基于随机博弈模型的网络安全分析与评价

林闯 王元卓 汪洋 著

清华大学出版社

基于随机博弈模型的网络安全分析与评价

林 闯 王元卓 汪 洋 著

清华大学出版社
北 京

内 容 简 介

本书全面论述了随机博弈模型的相关知识，以及如何应用其对具体网络安全问题进行分析与评价。第1章至第4章介绍了基础模型理论和相关知识，包括概率论、随机模型、排队模型、随机 Petri 网模型以及博弈与随机博弈的相关知识；第5、6章阐述了网络安全模型分析框架及网络攻击模型与评价技术，给出了基于模型的网络安全分析的一般框架；第7章讨论了基于随机模型的 DoS 攻击及邮件攻击问题的模型及安全分析；第8章介绍了基于博弈模型的无线网络路由机制、信任评估以及节点合作信任激励方面的模型和应用分析；第9章给出了随机博弈网模型的具体应用，包括企业网机密性与完整性分析、企业网防御机制的分析、电子商务的安全分析、网上银行的安全分析等。

本书可用作计算机、通信、信息等专业的教材或教学参考书，也可供这些专业的研究人员和工程技术人员阅读。

图书在版编目(CIP)数据

基于随机博弈模型的网络安全分析与评价/林闯，王元卓，汪洋著. --北京：清华大学出版社，2011.12
ISBN 978-7-302-26875-8

Ⅰ. ①基… Ⅱ. ①林… ②王… ③汪… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 191844 号

责任编辑：薛　慧
责任校对：赵丽敏
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：18.25　**字　数**：433 千字
版　　次：2011 年 12 月第 1 版　　**印　　次**：2011 年 12 月第1次印刷
印　　数：1～3000
定　　价：39.00 元

产品编号：041634-01

前言

PREFACE

一、背景

随着网络时代的来临，互联网络的规模和应用领域不断发展，已经渗透到经济、军事、科技、教育以及人们的日常生活等各个领域，其基础性、全局性的地位和作用日益增强。作为重要基础技术与设施的网络安全问题已经成为影响社会经济发展和国家发展战略的重要因素，是当前世界各国共同关注的焦点。然而，面对网络日趋复杂的结构和庞大的规模，特别是随着网络攻击和破坏行为的日益普遍和攻击工具的逐渐多样化，传统的网络安全防护已经不能满足网络发展的实际需求，迫切需要新的基础理论和研究方法。

网络安全研究的一个重要理论基础是安全分析与评价，特别是定量刻画网络系统的安全性，评价各种防护机制保证的安全程度，并从理论上指导构建网络安全机制。例如，入侵检测机制的参数获取、网络流量的设定等都需要基础理论与分析方法。目前，大部分的网络安全性评价工作都是针对网络安全属性进行定性分析，验证系统是否满足某些安全特征，这种情况下得到的安全性指标往往有一定的偏差，对具体网络系统的安全性判断不够准确，很难指导构建新的网络安全措施。因此，网络安全的量化分析与评价是一个重要的研究方向。目前，网络安全性的定量评价主要基于两种思路：一是通过建立形式化的数学模型分析网络安全性，二是使用实验模拟来分析网络系统和攻击行为，验证网络的安全性。尽管现有的这两种方法在确认网络攻击方面有一定的价值，但仍存在很大的局限性，较难应用在大规模的系统中，特别是在面临网络系统的日益复杂的结构时，它们会很难适用。1993 年，Littlewood 开始将系统可信赖性的分析方法引用到网络安全性评价中来，随后的研究也得到了很好的效果。到目前为止，网络可信赖性的研究已经形成了系统的理论和方法。值得注意的是，安全性评价与可信赖性评价具有相似性：可信赖性分析中认为系统失效是由部件故障引起的，而安全性评价中网络的安全事故是由于存在攻击和破坏行为影响了系统的正常服务。可信赖性评价主要采用基于随机模型的分析方法。实际上，随机模型的分析方法已经广泛应用于各种系统的性能评价中，包括网络安全性评价。这是由于随机假设在描述系统某些因素，特别是在描述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，建立网络攻击模型还必须考虑利益驱动因素，并分析安全问题中的博弈过程。在这些工作中，攻击者与防御者之间的行为被描述成一种博弈关系。人们可以通过一个随机博弈模

型来找到纳什均衡(Nash equilibrium)。一个随机博弈可以使人们找到更多潜在的纳什均衡。根据纳什均衡的计算结果,能够知道攻击者的策略及其能够获得最大收益的方案。使用随机博弈模型,我们还能够获得状态转移的概率特性,这具有很强的现实意义。上述研究工作通常需要建立在一定假设的基础之上,对系统和人的行为所进行的这些随机假定在一定程度上是合理的。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,它形成的根本原因是利益的驱动。这与经典可信赖性分析中系统失效的原因存在较大差别。因此,随机模型和博弈模型的分析方法在网络安全性分析与评价中的应用还存在新的挑战和问题。随机博弈模型分析方法为网络安全性评价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。

作者在基于随机模型和博弈模型的网络安全分析与评价领域进行了一系列深入而系统的研究工作,本书主要以排队论、随机 Petri 网、博弈论以及随机博弈网为模型基础,深入地探讨网络安全威胁的模型方法,并结合具体应用对网络中的典型安全问题进行建模、分析与量化评价。书中绝大部分内容取材于我们近期在国际、国内一流学术期刊和会议上发表的论文,全面、系统地展示了很多新的研究成果和进展。

二、内容安排

本书共 9 章,从结构上可分为 3 个部分:

第 1 部分是对基础理论的介绍,包括第 1 章~第 4 章。

第 1 章给出了本书所介绍的网络安全模型中所需要的概率论和随机过程的一些基本概念和知识。

第 2 章介绍了排队模型和随机 Petri 网模型,其中排队论作为运筹学研究的一种有效手段,在计算机网络和计算机系统建模与性能评价中占有相当重要的地位。应用排队模型对计算机网络和计算机系统进行性能预测、分析和评价,已成为研究人员的一个重要手段。近年来,随着网络安全问题的日益严峻,排队模型也在网络安全建模中发挥了十分重要的作用。随机 Petri 网为系统模型的量化评价提供了一个新的数学描述工具,尤其是对并行系统的资源共享的描述和对非乘积解的排队论的分析,给 Petri 网的应用领域的拓宽和发展带来了勃勃生机。本书第一作者从事各种随机 Petri 网模型的研究已有 20 余年,在国际上首先提出了随机高级 Petri 网(stochastic high-level Petri net, SHLPN)及其分析技术,并在系统性能评价中有了应用。本章内容将使读者能够基本掌握排队论以及随机 Petri 网的理论、模型方法、分析技术和应用思路,为读者的学习、工作和研究课题提供一条有效途径。

第 3 章介绍了博弈模型与随机博弈模型。博弈理论已逐渐引入到计算机网络安全研究领域,攻击者和系统防御者之间的行为通常可以描述为二人随机博弈,可以通过计算得到纳什均衡策略。本章介绍后面章节中应用到的博弈论的基本概念和性质,主要包括非合作博弈与合作博弈的基本知识、纳什均衡的存在性和混合策略的纳什均衡求解、拍卖理论、随机博弈等。

第 4 章介绍了随机博弈网理论及模型方法,该理论是本书作者近年来在国际上首先提出来的新的模型方法,它有效地解决了传统博弈论在分析网络安全问题时所遇到的主要问题,包括:(1)在复杂的网络结构下,传统博弈论描述事件互相作用关系的模型能力不足,较

难建立全面和精确的模型；(2)复杂的机制描述和状态转移图使人们难以理解其真实的含义，且难以描述局中人的行为能力。同时，当某些环境或条件发生改变时，模型很难做出相应变化；(3)对一般的博弈模型，其完全的状态空间往往非常庞大，这样的随机模型非常难以求解。而通常在安全分析中，我们只关注其中受到攻击的那个部分，而不是全部模型。另一方面，它扩展了随机 Petri 网理论，在继承随机 Petri 网理论基础和研究成果的同时，增强了 Petri 网的模型能力和适用范围，使之更适应建模分析网络安全问题。随机博弈网模型理论的提出为网络及信息安全分析与评估提供了科学的理论基础，同时也为其他博弈问题的模型与分析提供了有效的解决途径。

第 2 部分是网络安全模型与评价方法，包括第 5 章和第 6 章。

第 5 章分析了网络安全的主要威胁以及攻击与防御行为，并就其中存在的博弈问题进行了分析，对后面的网络安全模型的具体应用提供了方向。

第 6 章通过对当前最新研究成果的综述，论述了应用随机模型是研究网络安全性的一种可行而有效的方法，并且已经取得了一定的成果。当然，建立评价网络系统安全性随机模型，并进行求解分析并非易事，仍面临着一些主要的挑战，如：(1)攻击者模型的建立。攻击和破坏行为是人为的，人为因素的随机分析是一个关键的问题，讨论攻击者的学习能力和决策模型将很有意义。人们已经开始使用决策和博弈论分析攻击者与系统行为。(2)未知攻击分析。未知攻击的不断涌现是网络安全受到的最严峻的挑战之一。如何评价大量未知攻击的破坏，这将是随机模型和分析方法中一个重要的研究课题。对于人们已经了解的网络攻击，可以较容易地从行为过程的角度进行描述，易于判断网络系统的状态。然而对于未知攻击，我们掌握的先验知识则很少，只能从系统受到的影响来分析。因此，基于系统受到的影响建立模型有可能涵盖一些未知的攻击行为。(3)随机模型求解。由于网络系统的复杂性和攻击行为的不确定性，随机模型通常复杂度较高，难以求解。如何求解大规模的随机模型和建立可求解的随机模型，将是未来的两个研究方向。

第 3 部分介绍了随机博弈模型在网络安全分析评价中的具体应用，包括第 7 章～第 9 章。

第 7 章介绍了基于排队模型的网络安全分析，主要关注如何应用排队模型方法对网络攻击进行建模和安全分析。以 DoS 攻击和邮件攻击两类典型的攻击为例，采用排队模型，在系统建模、复杂模型求解、安全指标分析等方面进行介绍。这部分工作是基于随机模型的网络攻击建模的初步工作，对几类典型攻击建模的创新和攻击模型的进一步发展提供了基础，为网络安全分析研究开辟了新的发展空间。

第 8 章介绍了基于博弈模型的网络安全分析。首先，将现有的针对无线网络中自私节点问题的各种机制进行了归纳分类，介绍和比较了几种典型机制的算法和性能。在此基础上，介绍了基于网络编码的机制优化策略，用于改进非合作无线网络的性能。同时，较为详细地分析了无线网络中的经典共谋问题，这也是非合作无线网络中的关键问题。通过以上归纳、分析和比较，对该领域进一步研究的方向和可以采用的分析工具提出了一些建议。然后，提出了一种基于博弈论的信任评估模型以及信任关系建立机制。该机制通过节点间动态属性的多维博弈，并结合对节点行为的直接观察，给出相对客观的信任评估结果。最后，从效用的角度对信任进行了定义，提出了一种面向邻居节点资源拍卖的信任评估模型，实现了信任的价值化；设计了一个基于二阶段拍卖的信任激励机制，证明了在这种机制中存在

一个优势策略，使得参与拍卖的节点有动机通过提高信任度来获得更大收益。

第9章将第4章介绍的随机博弈网模型分析方法具体应用于网络案例，应用竞争博弈网研究成果针对网络攻防问题展开讨论，包括：企业网机密性与完整性分析、企业网防御机制的分析、电子商务的安全分析以及网上银行的安全分析。这些分析既检验了模型理论研究成果的可用性，获得了很多对网络管理人员有用的分析结果，又可以指导网络系统以及防御机制的设计与配置，同时，这些应用案例也给出了随机博弈网进一步发展的方向。

作者的研究工作得到了国家自然科学基金项目（No. 60932003，60803123，61001075）和国家重点基础研究发展计划（“973”计划）项目（No. 2010CB328105，2009CB320504）的连续资助。

清华大学的姜欣博士参与了本书8.2节、8.3节内容的撰写工作，同时，北京科技大学的研究生喻民等同学参与了本书的排版、图表绘制、整理等工作，在此一并表示感谢。

由于作者水平所限，加之基于模型的计算机网络安全分析与评价的研究仍处于不断发展和变化之中，书中错误和不足之处在所难免，恳请专家、读者予以指正。

作　者

2011年6月于北京

目录

CONTENTS

第1部分 基础理论

第 2 部分　网络安全模型与评价方法

第1部分　基础理论

第1章

概率论与随机过程

在正式讨论基于随机博弈模型的网络安全分析与评价之前，我们首先给出最必要的概率论理论和随机过程的一些基本概念和知识，这些数学基础材料对于后续章节的分析讨论是很重要的，可供读者阅读和学习时参考。

1.1 概率论

1.1.1 概率的定义

概率关系着对事件的数量分配。一个事件 A 的概率 $P(A)$ 是对应事件 A 要发生可能性的数量分配。通常，我们考虑执行一个试验并获得一个结果。事件 A 是一个或一组特定的结果，且将某一概率分配给这个事件。

一般很难确切掌握概率的概念。不同的应用理论有着不同的概率表现方法。事实上，存在许多不同的概率定义。这里我们给出三种定义。

1. 公理化定义

一个概率的形式化方法是从一定数量的定义概率度量的公理出发，经过推导规则达到概率的有效计算。公理是必须被接受的简单断言。一旦公理被接受，每一条规则就可能证明。

在公理和规则中要使用下列来自集合论的概念。必然事件 Ω 是在每一次试验中都发生的事件，它包括所有可能结果的全集或称“样本空间”。两个事件 A 和 B 的并集 $A \cup B$ 是当 A 或者 B 或者两者都发生时发生的事件。交集 $A \cap B$，也可写做 AB，是当事件 A 和 B 都发生时发生的事件。如果一个事件的发生不包括另一个事件的发生，那么这两个事件是互斥的。事件 $\overline{A}$ 是当 A 不发生时发生的事件。这些概念借助维恩(Venn)图更容易理解，如图 1.1.1 所示。在每一个图中，阴影部分对应图下面的表达式。图 1.1.1(c)和(d)对应着 A 和 B 不是互斥的情况，即某些结果是作为事件 A 和 B 两者的一部分而定义的。图 1.1.1(e)和(f)对应着 A 和 B 是互斥的情况，在这种情况下 A 和 B 的交是空集。

通常用来定义概率的公理集合，包括如下：

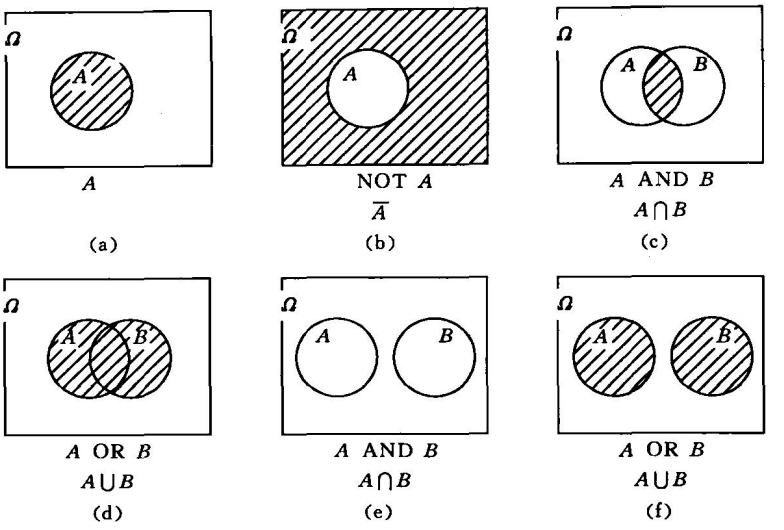

图 1.1.1 维恩(Venn)图

(1) 对于每一个事件 A,有 $0 \leqslant P(A) \leqslant 1$。

(2) $P(\Omega)=1$。

(3) 如果 A 和 B 是互斥的,则 $P(A \cup B)=P(A)+P(B)$。

公理(3)可以扩展到许多事件。例如,如果 A,B 和 C 是互斥的,$P(A \cup B \cup C)=P(A)+P(B)+P(C)$。应当注意到,这条公理并没有规定单个结果或事件的概率应该如何分配。基于上述公理可以推导出许多规则。下面是一些重要的规则:

$$P(\overline{A}) = 1 - P(A)$$

如果 A 和 B 是互斥的,则

$$P(A \cap B) = 0$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

例 1.1.1 抛骰子。

考虑抛一个骰子。存在六种可能的结果。其中必然事件是六面骰子的任何一面在上面总要发生。事件{偶数}和{小于 3}的并是事件{1 或 2 或 4 或 6},这两个事件的交是事件{2}。事件{偶数}和{奇数}是互斥的。如果我们假定六种结果的每一个都是同样可能的,并且分配给每一个结果的概率为 1/6,很容易看到上述三个公理都被满足了。我们能应用概率规则获得如下结果:

$P\{\text{偶数}\} = P(2) + P(4) + P(6) = 1/2$

$P\{\text{小于 3}\} = P(1) + P(2) = 1/3$

$P\{\{\text{偶数}\} \cup \{\text{小于 3}\}\} = P\{\text{偶数}\} + P\{\text{小于 3}\} - P(2) = 1/2 + 1/3 - 1/6 = 2/3$ □

2. 相对频率定义

相对频率方式使用下列的概率定义。将一个实验做许多次,每一次称为一个试验。对于每一个试验,观察事件 A 是否发生。事件 A 的概率 $P(A)$ 定义为如下极限:

$$P(A)=\lim_{n\to\infty}\frac{n_A}{n} \tag{1.1.1}$$

其中 n 是试验的次数，n_A 是 A 发生的次数。

例 1.1.2 投硬币。

一个人多次投掷硬币。在经过很多次投掷后，硬币正面出现的次数与总共投掷的次数的比率在 0.5 左右，其正面和反面出现的概率相同。 □

3. 古典定义

概率的古典定义如下：

$$P(A)=\frac{N_A}{N} \tag{1.1.2}$$

其中 N 是可能结果的总个数，假设全部结果出现的可能性相同，N_A 是事件 A 在其中发生的结果的个数。

例 1.1.3 抛两个骰子。

我们抛两个骰子并且确定总和为 7 的概率 p。你可能会想到有多个不同的总和，包括(2,3,…,12)，共 11 个，于是得出概率为 1/11。但这是不正确的。我们需要考虑等价可能的结果。为此目的，我们必须考虑到每一个骰子面的组合，并且要区分第一个骰子和第二个骰子。例如，结果(3,4)和(4,3)必须相区别。使用这种方法，总共有 36 种相同可能的结果，而且有 6 种结果(1,6)，(2,5)，(3,4)，(4,3)，(5,2)和(6,1)是我们所要求的。因此，$p=6/36=1/6$。 □

1.1.2 条件概率和独立性

我们经常希望知道在某些事件发生的条件下的概率。条件的影响是删除样本空间的一些结果。

形式化地说，假定事件 B 已经发生时事件 A 发生的**条件概率** $P(A|B)$可以定义为如下比率式：

$$P(A\mid B)=\frac{P(AB)}{P(B)} \tag{1.1.3}$$

这里我们假定 $P(B)$不为零。

如果 $P(AB)=P(A)P(B)$，事件 A 和 B 叫做相互独立的事件。进一步，如果事件 A 和 B 是相互独立的，我们就有 $P(A|B)=P(A)$和 $P(B|A)=P(B)$。

例 1.1.4 抛两个骰子。

在抛两个骰子时，如果我们知道至少一个骰子的面是偶数，得到总和为 8 的概率是多少？

解法 1：

我们可按如下方法推理：由于一个骰子是偶数且和为 8，另一个骰子必定是偶数。因此，有三个相同可能出现的合适结果——(2,6)，(4,4)和(6,2)，而我们要考虑的总结果数为{36－(两个骰子都是奇数)}＝36－3×3＝27。最后的概率是 3/27＝1/9。