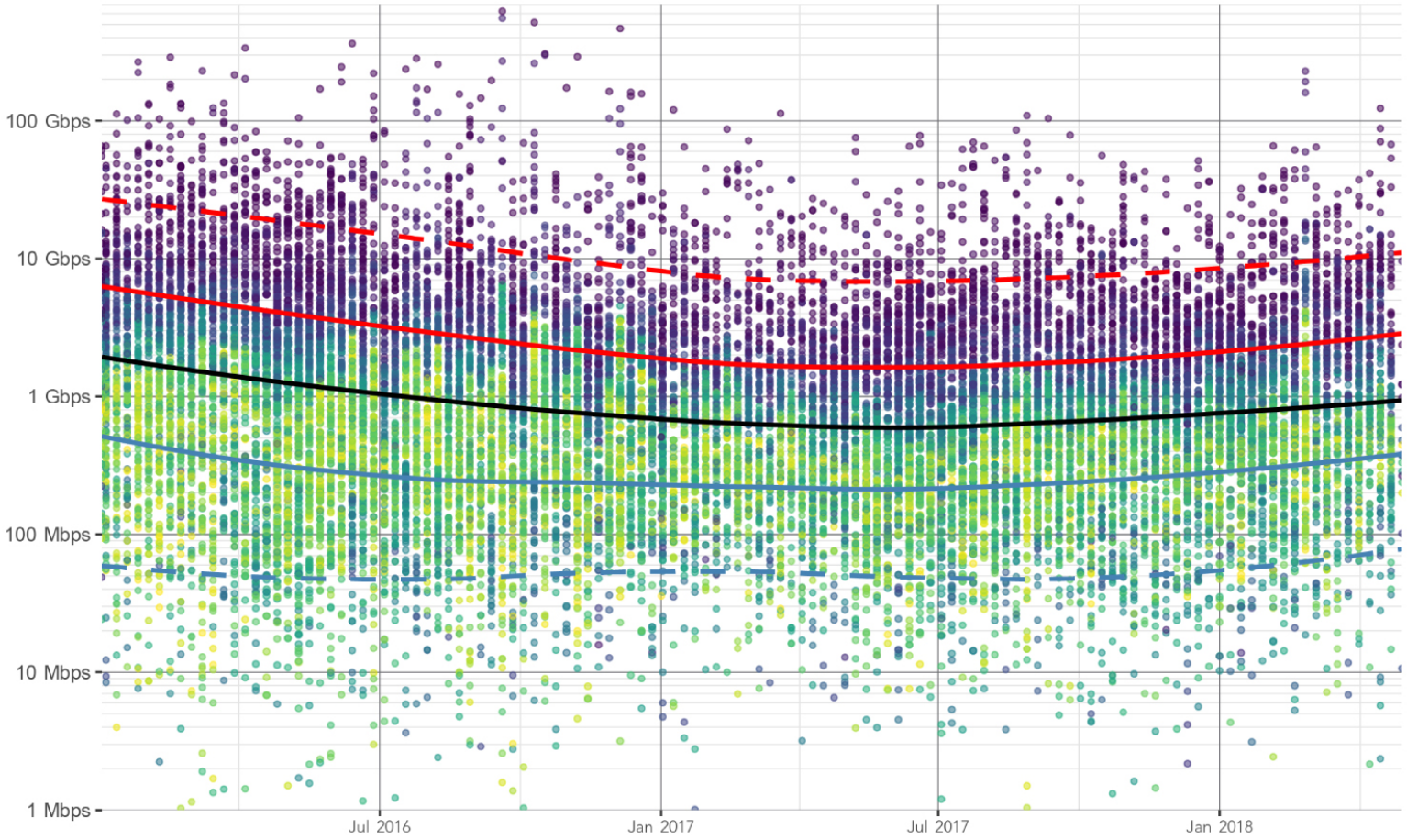
When DDoS Attacks meet Traffic Engineering

Christos Nikolaou

cn380@cam.ac.uk

http://www.cl.cam.ac.uk/~cn380/

Denial of Service Attacks – Attack Density

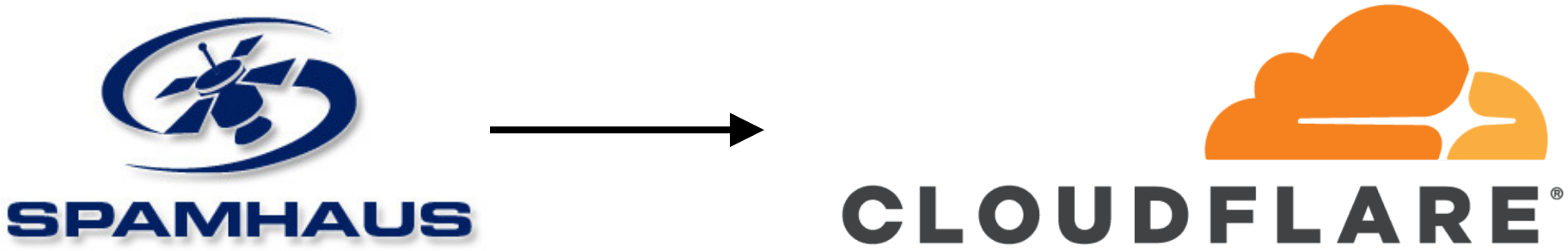



ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLIC
BIZ & IT —
Can a DDoS break the Internet?

https://arstechnica.com/information-technology/2013/04/can-a-ddos-break-the-internet-sure-just-not-all-of-it/2/

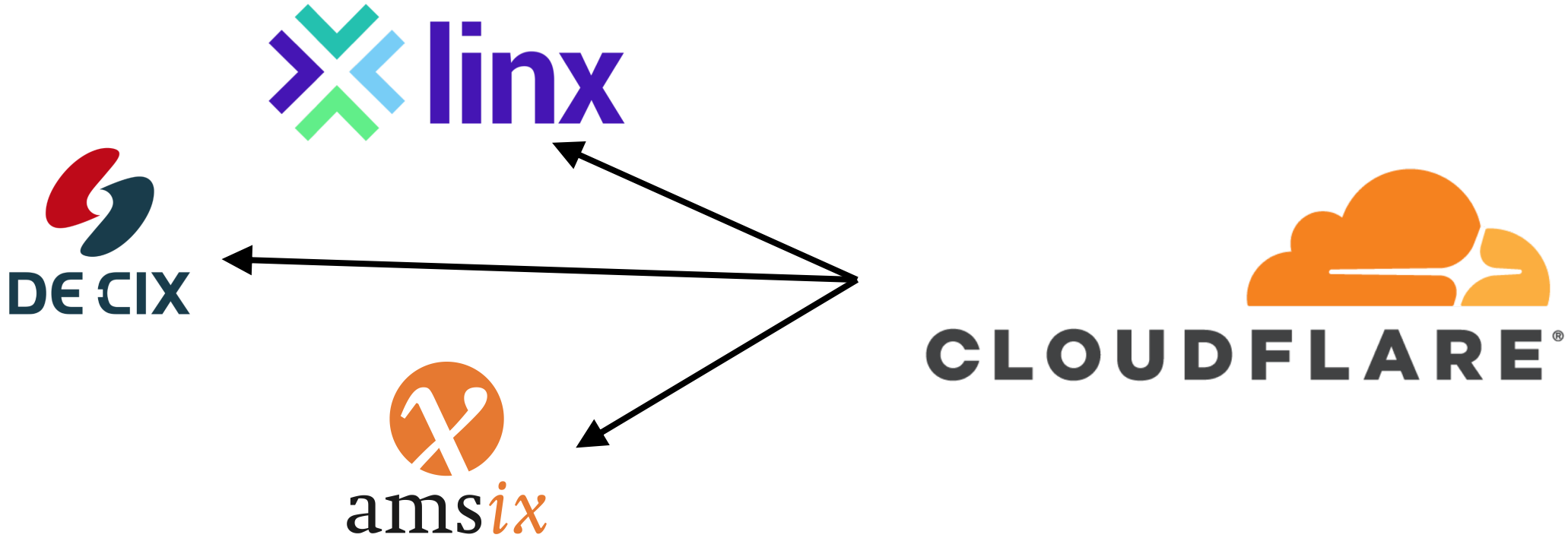
The Spamhause Attack (2013) – 10Gbps

The Spamhause Attack (2013) – 90Gbps



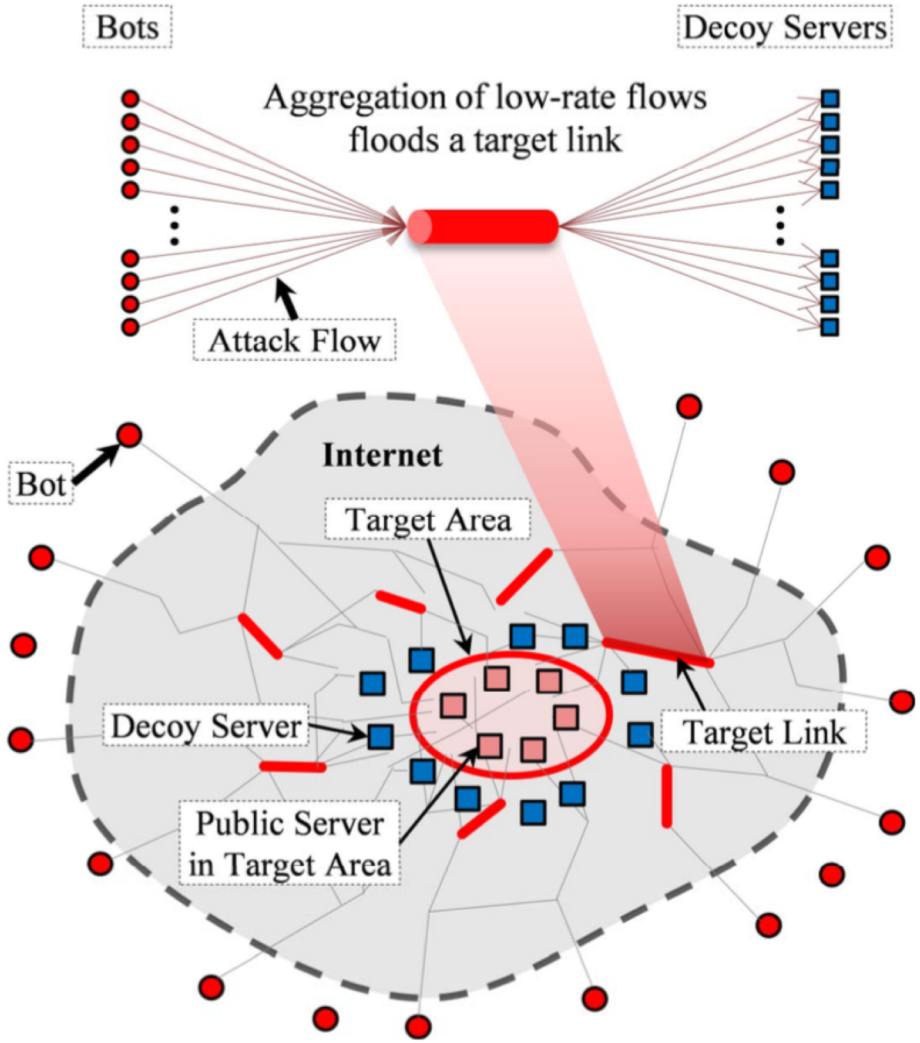
https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

The Spamhause Attack (2013) – 300Gbps



https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

The Crossfire Attack – Overview



- Bots send legitimate-looking traffic to a set of public webservers
- The traffic concentrates on specific links
- Effectively disconnects the real target

Kang, M.S., Lee, S.B. and Gligor, V.D., 2013, May. The crossfire attack. In *Security and Privacy (SP), 2013 IEEE Symposium on* (pp. 127-141). IEEE.

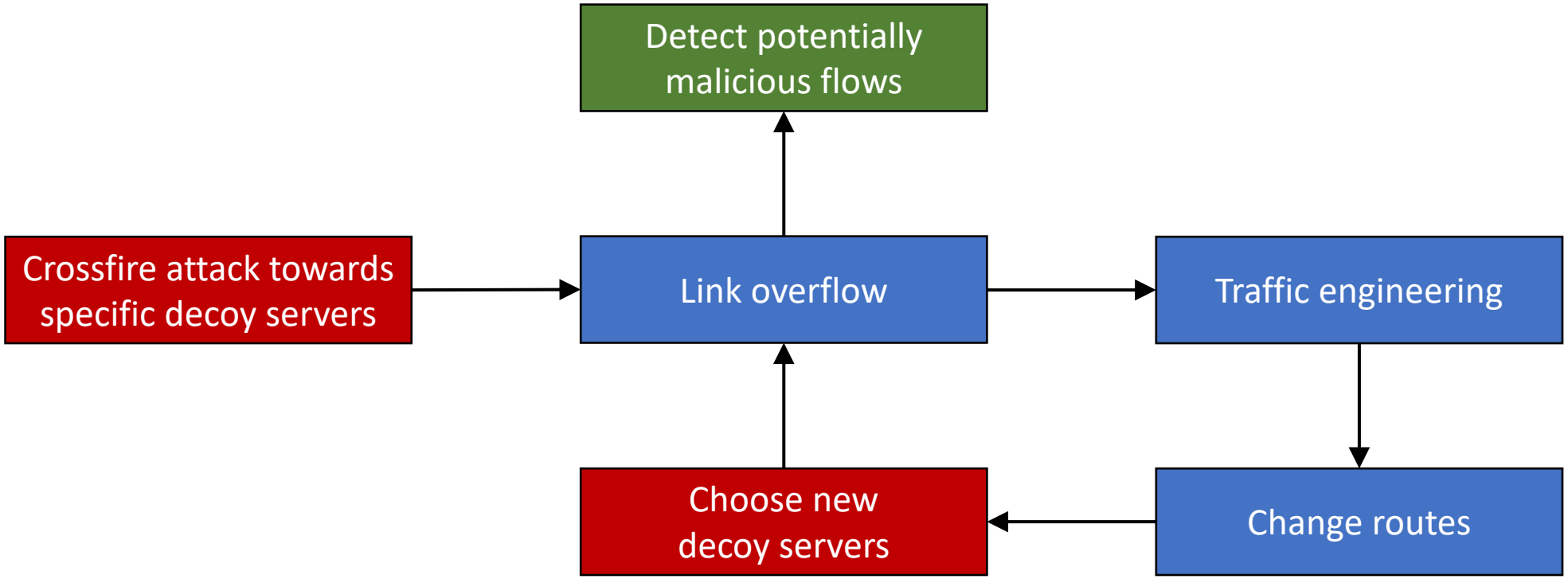
The Crossfire Attack – Why it Matters?

- Detection is hard:
  - affected host/area doesn't receive any traffic
  - routers receive only low-intensity legitimate-looking traffic
  - no IP-spoofing is required

- Persistency:
  - Bots can vary
  - Public servers (decoys) can change
  - The target links can change

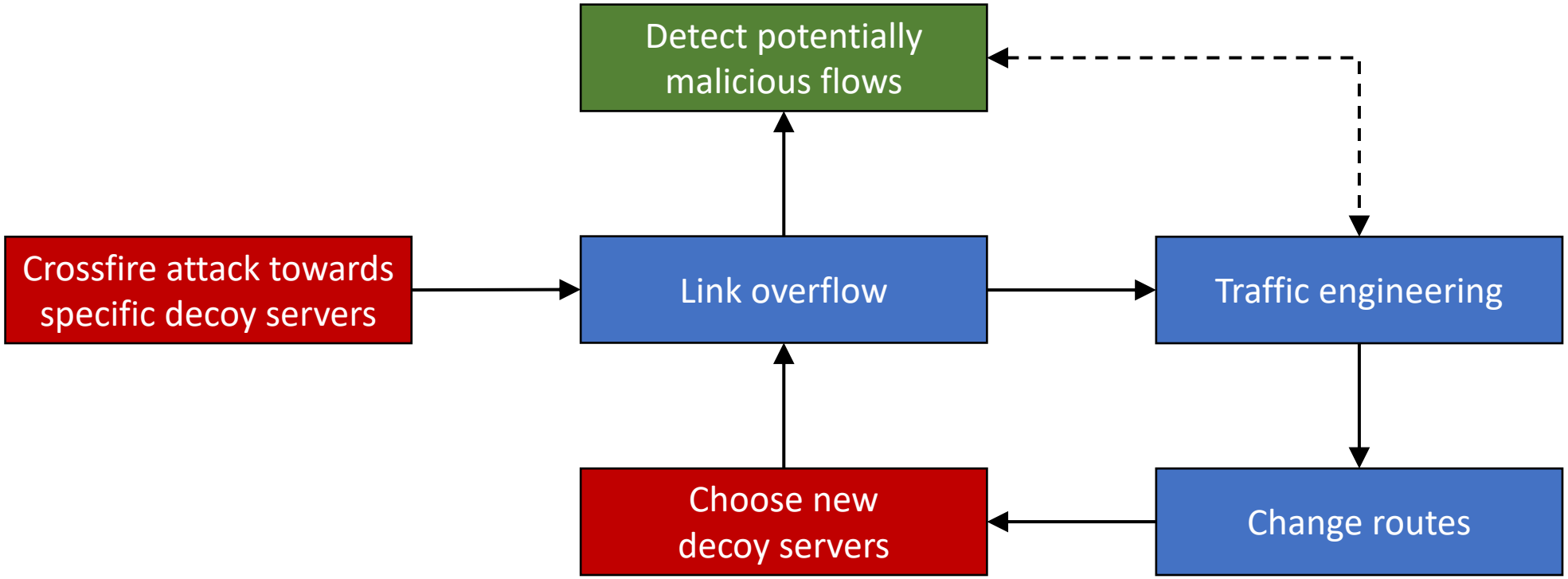
Kang, M.S., Lee, S.B. and Gligor, V.D., 2013, May. The crossfire attack. In *Security and Privacy (SP), 2013 IEEE Symposium on* (pp. 127-141). IEEE.

Link-flood Attacks and Traffic Engineering



Gkounis, D., Kotronis, V., Liaskos, C. and Dimitropoulos, X., 2016. On the interplay of link-flooding attacks and traffic engineering. *ACM SIGCOMM Computer Communication Review*, *46*(2), pp.5-11

Link-flood-aware Traffic Engineering



Gkounis, D., Kotronis, V., Liaskos, C. and Dimitropoulos, X., 2016. On the interplay of link-flooding attacks and traffic engineering. *ACM SIGCOMM Computer Communication Review*, *46*(2), pp.5-11

How do Traffic Engineering Algorithms behave when under DDoS attacks?

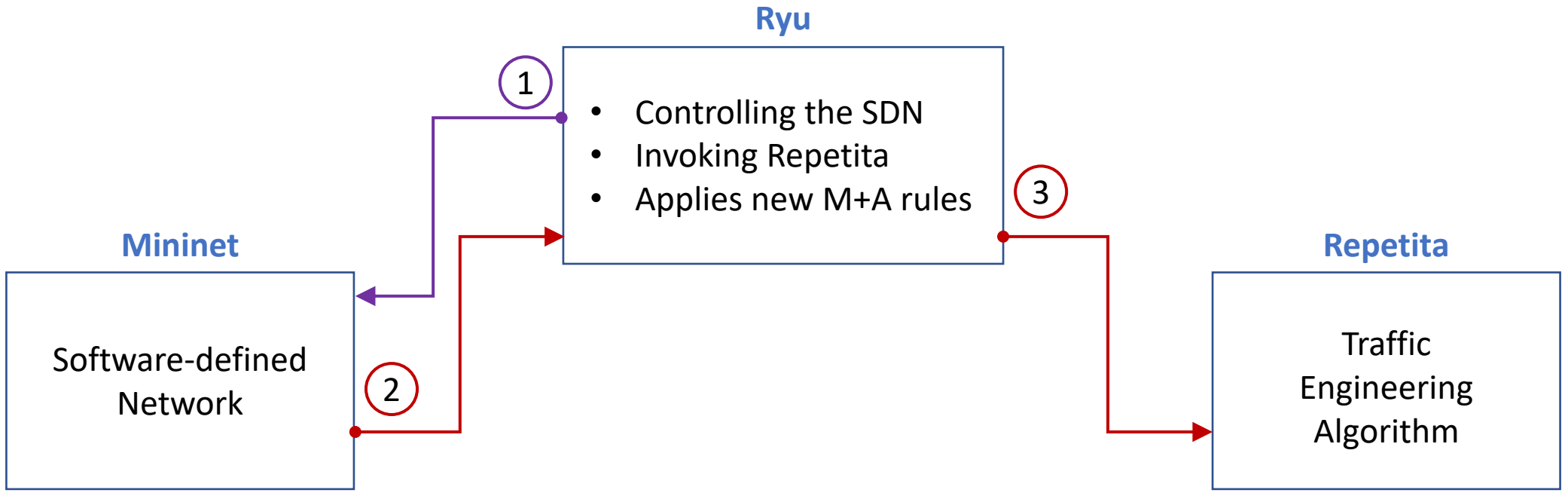
How to do it…

- Use a network simulator => Mininet
  - Written in Python
  - Easy-to-use: developed for teaching software defined networking
  - Controller-independent
  - http://mininet.org/

- Implement traffic engineering (TE) algorithms…
  - …or use Repetita
  - https://github.com/svissicchio/Repetita

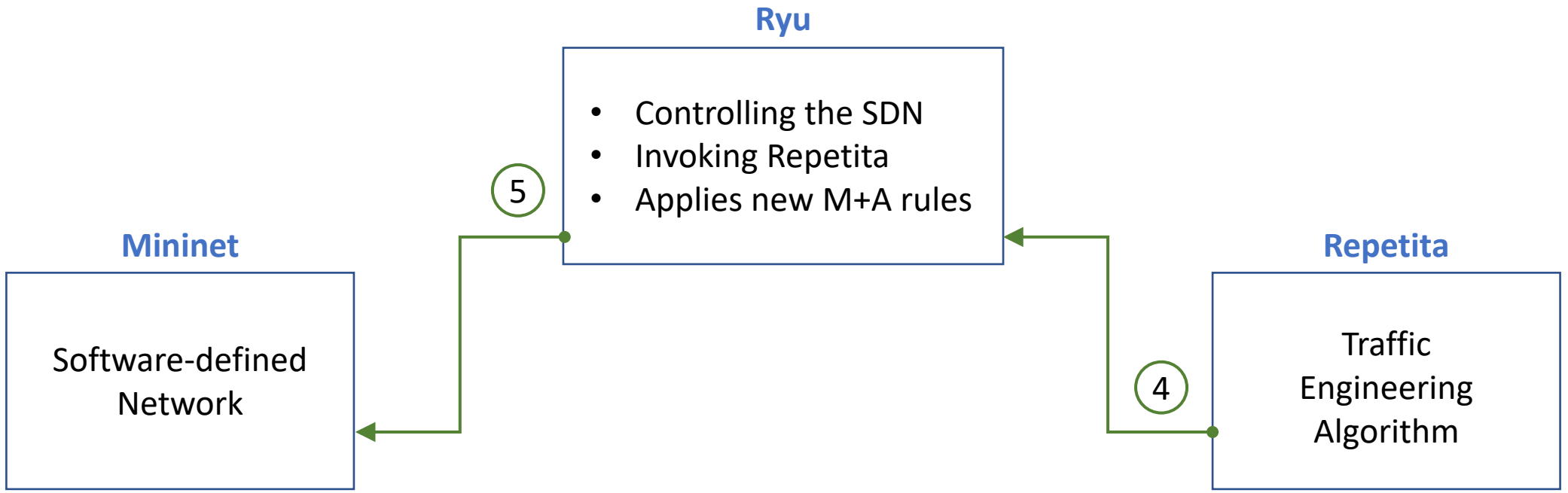
Gay, S., Schaus, P. and Vissicchio, S., 2017. REPETITA: Repeatable Experiments for Performance Evaluation of Traffic-Engineering Algorithms. *arXiv preprint arXiv:1710.08665*.

A Tool for TE dynamics – Network Measurements



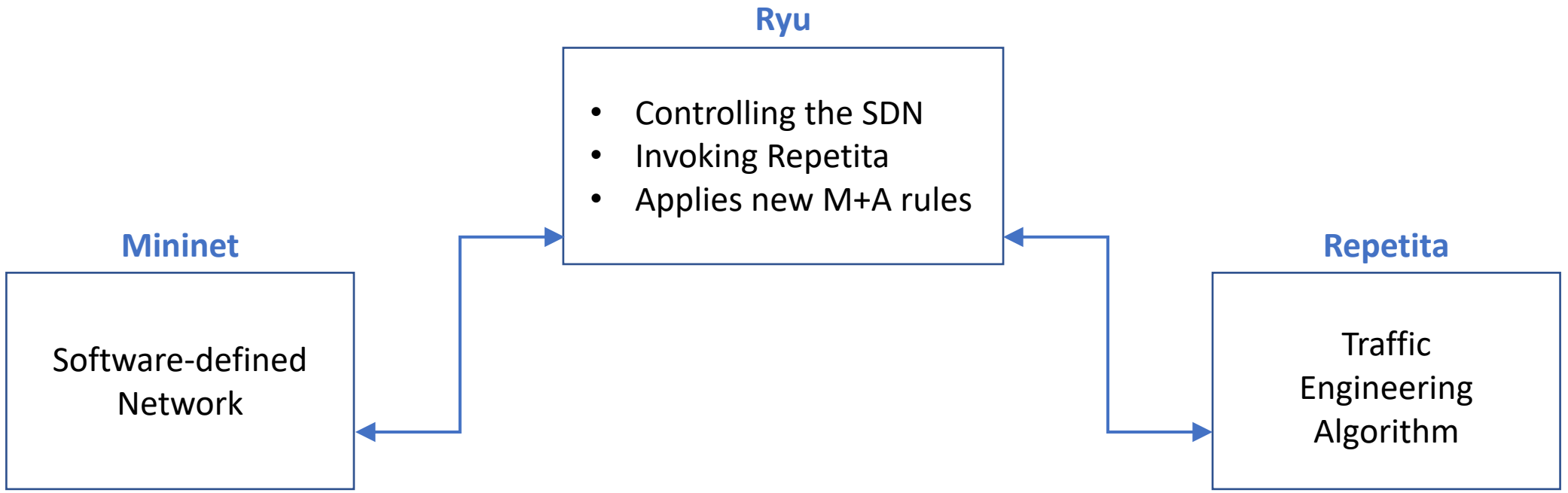
1: The controller asks for statistics of all the switches
2: Each switch send the statistics
3: Ryu calculates the traffic matrix and invokes the TE algorithm

A Tool for TE dynamics – Change Routing



4: Repetita calculates the new paths
5: Ryu parses the new data and ”extracts” the new M+A rules which then sends to the switches

A Tool for TE dynamics – Loop

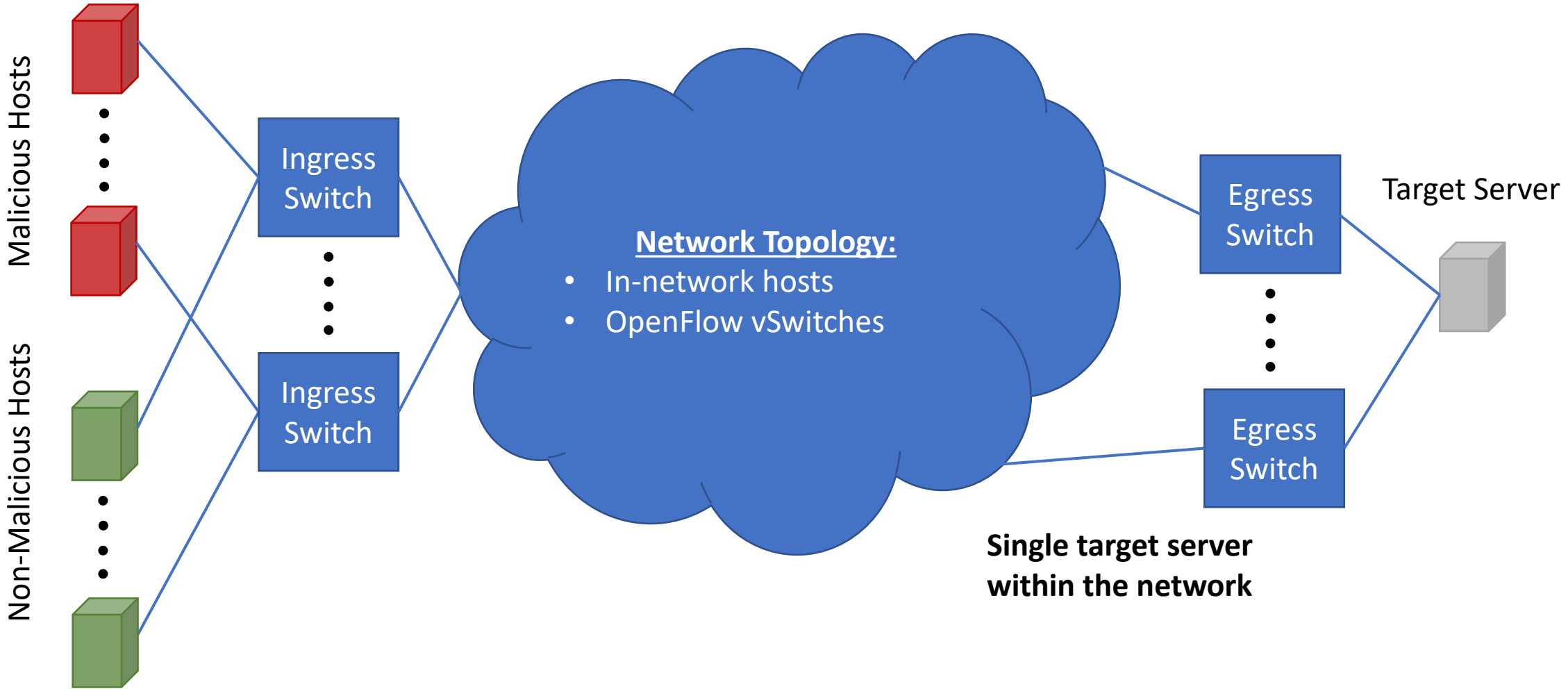


Traffic in the SDN changes over time and different scenarios can be simulated.

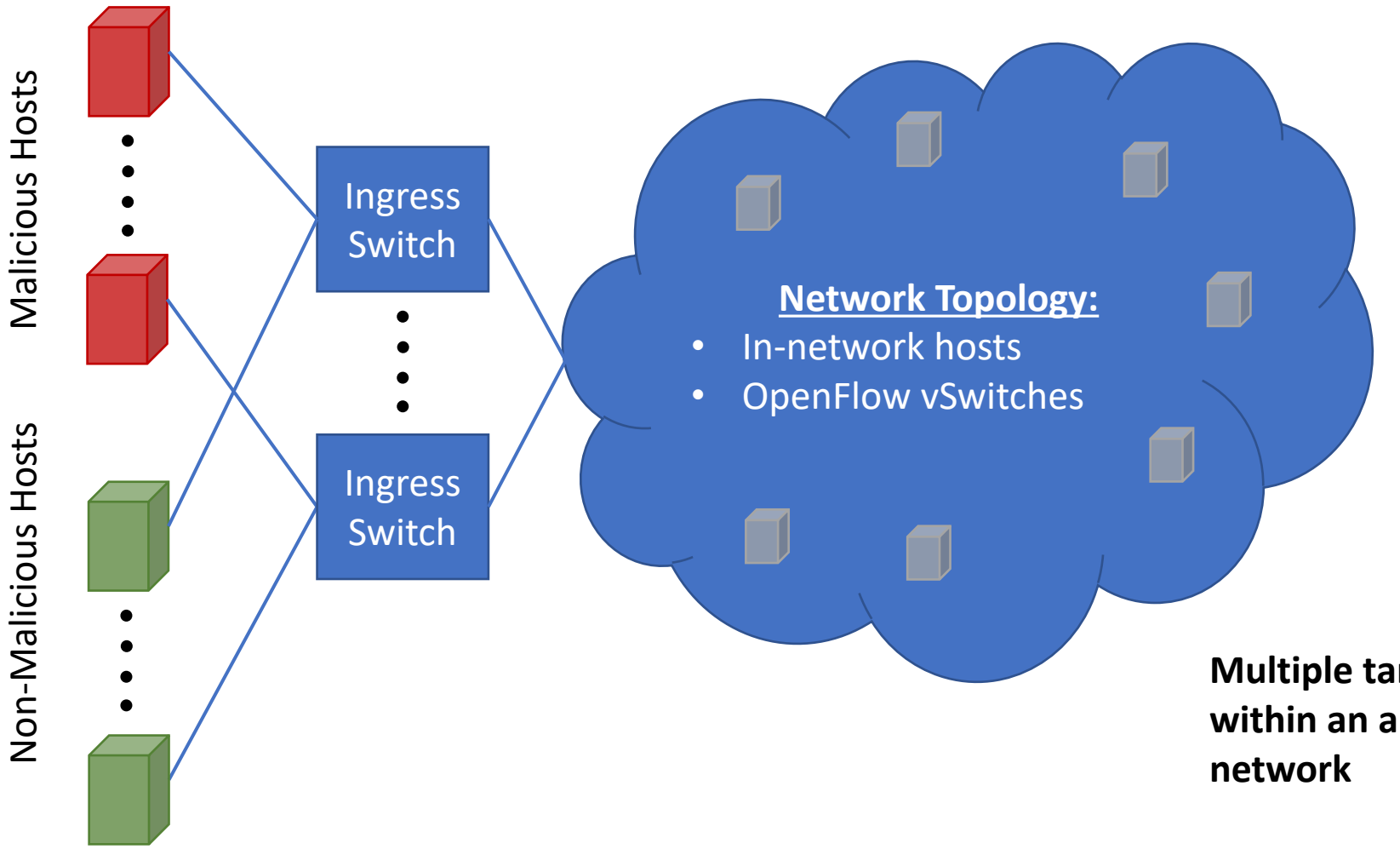
A Tool for TE dynamics – Why?

- Evaluate and compare different TE algorithms
- Reproducibility
- Different use-cases
  - Simulate different types of DDoS attacks
  - Simulate other network phenomena as well – i.e. heavy flows
- Develop new TE algorithms

Current Overall Topology



Optimal Topology



Multiple target servers within an area of the network

Future Work – Effectiveness of TE

- Under link-flood attacks
- Under other types of DDoS attacks
- Other network management tasks (such as heavy hitters)
- More complex scenarios:
  - Malicious hosts inside the network
  - More target servers

Team Members

Gianni Antichi – QMUL and UCAM

Stefano Vissicchio - UCL

Andrew W. Moore - UCAM

Thanks!