文章编号:1671-4598(2024)06-0173-07 DOI:10.16526/j.cnki.11-4762/tp.2024.06.026 中图分类号:TN929.5 文献标识码:A

基于SPEA-Ⅱ算法的网络多层次安全访问控制方法

宋岍龙
(中移互联网有限公司,广州 510640)

摘要:当前网络技术迅猛发展,网络安全问题日益突出,尤其是访问控制安全性;为了解决目前网络系统中存在的威胁检测精度和安全访问控制问题,引入SPEA-Ⅱ算法,提出一种新的网络多层次安全访问控制方法;深入分析网络多层次访问控制机制原理,明确安全访问控制目标;结合网络边界区域、传输信道区域及移动终端设备区域,建立边界访问控制目标函数、安全威胁检测目标函数、用户身份认证目标函数,提高网络系统安全威胁检测精度;利用SPEA-Ⅱ算法对联合目标函数进行求解,获取网络多层次安全访问控制机制最佳方案;通过迭代逐渐接近近似最优解集,建立最优安全策略组合,计算攻击流量因子完成网络多层次安全访问控制;实验结果表明,所提方法的网络多层次威胁检测精度为94%,安全评估为0.96;由此证明,所提方法的网络多层次安全访问控制效果较好,具有较强的安全性和适应性,能够为中移互联网领域的网络安全策略提供技术支持。

关键词:SPEA-Ⅱ算法;目标函数;近似最优解集;攻击流量因子

Multi-level Network Security Access Control Method Based on SPEA-Ⅱ Algorithm

SONG Qianlong
(China Mobile Internet Co., Ltd., Guangzhou 510640, China)

Abstract: With the rapid development of current network technology, network security issues are increasingly prominent, especially access control security. In order to solve threat detection accuracy and security access control in current network systems, a new network multi-level security access control method is proposed by introducing the SPEA-II algorithm. This paper deeply analyzes the principle of network multi-level access control mechanism, clarifies the security access control objectives. Combined with the network boundary area, transmission channel area and mobile terminal equipment area, boundary access control objective function, security threat detection objective function and user identity authentication objective function, the security threat detection accuracy of the network system is improved. The SPEA-II algorithm is used to solve the joint objective function, and obtain the best scheme of network multi-level security access control mechanism. The approximate optimal solution set is gradually approached by the iteration, the optimal security policy combination is established, and the attack traffic factor is calculated to complete the multi-level security access control of the network. Experimental results show that the detection accuracy of the proposed method is 94% and the security assessment is 0.96. This proves that the proposed method has good multi-level network security access control effect, it has strong security and adaptability, and can provide technical support for network security strategy in the field of China mobile internet.

Keywords: SPEA-Ⅱ algorithm; objective function; multi-level security access; approximate optimal solution set; attack traffic factor

0 引言

中移互联网作为中国移动旗下的互联网平台,拥有庞大的用户群体和丰富的业务应用。然而,随着互联网的发展,网络安全威胁也呈现出多样化、复杂化的趋势。在传统的网络访问控制方法中,单一的身份验证和授权方式已经无法满足复杂网络环境下的安全需求,容易导致网络遭受攻击和数据泄露等安全事件发生。许多研究者致力于访问控制技术,并提出了优秀的方法。文献[1]采用多项式混合密钥分配技术对网络簇内和簇间节点通信数据进行加密处理,保障网络传输数据的安全性。利用优化粒子群算法构造适值函数对最优簇首和分簇数量进行选择,最大限度地降低节点能量损耗,提升网络系统访问控制安全性。文献[2]在网络系统安全设计基础上,利用人工神经网络模型对网络系统安全态势进行实时监测与评估,并以网络安全态势评估结果为依据对网络安全控制机制进行

收稿日期:2024-01-23; **修回日期**:2024-04-23。
作者简介:宋岍龙(1989-),男,硕士,工程师。
引用格式:宋岍龙.基于SPEA-Ⅱ算法的网络多层次安全访问控制方法[J].计算机测量与控制,2024,32(6):173-179.

实时改进及调整，使网络安全水平满足网络与用户需求。文献［3］应用卷积神经网络模型对网络安全风险进行实时评估，并基于 PID 控制理论与遗传算法制定网络安全控制优化程序，结合攻击数据库（KDD Cup99）对制定程序进行测试，保障制定程序功能的稳定发挥，最大限度地提升网络系统安全性。文献［4］基于区块链的云存储数据访问安全控制算法，利用自适应处理方法提取数据特征量，再通过连续参数识别算法重组特征实现安全访问。文献［5］采用椭圆曲线加密中的简单标量乘法代替双线性配对，实现基于区域链防篡改溯源特性的事务访问控制。文献［6］提出基于动态异构网络的风险访问模型，在跨域云环境下增加了网络灵活性。文献［7］在云计算环境中提出基于属性和信任的 RBAC 模型，实现基于角色的访问控制。文献［8］提出基于 CP-ABE 的命名数据网访问控制方法，引入重加密模块和兴趣包过滤机制，实现细粒度访问控制和权限撤销。上述方法虽然在一定程度上能够提高网络系统访问控制安全性，但这些方法的效率仍然存在一定挑战。

SPEA-Ⅱ算法是一种改进的求解算法，主要用于解决多目标优化问题。SPEA-Ⅱ算法的基本原理是通过模拟自然界的进化过程，采用遗传算法搜索问题最优解。SPEA-Ⅱ算法能够同时考虑多个冲突的目标函数，通过维护一个外部存档存储非支配解集，并使用精英选择机制和拥挤度计算选择母体。在每一代中，通过对非支配解集进行更新和维护，逐渐收敛到一组近似最优解。此外，SPEA-Ⅱ算法还采用了“K-近邻”算法的基本思想，保证了种群多样性的维持，进一步提高了算法的搜索效率。为此，提出基于 SPEA-Ⅱ算法的网络多层次安全访问控制方法。在分析网络多层次访问控制机制原理的基础上，利用目标函数分别对网络边界区域、传输信道区域、移动终端设备区域建立边界访问控制、安全威胁检测、用户身份认证。采用 SPEA-Ⅱ算法对网络多层次的联合目标函数进行求解，并通过迭代逐渐接近近似最优解集。在最优安全策略组合下进行时间误差处理，提高网络安全策略执行效率，并获取攻击流量因子数值，完成网络多层次安全访问控制。

1 网络多层次安全访问控制方法

1.1 网络多层次访问控制机制原理

网络访问控制结构较为复杂，其安全控制机制主要针对网络中的边界区域、传输信道区域与移动终端设备区域[9]。其中，在边界区域建立明确的防火墙、逻辑隔离、物理隔离等网络边界，对所有网络行为进行一定访问控制，以此为基础将网络攻击行为阻挡在边界区域；在传输信道区域对网络中的传输内容进行实时监控，与此同时对网络安全威胁进行实时检测，当发现异常行为及时发出预警提示，提醒工作人员对异常响应进行处理；在移动终端设备区域通过身份认证机制对用户身份进行判定，防止攻击者通过终端设备进入网络，与此同时工作人员需对终端设备运行状况进行实时监控，当发现可疑终端设备入侵，需要对其进行及时阻隔，保障移动终端设备稳定运行。具体网络访问控制机制如图 1 所示。

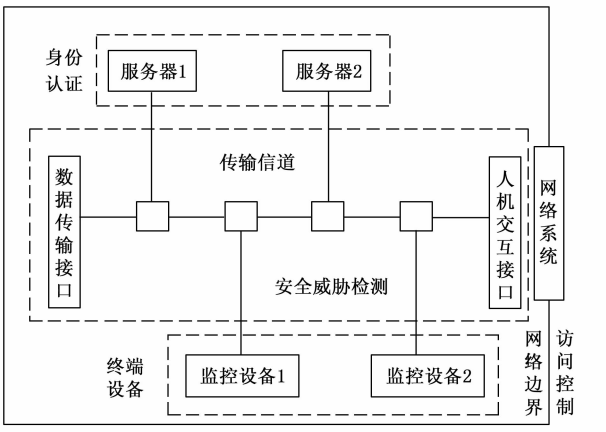

图 1 网络访问控制机制原理图

如图 1 所示，网络访问控制机制实施的关键环节为网络边界精准确定环节。由于移动终端设备应用范围较为广泛，其不仅仅承担着数据传输任务，还需要具备人机交互的功能。因此，将传输信道划分为两类，分别为数据传输接口与人机交互接口，以此最大限度地阻止异常网络行为发生，保障网络安全运行[10-11]。为了方便后续研究，针对不同网络区域，将网络安全控制机制进行合理划分，分别为边界访问控制机制（网络边界区域）、安全威胁检测机制（传输信道区域）与用户身份认证机制（移动终端设备区域）。随着网络系统应用范围不断扩大，用户规模也随之提升，致使其安全问题愈加严重，影响着网络系统的后续发展及其应用，故需要对网络系统安全控制机制进行优化处理，将安全控制机制功效发挥到最大化。

1.2 建立多层次安全访问目标函数

1.2.1 边界访问控制目标函数

边界访问控制机制主要关注网络边界区域的安全性，其目标是防止未经授权的访问和数据泄漏。建立边界访问控制目标函数，通过数学模型量化评估网络边界的安全性能，提高网络边界的安全防护能力，降低外部攻击的风险。从访问控制策略角度出发，制定系统隔离机制（逻辑隔离与物理隔离），以此为基础，基于信息约束理论优化网络访问控制机制建立目标函数，确保只有经过授权的用户或设备网络，防止未经授权访问。系统隔离机制主要依据安全级别的不同，对网络系统访问行为进行控制，即不同安全等级网络不能进行互相访问，最大限度地提升网络边界的安全防护效果。

1）逻辑隔离：逻辑隔离是指网络系统与其他网络的物理状态为连通，但是信息传递状态为断开，即防火墙隔离技术。防火墙隔离技术主要由硬件、软件、控制策略等结构构成，将其设置在网络系统与其他系统安全域之间，通过建立网关安全策略，达到网络系统安全控制目的。包过

滤型防火墙是一种基于数据包过滤技术的防火墙，在应用层、传输层、网络层和接口层中对进出网络的数据包进行筛选和过滤[12-13]。通过检查数据包的源地址、目的地址、端口号等信息，根据访问控制规则对每个进出网络的数据包进行检查，防止未经授权的访问和数据泄漏。同时，通过设置网络隔离规则，将不同的网络区域进行逻辑隔离，有效识别并阻止潜在的恶意数据包和攻击行为。因此，在逻辑隔离中选择包过滤型防火墙工具，其具体工作原理如图 2 所示。

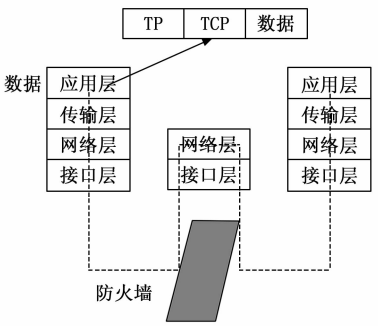

图 2　包过滤型防火墙工作原理示意图

2）物理隔离：物理隔离是一种静态的、被动的防护手段，主要采用物理方式将网络系统从自由、无边、开放的环境中独立出来，以此保障网络系统内部数据不会被破坏和窃取，为网络系统构造安全可靠边界。信任约束理论是一种基于信任关系的网络安全管理理论，通过建立信任关系和信任评估机制，对网络中的实体行为进行管理和控制，从而达到保护网络安全的目的[14]。该理论认为，信任关系是基于实体行为和历史的可靠性和可信度的一种评估，可以为网络安全提供一种可度量、可管理的安全约束机制，确保只有可信的实体能够访问网络系统[15-16]。引进信任约束理论完成物理隔离，其具体工作原理如图 3 所示。

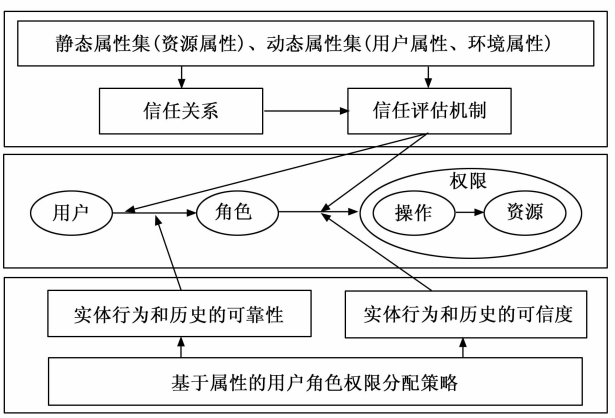

图 3　引入信任约束理论的工作原理示意图

通过上述分析可知，边界访问控制过程中的实体主要包括用户、角色、权限、资源与操作，具体实体与属性定义如表 1 所示。

表 1　实体与属性定义表

实体或属性	定义
用户集	$U=\{u_1,u_2,u_3,\cdots\}$
角色集	$R=\{r_1,r_2,r_3,\cdots\}$
权限集	$P=\{p_1,p_2,p_3,\cdots\}$
资源集	$O=\{o_1,o_2,o_3,\cdots\}$
操作集	$Q=\{q_1,q_2,q_3,\cdots\}$
用户属性集	$Ua=\{ua_1,ua_2,ua_3,\cdots\}$
角色属性集	$Ra=\{ra_1,ra_2,ra_3,\cdots\}$
资源属性集	$Oa=\{oa_1,oa_2,oa_3,\cdots\}$
环境属性集	$Ha=\{ha_1,ha_2,ha_3,\cdots\}$

确定用户分配角色规则 R'_u、角色分配权限规则 P'_r、权限过滤规则 α_u，表达式为：

$$R'_u=\begin{cases}R_u\cup\{u\times r\} & \text{if}\quad(U_a\subset Ua)\\ R_u & \text{else}\end{cases}$$

$$P'_r=\begin{cases}P_r\cup\{r\times p\} & \text{if}\quad(O_a\subset Ra)\\ P_r & \text{else}\end{cases}$$

$$\alpha_u=\frac{f\{U_a\times R_a\}}{f\{H_a\}},\quad\begin{cases}\alpha_u\geqslant\alpha_o & \text{赋予权限}\\ \alpha_u<\alpha_o & \text{撤销权限}\end{cases}\tag{1}$$

式中，R'_u 为最终确定的用户角色，R_u 为当前用户角色，U_a 为角色对应的用户属性集，P'_r 为最终确定的角色权限，P_r 为当前角色权限，O_a 为资源对应的角色属性集，α_u 为用户网络行为的信任等级，$f\{\cdot\}$ 为数值转换函数，方便信任等级的计算，α_o 为需求资源信任等级的约束阈值，需要根据用户需求资源的实际情况进行具体的设置。

以用户分配角色、角色分配权限与权限过滤正确性最大化作为访问控制目标，建立目标函数，其表达式为：

$$max\zeta_1=\frac{\beta(R'_u)+\beta(P'_r)+\beta(P[\alpha_u])}{\chi^{\wedge}\times I_o}\tag{2}$$

式中，$\beta(\cdot)$ 为正确性数值，$P[\alpha_u]$ 为权限过滤结果，$\chi^{\wedge}$ 为网络访问控制机制优化辅助参数，取值范围为 0～1，I_o 为正确性数值标准化处理因子。

1.2.2　安全威胁检测目标函数

安全威胁检测机制关注传输信道区域的安全性，其目标是及时发现和应对各种网络威胁。通过建立目标函数对传输信道区域进行威胁检测和阻断，提高威胁检测的准确性，为后续安全响应提供及时可靠的支持。安全威胁检测机制主要划分为网络安全威胁检测特征提取阶段与网络安全威胁检测阶段，常规情况下，网络系统受到的安全威胁较多，例如攻击者攻击、病毒侵入等，其会窃取网络信息，篡改网络程序等，降低网络系统与传输数据的安全性。通过网络安全威胁检测特征提取，及时发现恶意代码和漏洞等攻击行为，具体提取程序如图 4 所示。

由于网络安全威胁检测数据较多，对提取的网络安全威胁检测特征进行编码能够优化网络安全控制机制运算量，具体如表 2 所示。

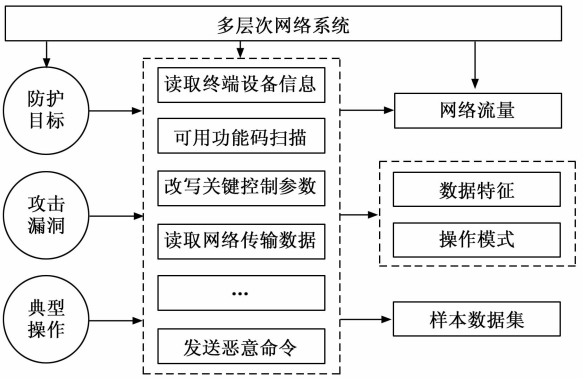

图 4 网络安全威胁特征提取程序图

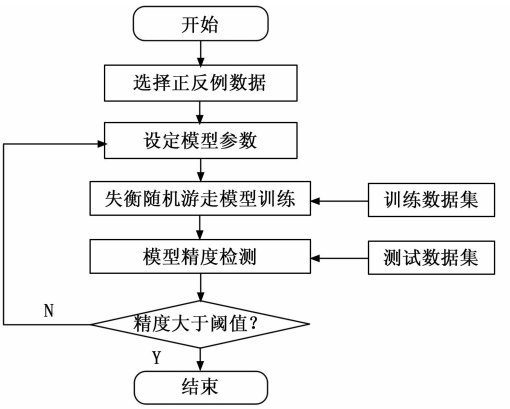

图 5 网络安全威胁检测程序图

表 2 网络安全威胁检测特征编码表

特征描述	特征编码	功能
源 IP 地址	x_1	网络通信方向标识
目的 IP 地址	x_2	网络通信方向标识
IP 包头部长度	x_3	IP 包头部长度检测
源端口	x_4	合法服务端口检测
目的端口	x_5	合法服务端口检测
功能码	x_6	执行功能揭示
协议标识符	x_7	通讯协议标识
长度	x_8	报文长度检测
数据地址	x_9	请求操作寄存器揭示
数据量	x_{10}	读写数据信息
事务处理标识符	x_{11}	响应事务或标识请求
单元标识符	x_{12}	网络通信传输标识

将表 2 中的网络安全威胁检测特征进行整合，记为 $X=\{x_1,x_2,\cdots,x_{12}\}$。失衡随机游走模型能够模拟网络中非均衡、动态的行为。在失衡随机游走模型中，移动节点可以朝不同的方向移动，并且每个方向的移动概率不同，以此反映网络中的非均衡特性。同时，移动节点在每个位置的停留时间和移动距离也是随机的，以此模拟网络中的动态行为[17-18]。由于失衡随机游走模型考虑了网络中的非均衡和动态特性，因此能够更好地识别出异常行为，并及时发现潜在的网络安全威胁，完成网络安全威胁检测，具体如图 5 所示。

如图 5 所示，网络安全威胁检测机制实质上为二分类模型，即将网络数据划分为异常数据与正常数据，产生异常数据说明网络安全威胁存在，需要工作人员及时处理，保障网络信息安全与完整。

当数据集中只有一小部分数据受到关注，致使某类样本数量显著少于其他类别样本，即为数据集失衡。因此，在网络安全威胁检测过程中，将失衡数据集与失衡随机游走模型融合，建立网络安全威胁检测目标函数，其表达式为：

$$max\zeta_2=\frac{N_c(x_i)}{N_{\text{total}}(x_i)}\times 100\% \tag{3}$$

式中，$N_c(x_i)$ 为网络数据分类正确数量，即网络安全威胁正确检测数量；$N_{\text{total}}(x_i)$ 为网络数据总数量，即网络安全运行全部数据。

1.2.3 用户身份认证目标函数

用户身份认证机制关注移动终端设备区域的安全性，其目标是保证用户身份的真实性和合法性。当前网络系统安全控制主要采用单一的身份认证技术，例如数字签名、口令认证、数字凭证、认证等，其虽然能够基本实现网络用户身份认证的功能，但是整体认证效率、精度较差，容易遭到攻击者入侵，影响网络系统整体安全性。为了有效防止非法用户访问网络资源，提高网络安全性，减少非法访问和网络攻击的风险，将网络用户身份认证机制优化为双层认证结构，使用融合口令认证和数字签名的方式，形成一种更为复杂和可靠的认证机制。利用数字签名的安全性和不可伪造性，确保用户身份验证过程的准确性和安全性，防止非法用户冒充他人身份[19]。利用口令认证的简单性和易用性，提高身份认证的速度和效率，减少用户等待时间，提升用户体验[20]。通过双重验证机制增强网络用户身份安全性，即使其中一种认证方式被攻破，攻击者也需要同时攻破另一种认证方式才能获得合法身份。

1）口令认证。口令认证是日常生活中比较常见的认证方式之一，需要用户在第一次登录移动终端设备时设定，通常以字母＋数字的形式为主。当用户再次登录终端设备时，直接输入设定好的口令，若与移动终端设备记录口令一致，则允许用户登录；若与移动终端设备记录口令不一致，则不允许用户登录。依据上述描述内容，制定口令认证规则：

$$\begin{cases}\delta_{\text{input}}=\delta_{\text{record}} & \text{允许登录}\\ \delta_{\text{input}}\neq\delta_{\text{record}} & \text{禁止登录}\end{cases} \tag{4}$$

式中，δ_{input}为用户输入口令，δ_{record}为终端设备记录的用户设定口令。

需要注意的是，口令认证方式虽然简单方便，但也存在着一定的安全风险，尤其是口令泄露风险，故应该在该技术中添加加密技术，最大限度地保障口令认证精准性。

2）数字签名。采用数字签名认证技术，进一步强化用户身份验证的安全性。使用字母代替纸上签名，并承担着签字与盖章的作用，对用户私密信息进行高级保护，防止私密信息被篡改或者窃取。需要注意的是，数字签名与口令认证具有相同特点，即唯一性。每一个网络用户有且仅有一个数字签名，表现形式为 RSA 签名、DSS 签名、HASH 签名等，以网络用户身份认证准确性最大化作为用户身份认证目标，建立用户身份认证目标函数，其表达式为：

$$max\zeta_3 = \frac{\delta_{\text{input}} M_c(u)}{M_{\text{total}}(u)} \times 100\% \tag{5}$$

式中，$M_c(u)$ 为用户身份认证准确数量；$M_{\text{total}}(u)$ 为终端设备登录用户的总数量。

1.3　基于 SPEA-Ⅱ算法的访问控制

SPEA-Ⅱ算法是一种经典的多目标优化算法，用于解决具有多个冲突目标的优化问题。基于遗传算法并融合了“K-近邻”算法策略思想，在多目标优化问题中找到一组最优或近似最优解[21-22]。SPEA-Ⅱ算法可以处理多目标优化问题，同时考虑到不同的安全目标和限制条件，例如访问权限、数据保密和完整性等。在网络多层次安全访问控制过程中，利用 SPEA-Ⅱ算法对目标函数进行求解，找到一组最优的安全策略组合，通过执行安全策略提高网络的整体安全性，实现多层次安全访问控制。SPEA-Ⅱ算法具有高效性、多样性和自适应性。SPEA-Ⅱ算法采用外部存档结构存储非支配解集，避免了对整个种群进行排序的开销，减少了算法的计算复杂度。通过拥挤度计算和外部存档的操作，能够在解空间中保持较好的多样性，并找到一组近似最优解。同时，SPEA-Ⅱ算法通过自适应参数设定和进化操作适应不同目标函数特征，提高算法的搜索能力。SPEA-Ⅱ算法原理如图 6 所示。

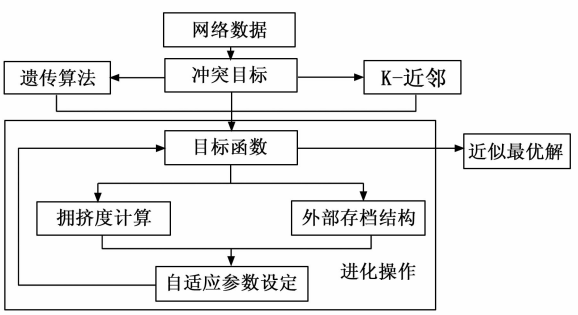

图 6　SPEA-Ⅱ算法原理示意图

1.3.1　基于 SPEA-Ⅱ算法的联合目标函数求解

在多层次安全访问控制中，以边界访问控制目标函数、安全威胁检测目标函数和用户身份认证目标函数作为基础，联合确定最终安全控制机制优化函数。利用 SPEA-Ⅱ算法对联合目标函数进行求解，获得安全控制机制优化最佳方案，实现多层次安全访问控制。网络多层次安全访问的联合目标函数表达式为：

$$\zeta = max\zeta_1 + max\zeta_2 + max\zeta_3 \tag{6}$$

由式（6）可知，联合目标函数是一个多目标优化问题。利用 SPEA-Ⅱ算法对联合目标函数进行求解，提高网络的整体安全性、降低安全风险、优化资源利用。基于 SPEA-Ⅱ算法的联合目标函数求解过程为：

步骤 1：通过遗传算法的方式生成初始种群 K_0，获取网络多层次安全访问机制全部方案。初始化外部存档结构，利用外部存档结构维护非支配解集，设置归档集合为 L_0。

步骤 2：通过选择、交叉和变异操作生成子代，并计算子代个体的适应度值，表达式为：

$$\Gamma = \frac{\zeta}{3 \times \upsilon^0} \tag{7}$$

式中，Γ 为适应度函数，υ^0 为适应度计算辅助参数，取值范围为 0～1。

步骤 3：对于外部存档中的每个解，其拥挤度是其支配解集合大小的倒数。即，如果一个解被更多的解支配，其拥挤度值更小。为了更好地维护外部存档的多样性，需要对非支配解按照拥挤度进行排序，并优先选择拥挤度较高的解进入外部存档，以维护外部存档的多样性，表达式为：

$$L = \frac{\sigma E_j}{\zeta \sum_{j=1}^{N} R_j} \tag{8}$$

式中，σ 为解的聚集程度，E_j 为第 j 个决策的变量值，N 为决策变量总数，R_j 为第 j 个决策的离散度。

步骤 4：通过精英选择和非支配排序获取集合 K_t 与 L_t 中全部非支配个体，将其存储至 L_{t+1} 中。若 L_{t+1} 绝对值大于阈值 L^*，则利用修剪方式对个体进行删减处理，直至 L_{t+1} 绝对值等于阈值 L^* 为止；若 L_{t+1} 绝对值小于阈值 L^*，则从 K_t 与 L_t 中随机选取多个支配个体保存至 L_{t+1} 中，直至 L_{t+1} 绝对值等于阈值 L^* 为止。

步骤 5：对归档集合 L_{t+1} 中全部个体进行降序排列后，设定终止条件为：当第 t 次迭代大于或者等于最大迭代 T 时，终止算法，按照顺序输出 L_{t+1} 中全部非支配个体，排在第一位的个体为最优个体。根据预设的终止条件，判断是否终止算法；如果不满足终止条件，则返回步骤 2。

1.3.2　结合最优安全策略组合的访问控制

通过 SPEA-Ⅱ算法的目标函数求解迭代逐渐接近近似最优解集，结合外部存档中的非支配解，将最优解集设定为安全策略组合：

$$P_i = \begin{cases} \zeta \sum_{I_i \in G}^{N} (I_i(t)) \\ 0, \text{otherwise} \end{cases} \tag{9}$$

式中，I_i 和 $I_i(t)$ 分别表示一组近似最优解集和 I_i 于第 t 次迭代过程中被选中的最优个体，G 为所有非支配解。

根据最优安全策略组合确定边界访问控制、安全威胁检测和用户身份认证的网络多层次安全访问优先级，并对时间误差进行处理，提高网络安全策略执行效率：

$$r_i = P_i \varphi \tag{10}$$

式中，φ 为最优个体节点的步长参数。

攻击流量因子 τ 是网络多层次安全访问控制的依据，当 $\tau \geqslant 0.1$ 时，表明网络实际运行过程中存在异常情况。因此结合网络运行实际状态，计算攻击流量因子：

$$\tau = 1 - \frac{a(t+1)r_i}{\varepsilon} \tag{11}$$

式中，a 表示流量阈值，ε 表示网络流量数据。通过判断 τ 数值，完成边界访问控制、安全威胁检测和用户身份认证的多层次安全访问控制，限制非法访问和恶意攻击，保证网络边界安全。至此，完成了基于 SPEA-Ⅱ算法的网络多层次安全访问控制方法的设计，可以有效提高网络的整体安全性、提高系统的运行效率，并降低系统遭受攻击和威胁的风险，避免由于未经授权的访问、恶意攻击或异常行为造成的数据泄露、服务中断等安全问题。

2 实验与结果分析

选取基于粒子群优化算法的无线传感网络安全分簇策略、基于大数据技术的农机调度系统网络安全优化与基于卷积神经网络的无线网络安全风险评估及控制作为对比方法 1、对比方法 2 与对比方法 3，联合所提方法共同进行网络多层次安全访问控制对比实验，以此验证所提方法的优化性能。

2.1 实验工况设置

为了提升实验结论的精准性，设置 10 种工况，具体如表 3 所示。

表 3 实验工况设置表

实验工况	用户数量/个	安全威胁数据量/MB	异常行为数量/次
1	10 245	236	54
2	20 154	321	56
3	15 247	451	59
4	13 256	120	60
5	14 250	210	21
6	16 987	248	30
7	24 156	145	24
8	20 132	169	51
9	20 159	257	67
10	21 547	236	70

如表 3 所示，设置的实验工况用户数量、安全威胁数据量与异常行为次数均不一致，表明每种实验工况对应的背景环境差异性较大，符合网络多层次安全访问控制性能的测试需求。

2.2 网络系统安全评估模型构建

依据网络系统实际运行情况，选取网络系统安全评估指标，主要包括攻击者数量、病毒攻击次数、人为误操作次数、硬件损坏程度、软件程序损坏程度等，将其记为 $Y = \{y_1, y_2, \cdots, y_n\}$，$n$ 表示的是安全评估指标的总数量。由于每个安全评估指标对于最终结果的影响程度是不同的，故应用层次分析法对每个安全评估指标权重进行计算与确定，将其记为 $W = \{\omega_1, \omega_2, \cdots, \omega_n\}$，以此为基础，确定网络系统安全评估模型，其表达式为：

$$S = \sum_{n=1} \omega_n \times y_n \tag{12}$$

式中，S 表示网络系统安全评估结果，取值范围为 0～1，S 数值越大，表明网络系统安全性越高；反之，S 数值越小，表明网络系统安全性越低。

2.3 实验结果分析

2.3.1 网络安全威胁检测性能分析

通过精确率指标计算网络安全威胁检测精准度，具体结果如图 7 所示。

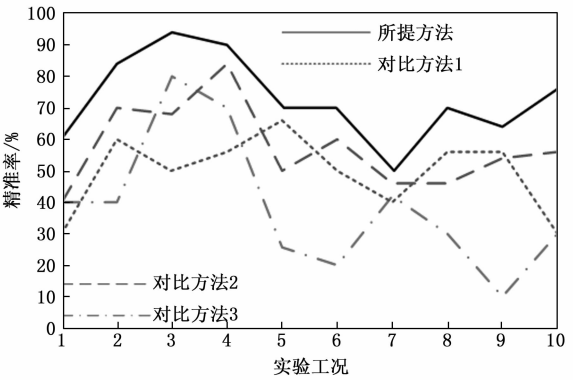

图 7 网络安全威胁检测精度示意图

如图 7 所示，应用所提方法获得的网络安全威胁检测精度范围为 50%～94%，应用对比方法 1 获得的网络安全威胁检测精度范围为 30%～66%，应用对比方法 2 获得的网络安全威胁检测精度范围为 40%～84%，应用对比方法 3 获得的网络安全威胁检测精度范围为 10%～80%。在不同实验工况背景下，通过数据比较可知，所提方法应用后获得的网络安全威胁检测精度均大于对比方法 1、对比方法 2 与对比方法 3，表明其网络安全威胁检测性能更佳。这是因为所提方法在网络边界、传输信道和移动终端设备等多个层次上建立目标函数，更全面地覆盖网络安全的不同方面，进而提高对各种安全威胁的检测精度，减少漏报和误报的情况。并且通过将多个目标函数整合到一个统一框架中，可以更好地协调和优化各种安全策略，有助于集中资源，提高检测算法的效率和精度，从而更好地应对不断变化的安全威胁。

2.3.2 网络安全控制效果分析

应用 2.2 节所示模型获取网络系统安全评估结果，具体如图 8 所示。

如图 8 所示，应用所提方法获得的网络系统安全评估结果范围为 0.5～0.96，应用对比方法 1 获得的多层次网络系统安全评估结果范围为 0.3～0.72，应用对比方法 2 获得的多层次网络系统安全评估结果范围为 0.2～0.74，应用对比方法 3 获得的多层次网络系统安全评估结果范围为 0.26～0.6。在不同实验工况背景下，通过数据比较可知，提出方法应用后获得的多层次网络系统安全评估结果均大于对

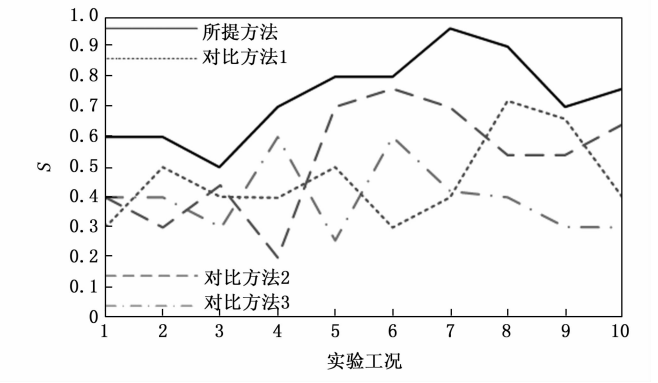

图 8　多层次网络系统安全评估结果

比方法 1、对比方法 2 与对比方法 3，表明其安全控制效果更好。这是因为所提方法采用 SPEA-Ⅱ算法对联合目标函数进行求解，通过迭代优化和外部存档结构的维护逐渐接近近似最优解集，并且在多层次目标之间进行权衡和优化，找到最佳的安全策略组合，从而提高了安全评估结果。

3　结束语

在当今网络技术飞速发展的时代，网络安全问题已成为一个不可忽视的重要问题。访问控制作为网络安全的重要组成部分，其安全性直接关系到网络的整体稳定性和数据的机密性。在这样的背景下，本研究针对网络系统中存在的威胁检测精度和安全访问控制效率等问题，引入 SPEA-Ⅱ算法，并提出了一种基于该算法的网络多层次安全访问控制方法。通过对网络多层次访问控制机制原理的深入分析和明确各个层次安全访问控制目标，建立边界访问控制目标函数、安全威胁检测目标函数和用户身份认证目标函数，有效提高安全访问控制的效率。采用 SPEA-Ⅱ算法对联合目标函数进行求解，并逐步接近近似最优解集，得到适用于网络多层次安全访问控制的最佳安全策略组合。同时，通过计算攻击流量因子完成对网络多层次安全访问控制的实施。实验结果表明，所提方法在网络多层次威胁检测精度达到 94%，安全评估达到 0.96，由此证明该方法在网络安全领域具有较好的可行性和实用性。在未来的研究中，为了应对快速变化的安全威胁并加强对未知恶意行为的识别和防控能力，将在本研究基础上结合机器学习和人工智能技术，通过训练模型和算法提高对未知恶意行为的识别能力，并自动识别和分类安全威胁，进一步保护网络系统安全，为构建安全可靠的中移互联网环境奠定坚实基础。

参考文献：

[1] 蒋建峰，孙金霞，尤澜涛. 基于粒子群优化算法的无线传感网络安全分簇策略 [J]. 计算机科学，2021，48 (s2)：452 - 455.

[2] 曹　斌. 基于大数据技术的农机调度系统网络安全优化 [J]. 农机化研究，2023，45 (4)：216 - 220.

[3] 颜　蔚. 基于卷积神经网络的无线网络安全风险评估及控制 [J]. 沈阳工业大学学报，2022，44 (5)：565 - 569.

[4] 王永刚. 基于区块链的云存储数据访问安全控制算法 [J]. 河北北方学院学报 (自然科学版)，2021，37 (11)：7 - 12.

[5] 董江涛，闫沛文，杜瑞忠. 雾计算中基于无配对 CP-ABE 可验证的访问控制方案 [J]. 通信学报，2021，42 (8)：139 - 150.

[6] 文　静，袁家斌，王诗璇，等. 跨域云环境下基于动态异构网络的风险访问模型 [J]. 河海大学学报 (自然科学版)，2020，48 (3)：284 - 290.

[7] 余　波，台宪青，马治杰. 云计算环境下基于属性和信任的 RBAC 模型研究 [J]. 计算机工程与应用，2020，56 (9)：84 - 92.

[8] 吴志军，许恩中. 命名数据网中基于 CP-ABE 的访问控制方法 [J]. 中国民航大学学报，2020，38 (2)：18 - 23.

[9] 王立春，顾娜娜，信建佳，等. RGB-D 双模态信息互补的语义分割网络 [J]. 计算机辅助设计与图形学学报，2023，35 (10)：1489 - 1499.

[10] 宁晓燕，王　影，孙志国，等. 多音干扰下 Nakagami-m 信道传输 Link16 数据链的性能分析 [J]. 系统工程与电子技术，2023，45 (2)：566 - 571.

[11] 相富钟，赵庆海. 基于 LSTM 模型的光通信网络数据传输负载预测方法 [J]. 激光杂志，2023，44 (2)：154 - 158.

[12] 李红映，张晓曼，张天荣. 基于信任机制的网络防火墙状态检测模型 [J]. 计算机仿真，2022，39 (4)：428 - 432.

[13] 陈传波，刘清慧，黄　刚. 基于 FreeBSD 的包过滤防火墙研究与开发 [J]. 计算机工程与科学，2006，28 (11)：1 - 3.

[14] 刘议聪，楚俊峰，王燕燕. 基于信任关系的 TODIM 群体多属性决策方法 [J]. 计算机工程与应用，2022，58 (3)：187 - 194.

[15] 韦　磊，徐江涛，郭雅娟，等. 基于信任机制的电力无线传感网络安全簇头选举算法 [J]. 中国电力，2023，56 (8)：61 - 67.

[16] 梁　花，李　洋，雷　娟，等. 基于模糊证据理论的物联网节点评估方法研究 [J]. 西南师范大学学报 (自然科学版)，2022，47 (3)：111 - 124.

[17] 腊志垚，钱育蓉，冷洪勇，等. 基于随机游走的图嵌入研究综述 [J]. 计算机工程与应用，2022，58 (13)：1 - 13.

[18] 马秀宝，崔国民，周志强，等. 带有个体淘汰的强制进化随机游走算法优化质量交换网络 [J]. 计算物理，2023，40 (3)：376 - 388.

[19] 杨小东，田　甜，王嘉琪，等. 基于云边协同的无证书多用户多关键字密文检索方案 [J]. 通信学报，2022，43 (5)：144 - 154.

[20] 倪　亮，张亚伟，王念平，等. 可证明安全的后量子两方口令认证密钥协商协议 [J]. 计算机应用研究，2023，40 (4)：1208 - 1213.

[21] 谈恩民，朱　峰，尚玉玲. 基于 SPEA-Ⅱ算法的 SoC 测试多目标优化研究 [J]. 国外电子测量技术，2015，34 (8)：29 - 33.

[22] 刘福英，王晓升. 基于 SPEA2 和 NSGA-Ⅱ算法的并行多目标优化算法 [J]. 信息通信，2016，23 (11)：28 - 30.