一种面向安全的虚拟网络功能动态异构调度方法

季新生 徐水灵* 刘文彦 仝 青 李凌书
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：网络功能虚拟化(NFV)为服务链构建带来了灵活性与动态性，然而，软件化与虚拟化环境可能存在软件漏洞、后门等安全风险，对服务链(SC)的安全产生影响。为此，该文提出一种服务链上虚拟网络功能(VNF)调度方法。首先，为虚拟网络功能构建异构镜像池，避免利用共模漏洞的大范围攻击；随后，以特定周期选择服务链虚拟网络功能进行调度，加载异构镜像对该网络功能的执行实体进行替换；最后，考虑调度对网络功能性能的影响，应用斯坦科尔伯格博弈对攻防过程建模，以最优化防御者收益为目标求解服务链上各网络功能的调度概率。实验表明，该方法能够降低攻击者攻击成功率，同时将调度产生的开销控制在可接受范围内。

关键词：网络功能虚拟化；服务链；网络安全；动态；异构；博弈论
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)10-2435-07
DOI: 10.11999/JEIT181130

A Security-oriented Dynamic and Heterogeneous Scheduling Method for Virtual Network Function

JI Xinsheng XU Shuiling LIU Wenyan TONG Qing LI Lingshu
(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: Network Function Virtualization (NFV) brings flexibility and dynamics to the construction of service chain. However, the software and virtualization may cause security risks such as vulnerabilities and backdoors, which may have impact on Service Chain (SC) security. Thus, a Virtual Network Function (VNF) scheduling method is proposed. Firstly, heterogeneous images are built for every virtual network function in service chain, avoiding widespread attacks using common vulnerabilities. Then, one network function is selected dynamically and periodically. The executor of this network function is replaced by loading heterogeneous images. Finally, considering the impact of scheduling on the performance of network functions, Stackelberg game is used to model the attack and defense process, and the scheduling probability of each network function in the service chain is solved with the goal of optimizing the defender's benefit. Experiments show that this method can reduce the rate of attacker's success while controlling the overhead generated by the scheduling within an acceptable range.

Key words: Network Function Virtualization(NFV); Service Chain (SC); Cyber security; Dynamic; Heterogeneous; Game theory

1 引言

网络服务的实现需要一组特殊的网络功能，如服务网关(Serving GateWay, S-GW)、分组数据网关(Packet data network GateWay, P-GW)等。网络功能之间的有序组合与相互链接形成服务功能链(Service Function Chain, SFC)，简称服务链(Service Chain, SC)，为用户提供端到端服务。在通信网的云环境下，网络功能虚拟化(Network Function Virtualization, NFV)[1]技术将网络功能与专用硬件设备解耦，通过软件编程实现的虚拟网络功能(Virtualized Network Function, VNF)具有灵活性与可扩展性的优点，利用NFV技术进行服务链的构建已经成为趋势[2,3]。然而，软件化与虚拟化的环境也带来了诸如软件漏洞、后门安插等一系列安全问题，使VNF相对于传统的中间件设备更容易遭受攻击者的攻击[4–6]。

在针对服务链的研究中，服务链的可靠性是一

收稿日期：2018-12-06；改回日期：2019-04-03；网络出版：2019-04-23
*通信作者： 徐水灵 slxuuu@163.com
基金项目：国家自然科学基金(61521003, 61602509)，国家重点研发计划项目(2016YFB0800100, 2016YFB0800101)
Foundation Items: The National Natural Science Foundation of China (61521003, 61602509), The National Key R&D Program of China (2016YFB0800100, 2016YFB0800101)

项重要的研究内容，主要关注物理服务器失效情况下的弹性服务，现有保证服务链可靠性的方法可分为两类：(1)故障发生后进行链路重映射的修复机制；(2)故障发生前的备份机制[7,8] 。然而，目前对服务链可靠性的研究缺少对攻击行为的考虑，据总结，缺少对VNF的控制与监控、底层物理资源的共享等都是NFV面对的安全威胁[5]，使用传统的安全规则比对方式进行防御[9]或使用可信平台模块构造可信的计算环境[10]都是已有的解决方案。但是，NFV环境下安全规则制定更加复杂且防御攻击类型有限；可信平台模块的部署需要使用的专用硬件，不利于NFV服务链的跨数据中心实现。文献[11]提出通过构建多样化的系统环境，对环境切换进行动态切换以提高系统的入侵容忍能力，而VNF的快速加载与调度的能力为其多样化动态部署提供了良好的条件。因此，为保障NFV服务链的安全，本文提出一种针对NFV服务链VNF节点的动态异构式调度方法，为服务链上的VNF节点构建异构镜像资源池以降低共模漏洞出现的概率，利用管理与编排层对执行实体进行动态异构式调度以降低漏洞的暴露时间，两者结合以提高攻击者的攻击难度。

2 模型设计及安全性分析

2.1 NFV服务链威胁模型

漏洞的不可预知性与必然性使服务链中任一VNF都存在被攻击的风险，图1显示了一种基于漏洞的攻击场景，攻击者利用软件漏洞构造恶意数据包发送给正在提供服务的VNF, VNF拆解后出现服务异常。

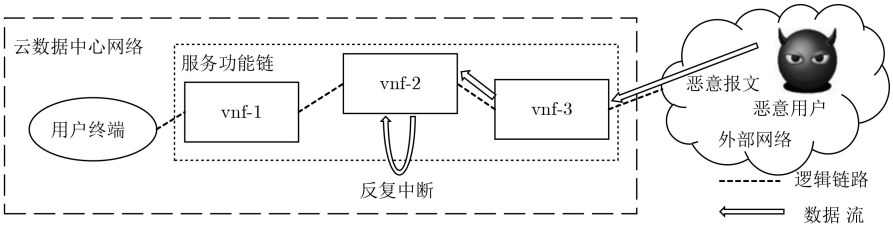

图 1 服务链攻击实例

对攻击者而言，可直接执行攻击指令造成VNF节点服务中断，通过镜像对VNF进行重新加载并部署是常见的故障恢复方法，然而在漏洞被修复之前，网络提供者无法杜绝相同攻击行为的再次发生。更普遍地，攻击者攻克一个节点之后，可将VNF节点作为攻击据点，进行持续性的信息窃取，或伺机对服务链上其它节点进行攻击[12]。

据以上分析，攻击者能够通过挖掘软件漏洞，对服务链任意节点展开攻击，这种攻击可以是重复的、大范围的，也可以是持续的、隐蔽的，而攻击者对服务链中任意VNF节点的攻克，由于破坏了正常的用户数据流，会对整条服务链的正常业务产生影响。此时，单独对某个VNF进行安全防护不足以维护整条服务链的安全性，维护服务链的安全需要从服务链整体上进行考虑，对服务链上VNF节点进行安全性的协调联动。如何从整条服务链的角度对VNF节点进行防护，应对攻击者重复的或潜伏式的攻击，是保障服务链安全的关键问题。

2.2 动态异构式服务链节点调度模型

为解决服务链上VNF节点的防护问题，本节利用移动目标防御中多样性与动态性的思想，提出一种动态异构式的服务链VNF节点调度策略。设计模型如图2所示：在欧洲电信标准化协会(European Telecommunications Standards Insti-

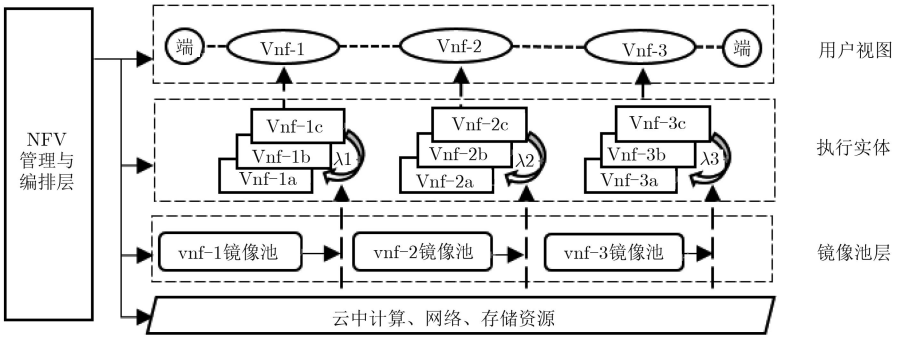

图 2 动态异构式服务链模型举例

tute, ETSI)标准架构的基础上构建异构的VNF镜像资源池，管理与编排层进行服务链的编排,选择VNF执行实体上线服务并以特定周期实施调度策略——随机挑选网络功能并对该网络功能的VNF执行实体进行异构替换。

(1) 服务链异构资源池表示

异构资源池用于VNF执行实体的异构式重新加载。假设串联服务链S由n个虚拟网络功能组成，记作$S=(S_1,S_2,\cdots,S_n)$，对于虚拟网络功能S_i，实现网络功能并在服务链上服务的实体称为该虚拟网络功能的执行实体。选择p个方面的特征对执行实体进行抽象，如服务端口、应用编程语言、操作系统版本、hypervisor类型等，表征为p元特征$(f_1,f_2,\cdots,f_p)$，若两个VNF执行实体的特征向量表示相同则称这两个执行实体同构，否则异构。为服务链上第i个VNF准备m_i个异构执行实体镜像，称作该VNF的异构资源池。

(2) 服务链资源池异构度表示

异构镜像资源池构建完成后，VNF镜像资源池的异构度成为该VNF的重要特征之一。目前，已有多种方式可以度量系统间的差异，如基于系统熵[13]的度量方法、基于共模漏洞[14]的度量方法等。为体现VNF执行实体的虚拟化层次结构，在p元特征上对资源池中的执行实体进行异构度度量，每两个异构执行实体(设为k与l)间的差异表示为$\left(d_{i1}^{kl},d_{i2}^{kl},\cdots,d_{ip}^{kl}\right)$，则资源池异构度可表示为$m_i\times m_i$对称矩阵$\boldsymbol{D}_i$，取矩阵均值为资源池异构度，表示为$\overline{D}_i=\left(\overline{d}_{i1},\overline{d}_{i2},\cdots,\overline{d}_{ip}\right)$。最终服务链的异构度可表示为$\boldsymbol{D}=\left(\overline{D}_1,\overline{D}_2,\cdots,\overline{D}_n\right)$。

(3) 服务链调度策略表示

服务链调度策略具有两层含义：(a)为防止重复攻击，在VNF发生异常时从异构资源池中选择异构镜像进行服务链的重构；(b)为防止潜伏式信息窃取，在未监测到运行异常时，以时间T为周期，每周期编排层以$\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_n)$为概率从服务链$S$中选择VNF节点进行调度，记为选择调度概率。在选定节点后，从该节点资源池中随机选择镜像并加载执行实体对正在服务的执行实体进行替换，实现服务链上VNF节点的动态调度。

相比云环境下虚拟机调度，VNF具有较高的性能需求，如包处理速率、网络时延等，盲目选择节点进行调度无疑会产生较大切换开销。因此，如何在服务链安全性与服务链性能需求之间进行平衡是需要解决的问题，在本节提出的调度模型的基础上，构建服务链的安全评估模型，对节点调度的周期、不同网络功能的选择调度概率优化是新研究重点。

2.3 基于博弈论的选择调度概率优化

为对选择调度概率进行优化，在服务链节点调度选择过程中应用斯坦科尔伯格博弈。斯坦科尔伯格博弈模型是一种非合作博弈模型，可将动态调度服务链节点的服务链编排层(防御者)看作领导者，将攻击者看作追随者。服务链编排层对节点随机调度的过程可以看防御者的混合策略。攻击者对服务链上VNF节点的攻击可看作追随者的策略，而由于攻击者可能存在多种类型，即博弈中的可能出现多个追随者，将博弈模型扩展为贝叶斯-斯坦科尔伯格博弈[15]进行求解。

对防御者与攻击者做出如下假设：

(1) 假设攻击者针对单条服务链中的网络功能实施攻击。暂不考虑针对物理层、编排层的攻击情况。

(2) 假设存在q组独立攻击者，每组攻击者对漏洞利用的能力一定，攻击者具有的能力用双元组$C=(\alpha,\beta)$表示，α是攻击者能力在系统特征上的映射，为p元组合变量$(\alpha_1,\alpha_2,\cdots,\alpha_p)$，$\forall i\in[1,p]$，$0\le\alpha_i\le1$，向量中每一项数值与攻击者在该特征上的能力正相关；β是攻击者能力在时间上的映射，假设攻击者完成攻击所需要时间为t，系统调度周期为T，定义$\beta=\lfloor t/T\rfloor$，若系统保持静态，攻击者会在第$\beta+1$时隙攻克执行实体。

(3) 防御者可根据经验推断出攻击者能力，攻击者可以通过多次嗅探推断出调度概率λ与资源池异构度D。因此假设，(α,β), λ, D对于双方是共同知识。

基于以上假设，将博弈模型定义为3元组$G(M,A,U)$，其中

(1) $G=\{\varnothing,G_1,G_2,\cdots,G_n\}$，是防御者的策略集合，表示攻击者的可调度服务链上的任一网络功能节点，或不对任何节点进行调度。

(2) $A=\{\varnothing,A_1,A_2,\cdots,A_n\}$，是攻击者的策略集合，表示攻击者可以选择任意节点进行攻击，或不对任何节点进行攻击。

(3) $U=(U_{\mathrm{D}},U_{\mathrm{A}})$为攻防双方的收益函数，$U_{\mathrm{D}}$为防御者的收益，$U_{\mathrm{A}}$为攻击者的收益。对双方收益函数的推论如下。

对于第k组攻击者，其能力为双元组$\left(\alpha^k,\beta\right)$，定义一轮博弈时长为攻击者所需的攻击时长$t$，则在一轮博弈中攻击者的期望收益可写为$U_A^k\left(\lambda,y^k\right)$。

$$U_A^k\left(\lambda,y^k\right)=\sum_{i\in[1,n]}\left(U_{Ai}^k\left(\lambda_i\right)-\mathrm{c_a}\right)\cdot y_i^k,$$

$$y_i^k=\begin{cases}0, & \text{不攻击节点}S_i\\ 1, & \text{攻击节点}S_i\end{cases}\tag{1}$$

其中，函数 $U_{Ai}^{k}(\lambda_i)$ 为攻击者攻击网络功能节点 S_i 的期望成功率，与节点调度概率 λ 有关；y_i^k 为0～1整形变量，指示攻击者是否对服务链节点 S_i 发动攻击，y^k 为第 k 组攻击者对服务链上节点的决策集合；c_a 为常数，表示攻击者发动攻击的固有开销。

假设攻击者拥有有限的攻击资源，攻击者能够对服务链上 $m^k(m^k \le n)$ 个VNF同时进行攻击，攻击者策略约束为

$$\sum_{i\in[1,n]} y_i^k \le m^k,\ y_i^k \in \{0,1\} \tag{2}$$

攻击者可根据节点调度概率 λ_i 推算出 S_i 的攻击成功率 $U_{Ai}^{k}(\lambda_i)$。假设攻击者对 p 元特征上每一特征的成功攻击都可看作攻破该VNF，若该VNF节点在 $\beta+1$ 个时隙内没有进行执行体的异构调度，攻击成功率为 $P_{\mathrm{st}}^{k}=\left(1-\prod_{j=1}^{p}\left(1-\alpha_j^k\right)\right)$；若进行1次调度，攻击者使用调度前攻击方式攻破新执行体的概率与前后执行体的异构度有关，攻击成功率为 $P_{\mathrm{dy}}^{k}=\left(1-\prod_{j=1}^{p}\left(1-\alpha_j^k\cdot\left(1-\overline{d}_{ij}\right)\right)\right)$。因此，$\beta+1$ 个时隙内攻击成功率 $U_{Ai}^{k}(\lambda_i)$ 可写为

$$\begin{aligned}U_{Ai}^{k}(\lambda_i)=&\left(1-\prod_{j=1}^{p}\left(1-\alpha_j^k\right)\right)\cdot(1-\lambda_i)^{\beta}\\&+C_\beta^1\cdot P\cdot\lambda_i(1-\lambda_i)^{\beta-1}\\&+C_\beta^2\cdot(P\cdot\lambda_i)^2\cdot(1-\lambda_i)^{\beta-2}\\&+\cdots+C_\beta^\beta\cdot(P\cdot\lambda_i)^\beta\end{aligned} \tag{3}$$

$$\begin{aligned}P=&\left(1-\prod_{j=1}^{p}\left(1-\alpha_j^k\cdot\left(1-\overline{d_{ij}}\right)\right)\right)\\=&\left(1-\prod_{j=1}^{p}\left(1-\alpha_j^k\cdot\left(1-\overline{d_{ij}}\right)\right)\cdot\lambda_i\right)^{\beta}\\&-\prod_{j=1}^{p}\left(1-\alpha_j^k\right)\cdot(1-\lambda_i)^{\beta}\end{aligned} \tag{4}$$

防御者收益由攻击开销与执行实体调度开销组成。其中，攻击开销由 q 组攻击者共同产生，且与攻击成功率负相关，为简化参数设置系数为1。执行体调度的期望开销为各资源池执行实体切换开销以调度概率 λ 的加权平均，由异构特征共同产生。因此，一轮博弈中防御者收益期望值为 $-\beta\sum_{i=1}^{n}\sum_{j=1}^{p}\lambda_i\overline{d_{ij}}$。设置调整系数 c_d，c_d 越小表示当前调度成本越小，或用户对网络安全的重视程度越高。

则 $U_D(\lambda,y)$ 可写为

$$\begin{aligned}U_D(\lambda,y)=&-\sum_{k=1}^{q}\sum_{i=1}^{n}\left(U_{Ai}^{k}(\lambda_i)\right)\cdot y_i^k\\&-c_d\cdot\beta\sum_{i=1}^{n}\sum_{j=1}^{p}\lambda_i\overline{d}_{ij}\end{aligned} \tag{5}$$

防御者策略约束

$$\forall i\in[1,n],\lambda_i\in[0,1],0\le\sum_{i=1}^{n}\lambda_i\le 1 \tag{6}$$

至此，通过博弈建模，可将管理与编排层对服务链节点的调度问题转化为混合整数非线性规划问题，在攻击者会选择最大化自身收益的策略情况下防御者的目标为最小化自身开销，求解目标函数下的 λ 即为防御者的最优调度概率。目标函数及约束条件为

$$\left.\begin{aligned}\min_{\lambda}\ &\left(\max_{y}\left(\sum_{k=1}^{q}\sum_{i=1}^{n}\left(U_{Ai}^{k}(\lambda_i)\right)\cdot y_i^k\right)\right.\\&\left.+c_d\cdot\beta\sum_{i=1}^{n}\sum_{j=1}^{p}\lambda_i\overline{d_{ij}}\right)\\\text{s.t.}\quad&\forall i\in[1,n],\lambda_i\in[0,1],0\le\sum_{i=1}^{n}\lambda_i\le 1\\&\forall k\in[1,q],\forall i\in[1,n],y_i^k\in\{0,1\}\\&\forall k\in[1,q],\sum_{i=1}^{n}y_i^k\le m^k\end{aligned}\right\} \tag{7}$$

3 实验分析及讨论

直接求解式(7)较为困难，本次实验使用CPLEX优化软件求解，其它通过matlab编程实现。由于防御者的收益非正，使用防御者收益的绝对值作图，记为防御者的开销。本次仿真考虑了具有3个VNF的服务链，选取两个特征对执行实体进行抽象。

3.1 动态异构调度安全增益测试

首先考虑只存在1组攻击者，且攻击者仅可同时对服务链中1个网络功能进行攻击的情况，设计两种系统，一种为动态跳变策略NFV服务链系统，服务链上网络功能节点选择概率为均匀分布，一种为完全静态NFV服务链系统，即VNF执行实体部署后不会主动跳变。假设 $\boldsymbol{D}=(\langle 0.2,0.8\rangle,\langle 0.5,0.5\rangle,\langle 0.8,0.2\rangle)$，$c_a=0.01$，$c_d=0.01$，$\beta=2$，改变攻击者能力 α 均值与 α 在不同特征上的分布，测试动态跳变策略对攻击者攻击成功率的影响。

图3显示，攻击成功概率随攻击者能力均值的提升而随之上升，动态跳变策略能够降低攻击成功

率，提升系统安全性。同时如图4所示，动态调度策略带来的开销较小。

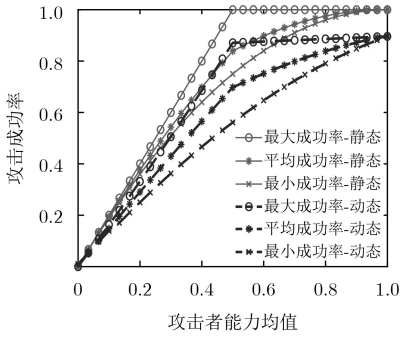

图 3 静态系统与动态系统攻击成功率对比

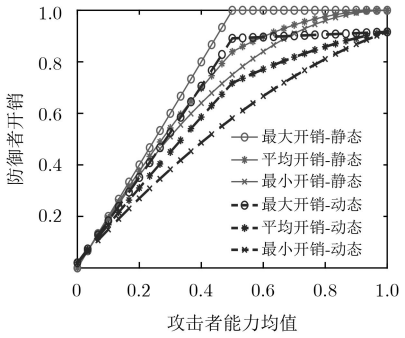

图 4 静态系统与动态系统防御者开销对比

3.2 最优化选择调度安全增益测试

同样仅考虑只存在1组攻击者，设计两种系统都使用动态异构式调度，而第1种服务链系统使用纯随机算法选择VNF进行调度，另一种使用基于博弈论的节点调度选择方法计算各节点的调度概率。其余设置同上，改变攻击者能力，对比攻击者攻击成功率、系统总开销。

结果如图5、图6显示，在防御者开销方面，最优化选择调度的开销相对随机调度节点选择策略进一步降低；在攻击成功率方面，在攻击者能力均值相同但不同分布情况下，基于博弈论的节点选择策略可将攻击成功率控制在一定范围内。

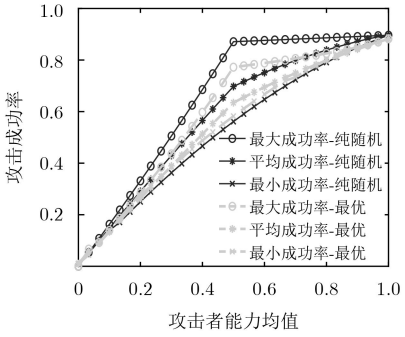

图 5 纯随机调度与最优化选择调度防御者开销对比

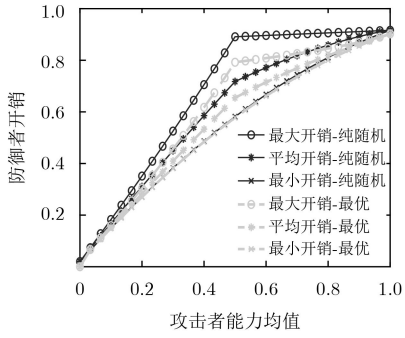

图 6 纯随机调度与最优化选择调度攻击成功率对比

3.3 多攻击者安全增益测试

为获得多攻击者条件下的安全增益，在不同攻击者数量p与不同攻击者最大攻击VNF数量m情况下，分别计算使用纯随机方法调度的系统与使用最优节点调度方法的系统相对静态系统的防御者收益增益，并与只存在1组攻击者且攻击者仅可对服务链中1个网络功能进行攻击的攻击场景下对比，其余设置不改变，结果如图7所示。对比结果显示，在多攻击者条件下调度策略能够取得更加明显的安全增益。

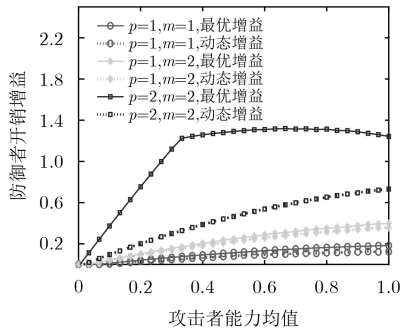

图 7 多攻击者安全增益对比

3.4 参数分析

3.4.1 VNF节点资源池异构度对防御效果的影响

首先测试异构度在服务链上的不同分布对防御效果的影响，为获得不同异构度分布进行3次实验，设置3节点服务链的初始异构度$\boldsymbol{D}=(\langle 0.1,0.1\rangle,\langle 0.1,0.1\rangle,\langle 0.1,0.1\rangle)$，每次实验分别对3节点上1个、2个、3个节点的异构度进行提升，观察攻击者成功概率与防御者开销。其余参数设置$\alpha=(0.9,0.9)$，$\beta=2$，$c_a=0.01$，$c_d=0.01$。

3次实验结果如图8所示：随着VNF节点资源池异构度均值的提升，攻击者攻击成功率与防御者开销随之下降，然而仅对3节点服务链上一两个节点进行异构度提升，攻击成功率与防御者开销下降不到5%，而同时服务链上所有节点进行异构度的提升使攻击成功率与系统开销下降近50%。

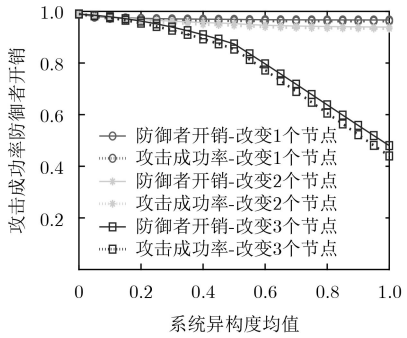

图 8 服务链整体异构度对防御者开销/攻击成功率影响

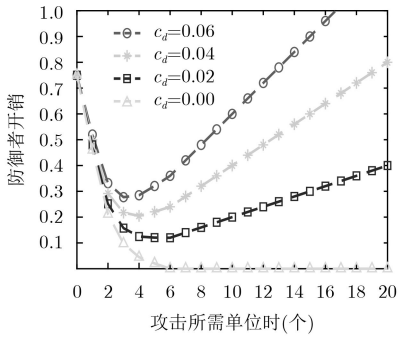

图 10 调度周期对防御者开销影响

随后测试服务链上节点异构度对其被选择调度概率的影响。实验设置服务链上两节点S_1, S_2异构度相同，改变节点的S_3资源池异构度均值。其余参数与前一实验相同，使用基于博弈论的节点调度选择方法计算选择概率。

在S_1, S_2异构度D_1, D_2分别为$\langle 0.3, 0.3\rangle$, $\langle 0.5, 0.5\rangle$, $\langle 0.8, 0.8\rangle$时，节点S_3被选择调度的概率如图9所示：随着节点异构度的提升节点被选择调度的概率下降，在异构度均值接近其余两节点异构度时，选择调度的概率接近1/3。

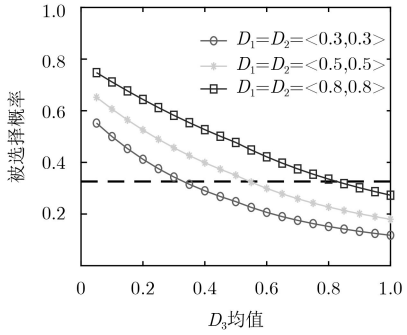

图 9 节点异构度对节点被选概率影响

3.4.2 服务链调度周期对防御效果的影响

为测试服务链调度周期T对防御效果的影响，假设攻击所需时间为t，服务链整体异构度$\boldsymbol{D}=(\langle 0.2, 0.8\rangle, \langle 0.5, 0.5\rangle, \langle 0.8, 0.2\rangle)$，攻击者$\alpha$=(0.5, 0.5), c_a= 0.01，在调整系数c_d分别为0, 0.02, 0.04, 0.06情况下，观察攻击成功率与防御者开销。

结果如图10所示：调整系数c_d= 0时，防御者开销仅由攻击产生，攻击成功率随调度周期的缩短而单调递减并趋近于0。$c_d \neq 0$时，防御者开销随调度周期的缩短先减小后增大，且c_d越大拐点出现越早，后续开销增大的速率越大，存在$\beta = \lfloor t/T \rfloor$使防御者开销最小。

4 结束语

本文围绕NFV服务链安全性进行研究，对NFV服务链中的攻击场景进行了分析，为防止重复攻击与潜伏式攻击，为服务链上VNF构建了异构镜像池并提出了一种动态异构式的调度方法以增强NFV服务链整体的安全性；为平衡调度策略产生的开销，将NFV服务链中的攻防过程建模为斯坦科尔伯格博弈模型，对服务链调度策略进行了优化。最终实验结果表明，动态异构式VNF调度策略能够增强系统安全性，同时将系统开销控制在一定范围之内。

参 考 文 献

[1] Network Functions Virtualization (NFV) ETSI Industry Specification Group (ISG). ETSI GS NFV 001: Network Functions Virtualisation (NFV); Use cases[EB/OL]. https://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf, 2013.

[2] MEDHAT A M, TALEB T, ELMANGOUSH A, *et al*. Service function chaining in next generation networks: state of the art and research challenges[J]. *IEEE Communications Magazine*, 2017, 55(2): 216–223. doi: 10.1109/MCOM.2016.1600219RP.

[3] SAHHAF S, TAVERNIER W, COLLE D, *et al*. Network service chaining with efficient network function mapping based on service decompositions[C]. The 1st IEEE Conference on Network Softwarization, London, UK, 2015: 1–5. doi: 10.1109/NETSOFT.2015.7116126.

[4] Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG). ETSI GS NFV-SEC 001: Network Functions Virtualisation (NFV); NFV security; Problem statement[EB/OL]. https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf, 2014.

[5] LAL S, TALEB T, and DUTTA A. NFV: Security threats and best practices[J]. *IEEE Communications Magazine*, 2017, 55(8): 211–217. doi: 10.1109/MCOM.2017.1600899.

[6] FIROOZJAEI M D, JEONG J, KO H, *et al*. Security challenges with network functions virtualization[J]. *Future Generation Computer Systems*, 2017, 67: 315–324. doi: 10.1016/j.future.2016.07.002.

[7] DING Weiran, YU Hongfang, and LUO Shouxi. Enhancing

the reliability of services in NFV with the cost-efficient redundancy scheme[C]. IEEE International Conference on Communications, Paris, France, 2017: 1–6. doi: 10.1109/ICC.2017.7996840.

[8] CARPIO F, JUKAN A, and PRIES R. Balancing the migration of virtual network functions with replications in data centers[C]. The 16th IEEE/IFIP Network Operations and Management Symposium, Taipei, China, 2018: 1–8.

[9] PATTARANANTAKUL M, HE R, MEDDAHI A, *et al*. SecMANO: Towards Network Functions Virtualization (NFV) based security management and orchestration[C]. 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 2016: 598–605. doi: 10.1109/TrustCom.2016.0115.

[10] ZHENG Yan, ZHANG Peng, and VASILAKOS A V. A security and trust framework for virtualized networks and software - defined networking[J]. *Security and Communication Networks*, 2016, 9(16): 3059–3069. doi: 10.1002/sec.1243.

[11] GUO Minzhe and BHATTACHARYA P. Diverse virtual replicas for improving intrusion tolerance in cloud[C]. The 9th Annual Cyber and Information Security Research Conference, Oak Ridge, USA, 2014: 41–44. doi: 10.1145/2602087.2602116.

[12] LI F, LAI A, and DDL D. Evidence of advanced persistent threat: a case study of malware for political espionage[C]. The 6th International Conference on Malicious and Unwanted Software, Fajardo, USA, 2011: 102–109. doi: 10.1109/MALWARE.2011.6112333.

[13] MA Duohe, WANG Liming, LEI Cheng, *et al*. Quantitative security assessment method based on entropy for moving target defense[C]. The 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, 2017: 9204–922. doi: 10.1145/3052973.3055161.

[14] GARCIA M, BESSANI A, GASHI I, *et al*. Analysis of operating system diversity for intrusion tolerance[J]. *Journal of Research and Practice in Information Technology*, 2014, 44(6): 735–770. doi: 10.1002/spe.2180.

[15] PARUCHURI P, PEARCE J P, MARECKI J, *et al*. Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games[C]. The 7th International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 2, Estoril, Portugal, 2008: 895–902.

季新生：男，1964年生，教授，博士生导师，研究方向为网络空间安全、拟态安全等.

徐水灵：女，1995年生，硕士生，研究方向为网络主动防御技术、NFV安全.

刘文彦：男，1986年生，博士，研究方向为网络空间安全、云安全.

仝　青：女，1992年生，博士，研究方向为网络空间安全防御技术、主动防御技术.

李凌书：男，1992年生，博士，研究方向为拟态防御技术、主动防御技术.