Internet Testbed der nächsten Generation – SCIONLab jetzt mit DFN-GVS

SCION (Scalability, Control and Isolation on Next-Generation-Networks) ist eine neue, sichere Internetarchitektur, die eine hohe Verfügbarkeit selbst im Falle von möglichen Angriffen verspricht. Der Ansatz gewährleistet Transparenz über die Wahl der Pfade und erlaubt Multipath-Routing über mehrere Netzwerkdomänen hinweg. Dank dem globalen Forschungsnetzwerk SCIONLab werden innovative Forschungsexperimente an pfadbewussten Netzen und Inter-Domain-Multipath-Kommunikation nun erstmals in einem globalen Testbed ermöglicht. Auch der DFN-Verein betreibt im Rahmen der DFN-GVS-Testbed-Infrastruktur (General-Virtualization-Service) einen SCIONLab-Knoten und ermöglicht es damit seinen Benutzern, Hosts auf der DFN-GVS-Plattform direkt mit dem globalen SCIONLab-Netzwerk zu verbinden.

Text: **David Hausheer** (OVGU Magdeburg und ETH Zürich)

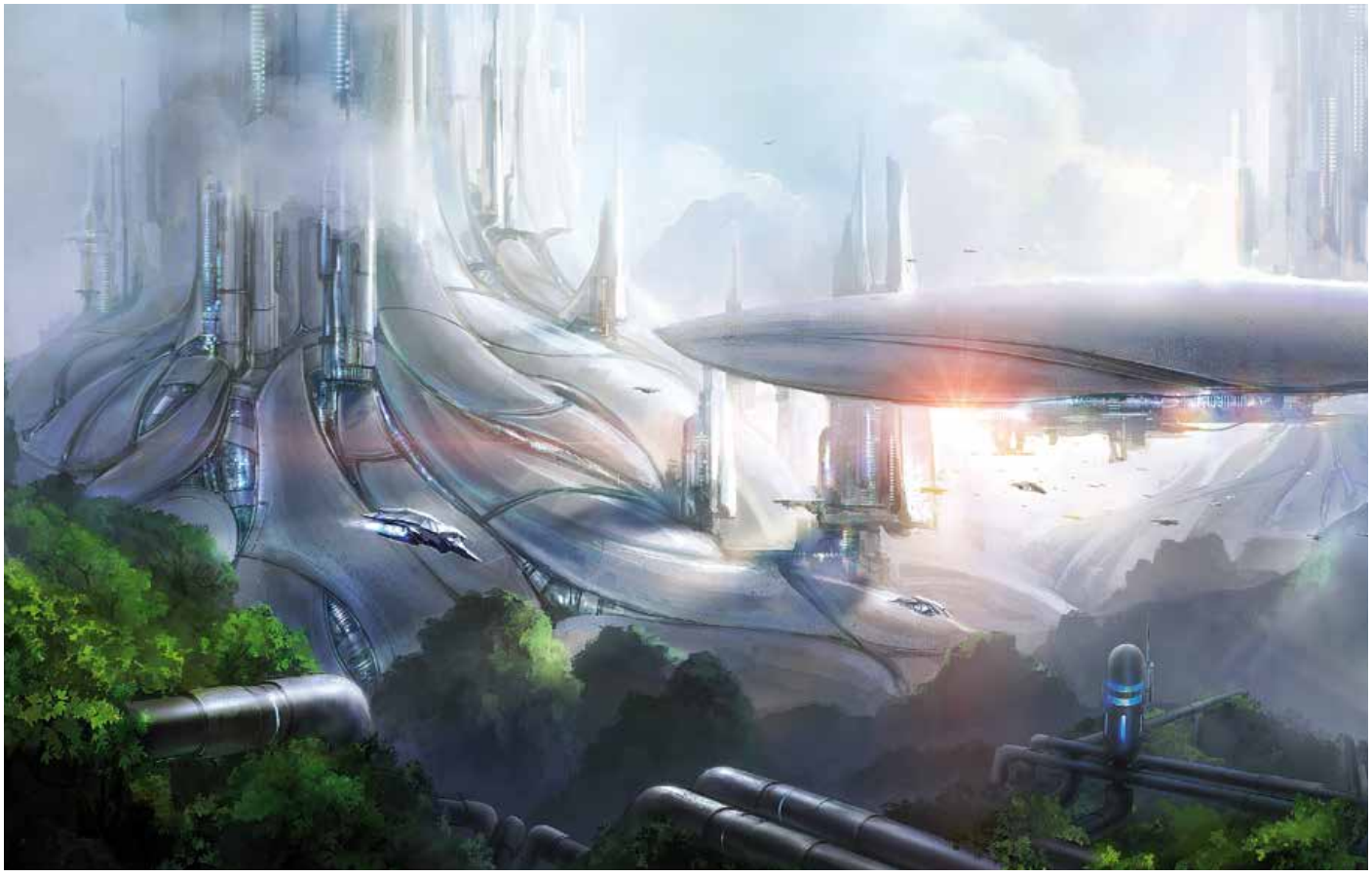

Illustration: liuzishan / Adobe Stock

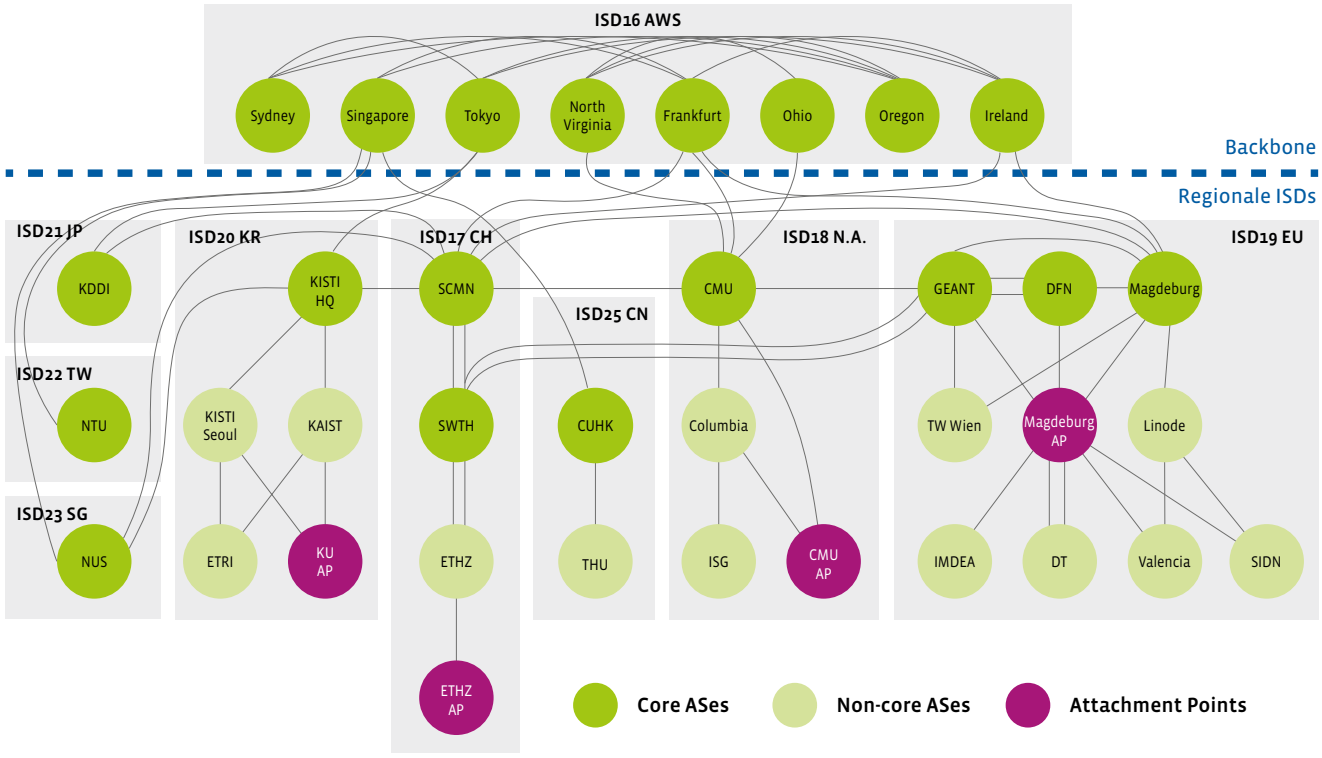

Abbildung 1: Die globale SCIONLab-Topologie

Netzwerk-Testbeds sind entscheidend für den wissenschaftlichen Fortschritt der Netzwerkforschung, durch sie ist es möglich, innovative Konzepte im Netzwerkbereich experimentell zu untersuchen. Die meisten verfügbaren Testbeds fokussieren allerdings hauptsächlich Experimente mit dem heutigen Internet. Mit dem Aufkommen neuer Netzwerkparadigmen und künftiger Internetarchitekturen bietet sich die Gelegenheit, die nächste Welle von Netzwerkanwendungen auszulösen. Insbesondere pfadbewusste Netze, Multipath-Kommunikation und netzwerkgestützte Sicherheitsmechanismen haben das Potenzial, die nächste Generation von Anwendungen voranzutreiben.

Mehr Transparenz durch pfadbewusste Netze

Pfadbewusste Netze ermöglichen es Endgeräten, Informationen über die zum Ziel führenden Netzwerkpfade vorzuhalten. So können sie den gewünschten Pfad aus einer Reihe von Pfaden, die das Netzwerk anbietet, auswählen. Diese Pfadauswahl stellt Anwendungen und Diensten spannende Eigenschaften wie die Pfadtransparenz, feingranulare Pfadkontrolle, schnelles Failover oder Routenoptimierung zu alternativen Pfaden sowie Geo-Fencing bereit. Diese Eigenschaften ermöglichen die Entwicklung neuer Transportprotokolle und fortgeschrittener Anwendungsfunktionen. Pfadbewusste Netze ermöglichen auch Multipath-Kommunikation: Falls das Endgerät mehrere Pfade vom Netzwerk erhält, kann es die Pfade paketweise auswählen. Die Multipath-Kommunikation erlaubt eine höhere Bandbreite oder niedrigere Latenz, eine verbesserte Zuverlässigkeit und eine effizientere Nutzung.

Fortgeschrittene Sicherheitsfunktionen, die in vielen pfadbewussten Netzwerkarchitekturen mit eingebaut sind, ermöglichen die Entwicklung neuer Anwendungen und Dienste. Diesen stellt das Netzwerk integrierte Mechanismen zur Vertrauensbildung und Schlüsselverteilung sowie die Abwehr von DDoS-Angriffen (Distributed Denial-of-Service) und Techniken zur Verbesserung der Privatsphäre bereit.

Um das volle Potenzial all dieser Möglichkeiten auszuschöpfen, müssen jedoch zuerst noch viele offene Forschungsfragen beantwortet werden: Welche Pfade und welche zusätzlichen Informationen sollen den Endgeräten angeboten werden? Wie soll die API-Schnittstelle zwischen Netzwerk-, Transport- und Anwendungsschicht aussehen? Wie arbeiten die verschiedenen Schichten zusammen, um die besten Pfade mit begrenztem Overhead auszuwählen? Welche Staukontrollalgorithmen sind geeignet, wenn Endgeräte die Pfade wechseln oder mehrere Pfade gleichzeitig benutzen?

Ein Testbed für innovative Netzwerkexperimente

SCIONLab ist ein globales Netzwerk-Testbed, das es Forschern ermöglicht, pfadbewusste Netzwerkarchitekturen zu erforschen und sie bei der Beantwortung dieser Fragen zu unterstützen. Basierend auf einer gut vernetzten Netzwerktopologie, die aus global verteilten Knoten besteht, ermöglicht SCIONLab innovative Netzwerkexperimente u. a. im Bereich Multipath-Kommunikation zwischen Domänen, pfadbewussten Netzen und Anwendungen sowie die Erforschung neuer Routing-Policies und neuer Ansätze zur DDoS-Abwehr.

Hinter dem SCIONLab-Ansatz verbirgt sich ein neuartiges Design für ein flexibles, skalierbares, erweiterbares und intuitives Testbed. Es basiert auf der SCION-Internetarchitektur und erbt damit deren Eigenschaften in Bezug auf Skalierbarkeit, Sicherheit und Effizienz. So verbessert SCION die Sicherheit auf verschiedenen Ebenen, z. B. durch Schutz vor bösartigen autonomen Systemen (AS) sowie durch Transparenz und Kontrolle über Pfade und Trustroots. Das Testbed ist seit 2016 in Betrieb und hat bereits verschiedene Forschungsprojekte unterstützt.

Die derzeitige Netzwerkinfrastruktur von SCIONLab (Abbildung 1) basiert auf 36 global verteilten AS. Jeder Knoten stellt dabei ein SCION-AS und jede Kante eine Netzwerkverbindung dar. SCION organisiert autonome Systeme in Isolationsdomänen (ISD), die untereinander verbunden sind, um globale Konnektivität zu gewährleisten. Eine ISD wird von einer Menge von AS (dem sogenannten ISD-Core) verwaltet, welche die Trustroots der ISD definieren, die Zertifikate für die AS in der ISD ausstellen und für die Konnektivität zwischen den ISD sorgen. Das DFN-SCION-AS ist eines dieser Core-AS für die Isolationsdomäne „EU“ im globalen SCIONLab-Netzwerk.

Benutzerzugang mit minimalem Aufwand

An der SCIONLab-Basisinfrastruktur hängen derzeit über 600 weitere sogenannte Benutzer AS, die sich über einen der Attachment Points verbunden haben, um am SCIONLab-Netzwerk teilzunehmen. Benutzer-AS sind vollwertige autonome Systeme, die von den Benutzern mit wenigen Mausklicks in kurzer Zeit erstellt werden können, um einen direkten, ungehinderten Zugang zum Inter-Domain-Routingsystem von SCION zu erhalten. Der zentrale Koordinierungsdienst, der SCIONLab-Koordinator, orchestriert die Infrastruktur und die Benutzer-AS, um eine nahtlose Vernetzung mit einer Vielzahl von Netzwerktopologien und Benutzerumgebungen zu unterstützen.

Um globale Konnektivität in SCIONLab zu erreichen, basieren die meisten Links derzeit auf einem IP-Overlay, welcher die Border Router zwischen benachbarten AS verbindet. Knoten, die hinter einem NAT-Gerät (Network-Address-Translation-Gerät) mit einer festen IP-Adresse liegen, können ebenfalls direkt verbunden werden, sofern der UDP-Zielport 50000 intern an den SCION-Border-Router weitergeleitet wird. Die Verbindung von Knoten mit dynamischen IP-Adressen wird über eine OpenVPN-Verbindung gewährleistet.

Illustration: NicoElNino/Adobe Stock

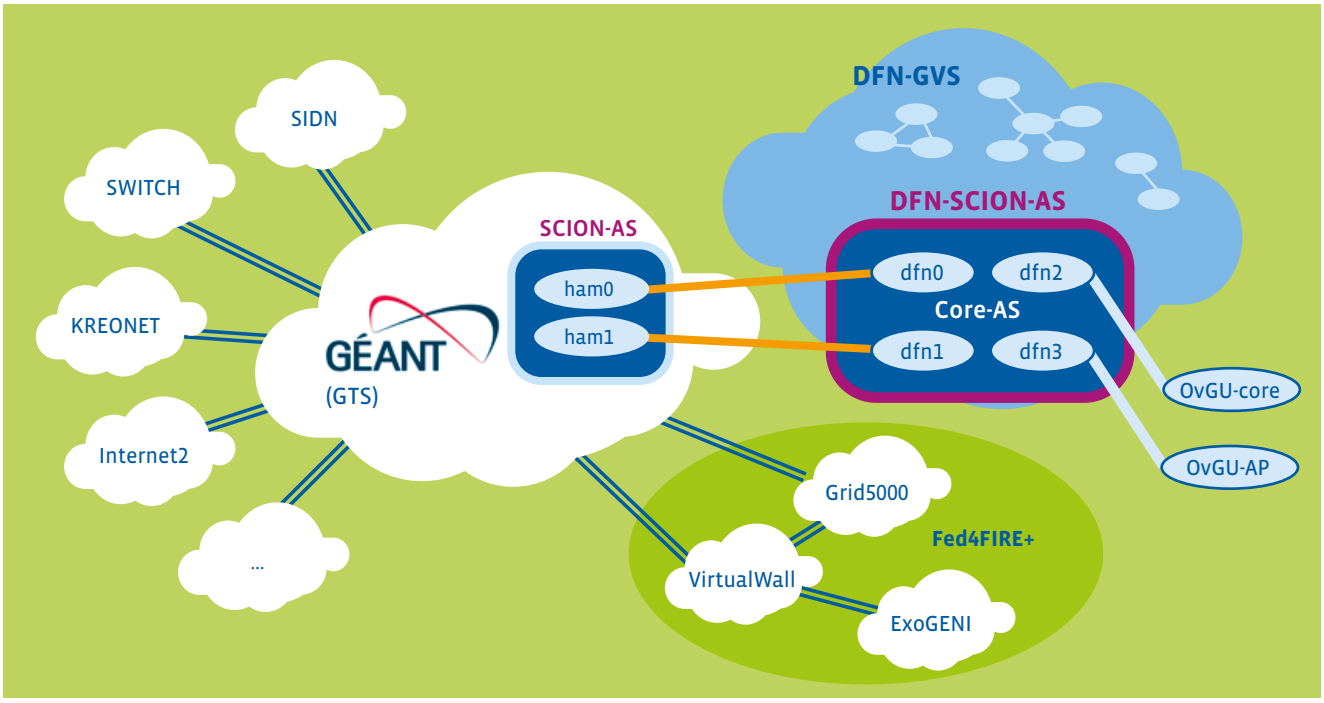

Abbildung 2: Übersicht DFN-GVS und DFN-SCION-AS

Jedes SCION-AS besteht aus einem Beacon-Service (BS), einem Zertifikatsdienst (Certificate Service-CS) und einem Pfaddienst (Path-Service-PS) sowie einem oder mehreren Border-Routern. Für Benutzer, die keine AS-Dienste betreiben wollen, wird auch die alleinige Installation eines SCION-Endgerätes unterstützt. Durch die Konfiguration des SCION-daemon (sciond) kann sich das Endgerät in ein bestehendes AS einklinken und mit den AS-Diensten kommunizieren, um Pfade und Zertifikatsinformationen zu erhalten.

Auf einem Endgerät kann eine Anwendung, die einen SCION-UDP- oder QUIC-Socket öffnet, die Auswahl eines Pfades aus einer Reihe von Pfaden treffen, die vom Netzwerk angeboten werden. Jeder SCION-Paket-Header enthält die Pfad-Informationen auf AS-Ebene. SCION-Border-Router leiten daher Pakete einfach an den nächsten Hop weiter, ohne dass eine Inter-Domain-Routingtabelle nachgeschlagen werden muss. Folglich können unterschiedliche Pfade mit einer feinen Granularität (pro Paket) eingesetzt werden.

AS-Ausführung auf heterogenen Systemen

Der SCIONLab-Koordinator (https://www.scionlab.org/) unterstützt derzeit verschiedene Möglichkeiten, um ein SCION-AS automatisiert aufzusetzen. Der einfachste Weg, um ein SCION-AS zu betreiben, ist innerhalb einer Virtuellen Maschine (VM). Dazu wird eine VM-Konfiguration vom Koordinator heruntergeladen, auf deren Grundlage ein vollwertiges SCIONLab-AS in einer Ubuntu-18.04-basierten VM mittels Virtualbox und Vagrant vollautomatisch installiert wird.

Alternativ können Benutzer die Installation eines SCIONLab-AS auf einem dedizierten Host einfach über vorkompilierte Softwarepakete vornehmen. Diese enthalten auch Anweisungen zur Konfiguration des AS. Derzeit unterstützt SCIONLab nur Debian-style-Pakete. Diese können auf einer Vielzahl von Linux-Systemen wie u. a. Debian oder Ubuntu installiert werden.

Für den speziellen Fall, dass der Benutzer die SCION-Dienste aus dem Quellcode kompilieren möchte, kann der Koordinator eine Konfiguration zurückgeben, die lediglich aus der Konfiguration der Dienste und einer Reihe von Supervisord-Dateien zum Starten und Stoppen der Dienste besteht.

Schließlich ist es auch möglich, SCION auf einem Android-Gerät zu installieren. Konkret ermöglicht es die SCION-App ein vollständiges SCIONLab-AS auf einem Android-Smartphone zu betreiben. Die Einrichtung des AS erfolgt in vollständig automatisierter Weise auf der Grundlage der AS-Konfiguration des Koordinators.

DFN-GVS stellt SCION-Core-AS zur Verfügung

Das DFN-SCION-AS ist physisch über mehrere Hosts auf der Infrastruktur des DFN-Pilotservice „General-Virtualization-

Service (GVS)“ im Regionalen Rechenzentrum Erlangen (RRZE) der Universität Erlangen-Nürnberg verteilt. Zwei dieser Hosts sind als SCION-Border-Router nativ über zwei dedizierte L2VLANs mit dem GÉANT Testbed Service (GTS) verbunden, in welchem wiederum das GÉANT-SCION-AS aufgesetzt ist. Gleichzeitig bietet das DFN-SCION-AS eine öffentliche IPv4-Schnittstelle, über welche beispielsweise das Core-AS und der Attachment Point an der OVGU Magdeburg verbunden sind. In Zukunft wird angestrebt, diese Verbindungen ebenfalls durch L2VLANs zu ersetzen und damit komplett BGP-frei (das heißt: unabhängig von BGP) zu gestalten.

Der DFN-GVS-Dienst ermöglicht es Nutzern, virtuelle Netze mit wenigen Mausklicks über ein Webportal selbst zu erzeugen. Der Ansatz basiert auf echtem Network Slicing der Hardware und eignet sich damit im Besonderen für Netzwerk-Forschungsexperimente wie SCION. Interessierte Forschungsgruppen können auf der DFN-GVS-Webseite (https://dfn-gvs.de/) einen Account beantragen, um damit Testbeds bestehend aus einem oder mehreren Hosts zu erstellen und diese untereinander zu verbinden. Jedes Projekt bekommt zudem ein Internet Access Gateway zugeteilt und 3GB+ Speicher zur freien Verfügung. Auch OpenFlow-Switches können für SDN-Tests einem Projekt zugeteilt werden. Internationale DFN-GVS-Netze können z. B. über Hamburg mit GÉANT-GTS erweitert werden.

Um Forschungsexperimente über SCIONLab durchzuführen, müssen die Hosts als ein (oder mehrere) SCION-AS konfiguriert werden. Dazu können sich Forscher auf der Webseite des SCIONLab-Koordinators registrieren und darüber SCION-Benutzer-AS erstellen und diese mit beliebigen SCIONLab Attachment Points verbinden. Auch im DFN-AS ist es geplant, einen entsprechenden Attachment Point anzubieten. Die erstellten SCION-AS-Konfigurationen können dann genutzt werden, um die Hosts im DFN-GVS-Testbed aufzusetzen und mit SCIONLab zu verbinden. Dank der lokalen Netzwerkanbindung können somit Experimente mit Bandbreiten im Gigabit-Bereich über das globale SCIONLab Testbed durchgeführt werden. Mittelfristig sollen sogar 10G-SCION-Verbindungen über das DFN-GVS ermöglicht werden.

Anbindung weiterer Testbeds

Im Rahmen eines „Fed4FIRE+“-Projektes, das innerhalb des EU-Programms Horizont 2020 gefördert wird, werden SCIONLab-AS derzeit auf weiteren Testbeds aufgesetzt. Dazu gehören VirtualWall, Grid5000 und ExoGeni. Während die ersten beiden Testbeds durch L2VLANs über GÉANT mit SCIONLab verbunden sind, läuft die Verbindung mit ExoGeni über das Internet2-Netz, das größte und schnellste Forschungs- und Bildungsnetz der USA, das über 300 Universitäten und Regierungsbehörden von Küste zu Küste versorgt. SCIONLab ermöglicht es, diese ansonsten voneinander weitgehend isolierten Testbeds über SCION mittels Inter-Domain-Multipath-Kommunikation zuverlässig miteinander zu verbinden und damit Testbed-übergreifende Forschungsexperimente durchzuführen, die insbesondere auch das DFN-GVS-Testbed mit einschließen können. Der SCION IP Gateway (SIG) ermöglicht es zudem, dass auch nicht-SCION-fähige Anwendungen über das SCIONLab-Netzwerk kommunizieren können.

Fazit

SCIONLab ist ein globales Testbed zur Erforschung und Entwicklung von Inter-Domain-Kommunikationsmechanismen der nächsten Generation. Es ermöglicht die Erstellung von eigenen, vollwertigen SCION-AS, die am globalen Inter-Domain-Routing teilnehmen können. Das SCIONLab Testbed bietet eine neuartige Infrastruktur, um innovative Forschungsarbeiten, z. B. an pfadbewussten und Multipath-fähigen Transportprotokollen, an globaler Schlüsselvereinbarung zur sicheren Kommunikation auf der Grundlage von Zertifikaten auf AS-Ebene, an Routing-Policies der nächsten Generation, an Traffic Engineering und an DDoS-Abwehrmechanismen zu unterstützen. Durch die Anbindung des DFN an das globale SCIONLab-Netzwerk über dedizierte L2VLANs kann das DFN-GVS-Testbed als Infrastruktur für Forschungsexperimente mit Bandbreiten im Gigabit-Bereich über SCION eingesetzt werden. ◆

WEITERFÜHRENDE LINKS

- SCION Internet Architektur: **https://www.scion-architecture.net/**
- SCIONLab Koordinator: **https://www.scionlab.org/**
- SCION Android App: **https://play.google.com/store/apps/details?id=org.scionlab.scion**
- SCIONLab Tutorial: **https://docs.scionlab.org/**
- General-Virtualization-Service des DFN: **https://dfn-gvs.de**