Chapter 9
Fortifying Large Scale, Geospatial Networks:
Implications for Supervisory Control and Data Acquisition Systems

Alan T. Murray
Arizona State University, USA

Tony H. Grubesic
Drexel University, USA

ABSTRACT

Large scale, geospatial networks—such as the Internet, the interstate highway system, gas pipelines, and the electrical grid—are integral parts of modern society, facilitating the capability to communicate, transport goods and services between locations, and connect homes and businesses to basic necessities like water and electricity. The associated management and protection of this critical infrastructure is a challenging task because it is often compromised or damaged by natural disasters, human error, or sabotage. Further, the cascading effects associated with disruptions can impact related interdependent infrastructure, such as supervisory control and data acquisition systems (SCADA). In this context, although the protection and/or hardening of network elements can reduce disruptive impacts, the cost to protect all equipment in the system is prohibitive. The purpose of this chapter is to detail an optimization approach for selecting elements on a network to be protected, under budget constraints, in order to maximize system performance if one or more components are damaged or destroyed. Applications results for a large scale, geospatial network are explored and presented, illustrating problem complexities as well as the potential for informed strategic investment decision making. The implications for SCADA systems relying on large scale geospatial networks, including the public Internet, are also discussed.

DOI: 10.4018/978-1-4666-4707-7.ch009

INTRODUCTION

Large-scale, geospatial networks are integral parts of modern society, facilitating the capability to communicate, transport goods and services between locations, as well as connecting homes and businesses to basic necessities like water and electricity (Grubesic and Murray, 2006).

Continued and uninterrupted performance of critical infrastructure systems is a top priority for federal, state and local governments, management agencies or service providers in charge of such systems. Unfortunately, service disruptions are inevitable. Everything from intermittent outages in Internet access to power blackouts and routine highway maintenance highlights the difficulties in continued and uninterrupted system performance. Critical infrastructure systems and associated network infrastructures (e.g. electrical grid, gas pipelines and telecommunication systems) are also vulnerable to catastrophic failure, natural disasters and sabotage, all of which disrupt systems in predictable (and sometimes unpredictable) ways.

Of particular importance is the increasing level of interconnectivity between critical infrastructure systems and supervisory control and data acquisition systems (SCADA). Although there are many ways to conceive of, represent and detail the complex interdependencies between these systems, their increasing level of interaction through remotely controlled Internet-based platforms can pose a significant threat to the global economy if they are not secured (Fernandez and Fernandez, 2005). Specifically, although there is a growing emphasis on the cyber security of SCADA systems (Igure et al., 2006), physical threats and destruction of industrial control systems remain the largest threat to critical infrastructure (Oman et al., 2001). Further, it is important to note that physical threats do not always represent a direct attack. Cascading failures (Little, 2002; Grubesic and Murray, 2006), where a disruption in one system triggers the failure of interconnected systems, are relevant when detailing interactions between large scale networks and SCADA systems.

Where critical infrastructure networks are concerned, they are typically composed of components identified as nodes/vertices and arcs/edges (Murray and Grubesic, 2007). Arcs connect pairs of nodes to form a graph. For example, in a telecommunications network, nodes often represent systems for routing data packets on the network and arcs represent the cables physically connecting routers. In a gas pipeline, the systems which control pumping stations can represent a node and the pipelines which transport the liquefied gas represents the arcs. Given the network, there are many ways that a system performs or operates. Commonly considered modes of performance associated with network vulnerability include (Murray 2012): maximum flow through the network (Wollmer 1964; Baran 1964), shortest path between an origin and destination (Harding 1977; Corley and Sha 1982), and connectivity and flow between all origins and destinations (Albert et al. 2000; Myung and Kim 2004; Murray et al., 2007).

Irrespective of the particular network system performance measure being examined, consequences arise when either components (nodes or arcs in a network) are interdicted or damaged in some way.[1] The loss of one, two or more components can result in a measurable decrease in system functionality. Given that components could be rendered inoperable due to failure, natural disasters and/or sabotage, management and oversight of network infrastructure has recognized the importance of protection and hardening of system controls and components, or more generally fortification (see Church et al. 2004; Brown et al. 2006; Sternberg and Lee 2006; Powell 2007; Scaparra and Church 2008a,b; Murray and Grubesic 2012).

The general problem of interest along these lines may be stated as follows: