专题：网络安全的智能化和高对抗性发展

基于异构冗余架构的拟态防御建模技术

秦俊宁[1]，韩嘉佳[2]，周升[3]，吴春明[4]，陈双喜[4,5]，赵若琰[4]，张江瑜[4]

（1. 浙江华云信息科技有限公司，浙江 杭州 310027;
2. 国网浙江省电力有限公司电力科学研究院，浙江 杭州 310027;
3. 国网浙江省电力有限公司，浙江 杭州 310027;
4. 浙江大学，浙江 杭州 310058；5. 嘉兴职业技术学院，浙江 嘉兴 314036）

摘　要：介绍了网络安全发展的不平衡现状，对渗透测试的主要危害和机理模型进行描述，分析并发现了现存的多种传统防御手段均存在其固有缺点；而拟态防御模型的新方法可以通过动态选择执行体集，适应性地改变系统组成，使得攻击者获得的攻击信息失效，相同攻击难以维持或再现，基于攻击链模型对传统防御技术和拟态防御技术进行了分析和对比，论证了拟态防御在攻击链的多个阶段均具有防护作用；最后，通过实验验证了拟态防御的有效性和优越性，并对该模型进行了总结和展望。

关键词：传统防御；非平衡态势；渗透测试；异构冗余；拟态防御

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2020143

Modeling of the mimic defense based on heterogeneous redundancy

QIN Junning[1], HAN Jiajia[2], ZHOU Sheng[3], WU Chunming[4], CHEN Shuangxi[4,5], ZHAO Ruoyan[4], ZHANG Jiangyu[4]

1. Zhejiang Huayun Info Technology Co., Ltd., Hangzhou 310027, China
2. State Grid Zhejiang Electric Power Co., Ltd. Research Institute, Hangzhou 310027, China
3. State Grid Zhejiang Electric Power Co., Ltd., Hangzhou 310027, China
4. Zhejiang University, Hangzhou 310058, China
5. Jiaxing Vocational and Technical College, Jiaxing 314036, China

Abstract: The unbalanced development status of network security was introduced. The main hazards and the mechanism model of penetration testing were described, and the inherent shortcomings of many existing traditional defense methods were analyzed. However, new method of the mimic defense model makes the attack information obtained invalid by dynamically selecting the executive set and adaptively changing the system composition. The same attack mode is difficult to be maintained or reproduced. Based on the attack chain model, the traditional defense

收稿日期：2020−02−25；修回日期：2020−04−25

通信作者：陈双喜，abelchen@zju.edu.cn

基金项目：国家电网总部科技项目（No.52110118001F）

Foundation Item: The Science and Technology Funding Project of State Grid (No.52110118001F)

technology and mimic defense technology were analyzed and compared, and it was demonstrated that it had a protective role in multiple stages of the attack chain. Finally, the effectiveness and superiority of the mimic defense was verified by experiments, and the model was summarized and prospected.

Key words: traditional defense, unbalanced situation, penetration test, heterogeneous redundancy, mimic defense

1 引言

漏洞的存在是近些年来各个网络安全事件发生的主要原因[1]，根据中国国家信息安全漏洞库的统计[2]，漏洞的总数量在近些年呈现线性增长的趋势。在多种多样的互联网安全问题中，Web 安全的影响和威胁非常大，通过攻击 Web 系统、植入木马等方式可以造成大范围内的安全攻击。基于以上情况，现阶段的解决途径是发展主动防御技术。

当前用的查病毒、杀木马、补漏洞等方式，都是一种“亡羊补牢”的工作模式，已经补过的漏洞即可看成科学理论中的确定性问题，而那些没有被发现的漏洞、没有被彻底翻出来的后门、还没有被感知的木马等，就是不确定威胁，现阶段典型的防御技术（如入侵隔离[3]、入侵检测[4]、入侵容忍[5]等）用不同的方法尝试对多种网络攻击方式进行防御，但是它们都是被动防御技术，均存在被攻击者绕过的可能性，而拟态防御则通过增加自身的不确定性，让攻击者难以看透，是一种能够与未知对手进行对抗，取得胜利的新方法，也是当前的主要研究趋势[6]。

1.1 渗透方法的主要危害

渗透测试是通过模仿黑客的行为进行攻击，进而掌握对方系统的主要信息，并收集目标系统的信息的方法。分析过程是多方面的，可以获得攻击者的位置信息，为利用安全漏洞创造有利条件。网络入侵是带有目的性与侵略性的非法攻击行为，而渗透测试是在授权下主动发现并修复漏洞的合法防御行为，它们之间存在着很大的区别。入侵、渗透测试、破解、漏洞恢复、漏洞等不同渗透行为之间的关系如图 1 所示，入侵带来的主要危害有网络攻击、控制系统、隐私泄露，防御人员首先通过漏洞挖掘和漏洞扫描来发现系统中存在漏洞，然后通过渗透测试来探测出系统的漏洞，最后通过一系列手段进行漏洞修复。

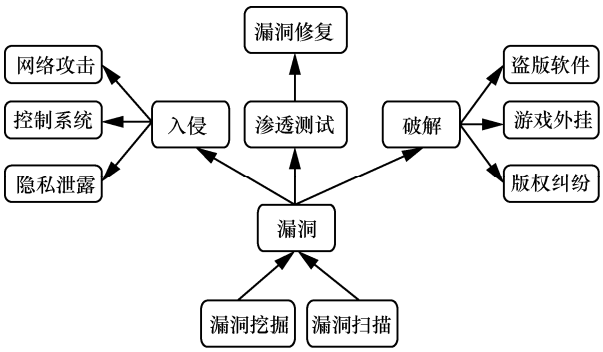

图 1 不同渗透行为之间的关系

漏洞的存在对系统安全存在的威胁不仅仅只限于它的直接可能性，入侵成功需要很多条件，比如需要经过收集信息、过滤无用信息、逐层进行深入等多个步骤。攻击者利用系统中存在的漏洞进行攻击，并以此来获得目标系统中管理员的权限，得到被攻击系统中的敏感信息，破坏系统，影响网络的正常运行，由此看来，安全漏洞对系统的危害性很大。因此，在日常的安全运维工作中，需要加强 Web 应用的目录权限配置，可以通过限制目录遍历功能，加强日常的密码管理等方式来减少系统中存在的安全漏洞。

1.2 渗透方法的机理模型

渗透测试是一个对系统进行综合评分的过程，渗透测试模型的主要流程如图 2 所示，可以细化为规划与准备、侦察与发现、分析与评估、尝试主动入侵、撰写报告与权限维持 5 个阶段。

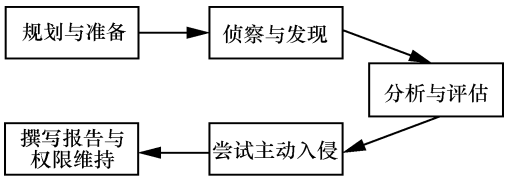

图 2　渗透测试模型的主要流程

（1）规划和准备阶段

测试人员在进行渗透测试之前，通过仔细分析用户提交的需求报告来了解用户需求，对需要进行的测试具有大致了解。

（2）侦察与发现

在探测目标系统信息的阶段，测试人员只知道目标测试系统的 IP 地址，测试人员通过主动或者向客户询问的方式获取有用信息。首先使用测试工具来对目标系统进行扫描探测，获取目标系统上开放的端口信息及其他对方攻击有用的信息，扫描这些对外开放的端口并查看其上运行的服务。

（3）分析与评估

测试人员根据之前阶段收集到的各种信息，进行综合分析，尝试多种方法对系统执行攻击行为。在分析评估阶段，潜在风险的存在也是测试人员需要关注的主要问题。

（4）尝试主动入侵

尝试主动入侵阶段基于前面收集到的信息以及分析得到的内容，对存在潜在风险的漏洞进行评估，测试人员建议消除这些漏洞和风险。

（5）撰写报告及权限维持

在撰写报告及权限维持阶段，需要介绍测试的整个过程，记录分析的潜在漏洞，修复存在漏洞的过程，并对漏洞进行优先级排序，提出对未来的安全建议。

2　现有防御模型的缺陷

Web 软件中的漏洞，存在普遍性与易安插性，功能越复杂的软件中，漏洞也相对来说更多[7]。我国的软件行业起步较晚，没有使用当前最先进的技术，而是大多采用国外相对成熟的技术，则会有被安装“后门”的可能，安全性能不能够得到保障[8]。攻击方掌握的信息往往超过防御方，所以防御具有很强的被动性，现阶段很多的软件都是被动的，系统中的各种缺陷无处隐藏，攻击者非常容易就可以找到其漏洞对其进行攻击。攻击的步骤大致可以分为“扫描探测”“漏洞挖掘”“攻击植入”“攻击维持”4 个阶段，这 4 个阶段之间联系紧密且层层相扣，破坏其中的一个或者多个环节就可以达到抵御攻击行为的目的[7]。传统的防御技术必须详细地了解攻击者的攻击手段，才能够对攻击者进行主动防御，这种被动防御体系以及技术上的缺陷则是导致目前网络空间安全“易攻难守”现象存在的主要原因。

为了解决被动防御中存在的问题，研究者提出了许多防御思路，如动态目标防御（moving target defense，MTD）[9]思想，但是 MTD 防御思想存在其固有的缺陷，它主要在扫描探测阶段发挥作用，而没有通用性，且由于它构造相对复杂，导致消耗的资源比较多。随后，*N*–变体系统被提出，它采用多个异构执行体，给予它们相同的输入，然后比较它们的执行结果是否相同，以此来判断系统是否遭受攻击。但是它也存在缺点，比如 *N*–变体系统中的异构执行体在运行过程中保持静态不变，因此攻击者在较长的一段时间内，仍然有很大的机会检测到 Web 系统中存在的漏洞，并对其进行攻击。随后，邬江兴院士经过进一步研究，结合移动目标防御的动态性和 *N*–变体系统的冗余特性，提出了拟态防御模型[10]。拟态防御的新方法使得攻击者几乎不能获取到目标系统中的有效信息，阻断其攻击链构造，使攻击行为很难进行下去。

3　拟态防御模型

由于漏洞以及后门的存在，网络空间组成成

分呈现单一性和静态性，现有条件下很难保证彻底发现和消除网络安全威胁。网络空间拟态防御（cyberspace mimic defense，CMD）[6]理论的提出改变了这种现状，动态异构冗余（dynamic heterogeneous redundancy，DHR）架构是其重要的组成成分，“非相似余度构造”（dissimilar redundancy structure，DRS）[11-12]是 DHR 的一个经典范例。

3.1 增大攻击植入难度

假设一个执行体集中有 3 个执行体，执行体有异构型，包括服务器异化、操作系统的异化以及文件系统的异化。在每一次的攻击行为中，系统的输入由攻击者提供，根据攻击行为的输出结果决定下一步将要进行的行动，若此次交互可以促进攻击行为或者在系统中显示出攻击成功的信号，则规定这一次的攻击交互过程是成功的，由于不同的执行体集性质不同，故其攻击攻击交互行为的成功率也各不相同。设对单一执行体 A 攻击成功的概率为 p_{A_i}，执行体 B 和 C 的攻击成功的概率为 p_{B_i} 和 p_{C_i}，那么在拟态防御结构中，攻击成功的概率则可以记为 $p'_i = p_{A_i} \times p_{B_i} \times p_{C_i} \times V_i$，其中，$V_i$ 是 3 个执行体的输出结果在表决时的一致性，即：

$$V_i = \begin{cases} 1, & \text{表决结果一致} \\ 0, & \text{表决结果不一致} \end{cases} \quad (1)$$

由于 $0 \leqslant p_{A_i}、p_{B_i}、p_{C_i} \leqslant 1$，即 $p'_i \leqslant \min\{p_{A_i}, p_{B_i}, p_{C_i}\}$，定义交互成功率下降幅度为 D，$D = (\min\{p_{A_i}, p_{B_i}, p_{C_i}\} - p'_i) / \min\{p_{A_i}, p_{B_i}, \cdots, p_{C_i}\}$，可以看出拟态防御方法的效果更佳[7]。

3.2 增大攻击维持难度

从各个功能相同的异构冗余体池中取出几个元素构成当前的服务集，构建出异构冗余体，或者对原先使用的异构冗余体做修复性质的清洗，从而使得攻击者难以复现攻击现场[6]。例如攻击者设置木马，运行在要攻击的主机上，获得其文件目录。但是，在新型的主动防御环境下，相互异构的主机之间的文件的目录之间不一致，使得攻击者不能按照预期获得想要的信息，因此拟态防御可以扰乱反馈给攻击者的信息，从而使攻击难度增大。

拟态防御的功能不局限于一种攻击方式，而对多种攻击方式都可以起作用，它从攻击的本质出发，对各种威胁都具有非常强的防御能力，本文将利用具体实验来说明拟态防御的优势。

4 实验环境

实验中使用宿主机作为攻击节点，3 个虚拟机部署相同服务作为执行体提供正常服务。实验中使用 Cobalt_Strike 渗透软件，该软件在渗透过程中通过 Team Server 来管理受害者节点的连接，在攻击过程中攻击节点连接 Team Server，Team Server 和受害者节点通信。实验机器配置见表 1。node1、node2、node4 为执行体，同时 node2 也作为 Cobalt_Strike 的 Team Server，node3 作为负载均衡服务器。

表 1 实验机器配置

名称	用途	内存	处理器	硬盘	系统
node1	执行体	2 GB	Intel® Core™ i5-6300HQ CPU @ 2.30 GHz	20 GB	Ubuntu16.04.6
node2	执行体	1 GB		20 GB	CentOS7
node3	负载均衡服务器	1 GB		20 GB	CentOS7
node4	执行体	2 GB		60 GB	Windows2012
Windows10	攻击节点	8 GB		1 TB	Windows10

在 node4 部署 Cobalt_Strike 生成的木马，测试开启和关闭拟态的木马连接性。负载均衡服务器采用 ip_hash 的负载策略，在节点正常工作情况时，相同 IP 地址的访问流量转发到固定的服务器节点。在 Team Server 节点设置 Cobalt_Strike 客户端连接密码为******，连接端口为 5050，同时设置并开启 reverse_http 的端口 23456，Team Server 服务开启成功如图 3 所示。

攻击节点通过 Cobalt Strike 客户端连接 Team Server，在 15:48:20 时，通过 admin has joined 标识表示攻击节点成功连接 Team Server。在 15:55:57 时，通过图片中的标识得知 IP 地址为 192.168.186.135，部署 Cobalt_Strike 生成的木马节点以 Administrator 的身份成功连接木马控制器，攻击节点木马程序成功连接如图 4 所示。

5　实验结果

5.1　实验工具

Apache JMeter 是一款用于测试客户端/服务器端结构的软件，能够测试出服务器端以及客户端上动态以及静态资源的性能，它可以分析出在不同负载条件下服务器的整体性能。通过手工在执行体中放置木马，测试木马连接性测试拟态防御下防御效果的有效性，选择 3 种常见的木马后门 Cobalt Strike[13]、灰鸽子和反弹 shell。Cobalt Strike 是 C/S 架构的商业渗透软件，分为客户端和服务器端；灰鸽子是一款远程控制软件；反弹 shell 是一种常见的攻击手段，由服务器主动向客户端发起连接。下面分析以 Cobalt Strike 为例，实验结果表明拟态防御对灰鸽子和反弹 shell 同样有防御效果。

5.2　未开启拟态防御时的实验结果

JMeter 测试工具会在 10 min 内创建 6 000 个线程，每个线程相当于一个用户，每 0.1 s 创建一个线程，通过这样测试网站的性能，未开启拟态时的响应时间趋势如图 5 所示，其中平均值代表每个请求的平均响应时间，最小值代表最小响应时间，最大值代表最大响应时间，单位均为 ms，异常百分比即错误率，计算方法为错误请求数量与请

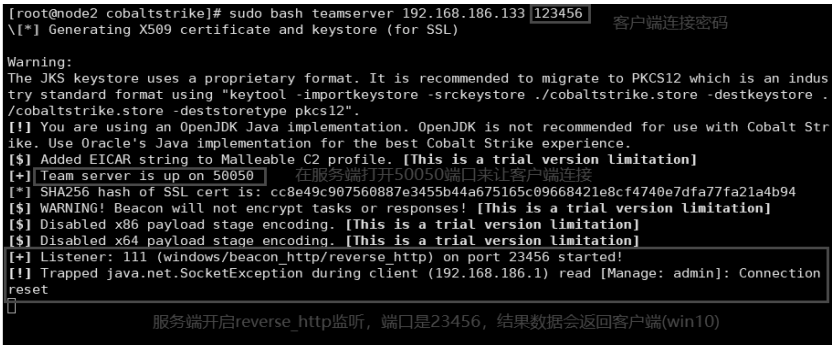

图 3　Team Server 服务开启成功

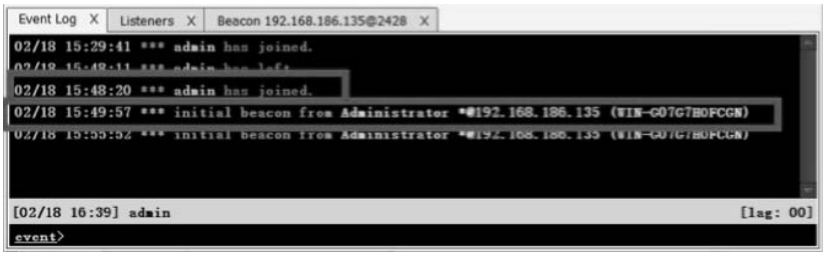

图 4　攻击主机木马成功连接

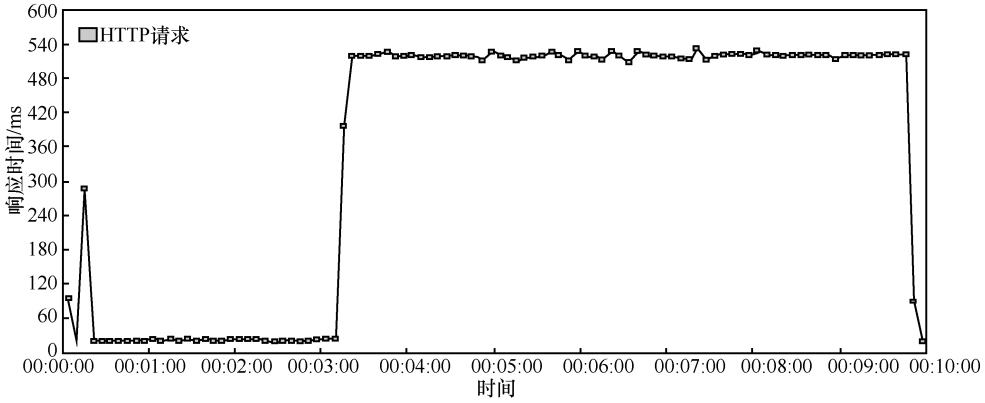

图 5　未开启拟态时的响应时间趋势

求总数的比值，吞吐量表示每秒完成的请求数。

未开启拟态防御时，样本数为 6 000，同时也代表 6 000 个 HTTP 请求，每个请求平均响应时间为 353 ms，最小响应时间为 8 ms，最大响应时间是 1 478 ms，网站吞吐量为每秒 10.0 个请求，考虑到 6 000 个点的可视化效果较差，均匀地选择了其中 100 个点构成响应时间趋势。

未开启拟态防御时的木马连接状态如图 6 所示，在控制窗口中输入 netuser 命令，等待 1 min 后，返回如图 6 所示的结果，返回的结果表明木马处于正常连接状态。

5.3　开启拟态防御后的实验结果

在开启拟态后，使用未开启拟态时的相同配置进行相同的性能测试。样本数为 6 000，代表 6 000 个 HTTP 请求，每个请求平均响应时间为 2 124 ms，最小响应时间为 7 ms，错误请求占比为 22.43%，网站吞吐量为 10 个/s，出于同样的考虑，从 6 000 个点中均匀地选择 100 个构成响应时间趋势，如图 7 所示。

开启拟态防御后的木马连接状态如图 8 所示。图 8 中 last 字段的数据表示的含义是距离上一次交互的时间，last 字段的值是 1m。该程序每 60 s 会自动连接目标主机，然后时间从 1 s 开始计算，

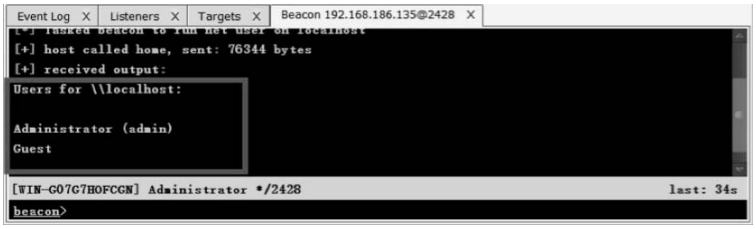

图 6　未开启拟态防御时的木马连接状态

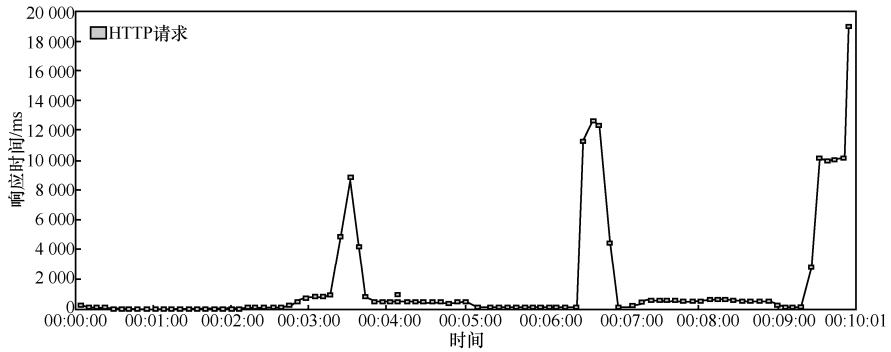

图 7　开启拟态防御后的响应时间趋势

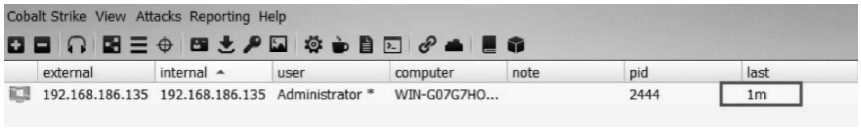

图 8　开启拟态防御后的木马连接状态

所以正常连接状态 last 字段的值应该是 0～59 s，如果显示 1m 则表示连接失败。因此在开启拟态防御功能后，木马无法正常连接，拟态防御功能生效。

5.4　实验结果对比分析

是否开启拟态的网站性能数据见表 2，未开启拟态防御和开启拟态防御相比，未开启拟态防御时，网络请求的平均响应时间更短，但是错误请求数量会更多，其他性能数据没有明显差距。错误数量更多的原因是短时间的大流量访问会导致部分执行体下线，由于没有开启拟态防御，下线执行体不会主动上线，因此增加了错误请求数。

开启拟态防御后，执行体会动态下线自愈，在执行体下线时无法提供正常服务，如果负载均衡器此时分配流量到该执行体，则负载均衡器需要等待一段时间，发现执行体无法正常响应后，再把流量转发到下一个执行体。因此开启拟态防御后，对于某些流量增加了等待响应的时间，从而增加了平均响应时间，如图 9 所示，开启拟态的响应时间有 3 段峰值，因为实验环境中部署了 3 个执行体，每个峰值分别对应每个执行体下线清洗。

从上面的实验结果可知，未开启拟态防御的环境下木马可以连接，开启拟态防御的环境下木马无法连接，这种现象的原因是开启拟态防御后，执行体会动态下线自愈，打断攻击链，从而使其无法实现有效攻击，因此拟态防御对后门的防御具有有效性。

6　结束语

拟态防御的方法提供了不同于以往的攻击途径，与传统的防御技术相比，新型的拟态防御环境下，攻击者在攻击链的任何阶段都很难攻击成功，它具有很强的动态性，不规律地改变系统的组成成分，从而使攻击者之前获得的信息失效，

表 2　是否开启拟态的网站性能数据

实验环境	样本数量	平均值	最小值	异常	吞吐量	接收	发送
未开启拟态防御	6 000	353	8	33.18%	10.0 个/s	19.01 KB/s	2.15 KB/s
开启拟态防御	6 000	2 124	7	22.43%	10.0 个/s	20.79 KB/s	2.25 KB/s

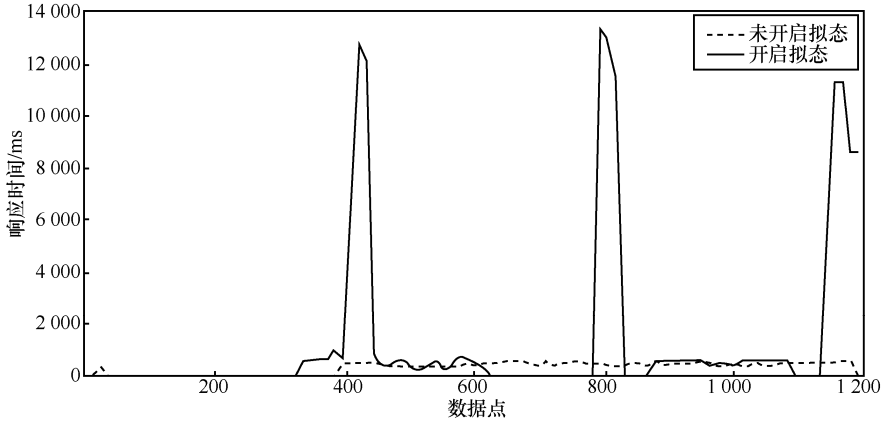

图 9　是否开启拟态响应时间对比

攻击行为不能够维持。本文首先对当前国内外的安全防御现状进行分析，然后通过具体的实验对拟态防御技术和传统防御技术进行多维对比，分析其实验结果，证明了拟态防御的效果。

参考文献：

[1] SUBRAHMANIAN V S, OVEKGONN M, DUMITRAS T, et al. The global cyber-vulnerability report[J]. Springer Int'l Publishing, 2015(10): 33-64.

[2] China Information Technology Security Evaluation Center. China national vulnerability database of information security[EB]. 2015.

[3] XU H, CHEN X, ZHOU J, et al. Research on basic problems of cognitive network intrusion prevention[C]//Proceedings of 9th International Conference on Computational Intelligence and Security (CIS). Piscataway: IEEE Press, 2013: 514-517.

[4] CHUNG C J, KHATKAR P, XING T, et al. NICE: network intrusion detection and countermeasure selection in virtual network systems[J]. IEEE Transaction on Dependable and Secure Computing, 2013, 10(4): 198-211.

[5] MADA B B, GOSEVAP K, VAIDYANATHAN K, et al. A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. Performance Evaluation, 2004, 56(14): 167-186.

[6] WU J X. Research on cyberspace mimic defense[J]. Journal of Information Security, 2016, 1(4): 1-10.

[7] 仝青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017, 28(4): 883-897.
TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense Web server[J]. Journal of Software, 2017(4): 883-897.

[8] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 2-7.
WU J X. The original intention and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 2-7.

[9] National Science and Technology Council. Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program[EB]. 2011.

[10] 邬江兴. 网络空间拟态防御原理[M]. 北京: 科学出版社, 2018: 317-367.
WU J X. Cyber mimic defense[M]. Beijing: Science Press, 2018: 317-367.

[11] VOAS J, GHOSH A, CHARRON F, et al. Reducing uncertainty about common-mode failures[C]//Proceedings of IEEE Symposium on Software Reliability Engineering (SRE' 97). Piscataway: IEEE Press, 1997: 308-319.

[12] LECITIN G. Optimal structure of fault-tolerant software systems[J]. Reliability Engineering & System Safety, 2005, 8(3): 286-295.

[13] LIU C, LI C Q, QIU G W. Research on intruder countermeasures based on CobaltStrike and office vulnerabilities[J]. Cyberspace Security, 2018(1): 56-61.

[作者简介]

秦俊宁（1972– ），男，浙江华云信息科技有限公司高级工程师，主要研究方向为信息安全管理。

韩嘉佳（1983– ），女，国网浙江省电力有限公司电力科学研究院高级工程师，主要研究方向为网络安全。

周升（1985– ），男，国网浙江省电力有限公司高级工程师，主要研究方向为网络安全。

吴春明（1967– ），男，浙江大学教授、博士生导师，主要研究方向为人工智能、柔性可重构网络体系、软件定义网络、网络主动防御创新安全技术等。

陈双喜（1980– ），男，嘉兴职业技术学院讲师，浙江大学博士生，主要研究方向为网络空间安全的渗透与主动防御。

赵若琰（1998– ），女，浙江大学硕士生，主要研究方向为云安全、拟态防御。

张江瑜（1998– ），男，浙江大学硕士生，主要研究方向为新型主动防御。