SCION

A Next-Generation Secure Internet Architecture

Prof. Dr. Adrian Perrig
Prof. Dr. David Hausheer
Juan A. García-Pardo
Dr. Markus Legner

SIGCOMM-Tutorial, August 14, 2020

ETH zürich

Meet the Instructors

Adrian Perrig [AP]

David Hausheer [DH]

Juan A. García-Pardo [JG]

Markus Legner [ML]

150+ Person Years Invested in Design, Implementation, and Verification

Tutorial Schedule

- Part 1: Introduction to SCION
  - 1:40 pm–2:10 pm: Introduction: (why) do we want/need a new Internet? [AP]
  - 2:15 pm–2:35 pm: How SCION works [ML]
  - 2:40 pm–3:00 pm: SCION implementation and the SCIONLab testbed [DH]
- Part 2: Hands-on session
  - 3:20 pm–5:00 pm: Set-up and explore a SCIONLab AS
  - 5:00 pm–5:10 pm: Summary, wrap-up, and outlook [AP]
  - 5:10 pm–5:30 pm: Q&A [AP]

Tutorial Format

- Tutorial will be recorded and made available after the conference
- Please join slack channel: #sigcomm2020-tutorial-scion
- Please ask questions on Slack, we will either answer there or live on Zoom
  - You can also “raise your hand” if you want to ask a question
- Short breaks between sessions can be used for Q&A
- Hands-on session
  - Please set up SCIONLab based on instructions here: https://docs.scionlab.org/content/sigcomm/preparation.html
  - Ask questions on Slack, 1:1 calls possible to resolve issues
  - At all times, one instructor is present in Zoom to chat about SCION
- Reconvene in Zoom for final wrap-up

Introduction:

(Why) do we want/need a new Internet?

SCION Intro and Use Cases

Why try a new Internet Architecture?

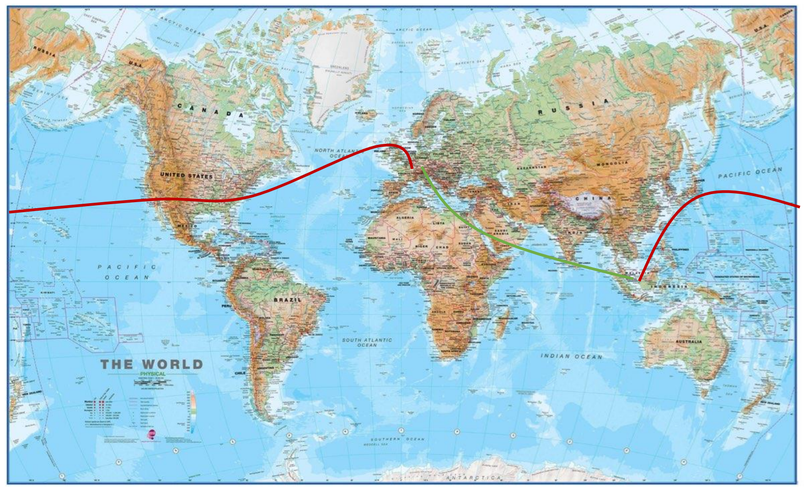
- We started our expedition asking the question:
  How secure can a global Internet be?
  - Answer: global communication guarantees can be achieved as long as a path of benign ASes exists
- During our journey we discovered that path-aware networking and native multi-path communication are powerful concepts that can provide higher efficiency than 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!

Why try SCION?

- Beneficial properties: scalability, native inter-domain multipath, security, path transparency, efficiency, …
- Maturity
  - 11 years of development
  - Approximately 150+ person-years of work
  - Open-source system
- Deployment
  - Global BGP-free production network (available at 60 locations)
  - Global SCIONLab research network

Importance of Path Awareness & Multipath Communication

- Generally, two paths exist between Europe and Southeast Asia
  - High latency, high bandwidth: Western route via US, ~450ms RTT
  - Low latency, low bandwidth: Eastern route via Red Sea, ~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!

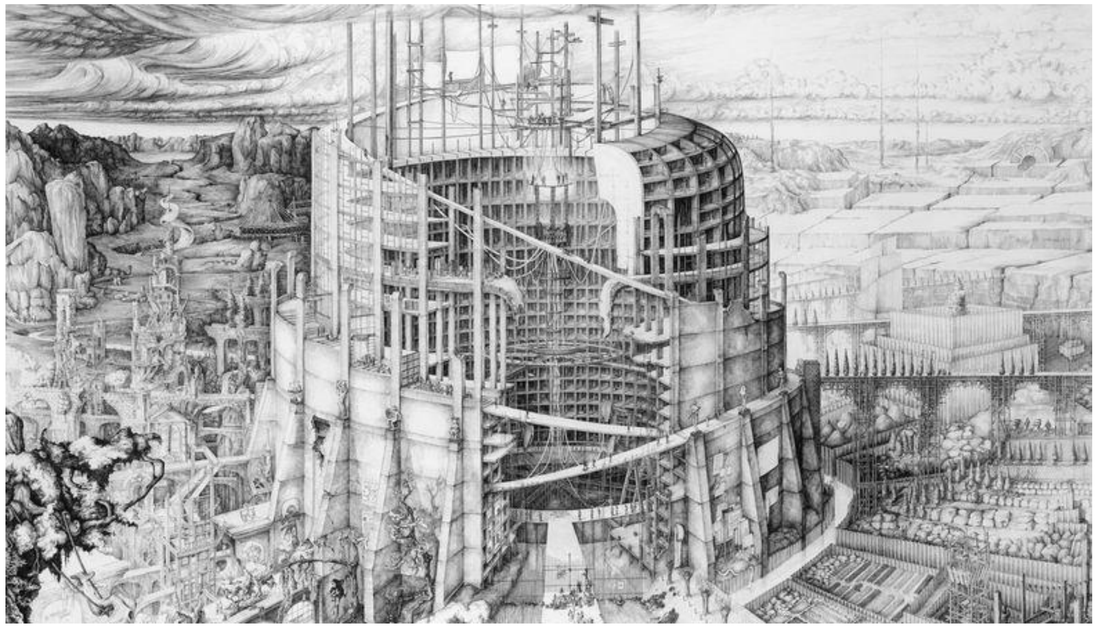


SCION Vision: A Global Next-Generation Public Internet

- High security and efficiency
- Path-aware networking with multipath communication
- Global communication guarantees

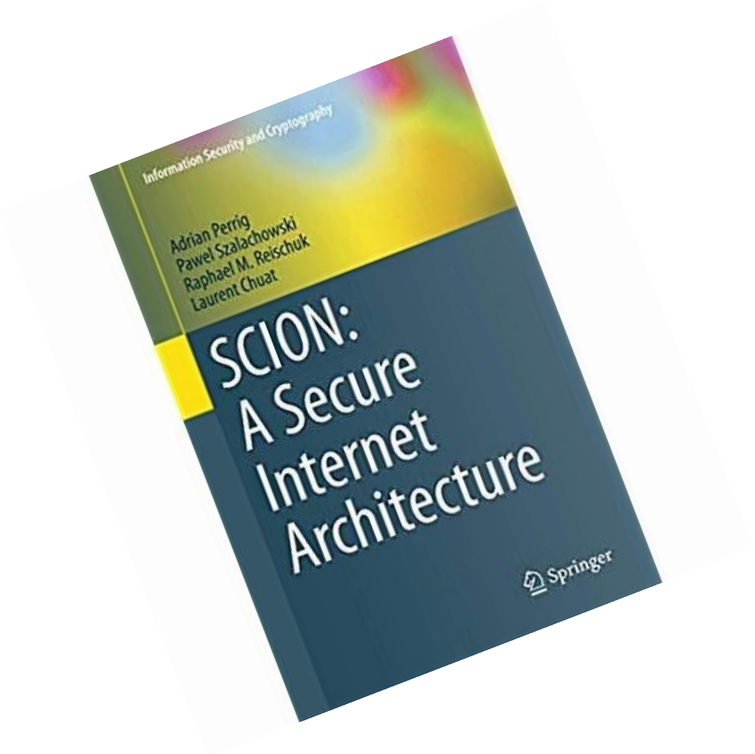
SCION Architecture Principles

- Stateless packet forwarding
- Convergence-free routing
- Path-aware networking
- Multi-path communication
- High security through design and formal verification
- Sovereignty and transparency for trust roots



Online Resources

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



SCION Overview in One Slide

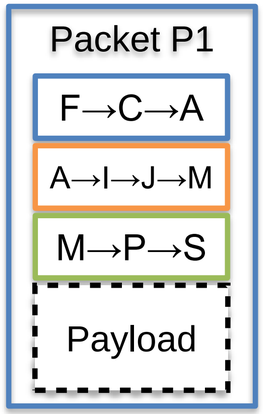
Path-based Network Architecture

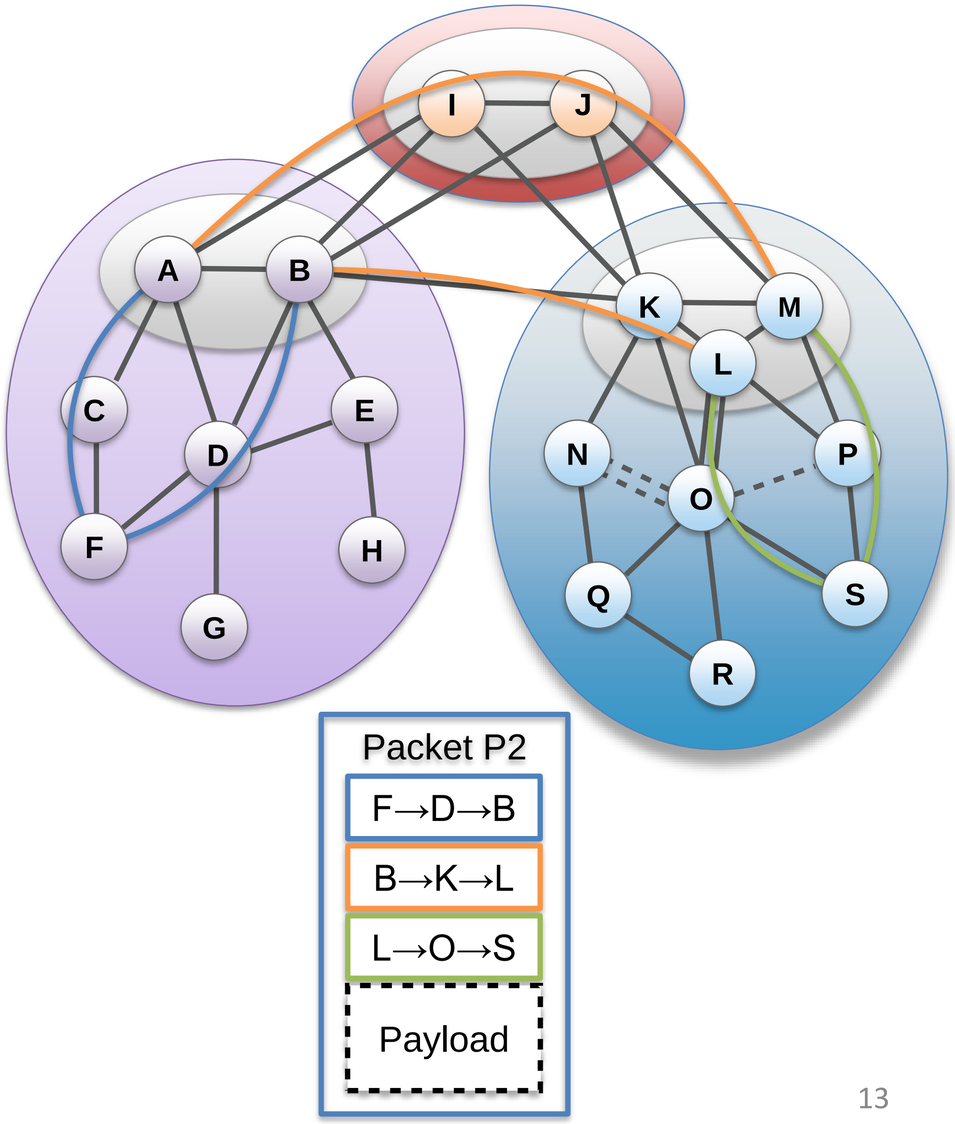
Control Plane - Routing

- Constructs and Disseminates Path Segments

Data Plane - Packet forwarding

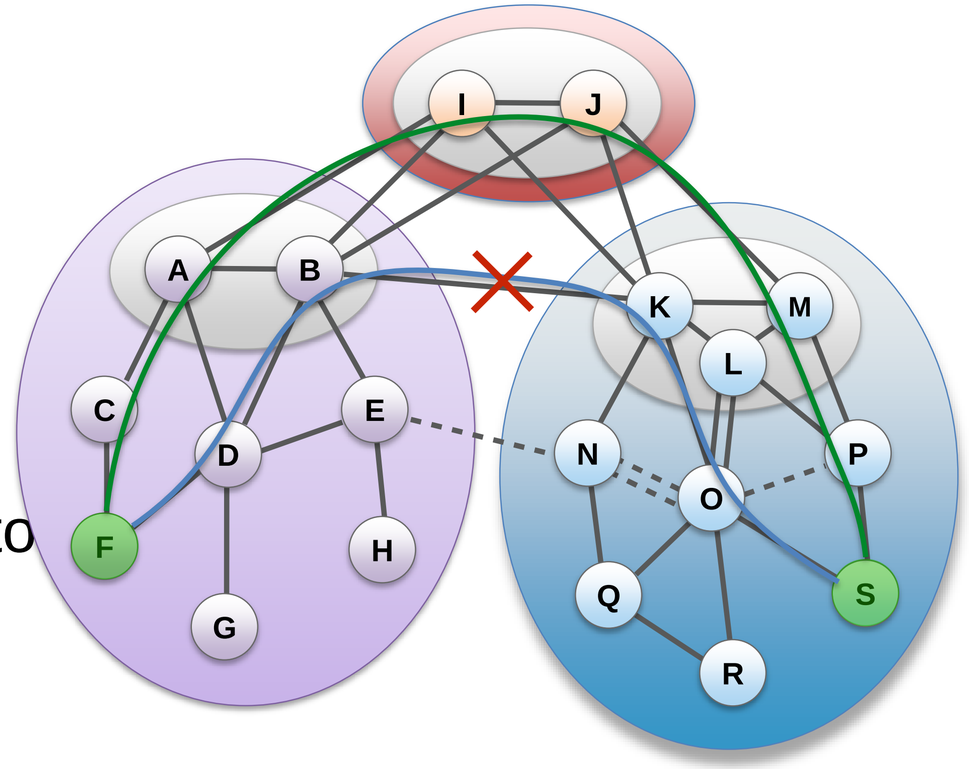
- Combine Path Segments to Path
- Packets contain Path
- Routers forward packets based on Path
  - Simple routers, stateless operation





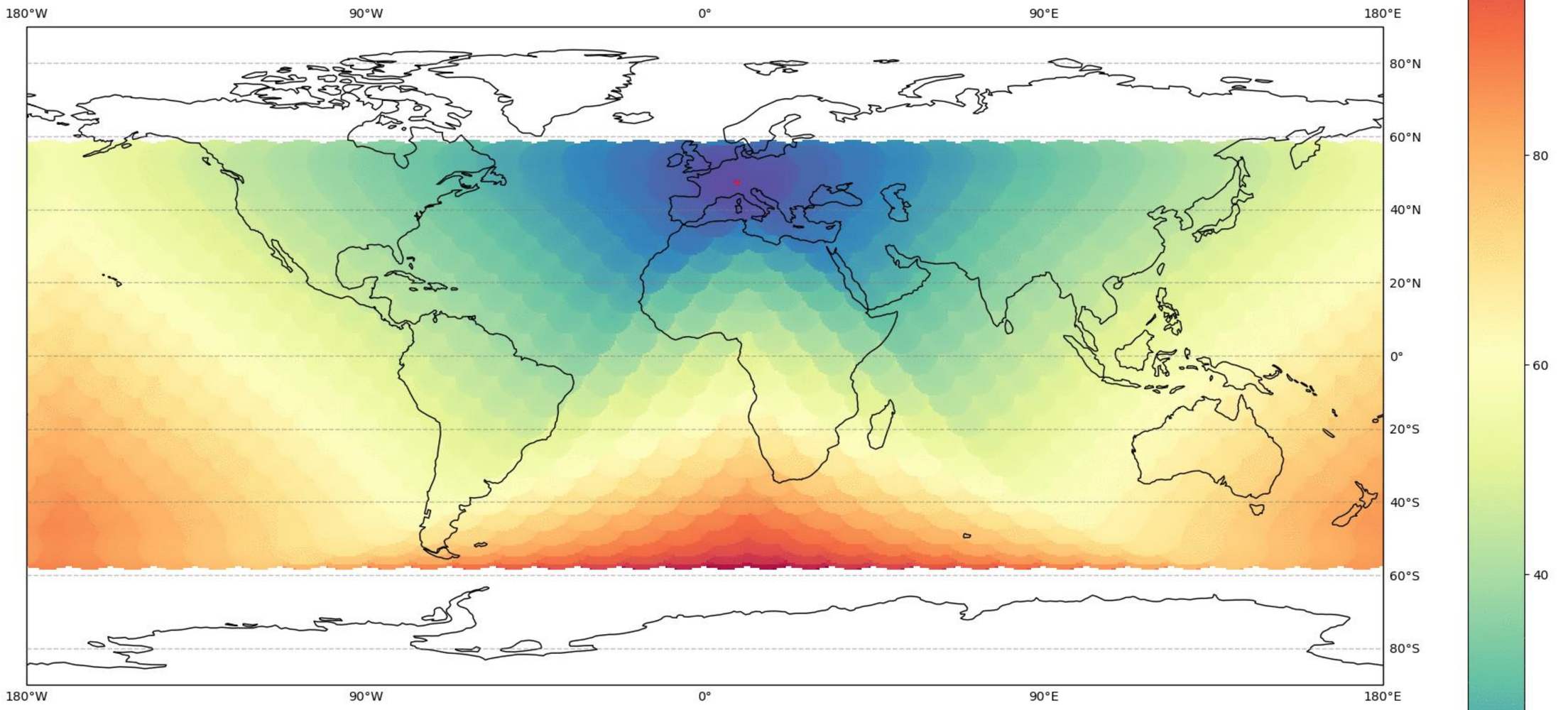
Use Case: High-Speed Interdomain Failover

- Common failure scenarios in current Internet
  - Long-term failures (infrequent): large-scale failures require hours until BGP re-stabilizes
  - Intermediate-term failures (at each inter-domain router or link failure): 3-5 minutes until path is cleanly switched
  - Short-term failures (frequent): during BGP route change, routing loop during 5-10 seconds
- SCION: backup path is already set up and ready to be used when a link failure is observed
- Result: failover within milliseconds!

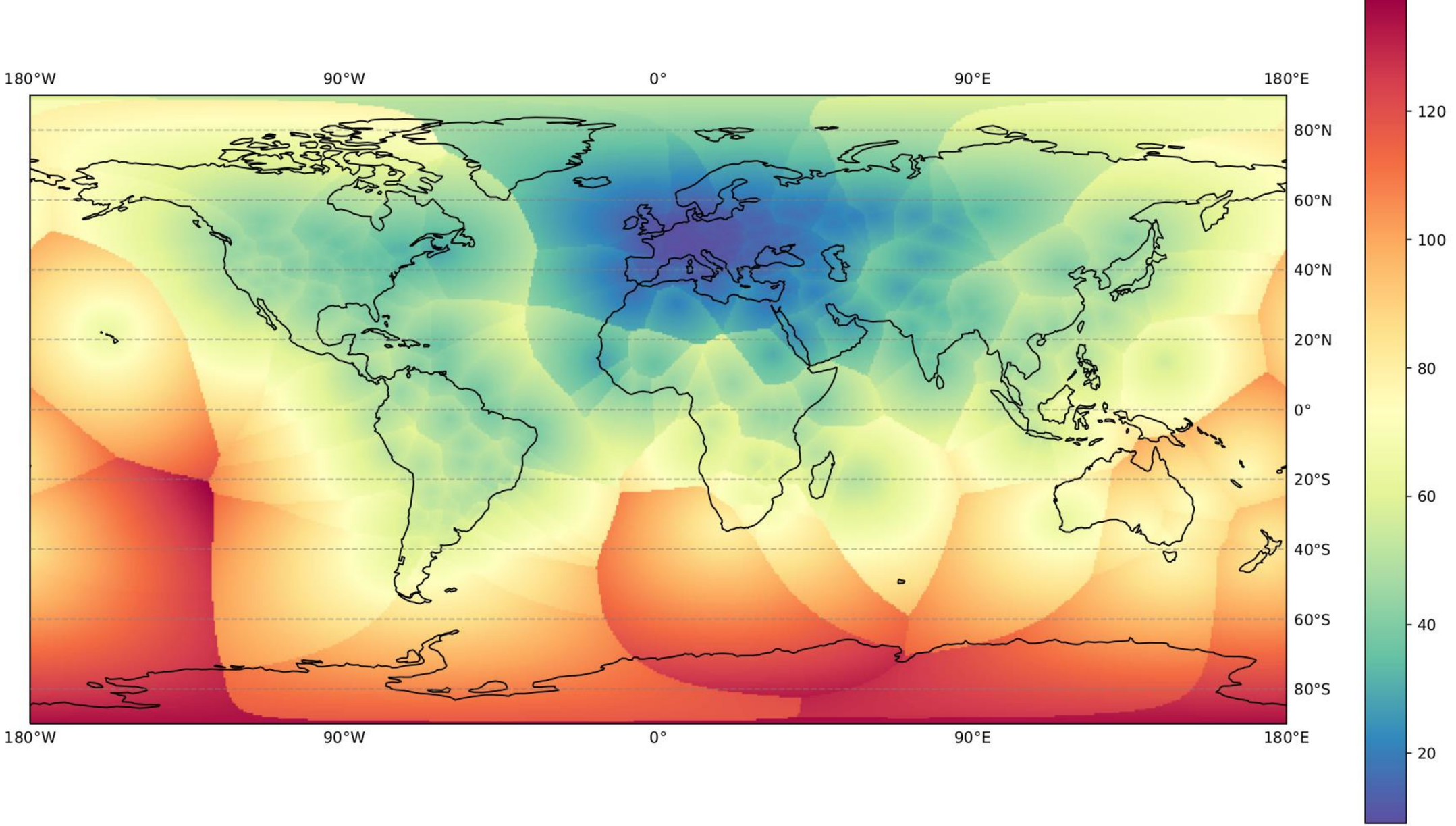


Use Case: Low Earth Orbit Satellite Networks

- Previous satellite networks suffered from high latency for communication between earth and satellite
  - Geostationary satellites are at a distance of about 40’000km from earth, ~130ms latency
- New Low Earth Orbit (LEO) satellite networks are much lower and thus only require around 5ms propagation latency between earth and satellite
  - Distance about 1200km, ~4ms latency
  - Inter-Satellite Laser (ISL) links enable global communication
- Disadvantage: large number of satellites needed to provide complete coverage



Latency from Zürich to the world (SpaceX old stage-1 constellation with ISLs)



Latency from Zürich to the world, Satellite + IXP connection path

SCION Naturally Supports LEO Networks

- BGP convergence is too slow to support frequent outages / short time windows of availability for during initial deployment stages of LEO network
  - Clouds / rain can also prevent or reduce communication with satellite
- SCION can optimally integrate LEO network into Internet fabric
  - Satellite network paths can be announced next to regular Internet paths: end host can select optimal path based on bandwidth, latency, and cost
  - Beacons can be sent out before path becomes available, including start / end validity time
  - Based on weather prediction, expected bw can be added to beacon
  - End host can also select which satellite uplink station to send packets to
  - Receiver can select appropriate return link, could be terrestrial or satellite
- Publication: Giuliari et al., “Internet Backbones in Space” , CCR 50(1), 2020

Sample Deployment 1:
SCION for ETH Domain (SCI-ED)

SCI-ED: Connectivity among ETH domain research institutions

- **Challenge:**

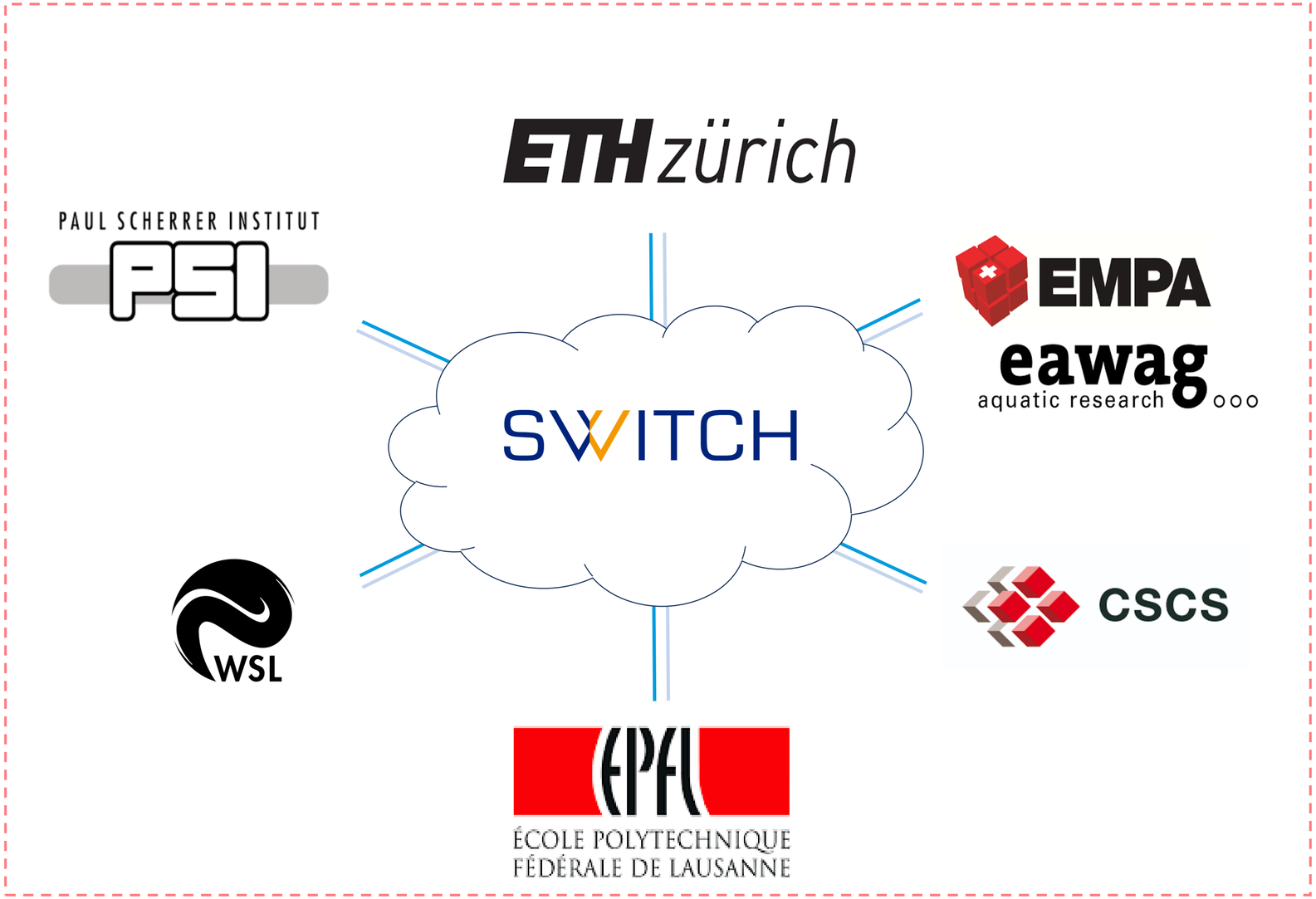
Highly available and efficient research network for communication across institutes and industry collaborators

- **Approach:**

SCION connectivity enables security and multipath communication. Leverage systems such as LightningFilter for high-speed firewall

- **Outcome:**

High efficiency and reliability, high security for critical infrastructure, compliance for medical use cases



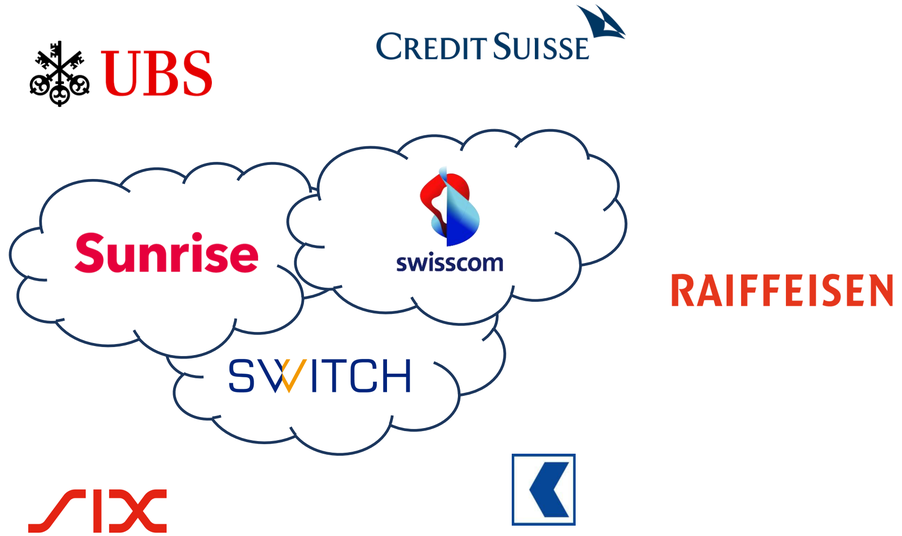
Sample Deployment 2: Networking Industry Verticals

Challenge

- An entire industry needs to exchange data securely, reliably and in a controlled way (nationally and also internationally)
- Flexible any-to-any communication patterns
- No single provider can serve all participants

Opportunity

- With SCION, providers can form flexible networks with cross-provider guarantees
- Customers will often use a multi-provider strategy increasing the overall number of network accesses needed
- Self-management of customers through access to central controller



Demo Time

- LightningFilter high-speed packet filter
- Hercules file transfer

LightningFilter:
High-Speed Packet Authentication and Filtering

Benjamin Rothenberger, Juan A. García-Pardo, Marc Frei, Dominik Roos, Jonas Gude, Pascal Sprenger, Florian Jacky, and Adrian Perrig

Example

- High-speed packet processing requires nanosecond operations
  - Example: 64-byte packets @ 100Gbps: ~5ns processing time

- Nanosecond scale key establishment
- Nanosecond scale packet authentication

- Trivia: how “long” is a nanosecond?
  - Answer: light travels about 30cm in 1ns

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
- Only symmetric crypto enables high-speed processing through parallel processing and pipelining

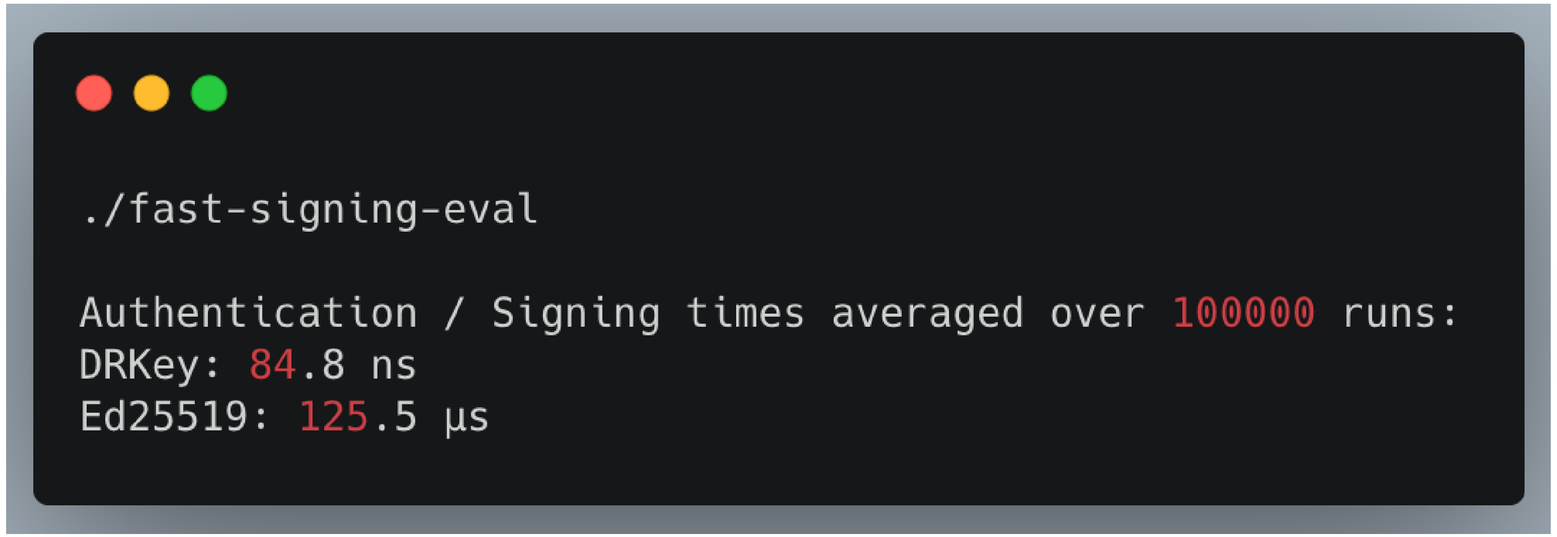
DRKey & Control-Plane PKI

- 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

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 SVX
  - KX→Y = PRFSVx (“Y”)
  - Intel AES-NI instructions enable PRF computation within 30 cycles, or 70 cycles for CMAC
    Key computation is 3-5 times faster than DRAM key lookup!
  - Any entity in AS X knowing secret value SVX can derive KX→*

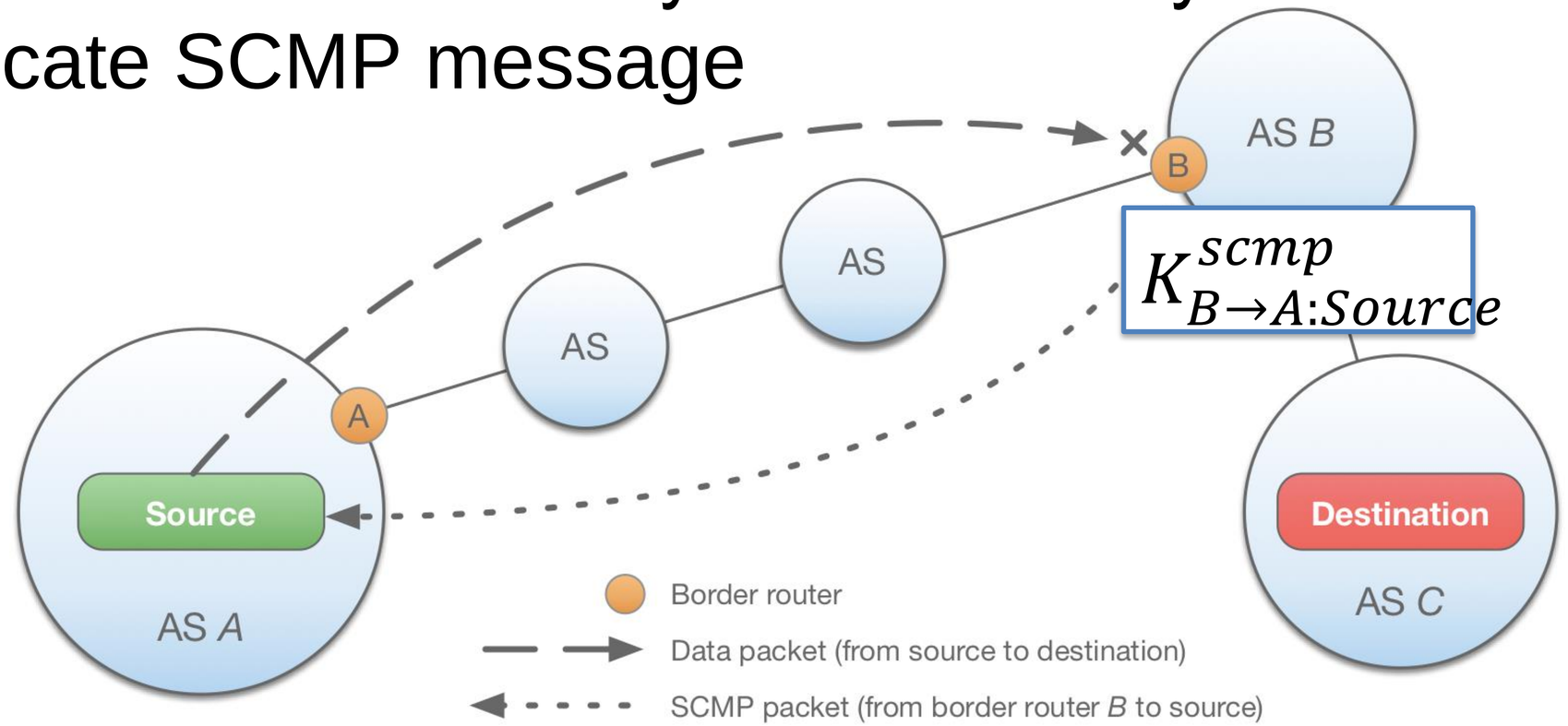
DRKey Performance



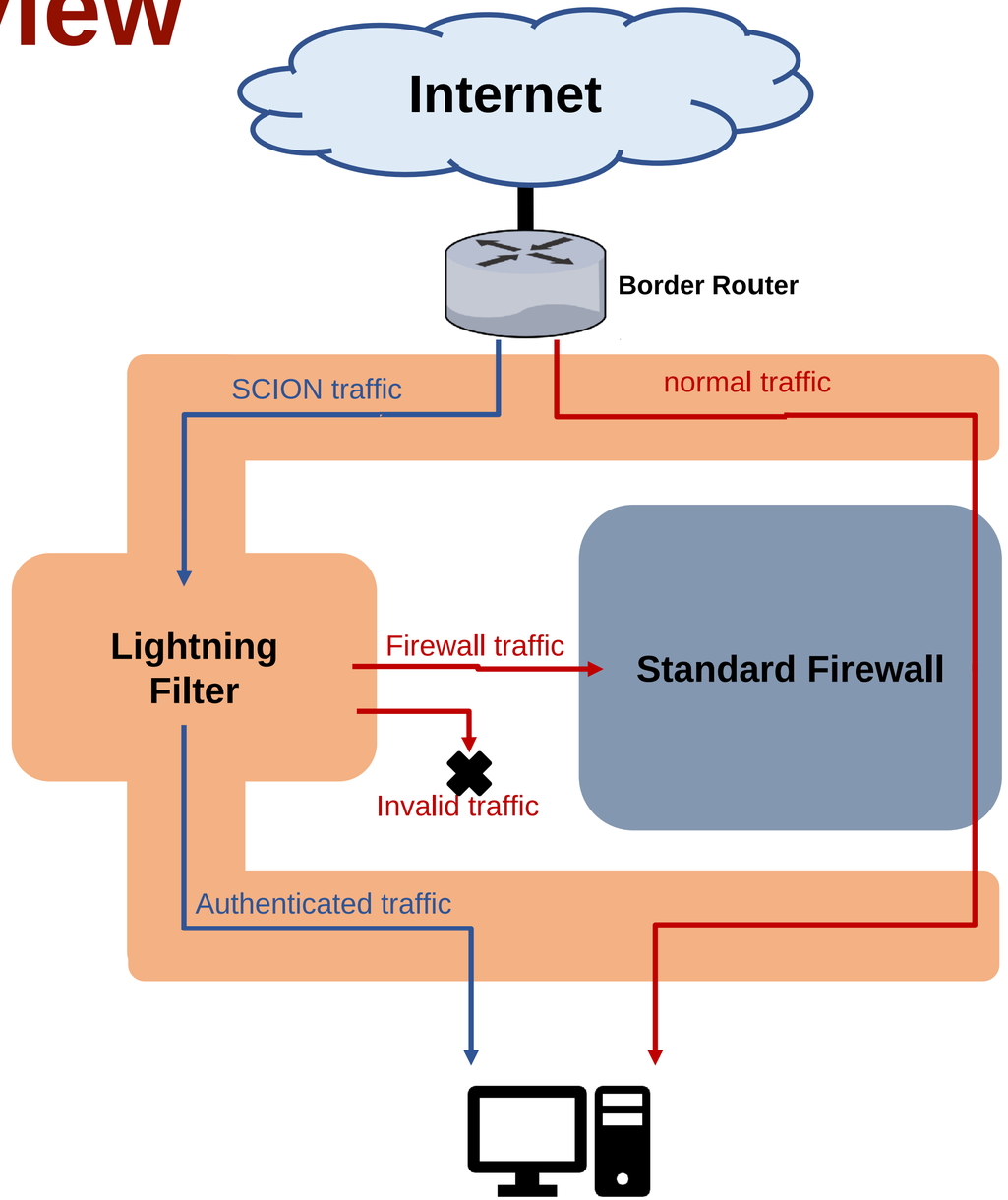
Factor:
~ 1450x

DRKey Use Case: SCMP Authentication

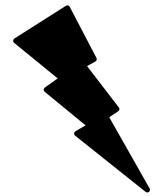
- Border router in AS B can derive key $K^{scmp}_{B \rightarrow A:Source}$ from SV_B
- Host “Source” can fetch key from local key server KS_A to authenticate SCMP message



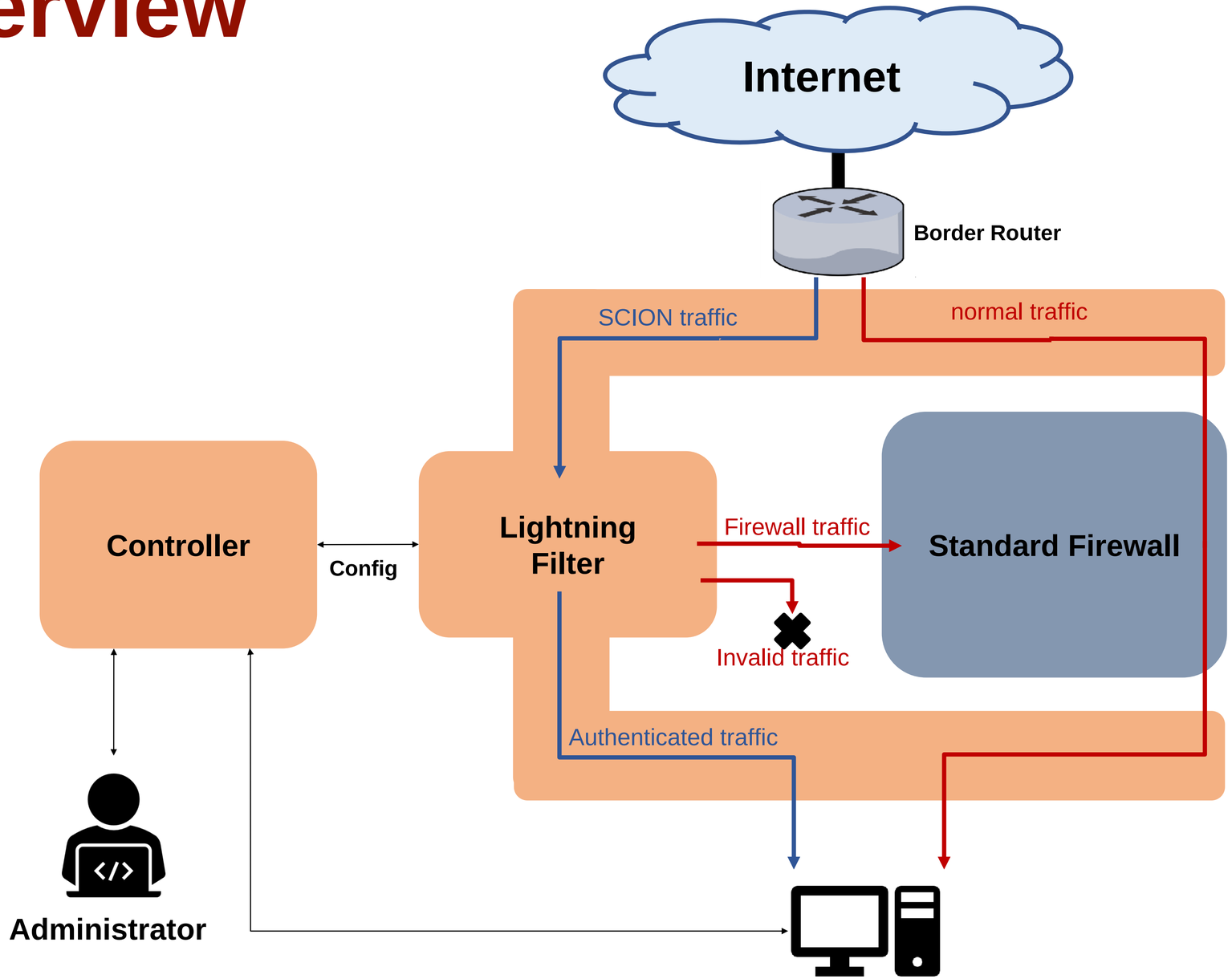
Design Overview

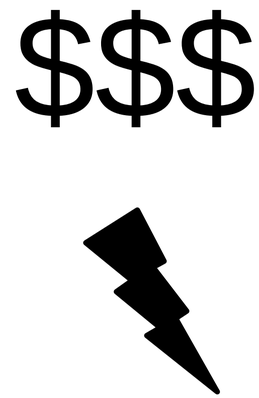


$$$



Overview


Internet
Border Router
SCION traffic
normal traffic
Controller
Config
Lightning Filter
Firewall traffic
Standard Firewall
Invalid traffic
Authenticated traffic
Administrator


$$$

Demo Outline

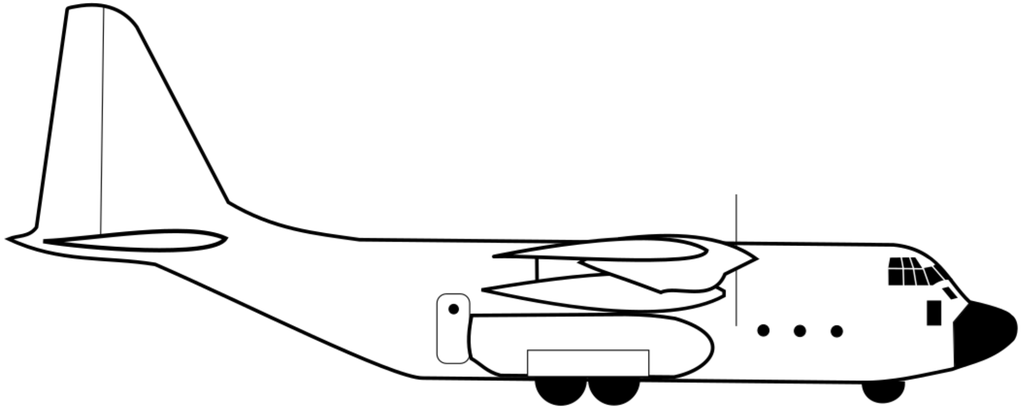
1. Attack scenario
   - Attacker located anywhere in Internet →Source authentication
2. Bandwidth capacity
   - 120 Gbps traffic volume
3. Filtering based on source authentication
   - Alternate between filtering and bypass every 30s
4. Duplicate suppression
   - 80 Gbps duplicates traffic, 40 Gbps legitimate traffic

Lightning Filter Demo

Network Security Group

ETH zürich

SCION



Hercules

Bulk Data Transfer over SCION

Matthias Frei and François Wirz

Project Scope

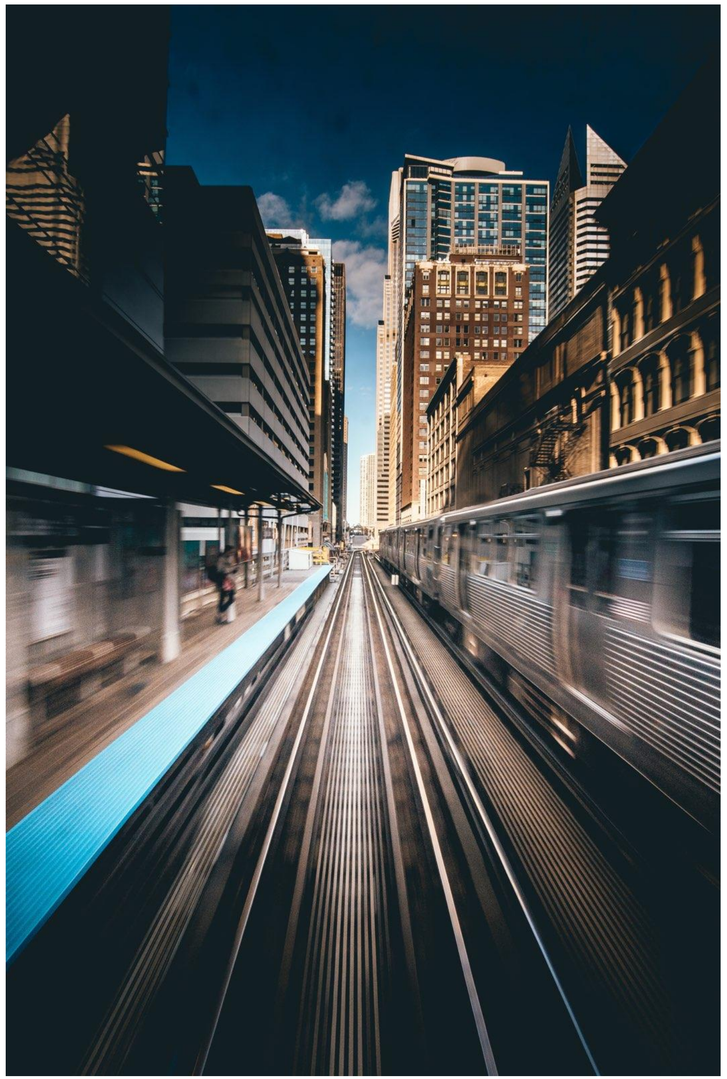
High-speed large file transfer over Internet

- Large = Terabyte-scale data transfers

Use Cases

- Data-intensive science: healthcare, physics, big data, etc.
- Remote processing, data needs to be transmitted beforehand
- Remote backup

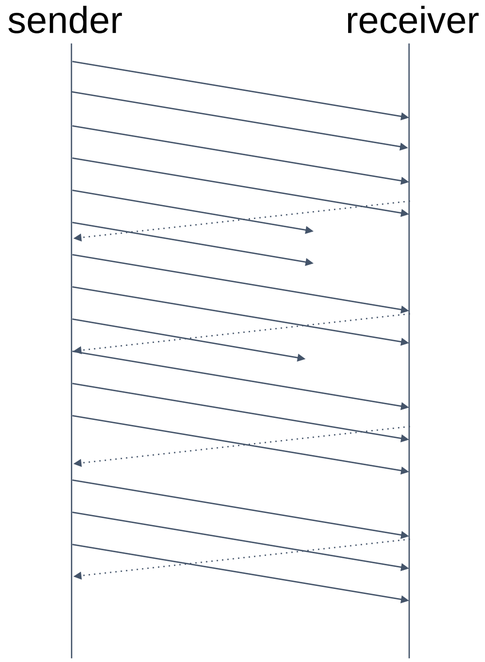
Approach for High-Speed Data Transmission



- Multipath communication, even backup links can be used simultaneously
- Path optimization: steering traffic across high-bandwidth paths
- QUIC instead of TCP
- Performance-oriented congestion control (PCC)
- Firewall bypassing thanks to high-speed packet authentication
- Data transmission appliance to avoid changing end host

Hercules

- SCION/UDP packet blasting + retransmits
  - “Reliable Blast UDP”[1]
- Range ACKs at fixed frequency
- Performance-oriented congestion control [2]
  - Link empirical performance to actions taken



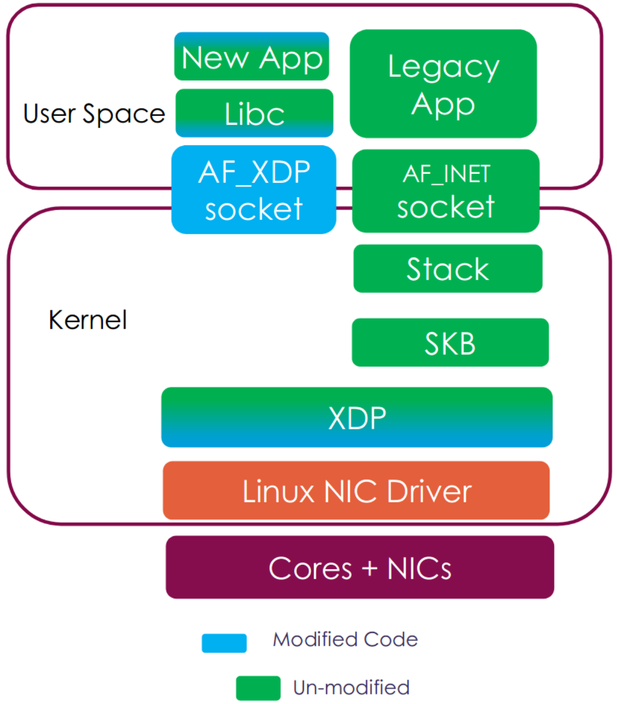
[1] "*Reliable Blast UDP : Predictable High Performance Bulk Data Transfer*", Eric He, Jason Leigh, Oliver Yu and Thomas A. DeFanti, Proceedings of IEEE Cluster Computing, Chicago, Illinois, September, 2002

[2] “PCC: Re-architecting Congestion Control for Consistent High Performance”, Mo Dong, Qingxi Li, Doron Zarchy, P. Brighten Godfrey, and Michael Schapira, 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)

Hercules

AF_XDP[3] for high performance SCION/UDP

- Published in December 2018
  available in Linux >= 4.18
  zero-copy mode in Linux >= 5.1
- Bypass Linux networking stack for send/receive
- Bypass SCION dispatcher

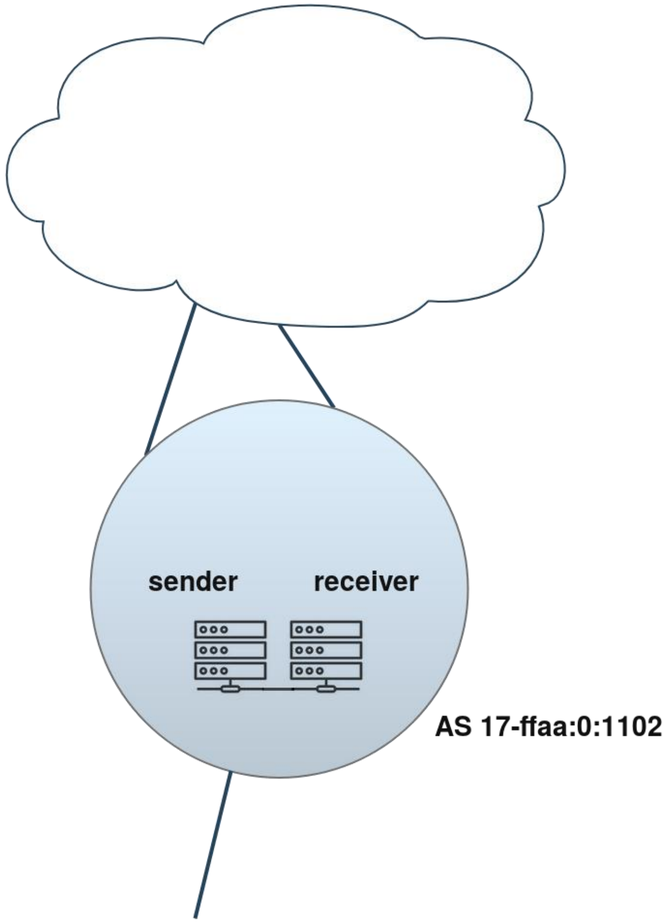


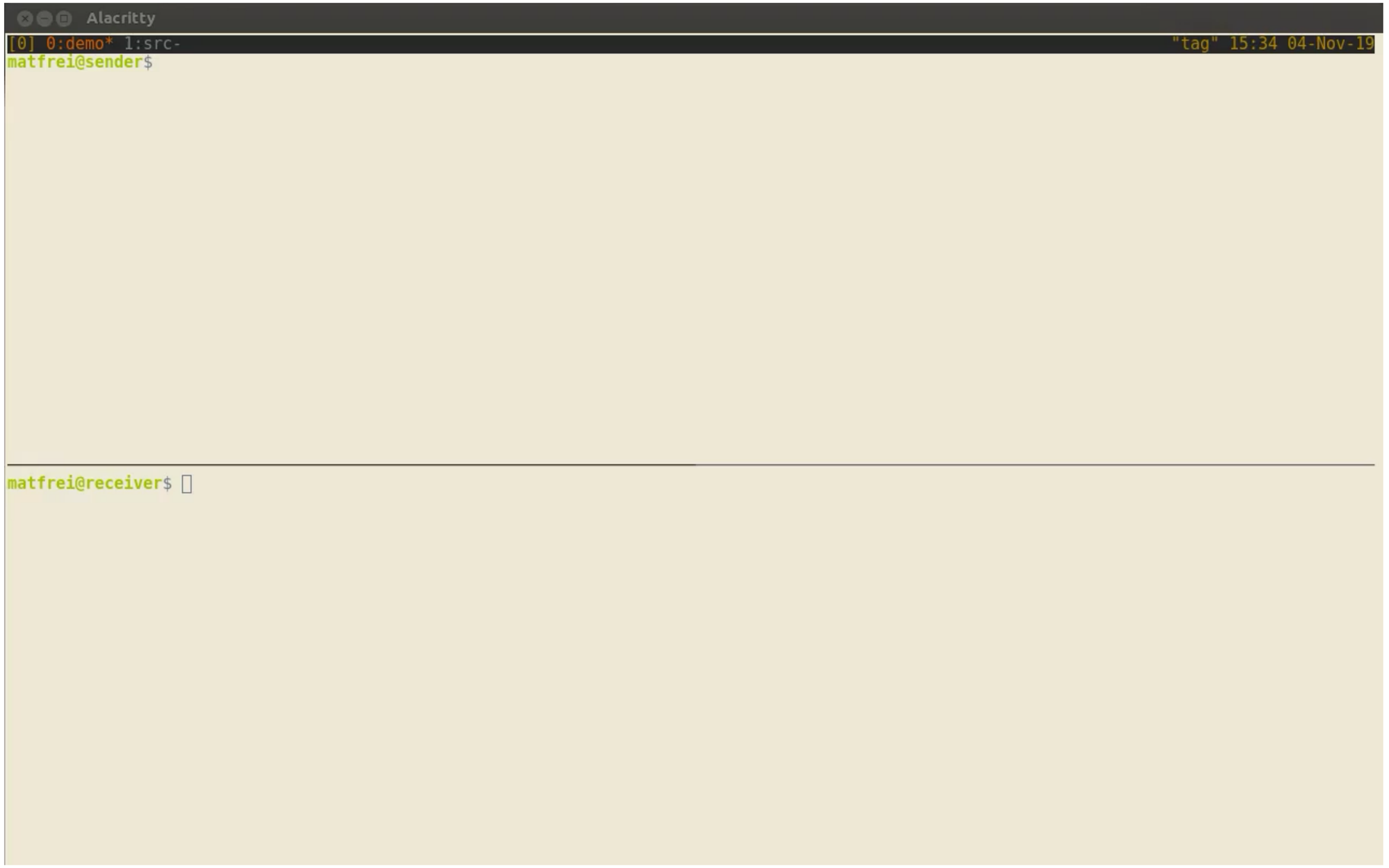
PMD for AF_XDP: Zhang Qi, Li Xiaoyun

[3] "Accelerating networking with AF_XDP", Jonathan Corbet, LWN.net, 2018

Demo

- Transfer file between two SCION hosts in *same* AS
- Directly connected, 40GbE
- *Not* the target use case, but high-performance SCION links are being established




Alacritty
[0] 0:demo* 1:src-
"tag" 15:34 04-Nov-19
matfrei@sender$
matfrei@receiver$

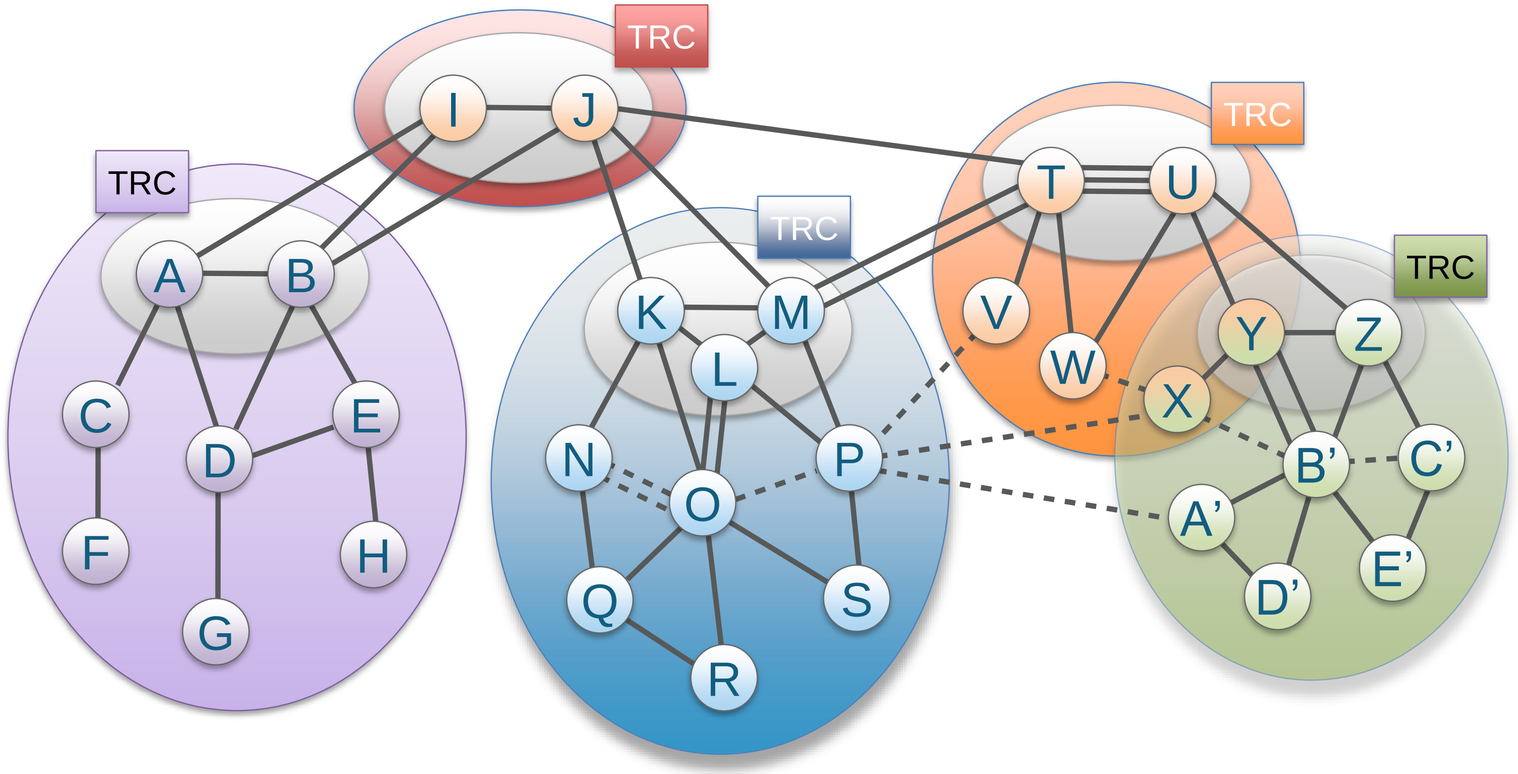
How SCION Works

What is SCION?

- Inter-domain routing architecture, to replace BGP
- Open: open-source Internet platform
- Highly efficient: faster than current Internet
- Highly secure: attacks are either impossible by design or significantly weakened
- Sovereign operation: local trust roots enable trust flexibility
- Communication guarantees: even across heterogeneous communication fabric in the presence of adversaries
- Verifiable: Security proofs through formal methods

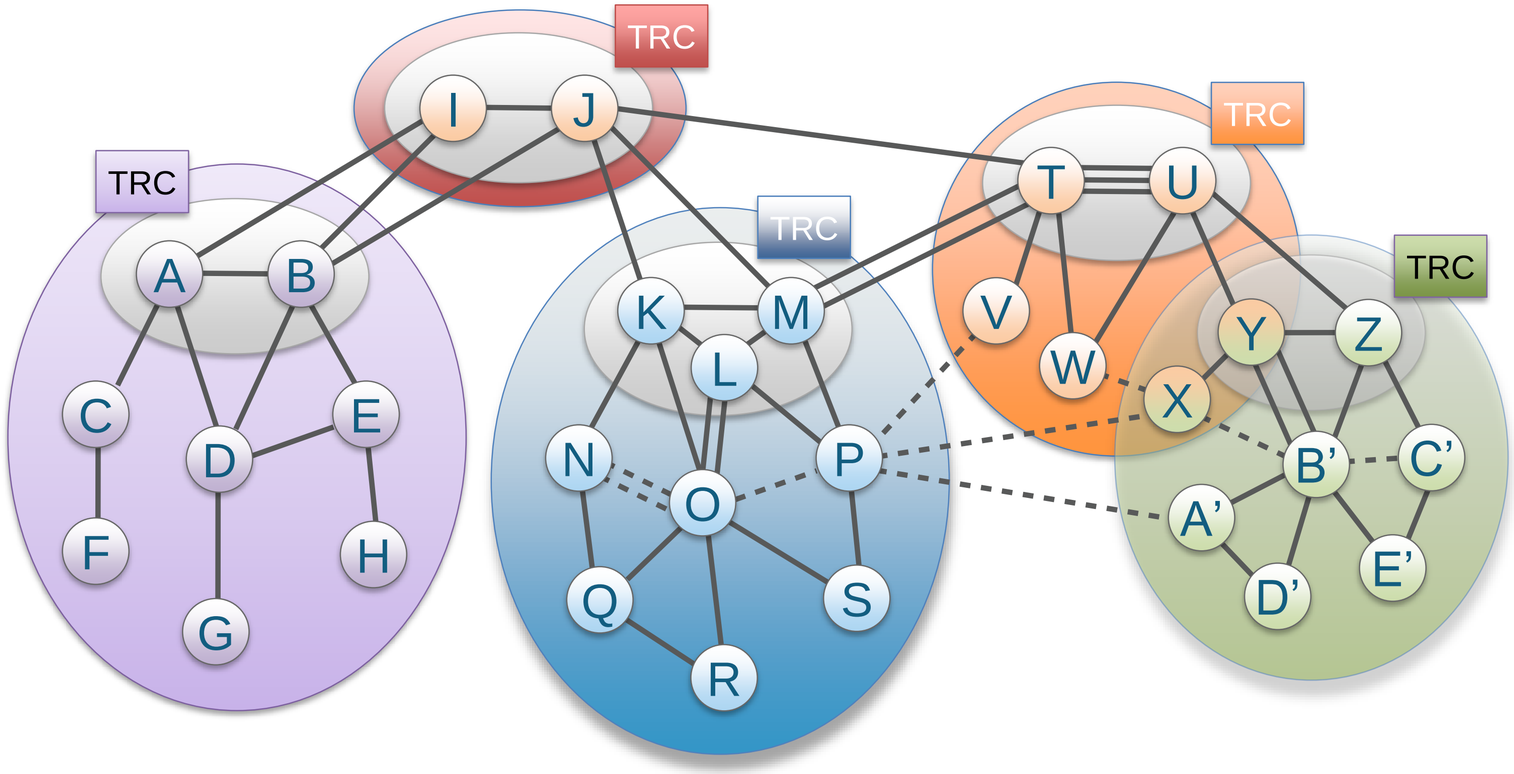
Approach for Scalability and Isolation: Isolation Domains (ISD)

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



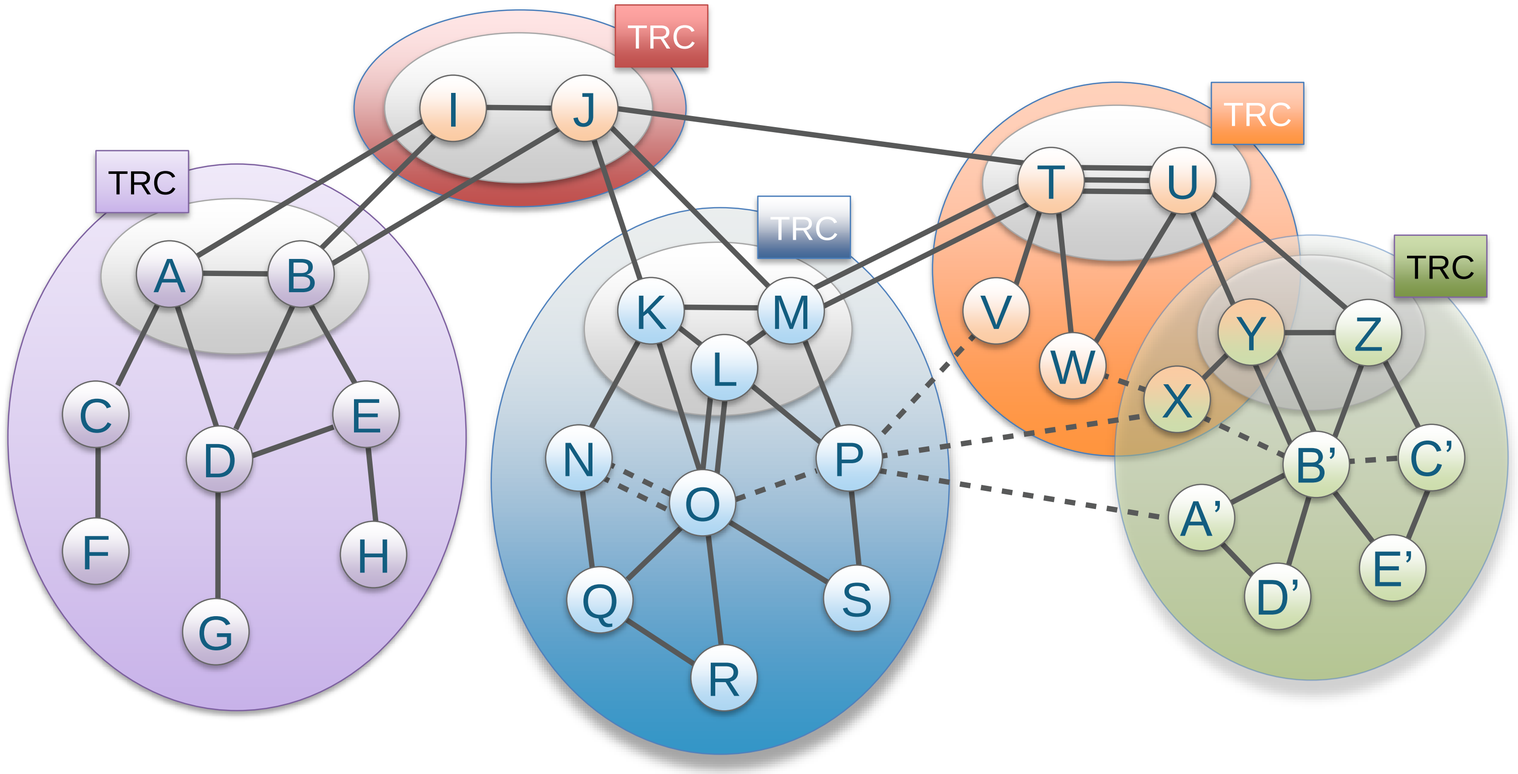
ISDs Improve Scalability

- Routing process can be separated into an *intra*-ISD and an *inter*-ISD process
- Similar to defining “areas” in OSPF or IS-IS



ISDs Enable Heterogeneous Trust and Sovereignty

- Every ISD defines their own trust roots in a “trust root configuration” (TRC)
  - Resolves issues of oligopoly models (Web PKI) and monopoly models (DNSSEC, RPKI)
- External attackers cannot compromise the routing process inside an ISD



SCION Overview in One Slide

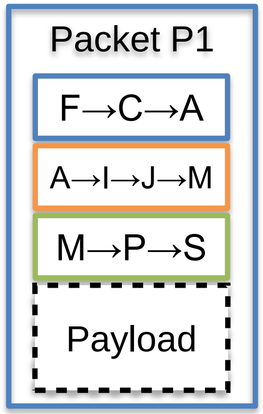
Path-based Network Architecture

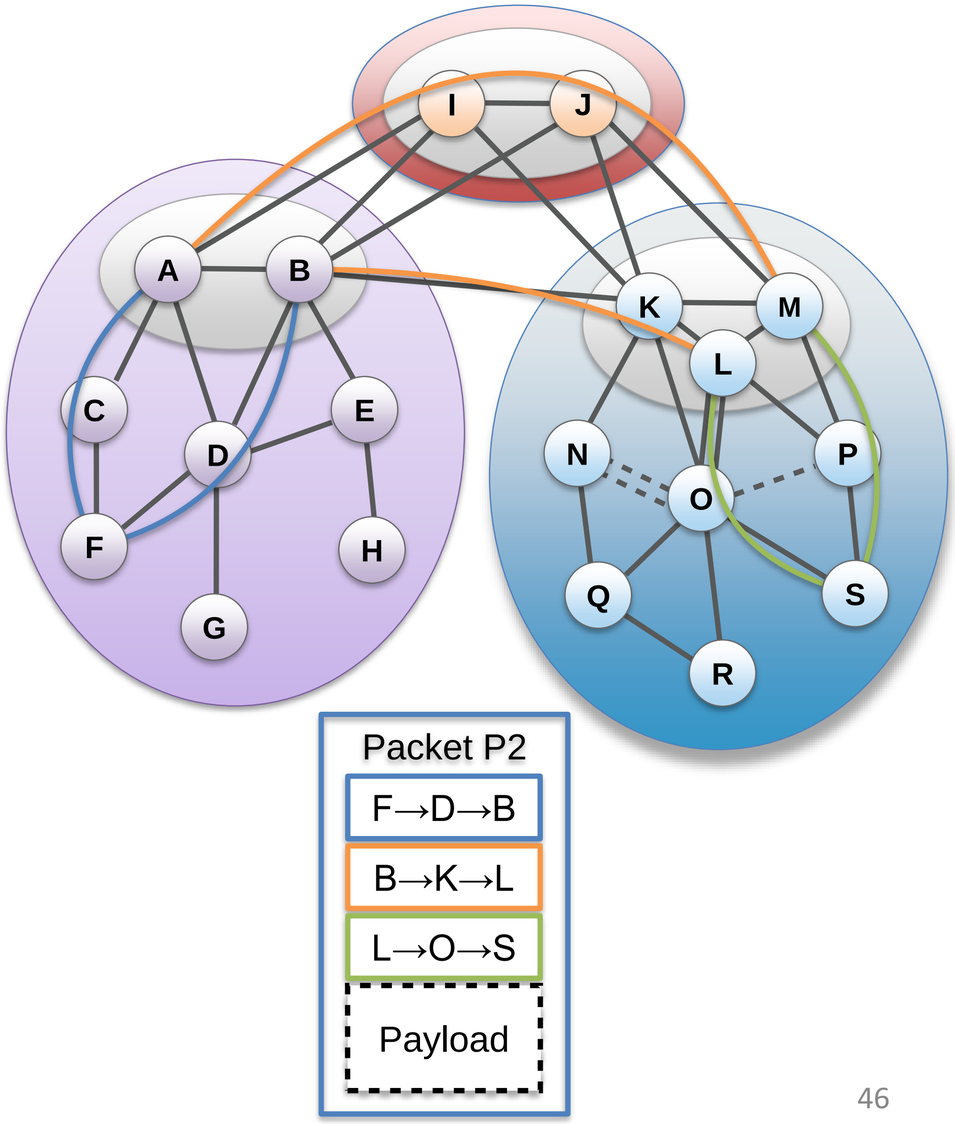
Control Plane - Routing

- Constructs and Disseminates Path Segments

Data Plane - Packet forwarding

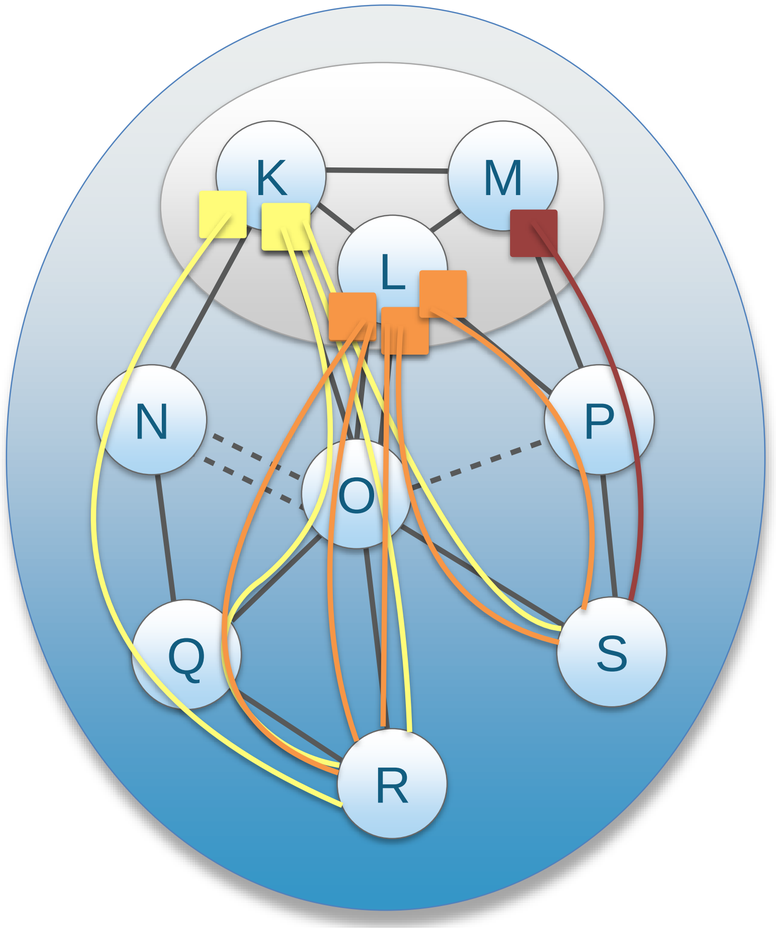
- Combine Path Segments to Path
- Packets contain Path
- Routers forward packets based on Path
  - Simple routers, stateless operation





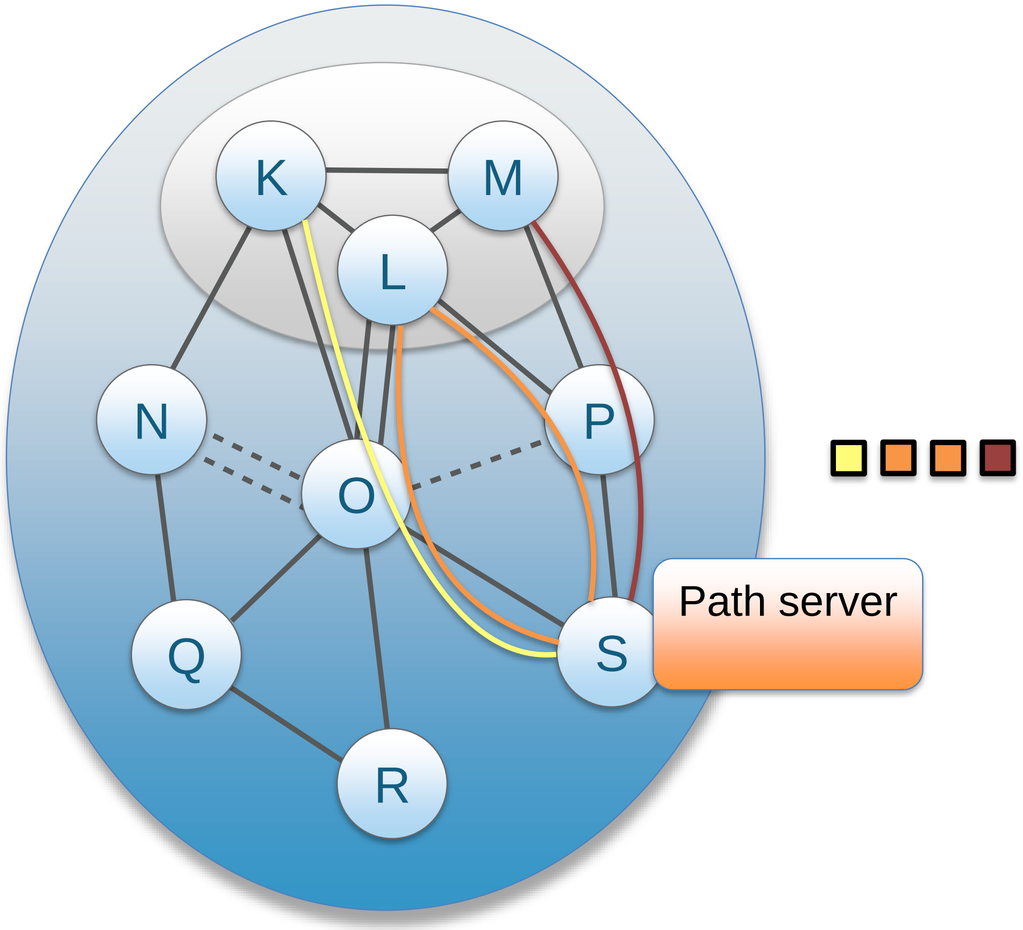
Intra-ISD Path Exploration: Beaconing

- 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 from/to a core AS



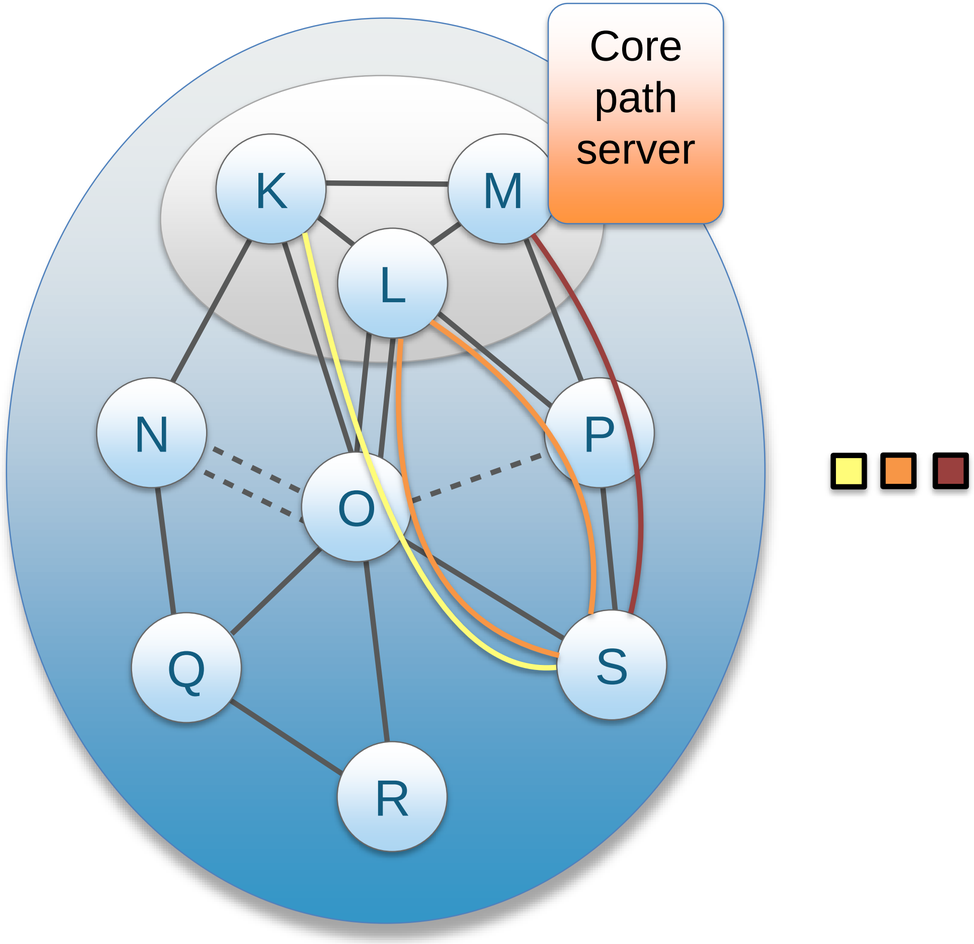
Up-Path Segment Registration

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



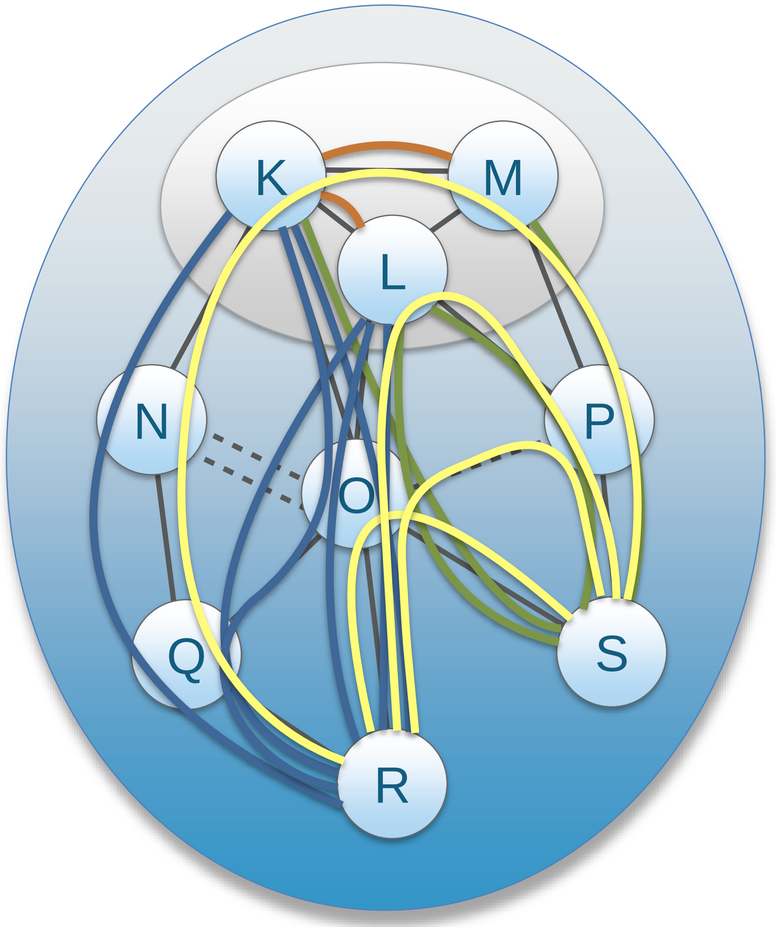
Down-Path Segment Registration

- 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



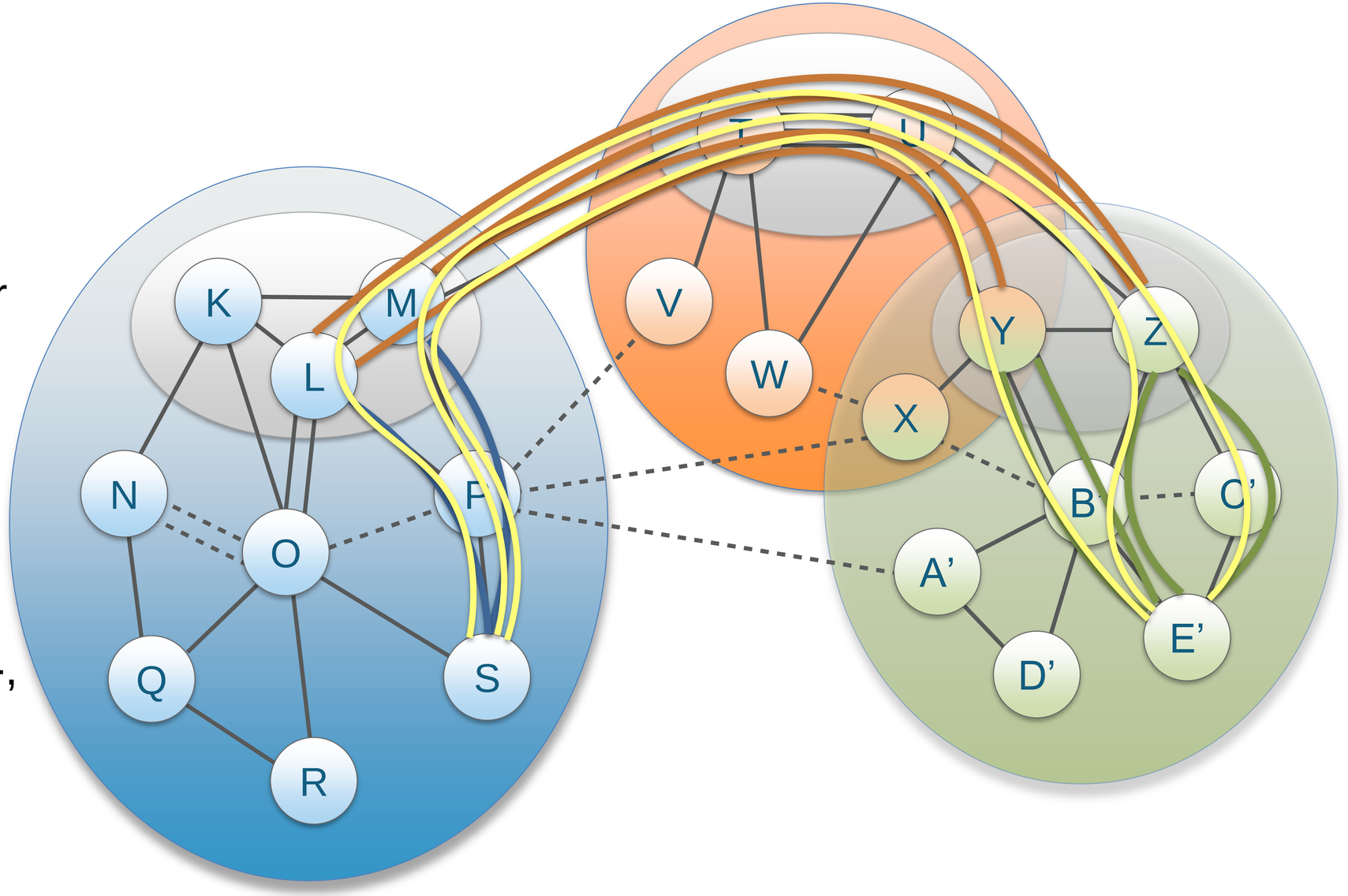
Communication within ISD

- 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



Beaconing vs. BGP(sec)

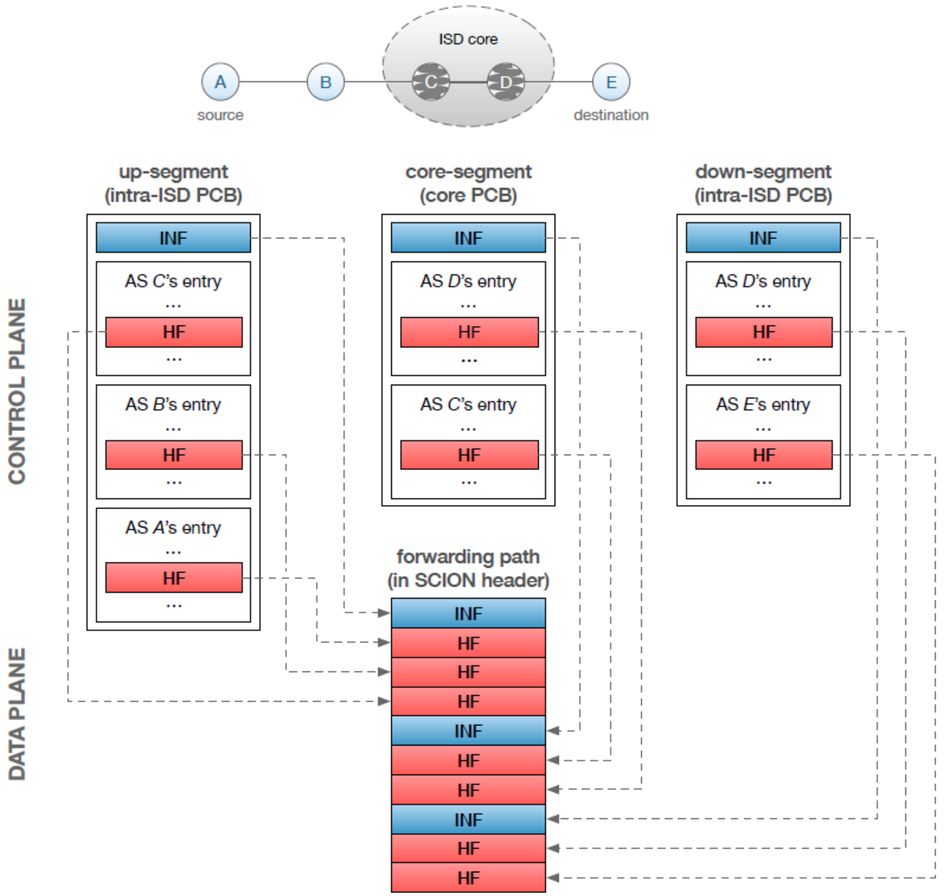
BGP	BGPsec	SCION
No Security	PKI with Kill Switch	Flexible PKI
Single Path	Single Path	Multipath
Poor Scalability	Worse Scalability	Better Scalability (ISDs)
Requires Convergence	Requires Convergence	No Convergence Required

SCION Resolves Routing Hijacks

- All control-plane messages are signed
- End hosts embed path in header → path cannot be changed by off-path attackers
  - End hosts can choose ASes they trust
- AS is an explicit part of end-host addresses
  - End-host address format: $ISD-$AS,$Address
- Extensions provide even stronger security properties
  - Source authentication
  - Path validation

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
  → one AES operation replaces longest-prefix match



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

SCION Production Network

- Led by *Anapaya Systems* (spin-off company of ETH Zurich)

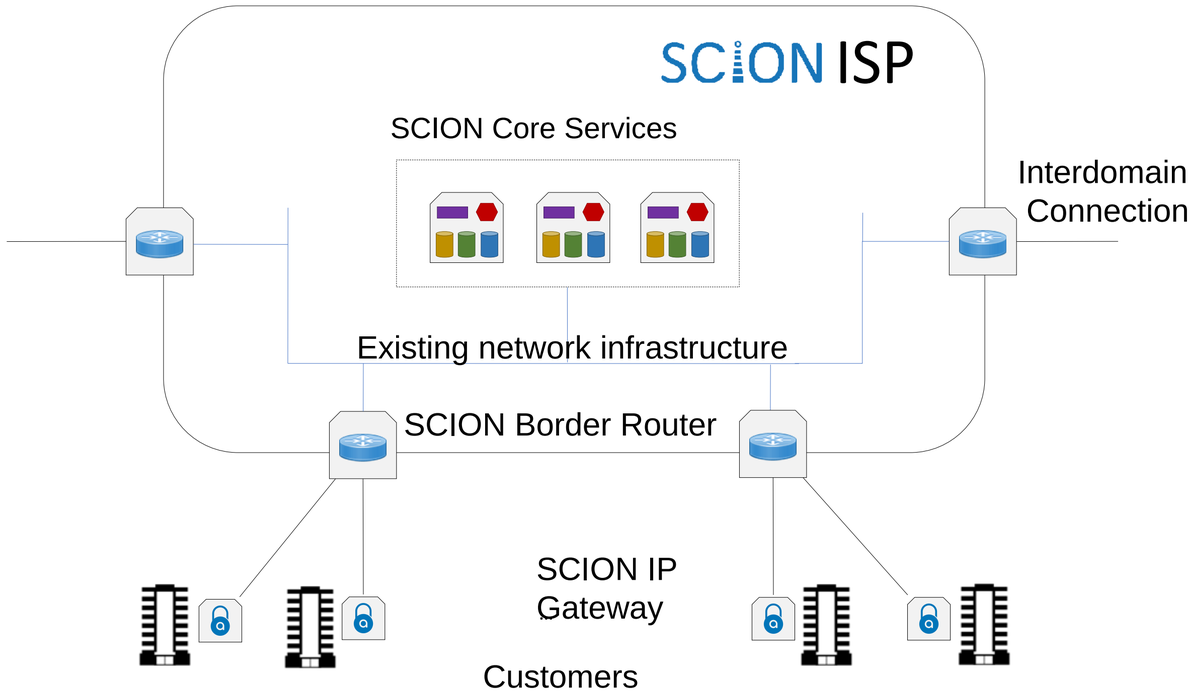
- **BGP-free global communication**
  - Fault independent from BGP protocol

- Deployment with domestic and international ISPs
  - First **inter-continental public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption
- In **production use** by major Swiss banks and Swiss government

SCION:
Implementation and the SCIONLab Testbed

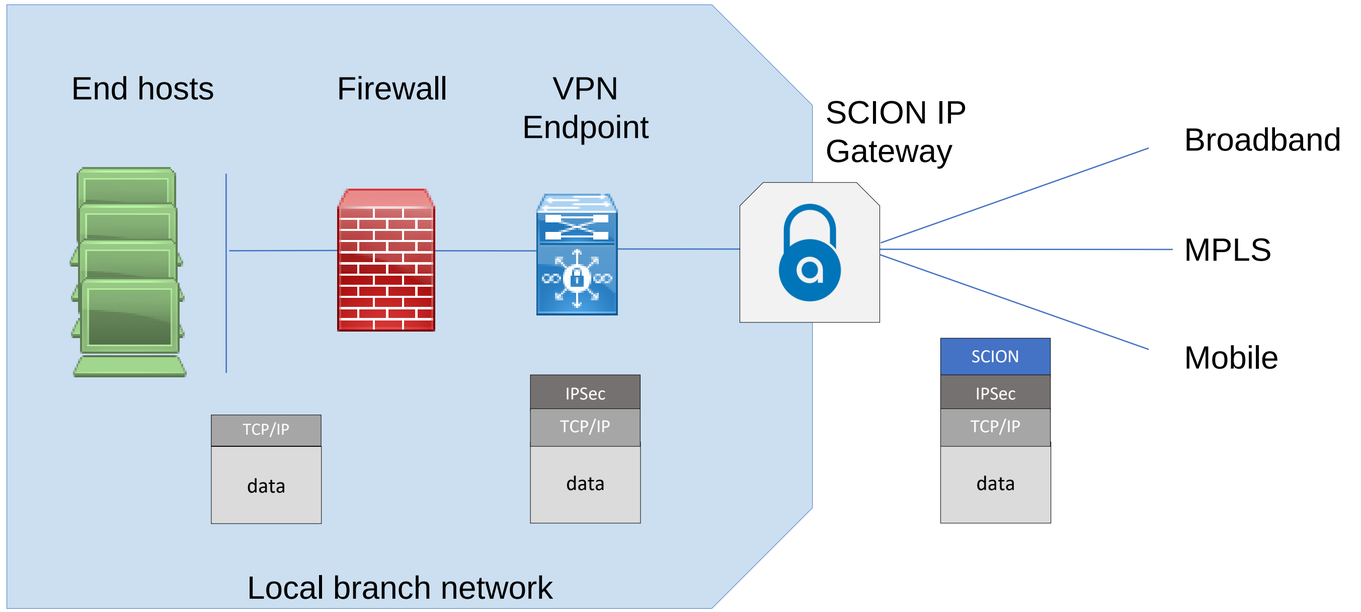
How to Deploy SCION – Core Network

- Two components: SCION core services (control plane) and SCION border routers (data plane)
- SCION reuses existing intra-domain networking infrastructure—no need to upgrade all networking hardware



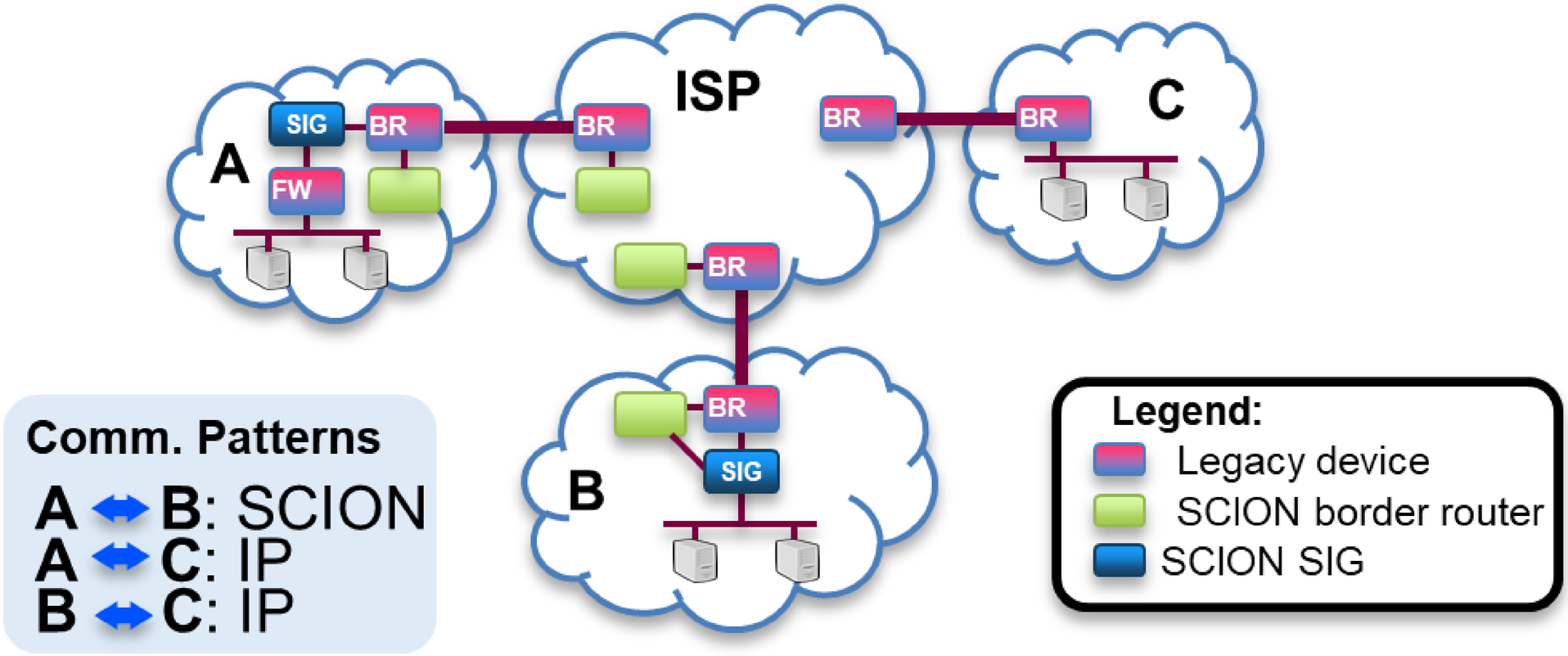
How to Deploy SCION – End Domains

- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or legacy applications needed
- SCION is transport-agnostic thus can work over many different underlaying networks



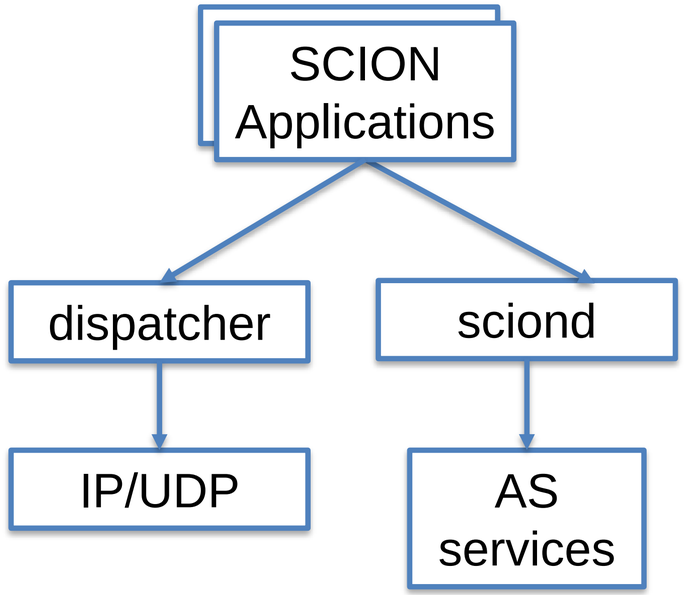
How to Deploy SCION – End Domains

- With SIG the communication over SCION can happen transparently for SCION enabled end domains



End-host Networking Stack

- Software stack for SCION end host application includes:
  - dispatcher: responsible for managing sockets and encapsulating/decapsulating SCION packets for IP/UDP overlay
  - SCION-daemon sciond: responsible for fetching, verifying and caching paths and certificate information from the AS services



- Similarities compared to the IP software stack:
  - dispatcher: corresponds to the kernels socket API
  - sciond: similar to a local caching DNS resolver daemon (like e.g. dnsmasq, unbound), except it's for paths and certificates, not for names

AS Configuration: Topology File

```
$ grep Interfaces -A15 /etc/scion/gen/ISD*/AS*/endhost/topology.json
    "Interfaces": {
      "1": {
        "Bandwidth": 1000,
        "ISD_AS": "17-ffaa:0:1107",
        "LinkTo": "PARENT",
        "MTU": 1472,
        "Overlay": "UDP/IPv4",
        "PublicOverlay": {
          "Addr": "10.0.8.133",
          "OverlayPort": 50000
        },
        "RemoteOverlay": {
          "Addr": "10.0.8.1",
          "OverlayPort": 50168
        }
      }
```

Id of the remote AS

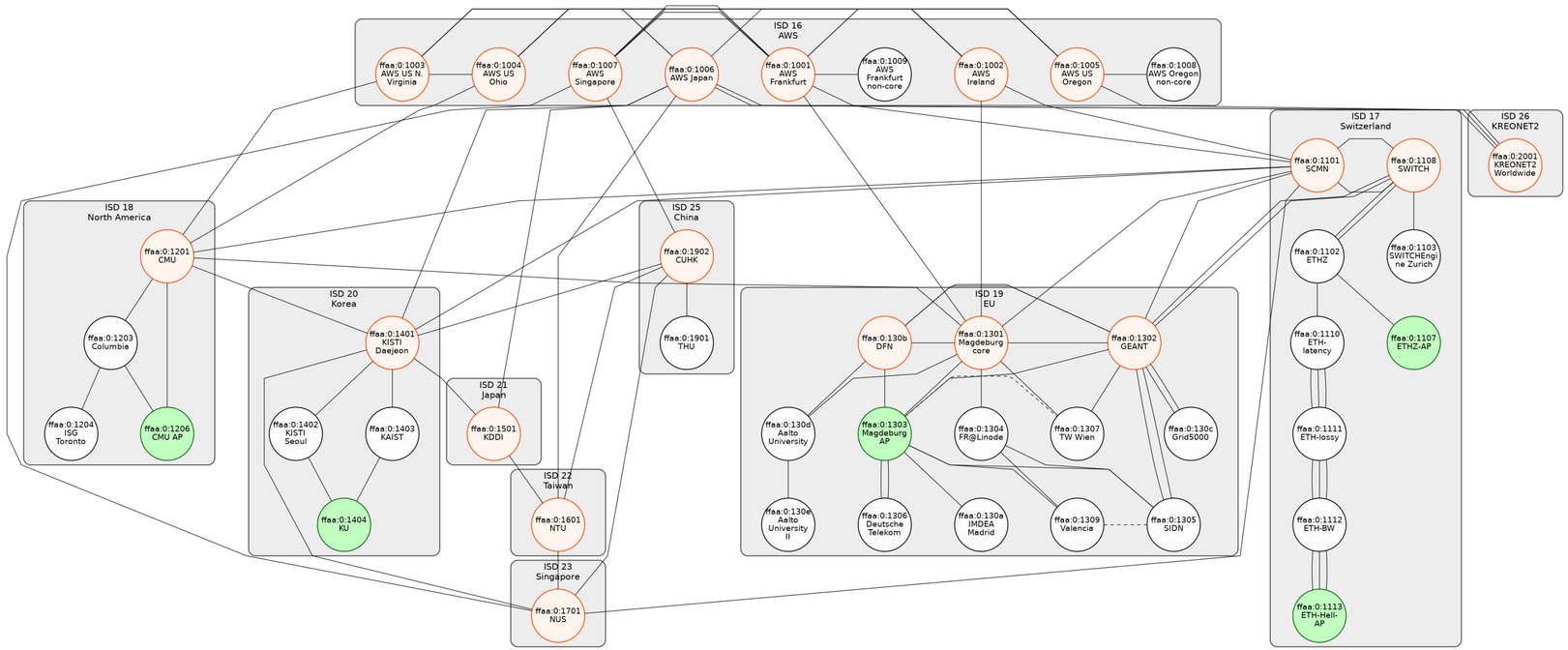
Type of SCION connection (Parent, Client, Peer)

PublicOverlay corresponds to the local address on your (tunnel) interface
In case of using a VPN based connection, the IP address is within the 10.0.8.0/24 subnet

Remote interface address

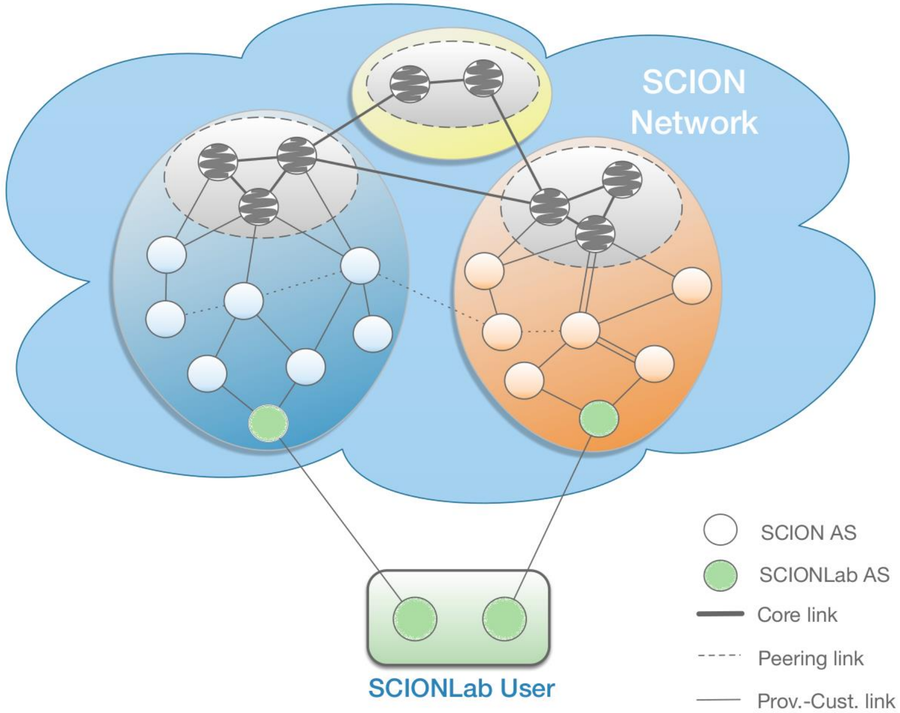
SCIONLab: A SCION-Based Global Networking Testbed

- Open to everyone: create and connect your own AS within minutes
- ISPs: Swisscom, SWITCH, KDDI, GEANT, DFN
- Korea: GLORIAD, KISTI (KREONET), KU, KAIST, ETRI
- Deployed 35+ permanent ASes worldwide, 600+ user ASes

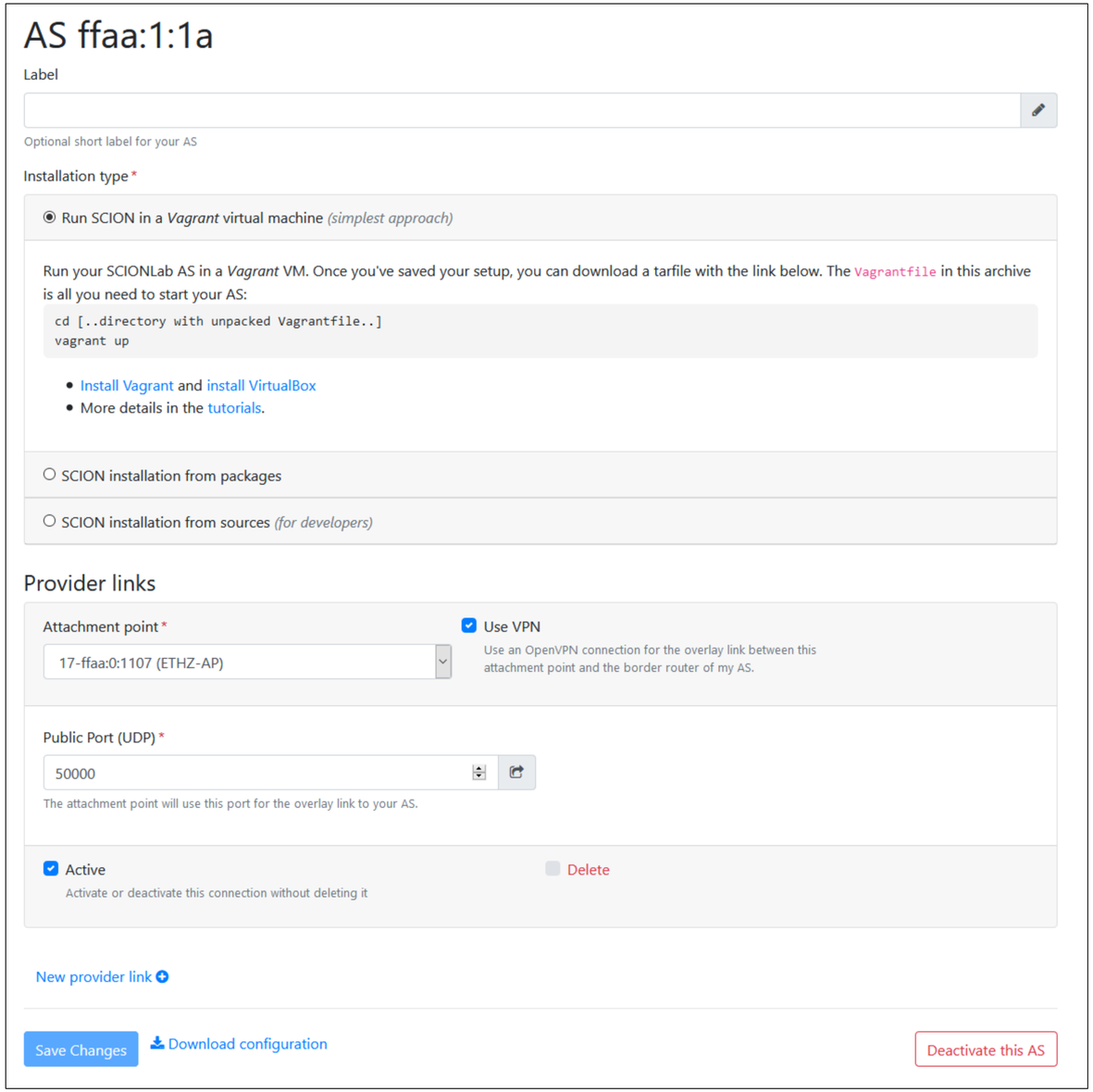


Details about SCIONLab

- http://www.scionlab.org/
- Fast setup, low entry bar for users
- Little required technical expertise: simple, intuitive and automated setup of SCION
- SCION AS can be instantiated as a VM in a few clicks taking around 10 min
- Multiple attachment points
- Support of NATed devices using OpenVPN
- Provision of Debian packages, including ARM (e.g. RaspberryPi)
- BYOC = Bring your own computation ➔ Scale deployment as desired and connect anywhere to SCIONLab



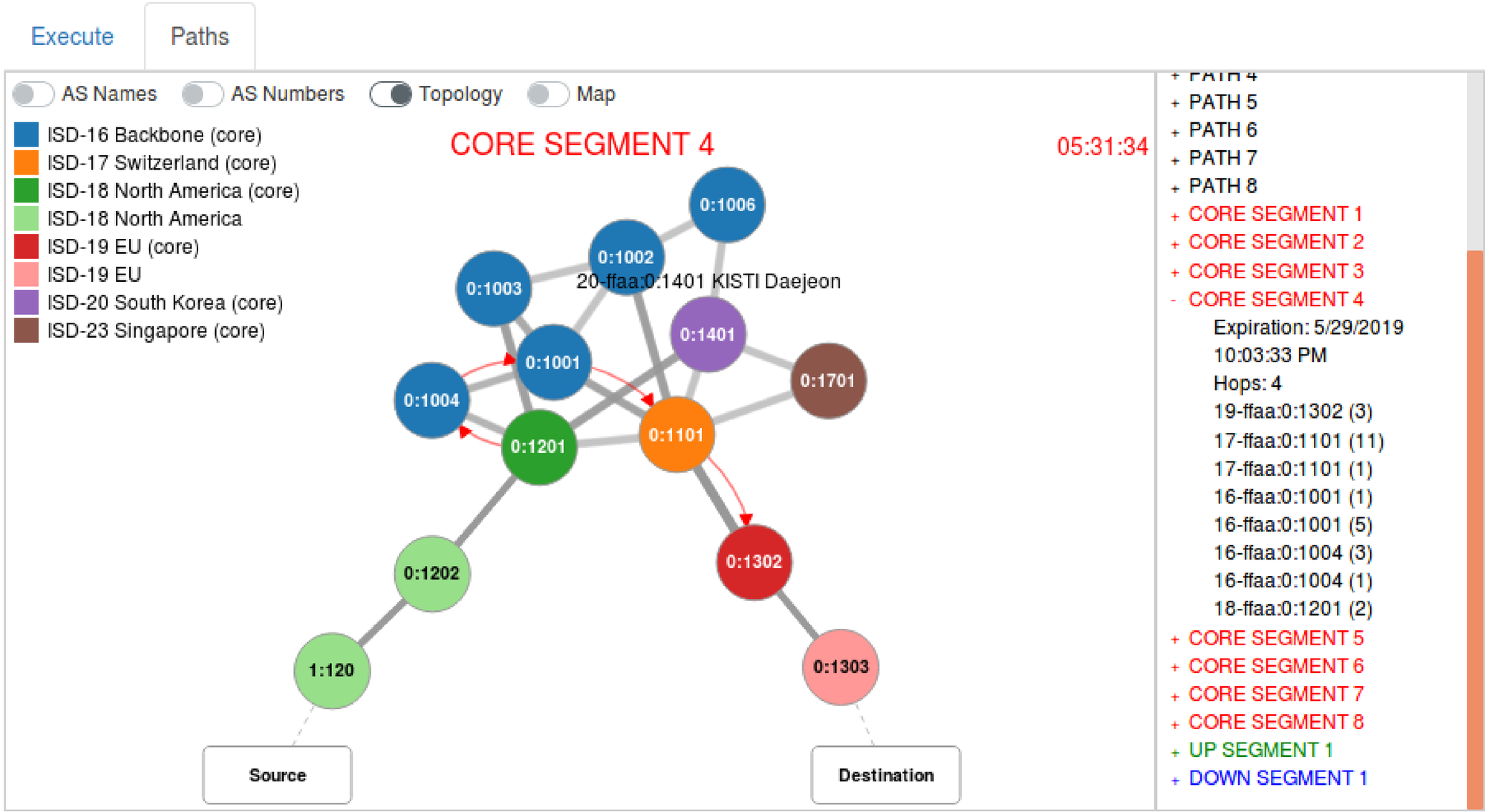
SCIONLab AS Configuration



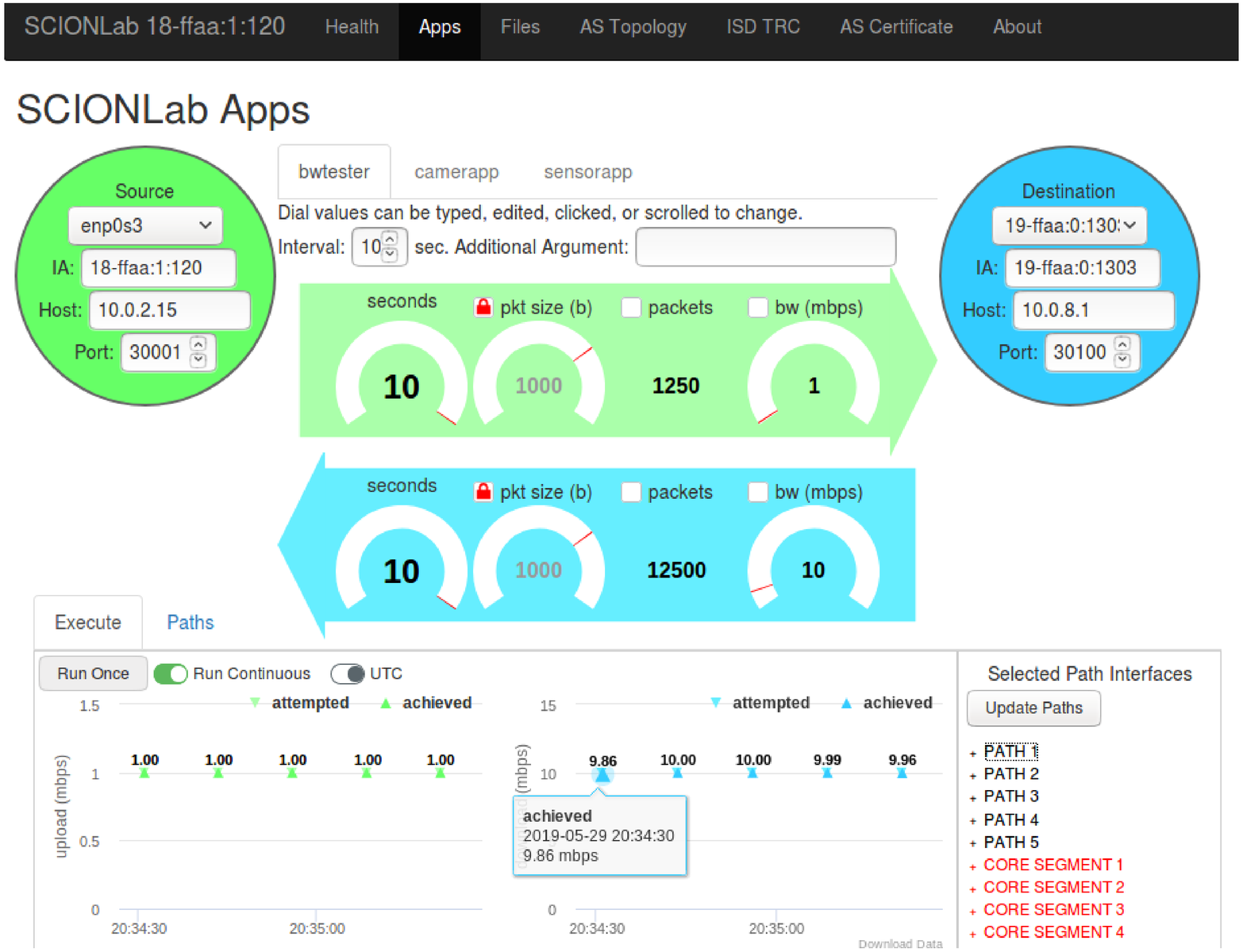
Exciting SCIONLab Research Opportunities

- Next-generation Internet architecture research
- Users obtain real ASes with all cryptographic credentials to participate in the control plane
- ASes can use their own computing resources and attach at several points in the SCIONLab network
- Path-aware networking testbed
- Hidden paths for secure IoT operation
- Control-plane PKI in place, each AS has certificate
- Network availability and performance measurement (bandwidth and latency)
- Supported features (PKI, DDoS defense mechanisms, path selection support, end host / application support)
- (Security) Usability research
- Inter-domain routing scalability research
- Multi-path research
- Multi-path QUIC socket
- End-to-end PKI system that application developers can rely on to build highly secure TLS applications
- SIBRA inter-domain resource allocation system
- DDoS defense research using in-network defense mechanisms
- Next-generation routing architecture policy definitions

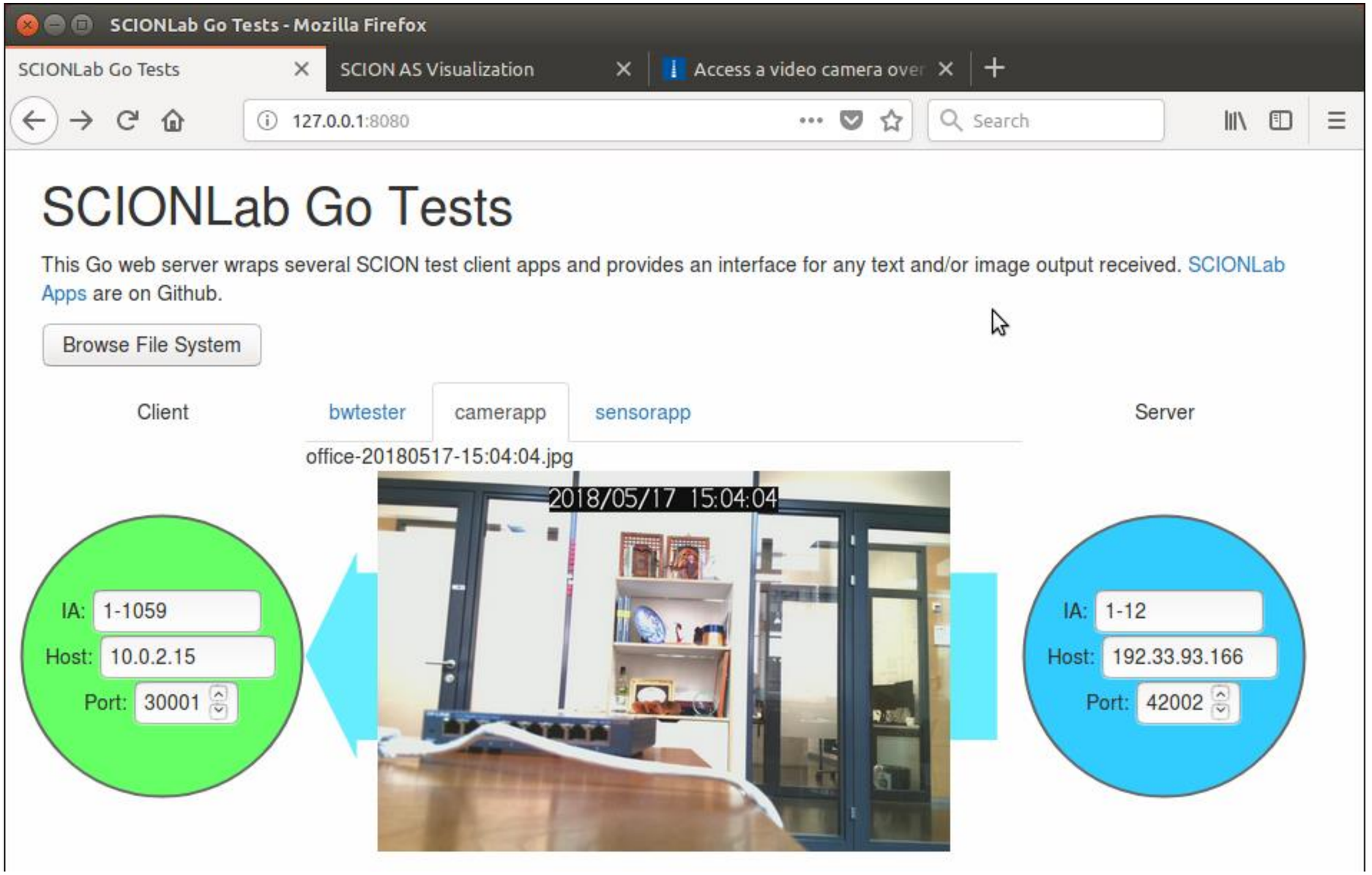
SCIONLab Visualization



Bandwidth Tester



IoT Camera

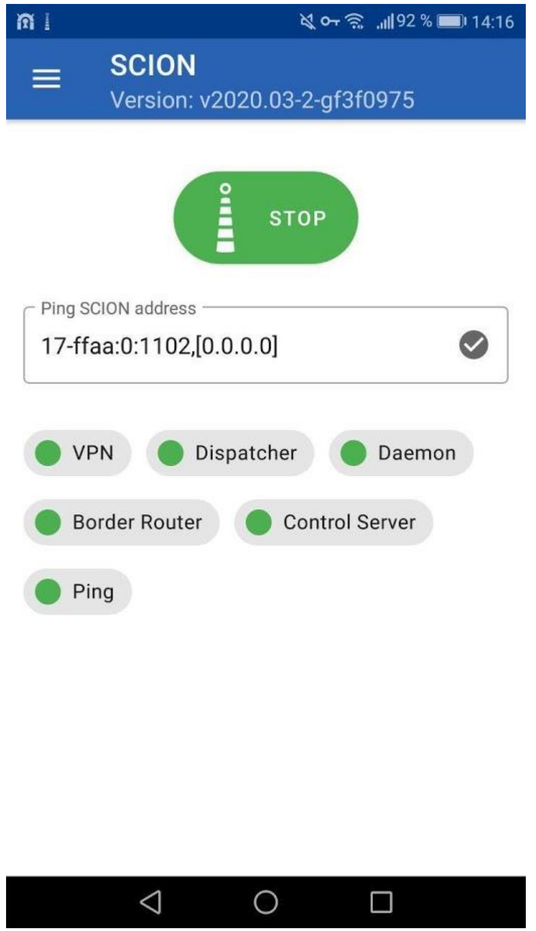

SCIONLab Go Tests - Mozilla Firefox
SCIONLab Go Tests
SCION AS Visualization
Access a video camera over
127.0.0.1:8080
Search
SCIONLab Go Tests
This Go web server wraps several SCION test client apps and provides an interface for any text and/or image output received. SCIONLab Apps are on Github.
Browse File System
Client
bwtester
camerapp
sensorapp
Server
office-20180517-15:04:04.jpg
2018/05/17 15:04:04
IA: 1-1059
Host: 10.0.2.15
Port: 30001
IA: 1-12
Host: 192.33.93.166
Port: 42002

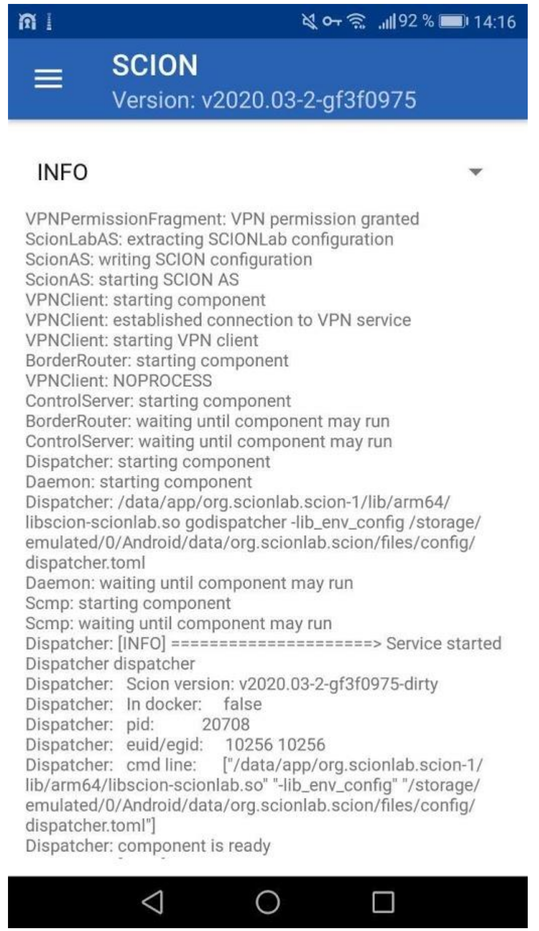
Sensor App


SCIONLab Go Tests - Mozilla Firefox
SCIONLab Go Tests
SCION AS Visualization
Read a temperature sensor
127.0.0.1:8080
Search
SCIONLab Go Tests
This Go web server wraps several SCION test client apps and provides an interface for any text and/or image output received. SCIONLab Apps are on Github.
Browse File System
Client
bwtester
camerapp
sensorapp
Server
Execute sensorapp to retrieve sensor data.
IA: 1-1059
Host: 10.0.2.15
Port: 30001
IA: 1-12
Host: 192.33.93.173
Port: 42003
Execute SCION Client
Reset Fields
Additional Argument:
t=2018-05-17T15:06:51+0000 lvl=info msg="Registered with dispatcher" ia=1-1059 host=10.0.2.15 port=30001
2018/05/17 15:07:36
Motion: 0
Illuminance: 577.9
UV Light: 1
CO2: 532
Sound intensity: 0
Humidity: 52.64
Temperature: 22.81

SCION Android App

- The SCION app enables to run an entire SCION AS attached to the SCIONLab network on an Android smartphone.
- Includes sensor app
- Available at https://play.google.com/store/apps/details?id=org.scionlab.scion

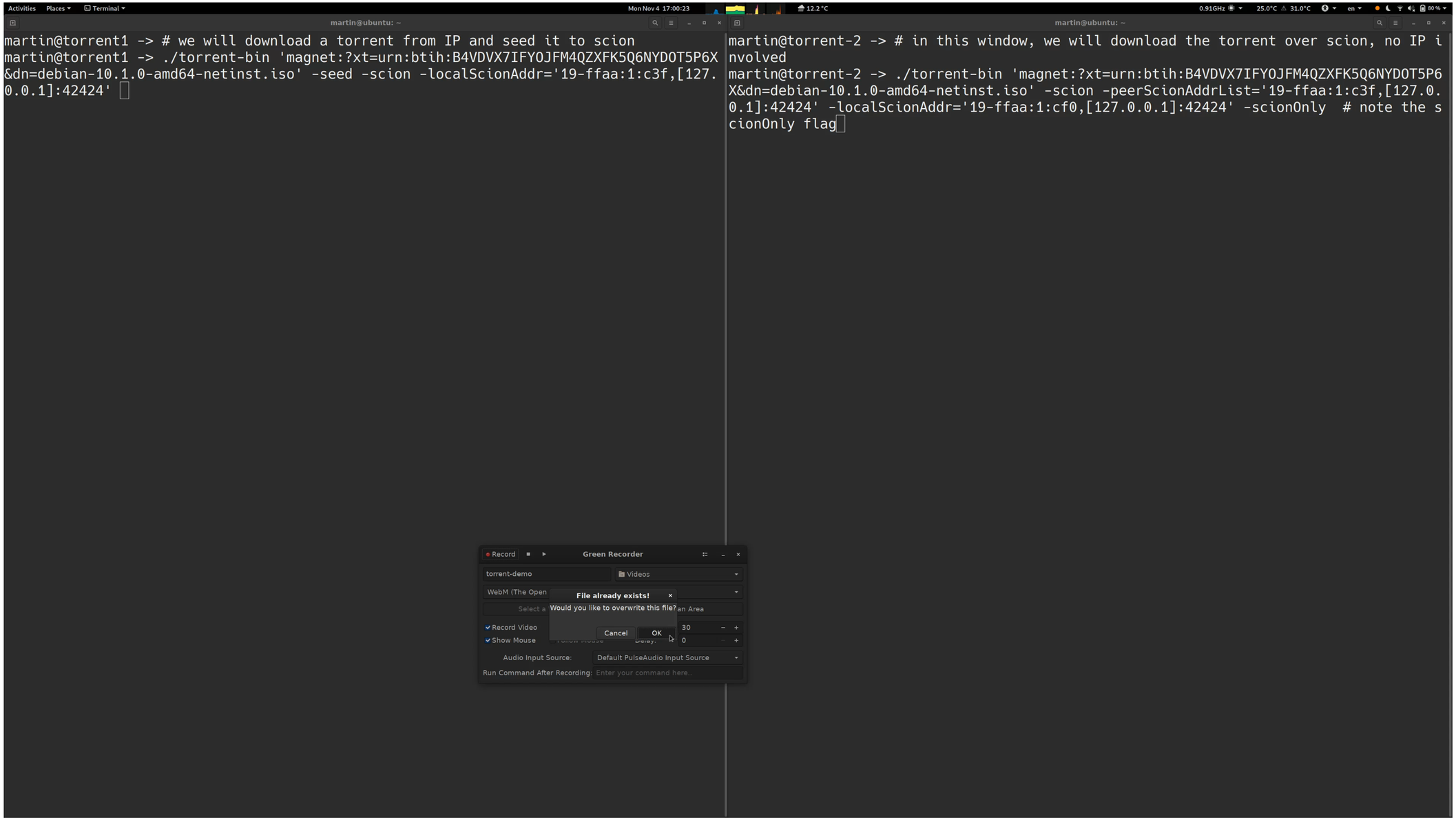




Demo: SCION BitTorrent

- SCION BitTorrent aims to leverage the path-awareness and multipath features of SCION to enable a fast content search and download
  - Find suitable paths to achieve a low search delay
  - Increase throughput of content download through multi-path connections

Demo: SCION BitTorrent



Hands-on Session

Instructions for Hands-on Session

- Visit https://docs.scionlab.org/content/sigcomm/
  - If you haven't done so yet, follow preparation steps
  - (Links posted on Slack)
- Follow step-by-step instructions to set up SCIONLab AS and experiment with it
- Try out optional exercises or explore the rest of the SCIONLab tutorials
- Ask questions on Slack
- Reconvene in Zoom at 4:50 pm for wrap-up

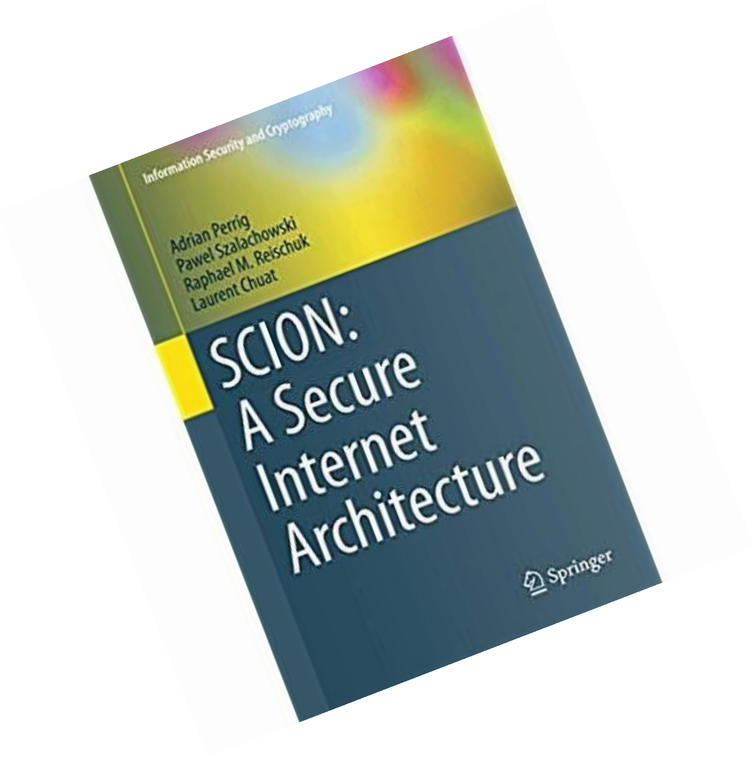
Summary, Wrap-up, and Outlook

SCION Summary

- It is possible to evolve Layer 3:
  - SCION can be deployed without global coordination
  - SCION is a secure Internet architecture that we can use today
  - Production and research networks deployed
- Secure control plane avoids routing attacks
- Path control for end hosts, multipath communication
- Lower latency possible than in today's Internet
- Simpler and more efficient routers
- Open-source implementation

Online Resources

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



Let’s Stay in Touch

- Join the SCION mailing list
- Contact us by email:
  - {adrian.perrig, juan.garcia, markus.legner}@inf.ethz.ch
  - hausheer@ovgu.de
- Join the development in our open-source repository

Thank you for participating!