

一种基于拟牛顿法蝙蝠算法的网络故障检测方法

张义良, 罗晓娟

(萍乡学院 计算机系, 江西 萍乡 337055)

摘 要: 针对现有的网络系统故障检测方式存在的检测精度不高、检测收敛速度慢和易陷入局部最优问题, 综合了蝙蝠算法和拟牛顿法, 提出了一种基于差分进化蝙蝠算法的网络系统故障检测方法(Quasi Newton-Bat Algorithm, QN-BA). 该方式通过搭建滤波模型和残差模型, 结合拟牛顿法蝙蝠算法得到模型的最优解, 有效地规避了现有方式存在的问题. 最后通过仿真实验深入研究了影响该故障检测方法的主要因素, 并对比分析了该方法与 NPSO-PF(新型粒子群优化滤波算法)和 LWRLR(变学习率变加权递推最小二乘算法)的性能, 验证了其有效性.

关键词: 故障检测; 蝙蝠算法; 拟牛顿法; 残差

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2017)01—0128—04

A Network System Fault Detection Based on Quasi Newton-Bat Algorithm

ZHANG Yi-liang, LUO Xiao-juan

(Department of Computer Science, Pingxiang College, Pingxiang 337055, China)

Abstract: In order to effectively solve the problems consisted in the method of existing network system fault detection, the problems includes that detection accuracy is not high, the detection convergence speed is slow, and it's easy to fall into local optimum. In this paper combined with the Bat Algorithm (BA) and Quasi Newton (QN) strategy, a novel model of network system fault detection based on QN-BA is proposed. In this way, the optimal solution of the model is obtained by combining the filtering model and the residual error model, which can effectively avoid the existing problems. Finally through the simulation experiment obtained the fault detection performance index chart, and by comparing the NPSO-PF and LWRLR verify the effectiveness of the proposed approach.

Key words: fault detection; bat algorithm; quasi Newton method; residual error

1 引言

近年来,网络系统的故障检测也日渐成了网络领域的研究热点. 为了有效识别和阻断基于同一未知漏洞的各种代码注入攻击,李闻等^[1]结合进程异常场景自动分析攻击载荷句法,提出了代码注入攻击自动分析和响应方法,以此降低响应虚警概率和系统对外服务的响应时间. 邢池强等^[2]引入一种故障恢复算法,避免了陷入传统方式存在的恢复效率低和中断时间长缺陷. 熊伟等^[3]基于蝴蝶突变模型来描述网络数据的异常行为,并提出了一种突变级

数的异常流量状态检测方法. 陈瑞川等^[4]基于对等网络提出了一种抵御 DoS 攻击的自适应安全框架,并采取轻量级协议交互方式来获取客户端和服务器的实时状态信息. 杨晓峰等^[5]基于正常行文样本的学习原理,采用改进的隐马尔可夫模型提出一种网络攻击检测方法,用来检测异常网络行为. 目前,常用的故障检测方法有:神经网络、粗糙集理论、分类算法、模糊方法及其他人工智能方法,等等. 其中较为有代表性的分类算法是通过从数据集中提取分类特征指标,并将其归纳到特定的已知类别中,它需要构造分类模型和划分实际数据到相应类别,但

是难点在于如何优化分类区间,分类区间过大或者过小都将直接影响数据检测性能。

对此,本文基于拟牛顿蝙蝠算法^[6-8]提出了新的网络系统的故障检测方法,提升了故障检测的性能,利于故障处理,解除了网络异常带来的困扰。

2 网络系统故障检测模型

令 t 时刻某网络系统的状态信息向量为 $\mathbf{x}_t$, 系统输入信息向量为 $\mathbf{I}_t$, 系统输出信息向量为 $\mathbf{O}_t$, 系统的未知扰动向量为 $\boldsymbol{\lambda}_t$, 系统故障信息向量为 $\boldsymbol{\varphi}_t$ ($\boldsymbol{\varphi}_t$ 为零向量表示正常状态, $\boldsymbol{\varphi}_t$ 为非零向量则表示系统存在故障)。网络系统的动态性则可描述为

$$\begin{cases} \mathbf{x}_{t+1} = \mathbf{K}_1 \mathbf{x}_t + \mathbf{K}_2 \mathbf{I}_t + \mathbf{K}_3 \boldsymbol{\lambda}_t + (1 + \alpha_t) \mathbf{K}_4 \boldsymbol{\varphi}_t \\ \mathbf{O}_{t+1} = \mathbf{K}_5 \mathbf{x}_t + (1 + \beta_t) \mathbf{K}_6 \boldsymbol{\lambda}_t + \mathbf{K}_7 \boldsymbol{\varphi}_t + (1 + \gamma_t) \mathbf{O}_t \end{cases} \quad (1)$$

式中,矩阵 $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3, \mathbf{K}_4, \mathbf{K}_5, \mathbf{K}_6$ 和 $\mathbf{K}_7$ 表示具有适当维度的矩阵,并且 $\alpha_t = 0$ 或 $1, \beta_t = 0$ 或 $1, \gamma_t = 0$ 或 1 。式(1)给出了网络系统的动态性表示,同时需要结合预测系统搭建系统滤波模型,计算并分析实际输出的残差状态。令滤波器如下所示。

$$\begin{cases} \hat{\mathbf{x}}_{t+1} = \mathbf{K}_1 \hat{\mathbf{x}}_t + \mathbf{K}_2 \mathbf{I}_t + \eta_t (\mathbf{O}_t - \hat{\mathbf{O}}_t) \\ \hat{\mathbf{O}}_t = \mathbf{K}_3 \hat{\mathbf{x}}_t \\ \boldsymbol{\varepsilon}_t = \mu_t (\mathbf{O}_t - \hat{\mathbf{O}}_t) \end{cases} \quad (2)$$

式中, η_t 和 μ_t 是随机参数,用来保证故障检测的灵敏度和鲁棒性。令其残差为

$$\begin{cases} \mathbf{e}_{t+1} = (\mathbf{K}_1 - \eta_t \bar{\mathbf{x}}_t) \mathbf{e}_t + (\mathbf{K}_4 - \eta_t \bar{\mathbf{O}}_t) \bar{\boldsymbol{\lambda}}_t + (\mathbf{K}_6 - \eta_t \bar{\mathbf{O}}_t) \boldsymbol{\varphi}_t \\ \boldsymbol{\varepsilon}_{t+1} = \mu_t \bar{\mathbf{x}}_t \mathbf{e}_t + \mu_t \bar{\mathbf{O}}_t \bar{\boldsymbol{\lambda}}_t + \mu_t \bar{\mathbf{O}}_t \boldsymbol{\varphi}_t + \boldsymbol{\varepsilon}_t \end{cases} \quad (3)$$

结合系统故障信息向量和残差,本文建立故障检测的最优目标函数:

$$Y = \min(a\varphi, b\boldsymbol{\varepsilon}, c\boldsymbol{\varepsilon}) \quad (4)$$

式中, a, b 和 c 表示权重系数。传统的求解算法容易陷入局部最优状态和故障检测精度不高的问题,因此本文拟结合蝙蝠算法和拟牛顿法来对上述目标优化模型进行求解。

3 拟牛顿蝙蝠算法

蝙蝠算法是一种模拟蝙蝠在复杂的自然环境中利用回声定位(超声波)系统来探测猎物、避免障碍物的随机搜索算法。其原理是将蝙蝠个体与搜索空间中的点进行映射,将蝙蝠个体移动和搜捕食物的过程类比为搜索和优化过程,将搜索和优化过程中用较优的可行解取代较差的可行解的迭代过程模拟为蝙蝠个体的优胜劣汰过程。但当蝙蝠算法寻优到

后期时,容易出现寻优进展缓慢的问题。而拟牛顿法是一种求解非线性最优化问题的有效方法,它克服了牛顿法在计算过程中需要求导和求逆的缺点,提高寻优进度和精度。

结合蝙蝠算法和拟牛顿法,本文给出网络系统故障检测的求解算法(Quasi Newton-Bat Algorithm, QN-BA)。

Step 1 令 t 时刻蝙蝠种群初始种群数量为 N , 蝙蝠 i 的速度、位置和声波频率分别表示为 v_i, d_i 和 τ_i , 初始搜索半径 d_i , 迭代次数为 MAX, τ_a, τ_b 分别为声波频率上下限。

Step 2 设置蝙蝠的适应度值函数:

$$f(Y) = \frac{e^Y}{1+Y} \quad (5)$$

Step 3 下一时刻 $t+1$, 蝙蝠 i 的声波频率、速度和位置更新规则如下所示。

$$\begin{cases} \tau_i(t+1) = \tau_b(t) + \text{randn}()(\tau_a - \tau_b) \\ v_i(t+1) = v_i(t) + \rho_1 \tau_i |Y_{\text{opt}}(t) - Y_i(t)| \\ f_i(t+1) = f_i(t) + \rho_2 v_i(t) \Delta t \end{cases} \quad (6)$$

式中, $Y_{\text{opt}}(t)$ 表示 t 时刻的最优解, ρ_1 和 ρ_2 分别为权重系数,并且 $0 < \rho_1 < 1, 0 < \rho_2 < 1, \text{randN}()$ 产生 $(0, 1)$ 之间的正态分布随机数。

Step 4 判断搜索半径 d_i 与 $(\tau_a - \tau_b) \text{randN}()$ 之间的关系,如果是大于关系则随机产生新解,并对新解进行越界处理。如果是小于关系,并且 $f(Y_i) < f(Y_{\text{opt}})$, 继续产生扰动因素优化和产生新解,并对搜索半径 d_i 进行更新:

$$r_i(t+1) = (1 + \tau_a) \exp((1 - \Delta\tau)t) \quad (7)$$

式中, $\Delta\tau$ 表示搜索频度的增加系数。同时对所有蝙蝠的适应度值进行排序,得出当前时间的最优值。

Step 5 同时结合拟牛顿算法对适应度值进行优化,来更新种群的最优解。

(1) 对 t 时刻的解 Y_t 和残差阈值 ϵ_0 , 判断适应度值 $||f(Y_t)|| < \epsilon_0$, 则算法结束,输出估计位置 Y_t ; 否则令 $L_t = (1 - H_t)f(Y_t)$ 。

$$H_t = \frac{Y_t \tau_t^T + \tau_t Y_t^T}{\tau_t^T Y_t} + \left(1 + \frac{\tau_t^T Y_t}{\tau_t^T Y_t}\right) \frac{\tau_t \tau_t^T}{\tau_t^T \tau_t} \quad (8)$$

(2) 沿着 L_t 方向进行搜索,求出满足 wolf 搜索条件的 δ_t , 使得 $f(Y_t + \delta_t L_t) = \min f(Y_t + \delta_t L_t)$ 。

(3) 计算 $|f(Y_{t+1})|$, 并校正 H_k , 跳转到步骤 (1) 重复执行。

Step 6 在算法完成一次迭代后,进入下一次迭代之前,判断是否到达迭代次数为 MAX, 如果是则退出算法并输出种群的最优解及种群的最优值,否

则跳转到步骤(3).

Step7 输出残差, 并进行故障判别. 先设置残差阈值 $\chi(\chi > 0)$, 与经过上述步骤得到的残差值比较. 如残差值大于阈值, 即 $\epsilon_i < \chi$, 可以判断系统存在故障, 否则系统正常.

4 仿真实验

为了验证本文提出的 QN-BA 算法在网络系统故障检测中的有效性, 这里将结合 NS2 和 MATLAB 进行联合仿真实验. 首先在 NS2 中构建如图 1 所示的网络仿真图, 并通过仿真实验得到了基于 QN-BA 的网络系统故障检测性能指标变换图. 同时比较分析了基于新型粒子群优化滤波算法(NPSO-PF)、变学习率变加权递推最小二乘算法(LWRLR)和本文提出的 QN-BA 算法在网络系统故障检测的效率. 网络参数设置为: 链路容量 15 Mb/s, 延时 10 ms, 各节点缓存大小 200 packets, 各数据包 200 Byte. 算法的相关参数为: 种群数量为 $N=200$, 搜索频度的增加系数 $\Delta\tau=0.2$, 最大和最小声波频度分别为 $\tau_a=0.8, \tau_b=0.2$, 迭代次数 $w=300$ 次.

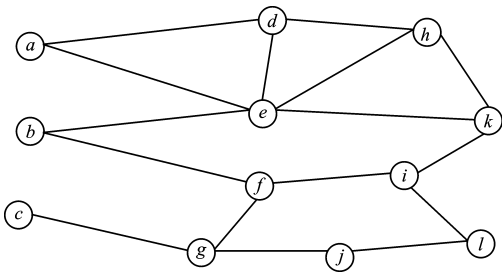


图 1 网络仿真图

其次, 图 2 给出了基于 QN-BA 的故障检测的三个主要性能指标随检测时间变化的曲线图. 随着检测时间的增加, 算法的稳健性越来越好, 故障检测的精确率随之增加, 而误报率和漏报率随之减小, 最终趋于稳定. 这也验证了一个可靠的故障检测模型应该保证误报率和漏报率应尽量小, 精确率高的规律.

同时, 图 3 是比较分析了 NPSO-PF、LWRLR 和本文介绍的 QN-BA 算法在故障检测中精确率的变化图. 相比 NPSO-PF、LWRLR, 本文的 QN-BA 算法性能较好, 算法收敛速度更快, 寻优精度更高.

为了进一步讨论 QN-BA 算法在故障检测中的有效性, 图 4 分别比较了三种算法下残差阈值的设置变化对漏报率的影响. 可以明显看出, 当残差阈值

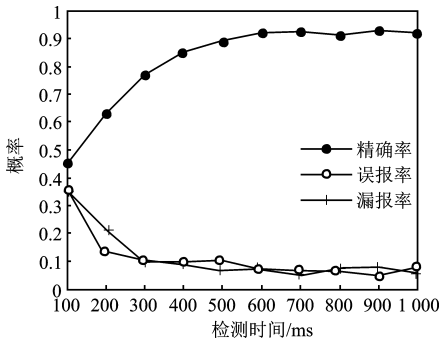


图 2 网络故障检测性能

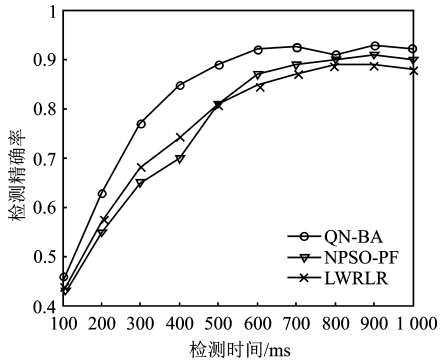


图 3 故障检测精确率

较小时, 漏报率都较小, 反之, 漏报率随阈值增加而快速增加. 在故障诊断中, QN-BA 的优势也很明显. 所以在现实的应用中, 在设置残差阈值时应该综合考虑平均代价和鲁棒性等性能指标的最佳权衡.

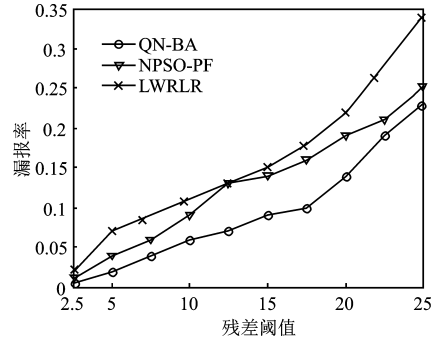


图 4 不同残差阈值下的漏报率

在故障检测算法的性能评价中, 检测的灵敏度也是一个极其重要的指标, 特别是对信号强度比较微弱的故障检测, 如果算法不够精确和比较迟钝, 对性能的影响比较大. 图 5 中比较了三种故障检测算法对故障信号的敏感程度. 相比之下, QN-BA 算法对故障信号的灵敏度较高, 即使对信号很微弱的故障信号. 这也造就了 QN-BA 算法能在较短的时间内检测到故障, 即 QN-BA 故障检测算法的及时性较好.

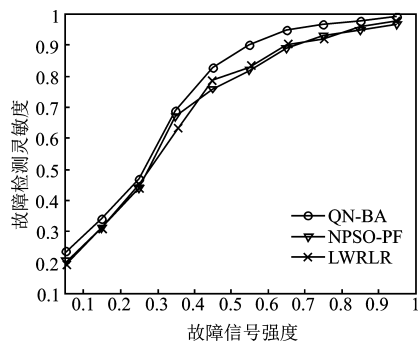


图 5 故障检测灵敏度

5 结束语

本文就目前网络故障检测系统存在的检测精度不高、检测收敛速度慢和易陷入局部最优的问题,在蝙蝠算法的基础上,引入了一种改进方法——拟牛顿蝙蝠算法,并提出了一种新的故障检测方式.通过该方式搭建了滤波器和残差模型,同时通过拟牛顿蝙蝠算法求出最优解.最后,对该方法进行了仿真实验分析,深入分析了影响该故障检测方法的主要影响因素,并与其它故障检测方法性能进行了比较.结果显示基于拟牛顿蝙蝠算法的网络系统故障检测方法更为有效.

参考文献:

[1] 李闻,戴英侠,连一峰,等. 基于异常诊断的代码注入攻击自动分析和响应系统[J]. 软件学报, 2008, 19(6): 1519-1532.

[4] 苏宛新,程灵燕,程飞燕. 基于 DSP+FPGA 的实时视频信号处理系统设计[J]. 液晶与显示, 2010, 25(1): 145-148.

[5] 赵高长,张磊,武风波. 改进的中值滤波算法在图像去噪中的应用[J]. 应用光学, 2011, 32(4): 678-682.

[6] 邢克飞. 星载信号处理平台单粒子效应检测与加固技术研究[D]. 长沙:国防科学技术大学, 2007.

[7] 贺朝会. 空间轨道单粒子翻转率预估方法研究[J]. 空间科学学报, 2001, 21(3): 266-273.

[8] Wang J J. Single event upset and hardening in 0.15 μm antifuse-based field programmable gate array[J]. IEEE Transactions on Nuclear Science, 2003, 50(6): 2158-2166.

[2] 邢池强,兰巨龙,胡宇翔. 基于等效资源的可重构服务承载网故障恢复机制[J]. 计算机应用, 2014, 34(7): 1965-1966.

[3] 熊伟,胡汉平,王祖喜,等. 基于突变级数的网络流量异常检测[J]. 华中科技大学学报(自然科学版), 2011, 39(1): 28-31.

[4] 陈瑞川,郭文嘉,唐礼勇,等. 一种抵御拒绝服务攻击的自适应客户端难题[J]. 软件学报, 2009, 20(9): 2558-2573.

[5] 杨晓峰,孙明明,胡雪蕾,等. 基于改进隐马尔可夫模型的网络攻击检测方法[J]. 通信学报, 2010, 31(3): 95-101.

[6] 郭业才,吴华鹏,王惠,等. 基于 DNA 遗传蝙蝠算法的分数间隔多模盲均衡算法[J]. 兵工学报, 2015, 36(8): 1502-1507.

[7] 谢健,周永权,陈欢. 一种基于 Lévy 飞行轨迹的蝙蝠算法[J]. 模式识别与人工智能, 2013, 26(9): 829-837.

[8] 郑红,李振,黄盈. 一种基于拟牛顿法的 CS 投影矩阵优化算法[J]. 电子学报, 2014, 42(10): 1977-1982.

作者简介:

张义良 男, (1978-), 硕士, 副教授. 研究方向为计算机网络. E-mail: zhangyl1978@163.com.

罗晓娟 女, (1975-), 硕士, 副教授. 研究方向为计算机网络.

作者简介:

陆 嵩 男, (1992-), 硕士. 研究方向为先进集成系统与 SoC. E-mail: sfhulusong@163.com.

付方发 男, (1984-), 博士, 讲师. 研究方向为片上网络体系结构.

谭龙玉 男, (1986-), 工程师. 研究方向航天器自主导航技术.

王进祥 男, (1968-), 教授. 研究方向为先进集成系统与 SoC.