A Study of Prefix Hijacking and Interception in the Internet

Hitesh Ballani [a], Paul Francis [a], Xinyang Zhang [a]

[a] Department of Computer Science, Cornell University, Ithaca, NY

Presented by: Anupam Das

CS 598 PBG Fall 2010
Advanced Computer Networks

Outline

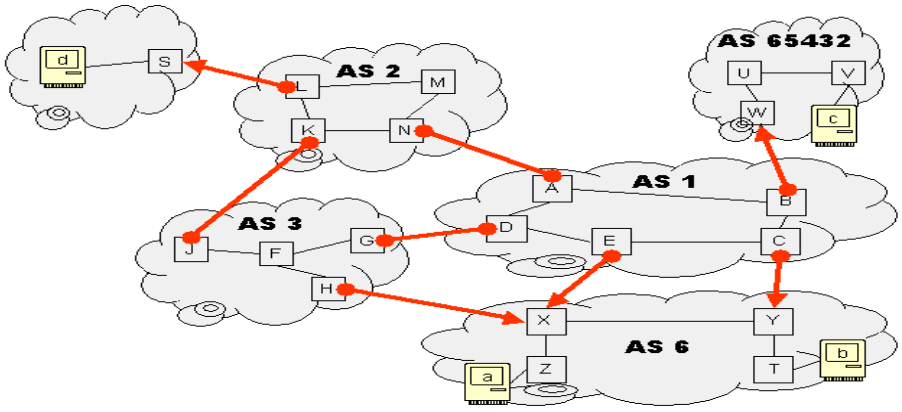
- Recap of BGP
- Common BGP Attacks
- Related Studies on some BGP attacks
- A Study of Prefix Hijacking and Interception in the Internet

Recap of BGP

1) An autonomous systems (ASes) communicate through border routers .
2) Runs over TCP
3) Path vector protocol
4) Incremental update (send to only neighbors)
5) Policies applied (through attributes) influences BGP path selection

For **AS 2**

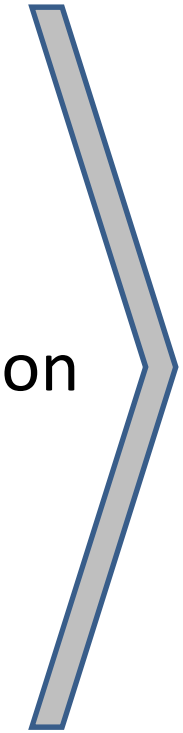
Destination	Path
prefix1	AS2-AS1-AS6
prefix2	AS2-AS3
prefix3	AS2-AS1-AS65432



Common BGP Attacks

The most common BGP attacks are-

1. Blackholing
2. Redirection
3. Interception/Subversion
4. Impersonation
5. Instability



Strategies:

Prefix/Sub-prefix Hijacking

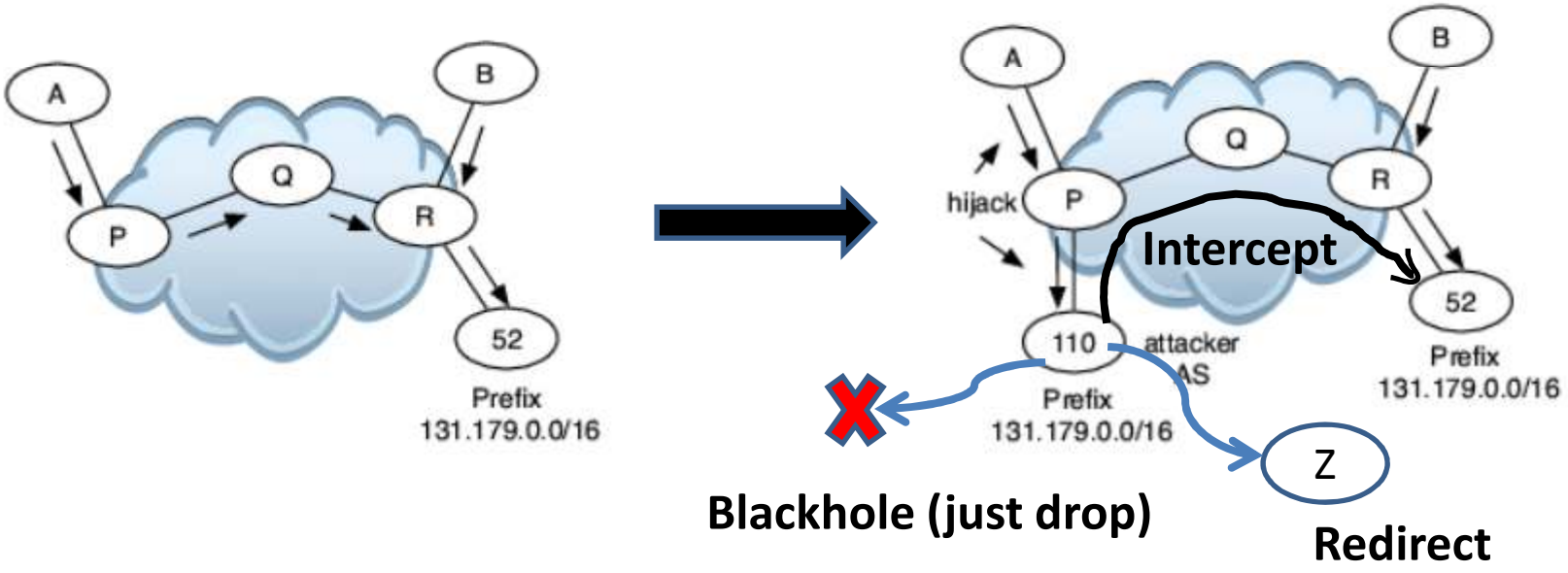
Shorter path advertisement

Violation of Export Policies

Prefix Hijacking

What is a prefix hijack?

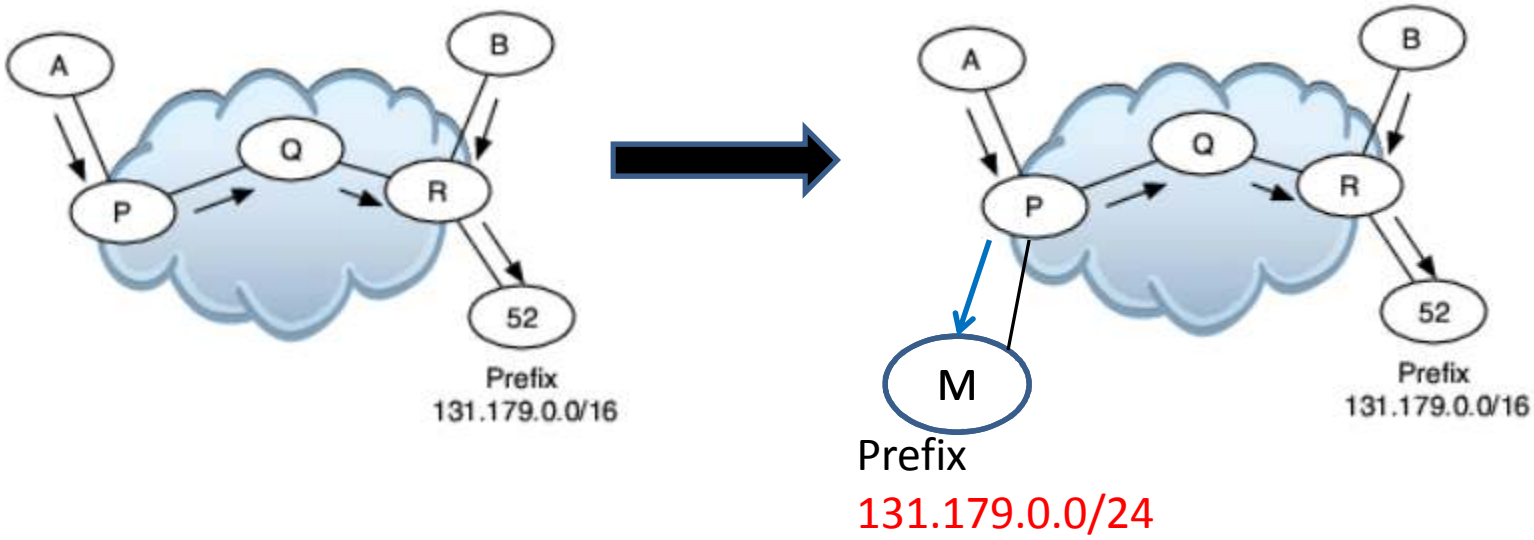
A prefix hijack occurs when AS originates a prefix that it does not own and is originated elsewhere.



Sub-Prefix Hijacking

What is a sub-prefix hijack?

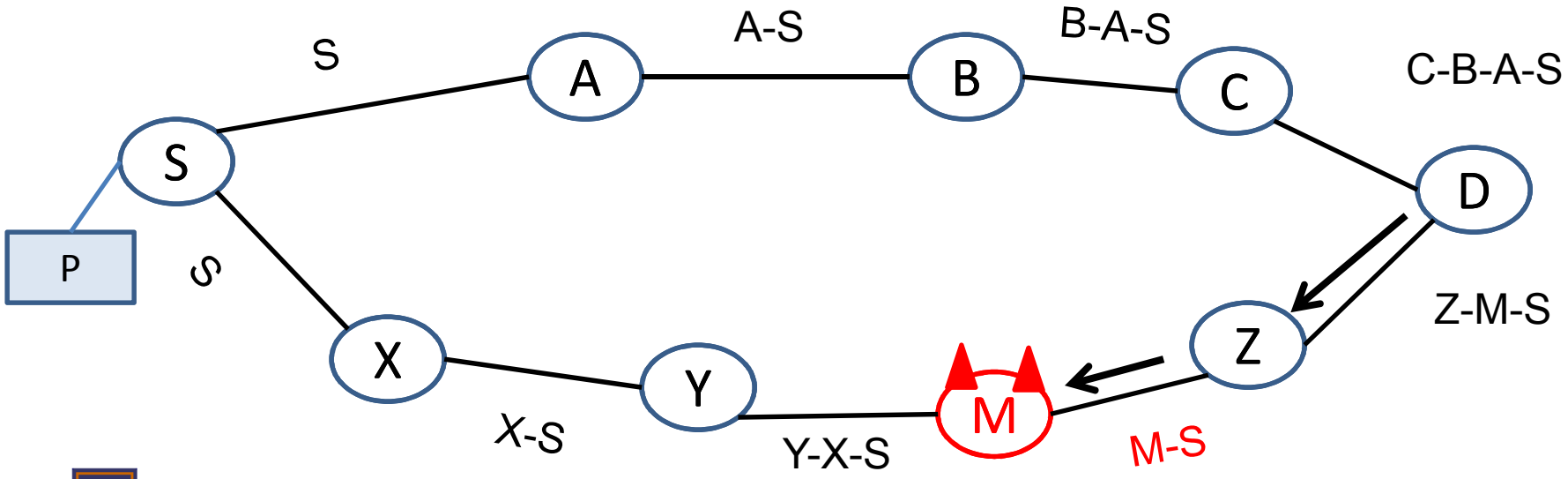
A sub-prefix hijack occurs when AS originates a prefix that it does not own and the space is originated elsewhere *and its space is wholly contained within another announced prefix block*



Shorter Path Advertisement

Instead of claiming to originate a prefix, an adversary can keep the correct originator, but shorten the remainder of the path to make it look more attractive.

- This attack is more stealthy than simple origination.
- Unlikely to occur as misconfiguration.



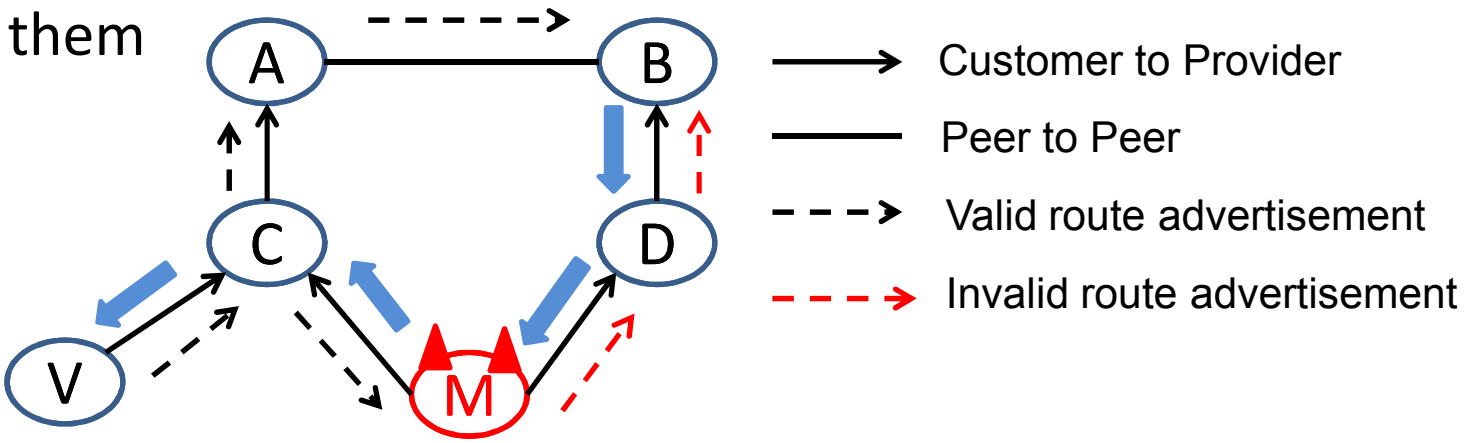
Violation of Export Policy

Standard route export rule-

Route Learned From	*Should Export Route to*
Provider	All customers
Peer	All customers
Customer	All neighbors
Local	All neighbors

This ensures "Valley Free" property

Malicious AS could exploit this to attract more traffic through them



Related Studies on some BGP attacks

PGBGP: Pretty Good BGP (Karlin et al.)

The main idea behind PGBGP is to slow down the process of routing table update to provide better investigation.

Learning phase: Keep track of the origin ASs of each prefix (first ***h*** days).

Suspicion phase: Update with new origin AS for a prefix =>Labeled suspicious (for ***s*** days). Lets operators verify new origin.

Database of Prefix Origins

Prefix	Origin
P1	A
P2	X
P3	D
P2	**Z**
Sub-P3	**Y**

After ***s*** days if the update is still in routing table then accept it.

Listen & Whisper

(Subramanian et al.)

There are 2 components to this mechanism-

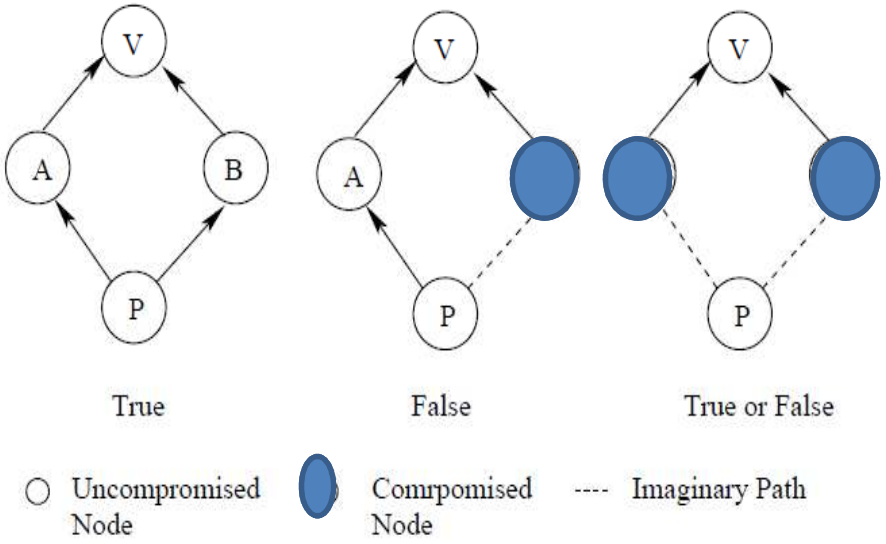
Listen : Checks the data plane for inconsistency .

Whisper : Guarantees path integrity for route advertisements using cryptographic functions.

These approaches neither require public key distribution nor do they require a central database.

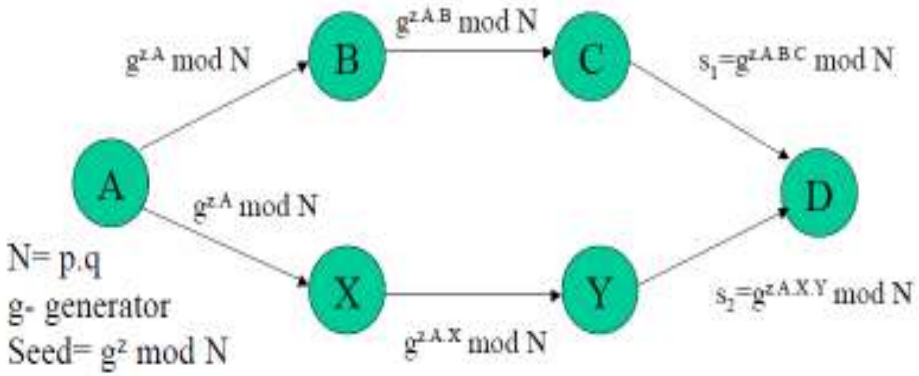
Listen & Whisper
(Subramanian et al.)

Whisper performs route consistency test on routes to the same destination. ***Route consistency provides the ability to trigger alarms if any node generate spurious update.***



RSA or SHA based techniques

An Example route consistency test construction



Consistency Checking of Routes (C,B,A) and (Y,X,A)

$$s_1^{X.Y} = s_2^{B.C} = g^{z.A.B.C.X.Y}$$

Listen & Whisper
(Subramanian et al.)

Listen: Checks whether a path really exists.

Basic approach: Monitor TCP flows to check route validity

If SYN is followed by DATA => TCP flow complete
If SYN is not followed by DATA (within 2 min)=>TCP flow incomplete

Challenge: Dealing with false positives and false negatives due to-

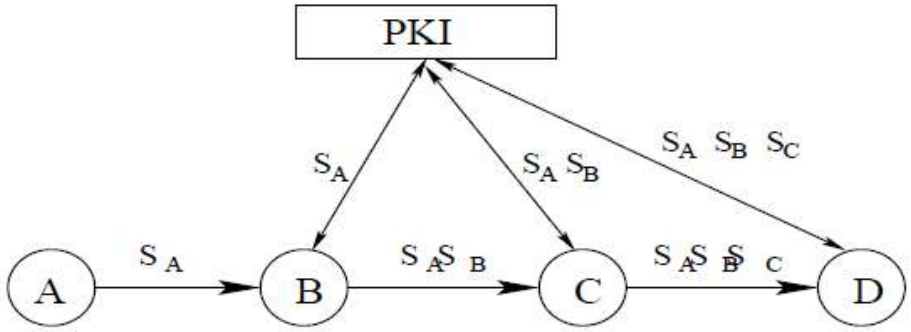
- Non-live destination
- Route change
- Port scanner generating SYN
- Malicious end hosts creating bogus TCP flow

Secured BGP (Kent et al.)

Makes extensive use of digital signatures and public key certification.

Uses:

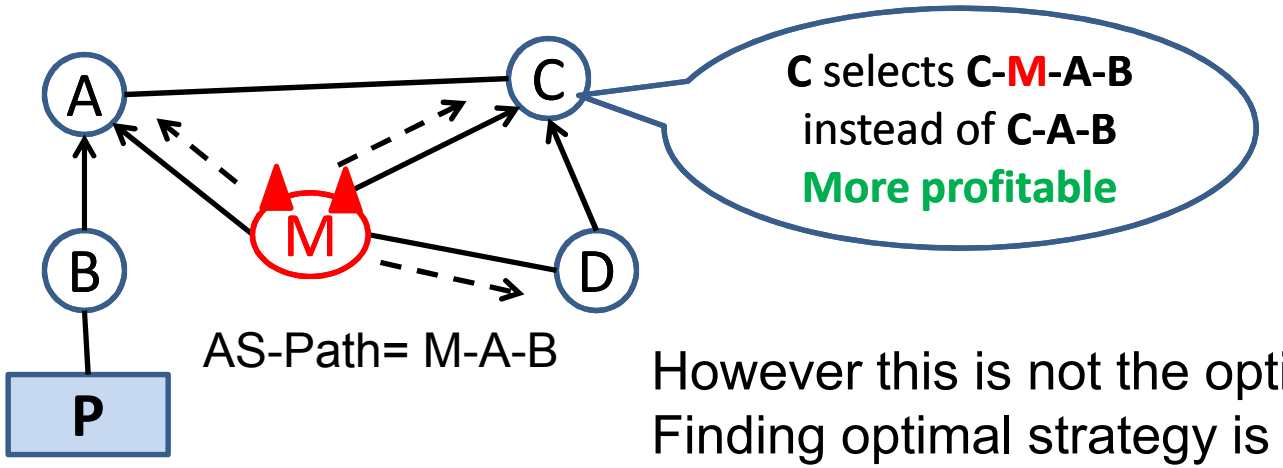
- IPsec --> authenticity and integrity of communication
- PKIs --> secure identification
- Attestations --> authorization to advertise
- Validation of UPDATEs using certificates and attestations
- Distribution of countermeasures information --> certificates, CRLs, AAs



Heavy infrastructural and management burden.

How Secure are Secure Interdomain Routing Protocols (Goldberg et al.)

The optimal strategy to attract traffic seems to advertise the shortest legitimate path to all neighbors. (**Shortest Path-Export All**)

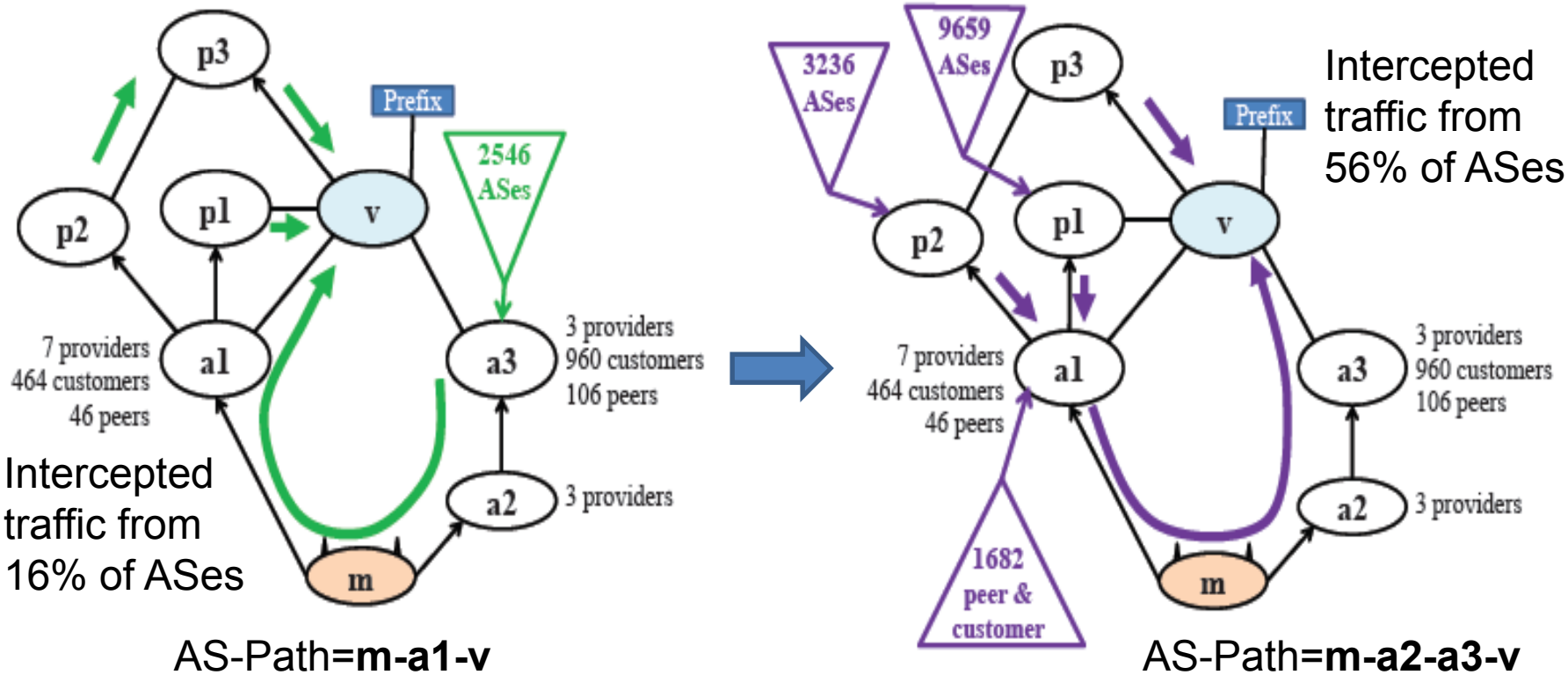


However this is not the optimal strategy !!
Finding optimal strategy is **NP-hard**

There are **Smarter Attacks** which are not optimal

How Secure are Secure Interdomain Routing Protocols (Goldberg et al.)

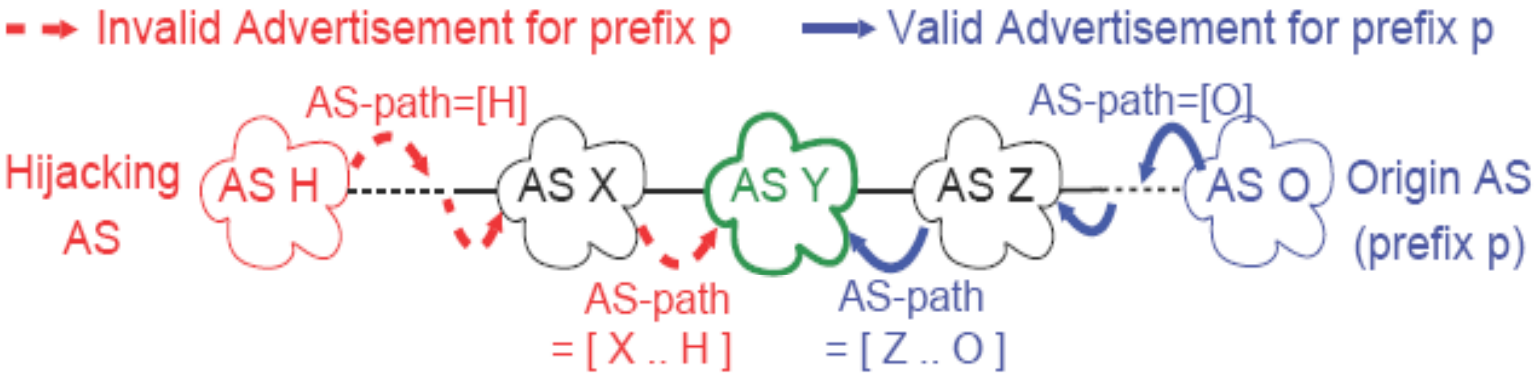
Strategy: Attract more by announcing longer paths !



A Study of Prefix Hijacking and Interception in the Internet (Ballani et al.)

Conditions for Hijacking

When are invalid paths accepted ?



Can AS H hijack prefix *p*'s traffic from AS Y?

AS Y needs to choose between

Invalid Route	Vs	Valid Route
AS-Path = [X : : :H]		AS-Path = [Z : : :O]
Length = i		Length = v

Conditions for Hijacking (cont..)

Decision depends upon:

- Routing policies (customer > peer > provider)
- Advertised AS-hop distance to destination

Invalid / Valid		Customer	Peer	Provider
Customer	v<i	✗	✗	✗
	v=i	–	✗	✗
	v>i	✓	✗	✗
Peer	v<i	✓	✗	✗
	v=i	✓	–	✗
	v>i	✓	✓	✗
Provider	v<i	✓	✓	✗
	v=i	✓	✓	–
	v>i	✓	✓	✓

v= valid route length
i=invalid route length

✗ Valid route chosen

✓ Invalid route chosen

– Depends upon other BGP factors

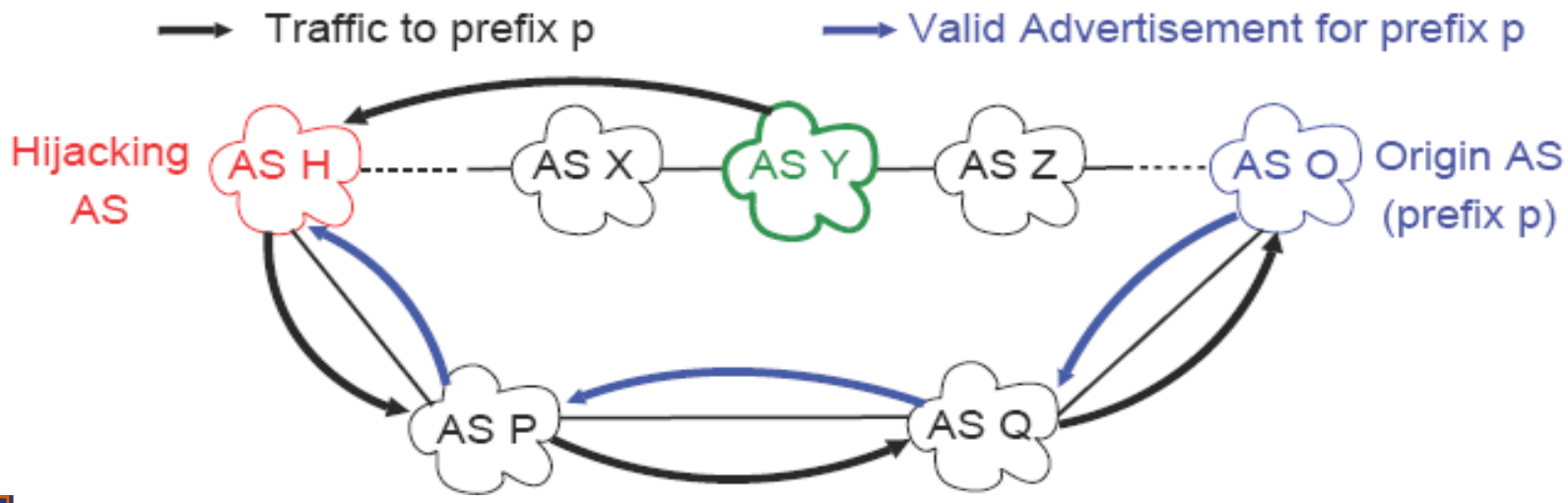
Conditions for Interception

Can AS H **intercept** prefix *p*'s traffic from AS Y?

1. Can AS H hijack prefix *p*'s traffic from AS Y?
2. Can AS H route the hijacked traffic back to AS O?

Safety Condition:

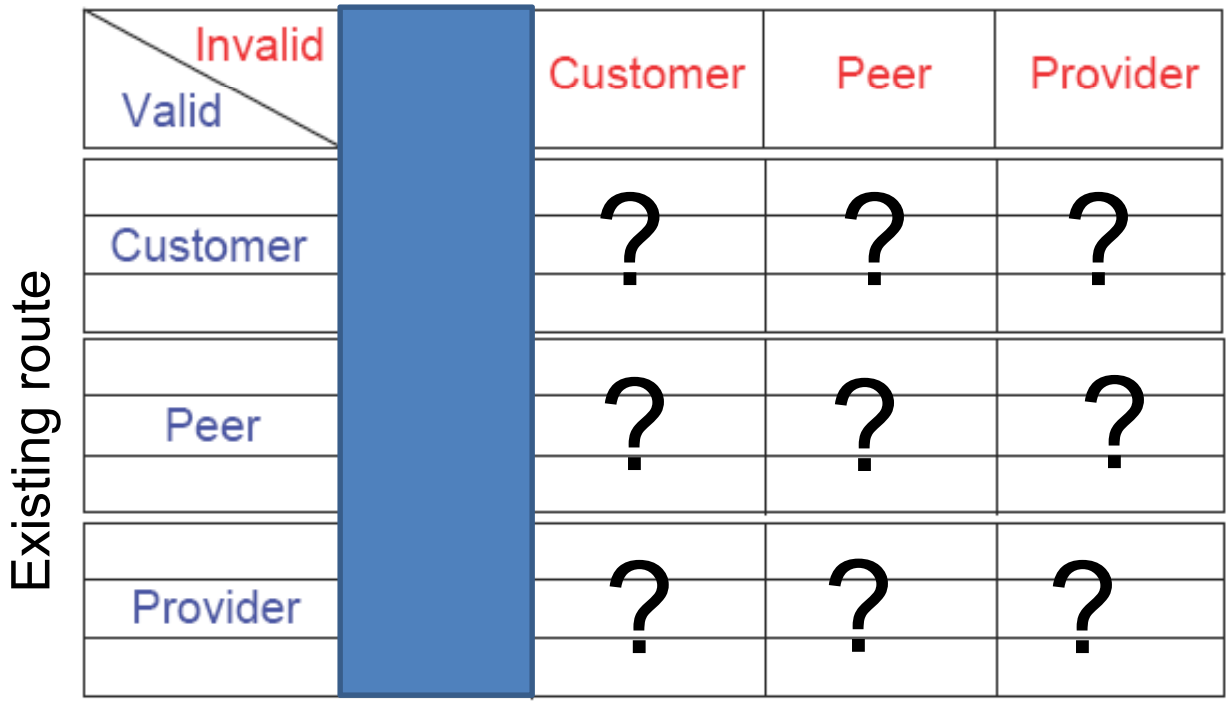
AS H should have a valid route for prefix *p* during Interception



Conditions for Interception (cont..)

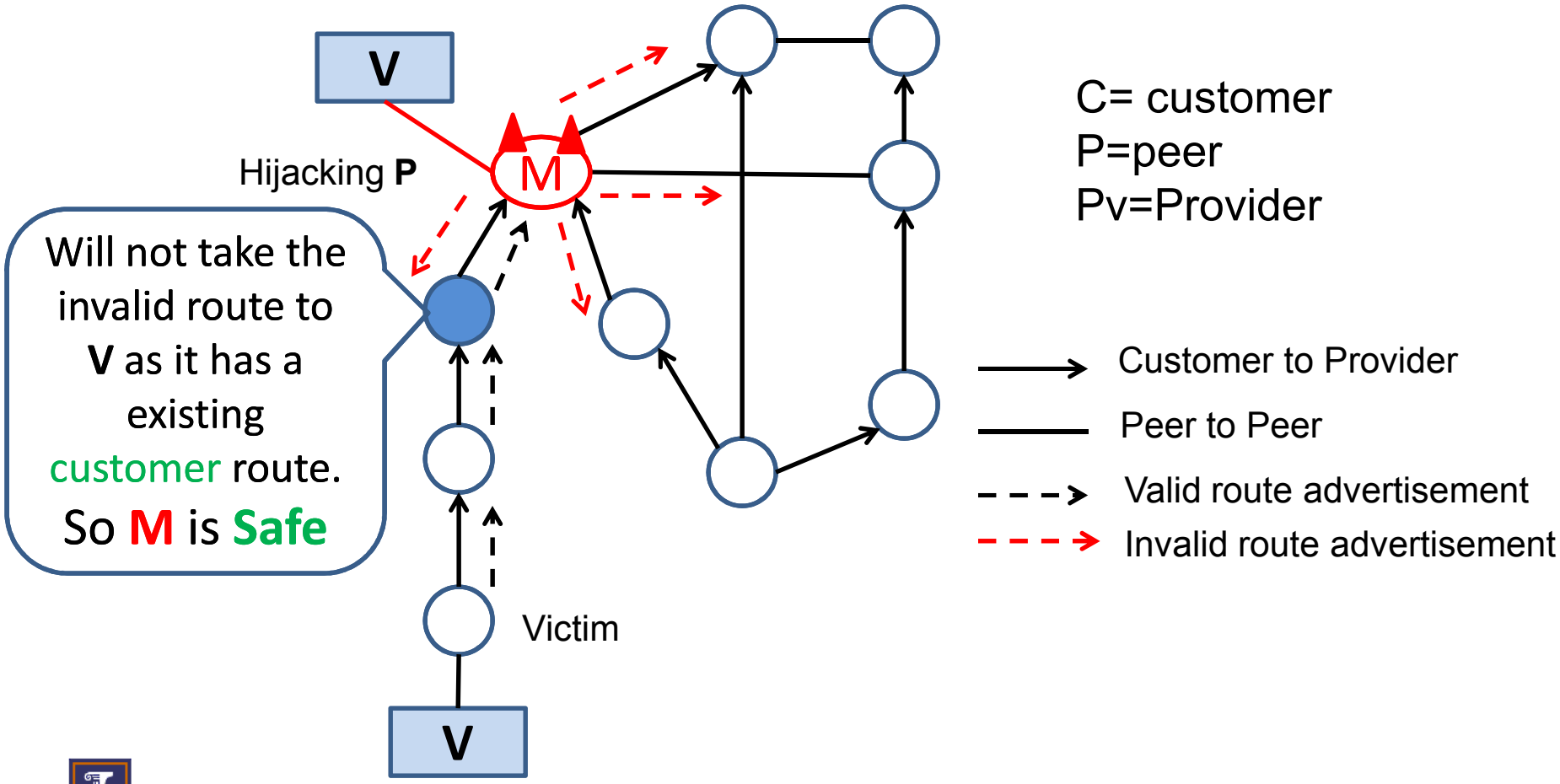
Can AS H advertise the invalid route to a neighbor without impacting its valid route?

Possible situations:



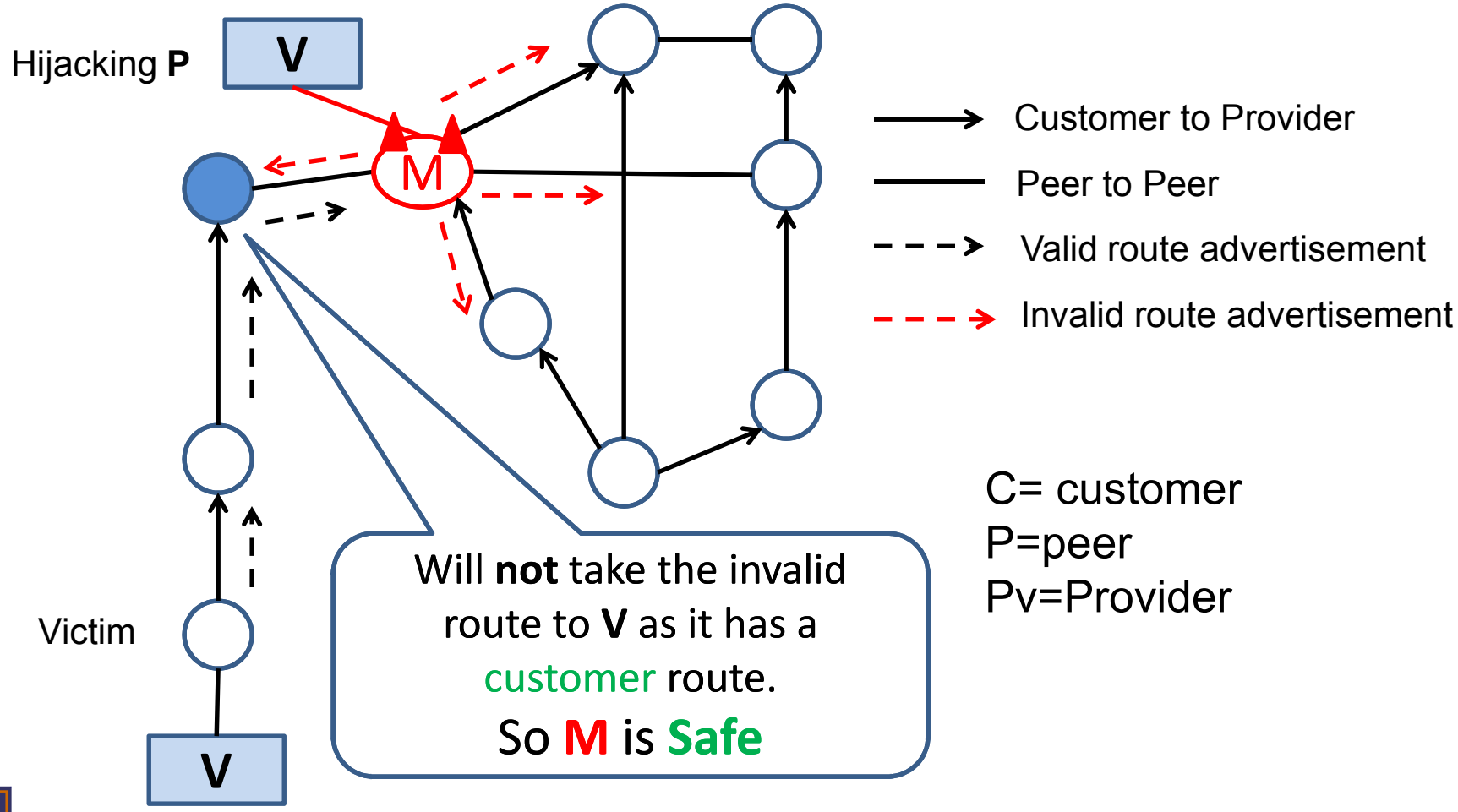
Maintaining Valid Interception Path

Case 1-3: Existing route=C & Advertising Invalid route to=C/P/Pv



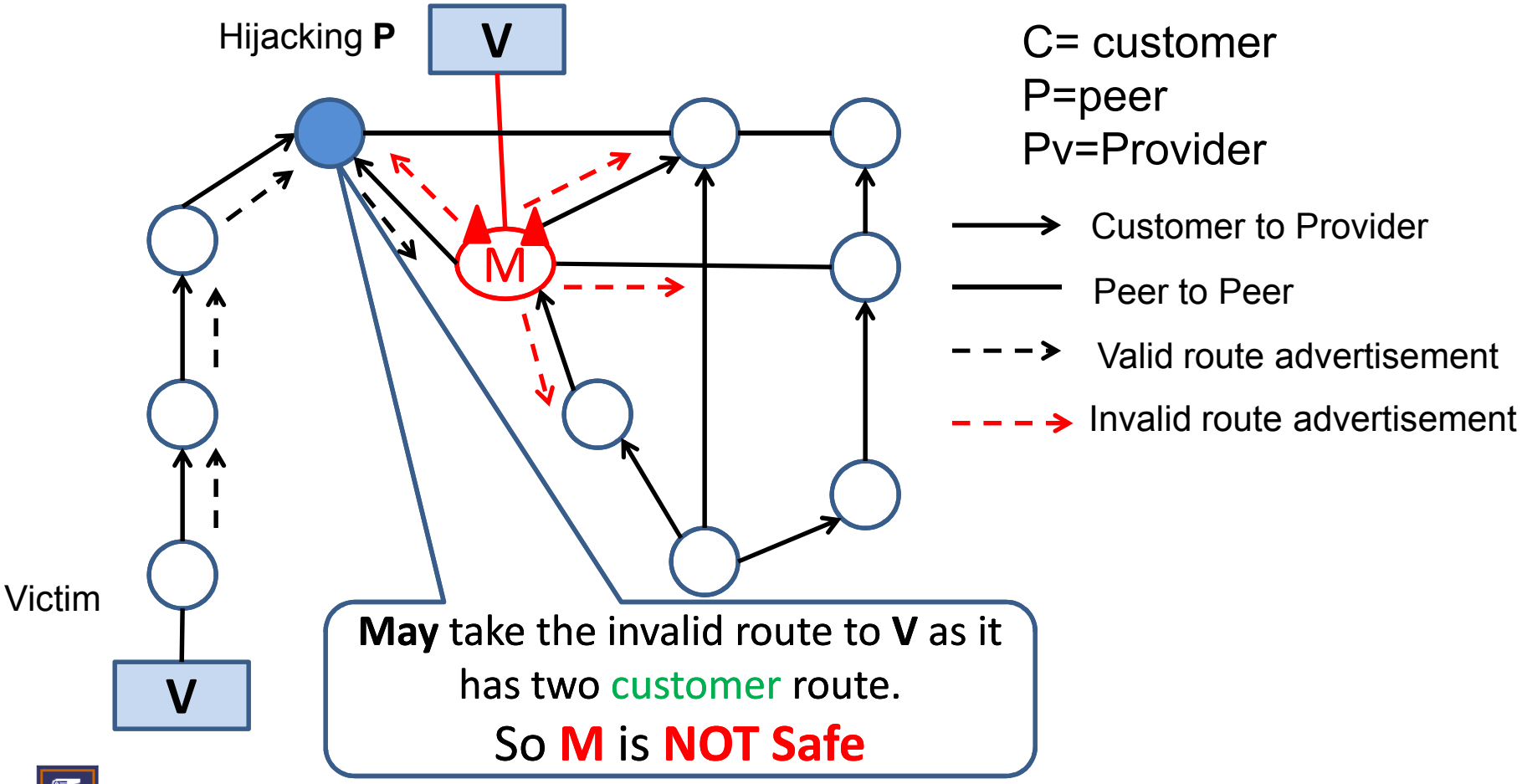
Maintaining Valid Interception Path

Case 4-6: Existing route=P & Advertising Invalid route to=C/P/Pv



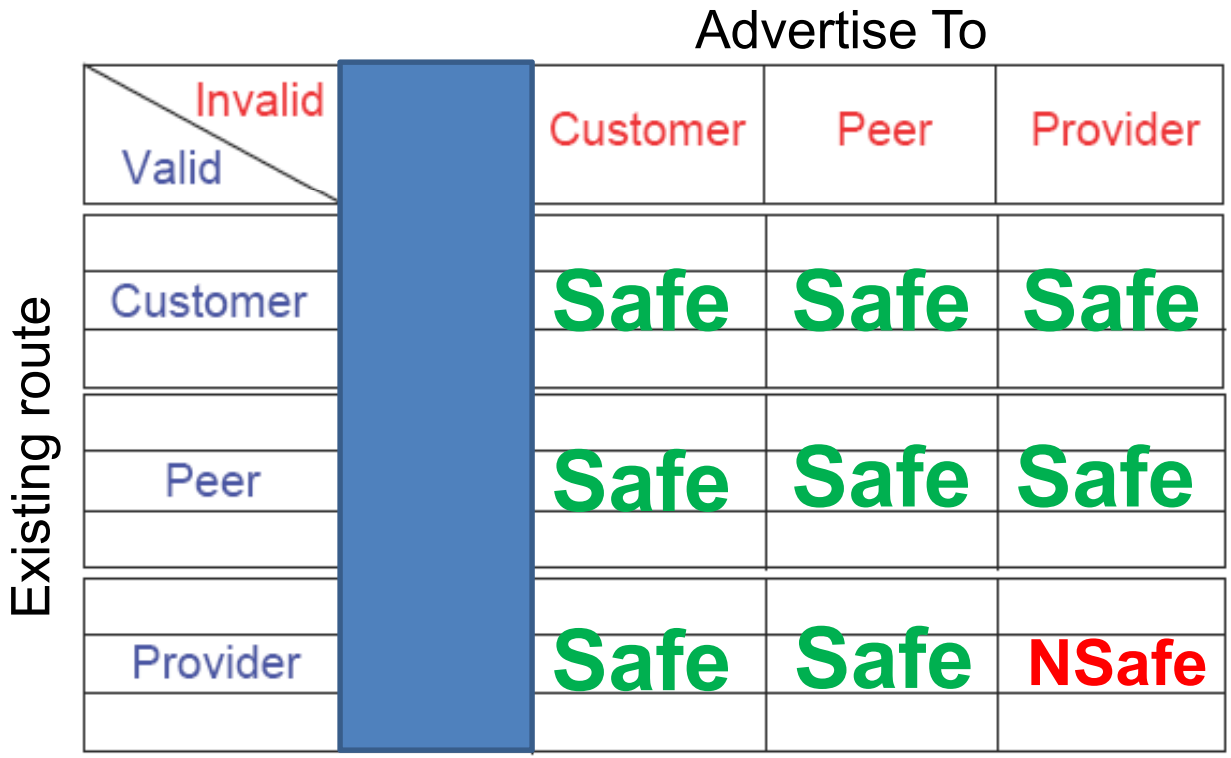
Maintaining Valid Interception Path

Case 7-9: Existing route=Pv & Advertising Invalid route to=C/P/Pv



Conditions for Interception

Invalid advertisement to a provider can violate the safety condition if the manipulator's valid route is through a provider

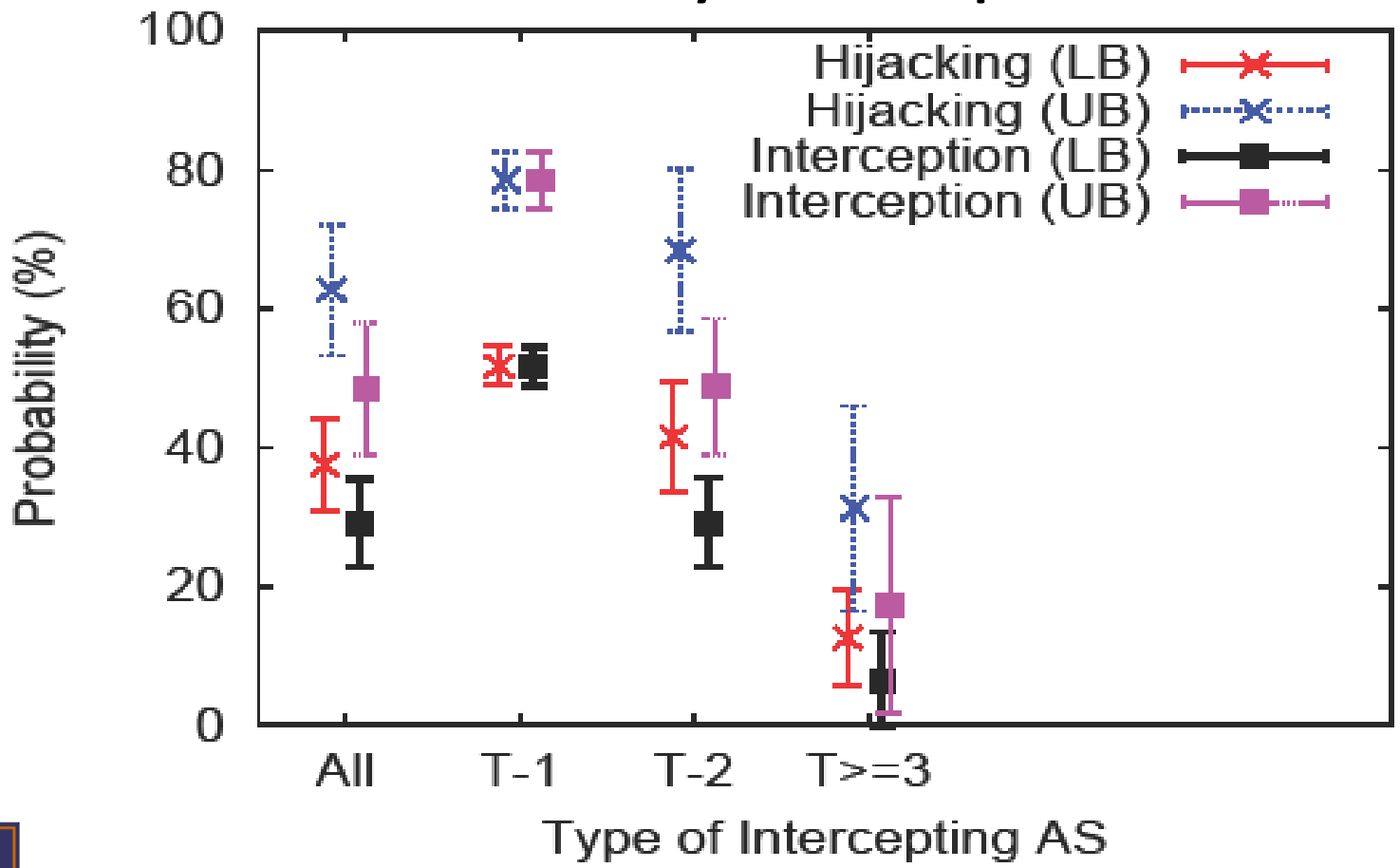


Safe = safe to advertise

NSafe = not safe to advertise

Hijacking and Interception Estimates

1. **Probability of Hijacking**
2. **Probability of Interception**



Verifying Estimates against known events

Prefix	Owner (AS name)	Hijacker	Estimated Hijacking LB-UB %	Actual Hijack--ing (%)
64.233.161.0/24	Google	Cogent	35.5-64.5	45.2
12.173.227.0/24	MarthaStewart Living	ConEd.	36.4-84.9	42.4
63.165.71.0/24	Folksamerica	"	39.4-72.7	39.4
64.132.55.0/24	OverseasMedia	"	18.2-51.5	18.2
65.115.240.0/24	ViewTrade	"	27.2-54.5	21.2
65.209.93.0/24	LavaTrading	"	39.4-72.7	45.5
66.77.142.0/24	Folksamerica	"	90.9-90.9	90.9
66.194.137.0/24	MacKayShields	"	18.2-57.5	27.3
66.207.32.0/20	ADI	"	45.5-66.7	63.6
69.64.209.0/24	TheStreet.Com	"	72.7-81.8	84.8
160.79.45.0/24	RhodesASN	"	27.3-75.8	51.5
160.79.67.0/24	TheStreet.Com	"	60.6-75.8	69.7
192.251.16.0/24	T&TForex	"	27.3-57.6	27.3
198.15.10.0/24	TigerFund	"	0-1	60.6
204.13.72.0/24	FTENNY	"	93.9-93.9	75.8
216.223.46.0/24	SDSNY	"	51.5-78.8	18.2

Thank You