Game-Theoretic Framework for Network Resilience, Reliability and Security

(9:00 – 10:45)

TAMER BAŞAR

ECE, CAS, CSL, ITI, and MechSE, UIUC

basar1@illinois.edu

IPAM Summer School on 'Games and Contracts for Cyber-Physical Security'

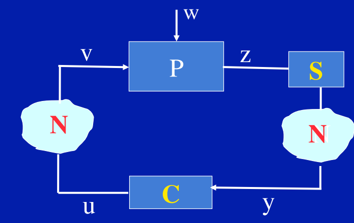
UCLA, Los Angeles, CA

July 21, 2015

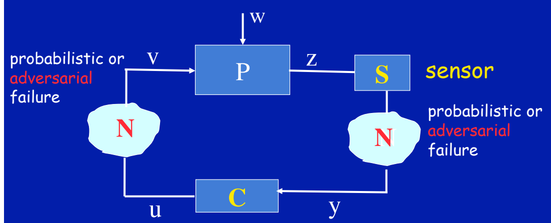
OUTLINE

- Networked (control) systems: Resilience, reliability & security
- Why a game-theoretic framework?
- An overview of GT: models, solution concepts, key results, algorithms
- Incentivizing agents toward efficiency
- Selected applications

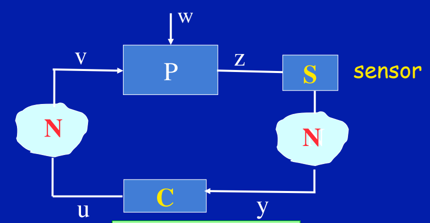
Networked Control System



Failure of Channels

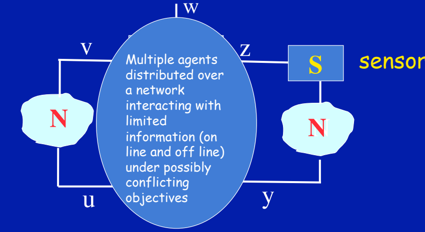


Multiple Criteria / Games



Non-cooperating controllers (agents) / multiple objectives / lack of trust

Multi-Agent Networked System with Multiple Objectives



Multi-agent networked systems

- Multiple heterogeneous agents connected in various ways, distributed over a network (or interacting networks) and interacting with limited information (on line and off line) under possibly conflicting objectives

Multi-agent networked systems

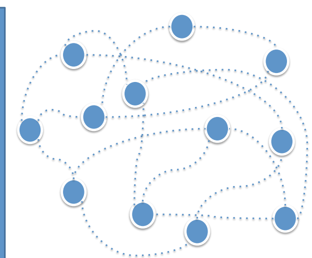
- Multiple heterogeneous agents connected in various ways, distributed over a network (or interacting networks) and interacting with limited information (on line and off line) under possibly conflicting objectives
- Multiple (layered) networks
  - Collaboration network
  - Information network
  - Physical communication network

Multi-agent networked systems as graphs

Network is a connected graph

Nodes are agents / dynamic systems /mobile

Links are one of three types of connections

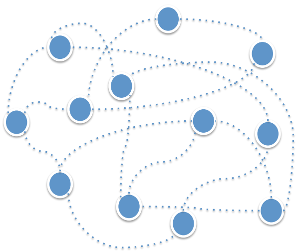


Multi-agent networked systems as graphs

Links are one of three types of connections:

- Communication
- Collaboration
- Physical

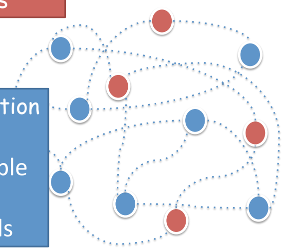
➔ Layered graphs



Some nodes/agents could be adversarial (and even mobile):

- jamming communication
- interrupting collaboration
- breaking physical links

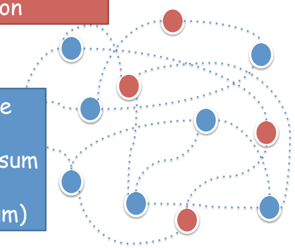
Leads to a game situation
➔ Dynamic zero-sum game between multiple agents as teams with directly opposing goals



Even friendly nodes/agents may have misaligned (but not directly opposing) goals due to:

- selfish interests
- localized information

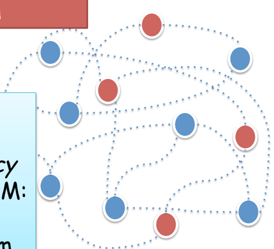
Leads again to a game situation
➔ Dynamic nonzero-sum (stochastic) game (with Nash equilibrium)



Even friendly nodes/agents may have misaligned (but not directly opposing) goals due to:

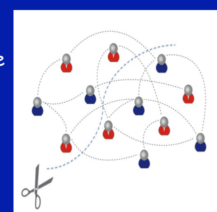
- selfish interests
- localized information

Nash equilibrium is generally ***inefficient!***
➔ Relieving *inefficiency* through hierarchical DM: mechanism design & Stackelberg equilibrium



Application
Control of Information Spread

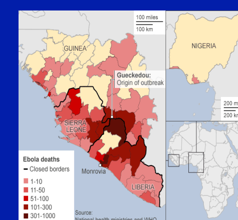
- **Social networks**
  - Optimal methods to limit the spread of misinformation
  - Measures and countermeasures to limiting popularity of products, candidates, etc.



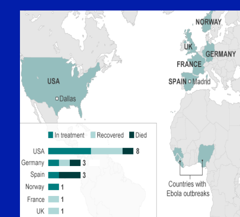
- Epidemics: prevent (or decelerate) the spread of disease
- Interaction between an intelligent adversary and a dynamical network

Application
Global Spread from Local Interaction

- Local interactions lead to fast spread of viruses
- Scale of spread requires finding *efficient* mitigation techniques
- Numbers of healthy/infected nodes and network topology *vary with time*



Ebola Spread in Africa, Oct 4-6 (BBC)



Global Spread of Ebola (BBC)

Application
Evolution of Opinions

- Understanding how an individual's opinion evolves over time when s/he is in (partial) contact with others
- Developing models to capture the underlying process of opinion formation (probabilistic or deterministic)

Most social interactions are affected by individuals' opinions, either directly or indirectly (s.a. voting, buying products)

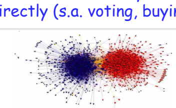
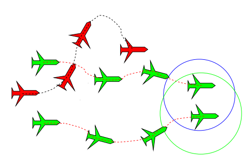


Figure: Network structure of political blogs prior to 2004 presidential election

Application
Aerial Jamming Attack on the CommNet of a team of UAVs

- The jammer wants to maximize the time for which communication can be jammed.
- The two UAVs want to minimize the time for which communication remains jammed.



Assessing Security and Resilience

➢ **Systems operate in adversarial environments**

- Adversaries seek to degrade system operation by affecting the confidentiality, integrity, and/or availability of the system information and services, or disrupting communication.
- "Resilient" systems aim to meet their ongoing operational objectives despite attack attempts made by adversaries (or failures due to environmental changes), take pre-cautionary measures (security), and **restore** normal operating conditions with minimum disruption.
- Reliability (trust) is an integral element of successful operation of a multi-agent network, which endows agents with confidence on the outcome of their strategic decisions and actions.

Games / Game Theory

Quantification of strategic interactions between entities/players

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development
- 10 Nobel Prizes (1994 / 2005 / 2007 / 2012)
  - 1994: John Harsanyi, John Nash, Reinhard Selten

    "for their pioneering analysis of equilibria in the theory of non-cooperative games"

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development
- 10 Nobel Prizes (1994 / 2005 / 2007 / 2012)
  - 2005: Robert Aumann, Thomas Schelling

    "for having enhanced our understanding of conflict and cooperation through game-theory analysis"

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development
- 10 Nobel Prizes (1994 / 2005 / 2007 / 2012)
  - 2007: Leonid Hurwicz, Eric Maskin, Roger Myerson

    "for having laid the foundations of mechanism design theory"

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development
- 10 Nobel Prizes (1994 / 2005 / 2007 / 2012)
  - 2012: Alvin Roth, Lloyd Shapley

    "for the theory of stable allocations and the practice of market design"

Games / Game Theory

Quantification of strategic interactions between entities/players

- 70+ years of scientific development
- 10 Nobel Prizes (1994 / 2005 / 2007 / 2012)
- Crafoord Prize (1999)
  - John Maynard Smith (with Ernst Mayr, G. Williams)

    " for developing the concept of evolutionary biology"

Robustness

- Economists have also been interested in "robustness"

In the preface of their 2008 PUP book *Robustness*, Lars Hansen & Thomas Sargent (2013 & 2011 NLs) say

"When we became aware of Whittle's 1990 book, *Risk Sensitive Control*, and later his 1996 book, *Optimal Control: Basics and Beyond*, we eagerly worked through them. These and other books on robust control theory, such as Başar and Bernhard's 1995 *H^∞-Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*, provide tools for approaching the `soft' but important question of how to make decisions when you don't fully trust your model."

Games / Game Theory

Rich in models and concepts

- Zero-sum vs Nonzero-sum games
- Non-cooperative vs Cooperative games
- Complete vs Incomplete information
- Deterministic vs Stochastic games
- Static vs Dynamic/Differential games
- Bargaining, bidding, auctions, ….

Game Theory: the beginning

- John von Neumann (1903-57) and
  Oskar Morgenstern (1902-76)

Theory of Games and Economic Behavior (1944/7)

Game Theory: the beginning

- Von Neumann (1903-57) and Morgenstern (1902-76)
  Theory of Games and Economic Behavior (1944/7)
- John von Neumann *(minimax theorem)*
  "Zur theorie der Gesellschaftspiele" (1928)

Game Theory: the beginning

- Von Neumann (1903-57) and Morgenstern (1902-76)
  Theory of Games and Economic Behavior (1944/7)
- John von Neumann *(minimax theorem)*
  "Zur theorie der Gesellschaftspiele" (1928)
- E. Borel (~1920) -- *"minimax theorem is false"*

Elements of Games

- Players: $1, 2, \ldots, M$
- Decision variables: $u_1, \ldots, u_M$; $u_i \in U_i$
- Cost functions $V_i(u_i, u_{-i})$, $i=1, \ldots, M$
- Nash equilibrium u^*:

  $\min \{V_i(u_i, u^*_{-i}): u_i \in U_i\} = V_i(u^*_i, u^*_{-i})$

Elements of Games

- Players: $1, 2, \ldots, M$
- Decision variables: $u_1, \ldots, u_M$; $u_i \in U_i$
- Cost functions $V_i(u_i, u_{-i})$, $i=1, \ldots, M$
- Nash equilibrium u^*:

  $\min \{V_i(u_i, u^*_{-i}): u_i \in U_i\} = V_i(u^*_i, u^*_{-i})$

Coupled constraints also possible: $u \in U$

$\min \{V_i(u_i, u^*_{-i}): (u_i, u^*_{-i}) \in U\} = V_i(u^*_i, u^*_{-i})$

Elements of Games

Coupled constraints also possible: $u \in U$

$\min \{V_i(u_i, u^*_{-i}): (u_i, u^*_{-i}) \in U\} = V_i(u^*_i, u^*_{-i})$

E.g.

- $u_i \in R^+$ $U = \{ u : \Sigma_i u_i \le C\}$ (capacity constraint)
- Cost fns $V_i(u_i, u_{-i}) = V_i(u_i)$, $i=1, \ldots, M$
- Multiple Nash equilibria :

  $(u_i^* = C, u_{-i}^* = 0)$, $i=1, \ldots, M$

Elements of Games

- Players: $1, 2, \ldots, M$
- Decision variables: $u_1, \ldots, u_M$; $u_i \in U_i$
- Cost functions $V_i(u_i, u_{-i})$, $i=1, \ldots, M$
- Nash equilibrium u^*:

  $\min \{V_i(u_i, u^*_{-i}): u_i \in U_i\} = V_i(u^*_i, u^*_{-i})$
- Saddle-point eqm ($M=2$, $-V_2=V_1 =:V$)

  $V(u^*_1, u_2) \le V(u^*_1, u^*_2) \le V(u_1, u^*_2)$

Strategically Equivalent Games
(no coupling constraints)

- SE transformation on V_i's based on positive scaling and self-action independent translation: for $a_i > 0$, b_i $\forall i$,

$V_i(u_i, u_{-i}) \rightarrow a_i V_i(u_i, u_{-i}) + b_i(u_{-i}) =: W_i(u_i, u_{-i})$

➔ Strategically equivalent games (even though agents/players incur different costs under each game)

Strategically Equivalent Games

- SE transformation on V_i's based on positive scaling and self-action independent translation: for $a_i > 0$, b_i $\forall i$,

  $V_i(u_i, u_{-i}) \rightarrow a_i V_i(u_i, u_{-i}) + b_i(u_{-i}) =: W_i(u_i, u_{-i})$
- NE of $\{W_i\}$ do not depend on $\{a_i\}$, $\{b_i\}$

  $\min \{W_i(u_i, u^*_{-i}): u_i \in U_i\} = W_i(u^*_i, u^*_{-i})$

Strategically Equivalent Games

- SE transformation on V_i's based on positive scaling and self-action independent translation: for $a_i > 0$, b_i $\forall i$,

$V_i(u_i, u_{-i}) \to a_i V_i(u_i, u_{-i}) + b_i(u_{-i}) =: W_i(u_i, u_{-i})$

- NE of $\{W_i\}$ do not depend on $\{a_i\}$, $\{b_i\}$

  $\min\{W_i(u_i, u^*_{-i}): u_i \in U_i\} = W_i(u^*_i, u^*_{-i})$

- For $\{V_1, V_2\}$ either $W_1 \equiv W_2$, or $W_1 \equiv -W_2$ OR neither (genuine game)

Strategically Equivalent Games

- A 2-player game could be team-equivalent (*potential game*), or 0-sum equivalent, or a genuine NZS game
- M-player game could be team-equivalent, or team vs team 0-sum, or genuine NZS
- Concept applies to games with stochastic parameters and stochastic information patterns, and dynamic games as well
- Congestion games, oligopoly games are team-equivalent

(First introduced in: TB-Ho, JET'74)

Example: Stochastic Duopoly Game

- 2 firms with production levels of q and r
- Linear demand curve: $p = a - b(q+r)$, where p is price, $b>0$ known to both firms, $a \sim N(\underline{a}, \xi)$
- Firms have access to a through noisy channels: $z_i = a + w_i$, $w_i \sim N(0, s_i)$, $i = 1, 2$

(TB-Ho, JET'74)

Example: Stochastic Duopoly Game

- 2 firms with production levels of q and r
- Linear demand curve: $p = a - b(q+r)$, where p is price, $b>0$ known to both firms, $a \sim N(\underline{a}, \xi)$
- Firms have access to a through noisy channels: $z_i = a + w_i$, $w_i \sim N(0, s_i)$, $i = 1, 2$
- Profit functions: $P_1 = qp - k_1 q^2$; $P_2 = rp - k_2 r^2$
- SE team utility: $W = P_1 + ra - (b+k_2) r^2$

(TB-Ho, JET'74)

Example: Stochastic Duopoly Game

- 2 firms with production levels of q and r
- Linear demand curve: $p = a - b(q+r)$, where p is price, $b>0$ known to both firms, $a \sim N(\underline{a}, \xi)$
- Firms have access to a through noisy channels: $z_i = a + w_i$, $w_i \sim N(0, s_i)$, $i = 1, 2$
- Profit functions: $P_1 = qp - k_1 q^2$; $P_2 = rp - k_2 r^2$
- SE team utility: $W = P_1 + ra - (b+k_2) r^2$
- By Radner'62, stochastic team E[W] admits a unique team-optimal solution--also unique NE

(TB-Ho, JET'74)

Example: Stochastic Duopoly Game

- 2 firms with production levels of q and r

Better information for one player (s_i lower) improves the average net profit $E[P_i]$ of that player while decreasing the net profit of the other.

$z_i = a + w_i$, $w_i \sim N(0, s_i)$, $i = 1, 2$

- Profit functions: $P_1 = qp - k_1 q^2$; $P_2 = rp - k_2 r^2$
- SE team utility: $W = P_1 + ra - (b+k_2) r^2$
- By Radner'62, stochastic team E[W] admits a unique team-optimal solution--also unique NE

(TB-Ho, JET'74)

Example: Stochastic Duopoly Game

- 2 firms with production levels of q and r

Better information for one player (s_i lower) improves the average net profit $E[P_i]$ of that player while decreasing the net profit of the other.

$z_i = a + w_i$, $w_i \sim N(0, s_i)$, $i = 1, 2$

- Profit functions: $P_1 = qp - k_1 q^2$; $P_2 = rp - k_2 r^2$

There're other examples showing better information for one player benefits both, with the benefit to the recipient being less than that to the other player.

TB Allerton'72

General Results
Von Neumann (1928)

- Every finite zero-sum matrix game has a SPE in mixed strategies – *minimax theorem*

Von Neumann (1928)

- Every finite zero-sum matrix game has a SPE in mixed strategies – *minimax theorem*
- P1, minimizer, has m possible actions: $x_1, \ldots, x_m$
- P2, maximizer, has n possible actions: $y_1, \ldots, y_n$
- Prob vector $p = (p_1, \ldots, p_m)$ – mixed strategy for P1
- Prob vector $q^T = (q_1, \ldots, q_n)$ – mixed strategy for P2
- m x n cost/utility matrix *A*
- There exist (p^*, q^*) such that $p^* A q \le p^* A q^* \le p A q^*$

Von Neumann (1928)

- Every finite zero-sum matrix game has a SPE in mixed strategies – *minimax theorem*
- P1, minimizer, has m possible actions: $x_1, \ldots, x_m$
- P2, maximizer, has n possible actions: $y_1, \ldots, y_n$
- Prob vector $p = (p_1,\ldots,p_m)$ – mixed strategy for P1
- Prob vector $q^T = (q_1,\ldots,q_n)$ – mixed strategy for P2
- m x n cost/utility matrix A
- There exist (p^*, q^*) such that $p^*Aq \leq p^*Aq^* \leq pAq^*$

Solving for MSSPE is equivalent to solving an LP

John Nash (1950/1951)

- Players: 1, 2, …, M
  - Decision/action for Player i: $u_i \in U_i$ – finite set
  - Net cost function for each player: $V_i(u_i, u_{-i})$
  - μ_i : probability vector on U_i
  - $J_i(\mu_i, \mu_{-i})$: Expected value of $V_i(u_i, u_{-i})$
- There exists a NE in mixed strategies, μ^*:

  $J_i(\mu^*_i, \mu^*_{-i}) \leq J_i(\mu_i, \mu^*_{-i})$ for all $\mu_i \in P(U_i)$, all i

  [*Uses Kakutani Fixed-Point Theorem*]

Extension to Infinite (Continuous-Kernel) Games

- Infinite Games; compact action spaces; continuity
  - There exists a NE in mixed strategies; *pms* on U_i
  - If further V_i is convex in u_i, NE in pure strategies

    $V_i(u^*_i, u^*_{-i}) \leq V_i(u_i, u^*_{-i})$ for all $u_i \in U_i$

  If V_i's are further differentiable, and U_i's are open,

  $D_i V_i(u^*_i, u^*_{-i}) = 0$, for all i
- Multiple NE are not necessarily interchangeable but multiple SPE are
- Refinements to remove non-uniqueness (*a bit later*)

Recursive Computation

- $u_i^{(n+1)} = \arg\min_\xi V_i(\xi, u_{-i}^{(n)})$, n=0, 1,…; for all i
  - The above is *parallel update* based on *best response*
  - If argmin is unique and the sequence converges, then there is a **unique** NE
  - In the update on the RHS, $u_{-i}^{(n)}$ can be replaced with delayed versions
- The iterate is: $u_i^{(n+1)} = v_i(u_{-i}^{(n)})$, n = 0, 1,…

  $\Leftrightarrow$ $\mathbf{u}^{(n+1)} = \mathbf{v}(\mathbf{u}^{(n)})$, n = 0, 1,… NE is FP of **v**

Recursive Computation

- $u_i^{(n+1)} = \arg\min_\xi V_i(\xi, u_{-i}^{(n)})$, n=0, 1,…; for all i

Also continuous-time gradient based algorithms:
$d\, u_i(t) / dt = - D_i V_i(u_i, u_{-i})$, i = 1,…,M

  - In the update on the RHS, $u_{-i}^{(n)}$ can be replaced with delayed versions, respecting also network imposed restrictions
- The iterate is: $u_i^{(n+1)} = v_i(u_{-i}^{(n)})$, n = 0, 1,…

  $\Leftrightarrow$ $\mathbf{u}^{(n+1)} = \mathbf{v}(\mathbf{u}^{(n)})$, n = 0, 1,… NE is FP of **v**

Recursive Computation

Four Specific Types of Update Mechanisms

All four are of the form

$u_i^{(n+1)} = v_i(u_{-i}^{(n)})$ if $i \in K_n$ (*subset of players who update at n*)

$= u_i^{(n)}$ else

1. Parallel update : $K_n = \{1, \ldots, M\} =: N$
2. Round robin : $K_n = \{(n+k) \bmod M + 1\}$, k arbitrary
3. Random polling : K_n independent process on N
4. Stochastic asynchronous : K_n independent set-valued process on all subsets of N

Recursive Computation

Four Specific Types of Update Mechanisms

All four are of the form

$u_i^{(n+1)} = v_i(u_{-i}^{(n)})$ if $i \in K_n$ (*subset of players who update at n*)

$= u_i^{(n)}$ else

1. Parallel update : $K_n = \{1, \ldots, M\} =: N$
2. Round robin : $K_n = \{(n+k) \bmod M + 1\}$, k arbitrary
3. Random polling : K_n independent process on N
4. Stochastic asynchronous : K_n independent set-valued process on all subsets of N

These all will have to respect the "exchange" restrictions due to network graph structure

Recursive Computation

Update Mechanism with Memory

It is possible also to introduce memory to tame convergence

$u_i^{(n+1)} = v_i(y_{-i}^{(n)})$ if $i \in K_n$ (*subset of players who update at n*)

$= u_i^{(n)}$ else

$y_j^{(n)} = \alpha_i u_j^{(n)} + (1-\alpha_i)$ Average $(u_j^{(n-m)})$, m=1, …, L_i)

j= 1, …, i-1, i+1, …, M

$0 < \alpha_i < 1$

Appropriate selection of α_i and L_i improves convergence

Recursive Computation

Update Mechanisms

- $u_i^{(n+1)} = \arg\min_\xi V_i(\xi, u_{-i}^{(n)})$, n=0, 1,…; for all i
  - The above is *parallel update* based on *best response*

Contraction mapping **v** on a complete space guarantees convergence to a unique NE

with delayed versions
- The iterate is: $u_i^{(n+1)} = v_i(u_{-i}^{(n)})$, n = 0, 1,…

  $\Leftrightarrow$ $\mathbf{u}^{(n+1)} = \mathbf{v}(\mathbf{u}^{(n)})$, n = 0, 1,… NE is FP of **v**

Dynamic Games: Discrete time

- State equation: $x_{k+1} = f_k(x_k, u_k)$, x_1 given
- $u := (u^1, \dots, u^M)$, $u^i_k = \gamma^i_k(\eta^i_k)$, $u^i_k \in U^i_k$
- Cost functions: $L_i(u^i, u^{-i}) = \Sigma_{k=1}^K g^i_k(x_{k+1}, u^i_k, u^{-i}_k)$
- Normal form: $J_i(\gamma^i, \gamma^{-i}) \rightarrow$ NE (dependent on IS)
- Selected information structures $\{\eta_k\}$:
  - open-loop : x_1
  - closed-loop with memory: $x_k, \dots, x_1 =: x_{[1,k]}$
  - closed-loop no-memory: x_k, x_1

Dynamic Games: Discrete time

- State equation: $x_{k+1} = f_k(x_k, u_k)$, x_1 given

Network structure: subsystems connected through physical links, players connected also through communication and collaboration links

- Normal form: $J_i(\gamma^i, \gamma^{-i}) \rightarrow$ NE (dependent on IS)
- Selected information structures $\{\eta_k\}$:
  - open-loop : x_1
  - closed-loop with memory: $x_k, \dots, x_1 =: x_{[1,k]}$
  - closed-loop no-memory: x_k, x_1

Dynamic Games: Discrete time

Network structure: subsystems connected through physical links, players connected also through communication and collaboration links

- Cost functions: $L_i(u^i, u^{-i}) = \Sigma_{k=1}^K g^i_k(x_{k+1}, u^i_k, u^{-i}_k)$

Information for each player could be "localized", becoming "less precise" on subsystems at multiple hops away—imperfect, noisy measurements

  - open-loop : x_1
  - closed-loop with memory: $x_k, \dots, x_1 =: x_{[1,k]}$
  - closed-loop no-memory: x_k, x_1

Dynamic Games: Discrete time

Network structure: subsystems connected through physical links, players connected also through communication and collaboration links

- Cost functions: $L_i(u^i, u^{-i}) = \Sigma_{k=1}^K g^i_k(x_{k+1}, u^i_k, u^{-i}_k)$

Information for each player could be "localized", becoming "less precise" on subsystems at multiple hops away—imperfect, noisy measurements

  - open-loop : x_1

Stochastic uncertainty can be introduced into both state dynamics and measurement equations (IS)

Dynamic Games: Continuous time
Differential Games

- State equation: $dx = f(x, u, t)\, dt$, x_0 given, $t \geq 0$
- $u := (u^1, \dots, u^M)$, $u^i_t = \gamma^i_t(\eta^i_t)$, $u^i_t \in U^i_t$
- Cost functions: $L_i(u^i, u^{-i}) = \text{int}_{[0,T]}\ g^i(x, u^i, u^{-i}, t)$
- Normal form: $J_i(\gamma^i, \gamma^{-i}) \rightarrow$ NE (dependent on IS)
- Selected information structures $\{\eta_t\}$:
  - open-loop : x_0
  - closed-loop with memory: $\{x_s, s \leq t\} =: x_{[0,t]}$
  - closed-loop no-memory: x_t, x_0

Dynamic Games: Continuous time
Differential Games

- State equation: $dx = f(x, u, t)$, x_0 given, $t \geq 0$
- $u := (u^1, \dots, u^M)$, $u^i_t = \gamma^i_t(\eta^i_t)$, $u^i_t \in U^i_t$

The beginning: Rufus Isaacs (early 1950's) within the zero-sum game framework (pursuit evasion games)

  - open-loop : x_0
  - closed-loop with memory: $\{x_s, s \leq t\} =: x_{[0,t]}$
  - closed-loop no-memory: x_k, x_0

Equilibrium Concept for Both Types

- Normal form: $J_i(\gamma^i, \gamma^{-i}) \rightarrow$ NE (dependent on IS)

Nash Equilibrium (in PS): $\gamma := (\gamma^i, \gamma^{-i})$
$J_i(\gamma^i, \gamma^{-i}) \leq J_i(\gamma^i, \gamma^{-i})$ for all $\gamma^i \in \Gamma^i$
and all i = 1, …, M

Solution approach: If compatible with the IS, temporal decomposition into single stage or otherwise static games, and iteration in the spirit of dynamic programming

Equilibrium Concept for Both Types

- Normal form: $J_i(\gamma^i, \gamma^{-i}) \rightarrow$ NE (dependent on IS)

Nash Equilibrium (in PS): $\gamma := (\gamma^i, \gamma^{-i})$
$J_i(\gamma^i, \gamma^{-i}) \leq J_i(\gamma^i, \gamma^{-i})$ for all $\gamma^i \in \Gamma^i$
and all i = 1, …, M

BUT, formidable difficulties if the game is one with ***asymmetric*** information; NE can be obtained in only some special formulations, and with a restricted equilibrium concept, such as MPE of a lifted common information game

Gupta-Nayyar-Langbort-TB SICON'14

Strategic Equivalence

- **Strategic equivalence** of different games (particularly equivalence to dynamic teams and ZSDGs) holds as before, but now one has to be careful with the dynamic nature of the information while scaling and translating cost functions
- Even the "same game" with OL and CL information (considered as two separate games) will not be strategically equivalent

Weak vs Strong Time Consistency

- All PSNE for a dynamic game are **weakly time consistent (WTC),** that is if the game is truncated at any time, say k, assuming that NE is respected until then (that is no deviation), then part of the original NE restricted to [k, K] is still a PSNE for the game on [k, K], with initial state x^*_k.
- A PSNE is **strongly time consistent (STC),** if it is WTC, and further the condition holds for all executions of past policies (particularly for all x_k). CL FB NE is STC.

Large Number of Players
(a certain interaction network → MFGs)

TGEB'44, pp. 13-14:

- "When the number of participants becomes really great, some hope emerges that the influence of every particular participant will become negligible and that the above difficulties may recede and a more conventional theory becomes possible."
- "It is well known phenomenon in many branches of the exact and physical sciences that very great numbers are often easier to handle than those of medium size. This is of course due to the excellent possibility of applying the laws of statistics and probabilities in the first case."

Mean Field Games

- A large number of players/agents, coupled (through dynamics or cost functions) through aggregate quantities, such as average of states of all (other) agents or fused information received from other agents.
- Each agent interacts not with an identifiable agent, but with a population of agents, and responds to the population.
- Aggregate of responses of all agents has to be consistent with the population behavior → requires existence of a fixed point (FPK equation)
- Makes a large class of stochastic dynamic games tractable, which otherwise would be impossible to solve

Refinements of NE

- *Coalition proof* given fixed coalition sizes
- *Resilient NE* (remains NE under any coalition)
- *Trembling hand NE* (remains NE under infinitesimal perturbations in the parameters of the game)—*proper, perfect, etc.*
- *Strongly time consistent (SGP) NE* (NE from any time point & state forward)
- *Efficiency*: NE u^* is also Pareto optimal, minimizing a convex combination of V_i's

Price of Anarchy

- Price of Anarchy (PoA):

  Sum of costs under NE / min sum

  $\Sigma_i V_i(u^*_i, u^*_{-i})$ / $\min_{u\epsilon U} \Sigma_i V_i(u_i, u_{-i})$

Price of Anarchy

- Price of Anarchy (PoA):

  Sum of costs under NE / min sum

  $\Sigma_i V_i(u^*_i, u^*_{-i})$ / $\min_{u\epsilon U} \Sigma_i V_i(u_i, u_{-i})$
- Different games in the same equivalence class (SE games) could have different PoA's
- But clearly |PoA| ≥ 1 (and generally > 1)

Incentivizing/Coordination

- Price of Anarchy (PoA):

  Sum of costs under NE / min sum

  $\Sigma_i V_i(u^*_i, u^*_{-i})$ / $\min_{u\epsilon U} \Sigma_i V_i(u_i, u_{-i})$

- How to get |PoA| closer to 1 ?
- Introduce a decision variable into utility functions – pricing variable

Leader-Followers Game

Leader's cost function: $V_0(\mathbf{r};\ \mathbf{u},\ \mathbf{w})$
Followers' cost functions:

$V_i\ (u_i;\ \mathbf{u}_{-i},\ \mathbf{r},\ \mathbf{w})$, i = 1, .. , M

r is the instrument variable of L, entering V_i through its different components --- *pricing/coordination*

w is a vector, with subcomponents private information to individual players

Leader-Followers Game

Leader's cost function: $V_0(\mathbf{r};\ \mathbf{u},\ \mathbf{w})$
Followers' cost functions:

$V_i\ (u_i;\ \mathbf{u}_{-i},\ \mathbf{r},\ \mathbf{w})$, i = 1, . . , M

Information available to L:

$y_L = \eta_L(\mathbf{u},\ \mathbf{w})$ → $r = \gamma_0(y_L)$

Information available to Fi: $y_i = \eta_i(\mathbf{w})$

→ $u_i = \gamma_i(y_i)$, i = 1, . . , M

Leader-Followers Game

Leader's cost function: $V_0(\mathbf{r};\ \mathbf{u},\ \mathbf{w})$
Followers' cost functions:
$V_i\ (u_i;\ \mathbf{u}_{-i},\ \mathbf{r},\ \mathbf{w})$, $i = 1, \ldots, M$
Information available to L:
$y_L = \eta_L(\mathbf{u},\ \mathbf{w}) \rightarrow r = \gamma_0(y_L)$
Information available to Fi: $y_i = \eta_i(\mathbf{w})$

Does there exist γ_0 such that NE of $\{V_i(u_i, u_{-i}, \gamma_0(y_L), w)\}$ is (nearly-)efficient while also optimizing V_0?

Leader-Followers Game

Leader's cost function: $V_0(\mathbf{r};\ \mathbf{u},\ \mathbf{w})$
Followers' cost functions:

Yes, depending on η_L, but in general case PoA (loss in efficiency) can be computed and corresponding γ_L be determined.

Information available to Fi: $y_i = \eta_i(\mathbf{w})$

Does there exist γ_0 such that NE of $\{V_i(u_i, u_{-i}, \gamma_0(y_L), w)\}$ is (nearly-)efficient while also optimizing V_0?

Leader-Followers Game

Leader's cost function: $V_0(\mathbf{r};\ \mathbf{u},\ \mathbf{w})$
Followers' cost functions:
$V_i\ (u_i;\ \mathbf{u}_{-i},\ \mathbf{r},\ \mathbf{w})$, $i = 1, .., M$
r is the instrument variable of L,

Through an appropriate *mechanism design* PoA can be driven closer to 1, AND solution could be made least sensitive to deviations from nominal cost functions.

players

Leader-Followers Game
(an example)

$U_i = -V_i = w_i \log(1+u_i) - 1/(C-u_{total}) - r_i$
w_i: F_i-specific parameter (random)
$r_i = \gamma_{0i}(w_i,u_i)$, $U_0 = -V_0(r) = r = \Sigma_i\, r_i$

U_i: utility for resource & disutility for excess

& cost to F_i of using a certain amount of the resource

Leader-Followers Game
(an example)—cont.

Complete information : L and Fs know precisely different F types, and this value of **w**

Incomplete information : L does not **have access to F type information; Fs may or may not**

Issues/Questions

- What is the best L can do?
- How can different pricing policies control the user population
- Asymptotics as M becomes large
- Impact of incompleteness of information on performance, and fair and efficient allocation of resources

General Mathematical Questions

- Structure of the stochastic Nash game at the lower level for different γ_0 ?
- What if NE does not exist or is not unique for some γ_0 ?
- Functional optimization by L on NE reaction set ?
- Tradeoff between complexity and optimality

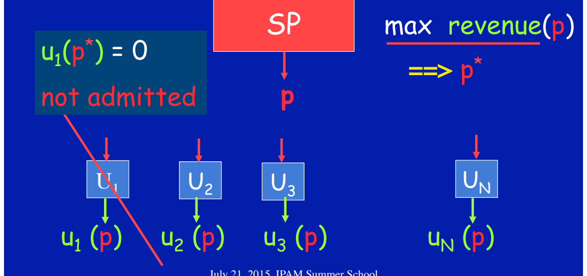
One Approach
parameterize L's policy

e.g. pick
$\gamma_{0i}(u_i) = p_i\, u_i$ (p_i : unit price charged to F_i)
==>
- Nash game does not depend structurally on γ_0
- Functional optimization on the NE reaction set is now a finite-dimensional optimization problem

But how much degradation in optimality?

Pricing and Admission

NE dictates whether a Follower will be admitted or not (zero resource allocation)



Nonlinear Pricing? General policies for L

- Incentive strategies / incentive design
- Mechanism design

Nonlinear Pricing? General policies for L

- Incentive strategies / incentive design
- Mechanism design
- Find (indirectly) the best L can do, and design a mechanism (policy) that achieves this in the face of uncertainty and rational responses of Fs

Nonlinear Pricing? General policies for L

- Incentive strategies / incentive design
- Mechanism design
- Find (indirectly) the best L can do, and design a mechanism (policy) that achieves this in the face of uncertainty and rational responses of Fs

==> Reverse engineering

With Complete Information

Best possible outcome for L (realistic team solution):

$\{(u_i^\dagger, r_i^\dagger)\} = \arg\max_{(u,r)\geq 0,\ u(\text{total}) < c} r_{\text{total}}$

s.t. $U_i(u_i; \mathbf{u}_{-i}, r_i, w_i) \geq U_i(0; \mathbf{u}_{-i}, 0, w_i)\ \forall i$

With Complete Information (cont.)

Realistic team solution:

$\{(u_i^\dagger, r_i^\dagger)\} = \arg\max_{(u,r)\geq 0,\ u(\text{total}) < c} r_{\text{total}}$

s.t. $U_i(u_i; \mathbf{u}_{-i}, r_i, w_i) \geq U_i(0; \mathbf{u}_{-i}, 0, w_i)\ \forall i$

Incentive design problem: Find $\{\gamma_{0i}\}$ s.t.

$\arg\max_{0 \leq z \leq c\text{ - other opt flows}} U_i(z; \mathbf{u}^\dagger_{-i}, \gamma_{0i}(z), w_i) = u_i^\dagger(\mathbf{w})$

$\gamma_{0i}(u_i^\dagger(w)) = r_i^\dagger(w)$ and $\gamma_{0i}(0) = 0$

Solution: single follower

$u^\dagger(w) = [1 + 2w - \sqrt{(1+8w)}] / 2w$

$r^\dagger(w) = w \log(1 + u^\dagger(w)) + 1 - [1 / (1 - u^\dagger(w))]$

There exists an ε-optimal incentive policy

--- **almost quadratic**

Comparing with best linear policy:

$u^s(w) = 1 - 2 / (1 + \sqrt[3]{w}) < u^\dagger(w)$

$r^s(w) = (1/4)(2\sqrt[3]{w} - 1)^2 (1 + 2\sqrt[3]{w}) < r^\dagger(w)$

Solution: large population

- Admittance: $w_i > w_{av} / 2$
- Team-optimal flows: $u_i^\dagger(w) \sim (2w_i/w_{av}) - 1$
- Team-opt charges:

  $r_i^\dagger(w) \sim w_i \log(2w_i/w_{av})$
- Team-opt revenue:

  $r^\dagger(w)(n) \sim \Sigma_i\, w_i \log(2w_i/w_{av})$

  higher than under linear pricing
- Fi's flow higher if $w_i > (w_{av} / \Sigma_j (\sqrt{w_j})/n)$

What does this lead to?

With non-linear pricing / complete information

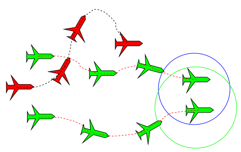
- L achieves almost maximum revenue as though all Fs that pass an admission threshold are fully cooperating (ε-*incentive controllable*)
- Increase in revenue (compared with linear pricing) could be as high as 38 % even with uniform types of Fs in high population regime. With diverse F types, it could be higher than 50%
- Fs willing to pay more benefit from nonlinear pricing, while "poor" Fs suffer.
- Details in Shen-TB (CDC'06, JSAC'07, TelecomSyst'11)

Revisit of UAV application: Adversarial jamming with mobiity

Communication jamming in teams vs teams, with application in formation of UAVs or AGVs

Aerial Jamming Attack on the CommNet of a team of UAVs

- The jammer wants to maximize the time for which communication can be jammed.
- The two UAVs want to minimize the time for which communication remains jammed.



Adversarial action: jamming

- Mobility (as a means for increasing the resilience in autonomous vehicular networks)
- Disruption of communication by adversary (team of adversaries)
- Dynamic/Differential game theory as an underlying framework for designing secure systems.
- Termination: Graph being disconnected, Fiedler value of its Laplacian to become zero.

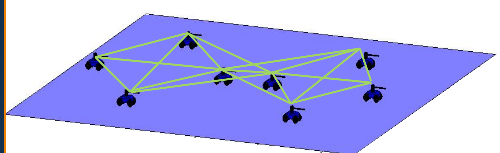
(Bhattacharya & TB JAR'11, Annals of ISDG'12, CDC'12)

Connectivity Maintenance

Many cooperative control tasks require connectivity of the underlying network. Challenge is that each agent has a limited communication range.

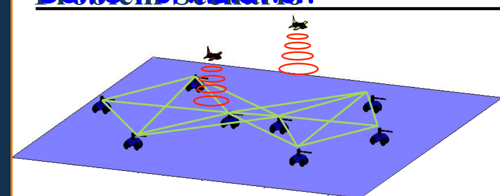
- Formation Control
- Mobile Sensor Networks
- Rendezvous
- Flocking

Problem Scenario



- The network is modeled as a graph G=(V,E(t)) → DYNAMIC GRAPH
- An edge exists between vertices i and j ⇔ Vehicle *i* and vehicle *j* can communicate with each other

Game Formulation



- The vehicles try to maximize the time for which the network remains connected.
- The jammers try to disconnect the underlying communication network, and the vehicles try to retain the connectivity.
- The jammers try to minimize the time for which the network remains connected.

Problem Formulation

Motion Model

$$\text{Pursuer: } \dot{\mathbf{x}}_i^p = f_i(\mathbf{x}_i^p, \mathbf{u}_i^1)$$

$$\text{Evader: } \dot{\mathbf{x}}_i^e = f_i(\mathbf{x}_i^e, \mathbf{u}_i^2)$$

$\mathbf{x}_i \in \mathbb{R}^{n_i}$, $\mathbf{u}_i \in \mathcal{U}_i \simeq \{\phi : [0,t] \to \mathcal{A}_i \mid \phi(\cdot) \text{ is measurable}\}$, $\mathcal{A}_i \subset \mathbb{R}^{p_i}$. $f_i : \mathbb{R}^{n_i} \times \mathcal{A}_i \to \mathbb{R}$ is uniformly continuous, bounded and Lipschitz continuous in $\mathbf{x}_i$ for fixed $\mathbf{u}_i$.

Communication Network

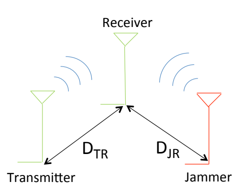
- A Dynamic Graph: $G(V, E(t))$
- Let x_i be represented as vertex $v_i \implies V = \{v_1, \cdots, v_n\}$
- $v_i v_j \in E(t) \Leftrightarrow$ A communication link exists between node i and node j at time t.

Disconnect the communication network $\Leftrightarrow \exists \; i, j$ s.t. no message can be exchanged between node i and node j in a single or multiple hops.

Jamming Model

Jammer to Signal Ratio (JSR)

1. R^n model
$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} 10^{n \log_{10}(\frac{D_{TR}}{D_{JR}})}$$
2. Ground Reflection Propagation
$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} \left(\frac{h_J}{h_T}\right)^2 \left(\frac{D_{TR}}{D_{JR}}\right)^4$$
3. Nicholson
$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} 10^{4 \log_{10}(\frac{D_{TR}}{D_{JR}})}$$



A transmitter-receiver channel is jammed if JSR is greater than a threshold value (JSR_{th}).

$$\Rightarrow \frac{D_{TR}}{D_{JR}} \le \eta = f\left(JSR_{th}, \frac{P_{J_T}}{P_T}, \frac{G_{JR} G_{RJ}}{G_{TR} G_{RT}}, \frac{h_J}{h_T}\right)$$

Laplacian of a Graph G

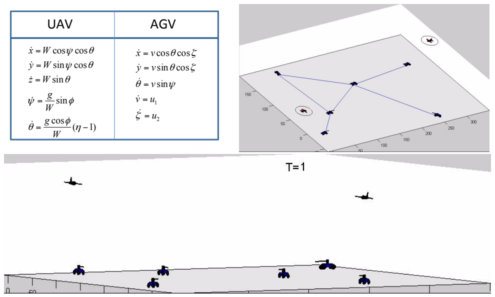
- L(G) is an nxn matrix with
  - ij'th entry -1 if i and j are connected; otherwise 0
  - a_{ii} = minus sum of all a_{ik}'s (except k=i)
- Second smallest eigenvalue of L(G) is the *Fiedler value* – $\lambda_2(L(G))$
- G is connected iff $\lambda_2(L(G)) > 0$

Solution Process

- Framework of differential (P-E) game theory, with termination defined as loss of connectivity — Laplacian L(G) having Fiedler value zero
- Express $\lambda_2(L(G)) = 0$ condition in terms of state variables, for the jamming model adopted ➔ terminal manifold for the Isaacs conditions
- Details in

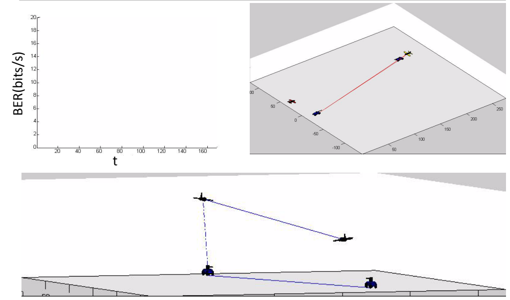
S. Bhattacharya & TB, "Differential Game-Theoretic Approach to a Spatial Jamming Problem," in Annals of DGs, December 2012

Heterogeneous Networks



[Bhattacharya & Başar, Autonomous Robots, 2011]

Double Sided Jamming



[Bhattacharya, Khanafer & Başar, WiOPT'11,CCA'11,GameComm'11, Annals'15]

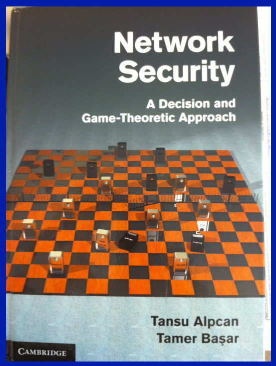
Closure: General Thoughts

- How to design agent interactions so that complex networks have predictable behavior, when
  - there is environmental uncertainty
  - there is adversarial action
  - there is mobility
  - there is mis-alignment of interests
  - there is a large population of agents
- **REVERSE ENGINEERING network architectures** as in mechanism design

Selected References on Game Theory and Security

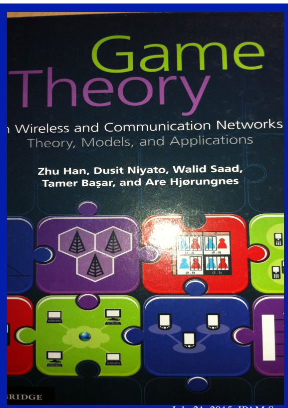
- *Network Security: A Decision and Game-Theoretic Approach* (Alpcan, TB, CUP, 2011)
- *Game theory meets network security and privacy* (Manshei, Zhu, Alpcan, TB, Hubaux; ACM Survey, '13)
- *A hierarchical security architecture for the smart grid* (Zhu, TB; in Hossain, Han, Poor, edts, Smart Grid Communications and Networking, CUP, 2012)
- *Hybrid learning in stochastic games and its applications in network security* (Zhu, Tembine, TB; in Lewis, Liu, edts, Comput Intell Series, IEEE'12)
- *Game Theory in Wireless and Comm Nets* (Han, Niyato, Saad, TB, Hjorunges; CUP, Oct 2011)

July 21, 2015 IPAM Summer School



- Network Security Concepts
- Security Games (SGs)
  - Deterministic SGs
  - Stochastic SGs
  - SGs w information limitations
- Decision Making for Network Security
  - Security risk-management
  - Resource allocation for security
  - Usability, trust, and privacy
- Security Attack and Intrusion Detection
  - Machine learning for intrusion and anomaly detection
  - Hypothesis testing for attack detection

July 21, 2015 IPAM Summer School



- Non-cooperative Games
- Bayesian Games
- Differential Games
- Evolutionary Games
- Cooperative Games
  - Bargaining theory
  - Coalitional game theory
  - Canonical coalitional games
  - Coalition formation games
  - Coalitional graph games
- Auction Theory and Mechanism Design
  - VCG auction / Share auction
  - Double auction
  - Physical layer security
- Applications
  - Multihop networks
  - Cooperative transmission networks
  - Cognitive radio networks
  - Internet networks

July 21, 2015 IPAM Summer School