计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications [doi: 10.15888/j.cnki.csa.009123]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 BN 模型的网络切片安全部署①

王　淼, 臧韦菲, 孙　磊, 赵　锟, 窦睿彧, 丁瑞阳

(战略支援部队信息工程大学, 郑州 450001)
通信作者: 臧韦菲, E-mail: zwfndsc@163.com

摘　要: 为了降低 NFV (network function virtualization) 架构下共用基础设施给网络切片带来的安全风险, 同时兼顾部署网络切片时的可用性, 本文提出了一种基于 BN (Brewer-Nash) 模型的网络切片安全部署方法. 该部署方法首先提出了基于 BN 模型的 5G 切片部署架构, 基于 BN 模型设计了网络切片中虚拟网元 (virtual network function, VNF) 的安全部署规则, 使不同利益冲突类垂直用户网络切片的 VNF 形成主机隔离, 提升了 VNF 运行时的安全性; 然后利用整数线性规划对该部署问题建模, 把部署成本最小化作为目标函数; 最后使用遗传算法求出部署结果. 仿真结果表明, 该方法在满足网络切片 VNF 安全部署规则的前提下降低了部署成本.

关键词: 网络切片; BN 模型; 安全; 网络功能虚拟化

引用格式: 王淼,臧韦菲,孙磊,赵锟,窦睿彧,丁瑞阳.基于 BN 模型的网络切片安全部署.计算机系统应用. http://www.c-s-a.org.cn/1003-3254/9123.html

Security Deployment of Network Slices Based on BN Model

WANG Miao, ZANG Wei-Fei, SUN Lei, ZHAO Kun, DOU Rui-Yu, DING Rui-Yang

(Information Engineering University, Zhengzhou 450001, China)

Abstract: In order to reduce the security risk of network slices caused by infrastructure sharing in network function virtualization (NFV) architecture and take into account the availability of network slices during deployment, this study proposes a security deployment method of network slices based on Brewer-Nash (BN) model. The deployment method first proposes a fifth-generation (5G) slice deployment architecture based on BN model. Based on BN model, the security deployment rules of virtual network function (VNF) in network slices are designed to make VNF of vertical user network slices with different conflict of interest classes form host isolation, which improves the runtime security of VNF. Then the deployment problem is modeled by integer linear programming, and the objective function is to minimize the deployment cost. Finally, the deployment result is obtained by a genetic algorithm. Simulation results show that the proposed method can reduce the deployment cost under the premise of meeting the security deployment rules of VNF of network slices.

Key words: network slice; Brewer-Nash (BN) model; security; network function virtualization (NFV)

随着 5G 移动通信技术的大规模应用, 垂直行业的相互融合也逐步深入. 增强型移动带宽 (eMBB)、海量机器类通信 (mMTC)、超可靠低时延通信 (uRLLC) 作为 5G 网络的典型应用场景, 为用户提供了高速优质的移动网络通信服务, 实现了真正意义上的“万物互联”. 基于 NFV 和 SDN (software defined network) 的端到端网络切片 (network slice, NS) 技术使得 5G 为用户提供个性化定制网络服务成为可能. 网络切片实质上就是一个虚拟网络, 通过将虚拟网元部署在物理主机上, 构建起了一个虚拟的网络, 为用户提供端到端的网络服务. 网络切片技术为 5G 网络赋予了特有的灵活性, 也使得 5G 网络方便维护的愿景得以实现. 但是不同虚拟

① 收稿时间: 2022-10-15; 修改时间: 2022-11-14, 2022-11-30, 2022-12-11; 采用时间: 2023-01-16; csa 在线出版时间: 2023-05-19

网络共用基础设施也带来了相应的风险挑战. 文献 [1] 介绍了一种恶意用户基于共享物理资源发动的测信道攻击. 恶意用户通过在部署切片的主机上大量部署虚拟机 (virtual machine, VM) 进行同驻检测发动测信道攻击, 进而窃取用户关键数据. 文献 [2] 的研究表明, 恶意用户可通过增加恶意 VM 数量占用主机计算资源和网络带宽, 最终使主机资源耗尽从而发动拒绝服务攻击. 目前, 随着智能仓储、智慧矿山、军用 5G 专网、城市应急指挥专网[3,4] 等垂直应用场景的出现, 垂直用户对专网部署切片的需求与日俱增, 5G 专网的安全问题也越来越引人关注[5], 虚拟网元共享基础设施会引发安全漏洞, 为了应对共用物理主机带来的风险挑战, 亟需研究一种安全的网络切片部署方法满足用户的安全需求.

1 相关研究

攻击者可以利用网络切片共享基础设施部署存在的漏洞发动侧信道攻击、资源耗尽型拒绝服务攻击以及 VNF 在线漏洞挖掘攻击, 为了抵御攻击者的恶意行为, 文献 [6,7] 均采用了拟态防御思想, 通过 VNF 的动态迁移缩短不同 VNF 在同一主机上运行的时间, 减少 VNF 暴露给攻击者的时间窗口, 从而达到增强防御能力的目的. 除此之外, 文献 [8] 利用底层网络的异构特性, 将 VNF 划分成 Run_Time 上任务的类型, 通过任务调度算法将 VNF 在不同架构的主机上动态运行以达到抵御硬件架构漏洞带来的安全威胁. 与此同时, 研究者们从网络切片的部署策略出发, 寻求更有效的防御手段. 文献 [9] 中通过对比分析不同预防侧信道攻击方式的 VNF 部署策略, 提出了集中部署同一用户 VM 最有效的防御策略. 文献 [10] 将中国墙的思想引入 VM 的部署中, 将切片拥有者之间的关系分为利益冲突类和非利益冲突类, 在部署 VM 时通过打标签的方式实现隔离部署, 该方法利用 Brewer-Nash (BN) 模型完成了安全性证明并推导出具有利益冲突类的 VM 不能部署到同一台物理主机上的重要结论, 但该方法并未从运营商的角度评估其部署机制带来的资源成本开销. 文献 [11] 将 VNF 和底层节点的不同指标量化为安全信任值并划分为不同等级, 以信任值等级排序为依据对 VNF 部署, 虽然在部署时考虑了其成本收益并且保证安全等级高的切片安全收益, 但牺牲了低等级切片的安全性. 文献 [12] 将切片实例分为不同的隔离等级, 然后以隔离等级差值作为虚拟节点作为是否可以共存的限制条件, 既提升了切片部署时的收益也兼顾了租户在安全性方面的需求, 但该隔离方法为自定义安全等级, 并没有严格的安全性证明. 切片的隔离部署带来的安全性提升是显著的, 可以为不同垂直用户提供一种共享基础设施部署切片的有效方法, 本文提出了一种基于 BN 模型的 5G 网络切片部署方法, 该方法根据 BN 模型设计了 5G 切片部署的安全规则, 首先将垂直用户划分为不同利益冲突类并赋予标签, 在部署时通过比对网络切片的 VNF 与主机上存在的标签是否相同, 确定切片 VNF 能否共用主机部署, 使不同利益冲突类垂直用户的 VNF 形成主机隔离; 而后通过建立混合整数规划模型模拟切片的部署, 并将部署成本作为目标函数; 最后利用遗传算法优化部署结果, 降低了切片部署的成本支出. 仿真结果表明, 该方法在保证安全性的同时, 降低了网络切片的部署成本.

2 问题描述

不同的垂直用户之间往往存在着竞争关系, 存在潜在发动攻击的可能. 为了规避竞争对手带来的安全风险, 垂直用户往往希望运营商为其提供相对独立的物理运行环境. 但是运营商在提供服务时的成本支出也是其考虑的重点, 因此为每一个垂直用户提供独立的物理环境是不现实的. 为了兼顾用户的隔离需求以及运营商的运营成本支出, 从发动攻击的潜在可能出发, 根据垂直用户利益竞争关系将其划分为不同的集合可以有效地缓解上述矛盾. 即将没有竞争关系的垂直用户归为一个集合, 在部署他们的网络切片时可以共用主机部署, 有竞争关系垂直用户的网络切片隔离部署. 例如垂直用户 A 与垂直用户 B 分属于医疗卫生行业、智能制造行业, 两者在涉及领域信息交互类型等涉及敏感信息方面几乎不存在交集, 若相互之间发动攻击并不会为自身带来直接的利益, 因此在他们之间发动攻击的概率较低, 所以他们可以共用主机部署网络切片; 垂直用户 A 与垂直用户 C 都属于医疗卫生行业, 但他们属于不同的公司, 若其中一方发动攻击, 便会对对方造成负面影响, 从而影响对方的收益, 因此它们彼此发动攻击的可能性极大, 因此它们的网络切片在部署时应采取主机隔离.

3 安全部署策略

3.1 BN 模型简介

BN 模型又称中国墙模型, 是 Brewer 等人在 1988 年根据现实的商业策略提出的中国墙 (Chinese wall)

安全模型[13]. 该安全模型试图解决相互竞争的客体通过主体访问的历史数据建立一道虚拟的墙来保护客体的数据不被非法访问. 其安全策略的本质是将全体数据划分为“利益冲突类”, 通过强制性约束, 主体至多访问每个“利益冲突类”的一个数据集. 该模型中包含主体、客体和“利益冲突类”这 3 个要素, 本文将该模型应用于 5G 移动通信网络系统中, 通过将不同垂直用户设置为不同的利益冲突类从而实现不同垂直用户切片间的物理隔离.

3.2 基于 BN 模型的 5G 切片架构

与 BN 模型机构类似, 5G 切片隔离架构分为 3 层, 如图 1 所示.

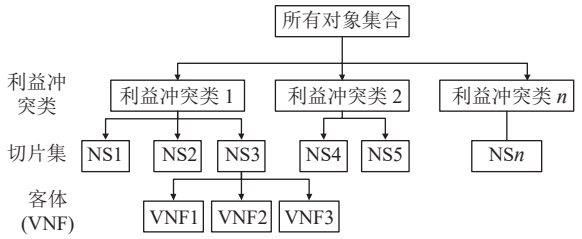

图 1 基于 BN 模型的 5G 切片架构图

① 最底层: 客体, 即具有特定功能独立的 VNF 实体, 每一个 VNF 都属于且仅属于一个切片的 VNF 集.

② 中间层: 切片集, 由属于该切片的所有 VNF 组成.

③ 最高层: 利益冲突类, 是所有具有利益冲突关系的切片集组成的集合.

确定客体之间关系的是客体所属于的切片集和切片集属于的利益冲突类. 利益冲突类可以按照切片拥有者来划分 (如垂直用户 A、垂直用户 B 等), 切片集可以按照不同垂直用户所含的切片划分. 为了便于理解, 假设一个 NFV 基础设施 (NFV infrastructure, NFVi) 域内包含 4 个切片, 分别是垂直用户 A 的切片 a_1、切片 a_2, 垂直用户 B 的切片 b_1、切片 b_2, 那么:

① NFVi 环境中 VNF 属于 4 个切片中的某一个.

② 此系统中包含 2 个利益冲突类, 一个是垂直用户 A 的切片, 一个是垂直用户 B 的切片. VNF 属于垂直用户 A 利益冲突类和垂直用户 B 利益冲突类之一.

5G 网络切片隔离架构模型与 BN 模型类似, 通过设定一堵虚拟的“墙”, 利用 BN 模型推导出的安全规则, 使不同利益冲突类的切片不能越“墙”部署. BN 模型为了保证数据的安全性是将数据集作为客体, 若客体被某一个利益冲突类访问过后就被打上了安全标签, 其他利益冲突类将无法访问该数据集. 在 NFV 架构中管理层对 VNF 的管理可以借鉴该理念, 为了避免因不同利益冲突类的恶意 VNF 发动攻击, 通过给物理主机打标签的方法避免不同利益冲突类的虚拟机发动虚拟机同驻攻击.

3.3 基于 BN 模型的 5G 切片架构的形式化模型

3.3.1 模型元素定义

在该模型中, 主要包括客体、主体、部署操作和安全标签 4 个元素, 分别定义如下.

定义 1 (客体集合 O). 待部署的 VNF 集合. $O=\{o_1, \cdots, o_n\}$, 其中, o_i 代表一个待部署的 VNF.

定义 2 (主体集合 S). VNF 的载体集合, 在 NFV 架构中, VNF 的载体是物理服务器. $S=\{s_1, \cdots, s_n\}$, 其中, s_j 代表一个物理主机.

定义 3 (部署操作 $EMB(i, j)$). 将客体虚拟网络功能 o_i 部署在主体服务器上 s_j.

定义 4 (安全标签). 用于定义客体所属的组织 VNF 集合与利益冲突类, L 表示一个安全标签集 (x, y), 其中 x 代表利益冲突类, y 代表组织 VNF 集合, 每一个客体都有一组安全标签集. 引入 $X(o_i)$ 和 $Y(o_i)$ 来表示将标签 (x, y) 赋予某一指定客体. 对于每一个 o_i, x_i 表示它的利益冲突类, y_i 表示它的切片集.

定义 5 (部署状态矩阵). 令 M 为一个布尔型矩阵, M 的行对应时每一个主体, M 列对应的是每一个客体, $EMB(i, j)$ 表示主体 s_j 是否部署了客体 o_i, 当为 True 时表示已部署, 为 False 时表示未部署. 客体在完成部署后要将相应的元素置为 True 并刷新矩阵 M, 被打上标签的主机在下一次部署时就不能被其他利益冲突类的主体部署客体.

3.3.2 安全部署策略

在完成相关定义后, 下面推导安全部署策略.

定理 1. $y_1 = y_2 \rightarrow x_1 = x_2$.

若两个不同的客体 o_i 和 o_j 属于同一个切片集, 则它们属于同一个利益冲突类.

推论 1. $y_1 \neq y_2 \rightarrow x_1 \neq x_2$.

推论 1 为定理 1 的逆否命题, 表示若两个不同的客体 o_i 和 o_j 属于不同的利益冲突类, 则它们不属于同一个切片集.

定理 2. 主体 s_i 能否在主机上部署客体 o_r 的判断条件为: 当部署矩阵 $EMB(i, j)$ 中所有的为真所对应的 o_r 满足下面的条件:

$$x_j \neq x_r \vee y_j = y_r$$

客体 VNF 只能部署在没有部署过且与其利益冲突类标签相同的物理服务器上, 部署过其他利益冲体类标签 VNF 的物理服务器不能部署与该 VNF 利益冲突类标签不同的 VNF. 本定理为基于 BN 模型的部署方法的重要规则.

3.3.3 中国墙问题模型描述 5G 切片架构示例

根据上文所述, 具有不同利益冲突类型网络切片中的 VNF 不能部署到同一个计算节点上, 目的是防止具有不同利益冲突类的 VNF 通过共享物理主机发动攻击. 在实际部署切片时, 切片属于不同的垂直用户使用, 不同垂直用户之间存在安全竞争, 若具有不同利益冲突类的垂直用户发动恶意攻击势必会影响其他切片的正常运行, 因此在实际部署切片时, 要把具有不同利益冲类垂直用户切片中的 VNF 分开部署, 从而达到物理隔离的效果, 如图 2 所示, 切片 1 和切片 2 属于两个不同的利益冲突类, 若两个切片需要在同一区域部署切片, 切片内各个网元不能部署在同一台物理主机上, 如切片 2 中的网元 1 在选取所要映射物理节点时检测到 S3 节点已经部署了切片 1 中的网元 2, 因此在映射切片 2 中的网元 1 时就要避免和切片 1 中的网元 2 部署在同一主机上.

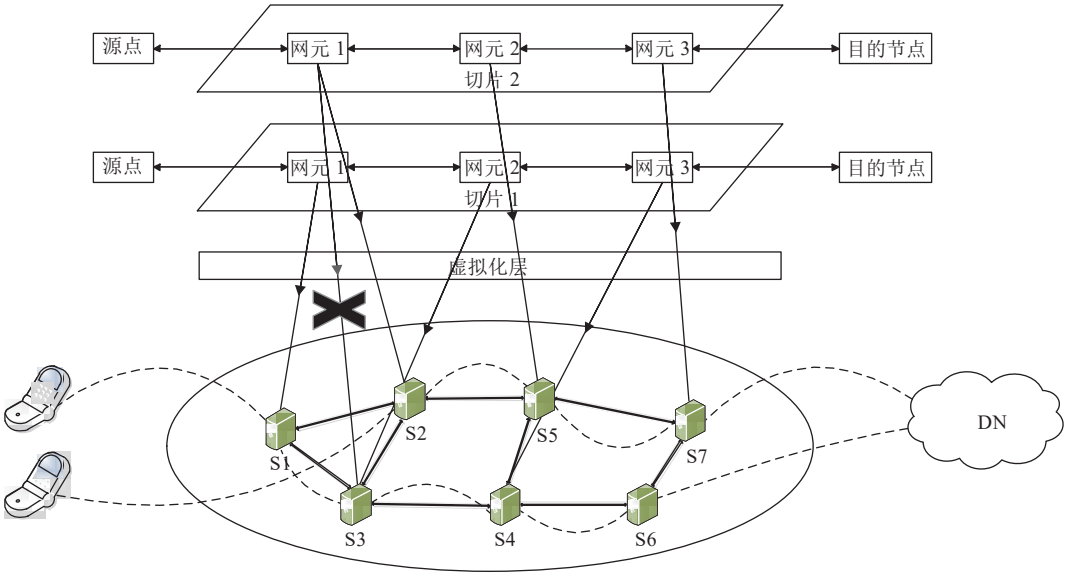

图 2 基于 BN 模型的切片映射示意图

4 部署模型建立

在部署切片时, 除了要考虑前文提到的隔离问题, 还要兼顾到底层物理节点能否承载 VNF 的计算资源需求, 以及逻辑链路映射时物理链路的带宽能否满足逻辑链路的带宽需求. 与此同时, 在部署切片时既要满足以上条件又要尽可能减少部署切片时产生的成本支出. 因此, 在部署时将条件作如下设置: ① 物理节点计算资源不得超过所承载 VNF 所需计算资源的总和; ② 承载逻辑链路的物理链路集中最低带宽不得超过所承载逻辑链路需求带宽的总和; ③ 属于不同利益冲突类切片的 VNF 不得部署到同一个物理节点上; ④ 在部署切片时尽量减少其成本支出.

4.1 网络模型

5G 系统的核心网采用基于服务架构 (service based architecture, SBA), 网络切片可以实例化为一个逻辑互联的 VNF, 以 uRLLC 切片为例, 将切片中 AMF、SMF、PCF 以及 UPF 定义为 VNF, 承载网元的 VNF 按照一定的逻辑顺序连接起来组成切片, 为用户提供接入管理、移动性管理、数据流定向、用户数据流锚点以及数据转发等服务. 底层的物理网络可由承载数据处理与存储的计算节点和路由转发数据的交换节点链路组成. 承载网元的 VNF 可以部署在任意的计算节点上, 并且 VNF 之间的逻辑链路可以选择任意的链路. 每个计算节点上都分配有 CPU 资源、ROM 资源以及 RAM 资源, 每条交换链路都分配有带宽资源, 为了降低计算复杂度, 将计算节点上分配的 CPU 资源、ROM 资源以及 RAM 资源统称为节点计算资源, 由于承载 VNF 的物理服务器分布在不同地点, 因此单位计算资源也

会产生差异, 将每个物理节点计算资源的单价设为 (50, 100) 的均匀分布, 用 p_i ($p_i \in P$) 表示第 i 台物理服务器的单位计算资源的单价.

切片在 NFVi 上的部署问题就是将 SFC 映射到底层网络. 为了方便建立数学模型, 首先将 NFVi 抽象为一个有权无向连通图 $G_S = \{N_S, L_S, C_N, C_L, P_S\}$, N_S 表示 NFVi 中的物理主机集合, L_S 表示 NFVi 中物理链路集合, C_N 表示 NFVi 中的物理主机剩余计算资源数的集合 (CPU 资源、ROM 资源以及 RAM 资源的总和), C_L 表示 NFVi 中物理链路剩余带宽资源数集合, P_S 表示 NFVi 中的物理主机计算资源单位计算资源价格的集合. 网络切片实例同样为一个有权无向连通图 $G_V = \{N_V, L_V, R_N, R_L, \Theta\}$, N_V 表示网络切片实例中 VNF 的集合, L_V 表示网络切片中虚拟链路的集合, R_N 表示 VNF 需求计算资源数的集合, R_L 切片逻辑链路需求计算资源数的集合, Θ 表示该切片属于的利益冲类标签. 为了后续建立约束条件计算方便, 本文将 Θ 的类型均定义为一组 one-hot 向量, 其维度与标签类型数量相同, 假设利益冲突类标签形成的矩阵为矩阵 Λ, 其行数为 VNF 的总数, 列数为利益冲类个数记为 δ.

4.2 目标函数

根据前文所述的模型架构以及网络切片部署模型, 网络切片的部署实际上就是将网络切片请求 G_V 映射到基础上设施 G_S 上, 假设当前第 q 个网络切片请求 G_V^q 等待部署, G_V^q 中共有 t 个虚拟节点和 f 个虚拟链路, 基础设施中共有 r 个计算机节点和 w 条物理链路, 当前共有 n 个 VNF 部署在基础设施中, 所有 VNF 的利益冲类标签形成矩阵为 $\Lambda_{n,\delta}$, 为了求解该部署问题定义两个二进制 (0-1) 决策变量. ① $\varpi_{q,x,y}$ 表示将 G_V^q 中的第 x 个虚拟网元 $n_V^x \in N_V^q$ 映射到基础设施中的第 y 个物理节点 $n_S^y \in N_S$ 上, 此时 $\varpi_{q,x,y}$ 的值为 1, 当前所有已部署的 VNF 形成的矩阵为 $\pi_{n,r}$. ② $\mu_{q,lm,\xi}$ 表示将 G_V^q 中的第 l 个虚拟网元 $n_V^l \in N_V^q$ 和第 m 个虚拟网元 $n_V^m \in N_V^q$ 之间的虚拟链路映射到 $n_S^a \in N_S$ (假设 u_V^l 映射到该节点) 到 $n_S^a \in N_S$ (假设 u_V^m 映射到该节点) 物理链路集 Ξ 上, 此时 $\mu_{q,lm,\xi}$ 的值为 1.

在实际情况中, 基础设施中的物理节点受场地租金、人员工资、设备单价以及承载能力等因素的影响, 单位计算资源的价格有所区别, 其单价为 $p_S^y \in P_S$, 因此在部署时运营商需要尽可能降低成本支出, 第 q 个网络切片请求中第 x 个 VNF 的计算需求数为 $r_V^{q,x} \in R_V^q$, 因此目标函数设为:

$$COST = \min\left\{\sum_{x=1}^{t} \varpi_{q,x,y} \times r_v^{q,x}\right\} \times p_S^y \tag{1}$$

4.3 约束条件

网络切片的成功部署要求所有 VNF 要成功映射到物理节点且物理节点剩余资源数不得小于虚拟节点的请求数, 同时所有虚拟链路也必须成功映射到物理链路上, 虚拟节点对应的物理节点间路径是可达的, 物理链路集 ξ 的最小带宽应大于等于该虚拟链路的带宽值.

① 设节点的计算资源数为 $c_S^y \in C_N$, 物理主机计算资源剩余数约束应当满足切片待部署 VNF 需求资源数, 因此节点计算容量约束:

$$\sum_{x,y=1}^{n,r} \varpi_{q,x,y}\left(c_s^y - r_v^{q,x}\right) \geqslant 0 \tag{2}$$

② 同理虚拟链路的映射也应满足约束条件, 设虚拟节点 w 为 $n_V^w \in N_V^q$ 和虚拟节点 h 为 $n_V^h \in N_V^q$, 它们分别映射到了物理节点 l 和物理节点 m 上 ($n_S^l \in N_S$, $n_S^m \in N_S$), u_V^w 到 u_V^h 最短路径集为 Ξ ($\Xi = \{\xi_i | i=1, 2, 3, \cdots, z; \xi_i \in L_S\}$), ξ_i 对应的带宽为 $c_S^i \in C_S$, 因此由 Ξ 形成的物理带宽数集合为 $\Psi = \{\psi_i | i=1, 2, 3, \cdots, z; \psi_i = c_S^i\}$, 该虚拟链路的带宽值为 $r_V^{q,f} \in R_V$, 约束要求虚拟链路的需求带宽不得大于相应链路集的物理带宽数 Ψ 中的最小值, 因此链路约束如下:

$$\sum_{o=1}^{f} \mu_{q,lm,\Xi}\left(\min(\psi_O) - r_V^o\right) \geqslant 0 \tag{3}$$

③ 在部署 VNF 只能映射到一台物理主机上, 不能对其分割, 如式 (4) 所示:

$$\sum_{x=1}^{t} \varpi_{q,x,y} \leqslant 1 \tag{4}$$

④ 网络切片的部署要具有完整性, 因此每个虚拟节点必须映射到物理网络中去, 完整性约束为:

$$\sum_{y=1}^{r} \varpi_{q,x,y} = 1 \tag{5}$$

⑤ 除了满足以上资源约束外, 还要满足前文所述的利益冲突类约束, 每个物理节点上应只部署利益冲突标签相同的 VNF, 如式 (6) 所示:

$$\sum_{y=1}^{r}\left(\sum_{z=1}^{\delta}\sum_{x=1}^{n}\pi_{x,y}\times\Lambda_{x,z}-\sum_{x=1}^{n}\pi_{x,y}\right)=0 \tag{6}$$

4.4 部署算法描述

网络切片的映射已经被证明为是一个 NP 难题[14], 本文将网络映射问题建模为混合整数规划模型, 启发式算法是解决线性规划问题有效手段, 因此为了在有效时间内求解出网络切片的部署结果, 本文采用遗传算法.

4.4.1 遗传算法

根据第 3.4 节所述, 将切片的部署成本作为目标函数, 力求减少切片的部署成本, 将式 (1) 作为目标函数, 优化目标为最小值, 个体适应度值计算公式为式 (1). 初始种群采取随机生成的策略, 对求解该问题的算法详细描述如图 3.

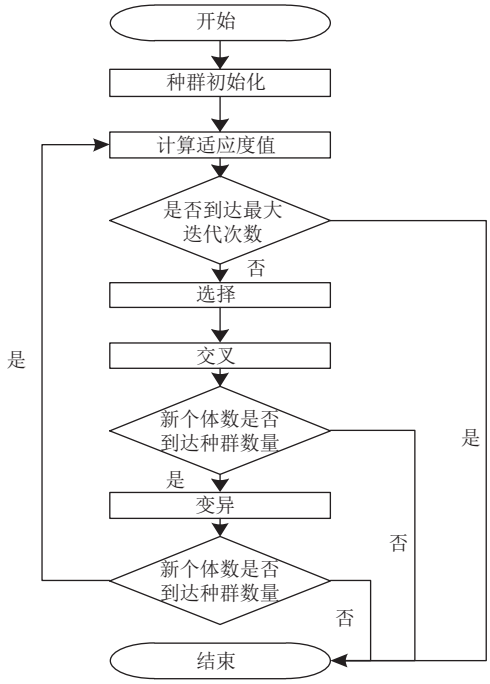

图 3 算法流程图

(1) 染色体编码: 为了方便计算采取十进制编码, 个体基因为一个向量, 其中该向量中的元素为 VNF 映射到物理主机的编号, 向量的长度为每一个 NS 请求中 VNF 的数量. 根据式 (4) 所述, 要求该向量中不能有重复的元素, 表示同一个切片中的 VNF 不能部署在同一台物理主机上.

(2) 生成初始种群: 初始种群采用随机生成的方法, 生成个体后看其是否满足约束条件, 若满足式 (2)–式 (6) 则将该个体加入种群.

(3) 选择: 实验表明采用最优个体的选择策略有利于该问题的求解, 由于本文的目标是减小部署成本, 因此将选择到的个体作为淘汰者, 将剩余的个体作为交叉、变异的候选对象.

(4) 交叉: 交叉操作采取随机选择个体, 随机选择的交叉基因点位的方式.

(5) 变异: 采用随机选择个体, 随机选择变异基因位的方式变异.

4.4.2 算法流程

为了避免基因交叉变异后种群个体数量不足情况的发生, 将交叉变异的循环次数设为 500. 在链路约束判断过程中采用 K 阶最短路径查找算法来筛选链路映射. 算法 1 和算法 2 是算法的详细描述.

算法 1. 部署算法

输入: G_S, G_V^q;
输出: 部署向量, 链路映射结果.

1) 设置种群规模 Scope_Numbers, 迭代次数 Round_Number;
2) 随机生成个体, 使用算法 2 筛选合格个体加入种群;
    If Scope_Numbers = 0
    Return 拒绝服务
3) 计算初始种群的适应度值;
4) while Round_Number do
5) 选择 Scope_Numbers 个体作为新种群;
6) 在新种群中按照 P_c 的概率选择两个个体交叉基因;
7) 判断个体是否满足约束条件, 若满足执行下一步, 否则执行步骤 6);
8) 在产生的新个体中按照 P_m 的概率选择个体变异;
9) 判断个体是否满足约束条件, 若满足执行下一步, 否则执行步骤 8);
10) 计算个体适应度值, 记录本轮最优个体;
11) Round_Number – = 1;
12) if Round_Number = 0
    从每轮记录的最优个体中选出最优个体作为输出.

算法 2. 个体基因判断算法

输入: 个体染色体编码, G_S, G_V^q;
输出: 是否存在链路, 链路映射结果.

1) if 个体基因满足式 (2) && 满足式 (4) && 满足式 (5) && 满足式 (6);
2) while L_V != NULL do
3) 获取虚拟节点映射的物理节点;
4) 使用 K 阶最短路径生成候选链路;
5) if 候选链路是否满足式 (3);
6) 删除该虚拟链路, G_S 修改中 C_L、C_N 属性, 保存该映射链路;
7) else return False;
8) else return False
9) return True, 链路映射结果;

5 仿真与结果分析

5.1 实验环境

在配置为 Intel(R) Core(TM) i5-4200H 2.8 GHz CPU, 12 GB 内存的 PC 机上, 仿真用 Networkx 集成环境生成 NFVi 网络和切片请求数据, 并使用 Python 对实验结果进行仿真分析. 网络和请求参数设置如表 1 所示, 仿真参数设置如表 2 所示. 实验通过对比不同数量利益同类网络切片部署时的请求接受率、部署成本以及资源占比等数据评估本文所提算法的有效性. 其中请求接受率为成功部署切片的数量与总的切片请求数量的比值, 该值越大说明成功部署的切片的数量越多; 部署成本为当前网络切片占用计算资源的总价 (见式 (1)), 该值越小说明成本支出越小; 节点计算资源利用率为当前切片占用的节点计算资源与物理网络所有节点计算资源的总和之比, 该值越大说明网络中节点计算资源利用率越高; 链路带宽资源利用率同节点资源利用率, 该值越大说明网络链路资源利用率越高.

表 1 网络参数

参数	物理网络	网络切片
网络模型	随机网络	随机网络
节点连接概率	0.2	0.5
节点个数	50	服从[3, 5]
节点和链路容量	服从[50, 100]	服从[5, 20]
请求到达	无	服从每20个时间单位到达一个的泊松分布
请求生命周期	无	服从均值为2 000个时间单位的指数分布

表 2 仿真参数

算法参数	取值
最大迭代次数	40
种群规模	100
P_c	0.6
P_m	0.2

5.2 结果分析

部署成本与贪心部署算法对比, 随机部署算法是在满足约束条件的前提下随机生成一个结果作为部署方案, 部署成本多次试验取平均值, 实验表明, 与贪心部署算法相比无利益冲突类的部署成本下降了 6.55%, 两个利益冲突类的部署成本下降了 6.88%, 3 个利益冲突类的部署成本下降了 8.83%.

图 4 显示了切片在不同数量利益冲突类标签 (切片的利益冲突类为随机生成) 网络切片的请求接受率变化情况. 随着利益冲突类的增多请求接受率出现了不同程度的下降, 如图 4 所示, 随着利益冲突类数量增多接受率出现首次下降越早, 最终接受率也随着利益冲突类数量的增加而出现降低.

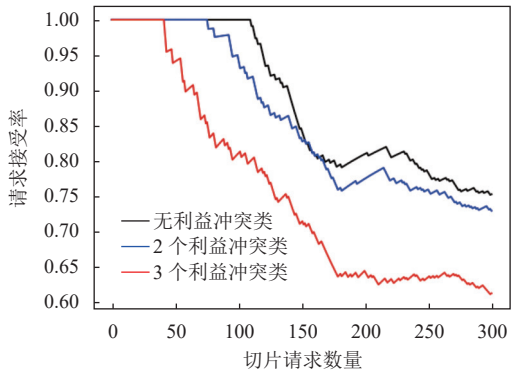

图 4 网络切片请求接受率

在部署成本方面, 通过对比本文部署算法和贪心部署算法评估本文算法在降低切片成本方面的有效性. 图 5 显示了部署成本的变化情况. 随着切片请求数量的增多两种算法的部署成本均呈现逐步上升的趋势, 本文算法的部署成本低于相同数量利益冲突类贪心部署算法的成本, 说明本文算法有效地降低了部署切片时产生的成本.

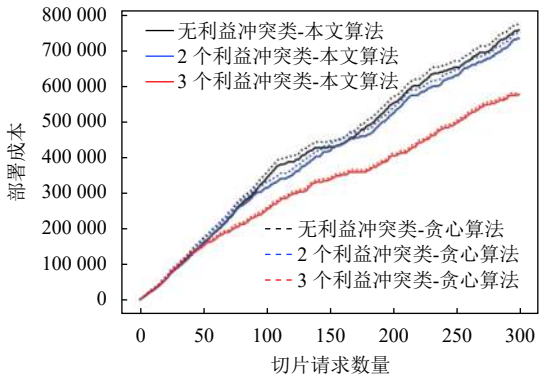

图 5 网络切片部署成本

图 6 显示了节点计算资源利用率情况. 节点资源利用率为所有被成功部署切片占用节点计算资源的总和与物理网络所有节点计算资源总和的比值. 如图所示, 随着切片请求的不断增多资源利用率呈上升趋势, 当请求到达一定数量后呈现稳定状态, 这是由于资源占用趋于饱和所造成的, 但随着利益冲突类数量增多, 趋于平稳时资源占用降低, 这是由于利益冲突类数量的增加会造成请求被拒绝的概率增加.

图 7 显示了链路资源利用率情况. 链路资源利用率为所有被成功部署切片占用链路带宽资源的总和与

物理网络所有链路带宽资源总和的比值. 随着切片请求的不断增多, 资源利用率呈上升趋势最终到达稳定状态, 但三者到达稳定状态的利用率大小随利益冲突类数量的增加而减少, 这是由于随着利益冲突类数量增加接受率降低导致的.

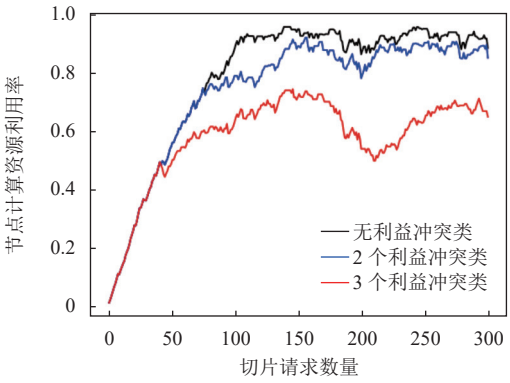

图 6 节点计算资源利用率

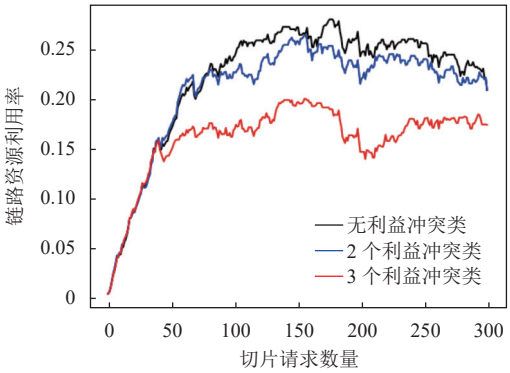

图 7 链路带宽利用率

6 结论与展望

网络切片技术的引入提高了 5G 网络运维的灵活性, 但其共享基础设施的机制也带来了相应的安全隐患, 本文从切片拥有者的角度出发提出了一种基于 BN 模型的网络切片安全部署方法; 基于 BN 模型设计了 VNF 安全部署规则, 并将该安全部署问题建立为混合整数规划模型, 然后采用了遗传算法将部署成本作为目标函数, 减小了网络切片部署的成本. 仿真结果表明, 该部署方法在开销下降方面较为明显, 这也是下一步研究将要改进的重点.

参考文献

1 Gulmezoglu B, İnci MS, Irazoqui G, *et al*. Cross-VM cache attacks on AES. IEEE Transactions on Multi-scale Computing Systems, 2016, 2(3): 211–222. [doi: 10.1109/TMSCS.2016.2550438]

2 Malioutov D, Cetin M, Willsky AS. A sparse signal reconstruction perspective for source localization with sensor arrays. IEEE Transactions on Signal Processing, 2005, 53(8): 3010–3022. [doi: 10.1109/TSP.2005.850882]

3 莫建荣, 赵涛, 王保华, 等. 基于 5G SA 公网切片技术实现工业园区虚拟专网部署. 推动网络演进 促进应用创新——5G 网络创新研讨会 (2021) 论文集. 北京: 中国电子科技集团公司第七研究所《移动通信》杂志社, 2021. 298305. [doi: 10.26914/c.cnkihy.2021.039158.]

4 孙茜, 田霖, 冯晨, 等. 基于 5G 的专用网络安全研究现状. 指挥与控制学报, 2020, 6(4): 299–309.

5 王鑫, 韩振东, 严斌峰. 基于安全隔离度的 5G 专网部署模式. 移动通信, 2020, 44(1): 44–47, 53.

6 徐水灵. NFV 环境下服务功能链主动防御关键技术研究 [硕士学位论文]. 郑州: 战略支援部队信息工程大学, 2020. [doi: 10.27188/d.cnki.gzjxu.2020.000009.]

7 孙志勇. 虚拟化环境下的 5G 核心网安全机制研究 [硕士学位论文]. 郑州: 战略支援部队信息工程大学, 2019. [doi: 10.27188/d.cnki.gzjxu.2019.000113.]

8 季新生, 徐水灵, 刘文彦, 等. 一种面向安全的虚拟网络功能动态异构调度方法. 电子与信息学报, 2019, 41(10): 2435–2441. [doi: 10.11999/JEIT181130]

9 Han Y, Chan J, Alpcan T, *et al*. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. IEEE Transactions on Dependable and Secure Computing, 2015, 14(1): 95–108. [doi: 10.1109/TDSC.2015.2429132]

10 孙磊, 杨星, 马自堂. 云环境下基于 BN 模型的虚拟机安全部署模型. 计算机科学, 2013, 40(3): 210–214. [doi: 10.3969/j.issn.1002-137X.2013.03.047]

11 牛犇, 游伟, 汤红波. 基于安全信任的网络切片部署策略研究. 计算机应用研究, 2019, 36(2): 574–579. [doi: 10.19734/j.issn.1001-3695.2017.08.0728]

12 潘启润, 黄开枝, 游伟. 基于隔离等级的网络切片部署方法. 网络与信息安全学报, 2020, 6(2): 96–105. [doi: 10.11959/j.issn.2096-109x.2020003]

13 Brewer DFC, Nash MJ. The Chinese wall security policy. Proceedings of the 1989 IEEE Symposium on Security and Privacy. Oakland: IEEE, 1989. 206–214.

14 Kuo TW, Liou BH, Lin KCJ, *et al*. Deploying chains of virtual network functions: On the relation between link and server usage. IEEE/ACM Transactions on Networking, 2018, 26(4): 1562–1576. [doi: 10.1109/TNET.2018.2842798]

(校对责编: 孙君艳)