Addressing Threats and Vulnerabilities in Critical Interconnected Systems

Jon Kleinberg

Cornell University
Florida Power Grid (Dale et al, Xu et al)
Facebook user’s friends (Marlow et al)
Financial Network

Loans among banks (Bech and Atalay)
First Mechanism: Transmission
First Mechanism: Transmission

Measles transmission (Currie et al)
First Mechanism: Transmission

HIV transmission (Potterat et al)
The wireless epidemic

Jon Kleinberg

As wireless communication technologies spread, so the potential for viruses to exploit them grows. Biological models of virus transmission will assume new relevance for assessing the emerging threat.

Ever since the first appearance of computer viruses on the digital landscape, our understanding of them has drawn on parallels with biology. Analogies of mutation, phylogenetic reconstruction and computational immune systems have all been investigated. But the central analogy has come from the use of epidemiological models to track how a computer virus spreads. A crucial ingredient in these models is a description of the contact network through which the epidemic propagates, where the links represent who has the potential to infect whom. Traditionally, computer viruses have propagated on networks that bear little resemblance to the networks of physical contact through which their biological counterparts spread. But a growing body of research shows that the increasing use of short-range wireless communication networks might cause the two models to converge.

Accurately modelling the network through which a disease epidemic spreads is difficult in almost any setting. Diseases in plant populations, or animal diseases such as rabies, are heavily constrained by geographical proximity and the relatively fixed physical locations of the infected individuals. Models of these diseases have been extended using detailed data on patterns of travel within cities and by air worldwide in attempts to analyse disease outbreaks in human populations.

Epidemics on the Internet are even more diverse. At the most general level, there is a distinction between computer viruses, which ‘piggyback’ on data exchanged between users, and computer worms, which more actively direct their own transmission through a network. The networks on which these types of malicious code spread are based on patterns of file transfer or e-mail communication, or even on structures that evolve implicitly as a computer worm scans the Internet for targets.

Mathematical models of these different networks lend new urgency to questions on how the spread of computer viruses can be controlled.
If node $B$ depends on node $A$, and node $A$ fails, then $B$ may fail.
Second Mechanism: Unraveling

If node $B$ depends on node $A$, and node $A$ fails, then $B$ may fail.
If node $B$ depends on node $A$, and node $A$ fails, then $B$ may fail.
If node $B$ depends on node $A$, and node $A$ fails, then $B$ may fail.
If node $B$ depends on node $A$, and node $A$ fails, then $B$ may fail.
Second Mechanism: Unraveling

Power grid (Schafer et al)
Themes for Network Cascades

(1) Critical nodes
(2) Cascading behavior as a design goal
(3) Predictability
(4) Early-warning signals
“Single point of failure”

- Can be either a good or a bad thing, depending on the objective.
Critical Nodes
LIFE

Flu shot Saturday specifics
Critical Links for Unraveling

Power grid (Schafer et al)
Cascading Behavior as a Design Goal
Cascading Behavior as a Design Goal

LinkedIn invitations (Anderson et al)
Themes for Network Cascades

(1) Critical nodes
(2) Cascading behavior as a design goal
(3) Predictability
(4) Early-warning signals
Sudden Onset

\[ p = 0.003 \]

\[ p = 0.006 \]

\[ p = 0.008 \]

\[ p = 0.015 \]

(Networkx, networkx.github.io)
Early-Warning Signals

Facebook reshares (Cheng et al)
Early-Warning Signals

Signals in financial network (Battiston et al, Squartini et al)
Themes for Network Cascades

(1) Critical nodes
(2) Cascading behavior as a design goal
(3) Predictability
(4) Early-warning signals