Sneak-Peek: High Speed Covert Channels in Data Center Networks

Rashid Tahir, **Mohammad Taha Khan**, Xun Gong, Adnan Ahmed, Amiremad Ghassami, Hasanat Kazmi, Matthew Caesar, Fareed Zaffar and Negar Kiyavash

Why is Cloud S… …portant?

…S FORCED TO

EVERNOTE HA…
RESET PASSW…
Trevor Mogg — March 4, 2013

INVESTMENT BANKING | LEGAL/REGULATORY

JPMorgan Chase Hac…

By JESSICA SILVER-GREENBE…

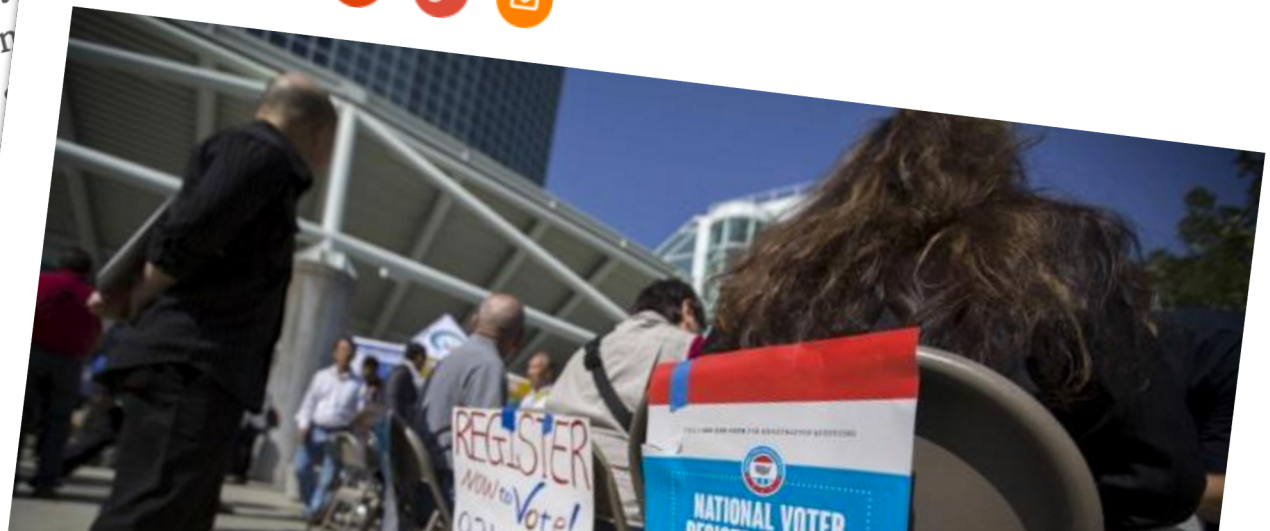
528 Comments

Online Cheating Site AshleyMadison Hacked

…line cheating site **AshleyMadison.com** have been
…claims to have completely compromised the
…proprietary information. The still-
…sers of the hookup service,

Database of 191 million U.S. voters exposed on Interne…

BY JIM FINKLE AND DUSTIN VOLZ



Household…

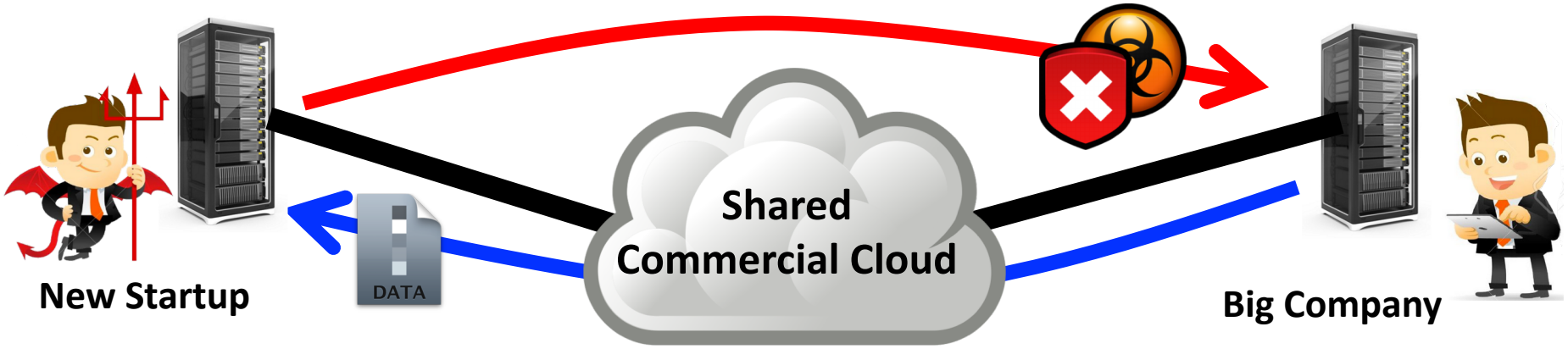
BER 2, 2014 12:50 PM

PHOTOS

Cloud Infrastructure

- Clouds share recourses to achieve **economies of scale**
- Current isolation mechanisms:
  - Hypervisor isolation
  - Fine grained access control
  - Information control flow
- Host based isolation mechanisms; **network is still shared**
- Possibility of **side and covert channel attacks**

Attack Scenario



- Clouds polices restrict communication
- Covert malware can transfer data using shared infrastructure
- Policy violation without cloud knowing

Covert Channels

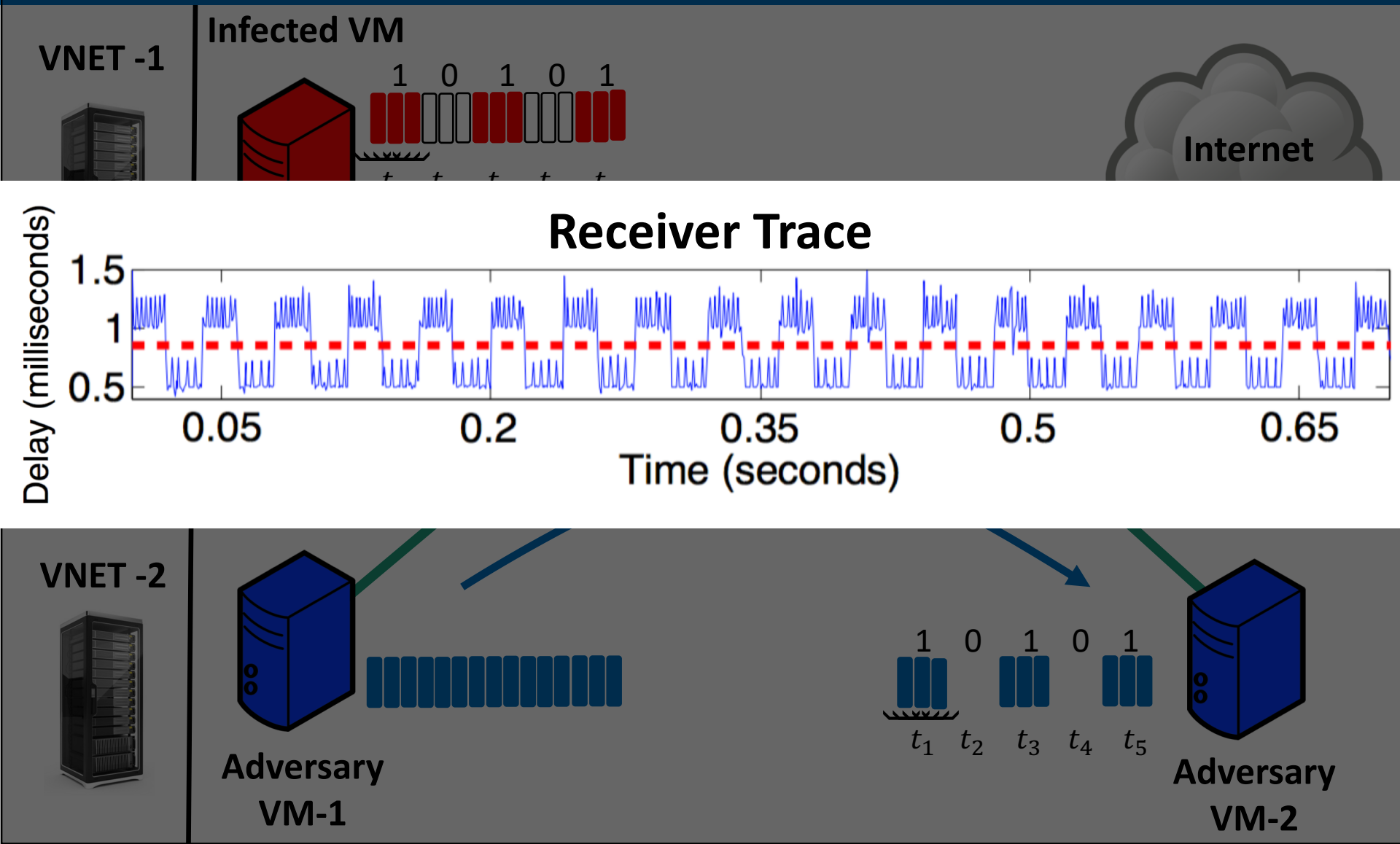
A type of an attack that creates a capability to transfer information between entities that are allowed to communicate directly.

Wikipedia

- Novelty:
  - Real world implementation
  - High Bandwidth
  - Low detectability
  - Practical defenses

- Our Model:
  - Entities: VMs on different virtual networks
  - Timing based covert channel
  - Inter packet delays
  - Shared queues

Simplistic Channel Model



Evaluation Platforms

- In-house Dumbbell Tested
  - 1GB links
  - GREENnet 8 port Full-Duplex Switch

- UIUC Oceans Tested
  - Pica8 Pronto 3290 switches

OCEAN

- Datacenter Networks
  - Emulab
  - Microsoft Azure
  - Amazon EC2

emulab
the utah network testbed

Microsoft Azure

amazon web services™ EC2

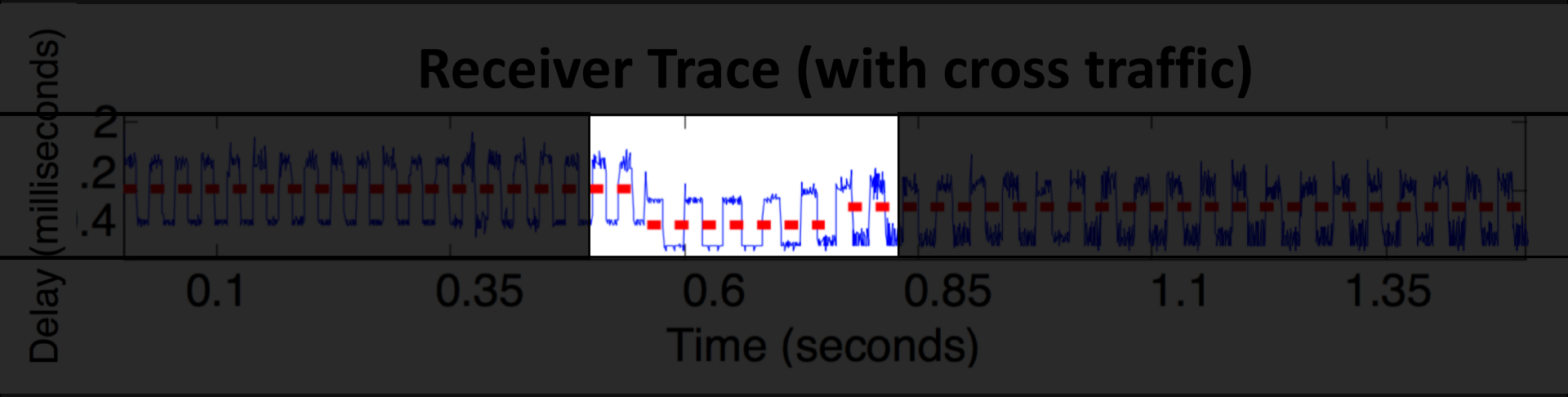
Challenges…

- Dealing with **cross traffic**
- Achieving **synchronization**
- Acquiring **co-resident links**
- Remaining **undetectable**
- Robustness in varying **networking configurations**

Adaptive Decoding Algorithm

Cross traffic sources

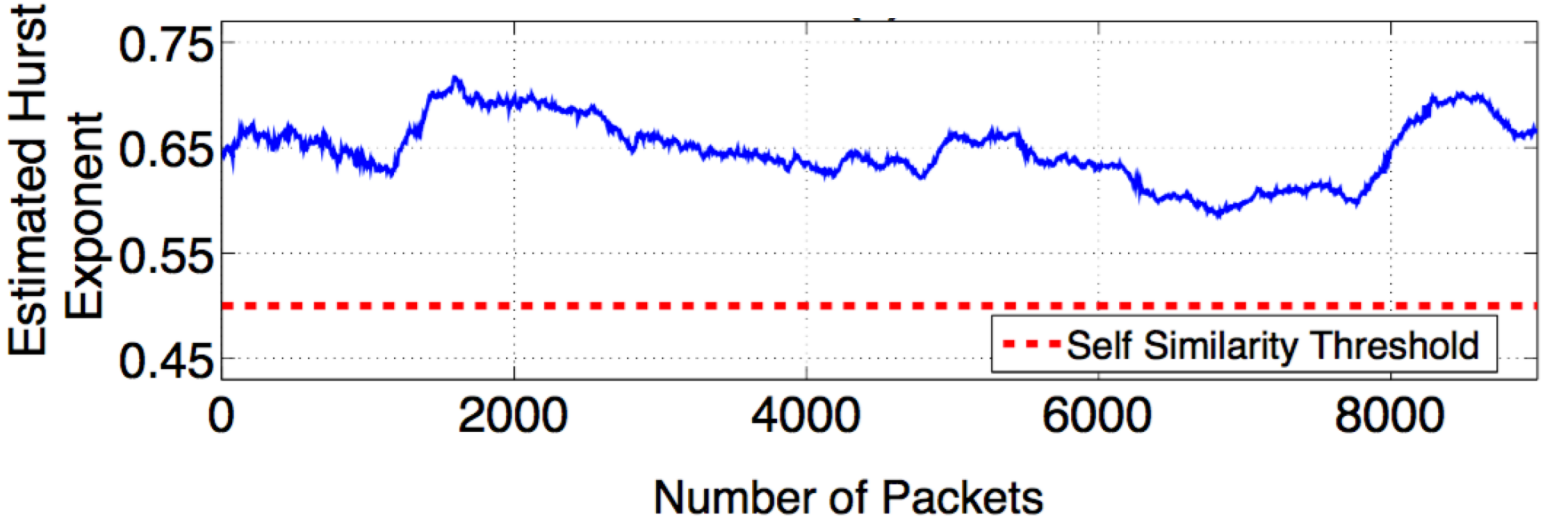
- Actual network traces (*IMC 2010*)



- Issue: Loss of synchronization between sender/receiver
- Solution: Send a preamble to maintain synchronization

Traffic Trace Logs: Network Traffic Characteristics of Data Centers in the Wild, *IMC 2010*

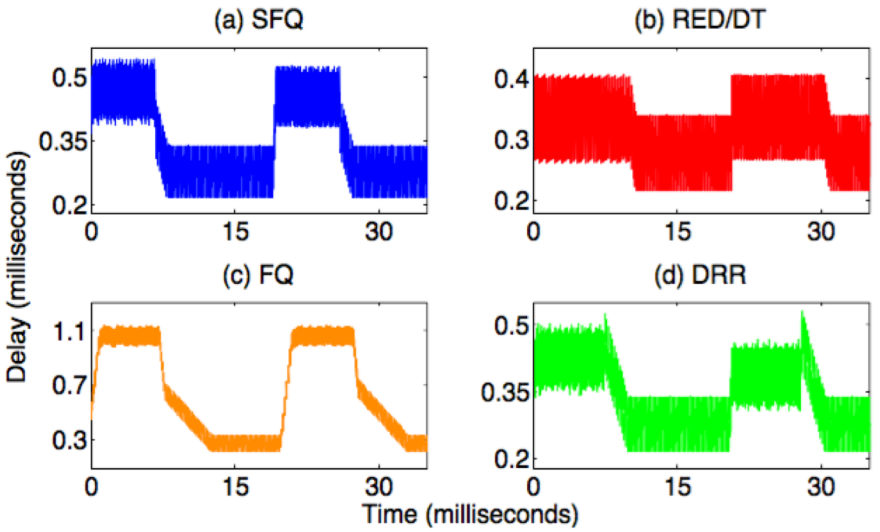
Covert Channel Detectability



- Datacenter traffic is of self similar nature
- Evaluate channel detectability using the **Hurst Parameter**
- A value of > 0.5 indicates that covert traffic in undetectable

Effect of Queuing Policy

- Queuing Mechanisms
  - Stochastic Fair Queuing
  - Drop Tail
  - Fair Queuing
  - Deficit Round Robin



- Run NS2 simulations for evaluation purposes
- Channel operation remains consistent

Achieved Bitrates

Bit Rate	Error Without Cross Traffic	Error With Cross Traffic + Brute Force Decoding	Error With Cross Traffic + Adaptive Decoding
67	0%	3.30%	0%
134	0%	42.80%	0%
335	0%	> 80%	8.68%

- ***Orange Book:*** *"A covert channel of 100 bits is considered high"*
- 5 minutes of human time for key exfiltration at 100 bits/sec

Mitigation

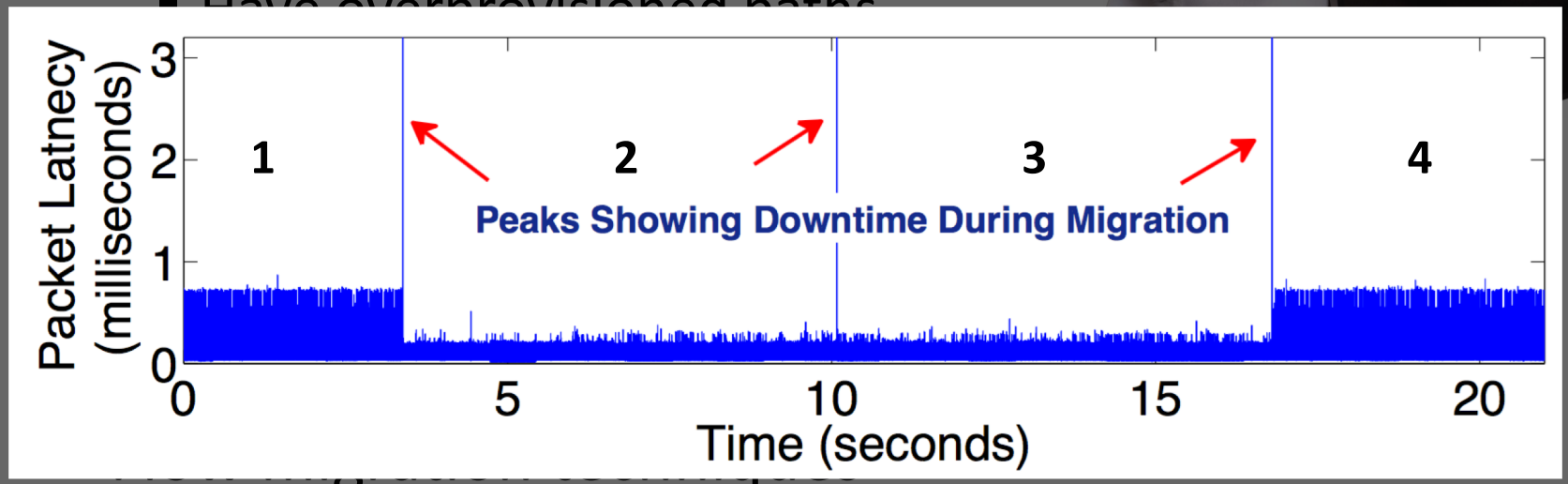
- Current Datacenters:
  - Have overprovisioned paths
  - Perform load balancing

- Our covert channel relies on **co-resident flows**

- Flow migration techniques
  - Random
  - Timing based
  - Self similar

Mitigation

- Current Datacenters:
  - Have overprovisioned paths
  - Use Migration techniques
    - Random
    - Timing based
    - Self similar



Questions?

Current clouds create the illusion of isolation by software mechanisms

Covert channels can leak information by using shared infrastructure

Present a real world covert channel mechanism along with a practical defense mechanism

Rashid Tahir, **Mohammad Taha Khan**, Xun Gong, Adnan Ahmed, Amiremad Ghassami, Hasanat Kazmi, Matthew Caesar, Fareed Zaffar and Negar Kiyavash