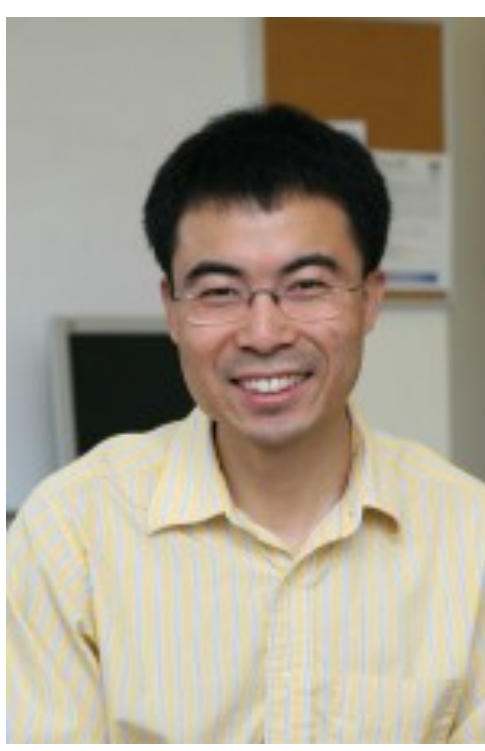


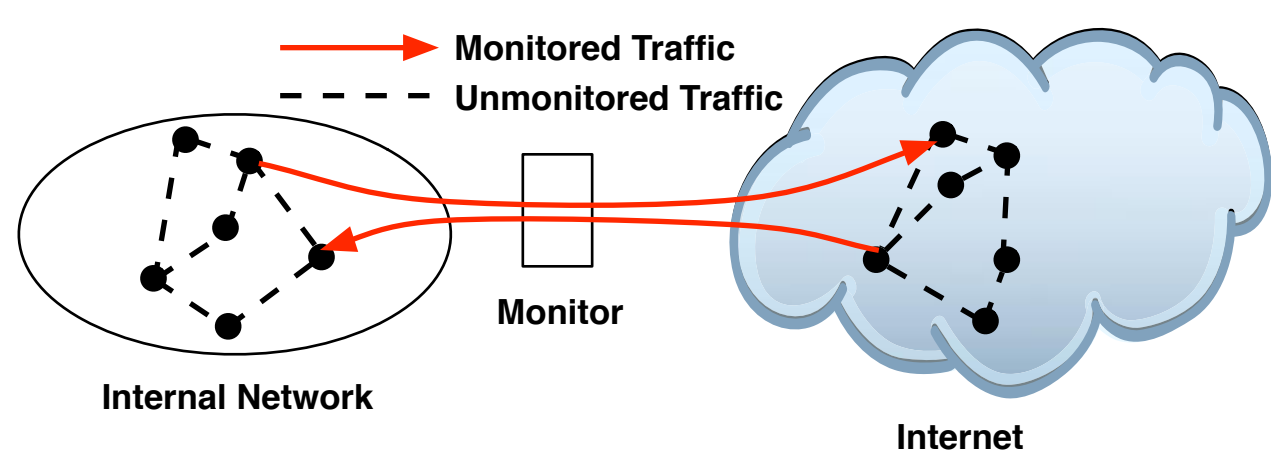
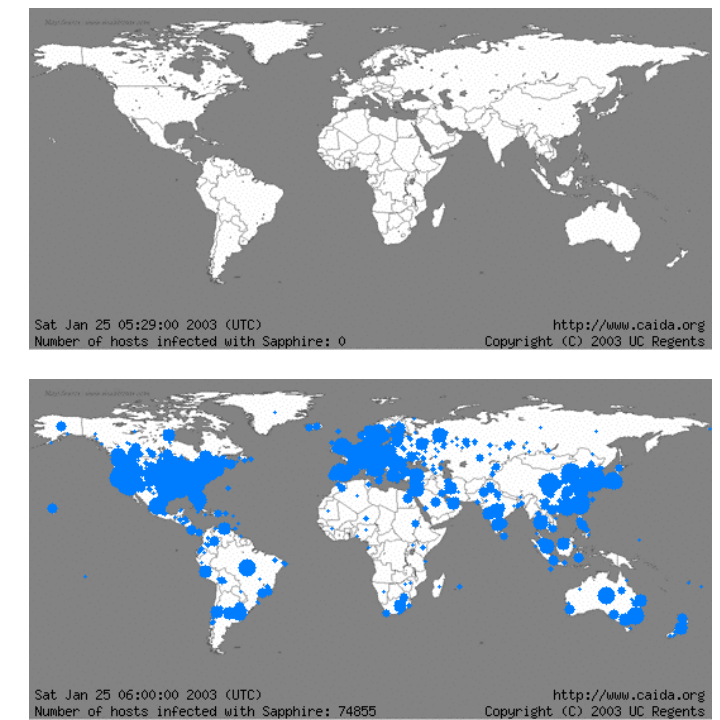
CAREER: A Behavior-Based Framework for Detecting Internet Worms



PI: Jun Li (lijun@cs.uoregon.edu) <http://netsec.cs.uoregon.edu/>

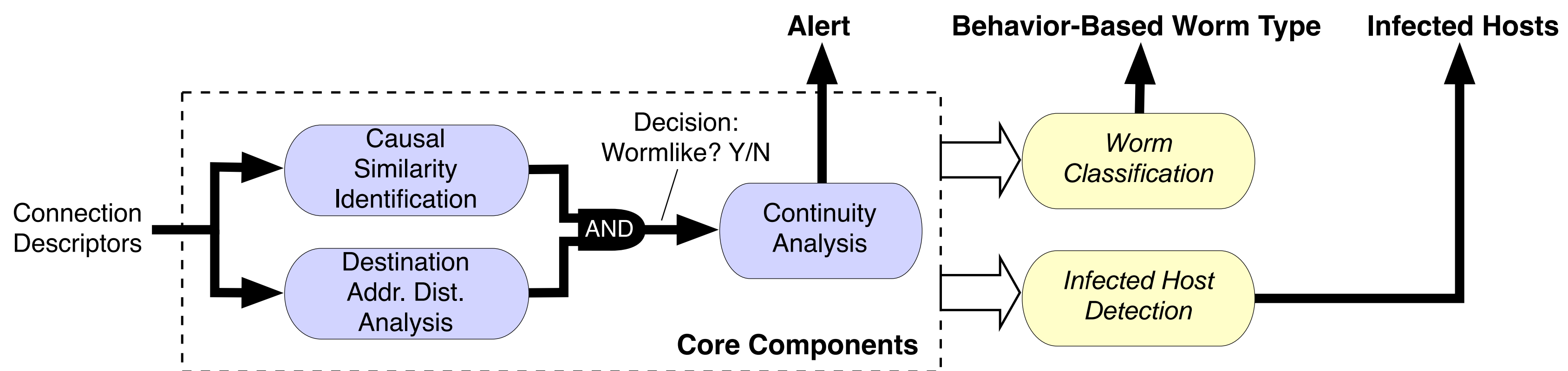
Motivation and Objectives

- The Internet is a critical infrastructure and at risk of shutdown from worm activity.
- Accurate detection of worms in their early stages remains an unsolved problem.
- Content-based approaches are vulnerable to worm polymorphism and are costly.
- Our **behavior-based** worm detection framework focuses on *payload-independent, essential* behaviors that a worm cannot (or hardly can) avoid exhibiting.



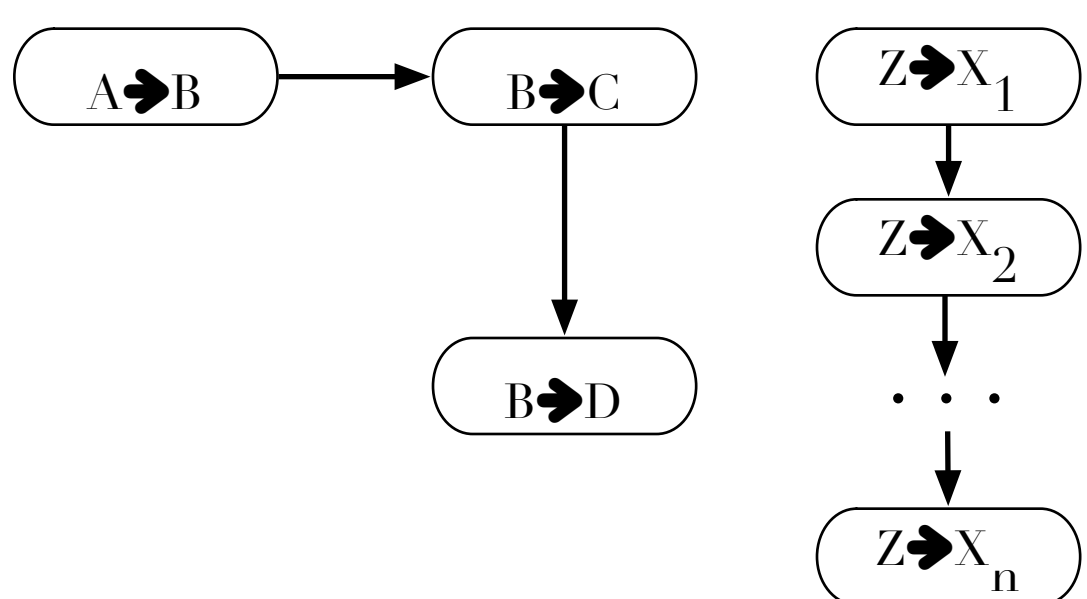
- We look at three major aspects of worm connections crossing the gateway of a domain: the relationship of worm connections, their destination visiting patterns, and their continuity as a worm spreads.

- Our framework further aims to classify a detected worm by the behavior exhibited, and identify which individual hosts are infected.



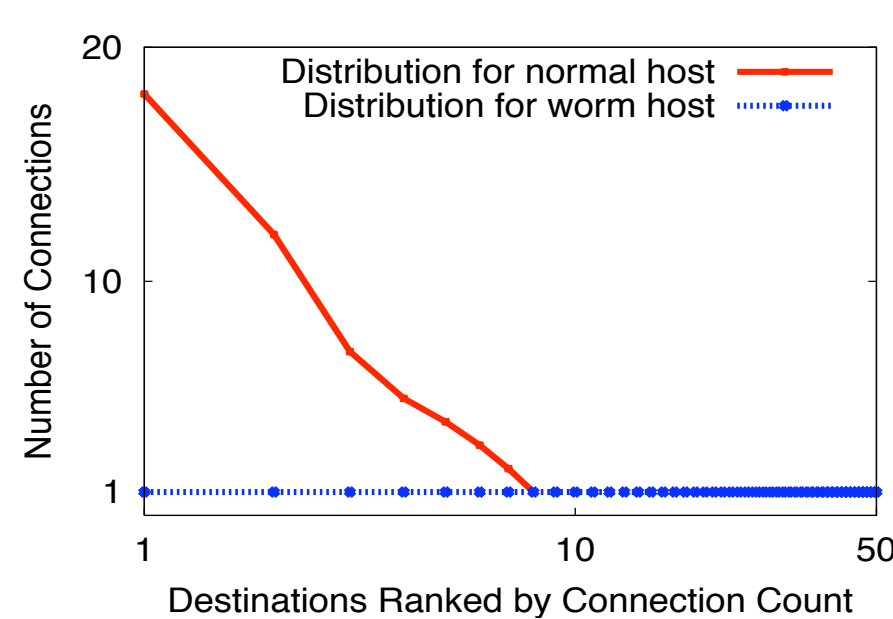
Causal Similarity Identification

- A connection of a worm *causes* more subsequent connections of the worm, and they are *similar*.
- We maintain a *causal connection graph* to represent possible causal relationship of connections. Each new connection is compared to its ancestors in search of similar or suspicious patterns.
- The two simplified examples below show different subgraphs from a causal graph that might help identify a connection as wormlike.



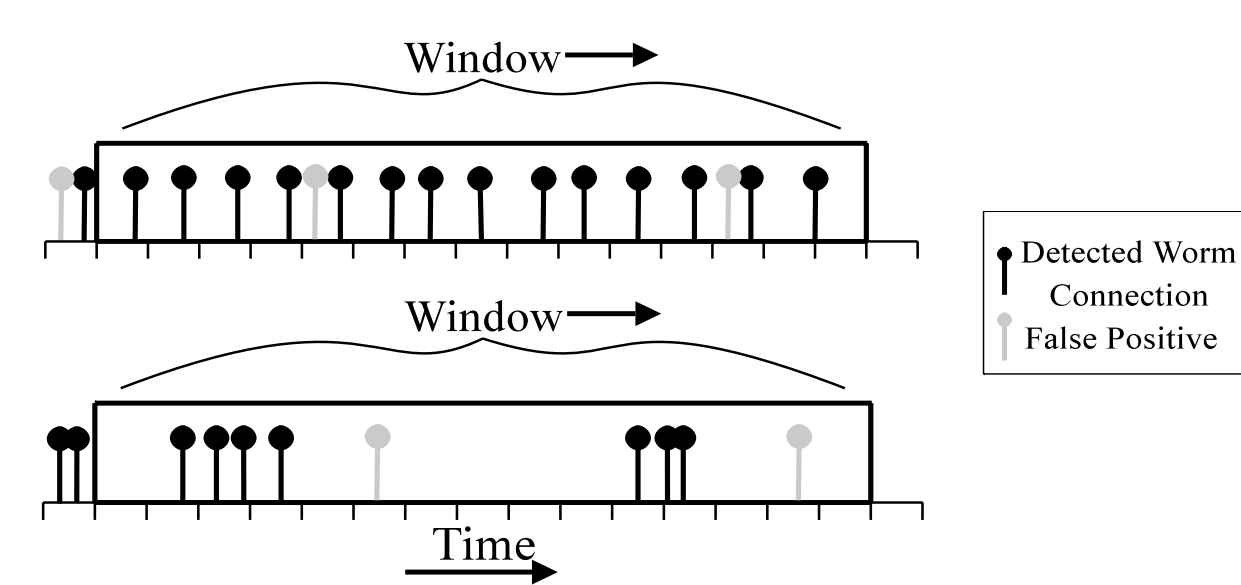
Destination Distribution Analysis

- A worm typically makes connections to a large set of target addresses. On the other hand, because a normal host typically visits a small number of destinations, its connection pattern resembles a zipf-like distribution.
- We seek rigorous statistical or mathematical methods to distinguish destination patterns of normal and infected hosts.
- The conceptual examples below show the difference in the plots of recent connection histories of a normal host and an infected host.



Continuity Analysis

- A worm continually initiates new worm connections. Otherwise its speed is significantly limited.
- We study how to leverage this behavior to avoid raising worm alerts because of wormlike but legitimate connections.
- In particular, we employ a fast, adaptive, and noise-resistant sliding-window-based mechanism to detect the unique continuity of worm connections.



Current Results with Our SWORD Prototype

- Evaluation of SWORD against recorded network traces with injected simulated worm traffic shows promising results.
- SWORD was always able to detect the presence of a worm within the monitored network and never reported a worm when one was not present.
- SWORD detected worms which employed a variety of scanning algorithms and rates, and did so without examining the payload of packets crossing the gateway.

