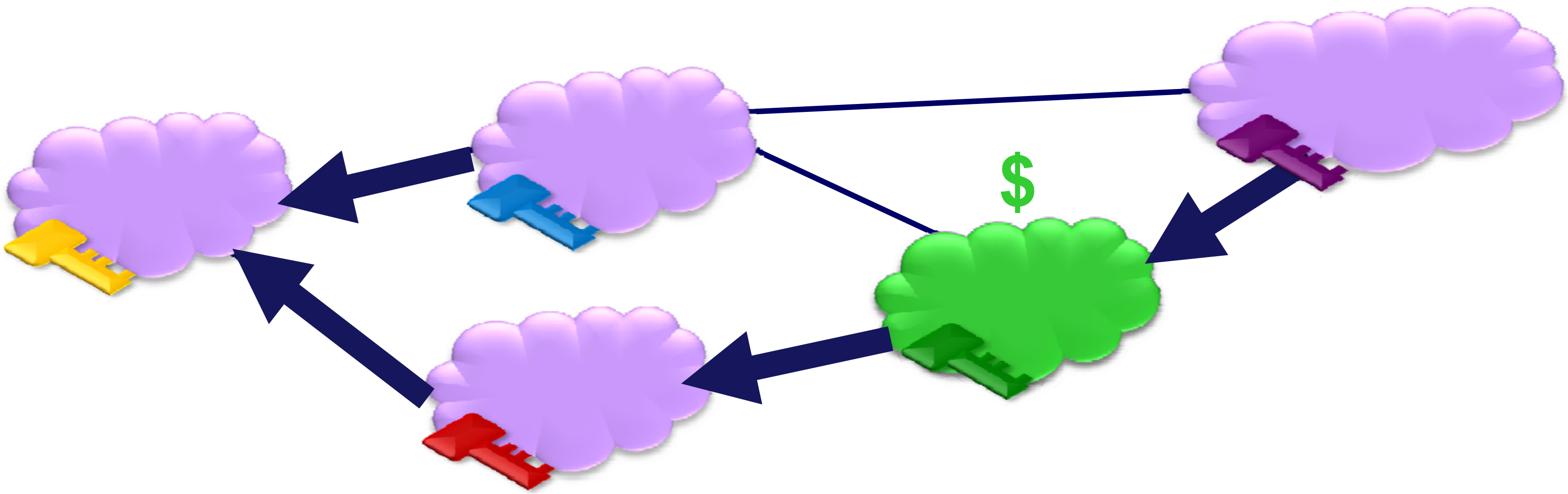
Jobtalk

Securing Internet Routing

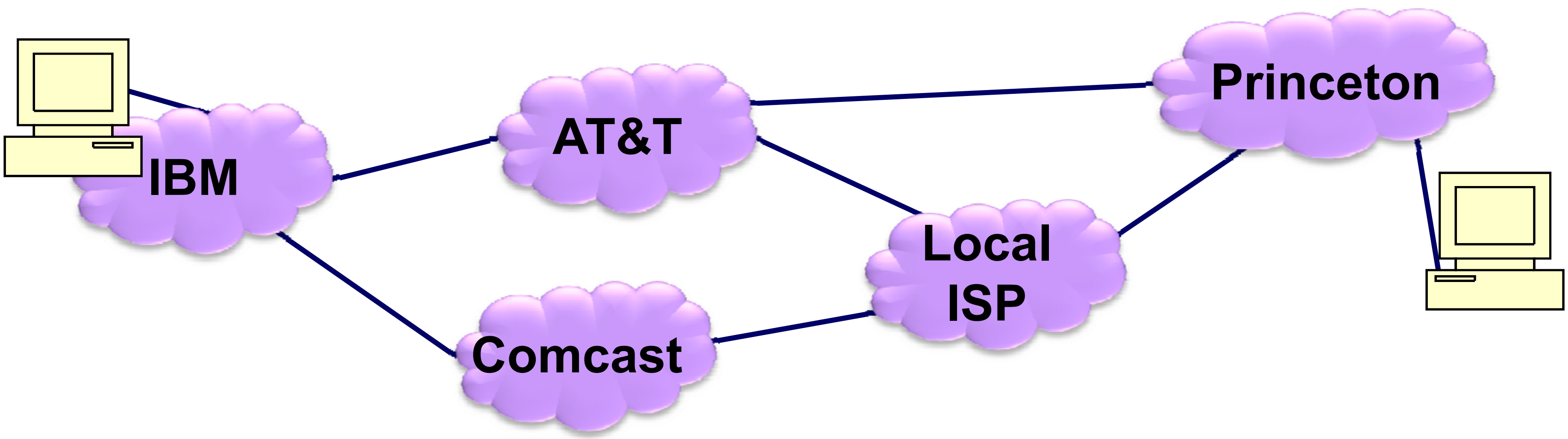


Sharon Goldberg
Princeton University

Based on work with:
Boaz Barak, Shai Halevi, Aaron Jaggard, Vijay Ramachandran,
Jennifer Rexford, Eran Tromer, Rebecca Wright, and David Xiao

The Internet (1)

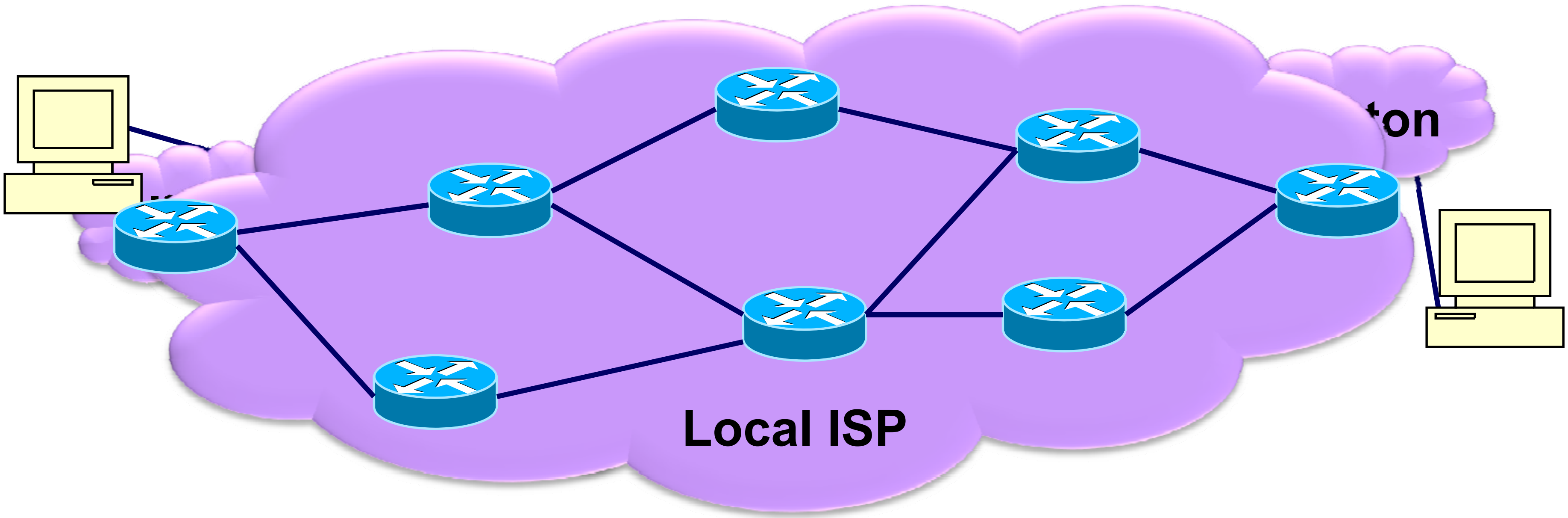
The Internet is a collection of Autonomous Systems (AS).



Connectivity requires competing ASes to cooperate.

The Internet (2)

Each Autonomous System (AS) is a collection of routers.



Different Failure Models & Formal Techniques

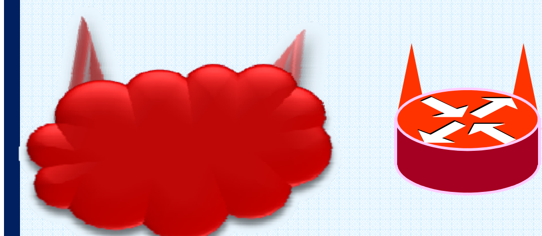
Honest
- Follows the protocol

Benign / Fail-Stop
- Stops responding

The Internet was designed for this.

Game Theory

Rational (Selfish)
- Deviates from protocol for personal gain



Cryptography

Adversarial
- Actively tries to “break” the protocol

Research Approach

Iterate

System
(Goal)

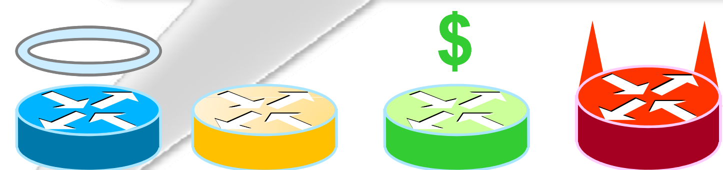
engineering & economic limitations

Define Security Property

+

Choose Failure Model

Prove **this** protocol satisfies security for failure model.

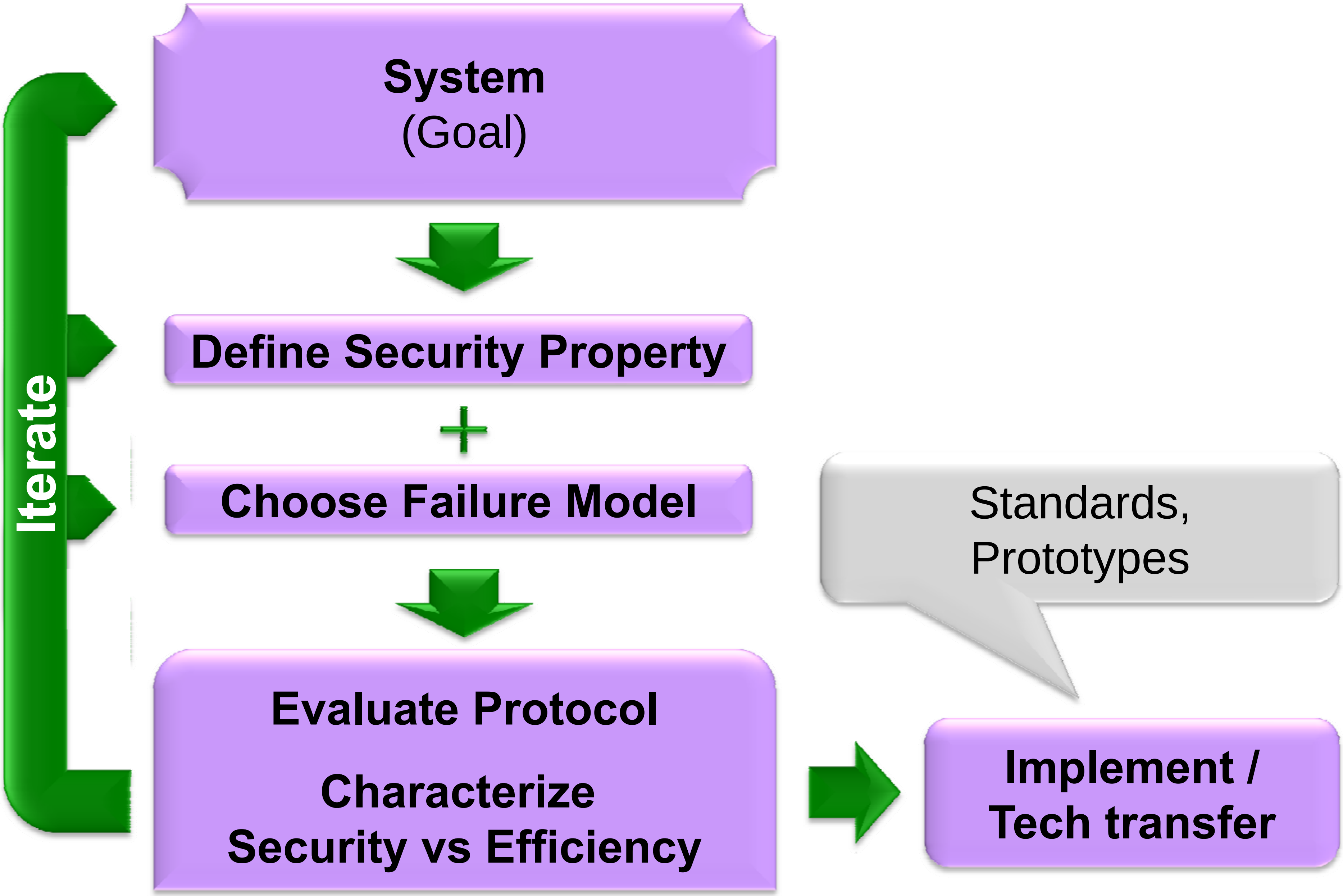


Evaluate Protocol

Characterize Security vs Efficiency

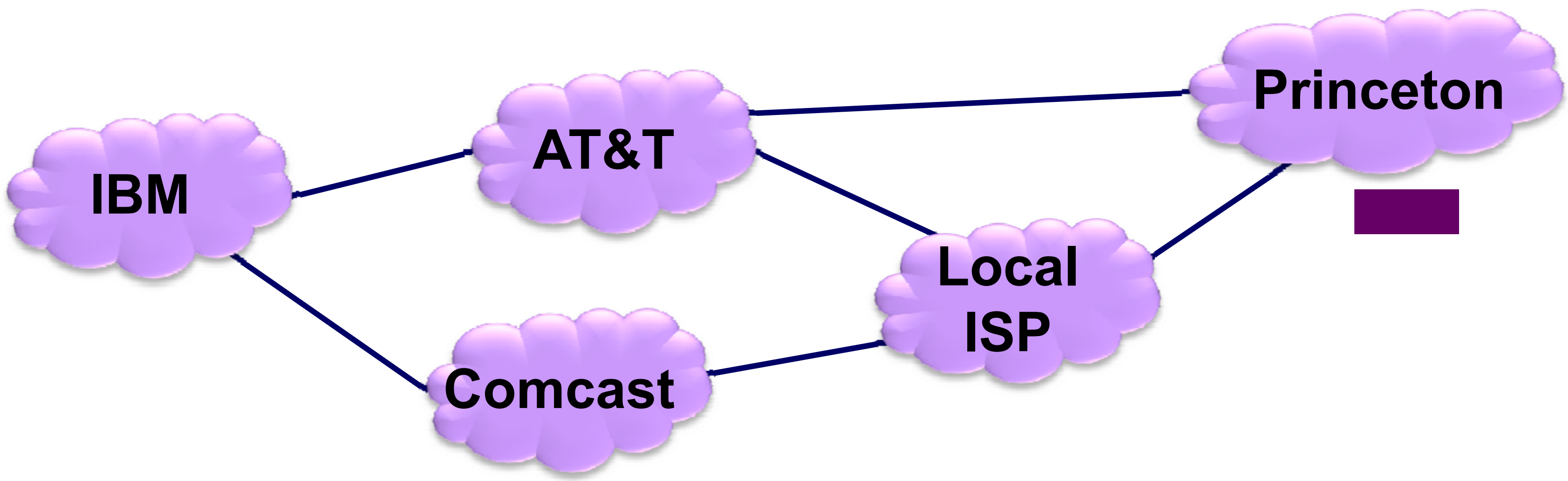
Any protocol with security property X needs resource Y

Research Approach



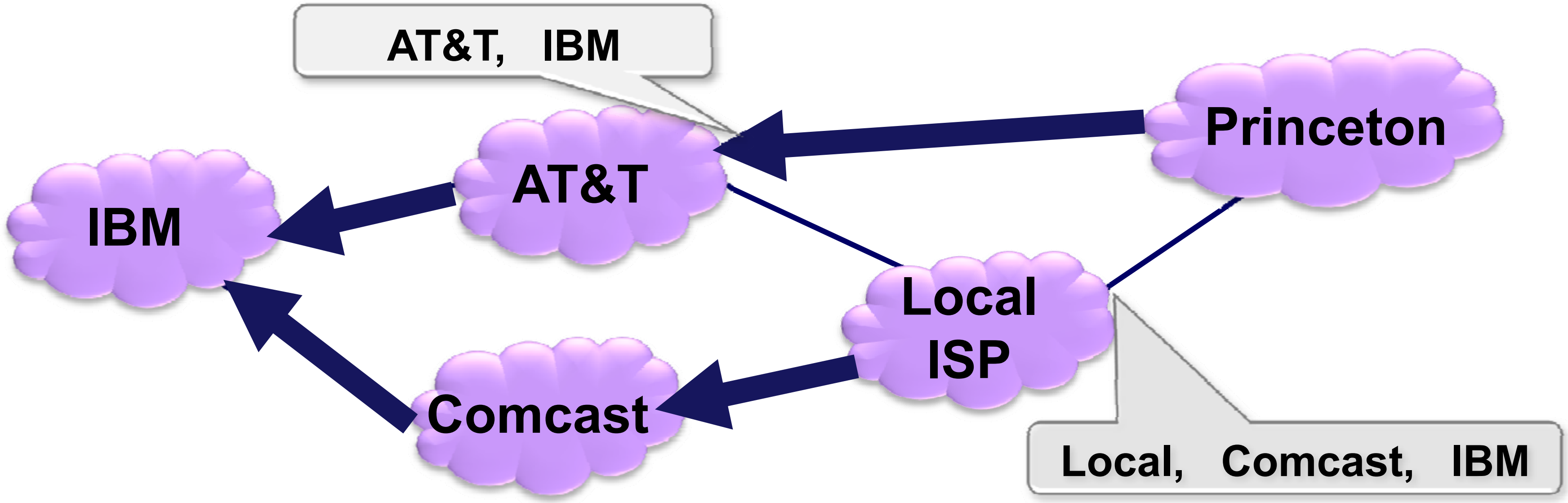
Secure Routing on the Internet

Goal: Ensure packets arrive at their destination.



Years of security research devoted to solving this problem.

Overview of Previous Work on Secure Routing



Control Plane (Routing protocols):

- Set up paths between nodes

Secure BGP [Kent Lynn Seo 00]	**soBGP, IRV, SPV, pgBGP, psBGP, Listen-Whisper, etc.,**

Data Plane:

- Given the paths, how should packets be forwarded?

NPBR [Perlman 88], Secure Msg Transmission [DDWY92], Secure/Efficient Routing [AKWK04], Secure TR [PS03], etc!

Overview of Previous Work on Secure Routing

To inform deployment efforts, my research focuses on:

1. Are we securing the right part of the system?
2. Characterizing the tradeoffs between security & efficiency

Control Plane (Routing protocols):

- Set up paths between nodes

Secure BGP [Kent Lynn Seo 00]

soBGP, IRV, SPV, pgBGP, psBGP, Listen-Whisper, etc.,

Data Plane:

- Given the paths, how should packets be forwarded?

NPBR [Perlman 88], Secure Msg Transmission [DDWY92], Secure/Efficient Routing [AKWK04], Secure TR [PS03], etc!

Overview of the Results in this Talk

Internet Routing
(Ensuring packets arrive at their destination)

Ensure packets actually follow announced paths.

+

$

Rational ASes

[GHJRW, SIGCOMM'08]
Known control-plane protocols, like Secure BGP

Detect packet loss & localize bad router.

+

Adversarial routers

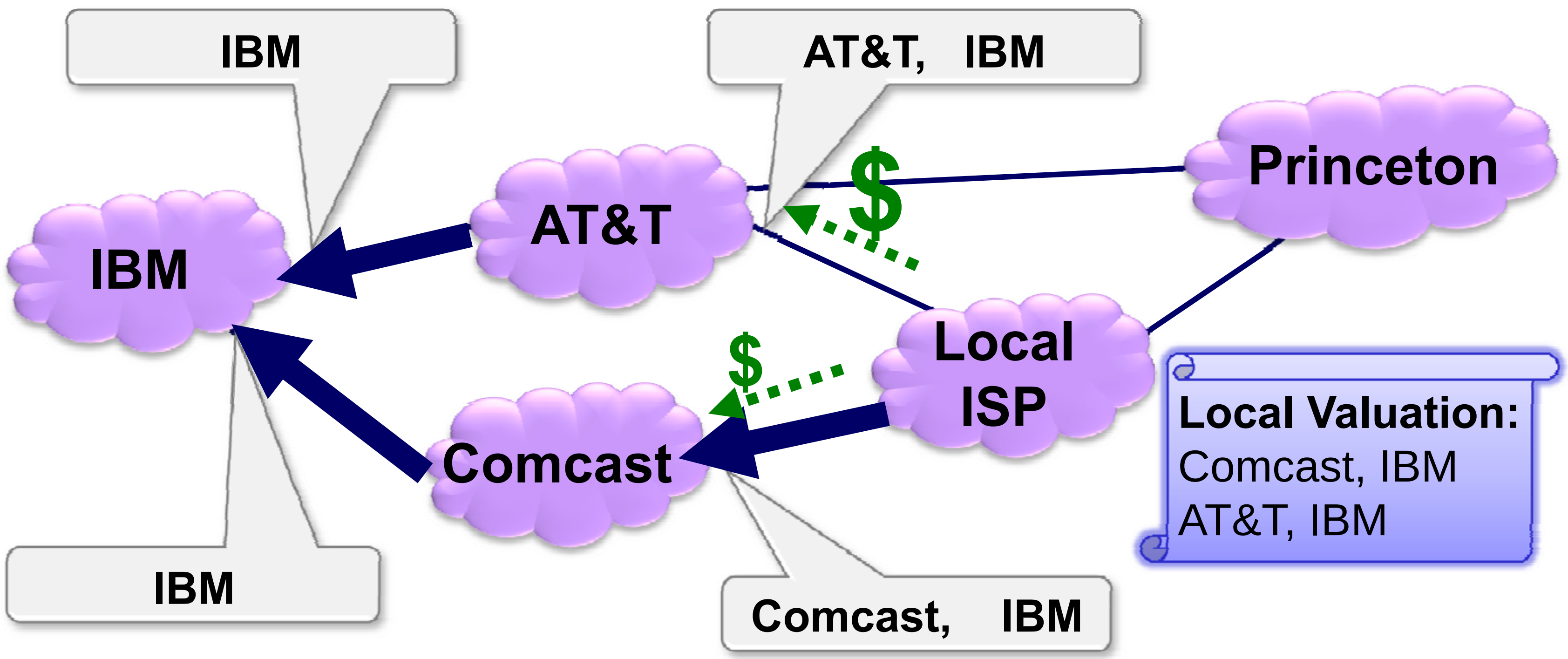
[GXTBR, SIGMETRICS'08]
[BGX, EUROCRYPT'08]
New data-plane protocols & characterization

Part I : The Control Plane

two counterexamples & a theorem

BGP: The Internet Routing Protocol (1)

Paths between Autonomous Systems (ASes) are set up via the Border Gateway Protocol (BGP).



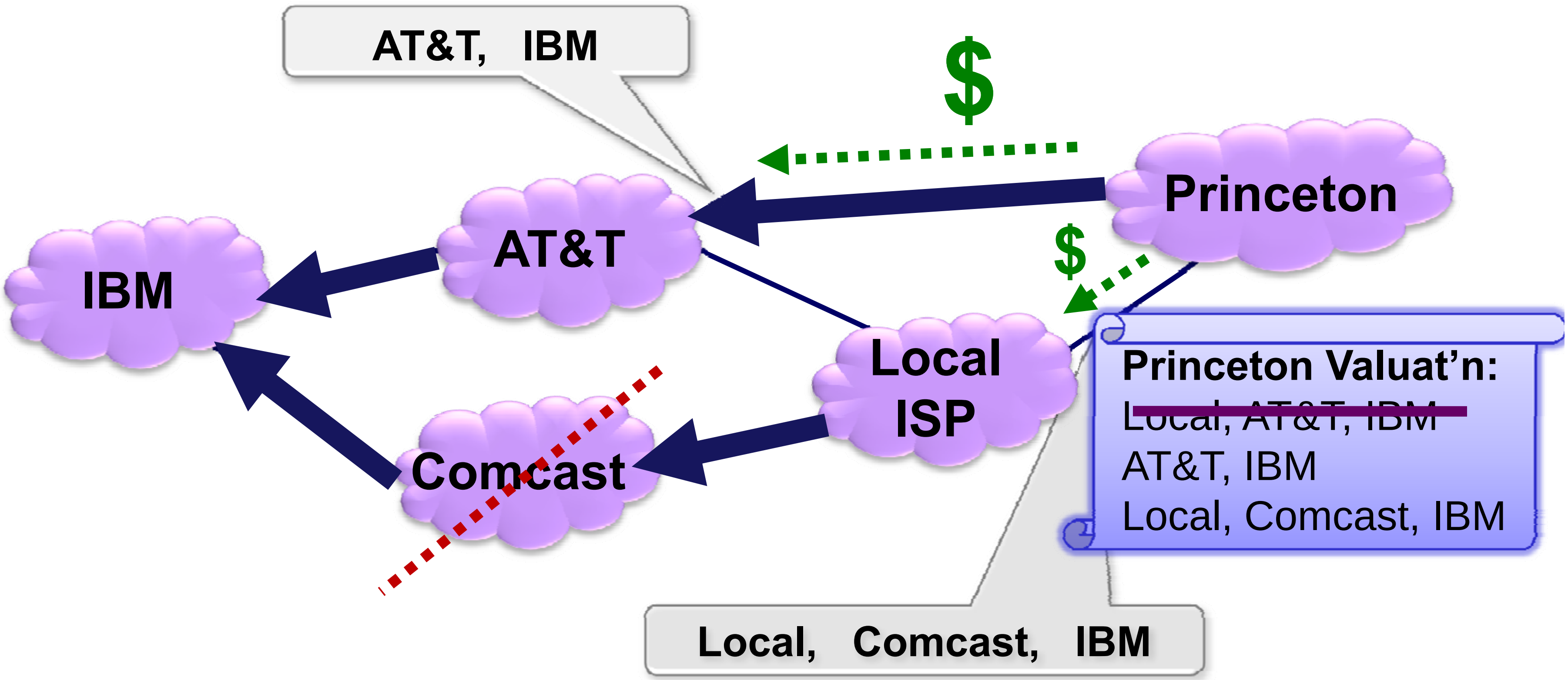
Forwarding: Node use **single** outgoing link for all traffic to destination.

Valuations: Usually based on economic relationships.

Here, we assume they are fixed at “beginning of game”

BGP: The Internet Routing Protocol (2)

Paths between Autonomous Systems (ASes) are set up via the Border Gateway Protocol (BGP).



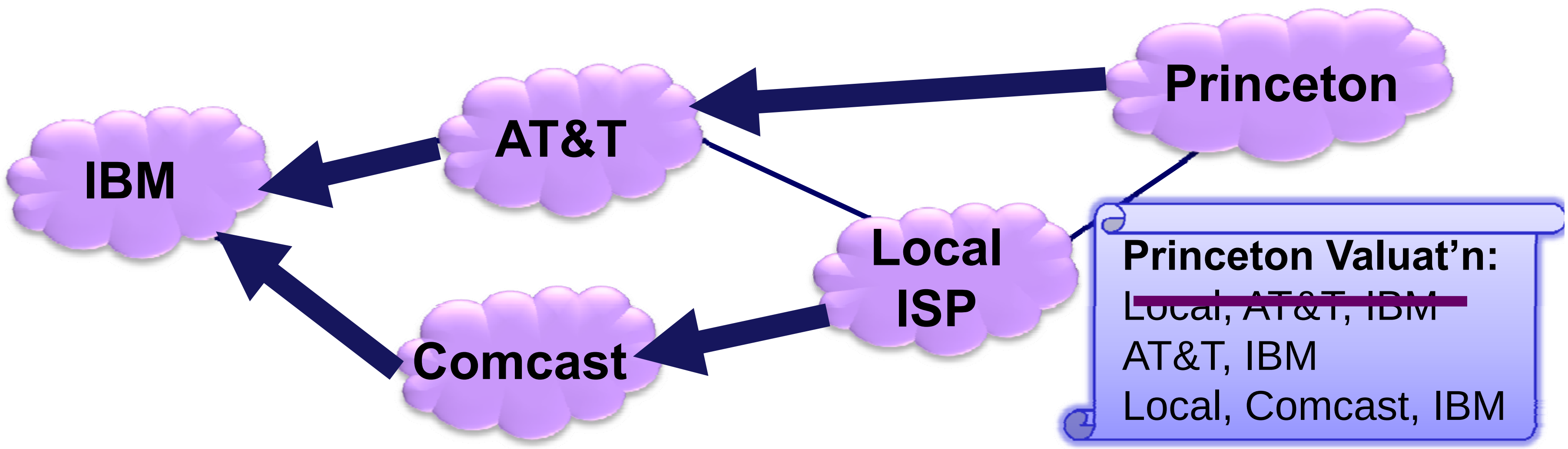
Forwarding: Node use **single** outgoing link for all traffic to destination.

Valuations: Usually based on economic relationships.

Here, we assume they are fixed at "beginning of game"

Our desired security goal…

BGP announcements match actual paths in the data plane.

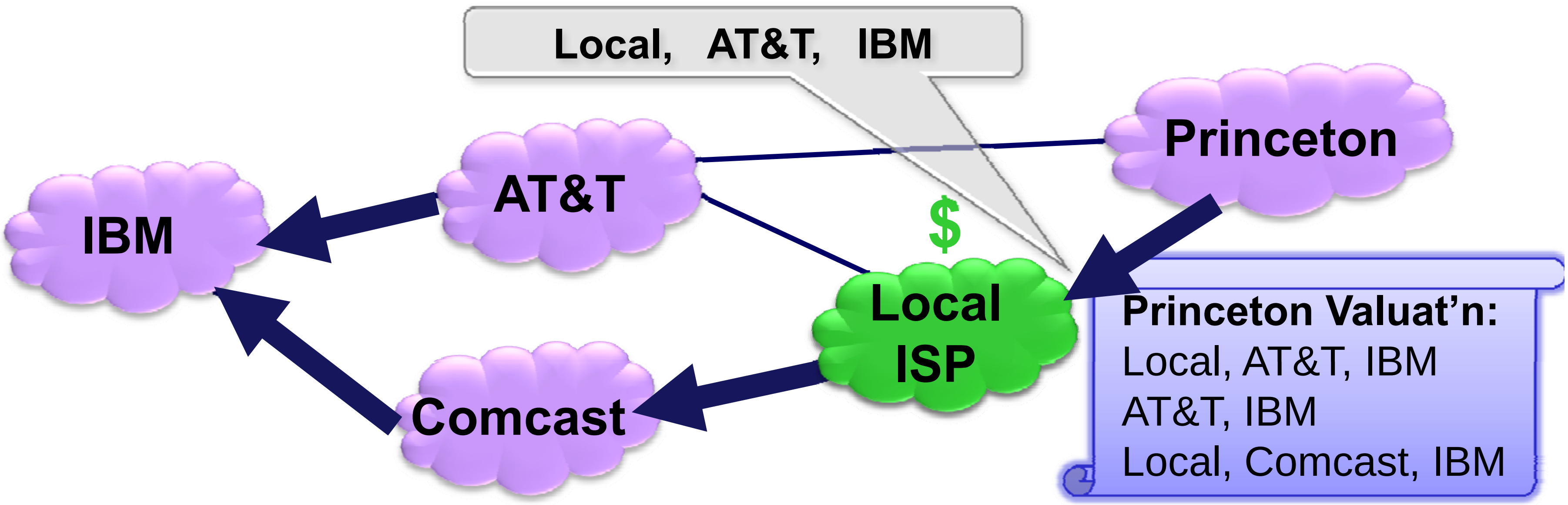


Then, can use BGP messages as input to security schemes!

1. Chose paths that avoid ASes known to drop packets
2. Protocols that localize an adversarial router on path.
3. Contractual frameworks that penalize nodes that drop packets.

Our desired security goal…

BGP announcements match actual paths in the data plane.

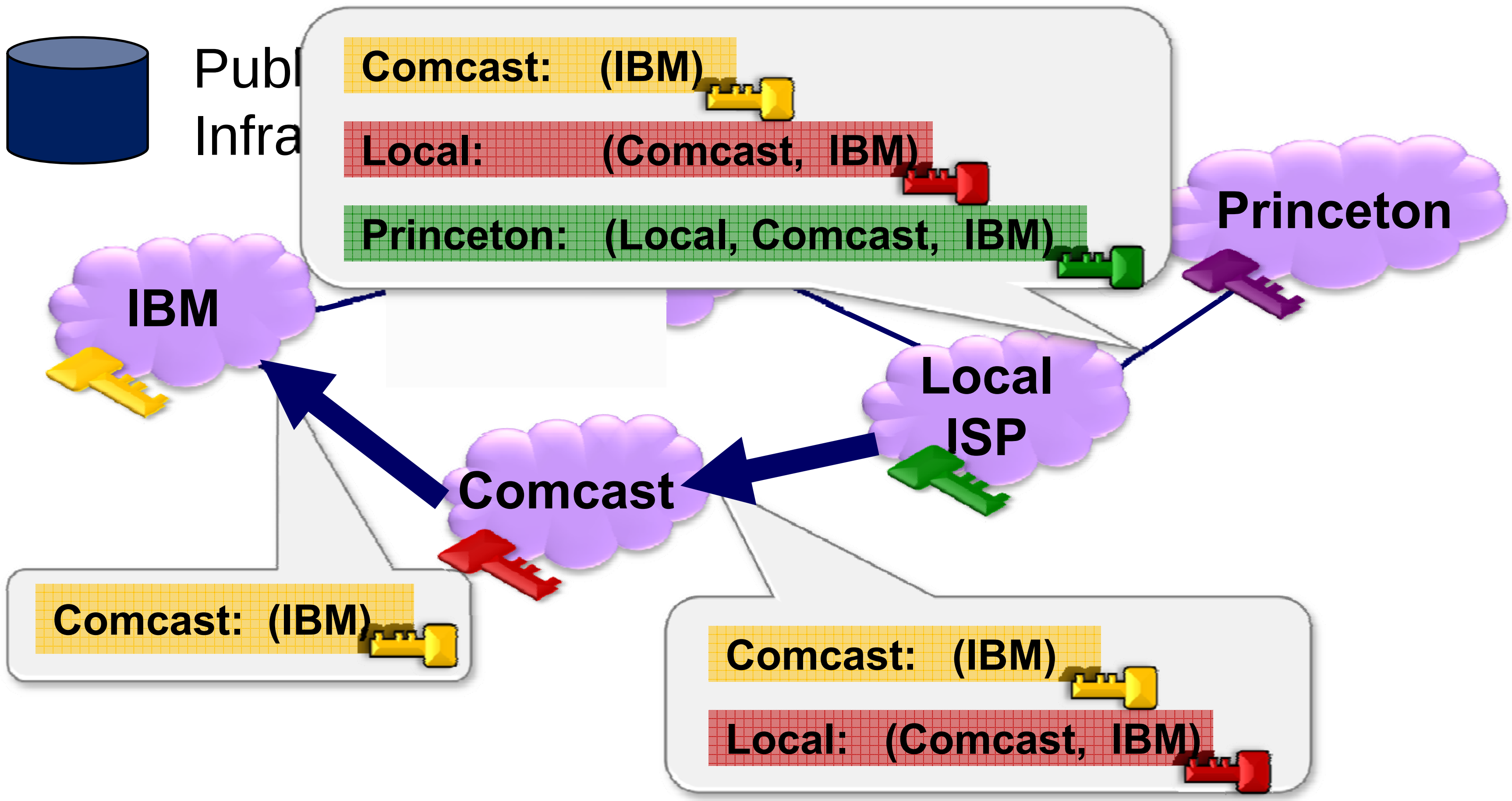


Then, can use BGP messages as input to security schemes!

1. Chose paths that avoid ASes known to drop packets
2. Protocols that localize an adversarial router on path.
3. Contractual frameworks that penalize nodes that drop packets.

The “Secure BGP” Internet Routing Protocol

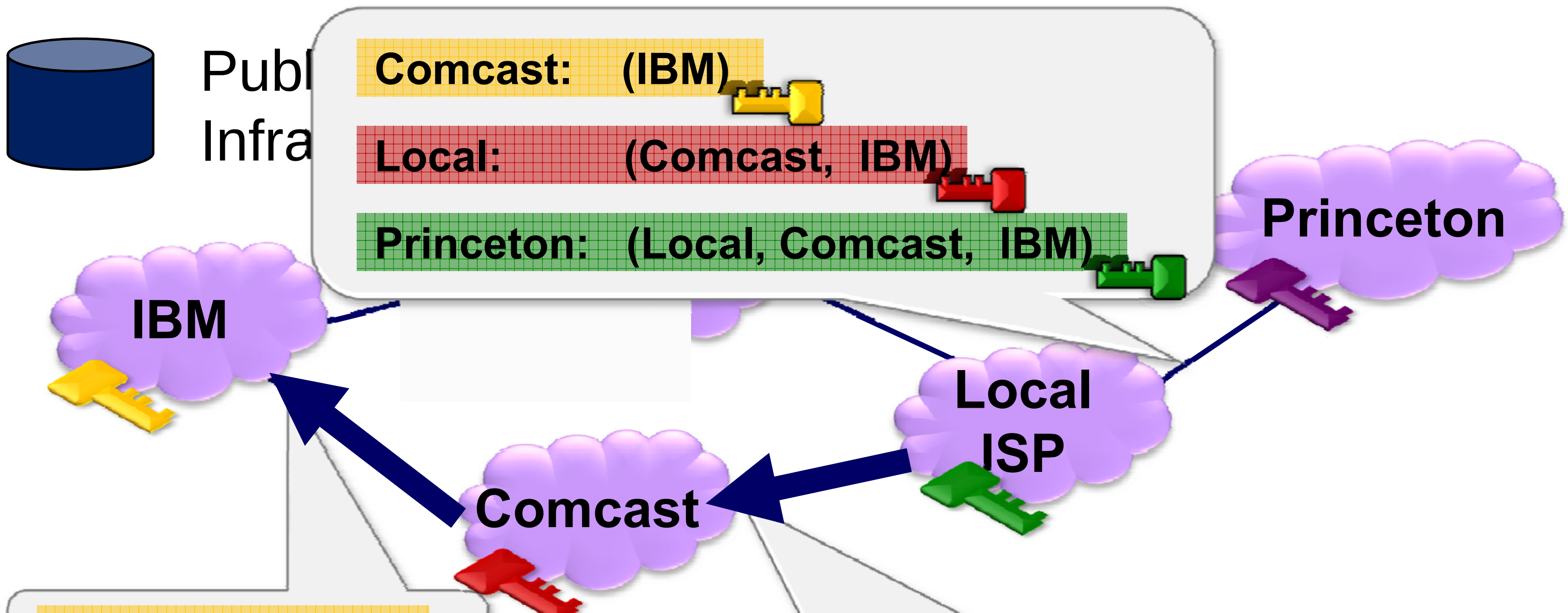
If AS **a** announced path **abP** then **b** announced **bP** to **a**



Public Key Signature: Anyone who knows IBM’s public key can verify the message was sent by IBM.

The "Secure BGP" Internet Routing Protocol

If AS **a** announced path **abP** then **b** announced **bP** to **a**



If we assume nodes are rational,
do we get security from "Secure BGP"?

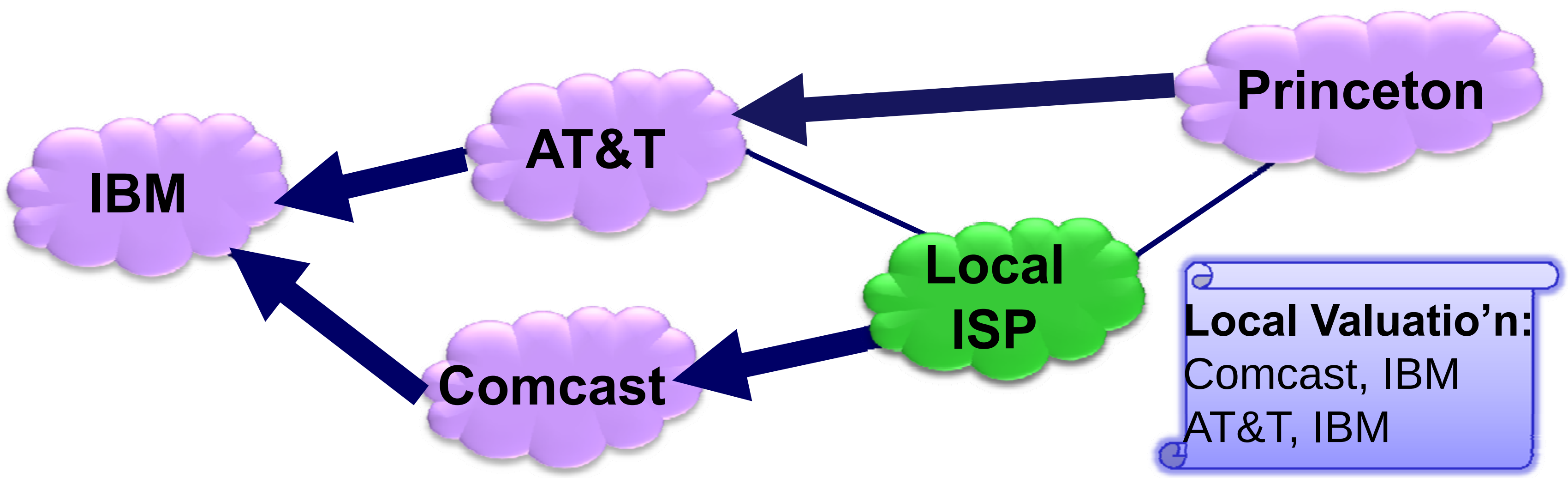
Yes - For certain utility models (prior work)

No - For more realistic ones (our work)

The "No Attractions" model of utility…

Model of utility in prior work:

Utility of **AS** **=** Utility of outgoing (data-plane) path



In all prior work: Utility is determined by the valuation function

Do control plane & data plane match?

Utility Model	Secure BGP
No Attractions	[LSZ]

✓ **Corollary: If __________, rational ASes have no incentive to send dishonest BGP announcements!**

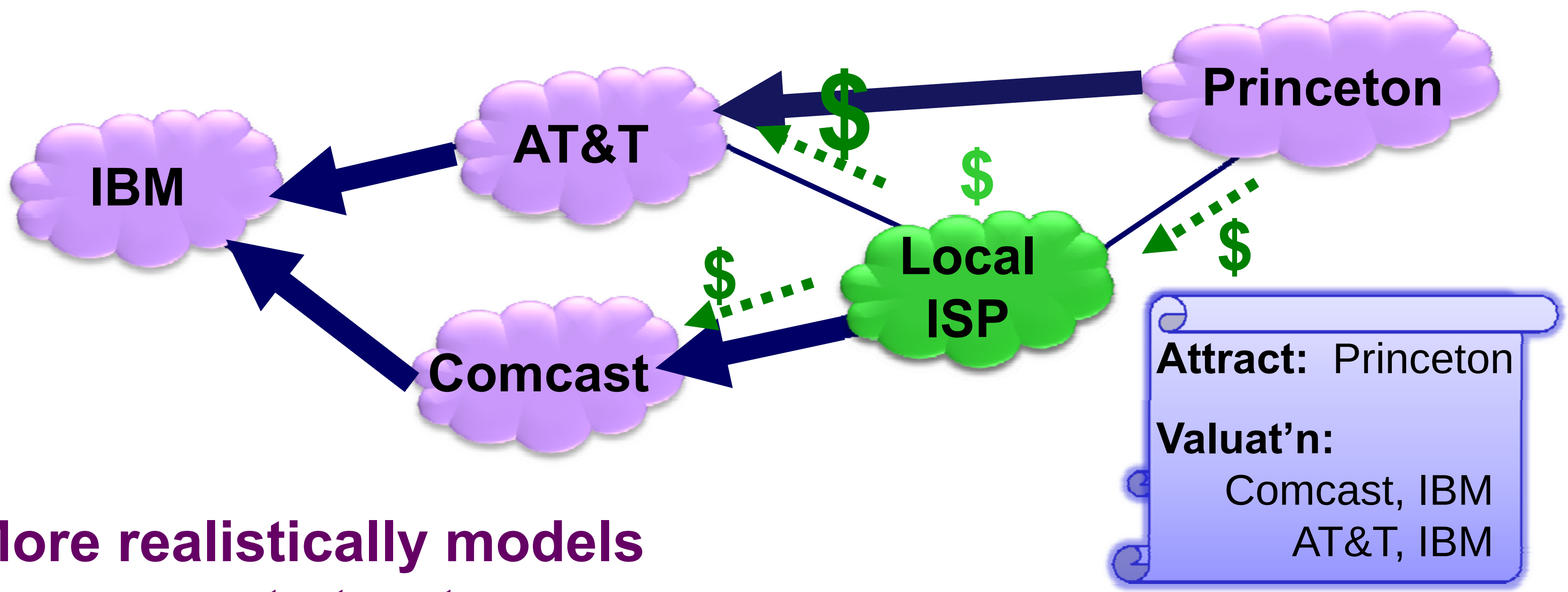
- [Feigenbaum-Ramachandran-Schapria-06], [Feigenbaum-Schapria-Shenker-07] [Levin-Schapira-Zohar-08]

- **These results build on**
- [Nisan-Ronen-01] [Feigenbaum-Papadimitriou-Shenker-01], [Parkes-Shneidman-04], [Feigenbaum-Karger-Mirrokni-Sami-05] Feigenbaum-Papadimitriou-Sami-Shenker-05],

The “Attractions” model of utility…

Our model of utility:

Utility of **AS** **=** Utility of outgoing (data-plane) path **+** Utility of attracted incoming traffic



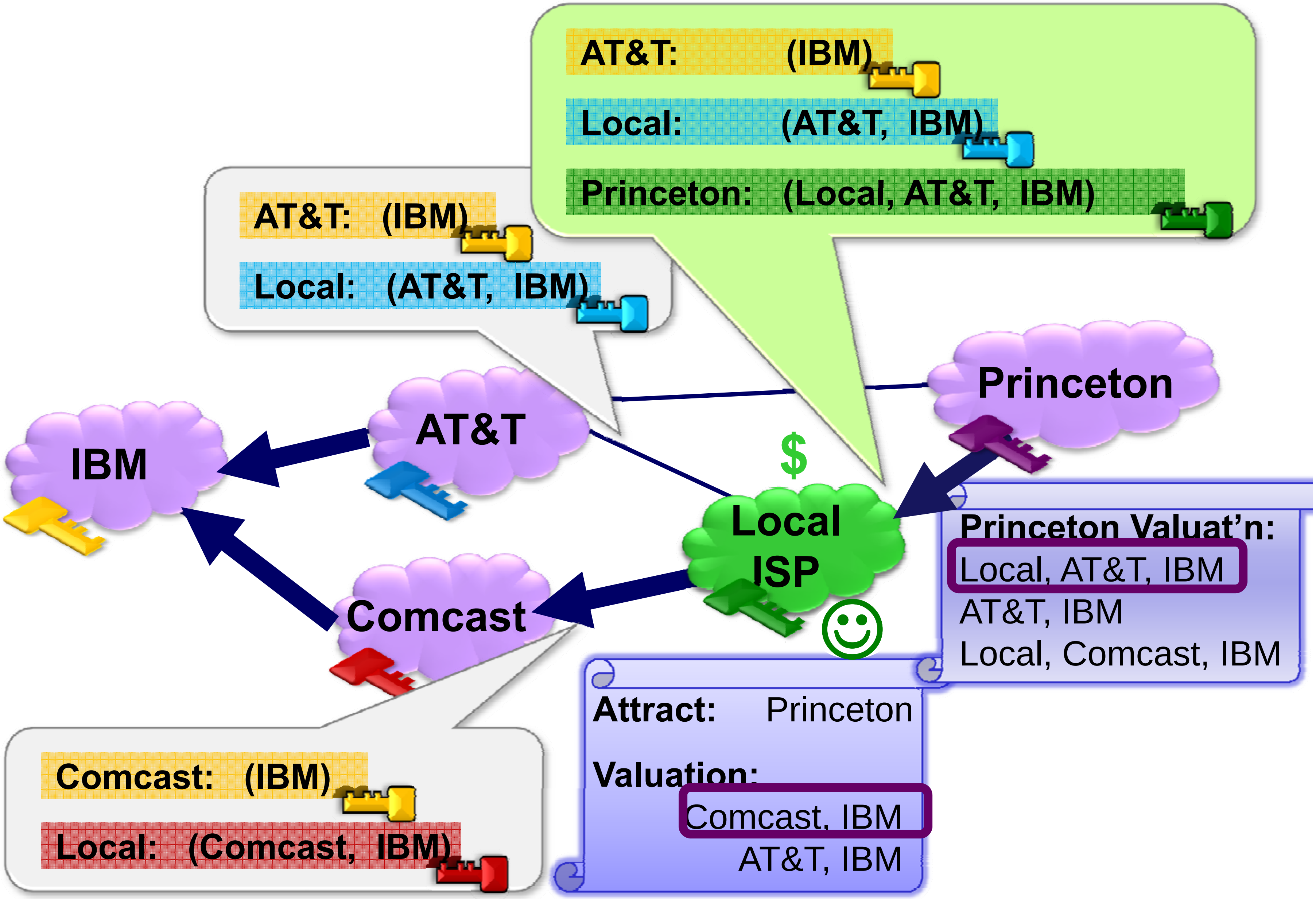
More realistically models payment structure.

Do control plane & data plane match?

Utility Model	Secure BGP
No Attractions	[LSZ]
Attractions	X

Negative result is network where a node has incentive to lie.

Counterexample: “Secure BGP” is not sufficient!



Do control plane & data plane match?

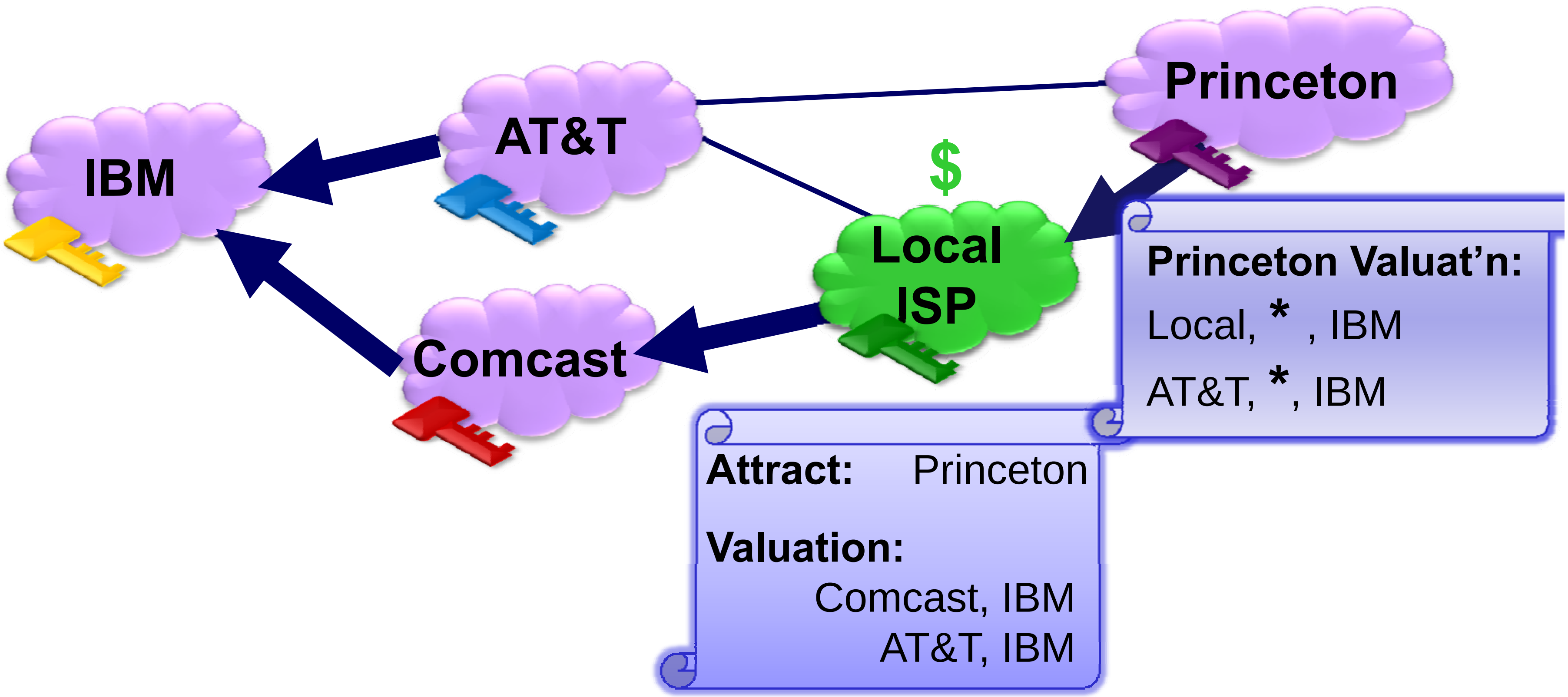
Utility Model	Secure BGP		Next-hop Policy
No Attractions	[LSZ]	OR	[FRS]
Attractions	X		?

Next-hop policy: Valuations depend only on 1st AS to receive traffic.

What if everyone used next-hop policy?

Next-hop policy: Valuations depend only on 1st AS to receive traffic.

The bad example goes away.

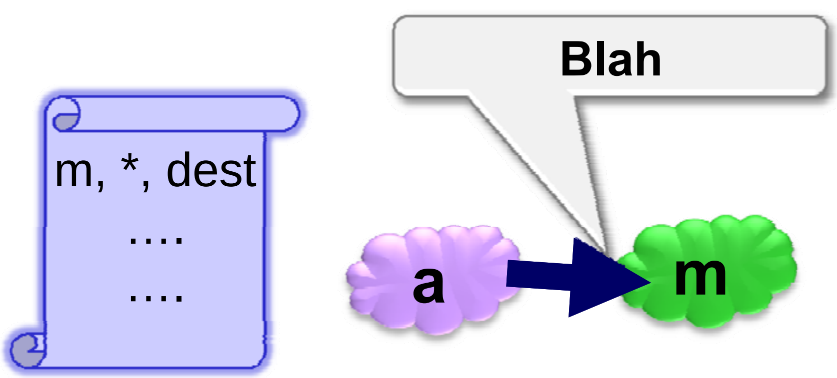


Do control plane & data plane match?

	Secure BGP		Next-hop Policy
No Attractions	[LSZ]	OR	[FRS]
Attractions	X		X

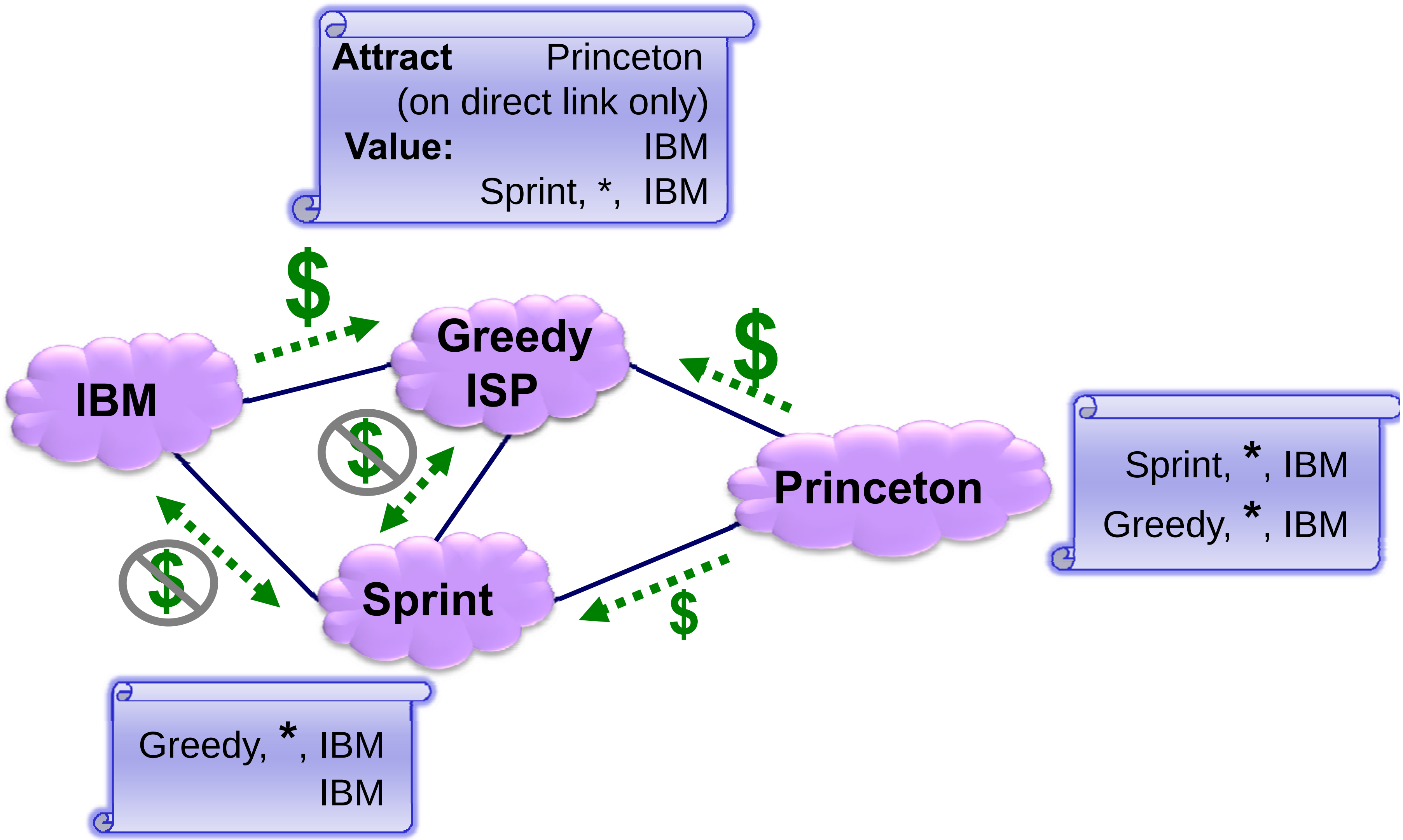
Next-hop policy, (naïve) intuition:

If **a** uses a next-hop policy, nothing **m** says affects **a.**

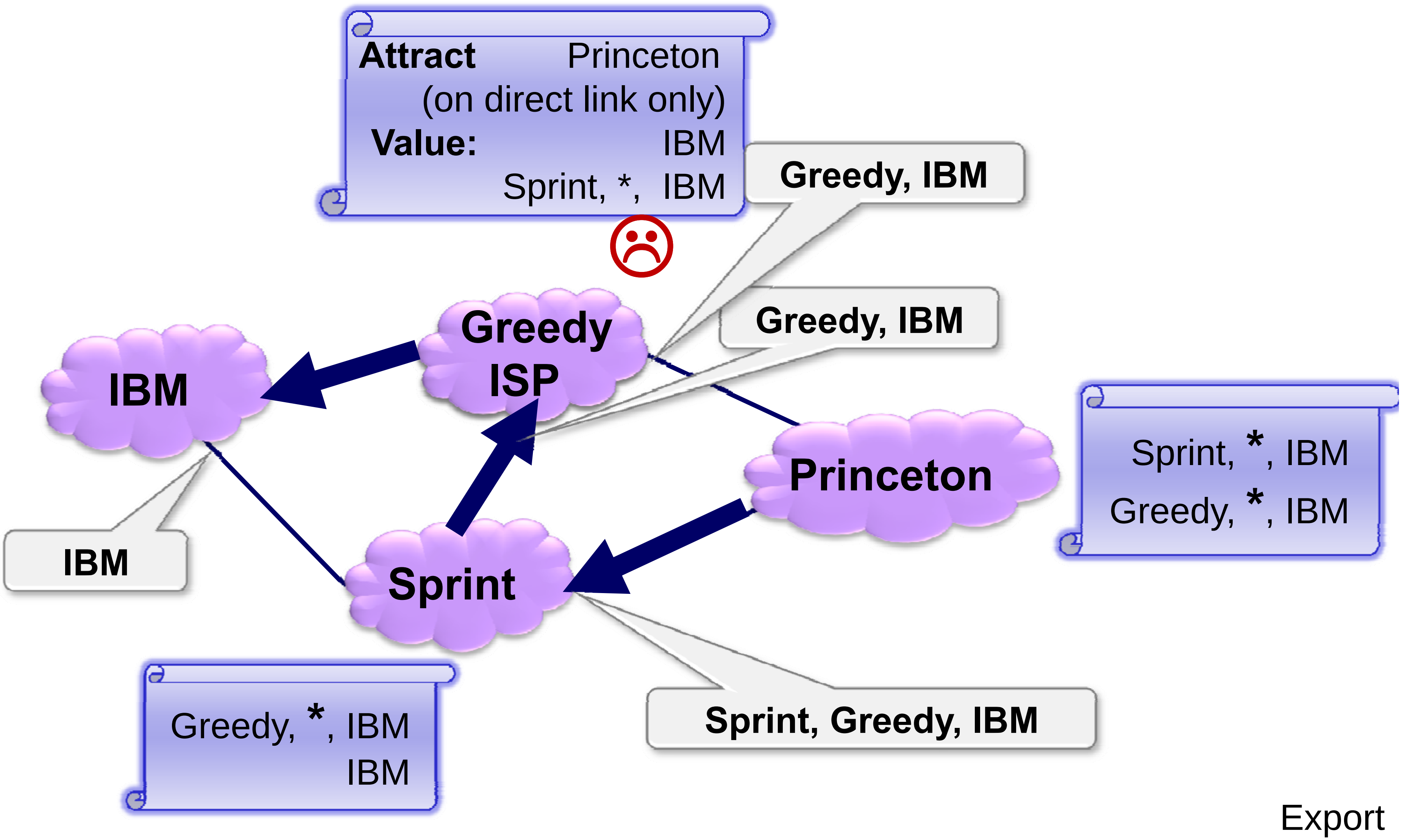


Surprisingly, intuition fails (again).

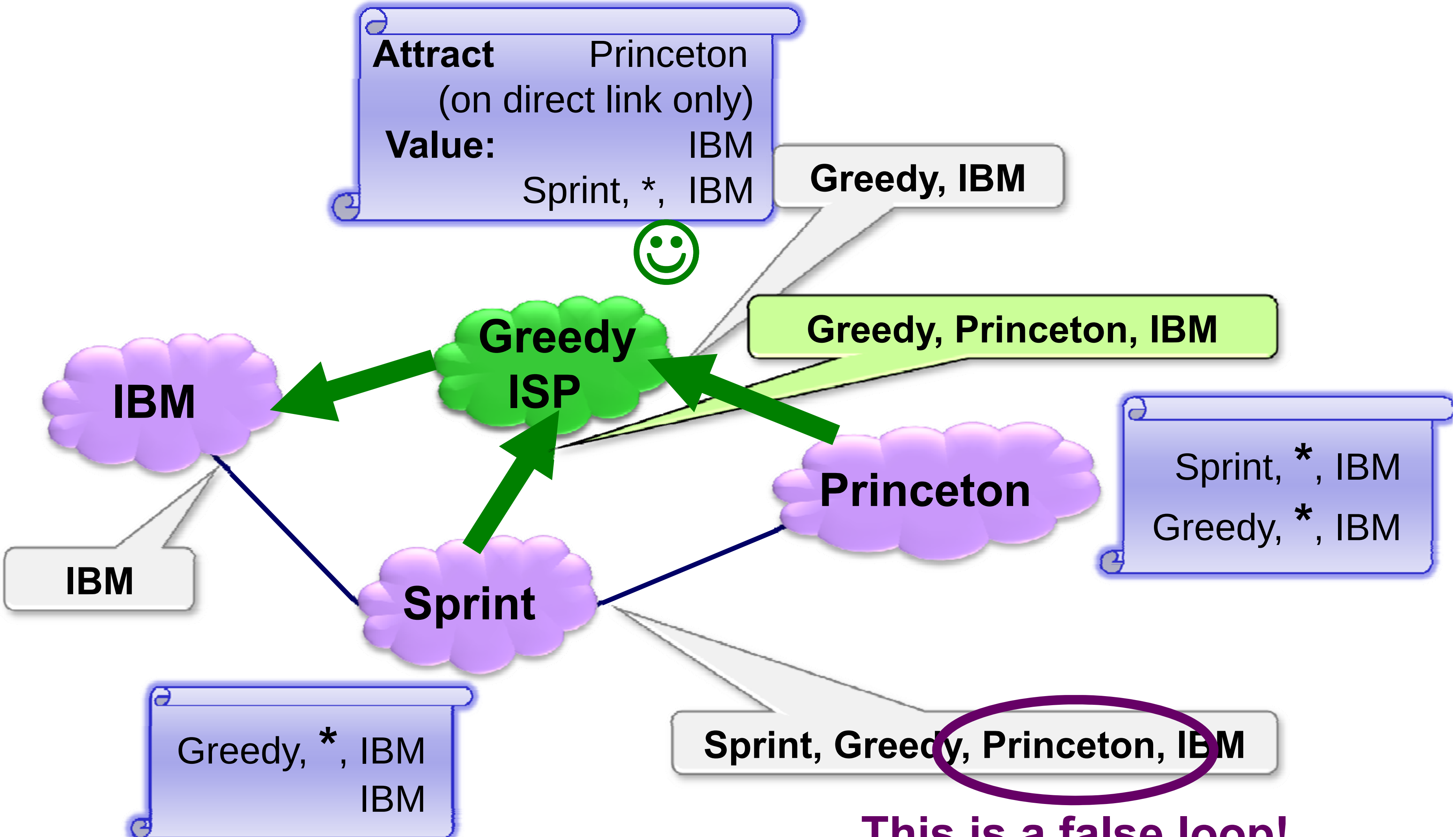
Counterexample: Next-hop policy is not sufficient! (1)



Counterexample: Next-hop policy is not sufficient! (2)



Counterexample: Next-hop policy is not sufficient! (3)

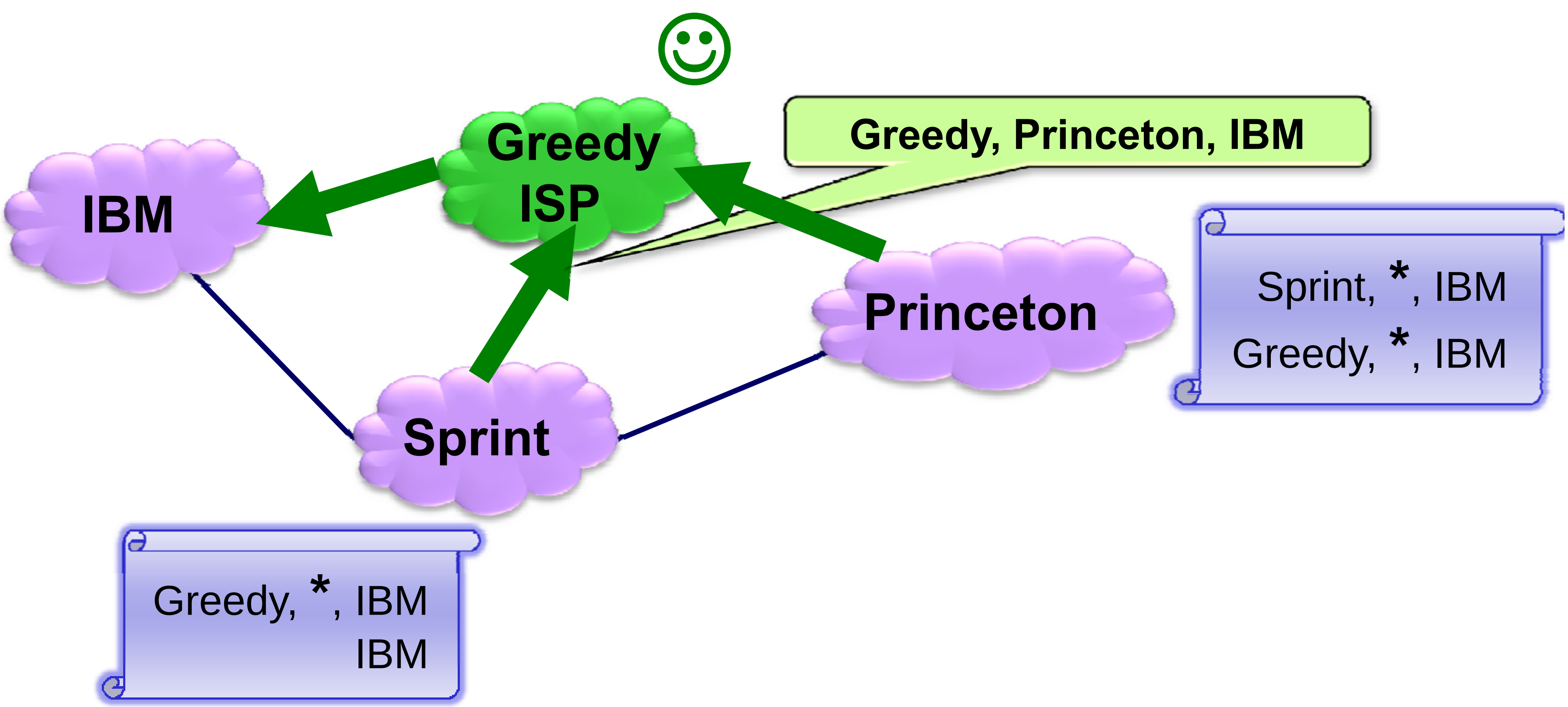


This is a false loop!

Counterexample: Next-hop policy is not sufficient! (3)

Observation: Manipulation not possible with Secure BGP.

(Also not possible if nodes use clever loop detection.)



Do control plane & data plane match?

	Secure BGP	Next-hop Policy
No Attractions	[LSZ]	[FRS]
Attractions	✓*	

Our Main Theorem

For a network with **traffic attraction** where all nodes have

1. **Next-hop valuations,** and
2. **Secure BGP;**

and there is no dispute wheel in the valuations

Then no node has an incentive to lie.

Proof Idea:

1. Assume some node gets **higher utility by lying**
2. Show some node must have announced a **false loop**.
3. Contradiction if nodes use **Secure BGP**.

Our Main Theorem

For a network with **traffic attraction** where all nodes have

1. **Next-hop valuations,** and
2. **Secure BGP;**

and there is no dispute wheel in the valuations

There is a set **H** of **“honest strategies”** such that for every node **m**, if all nodes except **m** use a strategy in **H**, then **m** has an optimal strategy in **H**.

“ex-post <u>set</u> Nash”

[Lavi-Nisan 05]

Proof Idea:

1. Assume some node gets **higher utility by lying**
2. Show some node must have announced a **false loop**.
3. Contradiction if nodes use **Secure BGP**.

Securing the Control Plane: Conclusions

	Secure BGP	Next-hop Policy
No Attractions	[LSZ]	[FRS]
Attractions	✓*	✓*

These routing policies are not realistic.

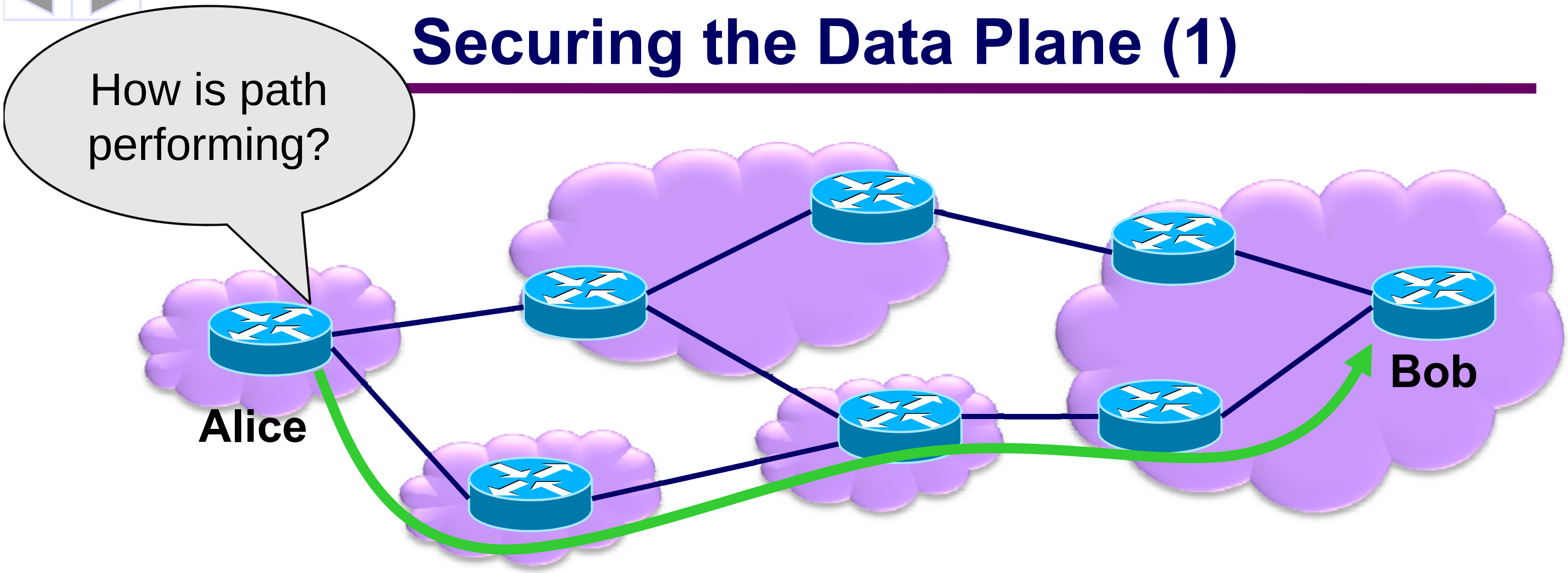
⇨ Incentives to announce false paths, even if ASes are rational and use "Secure BGP"

⇨ Motivates more work on data plane security

Part II : The Data Plane

two theorems & a protocol

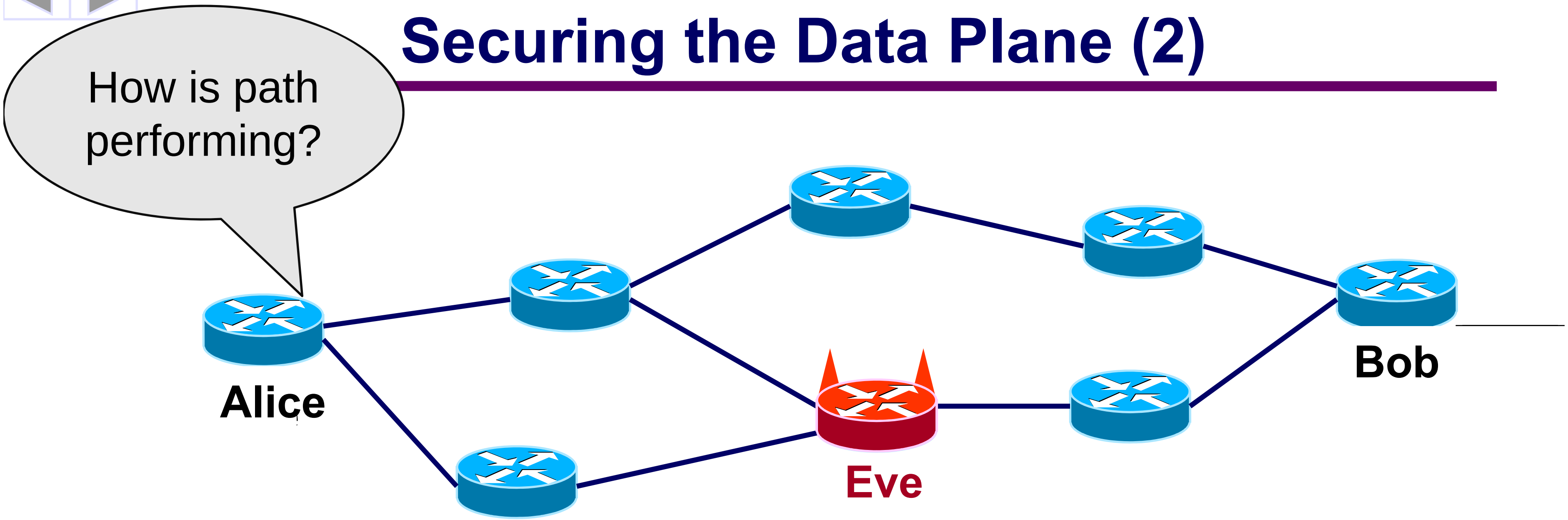
Securing the Data Plane (1)



Detection: Does packet loss / corruption rate exceed 1% ?

Localization: If so, which router is responsible?

Securing the Data Plane (2)



Knows monitoring protocol

Add / **drop** / **modify** / **reorder** packets

Wants to hide packet loss from Alice

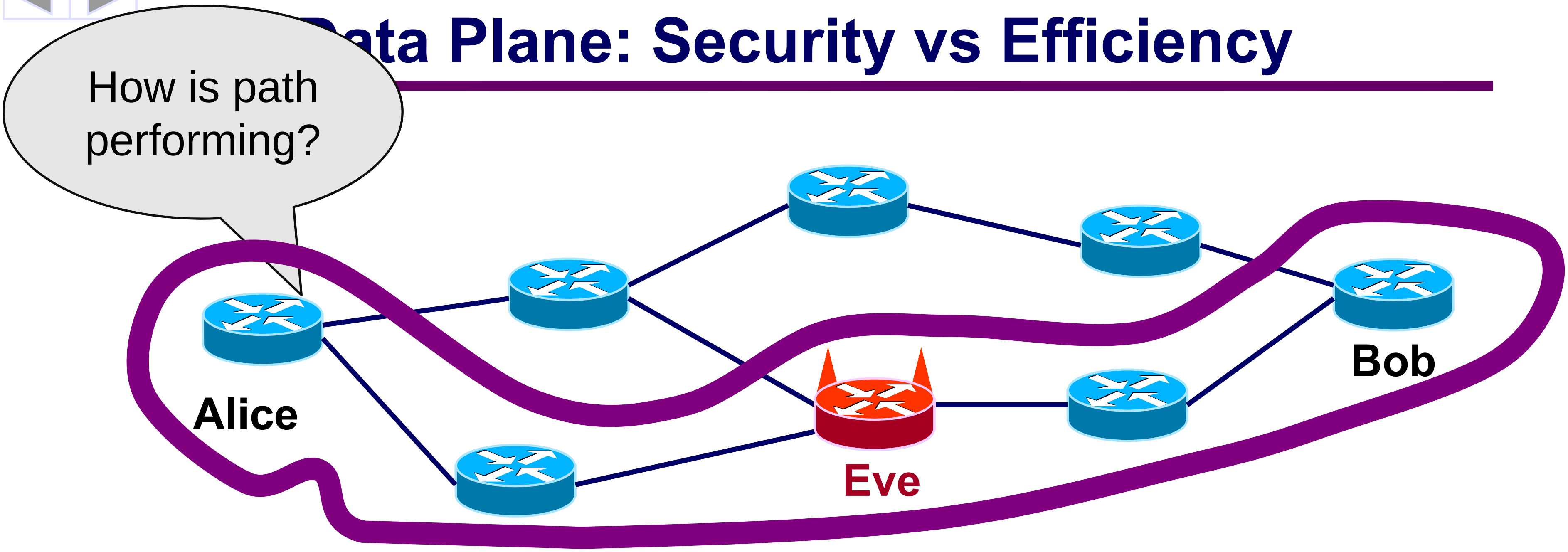
Detection: **Does packet loss / corruption rate exceed 1% ?**

Localization: **If so, which router is responsible?**

Today's approaches cannot withstand active attack

(**ping**, traceroute, active probing, marked diagnostic packets)

Data Plane: Security vs Efficiency



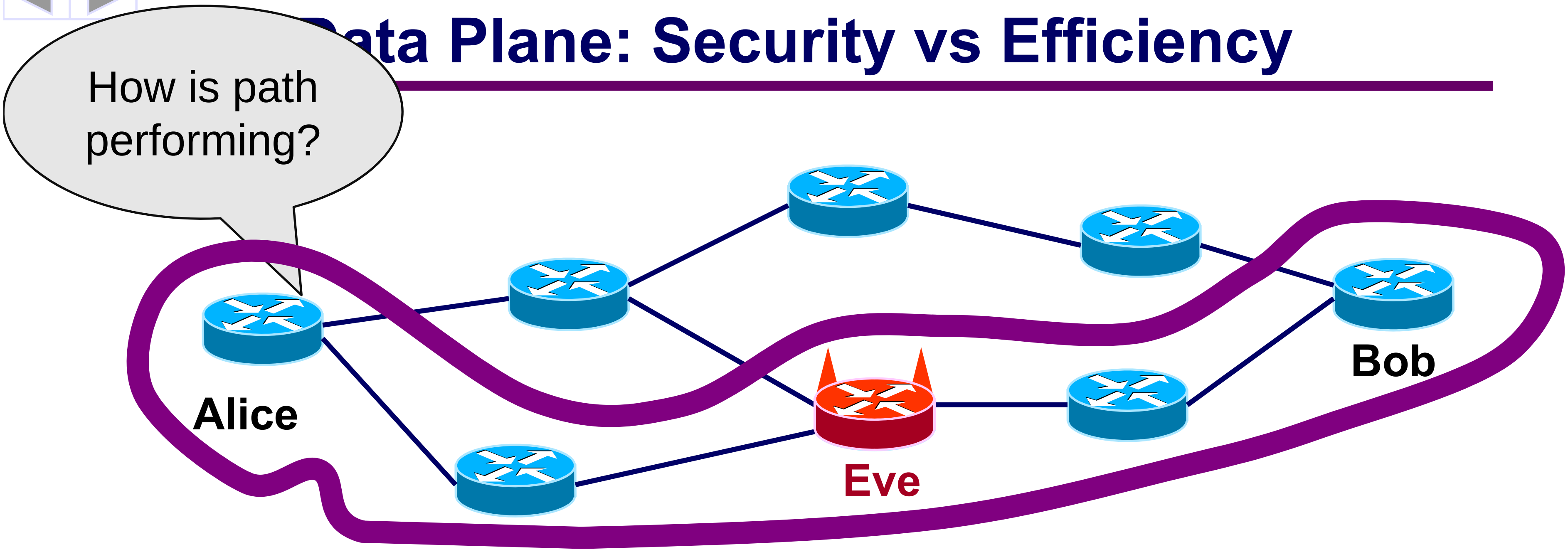
[GXTBR SIGMETRIC'08] Any protocol **detecting** loss on a path (with an adversary) needs keys and crypto at **Alice and Bob**.

Argued by reduction to one-way functions.

[BGX, EUROCRYPT'08] Any protocol **localizing** the adversary on a path, needs keys and crypto at **<u>every node on the path</u>.**

Argued with Impagliazzo-Rudich style black box separation.

Data Plane: Security vs Efficiency

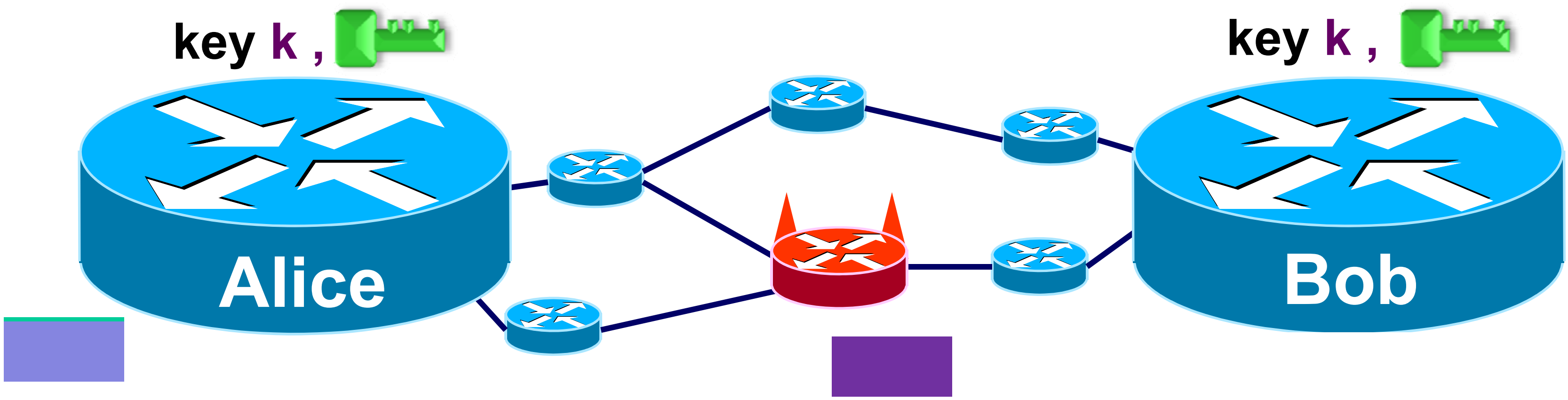


[GXTBR SIGMETRIC'08] Any protocol **detecting** loss on a path (with an adversary) needs keys and crypto at **Alice and Bob**.

[BGX, EUROCRYPT'08] Any protocol **localizing** the adversary on a path, needs keys and crypto at **every node on the path**. ☹

⇨ Limited incentives to deploy these protocols in the Internet.

Efficient & Secure Detection : Protocol



A | 0 | 0 | 1 | -2 | 1 | 0 | 1 | 0 | 3 | 1 |

| 0 | 0 | 1 | -1 | 1 | 0 | -1 | 0 | 4 | 0 | **B**

Hash each packet **f_k(d) = index**
Update sketch **A[index] += 1**

Hash each packet **f_k(d) = index**
Update sketch **B[index] += 1**

Send authenticated (MAC'd) sketch

Take difference sketch **X = A-B**
MAC and send

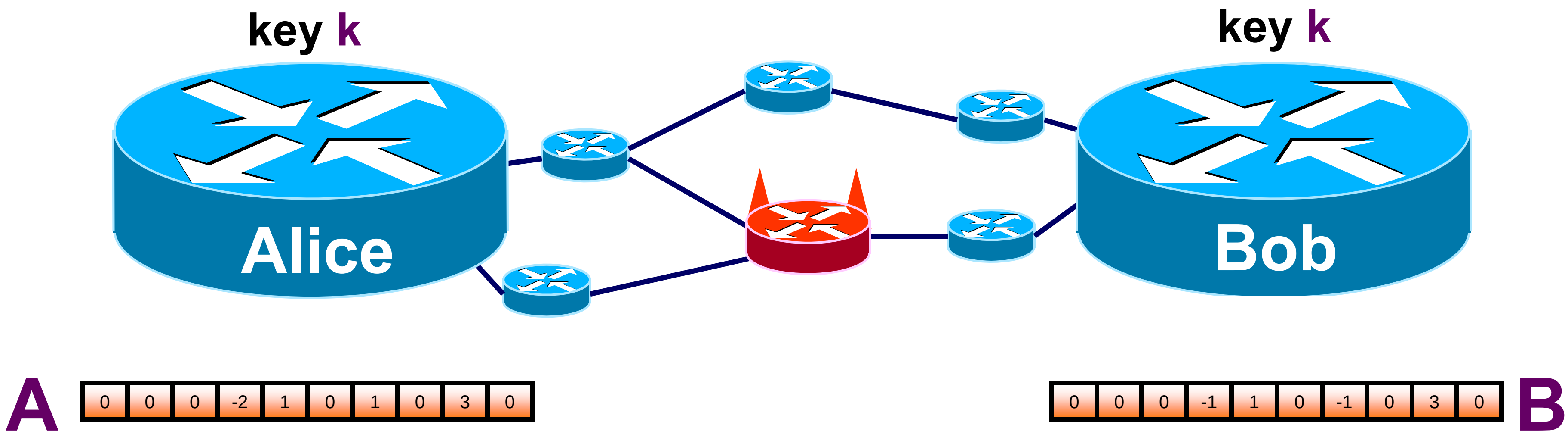
Decide btwn **> 1%** and **< 0.5%** loss:

- Compute the ℓ_2-norm **ΣX_i^2**
- Raise an alarm iff norm **> 0.66%**

Refresh hash key & Repeat

Refresh hash key & Repeat

Efficient & Secure Detection : Summary



Our protocol requires:

- **O(log(# packets))** storage at Alice & Bob
- compute one hash / packet at Alice & Bob
- no traffic modification
- 2 extra packets (communication)
- pairwise keys at Alice & Bob

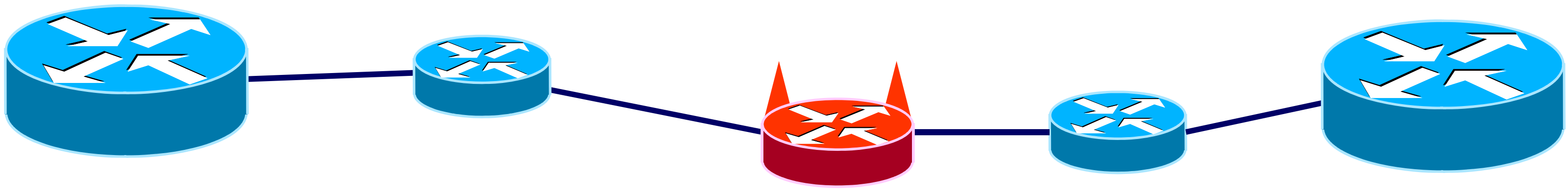
Pkts	Sketch
10^6	170 Bytes
10^7	200 Bytes
10^8	235 Bytes
10^9	270 Bytes

This was prototyped at Cisco in summer 2008.

Conclusions

Securing the control plane is not a panacea.

- Even if we assume ASes are **rational** and use "**Secure BGP**"



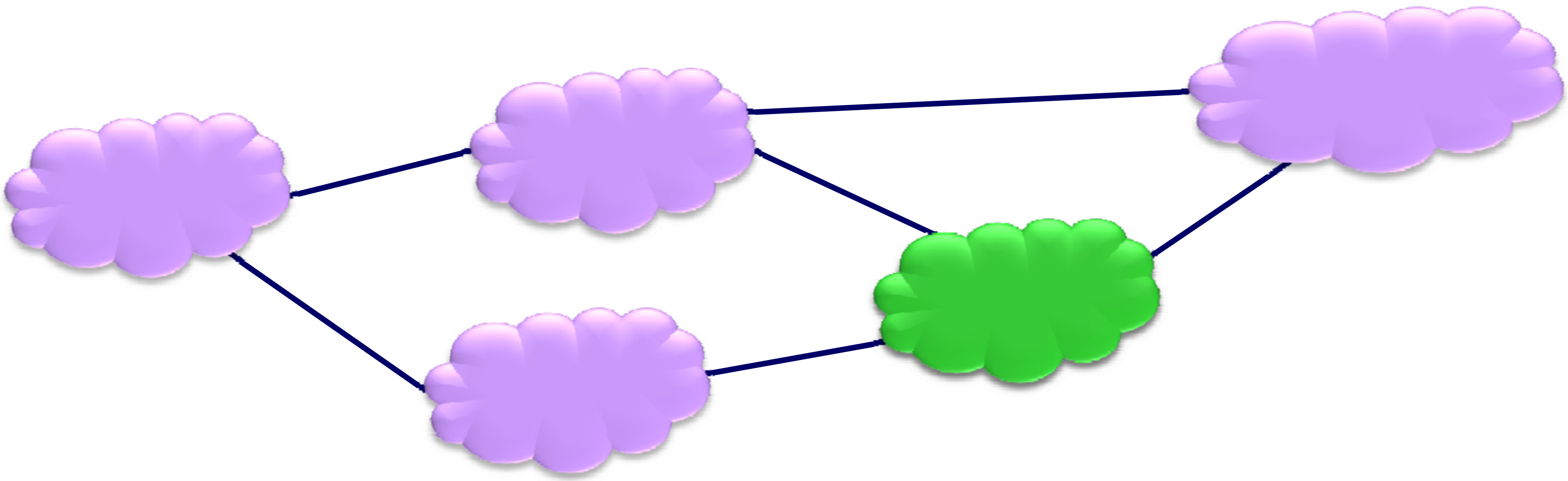
Availability schemes that require knowledge of paths?

- **Control-plane protocols** don't guarantee that
- … we know the paths packets actually take.
- **Data-plane protocols** that **localize an adversary** are
- …expensive; each node on the path has to participate.

Availability schemes that involve only the end points?

- Efficient protocols are possible, **even in the data-plane**
- … but with weaker security guarantees

Thanks!



Full versions of all papers available:

www.princeton.edu/~goldbe/