Thwarting Topological Worm Attacks in Peer-to-Peer Networks

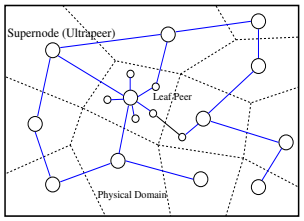
Liang Xie, Sencun Zhu

Self-propagating computer worms have been terrorizing the Internet for the last several yeas. Such threats become more imminent in P2P systems. We study the feasibility of constructing a self-defense infrastructure within an overlay topology to effectively contain worm propagation. Two general design principles are considered:

- to utilize some *worm-immune* nodes to stop worm spreads in the infrastructure, and
- to compete with a worm such that susceptible nodes may be immunized *before* the worm can reach them

A Partition-based Worm Containment Scheme

System Model and Attacks



Network model of P2P systems

System Model

- a dynamic random graph, or
- a two-tier overlay that follows the power law
- node states: vulnerable, infected, immune

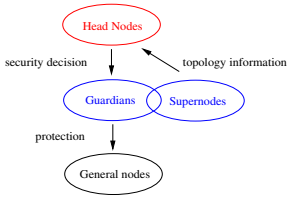
Attack Model of a Topological Worm

- starts by choosing initial victims from a hit list
- scans neighbors of the victims and locates those vulnerable as new targets
- spreads to the entire overlay in a flooding way

A Self-defense Infrastructure

Three-level Defense

- topology collection
- graph-partitioning & guardian deployment
- protection



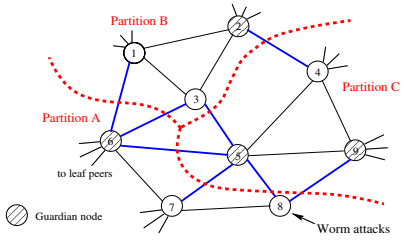
Basic Principle

- head nodes partition the overlay graph into as many separate pieces as possible
- guardians block worm propagation within each partition

Scheme Details

K-way Partitioning Algorithm

- coarse down -> divide and conquer -> project back
- the minimum vertex separate algorithm



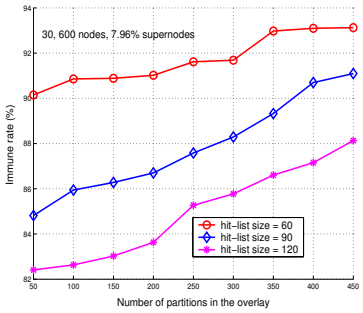
An example of the k-way partitioning on an overlay graph. Worm propagation is contained within partition A

Topology Collection

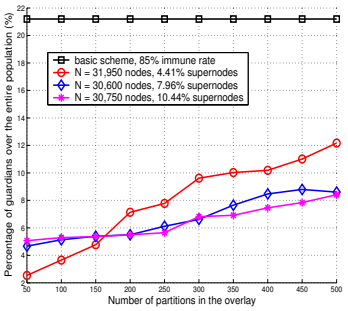
- super nodes crawls the overlay periodically
- head nodes assemble the topology

Performance Results

Comparisons with *Zhou's basic scheme [1];* *Metric:* immune rate vs. #guardians



Overlay topology with 7.96 super nodes

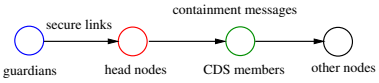


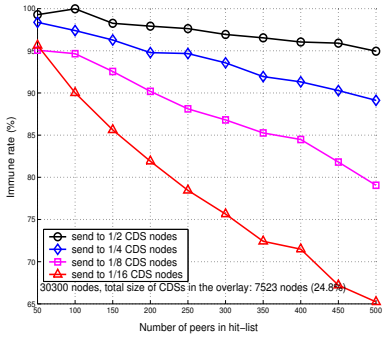
Fraction of guardians used

A CDS-based Defense Scheme

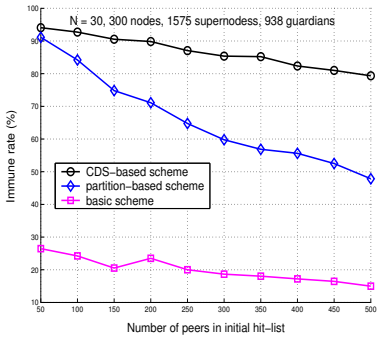
A reactive countermeasure to win a race between patch delivery and worm propagation

1. Periodically, head nodes construct snapshot of the overlay
2. Head nodes compute a Connected Dominating Set (CDS) of nodes
3. A guardian detects the worm attack and notifies head nodes
4. Head nodes generate and deliver containment messages to the CDS nodes





Immune rate of the CDS-based scheme



Performance comparison on different schemes

Features of Our Defenses

- The partition-based scheme uses an optimal way to deploy guardians (proactive)
- The CDS-based scheme wins the race against the worm spread (reactive)

Future Work

- Consider node diversities in worm detection
- Focus on both structured and unstructured overlay networks

[1] Zhou et. al., A first look a P2P worms: threats and defenses, in IPTPS'05