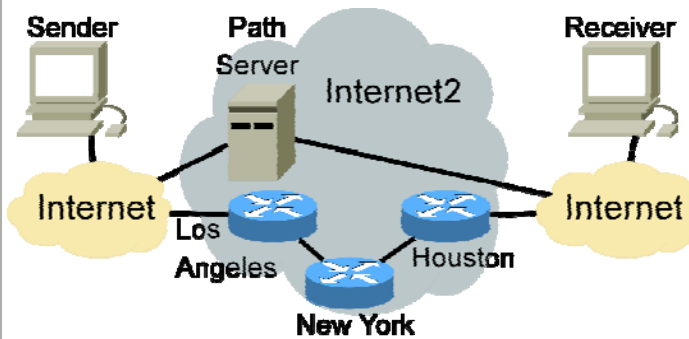


## Research Hypothesis

Strong **crypto** is fast enough to **enforce** practical **provenance** policies on network traffic



## Design Principles

- **Path validity**
  - Path in packet's header explicitly approved by router's realm
- **Provenance verification**
  - Packet verifiably transited all preceding (honest) routers/realms

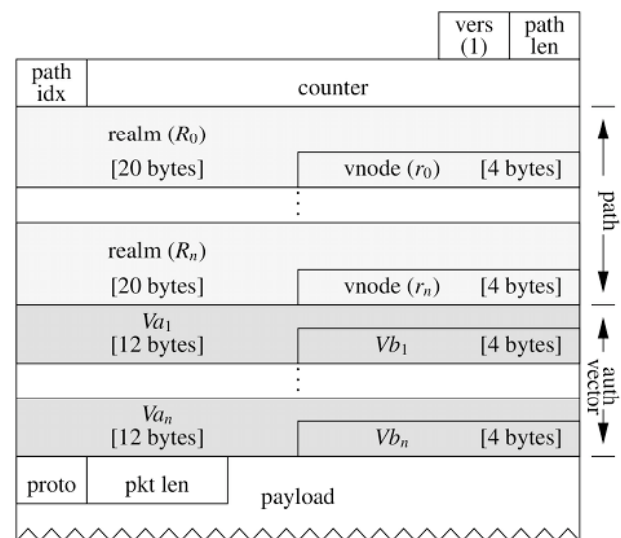
## Protocol Overview

- Path validity: **Proof-of-Consent**
  - Per-path auth'n key (PoC)  $P_{\Pi,R}$
  - Per-packet PoC authenticator  $A_{\pi,R}$
- Pkt provenance: **Aggregate MACs**
  - Routers share keys via NIDH
  - Upstream routers MAC packet  $\pi$
  - Downstream routers check MAC on  $\pi$
  - MAC aggregation keeps overhead low
- **DoS-hardening** via HW/SW split

## Technical Challenges

- Sustain line speed  $> 1$  **Gbps**
- Support **unilateral policy change** w/o global coordination
- Enable **mechanism upgrade** w/o modification to network core

## Match control traffic overhead



## Costs & Performance

