2022 IEEE 35th Computer Security Foundations Symposium (CSF)

N-Tube: Formally Verified Secure Bandwidth Reservation in Path-Aware Internet Architectures

Thilo Weghorn* Swisscom thilo.weghorn@swisscom.com
Si Liu* ETH Zurich si.liu@inf.ethz.ch
Christoph Sprenger ETH Zurich sprenger@inf.ethz.ch
Adrian Perrig ETH Zurich adrian.perrig@inf.ethz.ch
David Basin ETH Zurich basin@inf.ethz.ch

***Abstract*—We present N-Tube, a novel, provably secure, inter-domain bandwidth reservation algorithm that runs on a network architecture supporting path-based forwarding. N-Tube reserves global end-to-end bandwidth along network paths in a distributed, *neighbor-based*, and *tube-fair* way. It guarantees that benign bandwidth demands are granted *available* allocations that are *immutable*, *stable*, *lower-bounded*, and *fair*, even during adversarial demand bursts.**

We formalize N-Tube and powerful adversaries as a labeled transition system, and inductively prove its safety and security properties. We also apply statistical model checking to validate our proofs and perform an additional quantitative assessment of N-Tube, providing strong guarantees for protection against DDoS attacks. We are not aware of any other complex networked system designs that have been subjected to a comparable analysis of both their qualitative properties (such as correctness and security) *and* their quantitative properties (such as performance).

I. Introduction

Providing useful guarantees during DDoS attacks remains *in malicious contexts such that legitimate hosts obtain useful bandwidth guarantees.*

A core challenge is that current link-flooding attacks can be caused by a huge number of low-volume flows originating from colluding legitimate-looking bots, e.g., as seen in the Hidden Cobra DDoS Botnet Infrastructure [8]. Therefore, standard fairness notions that QoS solutions try to achieve, such as per source [9], per destination [10], per flow [11], per computation [12], and per class [13], are insufficient in such settings and result in unfair bandwidth allocations. These fairness notions suffer from the "tragedy of the commons" [14], whereby the incentive of rational agents to increase their share of a commonly available resource leads to infinitesimally small shares for less aggressive, honest agents. In particular, in today's Internet, congestion-control-based fairness is the most commonly used *per-flow fairness* notion, which allows adversarial agents to request arbitrarily many flows and thereby obtain a disproportional amount of bandwidth compared to