一种软件定义网络的安全服务链动态组合机制

熊 钢* 胡宇翔 段 通 兰巨龙
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：网络安全功能与硬件设备的紧耦合关系，造成传统网络安全服务模式静态僵化，难 以满足未来业务发展的多样化安全需求。为此，基于软件定义网络环境，该文提出一种灵活可配的安全服务链动态组合机制。首先，介绍了该机制的总体结构，并建立了基于向量空间和整数规划的组合模型。其次，设计了启发式算法进行模型求解，并构建了该机制的实现原型。最后，实验结果表明所提组合算法在性能指标上优于对比算法，并且试验验证了该机制的优势。

关键词：软件定义网络；安全服务；元能力；功能组合
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2016)05-1234-08
DOI: 10.11999/JEIT150876

A Dynamic Composition Mechanism for the Security Service Chain Oriented Software Defined Networking

XIONG Gang HU Yuxiang DUAN Tong LAN Julong
(*National Digital Switching System Engineering & Technological R &D Center*, *Zhengzhou* 450002, *China*)

Abstract: The close relationship between the network security function and the hardware devices causes the static rigidity of the traditional security service mode, which is difficult to meet the various security requirement of future network business development. Based on the features of the Software Defined Networking (SDN), a dynamic composition mechanism is proposed for the Composable Security Service Chain (CSSC). First, the overall framework is introduced, and a mathematical model about the composition problem is established by the vector space and integer programming. Then, a heuristic algorithm is designed for solving the model, and the prototype is achieved in SDN environment. Finally, the results of the experiments show that the proposed algorithm outperforms the compared ones, and the advantage of the CSSC is validated by the simulation.

Key words: Software Defined Networking (SDN); Security service; Atomic ability; Function composition

1 引言

电子商务、数据中心、社交网络等多样化网络业务的迅猛发展，向传统安全服务模式提出了严峻挑战，表现为[1]：一方面现有安全功能(防火墙、IDS(Intrusion Detection System)等)的硬件化，导致其存在可扩展性不足、灵活性差、建设成本高等弊端；另一方面安全功能的静态部署难以满足业务需求的动态变化，造成网络资源浪费。为此，新型网络安全服务模式研究成为当前一个热点[2–4]。

当前，软件定义网络(Software Defined Networking, SDN)[5–7]和网络功能虚拟化技术(Network Functions Virtualisation, NFV)[8]的兴起为此提供了支撑。SDN将控制功能从传统的分布式网络设备中迁移到集中的控制平台，进而通过开放可编程的软件模式来实现网络的自动控制。同时，NFV通过虚拟化方式打破了网络功能与硬件设备的紧耦合关系，为上层网络功能创新提供了条件。两者结合不仅可增强网络安全服务的灵活性，而且有利于提升网络整体效能。

对此，文献[9]提出FRESCO安全架构，其以安全模块组合的方式生成安全服务，但仅给出了功能上的验证。文献[10]提出的SIMPLE方案利用SDN技术设计了针对数据层中网络功能中间件的管理机制，然而其仍缺乏对应用层的组合策略。文献[11]通过对SDN/NFV技术的分析，提出通过组合虚拟安全应用模块来构建安全服务链(Security Service

收稿日期：2015-07-21；改回日期：2015-12-18；网络出版：2016-02-26
*通信作者：熊钢 xg1226@126.com
基金项目：国家重点基础研究发展计划(2012CB315901, 2013CB329104)，国家自然科学基金(61309019, 61372121)，国家高技术研究发展计划(2013AA013505)
Foundation Items: The National Basic Research Program of China (2012CB315901, 2013CB329104), The National Natural Science Foundation of China (61309019, 61372121), The National High Technology Research and Development Program of China (2013AA013505)

Chain, SSC)的技术思想，但并未给出服务构建策略。文献[12]也仅在假设网络节点具有安全服务能力条件下，研究了节点间的路由问题。因此，在现有研究基础上，本文更加侧重于满足SDN网络对安全服务构建策略的迫切需求。

近来，文献[13]提出通过网络功能单元的组合实现节点对应用需求的自适应匹配；文献[14]设计了控制平面OpenNF用于网络功能的控制和管理。本文通过借鉴这些新的研究思路，并结合向量空间、整数规划等数学工具对SDN中的安全服务构建问题进行建模分析，并提出一种可组合安全服务链机制(Composable Security Service Chain, CSSC)。

2　基本原理

2.1 总体结构

ISO7498-2标准[15]提出开放式信息系统安全体系结构，指出每类安全服务均可由相应的安全机制组合提供，如图1所示。基于此，文献[16]提出了可重构安全服务模式，其将安全业务与网络可提供的安全服务能力之间概括为“安全业务-安全元服务-安全元能力”的分层映射结构，如图2所示。其中，安全元能力(Security Atomic Capability, SAC)定义为能提供基本安全要素和功能的实体单元，对应于传统安全模型中的“安全机制”。安全元服务(Security Atomic Service, SAS)定义为由安全元能力按照相应关系构成的满足特定安全属性的网络服务，对应于传统安全模型中的“安全服务”。安全业务(Security Application Requirements, SAR)则是指网络业务应用所提出的完整安全需求。

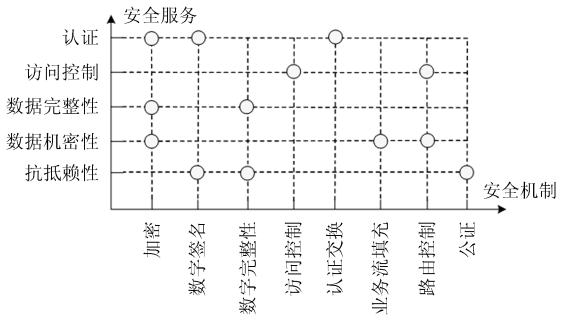


图 1 信息系统安全体系结构示意图

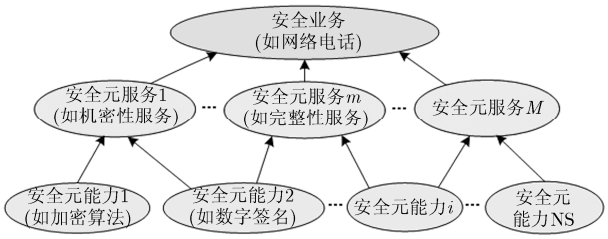


图 2 可重构安全服务模式示意图

基于上述安全服务构建思想，提出面向 SDN 的安全服务链组合机制总体结构图，如图 3 所示，该结构主要包括：控制层、应用层、数据层。控制层是网络的“大脑”，其作用有：存储和更新网络安全服务视图，包括网络拓扑、安全资源以及安全元能力配置等；分析顶层业务安全需求并结合网络状态形成安全服务链的构建决策。应用层主要包括各类安全元能力的软件虚拟化开发环境，依据控制层的决策结果对安全元能力进行组合，并生成相应的安全功能规则通过控制层进行下发。数据层是由标准化的硬件设备(如 OpenFlow 交换机)构成的网络数据报文处理和传输通道。其主要作用包括：接收控制层下发的安全功能规则，对数据报文执行具体的安全防护操作。

2.2 组合模型

可组合安全服务链可根据安全业务的不同请求，通过组合模型决策构建起相匹配的安全服务链。其中，组合模型的主要内容是指安全业务(SAR)向安全元能力(SAC)的映射关系。

2.2.1 安全业务表达　同一类安全元能力具有不同的实例，例如加密元能力可由 DES, AES, RSA 等不同的密码算法实例来实现。为此，需要对安全元能力进行统一描述。考虑其在物理意义上与向量空间中的基向量有相似性，可将具有某类安全功能的安全元能力等效为向量空间中某一维度上的基向量，设第 i 类安全功能的单位元能力 $\overrightarrow{\mathbf{Se}_i}$ 可以表达为向量空间中第 i 维度上的单位基向量，即

$$\overrightarrow{\mathbf{Se}_i}=\Big(0\ \cdots\ 0\ \underset{\text{第}i\text{位}}{1}\ 0\ \cdots\ 0\Big),\ i=1,2,\cdots,\mathrm{NS} \tag{1}$$

其中， NS 是安全元能力的种类数目。那么具备第 i 类安全功能的所有安全元能力(SAC_i)都可表达为相应单位元能力 $\overrightarrow{\mathbf{Se}_i}$ 与安全等级参数 SL_i 的组合，如式(2)所示。

$$\overrightarrow{\mathbf{SAC}_i}=\mathrm{SL}_i\overrightarrow{\mathbf{Se}_i} \tag{2}$$

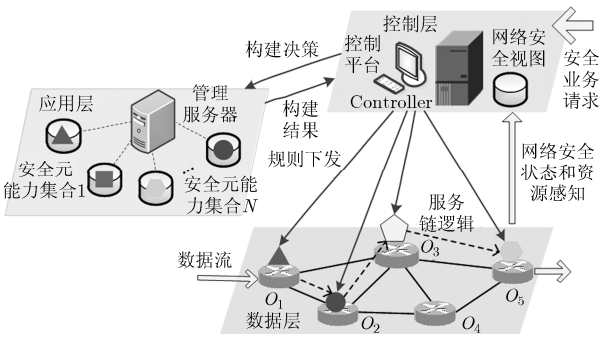


图 3 基于 SDN 的安全服务链组合机制总体结构图

其中，参数 $\mathrm{SL}_i \in \mathcal{N}\,(i{=}1,2,\cdots,\mathrm{NS})$，$\mathcal{N}$ 是自然数集合，取值大小可通过相关领域的研究得到。为简化分析，本文暂定将安全服务设定为 6 个等级，即“无”、“低”、“较低”、“中等”、“较高”、“高”等级，对应的 SL_i 取值为{0, 1, 2, 3, 4, 5}。依据式(2)，图 1 中所示的 8 类安全机制可采用向量描述，例如加密元能力为 $\overrightarrow{\mathbf{SAC}_1} = \mathrm{SL}_1(1,0,0,0,0,0,0,0)$，数字签名元能力 $\overrightarrow{\mathbf{SAC}_2}{=}\mathrm{SL}_2\,(0,1,0,0,0,0,0,0)$。

利用式(2)给出安全服务 $\overrightarrow{\mathbf{SAS}}$ 的向量表达如式(3)所示：

$$\overrightarrow{\mathbf{SAS}} = \sum_{i=1}^{\mathrm{NS}} \overrightarrow{\mathbf{SAC}_i} = \sum_{i=1}^{\mathrm{NS}} \mathrm{SL}_i \overrightarrow{\mathbf{Se}_i} \tag{3}$$

其中，$\overrightarrow{\mathbf{Se}_i}$ 确定了安全元能力的功能维度，参数 SL_i 决定了等级配置。进而，基于图 2 所示的安全业务分解和式(3)所示安全服务的向量表达，可得安全业务(SAR)的矩阵表达形式 $\mathbf{SAR}$ 为

$$\begin{aligned}\mathbf{SAR} &= \begin{bmatrix} \overrightarrow{\mathbf{SAS}_1} \\ \overrightarrow{\mathbf{SAS}_2} \\ \vdots \\ \overrightarrow{\mathbf{SAS}_M} \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{\mathrm{NS}} \mathrm{SL}_{1,i} \overrightarrow{\mathbf{Se}_i} \\ \sum_{i=1}^{\mathrm{NS}} \mathrm{SL}_{2,i} \overrightarrow{\mathbf{Se}_i} \\ \vdots \\ \sum_{i=1}^{\mathrm{NS}} \mathrm{SL}_{M,i} \overrightarrow{\mathbf{Se}_i} \end{bmatrix} \\ &= \begin{bmatrix} \mathrm{SL}_{1,1} & \mathrm{SL}_{1,2} & \cdots & \mathrm{SL}_{1,\mathrm{NS}} \\ \mathrm{SL}_{2,1} & \mathrm{SL}_{2,2} & \cdots & \mathrm{SL}_{2,\mathrm{NS}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{SL}_{M,1} & \mathrm{SL}_{M,2} & \cdots & \mathrm{SL}_{M,\mathrm{NS}} \end{bmatrix} \begin{bmatrix} \overrightarrow{\mathbf{Se}_1} \\ \overrightarrow{\mathbf{Se}_2} \\ \vdots \\ \overrightarrow{\mathbf{Se}_{\mathrm{NS}}} \end{bmatrix} \end{aligned} \tag{4}$$

式(4)中 $\mathbf{SAR}$ 是对安全业务请求的数学描述，其中 $\overrightarrow{\mathbf{SAS}_m}\,(m=1,2,\cdots,M)$ 是安全业务的安全元服务向量表达，而其中每一元服务又是由安全元能力 $\overrightarrow{\mathbf{Se}_i}\,(i=1,2,\cdots,\mathrm{NS})$ 构成。至此，基于向量空间建立了特定等级安全业务到安全元能力的定量映射形式。

2.2.2 组合策略描述 组合策略是综合考虑安全业务需求、安全元能力性能以及网络节点资源的情况，实现安全服务提供和网络资源利用效率的优化匹配。下面以图 4 所示网络单节点内的元能力组合为例进行分析。

图 4 中根据安全业务矩阵 $\mathbf{SAR}$，控制服务器选择安全元能力实例集合 $\mathbf{SE}$ 中每类安全元能力子集 SE_i 中的实例，并对其进行编排形成元能力组合实例链。设安全服务数 $M\,(m=1,2,\cdots,M)$；安全元能力种类数 $\mathrm{NS}\,(i=1,2,\cdots,\mathrm{NS})$；第 i 类安全元能力集合 SE_i 中的实例数为 $\mathrm{NZ}_i\,(n_i=1,2,\cdots,\mathrm{NZ}_i)$。设网络节点有 K 种资源约束，记为 $P^k\,(k=1,2,\cdots,K)$；设第 i 类安全元能力的第 n_i 个实例 se_{in_i} 的第 k 个指标取值记为 $p_{in_i}^k$，且安全等级参数为 sl_{in_i}，使用后产生的综合效用为 u_{in_i}；设服务 m 选择实例 se_{in_i} 的指示变量为 $x_{in_i}^m$，$x_{in_i}^m=1$ 表示选择，否则为 0。据此，以业务安全需求和网络节点的资源指标为约束，以安全服务链的总体网络效用最大化为目标，建立整数规划模型如式(5)。

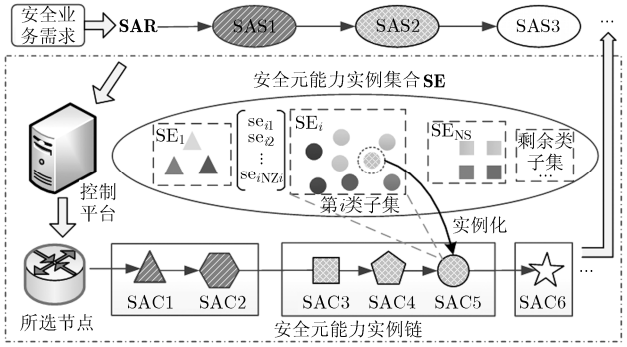


图 4 安全元能力组合模型示意图

$$\begin{aligned} \max\ & \sum_{m=1}^{M}\sum_{i=1}^{\mathrm{NS}}\sum_{n_i=1}^{\mathrm{NZ}_i} u_{in_i} x_{in_i}^m, \\ \text{s.t.}\ & \begin{cases} \sum\limits_{m=1}^{M}\sum\limits_{i=1}^{\mathrm{NS}}\sum\limits_{n_i=1}^{\mathrm{NZ}_i} p_{in_i}^{mk} x_{in_i}^m \le P^k,\ k=1,2,\cdots,\kappa \\ \sum\limits_{m=1}^{M}\sum\limits_{i=1}^{\mathrm{NS}}\sum\limits_{n_i=1}^{\mathrm{NZ}_i} p_{in_i}^{mk} x_{in_i}^m \ge P^k,\ k{=}\kappa{+}1,\kappa{+}2,\cdots,K \\ \mathrm{sl}_{in_i}^m x_{in_i}^m \ge \mathrm{SL}_{mi},\ m{=}1,2,\cdots,M, i{=}1,2,\cdots,\mathrm{NS} \\ \sum\limits_{n_i=1}^{\mathrm{NZ}_i} x_{in_i}^m = 1,\ x_{in_i}^m \in \{0,1\} \end{cases} \end{aligned} \tag{5}$$

式(5)中前 K 个约束指标 P^k 是网络节点的资源指标约束，元能力对前 κ 个指标(如计算能力、带宽、存储空间)的需求是越小越好，后 $K-\kappa$ 个指标(如时延)的需求是越大越好，节点资源指标可由网络管理平台通过资源感知获得。式(5)中第 $(K+1)\sim(K+M\times\mathrm{NS})$ 个约束表示安全等级约束。当问题规模较大时，式(5)所示 0-1 型整数规划模型为 NP-hard 问题，通常以启发式算法进行求解。

3 具体实现

3.1 组合模型求解

效用值 u_{SAC} 是安全元能力实例的综合性能反映，在此定义为安全元能力所有性能参数指标经效用函数转化后的函数值，第 i 类元能力的第 n_i 个实例 se_{in_i} 的效用值计算如式(6)：

$$\begin{aligned} u_{in_i} = & \sum_{k=1}^{\kappa} w_k T^{+}\left(r_{in_i}^k\right) + \sum_{k=\kappa+1}^{K} w_k T^{-}\left(r_{in_i}^k\right) \\ & + w_{K+1} T^{\mathrm{S}}\left(r_{in_i}^{K+1}\right) \end{aligned} \tag{6}$$

其中，w_k是缩放系数，用于调整各性能参数的影响因子，$\sum_{k=1}^{K+1} w_k = 1$,$w_k \geq 0$。T 为转换函数，为了与目标函数优化方向一致，前κ个参数定义关于 r 单增的函数T^+，后$K-\kappa$个参数定义关于r单减的函数T^-；对于安全性能参数，单独定义关于 r的增函数T^{S}。r是转换函数T的自变量，对安全元能力实例的性能参数进行归一化处理，得到取值在[0,1]之间的归一化参数$r_{in_i}^k$：

$$r_{in_i}^k = \frac{R_{in_i}^k}{\max\limits_{n_i \in \mathrm{SE}_i}\left(R_{in_i}^k\right)},\ r_{in_i}^k \in [0,1]\ , k = 1,2,\cdots,K+1 \quad (7)$$

其中，R表示性能参数 p 或安全功能参数 SL。参考效用函数理论，给出效用转换函数如式(9)。

$$T = \begin{cases} T^+ = \mathrm{e}^{-\left(1-r_{in_i}^k\right)/r_{in_i}^k}, \quad 0 < r_{in_i}^k \leq 1, \\ \qquad k = 1,2,\cdots,\kappa \\ T^- = \begin{cases} \mathrm{e}^{-r_{in_i}^k/\left(1-r_{in_i}^k\right)}, & 0 < r_{in_i}^k < 1 \\ 0, & r_{in_i}^k = 1 \end{cases}, \\ \qquad k = \kappa+1,\kappa+2,\cdots,K \\ T^{\mathrm{S}} = \sin\left(r_{in_i}^k \pi/2\right), \quad 0 < r_{in_i}^k \leq 1, \\ \qquad k = K+1 \end{cases} \quad (8)$$

为了简化算法搜索空间，提高求解计算效率，针对式(5)所示组合模型，本文设计一种“先选择后贪婪”的针对性启发式算法，具体过程如下：

(1)选择过程：根据安全业务的安全等级需求对安全元能力实例集合进行选择，得到满足需求的元能力子空间，从而缩小求解范围。首先，根据安全业务矩阵**SAR** 可得到第 m 个安全服务包含的NL_m类安全元能力为$\left\{\mathrm{SL}_{mi_j}\ \overrightarrow{\mathbf{SAC}_{i_j}}\ \middle|\ j = 1,2,\cdots,\mathrm{NL}_m\ , i_j \in [1,\mathrm{NS}]\right\}$，由此构造类别选择矩阵$\mathbf{CM}_m$和参数选择矩阵$\mathbf{PM}_m$，其形式为

$$\mathbf{CM}_m = \begin{bmatrix} \overrightarrow{\mathbf{cv}_1} \\ \overrightarrow{\mathbf{cv}_2} \\ \vdots \\ \overrightarrow{\mathbf{cv}_{\mathrm{NL}_m}} \end{bmatrix} = \begin{bmatrix} \mathrm{cv}_{1,1} & \mathrm{cv}_{1,2} & \cdots & \mathrm{cv}_{1,\mathrm{NS}} \\ \mathrm{cv}_{2,1} & \mathrm{cv}_{2,2} & \cdots & \mathrm{cv}_{2,\mathrm{NS}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{cv}_{\mathrm{NL}_m,1} & \mathrm{cv}_{\mathrm{NL}_m,2} & \cdots & \mathrm{cv}_{\mathrm{NL}_m,\mathrm{NS}} \end{bmatrix}$$

$$\mathbf{PM}_m = \begin{bmatrix} \overrightarrow{\mathbf{pv}_1} \\ \overrightarrow{\mathbf{pv}_2} \\ \vdots \\ \overrightarrow{\mathbf{pv}_{\mathrm{NL}_m}} \end{bmatrix} = \begin{bmatrix} \mathrm{pv}_{1,1} & \mathrm{pv}_{1,2} & \cdots & \mathrm{pv}_{1,\mathrm{NZ}_{i_1}} \\ \mathrm{pv}_{2,1} & \mathrm{pv}_{2,2} & \cdots & \mathrm{pv}_{2,\mathrm{NZ}_{i_2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{pv}_{\mathrm{NL}_m,1} & \mathrm{pv}_{\mathrm{NL}_m,2} & \cdots & \mathrm{pv}_{\mathrm{NL}_m,\mathrm{NZ}_{i_{\mathrm{NL}_m}}} \end{bmatrix}$$

其中，选择矩阵中的选择向量$\overrightarrow{\mathbf{cv}_j}$与参数矩阵中的参数向量$\overrightarrow{\mathbf{pv}_j}$生成方式为

$$\left.\begin{aligned} \overrightarrow{\mathbf{cv}_j} &= \begin{pmatrix} \mathrm{cv}_{j1} & \mathrm{cv}_{j2} & \cdots & \mathrm{cv}_{j\mathrm{NS}} \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}}_{\text{第}i_j\text{位}}{}_{1\times\mathrm{NS}}, \\ &\qquad \mathrm{SL}_{mi_j} > 0 \\ \overrightarrow{\mathbf{pv}_j} &= \begin{pmatrix} \mathrm{pv}_{j1} & \mathrm{pv}_{j2} & \cdots & \mathrm{pv}_{j\mathrm{NZ}_{i_j}} \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{SL}_{mi_j} & \cdots & \mathrm{SL}_{mi_j} & \cdots & \mathrm{SL}_{mi_j} \end{pmatrix}_{1\times\mathrm{NZ}_{i_j}}, \\ &\qquad \mathrm{SL}_{mi_j} > 0 \\ &\qquad i_j \in [1,\mathrm{NS}]\ \ j = 1,2,\cdots,\mathrm{NL}_m \end{aligned}\right\} \quad (9)$$

设安全元能力实例集合的安全等级参数矩阵为$\mathbf{SLM}_{\mathrm{SE}}$，因此通过类别选择矩阵$\mathbf{CM}_m$和参数选择矩阵$\mathbf{PM}_m$的选择操作，可得满足第 m 个安全服务需求的等级矩阵$\mathbf{SL}_m$，该过程矩阵运算如式(10)：

$$\begin{aligned} \mathbf{SL}_m &= \left(\mathbf{CM}_m \times \mathbf{SLM}_{\mathrm{SE}}\right) - \mathbf{PM}_m \\ &= \begin{bmatrix} \mathrm{cv}_{1,1} & \mathrm{cv}_{1,2} & \cdots & \mathrm{cv}_{1,\mathrm{NS}} \\ \mathrm{cv}_{2,1} & \mathrm{cv}_{2,2} & \cdots & \mathrm{cv}_{2,\mathrm{NS}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{cv}_{\mathrm{NL}_m,1} & \mathrm{cv}_{\mathrm{NL}_m,2} & \cdots & \mathrm{cv}_{\mathrm{NL}_m,\mathrm{NS}} \end{bmatrix} \times \begin{bmatrix} \mathrm{sl}_{1,1}^{\mathrm{se}} & \mathrm{sl}_{1,2}^{\mathrm{se}} & \cdots & \mathrm{sl}_{1,\mathrm{NZ}_1}^{\mathrm{se}} \\ \mathrm{sl}_{2,1}^{\mathrm{se}} & \mathrm{sl}_{2,2}^{\mathrm{se}} & \cdots & \mathrm{sl}_{2,\mathrm{NZ}_2}^{\mathrm{se}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{sl}_{\mathrm{NS},1}^{\mathrm{se}} & \mathrm{sl}_{\mathrm{NS},2}^{\mathrm{se}} & \cdots & \mathrm{sl}_{\mathrm{NS},\mathrm{NZ}_{\mathrm{NS}}}^{\mathrm{se}} \end{bmatrix} - \begin{bmatrix} \mathrm{pv}_{1,1} & \mathrm{pv}_{1,2} & \cdots & \mathrm{pv}_{1,\mathrm{NZ}_{i_1}} \\ \mathrm{pv}_{2,1} & \mathrm{pv}_{2,2} & \cdots & \mathrm{pv}_{2,\mathrm{NZ}_{i_2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{pv}_{\mathrm{NL}_m,1} & \mathrm{pv}_{\mathrm{NL}_m,2} & \cdots & \mathrm{pv}_{\mathrm{NL}_m,\mathrm{NZ}_{i_{\mathrm{NL}_m}}} \end{bmatrix} \end{aligned} \quad (10)$$

其中，矩阵乘法“×”表示类别选择过程，矩阵减法“−”表示参数选择过程。为了运算处理需要，可将每类安全元能力的实例数目设为相等，即$\mathrm{NZ}_1 = \mathrm{NZ}_2 = \cdots = \mathrm{NZ}_{\mathrm{NS}} = \mathrm{NZ}$。矩阵$\mathbf{SL}_m$中取值大于等于 0 的元素对应的实例构成满足第 m 个安全服务需求的解空间搜索子集，如式(11)：

$$\Omega_m^{\mathrm{sel}} = \left\{ \mathrm{se}_{i_j n_{i_j}} \left| \begin{matrix} \mathrm{sl}_{i_j n_{i_j}}^m \mapsto \mathrm{se}_{i_j n_{i_j}}, \mathrm{sl}_{i_j n_{i_j}}^m \in \mathbf{SL}_m \ \text{and}\ \ \mathrm{sl}_{i_j n_{i_j}}^m \geq 0, \mathrm{se} \in \mathbf{SE} \\ 1 \leq j \leq \mathrm{NL}_m, \quad i_j \in [1,\mathrm{NS}], \quad n_{i_j} \in [1,\mathrm{NZ}] \end{matrix} \right. \right\}, \quad m = 1,2,\cdots,M \quad (11)$$

其中，符号“$\mapsto$”表示对应关系。对安全业务矩阵**SAR** 中的每一个安全服务的等级要求对实例全集**SE** 进行选择可以得到经安全等级选择后的求解搜索子空间集合$\Omega_{\mathbf{SAR}}^{\mathrm{sel}} = \left\{\Omega_m^{\mathrm{sel}}\ \middle|\ m = 1,2,\cdots,M\right\}$。

(2)贪梦搜索过程：在所得解搜索空间$\Omega_{\mathbf{SAR}}^{\mathrm{sel}}$的基础上，采用使目标函数最大化的贪心策略对各个解

空间进行搜索，从而得到满足安全业务请求的各个安全元能力实例。具体的策略流程是：

步骤 1 对 SAR 中的安全服务，采用式(6)依次计算每一搜索空间 $\Omega_{\mathbf{SAR}}^{\mathrm{sel}}$ ($m=1,2,\cdots,M$)中各元能力实例的效能值；

步骤 2 利用式(12)搜索每一安全服务中每一类安全元能力中效能值最大的实例。

$$\Omega_m^{\mathrm{gre}}=\left\{\widehat{\mathrm{se}}_{i_j}^m\left|\widehat{\mathrm{se}}_{i_j}^m=\arg\max_{n_{i_j}}\left(u_{\mathrm{se}_{i_j,n_{i_j}}}\left|\mathrm{se}_{i_j,n_{i_j}}\in\Omega_m^{\mathrm{sel}}\right.\right),\right.\right.$$
$$\left.\left.j=1,2,\cdots,\mathrm{NL}_m\right\},\quad m=1,2,\cdots,M \tag{12}$$

步骤 3 得到元能力实例集合 $\Omega_{\mathbf{SAR}}=\{\Omega_1^{\mathrm{gre}},\Omega_2^{\mathrm{gre}},\cdots,\Omega_M^{\mathrm{gre}}\}$，并将该集合中各元能力的资源指标值带入式(5)中前 K 个性能指标约束项，如果能够满足网络资源约束，则 $\Omega_{\mathbf{SAR}}$ 是式(5)模型的解，转到步骤 5 输出求解成功，否则转到步骤 4；

步骤 4 判断是否有某类元能力实例全部遍历，若是，转到步骤 5 输出请求失败；否则以比例 λ 随机选择 $\Omega_{\mathbf{SAR}}$ 中的元能力实例，以 $\Omega_{\mathbf{SAR}}^{\mathrm{sel}}$ 中同类元能力的效能值次优实例对其进行替换得到 $\Omega_{\mathbf{SAR}}'$，再跳转至步骤 3；

步骤 5 迭代搜索结束，输出结果(成功或失败)。

3.2 机制原型构建

为支持安全服务链的组合构建，在 SDN 的应用层中建立安全元能力编排子层，如图 5 所示，该编排层主要包括了安全元能力描述模块、安全业务表达模块、安全元能力组合模块。针对具体的安全业务请求，各模块相互作用生成满足安全业务需求的服务链功能规则，并借助 SDN 控制器以 OpenFlow 流表项的形式下发到底层交换节点。例如将图 5 所示 SDN/OpenFlow 网络结构应用于数据中心，根据某数据业务需求，编排层制定了在接入交换机 OS3 中部署高等级(High)实例 Firewall, Confidentiality, IDS 的服务策略：<{OS3},{Firewall/High, Confidentiality/High, IDS/High}>。当该策略的规则下发到交换机的流表项执行后，相应规则可引导数据流通过交换机内的安全功能逻辑(如 Firewall)或外部运行的安全功能逻辑(如 Confidentiality)，进而提供安全保护。

4 实验结果与分析

4.1 算法性能评估

(1)实验设置：通过 Matlab 软件评估本文所提的选择贪婪组合算法(记为 M0-Proposed)。所对比算法是：分支定界法(记为 M1-Branch)，这是一种典型的全局搜索算法[17]，具有较好的全局求解能力；

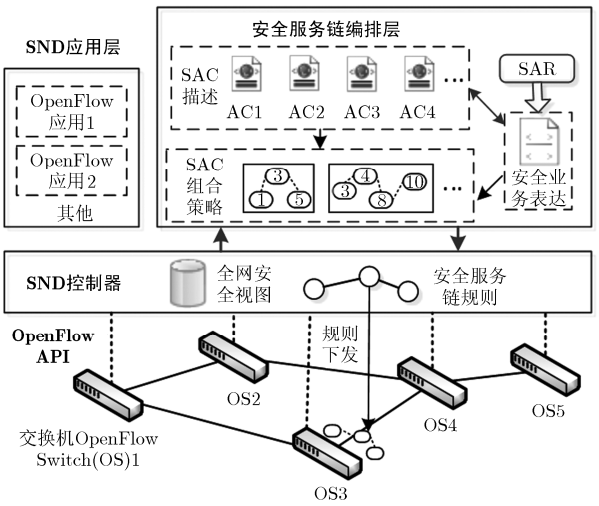


图 5 基于 SDN 结构的安全服务链实现范例

基于松弛求解的贪婪启发式搜索算法(记为 M2-Greedy)[13]，一种常用的启发式搜索算法，具有较强的时间效率。实验参数设置：元能力种类 NS=50，记为 $\mathrm{SE}_1\sim\mathrm{SE}_{50}$；每类元能力实例数为 NZ=20；每一实例的安全等级参数 $\mathrm{sl}\in\{1,2,3,4,5\}$取值满足均匀分布，性能指标 K=4(分别为计算、存储、带宽、时延)，取值满足高斯分布；网络节点上各指标约束量在一定范围内随机取值；迭代参数 $\lambda=0.2$ 。实验中，通过安全服务数(M)和各服务中元能力数目(NL)的不同取值策略，对各指标进行统计分析。

(2)实验结果及分析：

(a)负载均衡度：是指各类元能力实例在一定数量的业务请求内被使用的次数，其能够反映算法搜索的均衡程度，取值越小越好。实验中，通过统计每一类元能力实例的最大使用次数和平均使用次数进行衡量。设 M=3, NL=3 且在 $\mathrm{SE}_1\sim\mathrm{SE}_{50}$ 中随机选取。随机生成 10000 次业务请求，重复统计 10 次求平均值，得到如表 1 和图 6 所示的实验结果。表 1 给出 3 种算法中，50 类安全元能力实例使用的平均负载和最大负载的均值，其中 M1 在平均负载更大的情况下，最大负载更小，表明该算法使得各实例负载更为均衡，反之 M2 算法的实例负载均衡度较差，M0 算法居中。分析原因是，M1 的全局搜索策略提高了业务请求成功的次数使得平均负载增大，同时各实例得到均衡使用降低了最大负载取值。图 6 显示了 10 种安全元能力的最大负载和平均负载，分析结论与表 1 结果相一致。

表 1 各类安全元能力实例负载统计

算法	平均负载的均值	最大负载的均值
M0-Proposed	83	476
M1-Branch	87	382
M2-Greedy	79	520

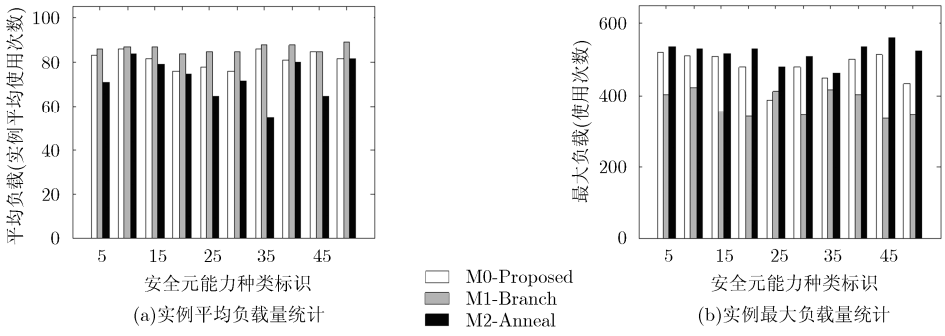


图 6 安全元能力实例负载均衡度统计结果

(b)时间复杂度：是指在一次业务请求中，从接收请求到完成安全服务链构建的时间间隔，反映了算法时间代价，取值越小越好；实验中，设 $M \in \{2,3,4\}$，$\mathrm{NL} \in \{3,4,5\}$。对每一$(M,\mathrm{NL})$的组合进行 10000 次请求，统计 10 次重复实验的均值结果如图 7 所示。图中数据表明 M1 算法的时间复杂度约为 M0 和 M2 两种启发式方法的 4~6 倍，并且随着安全服务链长度的增加，两者间的差距越大。M0 与 M2 的时间复杂度相近，其中 M2 算法易止于局部最优或者搜索失败，因此时间消耗更少。

(c)请求成功率：是指安全业务请求成功的平均概率，其反映了算法在解空间中的搜索性能，取值越大越好。与时间复杂度的实验设置相同，统计各算法成功满足业务请求的次数并转化为百分比，如图 8 所示。图中 M1 算法平均成功率约 97%，M0 算法成功率约 94%，M2 算法成功率约 84%；分析原因是：M1 算法采用全局搜索求解能力最好，M2 算法易受参数影响陷入局部搜索，本文 M0 算法是针对性启发式搜索，因此尽可能地保证了业务请求成功率。

综上所述，相比于 M1 算法和 M2 算法，本文所提 M0 算法根据安全元能力组合模型的具体情况而设计，因此在综合性能上具有更大优势，适用于在网络运行环境中构建安全服务链的需求。

4.2 试验验证

为了验证安全服务链机制的性能，下面以图 9 所示场景展开试验。其中美国科学基金骨干网络拓扑有 14 个节点和 21 条链路(链路上的数字代表物理距离)；可重构网络试验平台[1]是我们利用 NetFPGA-10G[18]器件搭建的具有 5 个节点的 10G 线速转发试验网。

(1)数据传输性能对比：数据传输性能通过网络传输时延进行描述。在不考虑拥塞情况下，传输时延由节点处理时延和链路传输时延构成，其中节点处理时延是节点上所有安全元能力的处理时延之和。在图 9(a)拓扑中，以节点 14 为数据流量出口，其它 13 个节点作为流量入口，并且在连接度最大的节点 6 和节点 9 上部署安全服务链。通常安全元能力等级越高，处理越复杂，其时延越大，实验中根据各实例安全等级的不同，设定其时延取值满足不同均值的正态分布。最后，基于文献[19]中的参数模拟产生真实数据流量，每隔单位长度(/s)随机为数据流生成相应的安全等级。

在传统网络环境和 SDN 中安全服务链环境下，统计结果如图 10 所示。图 10(a)所示为服务链长度固定为 5 的情况下，传统网络平均传输时延保持约为 35 ms，而 SDN 安全服务链机制的平均传输时延降低至 25 ms 上下波动。图 10(b)所示为不同服务链

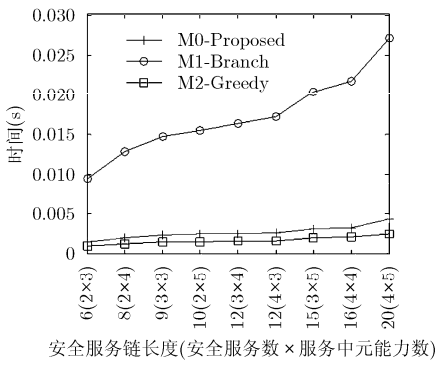


图 7 时间复杂度对比

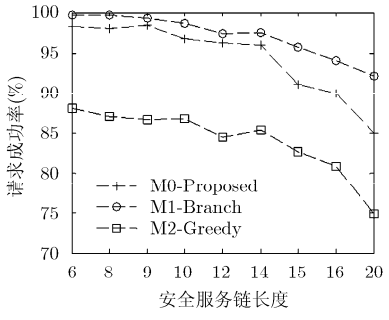
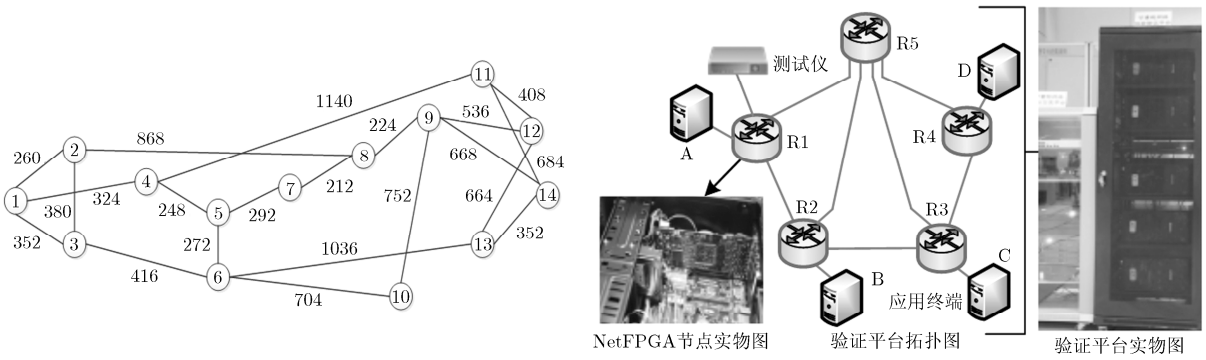


图 8 请求成功率对比



(a)美国科学基金骨干网络拓扑结构 (b)可重构网络试验验证平台

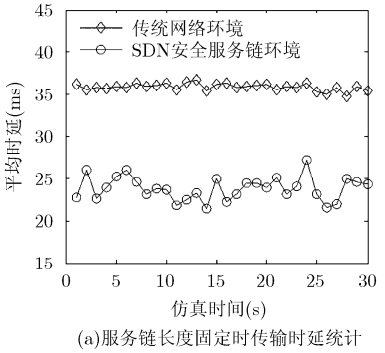
图 9 试验验证场景

长度下数据流的平均传输时延，其与服务链长度呈正相关，并且相比传统网络，SDN 安全服务链使得传输时延平均降低 30%左右。分析原因是：传统网络安全服务的静态部署模式使得各元能力实例需要配置最高等级，以满足不同需求。而 SDN 安全服务链机制则根据流量的安全等级需求动态配置各安全元能力等级，从而有效降低了处理时延。当然，该机制也引入了新的重构操作时间开销(包括请求处理、组合计算等)，据统计在服务链长度为 5 时一次重构开销约为 60 ms，远远小于以 s 或 min 为单位的重构请求时间间隔，因此以较小时间开销的重构操作来降低传输时延是有效的。

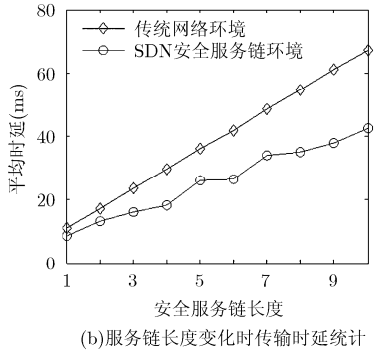
(2)资源利用效率对比：基于可重构网络试验平台，我们通过 openflow1.3 协议以多级流表的方式实现了节点内的功能规则组合，其中包括安全功能模块 Firewall 和 IDS[9]。各模块的流表规则通过 NOX 控制器进行部署，仅需要约 30 ms。试验中部署策略<{Firewall→IDS}>为图 9(b)中终端 A 到 D 的数据流提供安全防护，传统网络中数据流采用最短路径方式，即 R1→R5→R4，则在 R5 部署策略。而在 SDN 环境中，安全服务链机制根据网络状态灵活地在 R5 和 R2 节点上部署策略，分别得到路径 R1→R5→R4 和 R1→R2→R3→R4。试验中从 A 向 D 发送 10000 条仿真数据流[19]，图 11 统计结果显示了不同场景下各节点的负载情况(经过节点的流数目)。图 11 表明传统网络中节点 R2, R3 一直处于空载状态，导致其资源浪费，而所有流量经过节点 R5 处理导致其过载。而 SDN 安全服务链机制使得 R2, R3, R5 节点资源都得以利用，提高了网络资源利用效率，使得各节点负载更均衡。

5 结束语

针对传统网络安全服务模式难以适应未来业务安全需求发展的弊端，本文基于当前正蓬勃兴起的软件定义网络环境，提出了一种新的安全服务链动态组合机制。该机制通过具体组合算法对网络安全元能力进行组合，可灵活地满足安全业务的多样化需求。目前，网络安全功能组合的相关研究正不断兴起，下一步将继续完善本文研究，把安全服务链机制向多节点协同组合扩展，并深入开展服务链试验验证。



(a)服务链长度固定时传输时延统计



(b)服务链长度变化时传输时延统计

图 10 网络平均传输时延对比

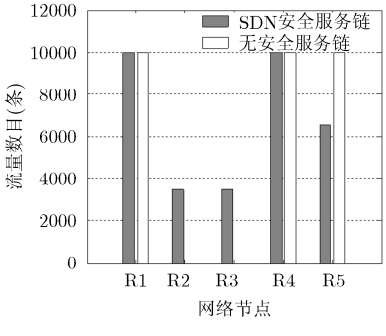


图 11 网络节点负载均衡度对比

参 考 文 献

[1] 兰巨龙, 程东年, 胡宇翔. 可重构信息通信基础网络体系研究[J]. 通信学报, 2014, 35(1): 64–76. doi: 10.3969/j.issn. 1000-436x.2014.01.015.
LAN J L, CHENG D N, and HU Y X. Research on reconfigurable information communication basal network architecture[J]. *Journal on Communications*, 2014, 35(1): 64–76. doi: 10.3969/j.issn.1000–436x.2014.01.015.

[2] PAUL S, PAN J L, and JAIN R. Architectures for the future networks and next generation internet: a survey[J]. *Computer Communications*, 2011, 34(1): 2–42. doi: 10.1016/j.comcom. 2010.08.001.

[3] 黄韬, 刘江, 霍如, 等. 未来网络体系架构研究综述[J]. 通信学报, 2014, 35(8): 184–197. doi: 10.3969/j.issn.1000-436x. 2014.08.023.
HUANG T, LIU J, HUO R, *et al*. Survey of research on future network architectures[J]. *Journal on Communications*, 2014, 35(8): 184–197. doi: 10.3969/j.issn.1000-436x. 2014.08.023.

[4] 张宏科, 罗洪斌. 智慧协同网络体系基础研究[J]. 电子学报, 2013, 41(7): 1249–1255. doi: 10.3969/j.issn.0372-2112. 2013.07.001.
ZHANG H K and LUO H B. Fundamental research on theories of smart and cooperative network[J]. *Acta Electronica Sinica*, 2013, 41(7): 1249–1255. doi: 10.3969/j.issn. 0372-2112. 2013.07.001.

[5] MCKEOWN N, ANDERSON T, BALAKRISHAN H, *et al*. OpenFlow: Enabling innovation in campus networks[J]. *ACM SIGCOMM Computer Communication Review*, 2008, 38(2): 69−74. doi: 10.1145/1355734.1355746.

[6] 左青云, 陈鸣, 赵广松, 等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报, 2013, 24(5): 1078–1097. doi: 10.3724/SP.J. 1001.2013.04390.
ZUO Q Y, CHEN M, ZHAO G S, *et al*. Research on OpenFlow-based SDN technologies[J]. *Journal of Software*, 2013, 24(5): 1078–1097. doi: 10.3724/SP.J. 1001.2013.04390.

[7] 周烨, 杨旭, 李勇, 等. 基于分类的软件定义网络流表更新一致性方案[J]. 电子与信息学报, 2013, 35(7): 1746–1752. doi: 10.3724/SP.J.1146.2012.01431.
ZHOU Y, YANG X, LI Y, *et al*. Classification based consistent flow update scheme in software defined network[J]. *Journal of Electronics & Information Technology*, 2013, 35(7): 1746–1752. doi: 10.3724/SP.J.1146.2012.01431.

[8] CHIOSI M, CLARKE D, WILLIS P, *et al*. Network functions virtualization-introductory white paper[R]. SDN and OpenFlow World Congress, Germany, 2012.

[9] SHIN S, PORRAS P, YEGNESWARAN V, *et al*. FRESCO: modular composable security services for software-defined networks[C]. Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2013: 1–16.

[10] QAZI Z, TU C C, and CHIANG L. SIMPLE-fying middlebox policy enforcement using SDN[C]. Proceedings of the ACM SIGCOMM'13, Hong Kong, China, 2013: 27–38.

[11] LEE W, CHOI Y H, and KIM N. Study on virtual service chain for secure software defined networking[J]. *Advanced Science and Technology Letters*, 2013, 29(13): 177–180.

[12] GUSHCHIN A, WALID A, and TANG A. Scalable routing in SDN-enabled networks with consolidated middleboxes[C]. Proceedings of the HotMiddlebox'15, London, United Kingdom, 2015: 55–60.

[13] CHENG G Z, CHEN H C, CHEN S Q, *et al*. How to make network nodes adaptive?[J]. *IEEE Communications Letters*, 2014, 18(3): 515–518. doi: 10.1109/LCOMM.2014.011714. 132622.

[14] AARON G J, RAAJAY V, CHAITHAN P, *et al*. OpenNF: enabling innovation in network function control[C]. Proceedings of the ACM SIGCOMM'14, Chicago, IL, USA, 2014: 163–174.

[15] ISO7498-2. Information processing systems-open systems interconnection basic reference model-part 2: security architecture[S]. British Standard, 1989.

[16] 陈杰, 刘建伟, 王蒙蒙, 等. 基于安全基片的可重构网络安全管控机制[J]. 电信科学, 2014, 30(7): 19–25. doi: 10.3969/ j.issn.1000–0801.2014.07.004.
CHEN J, LIU J W, WANG M M, *et al*. Security substrate based security management and control mechanism of reconfigurable network[J]. *Telecommunications Science*, 2014, 30(7): 19–25. doi: 10.3969/ j.issn.1000-0801.2014.07.004.

[17] MOORE R. Global optimization to prescribed accuracy[J]. *Computers & Mathematics with Applications*, 1991, 21(6/7): 25–39. doi: 10.1016/0898-1221(91)90158-Z.

[18] Gibb G. NetFPGA-10G project [OL]. https://github.com/ NetFPGA/NetFPGA-public/wiki, 2014.

[19] GEBERT S, PRIES R, SCHLOSSER D, *et al*. Internet access traffic measurement and analysis[J]. *LNCS*, 2012, 7189: 29–42. doi: 10.1007/978-3-642-28534-9_3.

熊　钢：男，1986 年生，博士生，研究方向为新型网络体系结构、网络安全.

胡宇翔：男，1982 年生，博士，主要研究方向为新型网络体系结构、网络安全.

段　通：男，1990 年生，硕士生，研究方向为新型网络体系结构.

兰巨龙：男，1962 年生，教授，博士生导师，主要研究方向为网络体系结构、信息安全.