IPv6 Operations
Internet-Draft
Intended status: Informational
Expires: 3 December 2026

L. He
Z. Jia
L. Gai
Tsinghua University
S. Zhang
Nankai University
Y. Liu
Tsinghua University

1 June 2026

Observations on the Reachability and Evasion of Packets with IPv6 Extension Headers on the Internet
draft-zedongjia-v6ops-ipv6eh-measurement-00

Abstract

IPv6 Extension Headers (EHs) are designed to provide protocol flexibility and support for emerging features, while maintaining a concise base header and efficient processing. However, their practical reachability has long been constrained by widespread middlebox interference, and paradoxically, their flexibility introduces significant security risks.

This document presents observations from a comprehensive, large-scale measurement study of IPv6 Extension Header path traversal across more than 23,000 autonomous systems. Using a feedback-driven measurement framework called 6Travel, we measure the reachability of 10 common IPv6 Extension Headers over ICMPv6, TCP, and UDP. Our analysis reveals a fundamental shift: contrary to past observations of heavy filtering, specific Extension Headers now achieve reachability comparable to plain traffic. We further identify two distinct forms of policy ossification across industry categories and expose a widespread Extension-Header-based firewall evasion vulnerability affecting nearly 5,000 autonomous systems, particularly under TCP and UDP. This threat stems from a dual failure of implementation flaws and security misconfigurations, spanning both on-path and host-side firewalls.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ZedongJia.github.io/draft-zedongjia-v6ops-ipv6eh-measurement/draft-zedongjia-v6ops-ipv6eh-measurement.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-zedongjia-v6ops-ipv6eh-measurement/.

Discussion of this document takes place on the IPv6 Operations Working Group mailing list (mailto:v6ops@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/v6ops/. Subscribe at https://www.ietf.org/mailman/listinfo/v6ops/.

Source for this draft and an issue tracker can be found at https://github.com/ZedongJia/draft-zedongjia-v6ops-ipv6eh-measurement.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IPv6 has been widely deployed around the world as an alternative to IPv4. A notable feature of IPv6 is the introduction of Extension Headers (EHs) [RFC7045] [RFC8200]. Located between the IPv6 base header and the upper-layer protocol header, EHs provide IPv6 with a high degree of flexibility, scalability, and support for new core functions of the protocol, while maintaining the simplicity of the base header and efficient processing. These EHs have been widely applied in various aspects, including Mobile IPv6 (MIPv6) [RFC6275], Segment Routing over IPv6 (SRv6) [RFC8754] [RFC9256], In-band Operations, Administration, and Maintenance (IOAM) [RFC9197], and IPSec [RFC4302] [RFC4303].

Given the increasingly widespread adoption of EHs, characterizing their reachability has become paramount. Researchers have extensively investigated their path traversal capabilities [RFC7872] [Huston-2022] [Custura2024] [JAMES] [FishNet]. Collectively, these studies reveal that IPv6 packets carrying EHs experience

significantly higher drop rates compared to plain IPv6 traffic, highlighting a fragmented and often restrictive deployment landscape across the global Internet.

However, these studies remain limited in providing a comprehensive understanding of EH reachability. Prior work has not analyzed the full spectrum of common EHs while achieving extensive Autonomous System (AS) coverage. Existing studies typically rely on serial traceroute tools or end-to-end measurements, which suffer from substantial resource overhead, limited measurement integrity, and constrained observation scope.

Despite their importance, the processing of EHs introduces significant security challenges [RFC9098] [RFC9099]. IPv6 requires all EHs to be processed to identify upper-layer protocols, which allows attackers to evade firewalls and packet filters that improperly handle or overlook inserted EHs during security enforcement [Atlasis2016] [RFC7112] [FragEvasion]. Moreover, specific EH types harbor inherent architectural flaws exploitable for targeted attacks, such as amplification [RFC5095], overlapping fragment evasion [RFC5722], processing of atomic fragments [RFC6946], information leakage [RFC7739], and Denial of Service (DoS) attacks [RFC8021].

Motivated by these observations, we conduct a comprehensive, large-scale measurement study of EH path traversal using 6Travel [_6Travel], a feedback-driven measurement framework. Our measurements cover 6.3 million /48 prefixes across more than 23,000 ASes, evaluating 10 common EHs over ICMPv6, TCP, and UDP. The key findings are summarized as follows:

* *EH Path Traversal Capability:* Specific EHs, notably the Destination Options header and the Atomic Fragment header, now achieve reachability comparable to plain traffic under TCP and UDP, contrary to historical observations of heavy filtering. This signifies an evolving IPv6 infrastructure that enables practical deployment of EH-based applications but simultaneously expands the attack surface.

* *Policy Ossification:* We identify two counter-posed forms of policy ossification across industry categories: (i) Availability-oriented ossification, which prioritizes utility at the expense of an expanded attack surface; and (ii) Security-oriented ossification, which secures the boundary but hinders IPv6 architectural evolution through rigid filtering.

* *EH-based Firewall Evasion:* We expose a widespread firewall evasion vulnerability affecting nearly 5,000 ASes, particularly under TCP and UDP. This vulnerability stems from implementation flaws (e.g., protocol blind spots for less common EHs, over-permissiveness for IPSec) and security misconfigurations (e.g., neglecting to parse EHs), spanning both on-path and host-side firewalls.

This document is organized as follows. Section 3 provides background on IPv6 Extension Headers. Section 4 describes the measurement methodology. Section 5 presents observations on EH path traversal capability. Section 6 presents observations on EH-based firewall evasion. Section 7 discusses security considerations. Appendix A and Appendix B provide supplementary information on ethical considerations and measurement caveats, respectively.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. IPv6 Extension Headers

Extension Headers are optional headers that may appear between the IPv6 base header and the transport layer. They are designed to extend the functionality of IPv6 packets without requiring modifications to the base header. All EHs include a Next Header field, which chains EHs together. Through this chaining mechanism, an IPv6 packet can include zero or more EHs, each serving different functional requirements.

[RFC8200] and the Internet Assigned Numbers Authority (IANA) [IANA-EH] have defined the following EHs:

* *Hop-by-Hop Options header:* Designed to carry optional information that must be examined by every node along a packet’s delivery path. Recent updates to its processing procedures are specified in [RFC9673].

* *Destination Options header:* Designed to carry optional information that need be examined only by a packet’s destination node(s). Used for purposes such as collecting measurement data [RFC9197] and measuring service performance [RFC8250].

* *Routing header:* Similar to IPv4's Loose Source and Record Route option, used in scenarios where packets need to visit one or more intermediate nodes. Specific types include the RPL Routing header [RFC6554], the Segment Routing Header (SRH) [RFC8754], and the Mobile IPv6 Routing header (type 2) [RFC6275].

* *Fragment header:* Essential for IPv6 fragmentation capability when transmitting large packets (e.g., DNS responses).

* *Encapsulating Security Payload (ESP) [RFC4303] and Authentication Header (AH) [RFC4302]:* Used in IPSec to provide data confidentiality, data integrity, and data authentication.

* *Mobility header:* Used for managing mobile node mobility in IPv6 networks [RFC6275].

* *Host Identity Protocol (HIP) header [RFC7401] and Shim6 Protocol header [RFC5533]:* Designed for locator/identifier separation and multi-homing support, respectively.

4. Measurement Methodology

This section describes the measurement methodology employed in this study, including the measurement framework, address dataset, and the selection of EHs and upper-layer protocols.

4.1. Measurement Framework

We use 6Travel [_6Travel], a feedback-driven measurement framework designed for large-scale EH path traversal measurement. The framework employs a hybrid approach that integrates traceroute-based and end-to-end methods to assess the traversal capability of crafted probe packets. Specifically, 6Travel first attempts end-to-end probing for each target; if no response confirming destination arrival is received, it conducts adaptive probing to locate the last responsive node along the path. All probe types (i.e., packets with different EHs) are measured in parallel using a pipelined scheduling mechanism, ensuring near-simultaneous probing that minimizes temporal lag between different probe types and enables rigorous comparative analysis.

The framework incorporates a global and local rate control strategy to mitigate the impact of ICMPv6 rate limiting while maximizing probing efficiency. It also includes a packet marking mechanism and path-change validation to ensure measurement consistency.

6Travel is open-source and publicly available at https://anonymous.4open.science/r/6Travel (https://anonymous.4open.science/r/6Travel).

4.2. Measurement Setup

We conduct the EH path traversal measurement in an education network with a single vantage point (VP). The network is confirmed to have no enforced access control policies on all EHs. The VP is equipped with a 24-core Intel(R) Xeon(R) CPU E5-2620 v3 and 64 GB of RAM.

We empirically set a timeout of 5 seconds for each probe to ensure sufficient time for responses. To mitigate the impact of ICMPv6 rate limiting and reduce the probing burden on target networks, we randomize the probing address list before each measurement round. Additionally, to minimize interference with both the local and target networks, we set the hop limits to 8--30. The probing rate is configured to 50,000 packets per second.

4.3. Address Dataset

To ensure a representative and large-scale perspective, we aggregate target addresses from three complementary sources, as detailed in Table 1.

Source	Description	# /48 Prefixes	# ASes	# Industry Categories
Source 1	IPv6 Hitlist (responsive hosts across diverse networks)	581,098	22,221	17
Source 2	AddrProbe (active target discovery for unseeded ASes)	1,485,873	2,158	17
Source 3	IPv6 Observatory (passive NTP traffic, prefix-level)	5,177,906	13,217	17
Total		*6,336,433*	*23,999*	*17*

Table 1: Details of three data sources

Source 1 uses the IPv6 Hitlist as a broad baseline of responsive hosts. Source 2 leverages AddrProbe [AddrProbe]'s pattern-learning capabilities to discover active targets in ASes lacking known active IPv6 addresses. Source 3 incorporates passive NTP traffic from the IPv6 Observatory [IPv6-Observatory] to capture hosts typically invisible to active probing.

Since access control policies for EHs are typically enforced at the prefix level rather than on individual hosts, we adopt prefix-level sampling by randomly selecting one address within each /48 prefix. The /48 prefix length represents the shortest globally routable prefix length commonly announced in the BGP system. Industry categories are determined using ASdb [ASdb].

4.4. Selection of EHs and Upper-layer Protocols

To evaluate the path traversal capability of EHs, we select the EHs depicted in Table 2, covering six application scenarios: data transmission (AFrag, Frag), secure communication (AH, ESP), Mobile IPv6 (RH2, MH), site multi-homing (HIP, Shim6), new Routing header type (RH127), and general function extension (Dst).

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].
Host Identity Protocol header (type 1)	HIP	48	All fields are set according to [RFC7401].
Shim6 Protocol header	Shim6	8	All fields are set according to [RFC5533].

Table 2: EHs measured

For each EH, the probe is constructed by adding the EH between the IPv6 base header and the upper-layer protocol header. The upper-layer protocols measured are ICMPv6, TCP/22 (SSH), and UDP/161 (SNMPv3).

Although our measurement vantage point does not explicitly block the Hop-by-Hop Options header, we observed that packets carrying it are dropped by default, likely due to default router configurations. Given that previous large-scale studies have consistently reported extremely poor reachability for the Hop-by-Hop Options header [RFC7872] [Huston-2022] [Custura2024] [JAMES] [FishNet], we exclude it from our path traversal measurements as its limited reachability is already well-documented.

5. Observations on EH Path Traversal

We conducted a comprehensive path traversal measurement across all combinations of EHs and upper-layer protocols. To ensure data quality, we apply a filtering process to identify and discard /48 prefixes exhibiting path changes during probing. Table 3 summarizes the filtered dataset.

Protocol	Unchanged /48 Prefixes	Rate	# ASes
ICMPv6	6,020,231	95.13%	23,572
TCP/22	5,963,940	94.24%	23,525
UDP/161	5,824,972	92.04%	23,509

Table 3: Number of /48 prefixes with path unchanged observed in probing results

5.1. Destination AS Reachability

We evaluate the destination AS reachability rate, defined as the proportion of /48 prefixes for which probes successfully reach their respective destination AS out of the total set of probed prefixes. The baseline represents EH-free probes per protocol. Table 4 presents the results for each EH across protocols.

EH	ICMPv6 (%)	TCP/22 (%)	UDP/161 (%)
Baseline	80.18	70.55	69.58
Dst	77.49	70.08	68.68
AFrag	77.68	70.28	69.02
Frag	63.00	61.86	61.40
RH0	62.01	59.40	58.29
RH2	65.56	58.80	58.26
RH127	67.32	60.24	58.92
MH	69.84	69.62	68.90
HIP	70.96	70.87	67.80
Shim6	70.18	70.00	69.54
AH	72.27	70.56	69.76
ESP	70.38	70.85	70.29

Table 4: Destination AS reachability rate for each EH across protocols compared to baseline

Our results reveal several critical insights:

Dst and AFrag achieve reachability comparable to the baseline, while Frag experiences significant drops (7.6%--14.8%), undermining the utility of fragmentation-dependent services such as DNSSEC.

Routing headers (RHs) exhibit consistently low reachability, with RH2 and RH127 being largely suppressed under TCP/UDP despite moderate ICMPv6 reachability. This pattern suggests a diagnostic-only tolerance, where network operators may relax filtering for ICMPv6 to preserve basic connectivity, while enforcing stricter policies on TCP/UDP.

A protocol-dependent disparity emerges for MH, HIP, Shim6, AH, and ESP. While these headers fall 7.9%--10.4% below the baseline under ICMPv6, they remain consistently within 2% of the baseline under TCP/UDP, with AH and ESP occasionally even exceeding it. This shift

suggests that these headers benefit from permissive inspection policies or preferential treatment (e.g., whitelisting of encrypted-like traffic).

These findings indicate a maturing IPv6 infrastructure where specific EHs have transitioned from high drop rates to near-parity with plain traffic. While this enables the practical deployment of EH-based applications (e.g., MIPv6, IPSec), it simultaneously expands the network attack surface for EH-based exploits.

5.2. Reachability Across Industry Categories

To dissect the security-reachability tradeoff across diverse network environments, we categorize the results by industry category (IC) for each /48 prefix.

The following tables display the ratio of destination AS reachability for EH-carrying probes relative to the EH-free baseline within each industry category. The ratio is calculated as R_EH / R_Baseline. Values of 1.0 denote parity with the baseline, while values <1.0 and >1.0 indicate EH-induced filtering and potential evasion, respectively. A /48 prefix is counted multiple times if it belongs to multiple industry categories.

IC	Dst	AFrag	Frag	RH0	RH2	RH127	MH	HIP	Shim6	AH	ESP
Tech	0.97	0.97	0.78	0.77	0.82	0.84	0.87	0.88	0.87	0.90	0.88
Other	0.99	0.99	0.83	0.88	0.84	0.88	0.94	0.94	0.94	0.95	0.94
Retail	0.98	0.78	0.69	0.82	0.77	0.83	0.75	0.74	0.75	0.92	0.74
Education	0.97	0.93	0.58	0.86	0.78	0.89	0.78	0.82	0.82	0.80	0.76
Agriculture	0.90	0.91	0.45	0.83	0.74	0.87	0.71	0.72	0.72	0.68	0.64
Manufacturing	0.95	0.94	0.61	0.87	0.81	0.90	0.84	0.83	0.83	0.84	0.80
Utilities	0.95	0.95	0.76	0.90	0.89	0.94	0.88	0.88	0.88	0.85	0.84
Nonprofits	0.96	0.95	0.43	0.84	0.69	0.93	0.69	0.69	0.69	0.73	0.67
Service	0.98	0.93	0.89	0.89	0.85	0.89	0.91	0.91	0.91	0.95	0.91
Media	0.69	0.70	0.61	0.29	0.27	0.29	0.62	0.91	0.91	0.93	0.89
Construction	0.97	0.97	0.35	0.89	0.64	0.93	0.62	0.63	0.63	0.62	0.60
Finance	0.96	0.95	0.44	0.84	0.72	0.92	0.70	0.70	0.70	0.73	0.70
Entertainment	0.91	0.93	0.35	0.82	0.67	0.88	0.66	0.67	0.67	0.65	0.56
Shipping	0.95	0.34	0.31	0.93	0.87	0.94	0.34	0.34	0.34	0.88	0.34
Health Care	0.96	0.96	0.42	0.84	0.77	0.91	0.76	0.76	0.76	0.76	0.69
Government	0.98	0.97	0.96	0.98	0.96	0.98	0.96	0.96	0.96	0.96	0.96
Travel	0.96	0.94	0.62	0.83	0.78	0.86	0.80	0.81	0.81	0.77	0.72

Table 5: Relative destination AS reachability under ICMPv6 by industry category

IC	Dst	AFrag	Frag	RH0	RH2	RH127	MH	HIP	Shim6	AH	ESP
Tech	1.00	1.00	0.86	0.87	0.85	0.87	0.98	0.98	0.98	0.98	0.98
Other	0.99	1.00	0.88	0.84	0.83	0.85	0.99	1.01	0.99	1.00	1.01
Retail	1.03	0.87	0.78	0.85	0.68	0.86	0.86	0.86	0.86	0.85	0.86
Education	1.00	0.97	0.70	0.92	0.88	0.94	0.93	1.02	1.02	0.94	0.96
Agriculture	0.79	0.86	0.48	0.75	0.72	0.76	0.74	0.77	0.77	0.72	0.70
Manufacturing	0.99	0.99	0.70	0.96	0.94	0.97	1.01	1.02	1.02	0.98	1.02
Utilities	1.01	1.02	0.85	0.98	0.96	0.99	0.97	0.99	0.99	0.95	0.96
Nonprofits	0.99	0.97	0.51	0.89	0.83	0.97	0.87	0.88	0.88	0.85	0.86
Service	1.00	1.00	0.40	0.97	0.70	0.97	0.71	0.73	0.73	0.69	0.70
Media	1.00	0.98	0.95	0.90	0.86	0.90	0.97	0.97	0.97	0.97	0.97
Construction	0.82	0.82	0.72	0.34	0.34	0.35	0.82	1.15	1.15	1.13	1.12
Finance	0.97	0.97	0.53	0.84	0.82	0.94	0.84	0.85	0.86	0.85	0.85
Entertainment	1.02	1.03	0.51	0.96	0.86	1.00	0.94	0.98	0.98	0.85	0.85
Shipping	1.01	1.01	0.54	0.92	0.88	0.99	0.93	0.96	0.96	0.86	0.89
Health Care	0.99	1.00	1.00	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
Government	1.00	0.44	0.43	0.98	0.44	1.00	0.46	0.46	0.46	0.46	0.46
Travel	1.03	1.03	0.79	0.98	0.98	1.01	1.04	1.07	1.07	0.97	0.98

Table 6: Relative destination AS reachability under TCP/22 by industry category

IC	Dst	AFrag	Frag	RH0	RH2	RH127	MH	HIP	Shim6	AH	ESP
Tech	0.99	0.99	0.88	0.84	0.84	0.84	0.99	0.97	1.00	1.00	1.01
Other	1.00	1.00	0.87	0.88	0.86	0.88	0.99	0.99	0.99	1.00	0.99
Retail	1.02	0.98	0.69	0.92	0.90	0.95	0.91	1.01	1.01	0.92	0.95
Education	1.00	0.99	0.91	0.80	0.79	0.80	1.00	1.00	1.00	0.99	1.00
Agriculture	0.82	0.82	0.47	0.78	0.79	0.80	0.75	0.77	0.78	0.72	0.70
Manufacturing	1.02	1.01	0.71	0.99	0.95	1.00	1.00	1.12	1.14	0.97	1.12
Utilities	1.01	1.00	0.84	0.97	0.98	0.99	0.97	0.99	0.99	0.94	0.94
Nonprofits	1.00	1.00	0.54	0.96	0.93	0.96	0.95	0.98	0.98	0.93	0.93
Service	0.99	0.99	0.96	0.89	0.87	0.89	0.99	0.99	0.99	0.99	0.99
Media	0.77	0.77	0.65	0.32	0.31	0.32	0.76	1.10	1.10	1.09	1.08
Construction	1.00	0.98	0.54	0.96	0.90	0.98	0.94	0.96	0.96	0.91	0.94
Finance	0.97	0.96	0.57	0.93	0.92	0.94	0.92	0.95	0.95	0.93	0.94
Entertainment	1.04	1.06	0.52	1.00	0.86	1.02	0.96	0.99	1.01	0.86	0.86
Shipping	0.99	0.93	0.91	0.99	0.94	0.99	0.98	0.99	0.98	0.98	0.99
Health Care	0.99	1.00	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
Government	1.01	1.01	0.53	0.96	0.95	1.00	0.98	1.01	1.02	0.90	0.93
Travel	1.03	1.02	0.67	0.97	0.94	1.00	0.97	1.33	1.33	0.87	1.18

Table 7: Relative destination AS reachability under UDP/161 by industry category

Our analysis reveals two distinct forms of policy ossification across industry categories:

Availability-oriented ossification: In industry categories like Travel, Construction, Media, and Manufacturing, reachability for certain EHs (e.g., MH, HIP, AH/ESP) significantly exceeds the baseline under TCP/UDP. This suggests a permissive ossification,

where inspection policies are fixed to prioritize service availability. While Media and Construction categories are generally permissive, they consistently suppress Routing headers, reflecting an ossified mitigation strategy against Routing header risks.

Security-oriented ossification: The Government category demonstrates a bifurcated ossification: it maintains reachability comparable to the baseline under ICMPv6 and UDP, yet enforces a strict filtering stance for almost all EHs under TCP, indicating a highly restrictive and legacy-driven security posture. This approach secures the boundary but hinders IPv6 architectural evolution through rigid filtering.

Protocol-neutral posture: The Health Care category maintains reachability consistently near the baseline across both TCP and UDP, reflecting minimal active filtering, suggesting a legacy of minimal middlebox interference.

6. Observations on EH-based Firewall Evasion

Building upon the measurement results presented in Section 5, several EHs exhibit destination reachability that exceeds the established baseline, indicating the presence of practical firewall evasion capability. This section presents a threat model, identifies threat scenarios, and quantifies the extent of firewall evasion observed.

6.1. Threat Model

We consider a remote adversary located outside the victim network, capable of crafting and sending arbitrary IPv6 packets, including those with EHs, from a controlled host. The adversary has no access to the firewall or end hosts and cannot compromise their implementations. Firewalls may be deployed either on-path or at end hosts.

In this context, firewall broadly refers to any middlebox or network device that enforces access control based on ACLs, including dedicated firewalls, border routers, and stateful appliances.

We assume a typical deployment where: (i) end hosts process supported EHs correctly and generate ICMPv6 Parameter Problem messages for unsupported EHs; (ii) the firewall is configured to allow legitimate TCP, UDP, and ICMPv6 traffic while attempting to block reconnaissance and unauthorized access; and (iii) the firewall may enforce access control only on ICMPv6, TCP, and UDP traffic without explicitly considering EHs, or improperly process packets carrying EHs.

The adversary's primary goals are to: (i) perform stealthy network reconnaissance to map hidden topologies and live hosts, and (ii) violate access-control policies by accessing internal services protected by firewalls.

6.2. Threat Scenarios

Building upon related work [IPv6-Vul] and validated through local proof-of-concept demonstrations (see Section 6.4.5), we identify two primary threat scenarios:

Scenario 1: Hidden Network Discovery. For EHs that require specific host-side processing support, an adversary can insert them into standard topology or host discovery probes (e.g., ICMPv6 Echo Request). These modified probes evade firewall filtering rules, allowing reconnaissance of otherwise hidden network topologies and hosts. The same technique can be combined with source address spoofing to launch reflection or amplification attacks.

Scenario 2: Unauthorized Access. For non-disruptive EHs (e.g., Destination Options header or Atomic Fragment header), an adversary can append them to otherwise legitimate TCP/UDP packets. These EHs are crafted so as not to interfere with the target's transport-layer protocol parsing, yet they cause firewalls to skip deep packet inspection, enabling unauthorized access to services that would otherwise be protected.

6.3. Identifying EH-based Firewall Evasion

To identify which EHs successfully evade firewalls, we compare the results of EH-carrying probes with those of EH-free probes. The design of 6Travel minimizes the time gap between EH-carrying and EH-free probing, and results affected by path changes are effectively detected and excluded.

We define the following response types:

Response Type	Notation
ICMPv6 Destination Unreachable (type 0, 2, 3)	DU_addr
ICMPv6 Destination Unreachable (type 4)	DU_port
ICMPv6 Destination Unreachable (type 1, 5, 6)	DU_deny
ICMPv6 Parameter Problem (from target)	PP_tgt
ICMPv6 Time Exceeded (code 0)	TE
ICMPv6 Echo Reply / TCP SYN-ACK or RST-ACK / SNMPv3 Response	Resp

Table 8: Response types and their notation

We define four rules to determine whether an EH-carrying probe type successfully evades a firewall:

* *Rule 1:* The EH-free probe type receives a DU_addr, whereas the EH-carrying probe type successfully receives a PP_tgt 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_tgt, or Resp.

* *Rule 4:* The EH-free probe type is silently discarded (receives a TE), but the EH-carrying probe type successfully receives DU_addr, DU_port, PP_tgt, or Resp.

For Rules 1--3, we can further identify the addresses of the firewall devices evaded via EHs by extracting information from the returned ICMPv6 Destination Unreachable messages.

6.4. Extent of Firewall Evasion

We quantify the number of affected /48 prefixes and ASes across different industry categories to evaluate the extent of firewall evasion.

6.4.1. Overall Impact

Protocol	# Affected /48 Prefixes	# Affected ASes
ICMPv6	93,630 (1.6%)	1,154 (4.9%)
TCP/22	218,954 (3.7%)	4,961 (21.1%)
UDP/161	195,175 (3.4%)	4,468 (19.0%)

Table 9: Overall impact of EH-based firewall evasion

While 93,630 /48 prefixes (1,154 ASes) are affected under ICMPv6, the impact nearly doubles under TCP/UDP, reaching 218,954 prefixes (4,961 ASes) for TCP and 195,175 prefixes (4,468 ASes) for UDP. This disparity aligns with the diagnostic-only nature of ICMPv6, where stricter, yet evadable, security policies are disproportionately focused on TCP/UDP.

6.4.2. Breakdown by EH Type

Table 10 presents the number of /48 prefixes affected by EH-based firewall evasion across different EH types and protocols.

EH	ICMPv6 (K)	TCP/22 (K)	UDP/161 (K)
Dst	6.0	54.4	37.0
AFrag	7.3	58.6	40.3
RH0	10.5	51.9	35.6
RH2	10.1	46.9	46.9
RH127	10.0	51.6	40.1
MH	8.4	79.3	69.1
HIP	18.6	110.6	91.5
Shim6	8.9	94.5	84.0
AH	71.7	117.7	110.6
ESP	79.3	158.2	150.2

Table 10: Number of /48 prefixes (in thousands) affected by EH-based firewall evasion across EH types

Evasion capabilities vary significantly across EH types, revealing diverse underlying causes:

* *AH and ESP* consistently exhibit the highest evasion rates, likely due to lenient inspection of IPSec-related traffic for service continuity.

* *MH, HIP, and Shim6* --- which are not defined in [RFC8200] --- show markedly higher evasion under TCP/UDP than Dst or RHs, suggesting that firewalls may fail to account for these less common headers, creating security blind spots.

* The spatial distribution of evaded firewalls further distinguishes these patterns: evasion predominantly occurs within intermediate ASes under ICMPv6, while this shifts toward destination ASes for MH, HIP, and Shim6 under TCP/UDP.

6.4.3. Breakdown by Industry Category

The following tables provide a breakdown of firewall evasion by industry category for each protocol. A /48 prefix or AS is counted multiple times if it belongs to multiple categories.

Industry Category	# Affected /48s	# Affected ASes
Agriculture	3 (0.2%)	2 (1.6%)
Nonprofits	18 (0.5%)	14 (2.8%)
Tech	93,005 (1.6%)	985 (5.9%)
Construction	10 (0.1%)	9 (1.5%)
Education	65 (0.7%)	28 (2.6%)
Finance	16 (0.2%)	11 (2.7%)
Shipping	10 (0.0%)	7 (3.3%)
Government	36 (0.0%)	10 (2.1%)
Health Care	3 (0.4%)	2 (1.1%)
Manufacturing	51 (1.2%)	12 (2.2%)
Media	2,293 (2.3%)	42 (3.7%)
Entertainment	5 (0.5%)	4 (2.3%)
Other	394 (0.2%)	103 (2.9%)
Retail	1,398 (0.6%)	39 (3.1%)
Service	241 (0.0%)	50 (2.6%)
Travel	6 (0.9%)	4 (2.7%)
Utilities	7 (0.4%)	5 (3.0%)
Total	*93,630 (1.6%)*	*1,154 (4.9%)*

Table 11: Firewall evasion under ICMPv6 by industry category

Industry Category	# Affected /48s	# Affected ASes
Agriculture	79 (4.2%)	17 (14.2%)
Nonprofits	248 (7.0%)	81 (16.5%)
Tech	210,516 (3.7%)	4,046 (24.3%)
Construction	216 (2.5%)	104 (17.5%)
Education	822 (9.1%)	211 (19.5%)
Finance	198 (2.4%)	55 (13.7%)
Shipping	76 (0.1%)	36 (17.0%)
Government	204 (0.1%)	67 (14.3%)
Health Care	85 (10.5%)	25 (13.4%)
Manufacturing	636 (13.9%)	92 (16.9%)
Media	13,690 (14.4%)	254 (22.5%)
Entertainment	66 (6.7%)	21 (12.3%)
Other	7,100 (2.8%)	435 (12.4%)
Retail	5,306 (2.4%)	222 (17.5%)
Service	4,141 (0.8%)	338 (17.7%)
Travel	61 (9.2%)	18 (12.4%)
Utilities	94 (5.7%)	30 (18.2%)
Total	*218,954 (3.7%)*	*4,961 (21.1%)*

Table 12: Firewall evasion under TCP/22 by industry category

Industry Category	# Affected /48s	# Affected ASes
Agriculture	78 (4.1%)	16 (13.3%)
Nonprofits	207 (5.8%)	77 (15.7%)
Tech	187,933 (3.4%)	3,658 (22.0%)
Construction	157 (1.8%)	84 (14.2%)
Education	853 (9.4%)	185 (17.0%)
Finance	131 (1.6%)	47 (11.6%)
Shipping	56 (0.0%)	31 (14.8%)
Government	181 (0.1%)	60 (12.9%)
Health Care	77 (9.6%)	29 (15.9%)
Manufacturing	537 (12.1%)	64 (11.7%)
Media	9,915 (10.5%)	210 (18.7%)
Entertainment	50 (5.1%)	16 (9.2%)
Other	6,014 (2.4%)	385 (10.9%)
Retail	2,037 (0.9%)	170 (13.5%)
Service	929 (0.2%)	277 (14.5%)
Travel	25 (4.2%)	11 (7.6%)
Utilities	75 (4.6%)	19 (11.4%)
Total	*195,175 (3.4%)*	*4,468 (19.0%)*

Table 13: Firewall evasion under UDP/161 by industry category

Industry-category-wise, the Tech category dominates the evasion landscape, followed by Media and Retail, which show significant susceptibility, particularly under TCP/UDP.

6.4.4. On-path vs. Host-side Evasion

Table 14 presents the spatial distribution of evaded firewalls across EH types and protocols. For each combination, we report the percentage of evaded firewalls located in intermediate ASes versus destination ASes, and the percentage of on-path versus host-side firewalls.

Protocol	EH	Intermediate AS (%)	Destination AS (%)	On-path (%)	Host-side (%)
ICMPv6	Dst	90.7	9.3	98.7	1.3
ICMPv6	AFrag	90.5	9.5	98.6	1.4
ICMPv6	RH0	86.0	14.0	97.8	2.2
ICMPv6	RH2	77.1	22.9	81.3	18.8
ICMPv6	RH127	88.8	11.3	98.8	1.3
ICMPv6	MH	91.4	8.6	97.5	2.5
ICMPv6	HIP	82.1	17.9	92.6	7.4
ICMPv6	Shim6	85.8	14.2	93.4	6.6
ICMPv6	AH	89.7	10.3	97.1	2.9
ICMPv6	ESP	82.4	17.6	97.3	2.7
TCP/22	Dst	71.8	28.2	92.0	8.0
TCP/22	AFrag	77.1	22.9	84.7	15.3
TCP/22	RH0	87.4	12.6	97.8	2.2
TCP/22	RH2	61.4	38.6	74.9	25.1
TCP/22	RH127	87.6	12.4	98.2	1.8
TCP/22	MH	21.3	78.7	97.2	2.8
TCP/22	HIP	25.1	74.9	90.6	9.4
TCP/22	Shim6	23.4	76.6	92.2	7.8

TCP/22	AH	89.5	10.5	97.7	2.3
TCP/22	ESP	29.2	70.8	97.8	2.2
UDP/161	Dst	87.1	12.9	94.8	5.2
UDP/161	AFrag	70.8	29.2	75.5	24.5
UDP/161	RH0	84.8	15.2	94.2	5.9
UDP/161	RH2	64.2	35.8	72.7	27.3
UDP/161	RH127	86.8	13.2	95.4	4.6
UDP/161	MH	13.4	86.6	98.6	1.4
UDP/161	HIP	29.8	70.2	97.3	2.7
UDP/161	Shim6	29.6	70.4	97.3	2.7
UDP/161	AH	91.7	8.3	94.0	6.0
UDP/161	ESP	59.5	40.5	97.2	2.8

Table 14: Spatial distribution of evaded firewalls across EH types and protocols

Several key patterns emerge from this analysis:

Evasion predominantly occurs within intermediate ASes under ICMPv6, with most EHs showing over 80% of evaded firewalls in intermediate ASes. However, this shifts dramatically for TCP/UDP: MH, HIP, and Shim6 exhibit 78.7%, 74.9%, and 76.6% destination AS evasion under TCP/22 respectively, potentially reflecting a deliberate policy to avoid disrupting TCP/UDP EH processing at the edge.

Conversely, evasion for Dst and AFrag remains concentrated in intermediate ASes (71.8% and 77.1% under TCP/22 respectively), possibly due to centralized upstream filtering that leaves downstream destination ASes exposed.

While most evaded firewalls are on-path, AFrag and RH2 exhibit a significant portion of host-side evasion (15.3% and 25.1% under TCP/22, 24.5% and 27.3% under UDP/161), underscoring a complex interplay between network-level and host-level security failures.

6.4.5. Real-world Examples

We conducted a small-scale test within a campus network and successfully identified firewall evasion issues on two ingress routers (Juniper MX 960 and H3C CR16K). After consulting with the campus network administrators, we learned that the evasion occurred because the ACLs on these routers are not configured for deep protocol inspection --- they only checked whether the IPv6 next header was TCP or UDP, and allowed all other types to pass. This allowed us to successfully establish connections to protected SSH services within the campus network by adding Dst and AFrag, effectively achieving unauthorized access. We also used other EHs (e.g., ESP) to discover live hosts and topology.

Prior work [IPv6-Vul] has measured firewalls on popular operating systems and confirmed that certain versions of FreeBSD firewalls can be evaded via two Atomic Fragment headers. These real-world examples provide additional validation for the reliability of our measurement results.

7. Security Considerations

This section discusses the security implications of the observations presented in this document.

7.1. EH-based Firewall Evasion

Our measurements reveal a widespread EH-based firewall evasion vulnerability affecting nearly 5,000 ASes. This vulnerability enables:

1. *Stealthy reconnaissance:* Attackers can use EH-carrying probes to discover hidden network topologies and live hosts that would otherwise be protected by firewalls.

2. *Unauthorized access:* Attackers can bypass access control policies by appending EHs to TCP/UDP packets, enabling access to internal services.

3. *Amplification of existing attacks:* EH-based evasion can be combined with other attack techniques, such as source address spoofing for reflection/amplification attacks.

The root causes of this vulnerability include:

* *Implementation flaws:* Firewalls may have protocol blind spots for EHs not defined in [RFC8200] (e.g., MH, HIP, Shim6), or over-permissive handling of IPSec-related EHs (AH, ESP).

* *Security misconfigurations:* Firewalls may be configured to inspect only the IPv6 next header field without parsing the full EH chain, effectively treating EH-carrying packets as non-TCP/non-UDP and allowing them to pass.

7.2. Attack Surface Expansion

The improved reachability of certain EHs, while beneficial for protocol evolution and application deployment, inadvertently expands the network attack surface. Coupled with known EH-based exploits [RFC7739] [RFC5095] [IPv6-Vul], this trend increases the potential for exploitation.

7.3. Recommendations

Several strategies can mitigate the firewall evasion issues observed with EHs:

1. *Enable deep packet inspection on firewalls:* Parse the full EH chain to identify the upper-layer protocol before applying access control rules. However, this may introduce a risk of DoS attacks if malicious probes with numerous or large EHs overwhelm processing capacity.

2. *Selective EH filtering:* Limit the type, length, and number of EHs allowed, filtering out EHs unnecessary for network operations, as recommended in [RFC9288].

3. *Layered approach:* For EHs that are permitted, apply deep packet inspection to enable transport-layer firewall rule matching. Such fine-grained, customized filtering can reduce evasion risks while preserving legitimate EH functionality.

4. *Outright blocking of EHs:* While this would prevent evasion, it would also hinder EH deployment and adoption, limiting long-term network evolution.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

9.2. Informative References

[AddrProbe]
Cheng, D., "AddrProbe: An Internet-Wide Active IPv6 Address Probing System With Limited Seeds", 2026, <https://doi.org/10.1109/TON.2025.3645923>.

[ASdb] Ziv, M., "ASdb: a system for classifying owners of autonomous systems", 2021, <https://doi.org/10.1145/3487552.3487853>.

[Atlasis2016]
Atlasis, A., "The Impact of Extension Headers on IPv6 Access Control Lists Real Life Use Cases", 2016, <https://troopers.de/media/filer_public/77/ad/77ad71b5-daea-441c-afb1-e14625ed11d0/tr16_aatlasis_the_impact_of_extension_headers_on_ipv6_access_control_lists.pdf>.

[Custura2024]
Custura, A., "Is it possible to extend IPv6?", 2024, <https://doi.org/10.1016/j.comcom.2023.10.006>.

[FishNet] Iurman, J. and B. Donnet, "The Razor’s Edge: IPv6 Extension Headers Survivability", 2025.

[FragEvasion]
Lin, B., "Research on Security Protection Evasion Mechanism Based on IPv6 Fragment Headers", 2024, <https://doi.org/10.1109/LCN60385.2024.10639756>.

[Huston-2022]
Huston, G. and J. Damas, "IPv6 Fragmentation and EH behaviours", 2022, <https://www.potaroo.net/presentations/2022-03-20-iepg-v6frag.pdf>.

[IANA-EH] IANA, "Internet Protocol Version 6 (IPv6) Parameters - IPv6 Extension Header Types", 2024, <https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml>.

[IPv6-Observatory] Rye, E. and D. Levin, "IPv6 Hitlists at Scale: Be Careful What You Wish For", 2023, <https://doi.org/10.1145/3603269.3604829>.

[IPv6-Vul] Bassetti, E., "Opening Pandora’s Packet: Expose IPv6 Implementations Vulnerabilities Using Differential Fuzzing", 2025, <https://doi.org/10.1007/978-3-031-95761-1_14>.

[JAMES] Las, R., Iurman, J., Vyncke, ., and B. Donnet, "Measuring IPv6 extension headers survivability with James", 2022, <https://doi.org/10.1145/3517745.3563019>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/rfc/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/rfc/rfc4303>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/rfc/rfc4443>.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/rfc/rfc5095>.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, DOI 10.17487/RFC5533, June 2009, <https://www.rfc-editor.org/rfc/rfc5533>.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, DOI 10.17487/RFC5722, December 2009, <https://www.rfc-editor.org/rfc/rfc5722>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/rfc/rfc6275>.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <https://www.rfc-editor.org/rfc/rfc6554>.

[RFC6946] Gont, F., "Processing of IPv6 "Atomic" Fragments", RFC 6946, DOI 10.17487/RFC6946, May 2013, <https://www.rfc-editor.org/rfc/rfc6946>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/rfc/rfc7045>.

[RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", RFC 7112, DOI 10.17487/RFC7112, January 2014, <https://www.rfc-editor.org/rfc/rfc7112>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/rfc/rfc7401>.

[RFC7739] Gont, F., "Security Implications of Predictable Fragment Identification Values", RFC 7739, DOI 10.17487/RFC7739, February 2016, <https://www.rfc-editor.org/rfc/rfc7739>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/rfc/rfc7872>.

[RFC8021] Gont, F., Liu, W., and T. Anderson, "Generation of IPv6 Atomic Fragments Considered Harmful", RFC 8021, DOI 10.17487/RFC8021, January 2017, <https://www.rfc-editor.org/rfc/rfc8021>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <https://www.rfc-editor.org/rfc/rfc8250>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/rfc/rfc9098>.

[RFC9099] Vyncke, ., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <https://www.rfc-editor.org/rfc/rfc9099>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/rfc/rfc9197>.

[RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <https://www.rfc-editor.org/rfc/rfc9256>.

[RFC9288] Gont, F. and W. Liu, "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers at Transit Routers", RFC 9288, DOI 10.17487/RFC9288, August 2022, <https://www.rfc-editor.org/rfc/rfc9288>.

[RFC9673] Hinden, R. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", RFC 9673, DOI 10.17487/RFC9673, October 2024, <https://www.rfc-editor.org/rfc/rfc9673>.

[_6Travel] Jia, Z., "6Travel: A Feedback-Driven Framework for IPv6 Extension Header Path Traversal Measurement", January 2026, <https://anonymous.4open.science/r/6Travel>.

Appendix A. Ethical Considerations

We strictly adhere to the ethical guidelines of network measurement and fully consider the measurement impact, benign probing, and anonymity.

Measurement Impact: In compliance with the standards outlined in [RFC4443], the number of packets sent to each target address is limited to one per second, and each probe is only sent once per hop. We distribute probes across multiple addresses by randomizing target

addresses, instead of repeatedly targeting a single address. Additionally, we impose an overall rate limit of 50K packets per second, which effectively reduces the impact on both the vantage point network and the target network.

Benign Probing: All probes are constructed using standard-compliant protocols. We do not exploit any vulnerabilities or craft malicious payloads. The probes do not carry harmful data, and the responses do not contain personally identifiable or sensitive information. For TCP/22, we perform only half-open probing without establishing full connections. For UDP/161, we send SNMPv3 Get Requests without any follow-up interaction.

Opt-out Mechanism: We maintain a public web portal providing our research identity and contact information. This allows network administrators to opt out of our scanning scope. To date, we have received no complaints or opt-out requests.

Anonymity: We do not publicly disclose raw IPv6 address details. We only report aggregated statistics and analysis results. The collected data is used solely for research purposes.

Disclosure: We have communicated with the administrators of a campus network and addressed the identified firewall evasion issues. For other ASes where potential firewall vulnerabilities were observed, we are actively contacting the relevant network operators to inform them of the findings.

Appendix B. Measurement Caveats

Our measurements are subject to several potential limitations that should be considered when interpreting the results.

Limited Response Visibility: Some destination ASes or hosts may not generate ICMPv6 responses, while others may process EHs without replying. Since our approach relies on responses from destination ASes or hosts, the absence of such responses may lead to underestimation of EH traversal capability. This limitation leads to conservative estimates rather than overestimation.

Single Vantage Point: Using a single vantage point may introduce measurement bias. Identifying vantage points with little or no EH filtering is challenging, as some ISPs filter even basic EHs. While absolute values may vary across vantage points, the observed trends and phenomena are unlikely to be artifacts of a specific vantage point.

One-Probe Measurement Noise: Each probe is sent only once to minimize impact on both the vantage point network and target networks. Packet loss and transient network fluctuations may affect a subset of the results, but such effects are inherently random and not systematically biased toward specific EH types.

Transient Host Dynamics: During parallel probing, some destination hosts may experience short-term changes in availability or port state. Our system incorporates mechanisms to identify and exclude unstable hosts, and this limitation does not materially impact the overall conclusions.

Appendix C. Reproducing the Measurements

The 6Travel measurement framework is open-source and publicly available at: https://anonymous.4open.science/r/6Travel (https://anonymous.4open.science/r/6Travel).

The address dataset and measurement results are also available at the same location. Researchers can use 6Travel to reproduce our measurements or conduct similar studies over time to observe changes in the handling of packets with IPv6 Extension Headers.

Acknowledgments

We would like to thank Daguo Cheng, Chentian Wei, Zhaoan Wang, Kun Guo, and Chenyi Liu for their contributions to this work. We also thank the network administrators who cooperated with our disclosure efforts and the reviewers who provided valuable feedback on earlier versions of this document.

Authors' Addresses

Lin He
Tsinghua University
Email: helin1170@gmail.com

Zedong Jia
Tsinghua University
Email: jzd25@mails.tsinghua.edu.cn

Le Gai
Tsinghua University
Email: gl25@mails.tsinghua.edu.cn

Shenglin Zhang
Nankai University
Email: zhangsl@nankai.edu.cn

Ying Liu
Tsinghua University
Email: liuying@cernet.edu.cn