网络空间安全拟态防御技术概述

李政[1] 白利芳[2] 唐刚[2] 朱信铭[2]
(1.联通系统集成有限公司,北京 100071;2.中国软件评测中心,北京 100048)

摘 要:本文扼要分析了网络空间安全攻防不对称的现状,概要阐述了拟态防御技术的发展历程,重点论述了主动防御的基础原理及其抗攻击性,最后就主动防御的测试评估和应用实践情况进行了介绍,并对其优势与挑战进行了分析。

关键词:网络安全;主动防御;拟态防御;动态异构冗余
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1671-2064(2018)20-0037-03

1 网络空间安全现状

作为“陆、海、空、天”后的第五空间,网络空间正处于“有毒带菌”,且“易攻难守”的不对称格局。一方面,网络空间自身在顶层架构设计,生产、供应和服务链等各环节均存在“已知”、“已知的未知”或“未知的未知”安全风险。“已知”风险不存在技术上的难度,但由于安全意识和管理不足往往导致应对策略落实不到位;“已知的未知”风险虽被识别,但不确定其发生概率和影响;而“未知的未知”风险(如0day),因无法知晓攻击相关任何信息,针对性防御无从谈起。此外,即便采取了应对策略或应急措施,仍可能存在次生风险和残留风险,即任何国家或组织都无法从根本上消除其网络设施和信息系统的安全隐患。

另一方面,现有防御体系存在基因缺陷。大多以检测、阻断为主,且基于攻击相关信息等先验知识,架构透明、处理空间单一,本质上是被动、静态的。攻击者用极小的成本即可让网络空间面临巨大的威胁,在易攻难守的不对称态势下,主动防御逐步成为研究焦点,优势渐显。主动防御即在攻击的具体方法和步骤被知悉前实现防御部署,有效弥补被动防御的缺陷。目前,典型的主动防御技术有入侵容忍[1,4,5]、移动目标[2,3]、拟态防御等,其中拟态防御[6,7]是我国自主研创的新兴主动防御技术,其理论技术和应用实践均通过权威的测试和评估,有望成为网络安全“再平衡战略”的有力抓手。

2 拟态防御发展历程

2007年,中国工程院院士邬江兴首次将拟态计算概念引入域名防御系统。2013年,首台拟态计算机原理样机研制成功,并提出网络空间拟态防御理论。2016年,“Web服务器拟态防御原理验证系统”和“路由器拟态防御原理验证系统”研制成功,并通过科技部委托组织的网络通信和安全领域的权威测评验证。2017年10月,工信部正式批复《关于开展拟态防御技术试点工作的通知》,确定河南联通与拟态团队开展拟态域名服务防御系统试点工作。2018年1月,全球首套拟态域名服务器在中国联通河南分公司上线,首次在运营商现网环境进行试点应用和量化评估。4月,全球首套拟态防御网络设备在郑州投入互联网线上服务,拟态防御在应用实践和产业化进程中迈出了里程碑式的一步。

3 拟态防御理论

3.1 拟态防御原理

拟态防御的灵感源于自然界基于内生机理的“拟态伪装”,在本征功能不变的条件下,能以不确定色彩、纹理和形状等变化给捕猎者或捕猎目标造成认知错觉。同理,在不影响服务功能和性能正常提供的条件下,类似于系统架构、运行机制、异常响应以及未知脆弱点等,均可通过类似

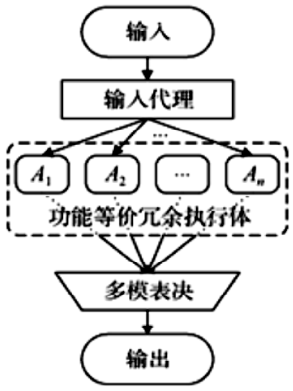

图1 异构冗余架构[7]

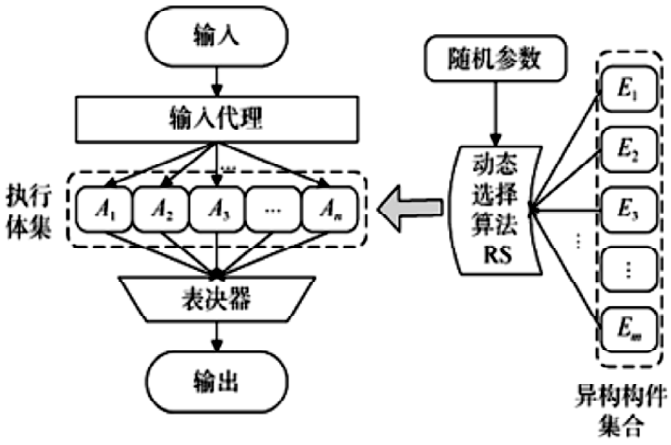

图2 DHR架构[7]

收稿日期:2018-07-09

作者简介:李政(1980—),男,北京人,硕士,高级工程师,研究方向:大数据信息安全;白利芳(1990—),女,山西吕梁人,硕士,工程师,研究方向:网络与信息安全。

拟态伪装的方式进行主动隐匿，以达到干扰或阻断攻击的目的，这种在网络空间中的拟态伪装称为“拟态防御”(Mimic Defense，MD)。将一个存在未知漏洞、后门或病毒、木马等软硬件代码的“有毒带菌”异构执行环境称为拟态防御界。

拟态防御的实现基于动态异构冗余[7](Dynamic Heterogeneous Redundancy，DHR)思想。异构冗余即异构冗余集合中的任意元素，无论是单独使用还是多元素并联或组合使用，均可实现等价功能的一种机制，其理论基础是异构的冗余元素共性设计缺陷导致共模故障属于小概率事件。该机制的典型范例即非相似余度构造，如图1所示。

DHR即在异构冗余的基础上加入动态性和随机性，使系统呈现相当程度的不确定性，扰乱攻击者信息链，攻击难度非线性增加，攻击成功成为极小概率事件。其实现主要基于异构冗余体池中冗余执行体集的内生构造，即拟态防御的核心过程——拟态伪装：从异构冗余池中根据动态调度算法随机选取若干元素组成执行体(如图2所示)，或重构、重组、重建冗余执行体自身，或借助虚拟化技术改变冗余执行体的资源配置，或对冗余执行体进行预防性或修复性的清洗、初始化操作等，增加服务功能与外在表征间的不确定性，实现隐匿拟态界内未知的漏洞和后门等脆弱性[6-9]。而DHR输出依然采用多模裁决机制，和区块链的原理有共通之处。

3.2 拟态防御抗攻击分析

本小节以图2所示的DHR构造为研究对象，分别从攻击发起难度、持续攻击难度何攻击再现难度进行分析。

(1)攻击发起难度。此处设异构构件集合为U，|U|=m，设执行体集合为V，|V|=n，则随机动态选择算法由U到V有C_m^n种可能，设每种可能经表决器输出后与正常输出不一致的概率为P_i(i=1，2，……，C_m^n)，则在该攻击环节成功的几率为：$Q=\sum_{i=1}^{C_m^n} Pi$。由于多模表决器本身的特性，P_i极小，可知Q极小，所以，在该环节的攻击成功率极小。

(2)持续攻击难度。一次成功的攻击往往由多个攻击环节组成，设某次成功的攻击行为共涉及r个攻击环节，若此次攻击成功，则需每个攻击环节均成功。则此次攻击成功的概率为：$P=\prod_{j=1}^{r} Q_j$。此时，P<<Q。若在某个环节失败，当攻击者再次尝试一次新的攻击时，由于每个环节的U经过再次的随机动态选择后，V发生改变，所以相当于发起一次新的攻击。可见在拟态防御机制中，攻击不具有持续性。

(3)攻击再现难度。某一次攻击偶然成功后，同上，当攻击者想再次复现攻击时，攻击目标已变，先前的攻击经验并不能作为先验知识库应用到后续的复现。

综上分析，拟态防御发起难、持续难、再现难，是有望扭转“易攻难守”不对称格局的一种新兴技术。

4 拟态防御测试评估

2016年1月至6月，受国家科技部委托，上海市科学技术委员会先后组织国内网络通信和安全领域的21名院士和110余名专家，对拟态防御理论和验证系统进行测试评估。测评对象为两种应用场下的拟态防御原理验证系统，测试评估内容涵盖[6]：能否隐匿拟态界内的未知漏洞和后门、能否利用拟态界内未知漏洞注入未知病毒木马、能否有效抑制拟态界内基于未知因素的协同攻击、能否允许拟态界内使用“不可信、不可控”的软硬构件、拟态界内运行环境能否允许“有毒带菌”。测试方法包括黑盒测试、白盒测试、渗透测试、对比测试等，也包括预置后门和配合注入病毒木马等方式。

2018年5月10日至12日，首届“强网”拟态防御国际精英挑战赛上，基于网络空间拟态防御理论开发的网络设备和系统作为“靶机”，接受来自国内外挑战队集中火力“打靶”测试，即对其进行高强度的安全测试。

综合测试分析表明，验证测试结果与理论预期完全吻合[6，10]。在功能等价异构冗余的多维动态重构机制作用下，几乎不可能实现拟态界内可靠、持续的协同逃逸，且允许拟态界内使用“不可信、不可控”的软硬构件，允许“有毒带菌”的运行环境[6，10]。此外，MD机制对现有网络空间安全在防御体制上具有互补性，技术上具有融合性，产品上具有自主可控性，还具有降低专用安全设施的更新升级代价、防护实时性要求、版本同步更新频度等综合性优势[6，10]。

5 拟态防御应用实践

时任国务院副总理的马凯、刘延东等中央领导同志先后就推进拟态防御技术研发和应用作出批示，工信部、河南省多次就拟态防御应用试点示范组织专家进行研讨、部署。2017年10月，工信部网安局下发《关于开展拟态防御技术试点工作的通知》，要求将拟态防御部署应用到现网环境，为拟态防御的推广应用开展量化评估，推动拟态防御技术及产业不断成熟完善。2018年1月，全球首套拟态域名服务器在河南联通上线运行，在不改变现有网络结构的前提下，通过将拟态构造全面植入传统域名服务器实现增量部署。4月，全球首套拟态防御网络设备落户景安网络科技股份有限公司，意味着我国自主创新的拟态防御继电信基础运营商后正式投入互联网线上服务。

6 拟态防御优势与挑战

在现有主动防御技术中，入侵容忍以维持系统可用性为主要目的，使系统具有较高的生存能力和可靠性[1]，但高成本的冗余和表决时延成为其发展的障碍。移动目标防御通过动态变化使系统静态性减弱，对攻击目标起到一定隐蔽作用[2]。然而性能和动态变化频率之间的平衡成了问题。此外，目标的多样呈现也可能给攻击者提供更大的攻击面，反而起到反作用[6]。拟态防御既能维持可用性，也能对被攻击目标起到隐蔽作用。相比入侵容忍技术，在防御目的上更倾向于对安全性整体的防护而不仅是可用性。较移动目标，其隐蔽原理不同，通过多模表决“中和”或掩盖被攻击目标的输出，从而对外表现为无异常或攻击无效，扰乱攻击者对攻击效果的判断[6]，且拟态防御可用相对较少的资源代价实现相对较高的防御能力。

我国对入侵容忍和移动目标防御技术的研究和应用处于落后状态，而拟态防御作为我国自主提出的网络空间主动防御技术，有望打造我国自主可控的防御策略体系，打破网络空间安全在攻防不对称、大国博弈不平衡的格

局。但拟态防御并不意味着可以解决所有领域范围的网络安全问题，其实现的前置条件，首先是要存在可判定异构冗余体之间功能等价性的“拟态界”，其次需在给定功能性能下存在软硬构件多元或多样化供应条件。也并不意味着没有被攻破的可能，在同时同地同手段的海量协同攻击的情形下，理论上不是不无可能，但在非配合的现实情况下，要刚好能同时同地利用同手段实施攻击并攻击成功可认为是不可能事件。

参考文献

[1]Nguyen Q L,Sood A.“A comparison of intrusion-tolerant system architectures.”Security& Privacy IEEE,vol.9,no.4,pp.24-31,2011.
[2]Manadhata P K.“Game theoretic approaches to attack surface shifting.”Moving Target Defense II.Springer,2013.
[3]Jajodia S,Ghosh A K,Swarup V,et al.“Moving target defense.”Springer, 2011.
[4]Levitin G.“Optimal structure of fault-tolerant software systems.”Reliability Engineering & System Safety, vol.89,no.3,pp.286-295,2005.
[5]Pal P, Webber F, Schantz R E, et al. “Intrusion- tolerant systems,” In Proc. IEEE.Information Survivability Workshop (ISW-2000).pp.24-26,2000.
[6]罗兴国,仝青,张铮,邬江兴.拟态防御技术[J].中国工程科学,2016,18(06):69-73.
[7]邬江兴.网络空间拟态防御研究[J].信息安全学报,2016,1(04):1-10.
[8]仝青,张铮,张为华,邬江兴.拟态防御Web服务器设计与实现[J].软件学报,2017,28(04):883-897.
[9]仝青,张铮,邬江兴.基于软硬件多样性的主动防御技术[J].信息安全学报,2017,2(01):1-12.
[10]张铮,马博林,邬江兴.web服务器拟态防御原理验证系统测试与分析[J].信息安全学报,2017,2(01)2017,2(01):13-28.

A Summary of Cyberspace Security Mimic Defense Technology

LI Zheng[1],BAI Li-fang[2],TANG Gang[2],ZHU Xin-ming[2]
(1. Unicom Systems Integration Ltd.,Beijing100071;2.China Software Testing Center,Beijing 100048)

Abstract: This paper briefly analyzes the current imbalance situation of cyber space security, outlines the development process of mimic defense (MD) technology, and focuses on the basic principle of MD and its anti-aggressivity. At last, introduces the test evaluation and application practice of MD and analyzes its advantages and challenges.

Key words:network security; active defense; mimic defense; dynamic heterogeneous redundancy

••••••上接第36页

规划过程不断迭代，最终采用改进的蚁群算法路径规划吻合度高达98.7%，高于采用蚁群算法的路径规划吻合度89.4%；同时，在路径规划效果达到稳定状态的过程中，改进的蚁群算法耗时257.4ms小于蚁群算法耗时329.2ms。

仿真结果表明：在路径规划吻合度方面，改进的蚁群算法搜索全局最优解的能力得到提升；在节约时间成本方面，改进的蚁群算法收敛速度更快。

6 结语

本文针对人工智能路径规划领域的蚁群算法进行改进，设计基于排序的精英蚂蚁策略改进的蚁群算法模型，采用排序策略、信息素挥发系数自适应策略和最大—最小蚂蚁策略改进信息素更新规则，以完善对全局最优解的搜索能力并提高算法的收敛速度。通过仿真，证明本设计具有理论优势和实际应用价值，并为后续的人工智能机器人路径规划研究提供了参考方案。

参考文献

[1]Colorni A, Dorigo M, Maniezzo V. Distributed Optimization by Ant Colonies[C]// Ecal91-European Conference on Artificial Life. 1991:134-142.
[2]喻环.改进蚁群算法在机器人路径规划上的应用研究[D].安徽大学,2017.
[3]赵凯,李声晋,孙娟,赵锋.改进蚁群算法在移动机器人路径规划中的研究[J].微型机与应用,2013,32(04):67-70.
[4]邱莉莉.基于改进蚁群算法的机器人路径规划[D].东华大学,2015.
[5]Gambardella M,Dorigo M. Solving symmetricand asymmetric TSPs by ant colonies[C]//Proc of the IEEE Conf on Evol Compu, 1996:622-627.
[6]Dorigo M, Maniezzo V, Colorni A. Ant system: optimization by a colony of cooperating agents[J]. IEEE Transaction on System, Man and Cybernetics: Part B, 1996, 26(1): 29-41.
[7]胡小兵.蚁群优化原理、理论及其应用研究[D].重庆大学,2004.
[8]B.Bullnheimer, R.F.Hart, C.Strauss. Applying the ant System to the Vehicle Routing Problem. Meta-Heuristics: Advances and Trends in Local Search Paradigms for Optimization. Kluwer, Boston, 1998:109-120.
[9]任瑞春.基于排序加权的蚁群算法[D].大连海事大学,2006.
[10]王鸿豪.基于蚁群算法的机器人路径规划及其在港口上的应用探讨[D].武汉理工大学,2007.
[11]申铉京,刘阳阳,黄永平,徐铁,何习文.求解TSP问题的快速蚁群算法[J].吉林大学学报(工学版),2013,43(01):147-151.