bdrmap-IT: Mapping AS Borders in the Internet

Alex Marder, Matthew Luckie, Amogh Dhamdhere,
Bradley Huffaker, kc claffy, and Jonathan M. Smith

Problem

- How do we infer router operators and interdomain links from a traceroute dataset?

- Why?
  - Public policy – interdomain link congestion
  - DDoS – analyze potential attacks against interdomain links

Previous Work

- bdrmap [Luckie et al. IMC ‘16]
  - Highly accurate
  - Limited to the border of the traceroute vantage point network

- MAP-IT [Marder & Smith IMC ‘16]
  - Identifies inter-AS links at Internet-scale
  - Precise, but lower recall

Goals: For All Routers and Links in Traceroute Dataset

- Synthesize bdrmap and MAP-IT
- Infer AS operators of routers
- Identify interdomain links
- Work with existing traceroute data
  - For all ASes seen in the dataset

Algorithm: 3 Main Components

1. Create hybrid router-interface graph from traceroutes

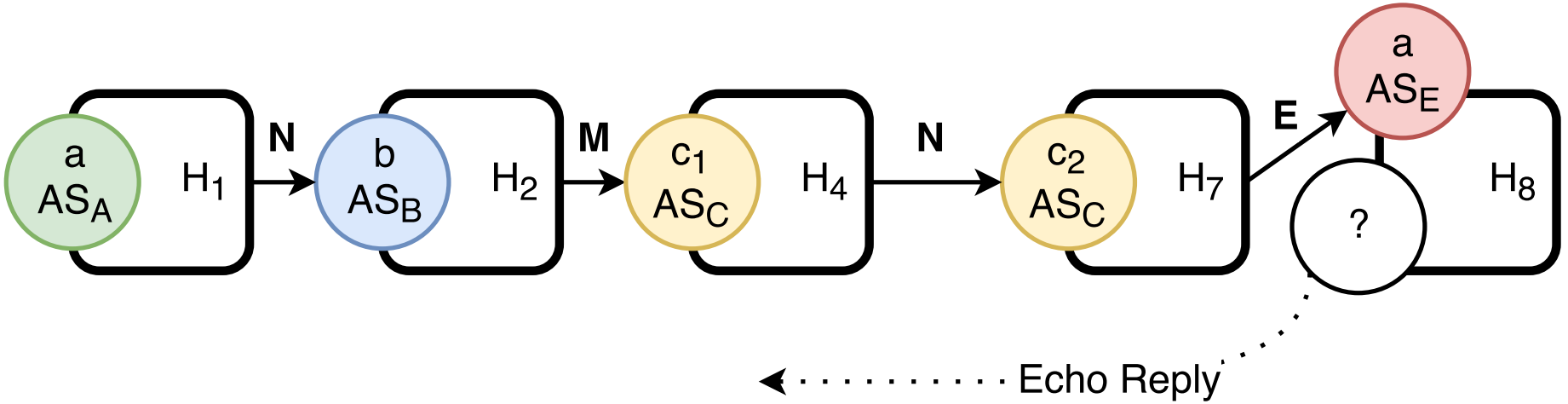
2. Identify last-hop router operators

3. Graph refinement loop:
   A. Determine router operators
   B. Infer inter-AS links

Graph Construction: Priority Edges

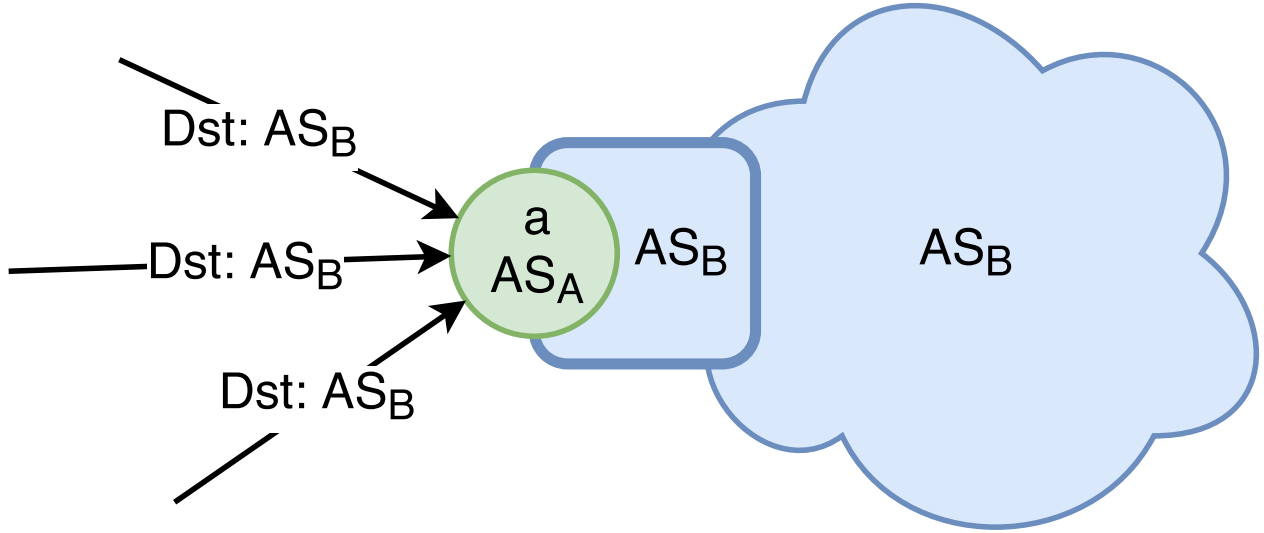
- 3 edge labels (in priority order):
  - N → - adjacent TTL Expired hops or same AS
  - E → - echo replies
  - M → - separated by unresponsive hops
- Edges from router to interface
- Only highest priority edges used for each router

Hops:	1	2		4			7	8
IP:	a	b	*	c1	*	*	c2	d
AS:	AS_A	AS_B		AS_C			AS_C	AS_D



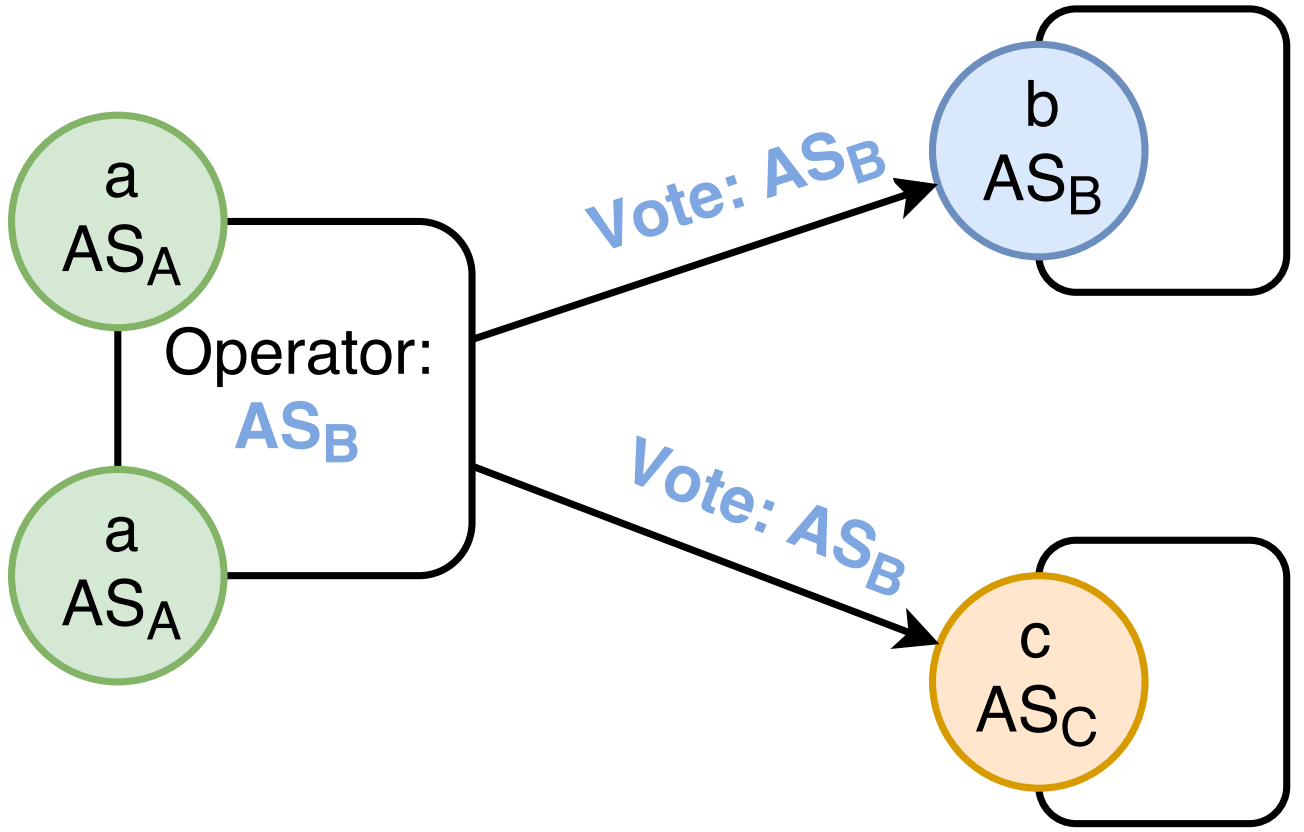
Identify AS Operators of Last Hop Routers

- Only routers which only appear last in their traceroutes
- Use traceroute destinations to determine AS operator
- 95% accurate



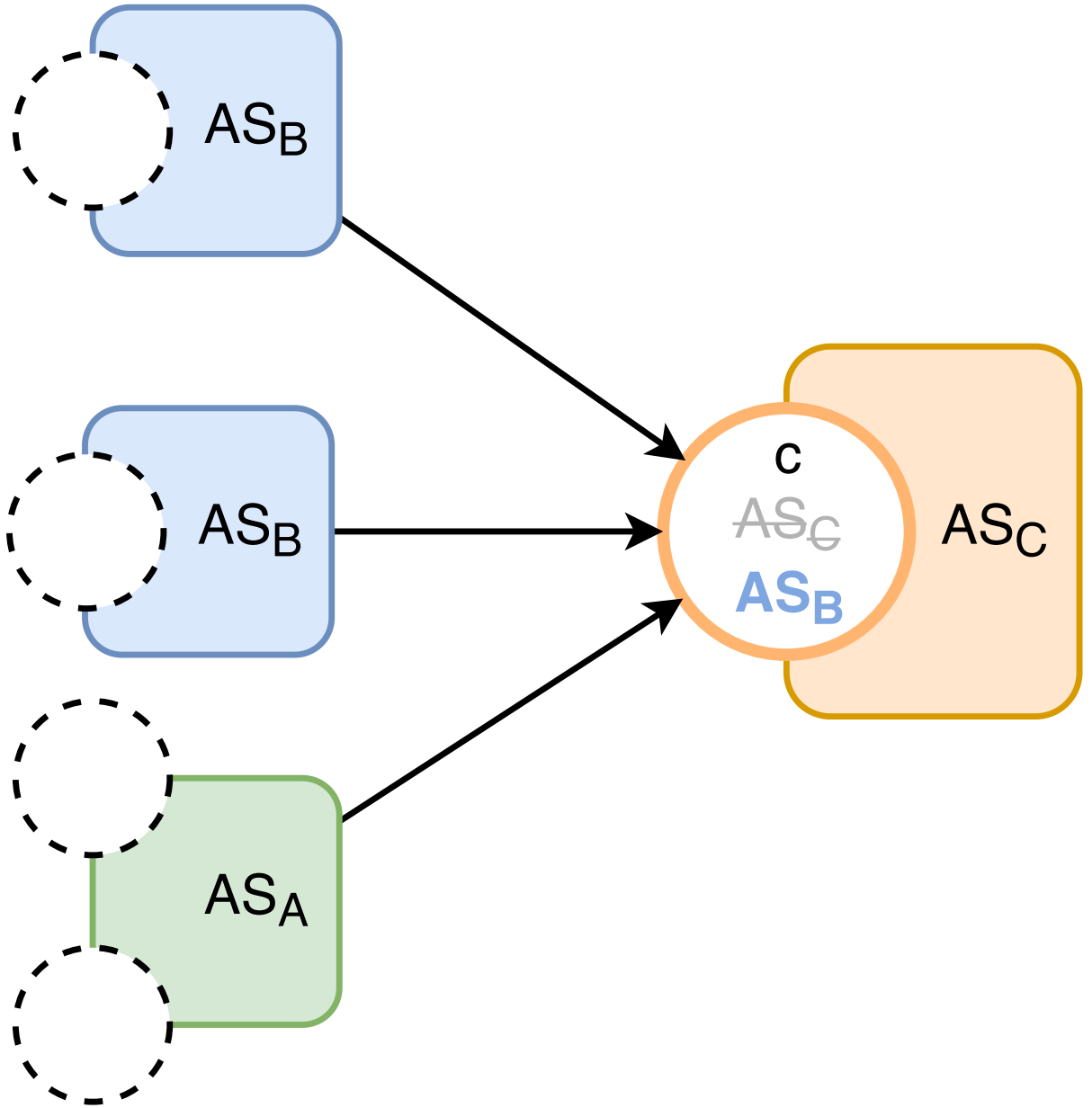
Graph Refinement Loop: Router Operators

- Lots of heuristics: IXP addresses, unannounced addresses, third parties, hidden ASes, etc.
- All highest priority edges get a vote
- Highest vote AS operates router



Graph Refinement Loop: Inter-AS Links

- Interface origin AS different from router operator
- Select most frequent AS from connected router operators



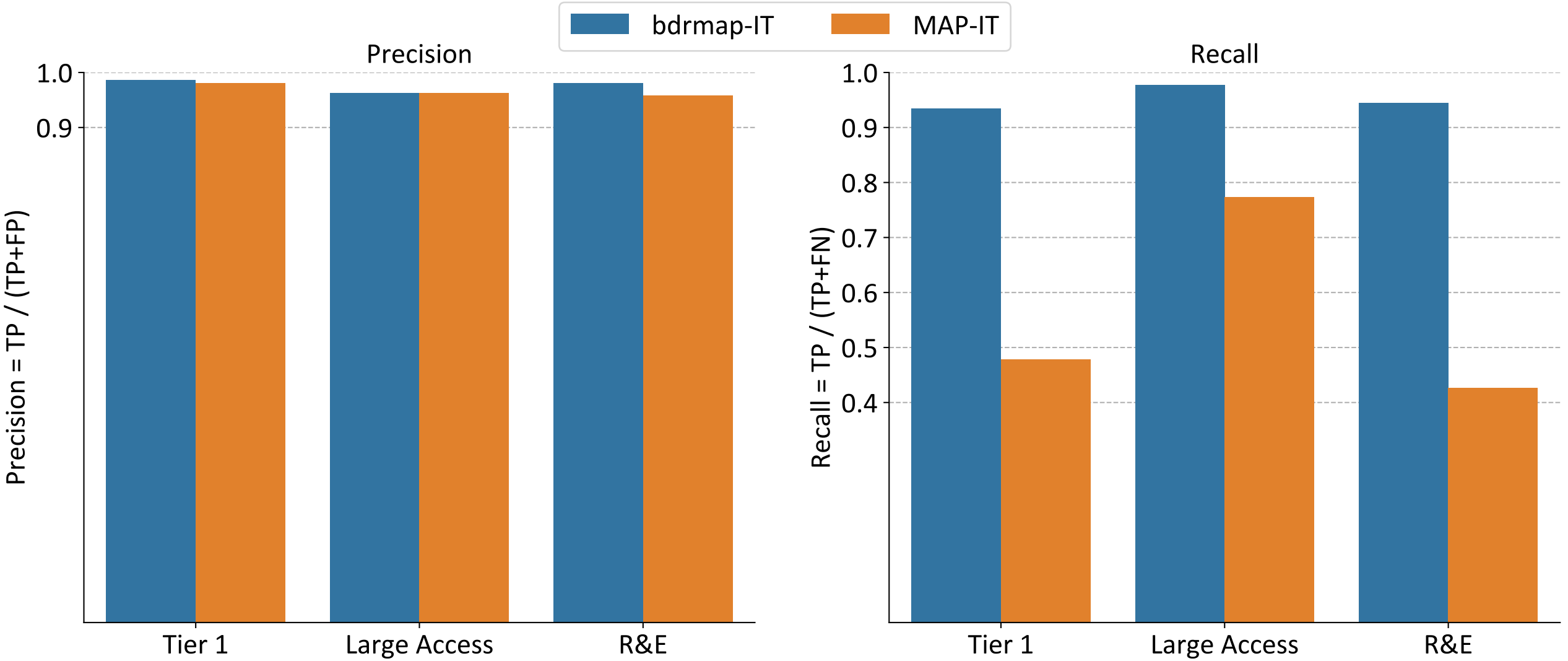
Results: Precision and Recall

- Ground truth with 3 networks – tier 1, large access, and R&E

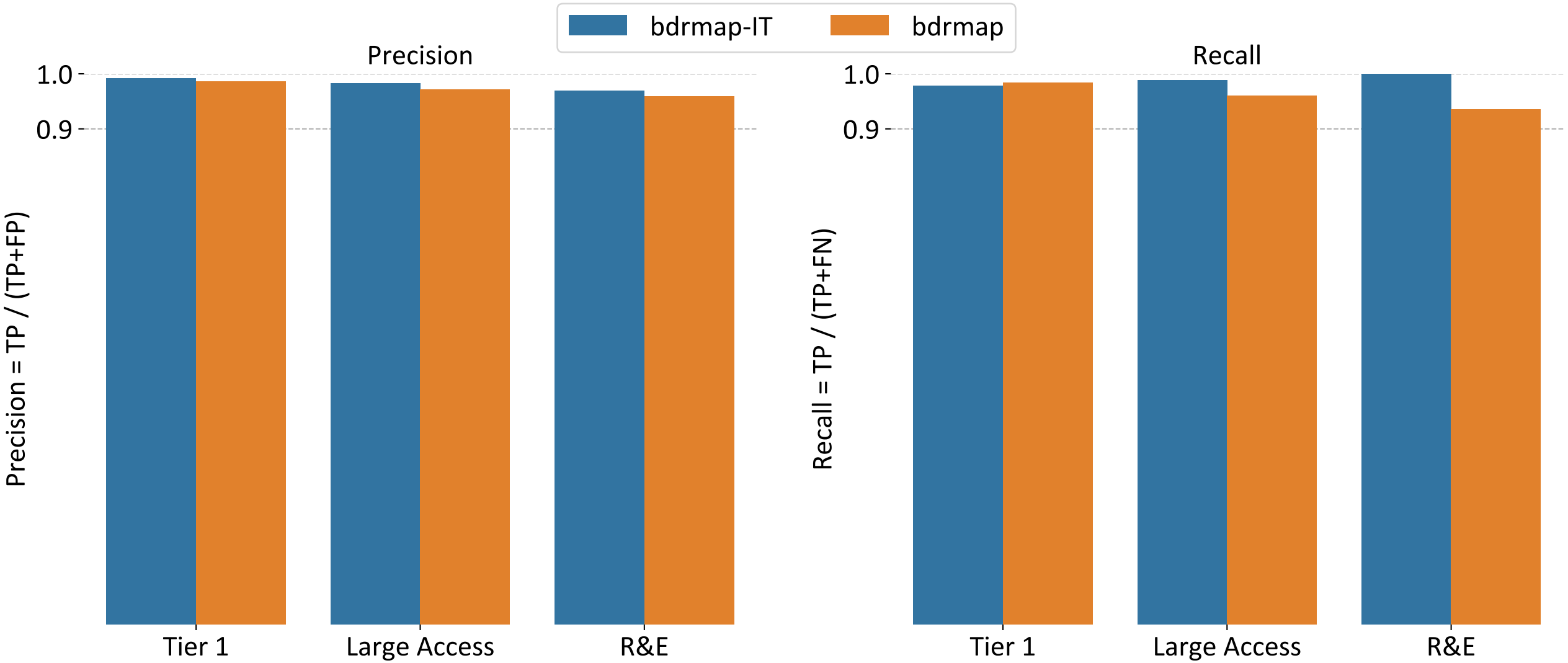
- **Precision:** fraction of inter-AS link inferences which were correct

- **Recall:** fraction of inter-AS links in the dataset correctly identified

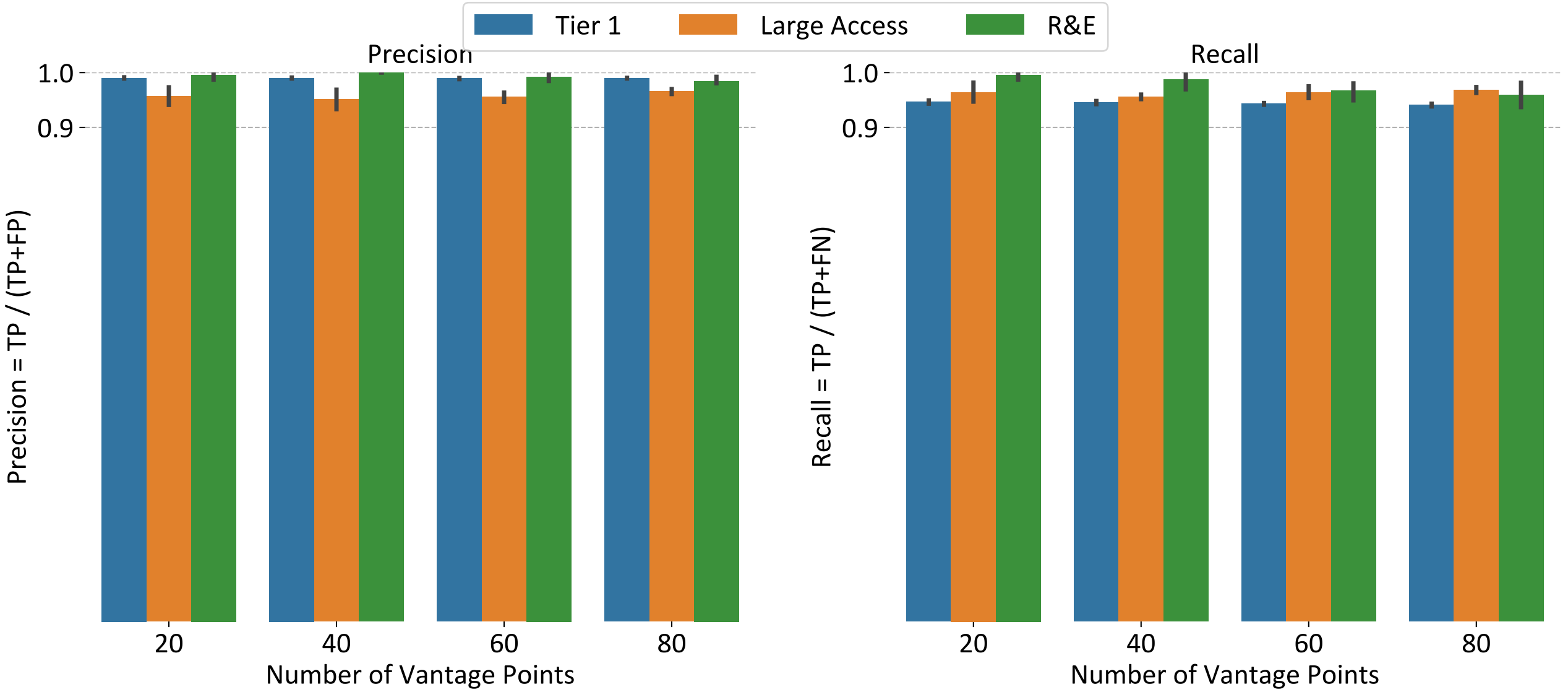
Results: bdrmap-IT Identifies Far More Inter-AS Links Than MAP-IT



Results: bdrmap-IT Performs Slightly Better Than bdrmap Restricted to the Vantage Point AS Border



Reducing the Number of Traceroute Vantage Points Doesn't Decrease Accuracy



Conclusions

- Maps the borders of ASes
- High accuracy for correctly identifying inter-AS links
  - At least as accurate as its component techniques
- Using on ITDK and RIPE Atlas traceroutes

- What we want:
  - People to use it, soon
  - Ground truth from networks