A Comparative Analysis of Routing Policies in BGP and SCION

Research Commissioned by SURF & SIDN Labs

Kaj Koole
University of Amsterdam
kkoole@os3.nl

Martyna Pawlus
University of Amsterdam
mpawlus@os3.nl

ABSTRACT

The SCION future Internet architecture aims to address many of the challenges of the current Internet. The architecture essentially provides an alternative for the current BGP-based Internet. On the current Internet, ISPs implement their inter-domain routing policies through BGP policy mechanisms. This leaves the question on how to implement common BGP routing policies in the SCION routing architecture. This paper aims to provide a comparative analysis of routing policies in BGP and SCION from the perspective of an ISP. Our methodology consists of determining current ISPs routing policies in BGP, analyzing their common routing policy elements, comparing their current implementation using BGP policy mechanisms to their SCION counterparts and finally, implementing one policy element using a SCION testbed. The findings show that due to the fundamental shift in path control to a model where the end-hosts construct the end-to-end paths, called path-awareness, makes it that in SCION ISPs lose control over the decision-making process of their child ASs. Although SCION offers more expressive path selection parameters and has greater flexibility for customization of routing decisions, from the perspective of ISPs, the current software implementation of SCION does not allow them to enforce specific routing policies.

July 14, 2023

1 INTRODUCTION

Scalability Control and Isolation on Next-Generation Networks (SCION) is an emerging technology that has the potential to address many of the challenges of the current Internet. It is being developed with a focus on improving scalability, security, and isolation, which are critical areas where the current Internet architecture faces limitations. Compared to the current Border Gateway Protocol (BGP)-based Internet, SCION introduces a different routing architecture where the source has control over the end-to-end path. This path control model is also referred to as path-aware networking.

Within the current BGP-based Internet, routing policies are used to influence the path selection process, an organization conveys their routing policy per their Autonomous System (AS). Within BGP, path selection criteria are often opaque and based on local decisions, this leads to suboptimal routing and limits support for multipath routing. In SCION the path selection mechanism is transparent, and it can use explicit path selection attributes, for example: latency, bandwidth, and trustworthiness. Additionally, SCION supports multipath routing, load-balancing, and leverages cryptography extensively to ensure integrity, authenticity, and confidentiality.

This research compares common routing policies implemented by Internet Service Providers (ISPs) in the current BGP-based Internet to how these could be implemented in the SCION architecture. Specifically, to determine whether current BGP routing policies would be desirable in the SCION architecture or if a different approach is needed to ensure optimal routing per the routing policy objectives of ISPs.

1.1 Context

Within the Internet architecture ISPs collectively form the global Internet. ISPs are an important part in providing connectivity to other networks. An ISP offers a service to customers in providing connectivity, connecting them to the global Internet. In general, the business of an ISP is concerned with moving customer traffic, thereby making a profit. On the Internet, an ISP participates in the global routing of Internet traffic made possible by BGP. An ISP wants to influence the routing of inter-domain traffic through their network by conveying what is called a routing policy. Current routing policies in BGP are well known to facilitate the business needs of ISPs. With the introduction of the future Internet SCION architecture new possibilities with regards to inter-domain routing are offered, but the new architecture also poses additional challenges due to the nature of what is called path-aware networking. Path-aware networking refers to the ability of end-hosts to discover and understand the characteristics of the paths they utilize to communicate within an internetwork. Additionally, it encompasses how endpoints react to these path properties, which in turn impact routing decisions and the transfer of data [5].

1.2 Related work

The book titled “The Complete Guide to SCION: From Design Principles to Formal Verification” [3] provides a theoretical background

on SCION's Path Policy. The authors discuss the approaches to implementing routing policies as well as provide sample path policies that can be implemented in SCION. Additionally, they highlight the differences between SCION and BGP policies, illustrating how BGP policies can be translated to be used in the SCION architecture.

In [1], Iljitsch van Beijnum explores the realm of Internet routing, focusing on BGP. The Internet, characterized as a network of numerous independent networks, enables seamless communication between users belonging to different networks. Acting as the cohesive force, BGP serves as a routing protocol that facilitates the exchange of information among networks. While BGP shares the fundamental objective of delivering packets to their intended destinations with other routing protocols, it faces additional challenges. In contrast to its counterparts, BGP must also consider the business aspect of Internet routing. Consequently, the book goes beyond the technical foundations of BGP and delves into the intersection between the technical and business dimensions of Internet routing.

In [2] Matthew Caesar and Jennifer Rexford describe the goals of network operators (ISPs) and routing policies implemented by them. They taxonomized routing policies in four general categories: business relationship policy, traffic engineering, scalability, and security-related policy. They attempt to isolate common design patterns and describe how these can be realized using BGP policy mechanisms.

In [7] Phillipa Gill, Michael Schapira, and Sharon Goldberg present a survey on business relationships and routing policies. The paper offers an in-depth analysis and discussion of the findings obtained from approximately 100 network operators. Additionally, the authors explain common routing policy models and they correlate the survey results with these models.

1.3 Research Questions

Our aim is to determine whether or not common BGP routing policies used by ISPs on the current Internet can be used in the SCION architecture. As such our main research question is as follows:

"How can common BGP routing policies be expressed in the SCION routing architecture?"

In order to answer this question, the following sub-questions will be answered as well:

- What components in the SCION architecture provide ways to enforce a routing policy?
- In what ways do these components compare to the way routing policies are enforced by ISPs on the current BGP-based Internet?
- Does the SCION architecture allow for routing policy implementations to achieve current ISPs goals on the BGP-based Internet?
- In what way is SCION more expressive regarding routing policy information?
- What are the limitations when implementing these routing policies in SCION compared to BGP?

2 BACKGROUND

To provide a comprehensive understanding of how routing policies are implemented in the current Internet architecture, this section begins with an overview of how current Internet routing works in BGP, followed by an explanation of the fundamental components in SCION. A more in-depth description of routing in SCION can be found in section 3.

2.1 Internet Routing Using BGP

Current Internet routing makes use of one de facto routing protocol, the Border Gateway Protocol (BGP) version 4 (BGP-4). Essentially, a network of networks, each network on the Internet is either part of or in itself an AS. Each AS has its own routing policy and administrative control over its network. In order to convey a routing policy various mechanisms in the protocol can be used. Though, each AS retains its autonomy and thus can decide whether or not to honor certain BGP attributes used in the routing policy of a peer. BGP was not developed with security in mind, the trust model of BGP assumes that routing information received from peers can be trusted. By default, no authentication of peers and integrity of information is validated. The protocol is vulnerable to various attacks such as prefix hijacking and redirection attacks. The protocol is described in Request for Comments (RFC) 4271 [11]. In a recent paper [10], the authors review the current state of affairs regarding BGP security. They describe the attacks against the BGP protocol and describe in detail the many BGP security extensions and detection-recovery systems that have been developed over the years. The authors conclude that current approaches only solve a negligible fraction of the problems and in most cases incur a large processing overhead.

2.2 Infrastructure Components of SCION

SCION, a future-Internet architecture aims to provide highly available and efficient point-to-point packet delivery. It introduces Isolation Domains (ISDs) that group ASs and are administered by core ASs. There are three types of links defined in SCION: core-links between core ASs, parent-child links between non-core and core ASs, and peering links between non-core ASs, as shown in figure 1 from [4]. ISDs serve various purposes, including supporting trust heterogeneity, providing transparency for trust relationships, isolating routing processes, and improving routing protocol scalability. SCION operates on intra-ISD and inter-ISD routing levels using Path-Segment Construction Beacons (PCBs) to explore network paths. PCBs carry cryptographically signed AS-level path information, known as Hop Fields (HFs), which are used by end hosts to create forwarding paths. Forwarding paths are obtained through path exploration, registration, and resolution processes. These steps enable efficient packet forwarding without the need for inter-domain forwarding tables [3].

There are three main components of SCION, namely: beacon service, path service, and certificate service. The beacon service is responsible for the propagation of PCBs and the construction of path segments. SCION, unlike Border Gateway Protocol Security (BGPsec), uses dedicated services for generating and verifying signatures, eliminating the need for expensive asymmetric cryptography at routers. The path service stores mappings of AS identifiers

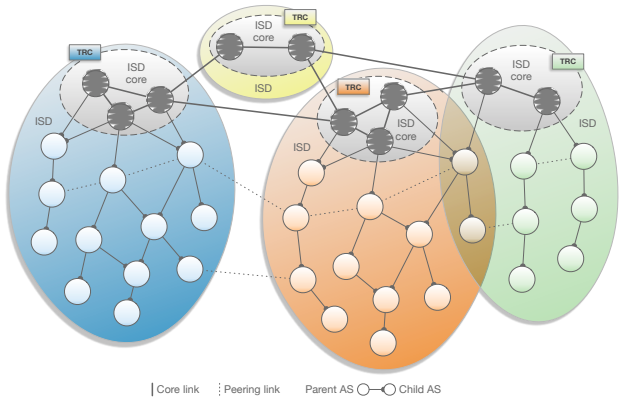

Figure 1: This overview illustrates an example SCION topology. In this topology, ASs are grouped into ISDs. ISDs are comprised of core ASs, which are interconnected using core links, and non-core ASs which are connected using parent-child and possibly peering links. ISDs isolate the routing processes and allow for the support of trust heterogeneity as each ISD hosts its own TRC.

to sets of path segments, so that ASs can select and upload their desired path segments through the beacon service. The certificates service manages keys and certificates for securing inter-AS communication, and the border routers connect different ASs in SCION, forwarding packets to the next border router of the destination host. SCION can operate with any intra-AS routing protocol and communication fabric, eliminating the need for changes to internal routers [3].

2.3 ISD and AS Numbering

In SCION, each AS is represented with a numeric scheme using the notation ISD-AS, where ISD is identified with a 16-bit value and AS with a 48-bit value. ISDs are represented as a decimal number ranging from 0 to 65535, where the number 0 is reserved for the wildcard ISD (meaning "any ISD"). The numbering scheme for ASs builds upon the existing BGP AS numbering scheme, using a format resembling hexadecimal numbers as used in Internet Protocol version 6 (IPv6). AS numbers are represented as a 16-bit colon-separated lowercase hexadecimal code or can be written in decimal. Similar to ISD numbers, the value 0 represents a wildcard AS, symbolizing "any AS" and as described in section 3.1.5 it is applicable to the path lookup process [3].

2.4 The Control-Plane Public Key Infrastructure (CP-PKI)

SCION prioritizes security and incorporates an authentication mechanism for all control-plane messages. The authentication relies on the CP-PKI, which manages and utilizes certificates, such as X.509 standard certificates, to verify signatures on PCBs. Additionally, SCION employs a unique trust model where trust anchors are special Trust Root Configurations (TRCs) called base TRCs, and multiple entities participate in a voting process to co-sign TRCs [3].

The CP-PKI encompasses various roles, certificates, and keys. All SCION ASs must possess at least one AS certificate and its corresponding private key for signing PCBs. Core ASs, listed in the TRC, have links to other core ASs and initiate beaconing. Certification Authoritiess (CAs) issue AS certificates to ASs, while voting ASs sign TRC updates. The trust within an ISD is anchored in the TRC, which contains root certificates for verifying CA certificates and subsequently verifying AS certificates. Different types of certificates, including root certificates, CA certificates, and AS certificates, form a chain of trust [3].

3 ROUTING ARCHITECTURE OF SCION

This section provides background information regarding routing concepts that are crucial to understanding the SCION architecture. Section 3.1 is based on chapters 2, 4, and 8, section 3.2 is based on chapters 2, and 5, and section 3.3 is based on chapter 6 of "The Complete Guide to SCION: From Design Principles to Formal Verification" [3].

3.1 Control Plane

In the SCION architecture there is a clear distinction between the control and data plane in terms of routing. The control plane's role involves identifying path segments and providing them to end hosts, along with the necessary certificates to authenticate those path segments.

3.1.1 Path-Segment Construction Beacons.

The path exploration and registration for both intra-ISD and inter-ISD are performed by what are called PCBs. In particular, a PCB represents a single path-segment that is defined as follows:

PCB = < INF || ASE(0) || ASE(1) || ... || ASE(N) >

Where the AS Entry (AS) ASE(I) is an AS entry with additional information about a specific AS, and INF represents an Info Field. The Info Field (INF) consists of three elements namely: the type and the direction of the constructed end-to-end path, a value used for the Message Authentication Code (MAC)-chaining mechanism, and a timestamp. The ASE consists of a signature, an unsigned, and a signed AS component. The signed AS component consists of the following elements:

- **Local** - is an Isolation Domain Autonomous System (ISD-AS) number of the AS,
- **Next** - is an ISD-AS number of an AS to which the PCB is forwarded to,
- **Hop Entry (HE)** - contains information about the ingress interface and a HF,
  - **HF** - this field defines both incoming and outgoing interfaces of the ASs between which the forwarding path is constructed. Additionally, it also contains a MAC.
- **Peer Entry (PE)** - a single ASE(signed) might contain multiple PEs as they specify peering links to another AS. PE itself contains HF, ISD-AS number of the peering AS, interface facing the peering AS, and the Maximum Transmission Unit (MTU) on the peering link [3].

Moreover, PCBs can define optional beacon extensions that can be used to communicate additional parameters. There are three

types of extensions defined, namely signed, unsigned, and detachable which leverages the benefits of both signed and unsigned extensions. These extensions play a crucial role in both the beaconing process and path construction. The two main categories of metadata are static and dynamic, with the key distinction being that static properties maintain a consistent value throughout the segment's lifetime. The specific metadata included depends on the type of beaconing process employed.

In core beaconing, the metadata includes the intra-ISD hop between the PCB ingress and egress interface and the inter-ISD hop at the egress interface.

In intra-ISD beaconing, on the other hand, the metadata includes the same information as in core beaconing and it can include additional information for three other use cases namely, the shortcut combination, combining up- and core-segments or core- and down-segments, and peering combinations [3].

There are seven types of metadata that can be included in the static metadata:

- **Latency** - it is defined as the static delay between two border routers in ideal networking conditions, without congestion and queuing delays,
- **Bandwidth** - it is defined as the available bandwidth between two border routers in ideal networking conditions,
- **Geographic information** - it refers to geographic coordinates or optionally a civic address, which can be provided for both border or intermediate routers,
- **Link type** - it represents the infrastructure used by links between border ASs. It can be one of the following: direct, multi-hop, or overlay links,
- **Internal hops** - it is defined as a number of internal hops between ingress and egress routers,
- **Power consumption and emissions** - power consumption and Carbon dioxide (CO2) emission can be included in the metadata,
- **Note** - represents plain-text notes designed to use for communication between network engineers [3].

3.1.2 Path Exploration (Beaconing).

In order to propagate the PCBs across the network the path exploration process, called beaconing, is initiated. During each propagation period, every AS generates a PCB and propagates it immediately. Upon receiving a PCB, an AS registers its contained path segment, extends the PCB, and forwards it to the next AS. The beaconing process differs inside the ISD and across ISDs due to the different purposes it should achieve, particularly in the core, where the goal is to create paths connecting every pair of core ASs. Hence, two types of beaconing are defined, namely intra-ISD beaconing, where PCBs are only distributed along parent-child links, and inter-ISD (core) beaconing, where PCBs are flooded to all core ASs.

Initiating the beaconing process involves core ASs periodically creating and propagating initial PCBs through their beacon services. The initial PCBs are sent to either child ASs (intra-ISD beaconing) or other core ASs (core beaconing). The initial PCB contains ASEs and an initial hop field that authenticates forwarding decisions within the AS. The signed PCBs are distributed to the neighboring beacon service using an outgoing interface field from the HF.

Once the beaconing process has been initiated the propagation of PCBs starts. When an AS receives a PCB, the beacon service verifies the signature of the PCB using its TRC. If the verification is successful then the PCB is added to the beaconing service local database.

During each propagation period, the beacon service selects the best PCBs based on local AS policies which are described in section 3.1.4. These selected PCBs are then sent to the associated egress interfaces to continue the path exploration process. In core beaconing, usually, multiple core PCBs are selected for connectivity purposes. The AS includes an ASE in the PCB for every chosen combination of PCB and egress interface. The newly created PCBs are forwarded to the beacon service of the next AS by using a one-hop path. To avoid loops during path creation, the core beacon service discards PCBs with self-created ASEs and can be configured to discard PCBs re-entering an already visited ISD. Lastly, the beacon service stores the PCB in its local database [3].

3.1.3 Path-Segment Registration.

Once the beaconing process is done, ASs start to create the path segments from the PCBs stored in the local database. There are two types of registering path-segments that differ from each other, namely intra-ISD and core path-segment registration. For intra-ISD registration, the beacon service selects up-segments, used to communicate with core ASs, and down-segments, which allow remote nodes to reach the local AS, from cached PCBs in each registration period. Then, it adds ASEs with appropriate hop fields, signs the modified PCBs, and registers the resulting path segments. The up-segments are registered with the local AS's path service and the down-segments are registered with the core path service of the originating AS.

For core path-segment registration, the core beacon service selects PCBs towards each core AS, adds ASEs with empty egress interfaces, signs the modified PCBs, and registers the resulting core-segments with the local AS's path service [3].

3.1.4 PCB and Path-Segment Selection.

When receiving intra-ISD or core PCBs, an AS needs to choose which PCBs to use for further beaconing and path segment registration. For non-core ASs, this selection involves determining PCBs to propagate downstream, selecting up-segments for registration at the local AS's path service, and choosing down-segments to register at a core path service. Core ASs, on the other hand, select PCBs to propagate to neighboring core ASs and choose core-segments for registration at the local AS's path service.

The beacon service performs PCB selection during the addition of PCBs from neighboring ASs, registration of PCBs at the path server, and determination of which PCBs to forward through specific egress interfaces. Various policies with different selection criteria can be employed during each of these steps. The following metrics outline some desirable properties used for PCB selection:

- **Path length** - this property is the number of hops from the remote AS to the local AS,
- **Peering ASs** - it is defined as a number of peering AS excluding core ASs,
- **Disjointness** - two definitions of disjointness are used: vertex-disjoint, meaning no common upstream or core AS,

and edge-disjoint, meaning no shared AS-to-AS link. Depending on the AS's objective, both definitions can be preferred,
- **Last reception** - it is defined as the time since the last PCB has been stored in the beacon database,
- **Propagated paths' lifetime** - it is an expiration time of a propagated path and it allows to renew paths that are about to expire,
- **Feature support** - additional functionality can be incorporated into beacon selection to accommodate diverse criteria such as bandwidth reservations, consistent support for specific SCION extensions, cryptographic algorithm preferences, geographic coordinates, latency information, or carbon footprint considerations.

Each AS has its own selection policy that governs how PCBs are stored and chosen at the AS's beacon service. The selection policy specifies various parameters, including the maximum number of candidate PCBs to store, the number of up-segments and down-segments to register at the local and core path services respectively, the number of PCBs to propagate, a blacklist of ASs and/or ISDs to exclude, allowable property ranges, and weights assigned to different properties for evaluating and selecting PCBs. Beacon policies are specific to each AS and may be kept private for commercial reasons. Based on the specific selection policy ASs calculate the overall quality of a PCB, and based on that the beacon service selects the preferred PCBs [3].

3.1.5 Path Lookup.

AS-local path service is used to resolve paths through a sequence of segment requests. The SCION daemon typically manages this process, where requests for up-segments are directly answered by the local path service, and the requests for core-segments and down-segments are forwarded to the responsible core path services. Replies to forwarded requests are cached to improve scalability and minimize latency.

The overall sequence of requests performed by the SCION daemon to resolve a path is as follows:

(1) Request up-segments,
(2) Request core-segments starting from core ASs reachable with up-segments, towards the core ASs in the destination ISD. If the destination ISD is the local ISD, this step requests segments from core ASs that are not directly reachable with an up-segment,
(3) Request down-segments starting from core ASs in the destination ISD.

Wildcard addresses as described in section 2.3 can be used in these requests and are expanded into actual addresses by the local and core path services. For up-segment requests, the destination, which is represented as a wildcard replacing the AS, is expanded by the local path service. For core-segment requests, the source is expanded by the local path service to all provider core ASs, and the destination by the core path service. Lastly, in down-segment requests, the source is expanded by the local path service to all core ASs of the specified ISD.

The resolver (SCION daemon) can employ different strategies, such as breadth-first search or depth-first search, to resolve paths efficiently. Currently, the breadth-first search approach, where concurrent queries for all segment types are made using wildcard addresses, is implemented [3].

The path lookup process in SCION involves interactions between the application, the local SCION daemon, the local segment-request handler, and the core segment-request handler. The summary of the process involves the following steps:

(1) The application sends a request to the local SCION daemon to obtain paths to a destination AS,
(2) If the destination is invalid or represents the local AS, an error message is immediately returned,
(3) The path request is split into segment requests. Cached segments are returned if available; otherwise, segments are requested from the local path service and added to the cache after validation,
(4) All segments are combined to form a set of paths,
(5) Paths with revoked on-path interfaces are filtered out,
(6) The paths are returned to the application.

The local segment-request handler in the path service follows these steps:

(1) The requested segment type is determined, and the request is validated,
(2) For up-segment requests, matching up-segments are loaded from the path database and returned,
(3) For core-segment requests:
    (a) The source wildcard is expanded into separate requests for each reachable core AS in the local ISD,
    (b) For each segment request:
        (i) If the source is the local AS, matching core-segments are loaded from the path database,
        (ii) If possible, segments are returned from the cache,
        (iii) Otherwise, the segment is requested from the core path service at the source, validated, and added to the cache.
(4) For down-segment requests:
    (a) The source wildcard is expanded into separate requests for every core AS in the source ISD,
    (b) For each segment request:
        (i) If the source is the local AS, matching down-segments are loaded from the path database,
        (ii) If possible, segments are returned from the cache,
        (iii) Otherwise, the segment is requested from the core path service at the source, and after validation, added to the cache.
(5) Revoked segments are filtered out.

The core segment-request handler in the core path service follows these steps:

(1) The request is validated:
    (a) The source must be the current core AS,
    (b) The request can be for a core-segment or a down-segment to an AS in the same ISD.
(2) If the destination is a core or wildcard address, matching core-segments are loaded from the path database and returned,
(3) Otherwise, matching down-segments are loaded from the path database and returned [3].

3.2 Data Plane

The fundamental difference between SCION's data plane and the current Internet Protocol (IP)-based data plane is path-awareness. This is done thanks to the fact that the path directives are embedded in the packet header. This solution provides control and transparency over the forwarding path. Additionally, it no longer requires routers to compute the longest-prefix match which requires expensive hardware and energy-intensive operations as the next hop is now embedded in the header.

SCION is an inter-domain network architecture that allows for separate inter-domain and intra-domain forwarding, meaning that each AS can choose its own intra-domain protocol for routing and forwarding, such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

The complete forwarding process within an AS involves several steps. First, the AS's SCION border router receives a SCION packet from a neighboring AS. The border router verifies the SCION header and determines the egress interface from the packet header. It then adds an appropriate IntraProtocol header, such as Multiprotocol Label Switching (MPLS) or IP, with the destination address set to the egress border router. Within the AS, routers and switches forward the packet based on the IntraProtocol header. When the packet reaches the egress border router, it removes the IntraProtocol header, updates the SCION header, and forwards the packet to the next SCION border router [3].

3.2.1 Path Authorization.

Path authorization in SCION ensures that data packets only follow paths authorized by all the ASs in the control plane. Unlike the IP-based Internet, where routers make forwarding decisions based on local information, SCION relies on the forwarding information carried within the packet itself. To ensure the security of the forwarding information encoded in hop fields, SCION employs symmetric cryptography by using MACs [3].

3.2.2 Path Construction (Segment Combination).

When establishing a connection between two end hosts in SCION, the forwarding path needs to be constructed. The end host receives multiple path segments (the complete PCBs) from the path server during the path-lookup process and combines them according to specific rules to create a forwarding path.

The SCION network architecture allows for the construction of forwarding paths by combining segments from different isolation domains (ISDs) to achieve global connectivity.

The composition of a SCION forwarding path can vary between one and three segments, depending on the specific characteristics of the network topology. To ensure the integrity of AS routing policies and prevent inefficient routing, certain conditions must be met when combining segments. These conditions include:

- Only one segment of each type (up-segment, core-segment, down-segment) is allowed,
- If an up-segment is present, it must be the first segment in the path,
- If a core-segment is present, it must come before the down-segment,
- If the Peering flag is set in any info field, there must be exactly two segments (up-segment and down-segment), both with the Peering flag set,
- Segments without the Peering flag must consist of at least two hop fields.

The possible segment combinations for communication across different ASs are described as follows:

- Communication through core ASs:
  - **Core-segment combination**: When the up-segment of the source and the down-segment of the destination do not have a common AS, a core-segment is needed to connect them. If either the source or destination AS is a core AS or both are core ASs, no additional up- or down-segments are required,
  - **Immediate combination**: When the last AS on the up-segment is the same as the first AS on the down-segment (both being core ASs), a simple combination of the up- and down-segments forms a valid forwarding path. In some cases, only one segment is needed for the combination.
- **Peering shortcut**: If a peering link exists between the up-segment and down-segment, the extraneous path segments to the core can be cut off,
- **AS shortcut**: In cases where the up-segment and down-segment intersect at a non-core AS, a shortcut path can be created by removing the unnecessary part of the path to the core,
- **On-path**: If the source's up-segment contains the destination AS or the destination's down-segment contains the source AS, a single segment is enough to construct a forwarding path.

To create a path between two non-core ASs that traverses a core AS, the source requires an up-segment, a core-segment, and a down-segment. If the up- and down-segments originate from the same AS, a core-segment is not needed.

When the source is in a non-core AS and the destination is in a core AS, there are two options: a direct up-segment from the destination AS if it is a direct or indirect parent of the source AS, or obtaining an up-segment to a core AS and a core-segment between that core AS and the destination AS if a direct up-segment does not exist.

Path construction between two core ASs is straightforward since the core guarantees the presence of a core-segment connecting them.

When both end hosts are in non-core ASs, alternatives such as peering path, shortcut path with a common AS, or destination AS on path can be used to avoid passing through the core.

An efficient path-construction algorithm is used to find and build the shortest forwarding path to a destination AS. The algorithm operates in two steps: graph construction and path construction. The graph construction step involves creating a weighted and directed graph based on the received up-, core-, and down-segments. The path construction step uses the graph to find the shortest path(s) in terms of AS hops [3].

3.3 SCION Path Policy

SCION offers ISPs the ability to implement path policies that align with their business models. Unlike the current Internet routing policies defined by BGP, SCION supports source-based policies and provides finer control over permissible paths. SCION faces challenges in defining path policies due to fundamental differences in path exploration, the need for multipath definitions, and the impact of client-based path selection on ISPs business models.

For core ASs, SCION closely resembles BGP's routing process, with the ability to learn and independently choose paths to other core ASs. BGP policies can be directly mapped to SCION path policies, although SCION ensures packets follow explored paths, unlike BGP. Additionally, SCION's path discovery does not rely on prefix aggregation.

Moving to non-core ASs, SCION's path exploration starts from core ASs and extends towards leaf ASs, while BGP constructs paths from leaf ASs to other ASs. This difference allows SCION to express a different set of path policies. An example illustrates BGP's limitation in controlling upstream paths compared to SCION.

In SCION, ASs can register different segments to influence their visibility to local and remote hosts. However, bidirectional paths in SCION make it challenging to implement source- or destination-based policies directly. The simplest SCION policies relate to paths towards the ISD core.

Unlike BGP, which allows routing policies based on IP prefixes, SCION's segments and forwarding paths are based solely on ASs and ISDs. This design decision offers advantages such as not requiring globally unique end host addresses, preventing routing information size explosion, and enhancing security by avoiding illegitimate sub-prefix announcements. However, it limits ISPs flexibility to route traffic differently based on end host subnets. A possible solution in SCION is to split a large AS into smaller ones, each corresponding to an IP prefix with specific routing policies in BGP. Such policy-defined ASs do not pose scalability issues within the hierarchical structure of ISDs, enabling efficient path discovery among non-core ASs.

SCION implements path policies through beaconing control, allowing ASs to choose which PCBs to send and which peering links to include. Explicit path policies can be added as beacon extensions, indicating permissible paths and enforcing accountability for policy violations. Hop field encryption with explicit path activation is another approach, where paths are encrypted and can only be activated by specific ASs. These features are not yet implemented but will be included in future releases [3].

4 METHODOLOGY

The research is of a qualitative nature, determining how current BGP routing policies could be compared to routing policies in SCION. Our overall methodology is comprised of four distinct phases. First, we start with a literature study to determine current BGP routing policies employed by ISPs, we supplement this literature study with a semi-structured interview with a network engineer at SURF who is an expert on BGP routing policies. The semi-structured interview allows us to obtain personal experiences regarding the operation of BGP routing policies in the context of an ISP. The interview consists of ten questions, these can be found in appendix B. Next, we analyze these current routing policies used by ISPs and identify three common routing policy elements using current BGP policy mechanisms. We model these routing policy scenarios into discrete topology examples based on the SCION testbed topology. Then, using these modelled routing policy scenarios we compare these routing policy elements to how these could be implemented in the SCION architecture. Next, we attempt to implement one such routing policy element on the SCION testbed and try to perform experiments to determine the policy's efficacy. Finally, we collect, analyze and discuss the results.

Phase 1: Literature Study on Common Routing Policies
The objective of this phase is to conduct a comprehensive review of existing literature regarding common routing policies used by ISPs. In order to identify relevant literature we conducted a search of scholarly publications, such as articles, papers, and theses. In addition, other credible sources such as standards documents and vendor documentation regarding the subject were used. We used the following academic databases and library resources: The ACM digital library[1], IEEE Xplore[2], Elsevier ScienceDirect[3] and Springer Link[4] to find relevant and up-to-date literature. Our criteria for inclusion of publications was the relevance of the literature regarding the subject of Internet routing policies, the Border Gateway Protocol (BGP), and routing policies in the context of an Internet Service Provider (ISP).

Table 1 lists the search terms and their related keywords used during the literature study.

Search Terms	Related Keywords
"ISP routing policies"	Internet Service Provider, Routing policies
"Internet routing policy"	Internet routing, Routing policy
"Inter-domain routing policies"	Inter-domain routing, Autonomous system, Routing policies
"BGP routing policies"	Border Gateway Protocol, BGP routing, Routing policies

Table 1: Used search terms and their related keywords.

In total, we found fifteen publications and after filtering based on our criteria, we ultimately reviewed three sources on Internet routing policies using BGP [6, 2, 7]. During our literature study, we found that due to the nature of the business model of an ISP their exact routing policies are often kept private. As such, it is difficult to find reliable sources on current routing policies employed by ISPs. Though, the identified sources give a good overview of common routing policy elements used by ISPs which we describe in section 6.1. Supplemented by the interview with an expert on the subject of BGP routing policies gives us additional perspectives, insights, and firsthand knowledge that might not be adequately covered by the existing literature. We describe the results of the interview in

[1] https://dl.acm.org/
[2] https://ieeexplore.ieee.org/Xplore/home.jsp
[3] https://www.sciencedirect.com/
[4] https://link.springer.com/

section 6.2.

Phase 2: Analysis of Routing Policy Elements
The purpose of this phase is to identify and analyze common policy elements used in Internet routing policies used by ISPs. By analyzing the results of the literature study and expert interview we come to a set of three common routing policy elements used by ISPs which we describe in section 6.3. We consider routing policy elements that are most important for ISPs based on their purpose, challenges, and benefits.

Phase 3: Comparison of Routing Policy Elements in BGP and SCION
During this phase, the identified routing policy elements currently implemented in BGP are compared to how these could be implemented in SCION. Due to differences in the inter-domain routing architectures of BGP and SCION it is difficult to directly compare policy mechanisms. For this, we model common inter-domain routing scenarios where the ISP is central in implementing the routing policy. In the modelled scenarios we describe often used BGP mechanisms to achieve policy goals. Next, we consider the same inter-domain routing scenario in SCION and map path policy mechanisms in order to achieve the same policy goals. We describe the modelled scenarios in section 7. The result of this phase is a clear comparison between BGP and SCION policy mechanisms to achieve routing policy goals in the identified inter-domain routing scenarios.

Phase 4: Implementation and Experimentation on SCION Testbed
The final phase involves the implementation of *one* of the identified routing policy elements on the SCION testbed provided by SURF, SIDN Labs, and the University of Amsterdam (UvA). During implementation and experimentation, we will evaluate the efficacy of the routing policy mechanisms currently implemented in the SCION software. The implementation of the SCION policy element is described in section 7.4.

5 EXPERIMENTAL SETUP

In this section, the used experimental setup is described. For testing routing policy mechanisms in the SCION routing architecture we used the SCION testbed provided by SURF, SIDN Labs, and UvA. Additionally, we extended the testbed infrastructure by using equipment provided by the Master Education Security and Network Engineering (OS3) and UvA.

5.1 The SCION Testbed Topology

The SCION .nl testbed consists of multiple nodes at various facilities in the Netherlands and has inter-connectivity with other SCION research networks. At the time of writing the SCION .nl testbed consists of a single ISD topology with ASs hosted at SURF, SIDN Labs and UvA. The testbed can also be connected to the SCION research networks of GÉANT[5], SCIONLab[6] and 2STiC[7].

Figure 2 from [8] depicts version 1.5 of the SCION .nl testbed.

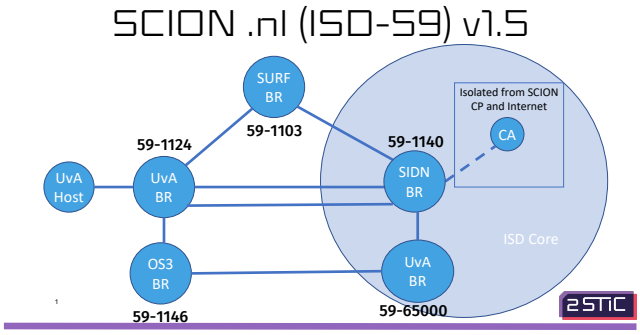

Figure 2: The SCION .nl testbed provided by SURF, SIDN Labs and UvA.

5.2 Extending The Topology

Using the infrastructure at OS3 we extended the topology of the SCION testbed by introducing three new ASs. Namely, 59-65011, 59-65012 and 59-65013. These networks are connected with AS 59-1124 at UvA. Additionally, a core AS, 59-65000 was added. The AS 59-65000 is hosted on UvA infrastructure.

Figure 3 depicts the ASs at OS3 and their connection with AS 59-1124 at UvA and AS 59-1140 at SIDN Labs.
Using this topology we can simulate several ISP scenarios to experiment with SCION's routing policy abilities.

The exact specifications of the infrastructure used at OS3 can be found in appendix A.

6 ROUTING POLICIES

Based on our findings from the literature study and expert interview we determined various common routing policy goals of ISPs that are currently implemented using BGP policy mechanisms. We explain how these policy elements can be implemented using BGP as the underlying inter-domain routing protocol.

6.1 BGP Routing Policies for ISPs

The paper "BGP routing policies in ISP networks" by Matthew Caesar and Jennifer Rexford [2] was our main source for establishing common routing policy goals of ISPs. In the paper the authors propose a taxonomy of routing policies, categorizing policy objectives into four distinct categories which we shortly describe below.

6.1.1 *Business relationships.*

The first category of BGP routing policies revolves around establishing and managing business relationships among ISPs. These

[5]https://geant.org/
[6]https://www.scionlab.org/
[7]https://www.2stic.nl/

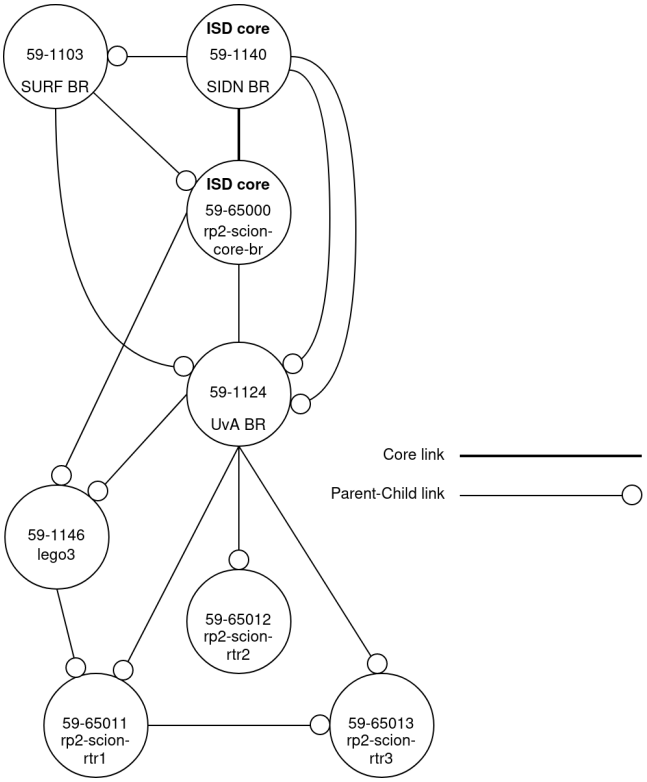

Figure 3: Extended SCION testbed topology by adding three new ASs hosted on OS3 infrastructure and one new AS hosted on UvA infratructure.

relationships can be classified into customer-provider, peer-to-peer, and backup arrangements. To express these policies in BGP, ISPs utilize mechanisms such as LocalPref and the Community attribute. LocalPref is assigned different values for different peering connections, enabling ISPs to prioritize customer-learned routes over those obtained from peers and providers. The Community attribute facilitates the tagging of routes with specific attributes, allowing ISPs to filter and control route import and export based on the associated business relationships.

6.1.2 Traffic Engineering.

The second category focuses on traffic engineering, wherein ISPs aim to optimize the flow of network traffic within and across their networks. Outbound traffic control involves adjusting import policies and Interior Gateway Protocol (IGP) link costs to achieve objectives such as hot-potato routing[8] and load balancing. Inbound traffic control poses challenges for ISPs due to limited visibility into neighboring ISPs' internal congestion and traffic engineering goals. To address this, ISPs employ mechanisms like the Multi-Exit Discriminator (MED) attribute to influence route selection in dual-homed scenarios or AS path manipulation to redirect traffic between different neighbors. Additionally, remote control mechanisms allow ISPs to manage the routing decisions of their peers through the configuration of routers and mapping Community attributes to specific routing preferences.

[8]Also referred to as early-exit routing.

6.1.3 Scalability.

Scalability is a critical consideration in BGP routing policies, given the potential for misconfigurations and other faults to cause route instability, service quality issues, and router failures. ISPs employ various measures to enhance network scalability. These include limiting routing table size by filtering long prefixes, promoting aggregation and default routes, and employing mechanisms like flap damping to minimize the number of routing changes, thereby improving network stability.

6.1.4 Security.

The final category pertains to security aspects associated with BGP routing policies. The BGP protocol is vulnerable to false information, which can disrupt routing goals, compromise routers, and degrade service quality. ISPs must employ defensive programming techniques to safeguard against these attacks. Discarding invalid routes through import filtering, protecting routing policy integrity through attribute rewriting, securing network infrastructure through export filtering, and defending against Denial of Service (DoS) attacks through filtering and damping mechanisms are some of the measures employed by ISPs to enhance the security of their BGP implementations.

6.2 Routing policies in non-commercial ISP scenarios

During the interview with the expert on BGP routing policies, we were able to contrast the results from the literature study on routing policies in ISP real-world scenarios. The expert gave us insights into the application of routing policies within a non-commercial ISP setting. Notably, the organization SURF, which is an National Research and Education Network (NREN), makes use of the concept of business relationships. Though, instead of being driven by financial profit, SURF as a not-for-profit organization, has different objectives. SURF is driven by collaboration with other research networks, and their routing policy reflects this. Their policy agreements are focused on path quality, path security and low latency. Additionally, within the SURF network the use of traffic engineering is employed. Though, traffic engineering is applied manually in scenarios of increased network load to distribute traffic over the available peering links.

6.3 Common Routing Policies in BGP

Next, we present three scenarios modelled using the SCION testbed topology as described in section 5.2, with each scenario exemplifying a distinct routing policy element within a selected policy category. The scenarios illustrated in the figures are presented on specific segments of the experimentation environment topology. For the purpose of modelling the policies in BGP omit SCION concepts in the diagrams. As such, the ISD-AS notation is changed for the traditional AS notation, naturally the SCION link types are also not used. To explain the specific cases more accurately we may discard links or change the roles between ASs. It is important to note that throughout all scenarios the AS 65011 (rp2-scion-rtr1) is the responsible ISP for implementing the routing policy.

6.3.1 Business Relationships.

In ISP networks, one widely implemented BGP routing policy is based on business relationships, strongly influenced by the concepts of the Gao-Rexford model (GR) as described in the paper "Stable Internet routing without global coordination" [6]. The GR model exploits the Internet's hierarchical structure and commercial relationships between ASs to impose a partial order on the set of routes to each destination. Using the proposed guidelines BGP is guaranteed to converge.

The GR model consists of two guidelines: GR preference and GR export. GR preference allows ISPs to prioritize routes learned from customers over routes learned via peers. Additionally, routes learned from peers should be given preference over routes learned from providers. In BGP, GR preference is implemented by assigning higher LocalPref values to customers compared to peers, and higher values to peers compared to providers.

GR export dictates that routes from peers should only be shared with customers and not with other peers. This arrangement ensures non-transitive peering, meaning peers do not receive routing information from other peers. Instead, peers can access transit services from providers. Conversely, routes from providers are only disclosed to customers, granting them transit access but not to peers. This routing structure maintains a "valley-free" configuration (described in section 6.3.1), ensuring that traffic follows a path from a provider "upwards" and then "downwards" towards the destination, without flowing downwards to a customer and then upwards again. In BGP, GR export can be achieved by utilizing the Community attribute "no-export" to control the export policies. This attribute prevents the routes from being shared beyond the immediate customer.

In the scenario illustrated in figure 4 we demonstrate the utilization of the GR preference routing policy. To modify the topology for this scenario, we introduced a new link between ASs 65012 and 65013, as well as between ASs 65012 and 1146. Furthermore, we removed a link between ASs 1124 and 65013, and transformed AS 1146 into a peer of ISP AS 65011.

With the updated topology in place, we can now depict a scenario where the ISP receives three distinct paths to AS 65012: one from its customer 65013, another from its peer 1146, and the third from its provider 1124. According to the GR preference policy, these routes should be prioritized in the following order: customer > peer > provider. In BGP, the ISP would implement this policy by assigning distinct LocalPref attributes for inbound routes to influence the outbound traffic. In particular, the ISP would assign the LocalPref values for routes learned from three AS in the following order 65013 > 1146 > 1124. Where a higher LocalPref value is preferred over a lower one. Consequently, the path to AS 65012 learned from its customer would be given the highest preference.

6.3.2 Traffic Engineering.

When multiple routes are available, ISPs must choose the preferred paths for traffic. A common routing policy for this purpose is hot-potato routing. Hot-potato routing is typically achieved by modifying import policies using LocalPref.

To control inbound traffic and to address congestion in the internal network, particularly for multi-homed ASs, ISPs may use the MED attribute to influence traffic distribution between gateways.

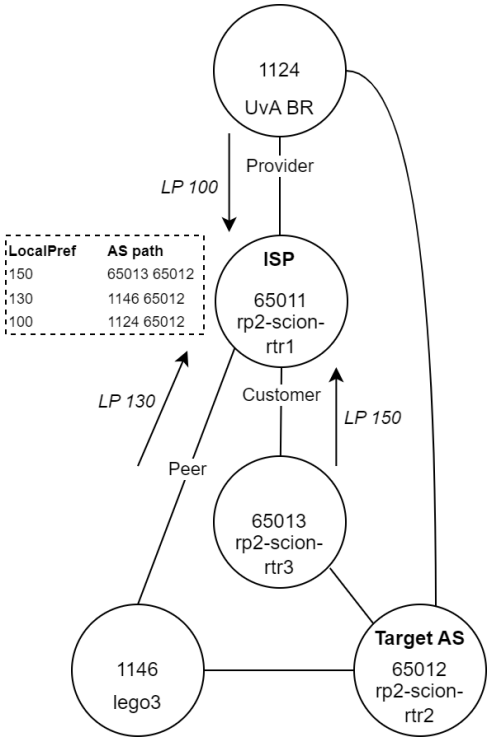

Figure 4: Modelled routing policy expressing business relationships according to the GR preference guideline. Outgoing traffic is influenced by setting LocalPref (LP) on incoming routes, higher LocalPref is preferred. The table next to the ISP AS 65011 shows the available paths to AS 65012 via AS 65011's customer, peer, and provider.

However, it should be noted that peers may not always respect the MED attribute as it can be overwritten or ignored.

Another important aspect for ISPs is selecting paths with low latency and high bandwidth to serve their customers effectively.

Figure 5 illustrates a scenario in a multi-homed environment where the implementation of routing policies by an ISP heavily relies on traffic engineering principles. In this particular use case, the ISP aims to prioritize routing the incoming and outgoing traffic of its customers through AS 1146, primarily driven by financial considerations. The secondary link, via AS 1124, would serve as a backup option in the event of a primary link failure. To achieve this objective using BGP, the ISP needs to establish policies for both incoming and outgoing traffic.

To direct customer traffic towards the primary link, the ISP sets a higher LocalPref value to the prefixes received from BGP peer from AS 1146 compared to AS 1140. However, ensuring the same outcome for incoming traffic is more challenging. One approach to influence path selection by other ASs involves artificially increasing the length of the AS path. This is achieved by prepending its own Autonomous System Number (ASN) a number of times to the customer's routes advertised to AS 1140. Consequently, the routes advertised by AS 65011 have shorter AS paths and are more preferred for the ISP. It is important to note that the ISP cannot

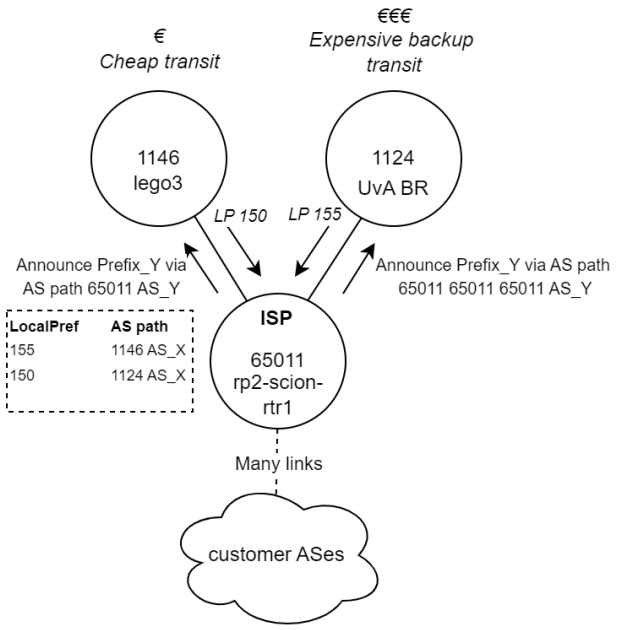

Figure 5: Modelled routing policy expressing a traffic engineering goal, preferring cheaper transit over more expensive transit. Prefixes reached by customer ASs are depicted as Prefix_Y, prefixes announced by customer ASs are depicted as Prefix_X. Outgoing traffic is influenced by setting LocalPref (LP) on incoming routes. Incoming traffic is influenced by prepending AS 65011 to the AS path three times, making it longer. The table next to the ISP AS 65011 shows the available paths to a fictitious destination AS X, the path via AS 1146 is preferred.

guarantee that all incoming traffic will consistently traverse via AS 1146, as other ASs may implement their own routing policies or even overwrite AS path attributes.

6.3.3 Security.

Ensuring security in routing policies is crucial for ISPs due to the lack of certain countermeasure mechanisms in BGP. A security-focused routing policy may include several elements. ISPs can discard invalid routes by implementing import filtering based on information from public databases like PeeringDB[9]. Another method to discard invalid routes is by implementing Resource Public Key Infrastructure (RPKI) which is a cryptographic technique for proving the association of IP prefixes and ASN's to the resource holders right to use them [12].

The second important element for routing policy security is protecting the integrity of the routing policy in case of violations by neighboring ASs. One way to achieve this is by rewriting BGP attributes that would impact routing decisions such as MED or NextHop[10].

[9]https://www.peeringdb.com/

[10]The NextHop attribute in a BGP message is used for forwarding traffic on the data plane, making sure that this value is equal to the configured BGP peer will prevent a hijacking scenario where the NextHop attribute is spoofed.

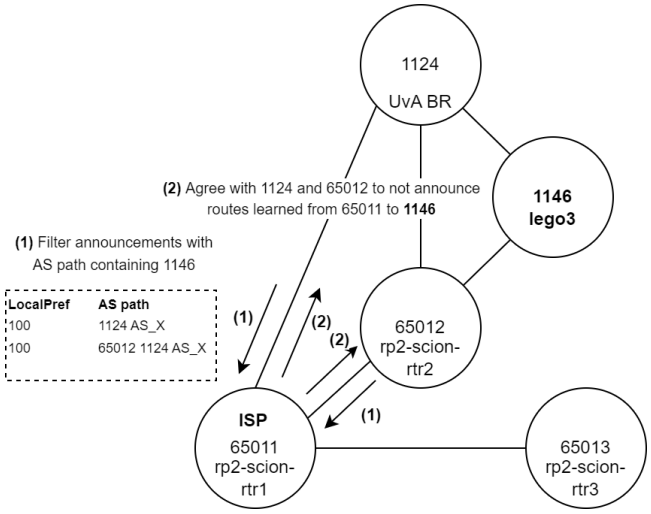

Figure 6: Modelled routing policy expressing a security goal, blacklisting AS 1146. Prefixes announced by customer AS 65013 are depicted as Prefix_X. In order to prevent outgoing traffic from traversing AS 1146 announcements containing AS 1146 in the AS path are filtered (1). Preventing incoming traffic can only be done by agreeing with neighboring ASs 1124 and 65012 to not announce routes learned from AS 65011 to AS 1146 (2).

We aim to apply a routing policy, as depicted in figure 6, to address a specific use case. In this scenario, our ISP intends to ensure that the traffic originating from its customer with AS 65013 does not traverse through AS 1146 due to security concerns.

To achieve this routing policy in BGP, the ISP would implement import route filtering based on the AS path attribute. This filtering mechanism will involve discarding routes that contain AS 1146 in their AS path. Additionally, the ISP must ensure that the customer's routes are not advertised to AS 1146. To accomplish this, ISP AS 65011 would establish an agreement with its neighboring ASs 1124 and 65012 not to propagate prefixes originating from AS 65013 to AS 1146. This agreement can be facilitated through the use of BGP Communities.

It is important to note that although ISP AS 65011 can enforce this routing policy within its own network, it cannot exert complete control over its neighboring ASs. As soon as the traffic leaves the local AS the ISP loses control of that traffic. Consequently, there is a possibility that the policy may be violated by these neighboring ASs. Moreover, it is worth considering that the AS path attribute can be manipulated or forged.

7 EXPRESSING POLICIES IN THE SCION ROUTING ARCHITECTURE

In this section, we describe how the routing policies presented in section 6.3 could be expressed in the SCION architecture. Furthermore, we present the components that can be used to enforce the routing policy and describe any limitations when implementing

those policies. In section 7.4 we described the results of implementing the security routing policy on the testbed.

7.1 Business Relationships

In SCION, the consideration of GR preference takes a different approach. SCION adheres to the principle of "valley-free" routing, which is achieved by enforcing specific rules for the propagation of intra-ISD PCBs on parent-child links. Moreover, the usage of path-segment combinations is limited to a maximum of one up-segment and one down-segment. These restrictions ensure that the path does not traverse "down" before going "up" in terms of parent-child links.

It is important to note that the path selection policy considers the possibility of a peering shortcut through the peering link. In the mechanism of constructing the path, AS 59-65012 can choose to utilize the path with the peering link between AS 59-1146 and AS 59-65011. Consequently, two potential paths are available to reach the ISP. Given that no additional policies are configured in AS 59-65012, the AS will prioritize the path that goes over the peering link. The rationale behind this preference lies in the selection process metric known as Peering ASs. This metric indicates that a higher number of peering ASs on a PCB increases the likelihood of discovering a shortcut.

There are limited options available to prevent the preference of the path over the peering or provider link. In [3] the authors suggest the application of explicit path policies at the link level. This approach involves implementing specific policies on the peering link by the ISP. The downstream ASs are unable to modify or alter these policies, as they are required to sign PCBs and register them in the core path service. Although, this solution would also require the implementation of an appropriate selection policy at AS 59-65012 that aligns with the specified path policy on the peering and provider link. Hence, the ISP cannot guarantee that the GR preference routing policy is achieved in the depicted use case shown in figure 7.

7.2 Traffic Engineering

The SCION architecture requires a different approach in achieving the desired routing outcome when compared to BGP. The increased control over path selection by end-hosts in SCION may limit the feasibility of influencing the path selection of child ASs in certain use cases.

SCION architecture leverages multipath routing which means that the parent AS can propagate multiple PCBs with paths via AS 59-1146 and AS 59-1124. Subsequently, the customer AS is responsible for selecting a preferred path based on its local policy.

In our particular use case presented in figure 8 filtering the PCBs with Access Control List (ACL) to propagate the paths only via 59-1146 is not viable as the ISP desires to maintain a backup path for customers.

To address this, the ISP may consider implementing charging mechanisms based on the usage of more expensive links or limiting the available bandwidth on those links. The former can be achieved by incorporating an additional bandwidth-reservation system like

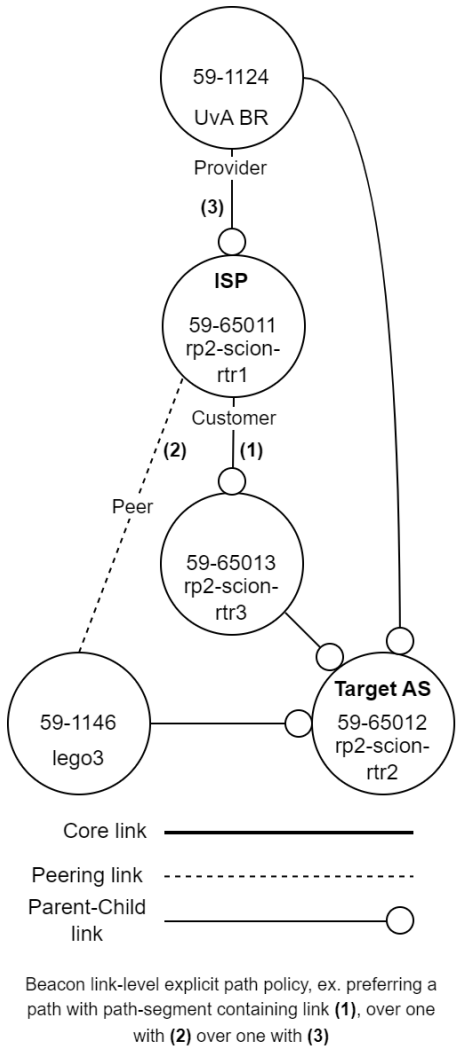

Figure 7: The architecture of SCION limits a routing policy based on business relationships due to path-aware networking. End-nodes have control over path selection and thus can only be influenced through explicit path policies at the link level which need to be coordinated with the selection policy used by the AS of the respective end-node.

Cooperative Lightweight Inter-domain Bandwidth-Reservation Infrastructure (COLIBRI)[11], while the latter involves including bandwidth information as metadata in PCBs using beaconing extensions. With this approach, customers should primarily base their path selection on the bandwidth parameter. Consequently, when the ISP sends PCBs with higher bandwidth for primary paths, customers would favor them over the backup path. However, both solutions require additional configuration on both the ISP and customer sides.

[11]During our research we did not consider COLIBRI as a policy mechanism, as it is not a routing policy technology but a bandwidth reservation technology first.

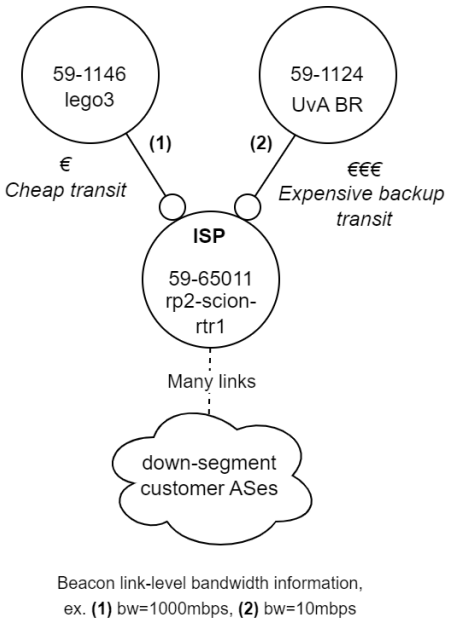

Figure 8: Implementing traffic engineering in SCION through link-level bandwidth information. The ISP AS 59-65011 propagates PCBs containing bandwidth information for the links to ASs 59-1146 and 59-1124 making the path through AS 59-1146 more attractive due to its higher advertised bandwidth.

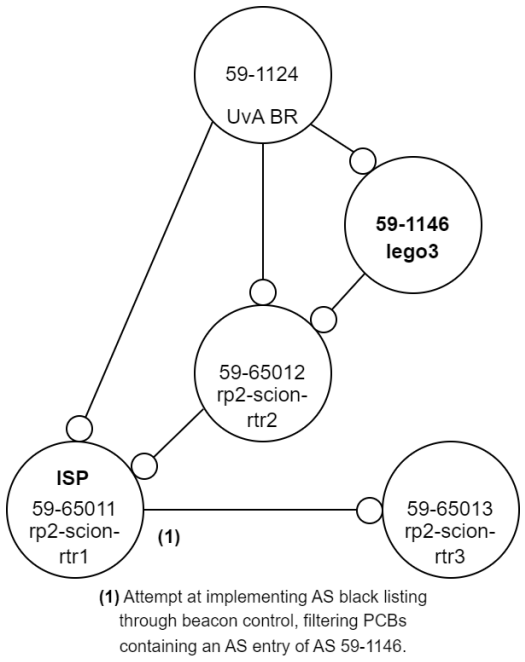

Figure 9: Filtering an AS through beacon control in SCION. In this scenario using beacon control will not prevent the AS 59-65013 from establishing a path through AS 59-1146 because the path can be constructed by requesting path segments via the core path service (not depicted).

7.3 Security

Expressing the routing policy from a scenario illustrated in figure 6 differs in the SCION architecture compared to BGP. Although the ISP can construct a routing policy that includes blacklisting AS 59-1146 in its propagation policy, this solution would not provide the desired outcome. By implementing this policy, the ISP only ensures that PCBs containing AS 59-1146 will not be propagated to AS 59-65013. However, AS 59-65013 can still construct a path to 59-1146 by requesting down-segments from the core path service, rendering the ISP unable to influence the path creation. Figure 9 illustrates the limited influence of the ISP in this scenario.

7.4 Implementation of the Routing Policy

In this section, we present the results obtained from deploying the security routing policy on the testbed. The reason for choosing to implement this particular policy is that the current SCION software[12] enables us to establish only fundamental path policies. These include specifying the maximum number of hops a segment can have, ASs that may not appear in a segment, ISD that may not appear in a segment, and indicating whether ISD loops should be filtered[13]. It is important to note that, as of the time of writing this research paper, the implementation of routing policies described in sections 7.1 and 7.2 is currently not possible as the policy mechanisms to support these routing policies are not implemented in the used SCION software.

[12]Version `v2021.10-142-g38afcbac6-scionlab`

[13]The policy definition is specified in the control/beacon/policy.go file in https://github.com/scionproto/scion

To implement the routing policy, we blacklisted AS 59-1146 in the propagation beacon policy type, this type is used to influence the propagation of the beacons to the child ASs. The configuration reflecting this change was applied to the file `/etc/scion/beacon_policy.yaml` as shown in listing 2 of appendix C. We explicitly specified to blacklist AS "0:0:47A" which is equivalent to decimal value 1146. Since the beaconing policy only allows blacklisting ASs within the same ISD, the notation for the blacklisted AS is 59-1146. Then, we included the beacon policy in the configuration file of the control service, as demonstrated in listing 1 of appendix C. By adopting this policy, we effectively prevented the ISP from propagating the PCBs downstream to the child AS. Consequently, no beacons containing the AS 59-1146 were registered in the beacon store located in `"/var/lib/scion/cs-1.beacon.db"` in AS 59-65013.

However, according to the path lookup which is described in section 3.1.5, when AS 59-65013 needs to construct a path to AS 59-1146 (which is not cached), it uses the core path service to request the necessary down-segments. We observed in the logs of the `scion-control-service` that the requests were sent to the core path services of core ASs 59-65000 and 59-1140. Upon receiving the down-segment, AS 59-65013 registered the segment successfully. The logs showing the segment request and successful segment registration are presented in listing 3 of appendix D.

As a result, AS 59-65013 was able to construct a path to AS 59-1146 as shown in listing 4 of appendix D, indicating that the blacklisting policy did not yield the desired outcome.

8 DISCUSSION

In this paper, we aim to conduct a comparative analysis of routing policies between BGP and SCION. By mapping the policy mechanisms in BGP to their equivalents in SCION in three common ISP routing policy scenarios, where possible. First, through a literature study and expert interview, we determined a selection of three common routing policy scenarios for ISPs. Next, using the SCION testbed topology we modelled the scenarios into discrete routing policy implementations using BGP policy mechanisms. Then, considering the SCION architecture, we mapped the same modelled scenario to policy mechanisms in SCION. Finally, we implemented one routing policy scenario on the SCION testbed.

8.1 Determining common routing policy scenarios for ISPs

Through results from the literature study and expert interview we have determined three common routing policy scenarios for ISPs. The taxonomy of BGP routing policies in ISP networks by [2] describes the four main policy objectives: business relationships, traffic engineering, scalability, and security. Due to our set scope we have selected the policy objectives: business relationships, traffic engineering and security for our study. Using the survey of inter-domain routing policies by [7] we found that ISPs primarily implement business relationships and traffic engineering in their routing policies, while policies for security are used but are considered to be less important, preferring connectivity over security. Though, it is important to note that the survey paper at the time of writing is almost ten years old and the views of network operators on routing security have changed. Efforts such as the Mutually Agreed Norms for Routing Security (MANRS) initiative[14] have improved adoption of security oriented routing policy mechanisms such as RPKI.

The interview with the expert on BGP routing policies augmented the results from the literature study. We were able to verify common routing policy elements used by ISPs as presented in the reviewed literature, though the results from the interview also allowed us to contrast typical commercial ISP objectives to those of a non-commercial ISP. Notably, path selection needs not follow preference for the cheapest path but can also be based on path quality, security and latency. Independent of the commercial or non-commercial objectives of the ISP, the used concepts and mechanisms for implementing routing policies in BGP are the same.

8.2 Comparison of policy mechanisms in BGP and SCION

The results that we obtained when comparing BGP policy mechanisms to how the routing policy could be implemented in SCION has shed light on the key differences in the architecture and routing policy enforcement between the two technologies. In this section, we delve into these differences as well as the implications regarding the policy implementations.

8.2.1 Path Selection.

Path selection mechanisms play a crucial role in routing policies. In BGP, each intermediate AS traversed to reach a destination independently performs path selection to determine the appropriate next hop to route the packet. Various attributes are used in the best path selection algorithm. Common BGP policy mechanisms are: LocalPref, AS path manipulation, MED and Communities.

However, in SCION, the paradigm diverges from BGP. Here, the end-hosts have control over their paths, and intermediate ASs forward the packets according to the path selected by the source. The parent ASs can announce preferred or non-permissible paths to their child ASs by using beacon extensions. Nevertheless, the efficacy of these solutions may vary as the end-host retains control over its local policies governing path selection.

8.2.2 Traffic Engineering.

Traffic engineering is another important aspect of routing policies. In BGP, outbound and inbound traffic can be influenced through the BGP attributes such as LocalPref, AS path prepending, MED, and Communities. While, in SCION, beacon extensions can be used to signal parameters such as bandwidth or latency, allowing for more fine-grained control over child path selection. SCION, therefore, is more expressive when it comes to defining the routing policies for traffic engineering as it allows to advertise multiple properties, which are mentioned in section 3.1.1, even on a link level.

8.2.3 AS-level Policy.

The AS-level policy implementation also differs between BGP and SCION. In BGP, a commonly used construct called a route-map, is used to influence route import and export. Route-maps allow network engineers to define specific criteria and actions to be applied to incoming and outgoing route advertisements. The enforced policies can include route filtering, attribute modification, or route redistribution, among other actions.

In contrast, SCION takes a distinct approach to the AS-level policy implementation, namely it relies on a local policy mechanism that operates through the registration and propagation of beacons. ASs use the path service to register beacons, specifying the up-segments and down-segments of the desired paths. Propagation of beacons, on the other hand, is done by the beaconing policy in SCION. ASs use the beaconing policy to control the dissemination of beacons, determining which beacons are shared with child ASs.

8.2.4 Security.

Security is a critical consideration in routing policies. BGP employs mechanisms such as maximum advertised prefix limitations, route filtering, or RPKI validation. These mechanisms help prevent routing anomalies, such as prefix hijacking, DoS attacks, or unauthorized route advertisements. By imposing restrictions on the prefixes accepted or advertised by an AS, network engineers aim to maintain higher integrity and authenticity of routing information.

However, these mechanisms are not necessary in SCION due to the architectural differences. In SCION, inter-domain forwarding decisions are not based on IP prefixes, and the control plane is authenticated using CP-PKI. This means that the control messages exchanged between ASs in SCION are authenticated using cryptographic keys and digital signatures as described in section 2.4. By verifying the authenticity of control plane messages, SCION enhances the trustworthiness and integrity of the routing infrastructure.

[14] https://www.manrs.org/

In summary, table 2 gives an overview of the resulting BGP policy mechanisms mapped to their SCION counterparts.

Having discussed the differences between BGP and SCION in terms of routing policy mechanisms, it becomes clear that the architecture of SCION significantly influences the implementation and enforcement of policies. SCION's path-aware networking approach provides end-nodes with control over their traffic paths, which can lead to a loss of control for ISPs. However, ISPs can still implement beaconing control to influence the paths disseminated to their child nodes, ensuring some level of control.

8.3 Implementing SCION path policies

Our implementation of a policy example using the SCION testbed revealed limitations in the current stable SCION packages. Specifically in version `v2021.10-142-g38afcbac6-scionlab`, which is currently considered a stable version actively undergoing development[15], also in the context of control plane policies. One significant limitation is the lack of beacon control beyond a limited set of policy options, which are specifying the following parameters: Hop Limit, Blacklist AS, Blacklist ISD, and Permit ISD loop. The results show that despite the ISP's attempt to blacklist AS 59-1146 in the propagation policy, it did not achieve the desired outcome, which was described in section 6.3.3. While the policy successfully prevented the propagation of PCBs containing AS 59-1146 to AS 59-65013, it was observed that AS 59-65013 could still construct a path to AS 59-1146. This indicates that the ISP's influence over path creation was limited in this scenario.

These findings show the limitations of the current SCION implementation of routing policies in effectively preventing the establishment of paths to untrusted ASs. Consequently, ISPs face challenges in exerting control over their customers' ability to construct paths traversing untrusted ASs. To address this limitation and enhance security, it is crucial to develop mechanisms that validate and filter routing decisions in the data plane.

Within the SCIONLab project the development of the SCION Path Policy Language specification has recently shifted, as it initially was meant to be used for path policy implementations in the SCION architecture regarding the path server, SCIOND and the beacon server for different but overlapping purposes. Currently, the SCION Path Policy Language is only used at the level of the SCION IP Gateway (IP) [9].

Discussions in the SCIONLab Slack channel[16] about the current implementation of path policies in the SCIONLab software pointed us to a abandoned implementation of the SCION path policy[17], though due to the scope of our research and time constraints we were unable experiment with it. One developer noted that simple beaconing control policies could be manually implemented through coding an ACL in the beacon propagator code[18].

[15] For the testbed environment we used the latest SCIONLab Ubuntu packages per the installation method from: https://docs.scionlab.org/content/install/pkg.html
[16] Available at: https://www.scionlab.org/
[17] https://github.com/scionproto/scion/tree/master/private/path/pathpol
[18] https://github.com/scionproto/scion/blob/master/control/beaconing/propagator.go

9 CONCLUSION

In this paper, we examined the routing policies implemented in the current BGP-based Internet architecture and explored how they could be expressed and realized in the emerging SCION architecture. Our goal was to determine whether the existing BGP routing policies used by ISPs can be effectively implemented in SCION and what policy mechanisms would then be used compared to those used in BGP. Our main outcome is the mapping of BGP and SCION policy mechanisms in section 8.2, in particular table 2 can be used as a frame of reference for operators wanting to translate their BGP routing policy mechanisms to those used in SCION.

We examined the common routing policy goals of ISPs in the BGP-based Internet based on the literature study and findings obtained from an expert interview on the topic of current BGP routing policies. Subsequently, we devised three scenarios to exemplify the implementation of these routing policies within the BGP architecture. The ways to enforce routing policies in BGP for an ISP include the usage of BGP attributes and mechanisms such as LocalPref, MED, Communities, or AS path manipulation. While these mechanisms are commonly utilized by ISPs, they do not always guarantee the desired outcome, especially when influencing incoming traffic. It is important to note that in BGP, ISPs lose control over the traffic once it has been forwarded outside their AS, meaning that it may be rerouted through parts of the Internet unintended by the ISP.

Based on our analysis, we conclude that while some of the BGP routing policies can be partially translated and implemented within SCION such as signaling the preferred routes to the child ASs for traffic engineering purposes, the overall implementation of routing policies differs due to the fundamental shift in path control from a hop-by-hop basis to the control by end-hosts in SCION's path-aware networking model. In SCION ISPs lose control over the decision-making process of their child ASs. However, they can still exert influence over these decisions by incorporating mechanisms such as explicit path policies through beacon extensions or applying the beacon filter policies in the configuration file. Consequently, there are limitations and challenges in implementing current routing policies commonly employed by ISPs within BGP in SCION.

Our analysis described in section 8.2 resulted in a mapping of BGP policy mechanisms to those used in SCION given the modelled routing policy goals. Table 2 gives a more general overview of the four compared policy components in BGP and SCION.

In SCION, routing policies are implemented at different levels, specifically in beaconing control and the path service. Through the creation of policies within these services, ISPs can influence how the beacons are propagated and registered locally, and which path segments are selected. SCION provides the capability to define diverse selection policies based on various types of selection properties, each associated with respective weights. Compared to BGP, SCION offers more expressive options for path selection, as it introduces new properties such as peering ASs, disjointness, latency, bandwidth, CO2 emissions, geolocation, internal hops, and more. This enhanced flexibility in property selection allows for greater customization of routing decisions. Our practical experiment on implementing a security policy in SCION, specifically blocking path creation through the ISP with a selected AS, proved ineffective. This was due to SCION's beaconing and path lookup architecture, which

Policy Component	BGP	SCION
Path Selection	Use various attributes such as **LocalPref, AS path, MED** and **Communities** to select the best path	End-hosts have control over their paths, ASs can announce **non-permissible paths** using **beacon extensions**
Traffic Engineering	Influence outbound traffic: **LocalPref, AS path prepending, Communities** Influence inbound traffic: **AS path prepending, MED, Communities**	**Beacon extensions** contain distinct parameters to influence child's path selection (e.g. **bandwidth, latency**)
AS-level Policy	Import and export routes using **route-maps**	Register beacons using **path service and beaconing policy** (local policy)
Security	**Max. prefixes, route filtering, RPKI validation**	Covered by **Control-Plane PKI**

Table 2: BGP policy mechanisms mapped to SCION counterparts.

prevents complete blacklisting of an AS within its control plane. Implementation of other scenarios are left to future work due to the current limitations in the SCIONLab software.

10 FUTURE WORK

There are several areas for work that can expand and enhance our findings from this research paper.

One direction for future work is the extension of routing policy use cases. In this study, we examined three routing policy elements within BGP and SCION. In order to provide a more comprehensive understanding of routing policies for ISPs, it is essential to extend our research for more use cases. By exploring additional routing policy elements, we gain deeper insights of the differences between BGP and SCION in terms of policy implementation, enforcement and possible implications for ISPs.

Another area concerns the usage of the Path Policy Language in SCION. The Path Policy Language specification [9] was initially intended to be applied at the path server, SCION daemon, and the beacon server. However, it has been limited in scope to only be included in the SIG at the time of writing this paper. Future work should focus on the development and adoption of the Path Policy Language within the broader SCION architecture. This would allow for the implementation of more fine-grained selection policies, therefore enabling more complex routing policies.

The current implementation of the SCION architecture is still limited in its functionality and deployment. To further validate the efficacy of the routing policies in SCION, it is crucial to have a more robust and feature-rich implementation of SCION. A future SCION testbed with fine-grained path policy mechanisms would enable the realistic evaluation of our modelled scenarios and provide valuable insights into the practical implications of the implementation of path policies in SCION. Additionally, a future implementation of SCION with support for hop field encryption with explicit path activation could provide another means of implementing path control.

During our investigation for this research paper, we actively engaged with the developers of the SCIONLab software. Through the discussions we acquired valuable insights into the ongoing research and development efforts focused on the implementation of the beaconing architecture and path policy enforcement within the SCIONLab software. Therefore, future work would include evaluating the effectiveness of implementing routing policies, which are currently not feasible within the existing beaconing architecture using the current path policy enforcement features. Manually coding beacon control mechanisms in the beacon propagator code as described in section 8.3 could be done to build policies beyond the current implementation of the beacon propagation policy.

Based on the findings and discussions presented in this paper, several recommendations should be considered in the implementation of SCION for future developers. Firstly, in terms of routing policy implementations, it is important to expand the use cases for ISPs in the BGP architecture and explore additional routing policy elements beyond the ones examined in this study. By doing so, a more comprehensive understanding of the ISPs needs in terms of policy implementation, enforcement, and implications can be achieved and included in future implementations. This would also provide necessary insights for ISPs to make informed decisions regarding the adoption of SCION.

In terms of security considerations, future implementations of SCION could provide mechanisms for ISPs to have control over the creation of paths to untrusted ASs by their customers. This may involve further validation mechanisms or filtering in the data plane to prevent undesirable routing decisions. Additionally, considering that not all ISPs charge their customers based on bandwidth, mechanisms related to artificially limiting bandwidth to make links less desirable may not be suitable for all ISPs as some of them would base their selection criteria on path quality attributes such as latency.

ACKNOWLEDGEMENTS

We want to thank our supervisors Marijke Kaat (SURF) and Ralph Koning (SIDN Labs) for their support and guidance during our research. Next, we would like to express our appreciation to Niels den Otter (SURF) for providing us with valuable insights regarding routing policies in BGP and inter-domain routing in general. Finally, we would like to thank the people from the SCIONLab community for answering our questions regarding various aspects of SCION along the way.

REFERENCES

[1] Iljitsch van Beijnum. 2022. URL: https://play.google.com/store/books/details/Internet_Routing_with_BGP?id=_NKaEAAAQBAJ&hl=pl&gl=NL.

[2] M. Caesar and J. Rexford. "BGP routing policies in ISP networks". In: *IEEE Network* 19.6 (2005), pp. 5–11. DOI: 10.1109/MNET.2005.1541715.

[3] Laurent Chuat et al. *The Complete Guide to SCION - From Design Principles to Formal Verification*. Information Security and Cryptography. Springer, 2022. ISBN: 978-3-031-05288-0. DOI: 10.1007/978-3-031-05288-0. URL: https://doi.org/10.1007/978-3-031-05288-0.

[4] Laurent Chuat et al. *The Complete Guide to SCION: From Design Principles to Formal Verification*. en. Information Security and Cryptography. Cham: Springer International Publishing, 2022. Chap. 2, p. 18. ISBN: 978-3-031-05287-3. DOI: 10.1007/978-3-031-05288-0. URL: https://link.springer.com/10.1007/978-3-031-05288-0.

[5] Spencer Dawkins. *Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)*. RFC 9049. 2021. DOI: 10.17487/RFC9049. URL: https://datatracker.ietf.org/doc/rfc9049.

[6] Lixin Gao and J. Rexford. "Stable Internet routing without global coordination". In: *IEEE/ACM Transactions on Networking* 9.6 (2001), pp. 681–692. DOI: 10.1109/90.974523.

[7] Phillipa Gill, Michael Schapira, and Sharon Goldberg. "A survey of interdomain routing policies". In: *ACM SIGCOMM Computer Communication Review* 44.1 (2014), 28–34. ISSN: 0146-4833. DOI: 10.1145/2567561.2567566.

[8] Ralph Koning. *SCION .nl testbed v1.5*. Slide 1. SIDN Labs, 2STiC, 2023.

[9] Lukas Vogel Lukas Bischofberger and Martin Sustrik. *Path Policy Language Design*. SCION Association. Aug. 2019. URL: https://docs.scion.org/en/latest/dev/design/PathPolicy.html (visited on 07/04/2023).

[10] Asya Mitseva, Andriy Panchenko, and Thomas Engel. "The state of affairs in BGP security: A survey of attacks and defenses". In: *Computer Communications* 124 (2018), pp. 45–60. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2018.04.013. URL: https://www.sciencedirect.com/science/article/pii/S014036641731068X.

[11] Yakov Rekhter, Susan Hares, and Tony Li. *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. Jan. 2006. DOI: 10.17487/RFC4271. URL: https://www.rfc-editor.org/info/rfc4271.

[12] *What is RPKI?* RIPE NCC. 2023. URL: https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/what-is-rpki (visited on 07/14/2023).

ACRONYMS

ACL Access Control List. 12, 15
AS Autonomous System. 1–16, 18, 22
ASE AS Entry. 3, 4
ASN Autonomous System Number. 10, 11
BGP Border Gateway Protocol. 1–3, 7–16
BGPsec Border Gateway Protocol Security. 2
CA Certification Authorities. 3
CO2 Carbon dioxide. 4, 15
COLIBRI Cooperative Lightweight Inter-domain Bandwidth-Reservation Infrastructure. 12
CP-PKI Control-Plane Public Key Infrastructure. 3, 14
DoS Denial of Service. 9, 14
GR Gao-Rexford model. 10, 12
HE Hop Entry. 3
HF Hop Field. 2–4
IGP Interior Gateway Protocol. 9
INF Info Field. 3
IP Internet Protocol. 6, 7, 11, 14, 15, 18
IPv6 Internet Protocol version 6. 3
IS-IS Intermediate System to Intermediate System. 6
ISD Isolation Domain. 2–9, 12, 13, 15
ISD-AS Isolation Domain Autonomous System. 3
ISP Internet Service Provider. 1, 2, 7–16
MAC Message Authentication Code. 3, 6
MANRS Mutually Agreed Norms for Routing Security. 14
MED Multi-Exit Discriminator. 9–11, 14, 15
MPLS Multiprotocol Label Switching. 6
MTU Maximum Transmission Unit. 3
NREN National Research and Education Network. 9
OS3 Master Education Security and Network Engineering. 8
OSPF Open Shortest Path First. 6
PCB Path-Segment Construction Beacon. 2–7, 12, 13, 15
PE Peer Entry. 3
RFC Request for Comments. 2
RPKI Resource Public Key Infrastructure. 11, 14
SCION Scalability Control and Isolation on Next-Generation Networks. 1–3, 5–9, 11–16, 18, 21
SIG SCION IP Gateway. 15, 16
TRC Trust Root Configuration. 3, 4
UvA University of Amsterdam. 8

A EXPERIMENTAL ENVIRONMENT

A.1 Lego3 Node Configuration

Item	Description	Note	Purpose
Chassis	Dell PowerEdge R630	-	AS 59-1124 node and hypervisor.
CPU	2x Intel(R) Xeon(R) CPU E5-2650L v4 @ 1.70GHz	14 core w/ HT for total of 52 vCPU cores	-
RAM	128GB DDR4	8x 16GB 2400MHz Dual-Rank DDR4	-
SSD	Samsung PM863 960GB	-	-
NIC	Intel(R) 2P X520/2P I350 rNDC	2x 1GbE RJ-45 & 2x 10GbE SFP+	-

Table 3: Lego3 node hardware specifications.

Item	Description	Version
Operating System	Ubuntu Server 22.04 LTS, General purpose OS, hosts SCION AS 59-1124, and is hypervisor for additional SCION infra at OS3.	Ubuntu 22.04.2 LTS
SCION stack	sciond, scion-dispatcher, scion-control-service and scion-border-router.	v2021.10-142-g38afcbac6-scionlab
Hypervisor stack	KVM/libvirt installed through Ubuntu repository packages.	QEMU 6.2.0 / libvirt 8.0.0
Networking	8021q Linux kernel module for IEEE 802.1Q support, Linux bridge for connecting VMs to the VLAN 999 network segment.	-

Table 4: Lego3 node software specifications.

A.2 Infrastructure Diagram

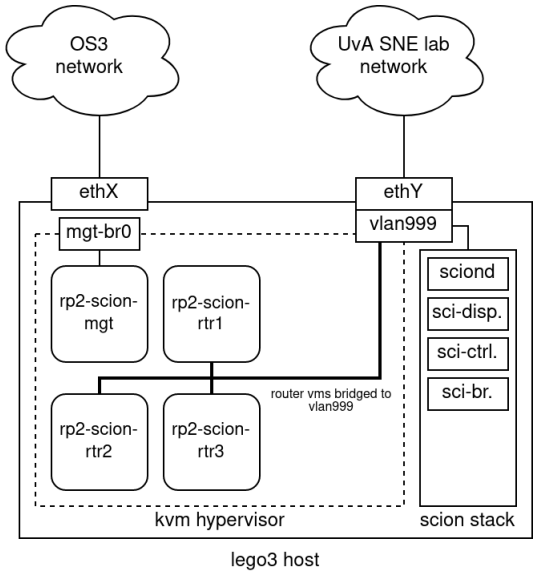

Figure 10: Infrastructure diagram depicting the lego3 server hypervisor, networking and SCION stack at OS3.

B INTERVIEW QUESTIONS

As described in the methodology section the expert interview was conducted using the following set of questions.

- **Q1:** Could you give a overview of the network of X regarding BGP routing?
- **Q2:** How do you define a single routing policy? How many policy elements does it use?
- **Q3:** Which BGP attributes do you use to achieve specific policy goals?
- **Q4:** Could you give us three business cases for defining different routing policies, and how would you implement those?
- **Q5:** Do you have any discrepancies in the configuration of routing policies across your Autonomous System, or is the policy consistent for all routers?
- **Q6:** On what basis are usually routing decisions made (prefix, AS path, community)?
- **Q7:** How do you control the BGP attributes advertised with the prefixes from your customers. Do you honor them or do you ignore them when setting the policy configuration?
- **Q8:** Do you implement traffic engineering? If so how and what are the use cases?
- **Q9:** Are X's interconnection agreements influenced by the Gao-Rexford (GR) routing policy model?
- **Q10:** Do you use the Routing Policy Specification Language (RPSL) to specify (your) routing policies?

C TESTBED CONFIGURATION

For the implementation of the security policy we applied the following configuration on the SCION testbed.

C.1 AS 59-65011 (rtr1) Beacon Propagation Policy Configuration

```
# /etc/scion/cs-1.toml
[general]
config_dir = "/etc/scion"
id = "cs-1"
reconnect_to_dispatcher = true

[metrics]
prometheus = "127.0.0.1:30454"

[path_db]
connection = "/var/lib/scion/cs-1.path.db"

[quic]
address = "127.0.0.1:30354"

[trust_db]
connection = "/var/lib/scion/cs-1.trust.db"

[beacon_db]
connection = "/var/lib/scion/cs-1.beacon.db"

[beaconing.policies]
propagation = "/etc/scion/beacon_policy.yaml"

[drkey.delegation]
colibri = [ "127.0.0.1",]

[drkey.lvl1_db]
connection = "/var/lib/scion/cs-1.lvl1.db"

[drkey.sv_db]
connection = "/var/lib/scion/cs-1.sv.db"

[log.console]
level = "debug"
```

Listing 1: Control Service Configuration File

```
# /etc/scion/beacon_policy.yaml
Filter:
  AsBlackList: ["0:0:47A"]
  AllowIsdLoop: false
Type: Propagation
```

Listing 2: Beacon Policy Configuration File

D TESTBED RESULTS

D.1 Blacklist AS Beacon Propagation Policy Logs

```
Jul 05 09:28:47 rp2-scion-rtr3 scion-control-service[73939]: 2023-07-05 09:28:47.969013+0000 DEBUG \
grpc/lookup.go:63 Received segment request {"debug_id": "88d41f37", "src": "59-0", "dst": "59-1146"}

Jul 05 09:28:47 rp2-scion-rtr3 scion-control-service[73939]: 2023-07-05 09:28:47.974672+0000 DEBUG \
messenger/addr.go:205 Sending SVC resolution request {"debug_id": "88d41f37", "req_id": "169ddd31", \
"request": {"Src":"59-1140","Dst":"59-1146","SegType":2}, "req_id": "54c7fd6a", \
"request": {"Src":"59-65000","Dst":"59-1140","SegType":3}, "isd_as": "59-65000", \
"svc": "CS A (0x0002)", "svcResFraction": 1.337}

Jul 05 09:28:47 rp2-scion-rtr3 scion-control-service[73939]: 2023-07-05 09:28:47.979613+0000 DEBUG \
messenger/addr.go:214

Jul 05 12:00:10 lego3 scion-control-service[419325]: 2023-07-05 12:00:10.645235+0000 DEBUG \
beaconing/writer.go:335 Successfully registered segment {"debug_id": "ae241e18", "seg_type": "down", \
"addr": "59-1140,CS A (0x0002)", "seg": "ID: 89adbbc621604dd384e387bb \
Timestamp: 2023-07-05 12:00:04+0000 Hops: 59-1140 4>4 59-1124 3>1 59-1146"}
```

Listing 3: Logs from the scion-control-service presenting requesting a path to AS 59-1146

```
scion showpaths 59-1146
Available paths to 59-1146
3 Hops:
[0] Hops: [59-65013 1>7 59-1124 3>1 59-1146] MTU: 9000 NextHop: 127.0.0.1:30001 \
    Status: alive LocalIP: 127.0.0.1
4 Hops:
[1] Hops: [59-65013 2>3 59-65011 1>5 59-1124 3>1 59-1146] MTU: 9000 NextHop: 127.0.0.1:30001 \
    Status: alive LocalIP: 127.0.0.1
[2] Hops: [59-65013 2>3 59-65011 2>3 59-65012 2>2 59-1146] MTU: 9000 NextHop: 127.0.0.1:30001 \
    Status: alive LocalIP: 127.0.0.1
5 Hops:
[3] Hops: [59-65013 2>3 59-65011 2>3 59-65012 1>6 59-1124 3>1 59-1146] MTU: 9000 \
    NextHop: 127.0.0.1:30001 Status: alive LocalIP: 127.0.0.1
```

Listing 4: The result of running the "scion showpaths 59-1146" command on AS 59-65013