可重构安全承载网络构建与重构算法研究*

邢池强，胡宇翔，兰巨龙，王文钊
（国家数字交换系统工程技术研究中心，郑州 450002）

摘 要：现有互联网安全体系结构僵化且效率低下。基于“以可变的有限节点资源支持多样安全应用需求、以内置的安全结构提供多级安全保障”这一认识，避免单一追求高安全等级或高服务质量的简单模式，提供更高的灵活性和可扩展性，提出一种基于重构的安全业务—服务—构件模型，并在此基础上给出可重构网络安全体系的初步构想和具有多级安全保障的可重构安全承载网络结构，给出了可重构安全承载网络构建及重构算法。仿真结果验证了算法的有效性和性能。

关键词：可重构网络；安全组合；多级安全；构建与重构；安全构件
中图分类号：TP393；TP301.6 **文献标志码**：A **文章编号**：1001-3695(2014)04-1167-05
doi:10.3969/j.issn.1001-3695.2014.04.051

Research on reconfigurable security carrying network construction and reconfiguration algorithm

XING Chi-qiang, HU Yu-xiang, LAN Ju-long, WANG Wen-zhao
(*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002, *China*)

Abstract: Current Internet security architecture is fixed and exhibits low efficiency. Based on the thinking of "supporting diverse security applications with the variable limited node resources and providing multilevel security guarantee by inherent security architecture", avoiding limitations of traditional model aiming at pursuing high security quality of service and ensuring security by providing more flexibility and scalability, this paper first presented a network reconfiguration-oriented security business-services-components model, and gave a preliminary conception of reconfigurable network security architecture as well. Then this paper proposed a novel security structure which was named reconfigurable security carrying network (RSCN for short) to provide multilevel security guarantee. At last, it gave the construction algorithm and reconstruction algorithm of RSCN. The simulation results show that the algorithms are effective.

Key words: reconfigurable network; security composition; multi-level security; construction and reconfiguration; security components

0 引言

网络内置的安全结构是目前信息安全领域的研究热点，网络安全体系的多年研究和实践已经证明：网络安全并不是特定协议栈某层的一个单独功能，而是每一个参与全局通信过程的重要通信功能的有机组合[1]。然而，现有互联网安全体系结构僵化且效率低下，其基础网络层面结构简单、功能单一，与丰富多样的上下层功能之间存在巨大的反差，对泛在的信息服务、多样化和全方位的网络业务、确保质量的通信效果、安全可信的信息交互等的支持能力已经严重不足[2]。

近年来，国内外纷纷开展新型网络安全体系研究，以解决传统 IP 网络存在的种种安全弊端，均提出了其内置的安全结构：XIA 项目中，文献[3]提出一种提供路由控制、失败隔离和精确端到端通信信任信息的网络安全体系；文献[4]给出一种层次化自验证的地址结构以达到将可问责性(accountability)作为网络安全体系首要特性的目的。Internet 3.0 项目中，文献[5]提出未来应提供可编程的隔离网络，安全管理策略分层执行是另一个重要方面；文献[6]强调安全所面临的挑战是如何协调执行多种安全服务来获得牢固的安全保障并同时具有灵活的解决方案。FIND 计划中，文献[7]研究了唯一标志记录来源的数据包，同时保留适当的主机和用户隐私强度；文献[8]提出关系导向的网络将关系作为网络中的首要实体以提供更好的可用性、安全和信任，以加密的实体身份代替现有不安全的基于名字的身份；文献[9]针对无处不在的计算设备可能带来的隐私泄露风险问题进行了研究，通过向不必要的实体隐藏网络端点的身份信息，解决身份信息泄露的问题。FP7 计划中，文献[10]为了测量和表达可信任性的程度，致力于探讨涉及相关的度量标准、方法和工具。除此之外，文献[11]给出一种针对 Web 服务的安全策略，其安全性由物理位置分散的不同种类安全服务器联合提供，并给出了安全服务的组合方法。

上述安全体系依然存在诸如网络层功能单一、业务与网络过度分离、无法满足多样化安全需求等问题，这些思路在提供

收稿日期：2013-07-03；**修回日期**：2013-08-28 **基金项目**：国家“973”计划资助项目(2012CB315901,2013CB329104)；国家“863”计划资助项目(2011AA01A103,2011AA01A101,2013AA013505)；国家科技支撑计划资助项目(2011BAH19B01)

作者简介：邢池强(1989-)，男，河北邢台人，硕士研究生，主要研究方向为宽带信息网络、网络安全、新型网络体系(xingchiqiang@126.com)；胡宇翔(1982-)，男，河南周口人，讲师，博士，主要研究方向为新型网络体系、路由与交换技术；兰巨龙(1962-)，男，河北张北人，教授，博导，主要研究方向为新型网络体系、网络建模；王文钊(1989-)，男，河北邯郸人，硕士研究生，主要研究方向为虚拟网络.

灵活的安全服务和可扩展性等方面仍存在缺陷,因此需要在体系结构的核心内嵌新型的基础安全结构,并基于内嵌的可重构能力[12]将诸多有限的安全功能要素自然配合、联合起效、融为一体,从而在根本上突破制约瓶颈。可重构网络的核心特征是其内在结构的时变性,即由时变的结构驱动时变的服务能力,最终实现网络服务对应用要求和特征的动态匹配[13]。

针对多样可变的网络安全业务与有限确定的网络安全资源之间的矛盾,本文提出一种基于重构的安全"业务—服务—构件"模型。模型中网络安全业务与安全服务呈现松耦合关系,网络的安全服务被分解成一组细粒度的基本网络安全元素(安全构件),网络可根据安全业务提供和删除相应的网络安全资源,从而提高安全模型的灵活性和可扩展性。之后提出一种具有多级安全保障的可重构安全承载网络,它是一种以用户安全业务为驱动、将安全业务映射到物理网络资源所构建的新型网络服务结构,在保证安全的同时,提供了更高的灵活性和可扩展性。本文还提出一种可重构安全承载网络的构建及重构算法,仿真结果验证了算法的有效性和性能。

1 可重构网络的安全体系初探

1.1 可重构网络的安全模型

网络安全业务的特征和需求是多样和可变的,相对而言,网络所能提供的安全服务能力却是有限和确定的。为有效弥合这种差异性,更加充分合理地利用网络安全资源,可重构网络以可变的有限节点资源支持多样的安全应用需求,以内置的安全结构提供全方位的安全保障,基于内嵌的可重构能力将诸多有限的安全功能要素自然配合、联合起效、融为一体,从而提供多样化可变的安全服务。

分析网络安全业务特征需求与网络承载的安全服务之间的映射关系,首先建立可重构网络的安全"业务—服务—构件"模型,如图1所示。

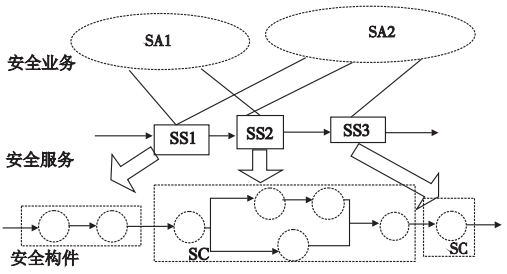


图1 安全"业务—服务—构建"安全体系模型

安全业务(security application,SA)指上层应用所提出的完整安全需求;将直接承载特定网络安全业务映射到一组安全服务(security service, SS)上;每一个安全服务需要一组提供基本安全要素和功能的实体单元予以支撑,每一基本实体单元即为一个安全构件(security component, SC)。构件[12]一词来源于可重构网络,是可重构网络中最小物理资源单位,构件的实现使可重构网络以搭积木的形式提供灵活可变服务。服务与构件之间、业务与服务之间有如下映射关系:

$$f_1(SC_1^j, SC_2^j, \cdots, SC_n^j) = SS_j, SC_n^j \in C_{SC} \quad (1)$$

$$f_2(SS_1^k, SS_2^k, \cdots, SS_m^k) = SA_k, SS_m^k \in C_{SS} \quad (2)$$

其中:C_{SC}、C_{SS}分别表示安全构件、安全服务的集合。

根据ISO7498的定义,安全服务主要包括机密性(confidentiality,Co)、完整性(integrity,In)、抗抵赖性(non-repudiation,Nr)、访问控制(access control, Ac)、鉴别(authentication and authorization, Aa)五种,即

$$C_{SS} = \{Co, In, Nr, Ac, Aa\} \quad (3)$$

为了提供多级安全保障以应对灵活多变的网络安全业务,各个安全服务必须具有多级安全,不同种类级别的安全服务由不同种类级别的安全构件有序组合而成。为此,以1~5表示安全服务等级为第一级、第二级、第三级、第四级、第五级,则有

$$SAR = \{r_{Co}, r_{In}, r_{Nr}, r_{Ac}, r_{Aa}\}, r \in [1,5] \quad (4)$$

其中:SAR为安全业务需求(security application requirement),由若干不同种类、级别的安全服务有序组合而成,形成了多样的安全保障等级。

1.2 可重构网络的安全架构

基于上述模型,给出基于网络重构的安全体系架构初步构想,如图2所示。在可重构网络安全体系中,首先由顶层应用提出特定等级的安全业务,网络基于依要求和依特征两种服务模型分别对满足安全需求的节点(可重构路由交换节点)安全构件库中的相应安全构件进行组合或者重构,实现满足要求的安全服务节点内在功能结构,进而为安全业务提供支持。这一安全体系是建立在面向服务提供机制基础上的安全服务按需动态重构的网络安全体系,能够实现对安全业务的量身定制。

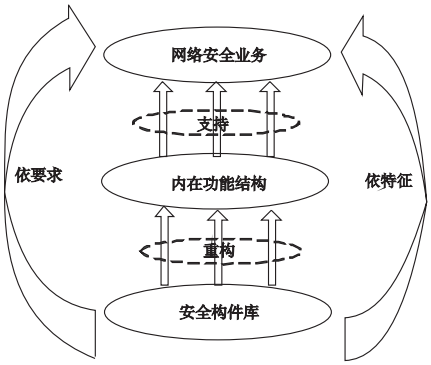


图2 基于网络重构的安全体系初步构想

由于上述不同种类级别的安全服务实际上是由网络中可重构节点提供的,定义节点的安全承载能力(security carrier ability, SCA)表示节点所能提供的安全服务种类级别,则有

$$SCA = \{a_{Co}, a_{In}, a_{Nr}, a_{Ac}, a_{Aa}\}, a \in \{1,2,3,4,5\} \quad (5)$$

其中:a代表各类安全服务的承载能力级别,同样,以1~5表示其承载能力级别。不同种类级别a_i组合构成许多但有限种类的节点安全承载能力。

综上所述,可重构网络的安全视图如图3所示,图中以不同的形状代表不同种类的安全服务,以不同的数字代表不同的等级,每一个节点的安全承载能力即为图示的一个标明各类安全服务及其等级的集合。

图3中,DS(domain supervisor)为域管理服务器,负责管理本域拓扑结构、统计节点安全资源及资源使用情况,并实现可重构安全承载网络构建及重构算法。

对于一个完整的可重构安全承载网络,往往需要多个节点联合起效,这就需要各节点的安全承载能力满足一定的安全业务。即

$$SCA \geqslant SAR, \text{if } a_i \geqslant r_i, a_i \in SCA, r_i \in SAR \quad (6)$$

其中:i({Co, In, Nr, Ac, Aa}。

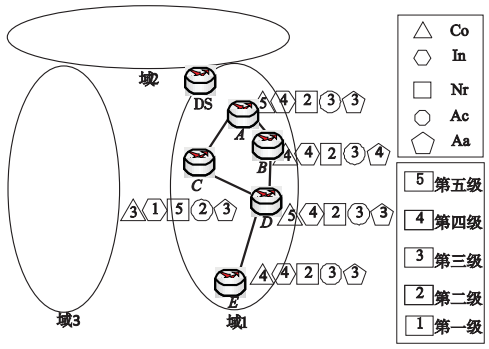


图3　网络安全承载能力视图

2　可重构安全承载网络

为了向用户提供安全、有效的服务,针对不同的应用场景和用户需求,将网络安全服务划分成多个等级并建立多级网络安全模型,然后基于多级安全强度构建面向不同安全等级需要的可重构安全承载网络。

作为可重构网络的内置安全结构——可重构安全承载网络是在上述可重构网络安全体系模型基础上建立在网络路由交换节点间的、对外提供一组按需定制安全服务的网络结构,即为上层应用提供一组按需定制安全服务及其运行环境的物理承载网络,并为网络内部各路由交换节点间传输的用户数据提供安全隧道传输服务。图 4 给出了可重构安全承载网络的总体结构。

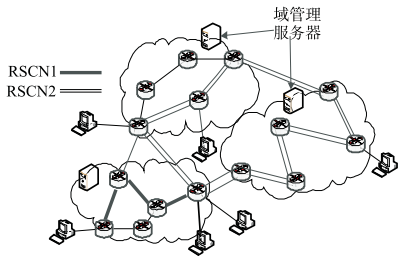


图4　可重构安全承载总体结构图

可重构安全承载网络的实现可分为网络级和节点级。网络级指在网络中选择安全承载能力可支持安全业务需求的多个节点之间构建,以组成一个满足一类特定等级安全业务的承载网络;节点级指被选中的节点按照图 1 所示有序灵活组配多种不同安全构件,组成不同种类级别的安全服务为多种多类安全业务提供服务。

2.1　构建算法

无向图 $G_P=(V_P, E_P, \mathrm{SCA}_P)$ 表示物理网络,其中 V_P 和 E_P 分别表示物理节点集和链路集,SCA_P 表示物理节点的安全承载能力等级。无向图 $G_S=(V_S, E_S, \mathrm{SAR}_S)$ 表示 RSCN 构建需求,其中 V_S 和 E_S 分别表示用户请求的 RSCN 节点集和链路集,SAR_S 表示 RSCN 的安全业务需求等级。RSCN 构建问题可以表示为一个满足 G_S 约定的 G_P 子集,用 G_P' 表示。

$$M: G_S \rightarrow G_{P'}, G_{P'} \subseteq G_P \tag{7}$$

其构建映射过程示意图如图 5 所示。图 5 中单、双线分别表示构建请求 1、2 的构建结果。RSCN 的节点可以直接映射到底层物理网络,而链路映射过程可表示为

$$e_s = P(v_s \rightarrow v_t), e_s \in E_S, (v_s, v_t) \in V_S \tag{8}$$

对于 V_P 中任意一个节点 v,具有两个参数 SCA_v 与 $c(v)$,前者表示节点的安全承载能力,后者表示节点所能够承载的 RSCN 个数。易知若 v 在路径 P 上,须有:

$$\mathrm{SCA}_v \geqslant \mathrm{SAR}, x(v,t) \leqslant c(v) \tag{9}$$

其中:$x(v, t)$ 为 t 时刻节点 v 已承载 RSCN 的个数。

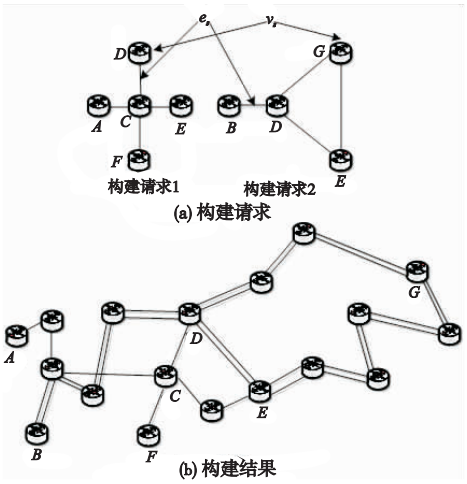


图5　RSCN构建请求及结果

进行映射时,首先剔除不能使用的节点,即不满足式(9),再在剩余拓扑上选择最优路径映射。所谓最优路径是指满足业务需求下,综合考虑节点的负载情况、节点安全资源使用情况和跳数等因素下的最优路径(一般承载网构建需考虑链路带宽,在此为简单起见,仅考虑节点安全资源)。为了量化上述因素,给出以下定义:

定义 1　节点负载强度 $S_N(t, v)$

$$S_N(t,v)=\frac{x(v,t)}{c(v)} \qquad S_N(t,v) \leqslant 1 \tag{10}$$

定义 2　单条 e_s 开销 $W(e_s)$

$$W(e_s)=\sum_{v \in e_s} S_N(t^-, v) \quad \forall v \in e_s \tag{11}$$

$W(e_s)$ 代表 e_s 对底层网络资源的消耗程度,$W(e_s)$ 包含了跳数因素,跳数越多,RSCN 经过的节点越多,开销也就越大。

构建的关键在于一方面要满足对安全业务的需求,另一方面需要高效地利用网络安全资源,以期在有限的物理网络上能够构建尽可能多地满足业务需求的可重构安全承载网络,提高网络安全资源的效率。

本文采用 Dijkstra 算法的路径发现方法进行 RSCN 拓扑管理,并提出一种基于 Dijkstra 算法的可重构安全承载网络构建算法(RSCN construction algorithm based on Dijkstra, RSCN-CAD)。假设可重构安全承载网络构建需求到达时刻为 t, 定义底层物理网络中相邻节点 $i \rightarrow j$ 链路的距离为

$$d_{ij}(t)=S_N(t^-, j) \tag{12}$$

RSCN-CAD 算法首先通过 Dijkstra 算法寻找使 $W(e_s)$ 最小的路径,然后依据上层的安全业务完成 RSCN 中链路集的映射。

基于 Dijkstra 算法的 RSCN 构建算法的详细描述如下:

算法 1　基于 Dijkstra 算法的可重构安全承载网络构建算法

a)剔除不满足 SAR 及负载强度为 1 的节点,得出可行底层物理拓扑 G。

b)for $\forall v_s \in V_s$,映射到 G 上。

c)for $\forall e_s \in E_s$,根据 Dijkstra 算法计算路径,得到所有 e_s 的所有中间节点集 $V(e_s)$。若有可行解,执行 d);否则执行

e)。

d)对所有 G 上节点 $v \in \{V_s, V(e_s)\}$ 进行可重构安全承载网络节点级构建,有序组合 SC_S 提供满足需求的 SS_S,转到 f)。

e)若构建次数小于最大构建循环数 K,则等待时间 Tw 后再次执行 c);否则,执行 f)。

f)结束算法。

上述算法在构建过程中综合考虑了节点负载及跳数等因素,从而优化构建过程,使网络负载均衡,同时提高网络资源的利用率。

2.2 重构算法

作为可重构网络最重要的特征,重构是全面提升对网络业务支持水平的一项结构性方法,其特点为网络资源的可扩展、可编程、可配置[14]。可重构安全承载网络也是可重构的,分为节点级重构和网络级重构。网络级重构,即对可重构安全承载网络的路径进行重构,即 E_S 的重构。文献[15]已就节点层面的资源重构过程和机制进行了讨论,本文仅就网络级重构展开讨论。

在可重构安全承载网络的动态构建过程中,由于新的需求抵达及旧的承载网络拆除,网络流量和资源状态会随之发生变化,可能出现负载不均衡的问题,使某些节点负载过重而影响新的承载网络构建成功率。为解决上述问题,动态条件下定期重构所有 e_s 可以有效提高资源利用的均衡程度,然而其代价较高。

针对上述分析,本文提出以下重构准则:

a)有限度的重构。标记部分负载较高的节点进行重构。

b)有选择的重构。对占用标记节点的所有 e_s 以概率 p 进行重构。

基于上述准则,提出一种 RSCN 局部选择性重构算法(RSCN local selective reconfiguration algorithm, RSCN-LSRA)。该算法给予关键 e_s 更高的重构优先级,"局部"表示只重构关键 e_s,"选择性"表示以概率 p 重构关键 e_s。该算法由两部分组成:标记过程和单个 e_s 重构过程。

a)标记。定期计算节点负载强度 S_N(标记周期记为 t_M),并依据以下公式确定关键节点。

$$V(t_M) = \{v \mid S_N(t_M, v) \geq k \times S_N(t_M, v)_{\max}, v \in V_S\} \quad (13)$$

其中:t_M 表示标记发生的时刻,$k \in [0,1]$ 是重构阈值。所有目前占用关键节点的 e_s 被标记为关键 e_s。

B)单个 e_s 重构。每条被标记的 e_s 以概率 p 进行重构。

图 6 给出了一个重构过程示例,重构结果如虚线部分所示。

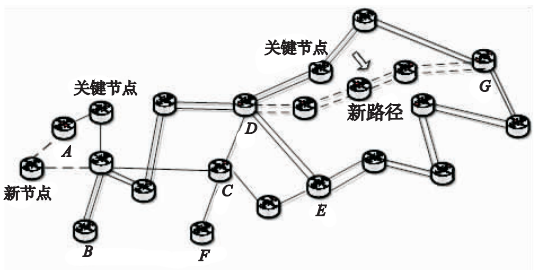


图6 重构过程示意图

综上所述,可给出如下可重构安全承载网络重构算法:

算法 2 可重构安全承载网络局部选择性重构算法(RSCN local selective reconfiguration algorithm, RSCN-LSRA)

a)重构周期 t_M 到达,确定物理网络中关键节点集 $V(t_M)$。

b)标记占用 $v \in V(t_M)$ 的所有 e_s 为关键 e_s。

c)for $\forall e_s$ 以概率 p 执行上述 Dijkstra 算法重新映射,若有除 e_s 之外的可行解,则替换;若无,则保留。

d)等待下一个重构周期 t_M 到达,回到 a)。

选择一个子集进行重构的 RSCN-LSRA 算法能够有效降低重构成本,且优化网络资源利用率。

3 实验结果及分析

3.1 仿真场景

仿真网络拓扑采用具有 14 个节点 21 条链路的 NSFNET 骨干网(图 7)。网络中每个节点均可提供五种安全服务,在此分别用 1 ~ 5 标志其等级,等级分布随机生成。构建请求达到过程服从泊松分布,100 时间单位到达个数均值为 5(单位:个);每个 RSCN 的生存时间服从均值为 1 000 的指数分布。RSCN 节点数为 2 ~ 4 个,节点随机选取,安全业务需求等级均匀分布,重构过程中 $p = 0.5$。每次仿真随机产生 2 000 个构建需求,仿真时间约为 4 万个时间单位,仿真采用 MATLAB 软件实现;仿真实验的硬件环境如下:处理器主频为 2.8 GHz,2 GB 内存,Windows XP 操作系统。

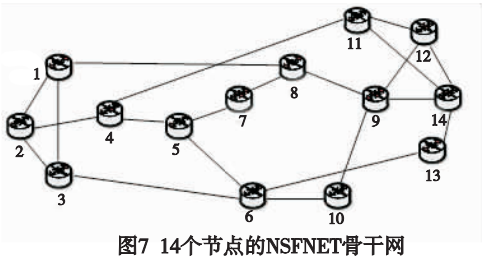
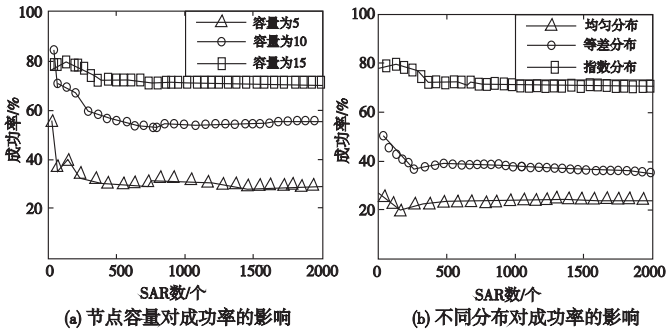


图7 14个节点的NSFNET骨干网

3.2 结果及分析

a)分析不同仿真参数对 RSCN 构建成功率的影响,图 8(a)给出了节点安全承载能力分布相同、节点容量(节点所能够承载的 RSCN 个数)不同时的构建成功率,节点容量分别为 5、10、15。图 8(b)给出了节点容量相同、节点安全承载能力分布不同时的构建成功率,分布情况分别为均匀分布、等差分布(1 ~ 5 等级的分布概率分别为 0.1、0.15、0.2、0.25、0.3)、指数比例分布(按 e^i 比例分布,$i \in [0,4]$)。



(a) 节点容量对成功率的影响 (b) 不同分布对成功率的影响

图8 不同参数下构建成功率

由图 8 可知,节点容量对构建成功率影响较大。节点容量为 5 时,构建成功率仅为 30% 左右,当容量为 15 时,成功率可增加到 70% 左右。同时,由于节点安全承载能力的分布情况直接影响了网络中节点能力的高低,因此也影响着构建成功率。均匀分布时,节点能力总体水平低,构建成功率约为

25%;等差分布时,构建成功率略有上升,约为 35%;指数分布时,节点总体能力提高,构建成功率稳定于 70%。本文后续仿真均在节点容量为 15、节点承载能力服从指数分布的条件下进行。

b)分析重构对 RSCN 成功率的影响,仿真结果如图 9 所示。

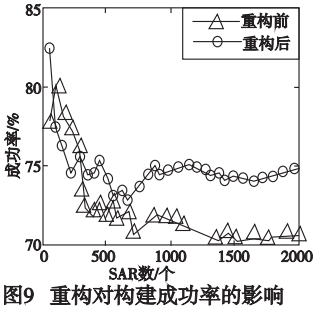


图9　重构对构建成功率的影响

由图 9 可知,与重构前相比,重构后的成功率增加了 5% 左右。分析其原因,这是由于网络级重构会使得网络中节点负载更趋均衡,减少满载节点的数目以提高节点总体可用性,使有限的节点资源承载更多的可重构安全承载网络。

c)分析重构对网络负载率的影响,结果如图 10 所示。图 10(a)为重构前节点的最大负载与平均负载分布图,图 10(b)为重构后节点的最大负载与平均负载分布图,图 10(c)为重构前后的平均负载差值(重构前的平均负载减去重构后的平均负载),图 10(d)为重构前后的最大负载差值(重构前的最大负载减去重构后的最大负载)。

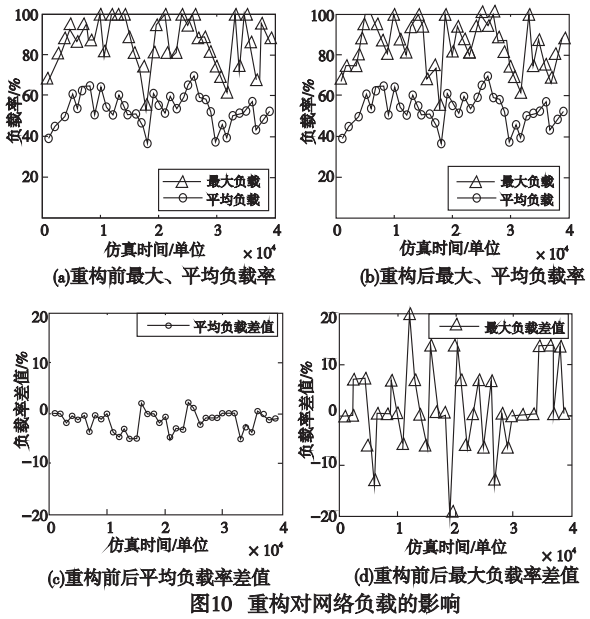


图10　重构对网络负载的影响

由图 10 可以看出,平均负载率差值负值较多,最大负载率差值正值较多,说明重构在增加网络节点平均负载率的情况下可降低网络节点最大负载率,从而使得网络负载均衡。

4　结束语

本文提出的基于重构的安全模型和提供多级安全服务保障的可重构安全承载网络结构,针对不同的应用场景和用户需求,将网络安全性划分成多个等级并建立多级网络安全模型,以网络安全资源充分利用和合理适配为原则进行优化,避免单一追求高安全等级或高服务质量的简单模式,从而为用户提供灵活适当的服务质量和安全保障。

同时,本文提出的基于重构的安全模型和提供多级安全服务保障的可重构安全承载网络均为新概念,现有研究仅为对其运行原理基本和初步的思考,仍需要在多方面进一步思考完善:a)可重构安全承载网络的组织管理及面对各种常见威胁时的韧性讨论;b)节点内部安全构件的重构,后续研究仍需要明确定义节点安全构件库中的元素组合机制以及服务与构件的对应关系;c)可重构安全承载网络构建及重构算法的优化改善,尤其是在大规模网络环境下如何实现分布式的高效计算和信息交互仍是本文下一步的工作。

参考文献:

[1] PAUL S, PAN Jian-li, JAIN R. Architectures for the future networks and the next generation internet: a survey [J]. Computer Communications, 2011, 34(1):2-42.

[2] ANAND A, DOGAR F, HAN Dong-su, *et al*. XIA:an architecture for an evolvable and trustworthy Internet[C]//Proc of the 10th ACM Workshop on Hot Topics in Networks. New York:ACM Press, 2011: 2.

[3] ZHANG Xin, HSIAO H C, HASKER G, *et al*. SCION:scalability, control, and isolation on next-generation networks[C]//Proc of IEEE Symposium on Security and Privacy (SP). [S. l.]: IEEE Press, 2011: 212-227.

[4] ANDERSEN D G, BALAKRISHNAN H, FEAMSTER N, *et al*. Accountable Internet protocol (AIP)[C]//Proc of ACM SIGCOMM Computer Communication Review. New York:ACM Press, 2008: 339-350.

[5] JIAN R. Internet 3.0: ten problems with current Internet architecture and solutions for the next generation[C]//Proc of Military Communications Conference. 2006: 1-9.

[6] PAUL S, JAIN R, PAN Jian-li, *et al*. Multi-tier diversified service architecture for Internet 3.0: the next generation Internet[D]. ST. Louis:Washington University, 2010.

[7] SNOEREN A C, KOHNO Y, SAVAGE S, *et al*. NeTS-FIND:enabling defense and deterrence through private attribution[D]. Seattle: Washington University, 2007.

[8] ALLMAN M, RABINOVICH M, WEAVER N. NeTS: FIND: collaborative research: relationship-oriented networking [D]. Seattle: Washington University, 2007.

[9] SESHAN S, WETHERALL D, KOHNO T. Collaborative research NeTS-FIND: protecting user privacy in a network with ubiquitous computing[D]. Seattle:Washington University, 2007.

[10] Workshop on measurability of trustworthiness of complex ICT systems and services[R]. Brussels:[s. n.], 2009.

[11] OPINCARU C A. Service oriented security architecture applied to spatial data infrastructures [D]. Munich: University of the Federal Armed Forces, 2008.

[12] 刘强,汪斌强,徐恪. 基于构件的层次化可重构网络构建及重构方法[J]. 计算机学报, 2010,33(9):1557-1568.

[13] 程东年, 汪斌强, 王保进, 等. 网络结构自调整的柔性内涵初探[J]. 通信学报,2012,33(8):214-222.

[14] 兰巨龙,程东年,王雨,等. 网络柔性重构的智能机理浅析[J]. 电信科学,2012,28(8):205-112.

[15] HU Yu-xiang, LAN Ju-long, WU Jiang-xing. Providing personalized converged services based on flexible network reconfiguration [J]. Information Sciences, 2011, 54(2):334-347.