Modeling Interventions in Complex Networks

ASIM: An Agent-based Integrated Model for Complex Networks

Steven Hofmeyr
Lawrence Berkeley National Laboratory
1 Cycltron Rd, Berkeley CA 94720

Stephanie Forrest
University of New Mexico
1 University Ave, Albuquerque, NM 87131

Abstract

A common characteristic of complex networks is the presence of malicious elements. These range from bacteria and viruses in the body to criminals in societies to malicious software (malware) in computer networks. At best, these malicious elements reduce the efficiency and reliability of the network; at worst they can cause catastrophic failure. Typical approaches to managing malicious agents are ad-hoc and localized. It can be very expensive and difficult to implement large-scale counter-measures (e.g., the immune system is an expensive part of the body), and equally difficult to understand their impact. The difficulty is exacerbated by the fact that multiple timescales are involved, and the networks evolve and change, as do the malicious elements themselves.

In our research we develop models of complex networks to study the impact of various interventions in a controlled manner, with the ultimate goal of providing a tool to policy-makers and others that could be used before implementing counter-measures in real systems. Over the past decade, there has been extensive research on generic models of complex networks that aim to explain high-level, common properties, such as degree distribution and other statistical properties of network structure. Our interest in interventions has led us to go deeper, incorporating domain-specific features that are relevant to the sorts of counter-measures that are possible.

In this talk, we focus on the Internet, which is one of the largest and most complex human artifacts ever created. The Internet resembles many technological networks within the purview of the DOE and is suitable for studying a wide variety of interventions. Specifically, we aim to answer the question of what high-level policies might best control the spread of malware in technological networks. For the Internet there is an emerging consensus among policy makers that interventions undertaken by Internet Service Providers (ISPs) are the best point to counter the rising incidence of malware. However, assessing the suitability of countermeasures at this scale is challenging.

To explore this issue, we used ASIM, an agent-based model of the Internet at the Autonomous Systems (AS) level. ASIM incorporates traffic, geography and economics as domain-specific components. Using a wide variety of metrics, we have shown that ASIM is an accurate model of the Internet at the AS-level, and is better than current alternative models. To study interventions, we used ASes as proxies for ISPs, which is reasonable because most large ASes are indeed ISPs. We extended ASIM to incorporate a simple notion of malware, and modeled the flow of malicious traffic across the AS network. We collected data on infections and used this to show that our model generates realistic distributions of malware.

We studied interventions that reduce the flow of malicious traffic, such as filtering egress traffic. Some of the results are to be expected, for instance, we found that coordinated intervention by the 0.2%-biggest ASes is more effective than uncoordinated efforts adopted by 30% of all ASes. Other results are more surprising, for example, blacklisting ASes that generate lots of malicious traffic can actually result in an *increase* in malicious traffic as the network evolves. Furthermore, using ASIM, we can quantify and compare positive externalities created by the different countermeasures. and explore which types and levels of intervention are likely most cost-effective at large scale. Our results illustrate the potential of agent-based models to help us understand how to deal with malicious elements in complex networks.