Virus on a Network (Official Notes)

WHAT IS IT?

This model demonstrates the spread of a virus through a network. Although the model is somewhat abstract, one interpretation is that each node represents a computer, and we are modeling the progress of a computer virus (or worm) through this network. Each node may be in one of three states: susceptible, infected, or resistant. In the academic literature such a model is sometimes referred to as an SIR model for epidemics.

HOW IT WORKS

Each time step (tick), each infected node (colored red) attempts to infect all of its neighbors. Susceptible neighbors (colored green) will be infected with a probability given by the VIRUS-SPREAD-CHANCE slider. This might correspond to the probability that someone on the susceptible system actually executes the infected email attachment.
Resistant nodes (colored gray) cannot be infected. This might correspond to up-to-date antivirus software and security patches that make a computer immune to this particular virus.

Infected nodes are not immediately aware that they are infected. Only every so often (determined by the VIRUS-CHECK-FREQUENCY slider) do the nodes check whether they are infected by a virus. This might correspond to a regularly scheduled virus-scan procedure, or simply a human noticing something fishy about how the computer is behaving. When the virus has been detected, there is a probability that the virus will be removed (determined by the RECOVERY-CHANCE slider).

If a node does recover, there is some probability that it will become resistant to this virus in the future (given by the GAIN-RESISTANCE-CHANCE slider).

When a node becomes resistant, the links between it and its neighbors are darkened, since they are no longer possible vectors for spreading the virus.

HOW TO USE IT

Using the sliders, choose the NUMBER-OF-NODES and the AVERAGE-NODE-DEGREE (average number of links coming out of each node).

The network that is created is based on proximity (Euclidean distance) between nodes. A node is randomly chosen and connected to the nearest node that it is not already connected to. This process is repeated until the network has the correct number of links to give the specified average node degree.

The INITIAL-OUTBREAK-SIZE slider determines how many of the nodes will start the simulation infected with the virus.

Then press SETUP to create the network. Press GO to run the model. The model will stop running once the virus has completely died out.

The VIRUS-SPREAD-CHANCE, VIRUS-CHECK-FREQUENCY, RECOVERY-CHANCE, and GAIN-RESISTANCE-CHANCE sliders (discussed in “How it Works” above) can be adjusted before pressing GO, or while the model is running.

The NETWORK STATUS plot shows the number of nodes in each state (S, I, R) over time.

THINGS TO NOTICE

At the end of the run, after the virus has died out, some nodes are still susceptible, while others have become immune. What is the ratio of the number of immune nodes to the number of susceptible nodes? How is this affected by changing the AVERAGE-NODE-DEGREE of the network?

THINGS TO TRY

Set GAIN-RESISTANCE-CHANCE to 0%. Under what conditions will the virus still die out? How long does it take? What conditions are required for the virus to live? If the RECOVERY-CHANCE is bigger than 0, even if the VIRUS-SPREAD-CHANCE is high, do you think that if you could run the model forever, the virus could stay alive?

EXTENDING THE MODEL

The real computer networks on which viruses spread are generally not based on spatial proximity, like the networks found in this model. Real computer networks are more often found to exhibit a “scale-free” link-degree distribution, somewhat similar to networks created using the Preferential Attachment model. Try experimenting with various alternative network structures, and see how the behavior of the virus differs.

Suppose the virus is spreading by emailing itself out to everyone in the computer’s address book. Since being in someone’s address book is not a symmetric relationship, change this model to use directed links instead of undirected links.

Can you model multiple viruses at the same time? How would they interact? Sometimes if a computer has a piece of malware installed, it is more vulnerable to being infected by more malware.

Try making a model similar to this one, but where the virus has the ability to mutate itself. Such self-modifying viruses are a considerable threat to computer security, since traditional methods of virus signature identification may not work against them. In your model, nodes that become immune may be reinfected if the virus has mutated to become significantly different than the variant that originally infected the node.

RELATED MODELS

Virus, Disease, Preferential Attachment, Diffusion on a Directed Network

NETLOGO FEATURES

Links are used for modeling the network. The `layout-spring` primitive is used to position the nodes and links such that the structure of the network is visually clear.

HOW TO CITE

If you mention this model in a publication, we ask that you include these citations for the model itself and for the NetLogo software:

- Stonedahl, F. and Wilensky, U. (2008). NetLogo Virus on a Network model. http://ccl.northwestern.edu/netlogo/models/VirusonaNetwork. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.
- Wilensky, U. (1999). NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.

COPYRIGHT AND LICENSE