i,R} \right\} \right\}$$

Analysis of Two-Way Untrusted Relaying with Friendly Jammers

◆ Game between Sources and Friendly Jammers

- Distributed Algorithm
  - From above, we have

$$m_i = I_i(\mathbf{m}) = -\frac{\left(p_{i\_opt}^J\right)}{c_i \dfrac{\partial p_{i\_opt}^J}{\partial m_i}}$$

    where $\mathbf{m} = [m_1, m_2, \ldots, m_N]^T$, $p_{i\_opt}^J$ is a function of $\mathbf{m}$, and $I_i(\mathbf{m})$ is the price update function for friendly jammer i.

  - The distributed algorithm can be expressed in a vector form as

$$\mathbf{m}(t+1) = \mathbf{I}(\mathbf{m}(t))$$

    where $\mathbf{I} = [I_1, I_2, \ldots, I_N]^T$, and the iteration is from time t to time t+1.

Outline

- Introduction
- System Model
- Analysis of Two-Way Untrusted Relaying with Friendly Jammers
- **Simulation Results**
- Conclusion

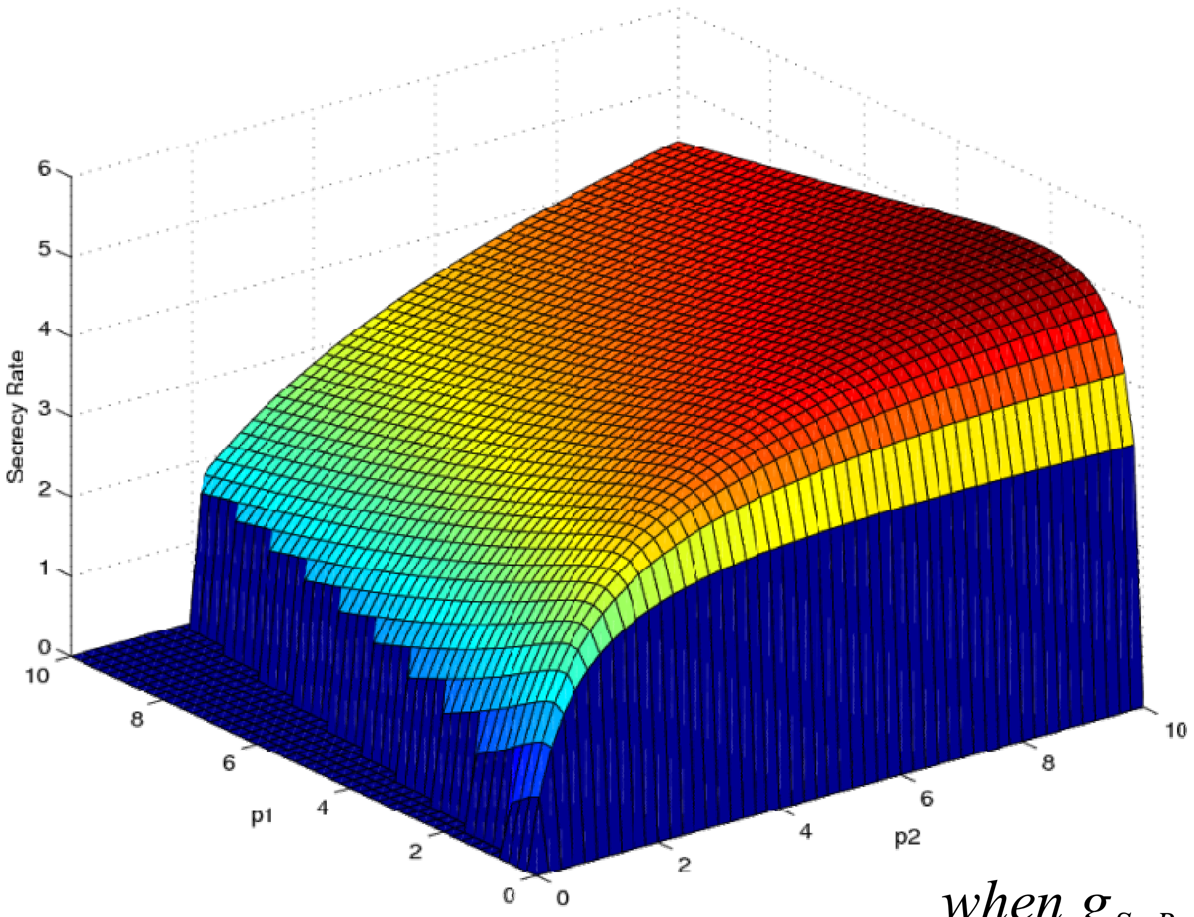
Simulation Results

- Simulation Conditions
  - The sources S_1, S_2, and the malicious relay R are located at the coordinate (-1,0), (1,0), and (0,0), respectively.
  - The maximum power constraint p_{max} is 10.
  - The noise variance is $\sigma^2 = 0.01$.
  - Rayleigh fading channel is assumed, where the channel gain consists of the path loss and the Rayleigh fading coefficient.
  - Here we select a = 1 for the source side utility.

Simulation Results

- **The Special Case without Jammers**

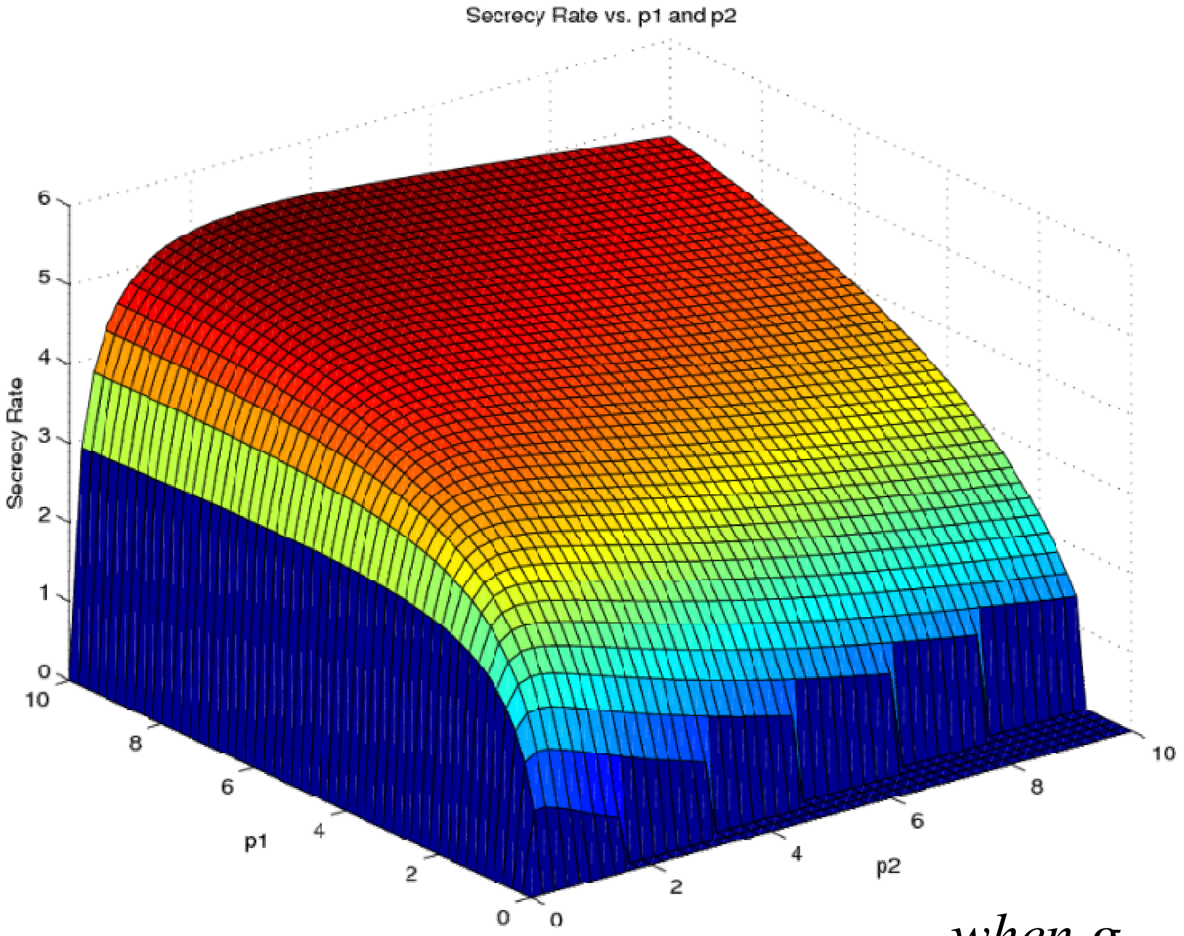
Secrecy Rate vs. p1 and p2



when $g_{S_1,R} > g_{S_2,R}$

Simulation Results

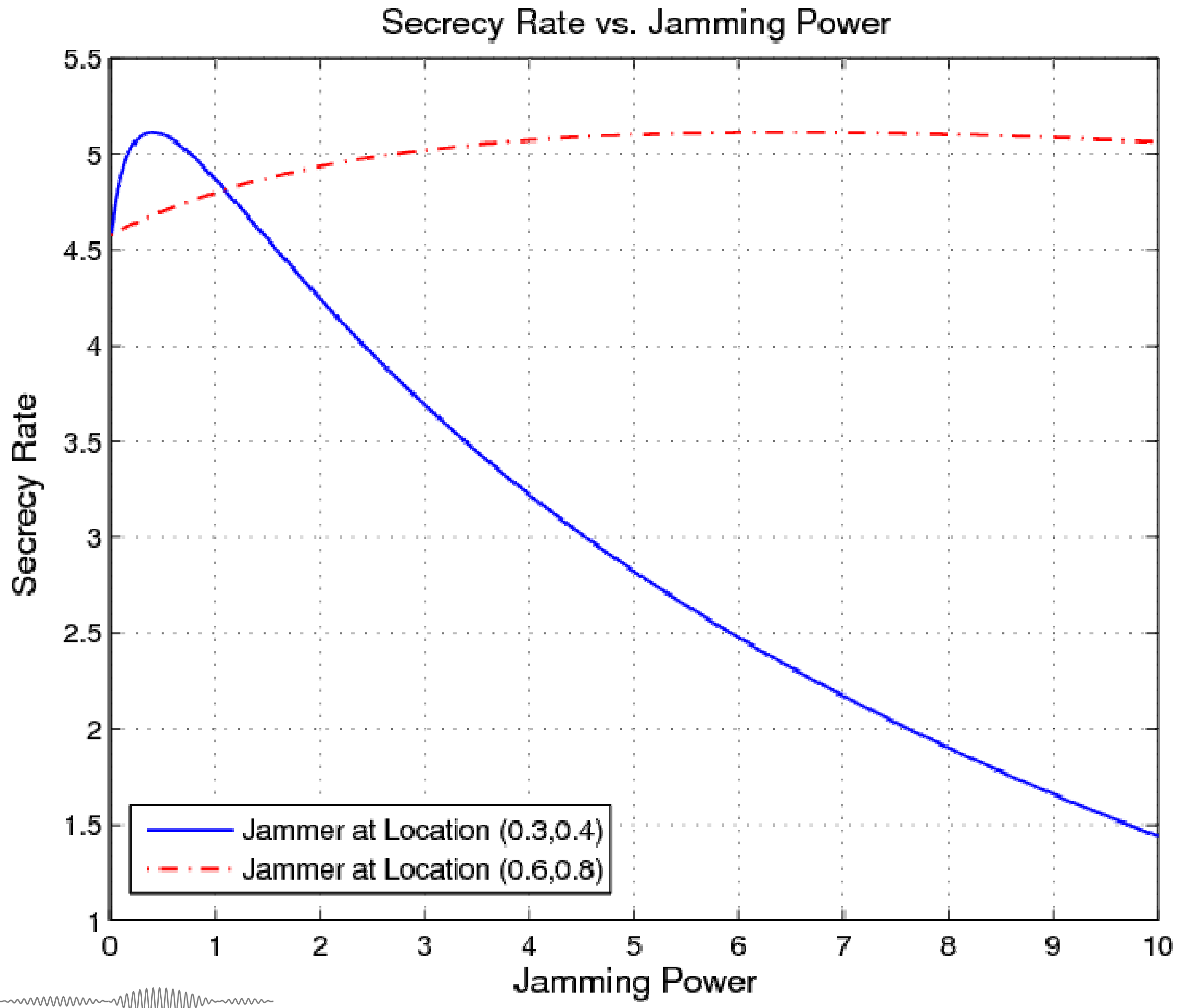
- **The Special Case without Jammers**



$when\ g_{S_1,R} < g_{S_2,R}$

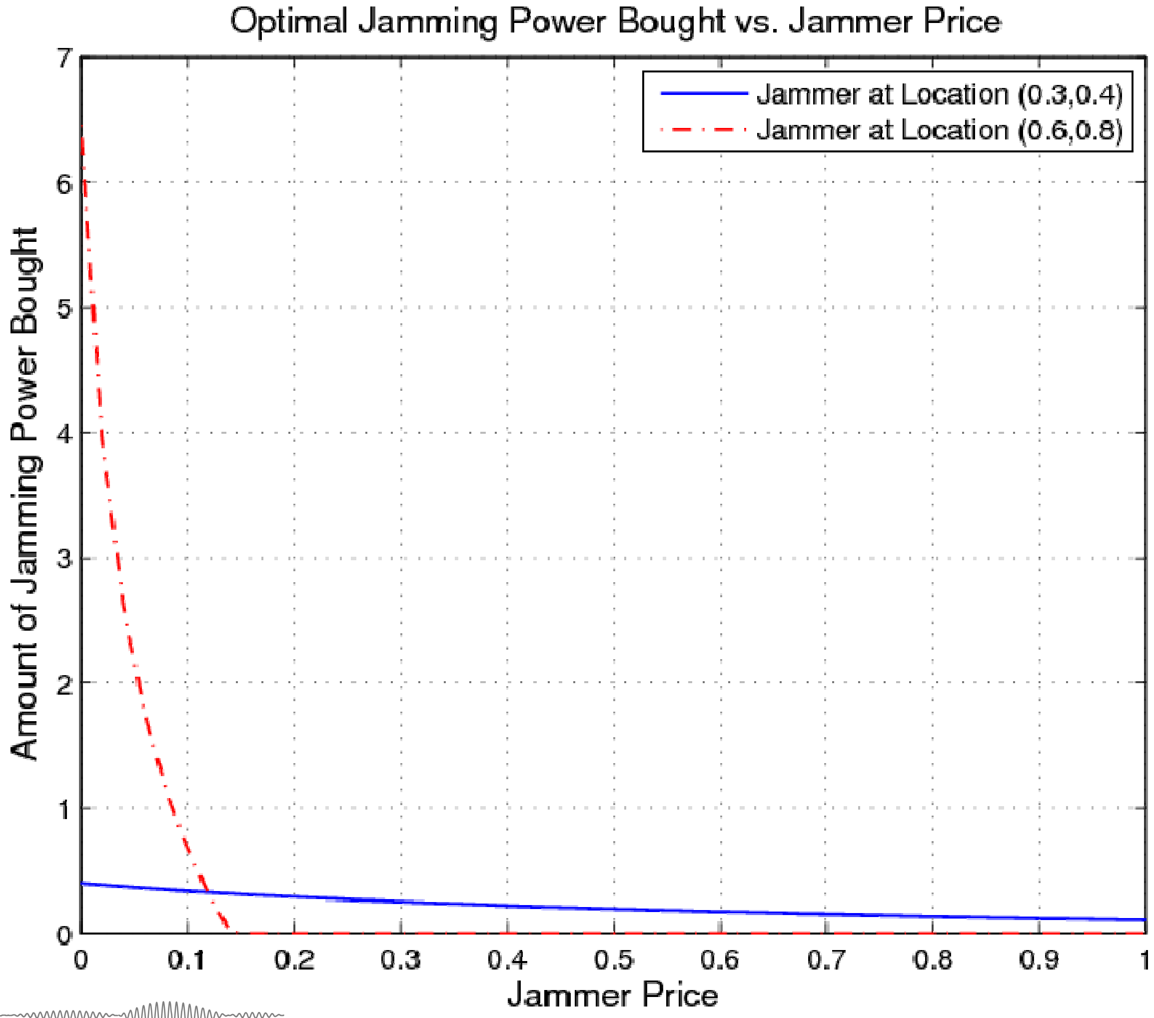
Simulation Results

- **Single-Jammer Case**



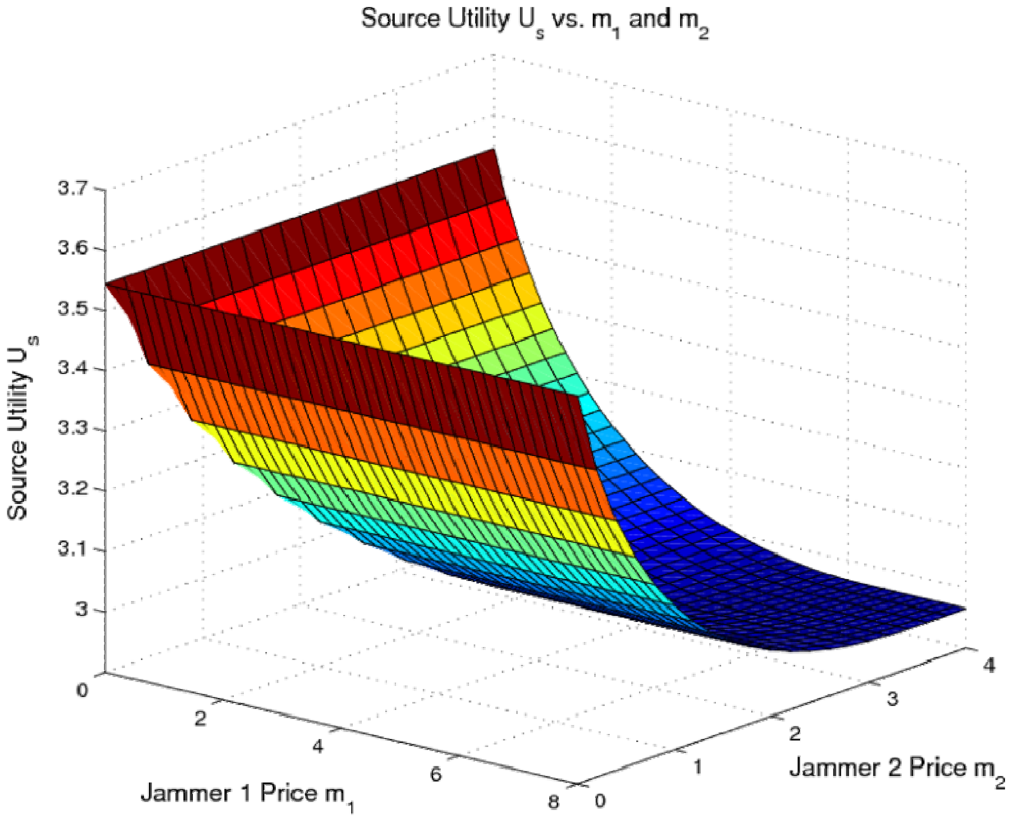
Simulation Results

- **Single-Jammer Case**



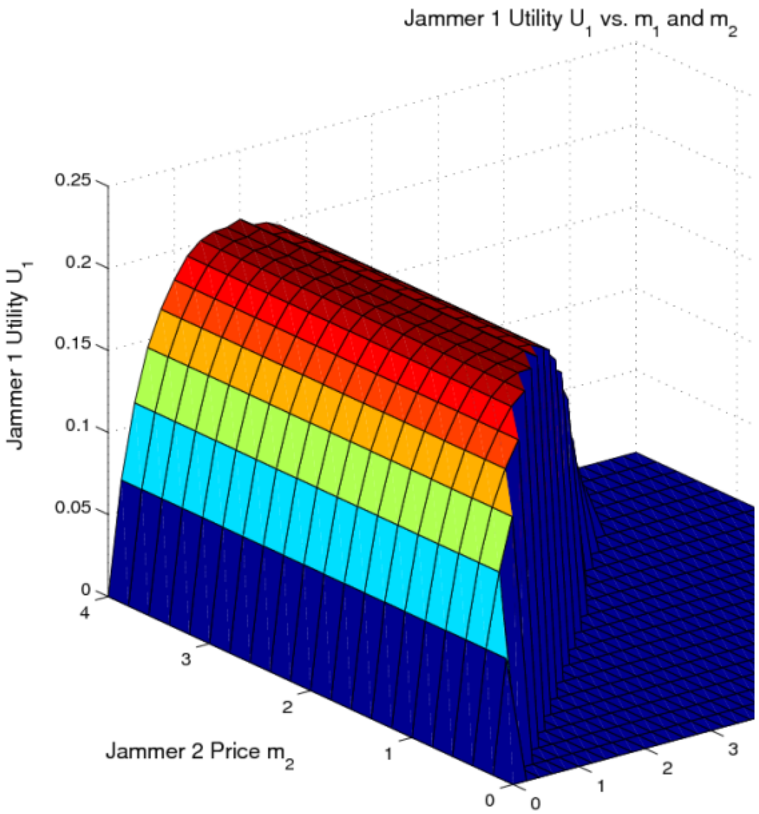
Simulation Results

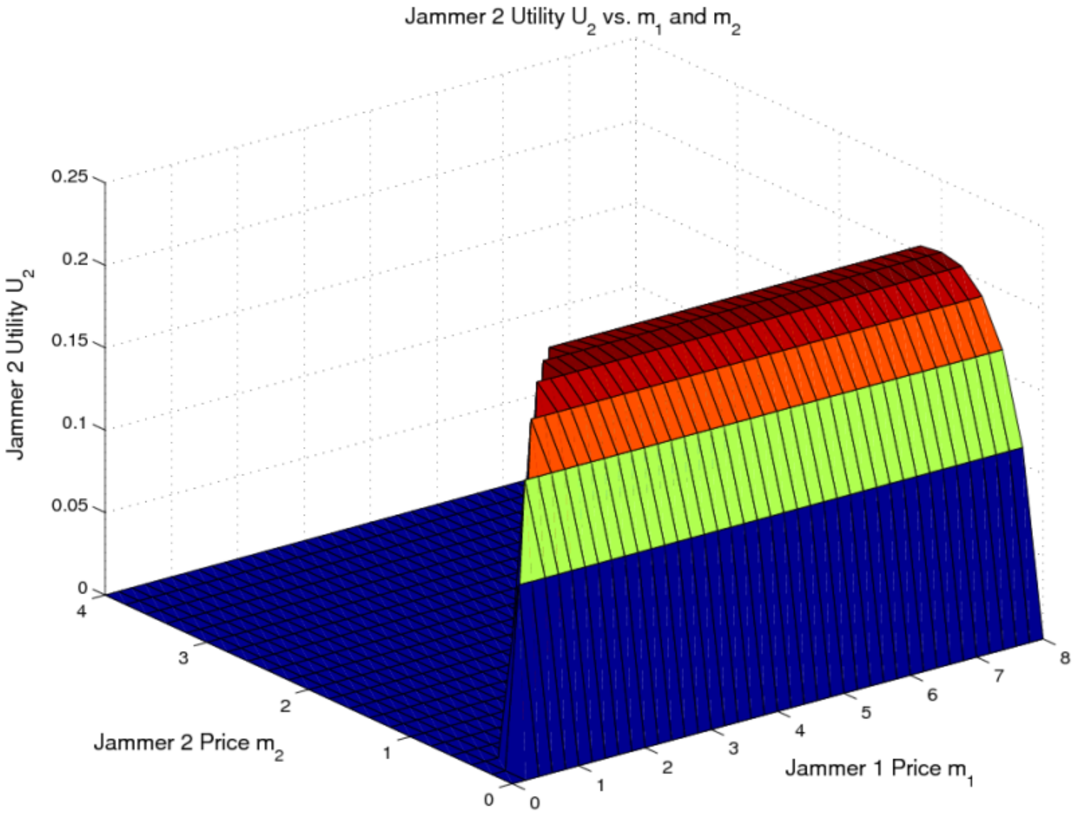
- **Multiple-Jammer Case**
  - We consider two jammers which are located at (0.3,0.4) and (0.5,0.5), respectively. The sources' utility U_S, the first jammer's utility U_1, and the second jammer's utility U_2 as functions of both jammers' prices are shown as follows.



Simulation Results

- **Multiple-Jammer Case**

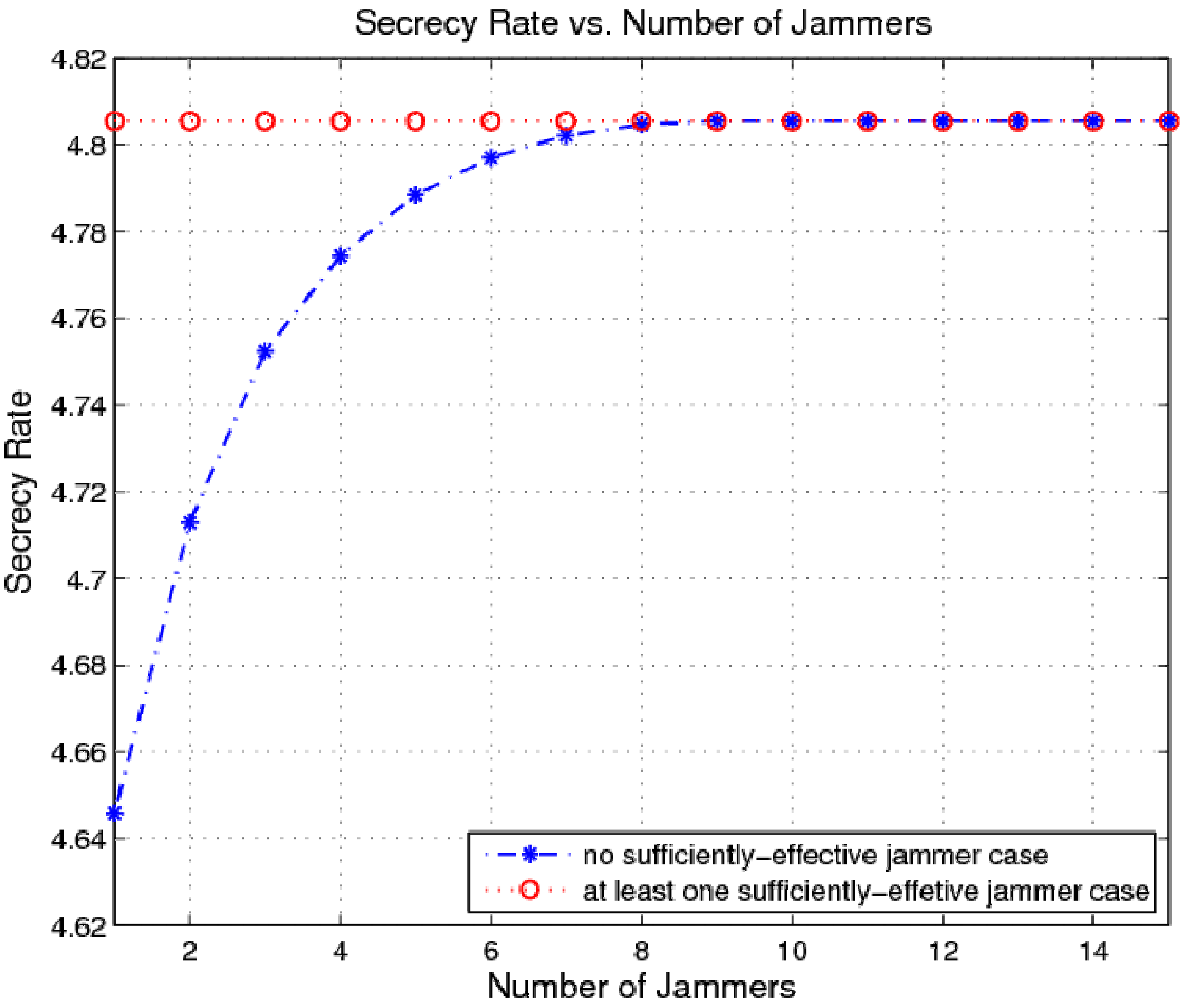




Simulation Results

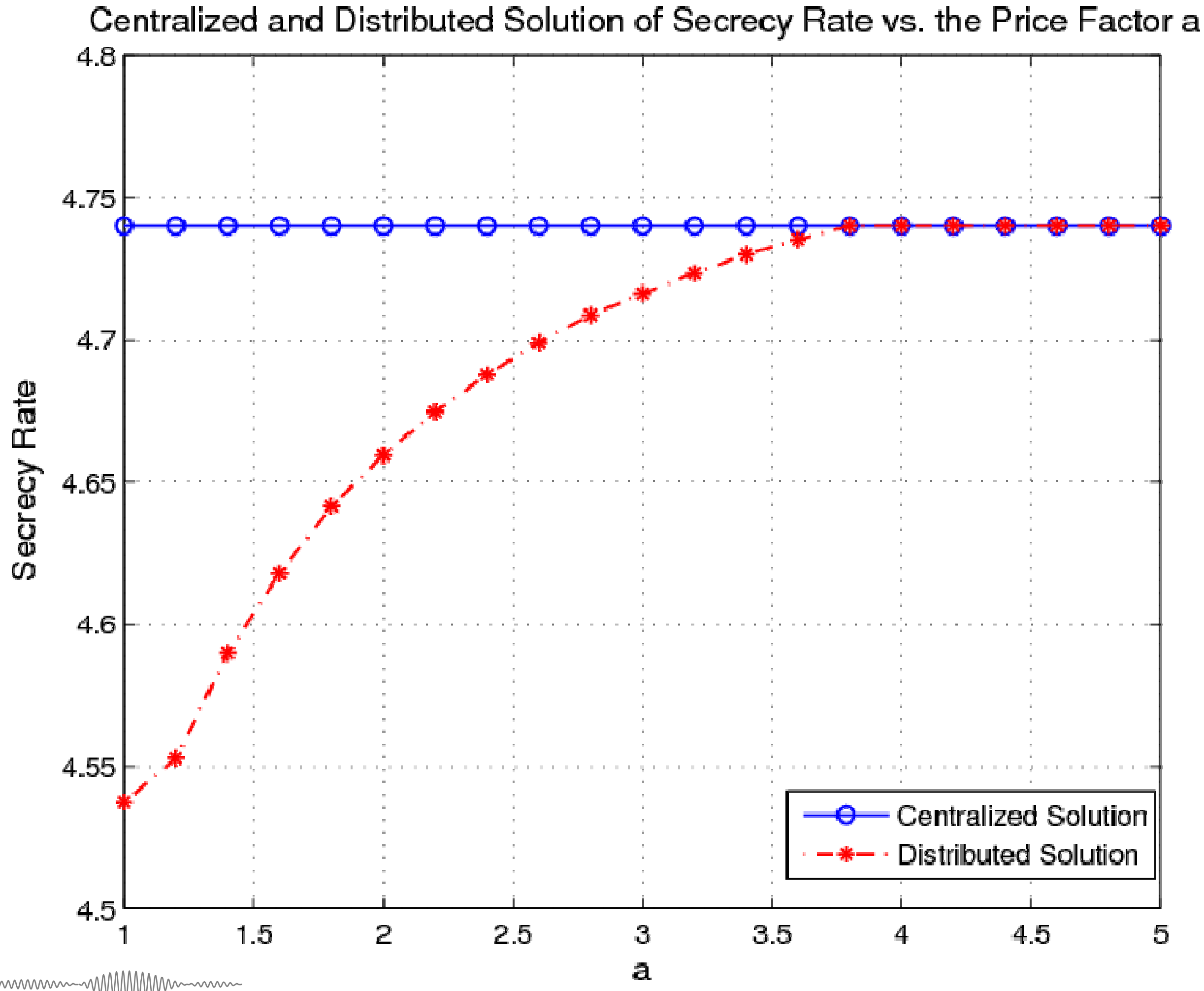
- **Multiple-Jammer Case**

Here we treat jammer i as a sufficiently-effective one if it can p_i^J $p_i^J \in (0, p_{\max}]$ offer a power , ,
making the secrecy rate improved up to the maximal value. In another word, no sufficiently-effective jammer means that the sources could not achieve the maximal secrecy rate with only one jammer's help.



Simulation Results

- **Distributed Solution vs. Centralized Solution of Secrecy Rate**



Outline

- Introduction
- System Model
- Analysis of Two-Way Untrusted Relaying with Friendly Jammers
- Simulation Results
- **Conclusion**

Conclusion

- Reinforce security in physical layer seems to be a very effective approach to further protect wireless networks.
- We therefore investigated the physical layer security for two-way relay communications with untrusted relay and friendly jammers.
- As a simple case, a two-way relay system without jammers is first studied, and an optimal power allocation vector of the sources and relay nodes is found.
- We then investigated the secrecy rate in the presence of friendly jammers. Furthermore, we defined and analyzed a Stackelberg type of game between the sources and the friendly jammers to achieve the optimal secrecy rate in a distributed way.
- From the simulation results, we can get the following:
  - A non-zero secrecy rate for two-way relay channel is indeed available.
  - The secrecy rate can be improved with the help of friendly jammers, and there is an optimal solution of jamming power allocation.
  - There is also a tradeoff for the price a jammer sets, and if the price is too high, the sources will turn to buying from others.
  - For the game, we can see that the distributed algorithm and the centralized scheme have similar performances, especially when the gain factor a is sufficiently large.

References

- Rongqing Zhang, Lingyang Song, Zhu Han, Bingli Jiao, and Merouane Debbah, "Physical layer security for two way relay communications with friendly jammers", accepted by IEEE GLOBECOM'2010.
- Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers", submitted to IEEE Trans. on Wireless Communications.
- Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao, "Improve physical layer security in cooperative wireless network using distributed auction games" submitted to Infocom 2011.
- Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao, "Improve physical layer security in cooperative wireless network using distributed auction games" submitted to IEEE Trans. on Networking.
- Jingchao Chen, Lingyang Song, Zhu Han, and Bingli Jiao, "Joint relay and jammer selection for secure two-way relay networks", in preparation for IEEE Transactions on Information Forensics and Security.

THANKS FOR YOUR ATTENTION!