Optimal Monitor Placement Policy Against Distributed Denial-of-Service Attack in Datacenter

Rajorshi Biswas, Jie Wu, and Yang Chen

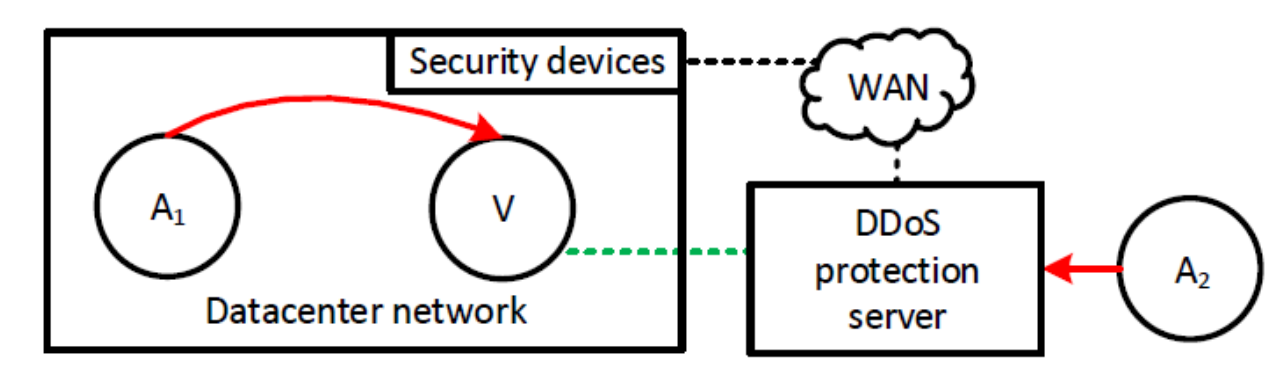
Dept. of Computer and Info. Sciences

Temple University

Outline

- Introduction to internal DDoS attack
- Previous works
- Monitoring system model
- Problem 1: Minimizing network overhead
- Problem 2: Minimizing network overhead with budget
- Simulation results
- Q & A

Internal DDoS attack and Commercial DDoS Protection Service

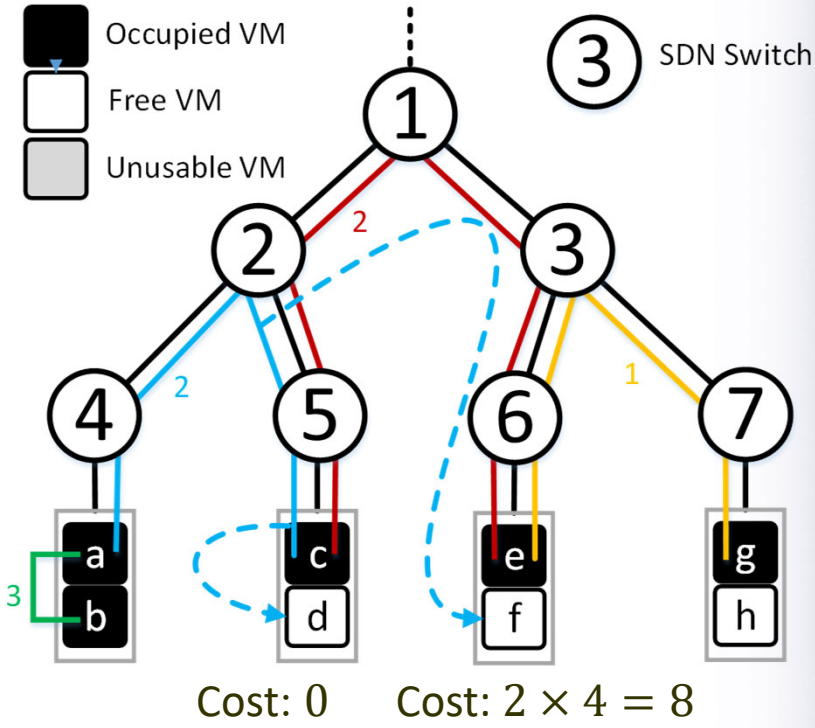


- Victim points their domain to DDoS protection server.
- DDoS protection server – Victim: Secure tunnel
- DDoS protection server
  - Forwards legitimate packets only.

Monitoring all the internal flows is necessary

System Model: Monitoring Internal Flows

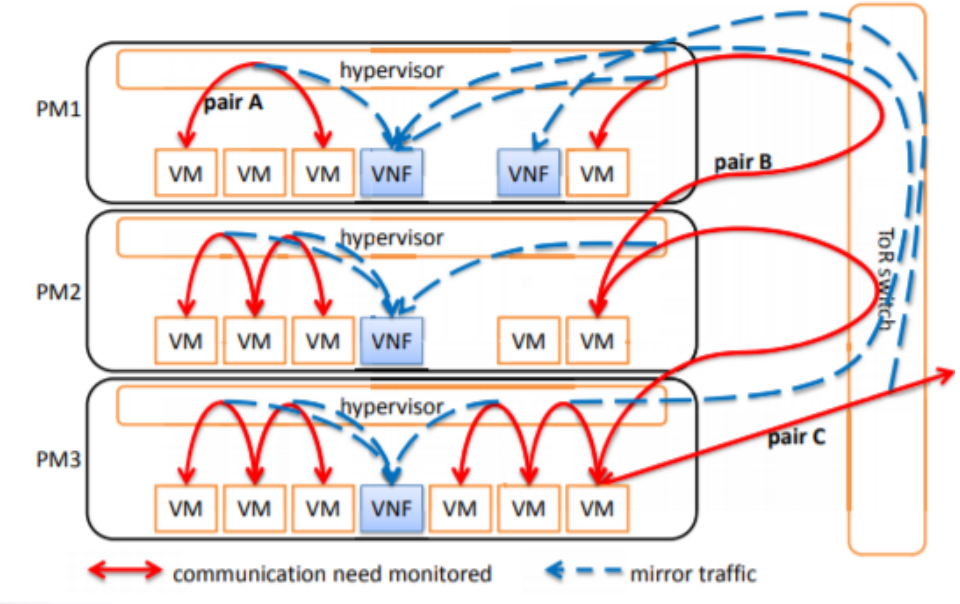
- Every switch is Software Defined Networking (SDN) switch.
- Each flow is copied to monitors.
- Unused VMs are used as monitors.
  - Detect DDoS traffic
  - Send report to controller
- If DDoS is detected:
  - Controller blocks the DDoS from hypervisor of the source



Monitoring cost= bandwidth × # of hops the flow copy travels

Minimize monitoring cost

Previous work



Greedy:
Each flow is monitored in closest monitor.

- Does not consider limited budget on VMs.
- 100% copy of flows cannot guarantee monitoring of all flows.

Optimal Placement of Network Security Monitoring Functions in NFV-Enabled Data Centers (P. lin et al. in *(SC2)*, Kanazawa, 2017)

Problem 1: Find Flow Assignment

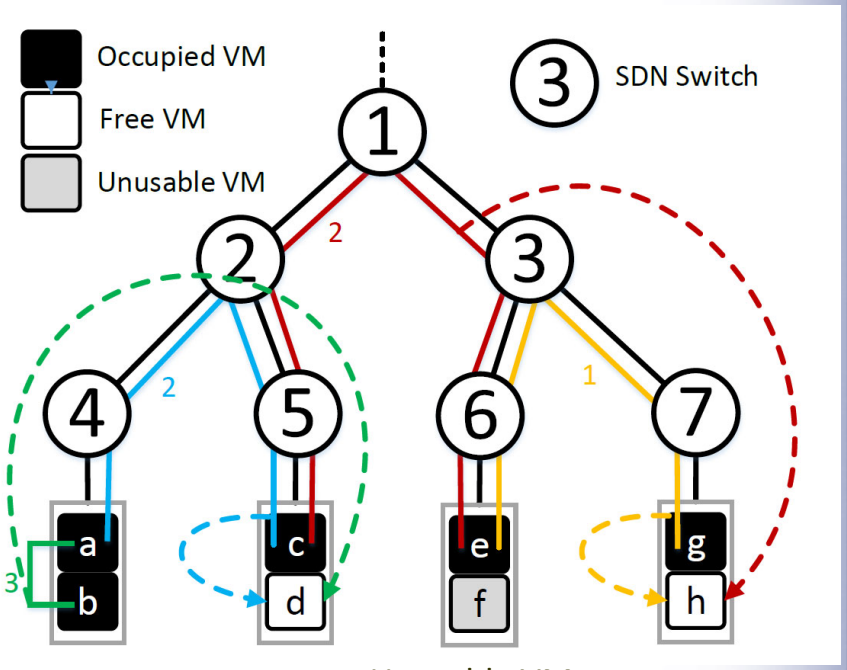
- Given topology, locations/VMs of monitors.
  - Find flow assignment that minimizes cost.
- Cost model
  - $C = \sum$ flow bandwidth × # of hops the flow copy travels
- Constraint
  - VM capacity ≥ number of assigned flows

Required capacity: $\left\lceil \frac{M}{K} \right\rceil$ flows

M: number of unused VM

K: budget for monitors

Monitor capacity: 2 flows



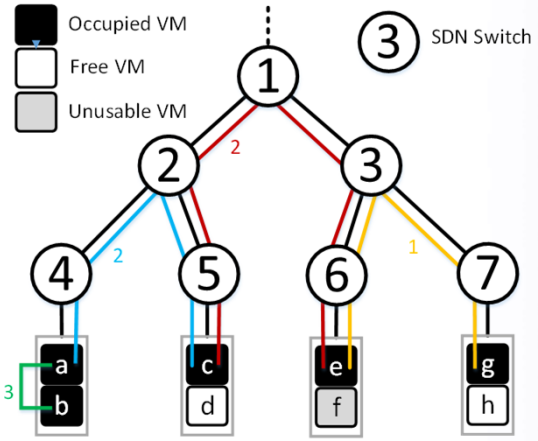
Unusable VM

If required capacity > actual capacity: partially copy flow

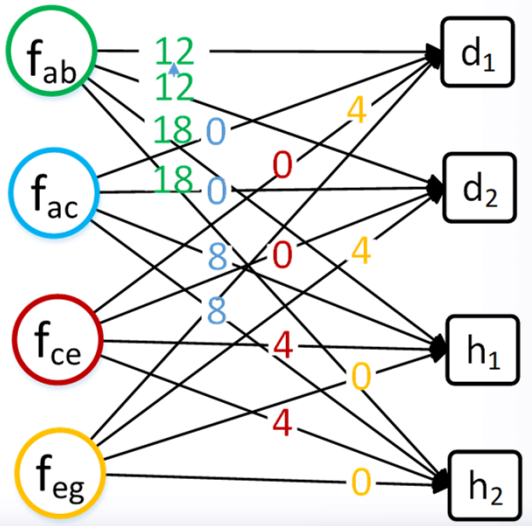
Monitoring cost: 12+0+0+4=16

Solution Steps

- Step 1: Create bipartite graph
  - Partition unused VMs.
  - Calculate cost between flow and VM.
- Step 2: Create flow graph
  - Add source and destination.
  - Set cost = 0 for new edges.
- Step 3: Find minimum cost maximum flow.
  - Cheapest augmenting path

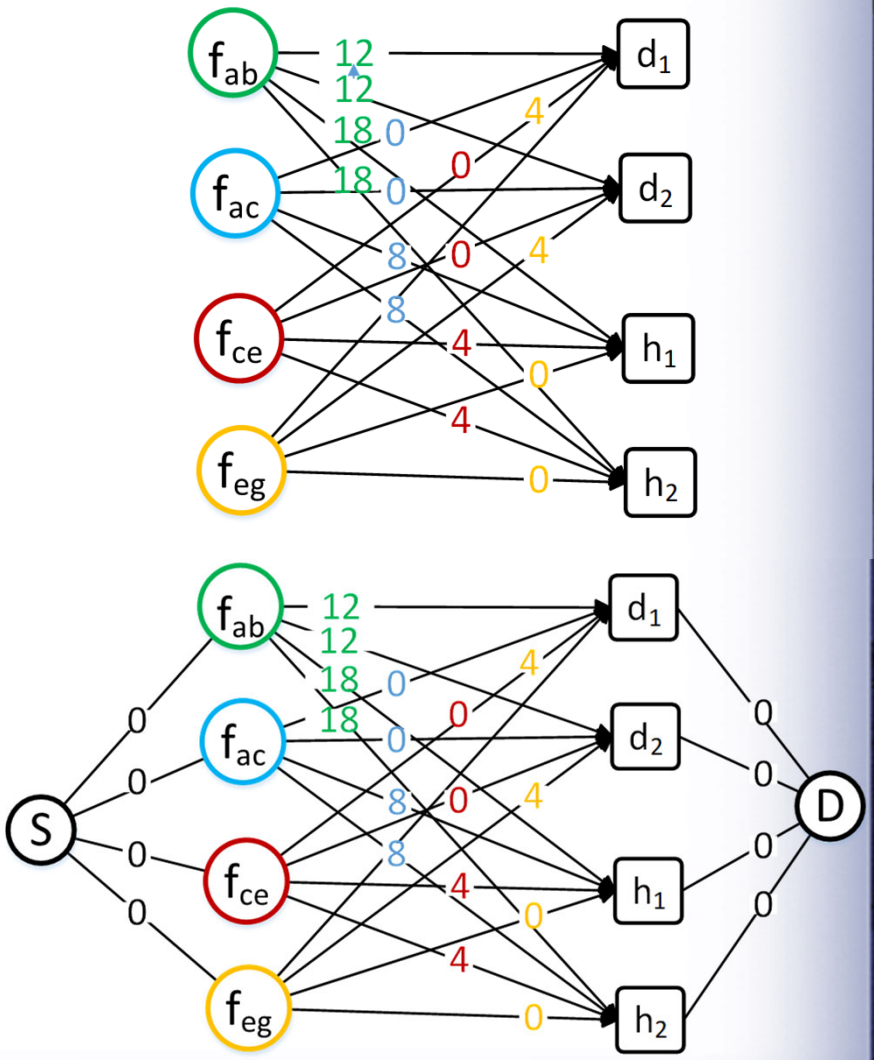


# of partitions=capacity



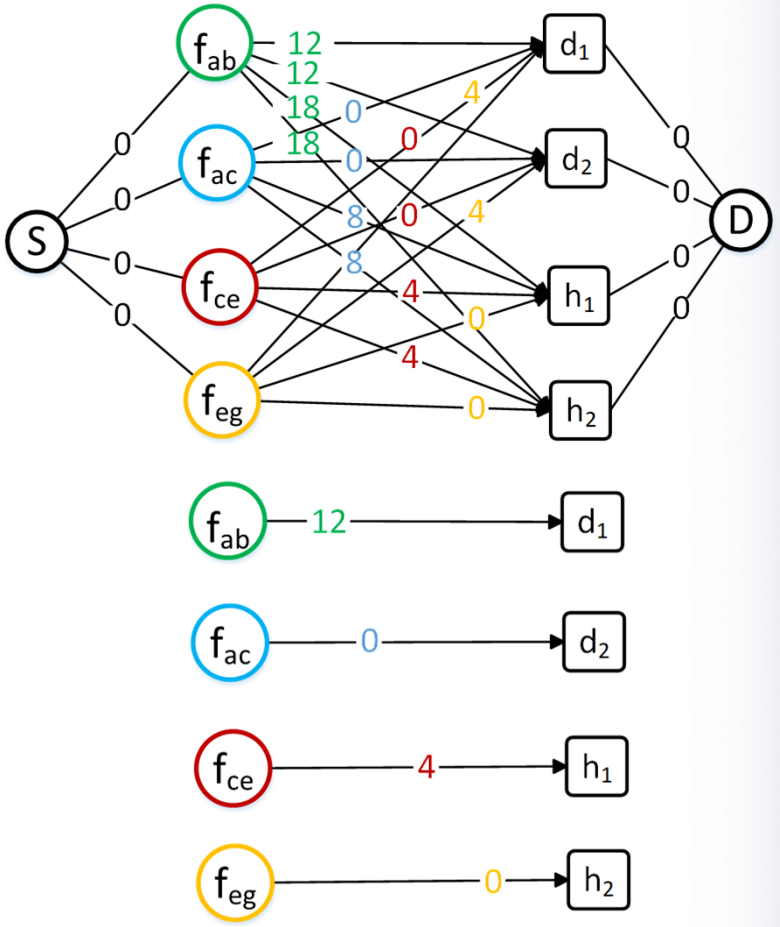
Solution Steps

- Step 1: Create bipartite graph
  - Partition unused VMs.
  - Calculate cost between flow and VM.
- Step 2: Create flow graph
  - Add source and destination.
  - Set cost = 0 for new edges.
- Step 3: Find minimum cost maximum flow
  - Cheapest augmenting path



Solution Steps

- Step 1: Create bipartite graph
  - Partition unused VM. according to capacity.
  - Calculate cost between flow and VM
- Step 2: Create flow graph
  - Add source and destination.
  - Set cost = 0 for new edges.
- Step 3: Find minimum cost maximum flow
  - Cheapest augmenting path

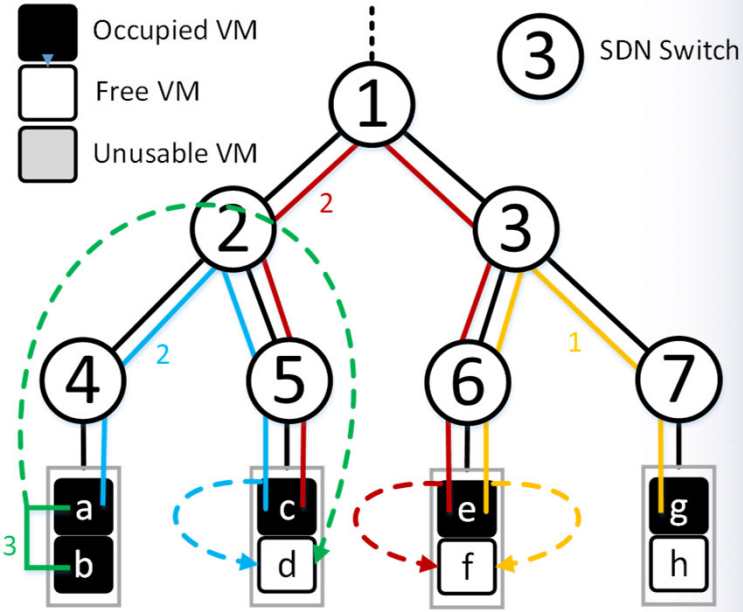


Complexity: $O(M^3 + S^3)$

M: # of unused VMs, S: # of SDN switches

Problem 2: Find Flow Assignment (Limited Budget)

- Given topology, number of VMs K
  - Find flow assignment that minimizes cost.
  - **Find K locations**
  - Find assignment (problem 1)
- Cost model
  - $C = \sum$ flow bandwidth $\times$ # of hops the flow copy travels
- Constraint
  - VM capacity $\geq$ number of assigned flows
- Best assignment:
  - $f_{ab} \rightarrow d, f_{ac} \rightarrow d, f_{ce} \rightarrow f, f_{eg} \rightarrow f$



Monitoring cost:
12+0+0+0=12

Solution Steps: M/K-lowest cost (MKLC)

- Step 1: Create cost matrix.
  - Find M/K-lowest cost.
- Step 2: Find assignment using problem 1
- Complexity: $O(M^3 + S^3)$
  - M=number of VMs
  - S=number of SDN switches

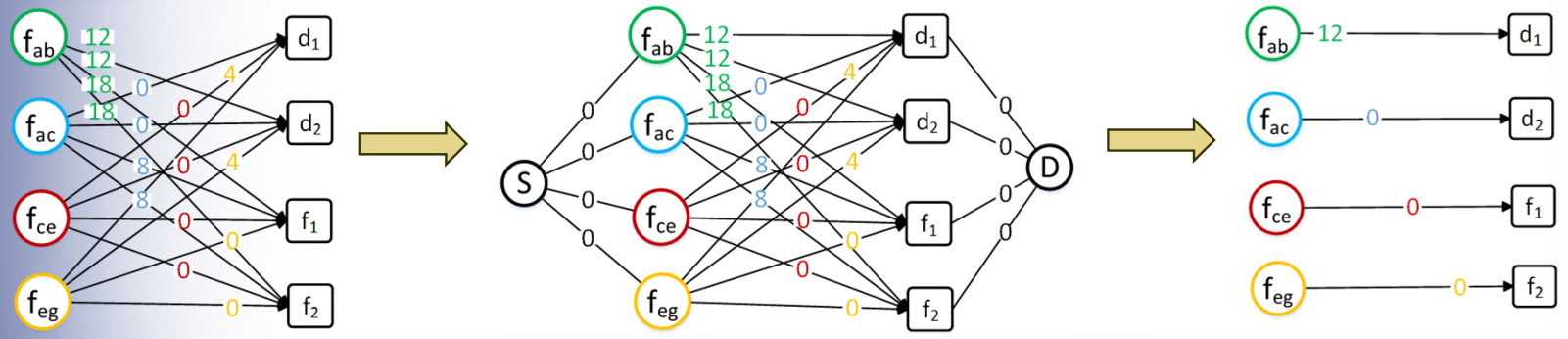
M=3, K=2
Monitor capacity required: 2

	d	f	h
f_{ab}	12	18	18
f_{ac}	0	8	8
f_{ce}	0	0	4
f_{eg}	4	0	0

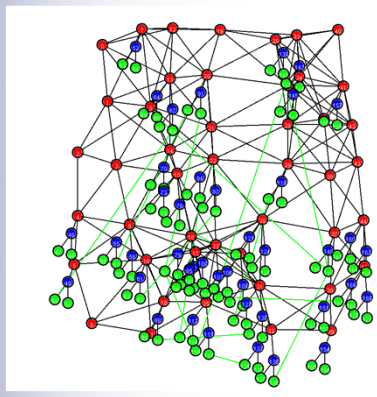
Cost matrix

2-lowest cost	0	0	4

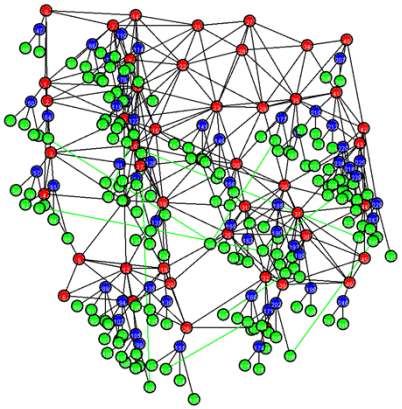
Selected VMs {d, f}



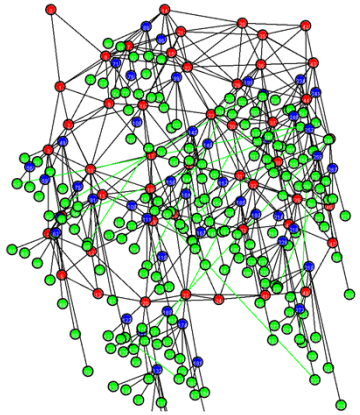
Simulation: Randomly Generated Topologies



Topology I
Nodes: 172
VMs/PMs: 84/43
SDN SWs: 46
Links: 304



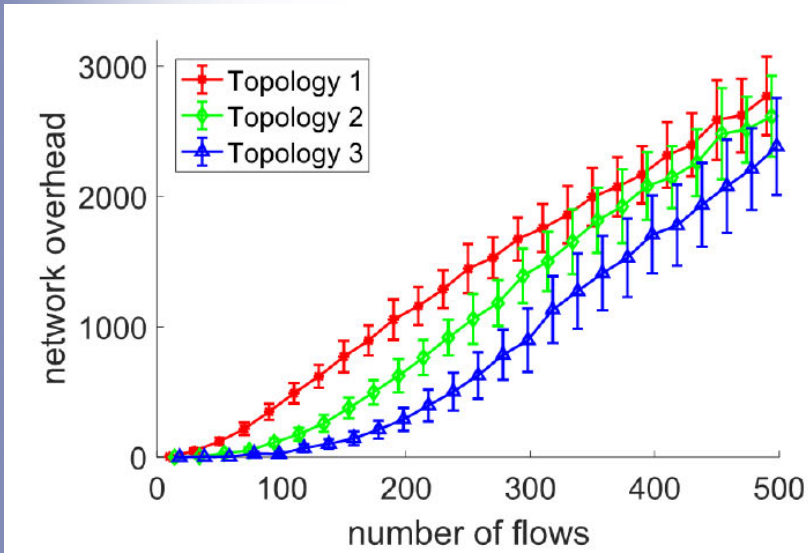
Topology II
Nodes: 249
VMs/PMs: 150/52
SDN SWs: 47
Links: 392



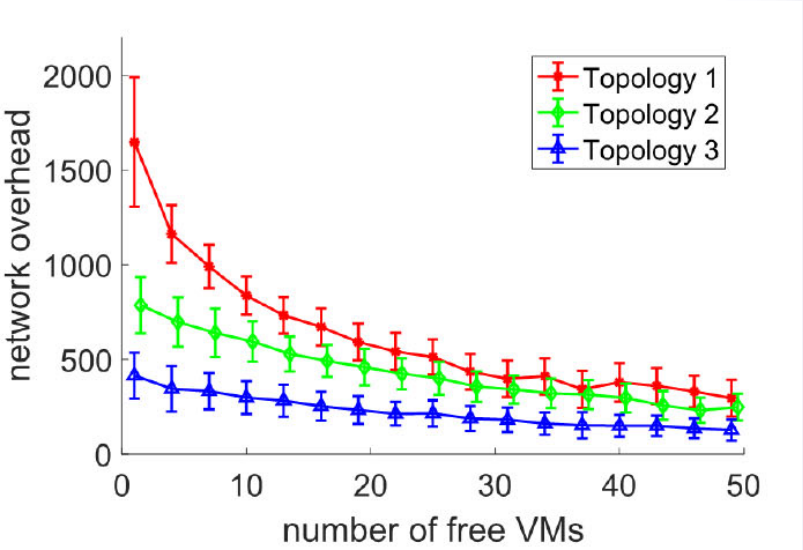
Topology III
Nodes: 277
VMs/PMs: 184/44
SDN SWs: 49
Links: 427

Unite disk graph, Randomly placed nodes (uniform), Randomly generated flows
Area: 500x500, Neighborhood radius: 70

Simulation: Different Number of Flows and Unused VMs

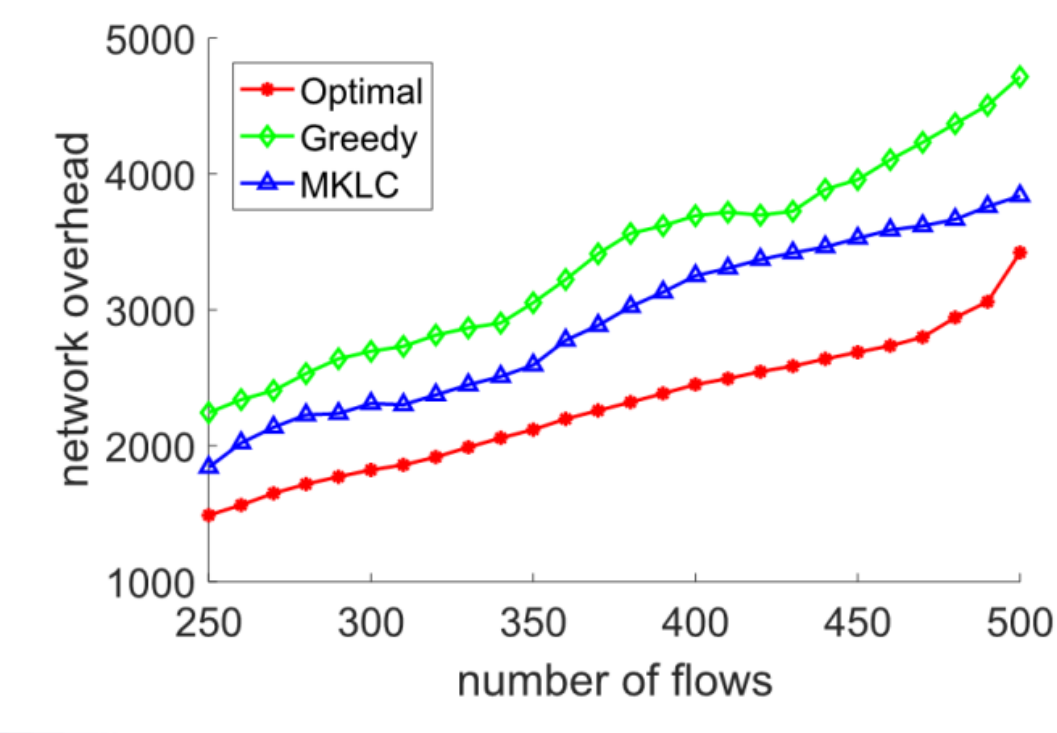


Network overhead linearly increases with the number of flows.
Number of free VMs=20



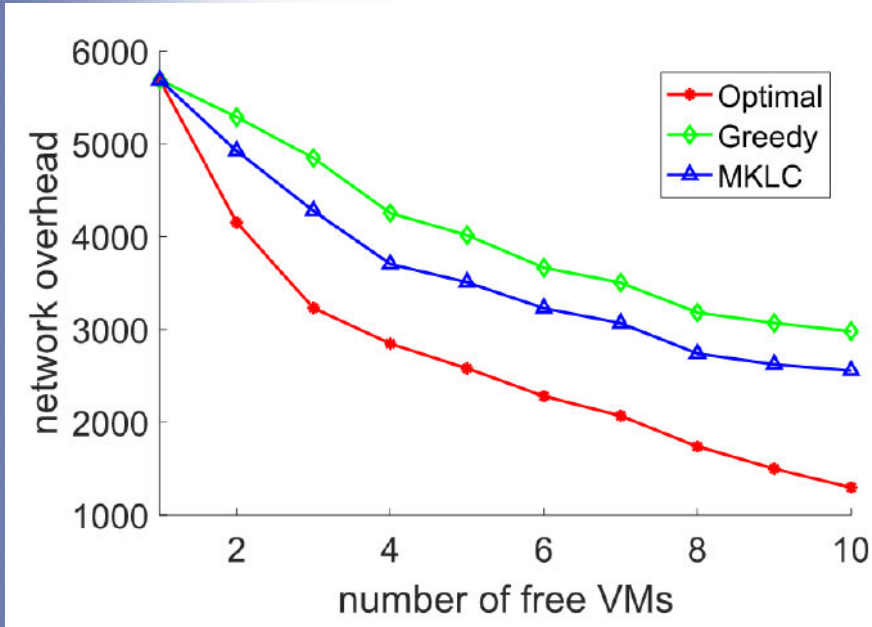
Network overhead decreases with the number of unused VMs.
Number of flows= 500

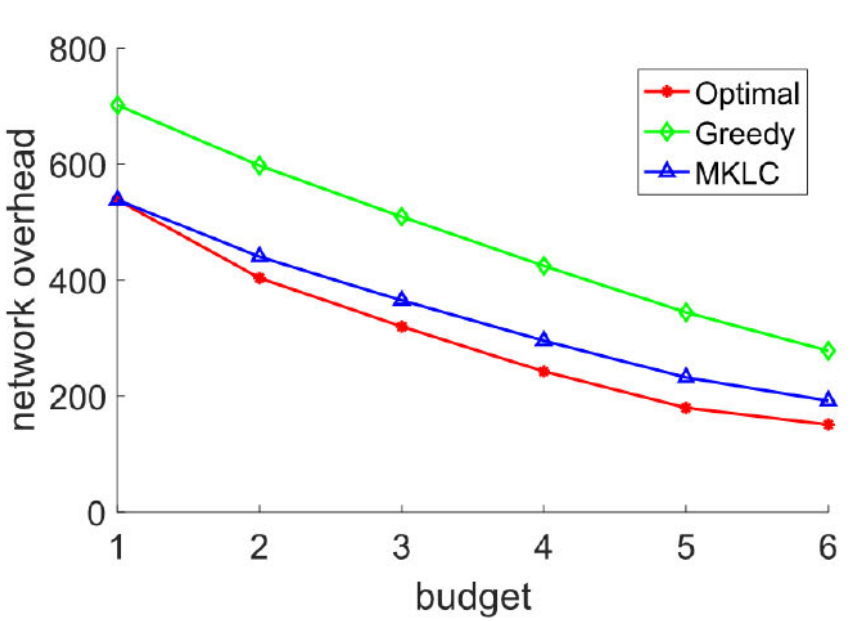
Simulation: Comparison with Existing Solutions



MKLC network overhead 27% is higher than optimal.
Greedy network overhead 48% is higher than optimal.

Simulation: Comparison with Existing Solutions

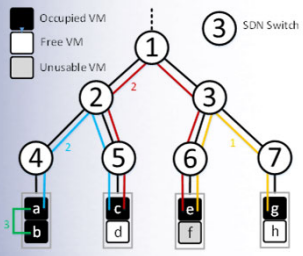




MKLC network overhead is lower than Greedy network overhead.

Summary

Our proposed M/K lowest cost approach can produce less network overhead is lower than the existing greedy approach.

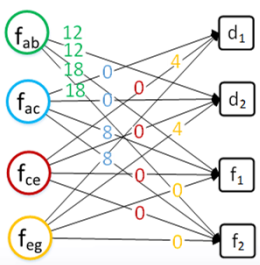


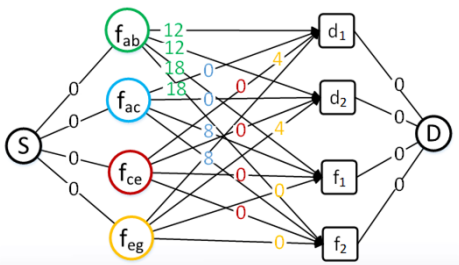
	d	f	h
f_{ab}	12	18	18
f_{ac}	0	8	8
f_{ce}	0	0	4
f_{eg}	4	0	0

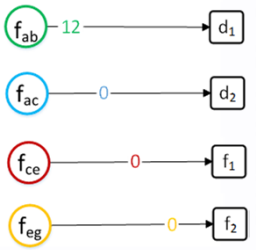
Cost matrix

2-lowest cost	0	0	4

Selected VMs {d, f}







Q & A ???