一种基于马尔科夫模型的网络安全风险实时分析方法

王 笑 李千目 戚 湧
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要 针对网络风险实时分析的迫切需求,研究并设计了适用于实时风险概率预测的马尔科夫时变模型,提出了一种网络安全实时风险概率预测方法。该方法鲁棒性较强,能够反应波动数据变化规律,起到了进行实时风险分析的作用。用 DRAPA2000 数据集进行了仿真,结果表明该方法具有较高的实时性和准确性。

关键词 安全风险预测,马尔科夫,时变模型,DRAPA2000
中图法分类号 TP393.08 **文献标识码** A

Real Time Analysis Method of Network Security Risk Based on Markov Model

WANG Xiao LI Qian-mu QI Yong
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract In view of the urgent need of real-time analysis of network risk, this paper studied and designed a Markov time variant model which is suitable for real-time risk probability prediction. The method has strong robustness and can react with the variation of the wave data, which has the effect of real time risk analysis. DRAPA2000 data sets were used to carry out simulation experiments to predict the probability of the network. The results show that the model mentioned in this paper has high real-time performance and accuracy.

Keywords Security risk prediction, Markov, Time varying model, DRAPA2000

1 引言

随着互联网应用的普及和因特网技术的飞速发展,网络用户规模随之扩大,同时近年来网络攻击事件的数量也逐年上升,网络安全的研究十分必要。以入侵检测技术、防火墙为代表的传统的全保护方式已经难以满足大规模网络对安全防护的要求,一种新的解决方法——网络安全态势感知应运而生,且得到了众多学者的关注。网络安全态势预测是建立在安全态势理解与安全态势评估的基础上进行的,它在网络安全态势感知系统中处于最后阶段。通过对网络态势的历史数据进行分析处理,构建符合网络态势的数学模型,利用建立的模型和现有的信息来预测网络安全态势的变化情况。

实时准确地预测网络中的安全风险概率对提高网络的安全性意义重大。近年来,研究人员在网络安全风险预测领域进行了许多研究。文献[1]采用 RBF 神经网络进行并行化预测,实现了多个节点快速实时预测,但在部分数据点存在一定范围的偏离;文献[2]提出了一种基于灰色理论的网络安全风险预测方法,但是该方法存在明显的误差,预测的准确性有待提高;文献[3]将支持向量机和混沌理论引入到网络安全事件预测中,给出一种基于数据挖掘技术的网络安全事件预测算法,但是该算法建模过程的复杂度高且 SVM 参数优化方法存在不足,导致建模效果具有一定的局限性;文献[4-6]采用了基于隐马尔可夫模型的网络安全风险预测方法,但是 HMM 模型存在参数估计的效率性问题,模型的建立过程有待优化。

马尔科夫模型对于波动性数据具有良好的预测效果,且建模复杂度可控。本文研究了适用于实时风险概率预测的马尔科夫时变模型,设计了基于此模型的实时风险概率预测方法,起到了实时风险预测的作用。

2 基于 Markov 时变模型的实时风险概率预测

符合在 t_0 时刻所处的状态已知时,$t(t>t_0)$ 时刻所处的状态与过程在 t_0 时刻之前的状态无关的随机过程就是马尔科夫过程(Markov Process),上述的特性称为无后效性。马尔科夫过程中的时间和状态可以是连续的,也可以是离散的。时间、状态离散的马尔科夫过程为马尔科夫链。

马尔科夫模型可以表示为 $\lambda=\{S,P,\pi\}$,其中,

1)S 是系统的状态空间,是由系统所有可能的状态所组成的非空的状态集。

2)$P=[p_{ij}(t,t+k)]_{n\times n}$ 是系统的状态转移概率矩阵,$p_{ij}(t,t+k)=P\{X_{t+k}=j \mid X_t=i\}$,$i,j\in S$ 表示系统在时刻 t 处于状态 i,但经过 k 步之后,即处于时刻 $t+k$ 时状态转移至 j 的概率,其中 X_t 表示系统在 t 时刻的状态。且存在对于任意 $i\in S$,满足 $\sum_{j=1}^{n} p_{ij}(t,t+k)=1$,$0\leqslant p_{ij}(t,t+k)\leqslant 1$,$i,j\in S$。

本文受中央高校基本科研业务费专项资金(30916015104),中兴通讯产学研合作论坛合作项目:基于马尔可夫时变模型的流量数据挖掘技术研究(2016ZTE04-11)资助。

王 笑(1992-),女,硕士生,主要研究方向为信息安全,E-mail:543681770@qq.com;李千目(1979-),男,教授,博士生导师,主要研究方向为信息安全,E-mail:Liqianmu@126.com(通信作者)。

3)$\pi=[\pi_1,\pi_2,\cdots,\pi_n]$是系统的初始概率分布矩阵，$\pi_i$ 表示系统在初始时刻处于状态 i 的概率，且满足$\sum_1^n \pi_i=1$。

一般来说，使用马尔科夫链进行预测，是通过确定一步转移概率矩阵 P(即 $k=1$)，然后结合当前状态计算出下一步转移到各个状态的概率。计算得到的概率越大，处于该状态的可能性越大，从而得到下一步可能所处的状态。传统的马尔可夫模型假设状态转移概率矩阵 P 并不随着时间的改变而改变。然而在许多实际问题中，状态的转移概率矩阵 P 是不断发生变化的。

使用马尔科夫时变模型对网络风险进行实时预测的建模过程如下：

(1)基础数据及数据预处理，对数据进行预处理，将一个时间序列所对应的安全状态值作为马氏链。

(2)确定状态划分标准，依照标准进行状态划分。

(3)生成马氏链状态表，并统计状态转移数量。

(4)采用频率近似概率的思想，根据马氏链状态表和状态转移数量计算状态转移概率，生成状态转移概率矩阵 P。

当有新数据加入时，重复步骤(3)、步骤(4)，实现状态转移概率矩阵的实时更新。

网络攻击一般由信息收集阶段、攻击进行阶段、攻击完成阶段 3 部分构成[7,8]。

根据攻击的阶段及网络所处的风险层次不同，将网络风险状态划分为：正常状态 L_0(即安全状态)、轻微风险状态 L_1(即网络被扫描探测)、低风险状态 L_2(此时网络中的漏洞可能被发现利用)、较严重风险状态 L_3(网络已经受到了攻击)以及严重风险状态 L_4(受到的攻击很大，网络已被攻陷)。

网络风险在这些状态之间以一定的概率相互转移，这些状态构成了马尔科夫时变预测模型中的状态空间，即 $S=\{L_0,L_1,L_2,L_3,L_4\}$，由此得到网络的风险状态转移如图 1 所示。

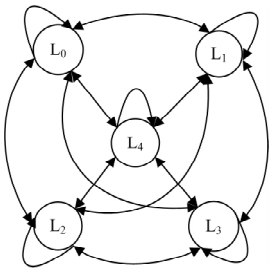

图 1　网络安全风险状态转移图

计算状态转移矩阵 P，转移矩阵中的每一个元素 p_{ij} 对应从状态 i 转移到状态 j 的概率，在计算时一般采用频率近似概率的原理，即

$$p_{ij}=\frac{n_{ij}}{\sum_j n_{ij}} \tag{1}$$

其中，n_{ij} 为从状态 i 出发，转移到状态 j 的样本数。

由此可以确定网络风险转移概率矩阵为：

$$P=\begin{pmatrix} P_{L_0L_0} & P_{L_0L_1} & P_{L_0L_2} & P_{L_0L_3} & P_{L_0L_4} \\ P_{L_1L_0} & P_{L_1L_1} & P_{L_1L_2} & P_{L_1L_3} & P_{L_1L_4} \\ P_{L_2L_0} & P_{L_2L_1} & P_{L_2L_2} & P_{L_2L_3} & P_{L_2L_4} \\ P_{L_3L_0} & P_{L_3L_1} & P_{L_3L_2} & P_{L_3L_3} & P_{L_3L_4} \\ P_{L_4L_0} & P_{L_4L_1} & P_{L_4L_2} & P_{L_4L_3} & P_{L_4L_4} \end{pmatrix} \tag{2}$$

当有新的数据加入时，将根据历史数据和当前数据一同统计，重新计算风险转移概率矩阵，以实现概率转移矩阵 P 的实时更新。

转移矩阵 P 中的每一个元素 p_{ij} $(i,j\in S)$表示系统经过 1 步之后，从状态 i 转移至状态 j 的概率。对于已知当前状态为 i 的情况下，p_{ij} 的值可以表示下一时刻处于各状态的概率，即 $p_j=P\{X_{t+1}=j\mid X_t\}(j\in S)$，其中 X_t 表示系统在 t 时刻的状态。引入一个代价向量 C，用来表示一个网络在每个状态的风险值，那么可以通过对代价向量及所处状态的概率加权的方式实现定量分析。即对 $C=\{c_1,c_2,\cdots,c_n\}$，可以利用公式计算网络的风险值为 $R=\sum_{i=1}^n p_i c_i$。

3　实验环境设置

为了验证马尔科夫时变模型对实时风险概率预测的有效性，本文选用了 DRAPA2000 数据集[9]来进行仿真试验。

DRAPA 2000 攻击场景测试数据集包含一系列的攻击，整个攻击过程是 DDoS 攻击的实现。攻击者先通过 IPSweep 进行活动主机的探测；然后进行端口扫描，查找到有 Sadmind 漏洞的主机之后，攻击该漏洞的 3 台主机，Pascal(172.16.112.50)、Mill(172.16.115.20)和 Locke(172.16.112.10)，使之成为傀儡机；再在被控主机上安装 DDoS 攻击的木马软件，通过 RSH 远程登录受害主机，并利用被控主机对攻击目标发起 DDoS 攻击。

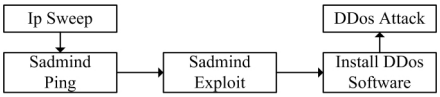

图 2　攻击步骤

Drapa 2000 数据集对应的攻击步骤如图 2 所示，攻击步骤的具体描述如下：

Step1　IP Sweep。攻击者对目标网络进行扫描以搜寻活跃的主机。

Step2　Sadmind Ping。对 Step1 中发现的活跃主机进行探测，探测有哪些主机在执行 Sadmind 远端管理者工具，进而锁定攻击目标。

Step 3　攻击 Pascal、Mill 和 Locke。对于 Step2 中锁定的 3 台主机 Mill、Pascal 和 Locke，尝试利用 Sadmind 的漏洞入侵直至成功入侵。

Step 4　在 3 台傀儡机上安装 DDoS 攻击工具。攻击者通过 RSH 服务远程登录傀儡机，并安装会产生真正 DDoS 攻击包的攻击工具，同时在其中一台受害主机上安装一个攻击代理，该代理提供了一个使用者界面并能控制安装在其他受害主机上的攻击工具。

Step 5　开始进行 DDoS 攻击。攻击者远程登录到安装了攻击代理的主机上，控制所有的安装了攻击工具的受控机器伪造 IP 地址并一起对远程服务器进行 DDoS 攻击。

根据 DRAPA2000 发布的 High-Level Attack Truth File，可以得出在 1～70min 处于安装攻击软件、收集信息等准备阶段；IP SWEEP 和端口扫描仅持续了约半个小时，发生在 80～125min 之间；sadmind exploit 发生在 126～240min；install ddos software 发生在 241～319min；最后发起攻击的时间是 320min。

4 仿真实验

4.1 eventlog 数据处理

采用 MIT 实验室公布的 NT 系统上获得的事件 log 作为实验数据。该 Log 中有信息、警告、错误 3 种类型的事件，出现的事件 ID 对应的事件信息如表 1 所列。

表 1 DRAPA 2000 数据产生的 eventlog 类型

事件 ID	级别	任务类别	关键字	来源
592	信息	详细追踪	经典,审核成功	Security
593	信息	详细追踪	经典,审核成功	Security
594	信息	详细追踪	经典,审核成功	Security
595	信息	详细追踪	经典,审核成功	Security
0	信息	无	经典	TimeServ
0	警告	无	经典	Ataman TCP Remote Logon Services
512	信息	系统事件	经典,审核成功	Security
514	信息	系统事件	经典,审核成功	Security
515	信息	系统事件	经典,审核成功	Security
517	信息	系统事件	经典,审核成功	Security
576	信息	特权使用	经典,审核成功	Security
577	信息	特权使用	经典,审核成功	Security
578	信息	特权使用	经典,审核失败	Security
528	信息	登录/注销	经典,审核成功	Security
538	信息	登录/注销	经典,审核成功	Security
2001	信息	-3	经典	Mail Service
2003	信息	-3	经典	Mail Service
1000	信息	-4	经典	Mail Service
5722	错误	无	经典	NETLOGON
7001	错误	无	经典	Service Control Manager
3216	错误	无	经典	REPLICATOR
560	信息	对象访问	经典,审核成功	Security
562	信息	对象访问	经典,审核成功	Security
564	信息	对象访问	经典,审核成功	Security
3007	警告	-4	经典	Mail Service
1008	错误	无	经典	Perflib
632	信息	帐户管理	经典,审核成功	Security
633	信息	帐户管理	经典,审核成功	Security
636	信息	帐户管理	经典,审核成功	Security
637	信息	帐户管理	经典,审核成功	Security

由于涉及的 log 事件类型并不多，且很多 log 事件属于同类操作对安全风险产生的效果极为类似，为了将评估结果数值化，参考文献[10,11]设定风险值的方式，根据每条告警的风险程度手工设置事件的风险值，如表 2 所列。

表 2 eventlog 中事件对应的风险值

事件 ID	级别	风险值
592,593,594,595	信息	1
0	信息	1
512,514,515,517	信息	1
576,577	信息	2
578	信息	3
528,538	信息	2
1000,2001,2003	信息	1
632,633,636,637	信息	3
560,562,564	信息	1
0	警告	4
3007	警告	5
5722	错误	6
7001	错误	8
3216	错误	6
1008	错误	6

如果一个网络的风险值在 1～200 之间，则认为该网络处于一个安全的状态，如果风险值在 200～1000 的范围，表示网络很可能被探测到了，而风险值在 1000～3000 之间则表示网络可能遭受了攻击，风险值在 3000～5000 的范围则表示已经遭受了攻击，如果风险值超过 5000，则表示已经受到了非常严重的攻击。

具体马尔科夫模型参数设置如下：初始概率：$\pi=\{1,0,0,0\}$；代价向量：$C=\{100,650,2000,4000,13000\}$。

为了方便以图表展示，以分钟为单位计算风险值，对一分钟以内产生的风险值进行统计。整个攻击从 8:00 开始，至 14:26 结束，持续时间为 386min。

4.2 仿真结果分析

图 3 显示了最终对网络安全风险进行实时预测的结果。图中实线为原始值，点线为预测值。

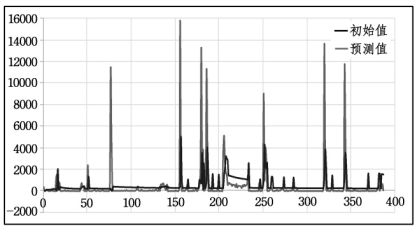

图 3 基于马尔科夫时变模型的安全态势预测结果

(1)0～69min 之间

这一阶段网络风险值不高，事实上这段时间攻击者在进行攻击软件的安装以及信息探测等准备工作。

(2)70～130min 之间

这一段网络风险出现了一个突然增高的现象，这是因为网络受到攻击者的端口 sweep 扫描和 Sadmindping 操作。

(3)131～250min 之间

风险值呈现了比较高的状态且风险值的波动性较大，在这一阶段，攻击者锁定 3 台主机 Mill、Pascal 和 Locke，并尝试利用 Sadmind 漏洞入侵，直至攻击成功获得完全控制权限。

(4)250～319min 之间

这一阶段的风险值明显降低，偶有小的波动，基本趋近于零。经过上一阶段的攻击，攻击者已经获得了 3 台主机的管理员权限，使之成为了傀儡机，这一阶段攻击者将分别在 3 台主机上安装攻击程序。由于主机没有对这步的攻击行为产生告警或者错误类型的日志，因此在图表中这段时间的网络风险值基本趋于零。

(5)320min 之后

这一阶段攻击者发起了 DDoS 攻击，出现非常高的风险值。

通过对 Darpa2000 的风险值数据和攻击步骤进行研究，可以得出每一步骤发生的大概时间。与数据集给出的攻击步骤对应时间段极其符合。

图 3 所示的网络风险预测结果与网络安全态势的实际变化相符合，风险值的变化规律符合 DDoS 攻击中的几个步骤。

实验结果表明，马尔科夫时变模型能够以较高的准确度预测安全风险发展的趋势，在所监控的网络受到攻击时，风险值显著增加，在网络受到的攻击减少时，风险值也随之降低。风险值的变化在时间上与原始信息非常吻合，该实验证明 markov 时变模型具有很高的的灵敏度及良好的时变预测效果。

结束语　实时的网络安全风险预测能够为管理员采取措施来提供支撑。网络安全风险预测对结果有实时性、灵敏性和准确性的要求，也间接要求模型建立和更新的复杂度不能过高。目前针对网络安全风险预测的研究较多，大多是基于数学建模的方式，对历史数据进行分析处理后进行建模和预测应用。网络安全风险值具有较大波动性，而一些模型并不适用于波动性数据的分析，另一部分模型则具有建模过程复杂的特点。马尔科夫模型既适用于波动性数据的预测分析，又具有建模复杂度可控的特点。因此本文设计了基于马尔科夫模型的网络安全风险预测方法，对日志文件进行分析，使用风险值的方式实现网络风险的量化，采用时变马尔科夫模型对风险值建模并进行预测。使用 DRAPA2000 的数据集进行仿真，实验结果表明该模型具有很好的实时性和较高的准确度，为网络安全风险预测提供了一种新的方式。但是风险值的设定基于经验判断，不同的风险值设定可能会对预测结果产生一定的影响，此处需要进一步开展研究，设定标准，从而高效、准确地对网络进行安全态势预测。

参 考 文 献

[1] 郭祖华，李扬波，徐立新，等. 面向云计算的网络安全风险预测模型的研究[J]. 计算机应用研究，2015(11)：3421-3425

[2] 王晋东，沈柳青，王坤，等. 网络安全态势预测及其在智能防护中的应用[J]. 计算机应用，2010，30(6)：1480-1482

[3] 陆科达，万励，吴洁明. 基于数据挖掘技术的网络安全事件预测研究[J]. 科技通报，2012，28(6)：37-39

[4] 李胜现，田东平，刘建华. 基于改进隐马尔可夫模型的网络动态风险评估[J]. 现代电子技术，2011，34(3)：76-77

[5] 黄同庆，庄毅. 一种实时网络安全态势预测方法[J]. 小型微型计算机系统，2014，35(2)：303-306

[6] 陈孟婕. 电力信息系统动静态风险评估技术研究[D]. 上海：华东理工大学，2015

[7] 刘刚，李千目，刘凤玉，等. 面向网络实时风险预测的马尔可夫时变模型[J]. 兵工学报，2012，33(2)：260-261

[8] 刘刚. 网络安全风险评估、控制和预测技术研究[D]. 南京：南京理工大学，2014

[9] MIT Lincoln Lab. 2000 Darpa Intrusion Detection Scenario Specific Data Sets[OL]. http://www.ll.mit.edu/ideval/data/2000data.html

[10] 董静. 改进的 HMM 网络安全风险评估方法研究[D]. 武汉：华中科技大学，2008

[11] 雷杰. 网络安全威胁与态势评估方法研究[D]. 武汉：华中科技大学，2008

(上接第 315 页)

PA 服务更多的 CA-GREEDY 用户。

总的来说，当供需匹配时，CA-GREEDY 的营收更高。如果拍卖期间的资源不像云拍卖那样可配置，CA-GREEDY 拍卖的效率也较高。但是如果资源像云拍卖那样可配置，则难以提前准确预测需求。此时，更应采用 CAM-DVMPA 机制，随着当今技术的发展，该机制可部署为一种无需大量人工干预的独立配置和分配工具。CAM-DVMPA 算法还有另一种用途，可以将 CAM-DVMPA 和 CA-GREEDY 结合起来，周期性地运行 CAM-DVMPA 以确定当前的市场需求，确定与需求最匹配的静态分配策略，然后运行 CA-GREEDY。如果资源利用率低于某一阈值，则调用 CAM-DVMPA 以便再次确定高性能资源配置。这可避免确定 CA-GREEDY 的高效率静态配置时进行详细的统计分析。

结束语　本文研究了云环境下虚拟机实例的动态供应问题，以便在确定基于组件拍卖的虚拟机分配策略时提高收益，并提出 CAM-DVMPA 机制以解决这一问题。利用真实的工作负载数据进行了全面的仿真实验，评估了本文方法的性能。结果表明，CAM-DVMPA 可有效确定市场需求，并针对需求供应计算资源，尤其是在需求较高时可提高云供应商的营收。我们认为本文算法是云环境下 VM 实例分配和供应技术的良好选择。在下一步工作中，我们打算建立一个私有云并在上面部署上述系统。

参 考 文 献

[1] 刘正伟，文中领，张海涛. 云计算和云数据管理技术[J]. 计算机研究与发展，2012，49(1)：26-31

[2] 张丽敏. 云计算中一种高效的虚拟机在线动态分配算法[J]. 电信科学，2015，31(4)：14-19

[3] 黄莉，丁一，姚锦元，等. 云采购平台虚拟供应商资源动态分配[J]. 计算机应用，2014，34(2)：377-381

[4] 丁晓波，马中，戴新发，等. 一种基于资源预分配的虚拟机软实时调度方法[J]. 计算机工程与科学，2015，37(5)：865-872

[5] Zaman S, Grosu D. Combinatorial auction-based allocation of virtual machine instances in clouds [J]. Journal of Parallel and Distributed Computing，2013，73(4)：495-508

[6] Krakov D, Feitelson D G. High-resolution analysis of parallel job workloads[C]// Job Scheduling Strategies for Parallel Processing. Springer Berlin Heidelberg，2013：178-195

[7] 师雪霖，徐恪. 云虚拟机资源分配的效用最大化模型[J]. 计算机学报，2013，36(2)：252-262

[8] Roughgarden T. Algorithmic game theory [J]. Communications of the ACM，2010，53(7)：78-86

[9] 贲飞，汪芸. 云计算下基于容错 QoS 的虚拟机资源分配策略[J]. 微电子学与计算机，2013，12(3)：33-35

[10] 谢文静，唐卓，杨柳，等. 基于随机规划的云计算中虚拟机分配优化研究[J]. 计算机工程与科学，2012，34(5)：95-100

[11] Chaisiri S, Lee B S, Niyato D. Optimization of resource provisioning cost in cloud computing[J]. Services Computing, IEEE Transactions on，2012，5(2)：164-177

[12] Peng Z, Xu B, Gates A M, et al. The feasibility and properties of dividing virtual machine resources using the virtual machine cluster as the unit in cloud computing[J]. KSII Transactions on Internet and Information Systems (TIIS)，2015，9(7)：2649-2666