基于模拟退火与K均值聚类的入侵检测算法

胡艳维[1,2] 秦 拯[2] 张忠志[3]
(萍乡高等专科学校 萍乡 337000)[1] (湖南大学软件学院 长沙 410082)[2]
(东莞理工学院计算机学院 东莞 523808)[3]

摘 要 K均值聚类算法对初始值的选取依赖性极大,易陷入局部极值。为此,结合模拟退火算法和K均值聚类思想,提出一种新的入侵检测方案。算法利用模拟退火算法对聚类分析中的聚类准则进行优化,以获得全局最优解,并进一步开拓模拟退火算法的并行性以加快算法收敛速度。在KDD CUP 1999上进行了仿真测试,实验结果表明该方案优于基于K均值聚类的入侵检测算法,有较低的误检率与虚警率。

关键词 入侵检测,模拟退火,K均值聚类,全局优化

Intrusion Detection Algorithm Based on Simulated Annealing and K-mean Clustering

HU Yan-wei[1,2] QIN Zheng[2] ZHANG Zhong-zhi[3]
(Pingxiang School, Pingxiang 337000, China)[1]
(Software School of Hunan University, Changsha 410082, China)[2]
(Computer School of Dongguan University of Technology, Dongguan 523808, China)[3]

Abstract Intrusion detection algorithms based on K-mean clustering have sensitive dependence on initial value and are easy to fall into local extremum. To solve this issue, a new intrusion detection scheme was presented by combing Simulated Annealing and K-mean clustering. The proposed algorithm uses SA to optimize the clustering pattern in the clustering analysis. It can achieve global optimization and better accuracy of the intrusion detection system. Moreover, parallelism of SA greatly quickened the convergence rate. Experiments were completed on KDD Cup 1999, and the results show that presented scheme has lower time consume, false positive rate, and false negative rate compared with intrusion detection systems based on K-mean clustering.

Keywords Intrusion detection, Simulated annealing, K-mean clustering, Global optimization, Parallelism

1 引言

1980年4月,James P. Anderson为美国空军做了一份题为"Computer Security Threat Monitoring and Surveillance"的技术报告,首先提出了入侵检测的概念,并将威胁分为外部渗透、内部渗透和不法行为3种,进一步提出了利用审计跟踪数据监视入侵活动的思想[1]。入侵检测IDS(Intrusion Detection System)是主动保护自己免受攻击的一种网络安全技术,是防火墙之后的第二道安全屏障,致力于实时的入侵检测,在不影响网络性能的情况下能对网络进行监测,从而提供对内部攻击、外部攻击和误操作的实时保护。入侵检测系统有两个重要部分:数据取得和检测技术,至少应包括3个功能模块:提供事件记录流的信息源、发现入侵迹象的分析引擎和基于分析引擎的响应部件。从不同角度划分,入侵检测系统可分类如下:(1)根据检测方法可划分为异常检测和误用检测。异常检测利用被监控系统正常行为的信息作为检测系统中入侵、异常活动的依据;误用检测是根据已知入侵攻击的信息(知识、模式等)来检测系统中的入侵和攻击。(2)根据数据来源的不同可分为基于主机的入侵检测和基于网络的入侵检测。(3)根据入侵检测系统对入侵攻击的响应方式可分为主动入侵检测系统(实时入侵检测系统)和被动入侵检测系统(事后入侵检测系统)。主动入侵检测系统在检测出入侵后,可自动地对目标系统中的漏洞采取修补、强制可疑用户(可能的入侵者)退出系统以及关闭相关服务等对策和响应措施;而被动入侵检测系统在检测出对系统的入侵攻击后只是产生报警信息通知系统安全管理员,而之后的处理工作由管理员完成[2]。

本文研究异常检测技术。根据使用者的行为或资源使用状况的正常程度来判断是否发生异常入侵,而不依赖于具体行为是否出现。即建立被检测系统正常行为的参考库,并通过与当前行为进行比较来寻找偏离参考库的异常行为[3]。W. K. Lee等[4]基于数据挖掘提出的入侵检测方法,其基本思想是利用审计程序提取大量的网络连接和主机会话特征,然后应用数据挖掘技术导出能正确区分正常和入侵行为的规

到稿日期:2009-07-18 返修日期:2009-10-05 本文受国家"973"项目子课题(2007CB310702),湖南省自然科学基金项目(09JJ3124),广东省自然科学基金项目(7007730),广东省科技计划项目(0711020400157),东莞市科技攻关项目(2006D1046,2007108101021)资助。

胡艳维 女,硕士,副教授,主要研究方向为数字水印、数据库、网络安全,E-mail:hyw92188@126.com;秦 拯 男,教授,主要研究方向为信息安全、计算机网络、项目管理;张忠志 男,教授,主要研究方向为信息安全、应用数学。

则。该方法可以检测未知的入侵行为，但误报率高。基于神经网络的异常检测系统[5]的缺点在于计算量较大，这将影响检测的实时性要求。而基于统计的异常检测[6]容易被入侵者通过大量训练，使入侵检测模型适应入侵行为，从而把入侵行为误认为是正常行为。这些检测方法的难点在于很难得到真正纯净的正常数据来建立检测模型。K 均值算法是一种典型的聚类算法，可较好地运用在异常检测技术中。用聚类方法建立的入侵检测系统不需要任何事先标记信息的数据记录，它在保持较低误检率的同时可以有很高的检测率。然而，该类算法很大程度上依赖初始聚类中心和输入数据的模式，并且很容易陷入局部极值[7]。为此，本文利用模拟退火算法对 K 均值聚类中的聚类准则进行优化，提出一种结合模拟退火与 K 均值聚类的入侵检测算法，以提高入侵检测模型的检测率。

2 基于模拟退火与 K 均值聚类的入侵检测算法

2.1 K 均值聚类算法

K 均值聚类算法是一种迭代的启发式算法，迭代过程中不断地移动簇集中的成员，直至得到理想的簇集为止。其基本思想是输入参数 k，将 $n(k<n)$ 个数据对象划分为 k 个类（簇），以使簇内具有较高的相似度，而簇间的相似度较低。算法首先从 n 个数据对象中随机选择 k 个对象作为初始聚类中心，而其他对象则根据它们与每个聚类中心的距离，分别将其赋给最相近的类；然后更新每个类的聚类中心（该聚类中所有对象的均值）。不断重复这一过程，直到准则函数开始收敛为止。通常采用平方误差作为准则函数，其定义为

$$E=\sum_{i=1}^{k}\sum_{x\in C_i}|x-v_i| \tag{1}$$

式中，E 为数据集中所有对象的平方误差的总和，x 为数据对象，v_i 为第 i 个类 C_i 的聚类中心，即

$$v_i=\frac{1}{n_i}\sum_{x\in C_i}x \tag{2}$$

式中，n_i 为第 i 个类 C_i 中数据对象个数。

K 均值聚类算法处理过程如下。

步骤 1　从 n 个数据对象中任意选择 k 个对象作为初始聚类中心；

步骤 2　计算数据集中每个对象与这些聚类中心的距离，并根据最小距离原则重新对相应对象进行划分；

步骤 3　重新计算每个聚类中心，即计算每个簇中对象的平均值；

步骤 4　如果聚类中心或 k 个聚类对象数据集合发生变化，则转至步骤 2，否则聚类运算终止。

K 均值算法原理简单，对大数据集有较快的计算速度，可有效应用于互联网入侵检测系统。但该算法对初始聚类中心选择非常敏感，随机选取不同的初始值可能导致不同的聚类结果，甚至可能得不到有意义的聚类结果。此外，由于该算法采取梯度法求解极值，易于陷入局部极值而无法达到全局最优。为此，本文提出在入侵检测系统中，将模拟退火算法与 K 均值算法相结合，以提高算法的全局寻优能力。

2.2 模拟退火基本思想

模拟退火法最早由 N. Metropolis 等人在 1953 年提出，直到 1983 年由 S. Kirpatrick 等人用来解组合最优化问题，主要是寻求问题的最优解。模拟退火算法由与 Metroplis 准则相对应的转移概率来确定是否接受从当前解到新解的转移。开始时让控制参数 t 有较大的值，在进行足够的转移之后，缓慢减小 t 的值。如此反复迭代，直至满足某个停止准则时算法结束。故模拟退火算法可看成是控制参数递减时 Metropolis 算法的迭代[8]。

模拟退火算法是解决组合优化问题的有效算法，广泛用于需要优化的场合，如最优控制、机器学习、神经网络等算法中的局部最优问题。K 均值聚类算法实际可看作是一个优化问题，因此可采用模拟退火算法对其进行优化，改进 K 均值算法的局限性，从而使算法跳出局部最优解，达到全局最优解。

2.3 结合模拟退火与 K 均值聚类的入侵检测算法

为克服 K 均值聚类算法易陷于局部极值的缺陷，本文利用模拟退火算法的全局寻优能力改进 K 均值算法，并应用于网络异常检测，以提高入侵检测算法的检测率。算法将基本 K 均值算法的聚类结果作为初始解，初始目标函数值作为初始温度，对当前解重复“产生新解-计算目标函数差-接受或舍弃新解”的迭代过程，并逐步降低温度值。算法终止时，当前解为近似最优解。这种算法开始时以较快的速度找到相对较优的区域，然后进行更精确的搜索，最终找到全局最优解。

然而模拟退火算法优化时间较长，当问题规模增大时，会因运算时间太长而使算法丧失可行性。为此，本文借鉴混乱松驰并行的特点，把概率接受新解的思想引入公共存储区的最优解接受中，并将传统模拟退火算法中的一条 Markov 链分裂为在一定时间内独立生长的多条 Markov 链，以获得可扩展的并行性。算法同时结合了 Powell 法则，既可跳出局部极值点，又可加快优化速度，提高局部收敛性能。在基于并行模拟退火与 K 均值聚类的入侵检测系统设计中，首先用 K 均值算法产生最优解 W_0，将其存储在公共存储区，给定公共存储区温度 t_g、初始值 t_{g0}、终值 t_{ge}，则每个节点执行如下算法。

步骤 1　输入系统数据并设定初始温度 t_{g0}、最终温度 t_{ge}、扰动次数 M 及降温系数 α，为使温度下降不至过快，α 取值于区间(0,1)，且一般接近于 1，设定退火代数 $j=0$；

步骤 2　对网络活动数据集进行 K 均值聚类，将聚类划分结果作为初始解 W_0，计算当前状态下目标函数值 $E_j=E_0$，则有 $t_{g0}=E_j$；

步骤 3　将循环计数变量 loop 置 0；

步骤 4　数据样本归类，计算新的聚类中心，loop 加 1；

计算新状态下目标函数 E_{j+1}，若 $E_{j+1}<E_j$，则接受新状态；若 $E_{j+1}\geqslant E_j$，求概率 $P=e^{\frac{(E_{j+1}-E_j)}{t_j}}$，$t_j$ 为当前温度，利用混沌序列产生一个随机概率 Q，$Q\in[0,1]$，若 $P\geqslant Q$，则接受新状态；否则，不接受新状态，以当前状态继续迭代；

步骤 5　以概率 $P(t_j)$ 调用 Powell 法；若满足抽样稳定准则，则转步骤 6；否则转步骤 4；

步骤 6　调用 Powell 法对当前最优解 W_j 进一步优化；

步骤 7　强制降温 $t_{j+1}=\alpha t_j$；

步骤 8　每经过 M 次退温后与公共存储区通信，若满足 *Tsallis* 准则，则更新公共存储区的最优解；否则，若扰动次数 $M<$loop，则 M 加 1，并以公共存储区中最优解为新状态继续循环；

步骤 9　公共区温度 t_g 退温；

步骤 10　若 loop$>M$，则令 loop$=0$，然后温度 t_j 回火；

步骤 11　若算法满足准则 $t_g<t_{ge}$，算法终止；否则，转步骤 4。

2.4 决策准则

在现实网络环境中，正常实例的规模远大于入侵行为数

目，因此入侵行为产生的记录在整个系统与网络行为记录集中只占很小一部分。由于入侵行为和正常行为之间存在较大的差异，在有入侵发生时，系统或进程将表现出异常行为。正常行为与异常的特性不同，它们应处于不同的聚类之中，于是可以把包含异常连接记录的聚类标记为异常聚类，而将包含正常连接记录的聚类标记为正常聚类。由于正常数据远远多于异常数据，因此可以根据聚类中所包含的数据的多少来识别它们。设由以上算法得到 k 个聚类簇中各类的样本数为 num_i，其中 $i=1,2,\cdots,k$，给定阈值 T，如果各聚类中样本数 $num_i \geqslant T$，则标记第 i 个类为“正常”类型；否则标记为“攻击”类型。由于正常数据可能被分成较小的子类，因此给各类加标记时还应考虑各类之间的距离。若一个类的样本数目较小且远离其他的类，则为该类标记为“攻击”类型，而为无法确定的类标记为“可疑”类型。在对训练集进行聚类分析，并加了类型标记后，就可对测试集中的数据进行测试，判断这个样本实例离哪个类最近，就将这个最近的类标记赋予该样本。

若已知训练集数据中异常行为的数据占正常行为数据的比例 η，$0 \leqslant \eta \leqslant 1$，测试集中所有数据对象个数为 num，则实验中可如下设定阈值 T：

$$T=\left[\frac{\eta \times num}{k}\right] \tag{3}$$

式中，k 为聚类个数，[·]表示四舍五入算子。

3 算法仿真实验与性能分析

为了检验基于模拟退火与 K 均值入侵检测算法的有效性，本文在 Visual C++环境下实现了该入侵检测算法，并进行了一些仿真实验。本文实验在 PC 上进行，PC 机配置为 3.0GHz Pentium4 处理器，1G 内存，操作系统为 Windows xp，实验数据集为 KDD CUP 1999 网络数据集[9]。该数据集中包含 22 种不同类型攻击，可以归纳为 4 种主要攻击类型：DoS(Back, land, Neptune, pod, smurf, teardrop)，U2R(Buffer_overflow, loadmodule, perl, rootkit)，R2L(ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster)，Probing(Ipsweep, nmap, portsweep, satan)。为了便于进行仿真实验，采用随机抽取的 6 组 15000 个样本数据集，其中 1 个为训练集，其余 5 个为测试集。每个数据子集中正常数据记录个数占本子集所有数据记录个数的比例约为 99%，同时各种入侵活动数据记录也相应被均匀分配到这 5 个数据子集中。表 1 给出了提出的方案在各样本集下的检测率、虚警率与误检率测试结果。

表 1 提出算法在各测试集上的检测率与误检率

测试集	检测率(%)	虚警率(%)	误检率(%)
测试集 1	98.31	0.57	6.2
测试集 2	99.47	0.86	5.7
测试集 3	98.78	0.63	6.9
测试集 4	99.01	0.79	7.1
测试集 5	98.64	0.94	5.4
Average	98.84	0.76	6.26

通过分析表 1 的数据可以看到，系统总检测率达到 98.84%，虚警率仅为 0.76%，误检率仅为 6.26%。这表明将并行模拟退火算法引入入侵检测是有效的，系统可有效地将正常行为和攻击行为区分开来，具有较高的检测率和较低的误报率。

为进一步测试算法性能，仿真实验中给出本文算法与其他基于 K 均值聚类入侵检测算法[7]的性能比较，图 1、图 2 分别给出误检率-检测率、虚警率-检测率性能比较结果。

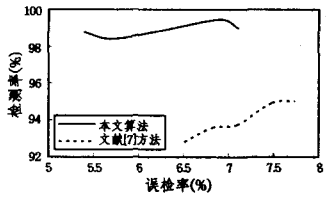

图 1 本文算法与文献[7]方法误检率-检测率性能比较

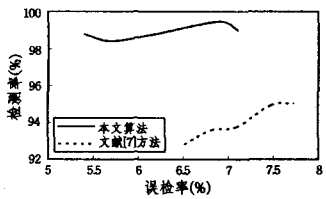

图 2 本文算法与文献[7]方法虚警率-检测率性能比较

从图 1、图 2 所示曲线可以发现，与文献[7]的入侵检测方案相比，本文算法检测率较高，并拥有更低的误检率与虚警率。这是由于本文提出的算法结合并行模拟退火的全局寻优能力，较好地克服了基于 K 均值的入侵检测算法易陷入局部极值的缺陷，提高了入侵检测准确率。

结束语 通常的基于 K 均值聚类的入侵检测算法对初始依赖性较强，易陷于局部最优。本文结合模拟退火思想与 K 均值聚类提出一种新的入侵检测算法，算法充分利用了模拟退火的全局寻优能力，对聚类分析中的聚类准则进行优化，以提高入侵检测模型的准确率和执行效率，并通过采用并行模拟退火算法加快了算法收敛速度。仿真实验结果表明，本方案具有较高的正确率、低的误检率和漏检率，可应用于实时环境网络入侵检测。

参 考 文 献

[1] Anderson J P. Computer Security Threat Monitoring and Surveillance [R/OL]. http://csrc.nist.gov/publications/history/ande80.pdf, 1980

[2] 许毓珊. A Hybrid IDS Framework via Descision Trees and SVMs[D]. 台北：台湾科技大学，2006：7-9

[3] 饶鲜，董春曦，杨绍全. 基于支持向量机的入侵检测系统 [J]. 软件学报，2003，14(4)：798-803

[4] Lee W K, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Models [C]// Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, California, USA: IEEE Computer Society, 1999: 120-132

[5] Shun J, Malki H A. Network Intrusion Detection System Using Neural Networks[C]// Proc. of Fourth International Conference on Natural Computation(ICNC '08). Jinan, China, Oct. 2008, 5: 242-246

[6] 王春枝，金伟健. 基于危险理论与数理统计的入侵检测模型 [J]. 计算机工程与应用，2008，44(11)：136-138

[7] 谷保平，许孝元，郭红艳. 基于粒子群优化的 k 均值算法在网络入侵检测中的应用 [J]. 计算机应用，2007，27(6)：1368-1370

[8] 康立山，谢云，尤矢勇，等. 非数值并行算法-模拟退火算法 [M]. 北京：科学出版社，2000：114-131

[9] KDD Cup 1999 Data [EB/OL]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 2009-09-08

[10] 孙亮，代存杰，张克云. 新型混合粒子群优化算法[J]. 重庆工学院学报：自然科学版，2008，22(2)：146-149