微分博弈与应用

引言

- 微分博弈是连续时间的随机博弈，由艾萨克斯（Isaacs，1954）引入。该理论起源于20世纪50年代美国空军开展的军事对抗中双方追逃问题的研究。
- 在时间连续的系统内，多个参与者进行持续的博弈，力图最优化各自独立、冲突的目标，最终获得各参与者随时间演变的策略并达到纳什均衡。微分博弈是最优控制与博弈论的结合。随着博弈种类的拓展和解法的完善，它已被应用于网络安全、经济学、管理学、环境科学等越来越多的领域。
- 典型应用：宏观攻防对抗中的最优策略选择；对抗APT攻击等。

引言

- 最优控制
  - 对一个受控的动力学系统或运动过程，从一类允许的控制方案中找出一个最优的控制方案，使系统的运动在由某个初始状态转移到指定的目标状态的同时，其性能指标值为最优。
- 微分博弈是一类最优控制问题
  - 最优控制涉及一个系统或过程，微分博弈则涉及两个或多个控制人，他们之间的控制方案会互相影响。

引言

❖ 最优控制典例

- 确定一个最优飞行控制方式使空间飞行器由一个轨道转换到另一轨道过程中燃料消耗最少；
- 选择一个温度的调节规律和原料配比使化工反应过程的产量最多；
- 制定一项最合理的人口政策使人口发展过程中老化指数、抚养指数和劳动力指数等为最优。
- 网络系统中的攻防双方分别制定各自的攻防策略使得系统安全状态变化过程中的安全损失最大/最小。（微分博弈）

❖ 上述问题都是连续动态变化的过程。

第一节：微分博弈基本概念

❖ 微分博弈定义及构成要素

- 假设一个时间连续系统状态的变化描述为 $\dot{x}(t) = f(t, x, u_1, u_2) \quad t \in [t_0, t_f]$，

  初始条件为 $x(t_0) = x_0.$

- 博弈参与人 $i = 1, 2.$

- 参与人 i 的控制策略 $u_i(t)$

- 参与人 i 的效益 $J_i(u_1, u_2) = h_i(x(t_f)) + \int_{t_0}^{t_f} g_i(t, x(t), u_1(t), u_2(t))\, dt,$ 其中，h_i 为最终效益，g_i 为所定义的效益。

- 参与人 i 的博弈目标 $\max_{u_i(t)} J_i(u_i, u_{-i}^*).$

第一节：微分博弈基本概念

- 典型最优控制问题：

用控制方案改变系统状态以达到最优性能指标

- 被控对象的状态方程为 $\dot{x}(t) = f(x(t), u(t), t), \quad x(t_0) = x_0.$
- 容许控制方案 $u \in U$，U 为控制集。
- 起始状态通常是已知的，即 $x(t_0) = x_0$，而最终所达到的状态（末态）可以是状态空间中的一个点，或事先规定的范围内。

对末态的要求可以用末态约束条件来表示 $\begin{cases} m(x(t_f), t_f) = 0 \\ m(x(t_f), t_f) \le 0 \end{cases}$

第一节：微分博弈基本概念

- 目标集，$x(t_f) \in S$

$$S = \{x(t_f); x(t_f) \in \mathbb{R}^n, m(x(t_f), t_f) = 0, m(x(t_f), t_f) \le 0\}$$

- 最优化性能指标，$J(u) = h(x(t_f), t_f) + \int_{t_0}^{t_f} g(x(t), u(t), t)dt.$

其中，$h(x(t_f), t_f)$ 为最终效益，$g(x(t), u(t), t)$ 为所定义的效益。

第一节：微分博弈基本概念

- 例小车的能量最优控制（无约束最优控制问题）
- x_1位置，x_2速度，u加速度，则质量为1的小车的状态方程为：

$$\dot{x}_1(t) = x_2(t),$$

$$\dot{x}_2(t) = u(t).$$

- 要将状态从初始的$x(t_0) = x_0$控制到$x(t_f) = x_f$，最小化能量：

$$\min J(u) = \int_{t_0}^{t_f} \frac{1}{2} u^2(t) dt$$

第一节：微分博弈基本概念

Given a functional $f : \mathcal{S} \to \mathcal{R}$, where $\mathcal{S}$ is a vector space, and given a subset $\mathcal{X} \subseteq \mathcal{S}$, by the optimization problem

$$\text{minimize } f(x) \text{ subject to } x \in \mathcal{X}$$

we mean the problem of finding an element $x^* \in \mathcal{X}$ (called a *minimizing element* or an *optimal solution*) such that

$$f(x^*) \leq f(x) \qquad \forall x \in \mathcal{X}.$$

最优解的存在性

let $g_j : \mathbb{R}^n \to \mathbb{R}$ be a continuously differentiable function, for $j = 1, \ldots, m$, where $m < n$. Let $\mathcal{X} = \{g_j(x) = 0,\ j = 1, \ldots, m\}$, and consider again the minimization of f over $\mathcal{X}$. This is known as an *optimization problem with equality constraints*. We can write these constraints also using the compact notation $g(x) = 0$, where $g := (g_1, \ldots, g_m)^T$. Let $x^* \in \mathcal{X}$ be a locally minimizing solution for this optimization problem, and x^* be a *regular point* of the constraints, meaning that the $m \times n$ matrix $dg(x^*)/dx$ is of full rank m, that is the *Jacobian* of g is full rank. Then, there exist m scalars, $\{\lambda_j, j = 1, \ldots, m\}$ (called *Lagrange multipliers*), such that the *Lagrangian*

$$L(x;\lambda) = f(x) + \sum_{j=1}^{m} \lambda_j g_j(x) =: f(x) + \lambda^T g(x)$$

has a stationary point at $x = x^*$, that is $\nabla_x L(x^*;\lambda) = 0$, along with the condition $g(x^*) = 0$. This is of course a necessary condition (under the regularity assumption) also for global minima.

第一节：微分博弈基本概念

Given a functional $f : \mathcal{S} \to \mathcal{R}$, where $\mathcal{S}$ is a vector space, and given a subset $\mathcal{X} \subseteq \mathcal{S}$, by the optimization problem

$$\text{minimize } f(x) \text{ subject to } x \in \mathcal{X}$$

we mean the problem of finding an element $x^* \in \mathcal{X}$ (called a *minimizing element* or an *optimal solution*) such that

$$f(x^*) \leq f(x) \qquad \forall x \in \mathcal{X}.$$

最优解的存在性

is the so called *Karush-Kuhn-Tucker constraint qualification condition*, which requires that the vectors

$$\frac{\partial g_j(x^*)}{\partial x}, j = 1, \ldots, m; \quad \frac{\partial h_k(x^*)}{\partial x}, k \in \mathcal{K}^*$$

be linearly independent. Then, there exist multipliers, $\lambda_j, j = 1, \ldots, m$; $\mu_k \geq 0, k = 1, \ldots, p$, such that the *Lagrangian*

拉格朗日(Lagrangian)函数：

$$L(x, \lambda, \nu) = f(x) + \sum_{j=1}^{m} \lambda_j g_j(x) + \sum_{k=1}^{p} \mu_k h_k(x)$$

第一节：微分博弈基本概念

- 最优控制问题的变分法求解
- 设系统状态方程

$$\dot{x}(t) = f(x(t), u(t), t), \quad x(t_0) = x_0, \; u \in U.$$

- 性能指标

$$J = h(x(t_f), t_f) + \int_{t_0}^{t_f} g(x(t), u(t), t)dt.$$

- 寻求最优控制 $u^*(t)$ 及最优状态轨迹 $x^*(t)$，使性能指标取极值。

第一节：微分博弈基本概念

- 初始时刻t_0及始端状态$x(t_0)$给定，t_f给定，终端自由
- 构造增广泛函

$$J_a = h(x(t_f), t_f) + \int_{t_0}^{t_f} \left\{ g(x,u,t) + p^T \left[f(x,u,t) - \dot{x} \right] \right\} dt.$$

- 构造汉密尔顿函数 $H(x,u,p,t) = g(x,u,t) + p^T f(x,u,t)$
- 则有 $J_a = h(x(t_f), t_f) + \int_{t_0}^{t_f} H(x,u,p,t) - p^T \dot{x}\, dt.$
- 令

$$\delta J_a = \left(\frac{\partial h}{\partial x}\right)^T \delta x\big|_{t=t_f} + \int_{t_0}^{t_f} \left(\frac{\partial H}{\partial x}\right)^T \delta x + \left(\frac{\partial H}{\partial u}\right)^T \delta u + \left(\frac{\partial H}{\partial p}\right)^T \delta p - \dot{x}^T \delta p - p^T \delta \dot{x}\, dt = 0.$$

第一节：微分博弈基本概念

- 注意到

$$\int_{t_0}^{t_f} p^T \delta \dot{x}\, dt = p^T \delta x \Big|_{t_0}^{t_f} - \int_{t_0}^{t_f} \dot{p}^T \delta x dt \quad \delta x(t_0) = 0$$

- 所以有

$$\delta J_a = (\frac{\partial h}{\partial x} - p)^T \delta x \Big|_{t=t_f} + \int_{t_0}^{t_f} \left[(\frac{\partial H}{\partial x} + \dot{p})^T \delta x + (\frac{\partial H}{\partial u})^T \delta u + (\frac{\partial H}{\partial p} - \dot{x})^T \delta p \right] dt = 0.$$

- 为使上式成立，应同时满足下列方程

  - 欧拉方程（协态方程） $\dot{p} = -\frac{\partial \mathrm{H}}{\partial x}$
  - 状态方程 $\dot{x} = +\frac{\partial \mathrm{H}}{\partial p}$
  - 控制方程 $\frac{\partial \mathrm{H}}{\partial u} = 0$

第一节：微分博弈基本概念

$$\delta J_a = (\frac{\partial h}{\partial x} - p)^T \delta x|_{t=t_f} + \int_{t_0}^{t_f} \left[(\frac{\partial H}{\partial x} + \dot{p})^T \delta x + (\frac{\partial H}{\partial u})^T \delta u + (\frac{\partial H}{\partial p} - \dot{x})^T \delta p \right] dt = 0.$$

- 横截条件

$$(\frac{\partial h}{\partial x} - p)^T \delta x|_{t=t_f} = 0$$

$$x(t_0) = x_0$$

$$p(t_f) = \frac{\partial h}{\partial x}|_{t=t_f}$$

❖ 对于两端固定的情况下横截条件为

$$x(t_0) = x_0, x(t_f) = x_f.$$

- **Pontryagin's minimum principle（PMP），庞特里亚金极值原理（由汉密尔顿方程组发展而来）**
  - 状态方程为 $\dot{x}(t) = f(x(t), u(t), t), \quad x(t_0) = x_0.$
  - 容许控制 $u \in U$
  - 最优化性能指标 $J(u) = h(x(t_f), t_f) + \int_{t_0}^{t_f} g(x(t), u(t), t)dt.$

第一节：微分博弈基本概念

- 汉密尔顿函数（Hamiltonian）

$$\mathrm{H}(x(t),u(t),p(t),t) \triangleq g(x(t),u(t),t) + p^{T}(t) f(x(t),u(t),t).$$

- 则最优控制 $u^{*} \in U$ 的必要条件如下

- 极值条件 $u,u^{*} \in U, \forall t \in [t_0, t_f]$

$$\mathrm{H}(x^{*}(t),u^{*}(t),p^{*}(t),t) \leq \mathrm{H}(x^{*}(t),u(t),p^{*}(t),t).$$

第一节：微分博弈基本概念

- 规范方程：$\forall t \in [t_0, t_f]$
- 状态（state）方程：$$\dot{x}^*(t) = +\frac{\partial \mathrm{H}(x^*(t), u^*(t), p^*(t), t)}{\partial p}$$
- 协态（costate）方程：$$\dot{p}^*(t) = -\frac{\partial \mathrm{H}(x^*(t), u^*(t), p^*(t), t)}{\partial x}$$
- 边界条件（用于处理目标集）：

$$\left[\frac{\partial h(x^*(t_f), t_f)}{\partial x} - p^*(t_f)\right]^T \delta x_f$$

$$+\left[\mathrm{H}(x^*(t_f), u^*(t_f), p^*(t_f), t_f) + \frac{\partial h(x^*(t_f), t_f)}{\partial t}\right]\delta t_f = 0$$

- 例：设系统状态方程为 $\dot{x}(t) = -x(t) + u(t)$
- 边界条件为 $x(0) = 1, x(t_f) = 0$
- 求最优控制 $u(t)$ 使下列性能指标最小。

$$J = \frac{1}{2}\int_{t_0}^{t_f}(x^2 + u^2)dt$$

- 解：构造哈密尔顿函数

$$H = \frac{1}{2}(x^2 + u^2) + p(-x + u)$$

- 协态方程 $\dot{p} = -\frac{\partial H}{\partial x} = -x + p$

第一节：微分博弈基本概念

- 状态方程 $\dot{x}(t)=\dfrac{\partial H}{\partial p}=-x+u$
- 控制方程 $\dfrac{\partial H}{\partial u}=u+p=0$
- 消除 u

$$\begin{cases}\dot{p}=-x+p\\ \dot{x}=-x+u=-x-p\end{cases}\Rightarrow\begin{bmatrix}\dot{p}\\ \dot{x}\end{bmatrix}=\begin{bmatrix}1 & -1\\ -1 & -1\end{bmatrix}\begin{bmatrix}p\\ x\end{bmatrix}$$

- 得到

$$x=\frac{1}{2\sqrt{2}}\left[(\sqrt{2}+1)e^{-\sqrt{2}t}+(\sqrt{2}-1)e^{\sqrt{2}t}\right]x(0)+\frac{1}{2\sqrt{2}}(e^{-\sqrt{2}t}-e^{\sqrt{2}t})p(0)$$

$$p=\frac{1}{2\sqrt{2}}\left(e^{-\sqrt{2}t}+e^{\sqrt{2}t}\right)x(0)+\frac{1}{2\sqrt{2}}\left[\left(\sqrt{2}-1\right)e^{-\sqrt{2}t}-\left(\sqrt{2}+1\right)e^{\sqrt{2}t}\right]p(0)$$

第一节：微分博弈基本概念

❖ 由边界条件 $x(0)=1, x(t_f)=0$

$$p(0)=\frac{\left(\sqrt{2}+1\right)e^{-\sqrt{2}t_f}+\left(\sqrt{2}-1\right)e^{\sqrt{2}t_f}}{e^{\sqrt{2}t_f}-e^{-\sqrt{2}t_f}}$$

❖ 得最优控制

$$u^*=-p=$$

$$-\frac{1}{2\sqrt{2}}\left\{e^{-\sqrt{2}t}-e^{\sqrt{2}t}+\frac{\left(\sqrt{2}+1\right)e^{-\sqrt{2}t_f}+\left(\sqrt{2}-1\right)e^{\sqrt{2}t_f}}{e^{\sqrt{2}t_f}-e^{-\sqrt{2}t_f}}\left[(\sqrt{2}-1)e^{-\sqrt{2}t}+(\sqrt{2}+1)e^{\sqrt{2}t}\right]\right\}$$

第一节：微分博弈基本概念

- 而对于微分博弈，博弈双方的状态方程为

$$\dot{x}(t) = f(x(t), u_1(t), u_2(t), t), \quad x(t_0) = x_0.$$

- 容许控制，即策略（一般叫做控制策略），$u_1 \in U_1, u_2 \in U_2$

- 二者均最优化各自的性能指标

$$J_1(u_1, u_2) = h_1(x(t_f), t_f) + \int_{t_0}^{t_f} g_1(x(t), u_1(t), u_2(t), t)dt.$$

$$J_2(u_1, u_2) = h_2(x(t_f), t_f) + \int_{t_0}^{t_f} g_2(x(t), u_1(t), u_2(t), t)dt.$$

第一节：微分博弈基本概念

- 一些假定
- 条件（A1）：对于任意可行的 $t, x, \forall q_1, q_2 \in \mathbb{R}^n$，方程组有唯一解

$$u_1^* = \arg\min_{u_1 \in U_1} \{q_1^T f(x, u_1, u_2^*, t) + g_1(x, u_1, u_2^*, t)\}$$

$$u_2^* = \arg\min_{u_2 \in U_2} \{q_2^T f(x, u_1^*, u_2, t) + g_2(x, u_1^*, u_2, t)\}$$

- 假定微分博弈的参与人具有如下共同知识
- 初始状态x_0，状态方程f，以及x，u_1，u_2的容许集合
- J_1，J_2的形式，即g_1，g_2，h_1，h_2

第一节：微分博弈基本概念

- 两人零和微分博弈的均衡求解（利用PMP）
- 博弈双方的状态方程为

$$\dot{x}(t) = f(x(t), u_1(t), u_2(t), t), \quad x(t_0) = x_0.$$

- 容许控制， $u_1 \in U_1, u_2 \in U_2$
- 局中人1最小化性能指标，局中人2最大化性能指标

$$J_1(u_1, u_2) = h(x(t_f), t_f) + \int_{t_0}^{t_f} g(x(t), u_1(t), u_2(t), t)dt.$$

第一节：微分博弈基本概念

❖ 定义汉密尔顿函数Hamiltonian

$$\mathrm{H}(x(t),u_1(t),u_2(t),p(t),t) \triangleq g(x(t),u_1(t),u_2(t),t) + p^T(t) f(x(t),u_1(t),u_2(t),t),$$

❖ 微分博弈的均衡 $u_1^* \in U_1, u_2^* \in U_2$ 满足极值条件

$$u_1, u_1^* \in U_1, u_2, u_2^* \in U_2, \forall t \in [t_0, t_f]$$

$$\mathrm{H}(x^*(t),u_1^*(t),u_2^*(t),p^*(t),t)$$

$$= \min_{u_1} \max_{u_2} \mathrm{H}(x^*(t),u_1(t),u_2(t),p^*(t),t)$$

$$= \max_{u_2} \min_{u_1} \mathrm{H}(x^*(t),u_1(t),u_2(t),p^*(t),t)$$

❖ 规范方程： $\forall t \in [t_0, t_f]$

第一节：微分博弈基本概念

- 状态（state）方程：

$$\dot{x}^*(t) = +\frac{\partial \mathrm{H}}{\partial p}(x^*(t), u_1^*(t), u_2^*(t), p^*(t), t)$$

- 协态（costate）方程：

$$\dot{p}^*(t) = -\frac{\partial \mathrm{H}}{\partial x}(x^*(t), u_1^*(t), u_2^*(t), p^*(t), t)$$

- 边界条件：

$$[h_x(x^*(t_f), t_f) - p^*(t_f)]^T \delta x_f$$
$$+[\mathrm{H}(x^*(t_f), u_1^*(t_f), u_2^*(t_f), p^*(t_f), t_f) + h_t(x^*(t_f), t_f)]\delta t_f = 0$$

第一节：微分博弈基本概念

- 两人零和微分博弈均衡的简单证明
- （固定$u_2^*(t)$，求局中人1最优控制）给定$u_2^*(t)$，$H_1 = H$，局中人1的最优控制满足

$$\mathrm{H}(x^*(t),u_1^*(t),u_2^*(t),p_1^*(t),t) \le \mathrm{H}(x^*(t),u_1(t),u_2^*(t),p_1^*(t),t).$$

$$\dot{x}^*(t) = \frac{\partial \mathrm{H}}{\partial p_1} = f(x^*(t),u_1^*(t),u_2^*(t),p_1^*(t),t)$$

$$\dot{p}_1^* = -\frac{\partial \mathrm{H}}{\partial x}$$

$$[h_x(x^*(t_f),t_f) - p_1^*(t_f)]^T \delta x_f$$

$$+[\mathrm{H}(x^*(t_f),u_1^*(t_f),u_2^*(t_f),p_1^*(t_f),t_f) + h_t(x^*(t_f),t_f)]\delta t_f = 0$$

- （固定$u_1^*(t)$，求局中人2最优控制）给定$u_1^*(t)$，局中人2

最小化 $$-J(u_1^*,u_2)=-h(x(t_f),t_f)+\int_{t_0}^{t_f}-g(x(t),u_1^*(t),u_2(t),t)dt$$

- 则有

$$\mathrm{H}_2(x,u_1,u_2,p_2,t)\triangleq -g+p_2 f=-\mathrm{H}(x,u_1,u_2,-p_2,t)$$

$$-\mathrm{H}(x^*(t),u_1^*(t),u_2^*(t),-p_2^*(t),t)\le -\mathrm{H}(x^*(t),u_1^*(t),u_2(t),-p_2^*(t),t)$$

$$\dot{x}^*(t)=\frac{\partial \mathrm{H}_2}{\partial p_2}=f(x^*(t),u_1^*(t),u_2^*(t),t)$$

$$\dot{p}_2^*=-\frac{\partial \mathrm{H}_2}{\partial x}=\frac{\partial \mathrm{H}(x^*,u_1^*,u_2^*,-p_2^*,t)}{\partial x}$$

$$[-h_x(x^*(t_f),t_f)-p_2^*(t_f)]^T\delta x_f$$

$$+[-\mathrm{H}(x^*(t_f),u_1^*(t_f),u_2^*(t_f),-p_2^*(t_f),t_f)-h_t(x^*(t_f),t_f)]\delta t_f=0$$

- （联立两组方程得均衡）以上分别得到给定对方策略的反应“函数”，联立得

$$p_1^* = -p_2^*, \forall t \in [t_0, t_f]$$

命题得证。

第一节：微分博弈基本概念

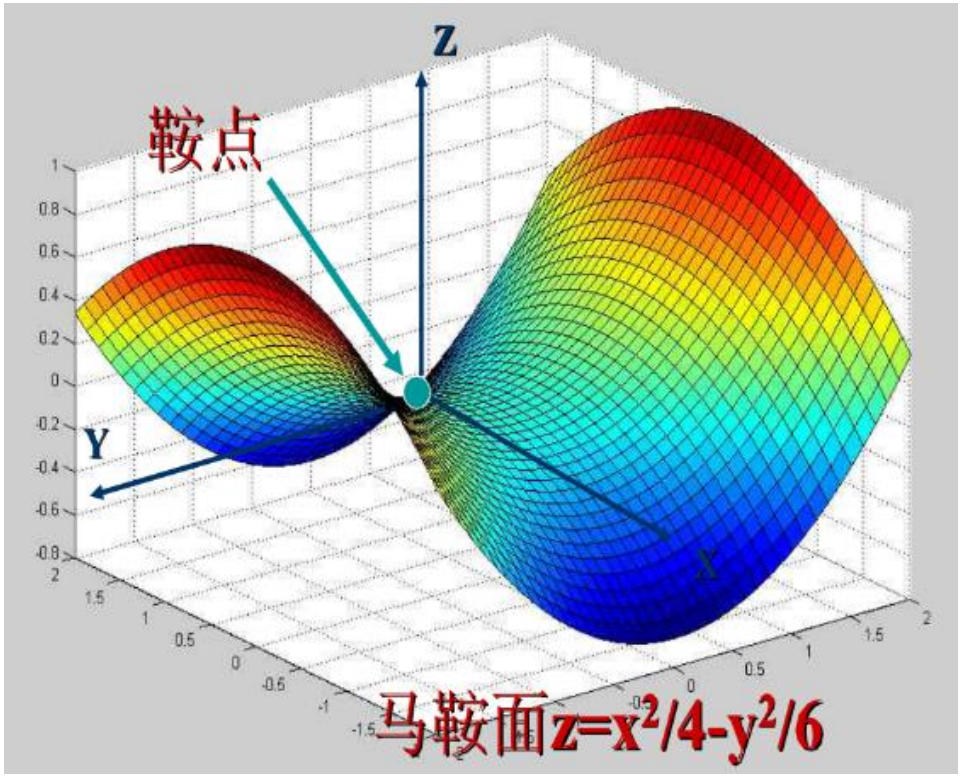
- 鞍点（saddle point）
- 物理上指在一个方向是极大值另一方向是极小值的点。
- 在矩阵中，一个数在所在的行中是最大值，在所在的列中是最小值，则被称为鞍点。
- 在微分方程中，沿着某一方向是稳定的，另一条方向是不稳定的奇点，叫做鞍点。

第一节：微分博弈基本概念

- 鞍点问题
- 在证券市场上，股民们总想“在最小风险下获得最大收益”。生产者总想“在最小投入下获得最大产出”，都是这一辩证思想的体现。
- 将这一思想用数学模型表述，即“极大中的极小”或“极小中的极大”。在数学中，把函数上具有此“极大-极小”性质的点称为鞍点，把同鞍点有关的数学问题称为鞍点问题

第一节：微分博弈基本概念

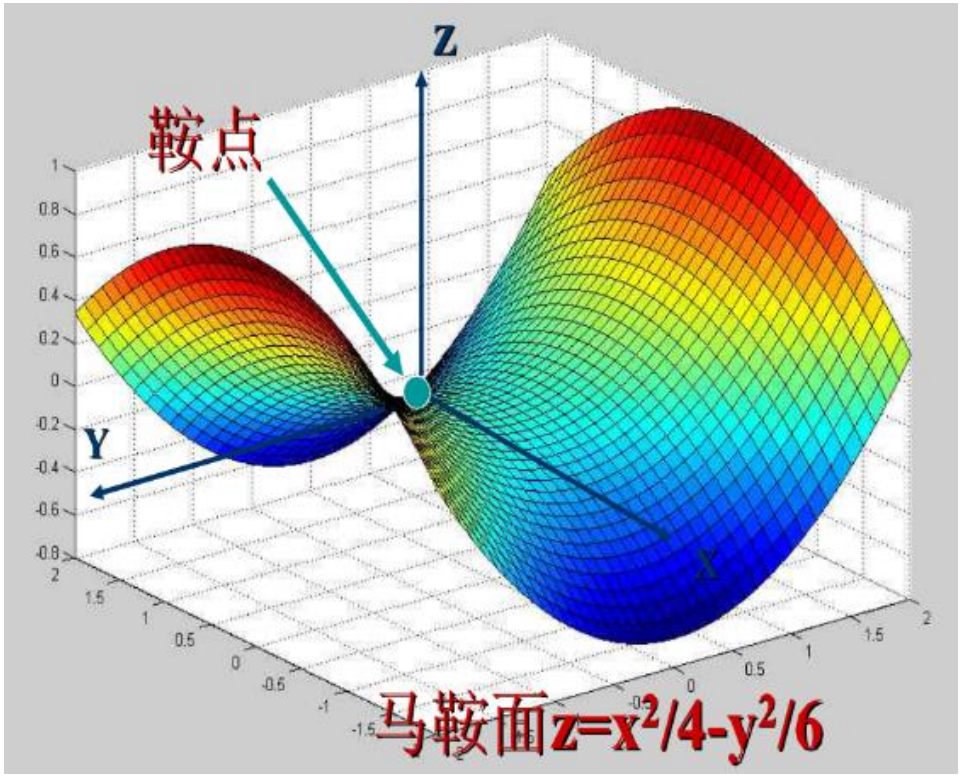
- 鞍点的数学定义
- 对于二元函数$z = f(x, y)$，(x^*, y^*)为其上一点，若在邻域$|x - x^*| < \Delta$，$|y - y^*| < \Delta$内，$f(x, y^*) \leq f(x^*, y^*) \leq f(x^*, y)$恒成立，则称$(x^*, y^*)$为函数的鞍点。



第一节：微分博弈基本概念

❖ 鞍点的数学性质

当$x = x^*$为常数， y变化时，函数$z = f(x, y)$在(x^*, y^*)取得极小值。当$y = y^*$为常数， x变化时，函数$z = f(x, y)$在(x^*, y^*)取得极大值。



第二节：微分博弈应用示例 1

- 追逃博弈：导弹希望命中目标，目标希望远离导弹
- 导弹（1）状态方程和目标（2）状态方程分别为

$$\dot{x}_1(t)=v_1(t),\dot{v}_1(t)=u_1(t),x_1(0)=-2,v_2(0)=1.$$

$$\dot{x}_2(t)=v_2(t),\dot{v}_2(t)=u_2(t),x_2(0)=0,v_2(0)=2.$$

- 导弹要在终止时刻$t_f=2$命中目标，$1/E_1$表示能量的权重

$$J_1(u_1,u_2)=\frac{b}{2}\left|x_1(t_f)-x_2(t_f)\right|^2+\int_{t_0}^{t_f}\frac{1}{2E_1}u_1(t)^2dt$$

- 目标要在终止时刻$t_f=2$远离导弹，$E_2<E_1$

$$J_2(u_1,u_2)=-\frac{b}{2}\left|x_1(t_f)-x_2(t_f)\right|^2+\int_{t_0}^{t_f}\frac{1}{2E_2}u_2(t)^2dt$$

第二节：微分博弈应用示例 1

- 零和追逃博弈的均衡（转化为零和博弈形式）
- 引入状态将原问题转化为两人零和追逃博弈

$$x = x_1 - x_2, v = v_1 - v_2$$

$$\dot{x}(t) = \dot{x}_1(t) - \dot{x}_2(t) = v_1 - v_2 = v. \quad x(0) = -2 - 0 = -2$$

$$\dot{v}(t) = \dot{v}_1(t) - \dot{v}_2(t) = u_1 - u_2. \quad v(0) = 1 - 2 = -1$$

- 以及统一的性能指标

$$J(u_1, u_2) = \frac{b}{2} x(t_f)^2 + \int_{t_0}^{t_f} \{\frac{1}{2E_1} u_1(t)^2 - \frac{1}{2E_2} u_2(t)^2\} dt$$

- 追逐者希望最小化$J(u_1, u_2)$，逃跑者则希望将其最大化

第二节：微分博弈应用示例 1

- （计算Hamiltonian，考察极值条件） Hamiltonian与两者的控制均有关

$$\mathrm{H}(x(t), v(t), u_1(t), u_2(t), p_1(t), p_2(t), t)$$
$$= \frac{1}{2E_1} u_1(t)^2 - \frac{1}{2E_2} u_2(t)^2 + p_1(t)v(t) + p_2(t)(u_1(t) - u_2(t))$$

- 极值条件为（对两策略分别求偏导，且都令为0）

$$\frac{\partial \mathrm{H}}{\partial u_1} = 0 \Rightarrow \frac{u_1}{E_1} + p_2 = 0 \Rightarrow u_1^*(t) = -p_2^*(t)E_1$$
$$\frac{\partial \mathrm{H}}{\partial u_2} = 0 \Rightarrow -\frac{u_2}{E_2} - p_2 = 0 \Rightarrow u_2^*(t) = -p_2^*(t)E_2$$

第二节：微分博弈应用示例 1

❖ 将极值条件带入规范方程

$$\mathrm{H}(x(t),v(t),u_1(t),u_2(t),p_1(t),p_2(t),t)$$
$$=\frac{1}{2E_1}u_1(t)^2-\frac{1}{2E_2}u_2(t)^2+p_1(t)v(t)+p_2(t)(u_1(t)-u_2(t))$$

状态方程

$$\dot{x}^*(t)=v^*(t)$$

$$\dot{x}^*(t)=+\frac{\partial \mathrm{H}}{\partial p}(x^*(t),u_1^*(t),u_2^*(t),p^*(t),t)$$

$$\dot{v}^*(t)=u_1^*(t)-u_2^*(t)=-p_2^*(t)(E_1-E_2)$$

协态方程

$$\dot{p}_1^*(t)=-\frac{\partial \mathrm{H}}{\partial x}=0 \quad => \quad p_1^*(t)=c_1$$

$$\dot{p}_2^*(t)=-\frac{\partial \mathrm{H}}{\partial v}=-p_1^*(t) \quad => \quad p_2^*(t)=-c_1t+c_2$$

$$\dot{p}^*(t)=-\frac{\partial \mathrm{H}}{\partial x}(x^*(t),u_1^*(t),u_2^*(t),p^*(t),t)$$

第二节：微分博弈应用示例 1

- 处理边界条件

- t_f固定，x_f自由。边界必要条件

$$0=\frac{\partial h}{\partial x}(x^*(t_f),v^*(t_f),t_f)-p_1^*(t_f)=bx^*(t_f)-p_1^*(t_f)$$

$$0=\frac{\partial h}{\partial v}(x^*(t_f),v^*(t_f),t_f)-p_2^*(t_f)=-p_2^*(t_f)$$

- 以及初值 $x(t_0)=x_0, v(t_0)=v_0$

$$p_2^*(t)=-c_1t+c_2,\ p_2^*(t_f)=0 \Rightarrow c_2=c_1t_f$$

$$p_2^*(t)=-c_1(t-t_f)$$

- 下面把p_2^*带入状态方程

第二节：微分博弈应用示例 1

- （把协态变量带回状态方程）
- 把协态变量 $p_2^*(t) = -c_1(t - t_f)$ 带入状态方程得到

$$\dot{v}^*(t) = -p_2^*(t)(E_1 - E_2) = (E_1 - E_2)c_1(t - t_f)$$

$$\Rightarrow v^*(t) = (E_1 - E_2)c_1\frac{(t - t_f)^2}{2} - (E_1 - E_2)c_1\frac{(t_0 - t_f)^2}{2} + v_0$$

- 再把v^*带入$\dot{x} = v$，

$$x^*(t) = (E_1 - E_2)c_1\frac{(t - t_f)^3}{6} - (E_1 - E_2)c_1\frac{(t_0 - t_f)^3}{6}$$

$$+(-(E_1 - E_2)c_1\frac{(t - t_f)^2}{2} + v_0)(t - t_0) + x_0$$

第二节：微分博弈应用示例 1

- 带入边界条件 $bx^*(t_f) - p_1^*(t_f) = 0$ 得到

$$c_1 = \frac{x_0 + v_0(t_f - t_0)}{1/b + (E_1 - E_2)(t_f - t_0)^3/3}, x^*(t_f) = c_1 / b$$

- 得到微分博弈均衡

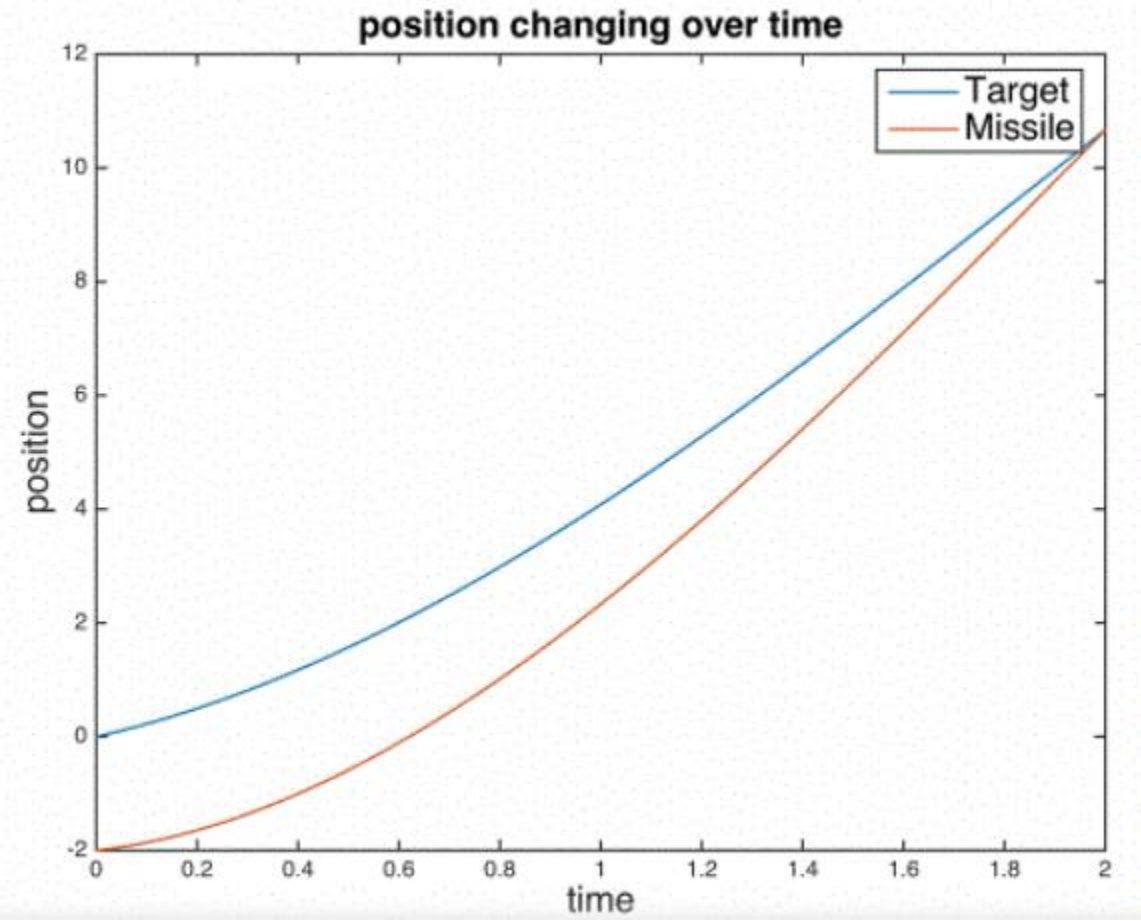
$$u_1^*(t) = -\frac{E_1(t_f - t_0)(x_0 + v_0(t_f - t_0))}{1/b + (E_1 - E_2)(t_f - t_0)^3/3}$$

$$u_2^*(t) = \frac{E_2}{E_1} u_1^*(t)$$

- 令$\mathbf{b} \to \infty$可得微分博弈均衡，$\boldsymbol{E_2 < E_1}$时$\boldsymbol{x^*(t_f) \to 0}$，命中。

第二节：微分博弈应用示例 1

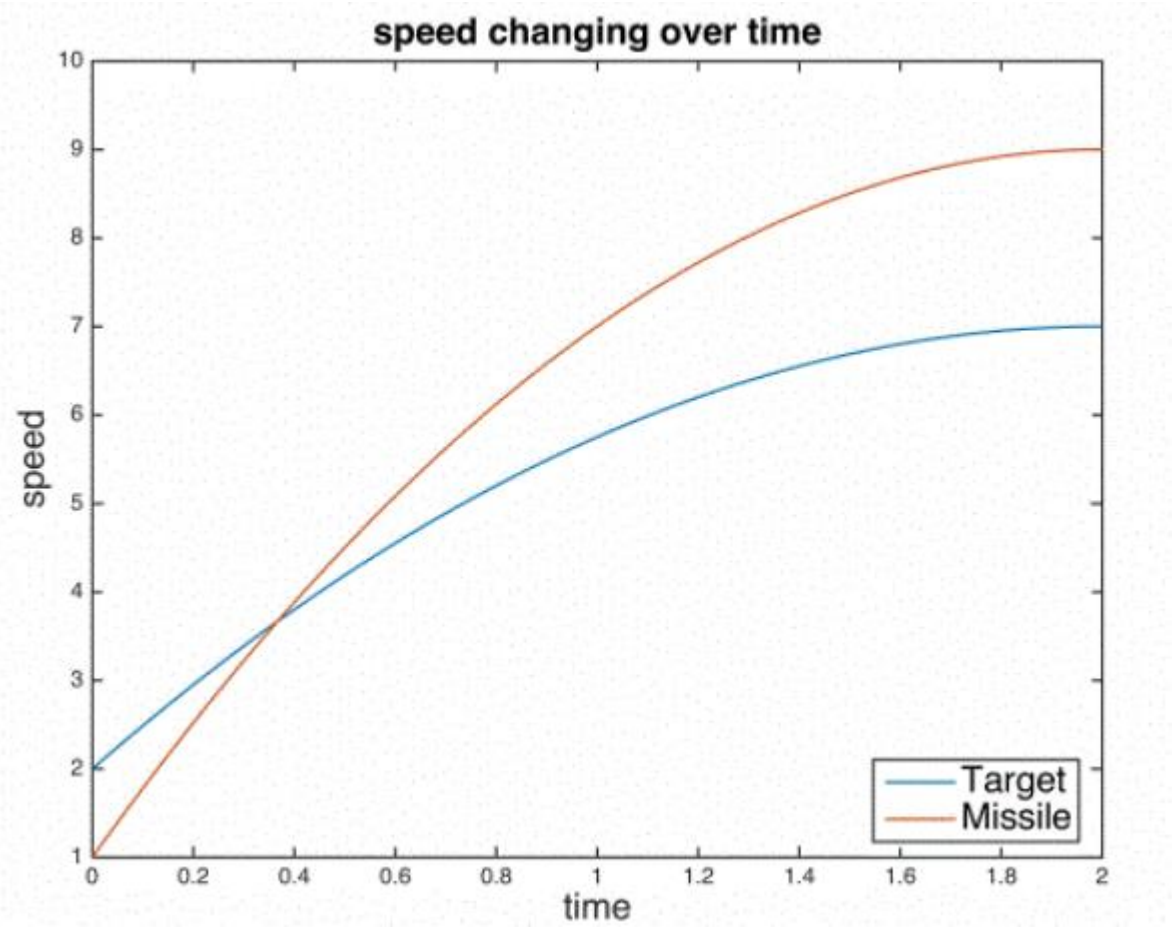
- 零和追逃博弈的均衡：位置--时间



导弹在终止时刻
$t_f = 2$时命中目标

第二节：微分博弈应用示例 1

- 零和追逃博弈的均衡：速度--时间

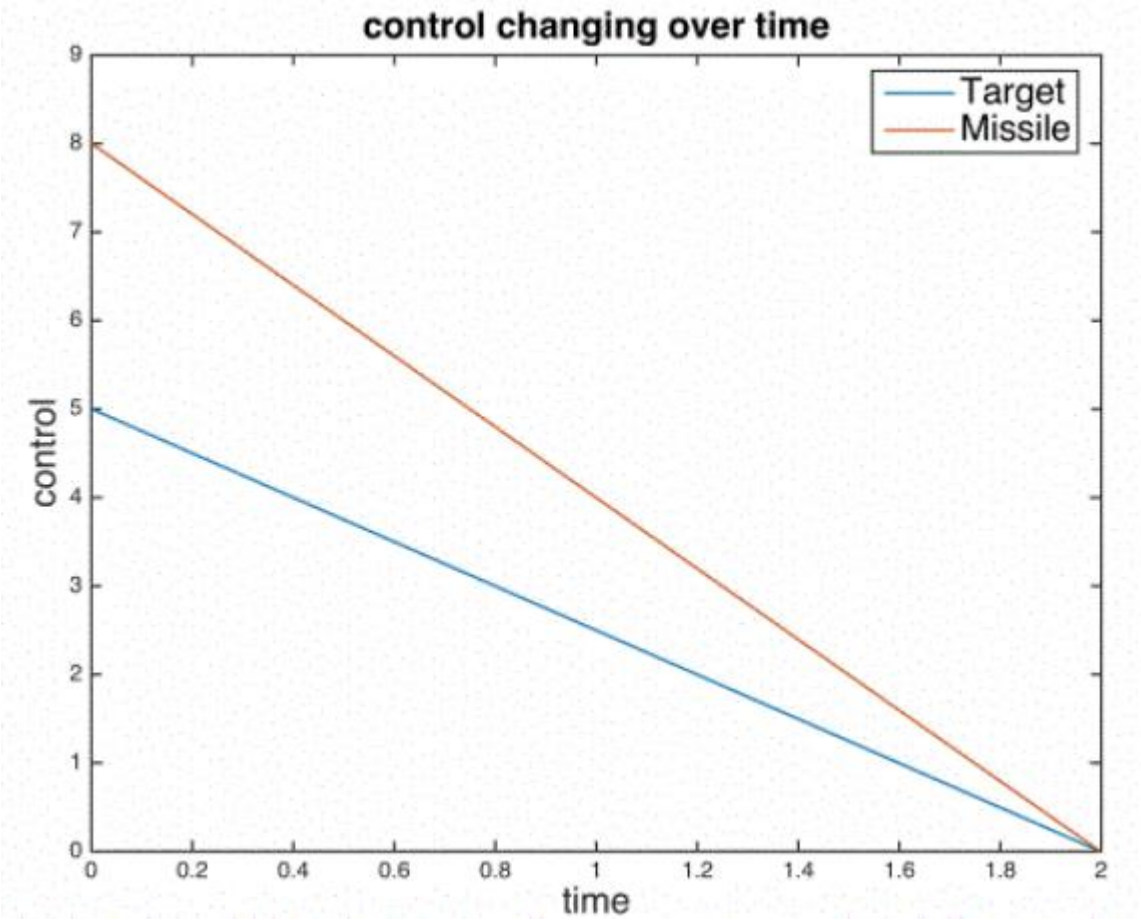


导弹为了命中目标，需提高速度。0.4S后，其速度比目标速度高，在终止时刻$t_f = 2$时命中目标。

第二节：微分博弈应用示例 1

- 零和追逃博弈的均衡：控制--时间。$J_1 = 26.706$，$J_2 = 26.651$

导弹加速度整体都高于目标，最终都为0，最终两者速度趋于平稳。



第二节：微分博弈应用示例 1

- 微分博弈求解的过程

① 固定对方策略，求解最优控制

② 固定己方策略，以对方立场求解最优控制

③ 联立方程组求解博弈均衡

- 微分博弈的缺陷：微分博弈只给出的是一种“按照最坏情况打算”的控制律，仅在对方符合理性人假设的情况下达到最优。

第三节：微分博弈应用示例 2

- 现有的解决网络安全问题的博弈论方法大多采用静态博弈（如矩阵博弈、贝叶斯博弈）或多阶段离散动态博弈（如repeated斯塔克伯格博弈，随机马尔可夫博弈），均无法满足网络攻防的实时性要求。
- 研究内容：把攻击和防御的交互看作动态、实时的过程，利用微分博弈来更准确地描述攻防对抗的快速性和连续性，并为网络防御提供更具及时性的理论指导。

H. Zhang, L. Jiang, S. Huang, J. Wang and Y. Zhang, "Attack-Defense Differential Game Model for Network Defense Strategy Selection," in IEEE Access, vol. 7, pp. 50618-50629, 2019, doi: 10.1109/ACCESS.2018.2880214.

第三节：微分博弈应用示例 2

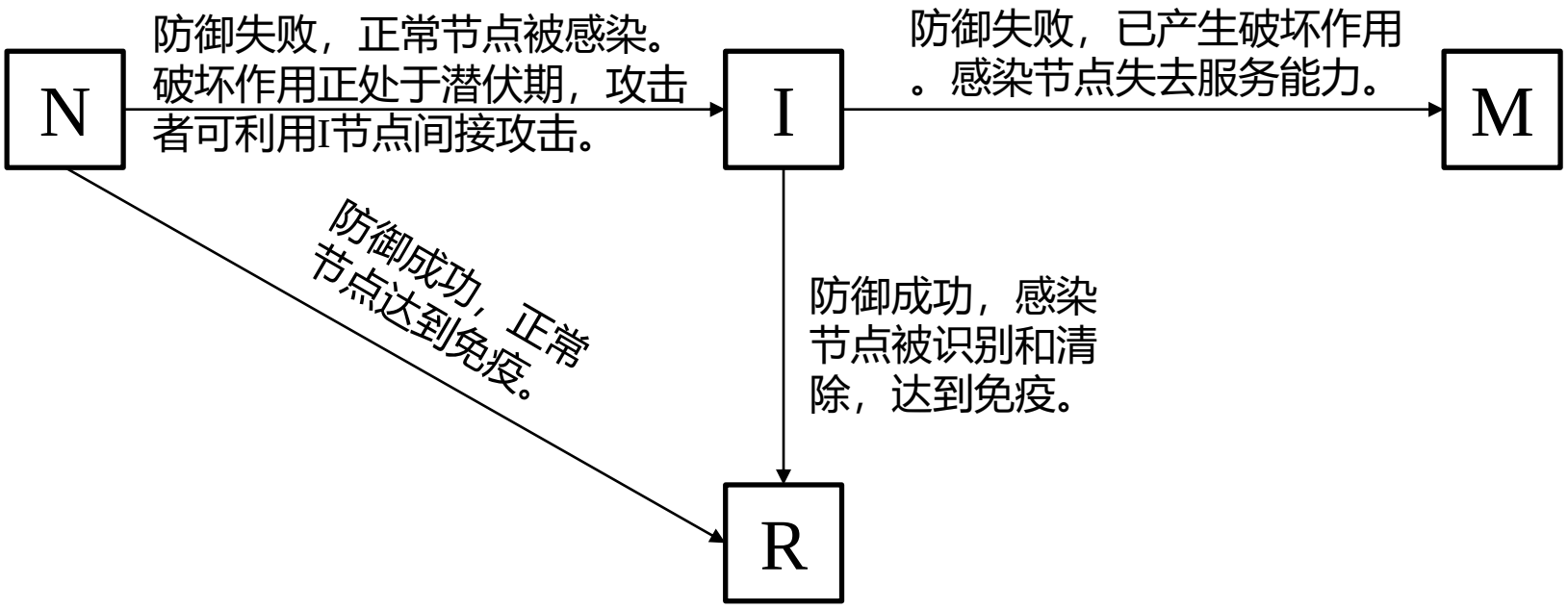
- 传染病动力学理论中的Susceptible Infected Recovered（SIR）模型描述了人群中疾病感染和爆发的动态过程。
- 在网络攻防中，攻击者利用网络节点的漏洞进行攻击。然后从单个节点渗透并感染系统中的其他节点，这类似于传染病的传播和破坏。在节点众多的网络中，攻击和防御也是一个动态演化过程：
  - 组成系统的节点的安全状态不断迁移
  - 处于不同安全状态的节点数量是动态变化的。

第三节：微分博弈应用示例 2

- 系统模型
- 为了描述演化过程，结合SIR模型和实际的网络攻防情况，将节点的安全状态分为：
  - Normal：网络节点工作正常，但节点本身存在漏洞，可能会受到攻击。
  - Infected：网络节点被攻击策略渗透或感染，但其服务质量尚未下降。此外，攻击者可以使用此节点攻击相邻节点。
  - Restored：网络节点受防御策略保护，对攻击策略免疫。
  - Malfunctioned：网络节点的服务质量严重恶化或服务能力丧失。

第三节：微分博弈应用示例 2

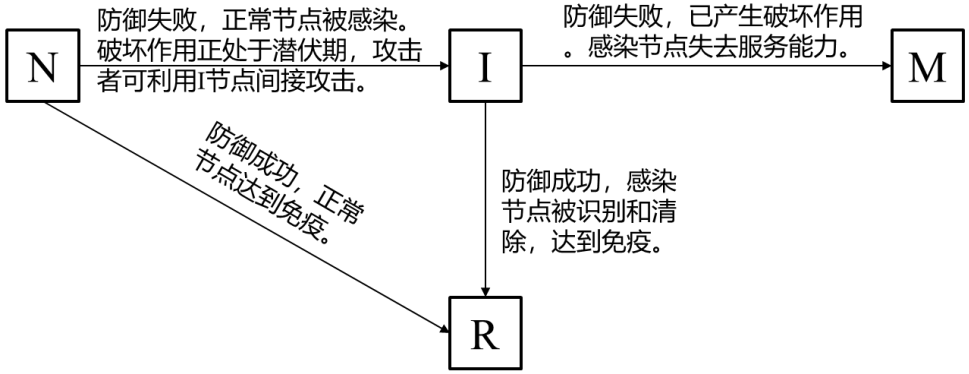
❖ 状态转移路径图示



第三节：微分博弈应用示例 2

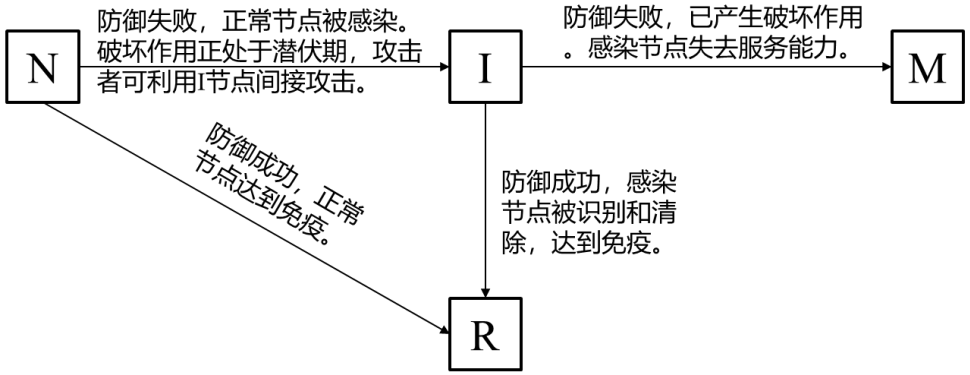
❖ 状态转移

- N→I：面对攻击策略，如果防御策略失败，节点就会被攻击者渗透或感染。此时，攻击破坏效应仍处于潜伏期，节点服务质量并未损失。但是，攻击者可以使用此节点攻击相邻节点进行更大范围的攻击。例如，攻击者使用病毒策略感染网络节点，但不会立即将其销毁。相反，它暂时潜伏并由受感染的节点传播，以争取破坏系统中更多的节点。
- N→R：当防御策略成功时，普通节点对攻击具有免疫力。例如，防御者安装修补程序或更新防病毒软件以抵御病毒。



第三节：微分博弈应用示例 2

- I→R：防御策略成功识别出感染节点，清除渗透或感染。从而限制尚未出现的攻击伤害效果，避免感染节点的损失，使节点进入免疫状态。例如，可以通过更新节点的杀毒软件来清除病毒。
- I→M：被感染节点受到攻击时，如果防御策略失败，会产生伤害效果，失去服务功能。这样，受损节点就无法修复，也无法再用于攻击相邻节点。例如，受感染的节点虽然更新了杀毒软件，但仍然无法在病毒攻击前清除病毒。最后，病毒攻击可能导致节点崩溃并退出网络系统。



第三节：微分博弈应用示例 2

- 通过对传染病动力学理论的研究和迁移路径的分析，总结出影响网络系统中节点状态的主要原因：

① 直接连接到受感染节点的正常节点数：攻击者可以使用受感染的节点攻击相邻的正常节点。因此，与受感染节点相邻的正常节点的数量越大，受感染节点的增长速度可能越快，安全风险往往会增加

② 攻防策略之间的博弈结果。结果是决定状态转换的关键因素。对于一个特定节点，对抗结果直接决定了其状态转移路径。

第三节：微分博弈应用示例 2

- 网络节点总数：Q
- 处于N、I、R、M状态的节点数分别为： N(t)、I(t)、R(t)、M(t)
- 在任意时刻$t \in [t_0, T]$，$N(t), I(t), R(t), M(t) \in \mathbb{N}, N(t) + I(t) + R(t) + M(t) = Q$
- 节点在网络中以密度α部署；对于一个节点，连接到此节点的节点数为：$\alpha\pi r^2$，r为两个节点的网络连接距离。$r = 1$时，表示两节点直连（directly connected）

第三节：微分博弈应用示例 2

- 对于处于感染状态I的节点，可以与其直接通信的相邻节点的数量为：$\alpha\pi$。
- 在时间t，所有节点中正常节点的比例为：N(t)/Q。
- 因此，在整个网络系统中，如果假设网络节点数目较大，且受感染节点之间距离较远，则在t时刻与受感染节点直接连接的正常节点的数目为：$\alpha\pi I(t)N(t)/Q$，（忽略受感染节点影响范围的重叠效应）。如果防御策略失败，上述正常节点将转化为受感染节点。

第三节：微分博弈应用示例 2

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防策略定义

攻击类型	高强度A_H	中强度A_M	低强度A_L
平均强度∈[0,1]	$\overline{e_A^H}$	$\overline{e_A^M}$	$\overline{e_A^L}$
攻击策略	$p_A^H(t)$	$p_A^M(t)$	$p_A^L(t)$
Expected attack utility	$a(t) = p_A^H(t)\,\overline{e_A^H} + p_A^M(t)\overline{e_A^M} + p_A^L(t)\overline{e_A^L}$		

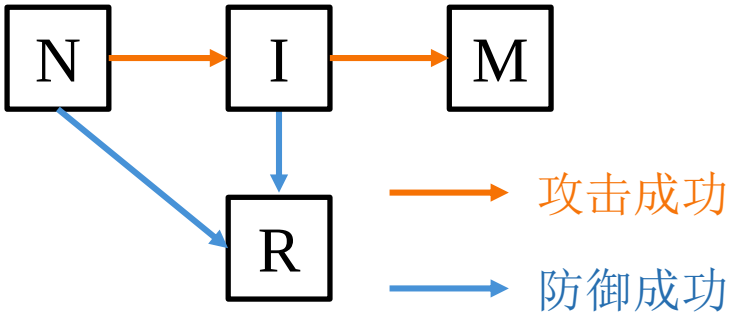
防御类型	高强度D_H	低强度D_L
平均强度	$\overline{e_D^H}$	$\overline{e_D^L}$
攻击策略	$p_D^H(t)$	$p_D^L(t)$
Expected defense utility	$d(t) = p_D^H(t)\,\overline{e_D^H} + p_D^L(t)\overline{e_D^L}$	

第三节：微分博弈应用示例 2

❖ 状态转移与攻防策略的关系

$$\eta(t) = a(t) - d(t) \begin{cases} >0, \text{攻击成功} \\ <0, \text{攻击失败} \end{cases}$$

$$|\eta(t)| \in [0,1]$$



攻击成功：

$$\eta_{\mathrm{NI}} = \begin{cases} 0, & \eta(t) \le 0 \\ \eta(t), & \eta(t) > 0 \end{cases}$$

$$\eta_{\mathrm{IM}} = \begin{cases} 0, & \eta(t) \le 0 \\ \eta(t), & \eta(t) > 0. \end{cases}$$

防御成功：

$$\eta_{\mathrm{NR}} = \begin{cases} |\eta(t)|, & \eta(t) \le 0 \\ 0, & \eta(t) > 0 \end{cases}$$

$$\eta_{\mathrm{IR}} = \begin{cases} |\eta(t)|, & \eta(t) \le 0 \\ 0, & \eta(t) > 0 \end{cases}$$

第三节：微分博弈应用示例 2

- 状态转移方程

$$\begin{cases} \dot{N} = -\eta_{NI}(t)\alpha\pi I(t)N(t)/Q - \eta_{NR}(t)N(t) \\ \dot{I} = \eta_{NI}(t)\alpha\pi I(t)N(t)/Q - \eta_{IM}(t)I(t) - \eta_{IR}(t)I(t) \\ \dot{R} = \eta_{NR}(t)N(t) + \eta_{IR}(t)I(t) \\ \dot{M} = \eta_{IM}(t)I(t) \\ \forall t \in [t_0, T], \quad N(t) + I(t) + R(t) + M(t) = Q \\ N(t), I(t), R(t), M(t) \in \mathbb{N} \end{cases}$$

- ADDG Model（Attack-Defense Differential Game）:（N ; Θ ; B ; t ; x ; S ; f ; U）=（players；type space of players；action space；time；state variable；control strategy；state transition function；payoff function）

第三节：微分博弈应用示例 2

- ADDG Model:（N ; Θ ; B ; t ; x ; S ; f ; U）
- **N**：攻防博弈的参与人集。N_D为防御者，N_A为攻击者；
- **Θ**：攻击者和防御者类型空间，是各参与人的私有信息；
- **B**：攻防行动空间，不少于1个；$AS = (\delta_1, \delta_2, \cdots, \delta_g)$ $DS = (\beta_1, \beta_2, \cdots, \beta_k)$
- **t**：博弈时刻，$t \in [t_0, T]$，系统状态、双方的控制策略轨迹和博弈收益都是关于t的函数；
- **x**：$x(t) = \{N(t), I(t), R(t), M(t) | N(t) + I(t) + R(t) + M(t) = Q\}$是网络系统的状态变量

第三节：微分博弈应用示例 2

- ADDG Model:（N ; Θ ; B ; t ; x ; S ; f ; U）
- **S：t时刻的控制策略，$\boldsymbol{S=(D(t),A(t))}$**

$$D(t)=\left\{P_D(t)\middle|P_D(t)=\left(p_D^i(t)\right),1\le i\le n\right\},\sum_{i=1}^{n}p_D^i(t)=1$$

$$A(t)=\{P_A(t)|P_A(t)=\left(p_A^j(t)\right),1\le j\le m\},\sum_{j=1}^{m}p_A^j(t)=1$$

- **f：状态转移方程**

$$f_N=\frac{\mathrm{d}N(t)}{\mathrm{d}t}=\dot{N},f_I=\frac{\mathrm{d}I(t)}{\mathrm{d}t}=\dot{I},f_R=\frac{\mathrm{d}R(t)}{\mathrm{d}t}=\dot{R},f_M=\frac{\mathrm{d}M(t)}{\mathrm{d}t}=\dot{M}$$

第三节：微分博弈应用示例 2

- ADDG Model:（N ; Θ ; B ; t ; x ; S ; f ; U）
- **U：收益函数（U_D,U_A）。** $U = \int_{t_0}^{T} g(t, x(t), P_A(t), P_D(t))\, dt$

在网络系统中，当网络节点状态从正常状态N变为感染状态I时，回报系数r_1表示节点及其相邻节点受到感染时的危害。当节点从感染状态I或正常状态N转换到恢复状态R时，回报系数r_2表示恢复节点在免疫攻击后可以减少的期望损失。当节点从感染状态I转变为故障状态M时，回报系数r_3为节点服务功能受损造成的损失。

第三节：微分博弈应用示例 2

- 回报函数：

$$r_D(t) = r_2[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)]$$
$$- r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q] - r_3[\eta_{IM}(t)I(t)],$$
$$r_A(t) = r_1[\eta_{NI}(t)\alpha\pi I(t)N(t)/Q]$$
$$+ r_3[\eta_{IM}(t)I(t)] - r_2[\eta_{NR}(t)N(t) + \eta_{IR}(t)I(t)].$$

- 成本函数：C_A，C_D为成本系数

$$v_D = \frac{d^2}{2}c_D\,(N(t) + I(t) + R(t) + M(t)),$$
$$v_A = \frac{a^2}{2}c_A\,(N(t) + I(t) + R(t) + M(t)).$$

第三节：微分博弈应用示例 2

❖ 收益函数U

回报函数

$$U_D(P_A(t), P_D(t)) = \int_{t_0}^{T} r_2[\eta_{NR}N + \eta_{IR}I] - r_1[\eta_{NI}\alpha\pi IN/Q] - r_3[\eta_{IM}I] - \frac{c_D}{2}d^2(N+I+R+M)]\,\mathrm{d}t,$$

成本函数

回报函数

$$U_A(P_A(t), P_D(t)) = \int_{t_0}^{T} r_1[\eta_{NI}\alpha\pi IN/Q] - r_2[\eta_{NR}N + \eta_{IR}I] + r_3[\eta_{IM}I] - \frac{c_A}{2}a^2(N+I+R+M)]\,\mathrm{d}t.$$

成本函数

❖ 均衡策略 $(P_A^*(t), P_D^*(t))$ ，需满足

$$\begin{cases} \forall P_A(t),\ U_A(P_A(t)^*, P_D(t)^*) \geq U_A(P_A(t), P_D(t)^*) \\ \forall P_D(t),\ U_D(P_A(t)^*, P_D(t)^*) \geq U_D(P_A(t)^*, P_D(t)) \end{cases}$$

第三节：微分博弈应用示例 2

❖ 求解均衡策略

- 建立汉密尔顿函数 $H\left(t, K_i(t), x, P_A(t), P_D(t)\right)$

$$= f\left((t, x(t), P_A(t), P_D(t)\right) K_i(t) + g\left(t, x(t), P_A(t), P_D(t)\right), \quad i \in \{D, A\}$$

- 协态变量 $K_D^N(t), K_D^I(t), K_D^R(t), K_D^M(t)$， $K_A^N(t), K_A^I(t), K_A^R(t), K_A^M(t)$.

- 状态方程与协态方程

$$\frac{d}{dt}K_i(t) = -\frac{\partial}{\partial x^*}H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right)$$

$$\frac{d}{dt}x^*(t) = \frac{\partial}{\partial K_i(t)}H\left(t, K_i(t), x^*, P_A^*(t), P_D^*(t)\right)$$

第三节：微分博弈应用示例 2

❖ 求解均衡策略

- 在利用动态规划方法来计算攻击者和防御者的协态变量的基础上，可进一步求解鞍点策略。
- 动态规划问题如右式：（包含了汉密尔顿优化问题、协态方程、微分方程及其边界条件）

$$\forall P_A(t), P_D(t), \quad t \in [t_0, T], \ x \in \{N(t), I(t), R(t), M(t)\}$$

$$\times \begin{cases} H\left(t, K_D(t), x^*, P_A^*(t), P_D^*(t)\right) \geq H\left(t, K_D(t), x^*, P_A^*(t), P_D(t)\right) \\ H\left(t, K_A(t), x^*, P_A^*(t), P_D^*(t)\right) \geq H\left(t, K_A(t), x^*, P_A(t), P_D^*(t)\right) \end{cases} \text{优化问题}$$

$$\begin{cases} \frac{dK_D^N(t)}{dt} = \lambda_D^N, \quad \frac{dK_D^I(t)}{dt} = \lambda_D^I, \quad \frac{dK_D^R(t)}{dt} = \lambda_D^R, \quad \frac{dK_D^M(t)}{dt} = \lambda_D^M \\ \frac{dK_A^N(t)}{dt} = \lambda_A^N, \quad \frac{dK_A^I(t)}{dt} = \lambda_A^I, \quad \frac{dK_A^R(t)}{dt} = \lambda_A^R, \quad \frac{dK_A^M(t)}{dt} = \lambda_A^M \end{cases} \text{协态方程}$$

$$\begin{cases} \frac{dN^*(t)}{dt} = -\eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q - \eta_{NR}(t)N^*(t) \\ \frac{dI^*(t)}{dt} = \eta_{NI}^*(t)\alpha\pi I^*(t)N^*(t)/Q - I^*(t)\left(\eta_{IM}^*(t) + \eta_{IR}^*(t)\right) \\ \frac{dR^*(t)}{dt} = \eta_{NR}^*(t)N^*(t) + \eta_{IR}^*(t)I^*(t), \quad \frac{dM^*(t)}{dt} = \eta_{IM}^*(t)I^*(t) \end{cases} \text{微分方程}$$

$$\begin{cases} N^*(t_0) = N(t_0), \quad I^*(t_0) = I(t_0), \\ R^*(t_0) = R(t_0), \quad M^*(t_0) = M(t_0) \end{cases} \text{微分方程边界条件}$$

第三节：微分博弈应用示例 2

- 求解均衡策略（分 $\eta(t)>0$ 和 $\eta(t)\leq 0$ 两种情况）
  - 通过令 $\frac{\partial H^*}{\partial p_D^H(t)} = 0$ 及 $p_D^L(t)^* = 1 - p_D^H(t)^*$
  - 可得到 $p_D^*(t) = (p_D^{H*}(t), p_D^{L*}(t))$
  - 通过令 $\frac{\partial H^*}{\partial p_A^H(t)} = 0,\ \frac{\partial H^*}{\partial p_A^M(t)} = 0$ 及 $p_A^L(t)^* = 1 - p_A^H(t)^* - p_A^M(t)^*$
  - 可得到 $p_A^*(t) = (p_A^{H*}(t), p_A^{M*}(t), p_A^{L*}(t))$
- 其中，$\eta(t) \leq 0$代表攻击失败，$\eta(t) > 0$表示攻击成功。$\eta(t)$的正负不同，求解出的策略也不同，表明攻防最优策略是相互影响的。

第三节：微分博弈应用示例 2

- 攻击行为、类型及强度（参考MIT行为攻防数据库及其他文献）

攻击行为分为三种强度类型：高、中、低，每种类型列举了三种示例的攻击手段，每种手段有其对应的强度值，取该类型里三个示例手段的平均强度值作为该攻击类型的平均强度值。

No.	Attack aciton	Attack strength	Attack type	Average strength
1	Remote buffer overflow	0.95	A_H	0.82
2	Install Trojan	0.8		
3	Steal account and crack it	0.7		
4	Send abnormal data to GIOP	0.5	A_M	0.45
5	LPC to LSASS process	0.4		
6	Shutdown Database server	0.45		
7	Oracle TNS Listener	0.35	A_L	0.3
8	Ftp rhost attack	0.3		
9	Sr-Hard blood	0.25		

第三节：微分博弈应用示例 2

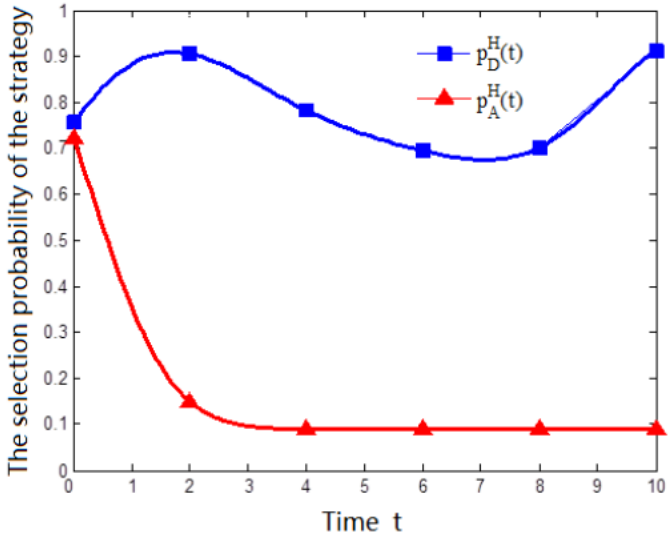
❖ 防御行为、类型及强度

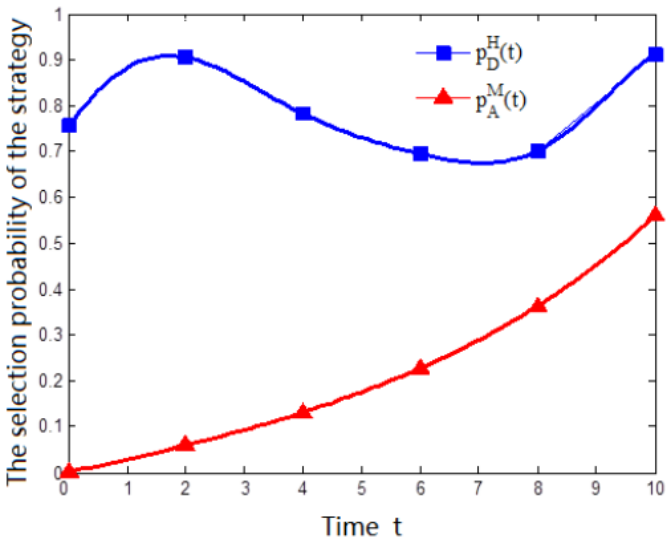
防御行为分为两种强度类型：高、低，每种类型列举了七种示例的防御手段，每种手段有其对应的强度值，取该类型里七个示例手段的平均强度值作为该防御类型的平均强度值。

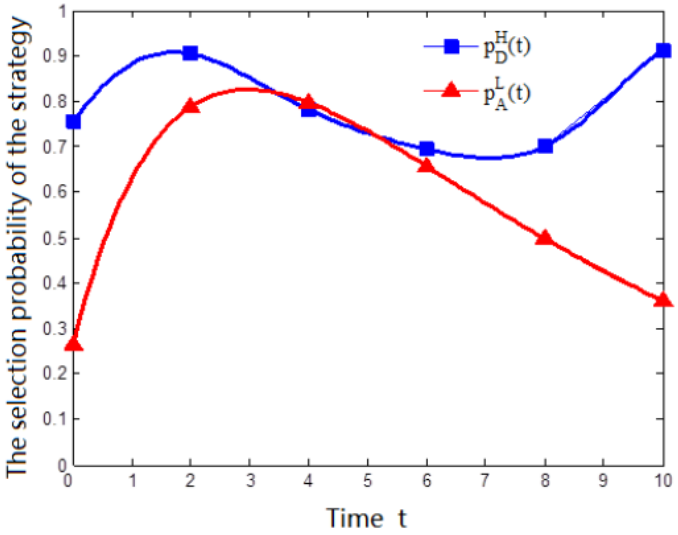
No.	Defense action	Defense strength	Defense type	Average strength
1	Limit packets from ports	0.8		
2	Install Oracle patches	0.8		
3	Reinstall Listener program	0.8		
4	Uninstall delete Trojan	0.7	D_H	0.71
5	Limit access to MDSYS.SDO_CS	0.7		
6	Renew root data	0.6		
7	Restart Database server	0.6		
8	Limit SYN/ICMP packets	0.5		
9	Add physical resource	0.5		
10	Repair database	0.4		
11	Correct homepage	0.4	D_L	0.34
12	Delete suspicious account	0.3		
13	Redeploy firewall rule and filtrate malicious packets	0.3		
14	Patch SSH on Ftp Sever	0.2		

第三节：微分博弈应用示例 2

- 攻防最优策略演化轨迹





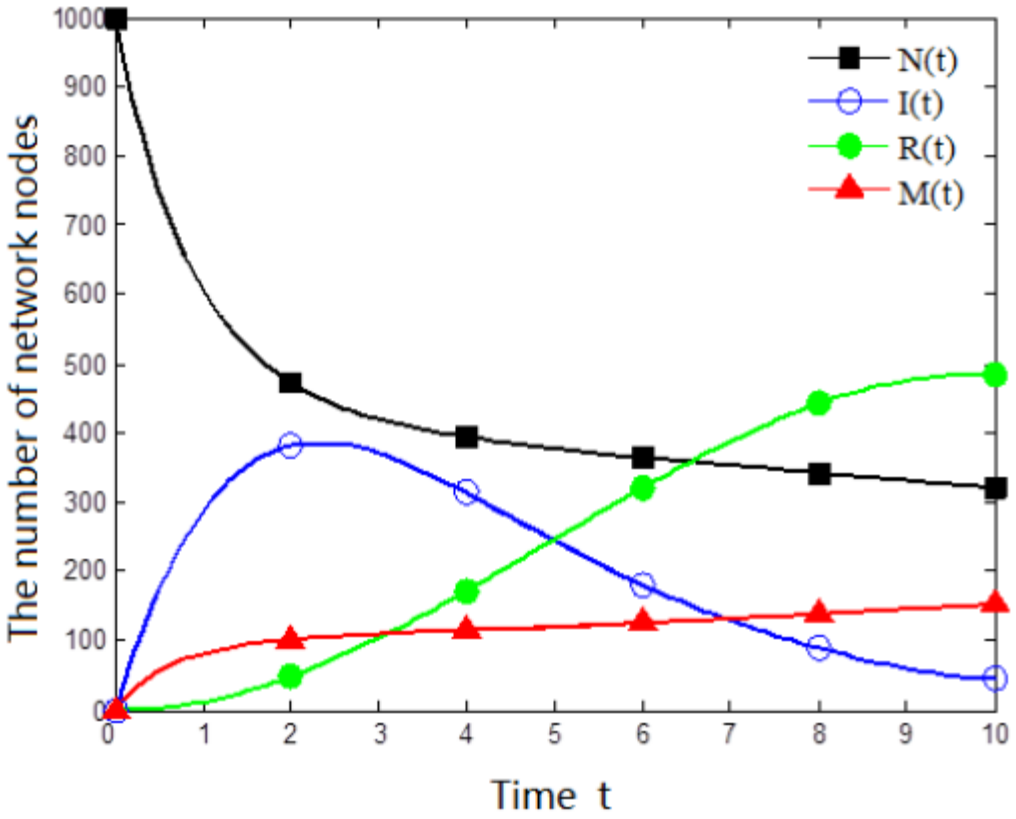


演化规律：攻击者一开始以较高的概率采取高强度攻击，在短时间内实施闪电战，尽量扩大感染节点的数量；之后考虑高强度攻击的实施成本较高，攻击强度逐渐减小。防御者一开始选择高强度防御来面对突然爆发的攻击，但是考虑到成本，之后概率有所降低但仍然保持在较高的水平。

第三节：微分博弈应用示例 2

❖ 网络节点状态演化

受感染节点在[0,2]迅速增加，瘫痪节点的数量增幅也较大，正常节点短时间内减少了一半。[2,3]防御策略有效抵挡了攻击，感染节点数量有所下降。之后，强攻击策略的概率维持在较低水平，强防御策略保持较高概率，所以绿色的修复节点数量显著增加，损坏节点增长缓慢。



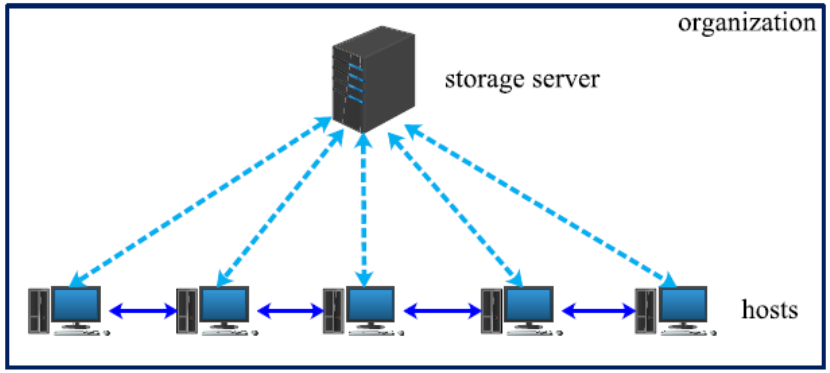
第四节：微分博弈应用示例 3

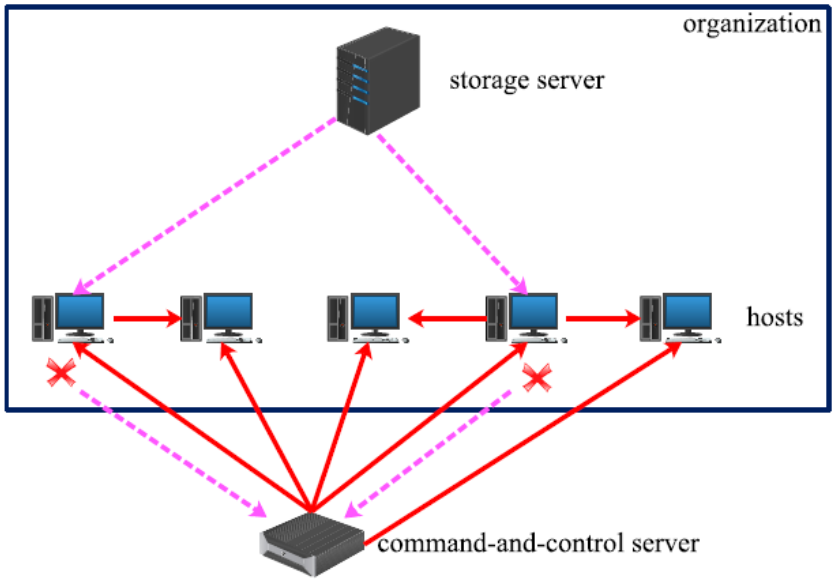
- 近年来，许多知名组织（如大型企业、金融机构、政府部门）都经历了一种新型的网络攻击——**Advanced Persistent Threat.**
- **Advanced Persistent Threat（APT）特点：**
  - 攻击者通常是资源丰富、组织良好的实体，其目的是从目标组织窃取敏感数据，而保持长期的隐蔽性。
  - 通过侦查及运用复杂的社会工程技术，APT可以避免传统的网络防御措施渗透到组织中，从而造成严重的数据泄露。

L. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou, “Effective repair strategy against advanced persistent threat: A differential game approach,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1713–1728, Jul. 2019.

第四节：微分博弈应用示例 3

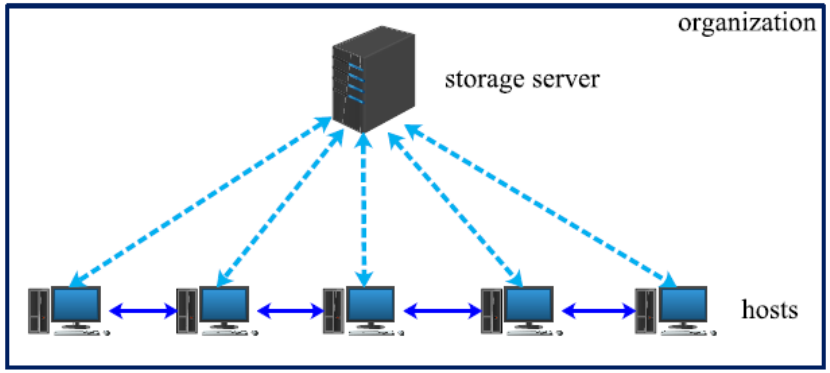
- 组织结构及APT攻击
- APT目标：存储服务器及各主机内的敏感数据
- APT攻击过程：攻击者收集和分析有关组织及人员的多维数据来寻找漏洞。基于此，对易受攻击的部分进行社会工程攻击，在其主机上隐秘安装后门。

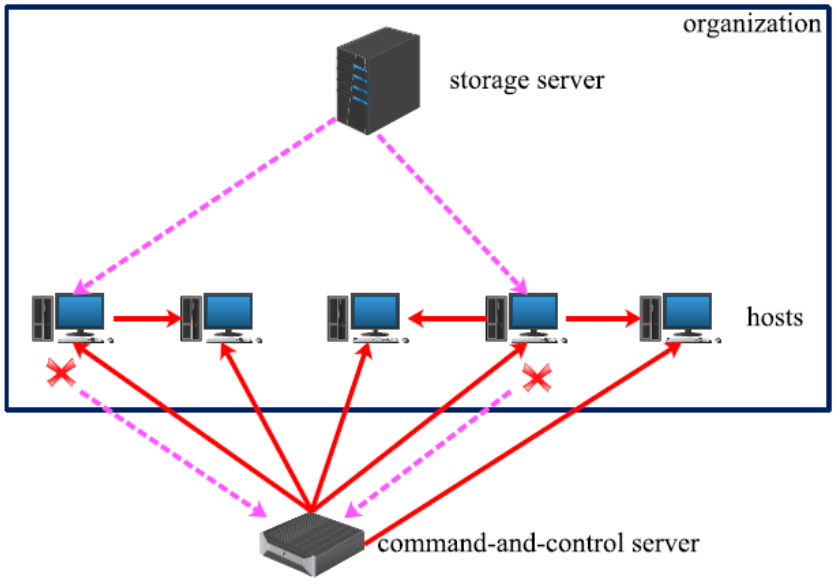




第四节：微分博弈应用示例 3

- 若成功，将在每个被攻击的主机和攻击者主机（命令控制服务器）之间建立秘密连接。因此，攻击者可以利用被攻击的主机来：①获得对存储服务器的部分访问权限；②通过横向移动（**lateral movement**）来渗透到其他安全的主机中以获得更多的敏感数据。





第四节：微分博弈应用示例 3

❖ APT检测

首先，为了减轻组织的APT风险，需要用APT检测技术来检测APT攻击是否存在。由于其统计特性，APT检测技术可相对精确地估计各主机不安全的概率，而无法做到完全精准地识别所有不安全的主机。

❖ APT修复

在检测的基础上，需及时查明和修复被攻击的主机来减轻组织的潜在损失。这项工作的耗时之处在于：

第四节：微分博弈应用示例 3

- 通过调用任务/进程管理器和注册表编辑器等进程，在可能不安全的主机中搜索可疑进程和文件。
- 检查来自潜在不安全主机的出站流量的目标主机，包括其IP地址、物理位置、端口、通信协议，以确定所有被攻击主机。
- 终止可疑进程，清除可疑文件，并删除所有被攻击主机的可疑注册记录。关机并重启。
- 如有必要，更改证书甚至在部分或所有被攻击主机中重新安装系统。

第四节：微分博弈应用示例 3

- 由于APT检测占用大量人力资源，且组织的安全预算及人力资源都是有限的
- 所以需要合理地为潜在不安全主机分配可用的修复资源，即本文所研究的问题：如何选择修复策略来为不安全主机合理分配修复资源，从而减轻组织的损失。
- 各主机的安全状态及攻击/修复策略都随着时间动态变化，所以可用微分博弈来刻画这种连续变化的过程。

第四节：微分博弈应用示例 3

- 系统包含一个存储服务器和N个主机。
- 各主机的情况及主机间关系：
  - 主机i和j之间是否可以通信

$$a_{ij}=\begin{cases}1, \text{主机}i\text{和}j\text{之间可以通信}\\ 0, \text{主机}i\text{和}j\text{之间不可通信}\end{cases}$$

  - 主机i是否开机

$$b_i=\begin{cases}1, \text{主机}i\text{开机}\\ 0, \text{主机}i\text{关机}\end{cases}$$

第四节：微分博弈应用示例 3

- 主机i和j之间是否成功通信

$$c_{ij} = a_{ij} b_i b_j \begin{cases} 1, \text{主机} i \text{和} j \text{之间通信成功} \\ 0, \text{主机} i \text{和} j \text{之间通信失败} \end{cases}$$

- 主机i是否安全

$$X_i = \begin{cases} 1, \text{主机} i \text{不安全} \\ 0, \text{主机} i \text{安全} \end{cases}$$

- 主机i的不安全概率 $I_i(t) = \Pr\{X_i(t) = 1\}$

❖ 各主机是否安全是不可确定的，但各主机的不安全概率是可预测的。因此，假设主机i的$X_i(t)$未知而$I_i(t)$已知。

第四节：微分博弈应用示例 3

- 攻击策略：$$\mathbf{x}(t) = (\alpha_1(t), \cdots, \alpha_N(t), \beta_{11}(t), \cdots, \beta_{1N}(t), \cdots, \beta_{N1}(t), \cdots, \beta_{NN}(t)), \quad 0 \le t \le T.$$
- $\alpha_i(t)$：主机i被直接攻击的速率，使得$X_i(t)$增加。其上界为 $\overline{\alpha_i}$。

  $\alpha_i(t) = 0$的情况：主机i关机、主机i原本处于不安全状态。

$$b_i(t) = 0 \text{ or } X_i(t) = 1$$

- $\beta_{ji}(t)$：从主机j向主机i进行横向移动的速率，使得 $X_i(t)$ 增加。

  其上界为 $\overline{\beta_{ji}}$。$\beta_{ji}(t) = 0$的情况：主机i和主机j通信失败、主机i原本处于不安全状态、主机j原本处于安全状态。

$$c_{ij}(t) = 0 \text{ or } X_i(t) = 1 \text{ or } X_j(t) = 0$$

第四节：微分博弈应用示例 3

- 修复策略：$\mathbf{y}(t) = (\gamma_1(t), \cdots, \gamma_N(t)), \quad 0 \le t \le T.$
- $\gamma_i(t)$：主机i被修复为安全的速率，使得$X_i(t)$降低。其上界为$\bar{\gamma}_i$。$\gamma_i(t) = 0$的情况：主机i关机、主机i原本处于安全状态。

$$b_i(t) = 0 \text{ or } X_i(t) = 0$$

- 定义主机i安全，主机j不安全的概率满足

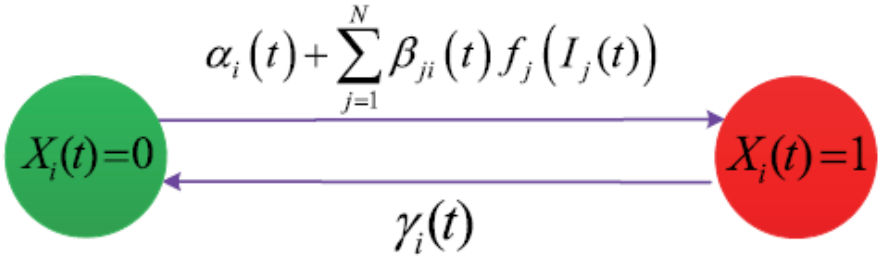
$$\Pr\{X_i(t) = 0, X_j(t) = 1\} \le [1 - I_i(t)]I_j(t)$$

- 则有假设（$\mathbf{H_1}$）：

$$\Pr\{X_i(t) = 0, X_j(t) = 1\} = [1 - I_i(t)]f_j(I_j(t)), \quad 0 \le t \le T,$$

第四节：微分博弈应用示例 3

- 其中，函数f_j严格递增，可微。



且满足

$$f_j(0) = 0, \text{ and } f_j(x) \leq x \text{ for } x \geq 0$$

- 定义组织的期望状态，$\mathbf{I}(t) = (I_1(t), I_2(t), \cdots, I_N(t))$
- 该状态将随着攻击和修复策略而演化，可得到演化的微分方程：

$$\frac{dI_i(t)}{dt} = \left[\alpha_i(t) + \sum_{j=1}^{N}\beta_{ji}(t)f_j(I_j(t))\right][1 - I_i(t)] - \gamma_i(t)I_i(t), \quad 0 \leq t \leq T, \quad 1 \leq i \leq N, \tag{1}$$

$$\mathbf{I}(0) = \mathbf{I}_0$$

第四节：微分博弈应用示例 3

- 定义攻击者的期望收益（最大化）：由于主机不安全而数据泄露的收益-直接攻击的成本-横向移动的成本

$$J_A(\mathbf{x},\mathbf{y}) = C_B(\mathbf{x},\mathbf{y}) - C_D(\mathbf{x},\mathbf{y}) - C_M(\mathbf{x},\mathbf{y})$$

$$= w_1 \int_0^T \sum_{i=1}^{N} b_i(t) I_i(t) dt$$

$$- \int_0^T \sum_{i=1}^{N} \phi_i(\alpha_i(t))[1 - I_i(t)]dt$$

$$- \int_0^T \sum_{i,j=1}^{N} \varphi_{ji}(\beta_{ji}(t))[1 - I_i(t)] f_j(I_j(t))dt$$

数据泄露收益：主机i不安全的概率，且需在开机状态下。

直接攻击的成本：直接攻击的成本函数*主机i安全的概率

横向移动的成本：横向移动的成本函数*主机i安全而主机j不安全的概率

- 其中，ω_1为单位时间的攻击平均收益，$\phi_i(\alpha)$为直接攻击主机i的平均单位成本，$\phi_i(0) = 0$，为增函数，$\varphi_{ji}(\beta)$为通过主机j横向移动来攻击主机i的平均单位成本，$\varphi_{ji}(0) = 0$，为增函数。

第四节：微分博弈应用示例 3

- 定义组织的期望总损失（最小化）：由于主机不安全而数据泄露的损失+修复的成本

$$J_R(\mathbf{x},\mathbf{y}) = C_L(\mathbf{x},\mathbf{y}) + C_R(\mathbf{x},\mathbf{y})$$

$$= w_2 \int_0^T \sum_{i=1}^{N} b_i(t) I_i(t) dt$$

$$+ \int_0^T \sum_{i=1}^{N} \psi_i(\gamma_i(t)) I_i(t) dt$$

数据泄露损失：主机i不安全的概率，且需在开机状态下。

修复成本：修复的成本函数*主机i不安全的概率

- 其中，ω_2为单位时间的组织平均损失，$\psi_i(\gamma)$为修复不安全主机i的平均单位成本，$\psi_i(0) = 0$，增函数。

第四节：微分博弈应用示例 3

- 求解最优策略
- 首先，定义汉密尔顿函数
- 其中，λ和μ分别为攻击者和组织的协态变量

$$H_A(\mathbf{I},\mathbf{x},\mathbf{y},\lambda) = w_1\sum_{i=1}^{N} b_i I_i - \sum_{i=1}^{N}\phi_i(\alpha_i)(1-I_i) - \sum_{i,j=1}^{N}\varphi_{ji}(\beta_{ji})(1-I_i)f_j(I_j) + \sum_{i=1}^{N}\lambda_i\left\{\left[\alpha_i+\sum_{j=1}^{N}\beta_{ji}f_j(I_j)\right](1-I_i)-\gamma_i I_i\right\}$$

攻击者收益

状态方程

$$H_R(\mathbf{I},\mathbf{x},\mathbf{y},\mu) = w_2\sum_{i=1}^{N} b_i I_i + \sum_{i=1}^{N}\psi_i(\gamma_i)I_i + \sum_{i=1}^{N}\mu_i\left\{\left[\alpha_i+\sum_{j=1}^{N}\beta_{ji}f_j(I_j)\right](1-I_i)-\gamma_i I_i\right\}$$

组织的损失

第四节：微分博弈应用示例 3

❖ 协态方程

$$
\begin{cases}
\dfrac{d\lambda_i(t)}{dt} = -w_1 b_i(t) - \phi_i(\alpha_i(t)) - \displaystyle\sum_{j=1}^{N} \varphi_{ji}(\beta_{ji}(t)) f_j(I_j(t)) + \sum_{j=1}^{N} \left[\varphi_{ij}(\beta_{ij}(t)) - \beta_{ij}(t)\lambda_j(t)\right]\left[1 - I_j(t)\right] f_i'(I_i(t)) \\
\qquad\qquad + \lambda_i(t)\left[\alpha_i(t) + \gamma_i(t) + \displaystyle\sum_{j=1}^{N} \beta_{ji}(t) f_j(I_j(t))\right], \\
\dfrac{d\mu_i(t)}{dt} = -w_2 b_i(t) - \psi_i(\gamma_i(t)) - \displaystyle\sum_{j=1}^{N} \beta_{ij}(t)\mu_j(t)\left[1 - I_j(t)\right] f_i'(I_i(t)) + \mu_i(t)\left[\alpha_i(t) + \gamma_i(t) + \displaystyle\sum_{j=1}^{N} \beta_{ji}(t) f_j(I_j(t))\right] \\
\qquad 0 \le t \le T, \quad 1 \le i \le N.
\end{cases} \tag{2}
$$

❖ 优化问题（由原优化问题消除无关常数项后简化而来）

$$\alpha_i(t) \in \arg\max_{\alpha} \left[\lambda_i(t)\alpha - \phi_i(\alpha)\right], \tag{3}$$

$$\beta_{ji}(t) \in \arg\max_{\beta} \left[\lambda_i(t)\beta - \varphi_{ji}(\beta)\right], \tag{4}$$

$$\gamma_i(t) \in \arg\min_{\gamma} \left[\psi_i(\gamma) - \mu_i(t)\gamma\right], \tag{5}$$

第四节：微分博弈应用示例 3

❖ **Nash Equilibrium（NE）：** $(\mathbf{x}^*, \mathbf{y}^*) \in \mathscr{U}_A \times \mathscr{U}_R$

$$J_A(\mathbf{x}^*, \mathbf{y}^*) \geq J_A(\mathbf{x}, \mathbf{y}^*), \quad \forall \mathbf{x} \in \mathscr{U}_A,$$

$$J_R(\mathbf{x}^*, \mathbf{y}^*) \leq J_R(\mathbf{x}^*, \mathbf{y}), \quad \forall \mathbf{y} \in \mathscr{U}_R.$$

❖ **Potential Nash Equilibrium（PNE）：** $(\mathbf{x}_P, \mathbf{y}_P)$

$$\begin{aligned}\mathbf{x}_P(t) = (&\alpha_1^P(t), \cdots, \alpha_N^P(t), \beta_{11}^P(t), \cdots, \beta_{1N}^P(t), \\ &\cdots, \beta_{N1}^P(t), \cdots, \beta_{NN}^P(t)), \quad 0 \leq t \leq T.\end{aligned}$$

$$\mathbf{y}_P(t) = \left(\gamma_1^P(t), \cdots, \gamma_N^P(t)\right), \quad 0 \leq t \leq T.$$

(1)-(5)组成APT修复博弈的potential system，联立可求解出均衡策略。将此系统的攻击和修复策略称作APT修复博弈的PNE，PNE可能是NE。

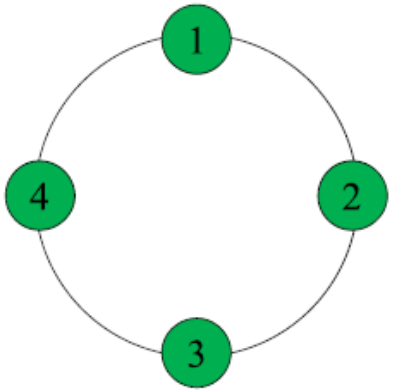
第四节：微分博弈应用示例 3

- **算法求解PNE的迭代过程：前向反向扫描法（forward—backward sweep method），在每次迭代中**
  - 基于（1）前向计算一个新的期望状态函数；
  - 基于（2）反向计算一个新的协态函数；
  - 最后基于（3）-（5）计算一个新的策略对；
- **当两个连续的策略对差距足够小或迭代次数足够大时，算法结束。**

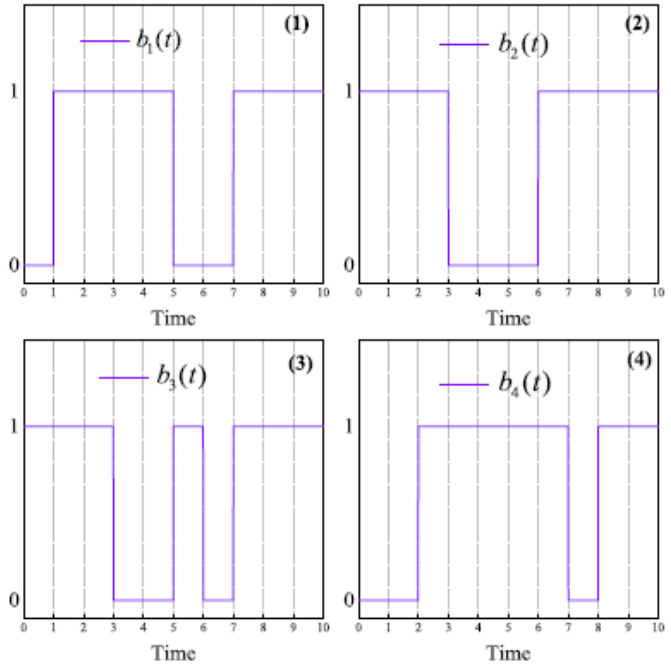
第四节：微分博弈应用示例 3

❖ 仿真

① **A toy example：图示为网络结构及节点开关机状态（schedule function）**



(a)



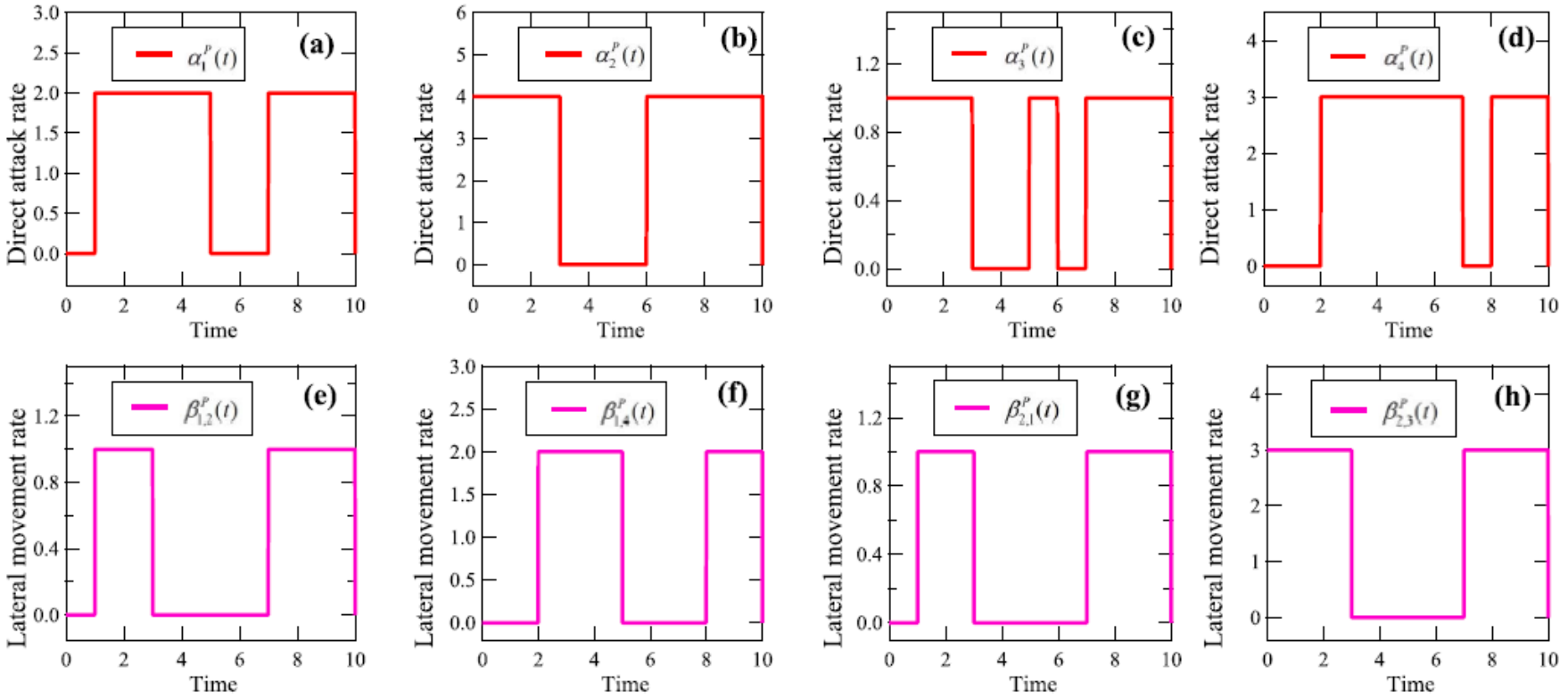
(b)

- 网络的拓扑结构如图(a)所示，节点i和j之间有连线表示$a_{ij}=1$，否则$a_{ij}=0$。
- 各网络节点在不同时刻的开关机状态如图(b)所示，$b_i=1$表示开机，$b_i=0$表示关机。

第四节：微分博弈应用示例 3

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

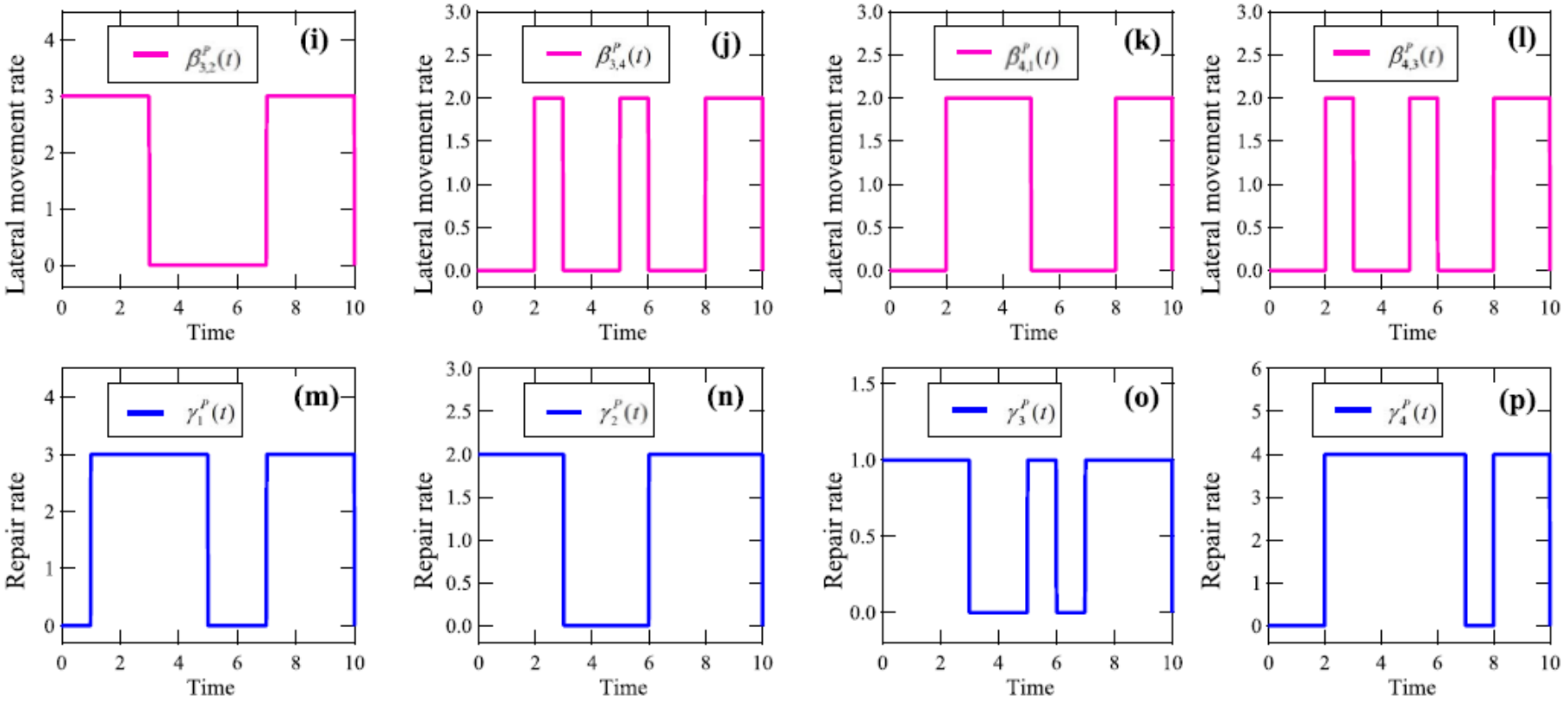
① A toy example的策略演化过程（直接攻击及横向移动速率）



第四节：微分博弈应用示例 3

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

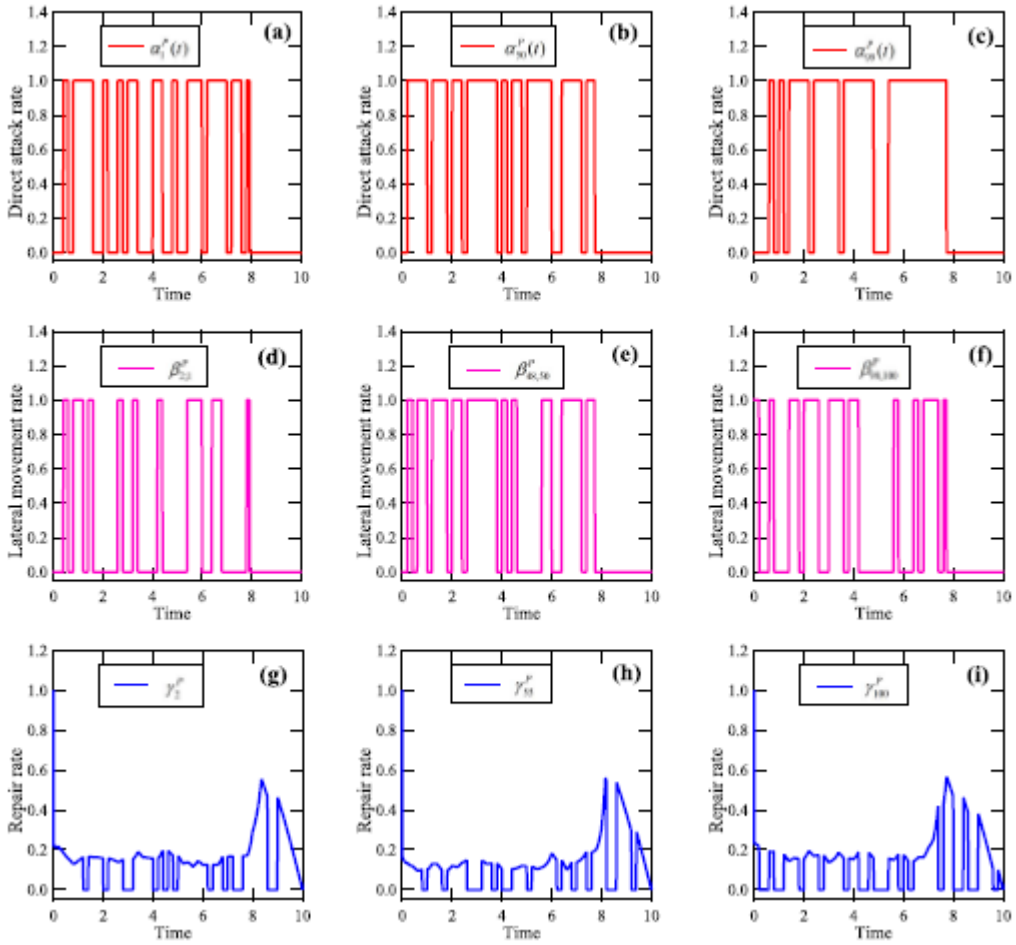
① A toy example的策略演化过程（横向移动及修复速率）

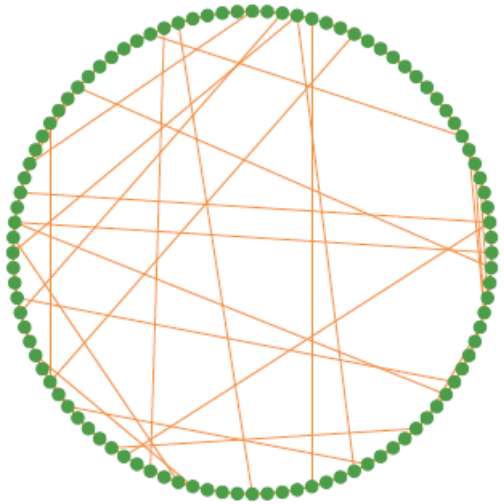


均为bang-bang控制策略

第四节：微分博弈应用示例 3

② 小世界网络（small world）的策略演化过程



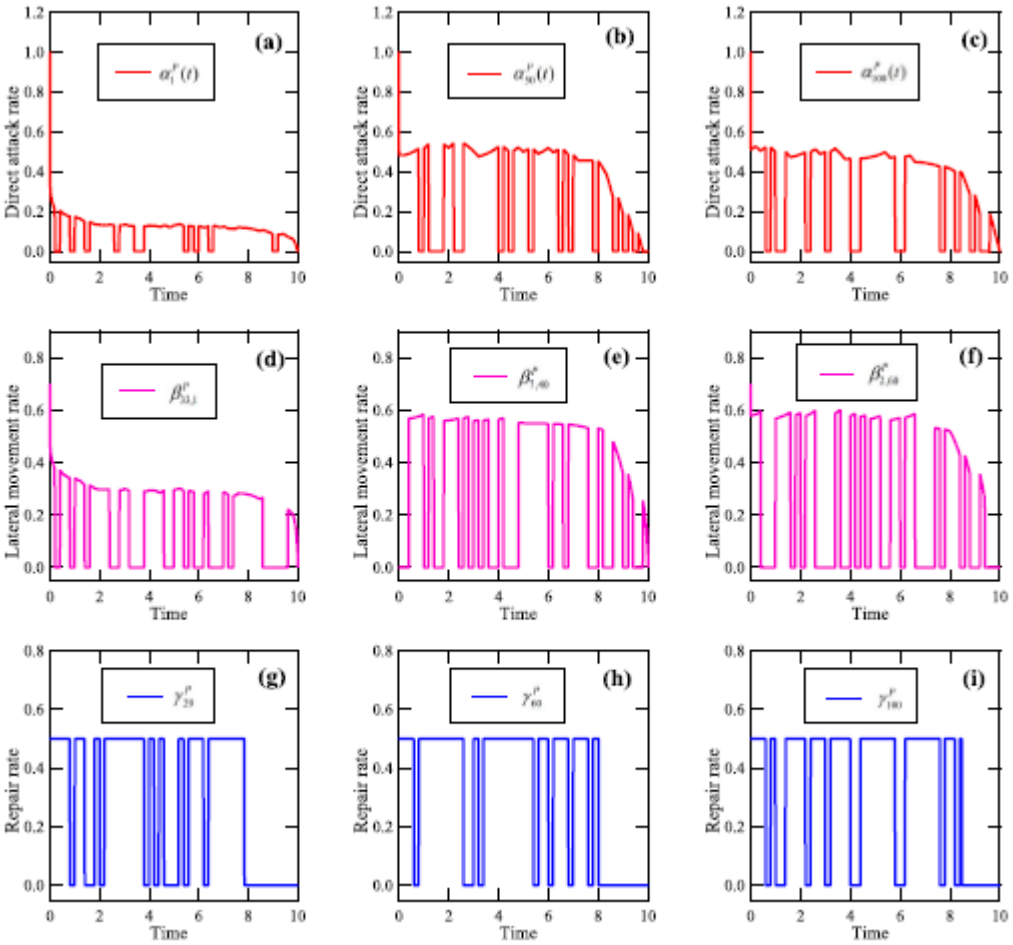


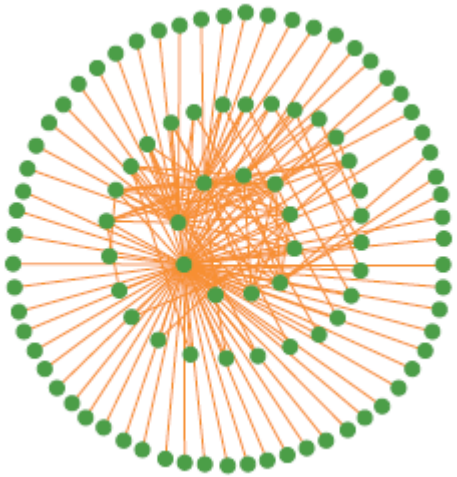
分为bang-bang策略

及piecewise策略

第四节：微分博弈应用示例 3

③ 无标度网络（scale—free）的策略演化过程





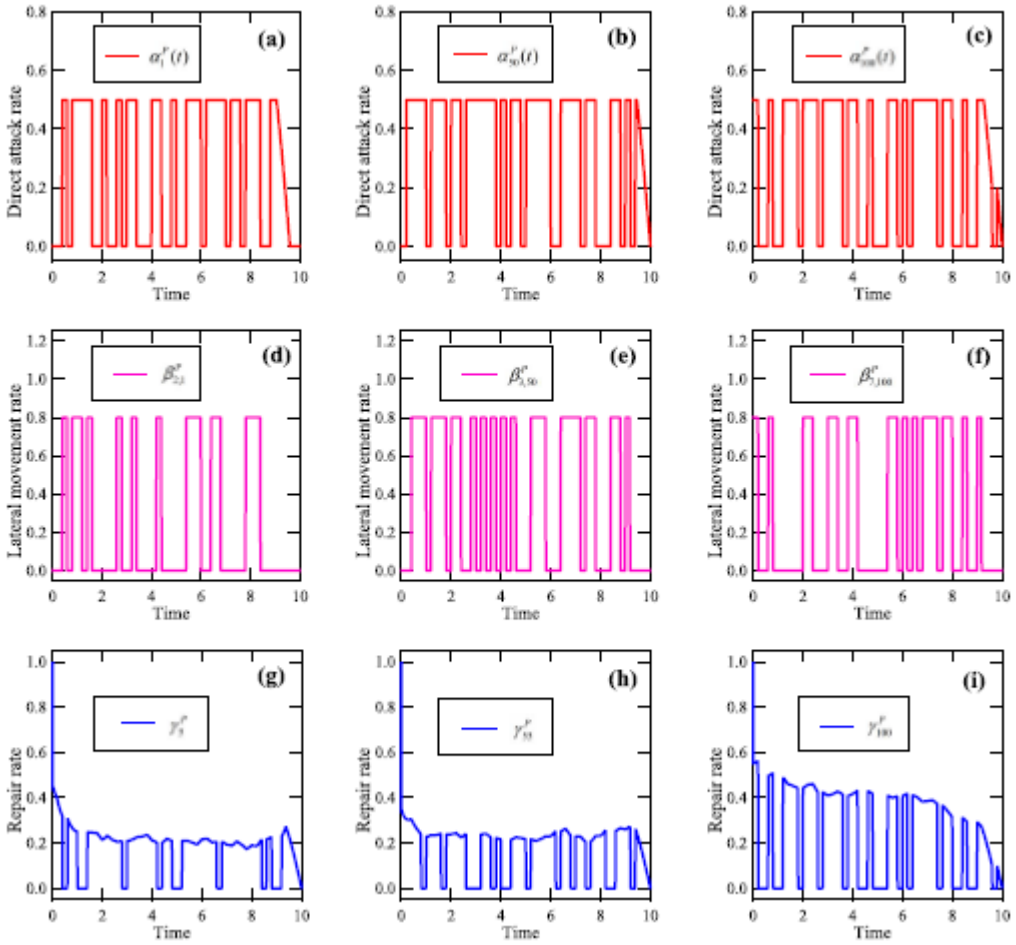
分为bang-bang策略

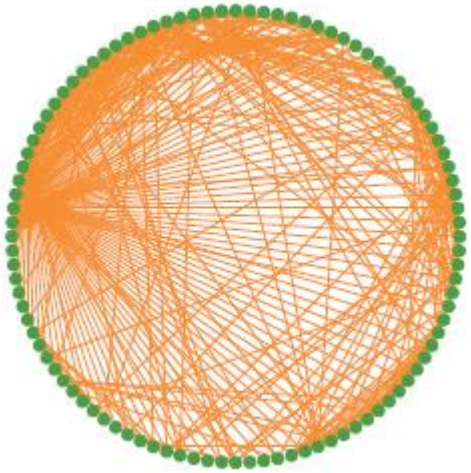
及piecewise策略

第四节：微分博弈应用示例 3

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

④ 真实世界（real—world）的策略演化过程



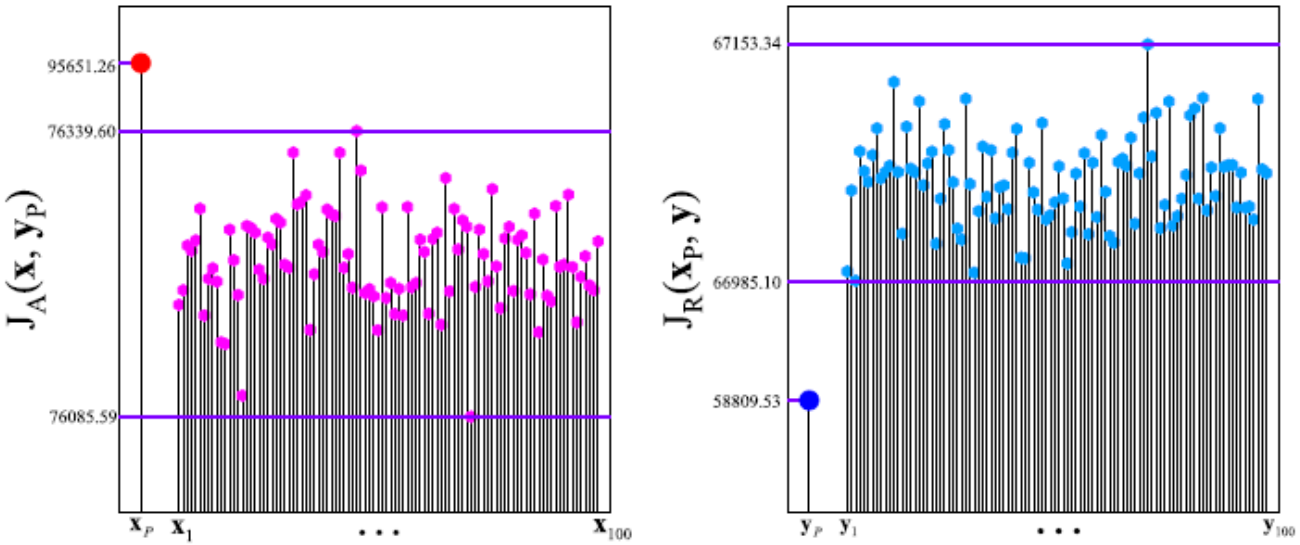


分为bang-bang策略

及piecewise策略

第四节：微分博弈应用示例 3

- PNE与随机策略的收益对比（以real-world为例）
- 修复策略固定为PNE策略，探究攻击策略。PNE攻击策略可提高攻击者收益。攻击策略固定为PNE策略，探究修复策略。PNE修复策略可降低组织的损失。

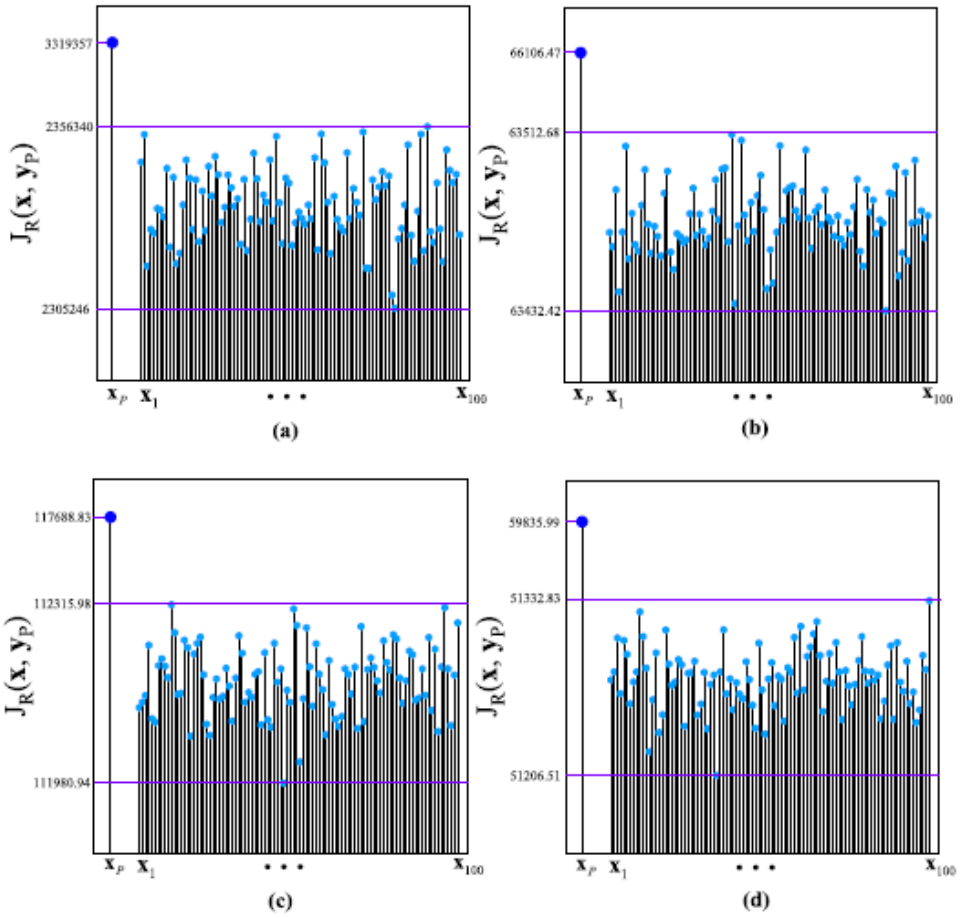


第四节：微分博弈应用示例 3

- PNE与随机策略的收益对比

  （图a,b,c,d分别toy example, 小世界，无标度，真实世界）

- 修复策略固定为PNE策略，探究攻击策略。PNE攻击策略可提高组织的损失。



本章小结

- 本章给出了微分博弈及最优控制论的基本定义，介绍了通过建立汉密尔顿方程、状态方程、协态方程，求解微分方程，来得到最优策略的基本思想。
- 通过网络安全实例（宏观攻防对抗中的最优策略选择及APT修复问题）分析了微分博弈的基本内涵和主要思想，并通过仿真直观展示了微分博弈对网络攻防建模的效果，即攻防策略的动态演化过程。