Lancaster University

Bang! And the DDoS is gone!*

School of Computing and Communications

NETLAB
NETWORKED SYSTEMS RESEARCH LABORATORY
University of Glasgow | School of Computing Science

Steven Simpson
Noor Shirazi
Angelos Marnerides
David Hutchison

Simon Jouet
Dimitris Pezaros

A Situation-Aware Information Infrastructure
(EPSRC EP/L026015/1)

*optimism

Lancaster University

Ping! And the Good Guys get through!

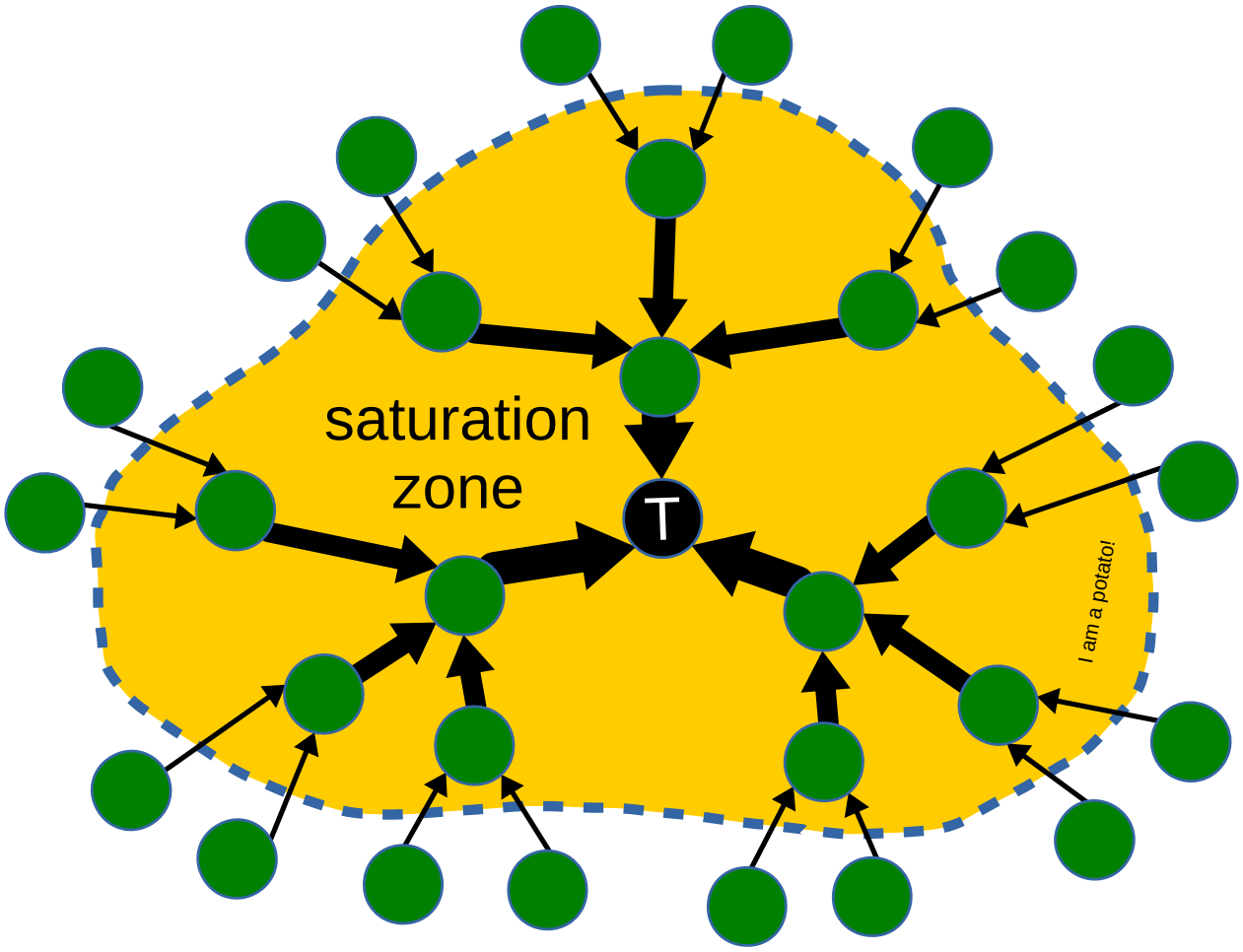
Lancaster University

Progress report: Antidose

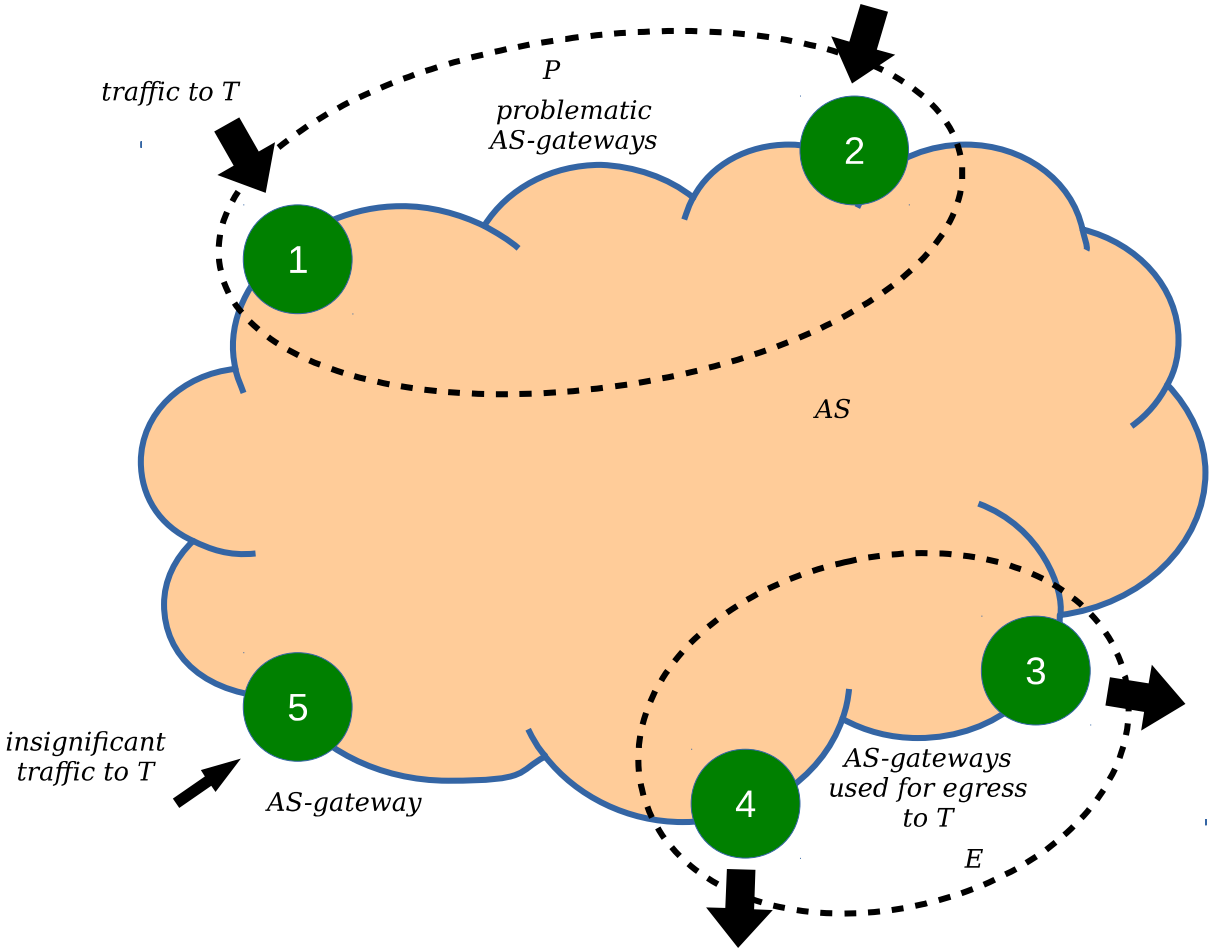
- Design updates
  - New client/target agents
  - New filter flow chart
- Implementation
  - Demonstration
  - False-positive rate
- Issues, choices

Lancaster University

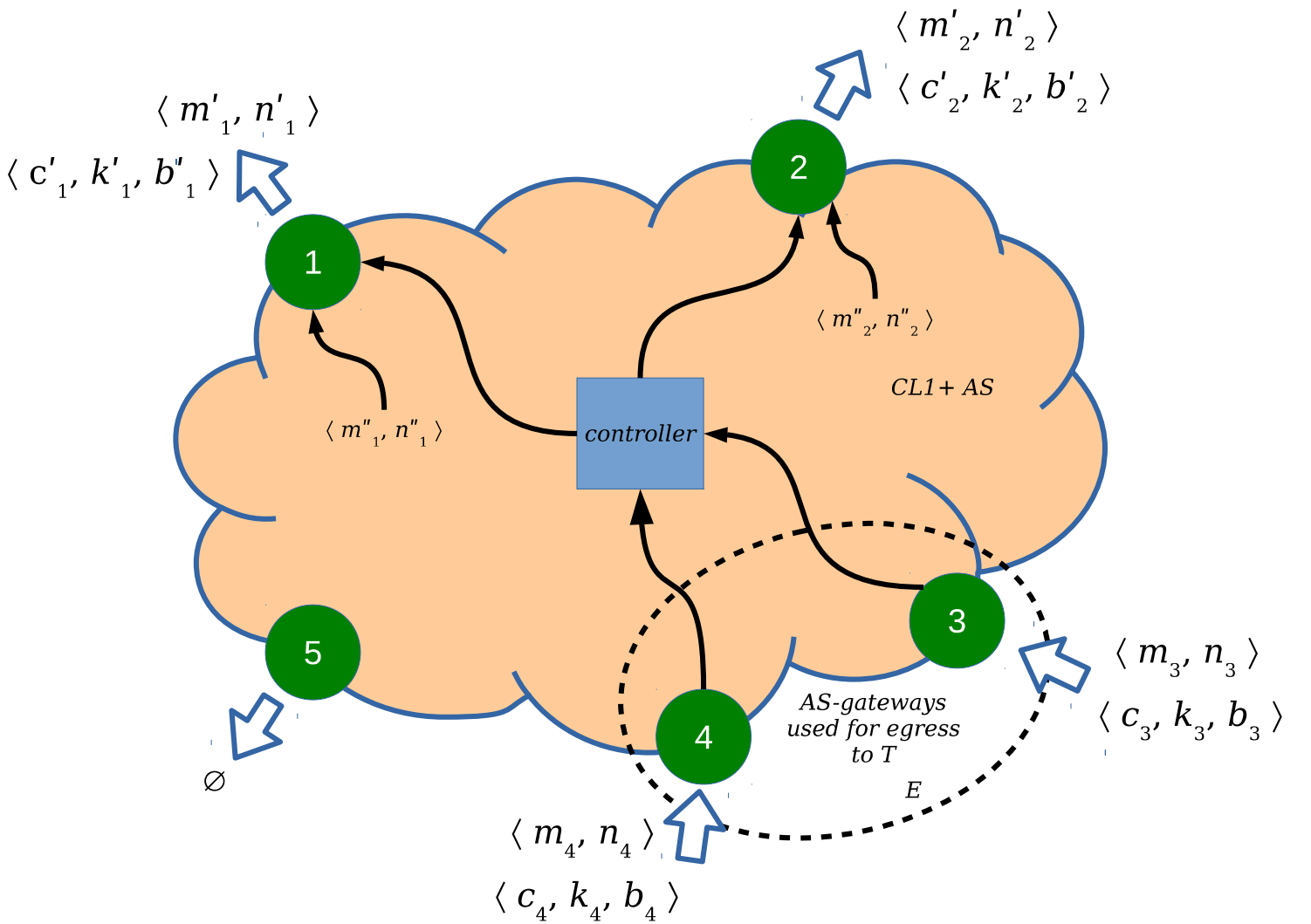
Saturation zone



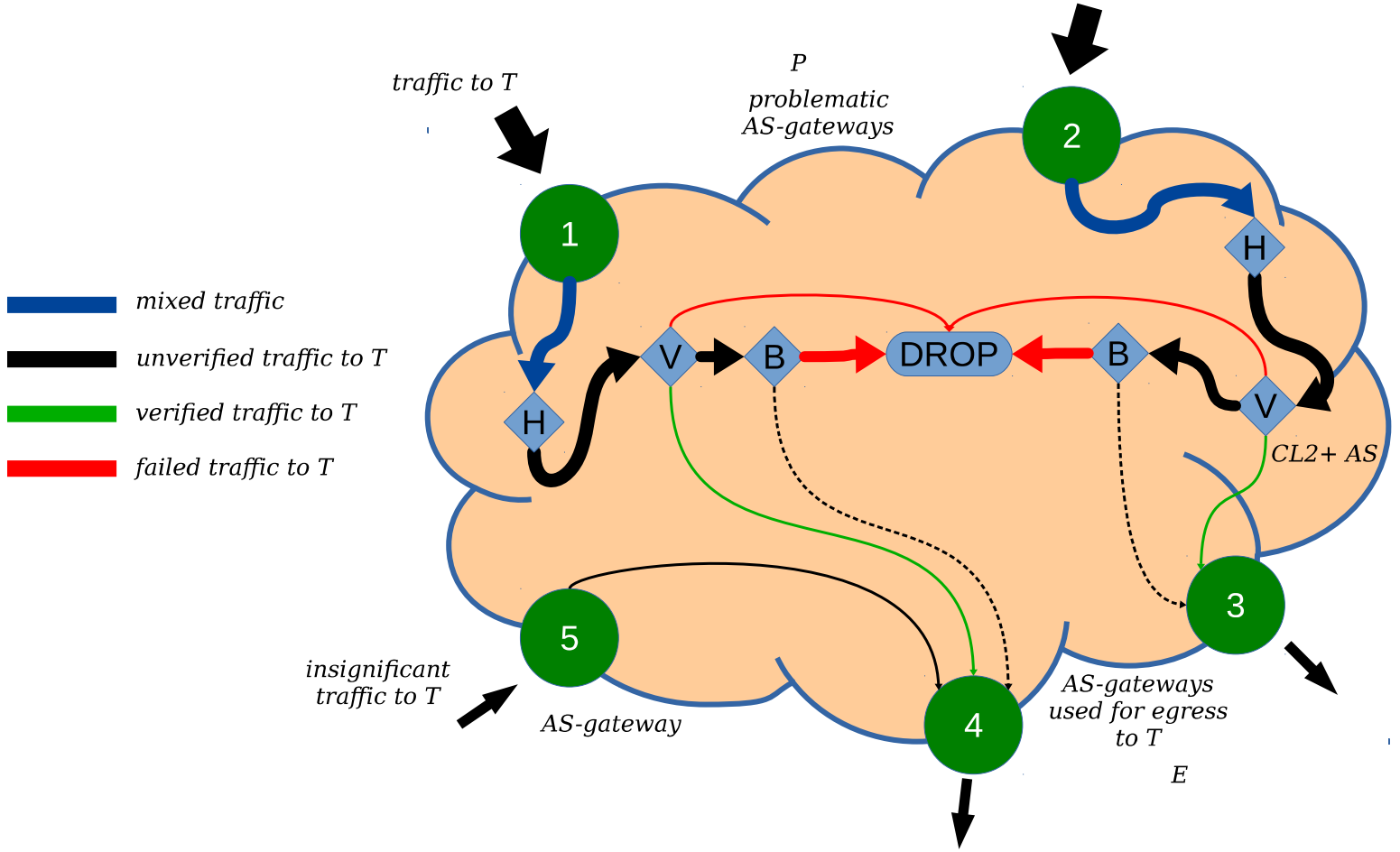
AS categorization of gateways



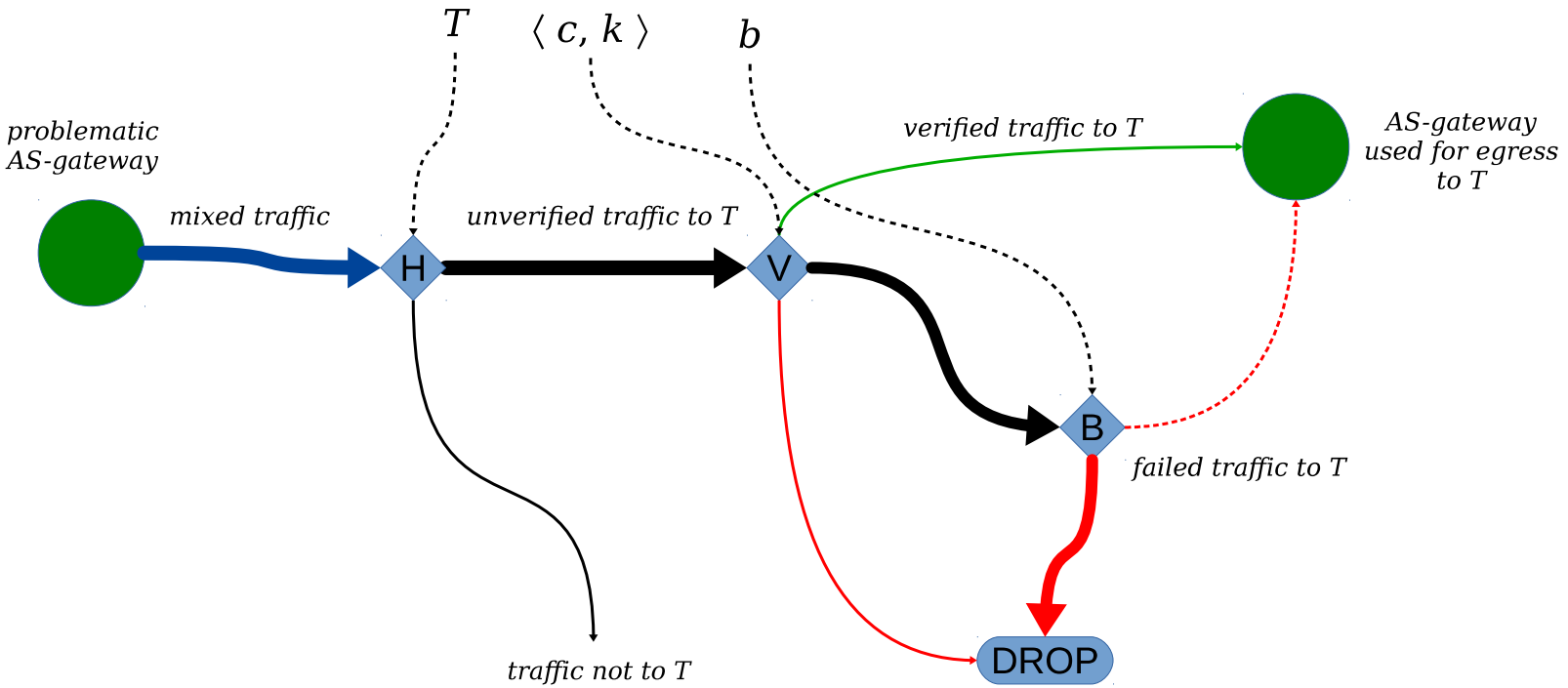
AS information flow



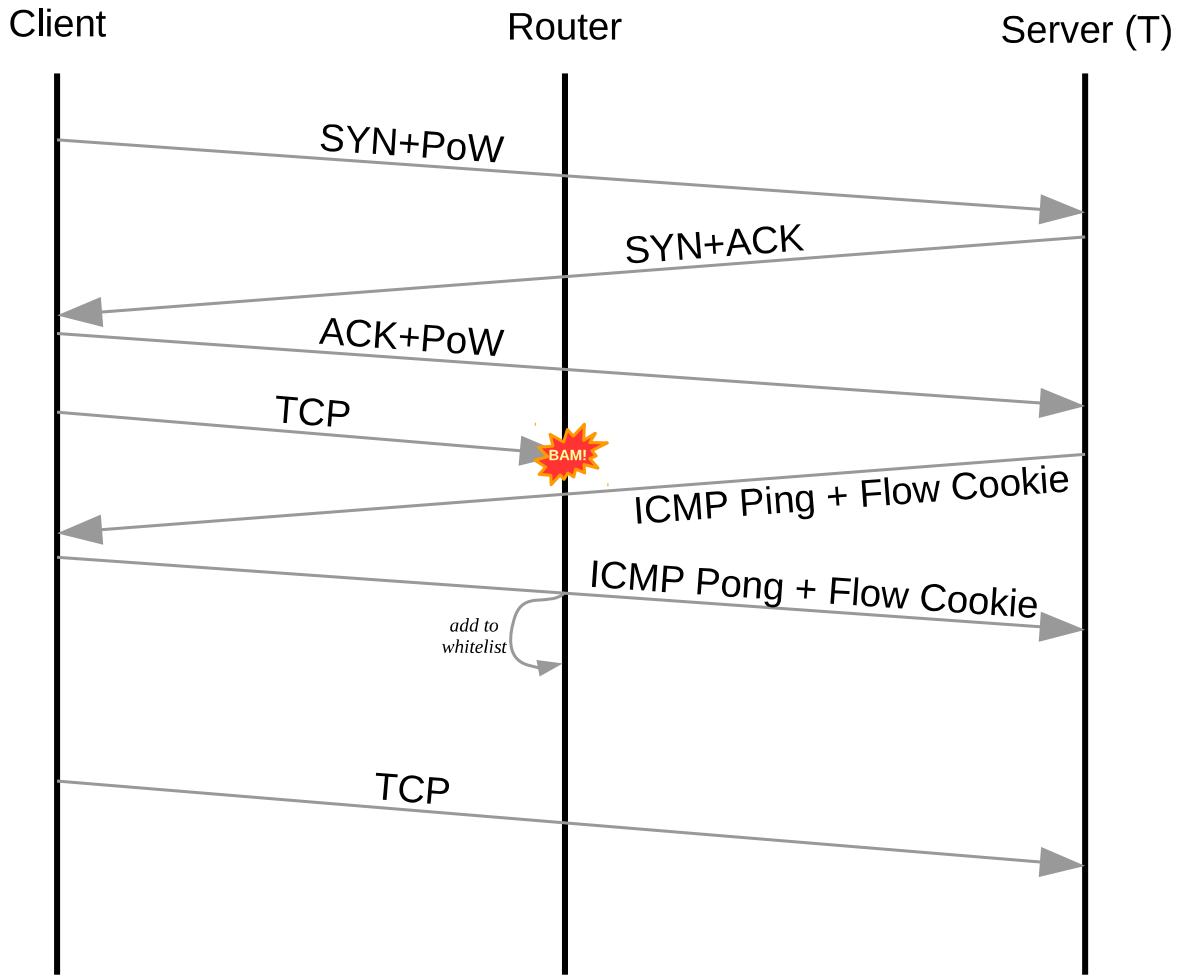
Filtering in AS



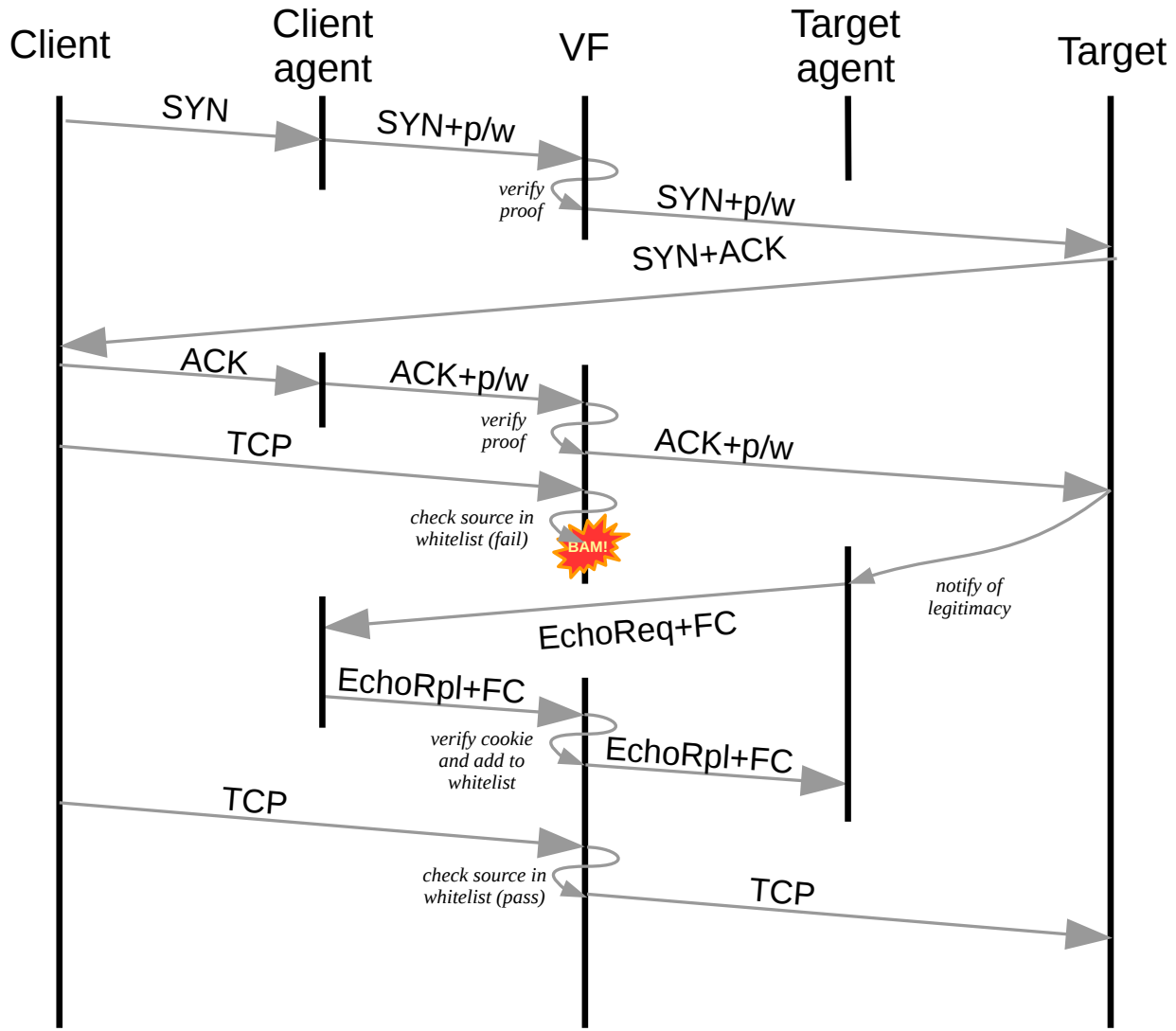
Filtering in AS



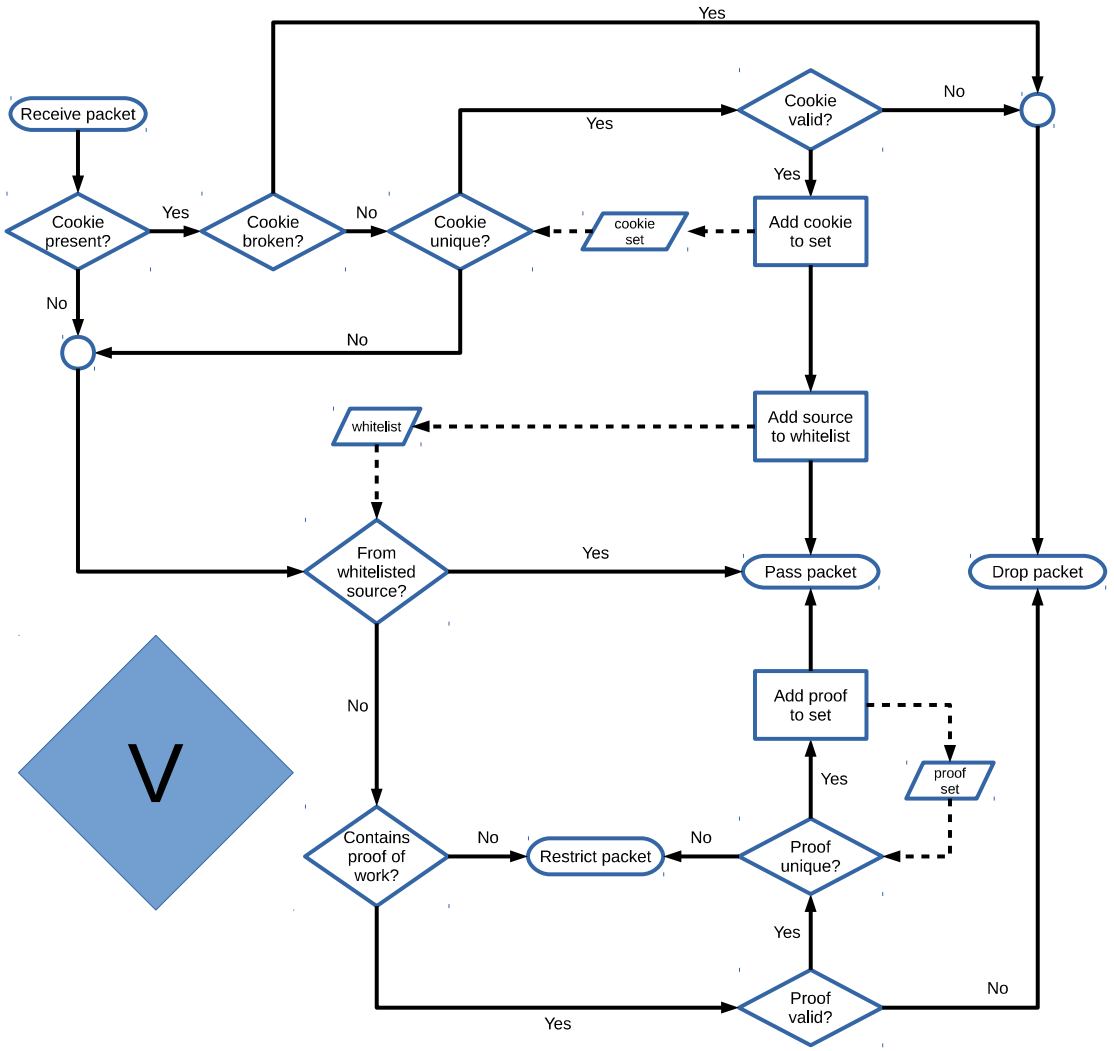
Proof-of-work & flow cookies (old)



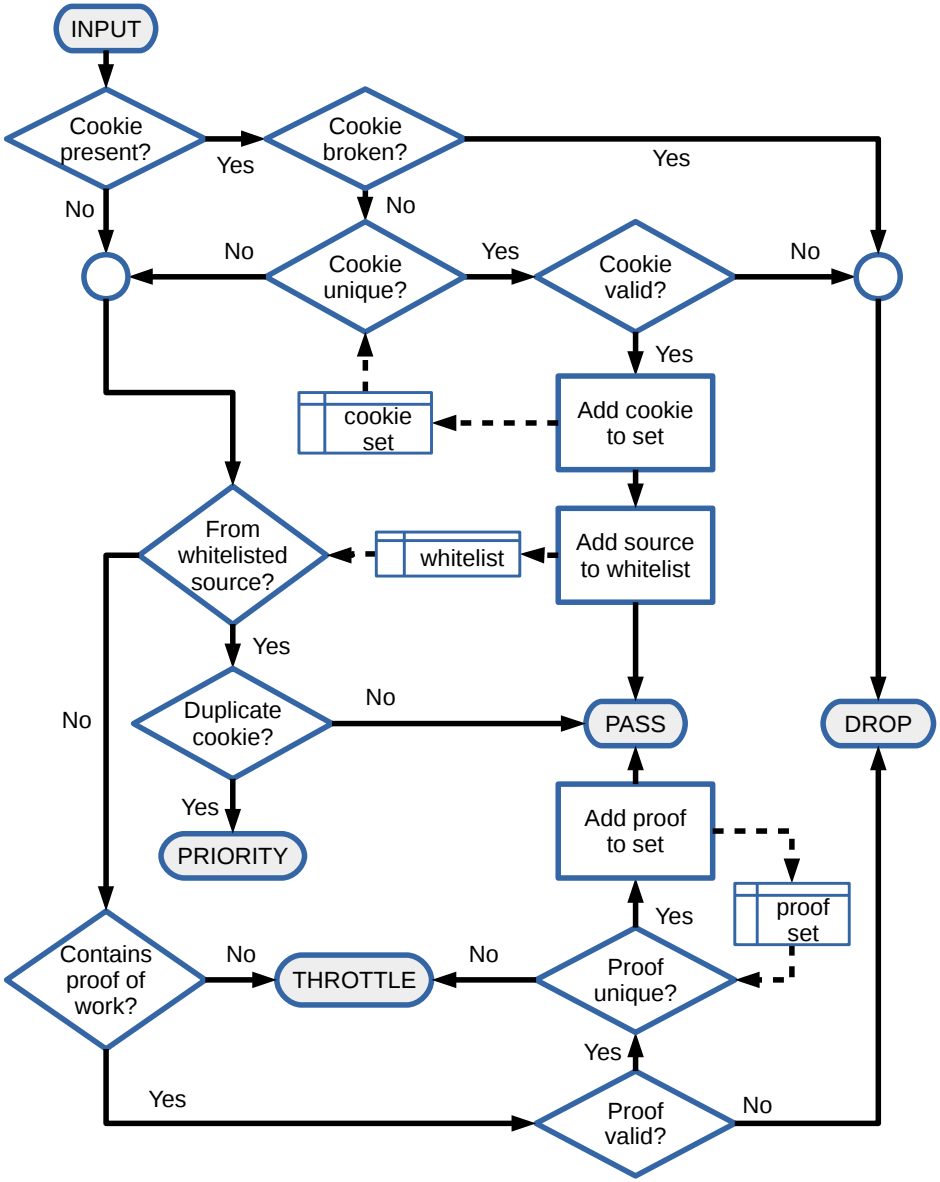
Proof-of-work & flow cookies (new)



Verification filter (old)



Verification filter (new)



Lancaster University

Verification filter

- Check for cookie before whitelist
  - Need to see refreshing cookies
- Check whitelist before proofs-of-work
  - PoW not useful to us if already whitelisted
  - Still useful downstream
- Counter-attacks
  - Share valid cookies and proofs (requires spoofing)
- New attack vectors
  - Flood with invalid cookies
    - Requires asymmetric signature verification per packet
  - Flood with invalid proofs
    - Requires hash computation per packet

Lancaster University

Signature verification in hardware

- BPFabric implementation
  - Translate from C to eBPF
    - Restricted
      - No dynamic memory
    - Push complex functions to edge of EE
      - Hashing
      - Signature verification
  - Validate on software switches
  - Switch between alternative BPFabric EEs
    - DPDK-assisted switch
    - Future NetFPGA implementation of BPFabric?
    - Operational portability?

Lancaster University

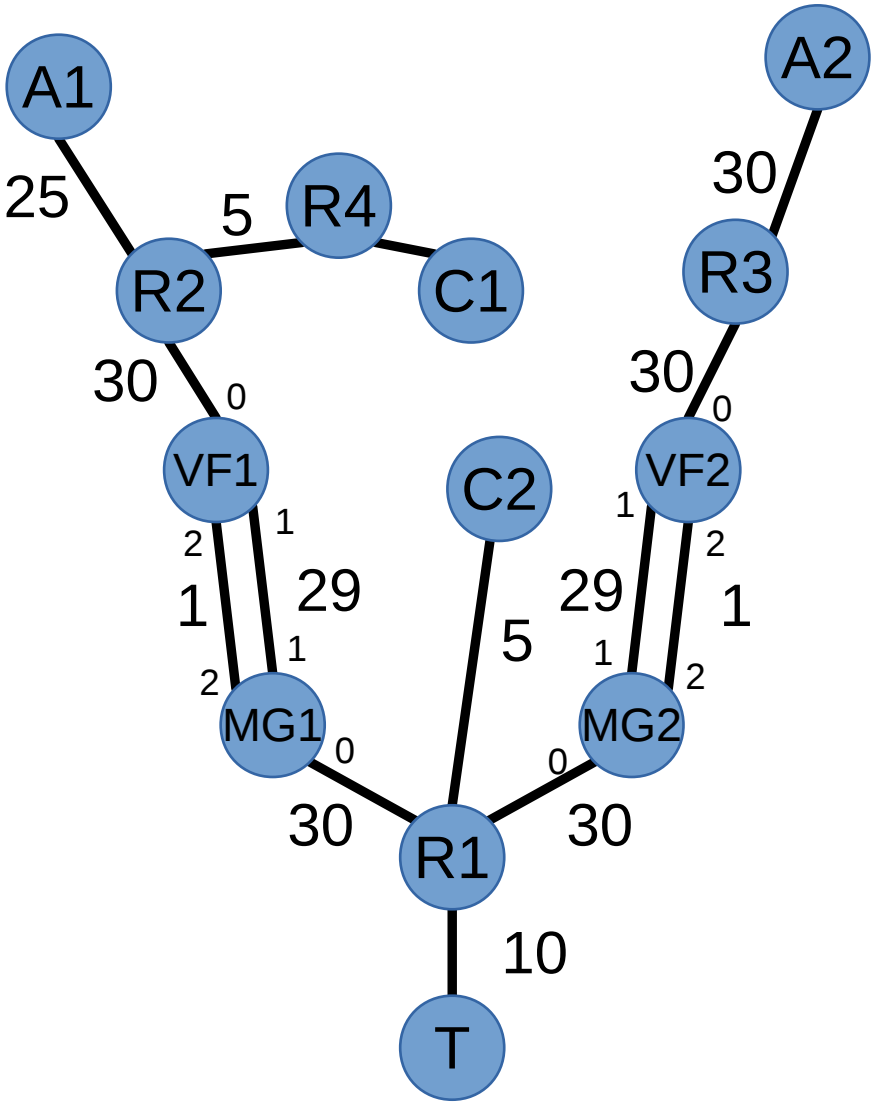
Issues

- eBPF implementation
  - Big structures out of range of addressing modes
  - Inappropriate kernel stack limit
  - Clang implicit memcpy
  - Hard to debug
- Data structures
  - Cookie set: Bloom filter, m=64k, n=10000, k=5
  - Proof set: Bloom filter, m=64k, n=10000, k=5
  - Whitelist: 4-bit counting Bloom filter, m=128k, n=10000, k=9

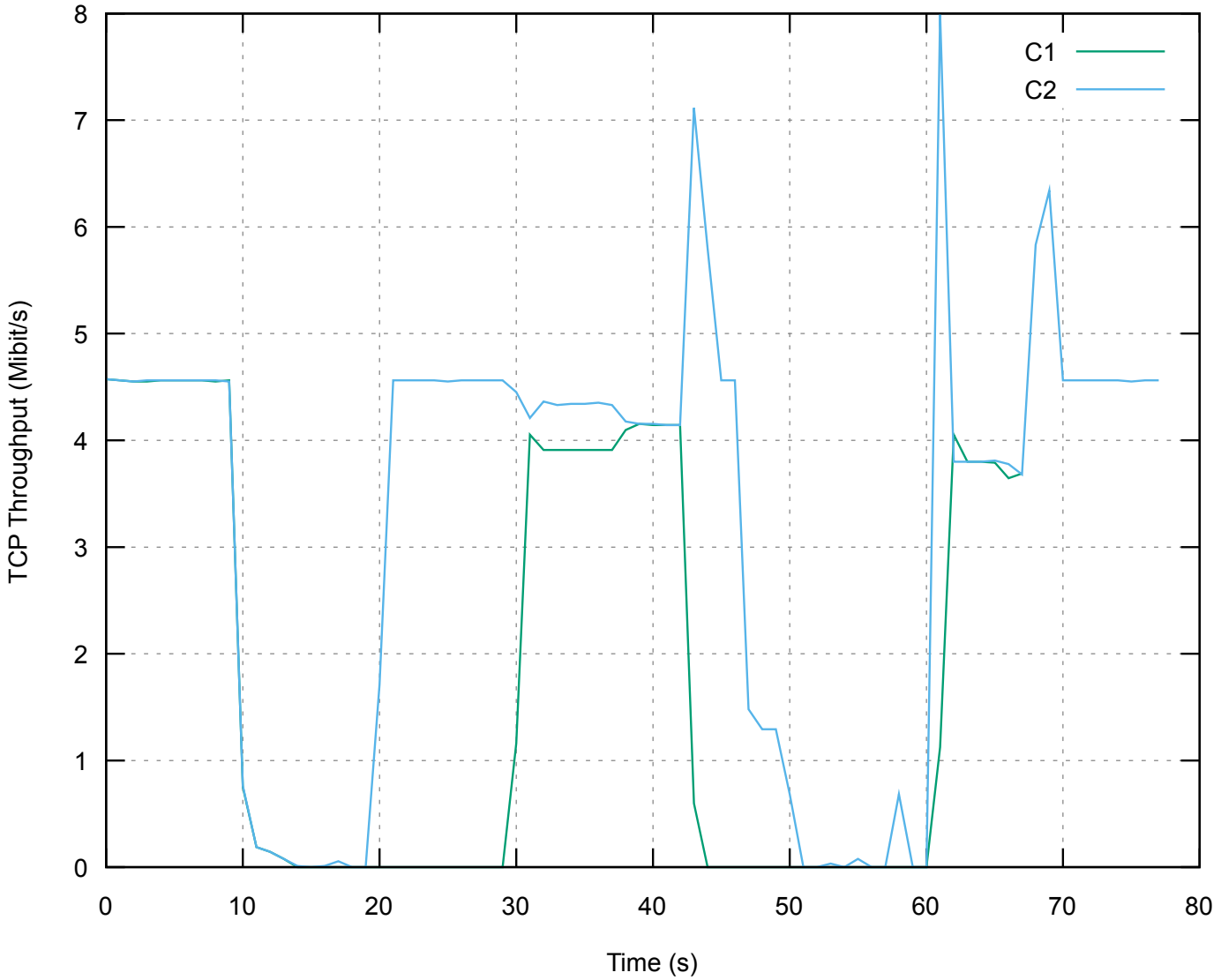
Lancaster University

Evaluation network

- Mininet topology
- BPFabric softswitches
- R1-R4: learningswitch.o
- VF1/2: simfilter.o
- MG1/2: merger.o

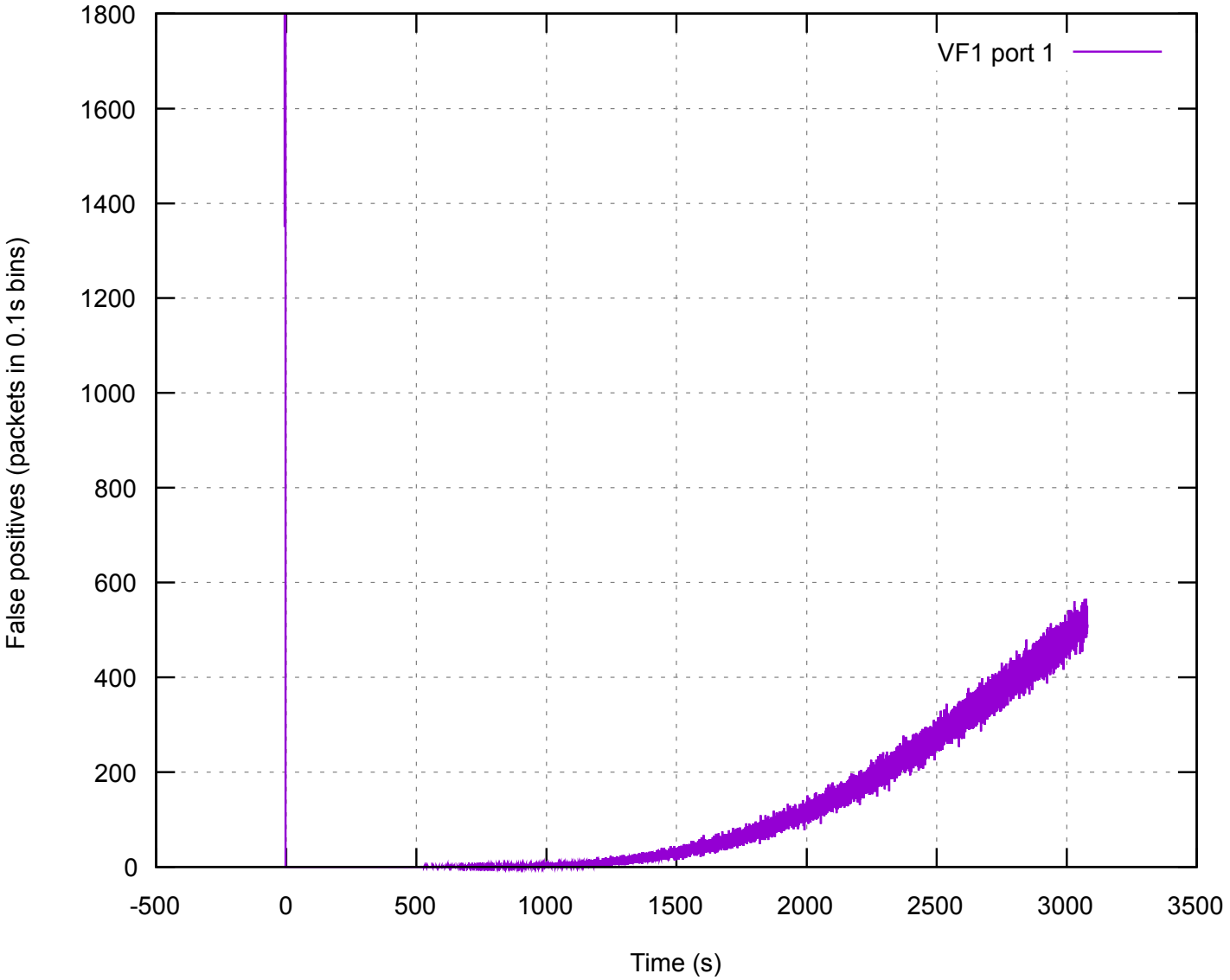


Demonstration



10	A1 starts
18	VF1 enabled
25	T cookie to C1
47	A2 starts
52	T cookie to C1
58	VF2 enabled
78	Stop

False-positive measurement



Lancaster University

Outstanding questions

- How fast can we go?
  - In each EE; but on back burner – what does it mean?
- PoW parameter distribution
  - Can we avoid flooding the network with PoW parameters?
    - Restrict to areas with clients?
    - Find another distribution system?
- AS interaction up to saturation boundary
  - Piggyback on BGP?
  - Prioritized channels?
- What h/w-assisted functions can we expect in real environments?
  - Hashing?
  - Signature verification?
  - Can we use this application to drive the design of future h/w and SDN functionality?

Lancaster University

Thanks!
Hmm?