网络安全数据可视化分析

李城均，郭家铭，黄 栋

（沈阳理工大学，辽宁 沈阳 110000）

摘 要：随着科学技术不断发展，网络信息技术的应用愈加广泛，提高了网络数据安全性问题。近些年来，网络安全数据可视化研究非常火热，更是一个新兴的交叉研究领域。通过采用一系列可视化工具，从而提高安全管理人员的感知程度、分析深度，提高网络安全问题解决效率。文章重点介绍了网络安全数据源，分析了网络安全问题和网络安全可视化方法。旨在提高网络数据的安全性。

关键词：网络安全；数据；可视分析

中图分类号：TN915.08 **文献标志码：**A **文章编号：**1672-3872（2017）06-0114-02

计算机技术作为21世纪中的标志性技术，在社会生产中的应用非常广泛，直接影响人们的生活质量。近些年来，网络安全问题层数不穷，给人们造成了巨大的风险。随着科学技术不断发展，人们对网络安全性的要求越来越高，同时也成为了网络质量评定的重要指标。人们也基于网络安全问题提出了一系列的监测方法与解决措施，例如防火墙、网关、杀毒软件等，这些技术在一定程度上都能够解决网络安全问题。但随着网络病毒制造者的技术水平越来越高，很多网络病毒防御工作更加困难、病毒程序也更加难以破解，从而造成网络安全隐患。基于此，通过加强网络安全数据可视化，采用图形的模式呈现安全数据，从而保障网络数据的安全性。

1 网络安全可视化的必要性

在网络安全防护中，很多人们都会选择网络安全产品，并对异常日志进行分析。这些方法都是计算机受到攻击之后再采用的措施，没有起到预防作用。对于计算机系统中的漏洞修补工作，亡羊补牢。用户一直处于被动攻击地位，给攻击者充足的时间开展攻击活动，这种形式无疑是给攻击者攻击机会。基于此，必须要做好提前防御准备，将被动攻击变为主动防御，从而保障网络数据的安全。对于可视化网安全数据来说，可以将网络数据以动态形式展现出来，也就是在数据存储或传输中，通过可视化技术能够分析数据的风险性，从而提高人们的预防意识，让管理人员提前做好预防准备，降低病毒入侵的风险。

2 网络安全数据可视化技术

2.1 科学计算可视化

科学计算机可视化通过图形的形式，将计算机内容进行可视化转变，这也是计算机安全发展的一大趋势。计算可视化主要是将工程计算和科学数据进行可视化分析，并将计算数据采用图形、表格的总是呈现在人们前面，从而提高计算数据的直观性，实现计算与模拟视觉的交互发展。

2.2 信息可视化

信息可视化作为现代计算机领域中的一个新的研究方向，在现实生活中占据着重要作用。随着信息技术可视化研究不断发展，将庞大数据信息变成图形，从而提高数据的可视性，加强工作人员对网络数据的理解深度。对于信息可视化技术来说，通过对大数据模型进行可视化处理，通过数据分析和人们理解将软件系统中的众多文件或程序代码，采用图形技术处理。并通过数学整理，从而将动态数据、静态数据进行图形分析，找出人们不容易发觉的危险因素，进而提高网络数据安全性。

2.3 安全数据可视化

网络安全数据可视化将数据内容进行可视化处理，应用可视化软件制造数据图形，并将管理人员所采集的数据融入到可视化图形中，通过人工分析、安全评估等方法，从中分析网络数据中哪些数据是安全数据；哪些数据带有安全隐患，并通过图表的形式将数据呈现出来，提高管理人员风险数据的鉴别质量。从本质上来说，网络安全数据可视化就是将数据传统频率、主体内容、异常现象的变化情况展现出来，能够实现危险数据的提前预警，从而实现高质量的安全防护。

3 网络安全可视化方法与形式

3.1 在数据信息安全下形成可视化模式

在网络数据信息可视化领域中，通过端口扫描、服务器攻击、系统病毒扩散等问题频繁发生，并且是一对一、一对多的形式出现，从而造成网络安全数据流量信息出现异常现象。对于数据信息流可视化方面来看，合理对流量进行可视化分析与监控，能够有效提高网络安全管理人员对网络系统的预测与分析，从而让网络数据信息得当防护和维护。网络数据信息可视化模式中，其属性大致为源IP属性、目的IP属性、数据时间、协议、网络端口等方面。

3.2 网络端口信息安全可视化模式

导致网络出现安全隐患的罪魁祸首就是黑客组织，黑客通过对网络系统进行数据分析，找出主机中的漏洞，从而研制针对性病毒开展攻击。由于网络的开放性与发展性，存在网络漏洞是必然趋势，这就要求加强端口的可视化处理，对端口数据进行可视化分析，一旦发现端口数据异常，即可封闭端口，从而降低网络病毒成功几率。

3.3 网络入侵技术可视化模式

绝大数多数网络安全技术都是由于第三方病毒侵入造成的，人为操控错误因素极少。因此，网络管理人员可以通过对入侵系统防御与识别的模式，判断网络病毒、木马的存在，也就是对入侵系统对存储网络病毒进行匹配与扫描，最终通过图形的形式将异常数据展现给管理人员面前，或者通过警报系统将网络安全数据信息传输给相关人员。工作人员通过对数据图形分析，从而找出方入侵的突破口，进而对计算机与网络的漏洞进行修补、及时更新相应的杀毒软件，最大程度上加强网络安全性能。

3.4 防火墙时间安全与可视化模式

防火墙作为网络安全中应用最为广泛的技术之一，能够在网络传输通道设置一道防止病毒侵害的过滤墙。如果信息传输过程中存在异常问题，防火墙即会将异常数据进行阻隔，将安全数据传输出去，从而提高数据安全性能。对于防火墙时间安全可视化模式来说，能够将存储目标主机中的信息日志进行定期进行检测分析，并且记录目标主机与外部主机连接的精准性与操作性。将日志内容制作成图标，从而分析防火墙在检测中的异常数据，通过加以分析提高网络数据的安全性。

（下转第117页）

作者简介：李城均（1995-），男，辽宁沈阳人，研究方向：网络工程。

确定参数k_p、k_i、k_d大致范围，利用迭代法进行计算得出最大迭代次数 G。

$$x_{ij}(0)=rand_{ij}(0,1)(x_{ij}^U-x_{ij}^L)+x_{ij}^L \quad (9)$$

式中：x_{ij}^U为第 i 个个体的第 j 个染色体上界；x_{ij}^L为第 i 个个体的第 j 个染色体下较为合适。

$$x_{ij}(t+1)=\begin{cases}v_i(t+1), f(v_{i1}(t+1),\ldots,v_{in}(t+1)<x_{i1}(t),\ldots,x_{in}(t))\\ x_{ij}(t), f(v_{i1}(t+1),\ldots,v_{in}(t+1)\geq x_{in}(t),\ldots,x_{in}(t))\end{cases} \quad (10)$$

式中：w_1、w_2、w_3为目标函数权系数。

采样时间为 1ms，为了避免控制系统发生超调，以超调量作为界；$rand_{ij}(0,1)$为在区间 [0,1] 中随机取数。

$$h_{ij}(t+1)=x_{p1j}(t)+F(x_{p2j}(t)-x_{p3j}(y)) \quad (11)$$

式中：$x_{p2j}(t)-x_{p3j}(t)$为差异化向量；F 为变异因子，通常取值在 0 ～ 2。

$$v_{ij}(t+1)=\begin{cases}h_{ij}(t+1), & rand\quad l_{ij}\leq CR\\ x_{ij}(t), & rand\quad l_{ij}>CR\end{cases} \quad (12)$$

式中：CR 为交叉因子，0 ≤ CR ≤ 1。CR 取值在 0.6 ～ 0.9 一项优化指标，确定了目标函数，即式（12）。利用差分进化算法对 PID 参数进行优化，取样本个数为 30，变异因子 F=0.9，交叉因子 CR=0.6。参数k_p取值范围为 [0,2]、k_i取值范围为 [-1,1]、k_d取值范围为 [-50,50]，取权系数w_1为 0.9、w_2为 0.001、w_3为 10，最大迭代次数 G=50，利用 MATLAB/Simulink 仿真计算得出，如图 4 所示。基于差分进化算法优化后的 PID 参数：k_p为 0.7947，k_i为 0.1244，k_d为 -0.0051。

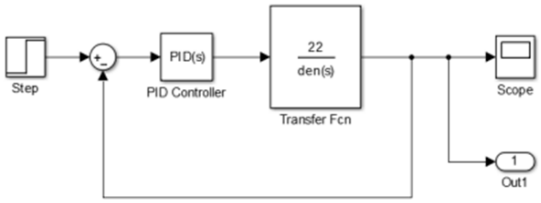

图 4 Simulink 仿真框图

优化前后的系统的阶跃响应如图 5 所示，对比可发现，利用差分进化算法优化 PID 参数后，系统的阶跃响应无超调现象，由于超调量和响应时间不可兼得，所以减小超调量会延长响应时间，这一点在图上也能体现出来。

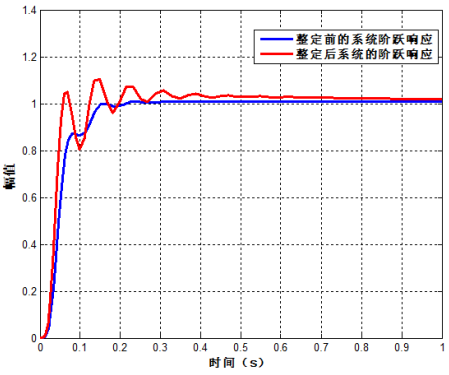

图 5 优化后系统的阶跃响应

3 结束语

文章介绍了皮带跑偏控制系统工作原理，在原系统上做了改进，采用 PID 控制器。并利用差分进化算法对 PID 控制器的参数进行优化，利用 MATLAB 对控制系统建模仿真。结果表明改进后，系统稳定性好，而且无超调现象，对于解决了皮带跑偏问题，增加皮带的使用寿命，避免皮带输送机运转过程中重大事故的发生具有非常重要的实践指导意义。

参考文献：

[1] 王耀，仝荣山．皮带输送机胶带跑偏的原因及控制方法 [J]．能源与节能，2009(6)：24-25.

[2] 宋志安．MATLAB/Simulink 与机电控制系统仿真 [M]．北京：国防工业出版社，2015.

[3] 刘金琨．先进 PID 控制 MATLAB 仿真 [M] 北京：电子工业出版社，2016.

[4] 彭力，李稳，何鸿鲲，等．二自由度 PID 控制器优化设计 [J]．仪器仪表学报，2003,24(Z1)：399-40.

（收稿日期：2017-3-17）

（上接第 98 页）中的应用 [J]．机械管理开发，2015(9)：80-81+92.

[3] 张英祥．机械制造与自动化中节能设计理念的应用研究 [J]．自动化与仪器仪表，2016(3)：64-65.

[4] 陶勇．机械制造与自动化设计中的节能设计探讨 [J]．西部皮革，2016(14)：63+70.

（收稿日期：2017-3-13）

（上接第 104 页）现代会计行业的发展需求。为达到会计的外部环境发展需求，就必须把握好互联网产业的发展形势，从而更好的发展会计系统。提高会计实务效率。

参考文献：

[1] 姜英杰，洪国玉．互联网对财务会计的影响思路探索 [J]．现代商贸工业，2016(16).

[2] 陶俊飞．互联网 + 推进对会计的管理的影响及改革措施 [J]．现代经济信息，2016(3).

[3] 李剑平．网络经济环境下对会计理论的影响研究 [J]．财会月刊，2015(23)：2-5.

（收稿日期：2017-3-17）

（上接第 114 页）

4 结束语

随着我国科学技术不断发展，当即信息网络技术的应用范围愈加广泛，网络安全问题广受社会各个阶层的关注。我国安全数据可视化研究还在不断深入，通过采用不同的研究方法和不同的应用手段，从而构建完善的可视化系统。从而实现有效病毒处理、实时处理、自动报警、自动防御，进而加强网络安全数据的安全性。

参考文献：

[1] 王慧强，赖积保，朱亮．网络态势感知系统研究综 [J]．计算机科学，2016(33)：5-10.

[2] 陈建军，余志强．数据可视化技术及其应用 [J]．红外与激光工程，2011(30)：239-243.

[3] 力煌宗．上网行为管理产品的发展力向 [J]．信息安全与通信保密，2009(9)：45-46.

（收稿日期：2017-3-11）