Cost-Aware Optimal Filter Assignment Policy Against Distributed Denial-of-Service Attack

Rajorshi Biswas, Jie Wu, and Avinash Srinivasan

Dept. of Computer and Info. Sciences

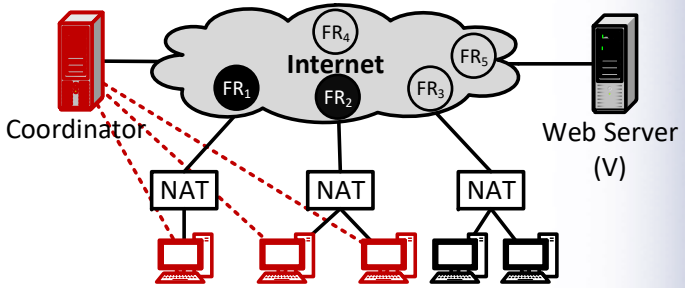
Temple University

Outline

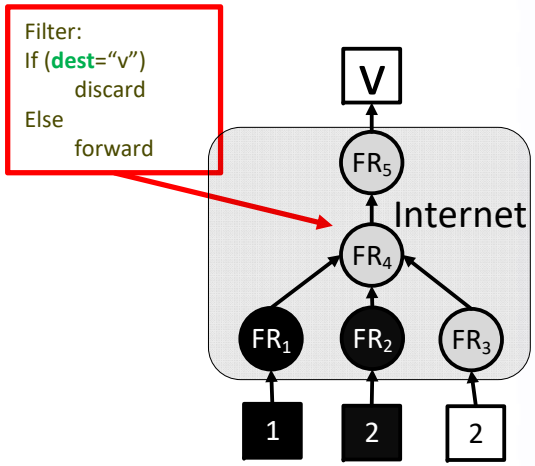
- Introduction to DDoS attack and filter router
- Previous works
- Four phase DDoS protection system model
- Problem: Minimizing blocked legitimate user
- Dynamic programming solution
- Simulation results
- Q & A

DDoS & Four-phase Protection System

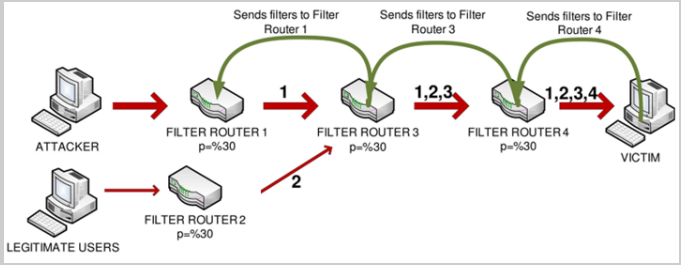
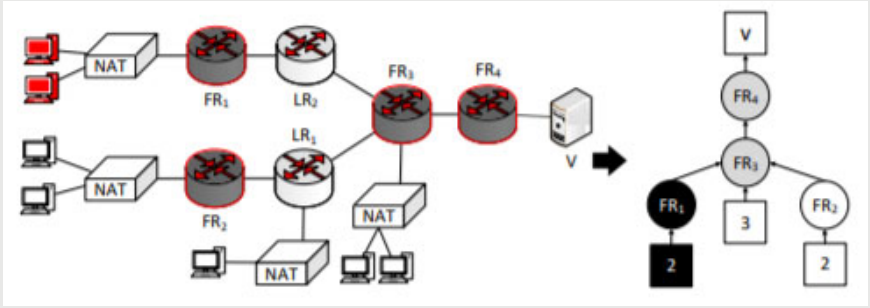
- DDoS
  - Attacker keeps the victim busy.
  - Millions of requests are fired by bots.
  - Bots are controlled by a master.



- Background
  - Filter router
    - Does packet marking.
    - Apply filter and block traffic according to filter.
  - Filter
    - Simple packet blocking rule.
    - Source-based, **destination based**.

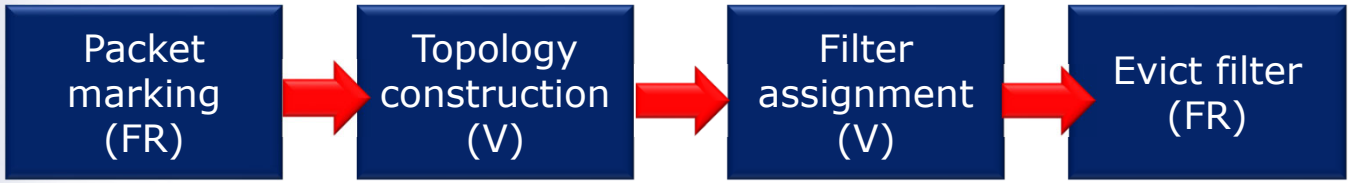


Previous work

Systems	Limitations
Probabilistic Filter Scheduling (packet marking)  PFS: Probabilistic filter scheduling against distributed denial-of-service attacks (D. Seo et al. in IEEE 36th Conf. Local Comput. Netw, Oct. 2011)	• Does not consider limited budget on filters. • Filter propagation takes some time. • Hard to send huge number of filters.
Filter Scheduling (block all attack traffic)  Filter Assignment Policy Against Distributed Denial-of-Service Attack (R. Biswas et al. in IEEE ICPADS, Dec. 2018,)	• Cannot assign filter optimally. • Blocking of all attack traffic increase blocking of legitimate users.

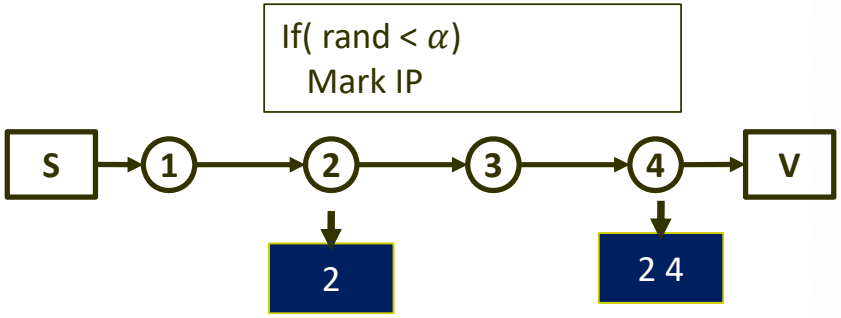
A Four-phase Protection Process

- Phase I: Packet marking by Filter Router.
- Phase II: Traffic topology and filter construction.
- Phase III: Assign filters to filter router.
- Phase IV: Evict unused filter from filter router.

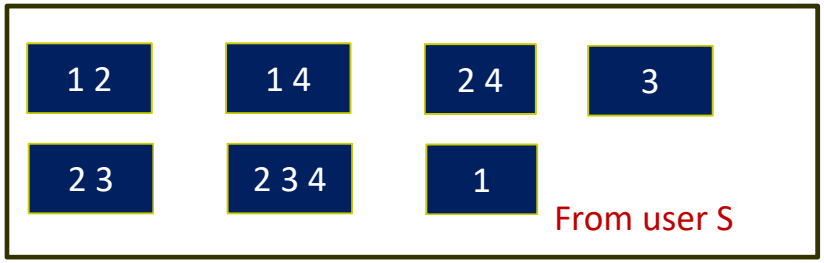


Phase I: Packet Marking by FR

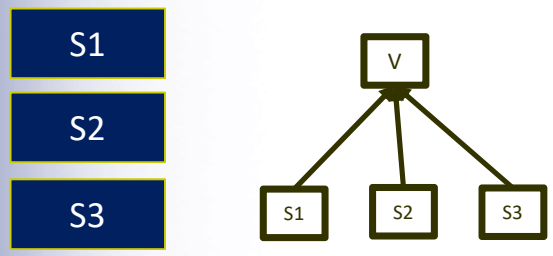
- Filter router (FR) probabilistically appends it own IP address to the packet.
- α = marking probability



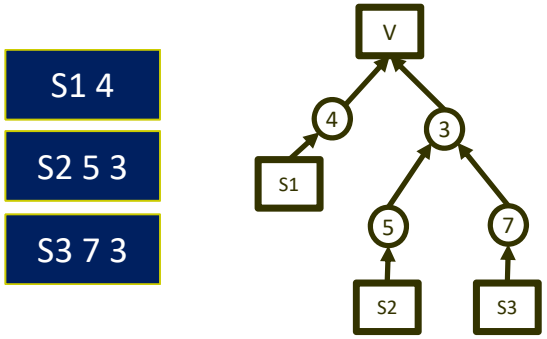
Example received packets, $\alpha = 0.5$



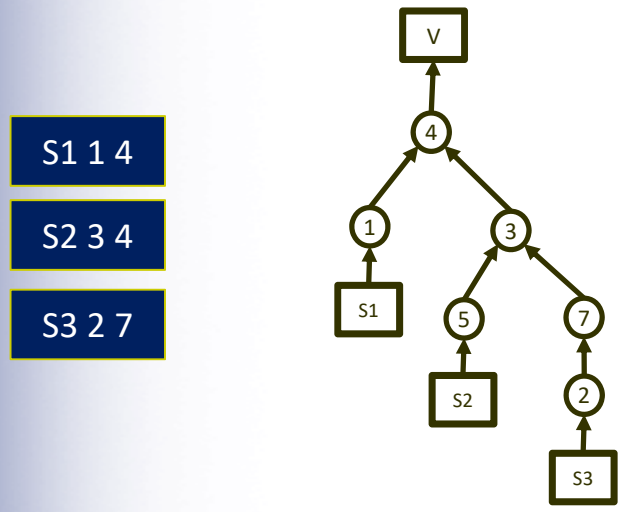
Phase II: Topology Construction



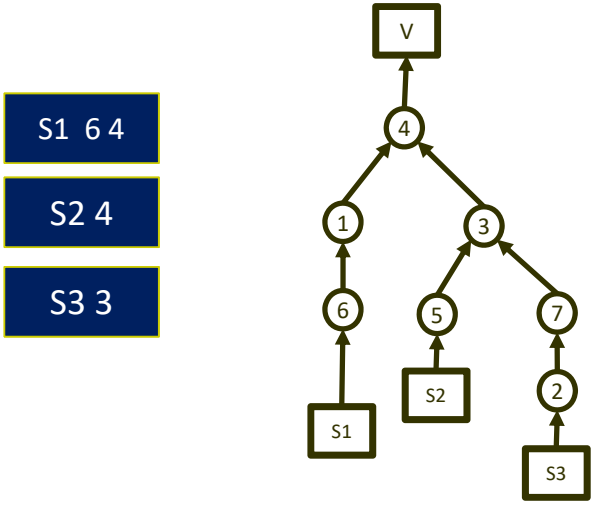
Without any marking



After few marking received



After few more marking received

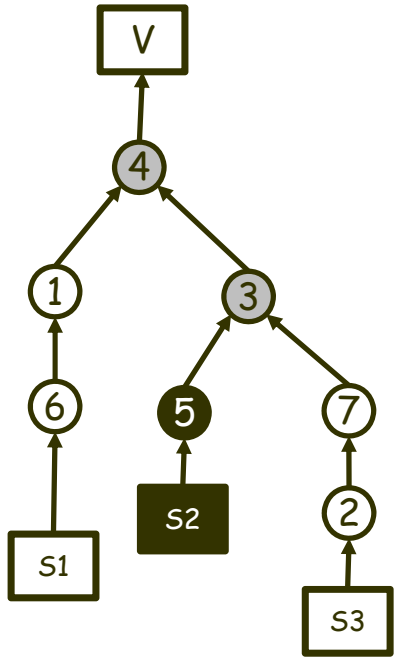


After some more marking received

Identifying Attackers' IP

- Victim can identify attacker.
  - Statistical approaches, packet arrival time, entropy, etc.

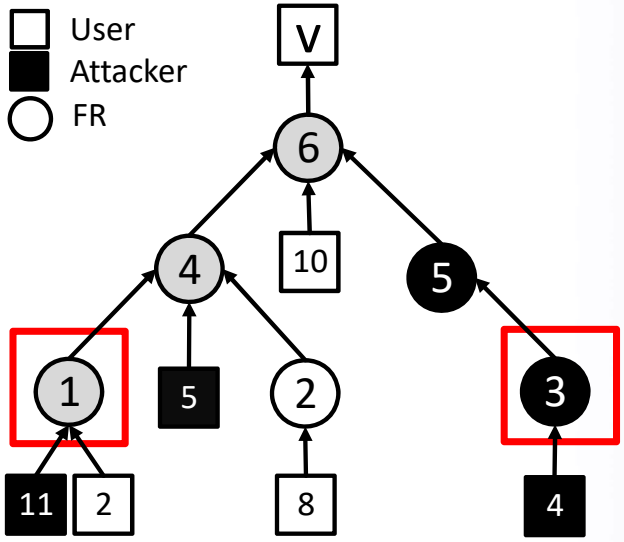
Black: only attacker traffic
White: only legitimate traffic
Gray: mixed traffic



Sending filters to large # of FR takes long time. The ISP of FR may charge money.

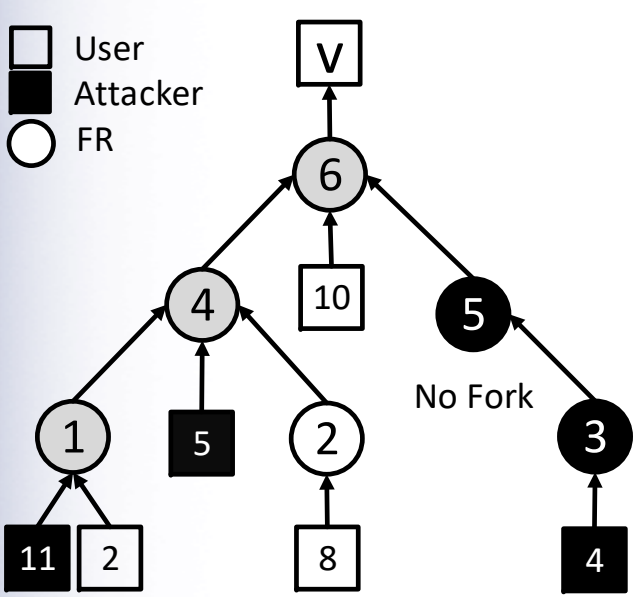
Problem: Minimizing Blocked Legit Users

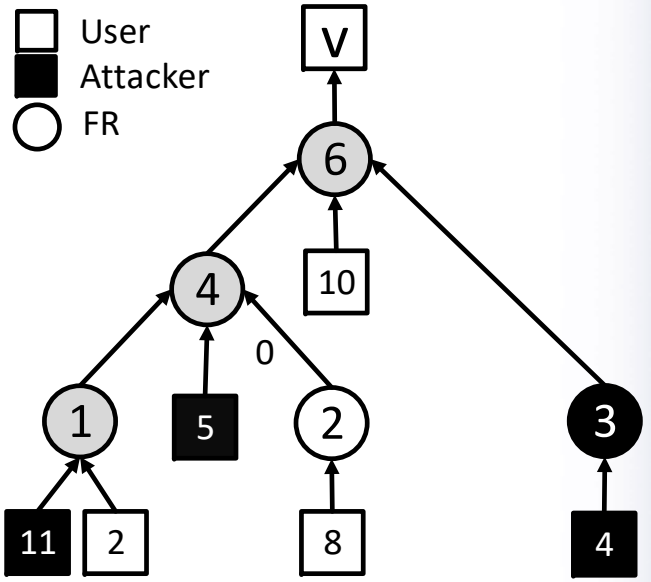
- Given topology, select K filters so that C is minimum.
- Cost model
  - C = Number of blocked legit user
- Constraint
  - Yielded traffic <= bandwidth of victim
- Best assignment for k=2 is $\{1,3\}$
  - $C = 2$, Yielded traffic= 23



Bandwidth =25

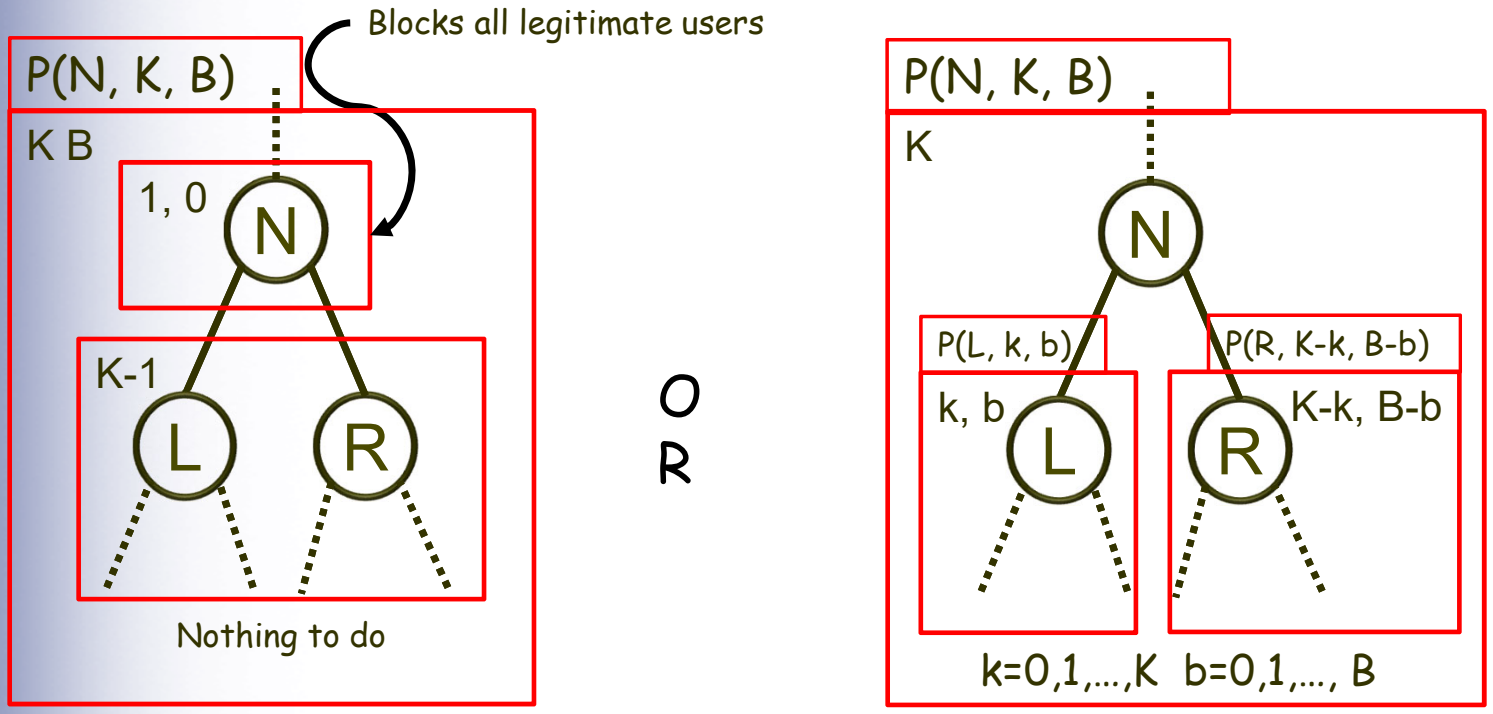
Simplifying the Topology





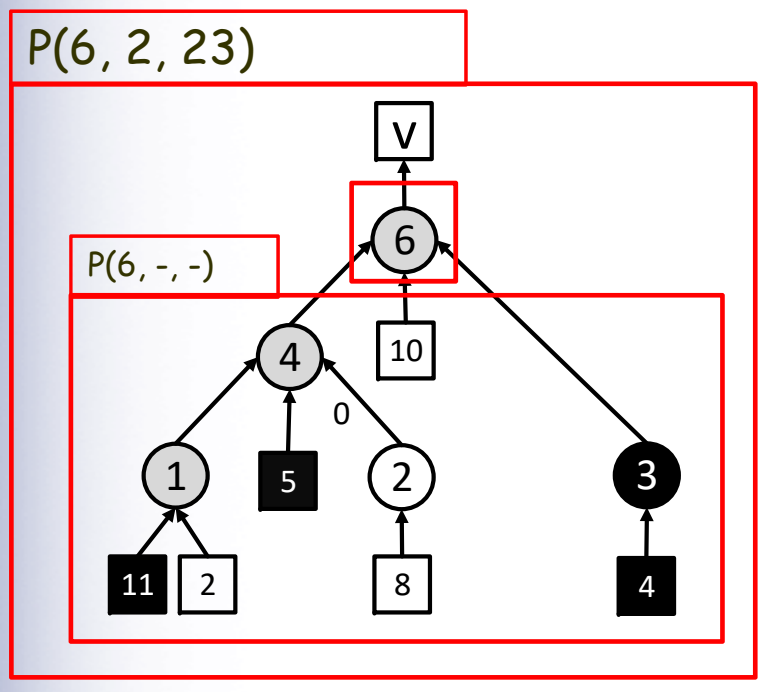
- Remove nodes with no fork.

A dynamic programming solution

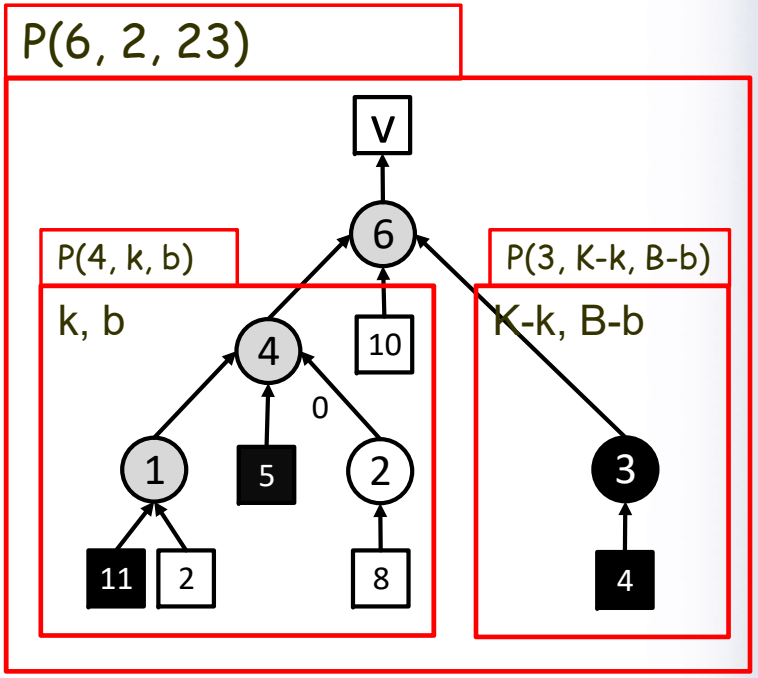


In subtree rooted by N : P(N, K, B)= Minimum blocked LU for K filters by yielding B traffic.
Complexity: $O(N(KB)^{(D-1)})$

A Dynamic Programming Solution: An Example



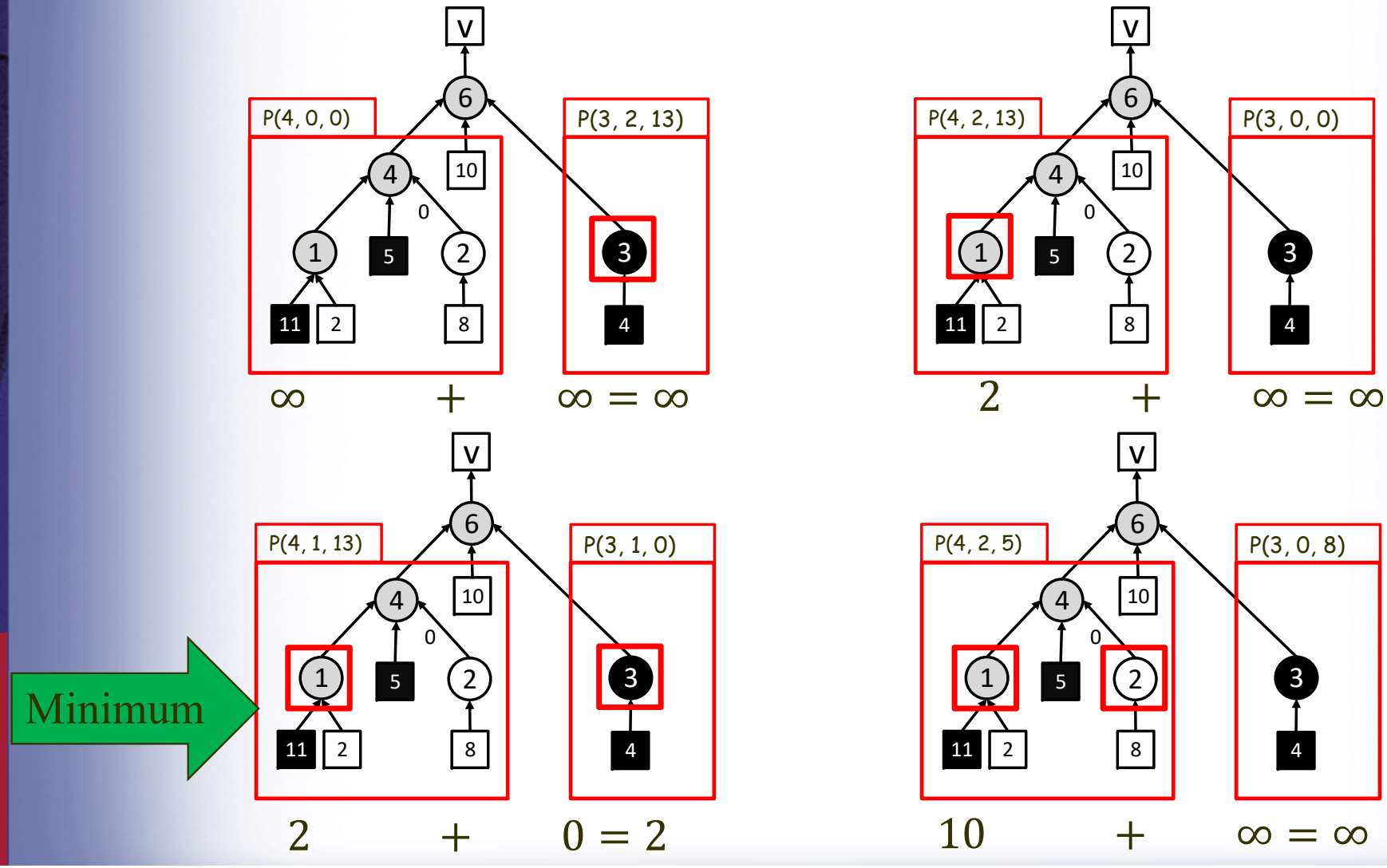
$C = 20$



k=0,1,2 b=0, 1,2,….,13=23-10

$C = 2$

A DP Solution: An Example



Simulation: Random Tree Generation

Tree(d, n)

If d=0

Return.

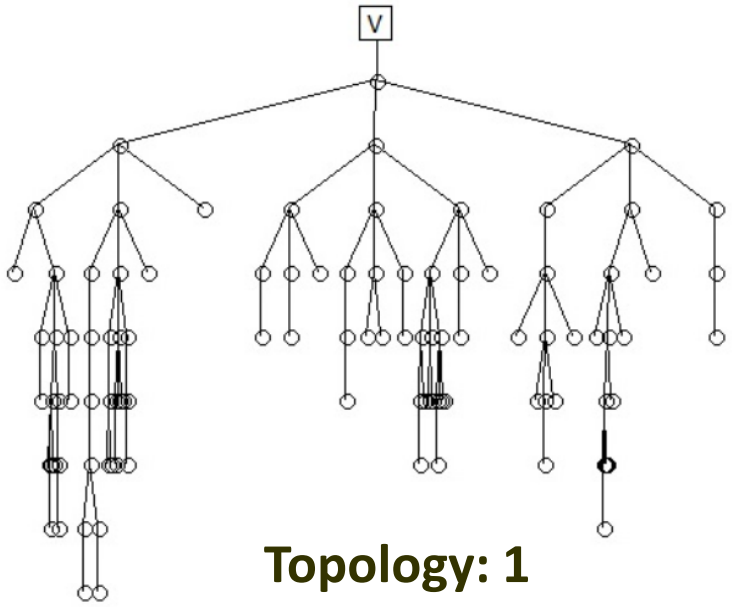
Else

For i=0 to rand [0, Δ]

Create node c_i.

Make c_i child of n.

Tree(d-1, c_i)



Topology: 1

Topology: 1

# of nodes : 100

Internal user probability: 0.1

Max node degree= 3

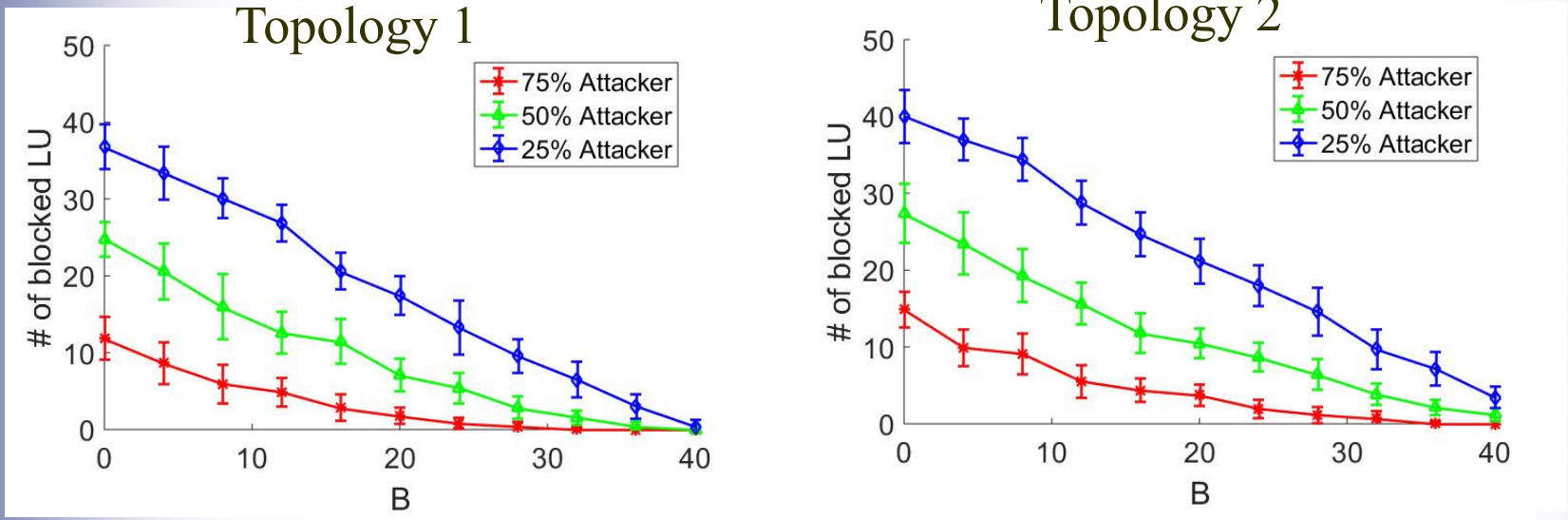
Topology: 2

# of nodes : 400

Internal user probability: 0.1

Max node degree= 20

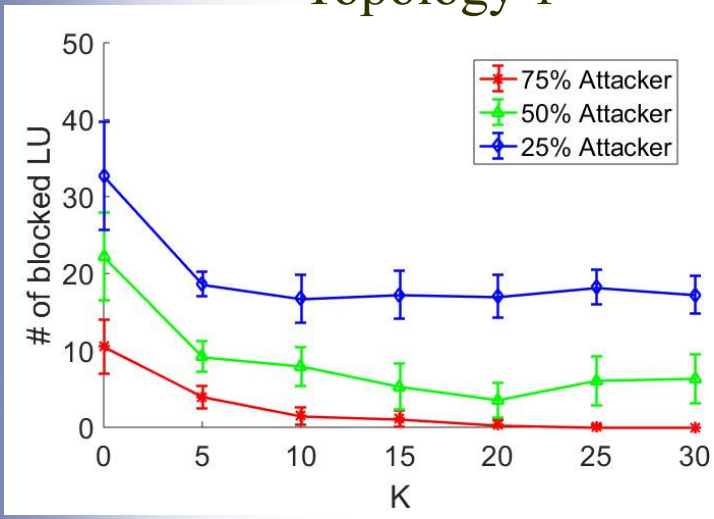
Simulation: Different Number of Filters



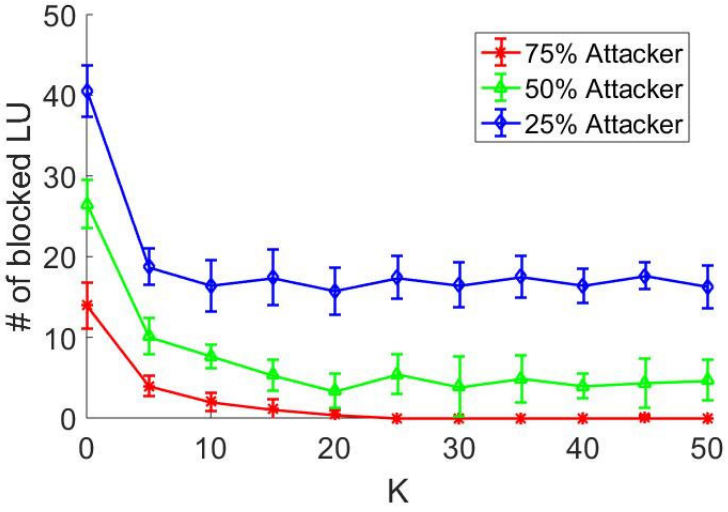
Number of blocked LUs decreases linearly with the increase of B.
The higher the number of attackers the higher the number of blocked LU.

Simulation: Different Incoming Bandwidth

Topology 1

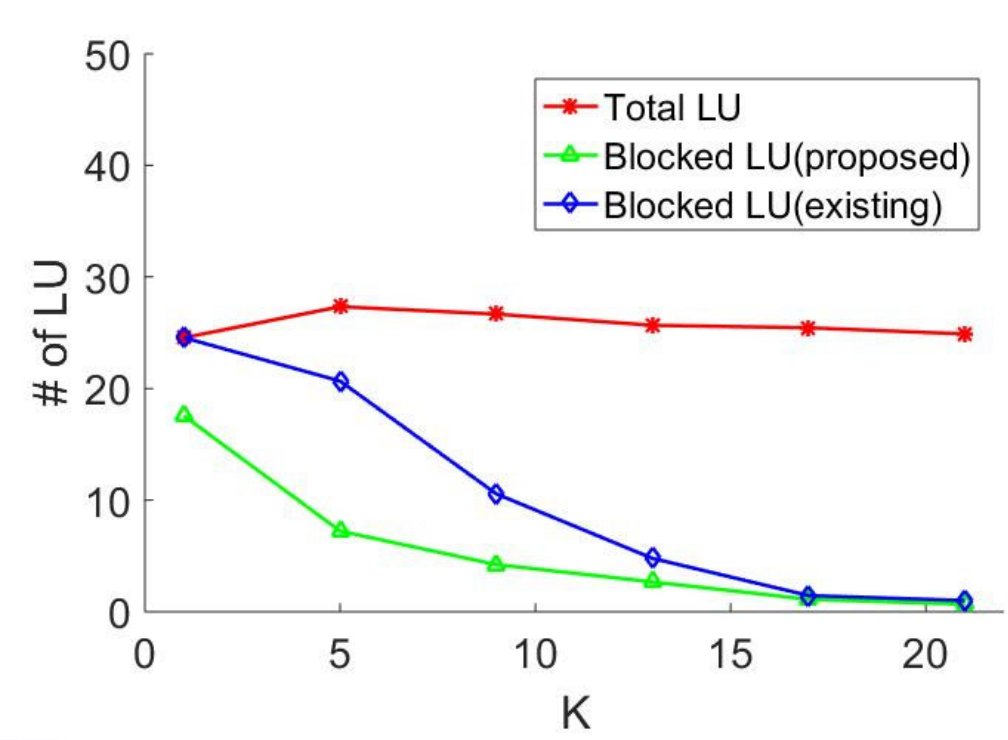


Topology 2



Number of blocked LUs decreases with the increase of K.
Number of blocked LU becomes stable after a certain value of K.

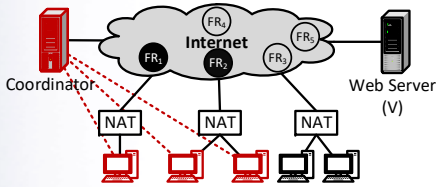
Simulation: Compare with Existing Work

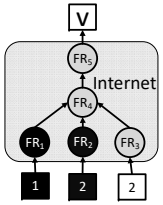


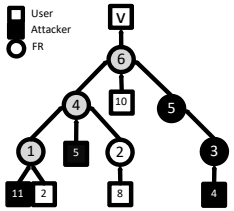
Number of blocked LUs in proposed system is less than the existing system.

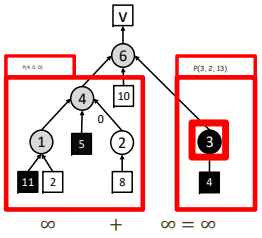
Summary

By allowing some attacker to reach victim we can significantly decrease the number of blocked legitimate user.









Thank You

Q & A !!!