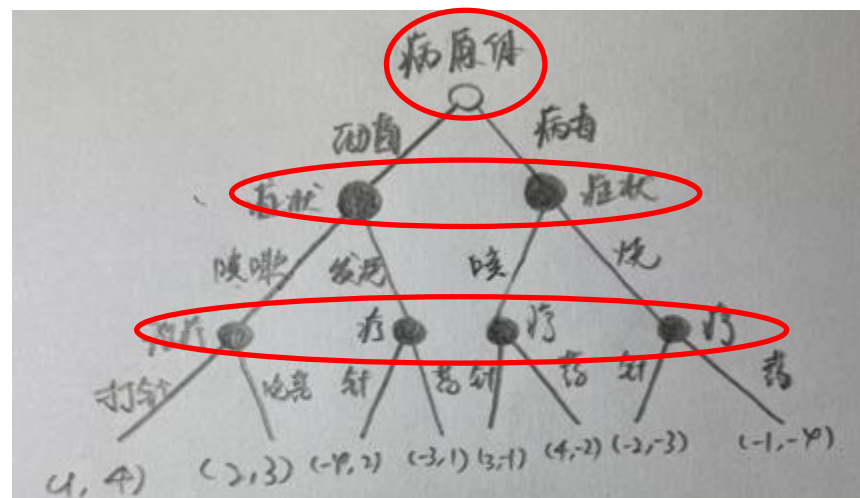
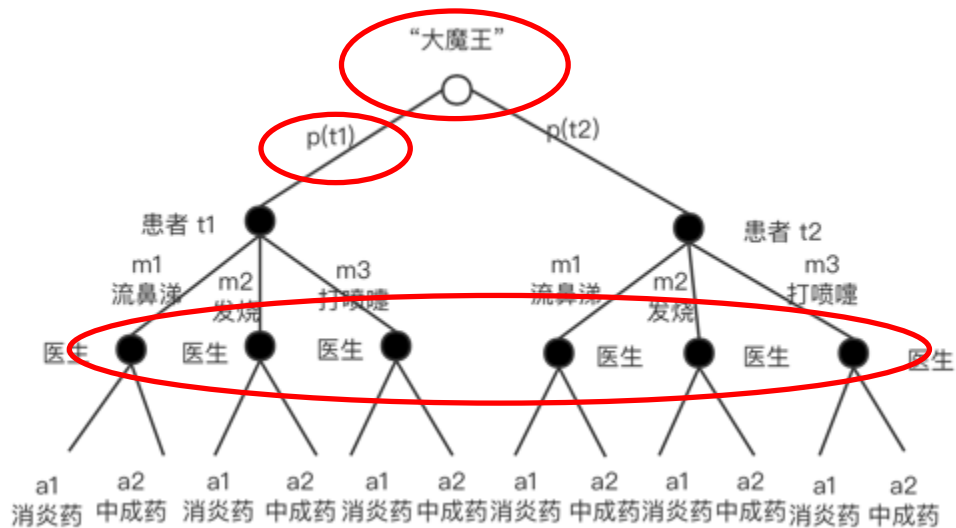
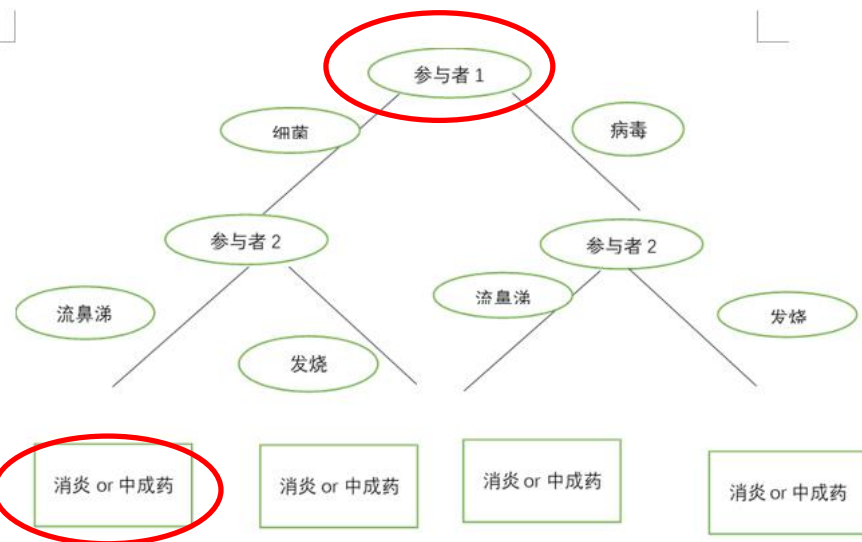
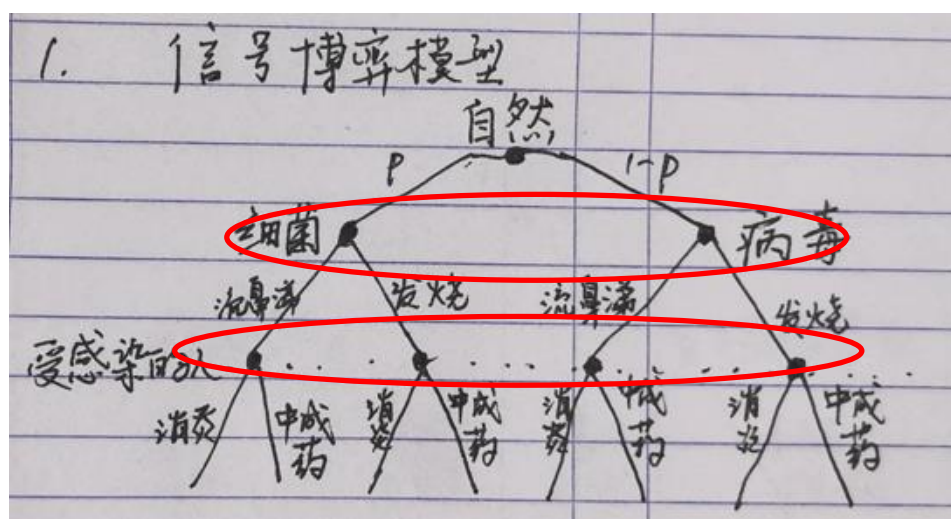
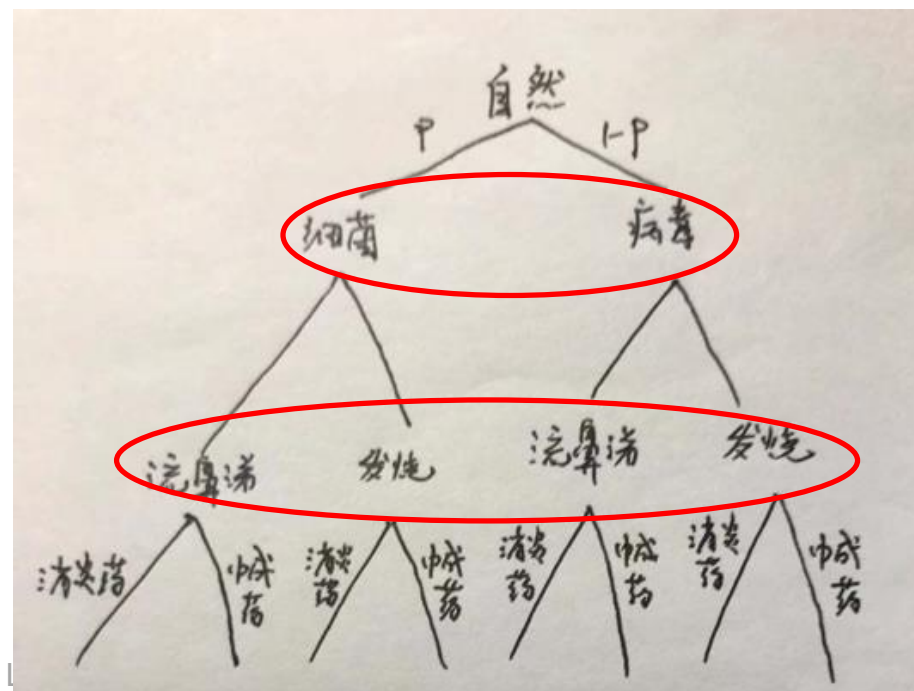
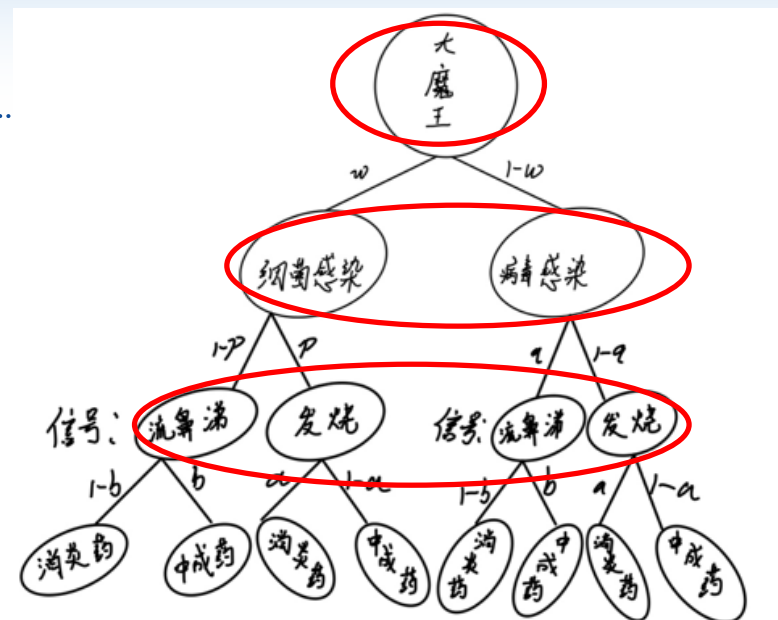
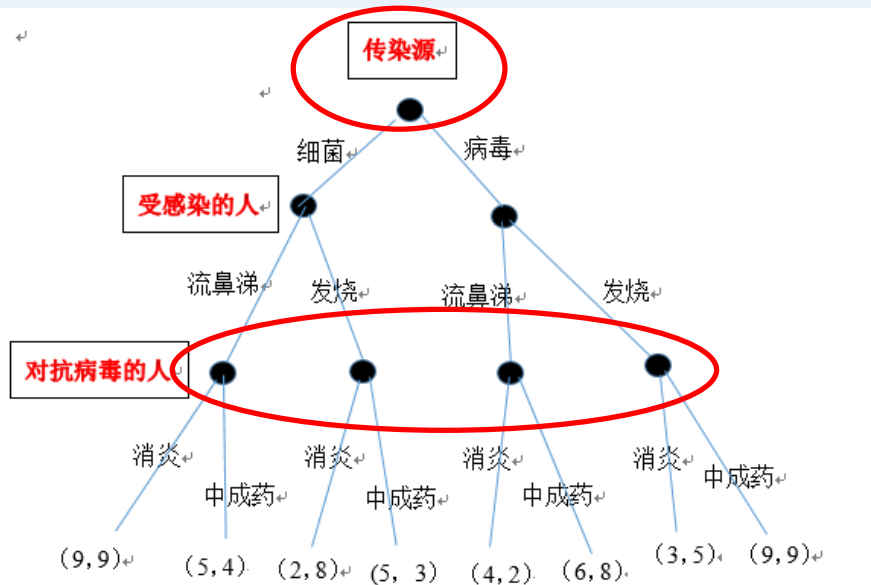
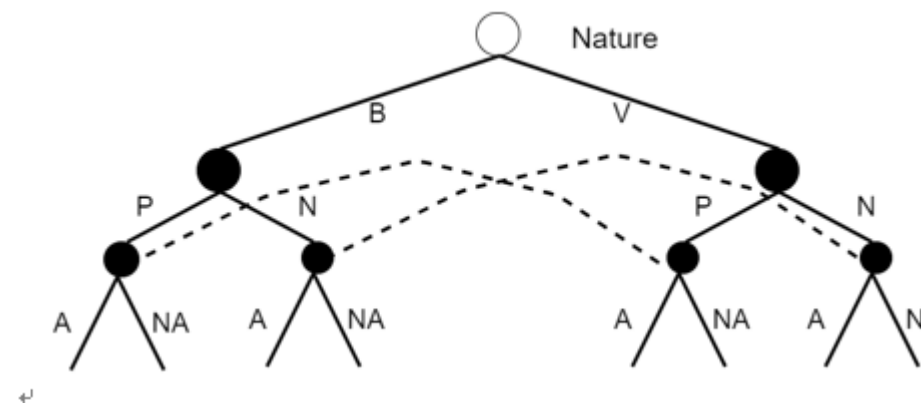
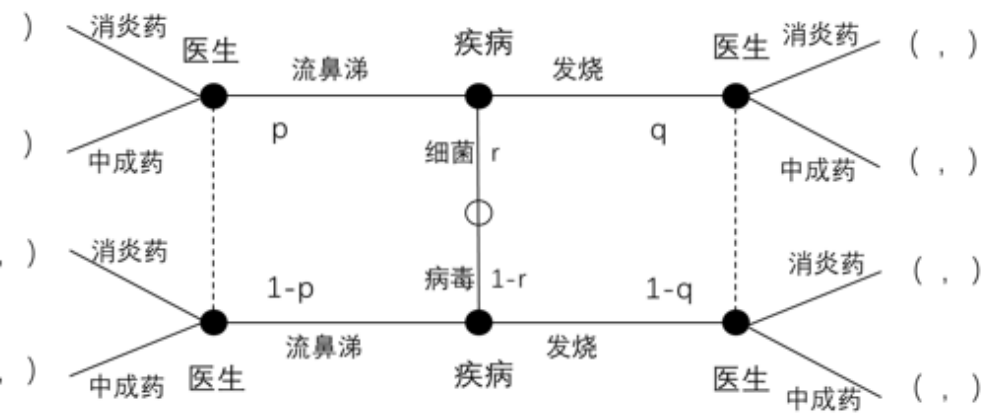
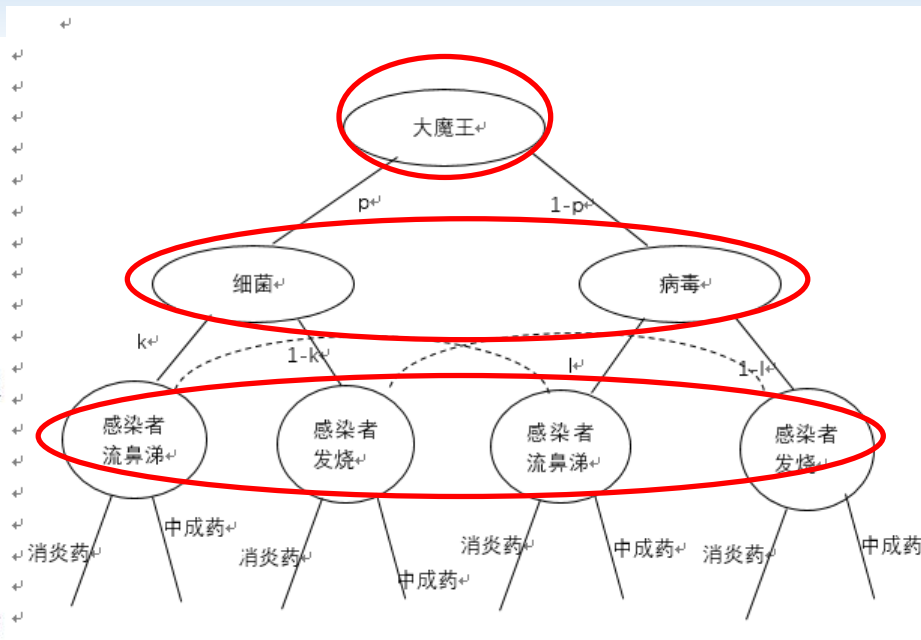
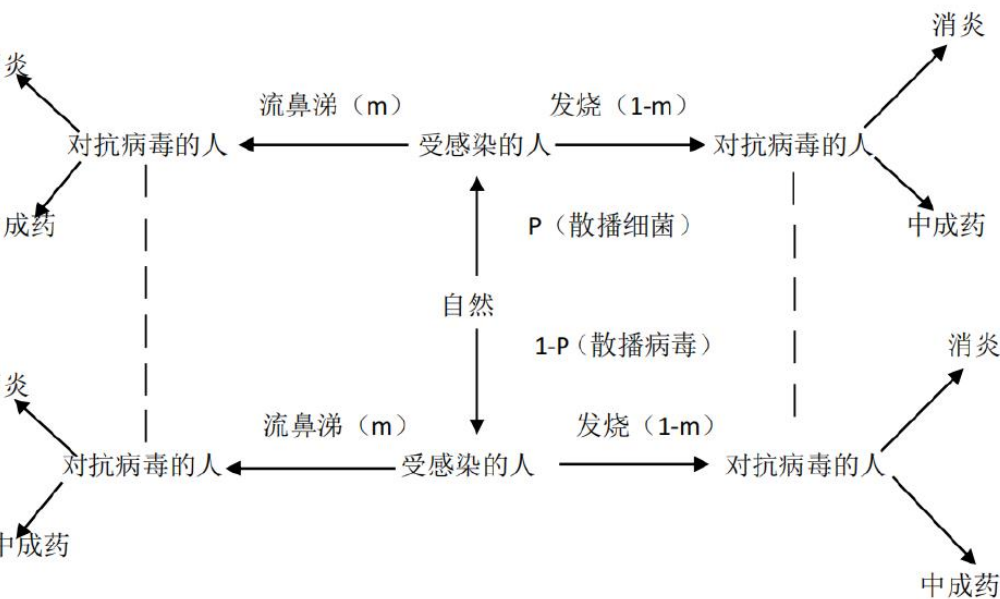


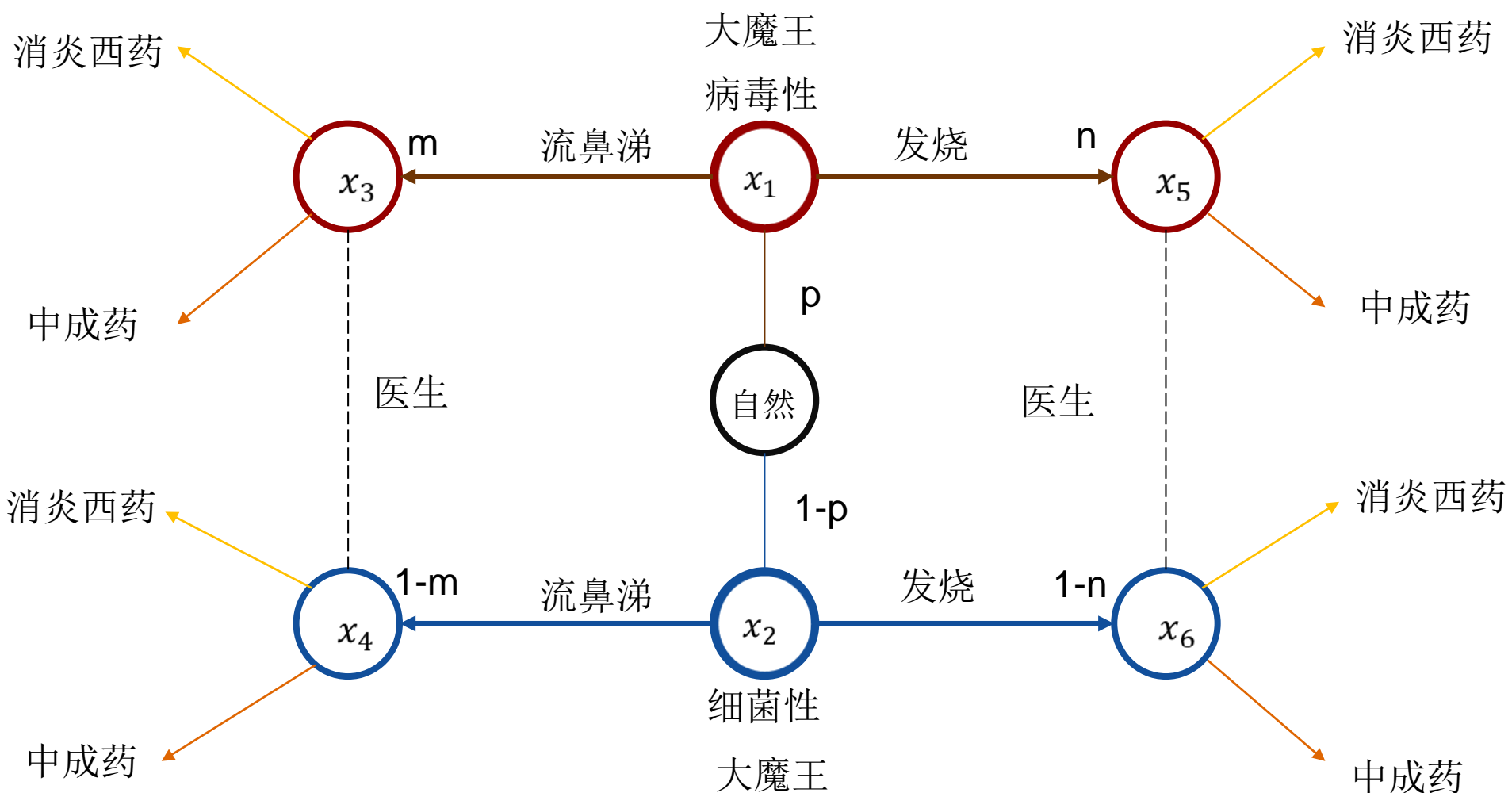


信号博弈与应用



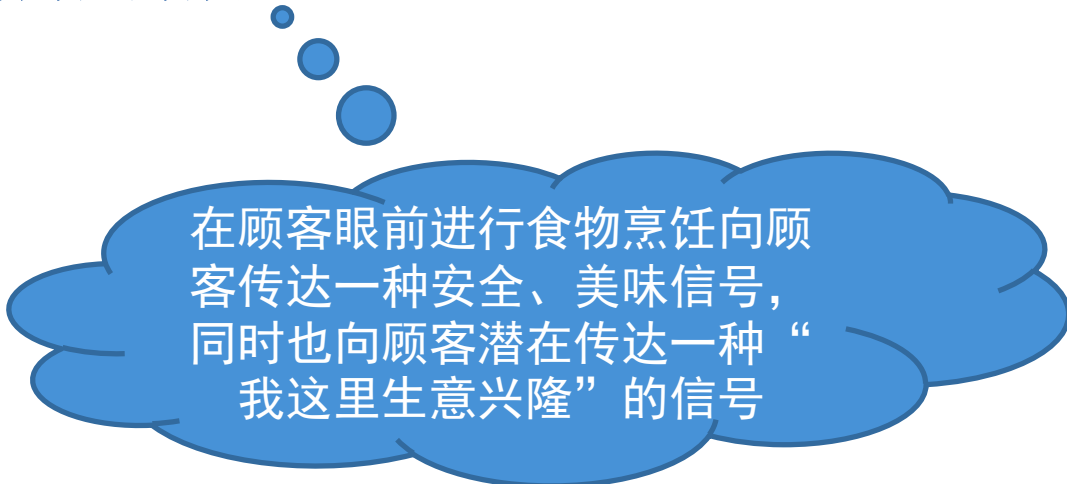






❖ 日常生活中信号博弈的应用——路边摊

- 路边摊、夜市有很多的现做小吃摊位，顾客多的话还需要等待店家现做，那为什么不提前炒好，有人买时只需要加热一下，就像便利店里那样省时省力



在顾客眼前进行食物烹饪向顾客传达一种安全、美味信号，同时也向顾客潜在传达一种“我这里生意兴隆”的信号

❖ 日常生活中的常见现象蕴含信号博弈——网购

- 网络购物市场是一个**不完全信息市场**，消费者不能如进入实体店那样，通过直接接触感受商品品质，此时**价格信号**则承载了商品质量的信息。
- 商家为信号发送者，消费者为信号接收者，商家根据**商品品质（即类型）**选择**价格（即信号）**，消费者根据价格判断商品品质的好坏决定要不要购买
- 商家可以花费一定的**伪装成本**发出**高价信号**销售**低品质商品**，比如：伪造销售量，伪造好评

❖ 日常生活中的常见现象蕴含信号博弈——劳动力雇佣

- 在劳动力市场上，当需要雇佣劳动力的企业（或雇主）对出卖劳动力的工人的能力不清楚时，工人如何通过选择自己接收教育的程度向企业传递有关自己能力的信息
- 工人为信号发送者，企业为信号接收者，工人根据自己的能力（即类型）选择接收教育的程度（即信号），企业根据工人的教育程度决定工人的工资（即接收者行动）

❖ 实例总结

- 信号博弈的参与者为信号发送者和信号接收者
 - 信号发送者拥有不同的类型，并根据自身的类型选择发送的信号
 - 信号接收者不可直接观察到发送者的类型，需根据接收到的信号推断发送者的类型，根据判断选择自己的行为

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 信号博弈的定义

- 信号博弈（**signaling games**）是一类比较简单而应用广泛的不完全信息动态博弈。
- 信号传递博弈是指有两个参与人，信号发送者发出私人信息，信号接收者在接受信息发送者的信息基础上做出决策的博弈。

第一节：信号博弈基本概念



❖ 博弈描述

- 博弈的参与人分为**信号发送者**（**Sender**）和**信号接收者**（**Reciever**），信号发送者首先发送一个关于**自身类型**的信号，信号接收者根据所接收到的信号选择**自身行动**。
- 在信号博弈中发送者发出的信号依赖于**自然赋予的类型**，因此，先行动的信号发送者的行动对于后行动的信号接收者来说，具有**传递信息**的作用。同时，这又使得接收者的行动依赖于发送者选择的**信号**。

第一节：信号博弈基本概念



❖ 具体博弈时序

- 自然根据特定的概率分布 $p(t_i)$ ，从可行的类型集 $T = \{t_1, t_2, \dots, t_n\}$ 中选择发送者类型 t_i ，这里对 $\forall i \in \{1, 2, \dots, n\}$ ，需满足 $p(t_i) > 0$ 且 $p(t_1) + \dots + p(t_n) = 1$ 。
- 发送方观测到 t_i ，然后从可行的信号集 $M = \{m_1, m_2, \dots, m_J\}$ 中选择一个发送信号 m_j ；
- 接收者不能观测到 t_i ，但能观测到 m_j ，接收者从可行的行动集 $A = \{a_1, a_2, \dots, a_K\}$ 中选择一个行动 a_k ；

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 博弈描述

- 在信号博弈中，发送者发出的信号依赖于自然赋予的类型，因此，先行动的信号发送者的行动，对后行动的信号接收者来说，具有传递信息的作用。同时，这又使得接收者的行动依赖于发送者选择的信号。

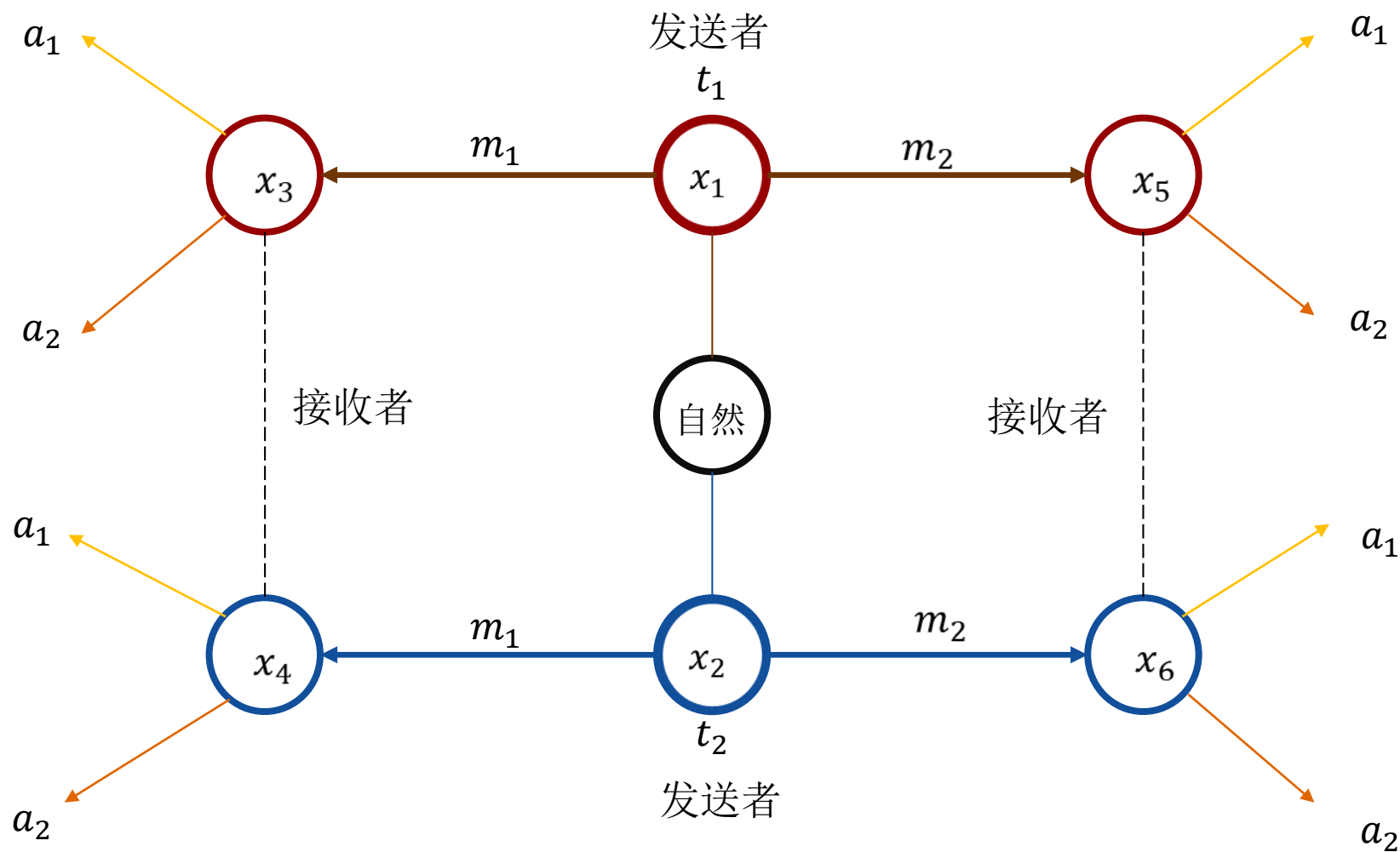
第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 具体博弈描述



第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 基本特征

- 发送者的信息集为 $I_s(x_1)$ 和 $I_s(x_2)$ ，对应观测到自然的选择为 t_1 和 t_2 ，行动分别为 m_1 和 m_2 ，因此发送者的发送策略为：

$$s: H_s \rightarrow M$$

- 其中 H_s 为发送者的信息集合，即为：

$$H_s = \{I_s(\{x_1\}), I_s(\{x_2\})\}$$

第一节：信号博弈基本概念



❖ 发送者的四种纯策略

- 策略(m_1, m_1)——自然赋予发送者 t_1 状态，发送者选择 m_1 信号，即 $s(t_1) = m_1$ ；自然赋予发送者 t_2 状态，发送者仍选择 m_1 信号，即 $s(t_2) = m_1$
- 策略(m_1, m_2)——自然赋予发送者 t_1 状态，发送者选择 m_1 信号，即 $s(t_1) = m_1$ ；自然赋予发送者 t_2 状态，发送者选择 m_2 信号，即 $s(t_2) = m_2$

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 发送者的四种纯策略

- 策略(m_2, m_1)——自然赋予发送者 t_1 状态，发送者选择 m_2 信号，即 $s(t_1) = m_2$ ；自然赋予发送者 t_2 状态，发送者选择 m_1 信号，即 $s(t_2) = m_1$
- 策略(m_2, m_2)——自然赋予发送者 t_1 状态，发送者选择 m_2 信号，即 $s(t_1) = m_2$ ；自然赋予发送者 t_2 状态，发送者仍选择 m_2 信号，即 $s(t_2) = m_2$

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 发送者策略分类（根据发送者类型与发送信号的相互关系）

- 混同（**pooling**）策略：对于第1个和第4个策略，在不同类型时发送者都发送相同信号，称为混同策略
- 部分混同（**partially pooling**）策略：在多于两种类型的模型中，所有术语给定类型集的类型都发送同样的信号，但不同的类型集发送不同的信号，成为部分混同策略

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 发送者策略分类（根据发送者类型与发送信号的相互关系）

- 分离（**separating**）策略：对于第2个和第3个策略，在不同类型时发送者发送出不同信号，称为分离策略，分离策略意味着不同类型的发送者发送的信号不同

第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

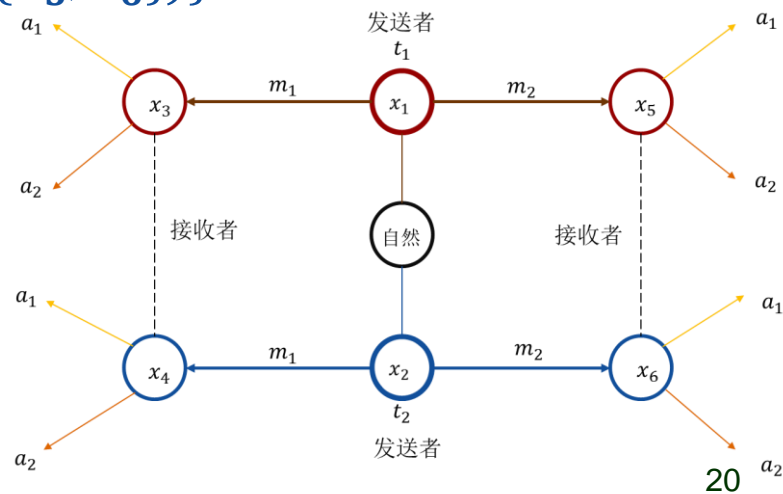
❖ 接收者

- 接收者的信息集为 $I_R(\{x_3, x_4\})$ 和 $I_R(\{x_5, x_6\})$ ，分别对应观测到信号 m_1 和 m_2 ，行动为 a_1 和 a_2 ，因此接收者的策略为：

$$s: H_R \rightarrow A$$

- 其中， H_R 为接收者的信息集合，即

$$H_R = \{I_R(\{x_3, x_4\}), I_R(\{x_5, x_6\})\}$$



第一节：信号博弈基本概念



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 接收者的四种纯策略

- 策略(a_1, a_1)——发送者选择 m_1 信号，接收者选择 a_1 行动，即
 $s(m_1) = a_1$ ；发送者选择 m_2 信号，接收者仍选择 a_1 行动，即
 $s(m_2) = a_1$
- 策略(a_1, a_2)——发送者选择 m_1 信号，接收者选择 a_1 行动，即
 $s(m_1) = a_1$ ；发送者选择 m_2 信号，接收者选择 a_2 行动，即
 $s(m_2) = a_2$

第一节：信号博弈基本概念



❖ 接收者的四种纯策略

- 策略(a_2, a_1)——发送者选择 m_1 信号，接收者选择 a_2 行动，即
 $s(m_1) = a_2$ ；发送者选择 m_2 信号，接收者选择 a_1 行动，即
 $s(m_2) = a_1$
- 策略(a_2, a_2)——发送者选择 m_1 信号，接收者选择 a_2 行动，即
 $s(m_1) = a_2$ ；发送者选择 m_2 信号，接收者仍选择 a_2 行动，即
 $s(m_2) = a_2$

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- （1）在每一信息集中，应该行动的参与者必须对博弈进行到该信息集中的哪个节点有一个判断。对非单节信息集，推断是在信息集中不同节点的一个概率分布；对于单节的信息集，参与者的推断就是到达此单一决策节的概率为1
- 精炼贝叶斯Nash均衡定义中的信号条件：在观测到M中的任何信号mj之后，接收者必须对哪些类型可能会发送mj，持有一个推断。

这一推断用概率分布 $p(t_i | m_j)$ 表示，其中对，且

$$\forall t_i, p(t_i | m_j) \geq 0, \sum_{t_i \in T} p(t_i | m_j) = 1$$

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- 由于发送者知道自己的类型，其选择发生于单决策结信息集，因此，信号条件(R1)在应用于发送者时就无需附加任何条件；
- 接收者在不知道发送者类型的条件下观测到发送者的信号，并选择行动，也就是说接收者的选择处于一个非单决策结的信息集上，因此，信号条件(R1)应用于接收者的信息集。

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- （2）给定发送者的信号和接收者的判断，参与者的战略必须满足**序贯性**的要求。即在每一信息集中应该行动的参与者，对于给定的该参与者在此信息集中的推断，以及其他参与者随后的战略必须是**最优反应**
- 接受者应满足**信号条件**：对M中的每一 m_j ，并在给定对 $p(t_i | m_j)$ 的推断的条件下，接收者的行动必须使接收者的**期望效用**最大化，

即
$$a^*(m_j) = \arg \max_{a_k \in A} \sum_{t_i \in T} p(t_i | m_j) u_R(m_j, a_k)$$

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- 发送者的选择发生于单决策结信息集上，发送者拥有完全信息，并且发送者只在博弈的开始时行动，因此信号发送者应满足：
- 对T中的每一 t_i ，在给定接收者战略 $a^*(m_j)$ 的条件下，发送者选择的信号 $m^*(t_i)$ 必须使发送者的效用最大化，即

$$m^*(t_i) \in \arg \max_{m_j \in M} u_s(t_i, m_j, a^*(m_j))$$

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- （3）在处于均衡路径上的信息集中，推断由贝叶斯法则以及参与者的均衡战略给出
- 给定发送者的战略 $m^*(t_i)$ ，用 T_j 表示选择发送信号 m_j 的类型 t_i 的集合，即 $T_j = \{t_i \mid m^*(t_i) = m_j\}$
- 如果 T_j 不是空集，则对应于信号 m_j 的信息集就处于均衡路径之上；否则，若任何类型都不选择 m_j ，则其对应的信息集处于均衡路径之外。

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的**Nash**均衡，需将精炼贝叶斯**Nash**均衡定义中的条件（1）~（4）施加到信号博弈之上

- （3）在处于**均衡路径上**的信息集中，推断由贝叶斯法则以及参与者的均衡战略给出
- 对处于均衡路径上的信号，接受者的推断满足**信号条件**：
- 对每一 m_j ，如果在 T_j 中存在 t_i 使得 $m^*(t_i) = m_j$ 则接收者在对应于 m_j 的信息集中所持有的推断必须决定于贝叶斯法则和发送者的战略：

$$p(t_i | m_j) = \frac{p(m_j | t_i) p(t_i)}{\sum_{t_k \in T_j} p(m_j | t_k) p(t_k)} \stackrel{\forall t_i \in T_j, p(m_j | t_i) = 1}{=} \frac{p(t_i)}{\sum_{t_k \in T_j} p(t_k)}$$

第二节：精炼贝叶斯的Nash均衡



❖ 为求解精炼贝叶斯的Nash均衡，需将精炼贝叶斯Nash均衡定义中的条件（1）~（4）施加到信号博弈之上

- （4）对处于均衡路径之外的信息集，推断由贝叶斯法则以及可能情况下的参与者的均衡战略决定

- 对M中某一 m_j ，如果在T中不存在 t_i 使得

$$m^*(t_i) = m_j \Rightarrow T_j = \emptyset$$

- 则接收者在对应于 m_j 的信息集中所持有的推断必须决定于贝叶斯法则和可能情况下发送者的均衡战略。

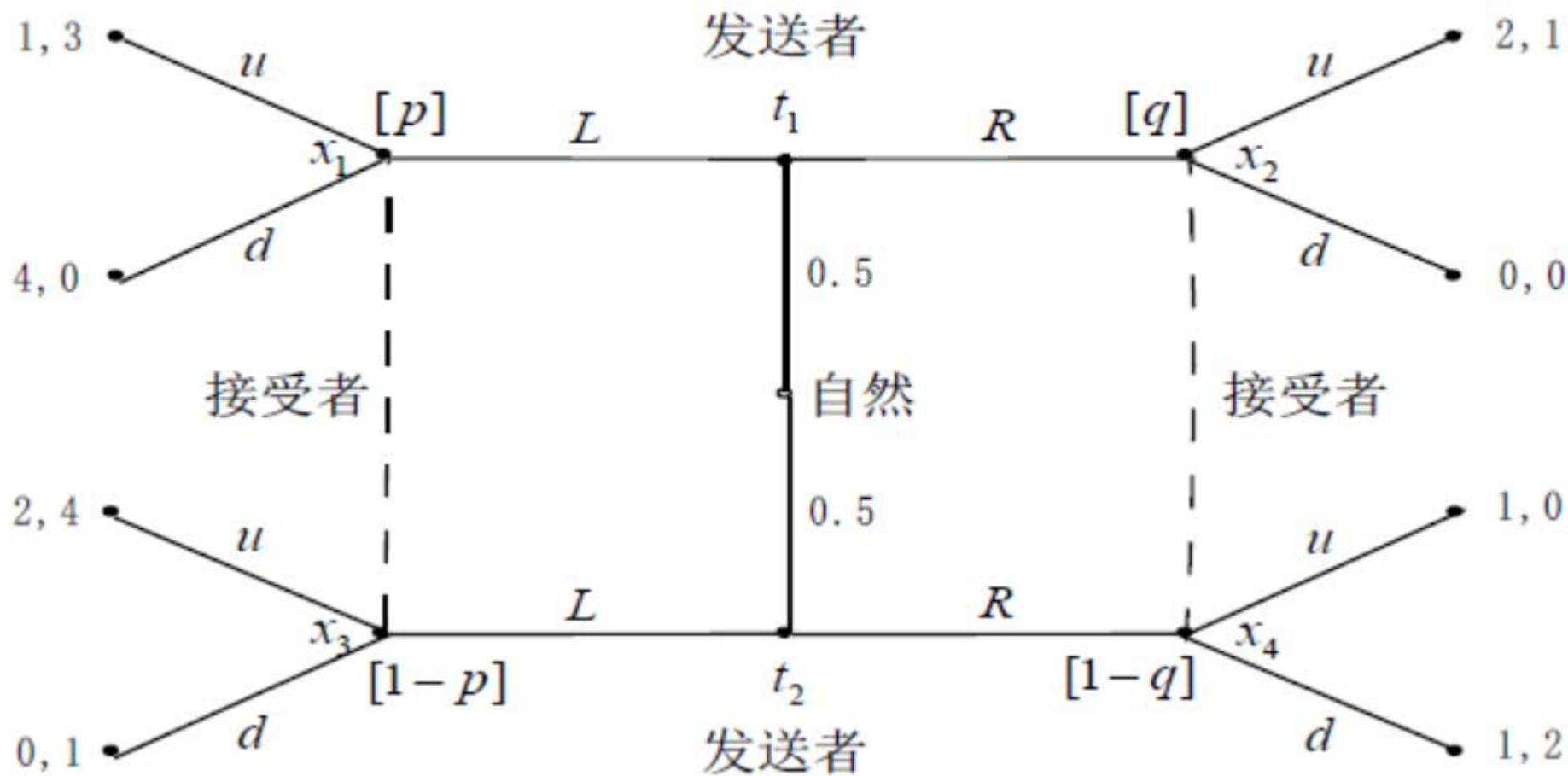
第二节：精炼贝叶斯的Nash均衡



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 例子



第二节：精炼贝叶斯的Nash均衡



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 发送者有4个纯战略，因此可能存在的纯战略精炼贝叶斯

Nash均衡有：

❖ (1)发送者的均衡战略为(L,L)；

❖ (2)发送者的均衡战略为(R,R)；

❖ (3)发送者的均衡战略为(L,R)；

❖ (4)发送者的均衡战略为(R,L)。

第二节：精炼贝叶斯的Nash均衡



- ❖ 假设存在一个混同于行动L的精炼贝叶斯Nash均衡，发送者的战略为(L,L)，则接收者对应于L的信息集 $I_R(\{x_1, x_3\})$ 处于均衡路径之上，于是接收者在这一信息集上的推断 $[p, 1-p]$ 决定于贝叶斯法则和发送者的战略，即

$$p = p(t_1 | L) = \frac{p(L | t_1) p(t_1)}{\sum_{i=1}^2 p(L | t_i) p(t_i)}$$

- ❖ 由于 $p(L | t_1) = p(L | t_2) = 1$ $p(t_1) = p(t_2) = 0.5$ 。 $p = 1 - p = 0.5$

与先验分布相同

第二节：精炼贝叶斯的Nash均衡



- ❖ 给定这样的推断，接收者在观测到信号**L**之后，根据行动**u**和**d**的期望收益，决定自己的选择。接收者选择**u**的期望收益为：
$$E_u = p * 3 + (1 - p) * 4 = 4 - p = 3.5$$
$$E_d = p * 0 + (1 - p) * 1 = 1 - p = 1.5$$
- ❖ 因此，接收者在观测到信号**L**之后的最优反应为选择**u**。此时，类型为**t1**和**t2**的发送者分别可得到的收益为**1**和**2**。
- ❖ 为了使两种类型的发送者都愿意选择**L**，即发送者的最优策略为**(L,L)**，需要确保：如果发送者选择信号**R**，接收者的反应(选择)给两种类型的发送者所带来的收益，小于它们选择信号**L**时的收益。

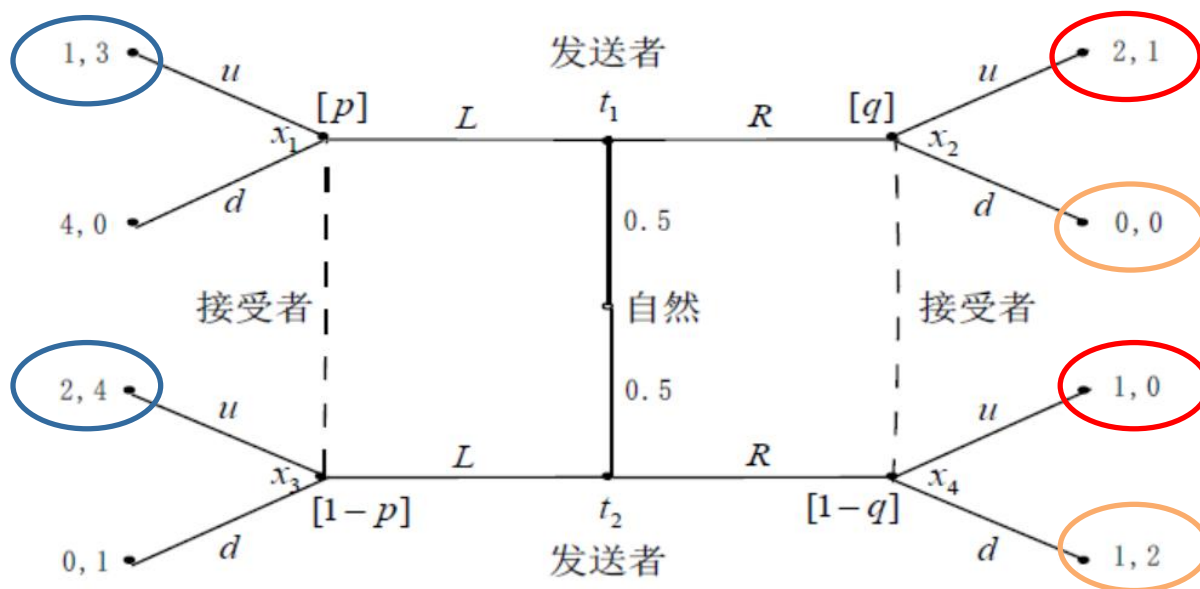
第二节：精炼贝叶斯的Nash均衡



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

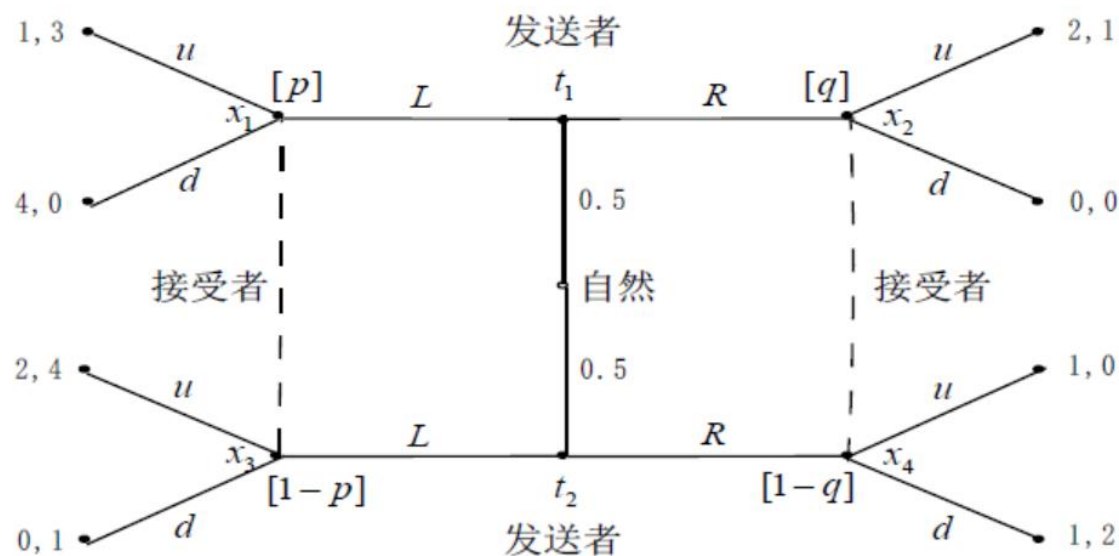
- ❖ (1) 如果接收者对R的反应为u，则类型为t1的发送者选择R的收益为2，高于自己选择L的收益1。此时，类型为t1的发送者不会选择L；
- ❖ (2) 如果接收者对R的反应为d，则通过选择R，类型为t1和t2的发送者的收益将分别为0和1，而他们选择L却可分别获得1和2。此时，类型为t1和t2的发送者都会选择L。



第二节：精炼贝叶斯的Nash均衡



- ❖ 因此，如果存在一个前面所假设的混同均衡，其中发送者的战略为(L,L)，则接收者对R的反应必须为d，于是接收者的战略必须为(u,d)。



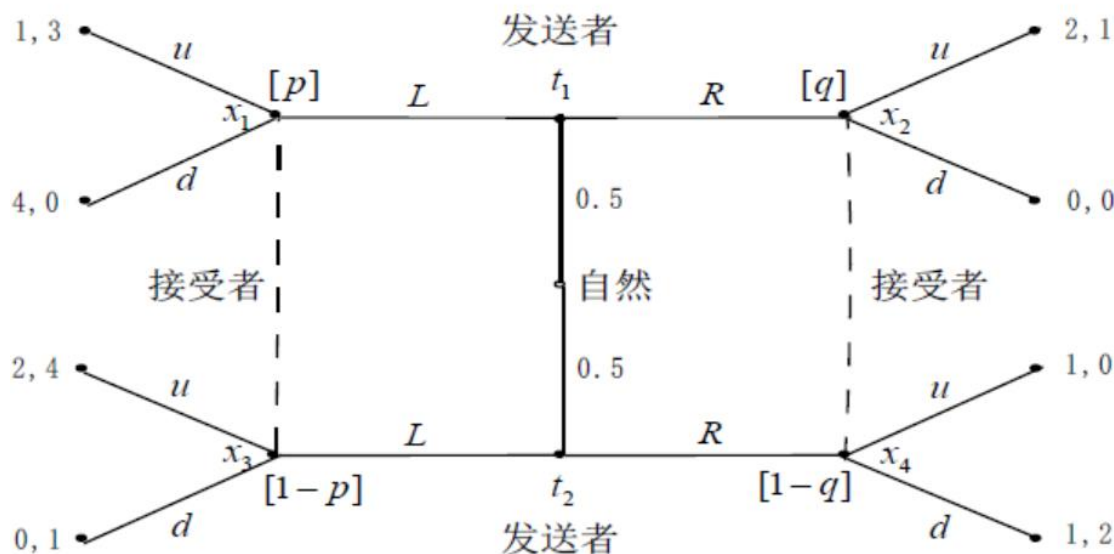
第二节：精炼贝叶斯的Nash均衡



- ❖ 此外，还需要考虑接收者在对应于**R**的信息集 $I_R(\{x_2, x_4\})$ 中的推断 $[q, 1-q]$ ，以及给定这一推断时选择**d**时是否最优的。在信息集 $I_R(\{x_2, x_4\})$ 上，接收者选择**u**和**d**的期望收益为：

$$E_u = q * 1 + (1 - p) * 0 = q$$

$$E_d = q * 0 + (1 - p) * 2 = 2 - 2q$$



第二节：精炼贝叶斯的Nash均衡



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 由于接收者在信息集 $I_S(\{x_2, x_4\})$ 上的最优反应为 d ，因此， $E[d] \geq E[u]$ ，所以

$$q \leq \frac{2}{3}$$

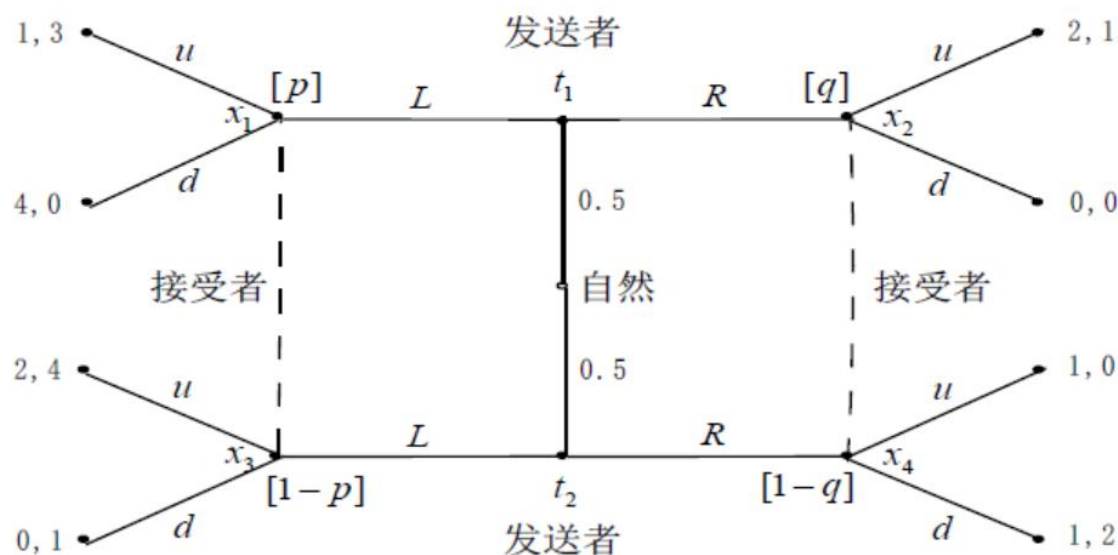
- 此时，得到上述博弈的混同精炼贝叶斯Nash均衡为

$$((L, L), (u, d), p = 0.5, q \leq \frac{2}{3})$$

第二节：精炼贝叶斯的Nash均衡



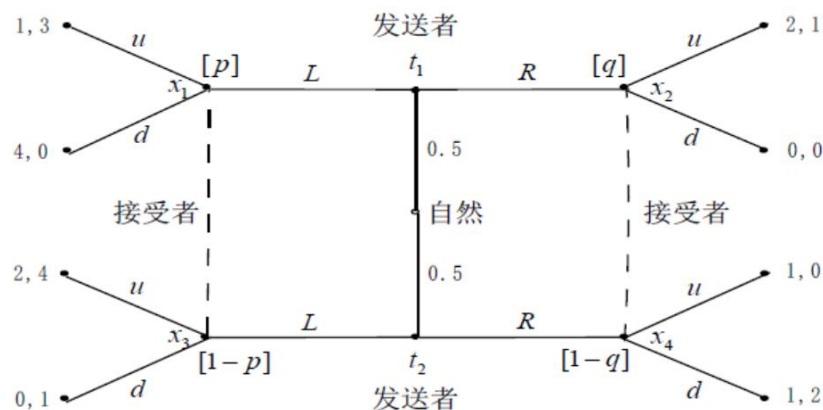
- ❖ 假设存在一个混同于行动R的精炼贝叶斯Nash均衡，发送者的战略为(R,R)，则 $q=0.5$ 。
- ❖ 接收者选择行动u和d的期望收益分别为0.5和1，所以接收者对R的最优反应为d。



第二节：精炼贝叶斯的Nash均衡



- ❖ 但是，如果类型为**t1**的发送者选择**L**，则无论接收者在信息集 $I_R(\{x_1, x_3\})$ 上的推断如何，接收者对**L**的最优反应都是**u**，这意味着类型为**t1**的发送者只要选择**L**，就确保可得到收益**1**，大于选择**R**的收益**0**。
- ❖ 因此，该博弈不存在发送者战略为**(R,R)**的混同精炼贝叶斯Nash均衡。



第二节：精炼贝叶斯的Nash均衡



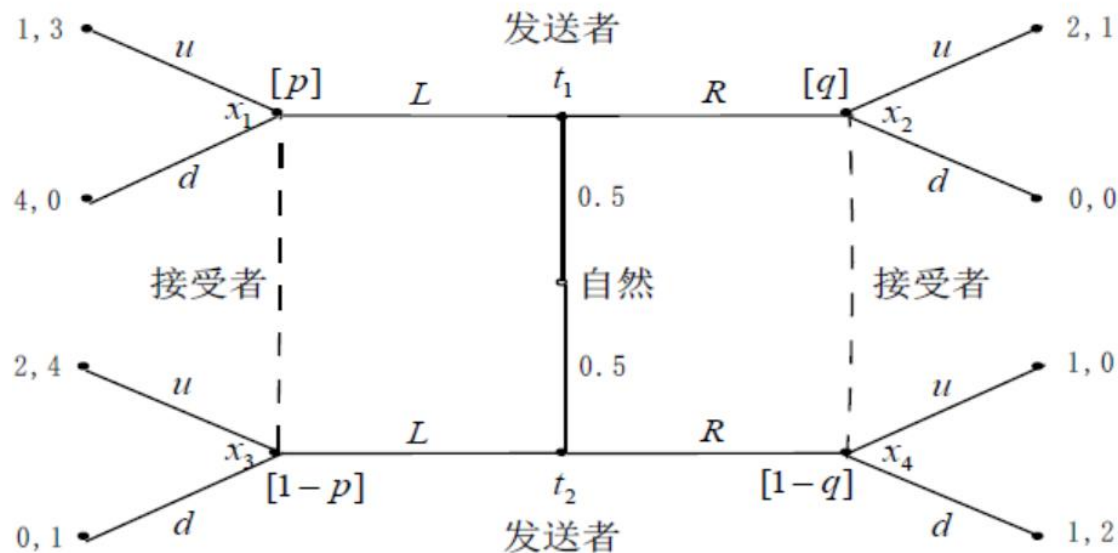
- ❖ 假设存在发送者的战略为(L,R)的分离均衡，则接收者的两个信息集 $I_R(\{x_1, x_3\})$ 和 $I_R(\{x_2, x_4\})$ 都处于均衡路径之上，于是两个推断都决定于贝叶斯法则和发送者的战略：

$$p=1, q=0.$$

$$p = p(t_1 | L) = \frac{p(L | t_1) p(t_1)}{\sum_{i=1}^2 p(L | t_i) p(t_i)}$$

$$p(L | t_1) = 1, \quad p(L | t_2) = 0$$

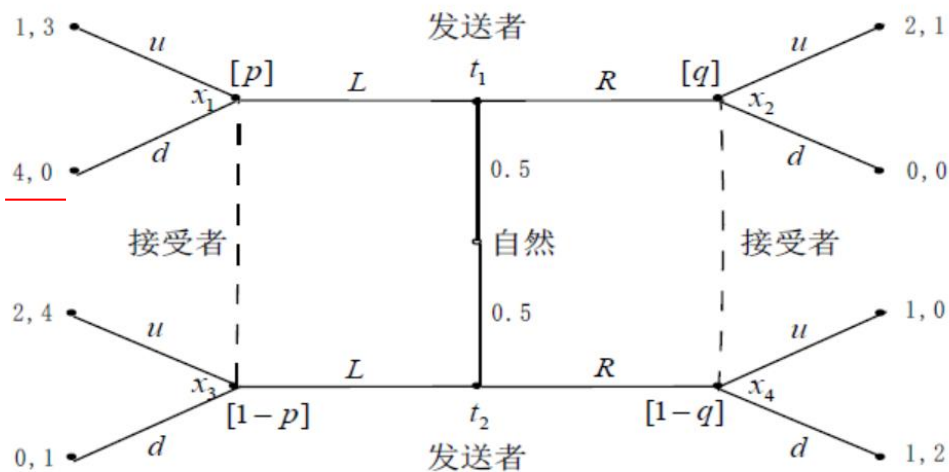
$$p(t_1) = p(t_2) = 0.5$$



第二节：精炼贝叶斯的Nash均衡



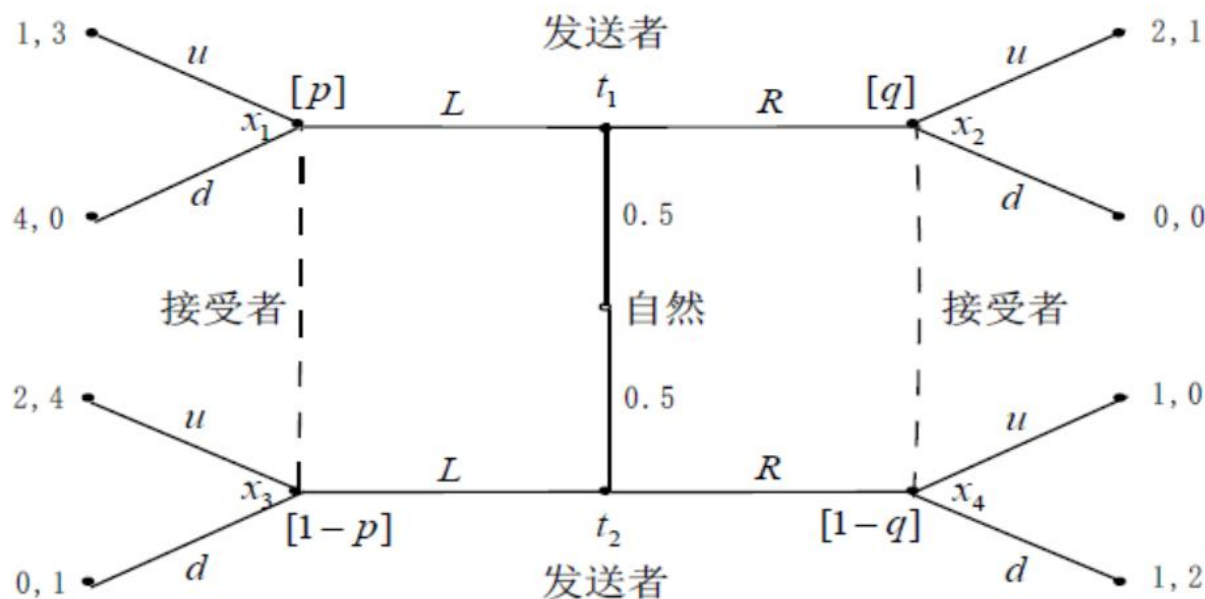
- ❖ 接收者在此推断下的最优反应分别为 u 和 d ，所以两种类型的发送者获得的收益都是 1 。此外，还需检验对给定的接收者战略(u, d)，发送者的战略是否是最优的。
- ❖ **t_1 类型下，接受者战略 u ，则发送者推断为 R 下的收益为 2 ，大于 1 ，发送者会选择 R**
因此，该博弈中不存在发送者战略为(L, R)的分离的精炼贝叶斯Nash均衡。



第二节：精炼贝叶斯的Nash均衡



- ❖ 假设存在发送者的战略为(R,L)的分离均衡，则接收者的推断必须为 $p=0, q=1$ ，于是接收者的最优反应为(u,u)，此时，两种类型的发送者都可得到2的收益。



第二节：精炼贝叶斯的Nash均衡



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

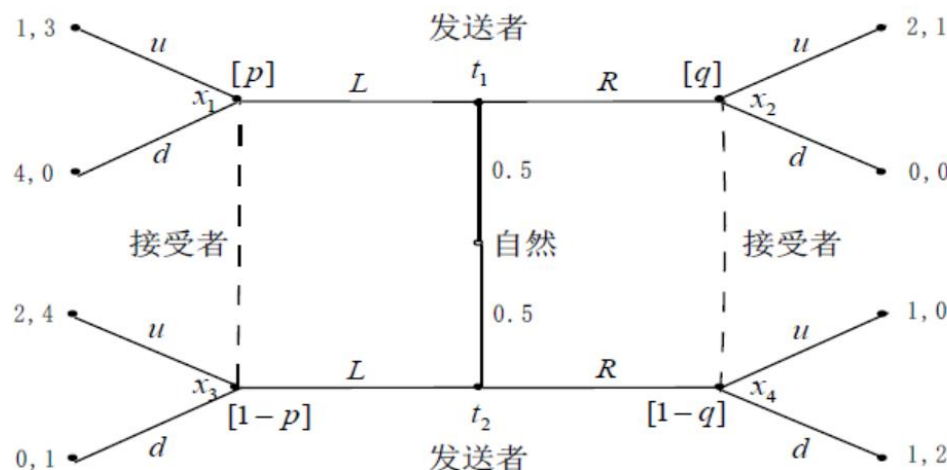
❖ 给定的接收者战略 (u,u) ，发送者是否会偏离战略 (R,L) 。

如果类型为 t_1 的发送者想偏离这一战略而选择 L ，则接收者的反应将会为 u ，则 t_1 的收益将减为 1 ，于是 t_1 没有任何动机偏离； t_2 类型下，给定接受者策略 u ，发送者选择 L 的收益为 2 ，大于 R 时的 1 ，发送者不想偏离 L

$((R,L), (u,u), p=0, q=1)$

为上述中博弈的分离精

炼贝叶斯Nash均衡



第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述

- 移动自组织网络是由无线链路连接的**移动节点**组成的自治分布式系统，不依靠固定通信网络基础设施，是没有任何中心实体、自组织、自愈的网络。网络节点能够动态地、随意地、频繁地进入和离开网络，而常常不需要事先示警或通知，而且不会破坏网络中其他节点的通信。移动节点兼具**主机和路由器**的功能。

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述——移动自组织网络特点

- 具备移动通信网络和计算机网络的特点
- 网络拓扑动态变化
- 无中心网络的自组性
- 多跳组网方式
- 有限的无线传输带宽(根据网络的不同)
- 移动终端的自主性
- 安全性差
- 网络的可扩展性不强

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述

- 自组网中的节点被攻占后成为恶意节点，恶意节点可以通过创建新的路由消息、发布不存在的链接和提供不正确的链路状态信息，给系统造成拜占庭式故障。

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 拜占庭将军问题

- 几个师包围着敌人的一座城市。每一个师都由它自己的司令统帅，司令之间只能通过报信者互相通信。他们必须统一行动。某一位或几位司令可能是叛徒，企图破坏忠诚的司令们的统一行动。
- 司令们必须有一个算法，使所有忠诚的司令能够达成一致，即使有少数几个叛徒也不能使忠诚的司令们做出错误的计划。
- 拜占庭将军问题：目标在于让爱国的将军达成一致，而不是找叛国的将军。

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述

- 攻击者的目的是从某个攻击节点发送恶意消息，意图攻击目标节点。当恶意消息到达目标机器而未被主机IDS检测到时，就认为入侵成功。我们认为，当可能的入侵者发送的消息被拦截时，主机IDS可以确定地说该消息本质上是恶意的，从而检测到入侵并阻止入侵节点。

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

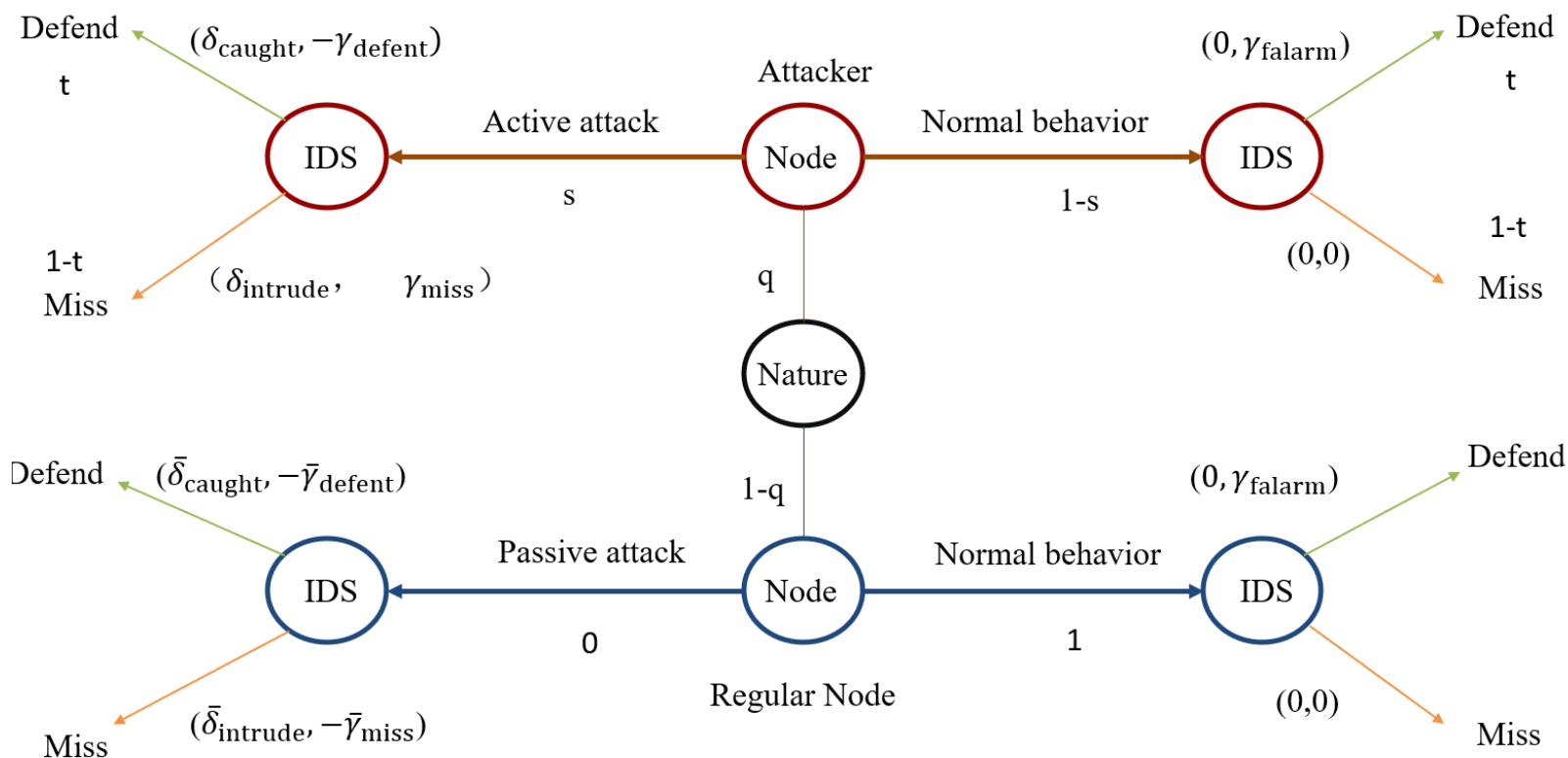
❖ 博弈模型

- 节点为信号发送者，入侵检测系统（IDS）为信号接收者。
- 节点共有两种状态：恶意节点、普通节点。恶意节点的决策是在显示恶意行为和显示正常行为之间做出选择。
- 入侵检测系统的两种行为：发出警报、什么都不做

第三节：移动自组网的入侵检测



❖ 博弈模型



第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 博弈模型的时间顺序

- 1. 自然决定节点的状态 θ ，它可能为恶意节点(**attacker**)可能为普通节点(**regular node**)，即 $\theta = \{attacker, regular\ node\}$ ，设节点为恶意节点的概率为 $p(attacker) = q$ ，则 $p(regular\ node) = 1 - q$

第三节：移动自组网的入侵检测



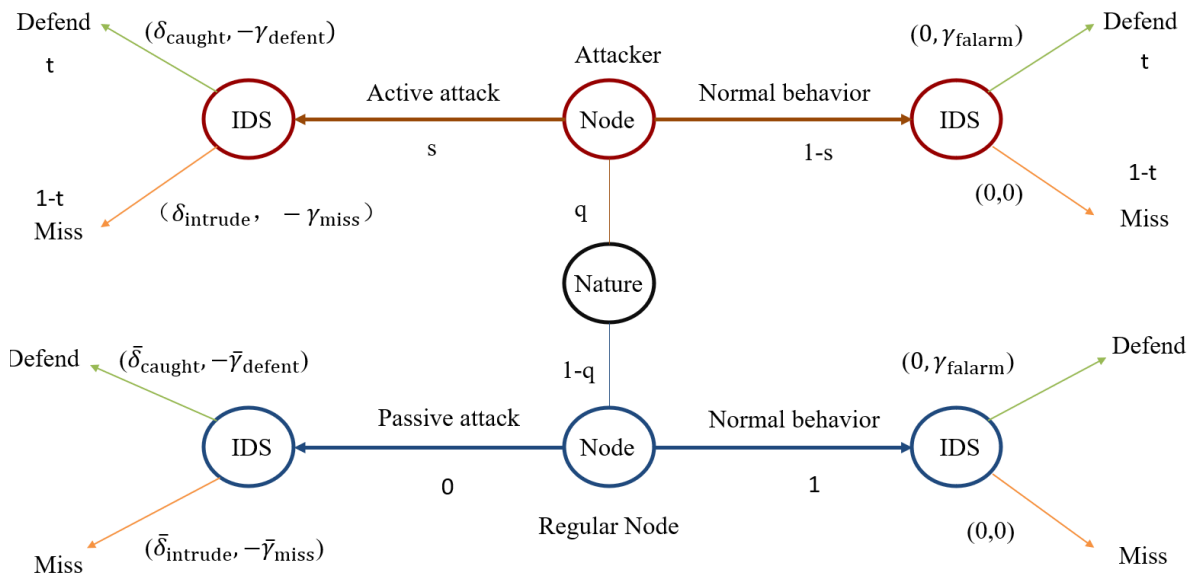
❖ 博弈模型的时间顺序

■ 2.节点明确自己的状态，并随后选择一个行动

- 攻击节点：恶意攻击(*active attack*)、正常行为(*nomal behavior*)

$p(\text{active attack}) = s$, 则 $p(\text{nomal behavior}) = 1 - s$

- 正常节点：正常行为(*nomal behavior*), $p(\text{nomal behavior}) = 1$



第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 博弈模型的时间顺序

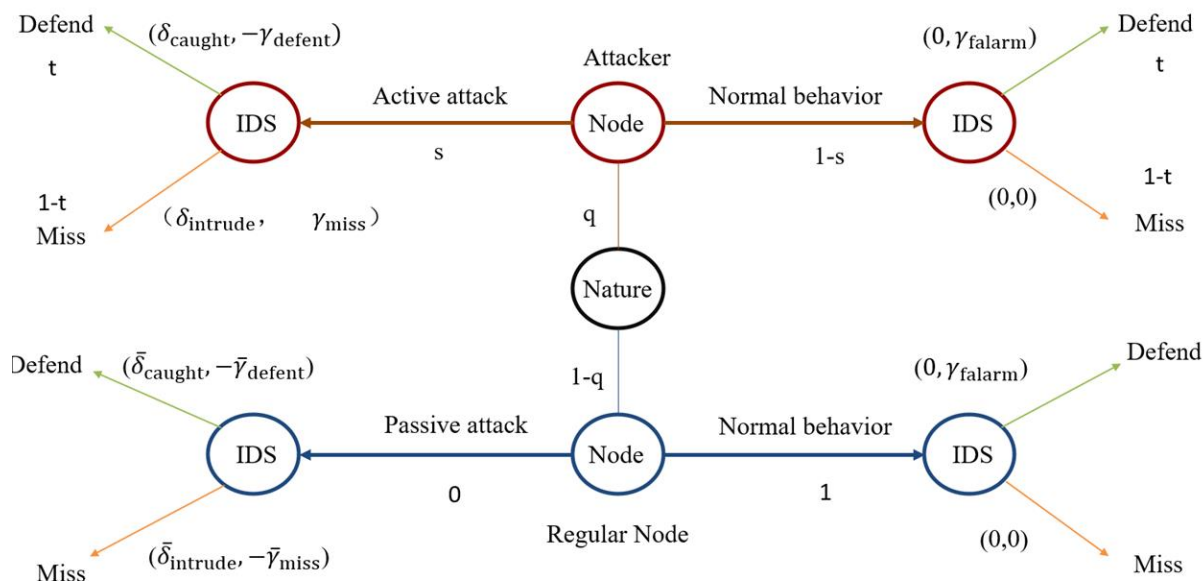
- 3.IDS观测到节点的行为，并根据节点行为选择自己是否进行防御
- 4.IDS收益
 - 成功检测一次入侵的收益为 $-\gamma_{defent}$
 - 没有采取行动错过一次入侵的损失为 γ_{miss}
 - 对正常节点采取了行动但错误预报损失为 γ_{falarm}
- 5.节点收益
 - 成功攻击的收益为 $-\delta_{intrude}$
 - 被防御到的损失为 δ_{caught}

第三节：移动自组网的入侵检测



收益

- IDS的期望收益 $st(-\gamma_{defent}) + s(1-t)\gamma_{miss} + (1-s)t\gamma_{falarm}$

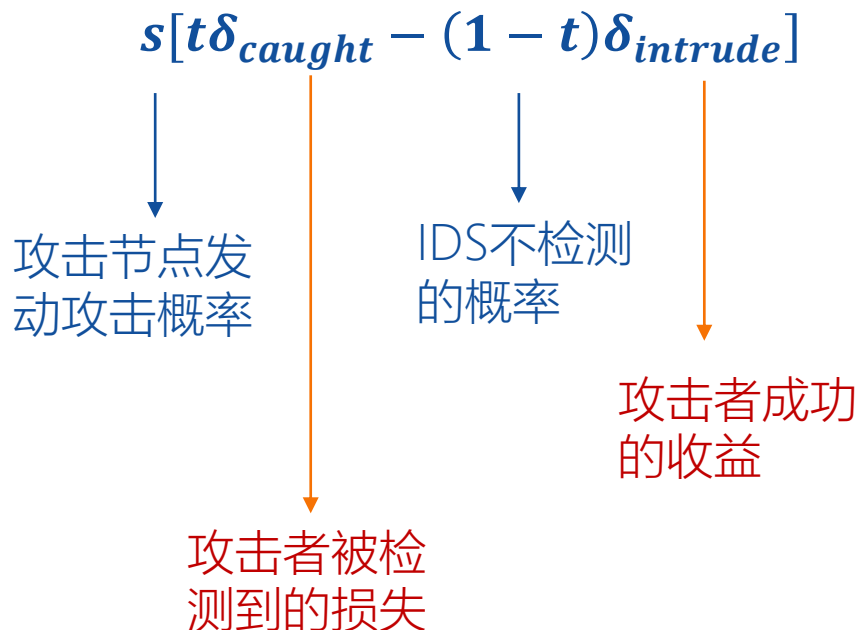


第三节：移动自组网的入侵检测



❖ 收益

■ 攻击者的期望收益



第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 均衡

- 从IDS的角度：对于节点的类型 θ 以正概率执行 a_1 行为，IDS计算 a_1 来自于某种类型 θ 的后验概率评估；根据Nash均衡，对于节点以状态 θ 执行的所有 a_1 行为，IDS的每个响应 a_2 应该是对给定的使用贝叶斯规则计算的信念的最佳响应。

第三节：移动自组网的入侵检测



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 均衡

- 从节点角度：给定IDS的策略，计算节点每种状态下的效用函数，调整节点的行为 a_1 的概率以使期望收益可以最大化

$$\forall \theta, \sigma_1^*(\cdot | \theta) \in \arg \max_{\alpha_1} u_1(\alpha_1, \sigma_2^*, \theta)$$

状态 θ 下的策略概率分布 收益函数

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述

- 在攻击发生前对可能的攻击目标、危害、时空特性等进行分析 and 预测，进而实施主动防御
- 基于博弈模型的网络安全研究中，构建博弈模型时需要面对 **2** 个关键问题：**博弈信息限制**和**博弈行动顺序**。

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题描述

- 完全信息假设在现实网络攻防中很难满足，降低了研究成果的价值和实用性。为解决攻防博弈中双方**信息受限**的问题，利用不完全信息博弈对信息战中参战双方的行为进行建模
- 如何在**非完全信息条件**和**攻防双方动态对抗**的情况下，构建攻防行为分析模型，对**主动防御方式**进行分析和研究是个十分复杂的问题

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 问题分析

- 从分析网络攻防过程出发，防御者**主动释放的信息**或防御行为被动泄露的各种信息都是攻击者重要的决策依据，这些信息即是防御者发出的**信号**，防御信号能够影响攻击者的行为，进而改变攻防双方的收益
- 从网络攻防的一般过程出发，防御者往往是**信号发送者**，而攻击者是**信号接收者**，并使用收到的信号对**防御者的类型**进行分析和判定，进而决定是否攻击、采取何种攻击方式。

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 策略收益量化

- 攻击者和防御者的策略收益量化是最优防御策略选取的**基础**，其量化是否合理直接影响防御策略选取结果。
- 系统损失代价（**Dcost, damage cost**）、攻击致命度（**AL, attack lethality**）、攻击成本（**AC, attack cost**）、防御成本（**Decost, defense cost**）。一般可将系统损失代价**Dcost** 作为攻击者的所得。

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 策略收益量化

- **伪装成本**（**CC, camouflage cost**）。伪装是指防御者释放与自身**真实防御等级不相符的信号**，用以达到欺骗攻击者的目的。伪装的代价称为伪装成本，通过不同等级防御行动所包含的防御措施的差异之和对伪装成本进行度量。
- 防御行动是**各项防御措施**的集合。低等级的防御者要想伪装较高等级，则需要伪装出高等级防御行动中的措施或者这些措施的结果。根据防御措施所防御的攻击行动**权限的不同**，可将伪装成本分为**3**个级别。



❖ 策略收益量化

■ 伪装成本分为3个级别

- **CL1**：低等级的防御行动、较高等级的防御行动缺少用于阻止 **Probe** 权限攻击的防御措施，则防御伪装成本可设为 **1~50**。
- **CL2**：低等级的防御行动、较高等级的防御行动缺少用于阻止 **User** 权限攻击的防御措施，则防御伪装成本可设为 **50~100**。
- **CL3**：低等级的防御行动、较高等级的防御行动缺少用于阻止 **Root** 权限攻击的防御措施，则防御伪装成本可设为 **100~200**。

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防信号博弈模型

- 网络攻防信号博弈模型是一个七元组 $ADSGM =$

$$(N, T, M, B, P_A, P, U)$$

- $N = (N_D, N_A)$ 是信号博弈的参与者空间，其中 N_A 为信号接收者， N_D 为信号发送者
- $T = \{T_D, T_A\}$ 是博弈者的类型空间，防御者类型由采取的防御行动所决定，是防御者的私人信息， $T_D = \{t_1, t_2, \dots, t_n\}$ 表示防御者的类型集合， $T_A = \{t\}$ 表示攻击者的类型集合

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防信号博弈模型

- 网络攻防信号博弈模型是一个七元组 $ADSGM = (N, T, M, B, P_A, P, U)$
 - M 为防御者的信号空间。 $M = (m_1, m_2, \dots, m_n)$ ，信号名称与防御者的类型相对应，防御者可自主选择发送的信号。由于伪装行为的存在，防御者发送的信号和其实际类型不一定完全一致
 - $B = (D, A)$ 是行动空间。 $D = \{d_1, d_2, \dots, d_g\}$ ， $A = \{a_1, a_2, \dots, a_h\}$ 表示防御者、攻击者的行动集合，双方的行动策略数均大于1

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防信号博弈模型

- 网络攻防信号博弈模型是一个七元组 $ADSGM = (N, T, M, B, P_A, P, U)$
 - P_A 是攻击者的先验信念集合。 $P_A = (p_1, p_2, \dots, p_n)$ 表示攻击者对防御者类型 t_j 的初始判断
 - \tilde{P} 是攻击者的后验信念集合。后验信念 $\tilde{P}(t_j | m_l) = (\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_n)$ 为攻击者观察到信号 m_l 后，使用贝叶斯法则调整后对防御者类型 t_j 的判断
 - $U = (U_D, U_A)$ 是收益集合表示参与者的博弈收益，由所有参与者的策略共同决定。

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防信号博弈模型

■ 攻击者在博弈中的收益期望

$$U_A(m_l, A_i, t_j) = \sum_e Dcost_{ij}(a_e) - AC_{ij} \rightarrow \text{攻击成本}$$

系统损失代价

攻击策略 防御类型 攻击策略包含的原子攻击

■ 防御者的期望收益

$$U_D(m_l, A_i, t_j) = \sum_e Dcost_{ij}(a_e) - Decost_{ij} - CC \rightarrow \text{伪装成本}$$

防御成本

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 攻防信号博弈模型

- 由于同一等级防御策略的投入大致相同，因此，可以认为它们的防御效果基本一致，若某一防御等级下共有 m 个防御策略，假设防御者采用等概率 $\beta_k = \frac{1}{m}$ 选择自身防御等级下的第 k 个防御策略，可以求得防御者在该防御等级下的收益期望

$$U_D(t_j) = \sum_{k=1}^m \beta_k U_{D_k}(m_l, A_i, t_j)$$

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

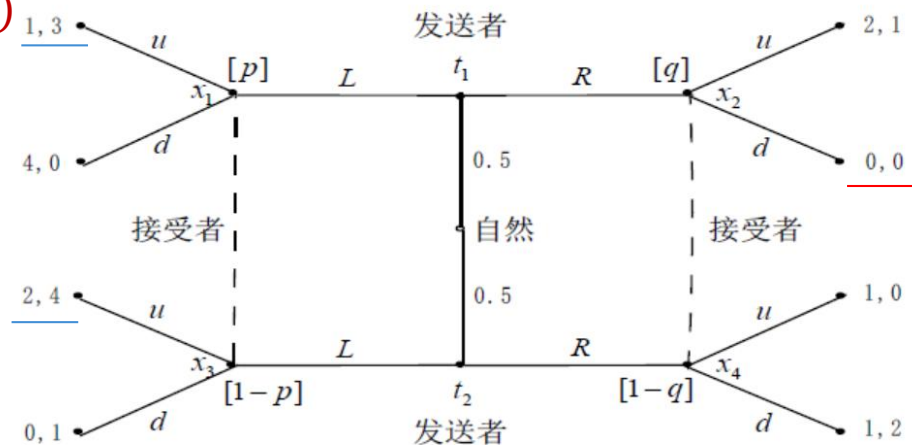
❖ 精炼贝叶斯求解

- 攻防信号博弈模型的精炼贝叶斯均衡由策略组合 $(m^*(t), a^*(m))$ 与后验信念 $\tilde{P}(t|m)$ 组成，并满足以下条件

- $a^*(m) \in \arg \max_{a \in A} \sum \tilde{p}(t|m) U_A(m, a, t)$ 表示在给定后验信念 $\tilde{P}(t|m)$ 后，攻击者针对防御者发出的信号所做出的最优行动

- $m^*(t) \in \arg \max_{m \in M} \sum U_D(m, a^*(m), t)$

$\tilde{P}(t|m)$ 是攻击者使用贝叶斯法则从先验概率 P_A 、观测信号 m ，和攻击者的最优策略 $a^*(m)$ 得到的



第四节：基于信号博弈模型的防御策略选取

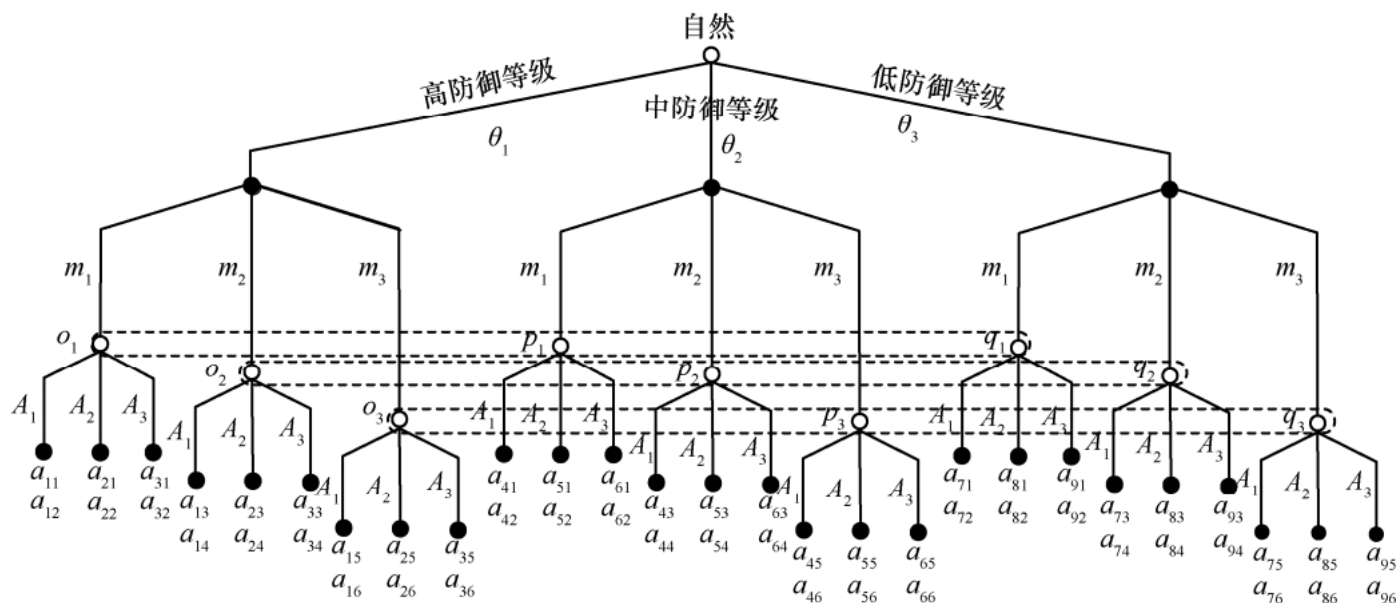


北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 实例

- 防御者类型 $T_D = (t_1, t_2, t_3) = (\text{高防御等级}, \text{中防御等级}, \text{低防御等级})$ ，
信号与防御者的类型相对应，即为 $M_D = (\text{高防御信号}, \text{中防御信号}, \text{低防御信号})$ ，
防御者收益为 $U_D(m, a, t)$



第四节：基于信号博弈模型的防御策略选取

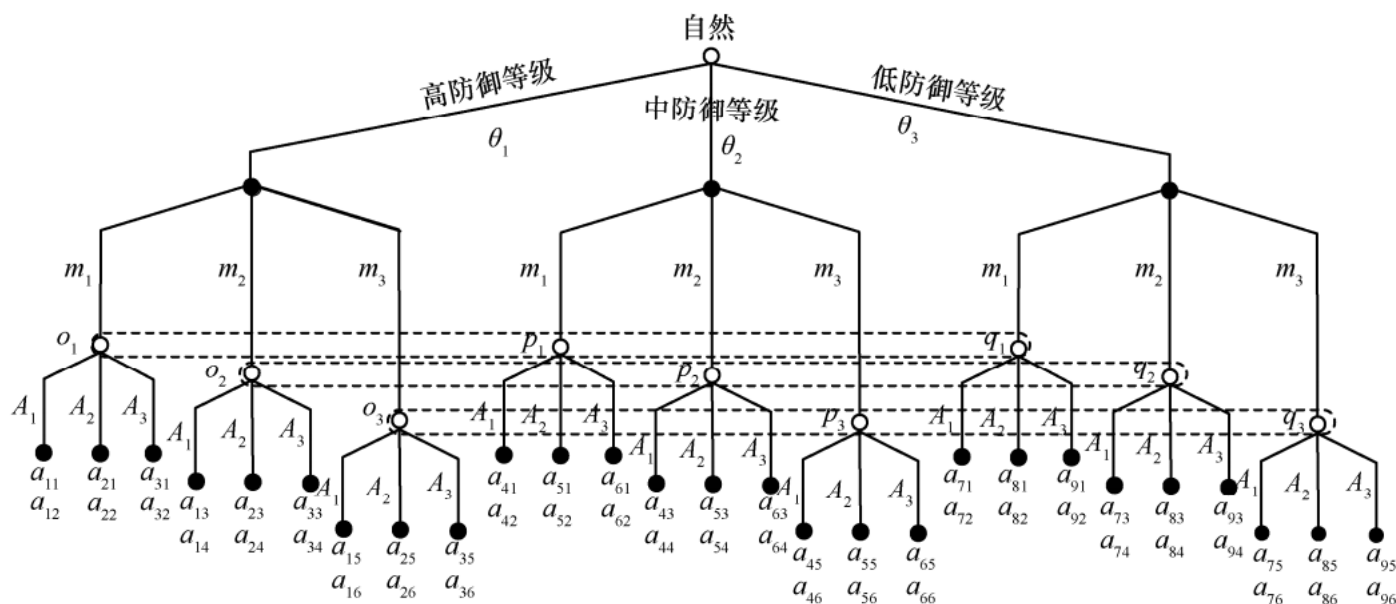


北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 实例

- 攻击者类型 $T_A = (t)$ ，行动空间(即其攻击策略)为 $A = (A_1, A_2, A_3)$ ，攻击者对防御者类型的先验信念为 P_A ，后验信念为 $\tilde{P}(t|m)$ ，收益为 $U_A(m, a, t)$



第四节：基于信号博弈模型的防御策略选取

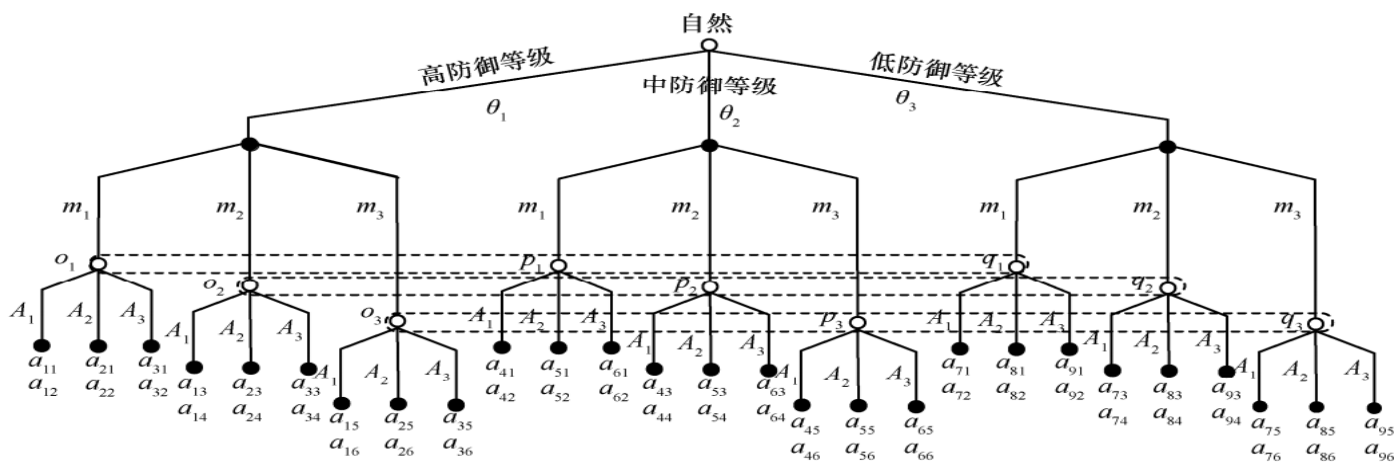


北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 实例

- 自然选择防御者类型，类型 t_1, t_2, t_3 的概率分别为 $\theta_1, \theta_2, \theta_3$ 。攻击者观察到 m_1, m_2, m_3 信号后，分别认为防御者类型 $\{t_1, t_2, t_3\}$ 的概率是 $\{o_1, o_2, o_3\}$ 、 $\{p_1, p_2, p_3\}$ 、 $\{q_1, q_2, q_3\}$ 。 (U_A, U_D) 表示双方博弈收益， a_{ij} 表示具体的收益值， $i = 1, 2, \dots, 9$ ， $j = 1, 2, \dots, 6$



第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 实例求解

- 1) 攻击者推断依存的子博弈精炼均衡策略

$$\max_{a \in A} \sum_{t_1, t_2, t_3} U_A(m_1, a, t) p(t|m_1)$$

- 2) 防御者推断的子博弈精炼均衡策略

$$\max_{m \in M} U_D(m, a^*(m), t)$$

- 3) 求解信号博弈的精炼贝叶斯均衡，已知 $m^*(t), a^*(m)$ ，求出满足贝叶斯法则的攻击者对防御者类型的推断 $\tilde{p}^* = \tilde{p}^*(t|m)$ ，如 $P(t|m)$ 与 $\tilde{P}(t|m)$ 不冲突，可得出信号博弈的精炼贝叶斯均衡策略 $\{m^*(t), a^*(m), \tilde{p}^*\}$

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 小结——最优防御策略选取算法

- 初始化 $ADSGM = (N, T, M, B, P, \tilde{P}, U_A)$;
- 构建防御者类型空间集合 $T_1 = \{t_i, 1 \leq i \leq n\}$;
- 构建防御者信号空间集合 $M = \{m_l, 1 \leq l \leq n\}$;
- 构建防御行动集合 $D = \{d_j, 1 \leq j \leq m\}$;
- 对防御者类型 $t_i \in T_1$ 及信号 $m_l \in M$, 有 $d_1 \in D$, $U_D(m_l, d_i, t_j) = \sum_e Dcost_{ij}(a_e) + Decost_{ij} + CC$;

第四节：基于信号博弈模型的防御策略选取



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

❖ 小结——最优防御策略选取算法

- 对攻击行为，有 $U_A(m_l, d_l, t_j) = \sum_e Dcost_{ij}(a_e) + AC_{ij}$;
- 建立先验概率推断 $P(t|m)$;
- 攻击者最优反应行动 $a^*(m) = \arg \max_{a \in A} \sum_{t \in T} U_A(m, a, t)p(t|m)$
- 防御者的最优策略 $m_p^*(t) = \arg \max_{m \in M} U_D(m, a(m), t)$;
- 求出满足贝叶斯法则的防御者类型的后验推断概率 $\tilde{P}(t|m)$;
- 如果 $P(t|m)$ 和 $\tilde{P}(t|m)$ 不冲突，求得精炼贝叶斯均衡 $\{d_p^*(m), m_p(t), \tilde{P}(t|m)\}$ 。

本章小结



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- ❖ 本章给出了**信号博弈**的基本定义：定义、特征、要素、具体描述、均衡类型
- ❖ 通过具体例子对所有可能的策略进行具体分析了解**信号博弈均衡求解**过程
- ❖ 通过网络安全实例：**移动自组网的入侵检测、基于信号博弈模型的防御策略选取**分析了信号博弈的基本内涵和主要思想