MULTOPS

A data-structure for bandwidth attack detection

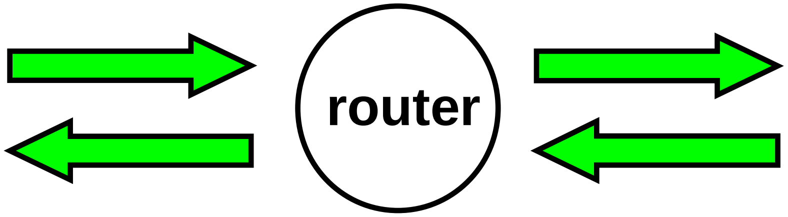
Thomer M. Gil
Vrije Universiteit, Amsterdam, Netherlands
MIT, Cambridge, MA, USA
`thomer@lcs.mit.edu`

Massimiliano Poletto
Mazu Networks, Inc., Cambridge, MA, USA
`maxp@mazunetworks.com`

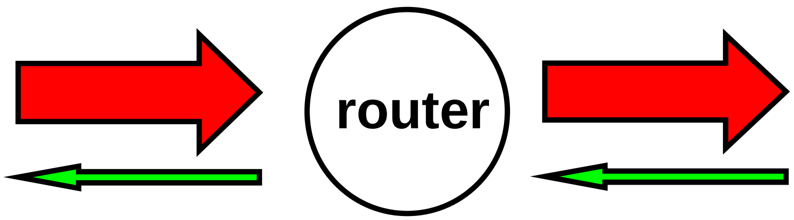
Bandwidth attacks

- Maliciously generated traffic congests links
- Traffic is typically ICMP, UDP, or TCP
- IP spoofing: fake IP source addresses
- Distribution: multiple hosts pounding one victim

MULTOPS heuristic



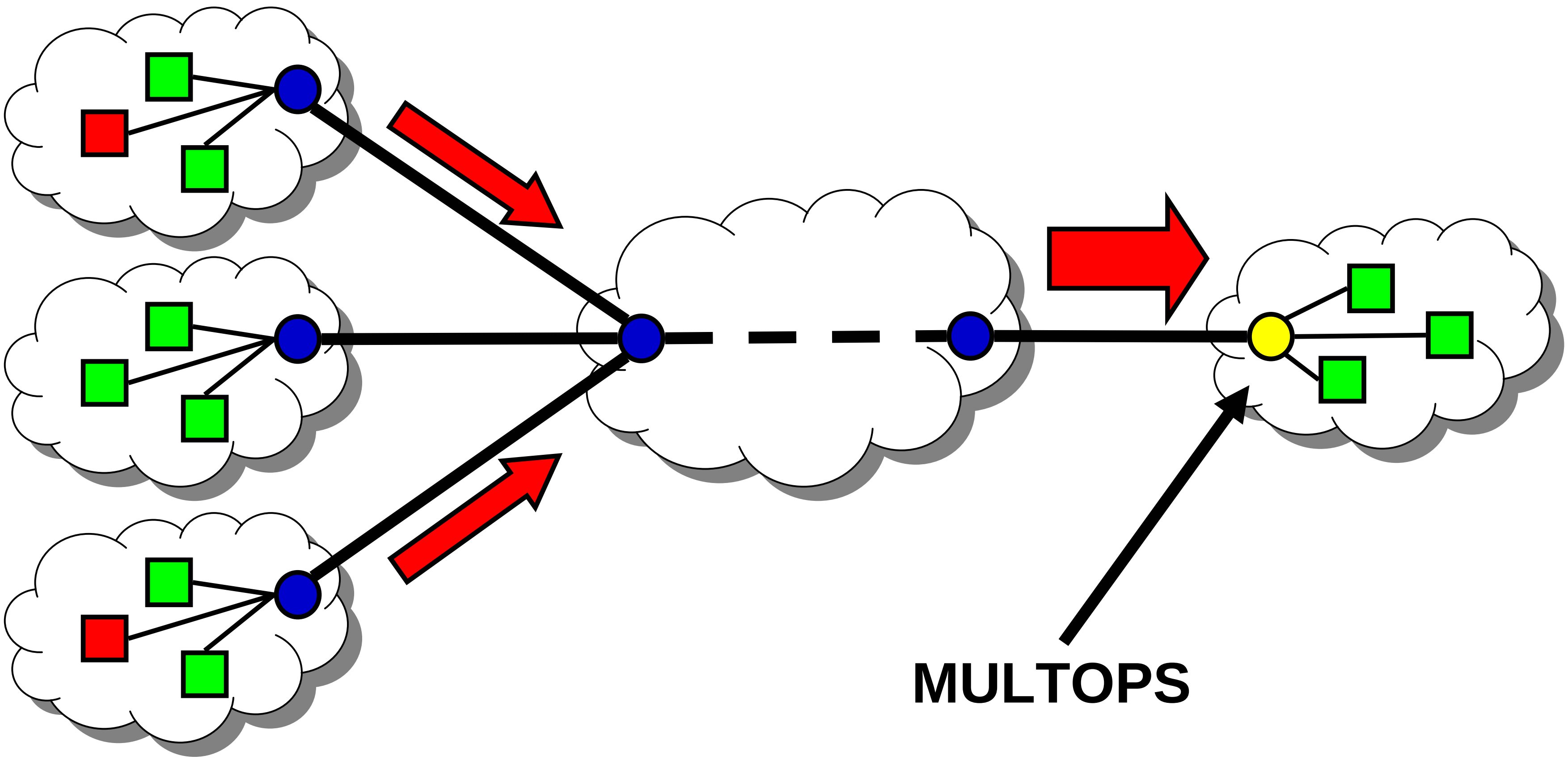
Normal: proportional packet rates



Attack: disproportional packet rates

Drop packets from sources sending disproportionate flows

Feb 2000: ICMP flood



+ MULTOPS identifies attackers' addresses
+ MULTOPS drops packets from those addresses

Implementation challenges

- Precise identification of malicious addresses
- Small memory footprint
- Minimal impact on forwarding performance

Naive data-structure

2^{32} entries

from-rate	to-rate	
2	0	0.0.0.0
...	...	
460	474	18.26.4.9
2,450	189	18.26.4.10
...	...	
0	0	255.255.255.255

+ Identifies individual attackers
- Requires too much memory
- Most entries are zero or insignificant
- Total packet rate per subnet expensive to calculate

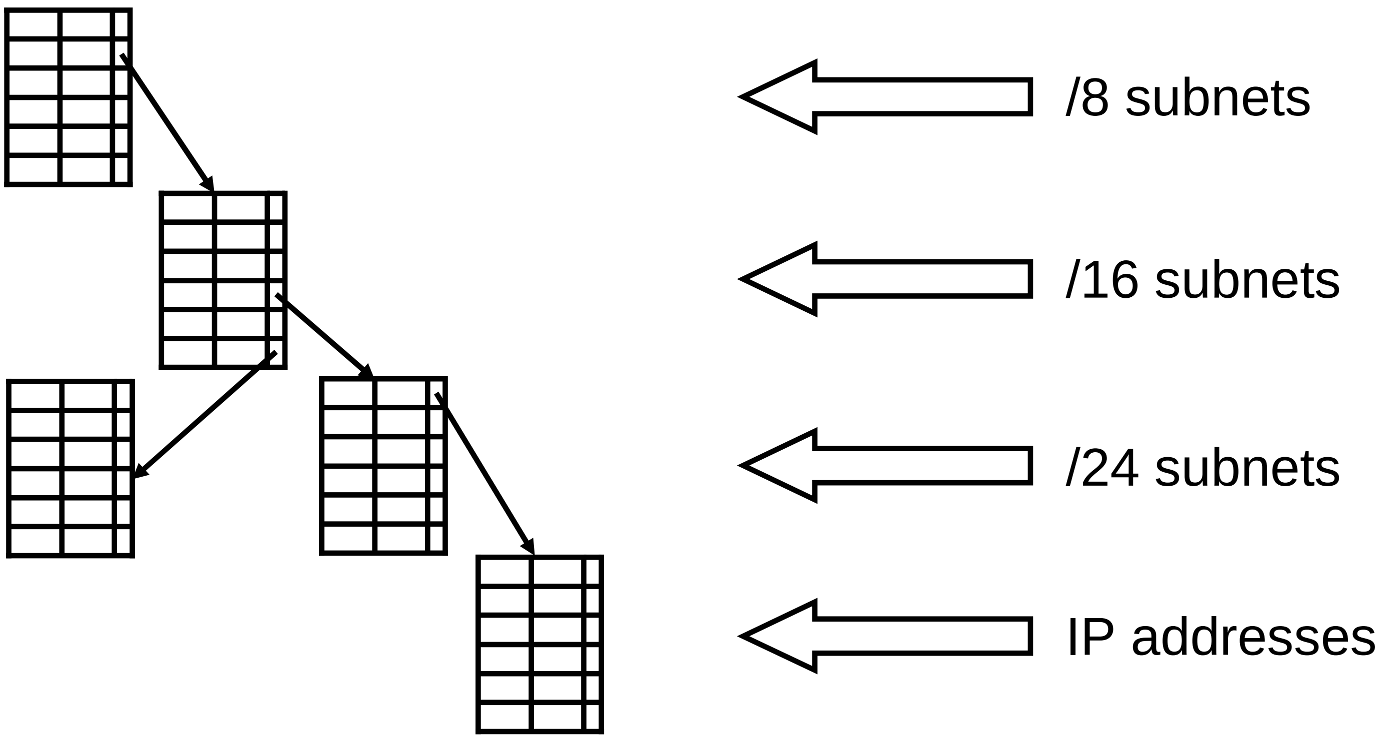
Less naive data-structure

256 entries

from-rate	to-rate	
204	0	0.0.0.0/8
...	...	
528,238	518,234	18.0.0.0/8
309,988	20,876	19.0.0.0/8
...	...	
0	0	255.0.0.0/8

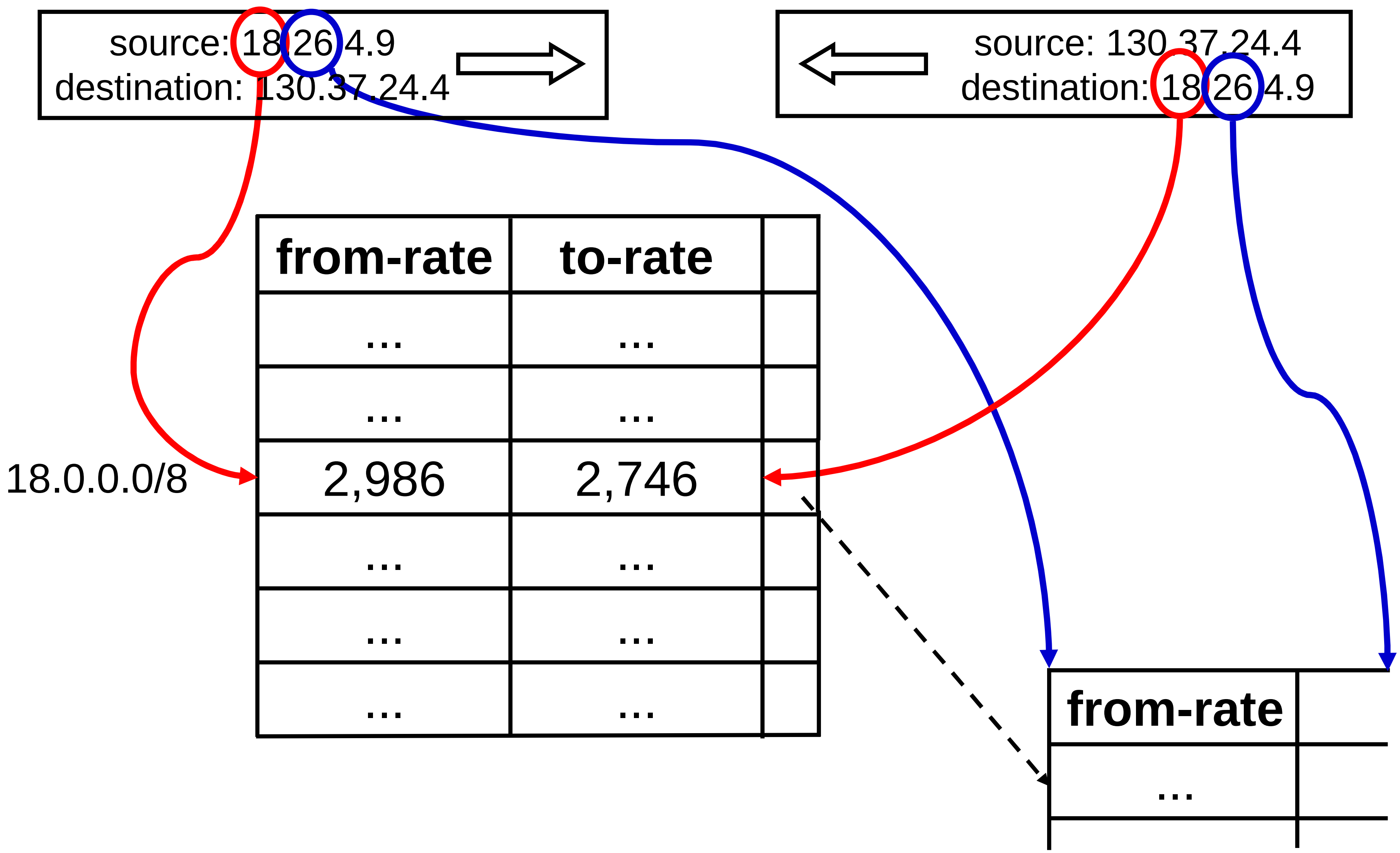
- \+ Requires little memory
- \- May not detect small attacks
- \- Prefixes very short; risky to use for dropping policy
- \- Impossible to collect finer grained data

MULTOPS



- + Provides packet rates on different aggregation levels
- + Expands and contracts dynamically
- + Disregards insignificant subnets and addresses
- + Memory efficient

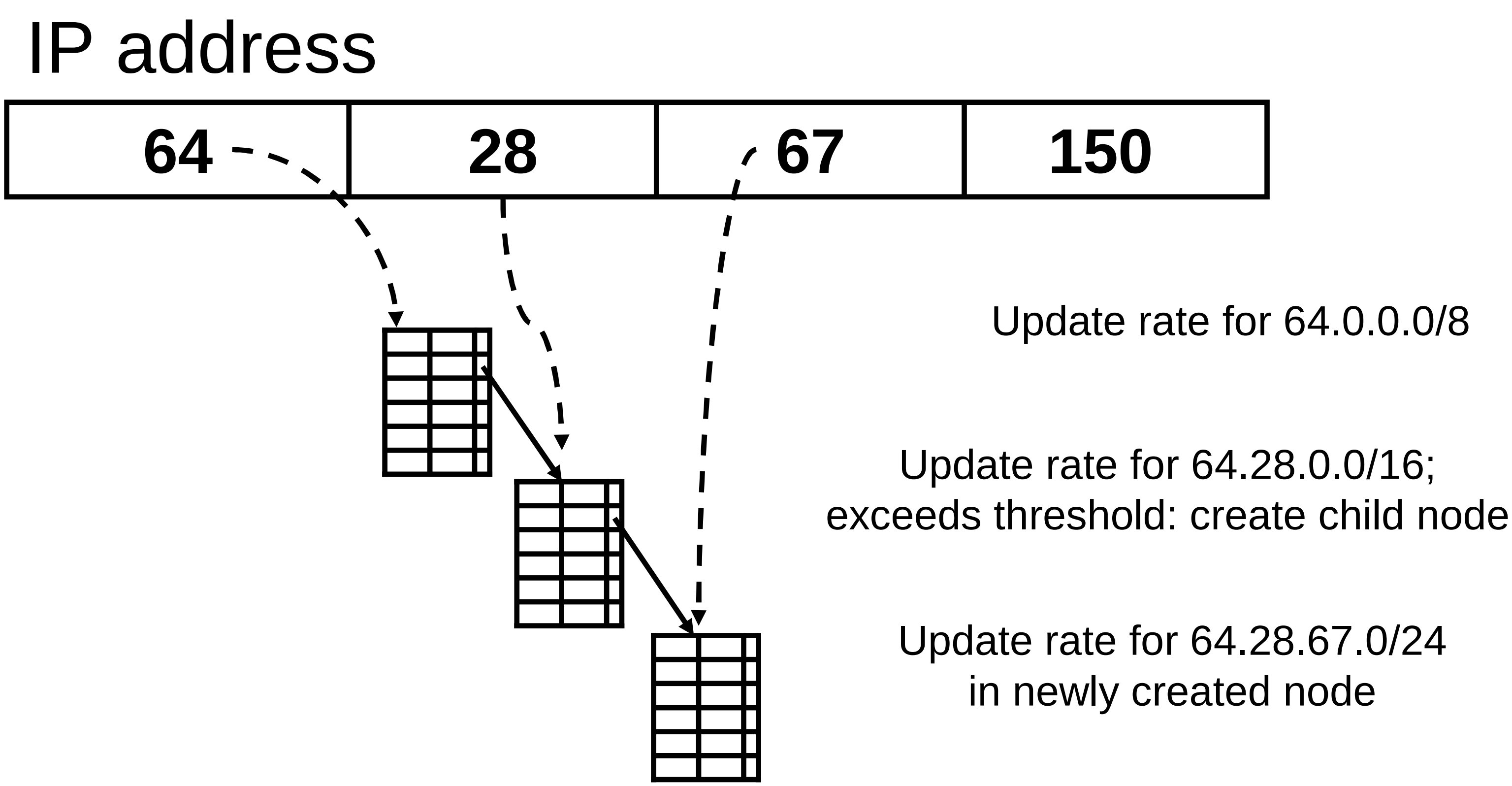
Algorithm



source: 18.26.4.9
destination: 130.37.24.4
source: 130.37.24.4
destination: 18.26.4.9
from-rate
to-rate
...
18.0.0.0/8
2,986
2,746
from-rate

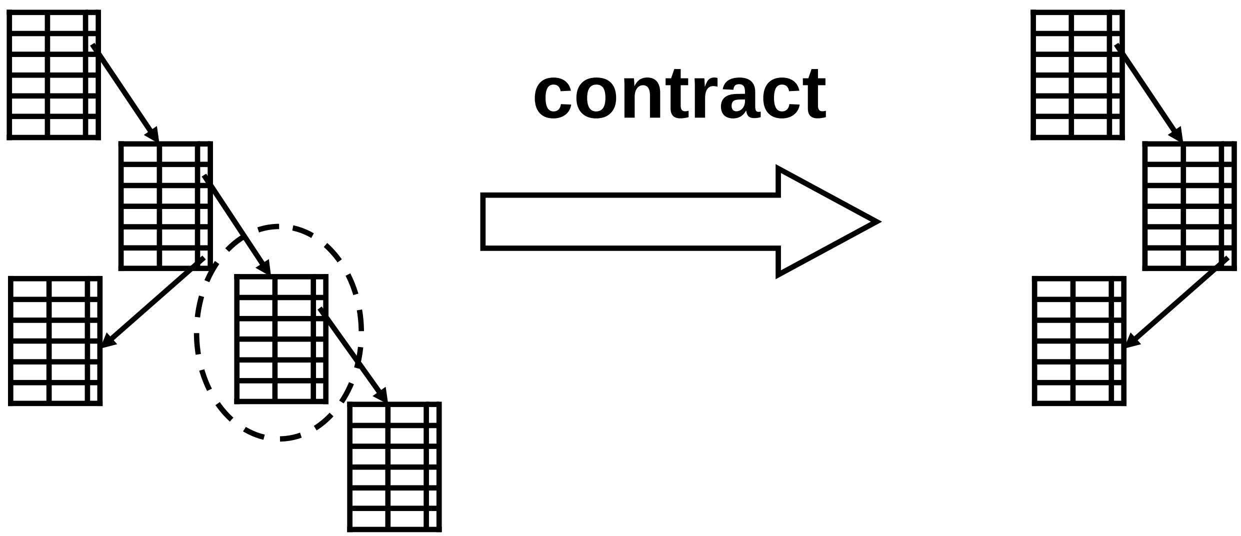
Expansion

Nodes dynamically created to track finer grained packet rates

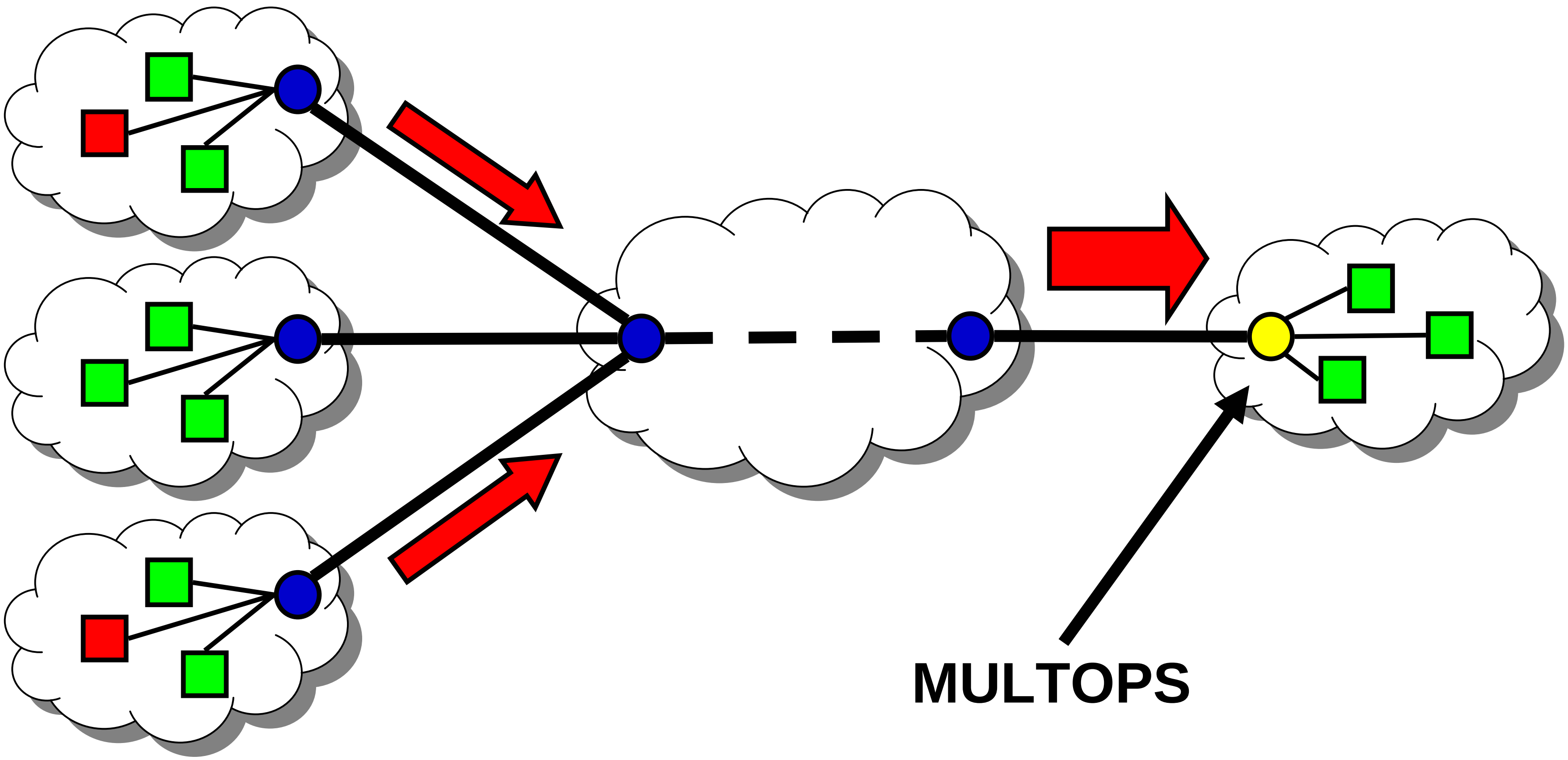


Contraction

- MULTOPS could run out of memory
  - Attackers may cause this intentionally
- Impose absolute memory limit
- Contract stale parts of the tree periodically



Scenario



+ MULTOPS drops packets with malicious address prefix
- Collateral damage depends on length of address prefix

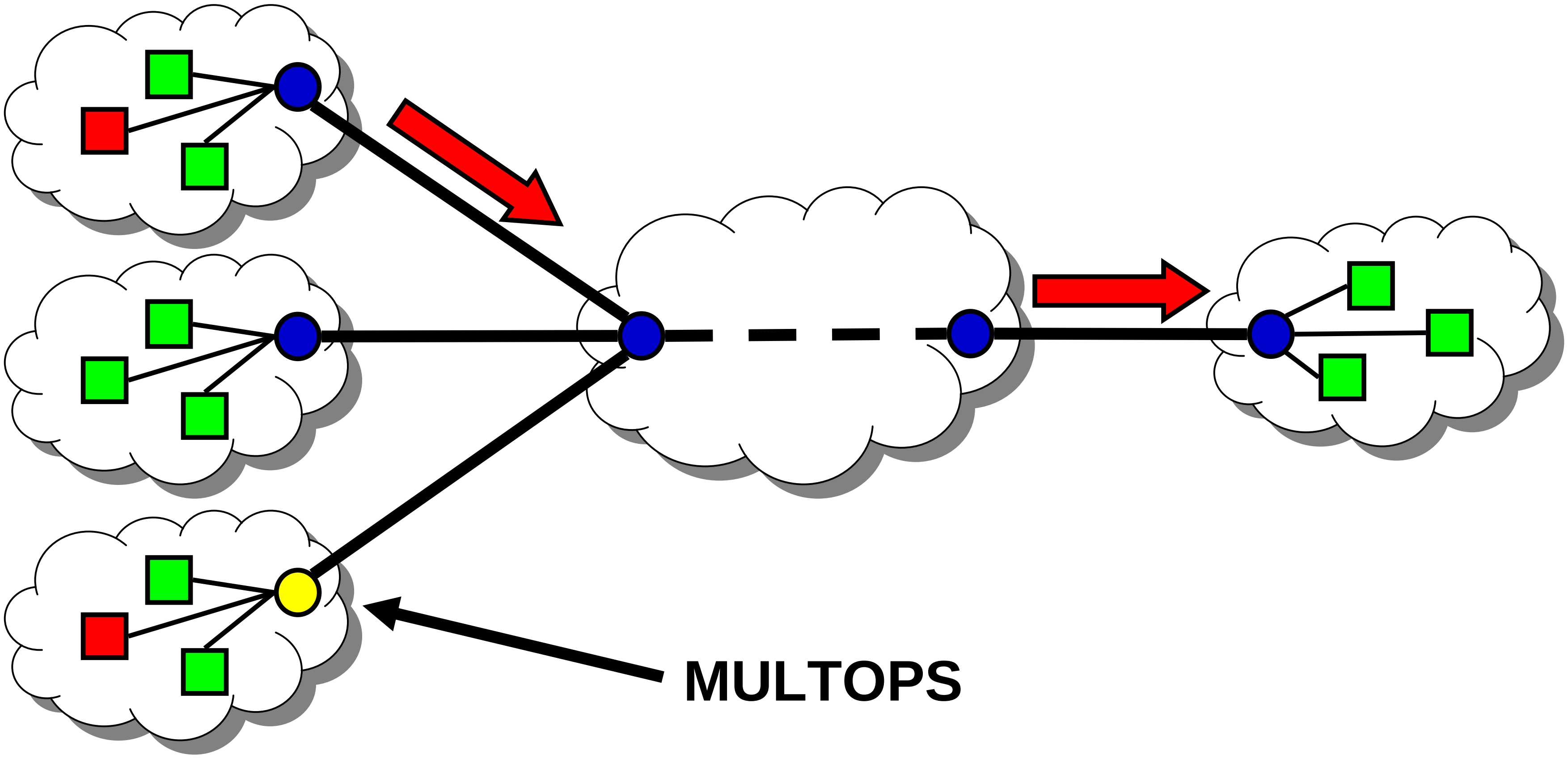
MULTOPS dropping decision

- Drop packet based on 2 criteria
  - Packet rate > 100 packets per second, and
  - Ratio > 1:3
- Values determined through experimentation

Randomized source addresses

- Impossible to identify attackers' addresses
- Easy to identify victim's address
- Drop packets based on victim's address
- 2 MULTOPS to stop both attack types
  - Source-based MULTOPS: non-randomized attacks
  - Destination-based MULTOPS: randomized attacks

Reverse orientation

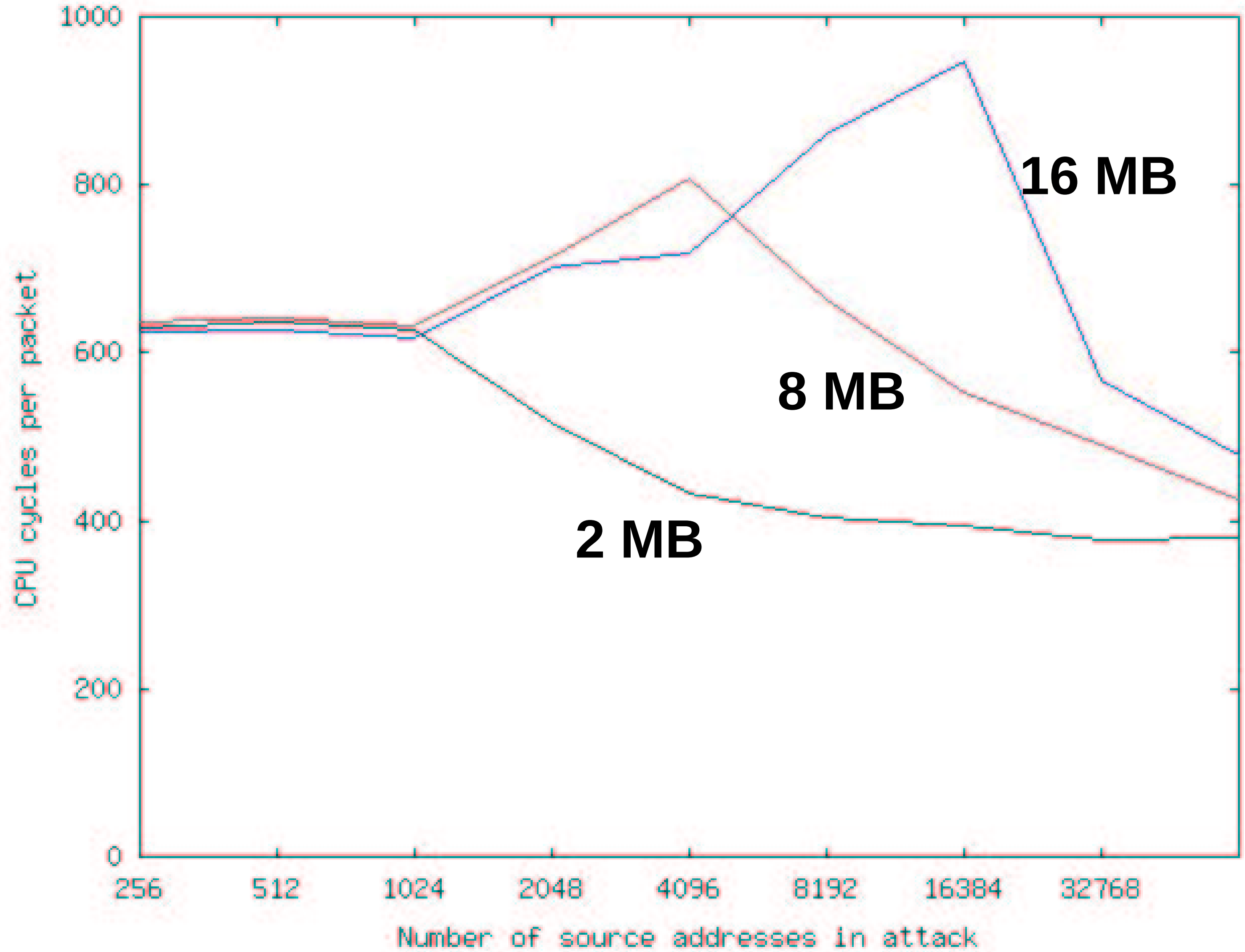


+ MULTOPS drops packets going to victim
+ Victim's network relieved from malicious traffic
- MULTOPS drops benign packets going to victim

Performance

- MULTOPS implemented in Click, a modular router
- Forwarding speed inversely related to size of tree
- Forwards up to 825,000 packets per second
  - Pentium III, 833MHz PC
  - 256MB main memory, 256KB cache
- Better performance than reported in paper
  - Simpler mechanism to compute packet rates

Cycles per packet for different attacks



Status

- Enhanced MULTOPS used by Mazu Networks

- Has detected TCP floods on commercial networks
  - Identified a single 8-bit malicious address prefix

Future work and problems

- Different ACK policies change ratio for valid traffic
- Not all Internet traffic is TCP
- Asymmetric routes
  - MULTOPS must see traffic in both directions
  - Requires distributed data collection

Related work

- Ingress/egress filtering (RFC2827)
- IP Traceback (Savage et al.)
- CenterTrack (Stone)
- Pushback (Bellovin et al.)
- RMON, Netflow (Cisco)

MULTOPS is complementary

Conclusion

- MULTOPS identifies attacker/victim addresses
- Effectiveness depends on
  - MULTOPS location on network
  - Randomized source address
- MULTOPS successfully detects and stops attacks