Our research in a nutshell

Synthesis

Network synthesis is the task of finding network inputs (routing announcements or router configurations) whose induced forwarding state satisfies a given formal specification. Our contribution to the area is particularly wide-ranging and "full of firsts", including: the first synthesizer of routing inputs (Fibbing); the first configuration synthesizer supporting multiple distributed routing protocols (SyNET) and autocompletion of partial configurations (NetComplete); the first synthesizer of safe configuration updates (Snowcap); or the first synthesizer of formal specifications (Config2Spec).

SIGCOMM'21
NSDI'20a
NSDI'18a
CAV'17
SIGCOMM'15
HotNets'14
SIGCOMM'11

Verification

Network verification is the task of proving the compliance of a network with a given specification. As for synthesis, our contribution to the area is wide-ranging, including: the first analyzer capable of catching problematic bugs in network models used in production-grade network verifiers (Metha); the first configuration verifiers supporting probabilistic *and* deterministic properties (NetDice and Bayonet); or the first race detector capable of analyzing production-grade SDN controllers (SDNRacer). We also explored the concept of automated network testing in 2 HOTNETS papers on the topic.

NSDI'21
SIGCOMM'20
PLDI'18
HotNets'17
PLDI'16
HotNets'15

Programmability

Network programmability is a set of software abstractions and tools to read (*sense*) and write (*actuate*) network states. Our group has again taken pioneering steps in developing these building blocks with: programmable monitoring techniques using on-off mirroring (Stroboscope); reasoning techniques that summarize forwarding behaviors (Net2Text); programmable packet scheduling techniques (SP-PIFO); together with SoftCell and the SDX projects which respectively brought programmability to cellular and wide-area networks.

NSDI'20b
HotNets'20a
HotNets'20b
NSDI'18b
NSDI'18c
NSDI'16
HotNets'16
SIGCOMM'14
CoNEXT'13

Security

When it comes to network security, our goal is to protect infrastructures from attackers and uncover unknown attacks. Our key contributions include techniques to prevent network analyses by obfuscating network information in real-time (NetHide, ditto). We are also known for shedding lights on the impact of routing attacks on anonymity networks and cryptocurrencies, and how one can protect from them (Sabre).

NDSS'22
NDSS'20
USENIX Sec'18
IEEE S&P'17
USENIX Sec'15

Internet routing

An ideal Internet routing system scales and converges fast. Our contributions aim at making these a reality. To speed up convergence, we leveraged data-plane programmability (Blink) and predictions (Swift). To improve scalability, we developed highly efficient distributed aggregation techniques (Dragon).

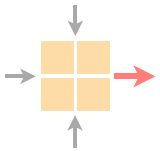
NSDI'19
SIGCOMM'17
CoNEXT'14

Our research in a nutshell

Fri 7 Jan 2022

Prof. Laurent Vanbever

https://nsg.ee.ethz.ch



Networked Systems

ETH Zürich — seit 2015