第 34 卷 第 15 期 计 算 机 工 程 2008 年 8 月
Vol.34 No.15 Computer Engineering August 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)15—0229—02 文献标识码：A 中图分类号：TP393.08

BIC 评分贝叶斯网络模型及其应用

王书海[1,2]，刘 刚[2]，綦朝晖[2]
(1. 天津大学计算机科学与技术学院，天津 300072；2. 石家庄铁道学院计算机与信息工程分院，石家庄 050043)

摘 要：针对入侵检测系统漏报率、误报率高的缺点，以贝叶斯信息标准(BIC)评分函数为尺度，结合爬山搜索算法，降低朴素贝叶斯网络模型的强独立性假设，提出更符合实际情形的 BIC 评分贝叶斯网络模型。对模型进行验证和性能分析，实验结果表明，基于 BIC 评分函数的贝叶斯网络模型对行为特征渐变的 DoS 攻击和刺探攻击具有较高识别率。

关键词：贝叶斯网络；BIC 评分函数；入侵检测系统

BIC Scoring Bayesian Network Model and Its Application

WANG Shu-hai[1,2], LIU Gang[2], QI Zhao-hui[2]
(1. School of Computer Science and Technology, Tianjin University, Tianjin 300072;
2. School of Computer Science and Information Engineering, Shijiazhuang Railway Institute, Shijiazhuang 050043)

【Abstract】 Because of the high false acceptance rate and false alarm rate of IDS, this paper proposes a Bayesian Information Criterion(BIC) scoring Bayesian network model, which makes use of BIC scoring function and mountain-climb searching algorithm, and weakens the strong independence relation assumption of Naive Bayes. It offers an experimental study and analysis, which shows that this improved Bayes network model enhances the detection precision in recognition of DoS and Probe attacks

【Key words】 Bayesian network; BIC scoring function; intrusion detection system

1 概述

现有入侵检测系统(Intrusion Detection System, IDS)存在很多缺点，例如在高速网络环境中性能较低、漏报率和误报率较高、检测深度和广度不足及 IDS 自身的安全问题等[1]。

多数入侵攻击没有明显特征，难以用明确的特征值来表示，导致基于误用的入侵检测技术失去效果。例如 DoS 攻击的数据包通常是正常的，但数量巨大，造成服务器阻塞，是量变到质变的典型过程。捕捉到的数据包可能出现异常现象，比如大量数据包的源 IP 地址来自可疑网络，目的 IP 地址是相同主机，或在短时间内有较多数量的数据包为 icmp 扫描数据包等，这些异常现象对入侵攻击的判断以概率形式存在。如果仅依靠上述异常现象的一个或几个方面简单地判断是否为入侵，可能导致误报或漏报。贝叶斯网络具有综合先验信息和样本信息的能力，能通过大量数据学习，揭示隐藏在不确定知识背后的概率关联，从而提高入侵检测的完备性和准确性[2]。

2 贝叶斯网络模型

贝叶斯网络是基于概率推理的数学模型，采用图形化网络结构直观地表达变量的联合概率分布及其条件独立性。一个贝叶斯网络是一个有向无环图(Directed Acyclic Graph, DAG)，由代表变量节点及连接这些节点的有向边构成。用符号 $B(G, P)$表示一个贝叶斯网络，它由 2 个部分构成：

(1)一个具有 N 个节点的有向无环图 G。图中的节点代表随机变量，节点间的有向边代表节点间的相互关联关系。节点变量可以是任何问题的抽象，用以代表属性、状态、客体、命题或其他实体，如测试值、观测现象等。

(2)一个与每个节点相关的条件概率表(Conditional Probability Table, CPT)。没有任何父节点的节点概率为其先验概率。因为有了节点及其相互关系、条件概率表，所以贝叶斯网络可以表达网络中所有节点(变量)的联合概率分布。

贝叶斯网络模型的关键是确定节点的联合概率分布。不同贝叶斯网络模型的区别在于它们以不同方式求解该联合概率分布。其中，朴素贝叶斯网络(Naive Bayes Network, NBN)是包含一个根节点、多个叶节点的树状贝叶斯网络[3]。如图 1 所示，其中，叶节点 $A_1, A_2,\cdots, A_n$ 是属性变量，描述待分类对象的属性，根节点 C 是类别变量，描述对象类别。

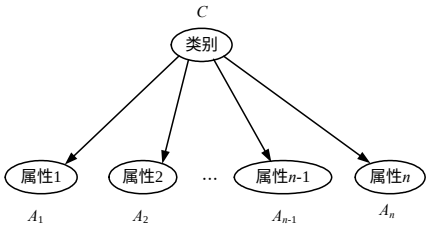

图 1 朴素贝叶斯网络

朴素贝叶斯网络包含一个局部独立假设，即给定变量 C，各个属性变量 A_i 相互条件独立，因此，联合概率分布满足如下等式：

$$P(C, A_1, A_2,\cdots, A_n) = P(C)\prod_{i=1}^{n} P(A_i \mid C)$$

该独立性假设使朴素贝叶斯网络的计算效率较高，但由于朴素贝叶斯网络要求各个属性之间完全独立，因此进行网络攻击行为的检测时，每个检测对象行为的分量应该是相互

基金项目：河北省自然科学基金资助项目(F2005000515)
作者简介：王书海(1969－)，男，教授、博士，主研方向：网络信息安全；刘 刚，硕士研究生；綦朝晖，讲师、博士
收稿日期：2008-07-12 **E-mail：**wangsh@sjzri.edu.cn

独立的，即各个属性变量 A_i 之间相互独立。实际操作中不可能完全满足上述要求，为了克服完全独立性假设带来的差异，本文以 BIC 评分函数[4]为尺度，结合爬山搜索算法[4]，提出更符合实际情形的贝叶斯网络模型。

3 基于 BIC 评分的贝叶斯网络模型

基于 BIC 评分的贝叶斯网络结构学习常采用如下方法：

(1)基于评分-搜索的学习方法。该方法过程简单规范，但搜索空间大，一般在节点有序的前提下，根据评分算法的可分解性进行局部确定或随机搜索(完全搜索是 NP 问题)。

(2)基于依赖分析的学习方法。该方法过程较复杂，但在一些假设下学习效率较高，且能获得全局最优结构。但在现有依赖分析方法中，冗余边检验在确定边的方向之前进行，无法准确地确定切割集，导致大量高维条件概率计算，通常不能定向所有边。这些缺点降低了学习效率和准确性。

本文主要研究基于 BIC 评分函数的评分搜索算法，它是在大样本前提下对边缘似然函数的一种近似，具有明确的直观意义且便于使用。

设 ξ 是一个由 n 个变量 $X=\{X_1, X_2,\cdots, X_n\}$ 组成的贝叶斯网络结构，其中，节点 X_i 共有 r_i 个取值 $1, 2,\cdots, r_i$，父节点 $\pi(X_i)$ 的取值共有 q_i 个组合，即 $1, 2,\cdots, q_i$ (若 X_i 无父节点，则 $q_i=1$)。ξ 相对数据集 $\Im$ 的优劣可用一个评分函数来度量。基于模型结构 ξ 的 BIC 评分[2]如下：

$$BIC(\xi \mid \Im) = \sum_{i=1}^{n}\sum_{j=1}^{q_i}\sum_{k=1}^{r_i} m_{ijk} \lg \frac{m_{ijk}}{m_{ij*}} - \sum_{i=1}^{n} \frac{q_i(r_i-1)}{2} \lg m$$

BIC 评分的第 1 项是模型 ξ 的优参对数似然度，它度量的是结构 ξ 与数据 $\Im$ 的拟合度。第 2 项是一个关于模型复杂度的罚项。若仅依据优参似然度来选择模型，会选到最复杂的完全贝叶斯网络，导致过度拟合。由于附加了一个复杂度的罚项，因此 BIC 能避免过度拟合。基于 BIC 的评分选择模型需要选择与数据拟合且较简单的模型。

利用 BIC 评分函数搜索优化模型时，本文采用爬山搜索算法，该算法的目标是找出评分最高的模型。它从一个无边的初始模型出发开始搜索，在搜索的每一步，首先用搜索算子对当前模型进行局部修改，得到一系列候选模型，然后计算每个候选模型的评分，并将最优候选模型与当前候选模型比较。若最优候选模型的评分大，则以它作为下一个当前模型，继续搜索；否则停止搜索，返回当前模型。

3 个搜索算子，即加边、减边和转边如图 2 所示。

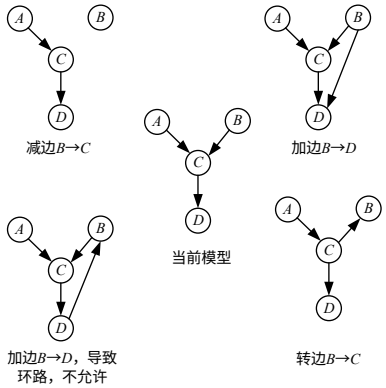

图 2 搜索算子

加边是在网络结构中添加一条边，减边是减去一条边，转边是把一条边的方向翻转。加边算子和转边算子的使用有一个前提，即不能在网络中形成环路。如果在网络中出现环路，环路中的节点就会互为父节点，在结构学习时，将形成无限循环。

4 实验过程及性能评价

4.1 数据预处理

实验使用的训练集和测试集来自第 5 届知识发现和数据挖掘国际会议为测试基于网络入侵检测系统所提供的数据集，该数据集提供的是网络连接数据，作为训练和测试入侵检测模型具有一定权威性[5]。该数据集中每条网络连接记录由 42 个属性构成，其中，34 个属性为连续值，8 个属性为离散值。每条网络连接记录由 41 个特征属性和 1 个类标记组成，例如 duration, protocol_type, service, flag,⋯, class。

为了处理方便，对数据集中连续型特性的取值要做离散化处理。本文中的数据离散采用等频区间法[6]。连续变量离散部分结果如表 1 所示。

表 1 数据集离散结果

特性名称	离散化区间
duration	0, (0, +∞)
src bytes	0, (0, 1 031), (1 031, +∞)
dst host rerror rate	0, (0, 0.03), (0.03, 0.37), (0.37, 1), 1
dst host srv rerror rate	0, (0, 0.02), (0.02, 0.33), (0.33, 1), 1

4.2 实验结果

在实验过程中，将入侵检测的每个特征变量(例如协议类型、服务类型、传输的字节数等)和由这些变量推理得到的攻击分类(如 pod 攻击、land 攻击、smurf 攻击等)分别作为贝叶斯网络的一个节点，结合 BIC 评分函数构造优化的贝叶斯网络模型。利用这个模型诊断推理数据集中的攻击类型，将结果分别与推理数据集的校正集进行比对，统计漏报率、误报率和正确率。通过相同的推理数据集和推理算法，得到的各项指标如表 2 所示。

表 2 BIC 评分贝叶斯网络模型的攻击识别率

攻击名称	识别率
ipsweep	0.980 392
land	0.555 556
neptune	0.987 948
nmap	0.952 381
normal	0.992 764
pod	0.908 046
portsweep	0.923 729
satan	0.853 464
smurf	0.998 385
teardrop	1.000 000
unknown	0.008 918

BIC 评分贝叶斯网络模型的漏报率、误报率、正确率分别为 0.076 196, 0.010 249, 0.913 555。

4.3 结果分析

由实验结果可以看出，本文 BIC 评分贝叶斯网络模型能较好地识别大部分 DoS 攻击和刺探攻击，主要原因如下：

(1)本文模型能克服朴素贝叶斯网络模型的强独立性假设带来的影响，更符合实际情形，对行为特征渐变、状态变化过程相关性较强的 DoS 攻击和刺探攻击具有很高识别率。

(2)在数据离散化工作中，本文采用等频区间法进行数据集的简化处理。等频区间法没有考虑各个特性节点之间的相关性，但本文 BIC 评分贝叶斯模型以 BIC 评分函数的形式弥补了数据简化处理过程中所散失的相关性，从而提高模型的入侵检测能力，使其更符合实际情形。

此模型对少部分 DoS 攻击，如表 2 中的 land 攻击等行为特征变化较大的攻击事件的识别率较低。主要原因是行为特

（下转第 233 页）