基于拟态防御的以太网交换机内生安全体系结构

宋克[1]，刘勤让[1]，魏帅[1]，张文建[1]，谭力波[2]
（1. 信息工程大学信息技术研究所，河南 郑州 450002；2. 天津市滨海新区信息技术创新中心，天津 300450 ）

摘 要：针对以太网交换机面临的未知漏洞和未知后门安全威胁，提出了一种基于拟态防御理论的交换机内生安全体系结构。介绍了所提体系结构的理论基础、构建方式、安全机理；提出并分析了 TAMA 的算法策略及安全提升效果；设计实现了拟态交换机原型样机并进行了白盒插桩及攻击链安全性测试。理论分析及测试结果表明，在各种攻击场景下，所提体系结构具有良好的未知漏洞和未知后门防御能力。

关键词：以太网交换机；拟态防御；动态异构冗余；内生安全
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020098

Endogenous security architecture of Ethernet switch based on mimic defense

SONE Ke[1], LIU Qinrang[1], WEI Shuai[1], ZHANG Wenjian[1], TAN Libo[2]
1. Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China
2. Information Technology Innovation Center of Tianjin Binhai New Area, Tianjin 300450, China

Abstract: Aiming at the unknown vulnerabilities and unknown backdoor security threats faced by Ethernet switches, a switch endogenous security architecture based on mimicry defense theory was proposed. The theoretical basis, construction mode and security mechanism of the architecture ware introduced, the algorithm strategy and security improvement effect of TAMA algorithm were proposed and analyzed, a prototype of mimic switch was designed and implemented, and the security tests of white box stuffing and attack chain were carried out. Theoretical analysis and test results show that the architecture has good unknown vulnerabilities and unknown backdoor defense capabilities in various attack scenarios.

Key words: Ethernet switch, mimic defense, dynamic heterogeneous redundancy, endogenous security

1 引言

以太网交换机作为信息网络中一种不可或缺的基础设施，其安全性越来越重要。

传统以太网交换机的安全防护主要通过在交换机中嵌入安全模块或外加防火墙等安全设备[1]，采用端口绑定、划分虚拟专用网络（VPN, virtual private network）、流量控制、配置访问控制列表（ACL, access control list）等防御手段，应对广播风暴攻击、海量 MAC（media access control）地址攻击、MAC 欺骗攻击、地址解析协议（ARP, address resolution protocol）欺骗攻击、生成树协议环路攻击、分布式拒绝服务（DDoS, distributed denial of service）攻击等协议层面的攻击行为[2-3]。

然而，随着以太网交换机功能由二层向三层、四层扩展，以及基于软件定义网络（SDN, software defined network）的以太网交换机的研究与应用，针对交换机控制管理层面的安全攻击越来越多。据

收稿日期：2019−12−16；**修回日期**：2020−03−19
基金项目：国家核高基重大专项基金资助项目（No.2017ZX01030301）
Foundation Item: The National Core Electronic Devices, High-end Generic Chips and Basic Software Major Projects (No.2017ZX01030301)

国家信息安全漏洞库数据统计，2015—2017 年，被发现的以太网交换机的安全漏洞总计 55 个，包括固件漏洞、操作系统漏洞、协议实现漏洞、软件漏洞等。

攻击者利用交换机主控 CPU、操作系统或协议栈、管理软件存在的漏洞及后门，直接获取交换机的控制权限，修改路由表及其他配置项，使传统的安全防护手段形同虚设；基于防火墙、杀毒软件、入侵检测系统的被动防护技术，对于未知的漏洞和后门造成的 0 day 攻击不能提前防御。近年来，多家公司的以太网交换机被曝出安全漏洞，这对网络信息安全造成重大隐患。

鉴于被动防御存在防护缺陷，许多国家都在开展网络信息安全主动防御技术的研究。美国的移动目标防御（MTD, moving target defenses）技术，针对外部利用未知漏洞的攻击防御，在假设内部安全可信的前提下，主要采用软件技术实现主动防御，应对逻辑层攻击[4-6]。我国邬江兴院士首创的网络空间拟态防御（CMD, cyber mimic defense）技术，采用动态异构冗余（DHR, dynamic heterogeneous redundancy）的系统架构和运行机制，既可防御外部利用未知漏洞的攻击，也可防御利用未知后门的攻击，在允许基本环境一定程度“有毒带菌”的情况下，采用软件技术和系统结构组合应用实现主动防御，可为信息网络基础设施或重要信息服务系统提供一种不依赖传统安全手段（如防火墙、入侵检测、杀毒软件等）的构造化内生安全增益或效应[7-8]。

随着网络空间拟态防御理论的完善，众多依据 CMD 技术构建的安全网络设备陆续出现。仝青等[9]设计实现了拟态防御 Web 服务器；马海龙等[10]设计实现了基于动态异构冗余机制的路由器拟态防御体系结构；魏帅等[11]实现了面向工控领域的拟态安全处理机架构。这些基于拟态防御构建的安全网络设备在测试中均取得了较好的效果。然而，拟态防御 Web 服务器和拟态防御路由器主要采用虚拟技术，其异构执行体主要在软件层面，底层处理器和操作系统仍为同构非冗余；而拟态安全处理机架构则主要从处理器层面实现了异构，对上层软件和操作系统仍采用同构形式。

在此基础上，本文构建了一种基于 CMD 技术、采用动态异构冗余机制的以太网交换机内生安全体系结构。与前述拟态安全网络设备相比，本文提出的体系结构从交换机的主控处理器、操作系统、协议栈和管理软件层面都实现了异构冗余，提出并采用自清洗大数表决算法（TAMA, trustiness based auto-cleanout majority algorithm）。测试结果表明，所提算法可有效抵御利用以太网交换机控制管理面未知漏洞和后门的攻击。

2　拟态防御交换机体系结构

2.1　DHR 典型结构

拟态防御技术的核心是动态异构冗余架构，其典型构造如图 1 所示[12]。其中，策略调度是中心控制环节，一方面，策略调度向策略分发环节下发指令，以实现激活执行体、执行体清洗修复或者执行其他给定的任务；另一方面，策略调度也是 DHR 架构中的反馈控制器，根据接收到的表决器异常状态按照预置策略执行相应动作。策略分发对应输入代理环节，主要功能是根据策略调度环节的指令决定是否将外部输入与当前服务集内的指定异构执行体联接，通常用一个路径和模式可定义的交换模块来具体完成互联分发功能。策略表决环节对应输出代理，主要功能是对多路执行体输出矢量采用一致性或多数判决策略，同时对出现的异常状态上报策略调度环节。异构体资源池是能够满足需求的所有异构行为体功能元素的集合。策略调度根据事先制定的重构重组方案从异构体资源池中抽取元素生成功能等价的新执行体，或者在现有的执行体中更换某些构件，生成或更新异构执行体集。

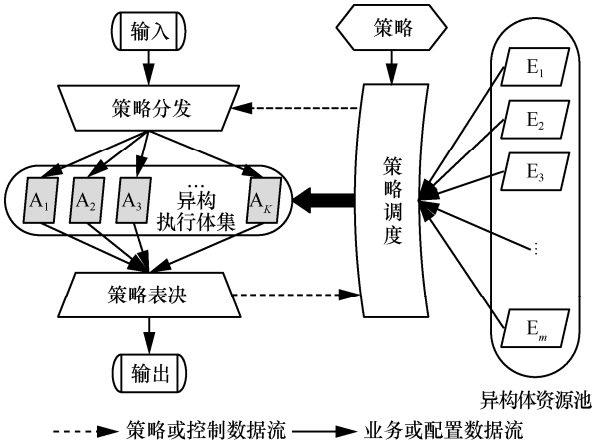

图 1　动态异构冗余典型结构

2.2　拟态防御以太网交换机体系结构

依据 DHR 的典型结构，本文设计的拟态防御以太网交换机体系结构如图 2 所示，主要由异构执

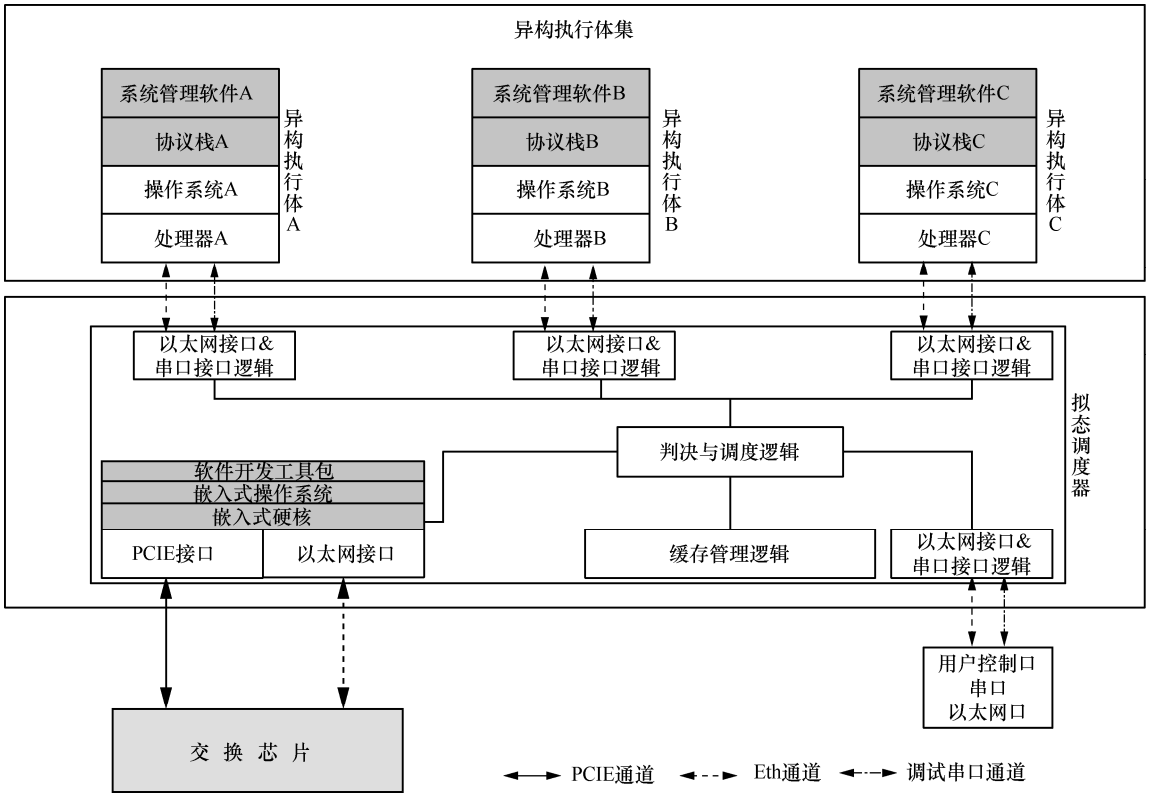

图 2　拟态防御以太网交换机体系结构

行体集、拟态调度器和交换芯片组成。

其中，异构执行体集由 3 个不同的异构执行体组成，每个执行体包含不同架构的 CPU，分别运行不同的操作系统及通过多样化编译生成的异构协议栈和管理软件。拟态调度器融合了 DHR 结构中的输入策略分发、策略表决输出及策略调度功能，是整个体系结构的核心控制环节。

拟态调度器与异构执行体之间通过以太网接口和串口连接；拟态调度器与交换芯片之间通过 PCIE（peripheral component interconnect express）接口及以太网接口连接；同时，拟态调度器与用户控制口和外部存储之间分别通过以太网、串口和存储控制接口连接。

2.3　拟态防御以太网交换机安全机理

基于拟态防御理论，依据图 2 构建的拟态防御以太网交换机（以下简称拟态交换机）的安全机理可描述如下。

1) 交换芯片上行的控制管理指令或协议解析数据通过透明传输通道，由调度器进行复制并分发输入异构执行体 A、B、C。

2) 异构执行体 A、B、C 独立响应并执行输入的指令或进行协议解析，结果分别输出到拟态调度器。

3) 拟态调度器将各异构执行体的输出数据进行分组解析、乱序处理、掩膜替代、哈希运算后，进行数据内容比对。

4) 正常情况下，异构执行体的输出数据应该是一致的，调度器将此结果正常输出到交换芯片。

5) 在面临差模攻击（即某一个执行体响应了攻击指令）时，遭受攻击的执行机输出数据与其他 2 个执行体不一致，调度器选择多数一致的正确数据输出，并对少数不一致的执行体进行清洗恢复处理。

6) 在协同或共模攻击时（即 2 个或 3 个执行体响应了攻击指令），各执行体的输出数据均不一致，或者多数一致的数据是错误数据，此时，系统将面临短时攻击逃逸，需要进行特殊处理。

通过上述分析，基于拟态交换机面临绝大多数的差模攻击场景时（由于各执行体的处理器架构、操作系统及执行软件都是同功异构的，绝大多数的攻击只会对其中一种执行体造成影响，因此差模攻击是交换机面临的主要攻击场景），通过调度器的择多判决，均能输出正确结果。而且，这种选择机制仅仅是根据输出结果的异同进行的，不关注到底是何种原因造成的结果不一致。无论是已知

的还是未知的安全威胁造成的输出不一致，该架构均能有效处理，不依赖病毒库、木马库、漏洞库等先验数据。因此，该架构可有效应对未知漏洞及后门造成的未知威胁。

当然，在小概率下也可能出现由于处理器架构、操作系统或执行软件的共同缺陷而引起的协同或共模攻击，这种攻击会引起攻击逃逸，这种逃逸最终会引起整个系统的故障。因此，为了实现系统的稳态可用，降低攻击逃逸概率，提高稳态非特异性感知概率，还需要采用合适的调度策略算法。

3　拟态交换机 TAMA

为了有效应对不同类型的攻击场景，特别是一些可能暂时不会引起输出异常的时间协同攻击，本文提出了基于可信度的 TAMA，在传统大数表决策略中增加了定时扰动机制，可有效解决各种协同及共模攻击。本节主要介绍 TAMA 的实现策略，并对其安全防御能力进行了量化分析。

3.1　TAMA

TAMA 在执行体出现不同结果时优先采用高优先级的执行体结果，执行体的信用度根据历史表现自动变化。该算法在大数裁决的基础上引入动态机制，使系统具有更多的不确定性，增大攻击实施难度、降低安全风险，但是会增加清洗次数、增大设计复杂度。

为了使系统在自清洗时能够保证正常运转，需要将系统分为执行队列和备选队列，执行队列中的执行体参与表决，备选队列中的执行体进行清洗，并在完成清洗后参与系统运算，以便能够随时加入系统。该算法主要由 2 种策略组成，具体如下。

1) 基于信任度的大数裁决策略

在系统开始运行时，将异构执行体赋予相等的信任权值，初始都为 0，本文设计的拟态交换机采用异构冗余三执行体，则$\omega_1=\omega_2=\omega_3=0$，判决算法将输出结果一致的执行体划分为一个组 G_k，构成集合序列$\{G_1, G_2, \cdots, G_k\}$，然后, 计算每个集合 G_k 的置信度 W_k 为

$$W_k=\sum_{i=1}^{k} \mathrm{e}^{-\omega_i} \tag{1}$$

其中，$\omega_k = G_k$。选取置信度最大的集合 G_p 作为输出结果，并根据输出结果的差异度进行信任权值的更新，每次进行判决时如果该执行体的输出结果与裁决输出结果不一致，则计算其和仲裁输出结果的差异率 S，并计算权值更新，如式(2)所示。

$$\omega_i = \beta S \omega_i \tag{2}$$

其中，$\beta > 0$ 为权值系数。同时，判断是否有执行体信任度大于阈值 K，如果有，则选择信任权值最高的进行清洗，若存在多个 K 值相同的执行体，则按照概率相等原则挑选一个进行清洗。

2) 定时清洗策略

网络攻击存在协同攻击方法，即先渗透攻击某个执行体，获取其权限，但是并不在输出中表现，接着渗透攻击其他的执行体，只有取得多数执行体权限后，才同时产生错误的输出结果。此外，虽然采用了异构执行体，但是很难保证异构执行体的完全异构，各个异构执行体之间不可避免地存在一些共同模块，如果这些共同模块存在的漏洞或后门被攻击利用，单纯根据输出进行裁决的拟态策略就无法有效防御。

为了有效防御协同或者共模攻击，需要执行体具有一定的自恢复能力，能够根据系统策略定期或者随机进行自恢复。在拟态交换机中，采用定时清洗策略，即设置定时器，达到固定时间间隔 T 则根据信任权值选取一个执行体进行清洗，信任权值为 ω_i 执行体的选取概率为 P，清洗过后执行体的信任权值恢复为 0。

$$P=\frac{\mathrm{e}^{-\omega_i}}{\sum_{i=1}^{j} j\mathrm{e}^{-\omega_i}} \tag{3}$$

3.2　算法效果及代价分析

一般而言，随着暴露给外界时间的增加，执行体运行时被攻击成功的概率也逐渐变大，安全性逐渐降低。假设函数 $p(t)$表示随时间推移当前时刻执行体的安全性（即未被成功攻破的概率），并且有

$$\lim_{p\to\infty} p(t) = 0 \tag{4}$$

式(4)表示当时间足够长时，系统肯定会被攻击成功。

同样地，可以认为存在一个函数 $q(t)$，表示在时刻 t 执行体处于清洗状态并且清洗成功的概率，可以用一个阶跃函数表示经过时间 M 执行体被清洗成功，清洗成功后其安全概率为 1，如式(5)所示。

$$q(t)=\begin{cases} 1, & t \geqslant M \\ p(t), & t < M \end{cases} \tag{5}$$

图 3 为 TAMA 抗攻击能力变迁曲线。执行体由于其自身存在的漏洞或后门，随着时间的推移，安全风险逐渐加大。如果不采用定时清洗策略，则其安全曲线如图 3（假设 $p(t)=\mathrm{e}^{-\frac{x}{50}}$，$M$=30）中曲线 2 所示，随着时间推移，抗攻击能力逐渐降低。而采用了定时清洗策略，可以对执行体进行定期清洗，使其状态恢复，安全风险降低，其抗攻击能力曲线如图 3 中曲线 3 所示。从图 3 中可以看出，TAMA 由于采用了定时清洗策略，随着时间推移，其安全性会在清洗后恢复，使其安全性一直都会维持一个较高的水平。非拟态交换机由于自身不可避免地存在后门和漏洞，所以如图 3 中曲线 1 所示，开始时即处于低安全等级状态，随着时间推移，假设没有采取补丁等安全措施，其安全风险会随着攻击试探急剧增加，使系统变得更加不可靠。

针对协同或者共模攻击，由于存在定时清洗策略，会对系统进行定期扰动，即使系统受到共模攻击，在执行体后进行清洗也会发现异常，通过一定的诊断即可使系统重新恢复正常。

TAMA 需要对执行体进行定时清洗。例如 3 个处理器都正常运作时，清洗一个正常运作的处理器会造成系统降级，并造成系统安全风险短期内突然跌落，如图 3 中曲线 3 出现的下端尖刺所示，并且定期清洗会加大清洗难度，增加系统设计风险。但是总体来说，定期清洗可以在较短时间内将抗攻击能力恢复到正常状态，并可以预防系统稳态安全降级，使拟态交换机整体处于高安全等级状态。

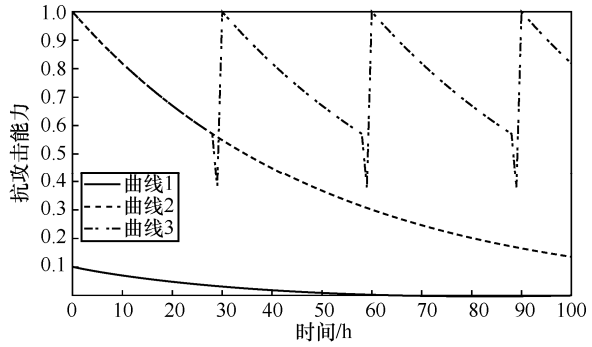

图 3　TAMA 抗攻击能力变迁曲线

4　拟态交换机设计实现与测试

4.1　拟态防交换机原理样机设计实现

本文依据拟态防御以太网交换机体系结构，设计实现了拟态交换机的原型样机。该拟态交换机采用盛科网络的 CTC5160 交换芯片，控制管理面包含 3 个异构处理模组和一个拟态调度器。其中异构处理模组 CPU 及操作系统如表 1 所示。拟态调度器由 Xilinx zynq-7045FPGA 实现，其内嵌的 ARM 处理器用于运行交换芯片的软件工具开发包（SDK, software development kit）。

表 1　　异构处理模组 CPU 及操作系统

异构处理模组	CPU	操作系统
A	Atom E3930	Ubuntu v16.04
B	QorIQ T1042	VxWorks v6.9
C	龙芯 2K-1000	Linus v3.10

CTC5160 交换芯片的上行数据通过 PCIE 通道交由拟态调度器进行透明复制分发到 3 个异构处理模组，由异构协议栈及管理软件进行协议处理；异构处理模组处理完成的数据经拟态调度器判决后交由 SDK 处理或直接下发交换芯片。

在拟态交换机中，由于所有上传主控的数据都要经过调度器，主控下发的数据要经过调度器的裁决，因此会造成系统处理时延的增加。根据对不同协议的测试统计，平均时延增加了 10 ms，普通协议如 RIP、OSPF 的时延都是秒级，因此在系统容许范围之内。

此外，拟态交换机构建的基于动态异构冗余的控制管理面，相对于常规的交换机需要新增 2 个主控 CPU 模组和一个调度器，在硬件实现成本上大概有 30%的提升。所以，该拟态交换机架构适合构建汇聚级或核心级的交换机，对于成本较敏感的接入级交换机不太适合。

4.2　基础协议解析功能测试

首先进行拟态交换机基础交换协议功能测试，选取以太网交换机的典型协议，测试在异构处理模组架构下是否能够正常进行协议解析及应答。常用的三层以太网交换机协议栈测试结果如表 2 所示。

4.3　白盒插桩安全测试

采用白盒插桩实验对拟态交换机的安全防御功能性进行测试，这是证明交换机具有拟态特性的核心测试内容。

拟态白盒插桩测试不是通过实际的漏洞或后门进行攻击，而是通过管理配置监测端配置各异构执行体，直接模拟并控制执行体的受攻击状态。不同的测试方式（差模、时间协同差模、N–1 模、共

表 2　三层以太网交换机常用协议栈测试结果

协议类别	协议名称及功能	测试结果
运维管理	syslog 功能	通过
	SNMP 功能	通过
	telnet 功能	通过
	SSH 功能	通过
	AAA 功能	通过
	带外管理功能	通过
二层功能	TRUNK 互联	通过
	STP 功能	通过
	MSTP 功能	通过
	STP 边缘端口功能	通过
	BPDU 保护功能	通过
	LLDP 功能	通过
	VLAN	通过
	单向链路检测	通过
	端口镜像	通过
	链路聚合	通过
	端口、MAC、IP 地址绑定	通过
	Dot1x 接入功能	通过
三层功能	静态路由	通过
	RIP 路由	通过
	OSPF 路由	通过
	VRRP	通过
	端口配置 IP 地址	通过
	ACL	通过

模）和不同的测试场景（应用程序、操作系统、协议等）对应不同的配置。配置完成后，通过数据输入端模拟输入流量（该输入流量也是针对具体测试场景定制的流量），在管理配置监测端对各异构执行体的输出数据进行监测，经过判决处理的数据通过数据输出端进行监测。拟态裁决采用 TAMA，其中权值系数 β=1，阈值 K=100。

1) 差模测试

差模测试方式是在各异构执行体上植入不同后门，使各异构执行体在输入相同时输出不同，且输出与正确结果不同。差模测试采用 2 种触发方式，分别如下所述。

触发方式 1，从管理配置监测端进行配置，一次触发一个异构执行体的攻击程序接口。这种触发测试方法即为常规的差模测试攻击。

触发方式 2，从管理配置监测端进行配置，一次性触发所有异构执行体的攻击程序接口。这种触发方式也称为时间协同差模攻击测试。

差模测试的测试结果如图 4 所示。

从测试结果可以看出，对于触发方式 1，从配置管理监测端观测到异常数据，但经过择多判决处理，异常数据并不能对拟态交换机正确执行任务产生任何影响。且经过一个清洗周期后，拟态交换机就能恢复正常工作状态。攻击逃逸概率为 0。对于触发方式 2，触发测试程序会导致拟态交换机出现瞬时攻击逃逸现象，但攻击逃逸现象会在周期 2 过

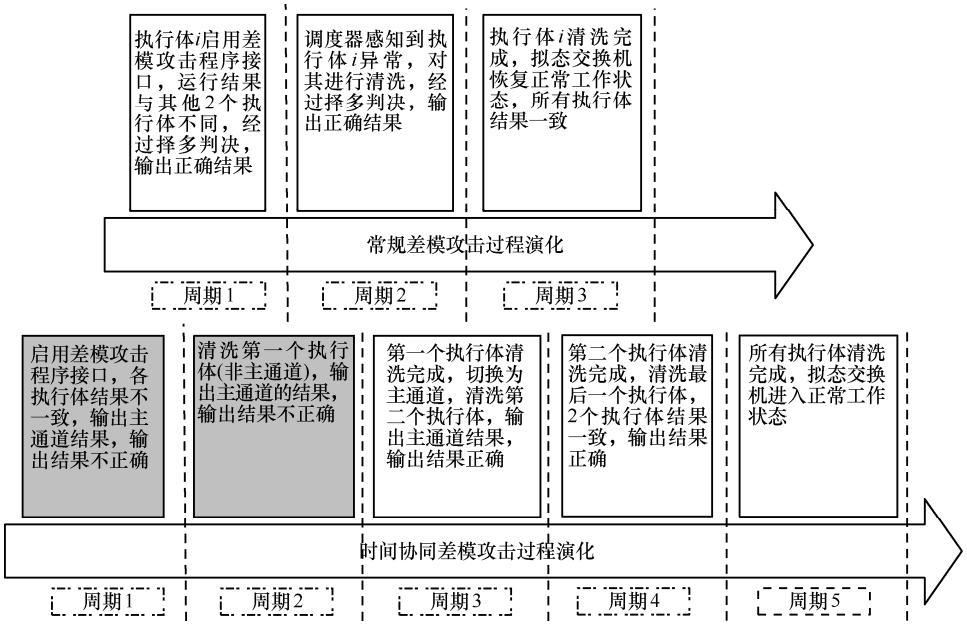

图 4　差模测试结果

后消失，且拟态交换机最终会恢复正常工作状态。

2) *N*–1 模测试

N 表示异构执行体的数量，在拟态交换机中采用了 3 个执行体，所以 *N*–1 模测试就是指 2 模测试。选取 2 个异构执行体插入后门，且插入的后门相同，使 2 个异构执行体在输入相同时，保证输出相同，且输出与正确结果不同。

2 模测试的测试结果如图 5 所示。从测试结果可以看出，测试期间会因为择多判决策略，导致拟态交换机出现瞬时攻击逃逸现象，但攻击逃逸现象会在周期 2 过后因后向验证机制的启动而消失，且最终恢复正常工作状态。

3) 共模测试

共模测试也称为 *N* 模测试，在拟态交换机中就是指 3 模测试，是在 3 个异构执行体上都插入相同的后门，使 3 个异构执行体在输入相同时保证输出相同，且输出与正确结果不同。

3 模测试的测试结果如图 6 所示。从测试结果可以看出，3 模测试启动后，拟态交换机会有一段时间对攻击行为无感，但随机扰动机制会随机选择执行体进行清洗，打破共模攻击所造成的无感状态，使攻击退化到 2 模状态，结合后向验证机制，拟态交换机也会在周期 2 过后开始输出正确的结果，并最终恢复正常工作状态。

从上述的测试结果可以看出，单个执行体受到攻击时，不会影响拟态交换机的运行结果；面对协同攻击或共模攻击，拟态交换机会出现短暂的攻击逃逸现象，但逃逸现象不能维持。在白盒插桩各种攻击测试模式下的逃逸概率及平均逃逸持续时间如表 3 所示，逃逸概率对比如图 7 所示。

表 3 白盒插桩攻击逃逸概率及平均逃逸持续时间

测试模式	瞬时逃逸概率	稳态逃逸概率	平均逃逸持续时间
常规差模测试	0	0	0
时间协同差模测试	1	0	错误识别时间+执行体清洗时间
2 模测试	1	0	错误识别时间+执行体清洗时间
3 模测试	1	0	$\frac{\text{扰动周期}}{2}$ + 执行体清洗时间

表 3 中，错误识别时间指从执行体开始输出错误结果，到其错误累积达到阈值、被调度器判定为状态异常所用的时间。

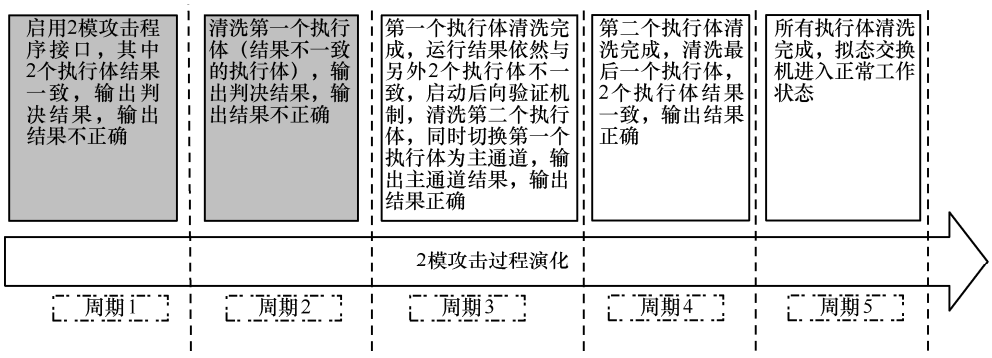

图 5 2 模测试结果

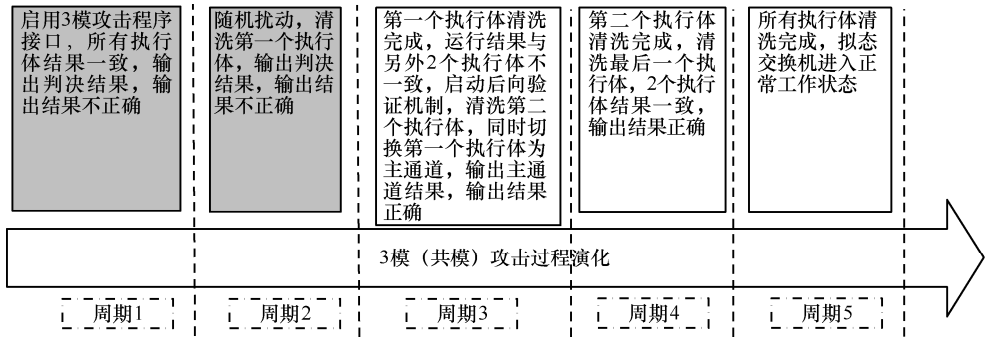

图 6 3 模测试结果

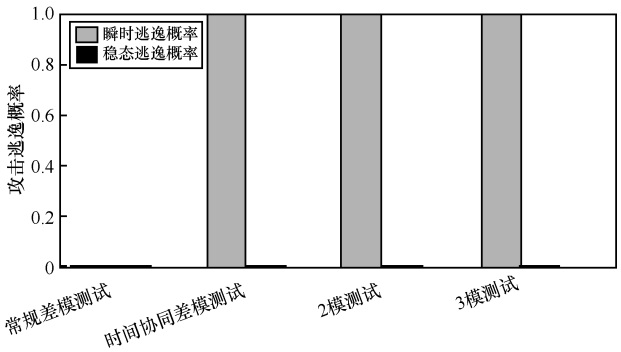

图 7　白盒插桩各攻击测试模式的逃逸概率

4.4　基于攻击链的交换机安全测试

4.3 节根据拟态防御理论，通过标准白盒插桩测试证明了交换机的拟态防御功能，本节从网络实际攻击角度来测试交换机的安全性。

实际网络攻击往往分为若干阶段，一般包括系统探测、漏洞发现、系统突破和系统控制等，交换机漏洞利用攻击链如图 8 所示。从拟态交换机的构造来说，白盒插桩测试也可以应用于交换机的不同层次，包括硬件层、操作系统层、应用软件层。在操作系统层，已知很多相关漏洞，可以找出不同内核版本的特异性或共性漏洞进行差模或者多模测试。协议层和应用层则更为灵活，可以编写插桩测试的应用程序编程接口（API, application programming interface），通过输入数据刺激插桩程序运行，进行插桩测试，观测交换机状态演化。

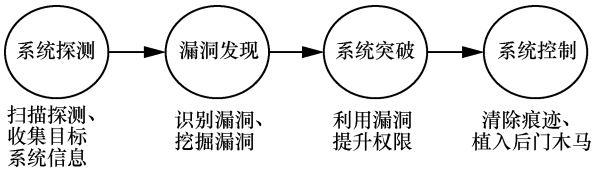

图 8　交换机漏洞利用攻击链

在系统信息探测阶段，首先关闭拟态系统，随机选择一个执行体执行，在调试机上通过 Nmap 扫描工具对交换机进行探测，观测是否可以得到操作系统、非授权开放端口及服务等信息；然后，开启拟态系统，进行相同步骤，观测是否可以得到操作系统、非授权开放端口及服务等信息。

在漏洞发现阶段，假设所有执行体都提供相同的服务，但服务的实现版本有所不同，其中一个执行体上的实现版本较低，或存在可以利用的漏洞。首先，开启拟态系统通过特定的漏洞扫描工具，观测能否通过统一接口，发现该版本的漏洞；然后，关闭拟态系统，观测能否发现该版本的漏洞。

在系统突破阶段，在执行体上采用白盒插桩方法模拟交换机漏洞，如思科旗下明星产品—Cisco Small Business 220 系列智能交换机 2019 年发现的 3 个高危漏洞，身份验证绕过（CVE-2019-1912，评级为致命，评分为 9.1）、远程命令执行（CVE-2019-1913，评级为致命，评分为 9.8）和命令注入（CVE-2019-1914，评级为中等，评分为 7.2）。首先，关闭拟态系统，观测能否利用这些漏洞；然后，打开拟态系统，多执行体同时执行，观测能否利用这些漏洞。

测试结果如表 4 所示。当关闭拟态系统时，攻击者很容易进行系统探测，一旦发现漏洞，进行突破和攻击的成功率就是 100%。而在拟态系统中，即使攻击者已知某执行体上存在漏洞，因为拟态机制的作用，攻击者通过漏洞触发的响应数据流是个体行为（针对同一个攻击漏洞输入仅有一个执行体进行响应），与其他执行体的响应行为不一致，因此无法通过裁决点，漏洞利用失败。而在攻击链的各个阶段都能有效屏蔽攻击行为，所以具有较高的抗攻击能力。

表 4　测试结果（拟态系统与单执行体结构对比）

测试内容	测试数量/个	拟态交换机攻击成功数/个	非拟态交换机攻击成功数/个
系统探测	15	0	10
漏洞发现	8	0	5
系统突破	5	0	5

5　结束语

本文针对以太网交换机面临的处理器、操作系统及协议栈存在的未知漏洞、后门等安全威胁，构建了一种基于动态异构冗余架构的拟态交换机体系结构，从系统架构层面使其具备内生安全特性。基于该体系结构，设计实现了拟态交换机原型样机，测试结果表明，该拟态交换机在正常处理各种交换协议的基础上，可以有效应对处理器、操作系统等层面的未知漏洞和未知后门安全威胁，具备十分理想的内生安全特性。

交换机的安全威胁主要存在于控制管理层面，但在数据转发层面，也就是交换芯片层面的安全威胁也必须予以重视。本文构建的拟态交换机采用国产交换芯片，虽然避免了采用国外芯片可能存在的

人为植入的设计后门风险，但是仍不能完全避免在设计、加工环节引入的未知漏洞和风险。因此，下一步的工作将会针对交换机数据转发平面的安全威胁，设计一种高安全以太网交换芯片系统架构，与本文提出的控制管理层拟态防御安全架构结合，构建一种全方位的交换机内生安全体系结构。

参考文献：

[1] 舒晓慧, 金小晰, 吴瑶. 网络交换机的安全威胁与防范[J]. 网络安全技术与应用, 2014(10): 130-131.
SHU X H, JIN X X, WU Y. Security treats and prevention of a network switch[J]. Network Security Technology & Application, 2014(10): 130-131.

[2] 武泽慧, 魏强, 任开磊, 等. 基于 OpenFlow 交换机洗牌的 DDoS 攻击动态防御方法[J]. 电子与信息学报, 2017, 39(2): 397-404.
WU Z H, WEI Q, REN K L, et al. Dynamic defense for DDoS attack using OpenFlow-based switch shuffling approach[J]. Journal of Electronics & Information Technology, 2017, 39(2): 397-404.

[3] YAN Q, YU F R, GONG Q, et al. Software-defined networking (SDN)and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622.

[4] ZHUANG R, DELOAC H, SCOTT A, et al. A model for analyzing the effect of moving target defenses on enterprise networks[C]// Proceedings of the 9th Annual Cyber and Information Security Research Conference. New York: ACM Press, 2014: 73-76.

[5] FENG X T, ZHENG Z Z, DERYA C, et al. A signaling game model for moving target defense[C]//IEEE INFOCOM 2017 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2017:1-4.

[6] ZAFFARANO K, TAYLOR J, HAMILTON S. A quantitative framework for moving target defense effectiveness evaluation[J]. Association for Computing Machinery, 2015(10): 3-11.

[7] 邬江兴. 拟态计算和拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 1-7.
WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7): 1-7.

[8] 扈红超, 陈福才, 王禛鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报, 2016, 1(4): 40-51.
HU H C, CHEN F C, WANG S P. Performance evaluations on DHR for cyberspace mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 40-51.

[9] 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, 28(4): 883-897.

[10] 马海龙, 伊鹏, 江逸茗, 等. 基于动态异构冗余机制的路由器拟态防御体系结构[J]. 信息安全学报, 2017, 2(1): 29-42.
MA H L, YI P, JIANG Y M, et al. Dynamic heterogeneous redundancy based router architecture with mimic defenses[J]. Journal of Cyber Security, 2017, 2(1): 29-42.

[11] 魏帅, 于洪, 顾泽宇, 等. 面向工控领域的拟态安全处理机架构[J]. 信息安全学报, 2017, 2(1): 54-74.
WEI S, YU H, GU Z Y, et al. Architecture of mimic security processor for industry control system[J]. Journal of Cyber Security, 2017, 2(1): 54-74.

[12] 邬江兴. 网络空间拟态防御导论[M]. 北京: 科学出版社, 2017.
WU J X. Introduction to cyberspace mimetic defense[M]. Beijing: Science Press, 2017.

[作者简介]

宋克（1976– ），男，河南许昌人，信息工程大学副研究员、博士生，主要研究方向为网络空间安全、计算机网络体系结构、集成电路设计技术。

刘勤让（1975–），男，河南商丘人，博士，信息工程大学研究员、博士生导师，主要研究方向为网络空间安全、软件定义互联、集成电路设计。

魏帅（1984– ），男，河南南阳人，博士，信息工程大学助理研究员，主要研究方向为计算机软件、网络体系结构。

张文建（1987– ），男，河南商丘人，信息工程大学助理研究员、博士生，主要研究方向为网络空间安全、通信与信息系统、集成电路设计。

谭力波（1981– ），男，内蒙古赤峰人，天津市滨海新区信息技术创新中心高级工程师，主要研究方向为网络空间安全、集成电路设计、软件定义互联。