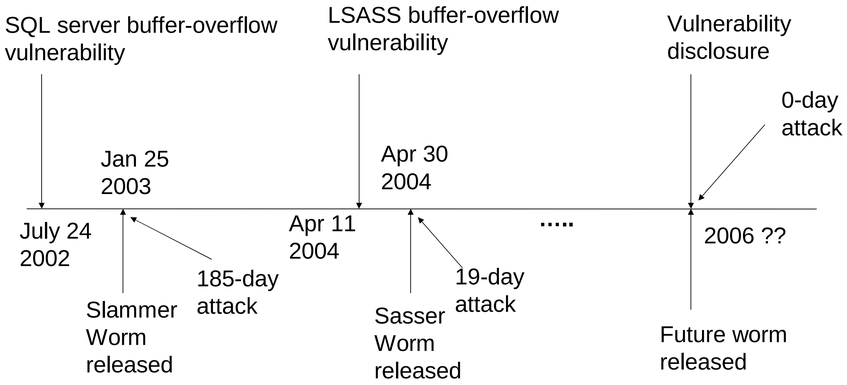
Reactive Zero-day Worm Protection

Kihong Park (PI), Bhagya Bethala, Ikyun Kim
Network Systems Lab, Department of Computer Sciences, Purdue University

Spread of Slammer worm

< 10 mins to infect the vulnerable population

Zero-day worms

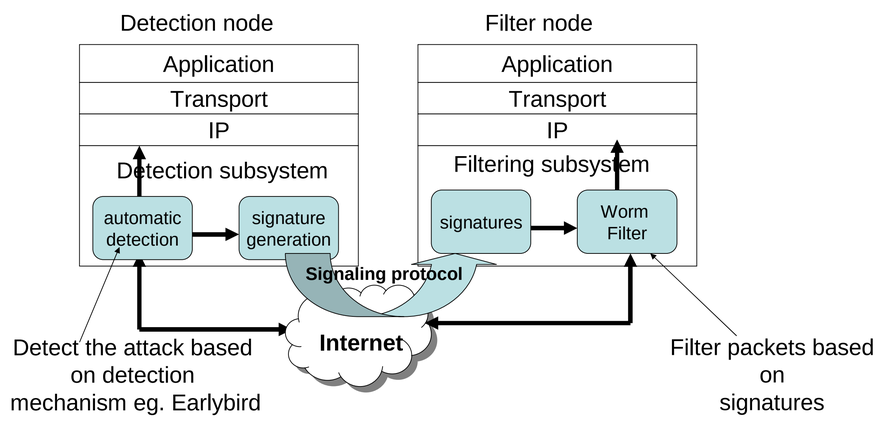


Time gap between vulnerability disclosure and release of a worm that exploits it is decreasing

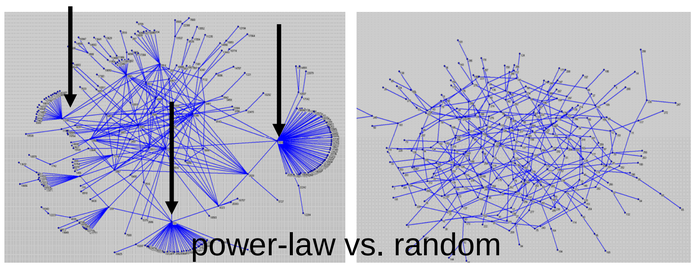
Global Protection

- Early detection at transit points
  - Earlybird, Polygraph etc.
- Dissemination of information to content-based filters to contain the spread

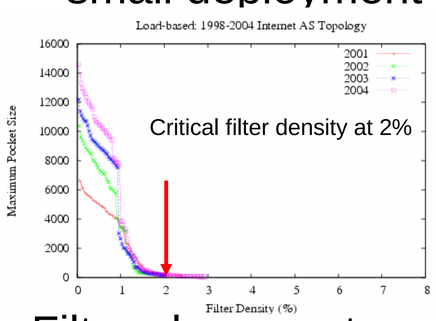
Approach: Cooperative Filtering



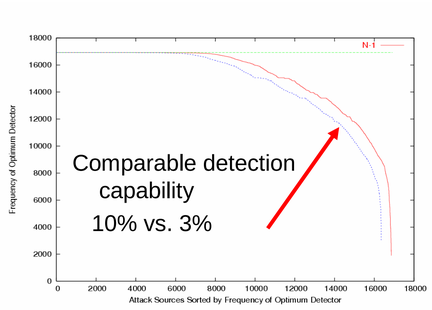
Deployment



power-law nature of Internet enables small deployment



Filter placement

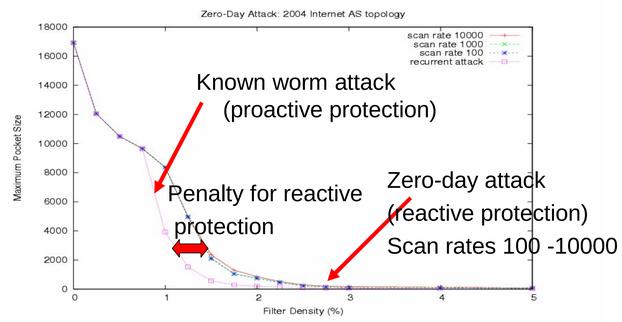


Detector placement

Performance Evaluation

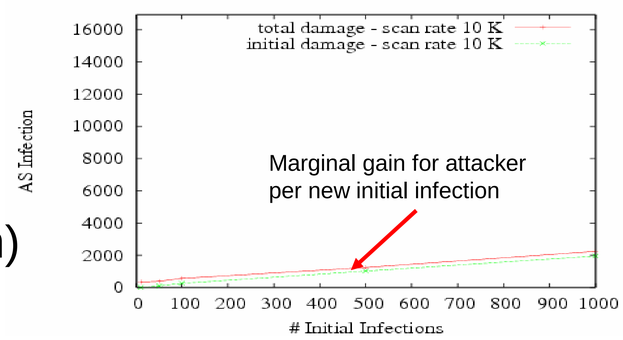
Simulation setup:

- 2004 AS topology with 16921 ASes and 2^32 hosts
- Live Earlybird-like detection



Key parameters

- Uniform random scanning
- Filter deployment: 3%
- Detector deployment: 3%
- Scan rate: 10K scans/sec
- Initial infections: 10 (random)



Other sponsors

DARPA
THE DOCUMENT COMPANY XEROX
Electronics and Telecommunications Research Institute
intel
PURDUE UNIVERSITY
PURDUE HOMELAND SECURITY INSTITUTE
CERIAS
REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING
Discovery Park e-Enterprise Center