Chapter IV

Network Robustness for Critical Infrastructure Networks

Anthony H. Dekker,
Defence Science and Technology Organisation, Australia

Bernard Colbert, Deakin University, Australia

Abstract

Events of the past few years have shown how today’s modern technological society is critically dependent on critical infrastructure networks such as telecommunications, transport and power. In this chapter, we examine the robustness of critical infrastructure networks and describe some simulation studies exploring this issue. These studies use an extension of data farming we call “network farming,” implemented within the CAVALIER network analysis tool suite. We then survey some historical data on actual terrorist attacks and show that the distribution of these attacks in time can be modeled by a Poisson statistical distribution. This fact can then be used to plan robust network architectures. We also
examine “scale-free networks,” and show how they relate to the robustness of physical and organizational networks. In particular, we study the implications for law-enforcement personnel responding to terrorist organizations, using two historical case studies. Finally, we briefly survey emerging trends in network modeling and intelligent software agents that may influence the robustness of future networks.

Introduction

In today’s modern technological society, we all are dependent on critical infrastructure networks such as telecommunications, transport and power. The terror attacks that destroyed the Twin Towers in New York City on September 11, 2001 also destroyed elements of the civilian telecommunications infrastructure, including Verizon’s central telephone switch. This underlined the vulnerability of network nodes to terrorist attack and the ability of terrorist organizations to launch multiple synergistic attacks.

In this chapter, we examine the robustness of critical infrastructure networks; specifically, aspects that relate to the network topology, or the shape of the network, rather than other network characteristics, such as management and control or physical security. We describe some simulation studies that use an extension of data farming (Horne, 1997), which we call network farming. This methodology is a natural way to explore network design, and our simulations identify a number of characteristics that make a network robust in the face of terrorist attacks. Specifically, node connectivity and symmetry are identified as important characteristics and, in general, networks begin to fail when the number of attacks is equal to the node connectivity.

We have developed a tool suite for analyzing, visualizing and simulating networks, called CAVALIER (Dekker, 2001, 2003), which we briefly describe. This tool suite forms the basis for a Network Information System in the sense of Carling and Carlsen (2002). The highly important role of critical infrastructure networks means that Network Information Systems are essential for managing them.

We also survey historical data on terrorist attacks by seven terrorist groups (International Policy Institute for Counter-Terrorism, 2004), and show that the distribution of these attacks can be modeled by a Poisson statistical distribu-
Related Content

Identification, Authentication, and Access Control
www.irma-international.org/chapter/identification-authentication-access-control/25674/

Joo S. Lim, Sean B. Maynard, Atif Ahmad and Shanton Chang (2015). International Journal of Cyber Warfare and Terrorism (pp. 31-52).
www.irma-international.org/article/information-security-culture/138277/

Critical Information Infrastructure and Cyber-Terrorism
Olivia Bosch (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization (pp. 31-40).
www.irma-international.org/chapter/critical-information-infrastructure-cyber-terrorism/72166/

The Value of Personal Information
www.irma-international.org/chapter/the-value-of-personal-information/141043/

Cyber Readiness: Are We There Yet?
www.irma-international.org/article/cyber-readiness/124129/