Path Switching in Content Centric and Named Data Networks

Ilya Moiseenko
Cisco Systems

Dave Oran
Network Systems
Research and Design

Outline

I. Introduction
II. Design
   - Path Discovery & Steering in regular ICN data plane
   - Path Switching ICN data plane
III. Evaluation
IV. Security considerations

I. Introduction

Motivation

- ICN communication is inherently multi-path and potentially multi-destination.
- No mechanism for consumers to direct traffic onto a specific path.

ICN challenges

1. Ability to discover, monitor and troubleshoot multipath network connectivity based on names and name prefixes:
   - Ping
   - Traceroute

2. Ability to accurately measure a performance of a specific network path.

ICN challenges

3. Ability to control multipath congestion:
   - Count number of available paths
   - Uniquely identify a path
   - Allocate traffic to each path

4. Ability for Traffic Engineering and SDN
   - Externally programmable end-to-end paths are highly desirable in Data Center and Service Provider networks

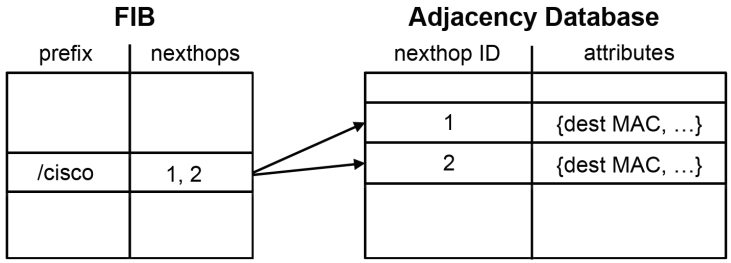
ICN challenges

5. Per-packet Longest Name Prefix Match (LNPM) FIB lookup seems to be a first-order bottleneck
   - Not clear if hardware acceleration is cost-effective
   - Energy consumption using conventional multi-core CPUs is not competitive with IPv4/IPv6, MPLS, Segment Routing data planes.

II. Design

How to label paths?

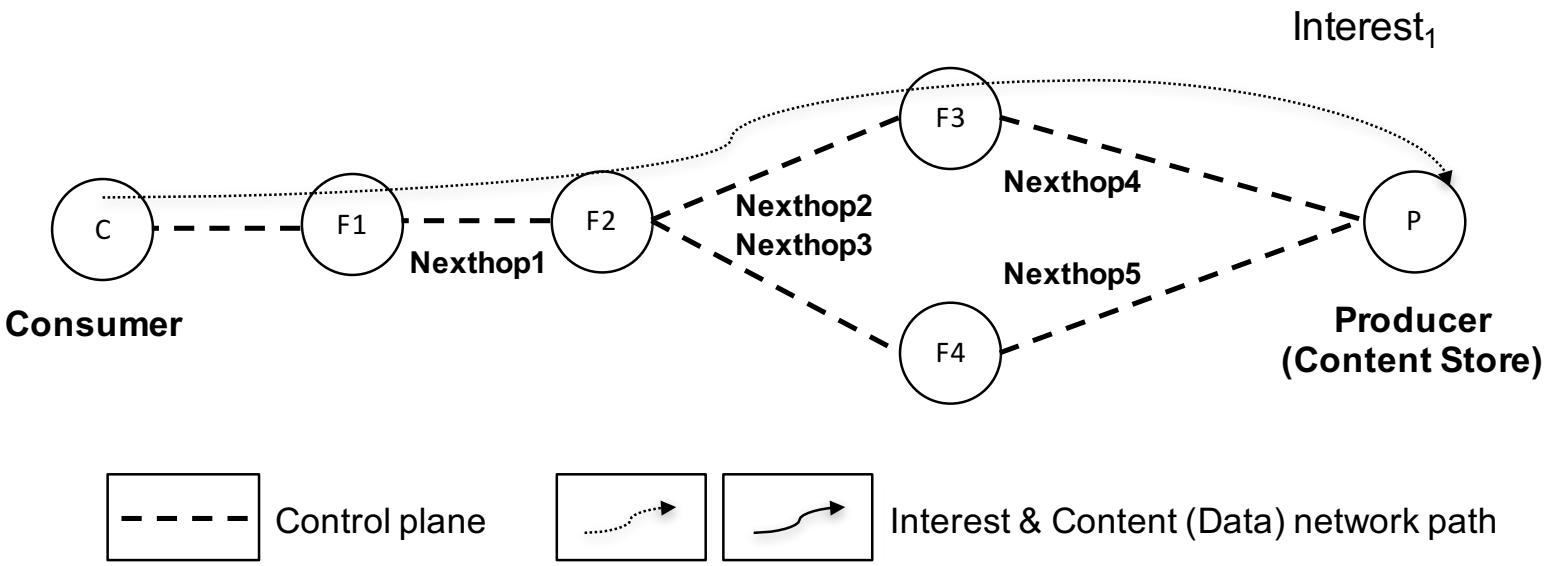
What is a path label? One or more nexthop IDs



Encoding options:

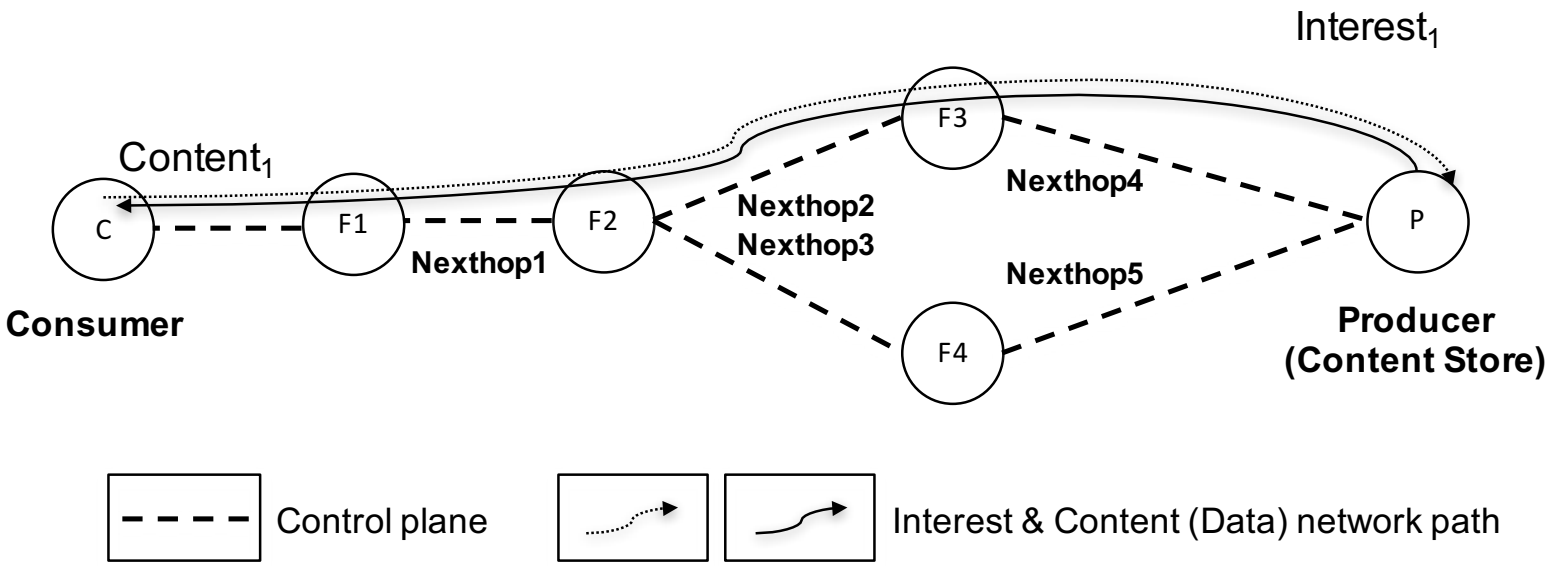
- Bloom filter
- Pairing function
- Fixed size labels
- Label Stack (similar to MPLS label stack)

Path discovery and steering



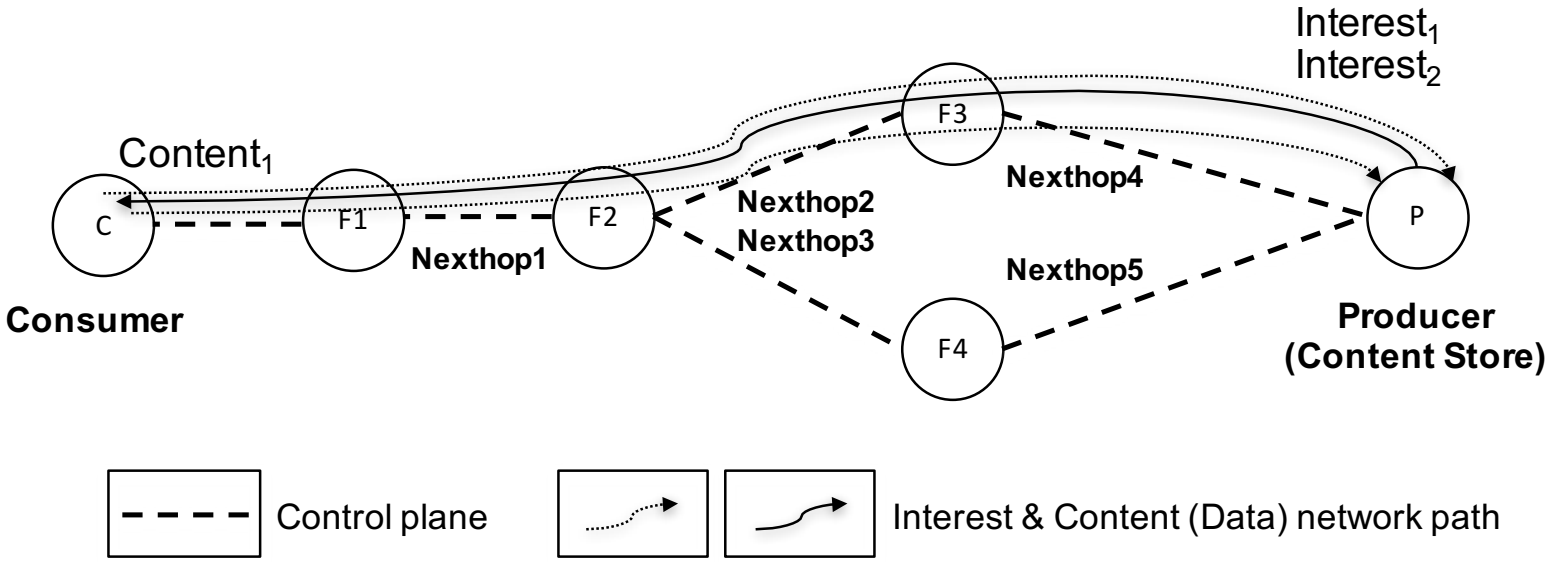
Interest$_1$ has no path label and is forwarded with LPM FIB

Path discovery and steering



Content$_1$ carries a path label modified on each hop

Path discovery and steering



Interest$_2$ has a path label and is forwarded with LPM FIB + nexthop selection

Advantages

- ICN **Ping** application can reliably measure path RTT
- ICN **Traceroute** application can iteratively discover multiple network paths
- Consumer multipath-aware **congestion control** can discover and distribute load across paths
- Consumer can mitigate **content poisoning** attacks
- **Traffic engineering** (TE) and SDN solutions can be built
- Can serve as a foundation for **overlay networks**

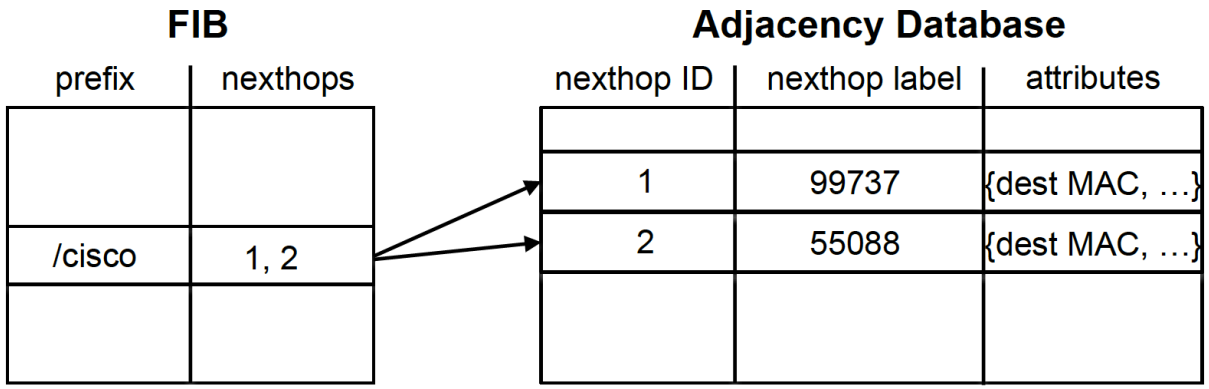
Route updates

- With path steering, LNPM FIB lookup is not bypassed.
- If nexthop selection fails:
  - Interest-Return (NACK) carrying a new “Invalid path label” error code
  - or silently forward an Interest through any available nexthop

Path Switching

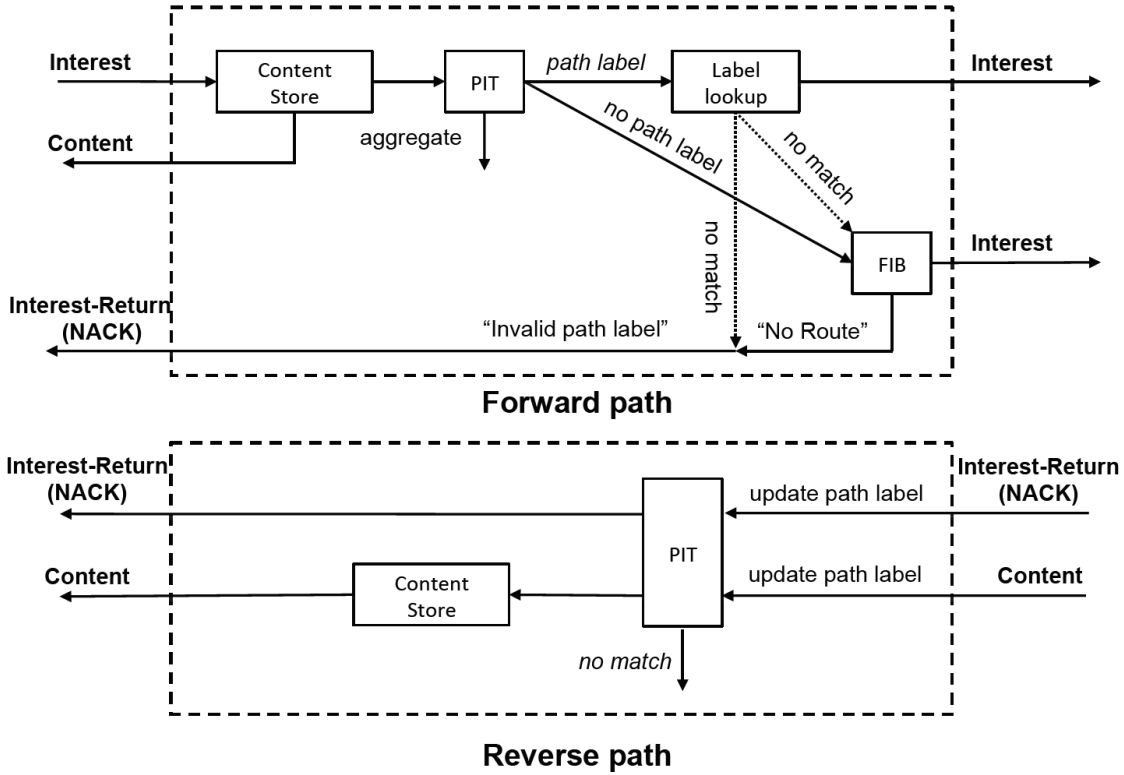
- Bypass LNPM FIB lookup.
- Content (Data) messages are forwarded based on PIT lookup as in regular CCN / NDN.
- Interest messages undergo the same Content Store and PIT lookup as in regular CCN / NDN.
  - Note: this wins over LNPM since the match is exact against full name
- Inherits the advantages of Path Steering alone.

Handling Route updates



- New nexthop label(s) assigned every time FIB entry changes
- On reverse path, Data and NACK is dropped
- On forward path, Interest is NACK'ed

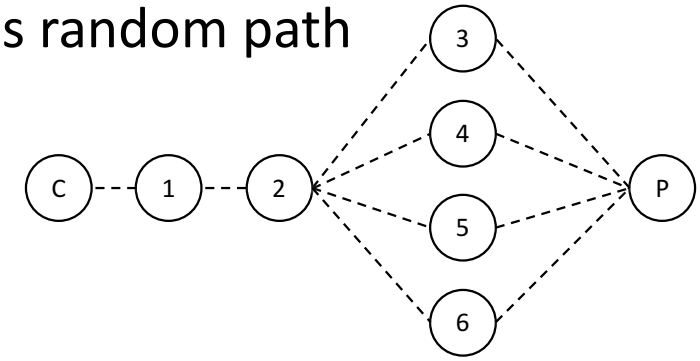
Path switching data plane



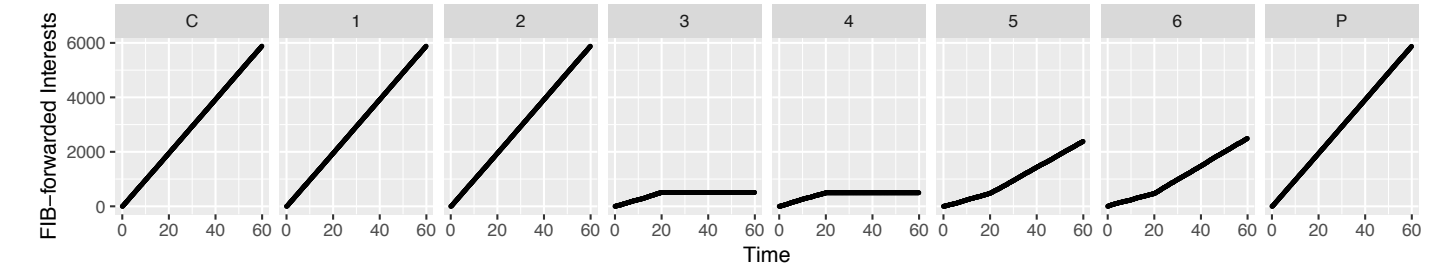
III. Evaluation

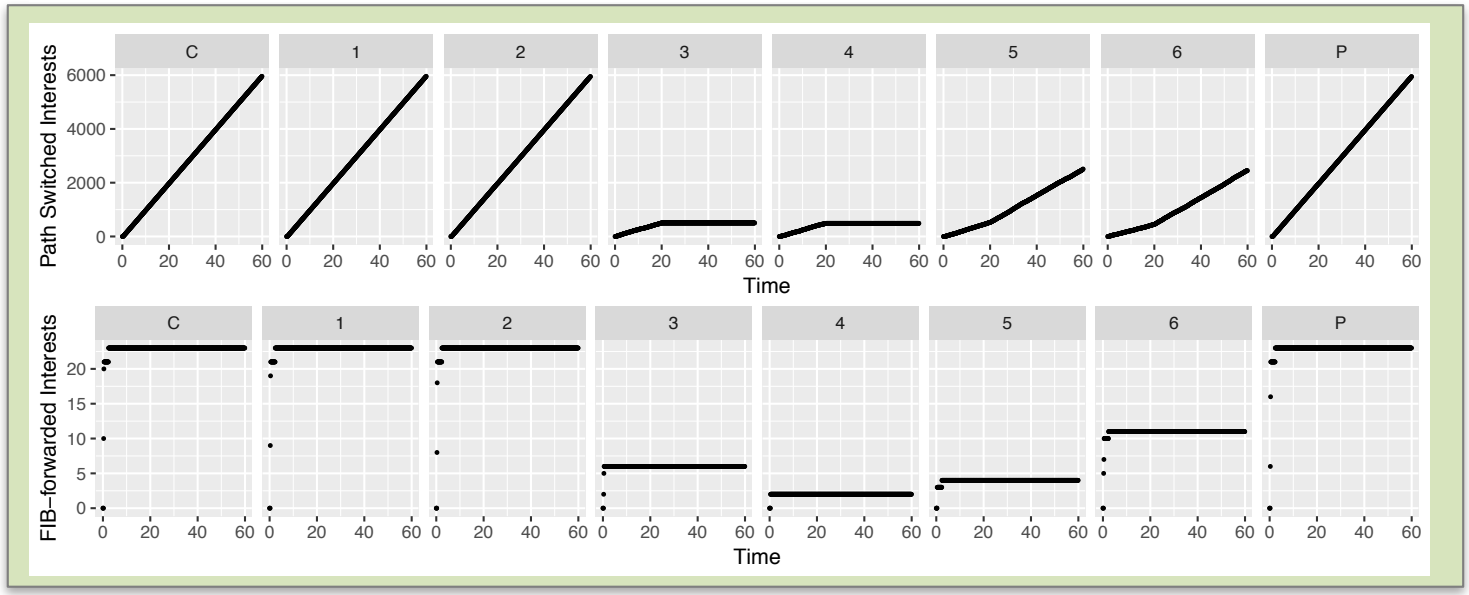
Single prefix route update

- Regular NDN data plane
  - Forwarding strategy selects random ECMP nexthop
- Path switching NDN data plane
  - Consumer has basic path switching capabilities: a) discovers network paths, b) keeps track of unique paths, c) selects random path



Single name prefix route update

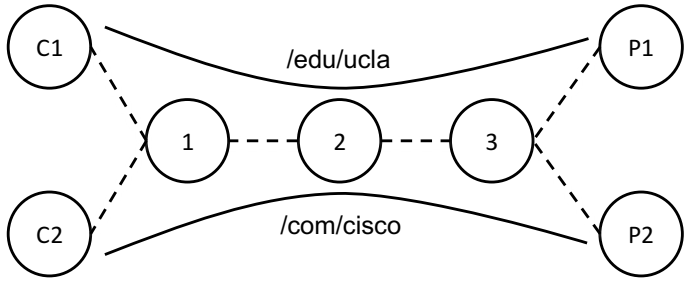




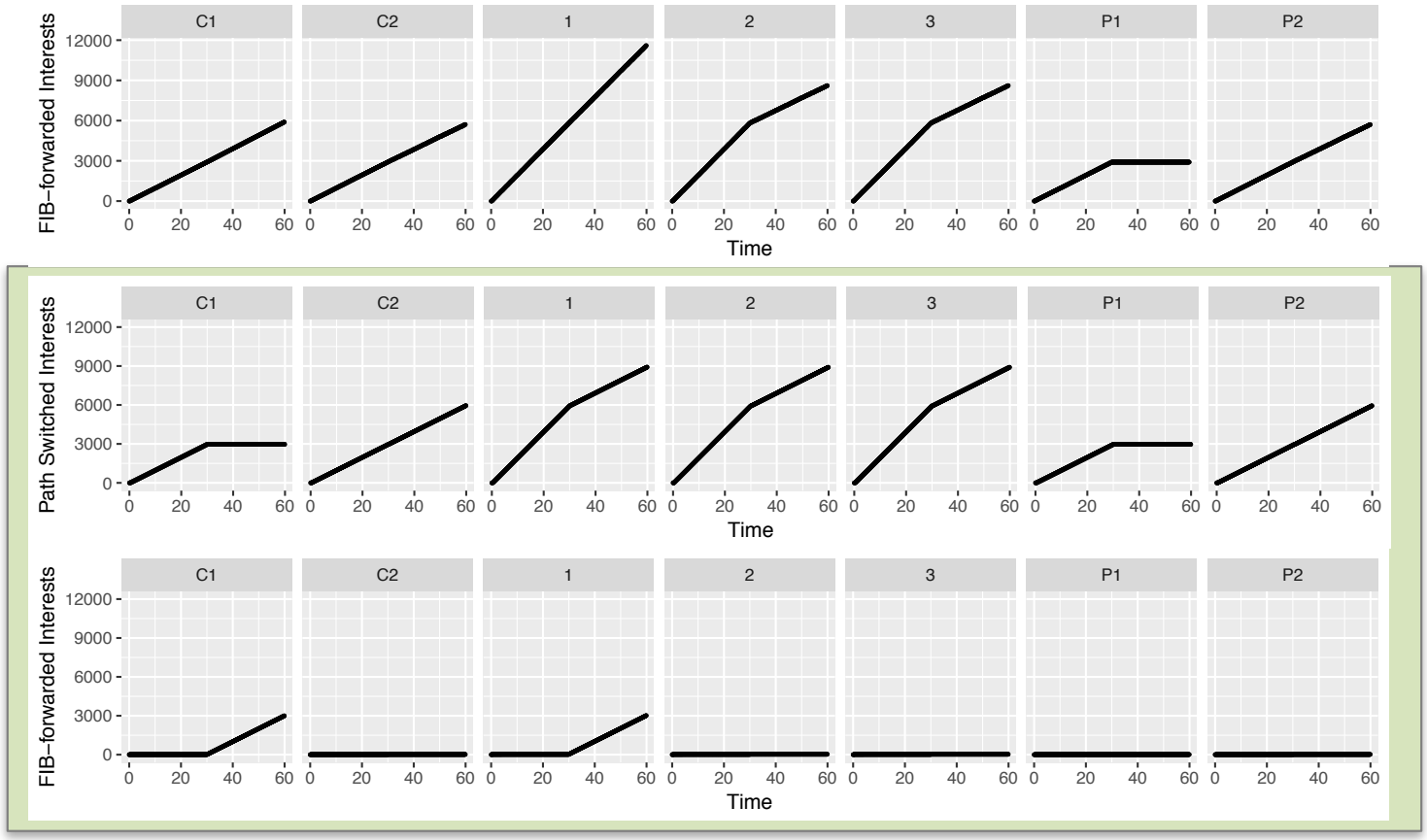
Route update on Node 2 removes the adjacency with Node 3 and Node 4 after 20 seconds of simulation.

Multiple prefix route update

- Path switching CCN/NDN data plane
  - Nexthop relabeling impacts other ongoing flows with unrelated name prefix if nexthops are shared between FIB entries



Multiple name prefix route update.



Route update on Node 2 removes C1 – P1 FIB entry after 30 seconds of simulation.

IV. Security considerations

Malicious mis-steering

Consumer can use probing with Interests to discover path labels and then steer packets over wrong paths or to wrong destinations to mount a DoS attack.

- 32-bit nexthop label requires on average 2^{31} Interests to discover by malicious consumer
- Mitigation: periodically update nexthop labels to limit the maximum lifetime of paths
- To foil divide-and-conquer, use a void Hop Count field in “Invalid path label” Interest-Return (NACK) message
- Path label can be encrypted hop-by-hop on the reverse path

Cache pollution

Malicious consumer & producer can inject an off-path and potentially bogus object in on-path caches.

- Mitigation: Cache entries must be annotated with the corresponding path label and only used to satisfy Interests with a matching path label.
- Mitigation: Cache entries must not evict entries for the same object with no path label, or a different path label.

Conclusion

- Enables Traffic Engineering, SDN, multipath congestion control, ping and traceroute applications.
- The speed of nexthop label lookup does not depend on the size and the contents of FIB.
- Simpler than MPLS because it does not require a separate label distribution protocol.

Q/A