

入侵检测系统可信问题研究及改进方法

赵晶莹,王德高,王玲芬

(大连民族学院 计算机科学与工程学院,辽宁 大连 116600)

摘要: 误报率和漏报率影响入侵检测系统检测结果的可信性. 通过从理论上分析误报和漏报产生的原因,提出了多检测系统协同工作提高检测可信度的方法. 多检测系统结果融合时采用推进贝叶斯分类方法,给每个检测模型不同的权值,将分类结果加权求和,选择值最大的作为最终分类. 实验分析表明,该方法降低了系统的漏报率和误报率,提高了报警的可信度.

关键词: 入侵检测系统;误报率;漏报率;推进贝叶斯方法

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2010)02-0115-04

Study of Creditability on Intrusion Detection System

ZHAO Jing-ying, WANG De-gao, WANG Ling-fen

(Department of Computer Science and Engineering, Dalian Nationalities University, Dalian 116600, China)

Abstract: False positive rate and false negative rate affected the detection creditability of intrusion detection systems (IDS). A method of multi-IDS cooperation to improve detection creditability was presented after analyzing false negative rate and false positive rate of IDS. The result fusion based on boosting Bayesian classification algorithm, which put different weights on single IDS and sum the result, then choose the greatest one. The experiments show that the method can reduce the false positive rate and false negative rate, then improve the detection creditability.

Key words: intrusion detection system; false positive rate; false negative rate; boosting Bayesian

1 引言

入侵检测系统(IDS)是目前保障网络安全的一种重要手段,但误报率和漏报率一直是影响其检测结果可信性的一个主要问题. 误报是指把系统的正常行为误判为入侵行为进行报警,漏报是指系统把某些入侵行为误判为正常行为而没有报警. 要提高入侵检测系统的报警可信性,必须尽可能降低检测的误报率和漏报率^[1-2].

2 入侵检测系统的可信问题

对于入侵检测系统,期望最大限度把系统中的入侵行为和正常行为区分开来,这主要取决于入侵检测系统对正常行为的描述方式、检测模型与检测算法的选择. 入侵检测系统可视为一个简单的二值假设检验

问题. 为便于分析,采用数学语言来描述. 假设 I 与 $\bar{I}$ 分别表示对目标系统的入侵行为和正常行为, A 代表检测系统发出了入侵报警, $\bar{A}$ 表示检测系统没有报警. 检测率指受到入侵攻击时,检测系统能够正确报警的概率,可表示为 $P(A|I)$. 误报率指检测系统在检测时出现误报的概率 $P(A|\bar{I})$,漏报率是指检测系统出现漏报的概率 $P(\bar{A}|I)$,且有 $P(\bar{A}|I) = 1 - P(A|I)$, $P(\bar{A}|\bar{I}) = 1 - P(A|\bar{I})$ ^[3].

入侵检测系统的可信度可用两个可信概率来表示: (1) 检测系统报警可信概率,由 $P(I|A)$ 给出,即检测系统报警时,目标系统实际受到入侵攻击的概率. 该参数小于1时,说明检测系统存在误报现象; (2) 检测系统不报警可信概率,由 $P(\bar{A}|\bar{I})$ 给出,即检测系统没有报警时,目标系统处于安全状态(没有受到入侵攻击)的概率. 该参数小于1时,说明

收稿日期: 2008-12-24; 修回日期: 2009-02-23

基金项目: 国家自然科学基金项目(60573124)

检测系统存在漏报现象.

显然,为了入侵检测系统更有效,系统的这两个参数值越大越好.应用贝叶斯定理可以求出入侵检测系统可信度的概率 $P(I/A) = \frac{P(I)P(A/I)}{P(I)P(A/I) + P(\bar{I})P(A/\bar{I})}$. 同理, $P(\bar{I}/\bar{A}) = \frac{P(\bar{I})(1 - P(A/\bar{I}))}{P(\bar{I})(1 - P(A/\bar{I})) + P(I)(1 - P(A/I))}$. 根据上面的分析,针对给定的实验数据或具体环境,可以通过已经获得的数据统计以及系统仿真获得 $P(I)$ 、 $P(\bar{I})$ 、 $P(A/I)$ 、 $P(A/\bar{I})$ 的先验概率,进而计算出 $P(I/A)$. 在一般情况下,入侵行为出现的概率是非常低的,即 $P(I) \ll P(\bar{I})$, 并且 $P(I) + P(\bar{I}) = 1$, 所以,在计算 $P(I/A)$ 式子中,分母主要取决于误报率 $P(A/\bar{I})$ 的影响. 因此,降低误报率,可以提高报警的可信度. 同理,降低漏报率,也可以提高报警的可信度.

3 入侵检测系统的误报和漏报问题分析

3.1 异常入侵检测系统误报和漏报问题

入侵检测一般分为异常入侵检测系统和误用入侵检测系统. 异常检测系统也称为基于统计行为的入侵检测系统. 其方法为:检测系统首先建立被检系统的正常行为轮廓,当检测系统发现被检系统的行为偏离正常轮廓的范围超出某个阈值时则认为有入侵发生. 但当某个入侵不会导致异常行为或者导致的异常行为偏离正常轮廓的范围很小,未超出检测阈值时,异常检测系统将会产生漏报. 同时,由于检测系统建立的正常行为轮廓不完善,不能涵盖所有正常活动所致,异常检测系统将会产生误报^[4-6].

3.2 误用入侵检测系统的误报和漏报问题

误用入侵检测也称为基于规则或知识的入侵检测,就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为. 由于缺乏对未知入侵活动或已知入侵活动的变异的先验知识,所以对新型攻击会有比较高的漏报率. 可能产生误报的原因是:入侵者可以通过人为地构造网络数据包来匹配攻击特征,从而控制入侵检测系统引起大量误报,麻痹系统管理员以利于后面的攻击^[7].

4 采用多入侵检测系统协作提高检测可信性

4.1 对采用相同检测机制的检测系统的协作

(1) 基于误用的入侵检测检测系统的协作

设检测系统 A 、 B 以及二者共同工作时的整体检测率分别为 p_{dA} 、 p_{dB} 及 p_d , 通过检测系统的能力互补,可以得到: $p_d = 1 - (1 - p_{dA})(1 - p_{dB}) = p_{dA} + p_{dB}(1 - p_{dA}) = p_{dB} + p_{dA}(1 - p_{dB})$. 若检测系统 A 、 B 的检测率小于 1, 必有 $p_d > p_{dA}$, $p_d > p_{dB}$. 因此, A 和 B 的协作可以提高整个检测系统的检测率,降低漏检率 $(1 - p_d)$, 增加被保护系统的安全性.

(2) 基于异常的入侵检测检测系统的协作

设检测系统 A 、 B 以及二者共同工作时的整体检测率分别为 p_{dA} 、 p_{dB} 及 p_d , 且对应的误报率分别为 p_{fA} 、 p_{fB} 及 p_f . 判定规则如下:两个检测器都认为正常时,判定为正常;若只有一个检测器认为正常,则进行报警或作进一步分析;两者都认为是异常时,才确定是异常. 一个正常的行为,只有两个检测系统都认为是入侵时才出现误报,所以针对检测系统,误报率有: $p_f = p_{fA} \times p_{fB}$, 并且 $p_f \leq p_{fA}$, $p_f \leq p_{fB}$. 因此,可以得出两个异常检测系统的协作可以有效降低系统的误报率. 针对漏报率 $(1 - p_d) = (1 - p_{dA}) + (1 - p_{dB})(1 - (1 - p_{dA})) = (1 - p_{dB}) + (1 - p_{dA})(1 - (1 - p_{dB}))$, 即 $p_d = p_{dA} \times p_{dB}$. 由于 $0 \leq p_{dA} \leq 1$, $0 \leq p_{dB} \leq 1$, 所以, $p_d \leq p_{dA}$, $p_d \leq p_{dB}$, 降低了漏报率.

4.2 对采用不同检测机制的检测系统的协作

由于不同的检测机制从不同的角度考虑入侵检测问题,所以,可以采用不同的机制检测系统协同工作的模式提高检测的可信性. 设系统 A 为基于异常的检测系统, B 为基于误用的检测系统. N 表示被保护系统的正常行为集合. 系统 A 把系统特征集合轮廓集合 A 之外的行为 $\bar{A}$ 都看作是异常的行为,而系统 B 则把已知入侵知识对应的入侵特征集 B 之外的行为 $\bar{B}$ 都看作是正常行为. 协作时,假设检测系统 B 能够检测出所有的已知入侵且具有很低的误报率,那对于已知入侵攻击手段,系统 B 可以用来验证系统 A 的检测结果,以降低 A 的误报率. 两个系统的协作分以下几种情况: (1) 当检测系统 A 和 B 同时检测到入侵时 ($\bar{A} \cap B$), 认为系统受到了入侵. (2) 当系统 A 检测到入侵,系统 B 认为正常时,则只是给出警告或进一步分析系统表现的特征. (3) 系统 A 认为是正常时,不验证. 根据上面的规则,系统 A 在验证模式下工作时,只有集合 $(\bar{A} \cap B \cap N)$ 所表示的系统正常行为可能被错误判为入侵行为. 而集合 $(\bar{A} \cap \bar{B} \cap N)$ 中的系统正常行为,在 A 系统单独工作时,被误判为入侵行为,但当系统 B 对其检测结果进行验证时,只是把它们判为可疑的行为,不

把它们作为入侵情况看待,从而降低了系统A的检测误报率.同理,可以证明,若采用系统A对系统B检测为正常的结果进行验证,就可以降低B的漏检率,提高检测率.

由上面的分析,若一个检测系统集成多个不同的检测子系统,这些检测系统的协作可以有效提高整个检测系统的性能,即能够降低检测的漏检、误报率,提高检测的可信性.

4.3 基于推进的贝叶斯分类法的多检测器结果融合决策方案

对于多个检测器的检测结果,最简单的判断方法是采用 K/N 投票表决法,但这种决策方法不仅需要选择 K 的取值来期望获得的最大的概率,而且没有考虑不同检测器性能的影响.针对这个问题,可以采用基于贝叶斯分类器的多检测器结果融合方案.利用多个检测子系统 $D_1, D_2, \dots, D_N$ 对同一个系统进行检测.当 N 个系统同时工作时,检测结果组成长度为 N 的一维向量 $(a_1, a_2, \dots, a_n)$,其中 $a_i \in (A, \bar{A})$ 作为输入,分别计算该检测向量出现时,目标系统正常的概率 $p(I/a_1, a_2, \dots, a_n)$ 或受到入侵的概率 $p(\bar{I}/a_1, a_2, \dots, a_n)$,通过收集这 N 个检测子系统的检测结果向量,并根据实际系统行为是否正常,获得 N 维检测结果的数据集,将其作为训练数据创建贝叶斯推理的结果融合决策分类.假设参与结果融合的检测器具有检测独立性,则可以给出如下的分类器定义: $v_{NB} = \arg$

$\max_p(v) \prod_{i=1}^N p(a_i/v) (v \in I, \bar{I})$. 因此,只需要通过比较各检测子系统的检测结果组成的向量属于“正常”的后验概率和属于异常的后验概率的大小,就可以判断系统是否真的遭到了入侵攻击.

虽然在理论上,贝叶斯分类法有最小的出错率,但是,在实践中贝叶斯分类相比其它分类法并没有优势.这主要是由于对其应用的假设条件的不准确性造成的.在这里,文中将数据挖掘中的推进技术用于贝叶斯分类,提高了检测正确率.

推进算法的主要思想是:根据每个分类模型的正确率,给予它不同的权值(正确率越高,权值越大),将分类结果加权求和,选择值最大的作为最终分类.针对入侵检测系统的分类模型生成算法主要流程如下:

(1) 对有 s 个样本的集合 S ,重复 k 次,每次从 S 中有放回的任意抽取总样本数的 γ_s ($0 < \gamma < 1$)作为训练集 s_t (t 为整数)且将 a_s ($0 < a < 1$)作为测

试集 E_t (t 为整数且 $1 \leq t \leq k$). 权值 w_t 初始为1 (t 为整数且 $1 \leq t \leq k$).

(2) 将抽取的 k 组样本作为 k 组训练集分别对当前的分类模型进行训练,这样一共得到 k 组新分类模型 c_i ($1 \leq i \leq k$).

(3) 随机从测试集选择样本 X 作正确性测试,将每个分类法 c_i 产生的类预测送到表决模块,将得票最多的类作为分类结果,将分类结果与 X 所属类相同的分类法的权值 w_i 加1.重复第(3)步 n ($n < k$)次,转(4).

(4) 定义阈值 u ($u < n$),将权值小于 u 的分类法 c_i 去除,得到最终分类模型.

对于推进算法中的参数 γ 和 u ,用户可以根据需要设定.如果用户希望测试集小一点,可以将 γ 变大,反之亦然;如果用户希望算法生成较多的分类模型,可以将 u 设小一点,反之亦然.

4.4 多检测器数据融合的检测模型

多检测器数据融合的检测模型如图1所示.

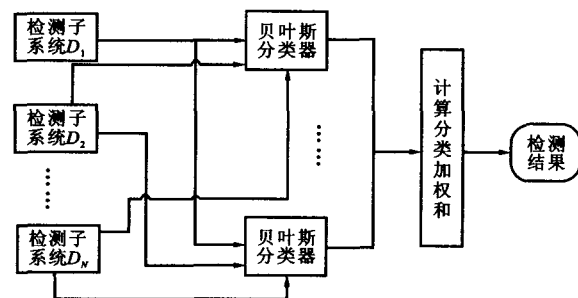


图1 多检测器数据融合的检测模型

5 实验及结果分析

实验数据选用KDDcup1999网络数据集,利用其中的TCP/IP数据测试本系统.为了方便实验从中选取了10000条数据,这些数据中包含100条异常数据.从实验数据中抽取4组数据组成3个训练子集 (T_1, T_2, T_3) 和一个测试集 E_1 .为了便于比较,采用了3个开放源代码的IDS系统:Snort、Bro、Dragon IDS,用到的网络数据包截取程序为libpcap.各IDS采用统一的数据接口,将检测到的相关信息送到融合中心.本系统开发环境为RedHat9.0,用Java语言编写代码,数据库为MySQL5.0.共选用5天时间测试,各检测器的漏报率如表1,误报率如表2.

通过对比实验数据可以发现,文中方法的漏报率和误报率与其他IDS系统相比均有所改善,本系统能较大提高检测的准确性和可靠性.

表 1 各检测器漏报率对比表

时间	snort	Bro	Dragon	文中方法
1	4.53	4.28	5.47	3.26
2	4.94	4.73	5.38	3.18
3	4.36	4.45	5.32	3.05
4	4.10	4.51	5.09	3.30
5	5.21	5.56	5.96	4.16

表 2 各检测器误报率对比表

时间	snort	Bro	Dragon	文中方法
1	2.18	3.23	3.48	1.36
2	2.42	3.36	3.91	1.65
3	2.37	3.45	3.56	1.41
4	2.30	3.04	3.40	1.63
5	1.91	3.15	3.28	1.22

6 结束语

文中分析了当前入侵检测系统存在的可信问题及误报和漏报产生的原因,给出了通过采用多检测系统协同工作的模式提高可信度的理论分析和方法,多检测系统融合时采用推进的贝叶斯分类方法.实验分析表明,该方法可以降低系统的漏报率和误报率,可以提高报警的可信度.如何进一步融合各种

技术,更好的降低入侵检测系统的报警率还有待于进一步研究.

参考文献:

- [1] 陈晓梅. 入侵检测产品的评价研究[J]. 微电子学与计算机, 2005,22(9):74-76.
- [2] 杨义先,钮心忻. 入侵检测理论与技术[M]. 北京:高等教育出版社,2006.
- [3] 闫巧,喻建平,谢维信. 入侵检测系统的可信问题[J]. 计算机研究与发展,2003,40(8):1203-1208.
- [4] 苏璞睿,冯登国. 基于数据融合的分布式入侵检测系统研究[J]. 电子学报,2006,36(10):1809-1811.
- [5] 廖年冬,田盛丰. 入侵检测规则动态生成研究[J]. 北京交通大学学报,2008,32(5):116-120.
- [6] Chowalit Tinnagonsutibout, Pirawat Watanapongse. A novel approach to process - based intrusion detection system using read sequence finite state automata with inbound byte proler[C]//ICEP2003. Spain: Catalonia, 2003.
- [7] 高丹,彭新光. 基于 DET 曲线的入侵检测评估方法[J]. 微电子学与计算机, 2008,25(8):134-135.

作者简介:

赵晶莹 女,(1978-),讲师.研究方向为网络安全、数字图像处理、模式识别.

王德高 男,(1969-),教授.研究方向为网络与信息安全.

王玲芬 女,(1960-),副教授.研究方向为操作系统、网络安全.

(上接第 114 页)

- [2] Inho Ko, Jongmoon Kim, Sanghyun Cho Lee. A 19mW 2.6mm L1/L2 dual-band COMS GPS receiver[J]. IEEE Journal of Solid State Circuits,2005,40(7):1414-1425.
- [3] Calvo B, Celma S, Sanz M T. High-frequency digitally programmable gain amplifier[J]. Electronics Letters, 2003,39(15):1095-1096.
- [4] Wang Ziqiang, Chi Baoyong, Wang Zhihua. An Overview CMOS variable gain amplifier[J]. Microelectronics,2005, 35(6):612-617.
- [5] Behzad Razavi. Design of analog CMOS integrated circuits [M]. New York: Mc Graw Hill,2001.

作者简介:

张佃伟 男,(1982-),硕士研究生.研究方向为模拟电路的设计与测试.

文治平 男,研究员,硕士生导师.研究方向为超大规模集成电路的设计与测试.

李卫民 男,研究员,硕士生导师.研究方向为超大规模集成电路的设计与测试.

文武 男,高级工程师.研究方向为射频与模拟集成电路的设计与测试.