Games of Strategy

For modeling conflict and cooperation

Schwartz/Teneketzis

CPS Infrastructures
: Effect of Technological Advancements

* Conflict and cooperation of CPS providers: an increase in
  * Cooperation (driven by technological complementarities)
  * Competition (driven by availability of numerous substitutes)

Complex parties' incentives ⇔ multiple externalities

* The role of central authority: improving parties' incentives
  * Higher competition and conflict ⇔ importance of resolving conflicts
  * Threats of security failures ⇔ Importance of investing in security

Central authority's role: conflict mitigation, coordination, and regulation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

CPS viewed as two-sided market : Models both Conflict and Cooperation

* Increased role of Central Authority : necessity to harmonize interactions and improve CPS robustness
  * Managers of infrastructure (platform)
  * Producers (suppliers)
  * Consumers (individual users)
  * Central authority (coordinator/regulator)
* Example: Electric grid
  * Platform Managers: Transmission/Distribution operators
  * Suppliers: Generation plants
  * Users: Customers (large and small)
  * Coordinator: ISO

Today’s talk: Two game-theoretic models

* Resource allocation in strategic multi-battlefield conflicts: Our focus is to solve Blotto games with
  * possibility to add extra fields and alliances
  * possibility to form alliances (cooperation)
* Network design with random faults and strategic attacks
  * Arbitrary (fixed) network structure (a given network topology)
  * Defender faces system failures, and cannot distinguish between
    * Random faults (reliability failures)
    * Strategic attacks (security failures)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

An age-old quest in Game theory: How to allocate scarce resources?

* Under given assumptions on
  * information
  * order of moves (simultaneous vs sequential)
  * player actions: (discreet vs continuous)
  * player objective: (plurality vs majority)
  * players: symmetric (homogenous) vs asymmetric (heterogeneous)
  * game: one-shot vs repeated / dynamic
* Original Colonel Blotto setup: deceptively trivial benchmark

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Colonel Blotto setup

- scare resource (time, money, effort) R
  - battlefields $n = 3$ (town, state, node, server, ...) $j = 1, 2, \ldots n$
  - the values of battlefields: identical $v_j = v$
  - contest (tournament) of two identical players, $i = A, B$ or $i = 1, 2$ or $i = \alpha, \beta$
  - order of moves: simultaneous
  - player actions: continuous
  - player objective (*plurality* vs *majority*)
  - players are symmetric (identical) $R_\alpha = R_\beta$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Applications of Blotto

- traditional warfare
  1. routing choices for supply support
  2. across distinct battlefields
- politics (elections under different rules)
  - optimization of fund raising strategy (time allocation)
  - optimization of resources during the contest
- Economics (IO) [Corporate strategy for multi-product markets]
  - research and development (R&D)
  - resource allocation for advertizement

Our research plan:

Blotto for CPS infrastructure protection & defense

Colonel Blotto: Identical players

- Two-players constant-sum complete information static game
- Identical (symmetric) resource case [formulated Borel 1921]
- Battlefields: identical value
- N battlefields ($N = 3$) [solved Borel & Ville (1938)]
- N battlefields ($N > 3$) [Gross & Wagner (1950)]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Colonel Blotto: Non-identical players

- Player α has resource α
- Player β has resource $\beta < \alpha$
- Battlefields: identical value
- with ($N = 2$) [Gross & Wagner (1950)]
- with ($N > 2$)[Roberson (2006), Kvasov (2007)]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Who wins the battlefield?

In a generic case, Colonel Blotto game admits no pure strategy equilibrium. CSF is a probability for player i $(i = \alpha, \beta)$ to win each contest j $(j = 1, \ldots, n)$, and let $x_{i,j}$ and $x_{-i,j}$ player i resources (investments) for contest j, other player(s) resources for j

$$p(x_{i,j}, x_{-i,j}) = \frac{x_{i,j}}{x_{i,j} + x_{-i,j}}$$

If noise is present, and $m \geqslant 0$ some noise is present, with $m = 0$ – all is noise, investments are irrelevant, if a higher m noise decreases.

$$p(x_{i,j}, x_{-i,j}) = \frac{x_{i,j}^{m}}{x_{i,j}^{m} + x_{-i,j}^{m}}$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

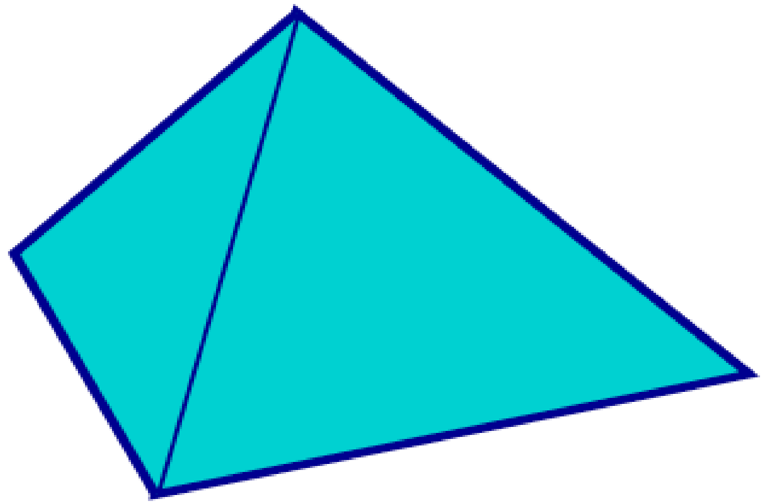
Payoffs

- Player A decides on the allocation of resources across the battlefields $\mathbf{a} = \{\alpha_1, \ldots, \alpha_N\}$
- Player B, decides on $\mathbf{b} = \{\beta_1, \ldots, \beta_N\}$
- Constraint Regions: $\mathcal{A} := \left\{\mathbf{a} : \sum_{i=1}^{N} \alpha_i \leqslant \alpha\right\}$ and $\mathcal{B} := \left\{\mathbf{b} : \sum_{i=1}^{N} \beta_i \leqslant \beta\right\}$
- On each battlefield, player with maximum resource wins and receives a payoff $\frac{1}{N}$
- If equal resource on a battlefield, both player share the payoff, that is, each player receives a payoff $\frac{1}{2N}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Overview of Results

- $\mathcal{A}$ and $\mathcal{B}$ looks like a solid simplex



- No Nash equilibrium in pure strategies
- Nash equilibrium exists in mixed strategies with unique player payoffs (Roberson 2006)
- Measures $\mu_i \in \wp(\mathbb{R}_+^N)$ such that $supp(\mu_A) \subset \mathcal{A}$ and $supp(\mu_B) \subset \mathcal{B}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Results

- The payoff functions are expressed as

$$J_i(N, \mu_A, \mu_B) = \sum_{j=1}^{N} \frac{1}{N} \int_0^\infty \pi^j_\# \mu_{-i}([0, x)) \pi^j_\# \mu_i(dx)$$

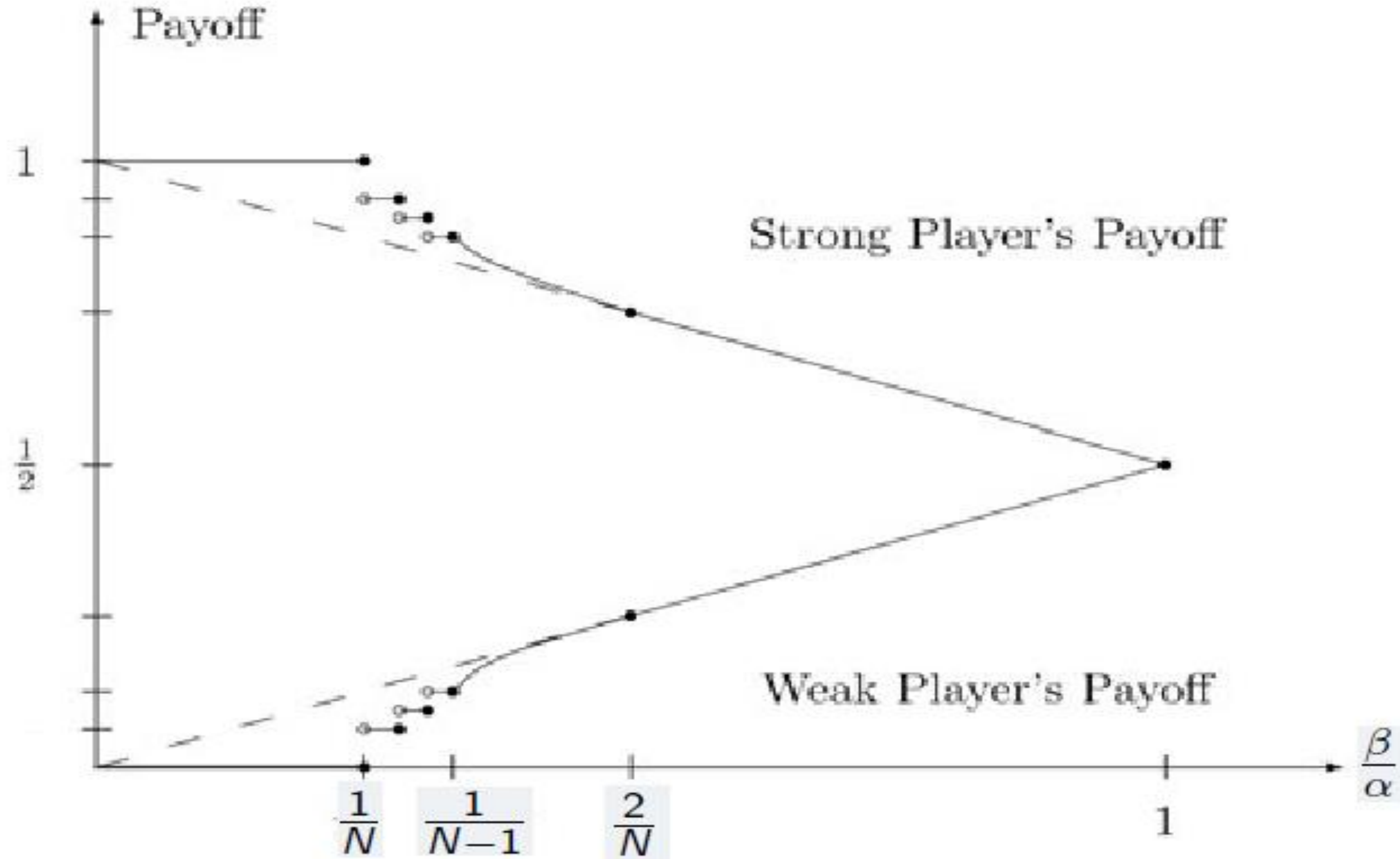
- Payoffs dependent on the marginal distributions on the battlefields

Main Result for $\alpha \leqslant \beta$

Case	Player A's Payoff	Player B's Payoff
$\frac{2}{N} \leqslant \frac{\beta}{\alpha} \leqslant 1$	$1 - \frac{\beta}{2\alpha}$	$\frac{\beta}{2\alpha}$
$\frac{1}{N-1} \leqslant \frac{\beta}{\alpha} < \frac{2}{N}$	$1 - \frac{2}{N} + \frac{2\alpha}{N^2\beta}$	$\frac{2}{N} - \frac{2\alpha}{N^2\beta}$
$\frac{1}{N} \leqslant \frac{\beta}{\alpha} < \frac{1}{N-1}$	complicated expression	1 − comp. expr.
$\frac{\beta}{\alpha} < \frac{1}{N}$	1	0

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Graphical Representation



Proof Outline

$$J_i(N, \mu_A, \mu_B) = \sum_{j=1}^{N} \frac{1}{N} \int_0^\infty \pi^j_\# \mu_{-i}([0, x)) \pi^j_\# \mu_i(dx)$$

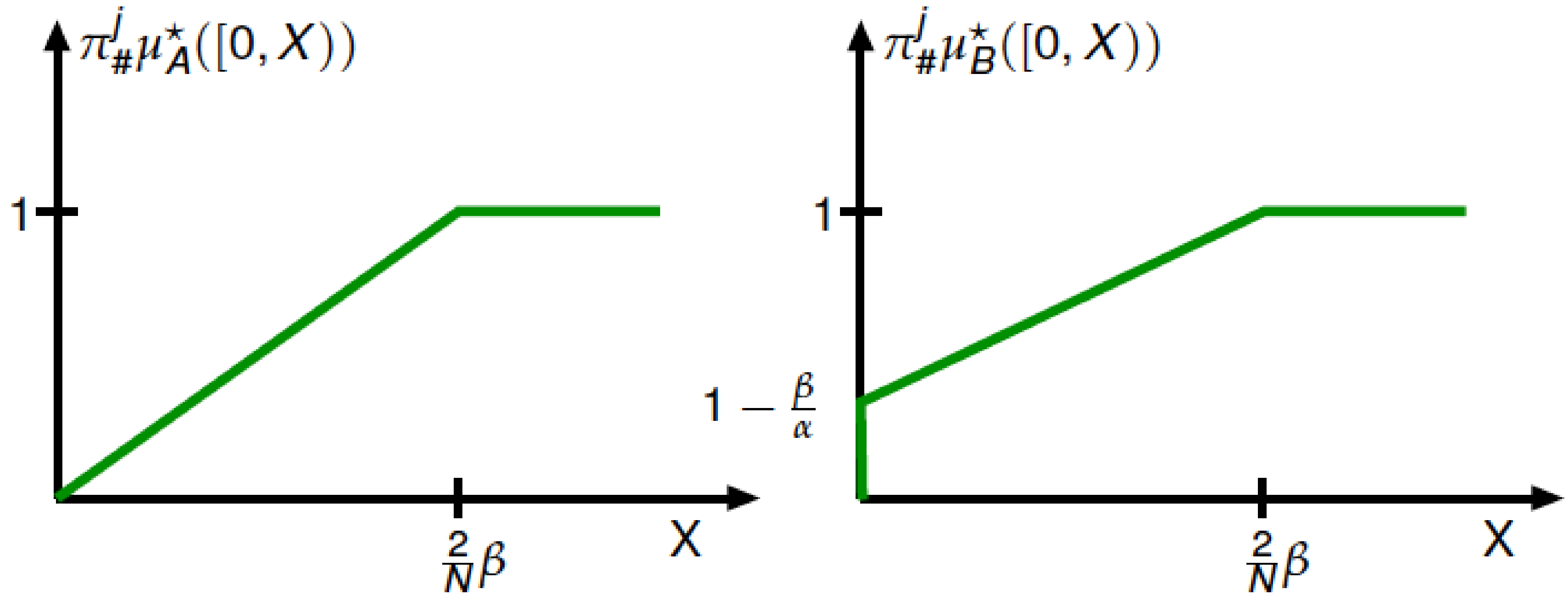
$$\text{such that} \qquad supp(\mu_A) \subset \mathcal{A}, supp(\mu_B) \subset \mathcal{B}$$

- Three steps in the proof
- Step 1: Find the reaction curves of the players
  - For a fixed strategy of one player, marginal distribution on each battlefield?
- Step 2: Equilibrium marginal distributions on the battlefields?
- Step 3: Is there a joint distribution that satisfies the constraint on $supp(\mu_i)$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Marginal distributions at Nash Equilibrium

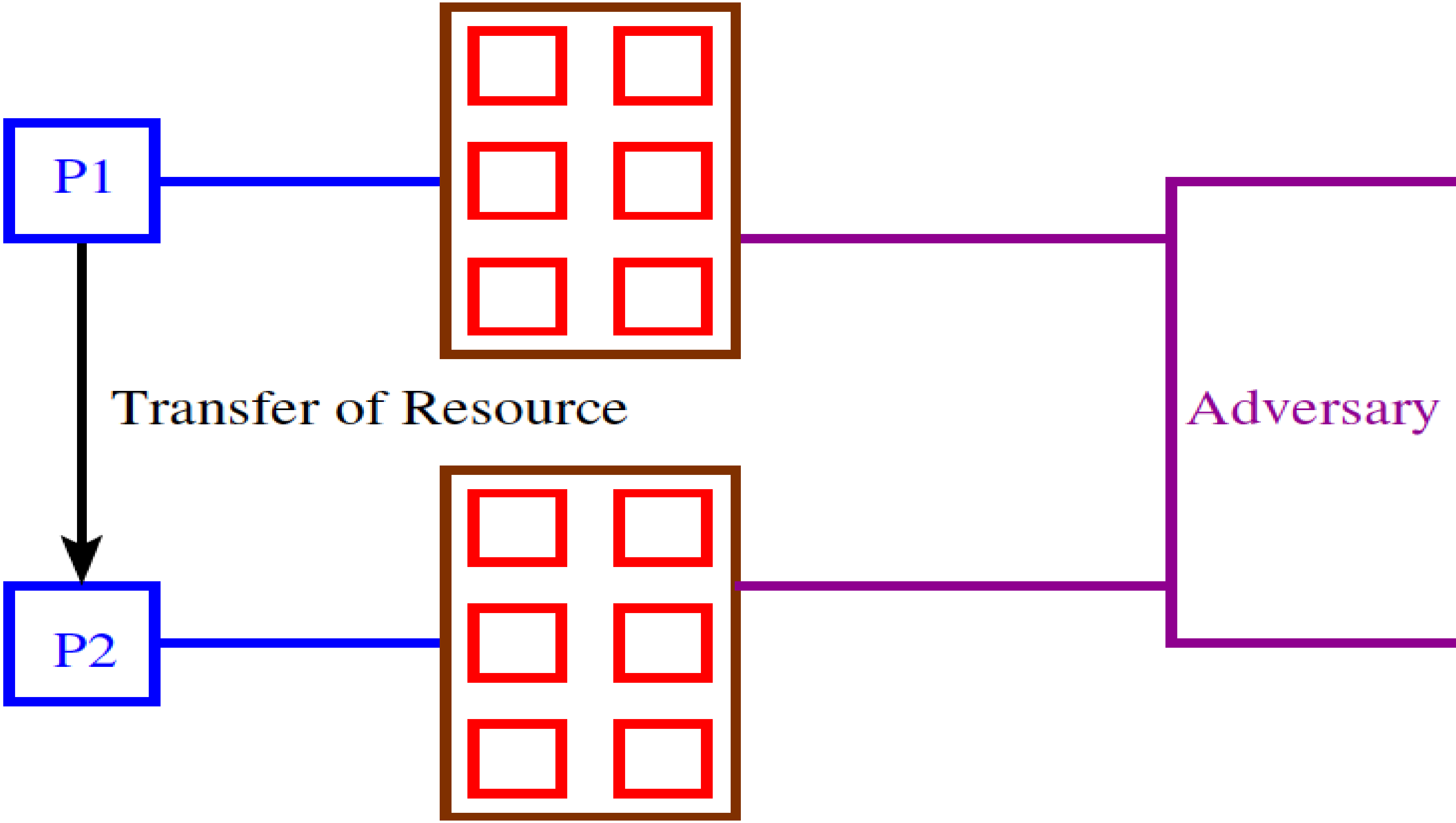
Assume $\frac{2}{N} \leqslant \frac{\beta}{\alpha} \leqslant 1$



Joint distributions μ_1 and μ_2 are constructed using the marginal distributions in the paper

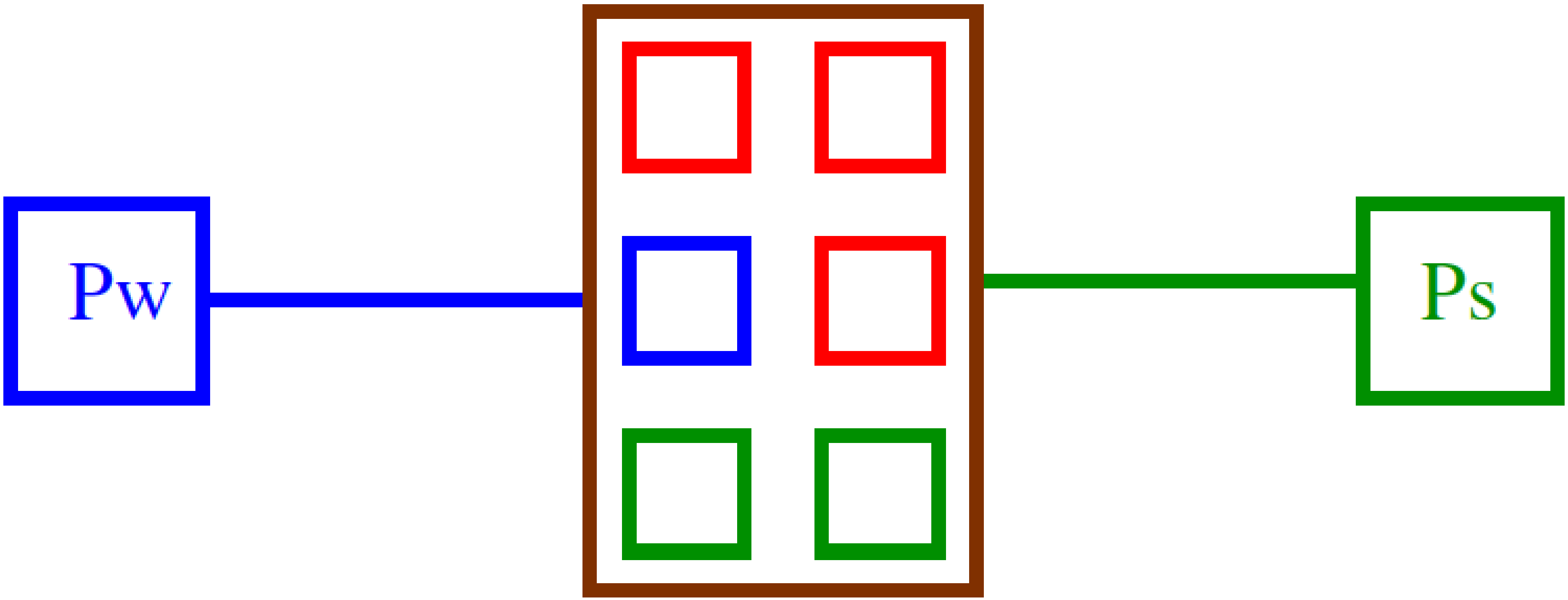
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Extension I: Coalitional Colonel Blotto

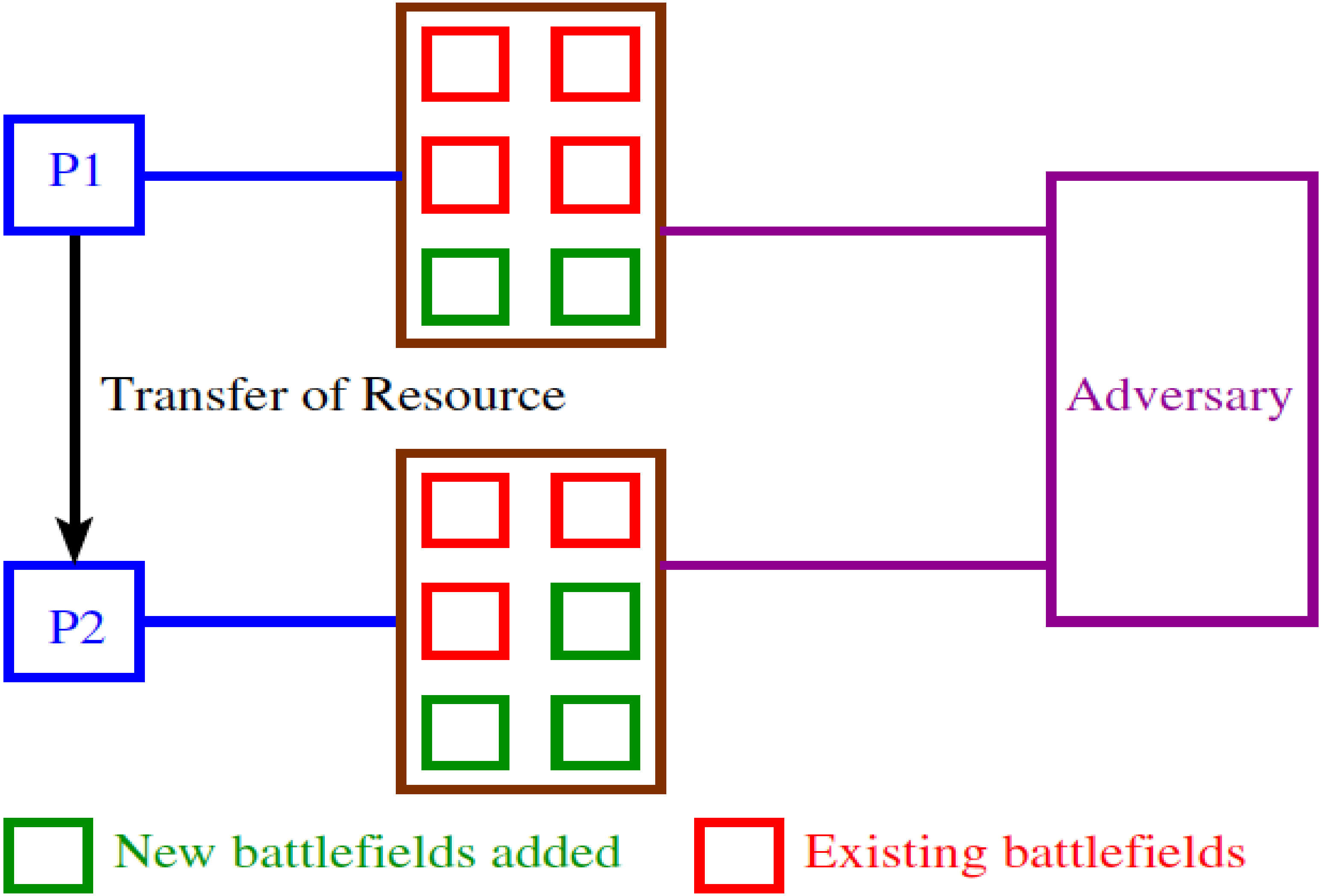


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Extension II: Colonel Blotto with Endogenous Battle fields



Our focus: Coalitional Colonel Blotto with Endogenous Battle Fields



Summary of Results on Blotto Games

- Blotto Games provide key insights into resource allocation
- Generically, Nash equilibrium only in mixed strategies
- Adding battlefields tend to be beneficial to players if it is “cheap enough”
- Voluntary coalitions may be beneficial to players due to effects on equilibrium behavior of the adversary
- Our work
  - We generalizes two extensions
  - provides characterization of Nash equilibrium in certain parameter regions

Network Design Game for CPS

A problem of information deficiency

Due to prohibitive costs of determining the cause of a failure, reliability and security failures are frequently indistinguishable.

Game with reliability-security failures

- Network: Undirected weighted graph $G = (V, E, w)$
- Network manager: defender
- Failures:
  - Reliability failure R: Due to *Nature*/random fault (π)
  - Security failure S: Due to a strategic attack ($1 - \pi$)
- How should defender design his defenses?

[G. Schwartz, S. Amin, et al.]

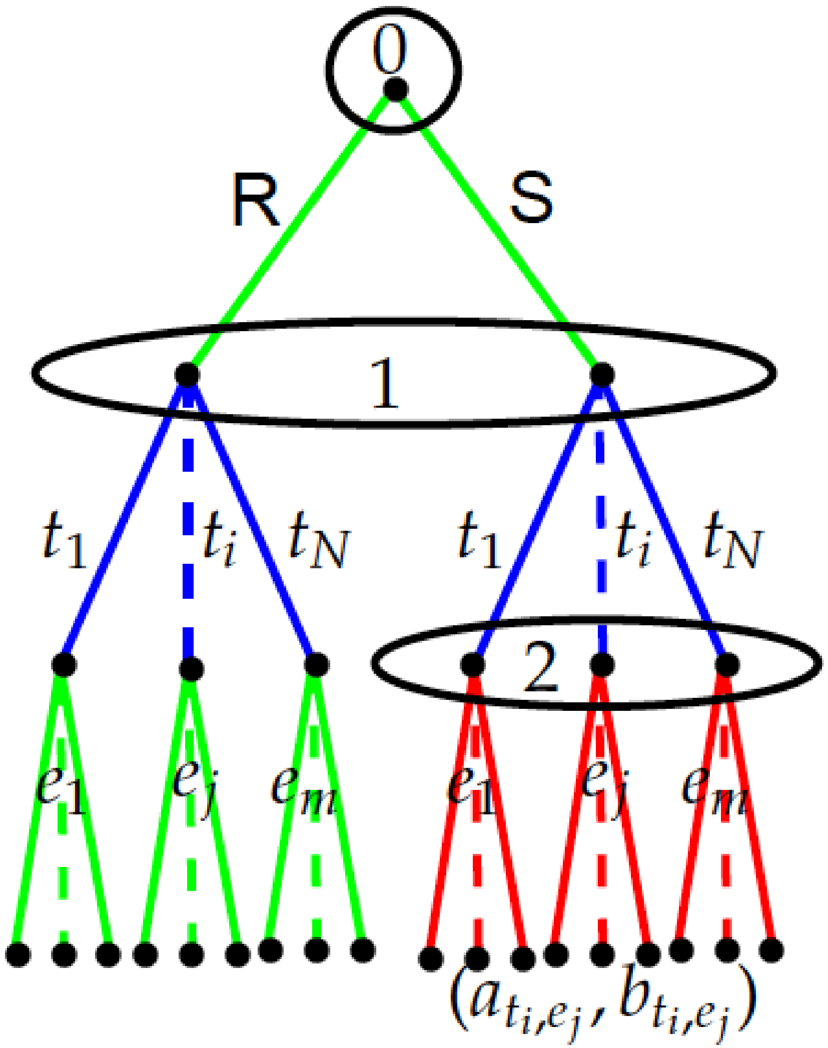
Reliability and Security Failures

Game with reliability-security failures

- Network manager: defender
- Failures:
  - Reliability R: random faults/*Nature* ($P(R) = \pi$)
  - Security S: strategic attacker $P(S) = 1 - \pi$
- Failure probability of an edge $e \in E$:

$$P(f_e) = \pi\gamma_e + (1-\pi)\beta_e, \quad \forall e \in E,$$

  - $\gamma_e = P(f_e \mid R)$, $\beta_e = P(f_e \mid S)$
  - Fault probabilities: $\gamma = (\gamma_{e_1}, \ldots, \gamma_{e_j}, \ldots, \gamma_{e_m})^T$
  - Attack probabilities: $\beta = (\beta_{e_1}, \ldots, \beta_{e_j}, \ldots, \beta_{e_m})^T$



Network Design Game

Attacker-Defender subgame

- Defender: chooses a spanning tree $t \in \mathscr{T}$
- Attacker: chooses an edge $e \in E$

Nature-Defender subgame

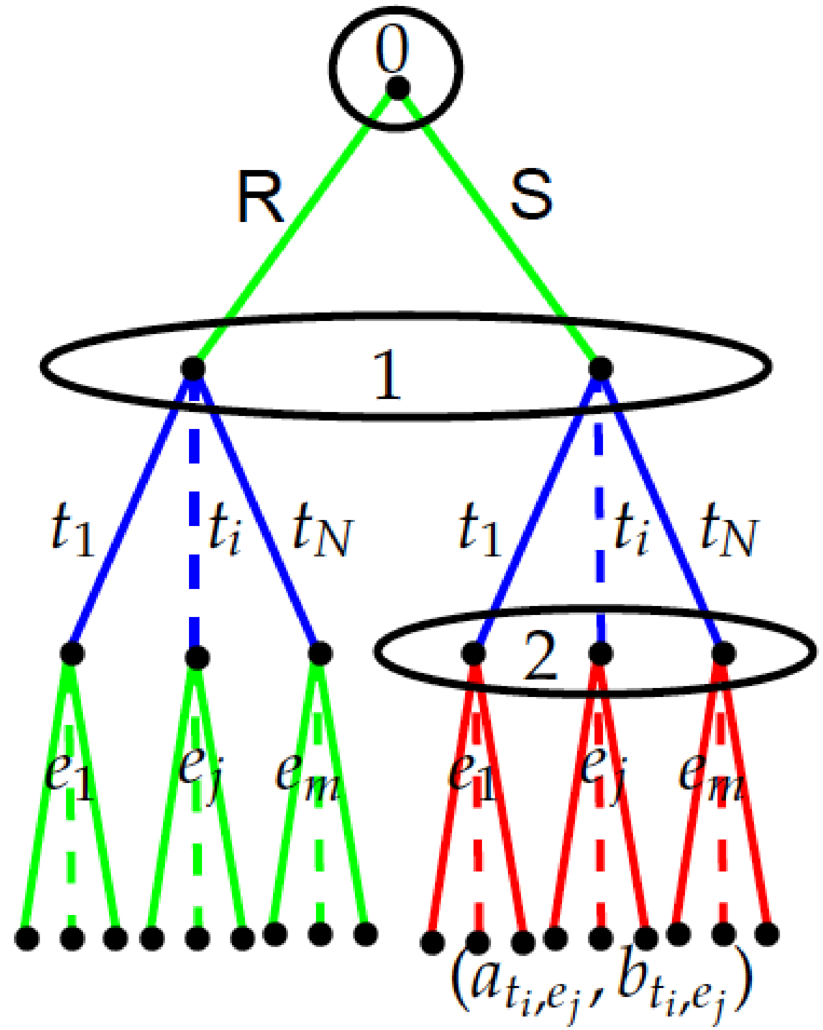
- Defender: chooses a spanning tree $t \in \mathscr{T}$
- Nature: given failure prob. γ_e over edges

Attacker-Nature-Defender game

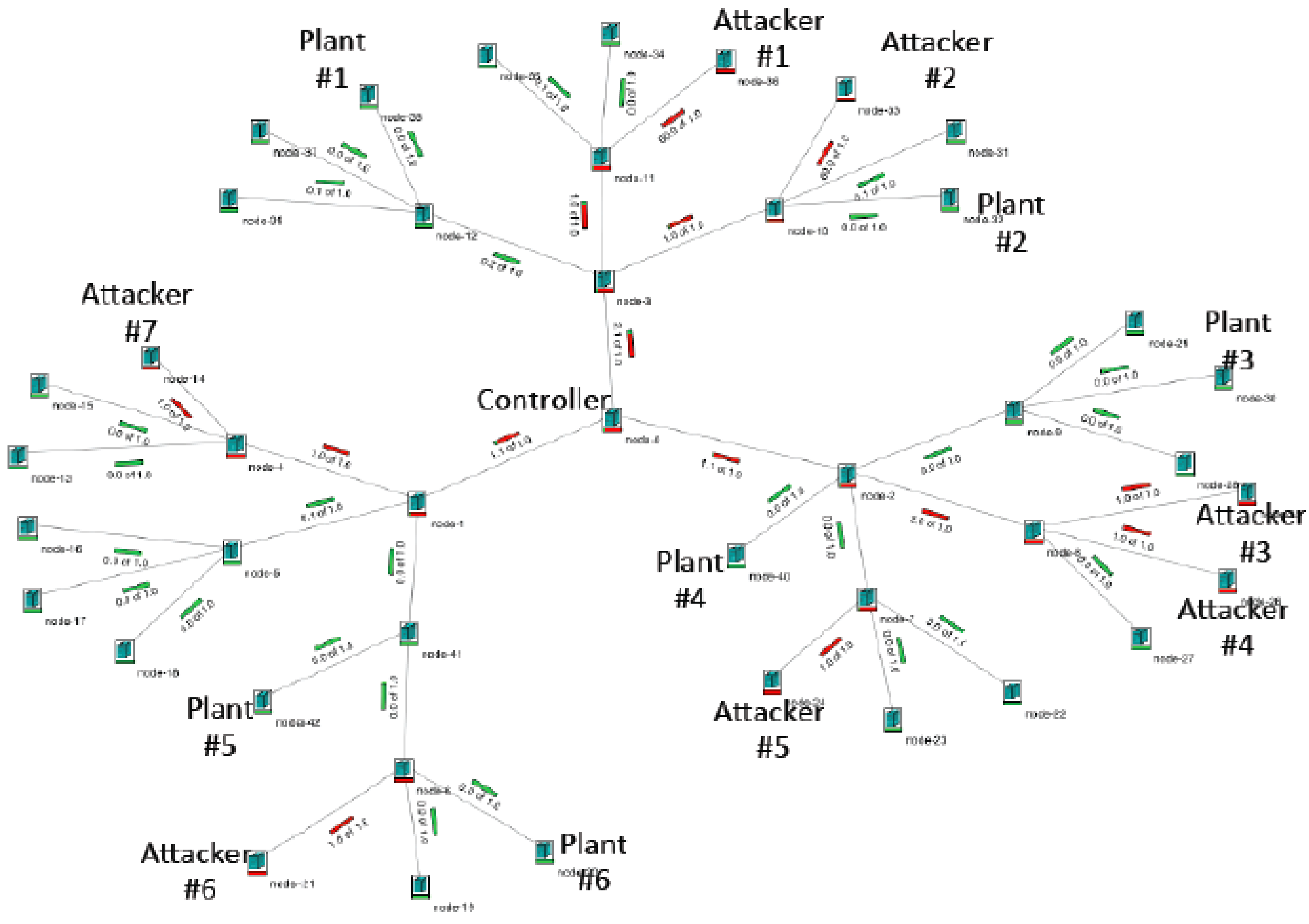
- Imperfect information: defender faces aggregate failure probabilities:

$$P(f_e) = \underbrace{\pi\gamma_e}_{\text{reliability}} + \underbrace{(1-\pi)\beta_e}_{\text{security}}$$

- Common knowledge: π and γ.
- How does Nash Eq. depend on π & γ?



Application



Summary of the talk

* Strategic resource allocation (Blotto games):
  We characterize equilibria of asymmetric Blotto game with
  (i) Endogenous number of battlefields
  (ii) Player alliances
* Network design with security and reliability failures:
  We find all equilibria for a game with
  (i) General network topology and values of the nodes
  (ii) Network operator knows only the relative frequencies of random faults and strategic attacks

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS