STEVENS
Institute of Technology

Secrecy Capacity for Multi-terminal Networks with Pricing

Anand Santhanakrishnan

asanthan@stevens.edu

Multimedia System, Networking, and Communications (MSyNC) Laboratory,

Department of Electrical and Computer Engineering,
Stevens Institute of Technology

(joint work with **R. Chandramouli**)

CHARLES V. SCHAEFER, Jr.
SCHOOL OF ENGINEERING
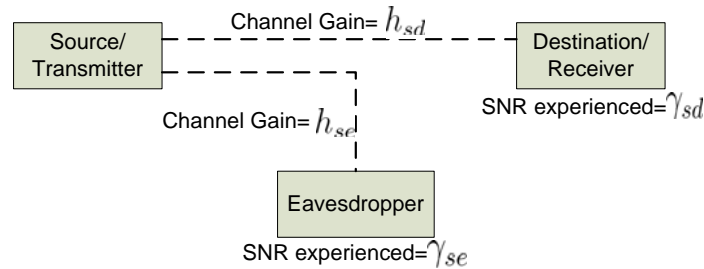
STEVENS
Institute of Technology

Outline

- Introduction to Secrecy Capacity
- Prior Work
- Motivation
- Problem Formulation
- Key Contributions
- Results
- Some Applications
- Conclusion and Future Work

2

STEVENS
Institute of Technology

Introduction to Secrecy Capacity (1/5)

Source/ Transmitter	Channel Gain= h_{sd}	Destination/ Receiver

SNR experienced= γ_{sd}

Channel Gain= h_{se}

Eavesdropper

SNR experienced= γ_{se}

3

STEVENS
Institute of Technology

Introduction to Secrecy Capacity (2/5)

- Studied for systems with "key-less" security (more a PHY aspect)
- Consider a system with a source, destination and eavesdropper
  - Eavesdropper is "passive", i.e., eavesdropper does not transmit any signal with the intention of jamming the destination
  - Eavesdropper only "listens" to the information transmitted by the source
- The channel between the source and destination is called the "**main channel**"
- The channel between the source and eavesdropper is called the "**eavesdropper channel**"

4

STEVENS
Institute of Technology

Introduction to Secrecy Capacity (3/5)

- Is it possible for the source to transmit in such a way that the information can be received properly by the destination but not by the eavesdropper?
  - This question is answered by measuring the "secrecy capacity"

5

STEVENS
Institute of Technology

Introduction to Secrecy Capacity (4/5)

- Secrecy Capacity is the maximum rate at which the source can transmit such that the BER at the destination is 0 and BER at the eavesdropper is 1/2
  - Does such a rate exist?
- For AWGN and MAI channels, Secrecy capacity can be computed the difference between the Shannon capacity of the main channel and that of the eavesdropper channel

6

Introduction to Secrecy Capacity (5/5)

- Let the Signal-to-Noise ratio (SNR) seen by the destination be γ_{sd} and that seen by the eavesdropper be γ_{se}.
- The Secrecy capacity, C_s, for a system with bandwidth W is given by

$$C_s = \left[W \log_2 \left(\frac{1+\gamma_{sd}}{1+\gamma_{se}} \right) \right]^+$$

- $x^+ = \max(0, x)$

7

A Numerical Example (1/2)

- Let $h_{sd} = 0.8$ and $h_{se} = 0.1$
- Let source transmit power $P_s = 2 \text{ Watts}$
- Let the bandwidth $W = 5 \text{ Mhz}$
- Let the AWGN power spectral density
  $N_0 = 10^{-14} \text{ Watts/Hz}$

8

A Numerical Example (2/2)

- $\gamma_{sd} = \frac{P_s h_{sd}}{N_0 W}$ and $\gamma_{se} = \frac{P_s h_{se}}{N_0 W}$
- Secrecy Capacity $C_s \approx 15 \text{ Mbps}$
- Shannon capacity of the main channel
  $C_{sd} \approx 142 \text{ Mbps}$
- If $h_{se} = 0.9$, then $C_s = 0$

9

Prior Work

- Studies on secrecy capacity classified into 3 categories
  - Single source-single destination-single eavesdropper
  - Using relay nodes to enhance the secrecy capacity
  - Multiple sources-multiple destination-single eavesdropper
- For systems with security key, co-operation between multiple terminals for generating a security key was studied

10

Single source-single destination-single eavesdropper

- Scenario as shown in slide 3
  - Full information about the main channel as well as eavesdropper channel
    - The source h_{se}^- knows all the statistics of   as well as
  - Information about main channel alone available
    - The source knows all the statistics of h_{sd} alone
  - Information of neither the main channel nor eavesdropper channel available
  - Determine the transmit power of the source, such that secrecy capacity is maximum such P_s that average power $\leq P_{ave}$

11

Systems with a Relay Node
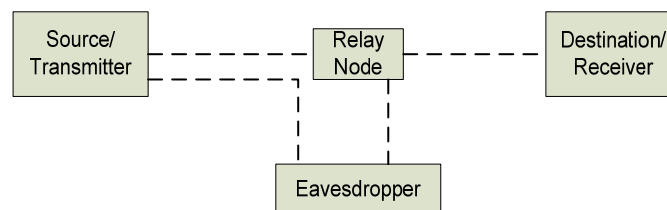
- Relay node receives the signal from the source and retransmits to the destination
- The relay node randomly transmits code-words NOT in the code book of the receiver so as to "confuse" the eaves dropper

12

Multiple-sources and destinations

- Multiple transmitters and receivers
- Single eavesdropper
- The objective was to obtain the transmit powers for the transmitters so as to maximize the total secrecy capacity of all the transmit-receiver pairs
- Solution obtained- All transmitters whose receivers experience positive secrecy capacity transmit at maximum power. All other transmitters turn off
- A set of transmitters co-operate and transmit such that the eavesdropper suffers large interference (called as "co-operative jamming")

13

Motivation for the problem

- Secrecy capacity for multiple transmit receive pairs not studied in detail
- Current formulations for multiple transmitters and receivers result in a subset of transmitters transmitting at maximum power
  - Not energy efficient
- Need to design systems such that the transmit powers are small and yet maximize the secrecy capacity
- Penalize transmitters transmitting with higher power

14

STEVENS
Institute of Technology

Key Contributions

- First formulate the secrecy capacity maximization problem as an *n* person non co-operative game
- Obtain conditions for Pareto optimality and the Nash equilibrium
- Introduce a pricing function to penalize users transmitting with higher power
  - A non-linear pricing function
  - A linear pricing function
- Solve the game with pricing to obtain the optimal powers to maximize the secrecy capacity
- Provide conditions under which a unique Nash equilibrium exists

15

STEVENS
Institute of Technology

System Model (1/2)

- We consider a system with M transmit receiver pairs and one eavesdropper
- Transmitter i transmits at power P_i and rate r_i
- The system has bandwidth W
- Each transmitter has a maximum transmit power
- Receiver i has gain G_i. If gain is due to spectrum spreading then $G_i = \frac{W}{r_i}$
- The SIR experienced by receiver i is x_i
- The AWGN power spectral density is N_0

16

System Model (2/2)

- The channel gain from transmitter i to receiver j is h_{ij}
- The channel gain matrix is $\mathbf{H} = [h_{ij}]_{\substack{1 \leq i \leq M \\ 1 \leq j \leq M}}$
- The channel gain from transmitter i to the eavesdropper is h_{ie}.
- The channel gain vector to the eavesdropper is denoted by $\mathbf{h}_e = [h_{ie}]_{1 \leq i \leq M}$

17

Problem Formulation

- The objective is to determine the transmit powers of all the transmitters so that
  - The secrecy capacity seen by each receiver is maximum
  - The sum secrecy capacity of all the receivers is maximum
- First assume that there is no eavesdropper
- Determine the transmit powers of all the transmitters so that the Shannon capacity of all the channel between each transmit-receiver pair is maximized
- Then show that this also maximizes the secrecy capacity of each transmit-receiver pair

18

A Typical Scenario

19
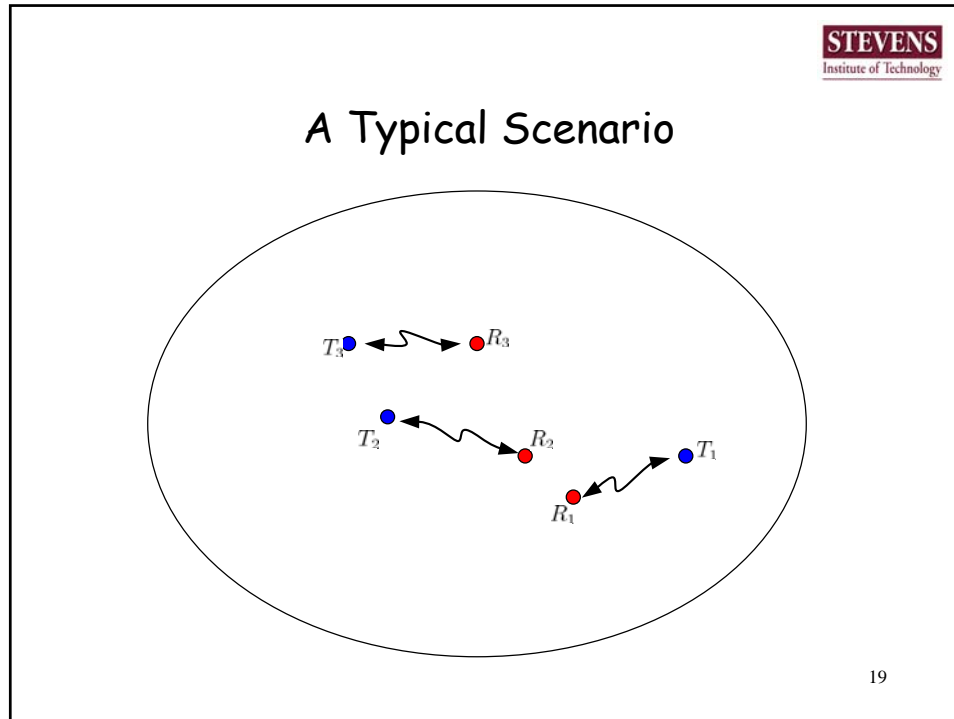
System with No Eavesdropper

- The Shannon capacity of the channel between the transmit-receiver pair i , C_i ,is given by
$$C_i = W \log_2(1 + x_i).$$

- The SIR experienced by receiver i is given by
$$x_i = \frac{P_i h_{ii} G_i}{\sum_{j \neq i} P_j h_{ji} + N_0 W}$$

- It is required to maximize $C_i, \ \forall \ i$ such that
$$0 \leq P_i \leq P_{max}, \ \forall \ i$$

- Note that the capacity of transmit-receiver pair i depends on the transmit powers of all the transmitters

20

Game Theoretic Formulation (1/3)

- The players are the transmit-receive pairs
- The strategy for each transmitter i is the transmit power P_i. The strategy set for transmitter i is the interval $[0, P_{max}]$
- Need to define the utility function
  - Needs to be a non-decreasing function
  - Needs to be a concave function
  - Needs to satisfy the law of diminishing marginal utility
    $\lim_{\alpha \to \infty} \frac{du}{d\alpha} = 0$
- The Shannon Capacity function C_i satisfies the above mentioned properties with respect to the SIR x_i

21

Game Theoretic Formulation (2/3)

- Need to obtain the Nash equilibrium and the Pareto optimal points for the game
- Theorem 1:

  A power vector $\mathbf{p} = \begin{bmatrix} P_1 & P_2 & P_3 & \cdots & P_M \end{bmatrix}$ is Pareto optimal if and only if $P_i = P_{max}$ for some i

- Implication of Theorem 1:
  - At least one transmitter transmits at maximum power
  - If all transmitters transmit at powers less than maximum, then it is possible to obtain an improvement in the capacity (utility) of all the transmit-receive pairs

22

STEVENS
Institute of Technology

Game Theoretic Formulation (3/3)

- Theorem 2:

  The Nash equilibrium of the Shannon capacity maximization occurs when $P_i = P_{max}, \forall\ i$. This equilibrium point is also Pareto optimal.

- Implication of Theorem 2:
  - All transmitters transmit at maximum power
  - Not energy efficient
  - Need to look at means to improve energy efficiency

23

STEVENS
Institute of Technology

Pricing based approach

- Formulate a pricing function
  - Pricing function should increase the penalty to users transmitting at higher power
  - However, it is the SIR that provides higher capacity to transmit-receive pairs
- We propose 2 pricing functions
  - Non-linear
  - Linear
- Our intuition
  - Imposing a price on transmit receive-pairs forces transmitters to transmit at lesser power
  - This decreases the signal to the eavesdropper thus improving the secrecy capacity for some receivers

24

Non-linear Pricing: Motivation

- Two scenarios occur
    1. A transmitter transmits at higher power to achieve a minimum BER
    2. A transmitter transmits at higher power to improve an already large SIR
- Case 2 mentioned above needs to be penalized higher penalty than those case 1

25

Pricing Functions

- Non Linear Pricing function
    - Compute the total power at a receiver .
    - Find what percentage of this received power is obtained from transmitter
    - Price higher if the above percentage is larger
    - If the percentages are equal, then price higher if transmission rate is higher

$$f_i(\mathbf{p}) = \lambda \frac{r_i P_i h_{ii}}{\sum_{j=1}^{M} P_j h_{ji} + N_0 W} = f_i(x_i) = \lambda \frac{r_i x_i}{x_i + G_i}$$

- Linear Pricing function
    - Price higher if SIR is larger. If SIR's are equal, then price higher if transmission rate is higher

$$f_i(x_i) = \lambda r_i x_i$$

26

Optimization with pricing (1/3)

- Maximize $C_i(\mathbf{p}) - f_i(\mathbf{p}) \ \forall \ i$ such that $0 \leq P_i \leq P_{max} \ \forall \ i$
- Note that C_i and f_i are functions of x_i
- Formulate the power allocation problem as an SIR allocation problem
  - Determine x_i that maximizes $C_i - f_i(P_i) \ \forall \ i$
  - From the SIR vector $\mathbf{x} = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_M \end{bmatrix}$ obtain the power vector $\mathbf{p} = \begin{bmatrix} P_1 & P_2 & P_3 & \cdots & P_M \end{bmatrix}$
  - Need to solve a system of equations given by the matrix equation

$$\mathbf{p} = N_0 W \left(\mathbf{I}_M - \mathbf{D}_1^{-1} \mathbf{A} \right)^{-1} \mathbf{D}_1^{-1} \mathbf{D}_2^{-1} \mathbf{1}$$

27

Optimization with pricing (2/3)

$$\mathbf{A} = \begin{bmatrix} 0 & \frac{h_{21}}{h_{11}} & \frac{h_{31}}{h_{11}} & \cdots & \frac{h_{M1}}{h_{11}} \\ \frac{h_{12}}{h_{22}} & 0 & \frac{h_{32}}{h_{22}} & \cdots & \frac{h_{M2}}{h_{22}} \\ \frac{h_{13}}{h_{33}} & \frac{h_{23}}{h_{33}} & 0 & \cdots & \frac{h_{M3}}{h_{33}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{h_{1M}}{h_{MM}} & \frac{h_{2M}}{h_{MM}} & \frac{h_{3M}}{h_{MM}} & \cdots & 0 \end{bmatrix},$$

$$\mathbf{D}_1 = \mathrm{diag} \begin{bmatrix} \frac{G_1}{x_1} & \frac{G_2}{x_2} & \frac{G_3}{x_3} & \cdots & \frac{G_M}{x_M} \end{bmatrix}$$

$$\mathbf{D}_2 = \mathrm{diag} \begin{bmatrix} h_{11} & h_{22} & h_{33} & \cdots & h_{MM} \end{bmatrix}$$

28

Optimization with pricing (3/3)

- The above mentioned procedure is a means to determine the unique Nash equilibrium of the capacity maximization game with pricing
- It is essential to obtain conditions under which such a unique Nash equilibrium exists and is feasible
- Work backwards- find the optimum SIR's and capacities had there been a Nash equilibrium and then compute the Nash equilibrium from those SIR's
- The Nash equilibrium thus obtained should be feasible

29

Solve for SIR (1/2)

- Solve for the optimum SIR x_i so as to satisfy the first order necessary conditions
$$\frac{d}{dx}\left(C_i(x) - f_i(x)\right)\big|_{x=x_i} = 0$$
- For the non-linear pricing function, the first order necessary condition yields
$$g(x_i) \triangleq (x_i + G_i)^2 C_i'(x_i) = \lambda r_i G_i$$
- For the linear pricing function, the first order necessary condition yields $g(x_i) \triangleq C_i'(x_i) = \lambda r_i$

- In both cases, for large gains, G_i, $g_i'(x_i) < 0$

30

STEVENS
Institute of Technology

Solve for SIR (2/2)

- Define $\lambda_0^{(i)} = \frac{G_i C_i'(0)}{r_i}$ for non-linear pricing, $\lambda_0^{(i)} = \frac{C_i'(0)}{r_i}$ for linear pricing and $\lambda_{max} = \min_i \lambda_0^{(i)}$.
- Theorem 3:

  The necessary condition for the optimization problem with pricing to have a feasible solution is $\lambda < \lambda_{max}$.

- Theorem 3 gives an upper bound on the pricing parameter. The condition is only necessary but not sufficient

31

STEVENS
Institute of Technology

Solve for Power (1/4)

- Need to solve a system of equations given by the matrix equation

  $\mathbf{p} = N_0 W \left(\mathbf{I}_M - \mathbf{D}_1^{-1} \mathbf{A} \right)^{-1} \mathbf{D}_1^{-1} \mathbf{D}_2^{-1} \mathbf{1}$

- Need to obtain conditions when the matrix equation yields positive solutions for $\mathbf{p}$ and such that

  $\mathbf{p} \le P_{max} \mathbf{1}$

- Need to use theory of $\mathcal{Z}$-matrices and $\mathcal{M}$-matrices to obtain these conditions

32

Solve for Power (2/4)

An n x n square matrix $\mathbf{B} = [b_{ij}]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$ is called a $\mathcal{Z}$ matrix if the off-diagonal elements are non-positive, i. e., $b_{ij} \le 0$, $\forall\, i \ne j$. A $\mathcal{Z}$-matrix $\mathbf{B}$ is called an $\mathcal{M}$-matrix if $\mathbf{B}^{-1} \ge \mathbf{0}_n$, i. e., every entry in the inverse matrix of $\mathbf{B}$ is non-negative

• Theorem 4

A positive SIR vector $\mathbf{x}$ results in a positive power vector $\mathbf{p}$ if and only if the $\mathcal{Z}-$matrix $\left(\mathbf{I}_M - \mathbf{D}_1^{-1}\mathbf{A}\right)$ is an $\mathcal{M}$-matrix

• Need to obtain conditions on the SIR vector $\mathbf{X}$ such that the Z-matrix $\left(\mathbf{I}_M - \mathbf{D}_1^{-1}\mathbf{A}\right)$ is an M-matrix

33

STEVENS
Institute of Technology

Solve for Power (3/4)

• Theorem 5

$\exists$ a positive SIR vector $\hat{\mathbf{x}}$ such that, $\forall\, \mathbf{x}$ such that $\mathbf{x} > \hat{\mathbf{x}}$, the matrix $\left(\mathbf{I}_M - \mathbf{D}_1^{-1}\mathbf{A}\right)$ ceases to be an $\mathcal{M}$-matrix and $\forall\, \mathbf{x}$ such that $\mathbf{x} \le \hat{\mathbf{x}}$, the matrix $\left(\mathbf{I}_M - \mathbf{D}_1^{-1}\mathbf{A}\right)$ is an $\mathcal{M}$-matrix

• Theorem 6

$\exists\, \lambda_{min}$ such that $\forall\, \lambda \in (\lambda_{min}, \lambda_{max})$, with λ_{max} as specified in Theorem 3, then the optimization problem $\max_{\mathbf{p}} C_i(\mathbf{p}) - f_i(\mathbf{p})\ \forall\, i$ subject to the constraints $0 \le P_i \le P_{max}\ \forall\, i$ has a feasible solution

34

Solve for Power (4/4)

• Theorem 6 only provides the existence of λ_{min} but does not provide a means of determining it.

• Complex numerical techniques are required to determine λ_{min}

• Theorem 7

The capacity maximization game with pricing, $\max_{\mathbf{p}} C_i(\mathbf{p}) - f_i(\mathbf{p}) \; \forall \; i$ subject to $0 \le P_i \le P_{max}$ $\forall \; i$ has a unique Nash equilibrium if and only if the pricing parameter λ satisfies $\lambda \in (\lambda_{min}, \lambda_{max})$

35

System with an eavesdropper

- The Secrecy capacity = Shannon capacity of the main channel-Shannon capacity of the eavesdropper channel for each transmit-receive pair
- In the absence of feedback or active transmission from the eavesdropper, the SIR of the main channel is independent of the SIR of the eavesdropper channel
- So maximum secrecy capacity occurs for the same SIR when Shannon capacity is maximum
- To maximize sum secrecy capacity, the sum secrecy capacity function is a separable function in all the SIRs and hence maximizing individual secrecy capacity maximizes the sum secrecy capacity

36

Numerical Results

- 10 transmit-receive pairs
- Two types of systems
  - A low bandwidth system with 5 MHz bandwidth and transmitters transmitting at rates less than 100 Kbps
  - A high bandwidth system with 20 MHz bandwidth with transmitters transmitting at about 1-2 Mbps
- Three Scenarios
  - Co-located transmitters
  - Co-located receivers
  - Randomly located transmitters and receivers
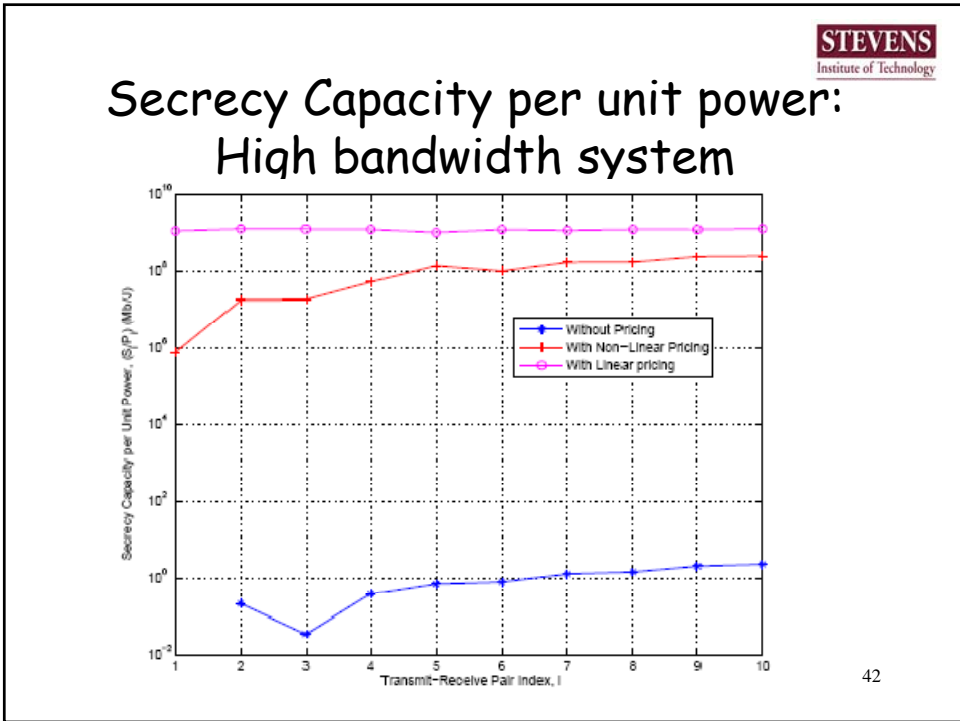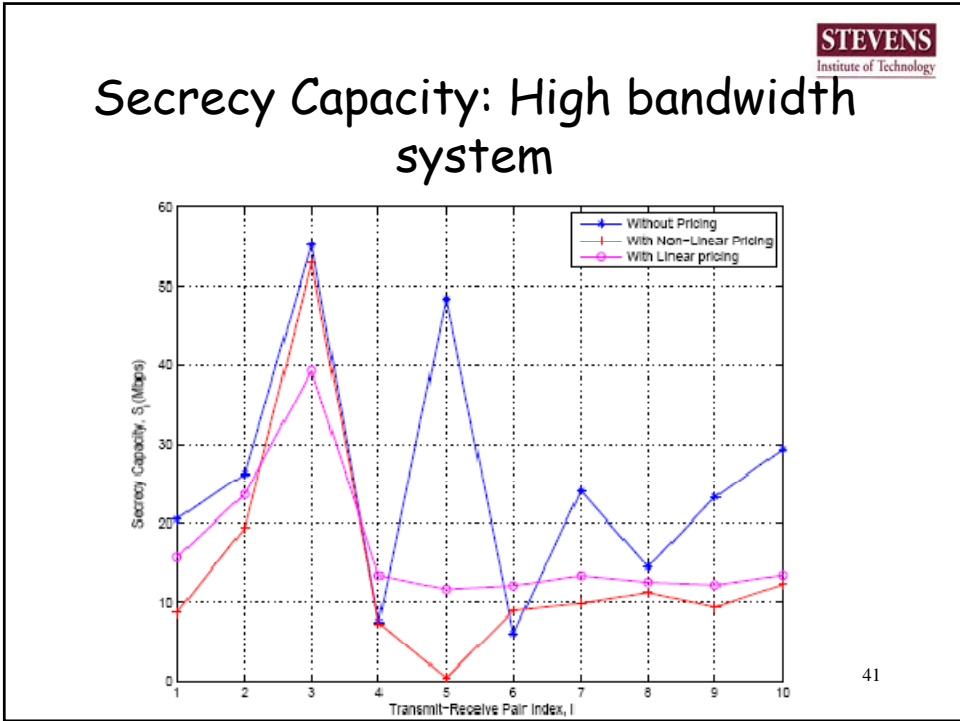- Jake's model to obtain the channel gain matrix and the channel gain vector to the eavesdropper

37

Co-located Transmitters

38

19

Secrecy Capacity: Low bandwidth system

Secrecy Capacity per unit power: Low bandwidth system

Secrecy Capacity: High bandwidth system

Secrecy Capacity per unit power: High bandwidth system
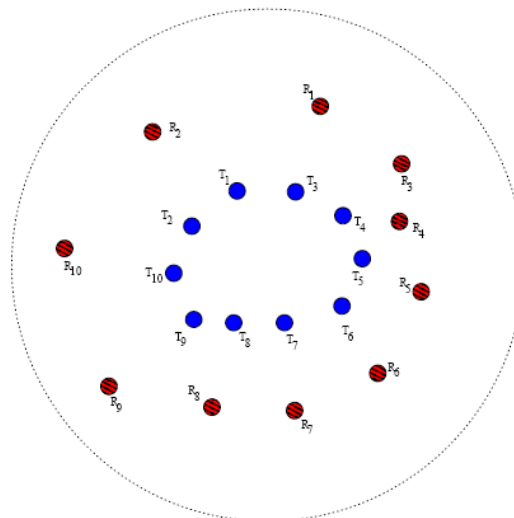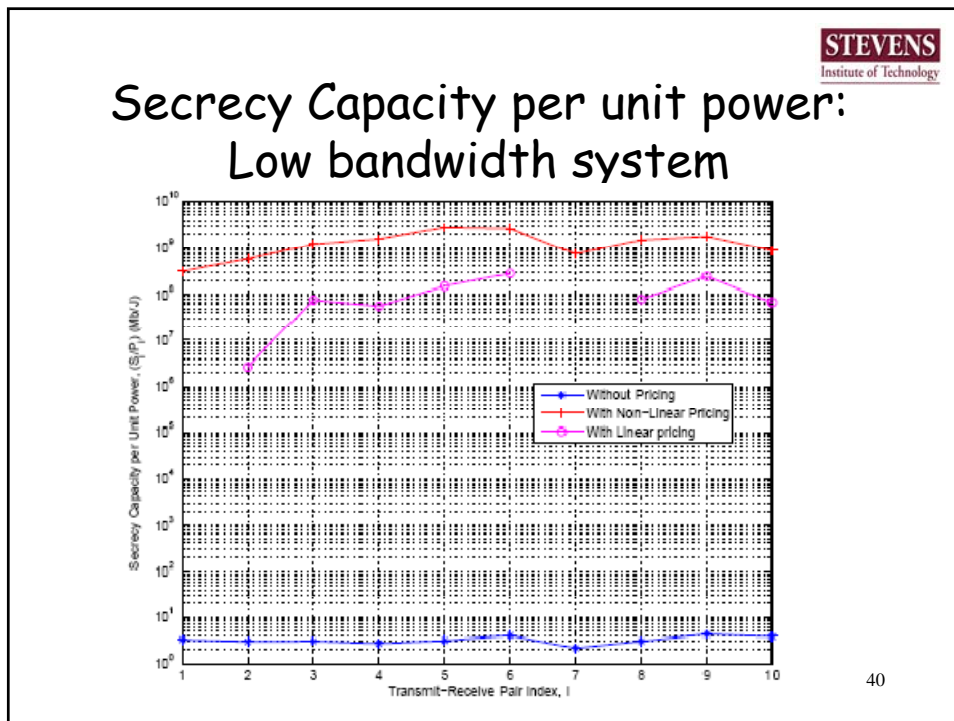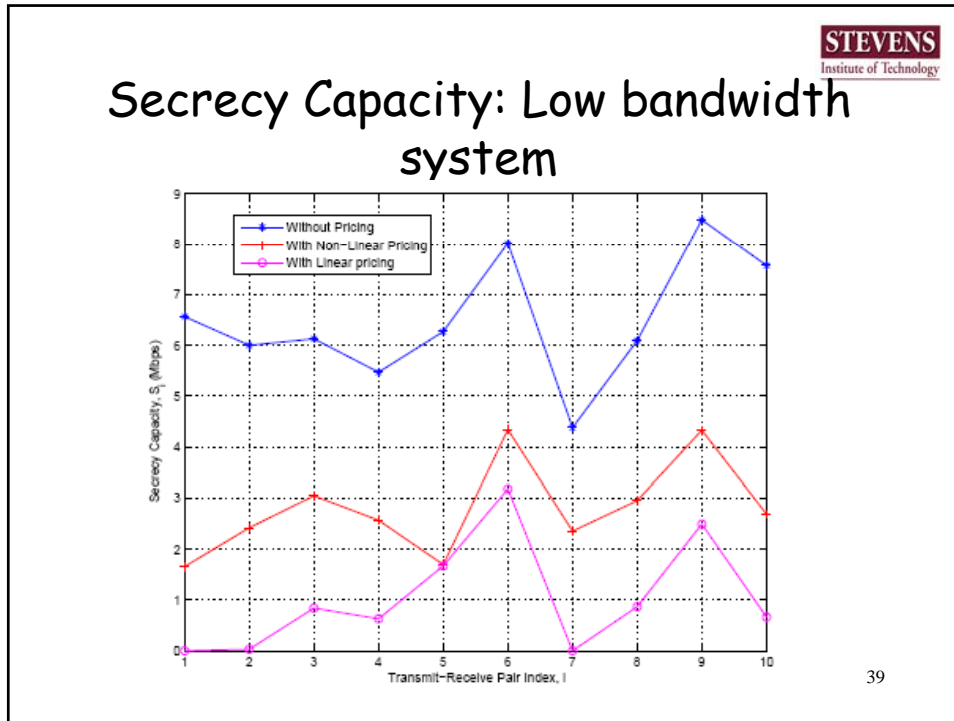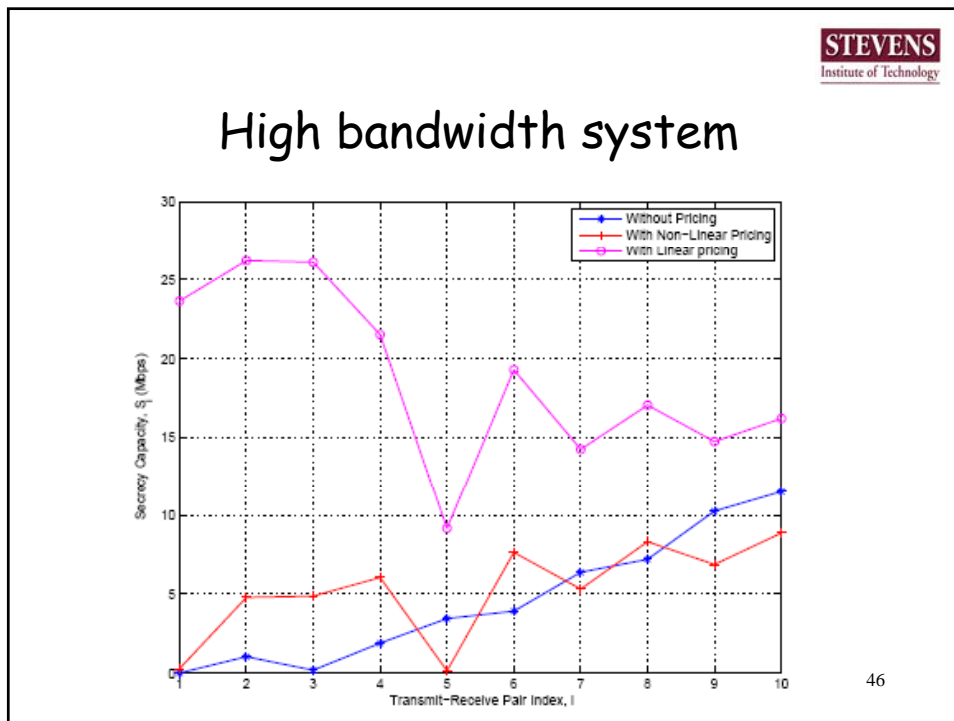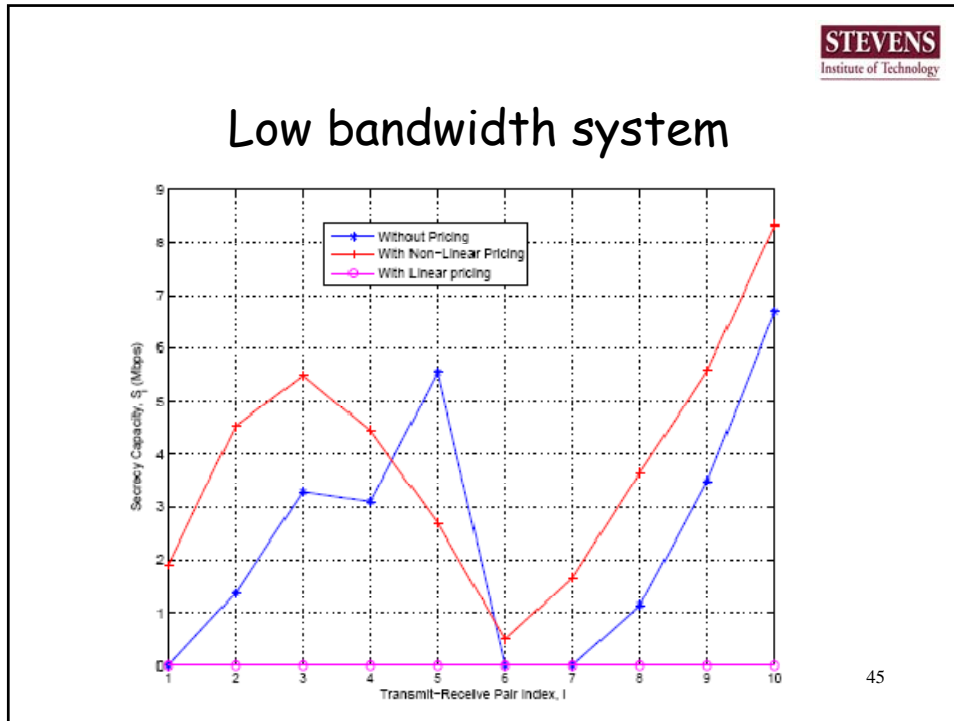
Observations

- The system without pricing provides higher secrecy capacity for most users
- Pricing provides energy efficiency
- Linear pricing performs better for lower gain (high bandwidth) systems and non-linear pricing performs better for higher gains (lower bandwidth) systems
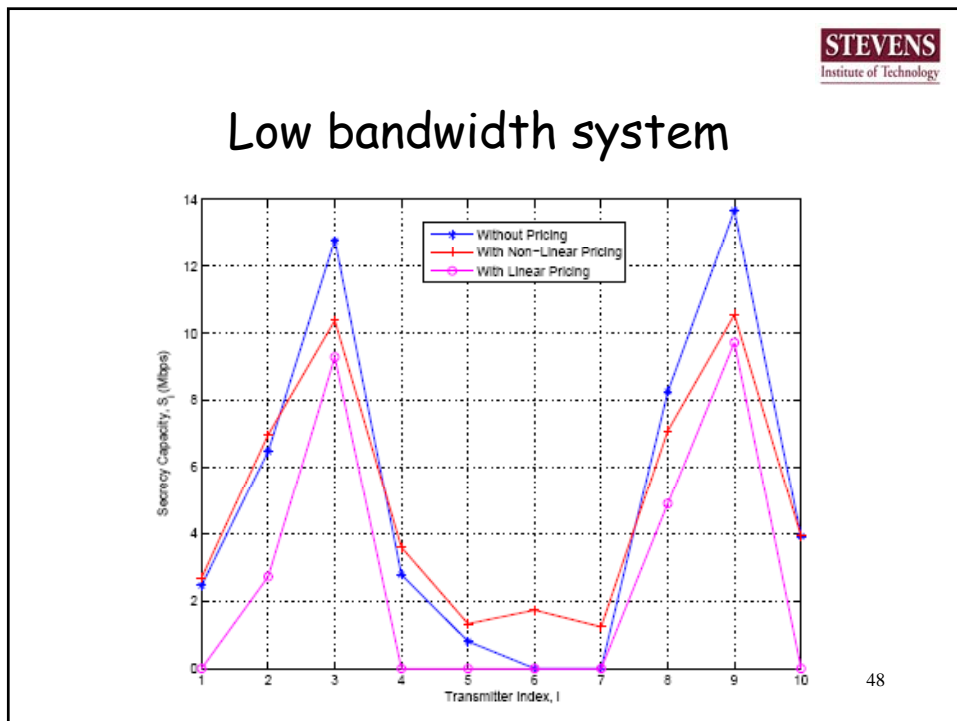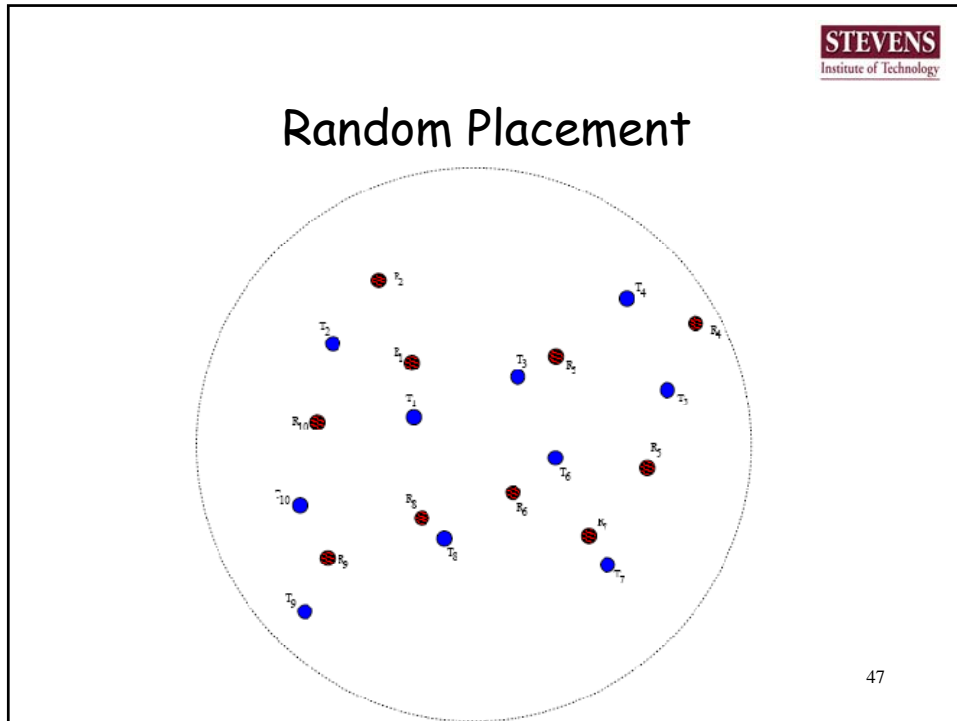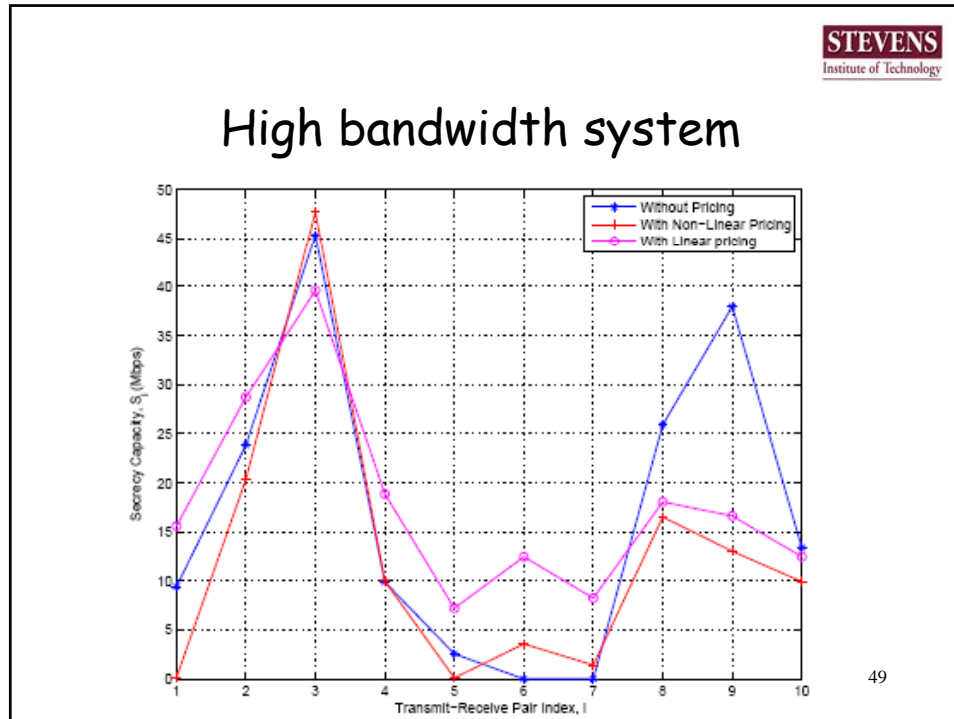
43

Co-located Receivers

44

Low bandwidth system

High bandwidth system

Random Placement

47

Low bandwidth system

48

High bandwidth system

49
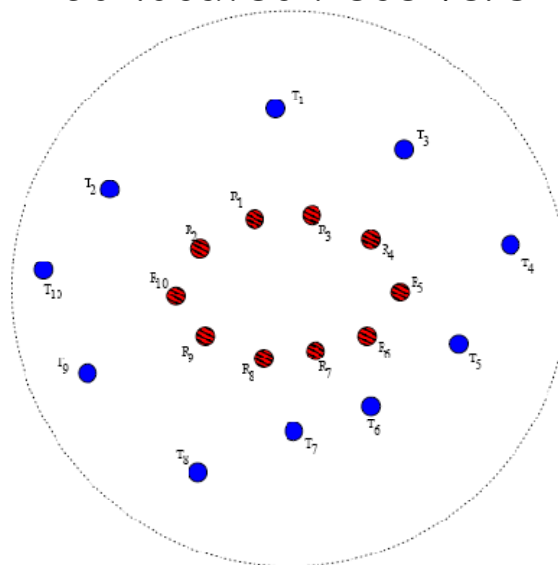
Observations

- Pricing improves secrecy capacity for users who suffer from lower secrecy capacity when no pricing
- Particularly useful in scenarios where the users suffering from low secrecy capacity form the "cut-edges"
- Linear pricing performs better for lower gain (high bandwidth) systems and non-linear pricing performs better for higher gains (lower bandwidth) systems

50

STEVENS
Institute of Technology

Additional Applications

- Admission control to satisfy secrecy capacity constraints
  - A new user enters with an SIR requirement
  - Admit if the conditions for the Z-matrix to remain and M-matrix are satisfied
  - Block otherwise
- Cognitive radio networks
  - Admit secondary users to satisfy secrecy capacity constraints in addition to interference constriants

51

STEVENS
Institute of Technology

Summary

- A pricing based approach for maximizing secrecy capacity of multi-terminal networks
- Conditions for obtaining feasible solutions
- Showed that the pricing is effective in terms of energy efficiency
- Showed that pricing can improve secrecy capacity of users
- Applications to Admission Control and Cognitive radio networks

52

Future Work

- Asymptotic Analysis
  - When the number of transmit-receive pairs and the system bandwidth are very large
- Multiple eavesdroppers
  - The eavesdroppers could be independent or co-operating
- Effects of mobility
  - Changes to the channel gain matrix
  - Can there be adaptive solutions?

53

54

55

Game theory fundamentals (1/5)

A *game*, $\mathcal{G}(\mathcal{P}, \mathcal{S}, \mathcal{U})$, is defined by a set of players, $\mathcal{P} = \{p_1, p_2, \cdots, p_n\}$, a strategy set, $\mathbf{S}_i$, for each player p_i $(\mathcal{S} \triangleq \{\mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_n\})$ and a pay off set or a set of utility functions, $\mathcal{U} = \{u_1, u_2, \cdots, u_n\}$, where $u_i : \mathcal{S} \to \mathcal{R}$, is the utility function or pay off function of the player p_i.

- Objective is to obtain a strategy $s_i^* \in \mathbf{S}_i$ such that the utility $u_i(s_1^*, s_2^*, \cdots s_n^*)$ is maximum for each player p_i

56

Game theory fundamentals (2/5)

For any strategy vector $\mathbf{s} = \begin{bmatrix} s_1 & s_2 & \cdots & s_n \end{bmatrix}$,

let $\mathbf{s}_{-i} \overset{\triangle}{=} \begin{bmatrix} s_1 & s_2 & \cdots & s_{i-1} & s_{i+1} & \cdots & s_n \end{bmatrix}$.
The strategy vector $\mathbf{s}$ is said to be a *Nash equilibrium*
of the game $\mathcal{G}(\mathcal{P}, \mathcal{S}, \mathcal{U},)$ if, $\forall\, i \in \{1, 2, \cdots, n\}$,
$u_i(s_i, \mathbf{s}_{-i}) \geq u_i(\hat{s}_i, \mathbf{s}_{-i}), \forall\, \hat{s}_i \in \mathbf{S}_i$.

- Nash equilibrium is a set if strategies such that each player's strategy is the best response to the strategies of all the other players
- A Nash equilibrium may or may not exist
- There can be multiple Nash equilibriums

57

Game theory fundamentals (3/5)

A strategy vector $\mathbf{s}$ is said to be *an improvement* to strategy $\tilde{\mathbf{s}}$
if, $\forall\, i \in \{1, 2, \cdots, n\}$, $u_i(\mathbf{s}) \geq u_i(\tilde{\mathbf{s}})$, and $\exists j \in \{1, 2, \cdots, n\}$
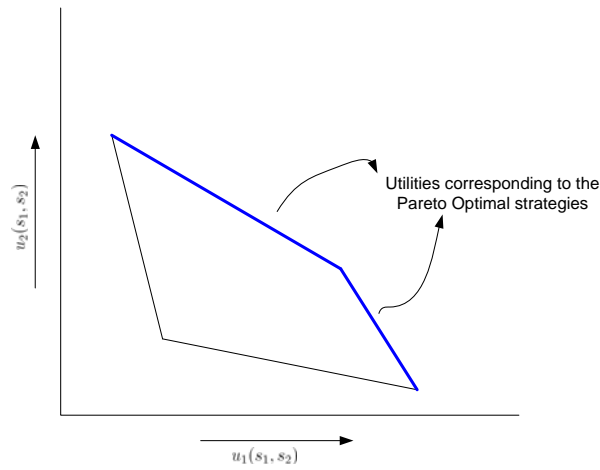such that $u_j(\mathbf{s}) > u_j(\tilde{\mathbf{s}})$.

- An improvement to a strategy is another strategy such that the utilities of all the player improve

A strategy vector $\mathbf{s}$ is said to be *Pareto optimal* if there
does not exist a strategy $\tilde{\mathbf{s}}$ such that $\tilde{\mathbf{s}}$ is an improvement to $\mathbf{s}$.

- A Pareto optimal strategy vector is a strategy vector such that no player can deviate from the strategy set to improve its own utility without decreasing the utility of any other user.
- A Pareto optimal strategy is a socially optimum strategy

58