doi:10.11887/j.cn.201805017 http://journal.nudt.edu.cn

网络安全实验平台 K - 划分映射方法*

王会梅[1],刘 建[1],荣 宏[1],欧阳红军[2],鲜 明[1]
(1. 国防科技大学 电子科学学院,湖南 长沙 410073;2. 国防科技大学 教学科研保障中心,湖南 长沙 410073)

摘 要:对网络安全实验平台映射问题进行形式化描述,提出基于 K - 划分的映射方法,其核心思想是为了尽量减少占用网络资源,尽可能将逻辑拓扑紧密连接的节点映射到同一台交换机上。基于 K - 划分的映射方法采用贪心法确定初始划分状态,根据评价函数进行节点移动,对生成的子图进行算法迭代,直到所有子图的节点数量不大于物理拓扑端口容量为止。基于 K - 划分的映射方法弥补了 K-L 算法中初始划分状态选取的任意性对最终结果产生较大影响的缺陷,实验结果表明该算法的求解时间远小于遗传算法,能在较短的时间内得到映射结果。

关键词:网络安全实验平台;映射方法;K - 划分;评价函数
中图分类号:TP393.08 **文献标志码**:A **文章编号**:1001-2486(2018)05-109-07

Mapping heuristics of network security testbed based on K - partition

WANG Huimei[1], *LIU Jian*[1], *RONG Hong*[1], *OUYANG Hongjun*[2], *XIAN Ming*[1]
(1. College of Electronic Science, National University of Defense Technology, Changsha 410073, China;
2. Teaching and Research Support Center, National University of Defense Technology, Changsha 410073, China)

Abstract: The network security testbed mapping problem was formally defined and a new mapping heuristics based on K - partition was presented. The insight of the heuristic is that the tightly connected nodes of the logic topology should be mapped in the same switch in order to save more network resources. This novel mapping determines the initial state by greedy method, and moves nodes according to the defined cost function. The iteration partition of subgraph is in progress until that the number of subgraph nodes is not more than the port capacity of the physical switch. The problem that the result is influenced by the random initial partition in K-L partition is resolved by the K - partition mapping heuristics. The experiment result shows that the runtime is far less than the genetic algorithm, and the proposed algorithm can find near-optimal solutions in shorter period.

Key words: network security testbed; mapping heuristics; K - partition; cost function

在进行网络安全新理论、新方法、新技术的研究过程中,需要开展实验验证。目前绝大部分网络信息安全只是在小规模的专用研究环境中进行测试和评估,很难具有代表性。除了规模限制外,进行网络信息安全实验面临的问题有:

1)不能满足真实网络对准确度和细致程度的要求;

2)缺乏有代表性的真实网络数据;

3)缺乏足够的网络防御机制模型;

4)缺乏足够的网络拓扑模型和背景流量、攻击流量数据。

为了解决这些问题,国内外研究人员正在建立干净、合法且封闭的网络安全实验平台来进行网络实验验证,现在实际运作的实验平台主要有 Emulab Testbed[1]、PlanetLab[2]、DETER[3-4]、FIRE[5]、CoreLab[6]、Testbed@TWISC[7]等。在这些平台上开展实验的核心问题之一是在一个规模较小的网络中模拟出实验者所需要的网络环境,即利用较少真实的物理网络资源来构建实验者所需要的网络拓扑,从而使更多的实验者在实验平台上并行实验。

为了更好地将实验者要求的逻辑拓扑映射到实验平台的物理拓扑之上,本文基于尽可能将逻辑拓扑紧密连接的节点映射到同一台交换机上,从而尽量减少网络资源的占用的核心思想,对网络安全实验平台映射问题进行了形式化描述,定义了评价函数,提出了基于 K - 划分的映射方法。

* **收稿日期**:2016-10-31
基金项目:国家863计划资助项目(2014AA7116082)
作者简介:王会梅(1981—),女,河北行唐人,讲师,博士,E-mail:freshcdwhm@163.com

1 问题描述

网络安全实验平台通常由多台交换机互连而成,每台交换机连接多个主机节点。在开展实验时,将实验者要求的逻辑拓扑映射到网络安全实验平台的物理拓扑上的瓶颈是交换机之间的链路带宽无法满足实验者的资源请求。为了充分利用实验平台资源,一个好的映射应该在满足实验者节点、链路、虚拟局域网(Virtual Local Area Network, VLAN)等资源需求的前提下,占用较少的交换机之间的链路带宽资源,即尽可能地将实验者要求的逻辑拓扑中连接紧密的节点映射到同一台交换机上,从而满足更多的实验者的资源需求。

在研究网络安全实验平台映射问题时,为了简化,进行如下假设[8]:

1)所有的节点是同构的,从而可以将节点映射到任何一个交换机上;

2)交换机之间以一定的带宽互联,忽略交换机之间详细的连接结构。

例如,可以通过把交换机的容量从标量转换为矢量,得到异构的节点;交换机之间带宽的独立性假设是对问题的简化,但是在进行实验床映射问题的研究时没必要引入更加复杂的模型。

下面给出了网络实验平台映射问题及其约束条件的形式化描述:

假设有一个物理网络拓扑,包含 n 个交换机 $(s_1,s_2,\cdots,s_n)$,每个交换机对应的容量分别为 $C_1,C_2,\cdots,C_n$,交换机之间的链路带宽分别为 $B_{11},\cdots,B_{1n},B_{21},\cdots,B_{nn}$;又有这样一个逻辑拓扑,包含 m 个节点 $(N_1,N_2,\cdots,N_m)$,节点之间的链路带宽需求为 $b_{11},\cdots,b_{mm}$。寻找映射 $\varphi:N\rightarrow s$ 满足:

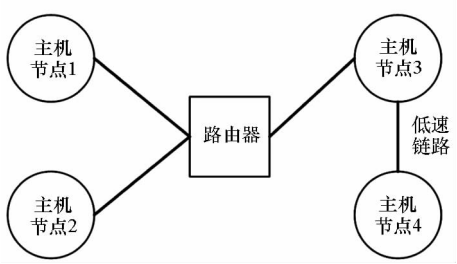
$$|\varphi(u)=i|\leqslant C_i \quad \forall i,1\leqslant i\leqslant n,\ u\in N \tag{1}$$

$$\sum_{\varphi(u)=i,\varphi(v)=j} b_{uv}\leqslant B_{ij} \quad u\in N,v\in N \tag{2}$$

任意满足式(1)、式(2)两个约束条件的映射都是合理的、可行的[8]。

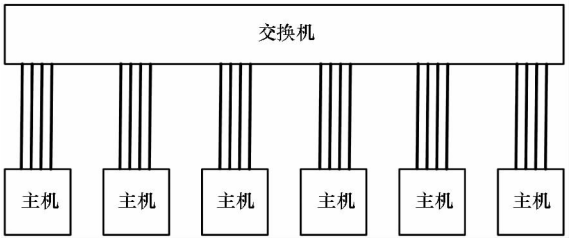
其中,交换机的容量是指此交换机可以连接的主机节点数目,一对交换机之间的带宽容量是指交换机之间的所有带宽。式(1)表示映射到交换机 s_i 上的节点个数不应大于该交换机的端口容量;式(2)表示映射到交换机 s_i 和 s_j 上的节点之间的带宽不大于交换机之间的链路带宽。

图 1 给出了一个简单的映射示例,图 1(a)中实验者要求的逻辑拓扑包含 4 个主机节点和 1 个路由器节点,其中主机 1、2、3 直接连接路由器,而主机 4 与主机 3 通过低速链路相连;图 1(b)中物理拓扑由 6 台主机节点和 1 台交换机构成,每台主机拥有 4 个网络接口。图 1(c)为映射结果,逻辑拓扑中的所有节点都被映射到物理节点上,图中的虚线为空闲链路,实线为实验占用的链路,节点 3 和节点 4 之间的低速链路映射可通过增加中间节点的方式解决[9]。



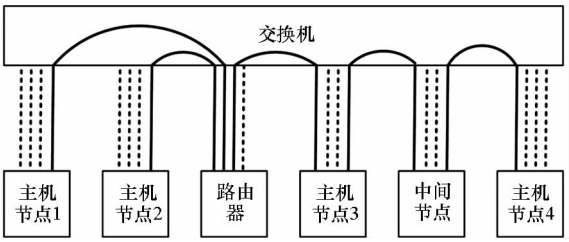
(a) 逻辑拓扑

(a) Virtual topology



(b) 物理拓扑

(b) Physical topology



(c) 映射结构

(c) Mapping instance

图 1 网络实验平台映射示例

Fig. 1 Network testbed mapping instance

2 相关研究

网络安全实验平台映射问题与虚拟网络映射问题类似,均是在共享的底层网络中为带有资源约束的逻辑拓扑分配相应资源。但不同的是,在虚拟网络映射过程中,底层网络允许不同的虚拟网络共享相同的底层节点[10]。网络安全实验平台映射主要是集中映射,现有的典型的集中映射算法[11]主要包括节点、链路不协同两步映射[12],节点链路一步映射[13],基于启发式算法映射[14-15],基于链路规划映射[16],基于路径规划映

射[17]以及基于图的分割的映射[8]等。

文献[8]通过把网络仿真测试床的映射问题转化为图的最小二分,证明了该问题为 NP 完全问题。对于该类复杂问题,可用穷举法求得最优解,但运算的时间复杂度呈指数型增长,在实际中是不可取的。一般情况下,可以运用启发式算法求得该类问题的近优解。比较有代表性的 3 种算法概述如下。

1)网络安全实验平台映射问题的模拟退火算法。模拟退火算法最初由 Metropolis 在 1953 年提出,Kirkpatrick 在 1983 年成功地将其应用在组合最优化问题中。用固体退火模拟组合优化问题,将内能 E 模拟为目标函数值 f,温度 T 演化成控制参数 t,即得到解组合优化问题的模拟退火算法:由初始解 i 和控制参数初值 t 开始,对当前解重复“产生新解→计算目标函数差→接受或舍弃”的迭代,并逐步衰减 t 值,算法终止时的当前解为近似最优解。这是基于蒙特卡洛迭代求解法的一种启发式随机搜索过程。

利用模拟退火算法解决网络实验平台映射问题时,在初始时刻,映射程序维护一个虚拟节点列表,选取一个空的映射方案作为初始解决方案,不断地从虚拟节点列表中选取新节点映射到物理节点上,直至列表为空。在映射的过程中,根据链路类型、物理节点等价类等定义了评价函数(cost function),用来评价一个拓扑映射方案的好坏[9];利用对节点的替换、置换等方式定义新映射方案的生成函数(generation function),用来实现映射方案的变迁。

2)网络测试床映射问题的图分割算法。文献[8]将网络测试床映射问题等价于图的分割问题,即将图分为两个部分,且保证连接两部分的边权重之和最小,基本思想是通过将两部分的节点相向移动,寻找使增益函数 Q 值最大的划分方法,其中 Q 定义为两部分内部边数之和减去两部分外部连接边数之和。

当将网络拓扑图转换为 leaf-DAG(leaf directed acyclic graph)时,采用图的 2 – 划分问题的经典算法 K-L(Kernighan-Lin)算法、F-M(Fiduccia-Mattheyses)算法对网络测试床映射问题进行分析,存在如下问题:

①由于拓扑图中边的权重表示链路的带宽,有可能会很大,从而导致增益序列索引的规模巨大,增加了算法的计算复杂度;

②传统 F-M 算法假设一个节点只能位于图的一个部分,而在 leaf-DAG 中这个结论并不成立,最优划分结果有可能某些节点同时属于两个部分。

因此文献[8]对 F-M 算法进行了相应的改进,使之适用于网络实验平台的映射问题。主要改进有:

①使用指数型 Trie 树结构代替传统算法中的增益序列索引;

②增加 clone 节点的概念,该类型的节点同时部署在图的左右两个部分。

3)基于子图划分的启发式算法。国内刘轶等提出了一种基于子图划分的启发式算法,用以解决网络安全实验平台的映射问题[18]。其算法思想是:为尽量少地占用实验平台的网络资源,应尽可能地将实验者要求的逻辑拓扑中连接紧密的节点映射到同一台交换机上。为此,将实验平台的物理拓扑以交换机为单位分成若干子图,之后在实验者要求的逻辑拓扑上进行迭代,每次迭代按边和权值选取节点进行子图划分,最终得到的划分图即为逻辑拓扑到实验平台物理拓扑的映射结果。

3　基于 K – 划分的网络安全实验平台映射算法

K-L 算法是解决网络安全实验平台映射问题的一个近似贪婪算法,这个算法对于网络拓扑图中顶点的平均度大于 3 的图有着比较令人满意的运行结果和运行时间[19],但是对于稀疏图来说,它所得到的运算结果往往是局部最优值,和实际的最优结果相差较大。另外,K-L 算法最终结果的好坏一定程度上取决于初始划分状态的选择,运算结果也会因初始值的不同相差较大。为了解决这些问题,本文提出了一种基于 K – 划分的网络安全实验平台映射算法。

3.1　算法思路

基于 K – 划分的网络安全实验平台映射方法的算法思路为:

1)根据网络安全实验平台映射问题及其约束条件的形式化描述,对逻辑拓扑进行划分的原则是将尽可能多的节点和带宽资源划分在一个子图中,同时要求划分子图之间带宽资源占用最少。

2)将物理拓扑以交换机为单位划分成若干个子图,每个子图包含一台交换机及与交换机相连的节点。为了简化问题,在此假设物理拓扑是同构的,即每台交换机所连接的节点的个数相同。

3)将逻辑拓扑分成若干子图,每个子图对应于物理拓扑中的一个子图,并且逻辑拓扑子图中节点的个数不大于物理拓扑中子图节点的个数。

3.2 问题描述

用无向图 $G^L=(V^L,E^L)$ 表示逻辑网络拓扑结构，点集 V^L 和边集 E^L 分别代表网络中的节点和节点之间的通信链路，边的权重 $\omega(e^L)$ 表示链路带宽。网络安全实验平台映射问题简化为无向图 G^L 的 K - 划分问题。

下面给出网络安全实验平台映射问题的 K - 最优划分的精确定义。

定义 1 给定一个网络拓扑图 $G=(V,E)$，V 和 E 分别为顶点集和边集。$\forall e\in E,\omega(e)$ 为 e 的权重。将顶点集 V 划分成 K 个子集 $V_1,V_2,\cdots,V_K$，使得该划分之间割边集的权重和最小，其中 $V_1\cap V_2\cap\cdots\cap V_K=\varnothing$，$V_1\cup V_2\cup\cdots\cup V_K=V$。

K - 划分之间割边集权重和表示为：

$$Cost=\sum_{\substack{x\in V_i,y\in V_j\\1\leqslant i\leqslant K,1\leqslant j\leqslant K,\\i\neq j}}\omega(x,y) \tag{3}$$

式中，$\omega(x,y)$ 表示连接顶点 x,y 边的权重。

为了解决无向图 G 的 K - 划分问题，根据图论相关知识[20-21]，定义评价函数。

定义 2 $\forall x\in V_i(1\leqslant i\leqslant K)$，若 $\exists y\in V_j(1\leqslant j\leqslant K,j\neq i)$，有 $e=(x,y)$，则边 e 称作点 x 相对于 V_i 的外部连接边。点 x 相对于 V_i 的外部连接边的权重和记为 E_x。

$$E_x=\sum_{e=(x,y),y\in V_j}\omega(e) \tag{4}$$

定义 3 $\forall x\in V_i(1\leqslant i\leqslant K)$，若 $\exists y\in V_i$，有 $e=(x,y)$，则边 e 称作点 x 相对于 V_i 的内部连接边。点 x 相对于 V_i 的内部连接边的权重和记为 I_x。

$$I_x=\sum_{e=(x,y),y\in V_i}\omega(e) \tag{5}$$

定义 4 $\forall x\in V_i(1\leqslant i\leqslant K)$，$E_x$ 和 I_x 分别为点 x 相对于 V_i 的外部连接边权重和和内部连接边权重和，定义 x 的评价函数为：

$$D(x)=I_x-E_x$$

3.3 具体算法

整个算法如算法 1 所示，令逻辑拓扑结构为 $G^L=(V^L,E^L)$，物理子图中交换机端口容量为 P。算法主要包括两个阶段：

第一阶段：采用贪心法来确定逻辑拓扑划分的初始状态。逐步去掉权重最小的边，直至 G^L 不再连通为止。V^L 被划分成两个子集，这两个子集之间的连边即为割边集，此时为初始划分状态。

在划分时应遵循以下规则：

1）在去边的过程中，不考虑叶子节点，这主要是因为如果边 e 的其中一个顶点为叶子节点，则去掉边 e 得到的两个子图顶点的个数相差太大，影响网络拓扑的平衡。

2）如果有多条边符合选取条件，即这几条边的权重相等，并且去掉它们当中的任何一条边，图都会不连通，则依据以下优先性：

①去掉某条边后，V^L 被划分的子图中至少有一个的节点数不大于物理子图的节点个数；

②如果没有边满足条件①，则在这些权重相等的边中，随机选取一条。

算法 1 基于 K - 划分的网络安全实验平台映射算法

Alg. 1 Network security testbed mapping heuristics based on K - partition

Input：逻辑拓扑 $G^L=(V^L,E^L)$，交换机端口容量 P。

Output：K - 划分结果

Stage1 令 $S=\varnothing$，E' 为图 G^L 中两个端点均非叶子节点的边组成的集合。

Step1 若 $|V^L|>P,E'\neq\varnothing,E'_{\min}=\{e\mid e\in E',\min\omega(e)\}$。

Case1：$\exists E_s\subseteq E'_{\min}$（去掉 E_s 中任何一条边，图 G^L 的连通度大于 1），$\exists e\in E_s$，去掉 e 后 G^L 划分的两个子图 G_1^L 和 G_2^L 的节点个数都小于物理子图的端口容量 P，则选择 e 进行操作，子图 G_1^L 和 G_2^L 为划分的最终结果，结束算法；

否则，选择 G_1^L 和 G_2^L 中有一个节点个数小于 P 的边 e，进行 Stage2；

如果上述两种情况都不满足，则随机选择一条边，进行 Stage2。

Case2：$\forall e\in E'_{\min}$，$G^L-\{e\}$ 后的图仍连通，则任取一条边 $e\in E'_{\min}$ 从 G^L 中去掉。

Step2 $S=S+\{e\}$，$G^L=G^L-\{e\}$，并更新 E'，进行 Step1。

Stage2 G_1^L 和 G_2^L 为 Stage1 确定的初始划分，V_1^L,V_2^L 为其顶点集，其中 $V_1^L\cap V_2^L=\varnothing$，$V_1^L\cup V_2^L=V^L$。设 $|V_1^L|\leqslant|V_2^L|$。

若 $|V_1^L|\leqslant P$，$|V_2^L|>P$，则从 V_2^L 中采用 MoveNode 算法移动 $P-|V_1^L|$ 个节点到 V_1^L 中，设移动节点集合为 V_M，则 $V_1^L=V_1^L+V_M$，$V_2^L=V_2^L-V_M$。

若 $|V_1^L|=P$，$|V_2^L|>P$，则令 $V^L=V_2^L$，从 Stage1 开始迭代划分。

若 $|V_2^L|\leqslant P$，算法终止。

第二阶段：根据评价函数进行节点移动。假如子图的节点个数仍大于端口容量 P，则进行算法迭代，直到所有子图的节点个数不大于端口容

量 P 为止。

在经过第一阶段后,V^L 被划分成两个子集 V_1^L 和 V_2^L,其中 $V_1^L \cap V_2^L = \varnothing$, $V_1^L \cup V_2^L = V^L$。设 $|V_1^L| \leqslant |V_2^L|$。

如果两个子集 V_1^L、V_2^L 中节点个数均小于物理拓扑子图中节点的个数,则不需要移动任何点,即 V_1^L、V_2^L 为划分结果。

如果子集 V_1^L 的节点个数小于物理拓扑子图中节点的个数,V_2^L 的节点个数大于物理拓扑子图中节点的个数,则从 V_2^L 中移动节点到 V_1^L 中,直到 V_1^L 或 V_2^L 中的节点个数等于物理拓扑子图中节点的个数。如果此时 V_2^L 中节点个数仍大于物理拓扑子图中节点的个数,则令 $V^L = V_2^L$ 进行算法迭代,即对 V_2^L 进行划分。

在第二阶段中进行节点移动(如算法 2 所示)。首先计算 V_2^L 中所有节点的评价函数 $D(x)$ 值,选择最小的点 x 进行移动,$V_2^L = V_2^L - \{x\}$, $V_1^L = V_1^L + \{x\}$。然后更新 V_2^L 中所有节点的 $D(x)$ 值,选择使 $D(x)$ 值最小的点进行移动直到满足终止条件。

算法 2　基于 K – 划分的节点移动算法

Alg. 2　Node moving algorithm based on K – partition

节点移动算法:**MoveNode**

Input:移动前的 V_1^L 和 V_2^L, P

Output:移动后的 V_1^L 和 V_2^L

1)计算 V_2^L 中所有点的 $D(x)$ 值($x \in V_2^L$)。

2)选取 $x \in V_2^L \mid \min D(x)$,令 $Q = Q + \{x\}$, $V_1^L = V_1^L + \{x\}$, $V_2^L = V_2^L - \{x\}$;

3)若 $|V_1^L| = P$,算法停止;否则回到步骤 1。

4　评价与分析

从定性分析和实验评价两个方面对本文提出的算法进行分析。定性分析方面主要选取了较新的几种典型集中映射方法进行了对比分析[11-16];在开展实验分析时,选取映射领域最基本的映射算法[9]和启发式算法[18]进行了比较。

4.1　定性分析

基于 K – 划分的网络安全实验平台映射方法属于集中式映射,需要有一个专门的中心实体负责整个映射过程。表 1 对几种典型的映射算法进行了分析。

表 1　典型映射算法分析

Tab. 1　Typical mapping algorithms

典型算法	参考文献	对比分析
节点、链路不协同两步映射	[11]	采用贪婪算法、多商品流算法,两步映射独立,收益较低
节点链路一步映射	[12]	转化为混合整数求解,需要较少的物理资源,但只能应用于小型网络场景
基于启发式算法映射	本文算法	基于 K – 划分的子图划分方法,可以减少物理资源利用,缩短映射时间
基于链路规划映射	[15]	整数规划,多商品流算法,可以获得最优解,但计算复杂度高
基于路径规划映射	[16]	列生成法求解整数规划,映射时间大大减少

4.2　实验评价与分析

对网络安全实验平台映射方法的评价主要从两个方面进行——映射算法的运行时间和映射算法的质量,采用实验实例的误差比例来进行映射算法质量的比较。

利用 BRITE 拓扑生成器,采用 Waxman 模型随机动态生成网络拓扑来验证基于 K – 划分问题的网络安全实验平台映射算法。

测试用的物理拓扑主要包括两种:

1)一种包含 120 个节点,分别连接到 3 个交换机上,用于测试 10 ~ 100 个节点的网络拓扑映射;

2)一种包含 525 个节点,分别连接到 7 个交换机上,用来测试 100 ~ 500 个节点的网络拓扑映射。

4.2.1　求解时间

图 2 和图 3 给出了基于 K – 划分问题的映射、启发式算法以及模拟退火算法最优解[9]之间的求解时间对比(纵坐标中 t_{run} 为运行时间,其单位为 ms),可以看出本文算法的计算开销要比模拟退火算法小得多,并且随着节点个数增加也很明显,说明本文算法的可扩展性更好。启发式算法的求解时间跟本文算法基本差不多。

4.2.2　误差比例

为了对映射问题求解质量进行比较,采用如式(7)所示公式进行误差比例的求解:

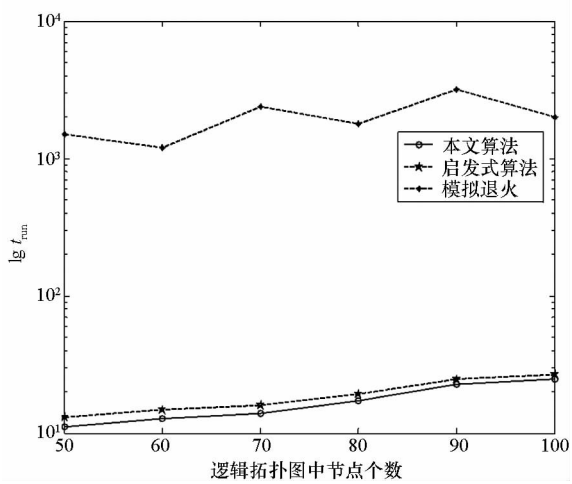


图 2 BRITE 120 测试集的运行时间

Fig. 2 Runtime for the BRITE 120 test set

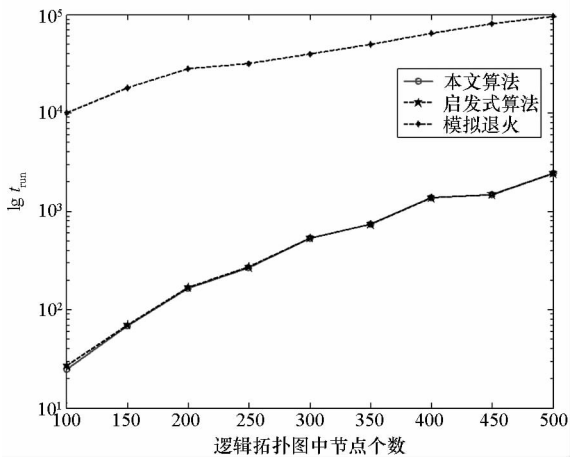


图 3 BRITE 525 测试集的运行时间

Fig. 3 Runtime for the BRITE 525 test set

$$Error = (median - opt)/opt \tag{7}$$

式中，*median* 为实验算法映射结果的平均值，*opt* 为映射结果的最优值。评价值为 K – 划分割边集的权重和，由式(3)进行计算。在实际计算中，最优值无法得到时，采用近优解来代替。

在网络安全实验平台规模较小时，用穷举算法求出最优解；随着规模的增大，由于穷举算法的求解时间过长，用遗传算法求出的近优解代替最优解。

图 4 给出了基于 K – 划分问题的映射算法、启发式算法与最优解的误差比例，可以看出本文算法可以得到近优解，启发式算法的误差比例稍大。节点个数小于 40 时，误差没有是因为此时所有节点分配到一个交换机上，同时算法能够很好地完成分配。

5 结论

基于网络安全实验平台开展实验时，一个重要的问题是将实验者需要的网络拓扑映射到实验平台上。本文对网络安全实验平台映射问题进行了形式化描述，定义了评价函数，提出了基于 K – 划分的映射方法。该算法采用贪心法确定初始划分状态，根据评价函数进行节点移动，对生成的子图进行算法迭代，直到所有子图的节点数量不大于物理拓扑端口容量为止。基于 K – 划分的映射方法解决了 K-L 算法中初始划分状态选取的任意性对最终结果产生较大影响的缺陷，实验结果表明该算法的求解时间远小于遗传算法，能在较短的时间内得到映射结果。

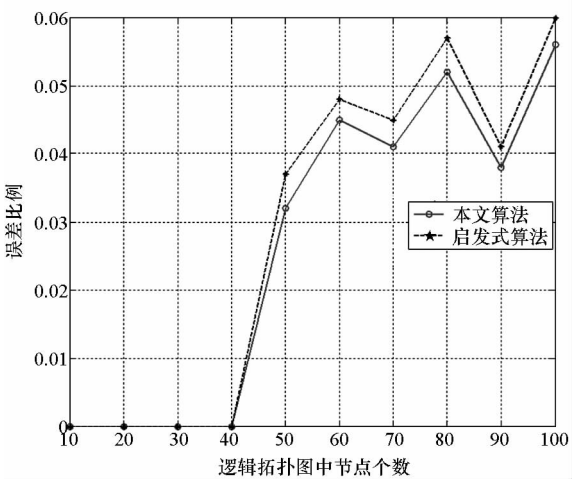


图 4 误差比例

Fig. 4 Error ratio

下一步研究基于 K – 划分的映射方法在虚拟网络映射、无线网络映射中的应用，为开展网络安全实验提供更好的实验平台。

参考文献(References)

[1] The University of Utah. Emulab-network emulation testbed home [EB/OL]. [2016 - 11 - 01]. http://www.emulab.net/.

[2] Karlin S. PlanetLab design notes[EB/OL]. [2016 - 10 - 15]. http://www.planet-lab.org/doc/pdn.

[3] Benzel T. The science of cyber-security experimentation: the DETER project [C]//Proceedings of the 27th Annual Computer Security Applications Conference, 2011: 137 - 148.

[4] Wroclawski J, Benzel T, Blythe J, et al. DETERLab and the DETER project[M]// McGeer R, Berman M, Elliott C, et al. The GENI Book. Switzerland: Springer International Publishing, 2016: 35 - 62.

[5] Gavras A, Karlia A, Fdida S, et al. Future internet research and experimentation: the FIRE initiative[J]. ACM SIGCOM Computer Communication Review, 2007, 37(3): 89 - 92.

[6] Nakao A, Ozaki R, Nishida Y. CoreLab: an emerging network testbed employing hosted virtual machine monitor[C]//Proceedings of the ACM CoNEXT Conference, 2008: 73.

[7] 郑毓芹, 陈立达, 曾世贤, 等. 台湾网络测试平台建置历程[J]. 资讯安全通讯, 2007, 13(4): 16 – 85.
ZHENG Yuqin, CHEN Lida, ZENG Shixian, et al. Construction process of Taiwan network testbed [J]. Communications of the CCISA, 2007, 13(4): 16 – 85. (in Chinese)

[8] McGeer R, Andersen D G, Schwab S. The network testbed mapping problem[C]//Proceedings of the 6th International ICST Conference, 2010: 383 – 398.

[9] Ricci R, Alfeld C, Lepreau J. A solver for the network testbed mapping problem [J]. ACM SIGCOMM Computer Communication Review, 2003, 33(2): 65 – 81.

[10] 程祥, 张忠宝, 苏森, 等. 虚拟网络映射问题研究综述[J]. 通信学报, 2011, 32(10): 143 – 151.
CHENG Xiang, ZHANG Zhongbao, SU Sen, et al. Survey of virtual network embedding problem [J]. Journal on Communications, 2011, 32(10): 143 – 151. (in Chinese)

[11] 胡帅. 虚拟网络映射算法研究[D]. 南京:南京邮电大学, 2017.
HU Shuai. Study on virtual network embedding algorithms[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2017. (in Chinese)

[12] Yu M L, 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.

[13] Shanbhag S, Kandoor A R, Wang C, et al. VHub: single-stage virtual network mapping through hub location [J]. Computer Networks, 2015, 77: 169 – 180.

[14] Wang X G, Zheng X W, Lu D J. A heuristic virtual network mapping algorithm [C]//Proceedings of International Conference on Intelligent Computing, 2014: 385 – 395.

[15] Inführ J, Raidl G. A memetic algorithm for the virtual network mapping problem [J]. Journal of Heuristics, 2016, 22(4): 475 – 505.

[16] Melo M, Carapinha J, Sargento S, et al. Virtual network mapping—an optimization problem[C]//Proceedings of the Third International ICST Conference, 2011: 187 – 200.

[17] Mijumbi R, Serrat J, Gorricho J L, et al. A path generation approach to embedding of virtual networks [J]. IEEE Transactions on Network and Service Management, 2015, 12(3): 334 – 348.

[18] 刘轶, 肖凯平, 李艳萍. 一种网络仿真实验床映射问题的启发式算法[J]. 西安交通大学学报, 2006, 40(8): 878 – 882.
LIU Yi, XIAO Kaiping, LI Yanping. Heuristic algorithm for mapping problem of network emulation testbed[J]. Journal of Xi′an Jiaotong University, 2006, 40(8): 878 – 882. (in Chinese)

[19] Selvakkumaran N, Karypis G. Multi-objective hypergraph-partitioning algorithms for cut and maximum subdomain-degree minimization [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and System, 2006, 25(3): 504 – 517.

[20] Ng T K, Oldfield J, Pitchumani V. Improvements of a mincut partition algorithm[J]. Environmental Science & Technology, 1984, 18(11): 340.

[21] 赵晶. 2 – 划分问题的算法改进和相关性质[D]. 天津: 南开大学, 2009.
ZHAO Jing. Improvement and properties of the two-way partitioning[D]. Tianjin: Nankai University, 2009. (in Chinese)