# 新型主动防御框架的资源对抗模型分析

陈双喜[1,2,3],吴安邦[1],岐舒骏[4],刘 会[2],吴春明[1]
(1. 浙江大学,浙江杭州 310058; 2. 嘉兴职业技术学院,浙江嘉兴 314036;
3. 阿拉巴马大学,阿拉巴马州塔萨卡鲁萨 35401;4. 杜克大学,北卡罗莱纳州达勒姆 27708)

**摘 要:** 本文提出了一种基于拟态理论的主动防御的新型框架. 通过引入常微分动态系统来表述新型主动防御框架的动态化和结构化特点. 通过常微分方程,将部分现实中的复杂网络攻防问题转化为简单的、准确定义的资源对抗模型. 由此,可以对通过异构冗余和自修复性构建的主动防御系统的关键构造获得一种对抗模型分析. 本框架可帮助实现对当前网络主动防御系统的有效性评估并通过选取有效的防御策略来加强系统安全性.

**关键词:** 网络主动防御; 拟态化; 常微分动态系统
**中图分类号:** TN915.08 **文献标识码:** A **文章编号:** 0372-2112 (2019)07-1557-09
**电子学报 URL:** http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.07.022

# Analysis of Resource Defense Model for Novel Active Defense Modeling

CHEN Shuang-xi[1,2,3], WU An-bang[1], QI Shu-jun[4], LIU Hui[2], WU Chun-ming[1]
(1. *Zhejiang University, Hangzhou, Zhejiang* 310058, *China*;
2. *Jiaxing Vocational and Technical College, Jiaxing, Zhejiang* 314036, *China*;
3. *The University of Alabama, Tuscaloosa* 35401, *USA*; 4. *Duke University, Durham, North Carolina* 27708, *USA*)

**Abstract:** In this paper, a brand-new active defense framework based on CMD (Cyberspace Mimic Defense) theory is proposed. The dynamic and structural characteristics of this framework are described by introducing ordinary differential dynamic systems. Through ordinary differential equations, some complex network attack and defense problems in reality are transformed into simple and precisely defined resource confrontation models. Hence, we can get a countermeasure model by constructing key structural details of the active defense system based on the characteristics of heterogeneity, redundancy and self-repairing. This framework can help to evaluate the effectiveness of current network active defense systems and enhance their security by selecting effective defense strategies.

**Key words:** network active defense; virtualization; ordinary differential dynamic system

## 1 引言

### 1.1 网络安全背景

网络安全的问题是一个重要且复杂的问题. 传统的信息安全保护方法具有静态性、相似性等特点,使得传统保护方法具有很强的被动性[1]. 随着攻击技术的发展,静态防御技术已经不能够很好地确保目标系统的安全. 被动的网络安全框架模型已经暴露出问题[2],面对日益复杂和千变万化的各种入侵事件,被动防御的方法和体系不足以解决现有的种种安全问题. 随着时间的推移,网络对抗环境中的动态防御趋势逐步加强,安全防护技术正在从静态保护转向纵深防御和动态防御发展[3~5].

主动防御的动态框架是一种在安全防御体系层面上部署动态变化的防御策略. 当前广泛使用的传统网络安全防御手段主要采用了防火墙、入侵检测和病毒防范组成的被动消极的封堵策略. 这样的防御策略就如同我们家中用的纱窗和蚊香,阻挡蚊虫进入家中和对进入的蚊虫范围性的灭杀. 几年前,这种防御技术仍被认为是网络安全空间中唯一有效的防御策略. 但随着网络安全的不断发展,这种静态被动的防御手段已然无法满足当前网络环境的安全需要,动态化的网络

收稿日期:2017-07-18;修回日期:2018-03-12;责任编辑:张奕翔
基金项目:浙江省公益技术应用研究 (No. 2016C31096);国家重点研发计划(No. 2016YFB0800102);浙江省重点研发计划(No. 2017C01064);国家留学基金委员会(No. 201608330492);嘉兴市科技计划(No. 2014AY21021)

防御手段也因此而生. 主动防御的动态化框架可部署于软件,网络,平台和数据等多个层面[6],配合重配置,内容分发,随机化等手段,使系统进入新的节点或是状态,而与之前的状态无较大的关联关系,并以此来实现对系统接收影响的动态变化,保证系统的安全性与持续性[1,6].

主动防御的异构是通过对整个系统各个不同组件采用不同的实现方式和运行方式来避免整个系统被单一的攻击策略所攻破,以此提升整个系统的安全性. 对目标系统环境的侦查往往是攻击方发动攻击的第一步,防御方通过对系统环境的异构,可以增加攻击方的攻击难度,甚至迷惑攻击方. 通常安全空间中系统的异构通过使用不同的软件和硬件构造、操作系统、虚拟机、不同的程序语言、不同的处理器等[7]方式来实现. 这种异构既可以是构建在空间层面上对整个系统的一个或多个层次进行异构,也可以部署在时间上对同个层次在时间链上的不同节点使用异构.

冗余的实现开始于计算机的起源,最开始时是为了规避意外等事故造成的不可预估的数据改变,使用多个设备对同一结果进行计算,从而保证结果的可靠性[8]. 美国空军战斗机的作战指令曾使用三台电脑同时发送,战机收到指令后对三条指令进行对比以防止指令传输中某台电脑出现问题的策略. 而之后冗余技术发展和融合运用到网络安全中,常常与异构相结合,实现时间和空间上的双重冗余,而不再局限于物理资源上的冗余[9]. 如 TCP 握手的重传机制等实现便是时间冗余的例子.

虚拟化技术的核心是对物理硬件层设计资源的抽象. 通过虚拟化技术,虚拟硬件层被提供给了虚拟服务器,虚拟服务器则向用户传递了一系列的服务[10]. 虚拟化技术的设计实现为安全系统提供了有效的隔离和分段手段,结合动态化特性,使得整个安全空间提供的虚拟服务与物理资源隔离变化,提升安全性.

网络安全中的自修复是指,系统在受到攻击,并被攻入后,系统能够容忍被入侵所带来的危害和影响,保持系统运行提供服务,并能自行从被入侵状态中回复为正常的运行状态以提供正常的服务. 如 SCIT 架构,通过轮转纯净的服务器上线服务,下线的服务器则进行清理. 通过实现服务运转的服务器进行轮转,可以保证整个系统的服务始终保持稳定,并能从已受到的攻击中恢复[11].

拟态安全思想是以异构冗余、动态化、随机化为核心的主动变迁机制作为主要核心的防御策略. 该策略突出两点:一是将安全空间中的系统进行组件的分隔冗余;二是实现变迁,使得攻击者难以探查到实际的、可攻击的系统漏洞. 从而增加攻击者进行攻击所花费的时间和成本,使攻击难以实现拟态安全防御思想模拟了自然界中生物拟态行为的表现形式,构成了网络安全空间中组件元素变迁的实现方法.

移动目标防御(Moving Target Defense,MTD)也称动态目标防御技术,是近几年来由美国提出的网络空间"改变游戏规则"的重要技术之一. 移动目标防御技术实现通过不断的动态化和多样化安全系统的构建、部署机制和策略,实现系统受攻击面的动态转移即"移动要保护的对象",使攻击者在进行攻击时难以对特定的漏洞和攻击面进行攻击,增加攻击者进行攻击所需要的代价和时间. 现有的移动攻击面、变形网络等技术结合了移动目标防御的概念实现动态化的防御手段.

### 1.2 网络安全研究概述

在此背景下,网络安全主动防御系统得以产生及发展. 同时,其主要技术框架经过近几年的快速发展,虽然不断有新方法被提出,但是总体上可以归结到如下两种策略:

(1)在系统被攻入前,通过增加系统防护能力,进而增加被攻入的难度;

(2)在系统被攻入后,通过某种快速恢复策略,进而增加系统的防护能力.

网络安全主动防御系统的实现打破了原有的防火墙、入侵检测和病毒查杀三位一体的静态封堵防御体系架构,实现了一种新型的防御体系. 这样的动态防御体系在性能实现上远远超过了以往的网络安全体系,将安全空间中攻防双方的主被动关系扭转,使防御方占据主动,而攻击方则处于相对被动的地位.

国内外对于主动防御方面都进行了一些的研究,但是研究点往往只局限于主动防御两种策略的其中之一,而难以将两种策略有效安全的结合. 国内有学者提出通过结合可信计算技术来构建主动防御的免疫双体系结构,实现在安全机制、安全保障和安全策略上的三重主动防御[12]. 这样的防御体系可有效地校验系统各个部件的可信以实现结构化的可信保障,增加系统被攻入的难度,但是无法为系统赋予自修复性. 另有国内学者提出构建模糊静态贝叶斯博弈模型,并在此基础上引入三角模糊数来描述攻防双方的效用函数,以此为依据来实现系统的策略选取[13]. 这样的防御模型更加的主动,运用数学方法实现对于特定攻击策略的防御策略选择,可以有效地增加被攻入的难度,但同样无法增加系统被攻入后恢复正常状态的能力. 与之对应,国外学者曾提出根据动态水印技术,实现系统数据安全的动态监测和数据修复[14]. 这样的系统体系可实现有效的自修复性,但是对于攻击的入侵反应较为被动,重点在于对入侵的监测和系统修复,难以增加系统的防御能力.

因此通过构建一种有效可行的主动防御体系(同时实现主动防御的两种策略),可以全面提升网络空间中系统的安全性,并构筑一种完整的动态化异构自修复空间架构. 两种策略的有效结合也是构筑主动安全体系所必须的.

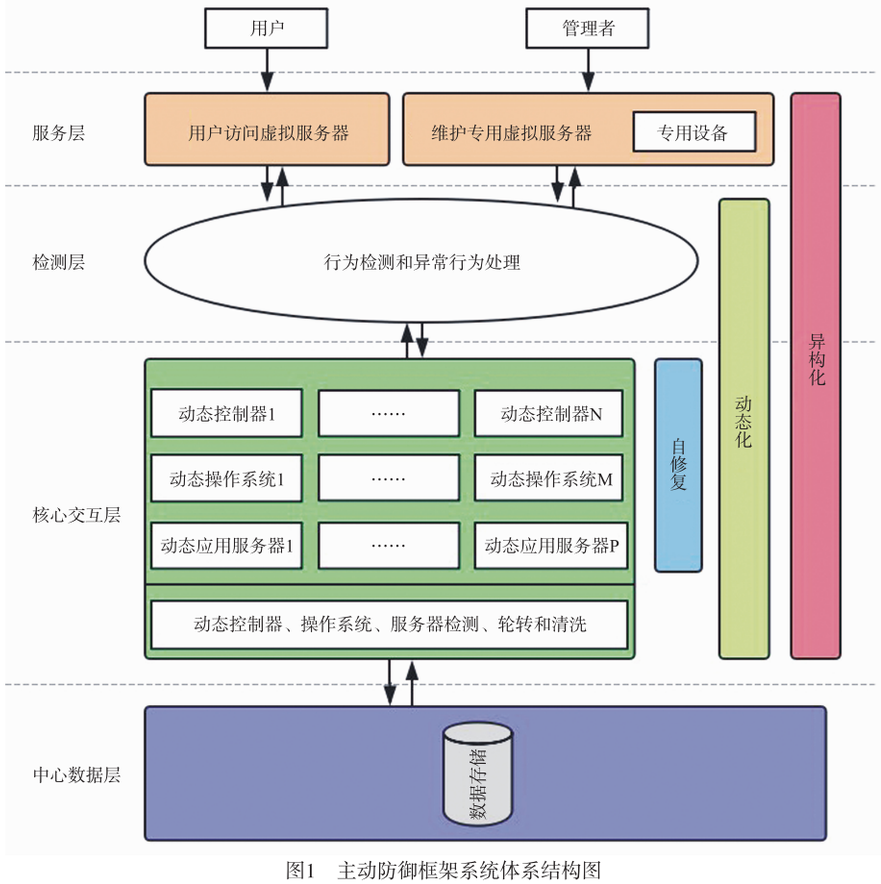


图1　主动防御框架系统体系结构图

### 1.3　网络安全框架概述

为了实现主动防御的有效可行框架,需要对主动防御系统的各个组件进行异构化和动态化的设计实现. 从操作系统,环境,服务器等多个方面进行异构冗余的部署,对每次系统服务的提供分配随机的操作系统,控制器和服务器,实现动态化的配置,使得攻击者难以对每次查找到的漏洞进行利用,增加攻击者进行攻击所需要的时间和代价,使系统难以被攻破. 同时采用轮换清洗技术,检查在用的部件状态是否正常,并定期更换在用的服务器,操作系统等部件,对不用的部件进行重置和清洗,对不正常的部件进行替换,实现系统的自修复能力.

这样的主动防御框架构建在异构的服务器、控制器等资源上,结合虚拟化和动态化思想,同时实现了主动防御的两种策略,可以有效增加系统的安全性,不易被攻破. 而由于系统所能异构的部件数量作为资源分配必然是有限可穷举的,则由动态化和虚拟化分配所产生的资源分配组合也必然是有限可穷举的. 这就说明主动防御可用策略实际上是有限可穷举的,而主动防御策略的有限性也就使得我们从数学上刻画主动防御系统的动态和结构性质的构想可能实现.

微分方程适用于解决实际中可以发现相互联系,但是难以建立数学函数的问题. 通过建立变量和导数关系,实际问题中各个方面的联系可通过微分方程求解获得未知变量的函数关系. 微分方程被用于许多生活领域,而其中在控制论上的应用更为广泛和突出,如通过对变分问题的研究以设计实现的最优控制器和线性控制系统的最优数学模型. 在其他方面,如在医学中是用微分方程构建放疗中放射性元素衰变周期的函数,在经济学中,微分方程被用来构建新产品推广的经济模型.

主动防御模型的构建基础是资源分配和策略选择,而网络安全问题上涉及到了攻防双方的资源和策略部署,这样的对抗模型难以单方面的获得整个攻防双方的函数关系,但是攻防双方的资源和策略部署有一定的联系,可以设置变量研究相互联系. 同时研究网

络安全主动防御系统也必定会获得系统达到安全与非安全状态之间的变换点和稳定态,即驻点问题,因而导数也会被引入到研究中.这样的研究思路使得该模型的研究与微分方程的问题求解非常的符合,因此可以假想,主动防御模型的研究可以通过微分方程的求解来实现.

网络信息系统和工业控制系统在安全主动防御系统结构上是相当类似的——网络安全主动防御系统也可以分成开环和闭环[15].开环主动防御系统使用固定的系统参数、资源和可选有限的防御策略,无法依据当前网络攻击形势动态调整防御策略;闭环主动防御系统可以依据当前网络攻击的实际情况动态调整系统资源、防御策略.开环系统技术简单、成本低廉,但只能应付有限的攻击形式,其数学模型也相对简单;闭环系统虽然复杂,但是面对网络攻击的适应性更强,其数学模型往往无法显式给出.通过借鉴工业[16],我们可以通过常微分动态系统来刻画网络安全主动防御系统的动态性质和结构性质,从而建立起为网络攻防的数学模型.

本文的贡献:(1)通过将一般的网络攻防问题转换为资源对抗问题,本文从资源的角度建立起整个主动防御研究框架;(2)本文引入微分方程来研究系统的稳定性(抵抗能力、恢复能力)和资源动态特性.本文主要从一般的主动防御框架出发,实现对一般的主动防御系统的资源动态特性的刻画.不针对特定的主动防御技术,如通信指纹跳变、安全态势感知、则多判断、异构化、冗余化、虚拟化等技术的刻画.

## 2 模型定义

对于现代的大型网络信息系统而言,往往通过云计算获得异构冗余的能力,例如对于淘宝而言,其在双11期间通过大量服务器的负载均衡来保持网站正常访问.基于docker等虚拟化服务的弹性托管通过docker实例的开启、关闭、数据迁移可以大大提高了服务的可持续性.一般的网络安全防御系统应该包含攻击防御和异常恢复两部分,我们假设在攻击防御部分存在服务器的异构冗余,在异常恢复阶段存在自动监控、自动修复机制.这样的假设对于基于云概念的网络服务而言是自然的.

使用微分方程方法对主动防御框架的内容来构建主动防御的模型,需要定义微分方程中的变量来进行求解.为对于模型中异构冗余内容的资源简化,可将动态异构的控制器,操作系统,服务器都看作服务器数量,对攻击者行为抽象为攻击策略,系统的主动防御行为抽象为防御策略.

假设服务器数量为 $N_{\text{server}}$,我们可以定义概率函数 $f:Z\times\alpha\times\beta\to[0,1]$,其中 $\alpha=\{\alpha_i\mid i\le n\}$ 是防御策略空间,$\beta=\{\beta_j\mid j\le n\}$ 是攻击策略空间,$Z$ 是服务器实例数量空间.则 $f(N_{\text{server}},\alpha_i,\beta_j)=f_{\alpha\beta_j}(N_{\text{server}})$ 定义了当主动防御系统采用防御策 $\alpha_i$ 应对攻击策略 $\beta_j$ 且当前系统服务器数量为 $N_{\text{server}}$ 时,系统被攻破的概率.

从安全防护的角度来说,服务器最重要的资源包括物理资源和数据资源两部分.物理资源主要可以分为计算资源和带宽资源,数据资源主要包括数据的一致性和保密性.在建立下面的框架时,我们主要从这些资源变化角度进行分析研究.由于虚拟化技术的技术特点,我们可以保持所有服务器实例的带宽资源和计算资源相同,那么物理资源只与服务器实例数量 $N_{\text{server}}$ 有关.同样地,服务器数据资源的一致性和保密性大小也可以用 $N_{\text{server}}$ 来刻画.因为如果某台服务器被攻陷,由于主动防御系统在此时无法获知网络攻击的真正类型,因此在理论上我们认为当前服务器的数据一致性和保密性已经被破坏,系统残余的数据一致性和保密性就可以使用当前服务器数量 $N_{\text{server}}$ 来刻画.所以,系统资源的变化可以使用 $r(N_{\text{server}})$ 来表示.

我们还需要定义一次成功攻击对系统产生的影响.对于破坏数据一致性的网络攻击来说,恢复机制通过对服务器数据的校验可以很容易地发现被破坏的服务器的数量;对于大量占用服务器计算资源的网络攻击而言,恢复机制通过进行数次的数据统计并和其他服务器的资源使用进行对比,就可以发现出现问题的服务器等等;总之,在实际的主动防御系统中总会存在相关的机制用于检测和恢复.我们将整个后台恢复机制抽象成一个黑盒,且只需要对黑盒的功能进行定义而不考虑其实现细节.

对于具有恢复能力的黑盒而言,其恢复的单元至少是一个(虚拟机或docker)实例,也就是功能意义上的一台服务器.所以,对于一次成功的攻击而言,无论其对实例的实际攻击效果如何,我们都认为该实例已经无法再正常工作.因此,攻击对系统产生的影响 $E$ 可以通过单位攻击需要恢复的服务器资源数量来定义.假设攻击者单位时间发起的攻击数目为 $Atk$,主动防御系统单位时间可以恢复的资源的比例为 $v$.

## 3 框架描述

### 3.1 安全区域

对于主动防御框架的研究,我们将从资源变化的角度进行研究.我们重点考察系统资源的变化.系统单位时间减少的资源为 $f_{\alpha,\beta_j}(N_{\text{server}})*Atk*E$,表示主动防御系统采用策略 $\alpha_i$ 应对 $\beta_i$ 攻击策略时单位时间会被攻破的资源的期望值;系统单位时间需要恢复的资源的期望值为 $v(N_0-N_{\text{server}})$,其中 $N_0$ 是初始服务器实例数目.所以有如下期望动态方程成立:

$$\frac{\mathrm{d}r(N_{\mathrm{server}})}{\mathrm{d}t}=-f_{\alpha_i\beta_j}(N_{\mathrm{server}})*Atk*E+v*(N_0-N_{\mathrm{server}}) \tag{1}$$

(1)在驻点处达到局部稳定,即

$$f_{\alpha_i\beta_j}(N_{\mathrm{server}})*Atk*E=v*(N_0-N_{\mathrm{server}}) \tag{2}$$

当系统达到局部稳态的时候,是主动防御系统以最少的资源达到最好的防御效果的时候,记此时的服务器实例数为 $N_{\mathrm{stasis}}$. 如果这时候攻击强度 $Atk$ 已经达到了最高值,那么系统在随后会逐渐恢复至初始状态(在中间过程中会达到若干次局部稳态);如果攻击强度 $Atk$ 持续增强,那么 $N_{\mathrm{stasis}}$ 会不断减小,并且当 $N_{\mathrm{stasis}}$ 小于某个极限值时,系统会出现雪崩式的崩坏,如图 2 所示.

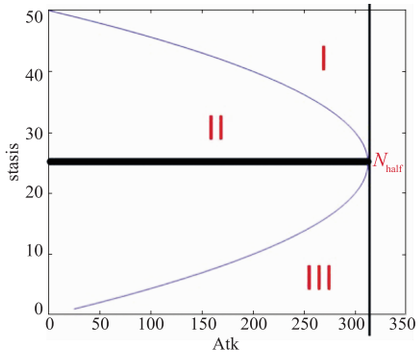


图2　$f_{\alpha_i\beta_j}(N_{\mathrm{server}})=N_{\mathrm{server}}^{-1}$,$E$=1,$v$=0.5

当 $N_{\mathrm{stasis}}>N_{\mathrm{half}}$,即在蓝色曲线的上半部分,我们发现,要使 $N_{\mathrm{stasis}}$ 下降,$Atk$ 必须不断增大,如果此时 $Atk$ 下降,那么系统会很快恢复到初始状态;但是当 $N_{\mathrm{stasis}}<N_{\mathrm{half}}$ 时,可以看到,达到稳态的攻击强度 $Atk$ 也在不断下降,也就是此时即便实际攻击强度 $Atk$ 在衰减,系统资源也可能持续衰减,直至被完全破坏. 在不考虑资源利用效率的情况下,从图 2 中可以知道,如果能始终保持 $N_{\mathrm{stasis}}>N_{\mathrm{half}}$,那么该主动防御系统是安全的,经过一段时间,系统稳定在图中 Ⅰ 区域. 我们称 Ⅰ 区域为安全区域,因为当($Atk$,$N_{\mathrm{server}}$)处于 Ⅰ 区域时,系统不会被完全攻破;Ⅱ 区域为不安全区域,系统面临被瘫痪的风险.

在主动防御模型中的检测系统会对系统的安全区域进行检测,对系统的安全状态进行评估,如果系统处于可能被攻破的不安全区域内,则对系统的资源分配进行调整,使系统再次回到安全区域内.

### 3.2　资源变化

上面的讨论都是针对特定的 $f_{\alpha_i\beta_j}(N_{\mathrm{server}})$ 而言的,下面的定理给出了一般情况下的理论.

我们称一个防御策略 $\alpha_i$ 针对攻击策略 $\beta_j$ 是有效的,则 $\frac{f_{\alpha_i\beta_j}(N_{\mathrm{server}})}{\mathrm{d}N_{\mathrm{server}}}<0$.

我们可以定义 Kronecker 系数 $\delta_i^j$,如果 $\alpha_i$ 针对 $\beta_j$ 是有效的,那么 $\delta_i^j=1$,否则 $\delta_i^j=0$. 特别地,我们假设 $\forall i$,$\exists\delta_i^j=1$,即对于任何攻击策略总是存在有效地防御策略.

**定理 1**　对于固定 $\alpha_i$ 和 $\beta_j$,如果 $\delta_i^j=1$,那么当 $N_0$ 足够大时,一定存在 $N_{\mathrm{bound}}$,$Atk_{\mathrm{bound}}$ 满足 *Eq.* (2),当攻击强度 $Atk$ 的峰值 $Atk_{\max}\le Atk_{\mathrm{bound}}$ 时,$N_{\mathrm{server}}\ge N_{\mathrm{bound}}>0$ 总是成立.

**证明**

由 *Eq.* (2*B*) 得 $Atk=\frac{v*(N_0-N_{\mathrm{server}})}{f_{\alpha_i\beta_j}*E}$,则 $\frac{\mathrm{d}Atk}{\mathrm{d}N_{\mathrm{server}}}=\frac{-v*f_{\alpha_i\beta_j}-v*(N_0-N_{\mathrm{server}})*f'_{\alpha_i\beta_j}}{f^2_{\alpha_i\beta_j}*E}$

当 $N_{\mathrm{server}}=N_0$ 时,$\frac{\mathrm{d}Atk}{\mathrm{d}N_{\mathrm{server}}}\Big|_{N_0}=\frac{-v*f_{\alpha_i\beta_j}}{f^2_{\alpha_i\beta_j}*E}<0$;

令 $N_0>\frac{f_{\alpha_i\beta_j}(0)}{-f'_{\alpha_i\beta_j}(0)}$,则

当 $N_{\mathrm{server}}=0$ 时,

$$\frac{\mathrm{d}Atk}{\mathrm{d}N_{\mathrm{server}}}\Big|_0=\frac{-v*f_{\alpha_i\beta_j}-v*N_0*f'_{\alpha_i\beta_j}}{f^2_{\alpha_i\beta_j}*E}=\frac{-vf'_{\alpha_i\beta_j}*\left(N_0-\frac{f_{\alpha_i\beta_j}}{-f'_{\alpha_i\beta_j}}\right)}{f^2_{\alpha_i\beta_j}*E}>0$$

则由介值定理可知,一定存在 $N_1$,使得 $-v*f_{\alpha_i\beta_j}(N_1)-v*(N_0-N_1)*f'_{\alpha_i\beta_j}(N_1)=0$,即

$$f_{\alpha_i\beta_j}(N_1)+(N_0-N_1)*f'_{\alpha_i\beta_j}(N_1)=0 \tag{3}$$

从而 $\frac{\mathrm{d}Atk}{\mathrm{d}N_{\mathrm{server}}}\Big|_{N_1}=0$. 不妨设 $N_1$ 是离 $N_0$ 最近的零点,那么当 $N_{\mathrm{server}}>N_1$ 时,$\frac{\mathrm{d}Atk}{\mathrm{d}N_{\mathrm{server}}}<0$,$Atk$ 随着 $N_{\mathrm{server}}$ 的减小不断增大.

下面证明 $N_1$,$Atk_1=\frac{v*(N_0-N_1)}{f_{\alpha_i\beta_j}(N_1)*E}=\frac{v*(N_0-N_1)}{f'_{\alpha_i\beta_j}(N_1)*(N_0-N_1)*E}=\frac{-v}{f'_{\alpha_i\beta_j}(N_1)*E}$ 即为所求的 $N_{\mathrm{bound}}$,$Atk_{\mathrm{bound}}$. 假设该主动防御系统是平稳的,网络攻击具有很小的惯性,那么我们从局部稳态 $N_{\mathrm{server}}=N_1$ 时出发考虑. 如果总是有 $Atk<Atk_1$,那么就有 $f_{\alpha_i\beta_j}(N_1)*Atk*E<v*(N_0-N_1)$,即恢复速度大于破坏速度,那么 $r(N_{\mathrm{server}})$,$N_{\mathrm{server}}$ 在极短时间内会增加,但是 $N_{\mathrm{server}}$ 增加会导致恢复速度减慢,所以该常微分系统最终会 $N_{\mathrm{server}}=N_2>N_1$ 处重新达到平衡. 同样地,我们可以证明对于任何 $N_{\mathrm{server}}>N_1$ 均可以作为 $N_{\mathrm{bound}}$. 我们称 $N_{\mathrm{bound}}$ 为安全分割点,简称分割点.

**定理 2**　如果 $\int_1^{\infty}|N^{-2}f_{\alpha_i\beta_j}(N)|^p\mathrm{d}N<\infty$,$p\in([1,\infty]$,

且$f''_{\alpha_i\beta_j}(N)>0$,则$\forall\varepsilon>0$,存在关于$\frac{1}{N}$的多项式$P_n\left(\frac{1}{N}\right)$使得

$$\sum_{N=1}^{\infty}N^{-2}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p<\varepsilon$$

**证明** 由于$\int_1^{\infty}\left|N^{-2}f_{\alpha_i\beta_j}(N)\right|^p\mathrm{d}N<\infty$作变量替换$x=\frac{1}{N}$,则有$\int_0^1\left|f_{\alpha_i\beta_j}\left(\frac{1}{x}\right)\right|^p\mathrm{d}x<\infty$,所以$f_{\alpha_i\beta_j}\left(\frac{1}{x}\right)\in L^p[0,1]$,由$L^p[0,1]$空间的可分性及多项式函数在$L^p[0,1]$空间中稠密可知,$\forall\varepsilon>0$,存在多项式函数$P_n(x)$,使得$\int_0^1\left|f_{\alpha_i\beta_j}\left(\frac{1}{x}\right)-P_n(x)\right|^p\mathrm{d}x<\varepsilon$,则

$$\begin{aligned}&\sum_{N=1}^{\infty}N^{-2}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p\\&<\int_1^{\infty}N^{-2}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p\mathrm{d}N\\&=\int_0^1\left|f_{\alpha_i\beta_j}\left(\frac{1}{x}\right)-P_n(x)\right|^p\mathrm{d}x<\varepsilon\end{aligned}$$

**推论1** 如果$N_0$存在上界$N_{0up}$,$f_{\alpha_i\beta_j}(N_{\mathrm{server}})$满足定理2中条件,则$\forall\varepsilon_1>0$,存在关于$\frac{1}{N}$的多项式$P_n\left(\frac{1}{N}\right)$使得

$$\sum_{N=1}^{N_{0up}}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p<\varepsilon$$

**证明** 在定理2的证明中令$\varepsilon=\frac{\varepsilon_1}{N_{0up}^2}$,则

$$\begin{aligned}&\sum_{N=1}^{N_{0up}}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p\\&<N_{0up}^2\sum_{N=1}^{\infty}N^{-2}\left|f_{\alpha_i\beta_j}(N)-P_n\left(\frac{1}{N}\right)\right|^p\\&<N_{0up}^2\varepsilon=\varepsilon_1\end{aligned}$$

推论1是一个很强的结论,它告诉我们对于任何实际的主动防御系统,$f_{\alpha_i\beta_j}(N_{\mathrm{server}})$都能够用多项式函数$P_n\left(\frac{1}{N_{\mathrm{server}}}\right)$来逼近. 所以,对于对抗函数$f_{\alpha_i\beta_j}(N_{\mathrm{server}})$的研究可以聚焦在多项式形式上,一般地记为$P^n_{\alpha_i\beta_j}\left(\frac{1}{N_{\mathrm{server}}}\right)$.

我们现在考察$N_0$变化对$N_1$的影响. 下面我们引入一个$K$阶相关的概念,即如果$\lambda_1N_0^K\geq N_1\geq\lambda_2N_0^K$总是成立,其中$\lambda_1,\lambda_2>0$为常量,则称$N_1$对$N_0$是$K$阶相关的,简称$K-$相关,记为$K=lor_{\Delta N_0}\Delta N_1$.

**命题1** 如果$lor_{\Delta N_0}\Delta N_1=1$,则有如下结论成立:

(1)$lor_{\Delta N_0}\Delta N_1=1$.

(2)$\lambda_1\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}\geq\frac{f'_{\alpha_i\beta_j}(N_1)}{f''_{\alpha_i\beta_j}(N_1)}\geq\lambda_2\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}$总是成立. 特别地,如果$\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}=\lambda\frac{f'_{\alpha_i\beta_j}(N_1)}{f''_{\alpha_i\beta_j}(N_1)}$,则可得通解$f_{\alpha_i\beta_j}(N)=C\left(\frac{1}{N}\right)^{\frac{\lambda}{1-\lambda}}$.

(3) 存在$C>0$使得$C\left(\frac{1}{N}\right)^{\frac{\lambda_1}{1-\lambda_1}}\leq f_{\alpha_i\beta_j}(N)\leq C\left(\frac{1}{N}\right)^{\frac{\lambda_2}{1-\lambda_2}}$.

**证明** 注意到当$N_0=0$时,$N_1=0$,则对$\lambda_1\mathrm{d}N_0\geq\mathrm{d}N_1\geq\lambda_2\mathrm{d}N_0$两边积分,可得$\lambda_1N_0\geq N_1\geq\lambda_2N_0$即$lor_{N_0}N_1=1$.

对于命题第二部分,由$N_0=N_1-\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}$,两边求导可知$\mathrm{d}N_0=\mathrm{d}N_1-\frac{f_{\alpha_i\beta_j}(N_1)*f''_{\alpha_i\beta_j}(N_1)}{(f'_{\alpha_i\beta_j}(N_1))^2}$,即得$\lambda_1\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}\geq\frac{f'_{\alpha_i\beta_j}(N_1)}{f''_{\alpha_i\beta_j}(N_1)}\geq\lambda_2\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}$,对于非线性微分方程$\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}=\lambda\frac{f'_{\alpha_i\beta_j}(N_1)}{f''_{\alpha_i\beta_j}(N_1)}$,令$f'=u(N)*f$,可得$u'=\frac{\lambda-1}{\lambda}u^2$,其为伯努利方程,可得$u=\frac{\lambda}{1-\lambda}\frac{1}{C_1-N}$. 由$f=C_2e^{\int u\mathrm{d}N}$,即可得$f_{\alpha_i\beta_j}(N)=C_2\left(\frac{1}{|C_1-N|}\right)^{\frac{\lambda}{1-\lambda}}$,因为$N_0=N_1-\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}$,且$N_0=0$应该有$N_1=0$,所以$C_1=0$,即$f_{\alpha_i\beta_j}(N)=C\left(\frac{1}{N}\right)^{\frac{\lambda}{1-\lambda}}$此时可计算得$N_1=\lambda N_0$.

对于命题第三部分,由于$lor_{N_0}N_1=1$,所以$\frac{1}{\lambda_1}N_1\leq N_0=N_1-\frac{f_{\alpha_i\beta_j}(N_1)}{f'_{\alpha_i\beta_j}(N_1)}\leq\frac{1}{\lambda_2}N_1$可知$\frac{\lambda_2}{1-\lambda_2}\frac{1}{N_1}\leq-\frac{f'_{\alpha_i\beta_j}(N_1)}{f_{\alpha_i\beta_j}(N_1)}\leq\frac{\lambda_1}{1-\lambda_1}\frac{1}{N_1}$,即$\frac{\lambda_2}{1-\lambda_2}\frac{1}{N_1}\mathrm{d}N_1\leq-\mathrm{d}\ln f_{\alpha\beta_j}(N_1)\leq\frac{\lambda_1}{1-\lambda_1}\frac{1}{N_1}\mathrm{d}N_1$

两边在区间$[1,N_1]$上积分,即得

$$\frac{\lambda_2}{1-\lambda_2}\ln N_1-\ln f_{\alpha_i\beta_j}(1)\leq-\ln f_{\alpha_i\beta_j}(N_1)\leq\frac{\lambda_1}{1-\lambda_1}\ln N_1-\ln f_{\alpha_i\beta_j}\tag{4}$$

也就是$C\left(\frac{1}{N}\right)^{\frac{\lambda_1}{1-\lambda_1}}\leq f_{\alpha_i\beta_j}(N)\leq C\left(\frac{1}{N}\right)^{\frac{\lambda_2}{1-\lambda_2}}$,其中$C=e^{\ln f_{\alpha_i\beta_j}(1)}=f_{\alpha_i\beta_j}(1)>0$.

主动防御模型中资源变化的控制体现在实际工程中对于异构的部件,如控制器,操作系统和服务器等部件的部署上. 通过对异构冗余部件的数量部署改变,和动态化的分配在用与不用的部件数量,可以实现对于$N_{\mathrm{server}}$的改变,从而改变系统的安全情况.

### 3.3 策略变化

下面开始考察$N_0$对$Atk_1$的影响. 在下面的处理

中,我们需要扩充 $K$ 阶相关的概念. 我们称 $K^- = lor_x^- y$ 为 $y(x)$ 对 $x$ 的左相关阶数,如果 $K^-$ 是最大的实数,使得存在 $\lambda > 0$ 满足 $\lambda x^{K^-} \leq y$;我们称 $K^+ = lor_x^+ y$ 为 $y$ 对 $x$ 的右相关阶数,如果 $K^+$ 是最小的实数,使得存在 $\lambda > 0$ 满足 $y \leq \lambda x^{K^+}$.

**定理 3**　$lor_x y = K$ 充分必要条件是 $K^+ = K = K^-$.

**证明**　充分性:由 $K^-$ 和 $K^+$ 的定义可知,存在 $\lambda_1$, $\lambda_2 > 0$,使得 $\lambda_1 x^{K^-} = \lambda_1 x^K \leq y \leq \lambda_2 x^{K^+} = \lambda_2 x^K$,所以 $lor_x y = K$.

必要性:由于 $lor_x y = K$,所以存在 $\lambda_1, \lambda_2 > 0$,使得 $\lambda_1 x^K \leq y \leq \lambda_2 x^K$,所以 $K^+ \leq K \leq K^-$. 下证 $K^- \leq K^+$.

如果 $K^+ < K^-$,那么 $\lim\limits_{x \to +\infty} x^{K^- - K^+} = +\infty$;因为存在 $C_1$, $C_2 > 0$ 使得 $C_1 x^{K^-} \leq y \leq C_2 x^{K^+}$,所以 $C_1 x^{K^-} \leq C_2 x^{K^+} \Rightarrow x^{K^- - K^+} \leq \frac{C_2}{C_1}$,矛盾. 所以 $K^- < K^+ \Rightarrow K^- = K^+ = K$.

**命题 2**　设 $lor_{N_0} N_1 = 1$,设 $\lambda_1 = \sup \frac{N_1}{N_0}$, $\lambda_2 = \inf \frac{N_1}{N_0}$,则有如下结论成立:

(1) $lor_{N_0}^- Atk_1 \geq \frac{1}{1-\lambda_2}$

(2) $lor_{N_0}^+ Atk_1 \leq \frac{1}{1-\lambda_1}$

**证明**　由 $Atk_1 = \frac{v(N_0 - N_1)}{f_{\alpha_i \beta_j}(N_1) * E}$ 及命题 1(3),

$$Atk_1 \geq \frac{v}{CE}(N_0 - N_1) N_1^{\frac{\lambda_2}{1-\lambda_2}} \geq \frac{v}{CE}\left(N_0 - \frac{1}{\lambda_1}N_0\right)\left(\frac{1}{\lambda_2}N_0\right)^{\frac{\lambda_2}{1-\lambda_2}} \geq \frac{v}{CE}\frac{1-\lambda_1}{\lambda_1}\lambda_2^{\frac{1}{1-\lambda_2}} N_0^{\frac{1}{1-\lambda_2}}$$

所以,$lor_{N_0}^- Atk_1 \geq \frac{1}{1-\lambda_2}$. 同理,$Atk_1 \leq \frac{v}{CE}(N_0 - N_1) N_1^{\frac{\lambda_1}{1-\lambda_1}} \geq \frac{v}{CE}\left(N_0 - \frac{1}{\lambda_2}N_0\right)\left(\frac{1}{\lambda_1}N_0\right)^{\frac{\lambda_1}{1-\lambda_1}} \geq \frac{v}{CE}\frac{1-\lambda_2}{\lambda_2}\lambda_2^{\frac{1}{1-\lambda_1}} N_0^{\frac{1}{1-\lambda_1}}$

所以 $lor_{N_0}^+ Atk_1 \leq \frac{1}{1-\lambda_1}$.

下面我们正式考察对抗函数 $f_{\alpha_i \beta_j}(N) = N^{-K}$, $K > 0$ 对系统性能的影响,由推论 1 的结论,我们主要考虑多项式形式的对抗函数. 下面的讨论,我们仍然假设 $lor_{N_0} N_1 = 1$. 由命题 1(3)可知 $C\left(\frac{1}{N}\right)^{\frac{\lambda_1}{1-\lambda_1}} \leq f_{\alpha_i \beta_j}(N) \leq C\left(\frac{1}{N}\right)^{\frac{\lambda_2}{1-\lambda_2}}$,所以我们下面重点研究形如 $CN^{-K}$ 的多项式对抗函数.

**命题 3**　设 $f_{\alpha_i \beta_j}(N) = N^{-K}$, $K > 0$,那么有如下结论成立:

(1) $N_1$ 随着 $K$ 的增大而增大;

(2) $Atk_1$ 随着 $K$ 的增大而增大.

**证明**　由 $N_0 = N_1 - \frac{f_{\alpha_i \beta_j}(N_1)}{f'_{\alpha_i \beta_j}(N_1)}$,可得 $N_1 = \frac{K}{K+1} N_0$,可见(1)成立.

由 $Atk_1 = \frac{v(N_0 - N_1)}{f_{\alpha_i \beta_j}(N_1) * E}$ 求解的 $Atk_1 = \frac{v}{CE}\frac{K^K N_0^{K+1}}{(K+1)^{K+1}}$,令 $y = \ln(Atk_1)$,则 $y = \ln \frac{v}{CE} + K\ln K - (K-1)\ln(K+1) + (K+1)\ln(N_0)$,故 $y' = \ln \frac{K}{K+1} N_0$,我们注意到 $\frac{K}{K+1} N_0 = N_1 \geq 1$,所以 $y' \geq 0$. 所以 $y$ 随着 $K$ 的增大而单调递增,即得(2)成立.

很显然,如果我们选取的对抗函数使得 $N_1$ 越小,那么服务器资源就可以得到充分的利用;反之,如果 $f_{\alpha_i \beta_j}(N_{\text{server}})$ 使得 $Atk_1$ 越大,那么服务质量(安全系数)也就越能够得到保证. 但是 Proposition3. 3 告诉我们资源利用和服务质量是无法通过设计系统同时增强的,在实际工程实践的时候必须按照实际情况做出取舍.

在实际的系统设计中,形如 $f_{\alpha_i \beta_j}(N) = N^{-K}$ 的策略函数是可实现的,例如,采用 $N$ - 异构服务器,那么对于攻击链长为 $K$ 的网络攻击的成功率即为 $N^{-K}$.

以此可以引入 mulplicative 算法,如算法 1.

**算法 1　The general resource battle algorithm**

```
Require: N0: initial server instances; N_bound: a security
boundary number for server instances; γ: increase rate;
Ensure: N_server > N_bound
   compute N0', Atkbound from Eq. (3) with N1 = N_bound
   if N0 < N0' then
      adjust N0 = γ * N0'
   end if
repeat
if N_server < N_bound then
   adjust N0 = γ * N0
else if N0 > γ * N' and Atk < Atkbound then
      adjust N0 = N0/γ
end if
end repeat
```

主动防御模型的策略选取在实际工程中体现为对于可用异构冗余部件的部署分配方法. 系统可能检测到提供服务过程中异常的行为和部件状态,针对这些异常状态和行为,系统会进行对应的动态化部署,采取轮转清洗或是调整在用控制器,服务器等部件的数量,实现对应的防御部署,即相应的策略选取.

## 4　结论和未来工作

在上一节中对主动安全模型的描述大致可以分成

三部分:(1) 给出系统的安全区域;(2) 给出系统资源变化对安全区域的影响;(3) 给出系统策略变化对安全区域的影响. 这三部分内容给出了一个完整的算法框架——算法通过测量当前系统的状态决定当前系统是否即将离开安全区域;如果是,则通过改变系统资源或者策略选取来改变安全区域,使得当前系统状态仍然落在安全区域的范围之内.

这样的主动防御模型,结合了异构化、动态化和自修复的特性,可以主动的对自身安全状态进行检测. 系统可运用于提供服务的网站部署中,如一些关键部门的门户网站,设置异构服务器提供服务信息,同时检查自身的服务器状态,对异常状态的服务器进行替换和清洗. 由于服务器异构冗余,个别异常服务器的替换并不会影响服务的提供,保证了系统的稳定性. 同时,清洗后的服务器可再次投入使用,随机化和动态化的服务器分配策略选取和资源变化,保证了系统难以被攻破,增加了安全性.

本篇文章的核心概念就是安全区域,通过数学化处理,使得我们可以准确判断出当前系统的安全状态,定理 1 给出了系统安全的理论保证.

模型接着给出了当系统即将离开安全区域时的资源变换应对方法. 在讨论改变系统总资源 $N_0$ 对系统安全区域的影响时,我们引入了 $K$ 阶相关的概念,并且内容主体上围绕 1 阶相关进行. 1 阶相关本质上是一种倍数关系,保证了 $N$ 和分割点 $N$ 的这种倍数关系,就可以引入 mulplicative 算法,如算法 1. 命题 1 从 $\frac{\mathrm{d}N_1}{\mathrm{d}N_0}$ 入手给出了 $lor_{N_0}N_1=1$,实际上,单独通过 $lor_{\Delta N_0}\Delta N_1$ 也可以设计资源变换算法,此时就是从增量(incentive)的角度出发了. 命题 2 给出了分割点所对应的攻击峰值 $Atk_1$ 对 $N_0$ 的阶数,通过计算可以大致给出 $Atk_1$ 随 $N_0$ 的变化情况,例如当 $N_0=2N_1$ 时,$Atk_1=\frac{v}{4E}N_0^2$ 可见当 $N_0$ 增大 1 倍,$Atk_1$ 将增大 3 倍.

模型最后讨论了对抗函数的选取系统安全区域的影响. 定理 2 和推论 1 给出了研究对抗函数的思路,将研究目标聚焦在了简单的多项式函数. 在 $N_1$ 和 $N_0$ 一阶相关的前提下,我们研究了具有实际工程背景的一类对抗函数 $CN^{-K}$,这类对抗函数可以通过异构冗余实现,同时也具有典型研究意义. 命题 3 不仅给出对抗函数变化时安全区域变化的具体数学关系,并且给出了实际系统设计中的资源利用和性能保障这两大问题在当前模型下的描述. 对抗函数的设计对于系统架构的设计是具有指导意义的.

在基于动态模型的主动防御研究框架当中,还存在一系列的工作待完成. 例如本文的模型中,在主动变换上假设 $N_1$ 和 $N_0$ 是 1 阶相关的,但是对于许多其他的对抗函数而言,1 阶相关的假设也许并不成立,那时我们可以研究 2 阶相关甚至更高阶相关情形下的系统理论. 在对对抗函数的讨论中,尽管我们已经对形如 $CN^K$ 的对抗函数有了全面的研究,但是我们仍然没有排除存在这样的对抗函数,使得资源利用和服务质量均能到达最佳,这一部分的结论依赖于变分分析,将体现在我们下一步的工作当中. 另外一个和实践结合的相对紧密的问题就是如何依据对抗函数构造主动防御系统,对于形如 $CN^K$ 的对抗函数我们已经给出了构造方法,但是更进一步的结果仍待研究. 我们当前提出的研究框架主要是从宏观上考虑整个攻防,在具体策略分解、设计方面尚不能给出明晰的理论指导,这正是我们下一步的研究方向.

## 参考文献


[1] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报,2016,1(4):1 - 10.
Wu Jiangxing. Research on cyber mimic defense[J]. Journal of Cyber Security,2016,1(4):1 - 10. in Chinese

[2] Bharat B Madana,et al. A method for modeling and quantifying the securityattributes of intrusion tolerant systems [J]. Performance Evaluation,2004(56):167 - 186.

[3] Sushil J, Anup K G, Vipin S, et al. Moving Target Defense—Creating Asymmetric Uncertainty for Cyber Threats [M]. [s. l. ]:Springer Press,2011.

[4] Han Y, Lu W, Xu S. Characterizing the power of moving target defense via cyber epidemic dynamics[A]. Symposium and Bootcamp on the Science of Security [C]. ACM,2014.

[5] Garcia M, Gashi I, Obelheiro N N A. Analysis of operating system diversity for intrusion tolerance [J]. Software—Practice & Experience,2014,44(6):735 - 770.

[6] Sushil J, Anup K G, Vipin S, et al. Moving Target Defense II:Application of Game Theory and Adversarial Modeling [M]. [s. l. ]:Springer Press,2013.

[7] 温涛,张玉清,刘奇旭,等. UVDA:自动化融合异构安全漏洞库框架的设计与实现[J]. 通信学报,2015,36(10):235 - 244.
Wen Tao, Zhang Yu-qing, Liu Qi-xu, et al. UVDA: Design and implementation of automation fusion framework of heterogeneous security vulnerability database[J]. Journal on Communications,2015,36(10):235 - 244. (in Chinese)

[8] 郑勇. 基于演化计算的模拟电路冗余容错方法研究[D]. 中国科学技术大学,2015.

[9] Hermann Kopetz, Paulo Veríssimo. Real time and dependability concepts[A]. Distributed Systems (2nd Ed. ). Sape Mullender (Ed. )[C]. New York, NY, USA: ACM Press/

Addison-Wesley Publishing Co,1993. 411 – 446.
[10] Shackleford D. Virtualization Security:Protecting Virtualized Environments[M]. SYBEX Inc. 2012. 96 – 98.
[11] Bangalore A K, Sood A K. Securing web servers using self-cleansing intrusion tolerance (scit)[A]. Second International Conference on Dependability(DEPEND'09)[C]. IEEE,2009. 60 – 65.
[12] 张大伟,沈昌祥,刘吉强,等. 基于主动防御的网络安全基础设施可信技术保障体系[J]. 中国工程科学,2016,18(6):58 – 61.
[13] 陈永强,吴晓平,付钰,等. 基于模糊静态贝叶斯博弈的网络主动防御策略选取[J]. 计算机应用研究,2015,32(3):887 – 889.
Chen Yong-qiang, Wu Xiao-ping, Fu Yu, et al. Active defense strategy a selection of network based on fuzzy static bayesian game model[J]. Application Reseach of Computers,2015,32(3):887 – 889.
[14] Satchidanandan B, Kumar P R. Dynamic watermarking: Active defense of networked cyber – physical systems[J]. Proceedings of the IEEE,2017,105(2):219 – 240.
[15] 董超. 网络安全2.0的发展思路和理念探索——基于网络安全监测预警服务体系的研究与开发[J]. 信息安全与通信保密,2015(9):67 – 67.
Dong Chao. Exploration of roads and ideas for the development of network scurity 2.0:Research and development based on network security monitoring and early warning service system[J]. China Information Security,2015(9):67 – 67. (in Chinese)
[16] Marvin Rausand. Reliability of Safety-Critical Systems: Theory and Applications[M]. Wiley,2014. 120 – 128.

## 作者简介

**陈双喜**　男,1980 年生于安徽安庆. 浙江大学博士研究生. 研究方向为网络空间安全、新型主动防御.
E-mail:rebel2004@qq.com

**吴安邦**　男,1995 年生于江西上饶. 浙江大学硕士研究生,研究方向为新型主动防御.
E-mail:610803328@qq.com

**岐舒骏**　男,1996 年生于浙江杭州. 浙江大学本科生,研究方向为新型主动防御.
E-mail:iqicheng@163.com