基于能力度量的网络安全实验环境多仿真规划

曾子懿 邱 菡 朱俊虎 周天阳

(战略支援部队信息工程大学 郑州 450001) (国家数字交换系统工程技术研究中心 郑州 450001)

摘 要 多种仿真技术的融合使用可为网络安全实验环境的构建提供灵活的资源分配,其难点在于如何兼顾逼真度需求。针对该问题,文中提出了一种"按需分配"的多仿真规划方法。首先,以仿真能力定义逼真度需求,将复杂、抽象、无结构化的需求表示为简单、具体、结构化的形式;接着,给出了一种基于默认拒绝策略的逼真度需求满足性判定准则以及一种基于贪心策略的多仿真方案求解算法。在蠕虫样本传播的仿真环境构建实验中,运用该方法求解的仿真方案可在满足逼真度需求的条件下取得最小的仿真代价。

关键词 能力度量,逼真度需求刻画,多仿真规划,贪心策略

中图法分类号 393.01 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.024

Network Security Experiment Environment Multi-emulation Planning Based on Capability Measurement

ZENG Zi-yi QIU Han ZHU Jun-hu ZHOU Tian-yang

(Information Engineering University, Zhengzhou 450001, China)

(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450001, China)

Abstract The combined usage of multiple emulation technologies can provide flexible resource allocation for construction of experimental environment for network security. Its difficulty lies in how to balance the fidelity requirements. A multi-emulation planning method based on "distribution on demand" was proposed for this problem. Firstly, the emulation capability is used to define the fidelity requirement, and then the complex, abstract and unstructured requirements are represented as simple, concrete and structured forms. Secondly, a fidelity satisfaction decision criterion based on default rejection strategy and a multi-emulation scheme solving algorithm based on greedy strategy are given. In the experiment of emulation environment construction of worm sample propagation, the emulation scheme solved by this method can obtain the minimum emulation cost under the condition of satisfying the fidelity requirement.

Keywords Capability measurement, Fidelity requirement representation, Multi-emulation planning, Greedy strategy

1 引言

由于网络安全技术具有破坏性,因此网络安全实验主要依靠仿真环境而非现网环境。网络仿真可分为模型模拟以及基于虚拟化的仿真两大类,前者包括诸如 opnet[1] 和 ns3[2] 的网络模拟软件,在抽象建模的基础上提供对大规模复杂网络行为的分析能力;后者采用虚拟化技术对网络进行仿真,虚拟化技术包括 xen[3] 和 docker[4] 等节点虚拟化技术以及 dummynet[5] 和 NVF[6] 等链路虚拟化技术,较前者可更为逼真地复现网络环境和用户行为,在网络安全实验环境构建领域中占据主流地位[7]。虚拟化技术在节点、链路的复现程度上存在差异,轻量级虚拟化技术由于缺失实现细节,其仿真逼真度与仿真代价都较低;重量级虚拟化技术相反,对节点、链路的刻画更为细致,其仿真逼真度与仿真代价都较高。

在网络仿真时,高仿真逼真度意味着高仿真代价[8],需要在两者之间做出权衡。Siaterlis 等[9] 指出,从满足实验需求的角度出发,仿真网络并不需要完全复制现实网络中的所有细节,仿真环境仅需提供足以支撑验证实验假设的逼真度即可,例如一些实验关注路由器的实现细节;而另一些实验可能仅需要使用软件路由或流量生成器即可。进一步来说,仿真网络的逼真度需求可能是多分辨率的,即一个仿真网络中不同网络节点和链路的逼真度需求可能是不同的。例如,在为广域网蠕虫传播样本设计的仿真实验中,路由节点的逼真度需求可能更高[10]。在网络安全测试床中,常常需要同时运行多组安全性实验。因此,按照实验的不同,逼真度需求在多仿真融合条件下分配仿真技术,能够在满足逼真度需求的前提下减少资源开销,以提升实验请求的接受率。

现有的研究多致力于解决多仿真框架的设计问题以实现多种仿真技术的融合使用。例如,著名的网络安全测试床 Deterlab 实现了一种基于 Container 的多仿真融合框架[10],能

到稿日期:2018-07-09 返修日期:2018-09-04 本文受国家自然科学基金(61502528)资助。

曾子懿(1989-),男,博士生,主要研究方向为网络建模仿真、网络空间安全,E-mail:zyzeng7@163.com;**邱 菡**(1981-),女,博士,副教授,主要研究方向为网络空间安全、网络安全行为建模与评估,E-mail:qiuhan410@aliyun.com(通信作者);**朱俊虎**(1974-),男,博士,教授,主要研究方向为网络空间安全;**周天阳**(1979-),男,博士生,副教授,主要研究方向为网络空间安全。

够同时融合使用 4 种节点虚拟化技术。然而,仅具备多仿真融合能力对于实现“按需分配”的最终目标是远远不够的,其第一步是逼真度需求的获取。Wroclawski 等[10]认为从实验描述和研究者意图的其他表达中提取对逼真度需求的充分理解并不容易。究其原因,是没有明确的逼真度需求刻画方法。因此,首先对逼真度需求刻画方法展开研究。

在刻画逼真度需求之后,多仿真规划需要解决两个问题:1)逼真度需求的可满足判定问题;2)以逼真度需求可满足为约束的仿真代价的最优化问题。第一个问题是任给一个仿真技术集,给出仿真技术是否满足仿真网络中每一节点、链路逼真度需求的判定准则;第二个问题以第一个问题的解为基础,求解满足最小化仿真代价的多仿真方案。

根据图 1,本文针对网络安全多仿真规划中的需求刻画问题,提出一种基于能力度量的需求刻画方法。在此基础之上,给出逼真度需求的可满足判定,并以逼真度需求可满足为约束,提出一种仿真代价的最优化算法。

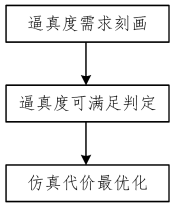

图 1　多仿真规划问题的分解

Fig. 1　Decomposition of multi-emulation planning problem

2　基于能力度量的逼真度需求刻画

在刻画逼真度需求之前,首先应该明确什么是逼真度需求。从多仿真规划的角度来看,逼真度需求是指确保网络安全实验环境和支撑实验假设验证的一些约束,能够指导后续多仿真方案的求解。从这一点出发,给出的约束应当越直接越好,最理想的方法是由实验设计者直接给出每个节点、链路的仿真技术。逼真度需求即为对节点、链路仿真技术的指派。仿真系统根据这些指派,直接构建仿真网络而无须进行判定和计算。这种方式要求实验设计者必须对仿真技术和多仿真系统都有比较深入的了解,这在大多数情况下是难以施行的。逼真度需求的刻画应该将实验设计者的知识水平纳入考虑范围。

逼真度需求作为一种能够指导后续多仿真方案求解的约束,应以简单、具体、结构化的形式表达。仿真能力是仿真技术对于节点或链路复现特性的一种描述,例如自然语言“xen 支持对 windows 操作系统的虚拟化”,表示 xen 能够虚拟出一个节点,在这个节点上可安装 windows 操作系统,并支持在 windows 系统之上进行各类操作。利用仿真能力来刻画逼真度需求是可行的,这是因为仿真能力是仿真技术的固有属性,通过限定仿真能力,能够约束仿真技术的选择。而对于仿真能力,可以构建一套简单、具体、结构化的方式来表达。不仅如此,通过调整仿真能力的描述粒度,可以在实验设计者的知识水平要求和逼真度需求描述精细度要求之间进行权衡。下面给出仿真能力的定义。

定义 1　仿真能力是一个描述节点或链路复现特性的有序二元组,记为 $\Delta=(\omega,\xi)$。

对于一个仿真能力 $\Delta=(\omega,\xi)$,ω 是仿真能力标识,用于区分不同的仿真能力;ξ 描述了在该仿真标识下的“取值”,可以是一个字符串类型或是一个由字符串组成的集合。仿真能力 $\Delta_1=$(“*running_env*”,“windows”)表示能够运行 windows 程序,而仿真能力 $\Delta_2=$(“*node_type*”,“router”)表示可复现路由节点。这种表述方式具有可扩展性,可以通过定义仿真能力 $\Delta_3=$(“*node_type*”,{“host”,“router”})来扩展 Δ_2。基于定义 1,可定义仿真能力与仿真技术的从属关系。

设 T 是仿真技术集,对于仿真技术 $t_j\in T$,将 t_j 的仿真能力集记为 $h(t_j)=\{\Delta_1,\Delta_2,\cdots,\Delta_n\}$。进一步,仿真技术集上的能力集可以记为 $A_T=\{h(t_j)\mid t_j\in T\}$。当 T 确定时,A_T 可在利用本体理论等知识工程手段对 T 中的仿真技术逐一分析的基础上进行构建。

定义 2　设网络 $G=(N,L)$,E 是 G 上的一个考察集,$E\subset N\cup L$。对于实体 $e_i\in E$,其逼真度需求是由一组仿真能力组成的集合,记为 $f(e_i)=\{\Delta\mid\Delta$ 描述了 e_i 的逼真度需求,$e_i\in E\}$。

定义 3　网络 G 在 E 上的逼真度需求是实体考察集 E 中实体对应的逼真度需求组成的集合,记为 $R_E=\{f(e_i)\mid e_i\in E\}$。

当实验者对网络中的某些部分有明确要求时,可预先指定网络中的部分节点与链路的仿真技术。此时,规划的对象实际上是网络中未指定的部分。因此在定义 2 和定义 3 中,引入考察集 E 的概念。

3　逼真度需求可满足判定

多仿真规划的第二个问题是逼真度需求可满足判定,即任给一个仿真技术集,判定其是否满足网络考察集上的逼真度需求。首先定义多仿真方案。

定义 4　多仿真方案 $S=(s_{ij})$ 表示从考察集 $E=\{e_i\}$ 到仿真技术集 $T=\{t_j\}$ 映射的一个矩阵,其中 $s_{ij}=1$ 表示采用 t_j 仿真 e_i,而 $s_{ij}=0$ 则表示不采用 t_j 仿真 e_i。

解决问题的第一步是定义仿真技术对实体逼真度需求的可满足性,其基础是定义仿真能力集合之间的运算。

定义 5　对于仿真能力 Δ 和仿真能力 Δ',$\Delta\oplus\Delta'$ 是 Δ 到 Δ' 的一次考察。

定义 6　对于 Δ 到 Δ' 的一次考察 $\Delta\oplus\Delta'$,当 $\omega=\omega'$ 且 ξ 与 ξ' 之间满足:1)$\xi=\xi'$;2)$\xi\in\xi'$;3)$\xi\subset\xi'$ 关系时,有 $\Delta\oplus\Delta'=1$,表示 Δ 可被 Δ' 满足;否则 $\Delta\oplus\Delta'=0$,表示 Δ 不可被 Δ' 满足。

举例说明考察运算:由定义 5 和定义 6 可知,对于仿真能力 $\Delta=$(“*running_env*”,“windows”)与 $\Delta'=$(“*running_env*”,{“windows”,“linux”}),有 $\Delta\oplus\Delta'=1$。对于仿真能力 $\Delta=$(“*interface_num*”,“4”)与 $\Delta'=$(“*interface_num*”,{“1”,“2”,“3”}),有 $\Delta\oplus\Delta'=0$。

实体 e_i 的逼真度需求 $f(e_i)$ 是一个仿真能力集。当 $f(e_i)$ 中的所有元素都可被满足或者都不可被满足时,判定逼真度需求 $f(e_i)$ 的可满足是相对容易的。可以认为:当 $f(e_i)$ 中所有的元素都被满足时,$f(e_i)$ 可被满足;反之,$f(e_i)$ 不可被满

足。而当 $f(e_i)$中部分元素可被满足时,根据不同的策略可以得到不同的结果。当采用默认拒绝策略时,判定 $f(e_i)$不可被满足;当采用默认接受策略时,判定 $f(e_i)$可被满足。默认拒绝策略是以仿真逼真度的"木桶效应"理论[11]为依据,其优点是有利于支撑实验假设验证,然而其对仿真技术的考察较严,逼真度需求不易被满足。与之相反,默认接受策略虽然可能放松对仿真技术的限制,得到更多备选的仿真技术,但对于实验假设的验证并无益处,反而影响了逼真度判定的准确性。因此,本文基于默认拒绝策略给出逼真度需求可满足判定准则。

定义 7 对于仿真能力集 U 和仿真能力集 U',$U\odot U'$是 U 在 U'上的一次考察。

定义 8 给定 U 到 U'的一次考察 $U\odot U'$,当对于任意 $\Delta\in U$ 都存在 $\Delta'\in U'$使得 $\Delta\oplus\Delta'=1$时,有 $U\odot U'=1$,否则 $U\odot U'=0$。

基于定义 7 和定义 8 可给出多仿真方案 S 对网络 G 在 E 上的逼真度需求的可满足性定义。

定义 9 给定网络 G 上的一个考察集 E 到仿真技术集 T 的一个多仿真方案 $S=(s_{ij})$,当对于任意 $s_{ij}=1$,都有 $f(e_i)\odot h(t_j)=1$时,S 满足网络 G 在 E 上的逼真度需求。

4 仿真代价最小化

在满足逼真度需求可满足的约束下,应通过最优化算法得到资源消耗最小的多仿真方案。首先需要明确仿真代价,接着将对问题进行形式化描述,最后基于贪心策略设计仿真代价最小化算法。

4.1 仿真代价

仿真代价是仿真过程中消耗的实际物理资源。为了简化表述,可直接使用仿真资源需求作为仿真代价。例如,Vsphere 生成多个虚拟机时,其仿真代价就表示为所申请的 CPU、内存大小。在单一仿真条件下,这种简化是合理的,这是因为相同的虚拟硬件资源消耗可转化为近似相同的实际物理资源消耗。然而在多仿真条件下,不同仿真技术的实现导致了相同的虚拟硬件资源需求对应的实际物理资源消耗可能具有较大差异。

不仅如此,多仿真中的实体可能运行在不同的层级。例如在包含 view-os[12] 和 QEMU[13] 的多仿真环境中,view-os 仿真的节点本身可能运行在 QEMU 虚拟机之上,与直接使用 QEMU 虚拟机仿真的节点处在不同的运行层级。这种仿真实现的"嵌套",使得虚拟资源需求向实际仿真代价的转化过程变得十分复杂。因此,在多仿真条件下直接使用虚拟硬件资源需求表示仿真代价并不合适。

解决上述问题的一种相对简单、有效的方式是通过为仿真技术集指定一组相对代价系数,使每一个相对转化系数对应一种仿真技术,来体现仿真实现对仿真代价的影响。相对转化系数并不是对转化率严格意义上的衡量,而是用来体现多仿真条件下资源需求向实际物理资源消耗转化的差异。那么,资源需求为 d_i 的实体 e_i 在相对代价系数为 α_j 的仿真技术 t_j 下的仿真代价为:

$$c_{ij}=d_i\times\alpha_j \tag{1}$$

用 $C=(c_{ij})$表示待考察的考察集 E 在仿真技术集 T 上的仿真代价,用 $D=\{d_i\mid e_i\in E\}$表示考察集 E 的一组资源需求,用 $A=\{\alpha_j\mid t_j\in T\}$表示仿真技术集 T 的一组代价系数。

4.2 问题的形式化描述

对于一次多仿真规划而言,希望找到一个满足 E 上逼真度需求的多仿真方案 $S=(s_{ij})$,使得 E 中每一个实体的仿真代价之和最小化。s_{ij} 指定实体 e_i 是否采用仿真技术 t_j 仿真,取值为 0 或 1;c_{ij} 表示实体 e_i 采用仿真技术 t_j 仿真的仿真代价。因此,总仿真代价的计算如式(2)所示:

$$\sum_{i=1}^{|E|}\sum_{j=1}^{|T|}s_{ij}c_{ij} \tag{2}$$

在总仿真代价最小的多仿真方案中,需做如下约束:1)每个实体仅被指定由一种仿真技术生成,即 S 中每一个行向量的元素之和为 1;2)实体仿真需求都可满足,即当仿真技术 t_j 满足 e_i 的仿真需求时,s_{ij} 可为 0 或 1。反之 s_{ij} 只能为 0。

因此,多仿真规划问题的整数规划形式可以表示为:

$$\text{minimum}\sum_{i=1}^{|E|}\sum_{j=1}^{|T|}s_{ij}c_{ij} \tag{3}$$

满足如下约束条件:

$$\sum_{j=1}^{|T|}s_{ij}=1(\forall e_i\in E) \tag{4}$$

$$s_{ij}\leqslant f(e_i)\odot h(t_j)(\forall e_i\in E,t_j\in T) \tag{5}$$

$$s_{ij}\in\{0,1\}(\forall e_i\in E,t_j\in T) \tag{6}$$

约束条件(4)保证了每个实体仅由一种仿真技术生成;约束条件(5)保证了实体仿真需求是可满足的;约束条件(6)是由定义 4 决定的。

4.3 基于贪心策略的仿真代价的最小化

通过观察约束条件可发现求解过程中 s_{ij} 的赋值顺序对目标函数的计算不会产生影响。在这种情况下,目标函数的最优化完全依赖于式(1)中每一项的最优值。因此,求解过程中前一步的最佳选择对于后一步来说也同样是最佳选择,设计的算法不必具备回溯能力。基于贪心策略的算法在解决上述问题时能够得到最优解。为此,本文基于贪心策略求解最优解,具体的算法如算法 1 所示。

算法 1 基于贪心算法的多仿真融合规划

输入:仿真需求 R_E,仿真技术能力集 A_T,资源需求集 D,相对代价系数集 A

输出:仿真方案 S

```
S←0,min c←∞
for i=1 to |E| do
  for j=1 to |T| do
      t←0,c_ij=d_i×α_j
    if f(e_i)⊙h(t_j)=1 & min c>c_ij then
          t←j,min c←c_ij
  if t=0 then
      return null
    s_it=1
return S
```

5 蠕虫样本传播实验

文献[14]指出蠕虫样本传播实验是一种典型的逼真度需求多分辨率场景,主要涉及端节点与路由节点两类网络节点。

本文使用该实验来验证所提方法的有效性。跨平台蠕虫样本传播实验的目的是探究实际蠕虫样本在无防护网络中传播的过程是否符合模型假设，其简化网络拓扑结构如图 2 所示，其中 1－8 是端节点，9－14 是路由节点。蠕虫样本经由网络在端节点之间传播。为了便于说明问题，仅考虑节点仿真技术的选取，因此考察集 E 包含节点 1－14。由于节点资源需求的设置对说明方法的有效性没有影响，因此假设 D 中的任意资源需求 $d_i=1$。

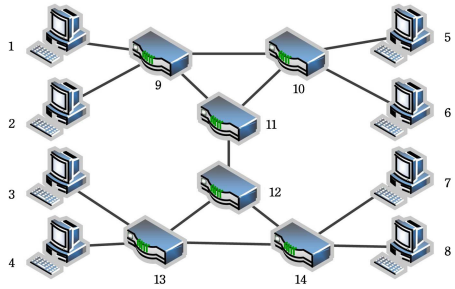

图 2　蠕虫样本传播实验的网络拓扑

Fig. 2　Network topology of worm sample propagation experiment

在该实验中，蠕虫样本利用内核漏洞对 windows 操作系统发起攻击。为了确保蠕虫样本能够正常感染主机，主机应该具备蠕虫样本的实际运行条件。虽然蠕虫样本不具备感染路由器节点的能力，但路由器节点提供路由功能，不同的路由配置会对蠕虫传播结果造成影响，因此仍需要对路由器节点进行仿真。节点逼真度需求只因节点类型不同而存在差异。

设仿真技术集 T 包含两个待考察的仿真技术 t_1 和 t_2，其中 t_1 为 QEMU，t_2 为 view-os。选择上述两种仿真技术的原因是其在仿真能力上具有一定代表性，其中 QEMU 构建了完整的硬件模型，可在一台物理机上仿真多个实验；view-os 是一种软件级抽象的虚拟化技术，能够为进程提供独立的资源视图，使进程之间的文件系统、网络栈等系统资源相互独立，相同的物理资源条件下，能够仿真更多的节点。根据仿真技术特点，设置 T 的仿真代价系数 $A=\{1.0,0.1\}$。根据式(1)，可计算出仿真代价 c_{ij}。当 $j=1$ 时，$c_{ij}=1$；当 $j=2$ 时，$c_{ij}=0.1$。

为了说明方法的有效性，假定基于 QEMU 虚拟化的仿真能力 $h(t_1)$ 为{(“*sim_level*”,“system”),(“*running_env*”,{“linux”,“windows”,“mac”}),(*node_type*,{“host”,“router”}),(“*router_type*”,“software”),(“*running_syscall*”,“unmodified”)}。基于 view-os 虚拟化的仿真能力 $h(t_2)$ 为{(“*sim_level*”,“process”),(“*running_env*”,{“linux”}),(“*node_type*”,{“host”,“router”}),(“*router_type*”,“software”),(“*running_syscall*”,“modified”)}。

5.1　基于能力度量的多仿真规划

逼真度需求可由定义 2 根据 $h(t_1)$，$h(t_2)$ 中划定的仿真能力要素得到。端节点 e_1 的逼真度需求 $f(e_1)$ 为{(“*sim_level*”,“system”),(“*running_env*”,“windows”),(“*running_syscall*”,“unmodified”)}，且 $f(e_1)=f(e_2)=\cdots=f(e_8)$。端节点逼真度需求明确指出需要对 windows 操作系统进行完整的仿真，并且不能修改系统调用，而路由节点仅需要仿真软路由功能即可。因此，路由节点 e_9 的逼真度需求 $f(e_9)$ 为{(“*node_type*”,“router”),(“*router_type*”,“software”)}，且 $f(e_9)=f(e_{10})=\cdots=f(e_{14})$。根据定义 4 可得逼真度需求 $R_E=\{f(e_i)\mid e_i\in E\}$。

在节点 e_1，e_9 上考察仿真技术 t_1 和 t_2 的可满足性，根据定义 5－定义 8 可得：

$$f(e_1)\odot h(t_1)=1 \tag{7}$$

$$f(e_9)\odot h(t_1)=1 \tag{8}$$

$$f(e_1)\odot h(t_2)=0 \tag{9}$$

$$f(e_9)\odot h(t_2)=1 \tag{10}$$

将 R_E，A_T，r，α 输入算法可得：

$$S_1=\begin{pmatrix}1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\end{pmatrix}^{\mathrm{T}}$$

此时总的仿真代价为 8.6。

5.2　仿真方案的比较

将仿真方案 S_1 与全 QEMU 仿真方案 S_2 以及全 view-os 仿真方案 S_3 在可满足性判定和仿真代价方面进行比较。具体来说，S_2 和 S_3 为：

$$S_2=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\end{pmatrix}^{\mathrm{T}}$$

$$S_3=\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\end{pmatrix}^{\mathrm{T}}$$

其可满足性和仿真代价如表 1 所列。其中，仿真方案 S_2 虽然可满足逼真度需求，但仿真代价较高；仿真方案 S_3 虽然仿真代价较低，但并不能满足逼真度需求；基于能力度量的多仿真规划方案在满足逼真度需求的基础上具有更小的仿真代价。

表 1　3 种仿真方案的比较

Table 1　Comparison of three emulaltion schemes

仿真方案	可满足判定	仿真代价
S_1	可满足	8.6
S_2	可满足	14
S_3	不可满足	0.14

结束语　多仿真规划的核心问题是逼真度需求的有效刻画。基于仿真能力的需求刻画方式能够将复杂、抽象、无结构化的需求表示为简单、具体、结构化的形式。在此基础之上，可以进一步给出逼真度需求的判定准则。不同仿真方案可由该准则判定是否满足逼真度需求，使得不同仿真方案能够进行量化比较，为仿真代价最小化提供约束条件。通过蠕虫样本传播实验可证明基于能力度量的网络安全实验环境多仿真规划方法的有效性。通过与两种单一虚拟化仿真方案进行比较，基于能力度量的网络安全环境多仿真规划求解的多仿真方案在满足逼真度需求的基础上具有更小的仿真代价。

本文的主要工作是探讨基于能力度量的多仿真规划的可行性与有效性。在实际使用过程中需针对不同的测试床实现，并归纳其仿真能力集。另外，如何衡量资源消耗和比较不同的仿真方法获取仿真代价系数，以支持可靠地预测资源消耗，也是亟待解决的问题。

（下转第 186 页）

[7] XIAO X,TAO Y. Personalized privacy preservation[C]// ACM SIGMOD International Conference on Management of Data. ACM,2006:229-240.

[8] XU Y,QIN X,YANG Z,et al. A personalized k-anonymity privacy preserving method[J]. Journal of Information & Computational Science,2013,10(1):139-155.

[9] WANG P. Personalized Anonymity Algorithm Using Clustering Techniques[J]. Journal of Computational Information Systems,2011,7(3):924-931.

[10] YE X,ZHANG Y,LIU M. A Personalized (a,k)-Anonymity Model[C]// The Ninth International Conference on Web-Age Information Management. IEEE Computer Society,2008:341-348.

[11] HAN J,YU H,YU J,et al. A Complete (α,k)-Anonymity Model for Sensitive Values Individuation Preservation[C]// International Symposium on Electronic Commerce and Security. IEEE,2008:318-323.

[12] SHEN Y,GUO G,WU D,et al. A novel algorithm of personalized-granular k-anonymity[C]// International Conference on Mechatronic Sciences, Electric Engineering and Computer. IEEE,2013:1860-1866.

[13] WANG B,YANG J. A personalized anonymous method based on inverse clustering[J]. Acta Electronica Sinica,2012,40(5):883-890. (in Chinese)
王波,杨静. 一种基于逆聚类的个性化隐私匿名方法[J]. 电子学报,2012,40(5):883-890.

[14] WANG B,YANG J. Research on Anonymity Technique for Personalization Privacy-preserving Data Publishing[J]. Computer Science,2012,39(4):168-171. (in Chinese)
王波,杨静. 数据发布中的个性化隐私匿名技术研究[J]. 计算机科学,2012,39(4):168-171.

[15] PRASSER F,BILD R,EICHER J,et al. Lightning:Utility-Driven Anonymization of High-Dimensional Data[J]. Transactions on Data Privacy,2016,9(2):161-185.

[16] SUN X,WANG H,LI J,et al. Enhanced P-Sensitive K-Anonymity Models for Privacy Preserving Data Publishing[J]. Transactions on Data Privacy,2008,1(2):53-66.

[17] KAN Y Y,CAO T J. Enhanced privacy preserving K-anonymity model:(α,L)-diversity K-anonymity[J]. Computer Engineering and Applications,2010,46(21):148-151. (in Chinese)
阚莹莹,曹天杰. 一种增强的隐私保护 K-匿名模型—(α,L)多样化 K-匿名[J]. 计算机工程与应用,2010,46(21):148-151.

[18] XU J,WANG W,PEI J,et al. Utility-based anonymization for privacy preservation with less information loss[J]. ACM SIGKDD Explorations Newsletter,2006,8(2):21-30.

[19] LIU X,XIE Q,WANG L. Personalized extended (α,k)-anonymity model for privacy-preserving data publishing[J]. Concurrency & Computation Practice & Experience,2017,29(6):e3886.

[20] BLAKE C. UCI repository of machine learning databases[OL]. http://www.ics.uci.edu/~mlearn/MLRepository.html.

(上接第 163 页)

参 考 文 献

[1] ALKHATHAMI M,ALAZZAWI L,ELKATEEB A. Large Scale Border Security Systems Modeling and Simulation with OPNET [C]// Computing and Communication Workshop and Conference (CCWC). IEEE,2017:1-8.

[2] MEHIC M,MAURHART O,RASS S,et al. Implementation of Quantum Key Distribution Network Simulation Module in the Network Simulator NS-3 [J]. Quantum Information Processing,2017,16(10):253.

[3] ORGERIE A C,ASSUNCAO M D,LEFEVRE L. A Survey on Techniques for Improving the Energy Efficiency of Large-scale Distributed Systems [J]. ACM Computing Surveys,2014,46(4):1-31.

[4] BOETTIGER C. An introduction to Docker for reproducible research[J]. ACM SIGOPS Operating Systems Review,2015,49(1):71-79.

[5] LUBKE R,BUSCHEL P,SCHUSTER D,et al. Measuring Accuracy and Performance of Network Emulators [C]// 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). IEEE,2014:63-65.

[6] MIJUMBI R,SERRAT J,GORRICHO J L,et al. Network Function Virtualization:State-of-the-art and Research Challenges [J]. IEEE Communications Surveys & Tutorials,2016,18(1):236-262.

[7] FANG B X,JIA Y,LI A P,et al. Cyber Ranges:State-of-the-art and Research Challenges [J]. Journal of Cyber Security,2016,1(3):1-9. (in Chinese)
方滨兴,贾焰,李爱平,等. 网络空间靶场技术研究[J]. 信息安全学报,2016,1(3):1-9.

[8] YANG R,LIU Y K. Simulation Fidelity Theory and Measurement:A Literature Review [J]. System Simulation Technology,2014,10(2):85-89. (in Chinese)
杨蓉,刘玉坤. 建模与仿真逼真度理论与方法研究综述[J]. 系统仿真技术,2014,10(2):85-89.

[9] SIATERLIS C,GARCIA A P,GENGE B. On the Use of Emulab Testbeds for Scientifically Rigorous Experiments [J]. IEEE Communications Surveys & Tutorials,2013,15(2):929-942.

[10] WROCLAWSKI J,BENZEL T,BLYTHE J,et al. DETERLab and the DETER Project [M]// The GENI Book. Springer International Publishing,2016:35-62.

[11] ROZA Z C. Simulation Fidelity Theory and Practice [D]. Netherlands:TU Delft,2005.

[12] GARDENGHI L,GOLDWEBER M,DAVOLI R. View-os:A New Unifying Approach against the Global View Assumption [C]// International Conference on Computational Science(ICCS 2008). 2008:287-296.

[13] SHUJA J,GANI A,BILAL K,et al. A Survey of Mobile Device Virtualization:Taxonomy and State of the Art [J]. ACM Computing Surveys,2016,49(1):1.

[14] DETER T. Building Apparatus for Multi-resolution Networking Experiments Using Containers:ISI-TR-683[R]. 2011.