Experiencing a new Internet Architecture

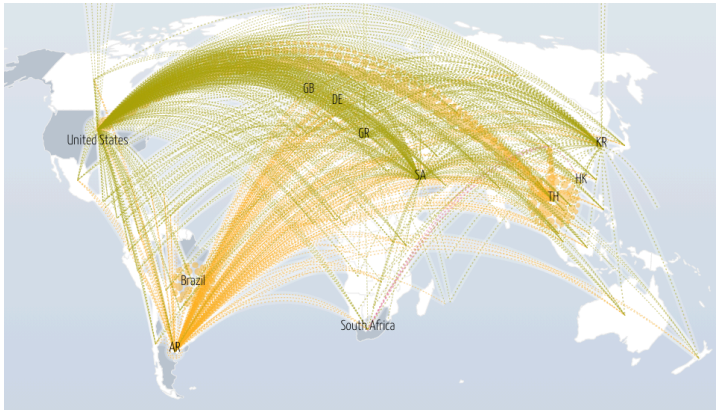
Adrian Perrig, Network Security Group

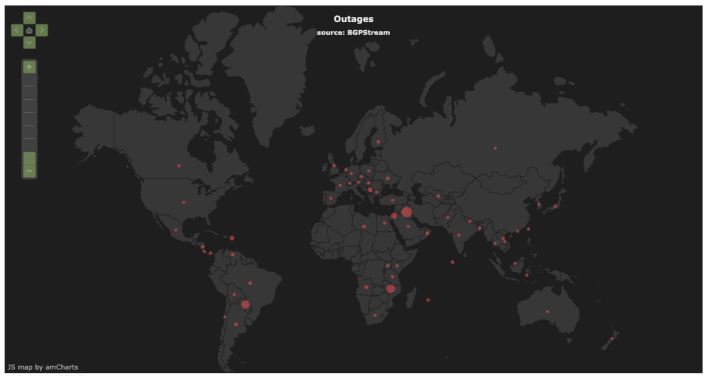
ETH zürich

SCION

The Internet is on Fire!

- Lack of sovereignty
- Frequent outages
  - https://downdetector.com
- Constant DDoS attacks
  - https://www.digitalattackmap.com
- Frequent routing attacks
  - https://bgpstream.com
- Lack of communication guarantees
- Expensive maintenance





All Events for BGP Stream.

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Possible Hijack		*Expected Origin AS:* ZOHO-EU, NL (AS 205111) *Detected Origin AS:* LVLT-3549, US (AS 3549)	2020-10-06 01:01:28		More detail
Possible Hijack		*Expected Origin AS:* ZOHO-EU, NL (AS 205111) *Detected Origin AS:* LVLT-3549, US (AS 3549)	2020-10-06 01:01:28		More detail
Outage		SWIFTNETBROADBAND-AS SWIFTNET BROADBAND PRIVATE LIMITED, IN (AS 133713)	2020-10-05 22:18:00	2020-10-05 22:22:00	More detail
Outage		U-LAN-AS, RU (AS 48128)	2020-10-05 21:24:00		More detail
Outage		TPODLASIE, PL (AS 39375)	2020-10-05 20:00:00	2020-10-05 20:52:00	More detail

ETH zürich

SCION

Inspirations for a New Beginning

- Many exciting next-generation Internet projects over the past 25 years
- General Future Internet Architectures (FIA)
  - XIA: enhance flexibility to accommodate future needs
  - MobilityFirst: empower rapid mobility
  - Nebula (ICING, SERVAL): support cloud computing
  - NIMROD: improved scale and flexibility
  - NewArch (FARA, NIRA, XCP)
  - RINA: clean API abstractions simplify architecture
- Content-centric FIAs: NDN, CCNx, PSIRP, SAIL / NETINF
- Routing security: BGPSEC, S-BGP, soBGP, psBGP, SPV, PGBGP, H-NPBR
- Path control: MIRO, Deflection, Path splicing, Pathlet, I3
- Inter-domain routing proposals: ChoiceNet, HLP, HAIR, RBF, AIP, POMO, ANA, ...
- Intra-domain / datacenter protocols: SDN, HALO, ...

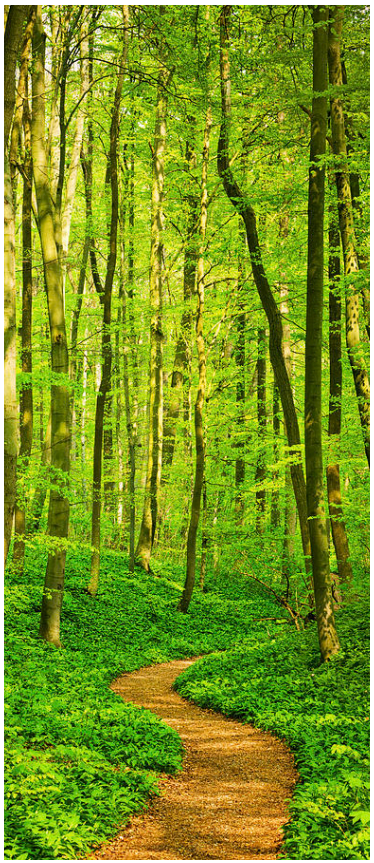
Why attempt redesigning Internet Architecture?

- We started our expedition asking the question:
  How secure can a global Internet be?
  - Answer: global communication guarantees can be achieved as long as a path of benign domain exists
- During our journey we discovered that path-aware networking and multi-path communication are powerful concepts that can provide higher efficiency than a single-path Internet
  - Enables path optimization depending on application needs
  - Simultaneous use of several paths unlocks additional bandwidth
- Explore new networking concepts without the constraints imposed by current infrastructure!

Discoveries on our Journey

- During our journey, we have encountered many interesting discoveries
- Several discoveries suggest new approaches for inter-domain networking

The real voyage of discovery consists not in seeking new landscapes, but in having new eyes. Marcel Proust



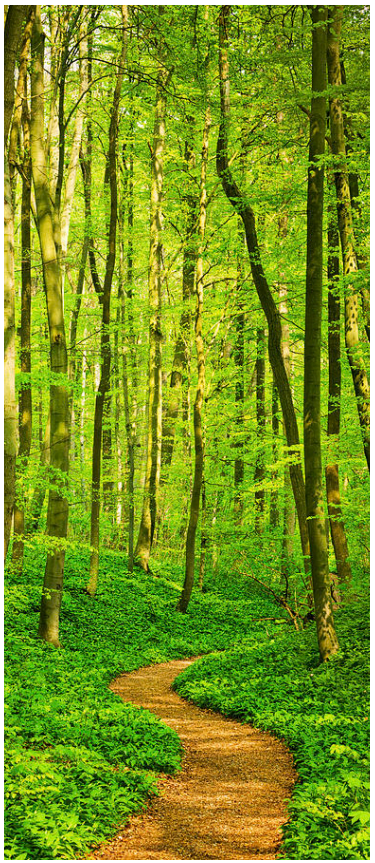
SCION Ambition: A Global Next-Generation Public Internet

SCION Architecture Principles

- Stateless packet forwarding (no inconsistent forwarding state)
- “Instant convergence” routing
- Path-aware networking
- Multi-path communication
- High security through design and formal verification
- Sovereignty and transparency for trust roots

Insight: Formal Security Verification Necessary

- To achieve strong assurance for a large-scale distributed system, formal security verification is necessary
- Performing formal verification from the beginning avoids “difficult-to-verify” components
  - Many design aspects of SCION facilitate formal verification
- Collaboration with David Basin’s and Peter Müller’s teams in the VerifiedSCION project

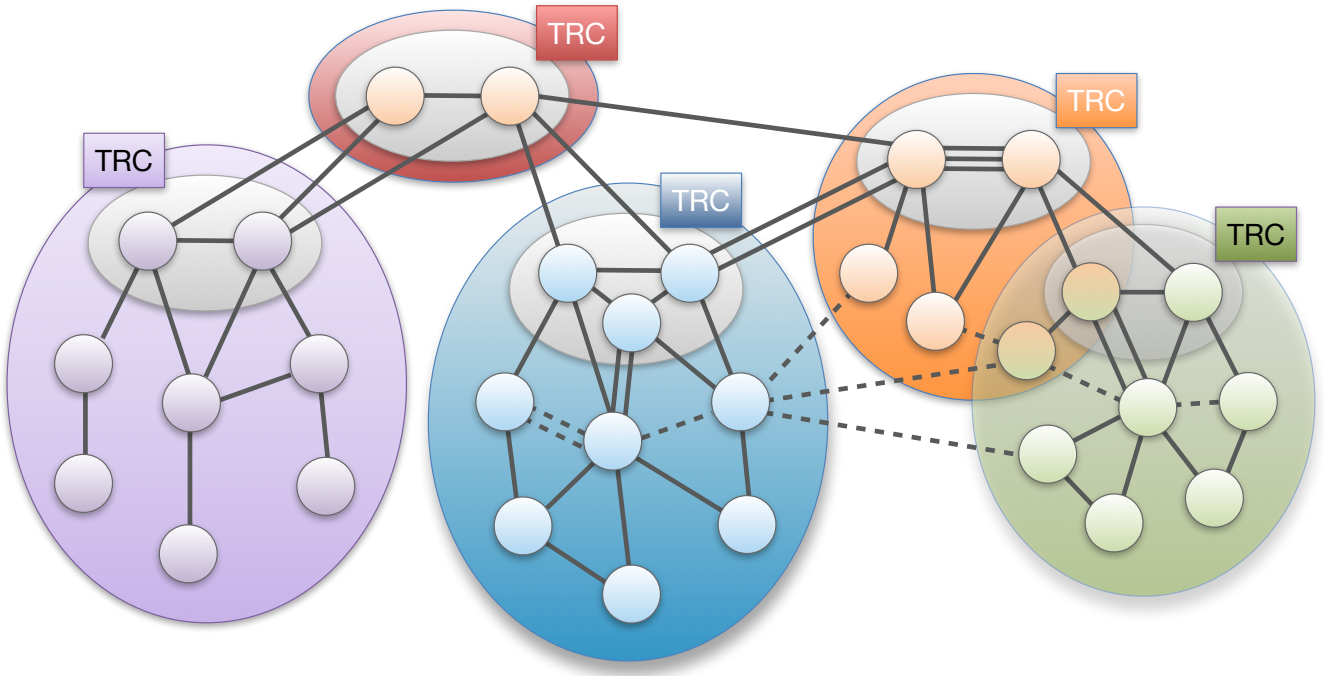


ETH zürich

VerifiedSCION

Approach for Scalability: Isolation Domain (ISD)

- Isolation Domain (ISD): grouping of Autonomous Systems (AS)
- ISD core: ASes that manage the ISD and provide global connectivity
- Core AS: AS that is part of ISD core



SCION Overview in One Slide

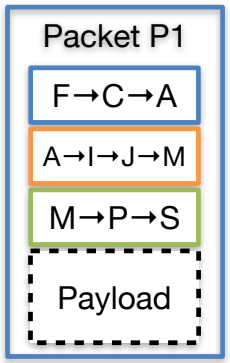
Path-based Network Architecture

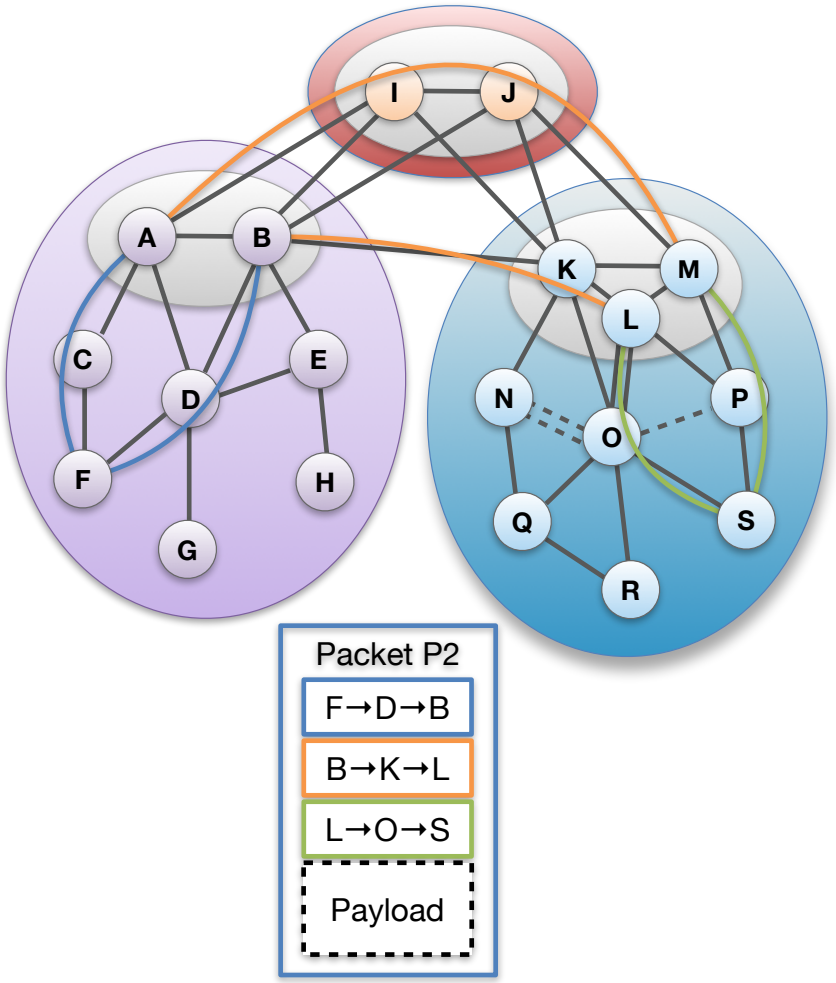
Control Plane - Routing

- Constructs and Disseminates Path Segments

Data Plane - Packet forwarding

- Combine Path Segments to Path
- Packets contain Path
- Routers forward packets based on Path
  - Simple routers, stateless operation

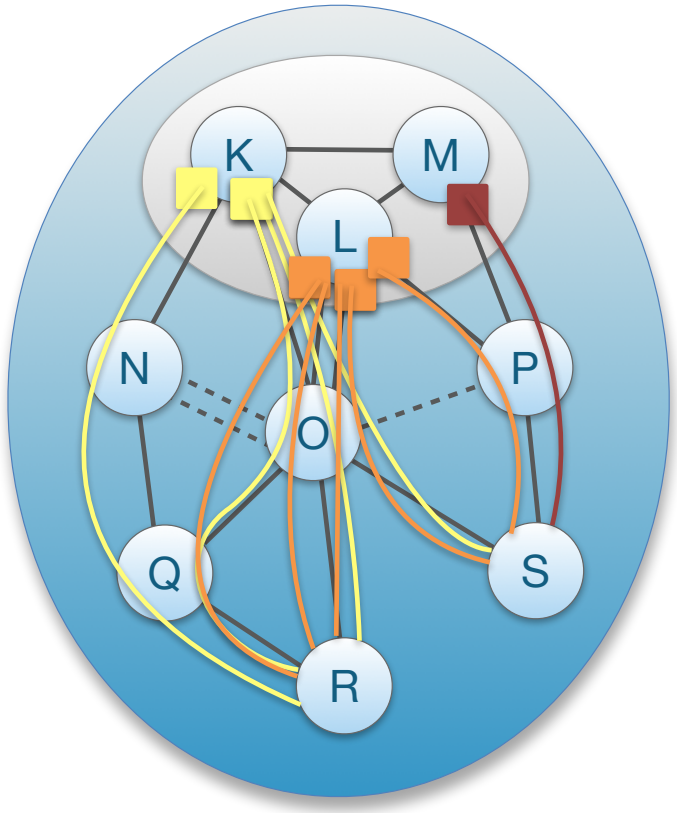




SCION

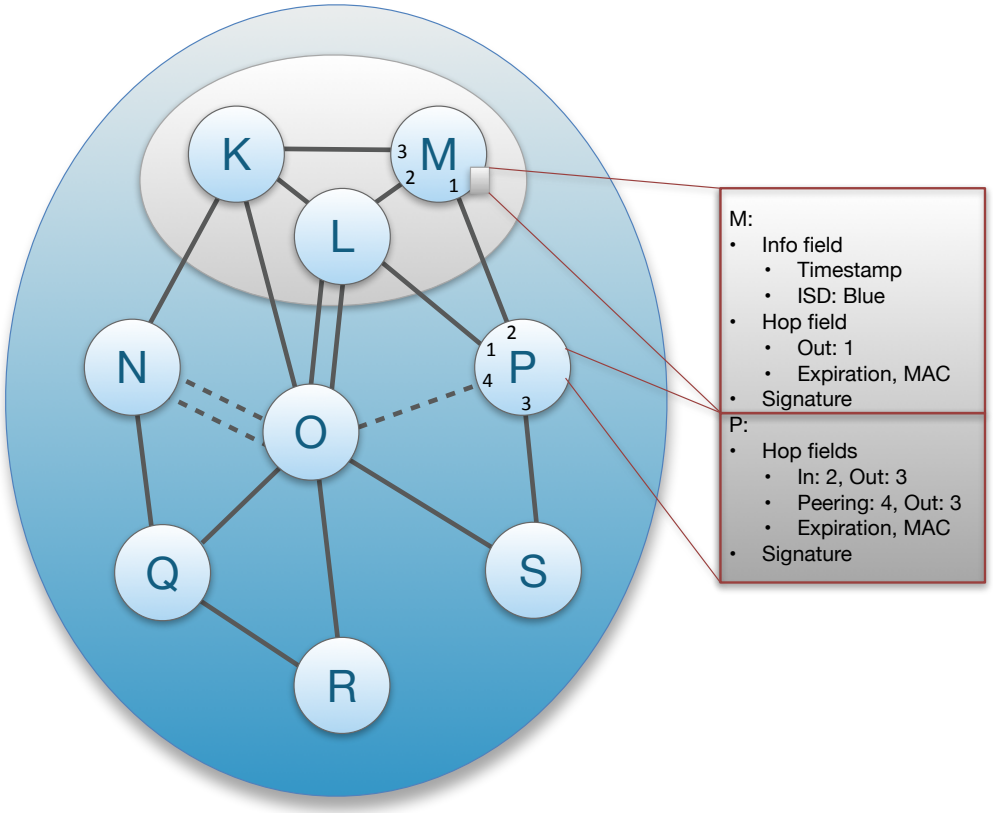
Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or "beacons"
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS



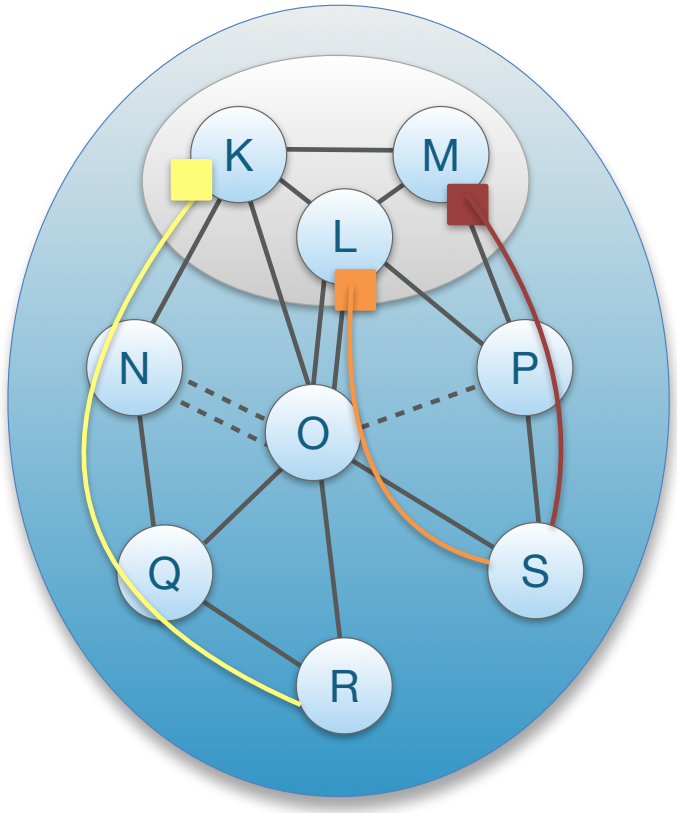
PCB Contents

- A PCB contains an info field with:
  - PCB creation time
- Each AS on path adds:
  - AS name
  - Hop field for data-plane forwarding
    - Link identifiers
    - Expiration time
    - Message Authentication Code (MAC)
  - AS signature

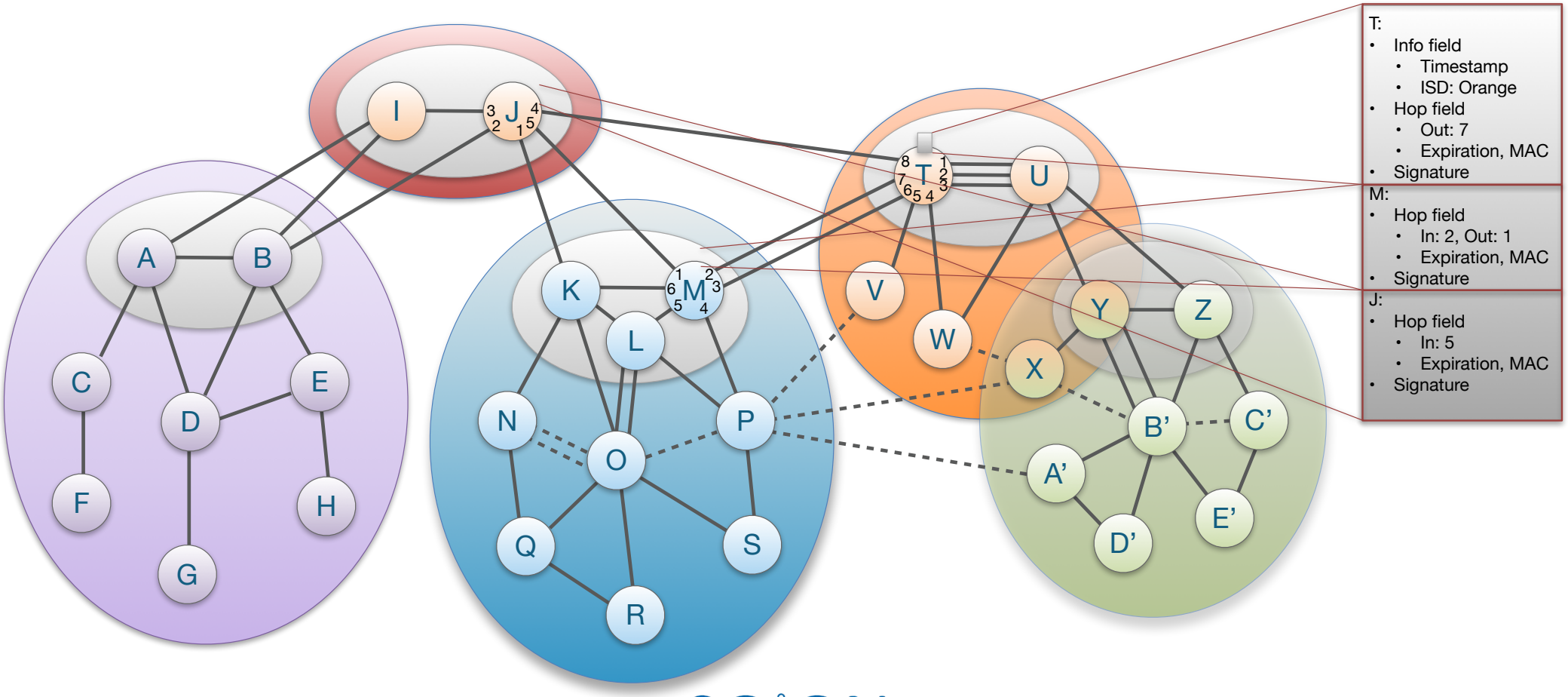


Up-Path and Down-Path Segments

- Intra-ISD beaconing process sends PCBs to ASes
- PCBs contain path segments that can be used as communication paths to communicate with the core AS that initiated it
- Up-path segment: PCB is used from AS to core AS
  - Example: R → K
- Down-path segment: PCB is used from core AS to AS
  - Example: M → S



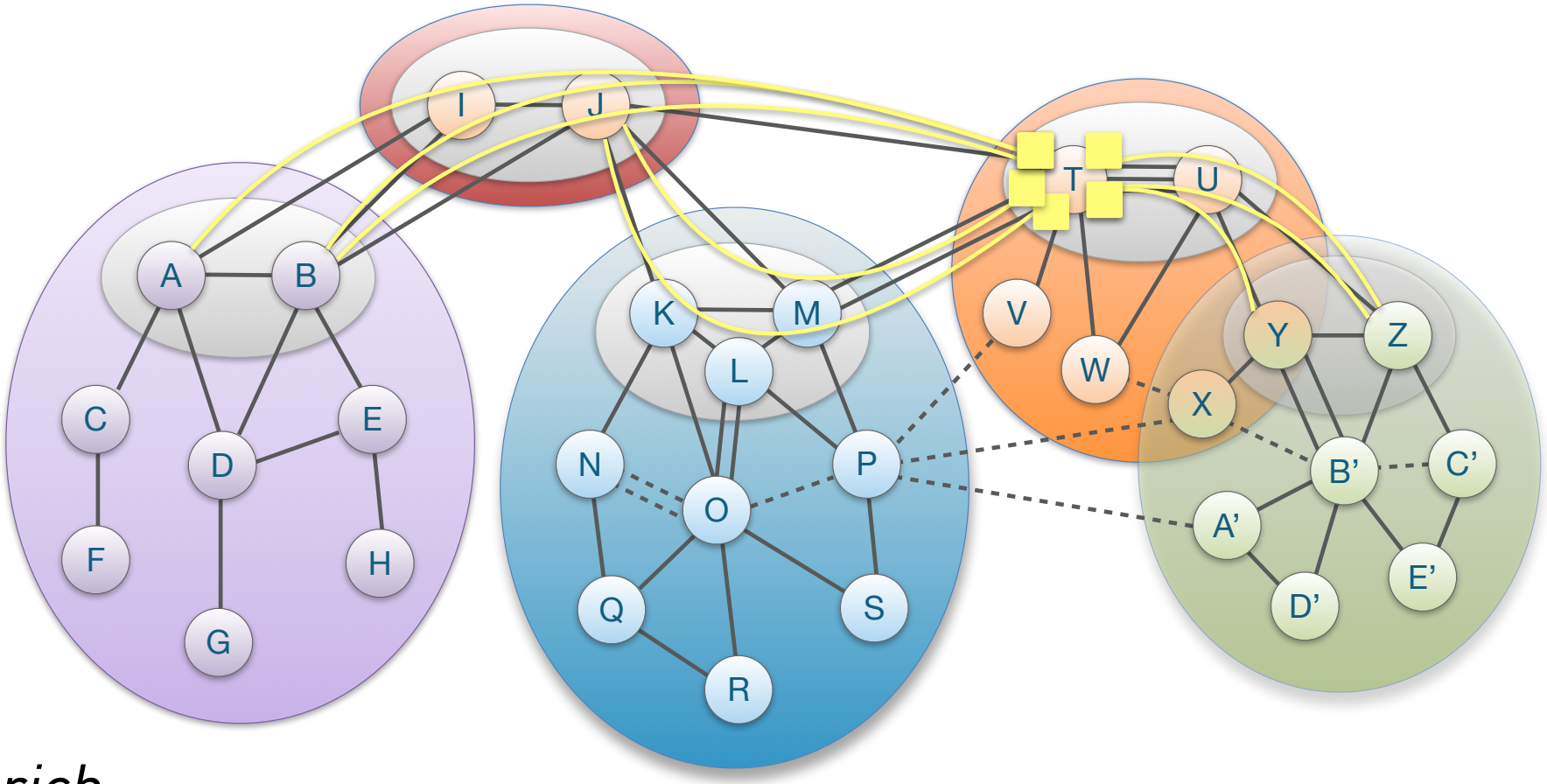
Core Beaconing for Inter-ISD Path Exploration



ETH zürich

SCION

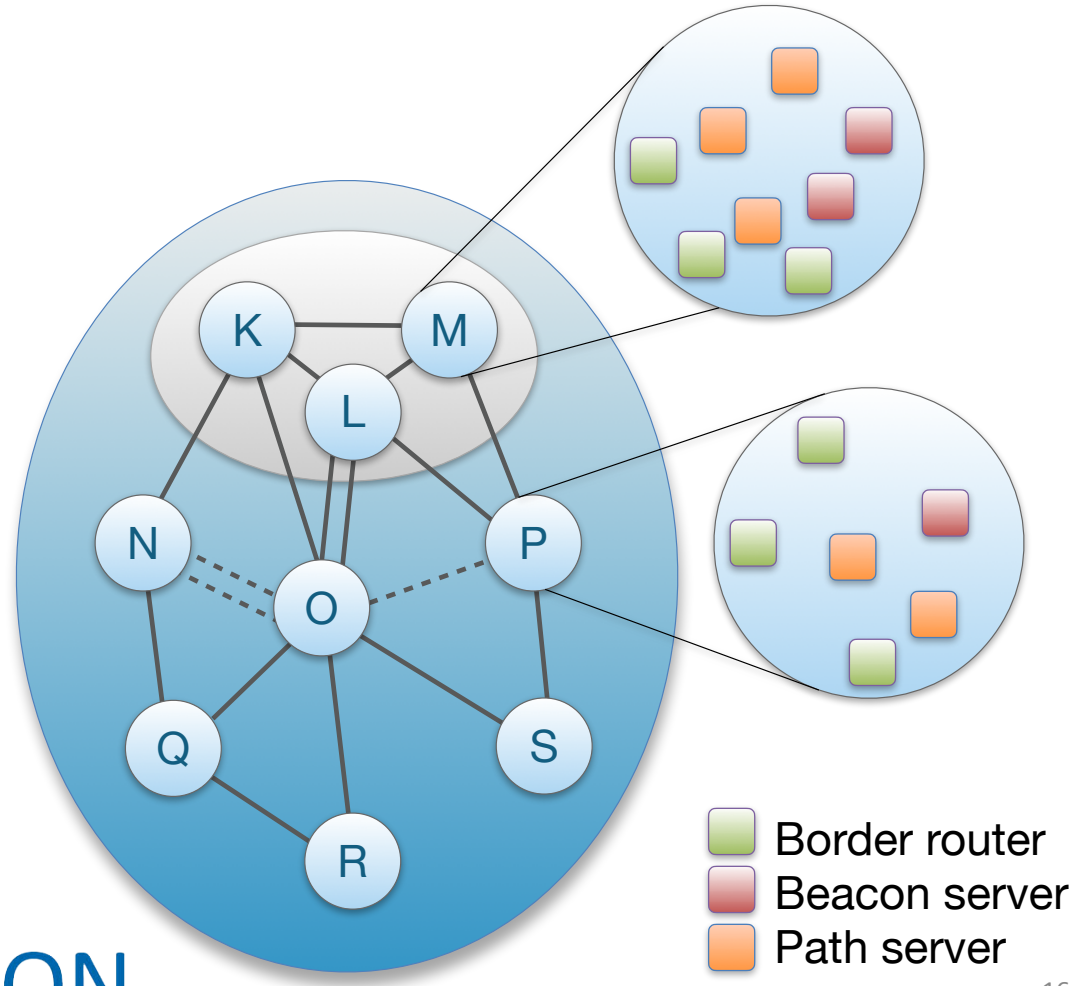
Inter-ISD Path Exploration: Sample Core-Path Segments from AS T



ETH zürich

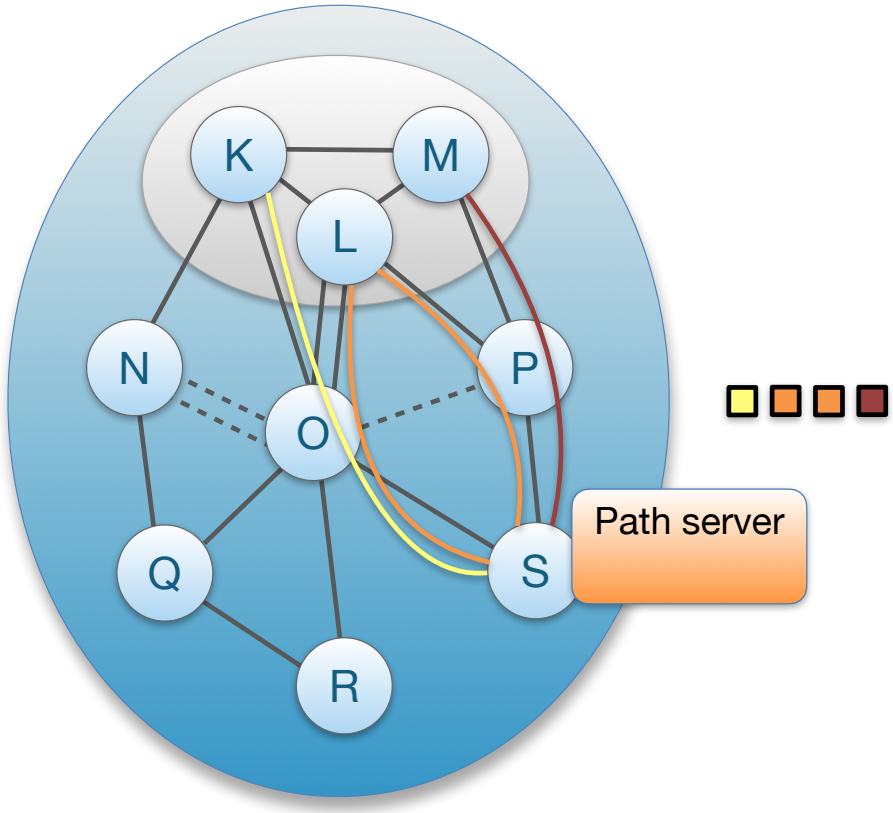
Path Server Infrastructure

- Path servers offer lookup service:
  - ISD, AS → down-path segments, core-path segments
  - Local up-path segment request → up-path segments to core ASes
- Core ASes operate core path server infrastructure
  - Consistent, replicated store of down-path segments and core-path segments
- Each non-core AS runs local path servers
  - Serves up-path segments to local clients
  - Resolves and caches response of remote AS lookups



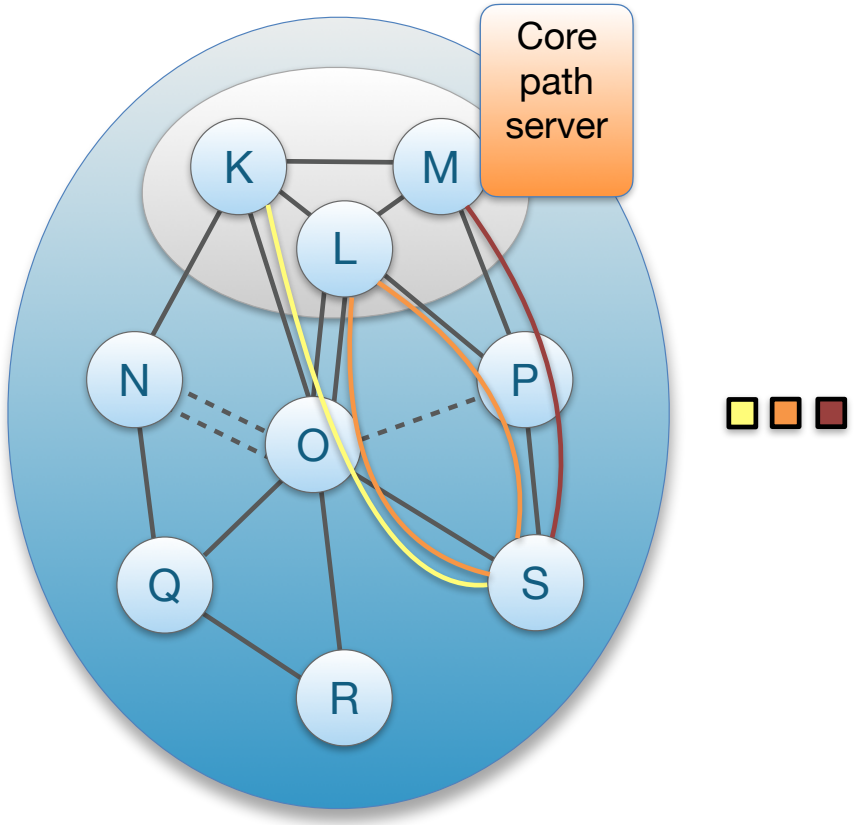
Up-Path Segment Registration

- AS selects path segments to announce as up-path segments for local hosts
- Up-path segments are registered at local path servers



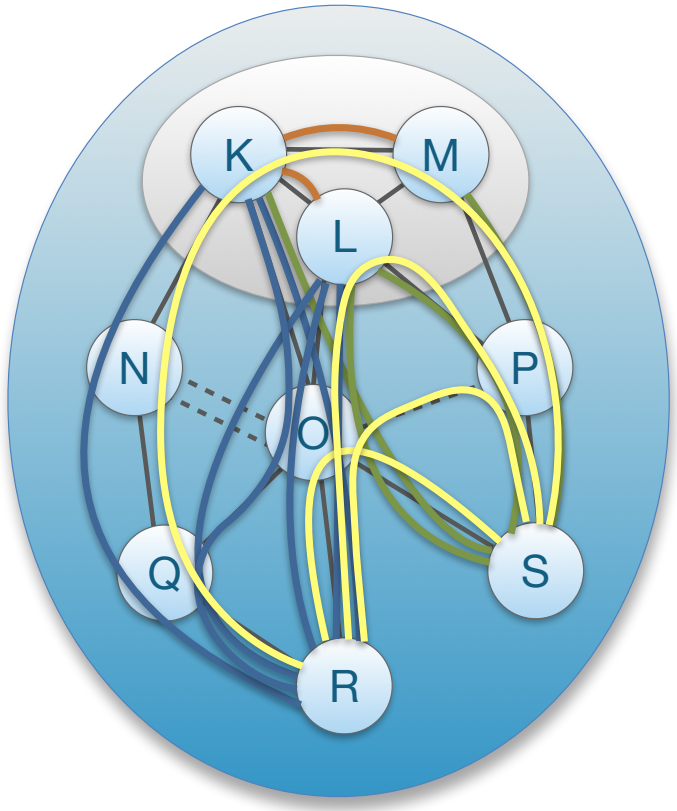
Down-Path Segment Registration

- AS selects path segments to announce as down-path segments for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS



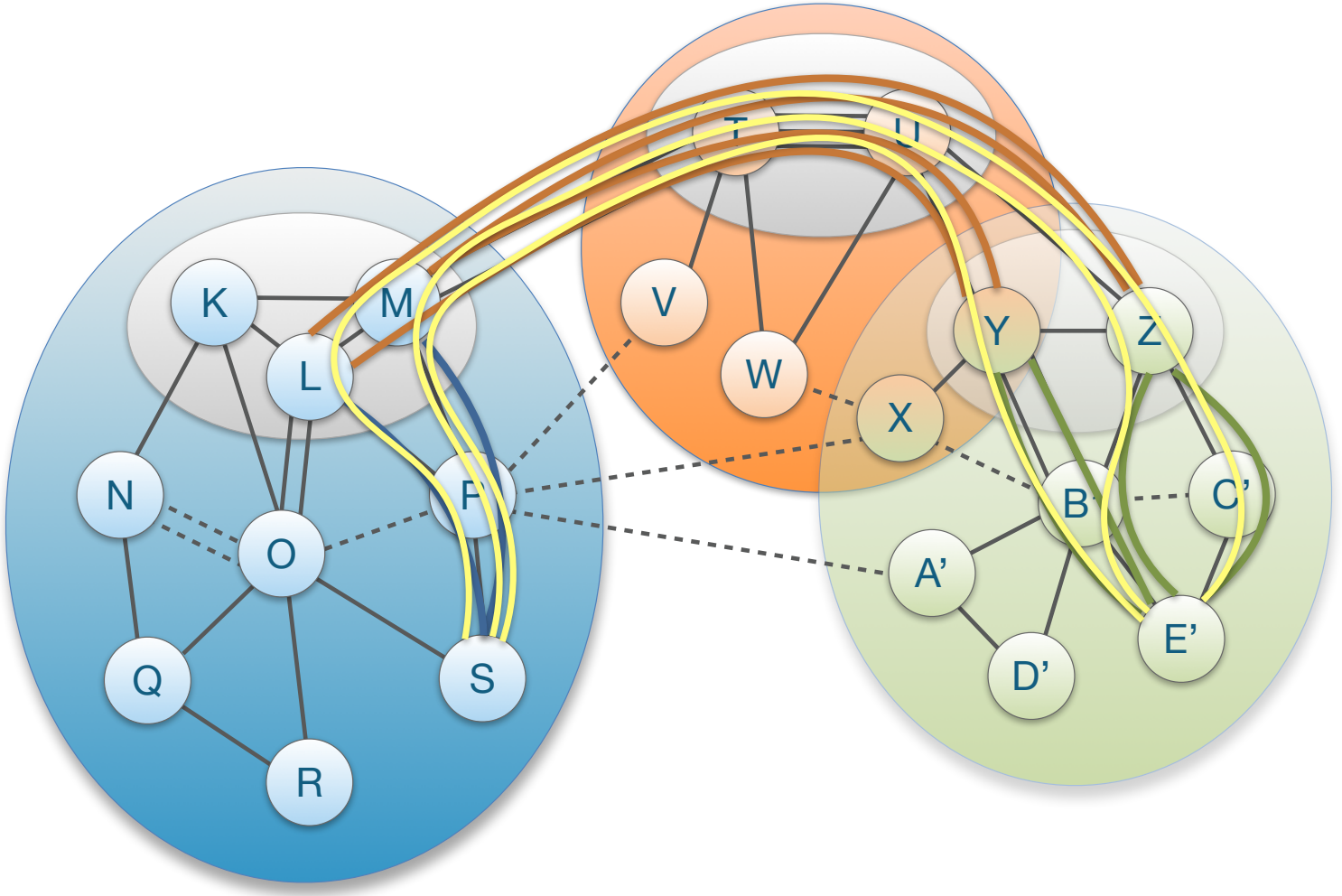
Communication within ISD

- Client obtains path segments
  - Up-path segments to local ISD core ASes (blue)
  - Down-path segments to destination (green)
  - Core-path segments as needed to connect up-path and down-path segments (orange)
- Client combines path segments to obtain end-to-end paths (yellow)



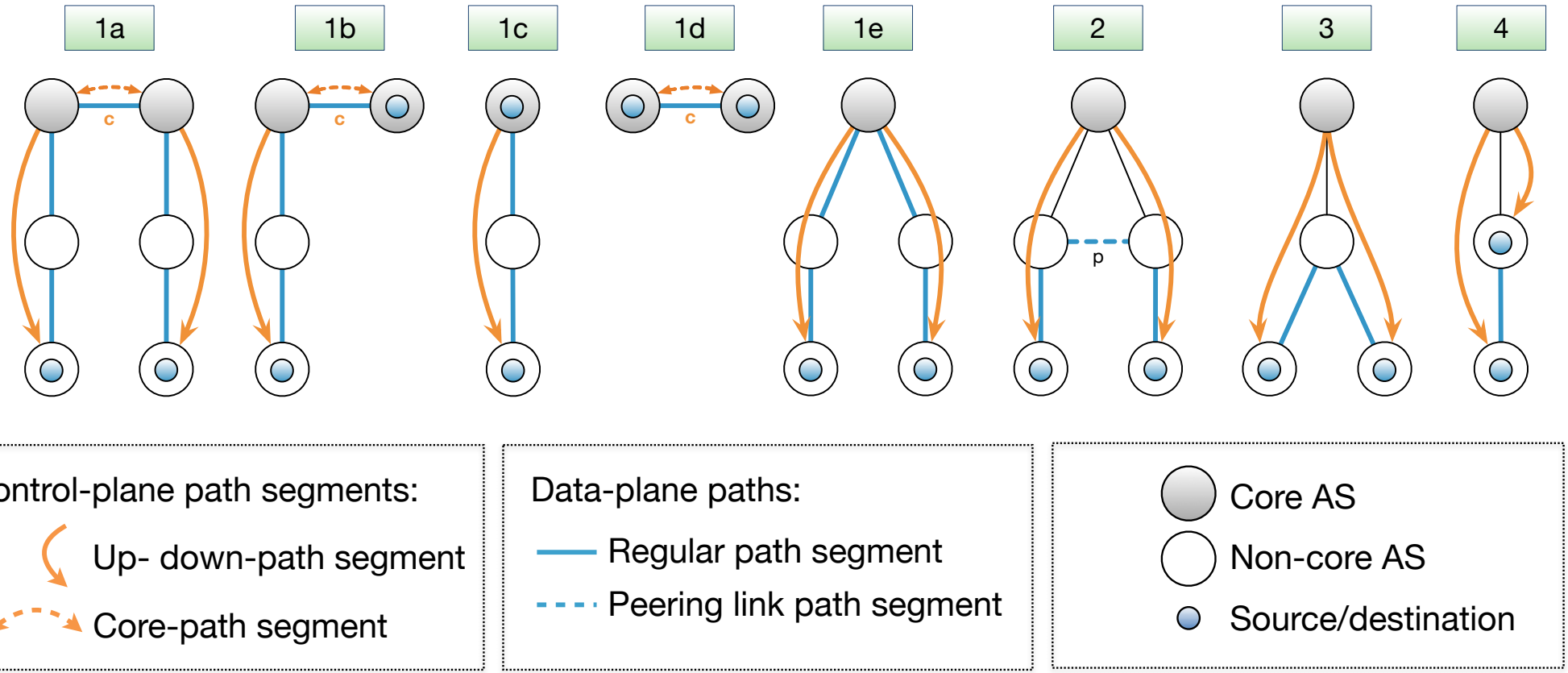
Communication to Remote ISD

- Host contacts local path server requesting <ISD, AS>
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-, core-, and down-segments



ETH zürich

Path Combination

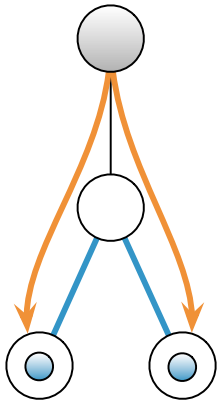


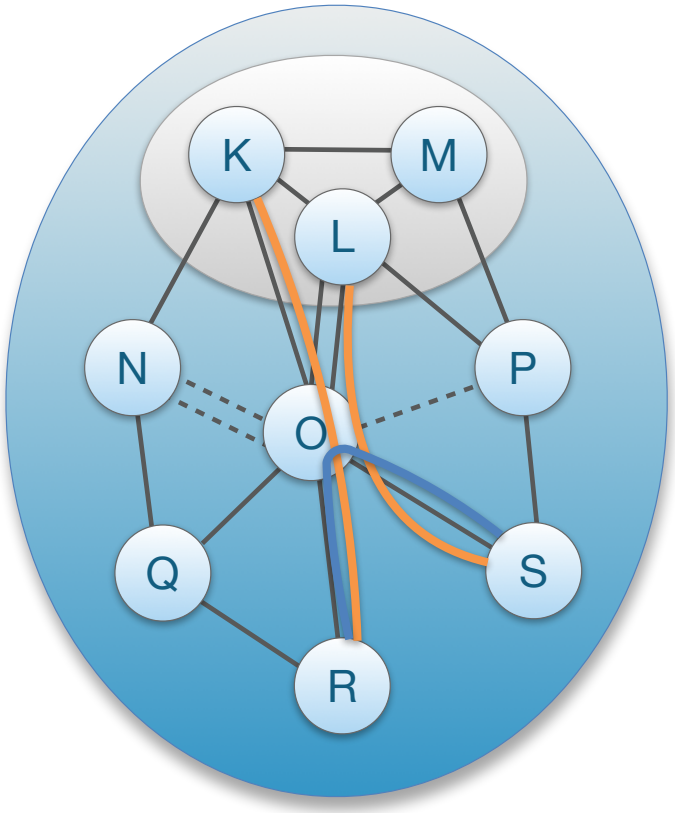
ETH zürich

SCION

Path Combination Example

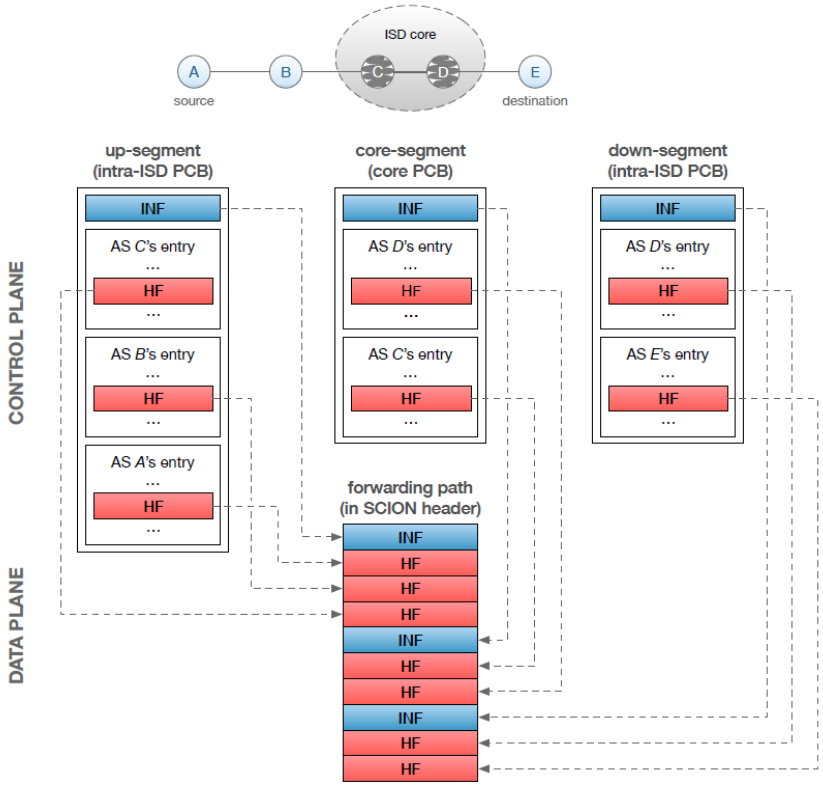
- AS shortcut path through common AS on up-path and down-path segment





SCION Control and Data Plane

- Three main functions of the control plane
  1. Path exploration → path segments
  2. Path dissemination → senders requests segments
  3. Certificate dissemination/renewal
     → needed for segment verification
- Path segments contain forwarding and meta information. Meta information can include geographical location of routers, MTU, bandwidth, link latency…
- Senders extract the forwarding information from the path segments to form complete end-to-end paths
- Forwarding information is encoded in the packet header. Routers only verify the authenticity of the information
  → two AES operations replace longest-prefix match



ETH zürich

SCION

SCION Drawbacks

Initial Latency Inflation

- ❖ Additional latency to obtain paths
- ✓ BUT amortized by caching & path reuse

Bandwidth Overhead

- ❖ Due to paths in the packets
- ❖ About 80 additional bytes
- ✓ Enables path control, simpler data plane, etc

Increased Complexity in Key Mgmt.

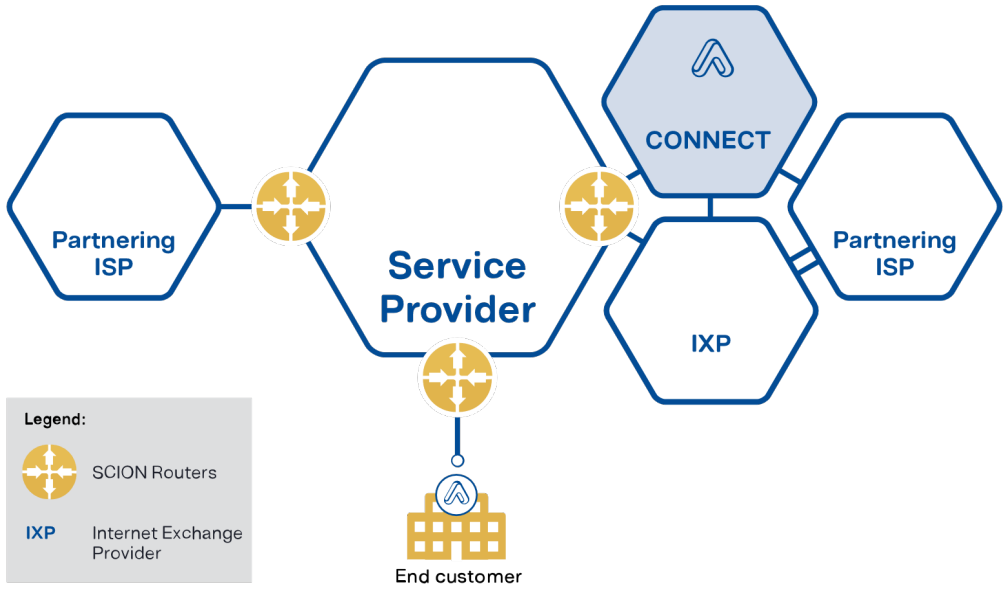
- ❖ New certificates (e.g., TRC Certificates)
- ✓ High security design

Initial Set-up Cost

- ❖ Training network operators
- ❖ Installing new infrastructures
- ✓ Offers methods to facilitate deployment

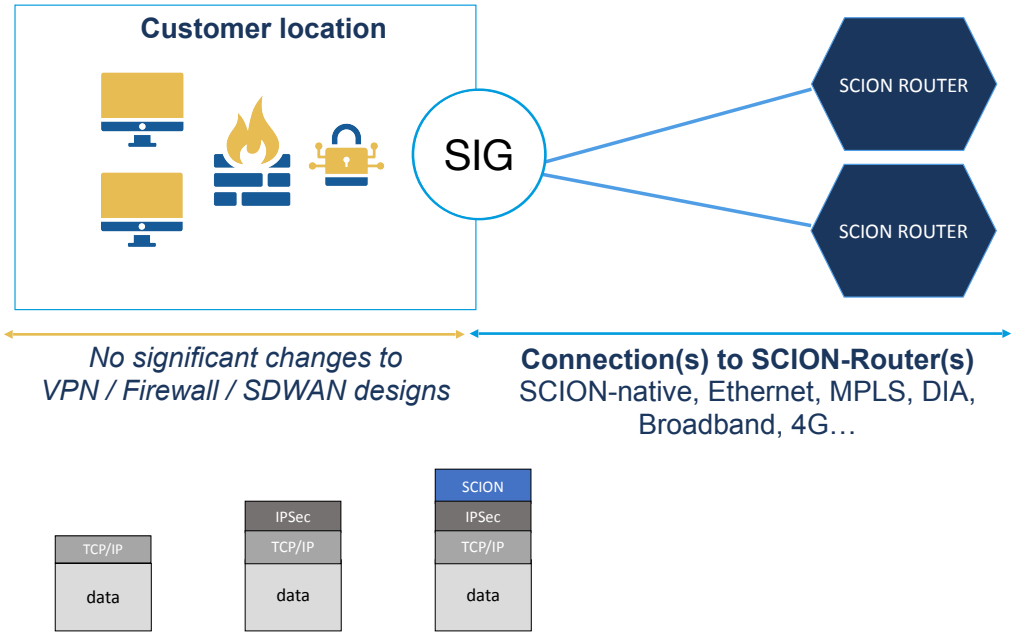
How to Deploy SCION: ISP

- CORE Routers are set up at the borders of an ISP
  - to peer with other SCION-enabled networks
  - to collect customer accesses
- No change to the internal network infrastructure of an ISP needed!



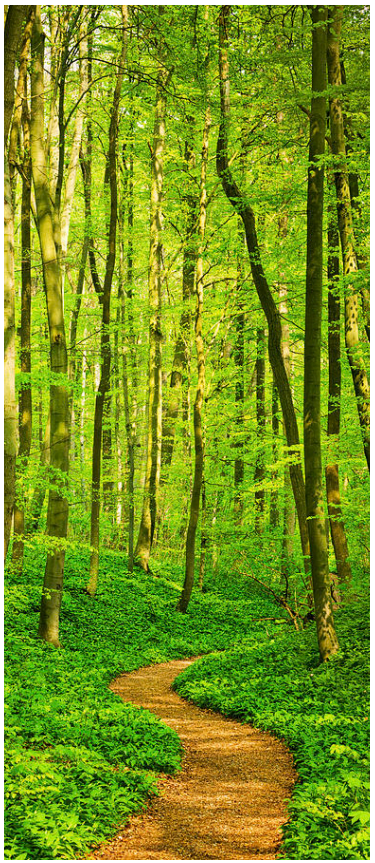
How to Deploy SCION: End Domain

- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed



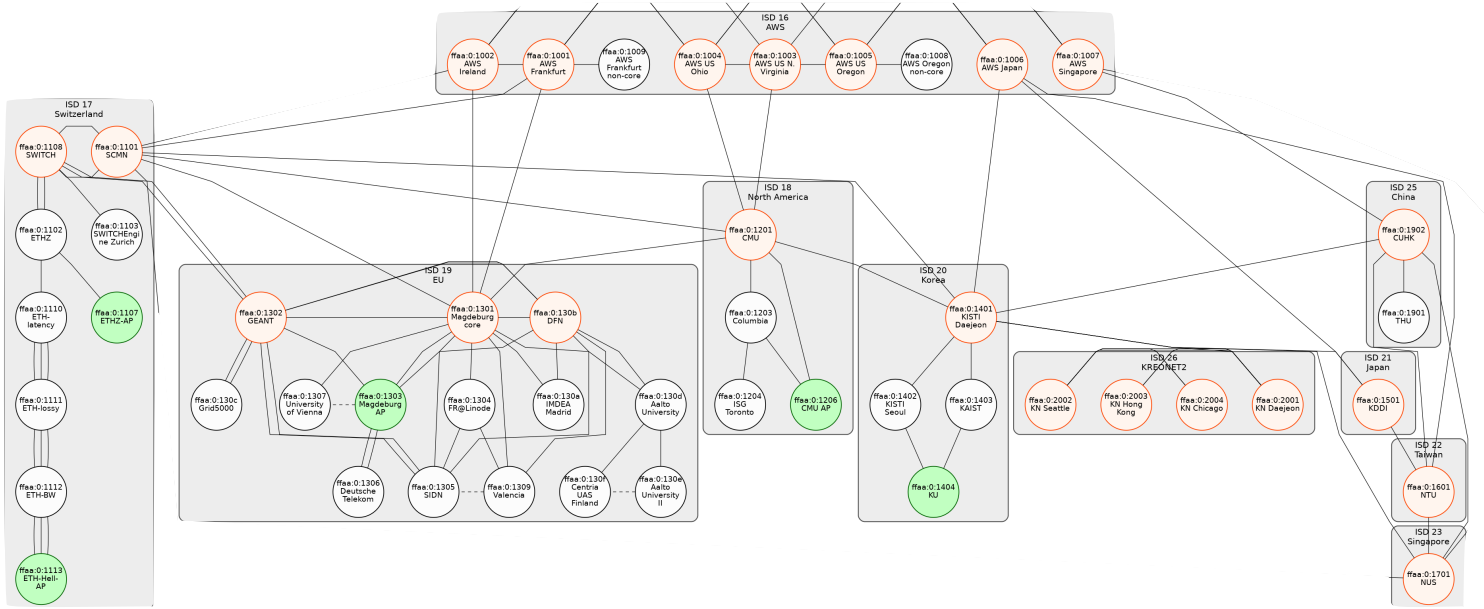
Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP
- For ISPs, new architecture can be deployed with minimal effort
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts
- Important: no reliance on BGP for inter-domain operation ("BGP-free")
  - Overlay / insecure underlay should be avoided not to inherit vulnerabilities
- Re-use of intra-domain network architecture for local communication



SCIONLab

- Global SCION research testbed: https://www.scionlab.org
- Collaboration with David Hausheer's team at University of Magdeburg
- Open to everyone: create and connect your own AS within minutes
- ISPs: Swisscom, SWITCH, KDDI, GEANT, DFN
- Deployed 35+ permanent ASes worldwide, 600+ user ASes
  - Contact us to become an infrastructure AS, we can provide HW
- Kwon et al., "SCIONLab: A Next-Generation Internet Testbed", ICNP 2020



Exciting SCIONLab Research Opportunities

- Next-generation Internet architecture research
- Users obtain real ASes with cryptographic credentials to participate in the control plane
- Path-aware networking testbed
- Hidden paths for secure IoT operation
- Network availability and performance measurement (bandwidth and latency)
- Supported features (PKI, DDoS defense mechanisms, path selection support, end host / application support)
- Inter-domain routing scalability research, next-generation routing architecture policy definitions
- Multi-path research
- Multi-path QUIC socket
- End-to-end PKI system enables building highly secure TLS applications
- Colibri inter-domain resource allocation system
- DDoS defense research using in-network defense mechanisms

SCION is reality today

- 11+ years of research, 150+ person-years of effort
- In production use by large Swiss bank since Aug 2017
- 8 ISPs offer SCION connectivity: Anapaya, Axpo, GEANT, Init7, LG (South Korea), Swisscom, Sunrise, SWITCH
- Swiss secure finance network is under development
- Anapaya has built global SCION backbone, with global connectivity (www.anapaya.net)

SCION

Three SCION Project Research Thrusts

- **Thrust I: Security**
  - Sovereignty
  - Transparency
  - Routing security
  - DDoS resilience
  - Secure web connectivity (PKI)
  - Formal verification of protocols and code

- **Thrust II: Efficiency**
  - Higher network capacity
  - Low-latency paths
  - High-bandwidth paths
  - Simultaneous use of multiple links
  - Fast failover
  - High-speed firewall

- **Thrust III: Green net**
  - Energy reduction vs. current Internet
  - More efficient forwarding
  - Use idle backup links
  - Improved network utilization
  - QoS savings (zero-loss, limited ACKs)

ETH zürich

SCION

Online Resources

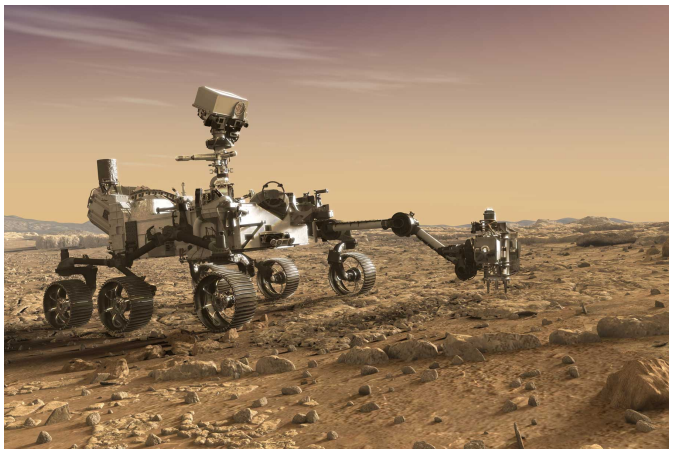
- https://www.scion-architecture.net
  - Book, papers, videos, tutorials
- https://www.scionlab.org
  - SCIONLab testbed infrastructure
- https://www.anapaya.net
  - SCION commercialization
- https://github.com/scionproto/scion
  - Source code

SCION Summary

- SCION: Next-generation Internet you can use today!
- High-performance
  - Path-aware network enables application-specific optimizations to provide enhanced efficiency
  - Multi-path communication enables simultaneous use of multiple paths, increasing available bandwidth
- Secure, high assurance, high availability
  - Per-packet authentication verification possible on routers
  - Formal verification of protocols and code
  - Immune against routing attacks, e.g., BGP prefix hijacking

Interesting Encounters on our Expedition

- Security
  - Global communication guarantees are possible
  - High-speed crypto enables line-rate processing
- Networking
  - Multi-path routing is a necessity, not a luxury
  - Global QoS is viable



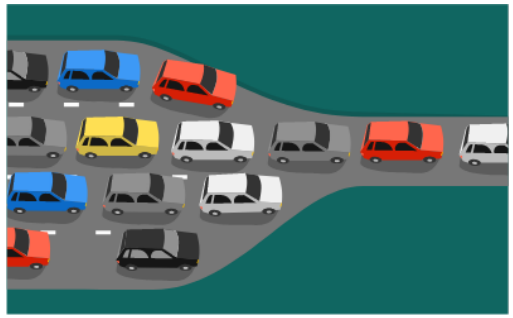
Global Communication Guarantees in the Presence of Adversaries

- Goal: If (routing policy compliant) path of benign ASes exists (with operational infrastructure), a sender can find, use, and achieve minimum bandwidth guarantees on that path
- Challenges
  - Network routing instabilities, misconfigurations, etc.
  - DoS attacks at various levels (control plane, data plane, end host)

Observation: Stable Forwarding + Multi-path Necessary

- Single-path forwarding cannot achieve strong availability guarantees
  - During routing protocol convergence, no path may be available
  - Equipment failure on path will result in unavailability until routing protocol updates and forwarding tables are adjusted
  - If forwarding path experiences high packet loss, then path is not usable for practical applications
- Approaches
  - Stable forwarding: packet-carried forwarding state protects forwarding from routing instabilities
  - Multi-path ensures presence of several paths, so as long as a single path works, end-to-end connectivity is assured

Bottleneck Routing Disrupts Availability



- Routing protocol switches route traversing a link with limited capacity (= bottleneck link)
- Bottleneck link traversal results in high packet loss
- Applications cannot operate and lose connectivity
- Since connectivity exists, often manual intervention needed to switch back to alternate path, outage typically persists for 30+ minutes
- Frequent reason for outage, caused by misconfiguration or attack

Cloudflare DNS goes down, taking a large piece of the internet with it

Devin Coldewey @techcrunch / 11:50 pm CEST • July 17, 2020 Comment

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."

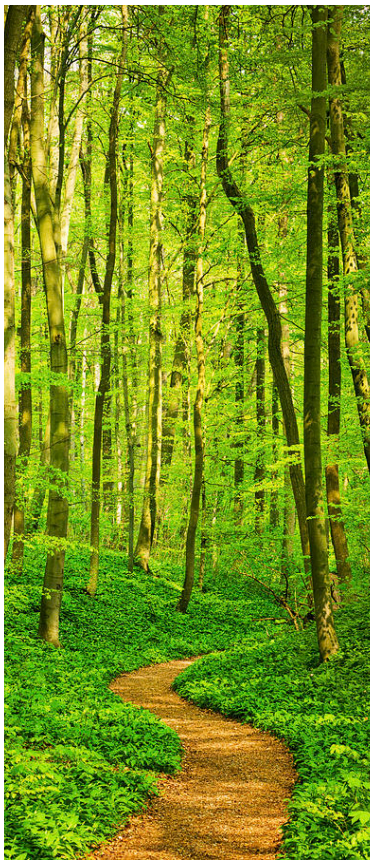
By Catalin Cimpanu for Zero Day | June 7, 2019 -- 19:41 GMT (20:41 BST) | Topic: Security

Announcement of Failed Routes

- In some cases, networks continue to announce routes that failed
- Example: August 30 CenturyLink/Level(3) Outage
  https://blog.cloudflare.com/analysis-of-todays-centurylink-level-3-outage
  "CenturyLink/Level(3)'s network was not honoring route withdrawals and continued to advertise routes to networks like Cloudflare's even after they'd been withdrawn"

Insight: Secure Routing Insufficient

- Secure routing protocol cannot prevent outages caused by bottleneck link or continuing announcement of failed or congested routes, as announcement in these cases is legitimate



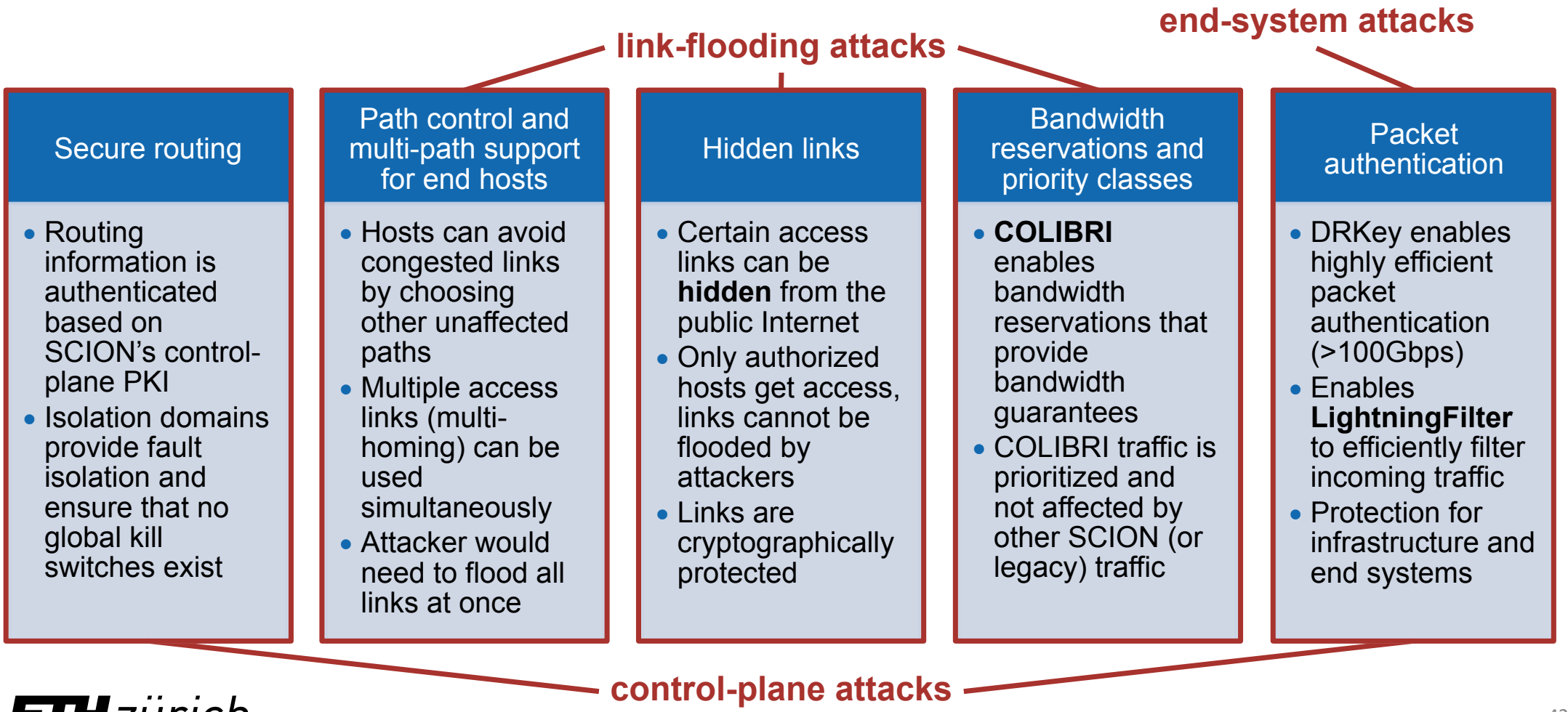
Global Communication Guarantees in the Presence of Adversaries

- Goal: If (routing policy compliant) path of benign ASes exists (with operational infrastructure), a sender can find, use, and achieve minimum bandwidth guarantees on that path
- Challenges
  - Network routing instabilities, misconfigurations, etc.
  - DoS attacks at various levels (control plane, data plane, end host)

Availability in a public Internet is threatened by different types of DoS attacks

Link-flooding attacks	Attacker floods network links with excessive amount of traffic
	Can target **access links** (last mile) or **core links** in the network
	Often executed using botnets and/or amplification techniques
End-system attacks	Attacker exhausts **computational** or **memory resources** of victim
	Often possible due to other defense mechanisms such as firewalls
	Examples: **state exhaustion**, **signature flooding**
Control-plane attacks	Attacker disrupts important **control-plane mechanisms** or **access to services**
	Services are essential for a functioning network
	Examples in SCION: beacon server, path server, certificate server

SCION is an Internet architecture with both *strong security* properties and *high availability*



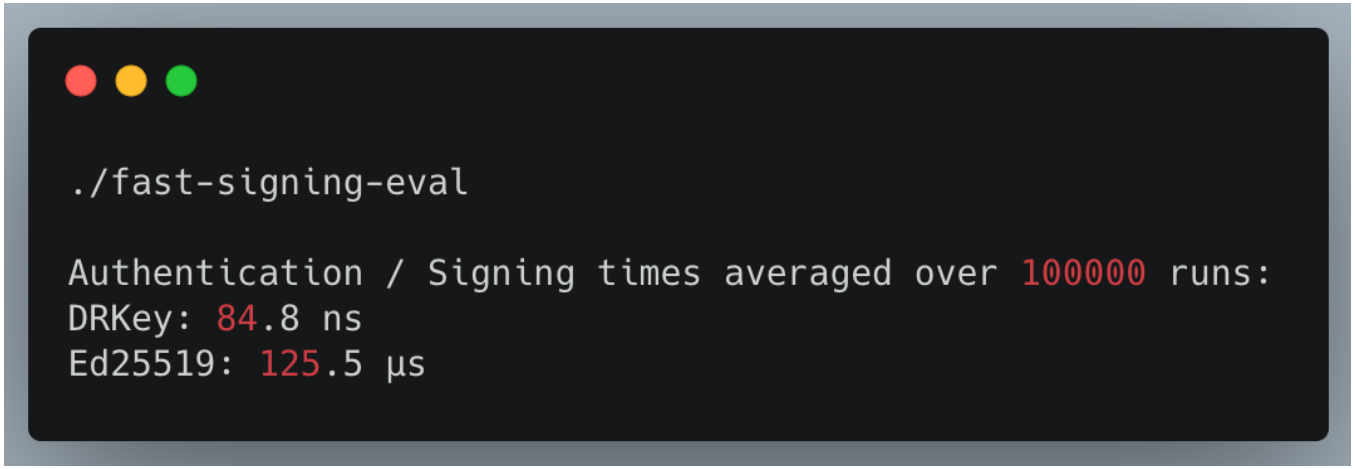
High-Speed Packet Processing

- Current high-speed Internet links: 400Gbit/s (Gbps)
- Arrival rate for 64-byte packets: one packet every 1.3 ns
- High-speed asymmetric signature implementation: Ed25519
  SUPERCOP REF10: ~ 100μs per signature
- AES-NI instruction only requires 30 cycles: ~ 10ns
- Memory lookup from DRAM requires ~ 200 cycles: ~ 70ns
- Symmetric crypto enables high-speed processing through parallel processing and pipelining

DRKey & Control-Plane PKI

- SCION offers a global framework for authentication and key establishment for secure network operations
- Control-pane PKI
  - Sovereign operation thanks to ISD concept
  - Every AS has a public-key certificate, enabling AS authentication
- DRKey
  - High-speed key establishment (within ~20 ns), enabling powerful DDoS defense mechanisms
- PISKES: Pragmatic Internet-Scale Key-Establishment System, Rothenberger et al., ACM Asia Conference on Computer and Communications Security (ASIACCS) 2020

Avoid Asymmetric Crypto for High Performance



Factor:
~ 1450x

ETH zürich

SCION

Dynamically Recreatable Key (DRKey)

- ***Idea***: use a per-AS secret value to derive keys with an efficient Pseudo-Random Function (PRF)
- Example: AS X creates a key for AS Y using secret value SV_X
  - $K_{X \rightarrow Y} = PRF_{SVx}$ ("Y")
  - Intel AES-NI instructions enable PRF computation within 30 cycles, or 70 cycles for CMAC
    Key computation is ~7 times faster than DRAM key lookup!
  - Any entity in AS X knowing secret value SV_X can derive $K_{X \rightarrow *}$

Notation Explanation

- Notation: $K_{X \rightarrow Y}$
  - Arrow indicates direction of key derivation, **not** the direction of communication
- Asymmetry in derivation
  - Entities in AS X can derive key based on a single local key (efficient (tens of nanoseconds), stateless)
  - Entities in AS Y need to contact local key server to fetch key (hundreds of microseconds, stateful)

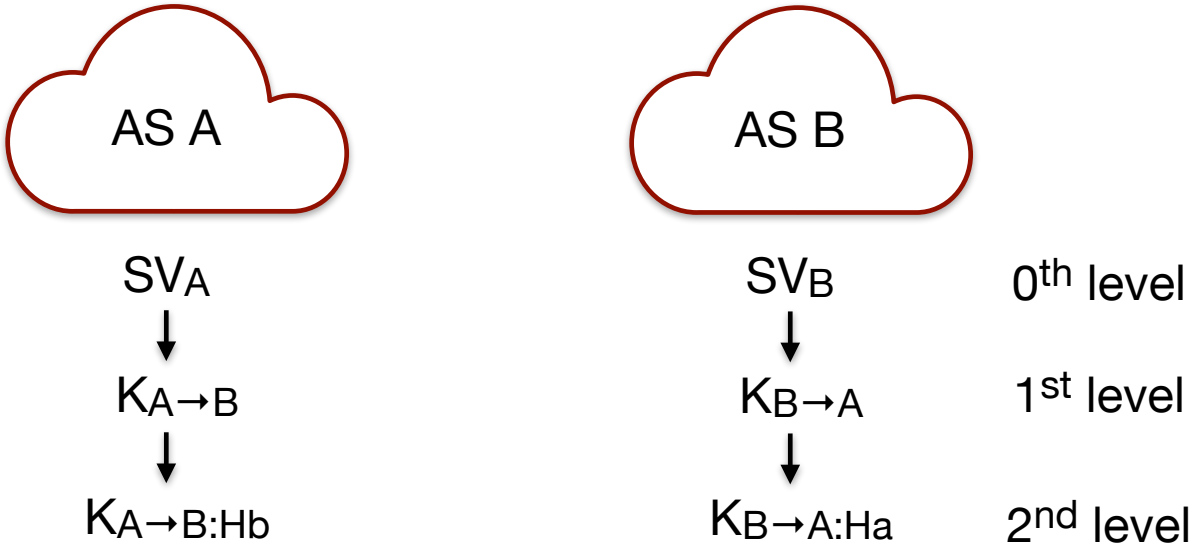
Key Server Infrastructure

- Key servers that are deployed in each AS build backbone of key hierarchy
  - Responsible for key exchange, local key establishment and key management

- After AS-level keys are established, symmetric keys for end hosts can be provided using key derivation
- Keys can be used to provide source authenticity of packet without costly key exchange between communicating parties
- Each host is required to contact their *local* key server

Key Hierarchy

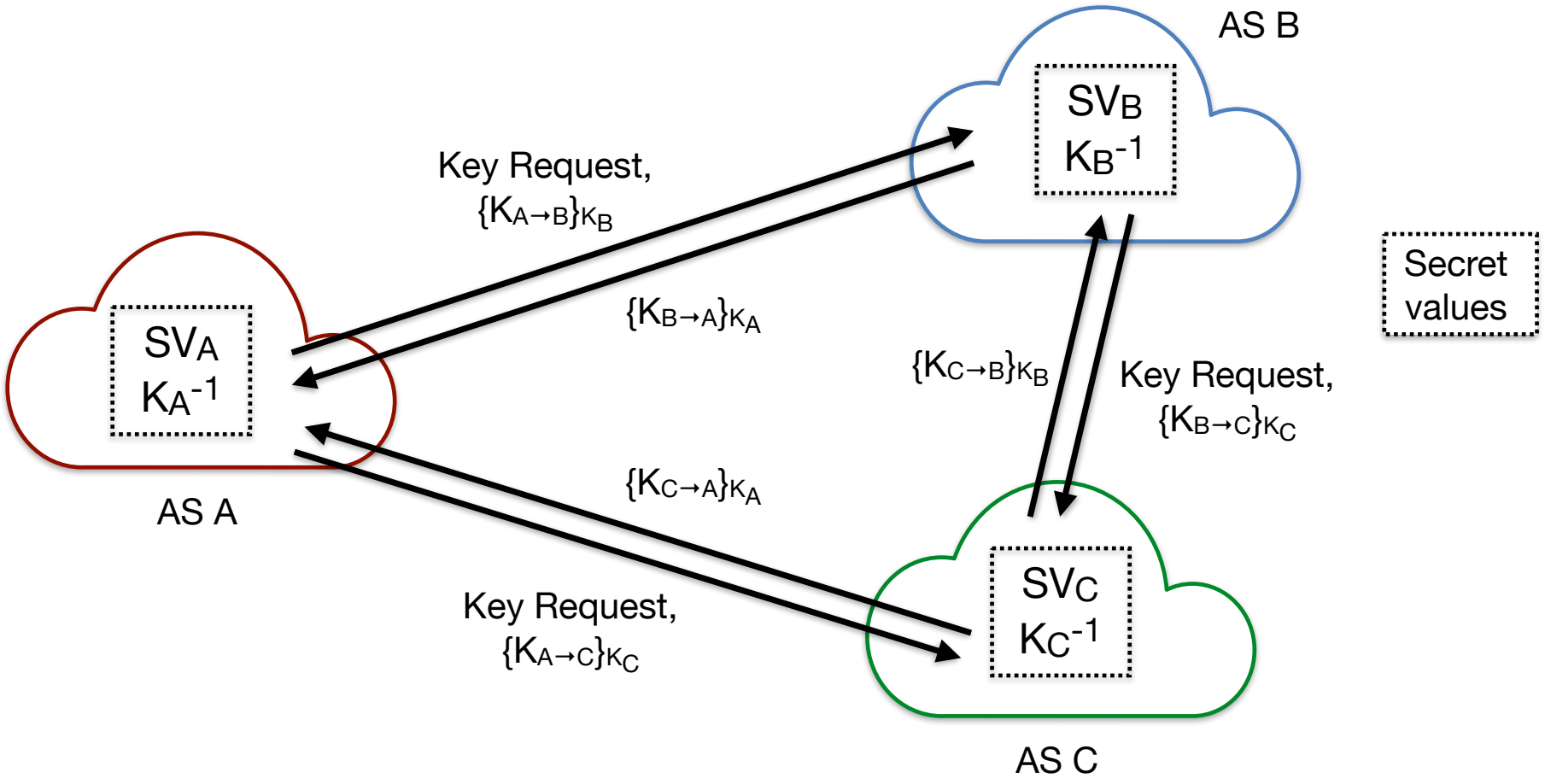
- AS A creates key hierarchy from secret value A (SV_A) using a pseudo-random function (PRF): $K_{A \rightarrow B} = PRF_{SVA}$ (“B”)
- Similarly, AS B creates key hierarchy based on SV_B



ETH zürich

SCION

First-level Key Exchange



ETH zürich

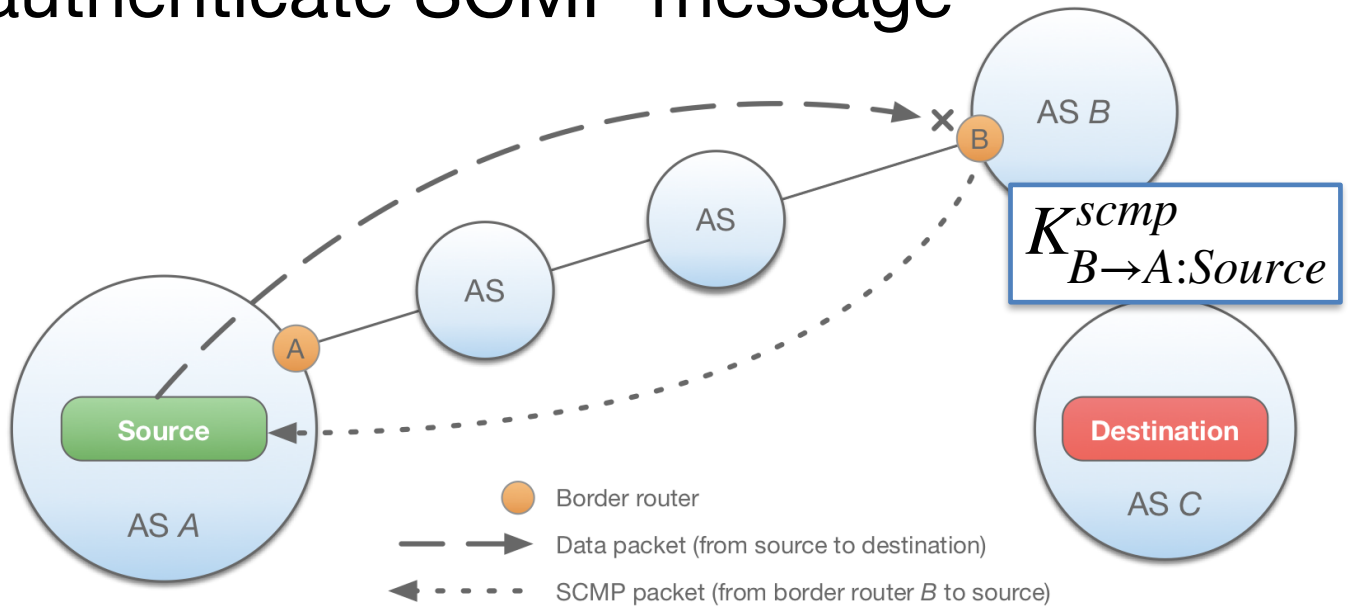
SCION

Second-level DRKey

- ***Idea***: apply PRF once more on AS-to-AS key to derive AS-to-Host symmetric key
- Example: AS X creates a key for Host H in AS Y
  - $K_{X \rightarrow Y} = PRF_{SVx}$ (“Y”)
  - $K_{X \rightarrow Y:H} = PRF_{Kx \rightarrow y}$ (“H”)
- Knowing secret value SV_X any entity in AS X can derive $K_{X \rightarrow *:*}$
- Knowing $K_{X \rightarrow Y}$, key server in AS Y can derive $K_{X \rightarrow Y:*}$
- Host-to-Host keys $K_{X:* \rightarrow Y:*}$ can be similarly derived

DRKey Use Case: SCMP Authentication

- Border router in AS B can derive key $K^{scmp}_{B \rightarrow A:Source}$ from SV_B
- Host “Source” can fetch key from local key server KS_A to authenticate SCMP message

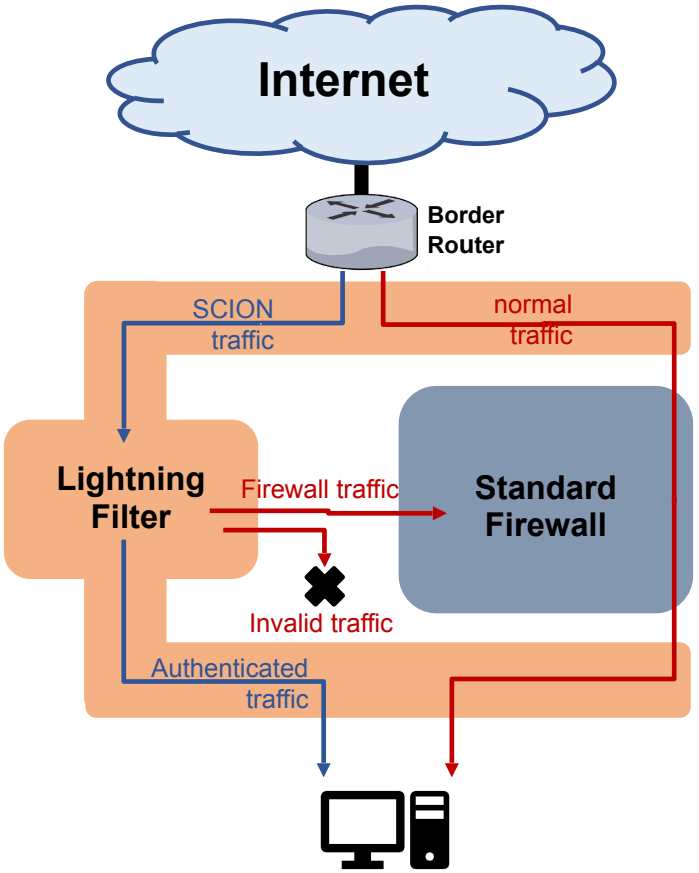


ETH zürich

SCION

DRKey Use Case: LightningFilter

- Approach
  - Sender locally fetches remote LightningFilter's key via DRKey
  - Remote LightningFilter can derive key within a few milliseconds and can authenticate packet
- Advantage: packet verification possible < 100ns at much lower overhead than heuristic-based firewalls

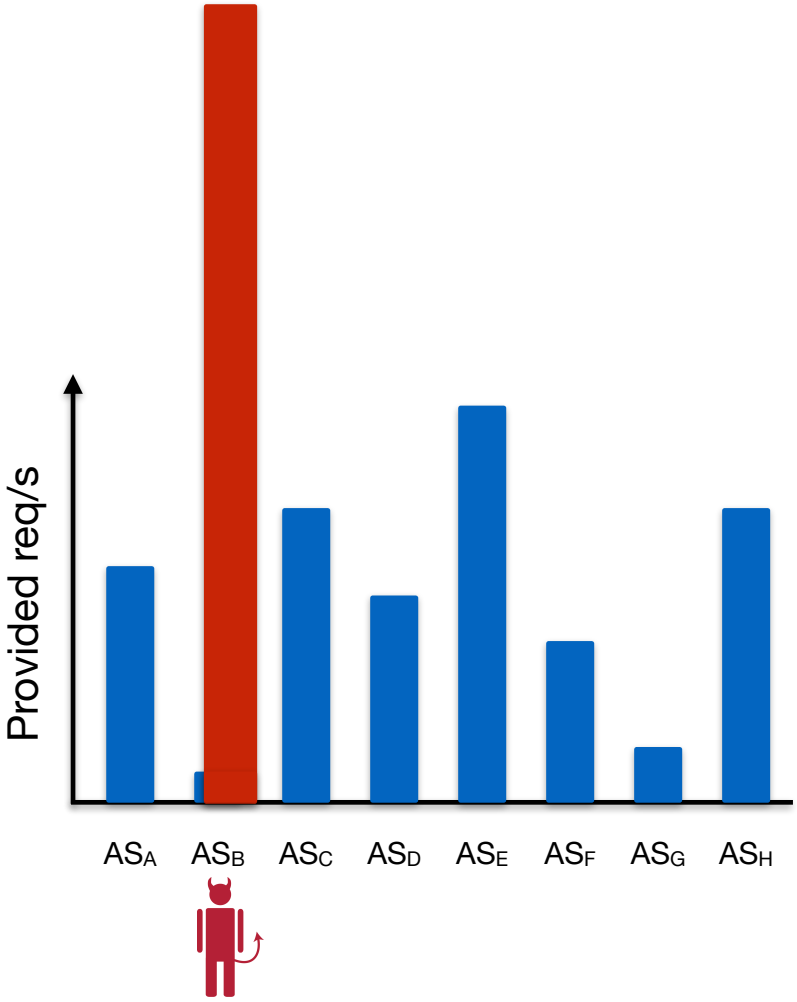


ETH zürich

SCION

LightningFilter History-based Filtering

- Filtering service that is deployed upstream of protected end server
- Performs:
  - Packet authentication (DRKey)
    → authentic source AS
  - Duplicate suppression (using Bloom Filter)
    → no duplicates
  - Per-AS history collection (using Cuckoo hash table)
  - History-based resource allocation and filtering during DoS
    → fair resource allocation based on historical usage
- Result: Guaranteed service as long as total number of requests from AS < allowed number of requests
  - Collateral damage only for hosts within attacker-controlled AS



ETH zürich

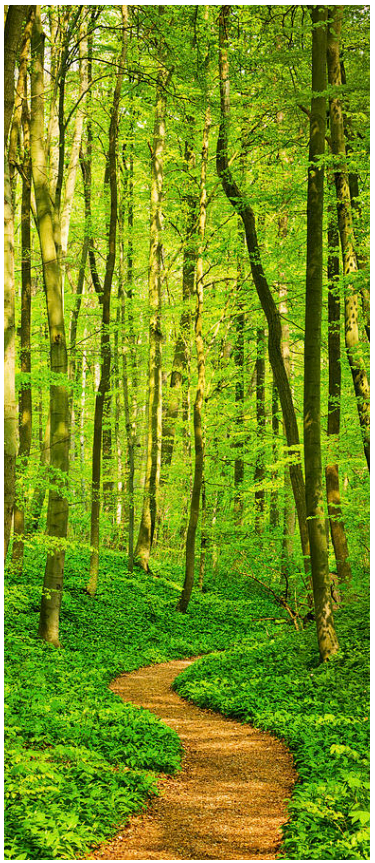
SCION

EPIC: Every Packet Is Checked

- Goals
  - Per-packet source authentication by every router and destination
  - Per-packet-unique hop fields
  - Path validation by destination
- Assumption: global time synchronization (± 100ms)
- Attacks prevented
  - Malicious router replays packets or increases packet size
  - Hop field MAC is brute forced and destination attacked until expiration time
- EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet, Legner et al., USENIX Security Symposium 2020

Insight: Cryptographic Processing at Line Rate Possible

- Symmetric-key cryptographic operations are possible within nanoseconds, thus enabling line-rate processing
- With hardware implementation, computing an AES block cipher can be accomplished within a few nanoseconds
- DRKey + EPIC systems enable per-packet source authentication in software ~ 100 ns
- This enables new approaches for network security

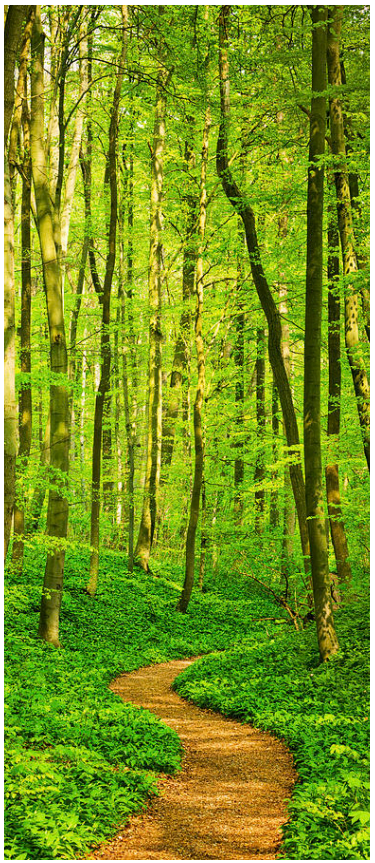


Importance of Path Awareness & Multi-path

- Generally, two paths exist between Europe and Southeast Asia
  - High latency, high bandwidth: Western route through US, ~450ms RTT
  - Low latency, low bandwidth: Eastern route through Suez canal, ~250ms RTT
- BGP is a “money routing protocol”, traffic follows cheapest path, typically highest bandwidth path
- Depending on application, either path is preferred
- With SCION, both paths can be offered!

Insight: Multi-Path is a Necessity for High Availability and Performance

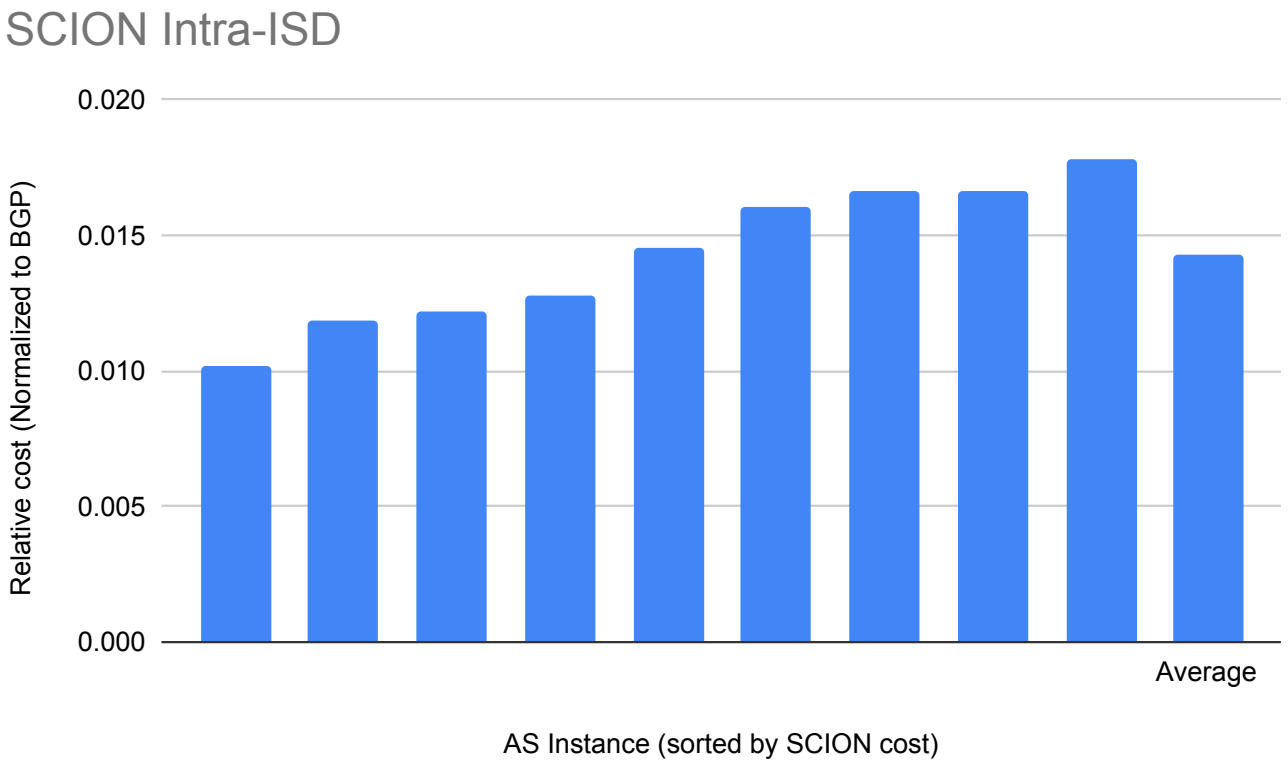
- Inter-domain multi-path is not a luxury, but a necessity to achieve high availability
- Rapid failover without routing system convergence
  - Routing bottlenecks can be avoided
- Enable higher network capacity
  - No more passive links for redundancy, all links can be active
  - Simultaneous use of several links
- Enables higher communication efficiency
  - Latency- vs. bandwidth optimal paths can be chosen
- Helps defend against DoS attacks, as adversary needs to congest all links
- QoS needs multi-path, as several alternatives need to be available to attempt resource reservations



Multi-Path Routing Approaches

- For a powerful multi-path system, we need a rich set of path choices: ideally dozens of paths if possible
- Problem: most prior multi-path routing algorithms are based on BGP, offering only 2-3 different path choices
  - Overhead increases linearly in the # of paths: hampering scalability
  - Notable exceptions: Pathlets, NIRA, HAIR
- The path segment combination of SCION provide a rich set of path choices
  - Extensible architecture: additional path segment generation algorithms can be added, and path server infrastructure can be used for dissemination

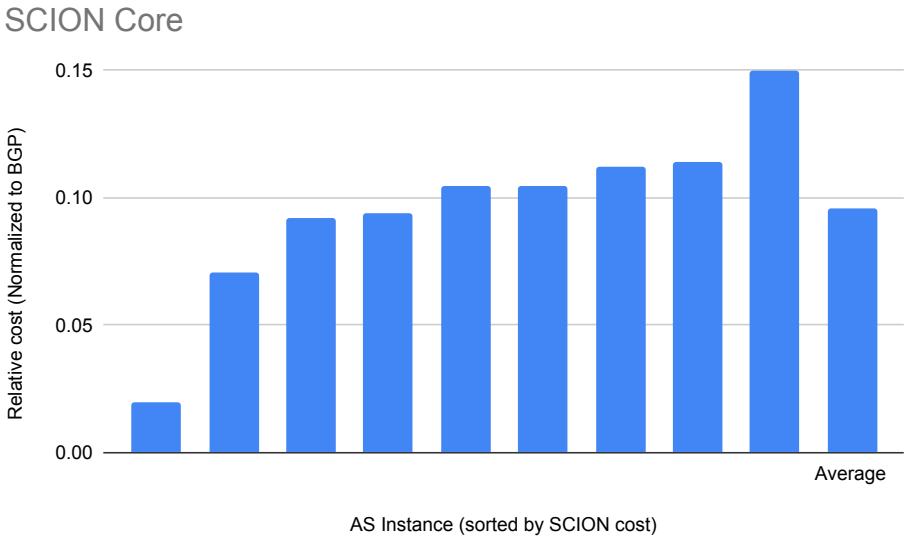
Scalability of SCION Intra-ISD Beaconing

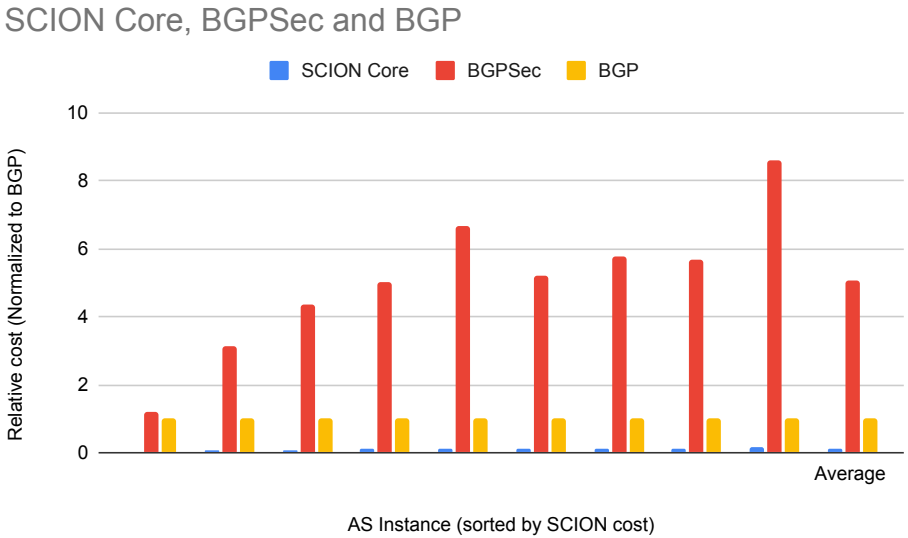


ETH zürich

SCION

Scalability of SCION Core Beaconing



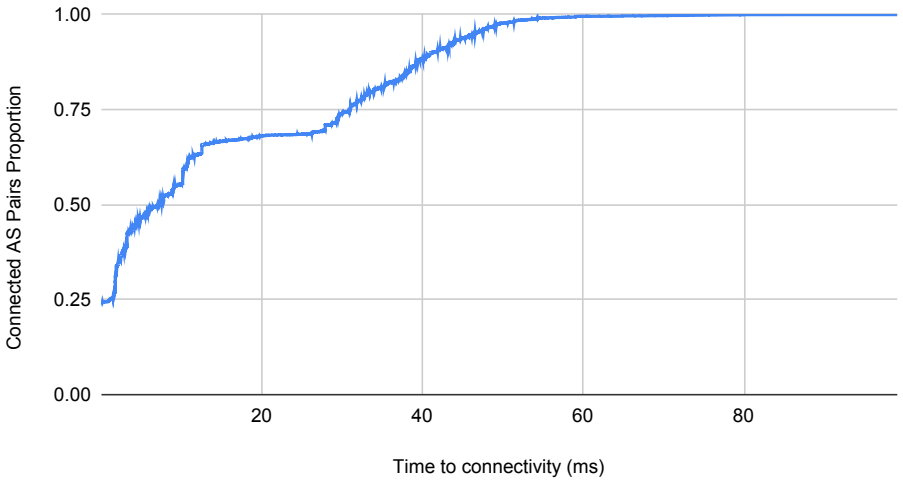


ETH zürich

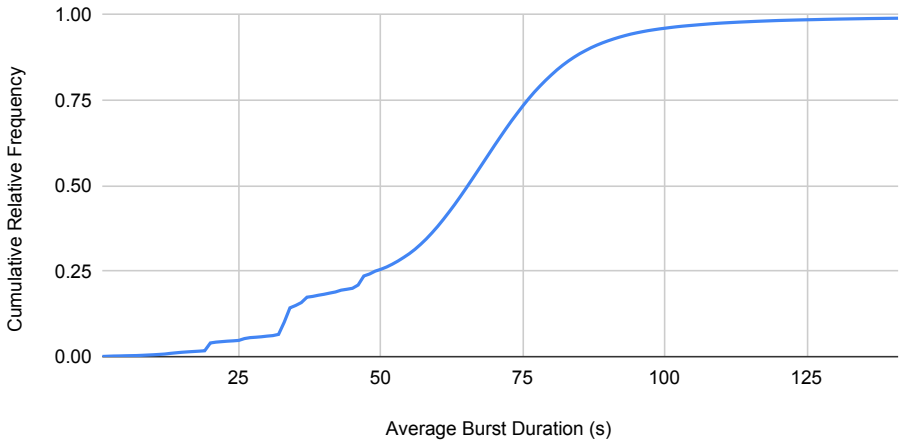
SCION

Time to Connectivity

Time to connectivity in SCION (Min Latency)



Distribution (99 %) of "average length of update bursts per prefix" during May 2020

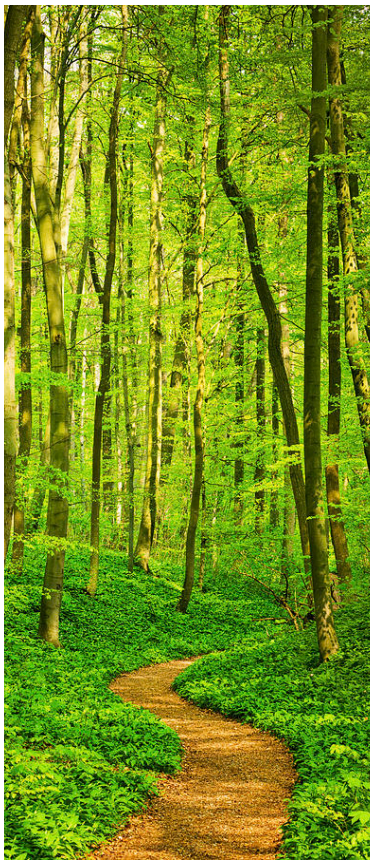


ETH zürich

SCION

Insight: SCION Provides Scalable Multi-Path Routing

- ISD decomposition offers scalability for segment exploration; and segment combination offers large number of path choices
- Overhead of beaconing is 10-100x lower than BGP, even though dozens of disjoint paths are being created
- Time-to-connectivity is approximately two orders of magnitude faster than BGP



ETH zürich

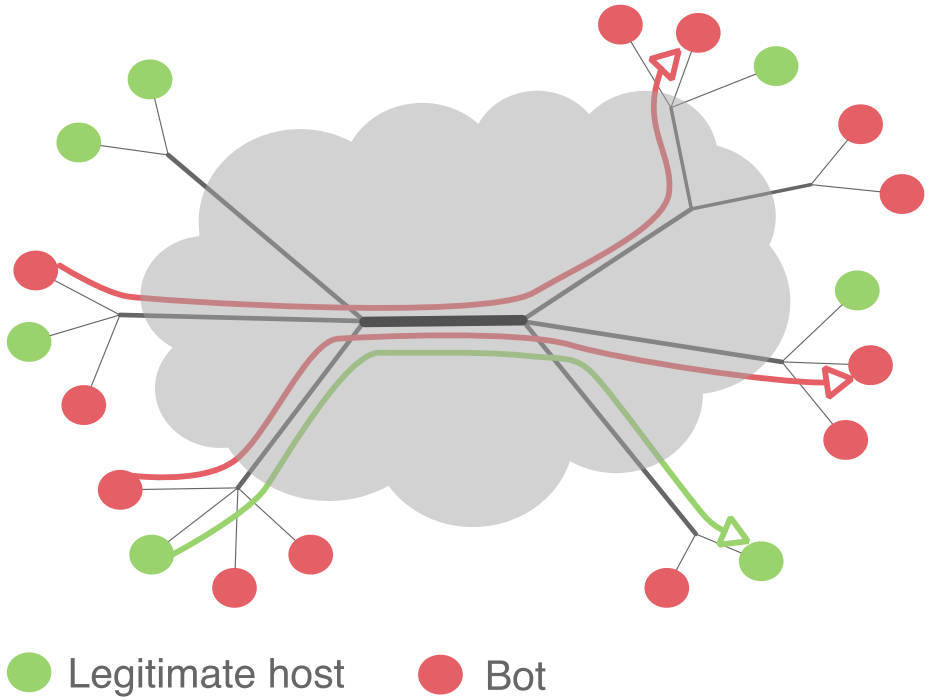
SCION

Volumetric DDoS Attacks

- Attacker overloads network link to induce congestion
- Defense requires sophisticated approaches
  - EPIC dynamic hop field computation
  - COLIBRI global resource allocation and reservation

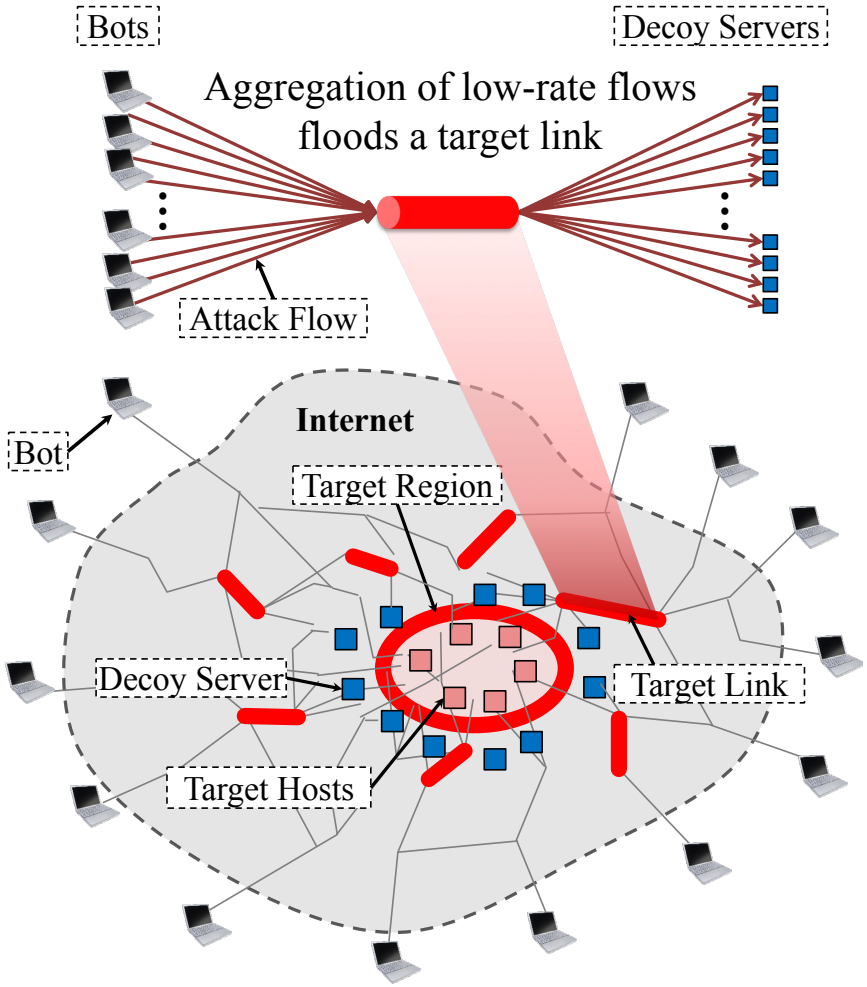
Coremelt Attack [Studer, Perrig, Esorics 2009]

- Adversary controls many bots distributed across the Internet
- Bots send traffic between each other, thus all traffic is desired by destination
  - Traffic is not sent to victim as in regular DDoS attacks
- Adversary can exhaust bandwidth on victim link
- Result: attack traffic exhausts bandwidth in per-flow fair sharing systems



Crossfire Attack [Kang, Lee, Gligor, IEEE S&P 2013]

- Adversary controls distributed bot army
- Observation: due to route optimization, few links are actually used to connect a target region to rest of Internet
- Adversary can contact selected servers to overload target links
- Result: disconnect target region from remainder of Internet



ETH zürich

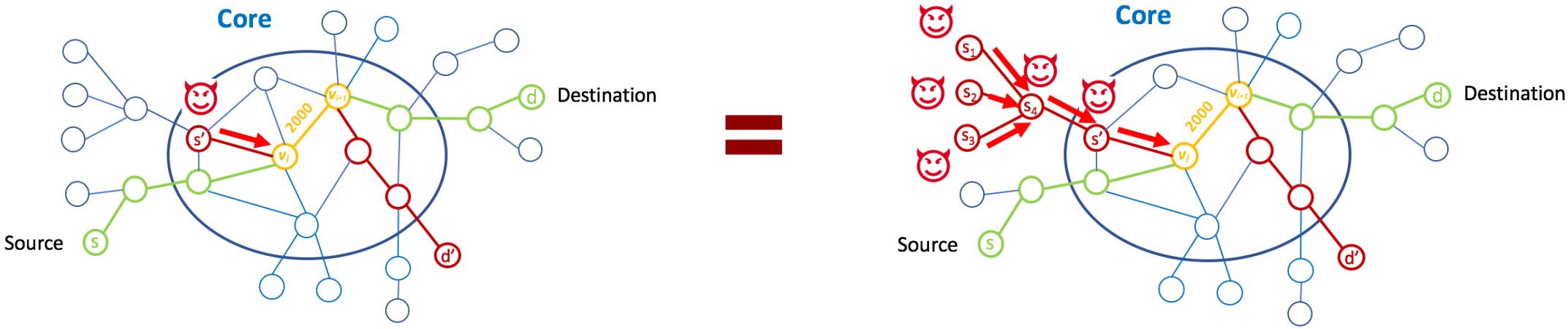
SCION

COLIBRI: Scalable Global QoS

- Thanks to several innovations, global QoS is now scalable and practical
- Stable paths ensure reservations are not affected by routing changes
- Multi-path enables searching for paths with sufficient bandwidth
- No per-flow state on routers, enabling scalability
  - DRKey enables high-speed per-packet source authentication
  - Efficient probabilistic large flow detection enable overuse detection
  - Per-flow stateful control-plane implemented on server infrastructure
- Per-neighbor fairness enables simple admission decision and configurations for ISPs

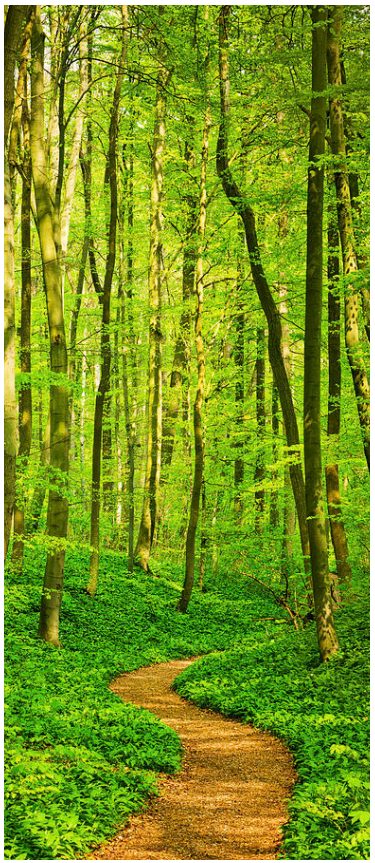
Admission Algorithm with Per-Neighbor Fairness

- Each AS defines neighbor-to-neighbor minimum bandwidth guarantees
- For any path, AS-to-AS minimum bandwidth guarantee can be computed, regardless of other demands
- Algorithm guarantees that no set of ASes can reserve a disproportionate amount of bandwidth through any link



Insight: Bandwidth Reservation Offers Many Advantages

- Explicit bandwidth admission simplifies transport layer
  - No need for sophisticated congestion control: simply use constant bitrate (CBR)
  - Reduce amount of acknowledgments due to very low loss rate
  - Fairness can be enforced at level of admissions
  - Possible reduction in energy utilization at end points
- Reserved but unused bandwidth can be used for best-effort traffic: no wasted bandwidth
- Fine-grained traffic engineering possible for ISPs
- Majority of traffic today is video: well suited for CBR traffic
  - Could simplify buffering and adaptive-bitrate algorithms



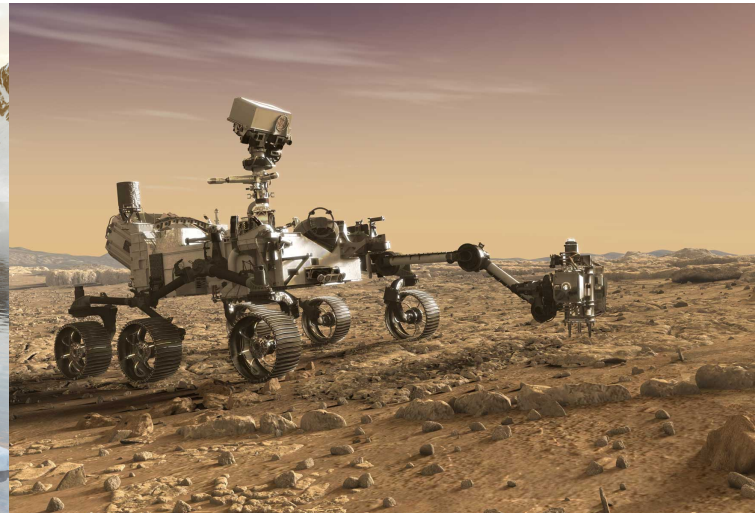
Lessons Learnt

- A global high-security public Internet is possible
  - Sovereign operation, yet globally connected
  - Global available communication is possible on public networks
  - Guaranteed DDoS resilience is possible
  - Protocol and code verification are necessary to obtain strong properties for large-scale distributed systems
- Static paths + multi-path routing enables powerful concepts
  - Fast failover: do not rely on network-based active failover but on redundancy with simultaneous use
  - Possibility to unlock additional network capacity

Expeditions Enable New Insights & Discoveries

- What started with the question “How secure can a global Internet be” has rewarded us with an exciting journey of insights and discoveries
- We hope to question engrained assumptions to counter Internet ossification
- Join the journey
  - https://www.scionlab.org
  - https://www.scion-architecture.net





SCION Team