

# Microscopic Simulation of a Group Defense Strategy

Linda Briesemeister and Phil Porras

SRI International  
Menlo Park, CA

Symposium on  
Measurement, Modeling, and Simulation of Malware (MMSM)  
June 3, 2005



# Background

- ▶ Part of **EMIST**/DETER project
- ▶ EMIST (Evaluation Methods for Internet Security Technology)
  - “Develop thorough, realistic, and scientifically rigorous testing frameworks and methodologies for particular classes of network attacks and defense mechanisms.”*



- ▶ Funded by NSF and DHS

# Worm Defense Strategies

Highlights of ongoing malcode defense research

**Resource Limitation** Delay worm propagation through the limiting of resources that aggressive worms consume

(Williamson 2002, Staniford 2004, Wong et al. 2004)

**Leap-Ahead** Cooperative information sharing recognizes the emergence of a propagating worms, allowing pre-attack defensive posture

(Nojiri et al. 2003, Anagnostakis et al. 2003)

**Mobile Combat** Interception and rapid patching using defensive self-propagating mobile code

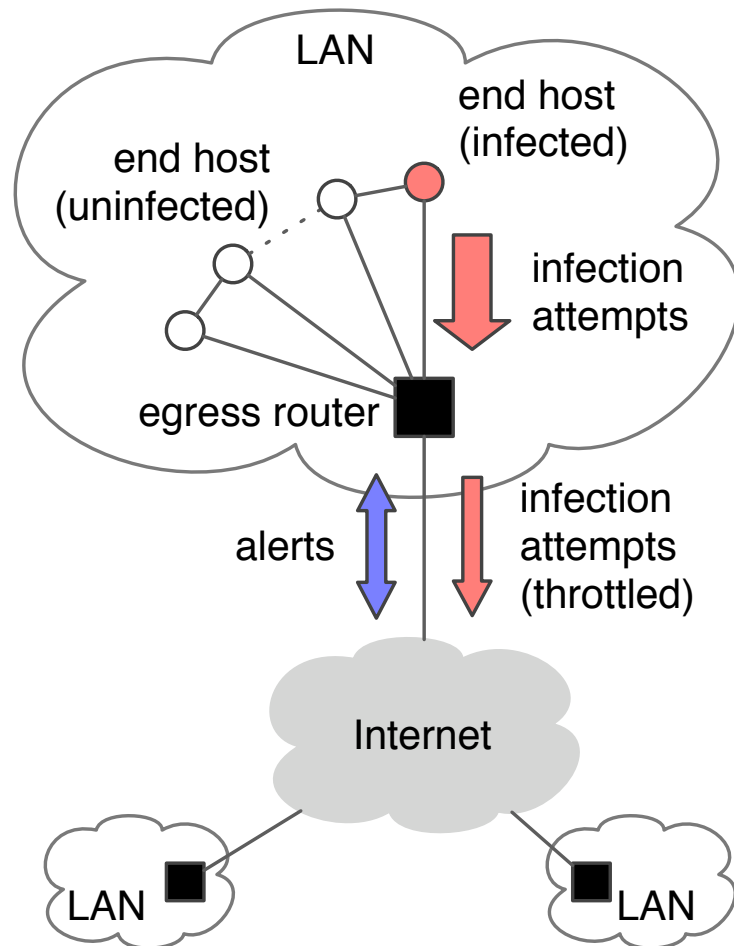
(Nicol and Liljenstam 2004, Toyozumi and Kara 2002)

**Infrastructure** Disrupt or thwart the discovery of susceptible nodes within an address space

(Ganger et al. 2002, Wang et al. 2004, Briesemeister et al. 2003, Provos 2004)

# Combination of Two Defense Strategies

Rate limiting & cooperative leap-ahead

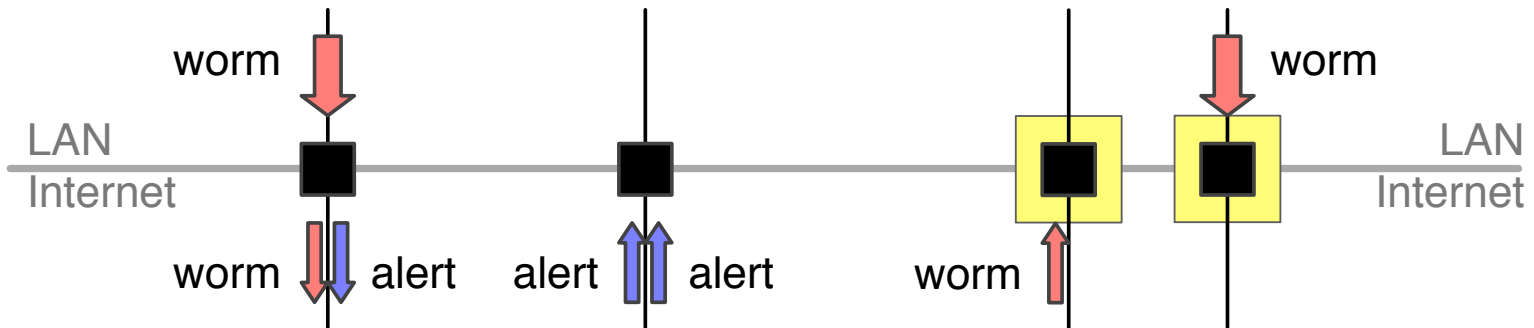
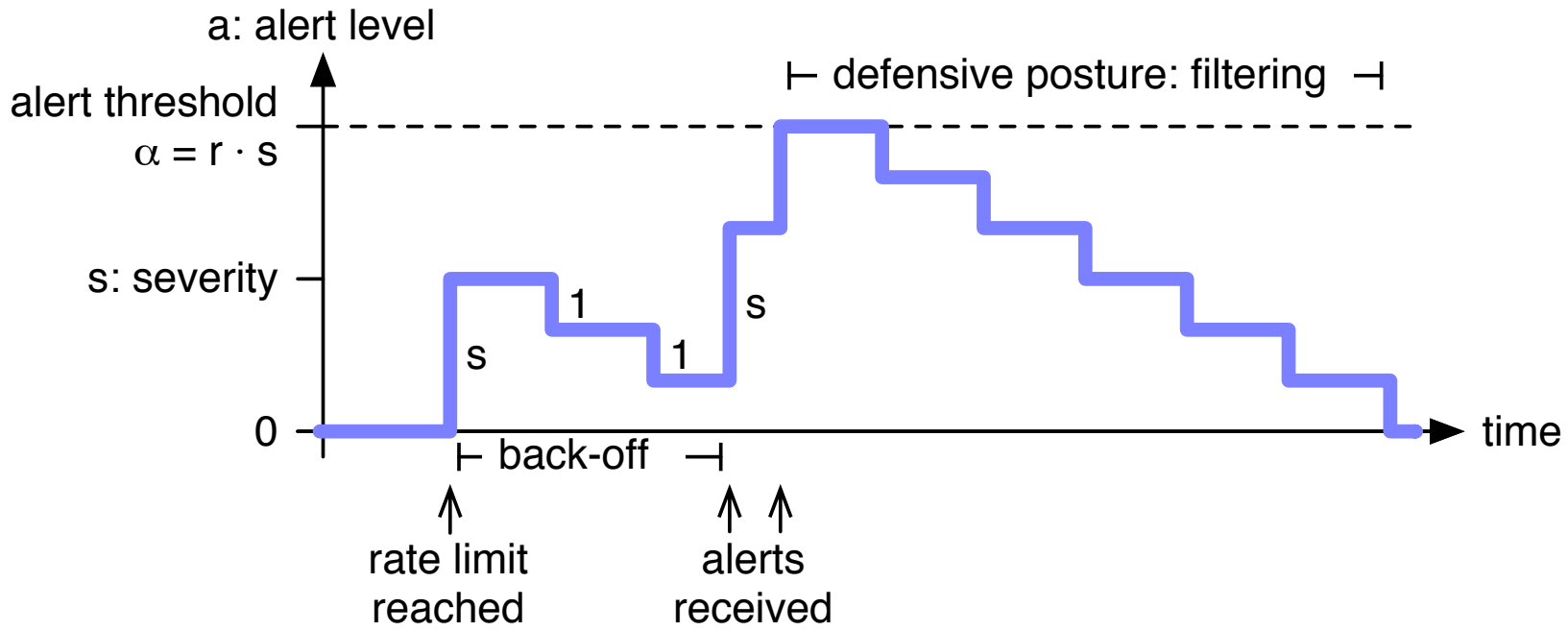


Idea:

1. Rate limit reached  
→ send alert to peers and self
2. Enough alerts obtained  
→ switch into defensive posture

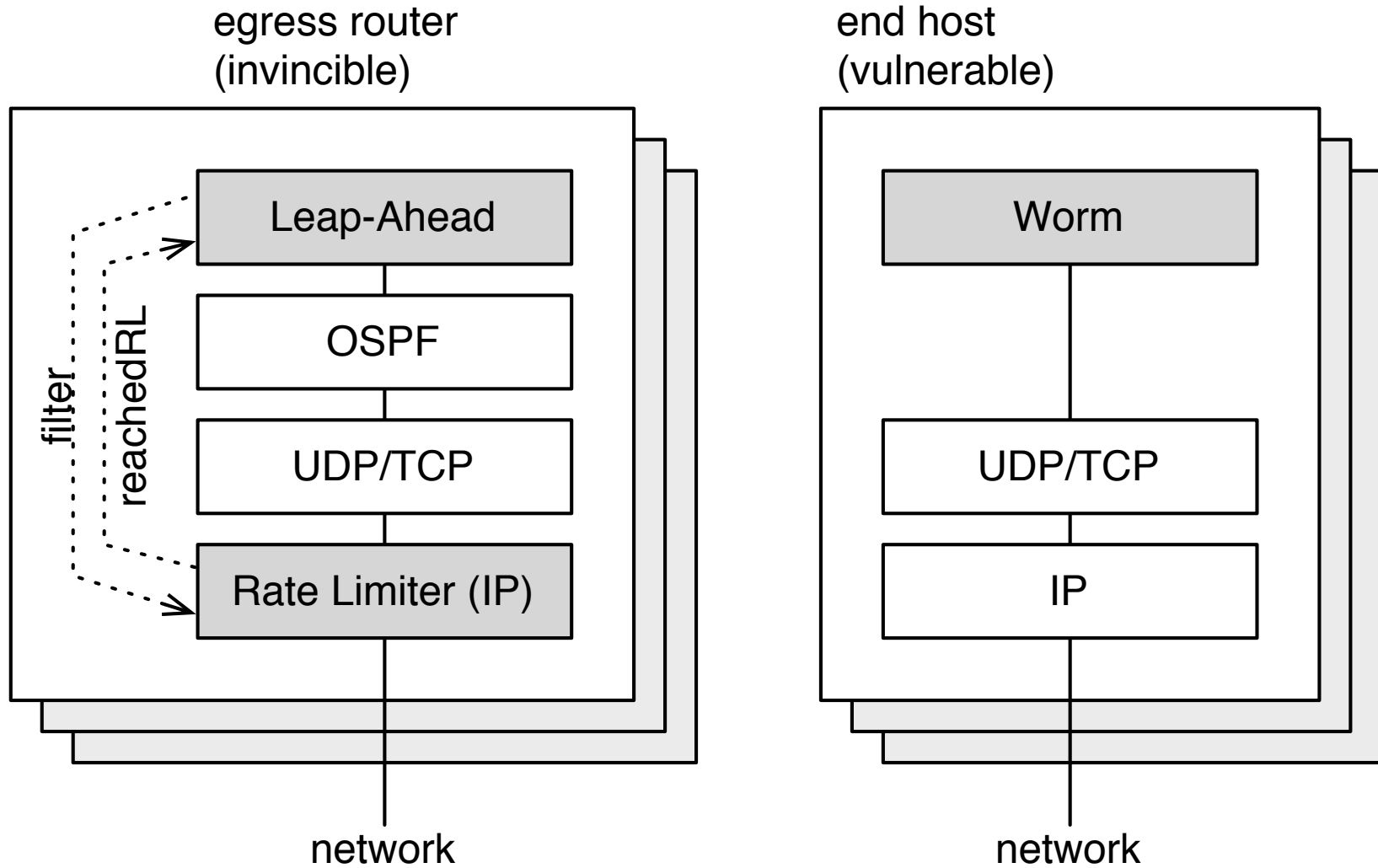
# Group-Based Defense Example

Implemented on egress router



# Implementation in SSFNet

In gray: our additions and modifications

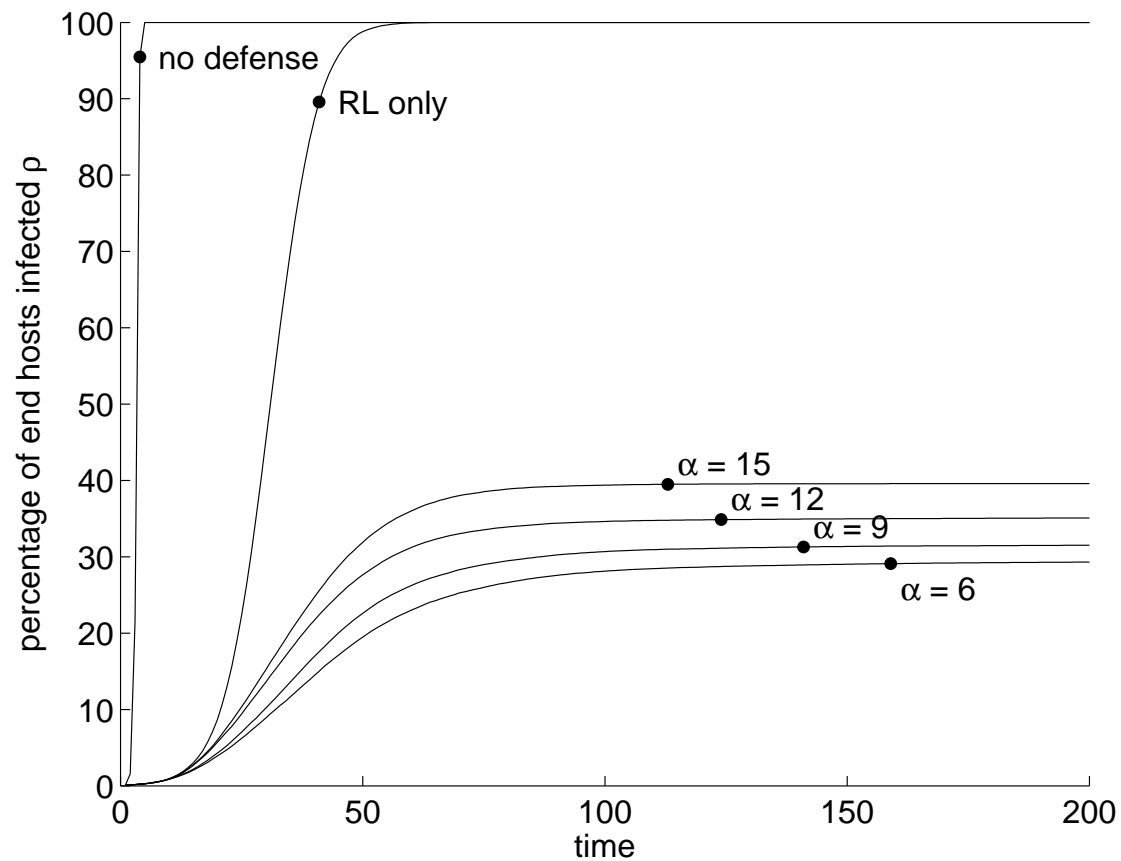


# Simulation Parameters

- ▶  $M = 100$  LANs
- ▶ Each LAN: 1 egress router and  $k = 10$  vulnerable end hosts
- ▶ Random scanning UDP worm in address space  $0..2^{16} - 1$
- ▶ 3 worm speeds:
  - ▶ 10 (low speed),
  - ▶ 100 (medium speed), and
  - ▶ 1000 (high speed) scans per second
- ▶ Worm defense:
  - ▶ rate limit = 10 different (external) IPs per second
  - ▶ group size  $G = 10$  and alert severity  $s = 3$
  - ▶ alert threshold  $\alpha = 6, 9, 12, 15$
- ▶ Max. simulated time 200 seconds and 100 repeated runs

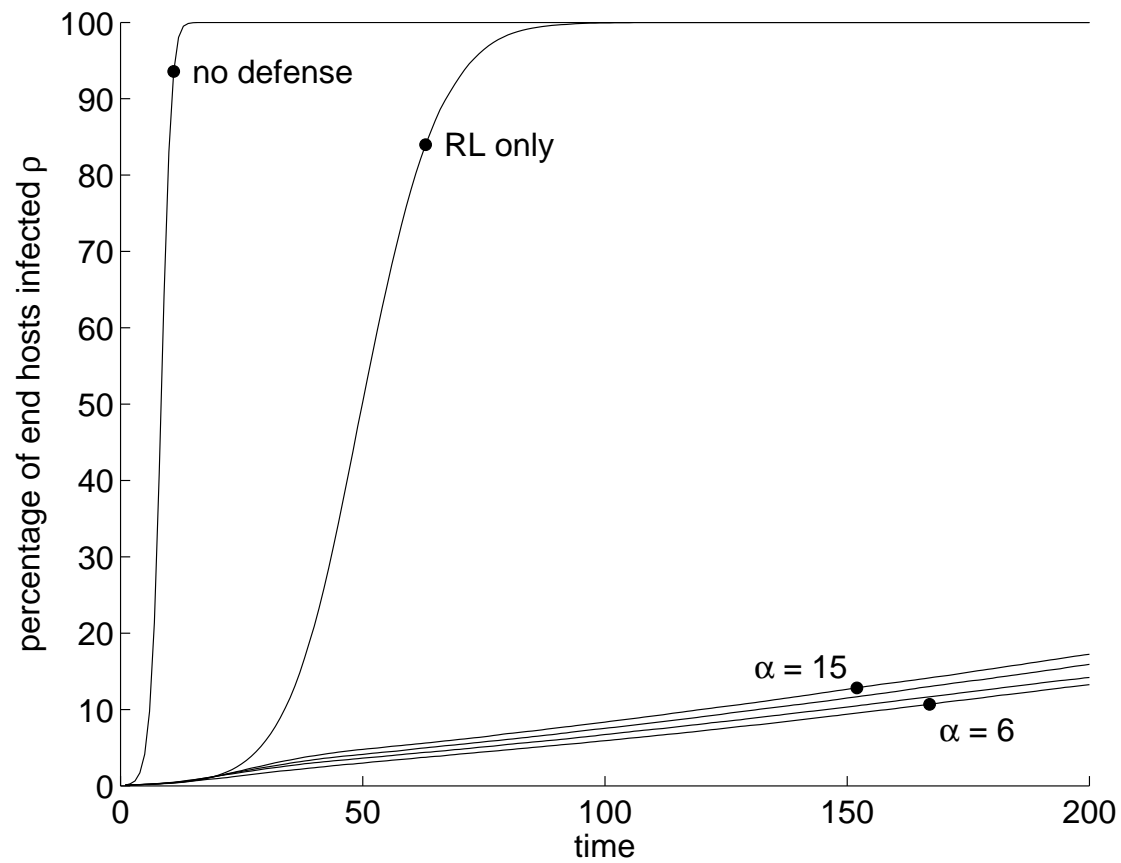
# Infected End Hosts

High-speed worm



# Infected End Hosts

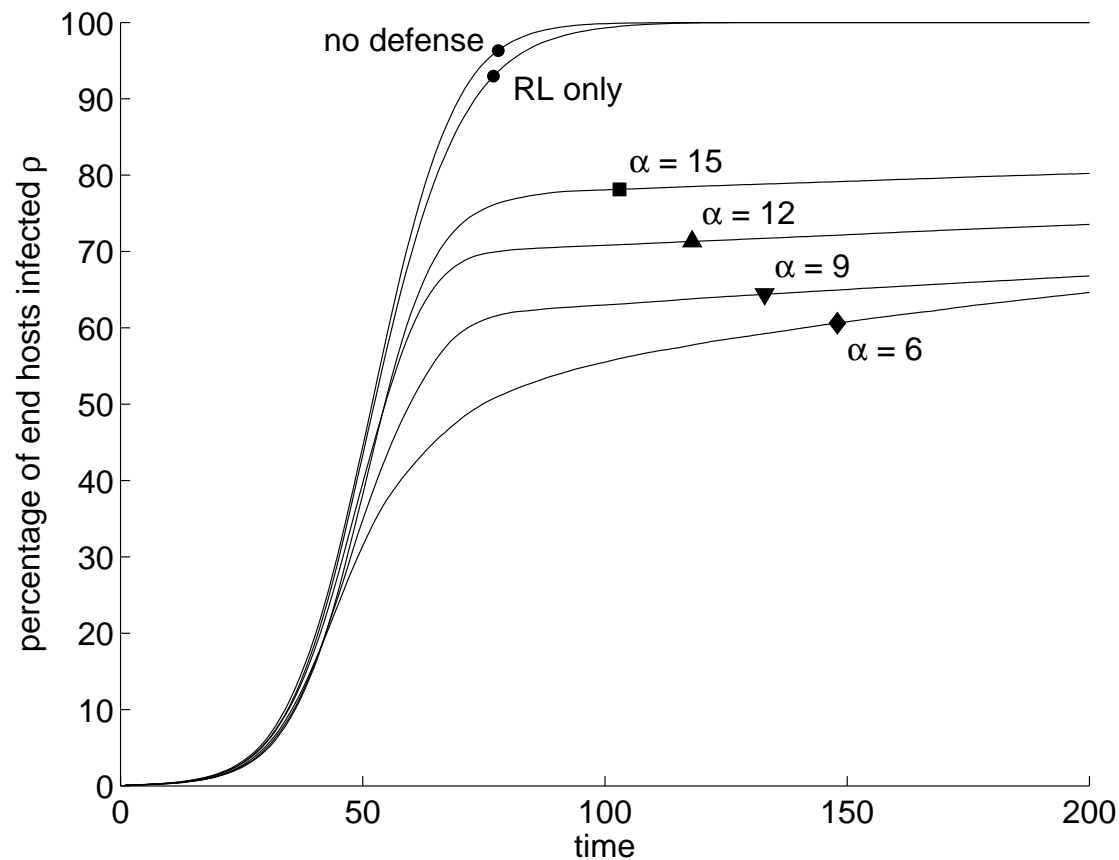
Medium-speed worm



# Infected End Hosts

Low-speed worm

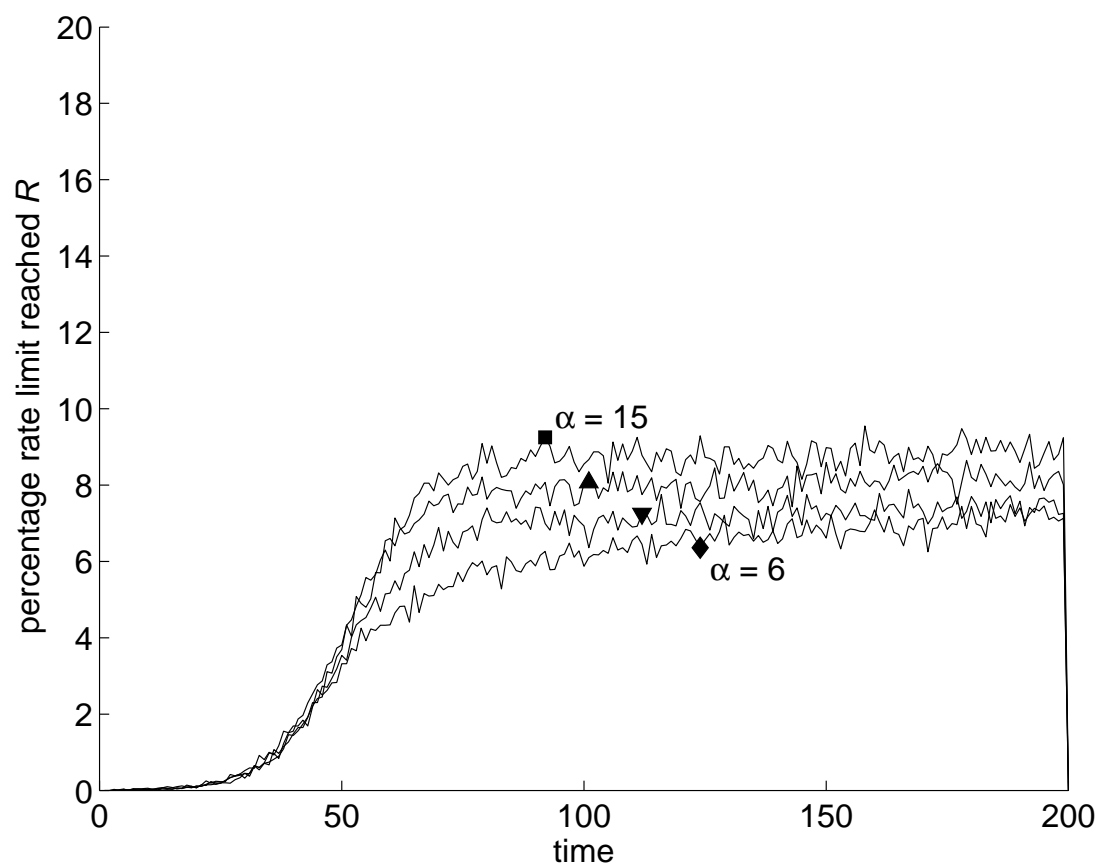
Worm operates at detection threshold (10 scans per second):  
Why aren't curves " $\alpha$ " similar to "RL only"?



# Rate Limiting Routers

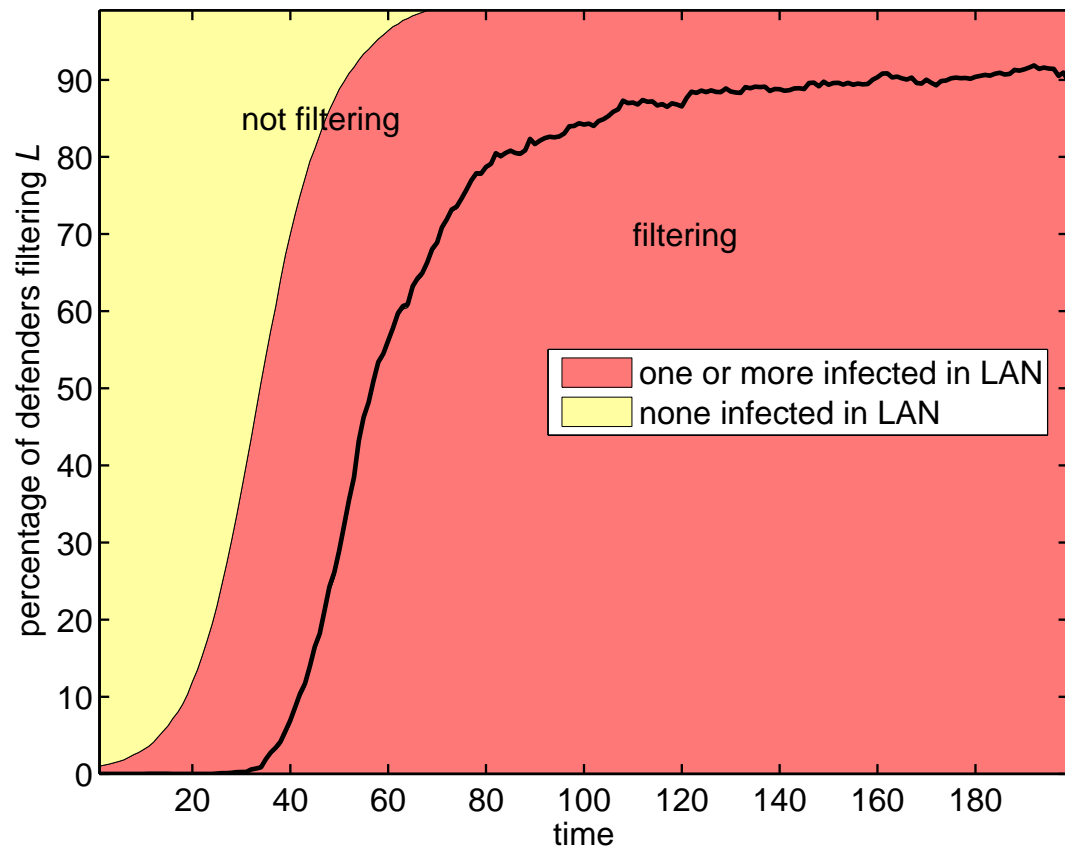
Low-speed worm

Metric is evidence for defense invocation under slow worm attack.



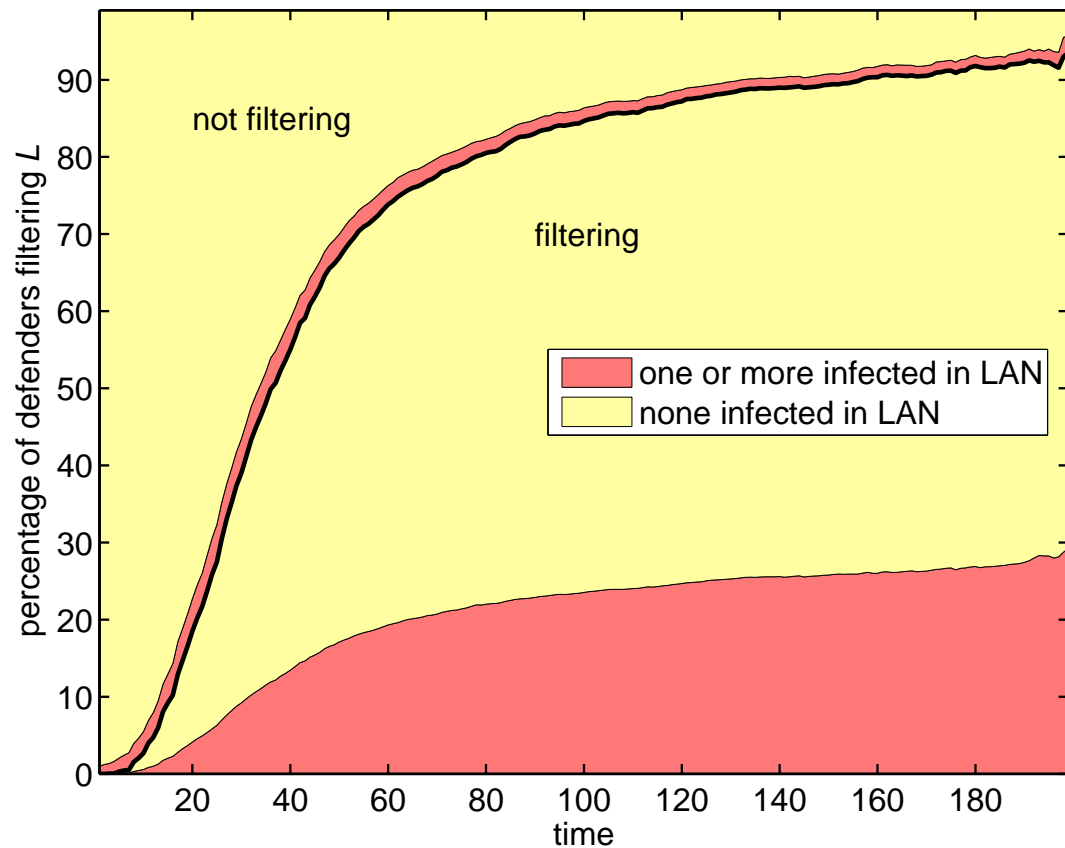
# Routers in Defensive Posture

Low-speed worm and  $\alpha = 6$



# Routers in Defensive Posture

Medium-speed worm and  $\alpha = 6$



# Conclusion

- ▶ Proposed novel integrated combination of rate limiting with group-based worm defense strategy
- ▶ Implemented in SSFNet framework to perform microscopic simulation of defense under random scanning worm attacks
- ▶ Results show worm defense curbs infection spread
- ▶ Combination of different metrics reveal effectiveness of group-based defense
  - ▶ High- & medium-speed worm: defensive posture before infected  
→ leap-ahead strategy successful
  - ▶ Low-speed worm: defensive posture after infected  
→ leap-ahead strategy not successful (but infection curbed!)

# Bibliography

- ▶ Anagnostakis, K. G., Greenwald, M. B., Ioannidis, S., Keromytis, A. D. and Li, D.: 2003, A cooperative immunization system for an untrusting internet, *Proceedings of the 11th IEEE International Conference on Networks (ICON'03)*.
- ▶ Briesemeister, L., Lincoln, P. and Porras, P.: 2003, Epidemic profiles and defense of scale-free networks, *Proceedings of the 2003 ACM workshop on Rapid malware (WORM)*, ACM Press, pp. 67–75.
- ▶ Ganger, G. R., Economou, G. and Bielski, S. M.: 2002, Self-securing network interfaces: What, why and how, *Technical report*, Computer Science Department, Carnegie Mellon University.
- ▶ Gualtieri, M. and Mossé, D.: 2003, Limiting worms via QoS degradation, *Technical report*, Computer Science Department, University of Pittsburgh.
- ▶ Nicol, D. M. and Liljenstam, M.: 2004, Models of active worm defenses, *Proceedings of IPSI Studenica Conference*.
- ▶ Nojiri, D., Rowe, J. and Levitt, K.: 2003, Cooperative response strategies for large scale attack mitigation, *DARPA Information Survivability Conference and Exposition*, pp. 293–302.
- ▶ Provos, N.: 2004, A virtual honeypot framework, *Proceedings of the 12th USENIX Security Symposium*, pp. 1–14.
- ▶ Staniford, S.: 2004, Containment of scanning worms in enterprise networks, *Journal of Computer Security*.
- ▶ Toyozumi, H. and Kara, A.: 2002, Predators: good will mobile codes combat against computer viruses, *Proceedings of the 2002 Workshop on New Security Paradigms (NSPW)*, ACM Press, New York, NY, USA, pp. 11–17.
- ▶ Wang, H. J., Guo, C., Simon, D. R. and Zugenmaier, A.: 2004, Shield: vulnerability-driven network filters for preventing known vulnerability exploits, *Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM)*, ACM Press, pp. 193–204.
- ▶ Williamson, M. M.: 2002, Throttling viruses: Restricting propagation to defeat malicious mobile code, *Proceedings of the 18th Annual Computer Security Applications Conference*, IEEE Computer Society, p. 61.
- ▶ Wong, C., Wang, C., Song, D., Bielski, S. and Ganger, G. R.: 2004, Dynamic quarantine of Internet worms, *Proceedings of the International Conference on Dependable Systems and Networks DSN-2004*.