Molecular networks provide insights for computer security

April 29 2014

The robust defenses that yeast cells have evolved to protect themselves from environmental threats hold lessons that can be used to design computer networks and analyze how secure they are, say computer scientists at Carnegie Mellon University.

Environmental "noise" is a key evolutionary pressure that shapes the interconnections within cells, as well as those of neural networks and bacterial/ecological networks, they observe in a paper to be published online April 30 by the *Journal of the Royal Society Interface*. The researchers factored this into an established model for the evolution of molecular connections, resulting in an algorithm that gives rise to a rich range of architectures found in biological, computer and other types of networks. Saket Navlakha, a post-doctoral researcher in CMU's Machine Learning Department, said this approach is particularly helpful in understanding how networks respond to cascading failures, whether it be an overloaded power grid or a computer network being overwhelmed by fake identities in a so-called sybil attack.

The generative model the CMU team developed can be used to tailor networks to the environments in which they are expected to operate. These strike a balance between highly connected networks that are efficient and fast but are prone to infections and cascading failures, such as the Internet and its large service providers, and more sparsely connected elements that are less efficient, requiring more time to relay information, but can better tolerate failures and attacks, such as peer to peer networks. That's a balance that evolution already has achieved in

yeast. A yeast cell has about 6,000 genes, of which 20 percent are considered essential—that is, if the gene is removed, the cell dies. But Ziv Bar-Joseph, an associate professor in the Machine Learning Department and the Lane Center for Computational Biology, said that view of what is essential and what isn't reflects how scientists study genes—by noting their effects on an organism when a gene is removed—not necessarily the gene's importance.

"The cell did not evolve to protect itself against the deletion of these 'essential' genes," Bar-Joseph said, noting that's an event that doesn't often occur in nature.

Rather, the fragility of genes, proteins and other cell components may reflect exposure to their environment. Those that lie near the cell surface, for instance, can expect to encounter lots of environmental stress, so the cell has evolved to tolerate the loss of some of them. Those involved in DNA duplication, on the other hand, normally don't experience that kind of exposure to noise and so don't have the same robust interconnections. That's why the cell dies if one of those genes is removed, Bar-Joseph noted.

Just as biologists study genes by knocking them out, one by one, computer scientists often evaluate network security by removing a server and seeing how the network responds. But Navlakha said that's not always realistic; many attacks or failures of computer and electrical networks can involve the loss of multiple, neighboring nodes.

To better understand the significance of how various networks are interconnected, the Carnegie Mellon researchers, including Christos Faloutsos, professor of computer science, and Xin He, a Lane Fellow in computational biology, modified the well-known duplication-divergence model used to explain the evolution of molecular networks. The concept is that gene duplication can result in two equivalent proteins that, over

time, diverge to develop specialized subtasks, while also maintaining common connections.

By adjusting the duplication-divergence model to account for the pressure of environmental noise, the researchers developed a method that can be used to generate or evaluate the interconnection, or topology, of networks that work in a variety of environments. A military network, for instance, might not worry about malevolent viruses and noise because access is restricted, while a wireless sensor network deployed over a wide area might need to tolerate continual losses of random nodes.

At the same time, the evolutionary role of external noise might well prove to be an insight that will enhance the understanding of biological networks, Bar-Joseph added.

More information: Topological properties of robust biological and computatonal networks, *Journal of the Royal Society Interface*, rsif.royalsocietypublishing.or … .1098/rsif.2014.0283

Provided by Carnegie Mellon University