Game Theoretic Issues in Security of CPS

D. Teneketzis
University of Michigan
Joint work with H. Tavafoghi, Y. Ouyang

January 2017

Outline

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Outline

- Salient features of CPS' security

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Outline

- Salient features of CPS' security
- Key sources of difficulties in stochastic dynamic games with asymmetric information (SDGAS)

Outline

- Salient features of CPS' security
- Key sources of difficulties in stochastic dynamic games with asymmetric information (SDGAS)
- Challenges/Consequences of Difficulties

Outline

- Salient features of CPS' security
- Key sources of difficulties in stochastic dynamic games with asymmetric information (SDGAS)
- Challenges/Consequences of Difficulties
- State-of-the-art in SDGAS

Outline

- Salient features of CPS' security
- Key sources of difficulties in stochastic dynamic games with asymmetric information (SDGAS)
- Challenges/Consequences of Difficulties
- State-of-the-art in SDGAS
  - Our contribution

Outline

- Salient features of CPS' security
- Key sources of difficulties in stochastic dynamic games with asymmetric information (SDGAS)
- Challenges/Consequences of Difficulties
- State-of-the-art in SDGAS
  - Our contribution
- Open research issues/problems in SDGAS for CPS security

Salient Features of CPS' Security

Salient Features of CPS' Security

- Many agents/decision markers (DMS) with asymmetric information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Salient Features of CPS' Security

- Many agents/decision markers (DMS) with asymmetric information
- Many agents/DMs with different objectives

Salient Features of CPS' Security

- Many agents/decision markers (DMS) with asymmetric information
- Many agents/DMs with different objectives
- CPS are stochastic dynamic systems, thus security status of CPS evolves dynamically over time.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Salient Features of CPS' Security

- Many agents/decision markers (DMS) with asymmetric information
- Many agents/DMs with different objectives
- CPS are stochastic dynamic systems, thus security status of CPS evolves dynamically over time.
  - Security status of CPS is affected by the DMs' actions.

Salient Features of CPS' Security

- Many agents/decision markers (DMS) with asymmetric information
- Many agents/DMs with different objectives
- CPS are stochastic dynamic systems, thus security status of CPS evolves dynamically over time.
  - Security status of CPS is affected by the DMs' actions.

- All features => Stochastic Dynamic Games with Asymmetric Information (SDGAS)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Illustrative Example

Energy System

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Two agents

Illustrative Example

Energy System

- Two agents
  - Attacker (A)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology
    - (D) knows location of critical information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology
    - (D) knows location of critical information
    - (D) does not perfectly know network’s security status

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology
    - (D) knows location of critical information
    - (D) does not perfectly know network’s security status
    - (A) does not know network topology

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology
    - (D) knows location of critical information
    - (D) does not perfectly know network's security status
    - (A) does not know network topology
    - (A) does not know location of critical information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Two agents
  - Attacker (A)
  - Defender (D)
- Asymmetric Information
  - On Cyber components
    - (D) knows network's topology
    - (D) knows location of critical information
    - (D) does not perfectly know network’s security status
    - (A) does not know network topology
    - (A) does not know location of critical information
    - (A) knows the components of the network (computers) it has under control

Illustrative Example

Illustrative Example

Energy System

Illustrative Example

Energy System

- Asymmetric Information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines
    - (D) knows control architecture/active devices

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines
    - (D) knows control architecture/active devices
    - (A) has incomplete information of above

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines
    - (D) knows control architecture/active devices
    - (A) has incomplete information of above
    - (A) can compromise a sensor, inject false data in automatic generation controller

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines
    - (D) knows control architecture/active devices
    - (A) has incomplete information of above
    - (A) can compromise a sensor, inject false data in automatic generation controller
    - (D) does not perfectly know what part of network was attacked

Illustrative Example

Energy System

- Asymmetric Information
  - On physical component
    - (D) knows interconnection of machines
    - (D) knows control architecture/active devices
    - (A) has incomplete information of above
    - (A) can compromise a sensor, inject false data in automatic generation controller
    - (D) does not perfectly know what part of network was attacked
    - (D) may see effects of attack but does not see the origin (fault or malicious)

Illustrative Example

Illustrative Example

Energy System

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)
- Different Objectives

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)
- Different Objectives
  - (A) and (D) have different partially conflicting objectives

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)
- Different Objectives
  - (A) and (D) have different partially conflicting objectives
  - (D) => to protect CPS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)
- Different Objectives
  - (A) and (D) have different partially conflicting objectives
  - (D) => to protect CPS
  - (A) => to damage CPS and get information about CPS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Illustrative Example

Energy System

- Asymmetric Information
  - (A) and (D) partially observe each others' actions
  - (A)'s and (D)'s information depends on the strategies employed by (A) and (D)
- Different Objectives
  - (A) and (D) have different partially conflicting objectives
  - (D) => to protect CPS
  - (A) => to damage CPS and get information about CPS
- Features => SDGAS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

Key Sources of Difficulties in SDGAS

- Asymmetric information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

$\Rightarrow$Agent's strategies are their own private information

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

$\Rightarrow$Agent’s strategies are their own private information

- Notation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

  $\Rightarrow$Agent's strategies are their own private information

- Notation
  - P_t^i:= Agent i's private information at t

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

$\Rightarrow$ Agent's strategies are their own private information

- Notation
  - P_t^i:= Agent i's private information at t
  - C_t:= Agents' common information at t

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Key Sources of Difficulties in SDGAS

- Asymmetric information
  - Agents have private information (and common information)
- Different objectives

$\Rightarrow$ Agent's strategies are their own private information

- Notation
  - P_t^i:= Agent i's private information at t
  - C_t:= Agents' common information at t
  - $g_t^i(C_t, P_t^i)$:= Agent i's strategy at t

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- At each time t agents need to form:

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- At each time t agents need to form:
  - Beliefs about the status of the game

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- At each time t agents need to form:
  - Beliefs about the status of the game
  - Prediction about other agent strategies

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- At each time t agents need to form:
  - Beliefs about the status of the game
  - Prediction about other agent strategies
- Beliefs about status of game are, in general, different among agents (asymmetric information)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- At each time t agents need to form:
  - Beliefs about the status of the game
  - Prediction about other agent strategies
- Beliefs about status of game are, in general, different among agents (asymmetric information)
- Agents' actual strategies may be different from their prediction (agents' strategies are their own private information)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequence of Difficulties

Challenges/Consequence of Difficulties

- Belief and strategy predictions must be defined/specified:

Challenges/Consequence of Difficulties

- Belief and strategy predictions must be defined/specified:
  - On-equilibrium paths: feasible/reachable information sets under the strategy prediction

Challenges/Consequence of Difficulties

- Belief and strategy predictions must be defined/specified:
  - On-equilibrium paths: feasible/reachable information sets under the strategy prediction
  - Off-equilibrium paths: infeasible/unreachable information sets under the strategy prediction

Challenges/Consequence of Difficulties

- Belief and strategy predictions must be defined/specified:
  - On-equilibrium paths: feasible/reachable information sets under the strategy prediction
  - Off-equilibrium paths: infeasible/unreachable information sets under the strategy prediction
- Above specification is necessary because agents' strategies are their own private information

Challenges/Consequences of Difficulties

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}_{t:T}^{-i}$ (all other agents' strategies) from t to T

Best response →

Agent i's actual strategy from t to T (Nash)

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}^{-i}_{t:T}$ (all other agents' strategies) from t to T

Best response → Agent i's actual strategy from t to T (Nash)

- Agent i's strategy prediction $\hat{g}^{i}_{1:t}$

= Agent i's actual strategy (Nash)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}_{t:T}^{-i}$ (all other agents' strategies) from t to T

Best response → Agent i's actual strategy from t to T (Nash)

- Agent i's strategy prediction $\hat{g}_{1:t}^{i}$

= Agent i's actual strategy (Nash)

- Agent i's belief at t

← Signaling — Agents i's prediction of $\hat{g}_{1:t-1}^{-i}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}^{-i}_{t:T}$ (all other agents' strategies) from t to T

Best response → Agent i's actual strategy from t to T (Nash)

- Agent i's strategy prediction $\hat{g}^{i}_{1:t}$

= Agent i's actual strategy (Nash)

- Agent i's belief at t

← Signaling — Agents i's prediction of $\hat{g}^{-i}_{1:t-1}$

•Strategies and beliefs are inter-dependent over time

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}^{-i}_{t:T}$ (all other agents' strategies) from t to T

Best response → Agent i's actual strategy from t to T (Nash)

- Agent i's strategy prediction $\hat{g}^{i}_{1:t}$

= Agent i's actual strategy (Nash)

- Agent i's belief at t

← Signaling — Agents i's prediction of $\hat{g}^{-i}_{1:t-1}$

- Strategies and beliefs are inter-dependent over time
- The domain of strategy $g^{i}_{t}(C_t, P^{i}_t)$ increases over time.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Challenges/Consequences of Difficulties

- Agent i's belief at t
- Agents i's strategy prediction of $\hat{g}_{t:T}^{-i}$ (all other agents' strategies) from t to T

Best response → Agent i's actual strategy from t to T (Nash)

- Agent i's strategy prediction $\hat{g}_{1:t}^{i}$

= Agent i's actual strategy (Nash)

- Agent i's belief at t

← Signaling — Agents i's prediction of $\hat{g}_{1:t-1}^{-i}$

- Strategies and beliefs are inter-dependent over time
- The domain of strategy $g_t^i(C_t, P_t^i)$ increases over time.
- What are appropriate equilibrium concepts?

Formalization

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$
- $u_t^i(X_t, A_t)$:= Agent i's utility at t, i=(A), (D)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$
- $u_t^i(X_t, A_t)$:= Agent i's utility at t, i=(A), (D)
- T := {1, 2,… ,T} := Time horizon

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$
- $u_t^i(X_t, A_t)$:= Agent i's utility at t, i=(A), (D)
- T := {1, 2,… ,T} := Time horizon
- C_t := Common information of (A), (D) at time t

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$
- $u_t^i(X_t, A_t)$:= Agent i's utility at t, i=(A), (D)
- T := {1, 2,… ,T} := Time horizon
- C_t := Common information of (A), (D) at time t
- P_t^i := Private information of agent i at time t, i= (A), (D)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- X_t := Dynamic system's state at time t (Cyber and physical)
- $A_t := (A_t^{(A)}, A_t^{(D)})$
- $u_t^i(X_t, A_t)$:= Agent i's utility at t, i=(A), (D)
- T := {1, 2,… ,T} := Time horizon
- C_t := Common information of (A), (D) at time t
- P_t^i := Private information of agent i at time t, i= (A), (D)
- $P_t^{-(A)} = P_t^{(D)}$, $g_t^{-(A)} = g_t^{(D)}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

Formalization

- $\mu_t^i(C_t, P_t^i)$: agent i's belief on $(\mathrm{X_t}, P_t^{-i})$, $i = (A), (D)$
- $(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)})$: prediction about agents' strategies

Assessment
$(\hat{g}_{1:T}^{i}, \mu_{1:T}^{i})$,
$i = (A), (D)$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- $\mu_t^i(C_t, P_t^i)$: agent i's belief on (X_t, P_t^{-i}) , $i = (A), (D)$

$(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)})$: prediction about agents' strategies

Assessment $(\hat{g}_{1:T}^i, \mu_{1:T}^i)$, $i = (A), (D)$

- Sequential rationality (Nash idea)

$$\hat{g}_{t:T}^i \in argmax_{g_{t:T}^i} \mathbb{E}_{\mu_t^i}^{\hat{g}_{t:T}^{-i}, g_{t:T}^i} \left\{ \sum_{\tau=t}^{T} u_\tau^i(X_t, A_t) \middle| C_t, P_t^i \right\},$$

$\forall t, C_t, P_t^i$, i=(A), (D)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- $\mu_t^i(C_t, P_t^i)$: agent i's belief on $(\mathrm{X}_t, P_t^{-i}), i = (A), (D)$
- $(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)})$: prediction about agents' strategies

Assessment $(\hat{g}_{1:T}^i, \mu_{1:T}^i)$, $i = (A), (D)$

- Sequential rationality (Nash idea)

$$\hat{g}_{t:T}^i \in argmax_{g_{t:T}^i} \mathbb{E}_{\mu_t^i}^{\hat{g}_{t:T}^{-i}, g_{t:T}^i} \left\{ \sum_{\tau=t}^{T} u_\tau^i(X_t, A_t) \middle| C_t, P_t^i \right\},$$

$$\forall t, C_t, P_t^i, \text{i=(A), (D)}$$

- Consistency

Formalization

- $\mu_t^i(C_t, P_t^i)$: agent i's belief on (X_t, P_t^{-i}) , $i = (A), (D)$

$(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)})$: prediction about agents' strategies

Assessment $(\hat{g}_{1:T}^i, \mu_{1:T}^i)$, $i = (A), (D)$

- Sequential rationality (Nash idea)

$$\hat{g}_{t:T}^i \in argmax_{g_{t:T}^i} \mathbb{E}_{\mu_t^i}^{\hat{g}_{t:T}^{-i}, g_{t:T}^i} \left\{ \sum_{\tau=t}^{T} u_\tau^i(X_t, A_t) \middle| C_t, P_t^i \right\},$$

$\forall t, C_t, P_t^i$, i=(A),(D)

- Consistency
  - On-equilibrium: $\mu_t^i = \mathrm{P}(X_t, P_t^{-i} | C_t, P_t^i, \hat{g}_{1:t-1}^{(A)}, \hat{g}_{1:t-1}^{(D)})$, i=(A), (D)

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Formalization

- $\mu_t^i(C_t, P_t^i)$: agent i's belief on $(\mathrm{X_t}, P_t^{-i})$, $i = (A), (D)$

$(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)})$: prediction about agents' strategies

Assessment $(\hat{g}_{1:T}^i, \mu_{1:T}^i)$, $i = (A), (D)$

- Sequential rationality (Nash idea)

$$\hat{g}_{t:T}^i \in argmax_{g_{t:T}^i} \mathbb{E}_{\mu_t^i}^{\hat{g}_{t:T}^{-i}, g_{t:T}^i} \left\{ \sum_{\tau=t}^{T} u_\tau^i(X_t, A_t) \middle| C_t, P_t^i \right\},$$

$\forall t, C_t, P_t^i$, i=(A), (D)

- Consistency
  - On-equilibrium: $\mu_t^i = \mathrm{P}(X_t, P_t^{-i} | C_t, P_t^i, \hat{g}_{1:t-1}^{(A)}, \hat{g}_{1:t-1}^{(D)})$, i=(A), (D)
  - Off-equilibrium: μ_t^i must comply with $\hat{g}_{1:t-1}^{(A)}, \hat{g}_{1:t-1}^{(D)}$ via Bayes' rule whenever possible

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Adopted Equilibrium Concept – Perfect Bayesian Equilibrium

Adopted Equilibrium Concept – Perfect Bayesian Equilibrium

- ***Definition.*** *An assessment* $(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)}, \mu_{1:T}^{(A)}, \mu_{1:T}^{(D)})$ *is a Perfect Bayesian equilibrium (PBE) if it is sequentially rational and consistent.*

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Adopted Equilibrium Concept – Perfect Bayesian Equilibrium

Key difficulties of determining a PBE

- Assessment $(\hat{g}_{1:\mathrm{T}}^{(\mathrm{A})}, \hat{g}_{1:\mathrm{T}}^{(\mathrm{D})}, \mu_{1:T}^{(A)}, \mu_{1:T}^{(D)})$ must satisfy sequential rationality and consistency along equilibrium and off-equilibrium paths.

$$(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)}) \xrightarrow{\text{Consistency}} (\mu_{1:T}^{(A)}, \mu_{1:T}^{(D)})$$

$$(\hat{g}_{1:T}^{(A)}, \hat{g}_{1:T}^{(D)}) \xleftarrow[\text{Sequential Rationality}]{} (\mu_{1:T}^{(A)}, \mu_{1:T}^{(D)})$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Adopted Equilibrium Concept – Perfect Bayesian Equilibrium

Key difficulties of determining a PBE

- Assessment $(\hat{g}^{(\mathrm{A})}_{1:\mathrm{T}}, \hat{g}^{(\mathrm{D})}_{1:\mathrm{T}}, \mu^{(A)}_{1:T}, \mu^{(D)}_{1:T})$ must satisfy sequential rationality and consistency along equilibrium and off-equilibrium paths.

$(\hat{g}^{(A)}_{1:T}, \hat{g}^{(D)}_{1:T})$ —Consistency→ $(\mu^{(A)}_{1:T}, \mu^{(D)}_{1:T})$

$(\hat{g}^{(A)}_{1:T}, \hat{g}^{(D)}_{1:T})$ ←Sequential Rationality— $(\mu^{(A)}_{1:T}, \mu^{(D)}_{1:T})$

- Growing complexity of Agent i's strategy $g^i_t(C_t, P^i_t)$ with increasing t (and thus, its prediction $\hat{g}^i_t(C_t, P^i_t)$).

State-of-the-art in SDGAS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static
- Problems in (C1) arise in engineering (e.g. CPS)

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static
- Problems in (C1) arise in engineering (e.g. CPS)
- Problems in (C2) arise primarily in economics

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static
- Problems in (C1) arise in engineering (e.g. CPS)
- Problems in (C2) arise primarily in economics
- Will concentrate in non-zero sum games in (C1)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static
- Problems in (C1) arise in engineering (e.g. CPS)
- Problems in (C2) arise primarily in economics
- Will concentrate in non-zero sum games in (C1)
  - Briefly review (C2), and zero-sum games in (C1)

State-of-the-art in SDGAS

- Two classes/categories of SDGAS
  - (C1): underlying system is dynamic
  - (C2): underlying system is static
- Problems in (C1) arise in engineering (e.g. CPS)
- Problems in (C2) arise primarily in economics
- Will concentrate in non-zero sum games in (C1)
  - Briefly review (C2), and zero-sum games in (C1)
- Consider N-agent games

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Problems in (C1)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Problems in (C1)
  - We assume that at each time t

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Problems in (C1)
  - We assume that at each time t
    - All agents have some common information C_t that is nested over time

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Problems in (C1)
  - We assume that at each time t
    - All agents have some common information C_t that is nested over time
    - Each agent i has some private information P_t^i

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS

- Problems in (C1)
  - We assume that at each time t
    - All agents have some common information C_t that is nested over time
    - Each agent i has some private information P_t^i
- Common-information-based (CIB) approach to SDGAS

Our Contribution: The Common Information Approach

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t \ , P_t^1 , P_t^2, \ldots , P_t^N)$

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \ldots, P_t^N)$
    - Π_t is common knowledge among all agents

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \dots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \ldots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\left(\Pi_t, l(P_t^i)\right)$ is an information state for agent i

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \ldots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\left(\Pi_t, l(P_t^i)\right)$ is an information state for agent i
    - $l(P_t^i)$ subset of P_t^i ($l(.)$ problem-dependent)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \ldots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\left(\Pi_t, l(P_t^i)\right)$ is an information state for agent i
    - $l(P_t^i)$ subset of P_t^i ($l(.)$ problem-dependent)
    - $\left(\Pi_t, l(P_t^i)\right)$ has fixed domain

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \dots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\big(\Pi_t, l(P_t^i)\big)$ is an information state for agent i
    - $l(P_t^i)$ subset of P_t^i ($l(.)$ problem-dependent)
    - $\big(\Pi_t, l(P_t^i)\big)$ has fixed domain
  - Consider CIB strategies $\sigma_t^i(\Pi_t, l(P_t^i))$;

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t\ , P_t^1\ , P_t^2, \ldots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\left(\Pi_t, l(P_t^i)\right)$ is an information state for agent i
    - $l(P_t^i)$ subset of P_t^i ($l(.)$ problem-dependent)
    - $\left(\Pi_t, l(P_t^i)\right)$ has fixed domain
  - Consider CIB strategies $\sigma_t^i(\Pi_t, l(P_t^i))$;
  - Consider CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$,

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

- CIB approach – Key ideas
  - At each t form CIB belief $\Pi_t(C_t)$ of $(X_t \ , P_t^1 \, , P_t^2, \dots, P_t^N)$
    - Π_t is common knowledge among all agents
    - $\Pi_{t+1} = f(\Pi_t, C_{t+1} \backslash C_t)$
  - Show $\left(\Pi_t, l(P_t^i)\right)$ is an information state for agent i
    - $l(P_t^i)$ subset of P_t^i ($l(.)$ problem-dependent)
    - $\left(\Pi_t, l(P_t^i)\right)$ has fixed domain
  - Consider CIB strategies $\sigma_t^i(\Pi_t, l(P_t^i))$;
  - Consider CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$,
    - $\hat{\sigma}_{1:T}^{1:N}$:=$(\hat{\sigma}_1^1, \dots, \hat{\sigma}_T^1, \dots, \hat{\sigma}_1^N, \dots, \hat{\sigma}_T^N)$, $\Pi_{1:T} := (\Pi_1, \dots, \Pi_T)$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE
- Define CIB-PBE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE
- Define CIB-PBE
  - A CIB assessment $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ is a CIB-PBE if it is sequentially rational and consistent

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE
- Define CIB-PBE
  - A CIB assessment $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ is a CIB-PBE if it is sequentially rational and consistent
- Use CIB-PBE to provide a sequential decomposition of the T-horizon SDGAS into a sequence of T-static games.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE
- Define CIB-PBE
  - A CIB assessment $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ is a CIB-PBE if it is sequentially rational and consistent
- Use CIB-PBE to provide a sequential decomposition of the T-horizon SDGAS into a sequence of T-static games.
  - Exponential (in time) reduction of complexity

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Our Contribution: The Common Information Approach

CIB Approach-Key Ideas

- Show that CIB assessments $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ are rich enough to capture a PBE
- Define CIB-PBE
  - A CIB assessment $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$ is a CIB-PBE if it is sequentially rational and consistent
- Use CIB-PBE to provide a sequential decomposition of the T-horizon SDGAS into a sequence of T-static games.
  - Exponential (in time) reduction of complexity
- Prove existence of CIB-PBE

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling
  - Strategies and beliefs are not inter-dependent

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling
  - Strategies and beliefs are not inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N})$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling
  - Strategies and beliefs are not inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N})$
  - Solution concept CIB Markov perfect equilibrium (CIB-MPE) instead of CIB-PBE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \dots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling
  - Strategies and beliefs are not inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N})$
  - Solution concept CIB Markov perfect equilibrium (CIB-MPE) instead of CIB-PBE
  - Sequential decomposition using CIB-MPE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-independent CIB beliefs $(\Pi_t, t = 1, \ldots, T)$ (Nayyar et al 2014, Gupta et al 2014)
  - One-step delay information structure
  - Absence of signaling
  - Strategies and beliefs are not inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N})$
  - Solution concept CIB Markov perfect equilibrium (CIB-MPE) instead of CIB-PBE
  - Sequential decomposition using CIB-MPE
  - Proof of existence of CIB-MPE

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t \;\; = (X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t = (X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t \;\; = (\,X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t \;= (X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, X_t^i)$;

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t = (X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, X_t^i)$;
  - Solution concept: CIB-PBE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t = (X_t^1, X_t^2, \ldots, X_t^N)$ Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, X_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t = (X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T})$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, X_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games
  - Proof of existence of CIB-PBEs for special cases

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Observable actions (actions are common information) (Energy Markets)
  - $X_t \;\; = (\, X_t^1, X_t^2, \ldots, X_t^N)$Agent i observes X_t^i
  - Agents' dynamics are independent conditioned on the agents' actions
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_{1:T}), \hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, X_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games
  - Proof of existence of CIB-PBEs for special cases
  - Results in Ouyang, Tavafoghi, Teneketzis (CDC 2015, IEEE TAC 2017)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_T)$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, P_t^i)$;

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_T)$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, P_t^i)$;
  - Solution concept: CIB-PBE

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_T)$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, P_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_T)$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, P_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games
  - Proof of existence of CIB-PBEs for special cases

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results based on CIB approach (non-zero sum games)

- Strategy-dependent CIB beliefs (signaling)
  - Unobservable actions (actions are private information)
  - Private, imperfect, observation of system's state
  - n-step delay-sharing information structure
  - Agents' dynamics are inter-dependent
  - Strategies and beliefs are inter-dependent
  - Assessments defined by $(\hat{\sigma}_{1:T}^{1:N}, \Pi_T)$, $\hat{\sigma}_t^i(\Pi_t, l(P_t^i))$=$\hat{\sigma}_t^i(\Pi_t, P_t^i)$;
  - Solution concept: CIB-PBE
  - Sequential decomposition of the game, using CIB-PBE, into T consecutive static games
  - Proof of existence of CIB-PBEs for special cases
  - Results in Tavafoghi, Ouyang , Teneketzis (CDC 2016)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results on Zero-Sum SDGAS

State-of-the-art in SDGAS – (C1)
Results on Zero-Sum SDGAS

- Infinite horizon (critical)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1) Results on Zero-Sum SDGAS

- Infinite horizon (critical)
- Dynamic system described by Markov chain

State-of-the-art in SDGAS – (C1) Results on Zero-Sum SDGAS

- Infinite horizon (critical)
- Dynamic system described by Markov chain
- Philosophy of approach inspired by Aumann's work on infinitely repeated games of incomplete information (Renault (2006), (2015))

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C1)
Results on Zero-Sum SDGAS

- Infinite horizon (critical)
- Dynamic system described by Markov chain
- Philosophy of approach inspired by Aumann's work on infinitely repeated games of incomplete information (Renault (2006), (2015))
- LP-approach Li-Shamma (2014)

State-of-the-art in SDGAS – (C2)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C2)

- SDGAS studied primarily by economists

State-of-the-art in SDGAS – (C2)

- SDGAS studied primarily by economists
- Infinitely repeated games

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C2)

- SDGAS studied primarily by economists
- Infinitely repeated games
  - Each agent knows perfectly part of the system state that does not change with time. Actions are publicly observed (common knowledge). Agents' utilities depend on system state and their actions (Aumann-Maschler (1995), Mertens-Zamir (2015), Sorin (2002), Forges (1994) etc.)

State-of-the-art in SDGAS – (C2)

- SDGAS studied primarily by economists
- Infinitely repeated games
  - Each agent knows perfectly part of the system state that does not change with time. Actions are publicly observed (common knowledge). Agents' utilities depend on system state and their actions (Aumann-Maschler (1995), Mertens-Zamir (2015), Sorin (2002), Forges (1994) etc.)
  - Imperfect publicly observed actions: Agents' utilities depend on their actions (Mailath-Samuelson (2006), Fudenbrg-Levine-Maskin)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

State-of-the-art in SDGAS – (C2)

- SDGAS studied primarily by economists
- Infinitely repeated games
  - Each agent knows perfectly part of the system state that does not change with time. Actions are publicly observed (common knowledge). Agents' utilities depend on system state and their actions (Aumann-Maschler (1995), Mertens-Zamir (2015), Sorin (2002), Forges (1994) etc.)
  - Imperfect publicly observed actions: Agents' utilities depend on their actions (Mailath-Samuelson (2006), Fudenbrg-Levine-Maskin)
  - Imperfect privately observed actions: Agents' utilities depend on their actions (Mailath-Samuelson (2006), Kandori (2002), Kandori-Matsushima (2002))

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.
- Attacker, defender have common information that is nested in time.

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.
- Attacker, defender have common information that is nested in time.
- Security games are beyond the current sate of the art.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.
- Attacker, defender have common information that is nested in time.
- Security games are beyond the current sate of the art.
- Does the CIB approach work in this case?

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.
- Attacker, defender have common information that is nested in time.
- Security games are beyond the current sate of the art.
- Does the CIB approach work in this case?
- Is there an information state $(\Pi_t, l(P_t^i))$ for agent i at time t that has a time-invariant domain?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Gap between state-of-the-art in non-zero sum SDGAS and security game in CPS

- Actions in CPS security games are usually not observable (not common knowledge), or partly observable at random times.
- Attacker, defender have common information that is nested in time.
- Security games are beyond the current sate of the art.
- Does the CIB approach work in this case?
- Is there an information state $(\Pi_t, l(P_t^i))$ for agent i at time t that has a time-invariant domain?
- n-step delay information structure, n large, may be a reasonable approximation to modeling security problems in CPS

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Work on SDGAS Supported by FORCES Grant

- Y. Ouyang, H. Tavafoghi and D. Teneketzis, “Dynamic Oligopoly Games with Private Markovian Dynamics”, *IEEE-CDC*, 2015.
- Y. Ouyang, H. Tavafoghi and D. Teneketzis, “Dynamic Games with Asymmetric Information: Common Information Based Perfect Bayesian Equilibria and Sequential Decomposition”, *IEEE-TAC*, January 2017
- H. Tavafoghi, Y. Ouyang and D. Teneketzis, “On Stochastic Dynamic Games with Delayed Sharing Information Structure”, *IEEE-CDC*, 2016

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS