Interactive Analysis of SDN-driven defence against Distributed Denial of Service attacks

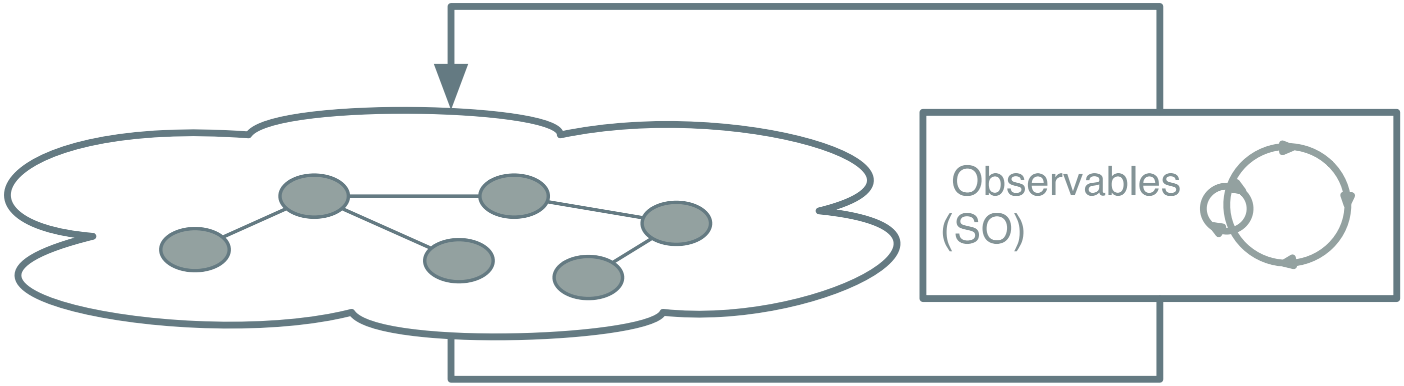
Ralph Koning, Ben de Graaff,
Cees de Laat, Robert Meijer, Paola Grosso
University of Amsterdam

Sec-VirtNet at NetSoft, June 10 2016, Seoul

This talk will:

- Show how visualisations can help with analyzing and understanding (DDoS) attacks.
- Elaborate on what kind of actions an SDN/SDI provide that can increase security of the tenants network.
- Tell what actions people choose to defend a network.
- That more changes/actions don’t necessarily result in a better solution to an attack.
- Give some insights in how to determine effectiveness of a set of countermeasures.

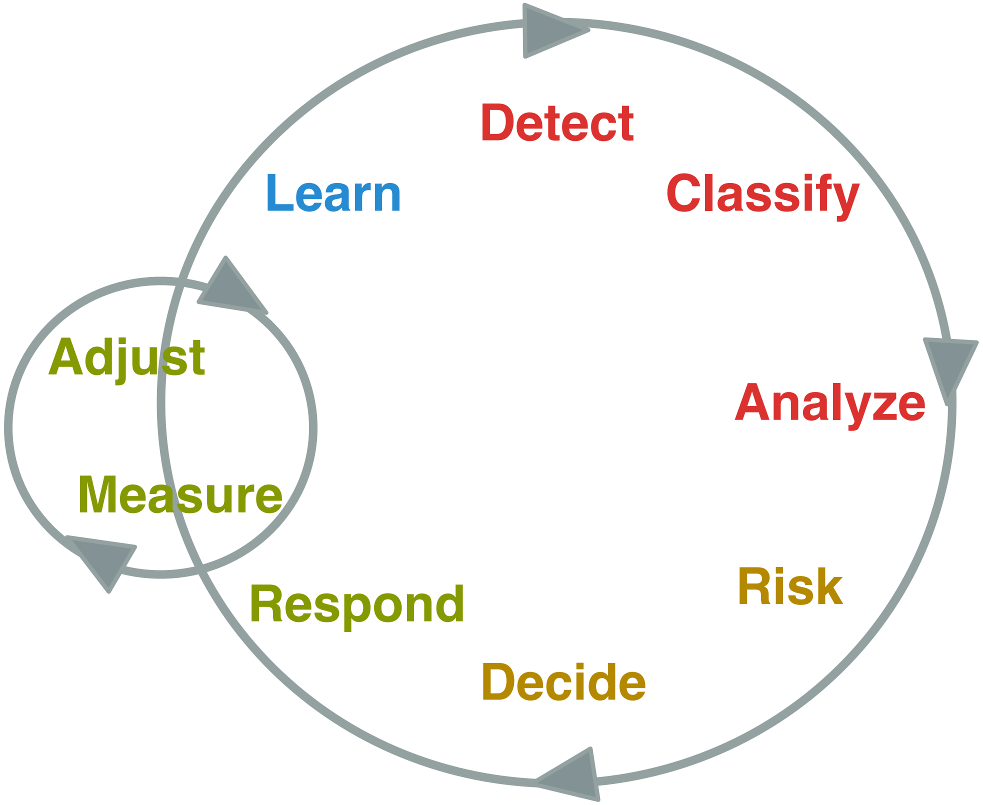
Secure autonomous response networks



Example observables:

Traffic to service provider x must pass via link y
Services request to service x is only allowed from y
Response time of the application should be < 30ms
CPU load of system x should not exceed y
Network bandwidth on link x cannot exceed 1 gb/s

Background: Control Loop



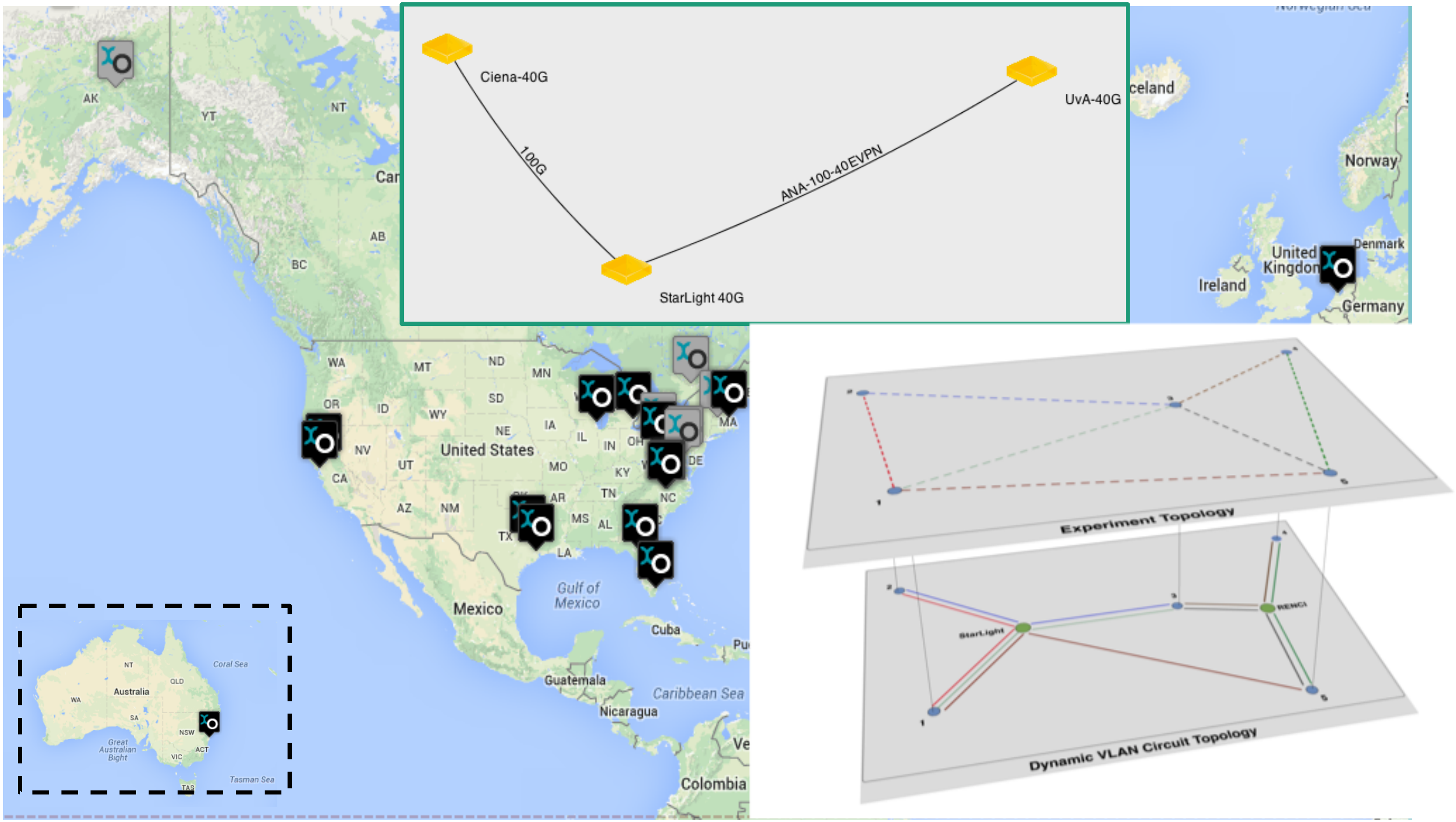
Detection phase: Detect, Classify, Analyze

Decision phase: Risk, Decide

Response phase: Respond, Adjust, Measure

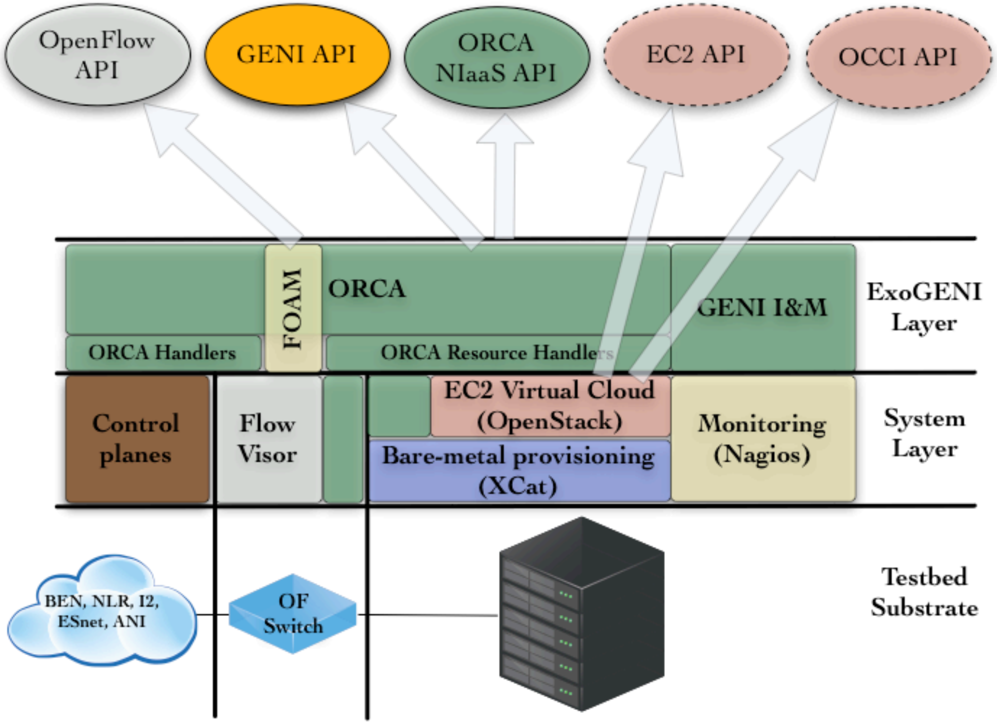
Learn phase: Learn (with input form other phases)

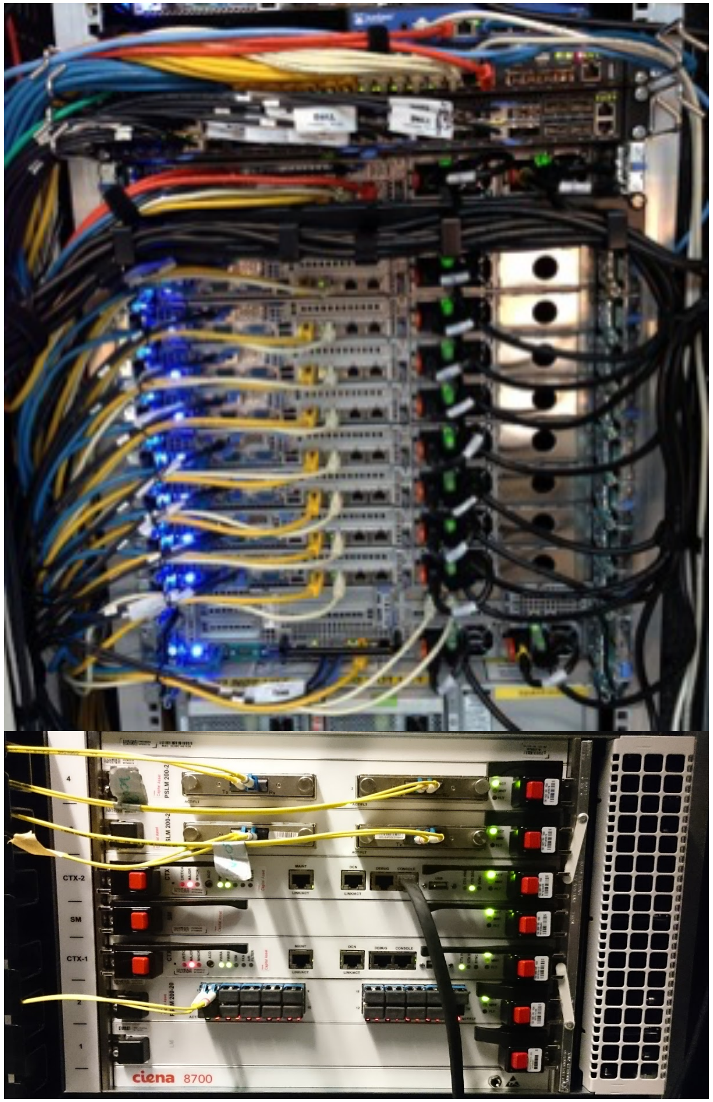
Platform: ExoGENI



Source: exogeni.net (2014)

Platform: ExoGENI





Source: exogeni.net (2014)

2015 functions

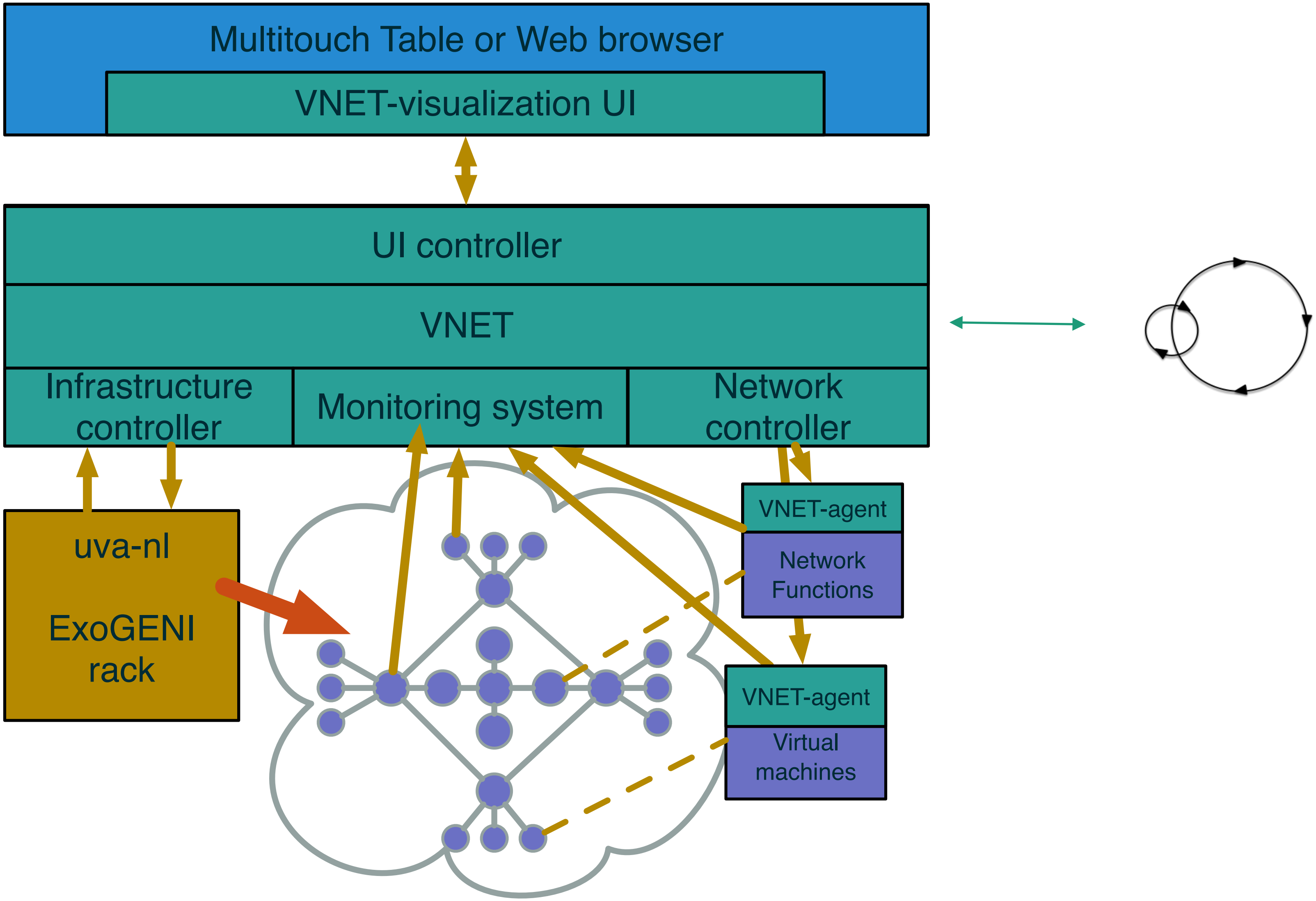
- Create slice
- Delete slice

2016 functions

- Create slice
- Modify slice
    - add, remove
    - host, links
- Delete slice

SuperComputing 2015

VNET stack



Multitouch Table or Web browser

VNET-visualization UI

UI controller

VNET

Infrastructure controller

Monitoring system

Network controller

uva-nl

ExoGENI rack

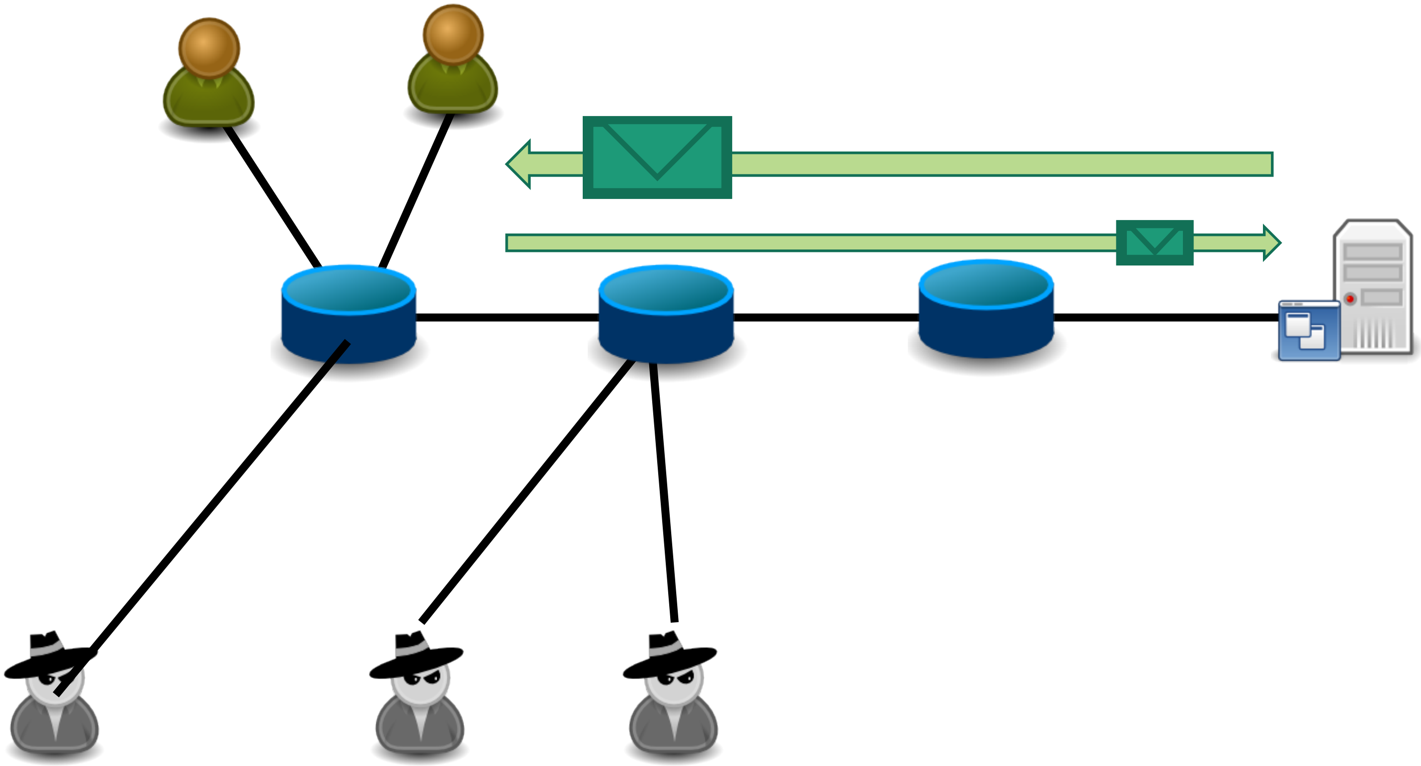
VNET-agent

Network Functions

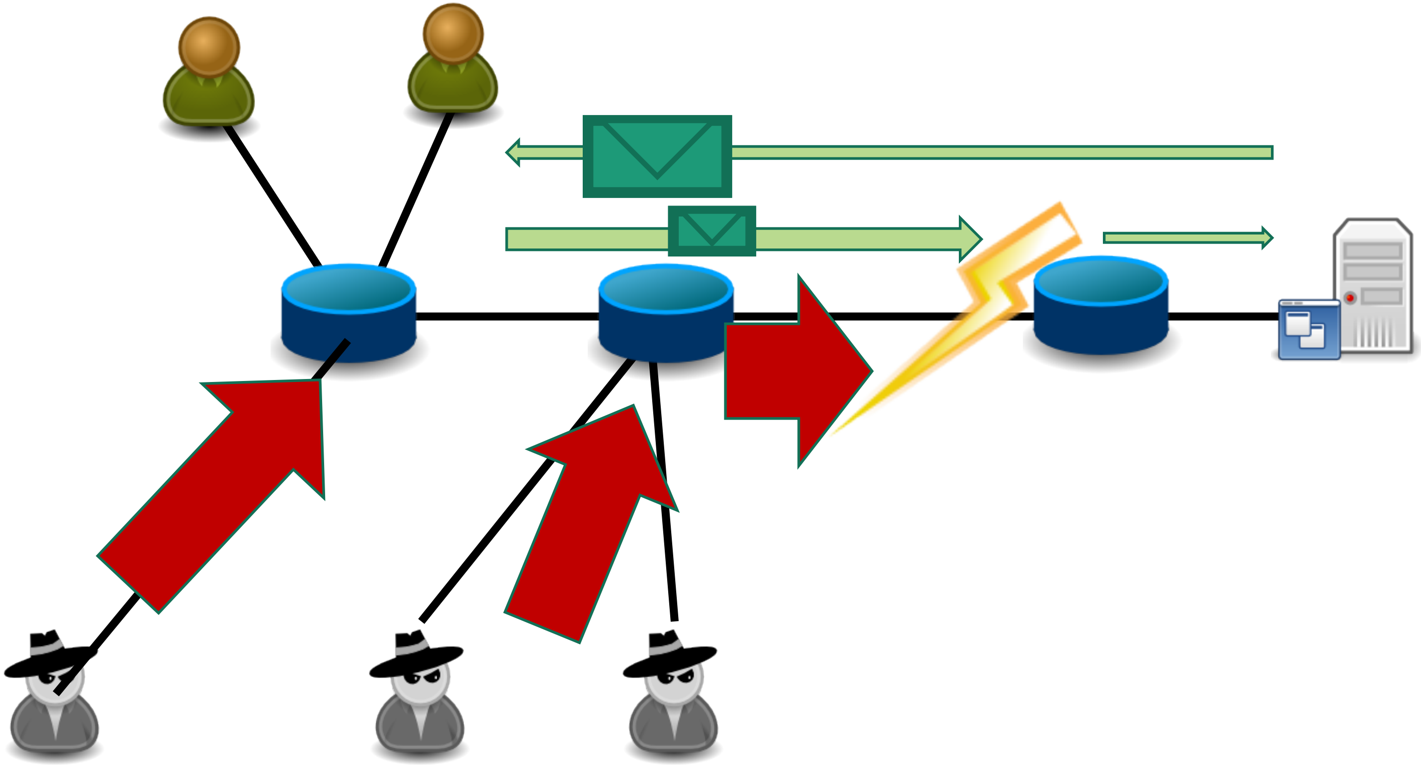
VNET-agent

Virtual machines

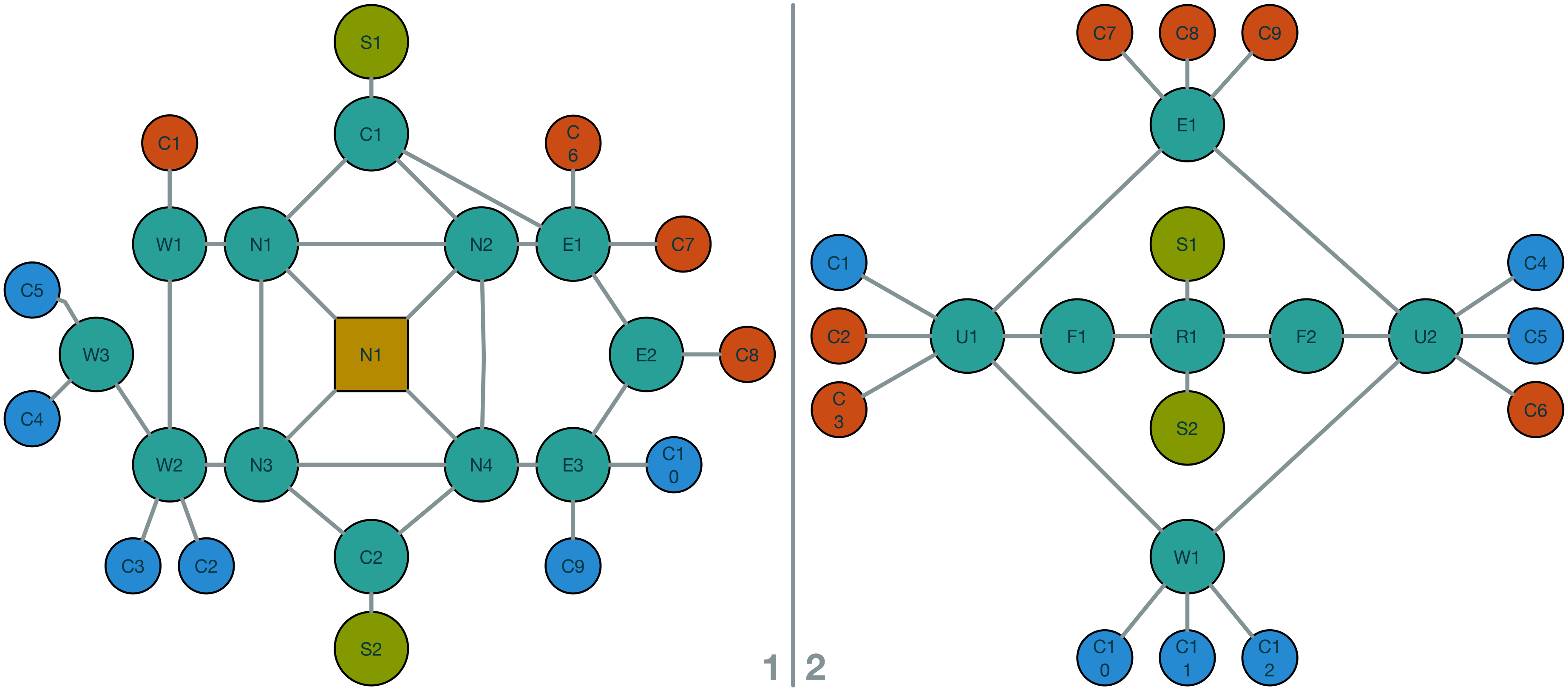
Attack scenario



Attack scenario

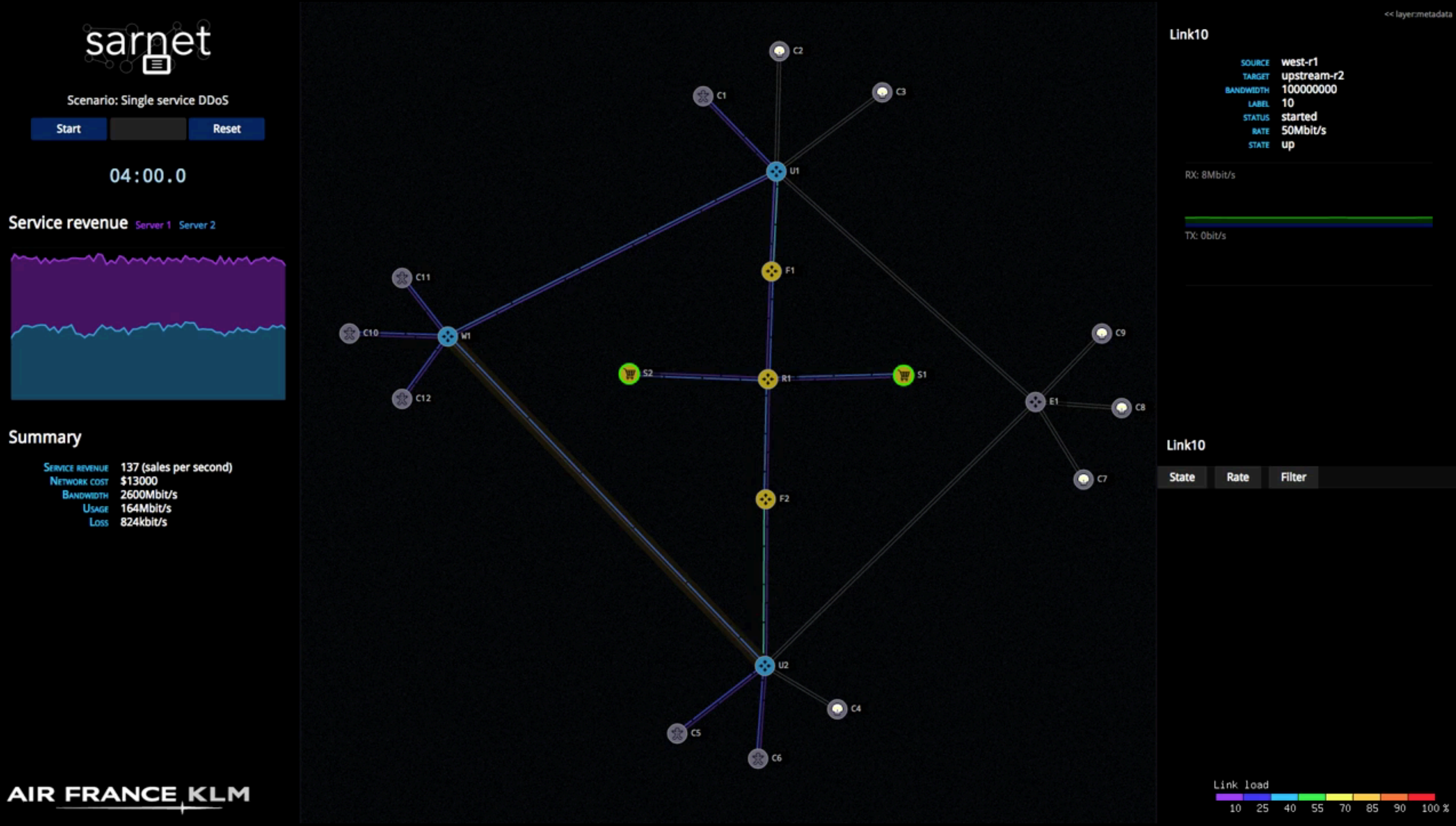


Networks


S1
C1
C1
C6
W1
N1
N2
E1
C7
C5
W3
N1
E2
C8
C4
W2
N3
N4
E3
C10
C3
C2
C2
C9
S2
1
2
C7
C8
C9
E1
S1
C1
C4
C2
U1
F1
R1
F2
U2
C5
C3
C6
S2
W1
C10
C11
C12

1

2



Scenario: Single service DDoS

04:00.0

Service revenue

Summary

Service revenue	137 (sales per second)
Network cost	$13000
Bandwidth	2600Mbit/s
Usage	164Mbit/s
Loss	824kbit/s

<< layer:metadata

Link10

SOURCE	west-r1
TARGET	upstream-r2
BANDWIDTH	100000000
LABEL	10
STATUS	started
RATE	50Mbit/s
STATE	up

RX: 8Mbit/s

TX: 0bit/s

Link10

Metrics: Revenue

- Revenue: transactions per second
  - Clients 1-10 make transactions to S1 and S2
  - The amount of transactions are summed together as revenue

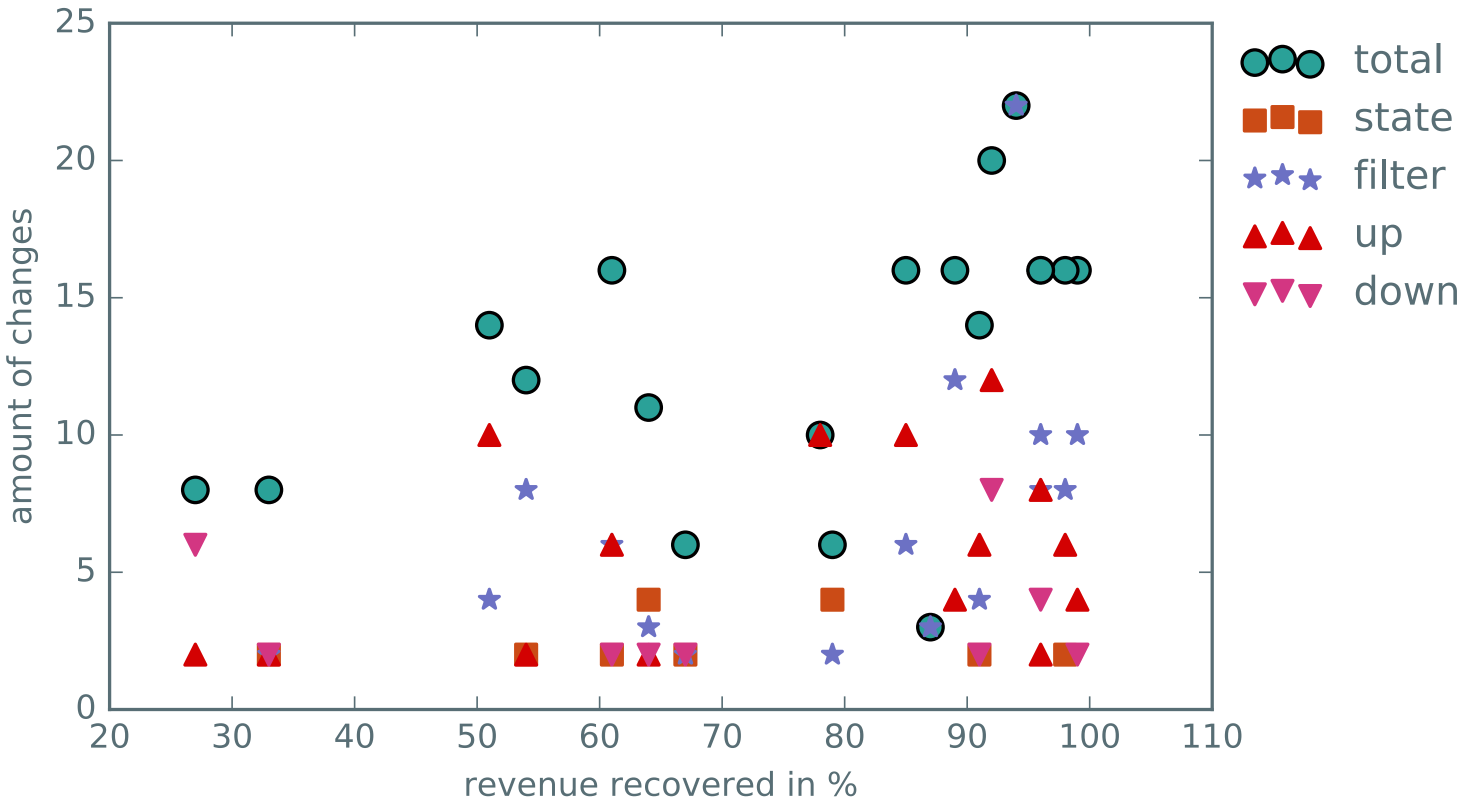
Metrics: Network cost

$$cost = b\frac{\sum_i r_i}{2} + f\sum_i a_i$$

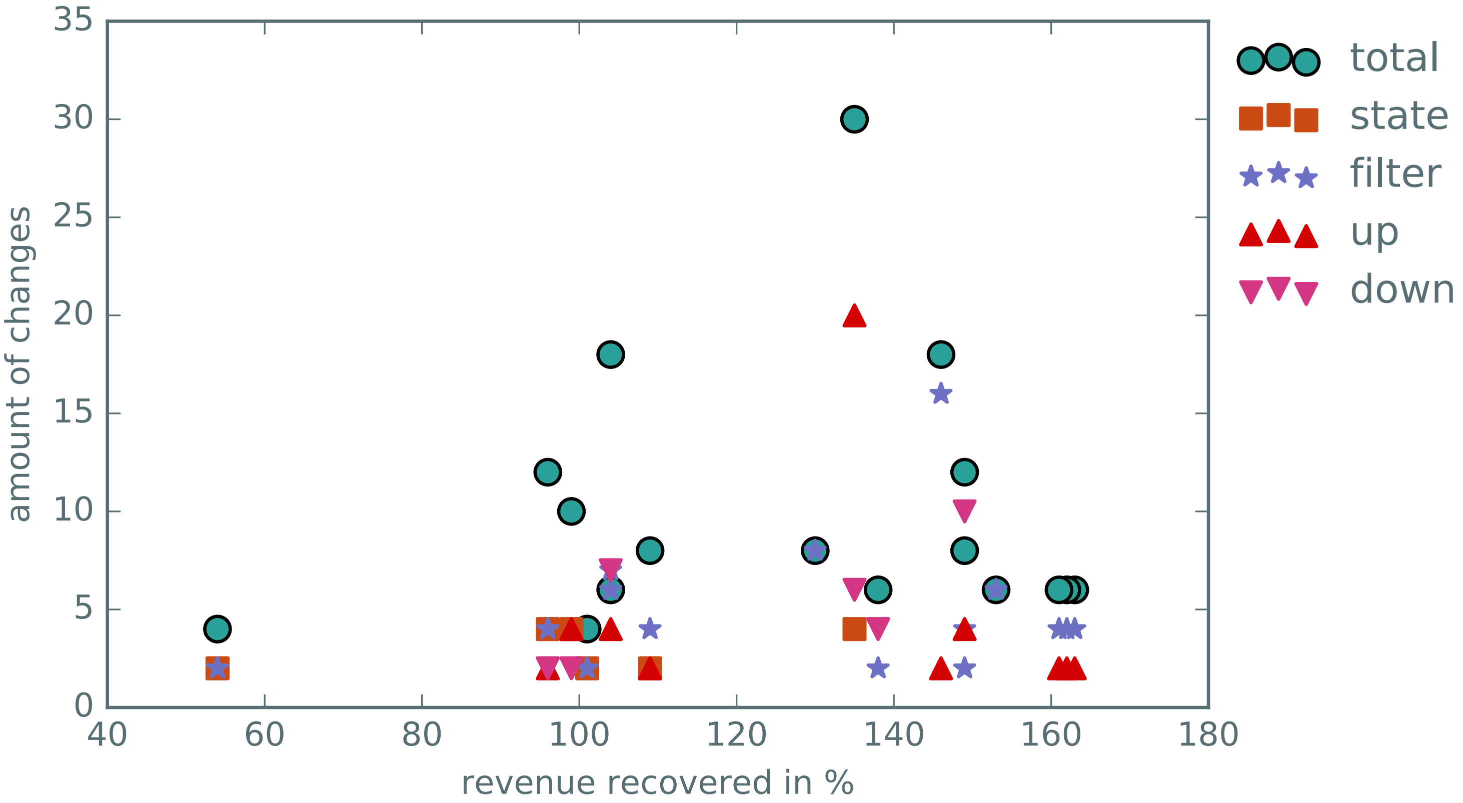
Where:

i is an active (enabled) interface
b is bandwidth cost in $ per megabit, we used b=10
f The cost of placing and activating a filter in $; we used f=500
r_i is the maximum bandwidth on interface i
a_i is the amount of activated filters on interface i, we used $a_i = \{1, 0\}$

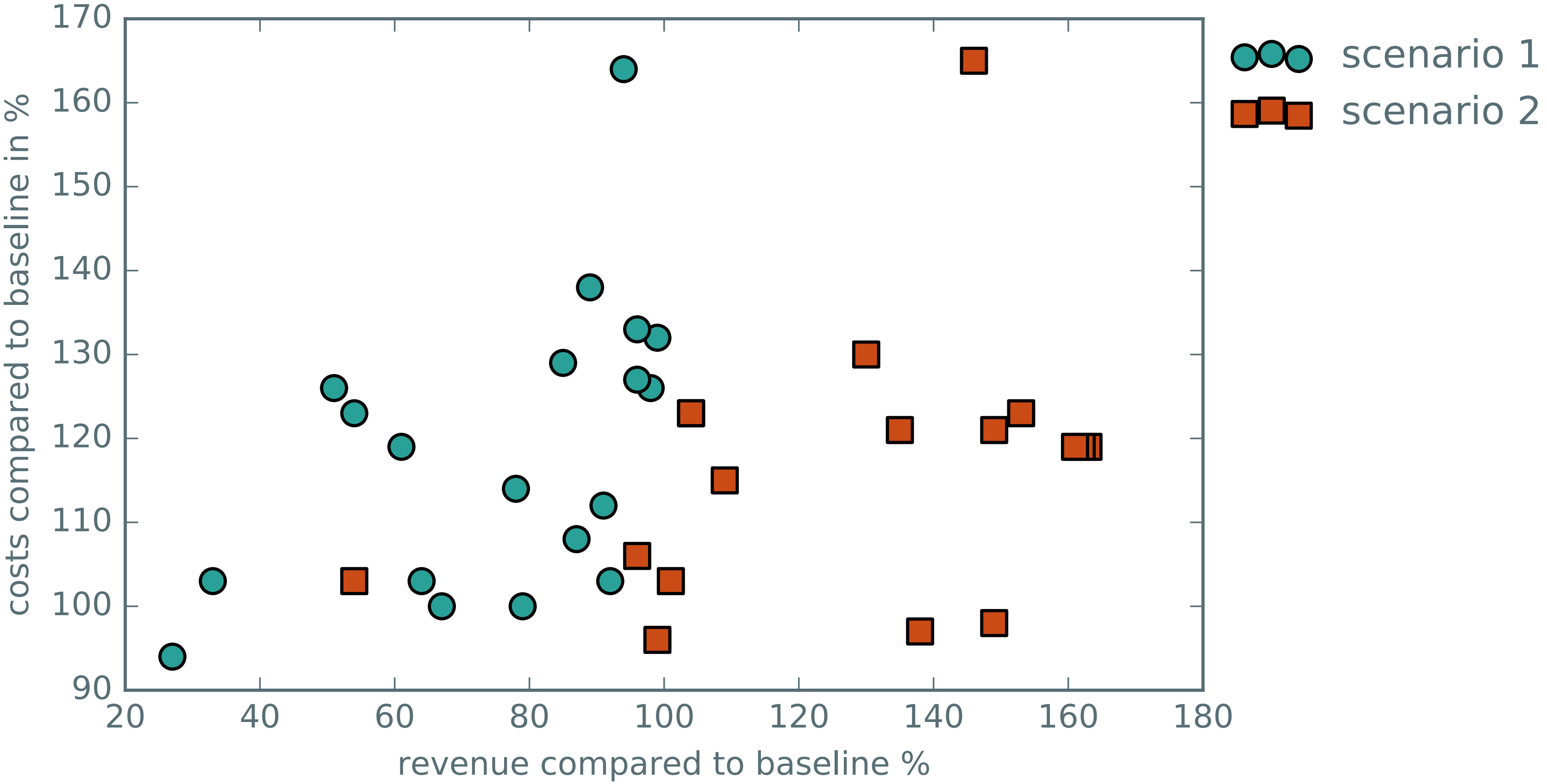
Actions vs Costs (scenario 1)



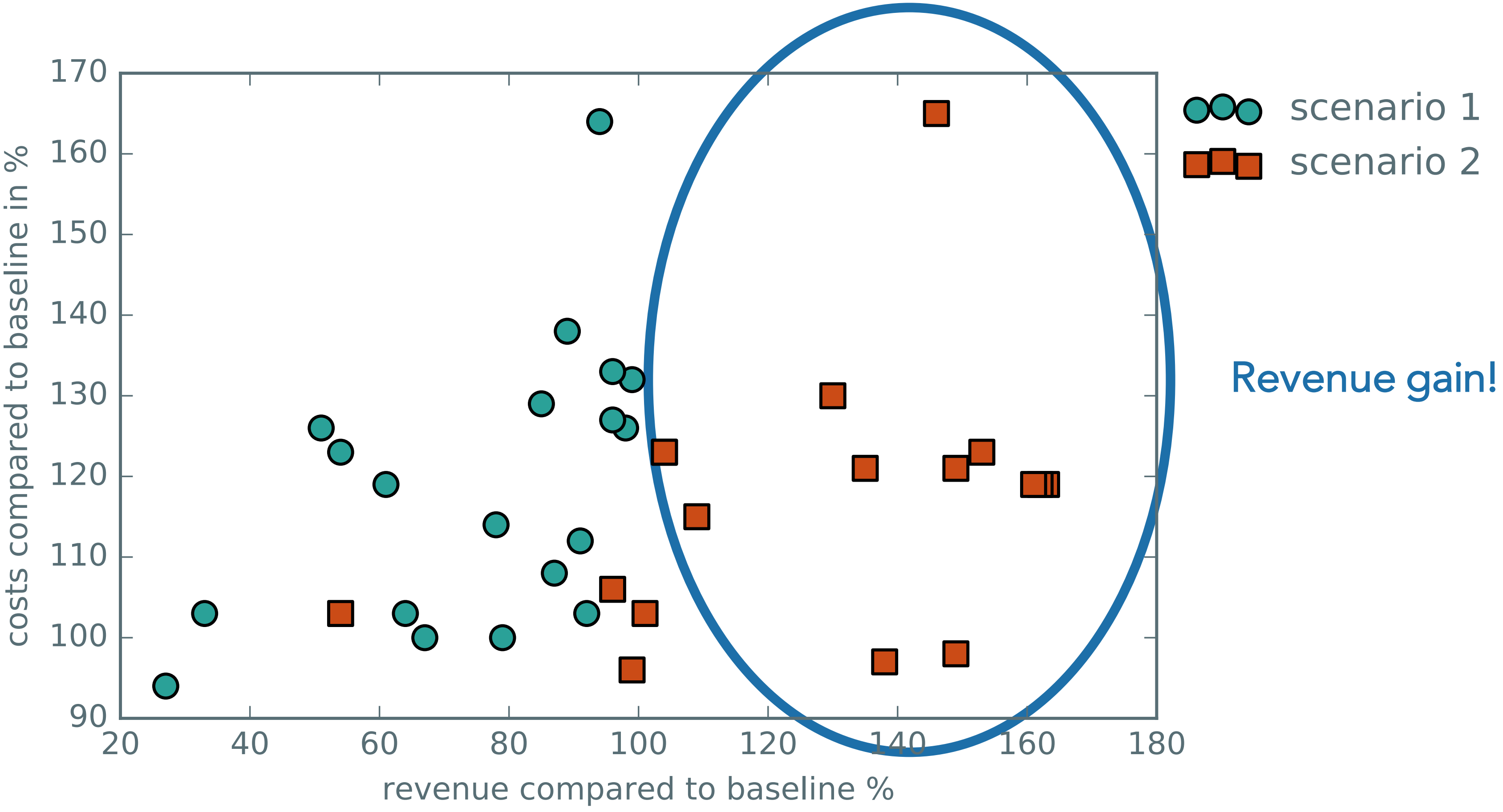
Actions vs Costs (scenario 2)



Solution cost and revenue recovery

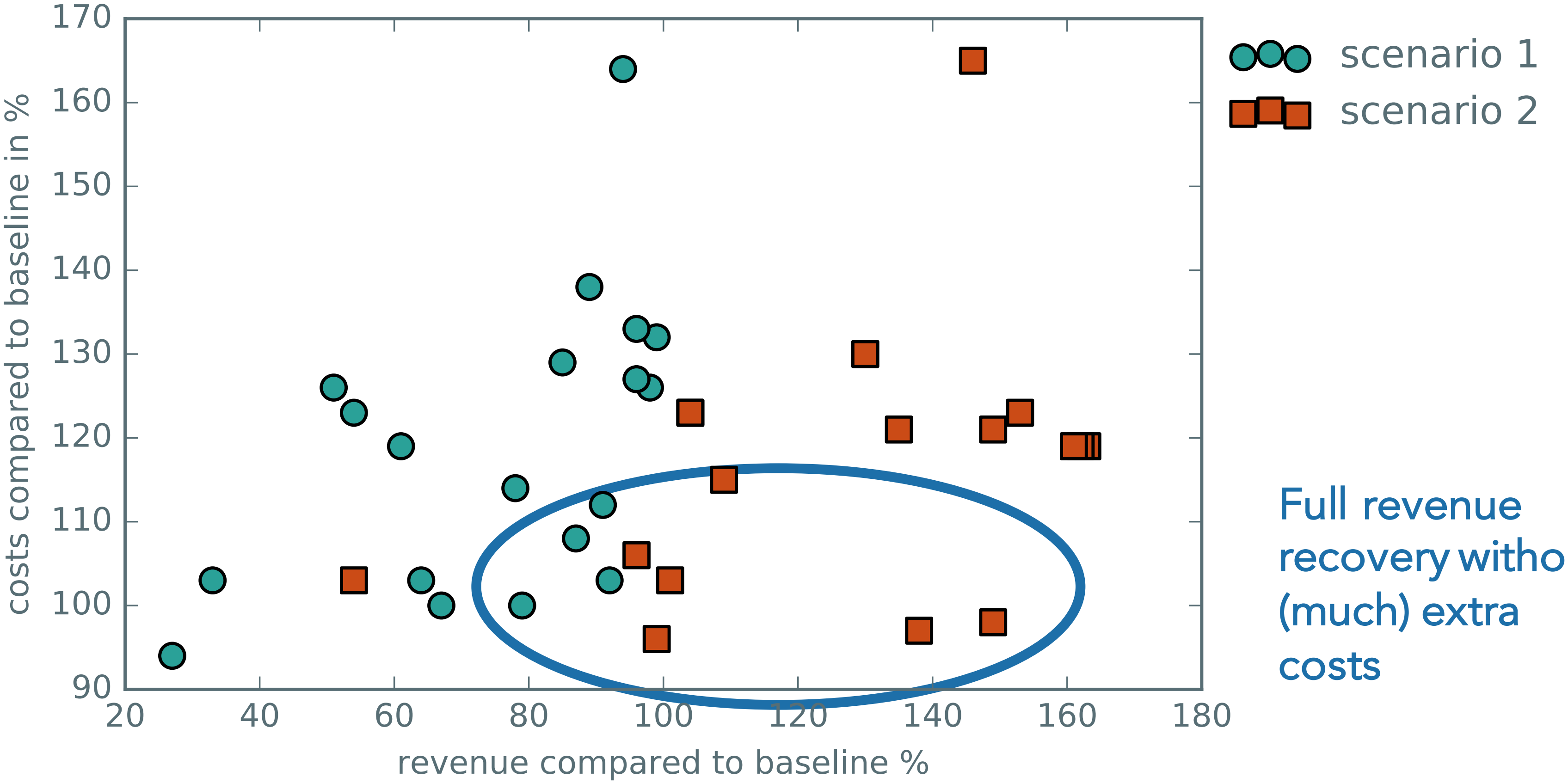


Solution cost and revenue recovery



Revenue gain!

Solution cost and revenue recovery



Full revenue recovery without (much) extra costs

Conclusion:

- Visualisations can help with analyzing and understanding (DDoS) attacks.
- To defend, People choose the naïve options based on:
  - Their prior experience
  - What information is presented
- More changes/actions don’t necessarily result in a better solution to an attack
- Actions are limited by the functions the underlying SDI exposes.

Future work

- We need to look at other variables to determine effectiveness of a solution besides cost and revenue:
  - Time of implementation
  - Temporary impact on current or other solutions
- Calculate the optimal solution for current and future attack scenarios
- What functions can be provided by the SDI to assist in enhancing the security of the overlay network.

UNIVERSITY OF AMSTERDAM

SAE

https://sarnet.uvalight.net/

TNO innovation for life

NWO
Netherlands Organisation for Scientific Research

COMMIT/

AIRFRANCE KLM

ciena