IPFS over SCION: Secure and Performant Content Retrieval on Next-Generation Networks

Marten Gartner
Otto-von-Guericke University
Magdeburg, Germany
marten.gartner@ovgu.de

Leon Rinkel
Otto-von-Guericke University
Magdeburg, Germany
leon.rinkel@st.ovgu.de

David Hausheer
Otto-von-Guericke University
Magdeburg, Germany
hausheer@ovgu.de

***Abstract*—The InterPlanetary File System (IPFS) offers a decentralized, content-addressable storage model. Operating on today's Internet, IPFS inherits the fundamental security and performance limitations of the Border Gateway Protocol (BGP). SCION, a next-generation Internet architecture, provides a compelling solution by introducing path-aware networking (PAN), which grants endhosts fine-grained path control, multipath capabilities, and a robust security foundation. In this work, we enhance IPFS with a native SCION integration. We engineer a multipath transport into libp2p, the networking stack of IPFS, and leverage SCION's Control-Plane Public Key Infrastructure (CP-PKI) for cryptographic peer validation. Our comprehensive evaluation across a testbed and a production network demonstrates that our approach hardens IPFS against routing-based attacks while reducing content retrieval times by up to 2.9x. These findings validate path-aware networking as a potent foundation for securing and accelerating decentralized systems.**

***Index Terms*—Networks, path-aware networking, PAN, multipath, IPFS, SCION, peer-to-peer**

I. Introduction

Web services have become increasingly centralized in clouds with major platforms such as Amazon or Google. Although these providers run their services in clusters or even data centers, they are still representing a single point of failure. Outages of these providers have caused significant financial losses [4], initiating the rise of the *Decentralized Web*. The InterPlanetary File System (IPFS) [10] is a key part of this movement, offering a decentralized, content-addressable storage and retrieval system. IPFS has seen growing adoption and is now also integrated into web browsers such as Brave, making it a strong alternative to centralized web infrastructures. However, a fundamental architectural mismatch arises because decentralized systems like IPFS operate atop the current Internet, which is orchestrated by the Border Gateway Protocol (BGP) [6]. BGP's singlepath routing paradigm, based on opaque policies, results in potentially underutilized network capacity [28]. More critically, BGP lacks intrinsic security mechanisms, leaving it vulnerable to routing attacks such as prefix hijacking [9]. allowing to intercept a node's peer discovery requests, flooding it with malicious peers to sever its connection to the honest network in an eclipse attack [22]. While security extensions like Border Gateway Protocol Security (BGPsec) [20] exist, their limited adoption and scalability issues leave the problem largely unsolved [18].

To overcome these challenges, researchers have explored clean-slate Internet architectures that leverage untapped capacities while incorporating modern security principles [15], [32]. Among these, SCION (Scalability, Control, and Isolation on Next-Generation Networks) [11] stands out as one of the most widely deployed next-generation Internet architectures. SCION fundamentally enhances inter-domain routing by providing path awareness, path control, multipath routing, and improved security. Previous research on integrating SCION with BitTorrent [13] indicates the potential for performance gains. We follow-up on that research and a master thesis by Rinkel [23], by incorporating native SCION support into IPFS in order to support multipath communication between peers and cryptographic peer validation based on SCION's Control Plane Public Key Infrastructure (CPPKI). We evaluate our SCION-based IPFS approach with a security analysis including a simulation, performance experiments, and a real-world deployment in a production SCION network. Our key contributions are:

- A native multipath transport for IPFS, implemented by integrating SCION with QUIC in `libp2p` [3] and Kubo [2], including cryptographic peer validation.
- A comparative analysis of path selection strategies for IPFS over SCION.
- A comprehensive performance and security analysis of IPFS over SCION, conducted in a testbed and a production research network.

We demonstrate that our integration not only hardens IPFS against sybil attacks but also significantly accelerates content retrieval by leveraging path diversity.

978-3-903176-75-1

II. Background

In this section we explain the fundamentals of IPFS and the SCION Internet architecture.

A. InterPlanetary File System

The InterPlanetary File System is a peer-to-peer distributed file system designed for decentralization, efficiency, and resilience. Unlike HTTP, which locates content by address, IPFS uses cryptographic hashes called *Content IDs* (CIDs) for content addressing, ensuring integrity and availability across multiple nodes. IPFS combines *Distributed Hash Tables* (DHTs) for discovery, *Merkle Directed Acyclic Graphs* (Merkle DAGs) for structuring data, and the *BitSwap* protocol for efficient exchange. By eliminating reliance on centralized servers, IPFS enhances resilience, reduces redundancy through de-duplication, and ensures verifiable content integrity.

Bitswap [10], [24] is a peer-to-peer protocol to request and exchange IPFS data blocks. Bitswap manages block discovery and transfer by maintaining so called *Wantlists* of requested content. Connected peers respond to requests with availability or directly transfer requested data. Nodes broadcast *Want-Have* messages to discover providers, select peers based on past reliability, and request blocks using *Want-Block* messages while canceling duplicates to optimize bandwidth. Bitswap groups transfers into batches (envelopes) and aggregates parallel streams to optimize efficiency. libp2p [3] is a modular, open-source networking stack that handles transport, security, and routing, serving as the backbone of IPFS and its components such as Bitswap. libp2p abstracts networking complexities by supporting multiple transport protocols and using transport-independent peer IDs for consistent addressing.

B. SCION

The SCION Internet architecture [11] addresses the limitations of BGP by enhancing security, preventing hijacking attacks, and eliminating single points of trust by design. It enables multipath communication, allowing applications to use multiple end-to-end paths in parallel for improved reliability and control. SCION's packet-carried forwarding state (PCFS) embeds complete inter-domain paths in packet headers, providing fine-grained path control for endhosts and applications. SCION organizes *Autonomous Systems* (ASes) into *Isolation Domains* (ISDs), structured around geographic or regulatory boundaries. Each ISD has a set of *Core ASes*, which manages a cryptographic *Trust Root Configuration* (TRC) and issues control plane certificates for authentication, avoiding centralized trust vulnerabilities. The ISD core also exchanges path information across ISDs. SCION's control plane uses a distribution mechanism for path segments called *beaconing*, where SCION Core ASes periodically send *Path Construction Beacons* (PCBs) signed with control plane certificates. These beacons propagate through ASes, forming up, core, and down path segments. The data plane combines these segments and embeds complete paths in packets in an efficient way, removing the need for per-flow state in routers. SCION has three major deployments: SCIONLab [19], the SCION production network [29], and SCIERA [31]. SCIONLab is a research-focused network that enables experimentation with multipath communication between domains. The SCION production network, managed by Anapaya Systems, provides a secure and scalable infrastructure for commercial use. SCIERA, the SCION Education, Research and Academic Network operates its own native ISD ensuring high performance and secure global connectivity for over 20 research institutions.

III. SCION Integration in IPFS

Our primary goal is to integrate IPFS with SCION to enhance security and accelerate performance. This requires modifying the core networking layer of IPFS. Since the IPFS reference implementation, Kubo [2], relies on `libp2p` [3] for all network communication, our efforts focus on integrating SCION natively into `libp2p`. Additionally, since libp2p uses multiaddr [1], a self-describing address format, we first need to implement support for SCION multiaddresses. This process involves four key steps:

1) Defining a multiaddr format for SCION addresses.
2) Implementing a multipath-capable transport for SCION based on the existing QUIC transport.
3) Designing and implementing path selection strategies to intelligently distribute traffic over multiple paths.
4) Integrating peer validation using SCION's control-plane PKI.

Notably, our SCION transport is implemented as an additional, modular component within libp2p. This design ensures backward compatibility, allowing SCION-enabled nodes to communicate seamlessly with standard IPFS peers over conventional IP-based transports within a mixed network. Our evaluation assumes peers operate with stable, publicly reachable addresses, which simplifies connection establishment. However, the transport is designed to be compatible with real-world network conditions. In environments with network address translation (NAT), the transport can function, though peer discovery and direct connection may require standard libp2p mechanisms such as AutoNAT for hole punching, which are orthogonal to the SCION transport itself.

A. SCION Multiaddresses

`libp2p` uses multiaddr [1], a self-describing address format, to represent network endpoints. To support

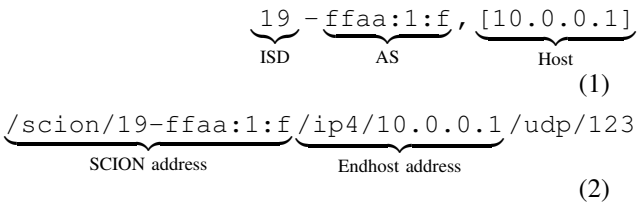

Fig. 1: A textual representation of a SCION address (1) and the resulting SCION Multiaddr format (2).

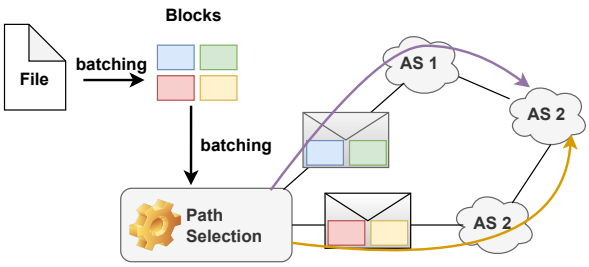

Fig. 2: Multipath content transfer in IPFS over multiple SCION paths.

SCION, we designed a new multiaddr format. A standard SCION address consists of an ISD-AS pair and a host address (e.g., an IP address). Our format, shown in Figure 1, separates these components. The '/scion/' component contains the ISD-AS identifier, and it encapsulates a subsequent multiaddr for the host, such as '/ip4/' or '/ip6/'.

B. Secure Multipath Transport

We introduce application-level multipath transport by extending `libp2p`'s QUIC implementation. QUIC is an ideal transport protocol due to its low-latency connection establishment, stream multiplexing, and robust congestion control. However, QUIC's congestion control algorithm assumes a relatively stable underlying path; to avoid RTT disruptions, our design pins each QUIC connection to a single, dedicated SCION path. To achieve multipath communication with a peer, we establish multiple parallel QUIC connections, one for each selected SCION path. This allows each connection's congestion controller to optimize for the specific characteristics of its path without interference. Upon initiating communication with a new peer, the transport queries the local SCION daemon to discover all available end-to-end paths. These paths are then cached for the duration of the session to minimize lookup overhead on subsequent connections. The transport layer manages this pool of connections, making them available to the Bitswap protocol for concurrent data transfer. Figure 2 depicts the process. The Bitswap server processes content requests by placing them in a priority queue. Worker threads then pull tasks from this queue, group them into batches called *envelopes* and send them concurrently over multiple paths. This concurrent dispatch mechanism provides the ideal point to schedule envelopes across the multiple available QUIC connections (and thus SCION paths).

C. Path Selection Strategies

Effectively utilizing multipath transport requires intelligent path selection. A poor choice of paths can lead to performance degradation. We leverage this information to implement a set of path selection strategies: The path selection strategies are as follows: (1) *Random* assigns paths randomly for each envelope, while (2) *Single shortest* uses the shortest available path for all transfers as a baseline comparison. The (3) *First free random* strategy selects the first available, unused path randomly; if none are free, it selects any path. (4) *First free lowest latency* chooses the first free path with the lowest latency based on static metadata, with a default of 0ms, and (5) *First free lowest lat. sub* is similar but with a default latency of 10 ms. The (6) *First free most disjoint* strategy prefers paths with minimal shared interface identifiers. (7) *First free shortest* selects the shortest available path that is not in use. Finally, (8) *First free highest bandw.* chooses the path with the highest estimated bandwidth based on metrics, with the shortest path as a fallback. Since each QUIC connection is pinned to a single SCION path, adaptive strategies like (8) do not cause instability; QUIC's congestion control on each path operates independently, preventing the rapid oscillations that could occur from switching an active stream between paths with different characteristics.

D. Peer Validation

Pervasive Internet-Wide Low-Latency Authentication (PILA) [5], [17] authenticates endhosts based on their addresses, offering a key advantage over name-based authentication (e.g., domain names): since all devices engaged in Internet-wide communication have an endhost address, they can seamlessly use PILA. Endhost certificates are issued by an AS and contain at least one SCION endhost address.

We provide the first PILA implementation for SCION [5] that allows hosts to obtain certificate chains for one or more SCION addresses, embedding them within the DNS names of the leaf certificate. This chain consists of three certificates: (1) The CA certificate of the issuing CA, (2) the AS certificate, and (3) the endhost certificate. With access to the relevant TRC, SCION entities can verify that (a) the full certificate chain is valid and (b) the peer's address matches one of the SCION addresses in the certificate. Validation involves ensuring that the

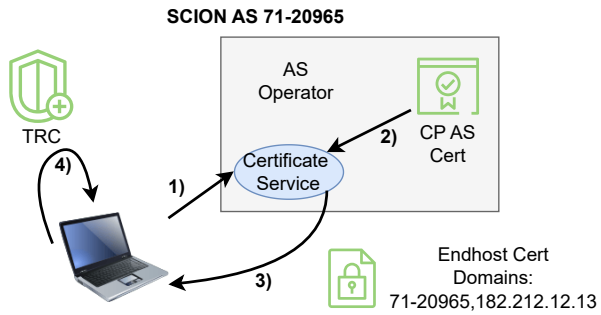

Fig. 3: SCION PILA Design: 1) Request Certificate, 2) Issue Certificate, 3) Return Certificate Chain, 4) Verify against TRC

AS certificate issued the leaf certificate and that the AS certificate itself is issued by a valid CA, which is authenticated against the TRC. Figure 3 depicts the certificate retrieval process. To obtain a certificate, the endhost sends a certificate request and the server verifies the request by checking the source IP to confirm that the endhost belongs to the AS. Upon validation, the server issues the endhost certificate via the AS certificate. The certificate chain is returned to the endhost, which verifies it against the ISD's TRC.

Libp2p itself already utilizes TLS 1.3 to secure peer-to-peer connections. During the handshake, the peers authenticate each other by embedding their public keys within a custom X.509 certificate extension. We integrate our authentication by adding another X.509 certificate chain to the TLS handshake and adapt the peer verification function without breaking existing authentication. While this second check adds computational overhead, this procedure is only done once per handshake and the peers authenticity status is cached for all subsequent communication over this connection.

IV. Security Analysis

Integrating IPFS with SCION provides inherent security advantages that mitigate several critical attack vectors present in today's Internet.

1) Mitigating Man-in-the-Middle (MitM) Attacks: In BGP, an adversary can perform a MitM attack by hijacking routes to intercept traffic. While IPFS's content hashing protects data integrity, the exchange of CIDs and provider records remains vulnerable. SCION's design prevents unauthorized route modifications, as all paths are explicitly chosen by the source and cryptographically verified at each hop. Combined with PILA-based authentication, this ensures that a peer is communicating with the intended node over a secure, untampered path.

2) Mitigating Sybil Attacks: In a Sybil attack, an adversary creates a large number of pseudonymous identities to gain disproportionate influence over the network. In IPFS, this can be used to poison DHT routing tables or eclipse honest nodes. SCION raises the cost of such attacks significantly. Each SCION AS must be cryptographically registered within its ISD, making it difficult to create fake ASes. Furthermore, PILA ties peer identities to these verifiable ASes, preventing an adversary from easily creating thousands of authenticated identities.

3) Mitigating Routing Attacks: BGP's vulnerability to prefix hijacking and route leaks allows attackers to redirect or blackhole traffic at a large scale. SCION eliminates this entire class of attacks. Path information is disseminated through the secure beaconing process and cannot be forged or announced illegitimately. Endhosts have full control and can select paths that avoid untrusted or malicious domains, guaranteeing that traffic follows authorized, verifiable routes.

4) Resilience to DDoS Attacks and Link Failures: SCION's native multipath capabilities provide enhanced resilience. If a path becomes unavailable due to a link failure or a DDoS attack, an endhost can immediately switch to an alternative, pre-validated path. SCION border routers can detect local link failures in milliseconds, enabling failover that is orders of magnitude faster than BGP's minutes-long convergence time [26]. The combination of path verification and PILA's certificate-based peer validation mitigates MitM, Sybil, and routing attacks while improving resistance to DDoS-induced disruptions.

V. Impact of Peer Validation on Sybil attacks

Our primary goal for this simulation is to evaluate the effectiveness of SCION-based peer validation in mitigating Sybil attacks. We designed a custom discrete-time event simulator to model an IPFS-like P2P network where a large fraction of nodes are malicious Sybil attackers attempting to perform an eclipse attack by poisoning the routing tables of honest peers. We generate the network topology based on the Barabási-Albert (BA) model [8], since it has been shown to accurately reflect the topological properties of many real-world P2P systems, namely the emergence of a scale-free, power-law degree distribution [21], commonly used for simulating the network environment for Kademlia-based systems.

Each node in the simulation is an object characterized by one of three roles: An *Honest Peer* is a legitimate network participant that follows the protocol correctly. An *Attacker Peer* is a malicious Sybil node controlled by an adversary. A *SCION Validator Peer* is an honest peer that has a cryptographically verifiable identity via SCION's CP-PKI, allowing other peers to trust it.

Each peer maintains a routing table, an abstraction of the k-buckets used in Kademlia-based DHTs like the one in IPFS with $k = 20$. Attacker node exclusively

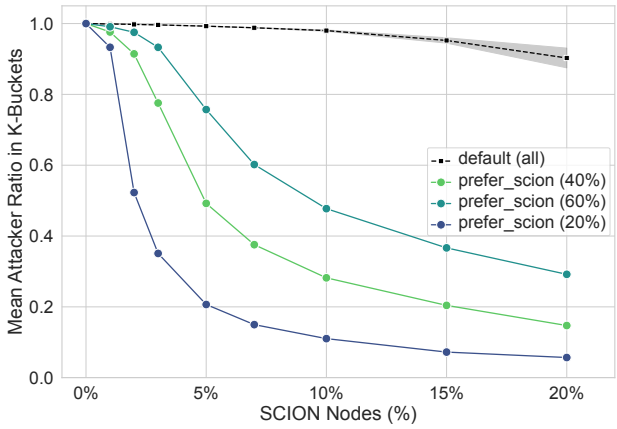

Fig. 4: Impact of SCION peer validation on Sybil attacks. The *mean attacker ratio* is defined as the average percentage of malicious peers in an honest node's routing table after the simulation converges.

returns a list of other known attacker nodes when being queried. A vulnerable honest peer, unable to distinguish these malicious responses, will unknowingly populate its routing table with adversaries. We model PILA-based authentication with a deterministic behavioral rule: An honest peer is considered *protected* if its routing table contains at least one SCION Validator. A protected peer can validate lookup responses and discard malicious responses. An *unprotected peer* (with no SCION validators in its table) will blindly accept all lookup responses. If a lookup response from an unknown peer contains a list of new peers, the protected node can query its known validator for a trusted list of honest peers. By cross-referencing, it can discard malicious entries from the untrusted response. We compare two routing table update policies: *Default*, where a new peer replaces a random entry in a full bucket, and *Prefer-SCION*, where a new SCION validator is preferentially kept, evicting a non-validator.

We simulate networks of up to $N = 10.000$ nodes with attacker populations from 20%-60%. Nodes are assigned roles based on the specified fractions and deployment strategy. The validator nodes are randomly selected uniformly from the list of honest nodes. The initial routing table of each node is populated with a random subset of its immediate neighbors in the graph. In each simulation step, every honest node performs one routing table refresh operation: it selects a random peer from its current table and performs a lookup. Based on the presence of a SCION validator in its table, the node either validates and potentially discards the lookup response, or blindly accepts it, before updating its routing table.

Figure 4 presents our simulation results. Validators using the *Default* update policy yielded only marginal improvements. For instance, in a network with 60% attackers, deploying even 20% SCION validators with this strategy still left honest nodes with routing tables over 90% polluted by attackers. This indicates that without an active retention mechanism, the protective effect of validators is quickly diluted by random network churn. A dramatic improvement is observed with the *Prefer-SCION* update strategy, which actively prioritizes keeping validator peers in the routing table. In the same 60% attacker scenario, the *Prefer-SCION* strategy reduced the attacker ratio to just 0.29 with a 20% validator deployment. Even under extreme threat levels (e.g., 60% attackers), the *Prefer-SCION* strategy significantly suppresses the attack's impact once a critical mass of validators ($> 10\%$) is deployed, whereas the passive *Default* strategy offers virtually no protection. In conclusion, our findings demonstrate that integrating SCION provides a foundational layer for security, but its full potential is only realized when the overlay P2P protocol is made aware of the underlying trust infrastructure. However, it is important to consider the trade-offs. The *Prefer-SCION* strategy, while highly effective, could introduce a centralizing tendency by prioritizing connections to validator nodes. As SCION adoption continues to grow, the pool of verifiable, trusted peers will expand organically. Consequently, the centralizing tendency of the *Prefer-SCION* strategy is expected to diminish, as honest nodes will have a much wider and more diverse set of validators to connect with.

VI. Performance Evaluation

Our performance evaluation of IPFS over SCION consists of an overhead analysis, an evaluation of path selection strategies in SCIONLab and a performance measurement in the SCIERA network. The primary goal of this evaluation is to perform a direct comparison of the network underlay (SCION vs. IP) and its impact on a real-world decentralized application.

A. Performance Evaluation in the SEED Emulator

First, we evaluate the computational overhead of IPFS over SCION compared to IP in an emulated environment. We deploy two ASes in the SEED Internet Emulator [12] connected via a single link, running both IP and SCION routing and each AS an IPFS node. We then conduct 100 repetitions of fetching a 100MB file, individually over SCION and BGP.

The results shown in Figure 5 indicate that SCION incurs only a minimal additional overhead, leading to an average increase of approximately 0.1 seconds in runtime. This aligns with our expectations, as SCION's additional header information and processing steps introduce a slight but manageable overhead (around 2%) when using

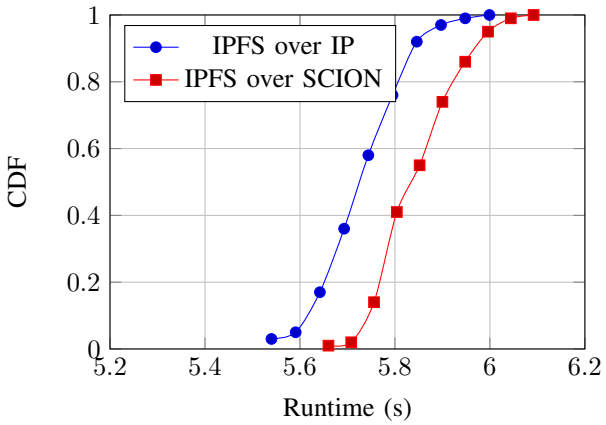

Fig. 5: CDF of 100 runs of `ipfs get` of 100 MiB data over a single inter-AS in an emulated setup.

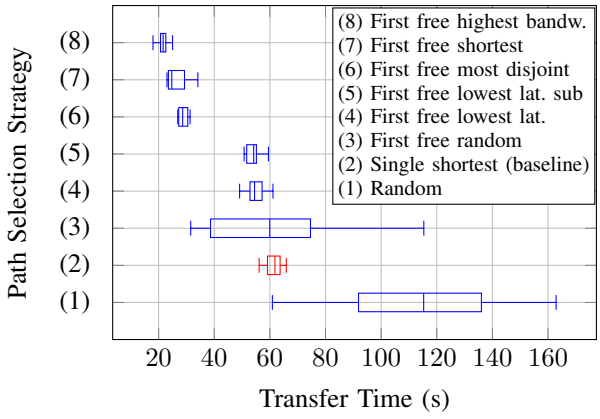

Fig. 6: Content transfer times in SCIONLab based on our selection strategies .

the same path as IP. This minor overhead is outweighed by SCION's multipath and security benefits.

B. Path Selection Strategies in SCIONLab

In SCIONLab, we transfer a 100 MB file between two Kubo nodes attached to OVGU Attachment Point (AP) and the CMU AP.

Figure 6 shows transfer time distributions for the path selection strategies presented in Section III-C in SCIONLab. All multipath strategies, except *Random*, outperform the *single shortest* baseline, which represents similar routing as BGP. Latency prioritizing strategies, such as *first free lowest latency*, demonstrate moderate improvements. The *highest bandwidth* strategy builds upon the *shortest* approach by dynamically selecting the fastest available paths, delivering a 2.9x speedup over the singlepath baseline, reducing transfer time from 61.83 s to 21.63 s.

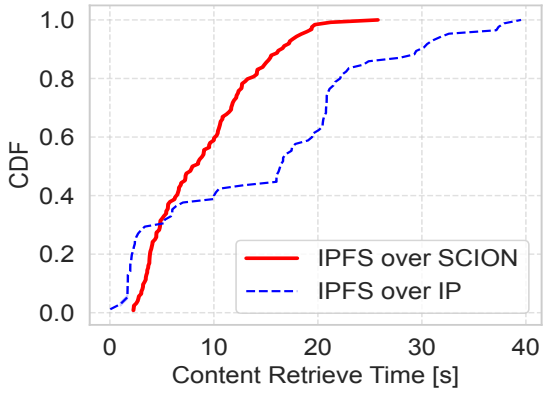

Fig. 7: Content retrieval time of a 50MB file with IPFS over SCION and IPFS over IP.

C. IPFS in SCIERA

In SCIERA, we deploy 11 IPFS nodes across 8 geographically diverse ASes (including sites in Europe, North America, and Asia) to assess real-world performance. These nodes connect as a single swarm, establishing peer connections using both native SCION connectivity and the conventional Internet. In each experimental run, a different node seeds a random 50 MB file, which is then fetched by all other peers. For SCION transfers, we use path selection strategy (8). We measure the time until each peer completes the download.

Figure 7 plots the CDF of content retrieval times. The SCION curve rises significantly steeper, demonstrating that a majority of transfers complete much faster than over the conventional Internet (IP). While some IP-based transfers achieve better performance, the distribution has a long tail, with some transfers taking over 30 seconds. SCION consistently mitigates this high-latency tail. This is because path-aware networking allows peers to bypass congested or suboptimal BGP routes that commonly affect inter-continental links, instead selecting from a set of diverse, high-performance paths offered by the SCIERA network.

VII. Related Work

Scherrer et al. analyzed the trade-offs in endhost path selection strategies, highlighting the tension between performance and stability [25]. John et al. developed DMTP, a deadline-aware multipath protocol for SCION that outperforms MPTCP and MPQUIC for latency-sensitive applications [16]. For bulk data transfer, Gartner et al. designed Hercules, a tool that uses a custom UDP-based protocol to maximize throughput on SCION [14]. Most relevant to our work, Gartner et al. also integrated SCION with BitTorrent, showing significant goodput improvements [13]. However, their approach treats each

path-peer pair as a distinct peer in the swarm. In contrast, our work integrates multipath control directly into `libp2p`'s connection management.

The performance of IPFS has been a subject of continuous research. Lajam et al. benchmarked IPFS in private networks, identifying I/O as a key bottleneck [7]. Shi et al. analyzed content availability in the public IPFS network, noting issues with centralization and performance variability [27]. Trautwein et al. proposed optimizations to the Kademlia DHT to improve lookup times for delay-sensitive use cases [30]. Our work complements these efforts by addressing the underlying network as a more fundamental bottleneck.

VIII. Conclusions

With our SCION integration into `libp2p`, we enabled secure multipath data transport and introduced strong, cryptographically-verifiable peer identities via SCION's CP-PKI. Our comprehensive evaluation results show that IPFS over SCION is more resilient to routing attacks and adversarial network manipulation. Furthermore, our adaptive path selection strategies leverage SCION's multipath capabilities to achieve significant reductions in content retrieval times, with a 2.9x speedup observed in the SCIONLab testbed and substantial gains in the production SCIERA network. These findings underscore the potential of path-aware networking to build a more robust and performant foundation for the decentralized web. Future research could investigate the use of SCION's trust architecture to secure the IPFS bootstrap process, and evaluate improvements in DHT lookup locality using SCION's path information.

References

[1] Composable and future-proof network addresses, https://github.com/multiformats/go-multiaddr, [Online; accessed 15-January-2025]

[2] An ipfs implementation in go, https://github.com/ipfs/kubo, [Online; accessed 15-January-2025]

[3] libp2p: the peer-to-peer network stack, https://libp2p.io, [Online; accessed 15-December-2024]

[4] The most expensive website downtime periods in history, https://www.statuscake.com/blog/the-most-expensive-website-downtime-periods-in-history/, [Online; accessed 13-February-2025]

[5] Pervasive internet-wide low-latency authentication implemented for scion, https://github.com/netsys-lab/scion-pila, [Online; accessed 15-February-2025]

[6] A border gateway protocol 4 (bgp-4). RFC 1771 (Mar 1995), https://www.rfc-editor.org/info/rfc1771

[7] Abdullah Lajam, O., Ahmed Helmy, T.: Performance evaluation of ipfs in private networks. In: Proceedings of the 2021 4th International Conference on Data Storage and Data Engineering. pp. 77–84 (2021)

[8] Albert, R., Barabási, A.L.: Statistical mechanics of complex networks. Reviews of modern physics 74(1), 47 (2002)

[9] Ballani, H., Francis, P., Zhang, X.: A study of prefix hijacking and interception in the internet. ACM SIGCOMM Computer Communication Review 37(4), 265–276 (2007)

[10] Benet, J.: Ipfs - content addressed, versioned, p2p file system (2014), https://arxiv.org/abs/1407.3561

[11] Chuat, L., Legner, M., Basin, D., Hausheer, D., et al.: The Complete Guide to SCION. From Design Principles to Formal Verification. Springer International Publishing AG (2022), https://link.springer.com/book/10.1007/978-3-031-05288-0

[12] Du, W.: SEED internet emulator. https://seedsecuritylabs.org/emulator/ (2024)

[13] Gartner, M., Krüger, T., Hausheer, D.: Leveraging the scion internet architecture to accelerate file transfers over bittorrent (2023), https://arxiv.org/abs/2301.13499

[14] Gartner, M., Smith, J., Frei, M., Wirz, F., Neukom, C., Hausheer, D., Perrig, A.: Hercules: High-speed bulk-transfer over scion. In: 2023 IFIP Networking Conference. pp. 1–9 (2023)

[15] Godfrey, P.B., Ganichev, I., Shenker, S., Stoica, I.: Pathlet routing. SIGCOMM Comput. Commun. Rev. 39(4), 111–122 (Aug 2009)

[16] John, T., Perrig, A., Hausheer, D.: Dmtp: Deadline-aware multipath transport protocol. In: 2023 IFIP Networking Conference (IFIP Networking). pp. 1–9 (2023)

[17] Krähenbühl, C., Perrig, A.: Ubiquitous secure communication in a future internet architecture. SN Computer Science 3(5), 350 (2022)

[18] Krähenbühl, C., Tabaeiaghdaei, S., Gloor, C., et al.: Deployment and scalability of an inter-domain multi-path routing infrastructure. In: Proceedings of ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT) (Dec 2021)

[19] Kwon, J., García-Pardo, J.A., Legner, M., et al.: Scionlab: A next-generation internet testbed. In: 2020 IEEE 28th International Conference on Network Protocols (ICNP). pp. 1–12. IEEE (2020)

[20] Lepinski, M., Sriram, K.: Bgpsec protocol specification. RFC 8205 (Sep 2017), https://www.rfc-editor.org/info/rfc8205

[21] Matei, R., Iamnitchi, A., Foster, P.: Mapping the gnutella network. IEEE Internet Computing 6(1), 50–57 (2002)

[22] Prünster, B., Marsalek, A., Zefferer, T.: Total eclipse of the heart–disrupting the {InterPlanetary} file system. In: 31st USENIX Security Symposium. pp. 3735–3752 (2022)

[23] Rinkel, L.: Leveraging the SCION Internet Architecture to Accelerate the InterPlanetary File System (IPFS). Master's thesis, Otto-von-Guericke University, Magdeburg, Germany (2024)

[24] De la Rocha, A., Dias, D., Psaras, Y.: Accelerating content routing with bitswap: A multi-path file transfer protocol in ipfs and filecoin 11 (2021)

[25] Scherrer, S., Legner, M., Perrig, A., Schmid, S.: An axiomatic perspective on the performance effects of end-host path selection. SIGMETRICS Perform. Eval. Rev. 49(3), 16–17 (Mar 2022)

[26] Sermpezis, P., Dimitropoulos, X.: Can sdn accelerate bgp convergence?—a performance analysis of inter-domain routing centralization. In: 2017 IFIP Networking Conference. pp. 1–9 (2017)

[27] Shi, R., Cheng, R., Han, B., Cheng, Y., Chen, S.: A closer look into ipfs: Accessibility, content, and performance. Proc. ACM Meas. Anal. Comput. Syst. 8(2) (May 2024)

[28] Spring, N., Mahajan, R., Anderson, T.: The causes of path inflation. In: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. pp. 113–124 (2003)

[29] Systems, A.: Anapaya systems, https://www.anapaya.net/, accessed 2020-08-22

[30] Trautwein, D., Wei, Y., Psaras, Y., Schubotz, M., Castro, I., Gipp, B., Tyson, G.: Ipfs in the fast lane: Accelerating record storage with optimistic provide. In: IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. pp. 1920–1929 (2024)

[31] Wirz, F., Gartner, M., van Bommel, J., et al.: Scaling sciera: A journey through the deployment of a next-generation network. In: Proceedings of the ACM SIGCOMM 2025 Conference. pp. 720–741 (2025)

[32] Xu, Y., Leong, B., Seah, D., Razeen, A.: mpath: High-bandwidth data transfers with massively multipath source routing. IEEE Transactions on Parallel and Distributed Systems 24(10), 2046–2059 (2013)