Chapter 10
A Theoretic Representation of the Effects of Targeted Failures in HPC Systems

A. Don Clark
West Virginia University, USA

ABSTRACT

High performance computing (HPC) systems are becoming the norm for daily use and care must be made to ensure that these systems are resilient. Recent contributions on resiliency have been from quantitative and qualitative perspectives where general system failures are considered. However, there are limited contributions dealing with the specific classes of failures that are directly related to cyber-attacks. In this chapter, the author uses the concepts of transition processes and limiting distributions to perform a generic theoretical investigation of the effects of targeted failures by relating the actions of the cyber-enemy (CE) to different risk levels in an HPC system. Special cases of constant attack strategies are considered where exact solutions are obtained. Additionally, a stopped process is introduced to model the effects of system termination. The results of this representation can be directly applied throughout the HPC community for monitoring and mitigating cyber-attacks.

INTRODUCTION

High performance computing (HPC) systems use supercomputers and computer clusters to perform complex processing and computational applications. In the scientific domain, HPC systems have been used to solve sophisticated computational problems in technical areas such as meteorology, fluid dynamics, and big data analytics. For military operations, these systems are currently being used for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Because data parallelism has enhanced the performance of HPC systems by several orders of magnitude (Nyland, Prins, Goldberg, & Mills, 2000; Ravichandran, Pantel, & Hovy, 2004), HPC systems will interest business of all sizes due to the increasing demands of processing power and speed. Although HPC systems have demonstrated computational prowess, in terms of solving complex problems efficiently, the reliability

DOI: 10.4018/978-1-5225-0287-6.ch010

of these systems is expected to decrease as more and more systems are moving towards the design of petascale and exascale class systems (Shroeder & Gibson, 2007; Chen & Dongarra, 2009). Furthermore, researchers have noted that when undesirable failure rates occur, troubleshooting HPC systems is difficult because they are massive in both component count and complexity (Robinson & Stearly, 2011). These factors also make HPC systems vulnerable to cyber-attacks. Therefore, care must be made to ensure that these systems are resilient.

In terms of HPC systems, resilience is defined as the ability of a system to continue operation despite the presence of faults associated with it (DeBardeleben *et al.*, 2009). With this in mind, researchers have focused their attention on developing quantitative and qualitative methods for reliability and resilience detection and analysis. Work in these areas include system failures, application failures, and fault tolerance (Daly, Pritchett, & Michalak, 2008; Jones, Daly, & DeBarteleben, 2008; Raicu, Foster, & Zhao, 2008), where the primary goal is to continue running within some performance threshold when one or more system failures occur. Although research in this area help to provide various classes of processes to handle certain general families of failures, these failures do not directly consider *targeted failures* – when deliberate attacks affect overall system performance. In these cases, continuing to run the system when failures occur could be detrimental because the cyber-enemy (CE) could learn about the system and submit subsequent attacks that manipulate and cause serious damage resulting in system shut-down. Furthermore, these attacks are not necessarily related to the system failure rate, which has an inverse relationship to the mean time between failures. In other words, attacks can happen when either the failure rate is both low, representing a more reliable system, or when the failure rate has increased. Additionally, flexibility, in stopping the system, needs to be accounted for to consider times when technicians and engineers stop the system when anomalies occur. Therefore, care must be made to account for the effects of targeted failures by considering when actions of the cyber-enemy (CE) while considering the failure rate of the system.

The author addresses these concerns by conducting a theoretical investigation of the effects of targeted failures in HPC systems by modeling the relationship between the failure risk levels and the actions of the cyber-enemy (CE). From the general abstract formulation, cases of continuous and constant-level cyber-attacks are considered, where closed-form dynamical solutions are obtained. Next, for the case of two-level constant attacks, extreme conditions related to the system failure rate are considered that include the most reliable and least reliable systems. Then, a theoretic formulation is proposed that models the effects of system termination in terms of a stopped process. The investigations posed in this chapter provide scientists, engineers, and technicians a universal understanding of the overall dynamics to design effective strategies for mitigation. Furthermore, the mathematical model posed provides technicians of HPC systems, such as systems administrators (SAs), the macro understanding prior to troubleshooting these systems on a micro, or component, level.

This chapter is organized in the following manner. The next section provides a summary of the background and literature review. This is followed by a section that describes the theoretical description of the model, which is based on the work of Faissol and Gallagher (Faissol & Gallagher, 2014). It is here where dynamical representations are posed for one and two-level constant attack strategies. Next, the description of system termination is also proposed in the third section. And, lastly, the conclusions along with the future directions of this work are presented in the final two sections.