Chapter 9

Information Data Fusion and Computer Network Defense

Mark Ballora
The Pennsylvania State University, USA

Nicklaus A. Giacobe
The Pennsylvania State University, USA

Michael McNeese
The Pennsylvania State University, USA

David L. Hall
The Pennsylvania State University, USA

ABSTRACT

Computer networks no longer simply enable military and civilian operations, but have become vital infrastructures for all types of operations ranging from sensing and command/control to logistics, power distribution, and many other functions. Consequently, network attacks have become weapons of choice for adversaries engaged in asymmetric warfare. Traditionally, data and information fusion techniques were developed to improve situational awareness and threat assessment by combining data from diverse sources, and have recently been extended to include both physical (“hard”) sensors and human observers (acting as “soft” sensors). This chapter provides an introduction to traditional data fusion models and adapts them to the domain of cyber security. Recent advances in hard and soft information fusion are summarized and applied to the cyber security domain. Research on the use of sound for human-in-the-loop pattern recognition (sonification) is also introduced. Finally, perspectives are provided on the future for data fusion in cyber security research.

INTRODUCTION

Historically, an enormous amount of research and development on information fusion has been conducted in support of military operations (e.g., fusion of multi-sensor data for target tracking, identification, and threat assessment and situation awareness) (Hall and McMullen, 2004) (Liggins et al., 2008). The research has included development of process models, creation of algorithms for signal and image processing, pattern recognition, state estimation, automated reasoning, and dynamic resource allocation.
This chapter adapts these models to the domain of cyber security. This is a field in which data fusion techniques and terminology are becoming increasingly relevant, given the complex tasks of maintaining overall awareness of a network’s current status, projecting future actions of adversaries, and making timely adjustments. Following a discussion of hard and soft information fusion and their relevance to the cyber security domain, we propose a novel means of situational awareness involving an auditory representation (sonification) of network traffic.

The Organization of this Chapter

This chapter is organized as follows. We begin by exploring some of the background research in three areas of interest—use of humans as soft sensors, data fusion technologies in cyber security, and sonification. The first content area of human-centric information fusion outlines the use of humans as “soft” sensors. The second content area presents the general data fusion framework (the JDL model) as it applies to the cyber security context. The third main content area, sonification, is construed as a cognitive refinement. The chapter concludes with a discussion of future research directions in cyber situational awareness.

BACKGROUND

The Changing Landscape: Humans as Observers

It is clear that for a variety of applications—ranging from asymmetric warfare to emergency crisis management to business applications—a need exists to characterize and understand the human landscape. In understanding and addressing natural disasters such as Hurricane Katrina in New Orleans (Palser, 2005), it is clearly insufficient to observe and predict weather patterns, model the interaction between high winds, buildings, and other structures. While these are clearly factors to be considered, we must also address information such as population locations and demographics. We must understand how people of different ages, socio-economic backgrounds, cultures and experiences might react to a major disaster and to each other. Information and models are needed that address attitudes, reaction patterns, reactions to outside aid agencies and people, and ways that the news media affect the dynamics of the interactions—to list just a few factors. In regards to the cyber-security domain, we will need an understanding of the adversaries who plan and effect network attacks (e.g., their strategies, weaknesses, rules of engagement, and cultural imperatives) if we ever seek to become predictive, rather than simply reactive, to cyber attacks.

The Data Fusion Process Model and Cyber Security

Historically, data fusion research has focused primarily on utilizing physical sensors to observe and characterize the physical landscape. The Joint Directors of Laboratories (JDL) Data Fusion Process Model (Kessler et al., 1991) has become a standard model to describe the process of receiving multi-sensor data, annotating it, and fusing common threads in order to create predictive capabilities. The process is broken down into a series of levels, each of which adds a layer of intelligence and inference.

The data fusion process for military applications can be leveraged to characterize the cyber “landscape.” The chapter summarizes the JDL model, illustrates its relevance to cyber security, and describes new trends in human-centered information fusion (Hall and Jordan, 2010) that impact cyber security (viz., the utilization of human observers to augment physical sensors, use of human pattern recognition and semantic level reasoning for improved inferencing, and collaborative decision-making).