基于安全感知的网络切片部署策略

吴　玄[1]，姬伟峰[1]，翁　江[1]，李映岐[1]，申秀雨[1]，孙　岩[2]
（1.空军工程大学信息与导航学院，西安，710077；2.95007 部队，广州，510080）

摘要　针对网络切片的安全部署问题，提出一种基于安全感知的网络切片部署策略。在网络切片部署阶段，先进行虚拟网络功能（VNF）映射，从安全需求的角度定义 VNF 与物理节点之间的安全约束条件；其次，提取切片部署过程中物理节点的安全特征矩阵，利用策略网络输出安全特征矩阵的概率分布并进行排序；最后，采用基于策略的强化学习方法求解 VNF 的映射结果。当 VNF 映射完成后，采用 Dijkstra 算法进行虚拟链路映射，得到网络切片安全部署结果。仿真结果表明，所提策略在长期收益开销比、请求接受率、网络资源利用率、带宽利用率与运行时间上均优于 GRC、VNE-RL 与 SVNE-RL 算法，且保证了部署过程中网络切片的安全需求。

关键词　网络切片；策略网络；强化学习；安全感知
DOI　10.3969/j.issn.2097-1915.2022.04.015
中图分类号　TP393.01　　**文献标志码**　A　　**文章编号**　2097-1915(2022)04-0096-07

A Network Slice Deployment Method Based on Security Perception

WU Xuan[1], JI Weifeng[1], WENG Jiang[1], LI Yingqi[1], SHEN Xiuyu[1], SUN Yan[2]
(1. Information and Navigation School, Air Force Engineering University, Xi'an 710177, China;
2. Unit 95007, Guangzhou 510080, China)

Abstract　In view of security deployment of network slices, a network slice deployment strategy based on security awareness is proposed. In the network slice deployment phase, virtual network functions (VNF) are mapped first, and security constraints between VNF and physical nodes are defined from the perspective of security requirements. Secondly, the security feature matrix of physical nodes in the slicing deployment process is extracted, and the probability distribution of the security feature matrix is output by the policy network and sorted. Finally, the strategy-based reinforcement learning is utilized for solving the mapping results of VNF. After the VNF mapping is complete, the Dijkstra algorithm is used to map virtual links to obtain the security deployment result of network slices. The simulation results show that the proposed strategy is superior to GRC and SVNE-RL algorithms in terms of long-term cost-benefit ratio, request acceptance rate, network resource utilization, bandwidth utilization and time complexity, and can meet the security requirements of network slicing during deployment.

Key words　network slicing; policy network; reinforcement learning; security perception

收稿日期：2021-12-21
基金项目：国家自然科学基金(61902426)；中国博士后科学基金(2021M692502)
作者简介：吴　玄(1998—)，男，安徽阜阳人，硕士生，研究方向为网络切片安全。E-mail:1766300243@qq.com

引用格式：吴玄，姬伟峰，翁江，等. 基于安全感知的网络切片部署策略[J]. 空军工程大学学报，2022，23(4)：96-102. WU Xuan, JI Weifeng, WENG Jiang, et al. A Network Slice Deployment Method Based on Security Perception[J]. Journal of Air Force Engineering University, 2022, 23(4): 96-102.

5G 旨在使用相同的网络基础设施为每个垂直行业提供定制业务需求，实现“万物互联”的愿景[1]。为满足不同垂直行业的业务需求，提出了网络切片(network slicing，NS)的概念，网络切片由多个异构虚拟网络构成，能够同时为多用户提供端到端定制化的虚拟网络服务。但网络切片在部署时，存在一系列安全问题，例如恶意节点对共享资源的网络切片发动侧信道攻击、存在漏洞的终端设备容易遭受底层网络攻击、网络切片服务在分布式拒绝服务攻击中变成中间跳板。同时，每个网络切片实例(network slice instance，NSI)都有资源配额，恶意用户可能会试图滥用资源配额，从而中断该切片的服务[2]。因此，网络切片安全部署策略研究对 5G 网络应用具有重要现实意义。

网络切片安全部署本质上是对 NSI 中的虚拟网络功能(virtual network f unction，VNF)进行部署与编排[3]。文献[4]提出了 5G 网络切片安全信任部署策略，采用网络切片安全部署的启发式算法有效解决了网络切片信任中的随机性、模糊性以及不确定性问题；文献[5]提出了基于信息熵的安全感知虚拟网络映射算法，利用信息熵 TOPSIS(technique for order preference by similarity to an ideal solution)对物理节点的重要性进行排序，以部署成本作为最小优化目标，在长期平均收益、长期收益成本比与运行时长方面取得了较好的效果；文献[6]提出了一种基于全局资源能力(global resource capacity)的虚拟网络映射算法，该算法通过考虑节点的资源属性和全局拓扑属性对节点部署进行优化，并采用蒙特卡洛算法求解映射结果获得了更高的请求接受率与部署收益；文献[7]提出了一种基于强化学习的虚拟网络映射算法(virtual network Embedding-Reinforcement learning，VNE-RL)，该算法未考虑部署过程中节点与链路的安全因素，根据节点的重要性程度进行排序与映射，在长期收益成本比与算法效率上得到了较好的提升，但其对全局资源感知程度不高；文献[8]提出了一种基于强化学习的安全虚拟网络映射算法(security virtual network embedding-Reinforcement learning，SVNE-RL)，该算法考虑了节点的安全因素，利用强化学习求解节点映射过程，在长期平均收益、长期收益消耗率与请求接受率方面提升较大，但该算法未考虑链路安全约束条件，且对节点的安全性考虑不够充分。

目前网络切片部署的安全需求主要考虑节点的安全因素与资源的重要性程度，未考虑到链路对网络切片部署过程中的影响。并且部署方法主要采用启发式算法与强化学习方法，但传统的启发式算法易陷入局部最优解[9]，无法感知底层物理资源变化情况，导致资源利用率低，而强化学习算法，存在评价策略时效率较低且方差较大等问题。

针对网络切片部署的安全需求与部署方法存在的问题，本文提出了一种基于强化学习的安全感知网络切片部署策略(security aware network slicing-reinforcement learning，SANS-RL)。在部署过程中利用安全等级与安全需求有效量化分析 VNF 和链路的安全性，采用带有基线算法的强化学习方法，对物理节点的安全性进行排序，实现对安全等级较高 VNF 的优先部署与重点保护。实验仿真表明本文所提出的 SANS-RL 策略比 GRC、VNE-RL 与 SVNE-RL 映射效率更高，同时保证了网络切片部署过程中的性能与安全需求。

1. 网络切片部署模型

1.1 安全部署需求描述

NSI 是一个专用的虚拟网络，VNF 按照一定约束顺序组成服务功能链(service function chain，SFC)，不同 SFC 组合构成 NSI，物理网络为 NSI 提供服务资源。NSI 到物理网络的映射过程称为网络切片实例部署，即将 VNF 映射到物理节点上，将虚拟链路映射到一组物理链路上[10]，图 1 为网络切片部署示意图。

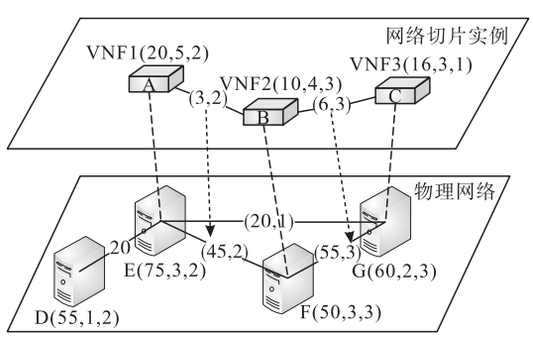

图 1　网络切片部署示意图

为了量化与描述网络切片的安全需求，引入安全等级这一概念。安全等级表示抽象的保护标准，由 5G 网络运营商分配，安全等级越高，其提供的安全机制越多。例如，支持数据加密和数字签名的物理节点将被分配更高的安全等级。因此，某些特殊的需求会被分配到同等或更高安全级别的资源上。

基于以上假设，本文得出以下 4 个抽象的安全约束。

1)物理节点的安全等级不能低于部署在其上的 VNF 安全需求。

2)VNF 的安全等级不能低于其映射到物理节

点的安全需求。

3)在已部署 VNF 的物理节点上部署新的 VNF 时,新 VNF 的安全需求不得低于已部署 VNF 的安全需求。

4)具有一定安全需求的虚拟链路应映射到具有足够安全级别的物理链路上。

图 1 中网络切片请求中 A 的属性值代表其所需 CPU 资源为 20、自身的安全等级为 5、需要物理节点对应的安全级别不低于 2,A 和 B 之间虚拟链路属性值代表其所需带宽资源为 3,需要对应的物理链路安全级别不低于 2,物理节点 E 的属性值代表其能够提供的 CPU 资源为 75、自身的安全等级为 3、需要部署在其上的 VNF 安全级别不低于 2。VNF 只能映射到满足其资源需求与安全需求的物理服务器上,虚拟链路只能映射到满足其带宽需求与安全需求的物理链路上。

1.2 安全部署模型描述

本文使用有权无向图 $G_P=(N_P,L_P,N_S,L_S)$ 来表示 5G 物理网络拓扑。物理网络中物理节点(物理服务器、交换机、路由器等设备集合)用 N_P 表示,而 L_P 表示节点之间的所有物理链路集合,N_S 与 L_S 表示物理节点与物理链路的属性值。其中 $N_S=\{cpu(n_s),dem(n_s),lev(n_s)\}$,$L_S=\{bw(l_p),lev(l_p)\}$,$dem$ 表示物理节点的安全需求,lev 表示物理节点与物理链路的安全等级,cpu 表示物理节点可用的 CPU 资源,bw 表示物理链路的可用的带宽资源。

网络切片请求用一个有向图 $G_V=(N_V,L_v,T_B,N_S^V,L_S^V)$ 表示,T_b 表示网络切片请求持续时间,N_V 表示 VNF 集合,L_V 表示虚拟链路集合,N_S^V 与 L_S^V 分别表示 VNF 属性与虚拟链路属性,其中 $N_S^V=\{cpu(n_v),dem(n_v),lev(n_v),L_S^V\{bw(l_v),dem(l_v)$,$dem$ 表示 VNF 与虚拟链路的安全需求,lev 表示 VNF 的安全等级,cpu 表示 VNF 需要的 CPU 资源,bw 表示虚拟链路需要的带宽资源。

1.3 网络切片部署过程描述

网络切片安全部署到基础设施网络中可以认为是典型的安全虚拟网络映射问题(secure virtual network embedding , SVNE)[11]。类似于 SVNE 问题,本文将网络切片部署过程分为 2 个阶段:VNF 映射与虚拟链路映射。

在 VNF 映射过程中,一个 VNF 只能映射到一个物理节点中,定义第 i 个 VNF 映射到第 k 个物理节点上,表示为 x_k^i,映射成功值为 1,否则为 0,即 $x_k^i\in\{0,1\}$,同时所有 VNF 应全部部署到物理网络上,如式(1)所示:

$$\sum_{k\in N^p}x_k^i=1,\forall i\in N_P \tag{1}$$

物理节点所分配的 CPU 资源不能超过其自身拥有的 CPU 的资源,其中 $cpu(x^i)$ 表示第 i 个 VNF 所需的 CPU 资源,$cpu(x_k)$ 表示物理节点 k 剩余的 CPU 资源,如式(2)所示:

$$X_k^i cpu(x^i)\leqslant cpu(x_k)\ \forall k\in N_P \tag{2}$$

物理链路分配带宽不能超过链路总带宽,其中 $bw(L_{uv}^{ij})$ 表示物理链路(u,v)分配给虚拟链路(i,j)的带宽资源,$bw(l_{uv})$ 表示物理链路(u,v)剩余的带宽资源,如式(3)所示:

$$bw(L_{uv}^{ij})\leqslant bw(L_{uv}) \tag{3}$$

上文中的安全约束条件如式(4~7)所示:

$$X_k^i dem(n_p)\leqslant lev(n_v) \tag{4}$$

$$X_k^i dem(n_p)\leqslant lev(l_p) \tag{5}$$

$$\begin{cases}\max\{dem(n_p),\max dem(n_v)\}\leqslant\\ \min\{lev(n_p),\min lev(n_v)\}\end{cases} \tag{6}$$

$$dem(l_v)\leqslant lev(l_p) \tag{7}$$

1.4 评价指标

本文以 VNF 部署的长期安全收益成本比、请求接受率、长期网络资源利用率与长期带宽利用率等 4 个方面对算法进行评价[12]。

1.4.1.长期安全收益成本比

对于 VNF 的部署收益,用节点与链路的安全收益情况表示,如式(8)所示:

$$R(G_V)=(\sum_{n_s\in N_s}\sum_{n_v\in N_v}dem(n_s)cpu(n_v)+\sum_{l_s\in L_s}\sum_{l_v\in L_V}lev(l_s)bw(l_v)T_b \tag{8}$$

式中:$dem(n_s)cpu(n_v)$代表 VNF 的安全收益,VNF 映射在安全需求越高的物理节点上,其部署安全收益越大;$lev(l_s)bw(l_v)$代表链路的安全收益,虚拟链路映射在安全等级越高的物理链路上,其部署安全收益越大;T_b 表示 VNF 请求持续时长。

VNF 部署成本如式(9)所示[13]:

$$H(G_V)=(\sum_{n_v\in N_v}lev(n_v)cpu(n_v))+\sum_{l_v\in L_v}\sum_{p\in P_S(l_v)} \tag{9}$$

式中:$lev(n_v)cpu(n_v)$代表 VNF 映射的部署成本,VNF 映射所需 cpu 资源越多,安全等级越大,其部署成本越高。$dem(l_v)hop(p)bw(l_v)$表示虚拟网络链路能源消耗,其中 $P_s(l_v)$表示虚拟链路 l_v 分配的路径集合,$hop(p)$表示路径 p 在物理网络上经过的跳数,虚拟链路映射所需带宽资源越多、链路跳数越大、虚拟链路的安全需求越高,其部署成本越大。

长期安全收益成本比可以表示为:

$$RC = \lim_{T\to\infty} \frac{\sum_{i=0}^{G} R^i(G_V)}{\sum_{t=1}^{G} H^i(G_V)} \tag{10}$$

1.4.2　请求接受率

VNF 请求接受率可以表示为：

$$ACC = \frac{\sum_{t=0}^{T_b} T_s}{\sum_{t=0}^{T_b} T} \tag{11}$$

式中：T 表示在 VNF 请求持续时间 T_b 内 VNF 请求的总个数，而 T_s 表示在 VNF 请求持续时间 T_b 内 VNF 请求成功映射的个数。

1.4.3　长期网络资源利用率

长期网络资源利用率可以表示为：

$$ACU = \frac{\sum_{t=0}^{T_b} C_s}{C} \tag{12}$$

式中：C 表示物理网络总 CPU 资源；C_s 表示在 VNF 请求持续时间内已消耗的 CPU 资源总量。

1.4.4　长期带宽资源利用率

长期带宽资源利用率可以表示为：

$$NBU = \sum_{t=0}^{T_b} \frac{B_s}{B} \tag{13}$$

式中：B 表示物理网络总带宽资源；B_s 表示在 VNF 请求持续时间内已消耗的带宽资源总量。

2　基于强化学习的网络切片部署策略

在 VNF 映射到物理节点过程中，物理节点存在的安全风险将会影响整个网络切片的部署。因此，通过建立物理节点的安全特征矩阵，确保网络切片的安全部署。

2.1　节点安全特征矩阵

提取物理节点的安全特征属性，包括节点计算资源、节点的度、度中心性、节点中心度与节点的安全因子。

1）节点计算资源（node computing resources）。节点计算能力是表征节点效率重要属性之一，节点计算能力越强，其承受的 VNF 越多，被映射的概率就越大，物理节点 n_k 计算资源如式(14)所示：

$$NCR(n_k) = cpu(n_k) \tag{14}$$

2）节点的度（the degree of node），节点的度表示连接到物理节点的链路数量，节点的度越大，其连接的节点就越多，更易于找到与其他节点之间较短的链路，物理节点 n_k 的度如式(15)所示：

$$DN(n_k) = \sum_{n_k \in N_p} B_{ij} \tag{15}$$

式中：B_{ij} 表示节点 n_k 与其相邻节点的连接关系，如果互相连接则为 1，否则为 0。

3）度中心性（degree of centricity）[14]，物理节点上所链接链路的带宽之和，总带宽越大，映射到物理节点的 VNF 链路选项越多，映射效果越好。物理节点 n_k 度中心性如式(16)所示：

$$DC(n_k) = \sum_{n_k \in N_P} bw(n_{ij}) \tag{16}$$

4）节点中心度[15]（the centrality of node）能够全局网络结构反映物理节点的重要程度，物理节点 n_k 中心度如式(17)所示：

$$CN(n_k) = \frac{1}{n_k \in N_P} O_{kj} \tag{17}$$

式中：O_{kj} 表示物理节点 n_k 与 n_j 之间的跳数；N_P 表示为满足约束条件的所有物理节点，节点中心度越大，物理节点越接近网络中心，物理节点越重要。

5）节点的安全评估因子。节点的安全评估因子是衡量节点整体安全性的重要指标，由节点计算资源、节点的度、度中心性、节点中心度与节点的安全需求共同组成，节点的安全评估因子越高，其安全性越好，应考虑对对其优先部署，并防止安全性较低的网络切片共享节点而导致的同驻攻击，物理节点 n_k 安全评估因子如式(18)所示：

$$SAF(n_k) = (NCR(n_k) + DN(n_k) +) DC(n_k) + CN(n_k))^* dem(n_k)/4 \tag{18}$$

本文利用节点的安全特征属性建立节点安全特征向量。物理节点 n_k^p 的安全特征向量 $\boldsymbol{sav}$（security attribute vector，SAV）如式(19)所示：

$$\boldsymbol{sav}_k^p (NCR_k^p, DN_k^p, DC_k^p, CN_k^p, SAF_k^p)^{\mathrm{T}} \tag{19}$$

物理节点的安全特征矩阵 $\boldsymbol{SE}$（safety eigenmatrix，SE）如式(20)所示：

$$\boldsymbol{SE} = (\boldsymbol{sav}_1, \boldsymbol{sav}_2, \cdots, \boldsymbol{sav}_n)^{\mathrm{T}} \tag{20}$$

2.2　基于策略的网络切片部署建模

网络切片的部署问题是一个 NP 难问题，相比于传统启发式算法与精确式算法求解 VNF 映射过程，机器学习算法可以根据现有数据智能调整网络参数，并做出预测。而强化学习（reinforcement learning，RL）作为一种机器学习算法，具有自适应的特点，通过与 Agent 与环境的相互作用，执行特定的动作，更新状态获取奖励，RL 能够充分感知 VNF 映射过程中的安全状态信息，在网络切片部署过程中取得更好的资源利用率。

本文将网络切片请求中的 VNF 映射过程建模为带有状态空间的 MDP $M(S, A, P, R)$ 过程[16]，具体表示为：利用物理节点的安全特征矩阵作为环境，Agent 定义为一个能够输出物理节点映射概率的策略网络，Agent 根据物理节点的安全特征矩阵输出物理节点映射概率，然后选择概率最大的物理节点作为动作，进行 VNF 映射，当 VNF 映射完成后，使

用 Dijkstra 算法进行链路映射，以长期收入消费比作为奖励函数，根据学习策略情况给予 Agent 奖励，同时更新状态信息，VNF 映射模型如图 2 所示。

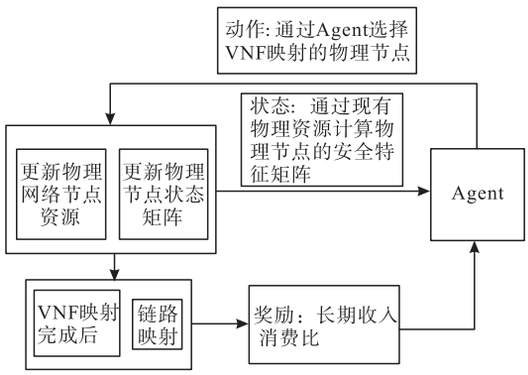

图 2 VNF 映射模型

将环境、Agent、状态、动作、奖励具体说明如下：

1）环境（environment）：

使用物理节点的安全特征矩阵作为部署过程中的环境。

2）Agent 结构：

本文采用基于策略的 RL 方法解决连续动作的 MDP 问题，引入了一种策略网络来解决 RL 问题。策略网络本质上是一个神经网络，以某一环境状态作为输入，通过正向传播输出该环境状态下所有候选动作的概率分布[17]。使用 MLP 作为 Agent 的策略网络并进行参数化，策略网络由输入层、隐藏层、输出层与节点选择层组成，Agent 结构如图 3 所示。

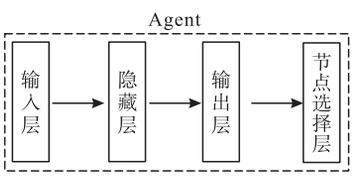

图 3 Agent 结构

输入层将物理节点的安全特征矩阵作为输入，由隐藏层输出每个物理节点的向量，用于映射某个虚拟节点，对于节点 k，向量计算公式为：

$$\boldsymbol{h}_k = \tanh(w_n \cdot \boldsymbol{sav}_k + b_n) \tag{21}$$

式中：w_n 为隐藏层的权重；b_n 为偏置；tanh 为激活函数。

然后将该向量转移到 Softmax 层，利用 Softmax Function 生成节点概率分布，概率计算如式(22)所示：

$$p(se_i) = \frac{e^{hk}}{\sum_{k=1}^{n} e^{hk}} \tag{22}$$

此时，概率分布对应一个 VNF 映射到所有物理节点的可能性大小，即 VNF 映射到概率越大的物理节点上其映射效果越好[18]。

节点选择层需要在所有候选节点中选择一组满足约束条件的物理节点进行 VNF 的映射，将不满足约束条件的节点进行删除。

3）动作（Actions）：

根据 Agent 输出节点的概率分布，选择概率最高的物理节点作为需要被映射的节点。当 VNF 映射完成后，在选择的物理节点和它的邻居节点之间运行 Dijkstra 算法，进行虚拟链路映射。

4）状态（States）：

在进行动作选择后，环境需要对基础网络设施中的物理节点进行资源更新，根据当前物理节点的资源计算节点安全特征矩阵，使得 Agent 得到新的状态表示。

5）奖励（Rewards）：

在 RL 模型中，Agent 仅根据奖励来估计模型是否正确。较大的奖励表明代理当前的行动是有效的，应该继续下去；一个小的奖励表明当前的行为是不适当的，应该调整，因此如何设置合理的奖励十分关键[19]。本文以网络资源利用情况作为奖励信号，当链路映射成功时，Agent 会收到奖励信号；当链路映射失败时，奖励值为 0，以避免 Agent 下次选择该策略，奖励计算如式(23)所示：

$$Reward = \begin{cases} \dfrac{C_s(n_v)}{C(n_p)}, NS \text{ 成功部署} \\ 0, \text{否则} \end{cases} \tag{23}$$

式中：$C_s(n_v)$ 代表 VNF 消耗的 CPU 资源；$C(n_p)$ 代表 VNF 映射到物理节点 n_p 的 CPU 总资源。如果部署策略网络资源利用高，则认为该部署策略较好，如果未部署成功，则设置奖励值为 0，以避免下次选择该策略。

3 仿真实验

3.1 实验环境

本文使用 GT-ITM 工具生成物理网络拓扑及网络切片实例请求，实验平台采用 Pycharm，采用 python 语言编写程序，利用 TensorFlow 构建策略网络，测试结果在 Origin 中绘图表示，网络参数设置表 1。

表 1 网络参数设置

参数	取值
物理节点数量	50
物理节点资源	[50,100]
物理链路资源	[50,100]
节点安全等级	U[0,5]
节点链接概率	0.5
每个 NSI 请求 VNF 数量	U[2,10]
VNF 节点资源	U[0,20]
VNF 节点安全等级	U[0,3]
VNF 虚拟链路资源	U[0,50]
请求持续时间	50 000 个时间单位

3.2　SANS-RL 模型性能评估

将本文提出的 SANS-RL 模型与文献[6]提出的 GRC 算法、文献[7]提出 VNE-RL 算法与文献[8]提出的 SVNE-RL 进行对比。

本文从请求接受率、长期安全收益成本比、长期网络资源利用率、长期带宽资源利用率与程序运行时间 5 个方面进行对比分析。

3.2.1　请求接受率与长期安全收益成本比

各算法 VNF 的请求接受率变化情况见图 4。

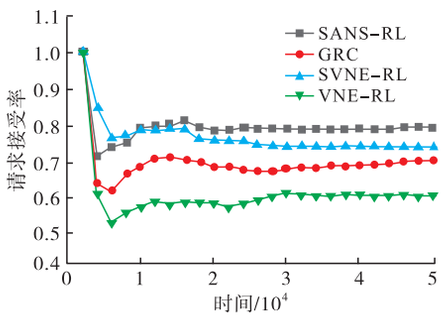

图 4　请求接受率

从请求接受率可以看出，SANS-RL 高于 SVNE-RL 高于 GRC 高于 VNE-RL。由于在初始时间时，由于物理资源丰富，可以满足更多的虚拟网络需求，所以各算法请求接受率都较高。随着物理网络资源的不断消耗，后期指标开始逐渐下降，而 SANS-RL 算法在测试阶段确定了 Agent 的最优化参数，使其能够更好地学习物理网络节点链路之间的关系，这更符合 VNF 的实际情况，所以其请求接受率最高。

而 VNE-RL 请求接受率最低，由于其考虑节点的拓扑属性较少，对于物理网络情形感知较差，VNE-RL 模型不能充分发挥其优势，难以获得最合适的嵌入策略，故其请求接受率最低；而 GRC 使用启发式算法，综合考虑了全局资源拓扑属性，其算法效率与物理网络资源状态变化无关，故其请求接受率高于 VNE-RL，而 SVNE-RL 对物理网络资源考虑较为全面，但其算法运行方差较大，导致算法效率低于 SANS-RL，故其请求接受率低于 SANS-RL。

长期安全收益成本比如图 5 所示，从图中可以看出，SANS-RL 长期安全收益成本与 SVNE-RL、GRC 算法较为接近，都高于 VNE-RL 算法。因为长期收益消费比主要取决于算法效率与物理节点数量无关，由于 SANS-RL 算法的 Agent 是在具有较多物理节点特征的环境中训练，其对物理网络感知程度最高，故其映射效率最高效果最好，而 VNE-RL 对物理网络感知程度较低，其在映射过程中需要反复寻找最优映射结果，从而导致算法效率降低，效果较差。

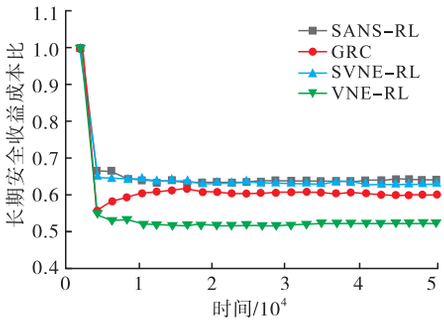

图 5　长期安全收益成本比

3.2.2　长期网络资源利用率与带宽利用率

长期网络资源利用率与长期带宽利用率见图 6、图 7。

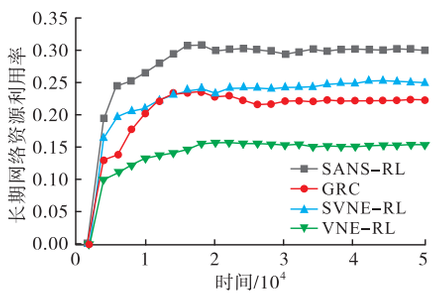

图 6　长期网络资源利用率

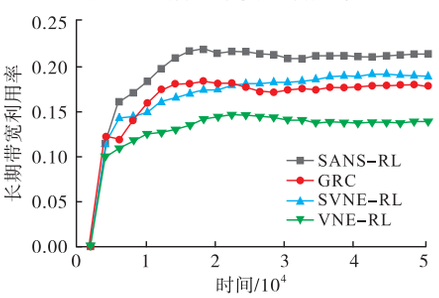

图 7　长期带宽利用率

由图 6 与图 7 可得，在所有算法中，SANS-RL 网络资源利用率与带框利用率最高，由于 SANS-RL 接收到的 VNF 请求最多，其请求接受率最高，则 SANS-RL 模型对带宽与网络资源的利用情况最好。而 SVNF-RL、GRC 与 VNF-RL 算法网络资源利用率与带宽利用率依次下降，与请求接受率实验结果相符，证明了 SANS-RL 算法效率的优越性与资源利用的高效性。

3.2.3　程序运行时间

图 8 显示了在相同的实验环境条件下，各算法的运行时长。

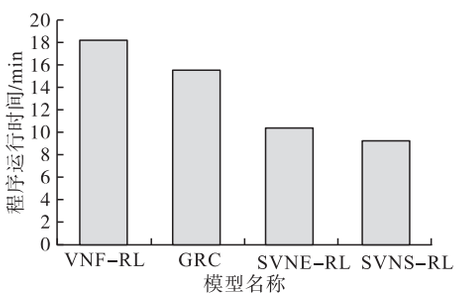

图 8　各算法运行时长比较

由于各算法的程序运行时长受操作系统与实验环境的影响，不同算法的程序运行时长仅在实时操作系统环境中有效。其中 VNF-RL 算法运行时间最长，因其对物理网络资源感知较差，其需要不断学习映射的最佳策略，导致算法运行时间较长且效率较低。而 GRC 算法综合考虑了物理节点资源与全局拓扑情况，算法较为复杂，但使用蒙特卡洛树搜索提高了算法性能减少了运行时间，使得其运行时间比 VNF-RL 较好。而 SVNE-RL 与 SANS-RL 运行时长相近，由于 SANS-RL 模型梯度求解过程使用带有基线的 REINFORCE 算法，减少了强化学习过程中方差使其学习效率更快，效率更高故其运行时间优于 SANS-RL。

4 结语

针对传统启发式算法解决网络切片部署问题易陷入到局部最优解，且部署过程中对网络切片节点与链路的感知程度不高的问题，本文提出了一种基于安全感知的网络切片部署策略，并通过仿真实验验证了部署模型的可行性与算法的高效性。在 VNF 映射部署阶段，首先利用安全等级量化了 VNF 的安全需求，然后提取物理节点的关键安全指标构建安全特征矩阵，利用策略网络输出安全特征矩阵的映射概率大小，实现 VNF 的安全部署。在虚拟链路部署阶段，采用最短路径方法进行虚拟链路映射。最终证明 SANS-RL 在满足安全约束的同时能够有效感知部署过程中的资源变化情况，获得较高的安全收益与部署收益。在后续研究中，将针对多层网络切片的安全部署进行研究，考虑复杂网络情况下的网络切片安全部署情形。

参考文献

[1] OLIMID R F, NENCIONI G. 5G Network Slicing: A Security Overview[J]. IEEE Access, 2020, 8: 99999-100009.

[2] CUNHA V A, SILVA E D, CARVALHO M B D, et al. Network Slicing Security: Challenges and Directions[J]. Internet Technology Letters, 2019, 2(5): 1-6.

[3] CAO H, WU S, HU Y, et al. A Survey of Embedding Algorithm for Virtual Network Embedding[J]. China Communications, 2019, 16(12): 33.

[4] 牛犇，游伟，汤红波. 基于安全信任的网络切片部署策略研究[J]. 计算机应用研究，2019，36(2)：575-579.

[5] ZHANG P, LI H, NI Y, et al. Security Aware Virtual Network Embedding Algorithm Using Information Entropy TOPSIS[J]. Journal of Network and Systems Management, 2020, 28(1): 35-57.

[6] LONG G, WEN Y, ZHU Z, et al. Toward Profit-Seeking Virtual Network Embedding Algorithm via Global Resource Capacity[C]//IEEE Conference on Computer Communications. Toronto, ON, Canada: IEEE, 2014: 1-9.

[7] YAO H, CHEN X, LI M, et al. A Novel Reinforcement Learning Algorithm for Virtual Network Embedding[J]. Neurocomputing, 2018, 284(APR. 5): 1-9.

[8] ZHANG P, WANG C, JIANG C, et al. Security-Aware Virtual Network Embedding Algorithm Based on Reinforcement Learning[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 1095-1105.

[9] 陈金涛，梁俊，刘波，等. 5G 卫星集成网络中控制器与网关可靠部署策略[J]. 空军工程大学学报(自然科学版)，2021，22(3)：68-73.

[10] 黄开枝，潘启润，袁泉，等. 基于性能感知的网络切片部署方法[J]. 通信学报，2019，40(8)：115-122.

[11] FISCHER A, MEER H D. Secure Virtual Network Embedding[J]. Praxis der Informationsverarbeitung und Kommunikation, 2011, 34(4). dol: 10.1515/piko.2011.040.

[12] LIU S, CAI Z, HONG X, et al. Security-Aware Virtual Network Embedding[C]// 2014 IEEE International Conference on Communications. Sydney, Australia: IEEE, 2014: 834-840.

[13] RKHAMI A, HADJADJ-AOUL Y, OUTTAGARTS A. Learn to Improve: A Novel Deep Reinforcement Learning Approach for Beyond 5G Network Slicing [C]// 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). [S. l.]: IEEE, 2021: 1-6.

[14] YU M, YI Y, REXFORD J, et al. Rethinking Virtual Network Embedding: Substrate Support for Path Splitting and Migration[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 17-29.

[15] 王子厚，韩言妮，林涛，等. 可重构网络中基于中心度与拓扑势排序的资源分配算法[J]. 通信学报，2012，33(8)：10-20.

[16] LI M, LU M L. A Virtual Network Embedding Algorithm Based on Double-Layer Reinforcement Learning [J]. The Computer Journal, 2021(6): 974-989.

[17] YAO H, CHEN X, LI M, et al. A Novel Reinforcement Learning Algorithm for Virtual Network Embedding[J]. Neurocomputing, 2018, 284(5): 1-9.

[18] YAO H, CHEN X, LI M, et al. A Novel Reinforcement Learning Algorithm for Virtual Network Embedding [J]. Neurocomputing, 2018, 284(APR. 5): 1-9.

[19] 董方昊，冯有前，尹忠海，等. 具有精英策略的深度强化学习无人机集群通信网络拓扑设计[J]空军工程大学学报(自然科学版)，2019，20(4)：52-58.

[20] WILLIAMS R J. Simple Statistical Gradient-Following Algorithms for Connectionist Reinforcement Learning[J]. Machine Learning, 1992, 8(3): 229-256.

[21] WANG C, ZHENG F H, ZHENG G C, et al. Modeling on Virtual Network Embedding Using Reinforcement Learning[J]. Concurrency Computation Practice and Experience, 2020, 32(23): 1-12.

(编辑：徐楠楠)