INF

FACULTY OF
COMPUTER SCIENCE

The SCION Global Research Network

Tony John, David Hausheer

SCION™

Networks and Distributed
Systems Lab (NetSys)

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Benefits of a SCION Connection

Security: Authenticated control plane and resilience against path hijacks.

Stability: Native multipath capability at the network level with rapid path failover ensures high stability despite occasional path failures.

Control: Path-awareness for end hosts enables application-specific path control and optimization

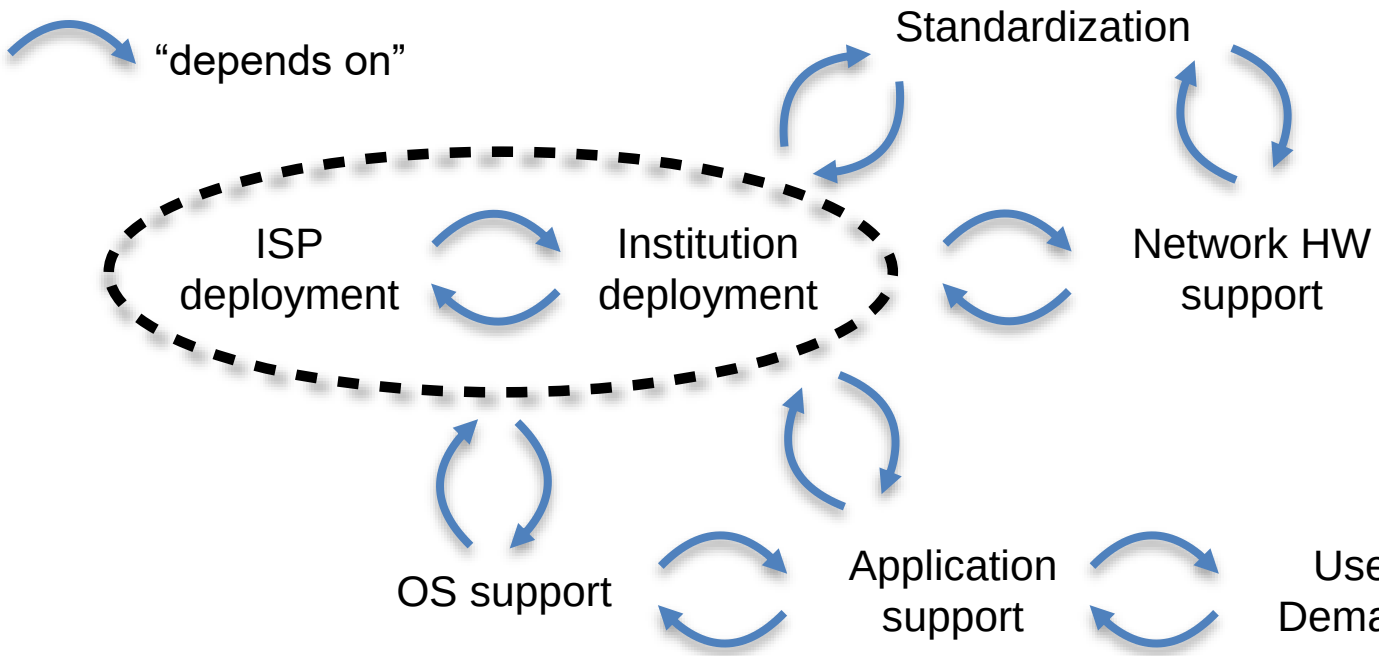
E.g., possibility for traffic geofencing determined by the sender

Protection: Hidden paths and sender-based path selection increase protection against DDoS attacks.

Performance: SCION applications can select the best paths based on latency, bandwidth, loss, or jitter.

Deployment Challenges

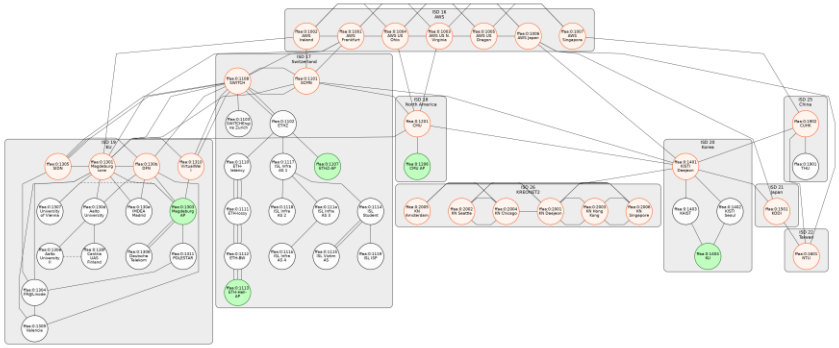
- Disruptive technology: potential risk for incumbents
- RFC 9049 analyses obstacles to deployment in relation to Path Aware Networking approaches
- SCION Overview draft (draft-dekater-panrg-scion-overview-06) also mentions this in Section "1.2.2.1. Avoiding Pitfalls"
- **Our take**: Several circular dependencies complicate deployment



OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

There are two Global SCION Deployments:

- SCIONLab
  - Global SCION research testbed: https://www.scionlab.org
  - Runs as an **overlay** on today's Internet
  - Open to everyone: create and connect own AS within minutes
  - Deployed 35+ permanent ASes worldwide, 600+ user ASes
  - Kwon et al., "SCIONLab: A Next-Generation Internet Testbed", ICNP 2020



- SCION Production Network
  - **Not an overlay!** BGP-free global communication
  - Fault independent from BGP
  - Deployment with ISPs
  - First global public secure communication network
  - cf. Fritz Steinmann (SIX): "SCION Deployment Experience: the Secure Swiss Finance Network (SSFN)", PANRG, IETF118

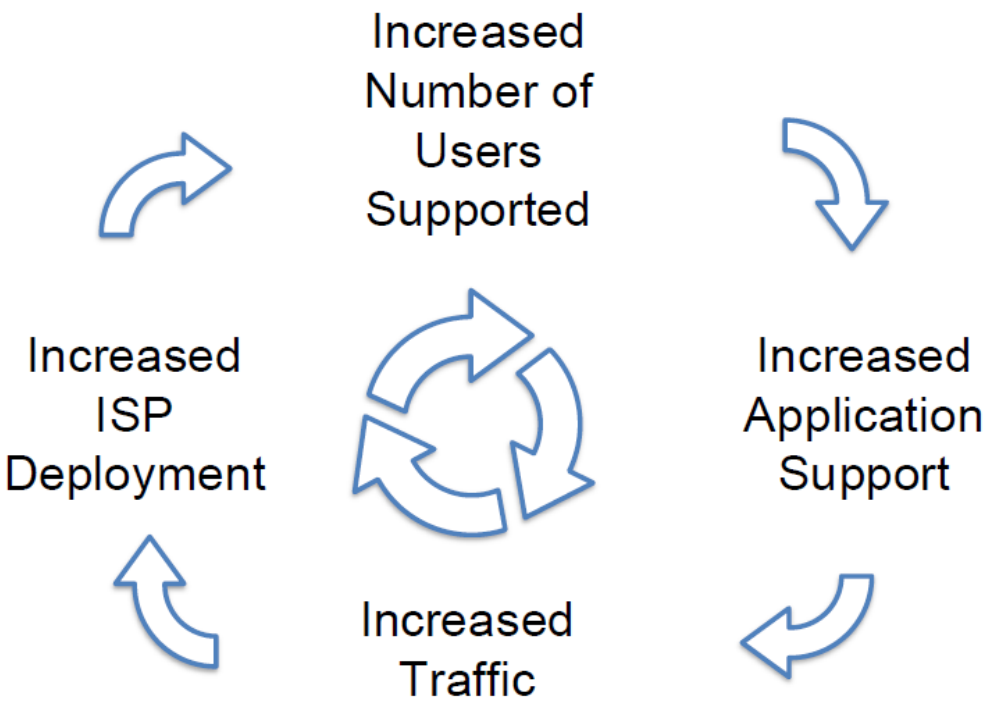
BGP FREE

ANAPAYA cyberlink swisscom interCloud
proximus SWITCH aspo
telindus LG U+ Sunrise KiSTi www.kisti.re.kr
swissix vtx
GÉANT KREONET

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Virtuous Cycle: Proposal to Reach Escape Velocity

- Observation: adoption fuels more adoption



OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

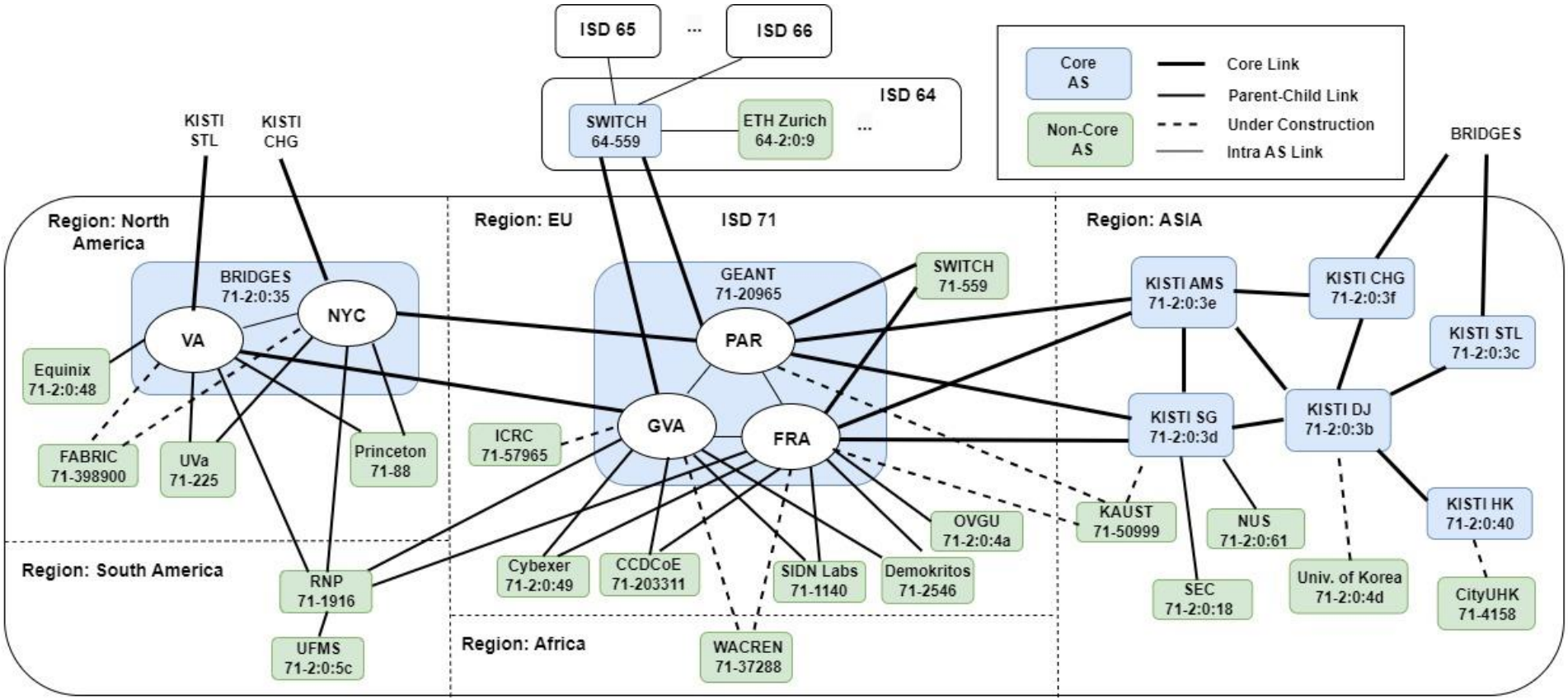
SCION Research and Education Network: Priming the Virtuous Cycle

- **Goal**: Provide universities and research institutes access to the SCION **Production** Network
- With the initial SCION research and education network, around 1/4 million users now have native SCION connectivity
- Initial institutions: BRIDGES/GMU/Internet2, CityUHK, Demokritos, ETH, GEANT, KAUST, KISTI, Korea University, NUS, OvGU Magdeburg, Princeton, SEC, SIDN, SWITCH, UFMS, U of Virginia, WACREN, …
- Applications with 4% user base at Universities will see 10'000 users with native SCION access
- Once applications deploy, traffic increases, setting the cycle in motion …

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

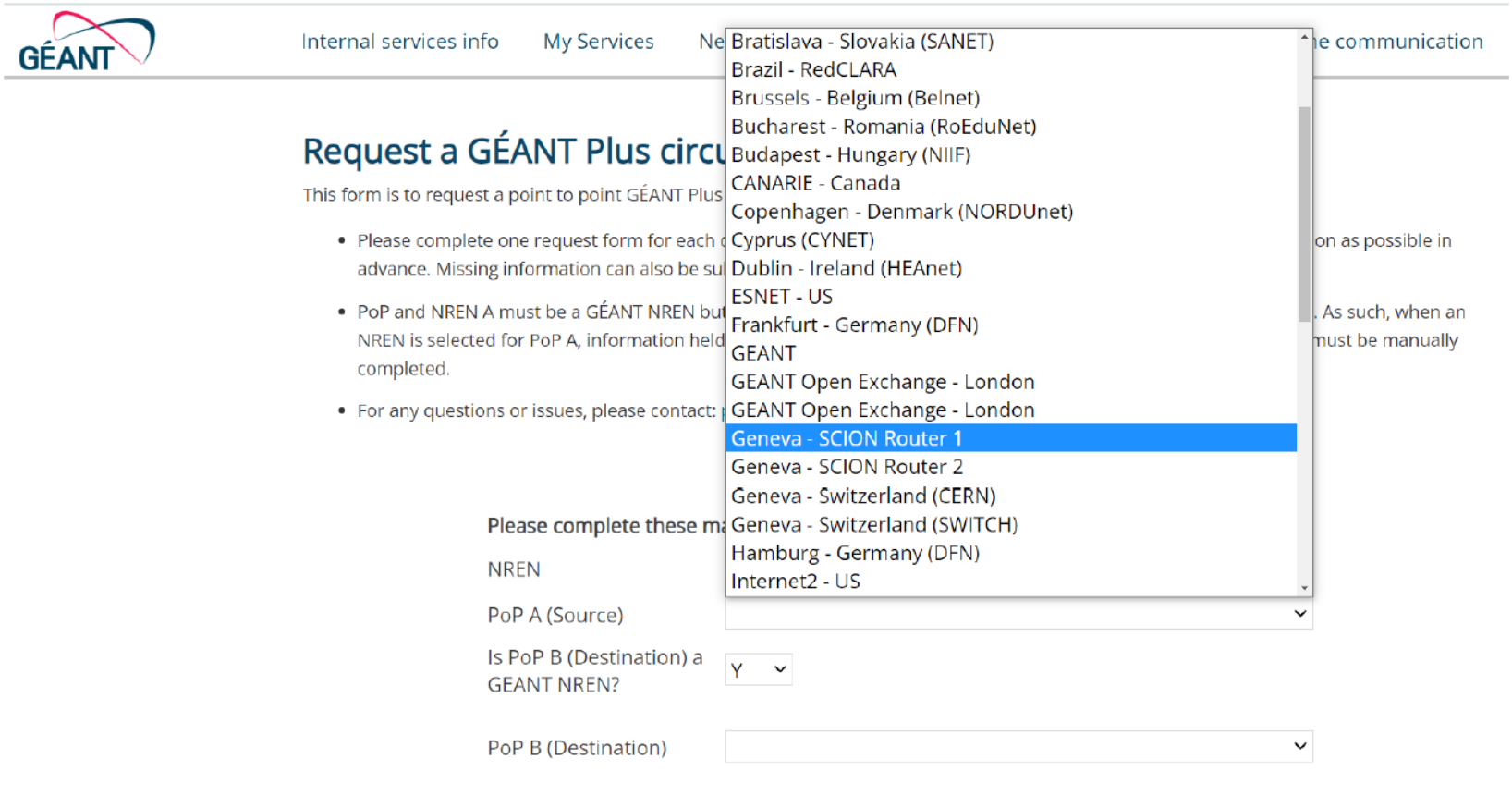
SCION Research and Education Network

- Main networks providing connectivity: GÉANT, Kreonet, Internet2, SWITCH
  - All links are L2 based (i.e. independent of BGP)



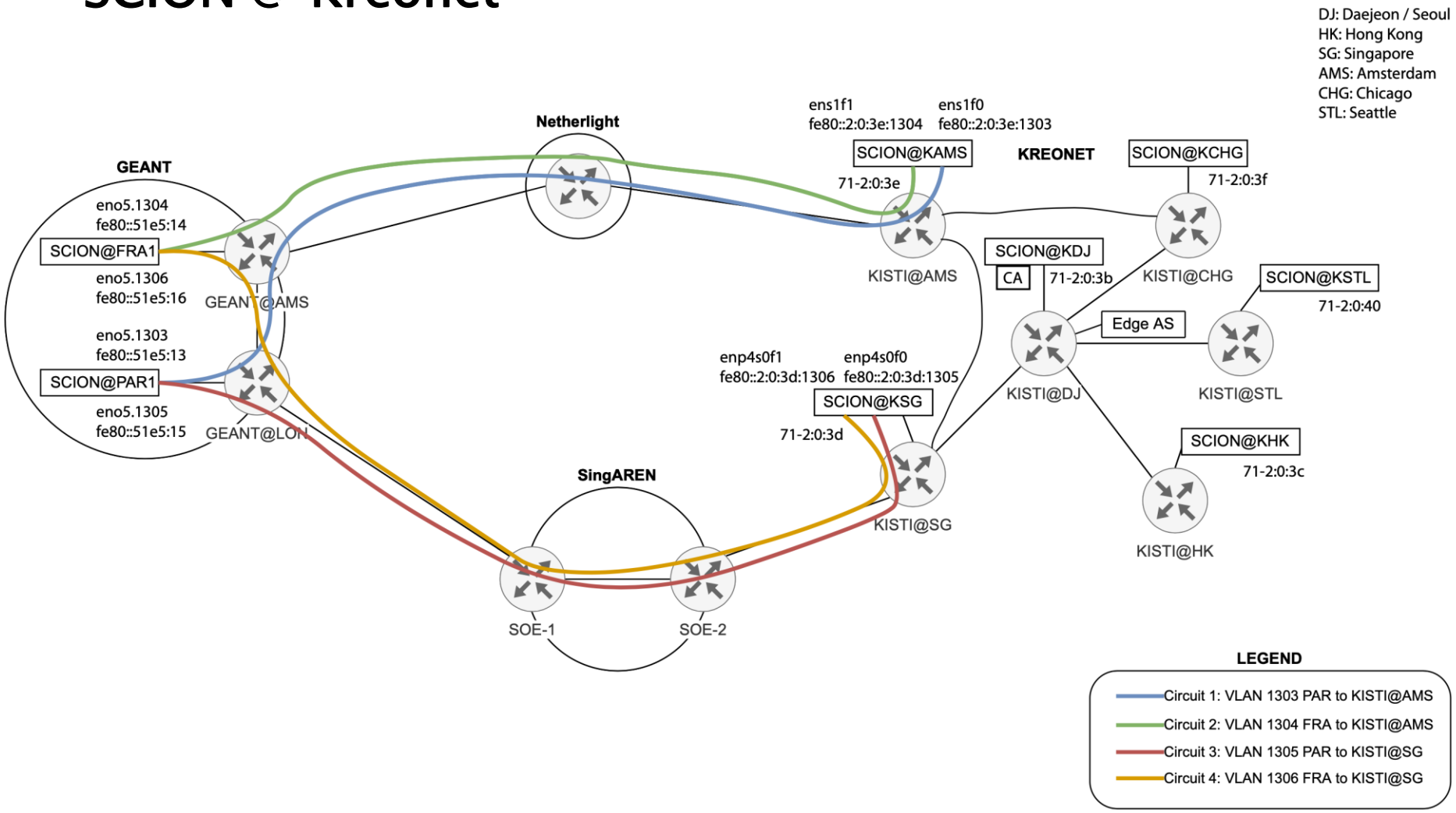
SCION @ GEANT

- GEANT members (NRENs) can establish SCION link by requesting a GEANT Plus (L2) circuit to one of 3 SCION PoPs (GVA, FRA, PAR)



OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

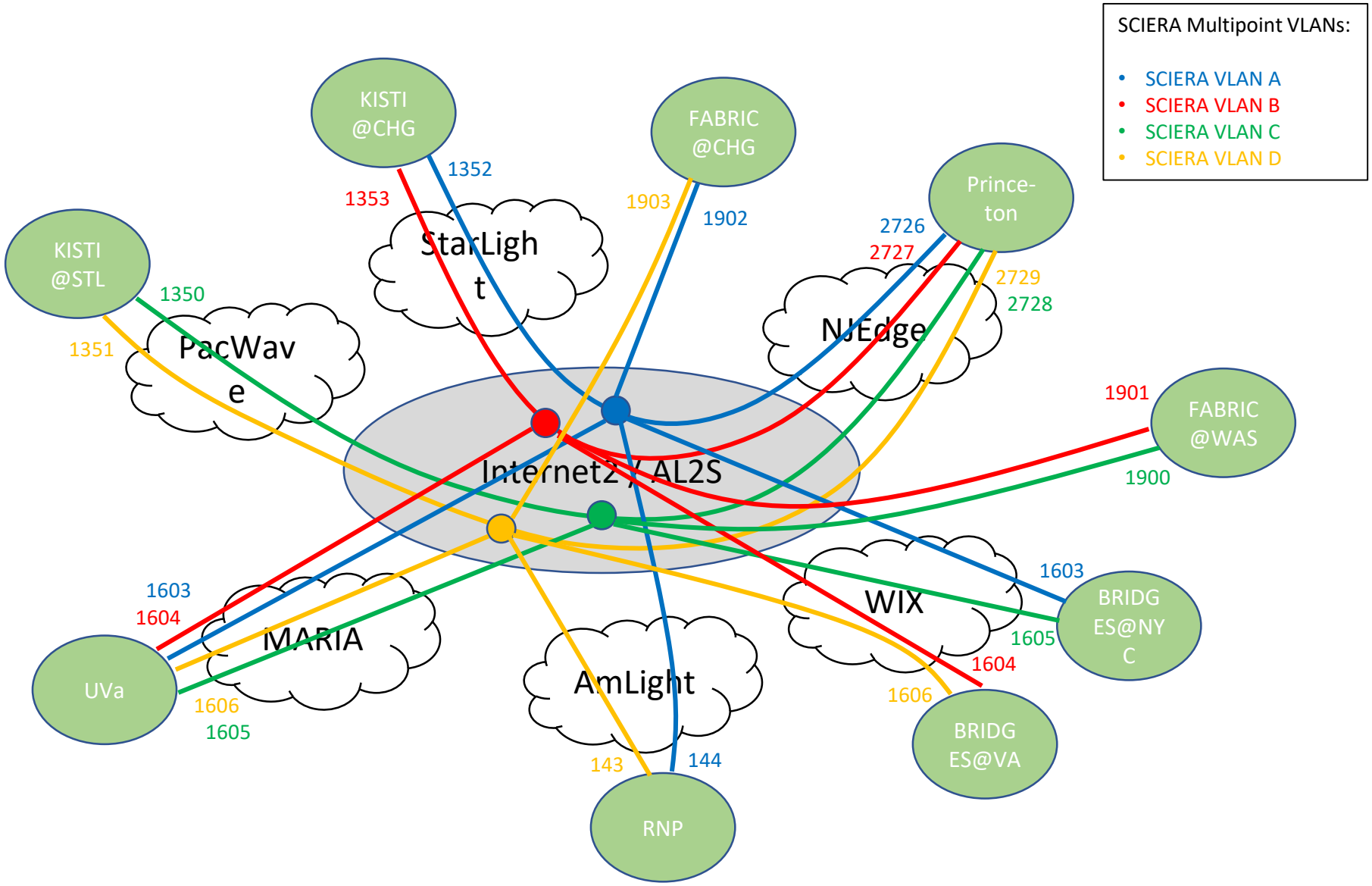
SCION @ Kreonet



➔ Kreonet facilitates SCION connectivity in both directions around the globe: Europe <> Asia <> US <> Europe

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

SCION @ Internet2



SCION @ SWITCH

SWITCHlan SCION Access

Factsheet

More security, reliability and control: SWITCHlan SCION access provides the best conditions for ensuring that your data is only transferred to the parts of the internet that you want it to reach.

The secure internet architecture of the next generation

These days, digitalisation requires secure networks that are easy to control. However, the foundation of the internet was laid last century without any special security mechanisms, and it has hardly been updated since. That makes it vulnerable. Nowadays, cybercriminals exploit vulnerabilities to such a degree that IT departments spend the majority of their time trying to prevent and eliminate cyber threats. This observation concerns not only the multitude of security risks, but also aspects of the transport network. It's high time for an upgrade. SCION (Scalability, Control, and Isolation On Next-Generation Networks) is that upgrade. SWITCHlan SCION access combines the security, reliability and control of private networks with the flexibility of the public internet. The technology was developed at the Swiss Federal Institute of Technology (ETH) in Zurich. SWITCH has supported SCION's development at ETH Zurich since 2015.

How you benefit

- **Security by design:** SWITCHlan SCION access protects against cyber attacks such as prefix hijacking and specific DDoS attacks
- **New security features:** path control and path verification
- **Path control:** you define the networks to which your data is confined; you define the route your data packets take
- **Path verification:** the path and integrity of all packages is cryptographically secured and verifiable
- **Multi-pathing:** reliable data transfer via multiple network paths at the same time
- **Cybersecurity:** your data can no longer be redirected during transfers; protection against DDoS reflection attacks
- **Isolation domains:** trust limited to participants of an ISD (no more global trust roots)

High degree of reliability

SCION's architecture gives you a high degree of reliability with various features and new concepts. As a result, some attacks can be prevented from the very outset: SCION is immune to prefix hijacking. What is more, the technology reduces the risk of exposure to distributed denial of service (DDoS) attacks through hidden paths and source authentication. The protection provided against address spoofing even prevents susceptibility to DDoS reflection attacks.

Reliability and performance through multi-pathing

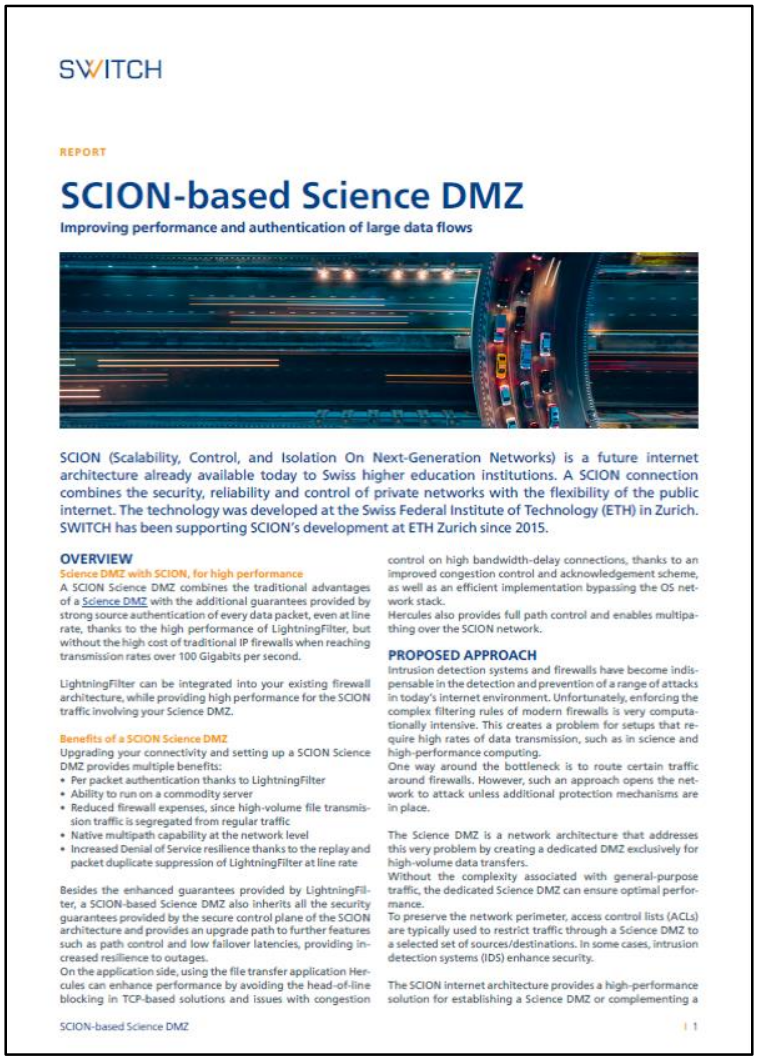
Multi-pathing allows the SCION protocol to open up multiple potential paths that can be used simultaneously. This increases the usable capacity in the network and enables faster switching in the event of path failures, provided that the application supports this function.

In this instance, the granularity of the path selection is restricted to the transfer points between networks (autonomous systems). The path within a network is not subject to the control of SCION, meaning alternative paths cannot be used there.

More control with SCION

SCION gives you path control over your end-to-end communication, allowing you to avoid certain network sections such as networks in unstable regions. Control over path choice also allows you to make selections regarding available bandwidths and latencies. This increases the security of your data in terms of how it is handled. You get more control over the transport route of your sensitive data.

SWITCH



SWITCH

REPORT

SCION-based Science DMZ

Improving performance and authentication of large data flows

SCION (Scalability, Control, and Isolation On Next-Generation Networks) is a future internet architecture already available today to Swiss higher education institutions. A SCION connection combines the security, reliability and control of private networks with the flexibility of the public internet. The technology was developed at the Swiss Federal Institute of Technology (ETH) in Zurich. SWITCH has been supporting SCION's development at ETH Zurich since 2015.

OVERVIEW

Science DMZ with SCION, for high performance

A SCION Science DMZ combines the traditional advantages of a Science DMZ with the additional guarantees provided by strong source authentication of every data packet, even at line rate, thanks to the high performance of LightningFilter, but without the high cost of traditional IP firewalls when reaching transmission rates over 100 Gigabits per second.

LightningFilter can be integrated into your existing firewall architecture, while providing high performance for the SCION traffic involving your Science DMZ.

Benefits of a SCION Science DMZ

Upgrading your connectivity and setting up a SCION Science DMZ provides multiple benefits:

- Per packet authentication thanks to LightningFilter
- Ability to run on a commodity server
- Reduced firewall expenses, since high-volume file transmission traffic is segregated from regular traffic
- Native multipath capability at the network level
- Increased Denial of Service resilience thanks to the replay and packet duplicate suppression of LightningFilter at line rate

Besides the enhanced guarantees provided by LightningFilter, a SCION-based Science DMZ also inherits all the security guarantees provided by the secure control plane of the SCION architecture and provides an upgrade path to further features such as path control and low failover latencies, providing increased resilience to outages.
On the application side, using the file transfer application Hercules can enhance performance by avoiding the head-of-line blocking in TCP-based solutions and issues with congestion control on high bandwidth-delay connections, thanks to an improved congestion control and acknowledgement scheme, as well as an efficient implementation bypassing the OS network stack.
Hercules also provides full path control and enables multipathing over the SCION network.

PROPOSED APPROACH

Intrusion detection systems and firewalls have become indispensable in the detection and prevention of a range of attacks in today's internet environment. Unfortunately, enforcing the complex filtering rules of modern firewalls is very computationally intensive. This creates a problem for setups that require high rates of data transmission, such as in science and high-performance computing.
One way around the bottleneck is to route certain traffic around firewalls. However, such an approach opens the network to attack unless additional protection mechanisms are in place.

The Science DMZ is a network architecture that addresses this very problem by creating a dedicated DMZ exclusively for high-volume data transfers.
Without the complexity associated with general-purpose traffic, the dedicated Science DMZ can ensure optimal performance.
To preserve the network perimeter, access control lists (ACLs) are typically used to restrict traffic through a Science DMZ to a selected set of sources/destinations. In some cases, intrusion detection systems (IDS) enhance security.

The SCION internet architecture provides a high-performance solution for establishing a Science DMZ or complementing a

https://www.switch.ch/scion/

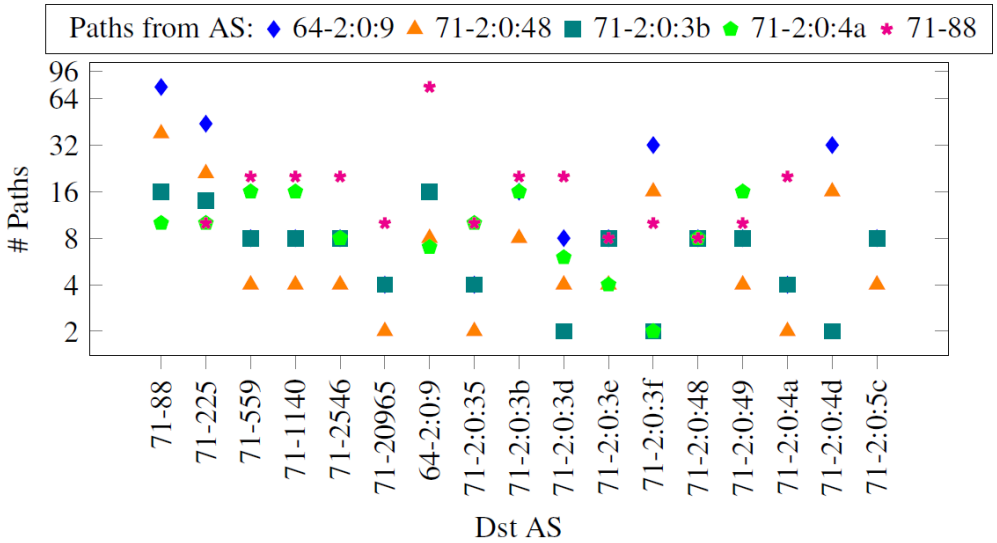
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

Deployment Observations

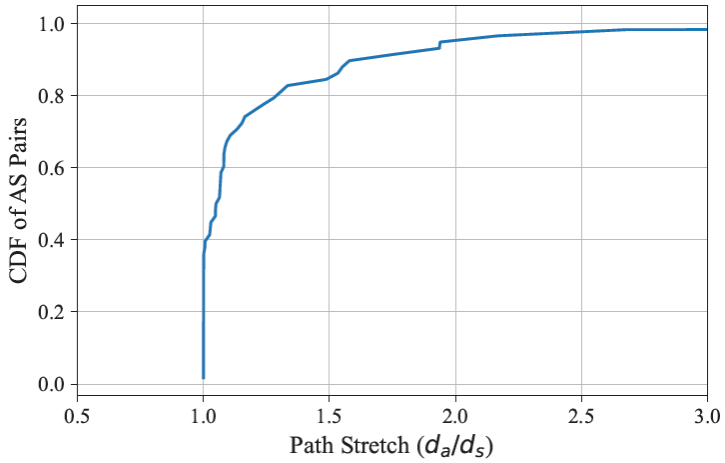
- **Heterogeneous** deployment with a mixture of
  - SCION implementations (Anapaya & Open Source) ➔ Interoperable!
  - Operation models (managed & self-operated)
- We probably encountered almost every corner case
- Over 25 ASes (NRENs, universities, research institutes)
- Presence in all major continents

Evaluation Results

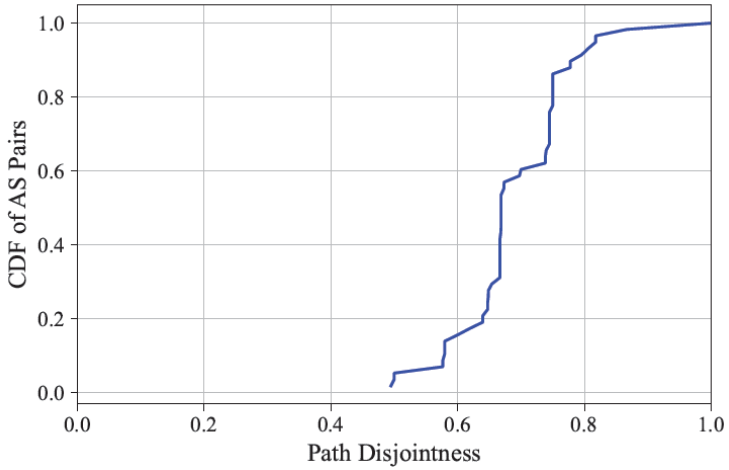
Number of paths measured by source



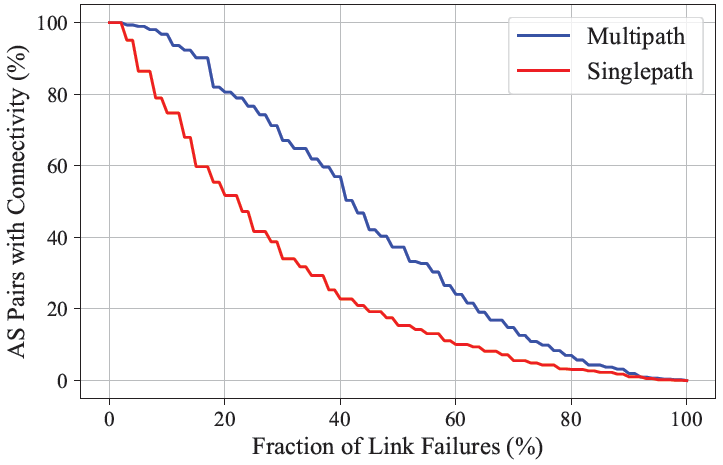
CDF of path stretches (d_a/d_s).



CDF of path disjointness for all AS pairs



Impact of link failures on AS connectivity



OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
Networks and Distributed Systems Lab
Prof. Dr. David Hausheer
Networks and Distributed Systems Lab (NetSys)

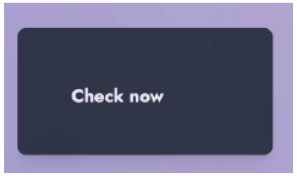
Simplify Native SCION Usage

- Bootstrapper infrastructure provides SCION configuration information to local applications, avoiding user configuration
- End host software facilitates building of native SCION applications
  - Simplest way is to use JPAN library with Java
  - Several SCION libraries for Golang
  - Many projects offering SCION support, listed on the “Awesome SCION” page: https://github.com/scionproto/awesome-scion

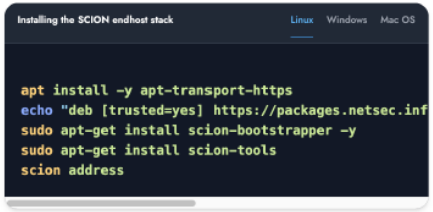
SCION Tools and Application Examples

- https://scion-architecture.net/apps/

Discover if you have SCION connectivity

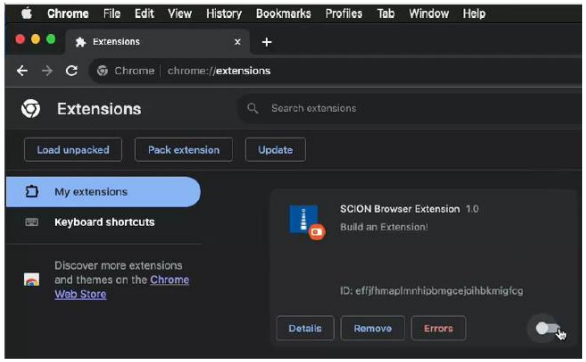


How to set up SCION on your host



Sending your first SCION packet

- chrome SCION Integration



- SCION Ping and Path Fetcher
  - `scion ping 71-2:0:5c,127.0.0.1`
  - `scion showpaths 71-2:0:5c`
- Dancing Gazelle: Is SCION Working?
  - http://gazelle.scionapps.com

- SCION Packet Inspector
  - https://scionpacketinspector.netsec.ethz.ch

Open Questions

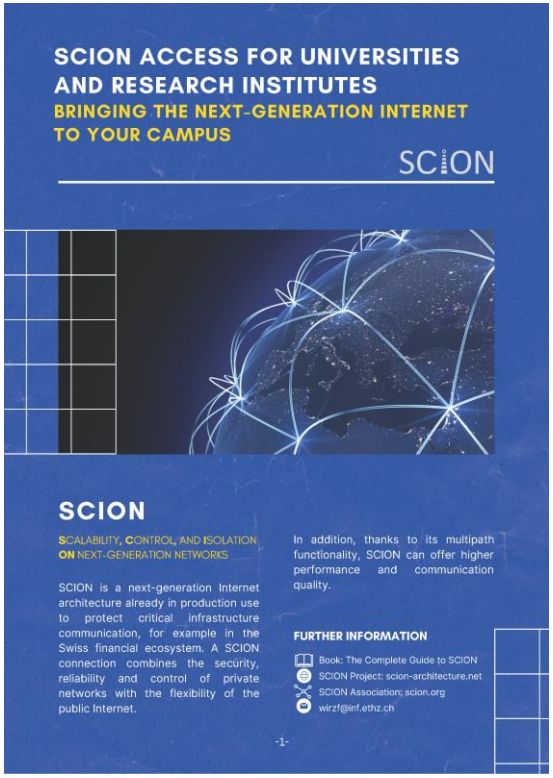
- How to better integrate SCION with endpoints (SVC-B RFC 9460, RFC 9461, Happy Eyeballs, MP-QUIC)?

- Proposal for Integrating Deadline-Aware Streams into Multipath QUIC using DMTP
  - https://github.com/quicwg/multipath/issues/453
  - https://mailarchive.ietf.org/arch/msg/quic/TnKyqN6XnaUEYt9zyDXc1soN9DM

Conclusion

- SCION production network is expanding
- With the SCION research and education network, around 1/4 million users now have native SCION connectivity
- Native SCION applications emerging
  - Possibility to use SCION after app update
- How to better integrate SCION with endpoints?

- More information:
  - https://sciera.readthedocs.io/
  - https://cloud.inf.ethz.ch/s/NRi3Za6pEd8Wyfy



Thank you for your attention!

Questions?

tony.john@ovgu.de, hausheer@ovgu.de
https://www.netsys.ovgu.de

Networks and Distributed Systems Lab (NetSys)

SCION™