UNIVERSITY OF OREGON

Detecting Co-Residency
with Active Traffic Analysis Techniques

Adam Bates

Ben Mood

Joe Pletcher

Hannah Pruse

Masoud Valafar

Kevin Butler

University of Oregon
OSIRIS Laboratory

CCSW'12, Raleigh, NC, USA
19 October 2012

To the Cloud?

UNIVERSITY OF OREGON

"An attacker can often place his or her instance on the same physical machine as a target instance... creating the ability of a malicious instance to utilize side channels to learn information about co-resident instances."

Co-Resident Watermarking

UNIVERSITY OF OREGON

This work...

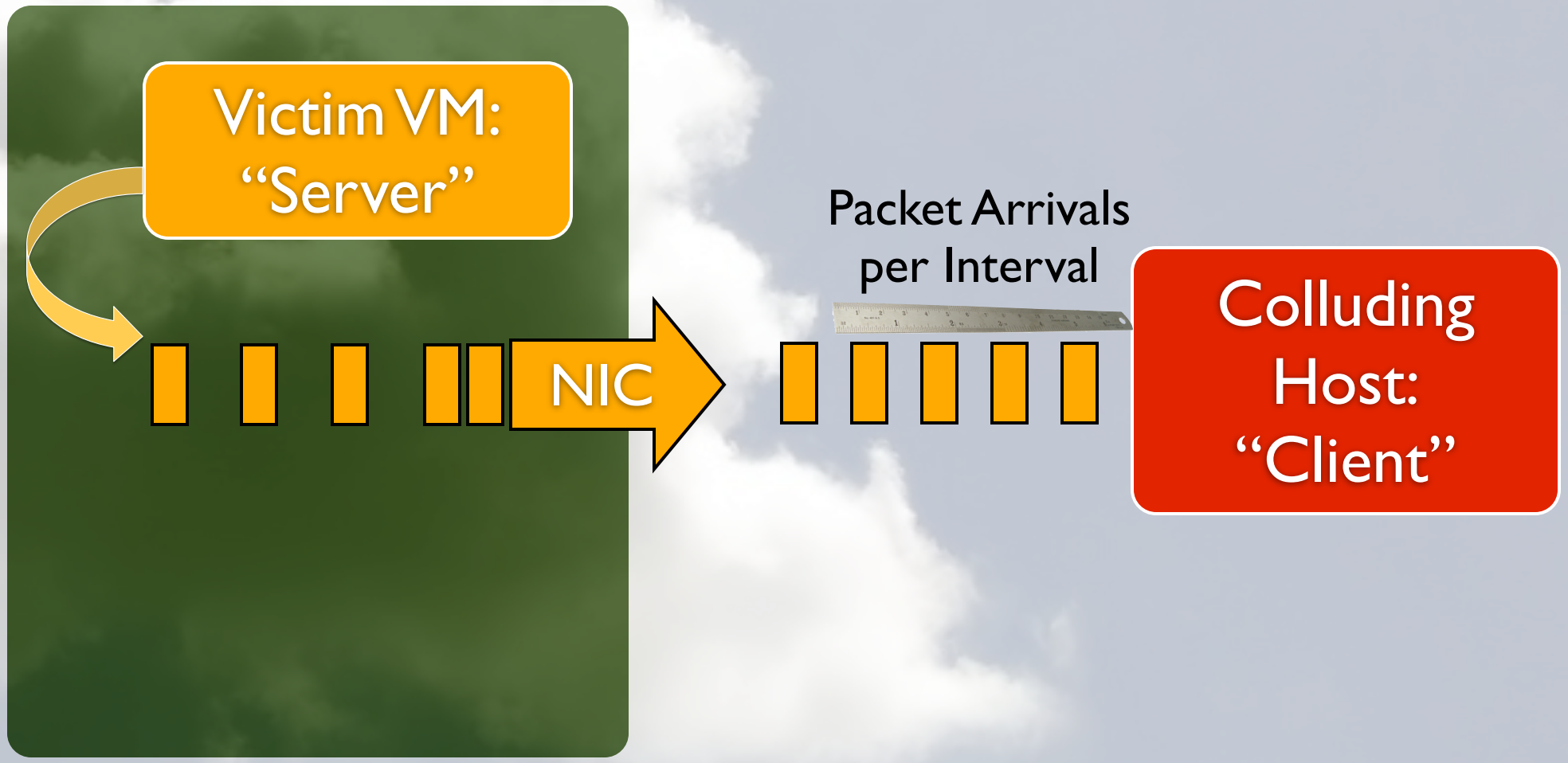
- **Investigates** cloud side channels at the hardware level via the network interface.
- **Introduces** *co-resident watermarking*, an attack that breaks VM isolation via a network timing channel.
- **Evaluates** methodology to confirm its efficacy in the adverse compute cloud conditions and configurations.
- **Demonstrates** further side-channel applications: covert communication, traffic profiling of victim VMs.

Design: Threat Model

UNIVERSITY OF OREGON

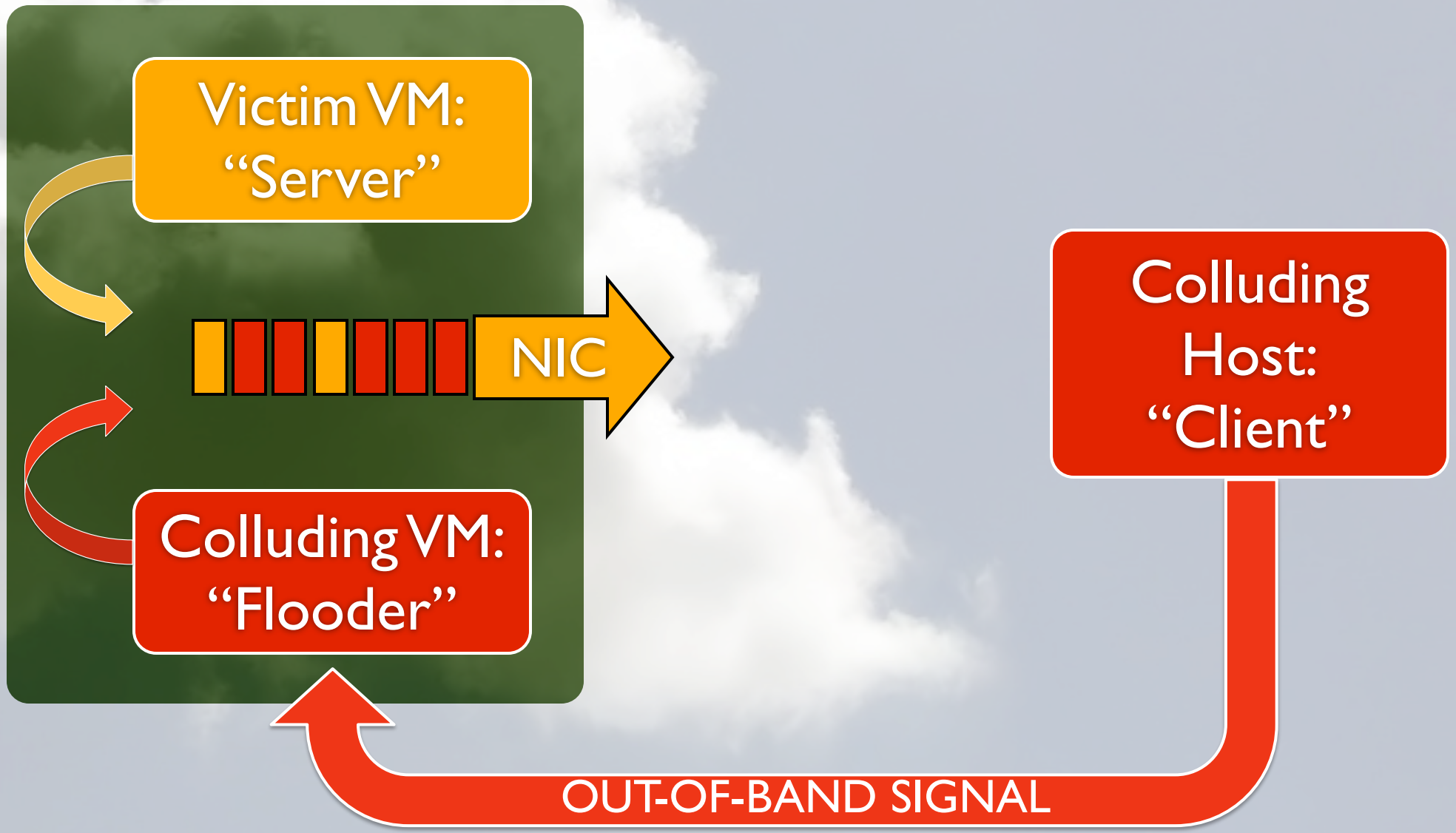
- Cloud Provider: patched all internal cross-VM side channels (e.g. L2 Cache).
- Adversary: manipulates own (legitimate) instances to find the victim's instances.
- Victim: business that runs a web-facing service.

Design: Attack Model



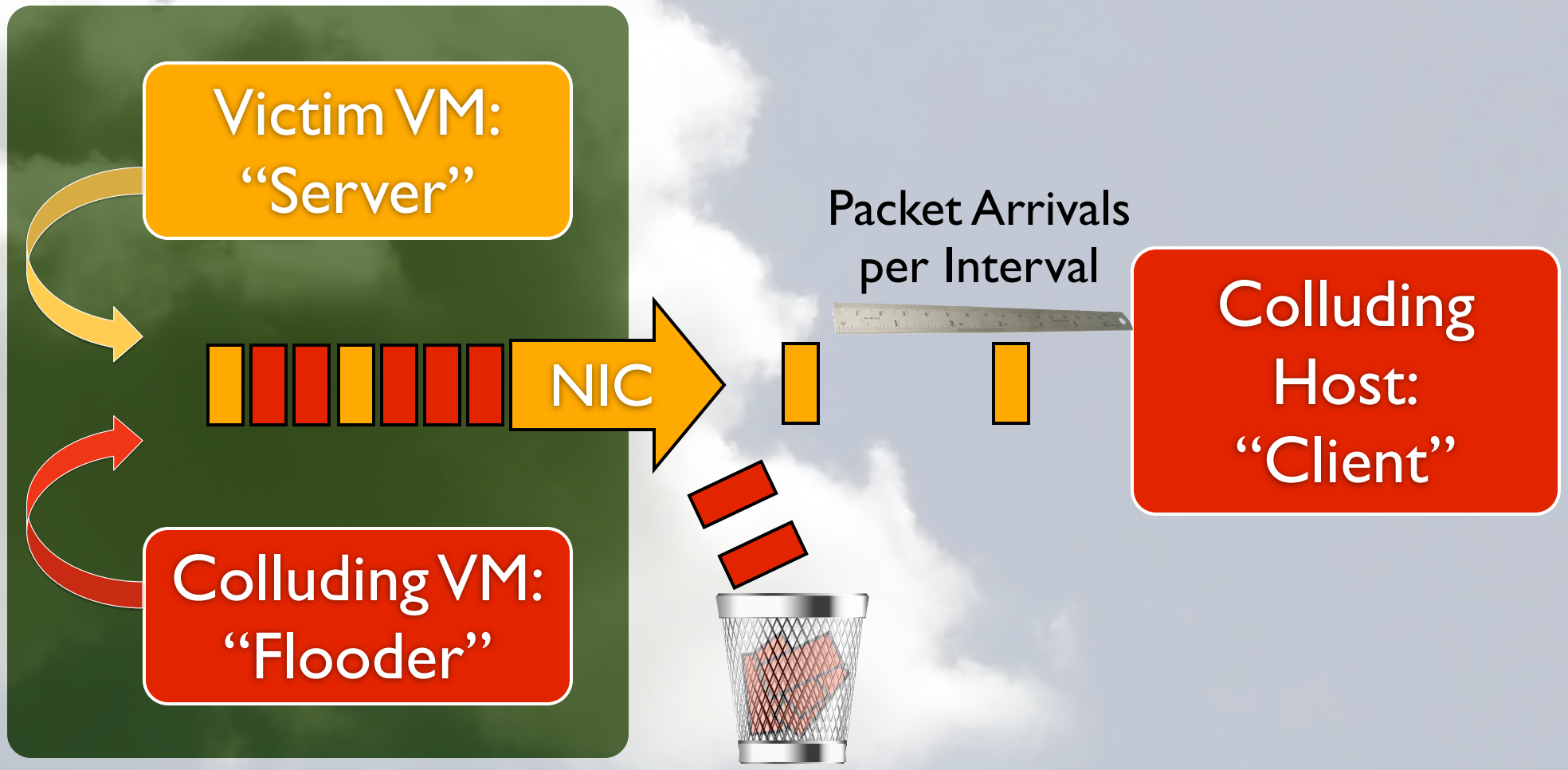
Design: Attack Model

UNIVERSITY OF OREGON



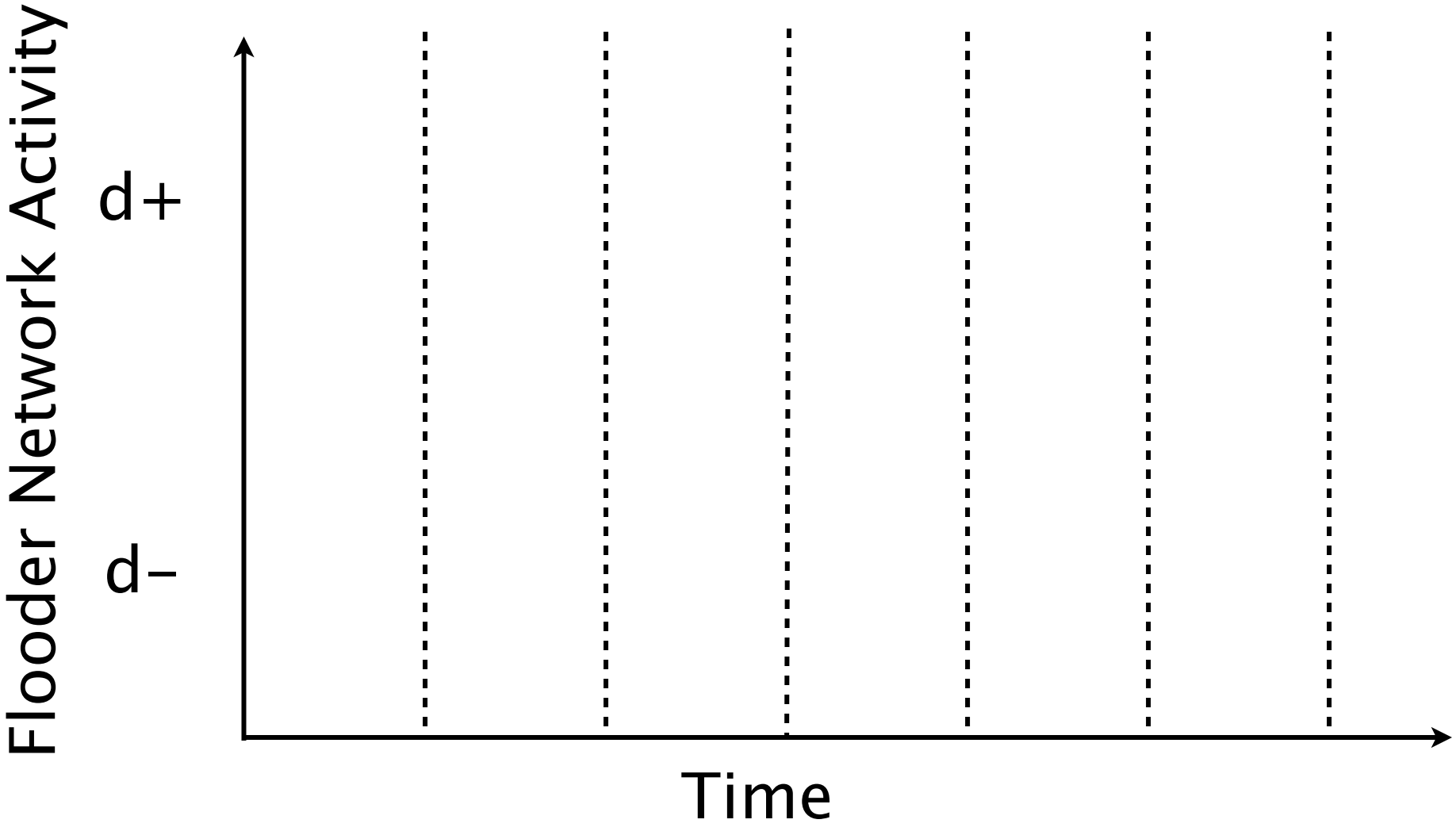
Design: Attack Model

UNIVERSITY OF OREGON



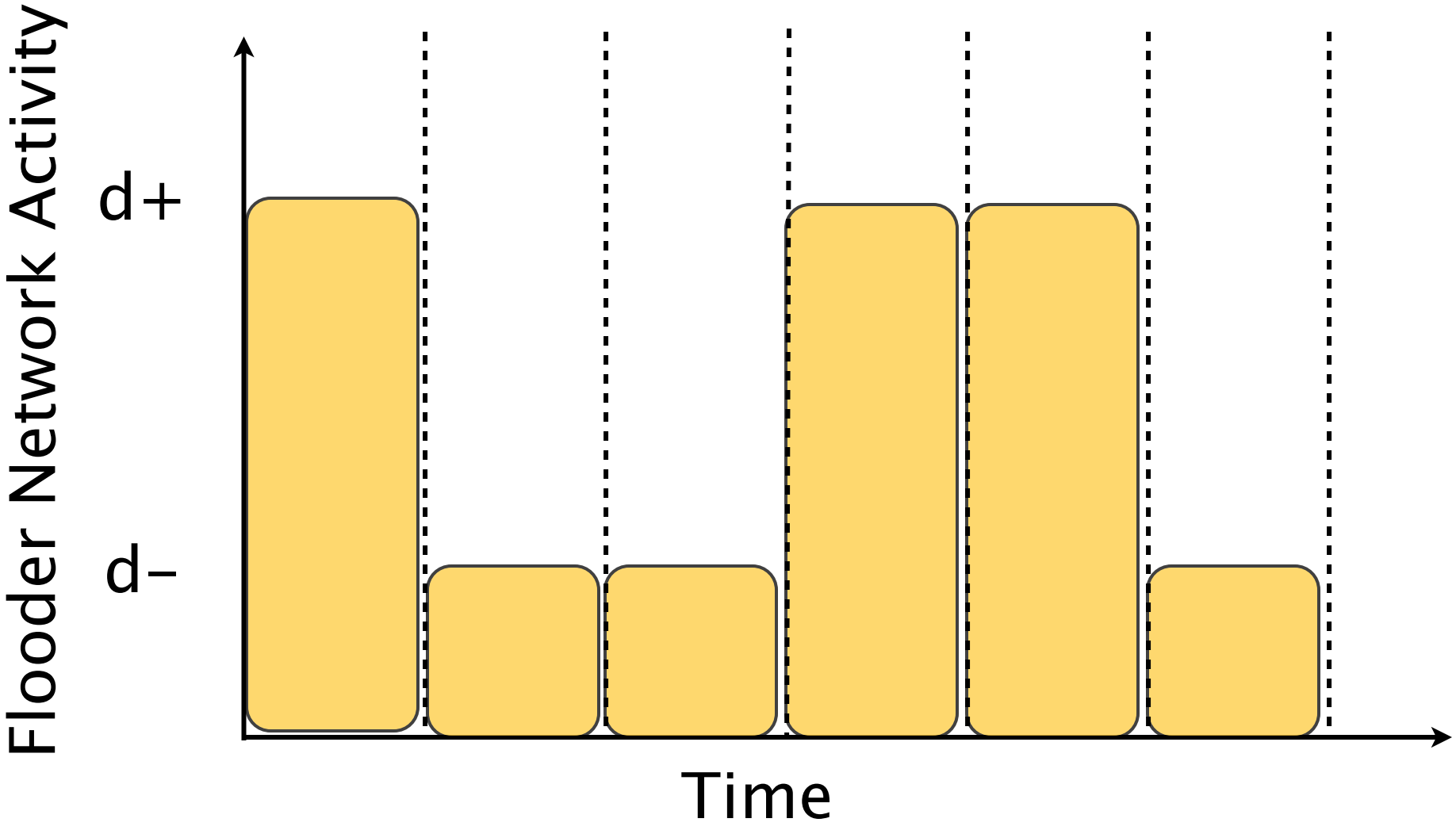
Design: Watermark Encoding

UNIVERSITY OF OREGON



Design: Watermark Encoding

UNIVERSITY OF OREGON



Evaluation: Goals

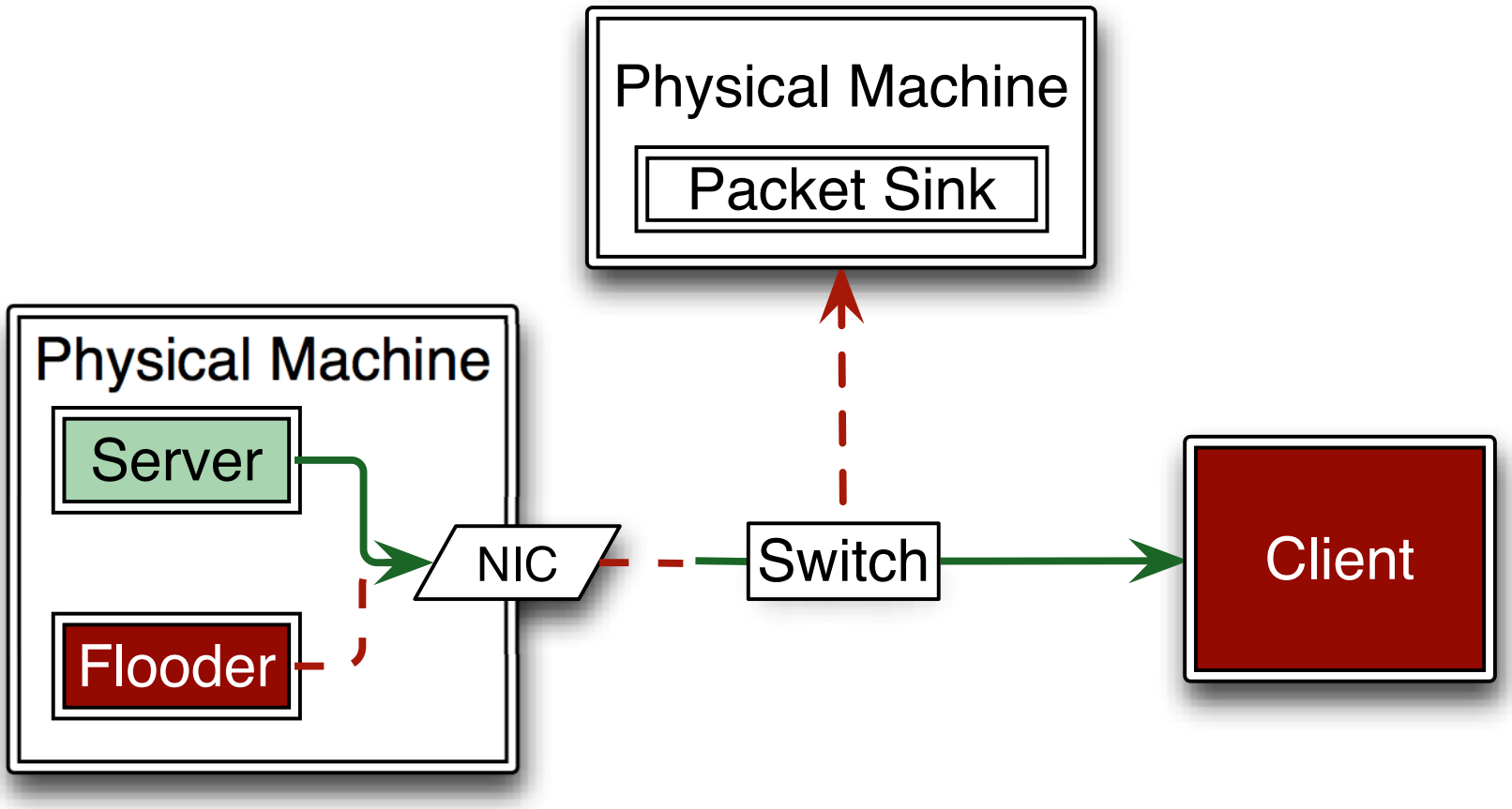
UNIVERSITY OF OREGON

Determine if *co-resident watermarking* works...

- independent of hypervisor or network/system load
- in production cloud environments
- in adverse cloud topographies
- on advanced network devices (SR-IOV)

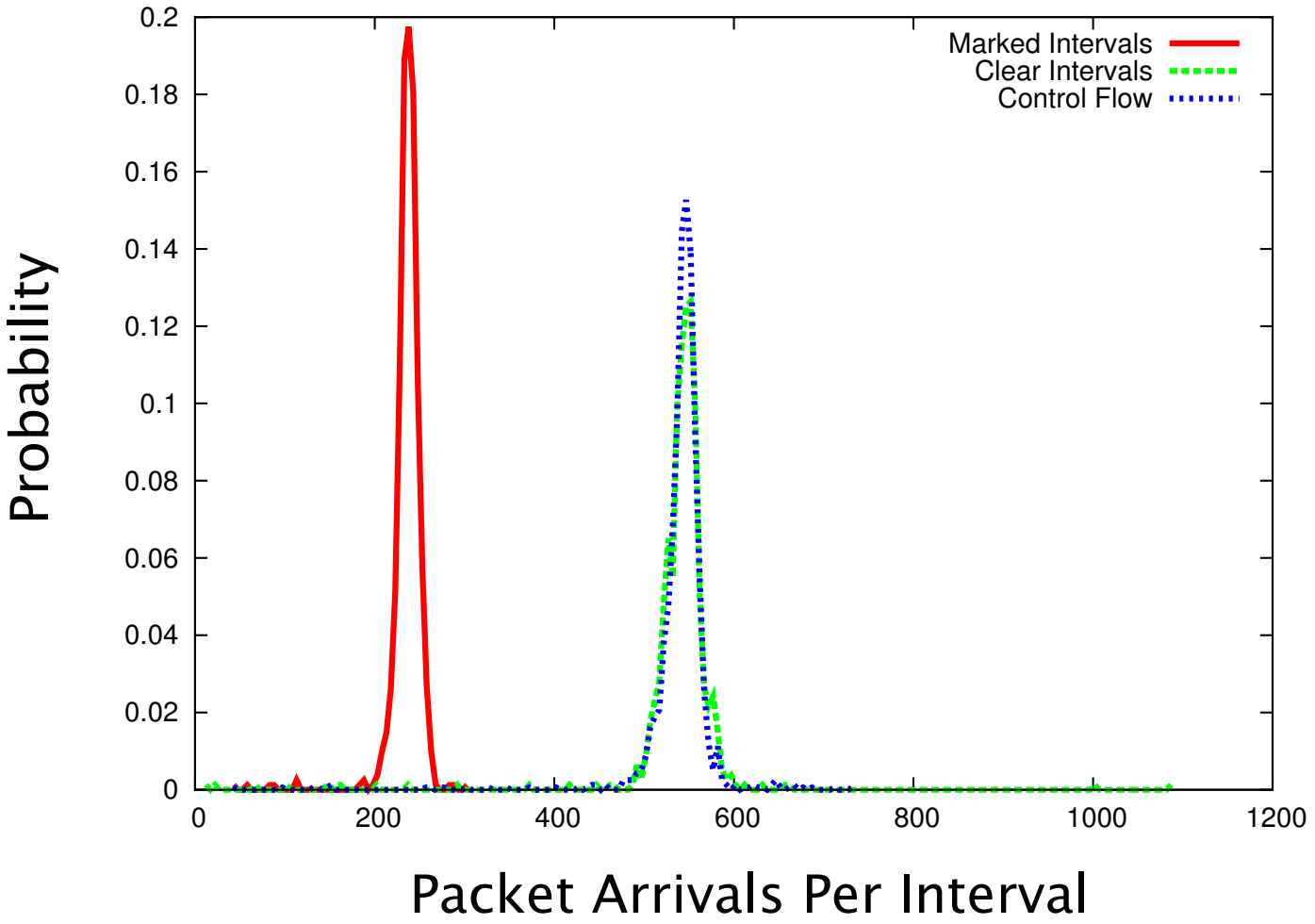
Do any conditions create false positives or negatives?

Evaluation: Participants



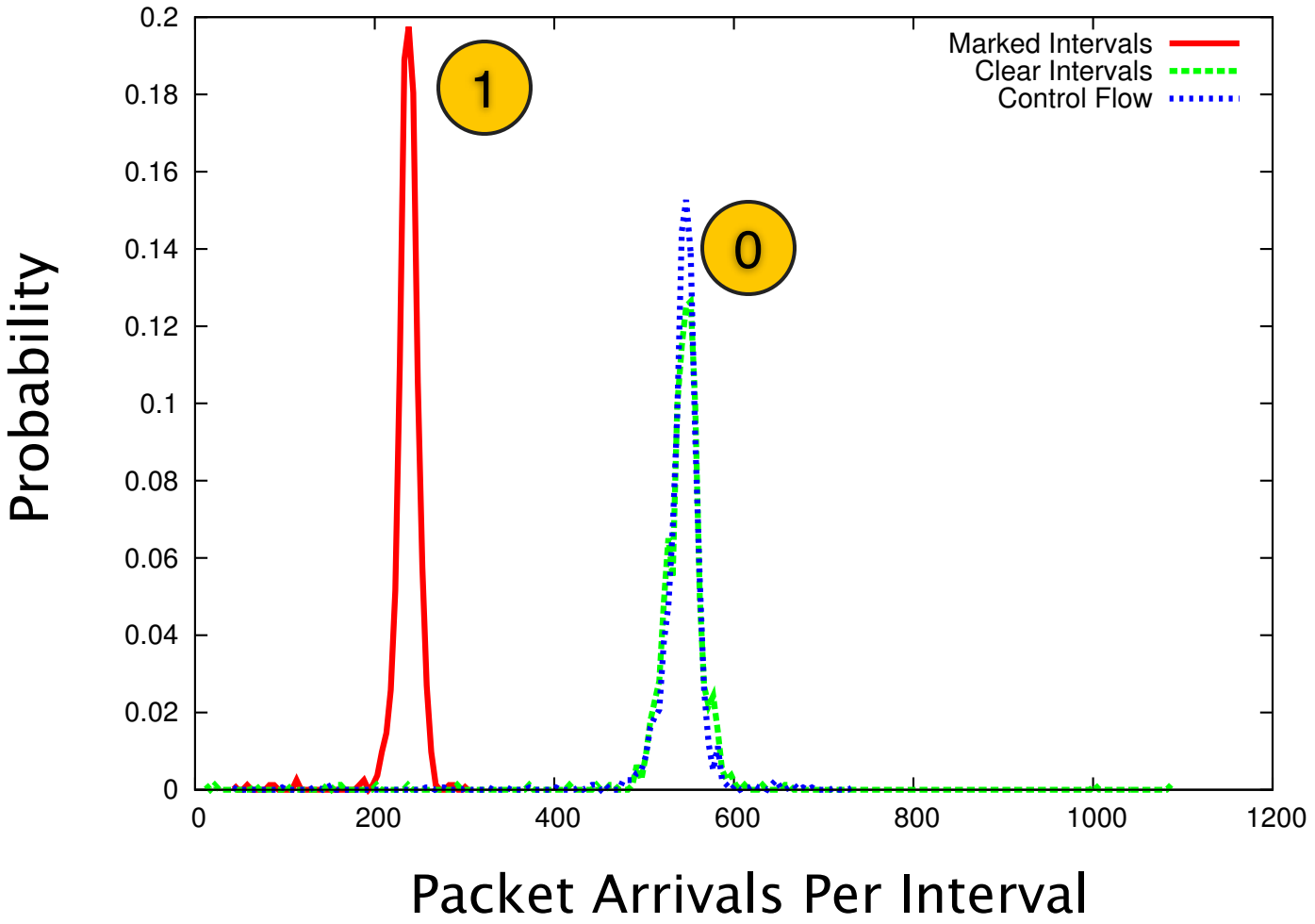
System configuration for local laboratory testbed.

Evaluation: Hypervisors



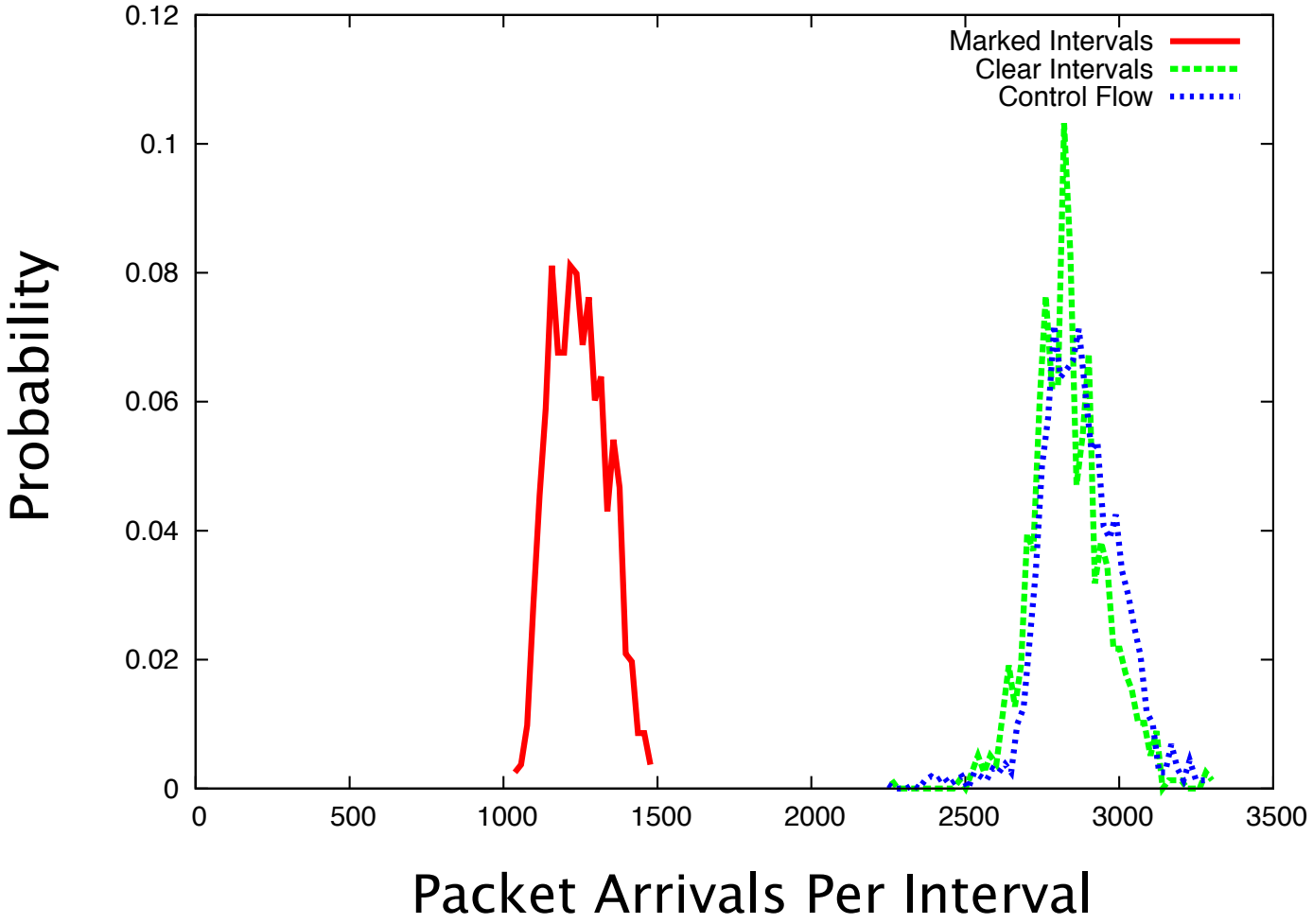
Xen

Evaluation: Hypervisors



Xen

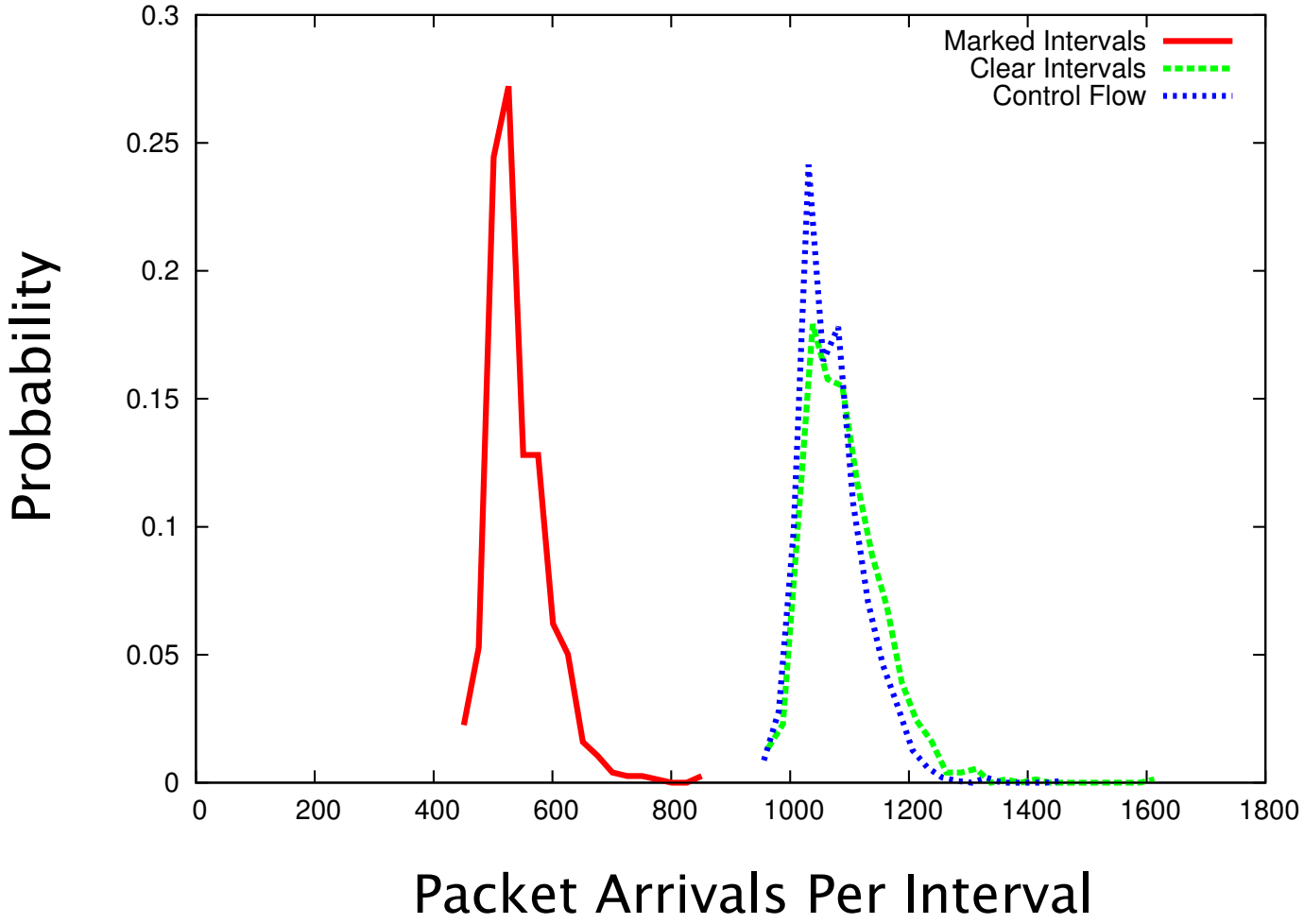
Evaluation: Hypervisors



VMWare ESXi

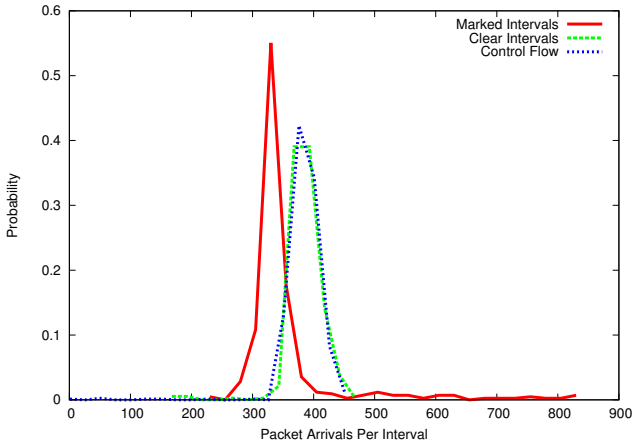
Evaluation: Network State

UNIVERSITY OF OREGON

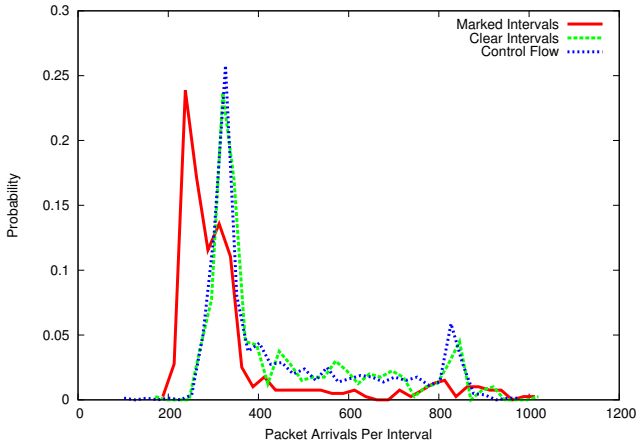


Xen, Coast-to-Coast Trial

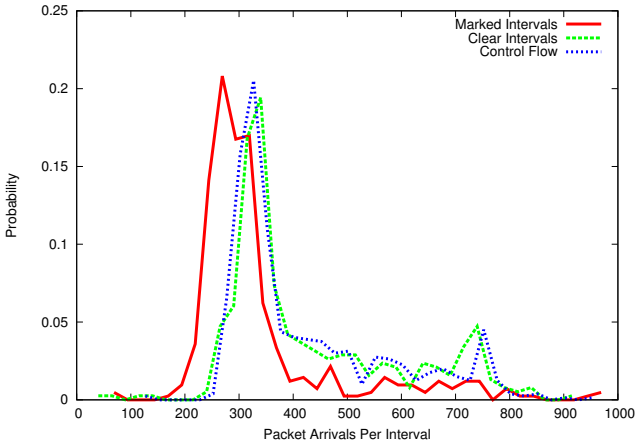
Evaluation: System Load



1 Extra Guest



2 Extra Guests

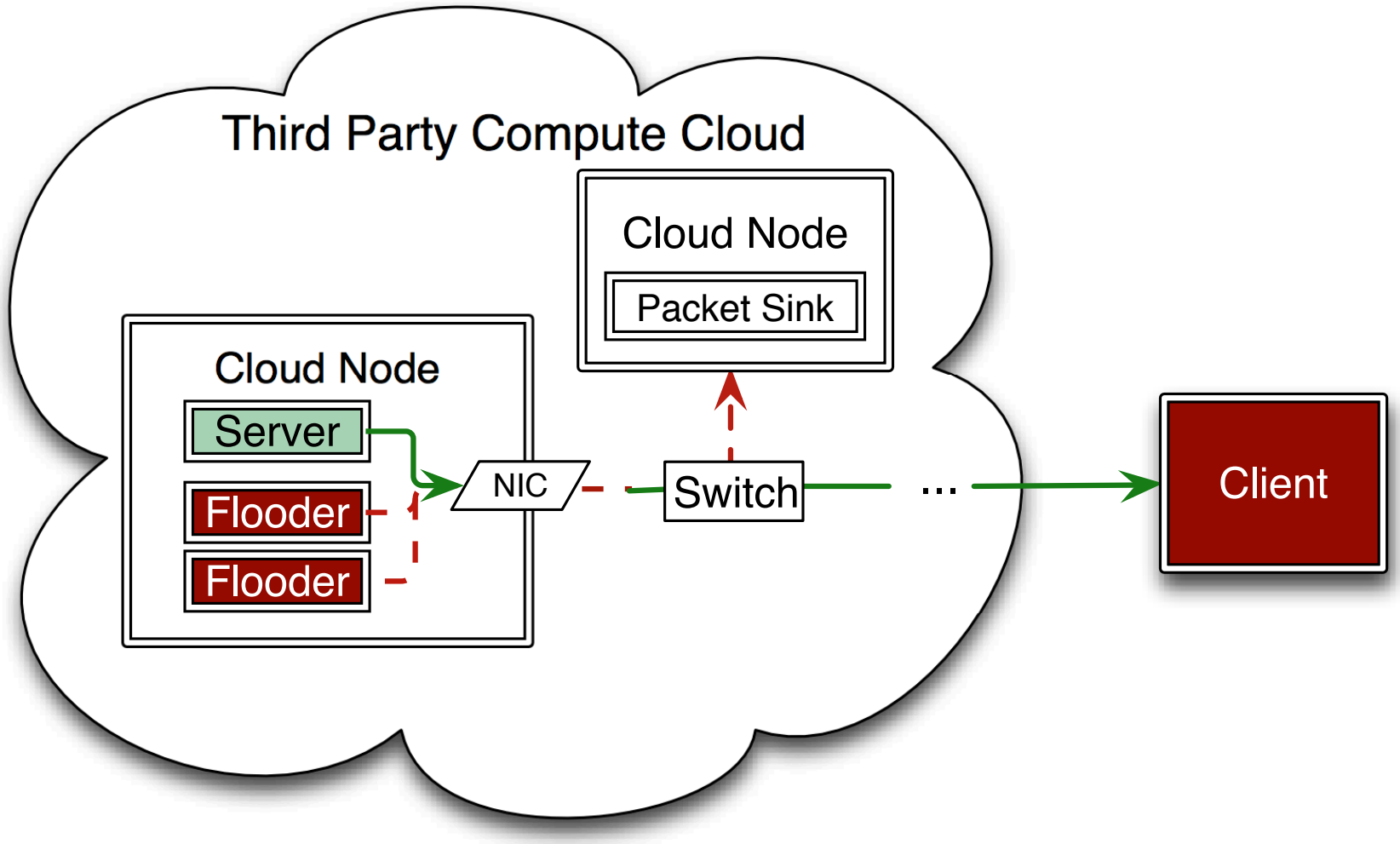


3 Extra Guests

Trial	Length	$KS_{+d,-d}$	p-val	Result
SERVER & FLOODER	2.5 *sec*	0.99	0.01	*Co-Res*
Add 1 GUEST	3.75 *sec*	0.78	0.05	*Co-Res*
Add 2 GUESTS	3.75 *sec*	0.91	0.01	*Co-Res*
Add 3 GUESTS	10 *sec*	0.49	0.05	*Co-Res*

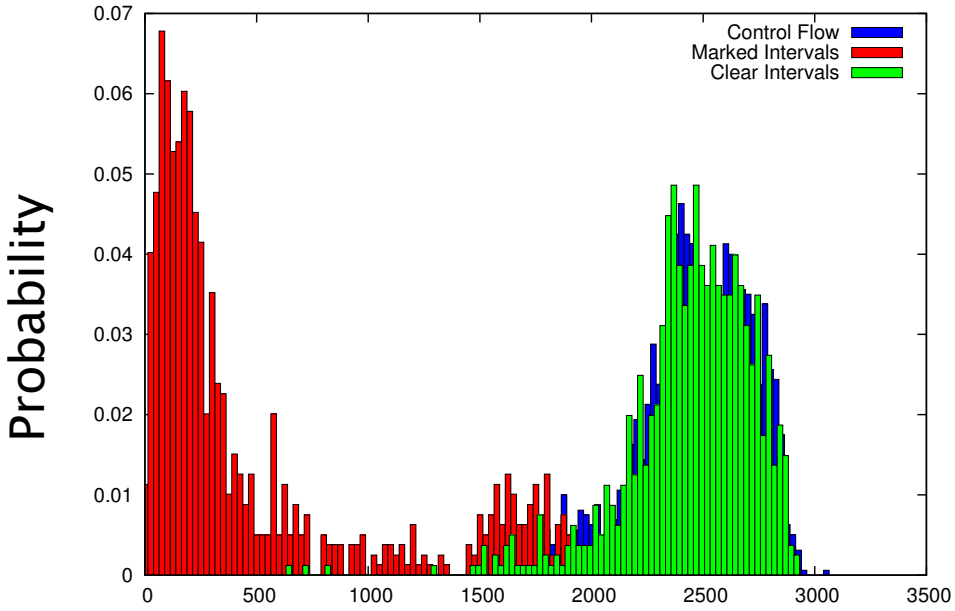
Evaluation: 3rd Party Clouds

UNIVERSITY OF OREGON

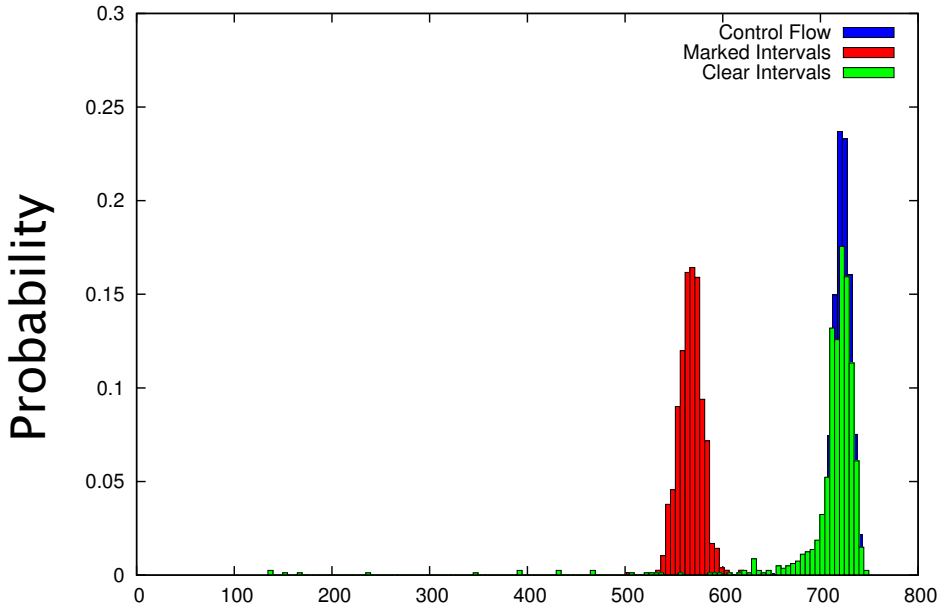


System configuration for ACISS and Futuregrid clouds.

Evaluation: 3rd Party Clouds



ACISS (KVM)

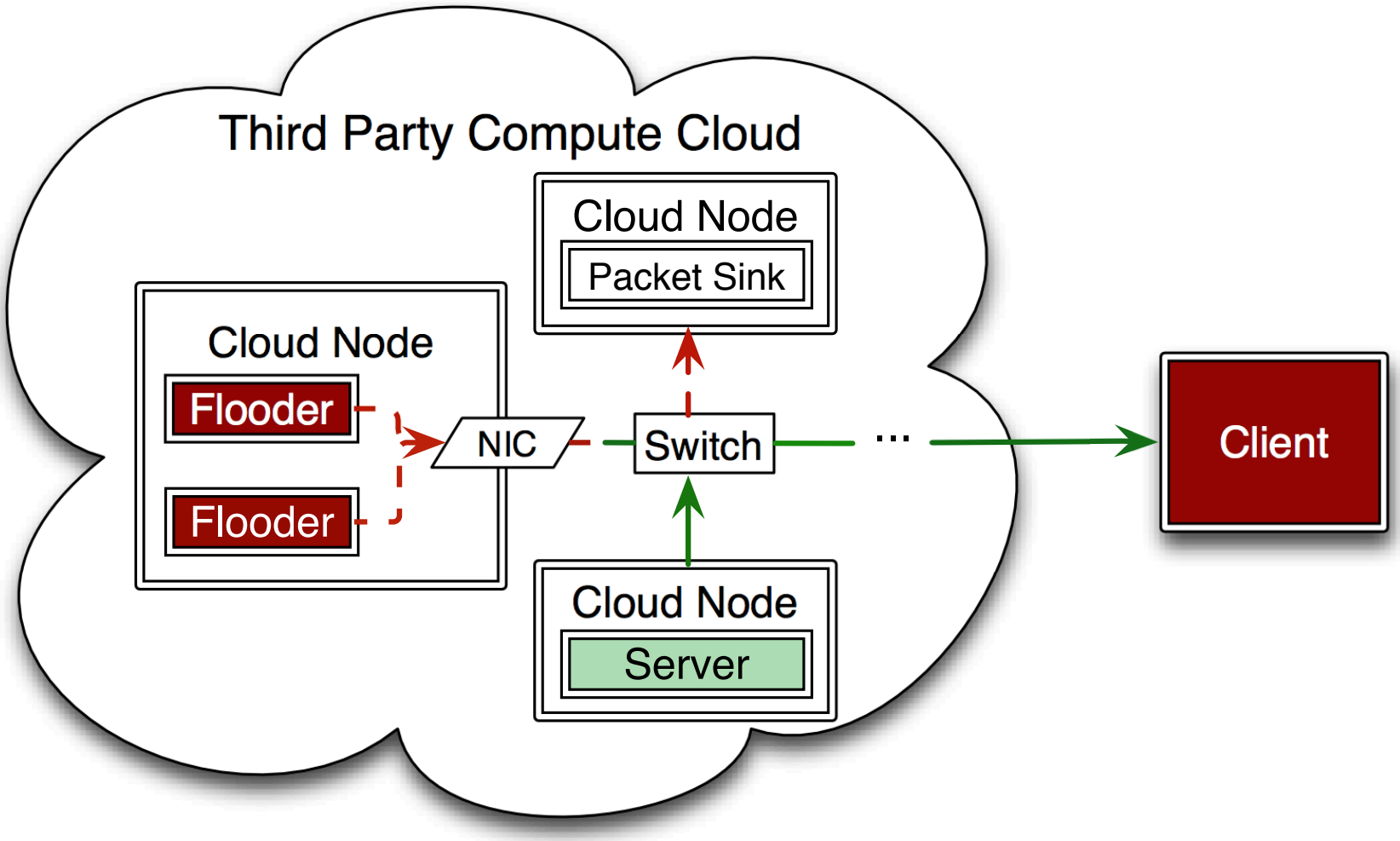


Futuregrid (Xen)

- *Co-resident watermarking* is a viable attack in production cloud environments.

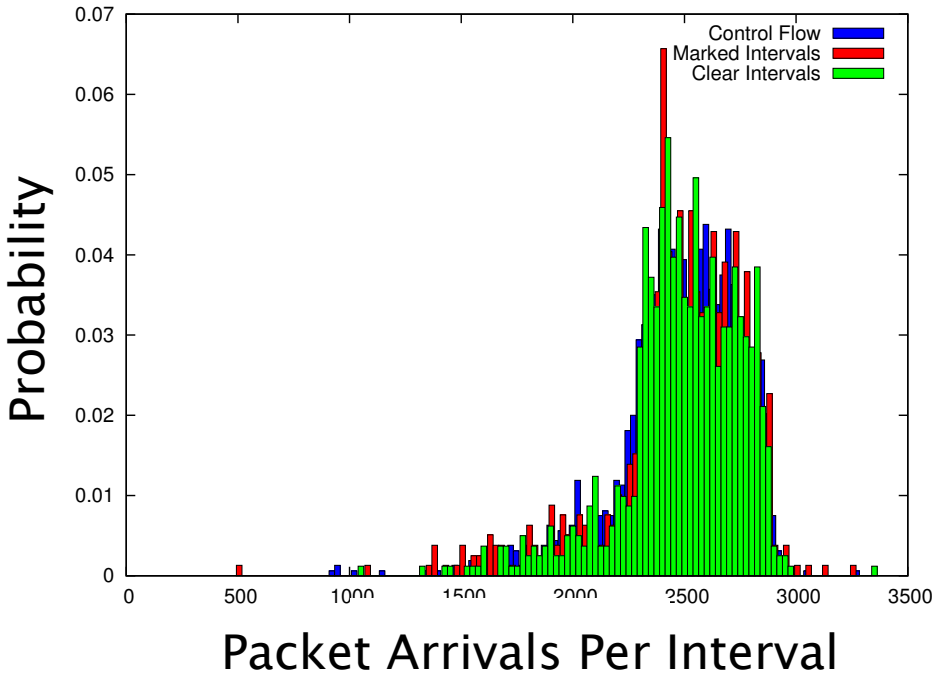
Evaluation: Cloud Topography

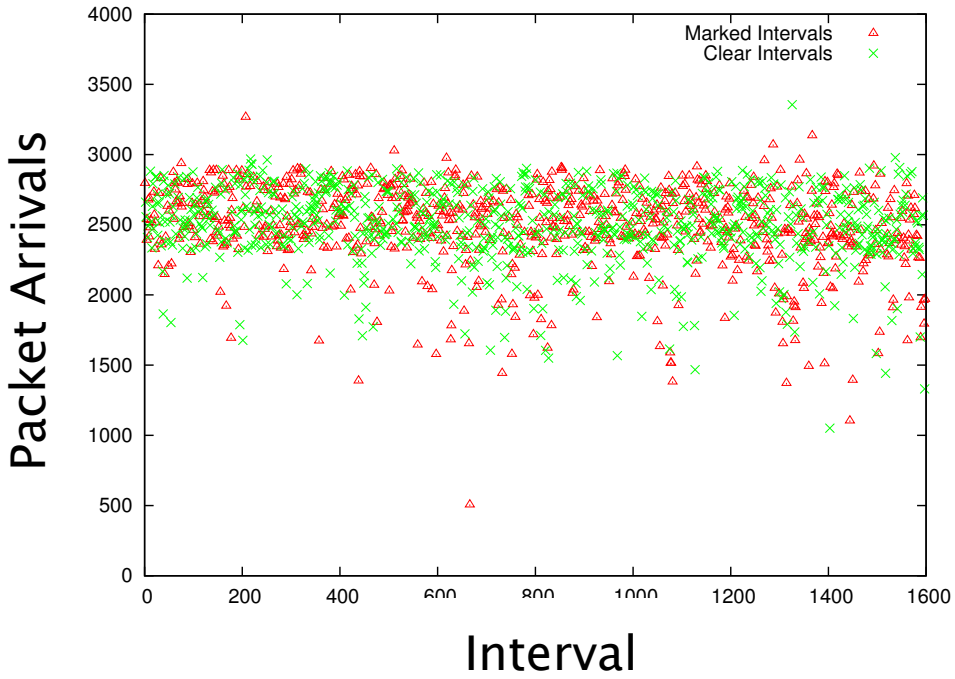
UNIVERSITY OF OREGON



Configuration where target and adversary share first hop.

Evaluation: Cloud Topography

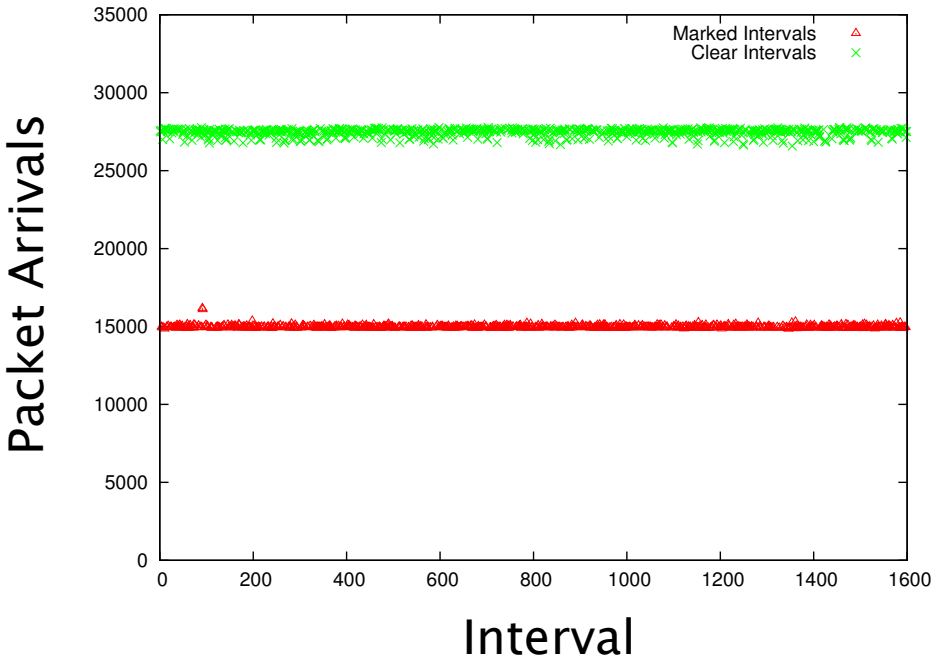




ACISS (KVM)

- *Co-resident Watermarking* does not produce false positives under adverse topographies.

Evaluation: SR-IOV Hardware



Xen, SR-IOV NIC

- Intel 10GbE Controller, SR-IOV enabled (*ixgbe*).
- Exposed virtual PCI devices that we bound to each VM.
- Pass-through technology *improved* the effectiveness of *co-resident watermarking*!

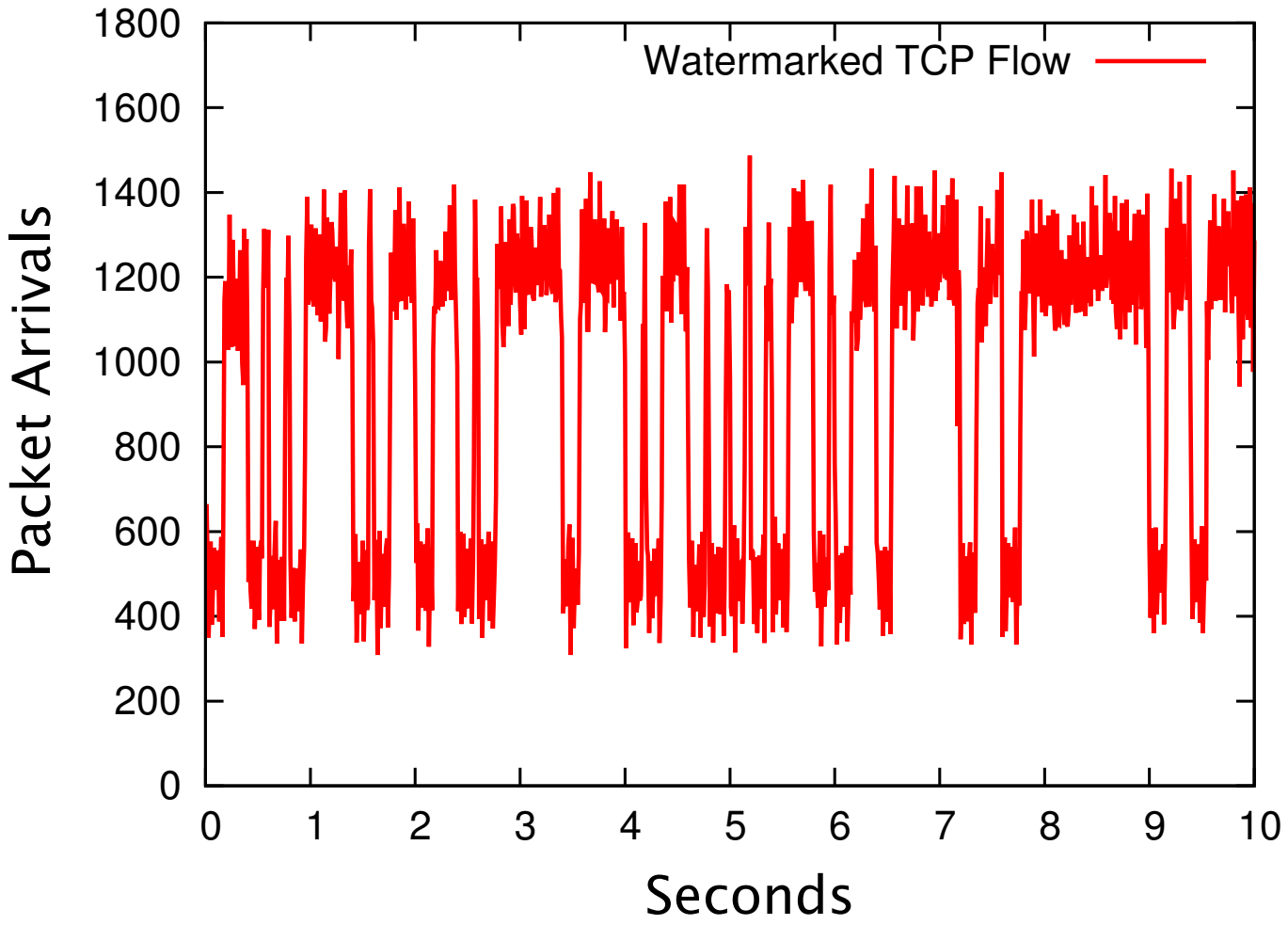
Analysis

UNIVERSITY OF OREGON

- So what else we can do?
  - Covert Multicast
  - Load Measurement

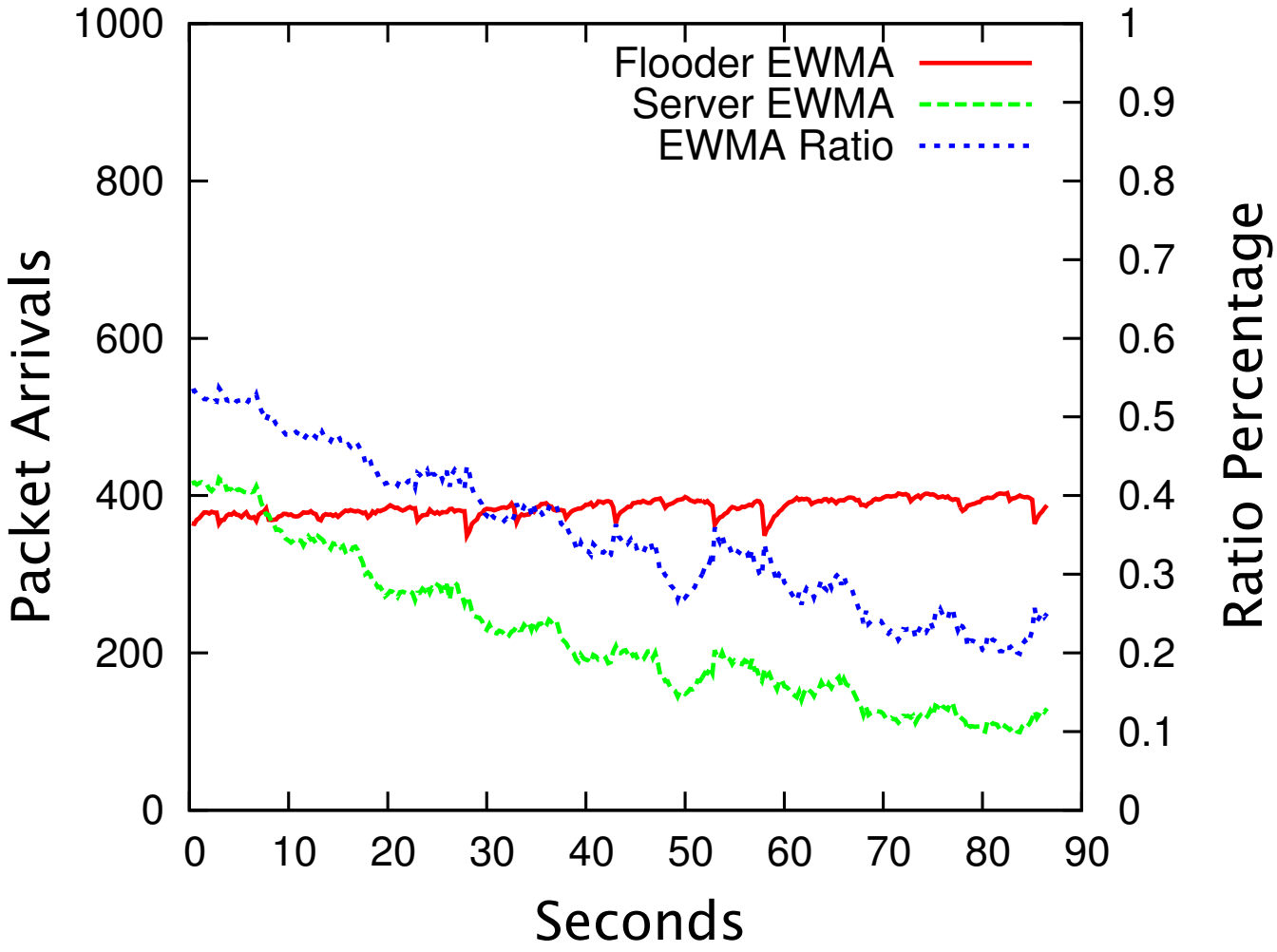
Analysis: Covert Multicast

UNIVERSITY OF OREGON



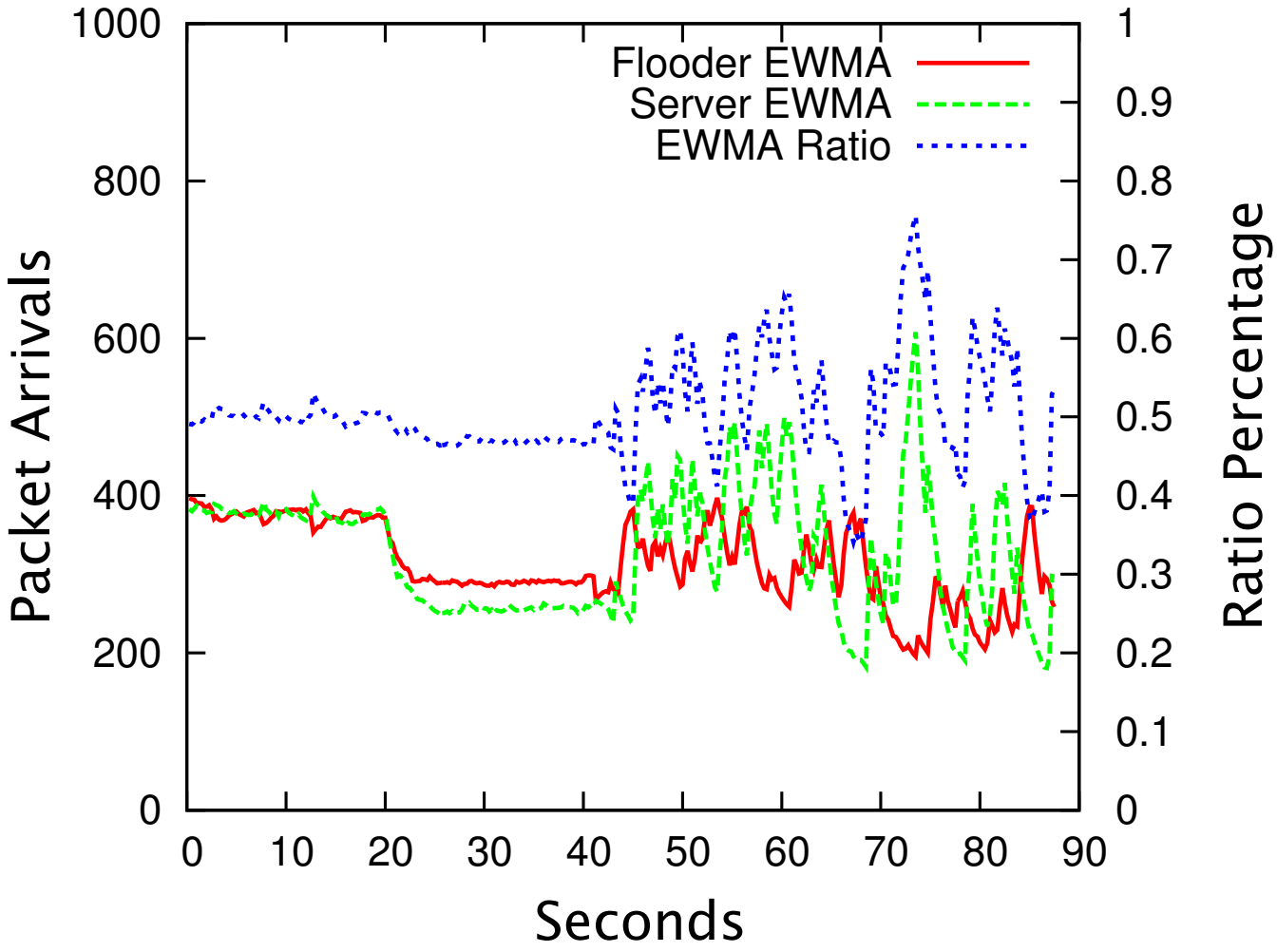
First 10 seconds of transmission of a 2048-bit key.

Analysis: Load Measurement



Flooder & Server Throughput as Server load increases.

Analysis: Load Measurement



Flooder & Server Throughput as System load increases.

Countermeasures

UNIVERSITY OF OREGON

- Underutilization
  - Dedicated network paths for each VM
  - Overprovision NIC's
  - Cap VM bandwidth
- L2 Cache defenses: equate to time-division multiplexing, another form of underutilization.
- Randomization: adverse effects on TCP performance.

Future Work

UNIVERSITY OF OREGON

- Implement an invisible network flow watermarking scheme for co-resident VMs.
- Use cross-VM network flows to profile internal conditions of cloud provider.
- Repeat trials successfully on Amazon EC2.

Conclusion

UNIVERSITY OF OREGON

- Co-resident watermarking exploits network flows to break virtual machine isolation.
  - 10 seconds or less for an accurate decision (Heuristic).
  - Effective independent of hypervisor, hardware, cloud state.
  - Works in production cloud environments.
- This preliminary work on the cross-VM network flow side channel underscores the difficulty of providing isolation in compute clouds.

Questions?

UNIVERSITY OF OREGON

Adam Bates

amb@cs.uoregon.edu