Resource Allocation for Wireless Physical Layer Security

Lingyang Song[+] and Zhu Han[*]

[+]School of Electronics Engineering and Computer Science,
Peking University, Beijing, China

[*] Department of Electrical and Computer Engineering
University of Houston, Houston, TX, USA

Tutorial Presentation at WCNC 2013, Shanghai, China

Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
- Variety of Applications
- Conclusion

Wireless Networks: Layers

Application (APP)	• Web Browsing, Voice, etc.
Network (NET)	• Routing, Flow Control, etc
Medium Access Control (MAC)	• Scheduling, Access Control, etc.
Physical (PHY)	• Data Transmission

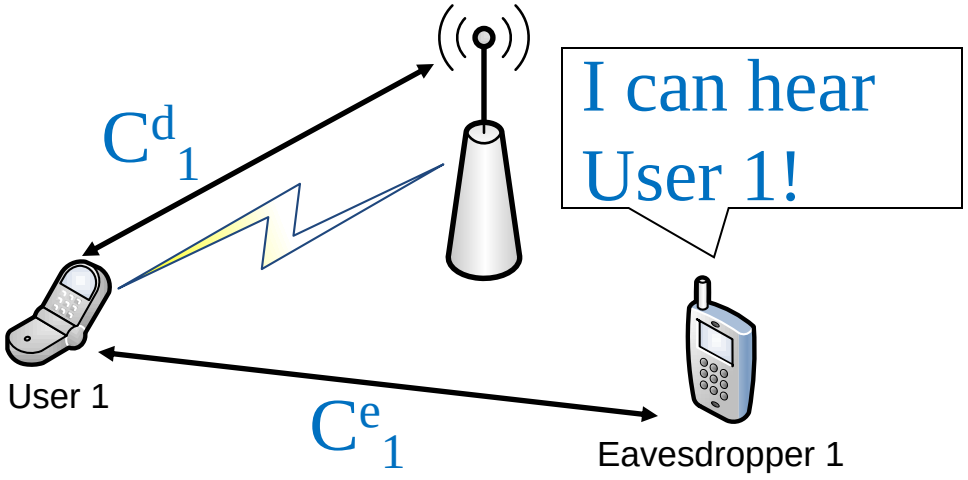
Physical Layer Security

- **Security of Wireless Networks**
  - Traditionally through higher layer techniques such as cryptography
    - *Unsuited and complex to implement in large scale decentralized networks*
    - *Encryption can be complex and difficult without infrastructure (e.g, in ad-hoc networks)*
- **Alternative: Physical Layer Security**
  - Main idea: exploit the wireless channel characteristics to secure wireless transmission in the presence of eavesdroppers
    - *Started with the seminal work of Wyner, 1975*
  - Recently received attention in multi-user wireless networks, such as Dr. Vincent Poor's group

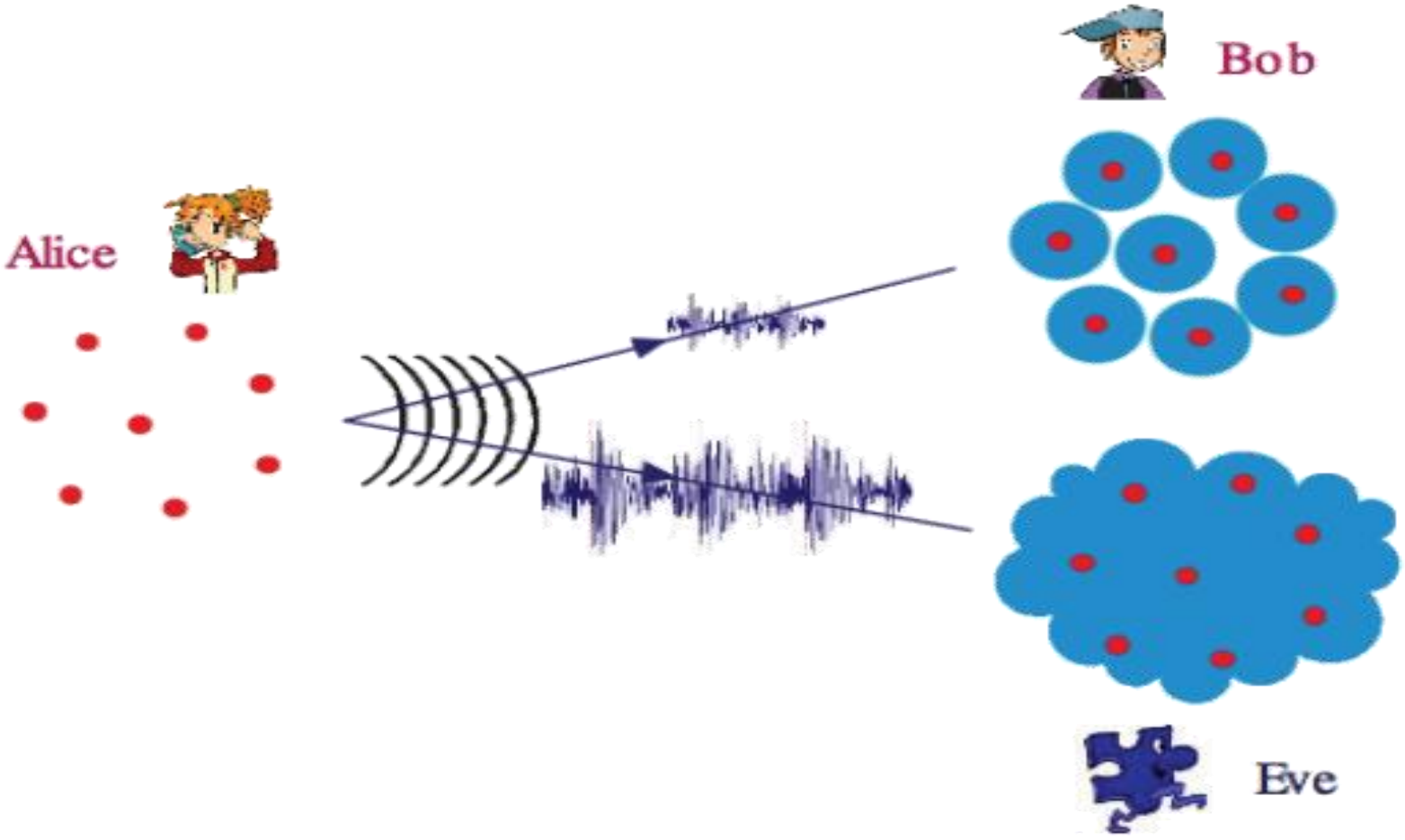
PHY Security: Simple Example

- **Wireless Transmission of a User**
  - Eavesdropped by an eavesdropper
- **Notion of Secrecy Capacity**
  - Maximum rate sent from a wireless node to its destination in the presence of eavesdroppers
- **Secrecy Capacity of User 1 :**

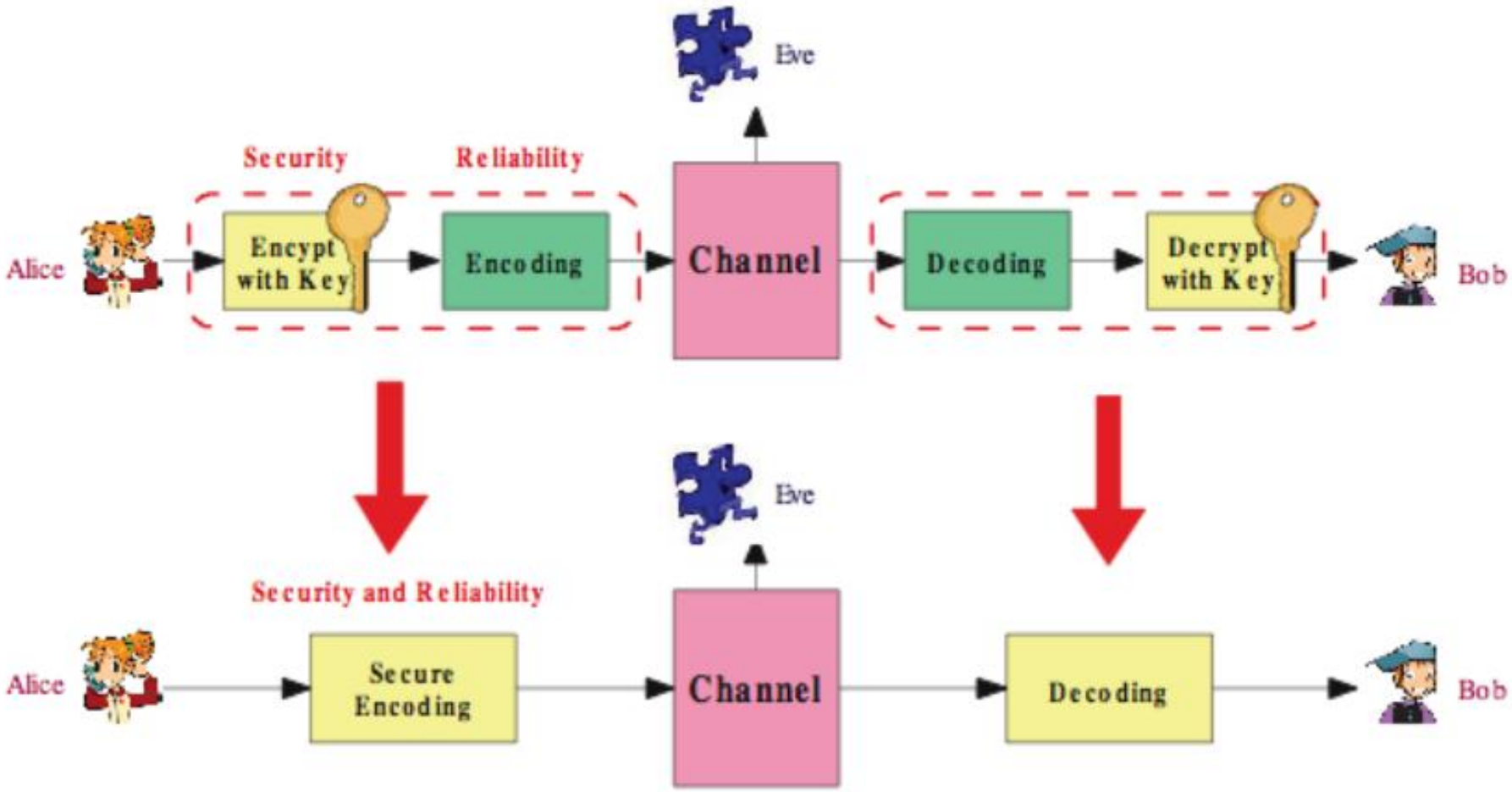
$$C_1 = (C^d_1 - C^e_1)^+$$



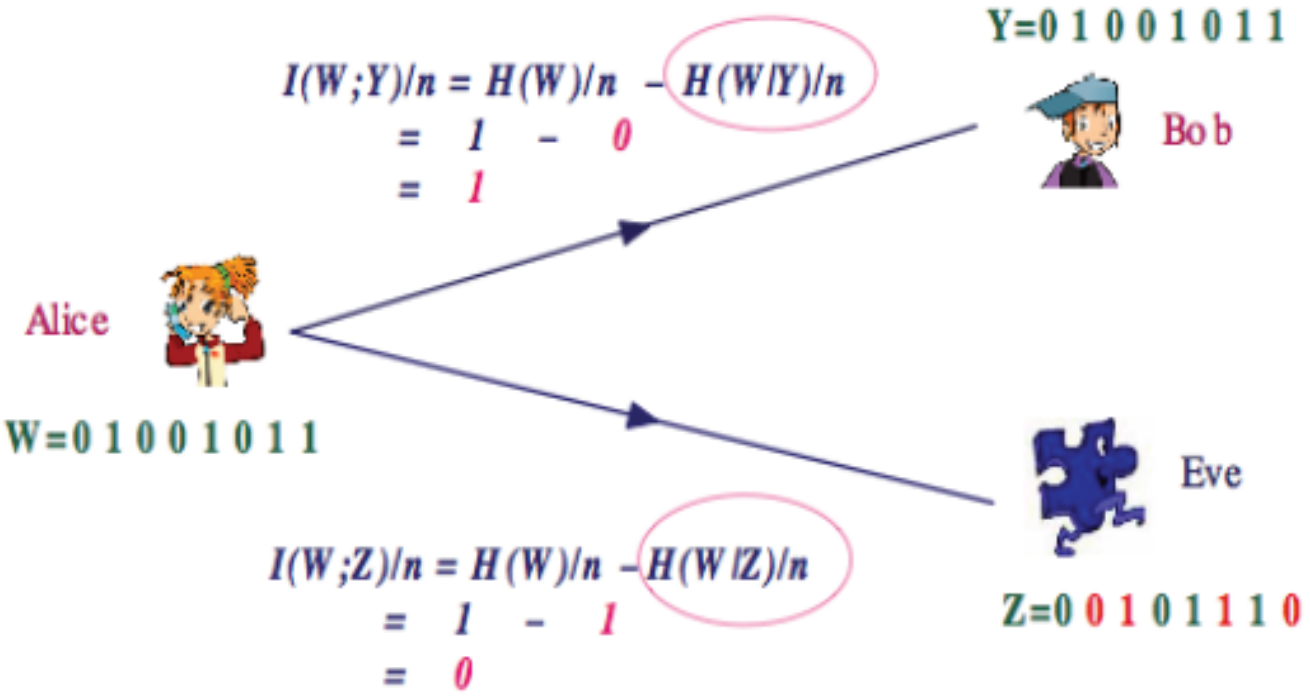
Physical Layer Security Intuition



Physical Layer Security



Quantifying Security: Equivocation



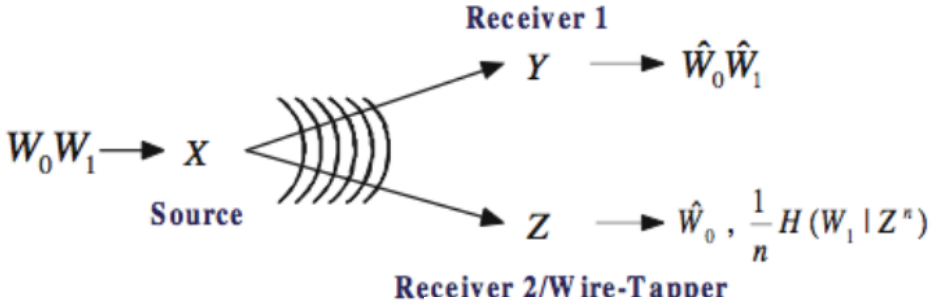
- Capacity-equivocation regions
- Secret capacity regions (rate = equivocation)

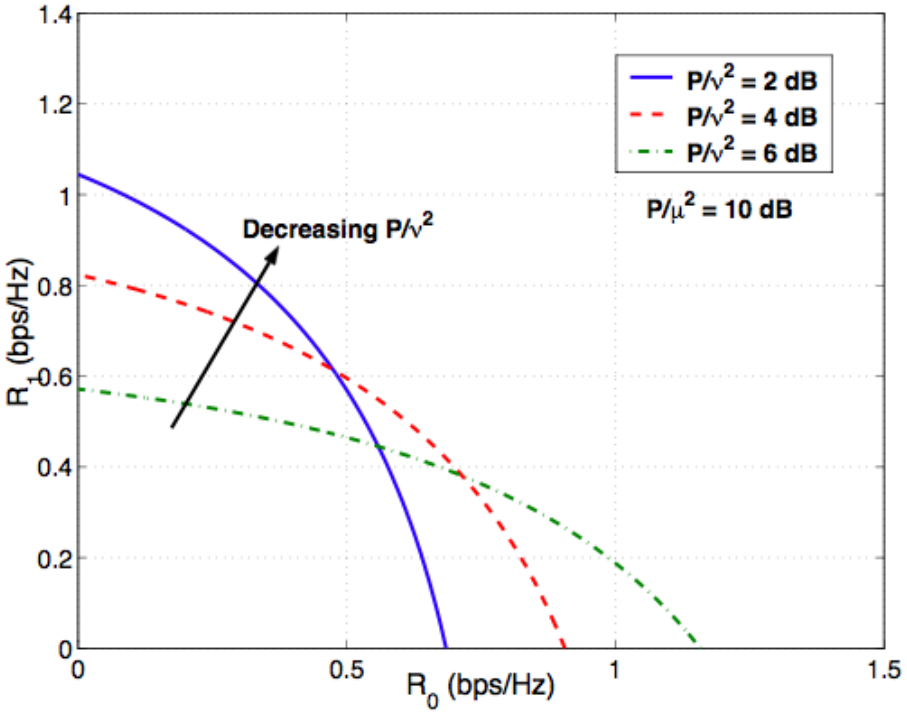
Outline

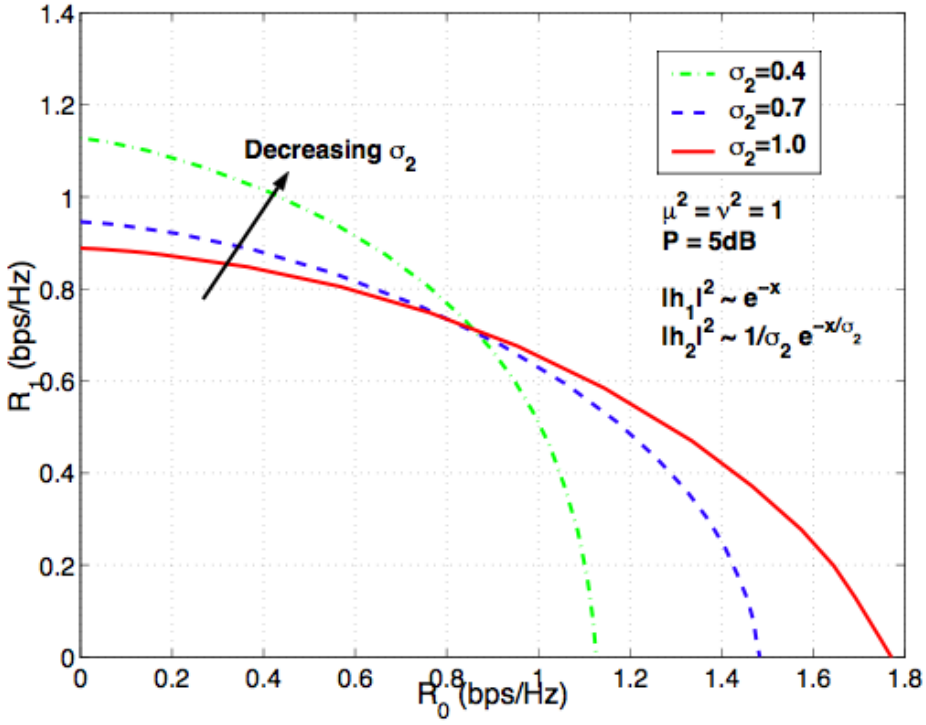
- Overview of Physical Layer Security
- Information Theoretic Fundamentals
  - Broadcast Channel
  - Multiple Access Channel
  - Other Channels
  - Other results and Open Issue
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
- Variety of Applications
- Conclusion

Broadcast Channel

- Liang, Poor & Shamai

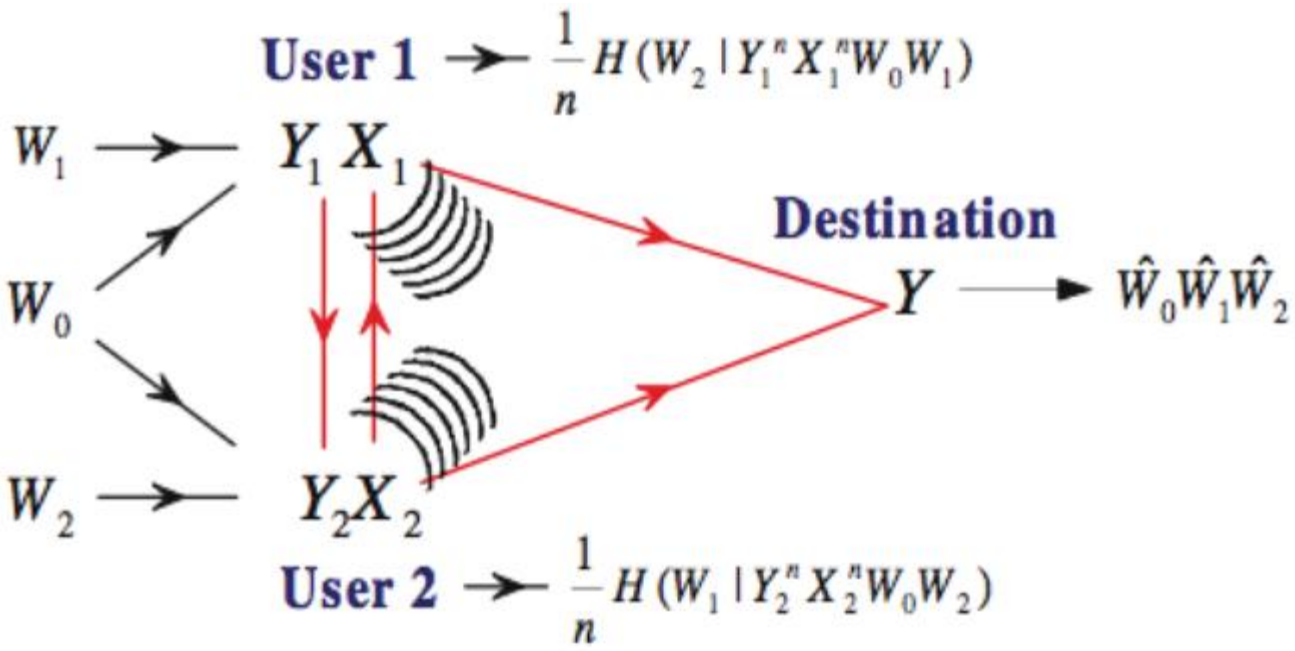


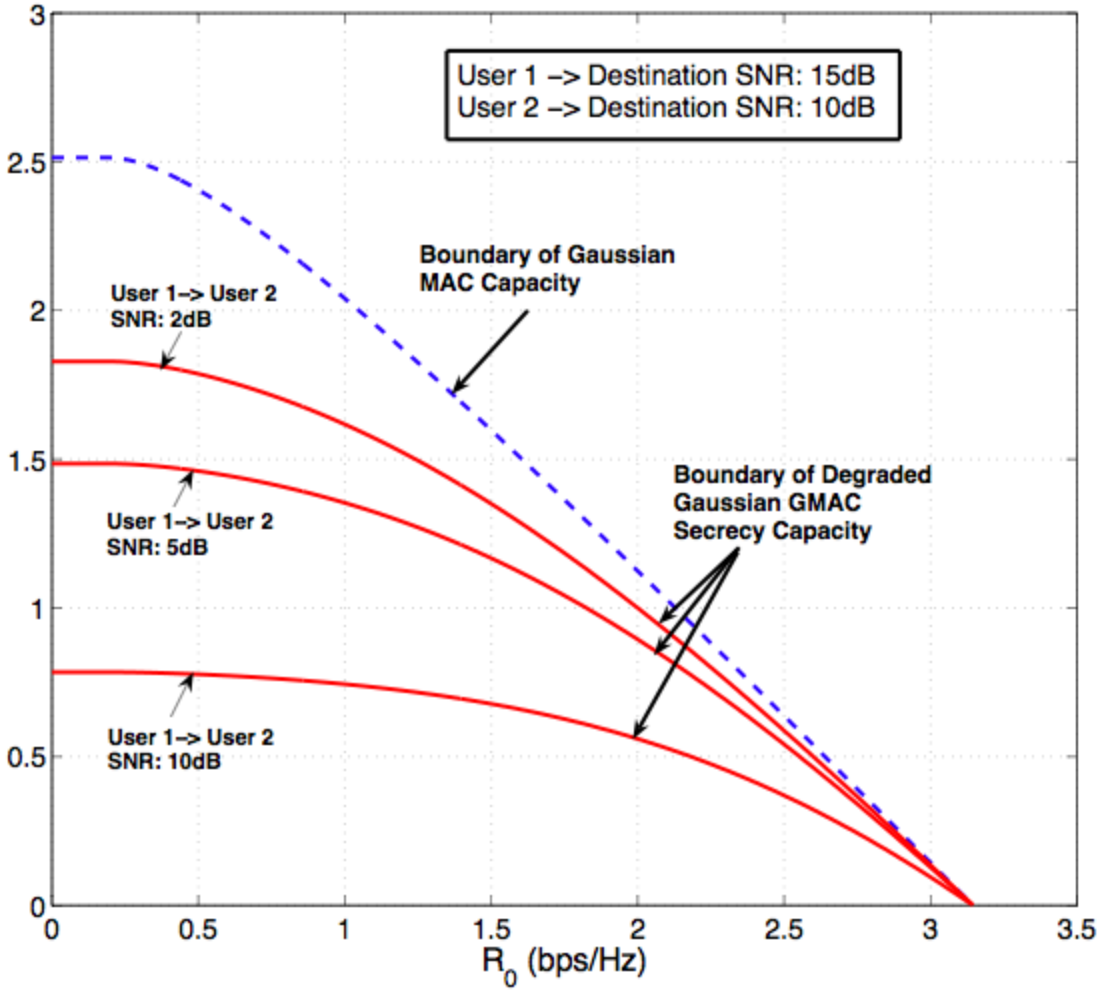




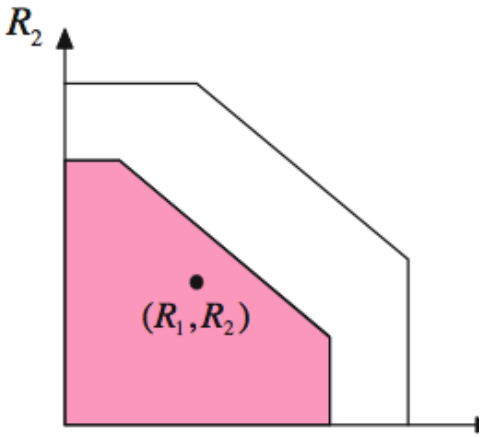
Multiple-Access Channel

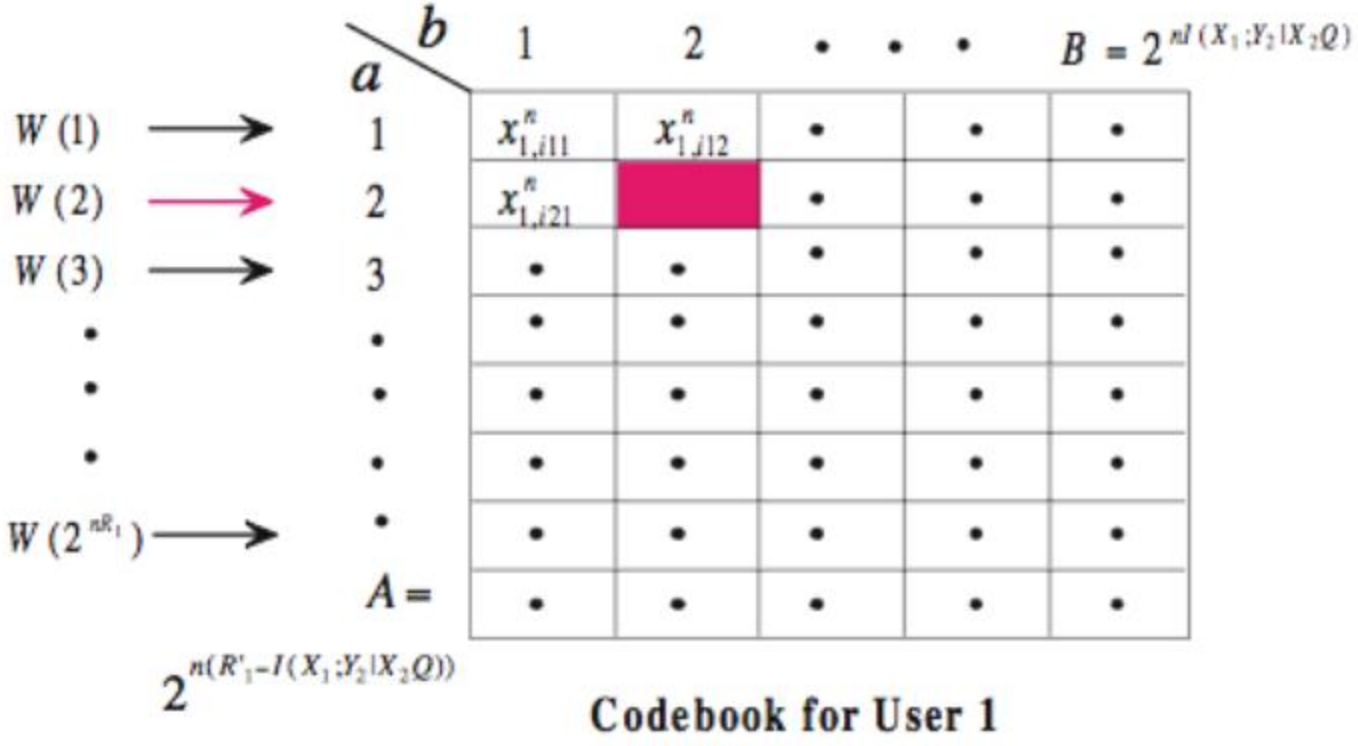
- Liang & Poor [IT08]




User 1 –> Destination SNR: 15dB
User 2 –> Destination SNR: 10dB
Boundary of Gaussian
MAC Capacity
User 1–> User 2
SNR: 2dB
User 1–> User 2
SNR: 5dB
User 1–> User 2
SNR: 10dB
Boundary of Degraded
Gaussian GMAC
Secrecy Capacity
3
2.5
2
1.5
1
0.5
0
0
0.5
1
1.5
2
2.5
3
3.5
R0 (bps/Hz)

Code Construction Principles

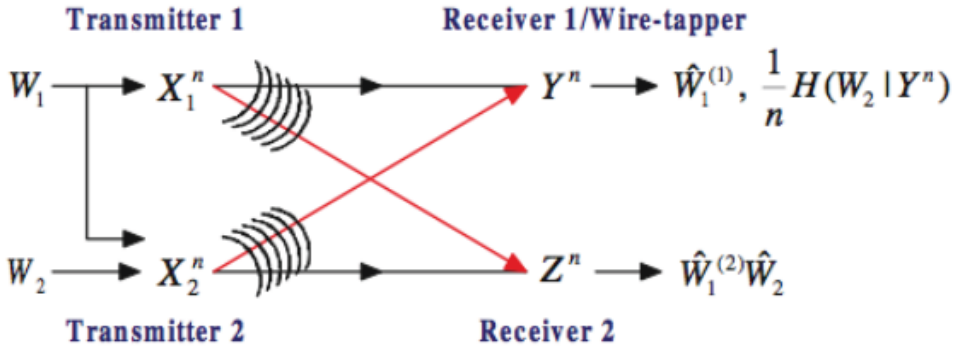




Codebook for User 1

Other Channels

- Interference Channel [w/ Liang, Someck-Baruch, Shamai, Verdú - IT'09 & w/ Koyluoglu, El Gamal, Lai - IT'11]:



- Relay Channels [e.g., w/ Aggarwal, Sankar, Calderbank – JWCN'09 & w/ Kim – IT'11]: Source and relay cooperate to improve security.

- MIMO [e.g., w/ Liu, Liu, Shamai – IT'10]: Use of multiple transmit & receive antennas allows simultaneous secure broadcast without rate penalty.

Other Recent Progress

- Authentication [w/ Lai, El-Gamal – IT'09]: "Cheating" probability is characterized for authentication in noisy channels.
- Feedback [e.g., w/ Lai, El-Gamal – IT'08, w/ Liu, Tang, Spasojevic – IT'09 & w/ Kim – IT'10]: Judicious use of feedback enhances security.
- Code Design [e.g., w/ Liu, Liang & Spasojevic – IT (under review)]: Nested structure for secure error-control codes for the wire-tap channel.
- Scheduling of Secure Broadcast [Liang, Poor & Ying [IFS11]
  - Reliability (low error probability)
  - Security (Perfect secrecy)
  - Stability (Queues remain finite)

Outline

- Overview of Physical layer security
- Information Theoretic Fundamentals
- Signal Processing Technique
  - Collaborative Beamforming
  - Jamming
- Resource Allocation and Game Theoretical Study
- Variety of Applications
- Conclusion

Cooperative System Model

- Cooperative Protocol
  - Stage one: source broadcasts its message signal locally to its trusted relays within the cluster.
  - Stage two: relays that successfully decode the message, together with the source, cooperatively transmit signal to the destination.
- Capacity at the destination

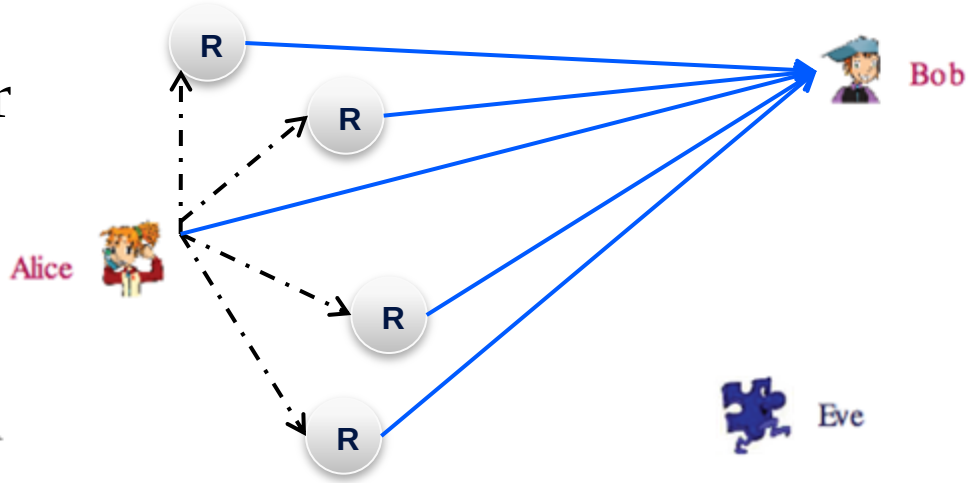
$$C_d = \frac{1}{2}\log_2\left(1+\frac{\mathbf{w}^H\mathbf{R}_\mathrm{h}\mathbf{w}}{\sigma^2}\right)$$

- Capacity at the eavesdropper

$$C_e^j = \frac{1}{2}\log_2\left(1+\frac{\mathbf{w}^H\mathbf{R}_\mathrm{g}^j\mathbf{w}}{\sigma^2}\right)$$

- Secrecy Capacity

$$C_s = \max\{0, C_d - \max(C_e^1, \ldots, C_e^J)\}$$



Secrecy Capacity Maximization or Power Minimization

- Secrecy Capacity: due to nulling, always have non-zero value

$$C_s = C_d - C_e = \frac{1}{2}\log_2\left(\frac{\sigma^2 + \mathbf{w}^H \mathbf{R}_\mathrm{h} \mathbf{w}}{\sigma^2 + \mathbf{w}^H \mathbf{R}_\mathrm{g} \mathbf{w}}\right)$$

- Secrecy capacity maximization or power minimization

$$\arg\max_{\mathbf{w}} \frac{\sigma^2+\mathbf{w}^H \mathbf{R}_\mathrm{h} \mathbf{w}}{\sigma^2+\mathbf{w}^H \mathbf{R}_\mathrm{g} \mathbf{w}} \quad \text{s.t. } \mathbf{w}^H \mathbf{w} = P_0$$

$$\arg\min_{\mathbf{w}} \mathbf{w}^H \mathbf{w} \quad \text{s.t. } \frac{\sigma^2+\mathbf{w}^H \mathbf{R}_\mathrm{h} \mathbf{w}}{\sigma^2+\mathbf{w}^H \mathbf{R}_\mathrm{g} \mathbf{w}} = 4^{C_s^0}$$

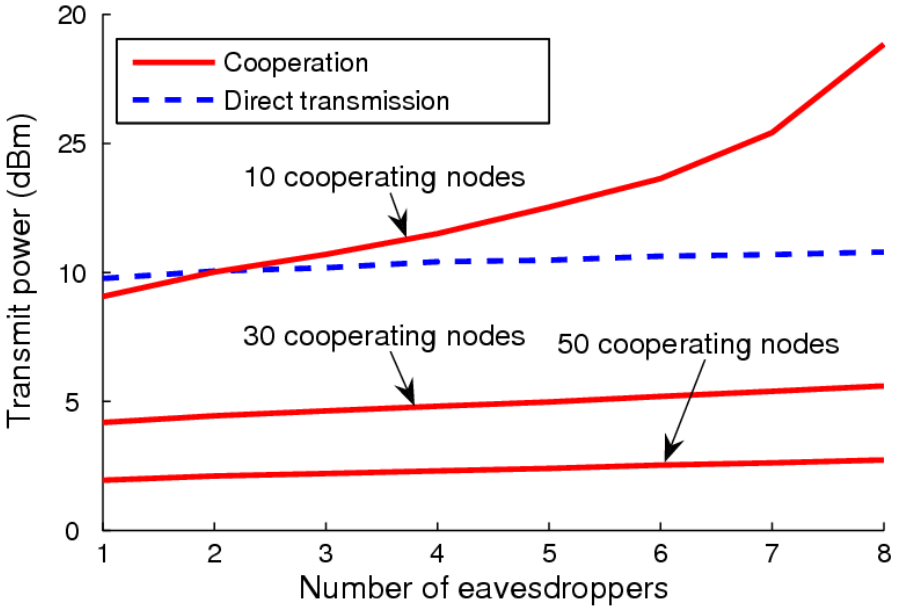
  - The solution of this Rayleigh quotient problem is the scaled eigenvector corresponding to the largest eigenvalue of the symmetric matrix $\tilde{\mathbf{R}}_\mathrm{g}^{-1}\tilde{\mathbf{R}}_\mathrm{h}$

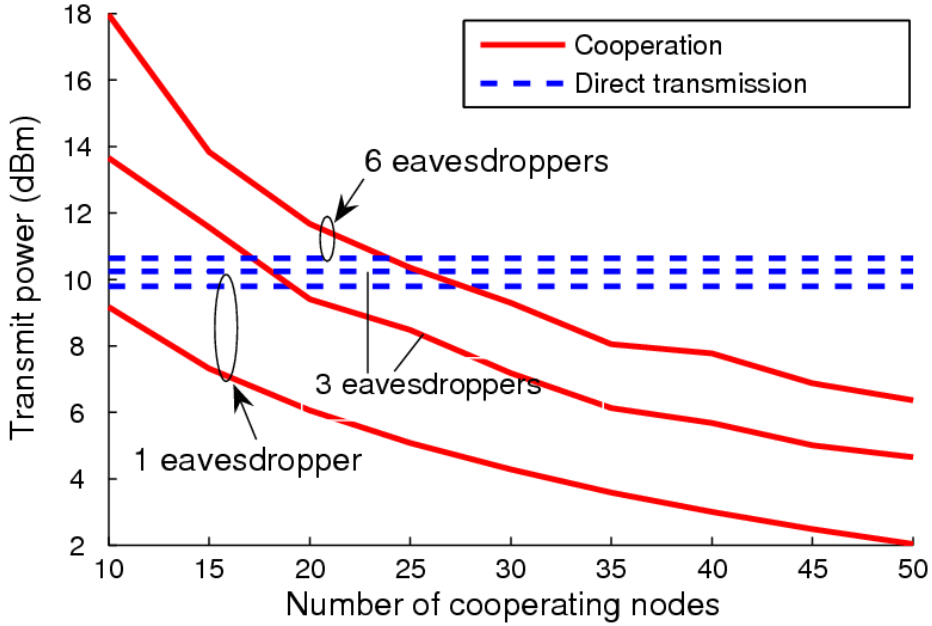
$$\tilde{\mathbf{R}}_\mathrm{h} \triangleq \frac{\sigma^2}{P_0}\mathbf{I}_N + \mathbf{R}_\mathrm{h} \qquad \tilde{\mathbf{R}}_\mathrm{g} \triangleq \frac{\sigma^2}{P_0}\mathbf{I}_N + \mathbf{R}_\mathrm{g}$$

Lun Dong, Zhu Han, Athina P. Petropulu and H. Vincent Poor, "Improving Wireless Physical Layer Security via Cooperating Relays", *IEEE Transactions on Signal Processing*, Volume: 58, Issue:3, p.p. 1875 - 1888, March 2010.

Simulation (Power Minimization)

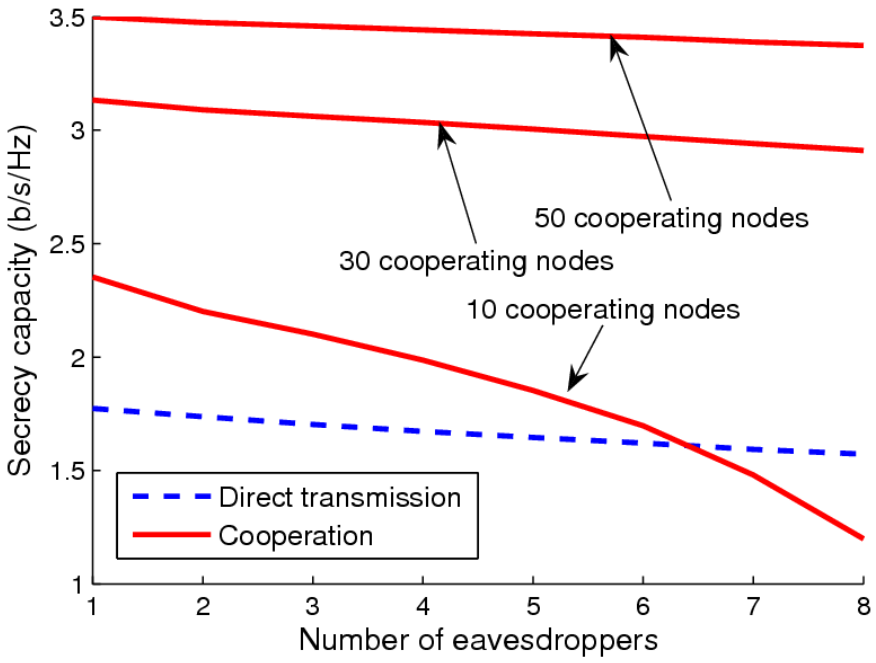
- The more eavesdroppers, the more power
- The more collaborative nodes, the less power
- Direct transmission without considering the security

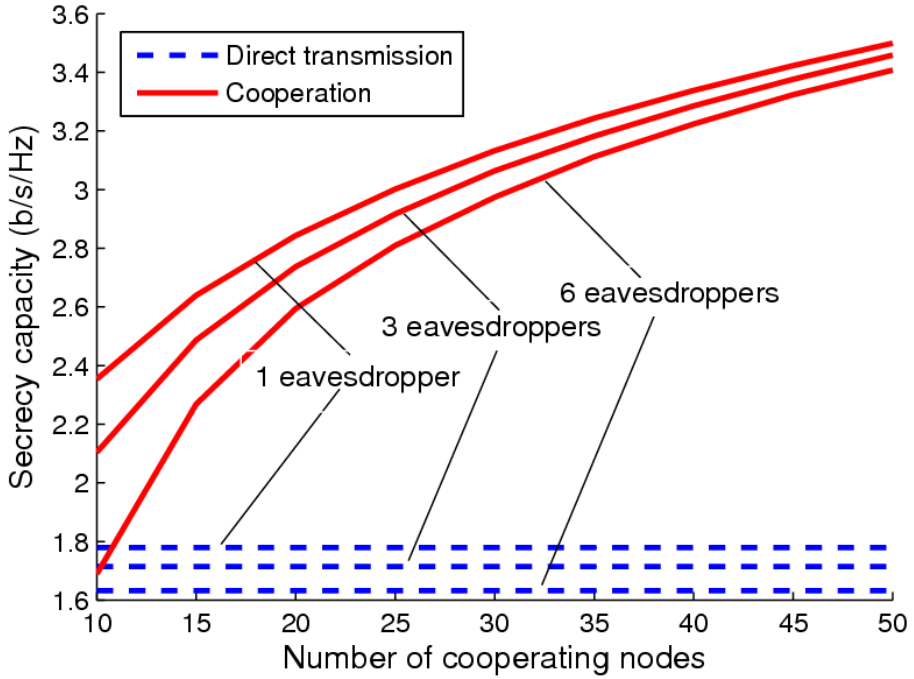




Simulation (Secrecy Capacity Maximization)

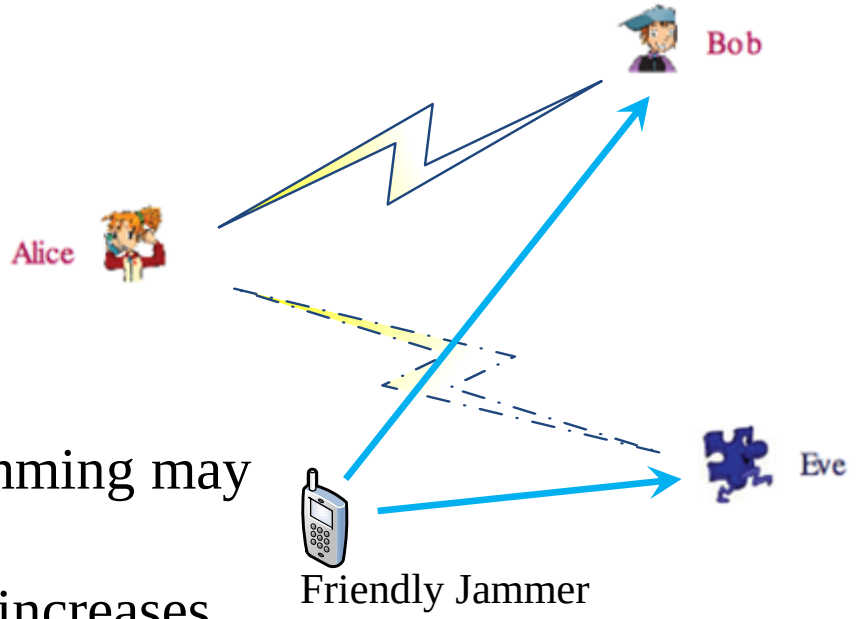
- Number of cooperating node increases, secrecy capacity increases
- Number of eavesdroppers increase, secrecy capacity drops





Jamming Techniques

- Cooperative (or Friendly) 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.
- Jamming Signal
  - Noise
  - Independent Codewords
- Jamming Power Control
  - Within a proper power region, jamming may improve the secrecy capacity.
  - But if the jamming power further increases, the secrecy capacity will approach zero.



Outline

- Overview of Physical Layer security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
  - Basics
  - Coalition Formation
  - Stackelberg Game
  - Auction Theory
- Variety of Applications
- Conclusion

History of Game Theory

- **John von Neuman** (1903-1957) co-authored, Theory of Games and Economic Behavior, with Oskar Morgenstern in 1940s, establishing game theory as a field.
- **John Nash** (1928 -) developed a key concept of game theory (Nash equilibrium) which initiated many subsequent results and studies.
- Since 1970s, game-theoretic methods have come to dominate microeconomic theory and other fields.
- Nobel Prizes
  - Nobel prize in Economic Sciences 1994 awarded to **Nash**, **Harsanyi** (Bayesian games) and **Selten** (subgame perfect equilibrium).
  - 2005, **Auman** and **Schelling** got the Nobel prize for having enhanced our understanding of cooperation and conflict through game theory.
  - 2007 **Leonid Hurwicz, Eric Maskin and Roger Myerson** won Nobel Prize for having laid the foundations of mechanism design theory.

John von Neumann
(December 28,1903 – February 8,1957)

John Forbes Nash, Jr.
(born June 13, 1928)
Winner of Nobel Prize in Economics (1994)

Introduction

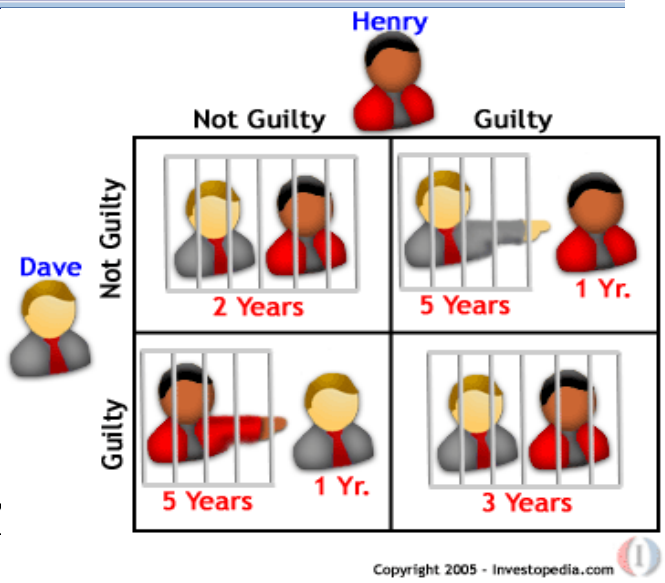
- Game theory - mathematical models and techniques developed in economics to analyze interactive decision processes, predict the outcomes of interactions, identify optimal strategies
- Game theory techniques were adopted to solve many protocol design issues (e.g., resource allocation, power control, cooperation enforcement) in wireless networks.
- Fundamental component of game theory is the notion of a *game*.
  - A game is described by a set of rational *players*, the *strategies* associated with the players, and the *payoffs* for the players. A rational player has his own interest, and therefore, will act by choosing an available strategy to achieve his interest.
  - A player is assumed to be able to evaluate exactly or probabilistically the outcome or payoff (usually measured by the utility) of the game which depends not only on his action but also on other players' actions.

Games in Strategic (Normal) Form

- A game in strategic (normal) form is represented by three elements:
  - A set of players N
  - Set of strategies of player S_i
  - Set of payoffs (or payoff functions) U_i
- Notation s_i strategy of a player i while $\mathbf{s}_{-i}$ is the strategy **profile** of all other players.
- Notice that one user's utility is a function of both this user's and others' strategies.
- A game is said to be one with complete information if all elements of the game are common knowledge. Otherwise, the game is said to be one with incomplete information, or an incomplete information game.

Rich Game Theoretical Approaches

- Non-cooperative Static Game: play once
  Prisoner Dilemma
  Payoff: (user1, user2)
  - Mandayam and Goodman (2001)
  - Virginia tech
- Repeated Game: play multiple times
  - **Threat of punishment** by repeated game. MAD: I
  - Tit-for-Tat (infocom 2003):
- Dynamic game: (Basar's book)
  - ODE for state
  - Optimization utility over time
  - HJB and dynamic programming
  - Evolutional game (Hossain and Dusit's work)
- Stochastic game (Altman's work)



Auction Theory

Book of Myerson (Nobel Prize 2007), J. Huang, H. Zheng, X. Li

Outline

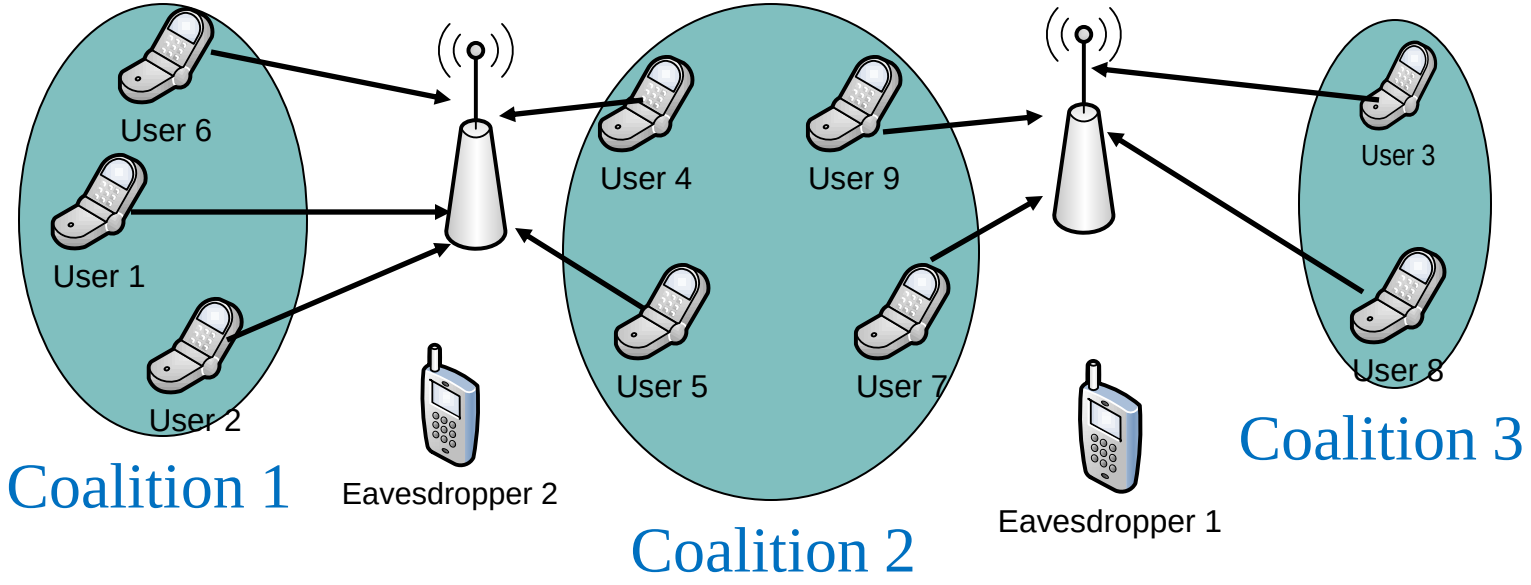
- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
  - Basics
  - Coalition Formation
  - Stackelberg Game
  - Auction Theory
- Variety of Applications
- Conclusion

Coalitional Games Preliminaries

- Coalitional game (*N*,*v*)
  - A set of players ***N,*** *a* ***coalition*** S is a group of cooperating players
  - Value (utility) of a coalition ***v***
  - User payoff x_i : the portion received by a player ***i*** in a coalition S
- Transferable utility (TU)
  - The worth ***v(S)*** of a coalition *S* can be distributed arbitrarily among the players in a coalition hence,
  - ***v(S)*** is a function over the real line
- Non-transferable utility (NTU)
  - The payoff that a user receives in a coalition is pre-determined, and hence the value of a coalition cannot be described by a function
  - ***v(S)*** is a set of payoff vectors that the players in *S* can achieve

$$v(S) \subseteq \mathbb{R}^{|S|}$$

Coalitional Game System Model



Non-cooperative TDMA transmission: 1 user per slot

User 1	User 2	User 3	User 4	User 5	User 6	User 7	User 8	User 9

Cooperative TDMA transmission: 1 coalition per slot (transmitting the data of the slot owner)

Coal.1: Data of User 1	Coal. 1: Data of User 2	Coal. 3: Data of User 3	Coal. 2: Data of User 4	Coal. 2: Data of User 5	Coal. 1: Data of User 6	Coal. 2: Data of User 7	Coal. 3: Data of User 8	Coal. 2: Data of User 9

PHY Security Coalitional Game (1)

- Coalitional game: the players are the **users (transmitters)**
- Utility function must account for
  - **Cooperation gains,** in terms of secrecy capacity
  - **Cooperation costs,** in terms of power for information exchange
- Secrecy capacity achieved by a user ***i*** part of coalition ***S*** transmitting data to its destination m_i **in a single slot**

$$C^{S}_{i,m_i} = \frac{1}{2}\log_2\left(1 + \frac{(\boldsymbol{w}_S^{opt})^H \boldsymbol{R}_S \boldsymbol{w}_S^{opt}}{\sigma^2}\right)$$

Function of:
-Users-destinations and users-eaves. channels
- Power available for transmission in the slot

Optimal weights that null the signal at the eavesdroppers (see paper or Dong et al. for expression)

Function of the users-destination channels
$\boldsymbol{R}_S = \boldsymbol{h}_S \boldsymbol{h}_S^H$

PHY Security Coalitional Game (2)

- Power considerations
  - Power constraint per coalition *S* (time slot)
  - The power available **in a slot** for a coalition ***S*** to transmit the data of a user ***i*** is given by

$$P_i^S = (\tilde{P} - \bar{P}_{i,\hat{i}})^+$$

Power constraint per slot

Power **cost:** the power needed for information exchange between user ***i*** and the farthest user in the coalition

- Security cost during information exchange

$$c_i(S) = \max(\hat{C}^e_{i,1}, \ldots, \hat{C}^e_{i,K})$$

  - where

$$\hat{C}^e_{i,k} = \frac{1}{2}\log\left(1 + \frac{\bar{P}_{i,\hat{i}} \cdot |g_{i,k}|^2}{\sigma^2}\right)$$

PHY Security Coalitional Game (3)

- The proposed PHY security game is modeled as a ***(N,V)*** NTU coalitional game, with a value given by a singleton set

$$V(S) = \{\boldsymbol{\phi}(S) \in \mathbb{R}^{|S|} | \quad \forall i \in S \ \phi_i(S) = (v_i(S) - c_i(S))^+ \\ \text{if } P_i^S > 0, \text{ and } \phi_i(S) = -\infty \text{ otherwise.}\}$$

  - $\boldsymbol{\phi_i}$ is the payoff of a user ***i*** when transmitting as part of coalition *S*
  - $\boldsymbol{v_i(S)} = \boldsymbol{C^S_{i,m_i}}$ = secrecy capacity using transmit beamforming given in previous slides
  - For a user that spends all of its power for information exchange, the utility is negative (no benefit from cooperating)

Properties of PHY Security Game

- The proposed NTU game is generally non-super-additive (cooperation is not always beneficial)
  - Traditional concepts such as the core or the Shapley value are not suitable as solutions
  - The **grand coalition** is **seldom** the optimal solution
    - *Due to the cooperation cost, as reflected by the false alarm*
- In the proposed game, the minimum coalition size is equal to ***K+1*** where ***K*** is the number of eavesdroppers
  - To null ***K*** eavesdroppers, ***K+1*** users are needed
- The proposed game is classified as a **coalition formation game**
  - The objective is to answer the question "Who should cooperate with who in the network?"

Coalition Formation: Merge and Split

- Define the Pareto order preference relation between two collections of coalitions *R* and *S*

$$\mathcal{R} \rhd \mathcal{S} \Longleftrightarrow \{\phi_j(\mathcal{R}) \geq \phi_j(\mathcal{S}) \ \forall \ j \in \mathcal{R}, \mathcal{S}\},$$

with *at least one strict inequality* ($>$) for a player k.

- **Merge rule:** merge any group of coalitions where

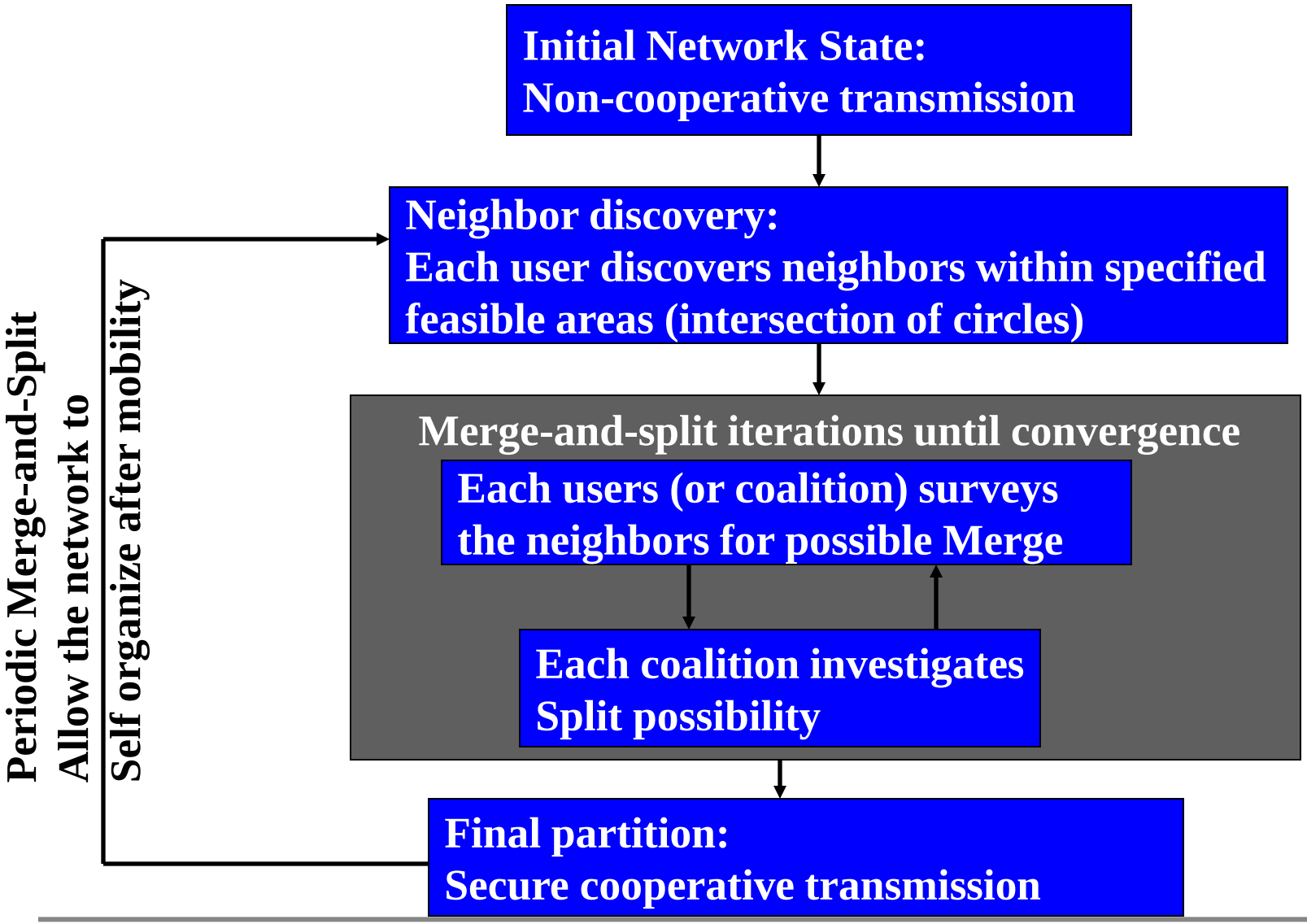
$$\{\cup_{j=1}^{l} S_j\} \rhd \{S_1, \ldots, S_l\}$$

- **Split rule:** split any group of coalitions where

$$\{S_1, \ldots, S_l\} \rhd \{\cup_{j=1}^{l} S_j\}$$

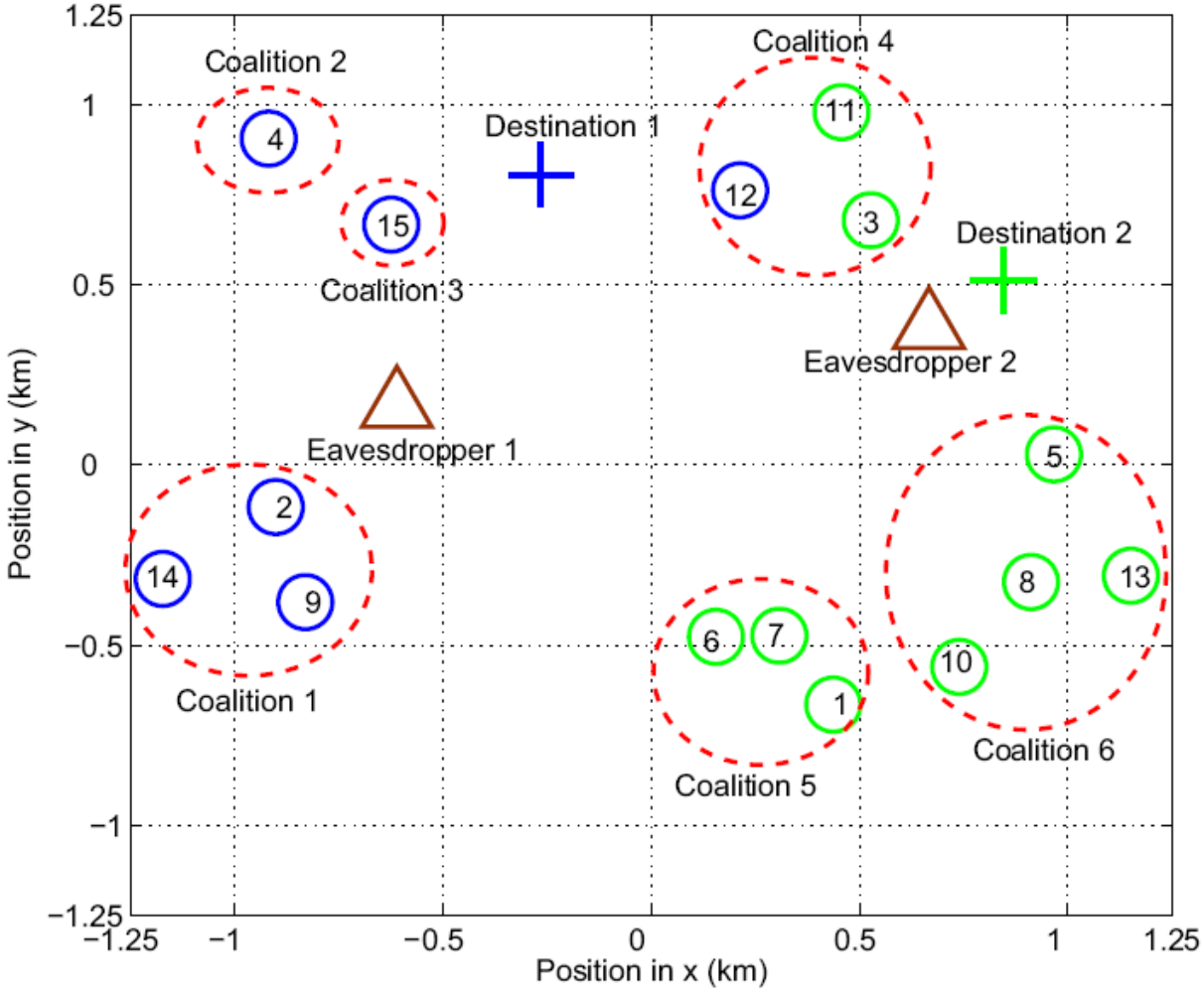
- A decision to merge (split) is an agreement between all players to form (break) a new coalition

Coalition Formation Algorithm



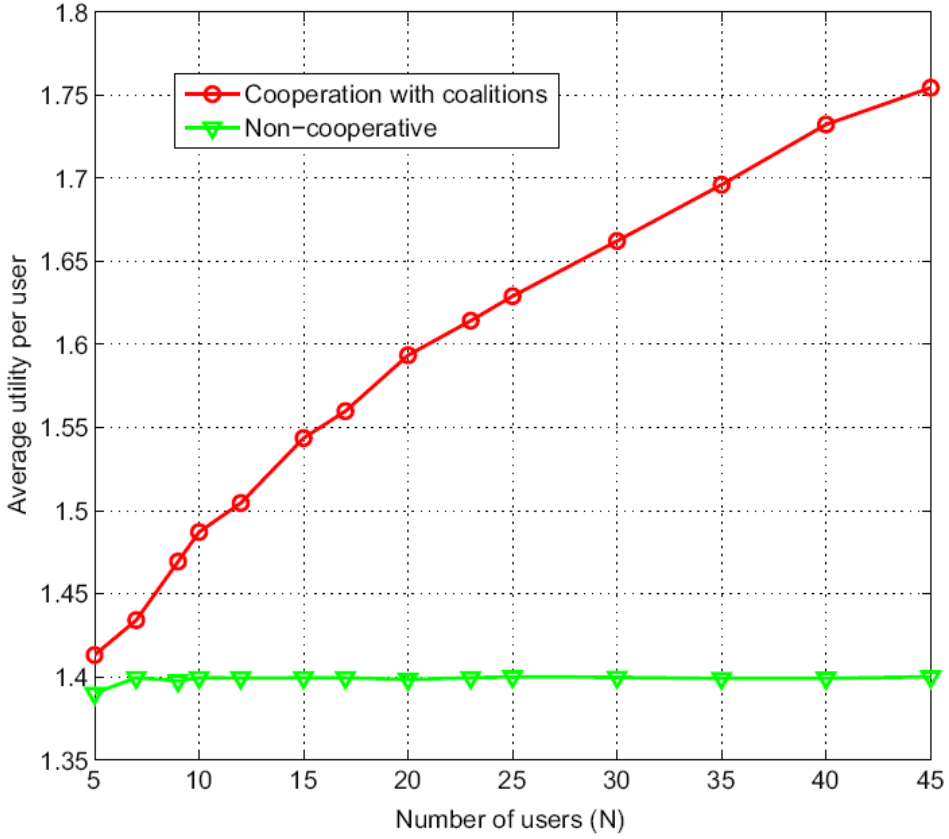
Simulation Results (1)

- Coalition example



Simulation Results (2)

- Utility vs. Number of users



Walid Saad, Zhu Han, M¶erouane Debbah, Are Hj¿rungnes, and Tamer Basar, “Distributed Coalition Formation Games for Secure Wireless Transmission," invited, Journal of Mobile Networks and Applications, Special Issues on Mobility of Systems, Users, Data and Computing, ACM/Springer, April 2011.

Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
  - Basics
  - Coalition Formation
  - Stackelberg Game
  - Auction Theory
- Variety of Applications
- Conclusion

Stackelberg Game Preliminaries (1)

- **Leader-Follower Strategy**
  - Given a two-person game, where Player 1 wants to minimize a cost function ( ) and Player 2 wants to minimize a cost function ( ) by choosing and from the strategies set.
  - The strategy set ( ) is called a Stackelberg strategy with Player 2 as leader and Player 1 as follower if for any and

$$J_2\ u_1^*, u_2^*\ \leq J_2\ u_1^o\ u_2\ , u_2$$

where

$$J_1\ u_1^o\ u_2\ , u_2\ \leq \min_{u_1} J_1\ u_1, u_2$$

$$u_1^* = u_1^o\ u_2^*$$

Stackelberg Game Preliminaries (2)

- **Applications in Physical Layer Security**
  - Appropriate for classes of system problems consisting of multiple criteria, multiple decision makers, decentralized information, and natural hierarchy of decision making levels.
  - To study the interactions between source-destination pairs and cooperative relays/jammers.
- **Source-Destination Pair as Buyer:**
  - The buyer-level game
  - Aim to achieve the best security performance with the relays/jammers' help with the least reimbursements to them.
- **Cooperative Relays/Jammers as Sellers:**
  - The seller-level game
  - Aim to gains as many profits as possible.

Date a Girl with her BF on the Same Table

- **Solution with my Friend: Distract the poor BF**
  - Both s-d capacity and s-e capacity reduced.
  - But the secrecy capacity can be increased.
- **Increase secrecy rate by buying jamming power.**
- **Jammer sets the optimal price to maximize profits.**

$$C_1 = W \log_2 \left(1 + \frac{P_0 G_{sd}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{id}} \right)$$

$$C_2 = W \log_2 \left(1 + \frac{P_0 G_{sm}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{im}} \right)$$

$$C_s = (C_1 - C_2)^+$$

Game Definition

- The source (buyer)

$$U_s = aC_s - \sum_{i \in \mathcal{J}} p_i P_i, \qquad \text{s.t. } 0 \le P_i \le P_{max},$$

  - a is the gain per unit capacity
  - P_{max} is the maximal power that a jammer can provide,
  - p_i is the price per unit power for the friendly jammer,
  - P_i is the friendly jammer's power, and
  - $\mathcal{J}$ is the set of friendly jammers.
- The source will not participate in the game if $C_1 < C_2$, i.e., if the secrecy capacity is zero
- The jammer (seller)

$$U_i = p_i P_i^{c_i},$$

  where $c_i \ge 1$.

Source Analysis

- The goal of the source as a buyer is to buy the optimal amount of power from the friendly jammers so as to improve its secrecy capacity.
- Solving

$$\frac{\partial U_s}{\partial P_i} = 0,$$

we get

$$P_i^* = P_i^* \left(p_i, \{P_j\}_{j \neq i}, P_0, G_{sd}, G_{sm}, \{G_{jd}\}, \{G_{jm}\}, \sigma^2\right).$$

Since $0 \leq P_i \leq P_{max}$

$$P_i^* = \min\left[\max(P_i, 0), P_{max}\right].$$

Jammer Analysis

- The jammer goal is to set the optimal price such that its utility is maximized
- We have to solve

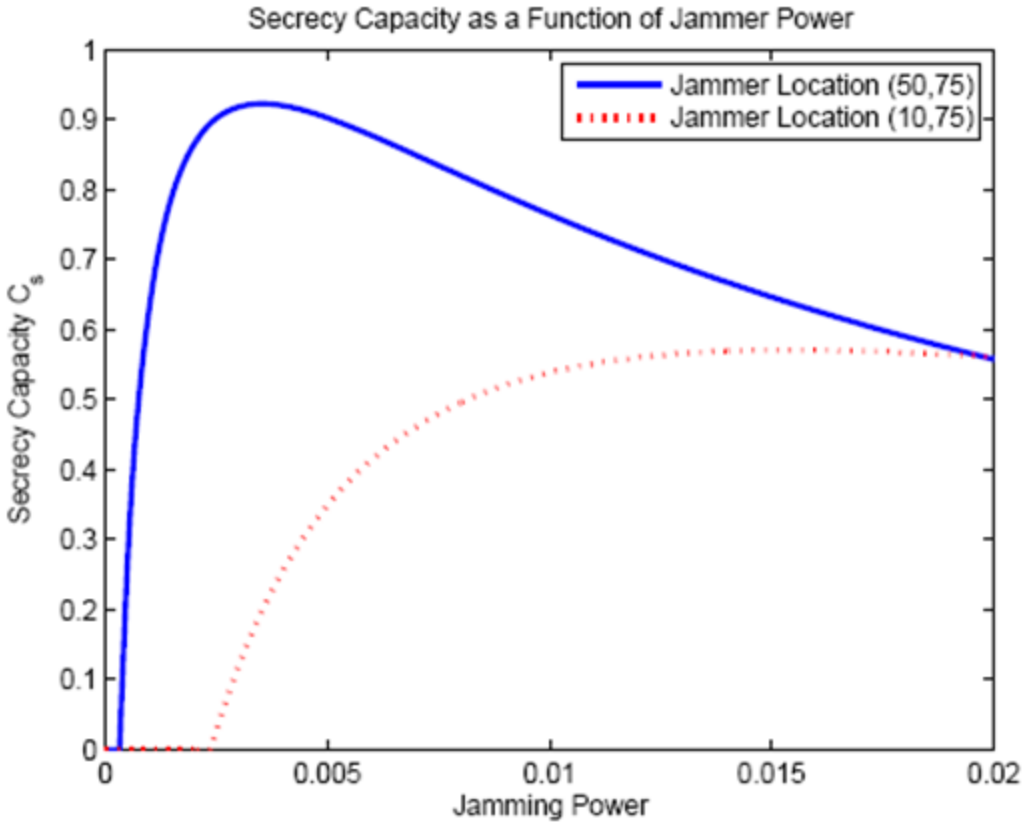
$$\frac{\partial U_i}{\partial p_i} = (P_i^*)^{c_i} + p_i c_i (P_i^*)^{c_i - 1} \frac{\partial P_i^*}{\partial p_i} = 0.$$

- From the closed form solution of P_i^*, the solution of p_i^* will be a function given as

$$p_i^* = p_i^*(\sigma^2, G_{sd}, G_{sm}, \{G_{id}\}, \{G_{im}\}).$$

Notice that p_i^* should be positive. Otherwise, the friendly jammer i would not play.

Results



Zhu Han, Ninoslav Marina, Merouane Debbah, and Are Hjorungnes, “Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer," EURASIP Journal on Wireless Communications and Networking, special issue on Wireless Physical Layer Security, Volume 2009, Article ID 452907, 10 pages, June 2009.

Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation and Game Theoretical Study
  - Basics
  - Coalition Formation
  - Stackelberg Game
  - Auction Theory
- Variety of Applications
- Conclusion

Auction Theory Preliminaries (1)

- Recently, **auction theory** (pioneered by Vickrey, etc) has been widely employed in wireless networks to solve the resource allocation issues.
- In an auction, each bidder bids for an item, or items, according to a specific mechanism, and the allocation(s) and price(s) for the item, or items, are determined by specific rules.
- **Auctioneers:** The players own resources (spectrum, power, etc) and expect to earn rewards by offering the resources.
- **Bidders:** The players hope to obtain the resources from the auctioneers to improve their performance but in return need to provide some rewards.

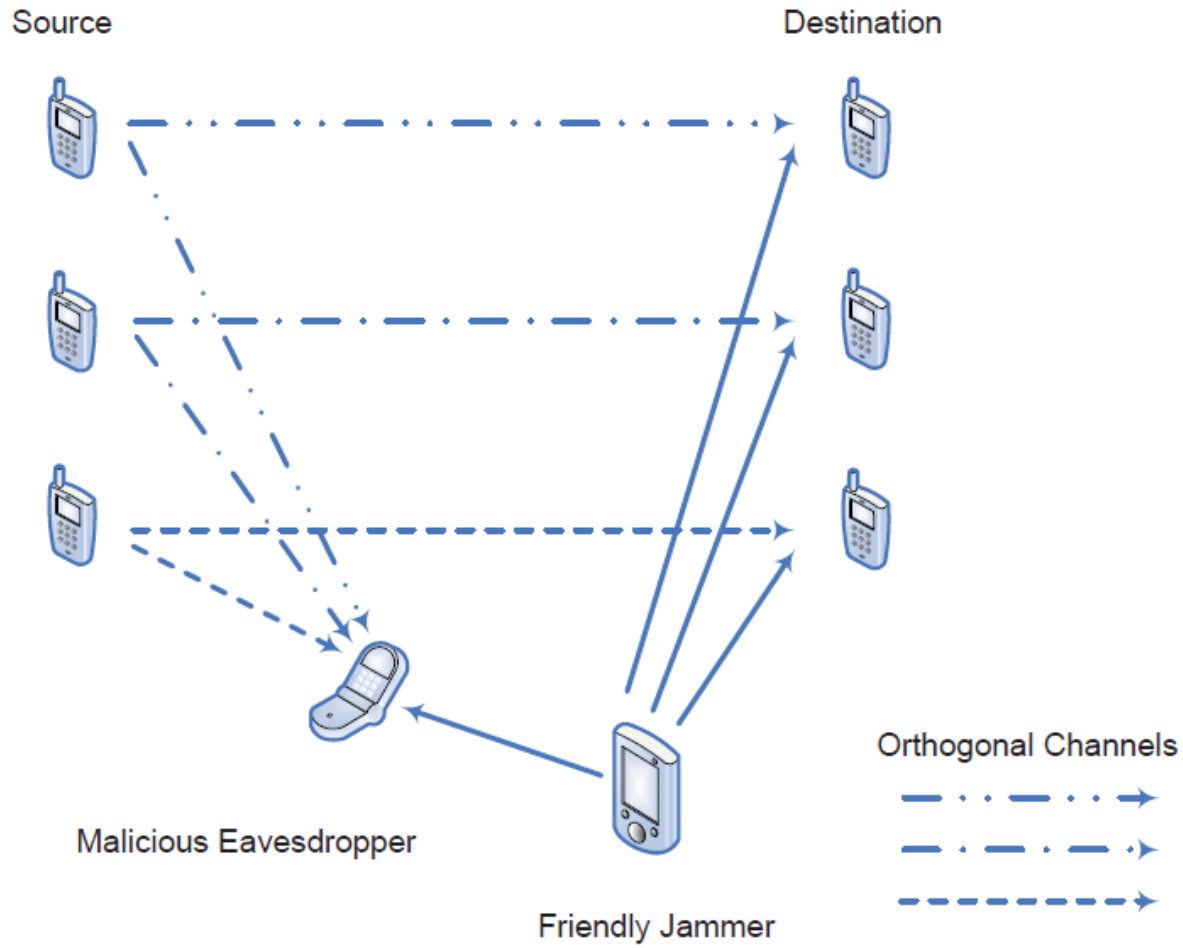
Auction Theory Preliminaries (2)

- **Various Types:**
  - Vickrey Auction [Vickrey'1961]
  - Ascending Auction [Ausubel'1997, Cramton'1998]
  - First Price Auction, Second Price Auction
  - Single Object Auction, Multiple Object Auction
  - Double Auction (multiple auctioneers and multiple bidders)
- **Hot Application Scenarios:**
  - Cognitive Radio Networks (PU as auctioneer and SUs as bidders)
  - WLAN (users compete for the transmission resources)
  - Cellular Networks (D2D, Femtocell)

Ascending Auction

- **Procedure of Ascending Auction**
  - The auctioneer announces an initial price to the bidders;
  - The bidders report back the quantities demanded at that price ;
  - The auctioneer raises the price;
  - This process repeats until the sum of the reported bids meet the total quantity of the on-sale resources.
- **Properties:**
  - With private values, this ascending auction yields the same outcome as the (sealed-bid) Vickrey auction, but has advantages of simplicity and privacy preservation.
  - With interdependent values, this ascending auction may retain efficiency, whereas the Vickrey auction suffers from a generalized Winner's Curse.

Jammer-Assisted System Scenario



[1] Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Improve Physical Layer Security in Cooperative Wireless Network using Distributed Auction Games," *INFOCOM Workshop on Cognitive & Cooperative Communications*, Shanghai, Apr. 10-15, 2011.
[2] Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Distributed Auction-Based Power Allocation for Improving Physical Layer Security in Cooperative Networks," IEEE Journal on Selected Areas in Communications, in revision.

Jammer-Assisted System Scenario

- **Secrecy rate for the source-destination pairs:**

$$C_s^i = \left[C_1^i - C_2^i \right]^+$$

$$= W \left[\log\left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2 + p_i^J g_{J,D_i}} \right) - \log\left(1 + \frac{p_i g_{S_i,E}}{\sigma^2 + p_i^J g_{J,E}} \right) \right]^+$$

- **With a proper amount of jamming power, the secrecy rate can be improved effectively.**
- **How to allocate the jamming power among multiple source-destination pairs efficiently and effectively?**
- **Auction!!**

Auction Definition

- **Players:**
  - Source S_i as one of the bidders;
  - Friendly jammer J as the auctioneer;
  - Sources submit bids to compete for the jamming power from the friendly jammer, in order to increase the secrecy rate.

- **Utilities:**
  - Source S_i can have a performance gain by successfully getting the jamming power, meanwhile it needs to pay for the jamming power offered by the friendly jammer.
  - Friendly jammer charges the sources for the jamming service at a price for every unit of jamming power.

Auction Definition

- **Source's Utility Function**
  - We consider source S_i as one of the bidders, while friendly jammer J as the auctioneer. The sources submit bids to compete for the jamming power from the friendly jammer, in order to increase the secrecy rate of their own data transmission.
  - Source S_i can have a performance gain by successfully getting the jamming power, meanwhile it needs to pay for the power offered by the friendly jammer.
  - Therefore, the utility function of source Si can be defined as

$$U_i\left(p_i^J, \lambda\right) = \mathrm{G}\left(p_i^J\right) - \mathrm{P}\left(p_i^J, \lambda\right)$$

where $\mathrm{G}\left(p_i^J\right)$ is the performance gain with the jamming power p_i^J, $\mathrm{P}\left(p_i^J, \lambda\right)$ is the cost paid for the friendly jammer, and λ represents the unit price of jamming power.

Auction Definition

- **Source's Utility Function**
  - Using linear pricing scheme as cost function, then we have

$$U_i\left(p_i^J, \lambda\right) = \square\left(p_i^J\right) - \square\left(p_i^J, \lambda\right)$$

$$= \square\left(p_i^J\right) - \lambda p_i^J$$

- **Jammer's Utility Function**
  - The friendly jammer charges the sources for the jamming service at a price for every unit of jamming power. Then the utility of friendly jammer J can be defined as

$$U_J\left(\{p_i^J\}, \lambda\right) = \lambda \sum_i p_i^J$$

$$\text{s.t.} \quad 0 \le \sum_i p_i^J \le p_{max}$$

Distributed Auction Games

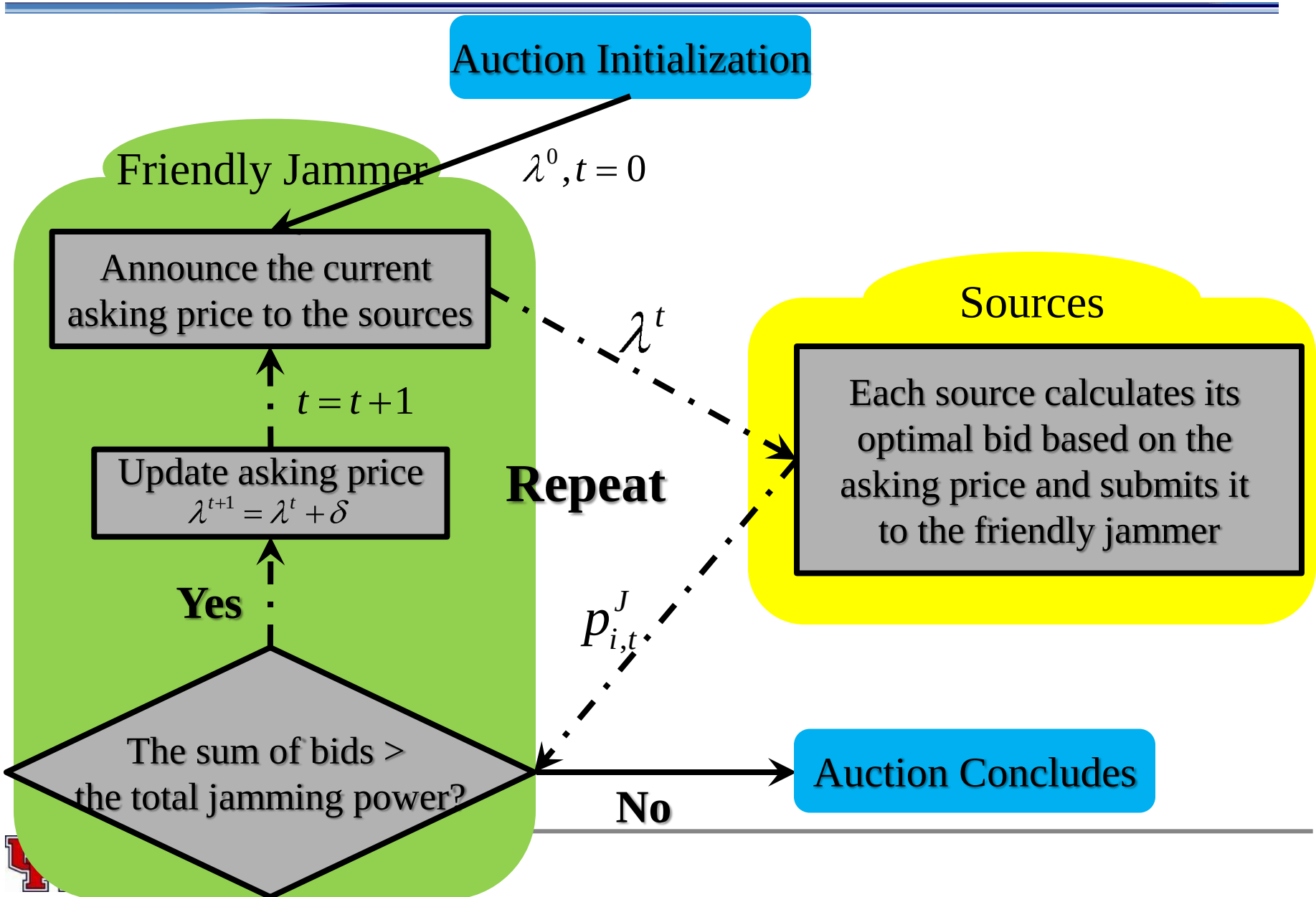
- **Power Allocation using Traditional Ascending Clock Auction (P-ACA-T)**

  - ✓ The P-ACA-T scheme is proposed based on traditional ascending clock auction, where each source is allowed to bid any power demand between 0 and $p_{\max}$ at every iteration.

  - ✓ In P-ACA-T, the friendly jammer sets an asking price which is increased at every iteration, then each source submits its optimal demand based on the current asking price to maximize its utility.

  - ✓ The friendly jammer will conclude the auction until the total jamming power bids satisfy the condition that $p_{total}^{J} \leq p_{\max}$.

P-ACA-T


Auction Initialization
$\lambda^0, t = 0$
Friendly Jammer
Announce the current asking price to the sources
λ^t
Sources
Each source calculates its optimal bid based on the asking price and submits it to the friendly jammer
$t = t + 1$
Update asking price
$\lambda^{t+1} = \lambda^t + \delta$
Repeat
Yes
$p_{i,t}^J$
The sum of bids > the total jamming power?
No
Auction Concludes

Distributed Auction Games

- **Power Allocation using Alternative Ascending Clock Auction (P-ACA-A)**

  ✓ The P-ACA-A scheme is proposed based on alternative ascending clock auction which can guarantee the cheat-proof property.

  ✓ The procedures of P-ACA-A are the same as P-ACA-T except that at every iteration in P-ACA-A, the friendly jammer computes the cumulative clinch, which is the amount of jamming power that each source is guaranteed to win at every iteration.

$$L_i^t = \max\left(0, p_{max} - \sum_{j \neq i} p_{j,t}^J\right)$$

Distributed Auction Games

- **Key difference between P-ACA-T and P-ACA-A:**

  - ✓ In P-ACA-T, the final payment of source S_i, based on only the final allocated jamming power and the final asking price:

$$P_i^{\text{å}}(p_i^{J\text{å}}, \lambda^T) = \lambda^T p_i^{J\text{å}}$$

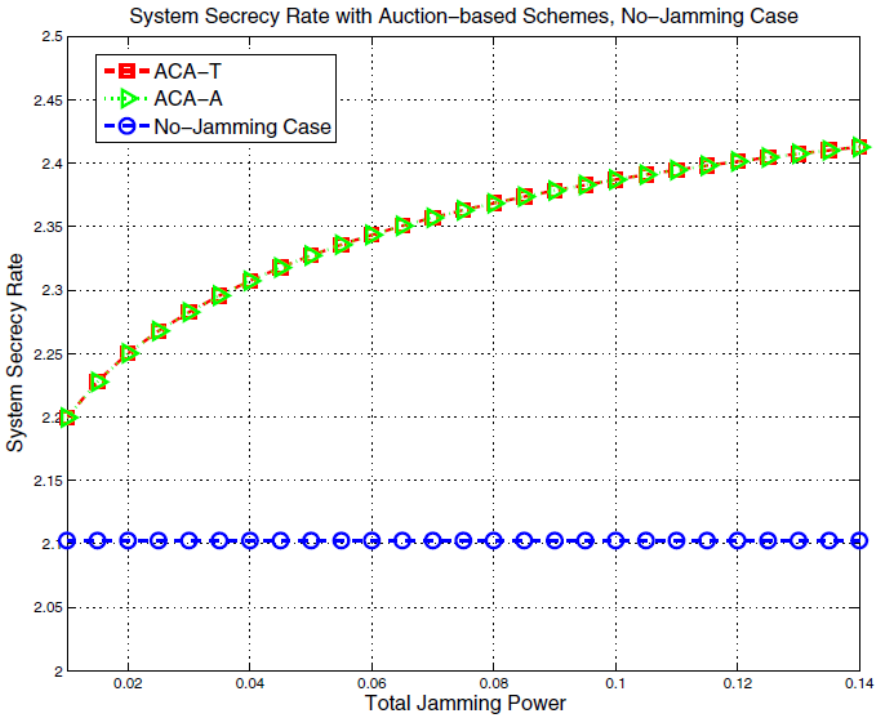
  - ✓ In P-ACA-A, the final payment of source S_i, based on the cumulative clinch and the asking price at every iteration during the auction:

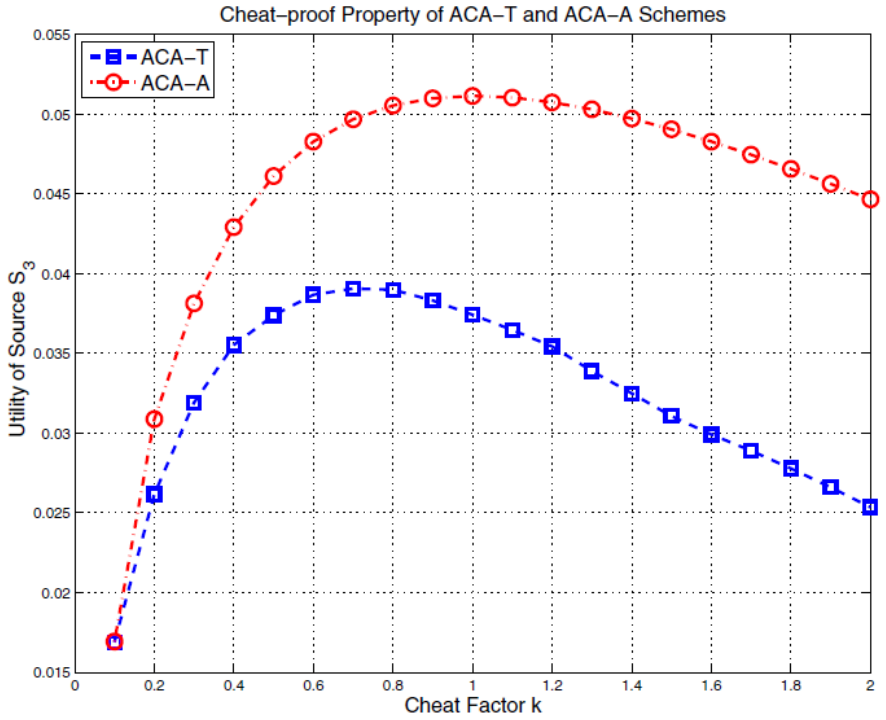
$$P_i^{\text{å}}(\{L_i^t\}, \{\lambda^t\}) = \lambda^0 L_i^0 + \sum_{t=1}^{T} \lambda^t \left(L_i^t - L_i^{t-1} \right)$$

  - ✓ The different payment rules lead to different cheat-proof properties of these two auction-based schemes

Simulations (Cheat-proof and Secrecy Rate)

- P-ACA-T and P-ACA-A can improve the system secrecy rate effectively.
- P-ACA-A is cheat-proof, while P-ACA-T is not.
  - Cheat-proof: Reporting true optimal demand at every iteration is a mutually best response for each source and there is no incentive for the sources to cheat since any cheating may lead to a loss in utility.





Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation Game Theoretical Study
- Variety of Applications
  - Cognitive Relay Network
  - Two-Way Relay Network
  - Femtocell Network
  - RFID
  - Satellite Network
- Conclusion

PHY Security in CR Networks

Power Allocation using Vickrey Auction and Sequential First-Price Auction Games for Physical Layer Security in Cognitive Relay Networks

[1] Tianyu Wang, **Lingyang Song**, Zhu Han, Xiang Cheng, and Bingli Jiao, "Power Allocation using Vickrey Auction and Sequential First-Price Auction Games for Physical Layer Security in Cognitive Relay Networks," IEEE International Conference on Communications, Ottawa, Canada, Jun. 2012.

[2] Tianyu Wang, Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Power Allocation for Two-Way Relay System Based on Sequential Second Price Auction," *Wireless Personal Communications*, Aug. 2012.

Introduction

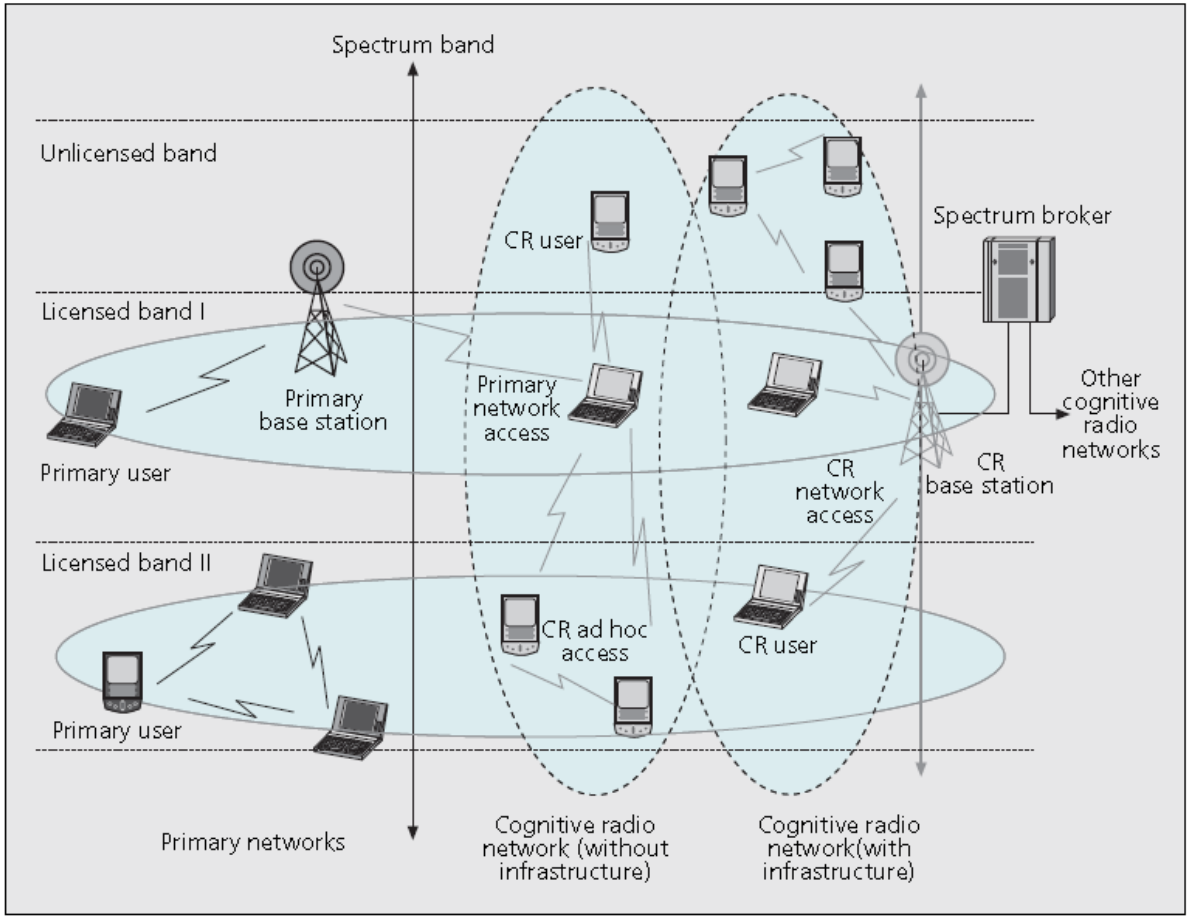
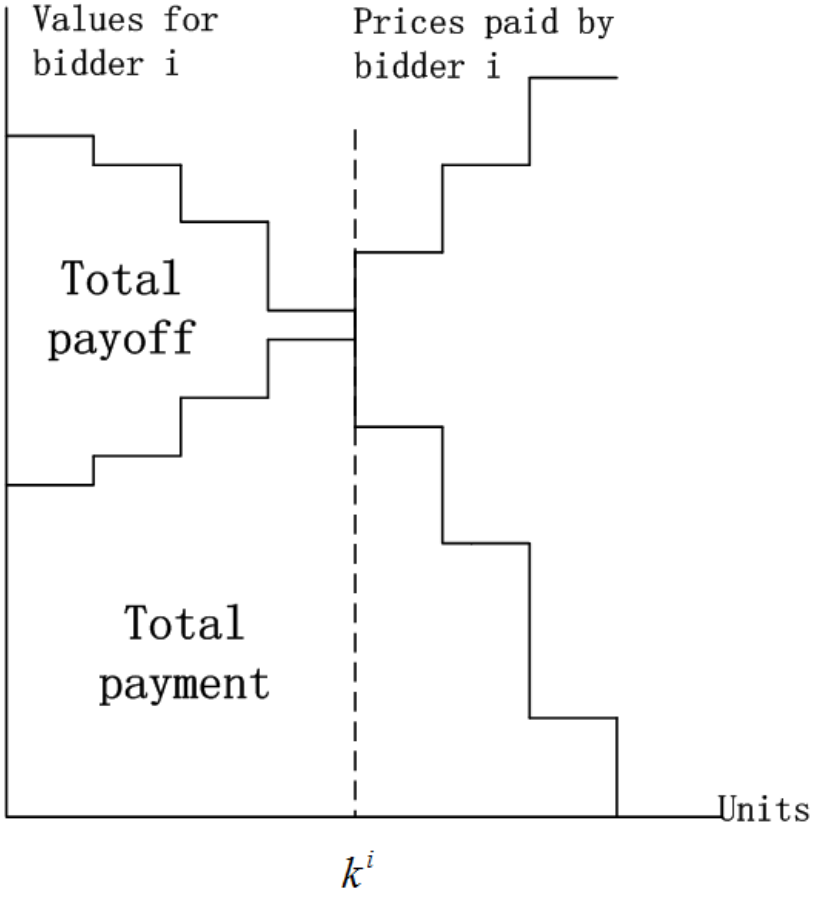


Figure 2. *Cognitive radio network architecture.*

Cognitive Radio Network

Introduction

- **Vickrey Auction**



Each of N bidders is asked to submit K bids, $b_k^i, 1 \le k \le K$ satisfying $b_1^i \ge b_2^i \ge ... \ge b_K^i$, to indicate how much he is willing to pay for each additional unit.

Thus, a total of $N \times K$ bids are collected and the K units are awarded to the K highest of these bids, i.e., if bidder i has $k \le K$ of the K highest bids, then bidder i is awarded k units.

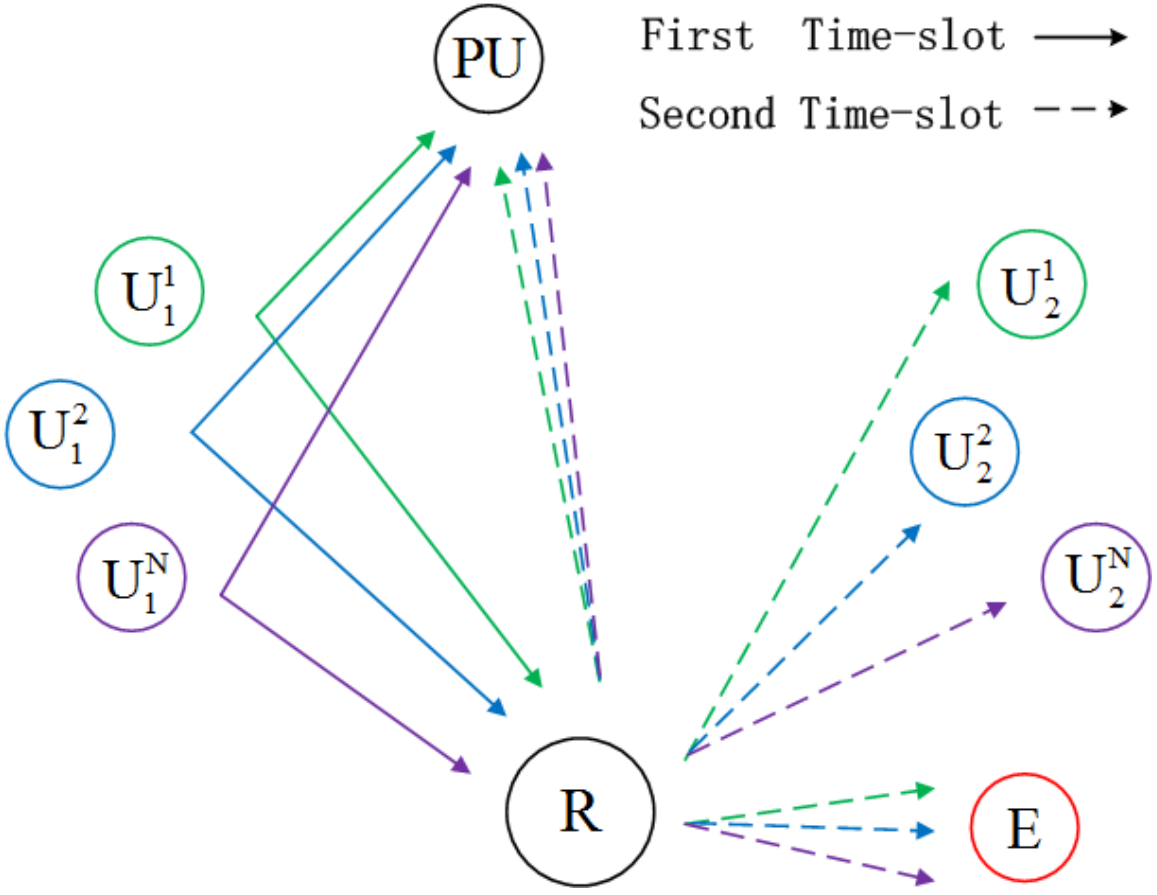
Any bidder i who wins k^i units pays the highest k^i losing bids of the other bidders, i.e., the highest losing bids not including his own.

Introduction

- **Sequential First-Price Auction**
  - The sequential first-price auction is an auction where the K identical units are sold to N > K bidders using a series of first-price sealed-bid auctions.
  - Specifically, one of the units is auctioned off at one round, where the unit is sold at the price of the highest bid to the corresponding bidder and the knocking down price is announced immediately.
  - After K first-price sealed-bid auctions, the sequential first-price auction ends.

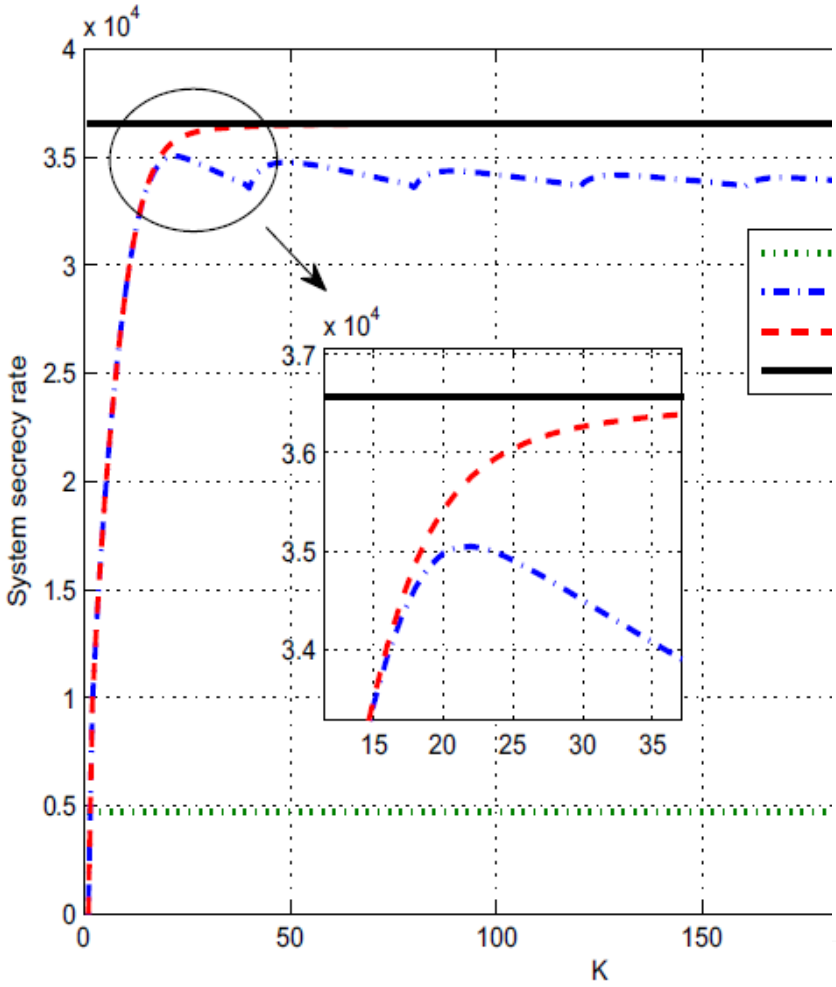
System Model

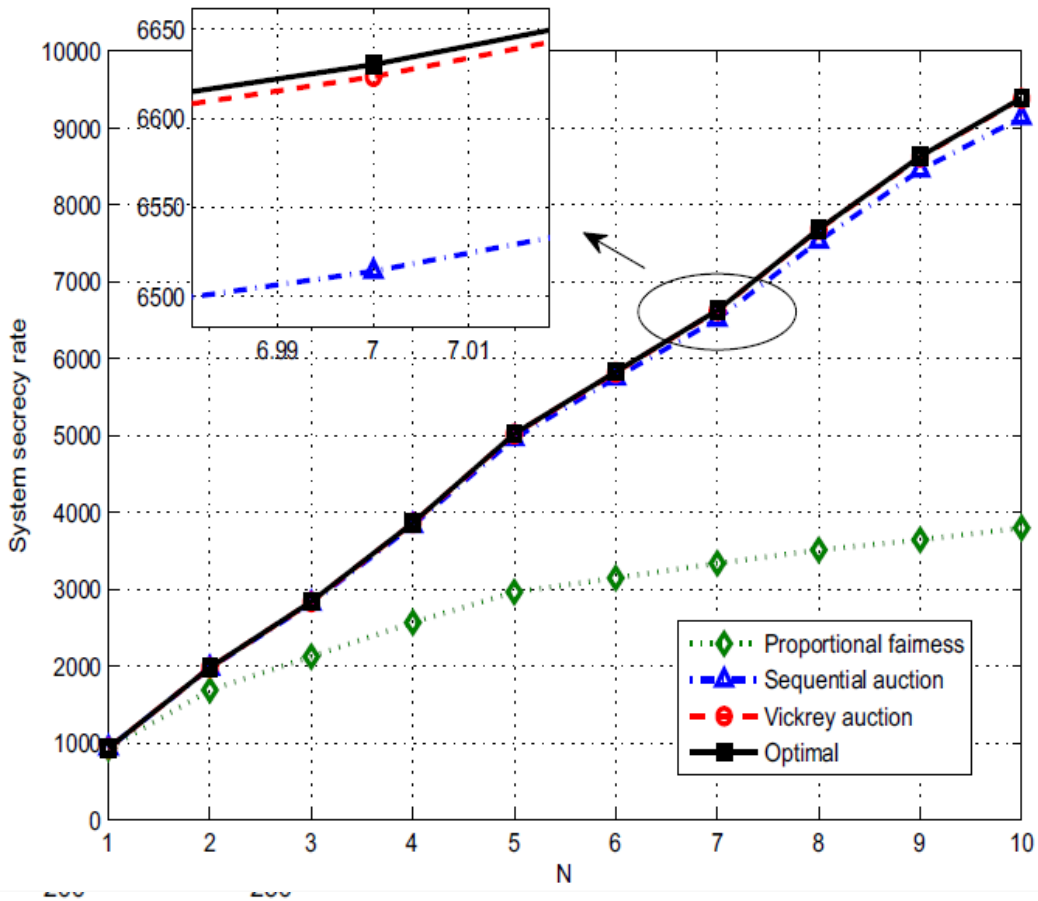
- **Cognitive Relay Network**



Simulations

- ✓ Both the algorithms achieve high performances in system secrecy rate.
- ✓ The Vickrey auction obtains better performance in efficiency while the sequential first-price auction achieves more fairness among SU pairs.





Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation Game Theoretical Study
- Variety of Applications
  - Cognitive Relay Network
  - Two-Way Relay Network
  - Femtocell Network
  - RFID
  - Satellite Network
- Conclusion

Joint Relay and Jammer Selection for Secure Two-Way Relay Networks

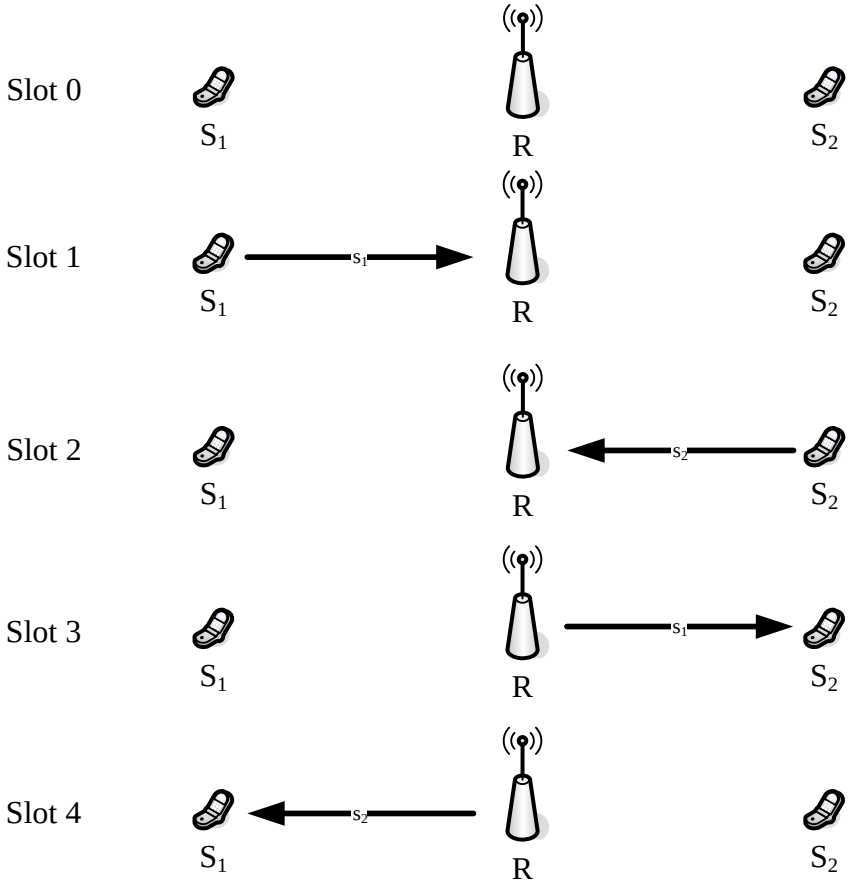
[1] Jingchao Chen, Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Joint Relay and Jammer Selection for Secure Two-way Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 388-396, 2012.

[2] Jingchao Chen, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Joint Relay and Jammer Selection for Secure Decode-and-Forward Two-Way Relay Communications," *IEEE Globe Communication Conference (Globecom)*, Houston, USA, Dec. 2011.

[3] Jingchao Chen, Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Joint Relay and Jammer Selection for Secure Two-way Relay Networks," *IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jun. 5-9, 2011.

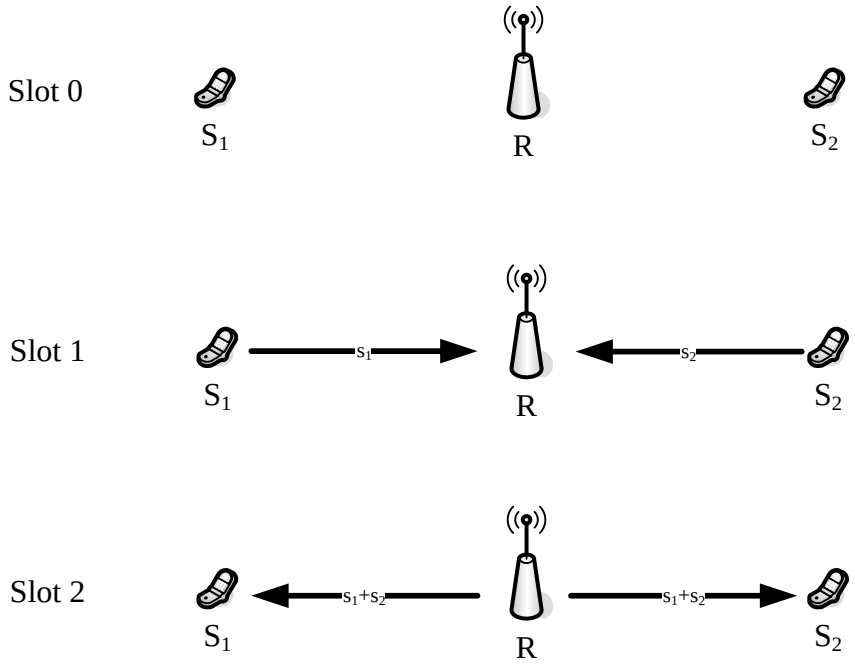
Literature Overview

- **Conventional Bi-Directional Relay Protocol**

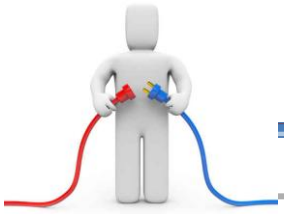


Literature Overview

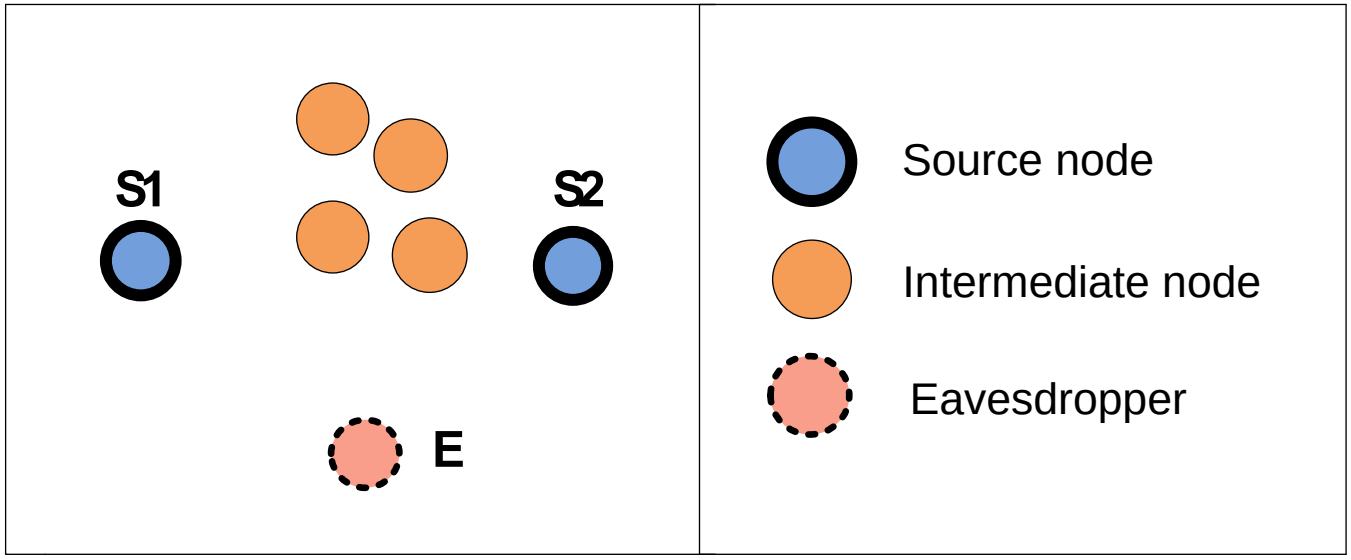
- **Amplify-and-Forward Bi-Directional Relay Protocol**



Analog Network Coding



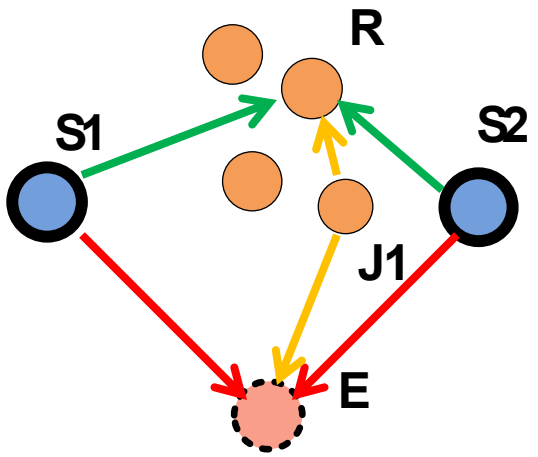
System Model



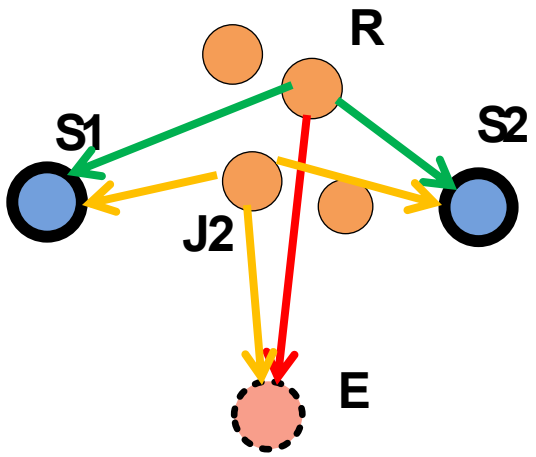
System Model

- **Two Phases (AF Relay):**

✓ 1st phase

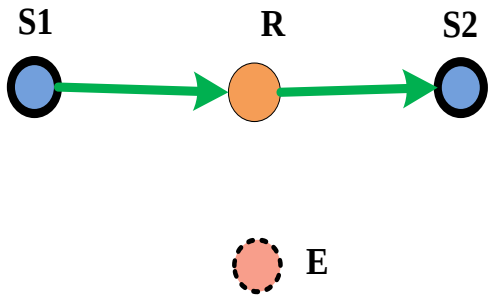


✓ 2nd phase



Key assumption in this two-way relay scenario: The eavesdropper can eavesdrop on the main communication channels in both phases.

System Model



- Overall SINR of channel $S_i \rightarrow S_j$:

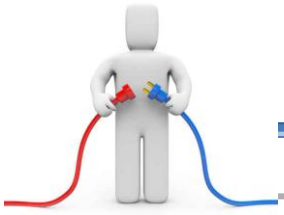
$$\Gamma_j = \frac{\gamma_{S_i,S_j}}{\gamma_{J_1,S_j} + \gamma_{J_2,S_j} + \gamma_{R,S_j} + 1}$$

$$\gamma_{S_i,S_j} = \alpha^2 P_R P_S \left|h_{S_i,R}\right|^2 \left|h_{R,S_j}\right|^2$$

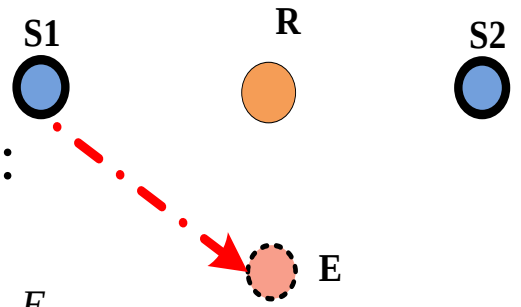
$$\gamma_{J_1,S_j} = \alpha^2 P_R P_J \left|h_{J_1,R}\right|^2 \left|h_{R,S_j}\right|^2$$

$$\gamma_{J_2,S_j} = P_J \left|h_{J_2,S_j}\right|^2$$

$$\gamma_{R,S_j} = \alpha^2 P_R \left|h_{R,S_j}\right|^2$$



System Model



- Overall SINR of channel S_i → E (Optimal Case):

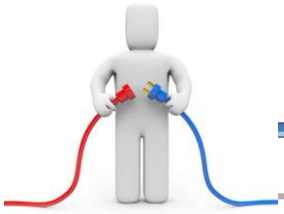
$$\Gamma_{E_i} = \frac{\gamma_{S_i,R,E}}{\gamma_{S_j,R,E} + \gamma_{J_1,R,E} + \gamma_{J_2,E} + \gamma_{R,E} + 1} + \frac{\gamma_{S_i,E}}{\gamma_{S_j,E} + \gamma_{J_1,E} + 1}$$

s.t. ψ_0 (Instantaneous knowledge of the eavesdropping channels)

$$\gamma_{S_j,E} = P_S \mid h_{S_j,E} \mid^2, \ \gamma_{J_j,E} = P_J \mid h_{J_j,E} \mid^2$$

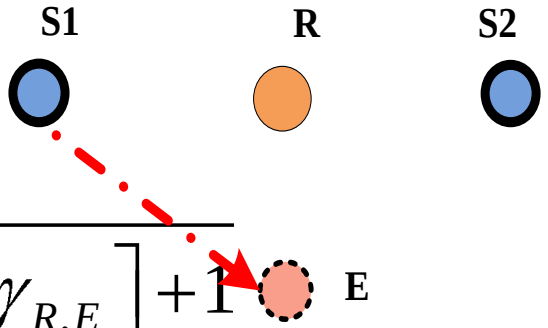
$$\gamma_{S_j,R,E} = \alpha^2 P_R P_S \mid h_{S_j,R} \mid^2 \mid h_{R,E} \mid^2, \ \gamma_{R,E} = \alpha^2 P_R \mid h_{R,E} \mid^2$$

$$\gamma_{J_1,R,E} = \alpha^2 P_R P_J \mid h_{J_1,R} \mid^2 \mid h_{R,E} \mid^2$$



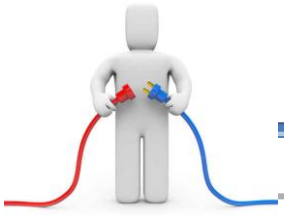
System Model

- Overall SINR of channel S_i → E (Suboptimal Case):



$$\Gamma'_{E_i} = \frac{\mathrm{E}\left[\gamma_{S_j,R,E}\right]}{\mathrm{E}\left[\gamma_{S_j,R,E}\right]+\mathrm{E}\left[\gamma_{J_1,R,E}\right]+\mathrm{E}\left[\gamma_{J_2,E}\right]+\mathrm{E}\left[\gamma_{R,E}\right]+1} + \frac{\mathrm{E}\left[\gamma_{S_i,E}\right]}{\mathrm{E}\left[\gamma_{S_j,E}\right]+\mathrm{E}\left[\gamma_{J_1,E}\right]+1}$$

s.t. ψ_1 (Average knowledge of the eavesdropping channels)



Problem Formulation

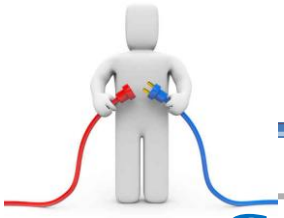
- Instantaneous secrecy rate of channel $S_i \rightarrow S_j$:

$$C_{S_i}\left(R, J_1, J_2\right) = \max\left\{\frac{1}{2}\log_2\left(1+\Gamma_i\right) - \frac{1}{2}\log_2\left(1+\Gamma_{E_j}\right), 0\right\}$$

- Overall secrecy rate of the system:

$$C_S\left(R, J_1, J_2\right) = C_{S_1}\left(R, J_1, J_2\right) + C_{S_2}\left(R, J_1, J_2\right)$$

- Select one conventional relay and one or two friendly jammers.



Selections without Jamming

- **Conventional Selection (CS)**

$$R^* = \arg\max_{R \in S_{in}} \; C_{S_1} \quad R \quad + C_{S_2} \quad R$$

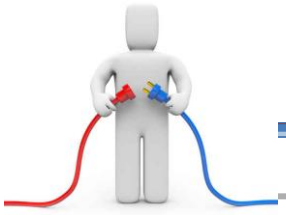
$$= \arg\max_{R \in S_{in}} \quad 1 + \Gamma_1^{CS} \quad \times \quad 1 + \Gamma_2^{CS}$$

$$\approx \arg\max_{R \in S_{in}} \left\{ \left(1 + \frac{\gamma_{S_1,S_2}}{\gamma_{R,S_2}} \right) \times \left(1 + \frac{\gamma_{S_2,S_1}}{\gamma_{R,S_1}} \right) \right\}$$

- **Optimal Selection (OS)**

$$R^* = \arg\max_{R \in S_{in}} \left\{ \frac{1 + \Gamma_1^{OS}}{1 + \Gamma_{E_2}^{OS}} \times \frac{1 + \Gamma_2^{OS}}{1 + \Gamma_{E_1}^{OS}} \right\}$$

$$\Gamma_i^{OS} \approx \frac{\gamma_{S_j,S_i}}{\gamma_{R,S_i}}, \Gamma_{E_i}^{OS} \approx \frac{\gamma_{S_i,E}}{\gamma_{S_j,E}} + \frac{\gamma_{S_i,R,E}}{\gamma_{S_j,R,E} + \gamma_{R,E}}$$



Selections with Jamming

- **Optimal Selection with Jamming**

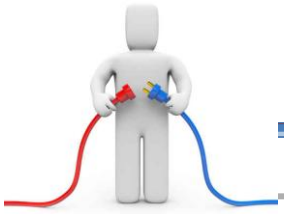
$$R^*, J_1^*, J_2^* = \arg\max_{\substack{R,J_1,J_2 \in S_{in} \\ R \neq J_1, J_2}} C_S\ R, J_1, J_2$$

$$= \arg\max_{\substack{R,J_1,J_2 \in S_{in} \\ R \neq J_1, J_2}} \left\{ \frac{1+\Gamma_2}{1+\Gamma_{E_1}} \times \frac{1+\Gamma_1}{1+\Gamma_{E_2}} \right\}.$$

- **Optimal Switching**

$$C_S\ R, J_1, J_2 > C_{S_1}^{OS}\ R + C_{S_2}^{OS}\ R$$

$$C_{S_i}^{OS}\ R = \left[\frac{1}{2} \log_2 \left(\frac{1+\Gamma_i^{OS}}{1+\Gamma_{E_j}^{OS}} \right) \right]^+$$

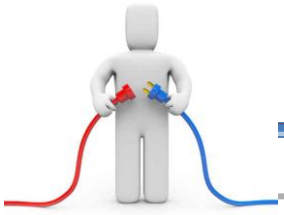


Selections with Jamming

- **Suboptimal Selection with Jamming**

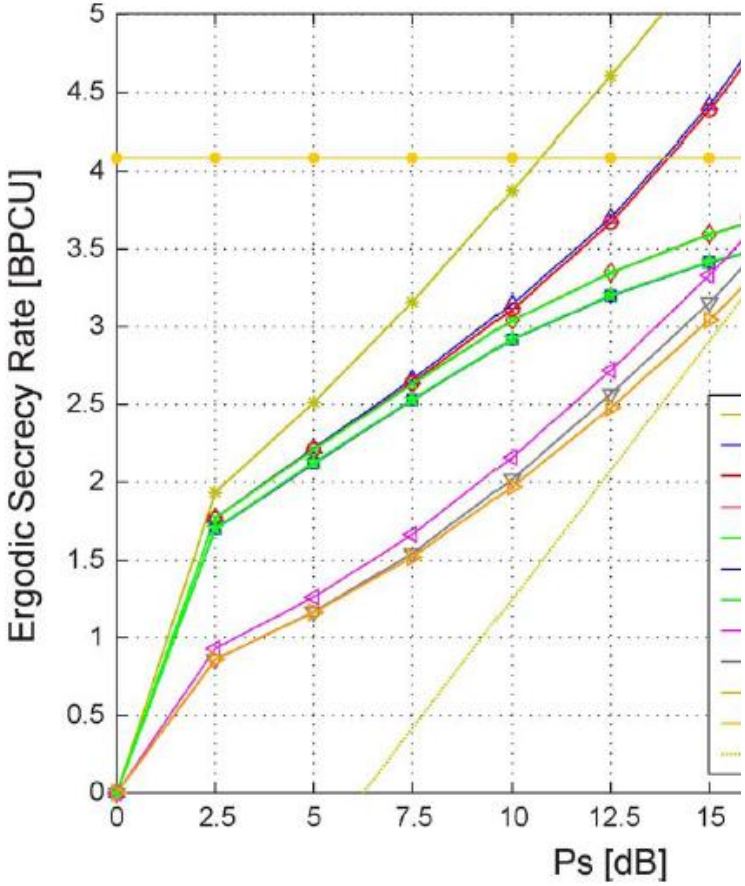
$$R^*, J_1^*, J_2^* = \arg\max_{\substack{R, J_1, J_2 \in S_{in} \\ R \neq J_1, J_2}} C_S \quad R, J_1, J_2$$

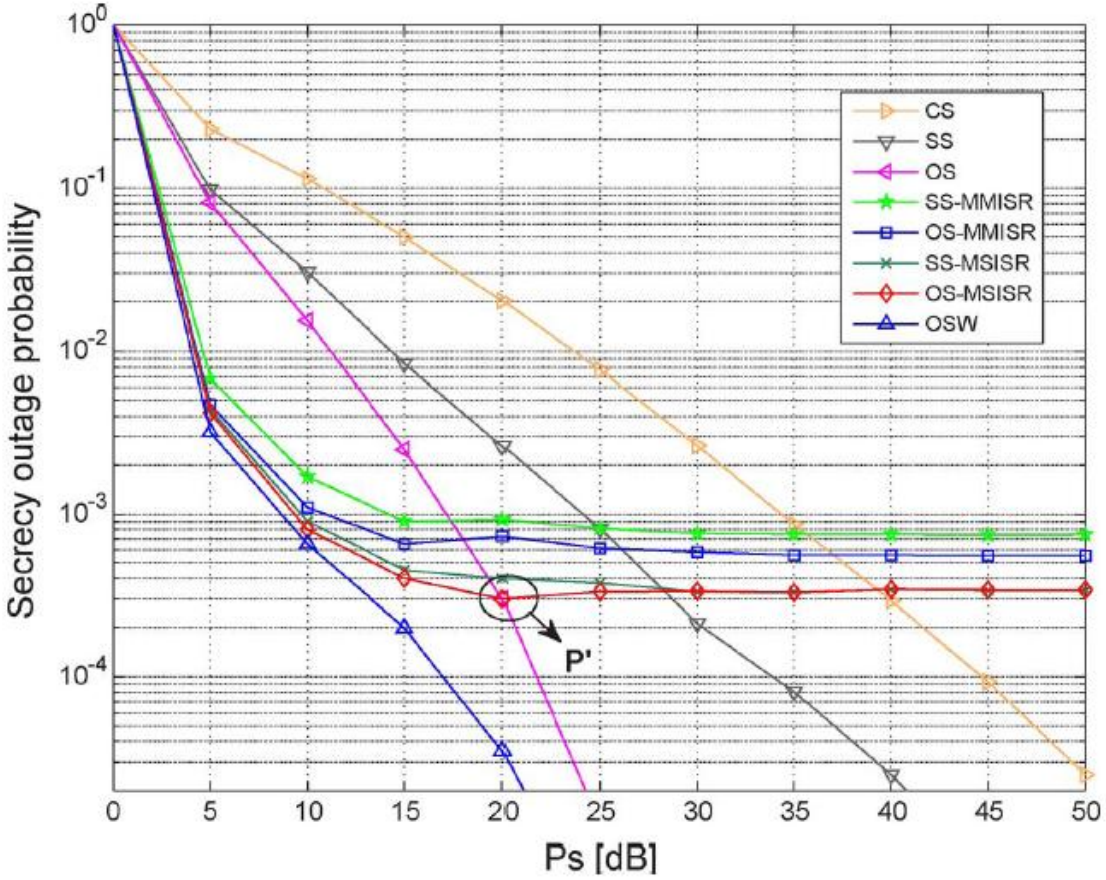
$$= \arg\max_{\substack{R, J_1, J_2 \in S_{in} \\ R \neq J_1, J_2}} \left\{ \frac{1+\Gamma_2}{1+\Gamma'_{E_1}} \times \frac{1+\Gamma_1}{1+\Gamma'_{E_2}} \right\}.$$



Numerical Results

The hybrid scheme (which switches intelligently between jamming and non-jamming modes) is efficient in providing the highest secrecy rate in almost the whole transmitted power regime.





PHY Security in Two-Way Relay Scenario

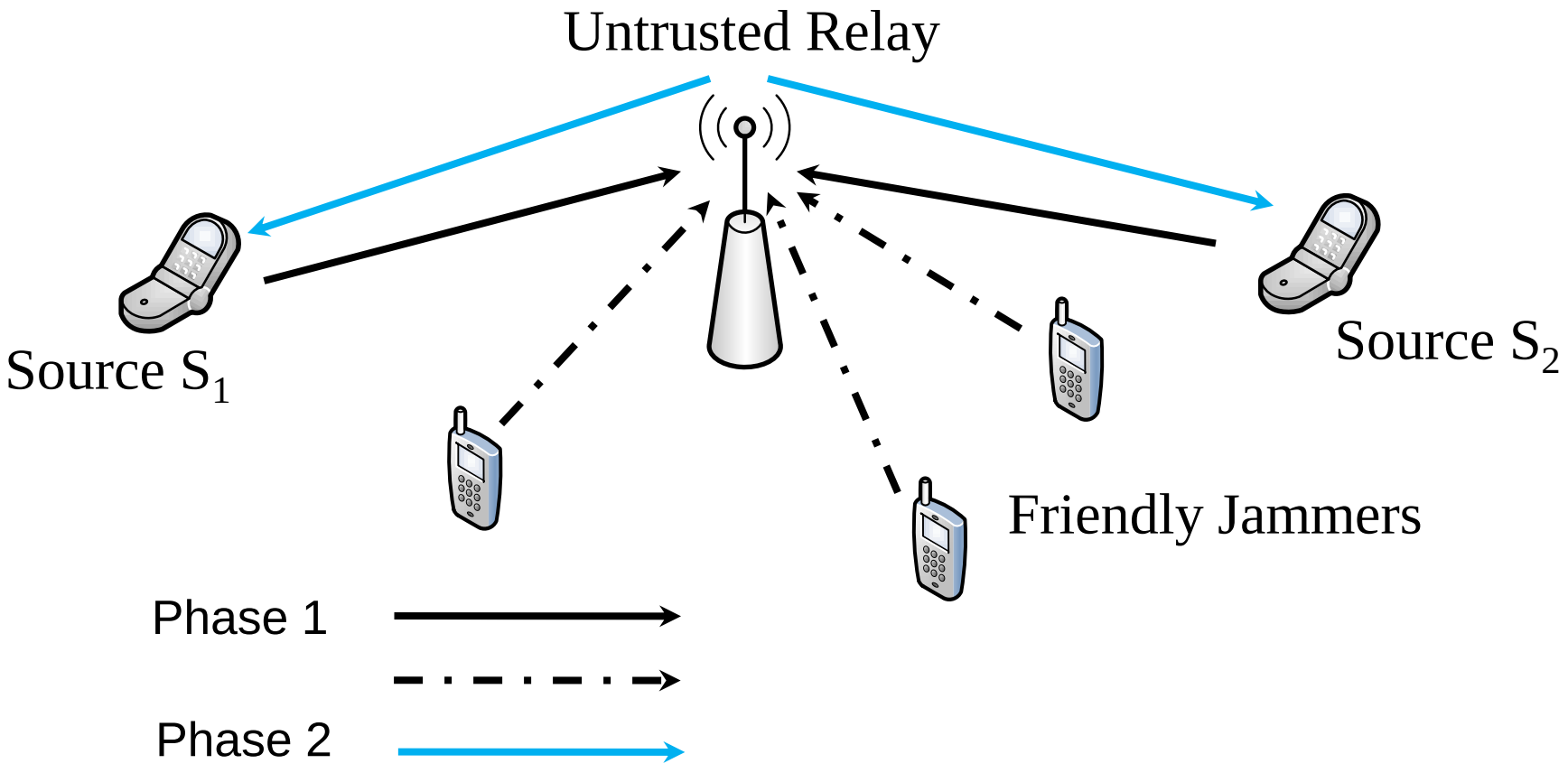
Physical Layer Security for Two-Way Relay Communications with Friendly Jammers

[1] Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Physical Layer Security for Two Way Relay Communications with Friendly Jammers," *IEEE Global Communications Conference (Globecom)*, Miami, Florida, USA, Dec. 6-10, 2010.

[2] Rongqing Zhang, **Lingyang Song**, Zhu Han, and Bingli Jiao, "Physical Layer Security for Two Way Relay Communications with Untrusted Relay and Friendly Jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693 - 3704, Oct. 2012.

System Model

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



System Model

- ✓ **Secrecy Rate for S_1 and S_2:**

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

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

- ✓ 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.

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

Game between Sources and Friendly Jammers

- **Stackelberg 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 $p_i, i \in \mathrm{N}$, should also be taken into consideration.

  - We employ the pricing scheme to the payment of the two sources. For simplicity, here we mainly consider linear pricing scheme.

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.
  - The source side game can be expressed as

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

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

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

$$U_i = m_i \quad p_i^J \quad {}^{c_i}, i \in \mathrm{N}$$

  - 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 $m_1, m_2, \ldots, m_N$, as the amount of jamming power that the sources will buy also depends on the prices that the friendly jammers ask.

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

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

Game between Sources and Friendly Jammers

- **Distributed Algorithm**
  - From above, we have

$$m_i = I_i(\mathbf{m}) = -\frac{p^J_{i\_opt}}{c_i \dfrac{\partial p^J_{i\_opt}}{\partial m_i}}$$

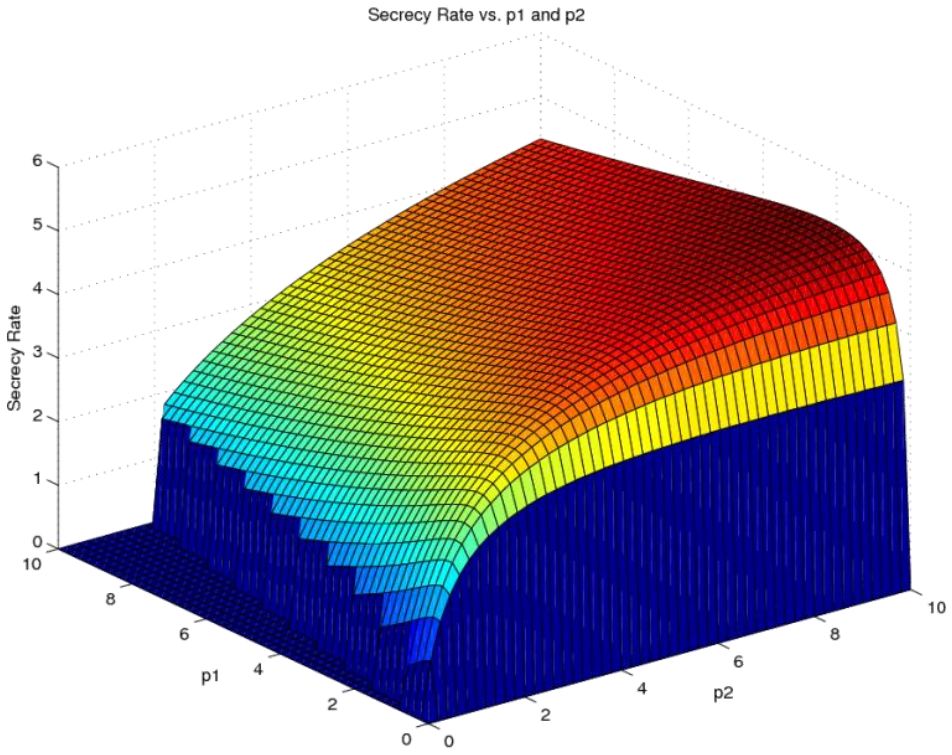
  - where $\mathbf{m} = (m_1, m_2, \ldots, m_N)^T$, $p^J_{i\_opt}$ is a function of m, and $I_i(\mathbf{m})$ is the price update function for friendly jammer i.
  - The distributed algorithm can be expressed in a vector form as

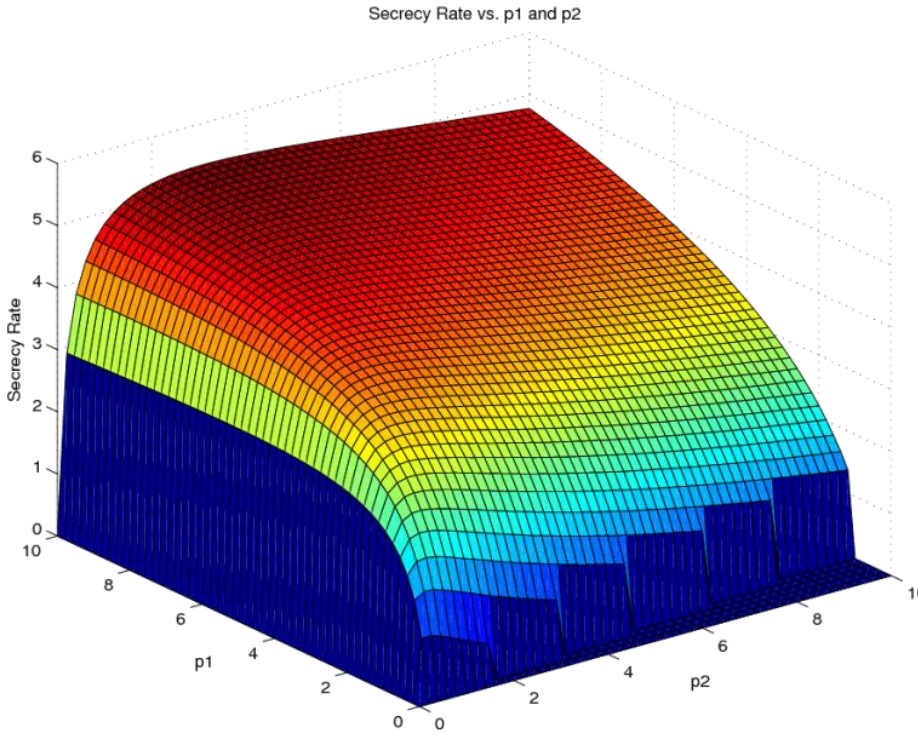
$$\mathbf{m}(t+1) = \mathbf{I}(\mathbf{m}(t))$$

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

Simulation Results

- ✓ **The Special Case without Jammers**



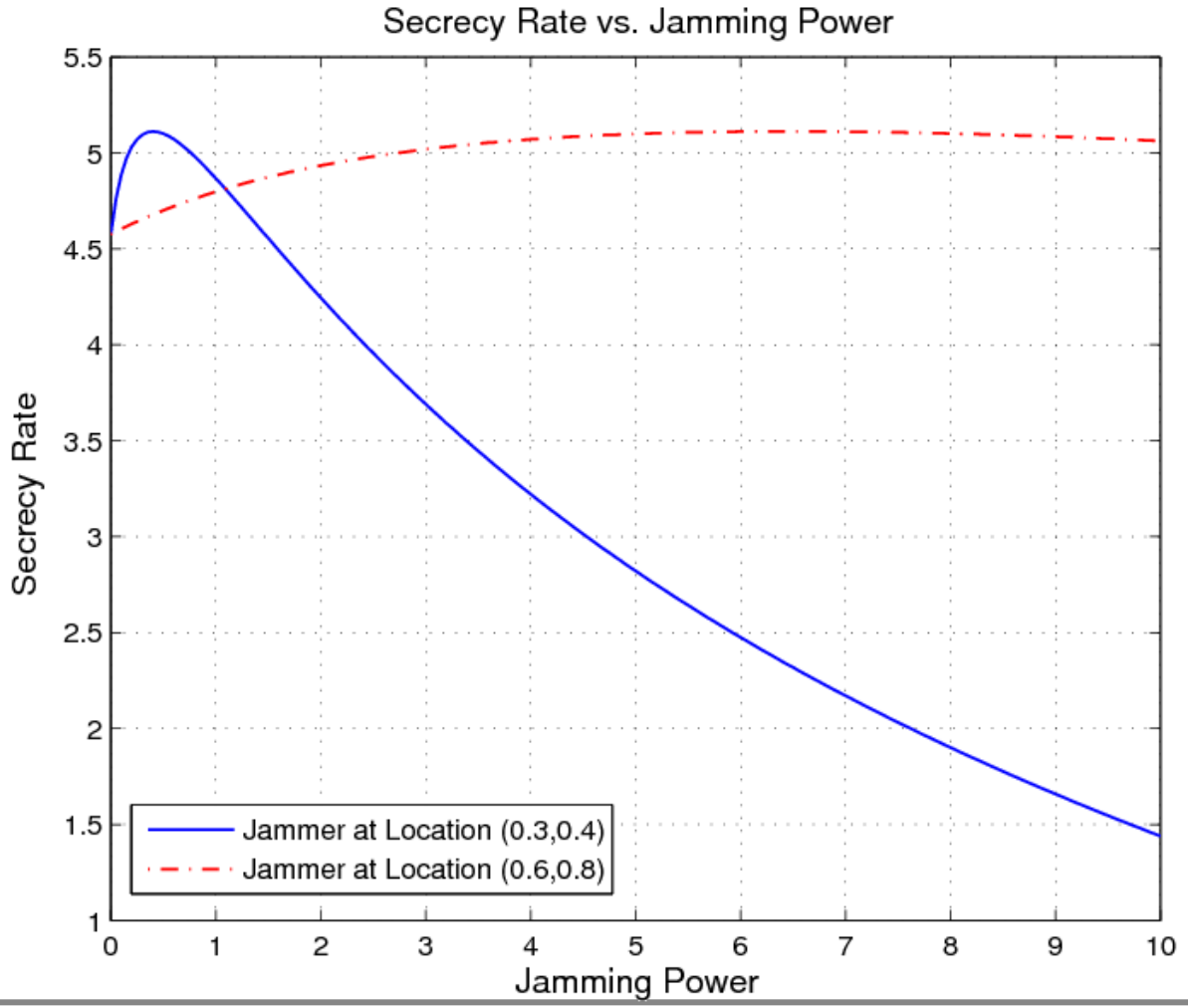


when $g_{S_1,R} > g_{S_2,R}$

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

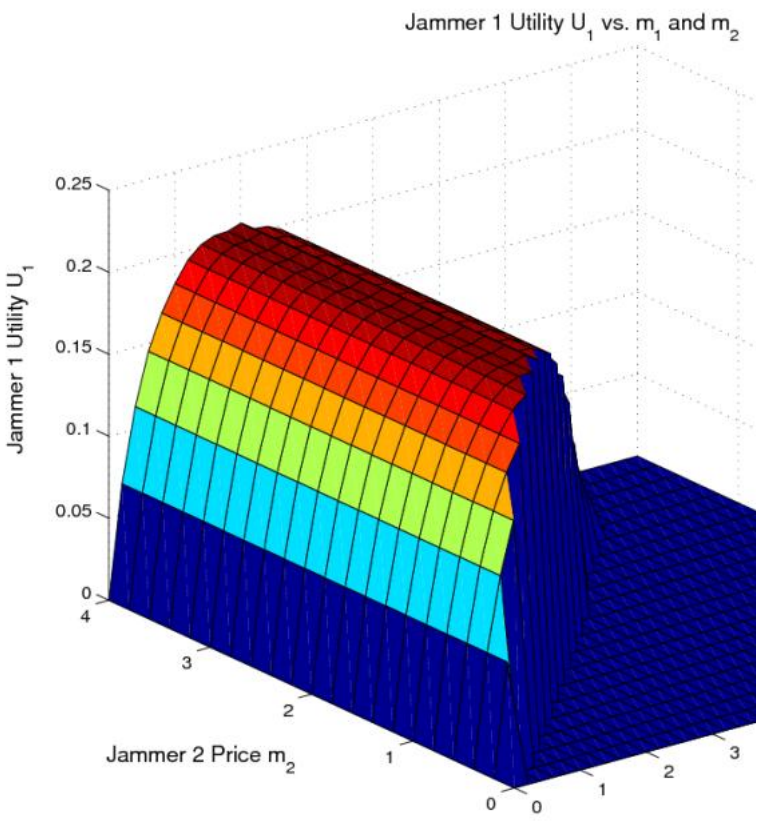
Simulation Results

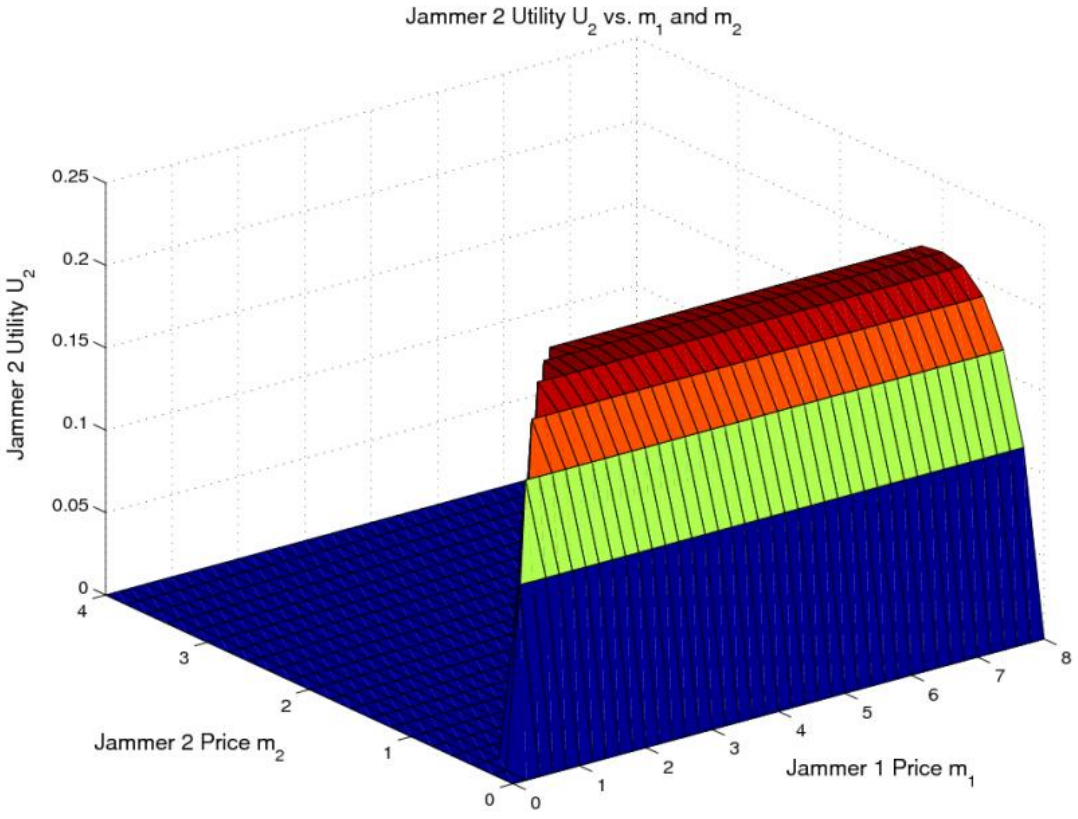
- ✓ **Secrecy rate vs. jamming power at different jammer locations**



Simulation Results

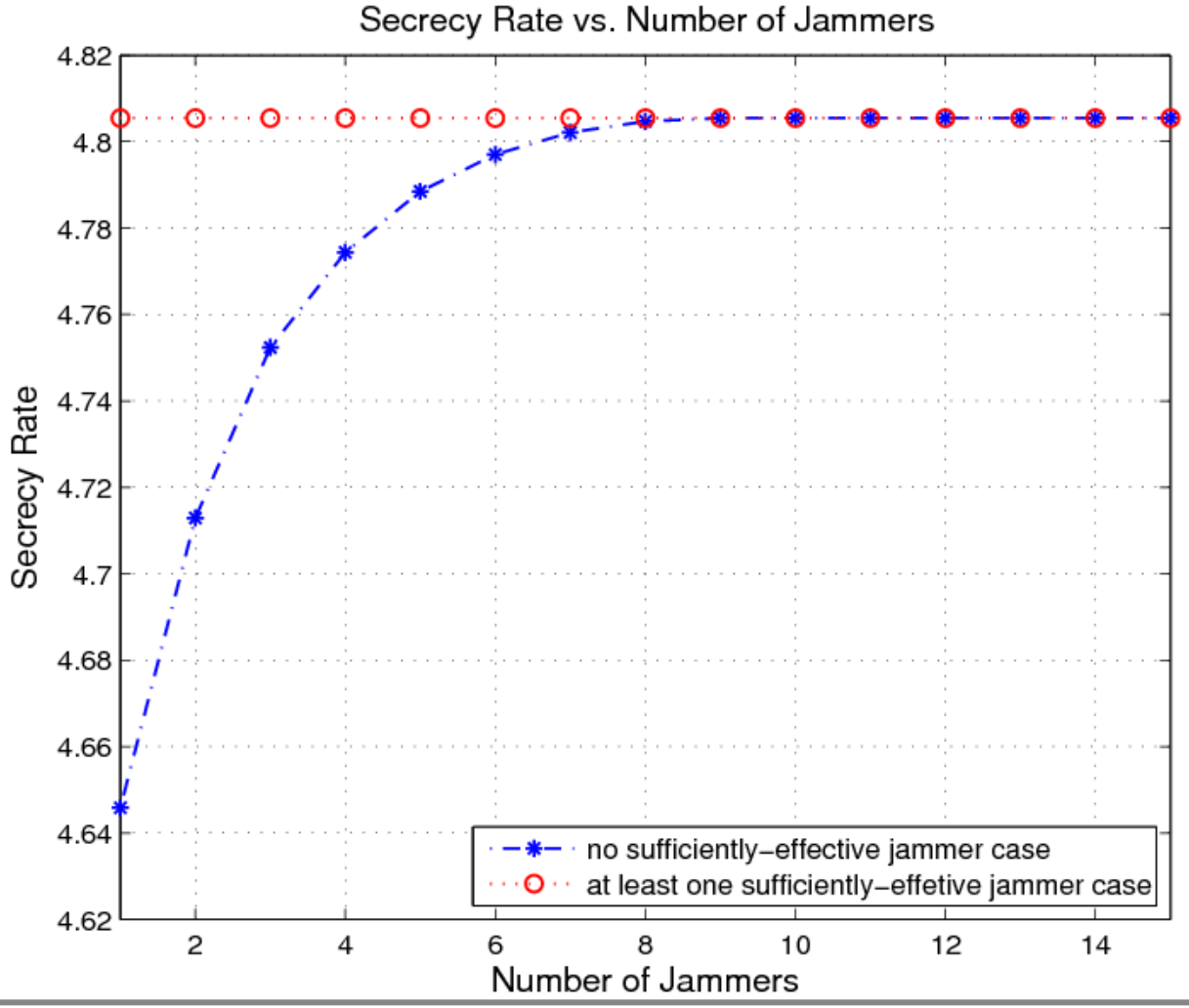
- ✓ **Multiple-Jammer Case**





Simulation Results

- ✓ **Multiple-Jammer Case**



Outline

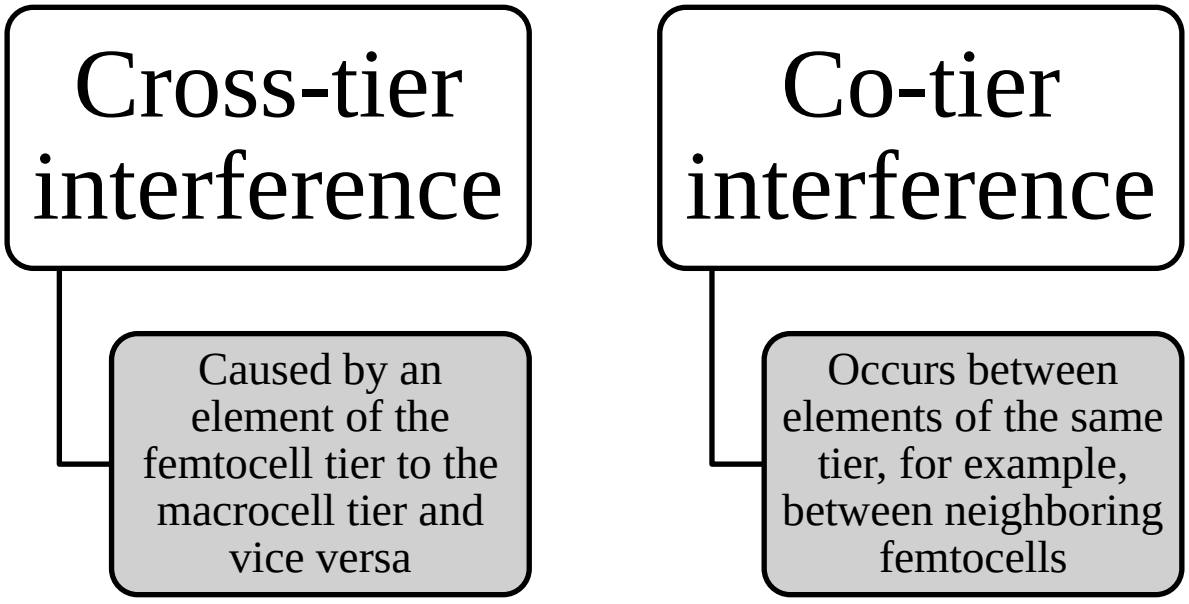
- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation Game Theoretical Study
- Variety of Applications
  - Cognitive Relay Network
  - Two-Way Relay Network
  - Femtocell Network
  - RFID
  - Satellite Network
- Conclusion

Truthful Mechanisms for Access Control in Femtocell Network

[1] Zhiqiang Feng, Jun Deng, Lingyang Song, and Zhu Han, “Joint Access Control and Subchannel Allocation Scheme for OFDMA Femtocell Network Using a Truthful Mechanism,” The first ACM international workshop on Practical issues and applications in next generation wireless networks (PINGEN'12), Istanbul, Turkey, Aug. 2012.

Introduction and Background

- ✓ **Interference in Femtocells**
  - The avoidance of interference is still an issue that needs to be addressed to successfully deploy a femtocell tier over existing macrocell networks.



Introduction and Background

✓ Access Control

Closed Access	Open Access	Hybrid Access
• Only a subset of users defined by the femtocell owner can connect to the femtocell	• All customers of the operator have the right to make use of any femtocell	• A limited amount of the femtocell resources are available to all users

Interference is strongly dependent on the type of access control.

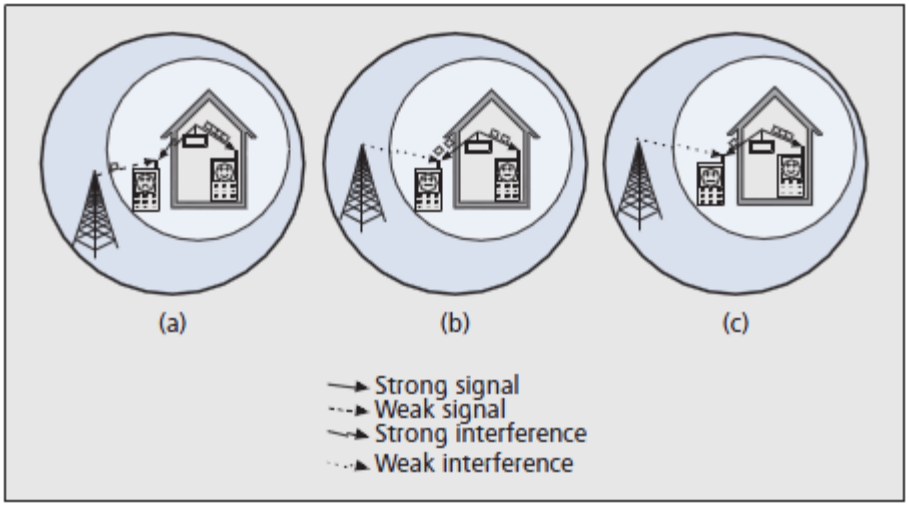


Fig. Three access control methods.

Introduction and Background

- ✓ Interference in different access controls

Closed Access

- Strong cross-tier interference exists between both tiers
- Co-tier interference also comes up between neighboring femtocells in dense deployments.

Open Access

- Avoid cross-tier interference but co-tier interference still exists.

Hybrid Access

- Both cross-tier and co-tier interference exist but not as strong as in the Closed Access scenario.

Introduction and Background

- ✓ Comparison between Closed Access Femtocells and Open Access Femtocells

Closed access femtocells	Open access femtocells
Higher interference	More handovers
Lower network throughput	Higher network throughput
Serves only indoor users	Increased outdoor capacity
Home market	SMEs, hotspots
Easier billing	Security needs

Table 1. *Closed vs. open access.*

Hybrid access methods reach a compromise between the impact on the performance of subscribers and the level of access granted to nonsubscribers.

Introduction and Background

- ✓ Access control mechanisms have a direct effect on interference.
- ✓ In Hybrid Access, the sharing of femtocell resources between subscribers and nonsubscribers needs to be finely tuned.
- ✓ Femtocells are mostly deployed by users and hybrid access may be one of the best access methods for users and service providers. However, femtocell owners do not have incentive to authorize others to use their own femtocells.
- ✓ Service providers shall pay femtocell owners for the access permission and in order to get more money, femtocells may not tell its true channel information.
- ✓ The AGV mechanism is a useful mechanism to guarantee truth-telling. So we try to use this mechanism to solve the truth-telling problems.

System Model

- ✓ We consider the system which contains N FAPs (femtocell access point) and M FUEs (femtocell user equipments). Each FAP contains K subchannels.

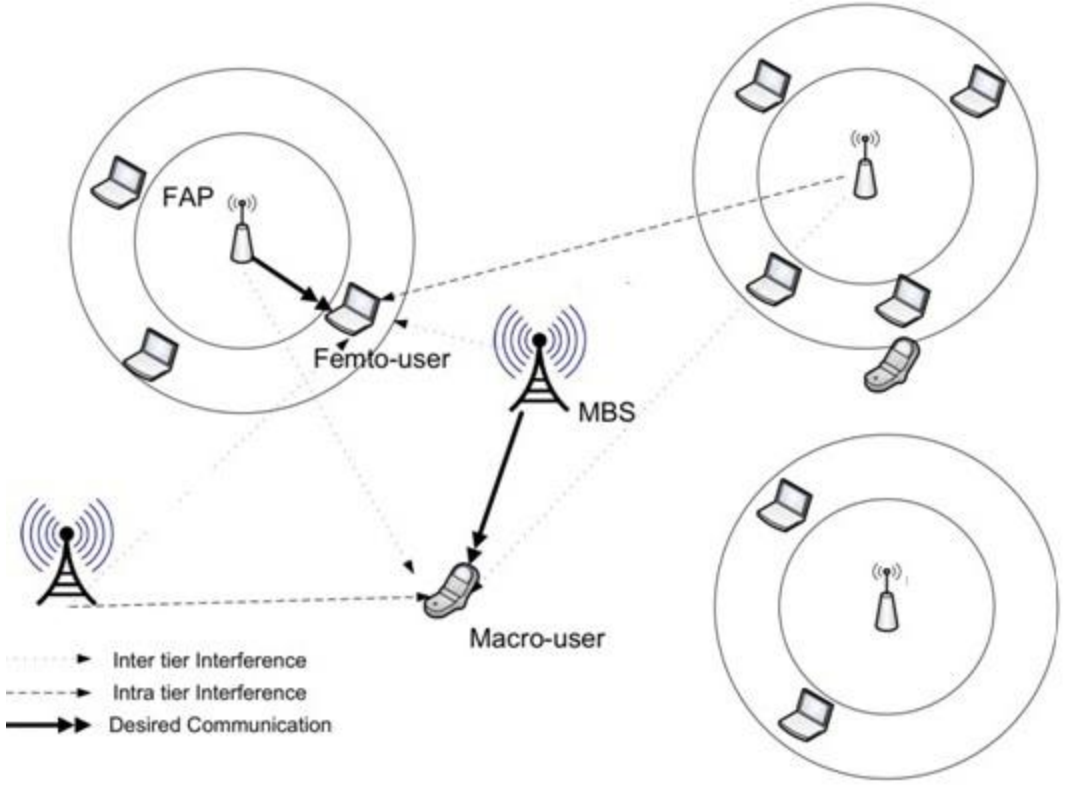
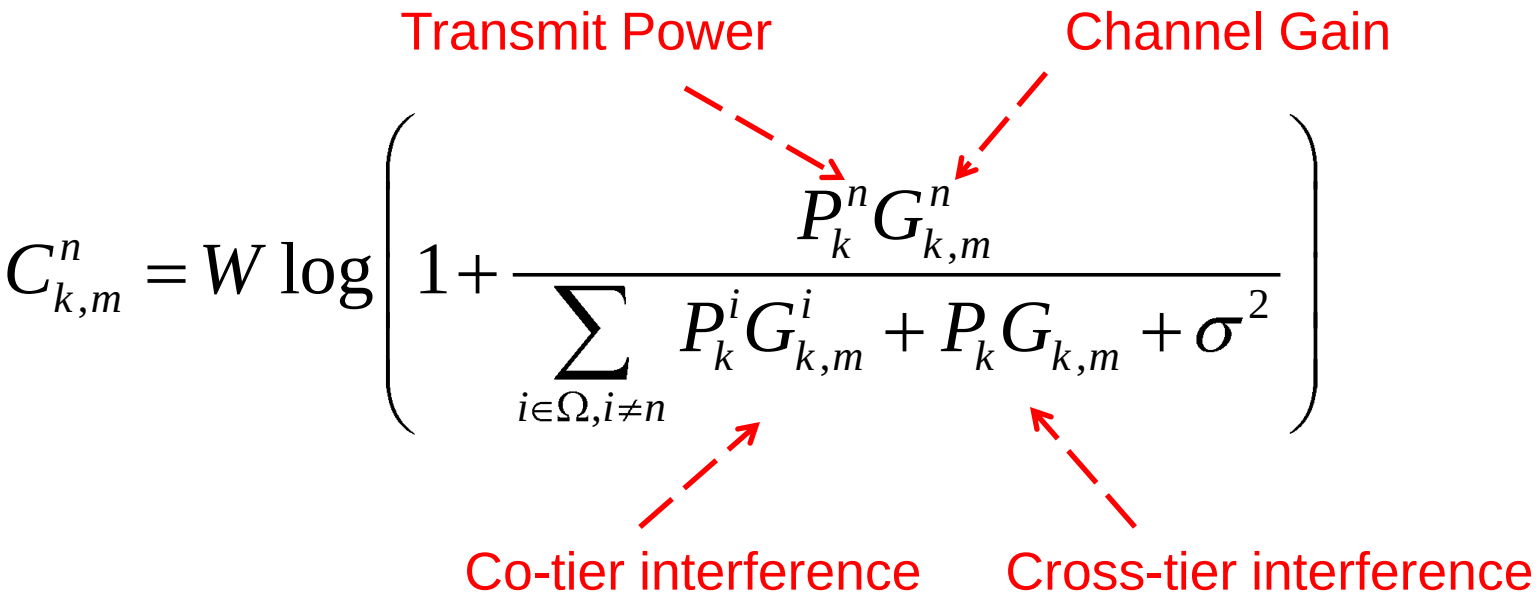


Fig. Two-tier femtocell system model.

System Model

- ✓ For FUE m, the Capacity of the kth subchannel of the nth FAP can be written as



System Model

- ✓ **Problems**
  - FAPs are willing to give as many access permissions as possible to FUEs to earn money. Their access permission is determined by their channel capacity.
  - FUEs want to get best service so they prefer larger channel capacities.
  - Service providers want to give proper money to FAPs which can really help them offload the data in the macrocell base stations.
  - We try to use AGV mechanism to guarantee FAPs tell their true information so that FUEs can choose the best femtocells and maximize throughput of the whole system in the meantime.

AGV Game Preliminaries

✓ **AGV Mechanism**

- An extension of the Groves mechanism (a kind of effective mechanism in auction theory).
- Can solve the truth-telling problem.
- Can achieve Bayesian Nash Equilibrium when all the FAPs reveal the truth.
- Can be budget balanced (i.e., the total transfer payment of all the relay nodes equals to zero).

Game Setup

- ✓ **Algorithm based on AGV mechanism**
  - The payoff of FAP n to FUE m can be expressed as

$$D_m^n = \pi \tilde{C}_m^n P \quad FAP_n \in \Omega_m$$

$$P \quad FAP_n \in \Omega_m \quad \propto \hat{C}_m^n$$

  - where $P \quad FAP_n \in \Omega_m$ means the possibility that FAP n is chosen by FUE m, π is the price per unit of capacity.
  - There is no balance because every FAP will report their capacity as large as possible.
  - By using a transfer function (according to the AGV mechanism) to balance the payoff allocation, FAP n can gain its largest expected total payoff only when it reports its true channel information

Game Setup

- ✓ **Utility Function：**
  - The payoff of FAP n to FUE m can be expressed as

$$D_m^n = \pi \tilde{C}_m^n P \quad FAP_n \in \Omega_m$$

  - Transfer payoff of FAP i to FUE m:

$$t_m^i \left(\hat{C}_m^1, \hat{C}_m^2, ..., \hat{C}_m^N \right) = \Phi_m^i \left(\hat{C}_m^i \right) - \frac{1}{N-1} \sum_{j=1, j \neq i}^{N} \Phi_m^j \left(\hat{C}_m^j \right)$$

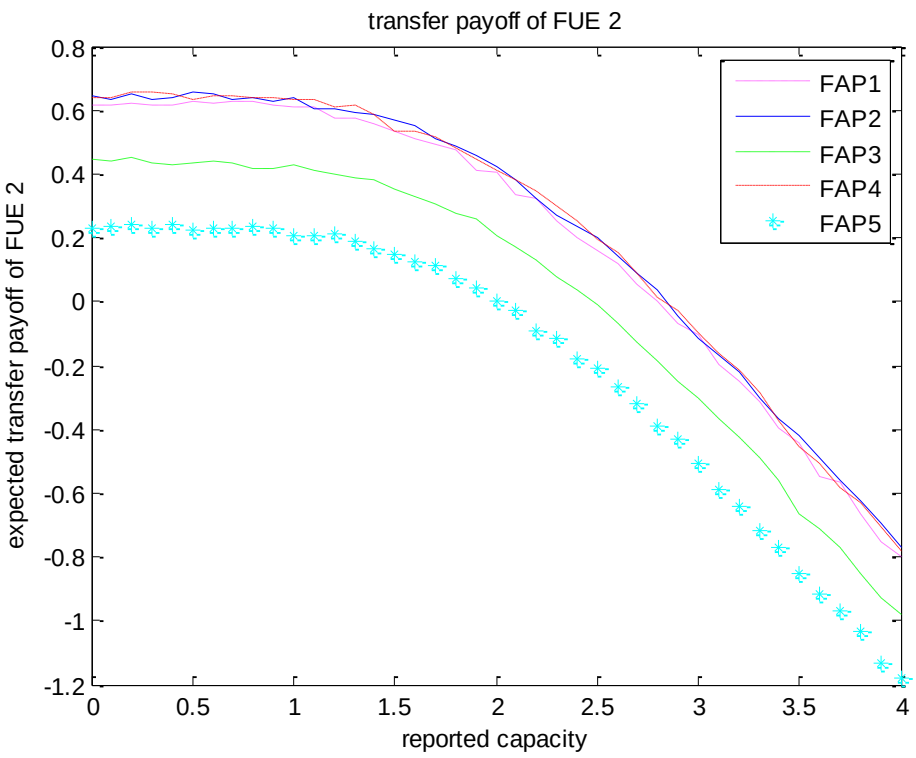
$$\Phi_m^i \left(\hat{C}_m^i \right) = \sum_{j=1, j \neq i}^{N} E\left[D_m^j \left(\hat{C}_m^i \right) \right]$$

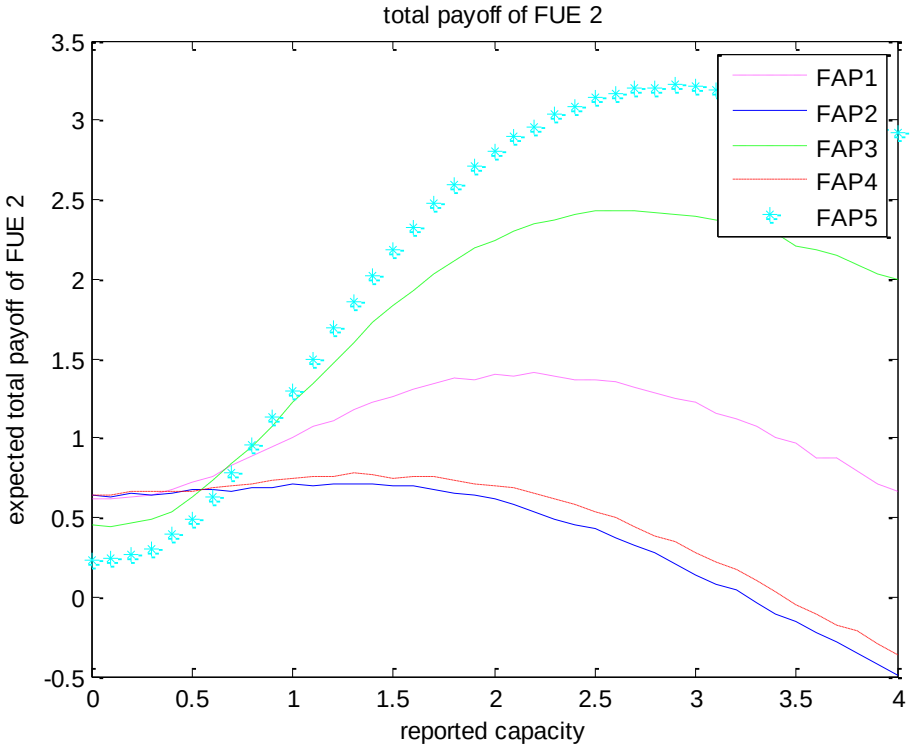
  - Total payoff of FAP i to FUE m:

$$U_m^i \left(\hat{C}_m^i \right) = D_m^i \left(\hat{C}_m^i \right) + t_m^i \left(\hat{C}_m^1, \hat{C}_m^2, ..., \hat{C}_m^N \right)$$

Simulation Results

- ✓ The transfer function are monotone decreasing because the larger the reported capacity is, the more transfer payoff they should be paid.
- ✓ Given that the other FAPs are honest, FAP i could get its maximum total payoff when reporting the truth.

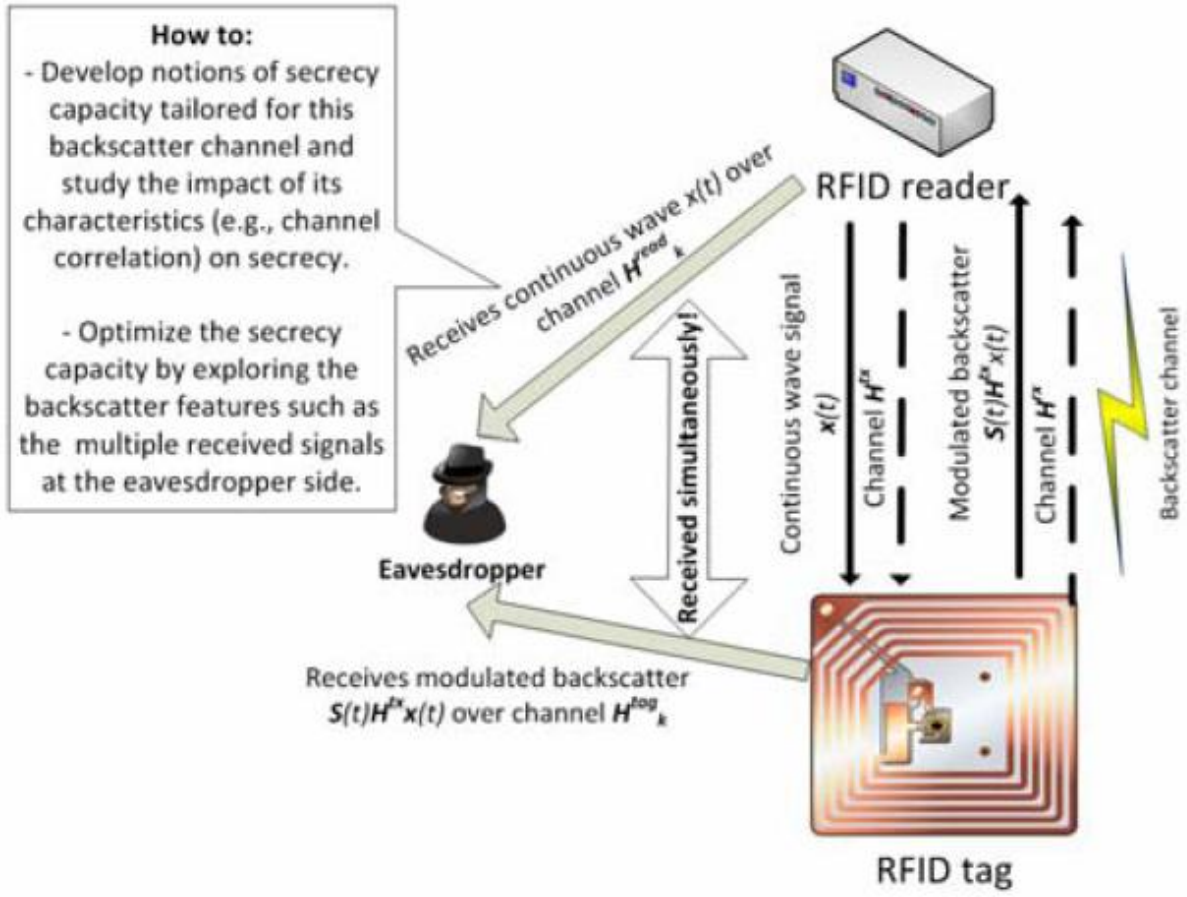




Outline

- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation Game Theoretical Study
- Variety of Applications
  - Cognitive Relay Network
  - Two-Way Relay Network
  - Femtocell Network
  - RFID
  - Satellite Network
- Conclusion

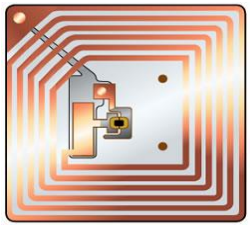
RFID



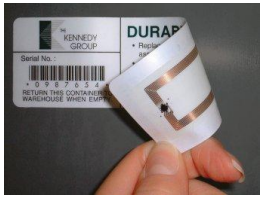
Walid Saad, Zhu Han, and H. Vincent Poor, "On the Physical Layer Security of Backscatter RFID Systems," invited, The Ninth International Symposium on Wireless Communication Systems, Paris, France, August 2012.

RFID Systems

- A Radio Frequency Identification (RFID) system is composed of two key components
  - **RFID tag:** electronic device that can store and transmit data to a reader in a contactless manner
  - **RFID reader:** Transceiver that can read and communicate with RFID tags



RFID tag

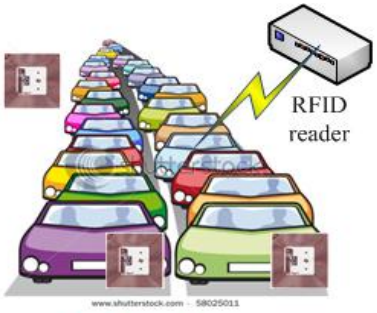


RFID Systems

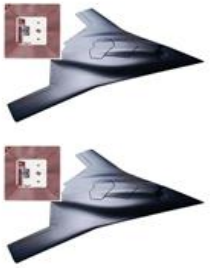
- Three types of RFID tags
  - **Passive:** cheapest – does not include any power source, harvests energy from the reader
  - **Semi-Passive**: can include some basic sotrage elements as well as a possible small battery to power the circuitry (but **not** for TX)
  - **Active:** has transmission capabilities – basically a small sensor
- Two main technologies
  - **Near-field communication (NFC):** operate at very short distances, e.g., few centimeters, over HF frequencies (i.e., 13.56 MHz).
  - **Ultra high frequency (UHF) RFIDs:** operate at UHF frequencies (typically 433 MHz), can be used at longer ranges (10 meters is common but recent research is looking at larger distances)

RFID Applications

RFID for smart tire, maintenance, etc.

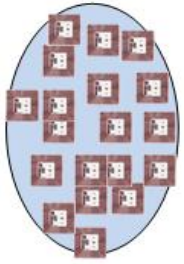


RFID for luggage tracking and managing.



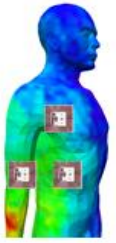
RFID in aviation, navigation, UAV, etc.

Automotive, aviation (automation), and transportation systems



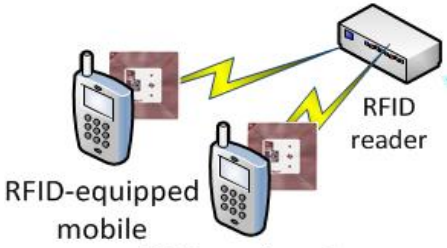
Dense smart dust

RFID in hospitals

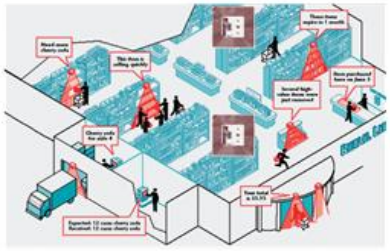


Body area network

Sensing and healthcare



Autopay and supply chain

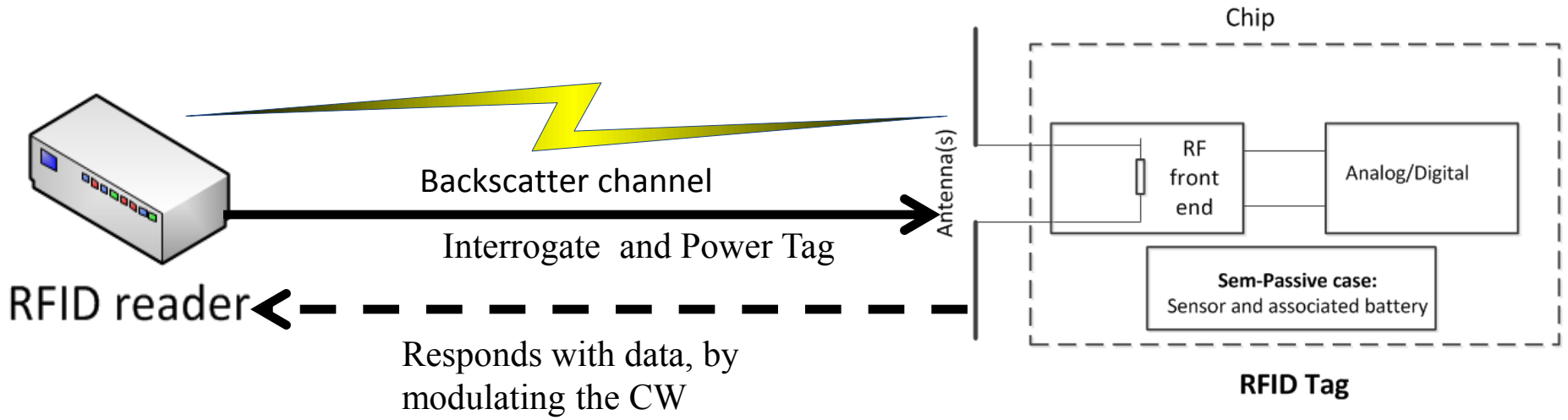


RFID in malls

RFID for inventory

Mobile RFID, payment systems, automated supply chain, and inventory control

Basic RFID Communication



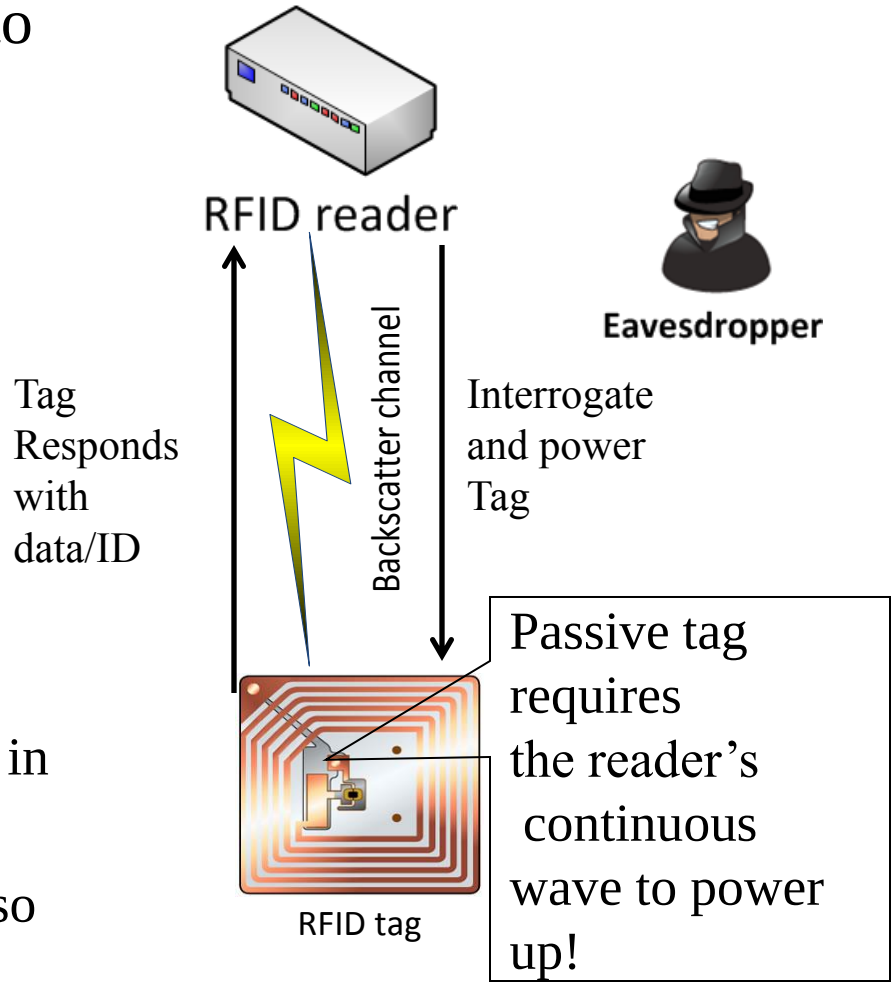
- **Reader** transmits a continuous wave (CW) carrier signal
  - Induces an RF voltage across the tag antenna that is converted to DC by a power harvesting circuit to power the tag's circuitry and demodulate the received command
- **Tag** transmits back its stored information by controlling the amount of **backscatter** of the impinging downlink signal by varying the impedance (mis)-match of the antenna front-end
  - Role of the reader in **energizing** the tag

RFID Backscatter: Challenges

- Tags must remain cheap and passive tags must harvest energy
  - Limitations on circuit design.
  - Design of innovative RFIDs is a key challenge.
- The uplink tag-to-reader communication has a strictly limited bandwidth due to limited backscatter power and tag collisions
  - How to improve the uplink communication?
  - Crucial to allow higher distances, better rate, and new applications!
- **Security** is probably the most critical issue
  - **Fact:** Classical cryptography cannot be implemented on RFID tags
  - Current solutions (lightweight cryptography) are non-scalable and still present many vulnerabilities
  - Big motivation for security solutions that can be implemented with little complexity => **Physical layer security!**

Presence of Eavesdroppers

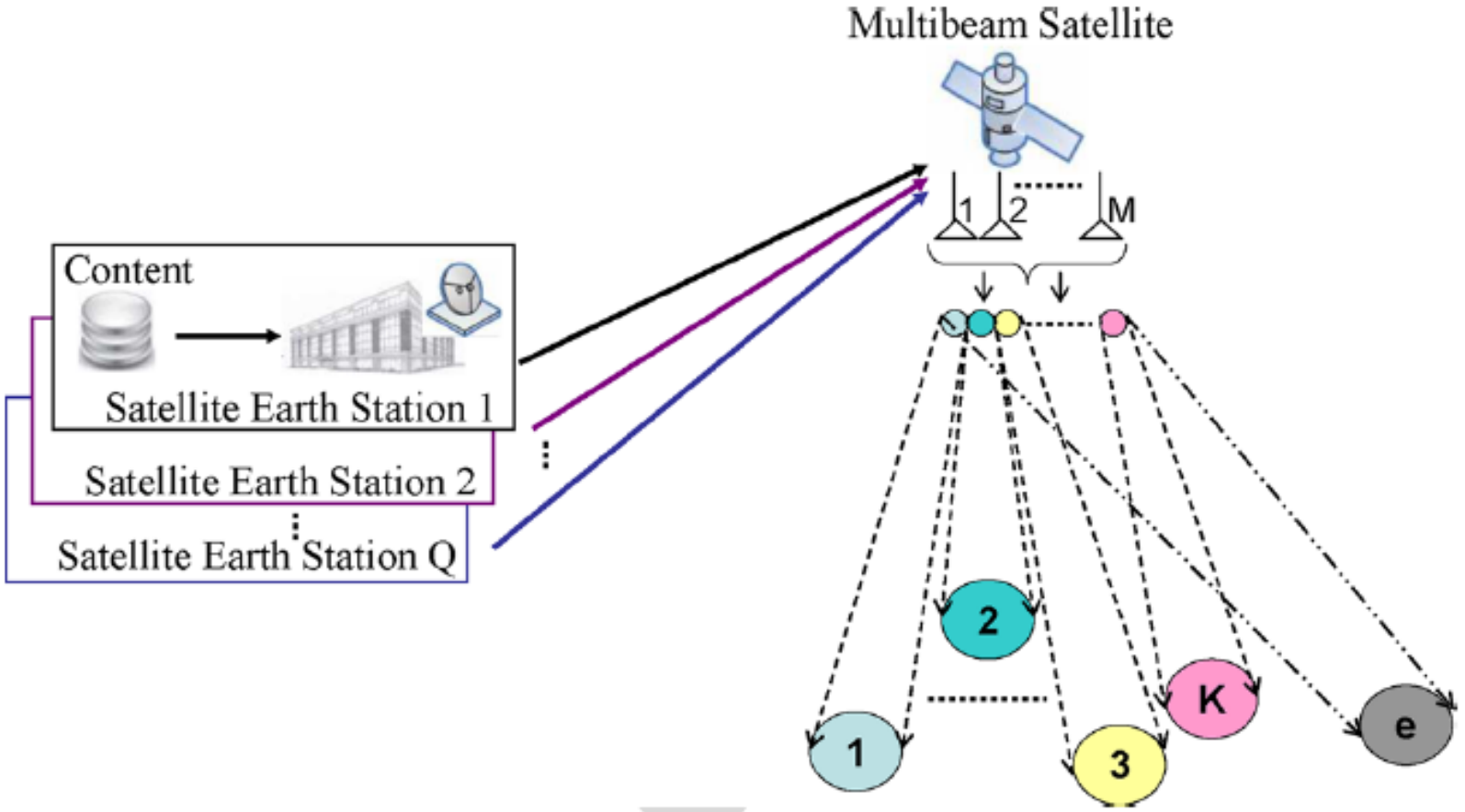
- A nearby eavesdropper can tap into the communication
- Classical cryptography cannot be implemented on RFID tags
  - PHY security in RFID: research frontier, no works done yet!
- Backscatter features
  - Eavesdropping is useful at close distances
  - Eavesdroppers are mainly interested in the uplink signal/tag data
  - The downlink reader-tag signal is also received by the eavesdropper during backscatter



Outline

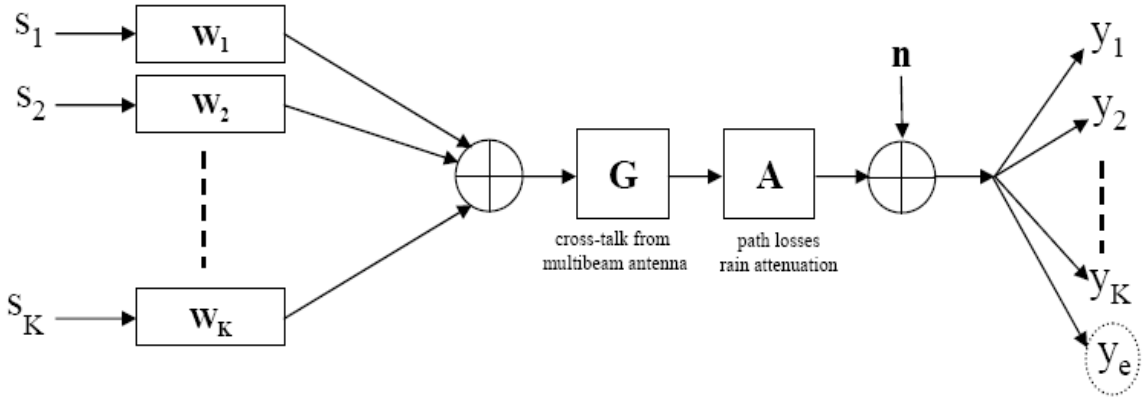
- Overview of Physical Layer Security
- Information Theoretic Fundamentals
- Signal Processing Technique
- Resource Allocation Game Theoretical Study
- Variety of Applications
  - Cognitive Relay Network
  - Two-Way Relay Network
  - Femtocell Network
  - RFID
  - Satellite Network
- Conclusion

Satellite Network



Jiang Lei, Zhu Han, M. A. Vazquez-Castro, and Are Hjorungnes, "Multibeam Satellite Power Control and Beamforming with Individual Secrecy Rate Constraints," *IEEE Transactions on Information Forensics and Security*, Special Issue on Using the Physical Layer for Securing the Next Generation of Communication Systems, vol. 6, no. 4, pp.661-671, Sept. 2011.

Matrix Model of Satellite Broadcast Channel



- The signals received by the kth user can be expressed as desired signal and interference as

$$y_k = \sqrt{P_k}\mathbf{h}_k^T\mathbf{w}_k s_k + \sum_{j\neq k}\sqrt{P_j}\mathbf{h}_k^T\mathbf{w}_j s_j + n_k,$$

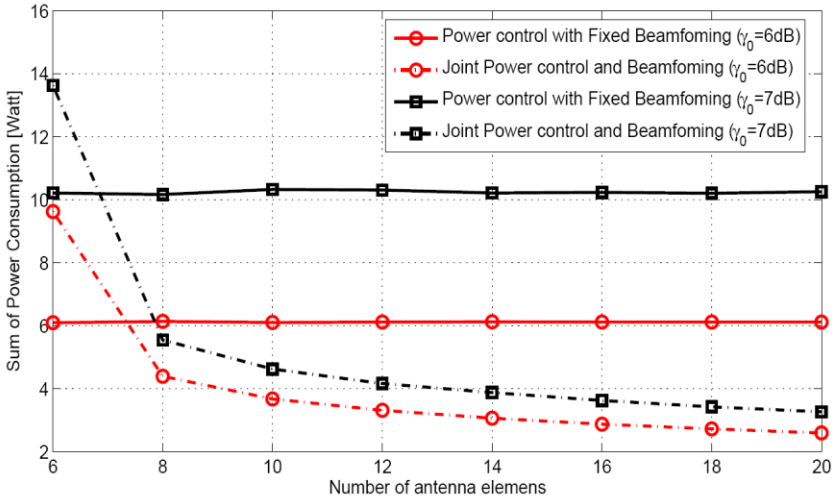
- The signal received by the eavesdropper is given as

$$y_e = \sqrt{P_k}\mathbf{h}_e^T\mathbf{w}_k s_k + \sum_{j\neq k}\sqrt{P_j}\mathbf{h}_e^T\mathbf{w}_j s_j + n_e,$$

1. How to realize security communication between satellite and legal users by beams cooperation?
2. A novel power control problem is studied taking into account both the co-channel interference and the eavesdropping interference.
3. Minimize the total power consumption subject to the individual target secrecy rate.

Selected Results

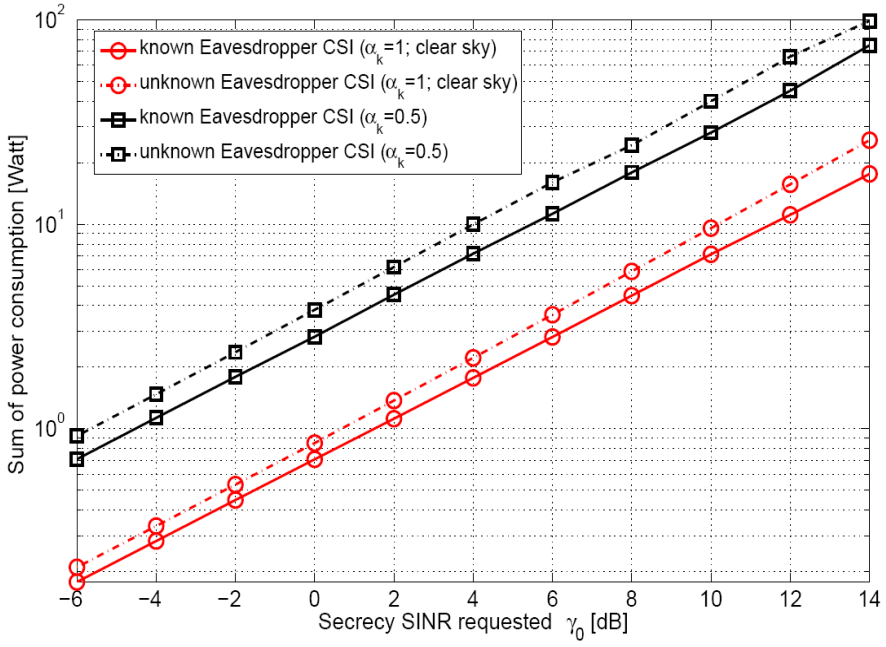
- Number of antenna elements Vs. Power consumption



- This figure shows the power consumption versus the number of antenna elements;
- For the joint power and beamforming case, the performance is better in the case larger number of antenna elements;
- For the power control with fixed beamforming, the power consumption is almost constant.

Selected Results

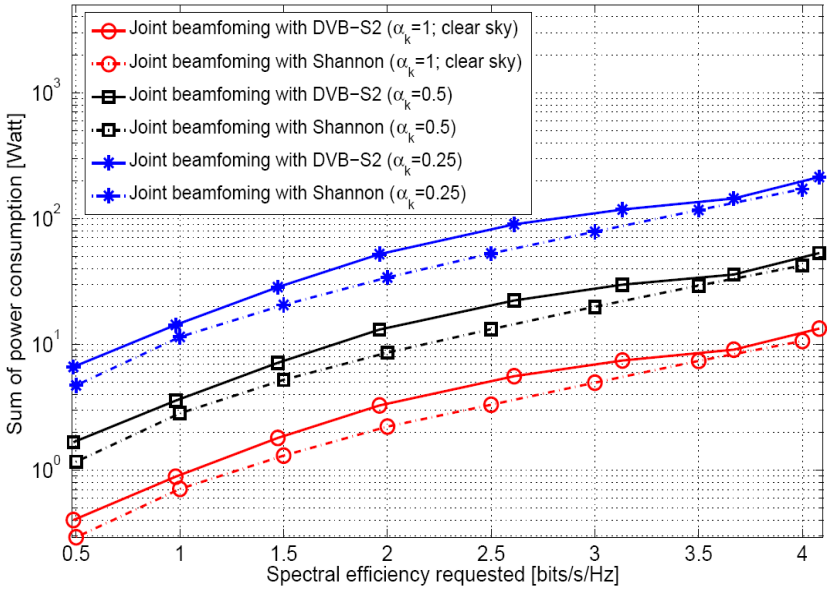
- Power allocation with or without the available the eavesdropper CSI



  - Under the given total power limitation (e.g., 100 Watts), the achieved secrecy SINR per user with known eavesdropper's CSI performs about 2 dB better than the case of no CSI available. In addition, this gap increases as the available total power increases.

Selected Results

- Total transmitted power comparison for the DVB-S2 air-interface and Gaussian inputs



  - For the case of the joint beamforming scheme, the sum of power consumption increases as the spectral efficiency requirement increases for both Gaussian inputs and DVB-S2 cases. The power consumption of the DVB-S2 case is always larger than the Gaussian inputs case, and the gap between them tends to decrease as the spectral efficiency increases.

Conclusions

- Wireless physical layer security is an alternative.
- Collaborative beamforming and jamming can improve secrecy performance.
- Game theory is a useful tool to allocate the system resources, e.g., transmit power, for security enhancement.
  - Coalition game: Collaborative beamforming;
  - Stakelberg game and Auction: Cooperative (Friendly) jamming;
  - Cross-layer optimization can further improve performance: subcarrier, space, and power
- Resource Allocation Perspective
  - Variety of applications such as cognitive radio, femtocell, relaying networks, the security problem can be leveraged by properly allocating the system resources.

Questions?

Thank you very much