High-Frequency Active Internet Topology Mapping

Homeland Security
Science and Technology

Cyber Security Division
2012 Principal Investigators' Meeting

October 10, 2012

Robert Beverly
Assistant Professor
Naval Postgraduate School
rbeverly@nps.edu
(831) 656-2132

Intro

- Project: *High-Frequency Active Internet Topology Mapping*
- TTA #7: *Network Mapping and Measurement*
  - “near-real time view of network maps that scale from enterprise to the global Internet”
  - “matching IP address interfaces to physical routers”
- Team:
  - Dr. Robert Beverly (PI, Naval Postgraduate School)
  - Dr. Geoffrey Xie (Co-PI, NPS)
  - Dr. Justin Rohrer (Postdoc, NPS)
  - Dr. Arthur Berger (Collaborator, Akamai/MIT)
  - 4-6 students (Master’s theses)

Objective

- Goal:
  - Obtain accurate network graphs, at router and AS granularities, even at very large scale (e.g. Internet) and amid sparsity (e.g. IPv6).
  - Obtain network topologies an order of magnitude faster than existing systems in order to capture transient dynamics, including malicious or misconfiguration events.
- Motivation:
  - Protect and improve critical infrastructure
  - Understand structural properties of the Internet topology, including robustness, vulnerability to attack, potential for correlated failures, IPv4/IPv6 interdependence, etc.

Background

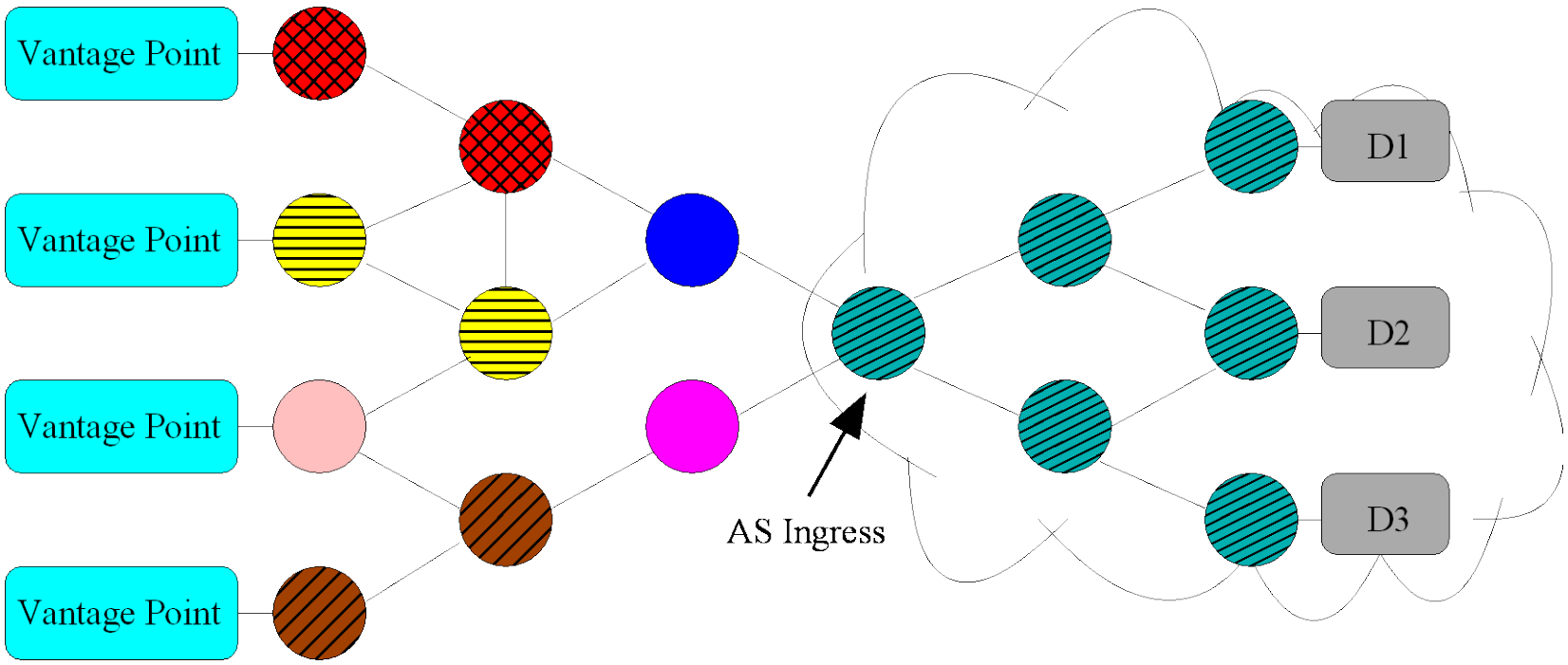
- Why it's hard:
  - Internet topology is dynamic and not designed to be measured; fragile inference techniques
  - Internet naturally hides information, both for scale (e.g. BGP) and economics (e.g. commercial ISPs)
  - Lack of ground truth
- State-of-the-Art:
  - Significant prior work, but not a solved problem
  - Production topology mapping systems (e.g. iPlane, Ark) must balance measurement load vs. fidelity
  - Takes several *days* to obtain an (incomplete) network map
  - Can miss transient dynamics (e.g. Nyquist sampling loss), which might reveal properties of interest
  - We seek to advance this state-of-the-art

Technical Approach (1)

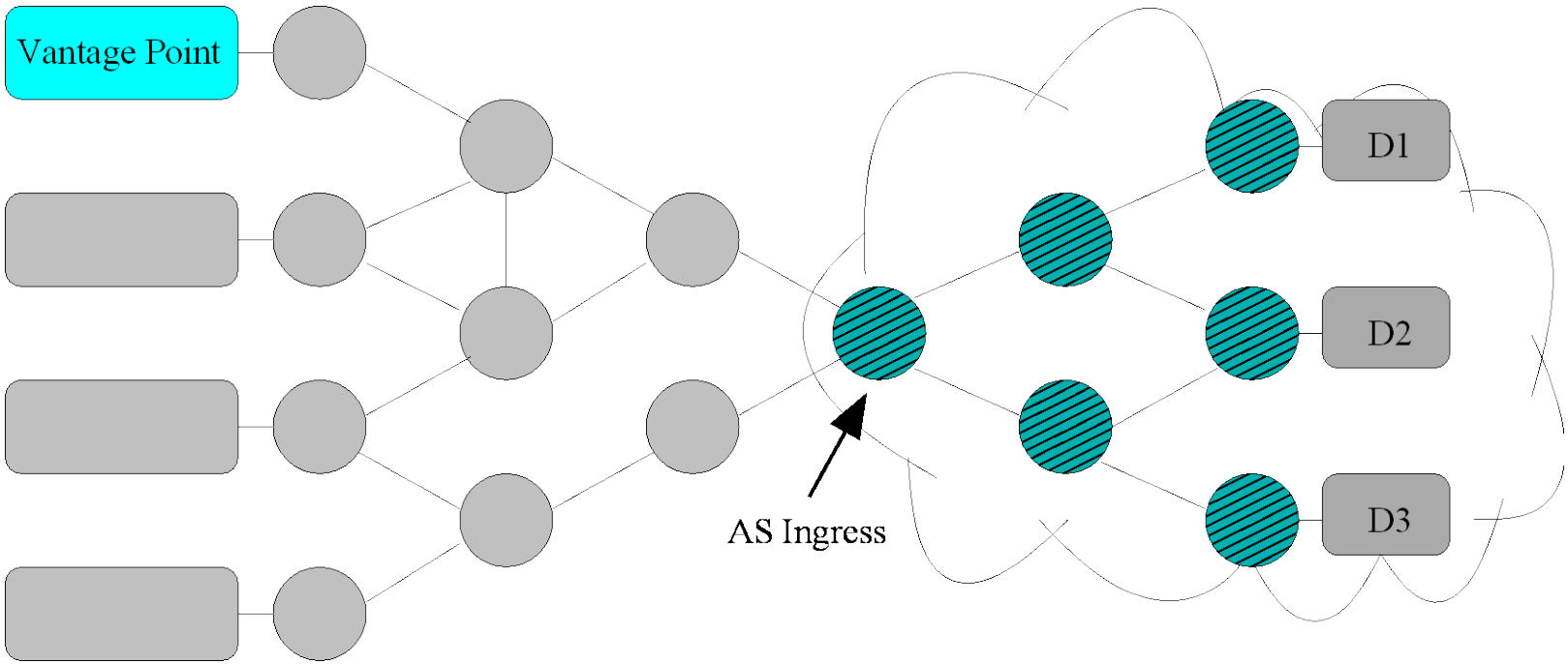
- Our prior work (Beverly et al., ACM IMC 2010):
  - Characterizes production mapping systems
  - Develops new primitives for active topology probing
- Main ideas:
  - Active probing from fixed set of vantage points
  - High-frequency, high-fidelity continuous characterization
  - Probe smarter, not harder
  - Use external knowledge, data from prior cycles, and adaptive sampling to solve:
    - Which destinations to probe
    - How/where to perform the probe
  - Maximize efficiency and information gain of each probe

Technical Approach (2)

- We develop [BBX10] three primitives
- Best explained by understanding sources of path diversity:

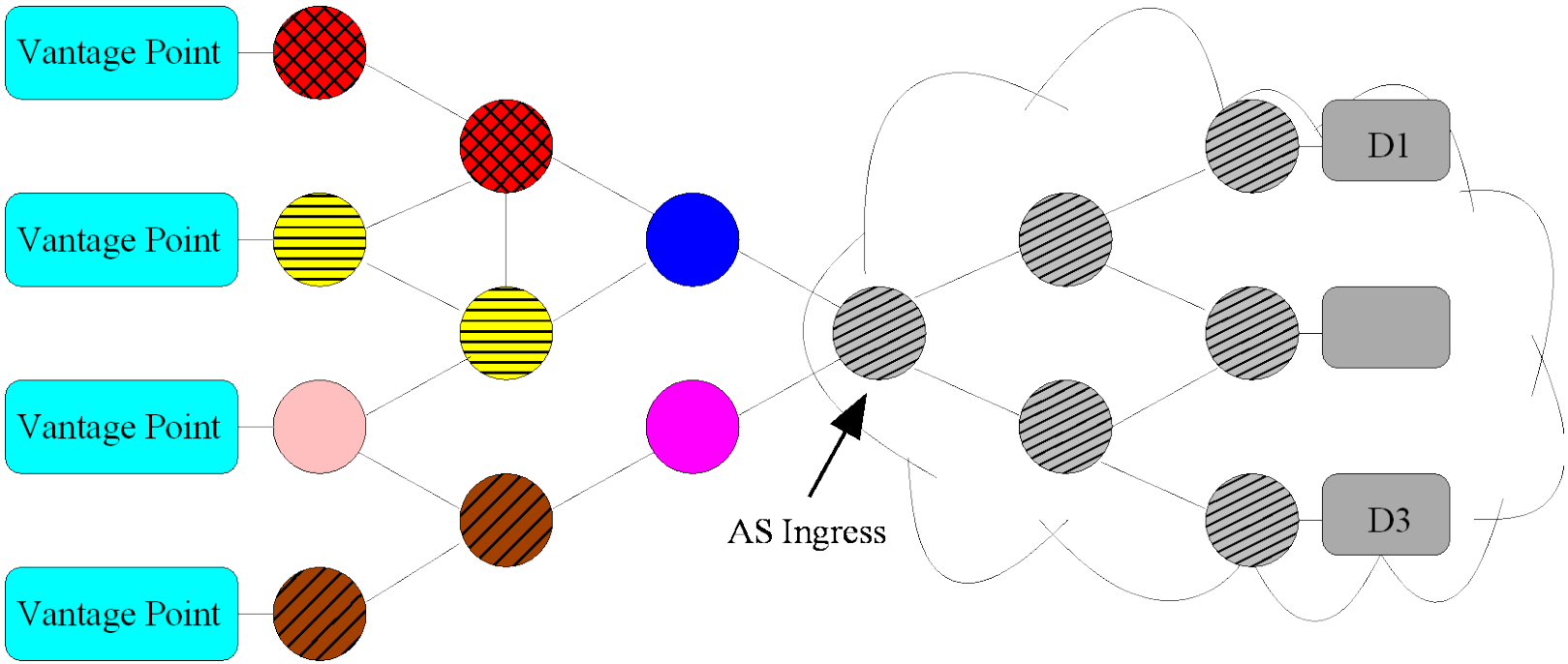


Subnet Centric Probing



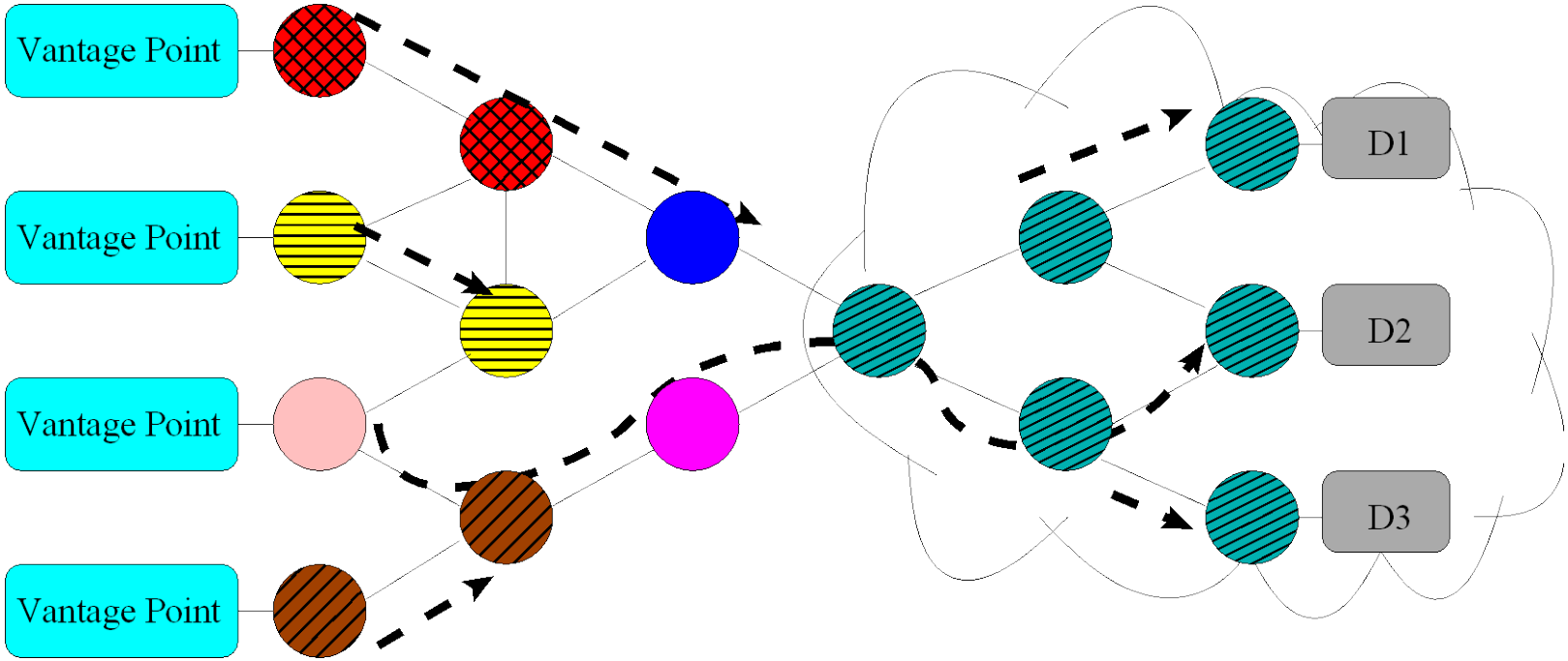
- Instead of probing at a fixed granularity (e.g. /24's), adapt to discover an AS's internal subnetting structure
- Operates on "least common prefix" principle with edit distance stopping criterion
- Especially important for IPv6

Vantage Point Spreading



- Discover AS ingress points and paths from multiple vantage points
- Use BGP knowledge to maximize the number of distinct vantage points per probed prefix

Interface Set Cover



- Multi-round: continuous probing while maintaining state
- Perform greedy minimum set cover approximation
- Select subset of prior round's probe packets for current round
- Generalizes DoubleTree [DRFC05] w/o parameterization

Promising Initial Results

- Result Highlights [BBX10]:
  - Subnet Centric Probing: captures >90% vertex and edge fidelity using 40% fewer probes
  - Vantage Point Spreading: 6% more vertices for free as compared to random assignment
  - Interface Set Cover: >70% probe savings while missing <2% of interfaces after two-weeks
- Now, the hard work…

Technical Challenges

- Non-trivial work to bring primitives to production fruition:
  - Integrate/unify primitives, e.g.:
    - SCP and VPS can be performed together
    - Use SCP to discover load balancing, ISC to verify
  - Refine algorithms, e.g.:
    - How ISC reacts to topology changes?
    - Understand how ISC's learned model decays
    - How SCP can accommodate load-balancing?
    - Updated edit distance metric
  - Integrate real-time BGP updates to drive probing:
    - Hybrid active/passive approach
    - Validation between control and data plane to detect events of interest (e.g. MOAS)

Deliverables

- Quarterly Reports (every 90 days from award)
- Software (1 year from award): Implement our three primitives (SCP, VPS, ISC) into a production mapping system (CAIDA's Ark)
- Refined algorithmic description (1 year from award): Publication of pseudo-code and algorithm details of combined primitives
- Gather data at high-frequency (1-2 years from award), i.e. hours for complete Internet topology
- Release topology data set (1-2 years from award)

Milestones and Schedule

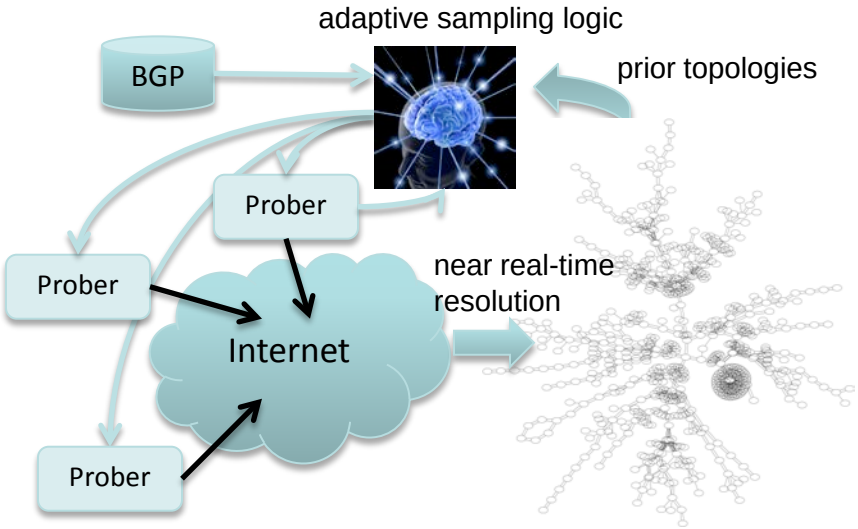
- Year 1:
  - Implement SCP on Ark, validate on ground-truth networks
  - Implement ISC on Ark, develop change-driven logic
  - Implement VPS on Ark
- Year 2:
  - Perform multi-cycle probing using combined primitives
  - Quantify load savings and ability to perform alias resolution
  - Begin gathering/analyzing network maps
  - Gather, annotate, analyze, and release topologies
- Year 3:
  - Gather, annotate, analyze, and release topologies
  - Apply system to probe IPv6 Internet topology

Technology Transition Plan

- Actively collaborating with CAIDA
- Use Ark infrastructure as initial target
- All software released publicly without restriction
- Datasets published to DHS PREDICT and/or CAIDA ITDK repositories
- Interface with Akamai technologies to use developed technologies in real-world applications

BAA Number: Cyber Security BAA 11-02
TTA#7: High Frequency Active Internet Topology Mapping

Homeland Security
Science and Technology



Operational Capability

1. Improve efficiency (time and induced load) of existing active network mapping techniques by an order of magnitude

2. Efficiency gains permit more detailed interface alias resolution and load balancing enumeration thus improving map fidelity

3. Provide improved router level maps in near real-time at scale

4. Discover structure, evolution, and temporal dynamics of critical infrastructure to enable network monitoring, modeling, and protection

Proposed Technical Approach:

1. Our active probing primitives from IMC2010 research use BGP, adaptive sampling, and prior traces to intelligently infer large network topologies

2. Employ these probing algorithms to dramatically reduce network mapping overhead while maintaining fidelity

3. Initial work demonstrates individual promise of primitives, reducing load by >80% without compromising recall

4. Unify algorithms into an operational system to provide near real-time view of large scale network topologies

5. Deploy on CAIDA's Archipelago infrastructure to gather maps at high frequency and uncover temporal dynamics

Schedule, Deliverables, & Contact Info:

Period of Performance: Oct 2012 – Sept 2015

Deliverables: Resultant topological data to be included in PREDICT or other data repositories without restriction, system code under free license, derivative technical reports, conference publications, etc.

Administrative Contact:

Daniella Kuska
Naval Postgraduate School
Monterey, CA 93943-5138
831-656-2099
831-656-2038
dkuska@nps.edu