PhD Open Days

StageRun

An Execution-Centric Runtime for In-Network Security Applications

João Veríssimo*, Eduard Marin**, Nuno Santos*

joao.verissimo@tecnico.ulisboa.pt

* IST · INESC-ID, Universidade de Lisboa,
**Telefónica Scientific Research

PhD programme: Computer Science and Engineering

RESEARCH QUESTION — **Can security defenses evolve on a switch without rebuilding its pipeline?**

01 THE PROBLEM: FAST NETWORKS, RIGID DEFENSES

WHAT IS A PROGRAMMABLE SWITCH?

NETWORK PACKETS →



Specialized hardware that applies custom security decisions to packets at very high speed.

WHY IS ADAPTATION DISRUPTIVE?

DDoS defense → PIPELINE RELOAD → Firewall

TRAFFIC PROCESSING INTERRUPTED

Different threats demand different defenses; replacing specialized programs delays response and leaves the switch unable to process traffic.

WHY CAN'T WE REUSE EXECUTION EASILY?

01 MULTI-STEP OPERATIONS
A logical action may span several execution steps.

02 STATE & DEPENDENCIES
Intermediate values and writes must stay consistent.

03 SPECIALIZED HARDWARE
Deparser, queues and packet generation need coordination.

Traditional specialized P4 programs replicate this complexity per defense.

02 STAGERUN: A REUSABLE EXECUTION ENGINE



StageRun — REUSABLE EXECUTION ENGINE

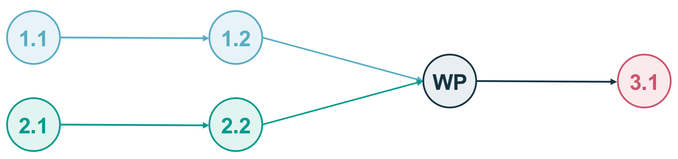
1 BUILD THE STAGERUN APP

NETWORK OPERATOR | ISA + ENGINE INSTALLED ONCE

StageRun program
ISA-level instructions
I1 I2 I3

→ **Compiler**
IEG + data dependencies (DFG)

DFG Expansion Program
Each logical instruction expands into reusable microinstruction calls



2 DEPLOY ON THE SWITCH

CONTROLLER PLACEMENT ALGORITHM

Availability / Ordering / State locality / Write Phases

SWITCH DATA PLANE / INSTALLED EXECUTION ENGINE

Stage 1	Stage 2	Stage 3	Stage 4
1.1	1.2	WP	3.1
2.1	2.2	commit	

INSTALL rules → ACTIVATE / CHANGE program

NO PIPELINE RELOAD · TRAFFIC FORWARDING CONTINUES

03 GENERALITY

14 APPLICATIONS

7 domains / Intel Tofino

Access control (6)
Bedrock / NetCap / P4Control / Poise / PortKnocker / Stateful Firewall

DDoS mitigation (3)
Mew / Poseidon / SmartCookie

Traffic obfuscation (1)
Ditto

Topology obfuscation (1)
NetHide

Stateful monitoring (1)
Cerberus

Covert-channel mitigation (1)
NetWarden

Censorship circumvention (1)
NetShuffle

04 EXPERIMENTAL EVIDENCE: AGILITY AND SECURITY BEHAVIOR

DEPLOY A NEW APPLICATION

8.09 – 9.15 s → **0.316 – 0.562 s**

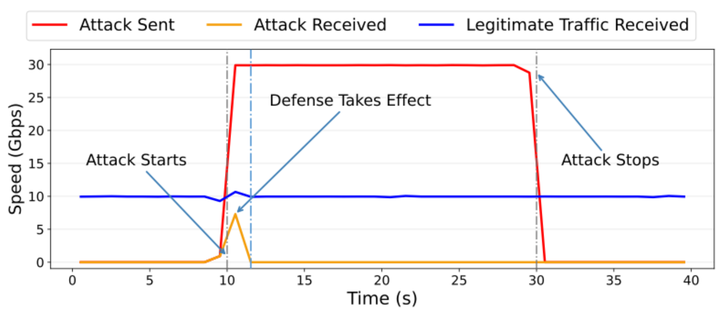
Native P4 — StageRun · 93.7–96.4% reduction

SWITCH BETWEEN INSTALLED APPLICATIONS

< 50 ms — **stateless activation**

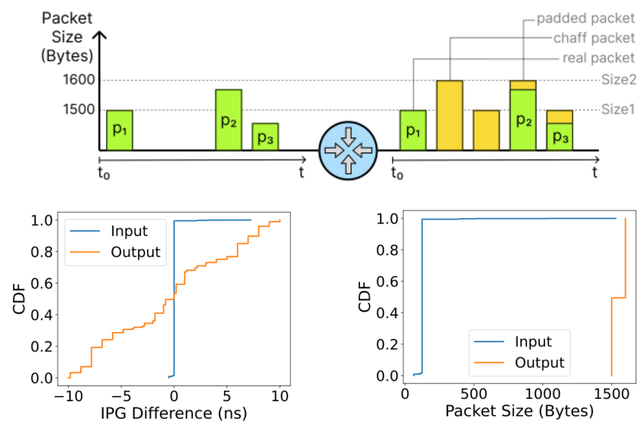
State cleanup or hardware reconfiguration add separate costs.

POSEIDON / HTTP GET FLOOD MITIGATION

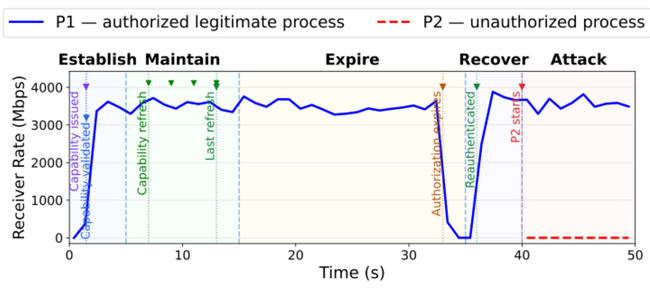


Attack redirected; legitimate traffic stable (paper Fig. 11).

DITTO / TRAFFIC OBFUSCATION



NETCAP / STATEFUL ACCESS CONTROL



KEY TAKEAWAY

StageRun is fast and flexible, which opens the door to a more **reusable** and **responsive** network defenses.

SPONSORS

Work supported by national funds through Fundação para a Ciência e a Tecnologia, I.P. (FCT) under projects UID/50021/2025 (DOI: https://doi.org/10.54499/UID/50021/2025) and UID/PRR/50021/2025 (DOI: https://doi.org/10.54499/UID/PRR/50021/2025) and under grant 2024.02131.BD (DOI: https://doi.org/10.54499/2024.02131.BD).

inesc id lisboa

fct Fundação para a Ciência e a Tecnologia

TÉCNICO UNIVERSIDADE DE LISBOA

phdopendays.tecnico.ulisboa.pt