NewsFactor Sci::Tech
Tech Innovation & Discovery

Click here
for one that does.
SOURCEFORGE™

Cascading Failures Could Crash the Global Internet

By Mike Martin
NewsFactor Network
February 06, 2003
http://sci.newsfactor.com/perl/story/20686.html

Eliminating central nodes -- for instance, backbone routers in the Internet -- "is likely to cause subsequent failures and generate a cascade, while eliminating peripheral nodes will have little effect," said Columbia University network expert Duncan Watts.

Could hackers ever shut down the entire Internet? Could terrorists ever cause a blackout so vast it would darken the entire continent?

Yes, say scientists at Arizona State University. Cleverly targeted attacks on complex, real-world networks, such as the Internet and power grids, could lead to a virtual cascade of overload failures that would crash the entire system.

"For networks where loads can redistribute among the nodes, intentional attacks can cause the entire or a substantial part of the network to collapse," mathematics researcher Adilson Motter and electrical engineering professor Ying-Cheng Lai claim in a new paper on the topic published by Physical Review E.

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at +1 (818) 528-1100 or visit http://www.newsfactor.com/about/reprints.shtml.

High-Load Nodes

"Our work shows that in continuously growing networks like the Internet, some nodes become naturally more important than others," Motter told NewsFactor. "From a global perspective, the important nodes are those with exceptionally high loads, which are not necessarily those with the largest number of connections."

Only a few thousand computers, for instance, transmit the bulk of information over the multimillion-computer Internet, Motter explained. "Our work suggests the attack on this small fraction of highly loaded computers may make the entire network collapse," he said.

"This model is an interesting contribution," said Columbia University sociology professor Duncan Watts, an expert in social and structural networks. "Previous models have looked at failures that are driven only by failures of immediate neighbors," he told NewsFactor, "but here failures can be driven by something happening several steps down the line."

The Motter and Lai paper is "an important precursor to a flood of research activity in this area," Los Alamos National Laboratory research scientist Zoltan Toroczkai told NewsFactor. "While simplistic in its assumptions," he said, "the article shows important effects: Knocking out certain nodes can collapse the whole network."

Diversity: Bad for Networks?

The Internet possesses a highly heterogeneous load distribution that creates special vulnerability to attacks on key nodes, Motter and Lai explained. Network nodes are the information equivalent of airline hubs, where electronic data or electrical power flows in and out in many directions.

"In a network of computers, the nodes are computers, and the load is the amount of information a node is required to transmit," Motter said. Networks exhibit homogeneity when the load is about the same in every node, he explained. Nodes in heterogeneous networks, on the other hand, have much more load than average.

In systems where some nodes are central -- for instance, backbone routers in the Internet, "eliminating those nodes is likely to cause subsequent failures and generate a cascade, while eliminating peripheral nodes will have little effect," Watts said. "In systems where all nodes have roughly the same importance -- homogeneous systems -- it doesn't matter much how you pick your targets."

The "really interesting" aspect of cascades, Watts added, "is how apparently insignificant failures can occasionally generate very large cascades. The August 10, 1996, failure in the western U.S. power transmission network is one such puzzling event."

Batten Down the Nodes

Attackers can find the nodes that carry higher loads simply by measuring the network's behavior, Motter pointed out. "For many technological networks, an attacker can obtain at least partial information about the loads, which means that a reliable security system cannot be based on hiding this information."

Nodes with higher loads "should be specially protected -- more protected than any other nodes," Motter said. "Additionally, it is desirable to design intelligent mechanisms of redistribution of load in case of failure of highly loaded nodes."

In certain networks, "vulnerability against intentional attack is mostly removed if one limits the number of links to a node, making the whole structure more homogenous," Toroczkai added. "This is easily achieved by inducing a cost for each link and regulating the maximum number of links a node can have."

Social contact networks provide a "beautiful example where this naturally happens," he noted. "A social contact has to be continuously maintained, which incurs costs and takes time." END

© Copyright 1998-2003 NewsFactor Network. All rights reserved. This material may not be published, broadcast, rewritten or redistributed in any form without written permission. Please click here for legal restrictions and terms of use applicable to this site. Use of this site signifies your agreement to the terms of use. If you would like to reprint content from the NewsFactor Network, click here for pricing information. Privacy Policy.

NewsFactor Front Page | E-Commerce Times | TechNewsWorld | Linux Insider
Wireless NewsFactor | osOpinion | TechExtreme | CRM Daily | CRM Buyer Magazine | FreeNewsFeed