计算机网络入侵检测系统匹配算法的研究

闫明辉
（天津农学院 计算机与信息工程学院，天津 300384）

摘要：为了能够对网络安全进行有效的保证，并且提高计算机网络入侵检测的性能及效率，实现计算机网络入侵检测系统匹配算法的研究。首先，对计算机网络入侵检测的基本模型进行分析，提出计算机网络入侵检测系统多模式匹配算法，在计算机网络中融入匹配算法；之后，对计算机网络入侵检测系统的多模式匹配算法进行分析，设计基于多模式匹配算法的计算机网络入侵检测系统，然后对多模式匹配算法进行改进，提高算法有效性；最后，对比常规匹配算法，得到满足计算机网络入侵检测系统需求的算法。通过对提出的匹配算法进行研究，表示此算法能够在计算机网络入侵检测中使用，具备一定实用性。

关键词：计算机网络；入侵检测；匹配算法；改进
中图分类号：TN99 **文献标识码：**A **文章编号：**1674-6236(2019)08-0034-04

Research on matching algorithms of computer network intrusion detection system

DOI:10.14022/j.cnki.dzsjgc.2019.08.008

YAN Ming-hui
(*School of Computer and Information Engineering*, *Tianjin Agricultural University*, *Tianjin* 300384, *China*)

Abstract: In order to guarantee the network security effectively and improve the performance and efficiency of computer network intrusion detection, the matching algorithm of computer network intrusion detection system is studied. Firstly, the basic model of computer network intrusion detection is analyzed, and a multi-pattern matching algorithm of computer network intrusion detection system is proposed, which integrates the matching algorithm into computer network. Then, the multi-pattern matching algorithm of computer network intrusion detection system is analyzed, and the calculation based on multi-pattern matching algorithm is designed. Computer network intrusion detection system, and then improve the multi-pattern matching algorithm to improve the effectiveness of the algorithm. Finally, compared with the conventional matching algorithm, we get the algorithm to meet the needs of computer network intrusion detection system. Through the research of the matching algorithm, it shows that the algorithm can be used in computer network intrusion detection, and has certain practicability.

Key words: computer network; intrusion detection; matching algorithm; improvement

在我国信息化进程不断发展的过程中，网络已经在国民经济各领域中所渗透，计算机系统也从独立主机发展成为相互连接、复杂化的开放式系统。在网络技术不断发展的过程中，为社会科教、经济、管理及文化等方面都注入了全新的活力。但是，在网络技术为人们带来便利过程中，还出现了相应的信息安全问题，比如拒绝服务攻击、黑客入侵、病毒等[1]。尤其是最近几年，社会发展要求各用户能够相互通信，并且实现资源共享，网络入侵及攻击事件不断增加，军事机构、政府部门、企业及金融机构等计算机网络频繁遭到黑客袭击，计算机网络安全性越来越突出。入侵检测使用历史较为悠久，因为计算机网络受到多因素的影响，容易受到入侵[2]。以此，研究计算机网络入侵检测系统匹配算法具有重要的现实意义。

1 网络入侵检测基本模型

网络入侵的基本过程为：侦查匹配进入到网络

收稿日期：2018-08-17 **稿件编号：**201808080
作者简介：闫明辉(1996—)，男，天津人。研究方向：计算机网络环境。

全部数据包中，对各个数据及规则模块是否吻合进行分析，将不安全的信息进行过滤。入侵检测系统为保护层，能够实现网络行为的实时监测，以此对网络性能进行保护，从而抵抗网络内部、外部的不定时攻击，避免出现错误操作。图1为网络入侵检测基本模型的结构。其中时间产生器主要目的就是实现网络可疑行为的抽取，行为特征模块实现异常行为特征的记录，此模块具备自我更新及学习的能力，规则模块能够对数据是否具备入侵判断提供基础[3]。

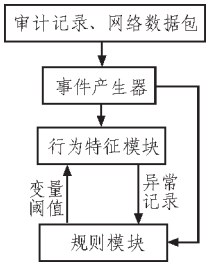

图1　网络入侵检测基本模型的结构

对入侵检测系统是否成功进行评价，其重点就是管理人员是否能够及时的掌握网络系统变化及异常信息，并且在发生事故的过程中，此系统是否具备相应安全策略实现全面保护。因为网络信息具有较大的数据量，并且较为复杂，所以需要相应优秀模式匹配算法实现不安全内容精准且高效的匹配，对网络安全进行保证。单一模式匹配算法具有较强的针对性，只能够实现单一种类网络攻击的匹配。所以，文中就实现多模式匹配算法，实现计算机网络入侵检测系统中多威胁、复杂化网络环境入侵检测需求的满足[4]。图2为计算机网络入侵检测系统多模式匹配算法。

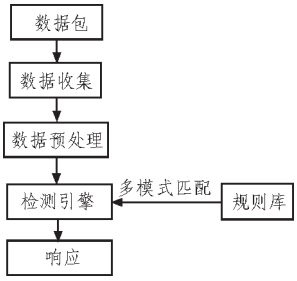

图2　计算机网络入侵检测系统多模式匹配算法

2　计算机网络入侵检测系统的多模式匹配算法

2.1　模式匹配算法分析

字符串模式匹配算法为计算机领域中的主要研究内容，其被广泛应用到语言翻译、拼写检查、数据压缩、搜索引擎等中，都要实现字符串模式的匹配。在入侵检测中，模式匹配算法可以定义为：指定入侵规则库中特点模式字符串P，在网络数据包中进行查找，从而对模式字符串是否出现在网络数据包中进行确定[5]。

网络入侵检测包括数据包捕获、预处理及攻击检测。网络入侵检测就是将网络数据包作为数据源，利用直接检测网络包，能够发现网络中攻击的入侵检测方式。数据包工资检测在网络数据包中对攻击字符串进行检测，此为入侵检测消耗的主要过程[6]。在入侵检测中使用模式匹配算法，需要解决一下问题：

1）提取模式。提高提取模式的质量，将入侵信号特征充分的展现出来，并且模式之间不能够发生冲突。

2）增加模式匹配或者删除。为了能够满足不断变化的攻击手段需求，匹配模式要具备动态变更的能力。

3）增量匹配。在事件流处理系统具有较大压力的时候，要求系统使用增量匹配方法使系统效率得到提高，或者实现高优先级事件的处理，之后处理低优先级事件。

4）完全匹配。匹配机制要能够具备实现全部模式匹配的能力[7]。

2.2　多模式匹配算法的特点

多模式匹配的主要特点为：

其一，在某时间，匹配的状态和匹配符号输出具有密切关系，传统状态对于输出并没有什么影响，也就是能够满足以下公式：

$$p(x_l=a_k|u_l=s_j,x_{l-1}=a_k,u_{l-1}=s_i,\cdots)=p(x_l=a_k|u_l=s_j)$$

$$a_k\in A(a_1,a_2,\cdots,a_q),\ \ s_j\in s\in(s_1,s_2,\cdots,s_j)$$

其二，在匹配状态的时候通过目前的输出符号及前一刻匹配状态唯一实现确定，也就是：

$$p(u_l-s_i|x_l=a_k,u_{l-1}=s_j)=\begin{cases}1\\0\end{cases}$$

在实际使用过程中，匹配信号符号的关联性较大，也就是具有大量记忆匹配，一般对此种符号关联性能够通过条件概率及联合概率进行说明，匹配模式具有记忆。多模式匹配也就是记忆匹配，而且具有重要的作用。一般来说，在匹配符号具有较强依赖性的时候，那么相应匹配熵就会变小，也就是这个时候和极限熵H_∞相互接近，此和最终匹配结果具有

密切的关系。所以,为了使匹配效率得到进一步的提高,能够利用多模式匹配算法实现[8]。

2.3 基于多模式匹配算法的计算机网络入侵检测系统

计算机网络具有自身的特点,可以通过RAC算法实现。此算法主要思想就是利用预处理中的3个函数实现,本文利用函数实现计算机网络遍历及匹配。此算法是利用密钥控制模式的置换检测,图3为置换模式的结构。也就是对图3中的模式树进行检测,包括内部节点是否存在变化[9]。

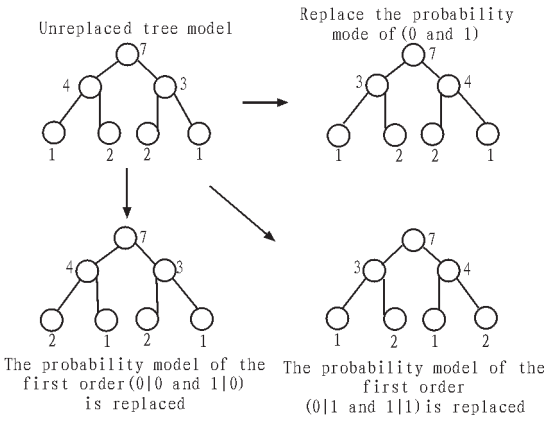

图3 置换模式的结构

检测模式利用以下方式进行实现:首先,利用随机数生成器能够得到256位随机数ri,通过实现模式是否实现置换进行有效的控制,不同的输入方式的种子具有一定的差异,从而能够得出和其相对应的随机数串,随意选择随机数生成器[10]。另外,假如随机数为1,并且其模式相应阶数为0,这个时候的对零阶概率模式中的0和1符号与概率值相互对应,而且实现交换。假如目前使用1阶模式,所以就需要和其相对应的概率值实现交换处理。如果0属于一个概率模式字符,那么这个时候使0|1、1|0中所对应的概率值实现交换。如果前一个字符属于1,那么需要交换的概率值就是0|1、1|1的概率值。图4为模式创建和检测的过程,以此可以看出来,能够利用0101100密钥下实现建模和检测[11]。

3 改进的多模式匹配算法

对于多模式匹配算法的滑动距离函数具有局限性及指针回溯的问题,从而提出改进多模式匹配算法,也就是NBM算法。此算法的主要思想就是在模式串中的第j和字符和文本串中的字符匹配失败的时候,就要对匹配失败目前字符是否出现在模式串中进行考虑。如果出现,那么要根据多模式匹配算法向后划过一段时间;如果不出现,那么就要对匹配失败目前字符中下个字符中是否和模式串P[1]相等。假如相等,就要使P[1]和T[j+1]相互对齐,之后从右到左以此的对不同的字符进行对比。如果不相等,就要对下个字符进行全面的考虑[12]。

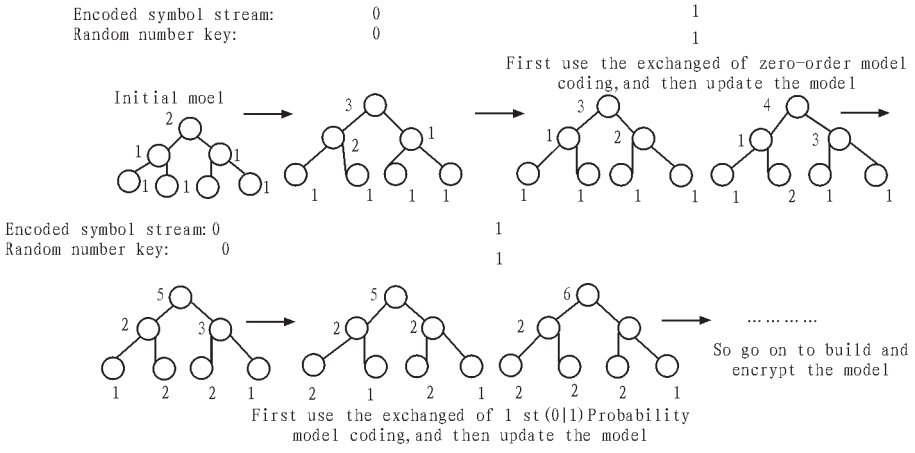

图4 模式创建和检测的过程

对P="abdcd"模式串及T="qoamdebcdabdcd"文本串根据NBM算法实现匹配的过程详见表1。

对假如文本串中字符T[j]不出现在模式串中进行全面的考虑,如果下个字符和模式串中的首字符

表1 NBM算法匹配的过程

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
文本串	q	o	a	m	d	e	b	c	d	a	b	d	c	d
第一趟	a	b	d	c	d									
第二趟										a	b	d	c	d

相同，可以实现滑动距离函数2（Slide2）的创建，实现判断过程的简化，从而降低比较次数，使匹配效率得到进一步的提高。其次，在对传统多模式匹配算法进行分析的过程中，模式串中具有重复字符的过程中，就会导致指针回溯问题的出现，以此可以在滑动距离函数中使用取子串的方式，使指针回溯问题得到解决[13]，主要步骤为：

1）假如使文本串从位置j到左边一个子串及模式串实现从右到左匹配的对比，如果不匹配，那么就要对滑动距离函数进行调用。

2）假如T[j]在P中，那么下次就要从正文j+Slidel的位置实现重新匹配。

3）假如T[j]不在P中，那么j=j+1，并且实现滑动距离函数的调用。

4）对第三步进行反复操作，直到寻找能够继续匹配位置的持续匹配，或者匹配失败。

5）实现模式串P在文本串中T起始位置输出[14]。

改进多模式匹配算法的重点就是，给定模式P=P1P2...Pm，对从字母到正整数映射进行定义：

$Slide$:c→{1,2,⋯,m}

4　实验仿真

对一个模式匹配算法优劣程度进行评价的主要指标就是字符匹配次数，本节实现不同模式匹配算法的实验对比。表2为3种算法在不同模式数量中的匹配时间统计。

表2　3种算法在不同模式数量中的匹配时间统计

模式数量	传统算法	多模式算法	改进多模式算法
10	150	89	38
20	162	101	42
50	213	115	51
100	245	120	68
200	270	123	74
300	305	140	86
500	350	156	94
800	405	177	105
1 000	495	202	135

通过表2可以看出来，改进多模式算法的性能是最优的，并且匹配时间比较短[15]。

另外，文中还对以上3种算法在运行过程中的内存消耗，详见表3。通过表3可以看出来，改进多模式算法的内存占比比较高。

总体来说，能够以实际的需求对匹配算法进行决定，如果计算资源比较少，那么需求算法的资源消耗也会比较少，所以可以使用多模式算法。如果使用的监测需求比较高，那么可以使用改进多模式算法，以此能够得出短的匹配时间及高匹配效率[16]。

表3　3种算法在运行过程中的内存消耗

模式数量	传统算法	多模式算法	改进多模式算法
10	3.2	4.0	10.2
20	3.5	4.2	11.6
50	5.2	6.3	13.3
100	8.9	10.6	17.2
200	18.1	20.5	24.6
300	26.5	27.6	34.6
500	35.2	40.6	50.6
800	56.6	62.3	77.6
1000	62.2	78.5	90.3

5　结束语

入侵检测系统为典型的数据处理系统，其利用分析大量系统审计数据对被监控系统是否受到入侵行为攻击进行判断。在具体到检测机制中，其实就是一个系统主体行为及事件分类系统，要求将系统具备恶意行为通过大量系统行为进行区分，再对此问题进行解决的过程中，就要根据高效入侵检测算法实现。目前，入侵检测系统算法比较多，比如统计分析、专家系统、数据挖掘、模式匹配及神经网络等。本文所分析的改进多模式算法能够有效满足入侵检测系统的需求，并且性能最优。

参考文献：

[1] 卢强，游荣义，叶晓红. 基于自适应卷积滤波的网络近邻入侵检测算法[J]. 计算机科学，2018，45（7）：154-157.

[2] 马占飞，陈虎年，杨晋，等. 一种基于IPSO-SVM算法的网络入侵检测方法[J]. 计算机科学，2018，45（2）：25-26.

[3] 沈沛，刘毅. 计算机网络入侵检测系统匹配算法的研究[J]. 电脑迷，2017，12（9）：29-30.

[4] 栾玉飞，白雅楠，魏鹏. 大数据环境下网络非法入侵检测系统设计[J]. 计算机测量与控制，2018，11（1）：194-197.

[5] 刘建. 基于改进神经网络的网络入侵检测[J]. 科技创新与应用，2018，16（2）：11-12.

[6] 陈超，曹晓梅. 改进差分进化算法优化BP神经网

（下转第43页）

LabVIEW的图形编程语言进行程序编写，所设计的程序采集精度高、速度快、显示直观、操作简单、功能完善且通用性高，满足用户的使用需求并且适用于新用户进行快速上手操作与二次开发，可以广泛地应用于相关的测试领域。

参考文献：

[1] 左明武，卢孔汉，朱郭豪，等. 基于LabVIEW的虚拟温度测控系统设计[J]. 机电工程技术，2015(2):35-37.

[2] 刘鹏，郑宾. 基于LabVIEW的PXI-5152数据采集系统设计[J]. 电子世界，2014(16):162-163.

[3] 杨磊，刘美枝. 虚拟仪器LabView在FPGA数据采集系统中的应用[J]. 电子技术与软件工程，2018(10):64.

[4] 王平，杨涛，侯守全，等. LabVIEW中DAQ数据采集系统设计[J]. 自动化仪表，2015,36(7):31.

[5] 王树东，何明，王焕宇. 基于LabVIEW的数据采集和存储系统[J]. 电气自动化，2015(1):99-101.

[6] 王树东，何明. LabVIEW在数据采集系统中的应用研究[J]. 国外电子测量技术，2014,33(6):103-106.

[7] 曹李莉，王有春，周雷. 通用化数据采集处理系统的LabVIEW实现[J]. 计算机测量与控制，2015,23(4):1375-1377.

[8] 张素萍，李朝强，高照阳，等. 基于RS485和LabVIEW的电参数测量仪数据采集系统[J]. 仪表技术与传感器，2015(6):24-27.

[9] 魏义虎，陈雷. 基于LabVIEW-VISA方式的串口通信研究[J]. 电子设计工程，2015(24):129-131.

[10]赵常寿，陈征祥，樊蓉. 基于LabVIEW和NI-VISA的RS232串口通信程序设计[J]. 电脑编程技巧与维护，2015(1):68-70.

[11]贺成佳，李磊. 基于LabVIEW的多功能虚拟测量系统设计[J]. 电子世界，2018(6):177-179.

[12]吴慧君，韩志引，柳溪. 基于LabVIEW的数据采集系统设计[J]. 数字技术与应用，2014(2):170-170.

[13]代聪，陶红艳，余成波. LabVIEW中利用LabSQL对数据库访问技术的研究[J]. 电子世界，2016(14):77-78.

[14]张璐. LabVIEW中利用LabSQL对数据库访问技术的探讨[J]. 电子测试，2015(2):84-86.

[15]刘杰，张亮，阳元泽. 基于LabSQL的LabVIEW数据库访问[J]. 数字技术与应用，2014(11):98-99.

[16]方毅然，李志斌. 基于LabVIEW的汽车排放检测系统通讯测试软件设计[J]. 仪表技术与传感器，2017(6):78-82.

(上接第37页)

络用于入侵检测[J]. 计算机应用与软件，2018,15(4):85-86.

[7] 刘海燕，张钰，毕建权，等. 基于分布式及协同式网络入侵检测技术综述[J]. 计算机工程与应用，2018,21(8):85-86.

[8] 王鹏. 入侵检测系统在计算机网络安全中的设计与应用[J]. 无线互联科技，2017,11(12):39-40.

[9] 刘日月，马红霞. 计算机网络安全中入侵检测系统的研究与应用[J]. 电脑迷，2017,21(1):29-30.

[10]刘涛. 机器学习算法在校园网入侵检测系统中的应用[J]. 黑河学院学报，2017,8(9):215-216.

[11]海小娟. 计算机网络安全入侵检测系统的设计与应用研究[J]. 自动化与仪器仪表，2017,21(10):142-143.

[12]李丛，闫仁武，朱长水，等. 融合FAST特征选择与ABQGSA-SVM的网络入侵检测[J]. 计算机应用研究，2017,34(7):2172-2179.

[13]麦涛涛，潘晓中，王亚奇，等. 基于预定义类的紧凑型正则表达式匹配算法[J]. 计算机应用，2017,37(2):397-401.

[14]庄夏. 基于局部参数模型共享的分布式入侵检测系统[J]. 计算机工程与设计，2017,11(11):2935-2939.

[15]曹耀彬，王亚刚. 免疫算法优化的RBF在入侵检测中的应用[J]. 计算机技术与发展，2017,27(6):114-118.

[16]张磊，蔡永新，陈潮. 基于时间序列分析的无线传感器网络入侵检测研[J]. 计算机时代，2017,15(12):24-27.