Observations on the Reachability and Evasion of Packets with IPv6 Extension Headers on the Internet

draft-zedongjia-v6ops-ipv6eh-measurement

Lin He, Zedong Jia, Le Gai, Shenglin Zhang, Ying Liu

Tsinghua University

IETF 126, Vienna, July 2026

Background

01. IPv6 Extension Headers (IPv6 EH)

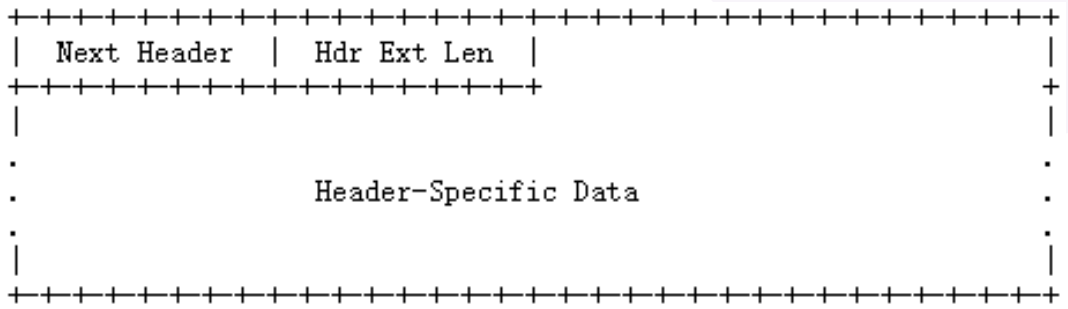
Sit between the IPv6 base header and upper-layer protocols. Provide flexibility for fragmentation, mobility, source routing, and IPsec while keeping the base header simple.

02. Wide Application

EHs underpin Mobile IPv6, SRv6, IOAM, and IPsec. As IPv6 adoption grows, middleboxes must handle them correctly to avoid breaking production traffic.

03. Security Concerns

Improper handling causes two risks: unknown EHs may bypass ACLs; over-parsing invites DoS. Known issues include RH0 amplification, overlapping fragments evading firewalls, and atomic-fragment exhaustion.



IPv6 Extension Header Structure

0	IPv6 Hop-by-Hop Option	[RFC8200]
43	Routing Header for IPv6	[RFC8200][RFC5095]
44	Fragment Header for IPv6	[RFC8200]
50	Encapsulating Security Payload	[RFC4303]
51	Authentication Header	[RFC4302]
60	Destination Options for IPv6	[RFC8200]
135	Mobility Header	[RFC6275]
139	Host Identity Protocol	[RFC7401]
140	Shim6 Protocol	[RFC5533]
253	Use for experimentation and testing	[RFC3692][RFC4727]

Common EH Type Taxonomy

Open Questions

01. Limits of Current Understanding

Prior work reports high drop rates for Hop-by-Hop, Destination Options, and Fragment headers [RFC7872], but characterizes WHAT is dropped, not WHY.

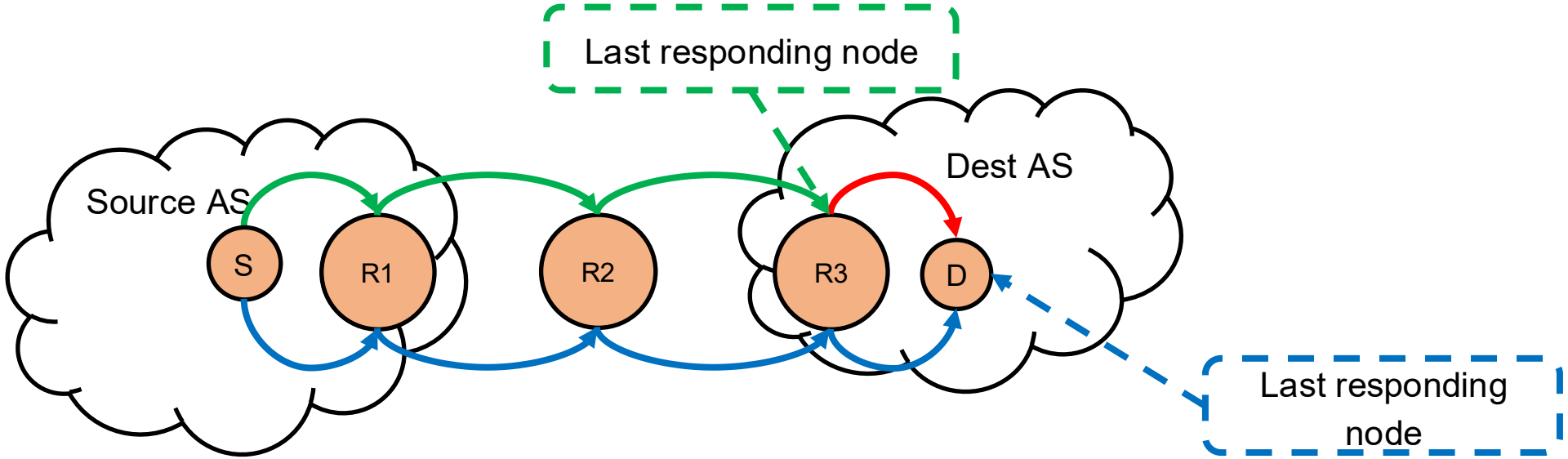
02. Unresolved Questions

Whether drops stem from parsing failures, ACL policy, or MTU remains unclear. The security implications are also open: whether EH-tagged packets can reach segments that standard traffic cannot has not been studied at Internet scale.

Methodology

Path Traversal: for a given probe type and end-to-end path, locate the last responding node to measure reachability.

Comparative Analysis: compare reachability of different probes to infer firewall filtering policy and potential bypass paths.



Note:
If the destination does not respond, the last hop is the last responding intermediate router.

Measurements are collected with 6Travel, a large-scale EH measurement tool.

Study Setup

EH	Alias	Default Size (octets)	Description
Destination Options header	Dst	8	The option is PadN.
Fragment header	Frag	8	The offset and M flag are set to zero and one, respectively
Atomic Fragment header	AFrag	8	The offset and M flag are both set to zero.
Routing header (type 0)	RH0	8	The segments left field is set to zero.
Routing header (type 2)	RH2	24	The home address is set to the target address.
Routing header (type 127)	RH127	8	The segments left field is set to zero.
Authentication header	AH	24	All IPSec-related fields are filled with zeros.
Encapsulating Security Payload	ESP	-	All IPSec-related fields are filled with zeros.
Mobility header type 0	MH	8	All fields are set according to RFC6275 [36]
Host Identity Protocol header (type 1)	HIP	48	All fields are set according to RFC7401 [42]
Shim6 Protocol header	Shim6	8	All fields are set according to RFC5533 [44]

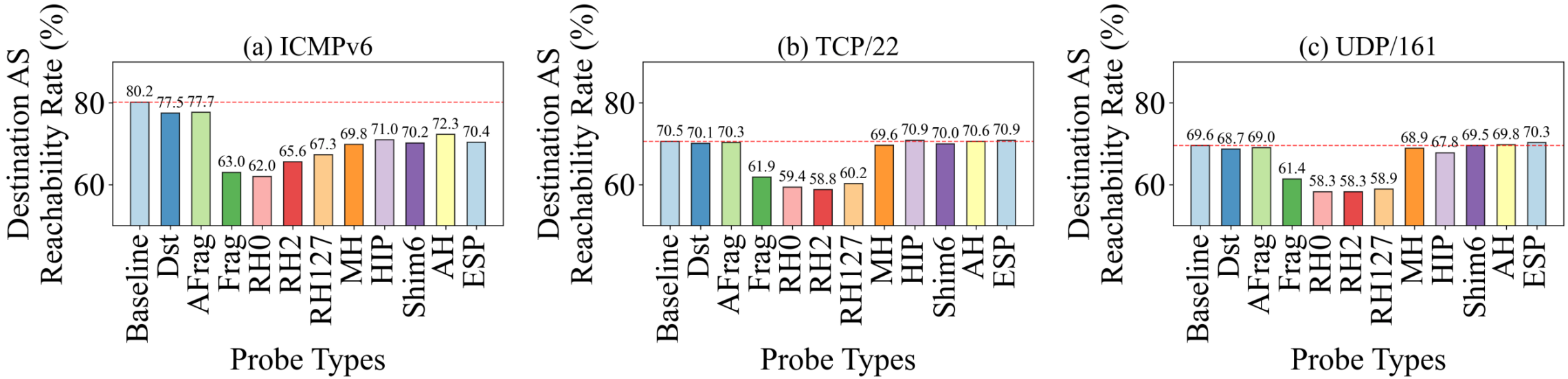
	Date	#Address	#/48	#AS	#IC
Source 1	January, 2026	240,160,125	581,098	22,221	17
Source 2		269,923,736	1,485,873	2,158	17
Source 3		-	5,177,906	13,217	17
Total	-	-	6,336,433	23,999	17

Measurements originate from a vantage point in an education network (Beijing, China), covering cross-border IPv6 paths to 6.3 million /48 prefixes across nearly 24,000 ASes and 17 industries; 11 common EH types are tested.

Results: Reachability

X-axis: Baseline = standard ICMPv6/TCP/UDP; other bars = probes with EHs (Routing, Dst, …).

Y-axis: Ratio of probes reaching the destination AS, normalized to 1.0 at baseline.



High Network Compatibility

The Destination Options and Atomic Fragment headers now reach the destination AS at rates close to standard TCP/UDP.

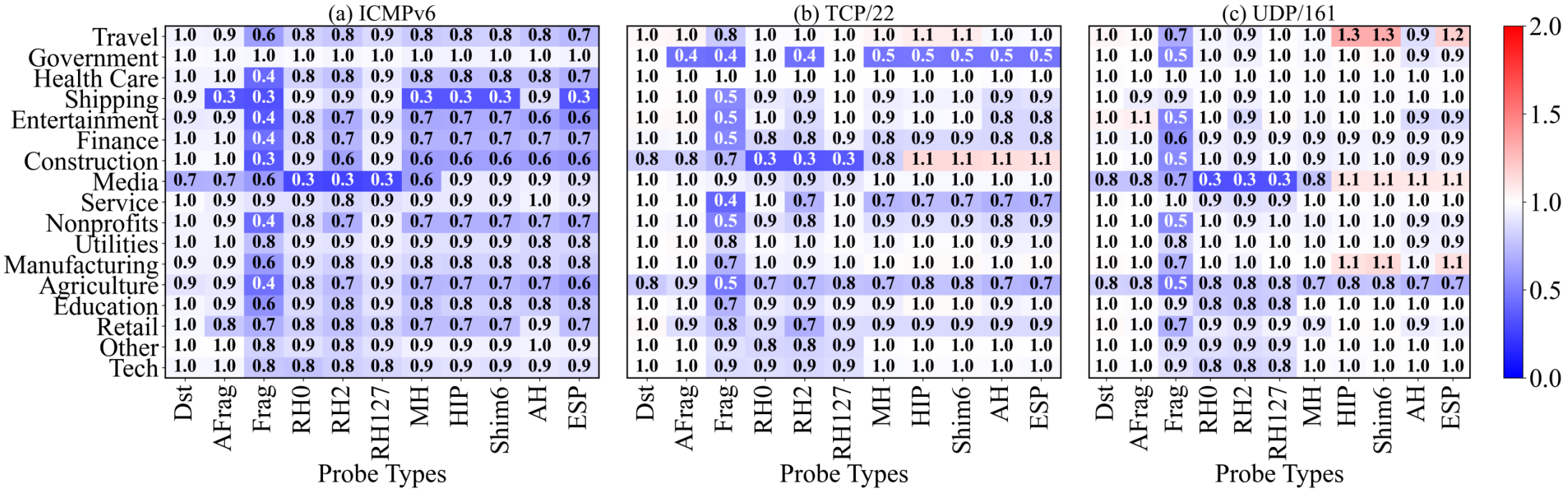
Deployment Implication

This suggests EH-based technologies (Mobile IPv6, IPsec, SRv6) can be reachable end-to-end on current paths.

Expanded Attack Surface

The same reachability may also allow malicious EH packets to traverse networks, expanding the attack surface.

Results: Reachability (cont.)



EH-vs-baseline reachability by industry indicates two contrasting forms of policy ossification.

01. Availability-Oriented Ossification

Travel, Construction, Media, and Manufacturing fix permissive policies: some EHs exceed baseline under TCP/UDP, prioritizing uptime but enlarging the attack surface.

02. Security-Oriented Ossification

Government enforces strict TCP filtering for nearly all EHs: it secures the boundary but hinders IPv6 feature evolution. (Health Care is protocol-neutral, with minimal filtering.)

Results: Potential Bypassing

01. Adversarial Capabilities Enabled by EH Bypass

- **Firewall ACL Evasion: uninspected EHs may slip past ACLs that do not parse the EH chain.**
- **Covert Mapping: internal topology may be probed where standard scanners are blocked.**
- **Restricted Access: internal services (management, DBs) that block standard traffic may become reachable.**

02. Identification Methodology

A potential bypass is characterized by a discrepancy: standard probes are blocked (timeout/reset) while EH-tagged probes reach the same destination, indicating that EH inspection is absent.

- **Rule 1:** The EH-free probe type receives a DU_{addr}, whereas the EH-carrying probe type successfully receives a PP_{dst} or $Resp$.
- **Rule 2:** The EH-free probe type receives a DU_{port}, whereas the EH-carrying probe type successfully receives a $Resp$.
- **Rule 3:** The EH-free probe type is denied access with a DU_{deny}, while the EH-carrying probe type successfully receives DU_{addr}, DU_{port}, PP_{dst} or $Resp$.
- **Rule 4:** The EH-free probe type is silently discarded (receive a TE), but the EH-carrying probe type successfully receives DU_{addr}, DU_{port}, PP_{dst} or $Resp$.

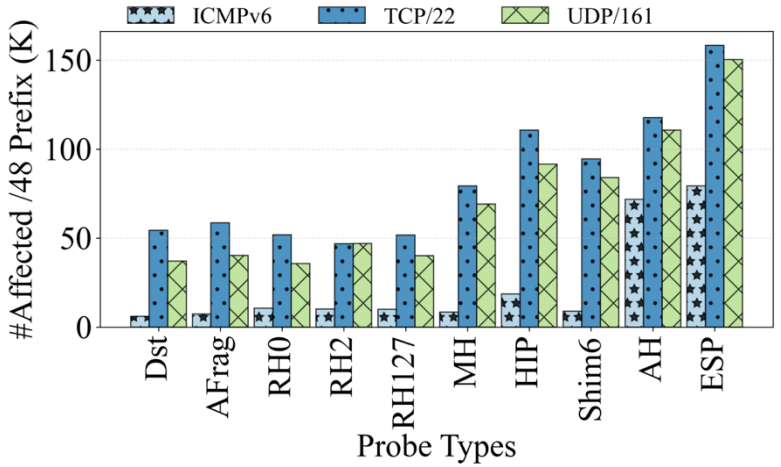
Results: Potential Bypassing (cont.)

IC	ICMPv6		TCP/22		UDP/161	
	#/48 Prefix	#AS	#/48 Prefix	#AS	#/48 Prefix	#AS
Agriculture	3 (0.2%)	2 (1.6%)	79 (4.2%)	17 (14.2%)	78 (4.1%)	16 (13.3%)
Nonprofits	18 (0.5%)	14 (2.8%)	248 (7.0%)	81 (16.5%)	207 (5.8%)	77 (15.7%)
Tech	93,005 (1.6%)	985 (5.9%)	210,516 (3.7%)	4,046 (24.3%)	187,933 (3.4%)	3,658 (22.0%)
Construction	10 (0.1%)	9 (1.5%)	216 (2.5%)	104 (17.5%)	157 (1.8%)	84 (14.2%)
Education	65 (0.7%)	28 (2.6%)	822 (9.1%)	211 (19.5%)	853 (9.4%)	185 (17.0%)
Finance	16 (0.2%)	11 (2.7%)	198 (2.4%)	55 (13.7%)	131 (1.6%)	47 (11.6%)
Shipping	10 (0.0%)	7 (3.3%)	76 (0.1%)	36 (17.0%)	56 (0.0%)	31 (14.8%)
Government	36 (0.0%)	10 (2.1%)	204 (0.1%)	67 (14.3%)	181 (0.1%)	60 (12.9%)
Health Care	3 (0.4%)	2 (1.1%)	85 (10.5%)	25 (13.4%)	77 (9.6%)	29 (15.9%)
Manufacturing	51 (1.2%)	12 (2.2%)	636 (13.9%)	92 (16.9%)	537 (12.1%)	64 (11.7%)
Media	2,293 (2.3%)	42 (3.7%)	13,690 (14.4%)	254 (22.5%)	9,915 (10.5%)	210 (18.7%)
Entertainment	5 (0.5%)	4 (2.3%)	66 (6.7%)	21 (12.3%)	50 (5.1%)	16 (9.2%)
Other	394 (0.2%)	103 (2.9%)	7,100 (2.8%)	435 (12.4%)	6,014 (2.4%)	385 (10.9%)
Retail	1,398 (0.6%)	39 (3.1%)	5,306 (2.4%)	222 (17.5%)	2,037 (0.9%)	170 (13.5%)
Service	241 (0.0%)	50 (2.6%)	4,141 (0.8%)	338 (17.7%)	929 (0.2%)	277 (14.5%)
Travel	6 (0.9%)	4 (2.7%)	61 (9.2%)	18 (12.4%)	25 (4.2%)	11 (7.6%)
Utilities	7 (0.4%)	5 (3.0%)	94 (5.7%)	30 (18.2%)	75 (4.6%)	19 (11.4%)
Total	93,630 (1.6%)	1,154 (4.9%)	218,954 (3.7%)	4,961 (21.1%)	195,175 (3.4%)	4,468 (19.0%)

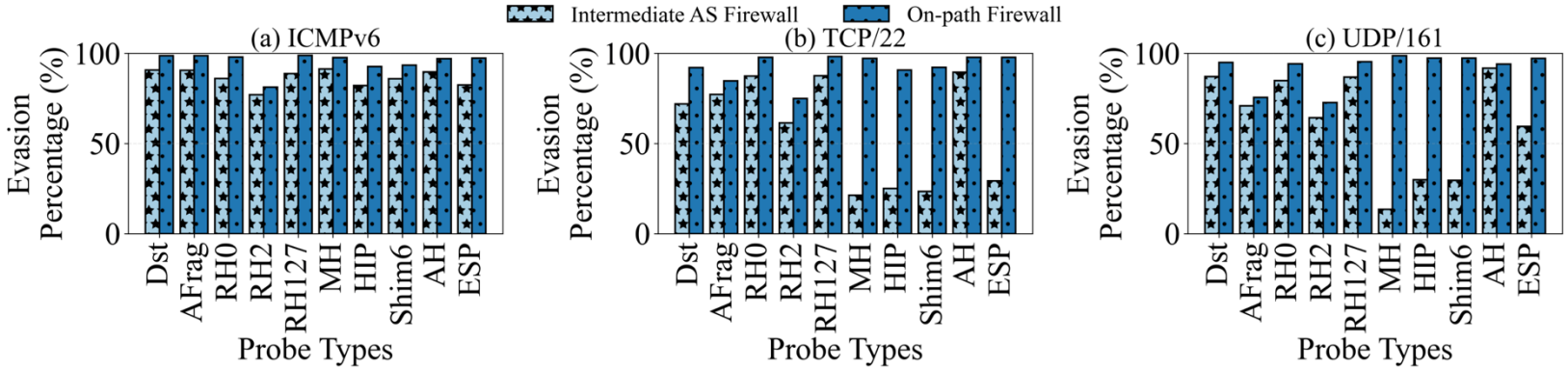
Scale of Affected Networks

1. ≈5,000 ASes exhibit bypass signatures
2. Protocol-specific risk profile
3. Cross-industry, global reach

Results: Security Issues



Affected Prefix Distribution by EH Type



Geographic Distribution of Bypass Points

Potential Root Causes

- Implementation Defects: firmware bugs may cause faulty EH parsing.
- Security Misconfigurations: overly permissive defaults, no explicit EH rules.
- Protocol Blind Spots: rare EH types may be implicitly allowed by legacy ACLs [RFC8200].

Results: Security Case Study

Case: An Observed Campus Network

Infrastructure Setup
Two edge routers (Juniper & H3C) at the perimeter — first line between the Internet and internal subnets.

Security Policy Objective
SSH management restricted to internal IPs; external SSH should be blocked at the edge firewall.

Critical Vulnerability Root Cause
The firewall inspects only the first Next Header; when it is not TCP/UDP, the packet is permitted. Prepending an EH (e.g., HbH) conceals the inner TCP/SSH payload.

Attack Vector: Extension Header Bypass Flow

01. Malicious Packet Forging
A packet is crafted with a non-TCP/UDP EH (e.g., HbH) as the first Next Header, concealing the TCP/SSH payload behind it.

02. Firewall Blind Spot
The firewall observes a non-TCP/UDP value in the first Next Header and forwards the packet without DPI.

03. Unauthorized Access
The internal host strips the EH and processes the embedded SSH request, permitting unauthorized management access.

Recommendations

Inspect the Full EH Chain

Deep Packet Inspection
Parse the full EH chain to identify the upper-layer protocol before applying ACLs; note the DoS risk from many/large EHs.

Selective EH Filtering
Limit the type, length, and number of permitted EHs; filter EHs unnecessary for operations, per RFC 9288.

Balance Security and Function

Layered Approach
For permitted EHs, apply DPI for transport-layer rule matching — reduces evasion while preserving legitimate EH use.

Outright Blocking
Blocking all EHs prevents evasion but hinders EH deployment and long-term network evolution.

Goal: mitigate EH-based evasion without foreclosing IPv6 evolution.

Q&A

draft-zedongjia-v6ops-ipv6eh-measurement