

# 面向安全虚拟网络功能的可信评估方法

刘浩<sup>1,3</sup>, 王翀<sup>3</sup>, 田志宏<sup>4</sup>, 吴中海<sup>1,2</sup>

<sup>1</sup> 北京大学软件与微电子学院 北京 中国 100871

<sup>2</sup> 北京大学软件工程国家工程研究中心 北京 中国 100871

<sup>3</sup> 奇安信科技集团股份有限公司 北京 中国 100044

<sup>4</sup> 广州大学网络空间安全学院 广州 中国 510623

**摘要** 软件定义安全中,需要组合并实例化一个或多个安全虚拟网络功能构成安全服务功能链,实现对目标业务的安全加固和保护。传统的安全服务功能链组链过程中,安全虚拟网络功能的选取一般是基于专家经验完成的,缺乏统一的选择标准。为此,本文针对安全虚拟网络功能的选择问题,以可信评估思想为指导,提出一种面向安全虚拟网络功能的可信评估方法。首先,分析了现有相关研究工作,在此基础上定义了安全虚拟网络功能评价指标;其次,基于动态信任评估模型中的多属性决策方法提出安全虚拟网络功能可信评估模型;然后,利用熵权法和模糊层次分析法计算安全虚拟网络功能评价指标的权重,采用组合赋权法弥补单一赋权法的不足,建立安全虚拟网络功能指标权重计算模型;最后,基于逼近理想解排序法和向量投影法在最优解确定方面的优势,将逼近理想解排序法的距离计算与向量投影法的相似度计算相结合,改进逼近理想解排序法的计算过程,提出基于逼近理想解排序法的安全虚拟网络功能可信等级确定方法,得到安全虚拟网络功能的可信评估结果。本文以防火墙为安全虚拟网络功能的实例,选取3款主流商业虚拟防火墙与2款主流开源虚拟防火墙部署到云环境中进行实验。实验结果证明了本文提出的评估方法的有效性。

**关键词** 安全虚拟网络功能;可信评估;可信性;软件定义安全;软件定义网络

中图法分类号 TP393 DOI号 10.19363/J.cnki.cn10-1380/tn.2025.11.03

## Trustworthiness Evaluation Approach for Security Virtual Network Function

LIU Hao<sup>1,3</sup>, WANG Chong<sup>3</sup>, TIAN Zhihong<sup>4</sup>, WU Zhonghai<sup>1,2</sup>

<sup>1</sup> Department of Software and Microelectronics, Peking University, Beijing 100871, China

<sup>2</sup> National Engineering Research Center for Software Engineering, Peking University, Beijing 100871, China

<sup>3</sup> QiAnXin Technology Group Co., Ltd., Beijing 100044, China

<sup>4</sup> Institute of Advanced Cyberspace Technology, Guangzhou University, Guangzhou 510623, China

**Abstract** In software-defined security, one or more security virtual network functions need to be combined and instantiated to form a security service function chain to achieve security reinforcement and protection of the target business. In the traditional construction stage of security service function chain, the selection of security virtual network functions is generally based on expert experience and lacks unified selection basis. Aiming to address the issue of selecting appropriate security virtual network functions, this paper proposes a evaluation approach for security virtual network functions, guided by the idea of trustworthiness measurement. First, the related research work is reviewed and analyzed. On this basis, the security virtual network function evaluation criterion is defined. Secondly, a security virtual network function trustworthiness measurement model is proposed based on the multiple attribute decision method from the dynamic trust evaluation model. Then, the entropy weight method and the fuzzy analytical hierarchy process are used to calculate the weight of the security virtual network functions evaluation criterion. The combined weighting method is used to eliminate the shortcomings of one single weighting method, and a security virtual network function criterion weight calculation model is established. At last, using the advantages of the technique for order preference by similarity to ideal solution and vector projection method, the distance calculation of the technique for order preference by similarity to ideal solution and the similarity calculation of vector projection method is combined. On the basis of improving the calculation process of these two methods, this paper proposes a trustworthiness evaluation approach for security virtual network functions based on the technique for order preference by similarity to ideal solution, and the trustworthiness evaluation results of security virtual network function are obtained. This paper takes firewall as instances of security virtual network functions, and selects three mainstream commercial virtual firewalls and two mainstream open source virtual firewalls to deploy them in a cloud en-

通信作者: 吴中海, 博士, 教授, Email: wuzh@pku.edu.cn。

本课题得到工业和信息化部2023年产业基础再造和制造业高质量发展专项(No. TC220H054)资助。

收稿日期: 2023-12-19; 修改日期: 2024-06-03; 定稿日期: 2025-10-15

environment for experiments. The experimental results demonstrate the effectiveness of the trustworthiness evaluation approach proposed in this paper.

**Key words** security virtual network functions; trustworthiness evaluation; trustworthiness; software defined security; software defined network

## 1 引言

在传统网络架构中, 服务供应商通常在网络中部署较多的专有设备(中间件)来达到满足云数据中心需求的目的, 但是中间件的部署导致了高额的运营支出与成本支出, 也使传统网络变得臃肿和僵化<sup>[1]</sup>。而虚拟网络功能(Virtual Network Function, VNF)以软件代替现有网络功能的形式缓解了这个问题。VNF 被应用于各种网络架构中, 如软件定义网络(Software Defined Network, SDN)、软件定义安全(Software Defined Security, SDS)和网络功能虚拟化(Network Functions Virtualization, NFV)等。其中, SDS 架构下则重点关注安全虚拟网络功能(Security Virtual Network Function, SVNf)。在安全场景中, NFV 可以将传统安全分解成 SVNf<sup>[2-3]</sup>, SDS 则可实现安全虚拟网络功能的管理和编排<sup>[4]</sup>。这些技术的结合可以让多种 SVNf 相互组合从而形成安全服务功能链(Security Service Function Chain, SSFC), 为用户提供安全服务, 保障用户的网络安全。

但是安全服务功能链的构建也面临着新的挑战, 即如何选取合适的 SVNf 用以构建安全服务功能链并进行合理的资源分配, 为用户提供满意的网络服务<sup>[5]</sup>。近些年, 国内外学者对 VNF 进行了广泛的研究, 并提出了各种评价指标来评价它们。其中, 性能指标方面主要包括 CPU<sup>[6-7]</sup>、内存<sup>[8]</sup>、带宽<sup>[7]</sup>、延迟<sup>[2]</sup>等。例如, 延迟是衡量 VNF 性能的关键指标<sup>[9-10]</sup>, 研究者通过测量 VNF 的延迟评估其响应能力。除了性能评估, VNF 的可靠性<sup>[11-12]</sup>、容错性<sup>[13-15]</sup>和可用性<sup>[16]</sup>也是 VNF 研究的重点。

然而, 这些研究工作主要以各自面对的不同应用场景为基础, 各有侧重地关注了 VNF 某一项或者某几项评价指标, 缺乏对 SVNf 的安全特性的评价。特别地, 面对具有复杂性和多样性的 SVNf 来说, 缺乏一个统一的且全面的评价指标体系。当前可信评估相关的研究表示<sup>[17-20]</sup>, 研究人员会基于可信评估构建评价指标或模型并对 Web 软件、移动终端软件、控制器等目标进行评价<sup>[21-22]</sup>。然而, 这些研究也并未涉及 SVNf。在本文中, 我们考虑如何更加充分利用可信评估方法, 基于多属性决策方法提出更为合理的 SVNf 评价模型, 其中基于 MITRE ATT&CK<sup>[23]</sup>提出了 SVNf 的功能属性(安全服务属性)的设计。该

模型利用模糊层次分析法(Fuzzy Analytic Hierarchy Process, FAHP)以及熵相关理论来协调主观指标和客观指标间的权重, 并融合逼近理想解排序法(Technique for Order Preference by Similarity to Ideal Solution, TOPSIS)和向量相似度作为计算方法用以得到 SVNf 评估结果。该定义模型及其计算方法则可以根据不同类型的 SVNf 来评测 SVNf 的实例。最后, 用实验验证了新模型下的 SVNf 评估方法具备合理性和可行性。

## 2 相关工作

可信度量及其建模主要基于动态信任评估模型完成, 包括行为分析模型、多属性决策模型和信誉模型<sup>[24]</sup>。行为分析模型可分为设备行为分析和用户网络行为分析。设备行为分析主要用于身份认证。行为分析模型一般用于恶意行为识别<sup>[25]</sup>、行为预测<sup>[26]</sup>等。多属性决策模型通过分析影响用户信任的属性和属性值来做出信任决策。信誉模型侧重于评价数据的采集和计算, 应用于多用户交互场景。

郎波等人<sup>[20]</sup>在 ISO/IEC 9126:2001 基础上提出了一种分层的软件可信分级模型, 建立了软件可信证据参考模型, 描述了可信属性、可信等级、可信证据以及可信评价指标之间的内在联系, 为后续研究奠定基础。赵玉洁等人<sup>[22]</sup>也基于 ISO/IEC 9126 构建了 Web 软件可信性评价指标体系。该评价方法用结构熵值法确定了各个可信指标的权重, 然后运用置信度识别准则对 Web 软件可信性进行了等级评价和得分计算, 并根据可信性决策规则集制定了相应的策略。Zhang<sup>[27]</sup>则认为目前的 Web 服务组合可信度评估方法偏向于服务提供者本身, 而忽略了服务发现者和用户的可信度。因此提出一种多角度 Web 服务组合可信度评估方法, 综合考虑 Web 服务组合的三个方面, 并利用服务查找器扩展服务中心。熊钢等人<sup>[18]</sup>在郎波等人<sup>[20]</sup>所提出的软件可信分级模型的基础上提出了面向网络组件性能的评估方法, 但仅面向控制器进行了评价应用验证。然而, 目前 ISO/IEC 9126:2001 已被 ISO/IEC 25000 标准替代, 该工作缺乏对此标准的考量。Liu 等人<sup>[28]</sup>则参考了 ISO/IEC 25000—25010, 基于智能层次分析法提出了 iTrustEval 框架进行软件可信度评估。iTrustEval 包含一种可扩展的可信模型, 能够按需与工业可信标准(例如 ISO

25010)集成。Zhou 等人<sup>[29]</sup>认为在综合评价软件质量时, 还需要额外考虑组件的权重和用户反馈的权重。根据组件的不同结构, 采用证据理论计算组件权重, 并根据组件权重和用户反馈建立不同的可信度度量模型。

SVNF 相比于 VNF 更加关注所能提供的安全服务能力, 目前主要相关研究工作包括 SVNF 的部署。Tamim 等人<sup>[30]</sup>面向网络服务提供商提出了一种部署服务功能链的方法, 安全虚拟网络功能属于该服务功能链的组成部分, 其核心思想在于如何在满足性能约束和安全虚拟网络功能操作规则的基础上, 通过混合整数线性规划模型给出满足约束的部署方案。Doriguzzi-Corin 等人<sup>[2]</sup>认为部署中除了性能约束外, 还应考虑用户应用程序的安全性和服务质量方面的约束, 并提出了一种安全虚拟网络功能的有效部署方法。Doriguzzi-Corin 等人<sup>[31]</sup>还研究了流量对特定网络的敏感性, 认为最小带宽、最大端到端延迟等约束也是需要考虑的因素, 因此提出了名为安全服务渐进式嵌入(PESS)的方法来满足这些约束。并给出了 PESS 的数学模型和启发式求解方法。Wu 等人<sup>[32]</sup>则认为现有的安全虚拟网络功能部署解决方案没有考虑安全服务链应该解决的流量可达性问题和策略冲突问题, 因此提出了一种方案用以快速有效地检查和消除策略冲突。

VNF 在实际应用场景中, 其相关的评价指标包括 CPU<sup>[6-7]</sup>、内存<sup>[8]</sup>、带宽<sup>[7]</sup>、延迟<sup>[2]</sup>等, 这些指标只能反映 VNF 的某一个或者某几个特性, 但也为本文解决 SVNF 的可信评估度量体系指标设计提供了方法参考。当前可信度量的主要研究工作<sup>[18,20]</sup>针对可信指标的权重计算问题提出了模糊分析法和熵值等方法, 缺少对 ISO/IEC 25000 以及 SVNF 评估的考量, 但为本文的 SVNF 可信评估体系构建和权重计算问题提供了有效的借鉴。本文基于上述研究成果, 提出一种基于可信评估的安全虚拟网络功能评估方法, 实现了可信评估下的 SVNF 指标评价体系构建, 为安全服务功能链中 SVNF 的选取提供了适当的依据和理论支撑。

### 3 基于可信度量的 SVNF 属性模型

#### 3.1 软件可信性

起初计算机领域的研究人员使用 dependability 表示软件可信性这一概念, 随着计算机网络技术的不断发展, 人们用 trustworthiness 一词替代 dependability 来描述软件可信性问题<sup>[22]</sup>。软件可信性涉及航空航天、军事科学、兵器、交通、医疗卫生等国民经济

的各个重要领域<sup>[33-34]</sup>, 而随着软件系统重要性和复杂性的不断增加, 即使是最小的故障也可能对用户的财产安全和生命安全构成威胁<sup>[27,35]</sup>。因此, 尽管人们对软件的功能性和多样性的需求持续增长, 但对软件故障的容忍度却逐渐下降<sup>[36]</sup>。这引起了人们对“软件可信度”问题的广泛关注, 现有的软件可信度研究可以分为软件可信度测量、软件可信度评估和软件可信度分配等方面<sup>[37]</sup>。软件可信度测量与评价相当于对软件系统进行定量评估, 为后续的设计和开发提供指导, 对于提高软件质量具有重要意义<sup>[38]</sup>。现有的软件可信度测量模型大多将高层属性分解为易于评估的低层属性, 然后利用不同的数学工具综合底层子属性的测量值<sup>[39]</sup>。

软件可信性(Software Trustworthiness)描述了软件系统在不稳定的环境中受到不确定因素的干扰时, 能够保持稳定并继续按照预期方式运行的程度<sup>[40]</sup>。软件可信性度量的问题其实就是软件可信性的属性选取和度量、用户预期的表达和依据对被选择属性的度量值 and 用户预期对两者符合性的量化问题<sup>[22]</sup>。软件可信性作为对功能性、可靠性、可维护性等软件质量度量的一种综合化延伸, 反映了软件实体多维质量特征的综合属性<sup>[41]</sup>。因此, 本文认为 SVNF 可信性是指 SVNF 的行为和结果符合设计预期, 且能够很好地抵御其他因素造成的干扰。

#### 3.2 基于可信度量的 SVNF 评价模型

在 NFV 中, VNF 是网络服务提供商使用基于软件的虚拟网络功能替换物理网络设备的方法<sup>[42]</sup>。而面向用户不同的网络安全需求, 网络服务提供商需要选择并利用若干 SVNF 按照一定的顺序部署在服务器节点上, 形成能够提供安全服务的网络功能序列, 即安全服务功能链, 它利用软件定义网络功能来创建一条连接网络服务的服务链(如防火墙、网络地址转换、入侵防护)并将其连接到虚拟链上, 并为用户提供对应的安全服务<sup>[43]</sup>。

但是由于应用场景的多样性以及 SVNF 运行环境的不确定性与复杂性, SVNF 可信性是 SSFC 组链成功的关键因素, 因此, 基于可信度量构建 SVNF 评价模型, 完成对 SVNF 进行可信性评估是重要的问题。经过对现有研究工作<sup>[18,20,23-24,44-45]</sup>的归纳和分析, SVNF 应具有的可信属性主要包括功能属性、可靠属性、安全属性、时效属性、可维护属性、可生存属性、可用属性, 如图 1 所示。其中, SVNF 相比于 VNF 更加关注所能提供的安全服务能力, 因此基于 MITRE ATT&CK<sup>[23]</sup>, 本文提出了 SVNF 功能属性(安全服务属性)的及其所有子属性如表 1 所示。SVNF

的所有可信子属性的评估数据获取方式主要分为两类: 客观评估与主观评估。客观评估可由漏洞扫描软

件、性能监控软件等各种工具完成。主观评估则借助专家的经验 and 专业知识完成。

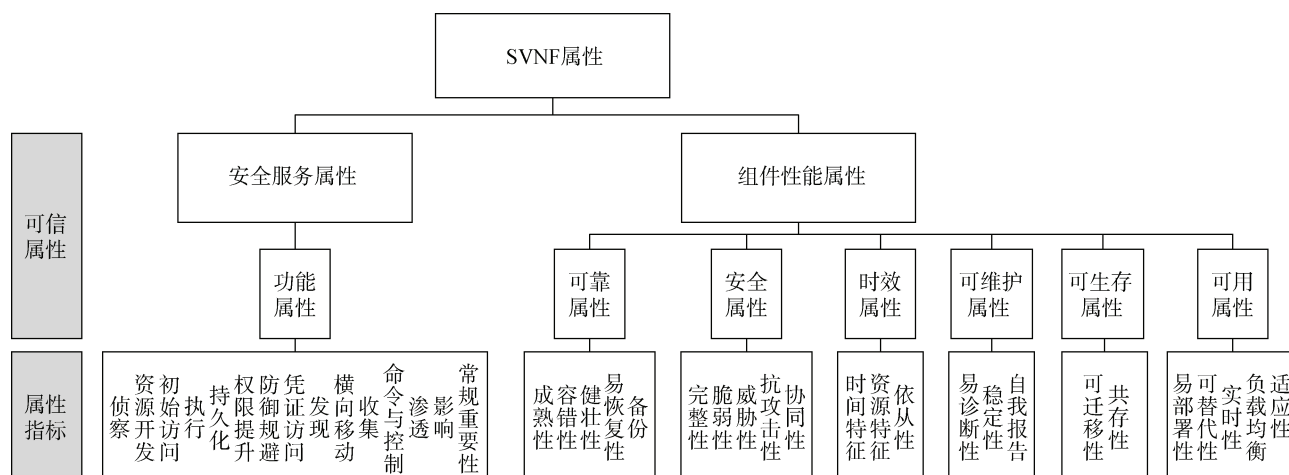


图 1 安全虚拟网络功能可信属性模型

Figure 1 Model of Trustworthy Attributes for SVNf

表 1 SVNf 功能属性子属性及说明

Table 1 Functional Attributes, Sub-Attributes, and Explanations of SVNf Features

| 子属性   | 属性说明            |
|-------|-----------------|
| 侦察    | 阻止攻击者侦察系统弱点能力   |
| 资源开发  | 阻止攻击者获取目标攻击资源能力 |
| 初始访问  | 防御攻击者渗透目标系统能力   |
| 执行    | 阻止攻击者运行恶意代码能力   |
| 持久化   | 阻止攻击者保持非法权限能力   |
| 权限提升  | 阻止攻击者提升权限能力     |
| 防御规避  | 检测伪装攻击能力        |
| 凭证访问  | 阻止攻击者获取合法凭证能力   |
| 发现    | 阻止攻击者深入探测系统能力   |
| 横向移动  | 阻止攻击者访问其他资源能力   |
| 收集    | 阻止攻击者收集攻击目标数据能力 |
| 命令与控制 | 阻止攻击者控制系统能力     |
| 渗透    | 保护数据安全能力        |
| 影响    | 防止攻击者破坏数据能力     |
| 常规重要性 | 设备在业务中的重要性      |

## 4 基于逼近理想解排序法和多属性决策模型的可信评估模型

### 4.1 SVNf 可信指标树构建

在实际安全服务中, SVNf 实例多样, 业务类型复杂, 政府、企业、学校以及家庭等不同应用场景有着不同的需求, 为了构建一个满足动态性与多样性要求的 SVNf 评价指标体系, 本文拟基于一种具有动态适应性的 SVNf 可信指标树(Security Virtual Network Functions Trustworthiness Index Tree,

SVNFTIT)构造 SVNf 评价模型。

#### 4.1.1 形式化建模

图 2 是安全虚拟网络功能可信指标树示意图, 图中每一层代表着不同级别的属性, 每个节点代表不同指标, 除根节点外, 每个节点有其对应的权重值与属性值, 用于计算其父节点的属性值。基于上述定义, SVNf 可信指标树可由一个三元组进行描述  $SVNFTIT = \{STNode, STWeight, STValue\}$ , 其中包含的各个元组的含义分别如下:  $STNode = \{SVNFroot, SVNfattribute, SVNfmiddle, SVNfleaf\}$  是可信指标节点集合, 其中  $SVNFroot$  是根指标,  $SVNFattribute = \{SVNFA_k, k \in N^*\}$  是属性指标集合,  $SVNfmiddle = \{SVNFM_m, m \in N^*\}$  是中间指标集合, 是对各属性指标的进一步细化,  $SVNFleaf = \{SVNFL_v, v \in N^*\}$  ( $N^*$  是正整数集) 是叶子指标集合。  $STWeight$  是节点指标权重集合, 属于同一父节点的所有子节点权重满足归一化原则。  $STValue$  是节点指标的可信度量数据(简称为“可信值”)集合, 其中, 叶子节点是 SVNf 实例的原始数据, 中间节点数据与根节点数据是其子节点数据通过对应权重计算获得的。

#### 4.1.2 可信指标树建立步骤

针对不同的应用场景, 构建 SVNf 可信指标集合, 首先构建属性指标集合, 将其作为根节点的子节点, 之后采用递归的方式, 对每层节点进行细化: 若该节点存在可细化的子属性, 则将其子属性作为其子节点; 若该节点不包含子属性, 则将其作为本树叶节点。按照该步骤逐层处理, 直至最后一层全

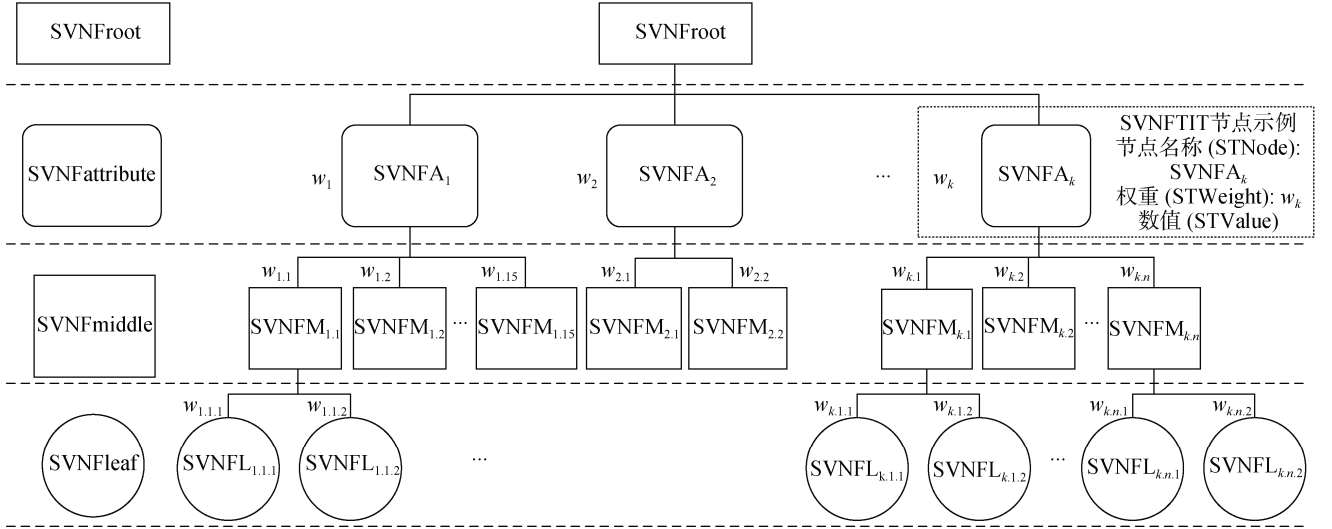


图 2 安全虚拟网络功能可信指标树

Figure 2 Trustworthiness Index Tree for SVNF

部为叶子节点。最终，基于形式化描述，将各节点可信指标赋权构成可信指标树，如图 2 所示。图 2 中 SVNRoot 为 VNF 实例的可信根指标，其由  $k$  个可信属性指标组成，而每一可信属性指标又可分解为若干中间指标 SVNFMiddle 或者叶子指标 SVNFLleaf，其中叶子指标是原始可信值的采集点。

## 4.2 模糊集合理论

### 4.2.1 模糊集合

在评估决策问题中存在着许多非精确关系，为了在数学的角度的刻画模糊的概念，Zadeh<sup>[46]</sup>通过量化中间过渡的方式，提出了模糊集合理论。经典集合通常采用 1、0 来表示是或者否，然而在决策问题中通常存在“较好”“较差”的概念，模糊集合理论提出了隶属度函数的概念，使用 0-1 之间的数值表示该对象在集合中的隶属关系。

### 4.2.2 三角模糊数

三角模糊数能够有效地表示某些难以用精确数值描述的信息，还可以灵活地与其他模糊数进行转换计算，本文采用三角模糊数(Triangular Fuzzy Number, TFN)对模糊集合进行描述，设一个三角模糊数为  $\tilde{k} = (k^l, k^m, k^r)$ ，其对应的隶属度函数为

$$F(x) = \begin{cases} \frac{x - k^l}{k^m - k^l}, & k^l \leq x \leq k^m \\ \frac{x - k^r}{k^m - k^r}, & k^m \leq x \leq k^r \\ 0, & \text{其他} \end{cases} \quad (1)$$

其中，参数  $k^l \leq k^m \leq k^r$ ， $k^l$ 、 $k^m$  和  $k^r$  分别表示描述

模糊事件的最小可能值、最有希望值和最大可能值。下面给出三角模糊数的三种运算法则，设两个三角模糊数分别为  $\tilde{x} = (x^l, x^m, x^r)$ ， $\tilde{y} = (y^l, y^m, y^r)$ ，其加法运算为  $\tilde{x} \oplus \tilde{y} = (x^l + y^l, x^m + y^m, x^r + y^r)$ ，乘法运算为  $\tilde{x} \otimes \tilde{y} = (x^l y^l, x^m y^m, x^r y^r)$ ，倒数运算为  $\tilde{x}^{-1} = (1/x^l, 1/x^m, 1/x^r)$ 。

### 4.3 主观赋权法

在计算权重时，常见主观赋权方法包括层次分析法、功效系数法、综合指数法等。在传统的层次分析法中，专家的评判是通过详细的实数来体现的，而专家经验通常不能用定量的数据完全体现，本文采用模糊层次分析法，将模糊集合理论与层次分析法结合，有效地解决了层次分析法不适合专家模糊经验的问题。

假设共有  $N$  个评价指标， $S$  名专家进行评估，则具体流程如下。

Step 1: 构建第  $s(s=1, 2, \dots, S)$  名专家的评价标准构建模糊矩阵：

$$\bar{A}^s = [\tilde{a}_{ij}^s] = \begin{bmatrix} 1 & \tilde{a}_{12}^s & \dots & \tilde{a}_{1N}^s \\ \tilde{a}_{21}^s & 1 & & \tilde{a}_{2N}^s \\ \vdots & & \ddots & \vdots \\ \tilde{a}_{N1}^s & \tilde{a}_{N2}^s & \dots & 1 \end{bmatrix}$$

其中，矩阵元素  $\tilde{a}_{ij}^s$  表示指标间的相对重要程度， $\tilde{a}_{ij}^s = (\tilde{a}_{ji}^s)^{-1} (i \neq j)$ 。借鉴层次分析法和三角模糊数<sup>[47-48]</sup>，本文将指标相对重要程度划分为同等重

表 2 指标相对重要性程度及其取值  
Table 2 Relative Importance Levels and Assigned Values of Evaluation Indicators

| 重要程度 | 三角模糊数     |
|------|-----------|
| 同等重要 | (1, 1, 2) |
| 稍微重要 | (2, 3, 4) |
| 明显重要 | (3, 4, 6) |
| 极其重要 | (5, 7, 8) |
| 绝对重要 | (7, 8, 9) |

要、稍微重要、明显重要、极其重要、绝对重要五个等级, 同时在表 2 中给出其对应的三角模糊数。

Step 2: 采用算术平均法融合  $S$  名专家的模糊判断矩阵, 融合矩阵  $\bar{A} = [\tilde{a}_{ij}]$ :

$$\tilde{a}_{ij} = \frac{(\tilde{a}_{ij}^1 \oplus \tilde{a}_{ij}^2 \oplus \dots \oplus \tilde{a}_{ij}^S)}{S} \quad (2)$$

即  $S$  个矩阵对应位置相加再除以  $S$ 。

Step 3: 计算模糊主观权重, 采用行算术平均值归一化的方法计算模糊主观权重向量  $\tilde{w}_i^{(1)} = (w_i^{(1)l}, w_i^{(1)m}, w_i^{(1)r})$ ,  $i=1, 2, \dots, N$ , 然后将特征向量归一化, 计算如公式(3)所示:

$$\tilde{w}_i^{(1)} = \frac{\frac{1}{N} \left( \sum_{j=1}^N \tilde{a}_{ij} \right)}{\sum_{i=1}^N \left( \frac{1}{N} \sum_{j=1}^N \tilde{a}_{ij} \right)} \quad (3)$$

Step 4: 对权重向量进行去模糊化处理, 去模糊化是一种将模糊数转换为清晰实数的方法。上述主观权重用三角形模糊数表示。当前存在有多种去模糊化方法如分级均值积分表示方法等, 本文参考现有研究工作<sup>[49-50]</sup>, 采取计算方法具体如公式(4)所示:

$$w_i^{(1)} = w_i^{(1)m} + \frac{(w_i^{(1)l} - 2w_i^{(1)m} + w_i^{(1)r})}{3} \quad (4)$$

#### 4.4 客观赋权法

信息论中, 熵是衡量所提供数据的有用信息量的标准。根据信息熵的定义, 对于某项指标, 可以用熵值来判断某个指标的离散程度, 其信息熵值越小, 指标的离散程度越大, 该指标对综合评价的影响(即权重)就越大, 如果某项指标的值全部相等, 则该指标在综合评价中不起作用。因此, 本文利用信息熵计算出各个指标的权重, 为多指标综合评价提供依据。熵权法包括以下步骤。

Step 1: 待评价 SVNf 实例集合为  $V = \{V_1, V_2, \dots, V_l\}$ , 评价指标集合为  $C = \{C_1, C_2, \dots, C_n\}$ , 构建原始数据评价矩阵:

$$P = \begin{matrix} & C_1 & C_2 & \dots & C_n \\ \begin{matrix} V_1 \\ V_2 \\ \vdots \\ V_l \end{matrix} & \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{l1} & p_{l2} & \dots & p_{ln} \end{bmatrix} \end{matrix}$$

其中,  $p_{ij}$  为 SVNf 实例  $V_i$  在评价指标  $C_j$  下的表现对应数据。

Step 2: 对各列进行归一化操作, 由于各项 SVNf 实例评价指标之间有不同的量纲和量纲单位, 为了消除其对数据分析的影响, 本文采用列归一化的方法, 将数据转化到  $[0, 1]$  的区间, 具体计算如下:

$$x_{ij} = \frac{p_{ij}}{\sum_{i=1}^l p_{ij}} \quad (5)$$

Step 3: 计算 SVNf 实例评价指标的信息熵:

$$E_j = -\ln(l)^{-1} \sum_{i=1}^l [x_{ij} \ln(x_{ij})] \quad (6)$$

当  $x_{ij} = 0$  时, 令  $x_{ij} \ln(x_{ij}) = 0$ ; 熵值  $E_j \in [0, 1]$ , 当  $x_{ij}$  全部相等时,  $x_{ij} = 1/l$ ,  $E_j$  取最大值 1。

Step 4: 计算客观权重向量为

$$w_j^{(2)} = \frac{1 - E_j}{\sum_{j=1}^n (1 - E_j)} \quad j=1, 2, \dots, n \quad (7)$$

其中,  $w_j^{(2)}$  是第  $j$  个评价指标的客观权重。

#### 4.5 联合权重计算

主观权重根据决策者意图确定权重方面具有更大的优势, 但客观性相对较差, 主观性相对较强, 客观权重不能反映出参与决策者对不同指标重视程度, 针对主客观权重方法的优缺点, 本文采用组合赋权法将二者组合起来, 弥补单一赋权的不足, 计算联合权重向量  $w$  为

$$w = \sum_{k=1}^2 \frac{1}{2} w^{(k)} \quad (8)$$

其中,  $w^{(1)}$  为基于模糊层次分析法获得的主观权重,  $w^{(2)}$  为基于熵权法确定的客观权重。

#### 4.6 基于 TOPSIS 的 SVNf 实例评级决策

SVNf 评级决策是在指标可信值与指标权重的基础上, 通过可信值计算、决策矩阵建立以及评级指标计算三步, 构建 SVNf 实例综合的评级决策。

##### 4.6.1 可信值计算

可信值原始数据一般包括定量指标数据(O)与定性指标数据(Q), 其中定性指标数据一般为客观数值, 定量指标数据一般由专家评估获得, 数据范围包括最

差(W)、较差(P)、平均(A)、较好(G)、最好(T)五个等级。

为了避免原始数据之间量纲和量纲单位的差异影响评级的客观性, 本文通过三角模糊数的方式对定性数据进行转换, 如表 3 所示。

表 3 指标评价等级及对应三角模糊数

Table 3 Evaluation Grades and Corresponding Triangular Fuzzy Numbers for Indicators

| 定性数据  | 三角模糊数            |
|-------|------------------|
| 最差(W) | (0.0, 1.0, 2.0)  |
| 较差(P) | (2.0, 4.0, 5.0)  |
| 平均(A) | (4.5, 6.5, 7.5)  |
| 较好(G) | (5.5, 7.0, 8.5)  |
| 最好(T) | (8.0, 9.0, 10.0) |

之后利用式(4)进行去模糊化操作, 将定性数据转化为定量数据, 同时代替  $\mathbf{P}=[p_{ij}]_{l \times n}$  中的对应值, 转化为定量数据矩阵  $\mathbf{U}=[u_{ij}]_{l \times n}$ , 定量数据中有些评估指标是效益指标(越高越好), 而有些评估指标是成本指标(越低越好)。

为了消除由于准则类型不同导致的评估偏差, 本文采用分段式函数对  $\mathbf{U}=[u_{ij}]_{l \times n}$  中的定量数据进行归一化操作:

$$z_{ij} = \begin{cases} \frac{\max_j u_{ij} - u_{ij}}{\max_j u_{ij} - \min_j u_{ij}}, & \text{成本标准} \\ \frac{u_{ij} - \min_j u_{ij}}{\max_j u_{ij} - \min_j u_{ij}}, & \text{效益标准} \end{cases} \quad (9)$$

$\mathbf{Z}=[z_{ij}]_{l \times n}$  即为 SVNf 指标数据可信值矩阵。

#### 4.6.2 决策矩阵构建

决策矩阵将 SVNf 指标权重与指标可信值相结合, 具体步骤分为以下两步。

Step 1: SVNf 实例属性可信值计算。该步骤是计算 SVNf 指标树中 SVNf 属性指标集合中各元素的可信值。设可信指标树 SVNf 存在  $K$  个属性指标  $\text{SVNFA}_k (k=1, 2, \dots, K)$ , 每一 SVNf 属性子树共有  $H$  层, 第 1 层为子树根节点, 即可信属性指标。树中第  $h (h=1, \dots, H-1)$  层的中间节点的可信值是通过第  $h+1$  层节点的可信值计算得到, 设第  $h$  层有  $M$  个中间属性节点, 某一节点  $\text{SVNFM}_m (m=1, 2, \dots, M)$  在第  $h+1$  层有  $T_m$  个子节点, 每一子节点的 SVNf 可信值  $u_i^{h+1} (i=1, 2, \dots, T_m)$ , 且该节点对于  $\text{SVNFM}_m$  节点的权重为  $w_i^{h+1} (i=1, 2, \dots, T_m)$ , 则  $\text{SVNFM}_m$  节点的可信值计算如公式(10)所示:

$$u_m^h = \sum_{i=1}^{T_m} u_i^{h+1} w_i^{h+1} \quad (10)$$

通过上述方法逐层计算, 最终获得每一 SVNf 评价指标的可信值。

Step 2: 构造 SVNf 可信决策矩阵  $\mathbf{D}$ , 设待评价 SVNf 实例集合为  $\{V_1, V_2, \dots, V_l\}$ , SVNf 属性指标可信值集合为  $\{\text{SVNFA}_1, \text{SVNFA}_2, \dots, \text{SVNFA}_K\}$ , 各实例每一属性的可信值为  $u_{ij} (i=1, 2, \dots, l; j=1, 2, \dots, K)$ , 则决策矩阵  $\mathbf{D}=[d_{ij}]_{l \times K}$  为

$$\mathbf{D} = \begin{matrix} & \text{SVNFA}_1 & \text{SVNFA}_2 & \dots & \text{SVNFA}_K \\ \begin{matrix} V_1 \\ V_2 \\ \vdots \\ V_l \end{matrix} & \begin{bmatrix} w_1 u_{11} & w_2 u_{12} & \dots & w_K u_{1K} \\ w_1 u_{21} & w_2 u_{22} & \dots & w_K u_{2K} \\ \dots & \dots & \ddots & \vdots \\ w_1 u_{l1} & w_2 u_{l2} & \dots & w_K u_{lK} \end{bmatrix} \end{matrix} \quad (11)$$

#### 4.6.3 SVNf 评估计算

SVNf 评估指标是对 SVNf 实例综合性能进行评估的定量依据。TOPSIS 是一种常用的利用原始数据进行综合评价的方法, 其基本原理是通过检测评价对象与最优解、最劣解的欧氏距离来进行排序。最优逼近的方式是衡量某一检测对象与最优数据之间的逼近程度, 本文将最优逼近和 TOPSIS 的方法结合, 将欧氏距离修改为相似度, 具体如下:

Step 1: 分别计算正负理想向量  $\beta^+ = (b_1^+, b_2^+, \dots, b_K^+)$ ,  $\beta^- = (b_1^-, b_2^-, \dots, b_K^-)$ 。在计算确定过程中, 正负理想向量计算可分为以下两种情况: (1)有明确需求目标时, 可根据具体需求直接给出  $b_i^+$  或  $b_i^-$  的值。(2)没有具体需求时, 可在决策矩阵  $\mathbf{D}$  的基础上计算  $\beta^+$  与  $\beta^-$  的具体数值, 计算如公式(12)、公式(13)所示:

$$b_i^+ = \max_{1 \leq j \leq l} (b_{ij}), i=1, 2, \dots, K \quad (12)$$

$$b_i^- = \min_{1 \leq j \leq l} (b_{ij}), i=1, 2, \dots, K \quad (13)$$

Step 2: 计算待评估组件可信属性向量  $\beta_j = (\beta_{j1}, \beta_{j2}, \dots, \beta_{jk}) (j=1, 2, \dots, l)$  (即矩阵  $\mathbf{D}$  的各行取值) 与正负理想解  $\beta^+ = (b_1^+, b_2^+, \dots, b_K^+)$ ,  $\beta^- = (b_1^-, b_2^-, \dots, b_K^-)$  之间的相对近似度, 计算

如公式(14)所示:

$$S_j^* = \begin{cases} \frac{\beta^* \beta_j}{\|\beta^*\|^2} = \frac{\|\beta^*\| \|\beta_j\| \cos \langle \beta^*, \beta_j \rangle}{\|\beta^*\|^2} \\ , \|\beta^*\| \|\beta_j\| \leq \beta^{*2} \\ \left( \frac{\beta^* \beta_j}{\|\beta^*\|^2} \right)^{-1} = \frac{\|\beta^*\|^2}{\|\beta^*\| \|\beta_j\| \cos \langle \beta^*, \beta_j \rangle} \\ , \text{其他} \end{cases} \quad (14)$$

其中,  $S_j^*$  等于  $S_j^+$  (与正理想解之间的相似近似度) 或  $S_j^-$  (与负理想解之间的相似近似度),  $\beta^*$  等于  $\beta^+$  (正理想向量) 或  $\beta^-$  (负理想向量),  $\beta^* \beta_j$  表示向量之间的内积,  $\|\beta^*\|$  表示向量  $\beta^*$  的模长,  $\cos\langle\beta^*, \beta_j\rangle$  是两向量之间的夹角余弦值。  $S_j^*$  表示向量  $\beta_j$  在向量  $\beta^*$  方向上的投影  $\beta_j \cos\langle\beta^*, \beta_j\rangle$  与向量  $\beta^*$  的模长  $\|\beta^*\|$  比值, 当向量  $\beta_j$  与向量  $\beta^*$  越接近, 比值就越接近 1, 反之越接近 0。

Step 3: 计算评级指标值  $\gamma_j$ , 参考 TOPSIS 的计算方法, 计算如公式(15)所示:

$$\gamma_j = \frac{S_j^-}{S_j^- + S_j^+} \quad (15)$$

我们给出 SVNf 实例评估参考等级如表 4 所示。

基于本章可信计算模型构建 SVNf 评估决策流程图 3, 整体流程共分为可信指标树构建、指标权重计算以及 SVNf 评估决策三步。基于评估指标构建的指标树清晰地展示了各项指标之间的计算关系, 指导了后续子指标数据采集与上层指标数据计算; 设计了基于熵权法的客观权重计算方式与基于模糊层次分析法的主观权重计算方式, 并计算二者的联合权重, 更加合理地将采集信息反馈到数据中; 最后基于最优逼近与 TOPSIS 结合的方法计算可信评分, 得到 SVNf 评估参考等级。

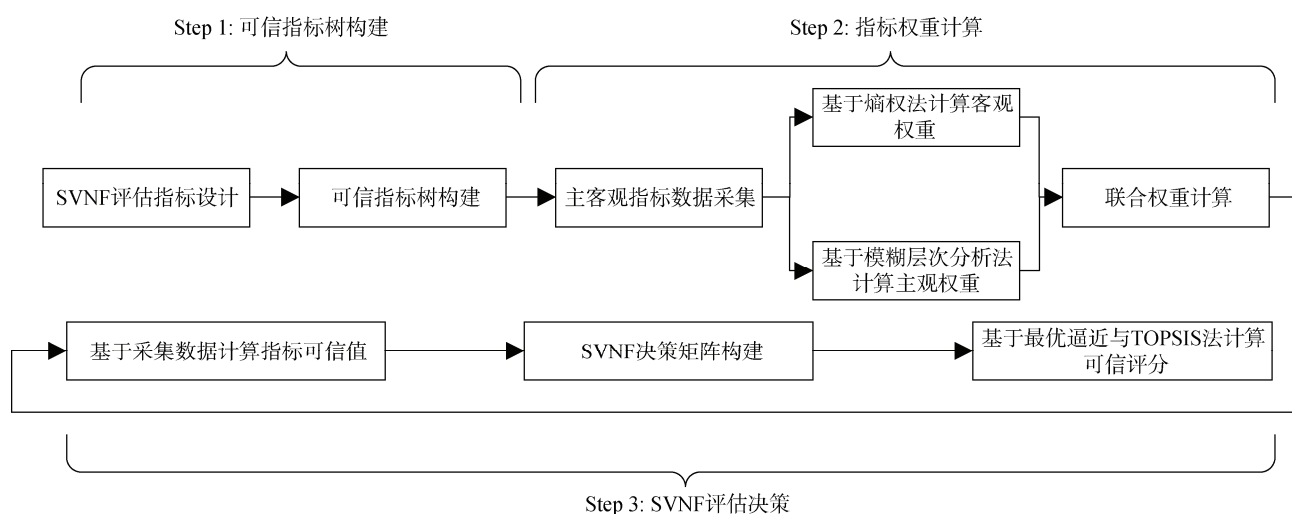


图 3 SVNf 可信评估流程

Figure 3 Process Flowchart for Trustworthiness Assessment of SVNfs

表 4 SVNf 实例评估参考等级

Table 4 Reference Grading Criteria for Evaluating SVNf Instances

| 指标值       | 等级 |
|-----------|----|
| [0,0.2)   | 极好 |
| [0.2,0.4] | 优秀 |
| [0.4,0.6] | 良好 |
| [0.6,0.8] | 一般 |
| [0.8,1.0] | 较差 |

## 5 实验

### 5.1 实验环境

本文选取了五款具有代表性的防火墙设备进行评估对比, 包括一款国外防火墙和两款国内防火墙: C、Q 和 H(为了避免商业因素, 以上三个商业防火墙分别用商业 1、商业 2、商业 3 替代), 两款开源防火

墙 IPFire、PFSense(分别用开源 1、开源 2 替代)。实验环境为 Rocky Linux 8.6 和 VMware ESXi 6.7.0; CPU 为 Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz; 内存为 8GB。主观评价的定性数据由三角模糊数或者专家打分组成, 客观评价的定量数据则由实验测试获取。

### 5.2 指标权重计算

依据评价指标数据, 则可利用第 4 节中的计算方法, 通过可信值计算权重。下面以时效属性为例进行介绍。

Step 1: 计算主观权重。邀请三位专家在图 1 与表 2 的评价规则基础上, 对时效属性的三个属性指标进行重要性打分, 构建模糊两两比较矩阵, 部分结果如表 5 所示。下一步通过式(2)对三位专家的数据进行融合, 融合结果如表 6 所示。之后在表 6 的基础上, 通过式(3)、式(4), 计算得到去模糊化的主观权

重值, 结果如表 7 所示。

表 5 SVNf(防火墙类)时效属性专家评分矩阵  
Table 5 Expert Evaluation Matrix for Temporal Attributes of SVNf (Firewall)

| 指标   | 专家 1          |               |               |
|------|---------------|---------------|---------------|
|      | 时间特征          | 资源特征          | 依从性           |
| 时间特征 | (1,1,2)       | (3,4,6)       | (2,3,4)       |
| 资源特征 | (1/6,1/4,1/3) | (1,1,2)       | (1/4,1/3,1/2) |
| 依从性  | (3,4,6)       | (1/6,1/4,1/3) | (1,1,2)       |

表 6 SVNf(防火墙类)时效属性专家评分融合矩阵  
Table 6 Integrated Expert Scoring Matrix for Temporal Attributes of SVNf (Firewall)

| 指标   | 时间特征                | 资源特征             | 依从性                 |
|------|---------------------|------------------|---------------------|
| 时间特征 | (1,1,2)             | (2,3,4)          | (2.289,3.302,4.579) |
| 资源特征 | (0.2,0.333,1)       | (1,1,2)          | (3,4,6)             |
| 依从性  | (0.188,0.303,0.794) | (0.167,0.25,0.5) | (1,1,2)             |

表 7 SVNf(防火墙类)时效属性指标主观权重  
Table 7 Subjective Weights of Temporal Attributes Indicators for SVNf (Firewall)

| 指标   | 模糊主观权重              | 主观权重  |
|------|---------------------|-------|
| 时间特征 | (0.589,0.585,0.508) | 0.565 |
| 资源特征 | (0.299,0.300,0.350) | 0.316 |
| 依从性  | (0.112,0.115,0.142) | 0.120 |

Step 2: 计算客观权重。表 8 提供了原始数据值, 首先通过式(4)将其中的三角模糊数值进行去模糊化处理, 之后通过式(5)将所有数据进行归一化操作, 结果如表 9 所示。最后通过式(6)与式(7)计算得到客观权重如表 10 所示。

表 8 SVNf(防火墙类)时效属性指标原始数据  
Table 8 Original Data of Temporal Attributes Indicators for SVNf (Firewall)

| 编号 | 实例   | 定量指标 |      |      |
|----|------|------|------|------|
|    |      | 时间特征 | 资源特征 | 依从性  |
| 1  | 商业 1 | 50   | 10   | 1000 |
| 2  | 商业 2 | 104  | 21.1 | 440  |
| 3  | 商业 3 | 550  | 5.5  | 32   |
| 4  | 开源 1 | 57   | 14.4 | 1300 |
| 5  | 开源 2 | 56   | 7.1  | 400  |

Step 3: 计算联合权重。基于主观权重  $w^{(1)}$  与客观权重  $w^{(2)}$ , 通过式(8)组合赋权法计算联合权重为 (0.570,0.218,0.212)。同样, 通过上述步骤计算其他 6

类属性指标的联合权重, 得到 SVNf 可信属性指标权重。图 4 展示了部分属性主观权重、客观权重以及联合权重的对比数据, 发现通过组合赋权的方式, 有效地平衡了主观权重与客观权重之间的差异, 消除了二者的片面性。

表 9 SVNf(防火墙类)时效属性指标归一化数据  
Table 9 Normalized Data of Temporal Attributes Indicators for SVNf (Firewall)

| 编号 | 实例   | 指标归一化数据 |       |       |
|----|------|---------|-------|-------|
|    |      | 时间特征    | 资源特征  | 依从性   |
| 1  | 商业 1 | 0.061   | 0.172 | 0.309 |
| 2  | 商业 2 | 0.127   | 0.363 | 0.142 |
| 3  | 商业 3 | 0.673   | 0.095 | 0.010 |
| 4  | 开源 1 | 0.070   | 0.248 | 0.402 |
| 5  | 开源 2 | 0.069   | 0.122 | 0.136 |

表 10 SVNf(防火墙类)时效属性指标客观权重  
Table 10 Objective Weights of Temporal Attributes Indicators for SVNf (Firewall)

| 名称   | 时间特征  | 资源特征  | 依从性   |
|------|-------|-------|-------|
| 信息熵  | 0.664 | 0.930 | 0.823 |
| 客观权重 | 0.576 | 0.120 | 0.304 |

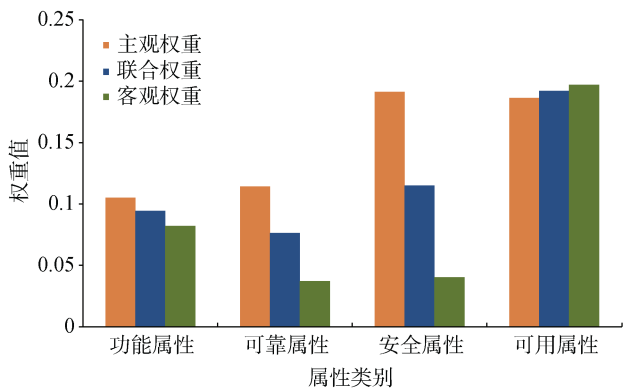


图 4 安全虚拟网络功能(防火墙类)部分可信属性指标权重比

Figure 4 Weight Distribution of Selected Trustworthy Attributes for SVNf (Firewall)

### 5.3 构建 SVNf 评级决策

下面通过评估指标计算方法构建 SVNf 评级决策。

Step 1: 计算可信值。以时效属性为例, 第一步对表 8 的数据进行转换, 首先依据式(4)进行去模糊化处理, 之后利用式(9)对指标数据进行效用转化, 得到 SVNf 时效属性指标的可信值如表 11, 采用相同方法获得所有可信属性的指标可信值。

表 11 SVNf(防火墙类)时效属性可信值  
Table 11 Trustworthiness Values of Temporal Attributes for SVNf (Firewall)

| 实例   | 时效属性  |       |       |
|------|-------|-------|-------|
|      | 时间特征  | 资源特征  | 依从性   |
| 商业 1 | 1     | 0.712 | 0.237 |
| 商业 2 | 0.892 | 0     | 0.662 |
| 商业 3 | 0     | 1     | 1     |
| 开源 1 | 0.986 | 0.429 | 0     |
| 开源 2 | 0.988 | 0.897 | 0.678 |

Step 2: 构建评级决策矩阵。依据指标权重和所有可信属性的指标可信值, 利用式(10)计算得到各防火墙可信属性的可信值如表 12 所示, 之后依据专家对 7 类可信属性之间的重要性打分, 重复主观权重计算步骤, 得到可信属性主观权重值, 依据表 11 重复客观属性计算步骤得到可信属性客观权重值, 通过式(8)组合赋权法计算联合权重为(0.096, 0.180, 0.133, 0.127, 0.241, 0.093, 0.130)。最后依据式(11), 计算得到防火墙评估决策矩阵表 13。

表 12 SVNf(防火墙类)各可信属性可信值  
Table 12 Trustworthiness Values of Trustworthy Attributes for SVNf (Firewall)

| 实例   | 可信属性  |       |       |       |       |       |       |
|------|-------|-------|-------|-------|-------|-------|-------|
|      | 功能属性  | 可靠属性  | 安全属性  | 时效属性  | 可维护属性 | 可生存属性 | 可用属性  |
| 商业 1 | 1     | 0.973 | 1     | 0.793 | 0.834 | 0.109 | 1     |
| 商业 2 | 0.903 | 0.611 | 0.972 | 0.627 | 0.460 | 1     | 0.855 |
| 商业 3 | 0.855 | 0.745 | 0.077 | 0.448 | 0.294 | 1     | 0.618 |
| 开源 1 | 0.171 | 0.331 | 0.844 | 0.688 | 0     | 0.109 | 0.484 |
| 开源 2 | 0.604 | 0.069 | 0.292 | 0.910 | 0     | 0.109 | 0     |

表 13 SVNf(防火墙类)可信评级决策矩阵  
Table 13 Decision Matrix for Trustworthiness Evaluations of SVNf (Firewall)

| 实例   | 可信属性  |       |       |       |       |       |       |
|------|-------|-------|-------|-------|-------|-------|-------|
|      | 功能属性  | 可靠属性  | 安全属性  | 时效属性  | 可维护属性 | 可生存属性 | 可用属性  |
| 商业 1 | 0.093 | 0.163 | 0.140 | 0.100 | 0.167 | 0.017 | 0.112 |
| 商业 2 | 0.083 | 0.103 | 0.136 | 0.079 | 0.922 | 0.160 | 0.096 |
| 商业 3 | 0.079 | 0.125 | 0.011 | 0.057 | 0.058 | 0.160 | 0.070 |
| 开源 1 | 0.016 | 0.056 | 0.118 | 0.087 | 0     | 0.017 | 0.054 |
| 开源 2 | 0.056 | 0.012 | 0.041 | 0.115 | 0     | 0.017 | 0     |

Step 3: 计算 SVNf 评级决策指标。根据 3.4 节的评级指标计算方法, 计算各防火墙实例的相对近似度, 本次评级针对无具体需求方式, 采用式(12)计算理想参考向量。最终通过式(13)与表 4 得到防火墙评级结果如表 14 所示。

表 14 SVNf(防火墙类)可信评级  
Table 14 Trustworthiness Evaluations for SVNf (Firewall Category)

| 指标    | SVNf(防火墙类) |       |       |       |       |
|-------|------------|-------|-------|-------|-------|
|       | 商业 1       | 商业 2  | 商业 3  | 开源 1  | 开源 2  |
| 相对近似度 | 0.111      | 0.144 | 0.201 | 0.434 | 0.676 |
| 等级    | 极好         | 极好    | 优秀    | 良好    | 一般    |

从表 14 的分析结果可以看出, SVNf 防火墙实例的可信值评估排名为: C, Q, H, PFSense, IPfire。通过综合分析<sup>[51-52]</sup>, 在商用防火墙领域中, C 作为全球数通与网络安全头部企业, 其商用防火墙的安全功能、

性能、可靠性等方面均有突出的优点, 相比其他产品具有较好的优势; 作为网络安全中坚企业, Q 和 H 的产品各有优势, Q 提供的安全功能较为丰富且安全性和时效性较好, 而 H 的可靠性、可生存性较高, 同时 Q 的市场份额大于 H, 因而综合上 Q 大于 H; 相比之下, PFSense 是一款性能较好的开源防火墙, 具有较多的开箱即用的功能, IPfire 则具备较高的更新频率。同时, 三款商业防火墙的评估结果均大于开源软件。因此, 本文提出的 SVNf 可信评估方法能够从多维度全面地评估 SVNf(防火墙)的可信性, 评估结果与实际相符, 进而可以为 SSFC 组链中的 SVNf 选型提供指导意见。

6 总结

本文针对当前软件定义网络中的服务链实例化问题展开分析, 在软件质量评估模型、软件可信评估模型等已有研究的基础上, 以可信评估为指导思想,

建立并完善了 SVNf 多属性决策模型。在评价过程中, 为了兼顾评估者主观判断的模糊性以及数值数据的客观性融合熵权法和模糊层次分析法的计算模型确定各个可信属性的权重, 模糊层次分析法根据专家的判断确定标准的重要性程度, 熵权法则能充分挖掘出原始数据的有用信息, 避免了权重的主观片面性, 然后采用组合赋权法兼顾主客观度量方式, 提高赋权的公平性。进而通过评估决策对 SVNf 的可信性进行量化, 将指标归一化、决策矩阵构建一并纳入评估决策指标计算中, 使得 SVNf 可信性计算更符合实际网络安全场景, 为服务链的实例化和 SVNf 的选择提供有力的支持。通过典型 SVNf 实例的实验对比分析表明, 本文的方法是一种较为有效 SVNf 可信评估的方法。

尽管本文的案例研究涉及特定的软件产品和行业, 但该评估模型的基本概念和方法可以应用于评估其他 SVNf、软件或者系统, 当评估其他 SVNf 或者软件时, 可能需要根据目标的具体情况而选取相应的可信属性进行评估。同时, 由于本研究以静态标准作为评价的基础, 未来的研究会考虑融合 SVNf 生命周期中的动态因素。

## 参考文献

- [1] Sun P H, Lan J L, Li J F, et al. Combining Deep Reinforcement Learning with Graph Neural Networks for Optimal VNF Placement[J]. *IEEE Communications Letters*, 2021, 25(1): 176-180.
- [2] Doriguzzi-Corin R, Scott-Hayward S, Siracusa D, et al. Application-Centric Provisioning of Virtual Security Network Functions[C]. *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks*, 2017: 276-279.
- [3] Ali A, Anagnostopoulos C, Pezaros D P. In-Network Placement of Security VNFS in Multi-Tenant Data Centers[C]. *2020 IEEE Symposium on Computers and Communications*, 2020: 1-6.
- [4] Liu W M, Qiu X F, Chen P C, et al. SDN Oriented Software-Defined Security Architecture[J]. *Journal of Frontiers of Computer Science and Technology*, 2015, 9(1): 63-70.  
(刘文懋, 裴晓峰, 陈鹏程, 等. 面向 SDN 环境的软件定义安全架构[J]. *计算机科学与探索*, 2015, 9(1): 63-70.)
- [5] Li Z Y, Wang X W, Yi B, et al. Network Service Conflict Detection and Avoidance Mechanism Based on VNF[J]. *Chinese Journal of Computers*, 2023, 46(2): 385-399.  
(李政宇, 王兴伟, 易波, 等. 基于 VNF 的网络服务冲突检测与避免机制[J]. *计算机学报*, 2023, 46(2): 385-399.)
- [6] Xie A, Huang H W, Wang X L, et al. Online VNF Chain Deployment on Resource-Limited Edges by Exploiting Peer Edge Devices[J]. *Computer Networks*, 2020, 170: 107069.
- [7] Sun J, Liu F, Wang H D, et al. Joint VNF Placement, CPU Allocation, and Flow Routing for Traffic Changes[J]. *IEEE Internet of Things Journal*, 2023, 10(2): 1208-1222.
- [8] Abbas K, Yoo J H, Hong J W. Adaptive Ensemble Learning-Based Network Resource Workload Prediction for VNF Lifecycle Management[C]. *2022 23rd Asia-Pacific Network Operations and Management Symposium*, 2022: 1-4.
- [9] Basu D, Jain A, Ghosh U, et al. QoS-Aware Dynamic Network Slicing and VNF Embedding in Softwarized 5G Networks[C]. *2022 National Conference on Communications*, 2022: 100-105.
- [10] Iwamoto M, Suzuki A, Kobayashi M. Optimal VNF Scheduling for Minimizing Duration of QoS Degradation[C]. *2023 IEEE 20th Consumer Communications & Networking Conference*, 2023: 855-858.
- [11] Wu Y Y, Zheng W C, Zhang Y B, et al. Reliability-Aware VNF Placement Using a Probability-Based Approach[J]. *IEEE Transactions on Network and Service Management*, 2021, 18(3): 2478-2491.
- [12] Huang M T, Liang W F, Shen X J, et al. Reliability-Aware Virtualized Network Function Services Provisioning in Mobile Edge Computing[J]. *IEEE Transactions on Mobile Computing*, 2020, 19(11): 2699-2713.
- [13] Mao W X, Wang L, Zhao J, et al. Online Fault-Tolerant VNF Chain Placement: A Deep Reinforcement Learning Approach[C]. *2020 IFIP Networking Conference*, 2020: 163-171.
- [14] Souza R, Santos M, Bonfim M, et al. KDN-Based Fault-Tolerant Scheduling for VNFS in Data Centers[J]. *IEEE Transactions on Network and Service Management*, 2022, 19(4): 4905-4917.
- [15] Yang B X, Xu Z C, Chai W K, et al. Algorithms for Fault-Tolerant Placement of Stateful Virtualized Network Functions[C]. *2018 IEEE International Conference on Communications*, 2018: 1-7.
- [16] Qu L, Khabbaz M, Assi C. Reliability-Aware Service Chaining in Carrier-Grade Softwarized Networks[J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(3): 558-573.
- [17] Yu X J, Xiao R. Credibility Verification Method and Calculation Based on Application Behavior Declaration[J]. *Computer Systems & Applications*, 2018, 27(11): 17-26.  
(于学军, 肖然. 基于行为声明的可信性测试方法与可信度计算研究[J]. *计算机系统应用*, 2018, 27(11): 17-26.)
- [18] Xiong G, Lan J L, Hu Y X, et al. Evaluation Approach for Network Components Performance Using Trustworthiness Measurement[J]. *Journal on Communications*, 2016, 37(3): 117-128.  
(熊钢, 兰巨龙, 胡宇翔, 等. 基于可信度量的网络组件性能评估方法[J]. *通信学报*, 2016, 37(3): 117-128.)
- [19] Shi L, Yang S L, Li K, et al. Developing an Evaluation Approach for Software Trustworthiness Using Combination Weights and TOPSIS[J]. *Journal of Software*, 2012, 7(3): 532-543.
- [20] Lang B, Liu X D, Wang H M, et al. A Classification Model for Software Trustworthiness[J]. *Journal of Frontiers of Computer Science & Technology*, 2010, 4(3): 231-239.  
(郎波, 刘旭东, 王怀民, 等. 一种软件可信分级模型[J]. *计算机科学与探索*, 2010, 4(3): 231-239.)
- [21] Yu X J, Gao C. Research on Software Trustworthiness Measurement Model Based on Mobile Terminal[J]. *Computer and Information Technology*, 2014, 22(4): 1-3.  
(于学军, 高潮. 移动终端软件可信性度量模型研究[J]. *电脑与信息技术*, 2014, 22(4): 1-3.)

- [22] Zhao Y J, Luo X X. Fuzzy Evaluation Method for Web Software Trustworthiness[J]. *Application Research of Computers*, 2014, 31(4): 1072-1076.  
(赵玉洁, 罗新星. Web 软件可信性的模糊评价方法[J]. *计算机应用研究*, 2014, 31(4): 1072-1076.)
- [23] Do T V, Do V T, Jacot N, et al. MITRE ATT and CK Threat Modelling Extensions for Mobile Threats[C]. *Mobile Web and Intelligent Information Systems*, 2023: 252-263.
- [24] Yin A S, Huang H P. Trusted Network Evaluation Model Based on Comprehensive Trust[J]. *Chinese Journal of Electronics*, 2021, 30(6): 1178-1188.
- [25] Jung J J. Trustworthy Knowledge Diffusion Model Based on Risk Discovery on Peer-to-Peer Networks[J]. *Expert Systems with Applications*, 2009, 36(3): 7123-7128.
- [26] Wu D P, Zhang F, Wang H G, et al. Security-Oriented Opportunistic Data Forwarding in Mobile Social Networks[J]. *Future Generation Computer Systems*, 2018, 87: 803-815.
- [27] Zhang Y H. Research on Trustworthiness Evaluation Based on Web Service Composition[C]. *2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms*, 2022: 1233-1239.
- [28] Liu Y, Tyszbrowicz S, Liu Z M, et al. ITrustEval: A Framework for Software Trustworthiness Evaluation with an Intelligent AHP-Based Method[C]. *2022 IEEE International Conference on Systems, Man, and Cybernetics*, 2022: 1778-1785.
- [29] Zhou W, Ma Y F, Pan H Y. A Novel Trustworthiness Measurement Model Based on Weight and User Feedback[J]. *Chinese Journal of Electronics*, 2022, 31(4): 612-625.
- [30] Tamim I, Jammal M, Hawilo H, et al. Introducing Virtual Security Functions into Latency-Aware Placement for NFV Applications[C]. *ICC 2020 - 2020 IEEE International Conference on Communications*, 2020: 1-7.
- [31] Doriguzzi-Corin R, Scott-Hayward S, Siracusa D, et al. Dynamic and Application-Aware Provisioning of Chained Virtual Security Network Functions[J]. *IEEE Transactions on Network and Service Management*, 2020, 17(1): 294-307.
- [32] Wu H J, Zhang Y, Yang H R, et al. Virtualized Security Function Placement for Security Service Chaining in Cloud[C]. *2018 IEEE 24th International Conference on Parallel and Distributed Systems*, 2019: 628-637.
- [33] Shen G H, Huang Z Q, Xie B, et al. Survey on Software Trustworthiness Evaluation: Standards, Models and Tools[J]. *Journal of Software*, 2016, 27(4): 955-968.  
(沈国华, 黄志球, 谢冰, 等. 软件可信评估研究综述: 标准、模型与工具[J]. *软件学报*, 2016, 27(4): 955-968.)
- [34] Lin C, Hu J, Li G L, et al. A Review on the Architecture of Software Defined Network[J]. *Chinese Journal of Electronics*, 2018, 27(6): 1111-1117.
- [35] Neumann P G. Trustworthiness and Truthfulness Are Essential[J]. *Communications of the ACM*, 2017, 60(6): 26-28.
- [36] Wang D X, Wang Q. Trustworthiness Evidence Supporting Evaluation of Software Process Trustworthiness[J]. *Journal of Software*, 2018, 29(11): 3412-3434.  
(王德鑫, 王青. 支持软件过程可信评估的可信证据[J]. *软件学报*, 2018, 29(11): 3412-3434.)
- [37] Wei H, Shan C, Hu C Z, et al. Software Defect Prediction via Deep Belief Network[J]. *Chinese Journal of Electronics*, 2019, 28(5): 925-932.
- [38] Tao H W, Chen Y X. A Metric Model for Trustworthiness of Softwares[C]. *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, 2009: 69-72.
- [39] Tao H W, Chen Y X, Wu H Y, et al. A Survey of Software Trustworthiness Measurements[J]. *International Journal of Performance Engineering*, 2019, 15(9): 2364.
- [40] Zhu M X, Luo X X, Chen X H, et al. A Non-Functional Requirements Tradeoff Model in Trustworthy Software[J]. *Information Sciences*, 2012, 191: 61-75.
- [41] Zhou J, Zhang M X. Survey on Trustworthy Software Evaluation[J]. *Application Research of Computers*, 2012, 29(10): 3609-3613.  
(周剑, 张明新. 软件可信评估综述[J]. *计算机应用研究*, 2012, 29(10): 3609-3613.)
- [42] Castañeda Cisneros J, Pomares Hernández S E, Pérez Sansalvador J C, et al. Coordination-Free Multi-Domain NFV Orchestration for Consistent VNF Forwarding Graph Reconfiguration[J]. *IEEE Transactions on Network and Service Management*, 2022, 19(4): 5133-5151.
- [43] Qu H, Wang K, Zhao J H. Priority-Awareness VNF Migration Method Based on Deep Reinforcement Learning[J]. *Computer Networks*, 2022, 208: 108866.
- [44] Irawan Y I, Negara E S. Evaluation of Software Quality Assurance Silampari Smart City of Lubuklinggau Based on ISO/IEC 25010: 2011 Analysis Model[C]. *2022 International Conference on Informatics, Multimedia, Cyber and Information System*, 2023: 154-160.
- [45] Yang Z. The establishment of component quality model and the research of evaluation approach based on the ISO/IEC25010Standard[D]. Kunming: Kunming University of Science and Technology, 2012.  
(杨喆. 基于 ISO/IEC 25010 标准的构件质量模型的建立与评价方法研究[D]. 昆明: 昆明理工大学, 2012.)
- [46] Zadeh L A. Fuzzy Sets[J]. *Information and Control*, 1965, 8(3): 338-353.
- [47] Saaty T L. Decision Making—The Analytic Hierarchy and Network Processes (AHP/ANP)[J]. *Journal of Systems Science and Systems Engineering*, 2004, 13(1): 1-35.
- [48] Han Z G. *Methods and applications of mathematical modeling*[M]. Beijing: Higher Education Press, 2005.  
(韩中庚. 数学建模方法及其应用[M]. 北京: 高等教育出版社, 2005.)
- [49] Jiang W Q, Jiang W Q, Dai Y W. Effect of Defuzzifying Triangular Fuzzy Number on Compromise Solutions in VIKOR[J]. *Operations Research and Management Science*, 2019, 28(10): 77-82.  
(糜万俊, 江文奇, 戴跃伟. 三角模糊数去模糊化对 VIKOR 妥协解的影响研究[J]. *运筹与管理*, 2019, 28(10): 77-82.)
- [50] Chen S H, Wang C C. Representation, Ranking, Distance, and Similarity of Fuzzy Numbers with Step Form Membership Function Using K-Preference Integration Method[C]. *Proceedings Joint 9th*

*IFSA World Congress and 20th NAFIPS International Conference*, 2002: 801-806.

[51] Neupane K, Haddad R, Chen L. Next Generation Firewall for

Network Security: A Survey[C]. *SoutheastCon 2018*, 2018: 1-6.

[52] GARTNER. <https://www.gartner.com/en/documents/3992870>. Nove.2020.



刘浩 于 2008 年在哈尔滨工业大学计算机科学与技术专业获得硕士学位。现在北京大学电子信息专业攻读博士学位, 任奇安信科技集团股份有限公司副总裁, CCF 高级会员、CCF 计算机安全专委会委员。研究领域为云计算与云安全技术。研究兴趣包括云安全、云原生。Email: nanjie-renxjtu@163.com。



王翀 现任奇安信科技集团股份有限公司安全研究员。研究领域为云安全。研究兴趣包括云安全、云原生。Email: wang-chong01@qianxin.com。



田志宏 教授, 博士生导师, CCF 杰出会员, 主要研究领域为网络攻防对抗、APT 检测与溯源、工控安全。Email: tianzhihong@gzhu.edu.cn。



吴中海 北京大学教授, 博导。主要研究领域为云安全与系统安全、数据智能与安全。Email: wuzh@pku.edu.cn。