使用随机 Petri 网的网络安全系统分析

焦 健 陈 昕
(北京信息科技大学计算机学院 北京 100101)

摘 要 网络攻击图一直是网络安全研究的重要手段,传统的攻击图和针对攻击路径的防御方案很难从概率的角度描述和分析攻击几率与防御技术对整体方案的影响程度。使用随机 Petri 网理论,给出了一种建立在攻击图之上的 Petri 网防御方案转换算法,使用该算法生成的随机 Petri 网模型可以实现对攻击和防御过程的并行分析。实验验证表明,该方法可以有效地量化攻击过程的发生几率,还可以协助分析不同防御技术对系统整体安全性的影响。

关键词 攻击图,随机 Petri 网,网络防御
中图法分类号 TP393.8 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.024

Analysis for Network Security by Stochastic Petri-net

JIAO Jian CHEN Xin
(School of Computer Science, Beijing Information Science & Technology University, Beijing 100101, China)

Abstract Network attack graph is an important means of network security. The traditional attack graph and the attack path solution are difficult to describe in terms of probability the influence degree of the attack probability and Defense Technology on the whole scheme. Using stochastic Petri-net theory, this paper presented conversion algorithm which can make attack graph to Petri network defense scheme. Using stochastic Petri-net model generated by the algorithm can implement parallel analysis of attack and defense process. Experimental results show that the method can quantify probability of attack process effectively, also can help to analyze the effect of different defense technology on the overall system security.

Keywords Attack graph, Stochastic Petri-net, Network defense

1 引言

传统网络安全系统主要涉及防火墙、IDS、防病毒等设备。随着网络容忍、灾备等概念的深入,新型网络安全设备不断出现,应变不同网络的网络安全方案也随之具有多样性。针对日益复杂的系统,网络安全的设计者需要从网络设计方案的目的出发,对设计方案的可行性进行深入的分析。

目前网络安全中通常采用攻击树[1]和攻击图[2]方法进行分析工作。基于攻击图的安全分析方法于1998年提出[3],目前已经成为一种重要的安全研究手段。由于网络攻击过程具有突发性特点,有必要在研究中引入随机因素。文献[4,5]分别使用 Markov 模型讨论了网络容侵结构下的攻击者行为和系统响应。文献[6]则使用 SAN 来分析入侵的模型,验证容侵机制的安全性能,建立入侵者对系统的影响并求解安全性能指标。文献[10]采用随机回报 Petri 网络,实现了对网络容灾技术的可行性的概率评估。

Petri 网模型虽然可以很好地分析和验证系统的性能,但其建模过程相对复杂繁琐,需要使用者具备较好的理论和丰富的建模经验,这对于广大网络安全管理人员来说有一定的困难。也正是由于该问题,导致网络安全模型分析技术难以推广普及。

本文提出了一种建立在网络攻击图基础之上的随机 Petri 网系统安全分析方法。该方法首先自动生成网络攻击图,将图中的攻击状态和攻击活动转换为 Petri 网中的库所与变迁,按照攻击活动发生的概率配置变迁的系数,并添加关于防御的顺时变迁。

本文第1节为引言;第2节论述网络攻击图的主要生成技术;第3节在构造网络攻击图的基础上给出攻击图到随机 Petri 网模型的转换算法;第4节则结合实际的应用对方法予以验证。

2 理论基础

网络攻击图最初应用于网络脆弱性的分析,主要内容为描述攻击者可能的攻击路线[11],帮助安全人员实现有针对性的安全防护。例如文献[7]通过引入 Agent 技术,在攻击图基础上构建多 Agent 风险评估模型。按照图中元素的含义又可以分为状态攻击图[8]和属性攻击图[9]两种。前者描述攻击后网络的全局状态,后者则分别表示攻击和攻击相关的前因后果信息。

最早提出的网络攻击图采用手工构建方法,随着网络规

到稿日期:2013-04-05 返修日期:2013-05-10 本文受北京市教委科技面上项目(KM201211232010)资助。
焦 健(1978-),男,博士,讲师,主要研究方向为网络安全、Petri 网理论与应用,E-mail:jiaojian@bistu.edu.cn;陈 昕(1965-),男,博士,教授,主要研究方向为网络测量与网络安全。

模的不断增大，该方法难以应对较大规模的网络，因而产生了攻击图自动生成方法。目前攻击图的生成方法可以分为3类，包括基于模型检验的方法[12]、基于搜索算法的方法[13]和基于逻辑推理的方法[14]。本文采用基于逻辑推理的方法，攻击图的基本生成元素可表示为网络中的安全状态和攻击操作两种元素，定义如下：

定义1 网络系统安全状态，表示为 $P=\{p_1,p_2,\cdots,p_n\}$。p_i 是表示系统属性状态的断言。p_i 的形式为 $P(X)$，其中 P 是谓词，X 为参数集。如：

hasService(host,servicename,protocol,port,privilege)

表示主机 host 是否以 privilege 权限运行 servicename 服务，使用 protocol 协议和 port 端口。

为描述方便，本文重点采用网络系统安全状态中系统的操作权限组成部分，例如攻击者在网络节点中的操作权限，以便完成网络的攻击建模。

定义2(攻击操作，A) 利用攻击手段使网络系统安全状态发生改变的操作，记为 $attack=(from,m,to)$。其中 $from$ 表示攻击操作的源节点，$m\in M$ 表示攻击操作使用的攻击手段，to 表示攻击的目标节点。源节点和目标节点是攻击操作的作用对象。

定义3(攻击图，Attack graph) 采用有向图结构描述攻击一个网络目标的所有攻击路径，记为 $AG=(P,A,E,p_{goal})$，其中，P 表示网络系统的属性状态集合，包括初始状态中的属性状态以及攻击操作产生或改变的属性状态；A 表示一系列攻击操作的集合，A 与 P 组成攻击图的顶点集合；$E\subseteq(P\times A)\cup(A\times P)$，表示攻击操作与属性状态之间的关系，是攻击图的边集合；$p_{goal}\in P$ 表示对攻击目标状态的期望，即攻击目的。

3 随机 Petri 网模型的生成

随着网络中攻击的发生，网络的防御也同时相应发生，因此在网络安全过程中需要考虑网络攻击与防御的并发性。本文可以采用如图1所示的方式，即在攻击和防御两个顺时变迁中，加入库所 P_pre 用于描述在持续攻击的过程中防御对攻击的制约活动。

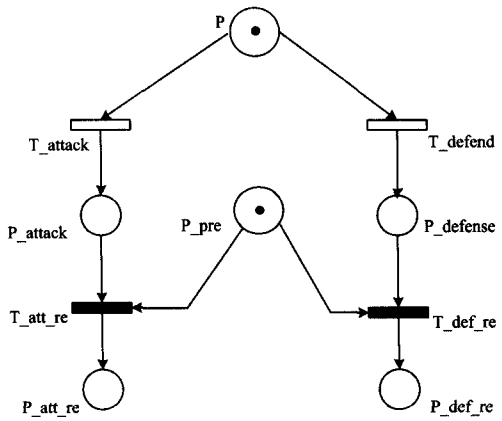

图1 攻击防御变迁发生图(sgn)

在构造网络攻击图的基础上，对攻击图实施基本的 Petri 网的模型转换，假设基本的 Petri 网模型表示为 $SGN=(N,P,T,M0)$，具体转换的算法如表1所列。

表1 Petri 网模型的转换算法

算法输入：攻击图 AG；输出：Petri 网 SGN
1)遍历 AG 中的 P，if P 不为空，取出 p 执行 2)，否则
2)IF $p()p_{goal}$ 执行 3) ELSE 跳到 7)
3)p→P P→SGN
4)IF p×t∈E∧ t(attack)in Defense Then sgn→SGN
5)ELSE T′→SGN
6)返回 1)
7)添加恢复态 T(返回终止状态)
8)退出

在转换过程中，攻击图中的状态 P 转换为 SGN 中的库所 P，攻击图中代表攻击动作的 t 操作则转换为 SGN 中的 T，如果操作的 t 对应防御动作，则在这种情况下，引入 P' 对 SGN 图实现防御活动的扩充。在算法的最后部分，为了实现 Petri 网的闭环结果，通过添加恢复 T 返回 SGN 的初始库所，其意义在于表示对攻击后的目标节点实施恢复工作，实现系统的复原。

4 实例验证

图2为计算机网络防御中典型的 DMZ 模型，Domain_A 中使用 FW1/IDS1 和 FW2/IDS2 对内部网络和服务区内部的网络实施保护，在 sendmail、oracle 和 Tomcat 中均存在一定漏洞，可被用于实现网络攻击。网络安全威胁从外部网络发起，可以由 Domain_A 渗透至 Domain_B 中，也可以由 Domain_B 重新对 Domain_A 目标实施攻击。在该网络中，假定从 Externalnet 发起的外部攻击可以首先向 Domain_A 中 Sendmail 发送带有病毒的邮件，而后感染病毒的邮件可以向 Domain_B 的主机实施病毒扩散，造成 H1—H3 的主机感染病毒，并由感染病毒向 Domain_A 中运行 Oracle 的服务器实施 DDOS 攻击；另一条攻击途径则是由感染病毒的 Sendmail 主机向运行有 Tomcat 的主机实施漏洞获取，在完成获权任务后，通过 Web 技术实现对 H1—H3 主机的感染和传播，继而完成由 Domain_B 向 Oracle 服务器的 DDOS 攻击。

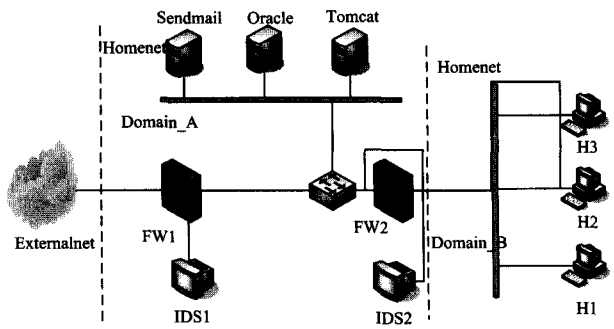

图2 基于 DMZ 的网络防御图

根据该网络防御的场景构建攻击图，如图3所示。网络中主要依靠 DMZ 中的 FW 和 IDS 充当防御功能，FW 负责对拒绝服务攻击实施阻断，IDS 则针对邮件和网页中的病毒代码实施检测预警和相应的响应动作。在该过程中，假定 W 与 IDS 都需要有一定的工作延迟，并且该延迟随机性满足指数分布。

执行模型的转换算法，获得构建描述该攻击/防御过程的 Petri 网模型，如图4所示。在该图中，P_init 表示系统的初始库所，在初始环境下，变迁 T_ids1_vir 表示在攻击开始阶段 IDS 检测到变化，进入库所 P_def_vir，触发顺时变迁 T_fi_virs

实现防火墙恶意攻击行为的阻断，进入安全状态 P_def_virs；当变迁 T_ids1_nvir 发生时，攻击避开 IDS 的检测，病毒进入 Sendmail 服务器，标示为 P_udet_vir；在该状态下，可以发生 Sendmail 到 Tomcat 服务器之间的攻击，T_ids1_web 表示 IDS1 对其攻击实现检测，进入库所 P_det_web 内容，最终到达安全库所 P_def_web；当变迁 T_ids1_web 发生时表示攻击已经从 Sendmail 服务器进入到 Tomcat 服务器中，而后通过变迁 T_ids2_uvir 越过 IDS2 实施针对 Domain_B 内部网络的攻击；当该变迁进入到 P_gain 状态时，病毒通过已经获得的 Domain_B 的主机权限实现拒绝服务工具。变迁 T_filt_DDOS 表示该拒绝服务攻击由 FW2 隔断，进入到正常状态 P_def_DDOS。变迁 T_filt_uddos 表示 FW2 的阻断失败，Oracle 最终遭受到攻击。

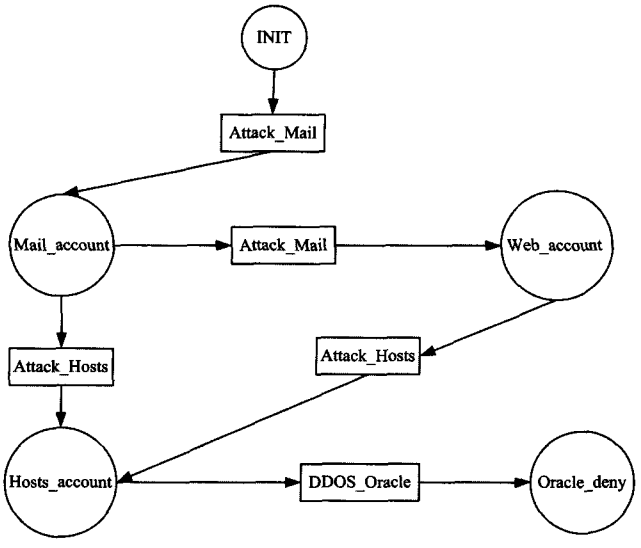

图 3　攻击图

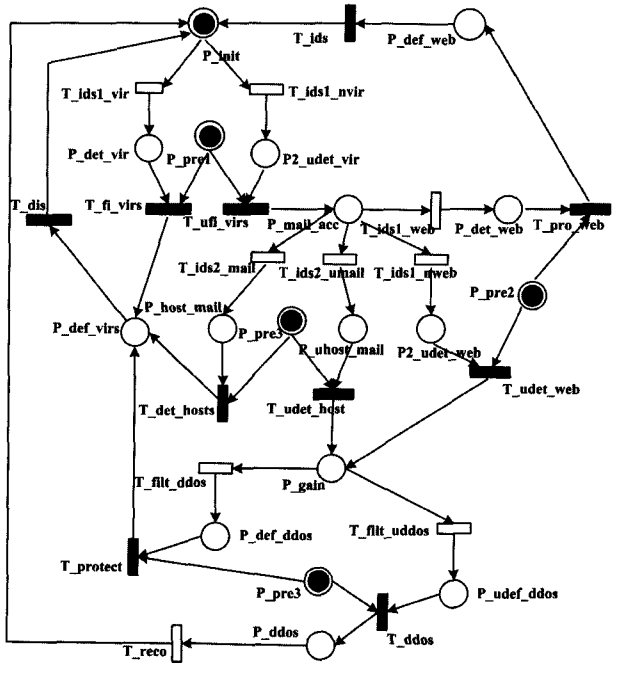

图 4　随机 Petri 安全防御模型

为保证系统的闭环特性，在随机 Petri 网模型中添加瞬时变迁 T_protect 表示系统在防御成功后立即返回到初始状态，增加随机变迁 T_reco 用于描述系统从遭受到 DDOS 攻击到系统恢复为正常状态的过程。

在安全系统的防御过程中，FW 和 IDS 反应延时的随机性是整个系统的安全的关键。对于整个网络而言，攻击的最终效果是用 DDOS 攻击使服务崩溃，在这种情况下，P_ddos 的稳态概率就是整个系统遭受攻击的可能性，因此整个系统的安全概率可表示为：$S=1-Pr(P\_ddos\geqslant 1)$。表 2 为通过实际测量和比对获得的关于变迁的 λ 初始值。

表 2　模型参数(λ)集

参数	初始值
T_ids1_vir	1.5
T_ids1_nvir	1.6
T_ids1_web	1.2
T_ids1_nweb	1.5
T_ids2_mail	1.3
T_ids2_umail	1.7
T_filt_ddos	1.8
T_filt_uddos	1.5
T_reco	0.5

为研究不同安全设备对整个网络安全的影响，在初始值一定的情况下，分别对 T_ids1_vir、T_ids1_web、T_ids2_mail 和 T_filt_ddos 的延时进行调整(其调整范围保持在 0～2 之间)，观察系统的稳定值变化，如图 5 所示。

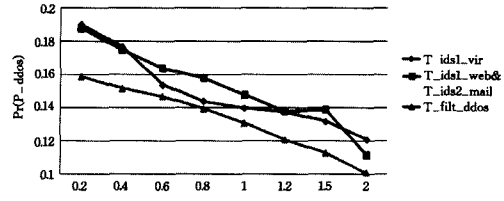

图 5　P_ddos 稳态概率趋势

从图中分析可知，随着 4 种变迁 λ 值的增加，系统遭受攻击的概率呈下降趋势。其中，T_ids1_vir 由于距 P_ddos 库所位置较远，因此对攻击概率影响较小；T_ids1_web 和 T_ids2_mail 在攻击图中所处的位置基本一致，因此其 λ 的变化程度对 P_ddos 稳态概率的影响是一致的。变迁 T_filt_ddos 直接决定最终攻击发生的成功概率，因此其变迁速率的改变对 Pr(P_ddos)的影响最为明显。由分析结果可知，网络安全防御过程中，距离最终安全目标较近的安全设备对整个安全方案的影响效果最为明显。

结束语　本文在网络安全攻击图的基础上，引入随机 Petri 网理论，实现了网络攻击图到 Petri 网的自动转换，在具有攻击和防御功能并发的 Petri 网模型中，通过对指定库所稳态概率的计算，得到整个系统的安全系数，同时可以通过分析其防御变迁速率的变化，进一步获得不同防御设备对整体防御方案的影响。

本研究接下来将引入人为因素对 Petri 网模型的影响，力图使模型的描述更加精确化，这对网络安全的推演具有一定的指导意义。

参 考 文 献

[1] Schneier B. Secrets and Lies: Digital Security in a Networked World [M]. New York, USA: John Wiley & Sons, 2000

[2] Man Da-peng, Zhang Bing, Yang Wu, et al. A method for global attack graph generation [C]// Proceedings of 2008 IEEE International Conference on Networking, Sensing and Control. Sanya, China: IEEE Computer Society Press, 2008: 236-241

(下转第 134 页)

聚集并快速传播。当然，在网络检测到恶意程序时，可以采取免疫策略，但如果对于网络的分割不在恶意程序爆发传播到度高的节点之前，那么免疫策略就会失效。

此外，为了仿真验证采用免疫策略后，改进的模型与原SEIR恶意程序传播模型的网络节点感染数的区别，假设$\gamma_k=0.06$，$\beta=0.5$，$\gamma=0.3$，采用动态免疫策略后，网络中被感染的I节点的个数随时间演化的曲线如图7所示。从图7中我们可以看出，在$t=22$之前，使用动态免疫策略时的病毒爆发速度较未使用免疫策略后的病毒爆发速度稍快，但当时间步数$t>22$后，使用动态免疫策略后的病毒爆发变得缓慢，网络最终被感染的节点数为2489；未使用免疫策略的网络在$t=23$后感染节点数继续增长，直到$t=36$时，增长速度减慢，几乎达到稳定状态，网络最终被感染的节点数为3021，比使用动态免疫策略多感染了近530个节点。

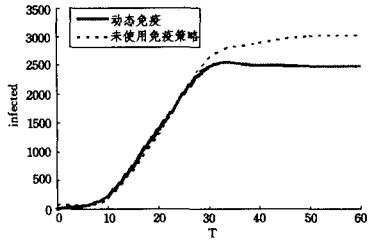

图7　网络中感染节点随时间演化的曲线

结束语　Ad hoc网络是一种新颖的移动计算机网络的类型，它既可以作为一种独立的网络运行，也可以作为当前具有固定设施网络的一种补充形式。其自身的独特性，赋予其巨大的发展前景。在Ad hoc网络的研究中还存在许多亟待解决的问题：设计具有节能策略、安全保障、组播功能和QoS支持等扩展特性的路由协议，以及Ad hoc网络的网络管理等。

本文针对传统模型预测的恶意程序感染率在实际应用中偏低的问题，通过引入网络拓扑特性和免疫力等概念对恶意程序传播模型进行了改进，结合网络拓扑动态演变恶意程序传播过程，设计出改进的传播算法和动态免疫策略算法。实验表明，该模型对遏制恶意程序的传播具有良好的效果。因此，研究无线环境下恶意程序的传播机制和改进流行病模型，对积极开展网络恶意程序的防治工作具有重要的促进作用。

参考文献

[1] 王长广. 无线环境下恶意程序的传播机制研究[D]. 西安：电子科技大学，2006

[2] 王长广，沈玉龙，马建峰，等. 一种蓝牙环境下恶意程序的传播模型[J]. 西安电子科技大学学报，2009，36(1)：94-98

[3] 陶智飞. 网络病毒传播模型及两阶段动态免疫策略研究[D]. 武汉：华中科技大学，2006

[4] 副帅，往长广，马建峰. 无线传感器网络中恶意程序的传播模型[J]. 计算机工程，2011，37(3)：129-131

[5] 杨春霞，胡丹婷. 动态演化的互联网病毒建模与分析[J]. 计算机应用研究，2012，29(7)：2678-2680

[6] 陈丹伟，唐平，周书桃. 基于沙盒技术的恶意程序检测模型[J]. 计算机科学，2012，39(6)：12-14

[7] Royer E，Melliar-Smith P M，Moser L. An analysis of optimum node density for ad Hoc mobile networks[C]// Proc. IEEE. ICC，June 2001：857-861

[8] Yoon J，Liu Ming-yan，Noble B. Random waypoint considered harmful[C]// Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. 2003：1312-1321

[9] Bettstetter C，Krause O. On border effects in modeling mo simulation of wireless ad hoc networks[C]// The 3rd IEEE International Conference on Mobile and Wireless Communication Networks. August 2001

[10] Bettstetter C，Resta G，Santi P. The node distribution of the random waypoint mobility mobility for wireless ad hoc networks [J]. IEEE Transactions on Mobile Computing，2003，2(3)：257-269

[11] 方宝平. 复杂网络的病毒传播及免疫策略[D]. 合肥：安徽大学，2011

（上接第121页）

[3] Phillips C，Laura S P. A graph-based syatem for network vulnerability analysis[C]// Proceedings of the 1998 Workshop on New Securityparadigms. VA，USA：ACM，1998：71-79

[4] Wang Da-zhi，Bharat B M，Kishor S. Security analysis of SITAR intrusi on tolerance system [C]// Proceedings of the 2003 Workshop on Survivable and Self-Regenerative Systems，in Association with 10th ACM Conference on Computer and Communications Security 2003. New York，USA：Association for Computing Machinery，2003：23-32

[5] Wang Fei-yi，Jou F，Gong Feng-min，et al. SITAR：Scalable intrusion tolerance architecture for distributed services [C]// Proceedings of the IEEE Second SMCInform at ion Assurance Workshop. West Point，New York，USA：IEEE Press，2001：38-45

[6] Singh S，Cukier M，Sanders W H. Probabilistic validation of an intrusion tolerant replication system [C]// Proceedings of the International Conference on Dependable Systems and Networks. San Francisco，USA：IEEE Press，2003：616-624

[7] 杨宏宇，江华. 基于攻击图的多Agent网络安全风险评估模型[J]. 计算机科学，2013，40(2)：148-152

[8] Swiler L P，Phillips C，Gaylor T. A Graph-Based Network-Vulnerability Analysis System[C]// Technical Report SAND97-3010/1，Sandia National Laboratories. Albuquerque，New Mexico and Livermore，California，1998

[9] Ammann P，Wijesekera D，Kaushik S. Scalable Graph-Based Network Vulnerability Analysis[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. New York：ACM Press，2002：217-224

[10] 张冬艳，陈红松. 基于随机Petri网的容灾系统安全性分析[J]. 清华大学学报：自然科学版，2011，51(10)：1281-1286

[11] Cynthia P，Laura P S. A graph-based system for network-vulnerability analysis system[C]// ACM New Security Paradigms Workshop. 1998

[12] Jha S，Sheyner O，Wing J M. Minimization and reliability analyses of attack graphs [R]. Technical Report CMUCS-02-109. Carnegie Mellon University，February 2002

[13] Jajodia S，Noel S，O'Berry B. Topological analysis of network attack vulnerability[C]// Managing Cyber Threats：Issues，Approaches and Challenges. Springer-Verlag，2005：248-266

[14] Ou Xin-ming，Boyer W F，McQueen M A. A Scalable Approach to Attack Graph Generation[C]// CCS'06. Alexandria，Virginia，USA，2007：336-345