# Bootstrapping **Accountability** and **Privacy** to IPv6 Internet without Starting from Scratch

**Lin He**, Gang Ren, Ying Liu

Tsinghua University

# Contents

- Background
- PAVI Design
- Analysis
- Implementation & Evaluation
- Conclusion

# Background

# Accountability

- No naïve support for accountability
  - Cannot stop in-progress attacks
    - Source spoofing
    - DDoS attacks
- Protocols
  - AIP [Sigcomm’08]
  - IPA [NSDI’11]
  - AaaS [SRUTI’07]

# Privacy

- No naïve support for privacy
  - Pervasive monitoring and mass surveillance
    - Prism event
  - IETF RFC7258 “Pervasive monitoring is an attack”
- Protocols
  - Tor
  - Mix Networks

# Accountability & Privacy

- Both valuable but conflicted
- Balancing accountability and privacy
  - APIP[Sigcomm’14], APNA[CoNEXT'16]
    - New communication identifiers
      - **NID:HID:SID** in APIP
      - **AID:EphID** in APNA
    - Large-scale modifications to fully deployed Internet infrastructure and protocols

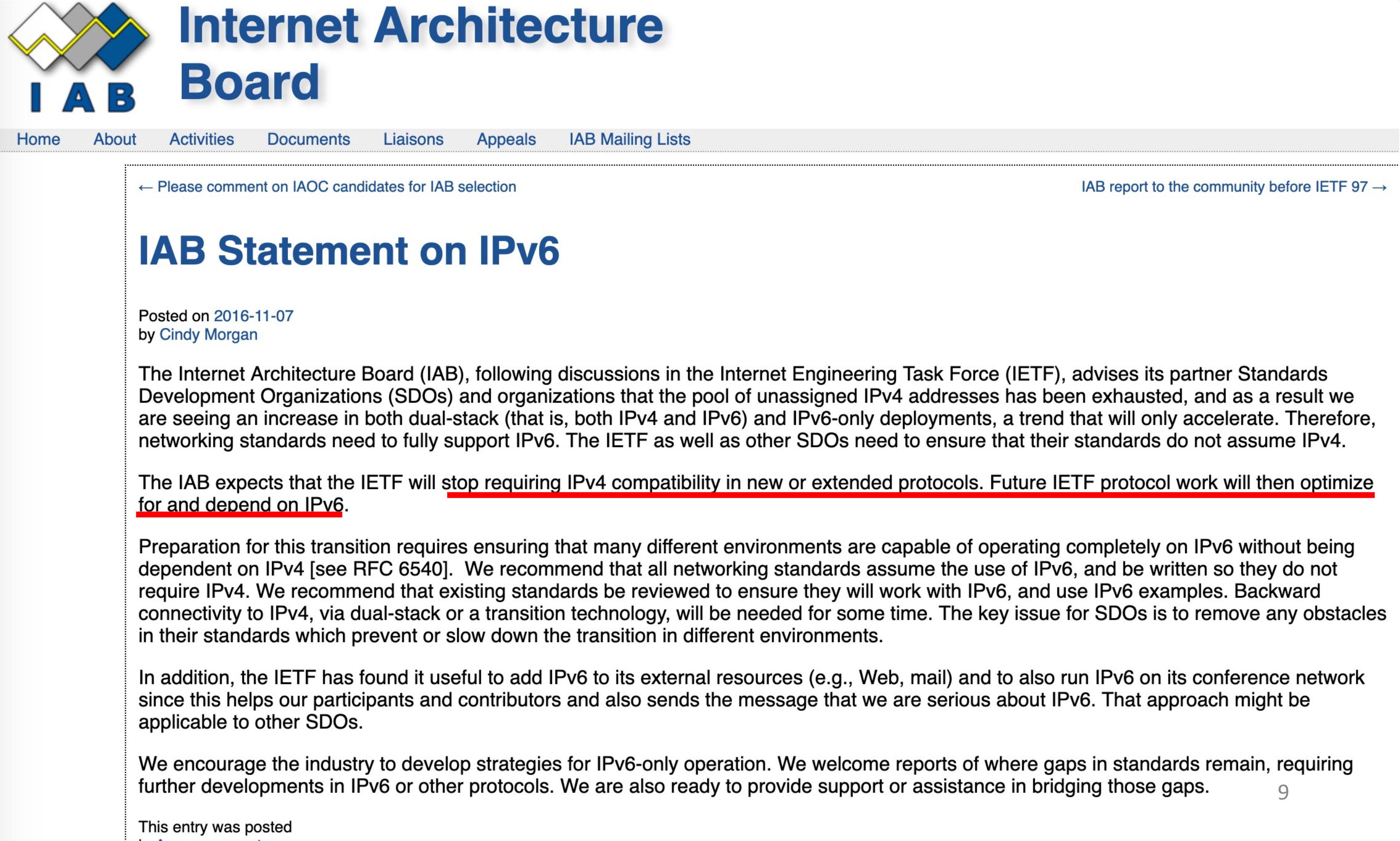
# Problem

- Is it possible to bootstrap accountability and privacy to the current Internet **without introducing new communication identifiers and large-scale modifications to fully deployed infrastructures and protocols**?

PAVI

# PAVI Design

# IPv6 deployment



← Please comment on IAOC candidates for IAB selection

IAB report to the community before IETF 97 →

## IAB Statement on IPv6

Posted on 2016-11-07
by Cindy Morgan

The Internet Architecture Board (IAB), following discussions in the Internet Engineering Task Force (IETF), advises its partner Standards Development Organizations (SDOs) and organizations that the pool of unassigned IPv4 addresses has been exhausted, and as a result we are seeing an increase in both dual-stack (that is, both IPv4 and IPv6) and IPv6-only deployments, a trend that will only accelerate. Therefore, networking standards need to fully support IPv6. The IETF as well as other SDOs need to ensure that their standards do not assume IPv4.

The IAB expects that the IETF will stop requiring IPv4 compatibility in new or extended protocols. Future IETF protocol work will then optimize for and depend on IPv6.

Preparation for this transition requires ensuring that many different environments are capable of operating completely on IPv6 without being dependent on IPv4 [see RFC 6540]. We recommend that all networking standards assume the use of IPv6, and be written so they do not require IPv4. We recommend that existing standards be reviewed to ensure they will work with IPv6, and use IPv6 examples. Backward connectivity to IPv4, via dual-stack or a transition technology, will be needed for some time. The key issue for SDOs is to remove any obstacles in their standards which prevent or slow down the transition in different environments.

In addition, the IETF has found it useful to add IPv6 to its external resources (e.g., Web, mail) and to also run IPv6 on its conference network since this helps our participants and contributors and also sends the message that we are serious about IPv6. That approach might be applicable to other SDOs.

We encourage the industry to develop strategies for IPv6-only operation. We welcome reports of where gaps in standards remain, requiring further developments in IPv6 or other protocols. We are also ready to provide support or assistance in bridging those gaps.

This entry was posted

# What we have

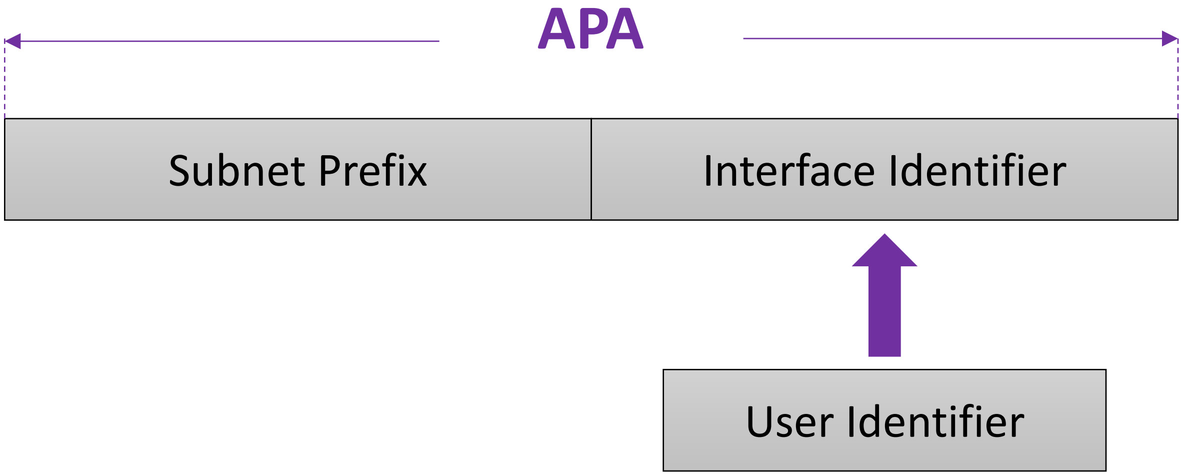
- Large IPv6 address space
  - Larger than IPv4
  - Assume 1M hosts in an AS and each with 3 addresses in a /64 IPv6 prefix
    - $U(3, 10^6, /64) \approx 2.27*10^{-13}$
- Multiple addresses per host
  - Two for SLAAC, one for DHCPv6
  - Assume 1M hosts in an AS and each with 100 addresses in a /64 IPv6 prefix
    - $U(100, 10^6, /64) \approx 7.26*10^{-12}$
- Standardized and well-maintained protocols
  - DHCPv6, SAVI, IPsec, RPKI, etc.
  - Encounter similar problems when designing new protocols

# Design Goals

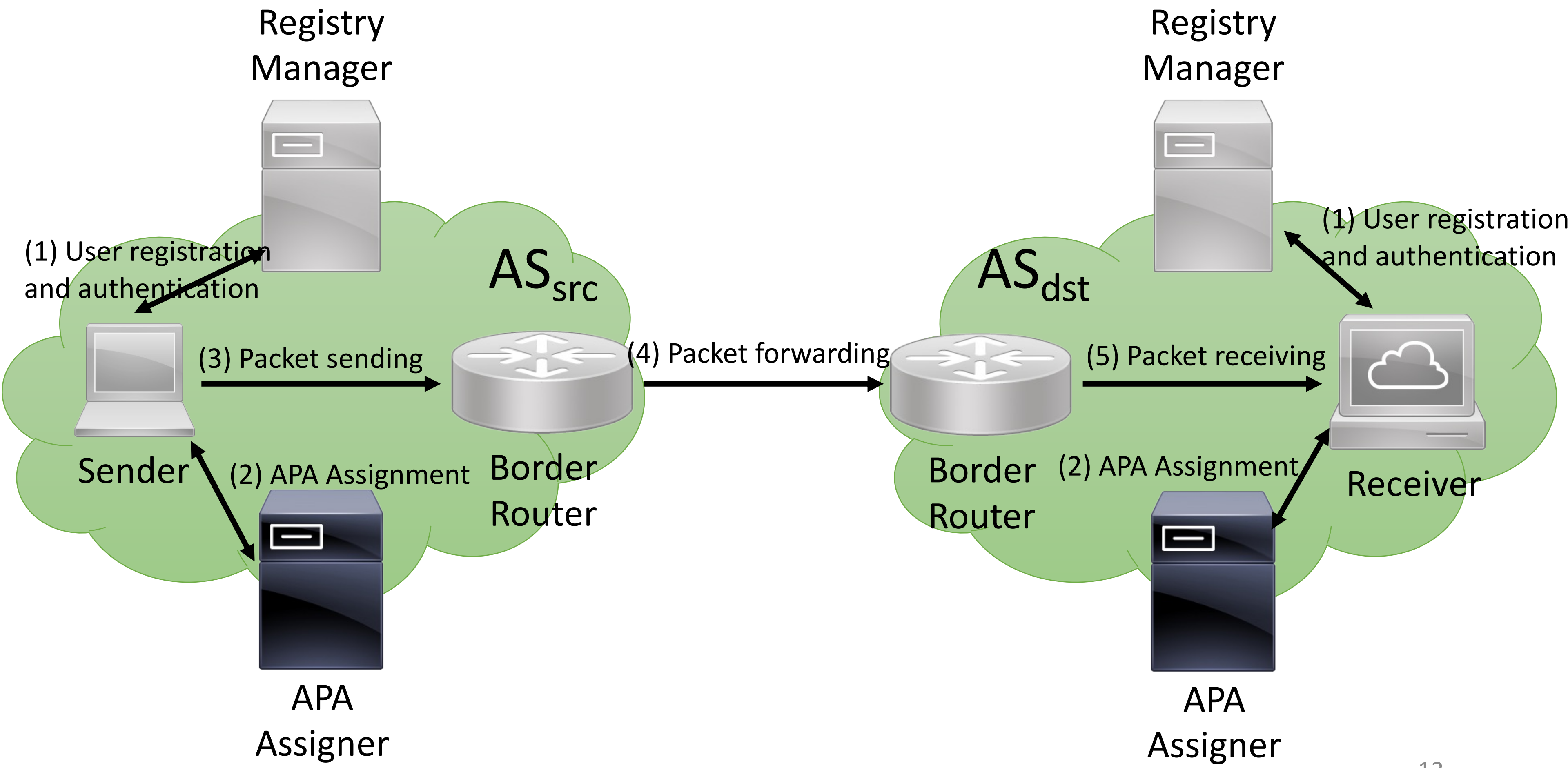
- Accountability
  - Authentic packets
  - Packet-identifier association
  - Unique identifiers
- Privacy
  - Sender anonymity
  - Sender-flow unlinkability
  - Sender-receiver unlinkability
  - Data confidentiality
- Deployability
  - Lightweight enhancements
  - Incrementally deployable

# PAVI Design

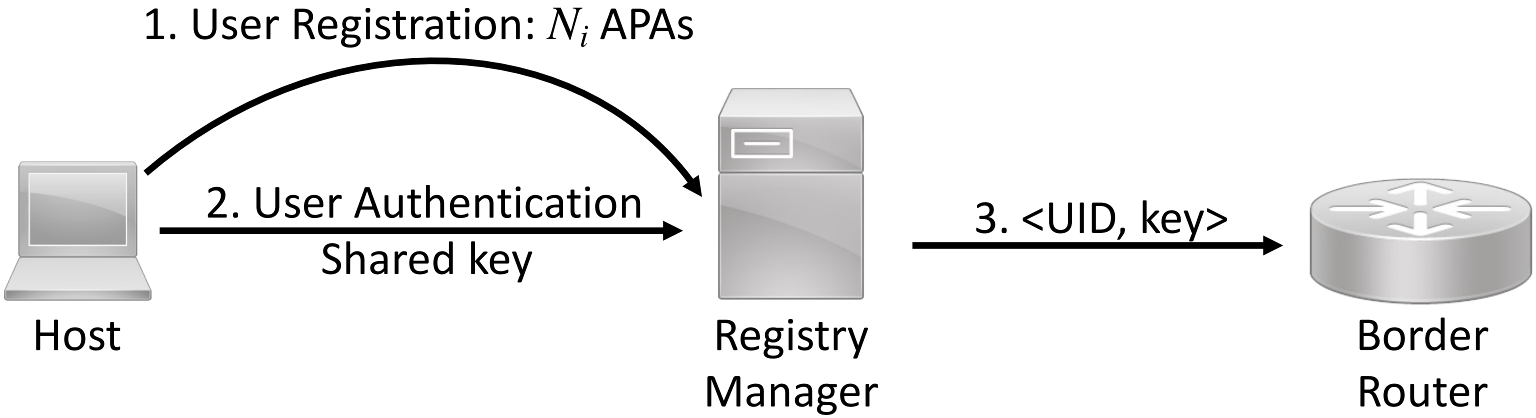
- Accountable and Private Address (APA)
  - Containing user identifier
  - Cryptographically generated
  - IPv6 address



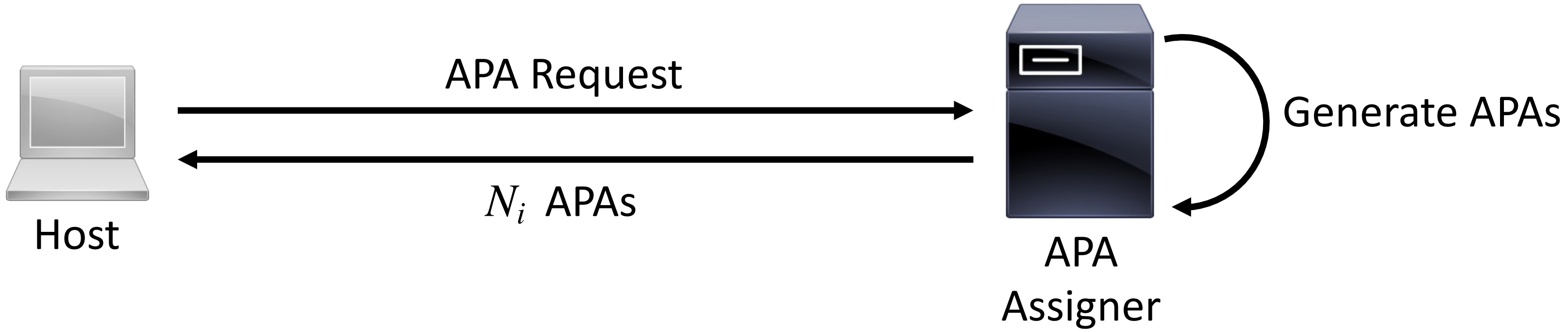
# PAVI Overview



# User Registration and Authentication



# APA Assignment

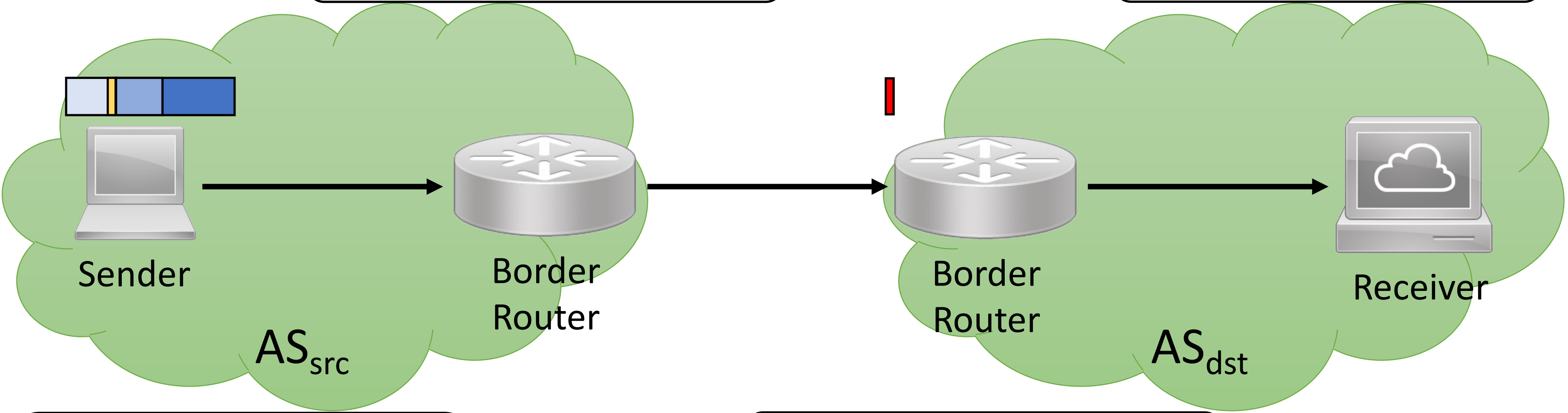


# Packet Flow

- 🟦 Payload
- ▨ PAVI Header
- □ IPv6 Header
- 🟥 Source Masking
- 🟨 Destination Masking

✓ Destination Demasking
✓ Destination Remasking

✓ Source Demasking

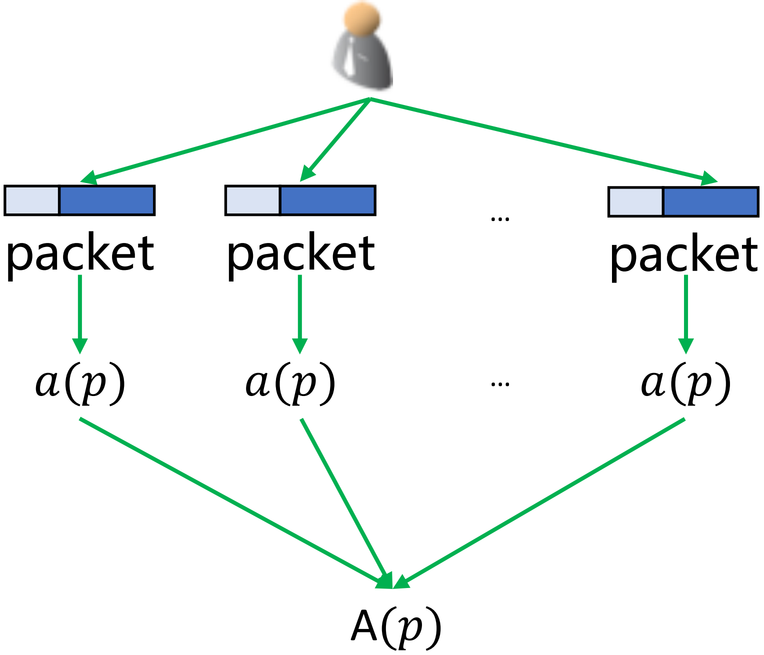


✓ APA Determination
✓ PAVI Header Insertion
✓ Destination Masking

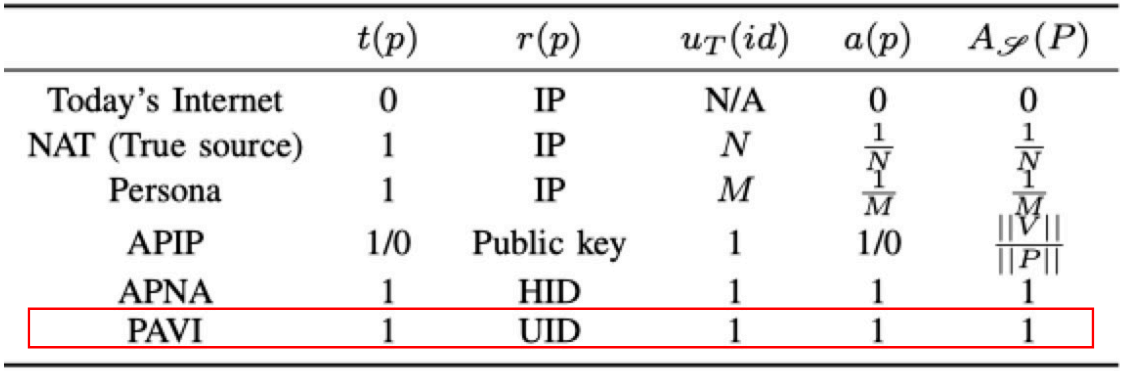
✓ Destination Demasking
✓ Source Masking

# Analysis

# Quantitative Analysis



- Accountability
  - $t(p)$: the authenticity of packet $p$
  - $r(p)$: extract sender identifier from packet $p$
  - $u_T(id)$: the number of entities that use $id$ during $T$
  - Accountability estimation for $p$ is: $a(p) = \dfrac{t(p)}{u_T(r(p))}$
  - For all the packets: $\mathrm{A}(P) = \dfrac{\Sigma_{p \in P} a(p)}{||P||}$



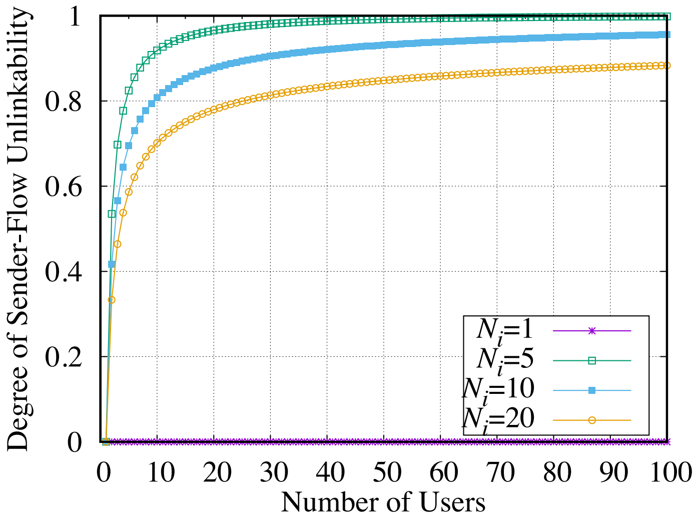
| | $t(p)$ | $r(p)$ | $u_T(id)$ | $a(p)$ | $A_{\mathscr{S}}(P)$ |
|---|---|---|---|---|---|
| Today's Internet | 0 | IP | N/A | 0 | 0 |
| NAT (True source) | 1 | IP | $N$ | $\frac{1}{N}$ | $\frac{1}{N}$ |
| Persona | 1 | IP | $M$ | $\frac{1}{M}$ | $\frac{1}{M}$ |
| APIP | 1/0 | Public key | 1 | 1/0 | $\frac{\|\|V\|\|}{\|\|P\|\|}$ |
| APNA | 1 | HID | 1 | 1 | 1 |
| PAVI | 1 | UID | 1 | 1 | 1 |

# Quantitative Analysis

- Privacy
  - Sender-flow unlinkability [PET’07]

$$U_{\mathsf{A}}(\mathscr{T}_{\emptyset}, \mathcal{U}) = log_2(B_N)$$

$$D_{\mathsf{A}}(\mathscr{T}_{\mathsf{H}}, \mathcal{U}) = \frac{U_{\mathsf{A}}(\mathscr{T}_{\mathsf{H}}, \mathcal{U})}{U_{\mathsf{A}}(\mathscr{T}_{\emptyset}, \mathcal{U})} = \frac{log_2(S(N, M))}{log_2(B_N)}$$



$\mathscr{T}_{\emptyset}$ Attacker knows nothing

$\mathscr{T}_{\mathsf{H}}$ Attacker knows hint H

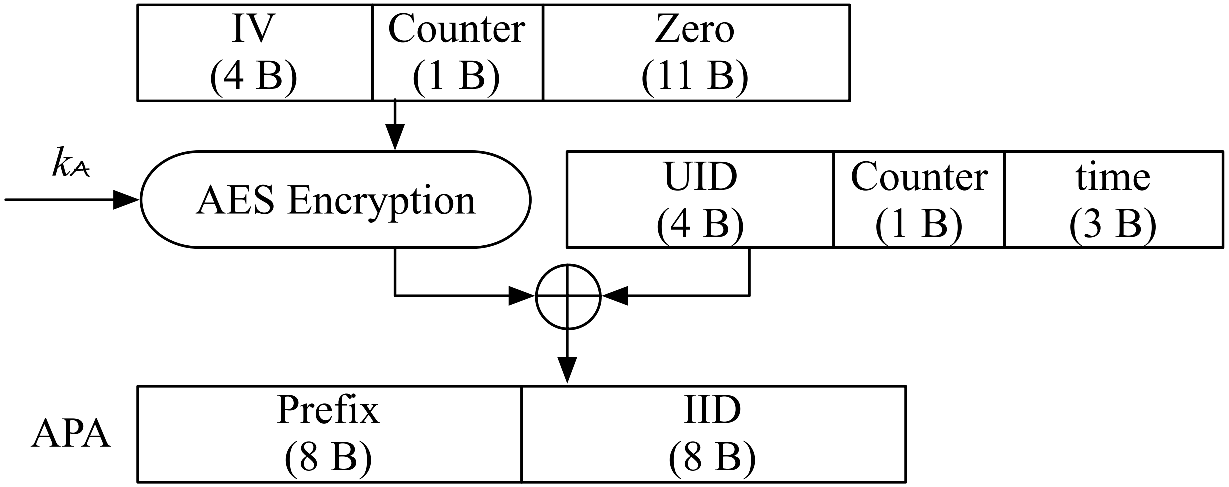
# Implementation & Evaluation

# Implementation

- APA Generation
  - Scheme 1:

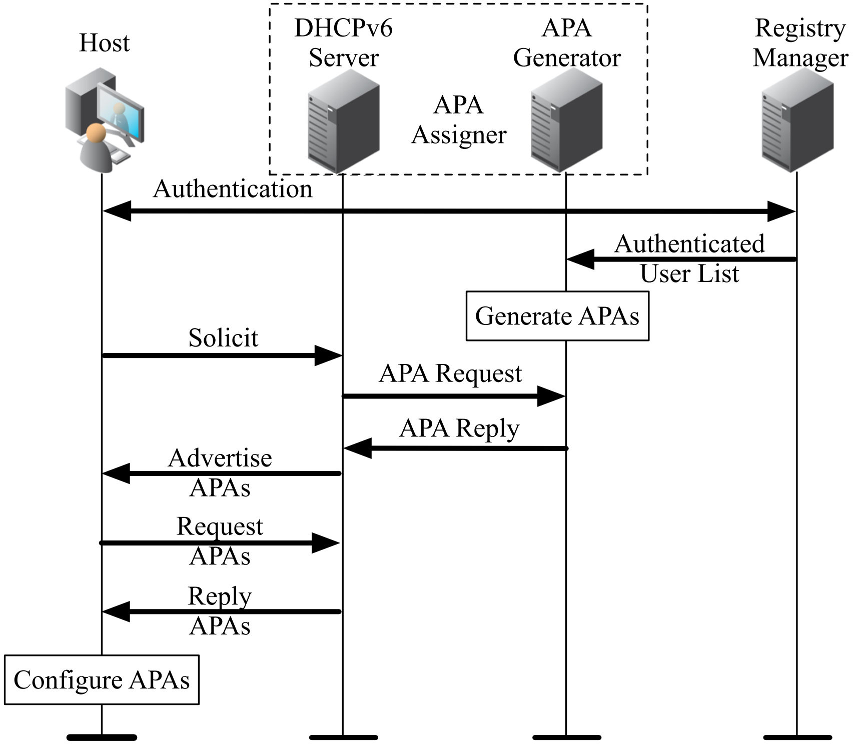
$$\mathsf{A}_j^{\mathcal{U}_i} = prefix||E_{k_{\mathcal{A}_{\mathcal{S}}}}(UID_i||n_j||t_j||d_j)$$

  - Scheme 2:

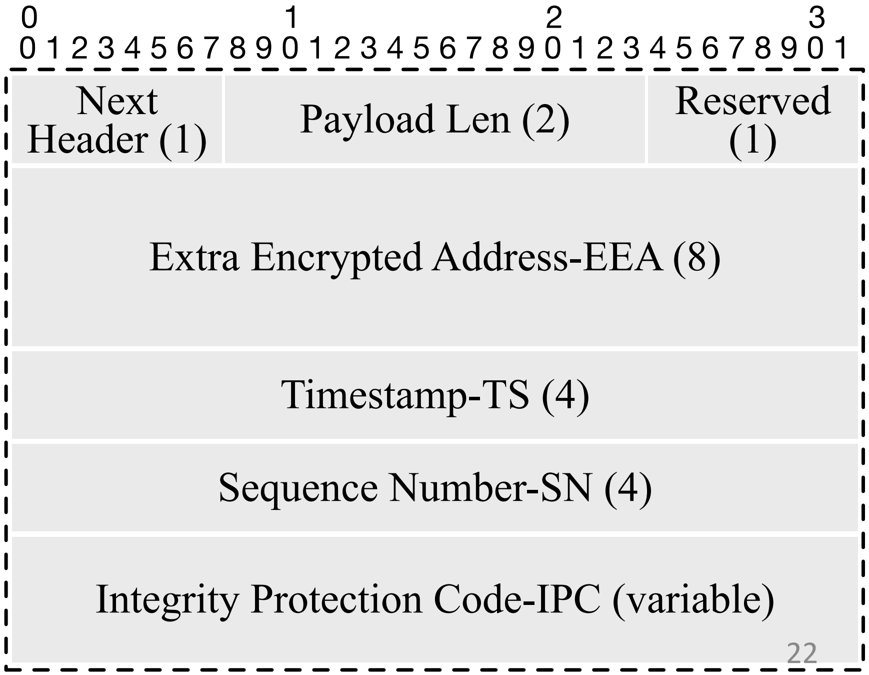


# Implementation

- APA Assignment
  - DHCPv6 extensions



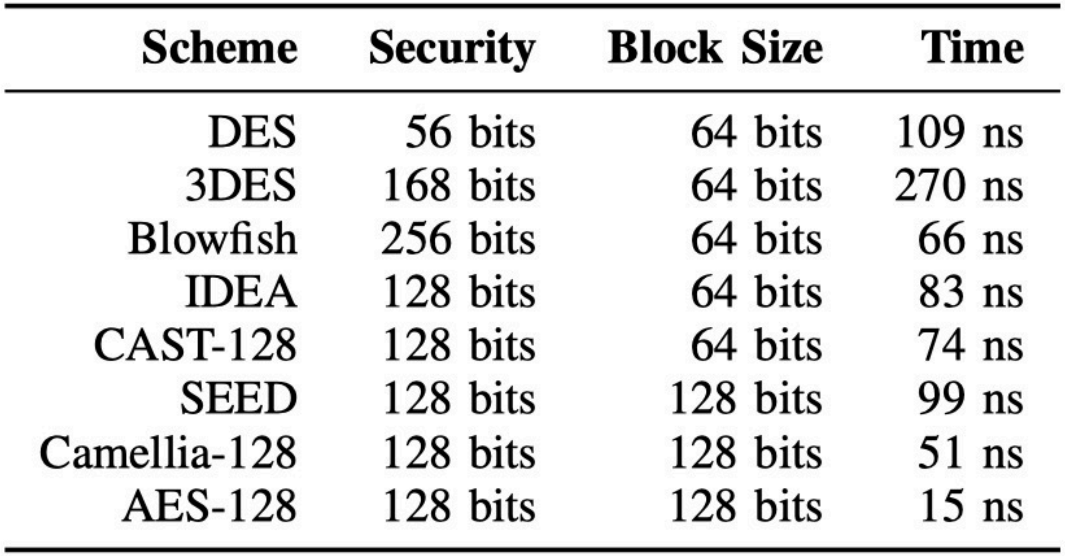
- Border Router
  - Intel Data Plane Development Kit
  - AES-NI
  - To compute IPC, we use CBC-MAC



| Next Header (1) | Payload Len (2) | Reserved (1) |
|---|---|---|
| Extra Encrypted Address-EEA (8) | | |
| Timestamp-TS (4) | | |
| Sequence Number-SN (4) | | |
| Integrity Protection Code-IPC (variable) | | |

# Evaluation

- APA Generation
  - OpenSSL

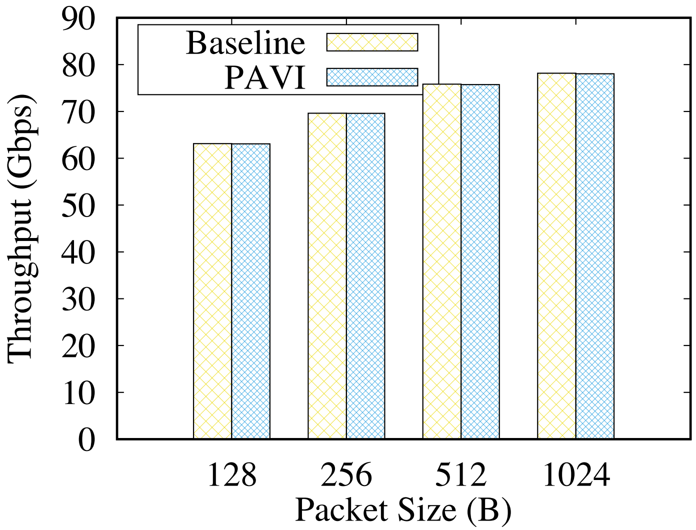


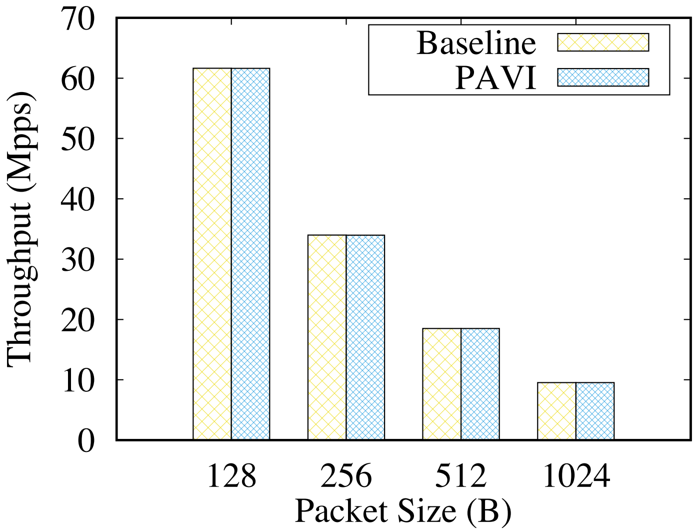
| Scheme | Security | Block Size | Time |
|---:|---:|---:|---:|
| DES | 56 bits | 64 bits | 109 ns |
| 3DES | 168 bits | 64 bits | 270 ns |
| Blowfish | 256 bits | 64 bits | 66 ns |
| IDEA | 128 bits | 64 bits | 83 ns |
| CAST-128 | 128 bits | 64 bits | 74 ns |
| SEED | 128 bits | 128 bits | 99 ns |
| Camellia-128 | 128 bits | 128 bits | 51 ns |
| AES-128 | 128 bits | 128 bits | 15 ns |

  - Storage
    - 1 host and 100 APAs: **12KB**
    - 1M hosts and each with 100 APAs: **11.2GB**

# Evaluation

- Data Forwarding
  - Bandwidth Overhead





  - Storage Overhead
    - AS Keys (~65500)
      - 128-bit keys and 4 bytes index: **1.25 MB**
    - Host keys (~1M)
      - 128-bit keys and 4 bytes index: **19 MB**

# Comparison

| | APIP | APNA | PAVI |
|---|---|---|---|
| Host | √ | √ | √ |
| Applications | √ | √ | × |
| Access router | √ | √ | × |
| Border router | √ | √ | √ |
| DNS | √ | √ | × |
| Intra-routing | √ | √ | × |
| BGP | √ | √ | × |

# Conclusion

# Conclusion

- PAVI bootstraps accountability and privacy to the IPv6 Internet
  - Accountability
  - Privacy
    - Sender anonymity
    - Sender-flow unlinkability
    - Sender-receiver unlinkability
    - Data confidentiality
  - Analysis: security, quantification
  - Performance evaluation: lightweight and deployable

# Thank you!