One Tunnel is (Often) Enough

Simon Peter, Umar Javed, Qiao Zhang, Doug Woos, Thomas Anderson, Arvind Krishnamurthy

University of Washington

Financial support: NSF, Cisco, and Google
Internet Routing Has Issues

Outages and poor performance due to:

- Pathological routing policies
- Route convergence delays
- Misconfigured routers
- Prefix hijacking
- Malicious route injection (route table overload)
- Distributed denial of service

Good technical solutions in most/all cases, but glacial progress towards adoption.
Why?

The fault lies not in our stars, but in ourselves.
– Cassius
Why?

The wheels of justice grind slow but grind fine.
– Sun Tzu
Why?

We don’t care, we don’t have to, we’re the phone company.
– Lily Tomlin
Local Problem => Global Outage

- Sprint
- AT&T
- Comcast
- Amazon
- FlakyISP
- ReliableISP
- PowerData

Blackholes
IP prefix hijacks
DDoS attacks

99.999% available!
Local Problem => Global Outage

Can we turn local reliability into global reliability?
Assumptions/Observations

Shorter paths are more reliable than longer paths

Simple packet processing is feasible at high-speed border routers
  - 10 Gb per core on commodity hardware

AS graph is relatively small and stable

See paper for quantitative justifications.
ARROW

ARROW: Advertised Reliable Routing Over Waypoints
- ISPs offer a QoS tunnel across their network to remote customers
- Paid service akin to AWS or Google Cloud

ARROW runs on a small ISP we control

Evaluation: ARROW effective even if only a single tier-1 ISP adopts
1. Consult atlas of ISPs offering ARROW services
2. Construct tunnel through ARROW ISP, to output target address
Use Cases

Enterprises
- More reliable access to cloud services
- QoS between physically remote locations
- Home health monitoring

Business-facing ISP or cellular telecom
- Market share driven by perceived data network performance, reliability
- Well-developed market for premium service
- 70% of data traffic exits telecom network
ARROW Mechanisms

How does endpoint/proxy know what tunnels are available?

- Atlas published by ISPs offering ARROW service: latency/bw/cost to which prefixes
- User/app-specific path selection

How are packets encapsulated?

![Image of packet encapsulation diagram]
ARROW Mechanisms

How are packets authenticated?
- Packet authenticator provided by ISP at setup
- Authenticator can be hashed with checksum of packet to prevent snoop-stealing

What ISP data plane operations are needed?
- Check authenticator
- Check packet is within rate limit envelope
- Handle fault isolation probe, if any
- Re-write destination address
Failover

Failure of a router internal to an ISP
- ARROW is a stateful service
- Local detection/recovery using Zookeeper

Failure of a border router
- End system/proxy detection/recovery
- Use backup route through another PoP

Failure of an entire ISP
- End system/proxy detection/recovery
- Use backup route through other ISPs
Failure Isolation

How does endpoint/proxy locate who is at fault for service disruption?
- Send probe packet to locate the failure
- Each hop:
  - Responds to the previous hop
  - Forwards the probe packet to next hop

See UW TR for efficient Byzantine-resilient solution
Implementation
# Overhead

What is the data plane overhead of ARROW?

<table>
<thead>
<tr>
<th>Protocol</th>
<th>RTT (us)</th>
<th>Throughput (Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP/TCP</td>
<td>96</td>
<td>9.4</td>
</tr>
<tr>
<td>Serval</td>
<td>81</td>
<td>9.5</td>
</tr>
<tr>
<td>ARROW 1 hop</td>
<td>132</td>
<td>9.5</td>
</tr>
</tbody>
</table>
Failover Latency

- Time to failover [ms]
- With Consistency
  - Failover only

- Edge router
- PoP
- ISP
BGP Outage

Original BGP path

Outage

New BGP path

Emulab src

GA Tech

WISC

ARROW path

UW dest

USC

ARROW path

700 ms

90 s
Link Failure Disconnections (Simulated: 1 ARROW Tier-1)
Prefix Hijacking (Simulated)

CCDF of prefix hijacks vs. Fraction of sources still polluted

- 4 ARROW ASes
- 2 ARROW ASes
- 1 ARROW AS
- BGP
Summary

ARROW: Advertised Reliable Routing Over Waypoints
- ISPs offer a paid QoS tunnel across their network to remote customers
- ARROW runs on a small ISP we control
- Also on Google Cloud Platform

One tunnel (through a tier-1) is often enough