Game-Theoretic Framework for Network Resilience, Reliability, and Security (NR^2S)

TAMER BAŞAR
ECE, CAS, CSL, ITI, and MechSE, UIUC
basar1@illinois.edu

ISRCS Keynote
Salt Lake City, Utah
August 14, 2012

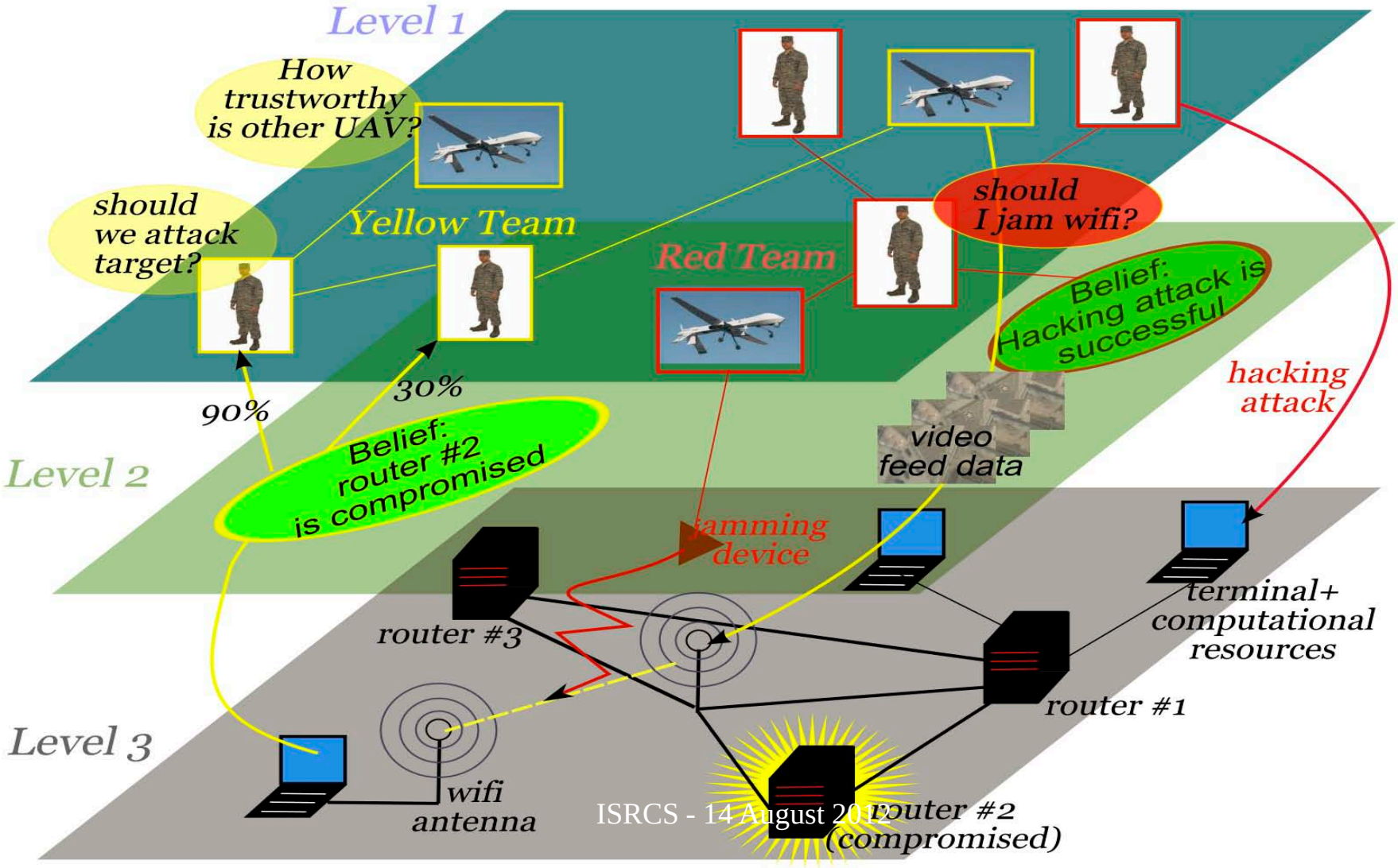
Outline

- Multi-agent networked systems
  - Structures: levels, layers
  - Issues: resilience, reliability (trust), security
  - Design of robust architectures
- Game-theoretic framework
  - Solution concepts
  - Efficiency, sensitivity
  - Incentive mechanisms
- Adversarial actions
  - Connectivity maintenance with mobile jammers
- Conclusions

Multi-agent networked systems

- Multiple heterogeneous agents connected in various ways, distributed over a network (or interacting networks) and interacting with limited information (on line and off line) under possibly conflicting objectives
- Issues that arise
  - Complexity of interactions
  - Handling uncertainty and adversarial actions
  - Trust, learning, common knowledge
  - Human agents alongside machines
  - Disruption of communication; resource constraints
  - Generation and transmission of actionable information
  - Design of architectures to facilitate efficient operation

Multi-Level Multi-Resolution (MLMR) Framework



Multi-Level Multi-Resolution (MLMR) Framework

Several dynamic networks in this 3-tiered hierarchy

Level 1: Collaboration network

Who needs to collaborate with whom among the agents

➔ A relational (logical) graph

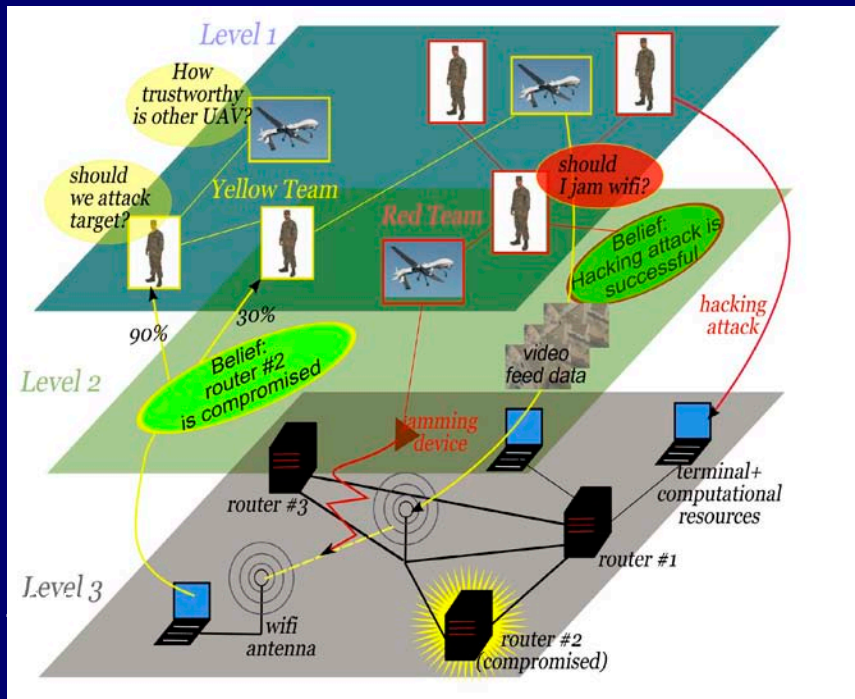
Level 2: Information network

How information is shared among agents

➔ Another relational graph

Level 3: Physical communication network

Physical connectivities, communication resources and constraints

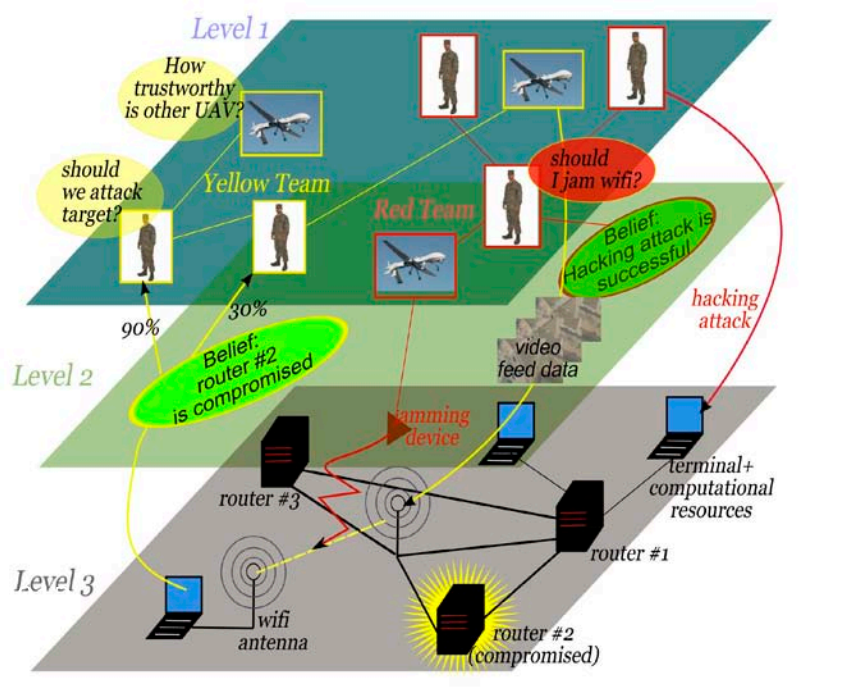


Multi-Level Multi-Resolution (MLMR) Framework

➔ *MLMR Games:*

Games played at different levels, interacting through their outcomes, action spaces, and costs

"Games within Games"
Zooming in and zooming out
providing game structures with different levels of granularity



Assessing Security and Resilience

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

Outline

- Multi-agent networked systems
  - Structures: levels, layers
  - Issues: resilience, reliability (trust), security
  - Design of robust architectures
- Game-theoretic framework
  - Solution concepts
  - Efficiency, sensitivity
  - Incentive mechanisms
- Adversarial actions
  - Connectivity maintenance with mobile jammers
- Conclusions

Elements of Games

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

Elements of Games

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

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

Elements of Games

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

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

Coupled constraints also possible: $u \in U$

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

Elements of Games

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

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

- Saddle-point eqm ($M=2$, $-V_2 = V_1 =: V$)

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

Elements of Games

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

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

- **Efficiency:** u^* is also Pareto optimal, minimizing a convex combination of V_i's

Refinements of NE

- *Coalition proof* given fixed coalition sizes
- *Resilient NE* (remains NE under any coalition)
- *Efficiency* : NE u^* is also Pareto optimal, minimizing a convex combination of V_i's
- *Sensitivity* : "small" departures in face of modeling errors

Price of Anarchy

- Price of Anarchy (PoA):

  Sum of costs under NE / min sum

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

Incentivizing/Coordination

- Price of Anarchy (PoA):

  Sum of costs under NE / min sum

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

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

Leader-Followers Game

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

Followers' cost functions:

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

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

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

Leader-Followers Game

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

Followers' cost functions:

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

Information available to L:

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

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

$$\rightarrow \quad u_i = \gamma_i(y_i), \quad i = 1, \ldots, M$$

Leader-Followers Game

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

Followers' cost functions:

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

Information available to L:

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

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

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

Leader-Followers Game

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

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

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

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

Leader-Followers Game

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

Followers' cost functions:

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

r is the instrument variable of L,

players

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

Outline

- Multi-agent networked systems
  - Structures: levels, layers
  - Issues: resilience, reliability (trust), security
  - Design of robust architectures
- Game-theoretic framework
  - Solution concepts
  - Efficiency, sensitivity
  - Incentive mechanisms
- Adversarial actions
  - Connectivity maintenance with mobile jammers
- Conclusions

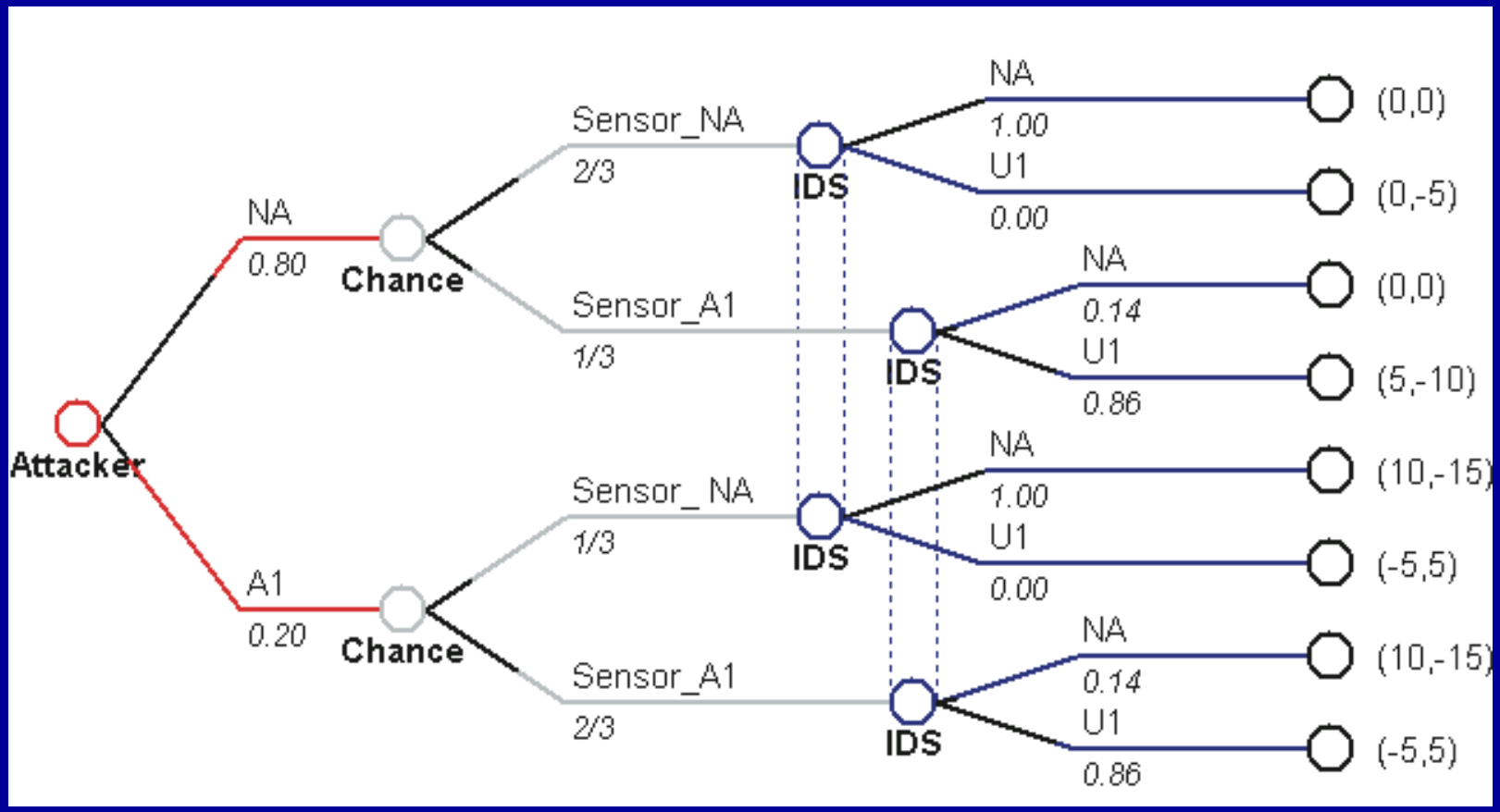
An Application Paradigm for Security
A Class of Network Security Games

- Interaction between attacker(s) and the IDS is modeled as a non-cooperative game
- A sensor network is introduced as a third, fictitious player, with a fixed probability distribution for each attack type
- Output of the sensor network is measurement to IDS, based on which it decides on the presence (or not) of an attack and its type
- Payoffs to attacker(s) and IDS for each triple of actions

A Class of Network Security Games (*continued; Alpcan, TB CDC'03, 04; CUP'10*)

- Finite or infinite (continuous-kernel) NZS games depending on whether # actions is finite or not.
- As a finite game, there is a NE in mixed strategies: worst probabilistic attacker behavior and corresponding best IDS strategy
- As a continuous-kernel game, there exists a unique NE under some mild conditions
- If payoffs are completely conflicting (zero-sum), there exist saddle-point solutions

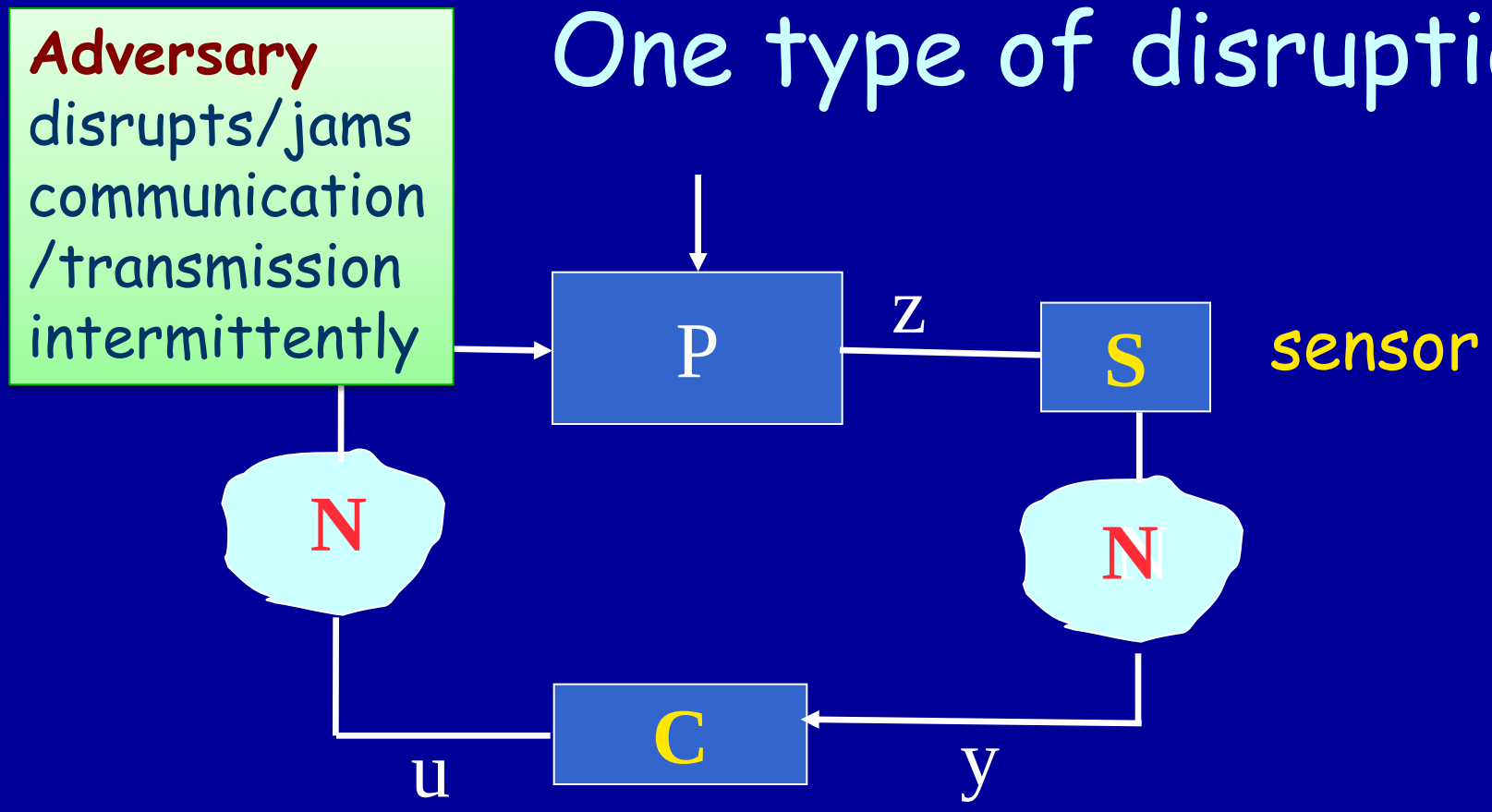
A Finite Security Game in Extensive Form (single subsystem, single detectable threat)



Another type of adversarial action

Jamming or disruption of communication

One type of disruption



Threshold based policies

Event generation

A different type of jamming

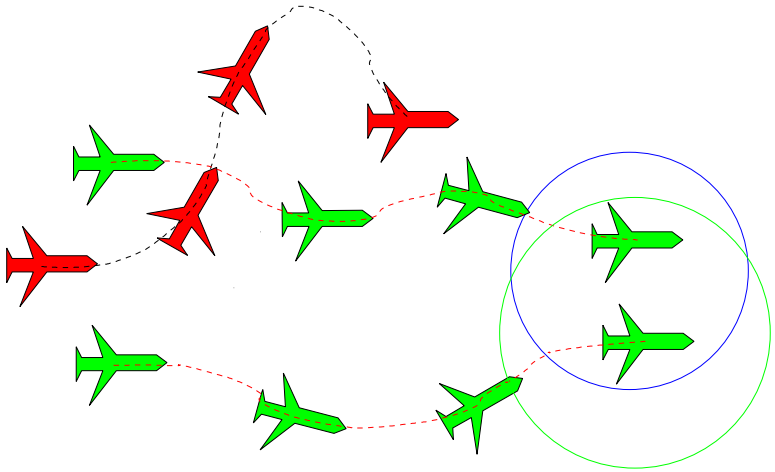
Communication jamming in teams vs teams, with application in formation of UAVs or AGVs

- Mobility (as a means for increasing the resilience in autonomous vehicular networks)
- Disruption of communication by adversary (team of adversaries)
- Dynamic/Differential game theory as an underlying framework for designing secure systems.

Aerial Jamming Attack on the CommNet of a team of UAVs

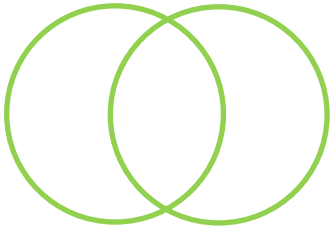
-

inimize the time for which communication remains jammed.

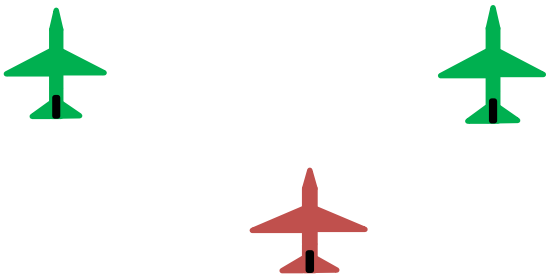


Intrusion Evasion

- The **jammer** wants to maximize the time for which the communication can be jammed.



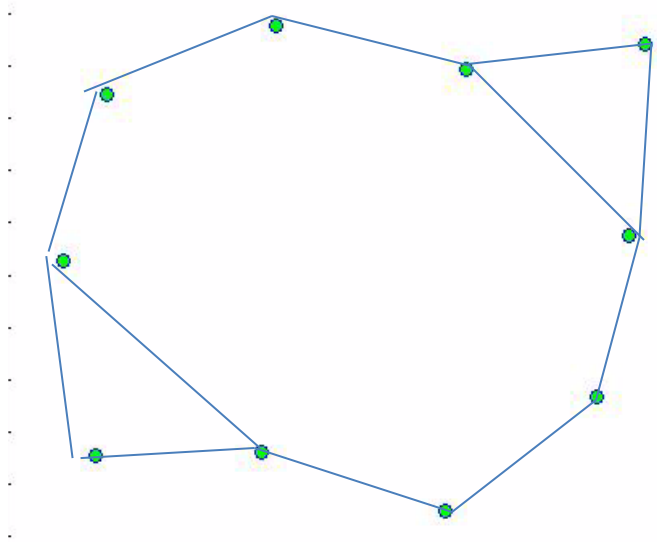
- The **two UAVs** want to minimize the time for which communication remains jammed.



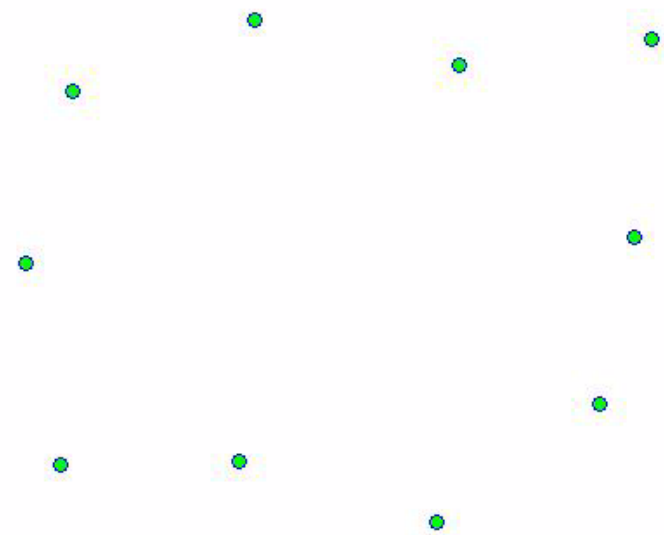
Intrusion in Mobile Networks

A group of mobile agents need to accomplish a task while maintaining connectivity of the communication network. What are the strategies of the agents in the presence of a mobile jammer in the vicinity?

$$\dot{x}_i = \frac{1}{|N(i)|}\sum_{j\in N(i)}(x_j - x_i)$$



Agreement protocol for rendezvous



Agreement protocol in the presence of a jammer

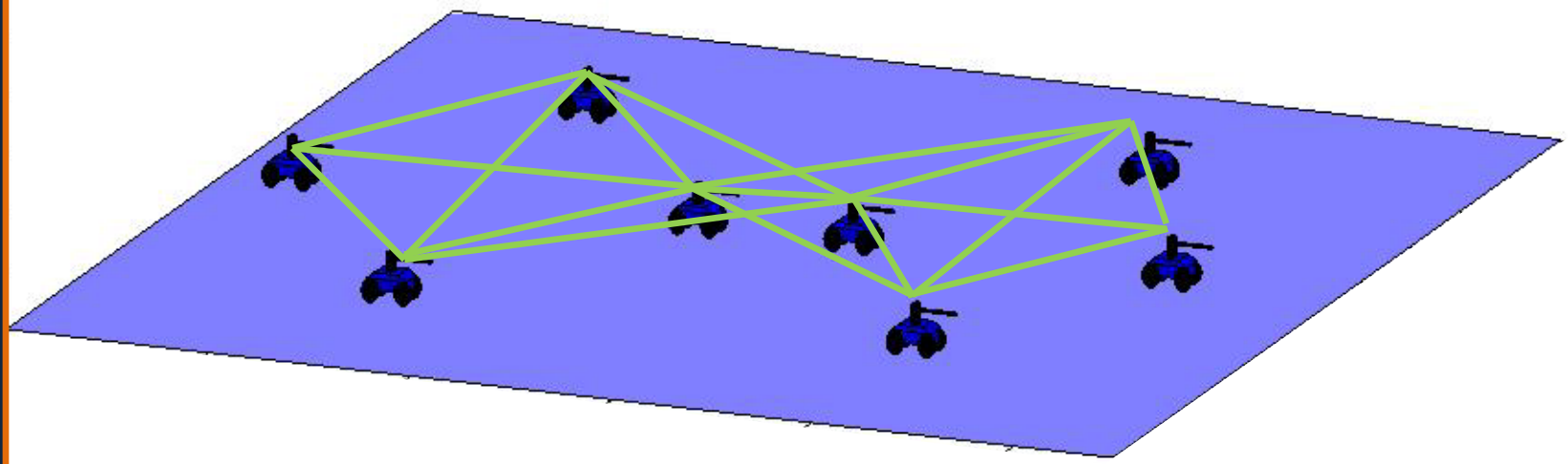
Connectivity Maintenance

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

- Formation Control
- Mobile Sensor Networks
- Rendezvous
- Flocking

Connectivity as a control objective: Ando et al. [1999], Zavlanos and Pappas [2005,2007], Boyd [2006], Spanos and Murray [2005], Langbort and Gupta [2009], Schuresko and Cortes [2007], Ji and Egerstedt [2007], de Gennaro and Jadbabaie [2006], Kim and Mesbahi [2006], Bullo et al. [2009], Mesbahi and Egerstedt [2010].....

Problem Scenario

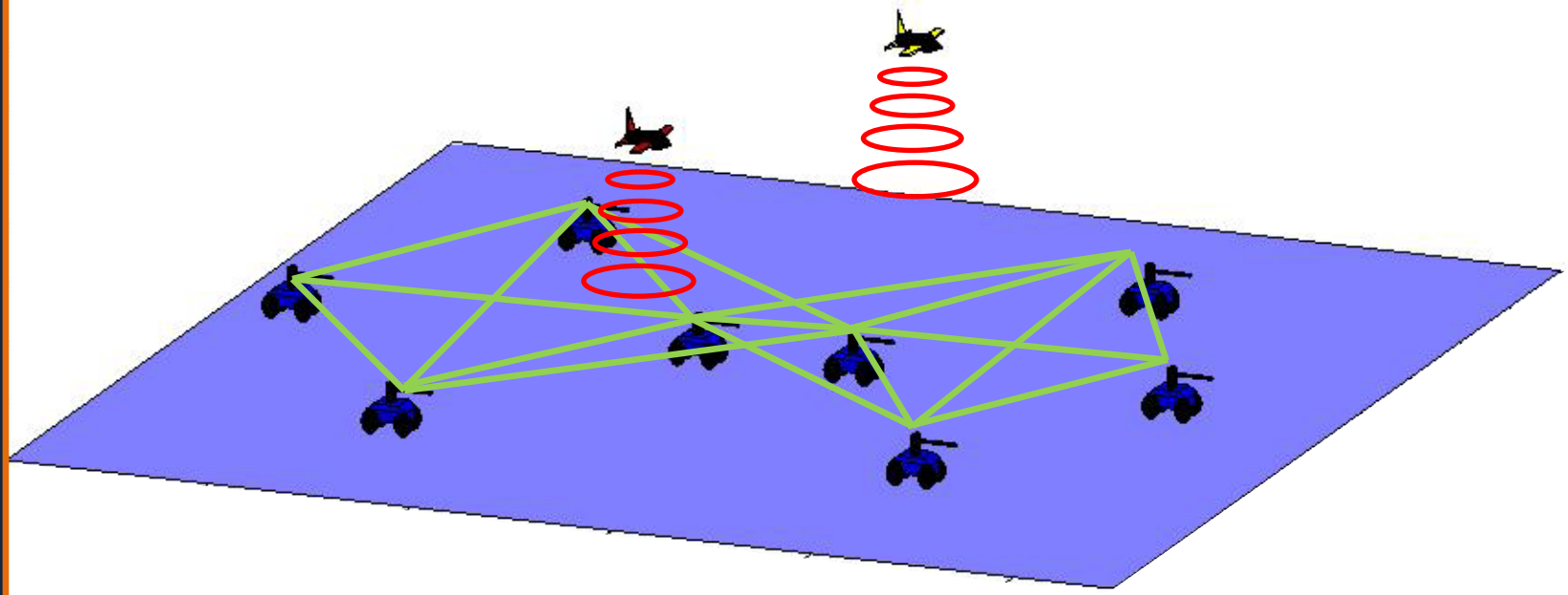


- The network is modeled as a graph G=(V,E(t)) → **DYNAMIC GRAPH**

$$\dot{x}_i^V = f_i^V\left(x_i^V, u_i^V\right)$$

- An edge exists between vertices *i* and *j*, ⇔ Vehicle *i* and vehicle *j* can communicate with each other

Game Formulation



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

Problem Formulation

Motion Model

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

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

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

<u>Communication Network</u>

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

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

Jamming Model

Jammer to Signal Ratio (JSR)

1. R^n model

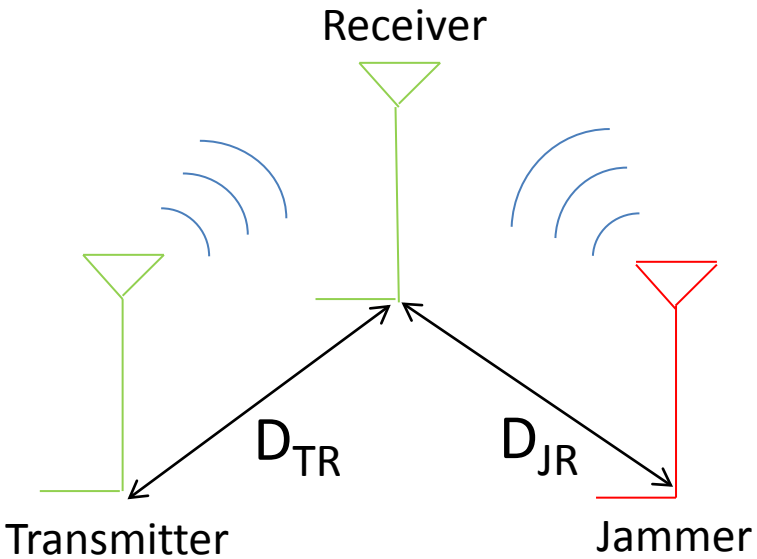
$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} 10^{n \log_{10}(\frac{D_{TR}}{D_{JR}})}$$

2. Ground Reflection Propagation

$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} (\frac{h_J}{h_T})^2 (\frac{D_{TR}}{D_{JR}})^4$$

3. Nicholson

$$\xi = \frac{P_{J_T} G_{JR} G_{RJ}}{P_T G_{TR} G_{RT}} 10^{4 \log_{10}(\frac{D_{TR}}{D_{JR}})}$$



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

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

Zero Sum Differential Games

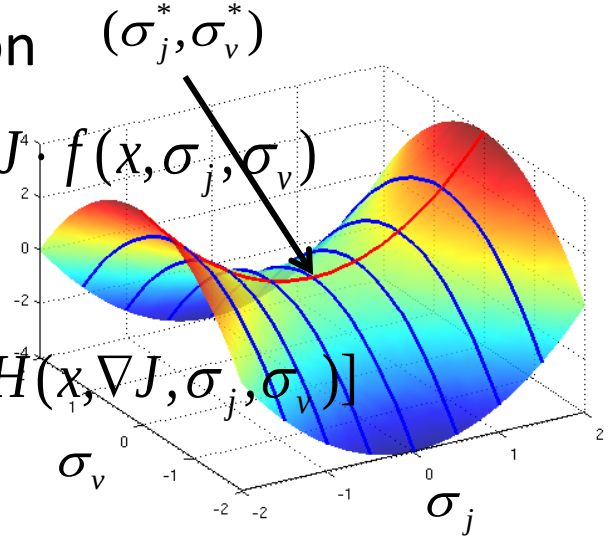
- Hamiltonian Function

$$H(x,\nabla J,\sigma_j,\sigma_v) = 1 + \nabla J \cdot f(x,\sigma_j,\sigma_v)$$

- Isaacs' Conditions

$$1)\ H(x,\nabla J,\sigma_j^*,\sigma_v^*) = \mathrm{SP}\,[H(x,\nabla J,\sigma_j,\sigma_v)]$$

$$2)\ H(x,\nabla J,\sigma_j^*,\sigma_v^*) = 0$$



- Retrogressive Path

$$\pi(x_0,\sigma_j^*,\sigma_v^*) \le \pi(x_0,\sigma_j^*,\sigma_v^*) \le \pi(x_0,\sigma_j,\sigma_v^*)$$

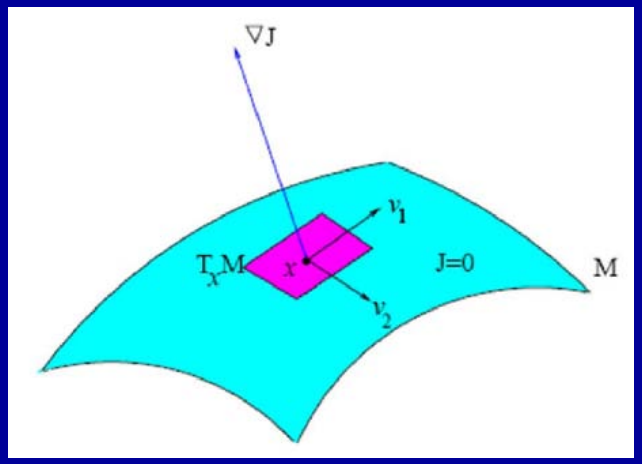
$$\frac{d(\nabla J)}{dt} = -\frac{\partial H(x,\nabla J,\sigma_j^*,\sigma_v^*)}{\partial x};\ \nabla J \cdot v_i\big|_{t_f} = 0 \quad \forall v_i \in T_x M$$

Players have no motivation to deviate from their saddle-point strategy!

Laplacian of a Graph G

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

Terminal Conditions



- $\nabla J^0 \cdot v_i = 0 \quad \forall \quad v_i \in T_x\mathcal{M}$

Algebraic Graph Theory

- $\mathcal{L}(G) = \Delta(G) - A(G)$
- It is a positive semi-definite symmetric matrix.
- $\lambda_1(\mathcal{L}(G)) = 0 \leq \underbrace{\lambda_2(\mathcal{L}(G))}_{\text{Fiedler Value}} \leq \cdots \leq \lambda_n(\mathcal{L}(G))$
- G is connected iff $\lambda_2(\mathcal{L}(G)) > 0$

Theorem

Let $\tilde{G}$ denote the set of all disconnected graphs.

$$\tilde{G} = \{G \mid F_\lambda(\lambda, G)|_{\lambda=0} = 0\}$$

where $F(\lambda, G) = det(\mathcal{L}(G) - \lambda I_n)$ and F_λ denotes derivative with respect to λ.

Termination Manifold

Termination Manifold

Theorem

Let $F(\lambda, G) = \det(L(G) - \lambda I_n)$ where, I_n denotes the identity matrix of dimension $n \times n$. Let $\tilde{G}$ denote the set of graphs that correspond to disconnected networks.

$$\tilde{G} = \{G \mid F_\lambda(\lambda, G)|_{\lambda=0} = 0\}$$

Integer Program

$$F_\lambda(\lambda, G)\,|_{\lambda=0} = -\sum_{i=1}^{m} M_{ii}^{L(G)} = f(a_{12}, a_{13} \cdots a_{(n-1)n}) = 0$$

$$a_{ij} = \{-1, 0\} \quad \forall i \in \{1, n-1\}, j \in \{2, n\}$$

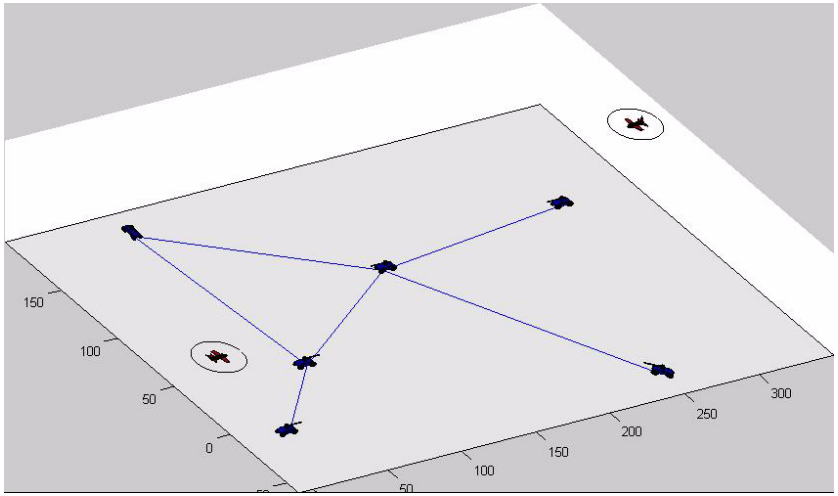
Closing the Loop

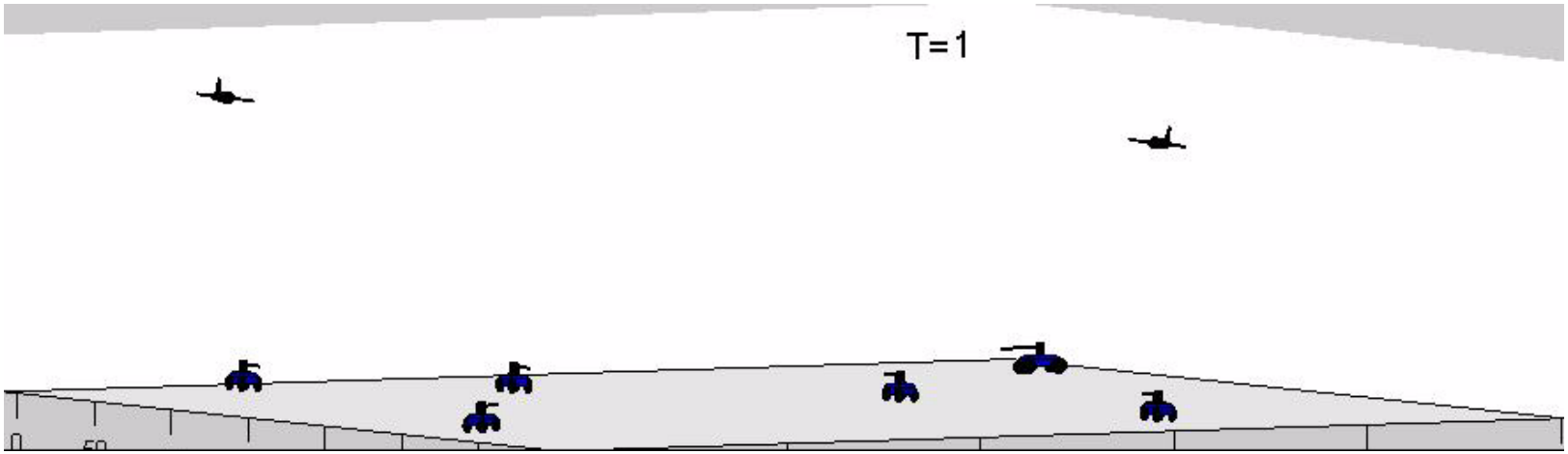
- Express $\lambda_2(L(G)) = 0$ condition in terms of state variables, for the jamming model adopted ➔ terminal manifold for the Isaacs conditions
- Details in

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

Heterogeneous Networks

UAV	AGV
$\dot{x} = W\cos\psi\cos\theta$ $\dot{y} = W\sin\psi\cos\theta$ $\dot{z} = W\sin\theta$ $\dot{\psi} = \frac{g}{W}\sin\phi$ $\dot{\theta} = \frac{g\cos\phi}{W}(\eta - 1)$	$\dot{x} = v\cos\theta\cos\zeta$ $\dot{y} = v\sin\theta\cos\zeta$ $\dot{\theta} = v\sin\psi$ $\dot{v} = u_1$ $\dot{\zeta} = u_2$





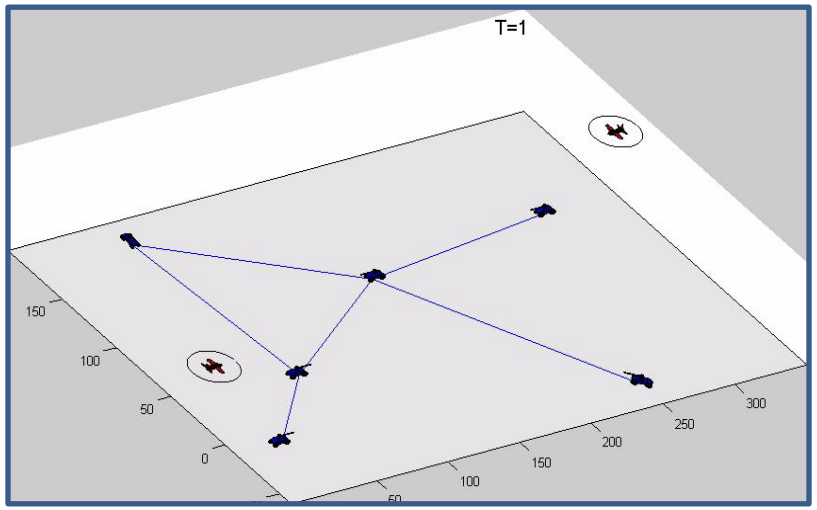
[Bhattacharya & Başar, Autonomous Robots, 2011]

Variations

- **Decentralized scheme**

$$\bar{u}(x) = \frac{\int u^*(x)dA}{\int dA}; \quad \frac{\mathrm{J}(x)}{(1+\delta)} \le T(x)$$

[Bhattacharya, Gupta & Başar, IFAC'11]



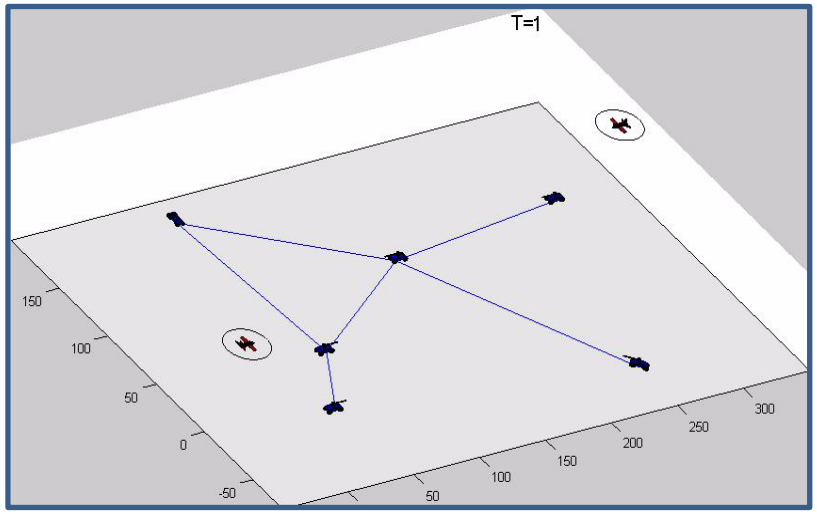
- **Greedy Strategy**

$$\max_{\sigma_v} \frac{d\lambda_2}{dt}$$

$$\frac{d\lambda_2}{dt} = \frac{\partial \lambda_2}{\partial x} \cdot \frac{dx}{dt} \longrightarrow$$

Depends on σ_j and σ_v

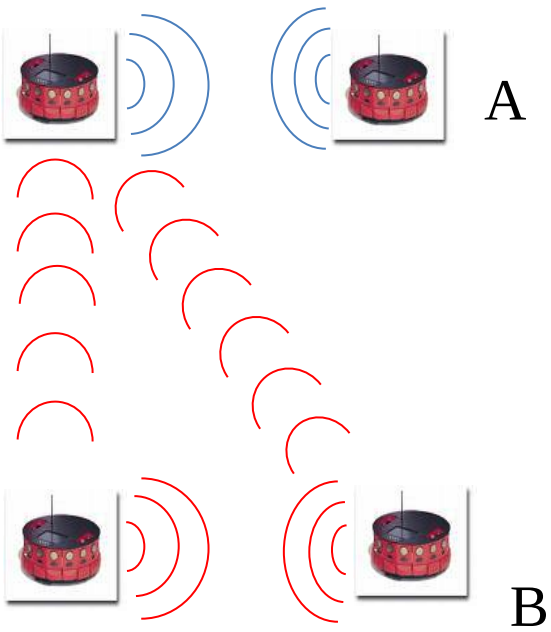
[Bhattacharya & Başar, CDC'11]



Double-Sided Jamming

Dynamic Model

$$\dot{x}_i^a = f_{x_i}^a(\mathrm{x}_i^a, \mathrm{u}_i^a, t) \quad , \quad \dot{y}_i^a = f_{y_i}^a(\mathrm{x}_i^a, \mathrm{u}_i^a, t)$$



Communication Model

$$P_R = \rho P_T (1+d)^{-\alpha} \text{ ,SINR (s)} = \frac{P_R}{I+\sigma}$$

$$\text{Bit Error Rate (p)} = g(s)$$

Power Constraint

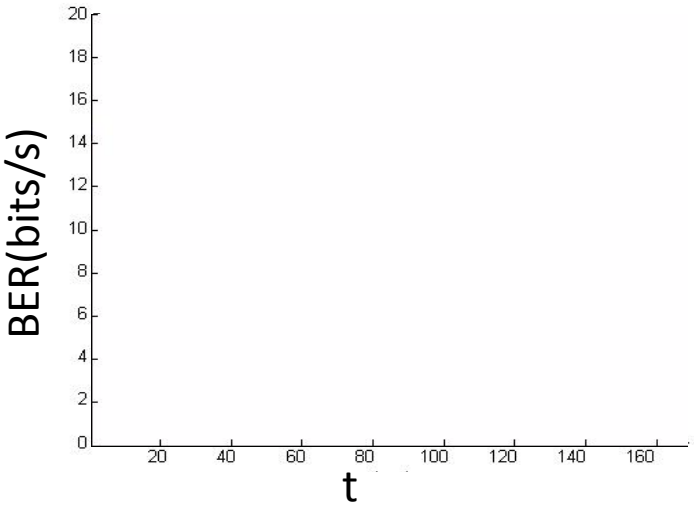
$$P_i^a(t), P_i^b(t) \le P_{\max}$$

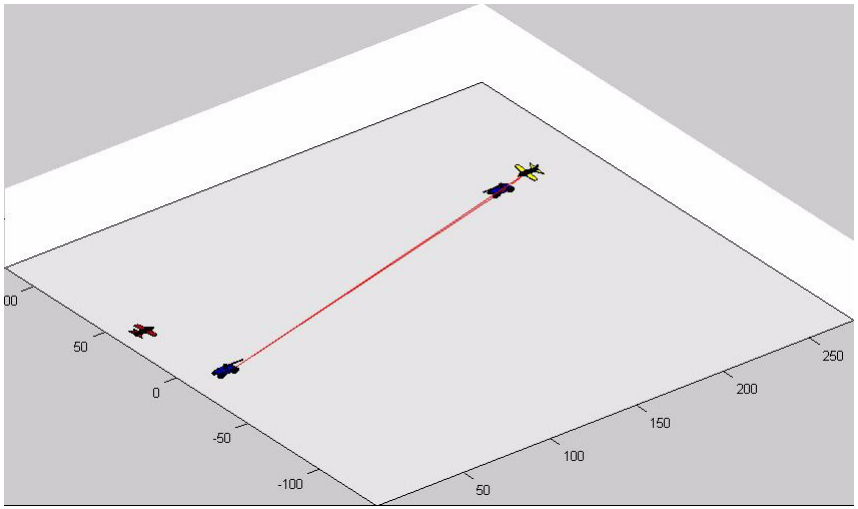
Energy Constraint

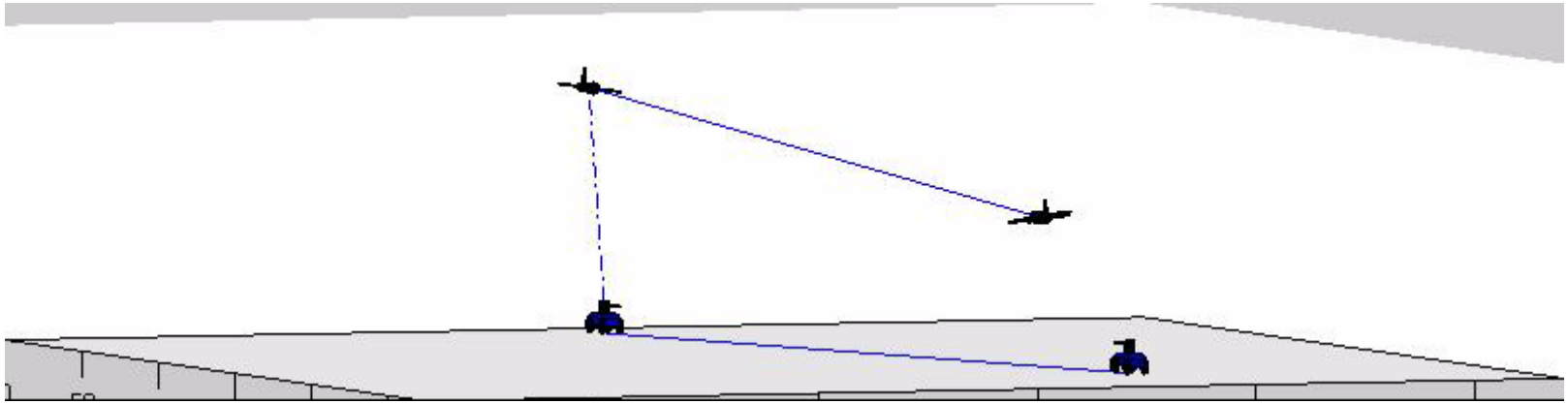
$$\int_0^T P_i(t)dt \le E$$

$$\pi(\mathrm{U},\mathrm{P}) = \int_0^T \underbrace{N\left[p_1^a(t) + p_2^a(t)\right]}_{\text{Team A}} - \underbrace{N\left[p_1^b(t) + p_2^b(t)\right]}_{\text{Team B}} \mathrm{dt}$$

Double Sided Jamming







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

Hierarchical Solution

Optimal Control

Differential Game

$$\left.\begin{aligned} u_i^{a*} &= \min_{u_i^a} \frac{\partial J}{\partial x_i^a} \bullet f_{x_i}^a(x_i^a, u_i^a, t) \\ u_i^{b*} &= \max_{u_i^b} \frac{\partial J}{\partial x_i^b} \bullet f_{y_i}^b(x_i^b, u_i^b, t) \end{aligned}\right\} \quad i = 1,2 \qquad \frac{d\nabla J}{d\tau} = \frac{\partial H}{\partial x}$$

What are the optimal controls of the agents?

$\delta_i^1, \delta_i^2, \delta_{ij}$

$\gamma_1^i, \gamma_2^i, \gamma^{ij}$

Power Allocation

Continuous Kernel Game

Team A

$$\min_{P_i^a, \gamma_1^i, \gamma_2^i, \gamma^{ij}} (p_n^a + p_n^b - p_n^b)$$

$$0 \le P_i^a(t) \le P_{\max}, \gamma_1^i, \gamma_2^i, \gamma^{ij} \in \Delta^3$$

Team B

$$\max_{P_i^b, \delta_i^1, \delta_i^2, \delta_{ij}} (p_n^a + p_n^a - p_j^b)$$

$$0 \le P_b^i(t) \le P_{\max}, \delta_i^1, \delta_i^2, \delta_{ij} \in \Delta^3$$

What is the optimal power allocation of the agents?

M^a, M^b

Communication Scheme

Matrix Game

	$M^b(1)$	$\cdots$	$M^b(m)$
$M^a(1)$	$L(M^a(1), M^b(1))$	$\cdots$	$L(M^a(1), M^b(m))$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$M^a(n)$	$L(M^a(n), M^b(1))$	$\cdots$	$L(M^a(n), M^b(m))$

What is the optimal communication scheme within a team?

Double Sided Jamming

Unintentional Fratricide from Team Members

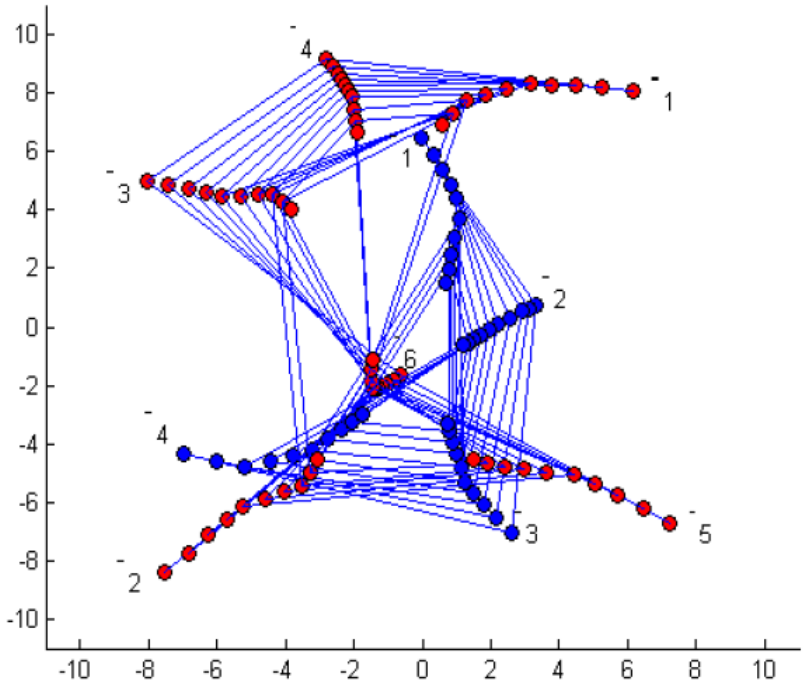
- SINR received at a_j due to transmission from a_i

$$s_{ij}^{a} = \frac{P_i^a \gamma_{ij} (1 + d_{ij}^a)^{-\alpha}}{\frac{\sigma^2}{\rho} + \underbrace{\sum_{k \neq i,j} P_k^a \gamma_{kj} (1 + d_{kj}^a)^{-\alpha}}_{\text{Interference from team members}} + \underbrace{\sum_{k=1}^{m} P_k^b \delta_k (1 + d_{kj}^{ba})^{-\alpha}}_{\text{Jamming from the opponent team}}}$$

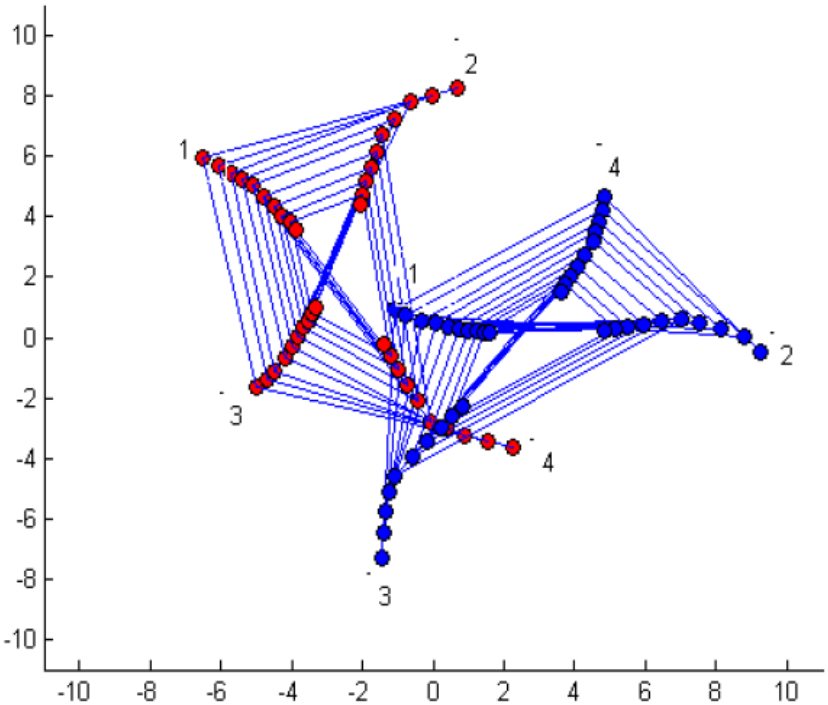
[*Bhattacharya & Başar, CDC'12*]

Double Sided Jamming

4 Blue v. 6 Red



4 Blue v. 4 Red



Max speed= 0.1 units/sec
T=10 sec
f(red)=370 MHz, f(blue)=60 MHz,

[Bhattacharya & Başar, CDC'12]

Conclusion

- Multi-agent networks loaded with challenging issues: sensing, control, communication, coordination, trust, jamming, adversarial action, resilience, …
- What/when/how to transmit, receive, control, and jam with limited opportunities and under limited resources
- Working with minimal inform on intentions, actions, objectives of other agents – learning along the way
- Complications mobility brings in when there are primary tasks (formation, connectivity) and secondary objectives (jamming)

Conclusion

- Multi-agent networks loaded with challenging issues: sensing, control, communication, coordination, trust, jamming, adversarial action, resilience, …
- **Systems and Control with elements of game theory and emerging network science is a fertile area of research with promising returns**
- Complications mobility brings in when there are primary tasks (formation, connectivity) and secondary objectives (jamming)

THANKS !