

基于异构备份与重映射的服务功能链部署方案

谢记超¹, 伊鹏¹, 张震¹, 张传浩^{1,2}, 谷允捷¹

(1. 国家数字交换系统工程技术研究中心, 河南 郑州 450002;

2. 铁道警察学院公安技术系, 河南 郑州 450053)

摘要: 网络功能虚拟化技术提高了服务功能链部署的灵活性, 然而虚拟网络功能面临着不确定失效和恶意攻击问题, 现有的冗余备份部署方法能在一定程度上解决虚拟网络功能的失效问题, 但未考虑节点同构性在面临恶意攻击时的缺陷。为此提出一种考虑节点异构性的部署方法, 在进行冗余备份和重映射时保证节点的异构性。实验表明, 相比于同构备份方法, 所提方法在请求接受率下降 3.8%, 带宽消耗增加 9.2% 的情况下, 显著提高了攻击者的攻击时间成本。

关键词: 网络功能虚拟化; 服务功能链; 虚拟网络功能; 可靠性; 备份; 同构性; 异构性

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018051

Service function chain deployment scheme based on heterogeneous backup and remapping

XIE Jichao¹, YI Peng¹, ZHANG Zhen¹, ZHANG Chuanhao^{1,2}, GU Yunjie¹

1. National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China

2. Public Security Technology Department, Rail Police College, Zhengzhou 450053, China

Abstract: Network function virtualization technology improves the flexibility of service function chains' deployment. However, the virtual network functions are under the pressure of uncertain failures and malicious attacks. The existing redundant backup methods can solve the problem of VNF failures to some extent, it does not consider the defects of node homogeneity in the face of malicious attacks. A deployment method considering the heterogeneity of nodes was proposed, guaranteeing the heterogeneity of nodes when perform redundant backup and remapping. Simulation experiments demonstrate that the proposed method significantly increases attacker's attack time cost under the cost of the request acceptance rate decreases by 3.8% and the bandwidth consumption increase by 9.2% comparing to the homogeneity backup method.

Key words: NFV, SFC, VNF, reliability, backup, homogeneity, heterogeneity

收稿日期: 2018-04-17; 修回日期: 2018-05-26

通信作者: 谢记超, 912104210329@njust.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2016YFB0801200, No.2017YFB0801200); 国家网络空间安全专项基金资助项目 (No.2017YFB0803204); 公安部科技计划基金资助项目 (No.2017JSYJC08)

Foundation Items: The National Key Research and Development Project of China (No.2016YFB0801200, No.2017YFB0801200), The National Cyberspace Security Special Project of China (No.2017YFB0803204), The Ministry of Public Security Science and Technology General Project of China (No.2017JSYJC08)

1 引言

一般的网络服务都需要其流量经过一系列特定顺序的网络功能(NF, network function)处理,这些有序的网络功能序列被称为服务功能链(SFC, service function chaining)^[1]。传统的网络服务提供方式需要在网络中部署大量的专有硬件,如防火墙、入侵检测系统、代理服务器等。企业网络和数据中心网络中部署的专有硬件数量已和转发设备数量相当^[2],这些专有硬件在提升网络性能以及安全性方面发挥着不可或缺的作用,但也存在功能与硬件紧耦合、管理复杂、成本昂贵等缺点,使网络服务面临弹性扩展能力差、难以灵活部署、运维成本过高等问题^[3]。

网络功能虚拟化(NFV, network function virtualization)技术是一种解决方案,旨在利用虚拟化和云计算技术实现相关的NF,将虚拟网络功能(VNF, virtualized network function)以软件的形式运行在商用服务器、交换机和存储器上^[4],并基于VNF构建网络服务所需的SFC,极大地提高了网络服务部署的灵活性和效率,降低了网络的运维成本,促进了新服务的部署。当前国内外各大电信运营商都在积极地推进NFV技术的应用及部署,AT&T计划到2020年底将其75%的大型网络虚拟化^[5],国内三大运营商也在积极推进NFV技术的应用。

然而相比于高可靠的电信级网络设备,“软化VNF”的脆弱性也给网络带来了一定的可靠性风险^[6],导致VNF发生失效的因素复杂多样,如硬件(处理器、内存、存储、网络接口等)故障和软件(主机操作系统、管理程序、虚拟机、VNF软件等)故障。此外,NFV的开放市场环境,第三方供应商的软、硬件解决方案,也使软、硬件面临不可能彻底管控和消除后门、陷门和漏洞问题,这些潜在的风险使VNF面临一系列威胁。任何一个NF节点的失效都将导致相关SFC的故障^[7],造成服务中断、数据丢失和资源浪费。NF节点面临的不确定失效和不确定威胁问题,给网络服务的稳定性和可靠性带来了极大的挑战。亚马逊和谷歌的数据中心都曾发生过因软件问题而造成服务中断的事件^[8-9]。因此,设计一定的故障恢复和容

错机制是必不可少的,以确保网络服务满足签订的服务级别协议(SLA, service level agreement)。

为了应对网络功能节点的失效问题,现有的研究主要通过冗余备份方式增强SFC服务提供的可靠性。在工程实践方面,文献[10]在真实的工程实验环境中实现了具有自动恢复能力的VNF部署系统,当出现单个VNF失效时,通过将失效节点的流量重新路由到备份节点以实现故障恢复。

在理论研究方面,文献[11-12]均采用对整条SFC进行备份的方式来提高网络服务的可靠性,其中,文献[12]设计了一种迭代部署算法,为已部署的SFC主链路迭代地添加备份链路,当达到所需的可靠性要求或最大链路备份数量时停止算法,此外着重研究了不同数据中心架构对SFC冗余备份部署方案的适用性,研究结果表明,以交换机为中心的双层树和三层树结构最适宜SFC的备份部署。

针对备份整条SFC存在资源开销过大的问题,文献[13-16]对VNF采取了针对性的备份策略。文献[13]通过在不同的服务器集群为VNF提供冗余备份的方式来提高服务的可靠性,并设计了一个可变领域搜索部署算法,但未考虑VNF的成链问题,仅考虑了单一VNF的可靠性部署。文献[14]针对NFV基础设施(NFVI)存在的节点和链路失效问题以及SFC映射成功率低问题,设计了一种基于广度优先搜索的回溯式部署算法,但该方法随机地选择节点和链路进行备份,在备份选择策略上存在一定的缺陷。文献[15]考虑到备份的VNF可以被不同的SFC共用,设计了一个筛选模型,迭代地选择成本效率最高VNF进行备份,避免了过度备份导致的资源利用率急剧下降问题。文献[16]考虑到底层服务器节点的可靠性不同,通过将VNF从低可靠的服务器迁移到高可靠的服务器,以及为部分VNF提供冗余备份的方式来提高SFC的可靠性,但是这种方式会导致一定的负载不均衡问题,可靠性较高的底层服务器节点业务繁重,一旦失效,将造成较大范围的影响。

考虑到即使采用有针对性的冗余备份策略也存在备份链路资源开销过大问题,文献[17-19]分

别采取一定的方法以节约链路资源。其中,文献[17]迭代地选择可靠性最低的 VNF 进行串联式冗余备份,虽然节约了一定的链路资源,但是随着备份节点数量增多,将导致链路过长、服务延迟过大。该作者在随后的研究^[18]中改进了算法,采用串联与并联共存的混合备份方式,仅在延迟允许范围内采用串联备份方式,以实现备份链路资源节约与引入延迟的权衡。文献[19]考虑到一条 SFC 上的相邻 VNF 部署在同一服务器可以节约带宽资源这一特点,使用关键子拓扑映射的反馈信息来优化 VNF 组合,联合优化 SFC 拓扑设计和映射部署,并使用共享备份的方式进行冗余备份,使资源消耗最小化。

针对 VNF 的脆弱性问题,当前的 SFC 可靠性部署方案在应对 VNF 随机失效方面有很好的效果,但是在面对利用漏洞后门的恶意攻击时存在巨大的风险。由于未考虑节点间的同构性问题,原 VNF 与备份 VNF 是同构的(如同一种软件),原物理服务器节点与备份物理服务器也是同构的(如同一种 CPU 或同一种操作系统),使原节点与备份节点存在潜在的共性缺陷^[20]。恶意攻击者在成功攻击相关节点后不需要重新挖掘和探测系统缺陷,即可对备份节点进行新的攻击,造成备份 VNF 的再次失效,导致相关 SFC 长时间故障,造成相关服务的中断。

文献[20]研究表明,异构备份式的虚拟网映射方法能极大地提高虚拟网络的抗攻击能力,对于 SFC 面临的恶意攻击问题,进行冗余备份时考虑节点间的异构性对 SFC 抗攻击性提高也将具有较大增益。可从硬件、操作系统以及应用软件 3 个层面考虑备份节点的异构性。

硬件异构:如 Intel 和 AMD 的 CPU 芯片,Intel CPU 曾因设计缺陷而引发 Meltdown(熔断)和 Spectre(幽灵)漏洞,使普通程序可拥有内核级别的权限,对用户隐私和设备安全造成了极大威胁,而 AMD 芯片因芯片架构设计不同,只有其中一个漏洞对其产品有一定影响。

操作系统异构:如微软的 Windows Server 操作系统和基于 Linux 内核的操作系统(如 Ubuntu、Red Hat、Fedora、CentOS 等),在漏洞方面存在差异^[21]。

应用软件异构:如 Apache、Nginx 和 Internet Information Server (IIS) 这 3 种 Web 服务器的漏洞也存在差别。

本文将异构思想引入 SFC 的可靠性部署策略中,设计基于异构备份的服务功能链部署方法,以应对 SFC 面临的不确定失效和恶意攻击问题。考虑到冗余备份方法存在资源开销过大问题,本文仅对关键的、易失效的 VNF 进行备份,并以最小化带宽消耗作为目标函数,设计并实现了基于冗余备份与重映射结合的混合部署算法。

2 网络模型和问题描述

2.1 网络服务虚拟化模型

一条实现特定网络服务的 SFC 示例如图 1 所示,其流量需要依次经过防火墙、深度数据分组检测功能、加密功能的处理。

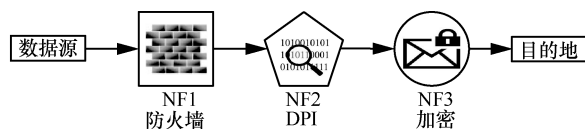


图 1 服务功能链示例

软件定义网络功能虚拟化(SDNFV, software defined network functions virtualization)系统架构如图 2 所示,它由控制模块、转发设备和 NFV 平台构成。SFC 部署的实质就是网络功能的部署和流量的引导,基于软件定义网络(SDN, software defined network)技术实现了控制与转发分离,基于 NFV 技术实现了功能与硬件解耦,SDN 与 NFV 技术的应用使网络具备集中控制和按需编排网络功能的能力,实现 VNF 的灵活部署和流量的高效引导。

本文采用基于 SDNFV 系统的服务功能链部署模型,如图 3 所示。SDNFV 系统资源管理和编排模块根据相关网络服务的请求信息以及底层网络资源的状态信息,完成相应 VNF 和虚拟链路的映射部署,各个 VNF 按照服务流程规定的执行顺序组成相应的 SFC 为用户提供服务。

2.2 网络模型

2.2.1 物理网络

用无向图 $\bar{G}=(\bar{S}, \bar{L})$ 表示物理网络,其中, $\bar{S}$ 、 $\bar{L}$ 分别表示交换机集合和物理链路集合,用

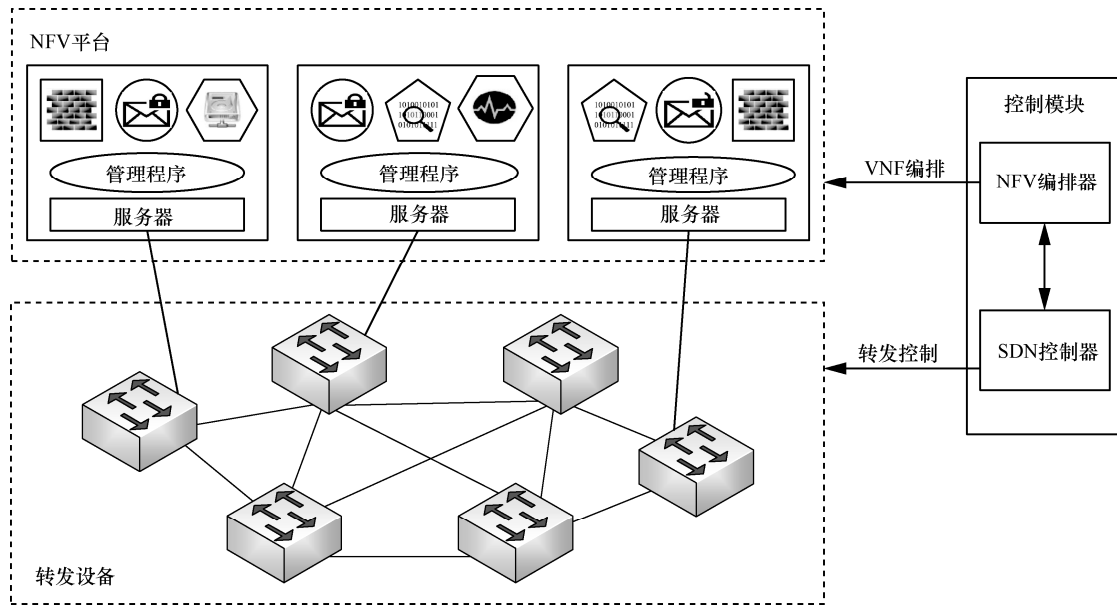


图2 软件定义网络功能虚拟化系统架构

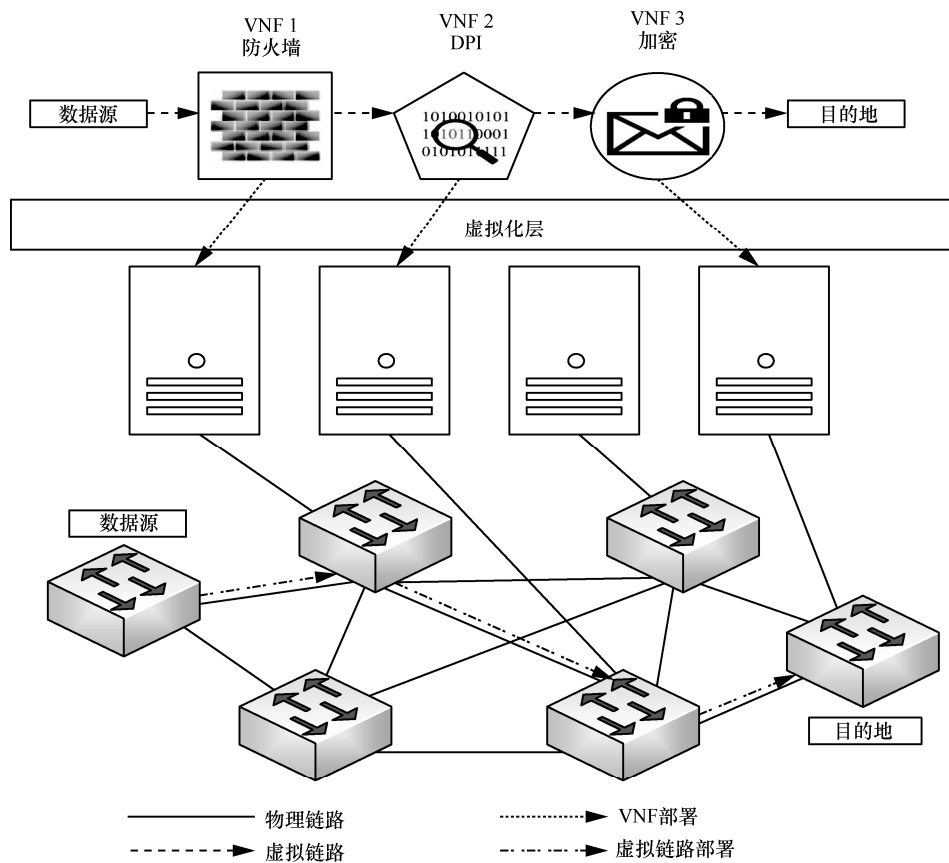


图3 服务功能链部署模型

$\bar{N}$ 表示可部署相关 VNF 的服务器集合, 用 s 、 l 、 n 分别表示底层网络中交换机、物理链路和服务器的总数量。定义矩阵 $B_{s \times s}$ 为交换机邻接矩阵,

表示所有交换机之间的邻接关系, 其中, 元素 $B_{i,j} \in R^+$ 表示交换机节点 $i \in \bar{S}$ 到 $j \in \bar{S}$ 的通信链路带宽。定义二值矩阵 $H_{n \times s}$ 为服务器与交换机连

接关系矩阵, 其中, 元素 $H_{i,j} \in \{0,1\}$, 若元素 $H_{i,j}=1$, 则表示服务器节点 $i \in \bar{N}$ 连接在交换机 $j \in \bar{S}$ 上, 且每个服务器只能与一个交换机相连, 即 $\sum_{j \in \bar{S}} H_{i,j} = 1, \forall i \in \bar{N}$ 。用集合 K 表示服务器节点可提供的资源类型集合 (CPU、内存、存储、硬件加速资源等), 并用 k 表示可提供资源类型的总数量。定义矩阵 $C_{n \times k}$ 为底层服务器资源容量矩阵, 表示服务器节点各类型资源的容量, 其中, 元素 $C_{i,j} \in R^+$ 表示服务器节点 i 上可提供的第 $j \in K$ 类资源容量。用集合 T 表示服务器节点类型集合 (不同的 CPU 或不同的操作系统均属于不同类型的异构服务器), 用 t 表示网络中服务器类型的总数量, 用数字 $1, 2, \dots, t$ 分别表示 t 种异构的服务器。定义行矩阵 $N_{1 \times n}$ 为服务器类型向量, 表示网络中服务器类型的组成, 其中, 元素 $N_{i,t} \in T = \{1, 2, \dots, t\}$ 表示服务器 i 的类型。

2.2.2 虚拟网络功能

用集合 P 表示可被整个网络提供的 VNF 集合 (如 Firewall、IDS、Encryption、Proxy 等), 用 z 表示网络可提供的不同功能的 VNF 总数量, 用 p 表示网络可提供的 VNF 类型总数量, 用数字 $1, 2, 3, \dots, 1+z, 3+z, \dots, 1+2z, 2+2z, 3+3z, \dots, p$ 分别表示 Firewall_1, IDS_1, Encryption_1, $\dots$, 异构的 Firewall_2, 异构的 IDS_2, 异构的 Encryption_2, $\dots$, 异构的 Firewall_3, 异构的 IDS_3, 异构的 Encryption_3 $\dots$ 每种 VNF 都有与处理流量大小相关的部署资源开销。定义矩阵 $Q_{p \times k}$ 为 VNF 资源需求系数矩阵, 单位为 unit (单位带宽), 元素 $Q_{i,j}$ 表示 i 类型 VNF 处理 1 单位带宽流量所需的 j 类资源数量。

考虑到运行某一类型的 VNF 可能需要特定类型的资源, 如某些 DPI 可能需要硬件加速资源, 但并不是每一台服务器都具备相应的资源。此外网络管理者可能会对特定类型的 VNF 采用一些部署策略, 如防火墙应尽量部署在网络的边界上, 因此假设每个类型的 VNF 仅可在一个较为有限的服务器集合进行部署, 而不是在任意的服务器节点进行部署。定义二值矩阵 $S_{n \times p}$ 为服务器节点可承载 VNF 类型矩阵, 元

素 $S_{i,j} \in \{0,1\}$ 表示服务器节点 i 是否支持 j 类型 VNF 的部署, 若 $S_{i,j}=1$, 则表示该服务器支持该类型 VNF 的部署。

2.2.3 SFC 请求

假定网络的运营者持续接收不同类型的 SFC 请求, 用 R 表示 SFC 请求集合, 用五元组表示第 r 个 SFC 请求, $r = \langle \bar{u}^r, \bar{v}^r, \beta^r, \tau^r, \psi^r \rangle$, 其中, $\bar{u}^r, \bar{v}^r$ 分别表示接入交换机和出口交换机, β^r 表示该请求所需处理的流量大小, τ^r 表示该请求的生存时长, ψ^r 表示流量必须经过的有序 VNF 序列 (如 Firewall $\rightarrow$ IDS $\rightarrow$ Encryption), 同时, 用 m 表示该 SFC 请求中 VNF 总数量。定义行向量 $T_{1 \times m}$ 表示 VNF 序列的组成类型向量。元素 $T_{i,i} \in \{1, 2, \dots, p\}$, $i \in \{1, 2, \dots, m\}$ 表示请求中第 i 个 VNF 的类型。

2.3 问题描述

依据文献[22]知, 攻击者实施攻击的过程可分为 3 个阶段: 信息探测阶段、漏洞挖掘阶段、攻击执行阶段。对攻击者来说, SFC 漏洞挖掘阶段需要花费大量时间, 而且还存在无法成功获取漏洞的可能性, 但是攻击者一旦掌握某种类型的漏洞信息, 即可对该 SFC 的相关 VNF 进行攻击, 造成节点故障、服务中断。

图 4 给出了一个简单的 SFC 请求实例, 图 5 给出了针对该请求的冗余备份实例, 图中不同灰度的长方形代表了不同类型的异构服务器, 如 CPU 异构、操作系统异构。现有的冗余备份方法未考虑节点的异构性问题, 使用同构的节点进行冗余备份。如图 5 所示, VNF_2^{primary} 部署于服务器 N1, 而其备份 VNF_2^{backup} 则部署在与服务器 N1 同构的服务器 N6, 当 VNF_2^{primary} 因恶意攻击而出现故障时, 备份节点 VNF_2^{backup} 接替当前故障节点继续提供服务。但是由于备份节点与原节点同构, 具有共性缺陷, 攻击者无需花费大量时间重新进行漏洞挖掘, 即可利用已掌握的漏洞信息再次进行攻击, 造成服务器 N6 上 VNF_2^{backup} 的失效, 造成服务中断。因此冗余备份节点的同构性在应对 SFC 可靠性问题方面存在巨大的缺陷。



图 4 SFC 请求实例

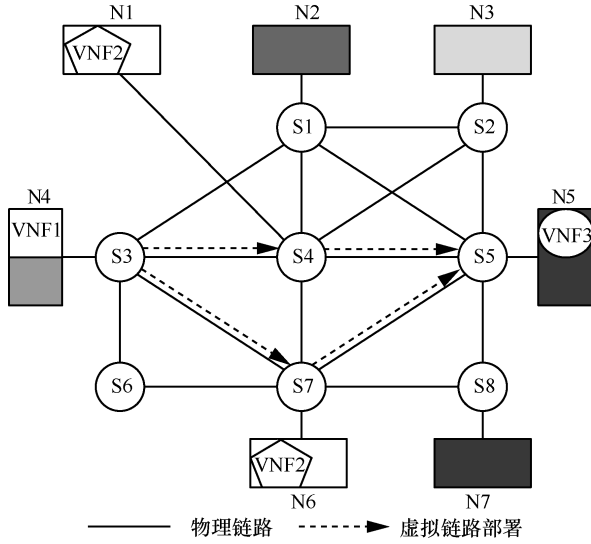


图 5 SFC 冗余备份实例

3 异构备份与重映射混合的部署方法

针对现有冗余备份方法未考虑节点的异构性问题, 本文将异构思想引入 SFC 的部署策略中。考虑到对 SFC 所有的 VNF 进行备份存在资源开销过大、资源利用率低、请求接受率低等问题, 本文采用异构备份与重映射结合的混合部署方法。

冗余备份方法是在部署阶段, 底层物理网络提前为 SFC 提供备份资源, 若相关 $VNF_i^{r, primary}$ 节点失效, 则迅速切换到备份 $VNF_i^{r, backup}$ 上, 从而保证服务的连续性。重映射方法则是当 SFC 相关 VNF_i^r 失效时, 将失效的 VNF_i^r 在网络中重新部署, 从而保证 SFC 继续为用户提供服务。冗余备份方法服务质量好, 但会造成较大的资源消耗; 而重映射方法虽然能节约资源消耗, 但会造成较长的服务中断时间。

本文结合冗余备份与重映射的优缺点, 采用异构备份与重映射结合的混合部署策略。对关键的、易失效的和可靠性低的节点采用冗余备份, 而对其他可靠性相对较高的节点采用重映射部署方法, 同时在进行冗余备份与重映射时考虑节点异构性 (底层服务器硬件异构性、操作系统的异构性以及 VNF 的异构性), 以避免原节点与新部署节点存在共性缺陷, 使攻击者对 SFC 掌握的漏洞缺陷信息无法持续有效, 即使当前攻击成功, 再次进行攻击时仍需要重新进行缺陷探测与漏洞挖掘, 显著增加攻击时间成本。下面对本文方法

进行具体描述。

3.1 异构备份

本文采用有针对性的备份策略, 仅对部分关键的 VNF_i^r 进行异构冗余备份。定义行向量 $BK_{1 \times m}^r$ 为第 r 个 SFC 中 VNF 的备份需求向量, 元素 $BK_{1,i}^r \in \{0,1\}$, 若 $BK_{1,i}^r = 1$, 则表示需要在部署阶段为 VNF_i^r 提供异构备份 $VNF_i^{r, backup}$ 。可依据相关 VNF 的可靠性统计规律, 承载 VNF 的物理服务器可靠性统计规律, 以及针对性的备份策略对相关 VNF_i^r 备份需求变量进行赋值。

在对 SFC 进行部署时, 本文先进行 SFC 基本链路映射, 再对有备份需求的 VNF_i^r 进行异构备份。如图 6 所示, 该 SFC 请求中包含 3 个 VNF, 其中, VNF_2 需要进行备份。首先在服务器 N4、N1、N5 完成对 SFC 基本链路的部署, 之后在异构的服务器 N2 完成备份节点 VNF_2^{backup} 的部署。

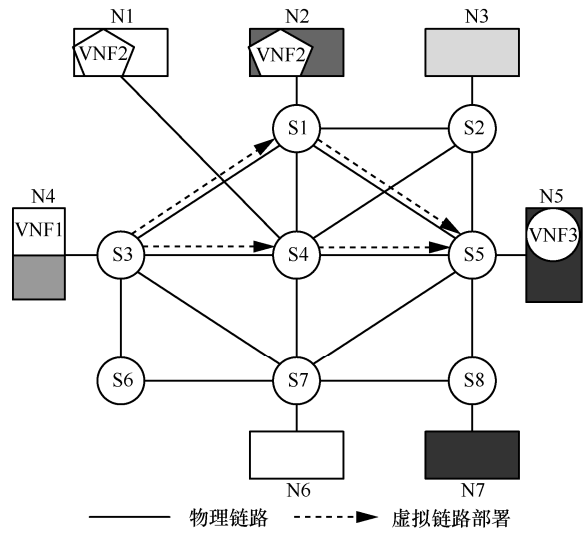


图 6 异构备份

3.2 异构重映射

对于已经进行备份的 VNF_i 节点, 当出现故障后可迅速由备份节点继续提供服务, 而对于未备份 VNF_i , 本文采用重映射的方式实现故障恢复, 即对相关 VNF_i 在出现故障后进行重新部署。如图 7 所示, 当部署于服务器 N5 的 VNF_3 因各种复杂原因而引发故障时, 控制模块发现异常, 并在异构服务器 N3 上完成 $VNF_3^{redeploy}$ 的重新部署, 可在一定故障恢复时间之后继续为用户提供服务。

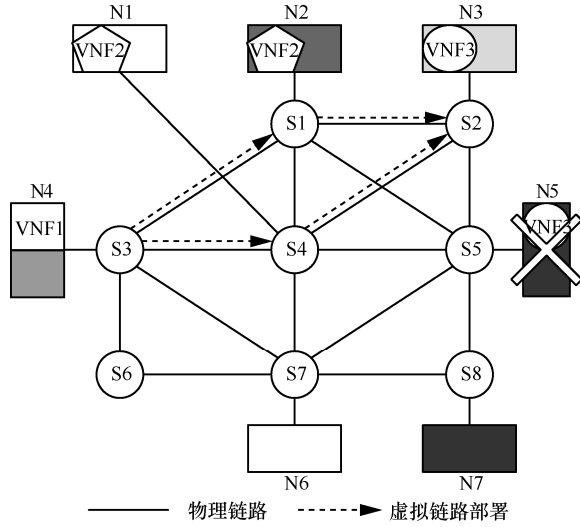


图7 异构重映射

4 异构备份与重映射部署模型和算法

4.1 异构备份与重映射部署模型

定义二值矩阵 $F_{m \times n}^r$ 表示第 r 个 SFC 请求中 VNF 与服务器节点的部署关系矩阵，元素 $F_{i,j}^r \in \{0,1\}$ ，若 $F_{i,j}^r = 1$ ，则表示第 r 个 SFC 请求中的第 i 个 VNF，即 VNF_i^r 部署在服务器节点 j 上。本文允许同一 SFC 请求中的不同 VNF 部署在同一服务器节点上。定义 $n_i^r \in \bar{N}$ ，表示 VNF_i^r 部署的服务器节点，此时 $F_{i,n_i^r}^r = 1$ 。定义 $s_i^r \in \bar{S}$ ，表示 VNF_i^r 部署的服务器节点为 n_i^r 所直连的交换机为 s_i^r ，此时有 $F_{i,n_i^r}^r = 1, H_{n_i^r, s_i^r} = 1$ 。此外当 $i=0$ 时，令 $s_0^r = \bar{u}$ ，表示接入交换机；当 $i=m+1$ ，令 $s_{m+1}^r = \bar{v}$ ，表示出口交换机。定义集合 $V=\eta(u) = \{v | B_{u,v} > 0\} \subseteq \bar{S}, u \in \bar{S}$ ，表示与交换机 u 直连的交换机集合。

定义二值矩阵 $E_{s \times s}^{s_i^r, s_{i+1}^r}$ 表示第 r 个 SFC 请求中 VNF_i^r 与 VNF_{i+1}^r 之间的虚拟链路 $L_{i,i+1}^r$ 与物理链路 $\bar{L}_{u,v}$ 之间的映射关系，元素 $E_{u,v}^{s_i^r, s_{i+1}^r} \in \{0,1\}$ ，若 $E_{u,v}^{s_i^r, s_{i+1}^r} = 1$ 则表示虚拟链路 $L_{i,i+1}^r$ 部署在物理链路 $\bar{L}_{u,v}$ 上，构建 VNF_i^r 与 VNF_{i+1}^r 所连接交换机之间的链路，以实现 VNF 的连接。定义矩阵 $C_{n \times k}^{rem}$ 和 $B_{s \times s}^{rem}$ 分别表示当前物理网络服务器资源和链路资源的剩余数量。

本文先进行 SFC 请求的基本链路部署，再对有备份需求的 VNF 进行部署，之后当 VNF 失效

时完成对未备份节点的重映射。

1) SFC 请求基本链路部署约束条件

VNF 部署约束条件为

$$S_{n_i^r, VNF_i^r} = 1 \quad \forall i \in \{1, 2, \dots, m\}, VNF_i^r \in \psi^r, n_i^r \in \bar{N} \quad (1)$$

$$\sum_{i=1}^m Q_{VNF_i^r, k} \beta^r F_{i,n}^r \leq C_{n,k}^{rem}, \forall k \in K, \forall n \in \bar{N} \quad (2)$$

$$\sum_{j \in \bar{N}} F_{i,j}^r = 1, \forall i \in \{1, 2, \dots, m\} \quad (3)$$

式(1)表示 VNF_i^r 所部署的服务器节点 n_i^r 必须支持该类型 VNF 的部署，式(2)表示该 SFC 请求中的全部 VNF 使用的资源数量不能超过所要占用的服务器节点各类资源的余量，式(3)表示每一个 VNF_i^r 能且仅能部署在一个服务器节点上。

链路部署约束条件为

$$\sum_{i=0}^m E_{u,v}^{s_i^r, s_{i+1}^r} \beta^r \leq B_{u,v}^{rem}, \forall u \in \bar{S}, v \in V=\eta(u) \quad (4)$$

式(4)表示该请求中的全部虚拟链路占用的带宽资源不能超过各条物理链路带宽资源的余量。

目标函数为

$$\text{Min} \left[\sum_{i \in \{0,1,\dots,m\}} \sum_{u \in \bar{S}} \sum_{v \in V=\eta(u)} E_{u,v}^{s_i^r, s_{i+1}^r} \beta^r \right] \quad (5)$$

对于一条 SFC 的部署，各个 VNF 部署到任意服务节点需要占用的服务器资源是相同的，但是虚拟链路的带宽资源消耗会因 VNF 部署服务器节点的不同而变化，为了降低资源开销，本文将式(5)带宽资源开销作为目标函数。

2) 异构备份约束条件

定义 $n_i^{rb} \in \bar{N}$ ，表示 $VNF_i^{r, backup}$ 部署的服务器节点，此时有 $F_{i,n_i^{rb}}^{rb} = 1$ 。定义 $s_i^{rb} \in \bar{S}$ ，表示 $VNF_i^{r, backup}$ 部署的服务器节点 n_i^{rb} 所直连的交换机为 s_i^{rb} ，此时 $F_{i,n_i^{rb}}^{rb} = 1, H_{n_i^{rb}, s_i^{rb}} = 1$ 。当备份需求向量 $BK_{1 \times m}^r$ 中存在元素 $BK_{i,i}^r = 1, i \in \{1, \dots, m\}$ 时，需要在部署阶段为相应的 VNF_i^r 提供异构冗余备份，首先完成 $VNF_i^{r, backup}$ 在服务器节点 $n_i^{rb} \in \bar{N}$ 的部署，其次完成 $VNF_i^{r, backup}$ 与 VNF_{i-1}^r 、 $VNF_i^{r, backup}$ 与 VNF_{i+1}^r 、 $VNF_{i-1}^{r, backup}$ 与 $VNF_{i+1}^{r, backup}$ （若 $BK_{i,i-1}^r = 1$ ，则存在该链路）之间的 2 条（或 3 条）虚拟链路部署，目标同样也是最小化链路带宽消耗。

$VNF_i^{r, backup}$ 的部署约束条件为

$$BK_{1,i}^r = 1, i \in \{1, \dots, m\} \quad (6)$$

$$VNF_i^{r, \text{backup}} = VNF_i^r + zj, i \in \{1, \dots, m\}, j \in \{1, 2\} \quad (7)$$

$$S_{n_i^{rb}, VNF_i^{r, \text{backup}}} = 1, n_i^{rb} \in \bar{N}, VNF_i^{r, \text{backup}} \in P \quad (8)$$

$$n_i^{rb} \neq n_i^r, N_{1, n_i^{rb}} \neq N_{1, n_i^r}, n_i^{rb}, n_i^r \in \bar{N} \quad (9)$$

$$Q_{VNF_i^{r, \text{backup}}, k} \beta^r F_{i, n_i^{rb}}^r \leq C_{n_i^{rb}, k}^{\text{rem}}, \forall k \in K \quad (10)$$

$$\sum_{j \in \bar{N}} F_{i, j}^{r, b} = 1 \quad (11)$$

式(6)表示提供冗余备份的前提条件, 式(7)表示提供的冗余备份 VNF 是异构的, 式(8)表示 $VNF_i^{r, \text{backup}}$ 所部署的服务器节点 n_i^{rb} 必须支持该类型的 VNF。式(9)提供备份的服务器节点要与原节点异构, 式(10)提供备份的服务器节点 n_i^{rb} 各类资源余量要满足部署需求, 式(11)保证 $VNF_i^{r, \text{backup}}$ 能且仅能被一个物理服务器承载。

备份虚拟链路部署约束条件为

$$\left(E_{u, v}^{s_{i-1}^{rb}, s_i^{rb}} + E_{u, v}^{s_i^{rb}, s_{i+1}^{rb}} + E_{u, v}^{s_{i-1}^{rb}, s_{i+1}^{rb}} \right) \beta^r \leq B_{u, v}^{\text{rem}} \quad (12)$$

$$\forall u \in \bar{S}, v \in V = \eta(u)$$

目标函数为

$$\text{Min} \left[\sum_{u \in \bar{S}} \sum_{v \in V = \eta(u)} \left(E_{u, v}^{s_{i-1}^{rb}, s_i^{rb}} + E_{u, v}^{s_i^{rb}, s_{i+1}^{rb}} + E_{u, v}^{s_{i-1}^{rb}, s_{i+1}^{rb}} \right) \beta^r \right] \quad (13)$$

3) 重映射约束条件

重映射约束条件与异构备份约束条件基本相同, 需要考虑故障 VNF_i^r 节点的代替节点 $VNF_i^{r, \text{redeploy}}$ 的异构部署, 以及 $VNF_i^{r, \text{redeploy}}$ 与 VNF_{i-1}^r , 以及可能存在的 VNF_{i+1}^r 与 $VNF_{i-1}^{r, \text{backup}}$ 、 $VNF_i^{r, \text{backup}}$ 之间的虚拟链路部署。

4.2 算法设计

以 4.1 节中各式为约束条件, 本文根据文献[23-24]设计了基于 Viterbi 的异构备份算法和重映射算法。算法流程分别在 4.2.1 和 4.2.2 节中介绍。本节以一个含有 3 个 VNF 的 SFC 请求为例, 用图 8、图 9、图 10 分别简单介绍了相关算法的实现细节, 图中圆圈代表交换机节点, 边代表交换机间的链路。

图 8 为基本链路部署多阶段图, 分为 3+2 个阶段。在阶段 0 和阶段 4 中, 仅含有已经确定位置的接入交换机节点 $X_{0,i}$ 和流出交换机节点 $X_{4,i}$ 。在阶段 1~3 中, 各阶段分别确定满足 VNF_i^r 部署要求的服务器节点集合, 并列出服务器节点

所直连的交换机节点 $X_{i,j}$ 。之后为相邻阶段交换机之间添加一条边, 代表交换机之间的链路, 每条边都有相应的链路部署代价。最后使用 Viterbi 算法求解该多阶段图的最短路径, 所求结果即为最优部署方案。

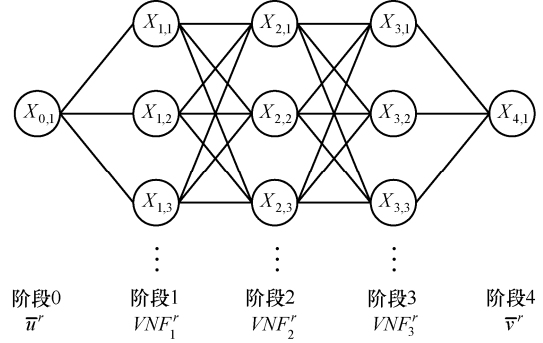


图 8 基本链路部署多阶段图

完成基础链路部署之后, 可确定接入交换机、流出交换机以及基础 VNF_i^r 的部署位置 s_i^r , 再对有备份需求的 VNF_i^r 进行异构备份。图 9 为异构备份部署多阶段图, 该图描述了对全部 VNF_i^r 进行备份的最复杂情景。分为 3 个阶段, 与基本链路部署阶段相似, 各阶段分别确定满足 VNF_i^{rb} 部署要求的服务器节点集合, 列出服务器节点所直连的交换机节点 $Y_{i,j}$, 并为相应的交换机之间添加边, 确定每条边对应的链路部署代价。最后, 使用 Viterbi 算法求解最优部署方案。

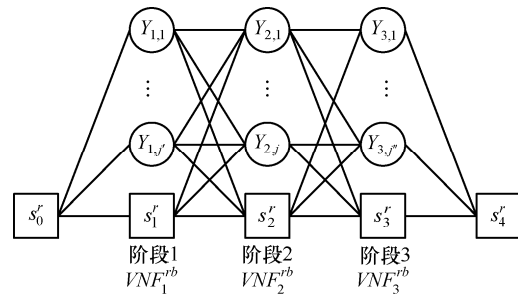


图 9 异构备份部署多阶段图

图 10 所示的重映射过程较为简单, 相关基础 VNF_i^r 和备份 VNF_i^{rb} 的部署位置已定, 仅需要在故障发生时, 为未备份节点 VNF_i^{redeploy} 确定满足部署要求的服务器集合, 并列出服务器节点所直连的交换机节点 $Z_{i,j}$, 为相应的交换机之间添加边, 确定每条边对应的链路部署代价, 选择总的链路部署代价最小的部署位置即可。

3) $\pi_{i,j} = \text{cost}(s_{i-1}^r, Z_{i,j}) + \text{cost}(s_{i+1}^r, Z_{i,j})$

4) **If** $BK_{i-1}^r = 1$

5) $\pi_{i,j} = \pi_{i,j} + \text{cost}(s_{i-1}^{rb}, Z_{i,j})$

6) **End if**

7) **If** $BK_{i+1}^r = 1$

8) $\pi_{i,j} = \pi_{i,j} + \text{cost}(s_{i+1}^{rb}, Z_{i,j})$

9) **End if**

10) **End for**

11) $\pi_{i,j}$ 中的最小值以及对应的节点和链路,

即为最小带宽占用的重映射方案

12) 更新网络资源状态

4.3 复杂度分析

本节对算法的计算复杂度进行分析。SFC 请求中 VNF 数量最多为 m , 服务器数量为 n 。在算法 1 中, 首先为每个 VNF_i^r 确定满足部署要求的服务器集合, 其计算复杂度为 $O(mn)$, 其次以 Viterbi 算法为核心的基本链路部署过程计算复杂度为 $O(mn^2)$, 之后基于 Viterbi 算法进行异构备份时的最大计算复杂度也为 $O(mn^2)$, 所以算法 1 的计算复杂度为 $O(mn^2)$ 。算法 2 中, $VNF_i^{r, redeploy}$ 确定可部署服务器集合的计算复杂度 $O(n)$, 确定最优部署方案的计算复杂度也为 $O(n)$, 所以算法 2 的计算复杂度为 $O(n)$ 。

5 实验仿真

5.1 实验环境设置

本文采用文献[23]提供的 DC.K8 数据中心网络拓扑, 包含 80 个交换机节点, 256 条链路, 链路带宽容量从 {10,20,30,40} 中选取。其中, 32 个交换机节点部署有服务器, 异构物理网络的服务器节点类型随机从 [1,6] 中选取, 同构物理网络的服务器节点类型只有一种, 每个服务器节点的计算资源随机从 {16,32,48,64} 中选取。有 6 种不同功能的 VNF, 每种 VNF 有 2 种异构的同功能 VNF, 每种 VNF 的部署资源需求系数如表 1 所示, 每个服务器节点可承载的 VNF 从 6 种 VNF 中随机选取 4 种。每个 SFC 请求所需处理的流量大小服从 [1,4] 的均匀分布, 请求中包含的 VNF 随机从 6 种 VNF 中选取 4 种, 请求的到达服从参数为 0.05 的泊松过程, 生命周期服从均值为 1 000 个单位时间的指数分布。算法使用 Python 实现, 运行在 Intel

Core i5-3230 2.6 GHz 内存为 16 GB 的个人计算机上。

表 1 相关 VNF 计算资源需求系数

VNF	计算资源需求
Firewall_x	1/单位带宽
Proxy_x	1/单位带宽
Nat_x	2/单位带宽
IDS_x	3/单位带宽
DPI_x	3/单位带宽
Encryption_x	4/单位带宽

为了评估算法的可行性和有效性, 本实验以请求接受率、平均每个请求占用的带宽、抗攻击能力以及故障恢复能力为评价指标。将文献[23]中不进行备份算法、同构备份算法以及本文提出的异构备份算法进行比较。为了便于描述, 在同构的物理网络环境下, 用 No-HomBackup (no homogeneous backup) 表示不对 VNF 进行同构备份, 用 Half-HomBackup (half homogeneous backup) 表示对 50% 的关键 VNF 进行同构备份, 用 All-HomBackup (all homogeneous backup) 表示对全部的 VNF 进行同构备份; 在异构的物理网络环境下, 用 No-HetBackup (No heterogeneous backup) 表示不对 VNF 进行异构备份, 用 Half-HetBackup (half heterogeneous backup) 表示对 50% 的关键 VNF 进行异构备份, 用 All-HetBackup (all heterogeneous backup) 表示对全部的 VNF 进行异构备份。

5.2 性能分析

5.2.1 请求接受率

图 11 表示了在本实验所设置的同构网络环境或异构网络环境下, 6 种情况的请求接受率比较。从图中可以看出, 请求接受率的高低顺序为 No-xxxBackup > Half-xxxBackup > All-xxxBackup, 这是因为对 VNF 进行备份时会占用更多的物理资源, 而底层网络物理网络资源有限, 每个请求占用的资源增多时, 会导致网络所能容纳的 SFC 数量下降, 进而导致请求接受率明显下降。其中, 在对全部的 VNF 进行备份时, 请求接受率下降严重, 极大地影响 SFC 的部署以及网络服务的提供, 而本文采用的仅对关键 VNF 进行备份的策略能在很大程度上减轻因冗余备份而导致的请求接受率下降问题。

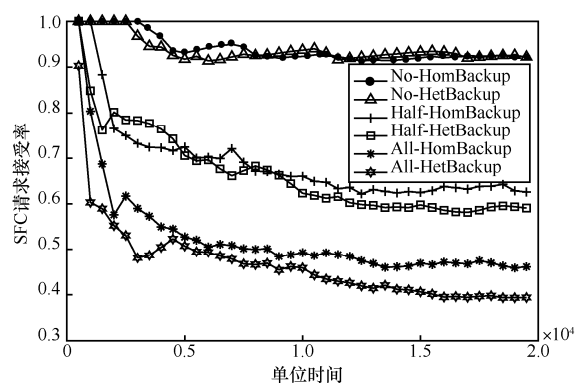


图 11 服务功能链请求接受率

在不进行备份时，No-HomBackup 与 No-HetBackup 的请求接受率基本相同，说明异构的网络环境在不进行备份情况下对请求接受率的影响很小，基本与同构的网络环境一致。在对关键的 VNF 进行备份时，Half-HomBackup 的请求接受率略高于 Half-HetBackup 的请求接受率，这是由于相比于不考虑节点异构性的同构备份方式，本文采用的异构备份方式因考虑备份节点的异构性会舍弃一些可用同构服务器节点，因此会导致一定程度的请求接受率下降，实验数据显示，系统稳定后下降约为 3.8%。

5.2.2 平均每个请求占用的带宽

图 12 表示了 6 种情况下，平均每个请求占用的带宽情况。冗余备份方式虽然能极大地提高 SFC 的可靠性，但由于备份时需要构建大量备份 VNF 与相关 VNF 之间的链路，占用的带宽资源相比于不进行备份时有明显的增加。特别是对全部的 VNF 进行备份时，会占用极大数量的链路带宽，而本文采用的仅对关键 VNF 进行备份的策略，能在一定程度上缓解因冗余备份而导致的带宽数量急剧增加情况。

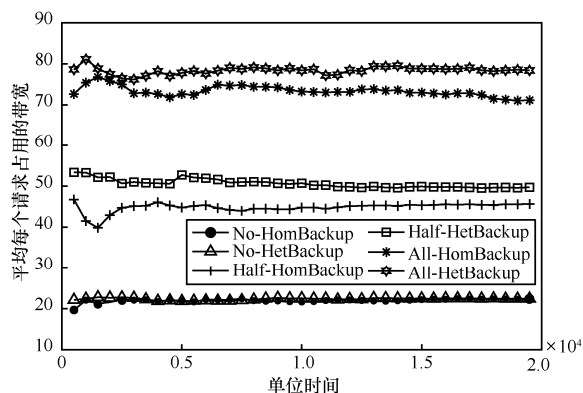


图 12 单个请求占用的平均带宽

在对关键的 VNF 进行备份时，Half-HetBackup 的平均带宽占用情况略高于 Half-HomBackup，这是由于在进行异构备份时，因考虑服务器节点的异构性，会舍弃一些较近的同构服务器节点，因此导致一定程度的链路增长，实验数据显示，Half-HetBackup 相比于 Half-HomBackup 增加约 9.2% 的带宽消耗。

5.2.3 抗攻击能力

为了比较 6 种情况下 SFC 的抗攻击性能，本实验对攻击者实施的恶意攻击进行了简单的建模，实验假设：1) 攻击者对一种服务器类型下的目标 VNF 进行漏洞挖掘和缺陷探测，并成功利用该漏洞或缺陷致使目标 VNF 瘫痪所需花费的时间服从均值为 1 000 的指数分布；2) 攻击者再次攻击一个已掌握漏洞或缺陷的 VNF 所花费的时间相对很少，可忽略不计，即时间主要花费在漏洞挖掘与缺陷探测；3) 攻击者极其具有耐心，可以承受的忍耐时间^[20]无限大，即攻击者会持续对一条目标 SFC 中的 VNF 进行攻击，不会因已花费的时间过大而放弃攻击尝试，若致瘫其中一个 VNF 但没有导致 SFC 服务中断时会继续进行攻击，直至成功使目标 SFC 失效，造成服务中断。本实验模拟并记录了攻击者在 6 种情况下成功致瘫一条目标 SFC 所花费的时间成本，并重复了 200 次实验，对数据进行统计分析，绘制了如图 13 所示的攻击时间成本与 SFC 失效概率关系图，以及图 14 所示的平均攻击时间成本图。

从图 13 和图 14 可以看出，同构网络环境下的相关同构备份方法并不能增加恶意攻击者的攻击难度和攻击时间成本，这是由于备份节点与原节点同构，存在共性缺陷，攻击者无需重新挖掘漏洞和探测缺陷即可实现对备份节点的快速攻击，造成 SFC 失效。而异构网络环境下的异构备份的方式能显著增加攻击者的攻击难度。如图 13 所示，当攻击时间投入 $T=2\ 000$ 时，All-HetBackup 情况下的 SFC 失效概率约为 0.25，Half-HetBackup 情况下的 SFC 失效概率约为 0.60，而其他 4 种情况下的 SFC 失效概率约为 0.85~0.9，存在极高的失效风险。如图 14 所示，在异构网络环境下，Half-HetBackup 能增加攻击者约 1 倍的攻击时间成本，而 All-HetBackup 能增加攻击者约 2.5 倍的攻击时间成本。

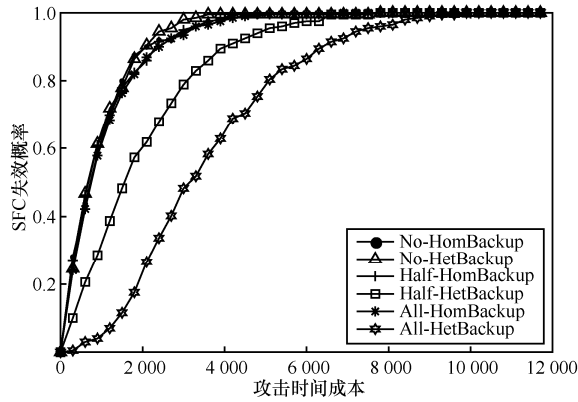


图 13 攻击时间成本与 SFC 失效概率关系

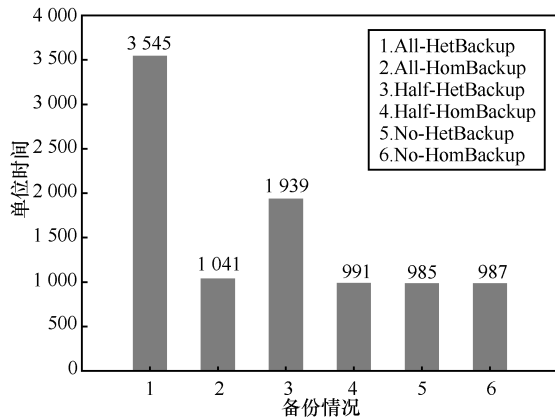


图 14 平均攻击时间成本

5.2.4 故障恢复能力

为了比较异构备份与重映射部署算法的故障恢复能力，本实验对故障场景进行了简单的建模。假设 SFC 的生命周期无限大，所包含的 4 个 VNF 具有不同的可靠性，VNF 会因各种原因而发生故障，无故障运行时间分别服从均值为 1 000、2 000、3 000 和 4 000 的指数分布，VNF 发生故障时将导致服务中断，可通过切换至异构备份 VNF 节点或重映射该 VNF 节点实现故障修复。本实验模拟并记录了不同备份比例下 SFC 累计服务中断时间以及故障修复时间，并对数据进行了统计分析，绘制了如图 15 所示的 SFC 累计服务中断时间图，以及如图 16 所示的平均故障修复时间图。

从图 15 可以看出，运行一段时间后，SFC 累计服务中断时间会因 VNF 冗余备份比例的提高而显著降低，这是由于当故障发生时，切换至备份节点的故障修复速度远快于重映射故障修复速度，减少了因故障而导致的服务中断时间，这是以一定的资源开销为代价换取的故障修复效率。

此外还可以看出，本文所采用的仅对关键 VNF 进行备份的策略整体效益较高，在一定程度上取得了资源消耗与故障恢复能力的权衡。由图 16 所示的平均故障修复时间可以看出，随着备份比例的提高，平均故障修复时间显著降低。这是由于当故障发生时，切换至备份节点的故障修复速度远快于重映射部署修复速度，因为切换至备份节点的故障修复方式仅需要新网络配置的执行下发，而重映射故障修复方式则需要网络配置设计、网络配置执行下发以及新 VNF 节点的实例化执行等。

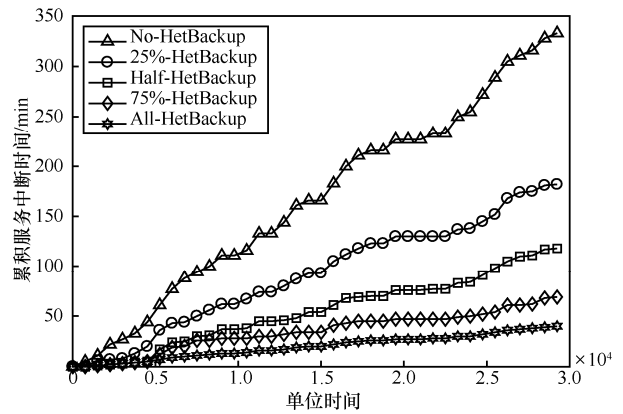


图 15 累计服务中断时间

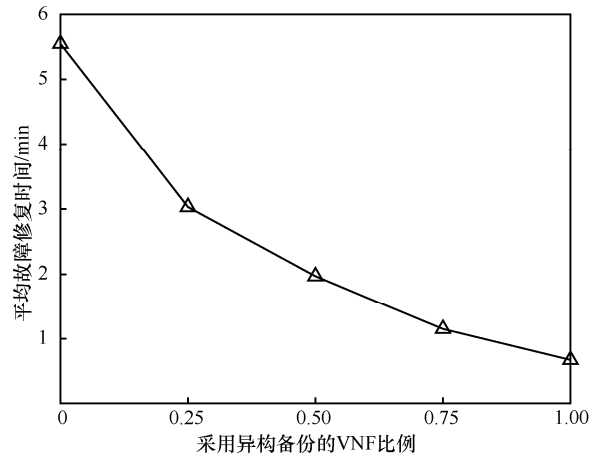


图 16 平均故障修复时间

6 结束语

本文分析了当前服务功能链冗余备份部署方法存在资源开销过大以及未考虑节点同构性的问题，提出了一种考虑节点异构性的服务功能链部署方法，以最小化链路带宽开销作为目标函数，构建

和设计了异构备份与重映射结合的服务功能链部署模型和算法。实验结果表明,在进行备份时考虑备份节点与原节点的异构性,能较为显著地增加攻击者的攻击时间成本,提高了服务功能链的可靠性。

参考文献:

- [1] 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.
- [2] SHERRY J, HASAN S, SCOTT C, et al. Making middleboxes someone else's problem: network processing as a cloud service[J]. ACM Sigcomm Computer Communication Review, 2012, 42(4): 13-24.
- [3] MIJUMBI R, SERRAT J, GORRICHIO J L, et al. Network function virtualization: state-of-the-art and research challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 18(1):236-262.
- [4] NFV ISG. Network functions virtualisation-an introduction, benefits, enablers, challenges & call for action[R]. 2012.
- [5] DONOVAN J. How do you keep pace with a 100,000 percent increase in wireless data traffic[C]// Open Networking Summit. 2015.
- [6] COTRONEO D, SIMONE L D, IANNILLO A K, et al. Network function virtualization: challenges and directions for reliability assurance[C]// IEEE International Symposium on Software Reliability Engineering Workshops. 2014:37-42.
- [7] Network functions virtualisation (NFV); reliability; report on models and features for end-to-end reliability[R]. 2016.
- [8] GUNAWI H S, HAO M, ELIAZAR K J, et al. Why does the cloud stop computing? lessons from hundreds of service outages[C]//ACM Symposium on Cloud Computing. 2016:1-16.
- [9] FAN J, GUAN C, REN K, et al. Guaranteeing availability for network function virtualization with geographic redundancy deployment[R]. 2015.
- [10] MEDHAT A M, CARELLA G A, PAULS M, et al. Resilient orchestration of service functions chains in a NFV environment[C]// Network Function Virtualization and Software Defined Networks. 2017:7-12.
- [11] HMAITY A, SAVI M, MUSUMECI F, et al. Virtual network function placement for resilient service chain provisioning[C]// International Workshop on Resilient Networks Design and Modeling. 2016.
- [12] HERKER S, AN X, KIESS W, et al. Data-center architecture impacts on virtualized network functions service chain embedding with high availability requirements[C]//IEEE Globecom Workshops. 2015:1-7.
- [13] CASAZZA M, FOUILHOUX P, BOUET M, et al. Securing virtual network function placement with high availability guarantees[C]// IFIP Networking Conference (IFIP Networking) and Workshops. 2017: 1-9.
- [14] BECK M T, BOTERO J F, KAI S. Resilient allocation of service function chains[C]//Network Function Virtualization and Software Defined Networks. 2017:1-6.
- [15] DING W, YU H, LUO S. Enhancing the reliability of services in NFV with the cost-efficient redundancy scheme[C]// IEEE International Conference on Communications. 2017:1-6.
- [16] CARPIO F, JUKAN A. Improving reliability of service function chains with combined vnf migrations and replications[J]. arXiv Preprint arXiv:1711.08965, 2017.
- [17] LONG Q, ASSI C, SHABAN K, et al. Reliability-aware service provisioning in NFV-enabled enterprise datacenter networks[C]// International Conference on Network and Service Management. 2017.
- [18] LONG Q, ASSI C, SHABAN K, et al. A reliability-aware network service chain provisioning with delay guarantees in nf-v-enabled enterprise datacenter networks[J]. IEEE Transactions on Network & Service Management, 2017, (99):1-1.
- [19] YE Z, CAO X, WANG J, et al. Joint topology design and mapping of service function chains for efficient, scalable, and reliable network functions virtualization[J]. IEEE Network, 2016, 30(3):81-87.
- [20] 季新生, 赵硕, 艾健健, 等. 异构备份式的虚拟网映射方法研究[J]. 电子与信息学报, 2018, 40(5):1087-1093.
- [21] 张森, 季新生, 艾健健, 等. 基于操作系统多样性的虚拟机安全部署策略[J]. 网络与信息安全学报, 2017, 3(10):35-43.
- [22] ZHANG M, JI X S, AI Jianjian, et al. Secure deployment strategy of virtual machines based on operating system diversity [J]. Chinese Journal of Network and Information Security, 2017, 3(10): 35-43.
- [23] SEXTON J, STORLIE C, NEIL J. Attack chain detection statistical analysis and data mining[J]. The ASA Data Science Journal, 2015, 8(5-6): 353-363.
- [24] BARI F, CHOWDHURY S R, Ahmed R, et al. Orchestrating virtualized network functions[J]. IEEE Transactions on Network & Service Management, 2016, PP(99): 1.
- [25] 刘彩霞, 卢干强, 汤红波, 等. 一种基于 Viterbi 算法的虚拟网络功能自适应部署方法[J]. 电子与信息学报, 2016, 38(11): 2922-2930.
- [26] LIU CX, LU GQ, TANG HB, et al. Adaptive deployment method for virtualized network function based on viterbi algorithm[J]. Journal of Electronics and Information Technology, 2016, 38(11): 2922-2930.

[作者简介]



谢记超 (1993-), 男, 河北石家庄人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为网络安全、网络功能虚拟化。

伊鹏 (1977-), 男, 湖北黄冈人, 国家数字交换系统工程技术研究中心研究员、博士生导师, 主要研究方向为网络空间安全、新型网络体系结构。

张震 (1985-), 男, 山东济宁人, 国家数字交换系统工程技术研究中心讲师, 主要研究方向为新型网络体系结构。

张传浩 (1979-), 男, 河南郑州人, 铁道警察学院讲师, 主要研究方向为网络信息安全、网络功能虚拟化。

谷允捷 (1994-), 男, 山东济宁人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为网络功能虚拟化。