COMPASS Workshop Agenda

Submit all COMPASS specific questions to COMPASS@darpa.mil by 1300

Introduction	
Time (ET)	**Speaker**
0915 - 1000	Online and In-person Registration
1000 - 1005	Dr. Evan Gorman & Major (U.S. Army) Nikesh Kapadia *DARPA Innovation Fellows - Welcoming Remarks*
1005 - 1020	Ms. Ana Saplan, DARPA ARC Manager *Introduction to DARPA & ARC Overview*
1020 - 1045	Dr. Evan Gorman & Major Nikesh Kapadia *COMPASS Overview*
1045 - 1100	Break

DoD Challenge Area # 1 – Decisions Under Uncertainty	
1100 - 1130 20 min speaker 10 min Q&A	Dr. Tim McDonald, RAND Associate Policy Researcher *Structuring Analysis for Complex National Security Challenges*
1130 - 1200 20 min speaker 10 min Q&A	Dr. Jorge Poveda, University of San Diego, Electrical and Computer Engineering *Stochastic deception in non-cooperative games*
1200 - 1300	Lunch
1300	Deadline to submit questions virtually to COMPASS@darpa.mil

DoD Challenge Area # 2 - Critical Infrastructure	
1300 - 1330 20 min speaker 10 min Q&A	Dr. David Alderson, Naval Postgraduate School, Center for Infrastructure Defense *Resilience in infrastructure systems*
1330 - 1400 20 min speaker 10 min Q&A	Dr. Filippo Radicchi, Indiana University Bloomington, Luddy School of Informatics, Computing, and Engineering *Assessing the robustness of critical infrastructures via network percolation*
1400 - 1415	Break

Other DoD Challenge Areas	
1415 - 1445 20 min speaker 10 min Q&A	Mr. Jon Jeckell, U.S. Army, Contested Logistics Cross Functional Team *Decision support for logistics networks*
1445 - 1515 20 min speaker 10 min Q&A	Dr. David Dewhurst, DARPA Program Manager *Establishing resilient supply chains and financial security*

Conclusion	
1515 - 1600	Dr. Evan Gorman & Major Nikesh Kapadia *COMPASS Answer Session and Closing Remarks*

DARPA Overview

Ana Saplan
Advanced Research Concepts

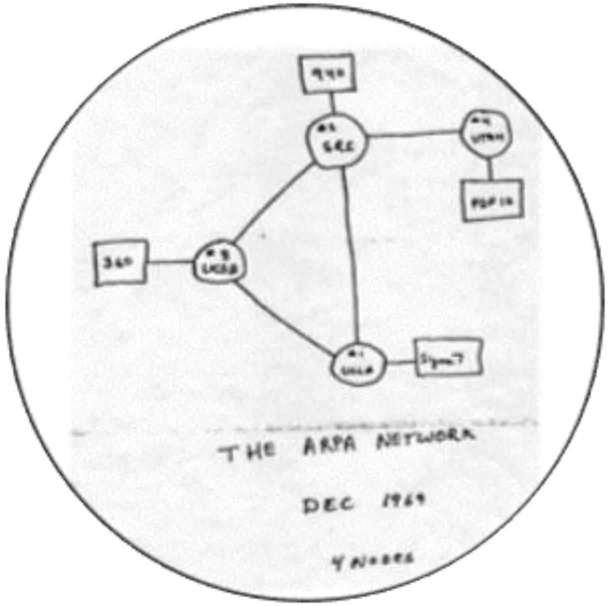
COMPASS Workshop

March 5, 2025

Create breakthrough, paradigm-shifting solutions

Accept and manage significant technology risk

Disrupt or massively accelerate technology roadmaps



The Internet

Foundations of GPS

Advanced Prosthetics

Prevent and Impose Technological Surprise

PEOPLE

- Exceptional technologists
- Limited tenure
- Autonomy

PROCESSES

- No in-house labs
- Metrics-based
- Programs have end-dates

CULTURE

- Drive for off-scale impact
- High risk / high reward
- Honor in public service

DARPA Technical Offices

Biological Technologies Office

- Maintain force readiness
- Tactical warfighter care and functional restoration
- Operational resilience and logistical security
- Biosensors and novel methods and materials

Defense Sciences Office

- Materials
- Sensing
- Computation
- Operations
- Collective intelligence
- Emerging threats

Information Innovation Office

- Proficient AI
- Advantage in cyber operations
- Confidence in the information domain
- Resilient, adaptable, and secure systems

Microsystems Technology Office

- Disruptive microsystems
- Edge processing
- Microsystems manufacture

Strategic Technology Office

- Advanced sensors and processing
- Battlefield effects
- Command, control, and communications
- System of autonomous systems
- Empowered human decision making

Tactical Technology Office

- Tactical systems
- Platforms, systems, and technologies that enable new warfighting constructs
- Reimagination of missions across maritime, ground, air, and space domains

DARPA: Create and prevent technological surprise

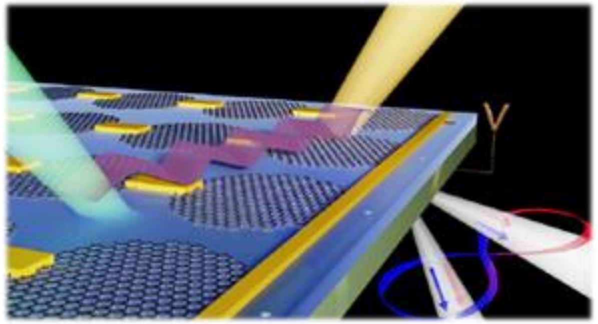
DSO—"DARPA's DARPA"

- Creates opportunities from scientific discovery
- Invests in multiple, often disparate, scientific disciplines--everywhere the rest of DARPA is, and more
- Focuses on mission-informed research

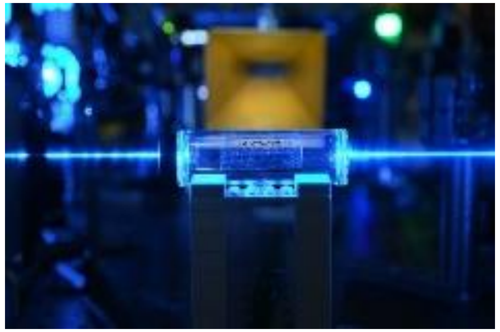
DSO: The Nation's first line of defense against scientific surprise

DARPA

DSO Thrust Areas

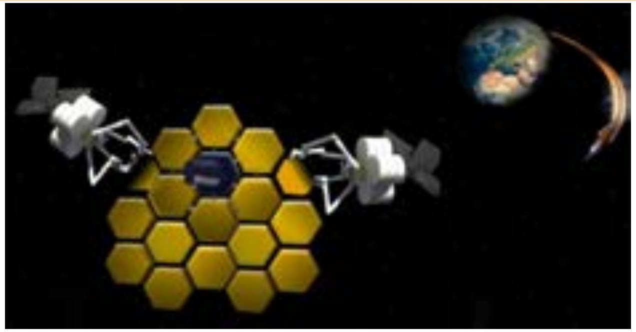


Novel Materials & Structures
Fundamentals to Fabrication



Sensing & Measurement
Micro/Macro; Quantum Limits

Computation & Processing
Classical Algorithms to Quantum Computing



Enabling Operations
Novel Phenomena to Systems and Structures

Collective Intelligence
Basics of Intelligence to People/AI

Emerging Threats
Uncertainty and Global Events

Advanced Research Concepts (ARC)

HyBRIDS
Hybridizing Biology and Robotics through Integration for Deployable Systems

CRYSTAL
Crystal Substrate Bonding Technologies and Algorithms

- ARC solicitations focus on exploring high-risk/ high-reward questions
- Sponsor "blue-sky" innovative ideas with scientists from academia, startups, industry, and government
- 8 topics targeted annually; ~20-30 ideas per topic
- Fund 1 person-year per idea, up to $300K
- Streamlined proposal and contracting process

Novel Topics

Assurance in AI	Neuroscience	Next-generation Biotechnology	Operating in Extreme Environments	Quantum Materials

DARPA Innovation Fellowship

- 2-year Fellowship for early career scientists and active-duty military officers
- Seek out ideas that can change the world (ARC topics)
- Work with the S&T community on high-impact, exploratory efforts at the cutting edge
- Assess the impact of further investment towards critical technology for national security
- Join an ecosystem of innovators, scientists, and military servicemembers

- To begin the application process, please visit this website: https://innovationfellowship.darpa.mil/
- U.S. citizenship is required

DARPA Innovation Fellowship

What is the Innovation Fellowship?

A 2-year Fellowship at DARPA for early career scientists and active-duty military officers, who received their Ph.D. within the last 5 years. Fellows develop and manage the Advanced Research Concepts (ARC), a portfolio of high-impact exploratory efforts to identify breakthrough technologies for the Department of Defense.

Why become an Innovation Fellow?

Drive technological innovation

Fellows have the opportunity to influence the direction of defense research through developing ARC topics, evaluating proposals, making funding decisions, and assessing the impact of further investment on problems of importance to national security.

Engage with prominent scientists

Fellows travel across the country to visit leading researchers at top university, industry, and government labs and learn about the revolutionary research they are conducting.

Strengthen your transferable skills

Fellows work across a broad range of scientific fields and gain a deep understanding of the big-picture scope of the state of the art of science and technology.

Advance your career opportunities

Join an extraordinarily rich, technologically-focused network of DARPA Program Managers, military service members, and scientific and technical experts.

Advanced Research Concepts (ARC)

- Portfolio of fundamental research efforts for assessing the impact of further investment on problems of national security importance.
- Several topics are released per year, each targeting a specific technical area.

https://www.darpa.mil/arc

For more information on the Fellowship visit: https://www.darpa.mil/work-with-us/darpa-innovation-fellowship

To begin the application process, please visit this website: https://innovationfellowship.darpa.mil/

U.S. citizenship is required

ARC Proposal and Award Structure

Advanced Research Concepts (ARC)

ARC solicitations focus on answering high-risk/high-reward questions

~ 8 topics per year

→

Streamlined application

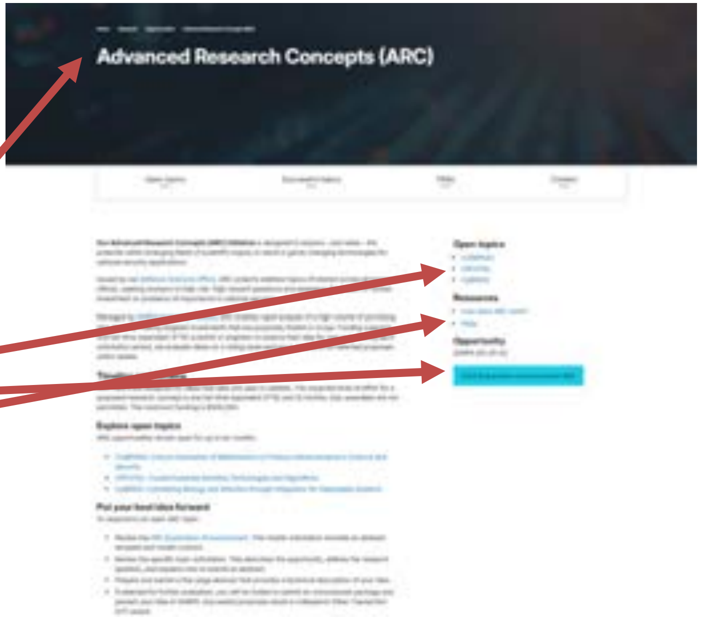
Selection to award in 2 weeks

Select ~30 ideas per topic
> 200 ideas annually

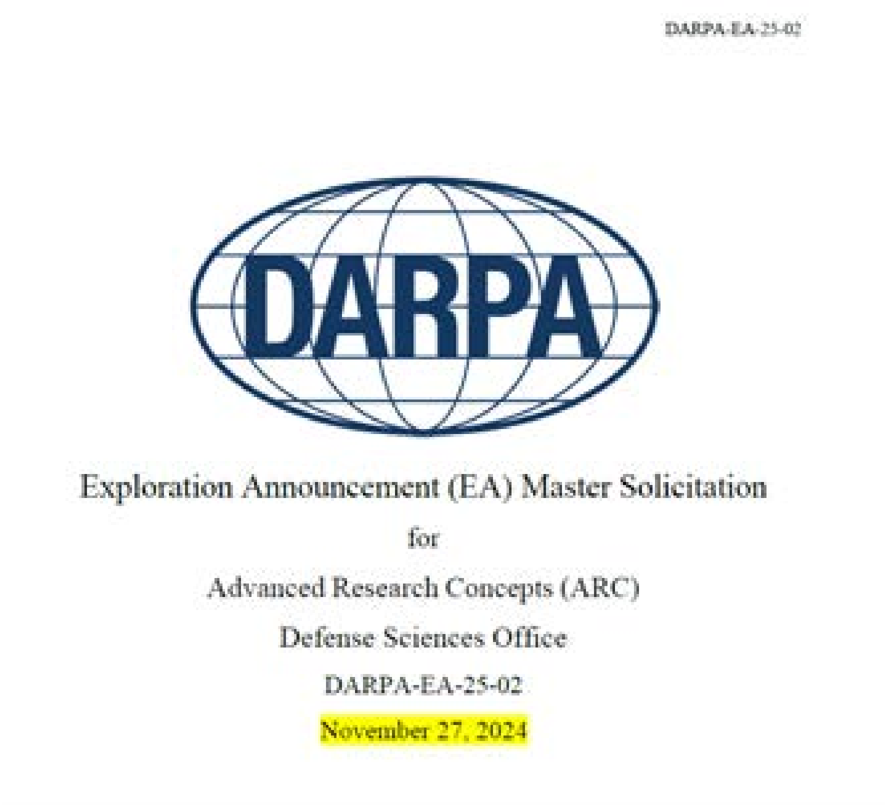
→

Each contract will fund one FTE for one year up to $300K

- Focused on soliciting and evaluating many ideas
  - Equipment, materials, and ODCs combined must not exceed $10,000
  - Subawardees, travel and publication costs not permitted
- Research Other Transaction (OT) awards
- More information: https://www.darpa.mil/research/opportunities/arc
  - DARPA-EA-25-02, posted here
  - Open ARC Opportunities posted here
  - Tutorial on how to propose / FAQs



ARC Structure – The Exploration Announcement


DARPA-EA-25-02

Exploration Announcement (EA) Master Solicitation

for

Advanced Research Concepts (ARC)

Defense Sciences Office

DARPA-EA-25-02

November 27, 2024

The Overarching Solicitation

- Describes the proposal process
  - Abstract Submission Process (Sections 3.1)
  - Oral Proposal Package (Sections 3.2)
- Provides Award information for negotiation-free Research Other Transaction (OT)
- Establishes Eligibility criteria
- Rolling submissions and evaluations

"ARC Opportunity" topics are released under the Master Solicitation as DARPA-EA-25-02-XX

COMPASS closes May 12th, 2025!

Email questions to: COMPASS@darpa.mil

ARC Structure – The Submission Process

3 Application and Submission Information

3.1 Abstracts

Proposers must submit an Abstract against an ARC Opportunity to be considered for an award. DARPA will only accept UNCLASSIFIED Abstracts. Proposers must use the Abstract template provided as **Attachment A** to this EA. The submitted Abstract must consist of the following sections and is limited to five (5) pages in length.

Master Solicitation, page 6

3.2 Oral Proposal Package (OPP)

Each ARC Opportunity will solicit for Abstracts only. DARPA may respond to conforming Abstracts with a Notice of Non-Selection, or an Invitation to Submit an OPP and participate in an Oral Presentation (see Section 7.1). Proposers will be notified of non-conforming determinations via letter. The following information is provided to ensure potential proposers know the anticipated content and format of the OPP. If the invitation to submit includes minimal deviations from this content and format, the invitation to submit will take precedence.

Master Solicitation, page 7

- Proposers submit 5-page Abstracts
- Abstracts are reviewed by DARPA for selectability
- DARPA issues invitation to submit an Oral Proposal Package (includes an oral presentation to DARPA) to selected abstract submitters
- Selected proposals issued a "Research Other Transaction" award have a maximum of 5 business days to sign and return the agreement to DARPA (Master solicitation, section 2)
    - DARPA does not expect to negotiate changes to the terms and conditions of this agreement in any OT issues to an awardee

Questions?

Submit questions to COMPASS@darpa.mil

Critical Orientation of Mathematics to Produce Advancements in Science and Security (COMPASS) Webinar

Dr. Evan Gorman
DARPA Innovation Fellow

MAJ Nikesh Kapadia (U.S. Army)
DARPA Innovation Fellow

Advanced Research Concepts (ARC)
Opportunity Overview
DARPA-EA-25-02-03

03/05/2025

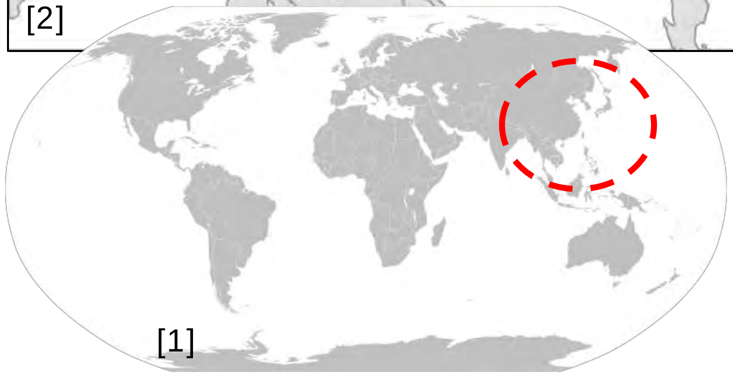
Overview of this presentation

Why do we need your help?

How can you help?

What are we asking for?

Imagine a hypothetical scenario where conflict erupts between North Korea and South Korea



The U.S. is called on evacuating thousands of civilians from South Korea.

What kinds of challenges would we face in this scenario?

How does the U.S. and South Korea deal with …

Congested roads

Finite transportation

Establishing assembly points

Managing crowds

We need your help to enhance decisions in complex situations

Why do we need your help?

How can you help?

What are we asking for?

[1] OpenStreetMap, CC BY SA 2.0

Why do we need your help?

Enhance decisions (speed, accuracy),
In today's environment (uncertain, dynamic, complex)

Key decisions

1. When/where should I apply my resources? (e.g., opening an assembly point in location X or location Y)
2. When/where do I accept risk? How much risk? (e.g., what would happen if I don't open an assembly point in location Y?)

Operating environment

1. Uncertain. Where will adversaries disrupt the evacuation? (e.g. attack on assembly point)
2. Dynamic. When will transportation (air, land, sea) arrive? (irregular schedule of international flights)
3. Complex. How will my actions impact other activities? (e.g. impact on security forces using the same roads)

How can we enhance decisions in an uncertain world?

Why do we need your help?

Enhance decisions (speed, accuracy)
In today's environment (uncertain, dynamic, complex)

How can you help?

What are we asking for?

- Today, national security challenges are more complex, dynamic, and uncertain than ever before.

- Success hinges on our ability to make real-time, accurate decisions within vast, interdependent systems.

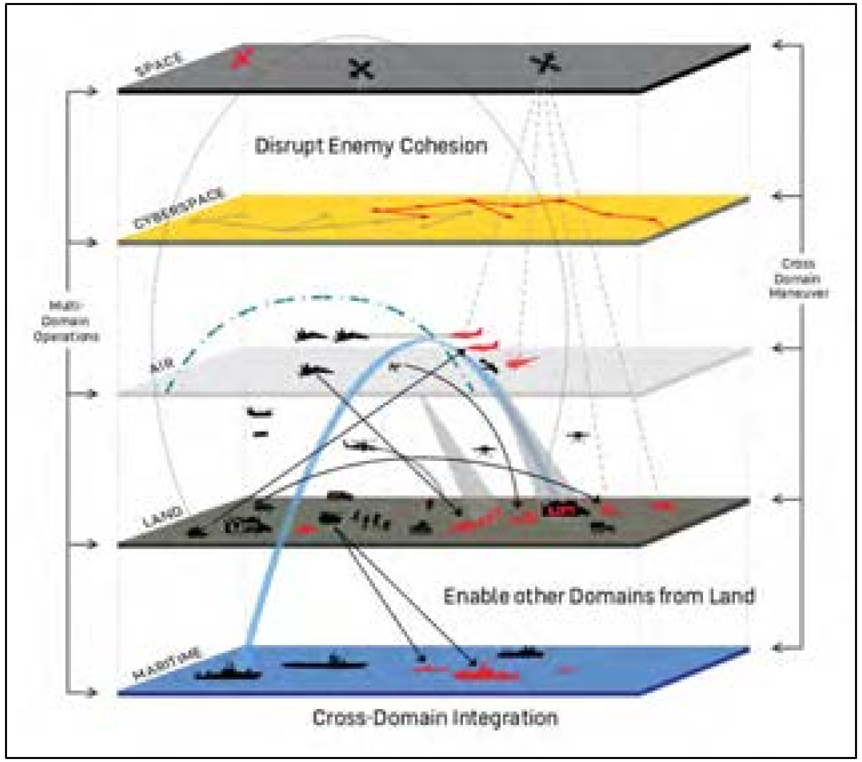


Illustration of the military's need to see the environment in multiple, interrelated domains (air, land, sea, cyber, space).

[1] U.S. Army, Public Domain

Focus Areas to enhance decisions in an uncertain world

Why do we need your help?

Enhance decisions (speed, accuracy)
In today's environment (uncertain, dynamic, complex)

How can you help?

What are we asking for?

How can you help?

Advancements in modern probability and complex systems are revealing potential frameworks to tackle these challenges.

Some examples:

- Heterogeneous and multiscale behavior in large systems or networks
  - McKean-Vlasov processes – Multi-agent, opinion dynamics, power systems
  - Graph signal processing – Infrastructure or logistics network analysis
- Stochastic processes in dynamic, random, or information-limited environments
  - Stochastic inverse problems – Noisy signal localization, decisions under uncertainty
  - Rough path theory – Intrusion detection, tracking, robust filtering
- Random geometric structures in high dimensions
  - Stochastic geometry – sensor placement, path planning, geospatial intelligence
  - Random graphs – distributed sensing, satellite constellations, communications

And much more... We encourage creative, far-reaching exploration of how your mathematical field could help support any aspect of national security.

It starts with formulating the problem

Why do we need your help?

Enhance decisions (speed, accuracy)
In today's environment (uncertain, dynamic, complex)

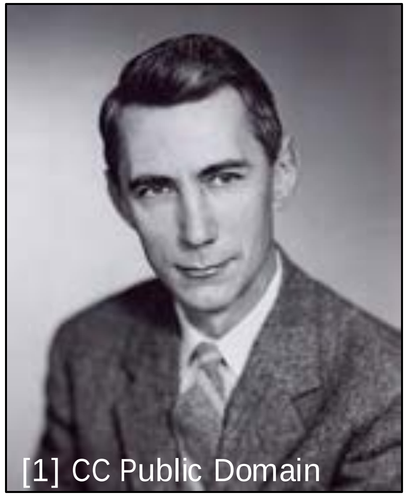
How can you help?

Modern probability and complex systems theories

What are we asking for?

Problem formulation

1948: Claude Shannon formulates information entropy



[1] CC Public Domain

$$\mathrm{H}(X) := -\sum_{x \in \mathcal{X}} p(x) \log p(x)$$

Applications

Reed–Solomon Codes (1960):
Space transmission

Linear Predictive Coding (1966):
Audio signal processing

Discrete Cosine Transform (1972):
Digital media compression

Turbo Codes (1993):
Wireless communications

Adaptive bitrate (2002):
Multimedia streaming

Locally Repairable Codes (2012):
Cloud storage

.
.
.

Robust problem formulation enables decades of technological advancements

COMPASS: Definitions and overview of scope

Why do we need your help?

Enhance decisions (speed, accuracy) In today's environment (uncertain, dynamic, complex)

↓

How can you help?

Modern probability and complex systems theories

↓

What are we asking for?

What are we asking for?

ARC Question: How can new mathematical frameworks enable paradigm shifting problem formulations that better characterize complex systems, stochastic processes, and random geometric structures?

By the end of COMPASS, each performer delivers:

1. Mathematical Framework: Investigate a completely novel connection between a mathematical framework and a Defense science or technology application area
2. Problem Formulation: Formulate a Defense related problem within this mathematical framework and justify that this new approach addresses significant gaps in current state of the art methods or enables entirely new capabilities
3. Roadmap: Chart-out a roadmap clearly identifying the mathematical problems that must be solved to realize a tractable solution and application in the future

Approaches that build incrementally upon existing frameworks or seek to solve existing problem formulations are explicitly out of scope.

Key Definitions

Mathematical framework: coherent system of assumptions, definitions, methods, and rules that provides a structured foundation for the formulation, rigorous analysis, and solution of problems.

Problem formulation: process of formalizing a real-world problem into a mathematical framework, which includes defining assumptions, constraints, parameters, relationships, and variables.

COMPASS: Successful submissions

A successful abstract will include:

High-risk Ideas
Approaches that build incrementally upon existing frameworks or solve existing problems are explicitly out of scope

Substantial Technical Argument
Clearly demonstrate the novelty of the approach detailing how it could:

- Offer breakthrough potential to advance current state-of-the-art methods
- Or enable entirely new capabilities or areas of application

Comprehensive Literature Review
Conduct a thorough review of existing mathematical frameworks and problem formulations relevant to the intended Defense application identifying:

- Gaps, limitations, or overlooked areas in current approaches
- Specific opportunities where the new framework could make a substantial impact

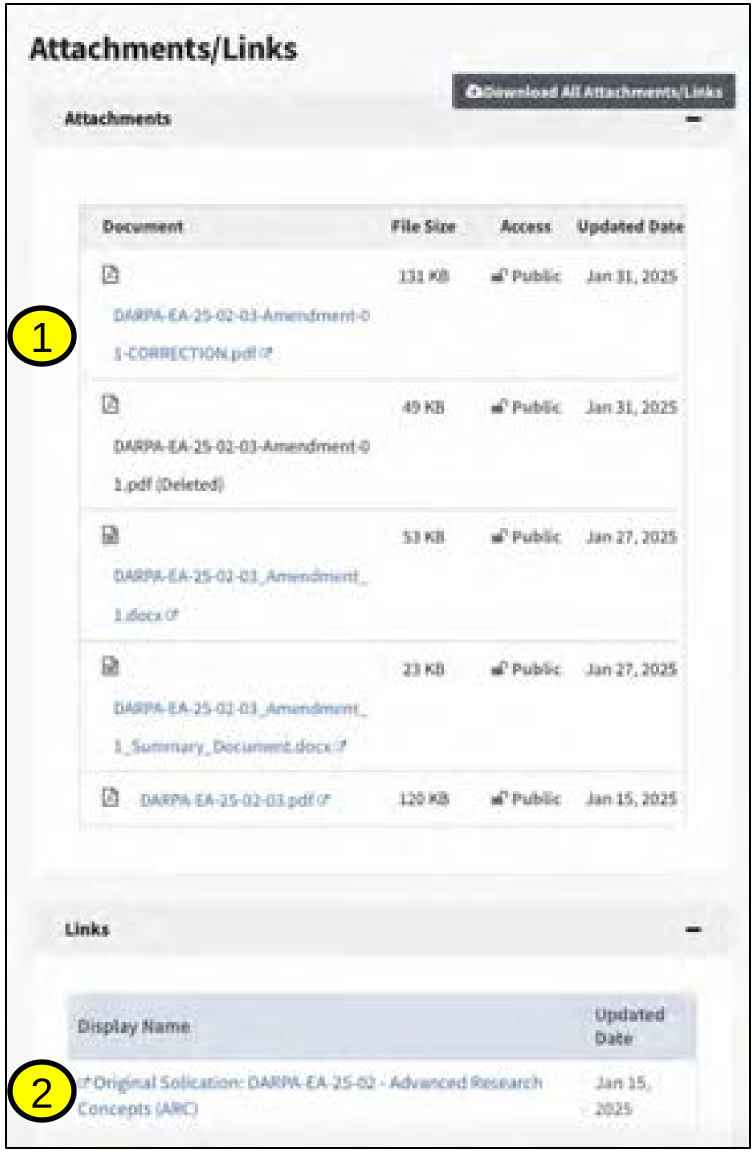
Evaluation Criteria
Provide detailed criterion to evaluate the effectiveness of the proposed approach against existing methods

Submitters with or without prior DoD-related research experience are highly encouraged to apply

We are looking for the most bold and audacious ideas!

Visit SAM.GOV for full submission details

https://www.darpa.mil/research/opportunities/arc > COMPASS > Button "Program Solicitation" > Redirected to SAM.GOV



Read TWO documents for full details.

1 DARPA-EA-25-02-03 (COMPASS)

- Provides COMPASS specific submission requirements

2 DARPA-EA-25-02 (The Overarching Solicitation)

- Describes the proposal process
  - Abstract Submission
  - Oral Proposal Package
- Provides Award information for negotiation-free Research Other Transaction (OT)
- Establishes Eligibility criteria

Submit Early! Solicitation Closes: May 12th 2025

- Abstracts evaluated on a rolling basis.
- Opportunity to address deficiencies and resubmit their revised abstract for consideration.
- Email questions to: COMPASS@darpa.mil

A primer for DoD challenges

- Guest Speakers for the workshop are organized in three DoD Challenge Areas.
- COMPASS explores a wide range of mathematical frameworks and domain applications areas.

DoD Challenge Area # 1 – Decisions Under Uncertainty
Dr. Tim McDonald, RAND Associate Policy Researcher *Structuring Analysis for Complex National Security Challenges*
Dr. Jorge Poveda, University of San Diego, Electrical and Computer Engineering *Stochastic deception in non-cooperative games*

DoD Challenge Area # 2 – Critical Infrastructure
Dr. David Alderson, Naval Postgraduate School, Center for Infrastructure Defense *Resilience in infrastructure systems*
Dr. Filippo Radicchi, Indiana University Bloomington, Luddy School of Informatics, Computing, and Engineering *Assessing the robustness of critical infrastructures via network percolation*

DoD Challenge Area # 3 – Contested Logistics
Mr. Jon Jeckell, U.S. Army, Contested Logistics Cross Functional Team *Decision support for logistics networks*
Dr. David Dewhurst, DARPA Program Manager *Establishing resilient supply chains*

- Proposers are not limited to the areas mentioned at the workshop.
- All abstracts require rigorous justification of a connection between a mathematical framework and application area.

www.darpa.mil

Structuring Analysis for Complex National Security Challenges

Approaches and Opportunities

Tim McDonald, RAND

Presentation to DARPA COMPASS Workshop

March 5, 2025

Background

Education

PhD, Policy Analysis

MPP, Business and Government

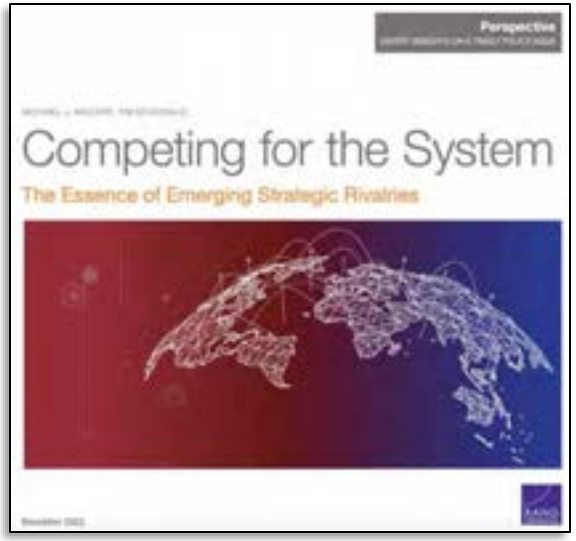
BA, Political Science

Background

Systems Analysis
Leadership & Negotiation
Deep Uncertainty

Nat Sec and Competitiveness

Social Policy



Informing National Security Decisions in Complex Settings and Under High Uncertainty

Examples: Biosecurity; AI development and governance; nuclear proliferation; shifting global order; climate change and its effects; political extremism; economic espionage

National security and public policy challenges are functions of complex adaptive systems (CAS).

CAS | Many interconnected components; agents; emergent behaviors; adaptation; nonlinearity; self-organization; heterogeneity; feedback; openness and nested systems; dynamics; evolution…

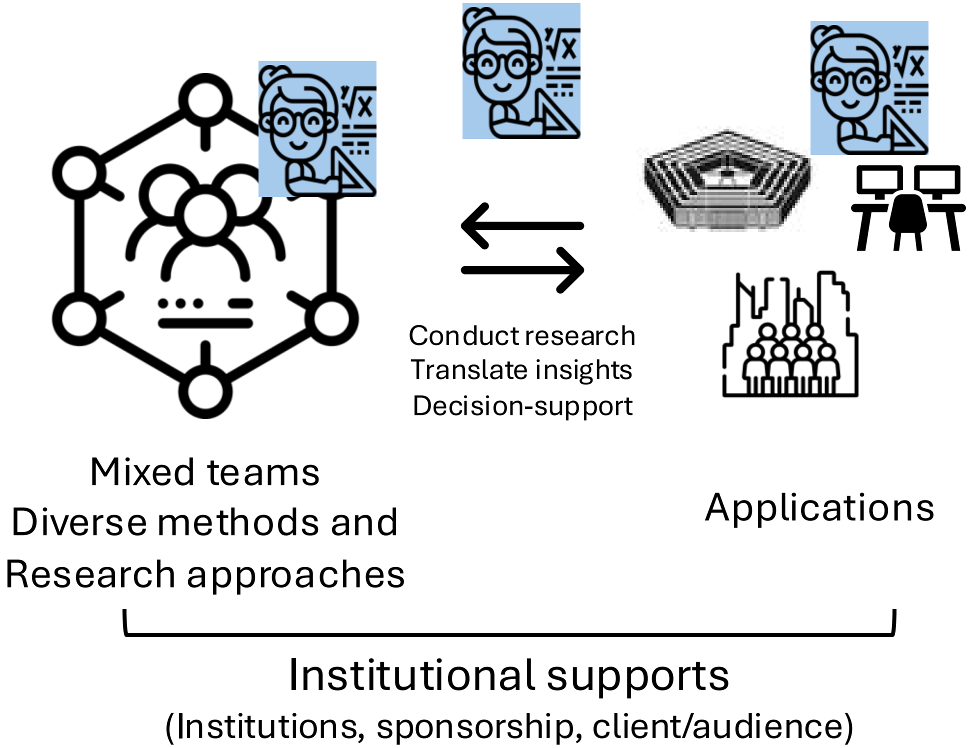
The problems have “wicked” characteristics.

Wicked | Disagreement on goals and problem definition; no clear end point; multi-causal; resist single-factor interventions; not “solvable”; effectiveness is subjective; highly uncertain; often high stakes…

“Where do I fit?”

- Mathematician

The Scientific Challenge: **How to conduct rigorous analysis to inform complex policy and defense problems?**



"The task for analysis is not to say, 'I'm an [insert discipline], let me shape the problem to fit my tools,' but to say, 'here is the problem. Let's bring to bear all relevant tools from all relevant disciplines."

- Alain Enthoven

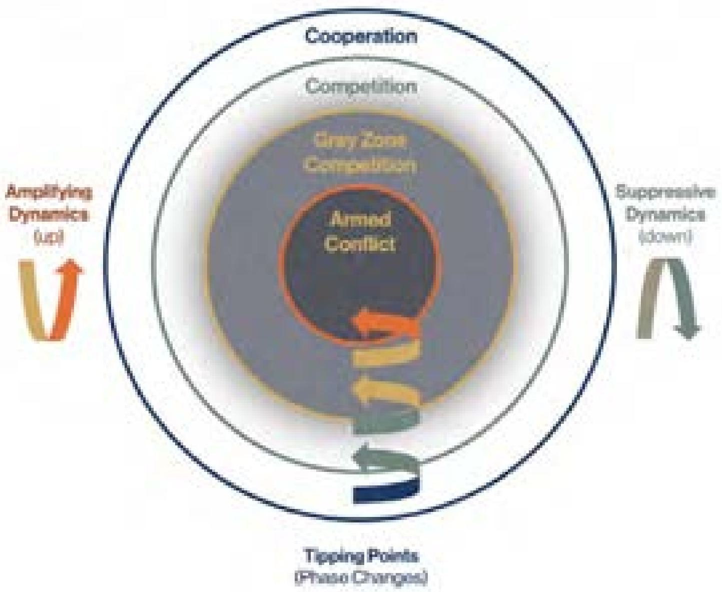
- Policy/defense problems have special characteristics vs. social science (via CIA): time constraints; unable to control variables; unknown data quality; emphasis on prediction; focus on utility…
- Science as structured approach with theory, hypotheses, use of reason and evidence; stating assumptions and seeking alternative explanations.
- Mixed teams and diverse methods, fitting approach to problem, connecting analysis to applications with decision-makers and institutional support.
- Analysis campaigns working at multiple levels and asking multiple kinds of questions; iterative research.

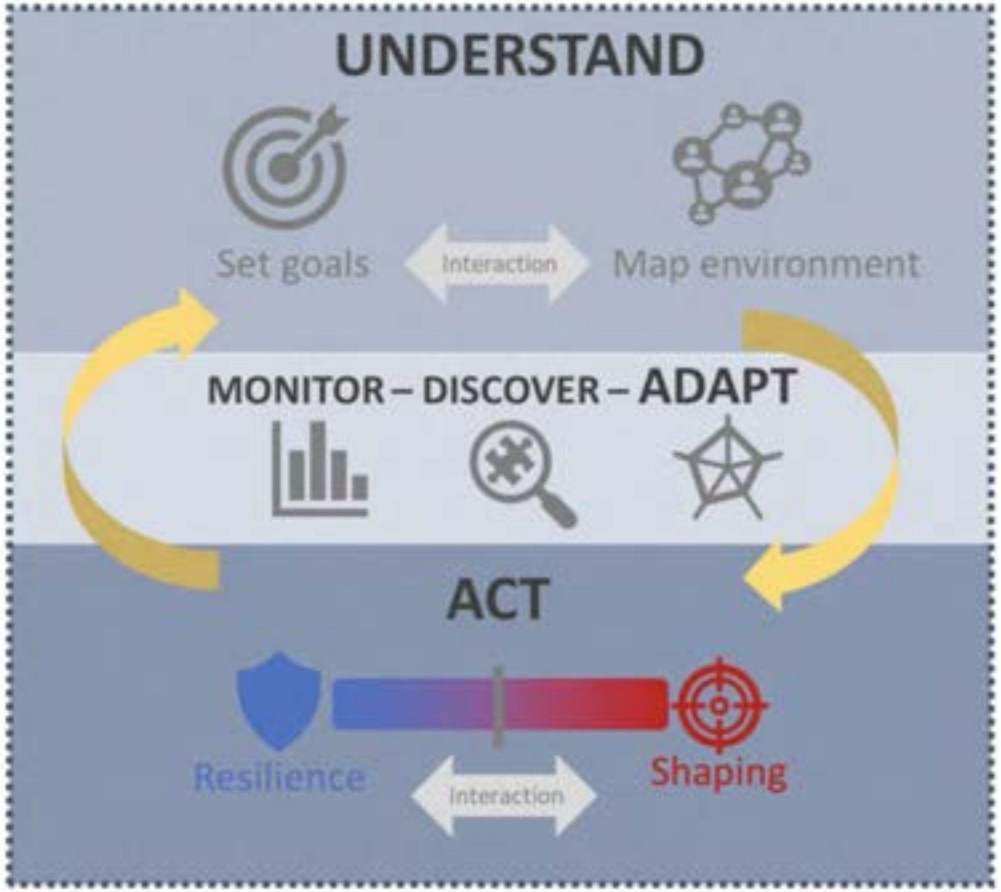
Table 1: Principles of Military Operational Planning vs. Grey Zone Competition[19]

Source: *Monaghan McDonald 2023*

Military Operational Planning (above the threshold of war)	Grey Zone Competition (below the threshold of war)
Complicated	Complex
Closed system	Open system
Cause-and-effect	Multi-causal
Determinate	Indeterminate
Linear	Non-linear
Additive	Emergent
Risk	Uncertainty

Figure 1. Grey Zone Competition within International Relations

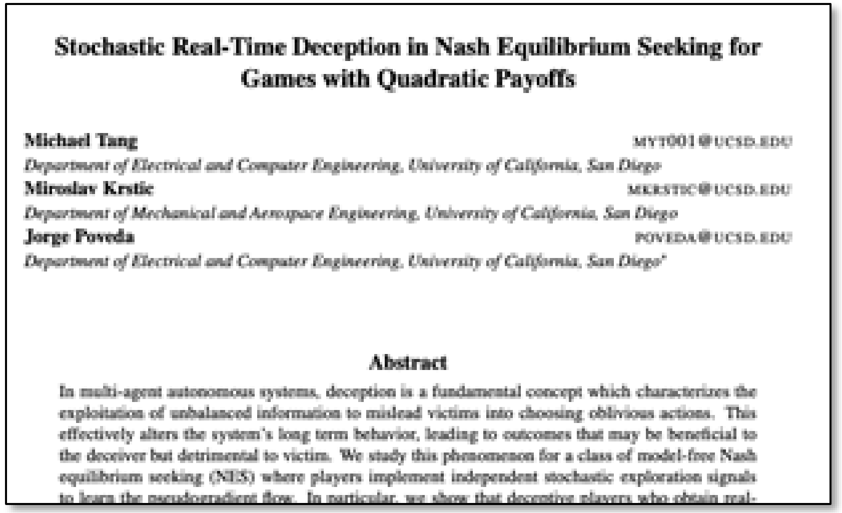




Scenario: Information Operations in Grey Zone

Tang, Krstic, Poveda (2025): Imbalance of information can be exploited to steer adversary in your desired direction.

- Multiple autonomous agents operating within a structure
- Probe counterparts; incorporate responses into actions
- Alters long-term behavior (dynamics) of system
- Deceptive players can use insight to shift behaviors


Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs

Michael Tang MYT001@UCSD.EDU
Department of Electrical and Computer Engineering, University of California, San Diego
Miroslav Krstic MKRSTIC@UCSD.EDU
Department of Mechanical and Aerospace Engineering, University of California, San Diego
Jorge Poveda POVEDA@UCSD.EDU
Department of Electrical and Computer Engineering, University of California, San Diego

Abstract

In multi-agent autonomous systems, deception is a fundamental concept which characterizes the exploitation of unbalanced information to mislead victims into choosing oblivious actions. This effectively alters the system's long term behavior, leading to outcomes that may be beneficial to the deceiver but detrimental to victim. We study this phenomenon for a class of model-free Nash equilibrium seeking (NES) where players implement independent stochastic exploration signals to learn the pseudogradient flow. In particular, we show that deceptive players who obtain real-

Linking mathematical formulation with strategic decision-making:

More strategic

More tactical

Macro	What are implications for shaping the architecture of international system of alliances? in areas like technology, climate change, or nuclear proliferation?
Meso	How can insights be operationalized in grey zone campaigns of information operations? What are potential roles for AI?
Micro	How can deception be used to exploit information asymmetries to influence perceptions and actions of counterparts or adversaries?

Possible Research Directions

Some thoughts on research questions on information operations in grey zone:

Optimizing information dissemination

How can AI models effectively deploy or counter disinformation?

Networked influence operations

How to identify and neutralize malicious influence networks in social media?

Game theory for cyber and info ops

How to predict, counter, influence adversaries using information?

Modeling cascading effects

What frameworks could model and predict spread of disinformation across platforms, and/or reaching phase changes or tipping points?

Detecting anomalies in communications

What statistical methods could improve identifying communication patterns indicative of covert information ops?

Understanding the new power

How to define and measure power in social relationships?

Simulating complex information environments

What simulation techniques can model interaction of actors in complex info environments?

And more…

Discussion

Contact

tmcdonald@rand.org

RAND

Stochastic Deception in Noncooperative Games

Jorge I. Poveda

Department of Electrical and Computer Engineering

UC San Diego

Motivation: Real-Time Decision-Making in Contested Environments

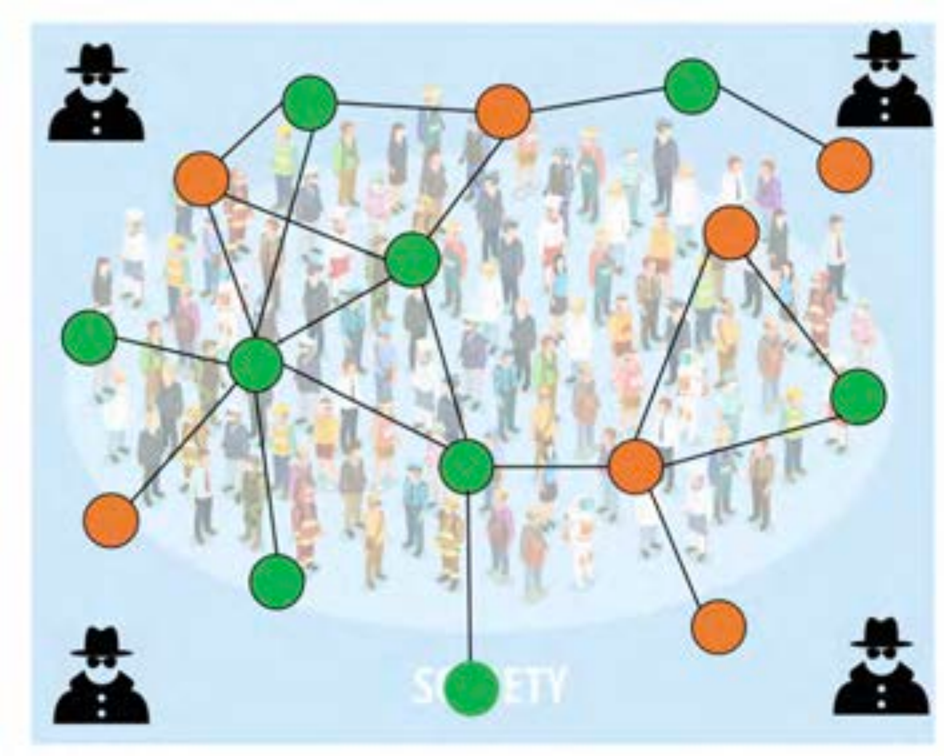
- Strategic decision-making in complex and uncertain multi-agent systems

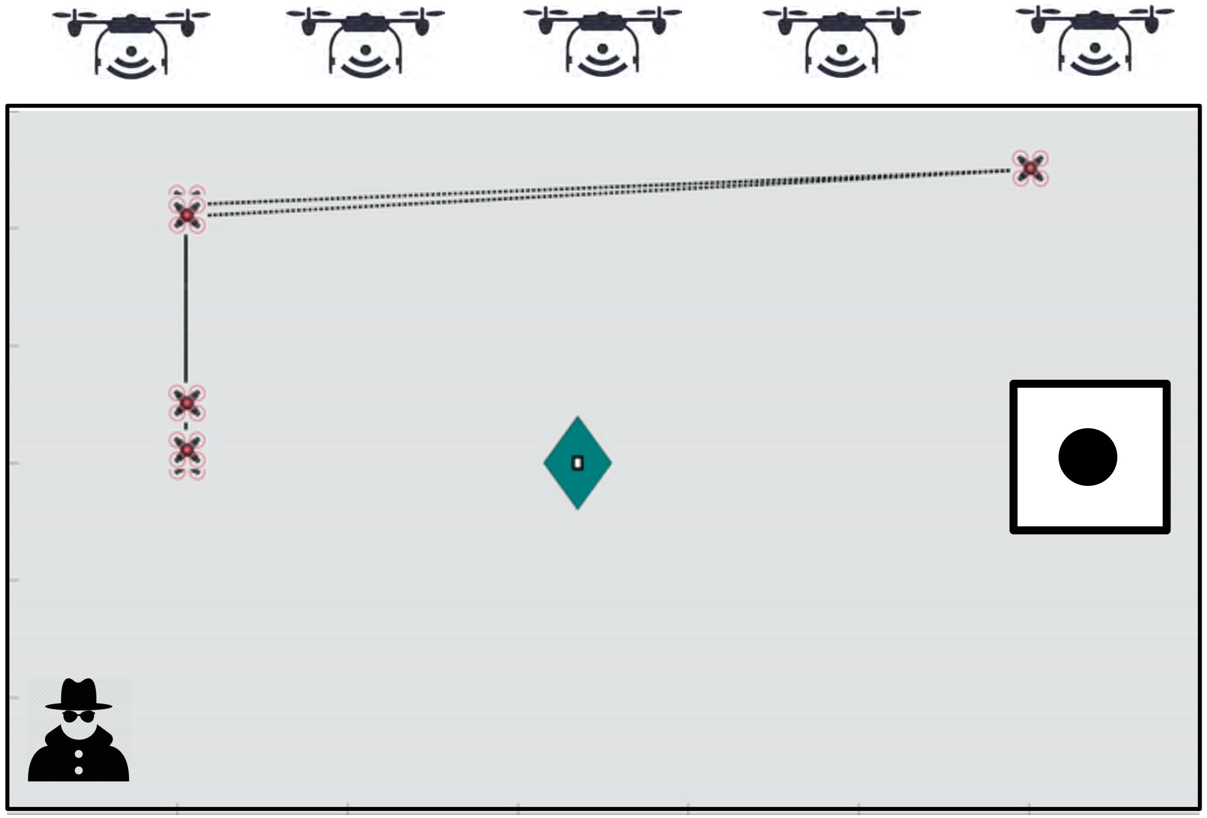
Motivation: Real-Time Decision-Making in Contested Environments

- Strategic decision-making in complex and uncertain multi-agent systems
- Example: Optimal deployment and allocation of resources

Motivation: Real-Time Decision-Making in Contested Environments

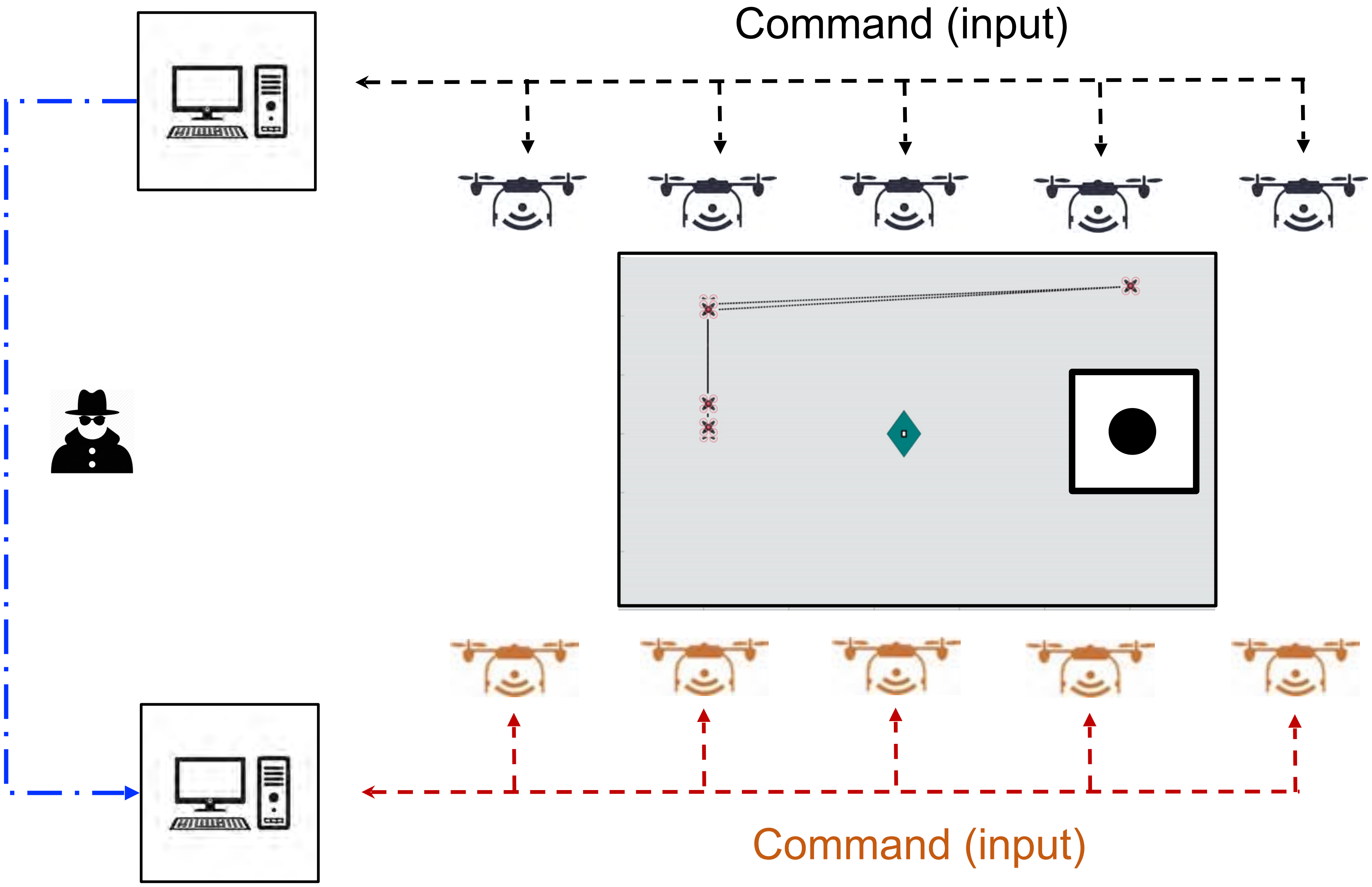
- Strategic decision-making in complex and uncertain multi-agent systems
- Example: Optimal deployment and allocation of resources



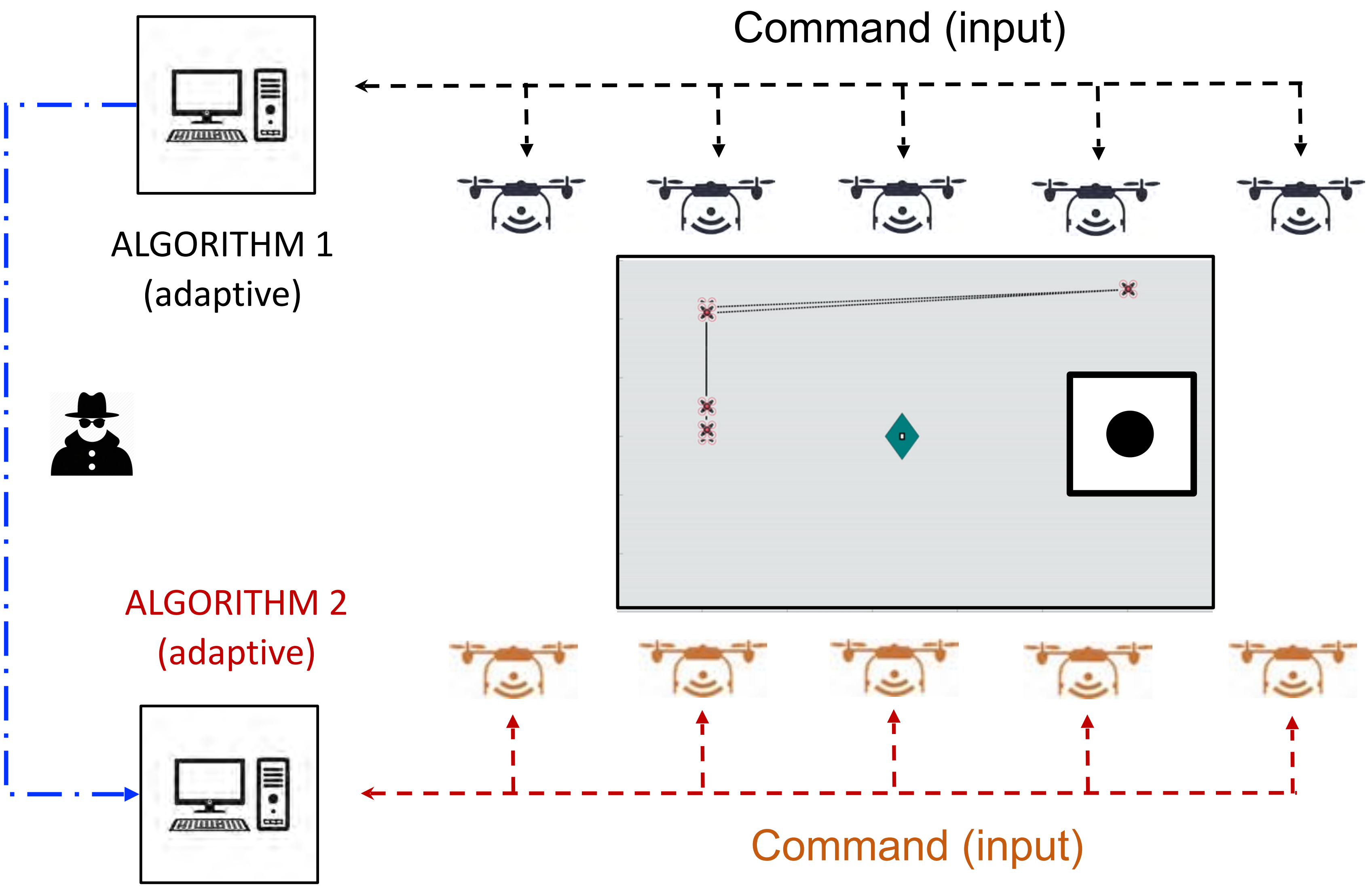


Motivation: Real-Time Decision-Making in Contested Environments

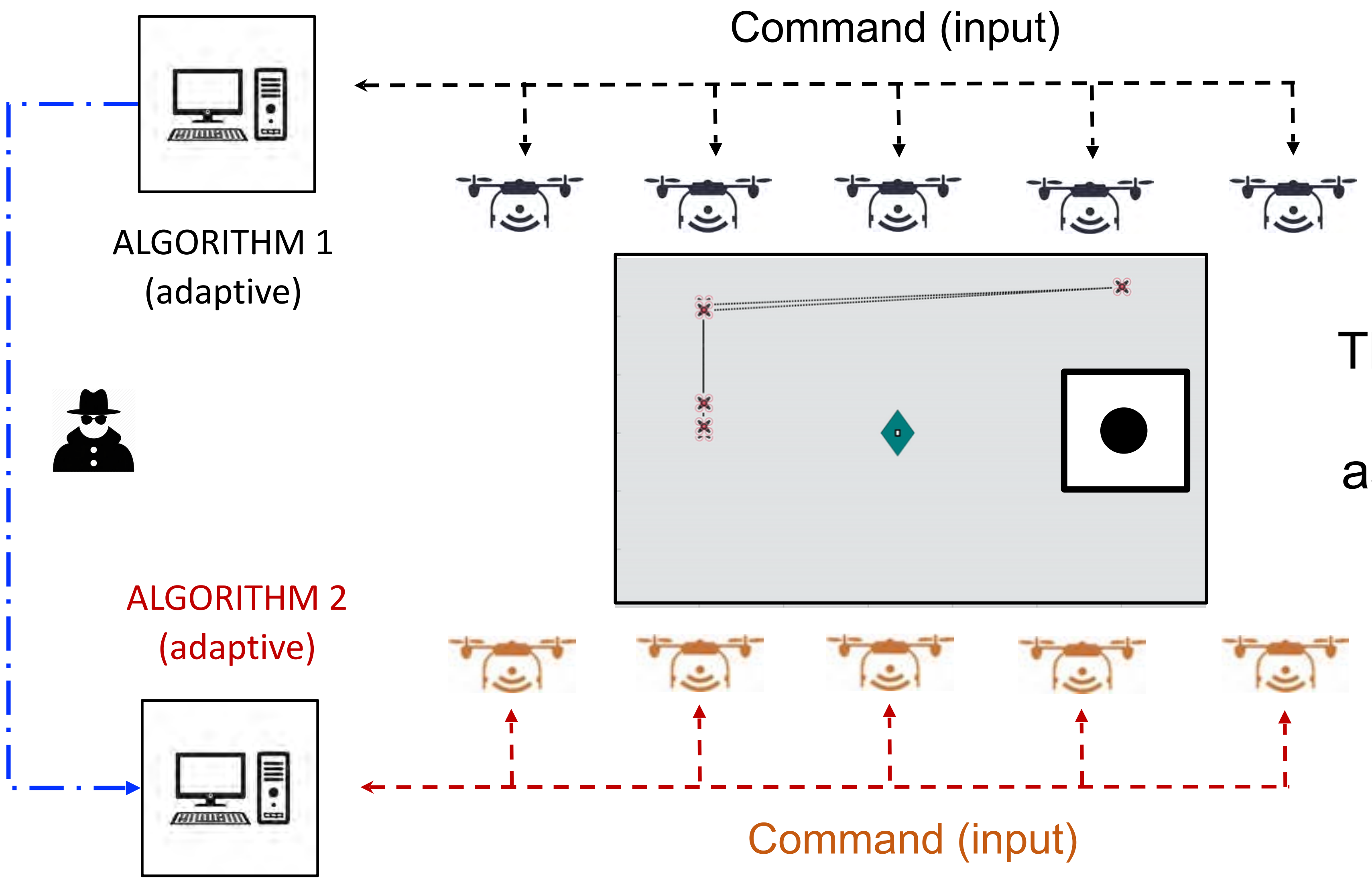
Motivation: Real-Time Decision-Making in Contested Environments



Motivation: Real-Time Decision-Making in Contested Environments



Motivation: Real-Time Decision-Making in Contested Environments



The role of asymmetric information in the asymptotic behavior of the system

Motivation: Real-Time Decision-Making in Contested Environments

Goal: Characterize fundamental limitations and advantages of AI-enabled systems in contested environments

Motivation: Real-Time Decision-Making in Contested Environments

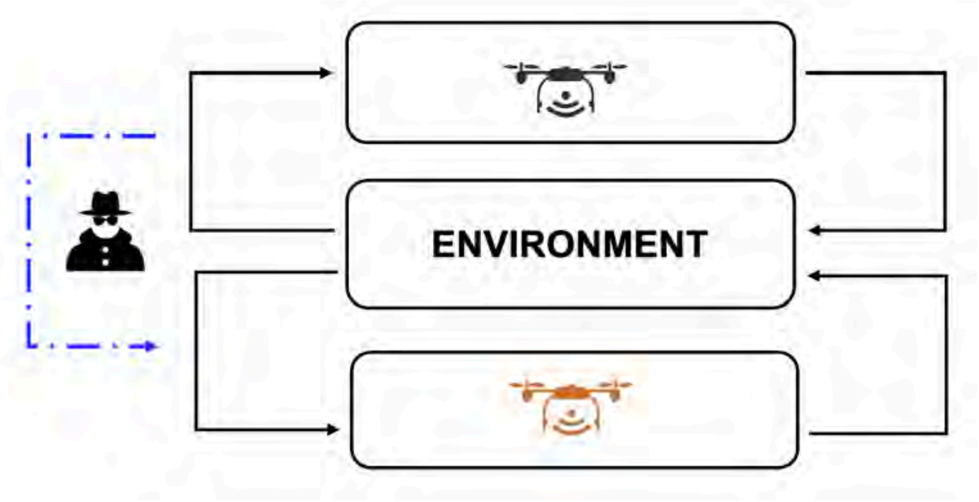
Goal: Characterize fundamental limitations and advantages of AI-enabled systems in contested environments

- We understand AI-enabled systems as **machines or algorithms** that autonomously adapt to the environment in real-time to achieve a desired goal

Motivation: Real-Time Decision-Making in Contested Environments

Goal: Characterize fundamental limitations and advantages of AI-enabled systems in contested environments

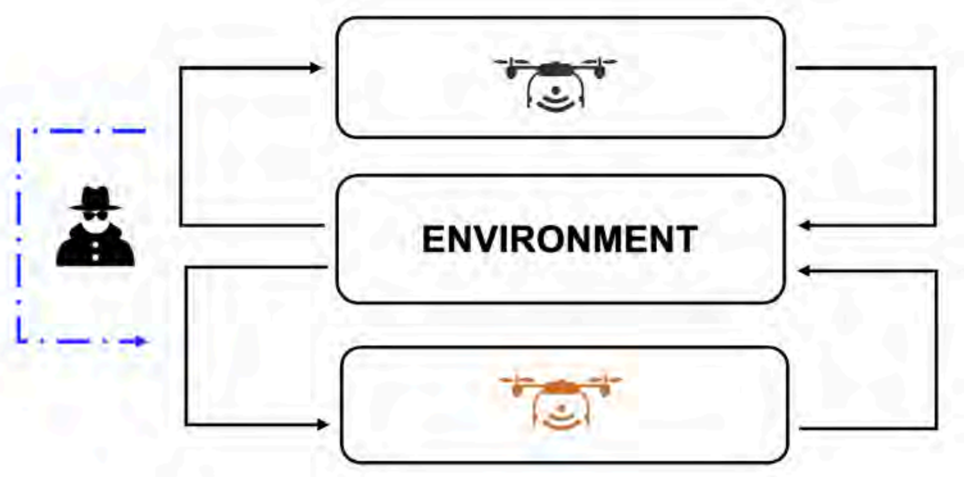
- We understand AI-enabled systems as **machines or algorithms** that autonomously adapt to the environment in real-time to achieve a desired goal



Motivation: Real-Time Decision-Making in Contested Environments

Goal: Characterize fundamental limitations and advantages of AI-enabled systems in contested environments

- We understand AI-enabled systems as **machines or algorithms** that autonomously adapt to the environment in real-time to achieve a desired goal

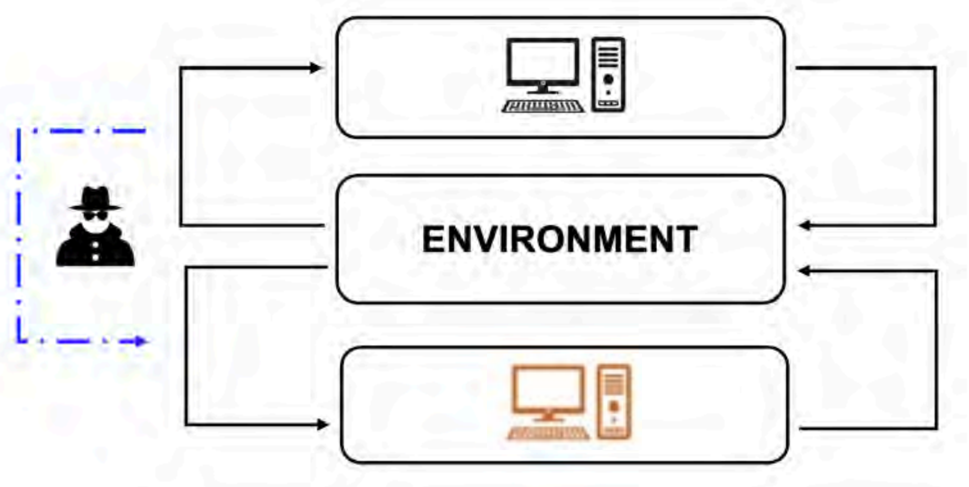


- We understand contested environments as situations where agents have conflictive interests

Motivation: Real-Time Decision-Making in Contested Environments

Goal: Characterize fundamental limitations and advantages of AI-enabled systems in contested environments

- We understand AI-enabled systems as **machines or algorithms** that autonomously adapt to the environment in real-time to achieve a desired goal



- We understand contested environments as situations where agents have conflictive interests.

Game Theory: Noncooperative Games

Agents (or teams) can be seen as non-cooperative players seeking to optimize their **own** cost function

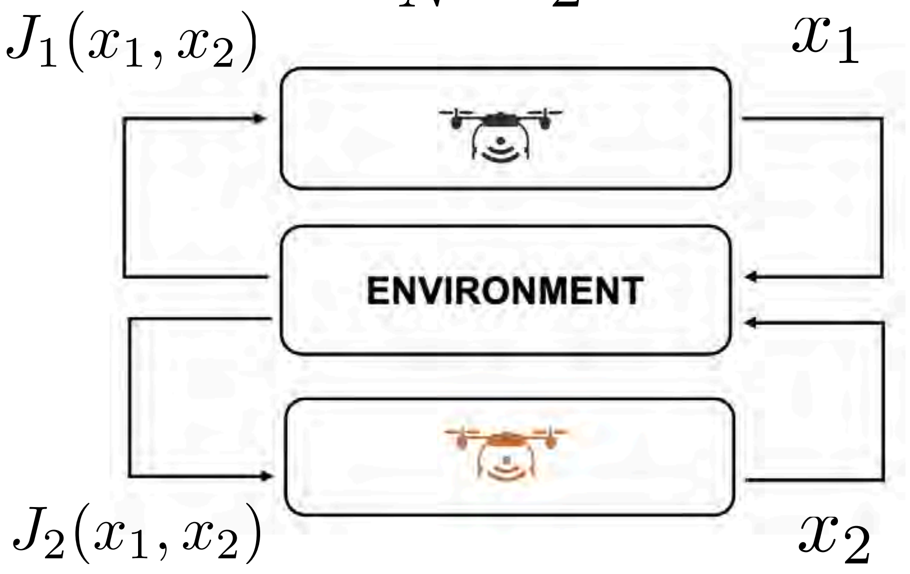
Game Theory: Noncooperative Games

Agents (or teams) can be seen as non-cooperative players seeking to optimize their **own** cost function

Key ingredients in a non-cooperative game:

- Number of Players: $\mathcal{V} = \{1, 2, 3, \ldots, N\}$
- Possible Actions: $x_i \quad i \in \mathcal{V}$
- Cost Functions: $J_i(x_1, x_2, \ldots, x_N) \quad i \in \mathcal{V}$

$N = 2$



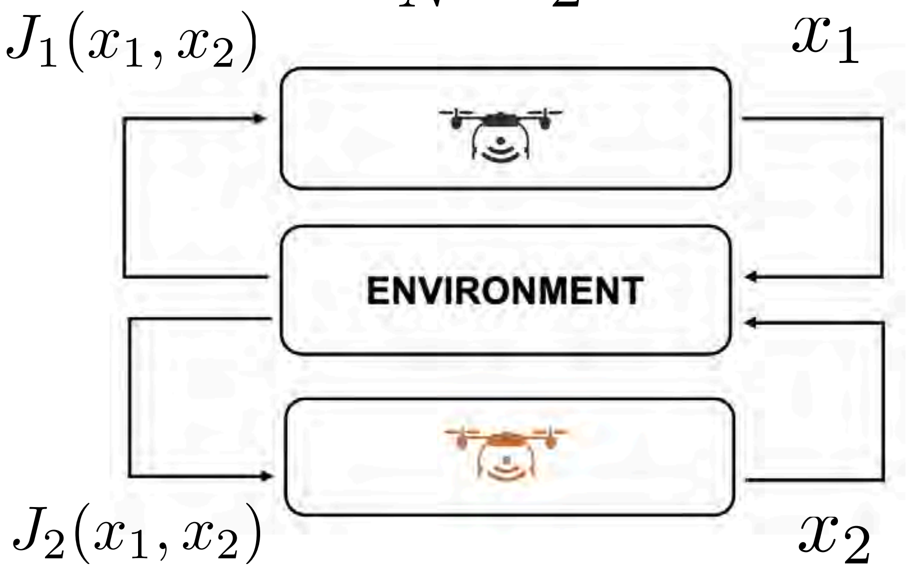
Game Theory: Noncooperative Games

Agents (or teams) can be seen as non-cooperative players seeking to optimize their **own** cost function

Key ingredients in a non-cooperative game:

- Number of Players: $\mathcal{V} = \{1, 2, 3, \ldots, N\}$
- Possible Actions: $x_i \quad i \in \mathcal{V}$
- Cost Functions: $J_i(x_1, x_2, \ldots, x_N) \quad i \in \mathcal{V}$

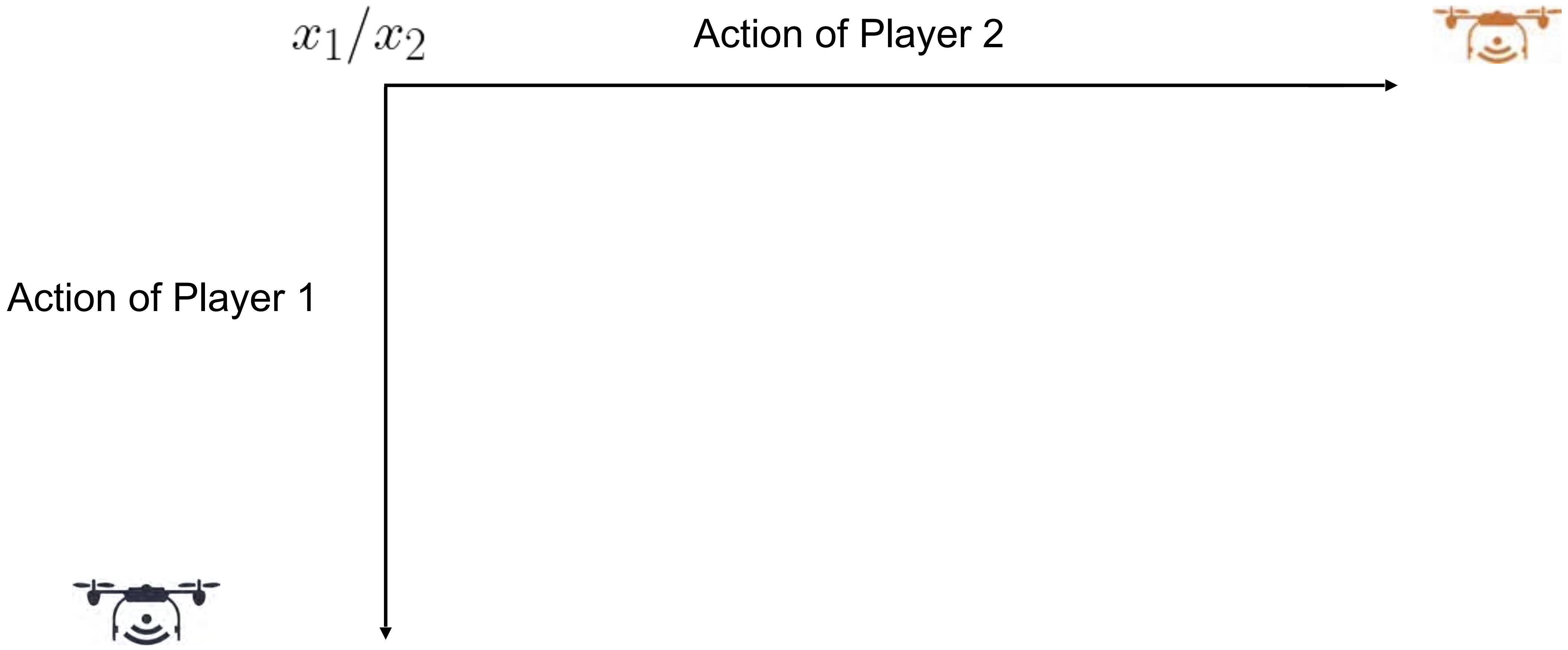
$N = 2$



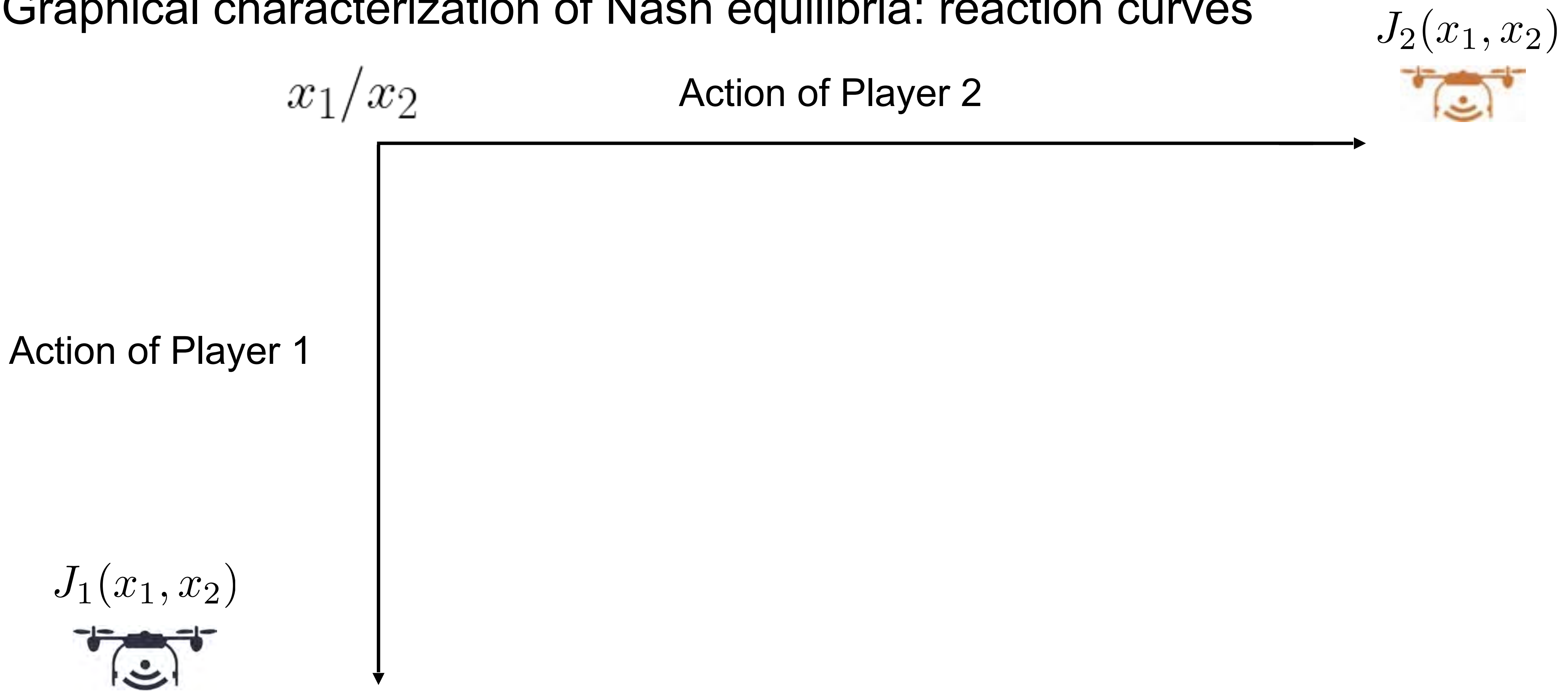
If agents reach a point (x_1^*, x_2^*) where they have no incentive to deviate, said point is called a Nash equilibrium

Game Theory: Noncooperative Games

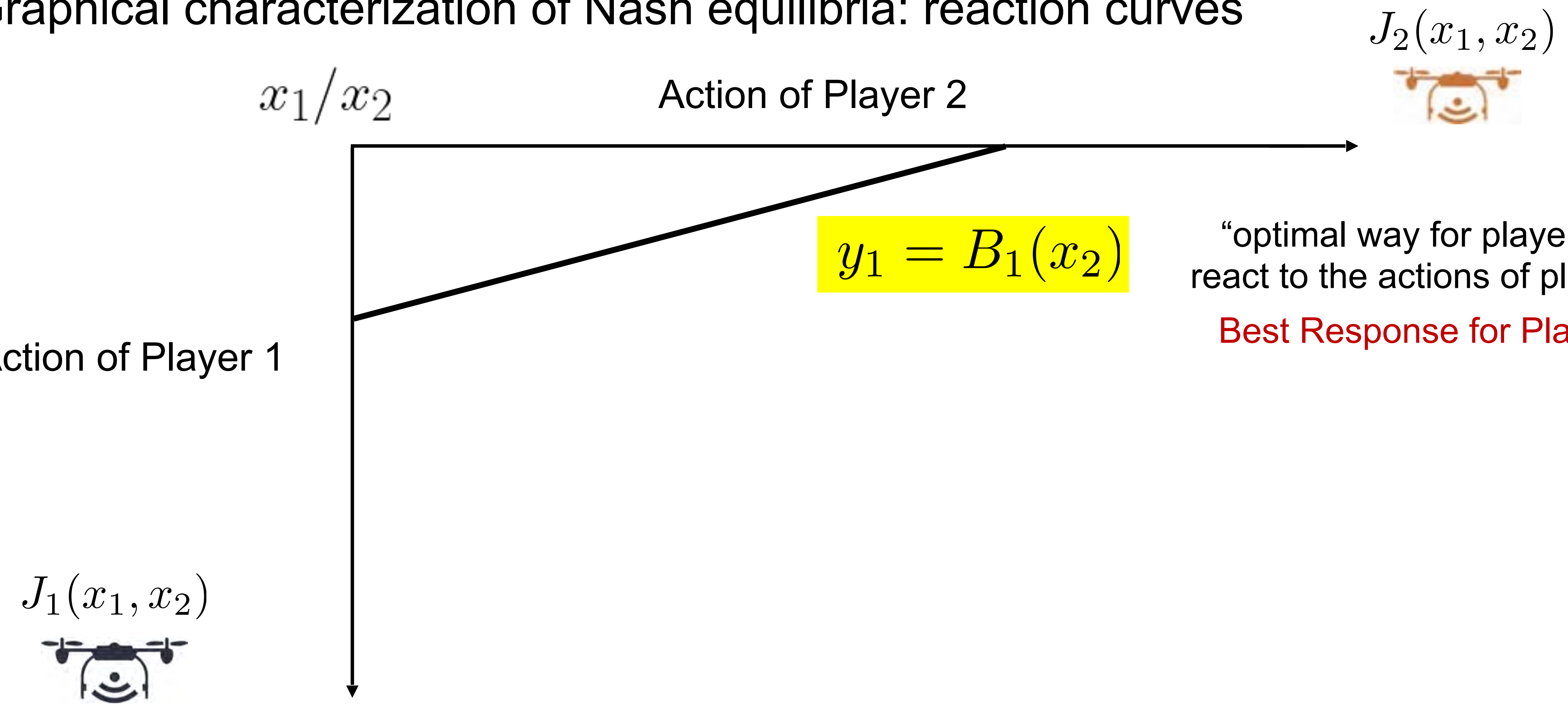
Graphical characterization of Nash equilibria: reaction curves



Graphical characterization of Nash equilibria: reaction curves



Graphical characterization of Nash equilibria: reaction curves



"optimal way for player 1 to react to the actions of player 2"

Best Response for Player 1

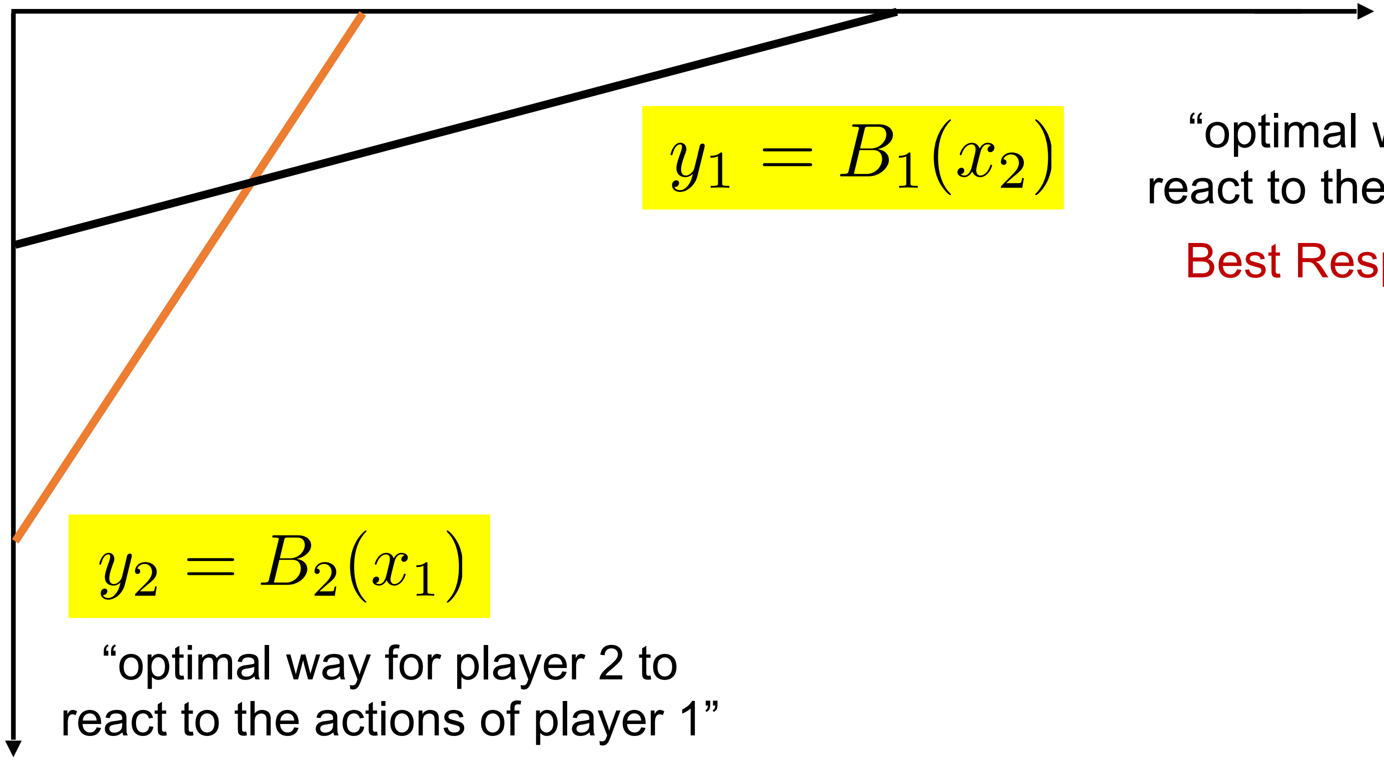
Game Theory: Noncooperative Games

Graphical characterization of Nash equilibria: reaction curves

$J_2(x_1, x_2)$

x_1/x_2

Action of Player 2



$y_1 = B_1(x_2)$

"optimal way for player 1 to react to the actions of player 2"

Best Response for Player 1

Action of Player 1

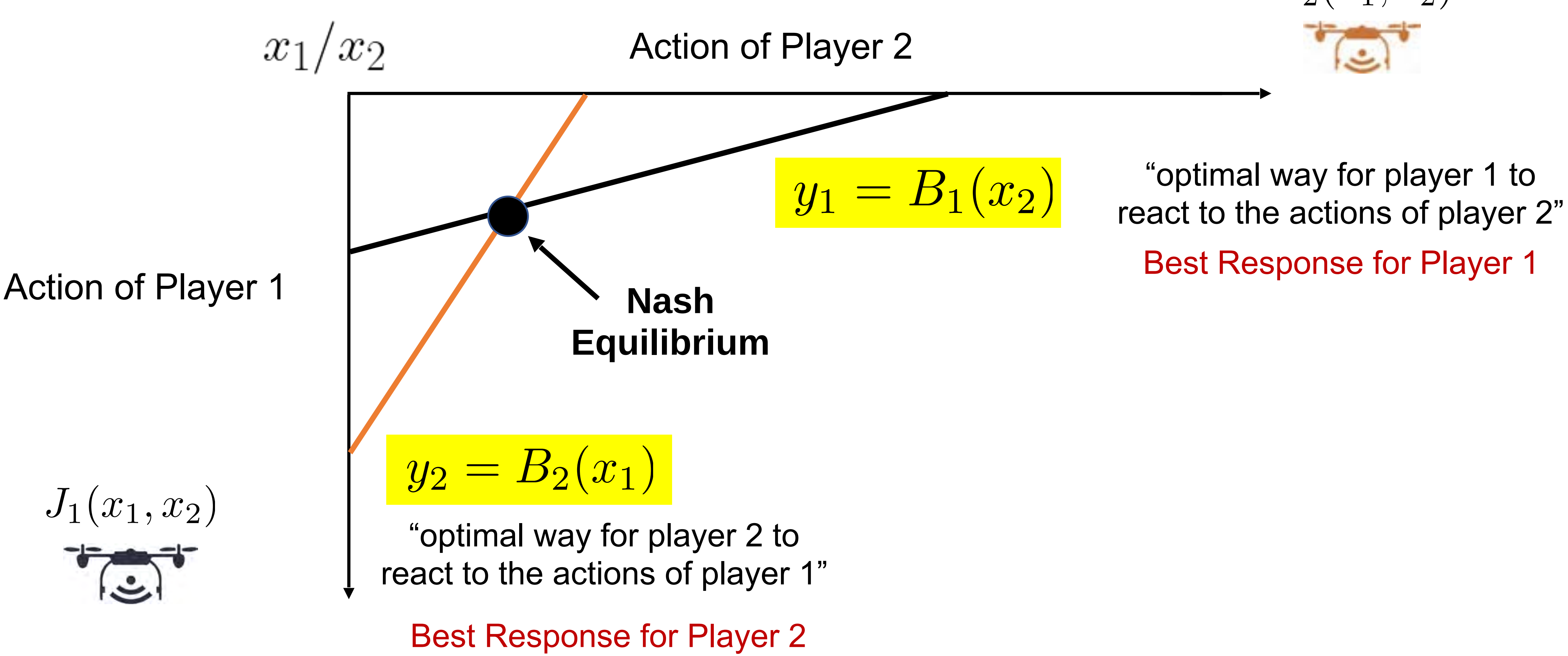
$y_2 = B_2(x_1)$

$J_1(x_1, x_2)$

"optimal way for player 2 to react to the actions of player 1"

Best Response for Player 2

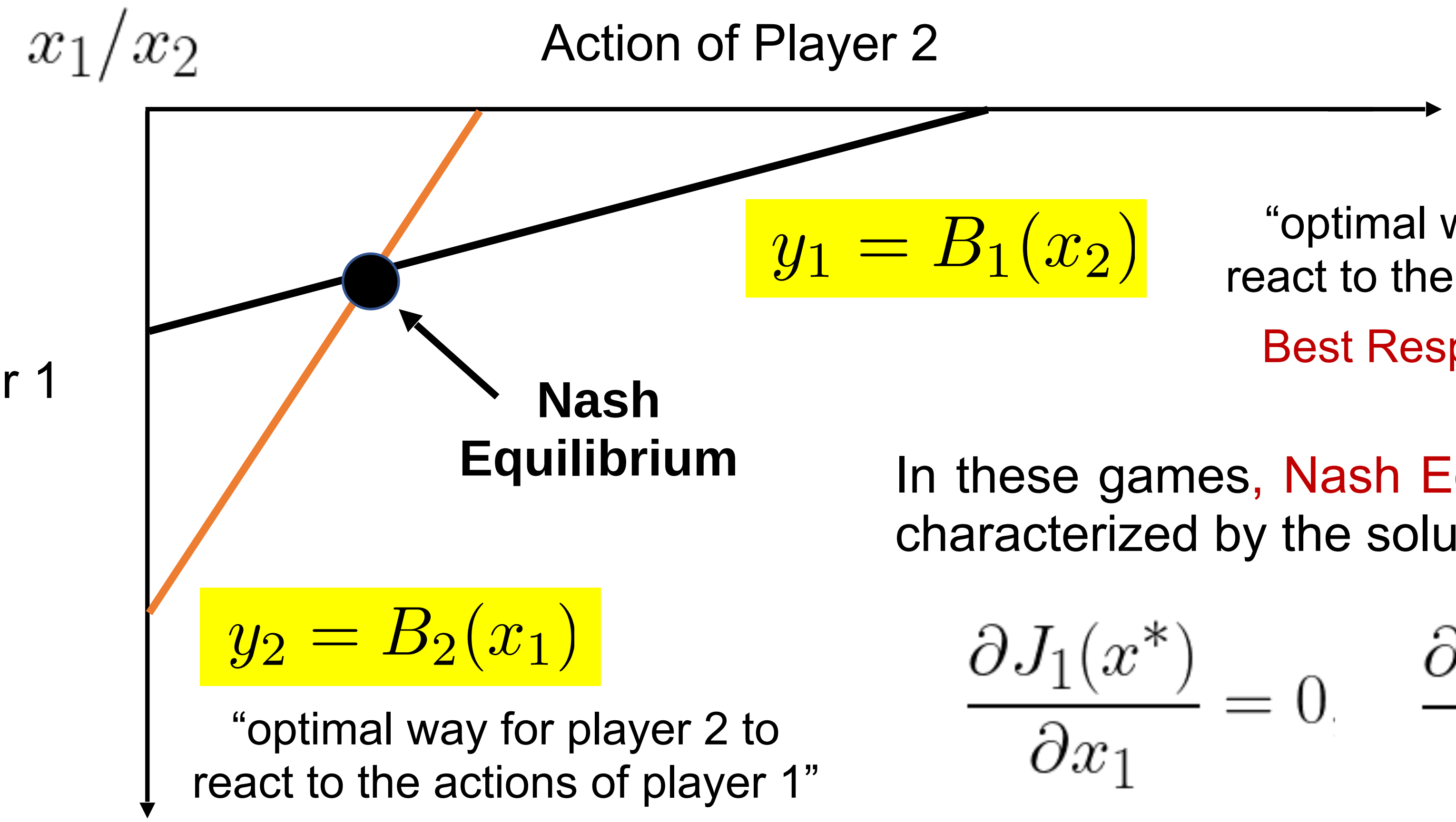
Graphical characterization of Nash equilibria: reaction curves



Game Theory: Noncooperative Games

Graphical characterization of Nash equilibria: reaction curves

$J_2(x_1, x_2)$



$y_1 = B_1(x_2)$

"optimal way for player 1 to react to the actions of player 2"

Best Response for Player 1

$y_2 = B_2(x_1)$

"optimal way for player 2 to react to the actions of player 1"

Best Response for Player 2

$J_1(x_1, x_2)$

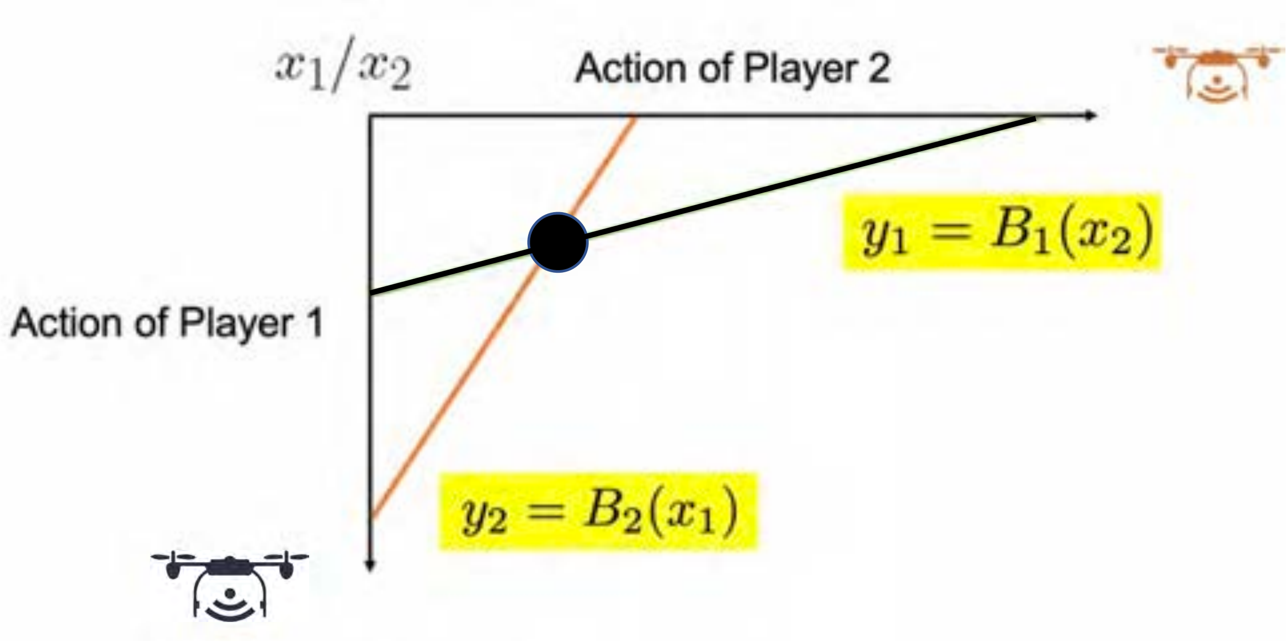
In these games, Nash Equilibria are characterized by the solution to:

$$\frac{\partial J_1(x^*)}{\partial x_1} = 0, \quad \frac{\partial J_2(x^*)}{\partial x_2} = 0$$

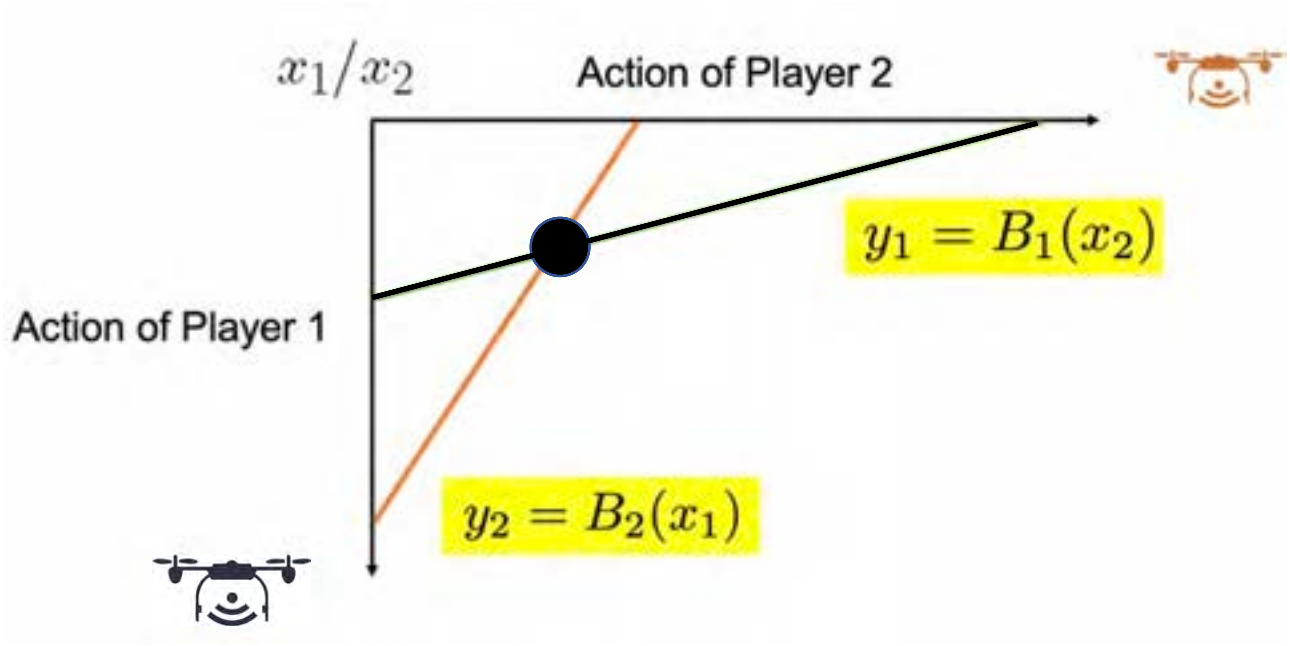
* plus some additional second-order conditions

Key principle: Many adaptive/intelligent algorithms aim to learn the best response of the agents (using past and real-time data)

Key principle: Many adaptive/intelligent algorithms aim to learn the best response of the agents (using past and real-time data)



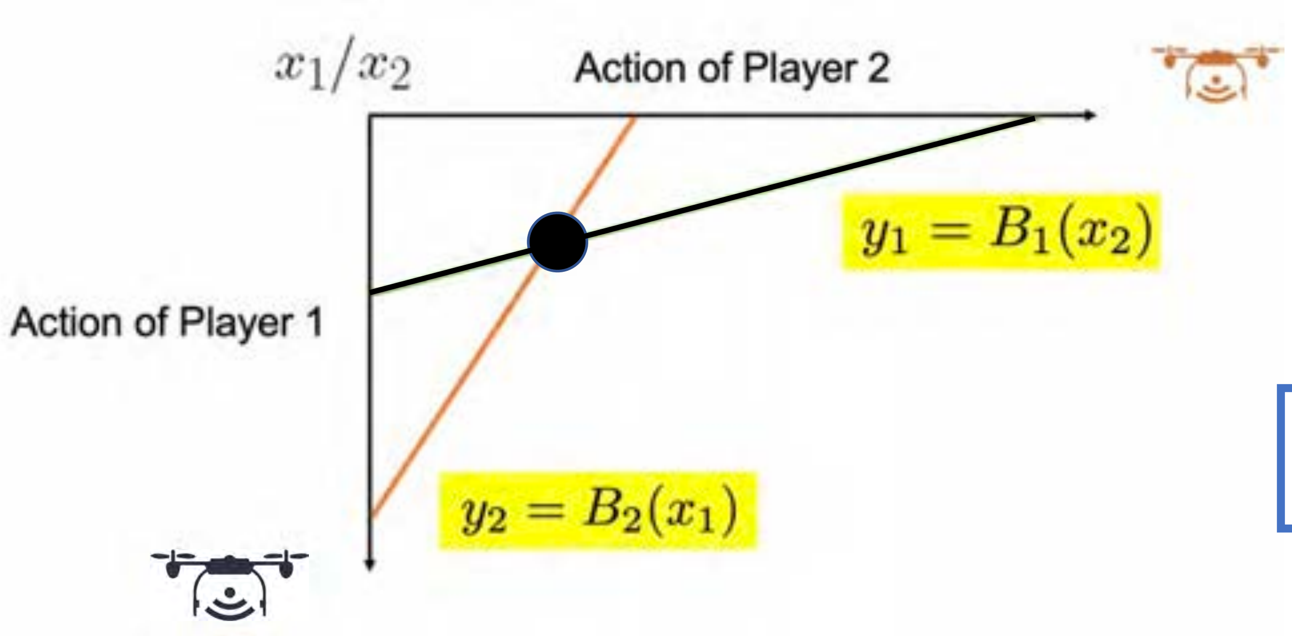
Key principle: Many adaptive/intelligent algorithms aim to learn the best response of the agents (using past and real-time data)



This is achieved via algorithms that integrate:

- ➢ Exploration policies
- ➢ Exploitation policies

Key principle: Many adaptive/intelligent algorithms aim to learn the best response of the agents (using past and real-time data)



This is achieved via algorithms that integrate:

- ➢ Exploration policies
- ➢ Exploitation policies

e.g., adaptive control, RL, zeroth-order optimization, approximation-based techniques, Nash-seeking dynamics, etc

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = u_i + a\sin(\omega_i t) \quad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = \underbrace{u_i + a\sin(\omega_i t)}_{\text{Exploration}} \qquad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

Nash Seeking Dynamics: A Deterministic Algorithm

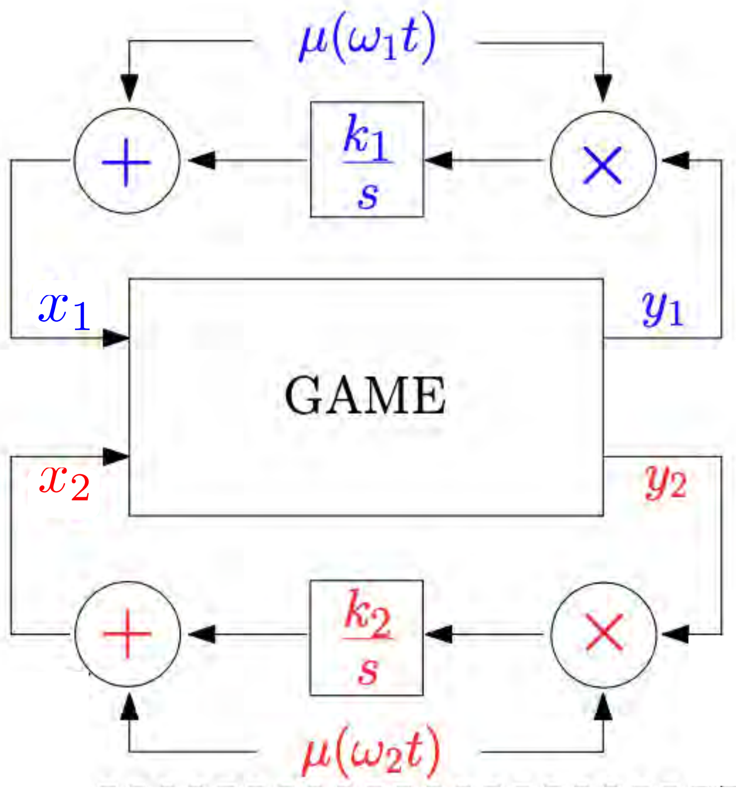
One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$\underbrace{x_i = u_i + a\sin(\omega_i t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_i = -\frac{2k}{a}J_i(x)\sin(\omega_i t)}_{\text{Exploitation}}$$

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = \underbrace{u_i + a\sin(\omega_i t)}_{\text{Exploration}} \qquad \dot{u}_i = \underbrace{-\frac{2k}{a} J_i(x)\sin(\omega_i t)}_{\text{Exploitation}}$$



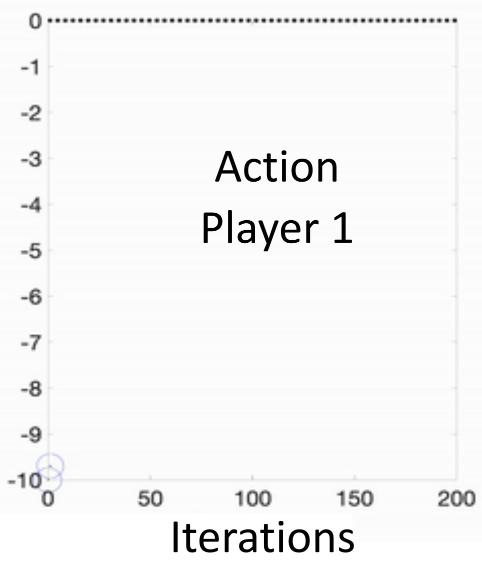
μ : sinusoidal probing signals

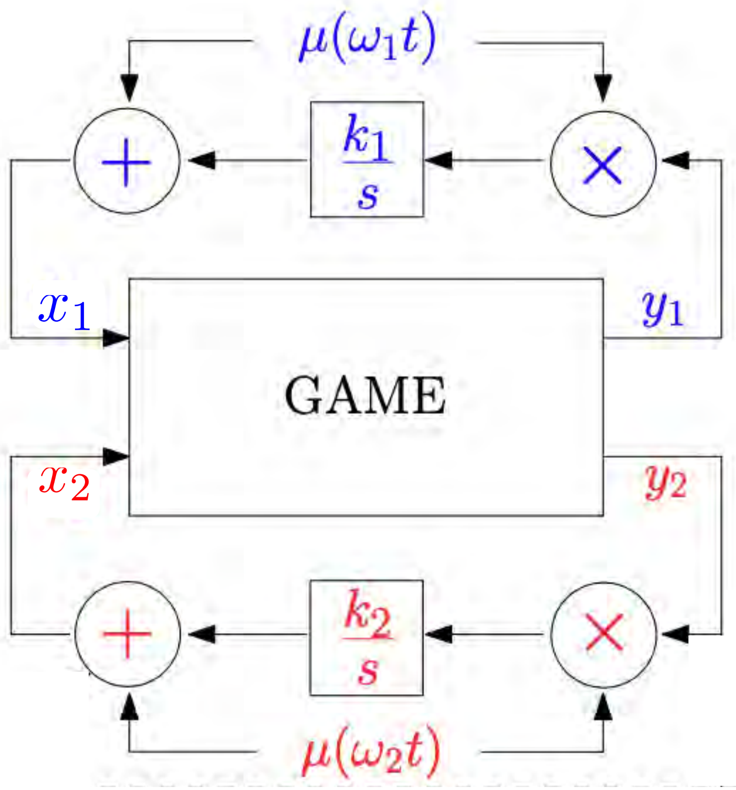
Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = u_i + a\sin(\omega_i t) \qquad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

Exploration (applies to $x_i = u_i + a\sin(\omega_i t)$) — Exploitation (applies to $\dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$)



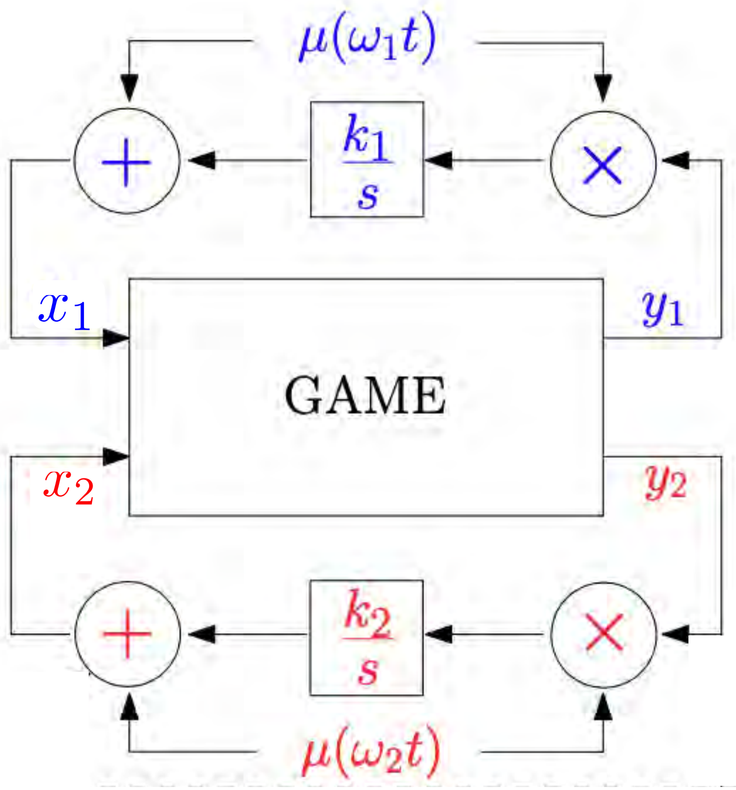


μ : sinusoidal probing signals

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = \underbrace{u_i + a\sin(\omega_i t)}_{\text{Exploration}} \qquad \dot{u}_i = \underbrace{-\frac{2k}{a} J_i(x)\sin(\omega_i t)}_{\text{Exploitation}}$$

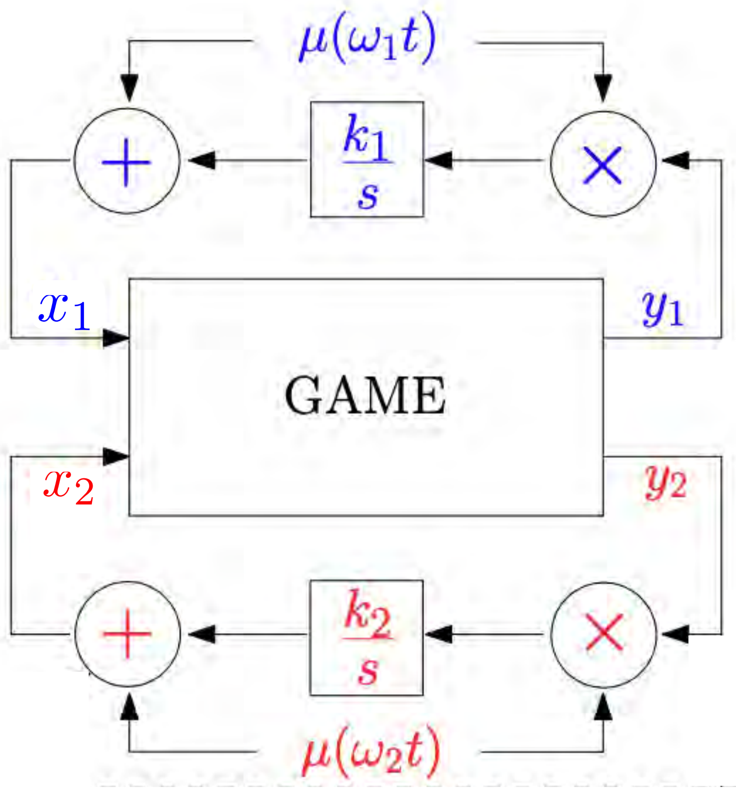


μ : sinusoidal probing signals

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = \underbrace{u_i + a\sin(\omega_i t)}_{\text{Exploration}} \qquad \dot{u}_i = \underbrace{-\frac{2k}{a} J_i(x)\sin(\omega_i t)}_{\text{Exploitation}}$$



μ : sinusoidal probing signals

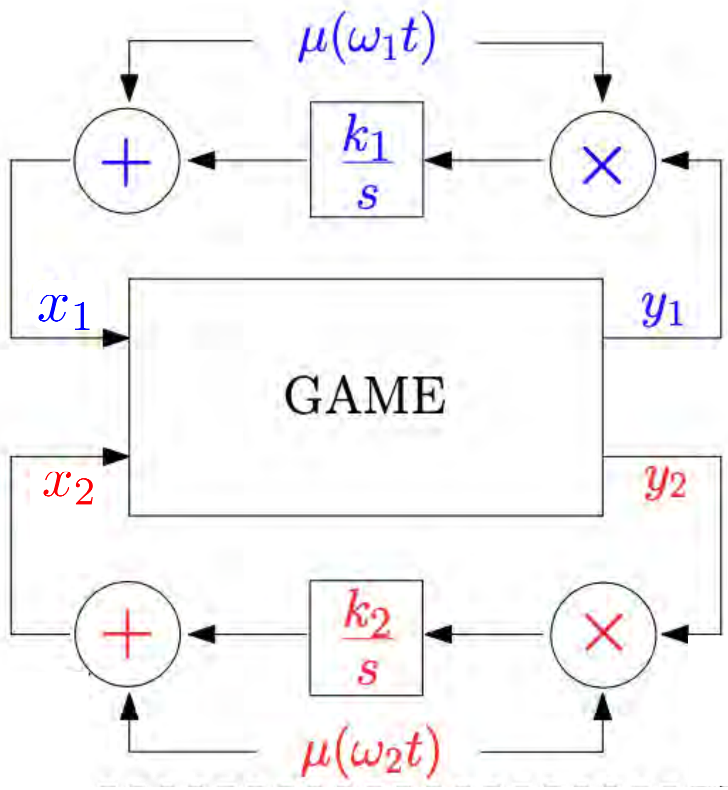
Frequencies of exploration need to be different between players!

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = u_i + a\sin(\omega_i t) \qquad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

Exploration Exploitation



μ : sinusoidal probing signals

Frequencies of exploration need to be different between players!

Nash Seeking Dynamics: A Deterministic Algorithm

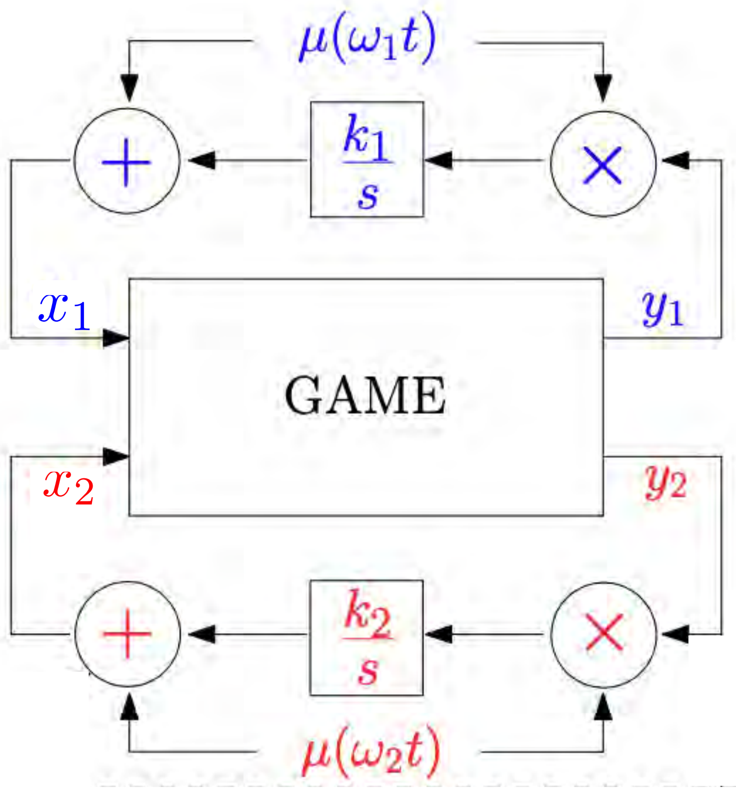
One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = u_i + a\sin(\omega_i t) \qquad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

Exploration — Exploitation

Stability and convergence guarantees are well-known for these methods:

$$|u(t) - u^*| \leq Me^{-mt}|u(0) - u^*| + \mathcal{O}\left(\frac{1}{\omega} + a\right)$$



μ : sinusoidal probing signals

Frequencies of exploration need to be different between players!

Nash Seeking Dynamics: A Deterministic Algorithm

One particular algorithm that achieves this task can be modeled by the following simple ODE:

$$x_i = u_i + a\sin(\omega_i t) \qquad \dot{u}_i = -\frac{2k}{a} J_i(x)\sin(\omega_i t)$$

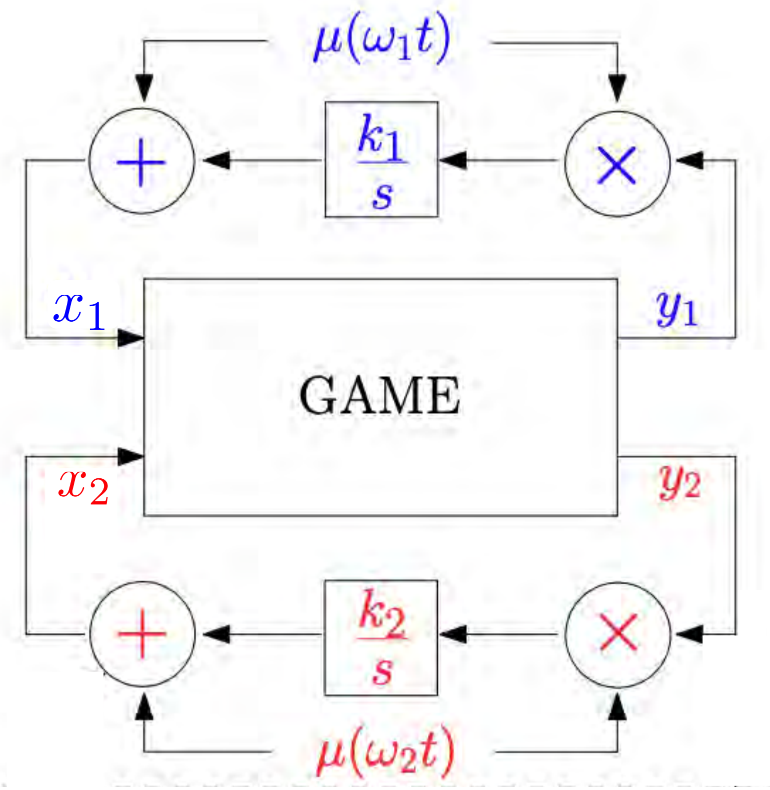
Exploration   Exploitation

Stability and convergence guarantees are well-known for these methods:

$$|u(t) - u^*| \leq Me^{-mt}|u(0) - u^*| + \mathcal{O}\left(\frac{1}{\omega} + a\right)$$

Stochastic and discrete-time variations also exist:

$$u_i^+ = u_i - \alpha\frac{2k}{a} J_i(u + aM)M_i$$



μ : sinusoidal probing signals

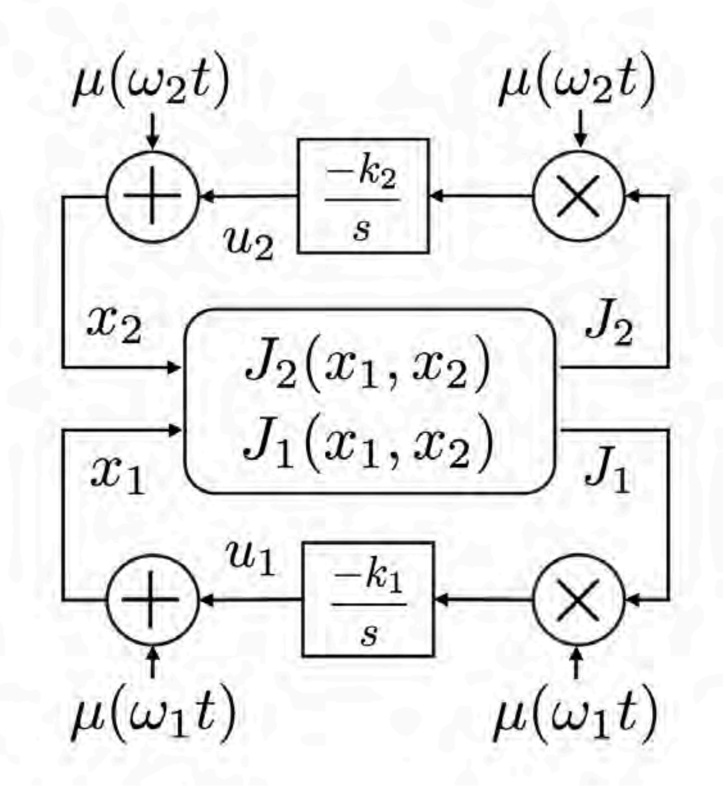
Frequencies of exploration need to be different between players!

P. Frihauf, M. Krstic and T. Basar, "Nash Equilibrium Seeking in Noncooperative Games," in *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1192-1207, 2012.
J. I. Poveda, M. Krstic, T. Basar, "Fixed-Time Nash Equilibrium Seeking in Time-Varying Networks", IEEE Transactions on Automatic Control, vol 68, No 4, pp. 1954-1969, Apr. 2023.

Connections to Encryption and Decryption: Symmetric Key Cryptography

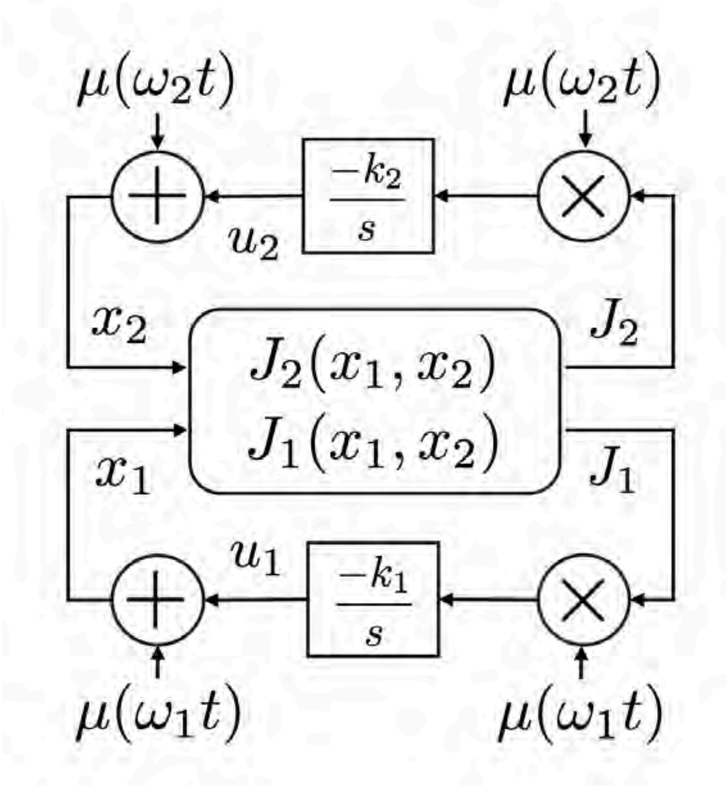
Exploration and **exploitation** mechanisms **in each play**er are coupled by the use of a **common "key"**

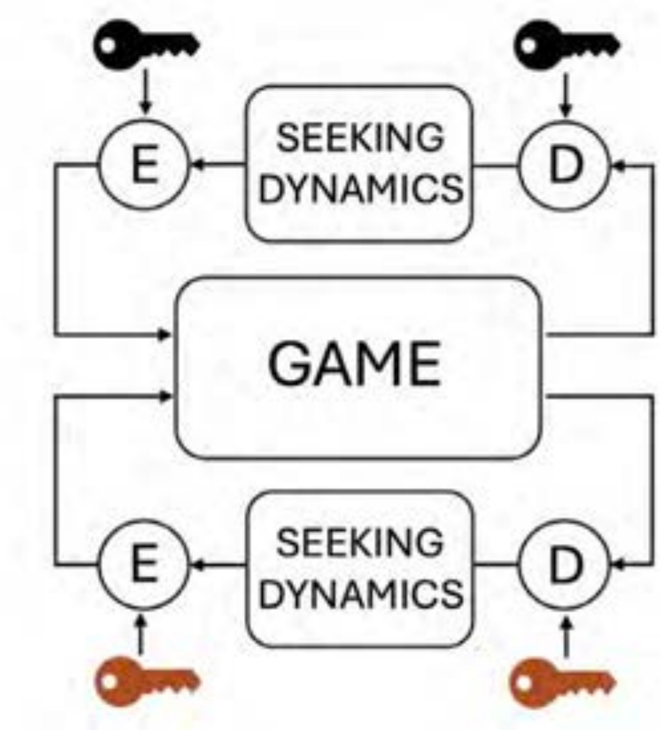
Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**



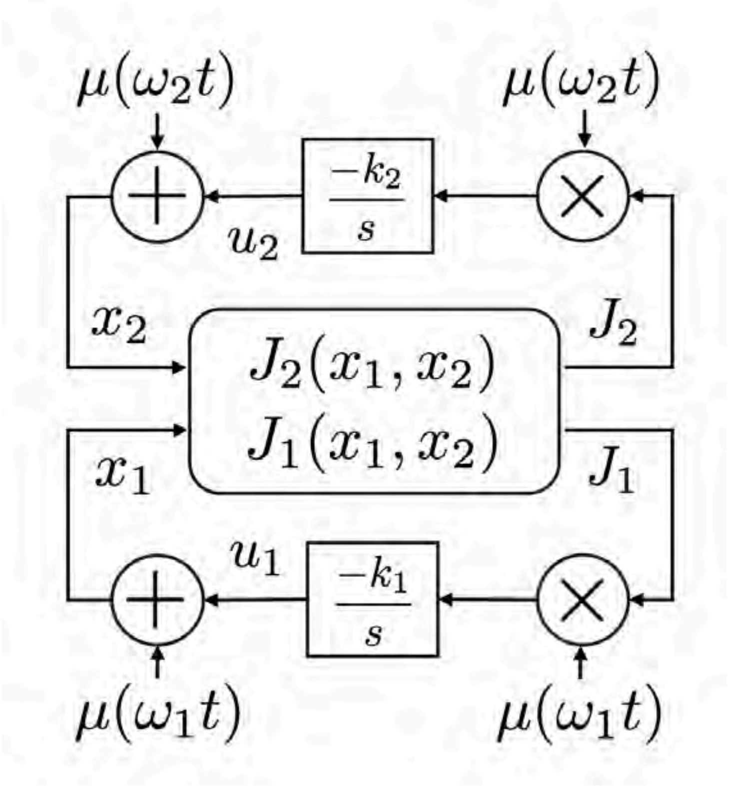
Connections to Encryption and Decryption: Symmetric Key Cryptography

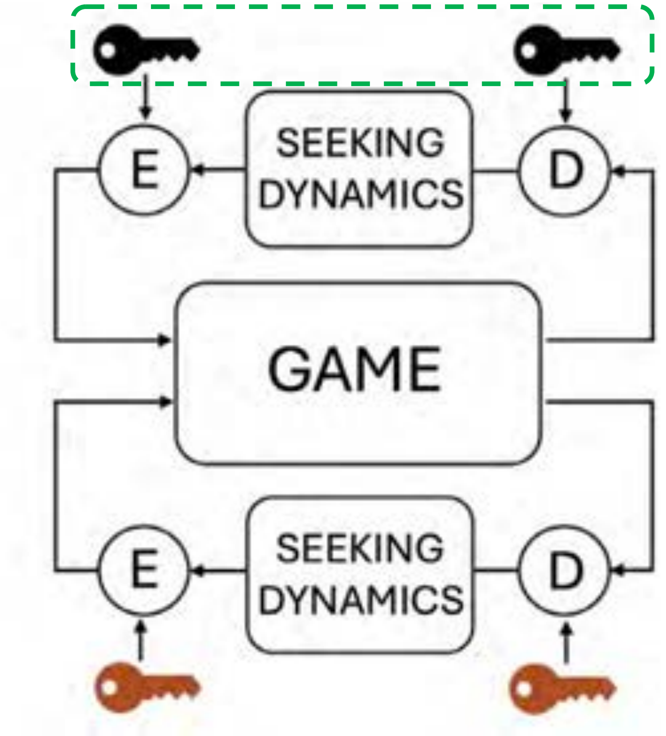
Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**



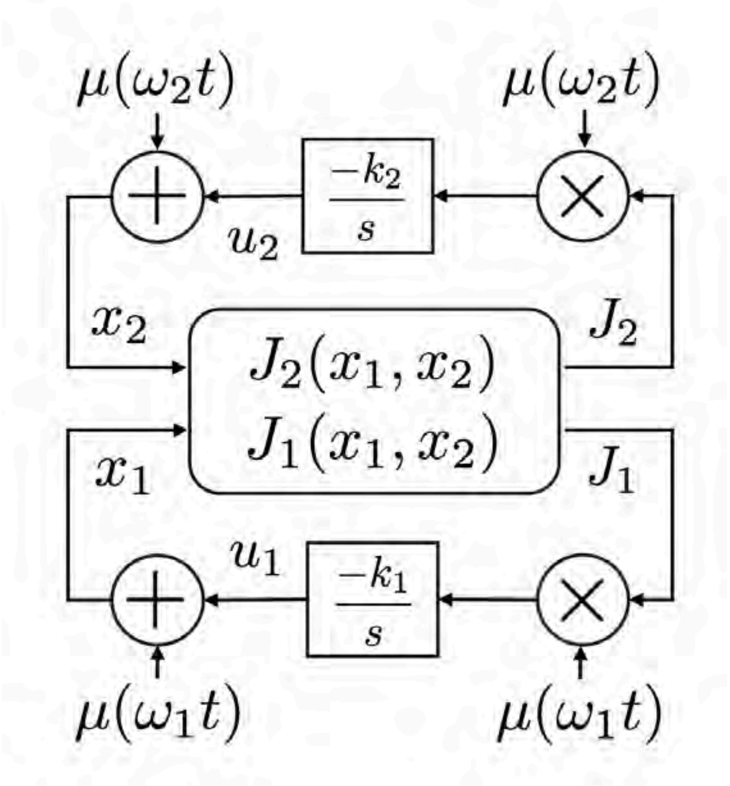


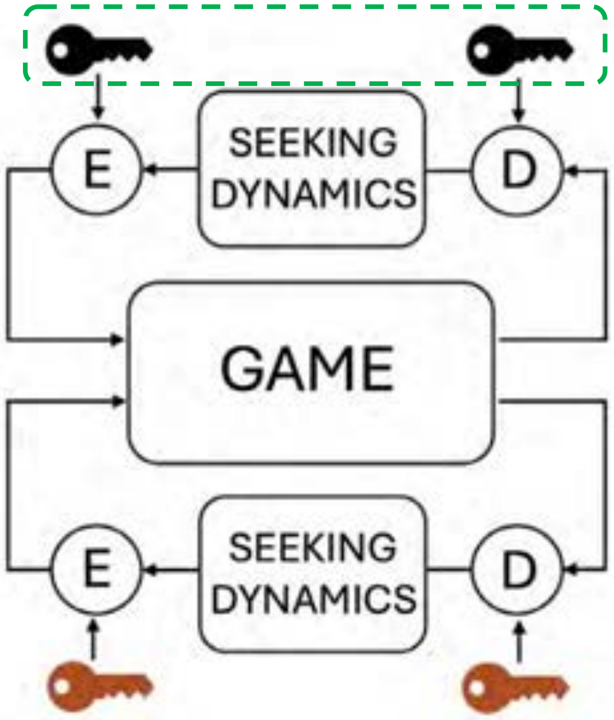
Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common “key”**





Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**

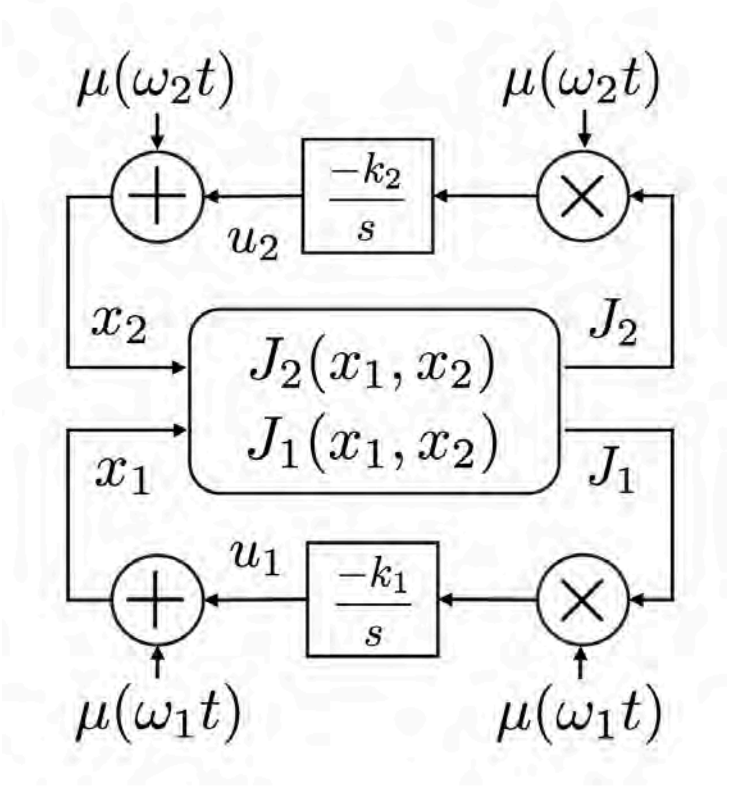


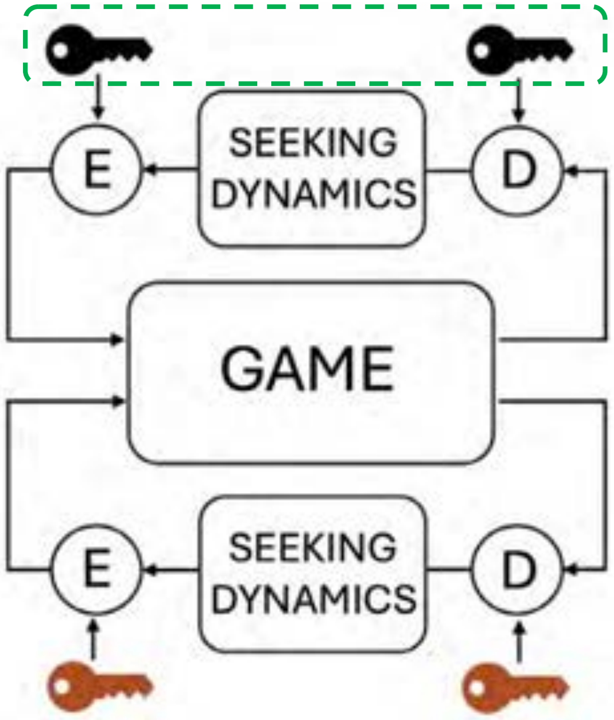


Convergence to Nash equilibria depends on **maintaining the individual key secret** from the other players

Connections to Encryption and Decryption: Symmetric Key Cryptography

Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**



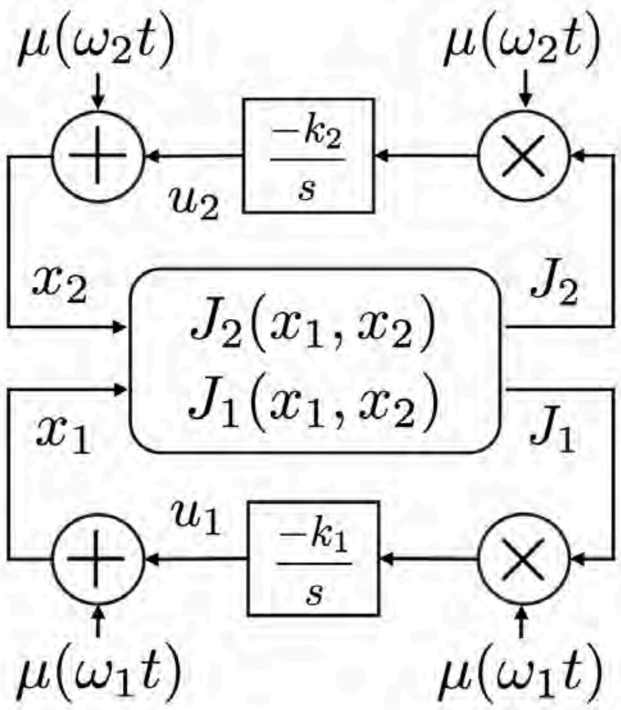


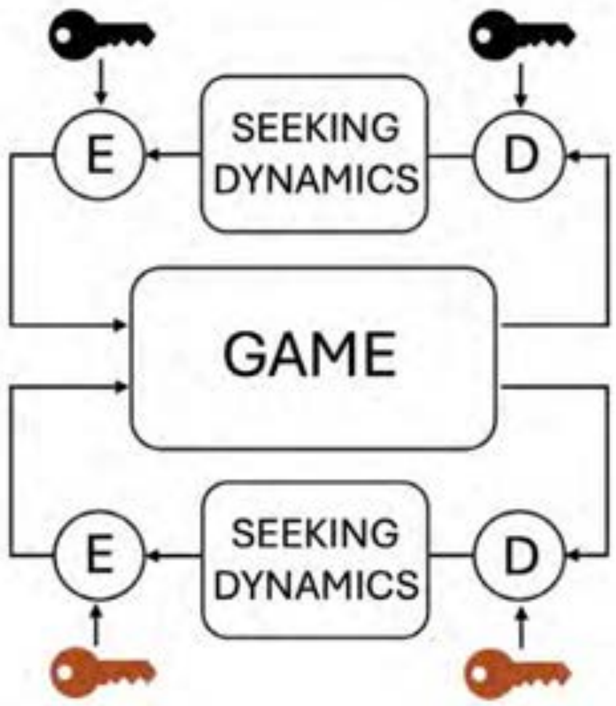
Convergence to Nash equilibria depends on **maintaining the individual key secret** from the other players

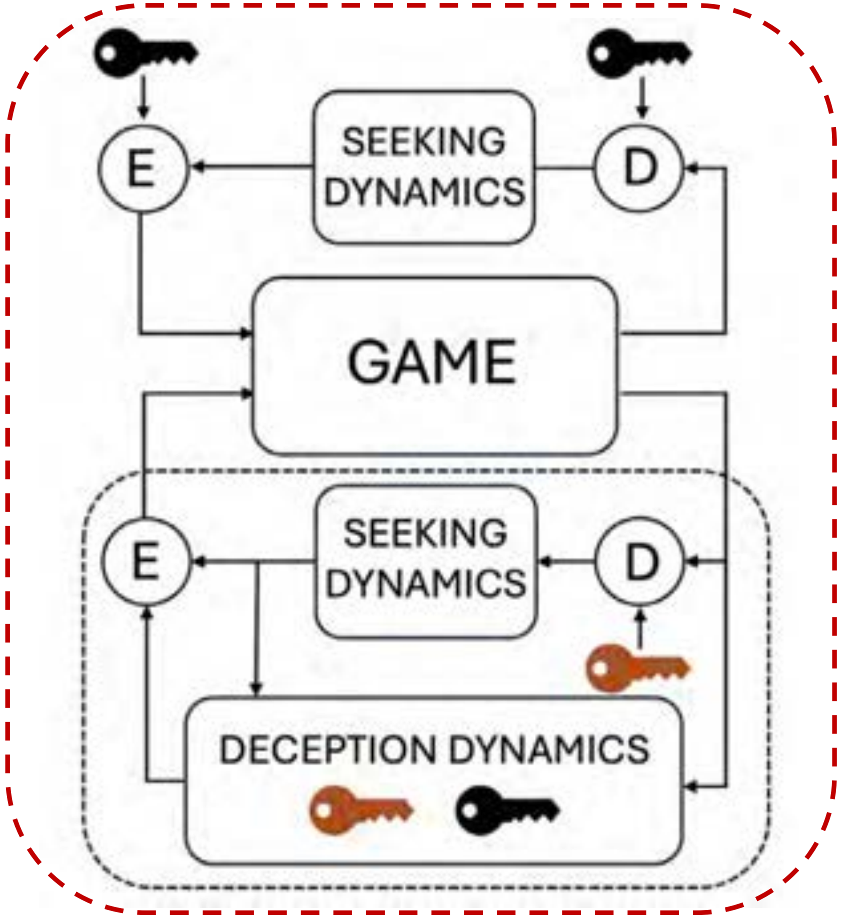
Situation of interest: one (or more) player gains access to the key(s) of the other player(s)?

Connections to Encryption and Decryption: Symmetric Key Cryptography

Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**

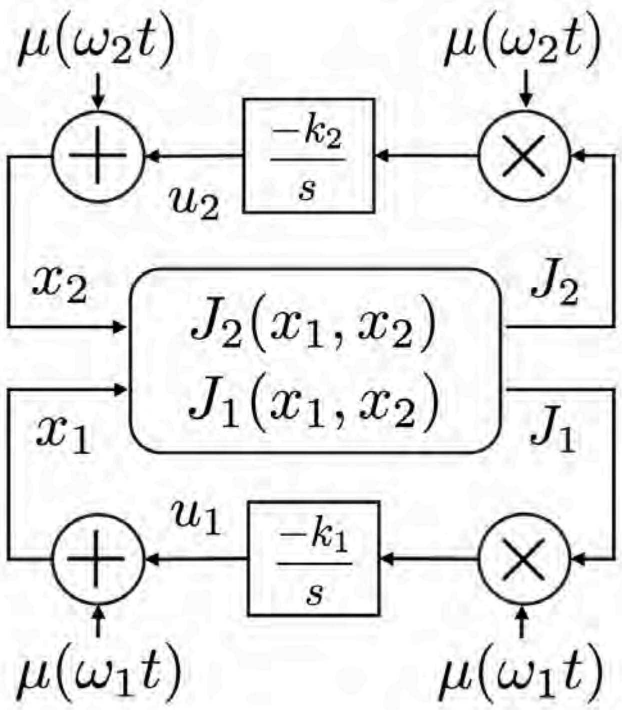


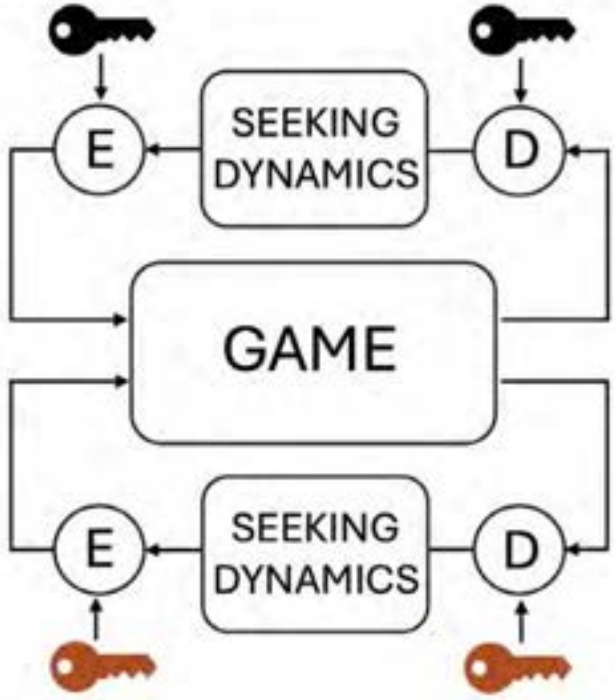


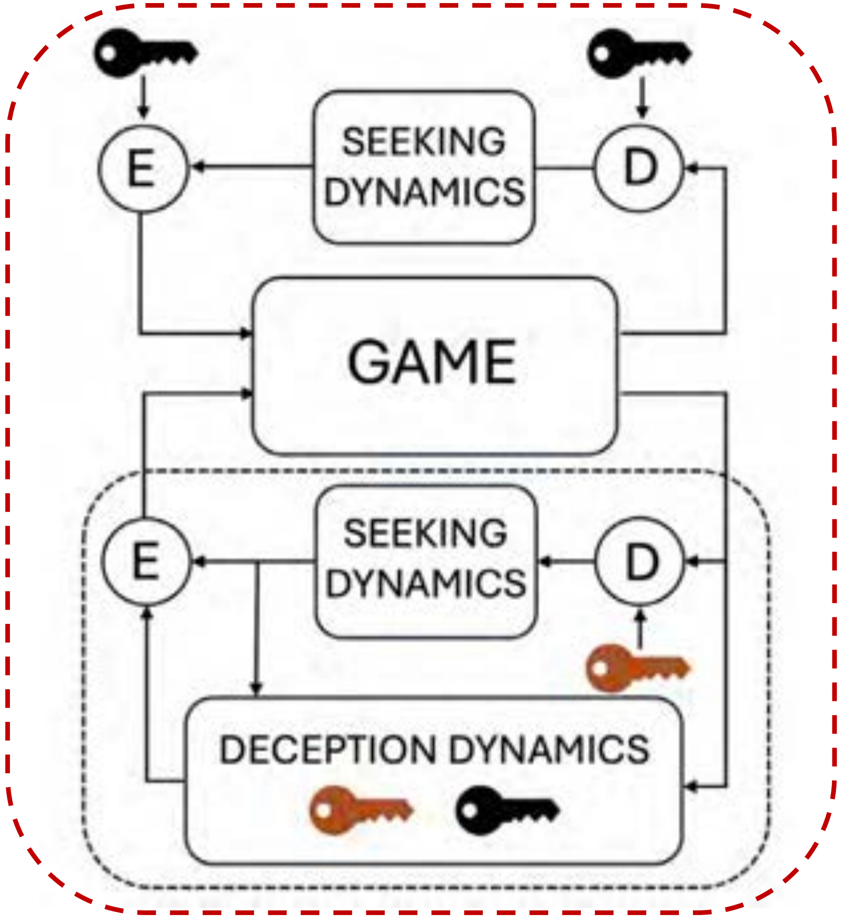


Connections to Encryption and Decryption: Symmetric Key Cryptography

Exploration and **exploitation** mechanisms **in each player** are coupled by the use of a **common "key"**

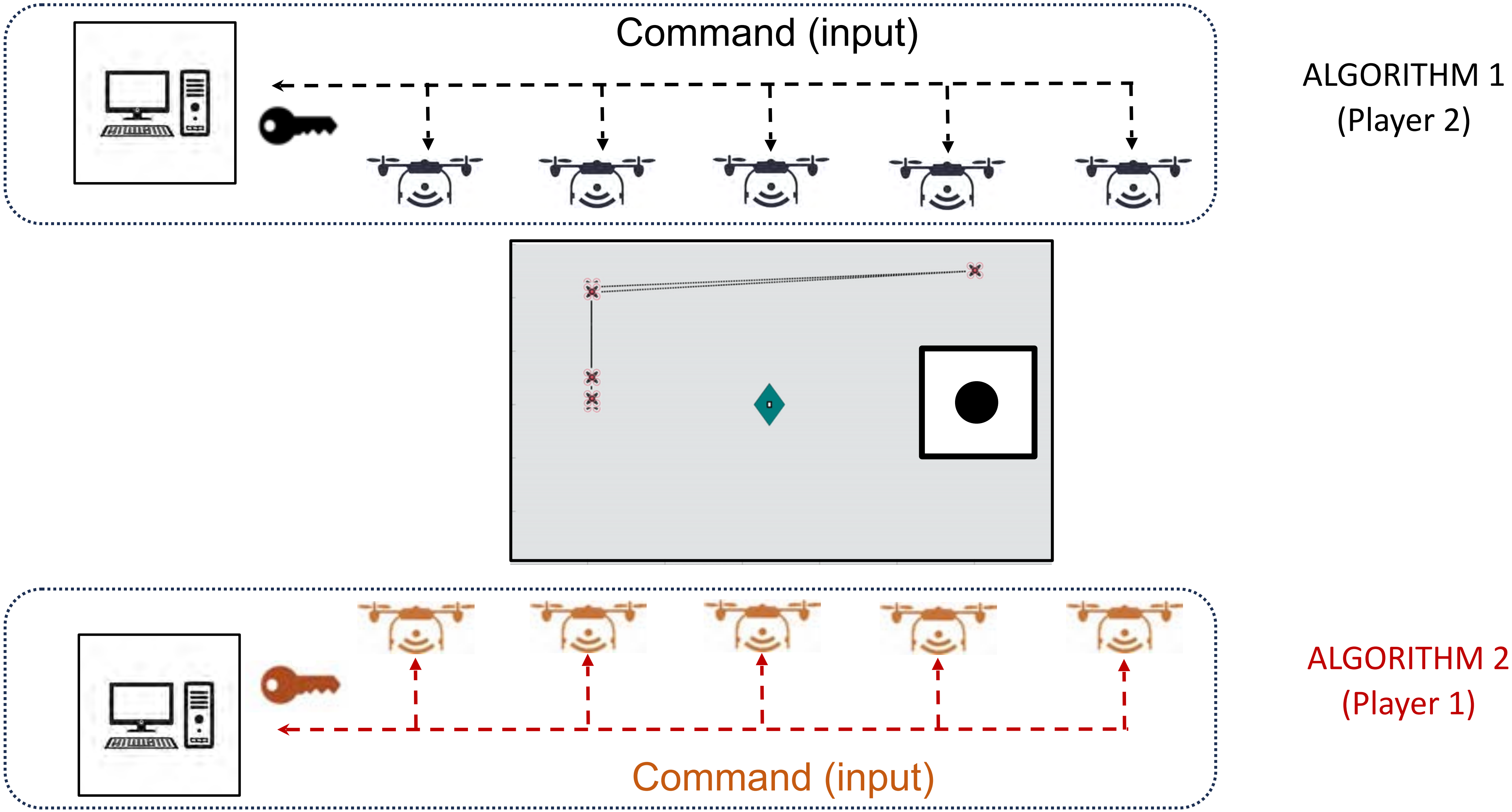




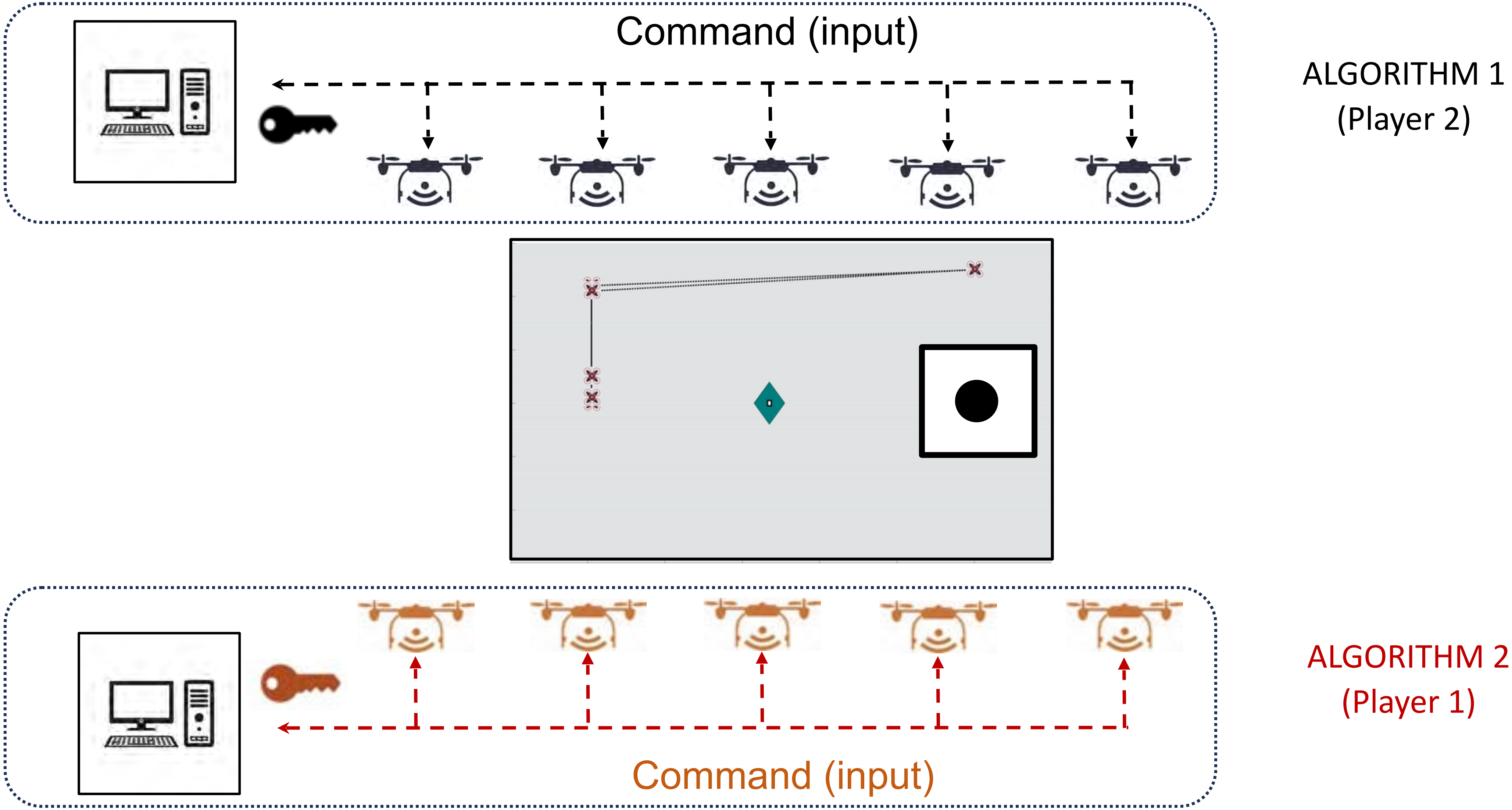


How to systematically exploit **privileged information** in algorithms for AI-enabled multi-agent systems?

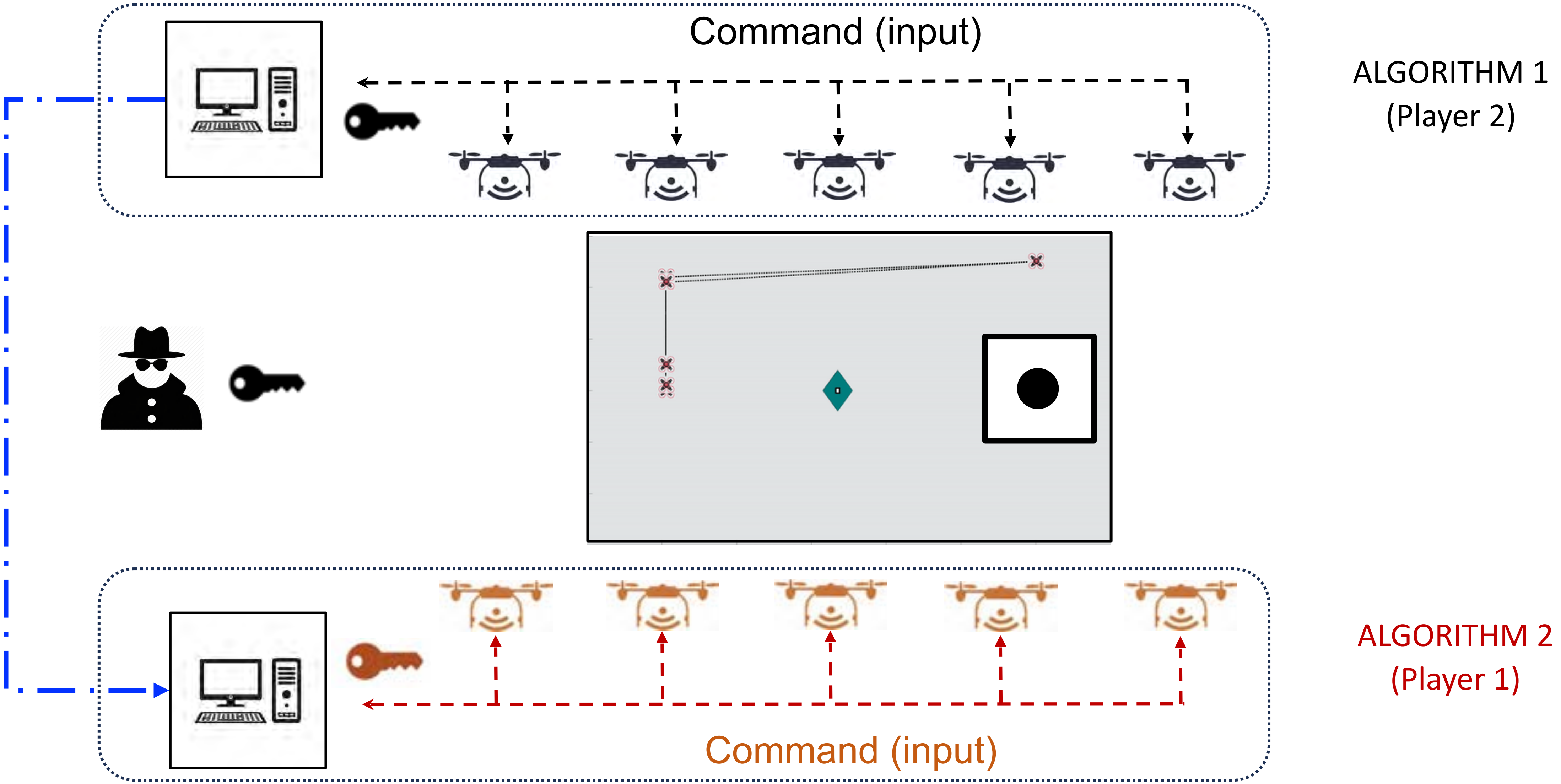
Exploiting Privileged Information: AI-Enabled Multi-Agent Systems



Exploiting Privileged Information: AI-Enabled Multi-Agent Systems



Exploiting Privileged Information: AI-Enabled Multi-Agent Systems



Asymmetric Information: Deception in Noncooperative Games

Key ideas: Players with privileged information want to:

a) Use privileged information to their advantage to obtain better payoffs

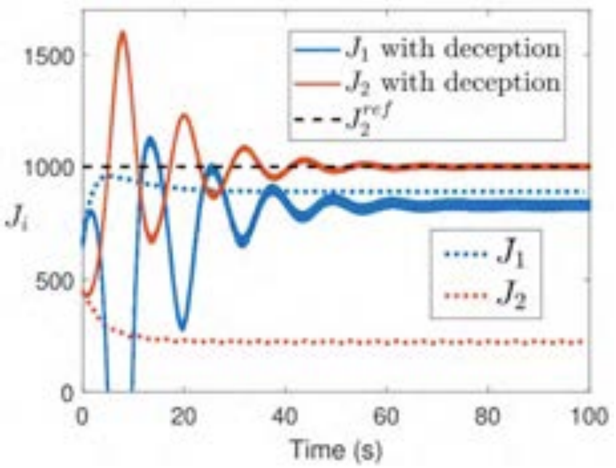
b) Maintain stability of the overall system ("keep business as usual")

Asymmetric Information: Deception in Noncooperative Games

Key ideas: Players with privileged information want to:

a) Use privileged information to their advantage to obtain better payoffs

b) Maintain stability of the overall system ("keep business as usual")

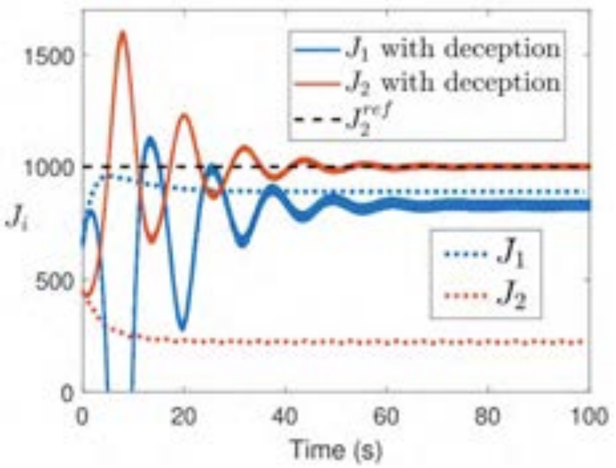


Asymmetric Information: Deception in Noncooperative Games

Key ideas: Players with privileged information want to:

a) Use privileged information to their advantage to obtain better payoffs

b) Maintain stability of the overall system ("keep business as usual")



How to achieve this?

a) Deliberately mislead the victims, without changing their algorithms, into **believing or learning** models of the game that are not truthful

b) Via appropriate design of multi-time scale adaptive feedback-based mechanisms that "**weaponize**" the exploration policies of the algorithms

Asymmetric Information: Deception in Noncooperative Games

Key ideas: Players with privileged information want to:

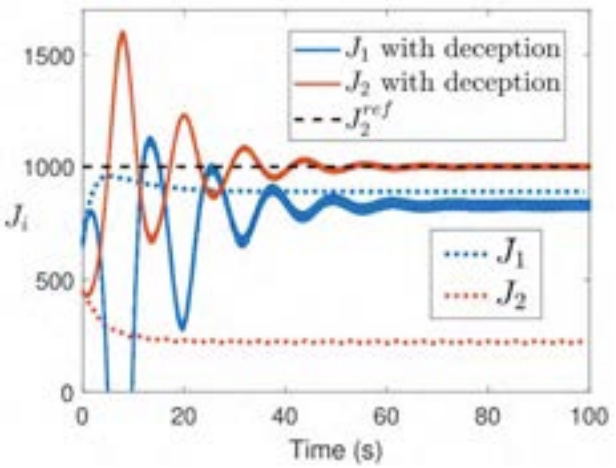
a) Use privileged information to their advantage to obtain better payoffs

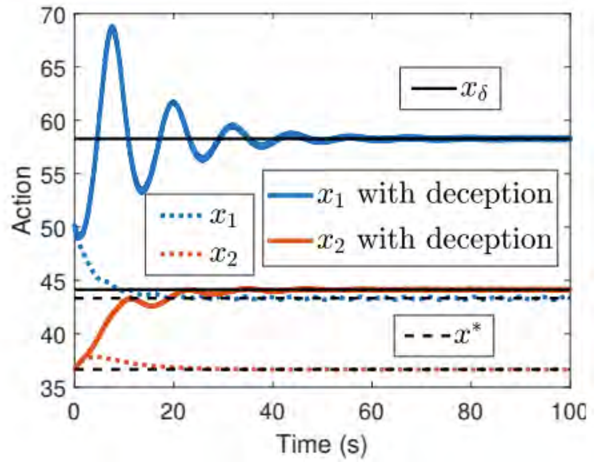
b) Maintain stability of the overall system ("keep business as usual")

How to achieve this?

a) Deliberately mislead the victims, without changing their algorithms, into **believing or learning** models of the game that are not truthful

b) Via appropriate design of multi-time scale adaptive feedback-based mechanisms that "**weaponize**" the exploration policies of the algorithms



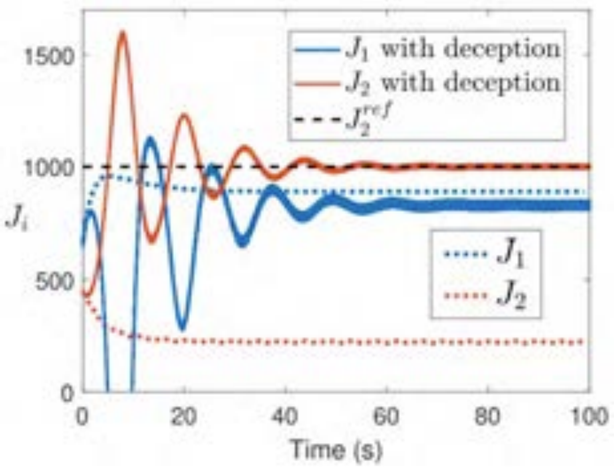


Asymmetric Information: Deception in Noncooperative Games

Key ideas: Players with privileged information want to:

a) Use privileged information to their advantage to obtain better payoffs

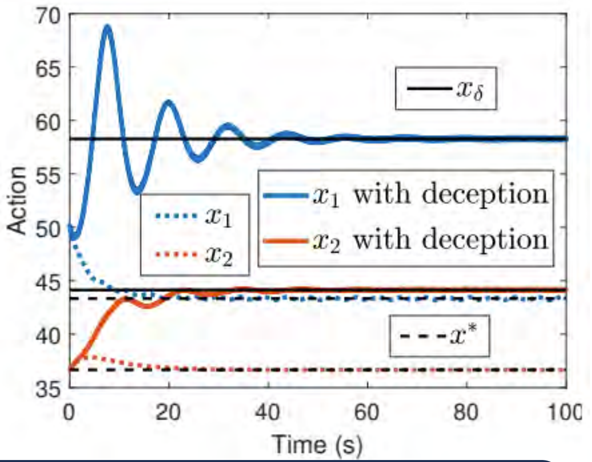
b) Maintain stability of the overall system ("keep business as usual")



How to achieve this?

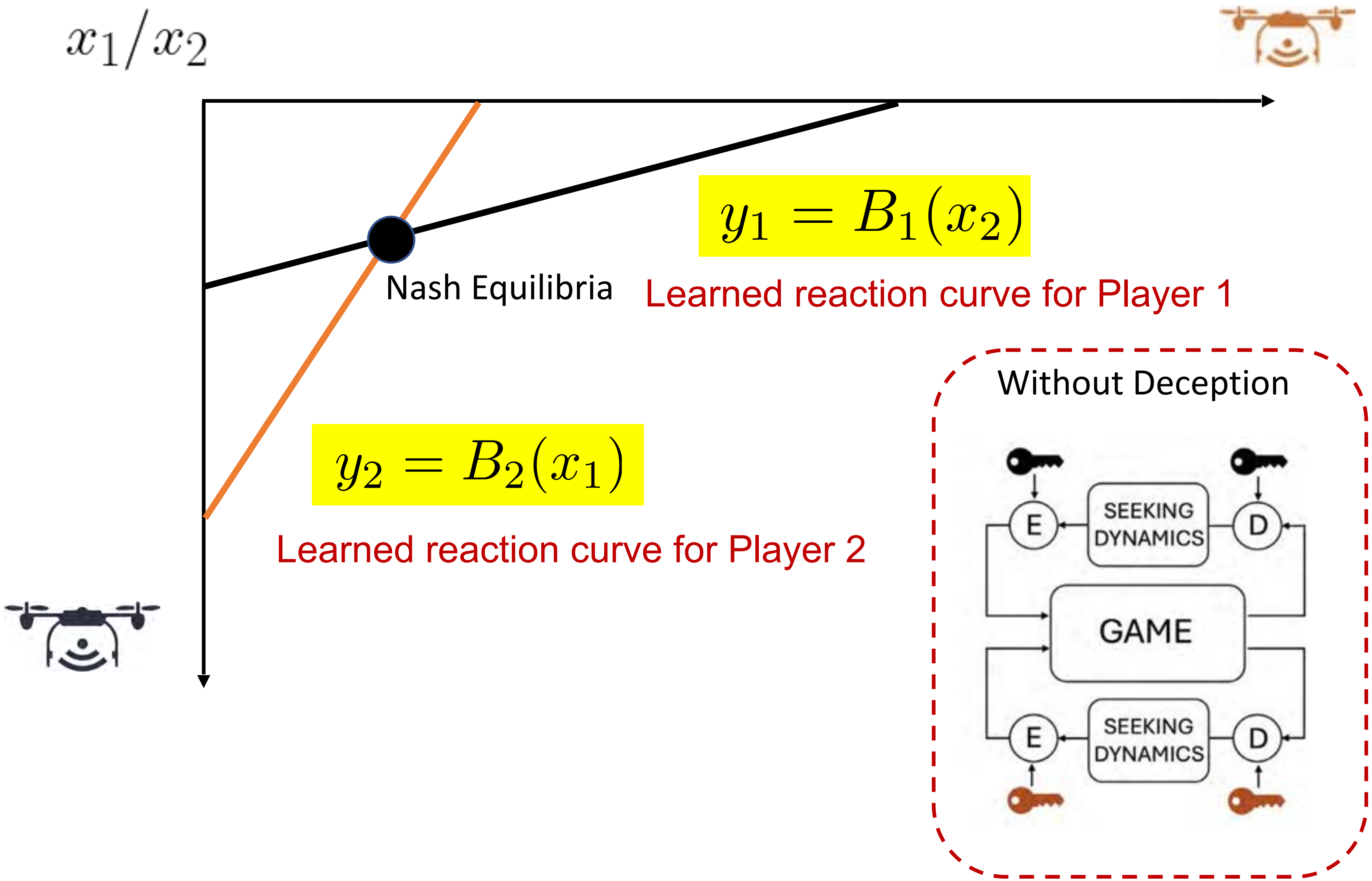
a) Deliberately mislead the victims, without changing their algorithms, into **believing or learning** models of the game that are not truthful

b) Via appropriate design of multi-time scale adaptive feedback-based mechanisms that "**weaponize**" the exploration policies of the algorithms

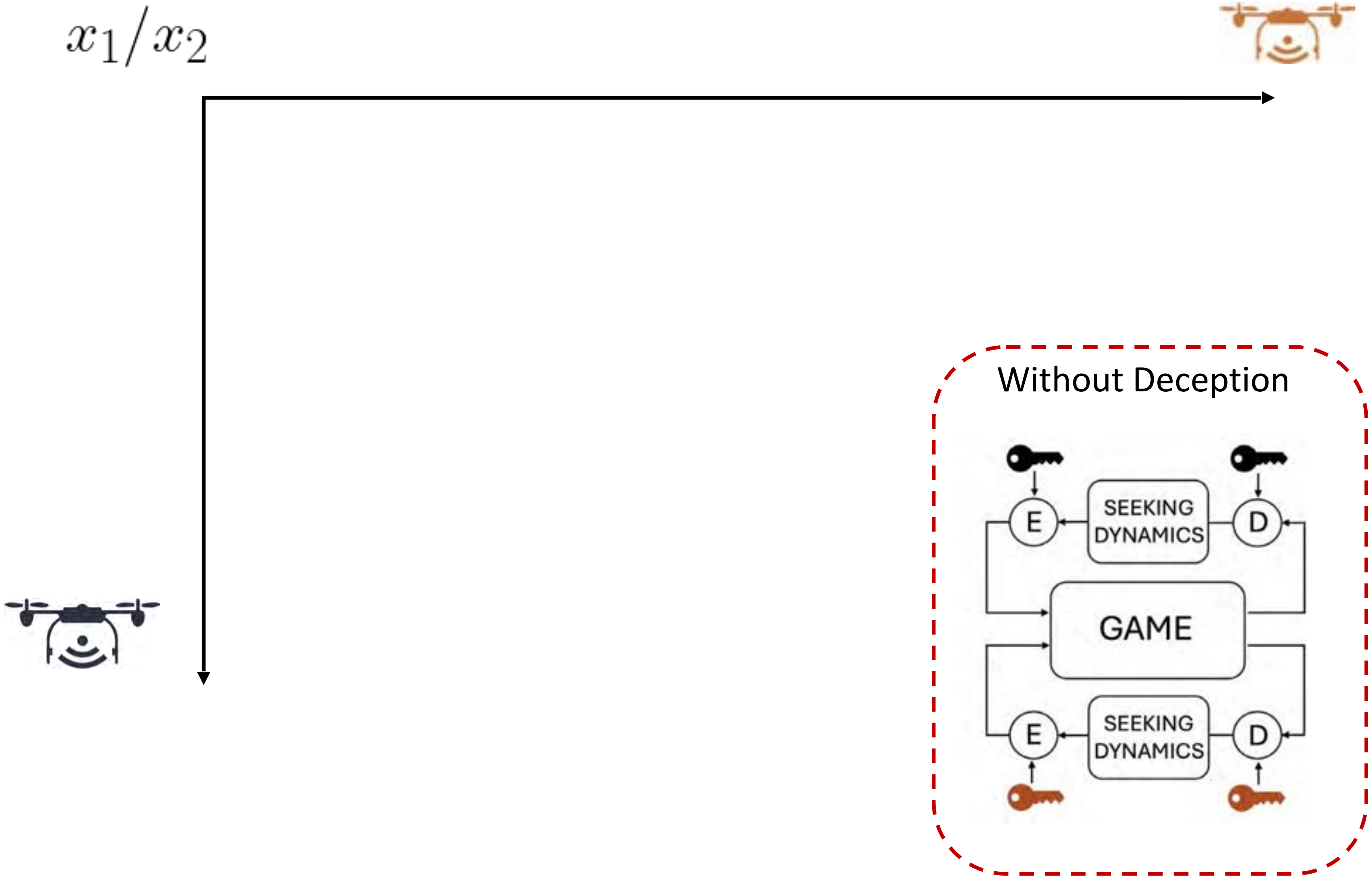


In the context of learning in games: control the "best response" that is learned by the victim

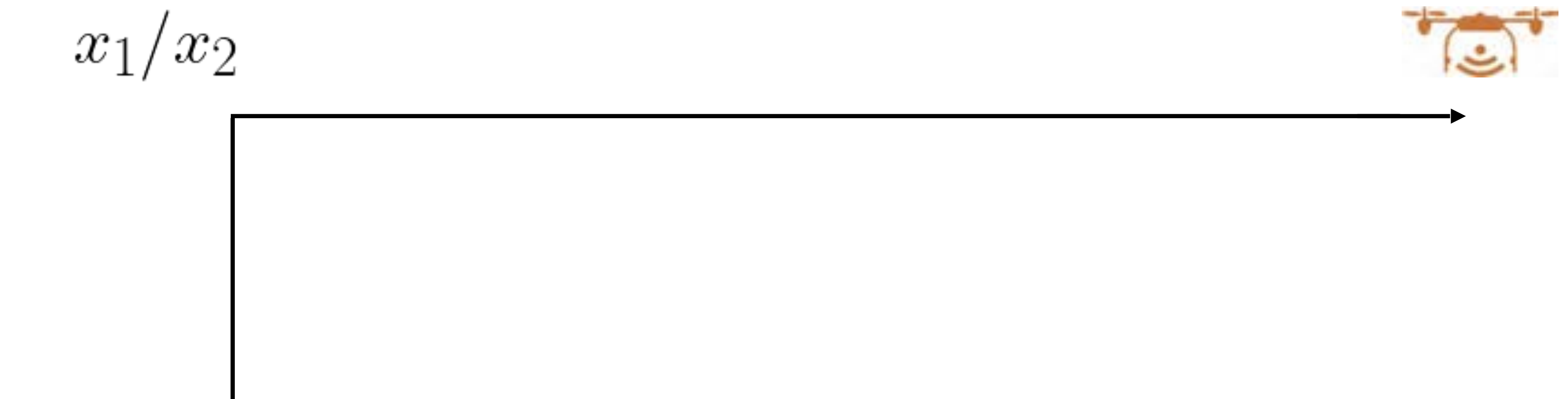
Asymmetric Information: Deception in Noncooperative Games



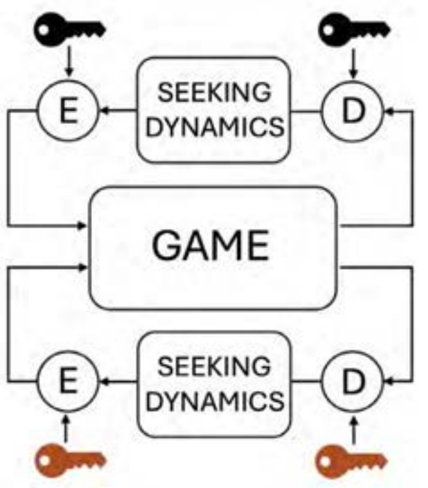
Asymmetric Information: Deception in Noncooperative Games



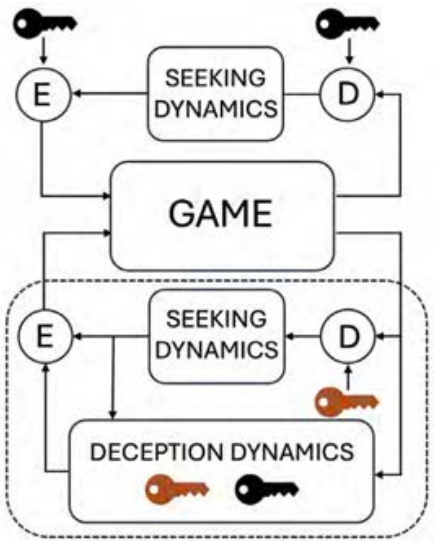
Asymmetric Information: Deception in Noncooperative Games



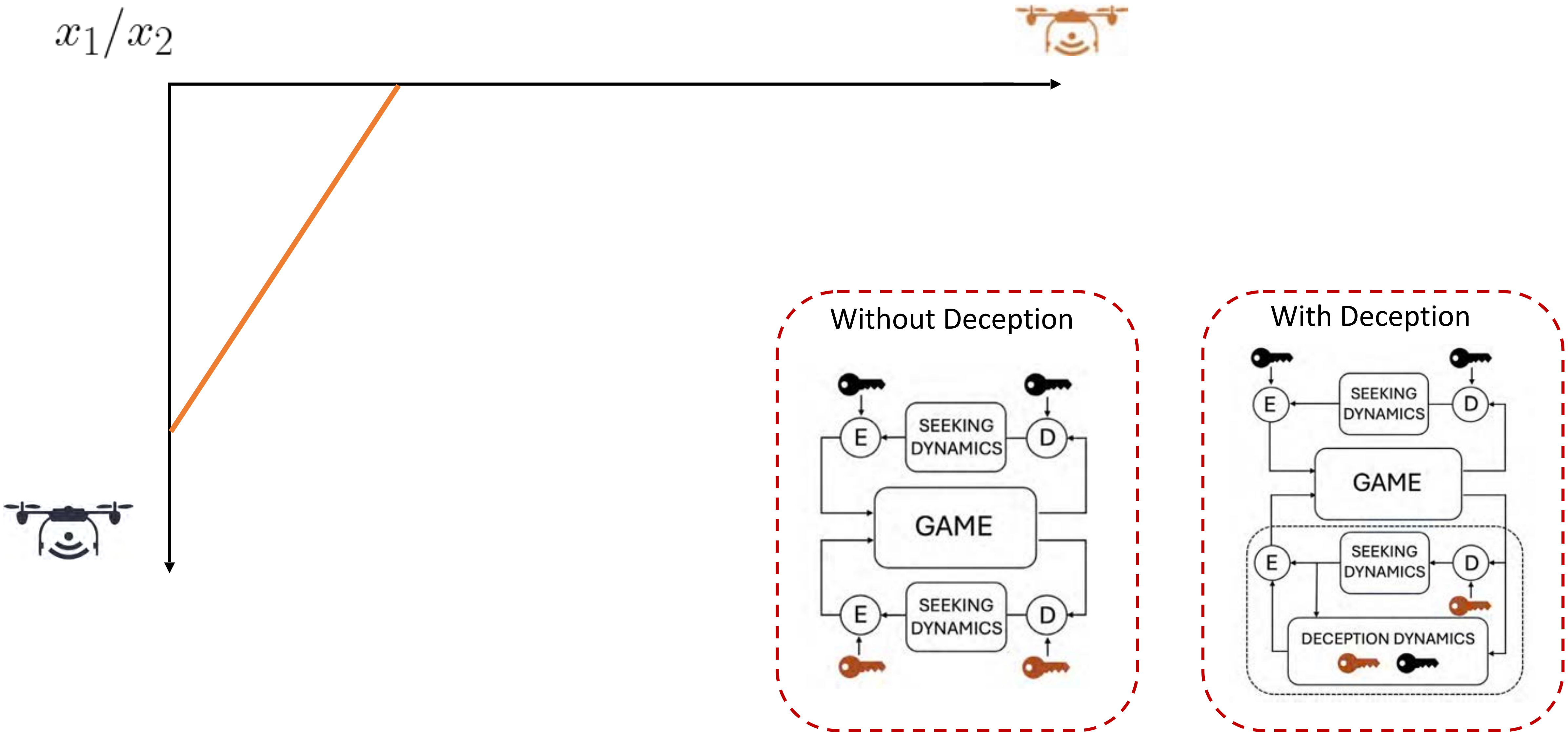
Without Deception



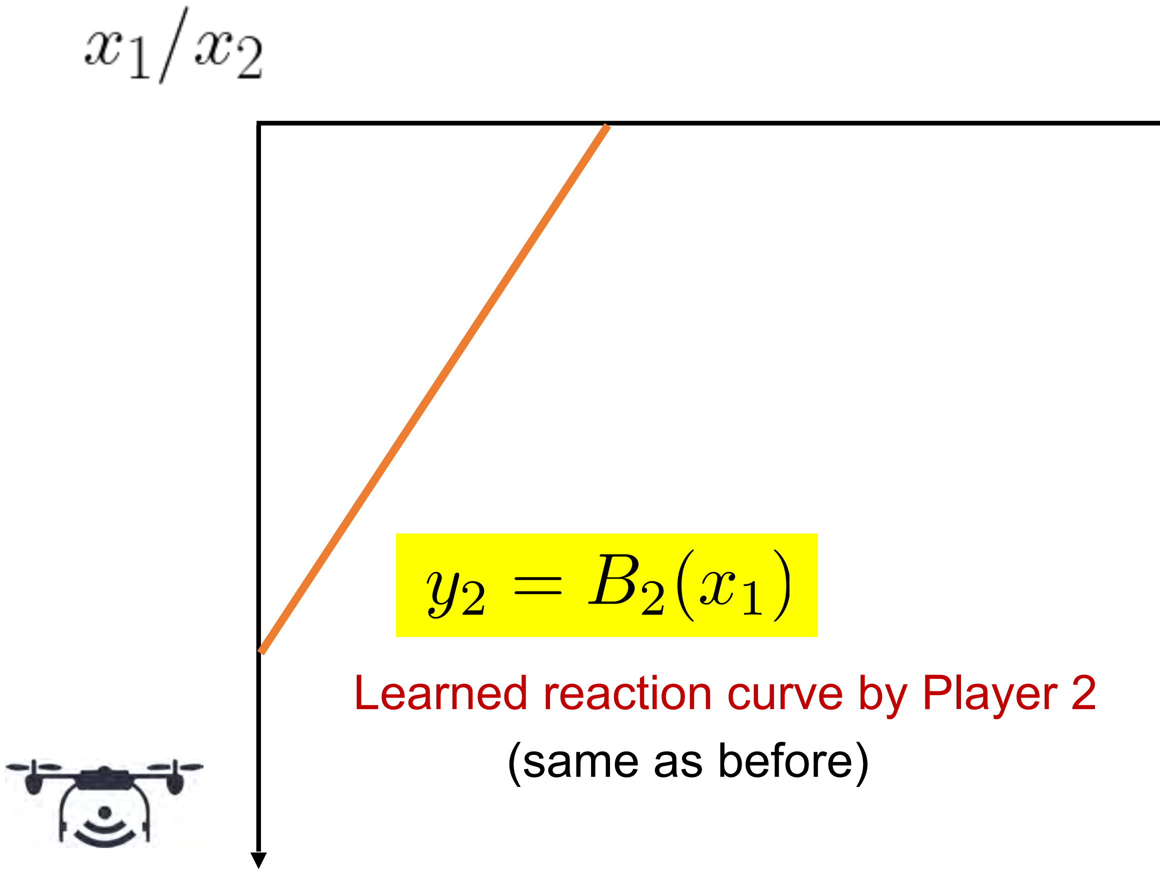
With Deception



Asymmetric Information: Deception in Noncooperative Games

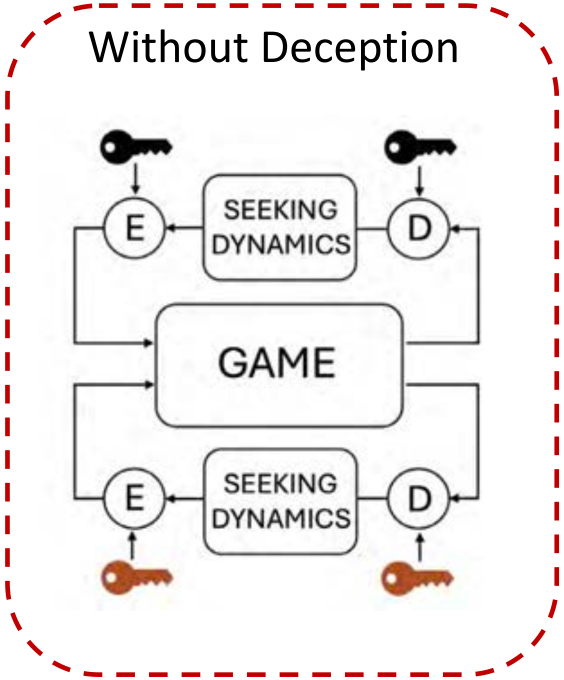


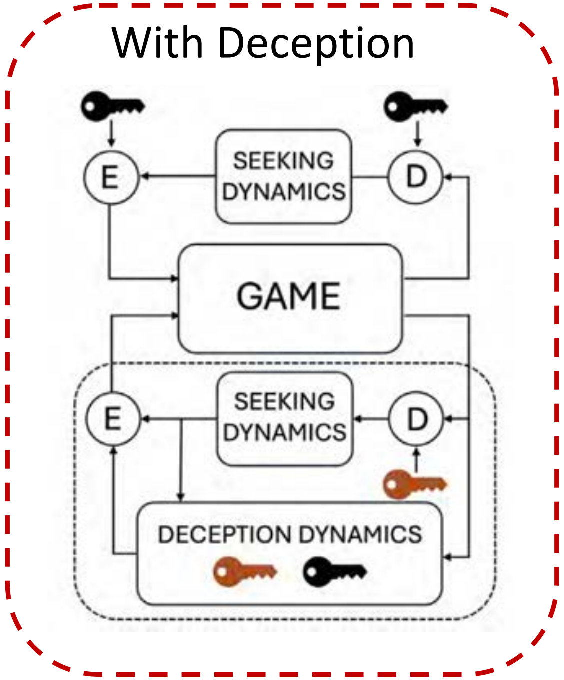
Asymmetric Information: Deception in Noncooperative Games



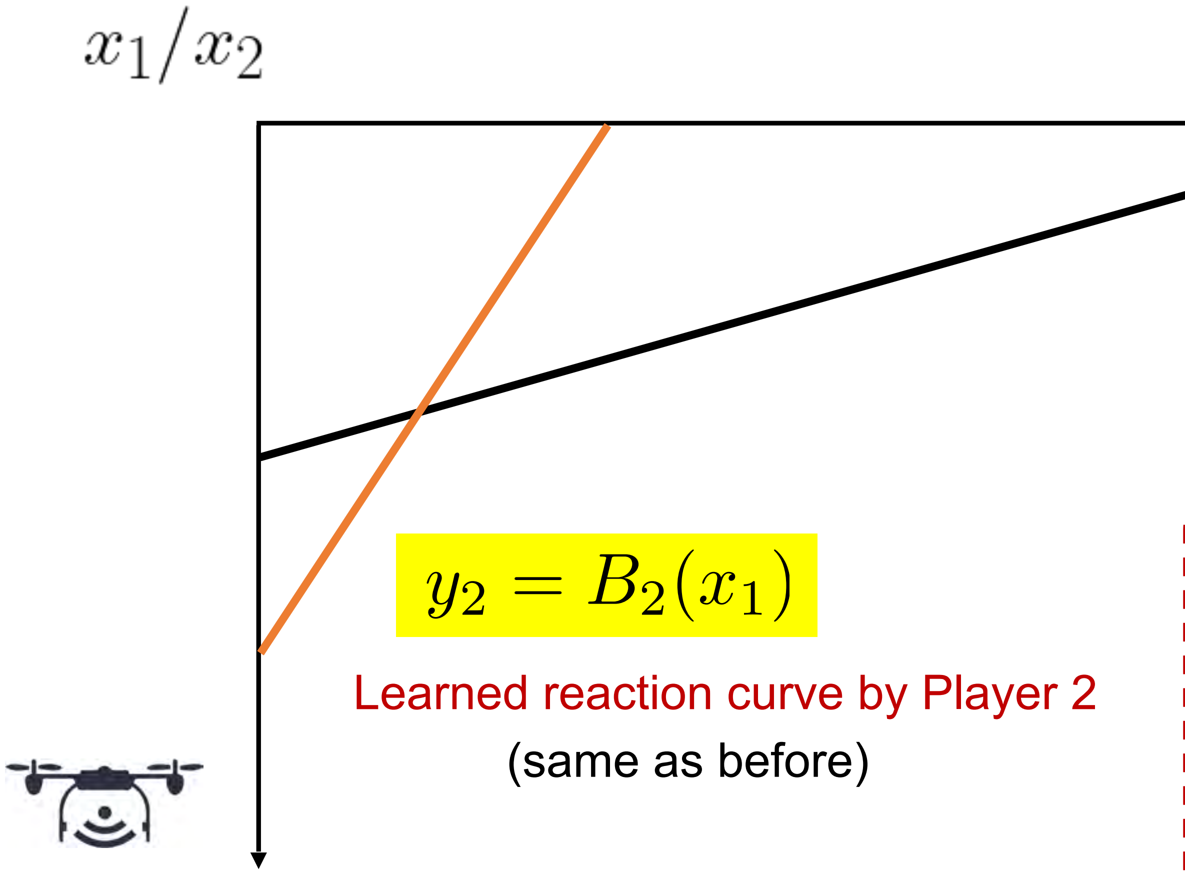
$$y_2 = B_2(x_1)$$

Learned reaction curve by Player 2
(same as before)



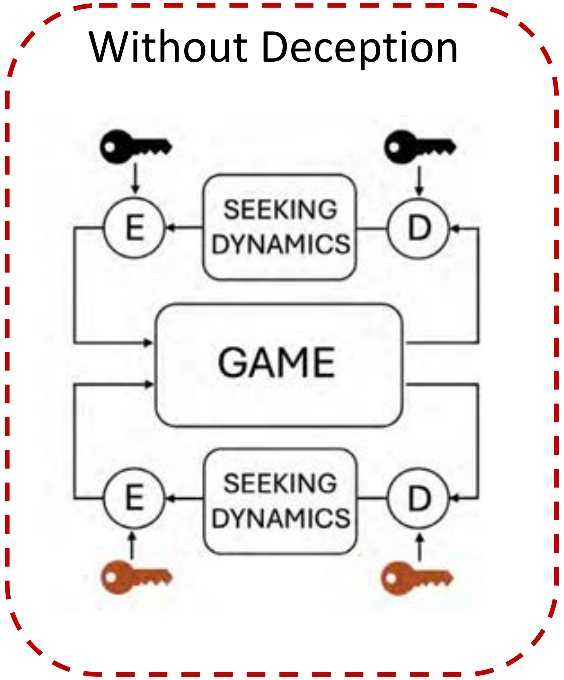


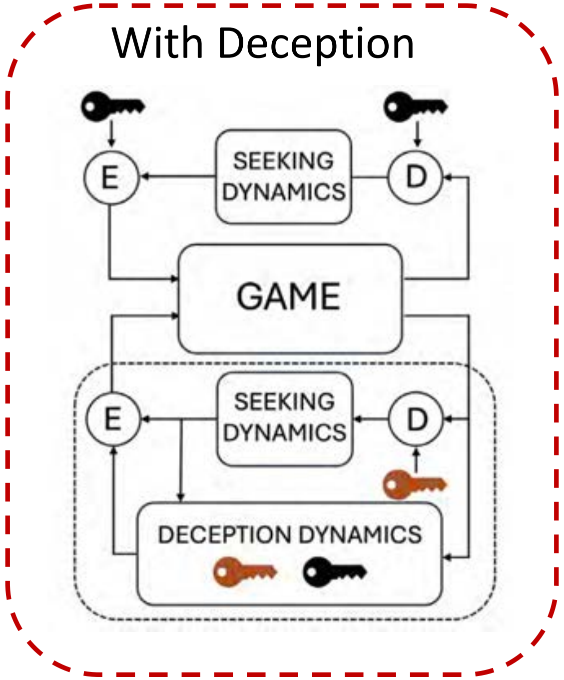
Asymmetric Information: Deception in Noncooperative Games



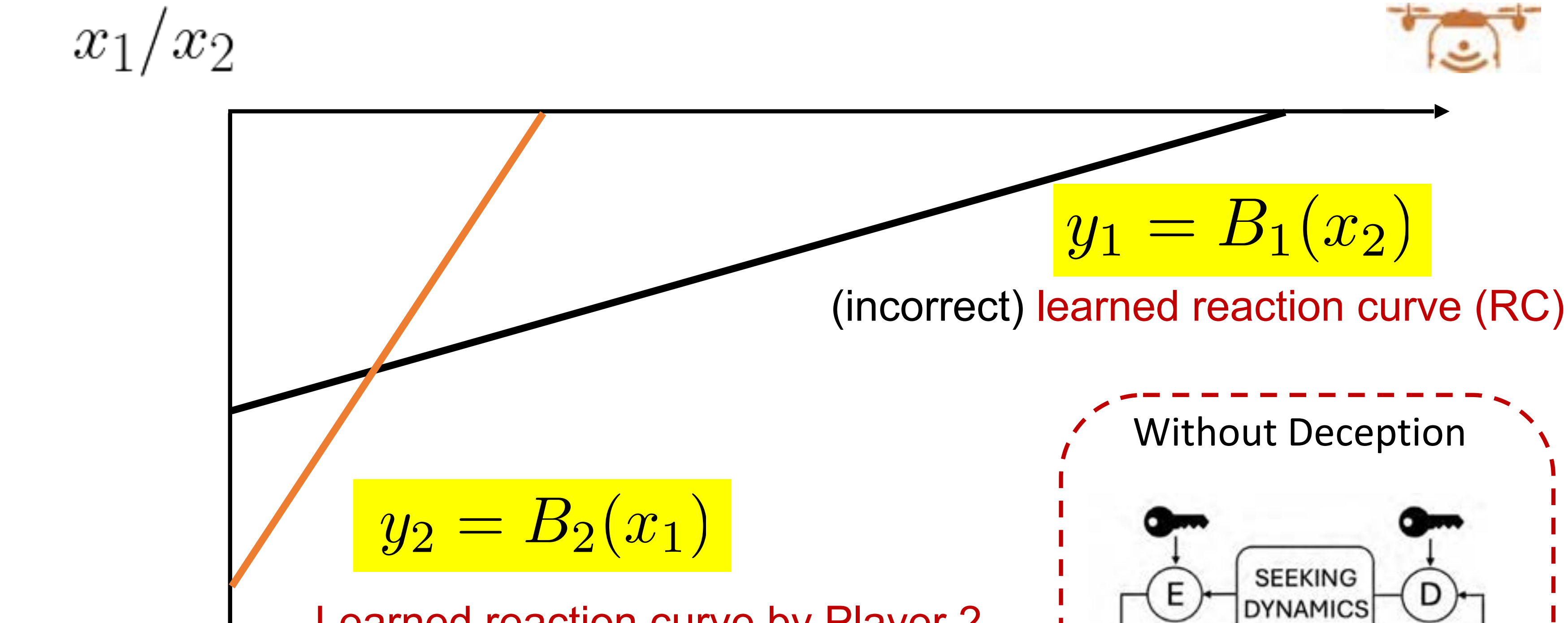
$$y_2 = B_2(x_1)$$

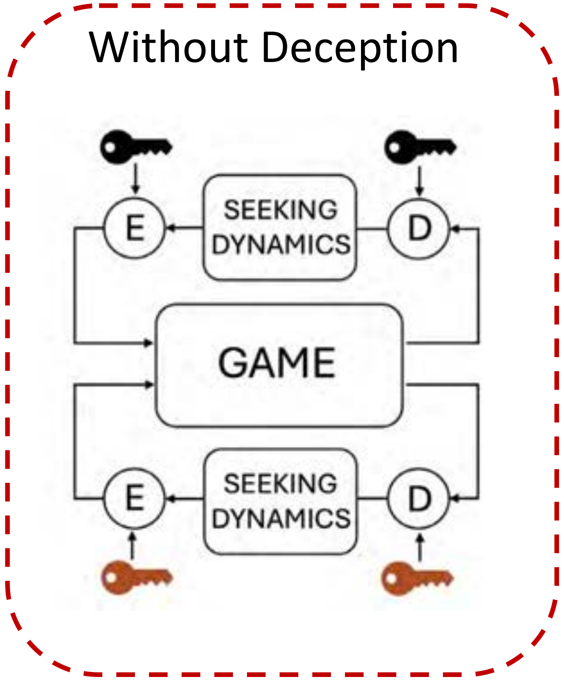
Learned reaction curve by Player 2
(same as before)

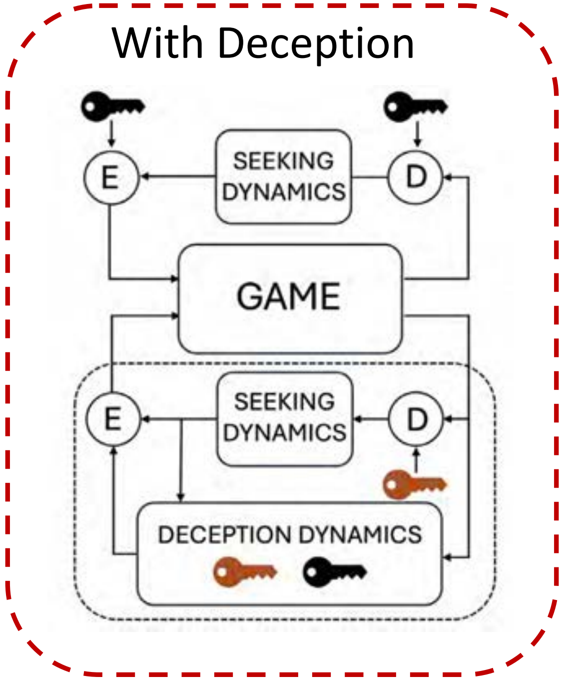




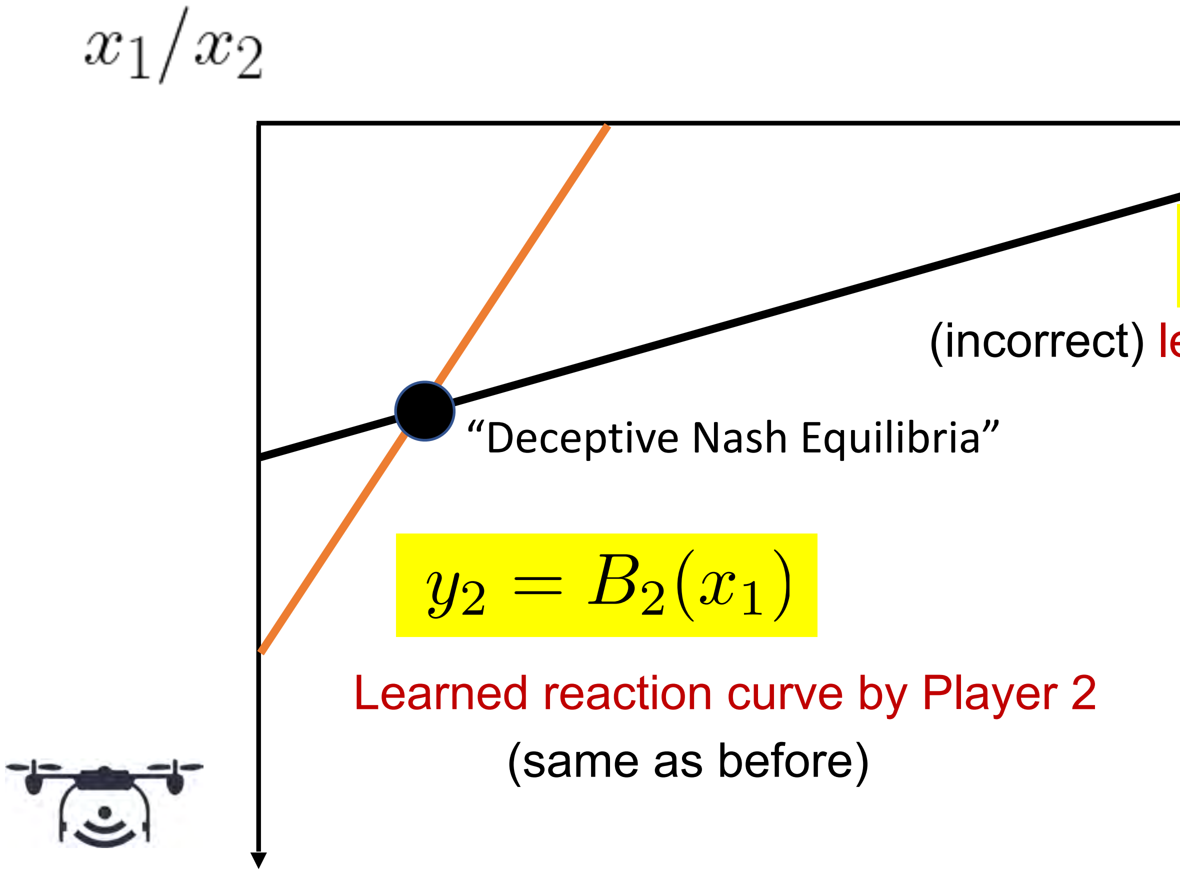
Asymmetric Information: Deception in Noncooperative Games

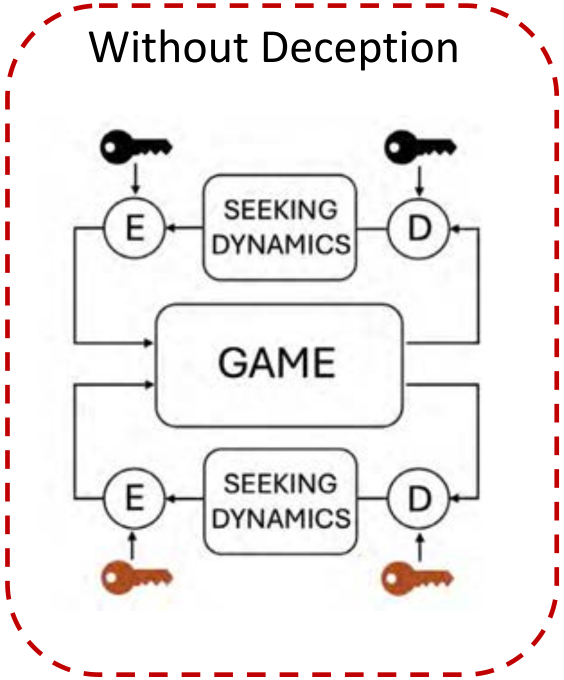


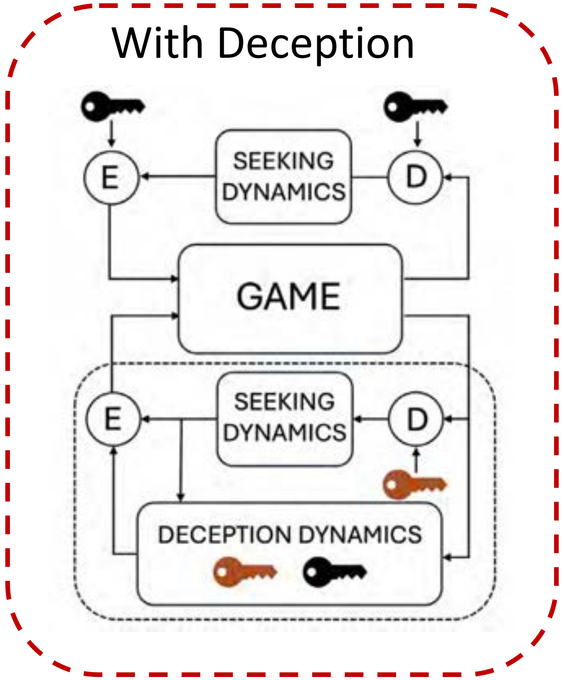




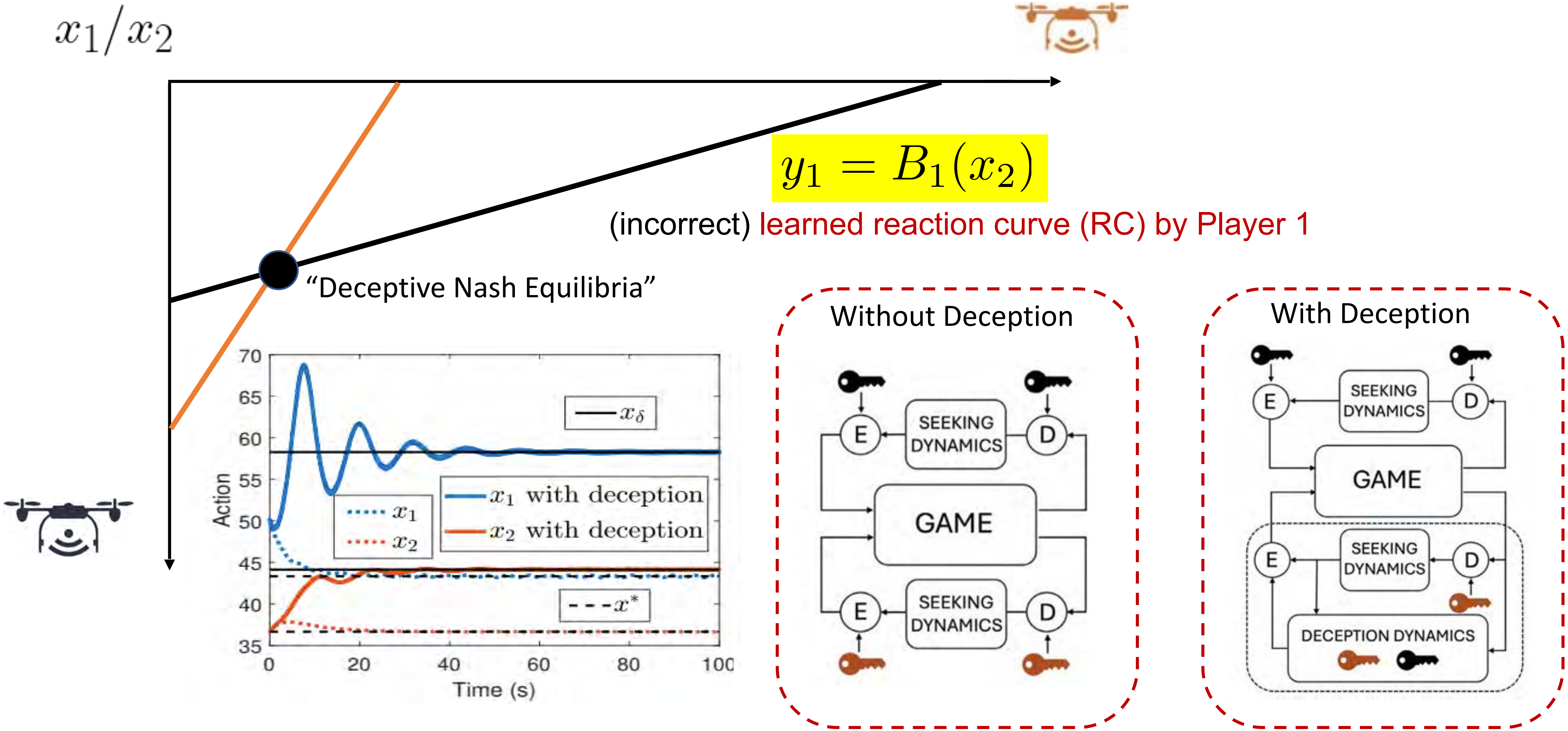
Asymmetric Information: Deception in Noncooperative Games



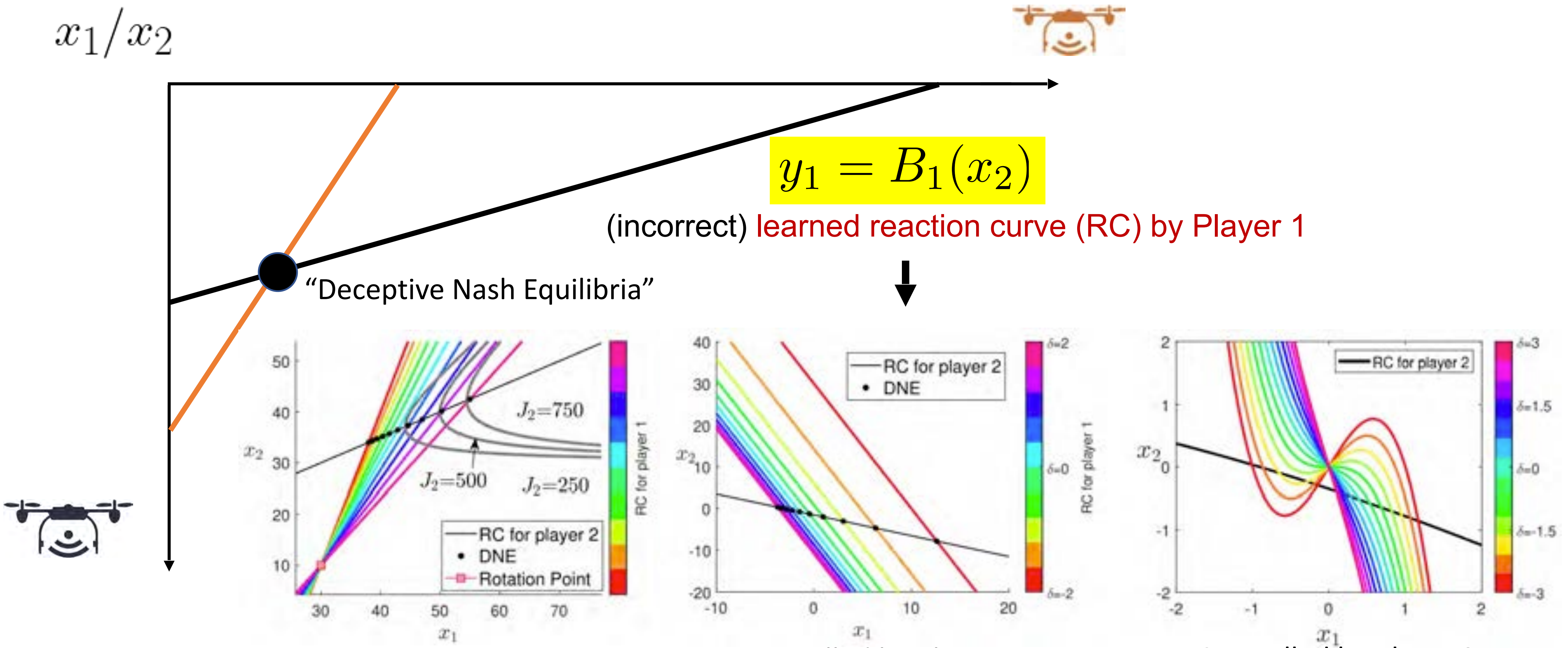




Asymmetric Information: Deception in Noncooperative Games



Asymmetric Information: Deception in Noncooperative Games

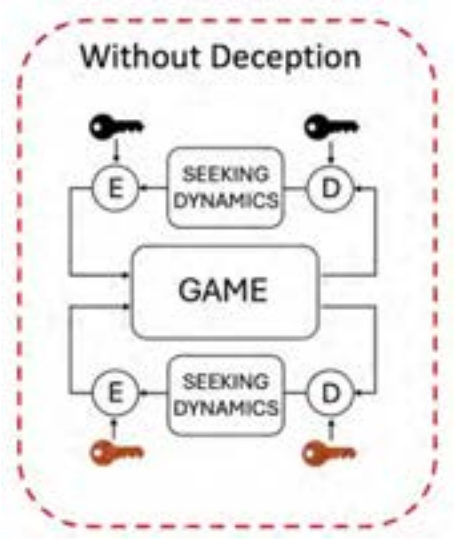


Controlled by player 2 via rotations

Controlled by player 2 via translations

Controlled by player 2 via deformations

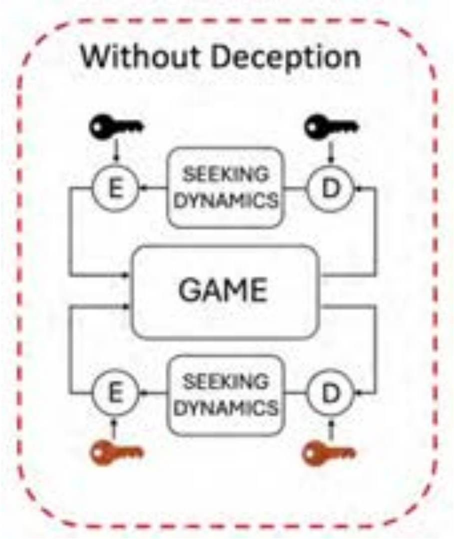
How to achieve this?



$$x_2 = u_2 + a\sin(\omega_2 t)$$

$$\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)$$

How to achieve this?



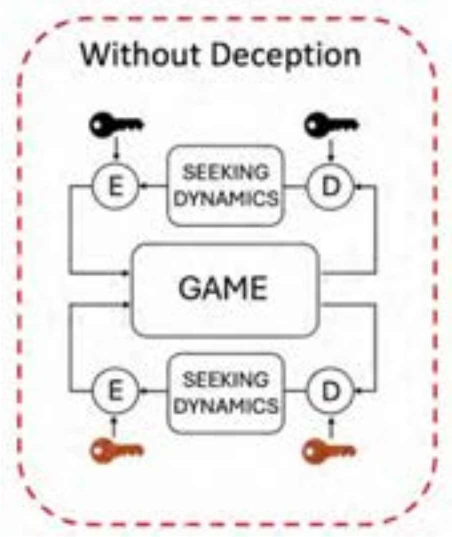
$$x_2 = \underbrace{u_2 + a\sin(\omega_2 t)}_{\text{Exploration}}$$

Exploration

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

Exploitation

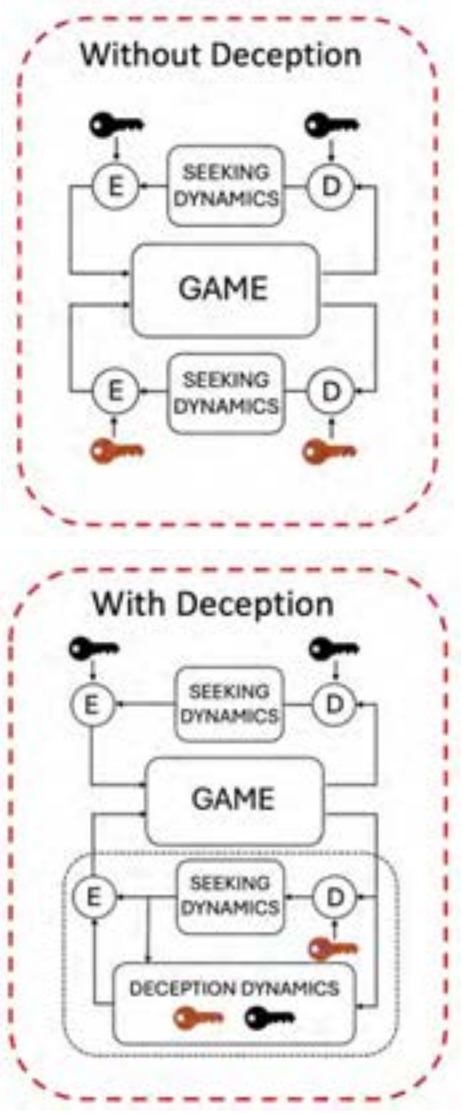
How to achieve this?



$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

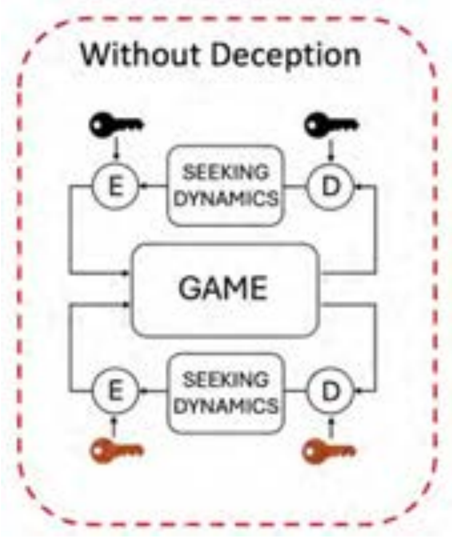
How to achieve this?

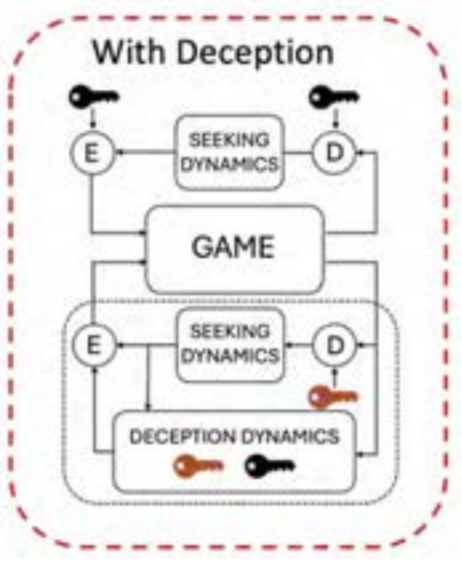


$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

How to achieve this?





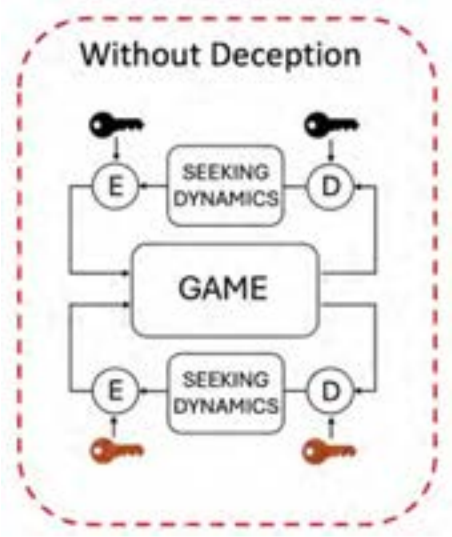
$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t)}_{\text{Exploration}}$$

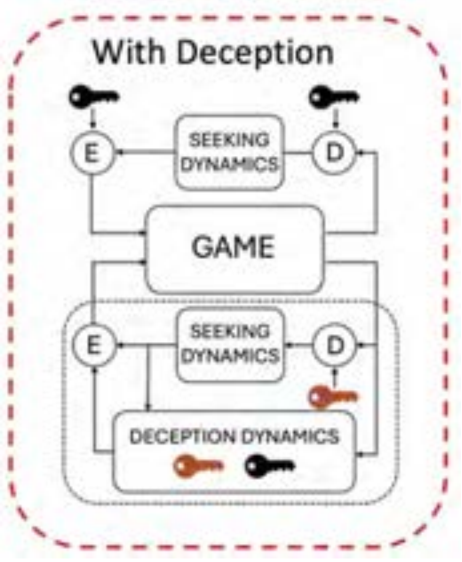
$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + a\sin(\omega_2 t) + \delta \sin(\omega_1 t)$$

$$\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)$$

How to achieve this?





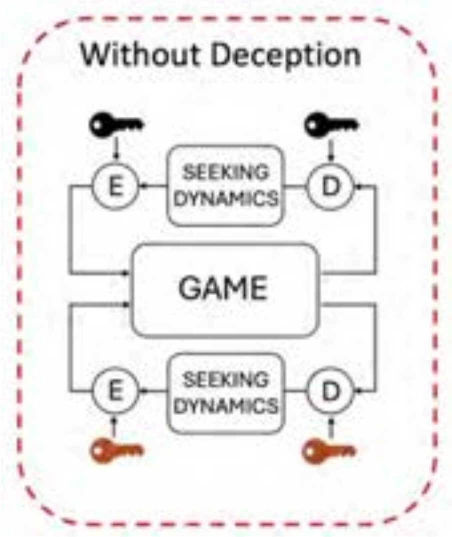
$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}}$$

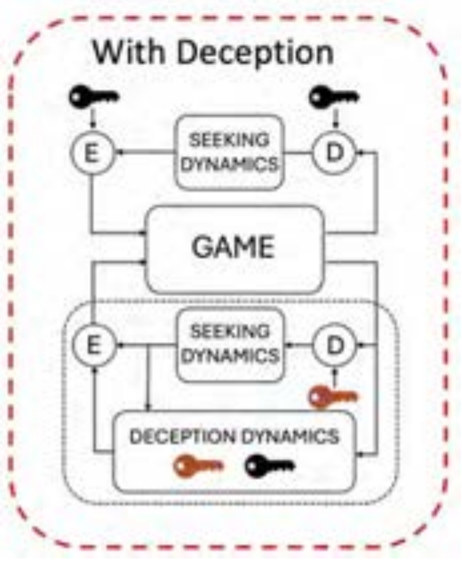
$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t) + \delta \sin(\omega_1 t)}_{\text{Exploration with Deception}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

How to achieve this?

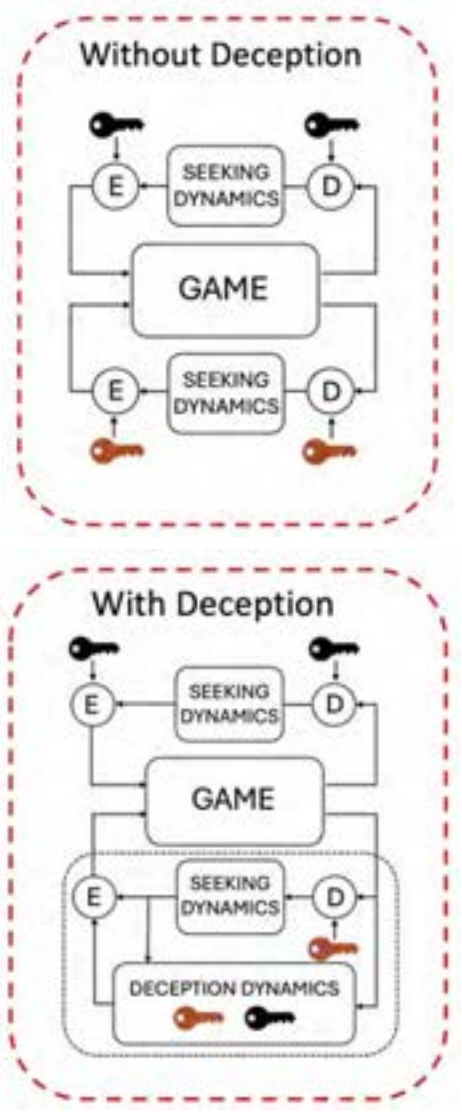




$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t) + \delta \sin(\omega_1 t)}_{\text{Exploration with Deception}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

How to achieve this?



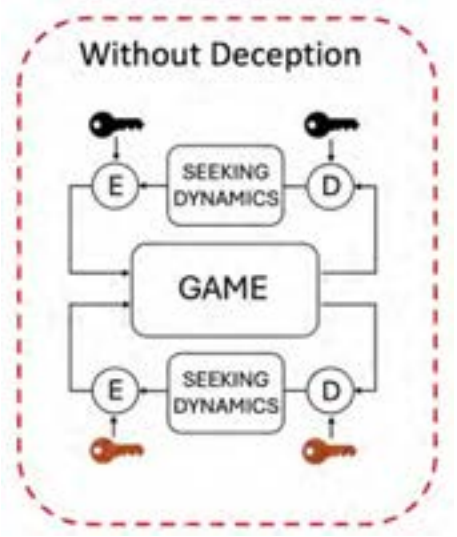
$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t)}_{\text{Exploration}}$$

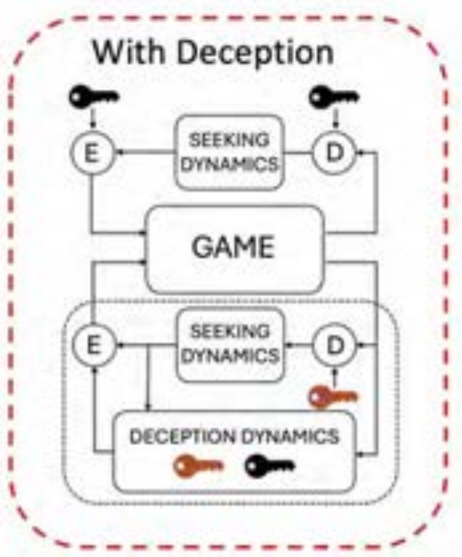
$$\underbrace{\dot{u}_2 = -\frac{2k}{a}J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t) + \delta\sin(\omega_1 t)}_{\text{Exploration with Deception}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a}J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

How to achieve this?

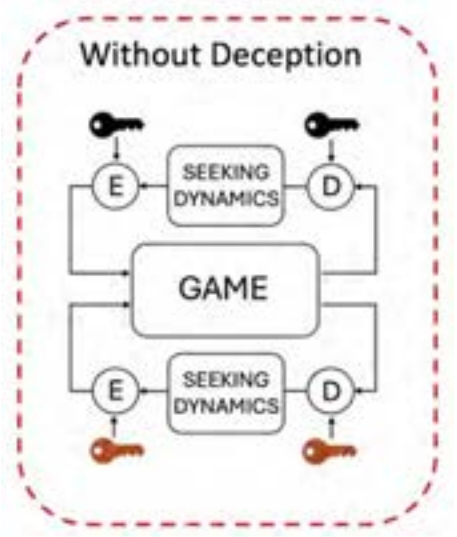


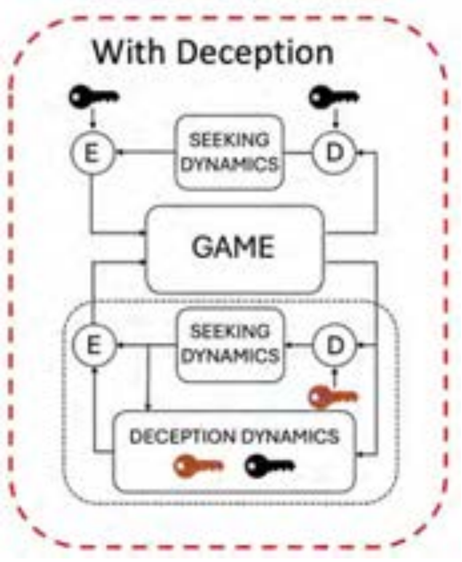


$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t) + \delta\sin(\omega_1 t)}_{\text{Dynamic Exploration with Deception}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

How to achieve this?



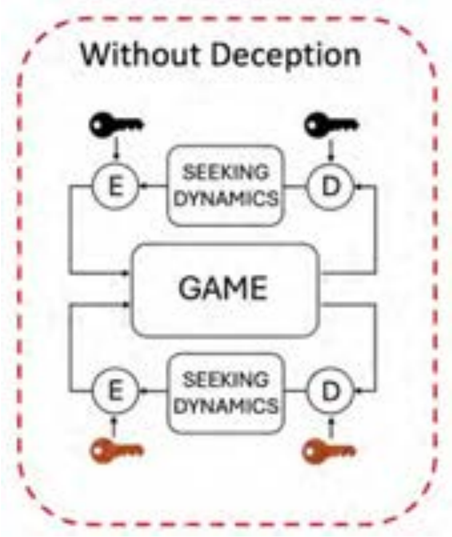


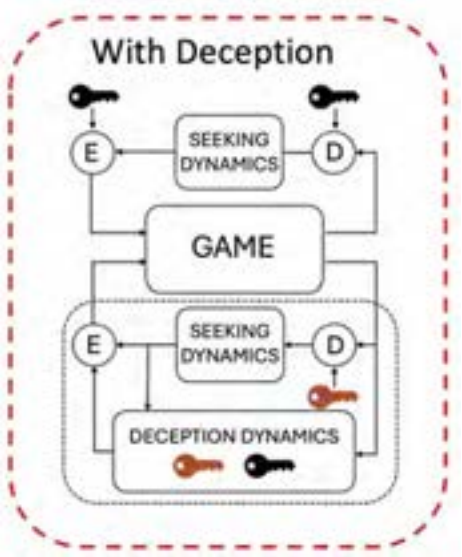
$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t) + \delta\sin(\omega_1 t)}_{\text{Dynamic Exploration with Deception}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$\dot{\delta}_2 = \varepsilon F_2(\eta_2, J_2, u_2)$$

How to achieve this?





$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t)}_{\text{Exploration}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

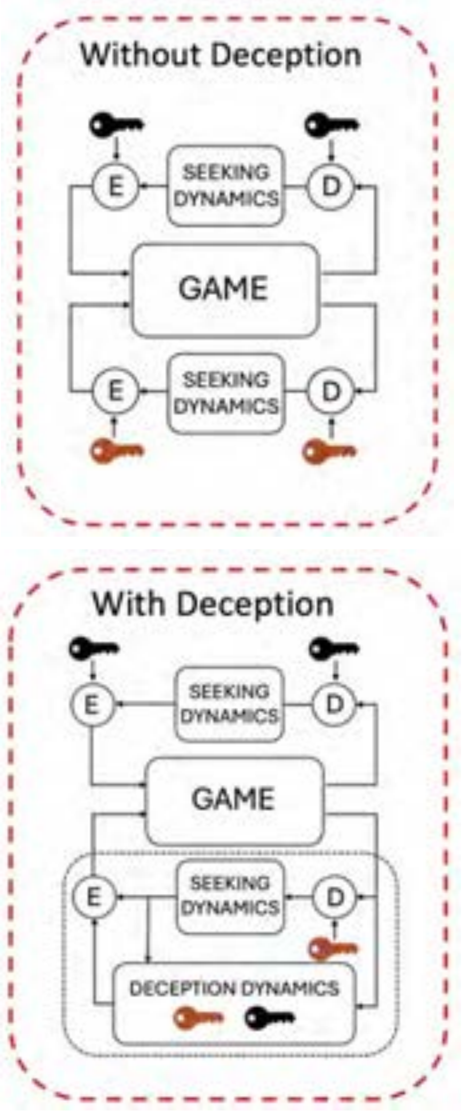
$$x_2 = u_2 + \underbrace{a\sin(\omega_2 t) + \delta \sin(\omega_1 t)}_{\text{Dynamic Exploration with Deception}}$$

$$\underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x)\sin(\omega_2 t)}_{\text{Exploitation}}$$

$$\dot{\delta}_2 = \varepsilon F_2(\eta_2, J_2, u_2)$$

Key idea: close the loop (slowly) to control the RC learned by the victim's algorithm

How to achieve this?



$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

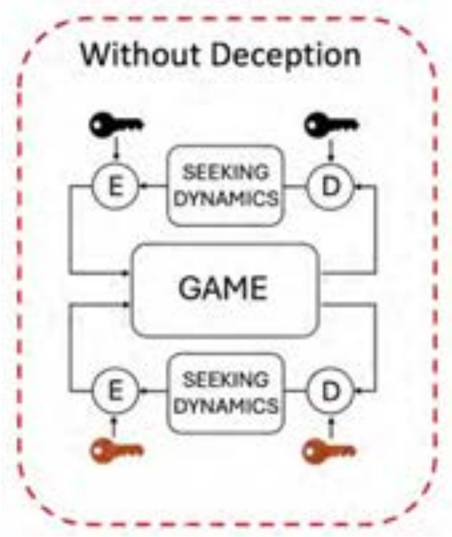
$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t) + \delta \sin(\omega_1 t)}_{\text{Dynamic Exploration with Deception}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

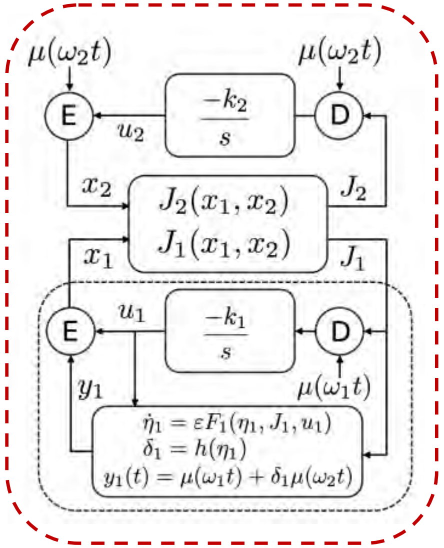
$$\dot{\delta}_2 = \varepsilon F_2(\eta_2, J_2, u_2)$$

Key idea: close the loop (slowly) to control the RC learned by the victim's algorithm

Example: $\dot{\delta}_2 = \varepsilon(J_2(x) - J_2^{\text{ref}})$ ← Desired reference payoff by the deceiver

How to achieve this?





$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t)}_{\text{Exploration}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

$$x_2 = u_2 + \underbrace{a \sin(\omega_2 t) + \delta \sin(\omega_1 t)}_{\text{Dynamic Exploration with Deception}} \qquad \underbrace{\dot{u}_2 = -\frac{2k}{a} J_2(x) \sin(\omega_2 t)}_{\text{Exploitation}}$$

$$\dot{\delta}_2 = \varepsilon F_2(\eta_2, J_2, u_2)$$

Key idea: close the loop (slowly) to control the RC learned by the victim's algorithm

Example: $\dot{\delta}_2 = \varepsilon(J_2(x) - J_2^{\text{ref}})$

Desired reference payoff by the deceiver

How to achieve this?

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t) \sum_{j=1}^{n} \mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i\big(\eta_i(t), J_i(x(t)), u_i(t)\big), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n}\mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i\big(\eta_i(t), J_i(x(t)), u_i(t)\big), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

It can be shown that the dynamics of the players approximately behave as:

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n} \mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i\big(\eta_i(t), J_i(x(t)), u_i(t)\big), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

It can be shown that the dynamics of the players approximately behave as:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n}\mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i(\eta_i(t), J_i(x(t)), u_i(t)), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

It can be shown that the dynamics of the players approximately behave as:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

→ For the "oblivious" players (victims)

→ For the "deceptive" players (attackers)

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n}\mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i(\eta_i(t), J_i(x(t)), u_i(t)), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

It can be shown that the dynamics of the players approximately behave as:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

→ For the "oblivious" players (victims)

→ For the "deceptive" players (attackers)

In words: deceptive players are able to dynamically inject **their externalities** into the best-response curves of the victims

How to achieve this?

Synthesis and analysis of general (deterministic) deception algorithms:

Dynamic Exploitation Policy:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$

Can be seen as the continuous-time limit of a "model-free" pseudo-gradient flow

Dynamic Exploration Policy:

$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n} \mu(\omega_{i_j} t)\Big),$$

$$\dot{\eta}_i(t) = \varepsilon F_i(\eta_i(t), J_i(x(t)), u_i(t)), \quad \varepsilon > 0.$$

$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

It can be shown that the dynamics of the players approximately behave as:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

→ For the "oblivious" players (victims)

→ For the "deceptive" players (attackers)

In words: deceptive players are able to dynamically inject **their externalities** into the best-response curves of the victims

M. Tang, U. Javed, X. Chen, M. Krstic, J. I. Poveda, "*Deception in Nash Equilibrium Seeking*", arXiv:2407.05168, 2024.

Some mathematical tools and results (for ODEs)

Algorithms of interest:

$$
\begin{aligned}
\dot{u}_i(t) &= -\tilde{k}J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,\\
x_i(t) &= u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n}\mu(\omega_{i_j} t)\Big),\\
\dot{\eta}_i(t) &= \varepsilon F_i\big(\eta_i(t), J_i(x(t)), u_i(t)\big), \quad \varepsilon > 0.\\
\delta_i(t) &= h_i(\eta_i(t), x_i(t)),
\end{aligned}
$$

Main results:

- Geometric characterization of **new reaction curves**: rotations, translations, etc
- Conditions for **local exponential stability** of the **deceptive Nash equilibria**
- Conditions for **attainability** of a desired reference payoff
- **Tuning guidelines** for deception algorithms and implications on basins of attraction

Averaging Theory for ODEs

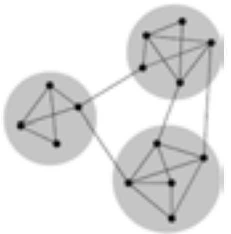
+

Perturbation-based Analysis

Approximate model of induced behavior:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

Convergence results depend on:



- **graph structure** describing interactions between players
- **structure of cost functions:** quadratic, strongly monotone, aggregative, etc
- how "**aggressive"** is the deceiver:

$$\dot{\delta}_2 = \varepsilon\big(J_2(x) - J_2^{\mathrm{ref}}\big)$$

- how "**sensitive"** is the victim

M. Tang, U. Javed, X. Chen, M. Krstic, J. I. Poveda, "*Deception in Nash Equilibrium Seeking*", arXiv:2407.05168, 2024.

Some mathematical tools and results (for ODEs)

Algorithms of interest:

$$\dot{u}_i(t) = -\tilde{k} J_i(x(t))\mu(\omega_i t), \qquad \eta > 0,$$
$$x_i(t) = u_i(t) + a\Big(\mu(\omega_i t) + \delta_i(t)\sum_{j=1}^{n}\mu(\omega_{i_j} t)\Big),$$
$$\dot{\eta}_i(t) = \varepsilon F_i\big(\eta_i(t), J_i(x(t)), u_i(t)\big), \quad \varepsilon > 0.$$
$$\delta_i(t) = h_i(\eta_i(t), x_i(t)),$$

Main results:

- Geometric characterization of **new reaction curves**: rotations, translations, etc
- Conditions for **local exponential stability** of the **deceptive Nash equilibria**
- Conditions for **attainability** of a desired reference payoff
- **Tuning guidelines** for deception algorithms and implications on basins of attraction

Averaging Theory for ODEs

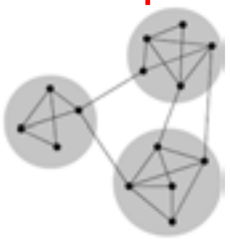
\+

Perturbation-based Analysis

Approximate model of induced behavior:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

Convergence results depend on:



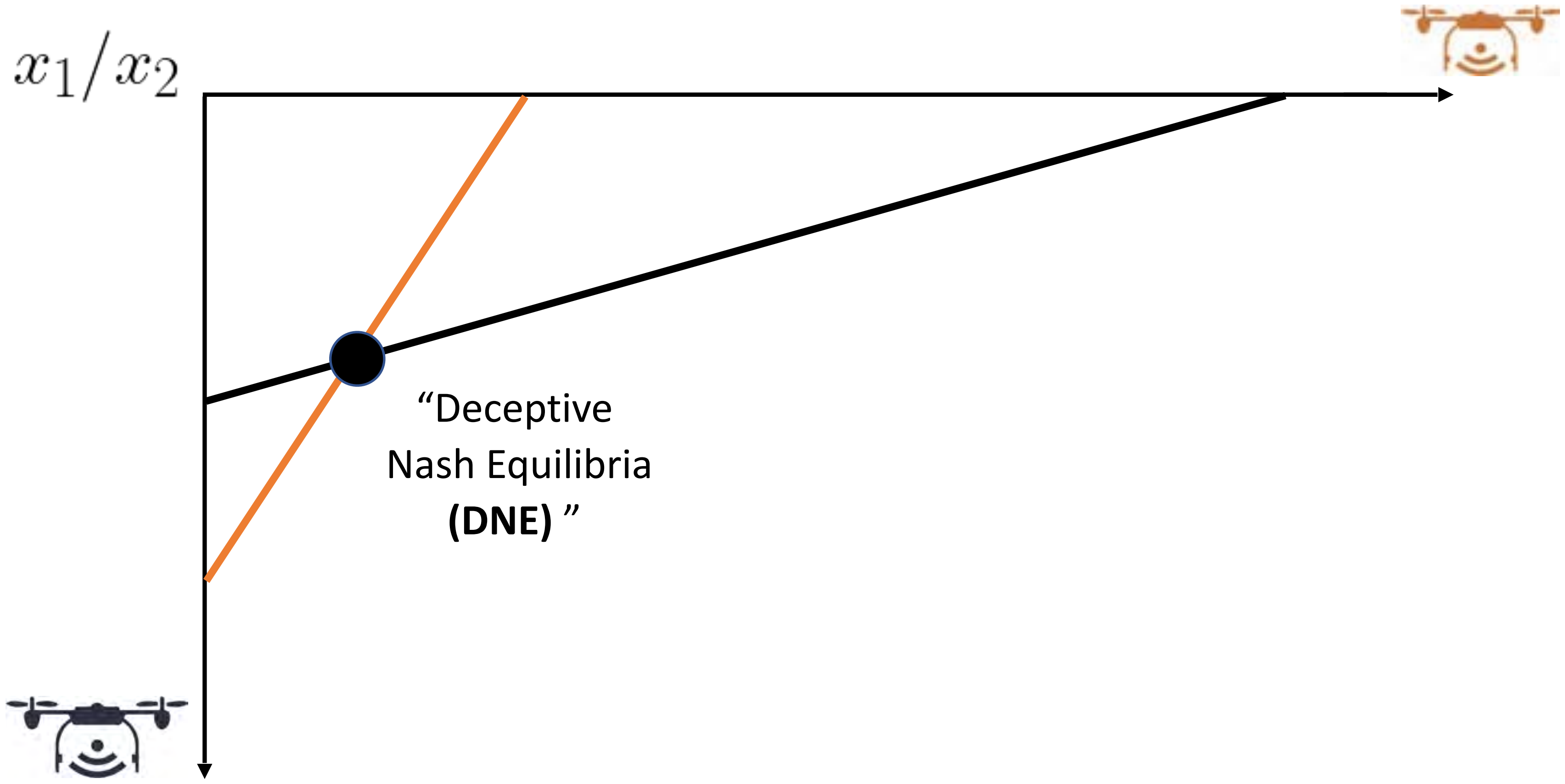
- **graph structure** describing interactions between players
- **structure of cost functions:** quadratic, strongly monotone, aggregative, etc
- how "**aggressive"** is the deceiver:

$$\dot{\delta}_2 = \varepsilon\big(J_2(x) - J_2^{\mathrm{ref}}\big)$$

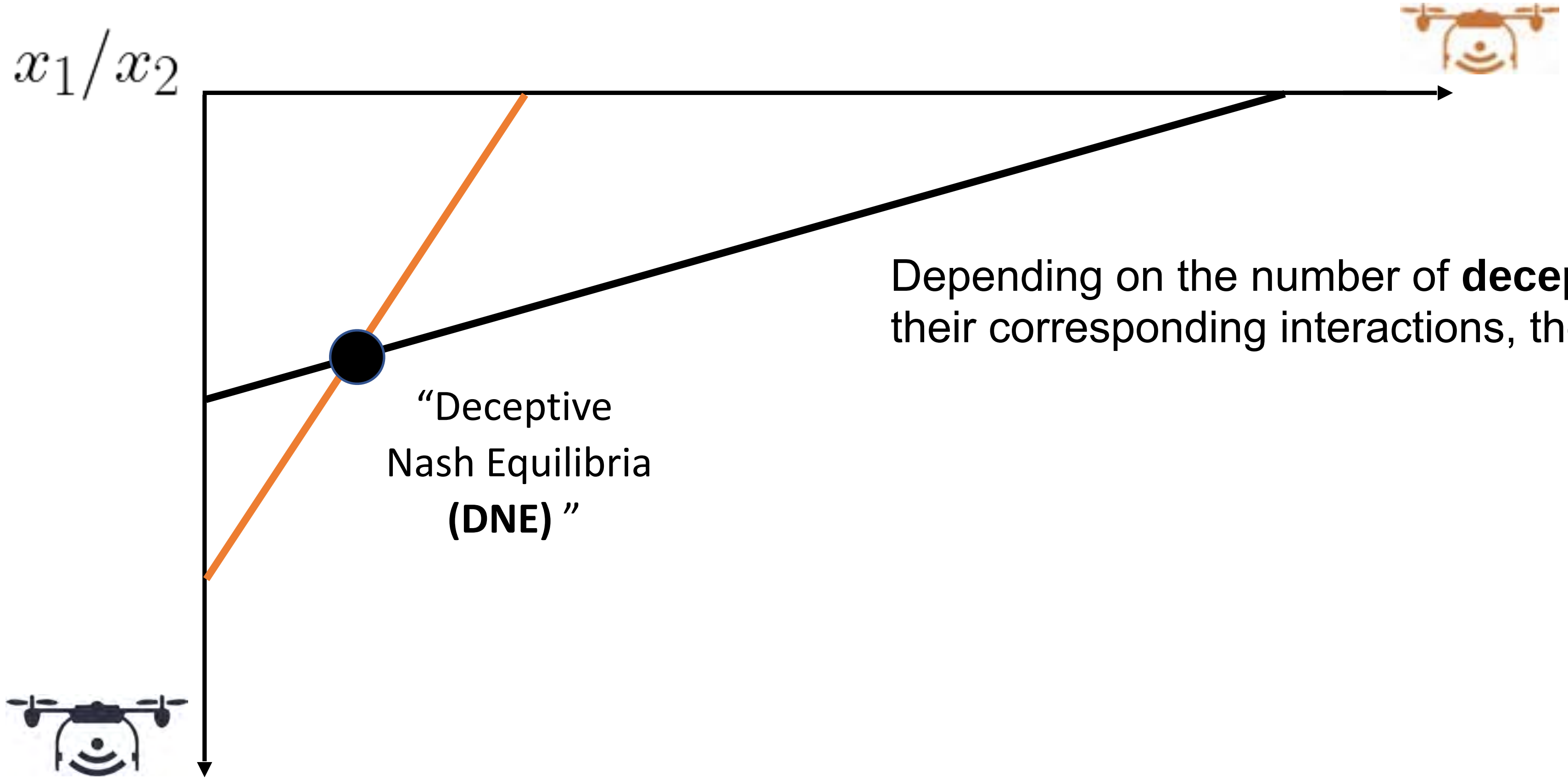
- how "**sensitive"** is the victim

M. Tang, U. Javed, X. Chen, M. Krstic, J. I. Poveda, "*Deception in Nash Equilibrium Seeking*", arXiv:2407.05168, 2024.

Some mathematical tools and results (for ODEs)

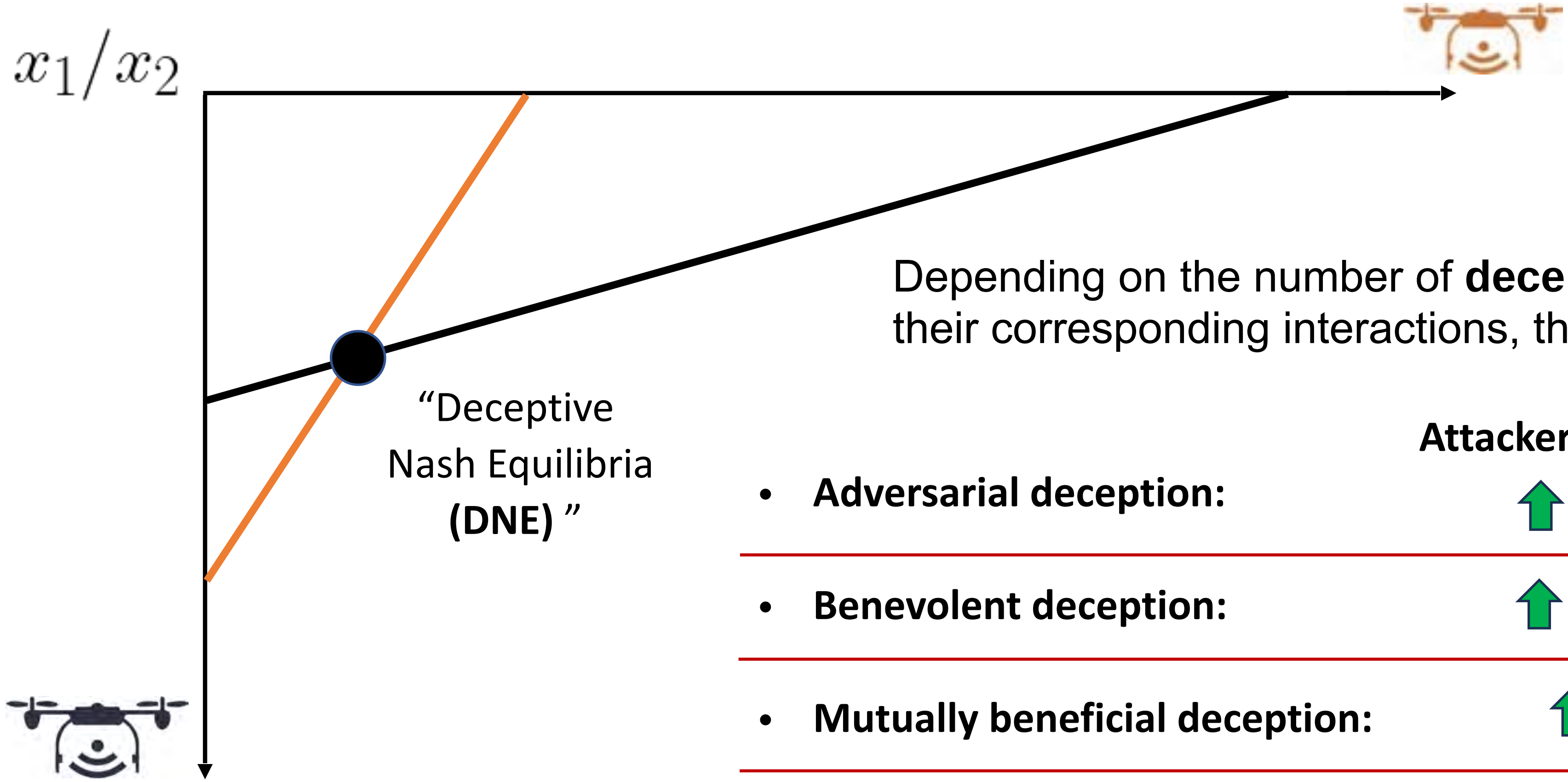


Some mathematical tools and results (for ODEs)



Depending on the number of **deceptive/oblivious** players and their corresponding interactions, the **DNE** can lead to:

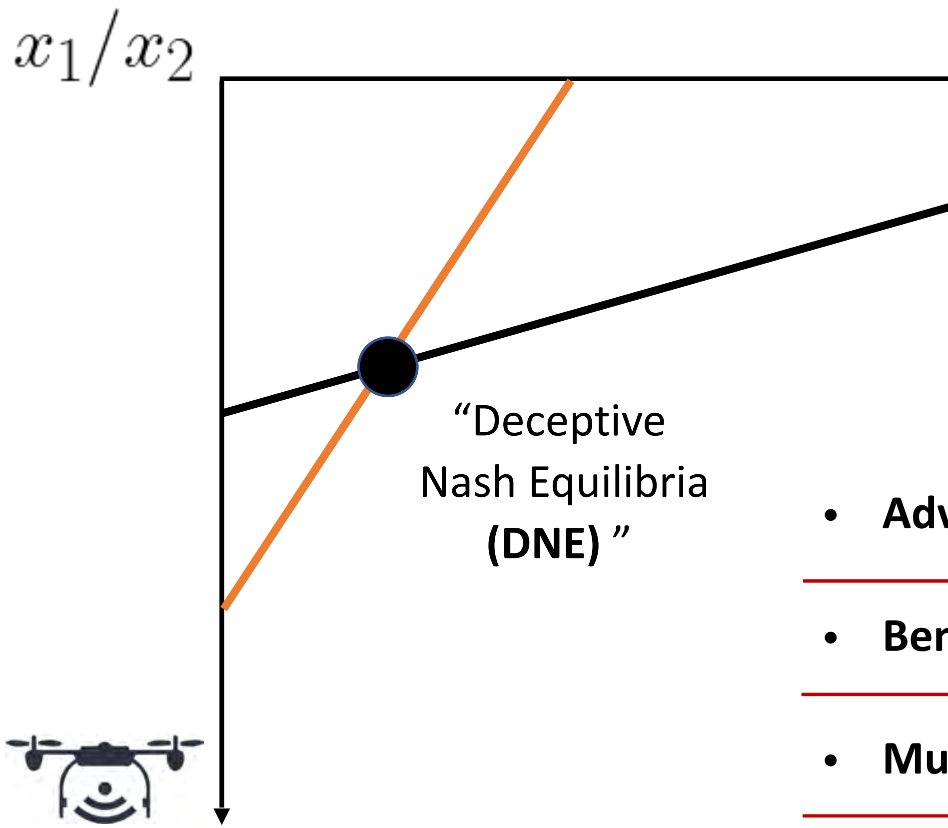
Some mathematical tools and results (for ODEs)



Depending on the number of **deceptive/oblivious** players and their corresponding interactions, the **DNE** can lead to:

	Attacker’s payoff	Victims' payoff
• **Adversarial deception:**	↑ ↓	↓
• **Benevolent deception:**	↑ ↓	↑
• **Mutually beneficial deception:**	↑	↑
• **Mutually adversarial deception:**	↓	↓
• **Immunity to deception:**	unaffected	unaffected

Some mathematical tools and results (for ODEs)

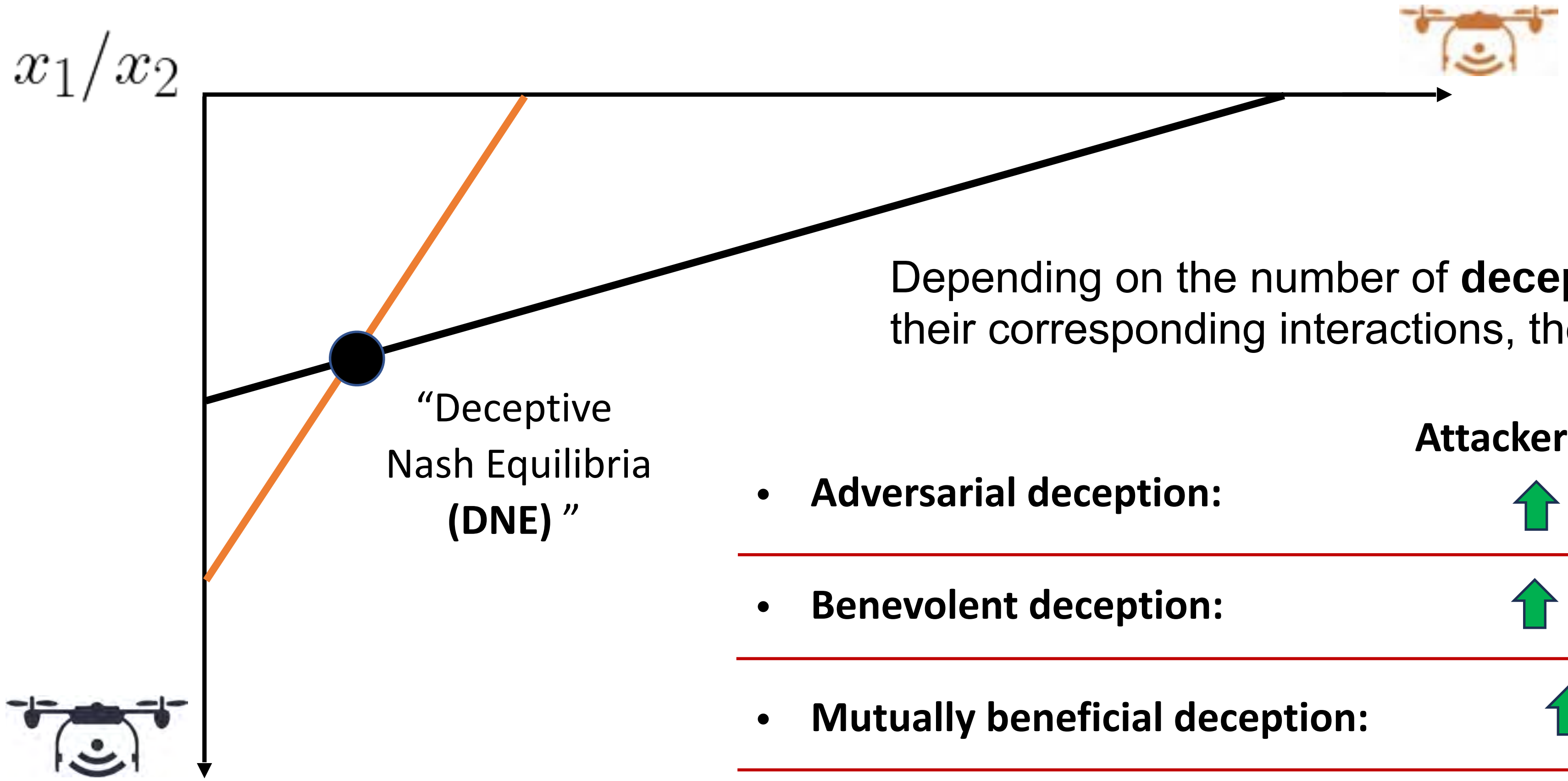


Depending on the number of **deceptive/oblivious** players and their corresponding interactions, the **DNE** can lead to:

	Attacker's payoff	Victims' payoff
• **Adversarial deception:**	↑ ↓	↓
• **Benevolent deception:**	↑ ↓	↑
• **Mutually beneficial deception:**	↑	↑
• **Mutually adversarial deception:**	↓	↓
• **Immunity to deception:**	unaffected	unaffected

(static) defense mechanisms ←

Some mathematical tools and results (for ODEs)



Depending on the number of **deceptive/oblivious** players and their corresponding interactions, the **DNE** can lead to:

	Attacker's payoff	**Victims' payoff**
• **Adversarial deception:**	↑ ↓	↓
• **Benevolent deception:**	↑ ↓	↑
• **Mutually beneficial deception:**	↑	↑
• **Mutually adversarial deception:**	↓	↓
• **Immunity to deception:**	unaffected	unaffected

(static) defense mechanisms ←

K. Vamvoudakis, F. Fotiadis, T. Başar, V. Gupta, J. I. Poveda, M. Tang, M. Krstic, Q. Zhu, "*Deception in Game Theory and Control: A Tutorial*", American Control Conference, to appear, 2025.

Stochastic Deception in Noncooperative Games

- adaptive/learning-based algorithms in multi-agent systems can also implement **stochastic exploration**

e.g., stochastic approximations, diffusion-based approaches, algo's based on stochastic inclusions, etc

M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.

Stochastic Deception in Noncooperative Games

- adaptive/learning-based algorithms in multi-agent systems can also implement **stochastic exploration**

  e.g., stochastic approximations, diffusion-based approaches, algo's based on stochastic inclusions, etc

- In stochastic settings, we see the **random exploration policy generator** as the **"key"**

M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.

Stochastic Deception in Noncooperative Games

- adaptive/learning-based algorithms in multi-agent systems can also implement **stochastic exploration**

  e.g., stochastic approximations, diffusion-based approaches, algo's based on stochastic inclusions, etc

- In stochastic settings, we see the **random exploration policy generator** as the **"key"**

One possible example of stochastic deception dynamics:

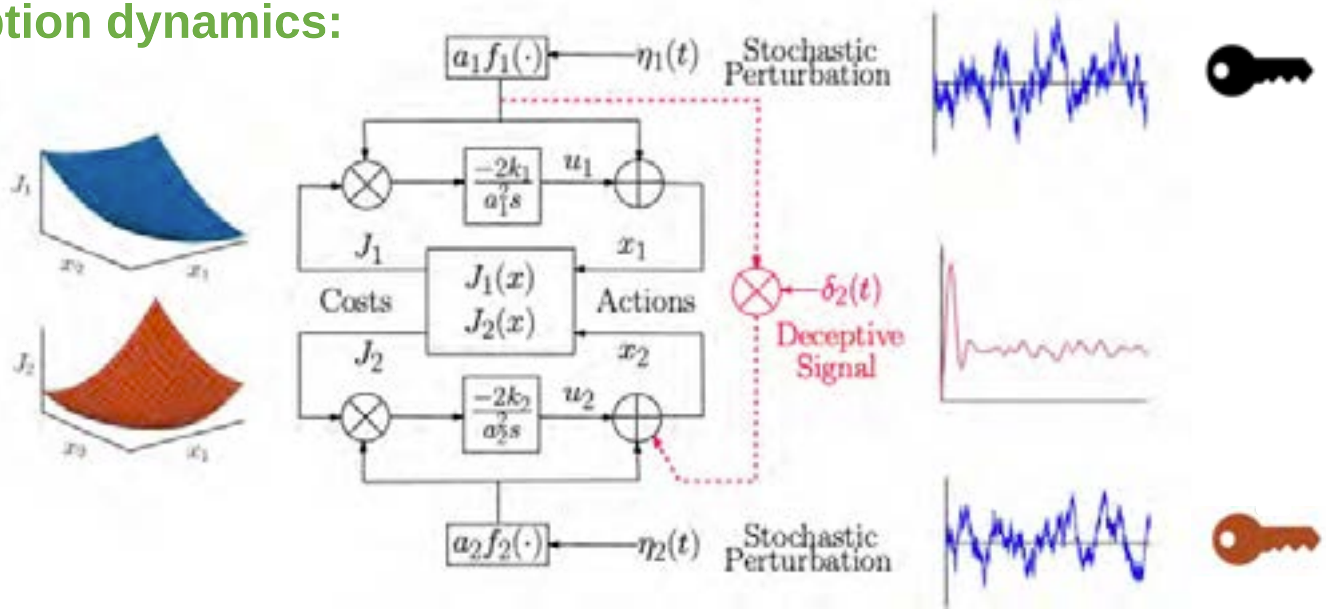
$$x_i(t) = u_i(t) + a_i f_i(\eta_i(t)) + \delta_i \sum_{k \in \mathcal{D}_i} a_k f_k(\eta_k(t))$$

$$\dot{u}_i = -\frac{\gamma_i k_i}{a_i} f_i(\eta_i(t)) J_i(x)$$

$$\gamma_i = \int_{-\infty}^{\infty} f_i^2(s) \frac{1}{\sqrt{\pi} q_i} e^{-\frac{s^2}{q_i^2}} ds$$

$$\vartheta_i d\eta_i(t) = -\eta_i(t)dt + \sqrt{\vartheta_i q_i} dW_i(t)$$

Ornstein-Uhlenbeck (OU) process



M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.

Stochastic Deception in Noncooperative Games

- adaptive/learning-based algorithms in multi-agent systems can also implement **stochastic exploration**

  e.g., stochastic approximations, diffusion-based approaches, algo’s based on stochastic inclusions, etc

- In stochastic settings, we see the **random exploration policy generator** as the **“key”**

One possible example of stochastic deception dynamics:

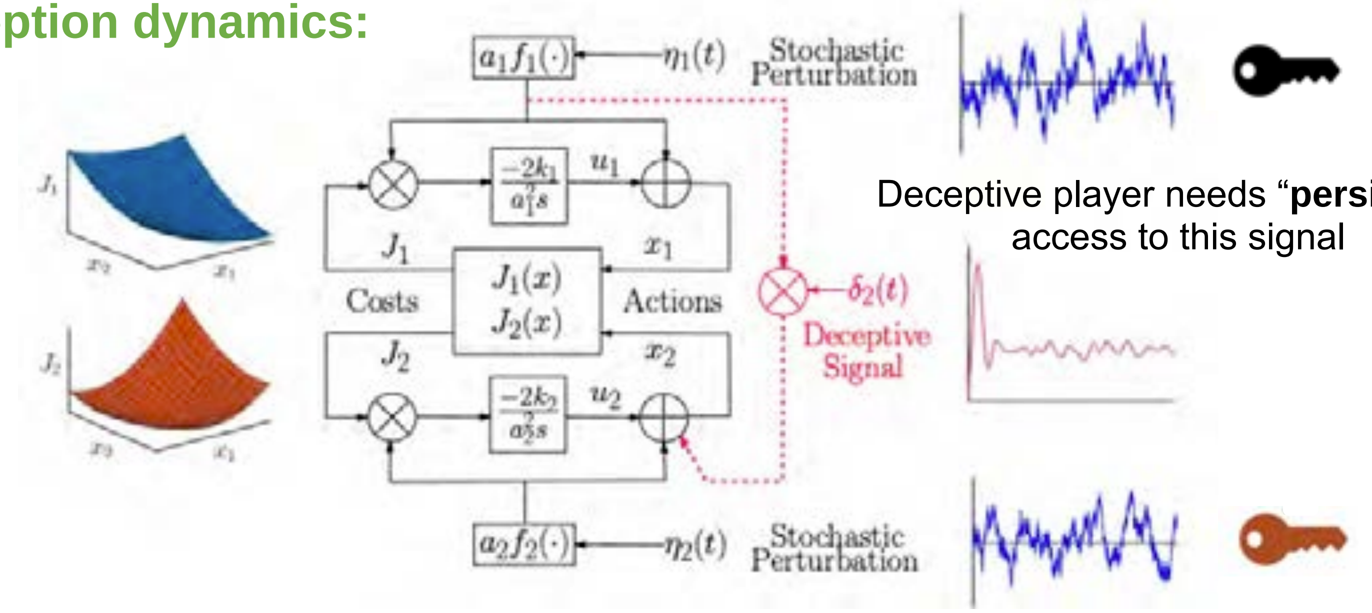
$$x_i(t) = u_i(t) + a_i f_i(\eta_i(t)) + \delta_i \sum_{k \in \mathcal{D}_i} a_k f_k(\eta_k(t))$$

$$\dot{u}_i = -\frac{\gamma_i k_i}{a_i} f_i(\eta_i(t)) J_i(x)$$

$$\gamma_i = \int_{-\infty}^{\infty} f_i^2(s) \frac{1}{\sqrt{\pi} q_i} e^{-\frac{s^2}{q_i^2}} ds$$

$$\vartheta_i d\eta_i(t) = -\eta_i(t)dt + \sqrt{\vartheta_i q_i} dW_i(t)$$

Ornstein-Uhlenbeck (OU) process



Deceptive player needs “**persistent**” access to this signal

M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.

Stochastic Deception in Noncooperative Games

Probabilistic convergence guarantees for quadratic games: $J_i(x) = \frac{1}{2}x^\top A_i x + b_i^\top x + c_i$

weak stochastic stability:

For any $\tilde{r} > 0$ *and any initial condition* $\zeta_0 \in \mathbb{R}^{N+n}$ *with* $|\zeta_0 - \zeta^*| < R$*, the solution satisfies*

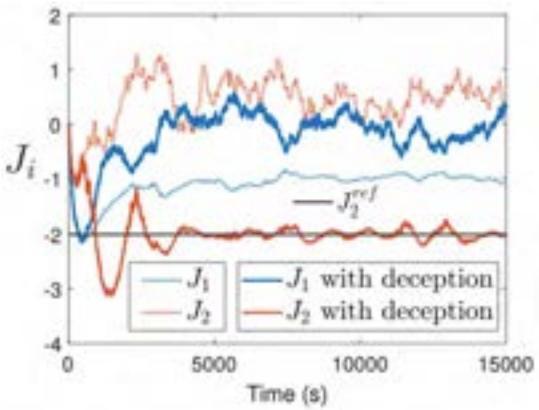
$$\lim_{\vartheta \to 0} \inf\{t \geq 0 : |\zeta(t) - \zeta^*| > C|\zeta_0 - \zeta^*|e^{-Mt} + \tilde{r}\} = \infty \quad a.s.$$

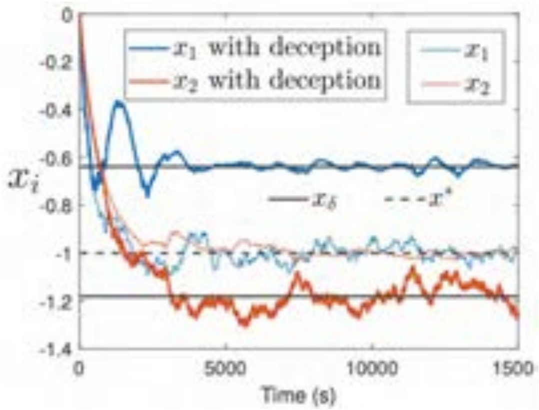
There exists $\varepsilon_0 > 0$ *and a function* $T : (0, \varepsilon_0) \to \mathbb{N}$ *such that*

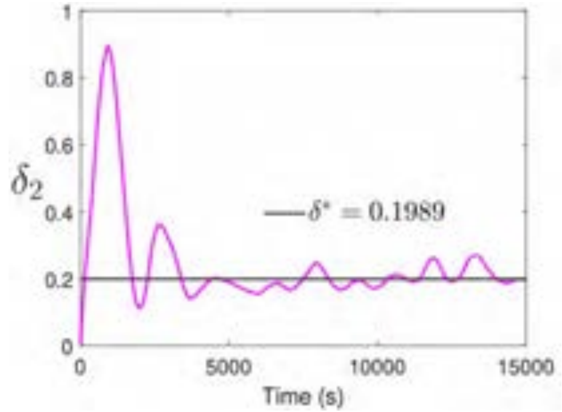
$$\lim_{\vartheta \to 0} P(|\zeta(t) - \zeta^*| \leq C|\zeta_0 - \zeta^*|e^{-Mt} + \tilde{r} \quad \forall t \in [0, T(\vartheta)]) = 1 \quad \textit{with} \lim_{\vartheta \to 0} T(\vartheta) = \infty.$$

attainability of desired payoff:

$|J_{d_k}(u^*) - J_{d_k}^{ref}| < \tilde{\varepsilon}$ *for all* $k \in [n]$







Some mathematical tools and results (for SDEs)

Stochastic algorithms of interest:

$$x_i(t) = u_i(t) + a_i f_i(\eta_i(t)) + \delta_i \sum_{k\in\mathcal{D}_i} a_k f_k(\eta_k(t))$$

$$\dot{u}_i = -\frac{\gamma_i k_i}{a_i} f_i(\eta_i(t)) J_i(x)$$

$$\gamma_i = \int_{-\infty}^{\infty} f_i^2(s) \frac{1}{\sqrt{\pi} q_i} e^{-\frac{s^2}{q_i^2}} ds$$

$$\vartheta_i d\eta_i(t) = -\eta_i(t)dt + \sqrt{\vartheta_i q_i} dW_i(t)$$

Main results:

- Geometric characterization of **new reaction curves**: rotations, translations, etc
- Conditions for weak stochastic convergence to **deceptive Nash equilibria**
- Conditions for **attainability** of a desired reference payoff
- **Tuning guidelines** for deception algorithms and implications on basins of attraction

Stochastic Averaging Theory for SDEs

\+

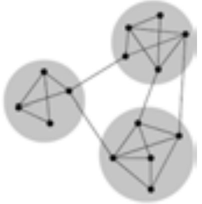
Perturbation-based Analysis

Approximate model of induced behavior:

$$\dot{\tilde{u}}_i = \nabla_i \tilde{J}_i(\tilde{u}) = \begin{cases} \nabla_i J_i(\tilde{u}) + \sum_{k\in\mathcal{K}_i} \delta_k \nabla_k J_i(\tilde{u}) \\ \nabla_i J_i(\tilde{u}) \end{cases}$$

(Weak) Stochastic Stability depends on:

- **Graph structure** describing interactions between players



- **Structure of cost functions:** quadratic
- how "**aggressive"** is the deceiver:

$$\dot{\delta}_2 = \varepsilon(J_2(x) - J_2^{\text{ref}})$$

- how "**sensitive"** are the victims

M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \left\{ \begin{array}{c} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{array} \right.$$

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{cases}$$

Simultaneous perturbations

(can be relaxed)

$$u_a := u + I(\delta_p) I(q) v \qquad u_b := u - I(\delta_m) I(q) v$$

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{cases}$$

$$u_a := u + I(\delta_p)I(q)v \qquad u_b := u - I(\delta_m)I(q)v$$

Simultaneous perturbations

(can be relaxed)

Random exploration directions

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{cases}$$

Simultaneous perturbations

(can be relaxed)

$$u_a := u + I(\delta_p) I(q) v \qquad u_b := u - I(\delta_m) I(q) v$$

Random exploration directions

Deception can be enabled by two different mechanisms:

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i (J(u_a) - J(u_b)) \end{cases}$$

Simultaneous perturbations

(can be relaxed)

$$u_a := u + I(\delta_p) I(q) v \qquad u_b := u - I(\delta_m) I(q) v$$

Random exploration directions

Deception can be enabled by two different mechanisms:

- **Interfere with learning via the design of correlated stochastic exploration signals**: Deceivers design their random proving such that correlation with other players is non-zero (similar as previous schemes, key properties of external random probing signals can still be “extracted” in certain cases (Krieger & Krstic, 2011))

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{cases}$$

$$u_a := u + I(\delta_p) I(q) v \qquad u_b := u - I(\delta_m) I(q) v$$

Simultaneous perturbations

(can be relaxed)

Random exploration directions

Deception can be enabled by two different mechanisms:

- **Interfere with learning via the design of correlated stochastic exploration signals**: Deceivers design their random proving such that correlation with other players is non-zero (similar as previous schemes, key properties of external random probing signals can still be "extracted" in certain cases (Krieger & Krstic, 2011))

- **Anticipatory behaviors (non-causal):** deceivers have access to the realization of the victim's random variable in order to modify their exploration in real-time (exploits the fact that sufficient Lyapunov conditions for stability in stochastic difference inclusions fail under lack of causality)

Stochastic Deception Algorithms for Noncooperative Games

Deception can also be induced in discrete-time algorithms based on stochastic approximations:

$$x_i^+ \in G_{\delta,i}(x_i, v^+) := \begin{cases} \{0,1\} \\ (1-q_i)(\ell_i + 1 - \rho) + q_i \max\{0, \ell_i - \rho\} \\ u_i + \delta_{s,i} q_i v_i \left(J(u_a) - J(u_b)\right) \end{cases}$$

$$u_a := u + I(\delta_p)I(q)v \qquad u_b := u - I(\delta_m)I(q)v$$

Simultaneous perturbations

(can be relaxed)

Random exploration directions

Deception can be enabled by two different mechanisms:

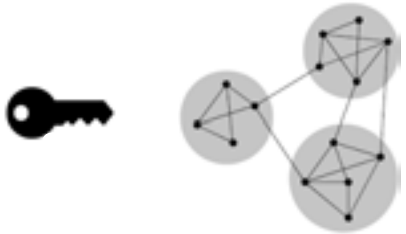
- **Interfere with learning via the design of correlated stochastic exploration signals**: Deceivers design their random proving such that correlation with other players is non-zero (similar as previous schemes, key properties of external random probing signals can still be "extracted" in certain cases (Krieger & Krstic, 2011))

- **Anticipatory behaviors (non-causal):** deceivers have access to the realization of the victim's random variable in order to modify their exploration in real-time (exploits the fact that sufficient Lyapunov conditions for stability in stochastic difference inclusions fail under lack of causality)

Poveda, Nesic, Teel, "Flexible Nash seeking using stochastic difference inclusions", American Control Conference, 2015

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**

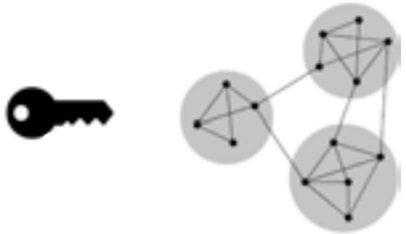


$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**



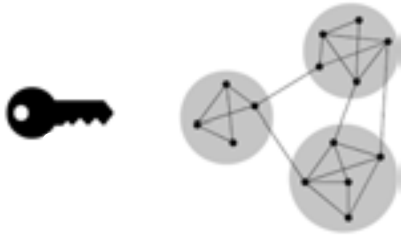
$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

- **Continuous-time dynamics** provide suitable qualitative models of algorithmic analysis before discretizing

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**



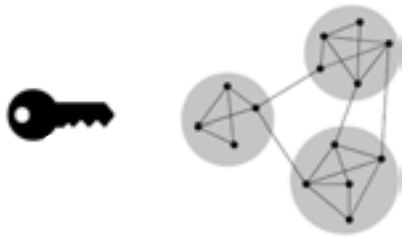
$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

- **Continuous-time dynamics** provide suitable qualitative models of algorithmic analysis before discretizing
- **Discrete-time dynamics** allow us to incorporate "**if-then**" rules in our algorithms, e.g.,
  - switching between multiple algorithms in real-time
  - resets implemented by the algorithms
  - stochastic events triggered by uncertain environments, switching network topologies for defense, etc

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**



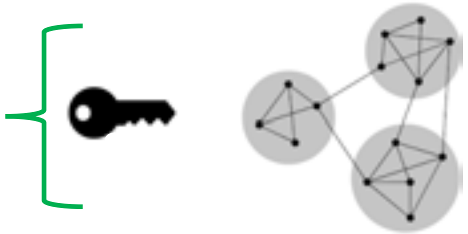
$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

- **Continuous-time dynamics** provide suitable qualitative models of algorithmic analysis before discretizing
- **Discrete-time dynamics** allow us to incorporate "**if-then**" rules in our algorithms, e.g.,
    - switching between multiple algorithms in real-time
    - resets implemented by the algorithms
    - stochastic events triggered by uncertain environments, switching network topologies for defense, etc
- **Hybrid** approaches allow us to:
    - "achieve more" when it comes to "transforming" the **reaction curves** of the oblivious players
    - open the door to other mechanisms to exploit privileged information
    - establish rigorous stability and convergence guarantees via control-theoretic tools (Lyapunov functions, invariance properties, etc)

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**



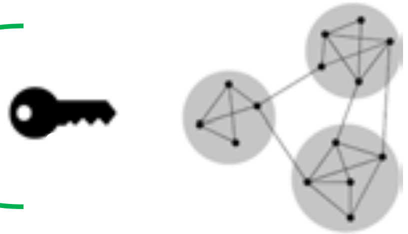
$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

- **Continuous-time dynamics** provide suitable qualitative models of algorithmic analysis before discretizing
- **Discrete-time dynamics** allow us to incorporate "**if-then**" rules in our algorithms, e.g.,
  - switching between multiple algorithms in real-time
  - resets implemented by the algorithms
  - stochastic events triggered by uncertain environments, switching network topologies for defense, etc
- **Hybrid** approaches allow us to:
  - "achieve more" when it comes to "transforming" the **reaction curves** of the oblivious players
  - open the door to other mechanisms to exploit privileged information
  - establish rigorous stability and convergence guarantees via control-theoretic tools (Lyapunov functions, invariance properties, etc)

Stochastic Deception Algorithms for Games

Our current work aims for more general models of deception dynamics: **Stochastic + Hybrid**



$$dx \in F(x)dt + B(x)dw, \quad x \in C$$

$$x^+ \in G(x, v^+), \quad v \sim \mu(\cdot) \quad x \in D$$

- **Continuous-time dynamics** provide suitable qualitative models of algorithmic analysis before discretizing
- **Discrete-time dynamics** allow us to incorporate "**if-then**" rules in our algorithms, e.g.,
  - switching between multiple algorithms in real-time
  - resets implemented by the algorithms
  - stochastic events triggered by uncertain environments, switching network topologies for defense, etc
- **Hybrid** approaches allow us to:
  - "achieve more" when it comes to "transforming" the **reaction curves** of the oblivious players
  - open the door to other mechanisms to exploit privileged information
  - establish rigorous stability and convergence guarantees via control-theoretic tools (Lyapunov functions, invariance properties, etc)

Abdelgalil, Ochoa, Poveda, "Multi-time scale control and optimization via averaging and singular perturbation theory: From ODEs to Hybrid Dynamical Systems", Annual Reviews in Control, 2024
Poveda, Benosman, Teel, "Hybrid online learning control in networked multiagent systems: A survey", International Journal of Adaptive Control and Signal Processing, 2019.

Stochastic Deception in Noncooperative Games

Some related references:

- M. Tang, U. Javed, X. Chen, M. Krstic, J. I. Poveda, "*Deception in Nash Equilibrium Seeking*", Arxiv, 2024.
- M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.
- M. Tang, M. Krstic, J. I. Poveda, "Deception in Oligopoly Games via Adaptive Nash Seeking Systems", 13th International Conference on Game Theory for Networks, Cambridge, UK, 2025, to appear.
- Poveda, Nesic, Teel, "Flexible Nash seeking using stochastic difference inclusions", American Control Conference, 2015
- K. Vamvoudakis, F. Fotiadis, T. Başar, V. Gupta, J. I. Poveda, M. Tang, M. Krstic, Q. Zhu, "***Deception in Game Theory and Control: A Tutorial***", American Control Conference, to appear, 2025.
- M. Abdelgalil, J. I. Poveda, "*On Lie-Bracket Averaging for a Class of Hybrid Dynamical Systems with Applications to Model-Free Control and Optimization*", IEEE Transactions on Automatic Control, 2025.
- F. Galarza-Jimenez, J. I. Poveda, G. Bianchin, E. Dall'Anese, "*Extremum Seeking Under Persistent Gradient Deception: A Switching Systems Approach*", IEEE Control Systems Letters, Vol. 6, pp. 133-138, 2021.

Michael Tang
UCSD

Stochastic Deception in Noncooperative Games

Some related references:

- M. Tang, U. Javed, X. Chen, M. Krstic, J. I. Poveda, "*Deception in Nash Equilibrium Seeking*", Arxiv, 2024.
- M. Tang, M. Krstic, J. I. Poveda, "*Stochastic Real-Time Deception in Nash Equilibrium Seeking for Games with Quadratic Payoffs*", 7th Learning for Dynamics and Control Conference, 2025, to appear.
- M. Tang, M. Krstic, J. I. Poveda, "Deception in Oligopoly Games via Adaptive Nash Seeking Systems", 13th International Conference on Game Theory for Networks, Cambridge, UK, 2025, to appear.
- Poveda, Nesic, Teel, "Flexible Nash seeking using stochastic difference inclusions", American Control Conference, 2015
- K. Vamvoudakis, F. Fotiadis, T. Başar, V. Gupta, J. I. Poveda, M. Tang, M. Krstic, Q. Zhu, "***Deception in Game Theory and Control: A Tutorial***", American Control Conference, to appear, 2025.
- M. Abdelgalil, J. I. Poveda, "*On Lie-Bracket Averaging for a Class of Hybrid Dynamical Systems with Applications to Model-Free Control and Optimization*", IEEE Transactions on Automatic Control, 2025.
- F. Galarza-Jimenez, J. I. Poveda, G. Bianchin, E. Dall'Anese, "*Extremum Seeking Under Persistent Gradient Deception: A Switching Systems Approach*", IEEE Control Systems Letters, Vol. 6, pp. 133-138, 2021.

Michael Tang
UCSD

Thank you for your time

poveda@ucsd.edu

Resilience in Infrastructure Systems

Dr. David L. Alderson
Executive Director - Center for Infrastructure Defense
Professor - Operations Research
Naval Postgraduate School (NPS) - Monterey, CA USA

DARPA Workshop

COMPASS: Critical Orientation of Mathematics to Produce Advancements in Science and Security

05 March 2025

Today's Agenda

Act I: Societal Need for Infrastructure Resilience

Act II: (Getting Stuck in) Modeling + Simulation of Lifeline Infrastructure Interactions as a Path to Resilience

Act III: A Need for Different Mathematics (enabled by new science based on patterns)

Acknowledgments: Daniel Eisenberg (NPS) and David Woods (Ohio State)

This work was supported by the Office of Naval Research, the Air Force Office of Scientific Research, the Defense Threat Reduction Agency, and the DOD Strategic Environmental Research and Development Program.

Nouns vs Verbs

Resilience is not about what you have,
it's about what you do!

Question: Are our mathematics too focused on nouns?

Resilience as a verb in the future tense?

See also: Woods, D. D. (2018). "Resilience is a verb." In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

Journal of Economic Behavior and Organization 205 (2023) 638–647

Contents lists available at ScienceDirect

Journal of Economic Behavior and Organization

journal homepage: www.elsevier.com/locate/jebo

Economics in nouns and verbs

W. Brian Arthur[a,b]

[a] Santa Fe Institute, Santa Fe, NM, USA
[b] Intelligent Systems Lab, PARC, Palo Alto, CA, USA

ARTICLE INFO

Article history:
Received 10 June 2022
Revised 11 October 2022
Accepted 25 October 2022
Available online 13 December 2022

JEL classification:
B41 (Economic Methodology)
B59 (Current Heterodox Approaches-Other)
C02 (Mathematical Methods)

Keywords:
Economic theory
Mathematics in economics
Algorithms
Complexity economics
Computational economics

ABSTRACT

Standard economic theory uses mathematics as its main means of understanding, and this brings clarity of reasoning and logical power. But there is a drawback: algebraic mathematics restricts economic modeling to what can be expressed only in quantitative nouns, and this forces theory to leave out matters to do with process, formation, adjustment, and creation—matters to do with nonequilibrium. For these we need a different means of understanding, one that allows verbs as well as nouns. Algorithmic expression is such a means. It allows verbs—processes—as well as nouns—objects and quantities. It allows fuller description in economics, and can include heterogeneity of agents, actions as well as objects, and realistic models of behavior in ill-defined situations. The world that algorithms reveal is action-based as well as object-based, organic, possibly ever-changing, and not fully knowable. But it is strangely and wonderfully alive.

Today's Agenda

Act I: Societal Need for Infrastructure Resilience

Act II: (Getting Stuck in) Modeling + Simulation of Lifeline Infrastructure Interactions as a Path to Resilience

Act III: A Need for Different Mathematics (enabled by new science based on patterns)

Acknowledgments: Daniel Eisenberg (NPS) and David Woods (Ohio State)

This work was supported by the Office of Naval Research, the Air Force Office of Scientific Research, the Defense Threat Reduction Agency, and the DOD Strategic Environmental Research and Development Program.

The study of critical infrastructure systems is not new…

- ***Critical Infrastructure (CI)***: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" ***-- Section 1016(e) of the USA PATRIOT Act of 2001***

Image Source: European Commission Newsletter, "Critical Infrastructure Resilience: News, Updates and Events," https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

The study of critical infrastructure systems is not new…

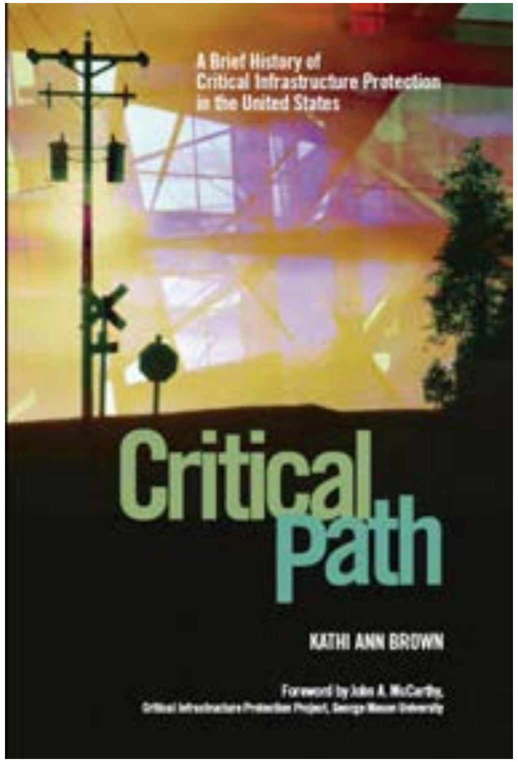
Within the U.S., the development and understanding of critical infrastructure systems was closely tied to war mobilization

- World Wars I & II

1950s-1970s:

- Identification of key assets and facilities (organized as lists)
- Connections to civil defense

Brown, K.A. (2006), Critical Path: A Brief History of Critical Infrastructure Protection in the United States, Fairfax, VA: Spectrum.



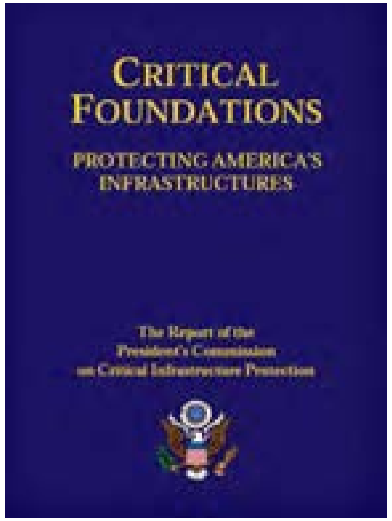
- ***Critical Infrastructure (CI)***: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" ***-- Section 1016(e) of the USA PATRIOT Act of 2001***

Image Source: European Commission Newsletter, "Critical Infrastructure Resilience: News, Updates and Events," https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

The study of critical infrastructure systems is not new…

1997

Drivers



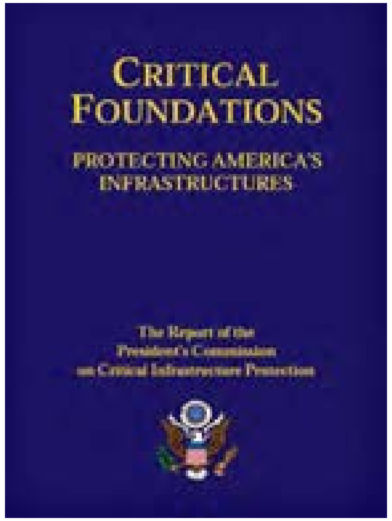
President's Commission on Critical Infrastructure Protection

The study of critical infrastructure systems is not new…

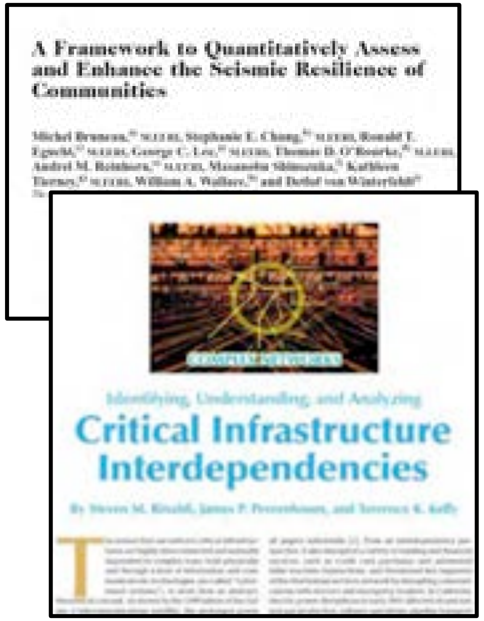
Act I: The US Infrastructure Resilience Renaissance

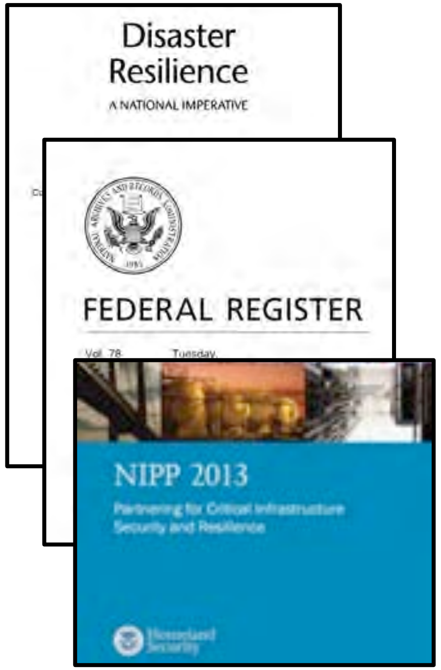
1997 → **2001 – 2005** → **2009 – 2010** → **2012 – 2013**

Drivers | **Theories** | **Frameworks** | **Policies**



President's Commission on Critical Infrastructure Protection





Operations Research has enabled the development of an “optimized world”

Image Source: European Commission Newsletter, “Critical Infrastructure Resilience: News, Updates and Events,” https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

Operations Research has enabled the development of an "optimized world"

increasing complexity

nonlinear behavior

large scale

hidden dependencies

changing tempos of activity

new goals

re-prioritization

accidents

extreme weather

surprise events

failures

attacks

unintended consequences

cascading failures

system collapse

mission failure

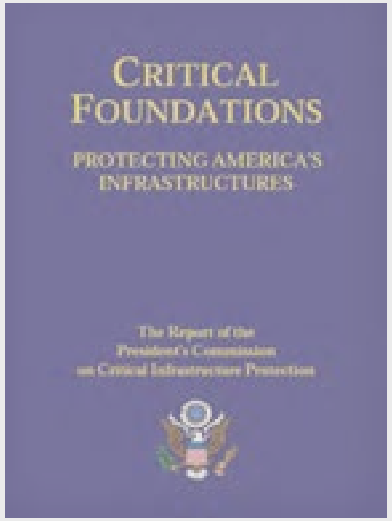
Image Source: European Commission Newsletter, "Critical Infrastructure Resilience: News, Updates and Events," https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

The study of critical infrastructure systems is not new…

Act I: The US Infrastructure Resilience Renaissance

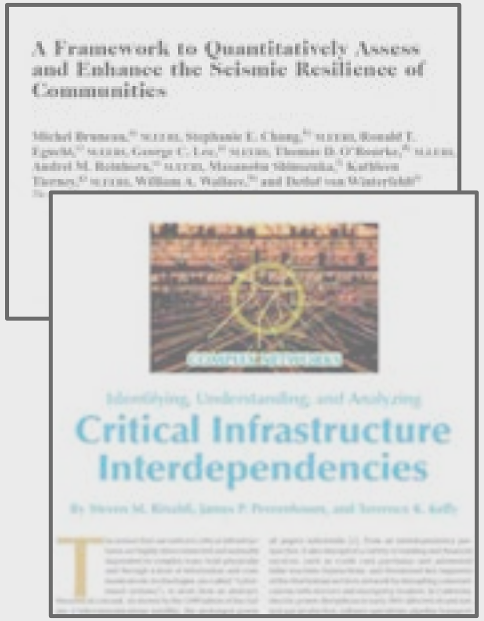
1997 → **2001 – 2005** → **2009 – 2010** → **2012 – 2013**

Drivers



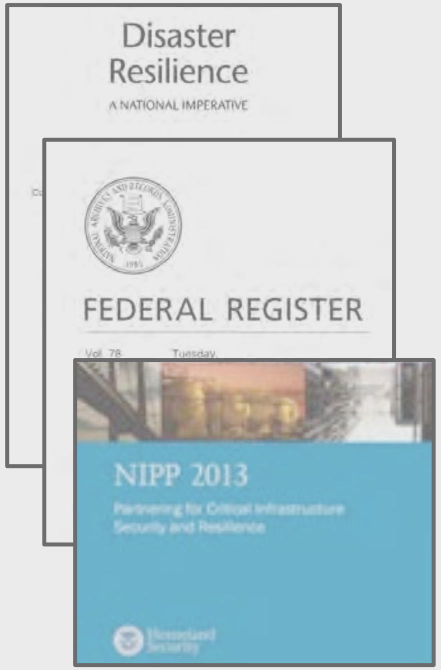
President's Commission on Critical Infrastructure Protection

Theories



Frameworks

Policies



Act II:

→ **2013 – now**

Modeling
+
Simulation

Conferences
Journals
National Funding
Centers of Excellence

Universities
National Laboratories
FFRDCs
Defense Contractors

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

Act II:

2013 – now

Modeling
+
Simulation

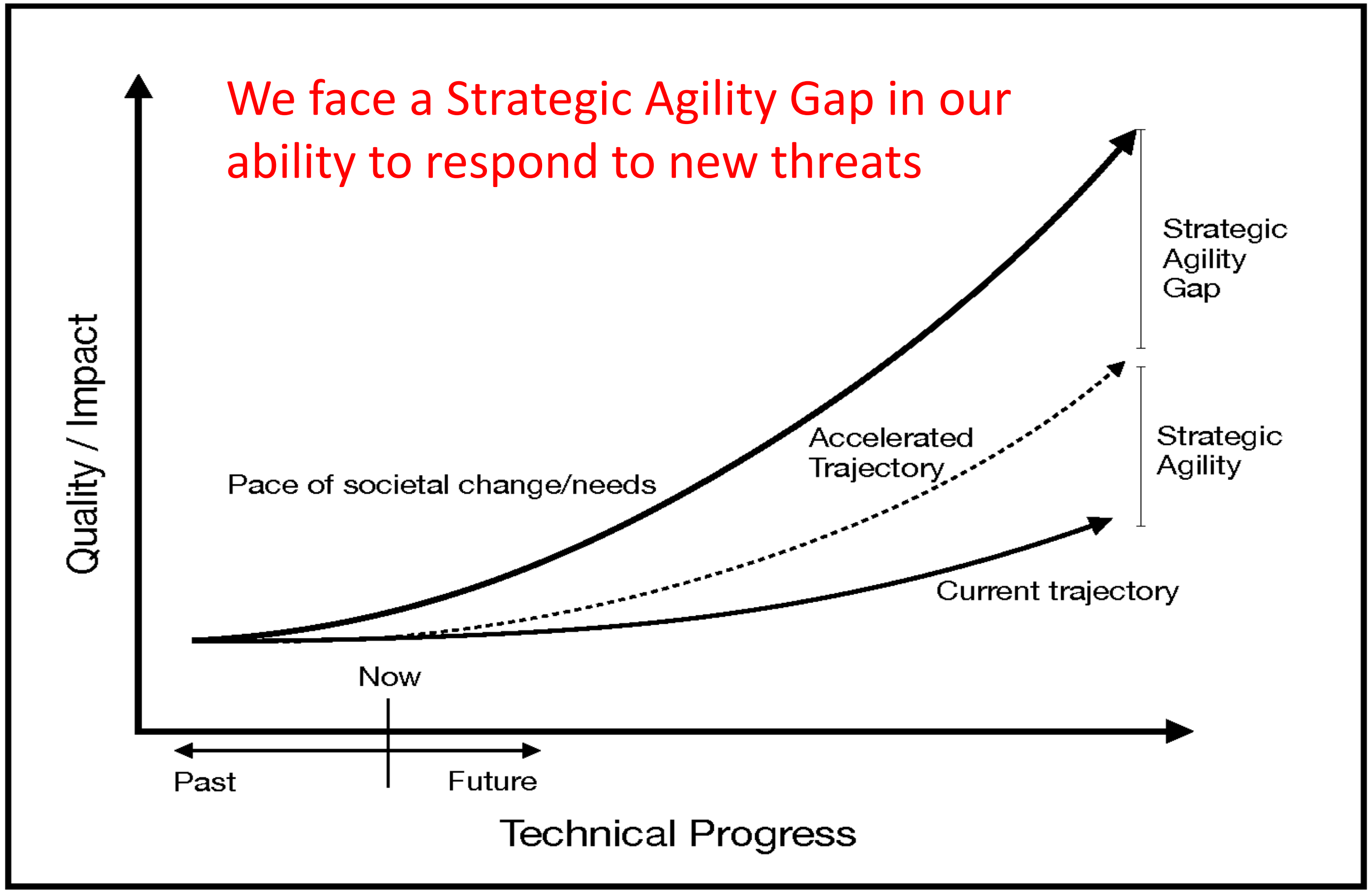
Conferences
Journals
National Funding
Centers of Excellence

Universities
National Laboratories
FFRDCs
Defense Contractors

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

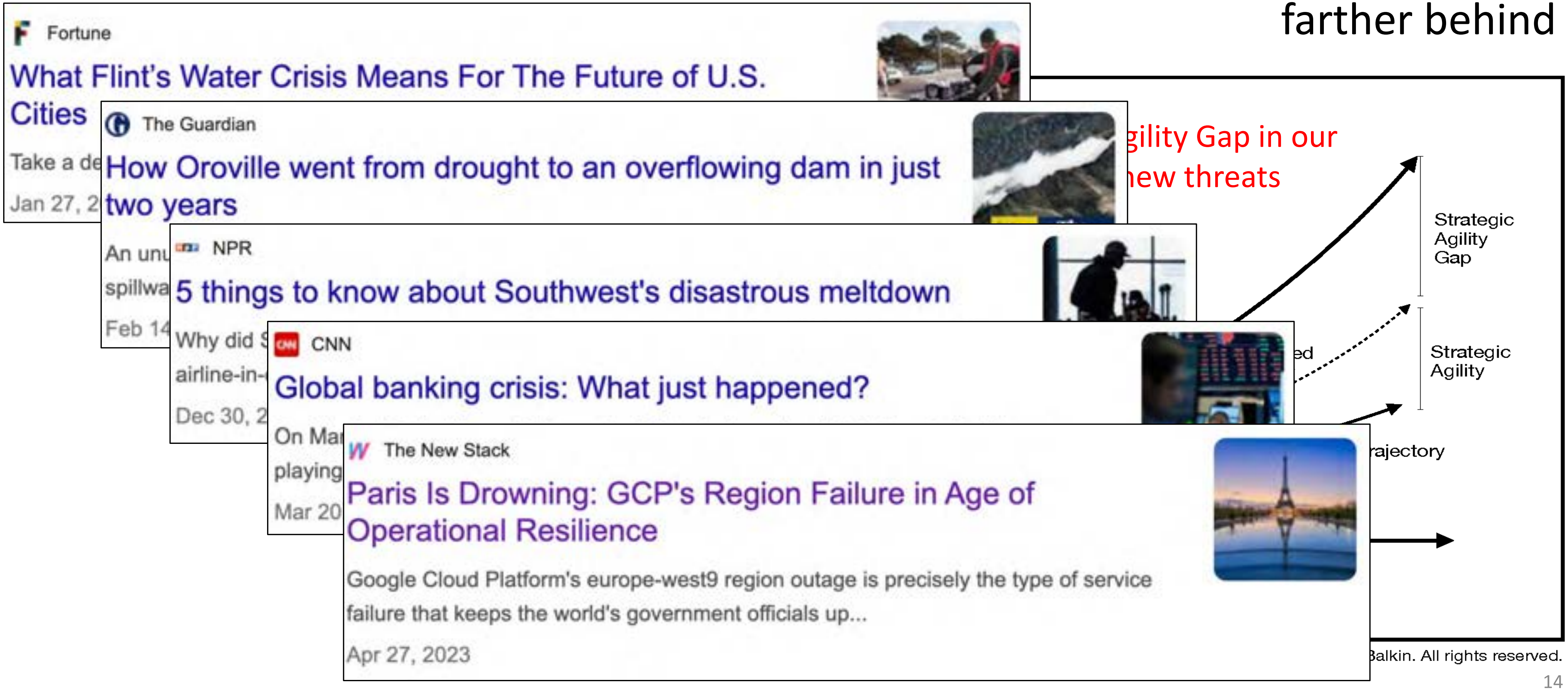
But it hasn't worked out this way. If anything, we seem to be falling farther behind



Evidence that we are stuck in the Gap:

- *According to Plan*, things appear to be going great.
- Getting better and better, or so it seems! Until it isn't.
- And then it's *bad*… And unclear how to respond.

But it hasn't worked out this way. If anything, we seem to be falling farther behind



Journal of Critical Infrastructure Policy • *Volume 2, Number 2* • *Fall / Winter 2021*

Strategic Perspectives

Progress toward Resilient Infrastructures: Are we falling behind the pace of events and changing threats?

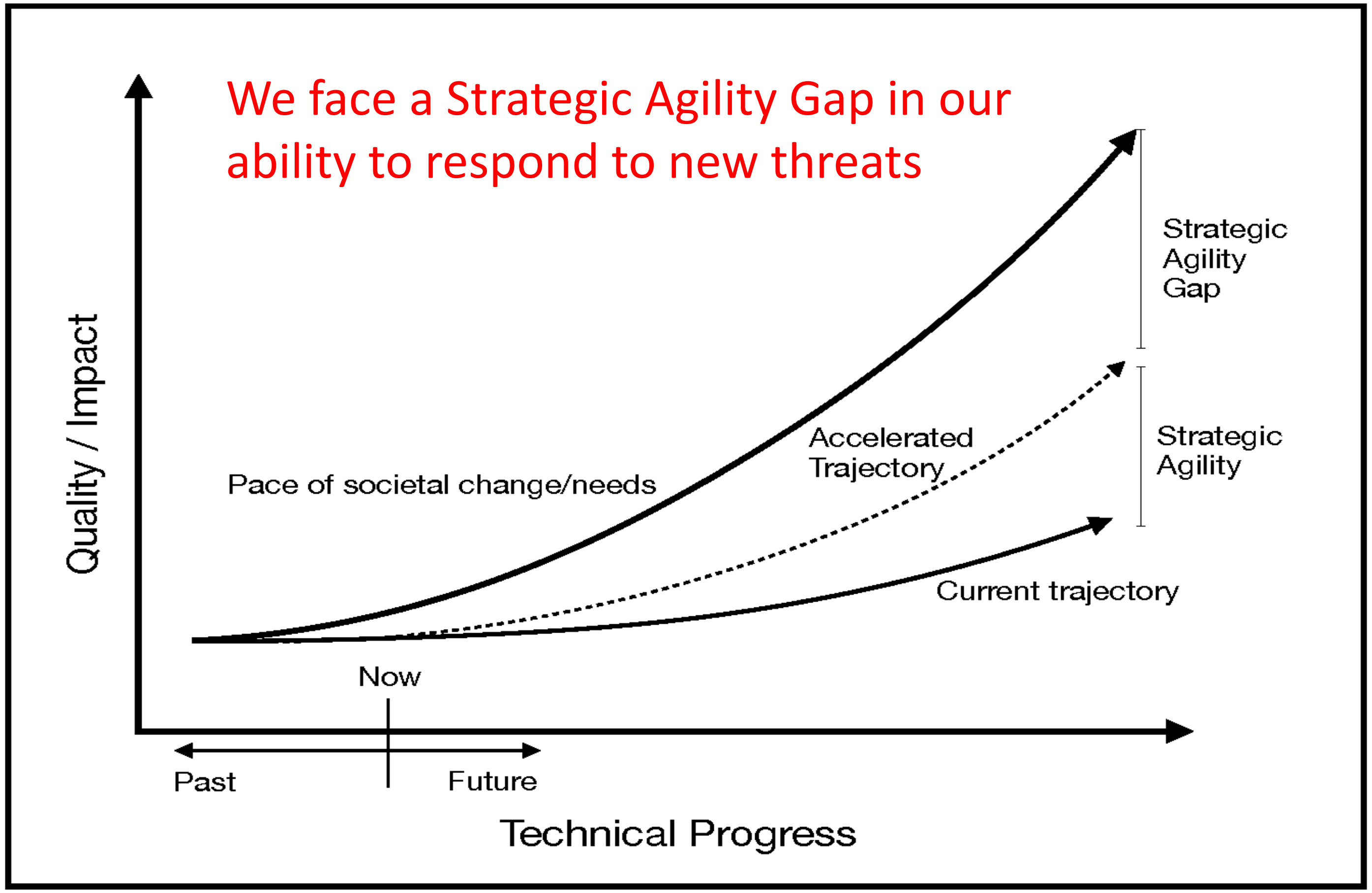
David D. Woods[1] and David L. Alderson[2]

[1] Professor Emeritus, Dept of Integrated Systems Engineering, Ohio

[2] Professor, Operations Research Dept, Naval Postgraduate School, d

But it hasn't worked out this way. If anything, we seem to be falling farther behind

- Growing system complexity
- New conflicts & threats
- Changing environment
- Changing tempos of activity



The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

…This Is Not Working!!

- We don't know our systems in their absolute entirety, and we never will!
- There is no single vantage point from where we can "see" everything
- And things are always changing
- There will always be hidden dependencies
- There will always be surprises!

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

…This Is Not Working!!

Resilience is not about what you have,

it’s about what you do!

- We are focused on the wrong things
- Nouns = the stuff we have
- Verbs = the processes for adaptation
- Need to focus: time, tempo, process.
- Our math is stuck on nouns
- We need (better) math for verbs

Critical Digital Services & Internet "Survivability"

Internet function is more than routing!

- all the value-added layers above routing
- an ecosystem of ***critical digital services***

"cyber" is noun-centric

Both transactions + controls!

All the software that enables critical digital services!

- ***You will never have complete knowledge of the system*** (components, software, users)
- The ***tangle of dependencies*** does not conform to traditional network layering (OSI 7-layers)
- You can ***learn only by operating*** it.
- The system is always adapting. Can we learn fast enough?

ACT II: Modeling + Simulation
Making sense of "Resilience"

- The concept of resilience is <u>important</u> and <u>popular</u>
  - Represents a new societal need, particularly given frequent surprise

- Over the last 10+ years, it has been <u>overused</u> to mean many different things
  - It has bureaucratic definitions that are not helpful for assessing systems
  - The use of resilience as a term is noisy and confusing

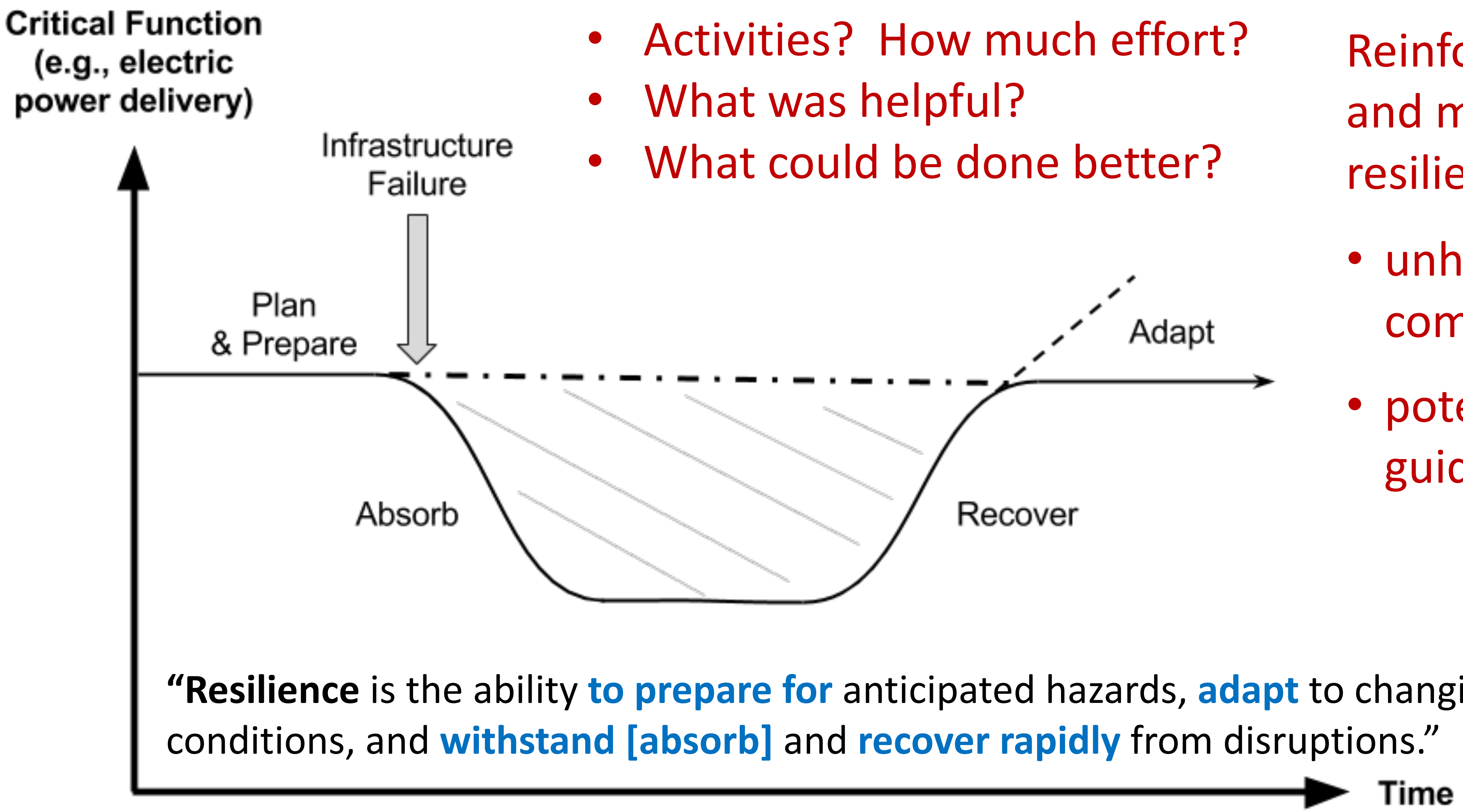
Notions of resilience have become noisy

Four ways that *resilience* is used.

easier to understand ↓	$\mathbb{R}_1$	***rebound***	return to previous levels of performance
	$\mathbb{R}_2$	***robustness***	copes successfully from well-modeled challenges
	$\mathbb{R}_3$	***graceful extensibility***	stretches to meet challenges at the boundaries
more generality	$\mathbb{R}_4$	***sustained adaptability***	sustains the ability to adapt over cycles of change

modified from Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety* 141 (2015) 5-9.

The "Rebound Curve" is a Poor Model of Resilience



Process-Outcome Confusion
- Activities? How much effort?
- What was helpful?
- What could be done better?

Reinforces oversimplifications and misconceptions about resilience

- unhelpful for understanding complex systems
- potentially dangerous for guiding decisions

"**Resilience** is the ability **to prepare for** anticipated hazards, **adapt** to changing conditions, and **withstand [absorb]** and **recover rapidly** from disruptions."

Official Definition for Resilience from NIST, DHS, FEMA, etc.

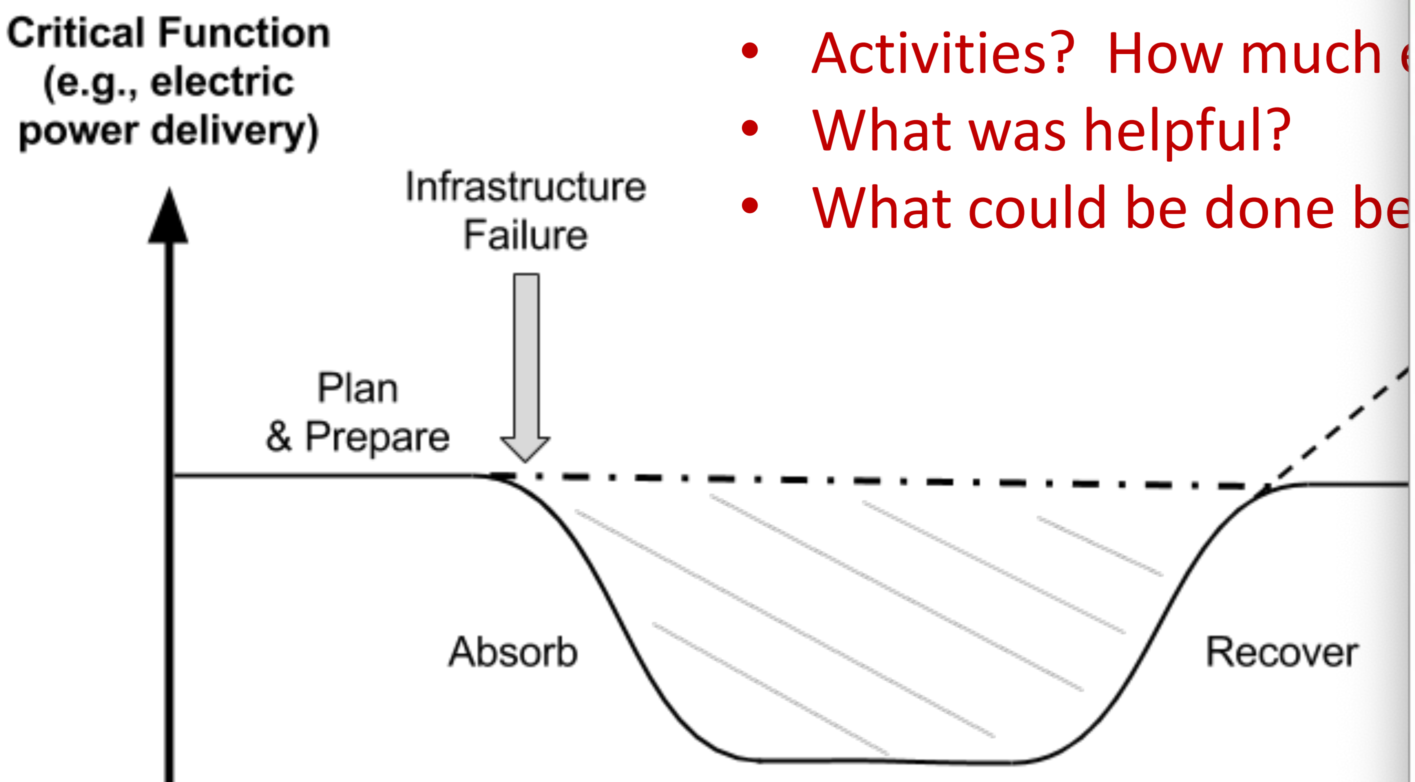
The “Rebound Curve” is a Poo

Process-Outcome Confusi

- Activities? How much
- What was helpful?
- What could be done be

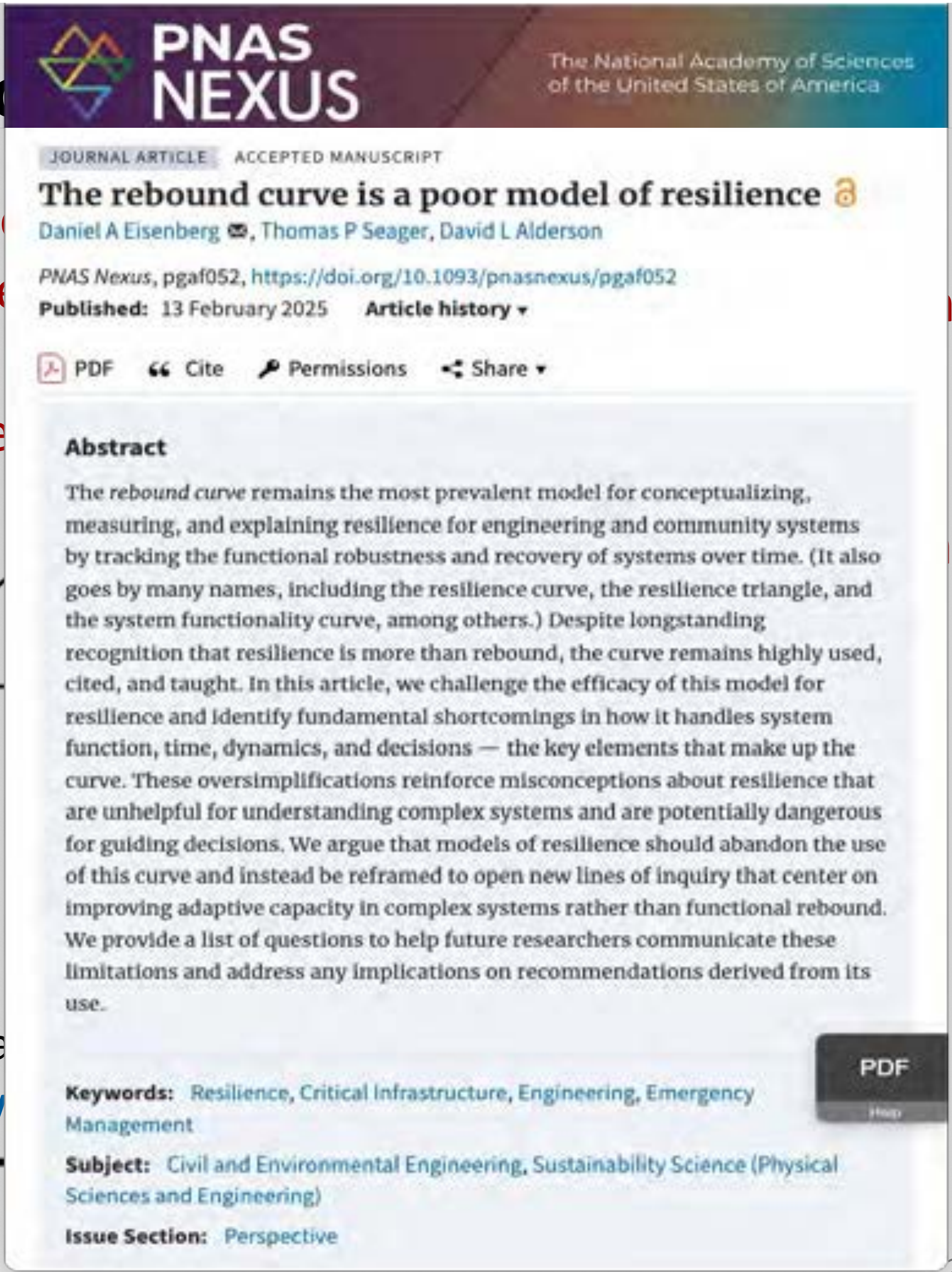
s

g



“**Resilience** is the ability **to prepare for** anticipated haza conditions, and **withstand [absorb]** and **recover rapidly**

Official Definition for Resilience from NIST, DHS, FEMA, etc.



PNAS NEXUS

The National Academy of Sciences of the United States of America

JOURNAL ARTICLE ACCEPTED MANUSCRIPT

The rebound curve is a poor model of resilience

Daniel A Eisenberg, Thomas P Seager, David L Alderson

PNAS Nexus, pgaf052, https://doi.org/10.1093/pnasnexus/pgaf052
Published: 13 February 2025 **Article history**

PDF Cite Permissions Share

Abstract

The *rebound curve* remains the most prevalent model for conceptualizing, measuring, and explaining resilience for engineering and community systems by tracking the functional robustness and recovery of systems over time. (It also goes by many names, including the resilience curve, the resilience triangle, and the system functionality curve, among others.) Despite longstanding recognition that resilience is more than rebound, the curve remains highly used, cited, and taught. In this article, we challenge the efficacy of this model for resilience and identify fundamental shortcomings in how it handles system function, time, dynamics, and decisions — the key elements that make up the curve. These oversimplifications reinforce misconceptions about resilience that are unhelpful for understanding complex systems and are potentially dangerous for guiding decisions. We argue that models of resilience should abandon the use of this curve and instead be reframed to open new lines of inquiry that center on improving adaptive capacity in complex systems rather than functional rebound. We provide a list of questions to help future researchers communicate these limitations and address any implications on recommendations derived from its use.

Keywords: Resilience, Critical Infrastructure, Engineering, Emergency Management

Subject: Civil and Environmental Engineering, Sustainability Science (Physical Sciences and Engineering)

Issue Section: Perspective

PDF

Notions of resilience have become noisy

Four ways that *resilience* is used.

easier to understand ↓ more generality			
	$\mathbb{R}_1$	***rebound***	return to previous levels of performance
	$\mathbb{R}_2$	***robustness***	copes successfully from well-modeled challenges
	$\mathbb{R}_3$	***graceful extensibility***	stretches to meet challenges at the boundaries
	$\mathbb{R}_4$	***sustained adaptability***	sustains the ability to adapt over cycles of change

- Woods DD, 2015, “Four concepts for resilience and the implications for the future of resilience engineering,” *Reliability Engineering and System Safety* 141: 5-9.
- Woods DD, 2018, “The theory of graceful extensibility: basic rules that govern adaptive systems,” *Environment Systems and Decisions*, 38(4):433–457.
- Sharkey TC, Nurre Pinkley SG, Eisenberg DA, Alderson DL, 2020. "In search of network resilience: An optimization-based view," *Networks* 77(2): 225-254. https://doi.org/10.1002/net.21996

Today's Agenda

Act I: Societal Need for Infrastructure Resilience

Act II: (Getting Stuck in) Modeling + Simulation of Lifeline Infrastructure Interactions as a Path to Resilience

Act III: A Need for Different Mathematics (enabled by new science based on patterns)

Acknowledgments: Daniel Eisenberg (NPS) and David Woods (Ohio State)

This work was supported by the Office of Naval Research, the Air Force Office of Scientific Research, the Defense Threat Reduction Agency, and the DOD Strategic Environmental Research and Development Program.

Another Way Forward

We need to study these ***patterns of complexity*** as empirical phenomena

- Patterns of **behavior in time**, not just structure
- Patterns in how systems fail
- Patterns in how systems adjust, adapt, and survive

Where we agree…

Oversimple abstractions don't work
(at least, not for long)

✗ Linear systems with predictable cause-effect

✗ Root-cause analysis (e.g., blame the human!)

✗ Stationarity in time

Where it's noisy…

- What are the patterns?
- What drives them?
- How to represent them?
- What to do about them?

Making infrastructure more operational (My take)

- Infrastructure is not static. Things are moving. In support of a mission.
- Operations will be contested (meaning there are disruptions).
- We want the mission to succeed, even when disrupted.

- ***Viability*** (not readiness) should be the primary system objective
- ***Systems are always adapting***
  - ***pursuing opportunity*** (growth in the face of constraints)
  - ***handling challenge*** (extensibility in the face of brittle collapse)
- They are doing both simultaneously
- The same processes are at work for both
- ***Management of tradeoffs / constraints is fundamental***

What are the patterns that matter? (My take)

- A plan is in progress over an infrastructure network (perhaps logistics)
- ***How do you modify the plan in-progress*** as you discover changes in obstacles, goals, priorities, objectives?
  - (Particularly when you can't go back and rerun the original planning tools because things are moving and changing)
  - Your plan will become stale. Your model of the world will become stale.
  - Redirecting things on the move imposes ***friction*** and ***lag*** (how to represent this?)

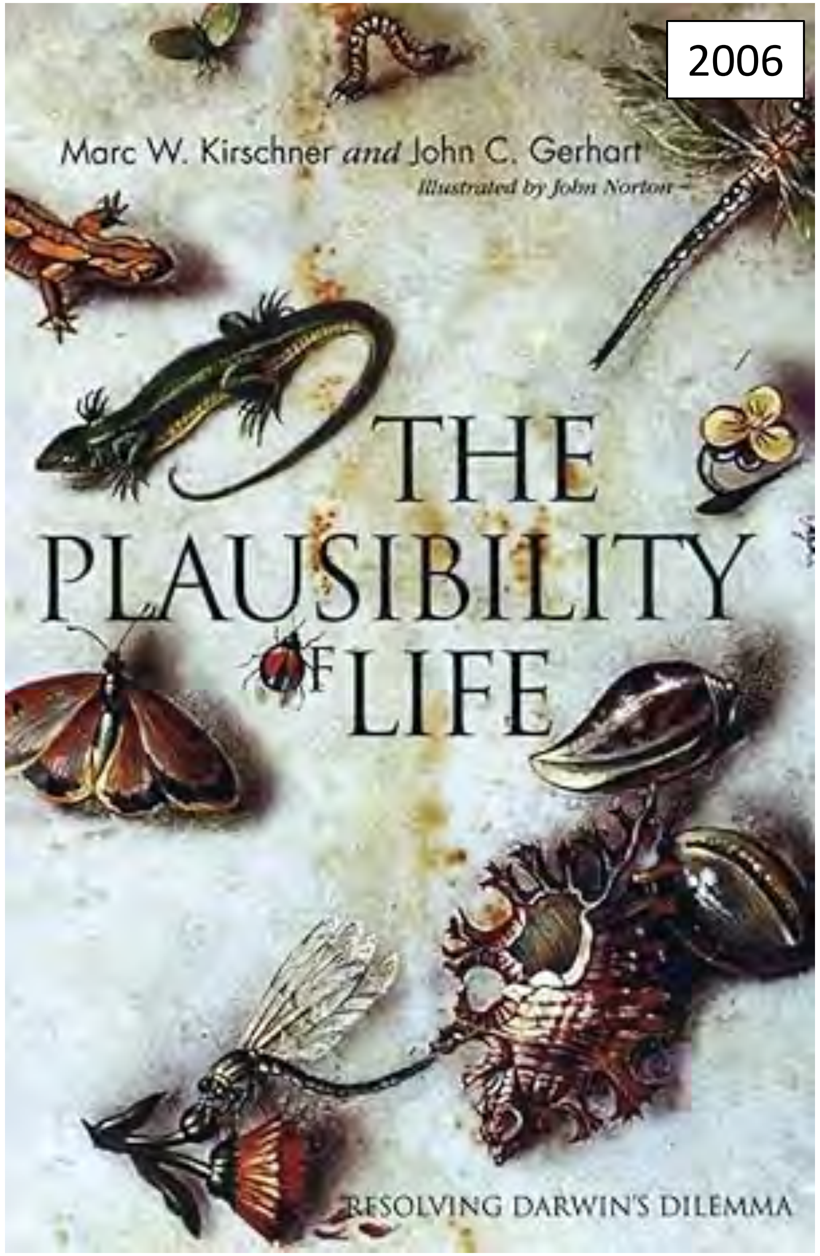
- *What can I adjust midstream?*
- *What do I need to have around to maximize my ability to adjust midstream?*
- *If I can get you another [X], would that make a big difference?*

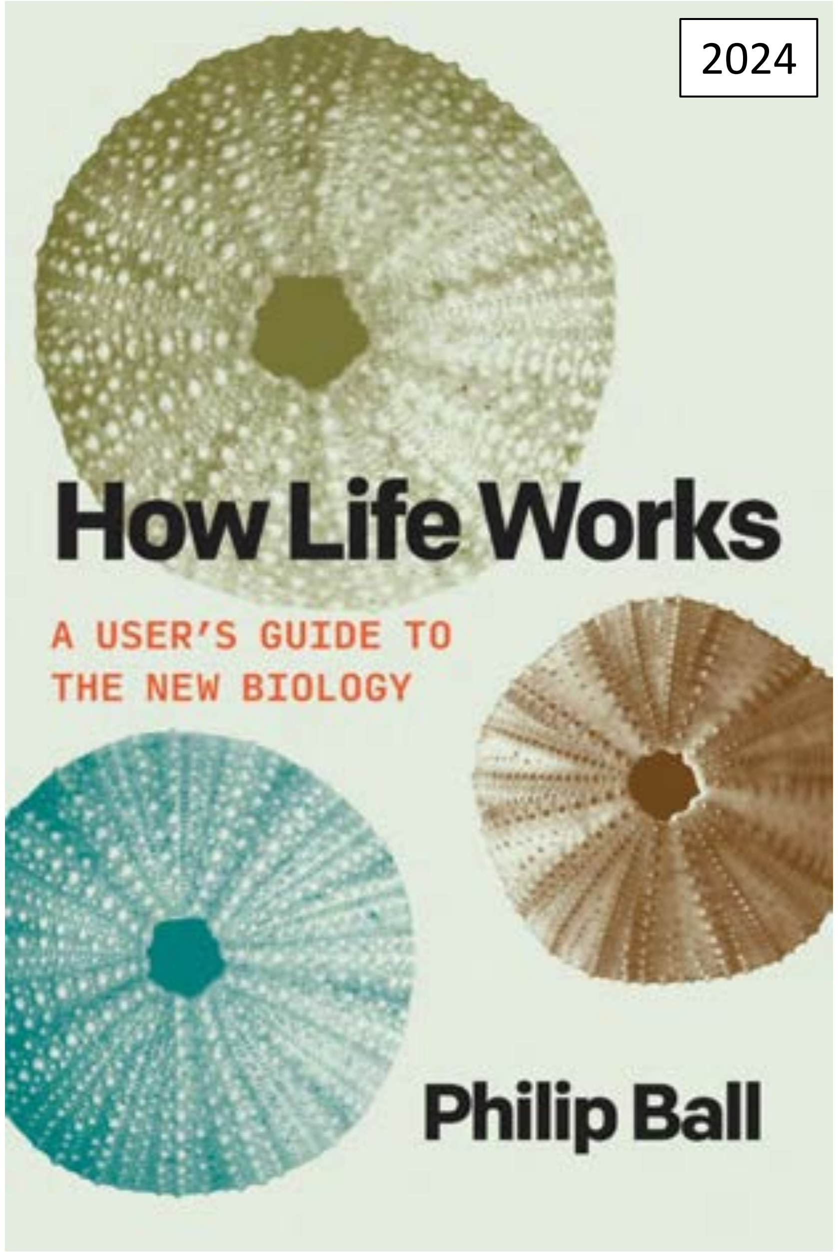
adaptive capacity

A system's capacity to adapt to challenges ahead,
when the exact challenge to be handled
***cannot* be specified completely in advance.**

We need mathematics to help us understand the complex dynamics of building deployable adaptive capacity.

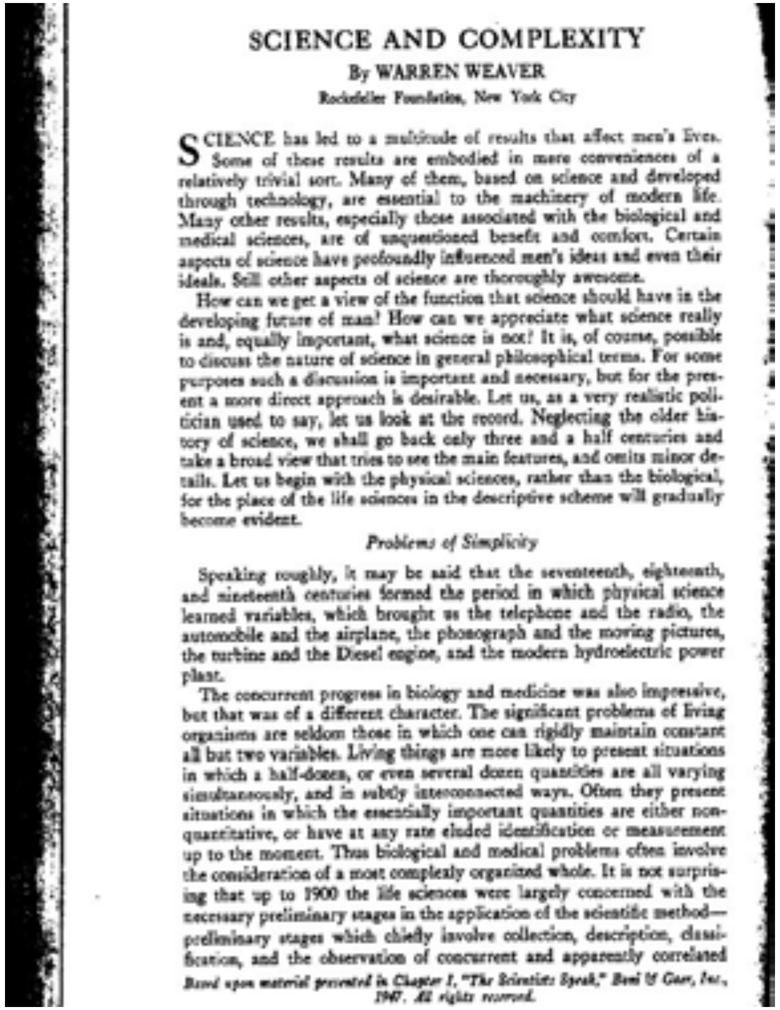
Biology-inspired mathematics





Question: Is infrastructure viability more like biology than engineering?

Role of Organization



SCIENCE AND COMPLEXITY

By WARREN WEAVER

Rockefeller Foundation, New York City

SCIENCE has led to a multitude of results that affect men's lives. Some of these results are embodied in mere conveniences of a relatively trivial sort. Many of them, based on science and developed through technology, are essential to the machinery of modern life. Many other results, especially those associated with the biological and medical sciences, are of unquestioned benefit and comfort. Certain aspects of science have profoundly influenced men's ideas and even their ideals. Still other aspects of science are thoroughly awesome.

How can we get a view of the function that science should have in the developing future of man? How can we appreciate what science really is and, equally important, what science is not? It is, of course, possible to discuss the nature of science in general philosophical terms. For some purposes such a discussion is important and necessary, but for the present a more direct approach is desirable. Let us, as a very realistic politician used to say, let us look at the record. Neglecting the older history of science, we shall go back only three and a half centuries and take a broad view that tries to see the main features, and omits minor details. Let us begin with the physical sciences, rather than the biological, for the place of the life sciences in the descriptive scheme will gradually become evident.

Problems of Simplicity

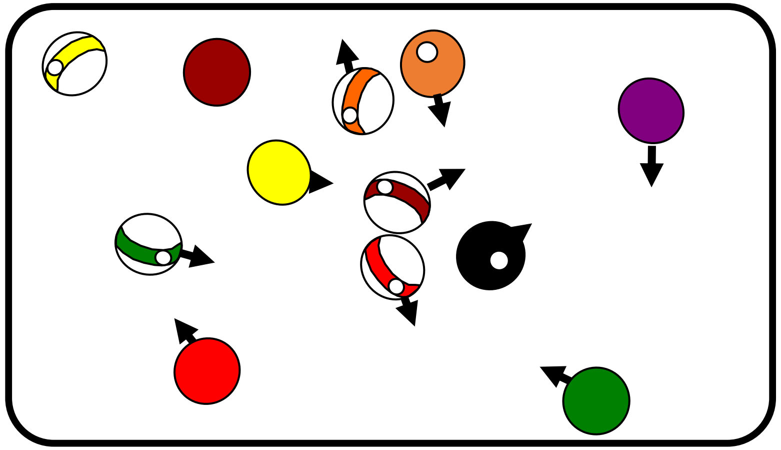
Speaking roughly, it may be said that the seventeenth, eighteenth, and nineteenth centuries formed the period in which physical science learned variables, which brought us the telephone and the radio, the automobile and the airplane, the phonograph and the moving pictures, the turbine and the Diesel engine, and the modern hydroelectric power plant.

The concurrent progress in biology and medicine was also impressive, but that was of a different character. The significant problems of living organisms are seldom those in which one can rigidly maintain constant all but two variables. Living things are more likely to present situations in which a half-dozen, or even several dozen quantities are all varying simultaneously, and in subtly interconnected ways. Often they present situations in which the essentially important quantities are either non-quantitative, or have at any rate eluded identification or measurement up to the moment. Thus biological and medical problems often involve the consideration of a most complexly organized whole. It is not surprising that up to 1900 the life sciences were largely concerned with the necessary preliminary stages in the application of the scientific method—preliminary stages which chiefly involve collection, description, classification, and the observation of concurrent and apparently correlated

Based upon material presented in Chapter I, "The Scientists Speak," Boni & Gaer, Inc., 1947. All rights reserved.

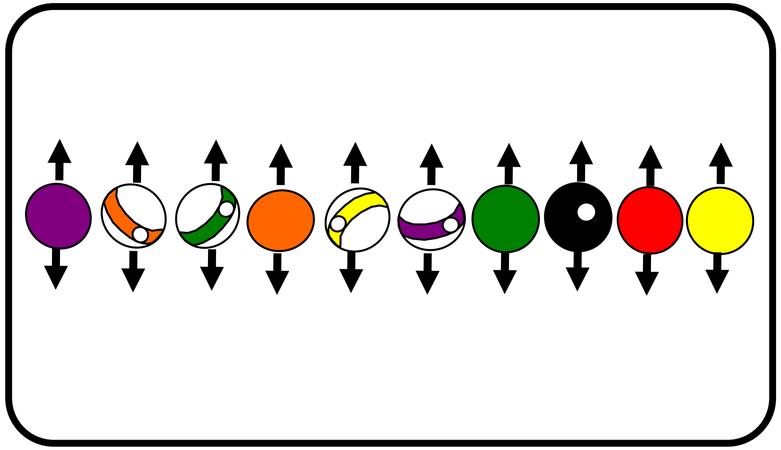
Weaver, W. 1948. Science and complexity. *American Scientist* 36 536-544.

Disorganized



"The methods of statistical mechanics are valid only when the balls are distributed, in their positions and motions, in a helter-skelter, that is to say a disorganized, way."

Organized



"For example, the statistical methods would not apply if someone were to arrange the balls in a row parallel to one side rail of the table, and then start them all moving in precisely parallel paths perpendicular to the row in which they stand. Then the balls would never collide with each other nor with two of the rails, and one would not have a situation of disorganized complexity."

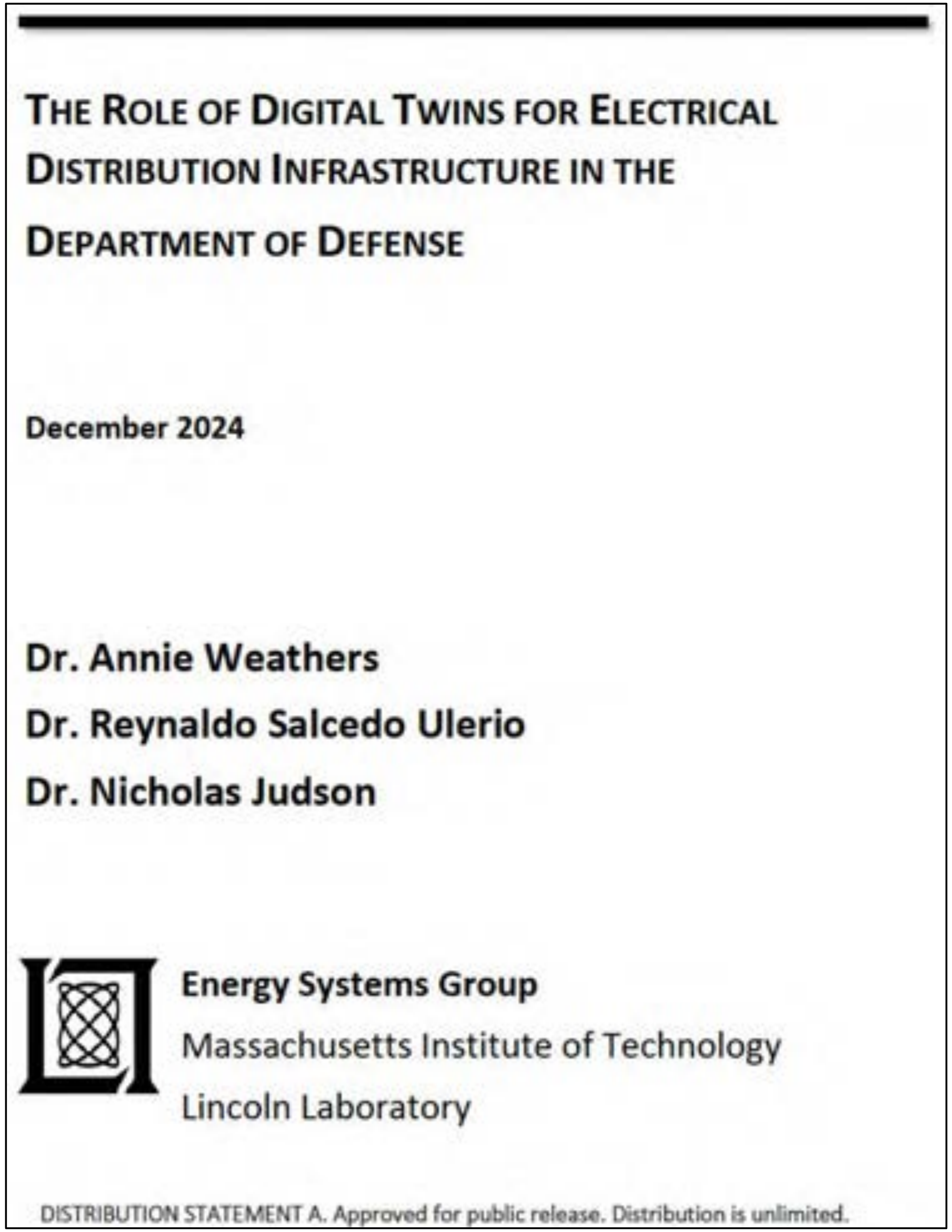
See also:

Alderson, D.L., and Doyle, J.C., 2010, Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures. IEEE Transactions on Systems, Man, and Cybernetics-Part A, 40(4): 839-852.

Alderson, D.L., 2008, Catching the "Network Science" Bug: Insight and Opportunity for the Operations Researcher. Operations Research 56(5): 1047-1065.

Digital Twins

- A specious approach to infrastructures
- Useful, but only in limited ways
- Models become stale!



THE ROLE OF DIGITAL TWINS FOR ELECTRICAL DISTRIBUTION INFRASTRUCTURE IN THE DEPARTMENT OF DEFENSE

December 2024

Dr. Annie Weathers

Dr. Reynaldo Salcedo Ulerio

Dr. Nicholas Judson

Energy Systems Group

Massachusetts Institute of Technology

Lincoln Laboratory

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Nouns vs Verbs

Resilience is not about what you have, it's about what you do!

Question: Are our mathematics too focused on nouns?

Resilience as a verb in the future tense?

See also: Woods, D. D. (2018). "Resilience is a verb." In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

Journal of Economic Behavior and Organization 205 (2023) 638–647

Contents lists available at ScienceDirect

Journal of Economic Behavior and Organization

journal homepage: www.elsevier.com/locate/jebo

Economics in nouns and verbs

W. Brian Arthur[a,b]

[a] Santa Fe Institute, Santa Fe, NM, USA
[b] Intelligent Systems Lab, PARC, Palo Alto, CA, USA

A R T I C L E I N F O

Article history:
Received 10 June 2022
Revised 11 October 2022
Accepted 25 October 2022
Available online 13 December 2022

JEL classification:
B41 (Economic Methodology)
B59 (Current Heterodox Approaches-Other)
C02 (Mathematical Methods)

Keywords:
Economic theory
Mathematics in economics
Algorithms
Complexity economics
Computational economics

A B S T R A C T

Standard economic theory uses mathematics as its main means of understanding, and this brings clarity of reasoning and logical power. But there is a drawback: algebraic mathematics restricts economic modeling to what can be expressed only in quantitative nouns, and this forces theory to leave out matters to do with process, formation, adjustment, and creation—matters to do with nonequilibrium. For these we need a different means of understanding, one that allows verbs as well as nouns. Algorithmic expression is such a means. It allows verbs—processes—as well as nouns—objects and quantities. It allows fuller description in economics, and can include heterogeneity of agents, actions as well as objects, and realistic models of behavior in ill-defined situations. The world that algorithms reveal is action-based as well as object-based, organic, possibly ever-changing, and not fully knowable. But it is strangely and wonderfully alive.

If we all agree on [resilience], why don’t we have it already?

Four barriers to resilience

1. AWARENESS: We don’t know we need it
2. KNOWLEDGE: We don’t know how to create it
3. INCENTIVES: We can’t justify the investment in it
4. GOVERNANCE: Incompatibilities across organizational boundaries that lead to working at cross purposes

REFS:
Alderson, D.L., 2019, Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience, in M. Ruth & S. G. Reisemann (Eds), Handbook on Resilience of Socio-technical Systems, Edward Elgar Publishing, Northampton, MA.
Flynn, S.E. (2015), ‘Bolstering critical infrastructure resilience after Superstorm Sandy: lessons for New York and the nation’, Global Resilience Institute, Northeastern University, Boston, MA.

Looking Forward

We need a different type of **architecture** for our mission critical systems.

One that goes beyond traditional optimization and design.

The principles are different, but ubiquitous in the real world.

We cannot escape the complexity traps if we don't build **adaptive capacity**.

How can mathematics help us achieve these outcomes?

We need to reframe how we think about resilience.

Adaptive capacity is about **more than handling challenge**.

It is about **seizing opportunity**.

The same processes are at work. We should stop using an emergency management / risk mindset.

Contact Information

- Dr. David L. Alderson

  Professor, Operations Research

  Executive Director, Center for Infrastructure Defense

  Naval Postgraduate School

  dlalders@nps.edu

  http://faculty.nps.edu/dlalders

- NPS Center for Infrastructure Defense

  http://www.nps.edu/cid

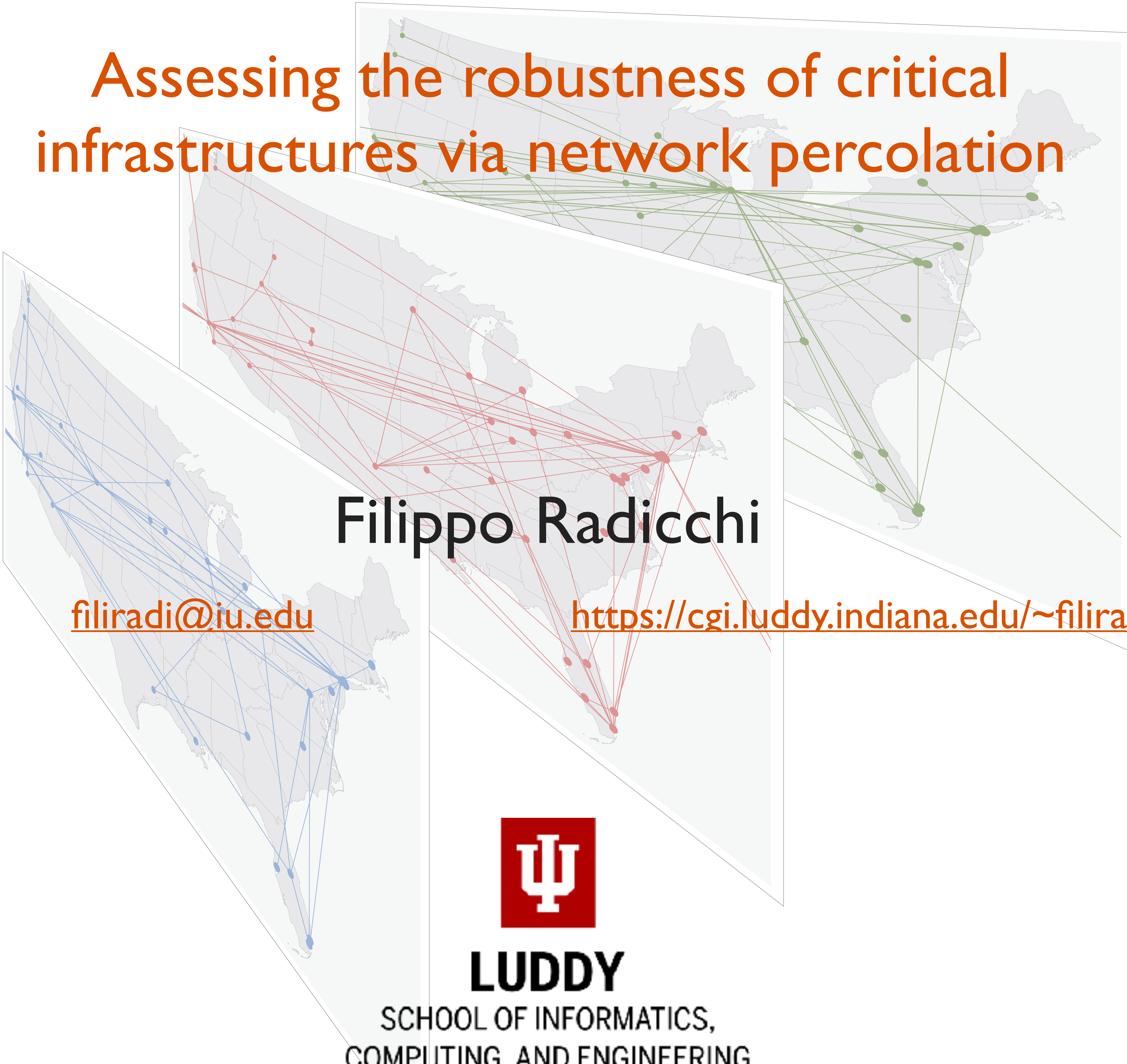
Additional References (1 of 2)

- Eisenberg, D.A., Seager, T.P., and Alderson, D.L., 2025, **"The rebound curve is a poor model of resilience,"** PNAS Nexus, pgaf052, https://doi.org/10.1093/pnasnexus/pgaf052
- Woods DD, Alderson DL, 2022 **"Progress Toward Resilient Infrastructures: Are we falling behind the pace of events and changing threats?,"** Journal of Critical Infrastructure Policy, 2(2):5-18. doi: 10.18278/jcip.2.2.2.
- Woods, D.D. (2020). **The Strategic Agility Gap: How Organizations are Slow and Stale to Adapt in a Turbulent World**. In Journé, B., Laroche, H., Bieder, C. and Gilbert, C. (Eds.), Human and Organizational Factors: Practices and Strategies for a Changing World. Springer Open & the Foundation for Industrial Safety Culture, Springer Briefs in Safety Management, Toulouse France, pp. 95-104 https://doi.org/10.1007/978-3-030-25639-5
- Sharkey TC, Nurre Pinkley SG, Eisenberg DA, Alderson DL, 2020. **"In search of network resilience: An optimization-based view,"** Networks. 2020;1-30. https://doi.org/10.1002/net.21996
- Woods, D.D. (2019). **Essentials of Resilience, Revisited**. In M. Ruth and S. G. Reisemann (Eds)., Handbook on Resilience of Socio-Technical Systems. Edward Elgar Publishing, pp. 52-65.
- Eisenberg, D.A., Seager, T.P., and Alderson, D.L., 2019, **"Rethinking Resilience Analytics,"** Risk Analysis, 39(9): 1870-1884.
- Woods, D. D. (2018). **The Theory of Graceful Extensibility: Basic rules that govern adaptive systems.** Environment Systems and Decisions, 38(4), 433-457.
- Woods, David D. **"Four concepts for resilience and the implications for the future of resilience engineering."** Reliability Engineering & System Safety 141 (2015): 5-9.

Additional References (2 of 2)

- Alderson, D.L., 2018, **“Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience, I**n M. Ruth & S. G. Reisemann (Eds), *Handbook on Resilience of Socio-technical Systems*, Edward Elgar Publishing.
- Salmerón, J., Alderson, D.L, and Brown, G.G., 2018, **"Resilience Report: Analysis of Hawaiian Electric Power Grid Vulnerability to Physical Attack (U)"**, Naval Postgraduate School Technical Report NPS-OR-18-001R, February.
- Alderson, D.L., Brown, G.G., Dell, R.F., Witwer, T.M., 2017, **“Studies of the Fuel Supply Chain in the Pacific Area of Responsibility (U),”** NPS Technical Report NPS-OR-17-003R, October.
- Alderson, D.L., Brown, G., and Carlyle, W.M., 2015, **“Operational Models of Infrastructure Resilience,”** *Risk Analysis* 35(4): 562-586 (received Award for Best Paper of 2015 in Risk Analysis).
- Alderson, D.L., G.G. Brown, W.M. Carlyle. 2014. **“Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems.”** A. Newman, J. Leung, eds., *Tutorials in Operations Research: Bridging Data and Decision*. Institute for Operations Research and Management Science, Hanover, MD, 180-215.
- Alderson, D.L., G.G. Brown, W.M. Carlyle, L.A. Cox. 2013. **“Sometimes there is no ‘most vital’ arc: assessing and improving the operational resilience of systems.”** *Military Operations Research* 18(1) 21-37.
- Brown, G., Carlyle, M., Salmerón, J. and Wood, K., 2006, **“Defending Critical Infrastructure,”** *Interfaces*, 36, pp. 530-544.

Assessing the robustness of critical infrastructures via network percolation



Filippo Radicchi

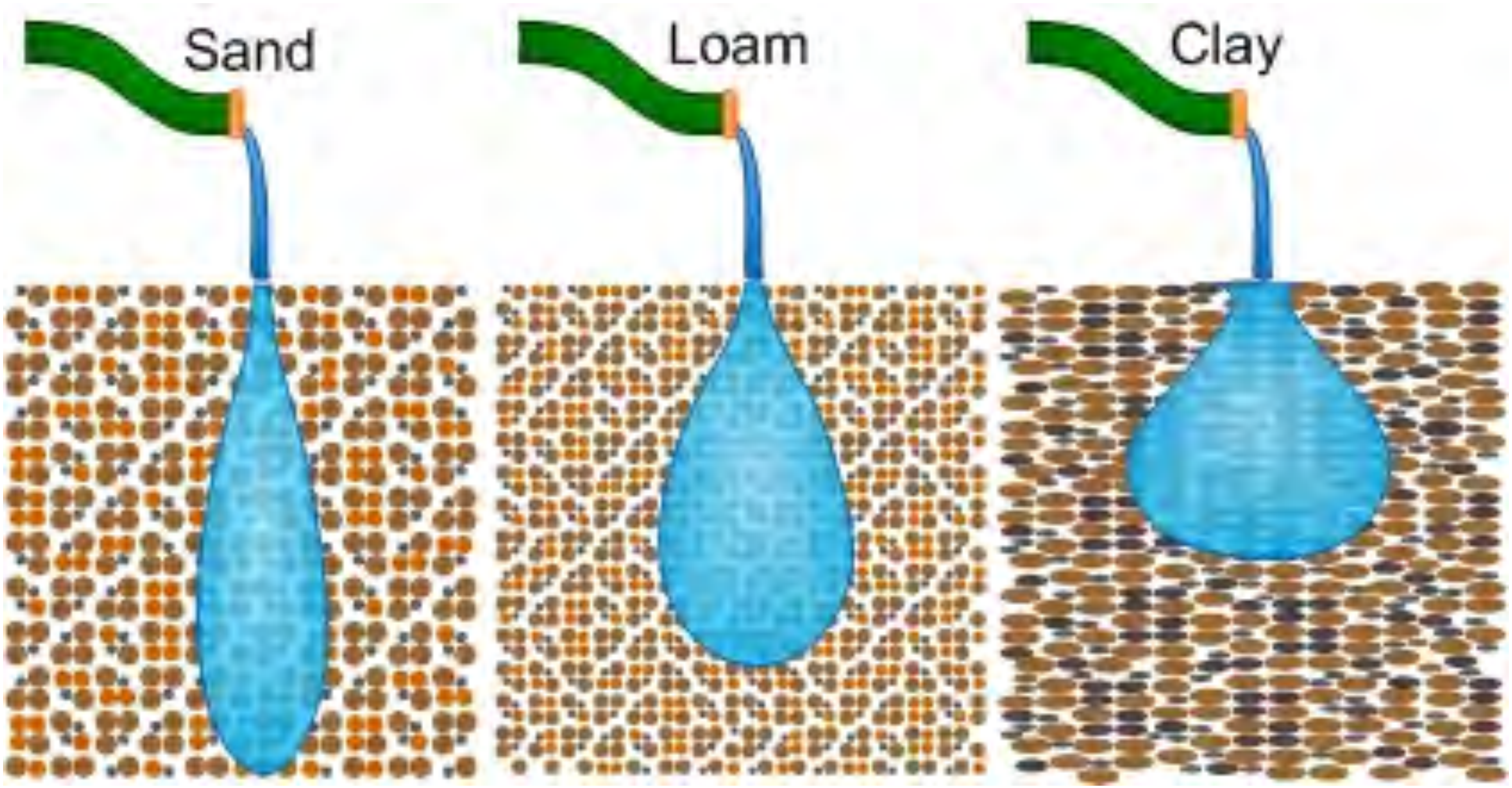
filiradi@iu.edu

https://cgi.luddy.indiana.edu/~filiradi

LUDDY
SCHOOL OF INFORMATICS,
COMPUTING, AND ENGINEERING

What is percolation?

percolation refers to the movement and/or filtering of fluids through porous materials



Coffee percolators

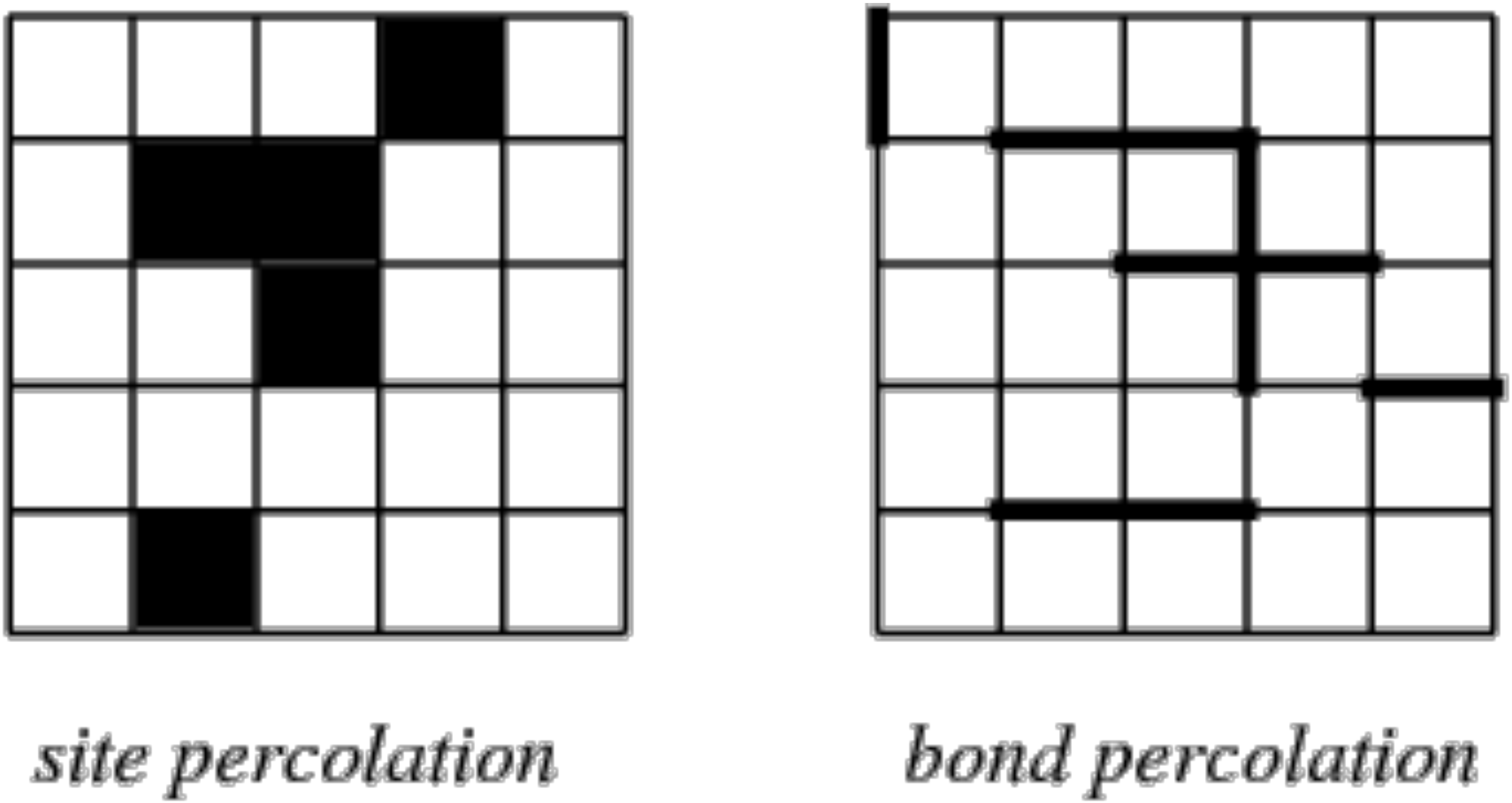
Filter machine

Neapolitan machine

Mocha machine

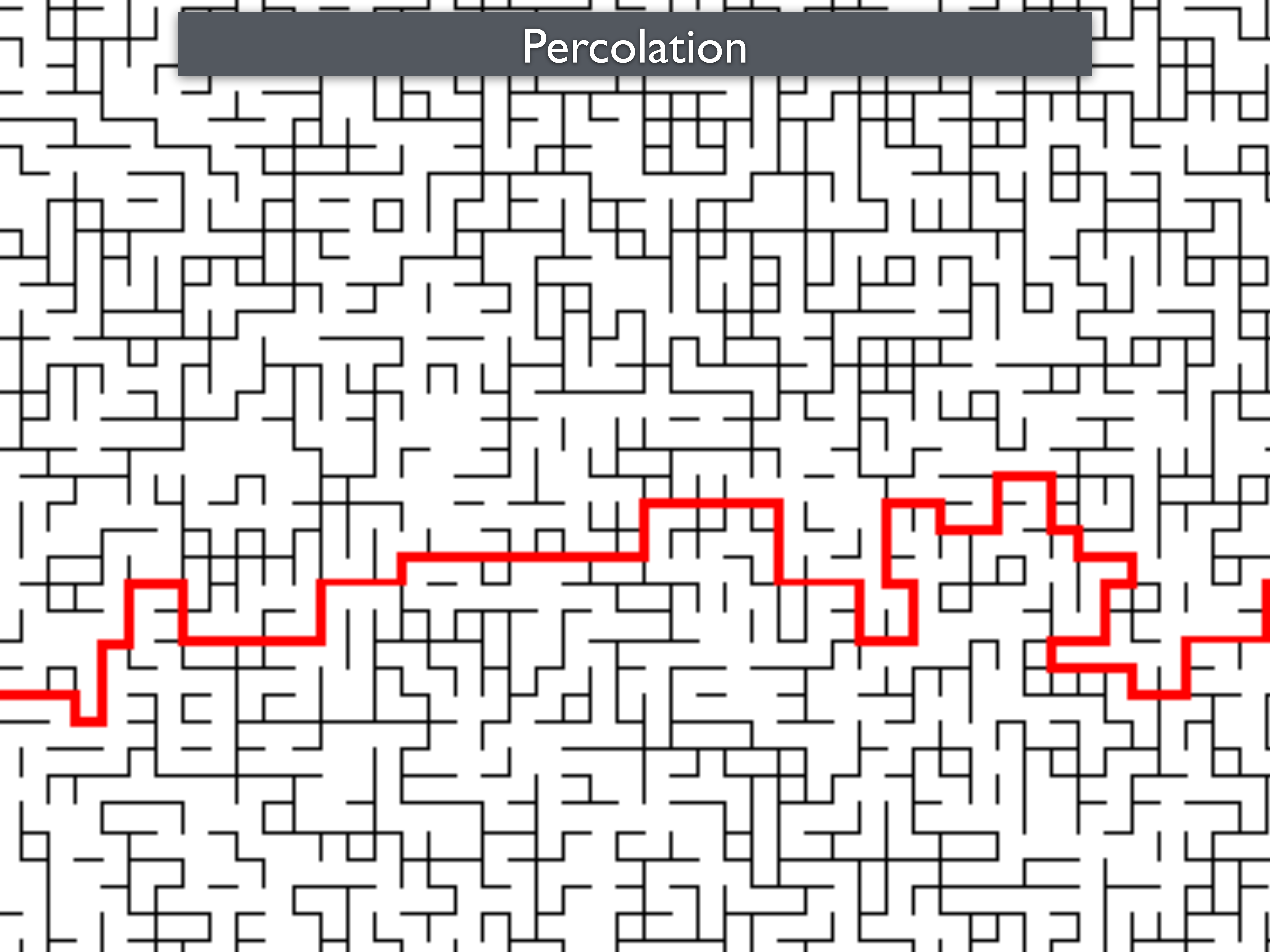
Espresso machine

Ordinary percolation models

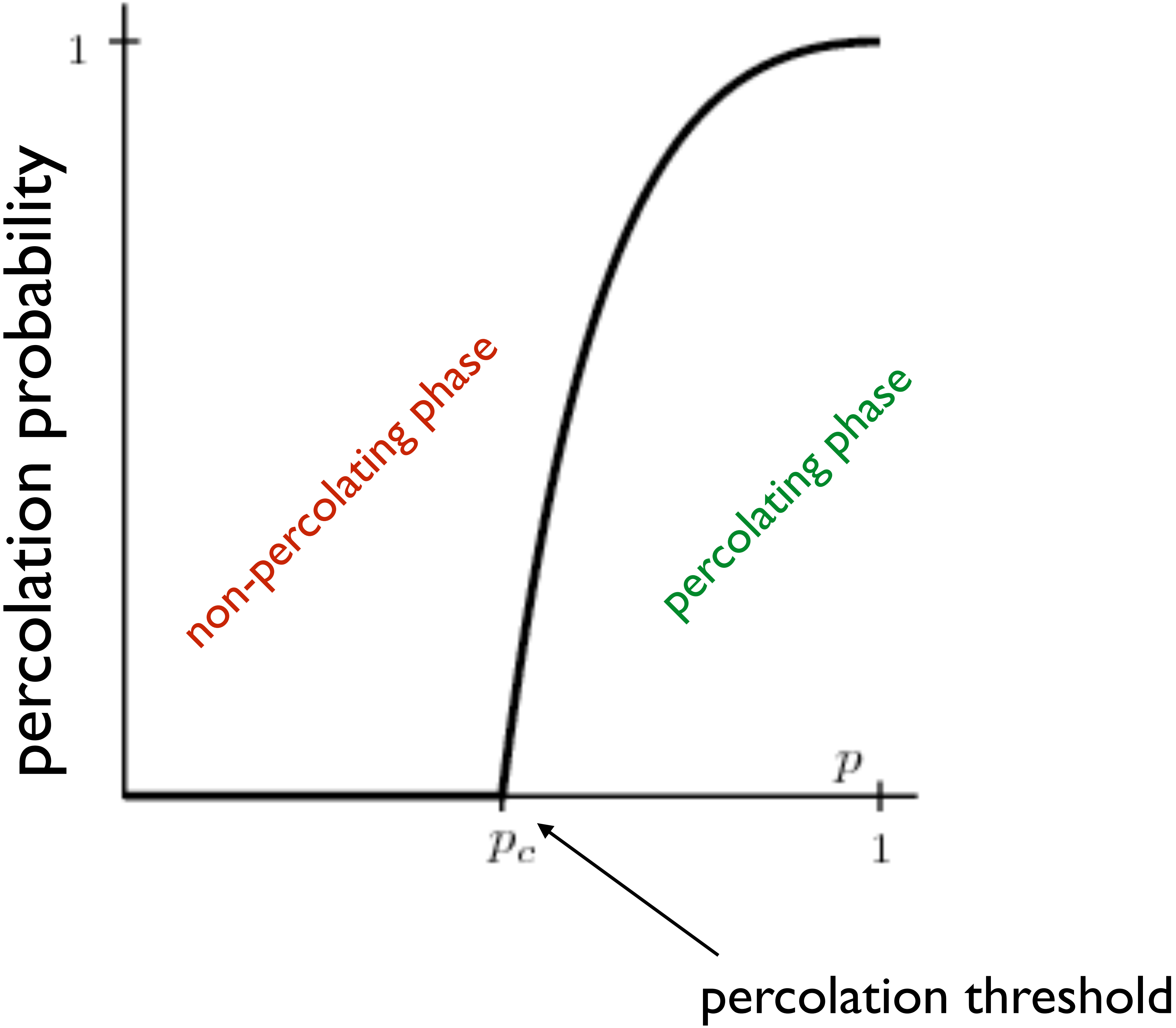


bonds or sites are occupied with probability p

Percolation

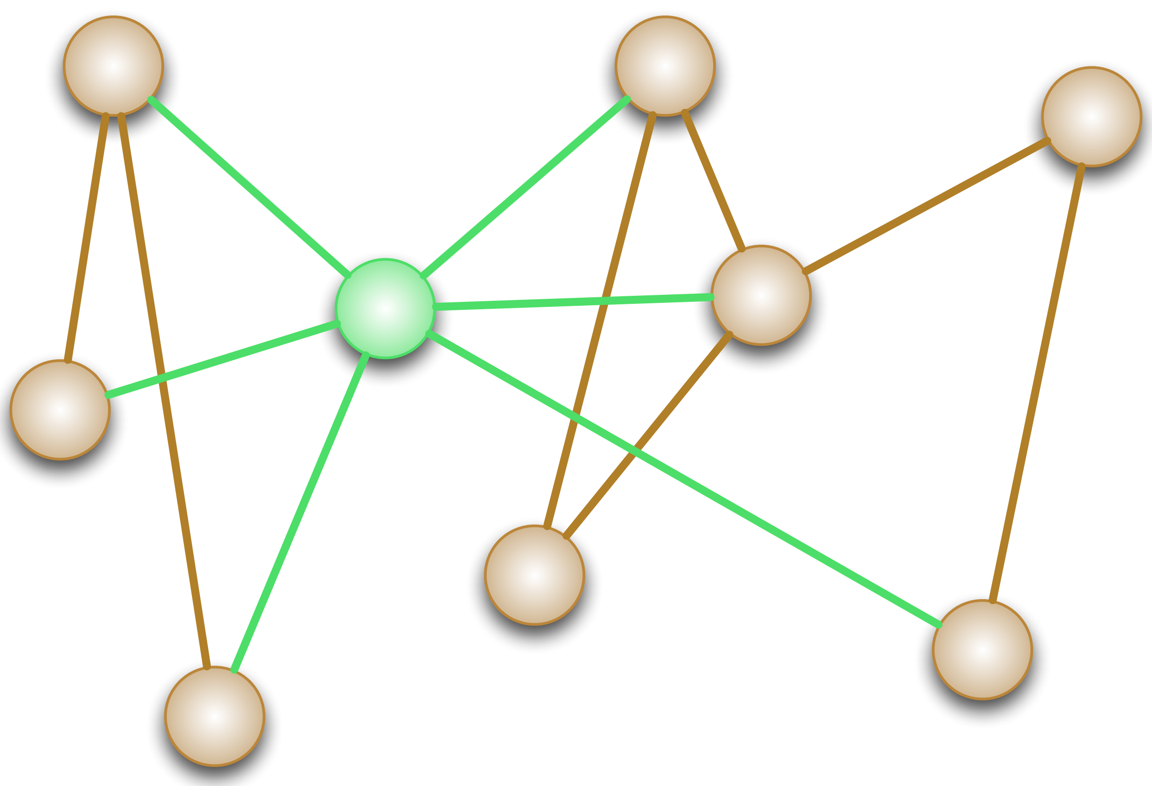


Percolation transition

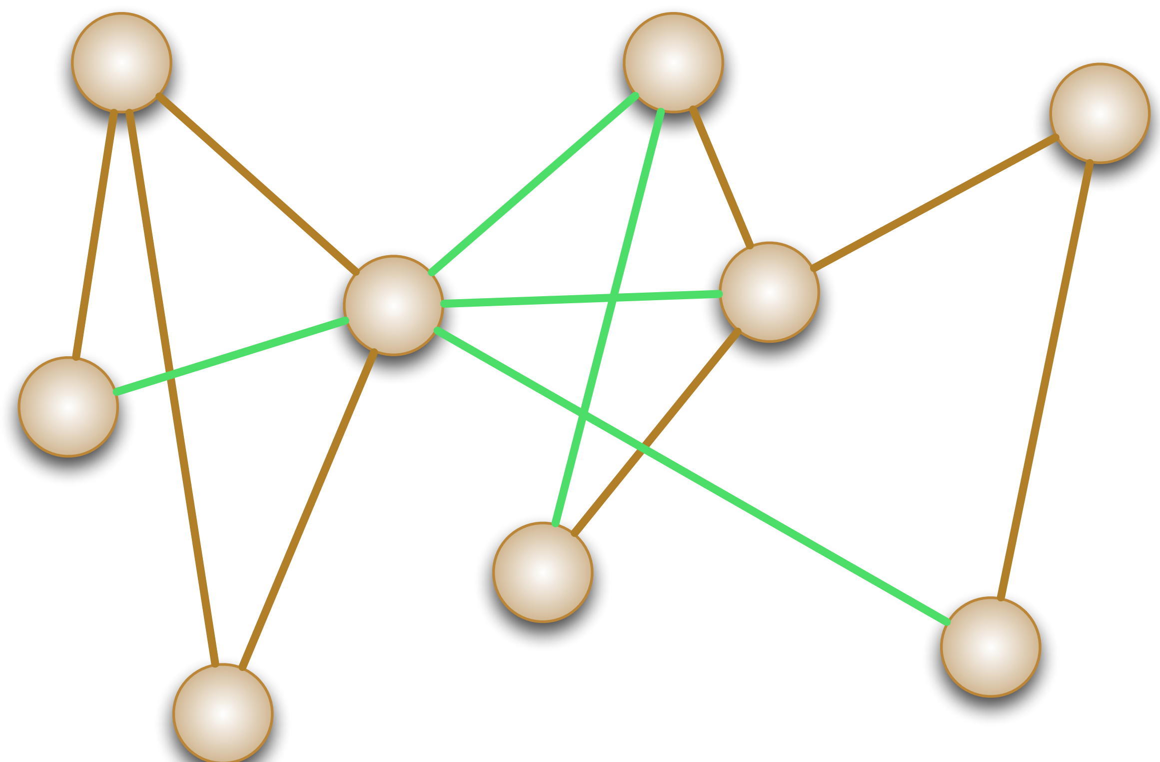


Ordinary percolation model in networks

site percolation



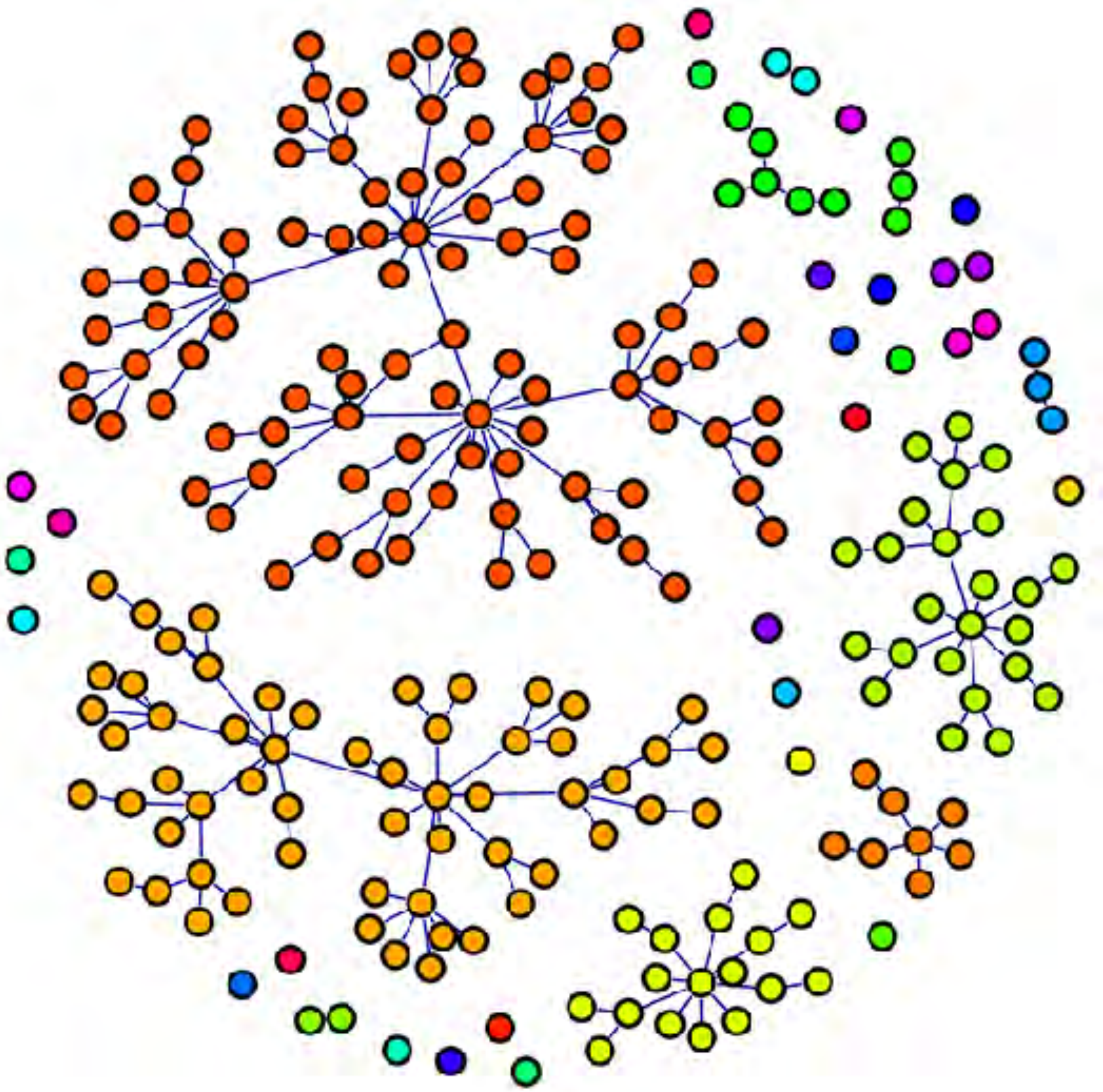
bond percolation



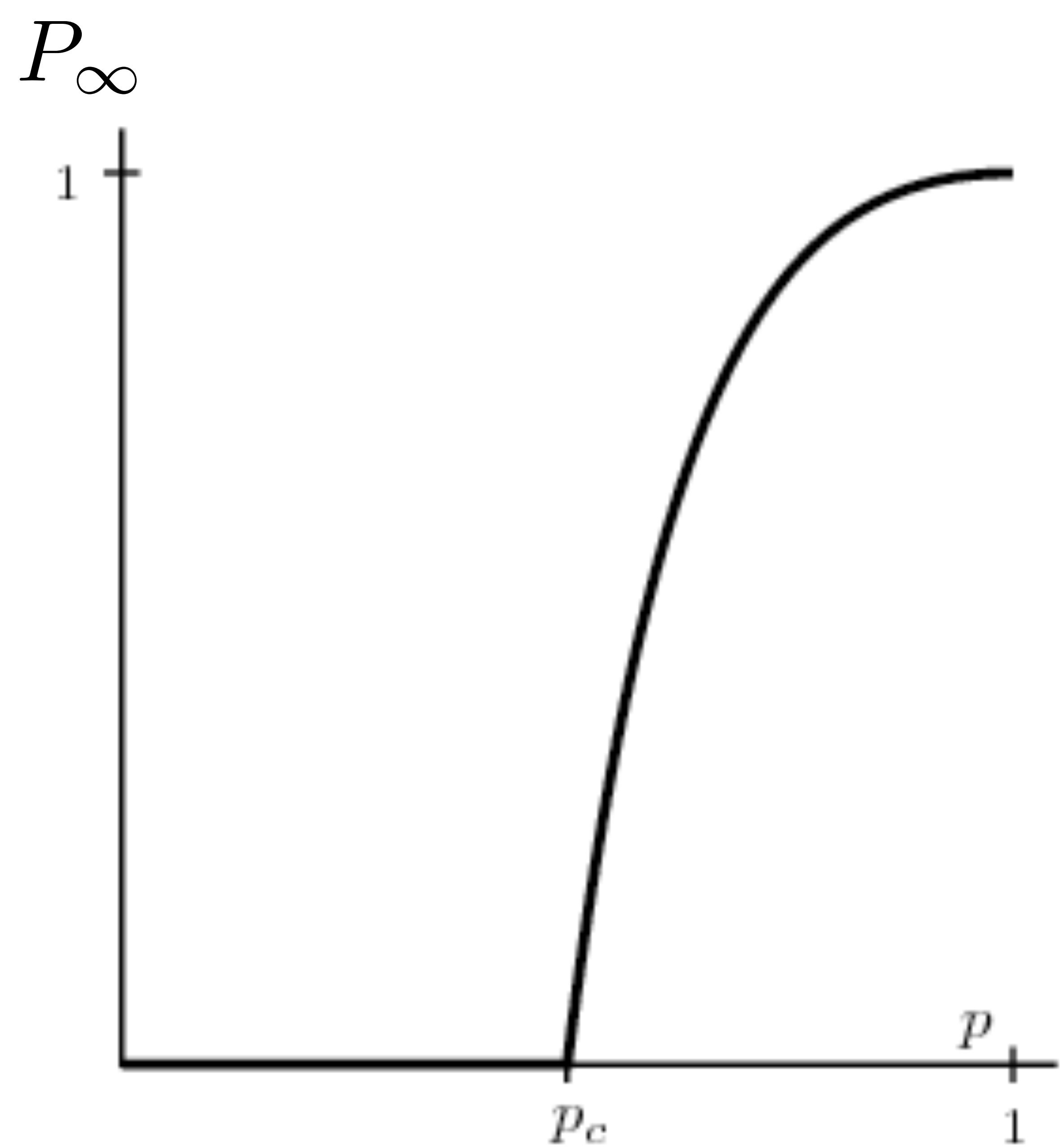
vertices or edges are occupied with probability p

Percolation transition in networks

order parameter = percolation strength

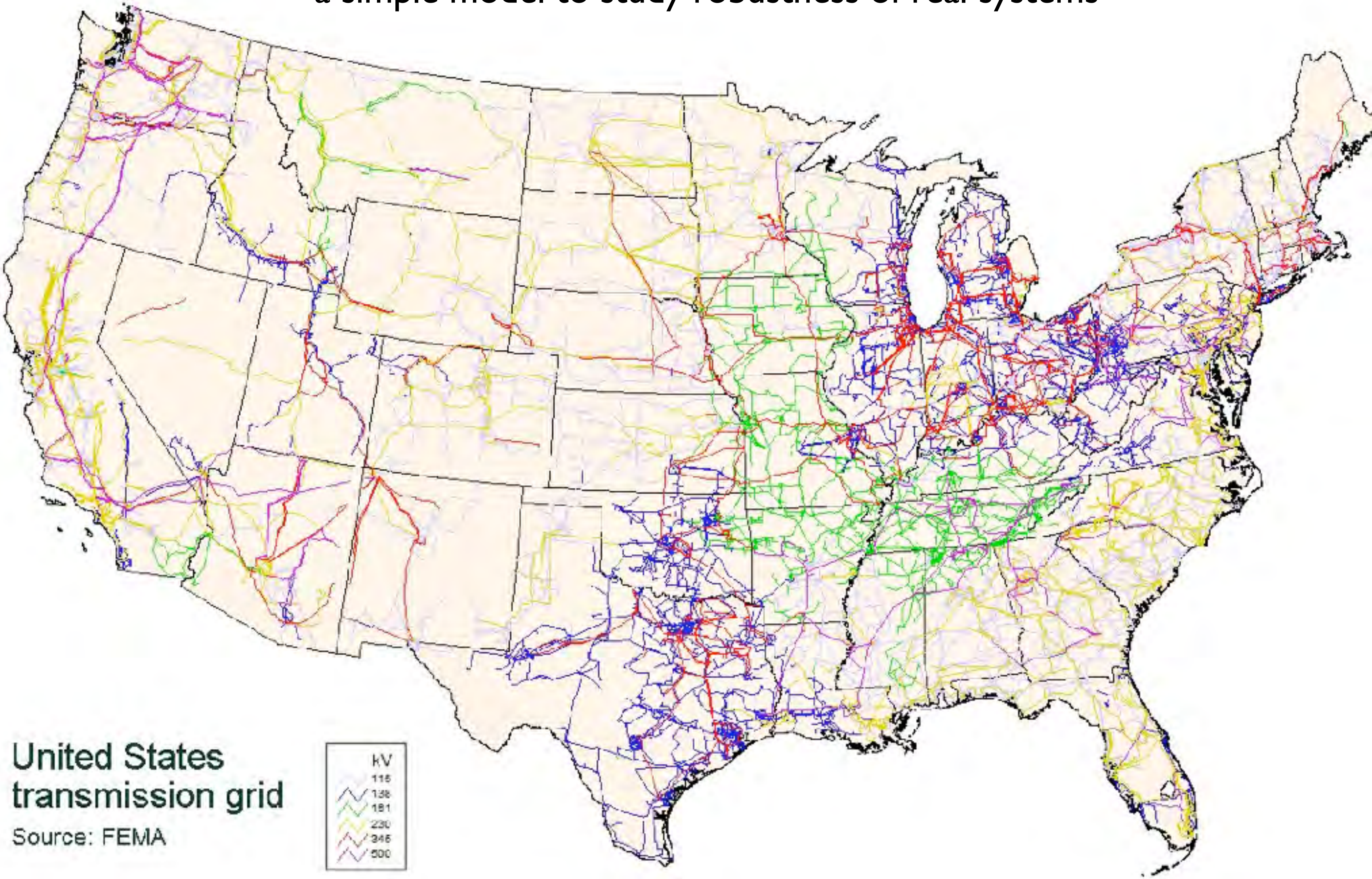


Nature Physics cover, July 2015



Percolation in networks

a simple model to study robustness of real systems

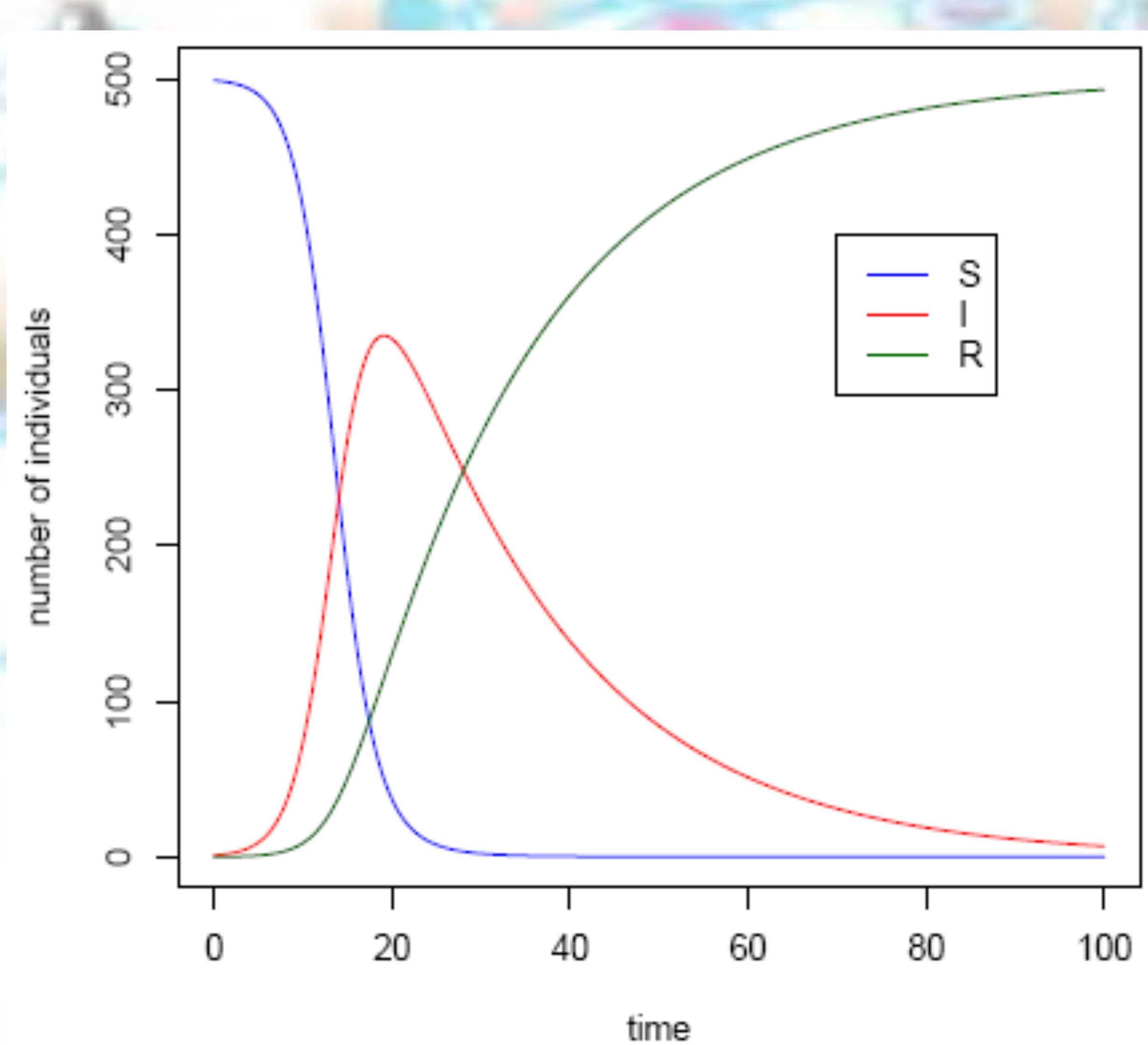


Percolation in networks

a simple model to study robustness of real systems

Percolation in networks

strict analogy with simple epidemiological models



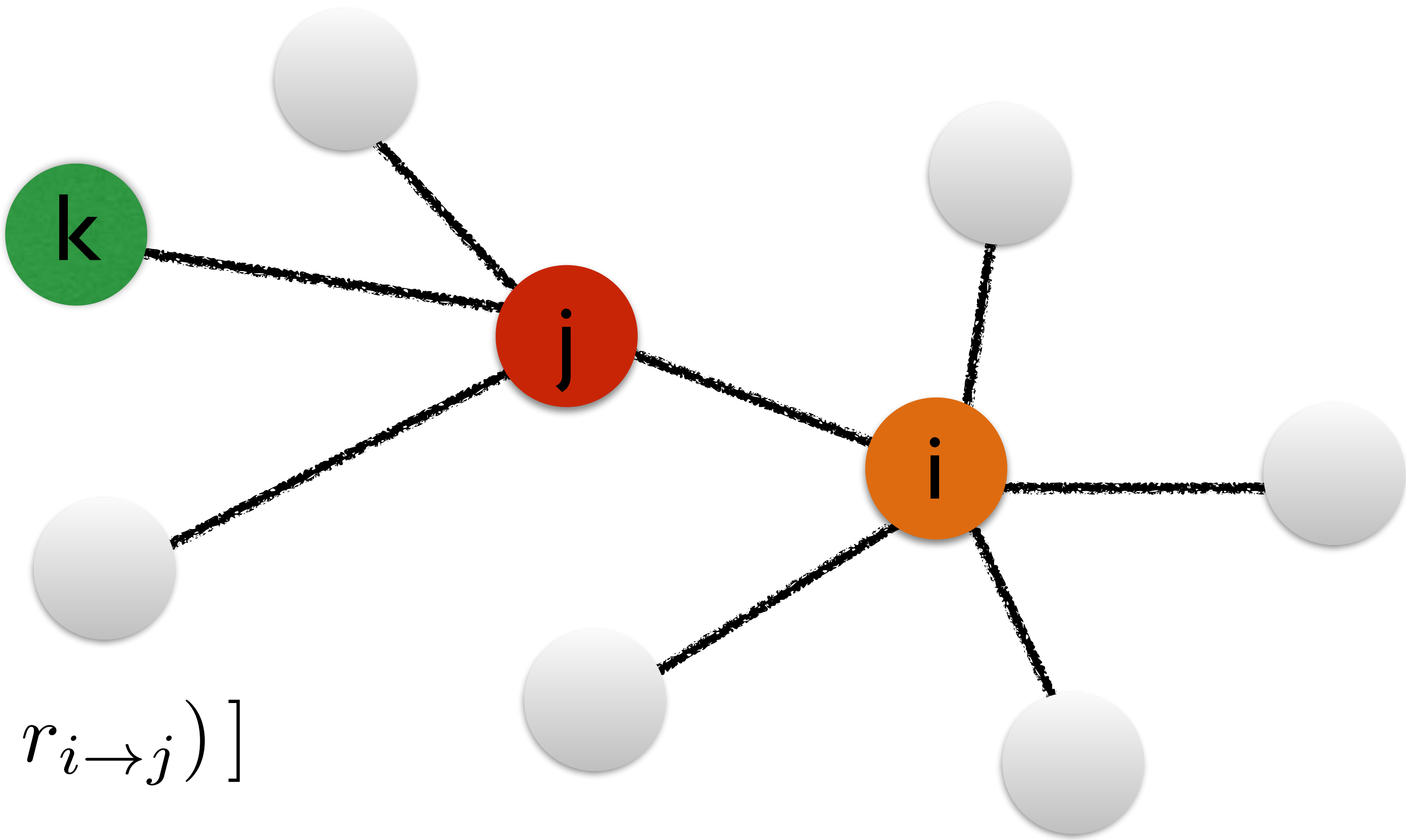
Grassberger, P. On the critical behavior of the general epidemic process and dynamical percolation. Math. Biosci. 63, 157–172 (1983).

Site percolation in real networks

mathematical theory: message passing

s_i = prob. node i in the GC

$r_{i\to j}$ = prob. node j in the GC disregarding node i



$$s_i = p\left[1 - \prod_{j\in\mathcal{N}_i}(1 - r_{i\to j})\right]$$

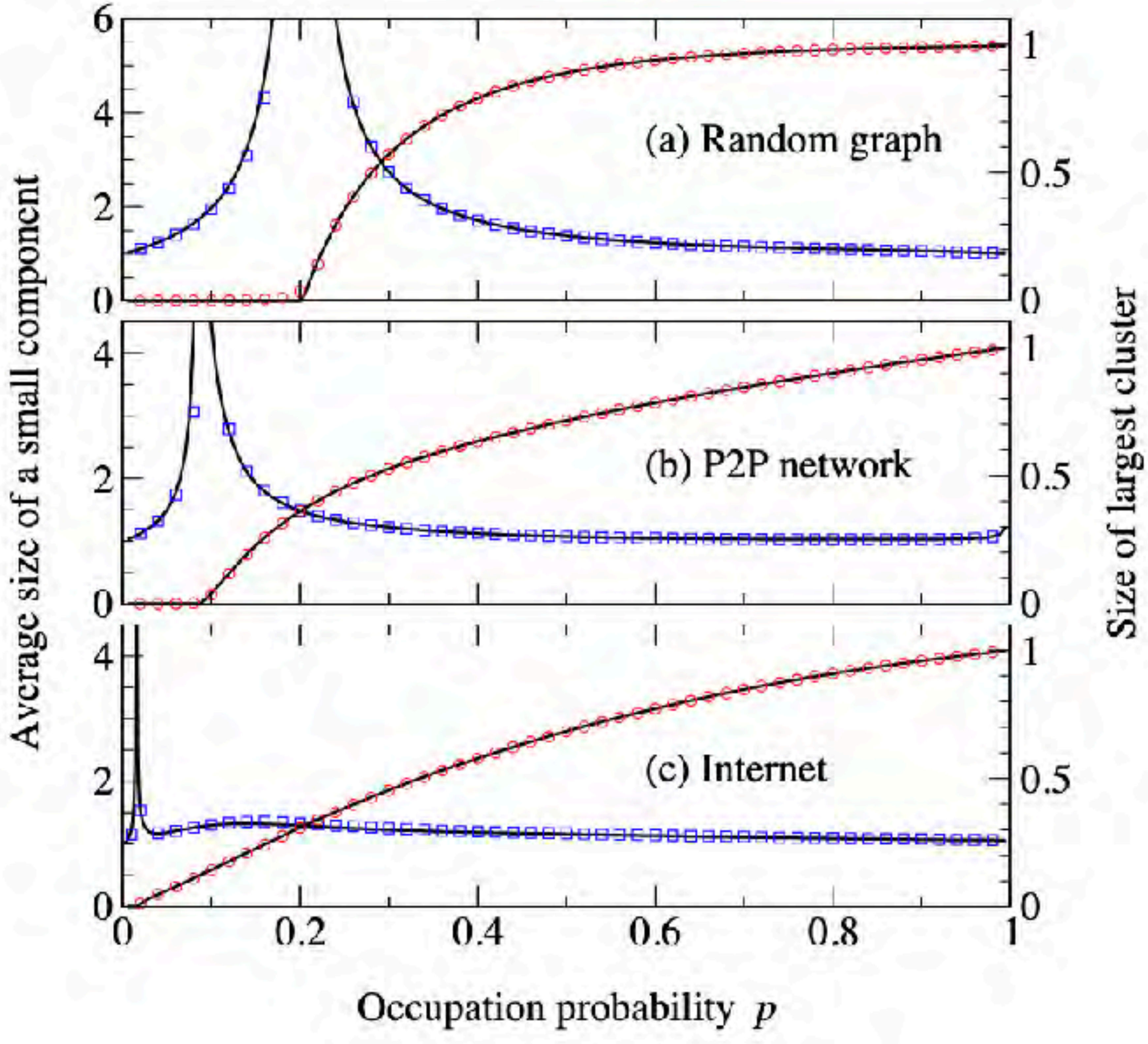
$$r_{i\to j} = p\left[1 - \prod_{k\in\mathcal{N}_j\setminus\{i\}}(1 - r_{j\to k})\right]$$

Karrer, B., Newman, M. E. J. & Zdeborova, L. *Phys. Rev. Lett.* 113, 208702 (2014).

Hamilton, K. E. & Pryadko, L. P. *Phys. Rev. Lett.* 113, 208701 (2014).

Site percolation in real networks

mathematical theory: message passing



Karrer, B., Newman, M. E. J. & Zdeborova, L. *Phys. Rev. Lett.* 113, 208702 (2014).

Hamilton, K. E. & Pryadko, L. P. *Phys. Rev. Lett.* 113, 208701 (2014).

Site percolation in real networks

$$r_{i\to j} = p\,[1 - \prod_{k\in\mathcal{N}_j\setminus\{i\}} (1 - r_{j\to k})\,]$$

$$w_{i\to j} = \ln(1 - r_{i\to j})$$
$$z_{i\to j} = \ln(1 - r_{i\to j}/p)$$
$$M_{i\to j,k\to\ell} = \delta_{j,k}(1 - \delta_{i,\ell})$$

↓

$$\vec{z} = M\,\vec{w}$$

↓

truncated Taylor expansion

$$\ln(1 - x) \simeq -x$$

eigenvalue/eigenvector problem

$$\vec{r} = p\,M\,\vec{r}$$

↓

Perron-Frobenius theorem

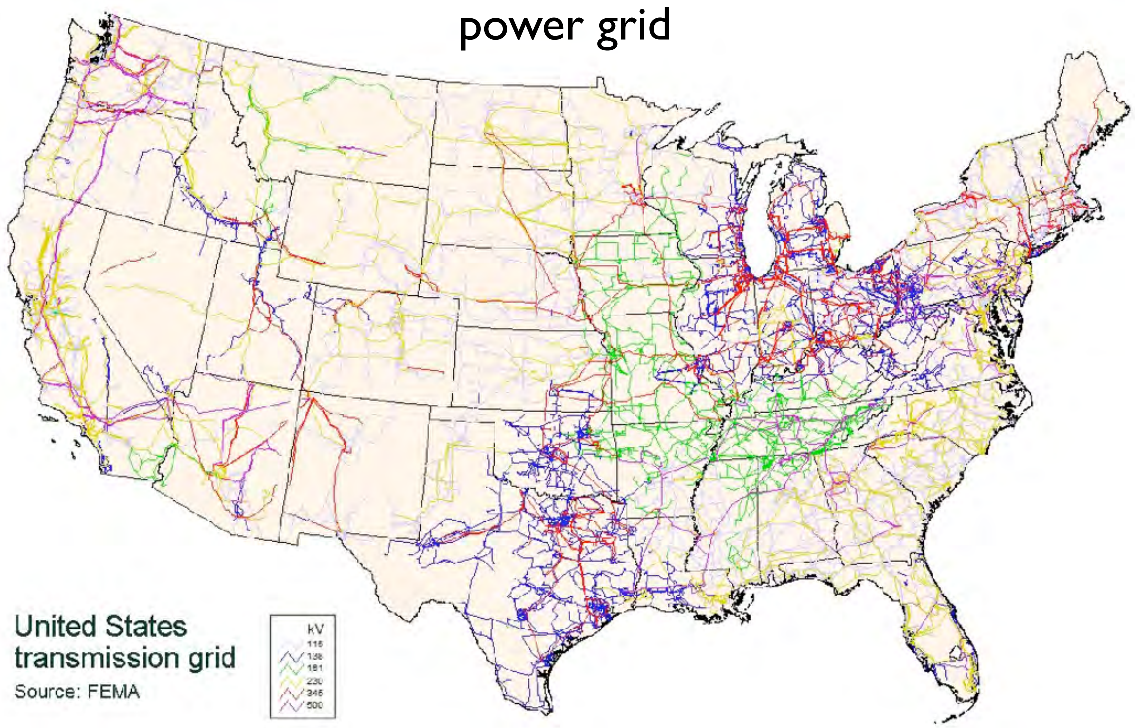
$$p_c = \frac{1}{\mu}$$

Karrer, B., Newman, M. E. J. & Zdeborova, L. *Phys. Rev. Lett.* 113, 208702 (2014).

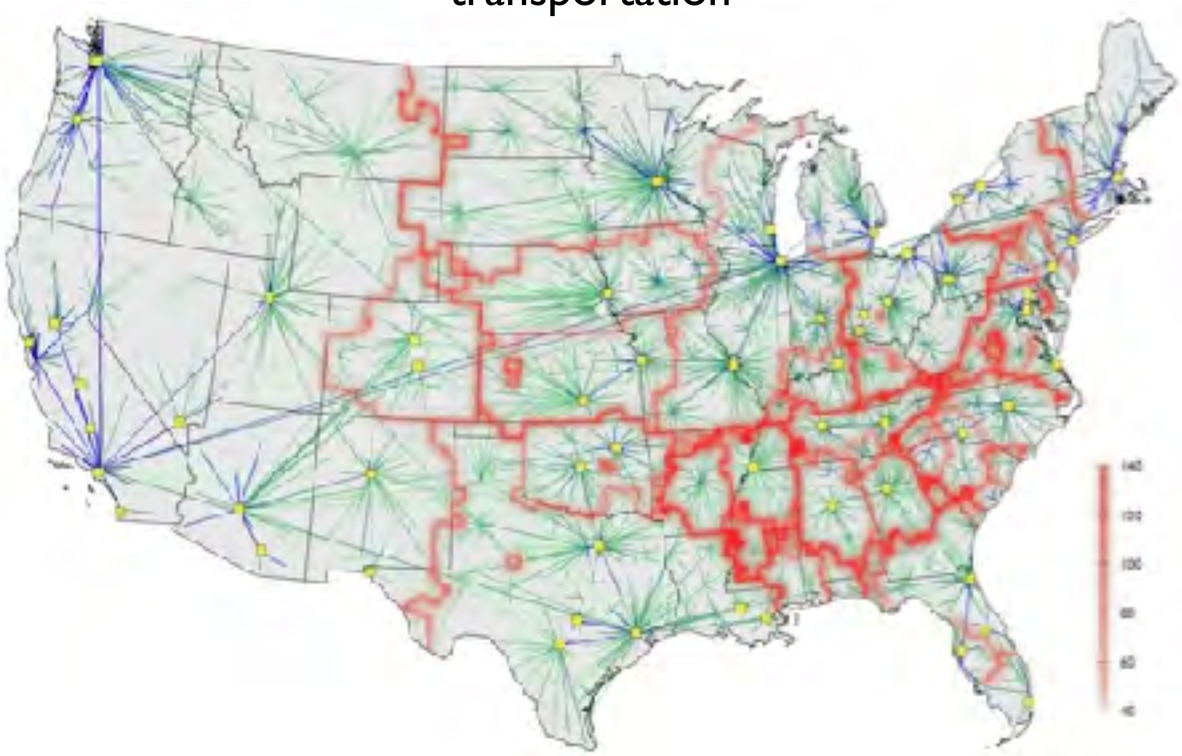
Hamilton, K. E. & Pryadko, L. P. *Phys. Rev. Lett.* 113, 208701 (2014).

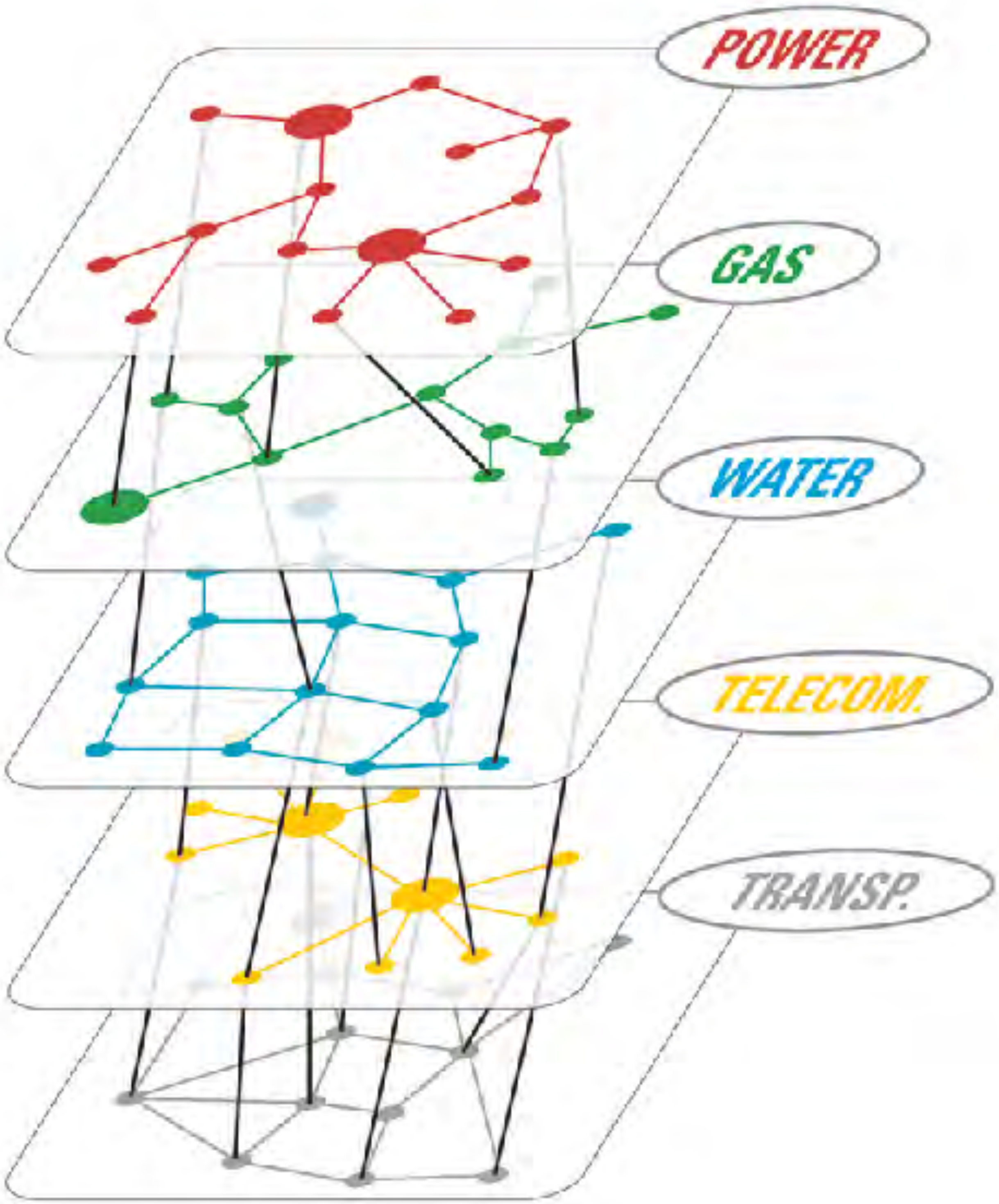
Critical interdependent infrastructures

power grid



transportation





G. D'Agostino and A. Scala. "Networks of Networks: The Last Frontier of Complexity."

La "notte bianca"

Rome, September 27-28, 2003

The darkest night ever!

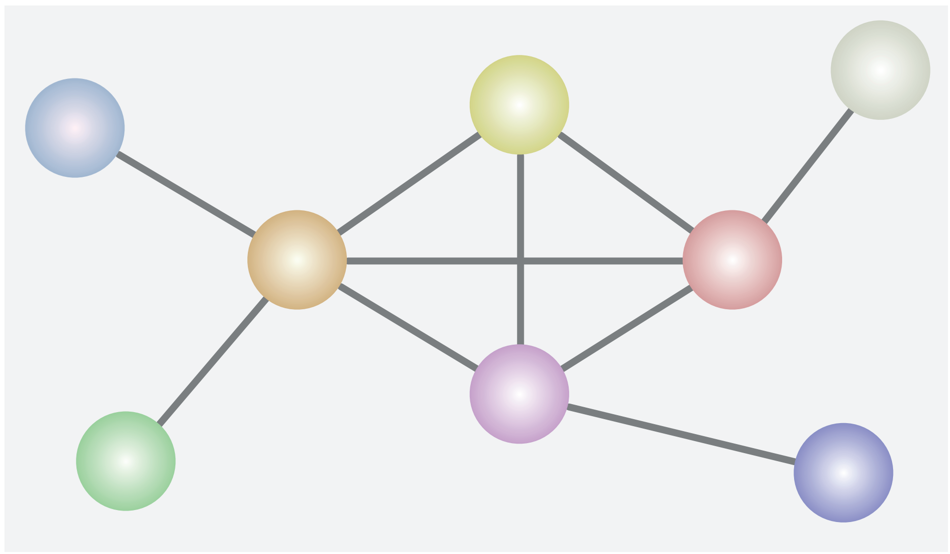
Buldyrev, Sergey V., et al. "Catastrophic cascade of failures in interdependent networks." *Nature* 464.7291 (2010): 1025-1028.

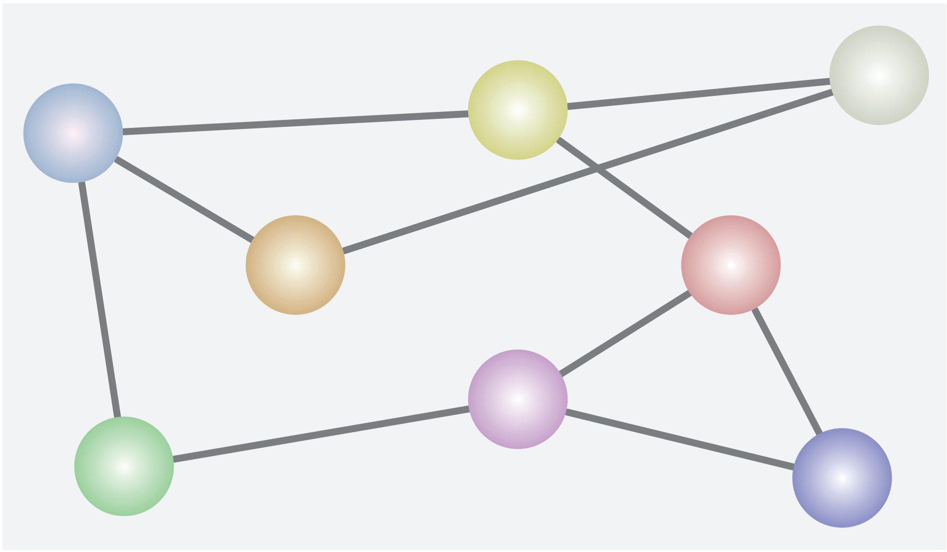
Power grid and the Internet are "interdependent"

A microscopic failure may trigger an avalanche of failures that propagate within and across networks of macroscopic size

Buldyrev, Sergey V., et al. "Catastrophic cascade of failures in interdependent networks." *Nature* 464 (2010): 1025-1028.

Site percolation in interdependent networks





$$s_i = p\left[R_{\mathcal{AB}_i} + \left(1 - R_{\mathcal{AB}_i}\right) R_{\mathcal{A}-\mathcal{B}_i}\, R_{\mathcal{B}-\mathcal{A}_i}\right]$$

$$r_{i\to j} = p\left[R_{\mathcal{AB}_j\setminus\{i\}} + \left(1 - R_{\mathcal{AB}_j\setminus\{i\}}\right) R_{\mathcal{A}-\mathcal{B}_j\setminus\{i\}}\, R_{\mathcal{B}-\mathcal{A}_j\setminus\{i\}}\right]$$

---

where

$$R_{\mathcal{X}_i} = 1 - \prod_{j\in\mathcal{X}} \left(1 - r_{i\to j}\right)$$

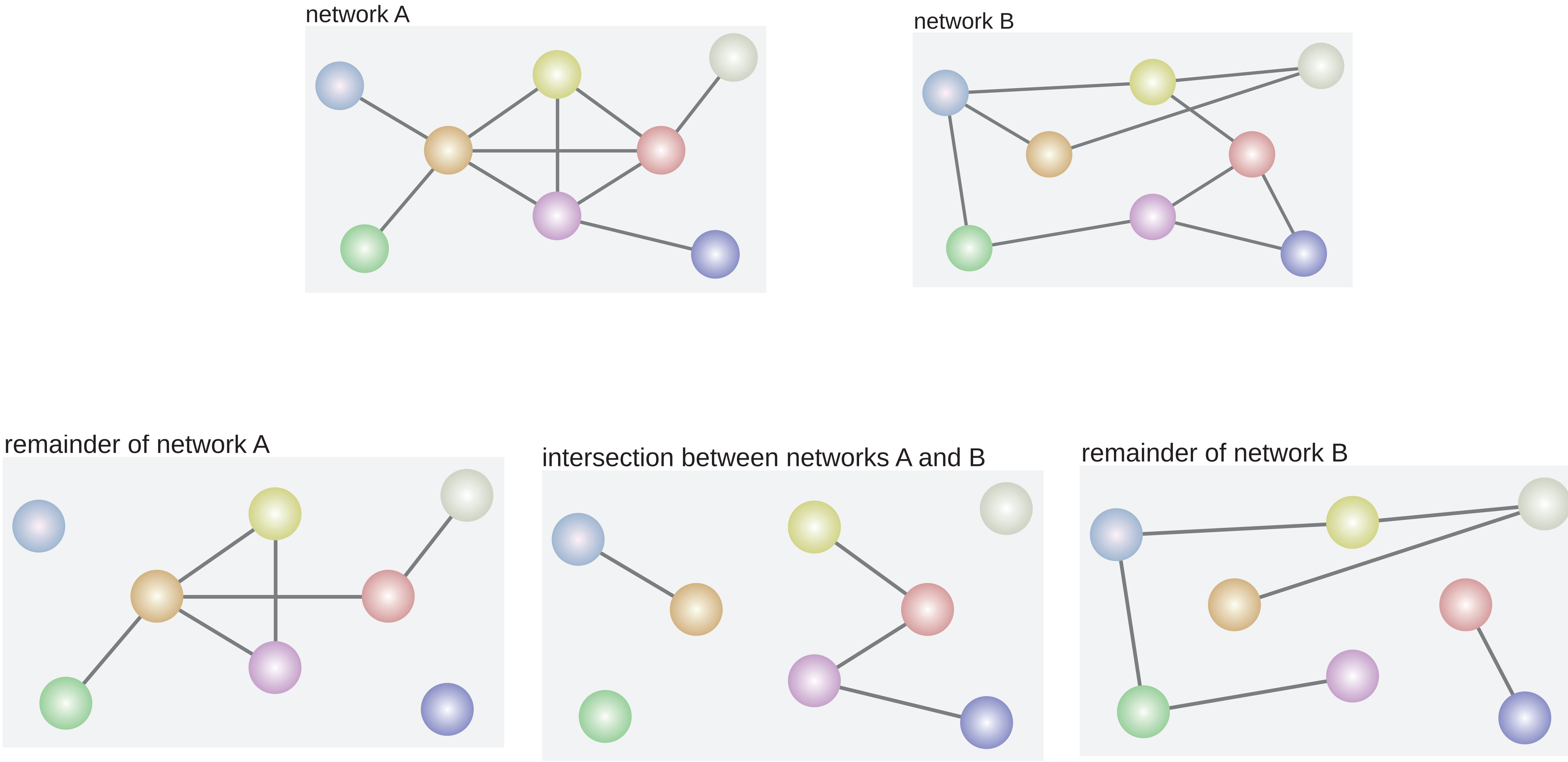
$\mathcal{AB}_i = \mathcal{N}_i^A \cap \mathcal{N}_i^B$ — neigh. in both layers

$\mathcal{A}-\mathcal{B}_i = \mathcal{N}_i^A \setminus \mathcal{AB}_i$ — neigh. only in layer A

$\mathcal{B}-\mathcal{A}_i = \mathcal{N}_i^B \setminus \mathcal{AB}_i$ — neigh. only in layer B

F. Radicchi, Percolation in real interdependent networks, Nature Physics 11, 597-602 (2015)

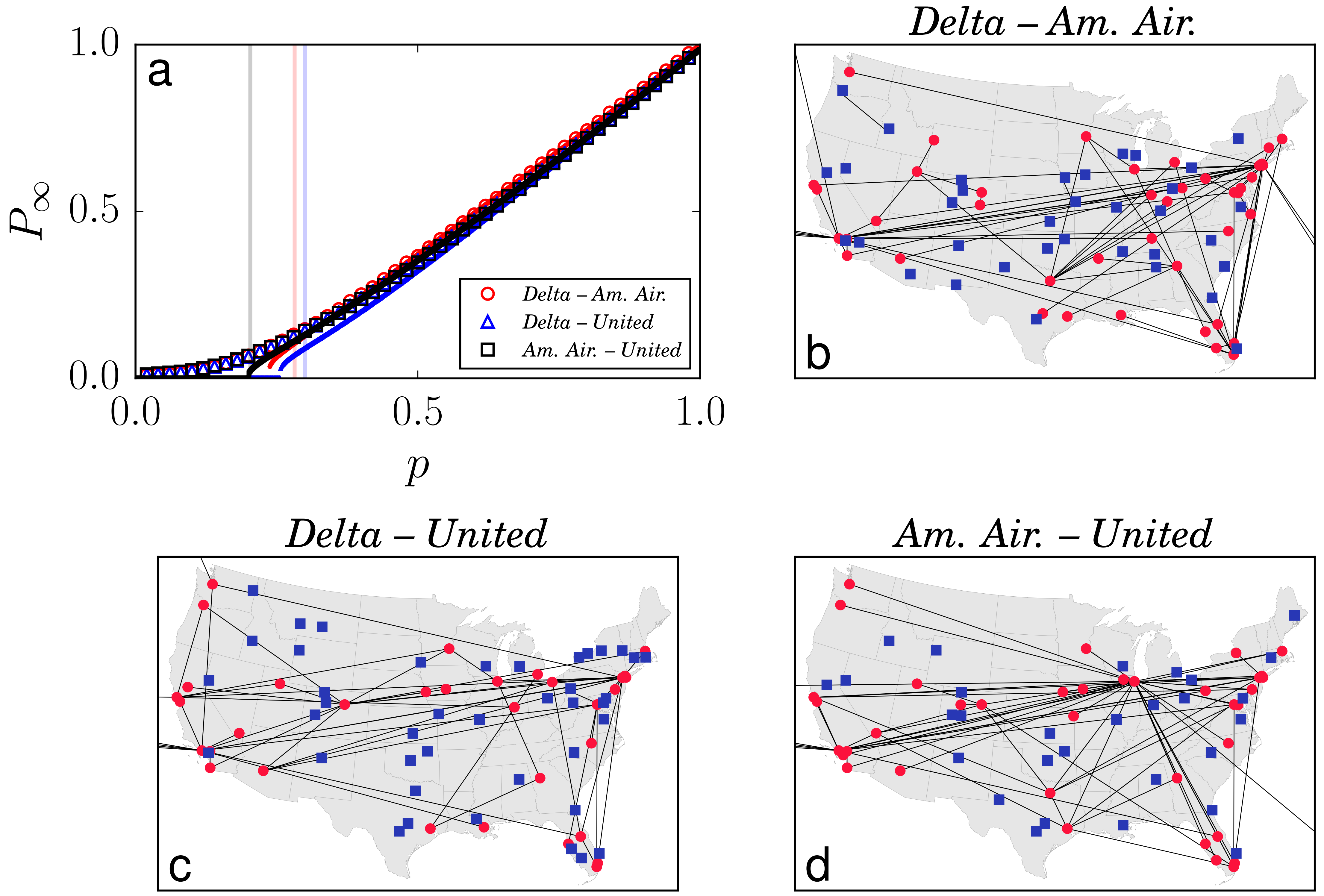
Decomposition of the interdependent network



Cellai,D.,Lopez,E.,Zhou,J.,Gleeson,J.P.&Bianconi,G.Percolation in multiplex networks with overlap. *Phys. Rev. E* 88, 052811 (2013)

Min, B., Lee, S., Lee, K.-M. & Goh, K.-I. Link overlap, viability, and mutual percolation in multiplex networks. *Chaos, Solitons & Fractals* (2015)

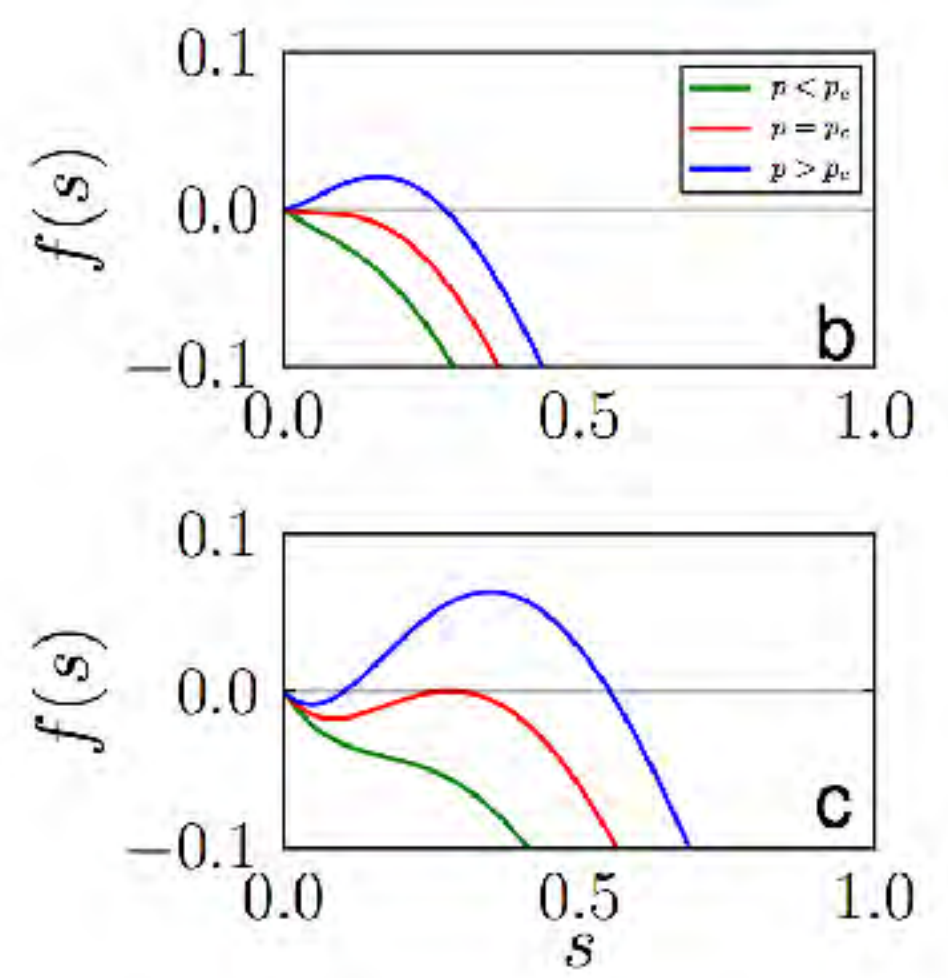
Results on real networks



F. Radicchi, Percolation in real interdependent networks, Nature Physics 11, 597-602 (2015)

What do the equations tell us?

Coupled regular graphs



k = valency of the intersection graph

t = valency of the remainders

$$s = p\left\{1 - (1-r)^k + (1-r)^k[1-(1-r)^t]^2\right\}$$

$$r = p\left\{1 - (1-r)^{k-1} + (1-r)^{k-1}[1-(1-r)^{t-1}]^2\right\}$$

for k = t = 2

$$r = \frac{1 \pm \sqrt{5 - 4/p}}{2} \longrightarrow \quad p_c = 4/5, \quad P_\infty(p_c) = 57/80$$

F. Radicchi, Percolation in real interdependent networks, Nature Physics 11, 597-602 (2015)

Percolation

the “complex systems” approach to assess the robustness of infrastructural networks

Most popular percolation models

ordinary percolation

description: elements of the network are randomly removed with uniform probability

goal: estimate network robustness against random perturbations

targeted attacks

description: elements of the network are removed based on their centrality/importance

goal: estimate network robustness against intentional damage

optimal percolation

description: elements of the are removed to dismantle the network as quickly as possible

goal: estimate network robustness under in a maximal stress scenario

Percolation

the “complex systems” approach to model resource consumption and exhaustion in infrastructural networks

minimum-cost percolation (MCP) model

description: elements of the network are removed if belonging to minimum-cost paths between pairs of demanded origin/destination nodes

goal: estimate the ability of the infrastructure to serve demand until its resources are exhausted

theoretical papers

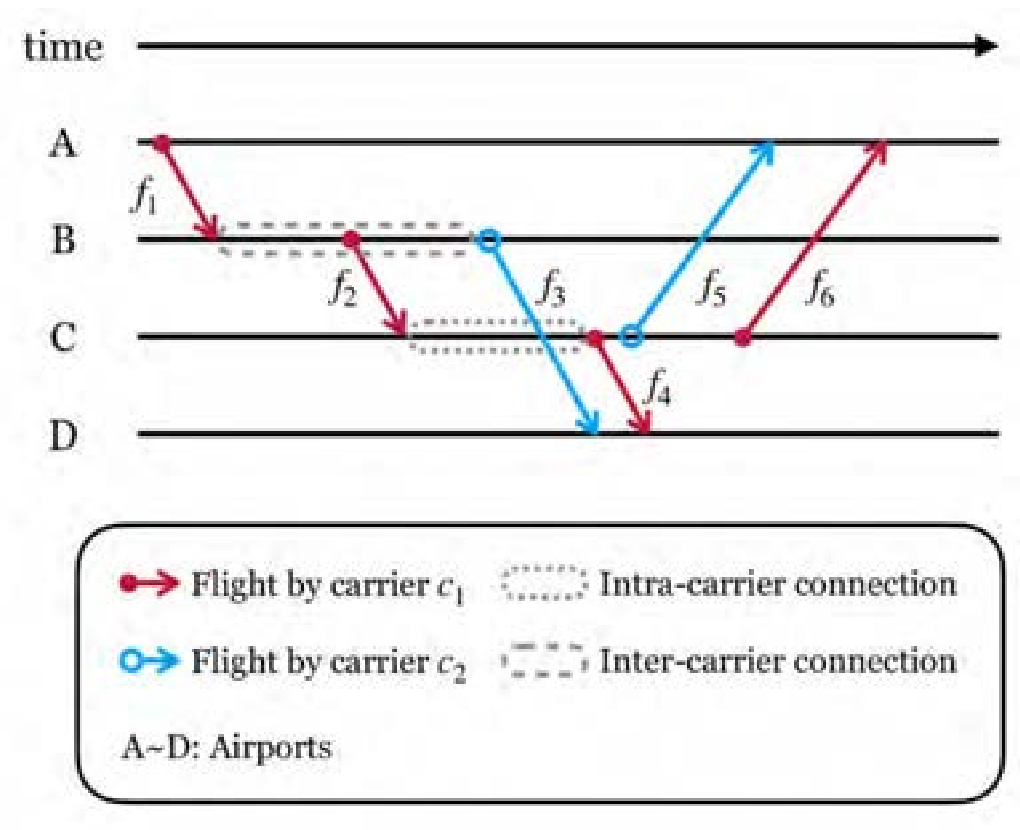
M. Kim and F. Radicchi, Shortest-path percolation on random networks, PRL 2024

M. Kim et al, Shortest-path percolation on scale-free networks, in preparation

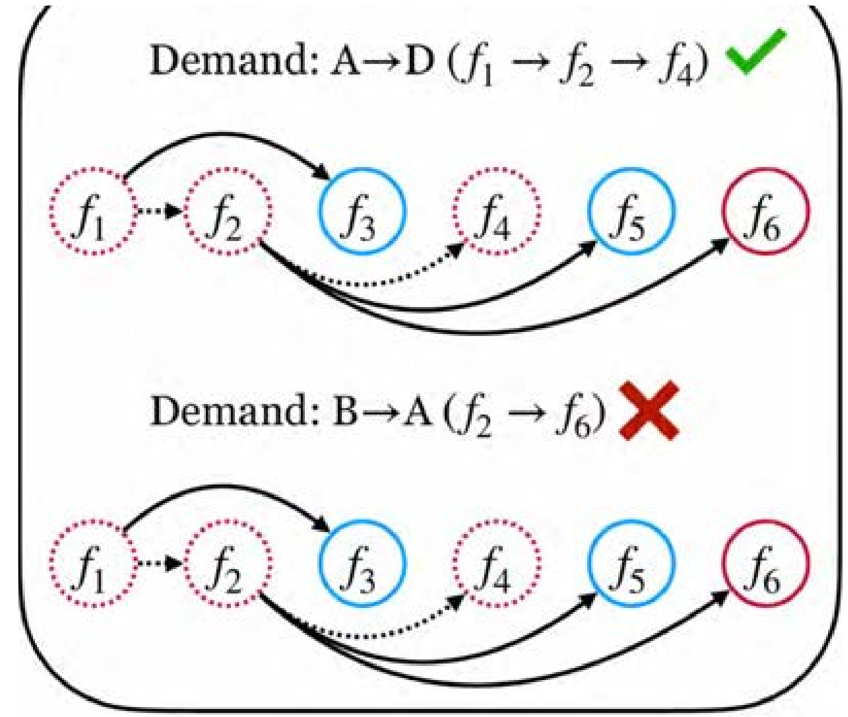
Percolation

application to the US air transportation system

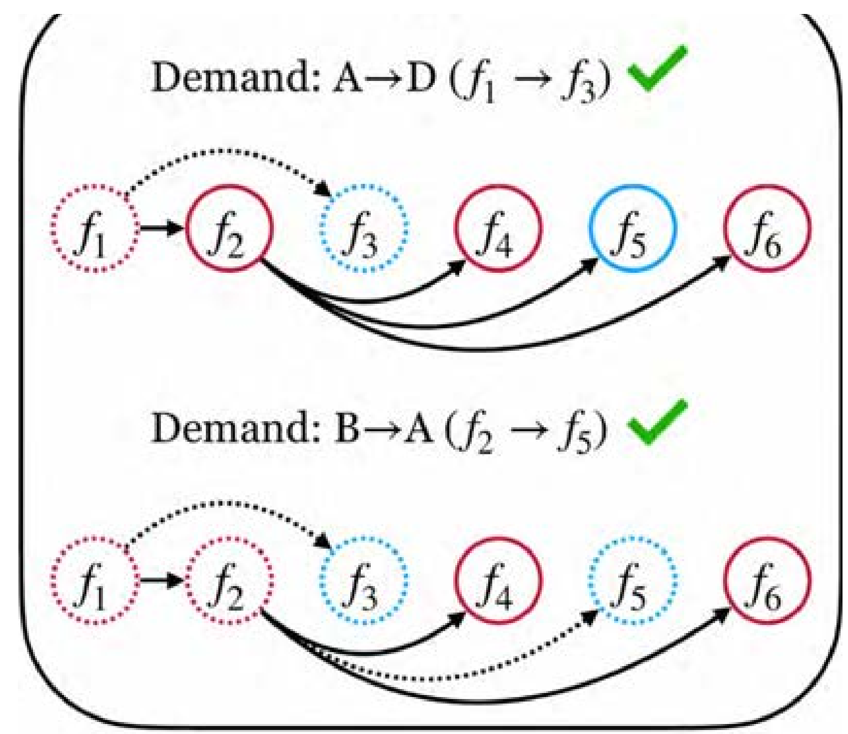
flight schedule

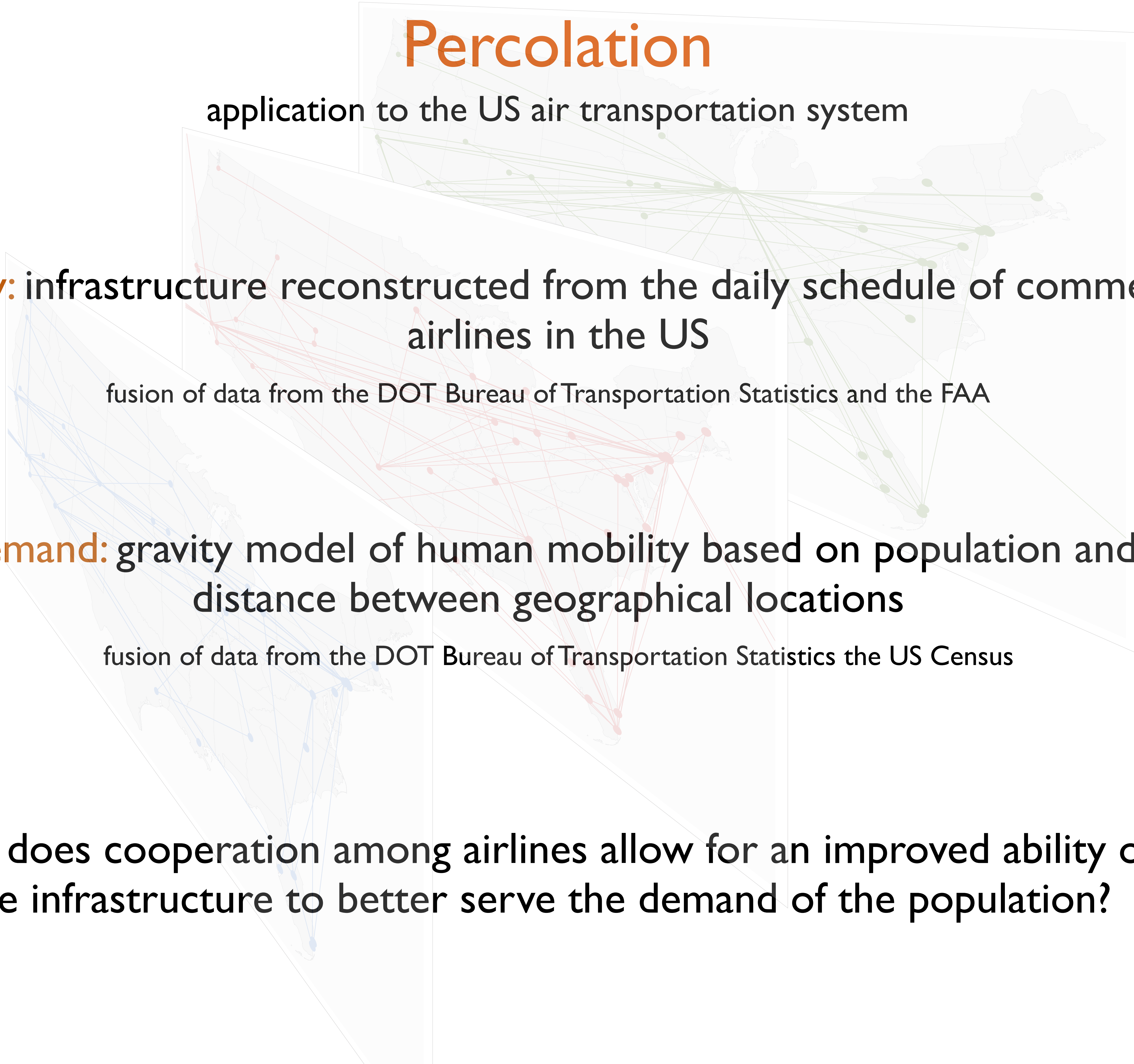


only single-carrier itineraries are allowed



multi-carrier itineraries are allowed too





Percolation

application to the US air transportation system

supply: infrastructure reconstructed from the daily schedule of commercial airlines in the US

fusion of data from the DOT Bureau of Transportation Statistics and the FAA

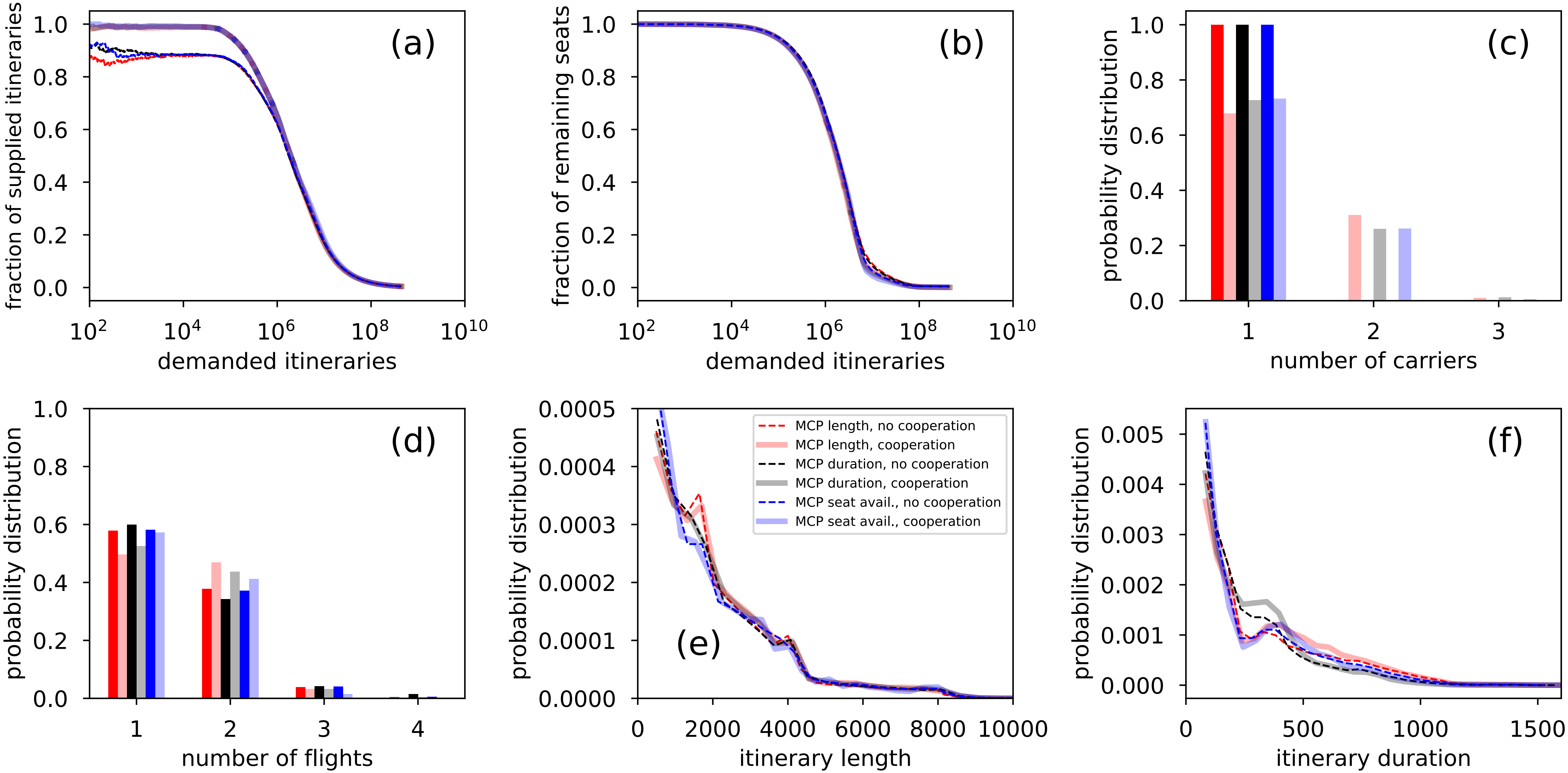
demand: gravity model of human mobility based on population and distance between geographical locations

fusion of data from the DOT Bureau of Transportation Statistics the US Census

goal: does cooperation among airlines allow for an improved ability of the infrastructure to better serve the demand of the population?

Percolation

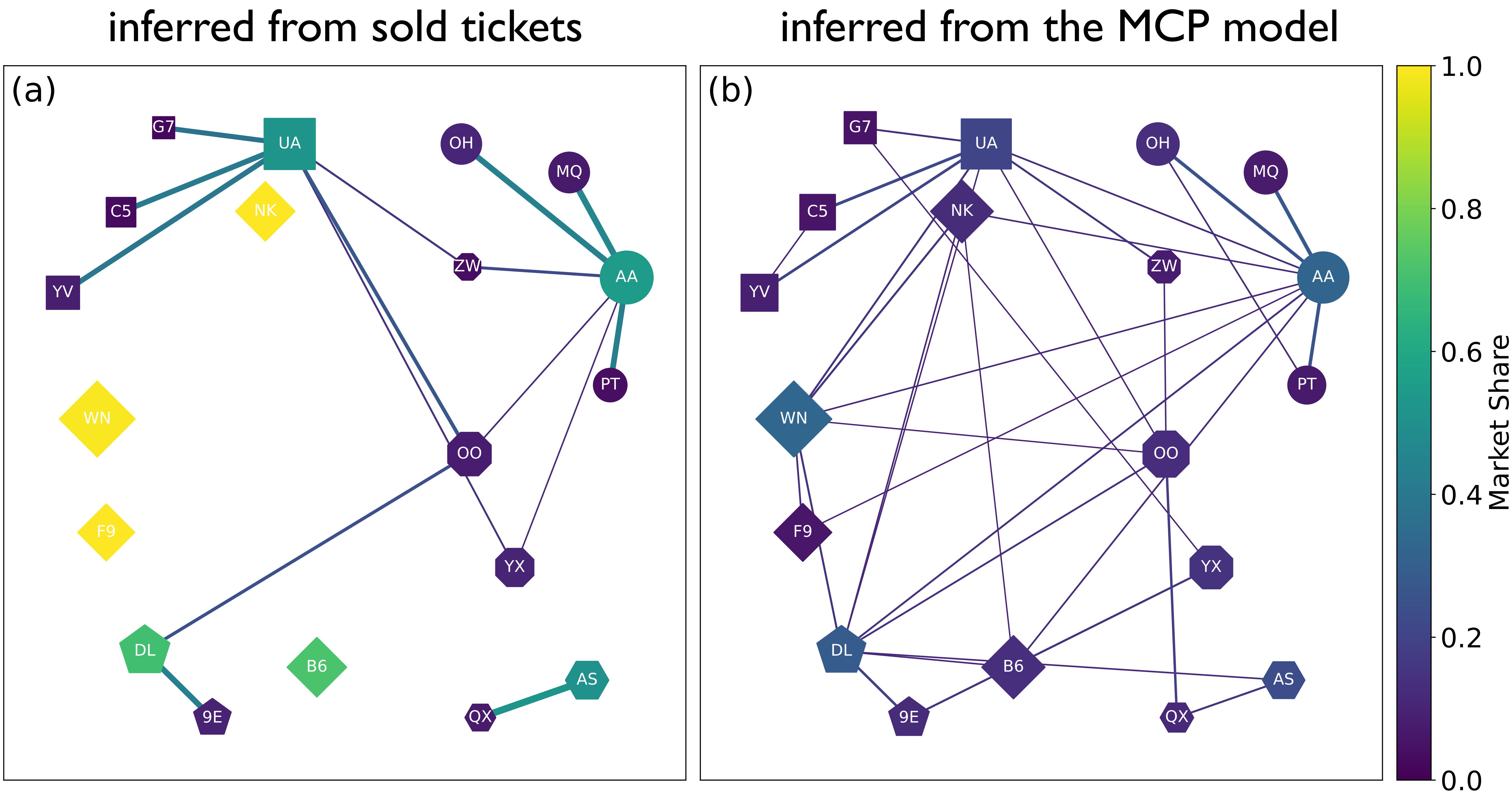
schedule for April 18, 2023



10 % improvement with no increase in the cost of operation

Market-share network

schedule for April 18, 2023



References

from the past 10 years

Shortest-path percolation on random networks
M. Kim and F. Radicchi
Phys. Rev. Lett. 133, 047402 (2024)

Robustness and resilience of complex networks
O. Artime, M. Grassia, M. De Domenico, J.P. Gleeson, H.A. Makse, G. Mangioni, M. Perc and F. Radicchi
Nat. Rev. Phys. 6, 114 (2024)

The dynamic nature of percolation on networks with triadic interactions
H. Sun, F. Radicchi, J. Kurths and G. Bianconi
Nat. Commun. 14, 1308 (2023)

Embedding-aided network dismantling
S. Osat, F. Papadopoulos, A.S. Teixeira, and F. Radicchi
Phys. Rev. Research 5, 013076 (2023)

k-core structure of real multiplex networks
S. Osat, F. Radicchi and F. Papadopoulos
Phys. Rev. Research 2, 023176 (2020)

Controlling the uncertain response of real multiplex networks to random damage
F. Coghi, F. Radicchi and G. Bianconi
Phys. Rev. E 98, 062317 (2018)

Characterizing the analogy between hyperbolic embedding and community structure of complex networks
A. Faqeeh, S. Osat and F. Radicchi
Phys. Rev. Lett. 121, 098301 (2018)

Observability transition in multiplex networks
S. Osat and F. Radicchi
Physica A 503, 745-761 (2018)

Optimal percolation on multiplex networks
S. Osat, A. Faqeeh and F. Radicchi
Nat. Commun. 8, 1540 (2017)

Redundant interdependencies boost the robustness of multilayer networks
F. Radicchi and G. Bianconi
Phys. Rev. X 7, 011013 (2017)

Percolation in real multiplex networks
G. Bianconi and F. Radicchi
Phys. Rev. E 94, 060301(R) (2016)

Observability transition in real networks
Y. Yang and F. Radicchi
Phys. Rev. E 94, 030301(R) (2016)

Breaking of the site-bond percolation universality in networks
F. Radicchi and C. Castellano
Nat. Commun. 6, 10196 (2015)

Percolation in real interdependent networks
F. Radicchi
Nat. Phys. 11, 597-602 (2015)

Predicting percolation thresholds in networks
F. Radicchi
Phys. Rev. E 91, 010801(R) (2015)

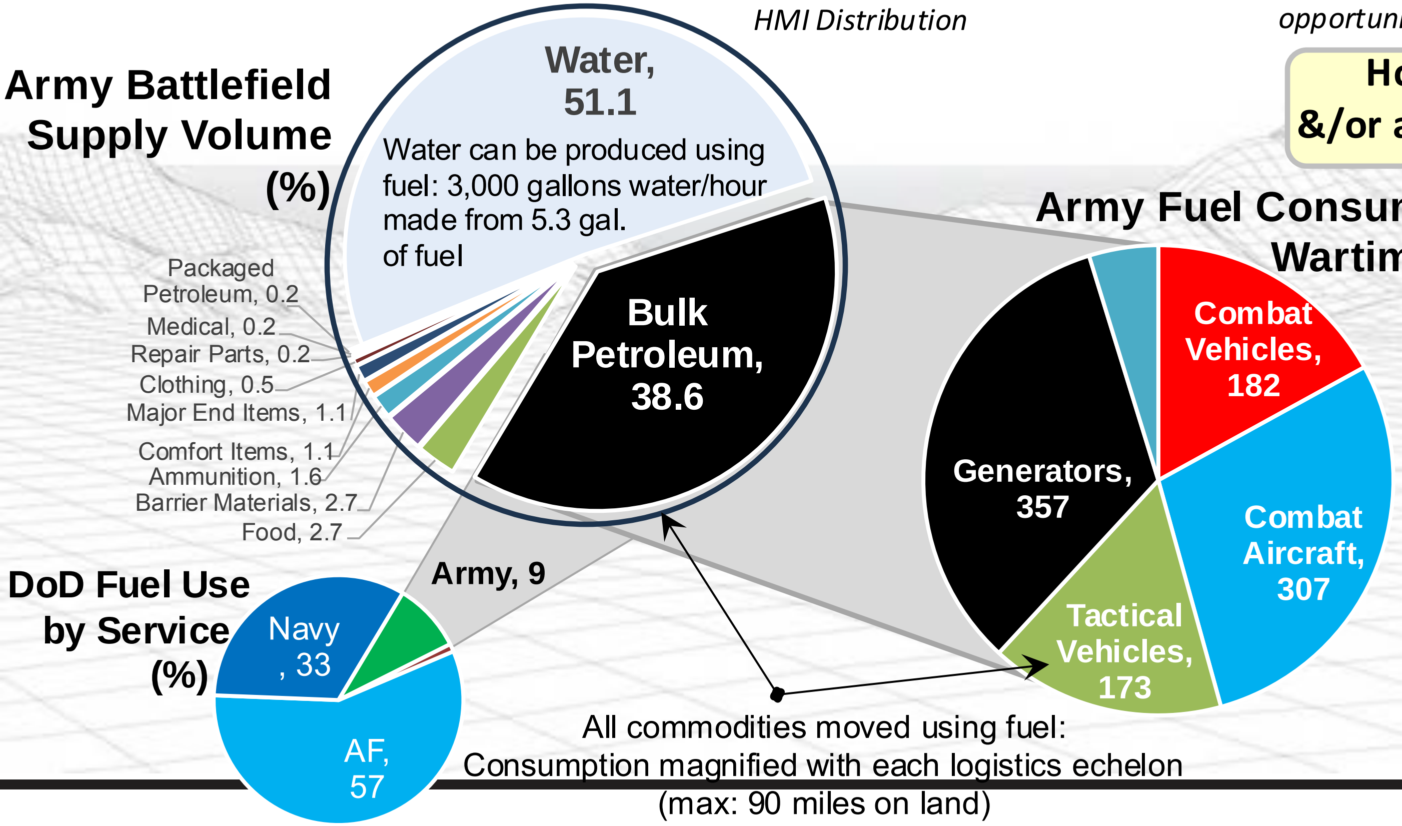
plus some additional manuscripts that will be soon finalized

Contested Logistics Problem

How to provide resources soldiers need to win in an environment where they are under layers of constant observation, prolific precision guided fires; with denied, degraded, intermittent, and limited communications and sensors; and across vast distances, challenging environmental conditions, and across multiple domains?

How to know where resources are needed most → **How to bring in outside resources** → **How to safely and accurately distribute resources** → **Need resources to operate** → **Need to operate**

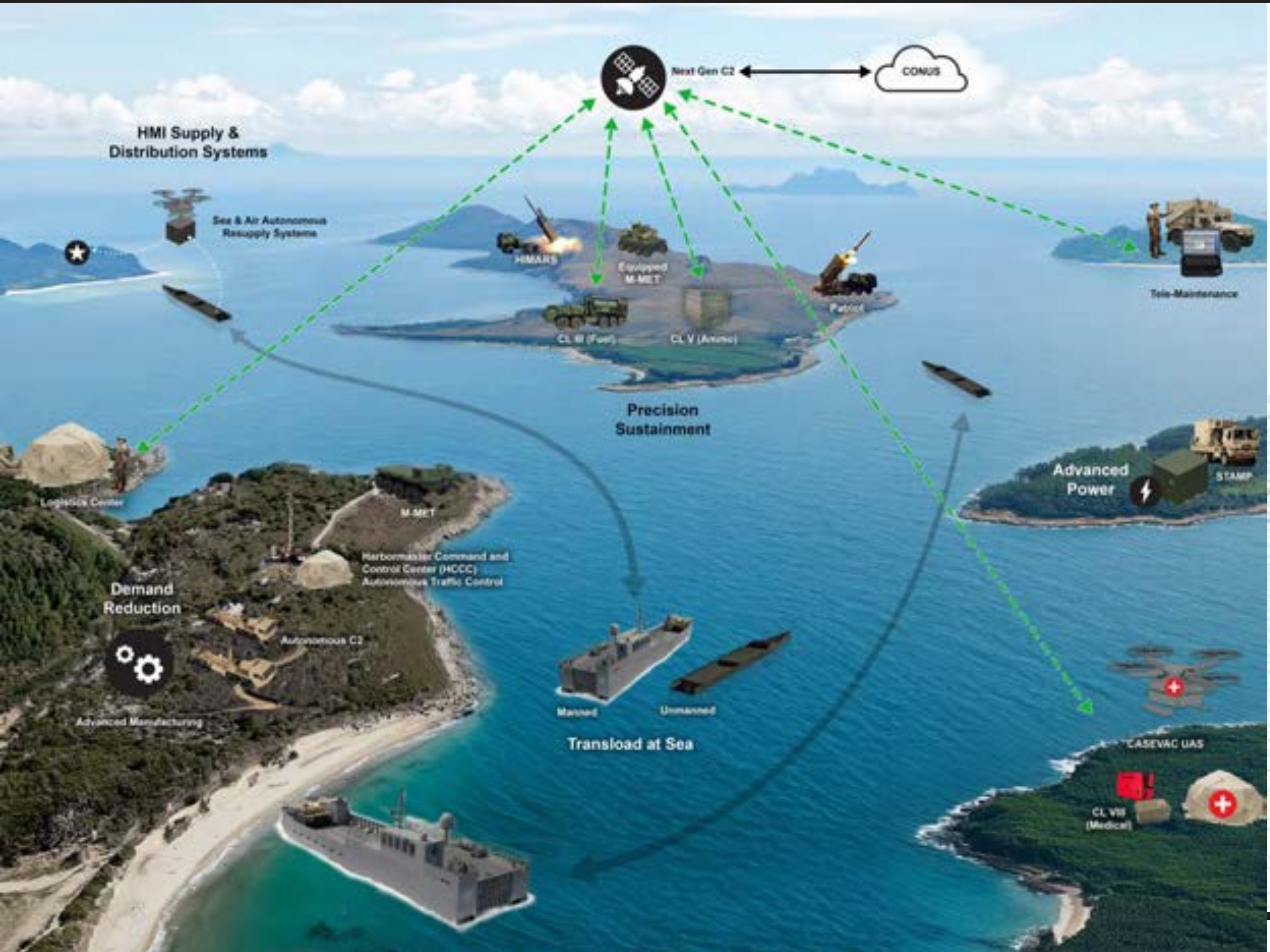
- How to know where resources are needed most — *Predictive Logistics*
- How to bring in outside resources — *long range delivery HMI Distribution*
- *Offset distribution risk*
- How to safely and accurately distribute resources — *Precision Sustainment & HMI Distribution avoid opportunity cost*
- Need resources to operate — *"35MM" **Fuel**, ammunition Maintenance, medical*
- Need to operate — *Freedom of action, operational reach, endurance*
- *Resilience* — **How to have multiple options or operate without**
- **How to use Local &/or alternate resources**
- **How to reduce resources needed** — *Demand Reduction--efficiency*



- 52% of OIF casualties in land transportation missions (mostly fuel); risk offset to contractors
- Batteries are an insignificant part of energy and transportation load but 15-20% of dismounted soldier combat load is batteries
- Power generation is the biggest fuel consumer on the battlefield
- Ammunition can be extremely time sensitive
- Repair parts: challenge of delivering the specific part needed to the specific user who needs it. A simple part can keep a critical system from being used, may become a mobility burden on the unit or lost altogether.
- Medical supplies: time sensitive and perishable.

Jonathan E. Jeckell, Contested Logistics CFT jon.e.jeckell.civ@army.mil

Contested Logistics Cross Functional Team CONOP



Predictive Logistics/Precision Sustainment:

How do we utilize key logistics and medical supply data to make better and faster decisions and provide more options for the means and mode of distribution? This includes helping commanders compare options and understand the long-term consequences of each option and anticipate requirements early enough to mitigate long shipping times.

Precision Sustainment delivers precisely what is needed, minimizing opportunity cost in materiel and distribution opportunities.

Human-Machine Integrated Re-supply:

How do we autonomously distribute critical supplies (ammo, fuel, maintenance, medical) to land-based formations dispersed over extreme distances in a contested environment, independent of stationary or fixed facilities?

Advanced Power:

How to reduce transportation requirements and risk from delivery of consumable liquid fuels and batteries into a contested environment.

Demand Reduction:

How do we reduce the frequency of & demand for resupply & distribution of critical supplies (ammo, fuel, maintenance, medical)

Jonathan E. Jeckell, Contested Logistics CFT jon.e.jeckell.civ@army.mil