Proactive Defenses Against DDoS and Worm Attacks

Harnessing the Power of Power-Law Topology for Scalable Network Security

Kihong Park (PI), Hyojeong Kim, Ali Selcuk, Bhagya Bethala, Humayun Khan, Wonjun Lee
Network Systems Lab, Department of Computer Sciences, Purdue University

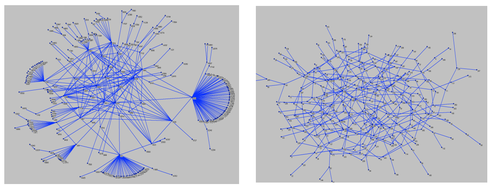
Objective

Proactive protection: Prevent attacks from imparting harm in the first place
Reactive protection: Respond, attribute, and contain new and non-preventable attacks

→ new approach: distributed packet filtering (DPF) → proactive & reactive filtering

Internet Power-Law Topology

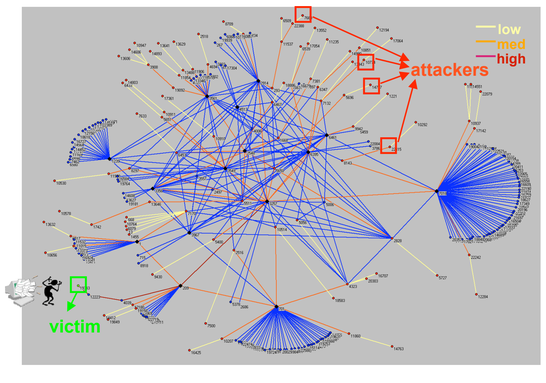
"A few are connected to many, many are connected to a few."



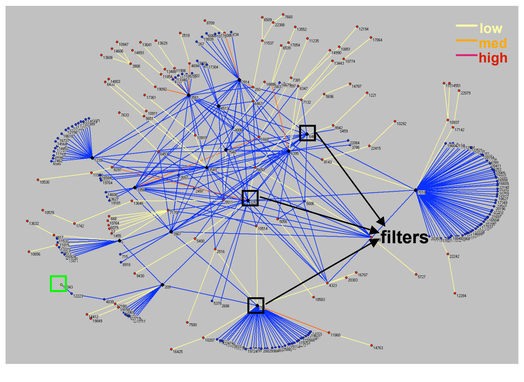
→ facilitates strategic & economic filter deployment

DDoS Attack Protection

→ DPF: route-based filtering "unde venis?"



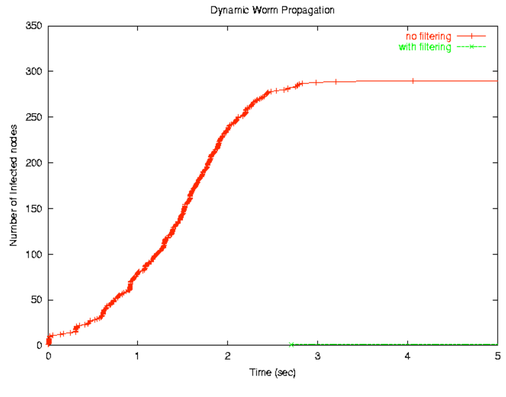
Without DPF



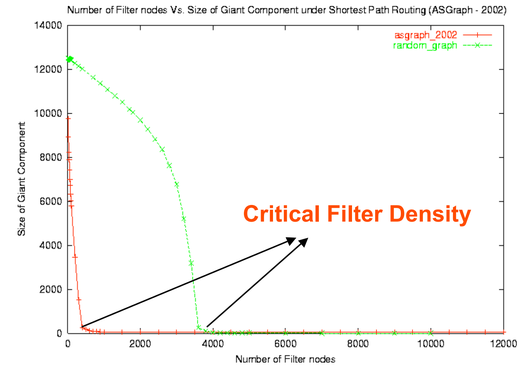
With DPF

Worm Attack Protection

→ DPF: content-based filtering



Infection Dynamics

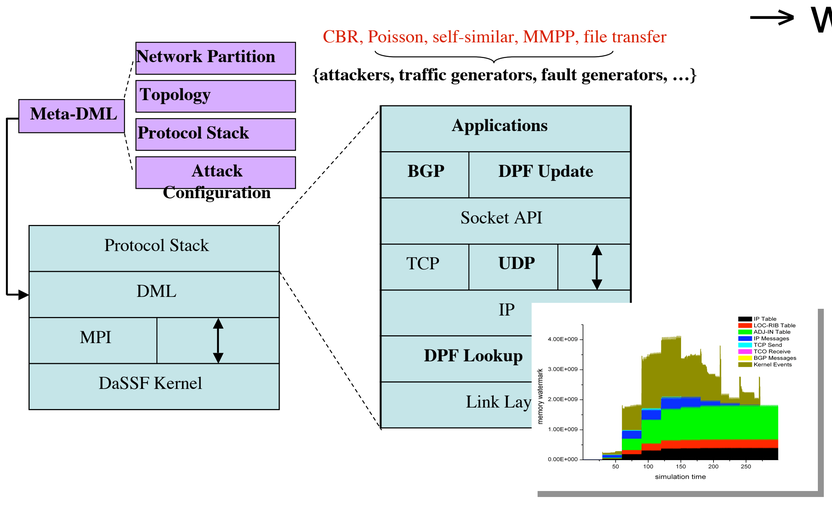


Percolation Threshold

→ 4% deployment achieves significant protection: containment & traceback
→ NLANR (1997-2002), CAIDA, RIPE, USC/ISI, UMich Internet AS measurement data

Tools: Large-Scale Simulation & Prototype System Building

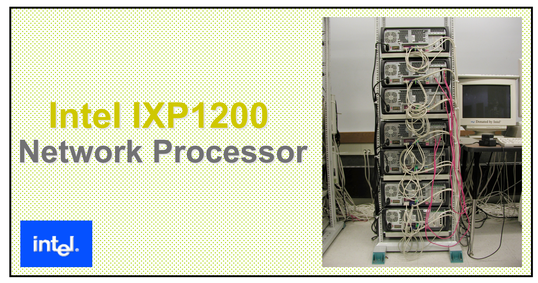
Dynamic DPF Simulator: Parallel Network Simulation



→ workstation cluster

- 12,500+ node networks
- Failure model
- Power-law partitioning
- System measurement
- Meta-DML configuration
- Trace-driven visualization

Network Processor Prototyping



- 7-node IXP1200 NP testbed
- DPF implementation & evaluation
- Teja development environment

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center