Determining a Cache Hit/Miss over RDMA

A NetCAT Replication

Emerson Ford Calvin Lee

CS 6465 - Fall 2019

NetCAT Overview

Claim

Using RDMA over Infiniband, a remote host can measure if a remote memory access is served from LLC or from RAM on a target host with DDIO enabled.

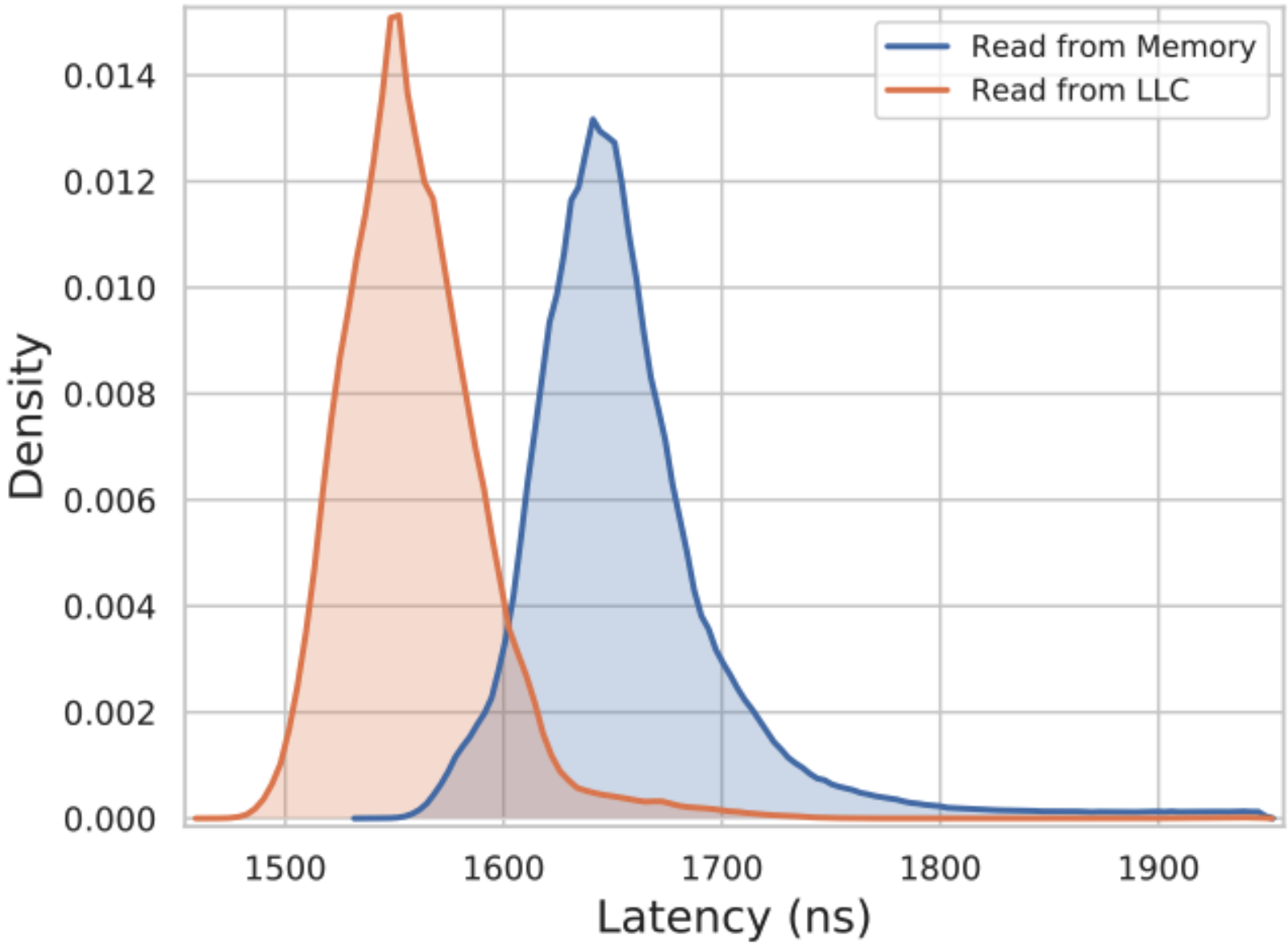
Impact

This enables cache-timing based attacks (such as PRIME+PROBE) over the network which then enables attacks like SSH keystroke timing attacks.

Key Replication Questions

1. Is it actually possible to measure cache hit/cache hit on a remote memory access?
2. If so, can we replicate their method of building a remote eviction set?

Key Graph to Replicate



RDMA Overview

1. Server and client both register memory to be used for RDMA.

Reads

2. Client specifies a remote address and fires off 'READ' verb.
3. Client NIC communicates with remote NIC to read remote memory address (no server CPU involvement).
4. Client NIC places remote memory contents into client's registered memory.

Writes

2. Client alters local registered memory.
3. Client specifies a remote address and fires off 'WRITE' verb.
4. Client NIC communicates with remote NIC to write local memory contents at remote address (no server CPU involvement).

RDMA/DDIO Quirks

1. Reads can be served from LLC or RAM. If served from RAM, the memory is **not** loaded into LLC.
2. Writes will load memory into the LLC.
3. DDIO is “restricted to 10% of the last-level cache”.

NetCAT Overview