

非均匀噪声环境下网络小扰动入侵源定位检测方法研究

蒋 帅¹ 罗天鑫²

(郑州工业应用技术学院现代教育技术中心¹, 机电工程学院², 郑州 451100)

摘 要 非均匀噪声环境下网络小扰动数据入侵具有信号振幅小、攻击性强等特点,传统方法对小扰动入侵检测准确率低、漏报率高,不能对小扰动入侵源进行准确的定位和检测。提出一种基于生物免疫学的入侵源定位检测系统设计,搭建适用于非均匀噪声环境下网络小扰动入侵检测的软硬件平台,对输入检测系统的数据进行预处理,模拟生物免疫系统信息处理机制,通过不断更新规则库识别出“友好”数据和“非友好”数据,最后进行亲和力计算和数据匹配,实现非均匀噪声环境下网络小扰动入侵源定位和检测。通过仿真试验证明提出的方法能够有效地完成对小扰动入侵源的定位和检测。

关键词 非均匀噪声环境下网络小扰动 生物免疫 入侵源定位检测

中图法分类号 TP393.08; **文献标志码** A

随着网络时代的到来,人们的工作生活已经深深地融入了互联网。网络给我们带来信息的互补和无缝对接的同时,也带来了愈来愈多的安全隐患。各种攻击方法和入侵类型不断地升级和多样化,其中非均匀噪声环境下网络小扰动数据入侵具有信号振幅小、攻击性强的特点,传统方法在应对和处理小扰动数据入侵时有效性较差。BP神经网络算法^[1-4]在应对一般数据入侵检测时效果良好,但应对振幅较小的小扰动数据检测时准确率低;数据挖掘算法^[5,6]能够提高检测的准确率,但计算复杂、稳定性差^[7,8];最小二乘法^[9,10]在对小扰动攻击信号源入侵源定位检测时,不能很好地控制其振幅性能,漏报率高。

本文提出一种基于生物免疫学的入侵源定位检测系统设计,首先搭建适用于非均匀噪声环境下网络小扰动入侵源定位和检测的硬件平台,然后建立与硬件平台匹配的系统软件。对进入检测系统的所有数据进行预处理,模拟生物免疫系统信息处理机制进行数据识别,通过不断更新规则库分离出“友好”数据和“非友好”数据。最后进行亲和力计算和

数据匹配,实现非均匀噪声环境下网络小扰动的入侵源定位和检测。本文通过仿真试验证明提出的方法能够有效地实现对非均匀噪声环境下网络小扰动入侵源的定位和检测

1 非均匀噪声环境下网络小扰动入侵源定位检测系统设计

针对小扰动数据入侵的特点设计了适用于入侵源定位和检测的硬件系统和软件系统,模拟生物免疫原理,能够提高检测精度同时降低漏报率,同时有效地控制振幅性能,实现对小扰动入侵源的定位和检测。

1.1 入侵源定位检测系统硬件设计

设计的定位和检测非均匀噪声环境下网络小扰动数据入侵的系统硬件设计包括6个模块:输入模块、控制中心模块、动态内存模块、电源模块、网络接口模块、预警输出模块,如图1所示。

数据输入和输出预警模块能够实现对小扰动入侵数据的识别、分析处理、归类到预警,是整个入侵检测的端口模块。

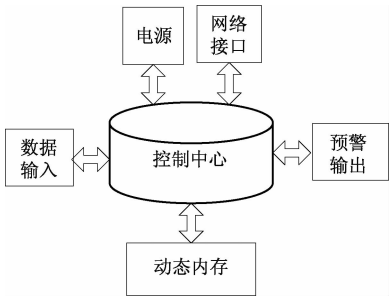


图1 入侵检测系统硬件设计

Fig. 1 Intrusion detection system hardware design

2016年8月21日收到
河南省高等学校重点科研项目(15B520036)资助
第一作者简介:蒋 帅(1984—),男,汉族,河南商丘人,硕士研究生,实验师。研究方向:计算机应用、计算机网络安全、软件工程。E-mail:jiangsuai951@163.com
引用格式:蒋 帅,罗天鑫. 非均匀噪声环境下网络小扰动入侵源定位检测方法研究[J]. 科学技术与工程, 2017, 17(5): 247—251
Jiang Shuai, Luo Tianxin. Design of intrusion detection system for intrusion detection system with small disturbance[J]. Science Technology and Engineering, 2017, 17(5): 247—251

控制中心模块是硬件系统的大脑和小扰动入侵数据信息处理中心,用于剥离和处理进入系统各种数据信息和对入侵数据及友好数据进行区识别和归类。

适用于小扰动数据入侵检测系统内存空间不足,需要增加外部数据存储装置。增加动态内存模块装置后其读写速度大幅度增加,比 Flash 存储器要有优势,且具备存取速度快、成本低等优点,这个优势被普遍使用在数据处理系统里。

网络接口模块是实现系统功能的核心部,选择 DM9000AE 作为以太网控制部分,Intel 芯片支持 150 Mbs 的快速以太网接入,其内部集成 MAC 控制器和物理层接口。该芯片使用较为简单,能够快速契合提供了基础硬件。

电源模块保证系统正常供电及整个控制中心模块运行的稳定性,系统电源模块具有自我保护功能,保证整个系统的供电稳定性和入侵检测活动的实现。

1.2 入侵源定位检测系统软件设计

适用于小扰动入侵源定位和检测系统软件设计是整个入侵检测系统的核心,本文采用微软 Windows10 操作系统当作基础操作系统,在软件设计时把解析技术和入侵报警技术连接起来。软件系统的设计构造由数据收集、数据解析、检测入侵数据误用模块和小扰动数据入侵警报模块等构成,其整体设计图如图 2 所示。

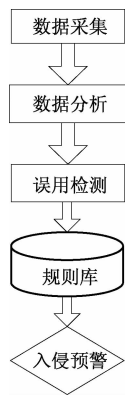


图 2 入侵检测系统软件设计

Fig. 2 Intrusion detection system software design

数据收集模块用以太网的数据输送方式,采用以太网的自身特性能达到对网络里输送数据采集的目的。

数据解析模块以系统的控制中心为载体,对输入数据收集模块数据讯息进行处理,和这一构造进行配对,加入结果不一样,那么判断成异常数据,调用入侵警报模块进行报警。反之,调用异常

检测模块对数据继续进行解析。这个模块容易扩展,可以对进入系统的小扰动数据进行分析和处理。

误用检测模块主要完成对协议分析模块提交的数据进行进一步审查,对入侵行为进行进一步识别。为了增加检测速率及检测准确度,使用模拟生物免疫学算法进行快速配对。误用检测模块能依据原有的入侵规律,达到对入侵行为检测的目的。还要考虑误用检测技术对未知攻击检测水平受限,系统增加了入侵规律获取技术,经过解析网络里数据报文获取出入侵特性,扩大特性规则库,补充误用检测模块识别效率。

入侵数据为小扰动数据时预警模块要是识别到异常数据或者系统被攻击时,可以实现此模块进行报警功能。系统把入侵行为分类成多个等级,一般状况下只能进行日志记录。在嵌入式系统里,把日志传送至和以太网连接的远程服务器里。若产生重大警情,能激活短信报警模块及时通知有关工作人员。

1.3 基于生物免疫学的小扰动入侵检测的实现

系统硬件和软件平台搭建完成后采用基于生物免疫学算法实现对小扰动入侵数据的检测。首先进入检测系统的数据进行预处理,模拟生物免疫系统信息处理机制,通过不断更新规则库识别出“友好”数据和“非友好”数据,最后进行亲和力计算和数据匹配,实现非均匀噪声环境下网络小扰动的入侵源定位和检测。

输入系统的非均匀噪声环境下网络小扰动数据一般具有多个属性,假如把原始数据直接用来检测,则对小扰动入侵数据的检测后果有偏差,且检测效率低。在采用生物免疫算法对数据实行检测前一定对数据实行预处理,分离数据属性特点,详细方法是对小扰动数据进行标准化处理,使属性基点和变化范围趋于一致,让各属性的均值是 0,方差是 1,然后对他进行正规化处理让属性的取值处在 $[0, 1]$ 区间。

对小扰动数据进行标准化处理,设 a_{ij} 表示输入系统的多维数据属性, $\bar{a}_j$ 为属性 a 的均值, σ_j 是 a 第 j 维的方差:

$$\bar{a}_j = \frac{1}{n} \sum_{i=1}^n a_{ij} \quad (1)$$

$$\sigma_j = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (a_{ij} - \bar{a}_j)^2} \quad (2)$$

$$a_{ij} = \frac{a_{ij} - \bar{a}_j}{\sigma_j}; \quad i, j = 1, 2, \dots, n \quad (3)$$

经过对数据的标准化预处理后能够使其属性取

值在 $[0,1]$ 范围内,并且简化匹配算法,降低入侵检测的偏差,提高准确率。

模拟生物免疫的基本原理,把输入网络的数据按照免疫系统自我保护原理,把属于自我并对自我无害的数据信息定义为“友好”,而把有入侵风险的数据信息定义为“非友好”,通过区别判别入侵活动,其原理可表述如下:

$$f(a)_{ij} = \begin{cases} 1, & \text{if match}(\bar{a}, \text{nonself}) \\ 0, & \text{else} \end{cases} \quad (4)$$

$$\text{match}(\bar{a}, \text{nonself}) = \min(\text{match}(\bar{a}, \bar{\sigma})) \quad (5)$$

式(4)和式(5)函数表达式说明,当一组数据属性特征和系统已知“友好”数据相同时可以判别为合法行为,否则可以判定为入侵行为。模拟生物免疫学规则库,需要不断地更新规则,完善友好数据的匹配标准。有效准确的规则数目需要增加,新规则代替旧规则。引入平均相似度概念 S_{avg} ,可以实现规则库的自动更新,并且识别标准更加清晰, R 为数据集合, R_i 与 R_j 为该数据集合中任意的两个数据,在检测输入数据时,平均相似度可以提高检测小扰动数据入侵的准确率。

$$S_{\text{avg}} = \frac{\sum_{R_i, R_j \in R}^n \text{similariry}(R_i R_j)}{S_{ij}};$$
$$ij = 1, 2, 3, \cdots, n; \quad i \neq j \quad (6)$$

平均相似度能够使规则库实现自动更新,最后对输入的小扰动数据模拟生物免疫系统进行数据匹配及亲和力计算,最终达到对小扰动入侵数据进行定位和检测的目的。

模拟检测器经过使用持续配对算法把获取的网络入侵数据字符和检测器聚集的每一个检测器实行配对及入侵数据亲和力计算。假如有两个或两个以上检测器配对待检测字符串,则此时检测器就对网络入侵控制中心进行报警。入侵检测系统主机把他和本身的检测器集进行配对,假如数据不符合,那么就确定是入侵行为,向控制中心报警。 w_i 为规则库中的数据匹配标准, Δt 为匹配规则出现的间隔时间,根据此匹配标准对输入数据进行亲和力计算,最终是小扰动入侵源的定位和检测。

$$w_i = \frac{\sum_{R_i \in R}^n \text{sign}(\text{similariry}(R_i R_j) \geq S_{\text{avg}})}{|S_{ij}|};$$
$$i = 1, 2, 3, \cdots, n \quad (7)$$

判别数据亲和力 q 的公式可以表达为:

$$q = f(\Delta t, w_i, S_{\text{avg}}) \quad (8)$$

数据亲和力是模拟生物免疫抗原抗体间的连

接、融合水平,就是抗原基因及抗体基因间的匹配度,对小扰动入侵数据和入侵源实行有效地定位及检测。所以本文采用连续匹配算法计算入侵数据亲和力和,能够有效地对网络数据,尤其是振幅小的小扰动检测更为有效。

通过搭建适合于小扰动网络入侵的软硬件平台,采用生物免疫学算法实现对非均匀噪声环境下网络小扰动入侵源的定位和检测。

2 实验结果与分析

为了验证本文方法在定位和检测小扰动入侵源的有效性,搭建检测入侵数据的仿真平台。通过对比数据挖掘算法与文章提出的生物免疫算法在小扰动数据源定位、检测的准确率、漏报率的统计数据,证明本文算法的优势。

由于非均匀噪声环境下网络小扰动数据入侵振幅小,更不易检测和识别,如表 1 所示传统数据挖掘算法,在输入检测过程中运算量大,而且稳定性差。在随机抽取的 4 组训练数据中,本机基于生物免疫学的算法,准确率表现良好,而且稳定性高。

表 1 准确率数据对比

Table 1 Accuracy of data contrast

攻击类型	训练数据 1	训练数据 2	训练数据 3	训练数据 4
数据挖掘	0.876	0.789	0.901	0.801
本文算法	0.925	0.931	0.929	0.930

如图 3 所示,将两种方法准确率曲线进行对比,随着迭代次数的增加,数据挖掘算法对入侵的检测率波动较大,而本文算法准确率波动性,而且准确均值 90% 以上。

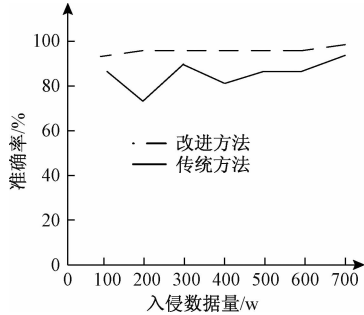


图 3 两种算法准确率对比曲线

Fig. 3 Two kinds of algorithm accuracy contrast curve

在小扰动入侵数据检测的漏报率方面,如表 2 所示,数据挖掘算法,在随机抽取的 4 组数据中漏报率分别为 0.046 7、0.049 8、0.049 8 和 0.04 9,说明算法对于非均匀噪声环境下网络小扰动入侵检测效果不良。而对比本文的算法得出的数据,在漏报率方面有较大幅度的降低。

表 2 漏报率数据
Table 2 Non-response rates data

攻击类型	训练数据 1	训练数据 2	训练数据 3	训练数据 4
数据挖掘	0.046 7	0.048 9	0.045 9	0.049 0
本文算法	0.025 6	0.029 1	0.028 7	0.027 9

图 4 和图 5 是数据挖掘算法和本文算法在经过多次迭代后的漏报率的收敛曲线,可以看出本文的生物免疫算法控制小扰动入侵漏报率方面具有优势。

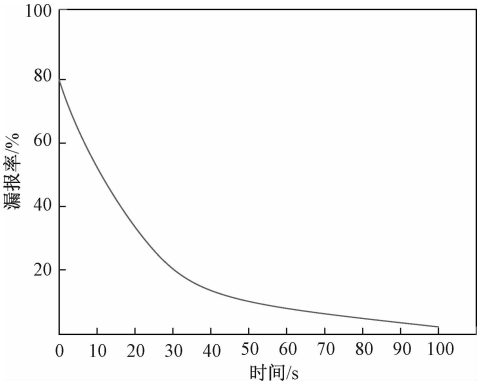


图 4 数据挖掘算法漏报率收敛曲线
Fig. 4 Non-response rates convergence curve data mining algorithm

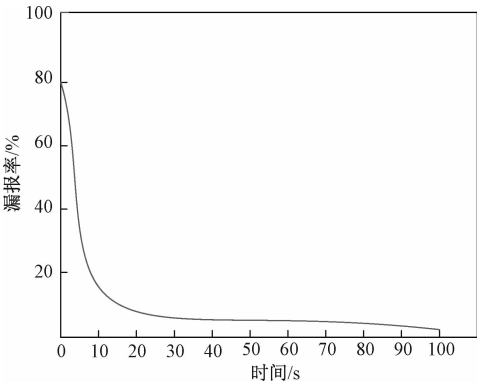


图 5 本文算法漏报率收敛曲线
Fig. 5 Non-response rates convergence curve method

为了测试本文算法在实现小扰动入侵定位和检测的性能,假定入侵攻击信号进入系统的时间间隔服从指数分布,数据挖掘算法在检测小扰动入侵(图 6)数据时,难以控制较小的振幅,并且很难对入侵源的位置进行定位。

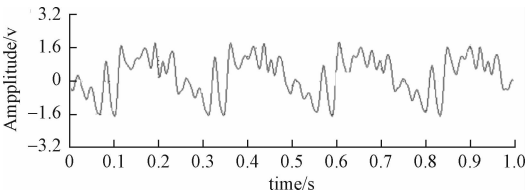


图 6 网络攻击小扰动入侵信号
Fig. 6 Network attack invasion small disturbance signal

经过本文算法处理,模拟生物免疫过程,能够有效地按照规则计算数据亲和力,有效地识别出友好数据和非友好数据,最终实现对小扰动入侵源的定位和检测。如图 7 所示,为本文算法定位后的信号检测输出,定位更为准确,收敛更好。

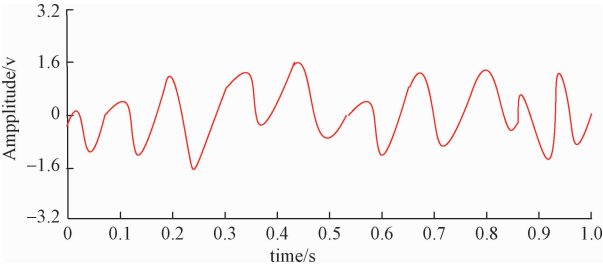


图 7 本文算法定位后的检测输出
Fig. 7 In this paper, positioning algorithm using the test output

本文通过大量的仿真试验,利用试验数据从准确率、漏报率等不同的角度证明的本文的算法能够更加有效地实现对非均匀噪声环境下网络小扰动入侵源的定位和检测。

3 结束语

针对入侵检测结果一直存在检测不准确的问题,提出基于生物免疫学的入侵源定位检测系统设计,并且搭建适用于非均匀噪声环境下网络小扰动入侵检测的软硬件平台,对进入检测系统的数据进行预处理。文章模拟生物免疫系统信息处理机制,通过不断更新规则库知识,对输入系统的“友好”数据和“非友好”数据进行检测和区分,最后进行亲和力计算和数据匹配,实现非均匀噪声环境下网络小扰动的入侵源定位和检测。通过仿真试验证明本文提出的方法能够有效地完成对小扰动入侵源的定位和检测,是一种应对网络入侵和攻击的新模式。

参 考 文 献

1 Kumar D S. A fuzzy decision making approach for analogy detection in new product forecasting. Journal of Intelligent & Fuzzy Systems, 2015; 6(1):1—8

2 谭爱平,陈 浩,吴伯桥. 基于 SVM 的网络入侵检测集成学习算法. 计算机科学, 2014; 41(2):197—200
Tan Aiping, Chen Hao, Wu Boqiao. Network intrusion intelligent detection algorithm based on AdaBoost. Computer Science, 2014; 41(2):197—200

3 Quintanar J L, Salinas E. Mining association rules to evade network intrusion in network audit data. International Journal of Advanced Computer Research, 2014; 4(15):1051—1056

4 Weller-Fahy D J, Borghetti B J, Sodemann A A. A survey of distance and similarity measures used within network intrusion anomaly detection. IEEE Communications Surveys & Tutorials, 2015; 17(1):

70—91

5

饶雨泰,杨 凡. 网络入侵搅动下的网络失稳控制方法研究. 科技通报,2014;30(1):185—188

Rao Yutai, Yang Fan. Network intrusion stir the network instability control methods of the research. Bulletin of Science and Technology, 2014;30(1):185—188

6

温聪源,徐守萍. 基于改进动态源路由协议的 MANET 灰洞攻击检测和缓解研究. 科学技术与工程,2014;14(29):54—60

Wen Congyuan, Xu Shouping. The research of detecting and mitigating gray hole attacks in MANET based on modified dynamic source routing protocol. Science Technology and Engineering, 2014;14(29):54—60

7

马 勇. 模糊推理结合 Michigan 型遗传算法的网络入侵检测方案. 电子设计工程,2016;24(11):108—111

Ma Yong. A network intrusion detection schemer based on fuzzy inference and Michigan genetic algorithm. Electronic Design Engineering, 2016;24(11):108—111

8

Korczynski M, Hamieh A, Huh J H, *et al.* Hive oversight for network intrusion early warning using DIAMoND: a bee-inspired method for fully distributed cyber defense. IEEE Communications Magazine, 2016;54(6):60—67

9

黄国兵,金 勇,贾荣兴,等. 某电能量远方终端双平面网络接口设计. 西安工程大学学报,2016;30(1):102—106

Huang Guobing, Jin Yong, Jia Rongxing, *et al.* Design of double network interface for an energy remote terminal unit. Journal of Xi'an Polytechnic University, 2016;30(1):102—106

10

Malialis K, Devlin S, Kudenko D. Distributed reinforcement learning for adaptive and robust network intrusion response. Connection Science, 2015;27(3):234—252

Design of Intrusion Detection System for Intrusion Detection System with Small Disturbance

JIANG Shuai¹, LUO Tian-xin²

(Zhengzhou University of Industrial Technology Modern Education Technology Center¹, Mechanical and Electrical Engineering College², Zhengzhou 451100, P. R. , China)

[Abstract] In the non uniform noise environment, the intrusion of small disturbance data in the network has the characteristics of small signal amplitude, strong attack and so on, the traditional method of disturbance intrusion detection of low accuracy, high failure rate of small, the accurate localization and detection of the small disturbance source can not be carried out. A design of intrusion detection system based on biological immune system is presented, the software and hardware platform for the intrusion detection of small disturbance in the environment of non uniform noise is set up, preprocessing the data of input detection system, information processing mechanism of simulated biological immune system, by constantly updating the rule base to identify the “friendly” data and “non friendly” data, Finally, affinity calculation and data matching, localization and detection of small disturbance intrusion in the environment of non uniform noise. Through simulation experiment, the proposed method can effectively accomplish the localization and detection of small disturbance intrusion sources.

[Key words] heterogeneous network small disturbance in noise environment biological immune intrusion detection