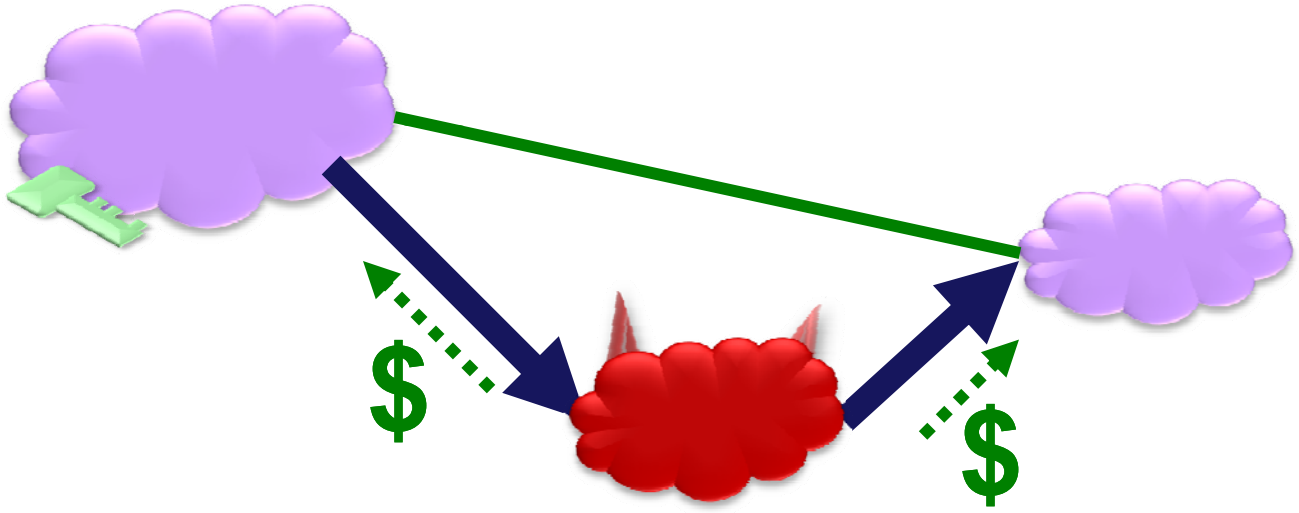
NANOG 49, San Francisco
Tuesday June 15 2010

How Secure are BGP Security Protocols?



Sharon Goldberg
Microsoft Research & Boston University

Michael Schapira
Yale & Berkeley

Pete Hummon
AT&T Research

Jennifer Rexford
Princeton

Overview (1)

"BGP traffic attraction attacks" can cause major problems

- Prefix hijacks causing blackholes, loss of connectivity
- … e.g., Pakistan Telecom / YouTube incident
- BGP "Man-In-The-Middle" attacks
- … e.g., Pilosov & Kapela traffic interception demo

If we had "BGP security" these problems go away…. right?

- Different protocols have different properties.
- Which one is most effective at stopping attacks?
- Can we quantify this? Can we compare them?

Overview (2)

We quantify & compare how well the major "BGP Security" protocols prevent traffic attraction attacks

- origin authentication (ROA/RPKI)
- defensive filtering (prefix lists)
- soBGP
- Secure BGP

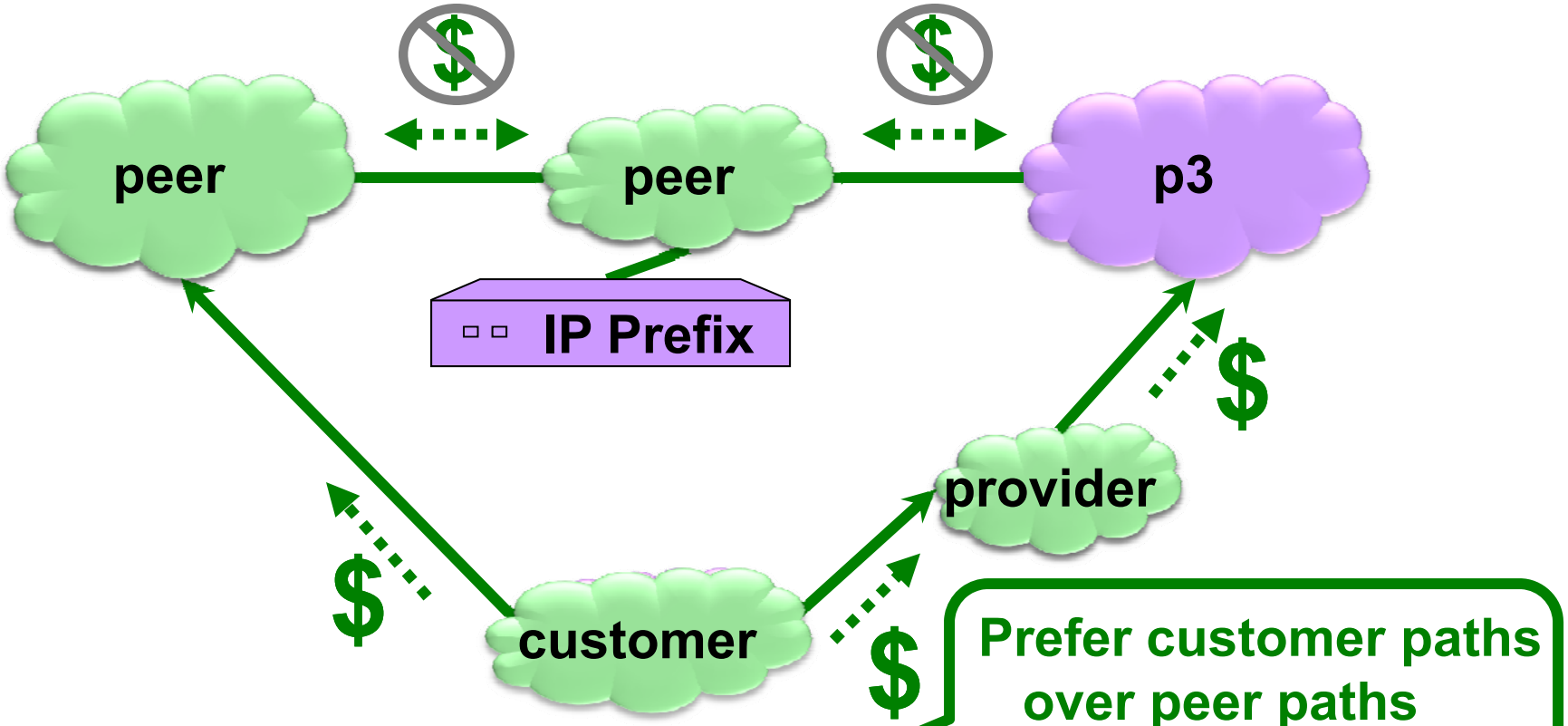
Our approach: Evaluate via simulation on AS topology data.

- Assume a "BGP security" protocol is fully deployed.
- … How much traffic can an attacker attract?

- To determine this, we use a model of BGP routing policies
- … based on the business relationships & AS-path length
- And run simulations on [CAIDA] & [UCLA Cyclops] data
- … (maps of the AS-level Internet w business relationship)

A model for BGP Routing Policies (1)

In order to figure out how traffic would flow as result of an attack, we need to know how each AS chooses paths in BGP
BUT, we don't know exactly how you do this. So we use a model.

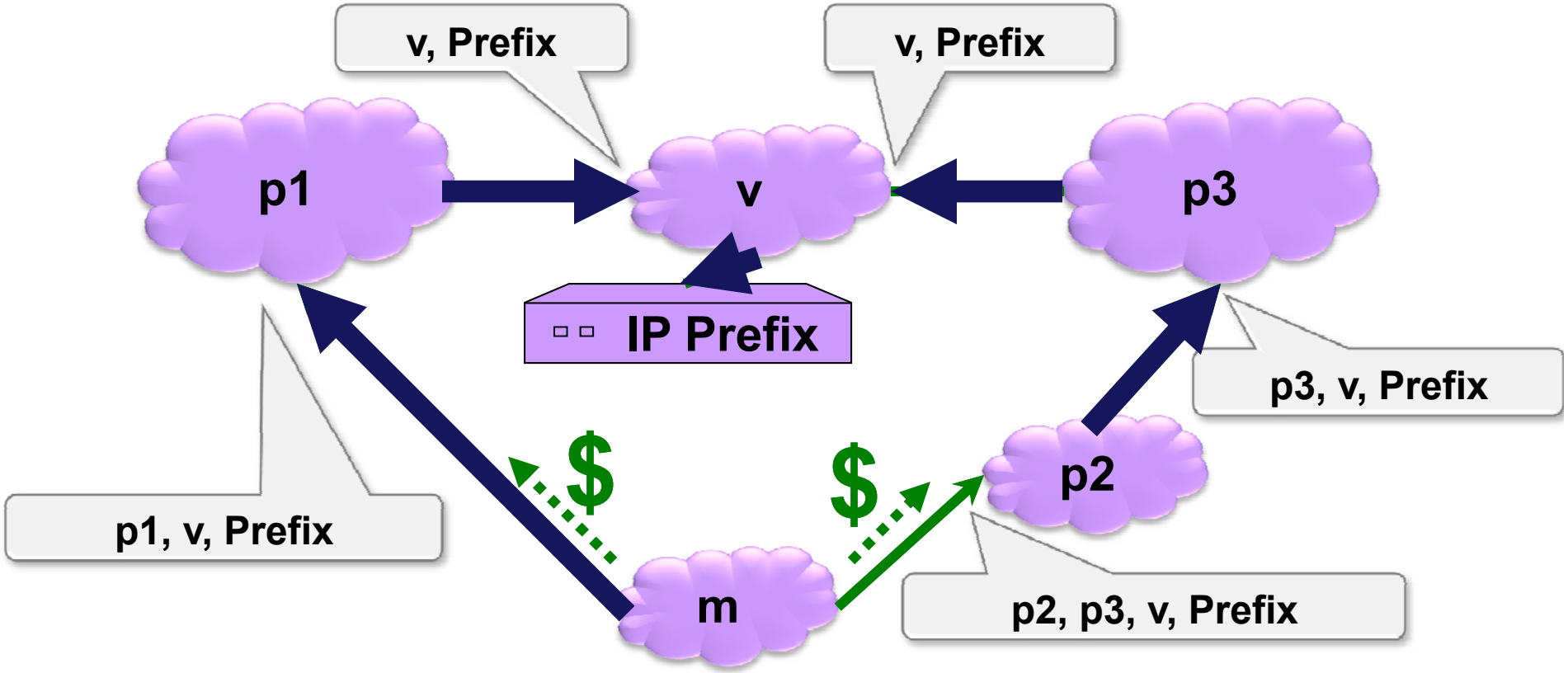


A model of routing policies:

- Prefer cheaper paths. Then, prefer shorter paths.

A model for BGP Routing Policies (2)

In order to figure out how traffic would flow as result of an attack, we need to know how each AS chooses paths in BGP.

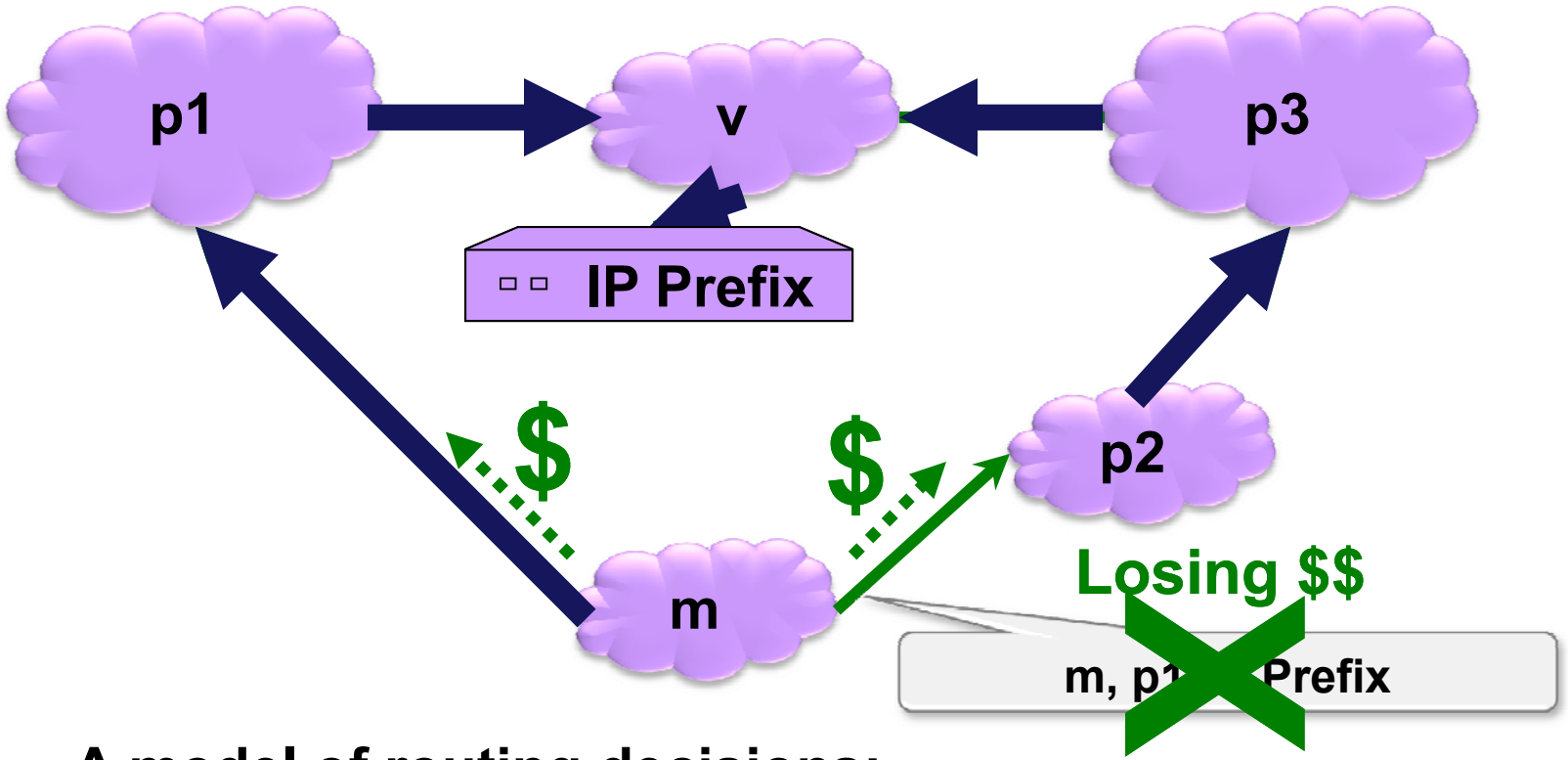


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.

A model for BGP Routing Policies (3)

In order to figure out how traffic would flow as result of an attack, we need to know how each AS chooses paths in BGP.



A model of routing decisions:

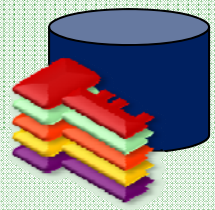
- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

This talk

Part 1: A model of BGP Routing Policies

Part 2: Secure Routing Protocols and Attacks

- Prefix hijacks on BGP
- Attacks on Origin Authentication (RPKI)
- Route Leaks with Secure BGP
- Interlude: Finding the Optimal Attack
- Filtering attacks by stubs via prefix lists



Part 3: Graphs of Simulation Results

Part 4: Conclusions and Implications

I'll start with a single "anonymized" example from CADIA's 11/20/2009 AS relationship data.

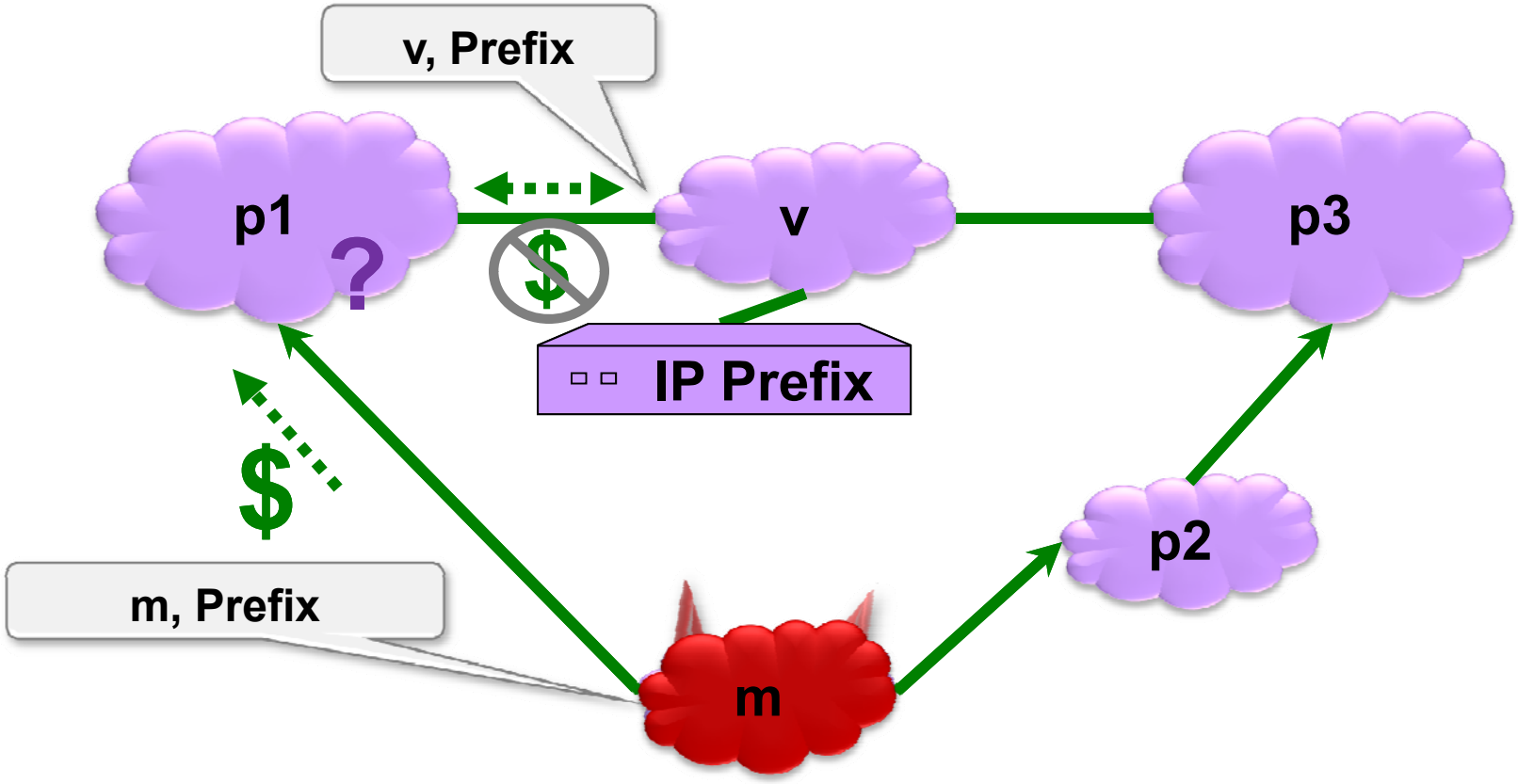
I'll use this example to present possible attacks on each "BGP security" protocol

For now, I'll have have one attacker and one victim

Later I'll consider multiple (attacker, victim) pairs

Traffic Attraction Attacks

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

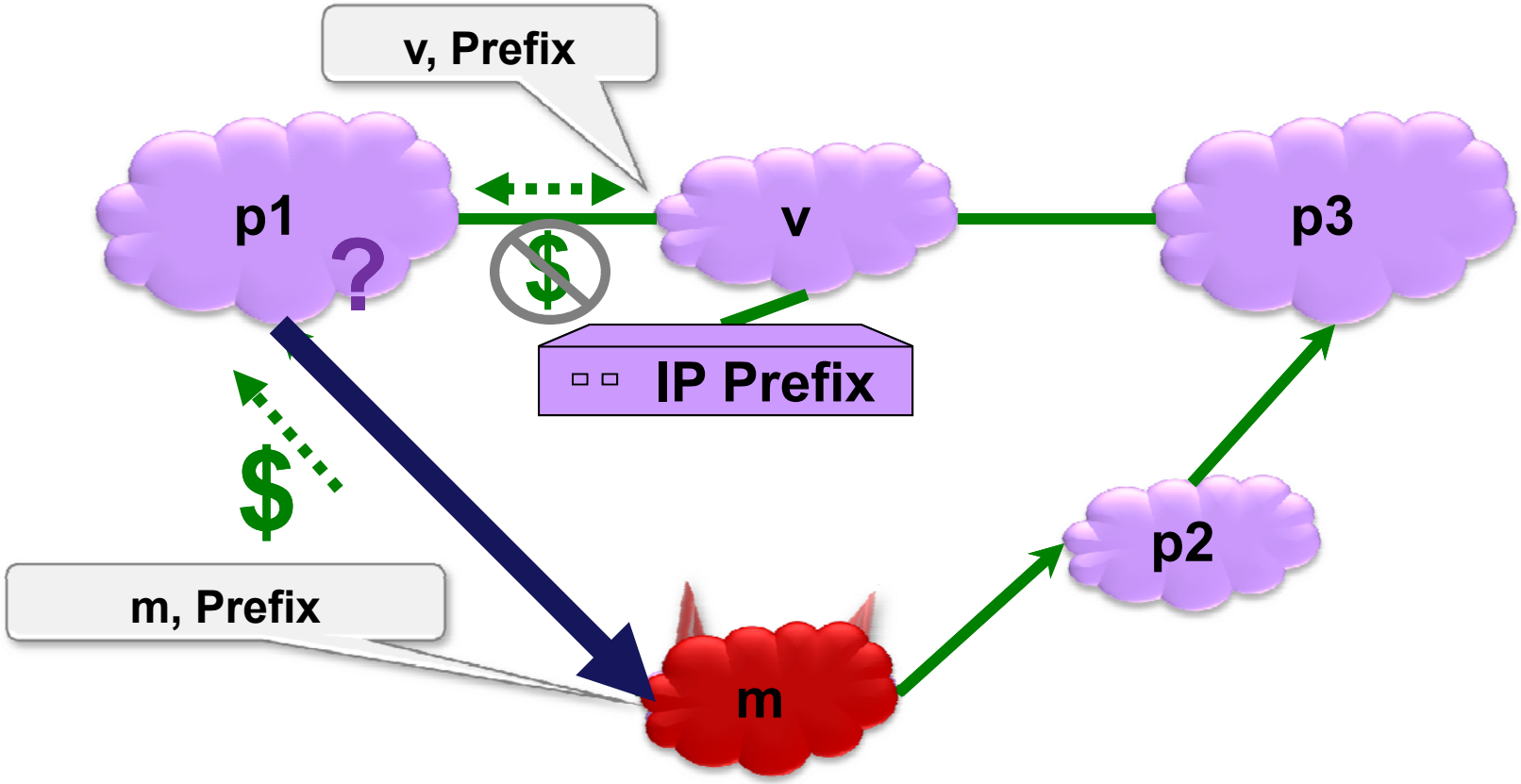


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

Traffic Attraction Attacks

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

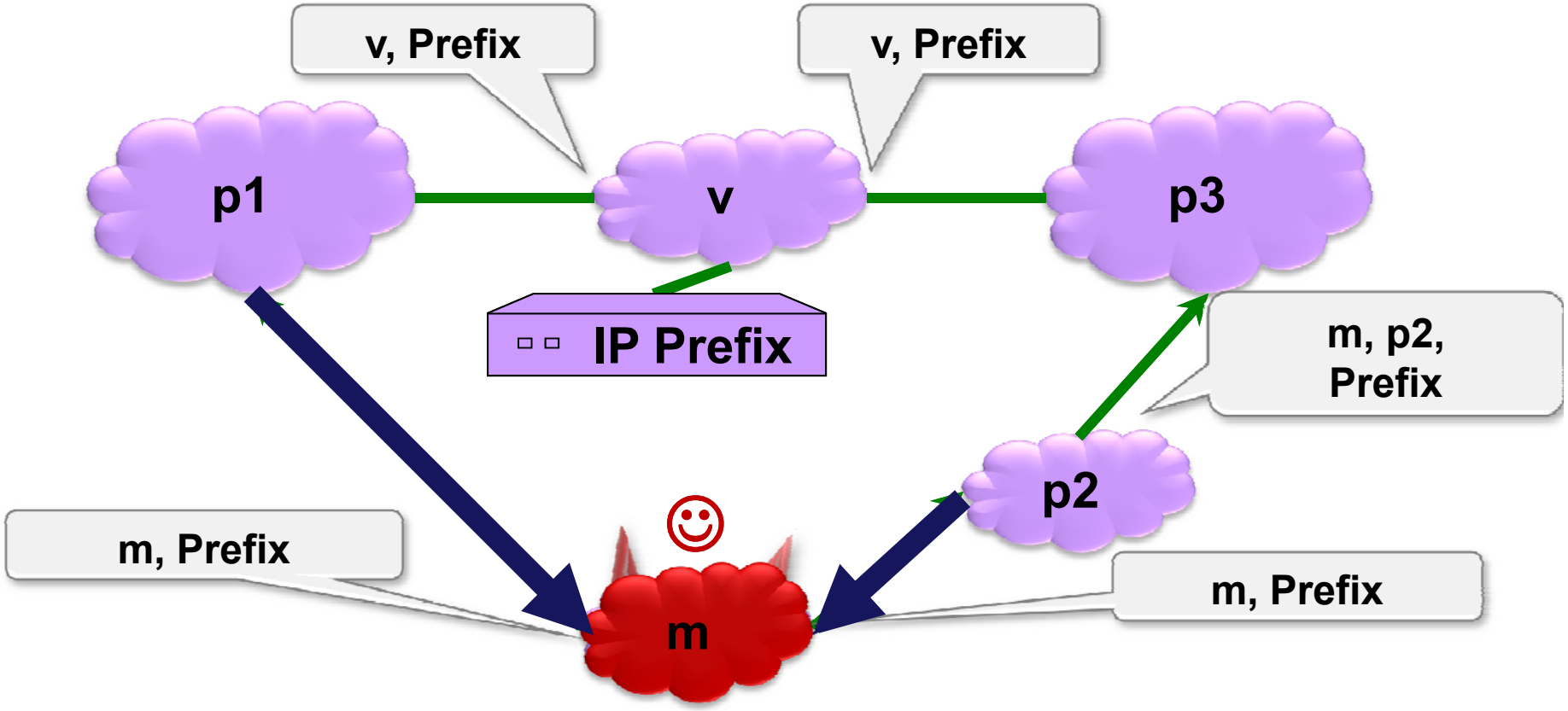


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

Traffic Attraction Attacks

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

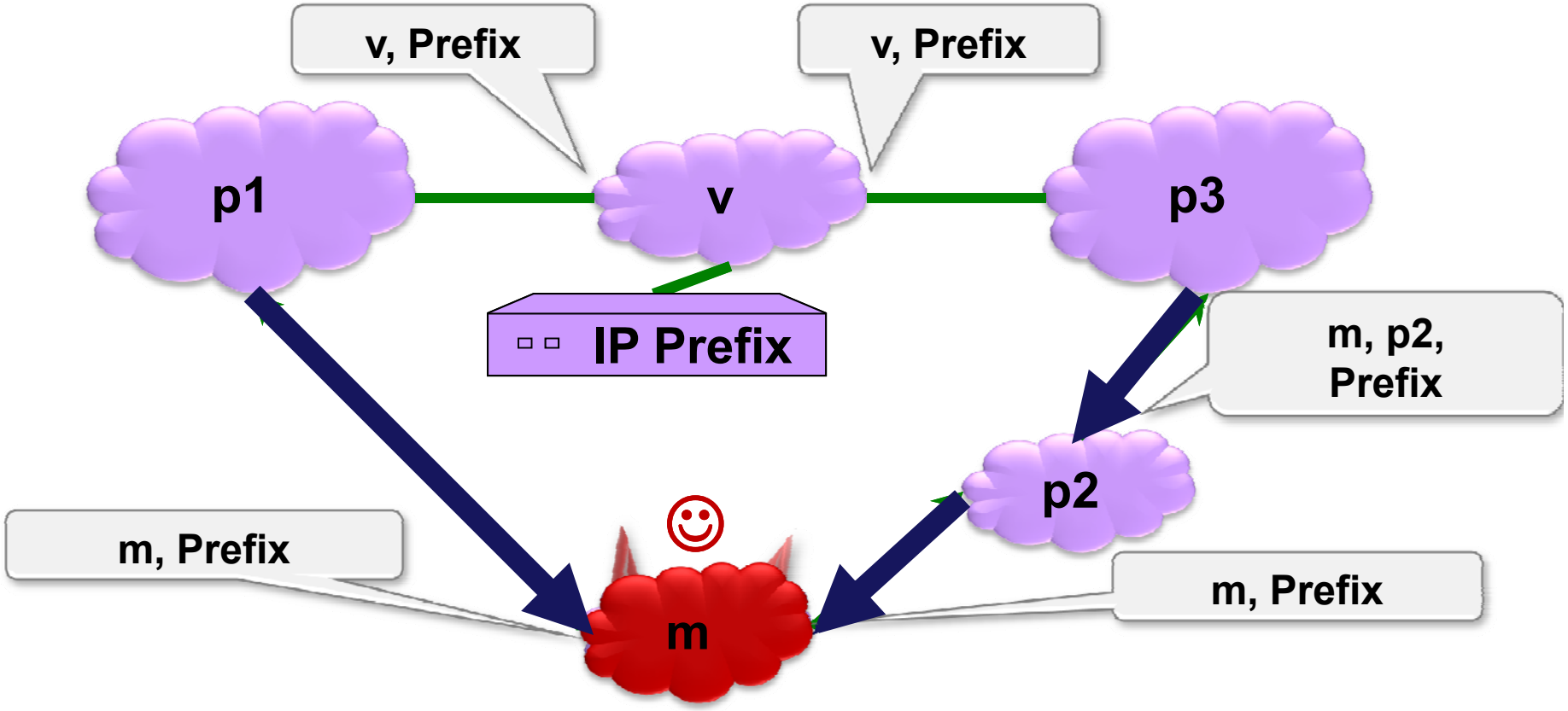


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

Traffic Attraction Attacks

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)

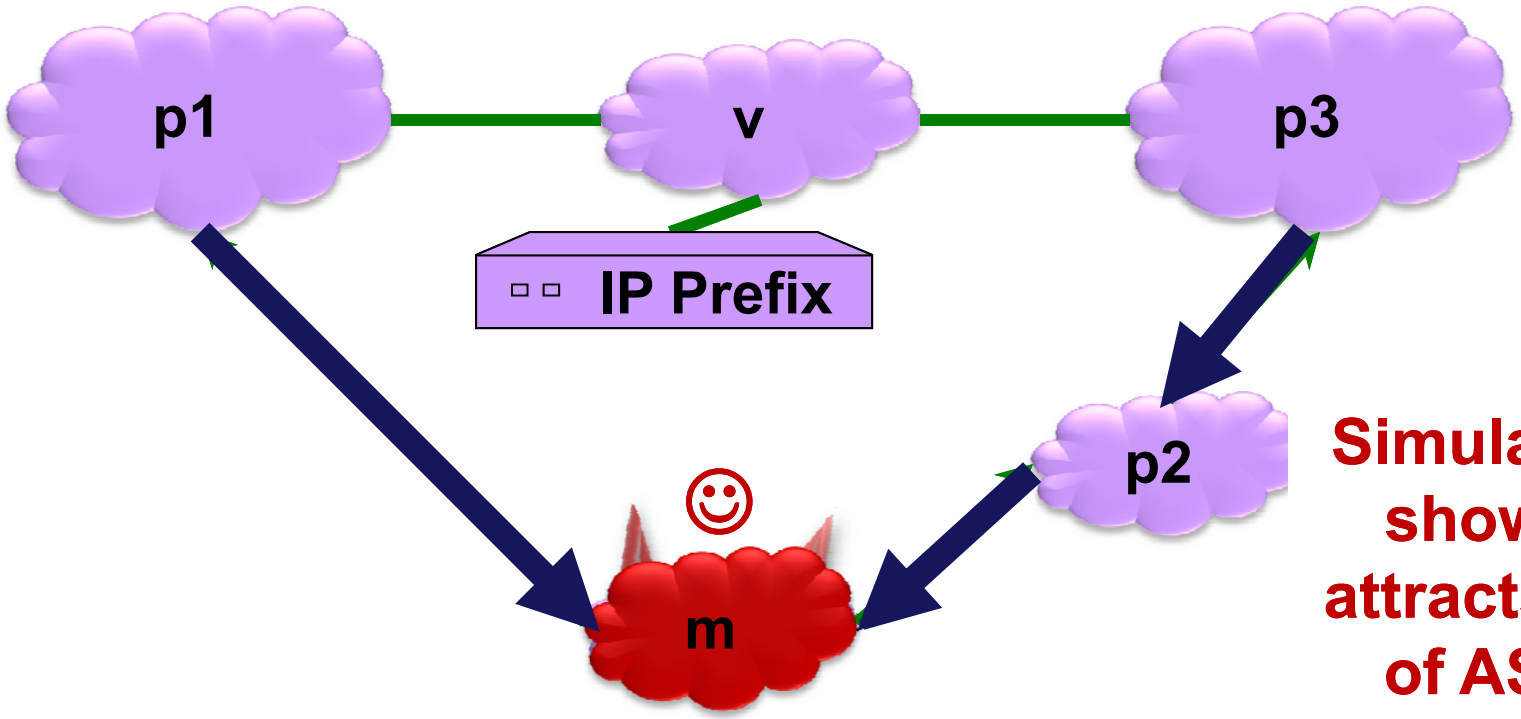


A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

Traffic Attraction Attacks

Attacker wants max number of ASes to route thru its network.
(For eavesdropping, dropping, tampering, …)



Simulations show he attracts 62% of ASes!

A model of routing decisions:

- Prefer cheaper paths. Then, prefer shorter paths.
- Only transit traffic if it earns you money, ie. for customers.

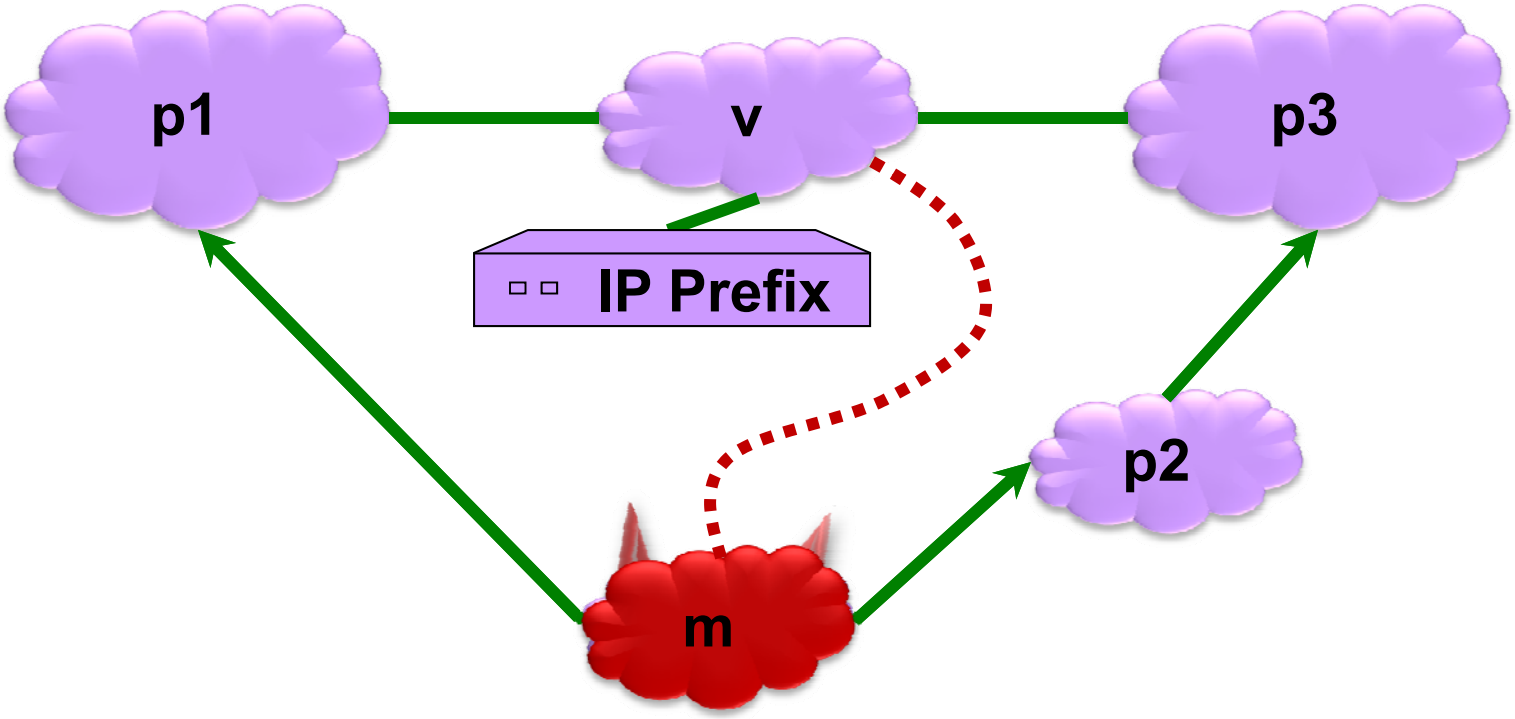
The attack we just saw could have been prevented with origin authentication (ROA/RPKI).

Now, suppose we had ROA/RKPI.
Can the attacker still launch an attack?

(Yes)

Security Mechanism: Origin Authentication RPKI/ROA

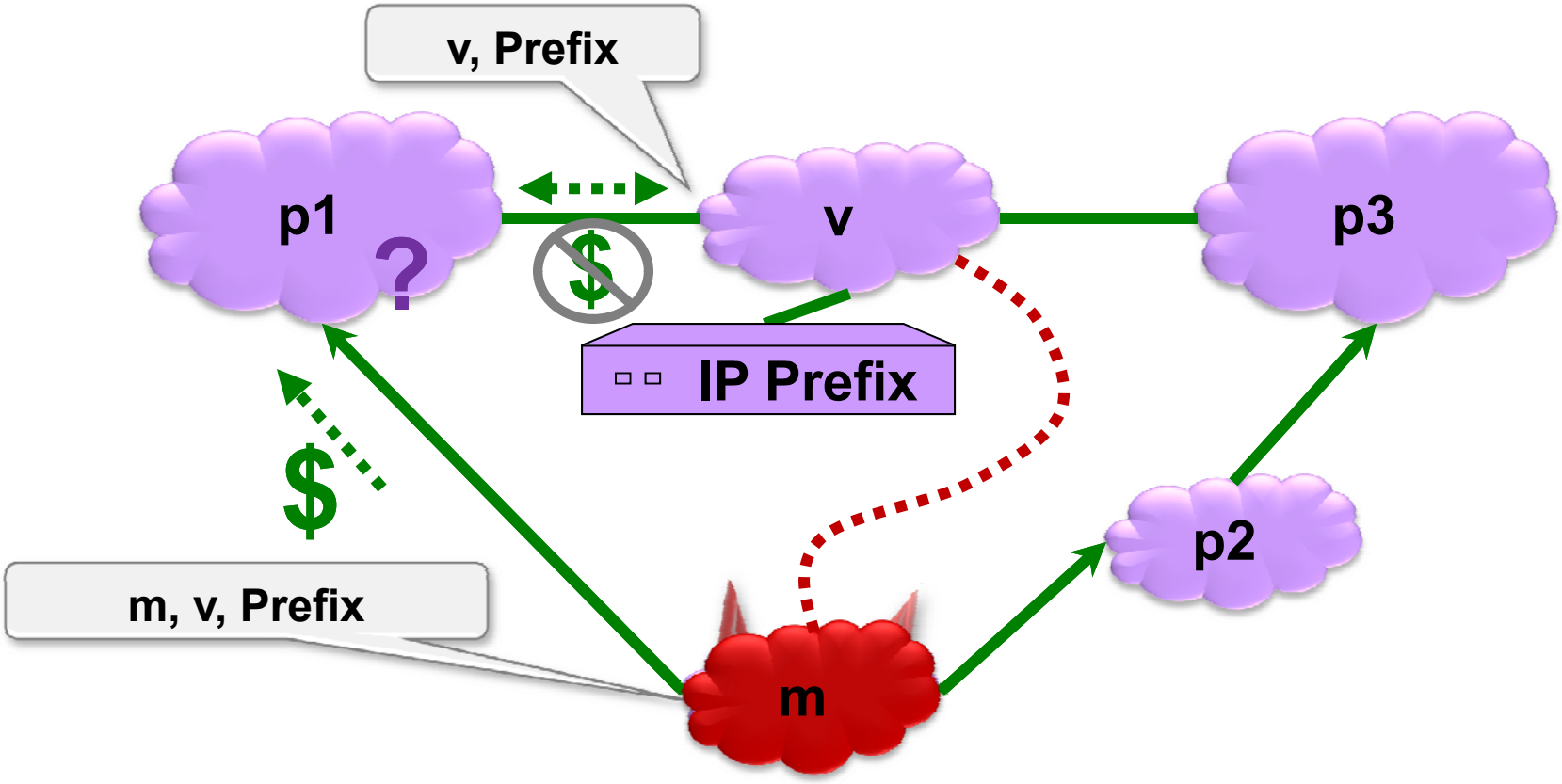
A secure database that maps IP Prefixes to owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication RPKI/ROA

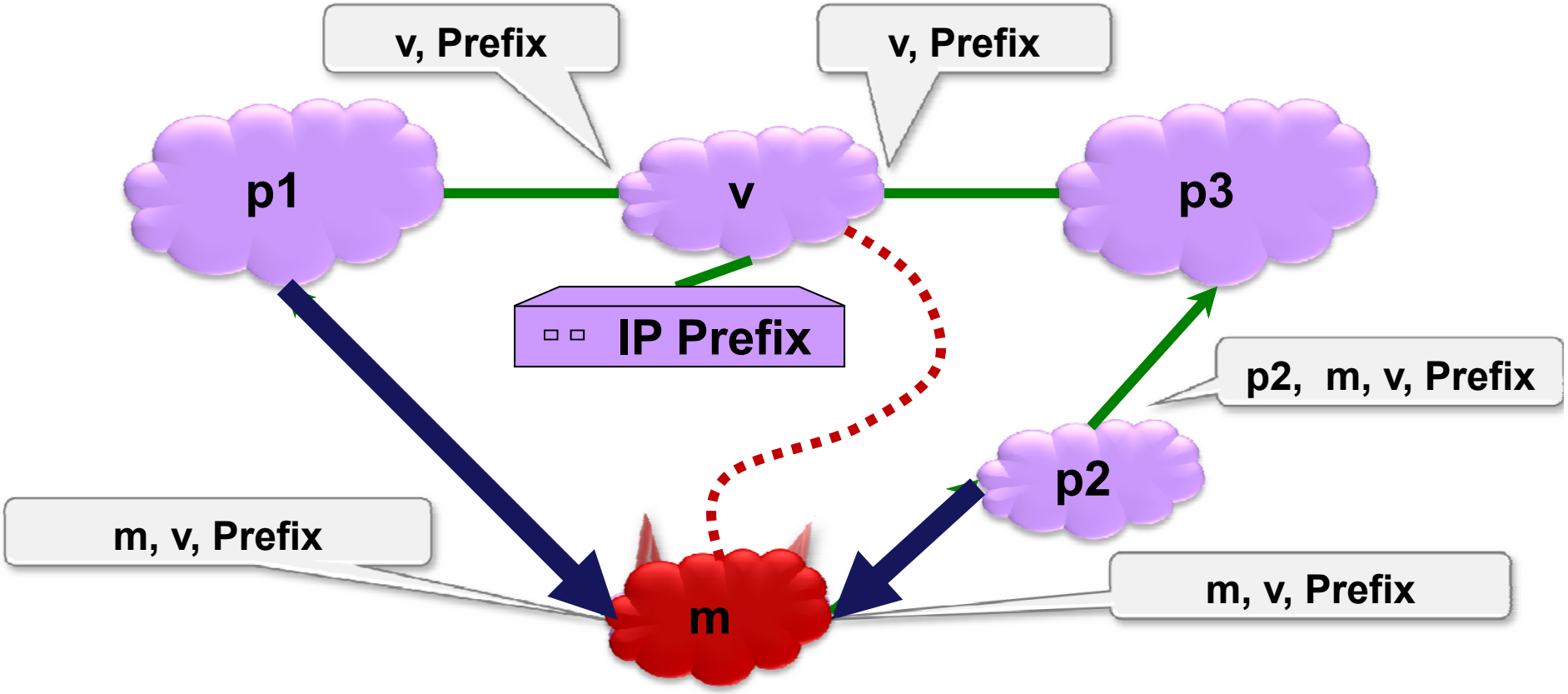
A secure database that maps IP Prefixes to owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication RPKI/ROA

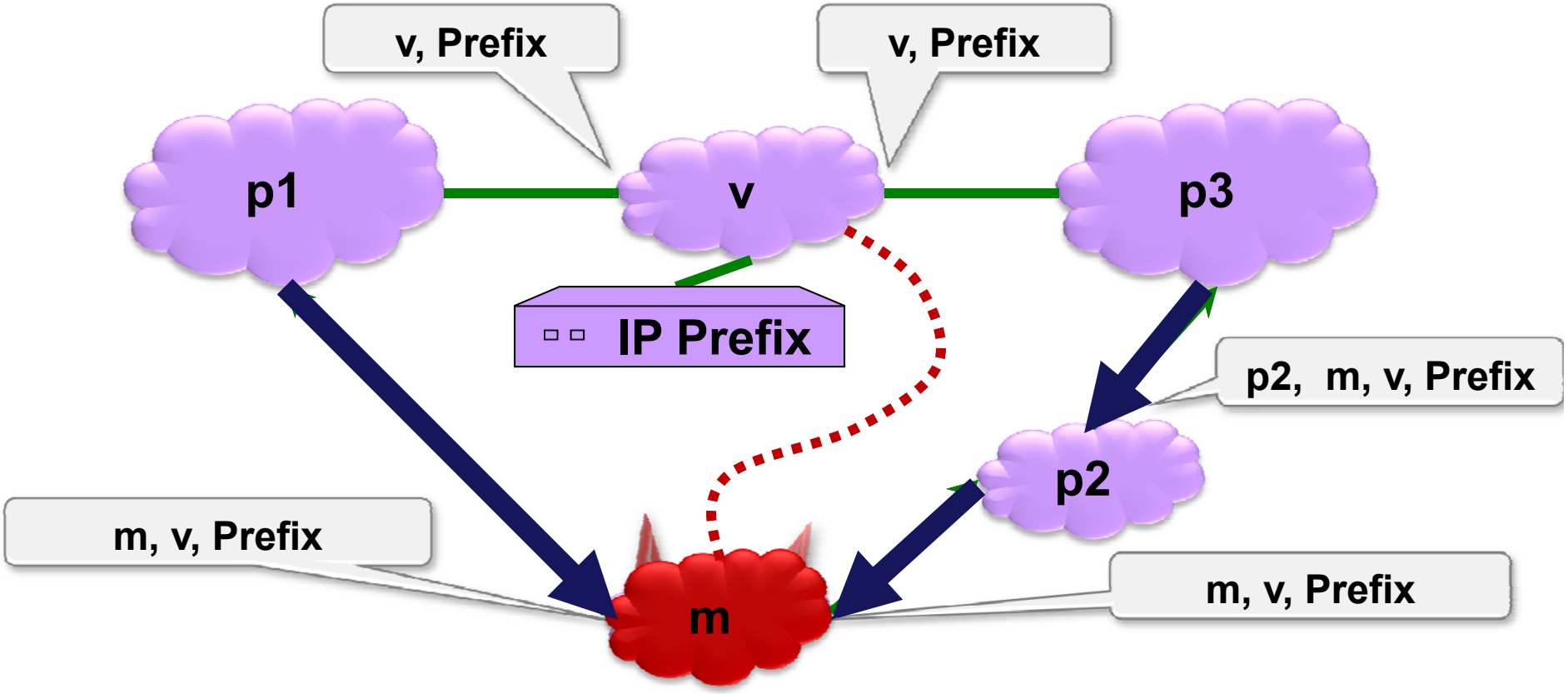
A secure database that maps IP Prefixes to owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication RPKI/ROA

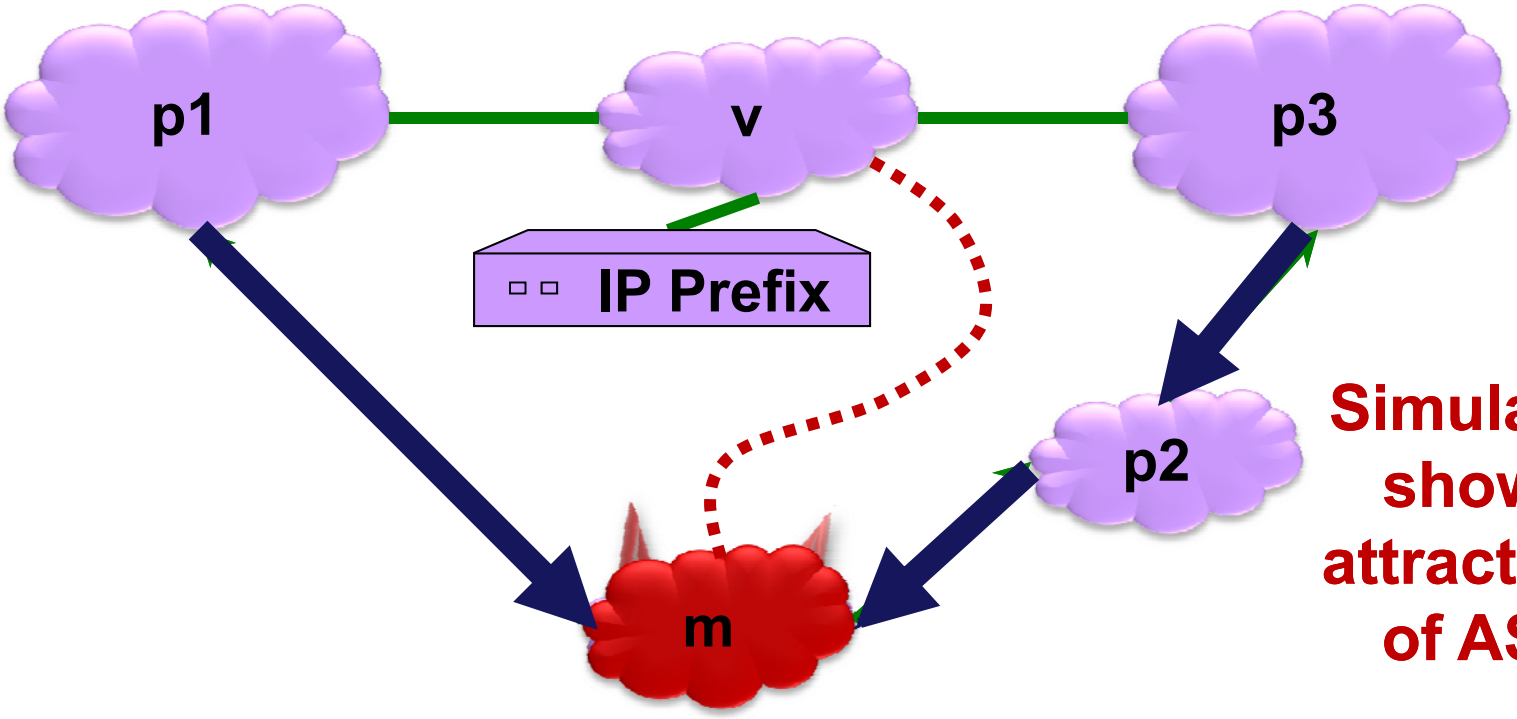
A secure database that maps IP Prefixes to owner ASes.



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Security Mechanism: Origin Authentication RPKI/ROA

A secure database that maps IP Prefixes to owner ASes.



Simulations show he attracts 58% of ASes!

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

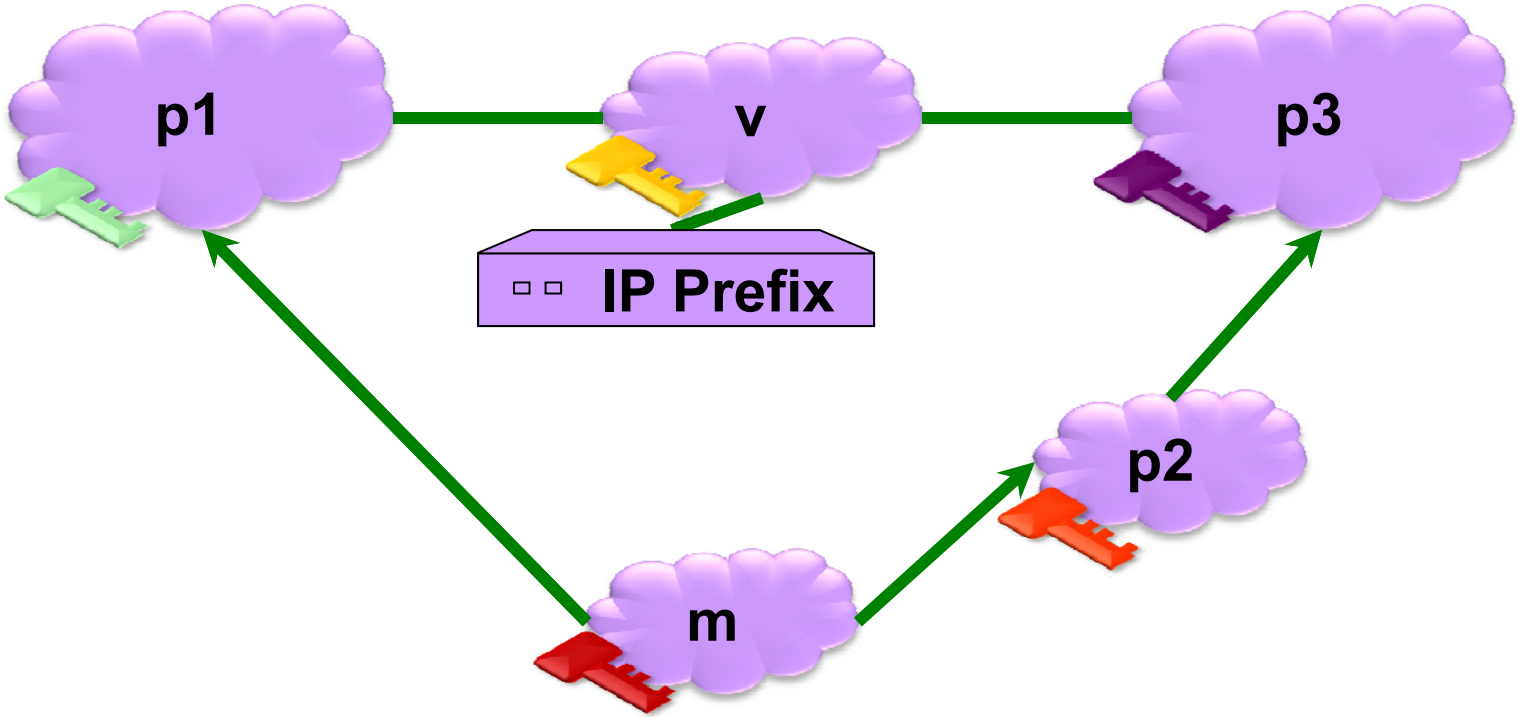
The attack we just saw could have been prevented with soBGP or Secure BGP.

Now, suppose we had Secure BGP.
Can the attacker still launch an attack?

(Yes, using route leaks)

Security Mechanism: "Secure BGP" [KLS98]

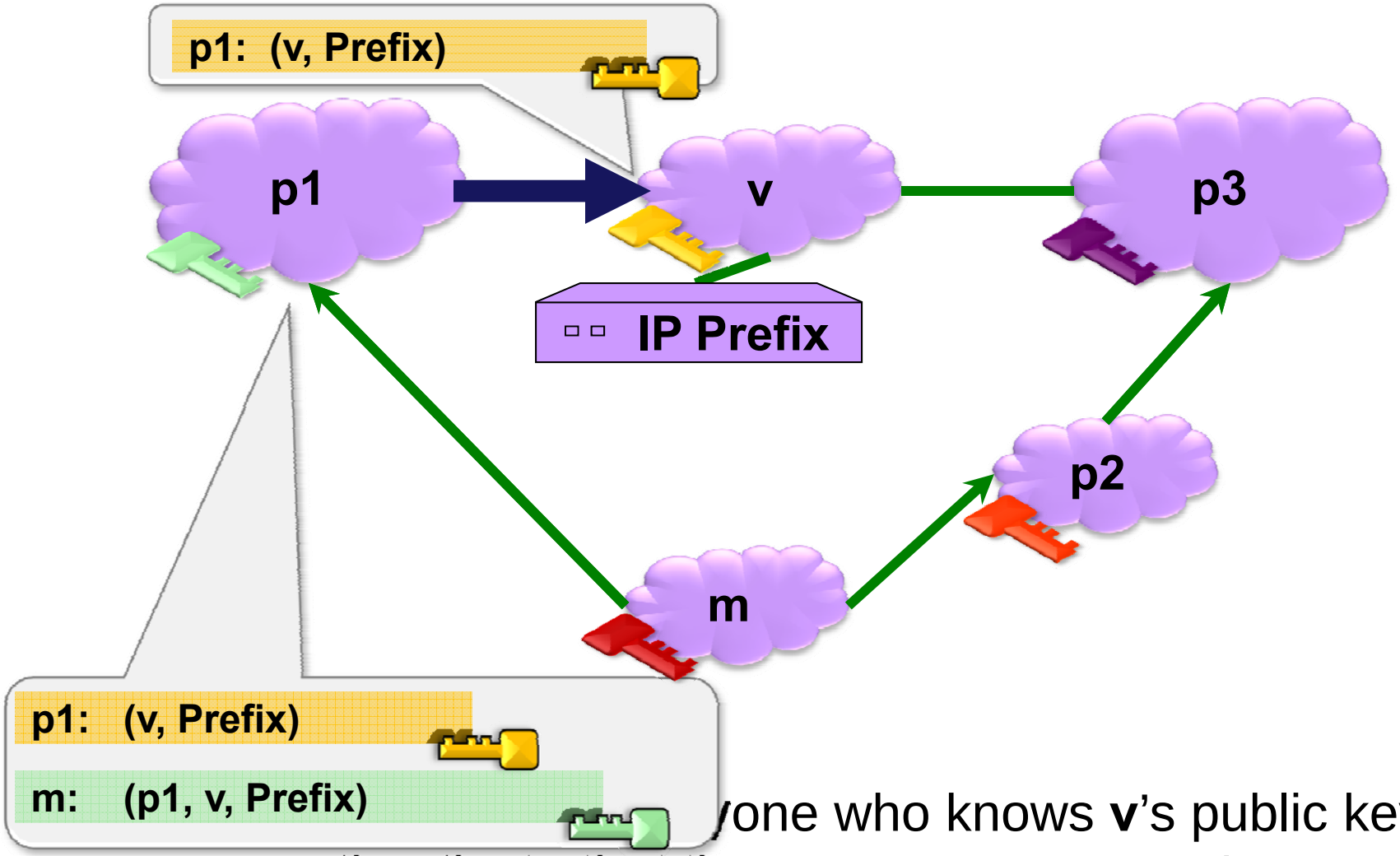
Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



Public Key Signature: Anyone who knows **v**'s public key can authenticate that the message was sent by **v**.

Security Mechanism: "Secure BGP" [KLS98]

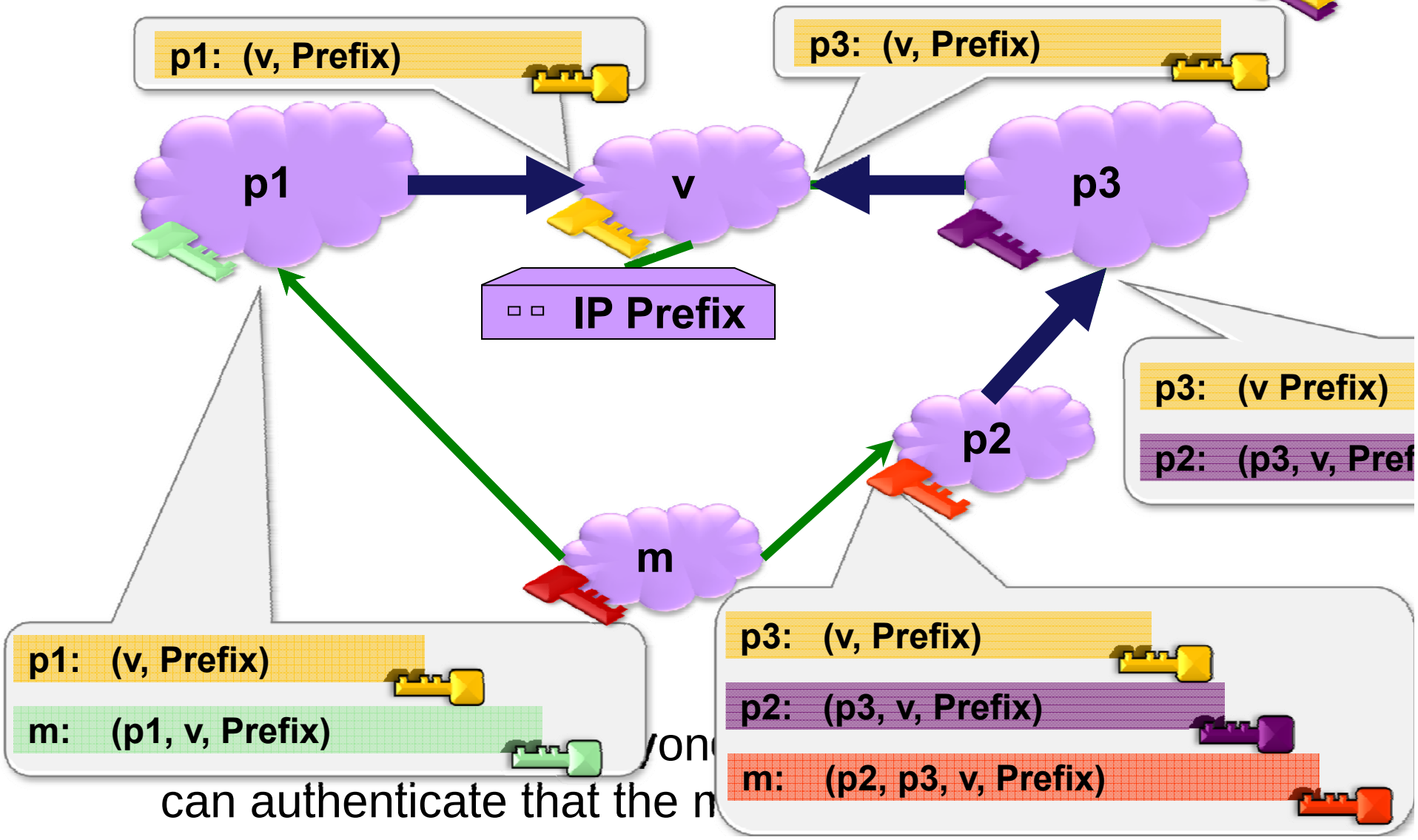
Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



/one who knows **v**'s public key can authenticate that the message was sent by **v**.

Security Mechanism: "Secure BGP" [KLS98]

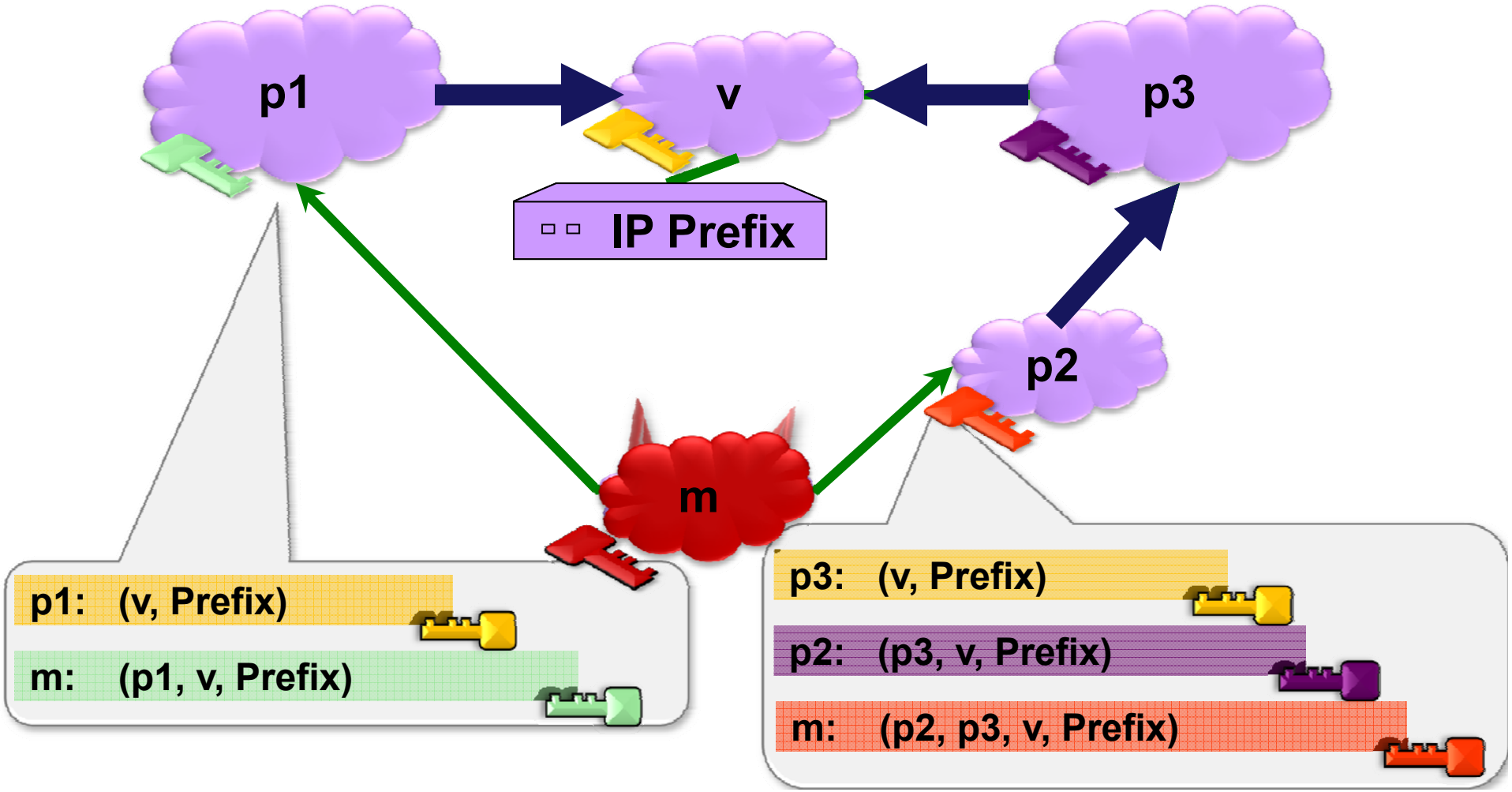
Secure BGP: Origin Authentication +
Cannot announce a path that was not announced to you.



can authenticate that the m

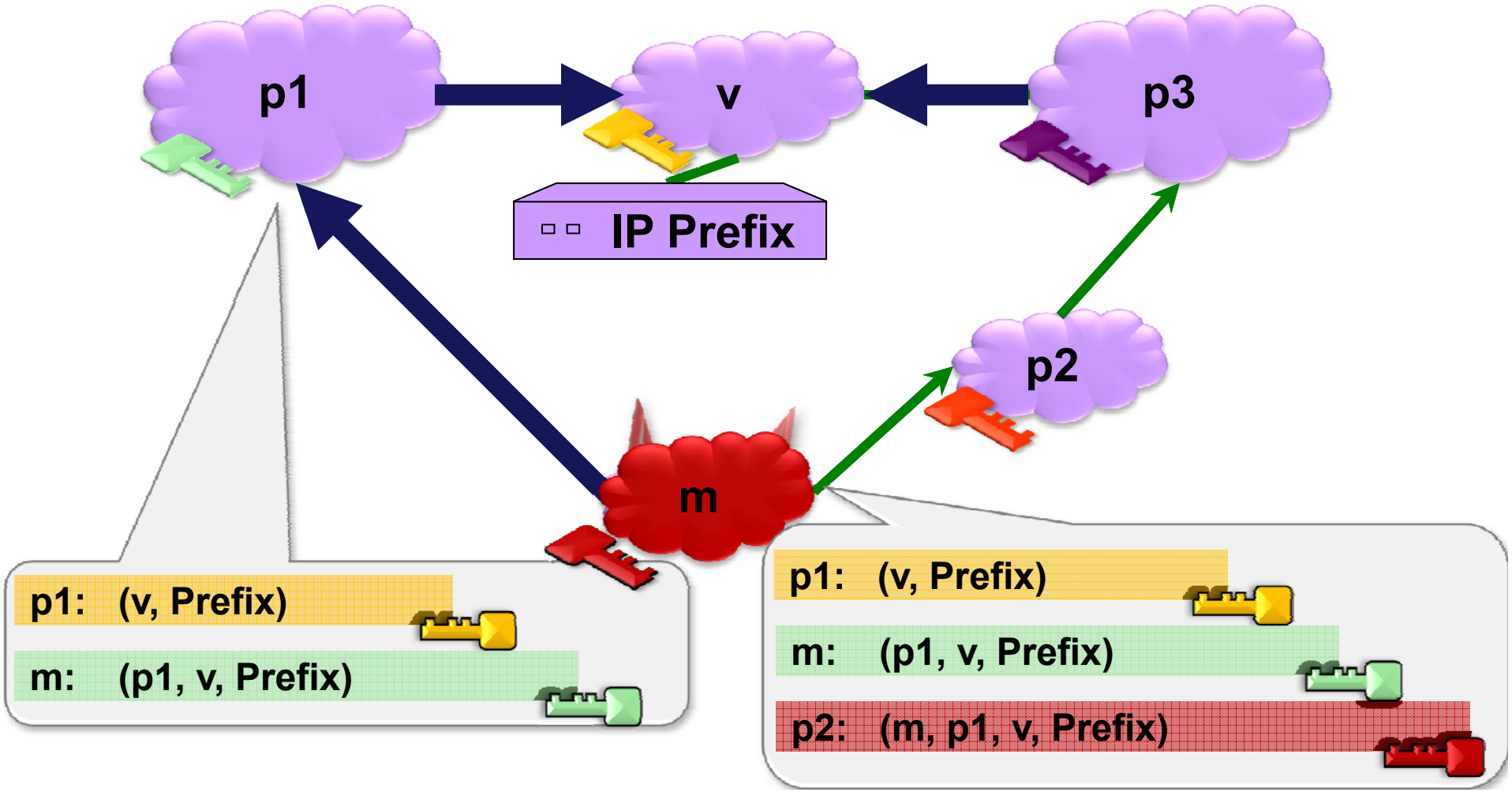
Are attacks still possible with Secure BGP? (1)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



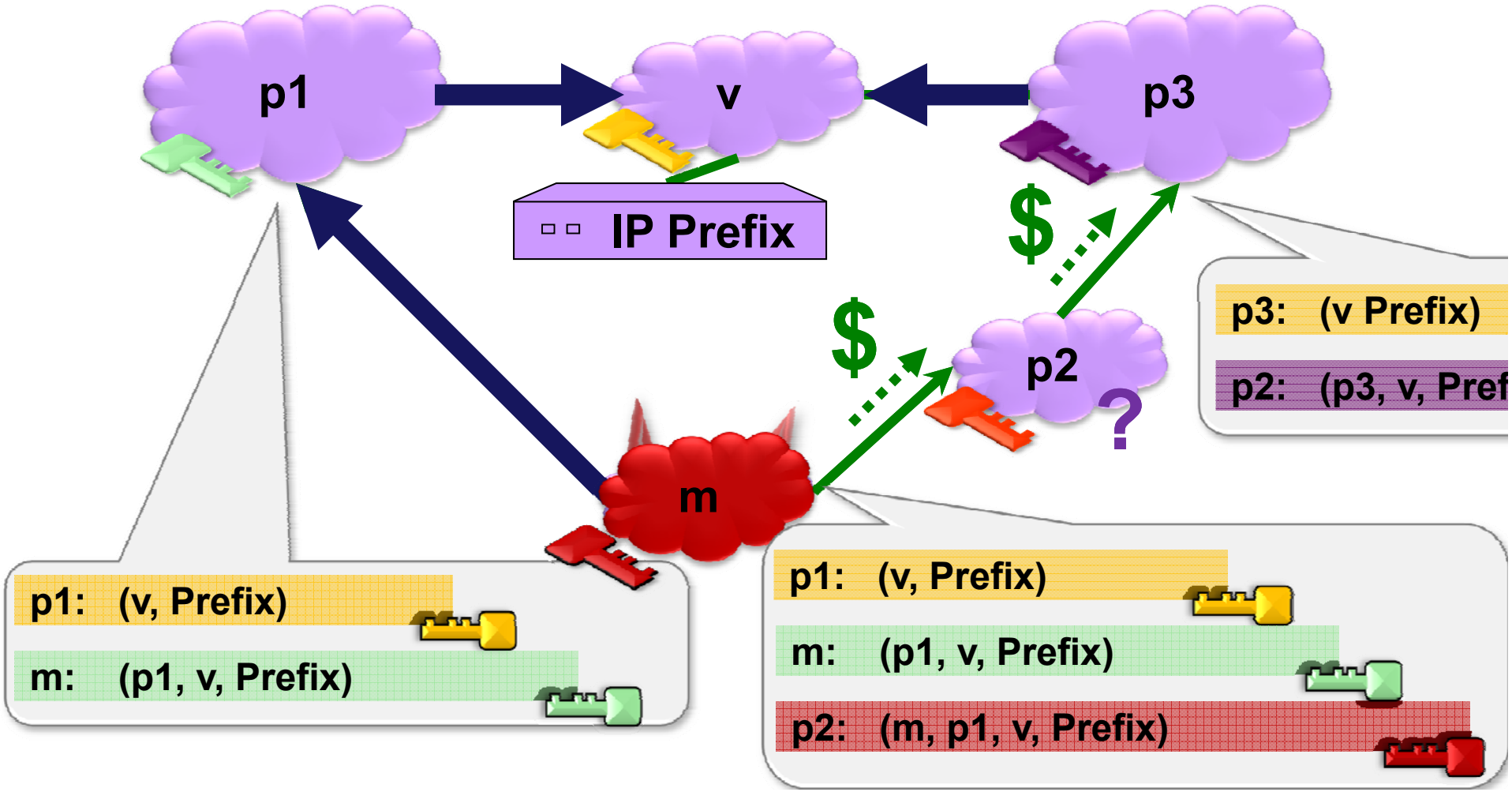
Are attacks still possible with Secure BGP? (2)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



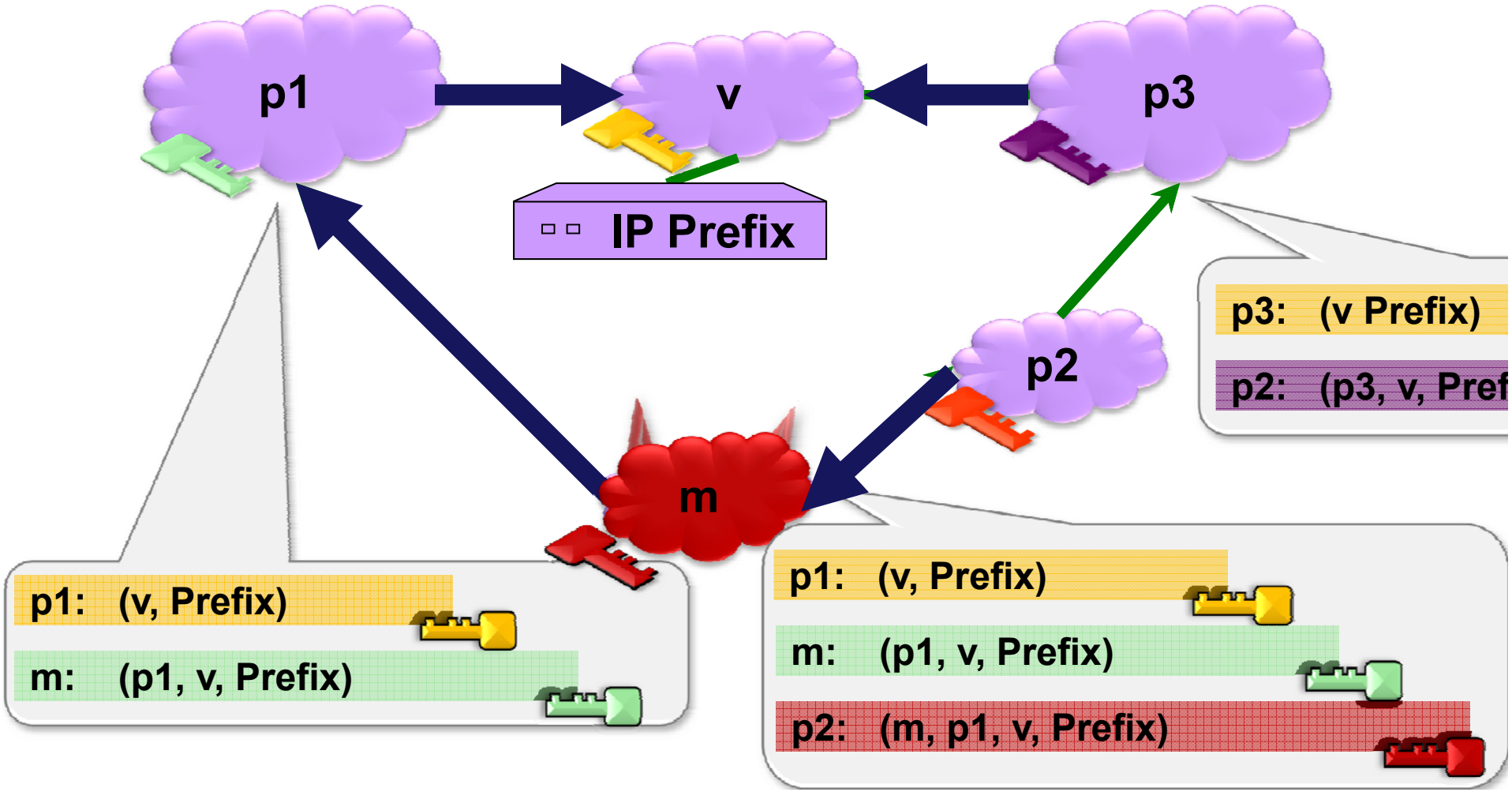
Are attacks still possible with Secure BGP? (2)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



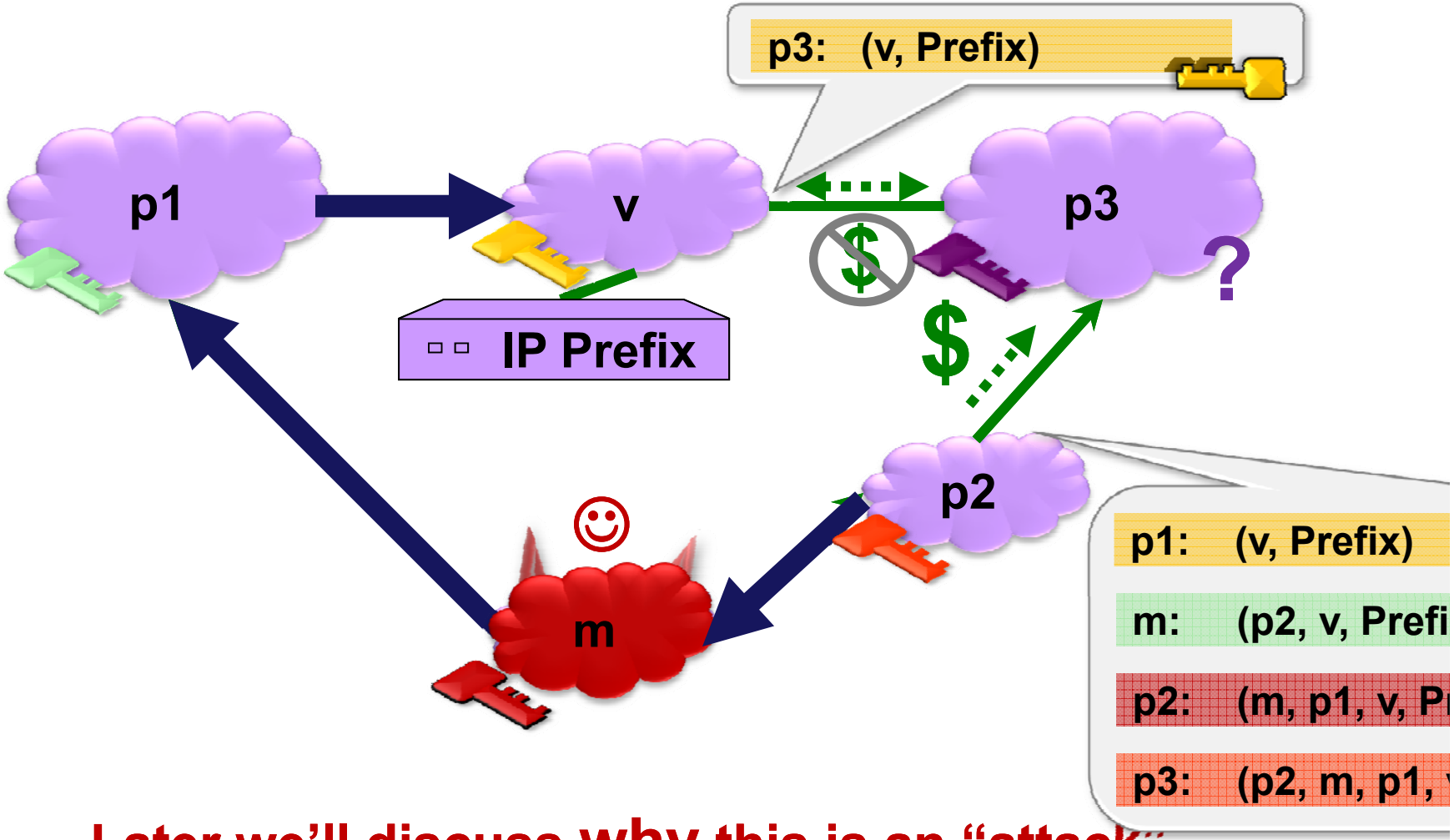
Are attacks still possible with Secure BGP? (2)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Are attacks still possible with Secure BGP? (3)

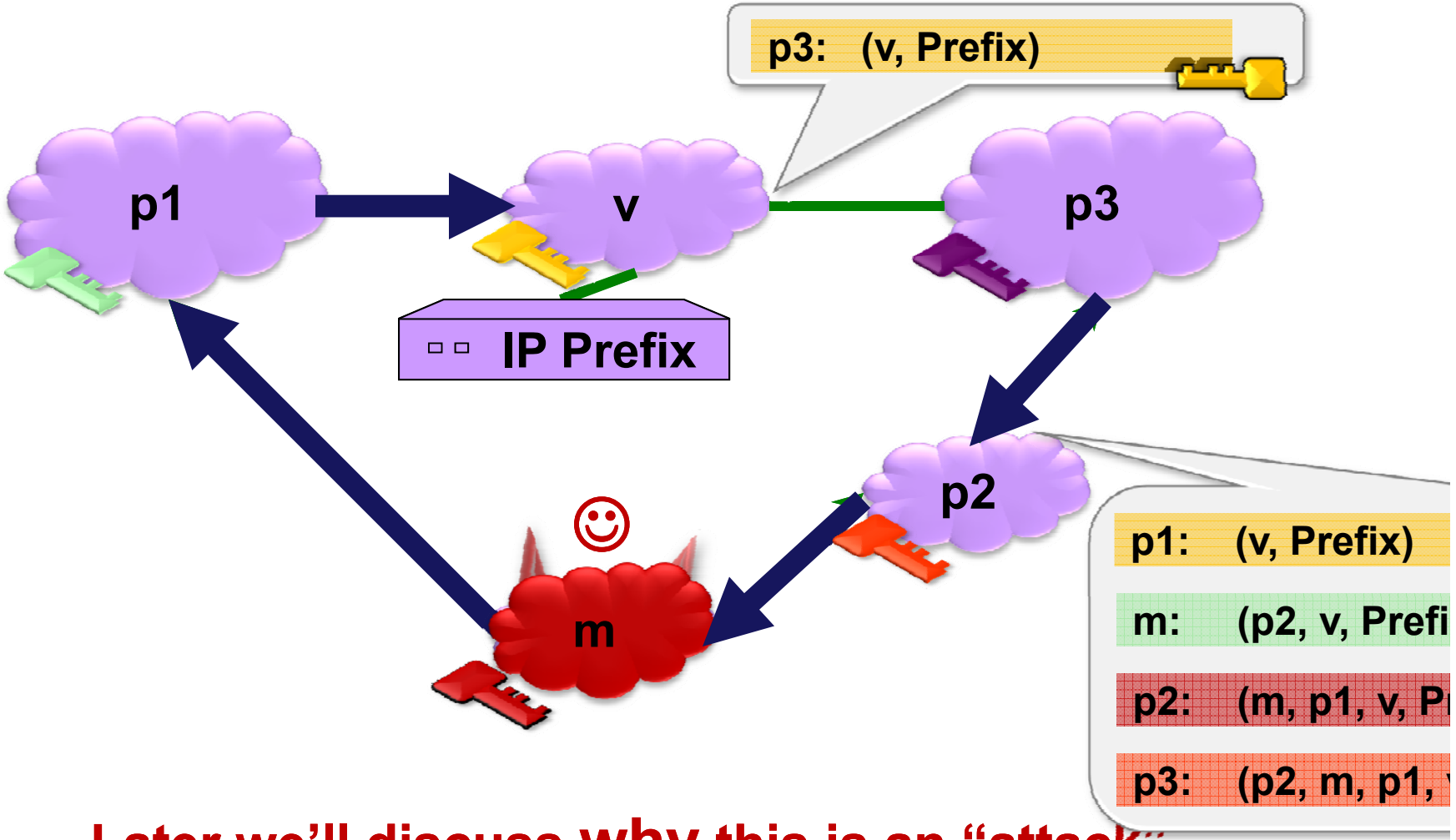
Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Later we'll discuss why this is an "attack"

Are attacks still possible with Secure BGP? (3)

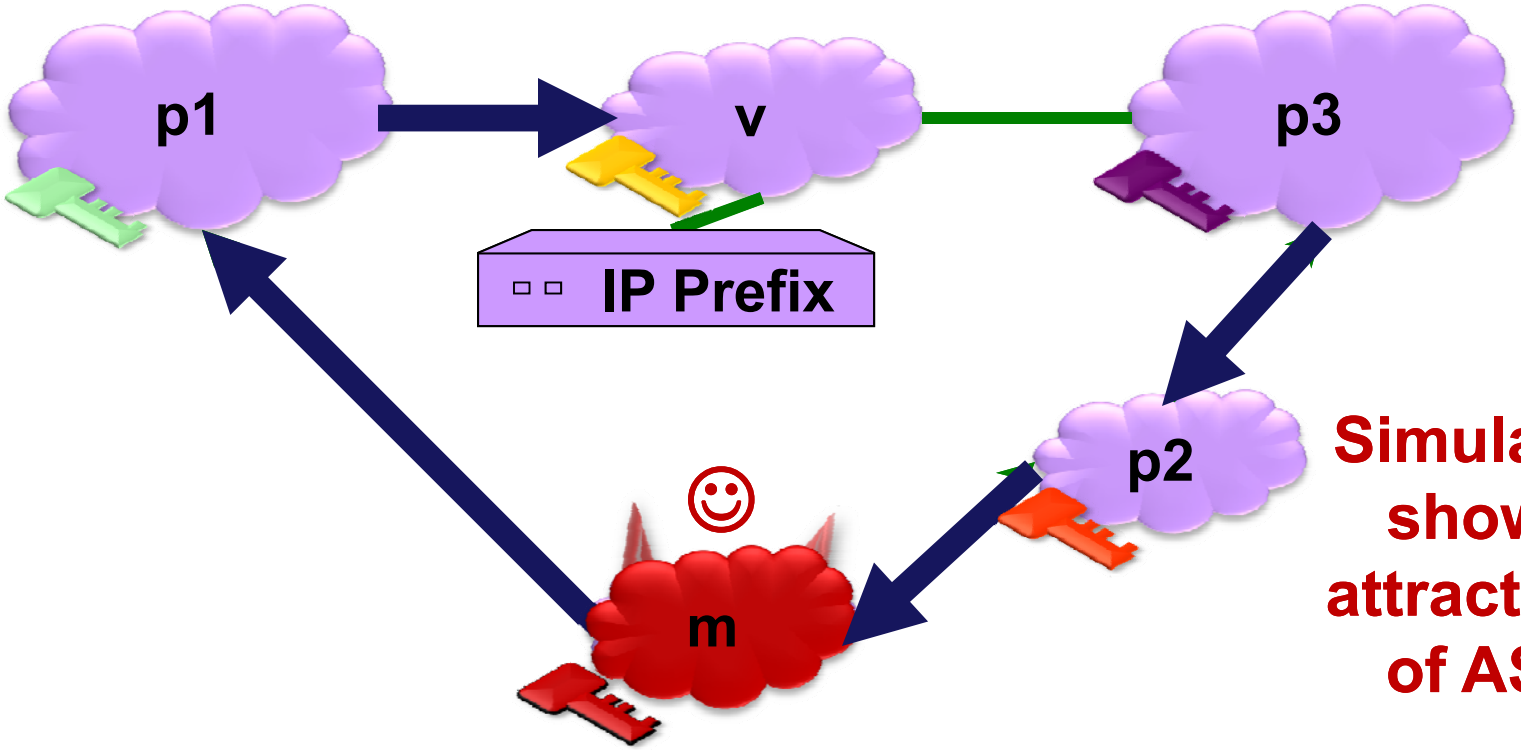
Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Later we'll discuss why this is an "attack"

Are attacks still possible with Secure BGP? (3)

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!



Simulations show he attracts 16% of ASes!

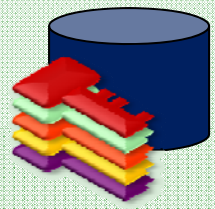
Later we'll discuss why this is an "attack"

This talk

Part 1: A model of BGP Routing Policies

Part 2: Secure Routing Protocols and Attacks

- Prefix hijacks on BGP
- Attacks on Origin Authentication (RPKI)

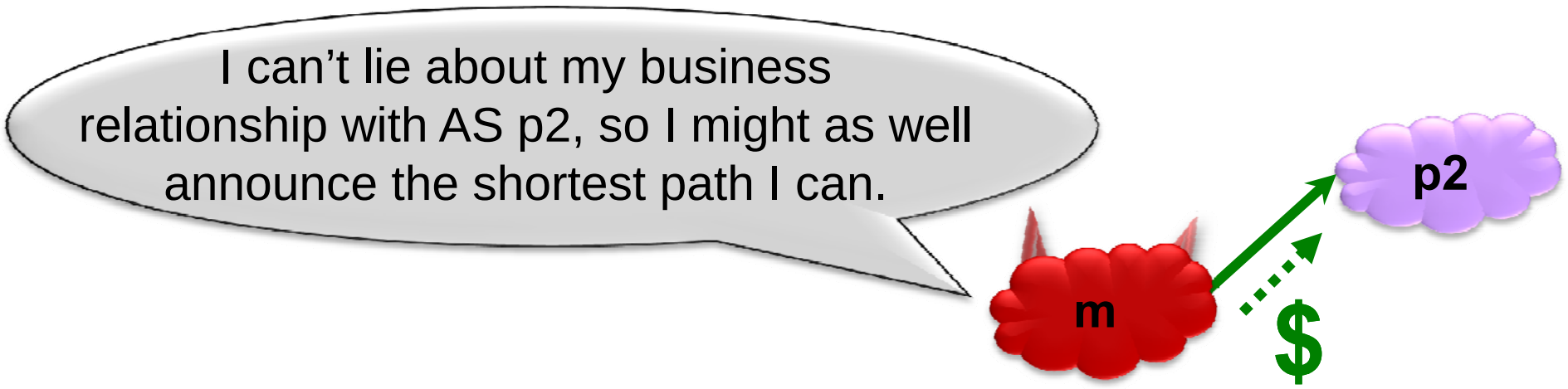


- Route Leaks with Secure BGP
- Interlude: Finding the Optimal Attack
- Filtering attacks by stubs via prefix lists

Part 3: Graphs of Simulation Results

Part 4: Conclusions and Implications

Wait! Is this the "best" attack strategy?!?



Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Wait! Is this the "best" attack strategy?!?

I can't lie about my business relationship with AS p2, so I might as well announce the shortest path I can.

But Not Optimal !

Smart Attack Strategy: Announce the shortest path I can get away with to all my neighbors!

Sometimes announcing to **fewer** neighbors is better**!**

Sometimes **longer** paths are better!

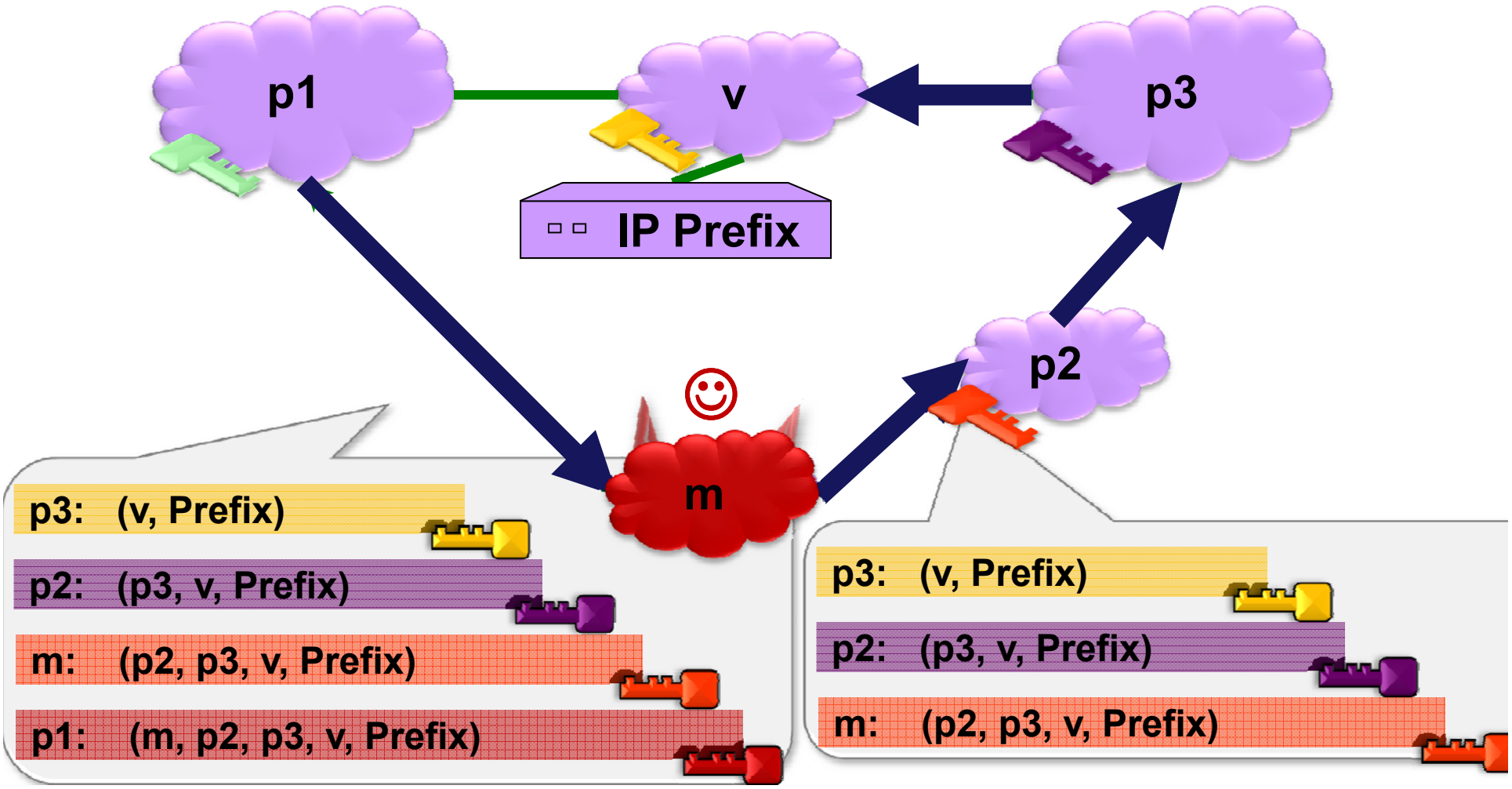
Btw, it's also NP hard to find the optimal attack strategy.

➔ Smart Attack Strategy **underestimates** damage.

Longer paths are better ?!?

Here's an example that shows why…

Sometimes longer paths are better! (1)

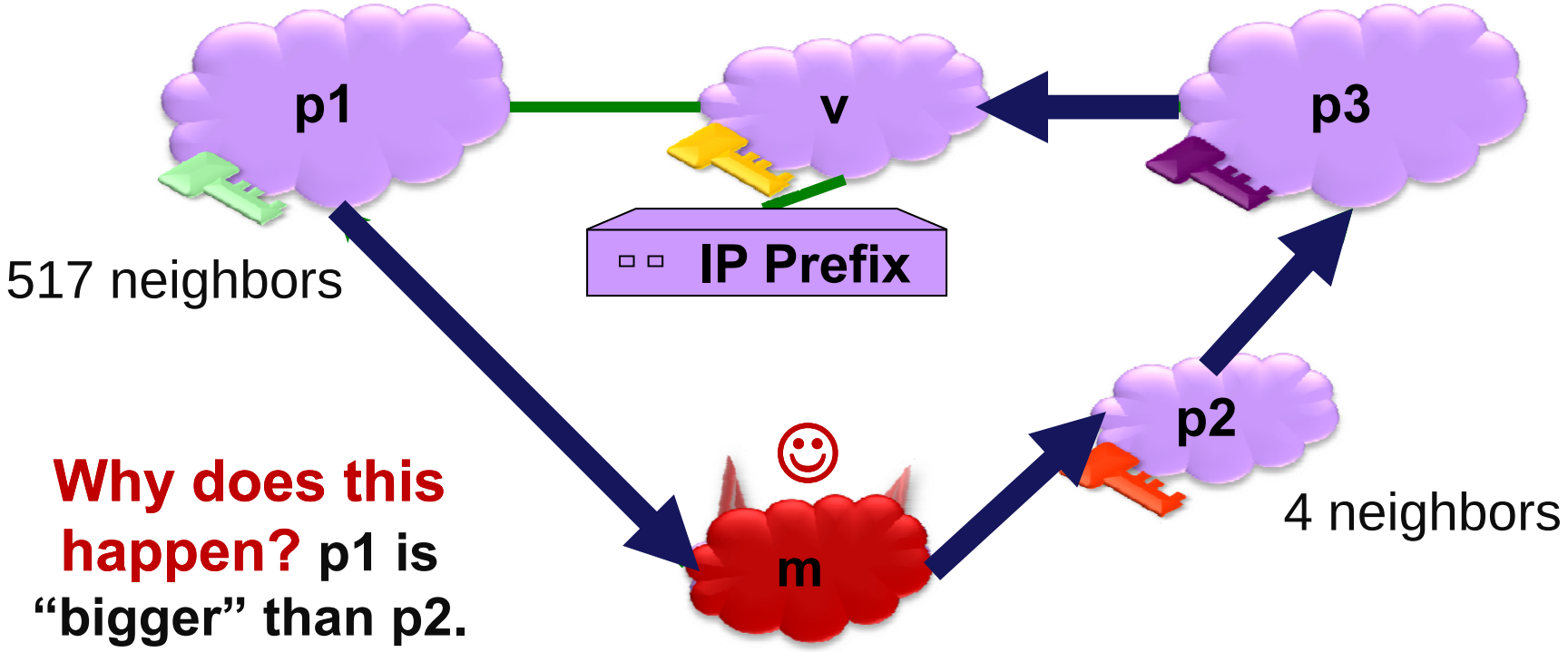


Sometimes longer paths are better! (2)

Simulations show he attracts 56% of Internet!

With the shorter path, he attracts only 16% of Internet!

This is almost as much as attack on insecure BGP: 62%!



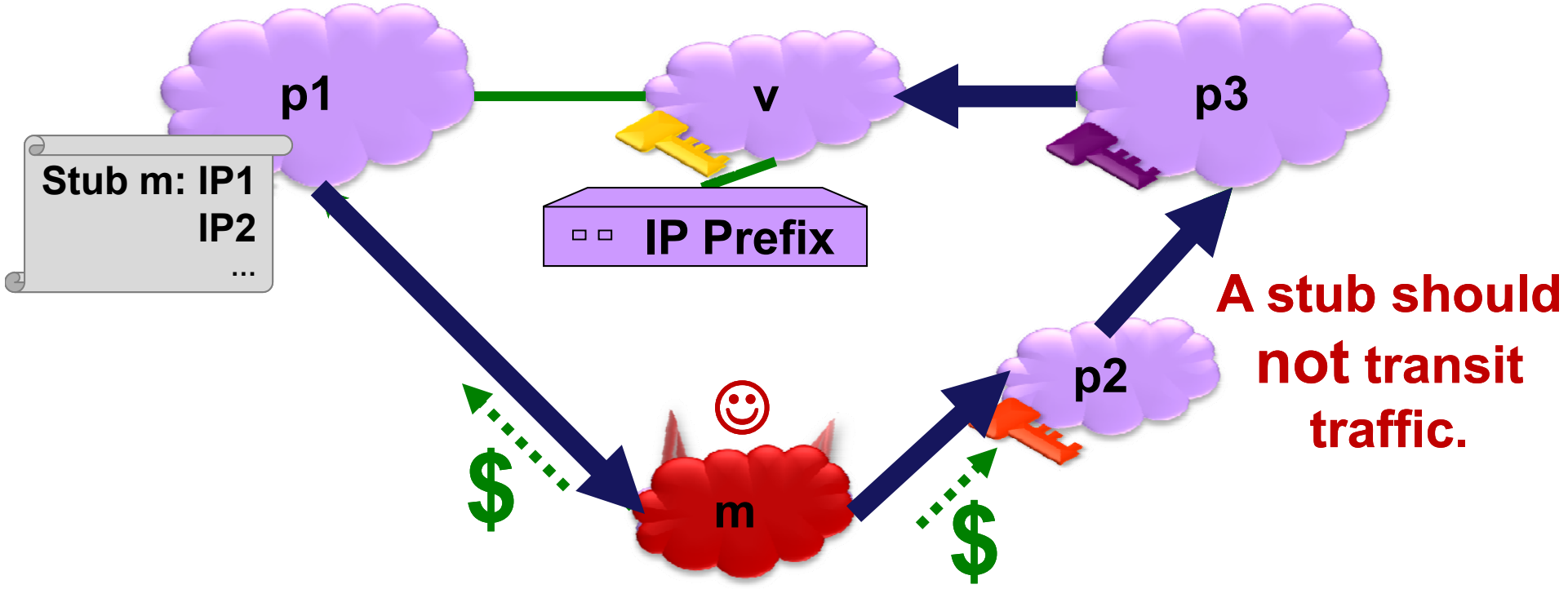
Why does this happen? **p1 is "bigger" than p2.**

Key Observation: **Who** you announce to is as important as **what** you announce.

Security Heuristic: Filtering Stubs on Prefix Lists (1)

Providers that filter stubs on prefix lists:

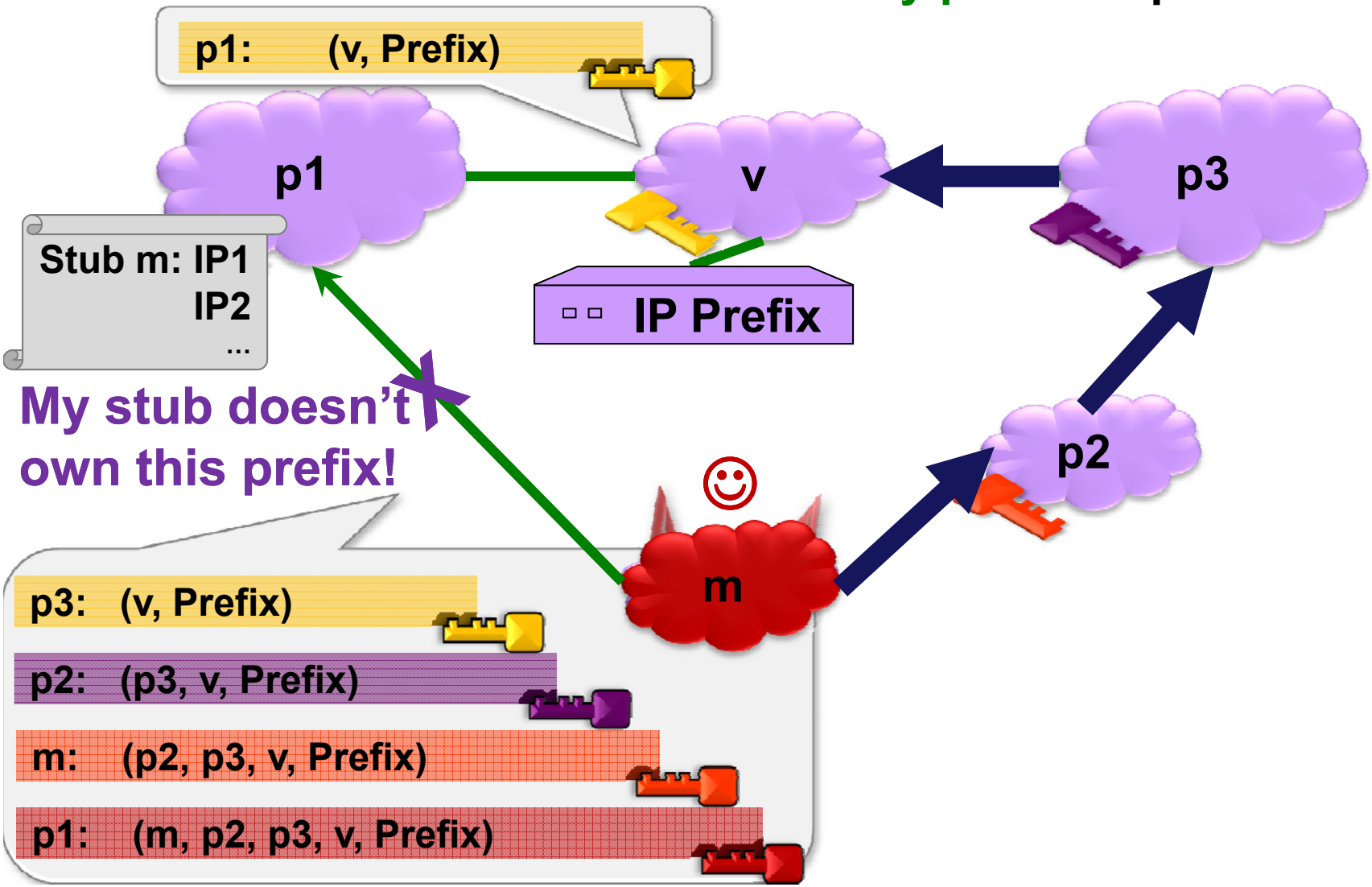
- keep lists of the prefixes owned by each stub customer
- filter if stub customer announces any path to a prefix not on list



Security Heuristic: Filtering Stubs on Prefix Lists (2)

Providers that filter stubs on prefix lists:

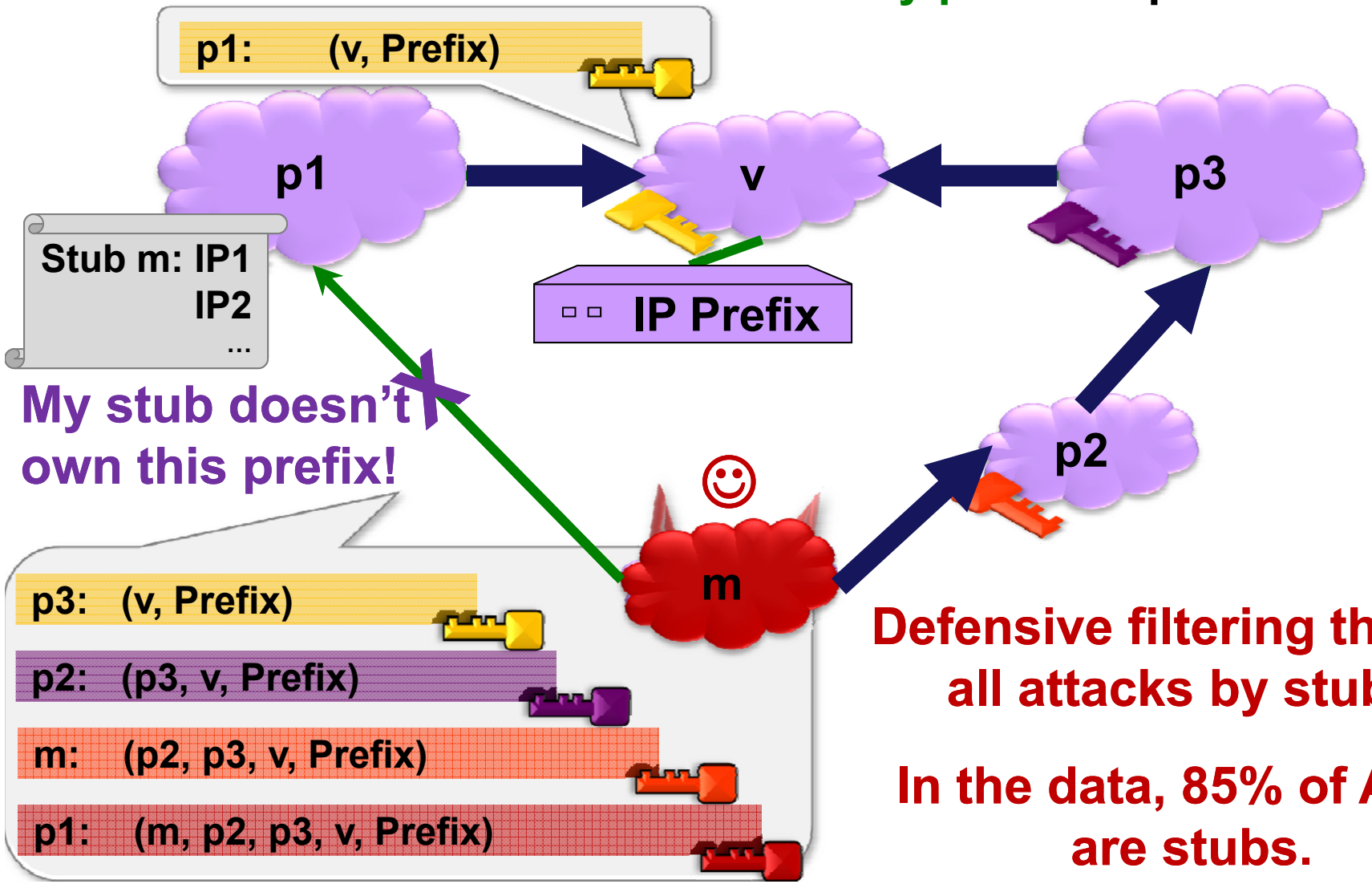
- keep lists the prefixes owned by each stub customer
- filter if stub customer announces any path to a prefix not on list



Security Heuristic: Filtering Stubs on Prefix Lists (2)

Providers that filter stubs on prefix lists:

- keep lists the prefixes owned by each stub customer
- filter if stub customer announces any path to a prefix not on list



Defensive filtering thwarts all attacks by stubs!

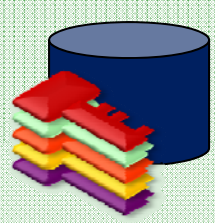
In the data, 85% of ASes are stubs.

This talk

Part 1: A model of BGP Routing Policies

Part 2: Secure Routing Protocols and Attacks

- Prefix hijacks on BGP
- Attacks on Origin Authentication (RPKI)



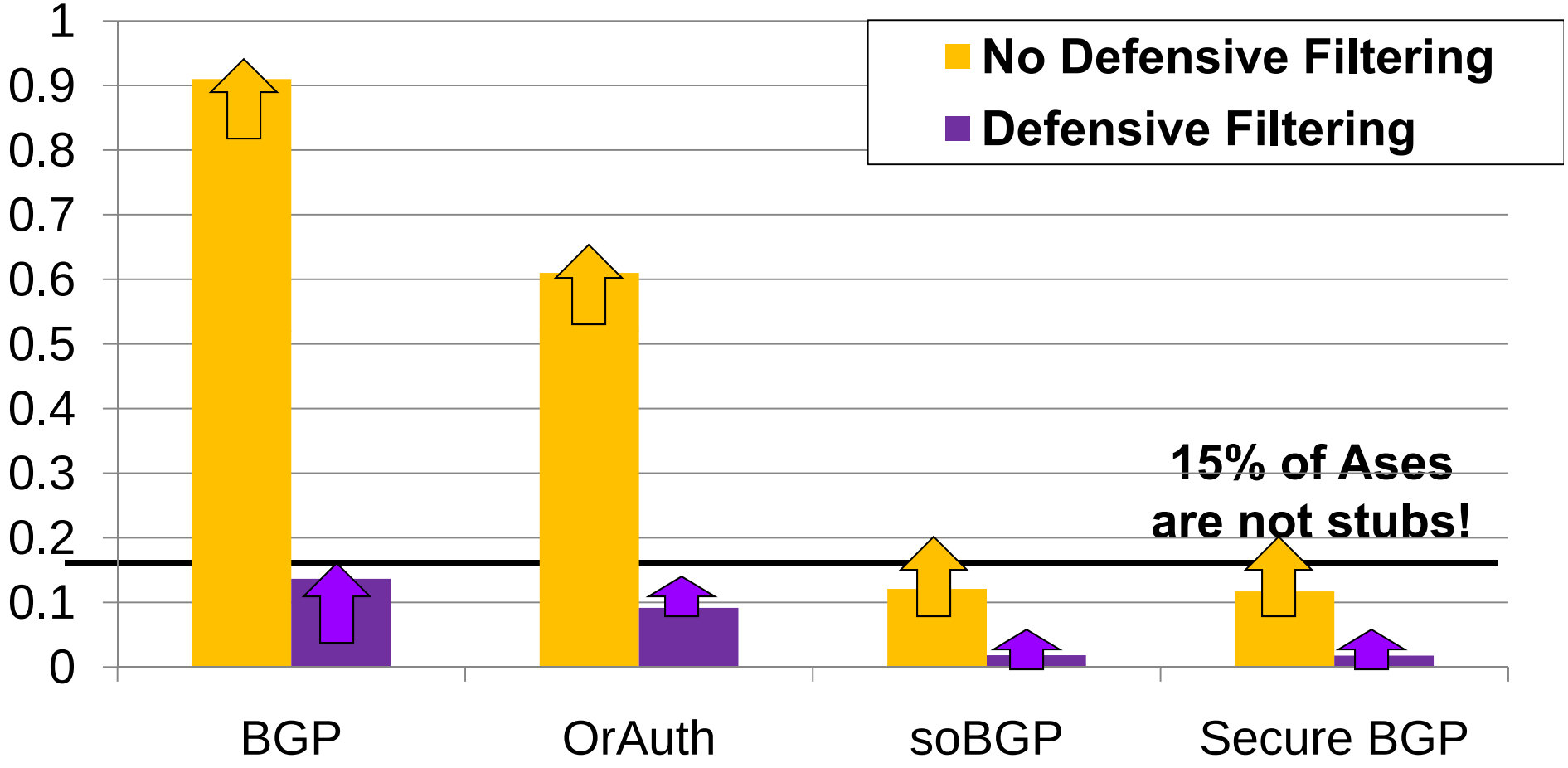
- Route Leaks with Secure BGP
- Interlude: Finding the Optimal Attack
- Filtering attacks by stubs via prefix lists

Part 3: Graphs of Simulation Results

Part 4: Conclusions and Implications

Probability* Smart Attack attracts 10% of Internet

*Probability is taken over random choice of attacker and victim.



Recall that the **Greedy Attack Strategy** **underestimates** damage.

We see that if every provider filters announcements from stubs based on prefix lists, is about as effective as having everyone implement Secure BGP!

Secure BGP is not a replacement for filtering, we need both in combination.

(S*-BGP is vulnerable to route leaks)

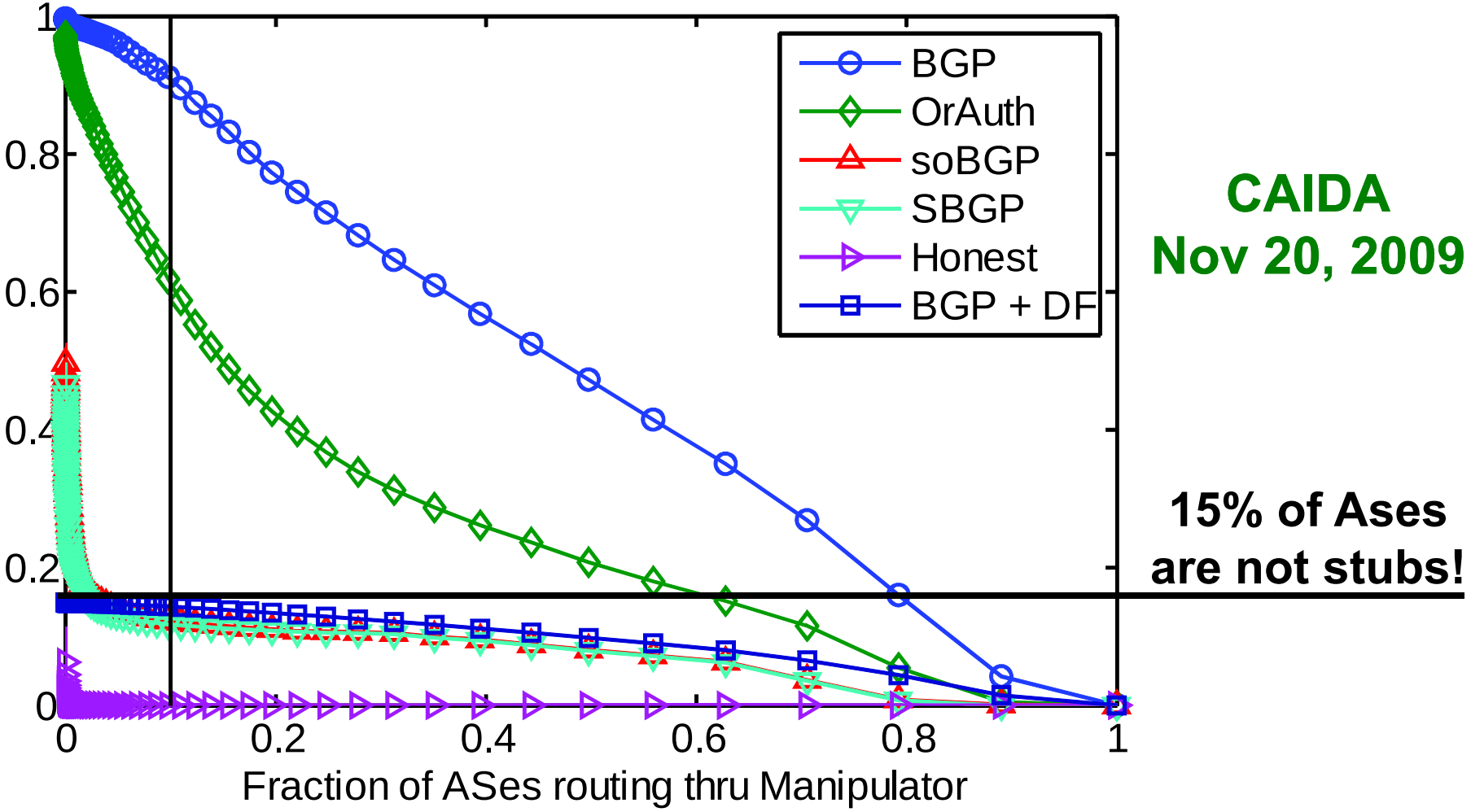
Now, graphs that show how well the results from [CAIDA] and [Cyclops] agree.

These two datasets are produced by independent researchers (not us) using different business-relationship inference algorithms.

But for our study, the trends we see across the datasets are remarkably consistent.

Probability* Smart Attack attracts >x% of Internet (1)

*Probability is taken over random choice of attacker and victim.



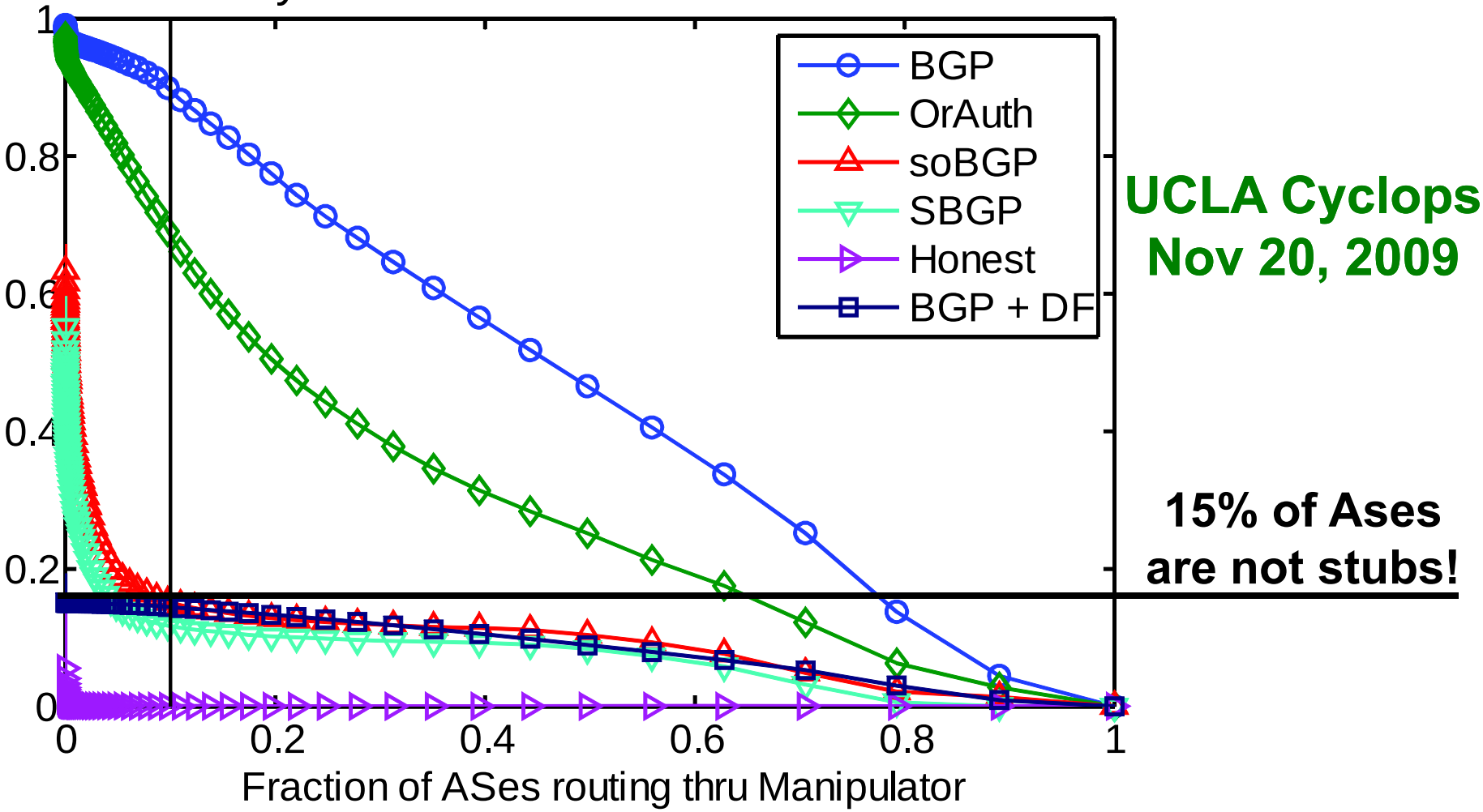
CAIDA
Nov 20, 2009

15% of Ases are not stubs!

Recall that the **Smart Attack Strategy** **underestimates** damage.

Probability* Smart Attack attracts >x% of Internet (2)

*Probability is taken over random choice of attacker and victim.



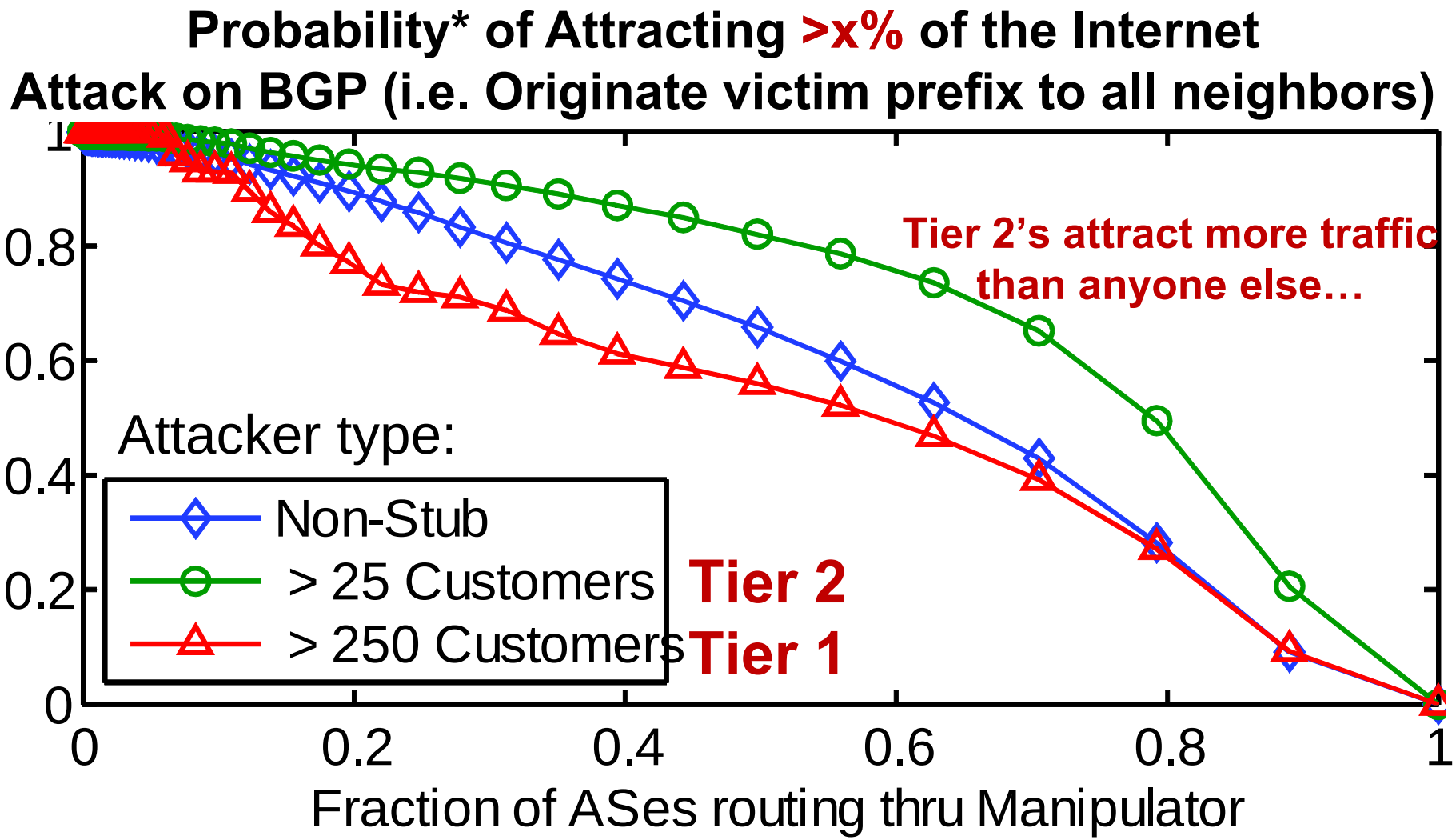
Recall that the **Smart Attack Strategy** **underestimates** damage.

Filtering stubs on prefix lists does not prevent attacks by Tier 1s and Tier 2s.

In fact, the next graph shows that Tier 2s make the most effective attackers.

Thus:
Filtering is not a replacement for Secure BGP, we need both in combination.

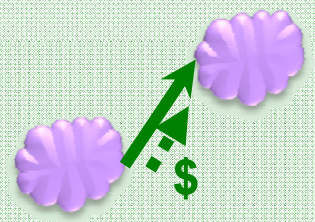
Tier 2's are the most effective attackers



*Probability is over random victim and attacker from different classes

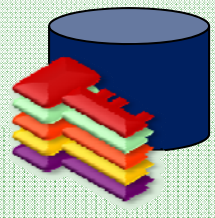
This talk

Part 1: A model of BGP Routing Policies



Part 2: Secure Routing Protocols and Attacks

- Prefix hijacks on BGP
- Attacks on Origin Authentication (RPKI)



- Route Leaks with Secure BGP
- Interlude: Finding the Optimal Attack
- Filtering attacks by stubs via prefix lists

Part 3: Graphs of Simulation Results

Part 4: Conclusions and Implications

Take away points

1) **Who you tell is as important as what you say.**
   - **Secure BGP** constrains the **paths** announced
   - … but not **export policies**.

2) **Defensive filtering is crucial even with S*-BGP**
   - S*-BGP prevents path shortening attacks,
   - ….but is still vulnerable to route leaks
   - Defensive filtering prevents attacks by stubs
   - … but is still vulnerable to attacks by Tier 1s and 2s
   - ... which are the most effective

Need a combination of filtering on prefix lists and S*BGP

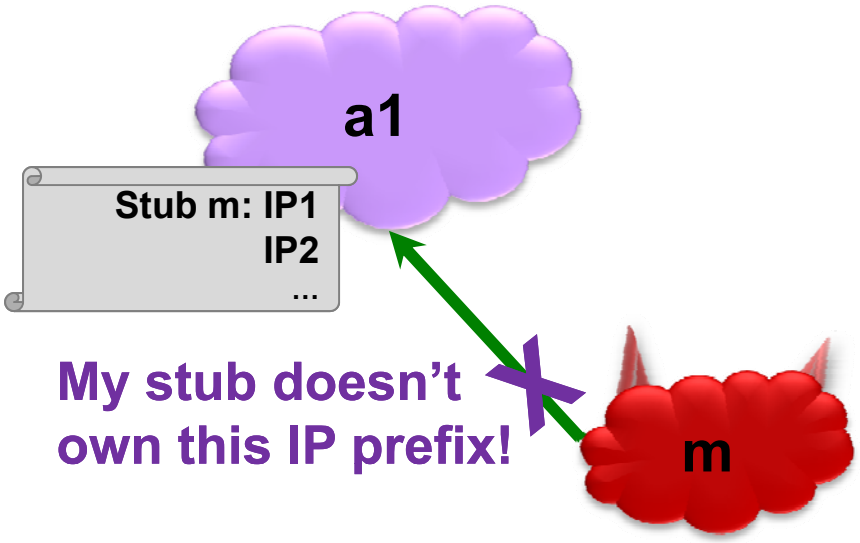
Implementing Filtering on Prefix Lists

Today: The provider locally maintains its prefix list.

Implementation is imperfect.

Why? Relies on **altruism**

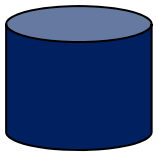
Also, other ASes have to **trust** that each provider has properly implemented prefix lists.



Maintaining prefix lists is annoying and hard.

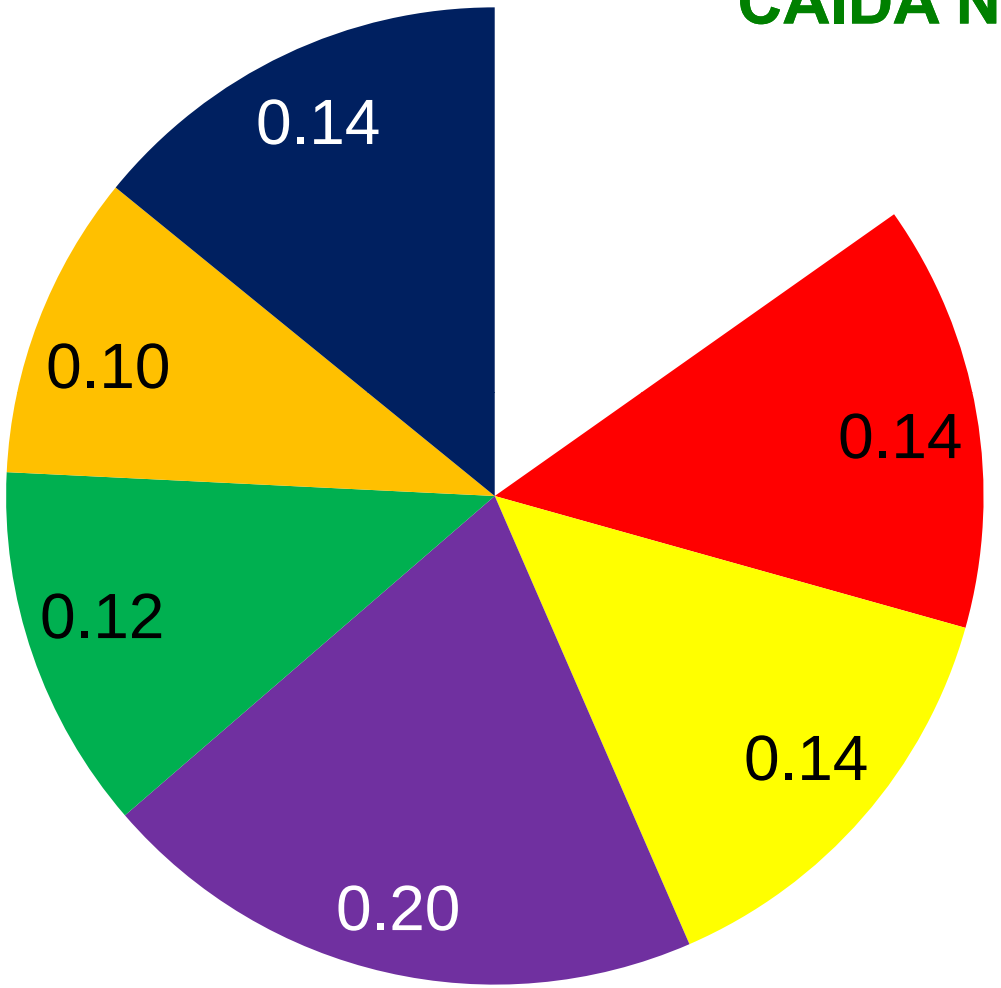
Why not use RPKI/ROA derive prefix lists?

RPKI / ROA: A secure database that maps IP Prefixes to their owner ASes.



What if only large ASes implement prefix lists? (1)

CAIDA Nov 20, 2009



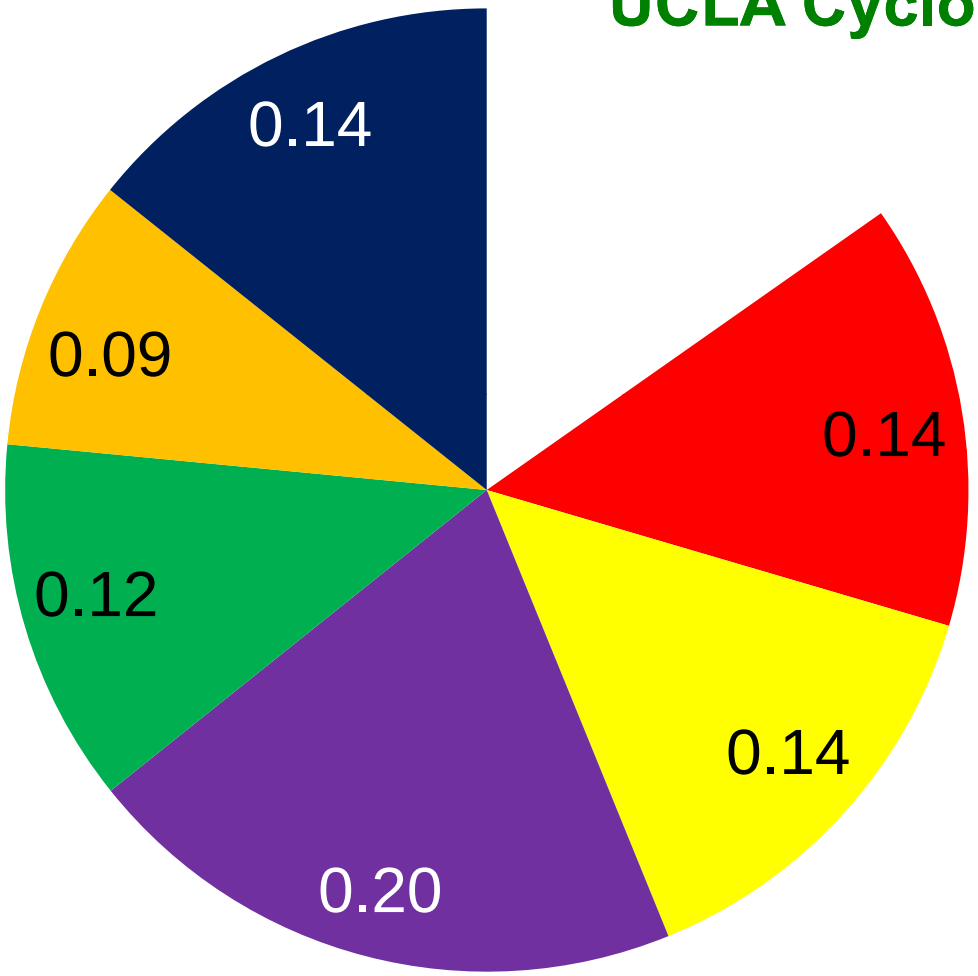
Stubs, size of smallest provider

- < 5 Customers
- (5,10] Customers
- (10,25] Customers
- (25,100] Customers
- (100,500] Customers
- > 500 Customers

If ISPs with > 10 customers filter, 56% of attacks stopped.

What if only large ASes implement prefix lists? (2)

UCLA Cyclops Nov 20, 2009



Stubs, size of smallest provider

- < 5 Customers
- (5,10] Customers
- (10,25] Customers
- (25,100] Customers
- (100,500] Customers
- > 500 Customers

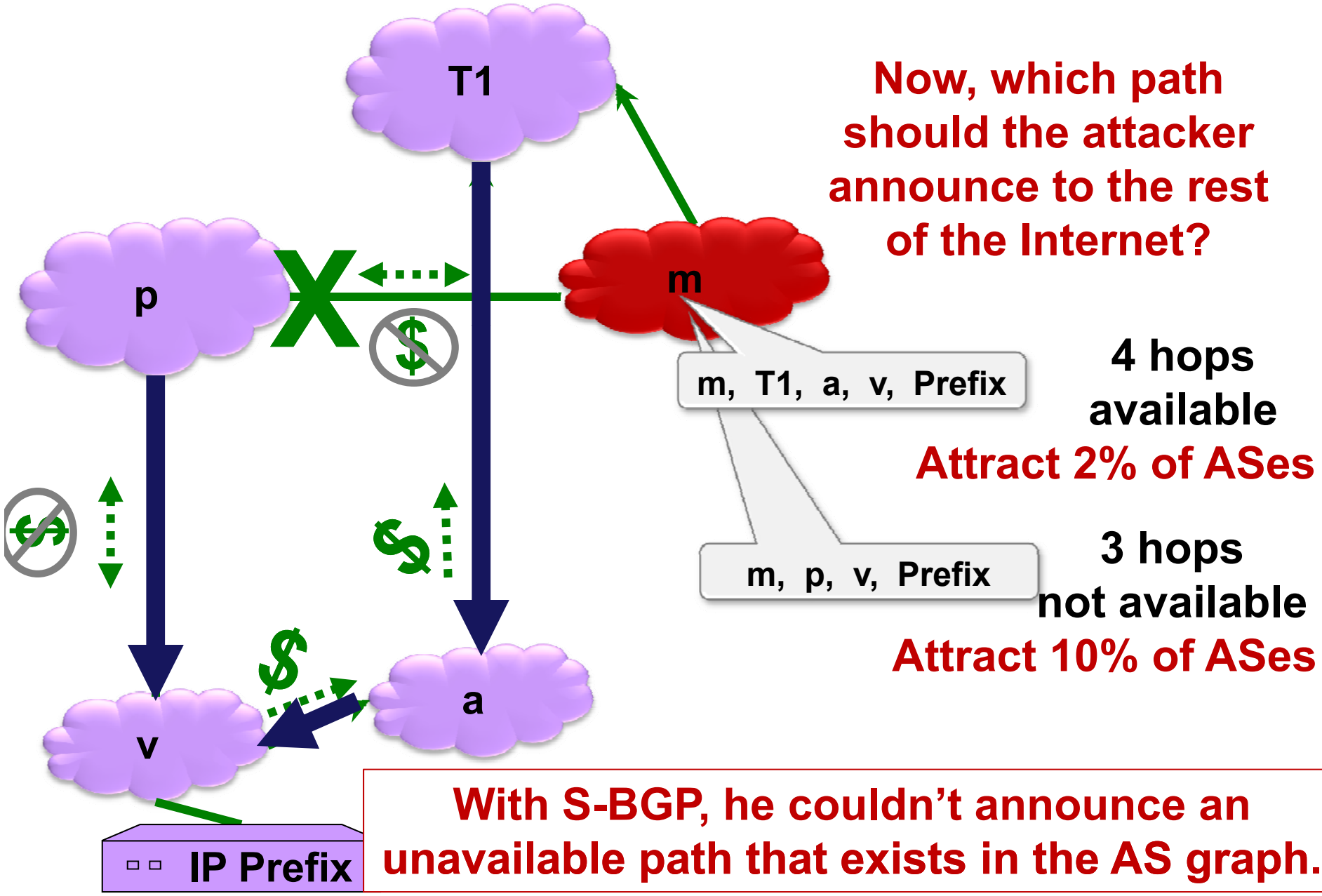
If ISPs with > 10 customers filter, 55% of attacks stopped.

This work will also appear at SIGCOMM'10

Full report available at: https://www.cs.bu.edu/~goldbe

goldbe@cs.bu.edu

soBGP is Weaker than S-BGP for Targeted Attacks



Now, which path should the attacker announce to the rest of the Internet?

4 hops available

Attract 2% of ASes

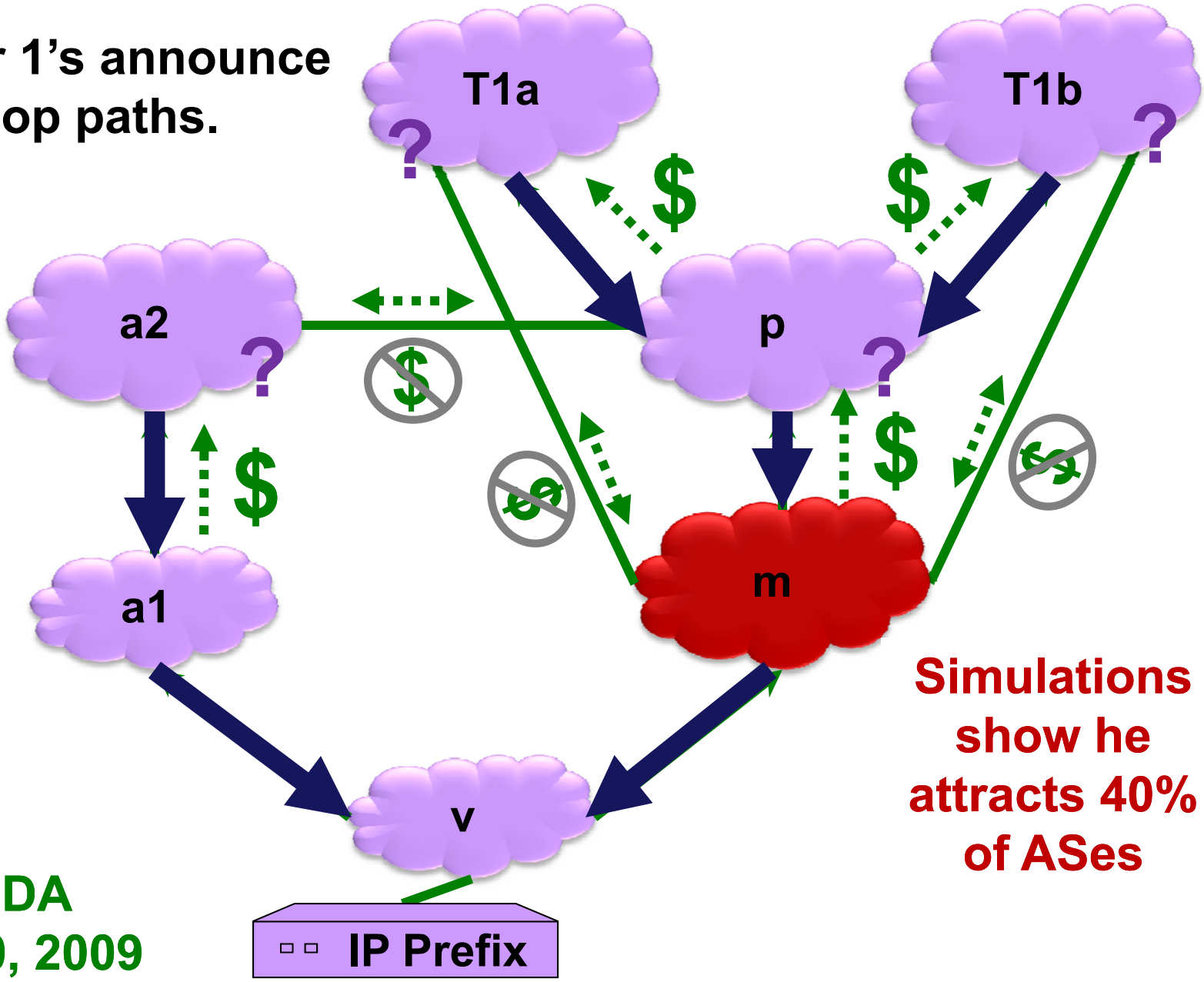
3 hops not available

Attract 10% of ASes

With S-BGP, he couldn't announce an unavailable path that exists in the AS graph.

Attract More by Exporting Less (1) !

The Teir 1's announce 4 hop paths.

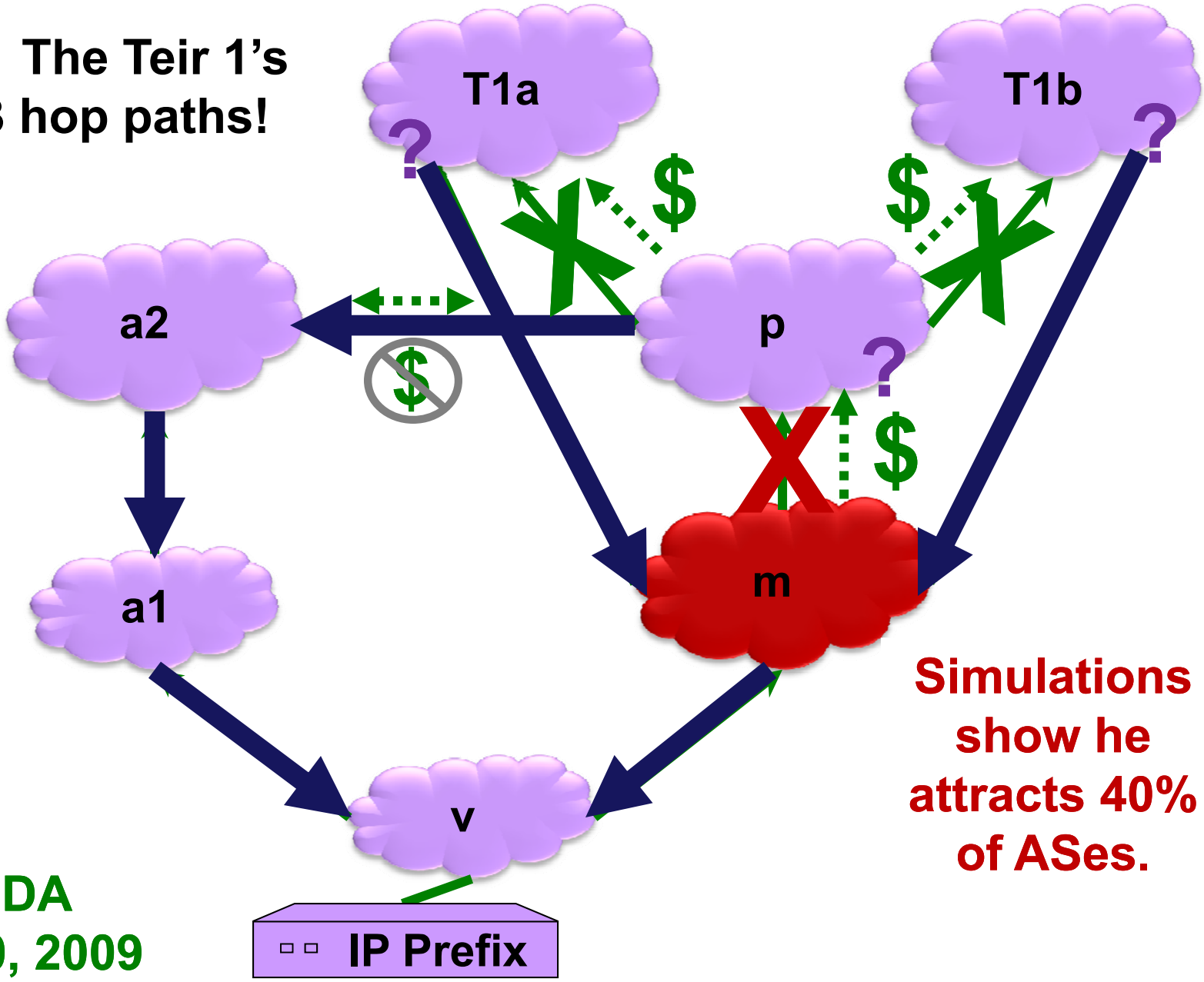


Simulations show he attracts 40% of ASes

CAIDA
Nov 20, 2009

Attract More by Exporting Less (2) !

Why? The Teir 1's use 3 hop paths!

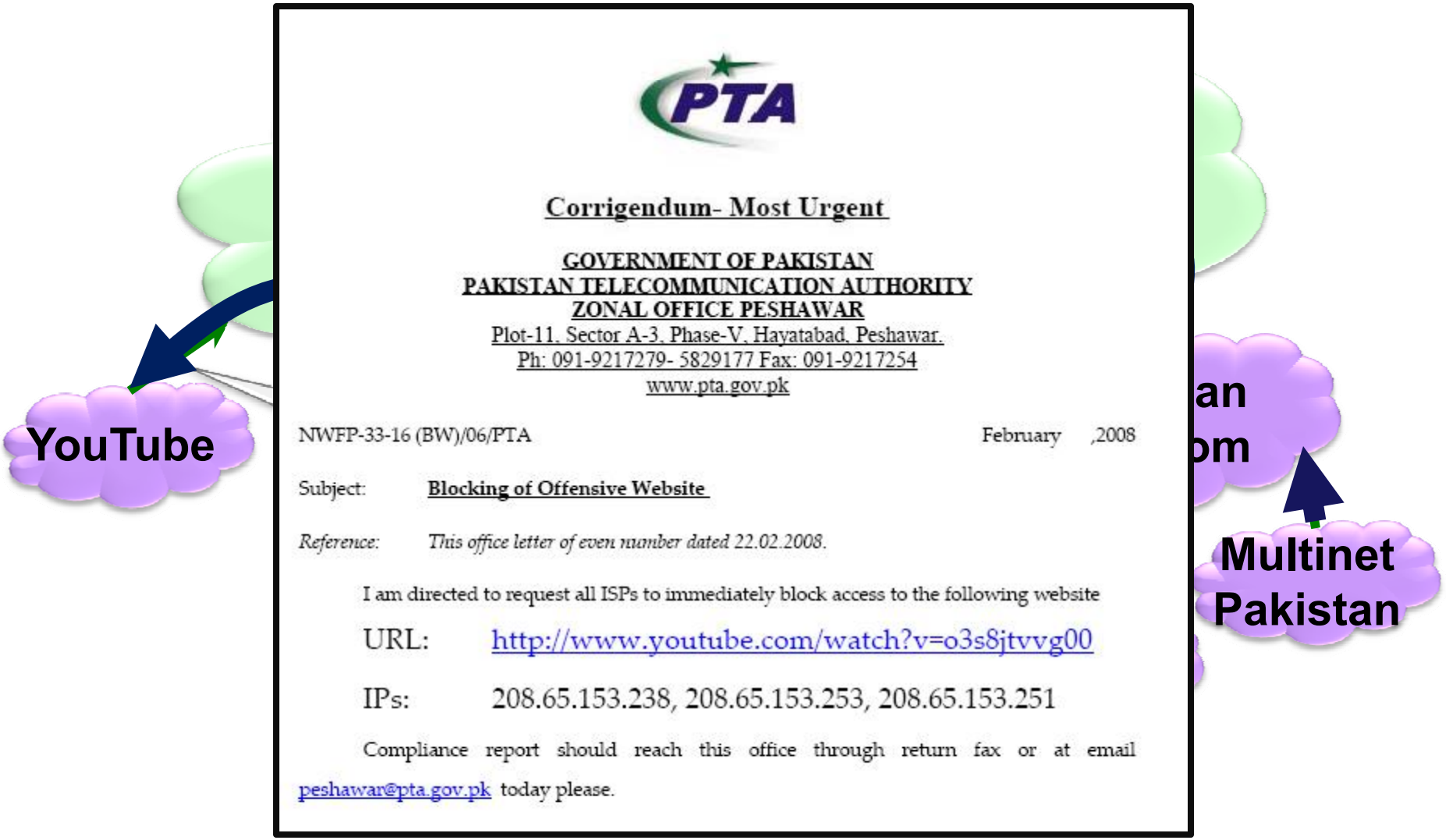


Simulations show he attracts 40% of ASes.

CAIDA
Nov 20, 2009

How Secure is Routing on the Internet Today? (1)

February 2008 : Pakistan Telecom hijacks Youtube



PTA

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.