

DefCOM against DDoS Attacks

PI: Jelena Mirković, NSL, University of Delaware

Co-PI: Peter Reiher, LASR, University of California at Los Angeles

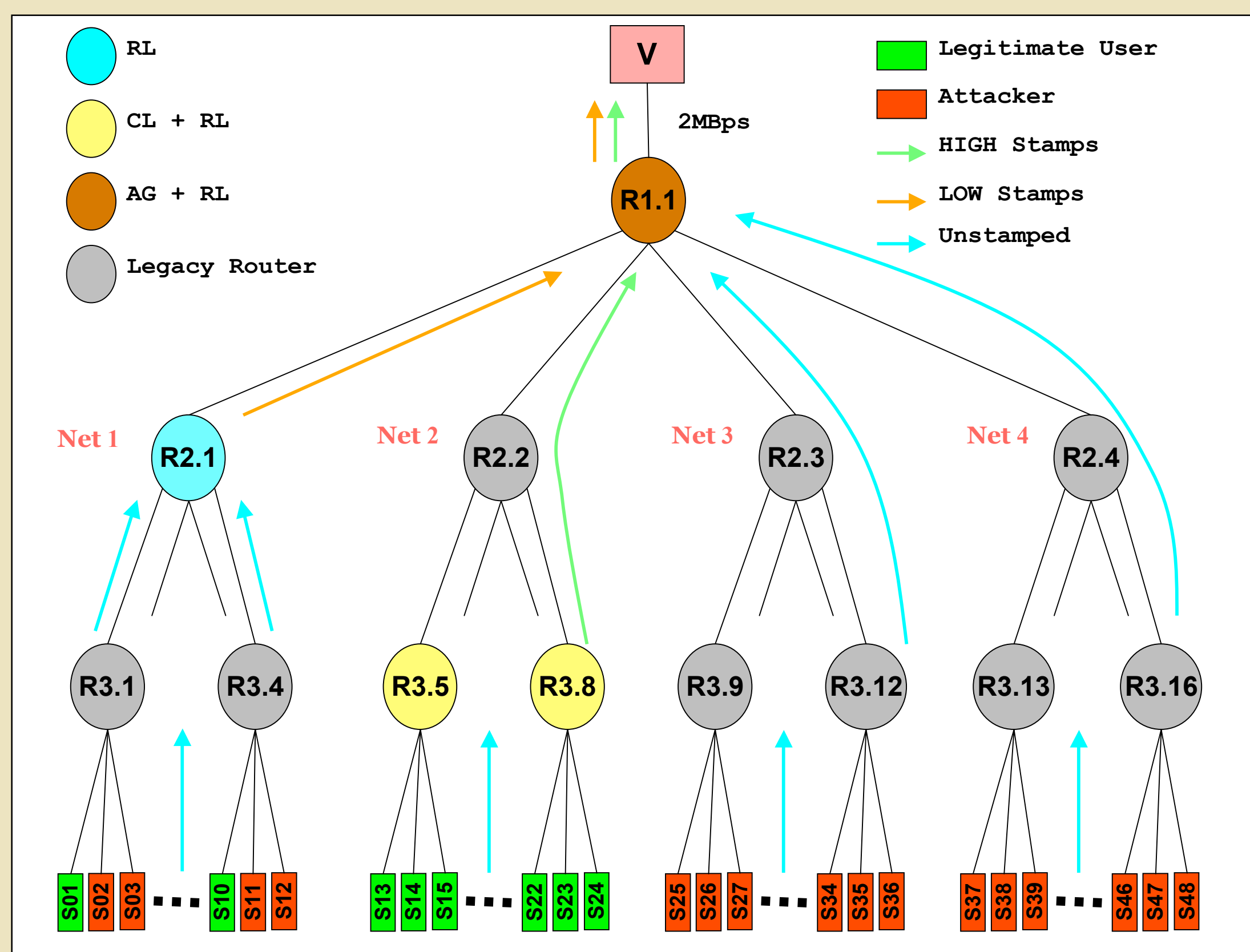
<http://www.nsl.cis.udel.edu/DefCOM>



Defensive Cooperative Overlay Mesh

A distributed DDoS defense framework, enabling cooperation of heterogeneous defense nodes. Nodes cooperate to identify legitimate traffic and provide guaranteed service to this traffic, while dropping the attack. Add-on modules augment existing defense systems.

1. The Alert Generator (AG) module interacts with an intrusion detection system at the victim and alerts the other defense nodes in the overlay about the attack.
2. The Classifier (CL) module interfaces with the source defense system and marks good traffic with HIGH-priority stamps. Suspicious traffic is marked with LOW-priority marks.
3. The Rate Limiter (RL) module, residing at routers, prioritizes traffic according to the stamps and controls any excess of traffic to the victim.



DefCOM reduces the overall DoS traffic, with minimal collateral damage

DefCOM's experimental topology in Emulab with 21 routers and 49 hosts

Approach and Impact

- Distributed, non-contiguous deployment
- Focus on minimizing collateral damage
- Dynamic way of constructing the overlay, used for exchanging control messages
- Installed protection mechanisms against malicious participants and outside intruders
- Victim services are protected during the DoS attack
- Legitimate traffic is safely delivered to the victim
- Easily installed modules augment the functionality of the existing defense systems
- DefCOM motivates wide deployment

