

基于安全分级的网络切片备份与重映射方法研究

孙志勇, 季新生, 游伟, 袁泉

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 在未来 5G 核心网虚拟化环境中通用的 X86 服务器使攻击者容易发掘漏洞, 底层网络也更易感染和传播病毒, 进而造成单个物理节点失效问题, 严重影响网络切片的服务性能。首先在现有节点备份和重映射应对方案基础上, 考虑节点间的安全约束关系对网络安全性能的影响, 提出网络切片中虚拟节点与物理节点的安全参数评估模型, 建立虚拟节点与物理节点之间的安全约束关系; 然后基于安全参数评估模型选出备份虚拟节点并设计备份映射方法; 最后在满足网络时延要求下设计节点重映射机制。实验结果表明, 所提方法能够在满足网络切片的服务性能要求下, 显著提升网络的入侵容忍能力。

关键词: 网络切片; 服务功能链映射; 备份; 重映射; 可靠性

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018088

Research on backup and remapping of network slice based on security classification

SUN Zhiyong, JI Xinsheng, YOU Wei, YUAN Quan

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

Abstract: In the future virtual environment of 5G core network, the general X86 servers make the attackers exploit vulnerabilities more easily, the substrate network is infected with and spreads the virus more easily, and the problem of single physical node failed will affect the service performance of the network slice seriously. Based on the existing node backup and remapping solutions, considering the impact of security constraints among nodes on network security performance, a security parameter evaluation model of virtual nodes and physical nodes were proposed in the network slicing, and the security constraint relationship was established between the virtual nodes and the physical nodes. Then backup virtual nodes were selected based on the security parameters evaluation model, and backup mapping methods were designed. Finally, the node remapping mechanism was designed with satisfying the requirement of network delay. Experiments show that the proposed method can significantly improve network intrusion tolerance with satisfying the requirements of network slicing service performance.

Key words: network slice, service function chain mapping, backup, remapping, reliability

1 引言

第五代移动通信(5G)系统不仅用于人与人

之间的通信, 还用于人与物以及物与物之间的通信, 实现真正的“万物互联”。国际标准组织 3GPP 已经定义了 70 多种 5G 的 SA1 需求文件^[1], 主要

收稿日期: 2018-09-20; 修回日期: 2018-10-15

通信作者: 孙志勇, sunxdstu@163.com

基金项目: 国家自然科学基金创新研究群体基金资助项目(No.61521003); 国家重点研发计划基金资助项目(No.2016YFB0801605)

Foundation Items: The Foundation for Innovative Research Groups of the National Natural Science Foundation of China (No.61521003), The National Key R&D Program of China (No.2016YFB0801605)

分为3种场景,即增强移动宽带、海量机器类通信和超可靠低时延通信,5G需要针对不同的应用场景提供不同的服务。5G核心网利用网络功能虚拟化(NFV, network function virtualization)/软件定义网络(SDN, software defined network)等虚拟化技术构造不同的网络切片以满足不同的业务场景需求,同时提高了网络灵活性和资源的利用效率^[2]。基于虚拟化技术的网络切片部署过程可抽象服务功能链(SFC, service function chain)映射模型^[3-5],在虚拟化云环境中,服务的实现需要一组有序的网络功能,该有序的功能集合被称为SFC^[6-7]。NFV将网元功能与专属硬件平台解耦,使服务提供商能够在通用分布式云平台上动态实例化SFC并向租户提供服务^[8]。

但网络虚拟化环境下底层网络通用的X86物理服务器使攻击者容易发掘系统漏洞,底层物理网络也更易感染和传播病毒,可能导致单个物理节点失效,失效物理节点承载的所有虚拟网络功能(VNF, virtual network function)和这些VNF所在的SFC将无法正常工作,大大影响用户的使用体验。攻击者发动攻击主要分为3个阶段^[9]:探测系统信息、挖掘系统漏洞、执行攻击,具体过程如下。①探测系统信息阶段:攻击者根据网络信息确定攻击目标并收集目标系统的相关信息;②挖掘系统漏洞阶段:攻击者从收集到的目标信息中提取可用的漏洞信息;③执行攻击阶段:利用系统漏洞获取系统的控制权,从而利用攻击工具发动攻击使系统无法正常工作。

对攻击者来说,挖掘系统漏洞阶段往往需要花费大量时间,而且可能无法成功挖掘到系统的漏洞。为了使节点免于潜在的网络攻击,确保信息的安全,用户往往选择将SFC映射在有特定安全级别的物理网络资源上,如虚拟网络节点需要映像在具有一定数据加密级别和防火墙级别的物理节点上^[10]。

现有针对单节点失效问题的研究主要有可生存性的虚拟网映射(SVNE, survivable virtual network embedding)方法^[11-12]。目前SVNE方法主要分为两类。

1) 节点备份^[13-16]:在映射阶段,提前为该SFC提供备份的物理资源,若SFC失效可迅速切

换至备份物理资源上,从而保证服务的延续性,但该方法存在备份资源开销过大、物理资源利用率低等局限性。

2) 重映射^[17-19]:当物理节点失效时,将其上承载的VNF以及相关的虚拟链路进行重映射,从而保证SFC可以为用户继续提供正常的服务,但由于移动通信系统往往对时延具有严格的限制,而对虚拟节点进行重映射将造成一定时间的服务中断,无法很好地满足网络切片的业务需求。

然而,上述SVNE方法均假设网络中的所有节点都安全,未考虑实际应用环境的安全需求,如安全需求高的虚拟节点映射至安全性低的物理节点会增加节点被攻击失效的风险。本文参考虚拟网络中节点映射的信任机制研究^[10],针对网络切片存在的物理节点攻击失效问题,研究虚拟节点和物理节点之间的安全约束关系对网络入侵容忍能力的影响,提出了一种基于安全分级的网络切片备份与重映射方法。首先,在SFC映射之前,建立安全参数评估模型并对VNF的安全需求和物理节点的安全等级进行数值评分,根据VNF的安全需求大小选出部分VNF进行备份,减少备份VNF的数量;然后,在SFC映射时,按照虚拟节点和物理节点的安全参数值大小进行映射约束,降低网络中物理节点失效概率;最后,设计非备份节点的重映射方法,在满足网络切片时延要求下保证切片的高可靠性。

2 网络模型与安全参数的评估

2.1 网络模型

SFC映像模型如图1所示。

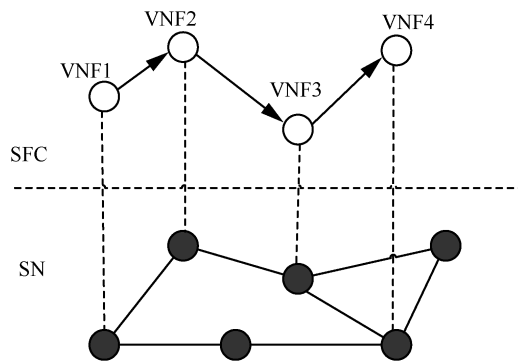


图1 SFC映像模型

1) 底层物理网络 (SN, substrate network)

通用的硬件设备平台组成底层物理网络, 表示为一个赋权无向图 $G^s = (N^s, L^s)$, 其中, N^s 、 L^s 分别表示物理服务器和物理链路的集合。对于每一个物理服务器 $u \in N^s$, 对应一个可用的 CPU 处理能力 $C(u)$ 。同样, 对于每个物理链路 $(u, v) \in L^s$, 对应一个可用的带宽资源 $B(u, v)$ 。

2) 服务功能链

特定 VNF 组成 SFC, 采用赋权有向图 $G^v = (N^v, L^v)$ 表示 SFC 中全部 VNF 节点及其关系的逻辑视图, N^v 表示 VNF 的逻辑节点集合, L^v 表示逻辑链路集合。

3) SFC 映射

虚拟化资源管理和编排模块根据 SFC 的请求信息和底层物理资源状况, 完成映射 $f: G^v \rightarrow G^s$ 。VNF 映射的空间维度优化采用的一般性方法为: 根据指定的目标函数设计相应的虚拟映射算法, 在空间维度找到 $f: G^v \rightarrow G^s$ 映射中 VNF 和虚拟链路所对应映像的最优位置。

2.2 节点的安全参数评估

对虚拟节点 $\bar{u}_i$ 引入安全需求参数 $\text{trd}(\bar{u}_i)$, 物理节点 u_i 引入安全等级参数 $\text{trd}(u_i)$, 安全参数的评估是一个复杂过程, 需要结合用户安全需求和具体服务功能进行。结合虚拟化网络环境的特点, 本文提出一种节点安全参数评估模型。

1) 虚拟节点 $\bar{u}_i$ 安全需求参数

首先对虚拟节点引入评估参量: 节点功能、节点中心度、物理资源需求, 对节点 $\bar{u}_i$ 的每个参量进行评分, 并用 0~1 之间的数字表示, 且各参量可评最大值的总和为 1。本文对 $\bar{u}_i$ 节点功能参量 $F(\bar{u}_i)$ 的评分范围为 0~0.4, $\bar{u}_i$ 若是用户面功能网元评 0.1 分, 控制面功能网元评 0.2 分, $\bar{u}_i$ 的信息处理量以低、中、高 3 个标准分别评 0 分、0.1 分、0.2 分, $F(\bar{u}_i)$ 为两项评分之和; 节点中心度参量 $D(\bar{u}_i)$ 评分范围为 0~0.3, 节点中心度反映与相邻节点的连接关系, 若 $\bar{u}_i$ 与 n 个虚拟节点连接, $D(\bar{u}_i)$ 评分标准见式(1); 物理资源需求参量 $R(\bar{u}_i)$ 评分范围为 0~0.3, 请求计算资源若低于网络平均值评 0.1 分, 高于平均值评 0.2 分, 请求存储资源若低于网络平均 $\text{trd}(\bar{u}_i)$ 值评 0, 高于平均值评 0.1 分, $R(\bar{u}_i)$ 为两项评分之和。

$$D(\bar{u}_i) = \begin{cases} \frac{n-1}{10}, & 1 \leq n \leq 4 \\ 0.3, & n > 4 \end{cases} \quad (1)$$

虚拟节点 $\bar{u}_i$ 安全需求参数 $\text{trd}(\bar{u}_i)$ 为上述评估参量之和。

$$\text{trd}(\bar{u}_i) = F(\bar{u}_i) + D(\bar{u}_i) + R(\bar{u}_i) \quad (2)$$

2) 物理节点 u_i 安全等级参数 $\text{trd}(u_i)$

首先对虚拟节点引入评估参量: 防火墙级别、数据加密级别以及系统异构性^[20], 对节点 u_i 的每个参量进行评分, 并用 0~1 之间的数字表示, 且各参量可评最大值的总和为 1。例如, 节点 u_i 的防火墙级别 $W(\bar{u}_i)$ 评分范围为 0~0.4, 数据加密级别 $E(\bar{u}_i)$ 评分范围为 0~0.3, 系统异构性 $S(\bar{u}_i)$ 评分范围为 0~0.3。系统异构性指服务器的操作系统与系统整体异同度, 若 u_i 的操作系统为多数服务器通用系统评 0.1 分, u_i 的操作系统为少部分服务器使用系统评 0.2 分, 为服务器专用操作系统评 0.3 分。物理节点 u_i 安全等级参数 $\text{trd}(u_i)$ 为上述评估参量之和。

$$\text{trd}(u_i) = W(u_i) + E(u_i) + S(u_i) \quad (3)$$

上述打分制度是安全评估模型的一种示例, 不同服务场景的网络切片可参考上述评估方法具体设置评估参量和评分标准。该评估模型符合网络切片适应多应用场景和灵活部署的需求。由安全参数评估模型可知, 安全需求越高的虚拟节点越容易被攻击者探测并发起攻击, 而安全等级越高的物理节点对攻击的防御能力更强。若虚拟节点 $\bar{u}_i$ 映射至物理节点 u_i , 为了降低攻击者挖掘系统漏洞阶段成功概率, 要求映射阶段满足安全约束

$$\text{trd}(\bar{u}_i) \leq \text{trd}(u_i) \quad (4)$$

基于节点的安全需求值, 根据用户安全要求选取需要进行备份的关键 VNF, 由用户安全需求对所需 SFC 确定参数 d , 虚拟节点 $\bar{u}_i$ 若满足

$$\text{trd}(\bar{u}_i) \geq d \quad (5)$$

则安全等级为高, 否则安全等级为低。由节点安全参数评估模型可知, 安全等级为高的这部分虚拟节点相对功能比较关键、相邻节点和链路多、请求资源大, 节点失效后若采用重映射方法难以保证在网络要求时间内成功完成映射, 故采用备份映射方案。安全等级为低的虚拟节点则可采用重映射方案, 以减少网络的物理资源开销。

3 基于安全分级的虚拟节点备份方法

高安全等级的虚拟节点失效时,需要能够迅速启用备份虚拟机继续提供服务,本节主要对备份映射过程建立数学模型并设计算法流程。

3.1 备份映射方法

虚拟节点备份映射方法如下:首先对安全等级为高的所有虚拟节点进行备份,如图2中节点b为高安全等级虚拟节点,由原服务功能链 G_i^v 得到增强服务功能链 G_i^w ,然后将增强服务功能链 G_i^w 映射至底层物理网络 G^s 。映射时满足资源需求的同时要求满足式(4)。当安全等级为高的虚拟机b失效时,快速切换至备份物理节点D继续为用户提供服务。

3.2 备份映射模型

1) 变量说明

$\alpha_u^{\bar{u}_i}$: 0-1 变量,当虚拟节点 $\bar{u}^i$ 映射到物理节点 u 上时, $\alpha_u^{\bar{u}_i}$ 为1,否则为0。

$\beta_{(u,v)}^{(\bar{u}_i,\bar{v}_i)}$: 0-1 变量,当虚拟链路 $(\bar{u},\bar{v})$ 映射到物理链路 (u,v) 上时, $\beta_{(u,v)}^{(\bar{u}_i,\bar{v}_i)}$ 为1,否则为0。

$\sigma_u^{\bar{u}_i}$: 0-1 变量,当虚拟节点 $\bar{u}^i$ 安全需求值 $trd(\bar{u}_i)$ 小于或等于物理节点安全等级值 $trl(u)$ 时, $\sigma_u^{\bar{u}_i}$ 为1,否则为0。

2) 约束条件

虚拟节点映射约束为

$$\sum_{u \in N^s} \alpha_u^{\bar{u}_i} = 1, \forall \bar{u}_i \in N_i^{vv}, \forall G_i^{vv} \in G^{vv} \quad (6)$$

$$\sum_{u \in N^s} \alpha_u^{\bar{u}_i} \leq 1, \forall u \in N^s, \forall G_i^{vv} \in G^{vv} \quad (7)$$

$$\sum_{u \in N^s} \sigma_u^{\bar{u}_i} \alpha_u^{\bar{u}_i} = 1, \forall \bar{u}_i \in N_i^{vv}, \forall G_i^{vv} \in G^{vv} \quad (8)$$

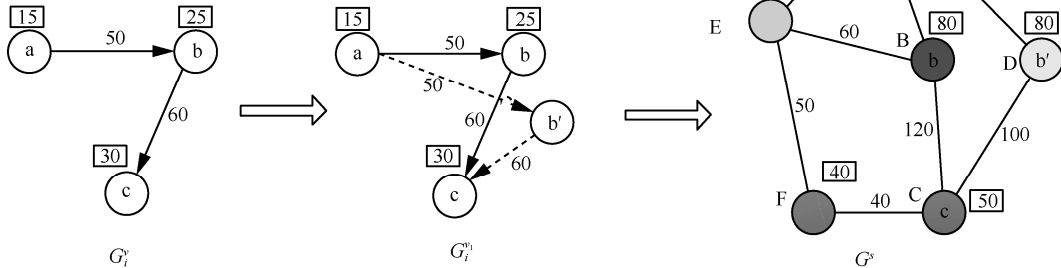


图2 基于安全分级的备份映射

$$\sum_{G_i^w \in G^w} \sum_{\bar{u}_i \in N_i^{vv}} C(\bar{u}_i) \alpha_u^{\bar{u}_i} \leq C(u), \forall u \in N^s \quad (9)$$

式(6)表示一个虚拟节点只能完整地映射到一个物理节点上;式(7)表示同一SFC中的不同虚拟节点不能映射到同一物理节点上;式(8)表示虚拟节点安全需求值小于或等于其映射至物理节点的安全等级值;式(9)表示一个物理节点上承载的所有虚拟机的CPU资源需求之和不能超过该物理节点的CPU资源。

虚拟链路映射约束为

$$\sum_{G_i^{vv} \in G^{vv}} \sum_{(\bar{u}_i,\bar{v}_i) \in L_i^{vv}} B(\bar{u}_i,\bar{v}_i) \beta_{(u,v)}^{(\bar{u}_i,\bar{v}_i)} \leq B(u,v), \forall (u,v) \in L^s \quad (10)$$

$$\sum_{v \in N(u)} \beta_{(u,v)}^{(\bar{u}_i,\bar{v}_i)} - \sum_{v \in N(u)} \beta_{(u,v)}^{(\bar{u}_i,\bar{v}_i)} = \alpha_u^{\bar{u}_i} - \alpha_u^{\bar{v}_i}, \forall \bar{u}_i, \bar{v}_i \in N_i^{vv}, \forall u \in N^s, \forall G_i^{vv} \in G^s \quad (11)$$

$$\sum_{(\bar{u}_i',\bar{v}_i') \in L_i^{vv}} \sum_{v \in N(u)} \beta_{(u,v)}^{(\bar{u}_i',\bar{v}_i')} = 0, \quad \text{if } \alpha_u^{\bar{u}_i} = 1, \forall u \in N^s, \forall G_i^{vv} \in G^s \quad (12)$$

式(10)表示一条物理链路上承载的所有虚拟链路的带宽资源需求之和不能超过该条物理链路的带宽资源;式(11)表示虚拟链路必须满足流约束条件;式(12)表示与备份虚拟机 $\bar{u}_i'$ 相关的备份虚拟链路 $(\bar{u}_i',\bar{v}_i')$ 不能经过虚拟机 $\bar{u}_i$ 所在的物理服务器。

3) 目标函数

在满足上述SFC的资源请求和安全需求条件下,以最小化映射成本为目标。

$$\min P(G_i^v) = \delta_i \sum_{\bar{u}_i \in N_i^{vv}} \alpha_u^{\bar{u}_i} (1 + trl(u_i)) C(\bar{u}_i) + \delta_B \sum_{(\bar{u}_i,\bar{v}_i) \in L_i^{vv}} \beta_{(u_i,v_i)}^{(\bar{u}_i,\bar{v}_i)} B(u_i,v_i) \quad (13)$$

SFC 映射成本主要分为两部分：虚拟节点映射调用的虚拟机资源成本和虚拟链路映射分配的物理链路带宽资源成本。其中，调用虚拟机成本包括物理主机 CPU 资源开销和安全成本。通过调节参数 d_i 和 δ_b 可调节目标函数中资源开销比重。

3.3 备份映射算法

以式(4)~(12)为约束条件，以式(13)最小化 SFC 的映射成本为目标，设计 SFC 备份映射算法，算法流程如下。

算法 1 基于安全分级的备份映射算法

输入 SFC 请求拓扑 $G_i^v = (N_i^v, L_i^v)$ ，物理网络拓扑 $G^s = (N^s, L^s)$ ，虚拟节点的安全等级分界值 d

输出 SFC 映射方案 $F_i: G_i^v \rightarrow G_i^s(N_i^s, L_i^s)$

1) **for each** $\bar{u}_i \in N_i^v$ **do**

if $trd(N_i^v) \geq d$ **then** $\bar{u}_i \in N_i^{v-high}$ //选择高安全需求虚拟节点

2) $N_i^{v'} = N_i^{v-high}$; $N_i^{vv} = N_i^v \cup N_i^{v'}$ //备份虚拟节点的集合；增强型服务功能链 G_i^{vv} 中 VNF 的集合

3) **for each** $\bar{u}_i \in N_i^{vv}$ **do**

4) $\bar{u}_i.mapping$; //虚拟节点映射

5) **for each** $u \in N^s$ **do**

6) **if** $u.ability \geq \bar{u}_i.requirement$

then //与已承载相邻虚拟节点的物理节点相距跳数升序寻找能够满足虚拟机映射资源及安全等级约束条件物理节点

7) **for each** $\bar{u}_i \in N_i^{v'}$ **then**

if $u'_i \notin N^s$ & $u'_i.ability \geq \bar{u}_i.requirement$ & $\alpha_{u'}^{\bar{u}_i} \cdot \alpha_{u'}^{\bar{u}_i} = 1$ //判断高安全等级虚拟节点是否满足备份约束

8) **continue**

9) **end if**

$\bar{u}_i.mapping = \text{true}$ and **break**

10) **end for**

11) $\bar{u}_i.mapping = \text{true}$ and **break**

12) **end if**

13) **end for**

14) **if** $\bar{u}_i.mapping = \text{false}$ **then** reject G_i^v and

return

15) **end if**

16) **end for**

17) $L_i^{v'} = L_i^v(N_i^{v'})$; $L_i^{vv} = L_i^v \cup L_i^{v'}$ //备份虚拟节点相关的虚拟链路的集合；增强型服务功能链 G_i^{vv} 中虚拟链路的集合

18) **for each** $(\bar{u}_i, \bar{v}_i) \in L_i^{vv}$ **do**

19) $(\bar{u}_i, \bar{v}_i).mapping$

20) **for each** $(u, v) \in L^s$ **do**

21) $P = \{path | (u, v).ability \geq (\bar{u}_i, \bar{v}_i).requirement, (u, v) \in L^s\}$ //满足虚拟链路 $(\bar{u}_i, \bar{v}_i)$ 所有物理路径的集合

22) 将集合 P 中元素按照跳数的大小进行升序排列；

23) **for** $i=1$ to $P.length$ **do**

24) **if** $(\bar{u}_i, \bar{v}_i) \in L_i^{v'}$ & $\alpha_{u'}^{\bar{u}_i} = 1$ **then** //判断是否是备份虚拟链路

25) **if** $\sum_{(\bar{u}_i', \bar{v}_i') \in L_i^{v'}} \sum_{v \in N(\bar{u}_i', \bar{v}_i')} \beta_{(u, v)}^{(\bar{u}_i', \bar{v}_i')} \neq 0$ **then** //备份虚拟链路 $(\bar{u}_i', \bar{v}_i')$ 是否经过虚拟机 $\bar{u}_i$ 所在的物理服务器

26) **continue** //若经过，则不选择该条路径，查看下一条物理路径

27) **end if**

28) **end if**

29) $\beta_{P[i]}^{(\bar{u}_i, \bar{v}_i)} = 1$ //满足目标函数的底层物理映射路径 $P[i]$

30) $(\bar{u}_i, \bar{v}_i).mapping = \text{true}$ and **break**

31) **if** $(\bar{u}_i, \bar{v}_i).mapping = \text{false}$ **then** reject G_i^v and **return**

32) **end if**

33) **end for**

34) **end for**

35) **end for**

在本文服务功能链部署模型中，设虚拟节点数量为 n ，底层物理网络节点数量为 m 。在节点映射阶段，首先虚拟节点按照安全需求参数选取高安全等级节点，优先满足高安全需求节点及备份节点的映射要求，且依次选取已映射节点相邻较高安全需求的未映射节点进行映射，节点映射的计算复杂度为 $O(nm)$ ，在链路映射阶段，根据 K 最短路径算法思想选取符合要求的最短路径，链路映射的计算复杂度为 $O(nm^2)$ ，故映射算法的计算复杂度为 $O(nm^2)$ 。

4 基于安全分级的虚拟节点重映射方法

对于低安全等级的虚拟节点失效时需要进行重映射过程,本节主要对重映射过程建立数学模型并设计算法流程。

4.1 重映射方法

虚拟节点的重映射方法:当安全等级为低的虚拟节点失效时,如图2中的虚拟节点a失效,可将虚拟节点a重映射至物理节点E。为保证不影响用户使用体验,可在不满足式(4)条件下进行对虚拟机的重映射:一是该节点本身安全需求度不高,二是减少重映射算法收敛时间。

4.2 重映射模型

1) 变量说明

$\alpha_{u_i}^{\bar{u}_i}(t)$:0-1 变量,虚拟节点 $\bar{u}_i$ 映射至物理节点 u_i 上,在 t 时刻,节点 u_i 正常工作时变量为0,节点 u_i 失效时变量为1。

2) 约束条件

虚拟节点失效进行重映射时,也需要满足式(5)~(7)和式(9)~(12)的映射约束条件,虚拟节点失效与其他虚拟节点是否失效是独立事件,低安全等级虚拟节点重映射过程会带来短暂服务中断。为满足正常服务时延要求,对映射目标节点的安全等级不做约束,但对确定目标节点时间进行约束,即最大映射算法收敛时间不超过 τ 。即

$$\alpha_{u_i}^{\bar{u}_i}(t+\tau)=0, \alpha_{u_i}^{\bar{u}_i}(t)=1, \forall \bar{u}_i \in N_i^{vv}, \forall G_i^{vv} \in G^{vv} \quad (14)$$

3) 映射目标

在有限映射时间内仍以最小化SFC的映射成本为目标。

$$\min \sum_{(\bar{u}_i, \bar{v}_i) \in L_i^{vv}} \beta_{(u_i, v_i)}^{(\bar{u}_i, \bar{v}_i)} B(u_i, v_i), \forall G_i^{vv} \in G^{vv} \quad (15)$$

因重映射过程不考虑安全约束,且重映射虚拟节点的节点物理资源是固定的,因此本文将最小化虚拟链路的带宽资源开销作为重映射的目标函数。

4.3 重映射算法

以式(5)~式(7)、式(9)~式(12)、式(14)为约束条件,以式(15)最小化SFC的映射成本为目标,设计节点重映射算法,算法流程如下。

算法2 基于安全分级的虚拟节点重映射算法

输入 物理网络拓扑 $G^s = (N^s, L^s)$

输出 虚拟机重映射方案 *Remapping*

```

1)  $Q' \leftarrow$  虚拟节点集合  $N_i^v$  按照安全需求值的大小进行升序排列;  $N_i^{v-low} = Q[1: \text{number}(\text{trd}(N_i^v) < d)]$  //低安全等级虚拟节点的集合
2) if work( $u$ ) == false &&  $\alpha_u^{\bar{u}} = 1$  &&  $\bar{u} \in N_i^{v-low}$  do //承载低安全等级的物理节点失效,对映射在该物理主机上的虚拟机 $\bar{u}$ 进行重映射
3) for each  $\bar{u}_i \in \text{locate}(u)$  do
4) 对位于物理主机 $u$ 上所有虚拟机放到集合 $Q$ 中
5) for ( $i=0$ ;  $i < \text{length}(Q)$ ;  $i++$ ) do
6) if ((remapping_security( $Q[i]$ ) == true) && (remapping_node( $Q[i]$ ) == true) && (remapping_links( $Q[i]$ ) == true)) then //重映射物理主机是否满足安全等级要求、虚拟机资源需求、虚拟链路资源需求
while (remapping_time  $\leq \tau$ )
7) remapping_cost( $Q[i]$ ) == min{remapping_cost( $N^s$ )} //在重映射允许时间内最小映射开销
8) end if
9) end for
10) end for
11) end if

```

在单物理节点失效时,物理节点之上所承载的虚拟机在约束时间 τ 内找到迁移开销最小且满足约束条件的虚拟节点,满足贪婪算法的思想,寻找迁移节点算法的计算复杂度为 $O(m)$,计算最小迁移开销路径的计算复杂度为 $O(m^2)$,故重映射算法的计算复杂度为 $O(m^2)$ 。

5 仿真实验

5.1 实验环境

本实验采用GT-ITM工具生成SFC及底层物理网络拓扑,采用C++编程语言实现备份和映射算法,并利用Matlab工具对实验结果进行分析。本次实验选取物理网络拓扑如图3所示,其中,物理节点有15个,物理链路24条。物理网络中的节点计算资源($300 \leq C \leq 500$)、链路的带宽资源($150 \leq B \leq 350$)为固定值,保证SFC映射过程中物理拓扑基本环境一致。每条SFC中虚拟节点数目服从[4, 6]的整数随机均匀分布,物理节点

的安全等级服从 $[0.3, 0.9]$ 之间的随机均匀分布, 虚拟节点安全需求服从 $[0.2, 0.8]$ 之间的随机均匀分布。安全分级参数 $d=0.7$ 。

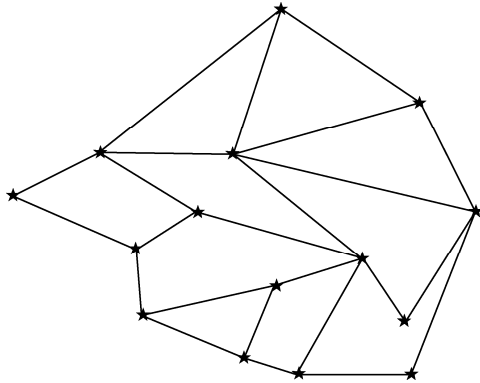


图 3 物理网络拓扑

实验以文献[12]、文献[13]和本文提出的方法进行对比。其中, 文献[12]是对所有的虚拟节点进行备份映像, 为便于描述, 本文用 SVNE 表示该方法; 文献[13]是对关键虚拟节点进行映射, 本文用 Pio-SVNE (pivotal-SVNE) 表示该方法; 基于安全分级的备份方法用 Sec-SVNE (Security-SVNE) 表示。

5.2 实验结果分析

实验从 SFC 的映射资源开销、映射成功率和网络安全性能方面对 SVNE, Pio-SVNE 和 Sec-SVNE 这 3 种方法的性能进行对比分析。

5.2.1 SFC 的映射资源开销

设置资源需求强度 Traffic 服从 $[100, 500]$ 的均匀分布, SFC 的节点计算资源与带宽资源需求与 Traffic 成正比。图 4 的实验仿真是随着 SFC 的资源需求强度变化, 不同备份映射方法的资源开销结果, 其中资源开销为

$$C = \delta_t \sum_{\bar{u}_i \in N_i^{vv}} \alpha_{\bar{u}_i} C(\bar{u}_i) + \delta_B \sum_{(\bar{u}_i, \bar{v}_i) \in L_i^{vv}} \beta_{(\bar{u}_i, \bar{v}_i)} B(u_i, v_i) \quad (16)$$

由图中可以看出, 3 种方案中的相同 Traffic 下资源开销 $\text{Pio-SVNE} < \text{Sec-SVNE} < \text{SVNE}$, 由于 SVNE 方法采用全备份方案, 所以资源开销远大于其他 2 种方案, Pio-SVNE、Sec-SVNE 方案中当虚拟节点 $\bar{u}_i$ 的安全需求参数 $\text{trd}(\bar{u}_i) \geq d$ 时对节点进行备份, 实验数据结果表明 Sec-SVNE 的平均资源开销比 Pio-SVNE 高 6.13%, 原因是 Sec-SVNE 方法映射过程中需要满足节点的安全约束。

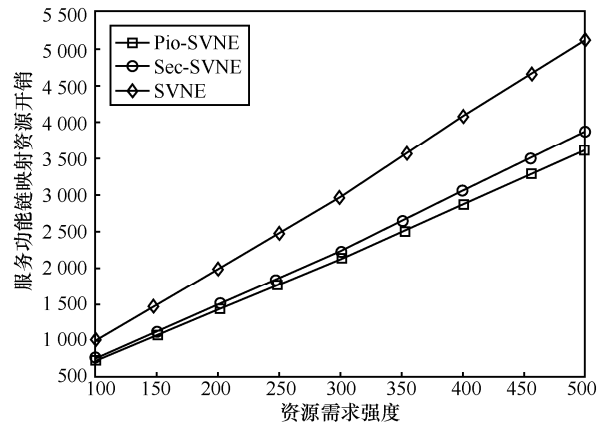


图 4 映射资源开销对比

5.2.2 SFC 的映射成功率

设置每次 SFC 请求的计算资源服从 $[3, 8]$ 的整数随机均匀分布, 带宽资源服从 $[1, 6]$ 的整数随机均匀, 单位时间内 SFC 的映射请求数量服从 $[0, 120]$ 的整数随机均匀。图 5 给出单位时间内的映射请求数量与 SFC 映射成功率的关系, 由图中结果分析可知, 相同单位时间的映射请求量, 请求成功率 $\text{SVNE} \leq \text{Sec-SVNE} \leq \text{Pio-SVNE}$, 在请求数量大于 40 时 SVNE 的映射成功率快速下降, 物理网络承载接近饱和。单位时间 SFC 请求数量到 120 时, Sec-SVNE 和 Pio-SVNE 方法映射的物理网络都接近饱和。而 Sec-SVNE 方式在映像量为 120 左右时, 比 Pio-SVNE 方法映射成功率降低了 5%~8%, 平均映像成功率下降了 3.77%。

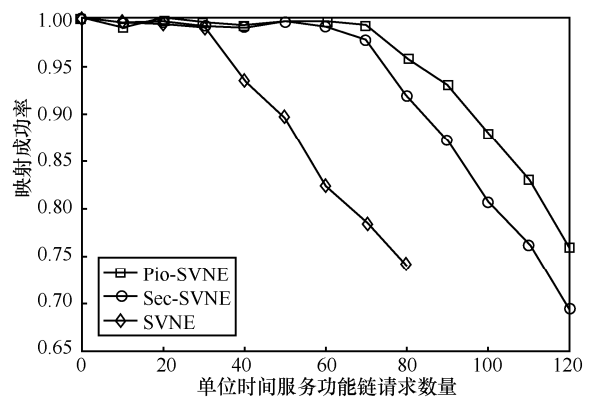


图 5 映射成功率对比

5.2.3 网络安全性能分析

由上文可知, 对攻击者来说, 完成攻击挖掘系统漏洞阶段往往需要花费大量时间, 本节实验把物理节点可持续承受漏洞挖掘的时间作为度量节点安全性能的标准, 物理节点的安全等级与节

点可承受漏洞挖掘攻击的难度和时间成正比, 所以将节点漏洞挖掘时间表示为

$$T = t \frac{\sum_{u_i \in N_i^{high}} trl(u_i)}{n}, n \neq 0 \quad (17)$$

其中, T 表示攻击者对一个 SFC 请求中高安全等级需求的虚拟节点成功进行漏洞挖掘需要的平均时间, t 为一个正数常数, n 为此 SFC 中高安全等级节点数目。令 $t=1$, 仿真实验得到第 i 个 SFC 映射请求对应的节点漏洞挖掘时间 T 如图 6 所示。对实验数据计算表明, Sec-SVNE 的映射方法比 Pio-SVNE 的高安全需求节点的漏洞挖掘时间平均提高了 23.02%, 明显提高了网络的入侵容忍能力。

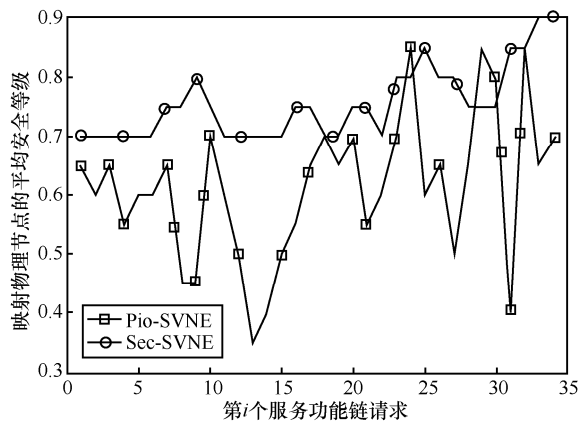


图 6 网络安全性能对比

6 结束语

对于未来 5G 核心网虚拟化云环境中单个物理节点失效问题, 目前主要有节点备份方法和重映射方法, 但当前的解决方案未考虑虚拟节点与物理节点之间的安全映射关系, 本文提出基于安全分级的网络切片节点备份与重映射方法。首先建立虚拟节点的安全需求参数和物理节点的安全等级参数的评估模型; 然后基于安全需求参数选择关键虚拟节点进行备份以减少物理资源开销, 建立虚拟节点与物理节点的安全约束映射以增加关键虚拟节点攻击失效的难度; 最后设计非备份节点的重映射方法保证节点失效造成服务中断时间满足网络时延要求。仿真实验表明, 本文的 sec-SVNE 方法虽比 Pio-SVNE 方法平均资源开销提高了 6.13%, 平均映像成功率下降了 3.77%,

但攻击者对关键节点的漏洞挖掘时间成本提高了 23.02%, 所以该方案能够在满足网络切片的可靠性和时延要求下较大地提升网络的入侵容忍能力。

参考文献:

- [1] 3GPP SA. 3rd generation partnership project service and system aspects[EB/OL]. <http://www.3gpp.org/specifications-groups/>.2017.9.
- [2] ORDONEZ-LUCENA J, AMEIGEIRAS P, LOPEZ D, et al. Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges[J]. IEEE Communications Magazine, 2017, 55(5): 80-87.
- [3] CHOYI V K, ABDEL-HAMID A, SHAH Y, et al. Network slice selection, assignment and routing within 5G networks[C]//Standards for Communications and NETWORKING. 2016: 1-7.
- [4] CHATRAS B, KWONG U S T, BIHANNIC N. NFV enabling network slicing for 5G[C]//Innovations in Clouds, Internet and Networks. 2017.
- [5] ORDONEZ-LUCENA J, AMEIGEIRAS P, LOPEZ D, et al. Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges[J]. IEEE Communications Magazine, 2017, 55(5):80-87.
- [6] HAN B, GOPALAKRISHNAN V, JI L, et al. Network function virtualization: challenges and opportunities for innovations[J]. IEEE Communications Magazine, 2015, 53(2):90-97.
- [7] HERRERA J G, BOTERO J F. Resource allocation in NFV: a comprehensive survey[M]. IEEE Press, 2016, 13 (3) :518-532.
- [8] BASTA A, KELLERER W, HOFFMANN M, et al. A virtual SDN-enabled LTE EPC architecture: a case study for S/P gateways functions[C]//IEEE Future Networks and Services. 2013: 1-7.
- [9] 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.
- [10] 龚水清, 陈靖, 黄聪会, 等. 信任感知的安全虚拟网络映射算法[J]. 通信学报, 2015, 36(11):180-189.
GONG S Q, JING J, HUANG C H, et al. Trust-aware secure virtual network embedding algorithm[J]. Journal on Communications, 2015, 36(11):180-189.
- [11] HERKER S, KHAN A, AN X. Survey on survivable virtual network embedding problem and solutions[C]// International Conference on Networking and Services (ICNS).2013:99-104.
- [12] RAHMAN M R, BOUTABA R. SVNE: survivable virtual network embedding algorithms for network virtualization[J]. IEEE Transactions on Network & Service Management, 2013, 10(2):105-118.
- [13] CHOWDHURY S R, AHMED R, KHAN M A, et al. Protecting virtual networks with drone[C]//Network Operations and Manage-

- ment Symposium (NOMS), IEEE/IFIP. 2016: 78-86.
- [14] CHOWDHURY S R, AHMED R, KHAN M M A, et al. Dedicated protection for survivable virtual network embedding[J]. IEEE Transactions on Network and Service Management, 2016, 13(4): 913-926.
- [15] ZHANG Q, ZHANI M F, JABRI M, et al. Venice: reliable virtual data center embedding in clouds[C]//INFOCOM, Proceedings IEEE. 2014: 289-297.
- [16] JARRAY A, KARMOUCH A. Cost-efficient mapping for fault-tolerant virtual networks[J]. IEEE Transactions on Computers, 2015, 64(3): 668-681.
- [17] SHAHRIAR N, AHMED R, KHAN A, et al. ReNoVatE: recovery from node failure in virtual network embedding[C]. Network and Service Management (CNSM). 2016: 19-27.
- [18] SHAHRIAR N, AHMED R, CHOWDHURY S, et al. Generalized recovery from node failure in virtual network embedding[J]. IEEE Transactions on Network & Service Management, 2017, (99): 1-1.
- [19] YU H, ANAND V, QIAO C, et al. Migration based protection for virtual infrastructure survivability for link failure[C]//2011 and the National Fiber Optic Engineers Conference on Optical Fiber Communication Conference and Exposition (OFC/NFOEC). 2011: 1-3.
- [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.

JI X S, ZHAO S, AI J J, et al. Research on heterogeneous-backup virtual network embedding[J]. JEIT, 2018, 40(5): 1087-1093.

[作者简介]



孙志勇（1994-），男，河南濮阳人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为新一代移动通信网络技术、移动通信网络安全。

季新生（1968-），男，江苏南通人，国家数字交换系统工程技术中心教授、博士生导师，主要研究方向为网络空间安全、拟态安全。

游伟（1984-），男，江西丰城人，国家数字交换系统工程技术中心讲师，主要研究方向为新一代移动通信网络技术、移动通信网络安全。

袁泉（1991-），男，山东青岛人，国家数字交换系统工程技术博士生，主要研究方向为新一代移动通信网络技术、网络功能虚拟化。