可信计算技术在网络信息安全中的应用

曹 宁
(昆明动物园, 昆明 650021)

摘 要: 为了保障网络信息安全性,降低网络信息安全防御时间,提高网络信息安全防御效率,提出可信计算技术在网络信息安全中的应用方法。采用可信计算技术,采集网络信息数据特征,优化网络信息风险类别算法,划分网络信息风险类别并进行安全防御,利用最小二乘法,计算网络信息最优拟合分布测度和风险值,运用信息安全主动防御原理,构建网络信息安全处理模型,保证可信计算技术在网络信息安全中的应用效果。实验结果表明,所提方法的网络信息安全防御效率较高,能够有效保障网络信息安全性,降低网络信息安全防御时间。

关键词: 可信计算技术; 网络信息安全; 最小二乘法; 风险度量
中图分类号: TP393 **文献标识码**: A **文章编号**: 1009 - 2552(2021)08 - 0150 - 06
DOI: 10.13274/j.cnki.hdzj.2021.08.028

Application of trusted computing technology in network information security

CAO Ning
(Kunming Zoo, Kunming 650021, China)

Abstract: In order to ensure the network information security, and reduce the time of network information security defense management, and improve the network information security defense efficiency, this paper proposes the application method of trusted computing technology in network information security. This paper uses trusted computing technology to collect the characteristics of network information data, optimizes network information risk classification algorithm, divides network information risk categories and carries out security defense. It uses the least square method to calculate the optimal fitting distribution measure and value of risk of network information, and uses the principle of active defense of information security to build a network data information security processing model to ensure that trusted computing technology is applied in the network application effect in information security. The experiment results show that the network information security defense efficiency of the proposed method is high, which can effectively guarantee the network information security and reduce the network information security defense time.

Key words: trusted computing technology; network information security; least square method; risk measurement

0 引 言

目前互联网在政府、社会、个人以及政治、金融、军事等各个领域的信息管理中得到了广泛的应用。然而,网络信息给人类带来巨大财富和便利的同时,也面临着对网络信息安全的严峻挑战[1-2]。因此,研究如何运用新的理论和技术手段构建网络安全保障体系,具有十分重要的现实意义。

该领域相关学者对其进行了研究,并取得了一定的研究成果。文献[3]提出贝叶斯网络模型

作者简介: 曹宁(1981 -),男,学士,高级工程师,研究方向为信息技术创新、电子政务云、大数据等。

在信息安全风险评估中的应用，该方法能够准确反映信息系统安全风险等级，但该方法的网络信息安全防御时间较长。文献[4]提出模糊综合评判法在电力企业网络信息安全评估中的应用，该方法能够提高电力企业的网络信息安全可操作性，但该方法的风险度量程度较低。针对上述问题，提出可信计算技术在网络信息安全中的应用，对大数据时代计算机网络信息安全的隐患进行了分析研究，完善网络信息安全保障措施，充分发挥网络价值，确保网络信息安全。

1 网络信息安全可信计算

1.1 网络信息风险类别算法

通过构建不同类型网络信息风险种类，进行网络信息特征采集分析，计算最优特征拟合分布情况，测定不同置信水平下的网络信息安全风险值 $\hat{X}$ 和变异系数 $\overline{\overline{N}}$。根据网络信息安全期望值 B^T 和标准差 P_L，计算不同类型数据泄露数值，具体算法为：

$$(B^T P_L \overline{\overline{N}})\hat{X} = D \tag{1}$$

其中：

$$\hat{X} = (B^T P)^{-1} + \overline{\overline{N}} \tag{2}$$

为确保网络信息在传输过程中不被篡改、丢失或损坏，保证网络安全环境，数据不被未授权方使用。首先设置用户认证，确保未经授权的用户或实体不能访问网络数据，防止非法入侵[5]。对不同用户提取的特征信息进行风险判定，通过可信计算技术保障公共网络系统中信息的机密性、完整性、可用性和可靠性。将网络信息风险权重矩阵定义为 $P = D^{-1}$，根据最小二乘法原则进行优化，可得到变异系数，在特征 B 矩阵的列满秩，记为 $V^T PV = \min B$，则采集到的特征数据进行风险观测处理，具体方法如下：

$$D(\hat{X}) = D^{-1} + (B^T P \overline{\overline{N}})^{-1} \tag{3}$$

$$E(L) = V^T PV - (B^T P_L)^T \hat{X} D(\hat{X}) \tag{4}$$

在对网络信息安全数据进行风险类别评估的过程中，其应用到的风险识别函数模型表示为：$[E(L), \hat{X}D] + [D(\hat{X}), delta_{(0)}^{(2)} B]$，进一步结合可信计算原理及 MATLAB 数据处理软件计算参商误差，当 $x = 3$ 时对网络信息风险特征导数值进行取值，具体取值原理可记为 $f'(3) = 1/3 = 0.333$，则进一步计算网络安全风险差值，具体算法如下：

$$f'(x) \approx \frac{f(x) - E(L)}{D(\hat{X}) + \ln h} \tag{5}$$

利用连续的迭代计算移动节点，反复计算，直到满足网络安全信息防御要求为止。通过连续迭代，最终完成对目标到样本集合密度的最大区间，也就是目标所在的区间的搜索[6]。针对入侵特征的网络风险信息进行处理，如果将网络入侵信号横向矢量表示为 α，网络入侵数据纵向矢量表示为 β，网络入侵特征信号的初始处理结果表示为 γ，那么防御系数可表示为：

$$\Delta k = \sqrt{\gamma}\alpha \cdot f'(x) + \beta \tag{6}$$

根据上述算法，对网络入侵风险等级进行划分。对比分析信号正常情况和信号处理后结果，比较网络入侵风险等级估计结果与小于等于 1 的分析结果。若比较结果大于正常情况下信号的安全阈值，则表明异常信号具有入侵特性，需要及时清除；若比较结果小于正常情况下信号的安全阈值，则表明异常信号正常，不需要后续处理[7]。考虑到网络入侵信号的多种不确定因素，在正常情况下，网络入侵信号的不同度量结果至少应有两个防御因素，因此，在网络安全风险度量中，设置入侵防御概率为 p_1，异常信号对网络的影响为 G，计算出的网络安全风险度量如下：

$$E = \Delta k \int \left(\frac{p_1 G}{h + m}\right)^h dh \tag{7}$$

式中，m 表示估算调整量；h 表示网络阈值，根据该公式可估算出网络入侵风险等级，依据以上入侵风险参数算法对多维信息安全进行评估[8]。从而更好地对正在载入的网络信息安全状态进行静态测量，并将测量结果及网络信息运行标准安全参数进行散列值对比并进行动态对比，有效识别网络信息中的非法编辑动态元素的动态变化范围。

1.2 网络信息安全防御

利用信息安全主动防御原理，建立网络数据信息安全处理模型，评估整个主动防御网络中的数据安全性，定位网络安全漏洞区域，检测局部区

域风险类别，查找潜在的多条主动防御安全性信息组合攻击途径[9]。为获得部分数据评估结果，收集有关于主动防御网络安全属性相关数据，与数据分析网络的数据以及存储结构相结合，根据分析结果，由此构建网络信息安全防御数学模型。当测量结果满足网络安全语义约束时，信息传输结果保持不变，当网络信息的动态特征元素和风险数据待评价对象的内容出现差异时，需要对网络信息风险差异因子进行校正处理，并对照规范校正步骤，具体网络信息风险校正流程框架结构如图 1 所示。

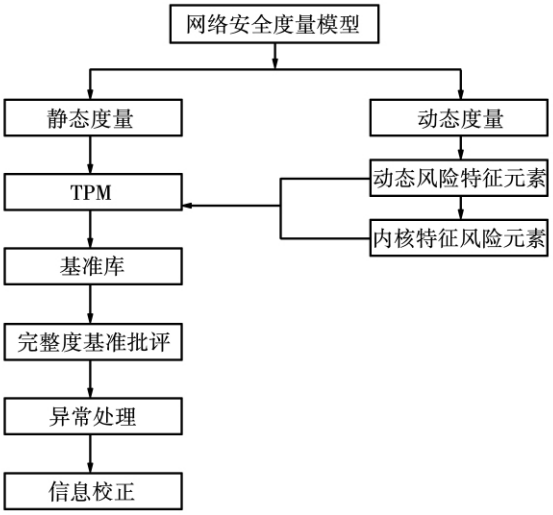

图 1　网络信息风险校正流程

进一步对不同的网络信息安全风险最优拟合分布。对不同网络环境下的信息传输安全评估方案进行优化，建立网络信息传输安全评估体系，从网络安全性、完整性和指向性等方面对安全评价指标进行分析。由于当前的网络安全防护技术采取的是堵漏洞、筑高墙、防攻击的模式，利用防火墙、入侵检测和防病毒技术构成信息安全系统来保障网络安全[10]。这种模式只能防御已知的攻击，难以应对混合型攻击，导致网络信息的防火墙越筑越高、入侵防御系统越来越复杂、病毒库升级越来越频繁，网络信息安全误报率随之增加，为了提高网络信息安全防御效率，结合可信计算基数分析出网络结构中存在的所有风险信息的渗透序列，获取网络信息的目标攻击路径，计算网络安全防御的可达概率，并规范网络安全防御处理步骤，具体如图 2 所示。

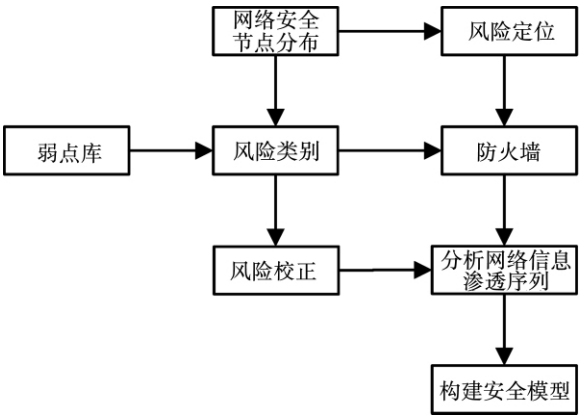

图 2　网络安全防御处理步骤

基于图 2 步骤，结合网络信息攻击数据特征，对主动防御安全性展开说明。并对网络信息安全处理算法进行规范，在信息安全通道上进行信息指令传输，提高数据安全处理响应能力，实现解密和认证功能，从而对用户私密信息进行全方位、多角度的安全保护，在网络结构中构建一个相对更加可信的安全环境。为方便进行网络安全性评估，对网络防御数据的数据安全集合进行构建，具体集合如表 1 所示。

表 1　数据安全集合

防御区域	安全信息
host_name	缺乏所在局部网络名称
vulnerability_id	缺乏唯一的网络地址
vulnerability_ range ={ local，remote}	缺乏所造成的局部网络攻击范围
vulnerability_service	缺乏利用局部网络信息服务
vulnerability_result	缺乏所造成的局部网络信息攻击成功后再获取相应权限
vulnerability_complexity	利用安全漏洞攻击的复杂程序

进一步利用网络安全漏洞的复杂程序对网络安全信息进行归一量化处理，并制定详细的网络信息安全防御方案，使用现有的攻击方案和工具对不同的网络风险特征类比进行详细方案的制定，并说明有效的防御方案。提取有关的网络信息异常数据，根据网络信息风险种类对入侵数据进行关联性采样和拓展性采样分析。优化网络信息安全压缩属性维度，消除冗余信息，并提出标准

的网络安全特征训练样本，并进行迭代计算，获取网络信息的区域过渡均值特征。对网络信息的区域过渡处理方法进行优化，具体如图 3 所示。

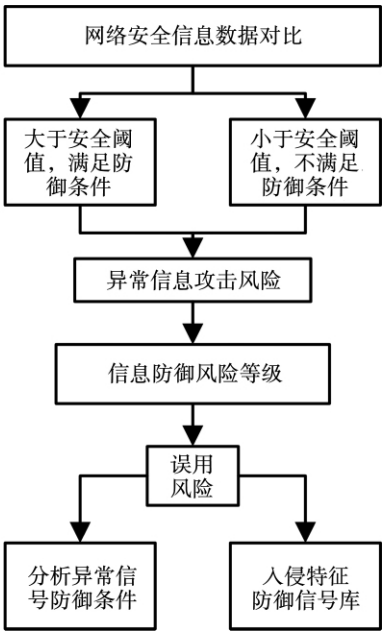

图 3　网络信息的区域过渡处理方法

1.3　网络信息安全处理的实现

为了加强网络信息安全防护效果，提高网络信息的安全性，从多方面、多角度加强网络数据信息的监管和防护，从而保证网络信息的安全性，可在网络信息处理的过程中，进程与进程之间，经常会发生干扰，会影响别的进程。为了防止安全行为中不正确的修改，导致网络安全效果，以时间为尺度为标准，搜索网络安全数据，设计建立数据熵模型，具体如下所示：

$$g(n) = [(t_1, n_1, x_1), (t_2, n_2, x_2), \cdots, (t_i, n_i, x_i)] \tag{8}$$

式中，x 代表按网络信息传输安全数据；t 代表了迭代次数；n 代表错误数据讯号。由于互联网存在安全威胁，因此网络不能正常运行时，基于前文方法，网络安全防御系统每 5 秒就会发出与错误属性数据相关的讯号，为了保证讯号的及时性，将 15 秒的间隔作为时间间隔，提取相应的运行信息，完成错误数据属性熵的计算，具体算法如下：

$$H(f) = -e\sum_{r=1}^{k-1} p(r)\lg(n) + E \tag{9}$$

式中，e 是安全常数；$p(r)$ 表示原始状态的信息个数，其大小表示互联网安全信息在规定时间间隔内所收到的峰值讯号。基于上述数值进行网络信息处理方法的规范。处理网络信息安全威胁事件的发生大致分为三个层次，具体包括网络安全事件的采集层，负责采集原始的网络安全数据，包括受到威胁情境下的主机、数据库以及应用系统的状态，判断其与正常情况下的不同之处；其次是网络安全受到威胁事件分析层，针对问题进行具体分析可以找到问题的症结所在，也就可以判断产生问题的大致方向；最后是网络安全威胁问题的事件展示层，找出问题并解决后，对问题以及解决方法进行展示，基于此对网络安全管理模块进行优化，具体如图 4 所示。

通过图 4 可以得出，网络安全受到威胁的解决方法包括前期的采集与分析，以及后期的案例展示。现有的基于行为的动态可信度量方法都是对可信系统中运行的每个程序的行为进行度量，提高网络安全信息运行可信度，综合考虑属性度量和行为度量的优点，建立了基于使用控制的行为度量模型，保证网络信息运行环境的动态安全属性。

2　实验结果分析

为了验证可信计算技术在网络信息安全中的应用效果，分别采用文献［3］方法、文献［4］方法与所提方法进行对比实验。

2.1　实验环境

为保障实验检测结果，对实验环境及参数进行统一设置，具体如表 2 所示。

表 2　实验参数

实验环境	实验参数
评估网络	通信网络
最大评估时间	15min－30min
操作系统	Windows-XP
基础模型	多元异构网络结构
分类算法	RIPPER 分类算法
信息融合算法	可信度算法
威胁度参数	TD

2.2　实验结果

通过改变某时段网络结构的安全设置，得到

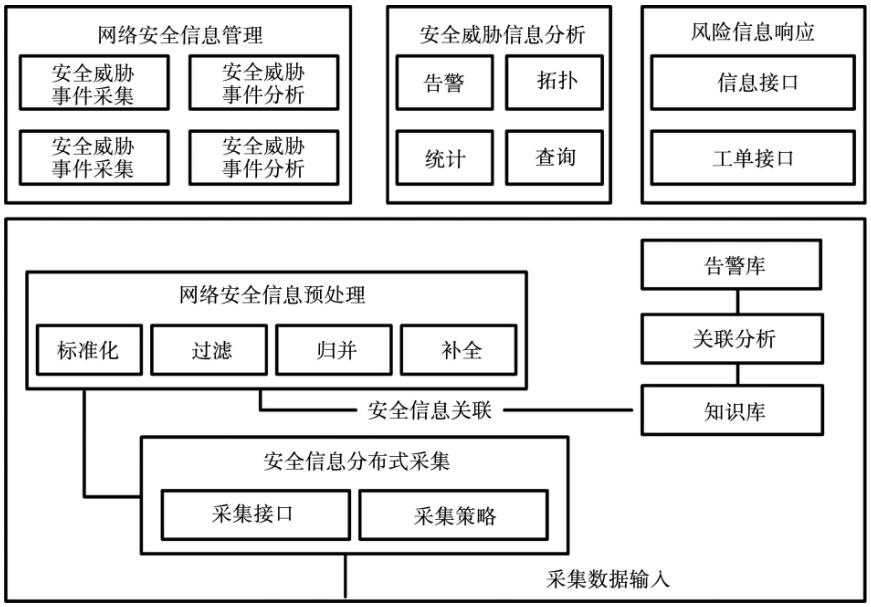

图 4　网络安全处理模型

网络信息传输安全机密性的向量 $A_z=(A_z(c))_n$、信息完整特征向量 $A_v=(A_v(c))_n$，信息可用特征向量 $A_t=(A_t(c))_n$ 作为标准测试数据，对文献[3]方法、文献[4]方法与所提方法的特征安全性进行风险度测量，不同方法的风险度量对比结果如图 5 所示。

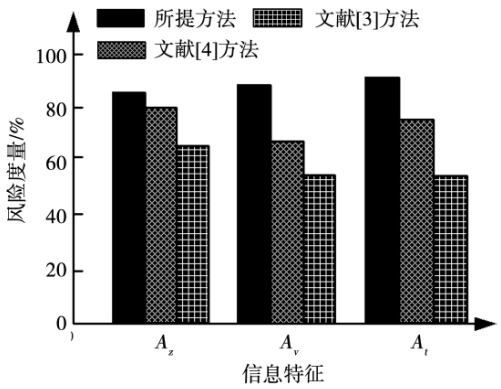

图 5　不同方法的网络安全风险度量对比结果

根据图 5 可知，在不同网络信息特征中，文献[3]方法的平均风险度量为 59%，文献[4]方法的平均风险度量为 72.7%，而所提方法的平均风险度量高达 89%，由此可知，相对于文献[3]方法和文献[4]方法而言，所提的可信计算技术在网络信息安全中的应用方法在实际检测过程中，其风险度量较高，可以有效保障网络信息处理的安全性，充分满足研究要求，因为所提方法能够从多方面、多角度加强网络数据信息的监管和防护，从而保障网络信息的安全性。

为了验证所提方法的网络信息安全防御效率，分别采用文献[3]方法、文献[4]方法与所提方法对比不同方法的网络信息安全防御时间，对比结果如图 6 所示。

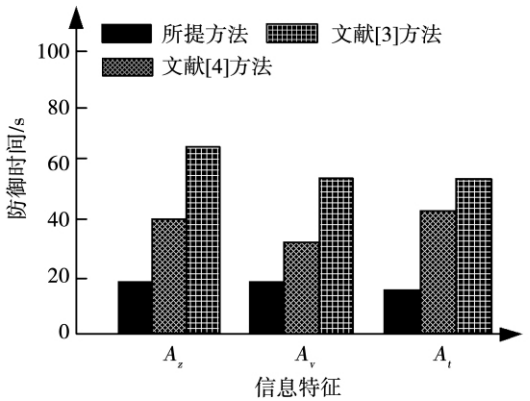

图 6　不同方法的网络信息安全防御时间对比

根据图 6 可知，在不同网络信息特征中，文献[3]方法的平均防御时间为 37.6s，文献[4]方法的平均防御时间为 59s，而所提方法的平均防御时间仅为 19.3s，由此可知，与文献[3]方法和文献[4]方法相比，所提的可信计算技术在网络信

息安全中的应用方法的防御时间较短，网络信息安全防御效率较高，因为所提方法结合可信计算技术，分析网络结构中存在的所有风险信息的渗透序列，获取网络信息的目标攻击路径，计算网络安全防御的可达概率，从而缩短了网络信息安全防御时间，提高了网络信息安全防御效率。

3 结束语

本文提出可信计算技术在网络信息安全中的应用方法，主要利用可信计算技术，采集网络信息数据，划分网络信息风险类别，实现网络信息的安全防御。满足对海量网络信息进行有效管理的研究要求，可信计算技术在网络信息安全的实际应用过程中，保障了网络信息处理的安全性，降低了网络信息安全防御时间，提高了网络信息安全防御效率。本文提出可信计算技术在网络信息安全中的应用方法能够为网络信息安全领域提供相应的应用参考，但针对可信计算技术下的协议存在的安全漏洞问题，还可以利用相关配套产品结合可信计算技术，实现网络信息安全的整体防御，因此，制定相应的网络信息安全标准以及管理要求是下一步的主要研究方向。

参 考 文 献:

[1] 刘敖迪，杜学绘，王娜，等. 区块链技术及其在信息安全领域的研究进展 [J]. 软件学报，2018，29(7)：2092－2115.

[2] 李晔锋，公备，徐达文，等. 可信计算环境下的数据库强制行为控制研究 [J]. 计算机应用与软件，2018，35(8)：66－72.

[3] 黄玉洁，唐作其. 基于改进贝叶斯模型的信息安全风险评估 [J]. 计算机与现代化，2018(4)：95－99，126.

[4] 刘道远，孙科达，周君良，等. 模糊综合评判法在电力企业网络信息安全评估中的应用 [J]. 电信科学，2020，36(3)：34－41.

[5] 张恒巍，黄世锐. Markov 微分博弈模型及其在网络安全中的应用 [J]. 电子学报，2019，47(3)：606－612.

[6] 张恒巍，李涛，黄世锐. 基于攻防微分博弈的网络安全防御决策方法 [J]. 电子学报，2018，46(6)：1428－1435.

[7] 赵超，王慧强，林俊宇，等. 面向大规模网络安全加固的攻击图分析方法 [J]. 计算机科学与探索，2018，12(2)：263－273.

[8] 周珑，郭威，王建永，等. 基于神经网络算法的网络安全评价模型 [J]. 沈阳工业大学学报，2018，40(4)：426－430.

[9] 王增光，卢昱，李进东. 基于贝叶斯攻击图的网络安全风险评估方法 [J]. 装甲兵工程学院学报，2018，32(3)：81－86.

[10] 章俊航，王轶群，王卉，等. B/S 模式下的医院网络信息安全防护系统设计与应用 [J]. 中国医学装备，2020，17(5)：181－185.

(责任编辑：陈文艳)

(上接第 149 页)

[7] 林梅芬，陈婷，王秋杰，等. 一种配电网基于模型诊断的最小碰集改进算法 [J]. 电力系统保护与控制，2020，54(8)：31－39.

[8] 何俊涛，车仁飞，孟庆萌，等. 基于广域录波数据和 FCM 聚类的电网故障诊断方法 [J]. 电力自动化设备，2019，39(6)：179－184.

[9] 刘飞，贲树俊，周嘉，等. 面向配网台区的综合评价模型研究与可视化应用 [J]. 电网与清洁能源，2017，33(5)：63－68.

[10] 刘志欣，程林，周章，等. 基于场景聚类分析的综合能源系统鲁棒运行策略 [J]. 电工电能新技术，2019，38(10)：9－19.

[11] 徐婧，顾煜炯，王仲，等. 基于数据挖掘的煤电机组能效特征指标及其基准值的研究 [J]. 中国电机工程学报，2017，37(7)：2009－2016.

[12] 李柳雅，贾宗璞. 基于 CFSFDP 聚类算法的 WSN 高能效分簇路由算法 [J]. 计算机应用研究，2018，35(3)：884－888.

[13] 陈海文，王守相，梁栋，等. 用户节电的大数据分析及应用 [J]. 电网技术，2019，43(4)：1345－1354.

[14] 徐源，程潜善，李阳，等. 基于大数据聚类的电力系统中长期负荷预测 [J]. 电力系统及其自动化学报，2017，29(8)：43－48.

[15] 曾楠，许元斌，罗义旺，等. 基于分布式聚类模型的电力负荷特性分析 [J]. 现代电力，2018，35(1)：71－77.

(责任编辑：陈文艳)