DoS attack mitigation in SDN networks using a deeply programmable packet-switching node based on a hybrid FPGA/CPU data plane architecture

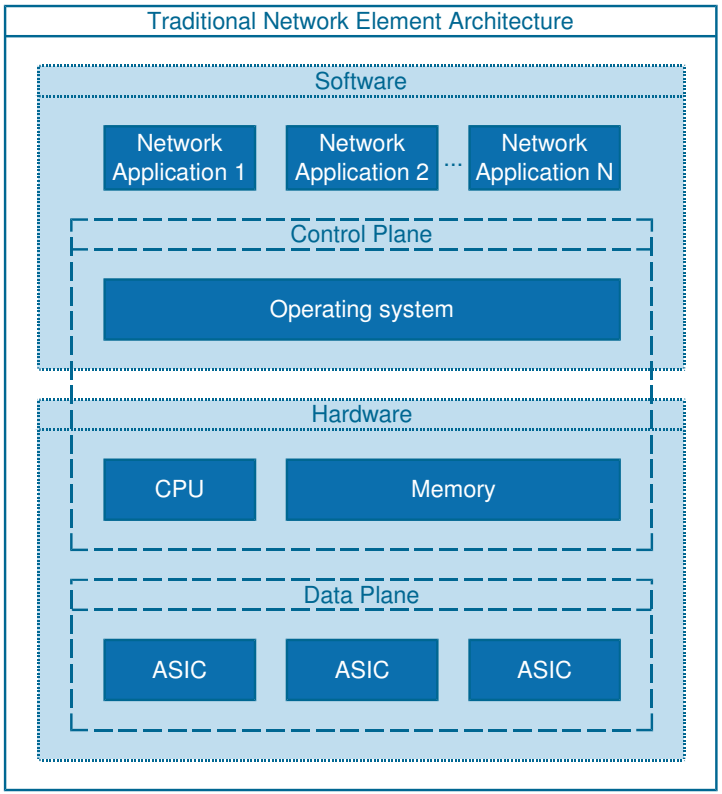
Enio Kaljic
Almir Maric
Pamela Njemcevic

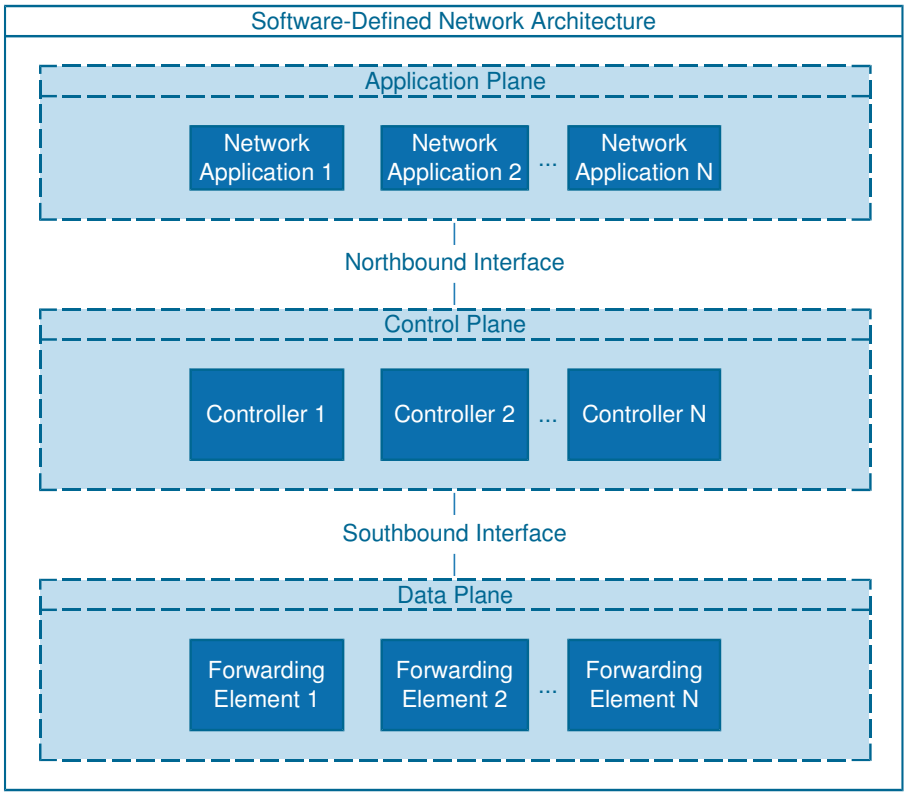
DEPARTMENT OF
TELECOMMUNICATIONS
Faculty of Electrical Engineering
University of Sarajevo

XXVII International Conference on Information, Communication and Automation Technologies (ICAT)
20-23 October 2019, Sarajevo, Bosnia and Herzegovina

Introduction

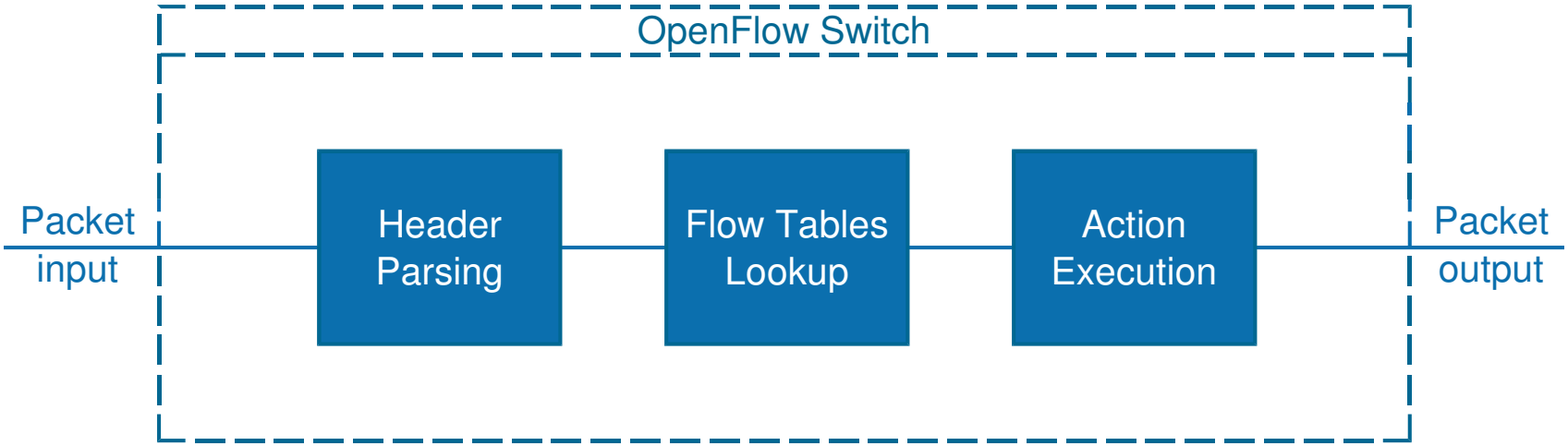
Transition from traditional to SDN architecture





Introduction

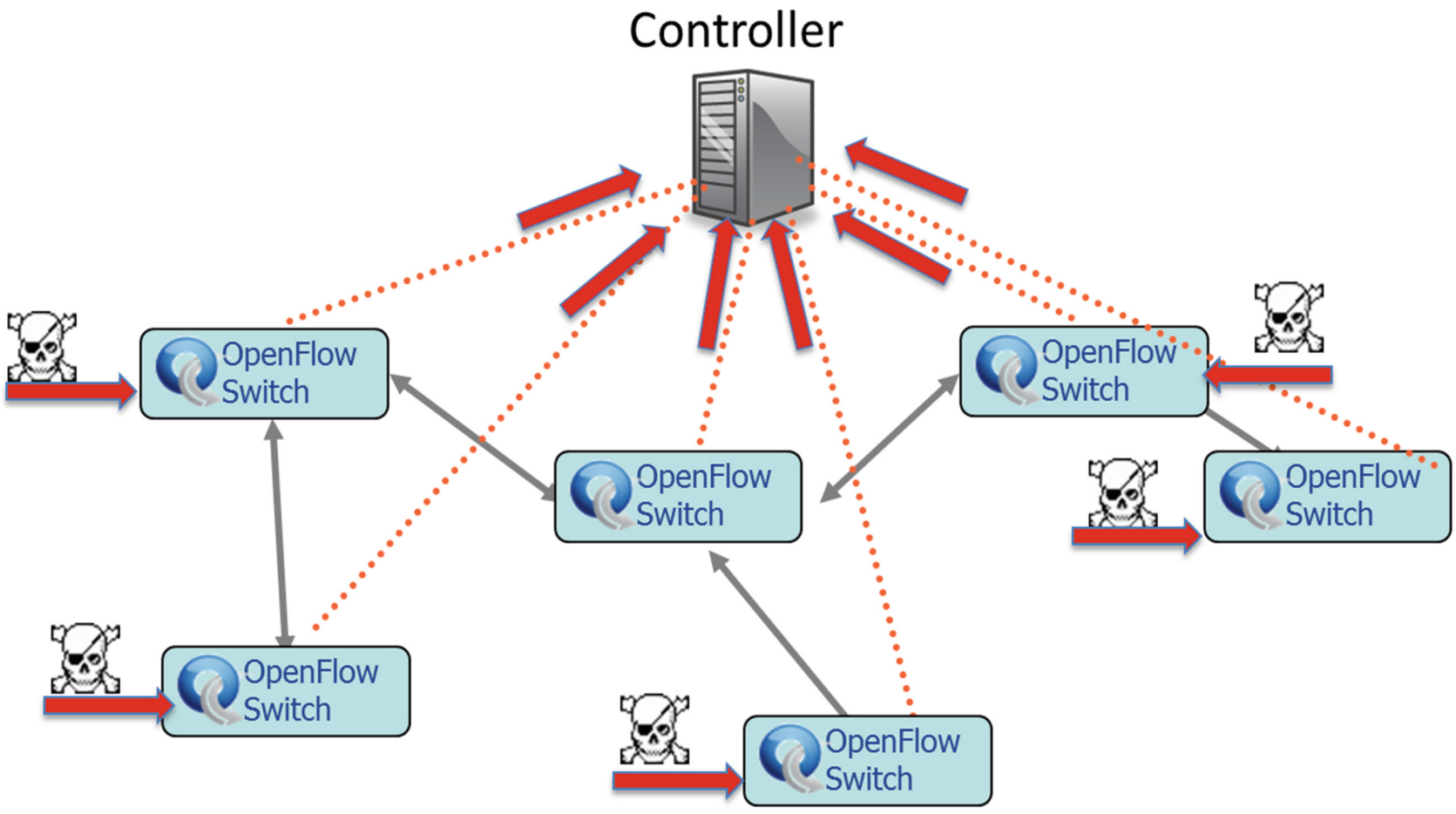
OpenFlow-based SDN – Switch architecture



- Three-stage packet processing
- Flow-level granularity
- Absence of advanced packet processing functionalities (e.g. DPI, DoS attack detection)

Motivation

OpenFlow-based SDN under DoS attack



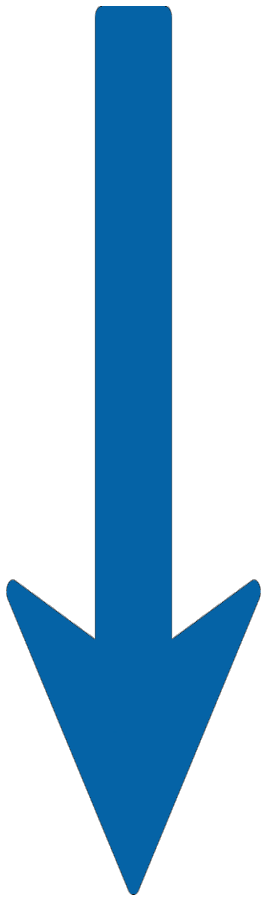
OpenFlow switch-controller communication overhead

Motivation

How can deep network programmability help?

Five levels of data plane programmability:

- Very low – flow table management
- Low – definition of arbitrary packet headers and parsers
- Medium – programming arbitrary actions
- High – management of basic processes after the action is taken (e.g. output queuing)
- Very high – full programmability of all data plane processes

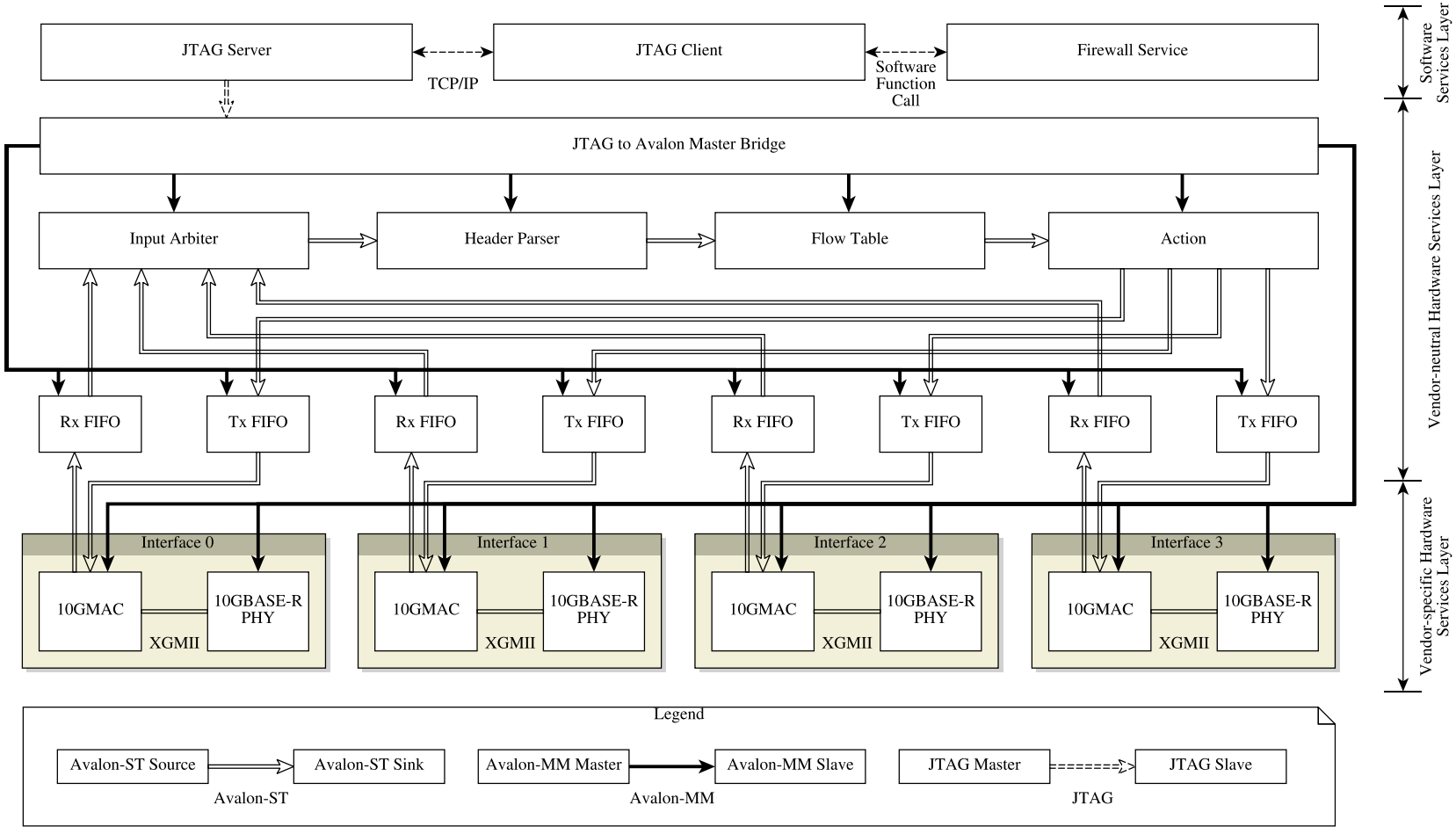


OpenFlow

Deep network programmability

Proposed solution

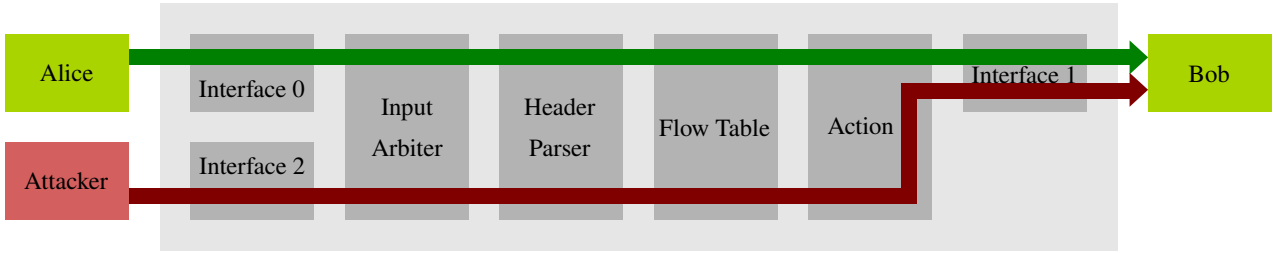
Firewall based on a deeply programmable hybrid FPGA/CPU data plane architecture



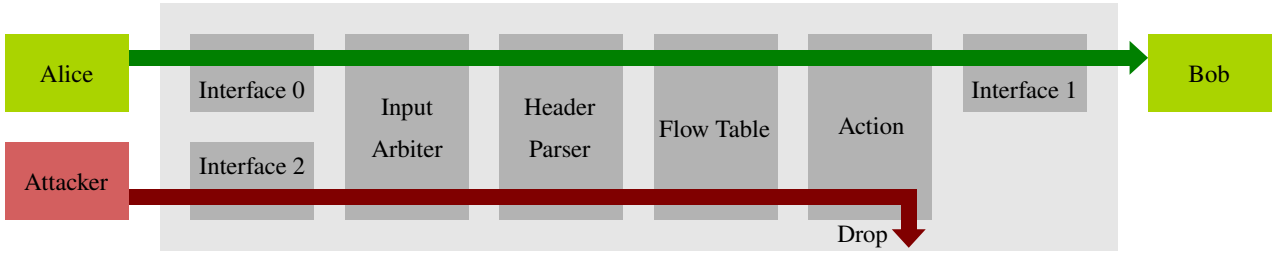
- Hardware Services Layer – FPGA for high-speed processing
- Software Services Layer – CPU for high level of flexibility

Experimental evaluation

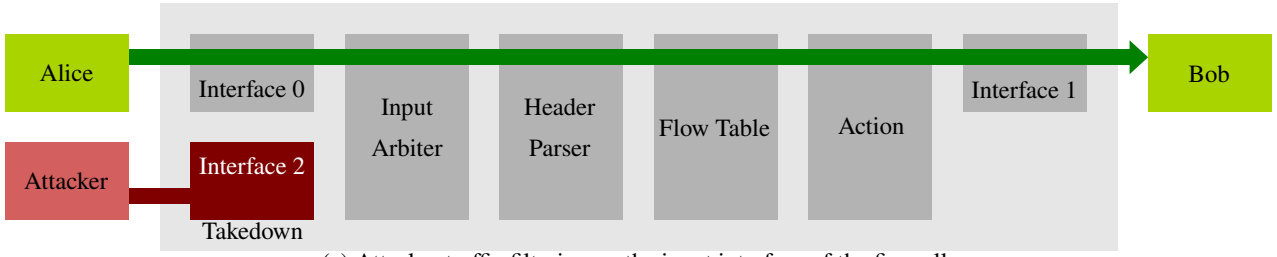
Scenarios



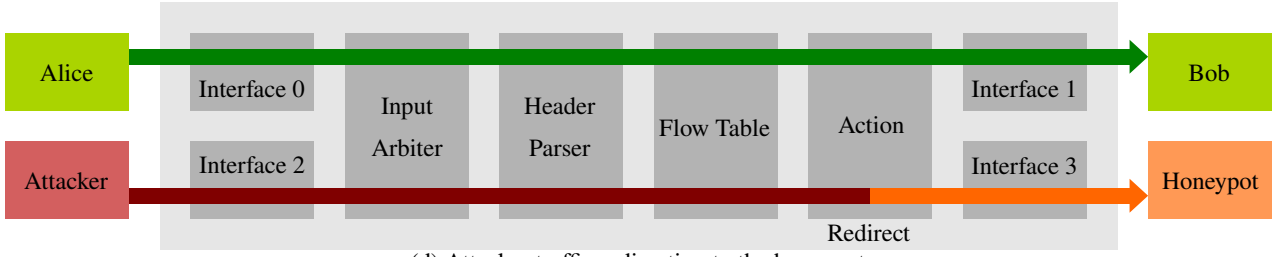
(a) User B under DoS attack



(b) Attacker traffic filtering on the output interface of the firewall



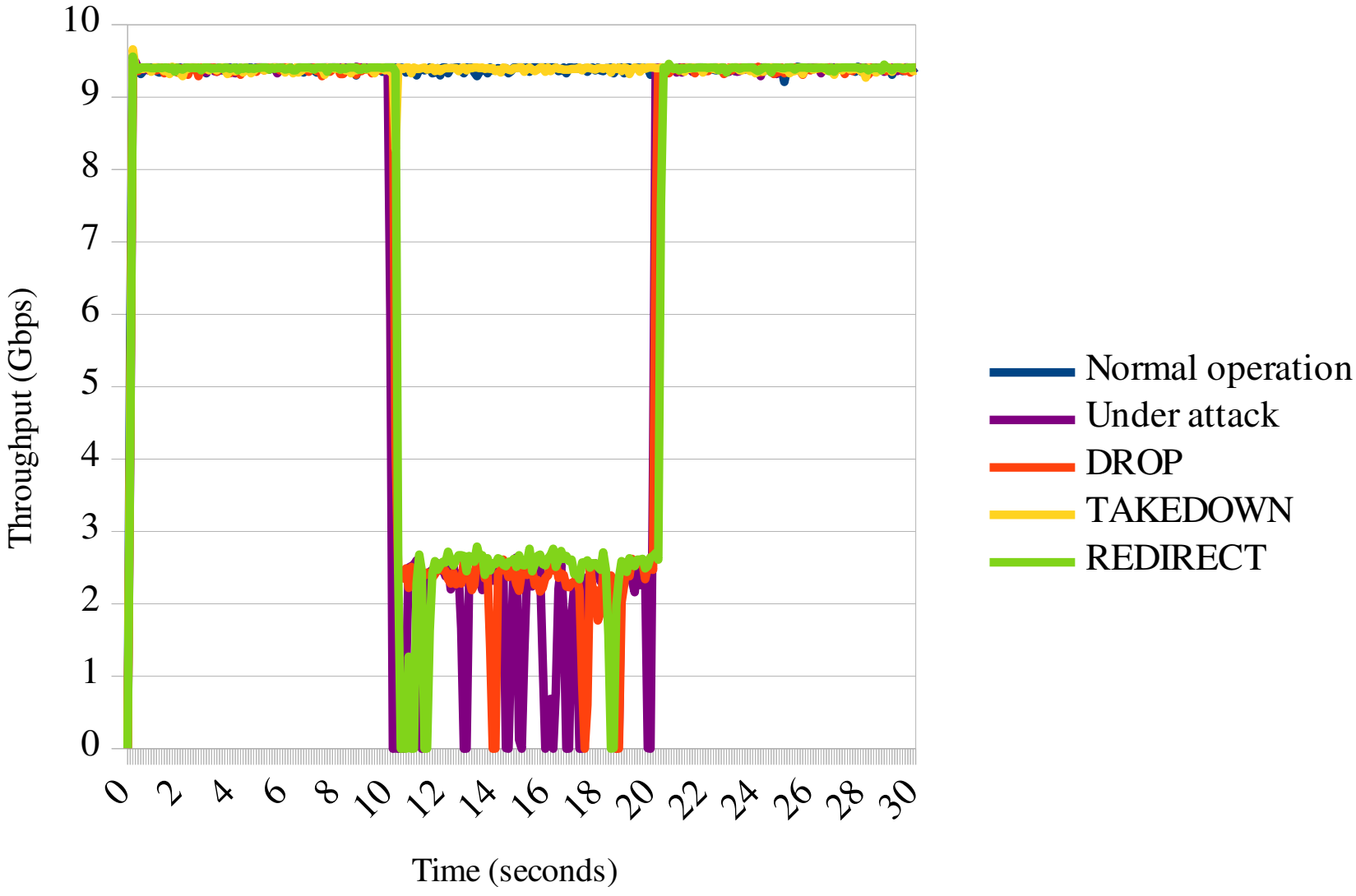
(c) Attacker traffic filtering on the input interface of the firewall



(d) Attacker traffic redirection to the honeypot

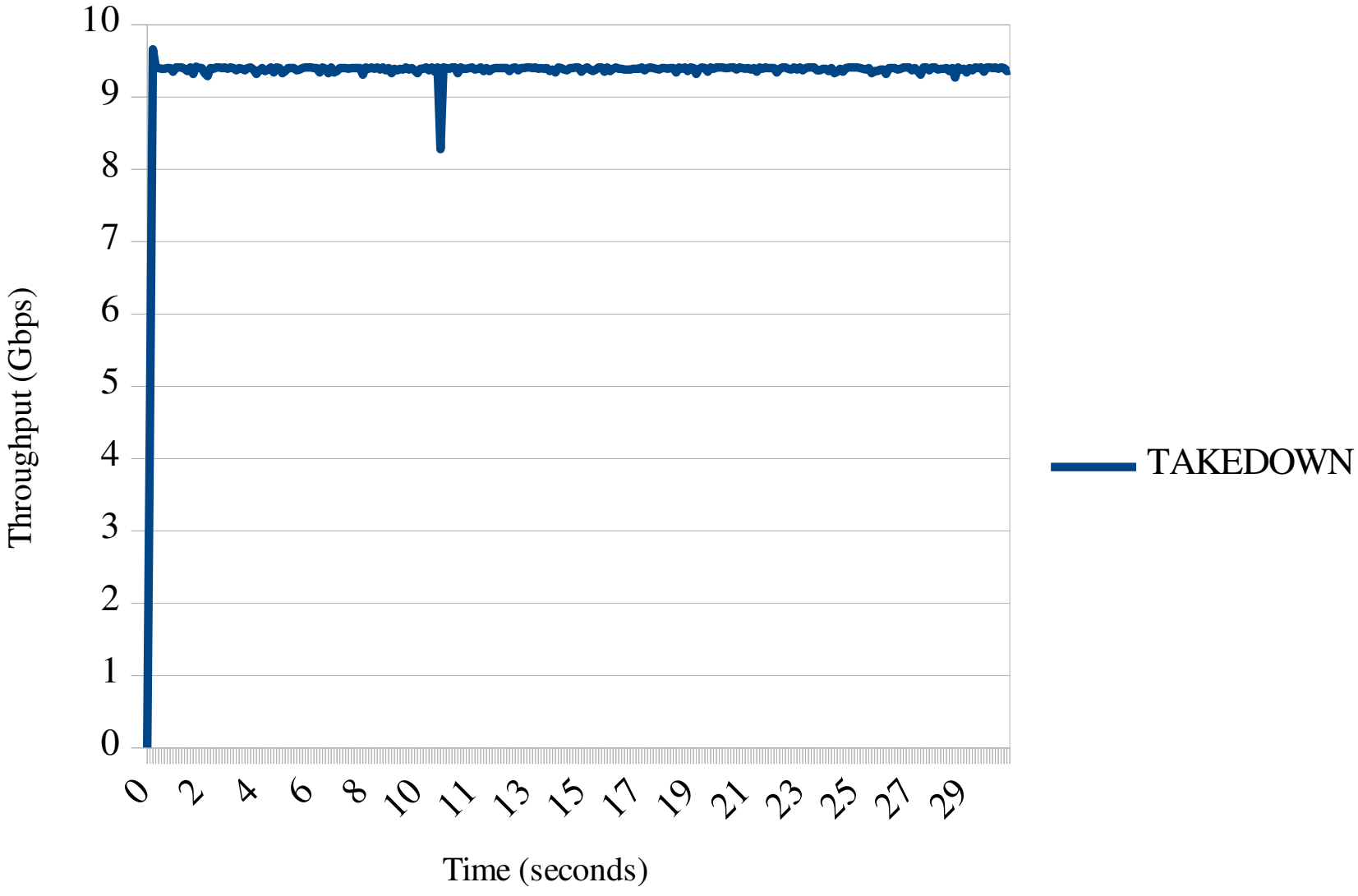
Experimental evaluation

Measurements – Forwarding throughput



Experimental evaluation

Measurements – Forwarding throughput



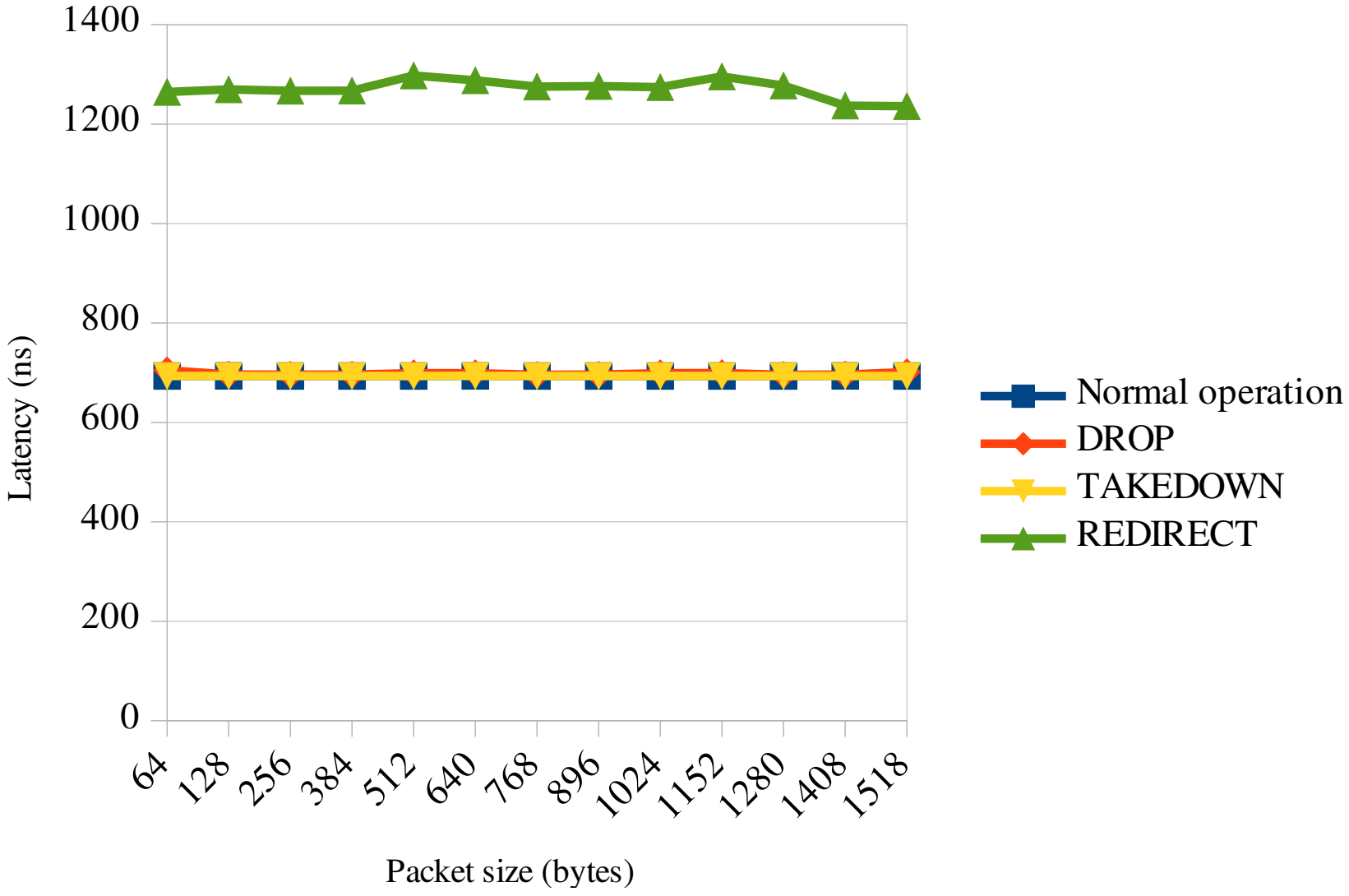
Experimental evaluation

Measurements – Forwarding throughput

Case	Throughput			
	Maximum (Gbps)	***Minimum (Gbps)***	***Average (Gbps)***	***Relative (%)***
Normal operation	9.57	9.31	9.39	100.00
Under attack	9.49	0.00	6.82	72.60
DROP	9.42	0.00	7.01	74.67
TAKEDOWN	9.66	8.28	9.39	99.95
REDIRECT	9.56	0.00	7.02	74.76

Experimental evaluation

Measurements – Forwarding latency



Conclusion

- SDN firewall based on a deeply programmable hybrid FPGA/CPU data plane architecture has been proposed
- Experimental evaluation showed that DoS traffic filtering on the firewall input interface (i.e. TAKEDOWN strategy) is the best strategy
- Negative impacts of DoS attacks in SDN network have been reduced by applying the concept of deep network programmability

DoS attack mitigation in SDN networks using a deeply programmable packet-switching node based on a hybrid FPGA/CPU data plane architecture

Questions?

enio.kaljic@etf.unsa.ba