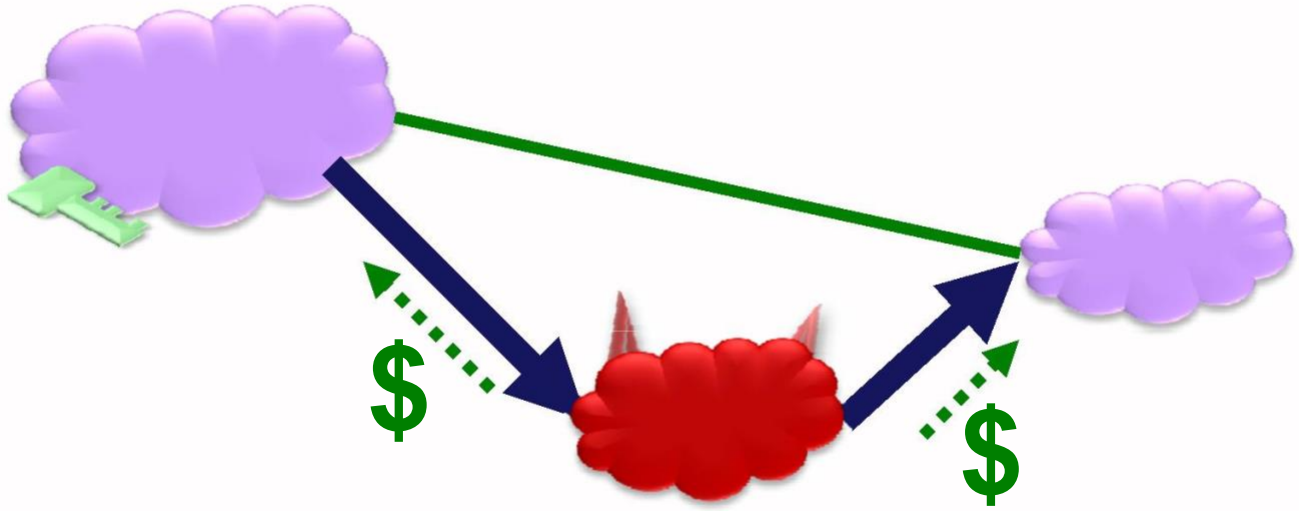
旧金山**NANOG 49**
2010年**6**月**15**日星期二

BGP安全协议有多安全？



Sharon Goldberg
微软研究院和波士顿大学

Michael Schapira
耶鲁大学&伯克利分校

Pete Hummon
AT&T研究

Jennifer Rexford
普林斯顿

概述（1）

“ BGP流量吸引攻击”可能会导致重大问题

- 前缀劫持导致黑洞，连接断开
- …例如巴基斯坦电信/ YouTube事件
- BGP“中间人”攻击
- …例如Pilosov和Kapela流量拦截演示

如果我们拥有“ BGP安全性”，这些问题将消失.....。对不对

- 不同的协议具有不同的属性。
- 哪种方法最有效地阻止攻击？
- 我们可以量化这一点吗？我们可以比较一下吗？

概述（2）

我们量化并比较主要的“ BGP安全性”
协议防止流量吸引攻击

- 原始身份验证（ROA / RPKI）ɣsoBGP
- 防御过滤（前缀列表）ɣ安全BGP

我们的方法：通过对**AS**拓扑数据进行仿真评估。

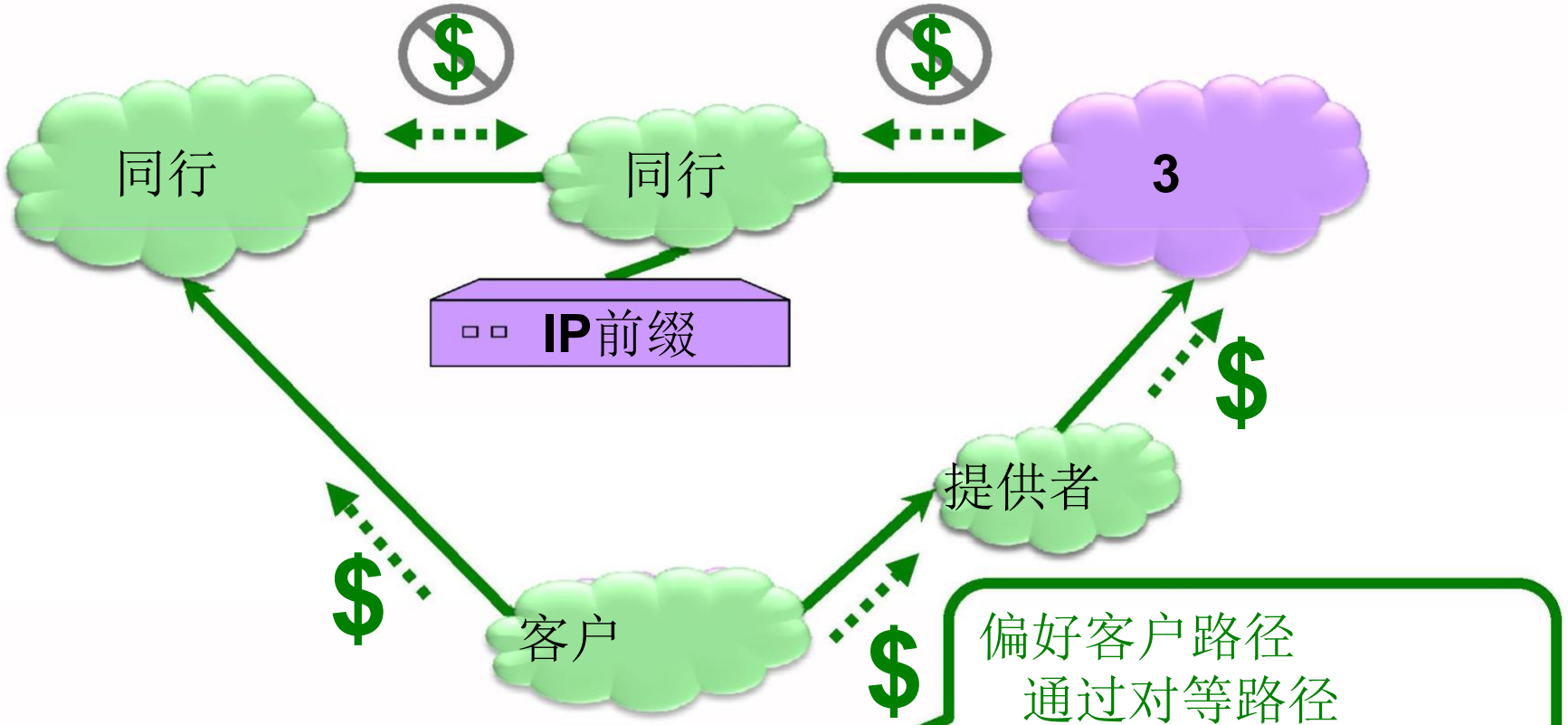
- 假设“ BGP安全”协议已完全部署。
- …攻击者可以吸引多少流量？
- 为了确定这一点，我们使用BGP路由策略模型
- …基于业务关系和AS路径长度
- 并针对[CAIDA]和[UCLA Cyclops]数据运行模拟
- …（AS级互联网与业务关系图）

BGP路由策略模型（一）

为了弄清攻击后流量的流向，

我们需要知道每个**AS**如何选择**BGP**中的路径

但是，我们不知道您如何做到这一点。因此，我们使用模型。



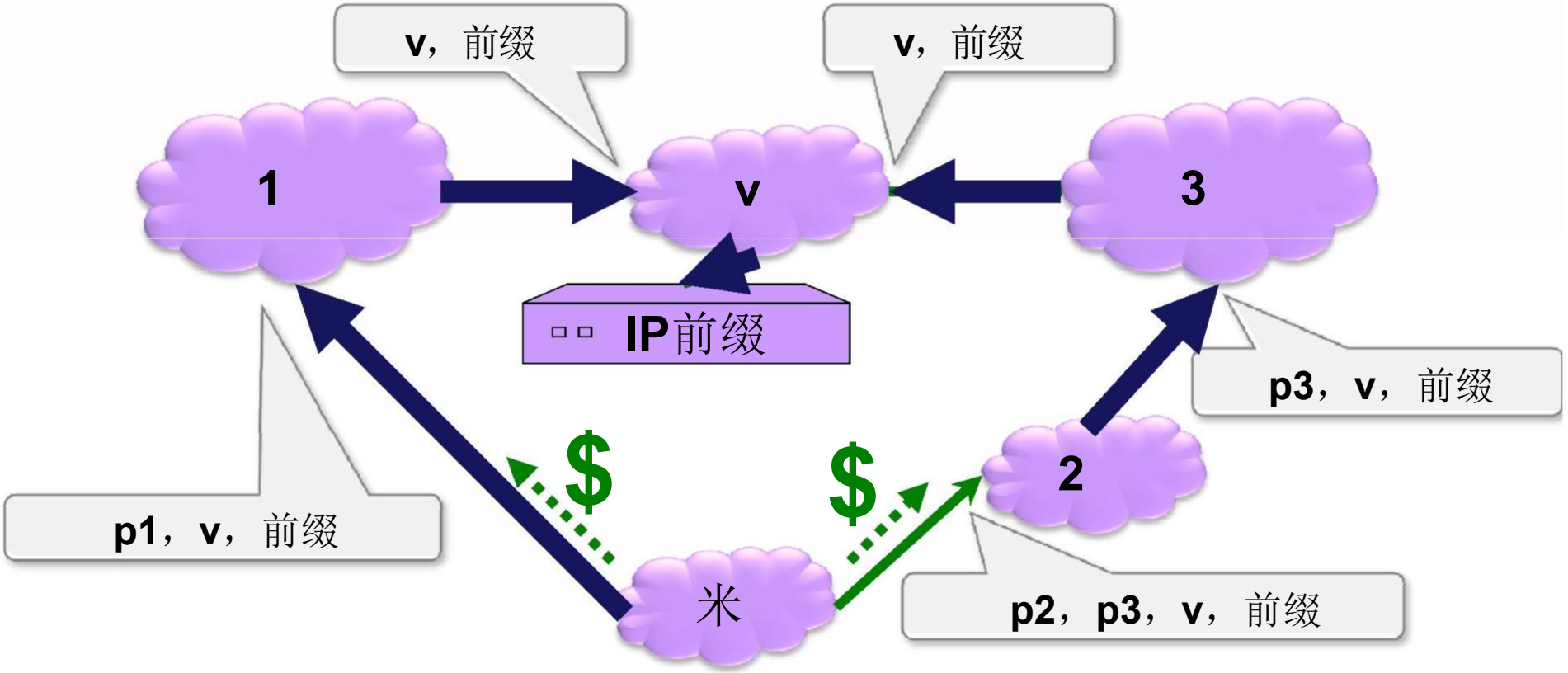
路由策略模型：

•首选便宜的路径。然后，选择较短的路径。

BGP路由策略模型（2）

为了弄清攻击后流量的流向，

我们需要知道每个**AS**如何选择**BGP**中的路径。



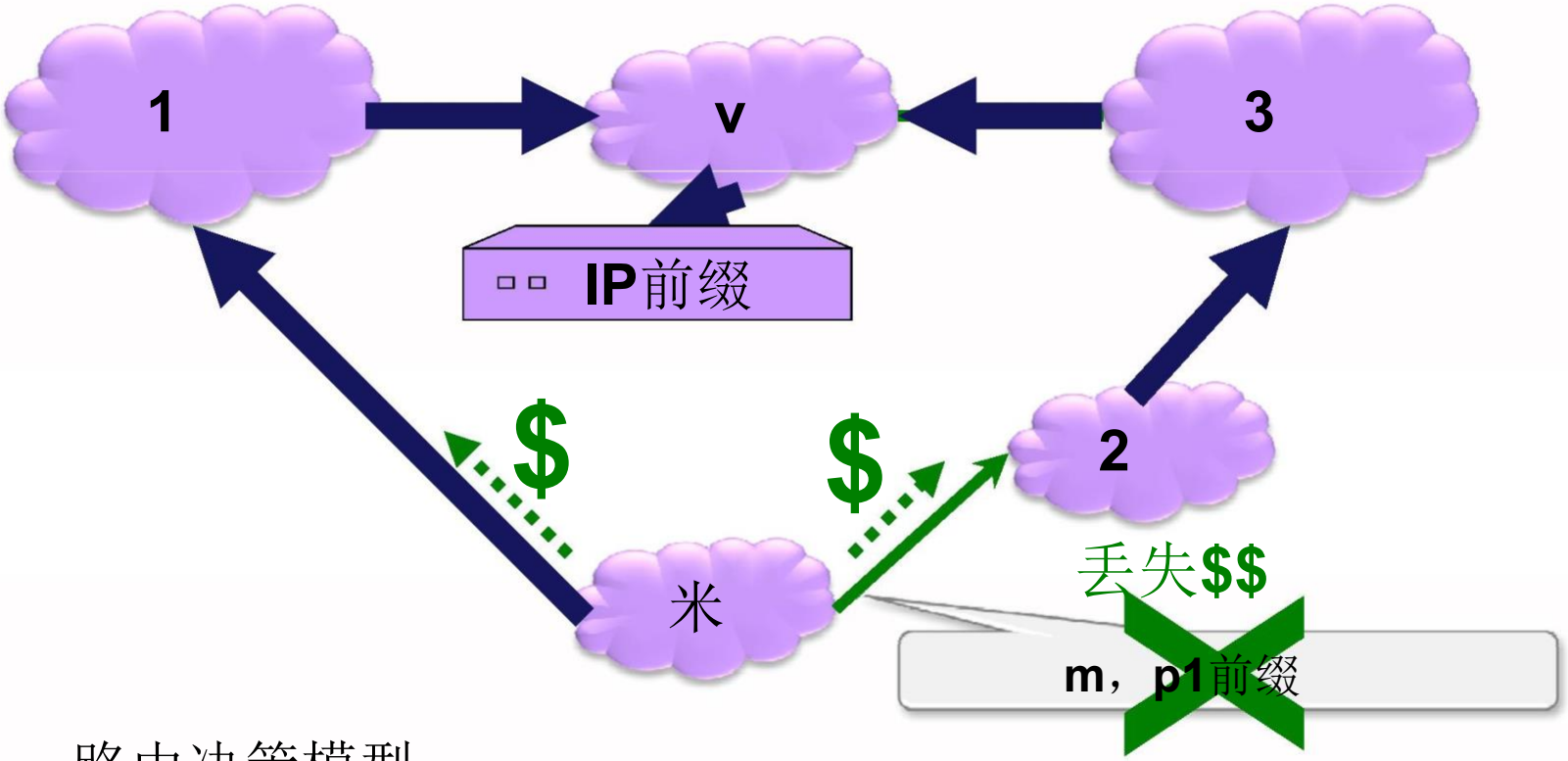
路由决策模型：

•首选便宜的路径。然后，选择较短的路径。

BGP路由策略模型（3）

为了弄清攻击后流量的流向，

我们需要知道每个**AS**如何选择**BGP**中的路径。



路由决策模型：

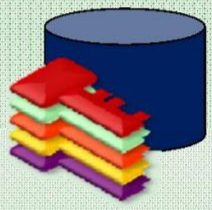
- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

这个演讲

第1部分：**BGP**路由策略模型

第2部分：安全路由协议和攻击

- **BGP**上的前缀劫持
- 原始身份验证攻击（**RPKI**）
- 使用安全**BGP**路由泄漏
- 插曲：找到最佳攻击
- 通过前缀列表过滤存根攻击



第3部分：仿真结果图

第4部分：结论和启示

我将从下面的一个“匿名”示例开始
CADIA的11/20/2009关联关系数据。

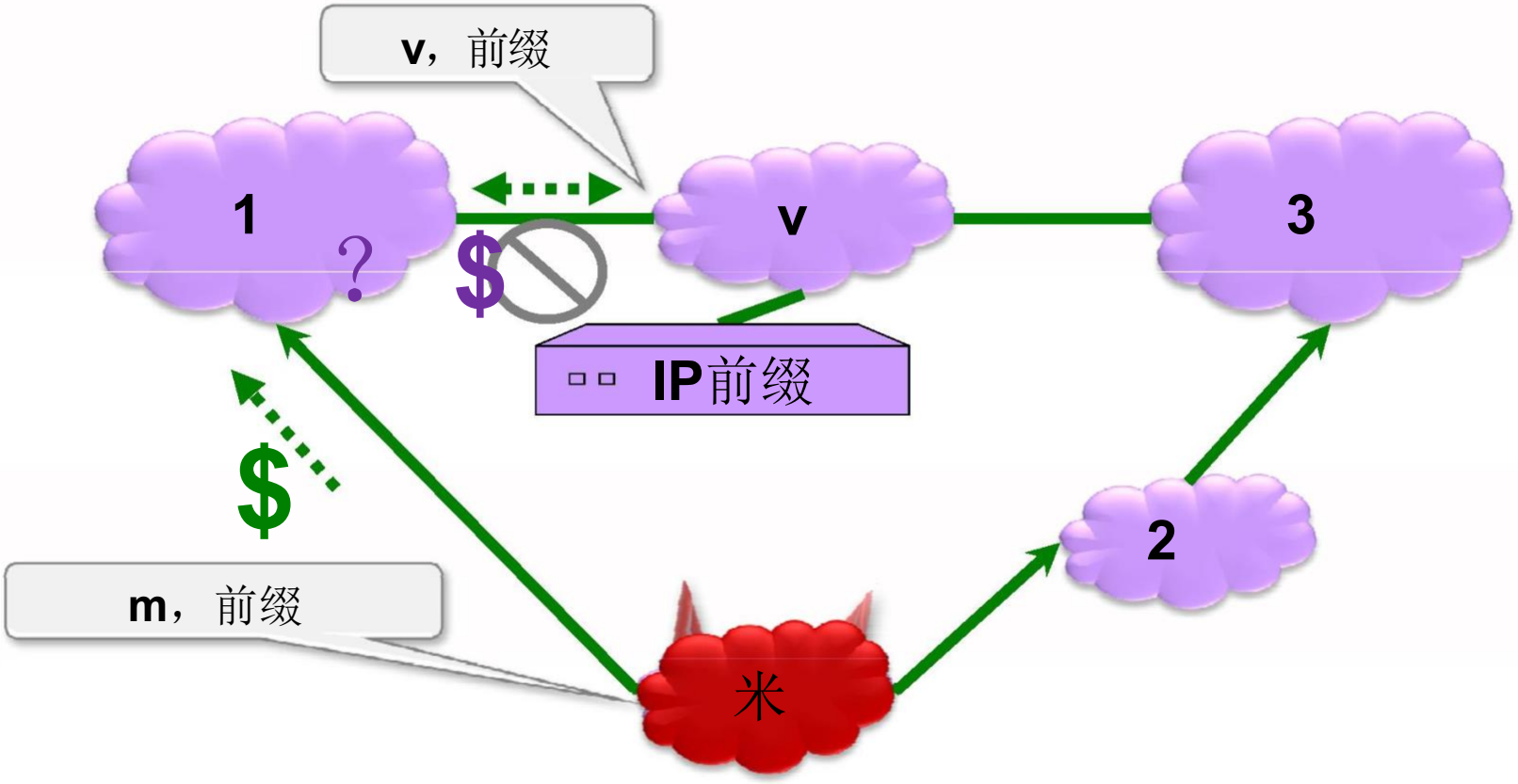
我将使用此示例介绍可能的
攻击每种“ **BGP**安全”协议

目前，我将有一名攻击者和一名受害者

稍后再考虑多个（攻击者，受害者）对

交通吸引攻击

攻击者想要通过其网络路由的最大数量的自治系统。
（用于窃听，丢弃，篡改.....）

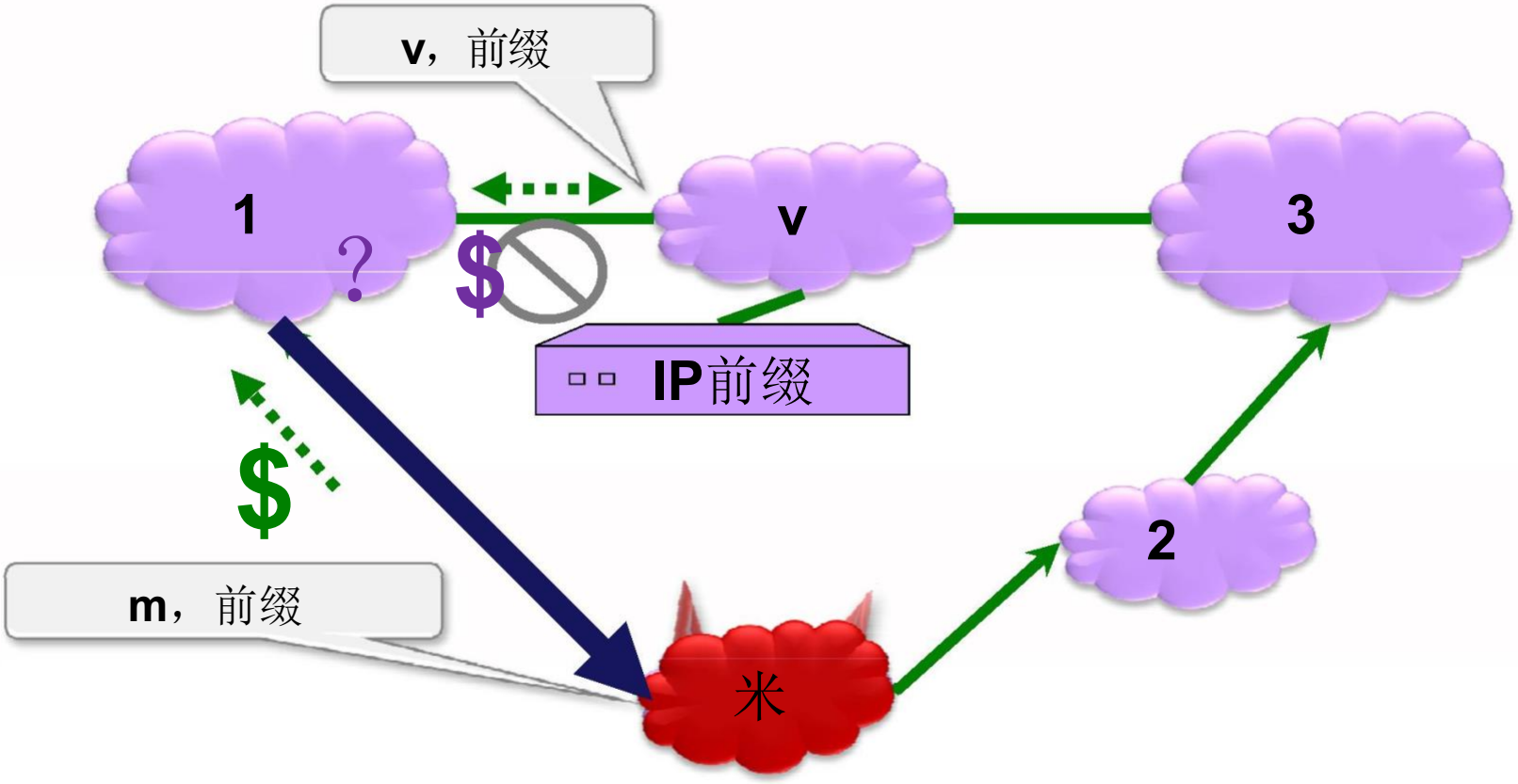


路由决策模型：

- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

交通吸引攻击

攻击者想要通过其网络路由的最大数量的自治系统。
（用于窃听，丢弃，篡改.....）

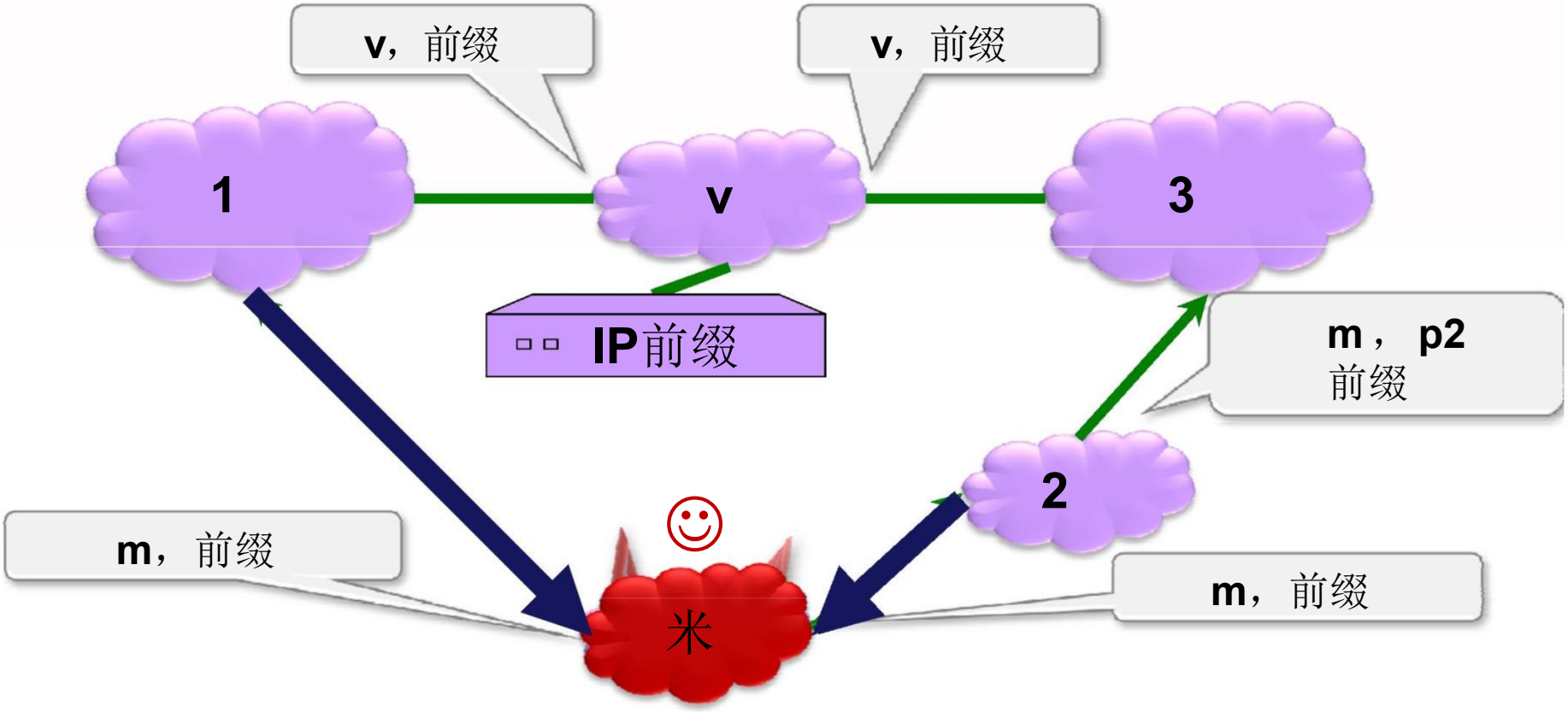


路由决策模型：

- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

交通吸引攻击

攻击者想要通过其网络路由的最大数量的自治系统。
（用于窃听，丢弃，篡改.....）

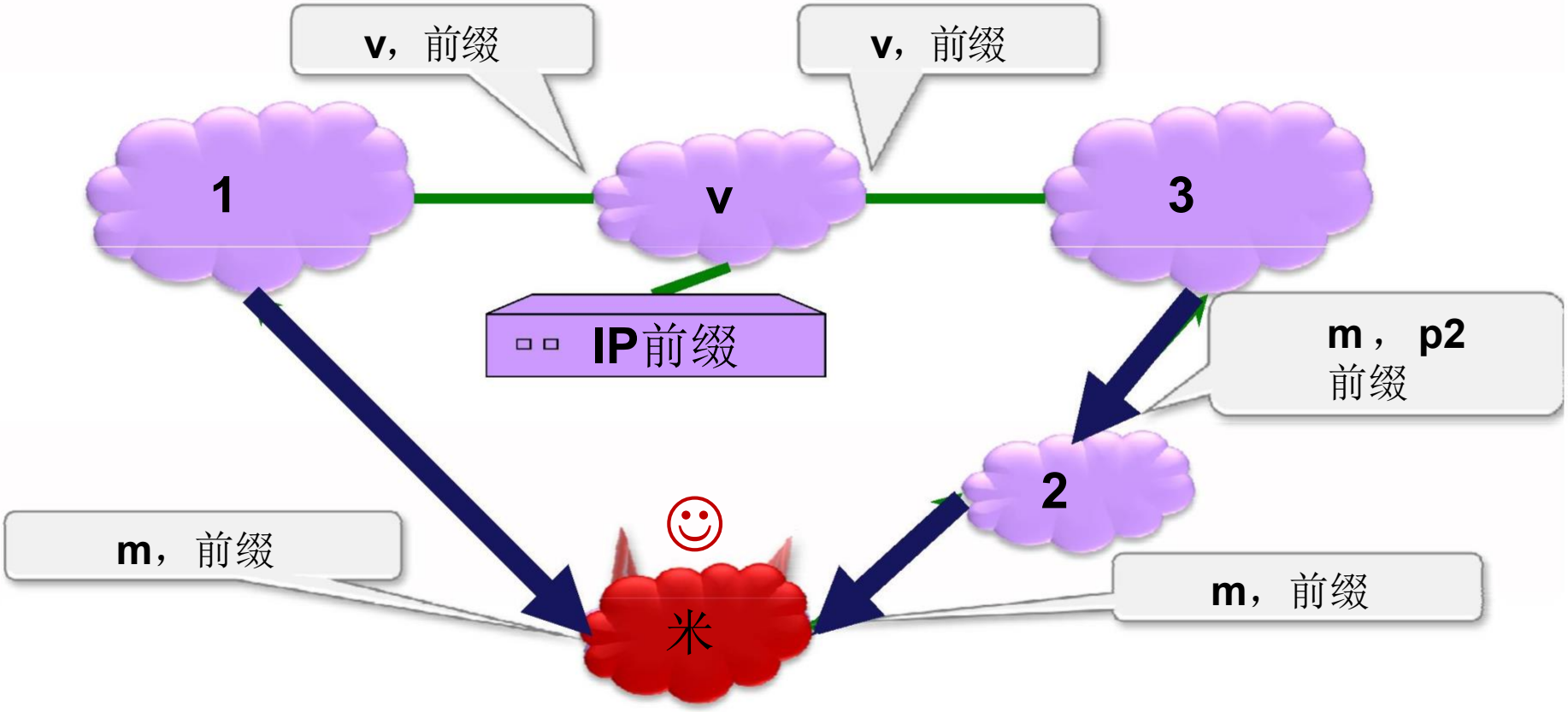


路由决策模型：

- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

交通吸引攻击

攻击者想要通过其网络路由的最大数量的自治系统。
（用于窃听，丢弃，篡改.....）

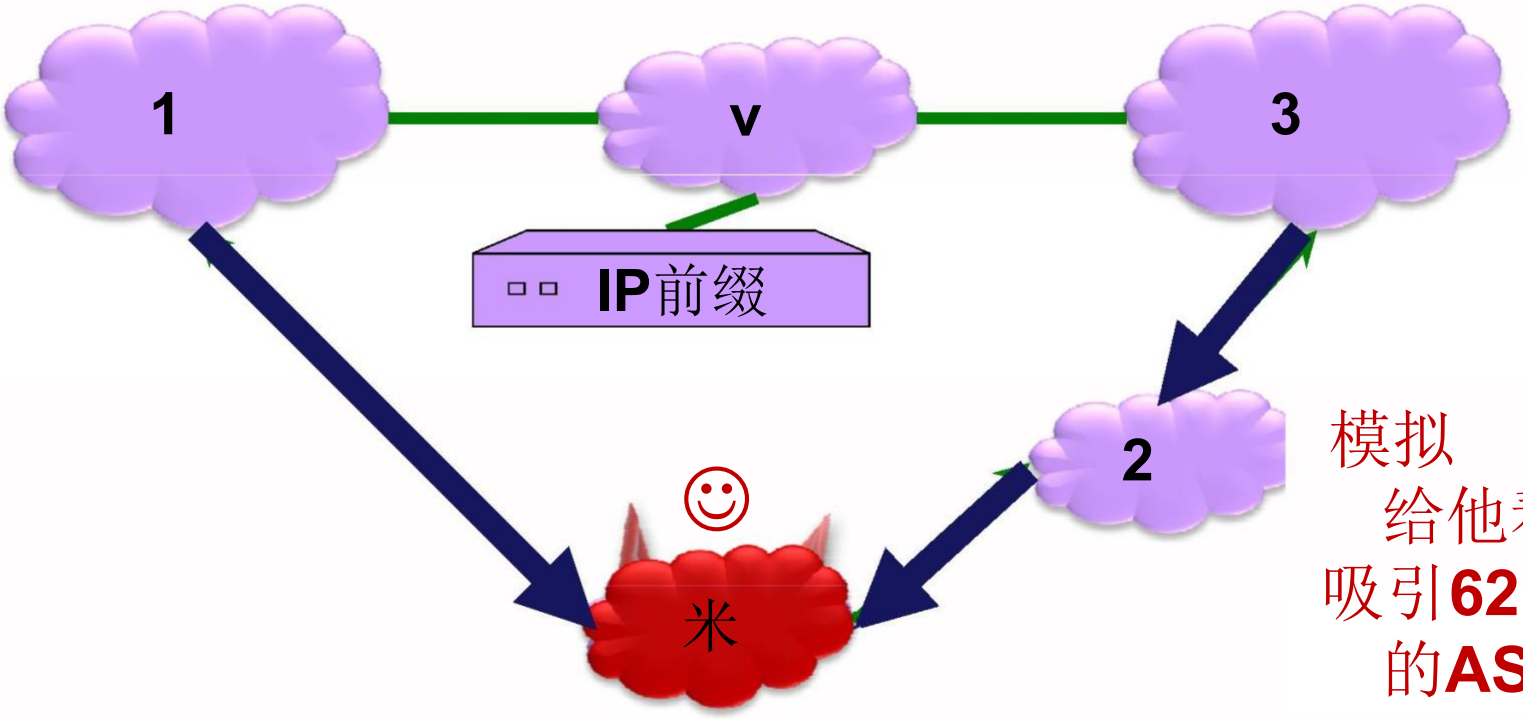


路由决策模型：

- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

交通吸引攻击

攻击者想要通过其网络路由的最大数量的自治系统。
（用于窃听，丢弃，篡改.....）



模拟
给他看
吸引62%
的ASes！

路由决策模型：

- 首选便宜的路径。然后，选择较短的路径。
- 仅在赚钱的情况下进行公交运输，即为客户。

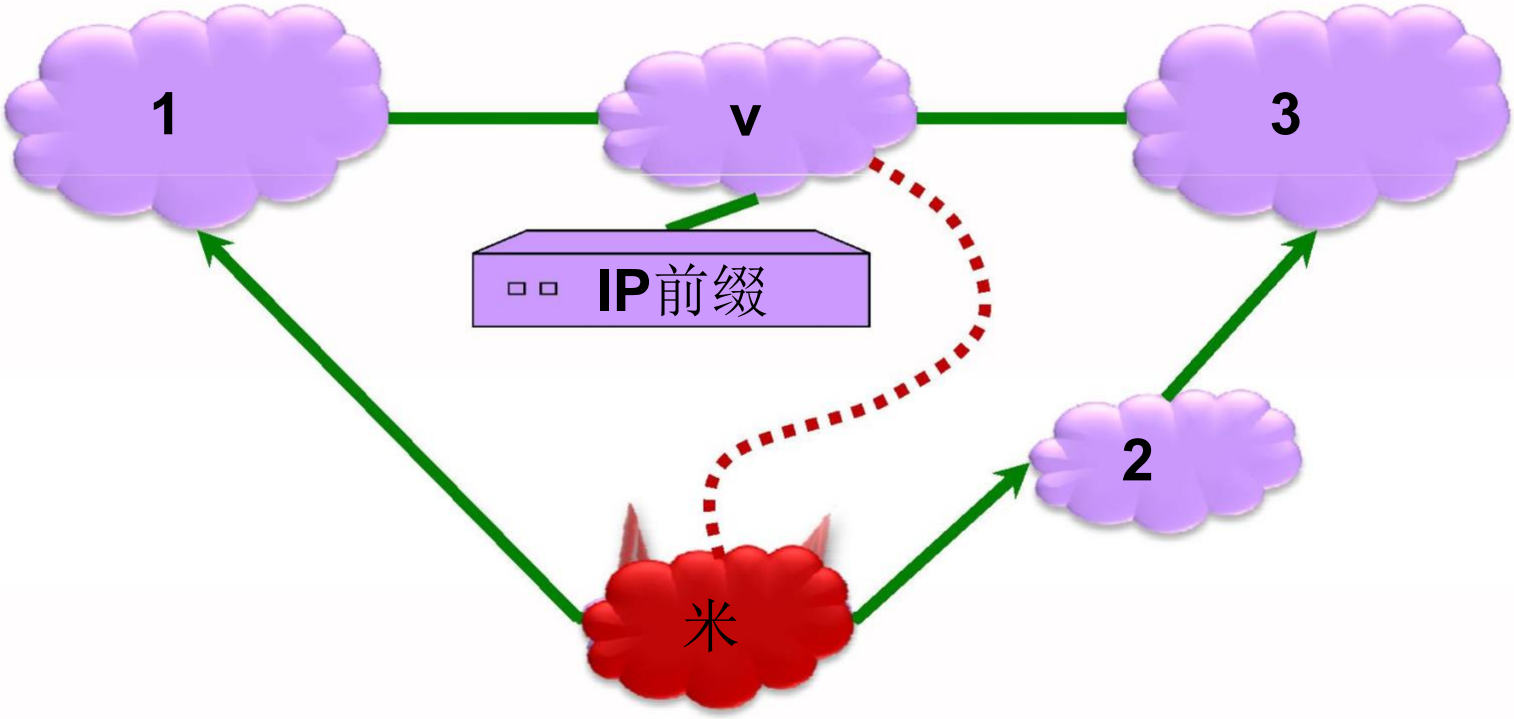
我们刚才看到的攻击本可以防止
带有原始身份验证（**ROA / RPKI**）。

现在，假设我们有**ROA / RKPI**。
攻击者仍然可以发起攻击吗？

（ 是 

安全机制：源认证RPKI / ROA

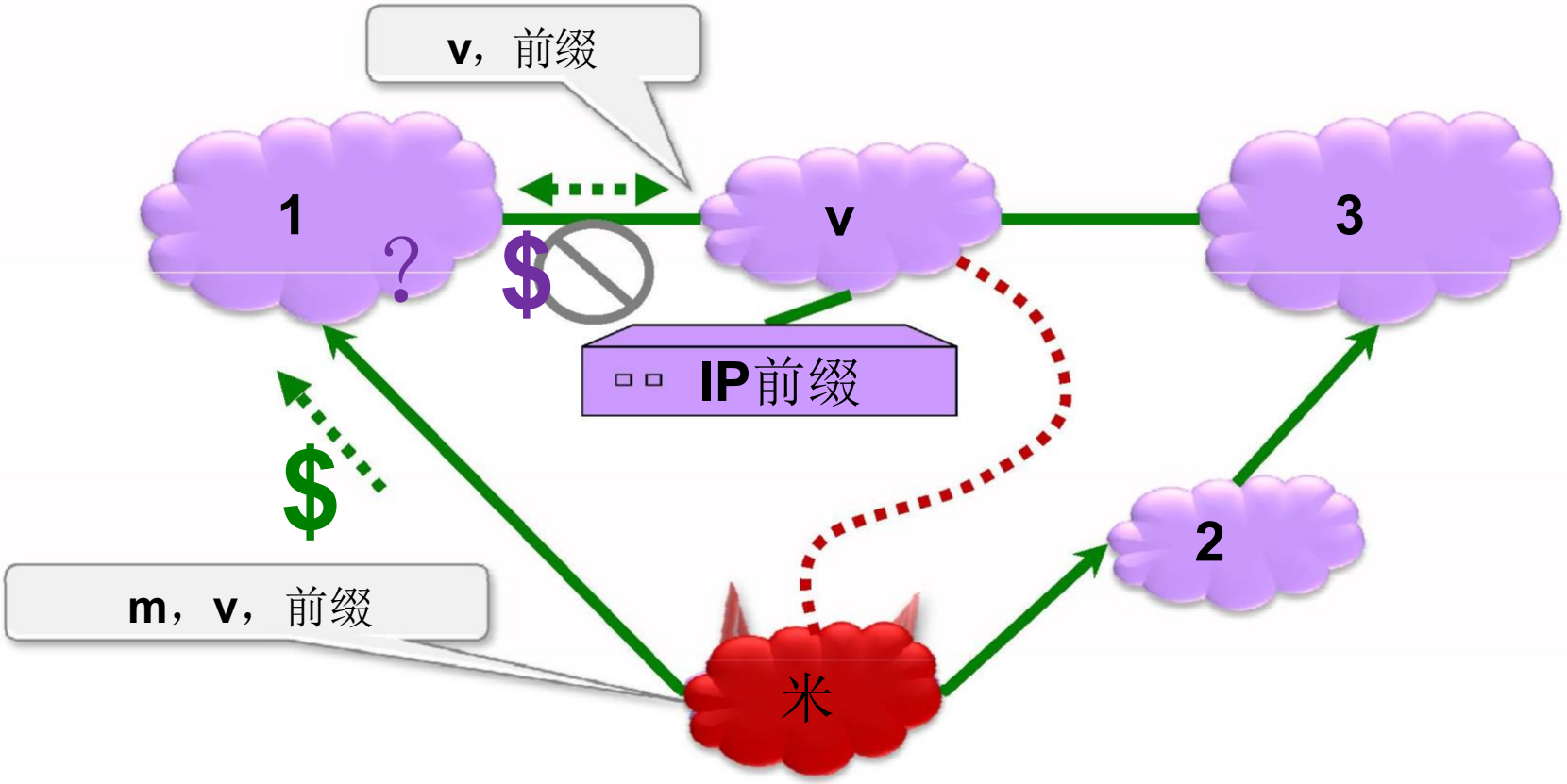
将IP前缀映射到所有者AS的安全数据库。



智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

安全机制：源认证RPKI / ROA

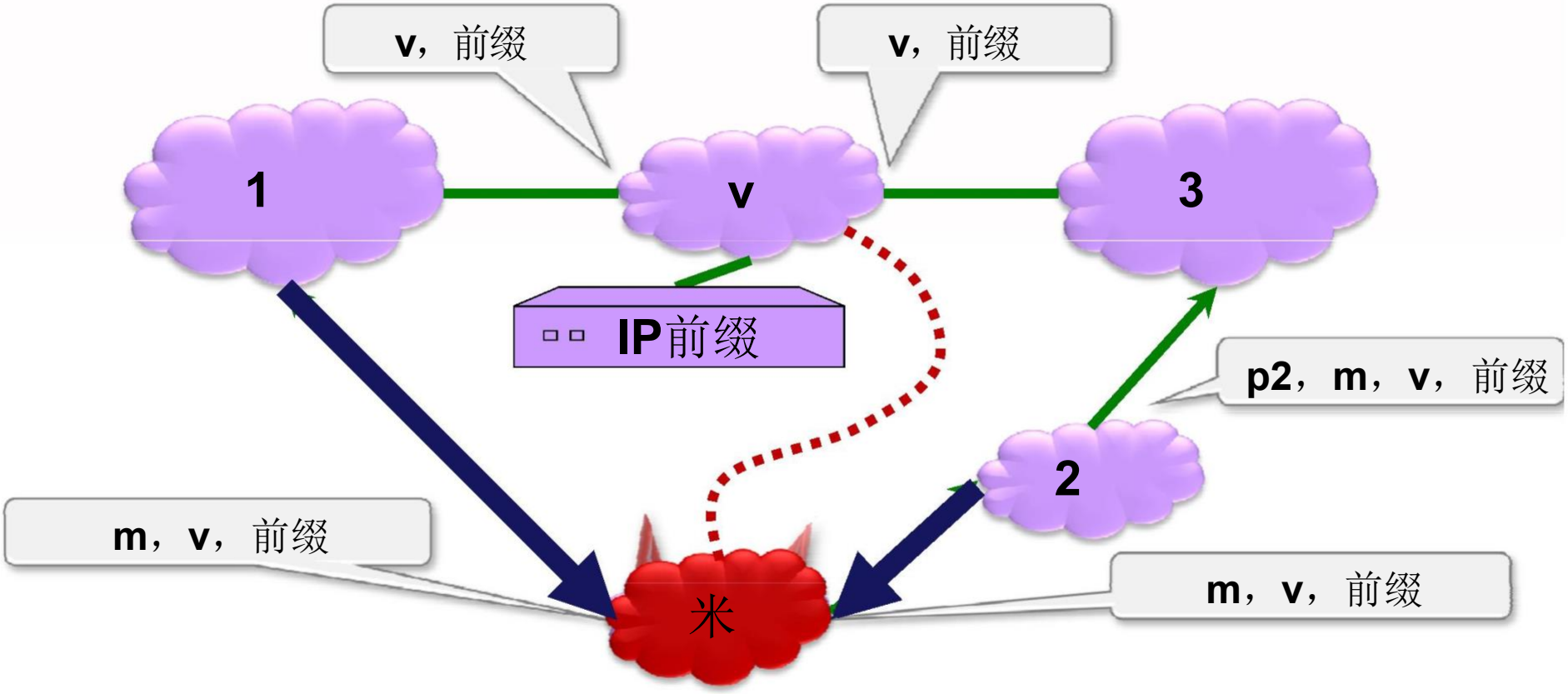
将IP前缀映射到所有者AS的安全数据库。



智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

安全机制：源认证RPKI / ROA

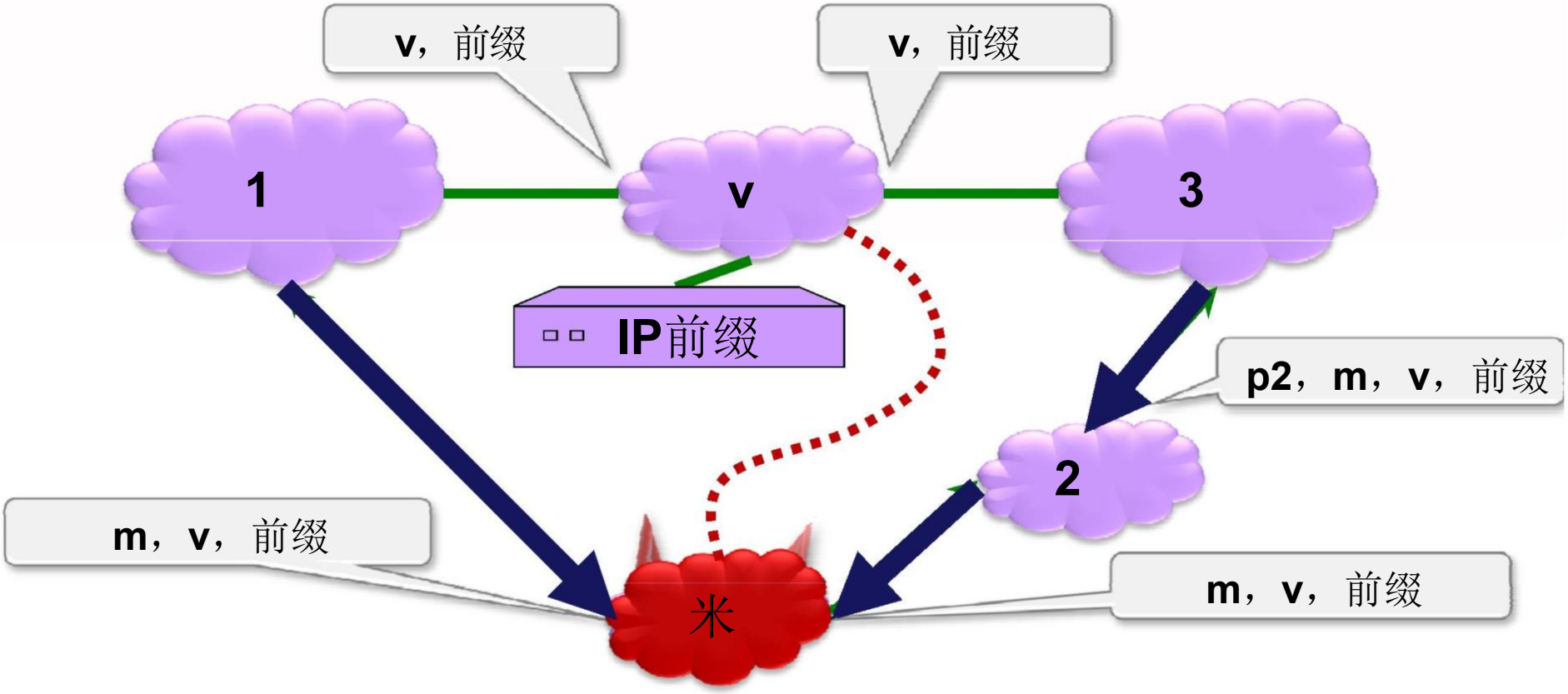
将IP前缀映射到所有者AS的安全数据库。



智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

安全机制：源认证RPKI / ROA

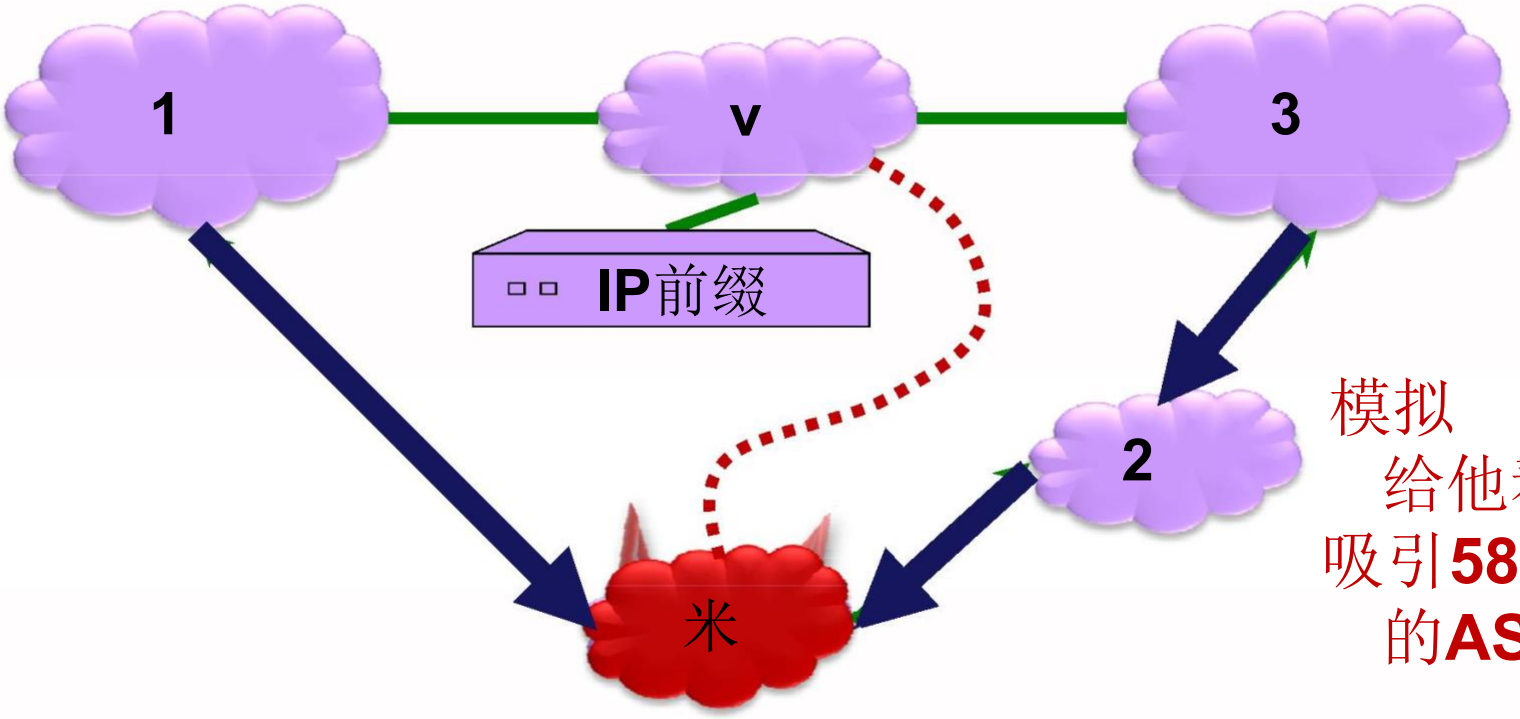
将IP前缀映射到所有者AS的安全数据库。



智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

安全机制：源认证RPKI / ROA

将IP前缀映射到所有者AS的安全数据库。



模拟
给他看
吸引58%
的ASes！

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

我们刚才看到的攻击本可以防止与**soBGP**或安全**BGP**

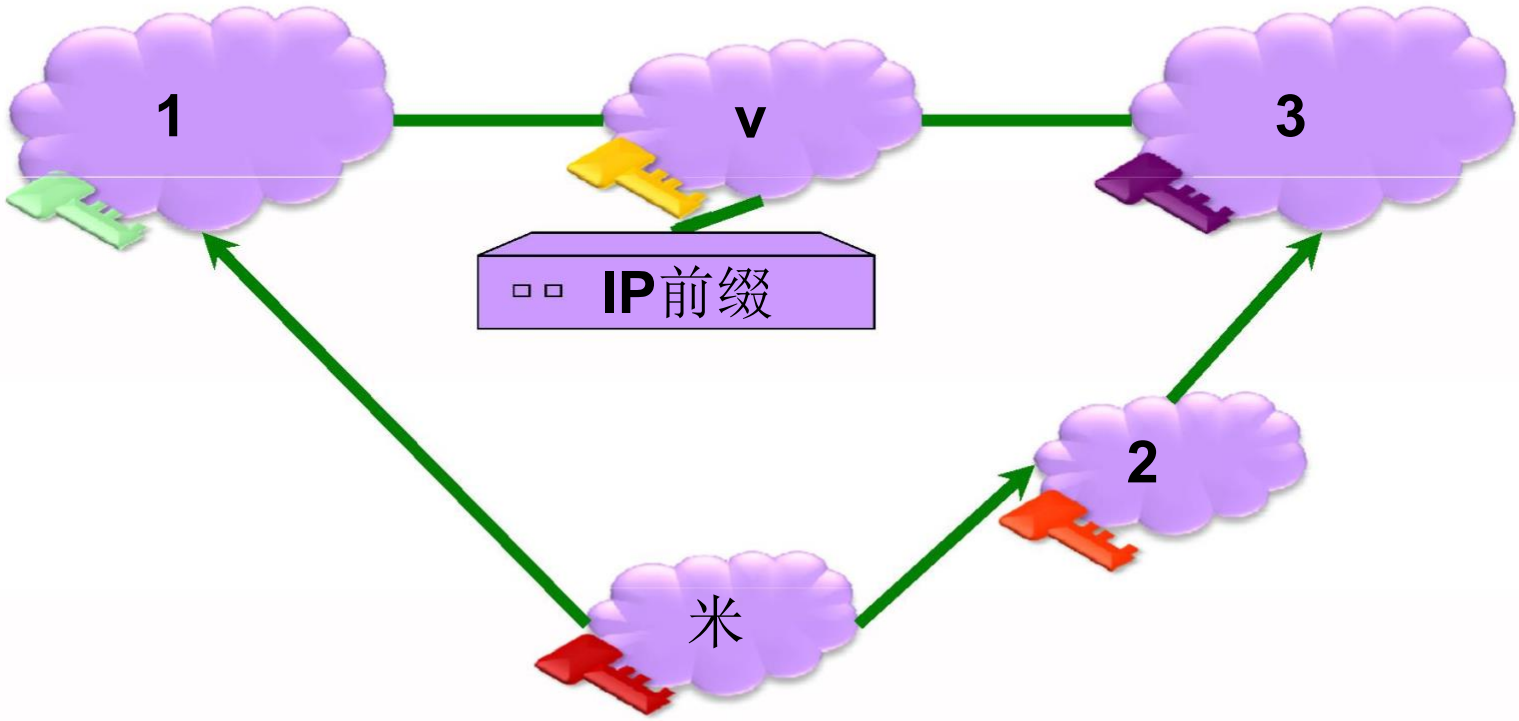
现在，假设我们有安全**BGP**。
攻击者仍然可以发起攻击吗？

（是的，使用路由泄漏）

安全机制：“安全BGP” [KLS98]

安全**BGP**：　　原始身份验证+

无法宣布尚未向您宣布的路径。

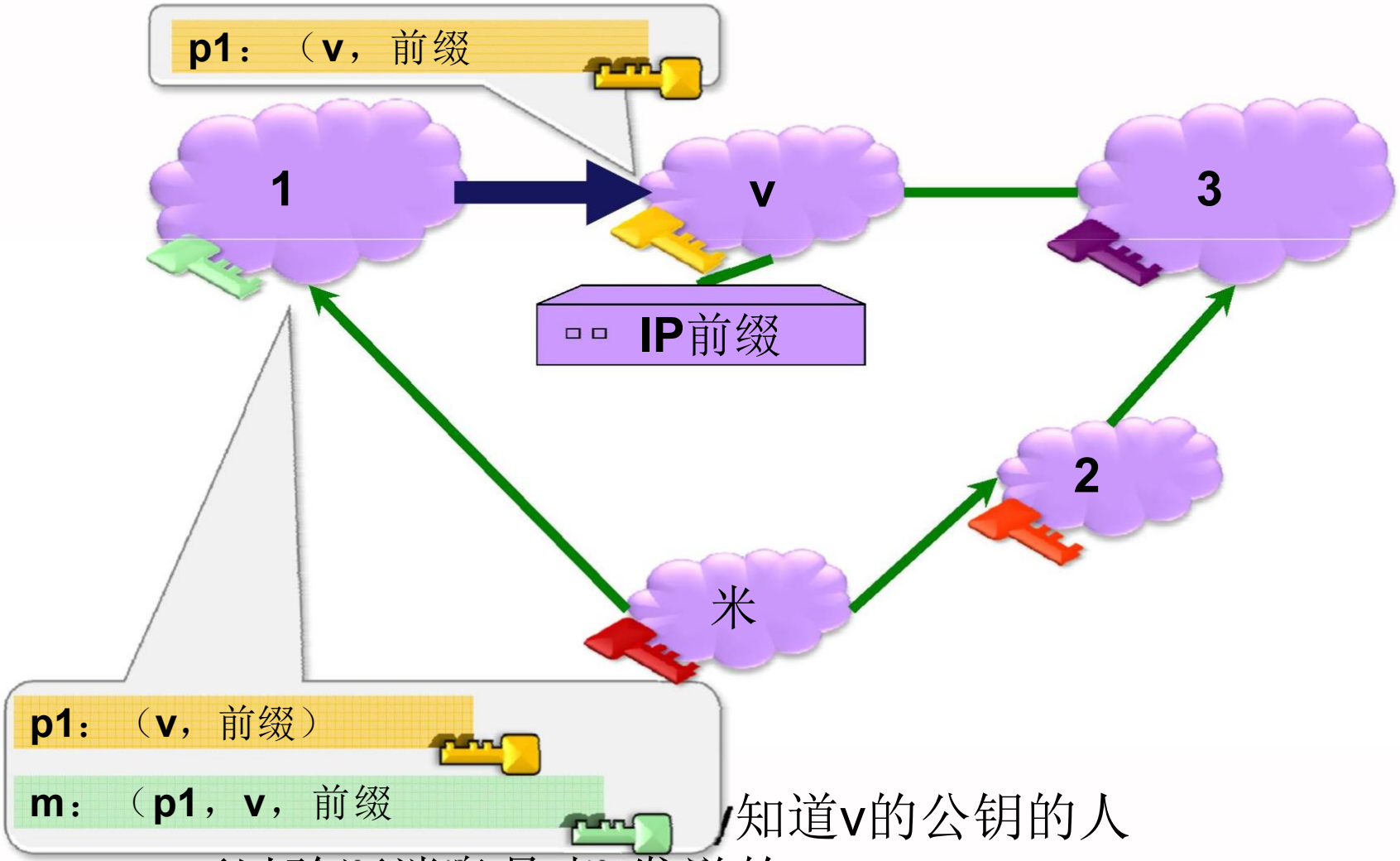


公钥签名：知道**v**公钥的任何人

可以验证消息是由v发送的。

安全机制：“安全BGP” [KLS98]

安全**BGP**：　　原始身份验证+
无法宣布尚未向您宣布的路径。

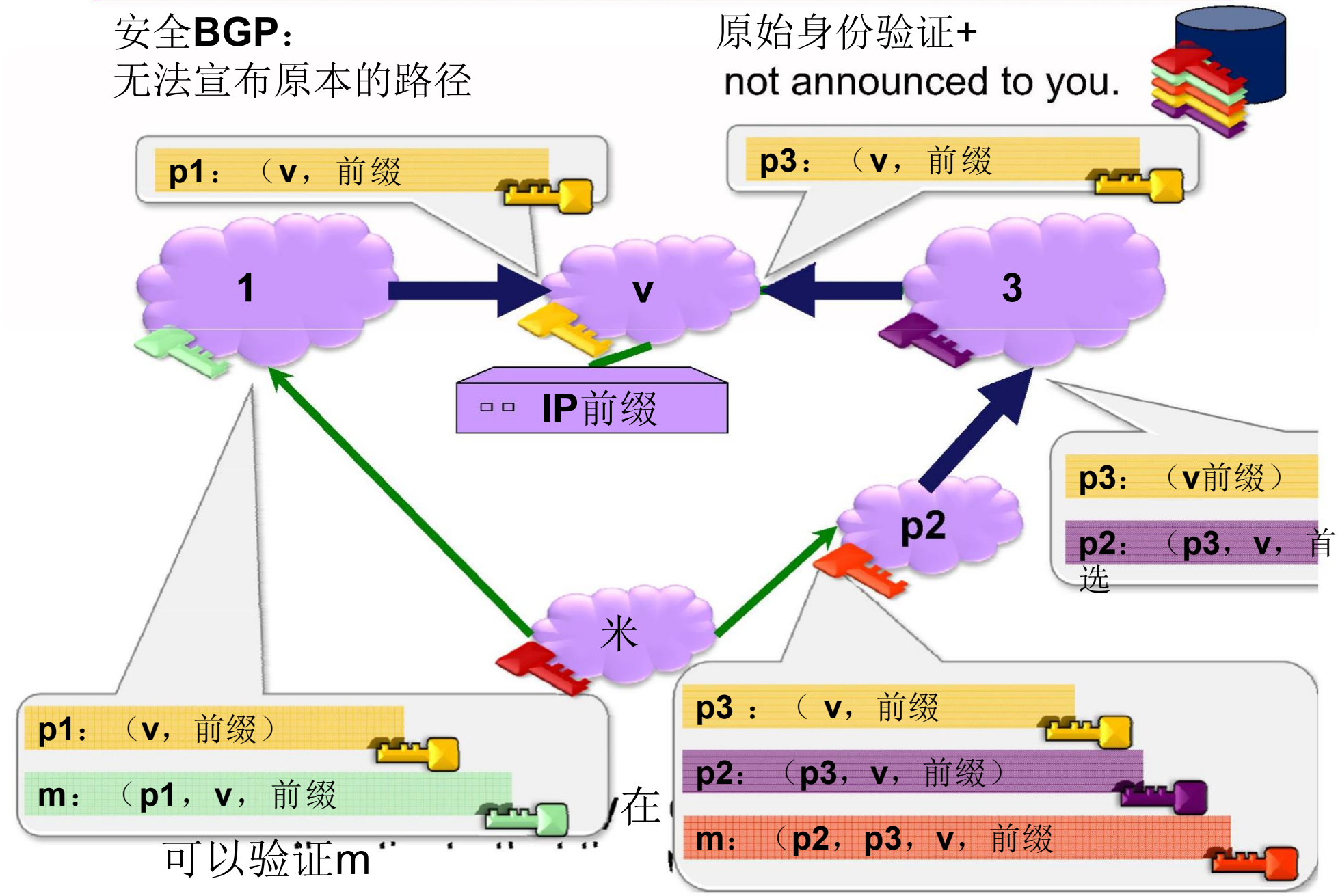


/知道v的公钥的人
可以验证消息是由v发送的。

安全机制：“安全BGP” [KLS98]

安全**BGP**：
无法宣布原本的路径

原始身份验证+
not announced to you.

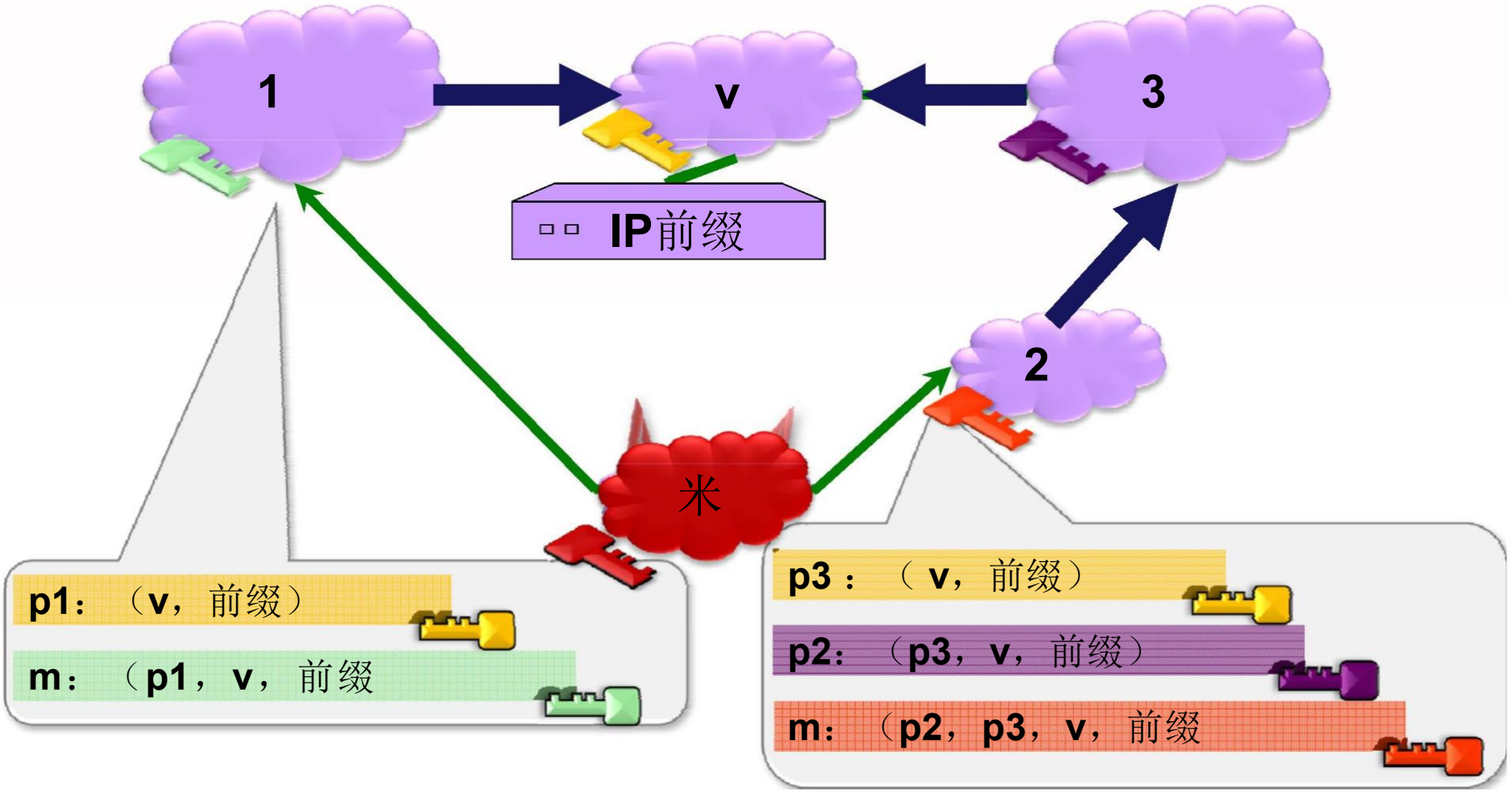


在

可以验证m

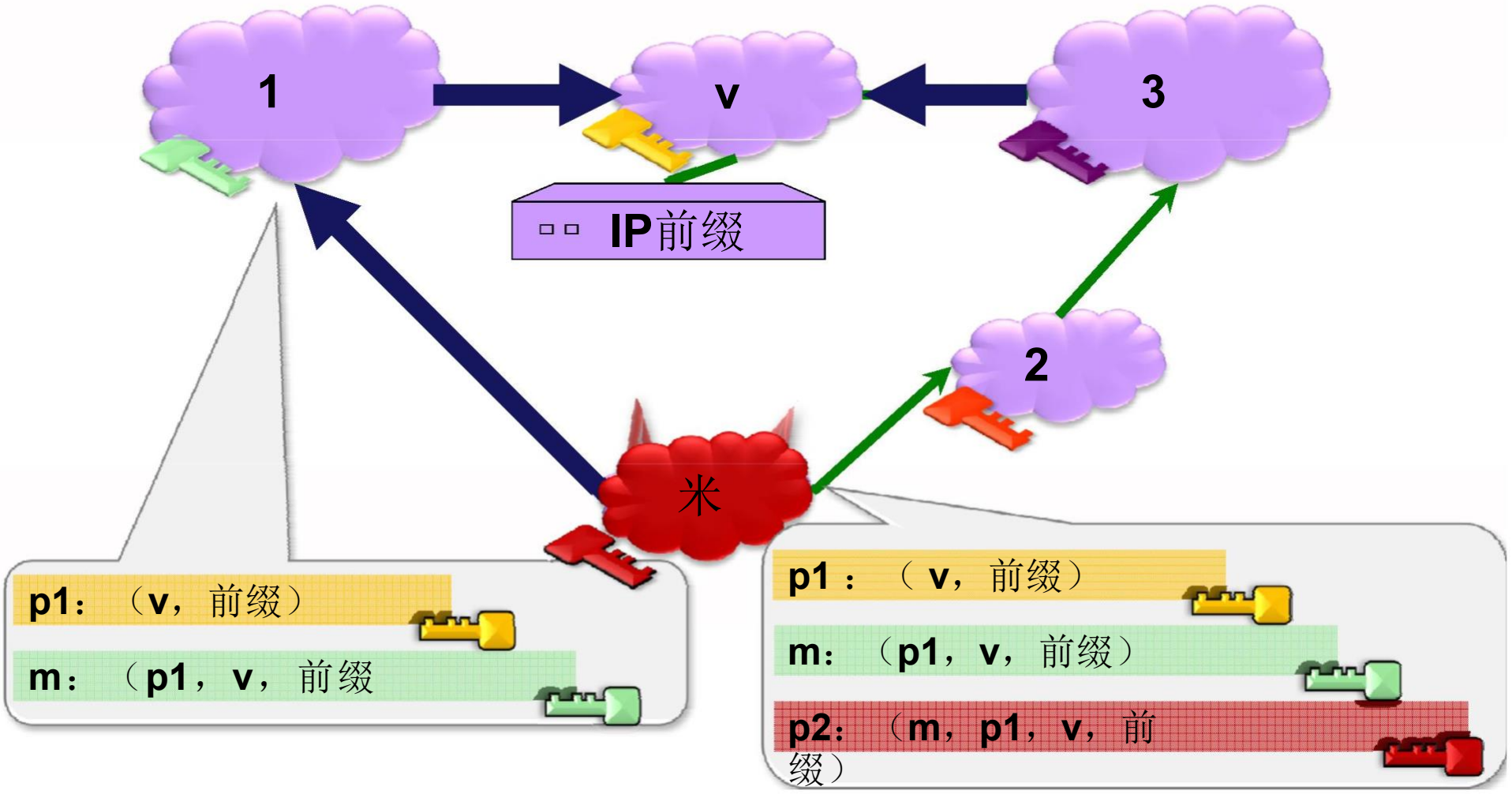
仍然可以通过安全BGP进行攻击吗？ （1）

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



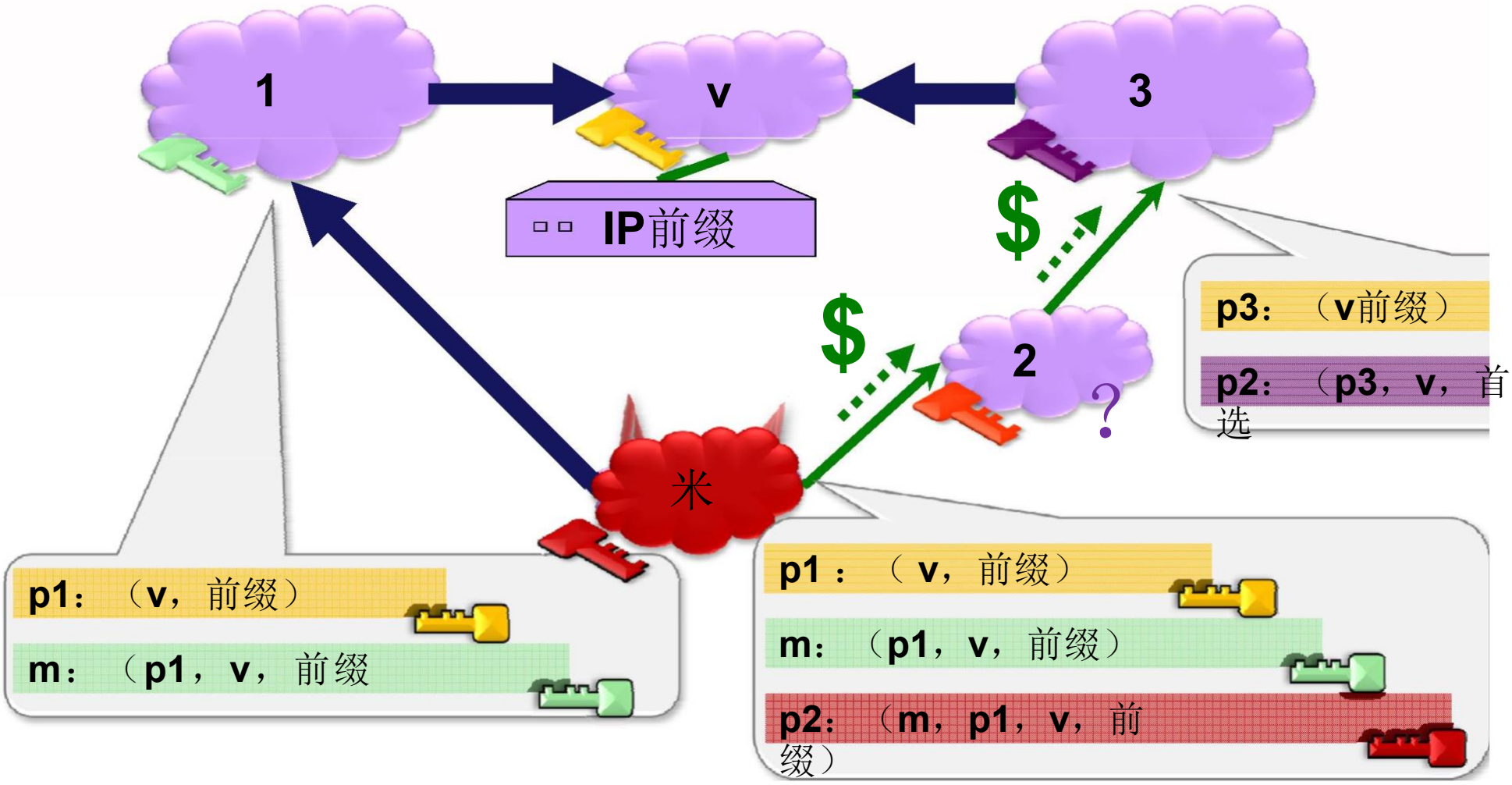
仍然可以通过安全BGP进行攻击吗？ （2）

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



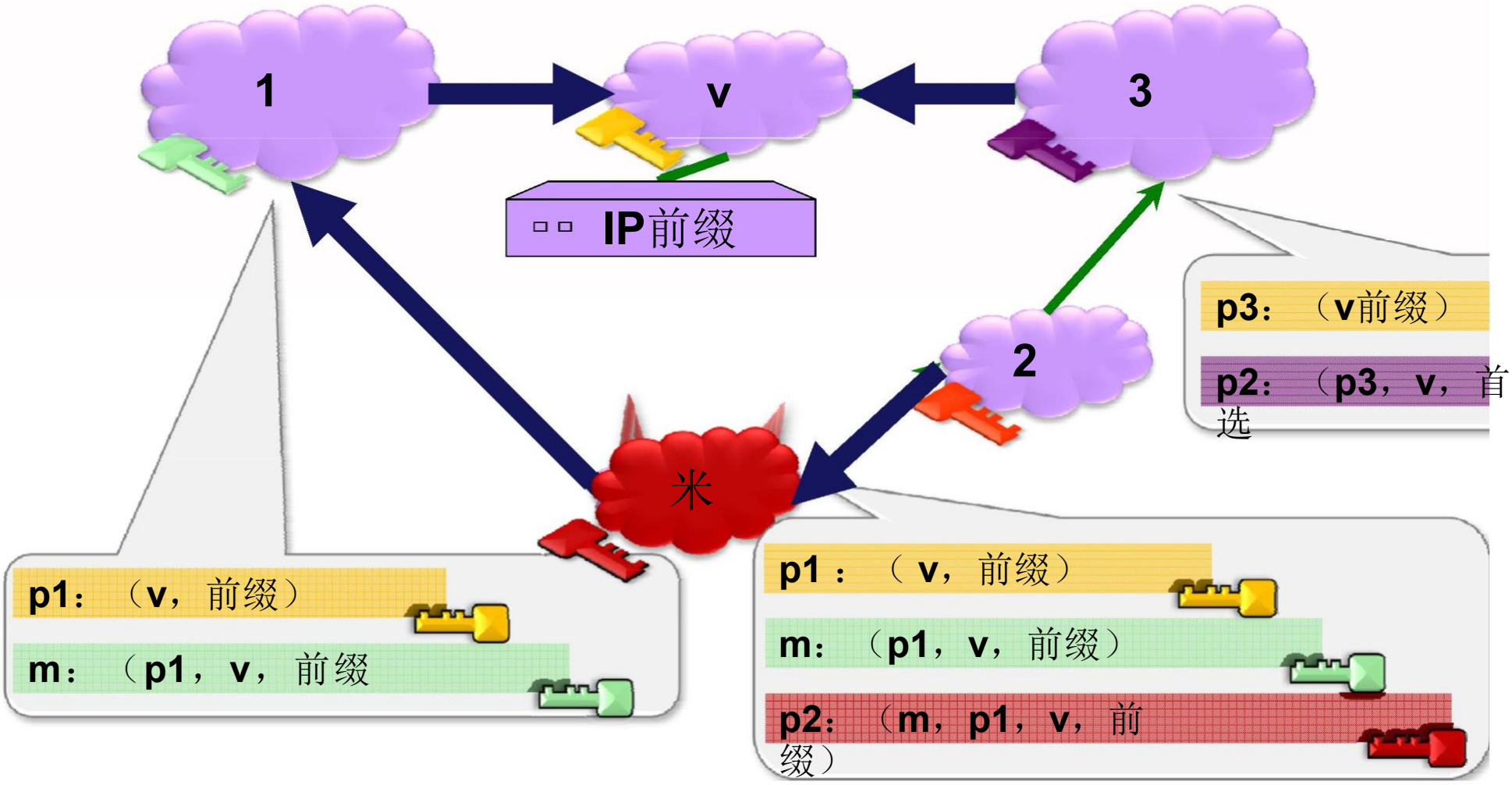
仍然可以通过安全BGP进行攻击吗？ （2）

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



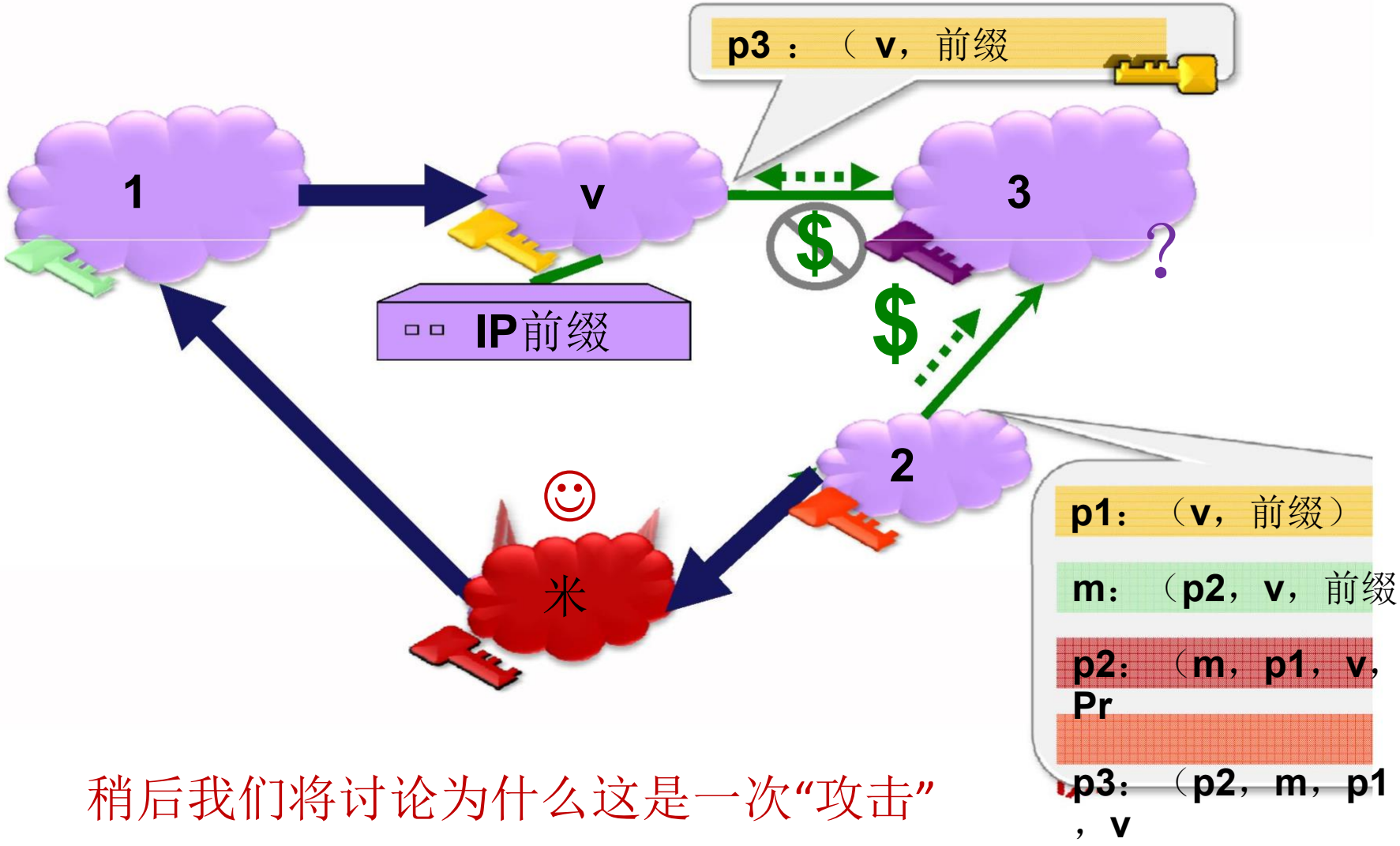
仍然可以通过安全BGP进行攻击吗？ （2）

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



仍然可以通过安全BGP进行攻击吗？ （3）

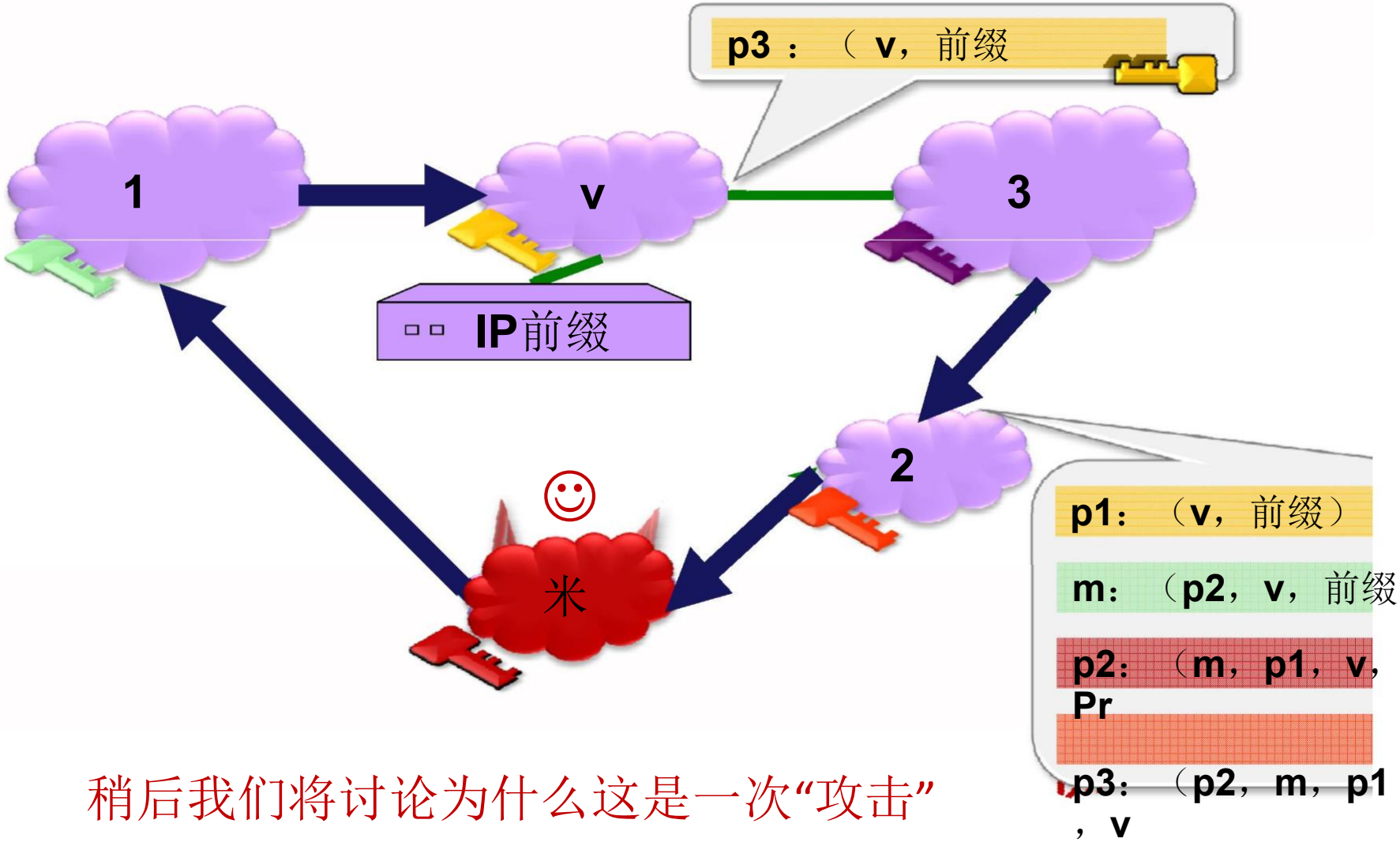
智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



稍后我们将讨论为什么这是一次“攻击”

仍然可以通过安全BGP进行攻击吗？ （3）

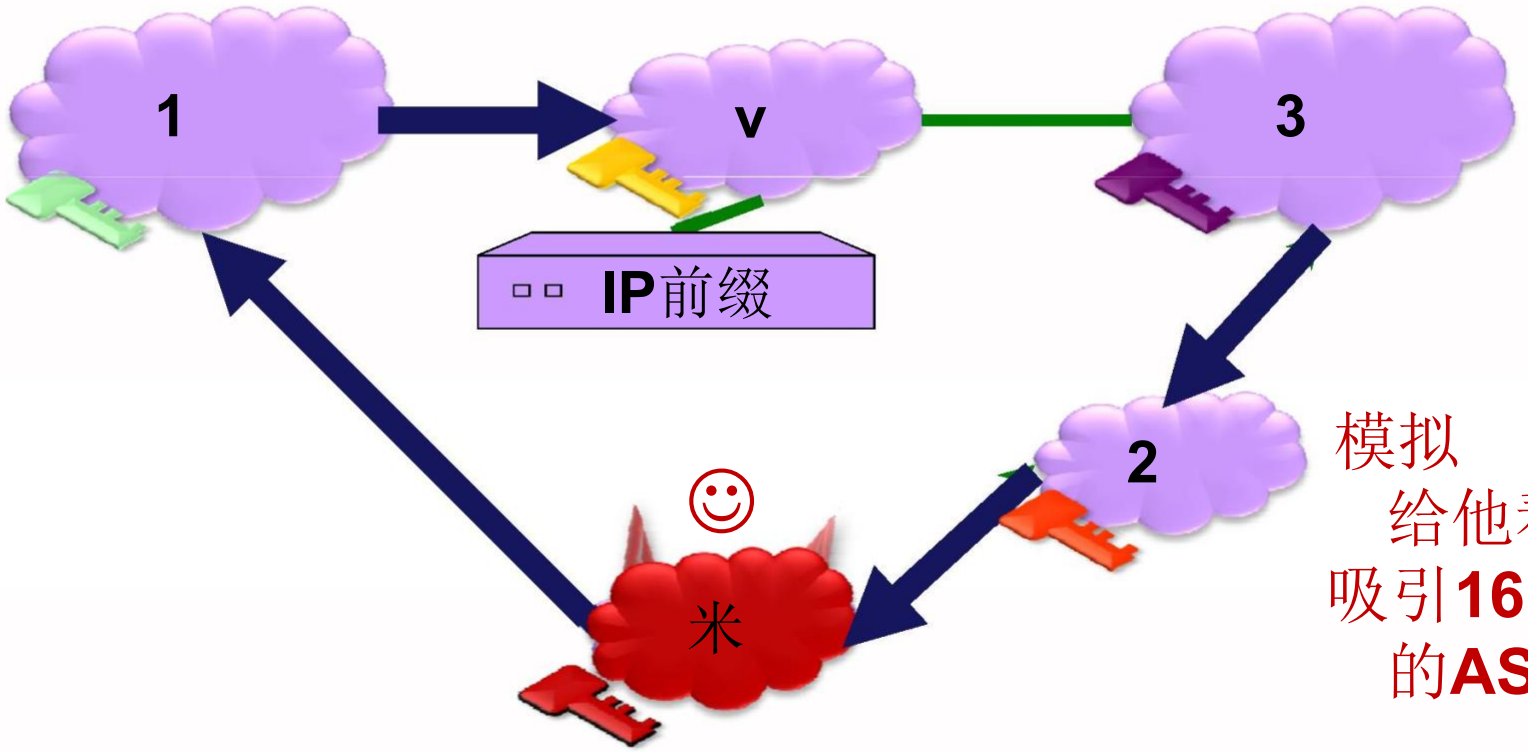
智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



稍后我们将讨论为什么这是一次“攻击”

仍然可以通过安全BGP进行攻击吗？ （3）

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！



模拟
给他看
吸引16%
的ASes！

稍后我们将讨论为什么这是一次“攻击”

这个演讲

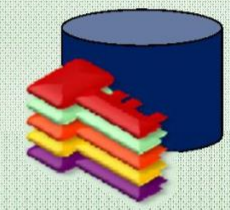
第1部分：BGP路由策略模型

第2部分：安全路由协议和攻击

BGP上的前缀劫持

原始身份验证攻击（RPKI）

使用安全BGP路由泄漏



插曲：找到最佳攻击

通过前缀列表过滤存根攻击

第3部分：仿真结果图

第4部分：结论和启示

等一下这是“最佳”攻击策略吗？！

我不能为自己的生意撒谎
与AS p2的关系，所以我也应该
宣布我可以的最短路径。

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

等一下这是“最佳”攻击策略吗？！

我不能为自己的生意撒谎
与AS p2的关系，所以我也应该
宣布我可以的最短路径。

但不是最优的！

智能攻击策略：宣布最短路径
我可以和所有邻居摆脱！

有时会宣布
邻居越少越好！

有时候
更长的路径
更好！

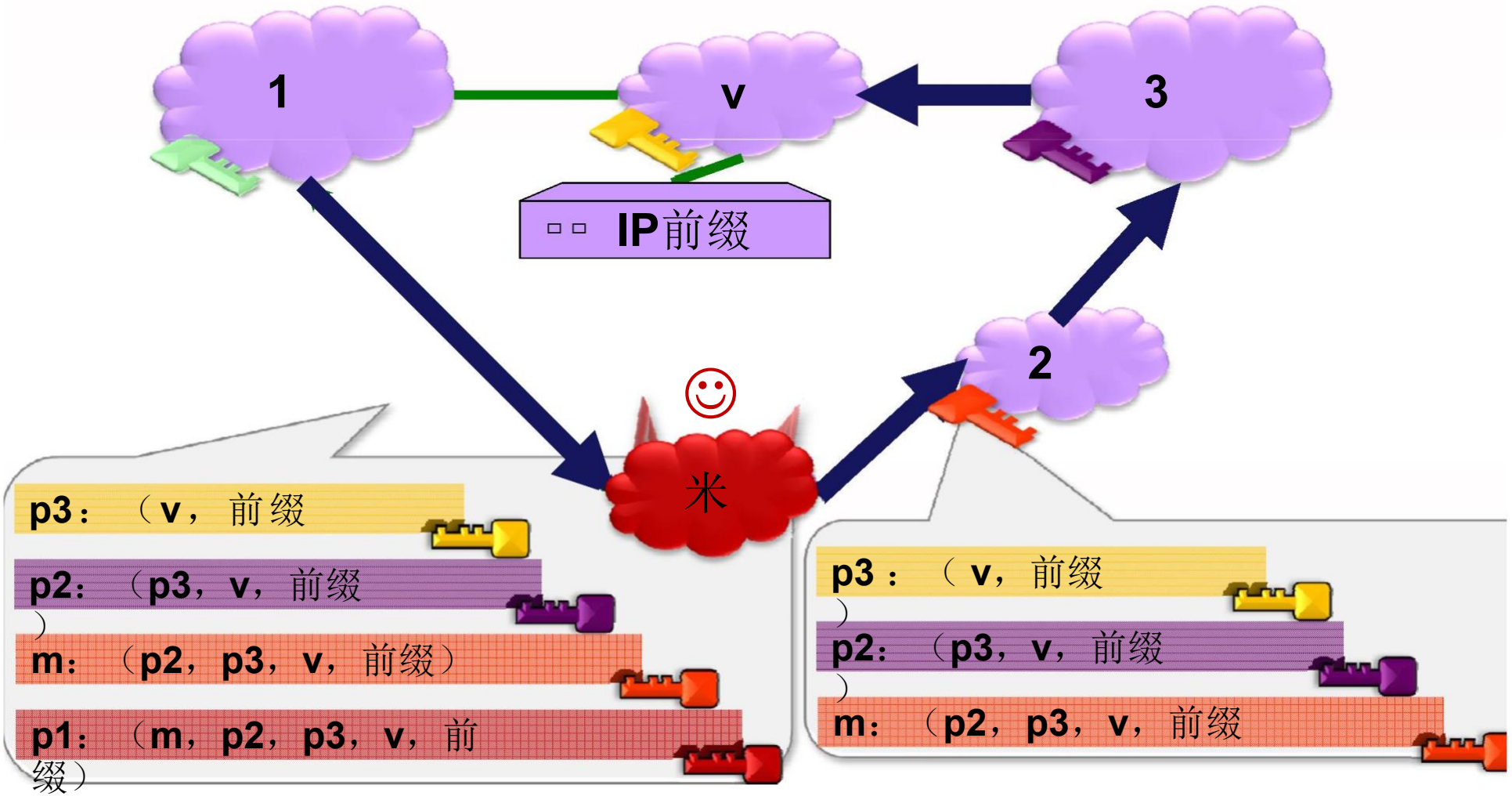
顺便说一句，**NP**也很难找到最佳的攻击策略。

➔智能攻击策略低估了损失。

路径越长越好？

这是一个示例，说明为什么

有时更长的路径更好！ （1）

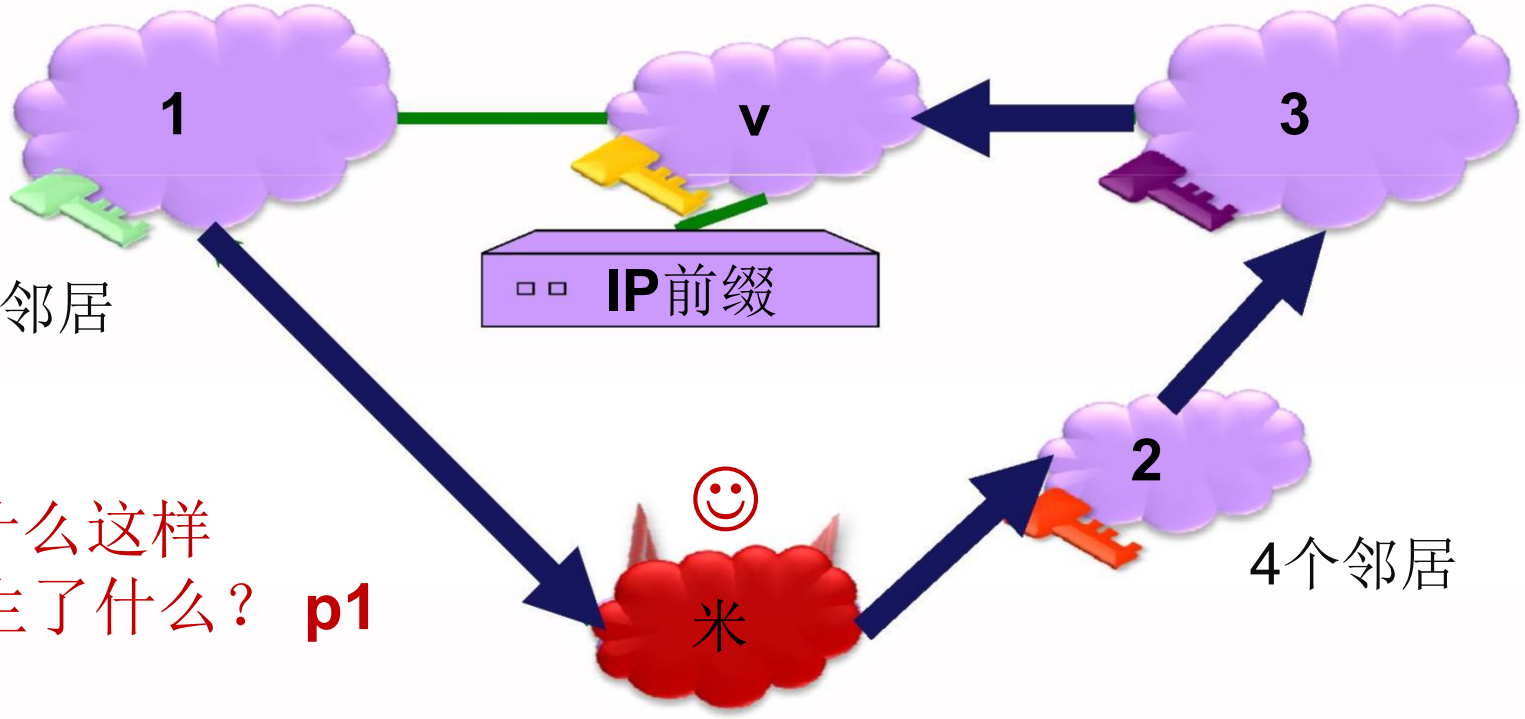

1
v
3
IP前缀
2
米
p3：（v，前缀
p2：（p3，v，前缀
）
m：（p2，p3，v，前缀）
p1：（m，p2，p3，v，前缀）
p3：（v，前缀
）
p2：（p3，v，前缀
）
m：（p2，p3，v，前缀

有时更长的路径更好！ （2）

模拟显示，他吸引了**56**%的互联网！

路径更短，他只吸引**16**%的互联网！

这几乎等同于对不安全**BGP**的攻击：**62**%！



517个邻居

4个邻居

为什么这样发生了什么？ **p1**是比**p2**“更大”。

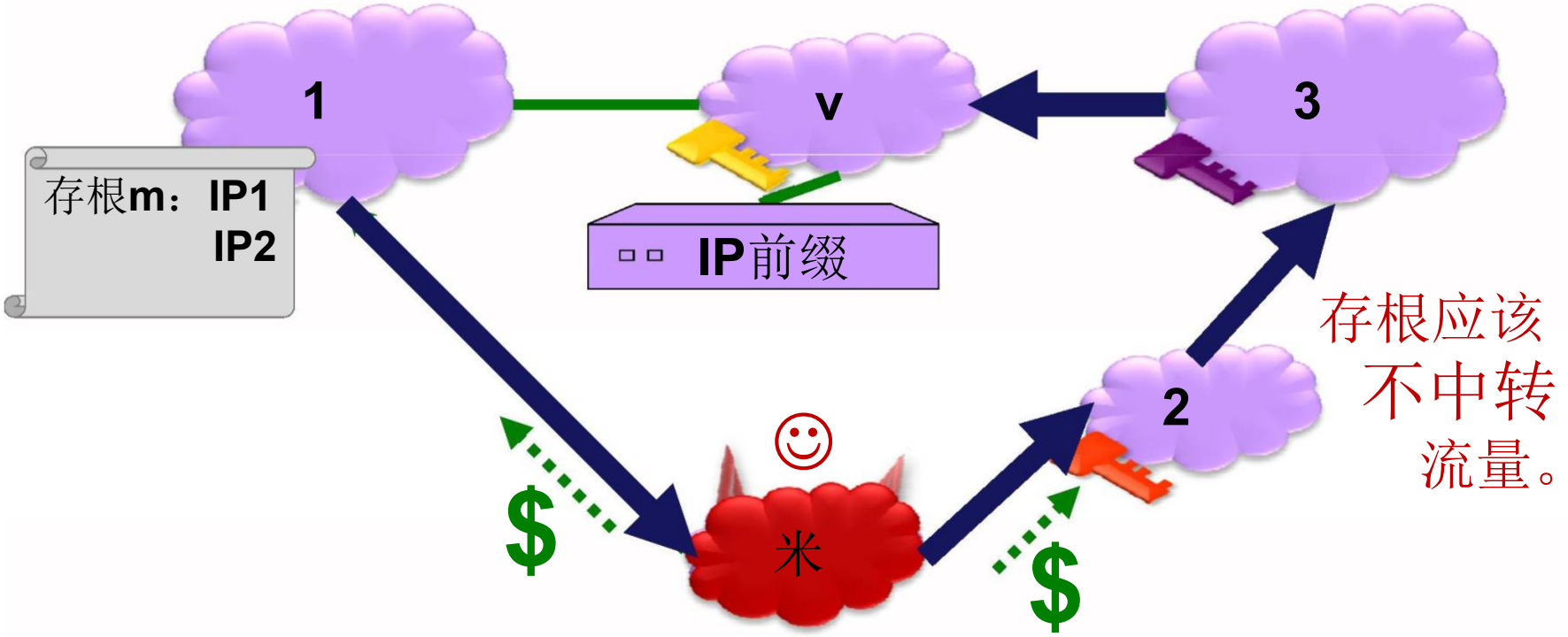
关键观察：向谁宣布与

重要的是您宣布的内容。

安全启发式：过滤前缀列表中的存根（1）

筛选前缀列表上的存根的提供程序：

- 保留每个存根客户拥有的前缀的列表
- 如果存根客户宣布前缀未列出的任何路径，则过滤



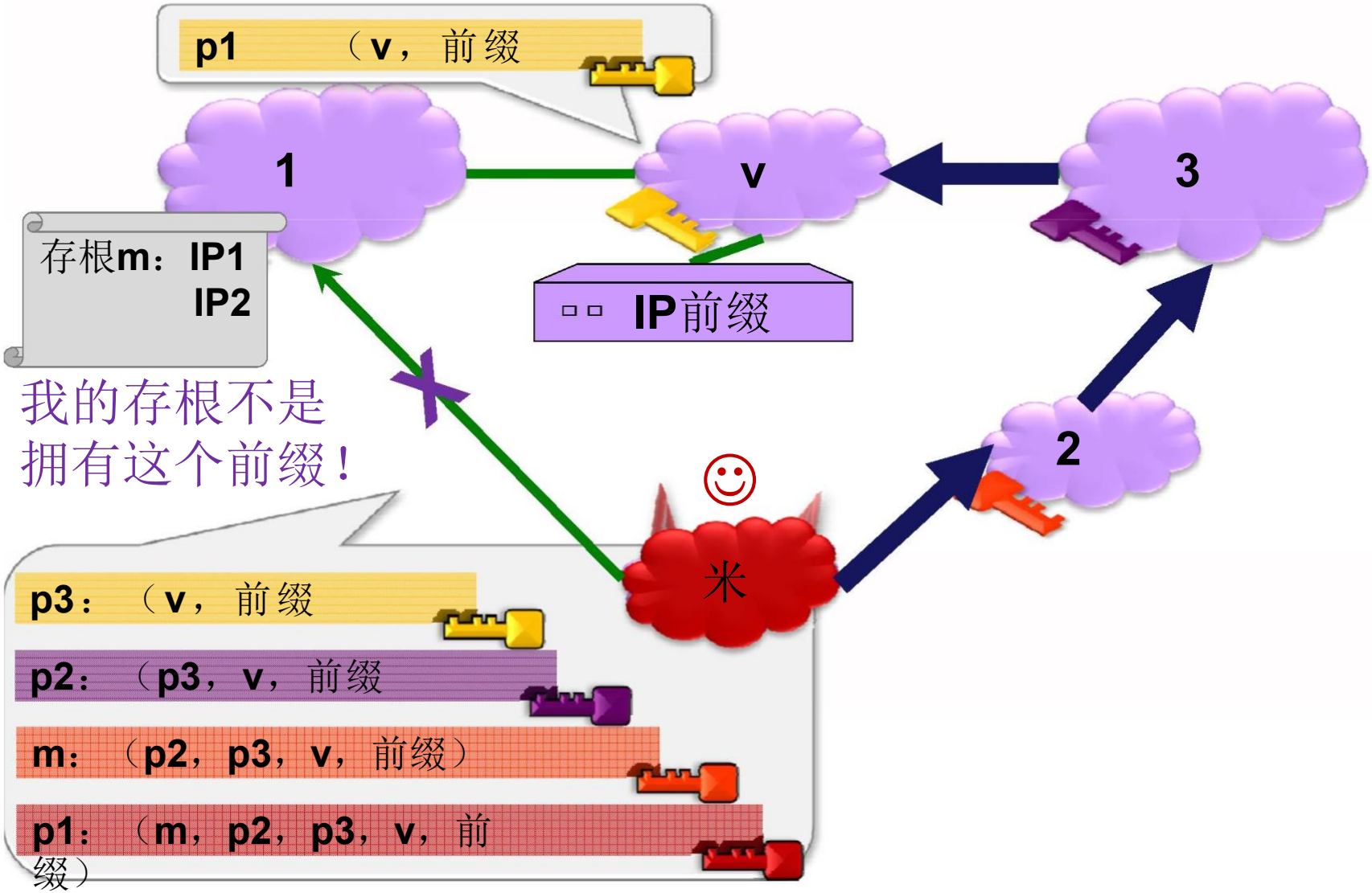
存根是具有以下内容的**AS**

没有客户。

安全启发式：过滤前缀列表中的存根（2）

筛选前缀列表上的存根的提供程序：

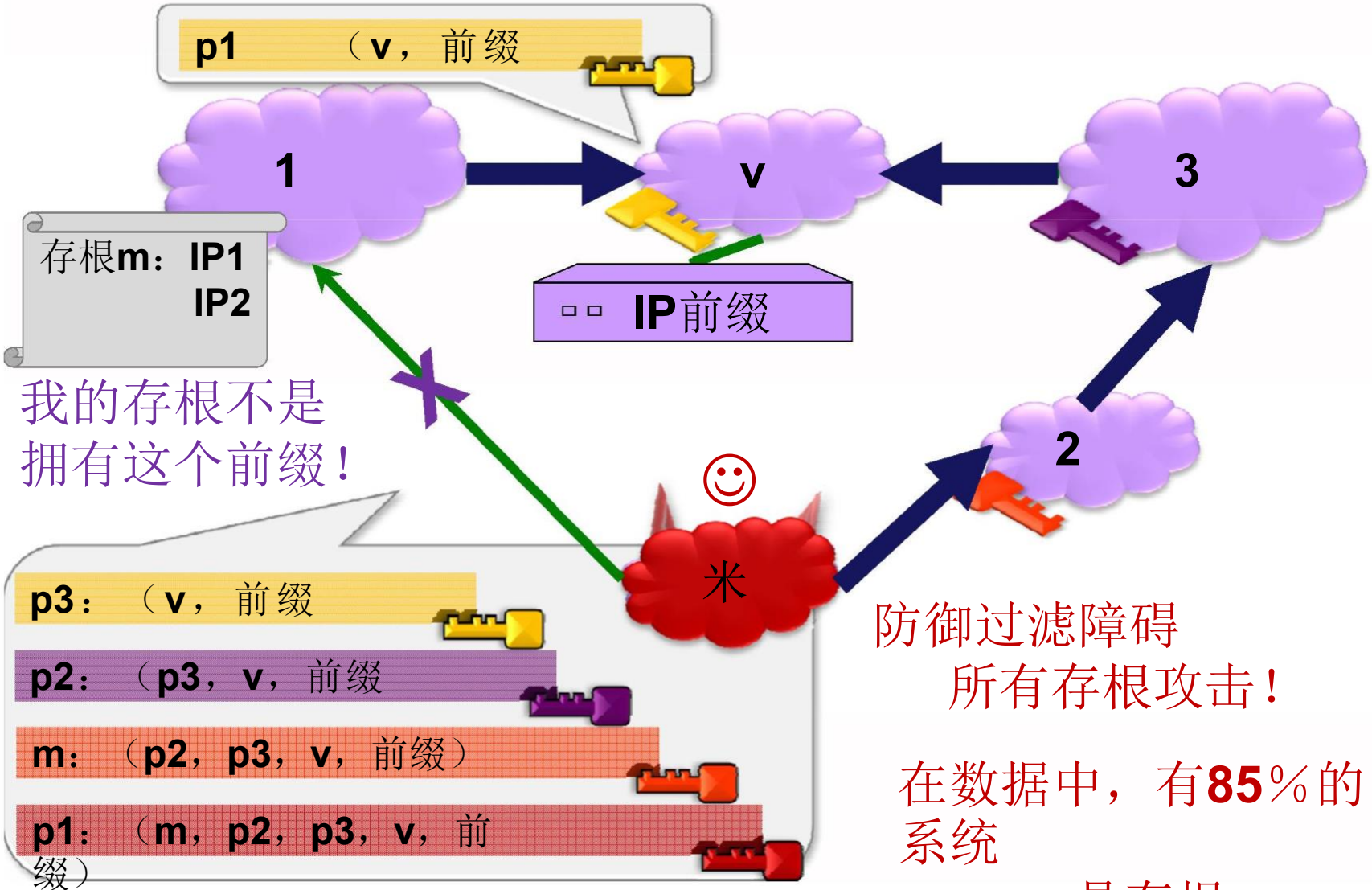
- keep列出每个存根客户拥有的前缀
- 如果存根客户宣布前缀未列出的任何路径，则过滤



安全启发式：过滤前缀列表中的存根（2）

筛选前缀列表上的存根的提供程序：

- keep列出每个存根客户拥有的前缀
- 如果存根客户宣布前缀未列出的任何路径，则过滤



防御过滤障碍
所有存根攻击！

在数据中，有85%的自治系统
是存根。

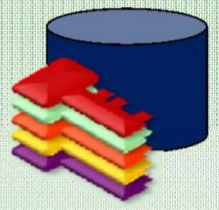
这个演讲

第1部分：BGP路由策略模型

第2部分：安全路由协议和攻击

BGP上的前缀劫持

原始身份验证攻击（RPKI）

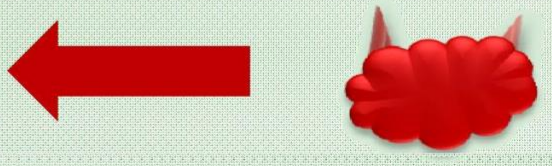


使用安全BGP路由泄漏

插曲：找到最佳攻击

通过前缀列表过滤存根攻击

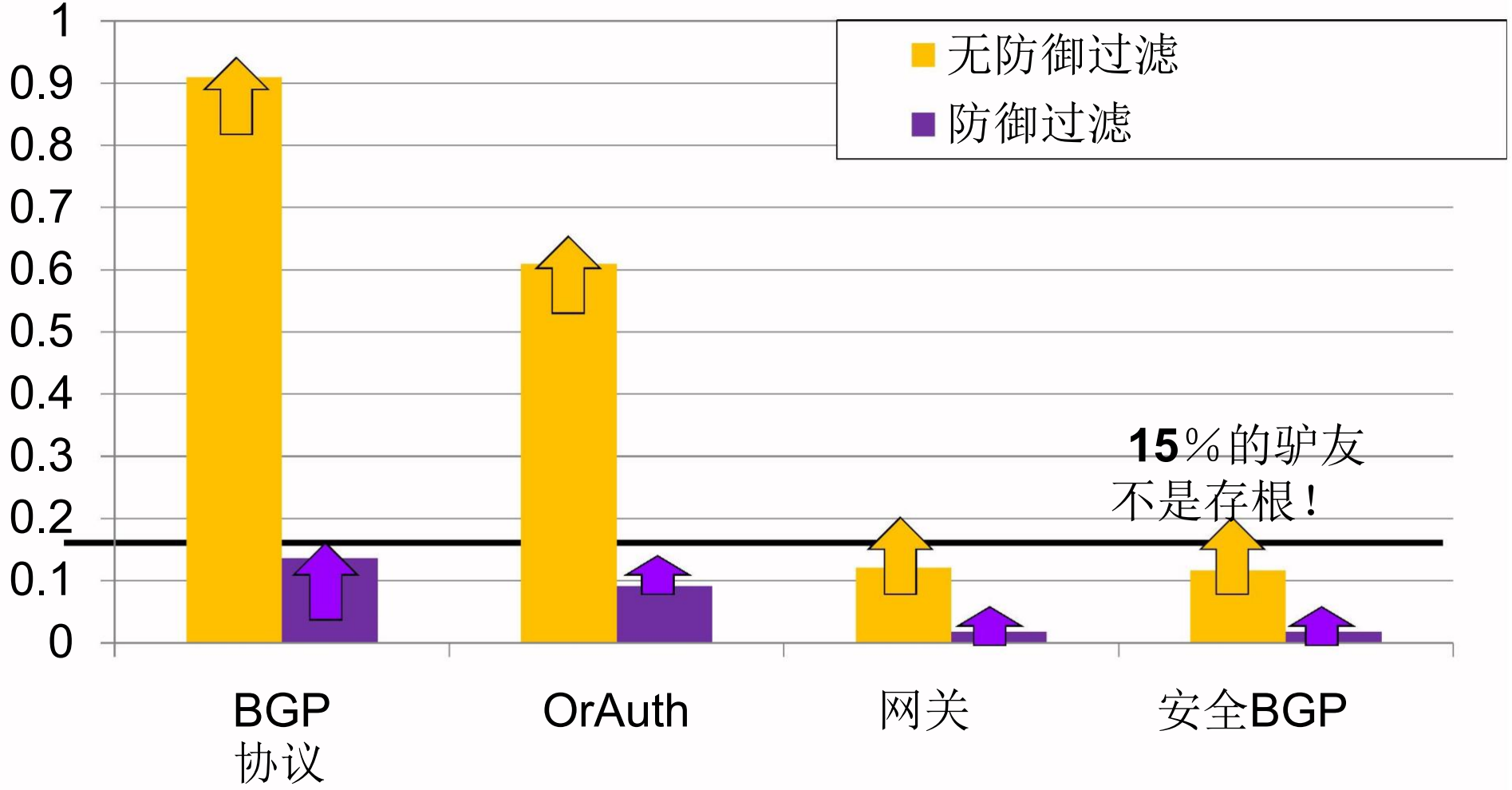
第3部分：仿真结果图



第4部分：结论和启示

概率*智能攻击吸引了10%的互联网

*概率是随机选择攻击者和受害者的。



回想一下，贪婪攻击策略低估了伤害。

我们看到，如果每个提供商都进行过滤存根基于的公告前缀列表，效果与让所有人实施安全**BGP**！

安全**BGP**不能替代过滤，我们需要结合使用。

（**S * -BGP**容易受到路由泄漏的影响）

现在，图表显示

[CAIDA]和**[Cyclops]**同意。

这两个数据集由独立的

研究人员（不是我们）使用不同的

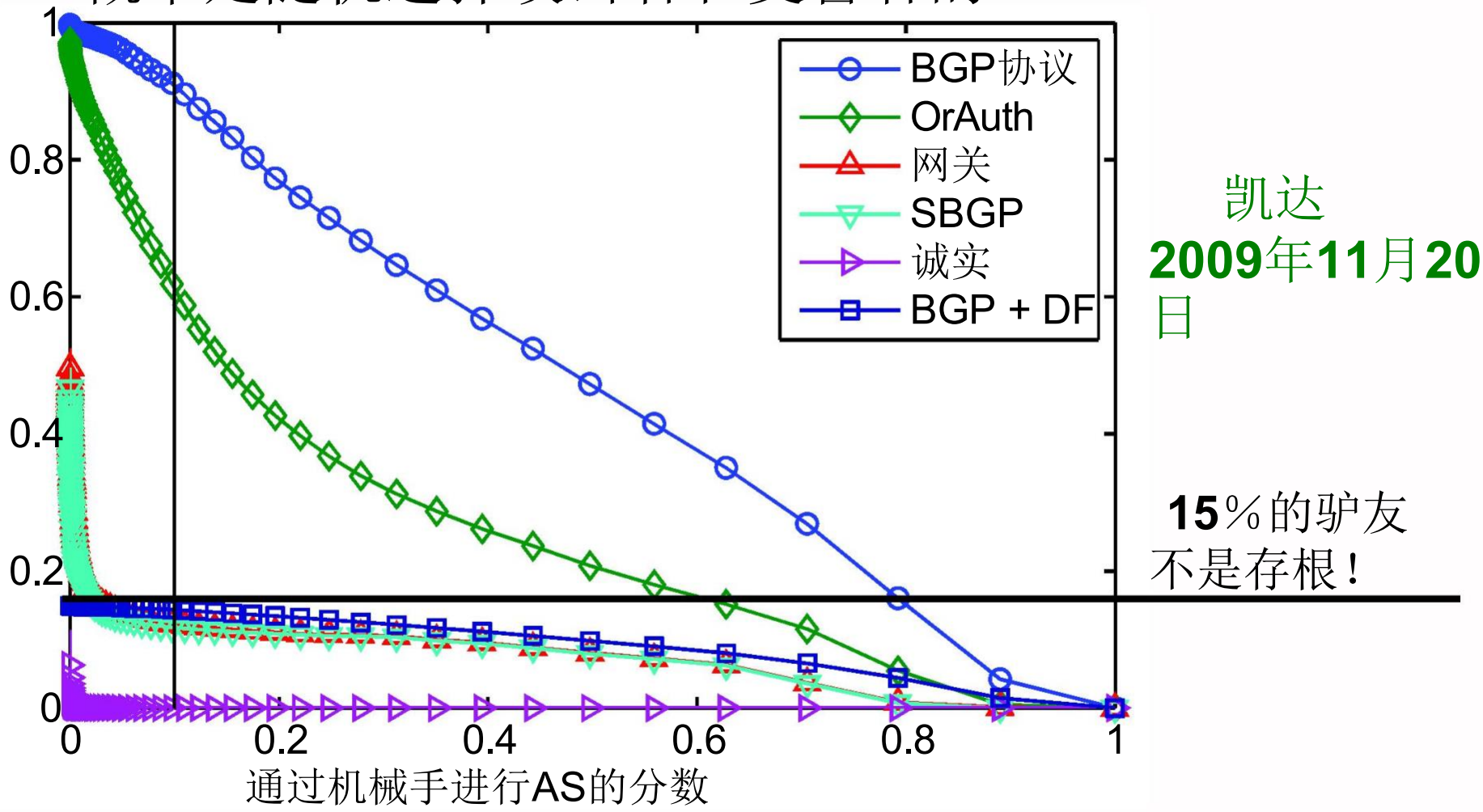
业务关系推理算法。

但对于我们的研究，我们看到的趋势

数据集非常一致。

概率*智能攻击吸引> x%的互联网（1）

*概率是随机选择攻击者和受害者的。



凯达

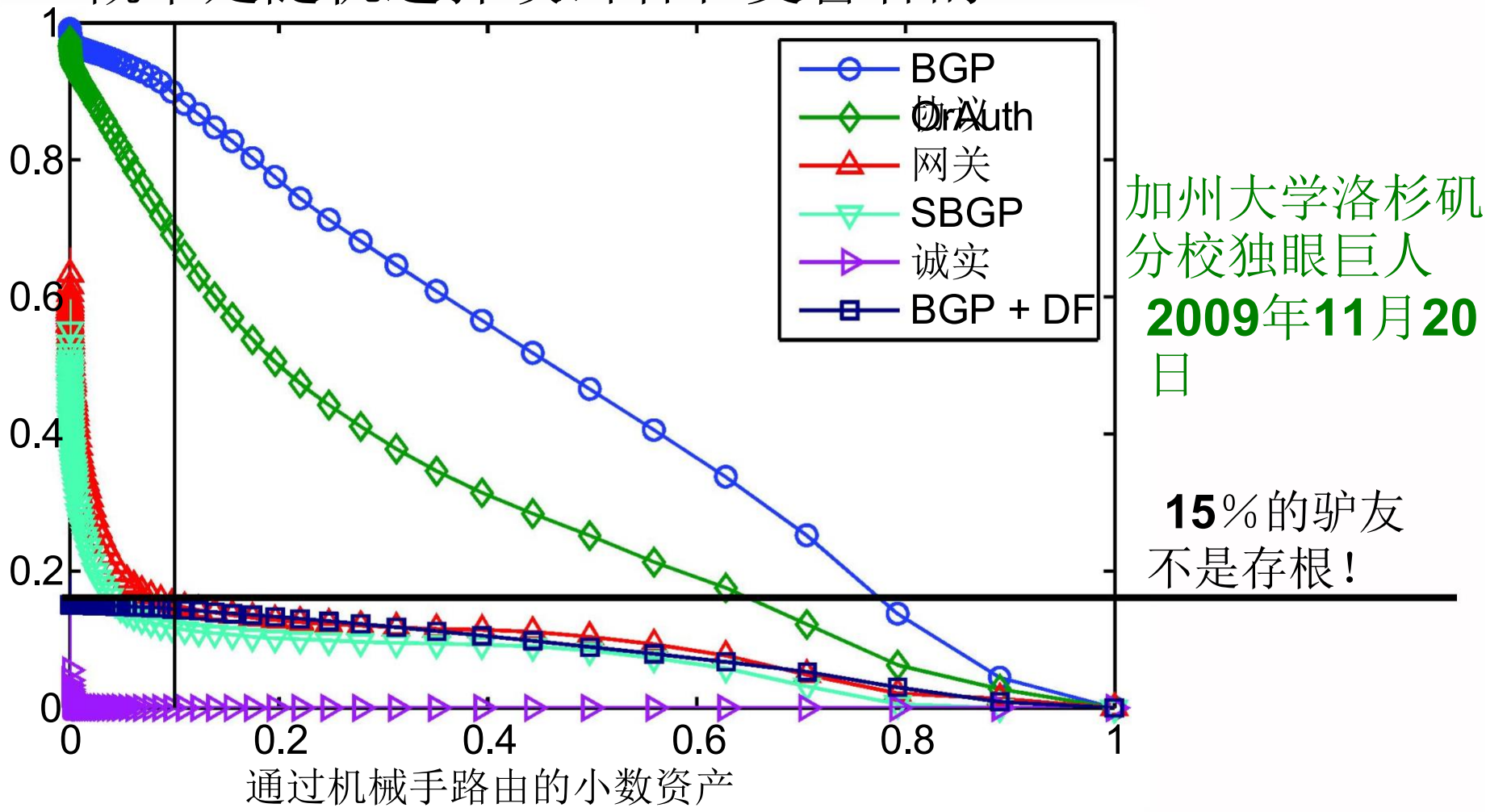
2009年11月20日

15%的驴友不是存根！

回想一下，智能攻击策略低估了损失。

概率*智能攻击吸引> x%的互联网（2）

*概率是随机选择攻击者和受害者的。



加州大学洛杉矶分校独眼巨人

2009年11月20日

15%的驴友不是存根！

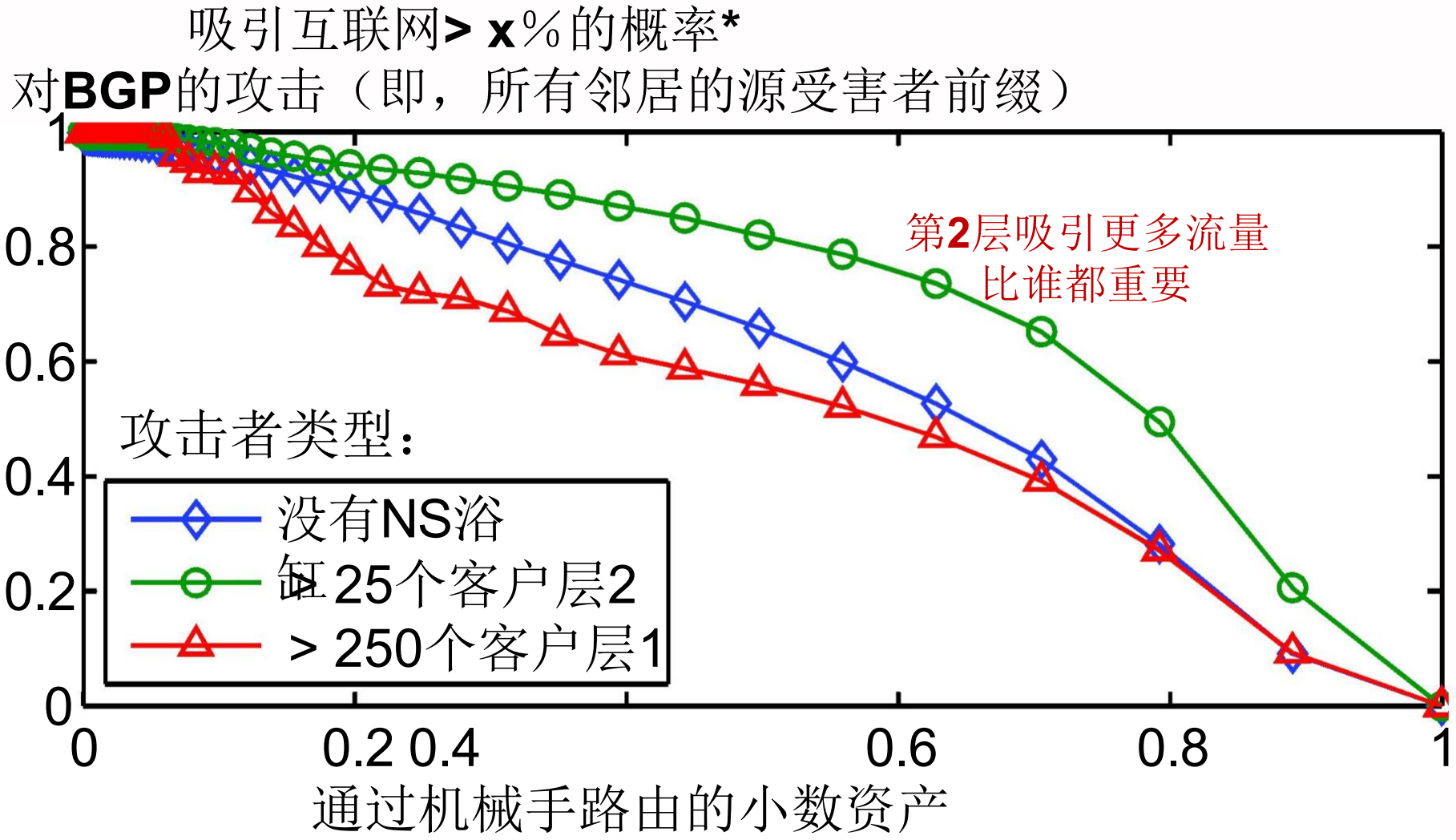
回想一下，智能攻击策略低估了损失。

过滤前缀列表中的存根
不能阻止攻击者
第**1**层和第**2**层。

实际上，下图显示了方法**2**
成为最有效的攻击者。

因此：
过滤不能代替安全
BGP，我们需要结合使用。

第2层是最有效的攻击者



*概率来自不同类别的随机受害者和攻击者

这个演讲

第1部分：**BGP**路由策略模型

第2部分：安全路由协议和攻击

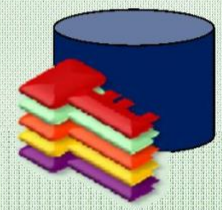
BGP上的前缀劫持

原始身份验证攻击（**RPKI**）

使用安全**BGP**路由泄漏

插曲：找到最佳攻击

通过前缀列表过滤存根攻击



第3部分：仿真结果图

第4部分：结论和启示

带走积分

1）你说的人和你说的话一样重要。

- 安全BGP约束发布的路径
- …但不是出口政策。

2）即使采用**S * -BGP**，防御过滤也至关重要

- S * -BGP防止路径缩短攻击，
- …。但仍然容易受到路由泄漏的影响
- 防御过滤可防止存根攻击
- …，但仍然容易受到等级1和等级2的攻击
- ...最有效

需要结合使用前缀列表过滤和**S * BGP**

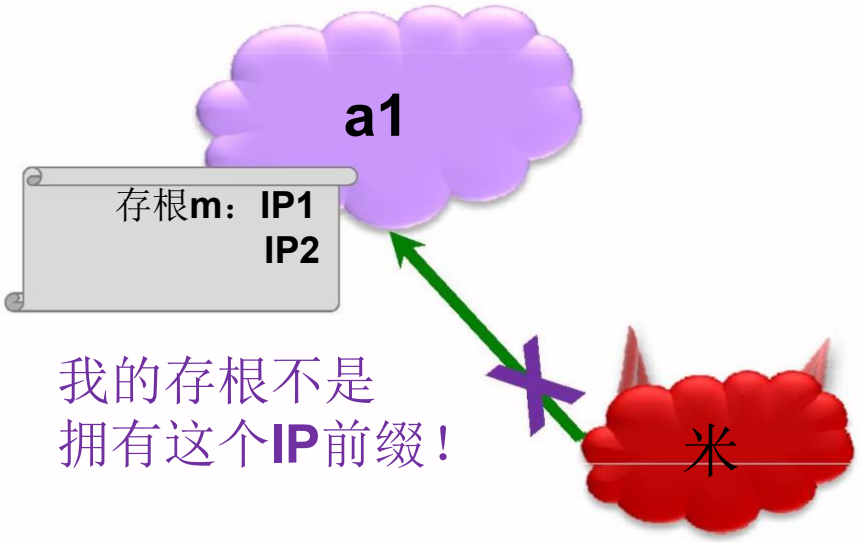
对前缀列表实施过滤

今日：本地提供商
维护其前缀列表。

实施不完善。

为什么呢依靠利他主义

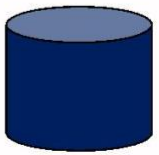
此外，其他AS必须信任
每个提供商都有适当的
实现的前缀列表。



维护前缀列表很烦人。

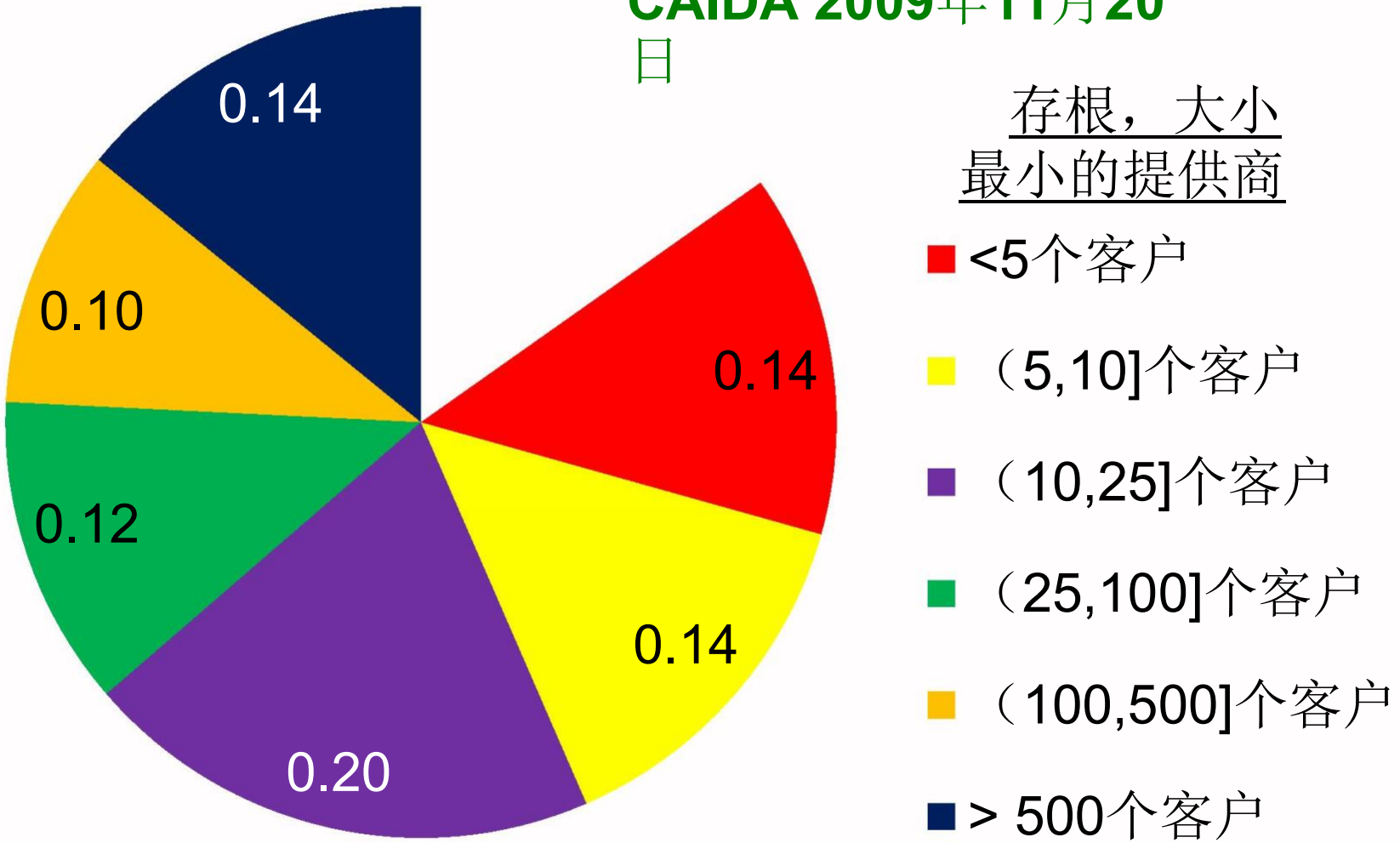
为什么不使用**RPKI / ROA**派生前缀列表？

RPKI / ROA：安全的数据库



如果只有大型自治系统实现前缀列表怎么办？ （1）

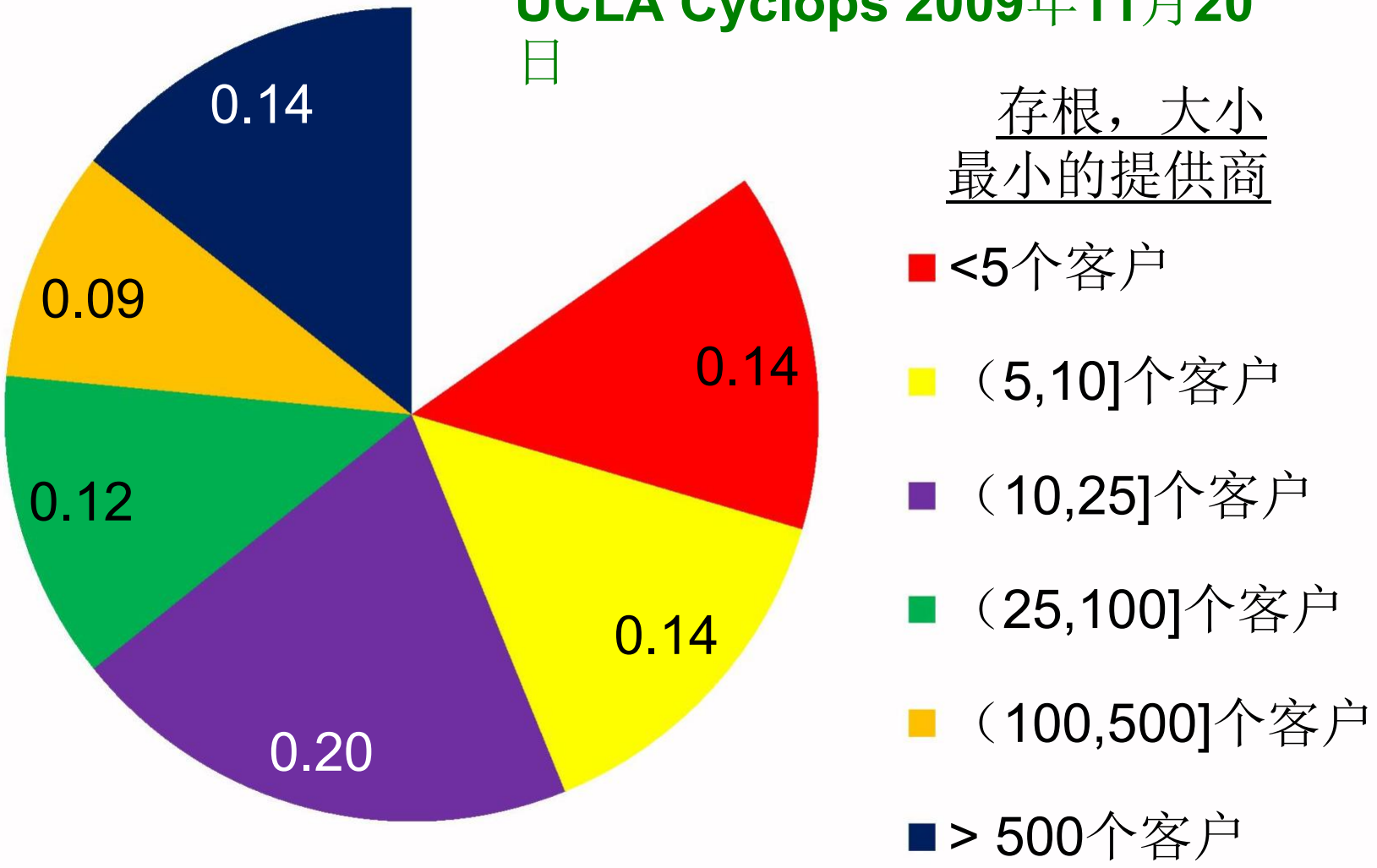
CAIDA 2009年11月20日



如果有**10**个以上客户的**ISP**过滤，将停止**56**%的攻击。

如果只有大型自治系统实现前缀列表怎么办？（2）

UCLA Cyclops 2009年11月20日



如果有**10**个以上客户的**ISP**进行过滤，将停止**55**%的攻击。

这项工作也将出现在

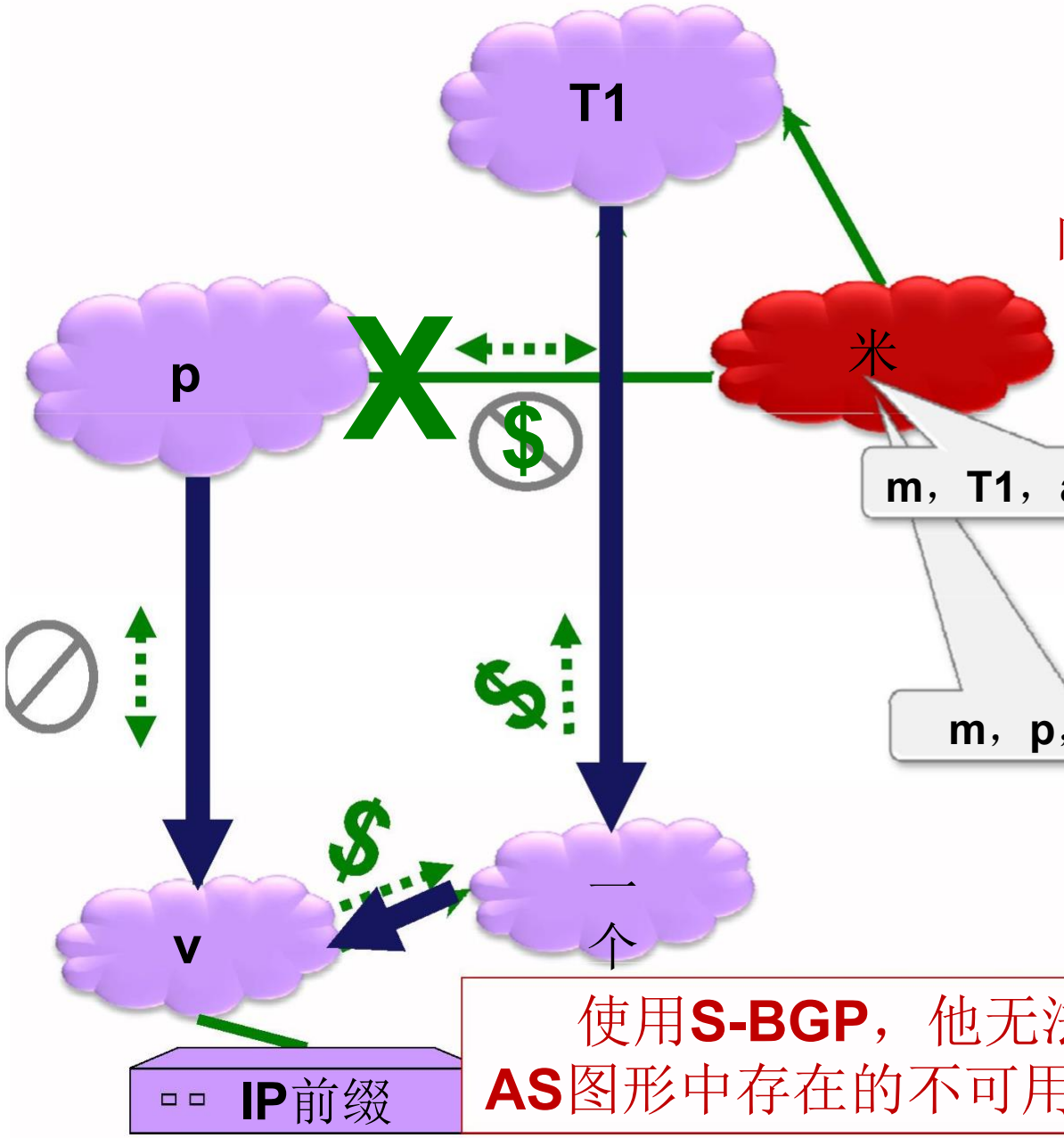
SIGCOMM'10

完整报告可在以下网站获得：

https://www.cs.bu.edu/~goldbe

goldbe@cs.bu.edu

因此，针对目标攻击，BGP比S-BGP更弱



现在，哪条路
攻击者应该
向其他人宣布
互联网？

m，T1，a，v，前缀

4跳
可用
吸引2%的ASes

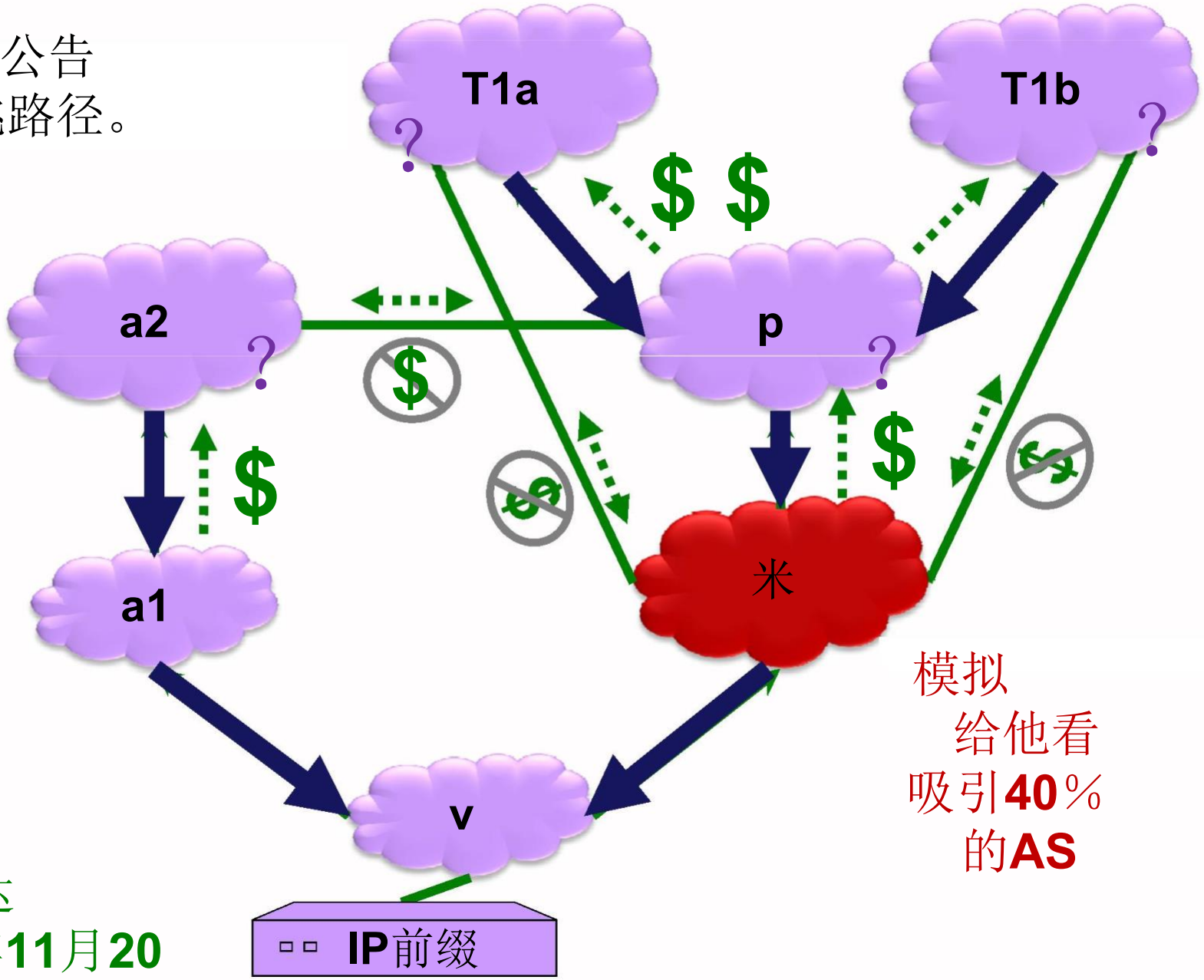
m，p，v，前缀

3跳
不可用
吸引10%的ASes

使用S-BGP，他无法宣布
AS图形中存在的不可用路径。

减少出口吸引更多人（1）！

Teir 1的公告
4跳路径。

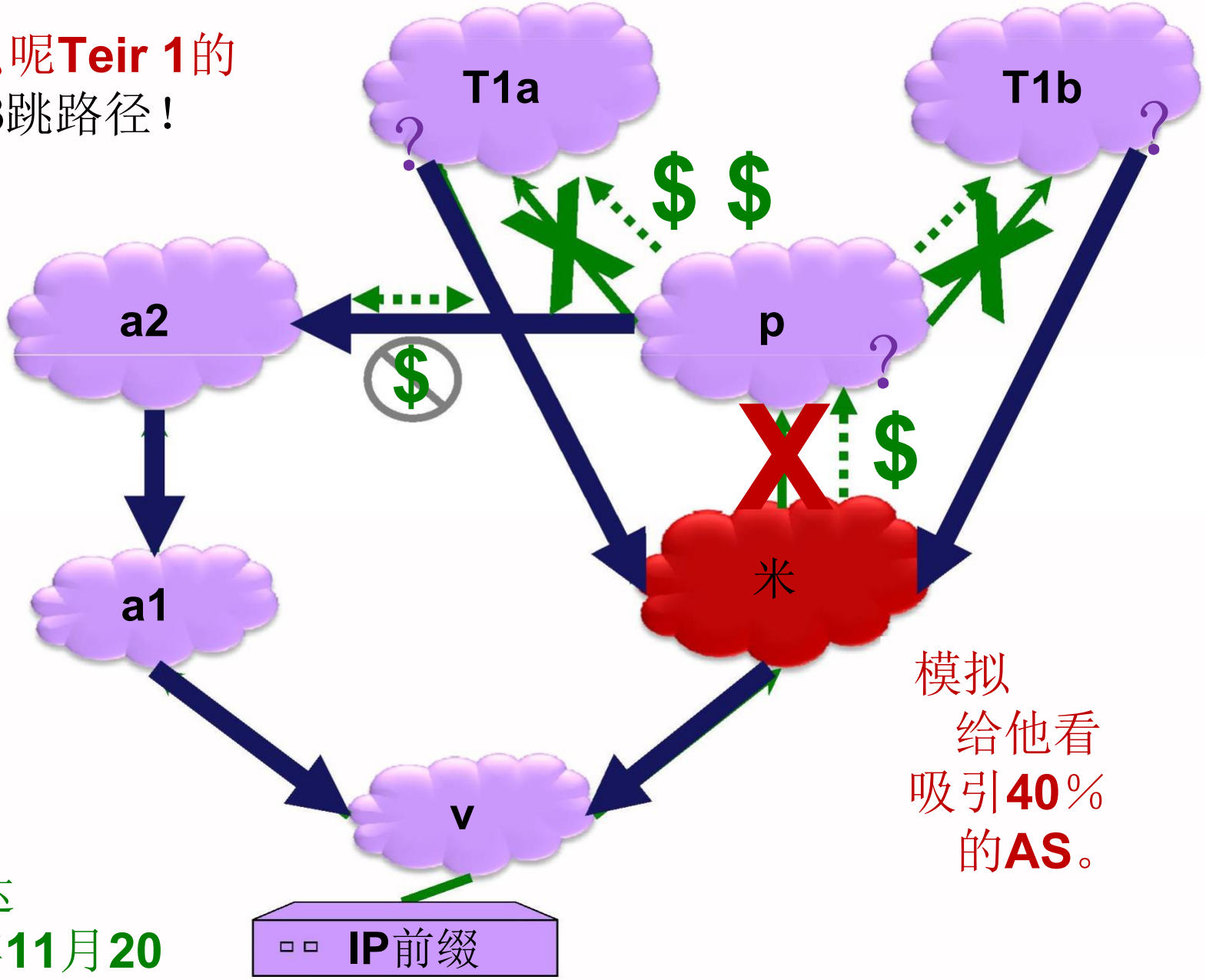


模拟
给他看
吸引**40**%
的**AS**

凯达
2009年**11**月**20**日

减少出口吸引更多人（2）！

为什么呢**Teir 1**的
使用**3**跳路径！



模拟
给他看
吸引**40**%
的**AS**。

凯达
2009年**11**月**20**日

当今互联网路由的安全性如何？ （1）

2008年2月：巴基斯坦电信劫持了YouTube