网络空间安全中的理论工具

清华大学

本章的内容组织

第一节
新的开始

- 畅想一个未来事件，提出五个亟待解决的实际问题

第二节
图论

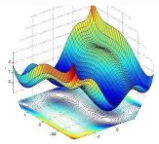
- 图论的基础知识
- 回答开辟根据地的问题

第三节
控制论

- 控制论的基础知识
- 回答获取策略集的问题

第四节
博弈论

- 博弈论的基础知识
- 回答策略选择的问题



第五节
最优化理论

- 最优化理论的基础知识
- 回答资源规划的问题

第六节
概率论与随机过程

- 概率论的基础知识
- 回答战略判断的问题

第1节 新的开始

- 如何开辟根据地?
- 如何设定策略集?
- 如何与敌人进行周旋?
- 如何充分利用我们的资源?
- 在什么地方拦截?

面临的问题

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

如何充分利用我们的资源？

在什么地方进行拦截，能够极大地缓解病毒的蔓延？

网络攻防的不对称性

已知的未知属于风险，风险可以用概率来表述，而未知的未知属于不确定性。

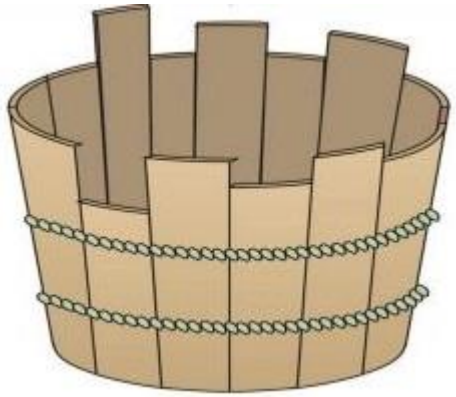
——弗兰克·奈特

只有千日做贼，哪有千日防贼。

——清•《中国现在记》

- 硬件、软件都是一些复杂系统的集成，在理论和实践上是难以避免存在漏洞的
- 在经济全球化的大趋势下，后门的存在也是不可杜绝的
- 从网络防御者的角度，基于未知漏洞和后门的未知攻击，是未知的安全威胁，我们不知道从何处下手才能够实施有效的、有针对性的防御

网络安全的木桶原理



一只水桶能装多少水取决于它最短的那块木板。

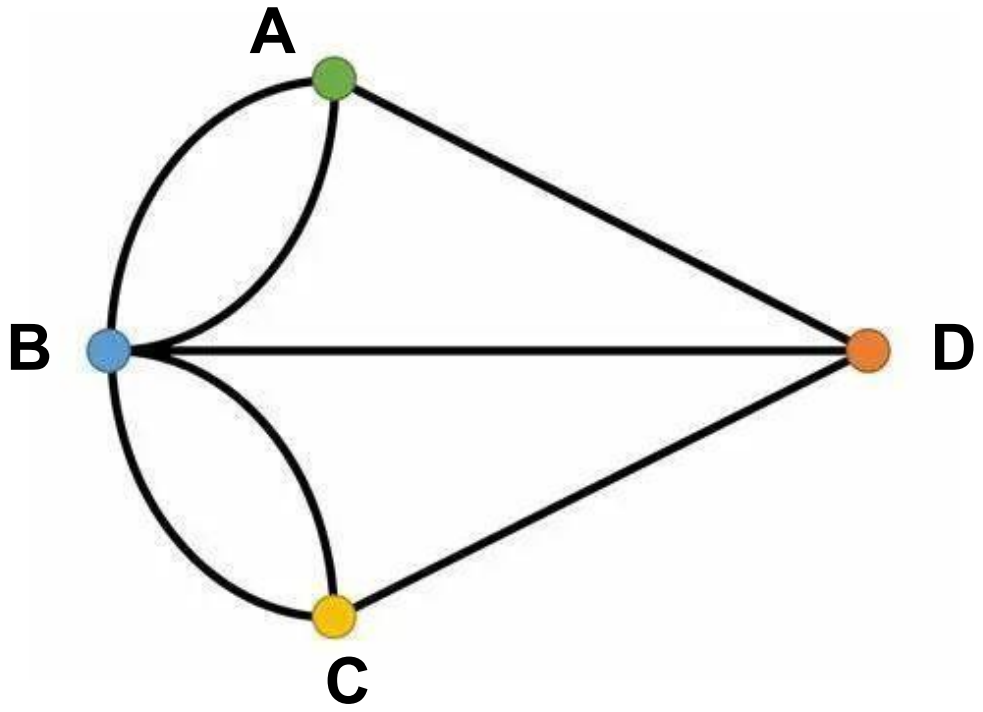
——劳伦斯·彼得

- 你的系统有10个漏洞，黑客总是寻找最容易攻破的漏洞，这就是所谓的“安全木桶”上的**短板，最弱的一环**
- 无论你其他安全措施多么强大，黑客只要找到**一块短板**就行了

第2节 图论

- 起源
- 着色问题
- 网络结构与网络行为

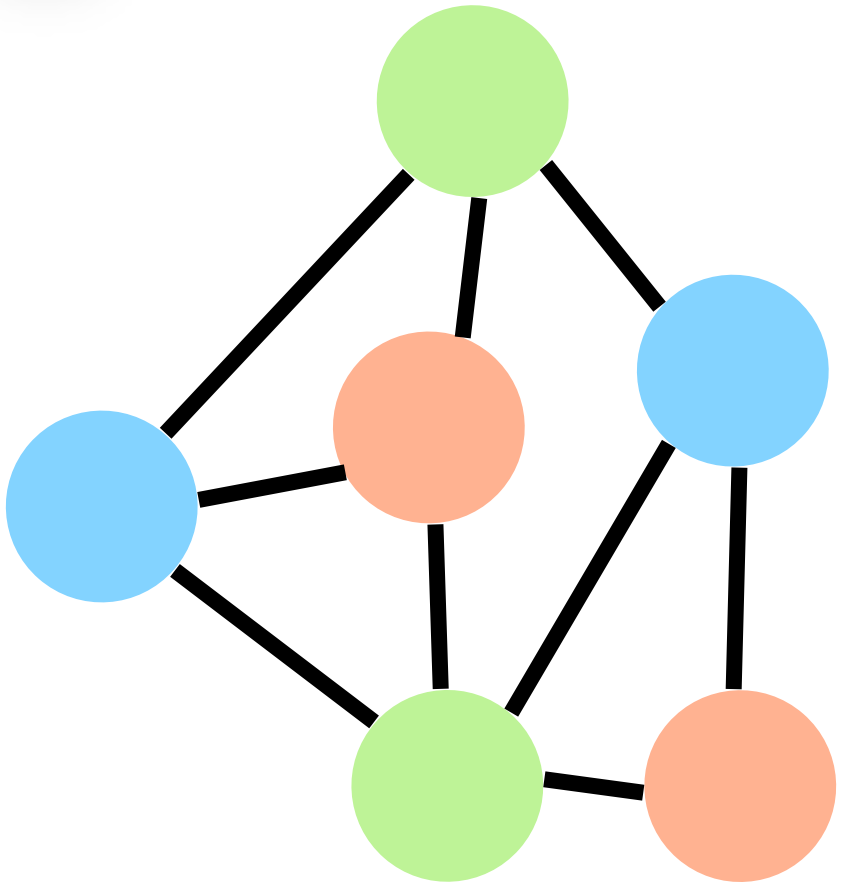
哥尼斯堡七桥问题



1736年，欧拉发表首篇关于图论的文章《关于位置几何问题的解法 》（ *Solutio Problematis ad geometriam situs pertinentis* ），研究了哥尼斯堡七桥问题，他也被称为图论之父

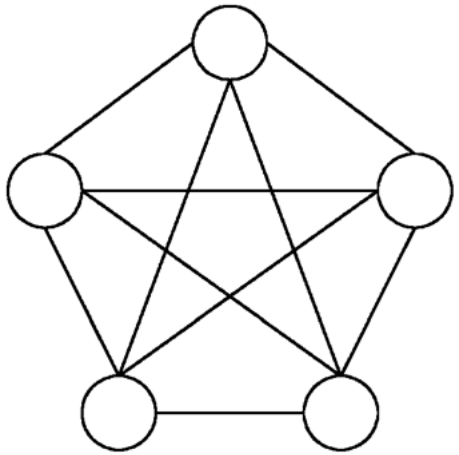
Google Scholar 1612

图的定义



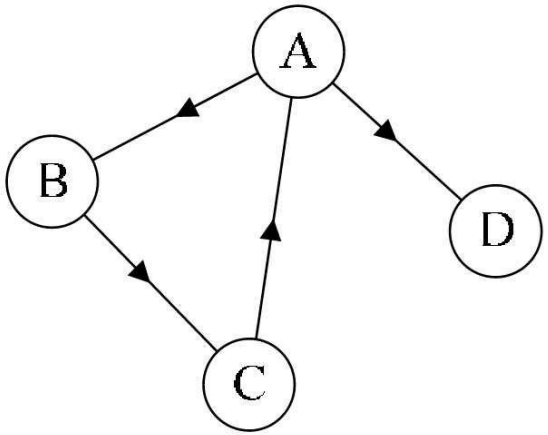
- 图论中所研究的图，并不是几何学中的图形，而是客观世界中某些事物联系的一个**数学抽象**
- 如左图所示，一般用顶点代表事物，用边表示事物间的关系
- 这种由顶点及边所组成的图就是图论中所研究的图，一般用**G**表示

两个重要定理



- 定理1：

设图G中有E条边，V个顶点，则G中所有顶点的度数之和为边数的两倍，即 $\sum D(V) = 2 * E$



- 定理2：

图G中度为奇数的顶点个数恰有偶数个

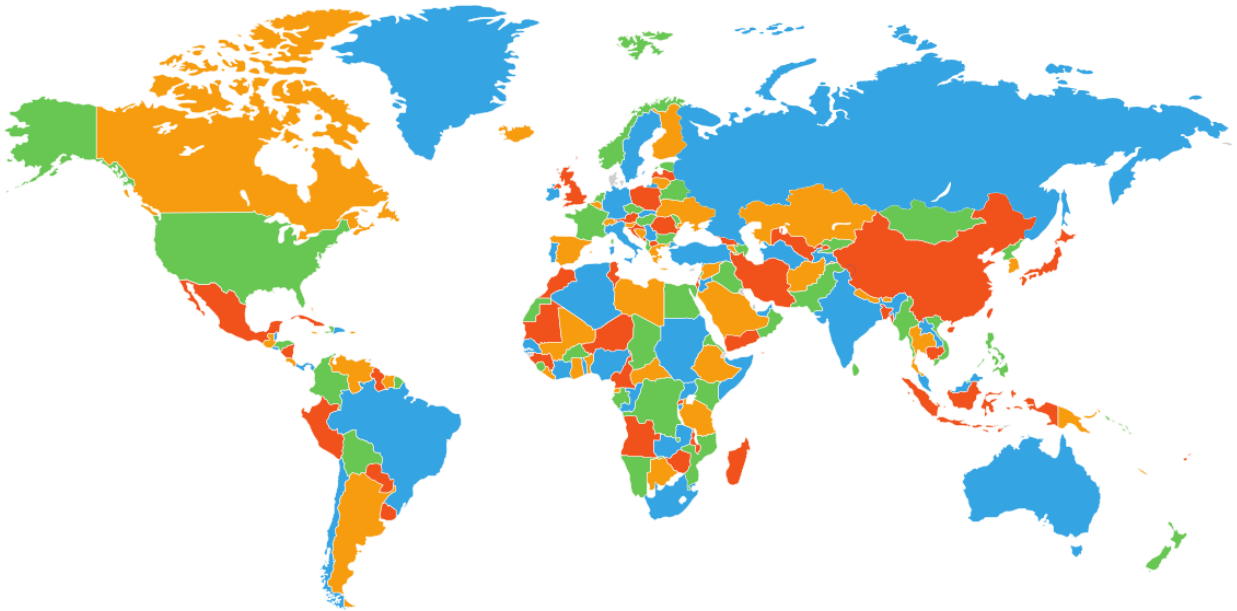
地图染色问题

对任意一幅地图的每个区域进行着色，使得相邻的区域不同色。**问最少需要多少种颜色才能实现?**

Hint: 每个地图可以导出一个图，用顶点表示国家，相应的边表示国家相邻

四色猜想

四色猜想现在应该叫做**四色定理**。四色定理的本质是**二维平面的固有属性**，即平面内不可出现交叉而没有公共点的两条直线。二维平面内无法构造五个或五个以上两两相连区域



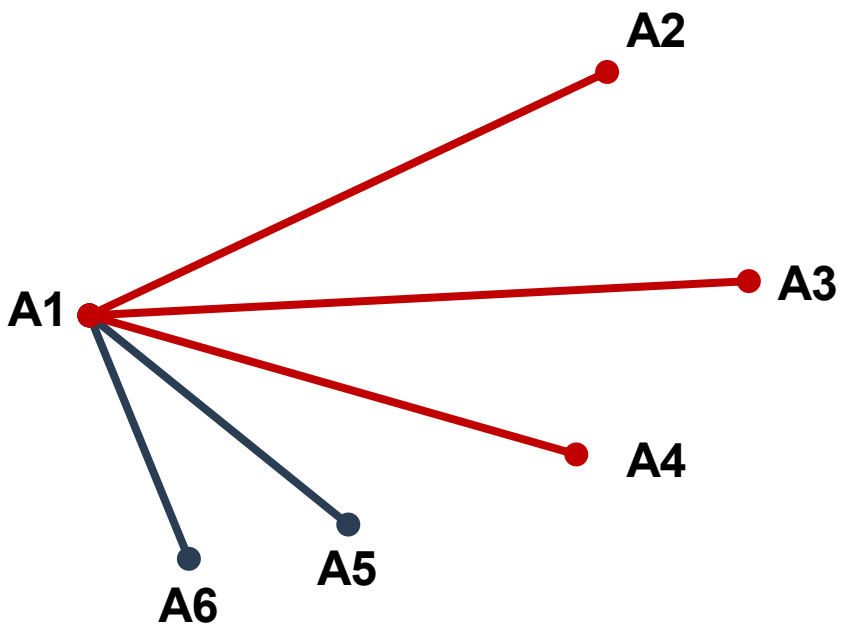
- 1976年，伊利诺斯大学的两台电子计算机，用1200个小时，100亿个判断，最终证明了四色定理。**但有很多人认为计算机证明无法给出令人信服的思考过程**

Ramsey问题

证明题：

任意6个人中，一定存在3个人相互认识，或者三个人相互都不认识

等价于证明6个顶点的完全图的边，用红、蓝二色任意着色，必然至少存在一个红色边三角形，或蓝色边三角形



- Ramsey数R(p,q)：代表了红蓝染色一个完全图，图中至少包含一个红色K_P或者蓝色K_q的完全图的最少边数
- 目前只有10个Ramsey数的值被确定，其他的都还是未知的
- 美国数学会前任主席R.L.Graham曾说过，要确定Ramsey数R(5，5)在100年之内是不可能的

网络结构对传播的影响——级联行为

- 场景
  - 一个社会网络；A，B两类事物要在其中流行
  - B是**“旧的”**，一直以来大家都采用B
  - A是**“新的”**，开始吸引了几个坚定份子
- 假设
  - 每个人只能采纳A或B之一
  - 两个相邻的人若都采用A，则得回报a；若都采用B，则得回报b；若采用不一样的，则回报0
  - 在从一种选择换到另一种过程中没有其他成本
  - **同时采用A和B，带来哪些不同?**

- 在一条边上的博弈
  - 如果v和w都选择A，它们分别得到回报a>0
  - 如果它们都选择B，分别得到回报b>0
  - 如果它们选择不同的选项，那么都得到回报为0
- **协调博弈：**一个节点v需要考虑其所有邻居选择的综合结果后再做决策

表达为一个博弈

节点V \ 节点W	A	B
A	a , a	0 , 0
B	0 , 0	b , b

网络节点的决策门槛

- 设v有d个邻居，在某一时刻，若占比p的邻居选A，占比1-p的邻居选B
- v选A的回报：pda

  选B回报：(1-p)db
- 如果pda ≥ (1-p)db，即若p≥b/(a+b)，则选A好；

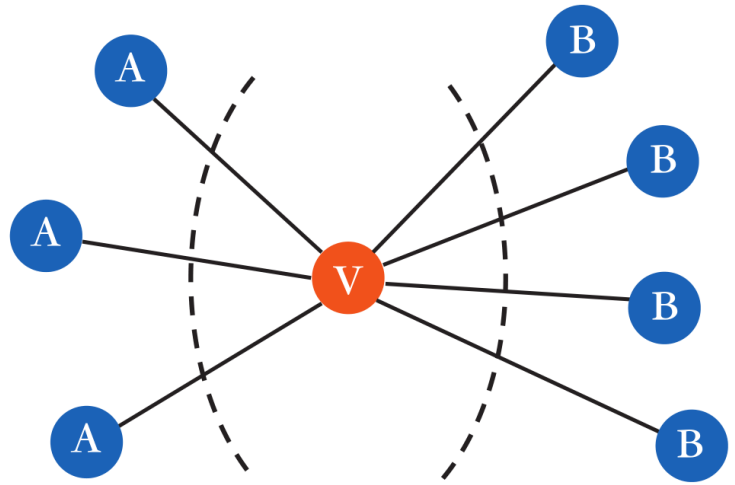
  否则，选B更好

博弈存在两个极端的情形，也是两个明显的均衡

- 所有节点都选择了A
- 所有节点都选择了B

（互为最佳应对，没人有动机改变）

有*(1-p)d* 邻居用B



有*pd* 邻居用A

门槛 $\frac{b}{a+b}=q$

如何开辟属于自己的“领地”

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

如何充分利用我们的资源？

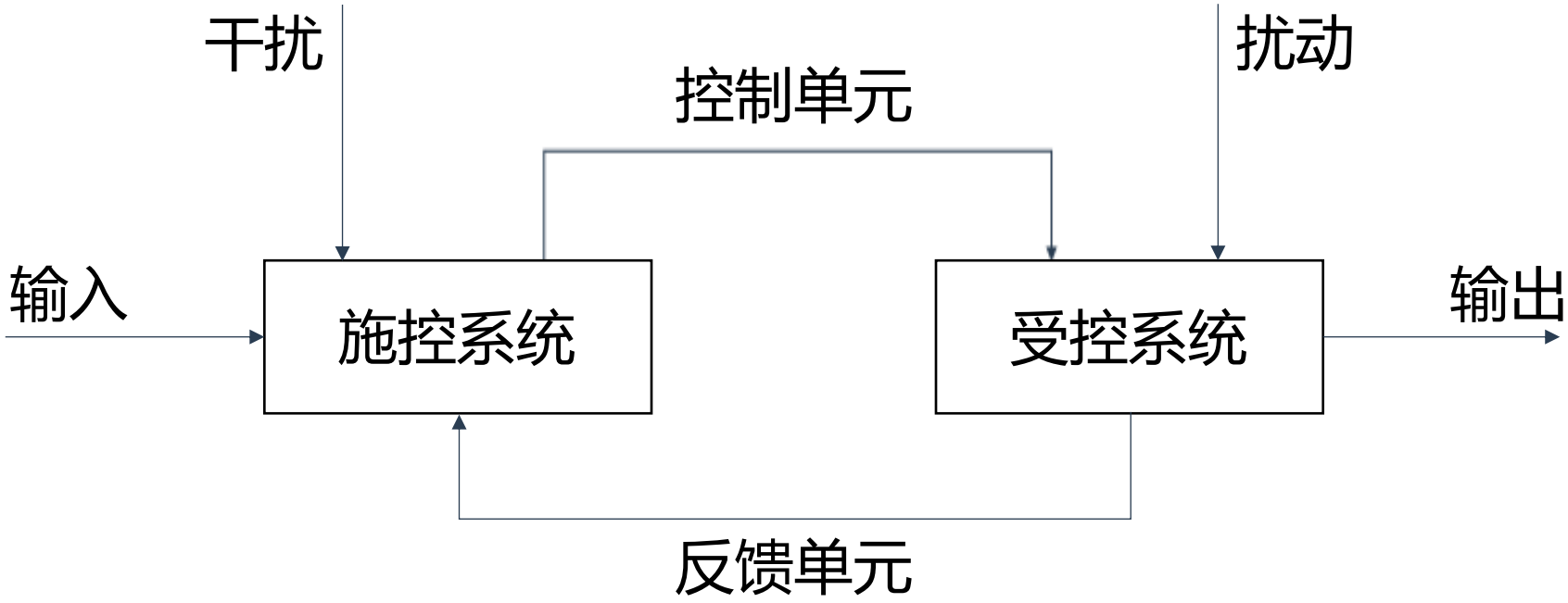
在什么地方进行拦截，能够极大地缓解病毒的蔓延？

- 对于“网络人”来说，工作、战场都在网络之上，因而我们不同的“网络人”要进行协作必须要有一个健康的网络作为支撑
- 开辟根据地的实质就是寻找擅长不同领域安全问题的红、白帽子集合与对应的边界节点集合之间的一个“最优”匹配

第3节 控制论

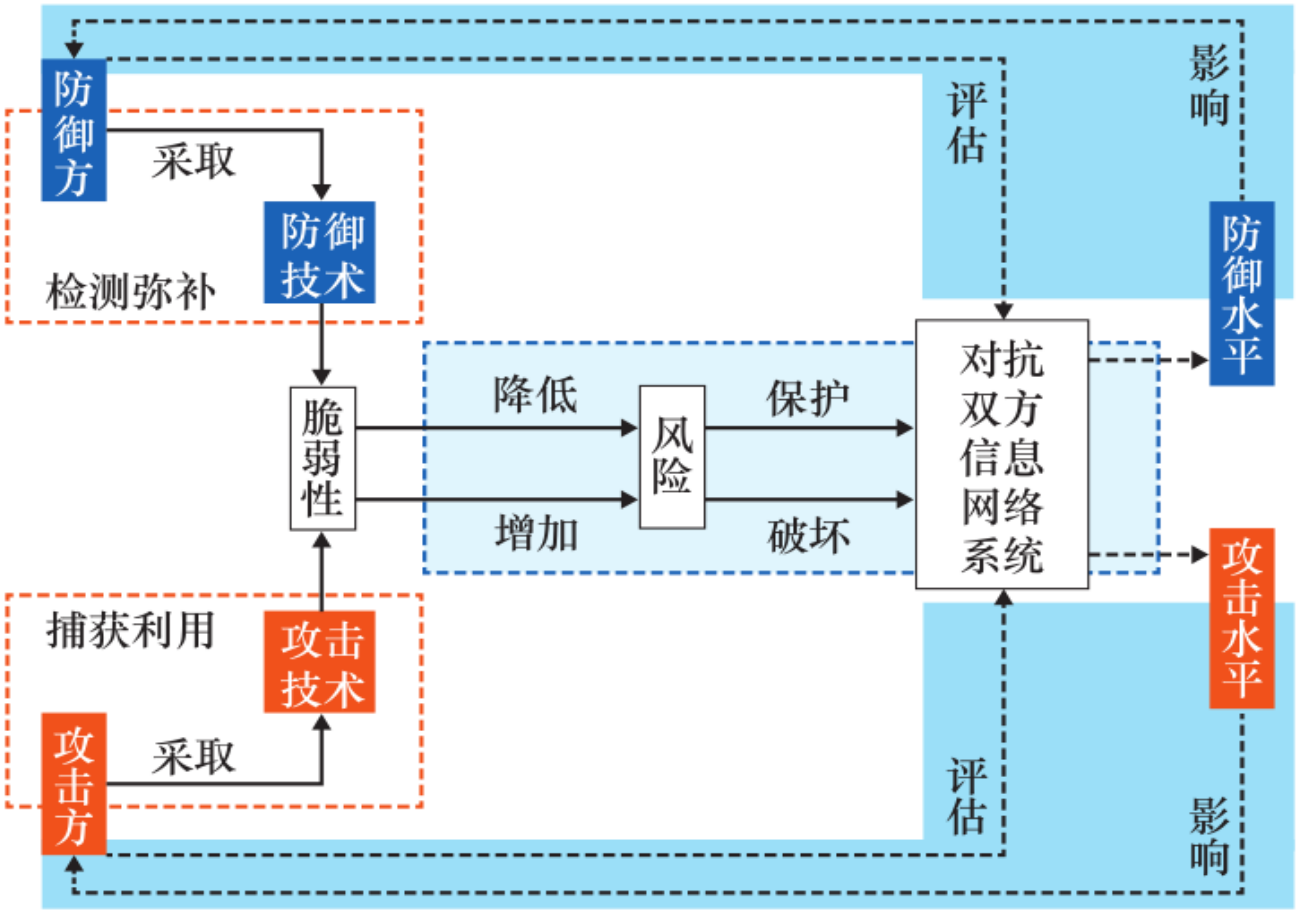
- 可能性空间
- 随机控制
- 有记忆控制
- 共轭控制
- 负反馈调节

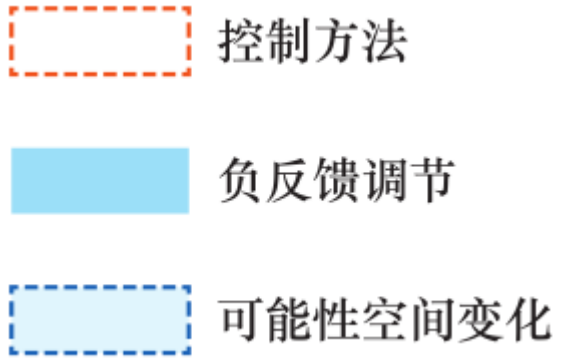
网络攻防控制模型



- 网络控制系统是典型的人机系统，由离散的事件驱动，并由离散事件按照一定运行规则相互作用来导致**状态演化**的动态系统
- 施控者可以作用与受控者，受控者也可以反作用于施控者。前者叫做控制，后者叫做反馈

网络攻防控制中的反馈模型

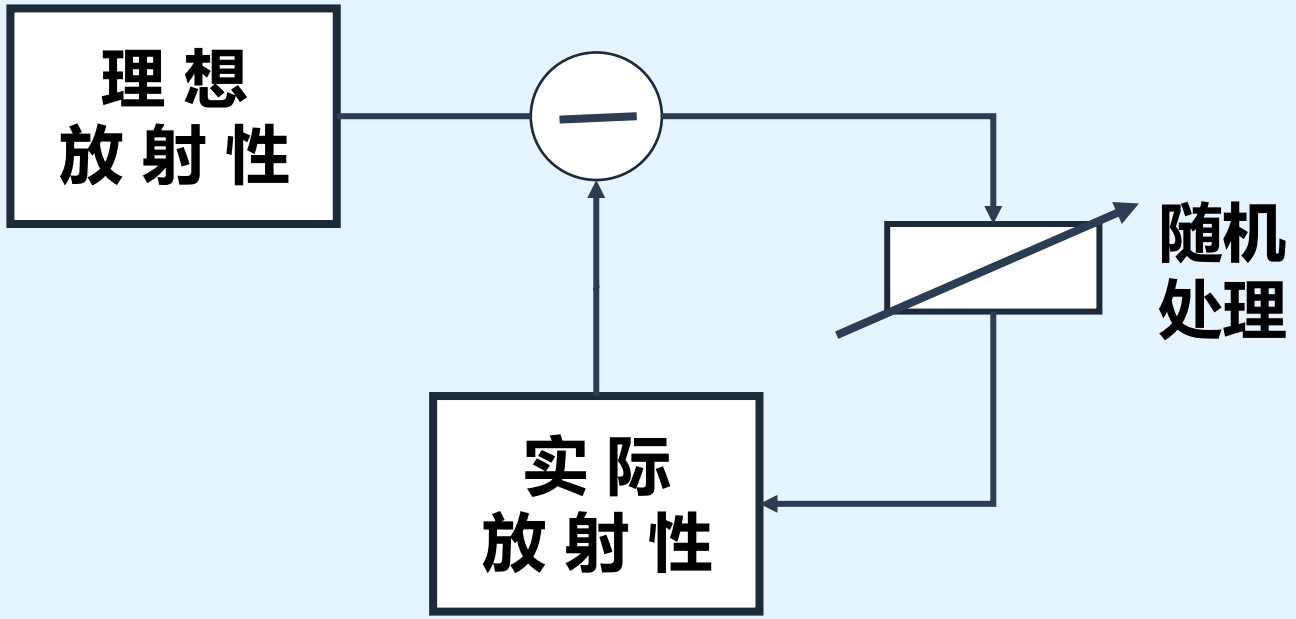




信息特别是与网络系统相关的**攻防知识**是网络攻防控制的核心

网络攻防控制就是网络攻防双方通过控制相关的网络攻防知识并根据做出决策的反馈来不断靠近目标的过程

负反馈调节



当人们一次的控制能力**不足以达到目标**时，通过收集到的信息，不断调整控制方案，直到达到目标的过程。其中，负反馈调节一定要有两个环节：

- 系统一旦出现目标差，便自动出现某种减少目标差的反应
- 减少目标差的调节一次一次地发挥作用，使得对目标地逼近进行积累

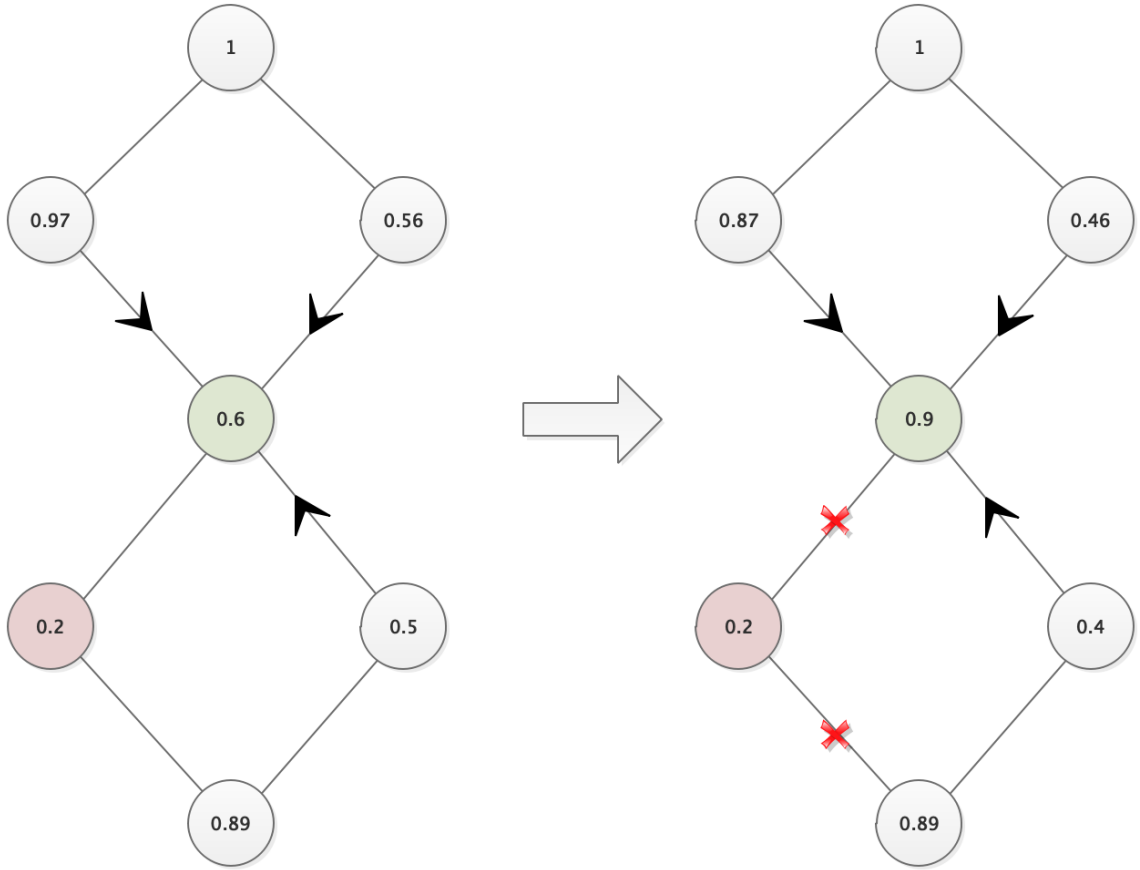
网络中的行为度分析

核心思想

通过对相关节点的观察和量化分析，获取节点信息反馈，并差异化的控制节点交互能力

意义

- 连接“真实性”与“安全性”
- 细化对节点可信、可靠程度的反馈，增加反馈的信息量
- 为网络态势和安全提供支撑



细化的反馈信息——行为度量

分类：直接偏离度、间接偏离度、推荐节点偏离度

直接偏离度

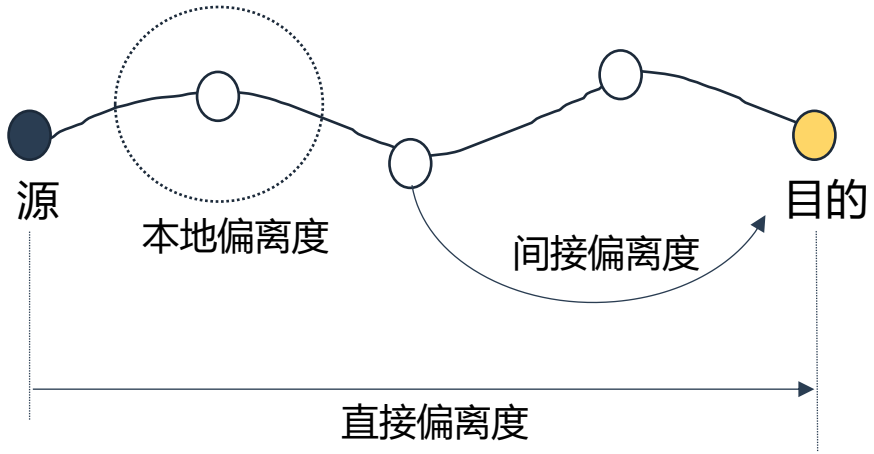
源端依据交互历史对目的端计算出的偏离度数值，按时间片更新，用以描述源端对目的端的直接评价

间接偏离度

转发路径上依据一定规则选取的推荐节点，针对目的节点给出的综合偏离度值，用以描述本次通信中相关节点对目的端的评价

推荐节点偏离度

根据与推荐节点直接相连的周边节点，对推荐节点的偏离度评价，计算得到的推荐节点自身偏离度，用以描述推荐节点本身的可靠性



通过引入偏离度，将节点信息映射目标由简单的离散二元空间转化为[0,1]连续实数空间，增强了反馈信息的容纳能力，从而提升了反馈控制能力

如何实施我们的策略集

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

如何充分利用我们的资源？

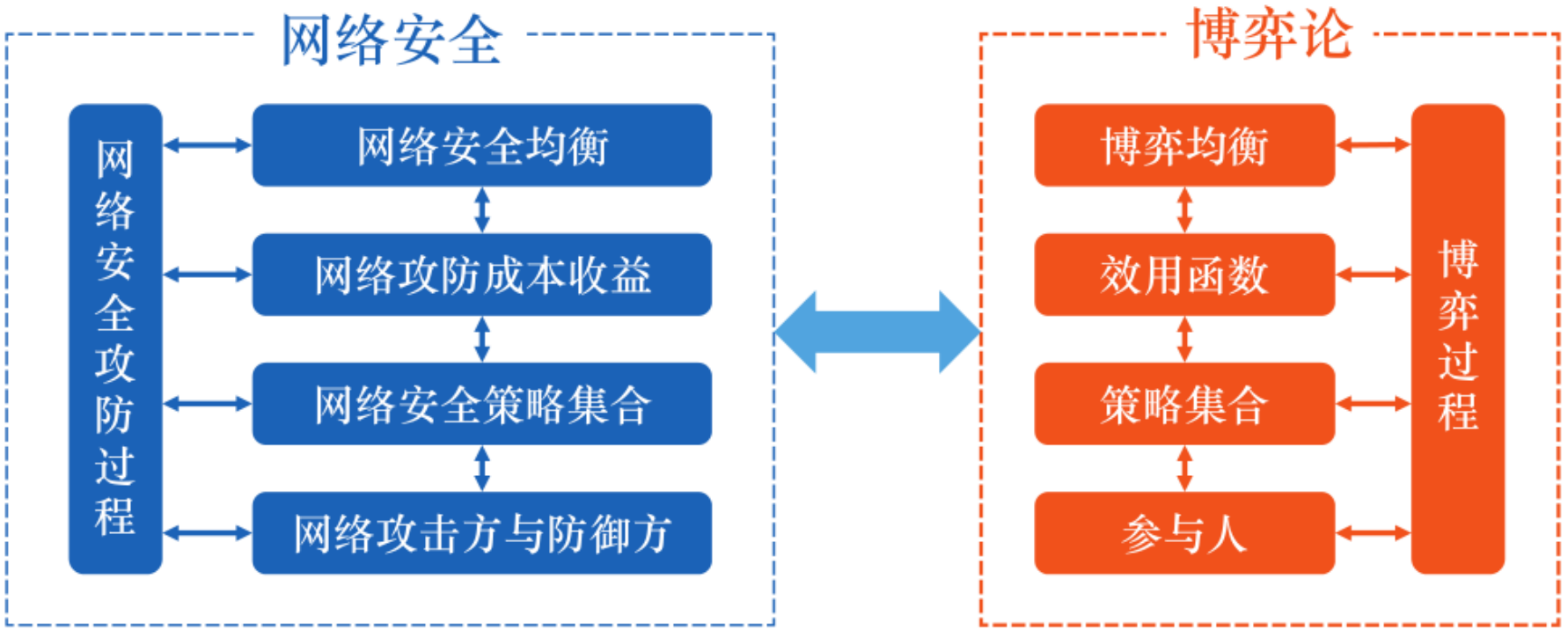
在什么地方进行拦截，能够极大地缓解病毒的蔓延？

- 在对“敌人”一无所知的时候，我们可以进行**随机接触**，随便挑选一种应对策略来应对对方
- 根据不同的反馈，逐步调整应对策略，最终找到一些行之有效的策略集合

第4节 博弈论

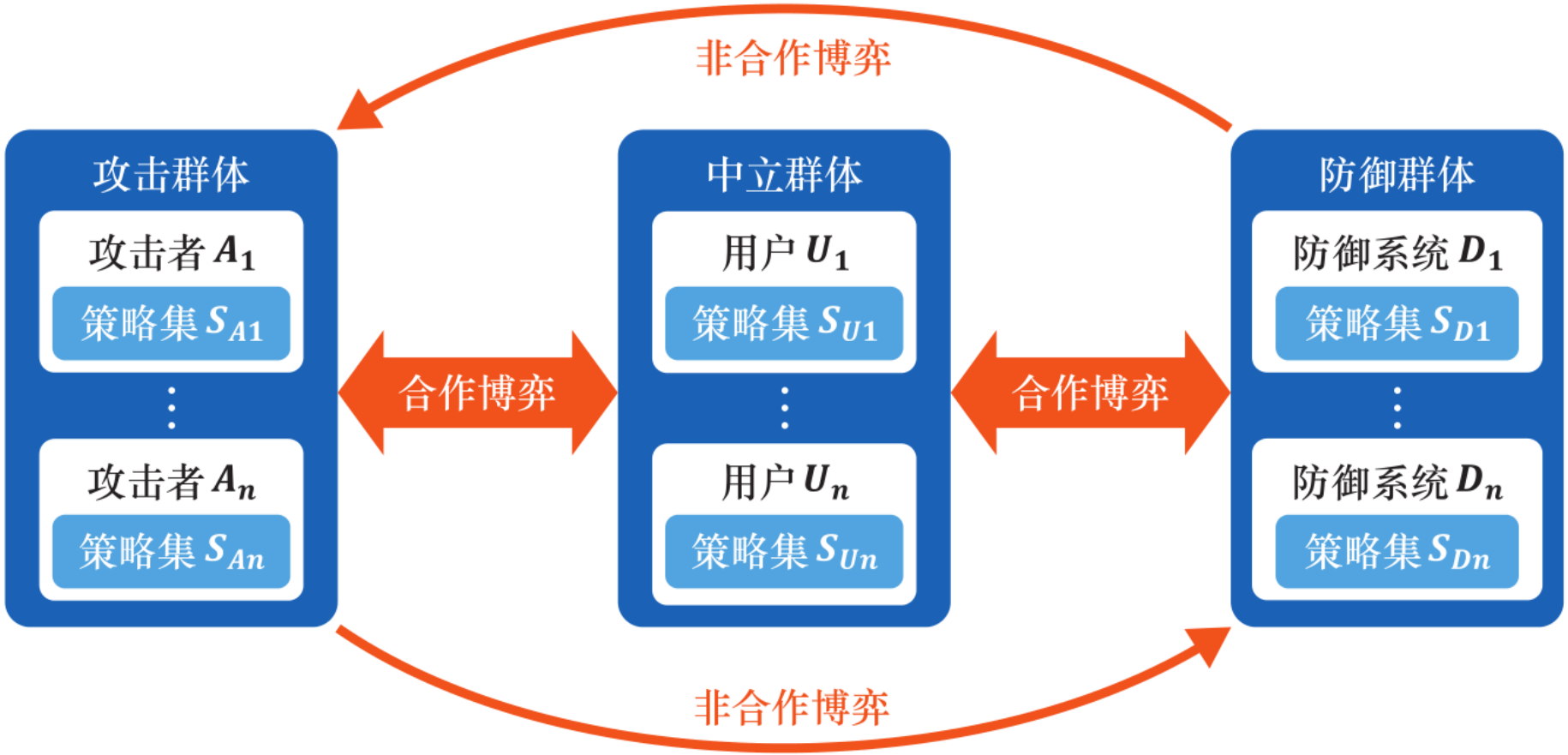
- 非合作博弈
- 合作博弈
- 纳什讨价还价

网络安全中的博弈论



网络安全的要素、特征与博弈论的元素、特征具有一致性和符合性。攻击者和防御者之间的对抗行为符合博弈论思想，而博弈论提供了一个解决网络安全分析和建模的**数学框架**，有助于理解攻防矛盾冲突、预测攻击行为和选取最优防御策略，因此将博弈论思想应用于网络安全问题研究具有较好的**合理性和可行性**

网络安全中的博弈论



网络安全态势博弈模型 NSG (Network Situation Game)

博弈论

博弈论 (Game Theory)

- 研究**互动的博弈**中参与者各自的选择策略
- 研究**机智而理性**的决策者之间的冲突及合作
- 参与者必须意识到他们的决策是相互影响的

博弈论把这些复杂关系**理论化**，以便分析其中的逻辑和规律，并对实际决策提供指导或借鉴

什么是一个博弈

- 博弈有下列要素
  - 至少**两个** 参与者
  - 每个参与者的**策略**
  - （策略）集合
  - 博弈结果的优先关系

什么是一个博弈

参与者

- 一般概念
- 个人，公司，国家，协议实体

策略（Strategy）

- 给定信息集下，一个策略决定了在每一个时间点上参与者选择何种行动
- 是参与者行动计划的一个完整描述，告诉参与者在每一种可预见的情况下选择什么行动

结果（Outcome）

- 由每个参与者的策略组合确定

支付（Payoff，收益）

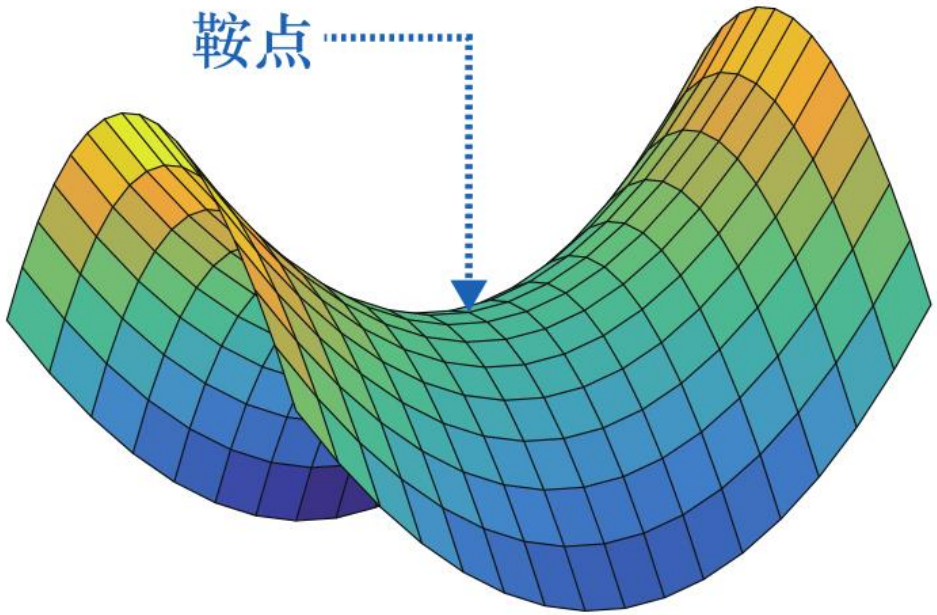
- 结果到效用的函数

优先关系

- 通过针对结果的效用（收益）函数来评价

博弈的求解

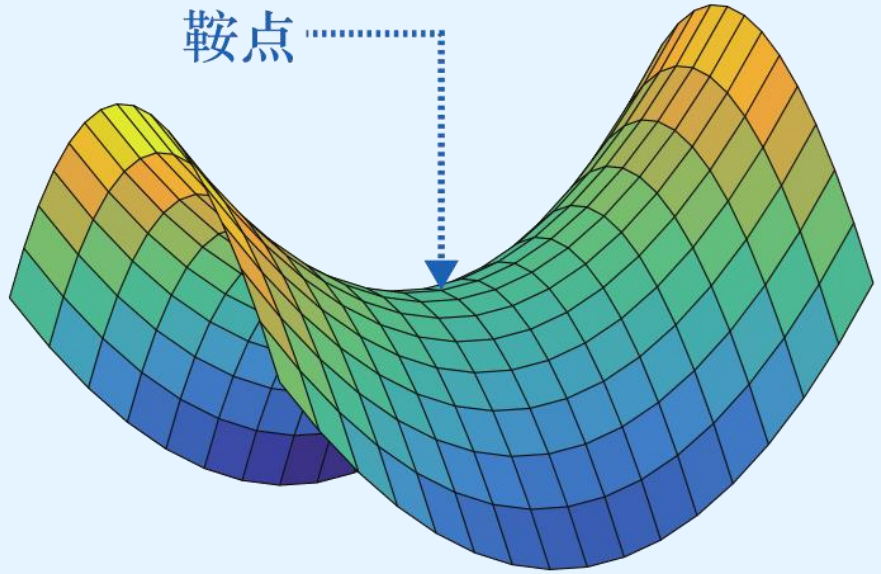
寻找收益矩阵中的鞍点



- 一个结果是鞍点，如果它是
  - **行中最小值、列中最大值**
- 鞍点原理
  - 参与人应该选择博弈中的鞍点
- 博弈的值
  - 如果鞍点存在，就是鞍点的值

博弈的求解

参与人1 \ 参与人2	A	B	D
A	12	-1	0
C	5	2	3
D	-16	0	-1



- 为什么参与人1相信参与人2会选择B?
  - 选择B能够保证**参与人2最多损失** v（这里是2）
- 为什么参与人2相信参与人1会选择C?
  - 选择C能保证**参与人1最少获得** v（这里是2）

这是为什么选择鞍点的合理原因!

混合策略

- 参与人为他的策略集关联概率分布
  - 参与人可以决定如何选择分布
- 按照**数学期望**计算收益

		参与人2	
		1/3	2/3
		C	D
参与人1	A	4	0
	B	-5	3

参与人1选择A时的收益 = (1/3)*4 + (2/3)*0 = 4/3

参与人1选择B时的收益= (1/3)*(-5) + (2/3)*3 = 1/3

应该如何决定概率分布?

极小极大定理

任何一个两人**零和**博弈都有一个混合策略的解（有时候是纯策略），解的收益是博弈的值

- Max-min = v = Min-max
- v 是唯一的
- 纯策略情况下可能存在多个均衡
- 完全可以互换

1928年冯•诺依曼给出了证明，标志着博弈论的诞生

纳什均衡

- 每个两人博弈都存在至少一个纯策略或者混合策略均衡
- 1950年纳什采用不动点定理进行了证明
- 获得1994年**诺贝尔经济学奖**（海萨尼，泽尔腾）
  - 在非合作博弈的均衡分析理论方面做出了开创贡献，对博弈论和经济学产生了重大影响

只要其它参与者不变换策略选择，任何**单个参与者不可能单方面通过变换策略来提高收益**

合作博弈

面对博弈，往往首先考虑**合作**，合作无法达成，则进行非合作博弈

合作的三种情况

- 事先可以达成有约束力的承诺，直接使用合作博弈方法
- 事先无法达成有约束力的承诺，使用能实现合作结果的非合作方法，如讨价还价博弈（Nash Bargaining）
- 无限次重复博弈，如无限次囚徒困境，仍然有可能达成合作解

合作博弈

- 一个**联盟**是参与人集合的子集，他们之间采取合作策略，并且就如何**分配收益**达成一致
- P是参与人集合，共有N个参与人

- 联盟用大写字母 S, T, U 表示
- 给定一个联盟 $S \subseteq P$，它的对手联盟则是

$$S^C = P - S = \{p \in P : p \notin S\}$$

合作博弈的解

功利主义：Shapley值

- 功利主义（utilitarianism），即效益主义，提倡追求“最大幸福”（Maximum Happiness）
- 主要代表人物约翰·斯图亚特·密尔（John Stuart Mill）、杰瑞米·边沁（Jeremy Bentham）等

平均主义：核

- 核中任意一个分配都不会导致参与者组合脱离总合作。如果核中包含一个解 x，那么参与者不会形成其他联盟来代替

Shapley值

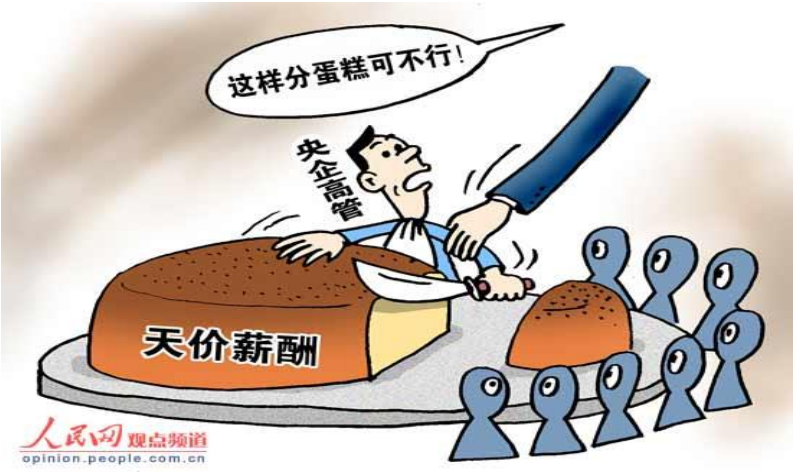
- 由 **L.S. Shapley** 于 1953 年提出，以一种公平的方式定义了一种分配，计算了每一位参与者的最终收益“应该”是多少
- 考虑了参与者对其所在联盟的边际效益
- 如果博弈的特征函数是v，参与者p_i所属联盟为S，那么

$$\delta(p_i, S) = v(S) - v(S - \{p_i\})$$

即为衡量该参与者对联盟的贡献大小（**称为边际贡献**）

纳什讨价还价(Nash Bargaining)

John F. Nash, Jr. The Bargaining Problem. Econometrica, Vol. 18, No. 2 (Apr., 1950), pp. 155-162，**Google 引用超过10000**



两人讨价还价场景：

- 两人合作的总收益大于各自单干的收益之和
- 两人需要一个规则来分配合作后获得的 “蛋糕”，每人都以自己的收益最大为目标，因此存在一个“讨价还价”的过程
- 如果两人达成协议，则按照协议分配收益；否则，只能单干，获取较少收益

纳什讨价还价(Nash Bargaining)

公理1：个体理性

- 合作后每个人的收益都不少于单干时的收益，即

$\varphi_1(F,v) \geq v_1$，$\varphi_2(F,v) \geq v_2$

公理3：对称性

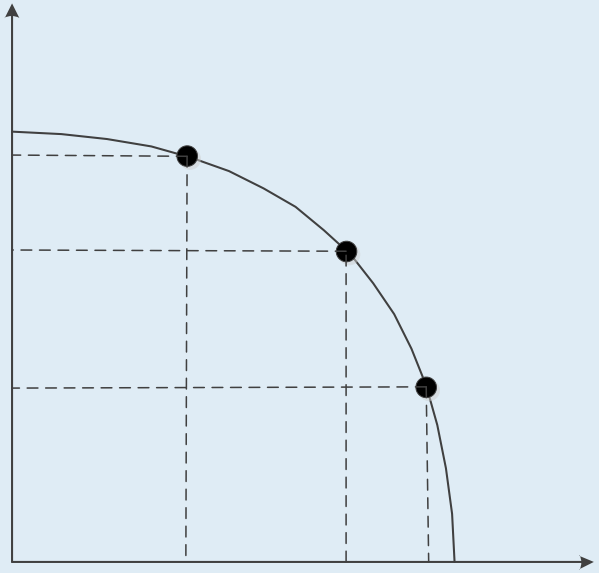
- 参与人的收益配置互换后也是可行的，地位相同的人待遇也相同，即：

如果$(x_1,x_2) \in F$，必有$(x_2,x_1) \in F$

如果$v_1 = v_2$，那么$\varphi_1(F,v) = \varphi_2(F,v)$

公理2：Pareto强有效

- 纳什讨价还价解必定位于Pareto边界上



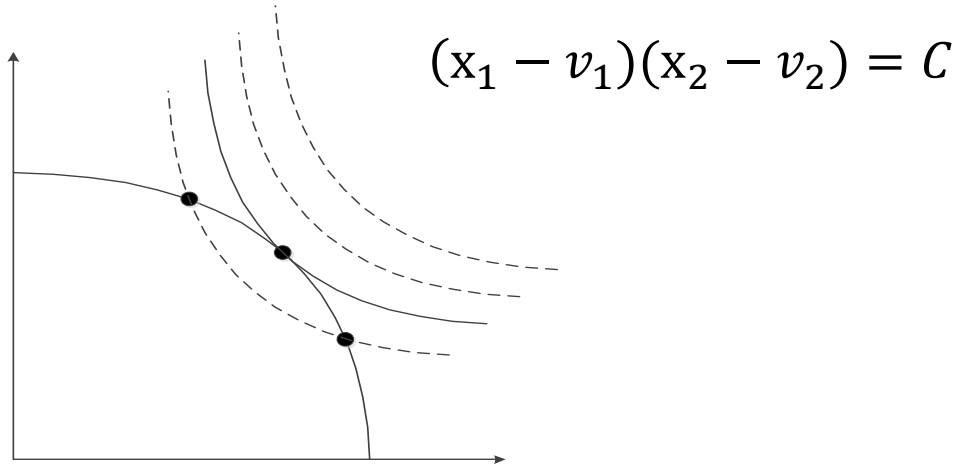
纳什讨价还价(Nash Bargaining)

公理4：等价盈利描述的不变性

- 一个讨价还价问题通过仿射变换变为另一个讨价还价问题，那么原讨价还价解通过仿射变换后也成为新讨价还价问题的解

公理5：无关选择的独立性

- 移除讨价还价解之外的点不会影响讨价还价解的求得



对于两人讨价还价问题 (F, v)，存在满足公理1-5的唯一讨价还价解

如何与我们的敌人进行周旋

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

如何充分利用我们的资源？

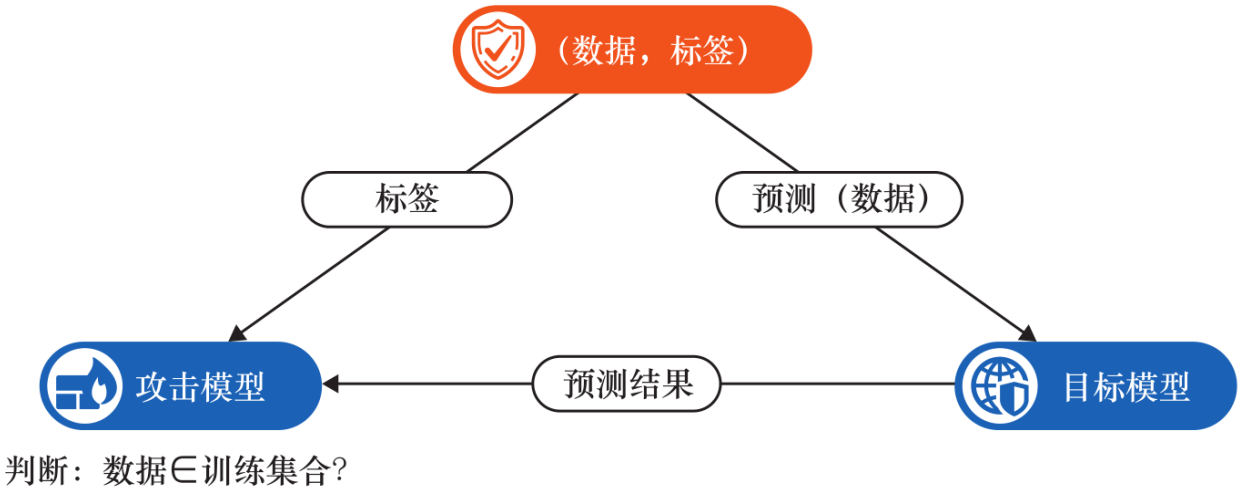
在什么地方进行拦截，能够极大地缓解病毒的蔓延？

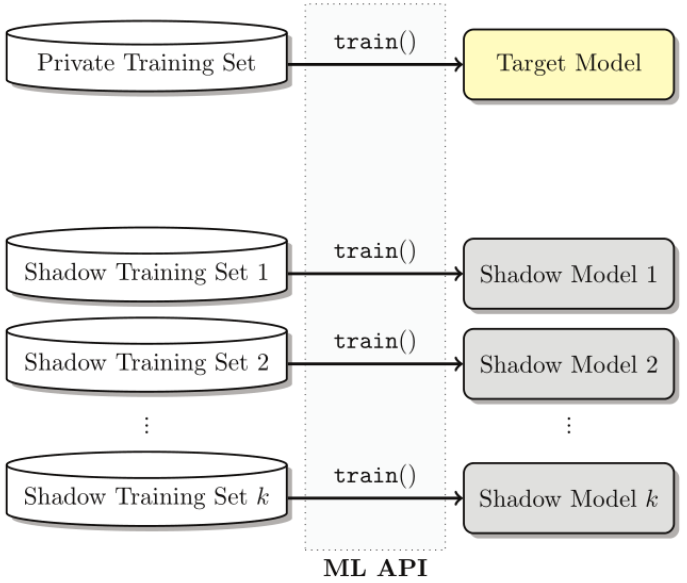
- 我们与对手之间是一个零和博弈，如何找到零和博弈的鞍点，从而能够知道理智对手最可能的行动策略
- 在网络之上，是否存在着第三方可供拉拢的中立组织，利用合作博弈的思想将他们拉拢过来，形成联盟，为最终的战斗胜利积聚力量

第5节 最优化理论

- 最优性条件
- 线性规划
- 凸优化
- 非凸优化

网络安全中的最优化





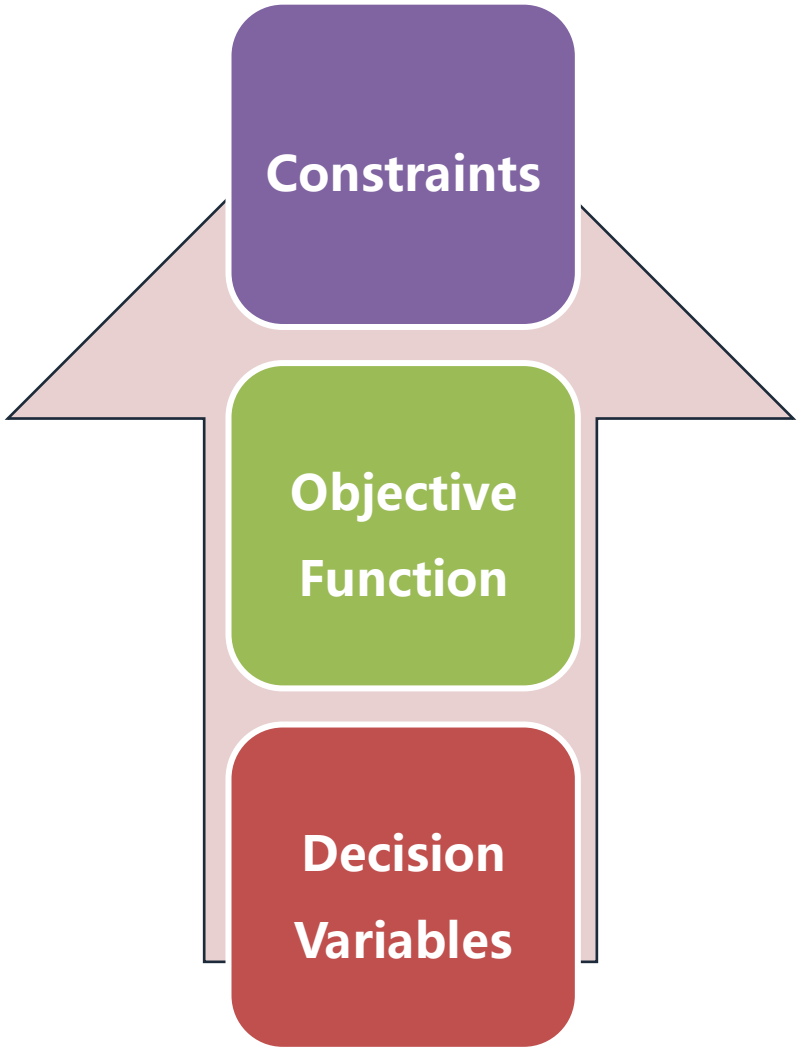
- 对互联网公司提供的黑盒机器学习模型服务进行攻击
- 挑战数据匿名问题，可以使得攻击者预测出相关数据是否在模型训练的数据集中
- 主要思想为优化，找到使得模型**预测信心最大的数据**（爬山算法）

最优化理论的描述

要做的决策是什么?
要达到的目标是什么
决策有什么约束?

$$\begin{aligned} \text{minimize/maximize}_x \quad & f(x) \\ \text{subject to} \quad & x \in \Omega \end{aligned}$$

- x: Decision
- $f(\cdot)$: Objective
- Ω: Constraints



线性规划

目标函数

$$\max(\min) Z = c_1 x_1 + c_2 x_2 + \cdots\cdots + c_n x_n$$

约束条件

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots\cdots + a_{1n}x_n \le (=\cdot\ge)\ b_1 \\ \quad\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots\cdots + a_{mn}x_n \le (=\cdot\ge) b_m \\ x_1 \ge 0 \cdots\cdots x_n \ge 0 \end{cases}$$

约束区域是n维超多面体，目标函数也是仿射函数的规划问题

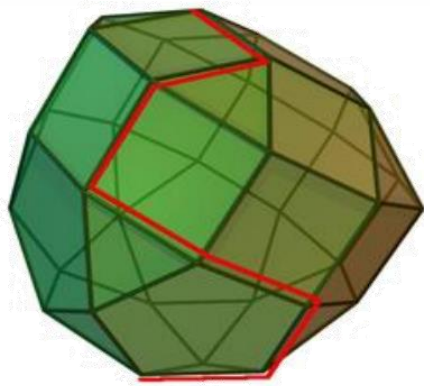
线性规划

George Bernard Dantzig

November 8, 1914 – May 13, 2005

Dantzig is "generally regarded as one of the three ounders of linear programming, along with John von Neumann and Leonid Kantorovich "

- **若线性规划问题有解，则必可在的某个顶点上取得最大值**
- **单纯形表的引入，寻找最优顶点**



最优性条件

$$\begin{aligned} \min \quad & f(\mathbf{x}) \\ \text{s.t.} \quad & g_j(\mathbf{x}) = 0, \quad j = 1, \ldots, m, \\ & h_k(\mathbf{x}) \leq 0, \quad k = 1, \ldots, p. \end{aligned}$$

根据优化问题，我们可以引入拉格朗日乘子，将问题**转化为相应的无约束问题**：

$$\begin{aligned} \nabla_{\mathbf{x}} L &= \mathbf{0} \\ g_j(\mathbf{x}) &= 0, \quad j = 1, \ldots, m, \\ h_k(\mathbf{x}) &\leq 0, \\ \mu_k &\geq 0, \\ \mu_k h_k(\mathbf{x}) &= 0, \quad k = 1, \ldots, p. \end{aligned}$$

一阶必要条件

Karush-Kuhn-Tucker (KKT)

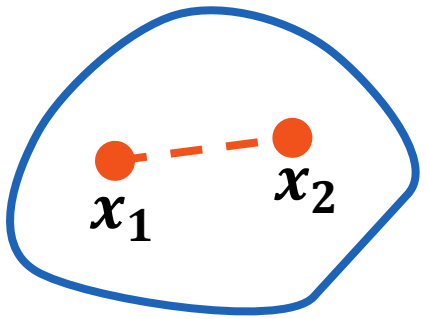
$$L\left(\mathbf{x}, \{\lambda_j\}, \{\mu_k\}\right) = f(\mathbf{x}) + \sum_{j=1}^{m} \lambda_j g_j(\mathbf{x}) + \sum_{k=1}^{p} \mu_k h_k(\mathbf{x})$$

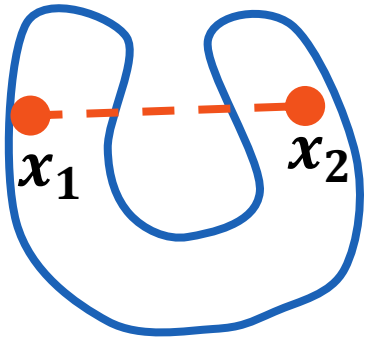
凸优化

- 定义：设S是n维欧式空间的点集，若$\forall x_1, x_2 \in S, t \in [0,1]$，都有：

$$X = tx_1 + (1-t)x_2 \in S$$

则称S为凸集



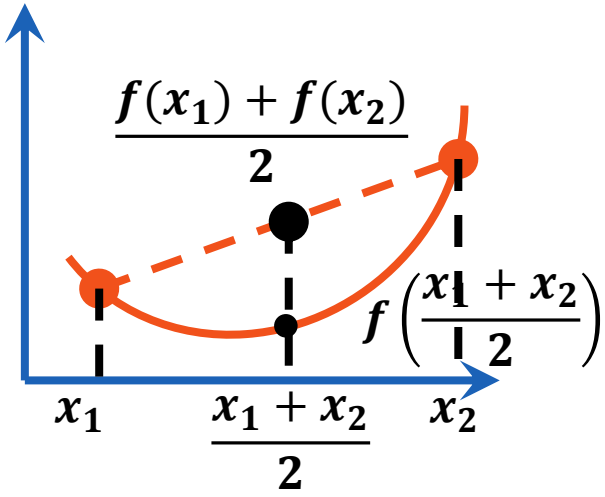


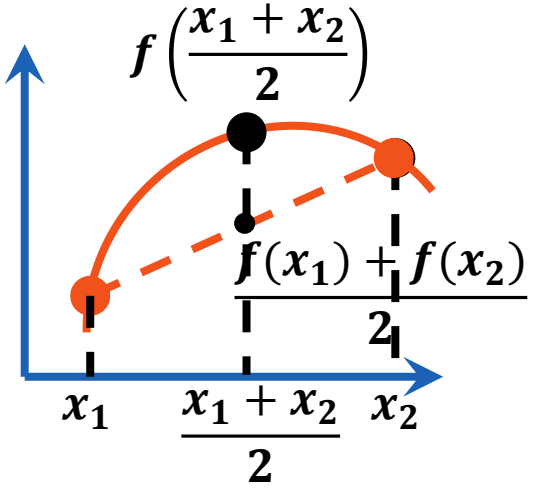
- 定义：设f是某个向量空间的凸子集S上的实值函数，$\forall x_1, x_2 \in S$，

$X = tx_1 + (1-t)x_2$，都有：

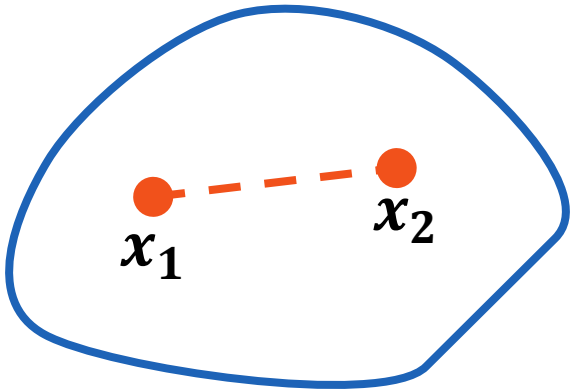
$$f(X) \leq tf(x_1) + (1-t)f(x_2)$$

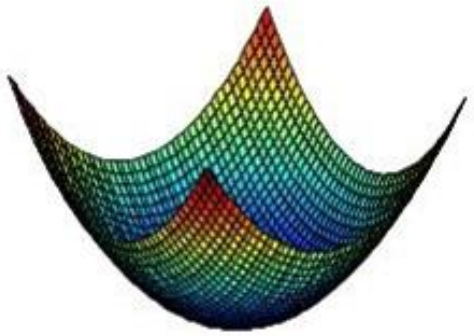
则称f为凸函数





凸优化

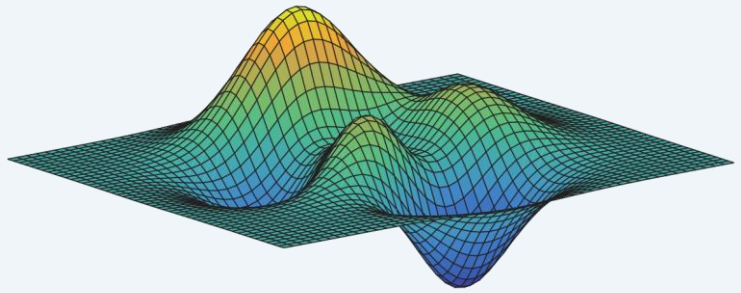




Unique optimum: global = local

- **可行域为凸集且目标函数为凸函数**的优化问题被称为凸优化问题
- 有良好的性质：**局部最优点一定是全局最优点**
- 此时KKT条件变为**充要条件**，KKT点即为全局最优解
- 各种数值优化算法：找到使得目标函数减小的方向，不断移动，直到收敛

非凸优化



- **Multiple local optima**
- **In high dimensions possibly exponential local optima**

- 非凸优化问题被认为是非常**难求解的**，因为可行域集合可能存在无数个局部最优点，通常求解全局最优的算法复杂度是指数级的（NP Hard）

- 蒙特卡洛投点法：随机选择任意一个点，通过凸优化算法找到附近的局部最优。如此重复，直到满足一定条件

如何充分利用我们的资源

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

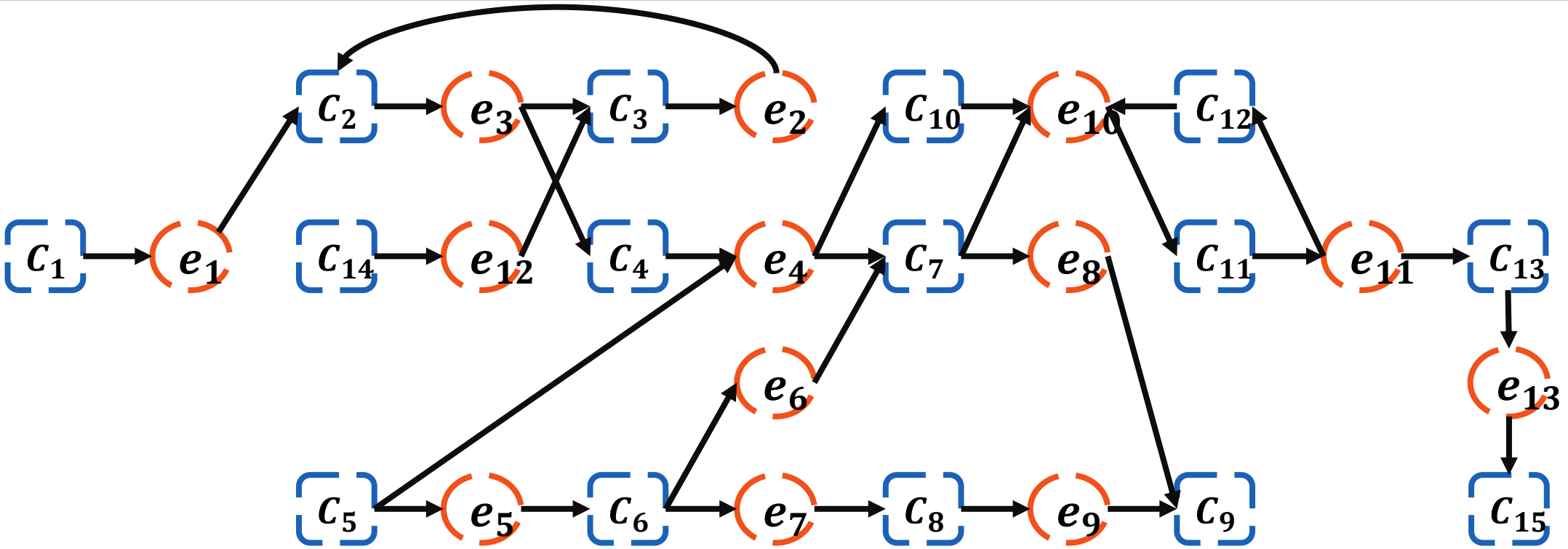
如何充分利用我们的资源？

在什么地方进行拦截，能够极大地缓解病毒的蔓延？

- 无论是人员调配还是物资统筹，都是一个具体的优化问题
- 通过优化问题的抽象、求解，得出内耗最小、外力最大的统筹调配方案，实现最优的作战意图

第6节 概率论与随机过程

网络安全中的概率论



- 通用安全脆弱点评估系统**CVSS(Common Vulnerability Scoring System)**，关注于单个脆弱点的属性量化，提供了在目标网络中攻击者成功渗透的概率
- 对目标网络进行安全评估，需要识别网络中攻击者利用各个脆弱点之间相互关系形成的潜在威胁
- 攻击图结合CVSS系统，形成了所示的**贝叶斯网络**

交互式零知识证明

Alice（证明者）

Bob（验证者）

You do have the solution!

- After n round, the probability of Alice has a solution will be

$$Pr[\cdot] = 1 - \frac{1}{|E|^n}$$

- If n is very large, Alice will convince Bob

通过n次交互，在n次Alice都提供了正确答案的情况下，事情发生的**概率降到了很小的水平**，于是Bob接受了Alice掌握正确答案的信息，同时Alice关于**正确答案的信息也没有泄露**

如果因为**传输错误**、或者**人为疏忽**，中间有提供了**错误答案**，我们该怎么办？

假设检验

核心思想：

“小概率事件”原理，其统计推断方法是带有概率性质的反证法

- 预先设定小概率值(小到多少是你能接受的“小概率”)
- 作出假设（一般是二元假设）
- 选择概率计算模型
- 计算如果假设为真的情况下，事件发生的概率
- 如果事件为小概率事件，则推翻原假设，否则接受

本意为假设为真的情况下，事件发生的概率很小，则认为它不会发生，从而证明假设不正确

Bob（验证者）

- Bob的假设：Alice不知道答案
- 选择概率计算模型：二项分布
- 若假设为真，Alice n次回答均正确的概率为 $P = \frac{1}{|E|^n}$
- 由于$\frac{1}{|E|} \leq 1$，所以存在某个n，n次之后，P小于小概率值
- Bob结论：Alice知道答案

Alice（证明者）

在什么地方拦截能够最大程度阻止敌人

战略准备 → 战略相持 → 战略反攻

如何开辟属于自己的“领地”？

如何实施我们的策略集？

如何和我们的敌人进行周旋？

如何充分利用我们的资源？

在什么地方进行拦截能够最大程度缓解病毒的蔓延？

- 每一个网络节点都有自己的防御系统，根据我们前期与敌人的接触，可以评估每一个节点**被渗透的概率**
- 同时，根据节点周边“敌人”的情况，构建一个贝叶斯网络，来获得所有节点被攻破的概率，从而判断敌人最有可能进攻的位置

第7节 总结和展望

总结

第一节
新的开始

- 网络安全事件，需要集合不同的理论知识来解决

第二节
图论

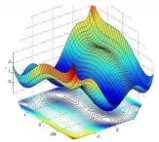
- 抽象为着色与匹配问题在网络上开辟根据地

第三节
控制论

- 用随机控制进行初步接触，用反馈调节进行修正

第四节
博弈论

- 用零和博弈的思想来分析双方的策略应对



第五节
最优化理论

- 用优化的思想来调度、规划人员和物资

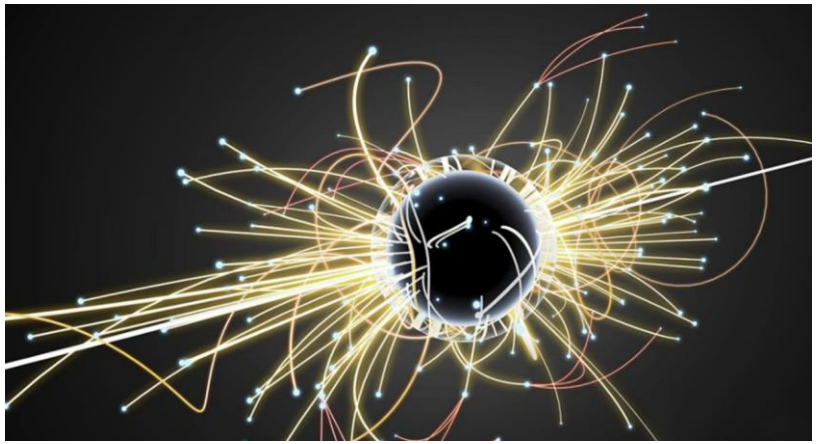
第六节
概率论与随机过程

- 通过节点建模和贝叶斯网络来找出对手的薄弱点

展望

新技术、新应用的出现，网络安全需要新的基础理论支撑

量子通信



量子计算

6G应用

- **传统基础理论**如何在**新的技术场景**、**新的网络应用**中支撑安全分析
- **新的理论突破**，以应对新的安全场景和安全应用