Chapter 53
A Fuzzy Cyber-Risk Analysis Model for Assessing Attacks on the Availability and Integrity of the Military Command and Control Systems

Madjid Tavana
La Salle University, USA & University of Paderborn, Germany

Dawn A. Trevisani
Air Force Research Laboratory, USA

Dennis T. Kennedy
La Salle University, USA

ABSTRACT

The increasing complexity in Military Command and Control (C2) systems has led to greater vulnerability due to system availability and integrity caused by internal vulnerabilities and external threats. Several studies have proposed measures of availability and integrity for the assets in the C2 systems using precise and certain measures (i.e., the exact number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, the effectiveness of the availability and integrity countermeasure in eliminating the threats, and the financial impact of each attack on the availability and integrity of the assets). However, these measures are often uncertain in real-world problems. The source of uncertainty can be vagueness or ambiguity. Fuzzy logic and fuzzy sets can represent vagueness and ambiguity by formalizing inaccuracies inherent in human decision-making. In this paper, the authors extend the risk assessment literature by including fuzzy measures for the number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, and the effectiveness of the availability and integrity countermeasure in eliminating these threats. They analyze the financial impact of each attack on the availability and integrity of the assets and propose a comprehensive cyber-risk assessment system for the Military C2 in the fuzzy environment.

DOI: 10.4018/978-1-4666-7456-1.ch053

INTRODUCTION

The military Command and Control (C2) systems are generally subject to high failure rates because the complex interactions among their components cannot be thoroughly planned, understood, anticipated and guarded against. Availability in military C2 systems is defined as "assured access by authorized users" and integrity is defined as "protection from unauthorized change" (Armistead, 2004, p. 71). Cyber-attacks have a direct impact on the C2 systems in terms of availability and integrity and several approaches have been suggested to eliminate or minimize them. Most system availability and integrity studies in the literature use *precise and certain* measures (i.e., the exact number of attacks on the availability and the integrity, the number of countermeasures for the availability and integrity attacks, the effectiveness of the availability and integrity countermeasure in eliminating the threats, and the financial impact of each attack on the availability and integrity of the assets). However, these measures are often uncertain in real-world problems. The source of uncertainty can be vagueness or ambiguity. Fuzzy logic and fuzzy sets can be used to represent vague and ambiguous information and formalize inaccuracy and uncertainty in human decision-making.

We develop a risk analysis model for assessing cyber-attacks on the availability and integrity of the military C2 systems. We measure availability and integrity and use an interactive model to plot the fuzzy availability and fuzzy integrity measures in a Cartesian coordinate system for various time periods. We identify whether the C2 system is in the possession, preservation, restoration, or devastation state. The remainder of this paper is organized as follows. We first provide a high-level overview of the existing approaches to operational risk quantification. The mathematical details of the cyber-risk analysis model proposed in this study is presented next. We then demonstrate a case study to exhibit the efficacy of the procedures and algorithms and show the applicability of the proposed method. We conclude with our conclusions.

LITERATURE REVIEW

Several methods have been proposed in the literature to deal with imperfect data. Imperfect data can be characterized as being imprecise or uncertain. Other types of imperfect data such as vague or ambiguous data can be considered a special form of imprecision or uncertainty (Smets, 1997). Bayesian theory is often used to deal with both imprecision and uncertainty (Fienberg, 2006; Howson & Urbach, 1993; Jaynes, 2003). The theory of evidence is also used to deal with data that contains both imprecision and uncertainty at the same time (Shafer, 1976; Dempster, 1967). However, rough sets theory is used to handle imprecision when uncertainty is involved but cannot be quantified (Pawlak, 1991). The theory of possibility is used to handle incomplete data, which is a combination of imprecise and uncertain data (Zadeh, 1978). In contrast with these theories that can only handle one type of imperfection, random sets and the conditional event algebra can handle all types of imperfect data (Goodman et al., 1997). We use fuzzy values in our model to represent vagueness and ambiguity. Fuzzy logic enables computation in the face of vagueness and ambiguity, generating approximate results (Nedjah & Mourelle, 2005). While uncertainty represents the state of knowledge about a piece of data, imprecision is the characteristic of the data that cannot be expressed with a single value. The theory of fuzzy sets has been proposed by Zadeh (1965) to deal with vague data which is a particular form of both imprecise and uncertain data. Fuzzy sets have been used to account for the vague data in various work flow management systems (Lin et al., 2007; Tsai & Wang, 2008). The membership function of a fuzzy set defines the mapping of