# An Expectation-Based Approach to Policy-Based Security of the Border Gateway Protocol

Jun Li, Josh Stein, Mingwei Zhang

UNIVERSITY OF OREGON

Olaf Maennel

TALLINN UNIVERSITY OF TECHNOLOGY

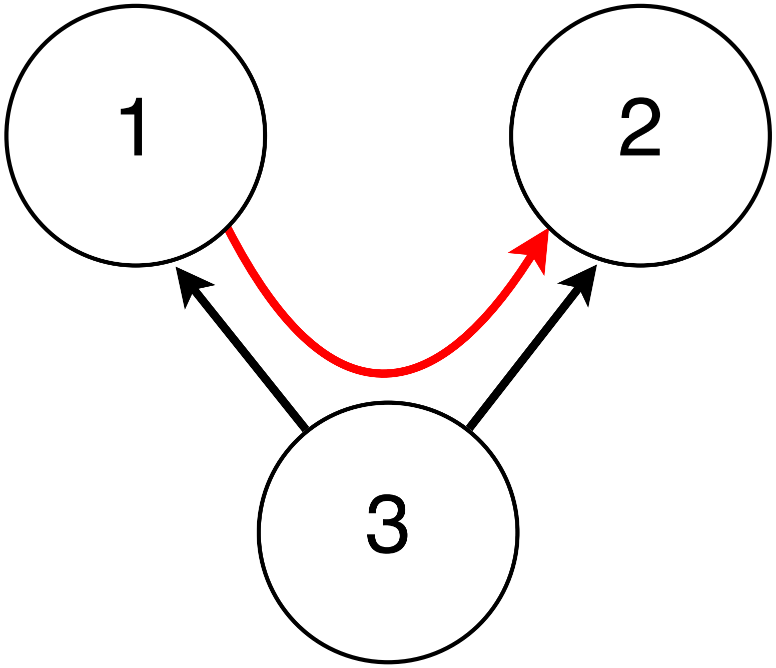
IEEE GI 2016

19th IEEE Global Internet Symposium
In conjunction with IEEE INFOCOM 2016, San Francisco, CA, USA, April 11, 2016

# The Problem

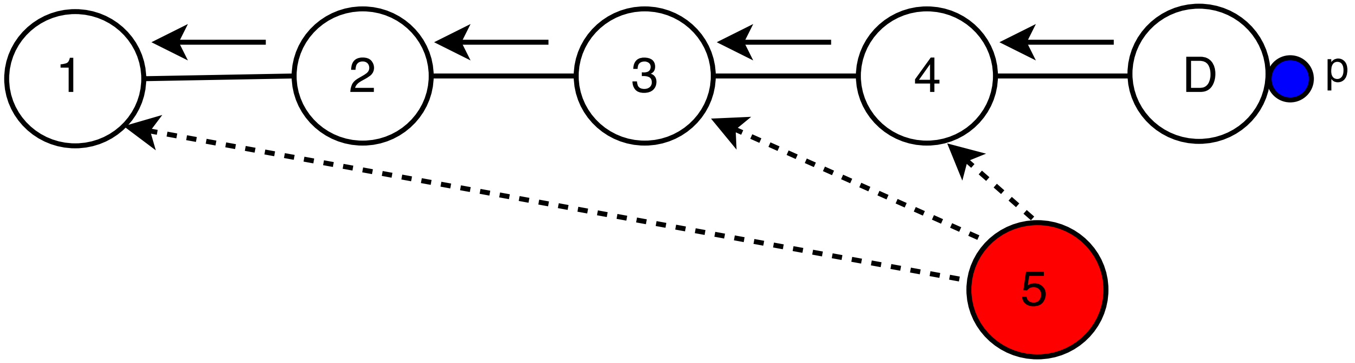
- The Border Gateway Protocol (BGP) is the *de facto* standard inter-domain routing protocol on the Internet
- Most BGP security solutions focus on **topology-based** security
    - origin authentication, path integrity
- They seldom consider policy-based security, esp. whether a path conforms to routing policies of ASes *en route* or not

# A Route Leak Example

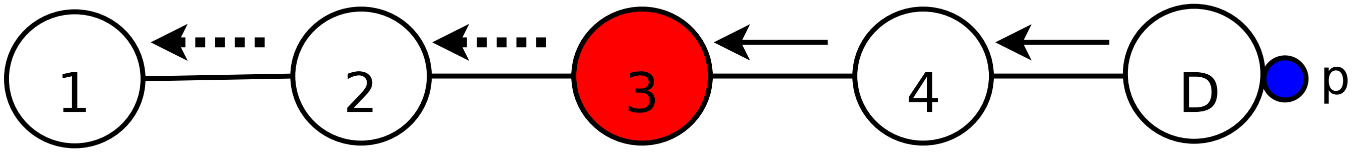


AS3 is a customer AS of AS1 and AS2, and it leaks to AS1 its route to AS2. AS1 thus learns a leaked route (in red) that AS1 should not use.

# Another Example



A topology-based security solution can defend against an attacker (node 5) impersonating the origin of prefix *p* or lying about its path to *p*.



A topology-based security solution *cannot* prevent an attacker (node 3) from leaking a route and obtaining traffic toward a victim prefix.

# Policy-based Security for BGP

- BGP is a policy-based routing protocol
- BGP security in the policy dimension is a significant concern
- Besides conventional routing policies, ASes should define and enforce policies w.r.t. the legitimacy of routes, such as
    - whether or not an AS can be included on a particular route
- Every AS can define its own policy at its discretion

# Our Approach

- A policy-based security solution called Expectation Exchange and Enforcement, or **E3**
- E3 exchanges and enforces routing policies between ASes
  - A newly advertised route must meet policy expectations of ASes
  - In the previous example, node 4 can tell node 2 that it does not expect to receive traffic from node 2 via node 3
- E3 runs alongside topology-based BGP security solutions (e.g., BGPSEC)

# What is an Expectation?

- *Expector*: an AS that produces an expectation
- *Expectee*: an AS that enforces an expectation
- *Subject*: an AS that is specified in an expectation and directly affected by the expectation
- A set of *IF-THEN* rules (conditions and actions)

# Types

- Unilateral Expectations: an expector's own expectation about a subject without consulting the subject
- Contractual Expectations: an expector and its subject constructs a contractual expectation
- Active Expectations: expectations that are actively enforced
  - Always associated with a contractual expectation

# Exchange of Expectations

- *Query mode*: a BGP router queries specific ASes to learn their expectations
- *Notification mode*: a BGP router notifies potential expectees of new expectations

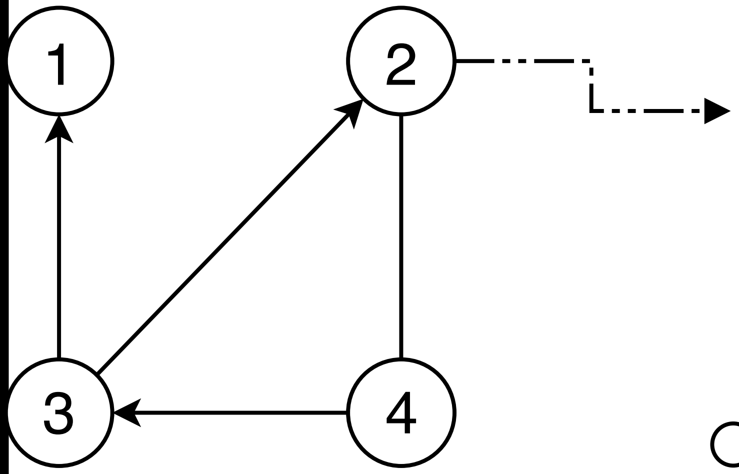
# Enforcement of Expectations

- BGP updates must be checked against expectations to ensure routing policy compliance, with two main tasks:

- Checking a BGP update against active expectations
  - Check every IF-THEN rule
  - If the condition of a rule (IF part) is met, take the action (THEN part)

- Checking an active expectation against its associated contractual expectation
  - All of the conditions in the active expectation must be a subset of the conditions in the contractual expectation
  - The action of the active expectation must be the same as the action of the contractual expectation

# An Example of Expectation Enforcement



AS2’s active expectations:

| Expector | Subject | Rule |
|---|---|---|
| 1 | 3 | RouteContainsLink(1,3) -> Discard |
| 4 | 3 | RouteContainsLink(3,4) -> LocalPref=200 |

○⟶○ The left AS is a customer, the right AS is a provider.

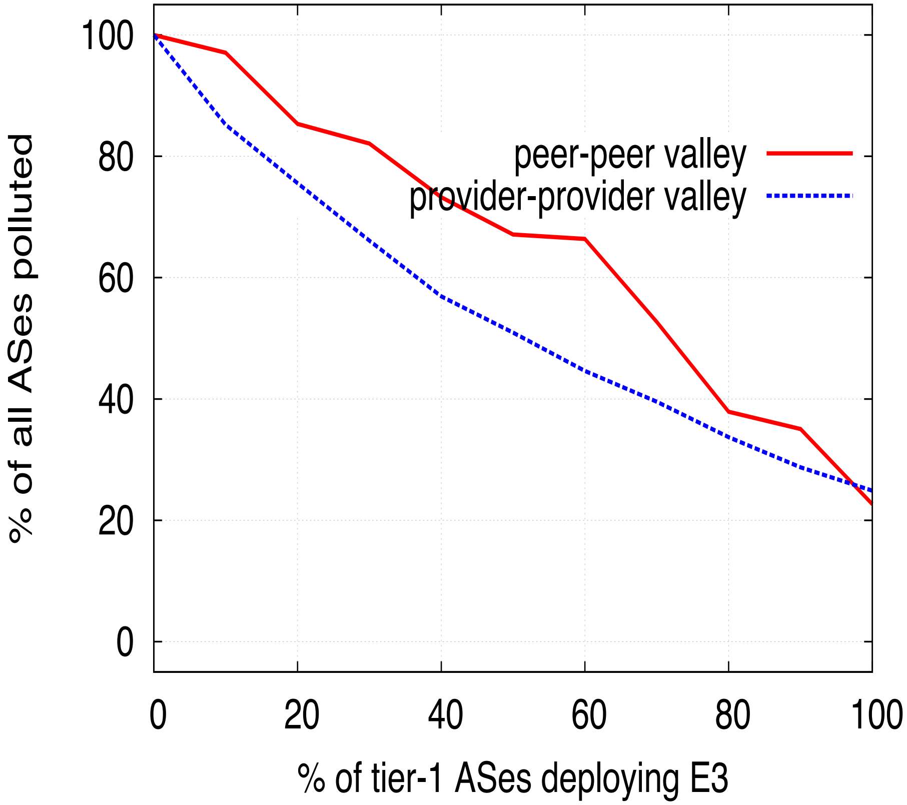
○—○ The two ASes are peers to each other.

# Evaluation Methodology

- We measure when E3 is deployed, how much ASes would still accept routes violating routing policies
- This study chooses one specific policy that requires routes to be valley-free
  - I.e., for any AS along the route, either its previous hop, or its next hop, or both are customers of the AS in question
  - Other policies can also be evaluated
- We classify ASes according to their AS rank
  - We classify the first 100 as tier 1 and the next 900 as tier 2

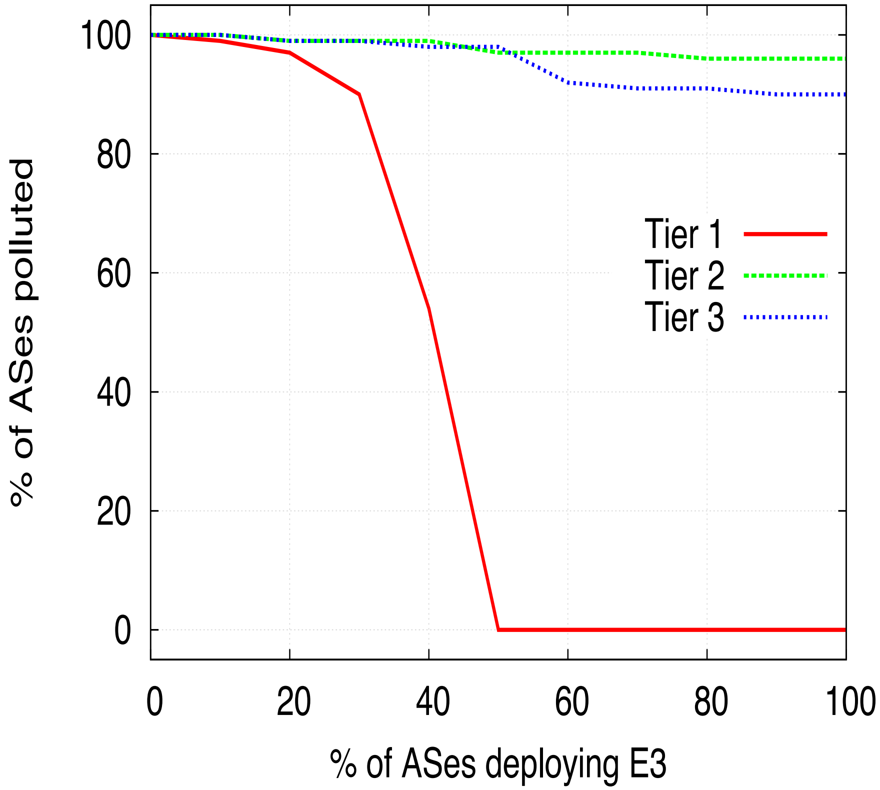
# Simulation: % of ASes Polluted with Invalid Routes

- When 100% tier-1 ASes deploys E3, nearly 80% of ASes originally polluted are then protected from invalid valley routes
- Only deploying E3 at certain tier-1 ASes won't be very effective
- A route-leaking BGP update does not always traverse an E3-enabled tier-1 AS
- More opportunities for provider-provider valley routes to be prevented.



# Case Study: 2012 Canada Route Leak Event

- On August 8, 2012, Canadian ISP Dery Telecom Inc (AS 46618) leaked all its routes acquired from one of its provider VideoTron (AS 5769) to its another provider Bell (AS 577)
- Affected 107,409 prefixes from 14,391 different ASes across the Internet
- Deploying E3 on tier-1 ASes has the best effectiveness



# Deployment Considerations

- Probably not easy to have a high percentage of tier-1 ASes to deploy E3
- Our analysis shows that the route leaks usually have bottleneck ASes that determine the propagation scope (which are not always tier-1 ASes)
- Deploying E3 on these bottleneck ASes can be most effective
  - Identifying them would be key to the success of E3

# Implementation Considerations

- E3 can be implemented on every BGP router (thus in-band expectations via BGP updates), or
- A dedicated server at every AS (thus out-of-band channels for ASes to communicate expectations)
- Expectation, in its current form, is an abstract concept, and could be formatted using Routing Policy Specification Language (or something similar)

# Conclusions

- Topologically valid BGP routes may be still illegitimate and violate routing policies
- We address policy-based BGP security, which has been largely overlooked
- We introduce E3 as a BGP extension for expressing and enforcing policies across ASes, thus to prevent policy-violating routes from propagating further

# Questions?

- Contact:

**Jun Li**
University of Oregon
lijun@uoregon.edu
541.346.4424

UNIVERSITY
OF OREGON