基于攻击检测的网络安全风险评估方法

陈天平[1] 许世军[2] 张串绒[1] 郑连清[1]
(空军工程大学电讯工程学院 西安 710077)[1] (西北工业大学365研究所 西安 710072)[2]

摘 要 为了实时评估网络安全风险,建立了用于描述主机安全状态的隐马尔可夫模型,以入侵检测系统的报警信息作为模型输入,计算主机处于被攻击状态的概率。针对攻击报警,提出了一种新的攻击成功概率计算方法,然后结合攻击威胁度计算主机节点的风险指数。最后利用主机节点重要性权重与节点风险指数量化计算网络风险。实例分析表明,该方法能够动态绘制网络安全风险态势曲线,有利于指导安全管理员及时调整安全策略。

关键词 网络安全,风险评估,入侵检测系统,隐马尔可夫模型
中图法分类号 TP393.08 **文献标识码** A

Risk Assessment Method for Network Security Based on Intrusion Detection System

CHEN Tian-ping[1] XU Shi-jun[2] ZHANG Chuan-rong[1] ZHENG Lian-qing[1]
(Telecommunication Engineering Institute, Air Force Engineering Univ., Xi'an 710077, China)[1]
(365 Institute of Northwestern Polytechnical University, Xi'an 710072, China)[2]

Abstract The Hidden Markov Model(HMM) for describing host security states was established to evaluate the real time security risk of network, whose input is Intrusion Detection System alers. The probability for host to be attacked was calculated by this model. Aimed at the attack alers, a new calculating method for attack success probability was presented, and used attack threat level to calculate the risk index of the host node. Finally, the importance weight and risk index of all the host nodes were used to calculated the risk of the network quantitatively. The case study demonstrated this method can provide the real-time risk curves of host system for security managers to adjust security policies.

Keywords Network security, Risk assessment, Intrusion detection system, Hidden markov model

基于静态数据分析的网络安全风险评估方法缺乏实时性,难以发现网络运行过程中存在的威胁状况。而基于IDS攻击检测的风险评估方法能够弥补这个缺陷,方便网络管理员动态管理网络安全。

国外相关文献中,Arnes认为主机可以处于不同的安全状态,每种安全状态的概率决定了其安全风险,而状态之间的转换由隐马尔可夫状态转换矩阵和观察矩阵决定[1];Salim Hariri等人基于网络性能度量指标,评估分析网络攻击对系统安全的影响,但这种方法只适用于分析拒绝服务类攻击[2];Blyth提出通过观察黑客的攻击足迹而定性评估其安全威胁,但该方法不能提供全局的安全威胁趋势[3]。国内相关文献中,文献[4]指出基于HMM的实时网络安全风险量化方法存在配置复杂、评估容易出现误差的问题,为此提出了优化方法,即利用参数矩阵自动生成代替手工设置,从而提高了准确性,简化了配置复杂度;文献[5]提出基于信息融合的网络安全态势评估模型,引入改进的D-S证据理论将多数据源信息进行融合,利用漏洞信息和服务信息,经过态势要素融合计算主机节点的安全态势,但攻击成功支持概率算法只考虑了漏洞因素,不够客观;文献[6]提出了一种基于网络图论模型的威胁态势分析方法,即对图中的边赋予代表攻击代价的权,利用最短可达路径算法分析节点的威胁态势;陈秀真博士利用IDS海量报警信息和网络性能指标,结合服务、主机本身的重要性及网络系统的组织结构,提出采用自下而上、先局部后整体评估策略的层次化安全威胁态势来量化评估模型及相应的计算方法[7]。

本文的主要工作体现在:(1)简化了隐马尔可夫模型,增强了实用性;(2)提出了攻击成功概率算法,提高了评估结果的科学性和合理性。

1 描述主机安全状态的HMM

为了解决IDS存在的漏报、误报问题,本文引入了HMM。HMM是双内嵌式随机过程,其中一个是状态转移队列,它对应输出符号组成的符号序列。这两个随机过程中,其中一个是不可直接观测的,只能通过另一个随机过程输出的观察符号序列来观测。

1.1 HMM的定义

为网络中每一个主机节点建立一套HMM,其具体描述如下:

到稿日期:2009-10-20 返修日期:2009-12-29 本文受国家自然科学基金项目(60873233),陕西省科技攻关项目(2008-k04-21)资助。
陈天平(1979—),男,博士生,主要研究方向为信息系统风险管理,E-mail:chentianping1979@163.com;许世军(1956—),男,高级工程师,主要研究方向为无线电测控技术;郑连清(1963—),男,教授,博士生导师,主要研究方向为信息安全等。

①状态空间

$S=\{s_0,s_1\}$，那么任一主机节点的状态序列表示为 $X=\{x_1,\cdots,x_T\}$，$x_t\in S$，$t=1,2,\cdots,T$。这里 s_0 表示主机处于安全状态，s_1 表示主机处于受攻击状态，状态数 $N=2$。

②观测符号空间

$V=\{v_0,v_1\}$，那么观测符号序列表示为 $Y=\{y_1,\cdots,y_T\}$，$y_t\in V$，$t=1,2,\cdots,T$。这里 v_0 表示没有攻击事件发生的符号，v_1 表示有攻击事件发生的符号，可观测值符号数目 $M=2$。

③状态转移矩阵

$A=[a_{i,j}]_{N\times N}$，其中 $a_{i,j}=P(x_{t+1}=s_j\mid x_t=s_i)$，$s_i,s_j\in S$。

④观测矩阵

$B=[b_i(v_k)]_{N\times M}$，其中 $b_i(v_k)=P(y_t=v_k\mid x_t=s_i)$，$s_i\in S$，$v_k\in V$。

⑤初始状态分布

$\pi=\{\pi_0,\pi_1\}$，其中，$\pi_0=P(x_1=s_0)$，$\pi_1=P(x_1=s_1)$。

根据上述定义，可用 $\lambda=(A,B,\pi)$ 来确定网络中主机节点的 HMM 模型。

1.2 基于 HMM 计算主机的状态分布概率

定义 HMM 前向变量 $\alpha_t(i)=P\{y_1,y_2,\cdots,y_t,x_t=s_i\mid\lambda\}$，$t\leqslant 1$，$s_i\in S$。

在初始时刻，当 $t=1$ 时

$$\alpha_1(j)=\pi_j b_j(y_1),j\in\{0,1\} \tag{1}$$

当 $t>1$ 时

$$\alpha_t(j)=\left[\sum_{i=1}^{2}\alpha_{t-1}(i)a_{ij}\right]b_j(y_t),1\leqslant t\leqslant T,j\in\{0,1\} \tag{2}$$

根据 HMM 的定义，定义主机状态概率分布为 $\gamma_t(i)=P(x_t=s_i\mid y_1,y_2,\cdots,y_t,\lambda)$，$t\geqslant 1$。由此可得主机在 t 时刻的状态概率分布计算公式为

$$\gamma_t(i)=\alpha_t(i)/\sum_{i=1}^{2}\alpha_t(i),t\geqslant 1,i\in\{0,1\} \tag{3}$$

2 基于入侵检测的网络安全风险评估思想

为了处理 IDS 产生的海量报警信息，首先需要评估这些报警信息的风险大小，然后过滤风险较小的报警，针对风险较大的报警进行重点防范。其评估步骤如下：

第一步：为主机节点部署 IDS 和相应的 HMM 模型，并以 IDS 产生的报警信息作为 HMM 的输入，计算主机处于被攻击状态的概率；第二步：针对 IDS 产生的攻击报警信息，计算该攻击在目标节点上成功执行的概率；第三步：利用攻击威胁度，计算主机节点的风险指数，最后采用加权法计算网络安全风险。

网络安全风险评估理论框架如图 1 所示。

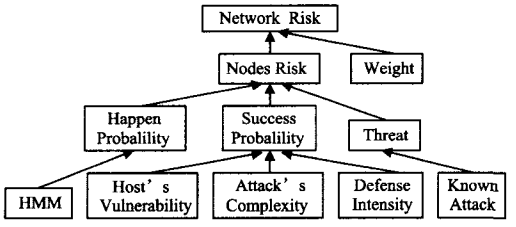

图 1 网络安全风险评估理论框架

下面给出风险评估过程中定义的一些术语。

定义 1(攻击，A) 引发 IDS 产生报警的所有攻击行为，表示为 $A=\{Name,Time,Type,SIP,DIP,SP,DP,Pre,E,V\}$。其中，$Name,Time,Type$ 表示攻击特征、发生时间和类型；SIP,DIP 代表源和目的地址；SP,DP 代表源和目的端口；Pre 表示攻击成功执行必须具备的前提条件(如 OS 版本、用户权限、漏洞等)；E 表示攻击复杂度；V 表示攻击的威胁度。

定义 2(攻击发生概率，$P[h]$) 是指主机节点处于被攻击状态的概率。

定义 3(攻击成功概率，$P[s]$) 是指攻击在目标节点上成功执行的概率。

定义 4(攻击复杂度，E) 弱点的攻击复杂度是用来衡量攻击者成功利用该弱点的难易程度。

定义 5(安全防护强度，I) 是主机节点所采取的安全防护措施对攻击执行过程造成的阻碍程度。

3 基于入侵检测的风险评估相关算法研究

基于入侵检测进行节点风险评估的流程如图 2 所示。

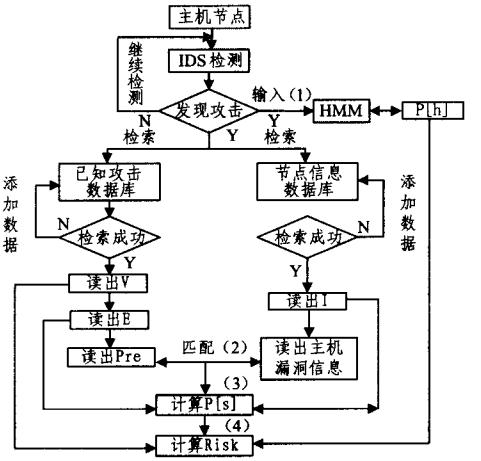

图 2 主机节点风险评估流程

图 2 中步骤(1)：对 IDS 产生的攻击报警发生于主机节点上的概率进行计算，此步骤已在本文第 1 节进行了介绍。

步骤(2)：对攻击执行的前提条件(Pre)与主机存在的漏洞(或错误配置)进行匹配。

设 M 用于描述二者之间匹配的吻合程度，称为匹配因子。在此不妨令 $M=0.1$ 表示二者完全不匹配；令 $M=0.5$ 表示二者不完全匹配；令 $M=1$ 表示二者完全匹配。

步骤(3)：计算攻击成功概率。

一般攻击执行过程需要目标主机具有相应的漏洞或配置，若这些条件(例如针对的端口没有打开，或是服务没有运行等)不满足，则攻击成功的可能性较低；反之，攻击成功的可能性较高。另外，应考虑攻击复杂度及安全防护措施对攻击执行过程的影响。

由于攻击复杂度及防护措施强度对攻击成功概率的影响为非线性关系，为了反映这一特点，在此使用指数函数来表达，以提高评估结果的可区分度，因此攻击成功概率估测式为

$$P[s]=M\times e^{-(E+I-2)} \tag{4}$$

式中，E 和 I 均为等级评价值，它们的详细分级定义分别如表 1 和表 2 所列[8]。

表 1 攻击复杂度的分级定义

等级	复杂度	攻击复杂度描述
1	1	不需要攻击工具，有详细的攻击方法
2	2	无攻击工具，但有较详细的攻击方法
3	3	公开报告此弱点，但未提及攻击方法

表 2　防护措施强度的分级定义

等级	强度	防护措施强度描述
1	1	无针对性的防护措施
2	2	有针对性的防护措施，但防护效果一般
3	3	有针对性的防护措施，而且防护效果好

因为 $E,I\in\{1,2,3\}$，所以 $0\leqslant E+I-2\leqslant 4$，故满足条件 $P[s]\in[0,1]$。

步骤(4)：计算主机节点风险指数。

攻击 $A(i)$ 在时刻 t 入侵主机 H 的风险指数为

$$R^t_{HA(i)}=P[h]\times P[s]\times V_i \tag{5}$$

若主机节点同时受到几种攻击，则将每种攻击对该主机的风险指数累加，作为该主机节点在时刻 t 受到的所有攻击的风险指数，即主机节点在时刻 t 的风险指数表示为 R^t_H，其计算公式如下。

$$R^t_H=\sum_{i=1}^{l}R^t_{HA(i)} \tag{6}$$

式中，l 为主机节点某一时刻受到的攻击数目。

假定被评估网络包含 n 个主机节点，然后根据网络提供服务的分布情况，确定主机节点的权重[7]，详细方法见文献[7]，此处不再赘述。

$$R^t_N=\sum_{j=1}^{n}\alpha_j\times R^t_{H(j)} \tag{7}$$

式中，R^t_N 为网络在时刻 t 的风险指数，α_j 为主机 $H(j)$ 的权重，$R^t_{H(j)}$ 为主机 $H(j)$ 在时刻 t 的风险指数。

4　实例应用分析

为了验证本文提出的方法，设置如下网络参数：

(1)被评估网络包含 m 个主机节点，编号分别为 $H(1)$，$H(2),\cdots,H(m)$。

(2)以主机 $H(1)$ 为例(其余主机类同)，用于描述该主机安全状态的 HMM 为

$$\pi=\{0.99,0.01\},A=\begin{bmatrix}0.99 & 0.01\\ 0.02 & 0.98\end{bmatrix},B=\begin{bmatrix}0.8 & 0.2\\ 0.3 & 0.7\end{bmatrix}$$

(3)假设 IDS 在时段 T 内监测网络，一共检测到 3 种不同的攻击，表示为 $A(1)$，$A(2)$ 和 $A(3)$。

针对主机节点 $H(1)$，所需评估参数如表 3 所列。

在表 3 中，$V(i)$ 为攻击 $A(i)$ 的威胁度；$E(i)$ 为攻击 $A(i)$ 的攻击复杂度；$I(i)$ 为 $H(1)$ 针对攻击 $A(i)$ 的防护措施强度；$M(i)$ 为匹配因子，其中 $1\leqslant i\leqslant 3$。

表 3　评估参数表

被评主机	A(1) E(2)=2 V(1)=5	A(2) E(2)=1 V(2)=3	A(3) E(3)=3 V(3)=7
H(1)	I(1)=3 M(1)=0.5	I(2)=2 M(2)=1	I(3)=1 M(3)=0.1

将监测时段 T 分为 6 等份，每段 $\Delta t=T/6$，Δt 为最小监测单位时间。假设在时段 T 内观测符号序列为 $Y=\{v_1,v_1,v_1,v_1,v_6,v_1\}$，IDS 攻击报警情况及主机风险指数如表 4 所列。

表 4　IDS 攻击报警及主机风险指数

时段	IDS 报警	$\gamma_t(1)$	$R^t_{H(1)}$
Δt	A(1)	0.03415	0.00424
$2\Delta t$	A(1),A(3)	0.13624	0.02982
$3\Delta t$	A(2)	0.36708	0.40487
$4\Delta t$	A(1),A(3)	0.66899	0.14623
$5\Delta t$	无	0.42011	0
$6\Delta t$(T)	A(3)	0.71499	0.06765

由表 4 中的计算结果进行绘图，可得主机 $H(1)$ 的风险态势曲线，如图 3 所示，图中横轴为时间，$T=12$h，$\Delta t=2$h(即 2h 为一个监测周期)，纵轴为主机 $H(1)$ 的风险指数 $R^t_{H(1)}$。

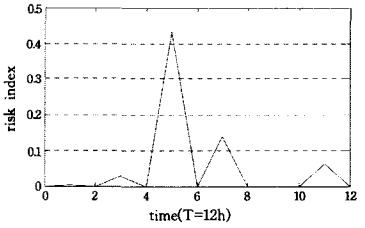

图 3　主机风险态势曲线图

从图 3 可以看出，①在时段 $3\Delta t$(即 4～6h)内，主机面临的风险最大，在该时段内 IDS 检测发现了攻击 $A(2)$，由表 3 可知，$A(2)$ 的复杂度小，而且 $A(2)$ 成功执行的前提条件与主机的漏洞或配置信息完全匹配，因此 $A(2)$ 对主机的威胁较大，这点与实验结果相吻合；②比较时段 $3\Delta t$ 与 $6\Delta t$，虽然 $\gamma_{3\Delta t}(2)<\gamma_{6\Delta t}(2)$，但是 $R(3\Delta t)>R(6\Delta t)$，说明主机的风险不仅取决于攻击发生概率，而且受到主机的安全防护措施、漏洞严重性等因素的影响；③在时段 $5\Delta t$(即 8～10h)内，因为 IDS 没有检测到任何攻击，所以主机风险为 0，这点恰好证明了 IDS 面临未知攻击时存在安全盲区。

按照以上方法依次评估 $H(2)$，$H(3)$，$\cdots$，$H(m)$ 在时段 T 内的风险指数，然后利用式(7)计算网络的风险大小，并绘制动态的网络安全风险态势曲线。

结束语　本文以 IDS 的报警信息作为输入，利用主机 HMM 计算主机处于被攻击状态的概率，并提出一种新的计算攻击成功概率的方法。最后定量计算了整个网络的安全风险指数，为网络安全量化管理提供了思路。

考虑到网络主机之间存在复杂的信任关系将影响整个网络安全风险的评估结果，因此下一步重点研究主机节点之间的互相关联问题，为进一步评估大规模复杂网络的安全风险奠定基础。

参 考 文 献

[1] Arnes A, Valeur F, Vigna G, et al. Using hidden Markov models to evaluate the risk of intrusions [A] // Proceedings of the RAID'06[C]. Hamburg, Germany, 2006: 145-164

[2] Hariri S, Qu G Z, Dharmagadda T, et al. Impact analysis of faults and attacks in large-scale networks [J]. IEEE Security & Privacy, 2003, 1(5): 49-54

[3] Blyth A. Footprinting for intrusion detection and threat assessment [J]. Information Security Technical Report, 1999, 4(3): 43-53

[4] 李伟明，雷杰，董静，等. 一种优化的实时网络安全风险量化方法[J]. 计算机学报，2009，32(4)：793-804

[5] 韦勇，连一峰，冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展，2009，46(3)：353-362

[6] 陈天平，乔向东，郑连清，等. 图论在网络安全威胁态势分析中的应用[J]. 北京邮电大学学报，2009，32(1)：113-117

[7] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006，17(4)：885-897

[8] 尚大鹏，周渊，杨武，等. 用于评估网络整体安全性的攻击图生成方法[J]. 通信学报，2009，30(3)：1-5