基于随机博弈模型的网络攻防量化分析方法

王元卓[1)] 林 闯[2)] 程学旗[1)] 方滨兴[1)]

[1)](中国科学院计算技术研究所 北京 100190)

[2)](清华大学计算机系 北京 100084)

摘 要 针对日益普遍和多样的网络攻击和破坏行为,如何利用模拟真实网络的虚拟环境,实现对网络各种攻防过程的实验推演,并分析评价网络系统安全性,已逐渐成为热点研究方向.对此文中提出了采用随机博弈模型的网络攻防实验整体架构,提出了由网络连接关系、脆弱性信息等输入数据到网络攻防博弈模型的快速建模方法,基于最终生成的攻防模型可以对目标网络的攻击成功率、平均攻击时间、脆弱节点以及潜在攻击路径等方面进行安全分析与评价.最后,应用研究所得的网络攻防模型与分析方法对一个典型的企业网络攻防过程进行分析和推演.结果表明了模型和分析方法的有效性.

关键词 网络安全;攻防模型;脆弱性;随机 Petri 网;随机博弈网

中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2010.01748

Analysis for Network Attack-Defense Based on Stochastic Game Model

WANG Yuan-Zhuo[1)] LIN Chuang[2)] CHENG Xue-Qi[1)] FANG Bin-Xing[1)]

[1)](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)

[2)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract Network ranges can be provided for network attack and defense experiments to simulate real network in a virtual environment, and deduct the process of network threats. This paper presents an overall framework of the network range based on security attack and defense model. In the model, the stochastic models and game model are used, and a series of security attack and defense model algorithm and the security analysis techniques are proposed. Finally, the application of network attack and defense modeling approach on a typical enterprise network attack and defense process of analysis and inference. The results show that the model and analysis approach above proposed is feasible and effective.

Keywords network security; attack-defense Model; vulnerability; stochastic Petri nets; stochastic game nets

1 引 言

近年来,网络空间的争夺日益激烈,控制信息权和话语权成为新的战略制高点;现实空间的渗透和恐怖袭击正与网络空间的渗透和恐怖袭击更紧密地结合在一起,成为人类社会面临的新威胁;不断增长和扩散的计算机病毒(如木马、蠕虫)和黑客攻击等

收稿日期:2010-04-25;最终修改稿收到日期:2010-08-12.本课题得到国家自然科学基金(60803123,60933005,60932003,60873245)资助.**王元卓**,男,1978 年生,博士,助理研究员,主要研究方向为网络及信息安全、系统性能评价、随机博弈模型等.E-mail: wangyuanzhuo@ict.ac.cn.**林 闯**,男,1948 年生,博士,教授,博士生导师,主要研究领域为系统性能评价、计算机网络、随机 Petri 网等.**程学旗**,男,1971 年生,博士,研究员,博士生导师,主要研究领域为信息安全、互联网挖掘与搜索、舆情计算.**方滨兴**,男,1960 年生,教授,博士生导师,中国工程院院士,主要研究领域为计算机体系结构、信息安全和计算机网络等.

大量信息时代的“衍生物”,对信息化程度较高的金融、交通、商业、医疗、通信、电力等重要国家基础设施造成严重的破坏,成为影响国家安全的新威胁.保护网络空间安全作为重大挑战之一,已与防止核恐怖事件、利用核聚变能量等一起被列为新世纪亟待解决的难题.

针对大规模复杂形态的网络空间安全问题,最有效的研究手段是在现实的网络空间中实现对网络协议、网络行为、网络性能等的分析,获得最真实有效的数据,并将研究成果应用到真实场景.然而在现实网络上进行各种实验和测试,由于其带来的潜在巨大影响甚至颠覆性破坏作用,几乎是不可行的,因而通常的手段是根据已有数据推演出的模型建立起网络仿真环境来试图重现真实的网络行为和模拟各种技术手段的实施.然而这种方法在实际运用中面临很多挑战,其最大难题是构造网络仿真环境的成本很高,重新配置或共享资源(如设备、软硬件系统等)非常困难,运用起来缺乏灵活性,所以一般只局限在小规模的网络范围,不能实现大规模网络中的多种通信流量、拓扑和行为的融合.此外,单一组织机构的资源有限,对于网络空间安全问题的快速响应和应对需要多个组织机构之间复杂、大规模的合作,这种合作不仅需要数据的共享,更要求计算资源、通信资源、设备资源、软件资源甚至人力资源等的共享和动态重组.

在网络模拟和测试中,协议模型、流量模型和拓扑模型的建立和处理,涉及到高密度的计算,要求很高的分析与计算能力,并且有一定的时限要求,同时具有计算密集型和数据密集型的特点.这种特点使得网络模拟通常因为受到软硬件资源的限制,而无法同时展现现实网络的全部特性,也很难对安全事件的影响进行分析.网络空间事件的分析和模拟需要先进的分布式计算技术提供高性能、高吞吐率的方法来管理、访问、整合、分析分布的海量数据,有效调动系统中的所有计算、存储和网络资源,为安全问题研究活动提供透明的分析计算服务.

人们已经越来越认识到专业计算基础设施在支持安全保障工作方面的重要作用.许多国家级安全保障和网络实验基础设施项目正在被立项或已经在实施当中,其中,网络攻防实验环境的概念已逐渐被各国和著名研究机构所认可,并将其的建设和关键技术的研究列为重点地研究和发展方向,使之成为模拟真实网络攻防的虚拟环境,针对电子攻击和网络攻击等手段进行实验.攻防实验环境的主要任务包括:在典型的网络环境中对信息确保能力和信息生存工具进行定量、定性的评估;对目前和未来可能出现的网络攻击行为、和用户反应进行模拟;在有限的基础设施上,同时进行多个独立的实验;通过使用科学方法对网络安全和性能进行测试和预测.

目前,网络攻防实验环境的实现可以通过真实设备、虚拟设备、网络模拟等多种技术手段.其中,由真实设备构建的网络攻防实验环境需要将目标网络的主要设备和网络结构进行复原,其测试的结果准确,但造价高且可扩展性差;基于仿真和模拟技术实现的实验环境相对造价较低,但仍需购置高性能计算设备,并作有针对性地仿真程序开发.所以尽管上述方法在确认网络攻击方面有一定的价值,但是存在很大的局限性,较难保证在大规模的系统分析中,特别在面临网络系统的日益复杂的结构时,他们会难以适用[1].文献[2]开始将基于随机模型的分析方法引用到网络安全性评价中来,并且后面的研究也得到了很好的效果[3-4].而随机假设在描述系统某些因素,特别是未知的网络攻击行为时是很必要的.同时,在网络安全问题上,对系统行为进行某些随机假定是合理的,例如,攻击的入侵和发现,攻击者对入侵手段的随机选择.然而,在网络安全性分析中,网络攻击是一种人为行为,它形成的根本原因与人的利益驱动具有很大的关系.与前面几种方法相比随机模型方法可以对系统局部行为进行有效的分析.且该方法具有很强的可扩展性和很低的造价.对未知的攻击手段的分析具有重要的意义.进一步引入博弈理论的随机博弈模型可以较好地描述网络攻防中“人”的因素对事态发展的影响,并可基于此模型分析各种安全防御策略和机制的有效性.因此,基于随机模型的网络攻防实验建模分析技术为网络安全性分析和预测提供了可行的新思路和新技术,这将是一个重要的充满前景的研究方向.

网络攻防模型与分析技术的研究主要包括如下4方面内容:

(1)网络设备及网络结构模型.作为网络攻防实验的基础,我们要以模块化建模思想,研究描述各种网络环境下,典型设备的功能模型,并提出根据实验拓扑关系快速生成描述实验目标的网络模型.

(2)网络攻防行为模型.从实际问题中抽象并建立攻击模型.网络攻击直接威胁网络安全性,通常是网络攻防实验的主要内容.当前新的网络攻击技术和工具不断出现,攻击具有随机性、多样性、隐蔽性和传播性,使用单一的规则很难对其进行描述.攻

击模型的建立主要存在两个困难：一方面网络攻击是攻击者发起的有意图的破坏行为[3-4]，人们很难精确刻画这些攻击行为的人为意图；另一方面网络的巨大规模和复杂结构使得网络安全性分析异常困难.

(3) 攻防博弈策略模型. 网络攻击成功与否，除了攻击能力的强弱外，针对性的防御措施也是重要的影响因素，在攻防行为交互的过程中博弈关系处处存在[5-6]，基于攻防博弈策略模型的研究不但可以清楚地分析攻防过程，同时也为有效的防御策略的选择提供有力的依据.

(4) 安全性分析与评价. 建立可量化和可操作的安全性分析与评价指标，是网络攻防实验最直接的结果展示，是实现上述模型应用价值的最终目标. 同时，针对特定的网络系统，人们需要一套系统的思路和方法来进行安全性的定量分析[7]. 建立一套方便有效的网络攻防模型的分析与评价方法是一个具有挑战性和应用价值的关键问题.

本文第 2 节讨论网络安全模型研究的相关工作；第 3 节给出基于安全攻防模型的网络攻防实验环境的整体框架设计；第 4 节主要研究网络攻防实验环境中用到的网络安全攻防模型；第 5 节研究基于网络攻防模型的安全分析与评价技术；第 6 节把模型与分析技术的研究成果应用到实际案例当中；最后在第 7 节总结全文并给出进一步的研究方向.

2 相关工作

目前，面向网络攻防实验的安全行为模型、博弈模型以及安全评估与分析方面的研究工作还处于起步阶段，尚未形成系统化的理论方法. 已有的相关领域的研究工作可概括为以下几个方面.

(1) 网络安全模型方法

网络安全的模型分析方法主要包括组合模型方法、模型检测、基于状态的随机模型方法和基于模型的高级随机模型方法. 组合模型方法主要包括故障树、攻击树和攻击图等[8-10]，这些方法依赖于事件的独立关系，思路简单，并对某些特定网络的分析比较有效. Ramakrishnan 等人提出了另一种使用模型检测器进行分析的模型方法[9,11]. 它主要针对主机配置进行安全分析. 要产生基于模型的脆弱性分析工具，除了建立适合实际的模型、实现模型的自动分析外，还需要模型的自动生成以及大量的渗透攻击技术进行自动建模的工具. 文献[12-13]对系统的形式化描述进行状态可达性分析. 相比之下，各种随机模型方法(例如：马氏链、马氏报酬过程、隐马氏过程、随机 Petri 网和随机决策方法等)[14-16]更易对网络系统状态进行全面有效的描述，精确刻画网络系统随机行为以及组件之间的相互关系，便于计算各种安全性指标. 其中随机 Petri 网是基于状态的随机模型分析方法中的一种行之有效的方法[17]. 它对系统的并发性、异步性和不确定性具有很强的动态分析能力，同时具有建模原语少、符合直观的图形表示等优点，它既能描述系统状态，又能表现系统行为，且全局的状态和行为不是最基本的概念，而是由局部的状态和行为组合得到的，特别适合于对系统建模与分析. 同时，又可以通过随机 Petri 网与马尔可夫过程同构的特性，求解网络系统的各种特性参数. 而直接使用基于马尔可夫过程的随机模型，却很难实现对模型的扩展. 例如在实际系统中，一旦系统的资源增加或减少，相应的马尔可夫链的结构就可能会发生很大的变化，而在随机 Petri 网模型中，只要通过增加相应位置中的标记数就可以建立相应的模型. 并且随机 Petri 网可以在一个系统模型的框架上采用图形化的方式完成系统的描述、安全性分析以及系统的验证和测试. 这是其它的方法所不具备的功能.

(2) 网络攻击模型

攻击是攻击者对系统进行的有特定目的的行为，可能造成系统的安全性破坏. 网络攻击模型可以进一步分为攻击者模型、攻击行为模型和攻击影响模型. 关于攻击者模型的研究还比较浅显，主要包括经验模型、先验知识模型，自学习能力模型. 例如，文献[18]在安全性评价的随机模型中比较详细地描述了攻击者的属性，包括熟练程度和经验技能等. 在此之上，文献[16]引入了攻击潜力，并借此刻画攻击行为的发起过程. 另外，攻击者的决策模型也将是攻击建模的一个重要方面. Jonsson 和 Olovsson[19] 针对一类特定的工作站系统进行实际的攻击实验，从攻击者的角度出发分析攻击行为过程及其定量的统计规律. McDermott 从攻击影响的角度将攻击行为分为多个状态阶段[16]，抽象了服务器的行为及其与攻击者之间的交互. 人们已经定义了两种安全性故障：随机故障[20]和发起故障. 随机故障从故障发生的类型和频率的角度描述；而发起故障则从攻击者的意图上进行描述，并采用攻击潜力指标来刻画. 文献[21]将存在攻击威胁的服务器分为 4 个状态：正常状态、脆弱状态、报警状态和失效状态. 服务器在各状态的停留时间分布与攻击潜力相关. 针对网络

环境和评价目标选择适当状态转移速率,可以获得必要的安全性指标.

(3)攻防博弈模型

博弈论已被应用于解决网络安全相关的研究中.文献[22]中,提出了一个基于博弈论的安全事件分析方法.攻击者与防御者之间的对抗被描述成一个二人的博弈问题,并希望通过均衡的计算来寻找最优策略.文献[23]提出了一个新的协议来阻止恶意侵占带宽以及如何用博弈论方法来描述,并说明该协议的有效性.文献[24]提出了一个基于攻击动机的博弈方法来模型攻击者的动机、目标和策略(AIOS).其中作者研究了一个基于博弈论的形式化描述框架,采用它可以捕获 AIOS 与防御者目标策略之间的内在关系,从而获得应对办法.文献[25]和文献[26]研究了基于博弈论中拍卖理论的机制,来抵御 DoS 和 DDoS 攻击.在文献[27]中,Xu 和 Lee 使用博弈论框架分析了他们所提出的防御 DDoS 攻击系统的性能.Browne 在文献[28]中描述了在复杂、异构的军事系统中,如何用静态博弈来分析网络攻击事件.文献[23]则采用 博弈论来定量分析攻击者的行为. 在随机模型的基础上,文献[29-30]提出了应用于网络攻防分析的随机博弈网模型,该模型可以较好地描述随机系统中的攻防博弈问题.

3　基于攻防模型的网络攻防实验环境

本文研究的基于攻防模型的网络攻防实验环境,以模块化的随机模型和博弈模型为基础,利用攻防实验环境提供的模型和分析工具,可以实现对目标网络系统的快速建模,并可通过参数的设置,描述多种网络环境和安全问题,并基于目标网络的模型,实现对相关安全指标的评估和有关安全问题的关联分析.

3.1　基于模型的网络攻防实验环境整体架构

基于模型网络攻防实验环境的整体架构如图 1 所示.

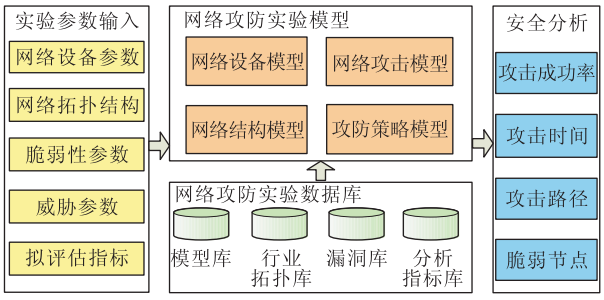

图 1　基于模型的网络攻防实验环境整体架构

在图 1 中,我们将基于模型网络攻防实验环境分为 4 个主要的部分,分别是实验参数输入、网络攻防实验数据库、网络攻防建模以及安全分析与评价.其中,实验参数输入部分,负责收集实验所需的对目标网络的描述和具体参数,包括目标网络中网络设备类型、参数和设备间的拓扑连接关系以及实验所需的脆弱性、威胁相关的参数和期望的输出结果.网络攻防实验通过数据库的形式将已有的研究成果模块化,供实验者调用,其中模型库包含典型网络设备和结构的模型,同时还针对不同的实验要求,提供基于模型的多种评价分析算法.利用这些模型算法和实验参数,使用者可以较方便地建立起目标网络的实验模型,根据实验需求的不同,可以分为网络设备模型、网络拓扑模型、网络攻击模型以及攻防策略模型等.基于这些模型我们可以对目标网络的安全性进行评估,并可对相关数据进行关联分析,为使用者提供更多有用的信息.

3.2　网络攻防实验中的建模与分析过程

在图 1 所示的整体架构下,我们采用下面的过程对一个网络攻防实验进行建模和分析,其中使用的一系列模型和分析算法,将在下面的章节中作重点介绍.

1. 根据网络设备参数,建立网络设备脆弱性模型;

2. 根据输入的网络拓扑结构,建立网络设备的连接关系模型;

3. 根据实验要求,描述攻击行为信息和防御手段信息;

4. 由算法 1 生成描述攻击关系的攻击图;

5. 由算法 2 生成对应的随机 Petri 网攻击图;

6. 在随机 Petri 网攻击图模型上引入策略和效用的信息生成攻击视角的攻防随机博弈网模型;

7. 建立防御视角的攻防随机博弈网模型;

8. 由算法 3 计算攻防双方的均衡策略;

9. 由算法 4 组合步 6、7 中生成的攻、防视角的攻防随机博弈网模型来描述整体攻防策略;

10. 计算组合模型稳态参数,并进行评价与分析.

4　网络安全攻防模型

在上节提出的整体架构中,实现攻防实验的主体为网络安全攻防模型,如何快速,有效地建立描述目标系统的实验模型是研究工作的关键.在本节中,我们将安全攻防模型的研究分为网络设备模型、拓扑结构模型、攻防策略模型和网络攻击模型.通过这些基本模型的研究为实验模型的建立和分析评估提供基础.

4.1 网络设备模型和拓扑结构模型

攻击模型的生成需要具有基本的模型元素，模型元素抽象于实际的攻击过程，攻击过程依赖于目标网络结构，如何抽象描述网络的逻辑结构，是决定生成攻击模型的基础因素. 本节结合多年的工作经验，抓住网络攻击中的关键因素，对一般的网络结构进行抽象描述.

网络攻击建立在实际的网络拓扑结构上，网络拓扑包括网络中的设备、设备的连接情况以及设备上存在的漏洞，这里的设备仅指服务器及个人计算机，不包括连接设备，如路由器、交换机等. 所以在生成模型图之前，需要描述好网络的拓扑结构，以便能生成建立基于拓扑结构的攻击模型. 具体的说，就是要描述好网络中的主机或服务器、主机或服务器之间的连接情况以及主机和服务器上的漏洞信息.

网络攻击知识也需要提前建立好，即要形式化地描述好所有的漏洞利用方法. 这样，在有网络设备漏洞后，即可自动地展开攻击，并根据攻击的结果实施下一步的攻击，直到最后达到攻击目标.

下面我们给出基于主机设备和连接关系的模型要素：

设备脆弱性描述：〈设备名称，运行软件，开放服务，漏洞列表〉

设备脆弱性描述包含了所有主机设备的脆弱性信息，通常可以数据库的表的形式存在，表中每条记录代表了某个主机设备的 1 个漏洞. 设备名称是该设备在网络中的唯一标识. 运行软件是主机上安装了并正在运行的软件系统名称和版本，其中既可以包括操作系统也可以包括应用软件. 开放服务指运行的软件对应的服务，主要是应用层的，如 http、ftp 等. 漏洞列表指开放的服务存在的漏洞，由于目前漏洞分类还没有统一的标准，故此处假设所有漏洞都有一个唯一的标识，设备中可以存在多个漏洞. 设备名称和漏洞名称共同组成漏洞列表中每条记录的关键字，保证每条记录在整个漏洞库中的唯一性.

连接关系描述：〈设备 1，设备 2，服务，用户权限〉

连接关系指两个主机设备之间的逻辑连接，逻辑上存在着的服务访问关系. 连接关系库包含了网络中所有的主机之间的连接关系. 主机设备名称是该设备在网络中的唯一标识，服务协议指主机设备 2 对主机设备 1 开放的服务，如 http、ftp 等，用户权限指主机设备 1 拥有主机设备 2 服务所需的最小用户权限. 如匿名用户、授权用户或超级用户. 所有字段共同构成关键字，如果同样的服务，对应所有的权限，则取最小的权限.

攻击信息描述：〈漏洞名称，攻击行为，发起端，需要权限，得到权限〉

攻击信息指某种威胁利用脆弱性实施攻击的过程和结果. 其中，漏洞名称是漏洞在攻击信息里的唯一标识，它表示为一个具体的漏洞，具有唯一的编号. 攻击方法是漏洞利用的方法描述，关于攻击行为的分类还没有统一的标准，文章把攻击行为分成 4 类. 一种攻击方法可以对应同类的多个漏洞. 攻击的发起点对应攻击行为，分为本地和远程两类. 需要具有的权限指攻击者在攻击发起端所应该具备的权限，攻击结果指攻击者实施攻击者应该取得的系统用户权限，此权限应该是从无到有、从小到大的优先顺序.

在网络攻击中，有这样一些共识，便于下面建立模型：

(1) 用户权限集. 匿名 anonymous，授权用户 guest，超级用户 root/admin；可将权限集设置为(1，2，3)，分别代表前面 3 种权限，值越大，权限越高. 低权限可实施的攻击，高权限同样能，反之则不能；

(2) 本机和本机是完全连接的，存在着〈local，local，all，any〉；

(3) 远程可以发起的攻击，本地一样可以；

(4) 攻击总是遵循权限的从无到有、从小到大、需要避免不必要的攻击的原则；

(5) 攻击会使受攻击方产生若干的损失，而攻击者则通常会从中获益.

4.2 网络攻击模型

4.2.1 基于随机 Petri 网的攻击模型

在前面网络拓扑模型的基础上，本节定义随机 Petri 网攻击模型. 模型从攻击者的角度出发，以攻击者在网络系统中获取用户权限为目的，模拟攻击者在整个攻击过程中的权限变化过程.

定义 1. 随机 Petri 网(SPN). 随机 Petri 网可以描述成一个四元组 $SPN=(P,T,F,\lambda)$，其中

(1) $P=\{p_1,p_2,\cdots,p_m\}$，是有穷位置集合；

(2) $T=\{t_1,t_2,\cdots,t_m\}$，是有穷变迁集合；$(P\cap T\neq\varnothing)$，$(P\cup T\neq\varnothing)$；

(3) $F\subseteq(P\times T)\cup(T\times P)$，是弧的集合；

(4) $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_n)$，是变迁平均实施速率集合.

定义 2. 基于随机 Petri 网的攻击模型. 攻击模型 $ASPN=\langle P(P_i,P_o),T(a,v,c,\pi,q),F,M_0,\lambda\rangle$，其中

(1) $P=\{P_0,P_1,\cdots,P_m\}$是攻击可能存在的位置集合,其中,$P_k=(P_k^i,P_k^o)$,表示与攻击 k 相关联的位置,P_k^i表示攻击者发起时所在设备的名称,并用 P_k^i表示攻击者在该位置上的权限;P_k^o表示攻击者在实行攻击行为 k 后可能所处的位置,该类位置集合主要用来分离同一状态下的不同攻击;P 是有穷的,因为对于特定网络,网络设备数量、系统权限是有限的;

(2) $T=\{T_0,T_1,\cdots,T_n\}$是表示攻击行为的变迁集合,其中,$T_j=T_j(a,v,c,\pi,q)$, a 表示某一具体攻击行为,v 表示攻击利用的脆弱性,c 表示发起攻击时用户的权限,π 表示攻击发起的可能性,q 表示发起攻击后成功完成的可能性;T 是有限集合,因为对于特定的网络,存在的漏洞及攻击行为总是有限的;

(3) F 是有向弧线集合,连接位置和变迁,F 仅连接 P 和 T 的元素,在 $ASPN$ 中由弧连接的由 P^i 到 P^o的连通图表示一个攻击路径;

(4) M_0是初始标识,表示攻击开始的位置;

(5)λ 是时间变迁的平均实施速率集合,它反映了攻击行为的能力,本文假设攻击行为具有随机性且服从指数分布.

4.2.2　随机 Petri 网攻击模型生成方法

攻击者从特定的节点出发,对整个网络系统发起攻击,攻击图生成算法要得到攻击者在网络中可能发起的所有攻击,同时避免那些不必要的攻击.攻击图的生成过程也是整个网络攻击的动态模拟过程.

攻击者从当前位置出发,查询与当前主机设备相连的所有其它设备,得到连接关系,然后依次查询每个连接主机的漏洞信息,得到每个主机的漏洞列表,并依次判断每个漏洞是否可以利用,如果可以利用,则生成状态节点和攻击节点,否则放弃该漏洞,继续判断下一个漏洞,直到所有漏洞判断完毕,然后再返回到主机连接列表,判断下一个主机的所有漏洞,如上步骤,直到所有连接主机的所有漏洞都判断完毕,然后取当前主机的下一个用户权限,直到所有权限取完,再取下一个网络主机,重复上面的过程.在检查连接主机的过程中,将新主机加入网络主机列表中,在生成新的状态节点时,将主机的新权限加入网络主机列表.算法描述如下.

算法 1.　攻击图生成算法.

输入:初始状态,连接关系,设备脆弱性,攻击信息

输出:攻击图

1. 初始设备名称及权限入队列;
2. 生成初始状态节点;
3. While(网络设备队列不为空)
4.　取网络设备队列中 1 个设备;
5.　While(权限队列不为空)
6.　　取权限队列的 1 个用户权限;
7.　　生成新的连接设备队列;
8.　　依据当前设备名称查询设备连接关系,得到该设备的所有连接设备名称并将其加入连接设备队列;
9.　If(这些设备名称不在网络设备队列里)
10.　　将不在网络设备队列的连接设备名称加入网络设备队列;
11.　While(连接设备队列不为空)
12.　　取连接设备队列中的 1 个主机,生成新设备脆弱性队列;
13.　根据连接设备名查询设备脆弱性信息库,得到该连接设备所有脆弱性并将其加入设备脆弱性队列;
14.　While(设备脆弱性队列不为空)
15.　　取设备脆弱性队列的 1 个脆弱性;
16.　　根据脆弱性名称查询攻击知识库,得到脆弱性的利用方法信息;
17.　If(脆弱性可利用)
18.　　生成攻击节点和状态节点;
19.　　连接攻击节点和状态节点;
20.　If(攻击结果权限不在权限队列里)
21.　　结果权限加入权限队列;
22. 结束.

在攻击图生成算法的基础上,本节提出随机 Petri 网攻击模型的生成算法,该算法是要将攻击图转换为随机 Petri 网,并将攻击者的攻击目标(设备+权限)加入到模型中.由于确定了攻击目标,使得攻击策略有所改变,本文规定在攻击目标上不再发起对其它网络主机的攻击.

算法主要对图中每个状态节点进行检查,如果是攻击目标节点,则删除和它相连的所有攻击节点,否则统计其出度,出度是指与状态节点相连接的攻击节点的个数,如果出度大于 1,则有攻击分枝,在每条分枝插入 1 个瞬时变迁和 1 个选择状态.算法描述如下.

算法 2.　随机 Petri 网攻击模型生成算法

输入:攻击图,攻击目标

输出:基于随机 Petri 网的攻击模型

1. 初始化;
2. While(攻击图中状态节点队列不为空)
3.　取 1 个节点;

```
4.  if(该节点是目标节点)
5.    删除所有相连的攻击节点
6.  Else
7.    统计其出度 k;
8.    if(k>1)
9.     While(k!=0)
10.     取 1 条攻击分枝,生成瞬时变迁节点;
11.     连接状态节点和瞬时变迁;
12.     生成选择状态节点;
13.     连接瞬时变迁和选择状态;
14.     连接选择状态节点和当前状态节点后面连接
        的攻击节点;
15.    k--;
16.   取下一个状态节点;
17.   生成循环时间变迁 T 和目标节点;
18.   连接目标节点和 T;
19.   连接 T 和初始节点;
20. 结束.
```

4.2.3 算法分析

假设目标网络中有 m 台主机设备,每台设备有 n 个脆弱性,每台设备最多可与 $m-1$ 台设备相连,则每台设备要处理的脆弱性个数为 $(m-1)\times n$,总共需要处理的脆弱性个数为 $(m-1)\times m\times n$. 假设 1 个脆弱性的处理时间为 t,则算法 1 的时间复杂度为 $O(m^2nt)$. 依据上述假设,网络设备队列长为 m,连接设备队列长为 $m-1$,脆弱性队列长为 n,假设每台主机有 k 种操作权限,不考虑输入数据的存储空间,则状态节点数为 $m\times k$,攻击节点数为 $(m-1)\times m\times n$,连接弧数最多为 $m\times k\times(m-1)\times m\times n$;则算法 1 的空间复杂度为 $O(m^3nk)$. 算法 2 的整个过程是一个二重循环,假设攻击图的状态节点数为 k,每个状态节点最多有 w 个分枝,那么算法 2 的时间复杂度为 $O(kw)$. 算法 2 新增的存储空间为 $2\times k\times w$,只考虑新增的存储空间,则算法 2 的空间复杂度为 $O(kw)$. 由分析可见,整个算法的复杂度可以满足攻防实验推延的需求.

4.3 攻防博弈策略模型

在基于随机 Petri 网攻击模型的基础上,我们提出描述攻防博弈策略模型的随机博弈网[26-27]和攻防随机博弈网模型的概念和分析方法.

4.3.1 攻防随机博弈网模型

定义 3. 随机博弈网(Stochastic Game Net, SGN). 一个随机博弈 Petri 网可以用一个 9 元组表示,$SGN=(N,P,T,F,\pi,\lambda,R,U,M_0)$,其中

(1) $N=\{1,2,\cdots,n\}$ 表示局中人的集合,这里 $n<\infty$;对于 $k\in N$,用 A_k 表示局中人 k 的行为标记集合,并记 $A=\bigcup_{k\in N}A_k$,用 A^+ 表示集合 A 的多重集合的集合;

(2) $P=P^1\cup P^2\cup\cdots\cup P^n$ 为位置集合,表示行为人可以采取行为的状态,P_i 表示行为人 i 的可采取行为状态集合;

(3) $T=T^1\cup T^2\cup\cdots\cup T^n$ 为行为集合,其中,T^k 表示局中人 k 的行为集合;

(4) $F\in I\cup O$ 为弧的集合,其中 $I\subseteq P\times T$,$O\subseteq(T\times P)T$,同时 $P\cap T=\varnothing T$ 且 $P\cup T\neq\varnothing$,T 其中 $\varnothing$ 是空集合. 对于 $Tx\in TP\cup TT$,T 用 ${}^{\cdot}x=\{y|(y,x)\in F\}$ 表示 x 的前置集合,同样,$x^{\cdot}=\{y|(x,y)\in F\}$ 表示 x 的后继集合;

(5) $\pi:T\to[0,1]$ 可以表示选择某个特定弧的选择策略,$w:F\to A$ 弧的权重函数,表示变迁发生所需要或生成的标记个数与类别;

(6) $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 表示变迁响应速率的集合;

(7) $R:T\to(\Re_1,\Re_2,\cdots,\Re_N)T$ 是每个变收的集合,$\Re_i\in(-\infty,+\infty)$,$i\in N$,用来表示某个局中人采取行为后的结果;

(8) $U^k(s_i)$ 表示局中人 k 在状态 s_i 时的效用函数,根据这个函数局中人可以选择最有利的行为;

(9) M 为标识集合. 对于标识 $M_i\in M$,用 $M_i(p)$ 表示该标识下位置 p 中的标记个数,常用 M_0 表示一个 SGN 的初始标识.

定义 4. 最优决策. 随机博弈网 $SGN=(N,S,A,F,\pi,\lambda,R,U,M_0)$ 中,局中人 k 根据效用函数所作的最佳选择 $a\in A$ 称作最优决策.

定义 5. 策略. 对于给定的随机博弈网 $SGN=(N,P,T,F,\pi,\lambda,R,U,M_0)$,对于局中人 k,$\pi^k=(\pi(t_1^k),\pi(t_2^k),\cdots,\pi(t_{|T^k|}^k))$ 为其策略,其中 $\pi(t_i^k)$ 为局中人 k 实施行为 t_i 的概率,且满足 $\sum_{t^k\in\{p^{\cdot}\cap T^k\}}\pi(t^k)=1$,$1\leq i\leq|T^k|$. 若 $|N|=n$,称 $\pi=(\pi^1,\pi^2,\cdots,\pi^n)$ 为该随机博弈网的策略,其中 π^k 为局中人 k 的策略.

对于传统的 Petri 网,通过把假设时间变迁发生的时间假设为随机变量,通过对其数字特征赋以不同数值来表现. 由于策略表示为选择特定行为的概率,因此可以用带有概率值的损失变迁来表示,为使随机博弈网表现更为简洁,我们常采用乘法原理,把瞬时变迁吸收到对应行为的时间变迁中.

定义 6. 效用函数. 对于随机博弈网 $SGN=(N,P,T,F,\pi,\lambda,R,U,M_0)$,局中人 k 的效用函数

可以表示为 $U^k(M_0,\pi)=f^k(M_0,\pi)=f^k(M_0;\pi^1,\pi^2,\cdots,\pi^n)$,其中,$\pi^k$ 为局中人 k 的策略,$f^k(\cdot)$ 为 $n+1$ 元函数. 若 M_0 为固定,在不引起混淆的情况下,$U^k(M_0)$可表示为 $U^k(\pi)$.

为方便应用计算机辅助计算均衡值,这里我们常用 SGN 状态和行为路径来计算效用函数. 实际上,我们可以对所有状态都赋予回报向量,用以表示局中人处于该状态可以获得的收益(如局中人获得的访问权限、得到的信息量等),由于局中人要到达特定的状态都至少需要若干步骤,每一步的实施都必将需要局中人付出一定的代价,因此我们可以对每一个变迁赋予一个消耗向量表示该变迁发生所需局中人付出的代价.

定义 7.　片面竞争随机博弈网(Unilaterally Competitive Stochastic Game Net,UCSGN). 对于给定的随机博弈网 $SGN=(N,P,T,F,\pi,\lambda,R,U,M_0)$,如果下列条件满足:对于任意的策略 π',π''和 $i,j\in N$ 且 $j\neq i$,若 $U^i(\pi')\geq U^i(\pi'')$,那么,必有 $U^j(\pi')\leq U^j(\pi'')$,则我们称其为片面竞争博弈网.

定义 8.　攻防随机博弈网(Attack-Defense Stochastic Game Net,ASGN). 对于给定的片面竞争随机博弈网 $SGN=(N,P,T,F,\pi,\lambda,R,U,M_0)$,若满足 $|N|=2$,则称该随机博弈网为攻防随机博弈网.

在建立 SGN 过程中,我们假设每一个理性的局中人都会尽量最大化自身的回报. 对于 SGN 中的每一个位置 p_i,可以描述为一个矩阵 $\boldsymbol{G}_i$. 假设参加博弈的局中人是攻击与防御的双方,且攻击者和防御者的行为集合可以分别表示为 $A_i=\{a_1,a_2,\cdots,a_K\}$ 和 $D_i=\{d_1,d_2,\cdots,d_L\}$. 对于攻击者,如果一个攻击行为在位置 p_i 被选中,并且攻击成功且未被检测到,则系统将会转移到其它的位置 p_j,并且博弈将在位置 p_j 继续进行. 输出结果可以被表示为 $K\times L$ 的矩阵,进一步,γ_{kl} 作为行为对(a_k,d_l)的总输出.

$$\gamma_{kl}=\begin{cases}r_{kl}+\sum_j \delta_j U(p_j), & \text{攻击成功}\\ c_{kl}, & \text{其它}\end{cases} \tag{1}$$

其中,r_{kl} 表示攻击者在位置 p_i 的回报,其中攻击者选择行为 a_k 并且防御者选择 d_l,考虑到其它位置的影响,我们用 $\boldsymbol{U}(p_i)$ 来表示在位置 p_i 的期望效用以及用 $\delta_i\in[0,1]$ 来表示折扣系数. 用同样的方法,我们可以为攻击者在位置 p_i 构建一个 $|A_i|\times|D_i|$ 介的矩阵,具体表示形式如下

$$\boldsymbol{U}(p_i)=\begin{bmatrix} & d_1 & \cdots & d_m\\ a_1 & \gamma_{11} & \cdots & \gamma_{1m}\\ \vdots & \vdots & \gamma_{kl} & \vdots\\ a_n & \gamma_{n1} & \cdots & \gamma_{nm}\end{bmatrix}.$$

我们希望博弈双方都能按照均衡条件下的策略 $\pi_i^1=(\pi_i^1(a_1),\pi_i^1(a_2),\cdots,\pi_i^1(a_K))$ 和 $\pi_i^2=(\pi_i^2(d_1),\pi_i^2(d_2),\cdots,\pi_i^2(d_L))$来选择行为. 在此博弈中的攻击者的效用为 $E(\pi_i^1,\pi_i^2)=\sum_{\forall a_k\in A_i}\sum_{\forall d_l\in D_i}\pi_i^1(a_k)\pi_i^2(d_l)r_{kl}$. 我们用零和博弈来描述攻击者与防御者之间的博弈关系. 攻击者不了解防御者的防御策略,因此将防御者看作与攻击者收益相反的局中人,即防御者的目标就是最小化攻击者的回报. P_i 处攻击者的最优化策略和其对应的防御策略可以通过求解下面的式子获得

$$\max_{\pi_i^1}\min_{\pi_i^2}E(\pi_i^1,\pi_i^2) \tag{2}$$

这些策略可以分别被描述为 π_i^1 和 π_i^2. 此时,博弈双方整体的效用可以被表示为 $\boldsymbol{U}(p_i)$,它是在博弈双方分别采用策略 π_i^1 和 π_i^2 时的期望输出

$$\boldsymbol{U}(p_i)=\max_{\pi_i^1}\min_{\pi_i^2}E(\pi_i^1,\pi_i^2) \tag{3}$$

随机博弈网络模型计算分析的目的之一就是预测描述攻击者策略的概率向量 $\boldsymbol{\pi}^{1*}=\{\pi_i^{1*}\}$ 以及防御者的转移概率矩阵 $\boldsymbol{Q}$.

π_i^{1*} 可以参考文献[31]来计算,我们给出基于 Shapley 算法[32]的均衡策略计算算法.

算法 3.　均衡策略计算算法.

输入:随机博弈模型

输出:均衡策略向量 $\boldsymbol{\pi}^{m^*}=\{\pi_i^{m^*}\}$

1. 初始化 $\boldsymbol{U}=\{\boldsymbol{U}(p_i)\}$;

2. 对每个位置 $p_i\in P^m$,通过公式(1)计算矩阵$\boldsymbol{U}(p_i)=[r_{kl}]$;

3. 对每个位置 $p_i\in P^m$将计算结果赋值到向量值 $N(i)$ 中,$N(i)\leftarrow Value[\boldsymbol{U}(p_i)]$;

4. 对每个 $p_i\in P^m$ 计算 $\pi_i^m\leftarrow Solve[\boldsymbol{U}(p_i)]$,直到所有 $N(i)\leftarrow Value[\boldsymbol{U}(p_i)]$,$\forall p_i\in P$ 为止;

5. 输出 $\boldsymbol{\pi}^{m^*}=\{\pi_i^{m^*}\}$; //用该集合中的均衡概率表示局中人 m^* 的行为策略

这里计算的均策略 $\boldsymbol{\pi}^*=\{\pi_i^*\}$将会给 SGN 模型的中变迁选择概率的设制提供依据.

4.3.2　攻防随机博弈网的模型组合方法

根据攻防随机博弈网的定义和模型方法,我们可以分角色地建立攻防双方的随机博弈网模型,并计算博弈策略等参数,但很多时候我们希望分析在各种博弈策略下,攻防行为对整个网络系统的影响,本节我们将提出角色模型的组合方法,从而实现攻防博弈策略模型对目标网络整体的模型与分析. 首先我们来研究攻防随机博弈网的有关性质.

定理 1.　若一个随机博弈网 SGN 为攻防随机

博弈网，对于 $i\neq j\in N$，P^i 和 P^j 分别表示局中人 i 和 j 的行为位置集合，那么，$P^i\cap P^j\neq\varnothing$.

证明. 用反正法证明. 假设 $P^i\cap P^j=\varnothing$，由于状态 P 决定了可能的行为集合，因此，对于 $\forall p_i\in P^i$，$p_j\in P^j$，我们都有

$$[(\bigcup_{p_i\in P^i}p_i^{\cdot})\cup(\bigcup_{p_i\in P^i}{}^{\cdot}p_i)]\cap[(\bigcup_{p_j\in P^j}p_j^{\cdot})\cup(\bigcup_{p_j\in P^j}{}^{\cdot}p_j)]=\varnothing \tag{4}$$

由于局中人的效用函数取决于其最终所处的状态与其所采用的策略，对于固定的初始状态，其最终状态取决于策略的选择，因此，我们可以得到局中人的效用只与其采用的策略有关. 对于局中人 i，用 π^i 表示其策略，用 $\pi=(\pi^i,\pi^i_-)$ 表示 SGN 的策略，其中 $\boldsymbol{\pi}^i_-=(\pi^1,\pi^2,\cdots,\pi^{i-1},\pi^{i+1},\cdots,\pi^N)$ 表示 SGN 中局中人 i 之外的其它局中人的策略向量，因此，必存在 $\pi'=(\pi^{i\prime},\pi^{i\prime}_-)$，$\pi''=(\pi^{i\prime\prime},\pi^{i\prime\prime}_-)$ 使得 $U^i(\pi')\geq U^i(\pi'')$. 同理，对于局中人 j，必存在 $\pi'''=(\pi^{j\prime\prime\prime},\pi^{j\prime\prime\prime}_-)$，$\pi^{\mathrm{IV}}=(\pi^{j^{\mathrm{IV}}},\pi^{j^{\mathrm{IV}}}_-)$，使得 $U^j(\pi''')\geq U^j(\pi^{\mathrm{IV}})$. 构造新的策略如下：$\pi^{\mathrm{V}}=(\pi^{i\prime},\pi^{j\prime\prime\prime},*)$，$\pi^{\mathrm{VI}}=(\pi^{i\prime\prime},\pi^{j^{\mathrm{IV}}},*)$，则 $U^i(\pi^{\mathrm{V}})\geq U^i(\pi^{\mathrm{VI}})$，$U^j(\pi^{\mathrm{V}})\geq U^j(\pi^{\mathrm{VI}})$，与 SGN 为片面竞争博弈网矛盾，因此，$P^i\cap P^j\neq\varnothing$.

推论 1. 若 SGN 为攻防随机博弈网，那么至少存在一个 $p_i\in P$ 满足下列条件：$p_i^{\cdot}\cap T_1\neq\varnothing$ 且 $p_i^{\cdot}\cap T_2\neq\varnothing$.

证明. 根据定理 1 可直接得到.

定理 2. 对于攻防随机博弈网 $(N,P,T,F,\pi,\lambda,R,U,M_0)$，若 $|P|<\infty$，$|T|<\infty$，那么该 SGN 存在混合策略下的纳什均衡策略.

证明. 根据随机博弈网的定义，我们不难看出，M_0 对应着随机博弈的开始状态，$T_k\times T_k\times\cdots\times T_k$ 为局中人 k 的行为集合，依据状态 P 可以构造效用函数，因此，存在与 SGN 对应的随机博弈，由于效用函数为凹函数，根据文献[33]，知该随机博弈存在混合策略的 Nash 均衡，因此，通过该 Nash 均衡可以得到 SGN 对应混合策略下的纳什均衡.

根据上述定理和推论，可知在不同视角的攻防随机博弈网模型中必有描述相同含义的位置存在，同时在此类模型中存在混合策略下的纳什均衡. 依据上述结论，我们可以分别建立攻击视角与防御视角的随机博弈网模型，并通过下面的定理将模型组合为描述完整攻击——防御过程的攻防博弈策略模型，并计算稳态和瞬态的参数.

算法 4. 生成攻防博弈策略模型.

输入：基于随机 Petri 网的攻击模型，防御行为，攻击防御行为实施后的回报效用描述

输出：攻防博弈策略模型

1. 将通过算法 1、2 生成的随机 Petri 网的攻击模型的变迁上引入攻击行为效用的描述建立攻击视角的随机博弈网模型；

2. 根据可采用的防御行为建立防御视角的随机博弈网模型；

3. 应用算法 3 计算上述随机博弈网模型中的均衡策略 π，并将攻防策略分别引入模型；

4. 通过合并攻击与防御视角的随机博弈网模型，生成支持安全分析的功防博弈策略模型.

5 基于攻防模型的安全分析技术

(1) 攻击成功概率

攻击成功概率是攻击者对某一个目标实施攻击取得成功的概率. 攻击者在位置 k 选择行为 i 的成功概率可以表示为 $p_{\mathrm{attack}}(a_i^k)$. 因此，对博弈策略模型中的每一个位置 k，所有可能攻击行为的期望成功率可以描述为如下的概率向量：

$$\boldsymbol{p}_{\mathrm{attack}}(a^k)=(p_{\mathrm{attack}}(a_1^k),\cdots,p_{\mathrm{attack}}(a_{m_k}^k)),$$

其中，$\sum_{i=1}^{m_k}\boldsymbol{p}_{\mathrm{attack}}(a_i^k)=1$，因此，$\boldsymbol{p}_{\mathrm{attack}}=\{\boldsymbol{p}_{\mathrm{attack}}(a_k)\mid i=1,\cdots,n\}$，将会被用于博弈策略模型中的决策向量的设置. 为了在位置 k 处继续攻击行为，攻击者不仅需要考虑哪个原子攻击行为给他带来的回报更大，同时也要考虑哪个行为成功的可能性更大. 假设变迁的回报和代价统一表示，则攻击者在位置 k 处，为了到达最终目标位置而选取的攻击行为成功的概率可以用式(5)计算.

$$\boldsymbol{p}_{\mathrm{attack}}(a_i^k)=P[M(p_r)\neq 0]=1-P[M(p_r)=0] \tag{5}$$

其中，$M[p_r]$ 表示在位置 p_r 处的标识数，p_r 表示攻击行为结果的位置. 即 $P_{\mathrm{attack}}(a_i^k)$ 表示攻击行为结果的位置中标识数不为空的概率.

(2) 攻击路径

这里我们研究的攻击路径是指在目标网络中的由可能遭到攻击的正常节点到根据需求定义的终端节点的过程. 在本文中我们将攻击者获得目标网络节点的 root 权限作为攻击结束的最终状态，因为此时已经意味着攻击可以成功地实施了. 故这里的攻击路径有一系列具有连接关系的网络设备组成，同时，根据攻击成功概率的计算，我们可以通过式(6)

计算攻击者成功通过该条路经的概率

$$P_{\text{path}}^{i}=\sum_{k=1}^{n}P_{\text{attack}}(a^{k})\times\bar{\omega}_{k} \tag{6}$$

其中,P_{path}^{i}表示攻击者成功通过路经 i 的概率,n 表示该条路径下共经过的节点数,$\bar{\omega}_{k}$表示路径中第 k 个结点的重要程度,且$\sum_{k=1}^{n}\bar{\omega}_{k}=1$. 攻击路径的生成算法如下.

算法 5.　攻击路径生成算法.

输入:攻防博弈策略模型,攻击目标,起始位置

输出:攻击路经{(起始设备,攻击者拥有的权限)…(目标设备,攻击者获 root 权限)}(成功实施的可能性)

1. 生成攻击目标位置集合;

2. 采用下面操作,精化攻防博弈策略模型;

3. 对存在弧$(p_i,t)(t,p_{i+1})$,且设备间存在的漏洞不可以被利用,那么删除弧$(p_i,t)(t,p_{i+1})$,否则,保持不变;遍历所有的变迁,并删除孤立的变迁;

4. 根据攻击信息中给出的变迁表示的攻击行为 a_i 与当前位置的关系判断是否存在攻击关系,若攻击行为可以作用于设备 p_i,且 p_i 的前置集合非空,则对其前置集合中的所有变迁增加标记 a_i,遍历所有设备对所有变迁标记,删除没有标记的变迁及与其相关联的弧,删除孤立的位置,则得到精化的模型;

5. 选取 p 为攻击目标位置,则采用回溯法搜索攻击路径;

6. 首先标识 p 的后置变迁为"已用",p 为"0"并设置集合 D,其初始值为 $D=\{p\}\cup p^{\cdot}$;

7. 对于任意 $b_i\in\{b\mid b\in D\wedge b=0\}$,对 ${}^{\cdot}b_i\cap\{M\backslash D\}$ 中元素标识 b_i;标识 b_i"1";

8. 重复步 7 中的操作直到没有符合条件的 b_i;

9. 对于任意 $c_i\in\{c\mid c\in D\wedge c=1\}$标识 ${}^{\cdot}c_i\cap\{M\backslash D\}$ 中元素"已用";标识 c_i"已用",$D={}^{\cdot}b_i\cup{}^{\cdot}b_i\cup D$;

10. 重复步 9 中操作直到没有符合条件的 c_i;

11. 重复步 6～10 中的操作,直到 ${}^{\cdot}D\in D$;

12. 以 $d_j\in\{d\mid d\in D\wedge{}^{\cdot}d=\varnothing\}$为起点,根据变迁的标识展开即可得到以 P 为攻击目标位置的所有可能攻击路径;

13. 对所有可能的攻击目标位置执行步 1～5 中操作,可以得到目标网络存在的可能攻击路径.

(3) 攻击时间

攻击者对某一个目标平均实施 1 次成功攻击行为所需要耗费的时间. 我们可以利用式(7)计算 SGN 模型中变迁的吞吐量.

$$TH_{\text{atttack}}=\sum_{M\in H}P[M]\lambda_{\text{attack}} \tag{7}$$

其中,H 攻击变迁的标记集合,λ_{attack}是攻击变迁的实施速率,故攻击响应时间可以通过式(8)计算.

$$T_{\text{attack}}=\frac{1}{TH_{\text{attack}}} \tag{8}$$

攻击者选择行为 $a_{m_k}^{k}$,如果攻击失败则不会对系统状态发生任何改变. 因此,在 SGN 模型参数设置时,要将攻击行为的选择概率与攻击行为的成功概率设置在相应的变迁处,以确保最终的 SGN 模型可以准确地反映攻击者的行为意图. 一次成功的攻击可能会通过多次攻击行为,并经历多个网络设备,最终到达攻击的目标. 故在计算攻击时间时,要考虑不同的攻击目标所带来的不同攻击过程,下节将具体介绍有关攻击路径的分析方法,若针对某一目标的有 n 条攻击路经,且平均每条路经上需要实施 m 次攻击行为,则我们可以计算达到统一目标的平均攻击时间为

$$T=\frac{\sum_{i=1}^{n}\sum_{k=1}^{m}T_{\text{attack}}^{k}}{n} \tag{9}$$

其中,k 表示每条路经上不同攻击行为,i 表示不同的攻击路经.

(4) 脆弱节点

在攻击路径上,我们可以得到一系列有关目标系统各设备受攻击的可能性,一方面取决于该设备本身的重要程度,另一方面取决于与该设备有连接关系的其它设备的重要程度. 我们可以通过计算每一个设备的受攻击的权重来排序网络节点的脆弱程度,具体计算方法如下.

算法 6.　节点的脆弱程度排序.

输入:攻防博弈策略模型,攻击路径

输出:可能发生攻击的网络节点及其脆弱性权重

1. 计算攻防博弈策略模型中稳定状态时各位置中平均标识的数量 m_i;

2. 建立可能攻击路径中出现的节点集合{IPi};

3. 标记出在不攻击路径下的同一节点{IPi(1,…,n_j)}; //其中在同一节点获得不同权限应累计计数

4. 计算脆弱性权重 $\sigma_i=\sum_{j=1}^{n_j}m_i^j$;

5. 按脆弱性权重对网络节点进行排序.

通过上述算法的计算我们认为计算所得的权重值最大的一个或几个节点为目标网络中的脆弱节点.

6　应用实例与分析

下面我们以典型企业网络作为实验目标,应用

前面提出的模型与分析方法,实现多种攻防行为在实验环境下进行推演.目标网络的拓扑结构(如图 2 所示)可分为外部网络和内部网络两个部分,攻击者可以通过外网对内网中各目标节点实施攻击,这里的内网由 Web 服务器、数据中心和若干的终端节点组成.它们通过路由器、交换机等网络设备互相连接,同时企业网络中也会连接防火墙,入侵检测设备等安全设备.

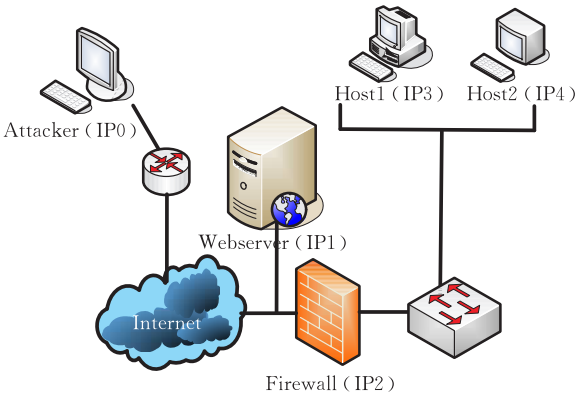

图 2 实验目标网络拓扑结构

根据第 2 节中对设备模型和拓扑结构模型的描述方法,实验网络环境的信息描述如表 1～3 所示.

表 1 设备脆弱性信息

设备	软件	服务	脆弱性
IP0	Unknown	Unknown	Unknown
IP1	Linux	ftp, database	ServU5.0, Dvbbs7.0 sp2
IP2	Linux	telnet	Linux7.0telnet
IP3	Linux	ftp, ssh	sshd buffer overflow, ftp.rhost overwrite
IP4	Windows	ftp, xterm	ftp.rhost overwrite, local buffer overflow

表 2 设备连接信息

设备 1	设备 2	服务	权限
IP0	IP0	any	0
IP0	IP1	ftp	1
IP0	IP1	database	1
IP0	IP2	telnet	1
IP1	IP1	any	0
IP1	IP2	any	2
IP2	IP1	ftp	1
IP2	IP1	database	1
IP2	IP3	ftp	2
IP2	IP3	ssh	2
IP2	IP4	ftp	2
IP2	IP4	xterm	2
IP3	IP3	any	0
IP3	IP4	ftp	2
IP4	IP4	any	0
IP4	IP3	ftp	2
IP4	IP3	ssh	2

表 3 攻击信息

脆弱性	攻击行为	发起设备	需要权限	获得权限
ServU5.0,	Overflow 攻击	IP0	1	3
Dvbbs7.0 sp2	Injection 攻击	IP0	1	2
Linux7.0 telnet	Overflow 攻击	IP0,IP1	1	3
sshd buffer overflow	Overflow 攻击	IP2,IP3,IP4	2	3
ftp.rhost overwrite	Exploit 攻击	IP2,IP3,IP4	2	2
local buffer overflow	Overflow 攻击	IP2,IP3,IP4	1	3

依据上述信息,由算法 1 和算法 2 我们可以得到随机 Petri 网攻击模型,并根据 4 对模型参数进行扩展,从而得到如图 3 所示的攻击视角随机博弈网模型,其中 P_o 为起始位置,P_{13},P_{33},P_{43} 分别表示 IP1,IP3 和 IP4 的 root 权限被攻击者获得的结束位置,因为当攻击者获得 root 权限后,他可以进行包括窃取文件、网络监听、DoS 攻击等各种深度攻击.其它位置描述如表 4 所示.图中的每个变迁表示一个攻击行为,为了简化模型,我们将瞬时变迁与对应的时间变迁压缩为一个时间变迁来表示.将变迁所描述攻击行为能力 λ 及其成功率 q 赋值,根据算法 4,在随机 Petri 网攻击模型中引入回报效用的描述,并利用算法 3 计算获得攻击者在均衡条件下的攻击策略 π.具体数据见如表 5.

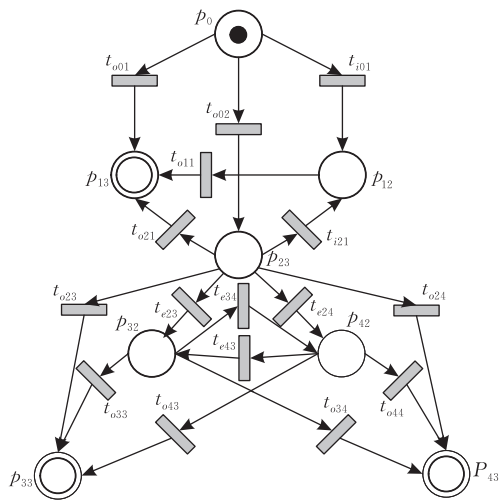

图 3 攻击视角随机博弈网模型

表 4 攻击视角随机博弈网模型中位置的含义

位置	描述
P_0	攻击者处于 IP0,网络处于正常状态
P_{12}	攻击者攻入 IP1,获得 guest 权限
P_{13}	攻击者攻入 IP1,获得 root 权限
P_{23}	攻击者攻入 IP2,获得 root 权限
P_{32}	攻击者攻入 IP3,获得 guest 权限
P_{42}	攻击者攻入 IP4,获得 guest 权限
P_{33}	攻击者攻入 IP3,获得 root 权限
P_{43}	攻击者攻入 IP4,获得 root 权限

表 5　攻击视角随机博弈网模型中变迁的含义

变迁	行为描述	行为方向	λ	q	r	π
t_{o01}	Overflow 攻击	IP0→IP1	1	0.6	3	0.1827
t_{o02}	Overflow 攻击	IP0→IP2	1	0.6	3	0.1827
t_{i01}	Injection 攻击	IP0→IP1	2	0.3	2	0.6346
t_{o11}	Overflow 攻击	IP1→IP1	1	0.9	3	0.9139
t_{o21}	Overflow 攻击	IP2→IP1	1	0.6	3	0.0001
t_{i21}	Injection 攻击	IP2→IP1	2	0.6	2	0.2937
t_{o23}	Overflow 攻击	IP2→IP3	1	0.7	3	0.1322
t_{o24}	Overflow 攻击	IP2→IP4	1	0.7	3	0.1322
t_{e23}	Exploit 攻击	IP2→IP3	1.5	0.5	2	0.2209
t_{e24}	Exploit 攻击	IP2→IP4	1.5	0.5	2	0.2209
t_{e34}	Exploit 攻击	IP3→IP4	1.5	0.5	2	0.4917
t_{e43}	Exploit 攻击	IP4→IP3	1.5	0.5	2	0.4917
t_{o33}	Overflow 攻击	IP3→IP3	1	0.9	3	0.5082
t_{o44}	Overflow 攻击	IP4→IP4	1	0.9	3	0.5082
t_{o34}	Overflow 攻击	IP3→IP4	1	0.7	3	0.0001
t_{o43}	Overflow 攻击	IP4→IP3	1	0.7	3	0.0001

针对上述脆弱性和攻击手段的防护视角的随机博弈网模型如图 4 所示. 其中位置和变迁具体描述如下:P_v表示可能遭到深入攻击的脆弱位置;P_0 表示网络处于正常状态. t_{d1}表示行为验证;t_d表示行为过滤;t_{d3}表示异常字段识别;t_{d4}表示注入工具检测;t_{d5}表示阻断连接.

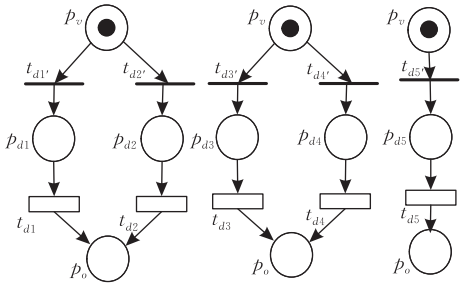

图 4　防御视角随机博弈网模型

由算法 4,将上述分角色的随机博弈网模型组合,可得攻防博弈策略模型,如图 5 所示. 其中组合后在攻击视角模型基础上新增加的表示防御行为用白色的变迁表示,其含义和相关参数如表 6 所示.

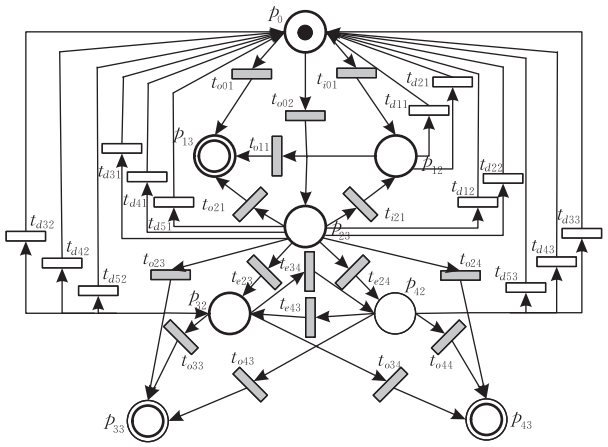

图 5　攻防博弈策略模型

表 6　防御视角随机博弈网模型中变迁的含义

变迁	行为描述	λ	q	r	π
t_{d11}	行为验证	1.0	0.4	2	0.0001
t_{d21}	行为过滤	1.5	0.6	3	0.9999
t_{d12}	行为验证	1.0	0.4	2	0.0001
t_{d22}	行为过滤	1.5	0.6	3	0.4024
t_{d31}	异常字段识别	1.0	0.5	1	0.0001
t_{d41}	注入工具检测	0.8	0.7	1	0.3671
t_{d51}	阻断连接	3.0	0.5	2	0.2303
t_{d32}	异常字段识别	1.0	0.5	1	0.0001
t_{d42}	注入工具检测	0.8	0.7	1	0.6931
t_{d52}	阻断连接	3.0	0.5	2	0.3068
t_{d33}	异常字段识别	1.0	0.5	1	0.0001
t_{d43}	注入工具检测	0.8	0.7	1	0.6931
t_{d53}	阻断连接	3.0	0.5	2	0.3068

下面我们计算随系统时间变化,图 5 所示的攻防博弈策略模型中,有关参数的变化情况.

图 6 和图 7 比较了攻击成功概率随系统时间的发展,而发生变化的情况,其中图 6 显示出当攻击速率为 1 时,以 IP1 为攻击目标的攻击者获得成功的可能性更大,而以 IP3,IP4 为目标的攻击者则可能具有较小的攻击成功率,并且由于 IP3 与 IP4 的对称关系,它们的数据基本相同. 图 7 中显示了在不同攻击发生速率的时候,目标系统遭到攻击的平均概率的变化情况. 可以看出,当攻击速率达到一定的数值后,变化趋势基本相同,且较快收敛到一个常数

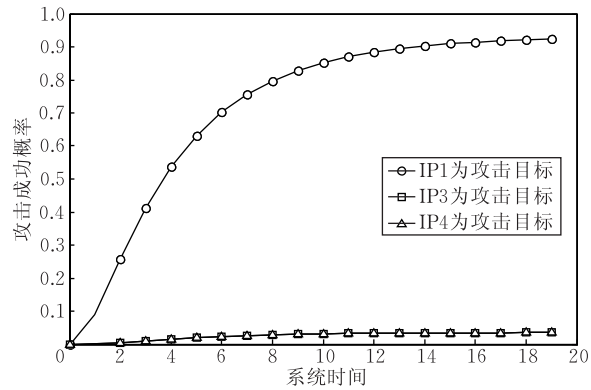

图 6　攻击成功率随系统时间变化情况

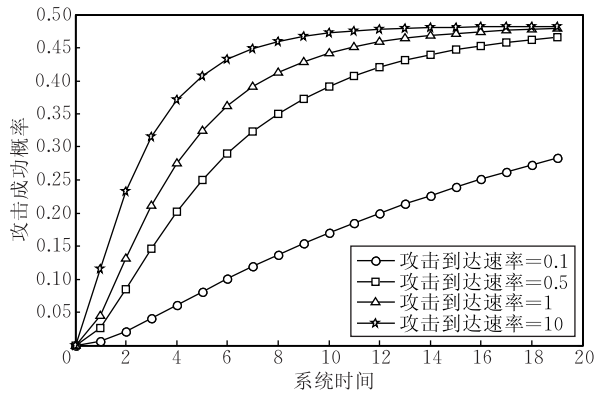

图 7　不同攻击到达情况下攻击成功率随系统时间变化情况

上,这表明在攻防能力确定的情况下,攻击成功的概率与攻击频繁程度无关.

将目标网络中的 IP1、IP3 和 IP4 3 个节点作为攻击的目标节点,根据算法 5 我们可以方便地找到目标网络中的各条攻击路径以及每条路径发成攻击的可能性.

攻击目标为 IP1:

{(IP0,1)(IP1,3)}(0.9614),

{(IP0,1)(IP2,2)(IP1,3)}(0.6412),

{(IP0,1)(IP1,2)(IP1,3)}(0.6411),

{(IP0,1)(IP2,3)(IP1,2) (IP1,3)}(0.4811);

攻击目标为 IP3:

{(IP0,1)(IP2,3)(IP3,2)(IP3,3)}(0.2589),

{(IP0,1)(IP2,3)(IP3,3)}(0.3451),

{(IP0,1)(IP2,3)(IP4,2)(IP3,3)}(0.2589),

{(IP0,1)(IP2,3)(IP4,2)(IP3,2)(IP3,3)}
(0.2071)

攻击目标为 IP4:

{(IP0,1)(IP2,3)(IP4,2)(IP4,3)}(0.2589),

{(IP0,1)(IP2,3)(IP4,3)}(0.3451),

{(IP0,1)(IP2,3)(IP3,2)(IP4,3)}(0.2589),

{(IP0,1)(IP2,3)(IP3,2)(IP4,2)(IP4,3)}
(0.2071)

通过攻击路径的分析,我们可以计算出针对不同攻击目标,攻击平均时间随系统时间的变化而变化的情况,如图 8 所示. 其中,从发展趋势上可以看出,在攻击初期,不同的攻击目标自身的特点对攻击时间的影响不大,而当时间发展到一定程度的时候,个体的差异性逐渐显现出来,此时,IP1 为攻击目标时,其被攻击的平均时间最短,而 IP4 则相对最难攻破.

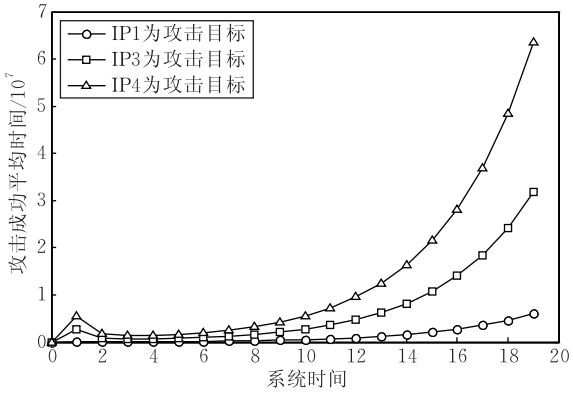

图 8 攻击平均时间随系统时间变化情况

在攻击路径分析的基础上应用算法 6 可以获得目标网络中可能受到攻击的各网络节点的脆弱性权重,如表 7 所示.

表 7 脆弱节点数据计算结果

目标网络节点	脆弱性权重计算结果
IP1	0.9237
IP2	0.0006
IP3	0.0349
IP4	0.0349

通过比较,容易看出 IP1 的脆弱性权重最高,它是目标网络中最易被攻击的节点,应该重点防范和加固.

7 结 论

本文针对网络系统安全评测的具体需求,提出了基于模型的网络攻防实验环境的整体架构,并提出了支持网络攻防推演的建模和分析方法,从网络设备模型、拓扑机构模型,到基于随机 Petri 网的网络攻防行为模型和基于随机博弈网的攻防博弈策略模型. 此过程中层层深入,提出了一系列模型和分析算法,应用这些方法,可以快速地生成描述目标网络的攻防模型,并可以对攻击成功率、可能的攻击路径、攻击成功平均时间以及脆弱性节点等方面进行分析和评价. 为基于模型的网络攻防实验及时有效地进行攻防推演以及对实验结果进行分析提供有效的方法. 最后应用研究成果,成功地对一个的网络攻防实例建模用于安全分析,实现了对目标网络快速建模、量化计算以及对攻防过程的推演和分析.

参 考 文 献

[1] Sanders W H, Cukier M, Webber F, Pal P, Watro R. Probabilistic validation of intrusion tolerance//Proceedings of the International Conference on Dependable Systems & Networks (DSN-2002). Bethesda, 2002: 78-79

[2] Littlewood B, Brocklehurst S, Fenton N, Mellor P, Page S, Wright D. Towards operational measures of computer security. Computer Security, 1993, 2: 211-229

[3] Nicol D M, Sanders W H, Trivedi K S. Model-based evaluation: From dependability to security. IEEE Transactions on Dependability and Security, 2004, 1(1): 48-65

[4] Avizienis A, Laprie J C, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11-33

[5] Jiang Wei, Fang Bin-Xing, Tian Zhi-Hong Zhang Hong-Li. Evaluating network security and optimal active defense based on attack defense game model. Chinese Journal of Computers, 2009, 32(4): 817-827(in Chinese)

(姜伟,方滨兴,田志宏,张宏莉. 基于攻防博弈模型的网络安全测评和最优主动防御. 计算机学报,2009,32(4):817-827)

[6] Hamilton S N, Miller W L, Ot t A, Saydjari O S. The role of game theory in information warfare//Proceedings of the 4th Information Survivability Workshop. Vancouver, Canada, 2002: 45-46

[7] Liu Y, Trivedi K S. A general framework for network survivability quantification//Proceedings of the 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems (MMB) Together with 3rd Polish-German Teletraffic Symposium (PGTS). Dresden, 2004: 369-378

[8] Daley K, Larson R, Dawkins J. A structural framework for modeling multi-stage network attacks//Proceedings of the ICPP Workshops. Regina, 2002: 5-10

[9] Sheyner O, Haines J, Jha S, Lippmann R, Wing J. Automated generation and analysis of attack graphs//Proceedings of the 2002 IEEE Symposium on Security and Privacy. Berkeley, CA, 2002: 273-284

[10] Jha S, Sheyner O, Wing J M. Two formal analyses of attack graphs//Proceedings of the Computer Security Foundations Workshop (CSFW). Cape Breton, Nova Scotia, 2002: 49-63

[11] Ramakrishnan C R, Sekar R. Model-based analysis of configuration vulnerabilities. Journal of Computer Security (JCS), 2002, 10(1/2): 189-209

[12] Besson F, Jensen J, Métayer D L, Thorn T. Model checking security properties of control flow graphs. Computer Security, 2001, 9(3): 217-250

[13] Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California, 2001: 156-165

[14] Wang D, Madan B, Trivedi K S. Security analysis of SITAR intrusion-tolerant system//Proceedings of the ACM Workshop Survivable and Self-Regenerative Systems. Fairfax, VA, 2003: 23-32

[15] Madan B, Goševa-Popstojanova K, Vaidyanathan K, Trivedi K S. A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation, 2004, 56: 167-186

[16] McDermott J. Attack-potential-based survivability modeling for high-consequence systems//Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05). Washington D. C., 2005: 119-130

[17] Lin Chuang, Wang Yuan-Zhuo, Yang Yang, Qu Yang. Research on network dependability analysis methods based on stochastic Petri net. Chinese Journal of Electronics, 2006, 34(2): 130-139(in Chinese)
(林闯,王元卓,杨扬,曲扬. 基于随机 Petri 网的网络可信赖性分析方法研究. 电子学报,2006,34(2):130-139)

[18] Lin Chuang, Wang Yang, Li Quan-Lin. Stochastic modeling and evaluation for network security. Chinese Journal of Computers, 2005, 28(12): 1943-1956(in Chinese)
(林闯,汪洋,李泉林. 网络安全的随机模型方法与评价技术. 计算机学报,2005,28(12):1943-1956)

[19] Jonsson E, Olovsson T. A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering, 1997, 23(4): 235-245

[20] Avizenis A, Laprie J, Randell B. Fundamental concepts of dependability//Proceedings of the 3rd IEEE Information Survivability Workshop. Boston, Massachusetts, USA, 2000: 7-12

[21] Goseva-Postojanova K, Wang F, Wang R, Gong F, Vaidyanathan K, Trivedi K S, Muthusamy B. Characterizing intrusion tolerant systems using a state transition model//Proceedings of the DARPA DISCEX II Conference. Anaheim, California, 2001, II(2): 211-221

[22] Lye K, Wing J M. Game strategies in network security//Proceedings of the 15th IEEE Computer Security Foundations Workshop. Copenhagen, 2002, 4(1-2): 71-86

[23] Mahimkar A, Shmatikov V. Game-based analysis of denial-of-service prevention protocols//Proceedings of the 18th IEEE Computer Security Foundations Workshop (CSFW-18). Aix-en-Provence, 2005: 287-301

[24] Liu Peng, Zang Wanyu, Yu Meng. Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security, 2005, 8(1): 1-41

[25] Wang X, Reiter M. Defending against denial-of-service attacks with puzzle auctions//Proceedings of the IEEE Security and Privacy'03. Oakland, California, 2003: 78-92

[26] Bencsth B, Buttyn L, Vajda I. A game based analysis of the client puzzle approach to defend against DoS attacks//Proceedings of the IEEE Conference on Software, Telecommunications and Computer Networks (SoftCom 2003). Ancona, Venice, 2003: 763-767

[27] Xu J, Lee W. Sustaining availability of web services under distributed denial of service attacks. IEEE Transactions on Computer, 2003, 52(4): 195-208

[28] Browne R. C4I defensive infrastructure for survivability against multi-mode attacks//Proceedings of the 21st Century Military Communication-Architectures and Technologies for Information Superiority. Los Angeles, CA, 2000, 1: 417-424

[29] Wang Yuanzhuo, Lin Chuang, Meng Kun. Security analysis for online banking system using hierarchical stochastic game nets model//Proceedings of the IEEE Global Communications Conference. Honolulu, Hawaii, 2009: 1181-1186

[30] Wang Yuanzhuo, Lin Chuang, Wang Yang, Meng Kun. Security analysis of enterprise network based on stochastic game nets model//Proceedings of the 2009 IEEE International Conference on Communications. Dresden, Germany, 2009

[31] Sallhammar Karin, Helvik Bjarne E, Knapskog Svein J. On stochastic modeling for integrated security and dependability evaluation. The Journal of Networks (JNW), 2006, 1(5): 31-42

[32] Shapley L S. Stochastic games. Proceedings of the National Academy of Science USA, 1953, 39: 1095-1100

[33] Kats A, Thisse J F. Unilaterally competitive games. International Journal of Game Theory, 1992, 21: 291-299

WANG Yuan-Zhuo, born in 1978, Ph. D., assistant professor. His current research interests include network security analysis, performance evaluation, and stochastic game nets.

LIN Chuang, born in 1948, Ph. D., professor, Ph. D. supervisor. His current research interests include computer networks, performance evaluation, logic reasoning, and Petri net theory together with its applications.

CHENG Xue-Qi, born in 1971, Ph. D., professor, Ph. D. supervisor. His main research interests include information security, network information retrieval, and P2P computing.

FANG Bin-Xing, born in 1960, professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include computer architecture, computer network and information security.

Background

This work is supported in part by the National Natural Science Foundation of China (Nos. 60933005, 60803123, 60932003, 60873245).

Network security is a rather important direction with many significant scientific and practical issues in the world, which is due to that network at tacks, are increasingly prevalent. Since it is hardly to build a completely secure system, how to quantify network security become more and more important. Network ranges can be provided for network attack and defense experiments to simulate real network in a virtual environment, and deduct the process of network threats. Most attempts to validate security mechanisms and strategies have been qualitative analysis by showing in the network experiment ranges. Inspired by the study of qualitative analysis, stochastic game models should lead to sound and promising methods in security evaluation. The authors' main objectives are to provide methodology and techniques for quantifying network attack and defense.

In this paper, the authors introduce status and evolvement in the study of based-model analysis techniques of network attack and defense. And they present an overall framework of the network experiment range based on security attack and defense model. In the model, the stochastic models and game model are used, and a series of security attack and defense model algorithm and the security analysis techniques are proposed. Finally, the application of network attack and defense modeling approach on a typical enterprise network attack and defense process of analysis and inference. The results show that the model and analysis approach above proposed is feasible and effective.