学 术 论 文

基于模糊概率赋值的新型贝叶斯异常检测模型

金　舒，刘凤玉
（南京理工大学计算机科学与技术系，南京　210094）

［摘要］　提出了一种结合模糊决策与贝叶斯方法的异常检测模型，该模型将系统中与安全相关的事件进行分类，并以模糊隶属度函数的形式给出各类事件发生异常的实时置信度。异常检测系统综合某时刻所有实时概率取值，做出贝叶斯决策。同简单使用阈值方法的贝叶斯入侵检测模型相比，采用了模糊概率赋值的贝叶斯异常检测模型，在提高对问题描述的精确性同时，由于它对多种类型安全相关事件提供支持而具有更好的适应性，可以更全面地对更复杂的系统行为进行建模。

［关键词］　入侵检测系统；异常检测；模糊概率赋值；贝叶斯置信网络
［中图分类号］　TP393.08　　［文献标识码］　A　　［文章编号］　1009－1742（2007）06－0058－06

1　前言

随着 Internet 在人类社会活动中日益广泛使用，安全性问题逐渐暴露出来。不断产生的多种形式的网络入侵、网络攻击，损害了网络用户的利益。网络安全系统主要有静态安全系统和动态安全系统，但是这些系统在较好地保证授权用户安全的同时，并不能对合法用户的攻击行为进行识别或对入侵者进行追踪。

入侵检测系统既能检测来自系统内部的攻击，同时也能对系统的运行情况进行监控，并对可能发生的入侵行为做出实时响应，以避免攻击的发生或尽可能减小攻击的危害。入侵检测系统按其执行入侵检测工作的不同，可分为 2 种类型[1,2]：误用（misuse）入侵检测系统；异常（anomaly）入侵检测系统。误用检测系统具有较高的效率但不能检测未知种类的网络入侵，漏检率（false negative）较高。异常检测系统可以检测出未知种类的入侵，通常较难实现且误检率（false positive）较高。

贝叶斯置信网络可以根据有限的先验知识及观测到的数据实时地做出最优决策[3,4]。笔者提出一种异常检测模型，综合某时刻各采样点的信息，可得出系统是否正受到某种方式的入侵。同使用阈值方法的贝叶斯入侵检测模型[5～9]相比，采用了在连续空间上进行模糊概率赋值的贝叶斯异常检测模型，提高了对问题描述的精确性，具有更好的适应性，可以更加全面地对系统正常运行状态下的各种复杂的用户行为进行建模。

2　异常检测模型

异常入侵检测系统中，假设入侵活动是异常活动的子集，并用统计方法建立系统正常运行状态的行为特征轮廓（Profile），在此基础上，通过检测系统实时运行情况与该模式之间的明显差异来发现入侵。如图 1 所示，异常检测系统在运行过程中不断获取系统中与安全相关的特征属性的实时数据，并分别对其进行相应的模糊概率赋值，给出各安全事件发生异常的概率，信息综合模块收集并处理这些概率值，把综合得到的结果送至决策模块，决策模块根据用户设定的宽容度范围，做出系统是否正受到入侵的决策。模型中，对系统正常运行状态的行为建模所形成的知识，以模糊隶属度函数的形式存

［收稿日期］　2006－02－28；修回日期　2006－05－09
［基金项目］　国家自然科学基金资助项目（60273035）
［作者简介］　金　舒（1979－），男，江苏南京市人，南京理工大学博士研究生，研究方向：信息系统安全

于各模糊概率赋值模块中。在信息综合模块中，可以仅采用易于实现且快捷高效的简单概率算法。贝叶斯置信网络算法，因其决策基于各系统安全相关事件间的相互作用和联系，能更全面有效地综合各安全事件发生的实时概率，更精确地反映系统运行时的安全性状况。根据不同需求，结合或分别使用这两种信息综合算法，可使整个异常检测系统对不同的系统安全问题具有更好的适应性。

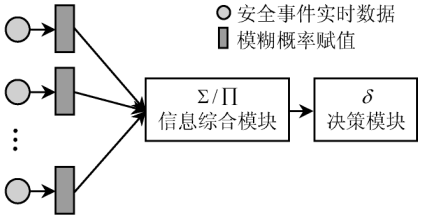

图 **1**　异常检测模型

Fig.1　Anomaly detection model

2.1　简单概率算法

系统运行状况异常事件的发生设为 I，某采样时刻系统行为异常（可能受到入侵）的确信度为 $P(I)$。系统中安全相关的特征属性集为 $\bigcup A_i$。异常检测系统的信息综合模块，对采集到的所有特征属性的实时数据，执行简单概率算法，以对系统运行的安全情况是否异常做出初步决策，并将结果送至决策模块。对于系统中的安全相关属性 A_i，异常检测系统并不认为其仅处于发生异常或不发生异常的离散二值状态，而是依据对系统正常行为进行训练所获得的参数，以及在各采样时刻与该系统属性相关的实时数值为其赋予一个连续的模糊概率值，即是否发生异常的确信度 $P(A_i)$。通过联立各安全特征属性发生异常的事件，用条件概率 $P(I/A_1, A_2, \cdots, A_n)$综合这些特征属性对系统安全状况的影响，即特征属性各自以 $P(A_i)$的确信度发生异常时系统状态发生异常的确信度。各采样时刻，特征属性 A_i 不发生异常的确信度可以简单地用 $P(\neg A_i) = 1-P(A_i)$来表示，或者同样为其赋予用模糊概率值表示的确信度 $P(\neg A_i)$。同样，条件概率 $P(\neg I/A_1, A_2, \cdots, A_n)$表示该采样点上各系统安全相关特征属性 A_i 发生异常的确信度，分别为 $P(A_i)$时系统不发生异常的确信度。不考虑各安全属性彼此间的相互影响，即各安全属性异常事件相互独立的情况下，有 $P(A_1, A_2, \cdots, A_n) = \prod_{i=1}^{n} P(A_i)$ 及 $P(A_n/I) = P(A_n/A_1, A_2, \cdots, A_{n-1}, I)$，综合这些条件有：

$$P(I/A_1, A_2, \cdots, A_n) = P(I, A_1, A_2, \cdots, A_n)/P(A_1, A_2, \cdots, A_n) = P(I)P(A_1/I)P(A_2/A_1, I)\cdots P(A_n/A_{n-1}, A_{n-2}, \cdots, A_1, I)/P(A_1, A_2, \cdots, A_n) =$$

$$P(I)P(A_1/I)P(A_2/I)\cdots P(A_n/I)/\prod_{i=1}^{n} P(A_i) =$$

$$P(I)\prod_{i=1}^{n} P(A_i/I)\Big/\prod_{i=1}^{n} P(A_i) \quad (1)$$

$$P(\neg I, A_1, A_2, \cdots, A_n) =$$

$$P(\neg I)\prod_{i=1}^{n} P(A_i/\neg I)\Big/\prod_{i=1}^{n} P(A_i) \quad (2)$$

一般有一种异常行为发生，则认为整个系统就处于受攻击状态下，即 $P(I/A_i)=1$，有

$$P(A_i/I) = P(A_i, I)/P(I) = P(A_i)P(I/A_i)/P(I) = P(A_i)/P(I),$$

$$P(A_i/\neg I) = P(A_i, \neg I)/P(\neg I) = P(\neg I/A_i)P(A_i)/P(\neg I) = [(1-P(A_i))/P(A_i)]P(A_i)/P(\neg I) = (1-P(A_i))/P(\neg I) = P(\neg A_i)/P(\neg I)。$$

在异常检测系统做出决策前，不妨设 $P(I) = P(\neg I) = 0.5$，$P(\neg A_i)$可以用 $P(\neg A_i) = 1-PA_i)$间接得到。通过计算 $P(I/A_1, A_2, \cdots, A_n)$与 $P(\neg I/A_1, A_2, \cdots, A_n)$，可以综合系统是否发生异常正反两方面的判断。把上面的结果代入式（1）和式（2），并用其的比值 R 作为系统异常与否的初步判断，有

$$R = \prod_{i=1}^{n} \frac{P(A_i)}{P(\neg A_i)} \quad (3)$$

$R>1$ 可以初步判定系统发生异常，而 $R<1$ 表示系统当前行为正常。考虑到各系统安全相关属性对安全性的决定在重要程度上不同，可以进一步依据各安全属性 A_i 对系统安全贡献的程度赋予权重因子 w_i，即采用

$$R_w = \sum_{i=1}^{n} P(A_i)w_i\Big/\sum_{i=1}^{n} P(\neg A_i)w_i \quad (4)$$

来计算其比值 R_w。各安全属性依据其对系统安全性的不同贡献，共同决定系统异常的判断结果。

2.2　贝叶斯置信网络算法

贝叶斯置信网络也称信念网、因果网，是一种基于条件概率的决策模型。其拓扑结构为有向无环图（DAG），问题空间中的待考察实体的属性在图中用一组结点来表示，相互间存在决定/依赖关系

的结点之间存在有向连接，方向由决定方（原因方）指向被决定方（结果方）。通过为这样的连接附上条件概率，贝叶斯置信网络可以精确地描述实体各属性间的相互依赖关系。利用贝叶斯置信网络做出决策，即在已知与某待考察属性相关的各属性取值的基础上，结合其与待考察属性间的条件概率关系，对待考察属性的各种可能取值赋予置信度。相较于仅考虑先验属性（即目标属性的决定属性）的简单概率方法，由于同时融合了先验属性与后验属性（决定于目标属性的属性），贝叶斯置信网络的推理结果基于更加精确细致的约束，可以在更全面使用条件的基础上做出决策。

针对异常入侵检测问题设计的贝叶斯置信网络如图 2 所示。可见，待决策（决定其各可能取值的置信度）的目标属性 X 表示系统的安全状态，取值为 I（系统行为正常）或 $\neg I$（系统行为异常）。$E_p=\bigcup E_{pi}$ 表示系统中与安全密切相关的一组先验特征属性（父属性），$E_{pi}=$ val 时，依据训练获得的模糊隶属度函数对其赋予模糊概率值 $P(X=I/E_{pi}=\text{val})$。类似地，对于决定于 X 的一组后验属性（子属性，即系统发生异常会对其取值产生明显影响的特征属性）$E_c=\bigcup E_{ci}$，用 $P(E_{ci}=\text{val}/X)$ 表示系统安全状态对它们的影响。异常入侵检测系统在综合采样时刻所有系统安全相关属性 $E=E_c\cup E_p$ 的实时数据后，依据

$$P(X/E)\propto P(E_c/X)P(X/E_p) \tag{5}$$

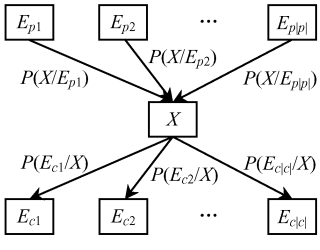

图 **2** 用于异常检测的贝叶斯置信网络

Fig.2 Bayesian belief network for anomaly detection

给出的贝叶斯置信网络的推理规则对属性 X 取值，即系统运行状态是否异常（$X=I$ 或 $X=\neg I$）做出决策。

在 $P(E_c/X)$ 的计算中，不考虑各先验属性间的相互影响，即各 E_{ci} 相互独立：

$$P(E_{c(n)}/E_{c(1)},E_{c(2)},\cdots,E_{c(n-1)},X)=P(E_{c(n)}/X),$$

计算 $r_c=P(E_c/X)$ 得到

$$P(E_c/X)=P(E_{c1},E_{c2},\cdots,E_{c|c|}\mid X)=P(E_{c1}/X)P(E_{c2}/X)\cdots P(E_{c|c|}\mid X)=\prod_{i=1}^{|c|}P(E_{ci}\mid X) \tag{6}$$

其中 $P(E_{ci}/X)$ 表示系统安全状态对各后验属性 E_{ci} 的影响，其取值既可以根据常识给出，也可以作为各后验特征属性受系统安全状态影响的敏感度参数，由系统安全管理人员定义。

如文献［3，4］中所描述，在 $P(X/E_p)$ 计算中的求和范围，是在不同先验属性（父结点）值所有可能的组合上进行，其中 P_{mn} 表示先验属性 P_m 在其值空间上的第 n 个取值。结合先验属性结点间统计独立的假设（因其间没有连接），即

$$P(P_{ij}/E_{p1},E_{p2},\cdots,E_{pi},\cdots,E_{p|p|})=P(P_{ij}/E_{pi}),\ P(P_1,P_2,\cdots,P_{|p|}/E)=\prod P(P_i/E),$$

计算 $r_p=P(X/E_p)$ 有：

$$P(X/E_p)=P(X/E_{p1},E_{p2},\cdots,E_{p|p|})=\sum_{\text{all}\,i,j,\cdots,k}P(X/P_{1i},P_{2j},\cdots,P_{|p|k}).$$

$$P(P_{1i},P_{2j},\cdots,P_{|p|k}/E_{p1},E_{p2},\cdots,E_{p|p|})=\sum_{\text{all}\,i,j,\cdots,k}P(X/P_{1i},P_{2j},\cdots,P_{|p|k}).$$

$$P(P_{1i}/E_{p1})P(P_{2i}/E_{p2})\cdots P(P_{|p|k}/E_{p|p|})=\sum_{\text{all}\,i,j,\cdots,k}P(X/P_{1i},P_{2j},\cdots,P_{|p|k}).$$

$$P(P_{1i})P(P_{2j})\cdots P(P_{|p|k}) \tag{7}$$

式（7）中的各 $P(P_{mn}/E_{pm})$ 表示先验属性结点 P_m 取其值空间中某个序号为 n 的值的概率，可以通过对系统正常运行状态下的该属性取值进行统计而获得。依据式（5）可知：

$$P(I/E)\propto r_{pI},\ P(I/E)\propto r_{cI},$$

$$P(\neg I/E)\propto r_{p\neg I},\ P(\neg I/E)\propto r_{c\neg I}。$$

把 $X=I$，$X=\neg I$ 分别代入式（6）和式（7），并做归一化处理，即令：

$$P(I/E)=r_{c1}r_{p1}/(r_{c1}r_{p1}+r_{c2}r_{p2}),$$

$$P(\neg I/E)=r_{c2}r_{p2}/(r_{c1}r_{p1}+r_{c2}r_{p2})。$$

与简单概率算法类似，通过计算 $P(I/E)$ 与 $P(\neg I/E)$ 之间的比值，作为系统运行状态异常与否的初步判断结果，即系统是否受到入侵，最终结果由决策模块 δ 做出。通过计算

$$R=P(I/E)/P(\neg I/E)=r_{c1}r_{p1}/r_{c2}r_{p2} \tag{8}$$

如果 $R>1$ 可以初步判定系统发生异常，$R<1$ 则相应地表示系统当前行为正常。因为 R 值是在与

系统异常事件相关的先验特征与后验特征的共同约束下求得，与简单概率算法相比，其结果更严格地符合用户建模的系统正常行为特征轮廓。

3　系统正常行为建模

异常检测系统依赖于对系统正常使用状态下的行为准确建模。通过采样时刻系统中各安全相关特征的实时取值与其进行比较，并发现异常，进而检测出可能的攻击。信息综合模块执行的简单概率算法中，在各采样时刻，对系统安全相关属性是否发生异常（A_i）所赋予的模糊概率值 $P(A_i)$，其所依据的模糊隶属度函数是来自于对该属性在系统正常状态下的建模。贝叶斯置信网络算法中的 $P(X/E_{pi})$的计算也来源于对属性 E_{pi} 正常取值的建模。$P(A_i)$，$P(E_{ci}/X)$，$P(P_{mn})$的计算则不同，这些概率的计算是基于对系统正常使用中相关系统属性取值的统计。考虑到建模对象为系统正常行为，用$\neg A_i$ 来表示系统特征属性 A_i 处于正常状态事件。

3.1　特征属性的模糊概率赋值

对系统中安全相关特征属性进行模糊建模所依据 4 种模型如图 3 所示。

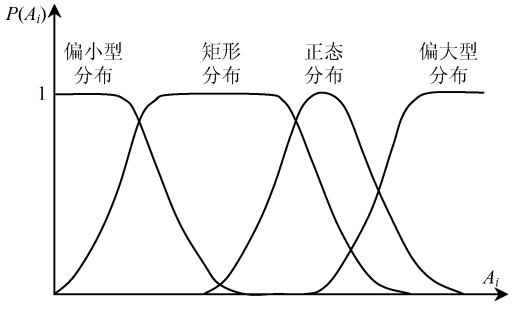

图 **3**　用于特征建模的模糊隶属度函数模型

Fig.3　Fuzzy membership function models

3.1.1　矩形分布模型　矩形分布模型为

$$\neg A_i(x)=\begin{cases}\exp[-((x-a)/\sigma)^2] & a<x\\ 1 & a\leqslant x\leqslant b\\ \exp[-((x-a)/\sigma)^2] & x>b\end{cases}\tag{9}$$

它描述这样一类系统特征属性，即其在系统行为正常时，取值通常在值空间的一个子区间内。这类系统特征属性的取值空间是离散的，如一段时间内某关键系统服务在日志中留下的记录条数（正常情况下，它只在启动、退出时记录一些相关信息，过多或过少的日志记录，表明有异常事件发生）。矩形分布的值空间也可以是连续的，通过为系统提供可配置功能，根据具体系统的情况，安全管理员可以为某些安全相关特征属性指定其正常取值范围。

3.1.2　偏小型正态分布模型　偏小型正态分布模型主要用来描述这样一类系统特征属性，即其取值一般不大于某个给定值，当其取值明显大于这一给定阈值时，可以认为系统行为发生异常，用

$$\neg A_i(x)=\begin{cases}1 & x\leqslant a\\ \exp[-((x-a)/\sigma)^2] & x>a\end{cases}\tag{10}$$

中的指数下降曲线来近似阈值 a 处其正常置信度的下降。符合该模型的系统特征属性有某段指定时间内计算机系统运行的时间、系统登录的次数等等，这些属性在系统的正常运行中取值都存在上限，比如办公用计算机每天开机一般不超过 9 h；以每天正常登录/退出一次计，每月登录/退出次数一般不超过 31−8 = 23 次。

3.1.3　偏大型正态分布模型　类似于偏小型正态分布模型，偏大型正态分布模型主要用来描述这样一类系统特征属性，即其取值一般不小于某个给定值，当其取值明显小于这一给定域值时，可以认为系统行为发生异常，用

$$\neg A_i(x)=\begin{cases}0 & x\leqslant a\\ 1-\exp[-((x-a)/\sigma)^2] & x>a\end{cases}\tag{11}$$

中的指数上升曲线来近似域值 a 处其正常置信度的升高。特征变量如两次登录的间隔时间就可以用该模型来描述。

3.1.4　正态分布模型　计算机系统中多数与安全相关的特征属性，如用户击键速度、各键按下的时间长短、CPU 利用率、I/O 利用率、网络数据流量、主要应用程序会话时间、执行的频度、关键文件访问的频率等等，在正常状态下的取值更适合用正态分布模型来描述。通过在系统正常行为建模的过程中记录的各特征属性，系统正常运行中不同时刻的取值形成一个训练集。在对其中数据的分析后，可以拟合出相应的正态模型

$$\neg A_i(x)=\exp[-((x-u)/\sigma)^2]\tag{12}$$

即形成式中的参数 u，σ。

3.2　系统行为建模

对系统正常运行状态下行为的建模，是一个记录并分析各选定的安全相关系统特征变量值的过

程。在收集了这些特征变量的取值后，结合其所对应的模型，从所收集的数据记录中抽取出相应的模糊隶属度函数的参数，即可完成对这些特征属性在系统行为正常状态下的建模。异常检测系统在运行中，将实时获得的各系统特征属性值代入各自相对应的模糊模型中，从而计算出一组模糊概率值，作为各系统特征属性正常与否的置信度。在采用简单概率模型的信息综合模块中，把所有特征属性事件看作系统异常事件的前件，并把任何一个特征属性产生的异常也看作是系统发生的异常，即认为 $P(A_i) = P(I/A_i)$。为简化问题，令 $P(\neg I/A_i) = P(\neg A_i) = 1 - P(A_i)$，即可以实时地计算出所需要的类条件概率。采用贝叶斯置信网络作为信息综合模块中执行的算法，可以用类似的方法计算出系统异常事件的后件类条件概率 $P(A_i/\neg I)$。

决策模块中的宽容度 δ(缺省值为 1) 直接决定了异常检测系统的敏感度，如设置过大可能导致较高的漏检率，而若将其设置过小将会使误检率升高。其值由安全管理员根据所检测系统的具体软硬件环境和安全要求进行设置。

4 实验

针对实验平台（IBM NetVista 3305HC3, Pentium4 2.4GB CPU, 256MB RAM, 10/100 MB 自适应网卡连接于 10 MB 交换机上）的具体使用环境和用途（宽带数据和资料下载，软件编码、编译）以及对诸多系统特征变量连续 30 d 的记录和分析，依据以下 4 个系统特征属性对系统正常行为进行建模：**a**. 登录频度（偏小分布模型，正常登录频度为 0～3 次/d，值域取 [0, 25]，该值过大则明显有异常发生）；**b**. 开机时间（矩形分布模型，每日 3～11 h，值域 [0, 24]）；**c**. CPU 利用率（正态分布模型，系统正常运行时约在 7%，值域 [0, 100%] ）；**d**. 网络带宽占用（正态分布模型，由于用户持续在后台进行基于 P2P 模型的网络下载，网络带宽平均占用约 58.9 kb/s，值域 [0, 3.7 Mb/s])。为了应用贝叶斯网络算法，构造了以登录频度和开机时间为前件事件、CPU 利用率和网络带宽占用为后件事件、系统异常与否为待判定事件的贝叶斯置信网络。

模拟异常检测实验中，通过均匀遍历 4 个选定系统特征属性的取值空间来模拟所有可能发生的事件组合，并在所产生的数据集上执行各种信息综合算法（δ 取缺省值 1)。从表 1 可见，各种异常检测算法报警比率均大于人工判决值，理论上没有漏警产生，即被几种异常检测算法检为异常并报警的输入事件集合，覆盖了被人工判断为异常的事件集合。贝叶斯置信网络算法因为具有较低的误警率而相对于其他算法显示出了一定的优越性。简单概率算法在加权后得到了整组对比中最坏的结果，这是源于权值决定的困难性（实验中采用的是 4 种特征变量4:4:1:1)。从实验结果可以看出，由于对安全相关事件发生的类条件概率采用了模糊概率赋值，简单概率算法与贝叶斯置信网络算法均取得了比简单阈值方法更好的结果。

宽容度 δ 作为异常检测模型的一个重要参数，需要在系统行为建模过程中由实验来确定。加权的过程对最终结果有近似的归一化作用，而不同于加权简单概率算法，简单概率算法中的宽容度 δ 对异常检测的准确度有很大的影响。在采用 4 个系统特征属性的模拟异常检测模型中，对 δ 赋于 (5～15 000)范围内不同间隔的 18 个整数值，得到图 4 所示结果，可见，δ 值约为 7 000 时，简单概率算法异常检测的结果与人工判决的结果最为符合。

表 **1** 模拟实验结果

Table 1 Results of simulations %

算法或判决	异常	正常	误警
人工判决	75.3	24.7	0
简单概率算法	80.9	19.1	7.4
加权简单概率算法	84.6	15.4	12.4
贝叶斯网络算法	79.2	20.8	5.2
简单阈值方法	83.5	16.5	10.9

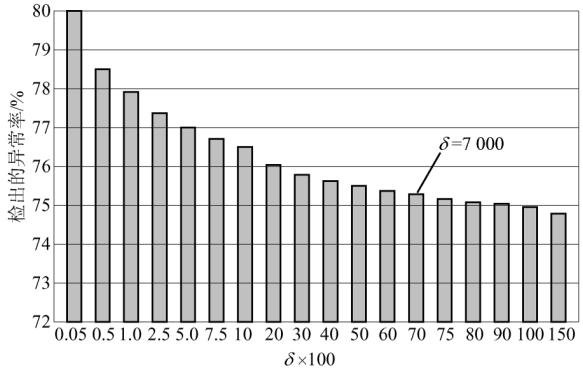

图 **4** 不同 δ 的检测出的异常率

Fig.4 Anomaly detection results with different δ

5　结语

通过模拟实验，基于模糊概率赋值的贝叶斯异常检测模型显示了比传统简单阈值方法更低的误警率，这得益于取值连续的模糊概率赋值所带来的对系统行为特征描述的精确性。为了描述更加复杂的系统安全相关事件发生的类条件概率，更加复杂的模糊概率赋值模型还有待研究。对于加权简单概率算法中的权值确定也需要进行更加深入的研究。在结合了先验知识的贝叶斯置信网和加权简单概率算法（权值为先验知识）中，可以通过推理过程的回溯来尝试确定异常发生的原因，这是下一步研究中的一个重点方向。

参考文献

[1] Kemmerer R A, Vigna G. Intrusion detection: a brief history and overview [J]. Computer, 2002, 35(4): 27～30

[2] Debar H, Dacier M, Wespi A. A revised taxonomy for intrusion detection systems [J]. Annales des Telecommunications, 2000, 55(7): 361～378

[3] Mitchell T M. Machine Learning [M]. New York: McGrall－Hill Press, 1997

[4] Duda R O, Hart P E, Stork D G. Pattern Classification [M]. New Jersey: Wiley Press, 2000

[5] Kruegel C, Mutz D, Robertson W, et al. Bayesian event classification for intrusion detection [A]. Proceedings of 19th Annual Computer Security Applications Conference [C]. 2003

[6] Sebyala A A, Olukemi T, Sacks L. Active platform security through intrusion detection using naive bayesian network for anomaly detection [A]. Proceedings of the London Communications Symposium [C]. London, 2002

[7] Puttini R S, Marrakchi Z, Mé L. A bayesian classification model for real-time intrusion detection [A]. AIP Conference Proceedings Vol 659 [C]. 2003. 150～162

[8] 张　琨，徐永红，王　珩，等. 用于入侵检测的贝叶斯网络[J]. 小型微型计算机系统，2003，24(5)：913～915

[9] 罗光春，卢显良，李　炯，等. 一种基于贝叶斯判决的先进入侵检测模型[J]. 计算机科学，2003，30(8)：50～51

A Novel Bayesian Anomaly Detection Model Using Fuzzy Probability Assignment

Jin Shu, Liu Fengyu

(*Computer Science Department, Nanjing University of Science & Technology, Nanjing* 210094, *China*)

[**Abstract**] To enhance the intrusion detection system with more accuracy and less false positive rate while still providing acceptable performance and adaptability, a Bayesian anomaly intrusion detection system using fuzzy probability assignment is presented in the paper. After categorizing the security related system events and properties into four models, which are represented by their corresponding fuzzy membership functions, the real-time probability of a specific security event will be calculated as according to the fuzzy membership function of the model it belongs to and a decision whether the supervised system is in a abnormal state is thus made from the synthesized probabilities of all these registered security events. Two separate algorithms, namely simple probability algorithm and Bayesian belief network algorithm, are provided in combining with the real-time fuzzy probabilities calculated. Simulations with a group of fine tuned coefficients prove the effectiveness of the two algorithms. Compared with previous work that employs the simple threshold methods in judging security related system events, the fuzzy approach suggested describes the probabilities of security events more accurately through utilizing the continuous fuzzy probability model and scales better as well for modeling various kinds of security related system properties in normal system behavior profiling.

[**Key words**] IDS; anomaly detection; fuzzy probability assignment; Bayesian belief network