Reliability Engineering and System Safety 169 (2018) 224–234

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Defending a cyber system with early warning mechanism

Die Chen [a], Maochao Xu [b,*], Weidong Shi [c]

[a] School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu, China
[b] Department of Mathematics, Illinois State University, Normal, IL, USA
[c] Department of Computer Science, University of Houston, Houston, TX, USA

ARTICLE INFO

Keywords:
Camouflage
Early warning
Optimal strategy
Resource allocation
Variance

ABSTRACT

Due to the increasing reliance on networks, defending a cyber system is of vital importance. In this paper, we consider an important mechanism of early warning for defending a cyber system that has become a key component of constructing network defense in practice. We study the reliability of a system under attack from single or multiple sources. In particular, we discuss the effect of an early warning mechanism on the system reliability. We then propose the optimal strategy for defending a cyber system with early warning components in the worst attack scenario. The theoretical results are further validated by simulation evidence.

1. Introduction and motivation

Cyber systems have become underlying pillars for various infrastructures and physical systems (e.g. network control systems and cars). Because the cyberspace is extremely difficult to secure due to its complexity, cyber attacks have become serious threats to cyber–physical systems, infrastructures, and even national security. Therefore, defending a system under attack has attracted much attention in the literature. In particular, much effort has been spent on the optimal defense strategies against attacks under some specific conditions. For example, Bier et al. [4] used the game theory approach to identify the optimal defense strategy in response to intentional attacks on the system reliability. Under certain conditions, they derived closed form results for series, parallel, and moderately general structure systems. Bier et al. [2] studied a strategic model in which a defender allocates defensive resources to several locations while an attacker chooses a location to attack. One may refer to [3,4,25] for more discussions on the game theory approach for defending a system. The optimal strategy for allocating an attacker's constrained resource to a parallel system is extensively studied in [5,12]. The optimal resource allocation in the scenario of multiple attacks against a single target is studied in [5]. Levitin and Hausken [15] discussed the optimal strategy to achieve the highest destruction probability of the target and the least expenditure of attacks. One may refer to [7] for a comprehensive review of recent developments on the defense and attack models.

The most effective way to improve the system reliability is to reduce the compromise probabilities of system working components. For an attacker, the cost of compromising a component depends on the component's vulnerabilities and the attacker skill level [17]. In the literature, there are some discussions on the approaches to improving a system reliability. For example, Levitin and Hausken [13] proposed three approaches to improving a system reliability which include component protections, camouflage components, and redundant components. Allocating more resources to the working components can certainly reduce the vulnerabilities of the components, and hence improve the system reliability. Distributing camouflage components can reduce the probability of critical components being attacked [18]. Hausken and Levitin [6] studied the optimal distribution of the defense resources between protecting the genuine system elements and deploying camouflage (false) elements in a series system. It is assumed that the camouflage and genuine elements cannot be distinguished by the attacker, and the system is destroyed if any genuine element is destroyed. Levitin et al. [10] studied a parallel system subject to external intentional attacks (e.g. malicious attacks) and unintentional impacts (e.g. natural disasters). The defender distributes the resource between the deployment of camouflage targets and the protection of genuine system elements. They suggested a framework for the optimal defense resource distribution to minimize the overall system vulnerability. Peng et al. [19] considered a system subject to external intentional attacks, where the defender can distribute the resource for camouflage and working components. It is assumed that the camouflage components are not perfect, i.e., there is a nonzero probability that a false target can be detected by the attacker. The attacker launches the attacks when a certain number of camouflage components has been detected. They discussed an optimal defense strategy under uncertain contest intensity. Levitin and Hausken [16] studied the optimal defense and attack strategies in

* Corresponding author.
E-mail address: mxu2@ilstu.edu (M. Xu).

http://dx.doi.org/10.1016/j.ress.2017.08.021
Received 23 January 2017; Received in revised form 13 August 2017; Accepted 29 August 2017
Available online 5 September 2017
0951-8320/

a system with camouflage components, where the system is under two sequential attacks. They considered the cases of perfect and imperfect detection of the targets destroyed in the first attack. The defender determines the number of camouflage components to deploy, the number of camouflage components to protect, and the defense strategy is analyzed based on a two period minmax game. Peng et al. [20] assumed that the detection probability of each camouflage target is a function of the intelligence and disinformation efforts allocated on the camouflage target. They investigated the optimal resource distribution between target identification and attack efforts via a non-cooperative two period minmax game. Redundancy is the duplication of critical components or functions of a system which can result in more time and resources for an attacker to compromise the system [14]. The strategies of allocating resources between deploying camouflage components and enhancing component protection are discussed in [11]. It is worth remarking that Wang et al. [23] discussed the approach to hide the location of core components of a system under cyber attacks to improve the system reliability. They discussed optimal resource allocation for improving system reliability under random attacks; see also [24].

In this paper we study a cyber system equipped with a particular defense mechanism known as cyber *early warning* [9]. This mechanism exploits cyber threat intelligence (e.g., the compromised or malicious computers) to mitigate the damages that can be caused by the threat in question (e.g., the attack attempts from those malicious computers are blocked before they reach their attempted targets). The cyber early warning can quickly react when the cyber attacks take place based on system security strategies like alarms, tracking, and blocking the cyber attack. The cyber early warning mechanism can be in the forms of a proxy firewall, network monitor, honeypot, and intrusion detection module etc. Although the early warning mechanism has become a key technology of constructing network defense, to the best of our knowledge, there is no study on the reliability analysis of a system equipped with early warning components under cyber attacks (at least in the domain of reliability engineering). The present study aims to study a cyber system with a limited defense resource under random attacks from one source or multiple sources. The early warning mechanism is in the form of network security components (or monitors). The early warning is activated when an early warning component is under attack, and it will block the attacks from the attack source (e.g., the IP address). In other words, the attack source (e.g. malicious IP address) observed by the early warning component during time interval t cannot launch any attacks against the system during time interval $t+1$ (see, for example, [26]). We assume that the defense resource can be used to create protections, camouflage components, and early warning components. We do not consider the redundancy since the critical components can be very expensive in practice. Through the reliability analysis of the cyber system, it is found that the early warning mechanism can significantly improve the system reliability. It can also reduce the variance of system reliability under certain conditions. We also discuss the optimal strategy for allocating the limited defense resources to the system under attack from a single and multiple sources. The simulation study is also presented to validate our theoretical results.

The rest of the paper is organized as follows. In Section 2, we first propose a novel cyber model with early warning mechanism. We then derive the reliability function of a system under attack from one or multiple sources are derived. Section 3 presents a detailed discussion of system reliability against its parameters including number of attacks, early warning mechanism, and number of attack sources. In Section 4, we discuss the optimal strategy for defending a system with a limited resource. The simulation study on the reliability function and variance of reliability function is presented in Section 5. In the last section, we conclude our results and discuss some future work.

The following table summarizes the main notations used in the paper:

N_p	number of working components
N_c	number of camouflaging components
N_w	number of early warning components
N_a	number of attacks
N_s	$N_p + N_c + N_w$
R_d	total defense resource
R_a	total attack resource
r_d	defense resource on each working component
r_a	attack resource needed per attack

2. Cyber model with early warning mechanism

2.1. A novel model

We assume that the cyber system consists of N_p working components. The system will be compromised only if all the working components are compromised. This phenomenon can be considered as a parallel system in the reliability engineering. The defender is granted a total defense resource R_d which can be used to create the protection for the working components, camouflage components, and early warning components. Assume that the cost for creating a camouflage component is C, and an early warning component is W. Then, the resource that can be employed on each working component is

$$r_d = \frac{R_d - N_c \times C - N_w \times W}{N_p}. \tag{1}$$

Assume that the attacks are random where the attacker cannot distinguish the differences among working components, camouflage components, and early warning components. The attacks are assumed to arrive in sequence. An early warning component is activated if it is attacked, and then it will block all the attacks from the same source. On the other hand, the attacker can decide the number of attacks to launch against the target. Assume the total amount of attack resources is R_a, and these resources are evenly distributed among the attacks. Then the cost of each attack is $r_a = R_a/N_a$, where N_a is the number of attacks launched by the attacker. We consider the following two scenarios:

- *Attacks from a single source*. For this scenario, the attacks are all from a single source, or the attacker only has one type of attacks. Fig. 1 illustrates the attack process. The system consists of three working components, two camouflage components, and an early warning component. Assume that an attacker launches random attacks against the system as the attacker cannot distinguish the working components from the others. In Fig. 1, it is seen that four of the first six attacks are on the working components while two of them are on the camouflage components. The seventh attack is caught by the early warning component (or activates the early warning mechanism), and the rest of the attacks are blocked. Since all the attacks are from a single source, the system is no longer under attack when the early warning mechanism is activated.
- *Attacks from multiple sources*. In this scenario, attacks are from multiple sources, or the attacker has different types of attacks. For example, an attacker can launch DDoS (distributed-denial-of-service) attacks, which focuses on disrupting the service to a system. For these attacks, the attacker often uses multiple computers to send the traffic or data to overload the system, leading to serious security breaches and financial losses. For this case, the attacks are from different sources. The attack process from multiple sources is similar to the aforementioned single source attack process. However, if an early warning component only captures attacks from partial sources, it can only block the attacks from those sources. The attacks from other sources may still harm the system.