

网络数据入侵中的路线图谱绘制方法研究

何小利¹, 宋 钰²

(1 四川理工学院 计算机学院, 四川 自贡 643000;

2 四川理工学院 网络管理中心, 四川 自贡 643000)

摘 要: 提出基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法. 该方法计算网络检测模块的平均入侵检测率, 组建实时网络数据入侵流量模型, 并获取网络数据入侵流量特征, 在此基础上利用竞争关联优化算法利用确定的入侵参数来选取网络数据入侵的簇头, 并利用加入竞争因子的蚁群方法对网络入侵中的各个路线进行检测, 有效完成了对网络数据入侵中的路线图谱绘制. 实验结果表明, 基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法有效地提升了网络通信的安全性及稳定性.

关键词: 数据入侵; 入侵检测; 路线图谱

中图分类号: TP393.1

文献标识码: A

文章编号: 1000-7180(2016)02-0109-04

Research on the Calculation Method of Network Data Invasion Route Map

HE Xiao-li¹, SONG Yu²

(1 School of Computer Science, Sichuan University of Science and Engineering,

Zigong 643000, China; 2 Center of Network Information Management, Sichuan

University of Science and Engineering, Zigong 643000, China)

Abstract: Associated optimization algorithm is proposed based on improved competition network data in the invasion route map calculation method. This method calculates the average rate of intrusion detection network detection module, a real-time invasion of network data flow model, and get the invasion of network data flow characteristics, on the basis of the use of competition associated intrusion parameters optimization algorithm is used to select data network intrusion of cluster heads, and use the add competition factor of ant colony method for each of the routes in the network intrusion detection, effectively completed the route map of network intrusion data calculation. The experimental results show that the associated optimization algorithm based on improved competition calculation method of the network data in the invasion route map can effectively enhance the security and stability of the network communication.

Key words: data invasion; intrusion detection; route map

1 引言

在国内,随着计算机科技技术与网络通信技术水平的飞速发展,网络规模在日益扩大,但与此同时网络数据入侵行为的泛滥也给网络的通信安全运行造成了极大的威胁^[1-3]. 在这种状态下,如何有效地保障网络的通信安全成为互联网技术与通信技术领

域中亟待解决的主要问题^[4-6]. 而网络数据入侵中的路线图谱绘制方法可以迅速地发现网络数据入侵行为,成为解决上述问题的根本途径,它引起了很多专家与学者的重视. 由于网络数据入侵中的路线图谱绘制方法具有深远的发展意义,因此也成为了业内人士研究的焦点课题,受到了广泛的关注,同时也出现了很多好的方法^[7].

收稿日期: 2015-04-15; 修回日期: 2015-06-03

基金项目: 四川省人工智能重点实验室基金(2014RYY02)

文献[8]提出了基于遗传距离和系统树的网络数据入侵中的路线图谱绘制方法. 该方法先建立最相邻种群间的遗传距离矩阵, 构建系统入侵检测的树状拓扑结构, 并利用该结构推测网络入侵的传播路径, 完成了对网络数据入侵中的路线图谱绘制. 该方法较为简单, 但是存在检测误差大的问题. 文献[9]重点讨论了基于强化规则学习的网络数据入侵中的路线图谱绘制方法.

该方法将规则学习算法融入到网络数据入侵中的路线图谱绘制中, 通过增强弱规则学习器对网络入侵审计数据的分类性能, 实现了对网络数据入侵中的路线图谱绘制. 该方法鲁棒性较强, 但是采用当前的算法进行网络数据入侵中的路线图谱绘制时, 需要进行多次簇头选择, 存在入侵检测误差大的问题. 文献[10]重点讨论了基于状态转换法的网络数据入侵中的路线图谱绘制方法. 该方法将网络数据入侵过程定义为一个行为序列, 将由这个行为序列而导致的系统(从初始状态到入侵状态)变化过程用状态转换图来表示, 实现了对网络数据入侵中的路线图谱绘制. 该方法较为精确, 但是存在计算较为繁琐的问题.

针对上述问题的产生, 本文提出了一种基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法. 该方法通过在网络系统的部分设备中增添入侵检测模块, 建立网络数据入侵模型, 提取网络数据入侵流量特征, 使用融合于自相关函数 ACF 和偏相关函数 PACF 的定阶方法来确定模型中的网络数据入侵参数, 利用竞争关联优化算法选取网络数据入侵的簇头, 运用加入竞争因子的蚁群方法对网络数据入侵的各个路线进行检测, 有效地实现了对网络数据入侵中的路线图谱绘制.

2 网络数据入侵中的路线图谱绘制优化原理

针对采用当前的算法进行网络数据入侵中的路线图谱绘制时, 需要进行多次簇头选择, 存在入侵检测误差大的问题, 提出了一种基于竞争关联优化算法的网络数据入侵中的路线图谱绘制方法.

2.1 网络数据入侵流量模型的组建

在网络数据入侵中的路线图谱优化计算过程中, 先在网络中的部分设备中增添入侵检测模块, 计算网络检测模块的平均入侵检测率, 利用该模块组建实时网络数据入侵流量模型, 并获取网络数据入侵流量特征, 融合于自相关函数 ACF 和偏相关函数 PACF 的定阶方法来确定模型中的网络数据入侵参

数. 具体的步骤如下所示.

设 e 代表网络的平均数据包错误率, p_{ij} 代表设备检测到网络入侵的可能性, 需要满足于 $1 \leq j \leq i$ 的条件, 则 i 代表从添加入侵检测模块的设备之后的跳簇, j 代表从簇头起 j 跳的入侵位置. 则入侵检测模块的路由设备在本簇内能够检测到网络入侵的概率, 利用下式可以表示为

$$p_{11} = \frac{(1 - e)}{p_{ij}} \quad (1)$$

式中, p_{11} 代表入侵检测模块的路由设备在本簇内能够检测到数据入侵概率.

假如网络通信的结构是处于网状拓扑结构, 则增添入侵检测模块后能够检测到网络数据入侵的比例, 利用下式表述为

$$p_{21} = \frac{(1 - e)}{p_{11}} \quad (2)$$

式中, p_{21} 代表增添入侵检测模块后能够检测到数据入侵的比例.

假如 a 代表的网络设备簇头没有添加入侵检测模块, 则由 S_a 代表网络设备簇头 a 的休眠概率, 利用下式可以计算出入侵检测模块能够检测簇外节点数据入侵的概率:

$$p_{22} = \frac{a(1 - e)(1 - S_a)}{p_{21}} \quad (3)$$

式中, p_{22} 代表入侵检测模块能够检测簇外节点数据入侵的概率.

利用下式可以计算出网络检测模块的平均检测率:

$$p_i = \frac{1}{i} \sum_{j=1}^i p_{22} \oplus p_{ij} = \frac{1}{2} \sum_{j=1}^2 p_{2j} = \frac{1}{2} [(1 - e) + (1 - e)(1 - s_a)] \quad (4)$$

式中, p_{2j} 代表入侵检测模块进行网络入侵时所形成的相对误差.

组建实时网络数据入侵流量模型, 并获取网络数据入侵流量特征的具体的步骤如下所示.

(1) 在网络数据入侵中的路线图谱优化计算过程中, $[X_0, X_1, \dots, X_n]$ 代表常规状态下网络的数据流量使用情况, 则利用下式可以建立实时网络数据入侵流量模型:

$$x_i = \frac{\mu_i + \varphi_i + \phi_i + \varepsilon_i + \phi_i \varepsilon_i + \sigma_i^2}{p_i \times [X_0, X_1, \dots, X_n]} \quad (5)$$

式中, x_i 代表组建的实时网络数据入侵流量模型, $\varphi_i, \phi_i, \sigma_i^2$ 分别代表入侵模型估计参数, ε_i 代表白噪声.

(2) 利用下式获取实时状态下的网络数据入侵流量特征.

$$\Phi_p = x_i \times \frac{p_i}{[X_0, X_1, \dots, X_n]} \quad (6)$$

式中, Φ_p 代表提取的网络数据入侵流量流量特征.

利用 $\{p_k\}$ 代表的网络入侵数据样本的自相关函数和 $\{\varphi_{kk}\}$ 代表的样本偏自相关函数的截尾性判定模型的入侵参数, 利用式方程组表述:

$$p_k \leq \frac{1}{\sqrt{n}} \sqrt{1 + 2 \sum_{i=1}^q p_i^2 \Phi_p} \quad (7)$$

$$p_k \leq \frac{2}{\sqrt{n}} \sqrt{1 + 2 \sum_{i=1}^q p_i^2 \Phi_p} \quad (8)$$

$$|\varphi_{kk}| \leq 1/\sqrt{np_k} \quad (9)$$

$$|\varphi_{kk}| \leq 2/\sqrt{n}\Phi_p \quad (10)$$

式中, p_i^2 代表 $\sqrt{n}$ 步截尾, q 代表模型入侵参数.

综上所述, 在网络数据入侵的路线图谱优化计算过程中, 先在部分网络设备中增添入侵检测模块, 计算网络检测模块的平均入侵检测率, 利用该模块组建实时网络数据入侵流量模型, 并获取网络数据入侵流量特征, 使用融合于自相关函数 ACF 和偏相关函数 PACF 的定阶方法来确定模型中的网络数据入侵参数, 为实现网络数据入侵中的路线图谱优化计算奠定了基础.

2.2 网络数据入侵中的路线图谱绘制优化原理的实现

在网络数据入侵的路线图谱优化计算过程中, 利用竞争关联优化算法以上式获取的入侵参数为依据, 选取网络数据入侵的簇头, 利用加入竞争因子的蚁群方法对网络入侵中的各个路线点进行检测. 具体的步骤如下所示.

利用竞争关联优化算法, 以式(10)获取的入侵参数为依据, 可以得出下式:

$$g(l) = \frac{F_{10} + \beta F + \chi_F}{\{p_k\} \times \{\varphi_{kk}\}} \oplus q \times \left(\frac{p_i^2}{\sqrt{n}} \right) \quad (11)$$

式中, $g(l)$ 代表网络各个入侵路线在数据传输过程中的异常情况, l 代表线路的序号, F_{10} 代表第 l 个入侵路线进行通信时的异常情况, β 代表当前线路的流量干扰因素, χ 代表邻近路线的流量干扰因素, F 代表邻近路线的消耗流量平均值, 可以利用下式计算 F :

$$F = \frac{1}{p-1} \sum_{j=1}^p \quad (12)$$

式中, $\frac{1}{p-1}$ 代表消耗流量最多的线路. 需要满足于 $j=1$ 的条件.

在网络数据入侵中的路线图谱优化计算过程中, 利用加入竞争因子的蚁群方法对网络入侵中的各个路线进行检测, 将上述两个公式进行综合, 可以得出带有竞争因子的适应性函数:

$$g(l) = F_{10} + \beta F + \frac{\chi}{p-1} \sum_{j=1}^p F \quad (13)$$

在网络数据入侵中的路线图谱优化计算过程中, 假设 $N \times N$ 代表网络覆盖区域的面积, 利用下式可以计算出入侵的网络路线簇头:

$$L = \sqrt{\frac{\psi_{p_i}}{\psi_{nq}}} \times \frac{N}{e^2} \times g(l) F \quad (14)$$

式中, ψ_{p_i} 代表入侵的网络的路线点的时间序列, ψ_{nq} 代表竞争因子的权重, e^2 代表设定入侵检测门限值.

综上所述, 在网络所有的路线中, 可以通过竞争关系, 检测出网络数据入侵的簇头路线点.

网络数据入侵中的路线图谱绘制优化原理, 有效的完成网络数据入侵中的路线图谱优化计算.

3 实验及仿真证明

为了证明提出的基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法的有效性需要进行一次实验. 实验设定网络覆盖区域全部路线的数量是 19 个, 由 1×10^5 代表采集的数据量, 则网络入侵路线分布情况能够用图 1 进行表述.

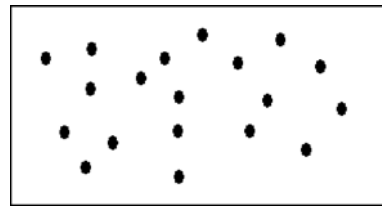


图1 网络入侵路线分布图

分别利用改进算法和传统算法进行网络数据入侵中的路线图谱绘制实验, 在不同的实验次数下, 将两种算法的网络入侵检测结果进行对比, 结果见图 2 和图 3.

将上述实验过程中的相关数据进行整理分析后可知, 改进算法进行网络数据入侵中的路线图谱绘制实验检测的准确率要远远高于传统算法, 充分显

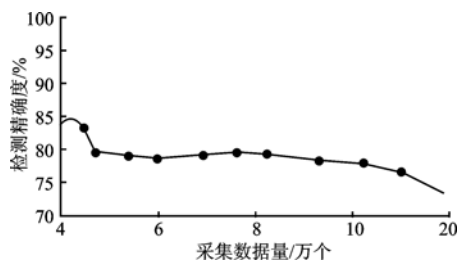


图2 传统算法检测结果

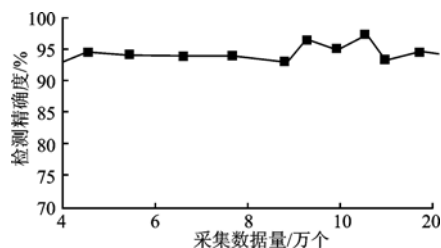


图3 改进算法检测结果

示了改进算法的优越性。

实验结果表明,基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法有效提升了网络通信的安全性及稳定性。

4 结束语

针对采用当前算法进行网络数据入侵中的路线图谱绘制时,需要进行多次簇头选择,存在入侵检测误差大的问题,本文提出了一种基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法。该方法先在网络中的部分设备中增添入侵检测模块,计算网络检测模块的平均入侵检测率,利用该模块组建实时网络数据入侵流量模型,并获取网络数据入侵流量特征,使用融合于自相关函数 ACF 和偏相关函数 PACF 的定阶方法来确定模型中的网络数据入侵参数,在此基础上利用竞争关联优化算法确定的入侵参数来选取网络数据入侵的簇头,并利用加入竞争因子的蚁群方法对网络入侵中的各个路线进行检测,有效地完

成了对网络数据入侵中的路线图谱绘制。实验结果表明,基于改进竞争关联优化算法的网络数据入侵中的路线图谱绘制方法有效的提升了网络通信的安全性及稳定性。

参考文献:

- [1] 许伟,褚玉晓. 基于竞争关联优化的无线网络入侵图谱分类算法[J]. 科技通报, 2013, 29(10): 127-129.
- [2] 沈渊. 基于入侵关联跟踪的 P2P 网络入侵检测方法[J]. 科技通报, 2013, 29(6): 32-34.
- [3] 程源,楚春颖. 一种基于 PSO 辨别树的 P2P 网络入侵检测方法[J]. 科技通报, 2013, 29(6): 56-58.
- [4] 张永俊,牟琦,毕孝儒. 基于云模型的增量 SVM 入侵检测方法[J]. 计算机应用与软件, 2013, 30(3): 311-314.
- [5] 姜参,王大伟. 一种改进蚁群聚类的入侵检测方法[J]. 计算机技术与发展, 2013, 23(12): 139-142.
- [6] 阳时来,杨雅辉,沈晴霓,等. 一种基于半监督 GH-SOM 的入侵检测方法[J]. 计算机研究与发展, 2013, 50(11): 2375-2382.
- [7] 池静,杨振宇,张婷. 基于贝叶斯和决策树的入侵检测方法[J]. 工矿自动化, 2013, 39(2): 62-65.
- [8] 王宇飞,赵婷,李韶瑜,等. 采用改进最小闭包球向量机的电力信息网络入侵检测方法[J]. 电网技术, 2013, 37(9): 2675-2680.
- [9] 李文锋. 浅谈入侵检测方法[J]. 电子技术与软件工程, 2015, 28(12): 224-224.
- [10] 杨盛明,李伟华. 基于失败连接分析和 P2P 的未知网络蠕虫检测[J]. 电子设计工程, 2013, 21(3): 142-146.

作者简介:

何小利 女, (1982-), 硕士研究生, 讲师. 研究方向为计算机网络、计算机信息安全和电子商务.

E-mail: lily_820456@163.com

宋钰 男, (1981-), 硕士研究生, 工程师. 研究方向为计算机网络安全.