QUEEN'S
UNIVERSITY
BELFAST

CSIT

CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

The 5 W's of Network Monitoring for SDN-based IDPS

DR. SANDRA SCOTT-HAYWARD, QUEEN'S UNIVERSITY BELFAST

UKNOF, BELFAST, 10 SEPTEMBER 2019

Queen’s University Belfast – Lanyon Building

Est. 1845

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Centre for Secure Information Technologies (CSIT)

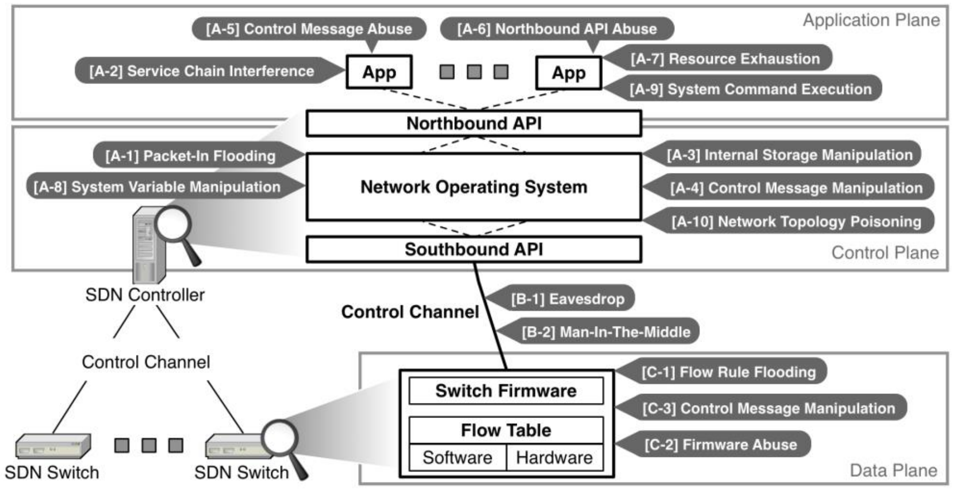
CSIT is the UK’s Innovation and Knowledge Centre for Cybersecurity

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

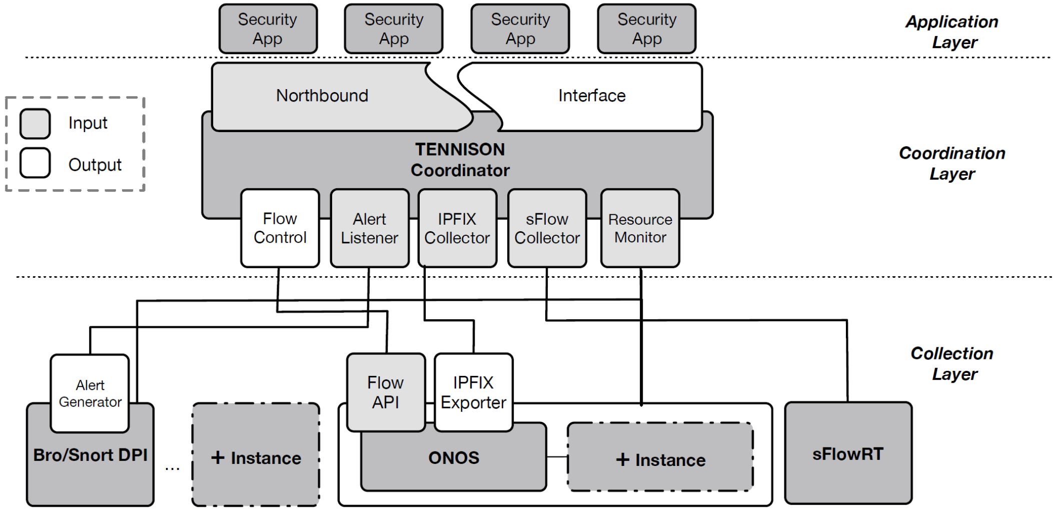
SDN/NFV Security Research - Objectives

Identifying, raising awareness, and recommending solutions to potential vulnerabilities in SDN/NFV network design and deployment.

Exploring scalable, analytics-based monitoring and forensics capabilities, and security solutions for these new network architectures.



Application Plane
[A-5] Control Message Abuse
[A-6] Northbound API Abuse
[A-2] Service Chain Interference
App
App
[A-7] Resource Exhaustion
[A-9] System Command Execution
Northbound API
[A-1] Packet-In Flooding
[A-8] System Variable Manipulation
Network Operating System
[A-3] Internal Storage Manipulation
[A-4] Control Message Manipulation
[A-10] Network Topology Poisoning
Southbound API
Control Plane
SDN Controller
Control Channel
[B-1] Eavesdrop
[B-2] Man-In-The-Middle
Control Channel
Switch Firmware
Flow Table
Software
Hardware
[C-1] Flow Rule Flooding
[C-3] Control Message Manipulation
[C-2] Firmware Abuse
Data Plane
SDN Switch
SDN Switch

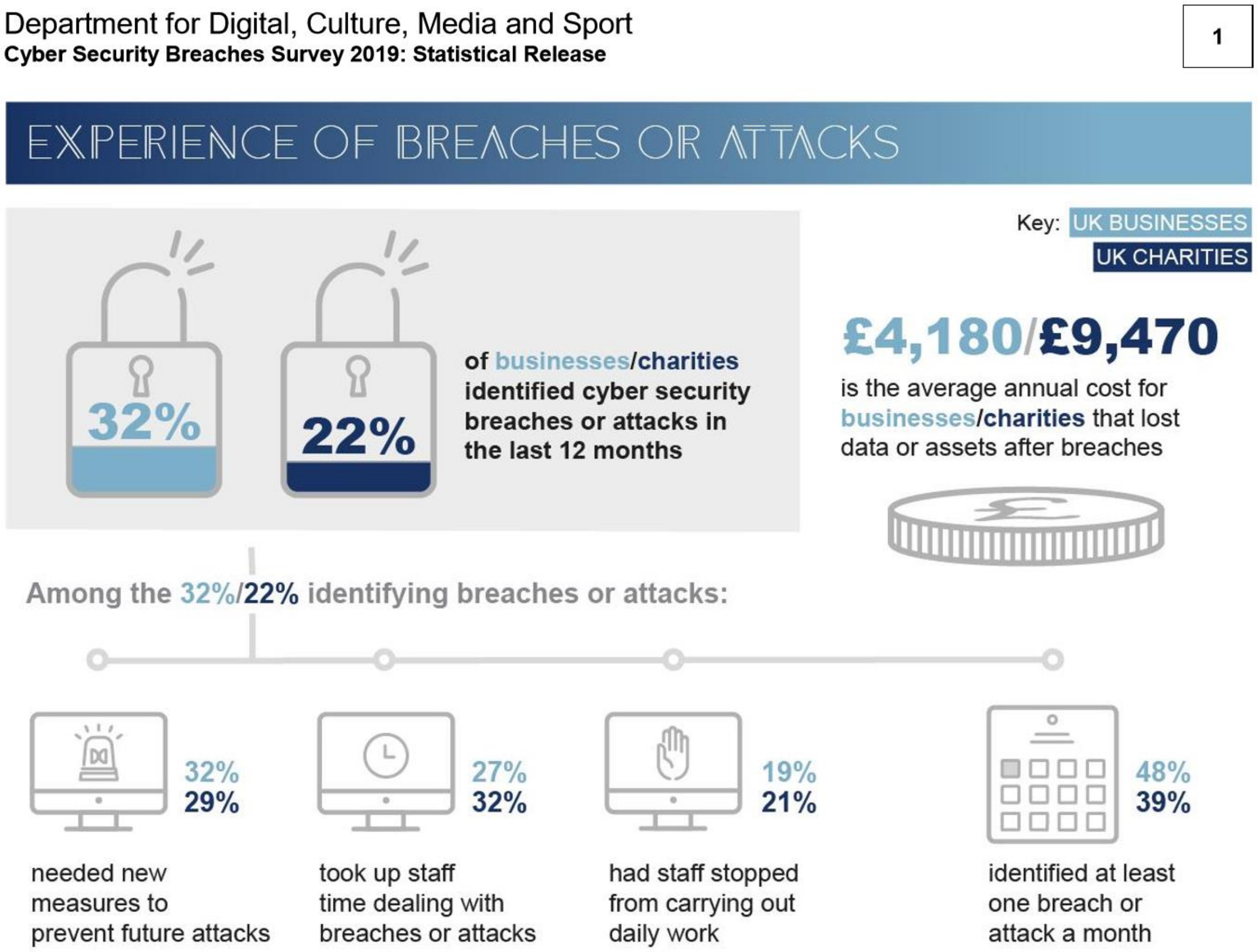


Agenda for the talk

Lessons learned and recommendations for efficient and proportionate network monitoring; the Who, What, When, Where, and Why (5 Ws) of network monitoring for SDN-based intrusion detection and prevention systems.

1. Why are we monitoring?
2. Who are we monitoring?
3. When are we monitoring?
4. Where are we monitoring?
5. What are we monitoring?
6. Recommendations

Why?



Department for Digital, Culture, Media and Sport
Cyber Security Breaches Survey 2019: Statistical Release

1

EXPERIENCE OF BREACHES OR ATTACKS

Key: UK BUSINESSES UK CHARITIES

32% 22% **of businesses/charities identified cyber security breaches or attacks in the last 12 months**

£4,180/£9,470 is the average annual cost for **businesses/charities** that lost data or assets after breaches

Among the 32%/22% identifying breaches or attacks:

32% 29% needed new measures to prevent future attacks

27% 32% took up staff time dealing with breaches or attacks

19% 21% had staff stopped from carrying out daily work

48% 39% identified at least one breach or attack a month

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

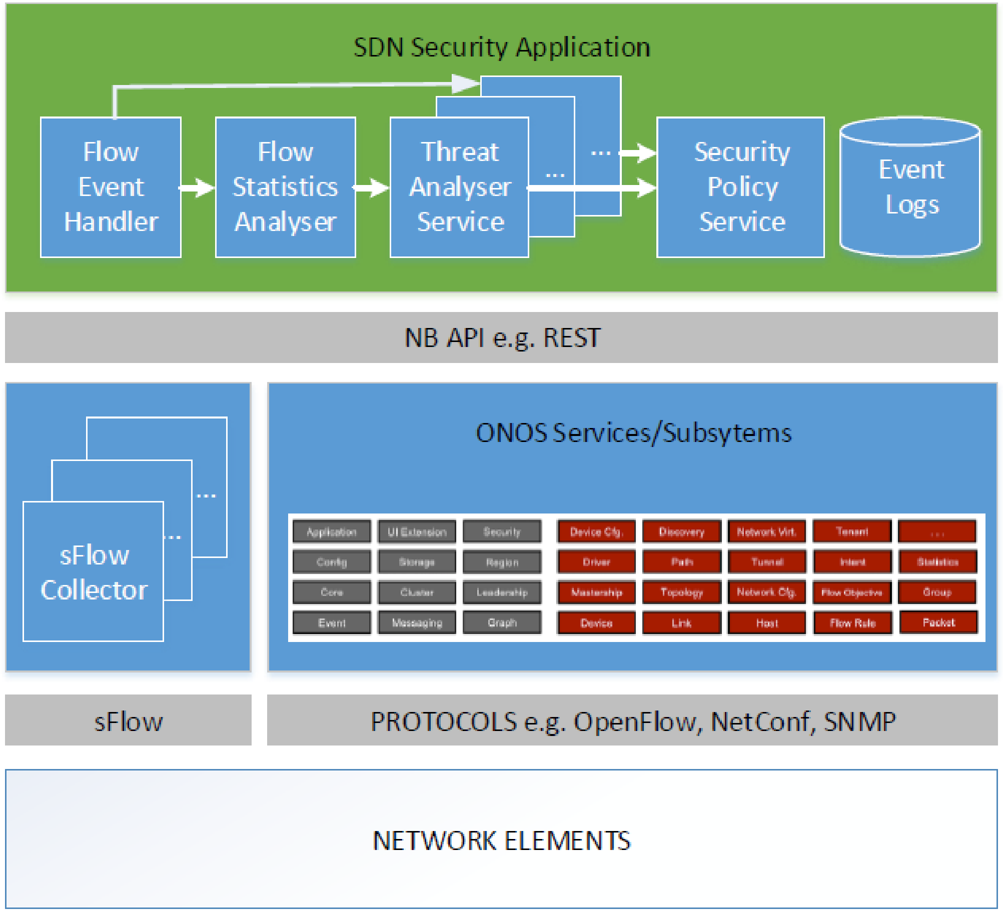
Who?

Taking an example of a botnet attack e.g. Mirai, who are we trying to detect?

Smart energy
Intelligent healthcare
Intelligent transportation
Smart recycle
Social network
Environment monitoring
Smart community
Smart home

[1] Antonakakis, M. et al., 2017. Understanding the Mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 1093-1110).
[2] Kumar, A. and Lim, T.J., 2019, March. Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-sampled Packet Traffic Analysis. In *Future of Information and Communication Conference* (pp. 847-867). Springer, Cham.
[3] Zhang, Kuan, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen. "Security and privacy in smart city applications: Challenges and solutions." *IEEE Communications Magazine* 55, no. 1 (2017): 122-129.

SDN Monitoring/IDPS - SWIFTGuard



SDN Security Application

Flow Event Handler

Flow Statistics Analyser

Threat Analyser Service

...

...

Security Policy Service

Event Logs

NB API e.g. REST

sFlow Collector

...

...

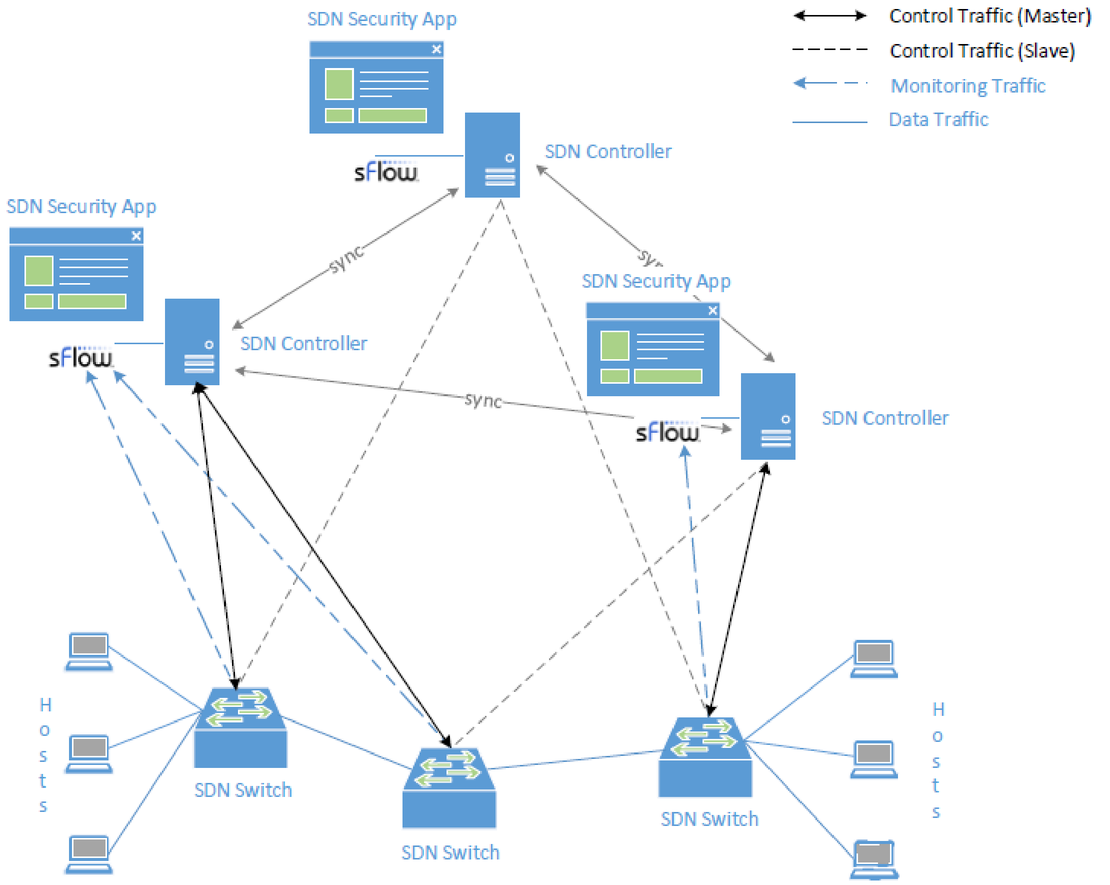
ONOS Services/Subsytems

Application	UI Extension	Security	Device Cfg.	Discovery	Network Virt.	Tenant	...
Config	Storage	Region	Driver	Path	Tunnel	Intent	Statistics
Core	Cluster	Leadership	Mastership	Topology	Network Cfg.	Flow Objective	Group
Event	Messaging	Graph	Device	Link	Host	Flow Rule	Packet

sFlow

PROTOCOLS e.g. OpenFlow, NetConf, SNMP

NETWORK ELEMENTS



Control Traffic (Master)

Control Traffic (Slave)

Monitoring Traffic

Data Traffic

SDN Security App

sFlow

SDN Controller

SDN Security App

sFlow

SDN Controller

SDN Security App

sFlow

SDN Controller

sync

sync

sync

Hosts

SDN Switch

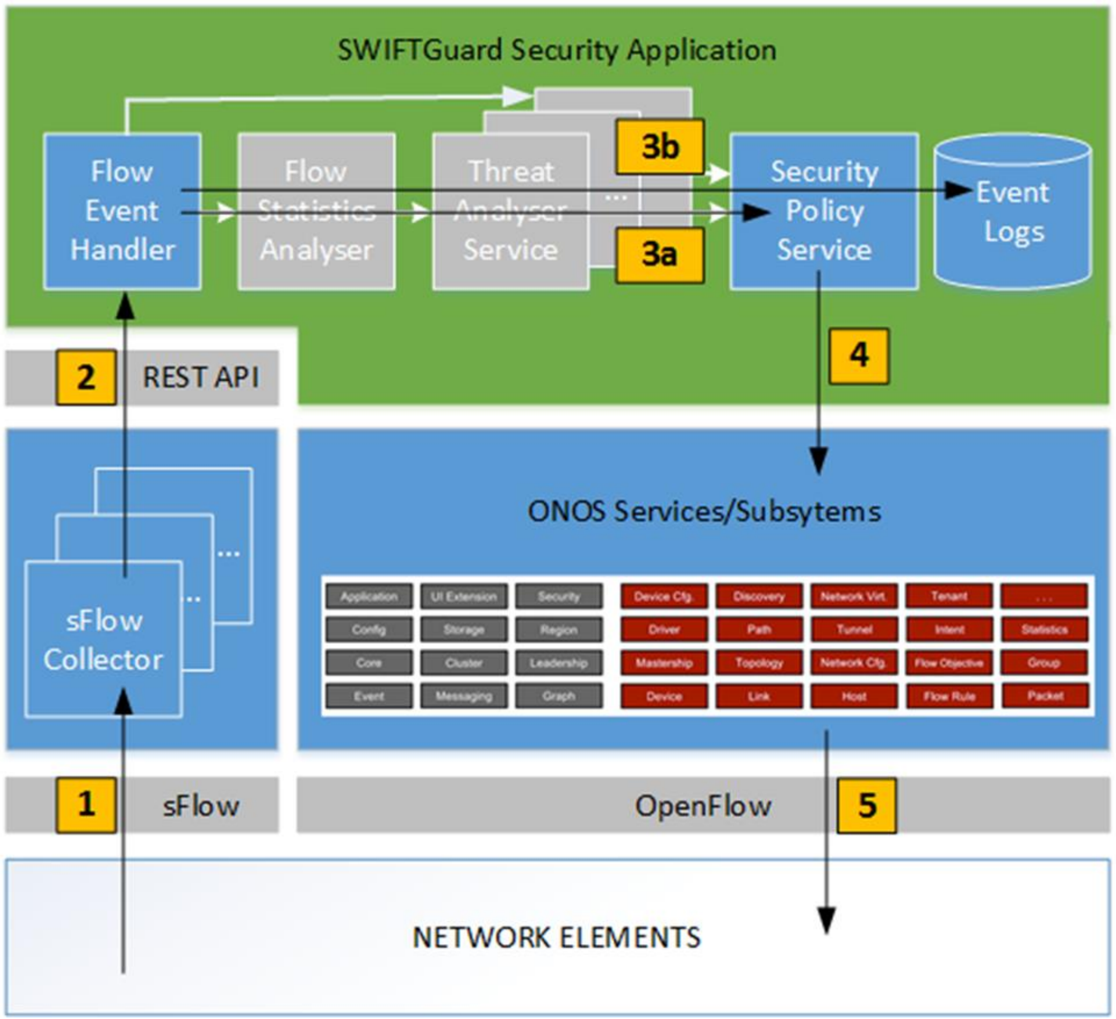
SDN Switch

SDN Switch

Hosts

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

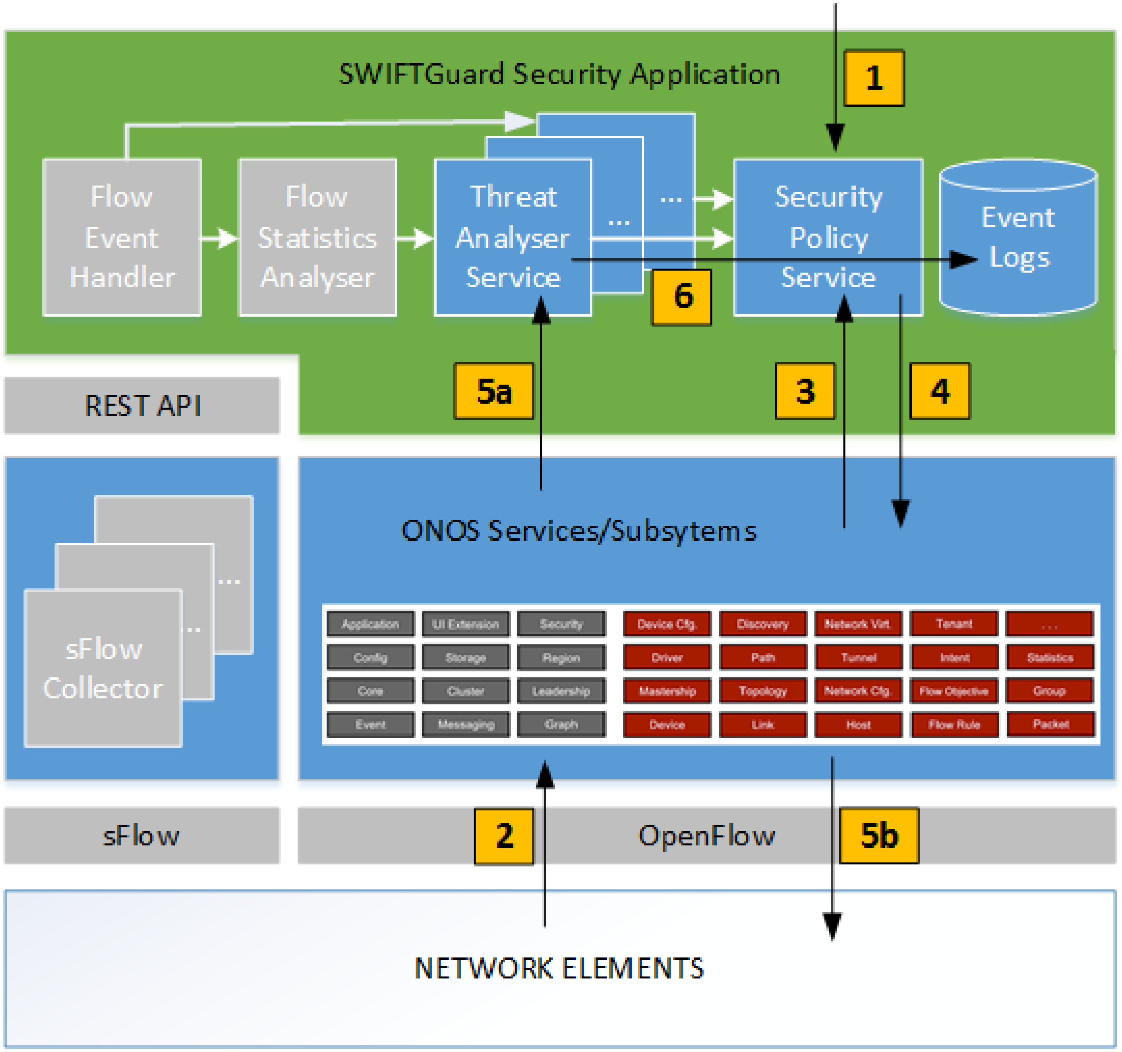
DDoS Detection/Protection



1. sFlow datagrams received by sFlowRT
2. DDoS event detected and sent to SWIFTGuard using RESTful API
3. Security policy generated by SWIFTGuard and event logged
4. Security policy received by ONOS flow rule subsystem
5. OpenFlow rules sent by ONOS to network elements

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

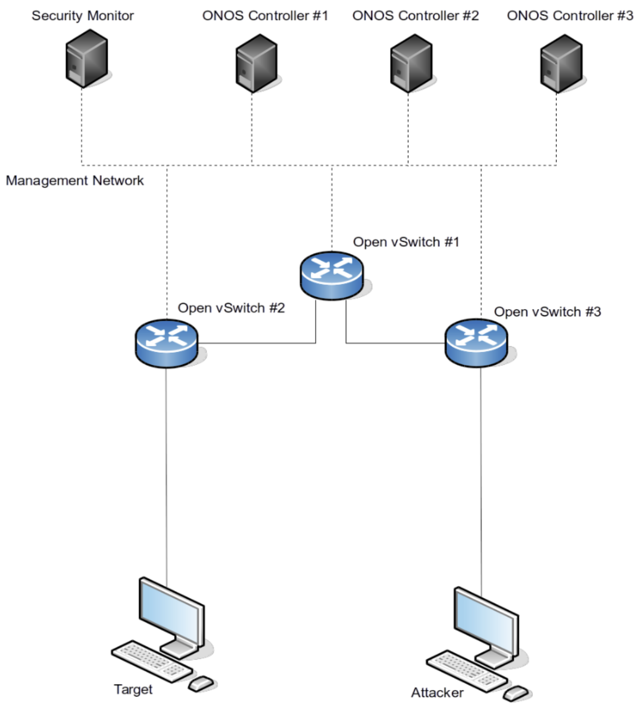
Malicious Host Detection/Traffic Mirroring

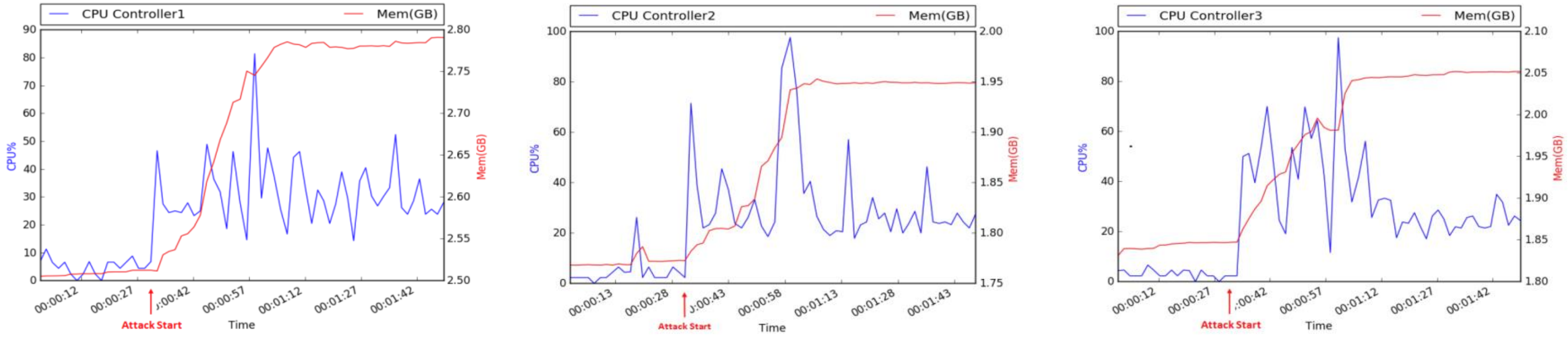


1. IP Monitor/Blacklist loaded to SWIFTGuard
2. Packet_In received by ONOS
3. Packet_In parsed and checked against SWIFTGuard security policy (e.g. monitor/blacklist)
4. Flow rule created to fwd/drop/mirror traffic
5. Packets of flow blocked/dropped/mirrored
6. Event of mirrored traffic logged

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Performance analysis – ONOS Distributed Control SDN

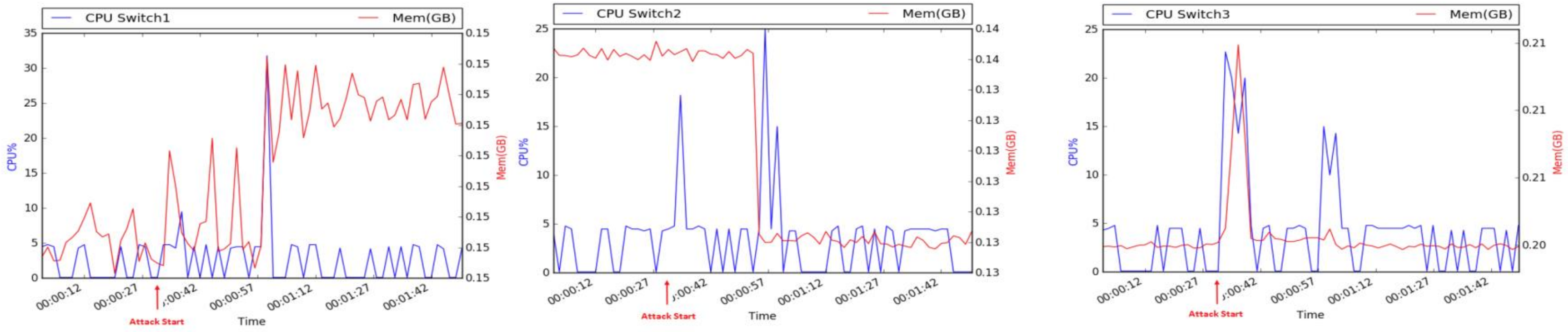




(a) Controller 1 Resource Usage

(b) Controller 2 Resource Usage

(c) Controller 3 Resource Usage



(a) Switch 1 Resource Usage

(b) Switch 2 Resource Usage

(c) Switch 3 Resource Usage

3s DDoS Attack

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Impact of DDoS

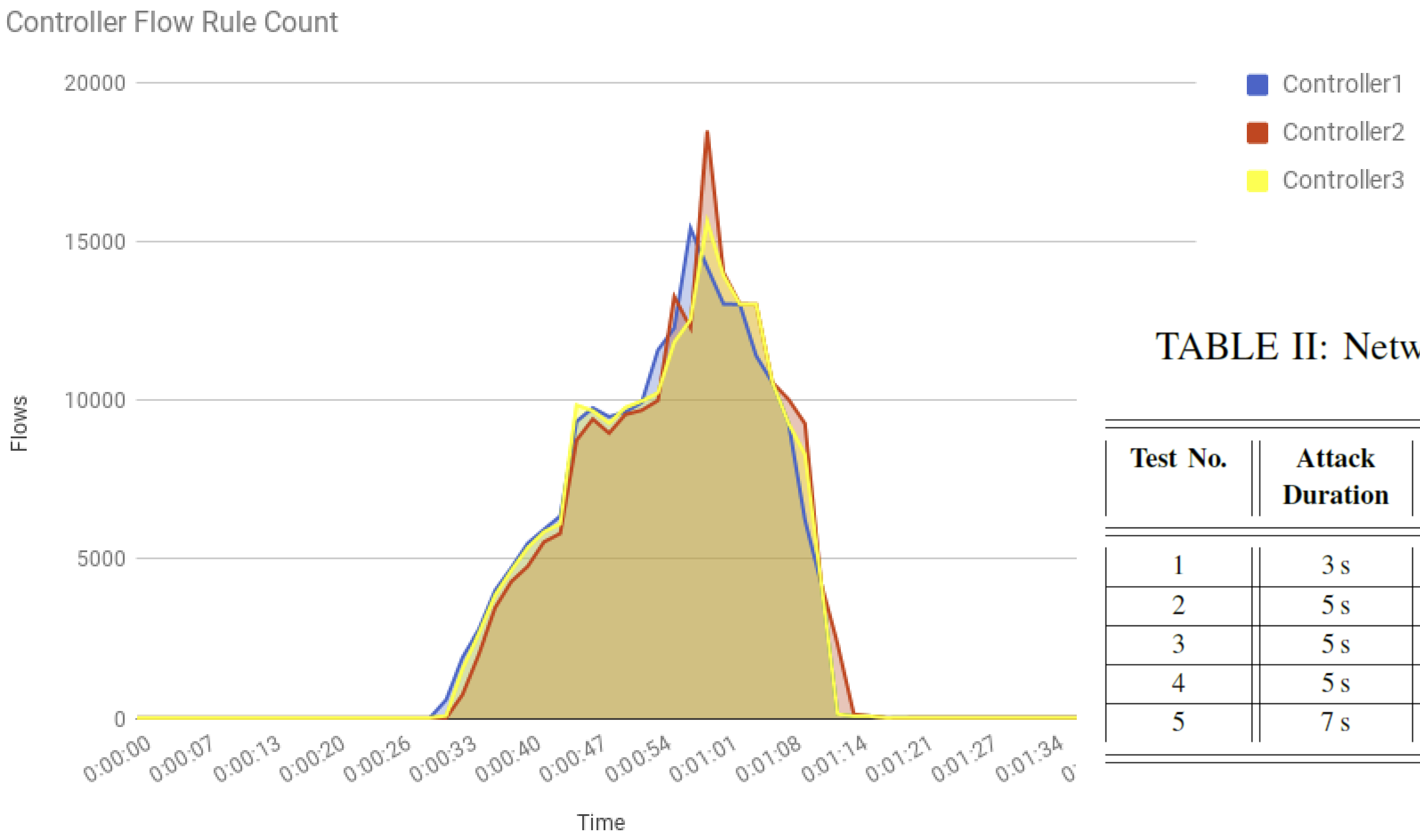
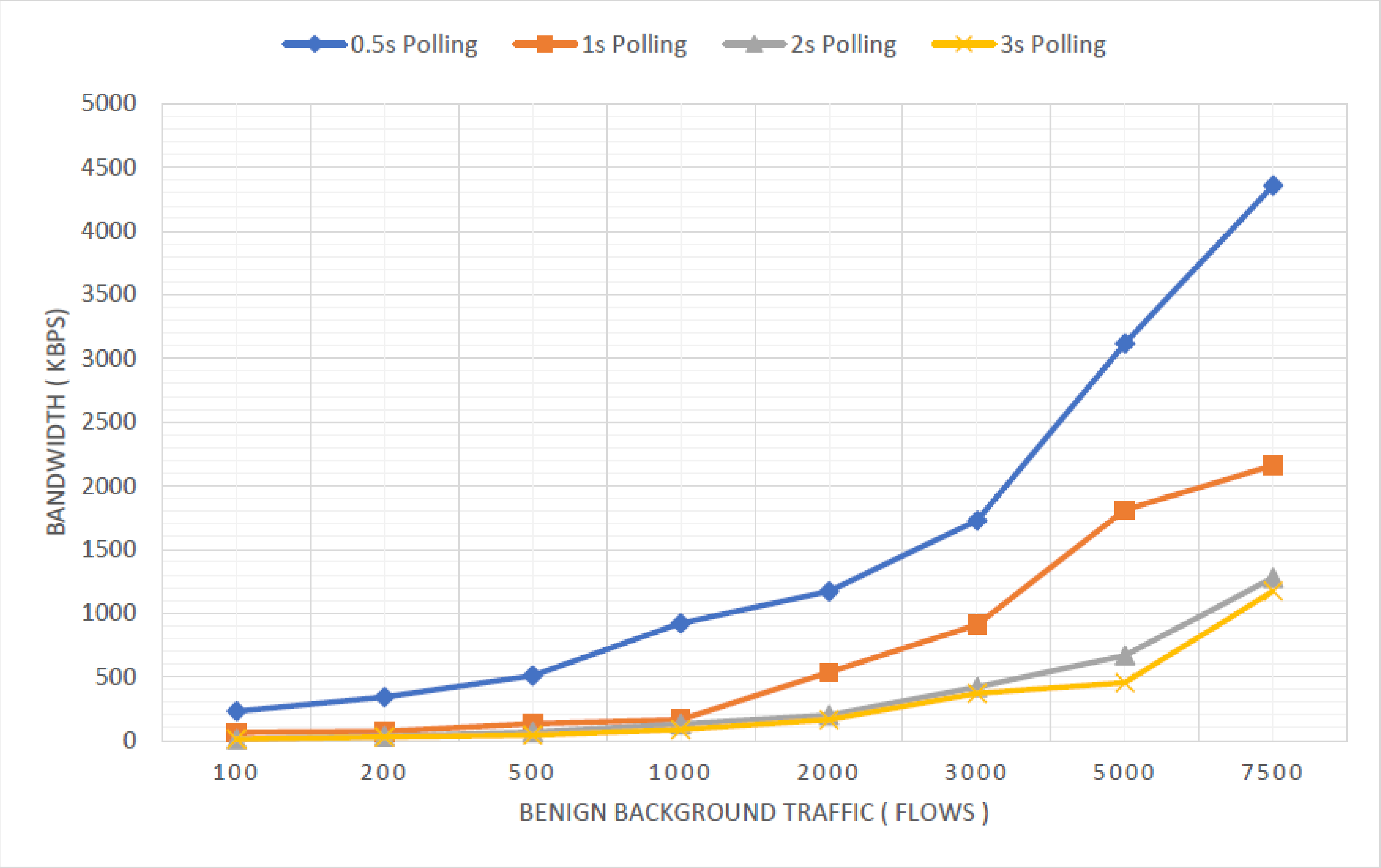


TABLE II: Network DoS Detection/Protection Times

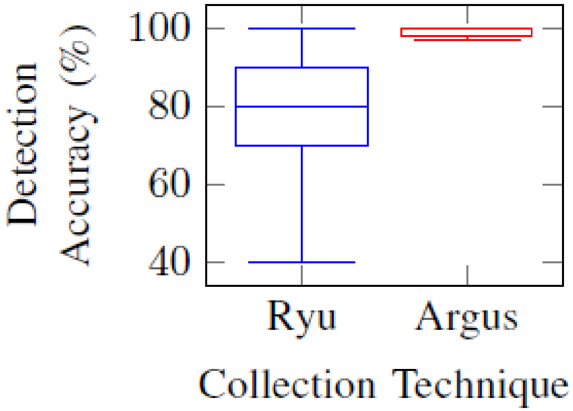
Test No.	Attack Duration	Detection Time	Protection Time	Network Recovery Time
1	3 s	1.313 s	1.511 s (+0.198 s)	43 s
2	5 s	1.210 s	1.393 s (+0.018 s)	85 s
3	5 s	0.695 s	0.716 s (+0.021 s)	100 s
4	5 s	3.367 s	3.389 s (+0.021 s)	302 s
5	7 s	4.162 s	4.181 s (+0.019 s)	N/A

When?

What’s the impact of when you monitor? Polling in SDN?

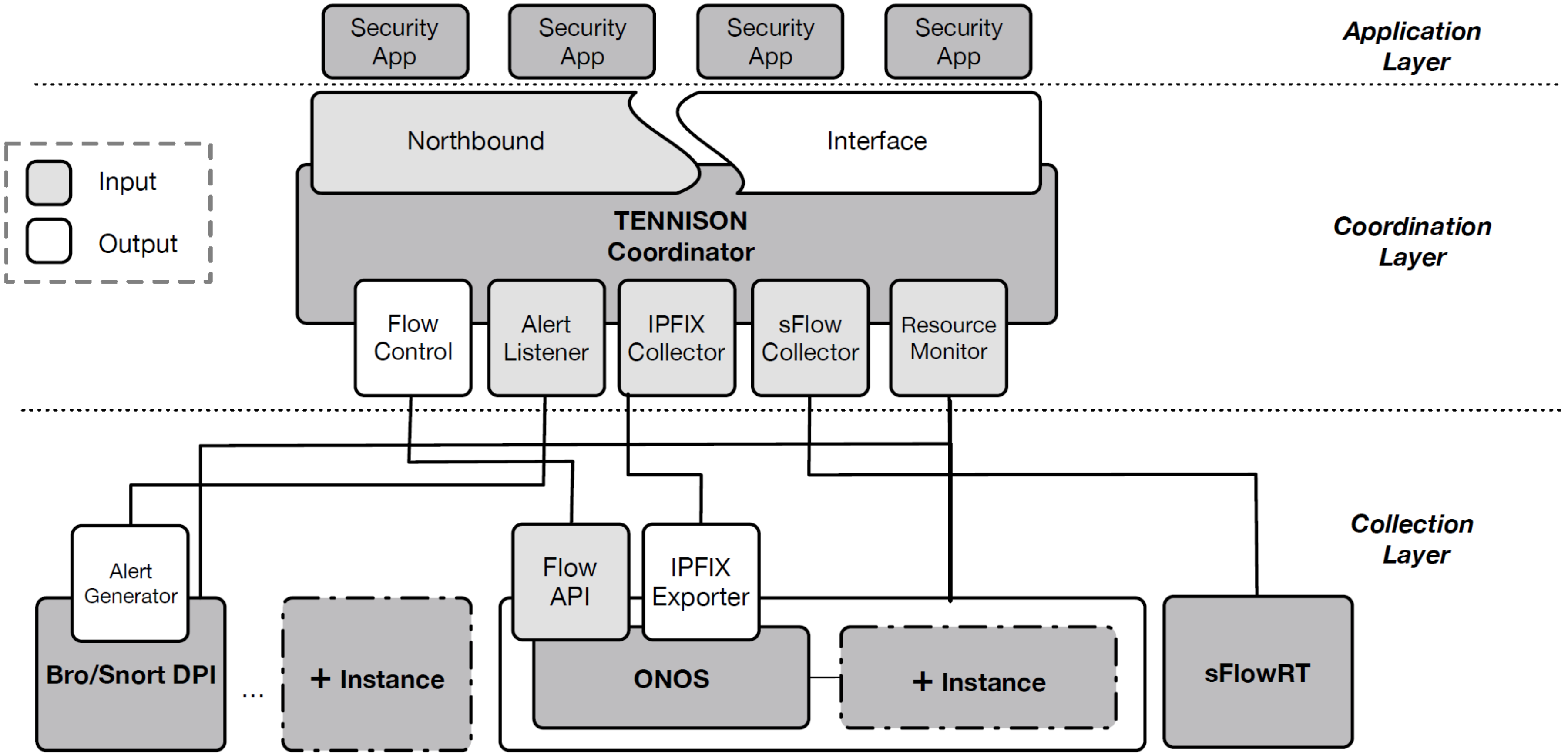


Comparison in SYN Flood Detection Accuracy



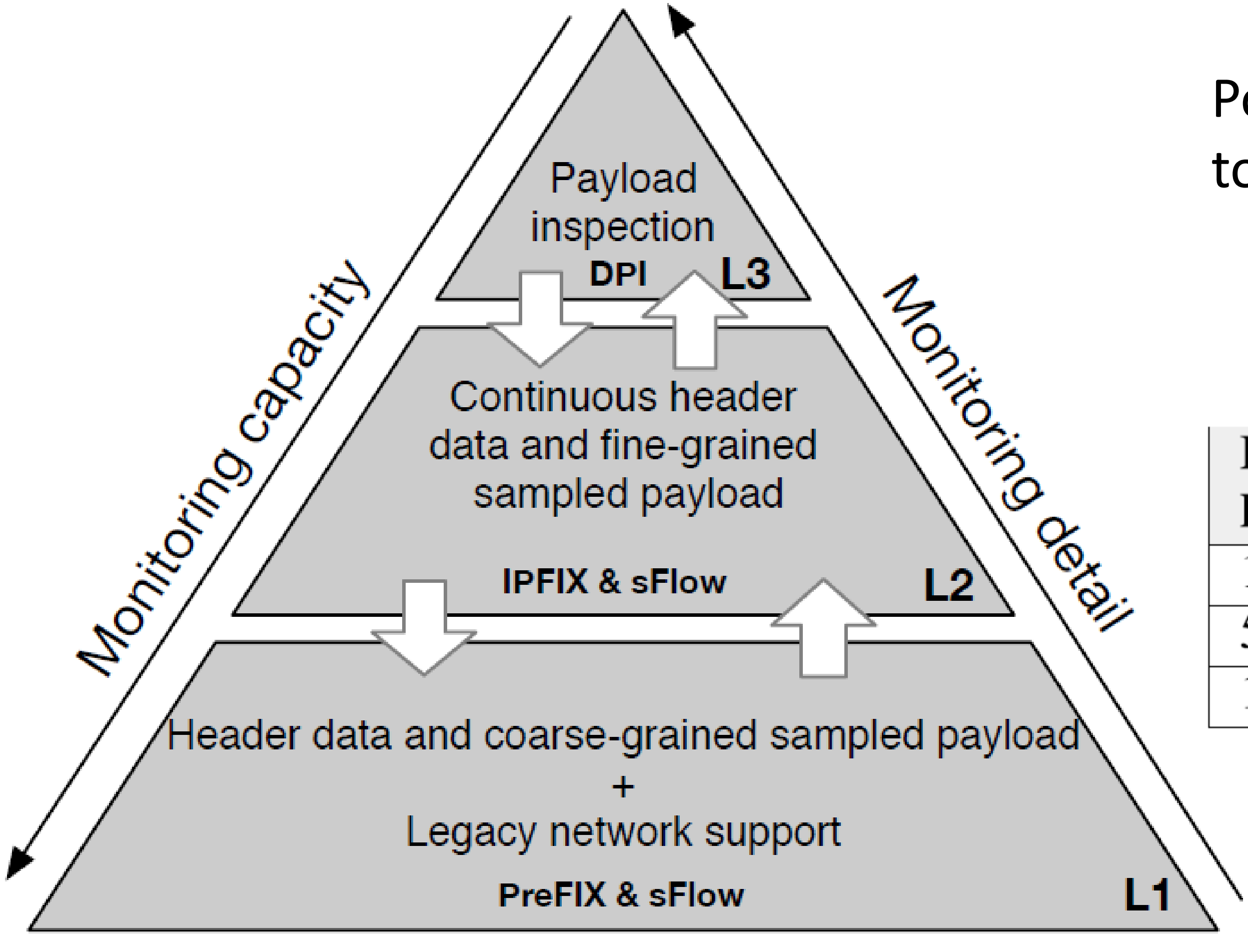
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

TENNISON multi-level monitoring

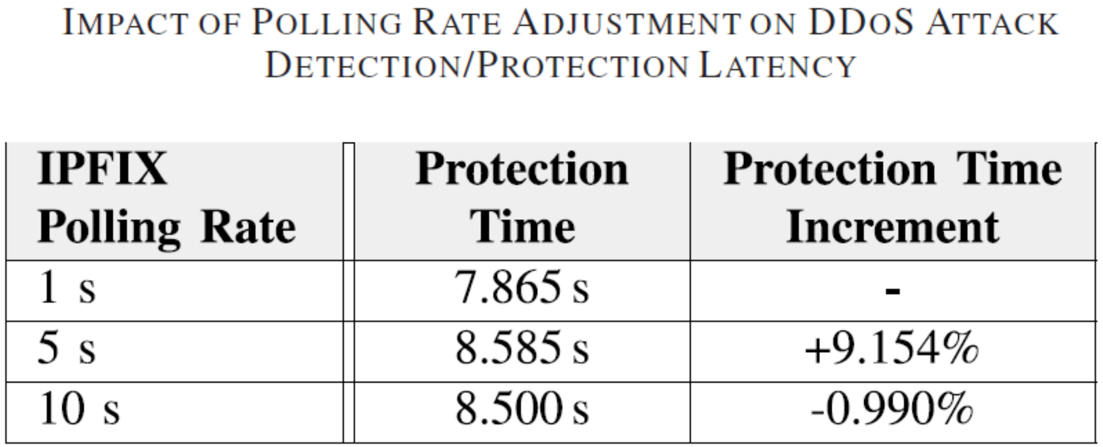


[4] Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A. and Race, N. "TENNISON: A distributed SDN framework for scalable network security", *IEEE Journal on Selected Areas in Communications, Dec*. 2018.

TENNISON multi-level monitoring



Polling interval adjusted to adapt monitoring to the load experienced at the controller.

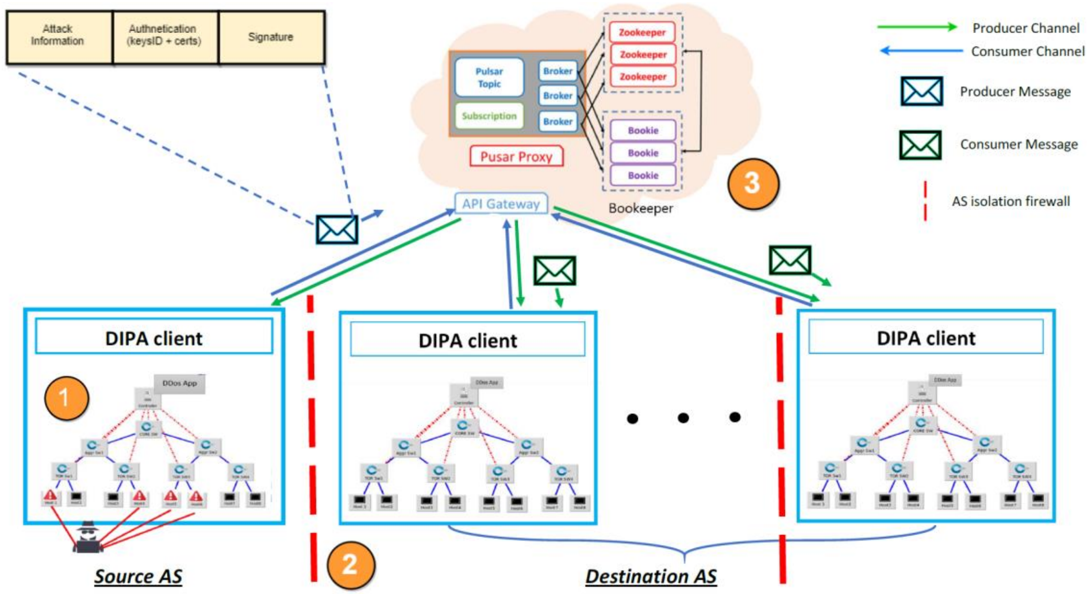


IMPACT OF POLLING RATE ADJUSTMENT ON DDOS ATTACK DETECTION/PROTECTION LATENCY

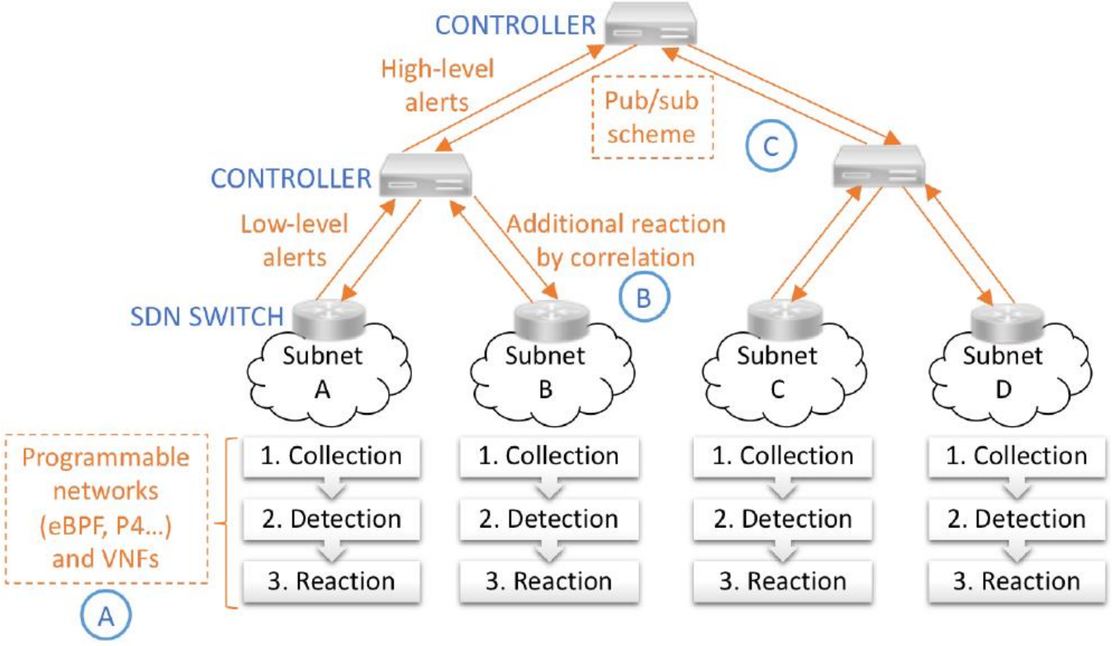
IPFIX Polling Rate	Protection Time	Protection Time Increment
1 s	7.865 s	-
5 s	8.585 s	+9.154%
10 s	8.500 s	-0.990%

Where?

Edge vs. Core, Switch vs. Controller?



Edge-based Network Protection using Apache Pulsar

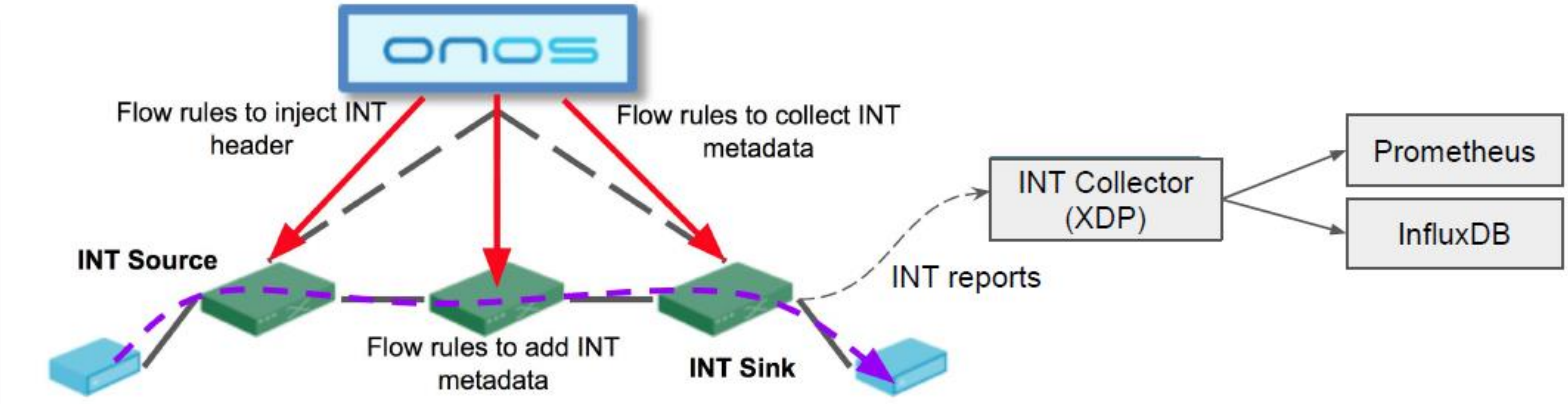


Scalable and collaborative SDNFV-based IDPS: local detection at the data plane enhanced by collaboration between ISPs [5]

[5] Blaise, A., Scott-Hayward, S., and Secci S., "Scalable and Collaborative Intrusion Detection and Prevention Systems based on Software-Defined Networking and Network Functions Virtualization", Book Chapter submitted for EU COST ACTION 15127 RECODIS, April 2019.

Where?

Data Plane monitoring … telemetry … attack detection

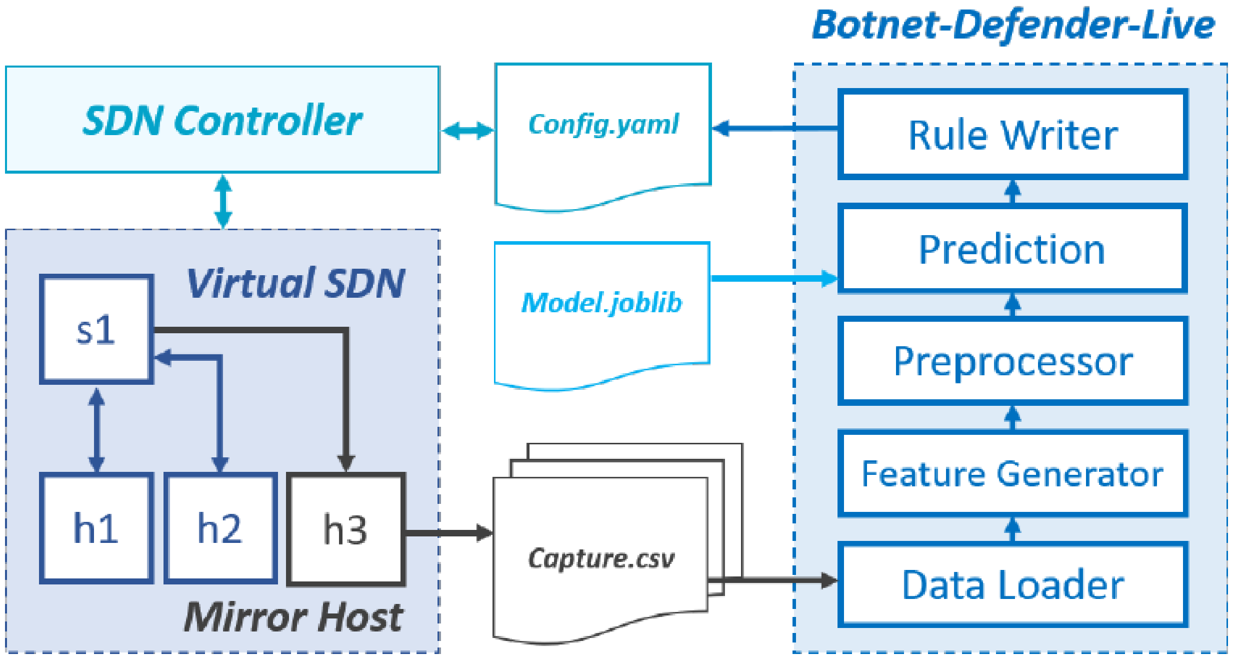

ONOS
Flow rules to inject INT header
Flow rules to collect INT metadata
INT Collector (XDP)
Prometheus
InfluxDB
INT Source
INT reports
Flow rules to add INT metadata
INT Sink

INT Architecture with ONOS [6]

[5] p4.org
[6] https://wiki.onosproject.org/display/ONOS/In-band+Network+Telemetry+%28INT%29+with+ONOS+and+P4

What?

We want to monitor network traffic but what information is interesting/useful?



Botnet Defender Architecture

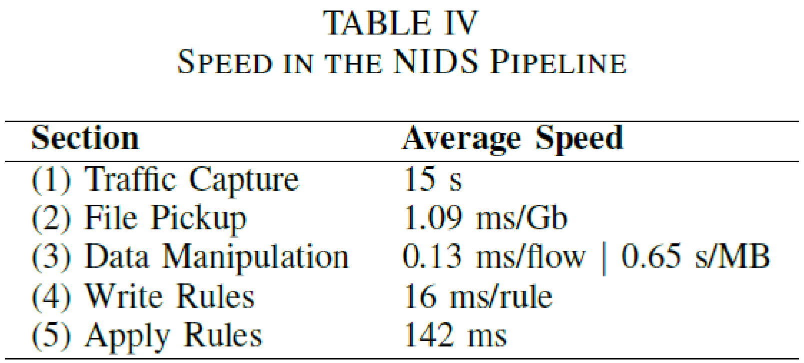
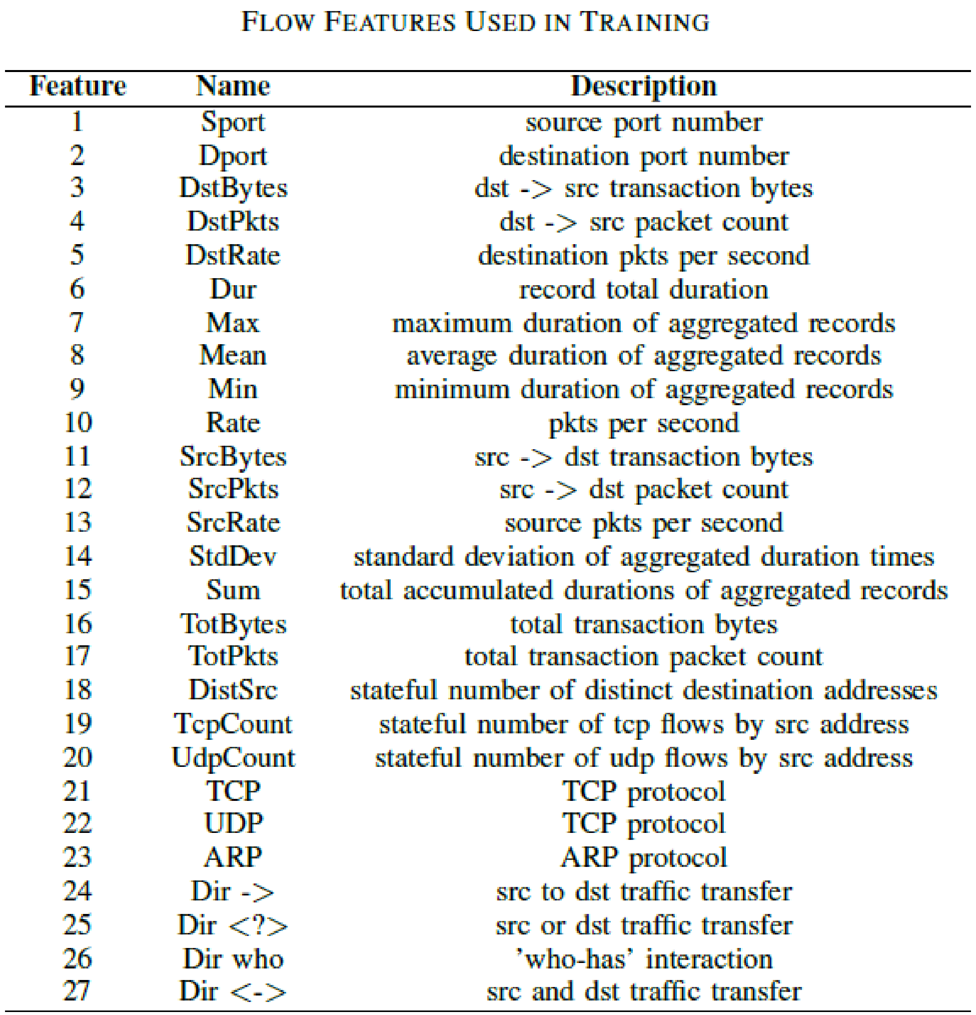


TABLE IV
Speed in the NIDS Pipeline

Section	Average Speed
(1) Traffic Capture	15 s
(2) File Pickup	1.09 ms/Gb
(3) Data Manipulation	0.13 ms/flow | 0.65 s/MB
(4) Write Rules	16 ms/rule
(5) Apply Rules	142 ms

What?

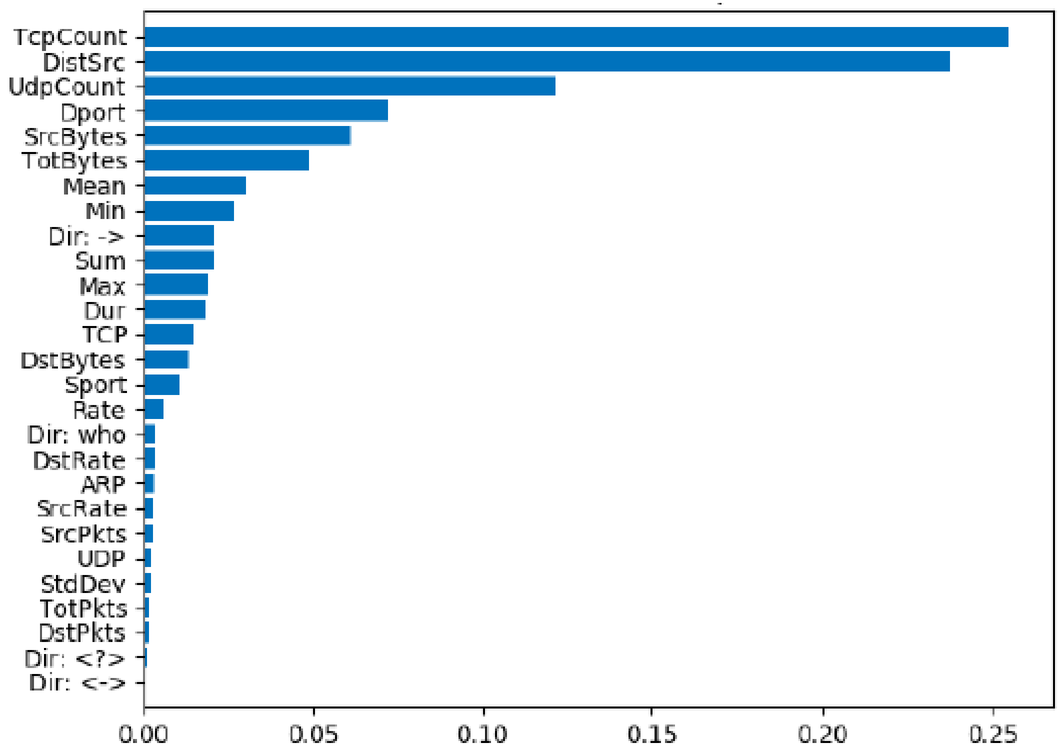
We want to monitor network traffic but what information is interesting/useful?



FLOW FEATURES USED IN TRAINING

Feature	Name	Description
1	Sport	source port number
2	Dport	destination port number
3	DstBytes	dst -> src transaction bytes
4	DstPkts	dst -> src packet count
5	DstRate	destination pkts per second
6	Dur	record total duration
7	Max	maximum duration of aggregated records
8	Mean	average duration of aggregated records
9	Min	minimum duration of aggregated records
10	Rate	pkts per second
11	SrcBytes	src -> dst transaction bytes
12	SrcPkts	src -> dst packet count
13	SrcRate	source pkts per second
14	StdDev	standard deviation of aggregated duration times
15	Sum	total accumulated durations of aggregated records
16	TotBytes	total transaction bytes
17	TotPkts	total transaction packet count
18	DistSrc	stateful number of distinct destination addresses
19	TcpCount	stateful number of tcp flows by src address
20	UdpCount	stateful number of udp flows by src address
21	TCP	TCP protocol
22	UDP	TCP protocol
23	ARP	ARP protocol
24	Dir ->	src to dst traffic transfer
25	Dir <?>	src or dst traffic transfer
26	Dir who	'who-has' interaction
27	Dir <->	src and dst traffic transfer

Random Forest Feature Importance for Botnet reconnaissance phase



Recommendations

Consider appropriate distribution of monitoring

- Implement monitoring in the data plane
- Split and coordinate monitoring across the network

Consider appropriate volume of monitoring

- Limit volume of data collected/post-processed
- Employ multi-level monitoring – adjust granularity or frequency to network state
- Reduce reliance on feature engineering – e.g. neural networks

Thank you

s.scott-hayward@qub.ac.uk

www.csit.qub.ac.uk

CSIT CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES