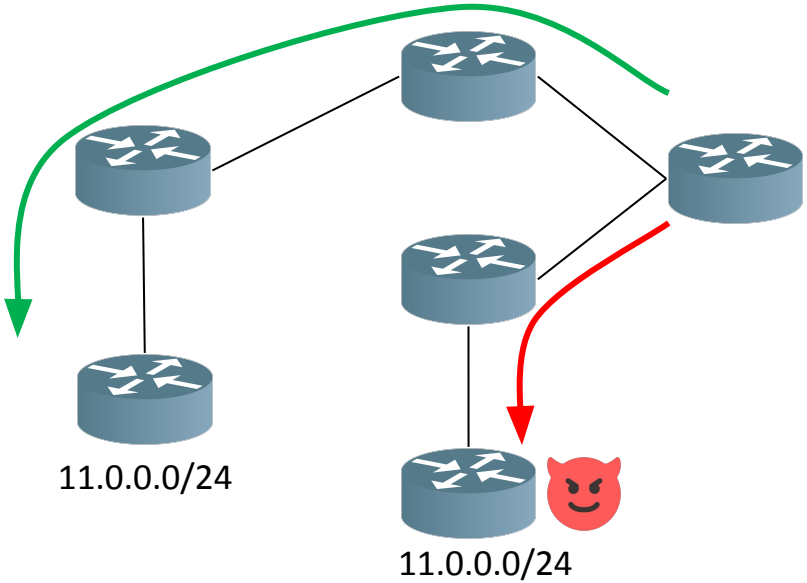
# DnD-DB: A Democratized Network Data Database for Tailored Routing and Security Campaigns

Karl Olson, **Bashayer Alharbi**, Gregory Cusack, Eric Keller

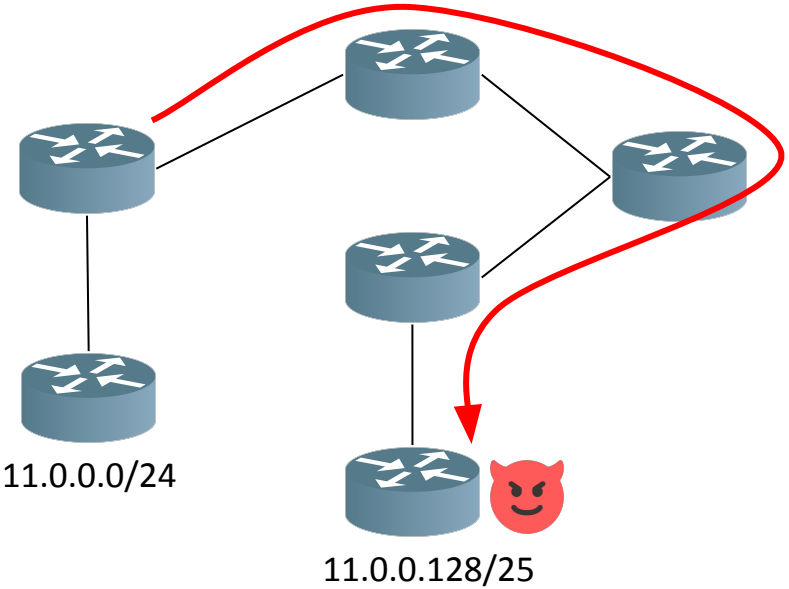
University of Colorado **Boulder**

# BGP Vulnerabilities: Hijacking

- Prefix Hijacking

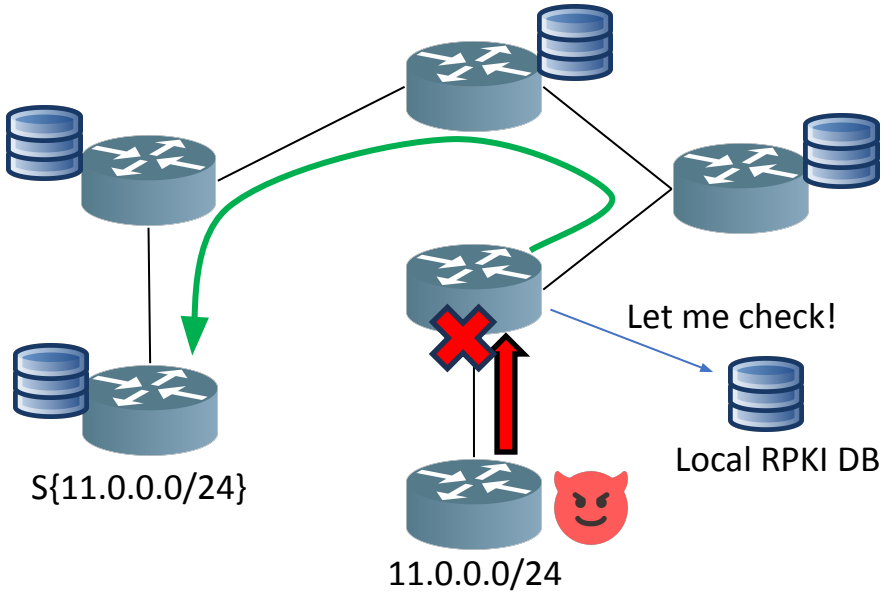



- Sub-Prefix Hijacking



# Current Security Solutions: RPKI

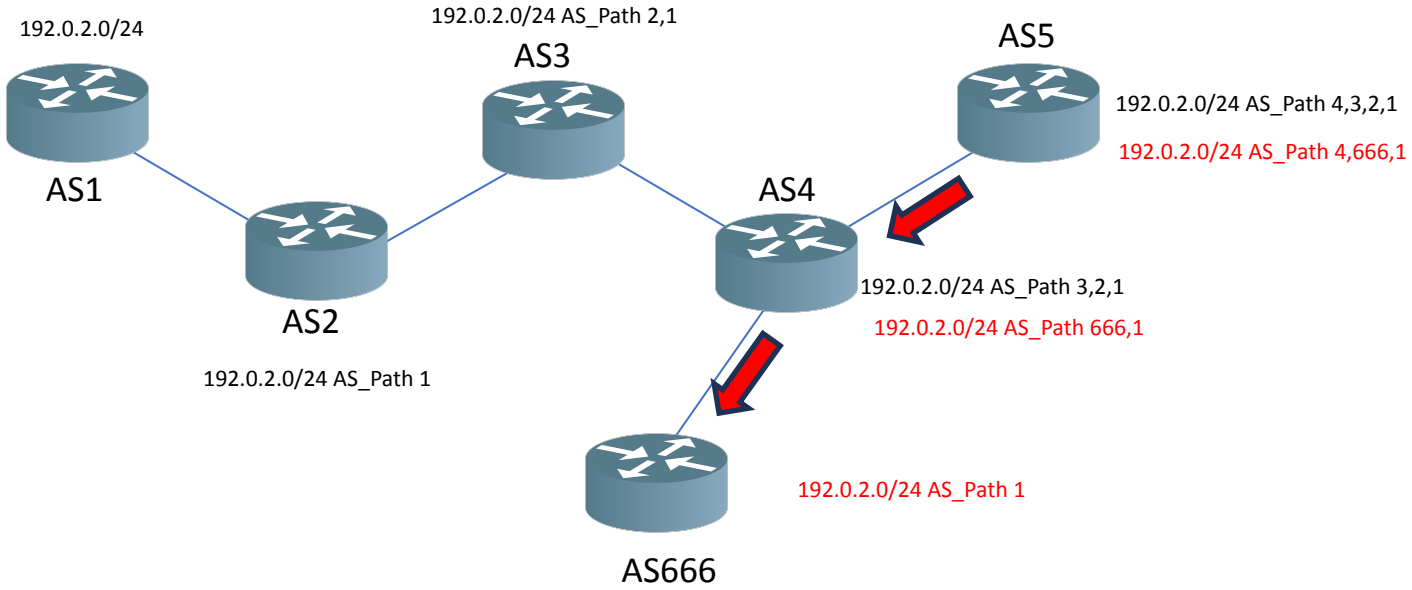
- **Solution:** Route Origin Validation - RPKI.




**RPKI** – Decade of deployment ~40% adoption

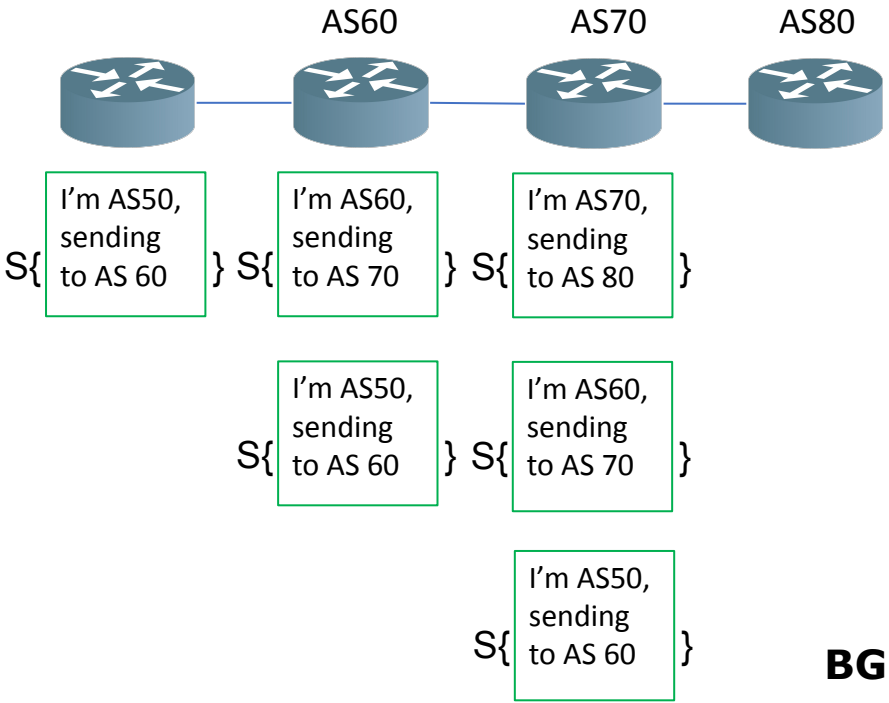
# BGP Vulnerabilities: AS_Path Prepending

- AS-Path Prepend



# Current Security Solutions: BGPsec

- **Solution**: Path Validation (BGPsec)




- All-or-nothing approach
- Too much processing

**BGPsec** – Decade of deployment ~0% adoption

# Core Problem: Misaligned Incentives

**Why providers don't adopt current solutions:**

1. Impossible universal adoption
2. Limited value in partial deployment
3. Complexity and cost
4. BGP works "well enough"
5. No advantage for early adopters

How can we better **incentivize** the adoption of security solutions or outcomes?

Focus on **providing value to administrators** to encourage adoption of new systems that enable security

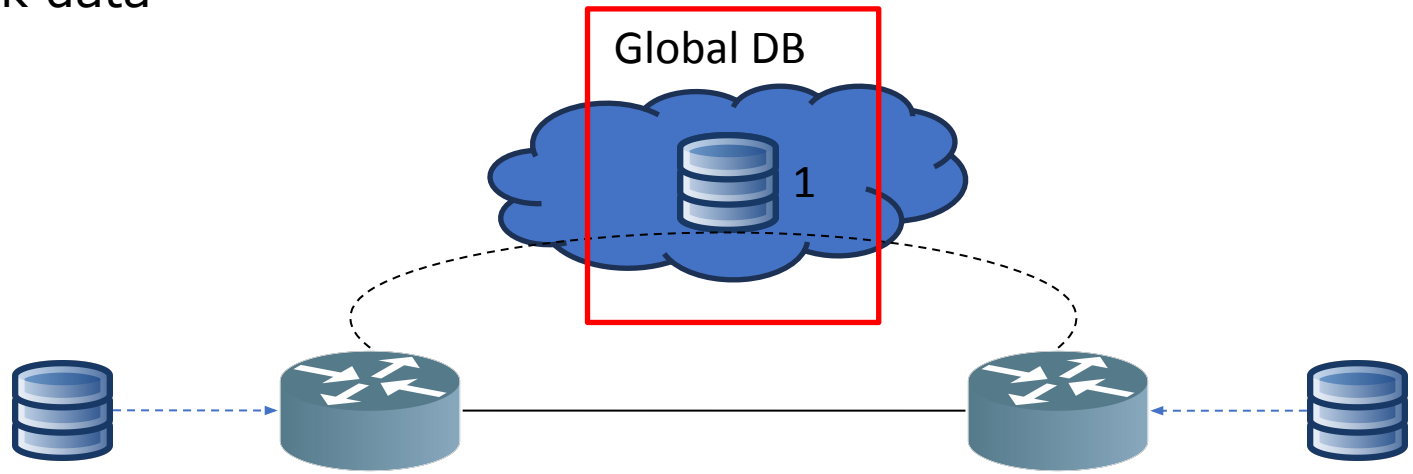
# Our Approach: DnD-DB

## Democratized Network Data Database

1. **Providing immediate business value** to administrators
    - Help with network management and troubleshooting
    - Enable cost optimization for transit
    - Support SLA management
2. Building a platform that security can be built on top of easily
3. **Enabling incremental adoption**

# DnD-DB Architecture

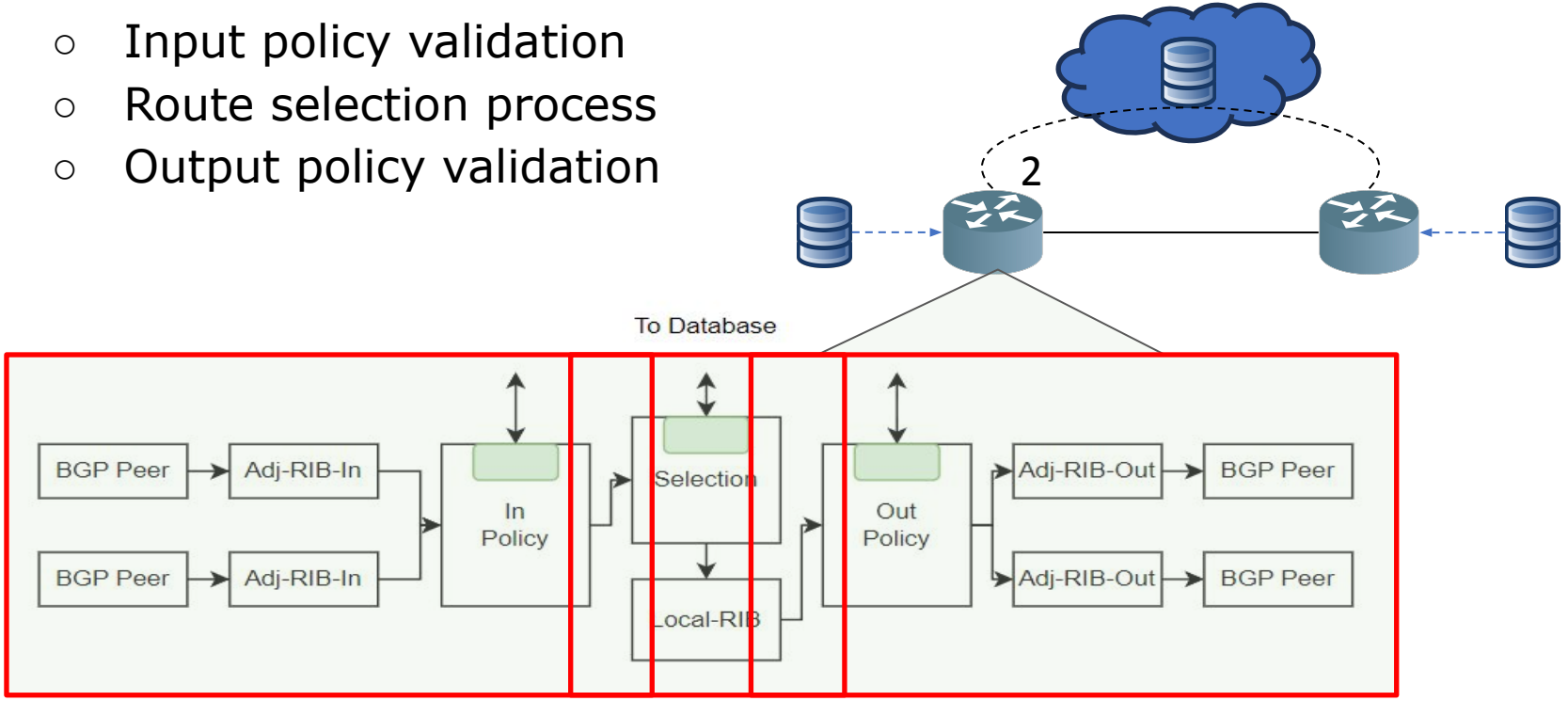
**[ 1 ] Global Routing Database:** Central storage for routing and network data



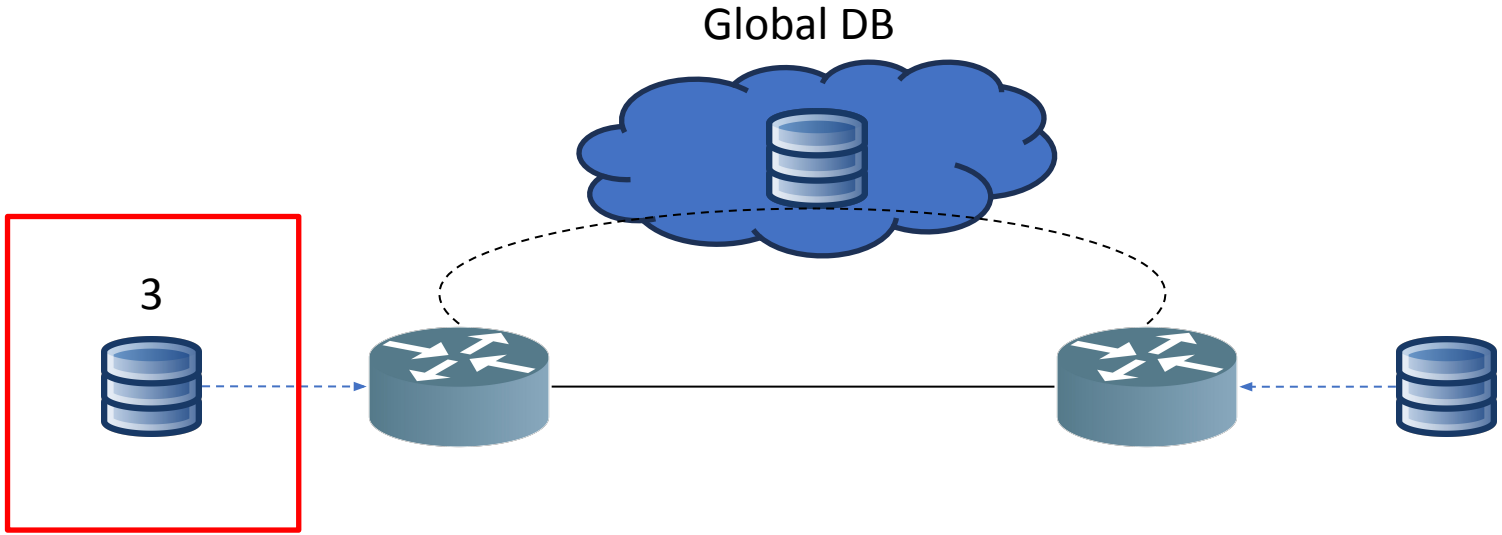
# DnD-DB Architecture

**[ 2 ] Router Integration:** In-network processing for real-time decisions

- Input policy validation
- Route selection process
- Output policy validation



**[ 3 ] Management Tools:** Local off-line processing for configuration, visualization, reporting



# Addressing Real Administrator Problems

- **Dual Advertisement:** Prefix advertised from multiple locations

  **Solution**→ Validate prior to advertisement for conflicts (Local, proactive control)

- **Outdated Contact Info:** Unable to reach network owners

  **Solution**→ Pre-validation of route announcements

- **Accidental Overlaps:** Advertised a /23 but some sub/24 prefixes were utilized/advertised elsewhere unexpectedly

  **Solution**→ Real-time alerts for routing conflicts

# Addressing Real Administrator Problems

- **Routing Asymmetry:** Different inbound/outbound paths

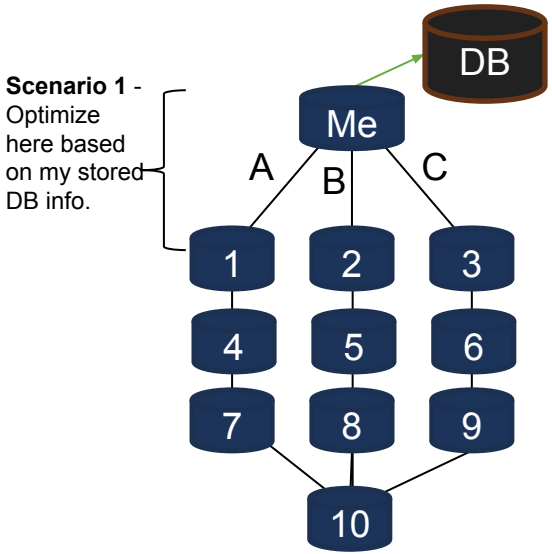
  **Solution** → Allow for AS-Path compared to target ASN (Them vs. Us route view)

- **Route Leaks:** Unintended propagation of routes

  **Solution**→ Historical trend data for troubleshooting

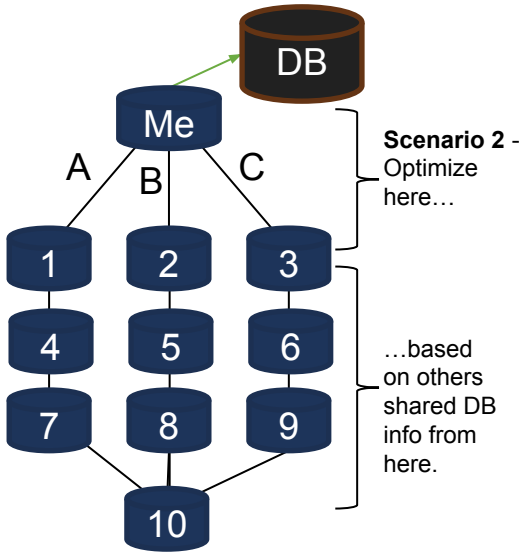
# Use Case: Service Level Agreements

## 1) **Sole Participant**



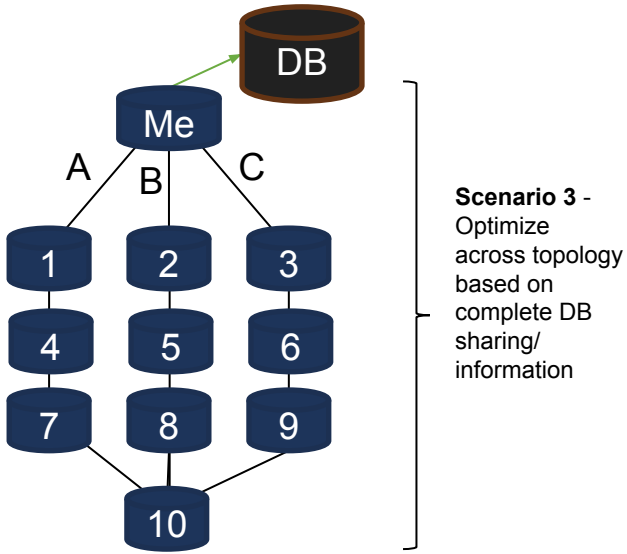
# Use Case: Service Level Agreements

## 2) **Partial Participation**



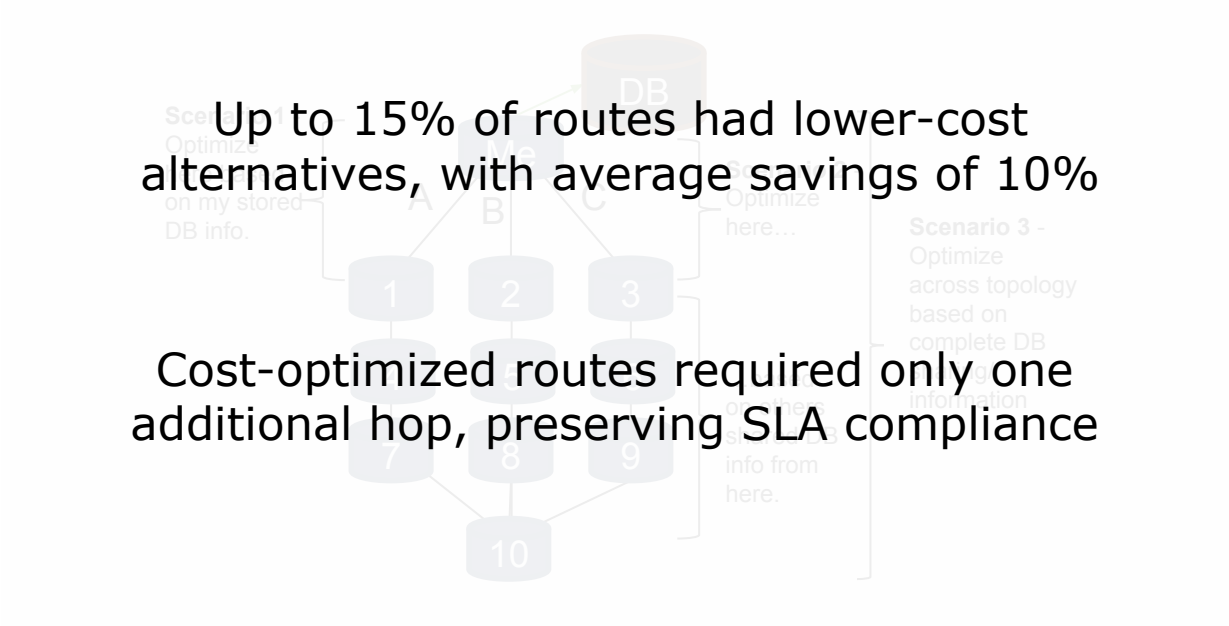
# Use Case: Service Level Agreements

## 3) **Full Participation**




**Scenario 3** - Optimize across topology based on complete DB sharing/ information

# Use Case: Service Level Agreements

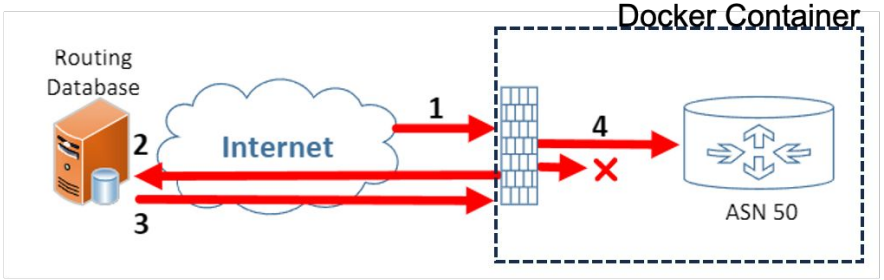


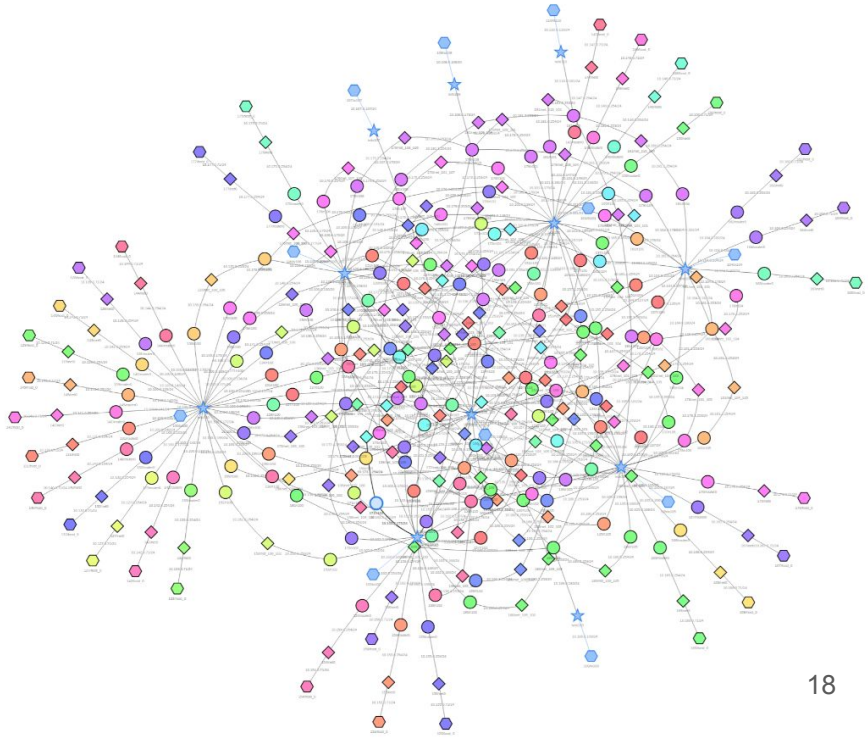

Up to 15% of routes had lower-cost alternatives, with average savings of 10%

Cost-optimized routes required only one additional hop, preserving SLA compliance

# Experimental Setup

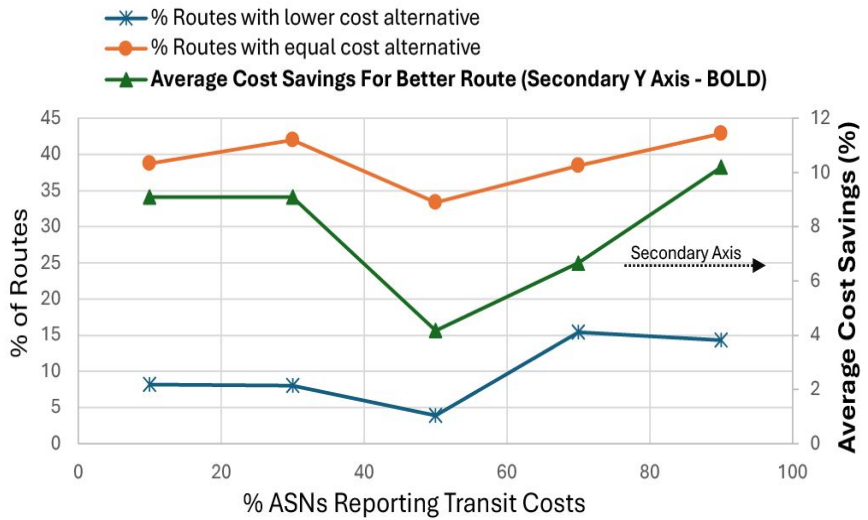
- Simulated 53 ASNs, 195 containers using SEED Internet Emulator
- CAIDA AS-Neighbor for realistic topology
- MongoDB for global DB
- Proxy packet processor



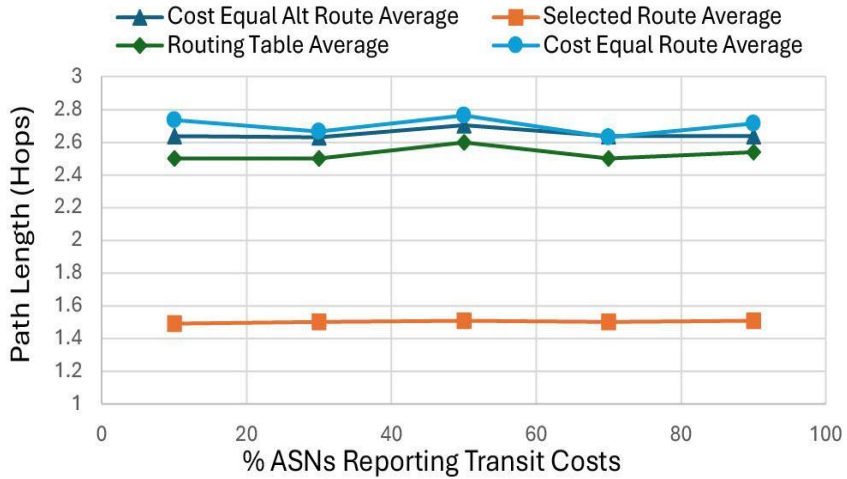



# Results: Business Value

## SLA-based Cost Optimization




Up to 15% of routes had lower-cost alternatives, with average savings of 10%



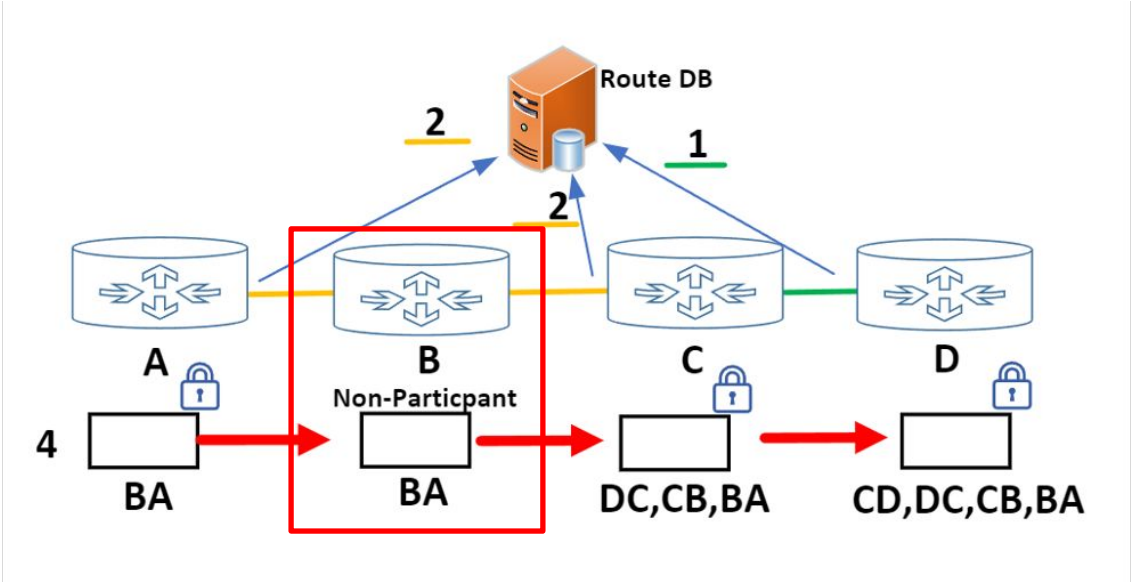

Cost-optimized routes required only one additional hop, preserving SLA compliance

# Experiment Results Measurement

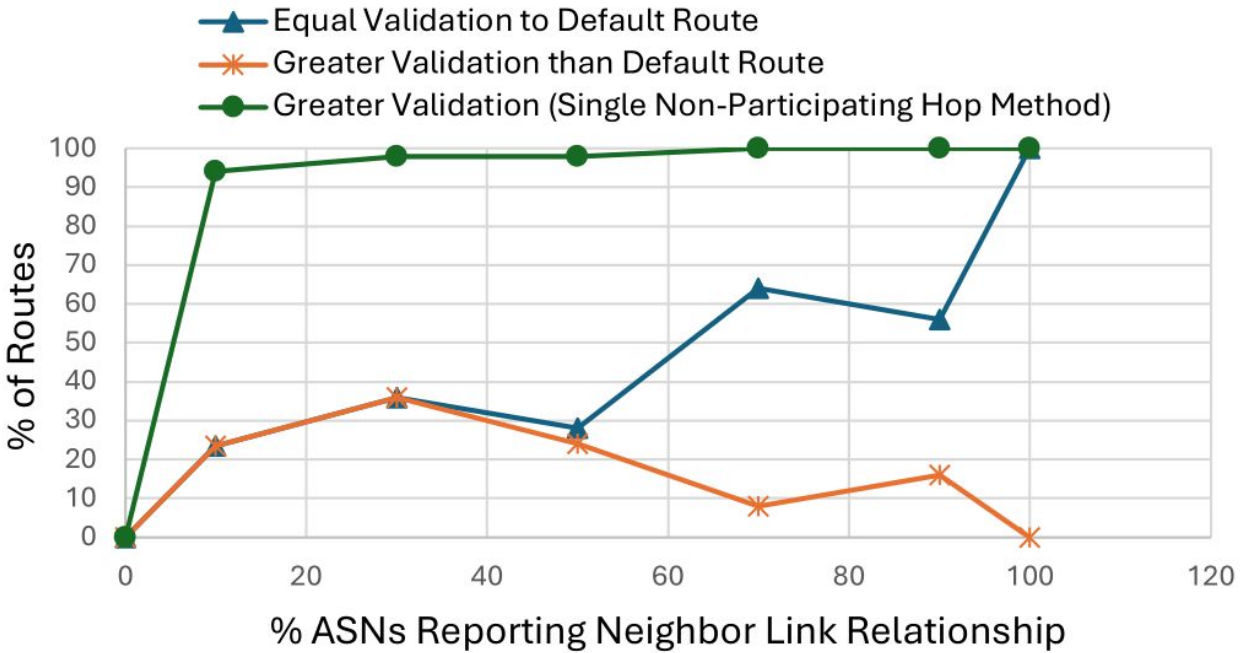
- Business & Security Value
- RPKI Equivalency
- Performance Analysis

# Results: Security Value

Path Validation with Partial Deployment

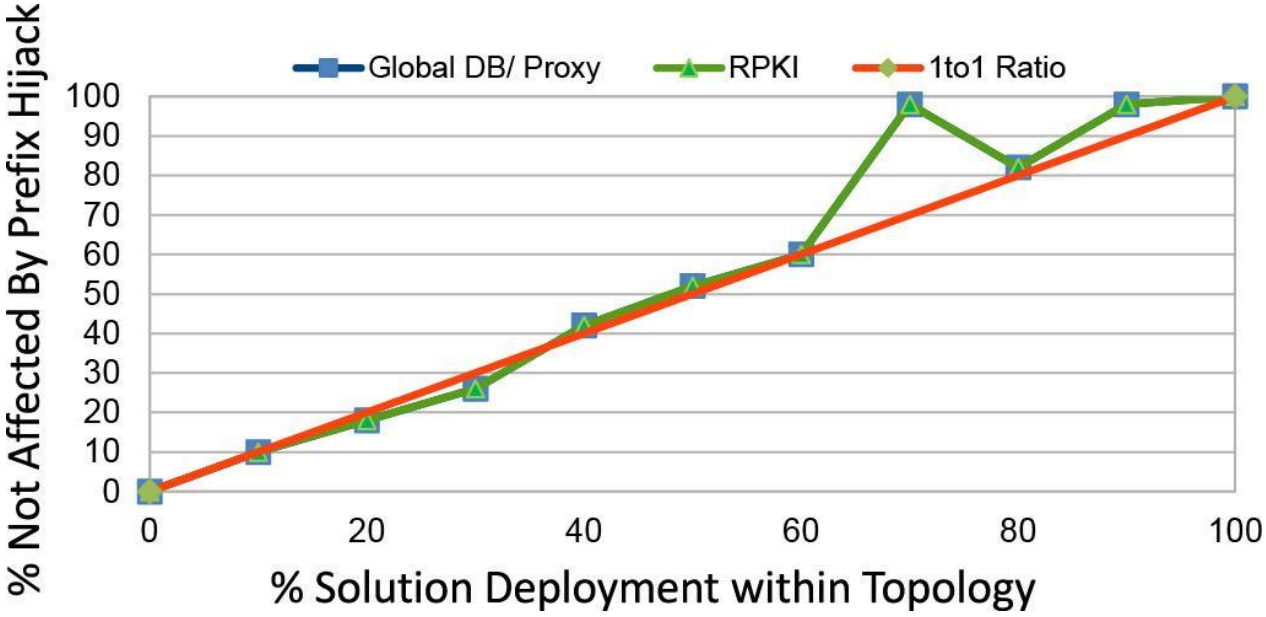


# Results: Security Value




Nearly 100% route validation can be achieved with the **Single Non-Participating** Hop Method even at low network participation rates

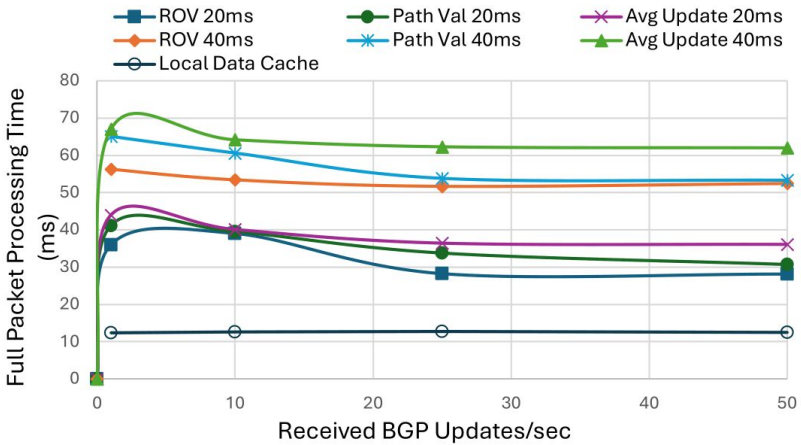
# Results: RPKI Equivalency



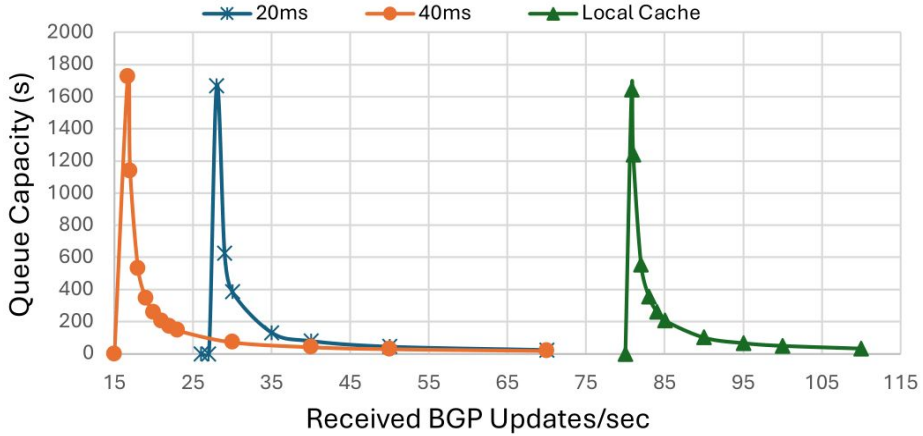

Equivalent security to **RPKI** while offering greater flexibility to leverage data for other business needs

# Results: Performance Analysis

Measured processing times across varying rates of updates being received




Used steady state throughput to calculate queue capacity and peak processing rates



# Conclusion

- Security solutions need business incentives for adoption
- DnD-DB delivers immediate value with equivalent security
- Works even with partial deployment
- Aligns security with business needs
- Security must be built-in