# 基于攻击图的分布式网络风险评估方法

方 明 徐开勇 杨天池 孟繁蔚 禹 聪
(信息工程大学电子技术学院 郑州 450004)

**摘 要** 对信息系统进行有效的风险评估,选择有效的防范措施,主动防御信息威胁,是解决信息系统安全问题的关键所在。将攻击图模型应用于信息安全的风险评估。首先针对信息安全风险评估的不确定性和复杂性,将脆弱点关联技术用于风险评估。其次,针对攻击图所描述的攻击路径对于定量指标的分析缺乏相应的处理能力,而风险因素的指标值具有很大的不确定性等问题,采用攻击路径形成概率对信息安全的风险因素的指标进行量化,对原子攻击成功概率进行预处理,提出了基于攻击图模型的分布式风险评估方法。该方法充分利用网络系统中各个主机的计算能力,极大地缩短了攻击图生成时间。

**关键词** 安全风险概率,网络安全风险评估,攻击图
**中图法分类号** TP309 **文献标识码** A

## Distributed Network Risk Assessment Method Based on Attack Graph

FANG Ming XU Kai-yong YANG Tian-chi MENG Fan-wei YU Cong
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

**Abstract** Evaluating risk effectively, selecting effective defence measures and defending information threats actively are the key points of resolving security problems of information system. Based on the actual requirements and status of risk assessment of information security, we integrated attack graph to apply it in studying risk assessment of information security. Firstly, focused on the uncertainty and complexity of risk assessment of information security, we integrated the technology of vulnerabilities associated with to apply it in studying risk assessment. On the other hand, since the attack path described by attack graph model is suited for the quantity data processing, and poor to the qualitative analysis, and risk is uncertain, we quantized the risk factors by the probability of attack path forming proposed in this dissertation, pre-treated the probability of atom attack, and proposed a risk assessment method based on attack graph model. The method takes full advantage of computing power of each host in the network, greatly shortens the attack graph generation time.

**Keywords** Network security risk assessment, Security risk probability, Attack graph

## 1 概述

在席卷全球的信息化浪潮中,信息技术已成为世界经济增长的重要动力。计算机网络在全球迅速普及,不仅极大地影响着人们的生活、学习和工作方式,而且使国家政治、经济、军事及整个社会对网络系统的依赖越来越大。与此同时,网络系统的脆弱性将会对国家关键基础设施构成直接威胁,网络安全风险制约着信息的有效利用并可能给经济安全、国防安全等带来威胁[1]。所有这一切都表明,网络安全已成为国家安全的基础之一,是保护信息化进程健康、有序、可持续发展的基本保障。

针对网络系统的应用环境、应用领域以及处理信息敏感度的不同,网络安全风险评估方法存在很大差别。目前,基于模型的风险评估主要采用以下几种模型。

1)故障树(FaultTree)模型

故障树模型及其分析方法是一种用于评估系统可靠性的形式化方法。Helmer[2]首先使用故障树模型对攻击者的入侵行为进行建模,在描述入侵、标识入侵和正确检测入侵3个部分作了分析。

2)攻击树(AttackTree)模型

攻击树模型是SchLneier[3]在1999年提出的一种系统脆弱性分析模型。攻击树模型可以看作是故障树的一种扩展,它的根节点表示攻击者最终要达到的攻击目标,低层节点表示攻击者为实现上一层目标而可能采取的手段和方法。每一条从根节点到叶节点的路径表示为了到达攻击目标而进行的一个完整的攻击过程。

3)其他树形结构

Clark和Dawkins[4]提出一种任务树模型。任务树的根

到稿日期:2012-04-13 返修日期:2012-07-14

方 明(1987—),男,硕士生,主要研究方向为密码模块分析、信息安全系统工程;徐开勇(1963—),男,研究员,硕士生导师,主要研究方向为信息安全技术、信息安全系统工程;杨天池(1978—),男,博士,主要研究方向为密码模块分析、信息安全系统工程;孟繁蔚(1987—),男,硕士生,主要研究方向为密码模块分析、信息安全系统工程;禹 聪(1986—),女,硕士生,主要研究方向为密码模块分析、信息安全系统工程。

节点为总任务的概括，任务目标和子目标形成层次结构，树的叶节点为各目标所对应的资产，允许重复出现。通过分析每一个网络弱点对资产完成任务目标的影响，得到资产的风险值，再通过分析各个资产在任务树中的重要度来评估网络系统的总体安全性。Edge 等人[5]使用攻击树模型对在线银行系统的安全性进行量化评估，并根据评估结果提出了一种与攻击树结构相同的保护树(Protection Tree)模型，用于制定安全策略。Bistarelli 等人[6]提出一种类似于攻击树结构的防守树(DefenceTree)模型，用于分析各种安全措施的投资回报。防守树采用三层结构：根节点为攻击者最终的攻击目标，第二层节点为攻击目标存在的脆弱性，叶节点为消除脆弱性的方法。在后续研究中，Bistarelli 等人[7]使用条件优先网对防守树进行分析。

4)攻击图(Attack Graph)模型

现实中的网络攻击行为往往需要利用多个弱点、跨越多个主机边界来完成。为了更客观地描述这些攻击行为，需要分析工具能够根据目标网络存在的弱点、运行的服务、物理链接以及访问权限等信息建立系统性的攻击场景。为此，研究人员形式化了发动攻击的前提条件、过程和结果，提出了攻击图模型[8,9]。

与其他树状模型相比，攻击图模型的优势在于它可以更好地实现攻击过程建模的自动化。对于规模较大的网络系统而言，攻击图模型可以有效降低风险评估的复杂度和工作量。

目前，基于模型的评估技术还主要以黑盒式的风险评估为主，并且存在着评估粒度较粗、模型的生成时间过长、算法复杂度过高等缺陷。本文在攻击图模型的基础上，提出了一种分布式的网络风险评估方法，部分地解决了待评估网络规模过大、脆弱点过多所带来的攻击图生成时间过长的缺陷，并借鉴最小关键节点集合方法，有效地降低了改善网络防范措施的成本。

## 2 网络系统主体描述

### 2.1 网络参数抽象

风险评估的前期工作主要是对待评估网络系统进行抽象，抽象的目的是提取网络系统参数，以便于更好地描述目标网络。

在攻击图模型中用三元组 $N=(H,C,T)$ 来描述待评估网络，其中 $H$ 代表网络中的主机集合，$C$ 描述了主机之间相互可达的连接关系，$T$ 代表主机之间的信任关系。用这个三元组，可以大致地描述待评估网络的规模、子网的划分，以及主机之间的连接关系。

在对待评估网络做进一步的分析后，可以发现对于网络信息的风险描述还要有以下几个方面内容：网络主体、威胁主体、脆弱性主体。

网络主体主要包括：

1)主机服务，描述某一主机的服务用如下五元组表示：

$Hostinfo=(Hostid,Srvs,Protocol,Port,Privilege)$

式中，*Hostid* 代表网络中主机的唯一标识符；*Srvs* 代表主机上网络中开放的服务；*Protocol* 代表该服务的通信协议；*Port* 代表该服务的侦听端口；*Privilege* 代表该服务运行时的权限。

2)网络连接关系，用如下四元组表示：

$Netconn=(Srchostid,DesHostid,Protocol,Port)$

式中，*Srchostid* 代表源主机的标识符；*DesHostid* 代表目的主机的标识符；*Protocol* 代表连接所运行的协议；*Port* 代表连接所使用的端口。

对网络主体的描述主要用于脆弱点特征的匹配。通过对网络主体的描述信息，扫描器可以确定待评估网络中脆弱点的种类和位置。

威胁主体用如下五元组描述：

$TA=(Hostid, Curplace, Connlist, Rightlist, AttackGoal)$

式中，*Hostid* 代表初始状态时威胁者所在的主机；*Curplace* 代表威胁者当前所在的位置；*Connlist* 代表威胁者所在主机与其他主机的连接关系；*Rightlist* 代表威胁者在攻击路径中各个主机上的权限；*AttackGoal* 代表威胁者的攻击目标。

描述威胁主体的目的是：通过设置不同的威胁主体特征模拟威胁者可能实施的攻击方式。

脆弱性主体主要分为 3 类：设计脆弱性、实现脆弱性、配置脆弱性。它们存在于与网络资产相关的组件当中(如服务器、路由器、交换机、安全组件、桌面工作站、家用电脑、笔记本电脑、存储设备、无线设备等)，所以在进行脆弱性识别的相关工作之前，首先要标识出网络系统中与资产相关的网络组件。

标识关键网络组件：用户访问信息资产时，也会访问相关的网络组件，网络组件用集合 $NC=\{nc1,nc2,\cdots,ncp\}$ 表示，设网络中共 $p$ 个组件。每个网络组件中都存在相关的脆弱性，识别这些脆弱性的工具主要有：操作系统扫描器、网络基础结构扫描器、专用软件扫描器(针对某一服务或应用程序)、检查表、脚本。

为了自动生成攻击路径，一个脆弱性的标示要反映出它的 3 方面特性：1. 脆弱性概况；2. 脆弱性发生的前提条件；3. 脆弱性导致的后果。脆弱性的描述模型如图 1 所示。

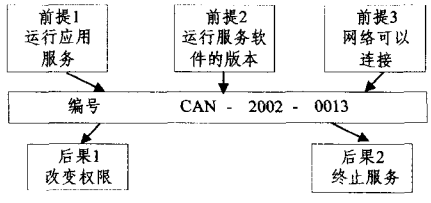



图 1 描述脆弱性模型

描述脆弱性概况主要有 3 个属性：NUM：描述脆弱性的唯一标识符；NAME：脆弱性的名称；TIME：脆弱性的发布时间。

脆弱性前提条件的属性：

1) OS：代表主机中运行的操作系统。OS 属性中有 4 部分内容：NAME：操作系统名称；Version：操作系统的版本；Archi：操作系统的架构(x86 或 sprc)；Kernel：操作系统内核版本(linux 或 unix)。

2) Application：代表与脆弱性相关的应用程序。主要有两方面的内容：NAME：有脆弱性的程序名称。Version：应用程序版本。

3) Acess：代表与访问相关的属性。主要由两部分组成：RANGE 和 SRCPRIVE，RANGE 的值为 0 时，表示本地渗透，指威胁主体必须在目标主机上具备一定的权限，RANGE 的值为 1 时，表示远程渗透，在目标主机外发起入侵，不需再

目标主机上具有权限。SRCPRIVE 表示威胁主体利用该脆弱性发起攻击时必须具备的权限，共有 3 个可利用的权限，Root：对主机资源有完全控制能力的用户；User：有自己独立的资源，具备相应的用户权限；Access：远程访问，不具备本地权限。

4) CONNECTION：代表与连接相关的属性，也是由两部分组成：CONNPROTO 和 CONNPORT，其中 CONNPROTO 描述网络连接的通信协议，CONNPORT 描述网络连接的通信端口。

5) PROBILITY：代表脆弱点被成功利用的概率。其值分为 5 个等级：E1：0.1：发现不久或未报告的脆弱性，不知如何渗透；E2：0.3：公开了报告但是还没有提及可能的渗透方法；E3：0.5：公开进行了报告并有粗略的渗透方法；E4：0.8：公开了报告并出现详细的渗透方法，但是没有现成工具；E5：1.0：有成熟的工具，很容易获得。

脆弱性导致的后果属性：

1) CIA：代表脆弱性被成功利用后对信息资产安全需求的影响，主要有 3 个方面：CIAC：脆弱性被成功利用后对资产机密性的影响；CIAI：脆弱性被成功利用后对资产完整性的影响；CIAA：脆弱性被成功利用后对信息资产可用性的影响。

2) CONNCHANGE：代表脆弱性被利用后网络连接的改变，主要由两个部分组成：CONNCHANGEPROTO：描述网络通信协议的改变；CONNCHANGEPORT：描述网络通信端口的改变。

3) PRIVECHANGE：描述脆弱性被成功利用后威胁主体在目标主机上所获得的权限，其值为：0、1、2，当值为 0 时，代表威胁主体所获得的权限只是一个普通的访问权限；当值为 1 时，代表威胁主体所获得的权限为普通用户的权限；当值为 2 时，代表威胁主体获得了目标主机的管理员权限。

4) SEVERITY：描述脆弱性被利用后对信息资产影响的严重程度。

在网络参数抽象过程中，对脆弱性主体的描述是该过程的核心部分，攻击图生成的自动化正是利用脆弱性主体的属性实现的。

### 2.2 信息资产安全目标

在目前的网络管理方法中，访问控制策略是十分有效的安全管理办法。根据资产信息敏感度的等级，为信息资产定义相应的安全目标。

定义一个特定资产的安全目标 $O_i$，主要体现在对其访问权限的控制等级上，如：

$$SR(o_i)=(TA.\ privilege[ip_1]<Root)$$

此式表示主机 $ip_1$ 的安全目标是：攻击者不能获取该主机上的 *Root* 权限。如果上面所列出的表达式结果不为真，则说明该安全目标存在安全风险。

### 2.3 信息资产重要度

在网络系统中，主要的信息资产包括以下 4 个方面：

1)网络系统中的数据；2)网络系统中所应用的软件和操作系统；3)网络系统中所必需的网络服务；4)网络系统中的硬件。根据不同网络中信息资产的功能和作用，对信息资产的重要度进行计算。

信息资产破坏给网络系统带来的不良后果涉及到多个属性，通常的后果属性主要有：收入的损失、信誉损失、客户流失、等。设有 $n$ 个后果属性 $P_1 \cdots P_n$，其对应的权重分别为 $a_1, \cdots, a_n$。根据以上分析得出的信息资产列表表 1 所列。

表 1 信息资产权重列表

| 信息资源 | $P_1(a_1)$ | $P_2(a_2)$ | …… | $P_n(a_n)$ |
|---|---|---|---|---|
| $assert_1$ | $\beta_{11}$ | $\beta_{12}$ | …… | $\beta_{1n}$ |
| $assert_2$ | $\beta_{21}$ | $\beta_{22}$ | …… | $\beta_{2n}$ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $assert_n$ | $\beta_{n1}$ | $\beta_{n2}$ | …… | $\beta_{nn}$ |

其中 $\beta_{ij}$ 在 0 与 1 之间，表示第 $i$ 个信息资产影响第 $j$ 个后果属性 $P_j$ 的权重系数。信息资产重要度的计算公式为：

$$A_i=\sum_{j=1}^{n} a_j\beta_{ij}$$

一个信息资产的安全需求主要有 3 种类型：1)机密性；2)完整性；3)可用性。每一个信息资产对上述 3 方面安全需求的侧重点不同，比如说 Web 网页信息，其机密性不是它安全需求的重点，维护它的可用性才是重中之重。对于一个信息资产，它的安全需求可以表示为：

$$SR(assert_i)=\{C(assert_i), I(assert_i), A(assert_i)\}$$

其中大括号内 3 个安全需求类型的取值可以是 0 或 1。将安全需求转换为安全目标，如：

$$SR(O_i)=(TA.\ privilege[ip_1]<某一权限)$$

表示威胁主体不可获得主机 $ip_1$ 上的某一权限。得到合理的安全需求后，把攻击目标与安全需求相对照，即(攻击目标用 $Sf$ 表示)：

$$Sf=\neg SR(O_i)$$

即将黑客的攻击目标转换为破坏某一信息资产的安全目标，即访问权限。

## 3 分析过程

### 3.1 本地分析

根据上一节对网络主体属性的描述，可以将网络系统风险分析分为本地分析和远程分析。值得一提的是，攻击者在发动远程攻击之前务必获取本地主机的 Root 权限，只有在获得 Root 权限之后，攻击者才可以实施构造数据包和打扫攻击痕迹的操作，否则这些违规操作很容易被主机的审计系统和网络中的入侵检测系统所发现。

下面对本文中所提出的本地风险分析方法的过程进行详细的介绍。本地风险分析主要由两部分组成：操作系统漏洞分析和应用程序漏洞分析，过程如下。

1) 根据攻击者所具备的初始条件，结合操作系统脆弱点的前提条件集合和后果集合，对本地操作系统进行入侵行为的模拟，并找出攻击者可能获取的最高权限(Access，User，Root)。

2) 如果攻击者不能获得主机的 Root 权限，则根据攻击者已获得的权限对信息资产进行安全目标评价(机密性、完整性、可用性)；如果攻击者已经获得 Root 权限，则说明本机上信息资产的安全目标已被完全破坏(最坏情况评估)，可以直接向风险分析小组提交本地分析报告。

3) 根据已获得的主机权限对本地主机上所有应用程序进行漏洞分析，如果攻击者所拥有的权限小于应用程序的运行权限，则停止分析该应用程序，转向下一个应用程序；如果攻击者拥有的权限大于某应用程序的运行权限，则根据该应用程序所暴露的漏洞对信息资产进行安全目标风险分析(机密性、完整性、可用性)，然后转回操作系统分析，检查攻击者根据该应用程序漏洞是否可以提升自己的权限。当遍历主机

中所有应用程序后，向风险分析小组提交本地分析报告。本地分析报告中的输出是：攻击者获得的主机权限、渗透路径和本机信息资产风险值。图 2 说明了本地分析的过程。

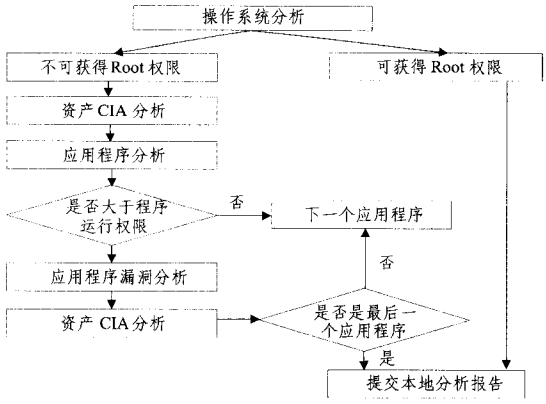



图 2　本地分析过程

3.1.1　本地分析攻击图生成方法

攻击图的绘制主要分为如下两个步骤：

1）根据脆弱点的前提集合与后果集合，将脆弱点进行排序，并转化为攻击路径。一个网络中会存在多条攻击路径，将可能的攻击路径一一找出。

2）对找出的攻击路径进行分析，绘制出攻击图，其算法如下：

输入：多条攻击路径，用 $Epl_i$ 表示($i\in[0,k]$)，路径中的节点用 $e_j$ 表示($j\in[0,k]$)。

输出：图形化的逻辑攻击路径。

设：Ns 为已经绘制的节点，Ns 初始化为空集。Ed 为已经绘制的边的集合，将 Ed 初始化为空集。

```
Bigin
  for Each epl_i∈Ep_l Do
    For Each e_j∈epl_i(j>0) Do
      If (e_j∉Ns) Then
        CreateNode(e_j);
          Ns=Ns+e_j;
        End If
        If(ed(e_j-1,e_j)∉Ed)Then
          CreateEdge(e_j-1,e_j);
          Ed=Ed+ed(e_j-1,e_j);
        End If
      End For
    End For
  END
```

经过以上的步骤，就获得了攻击者在某一台主机上可能实施的多条攻击路径。做两点假设：1）攻击者的能力是不受限制的，攻击者能熟练地应用一切攻击技能。2）攻击者是理智的，不会重复获得已经获得的权限及原子攻击节点。

依据这两条假设，每条攻击路径中，最后一个节点就是攻击者的攻击目标。同时，攻击路径中最后一个节点也是组成该攻击路径所有节点中权限最高、对资产影响最大的脆弱点。将每条攻击路径中最后一个节点的 PRIVECHANGE 项的值返回(0 为访问权限，1 为普通用户权限，2 为管理员权限)，与资产的安全目标进行对比，如果权限大于或等于资产安全目标中所定义的权限值(如 $SR(O_i)=(TA.\ privilege[ip_1]=root)$，则此资产存在风险；否则不受影响，并将资产的重要度作为风险值的输出。

## 3.2　远程分析

本地分析由网络系统中各个主机分别进行，并提交分析结果(结果包括所有的攻击路径、可获得的权限、资产风险值)。而远程分析则由风险评估小组依据本地分析过程中各个主机提交的结果进行，远程分析主要考虑网络系统中两方面的内容：

1）主机间的关联性。

2）生成网络系统的攻击图。

具体分析过程如下：

1）风险分析小组筛选出所有攻击者可能获得 Root 权限的主机，与其他主机相比，这些主机极有可能就是攻击者潜在的攻击平台。

2）风险分析小组会考察每台可以获得 Root 权限主机的 Connlist 项(所在主机与其他主机的连接关系)。

3）如果所连接的主机不能获得 Root 权限，则该主机就是网络系统中某一攻击路径的终点；如果该主机可以获得 Root 权限，继续比对 Connlist 项，直到遍历所有可获得 Root 权限的主机为止。

4）由风险分析小组生成网络系统的攻击图(节点为各个主机)，每个节点中包含该主机提交的本地分析的结果。风险分析小组依据生成的攻击图，对每条攻击路径中的节点主机的资产影响程度求和，得到最终的网络系统的风险值。

网络系统攻击图算法如下：

输入：多条攻击路径，用 $Epl_i$ 表示($i\in[0,k]$)，路径中代表主机的节点用 $e_j$ 表示($j\in[0,k]$)。

输出：图形化的逻辑攻击路径。

设：Ns 为已经绘制的节点，Ns 初始化为空集。Ed 为已经绘制的边的集合，将 Ed 初始化为空集。

```
BIGIN
  For Each epl_i∈Epl Do
  For Each e_j∈epl_i(TA. privilege[e_j]=Root&&e_j∉Ns) Do
      Cheak(e_j. Connlist);//查看连接列表
        For Each e_i∈e_j. Connlist Do
      If (e_i∉Ns) Then
        CreateNode(e_i);
        Ns=Ns+e_i;
      End If
      If(ed(e_i-1,e_i)∉Ed)Then
        CreateEdge(e_i-1,e_i);
        Ed=Ed+ed(e_i-1,e_i);
      End If
        End for
    End For
  End For
END
```

在网络系统攻击图的基础上，依据攻击路径上的节点，对信息资产影响程度求和，便可得到整体网络系统中存在的风险值。

## 3.3　计算攻击路径概率

3.3.1　概率评价

根据上一节的假设知道，攻击者的能力和知识是不受约束的，并且攻击者也具有足够的理性。也就是说，攻击者会寻找到一条成功概率最大的攻击路径来执行入侵行为。对于一个脆弱点而言，我们用三元组来表示与该脆弱点相关的概率集合：$[Ps(e_i),Pd(e_i),Pf(e_i)]$，其中，$Ps(e_i)$表示原子攻击成

功的概率，$Pd(e_i)$表示其被安全措施检测而导致失败的概率，$Pf(e_i)$表示其他原因导致执行失败的概率，且 $Ps(e_i)+Pd(e_i)+Pf(e_i)=1$。

在上一节描述的攻击图模型中存在分支结构，即一个脆弱点的后果集合同时满足多个脆弱点的前提集合。如图 3 所示，这时攻击者就要做出选择，引入脆弱点转移概率 $P(e_i, e_j)$。

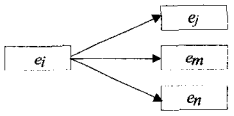



图 3　攻击节点关系

$P(e_i, e_j)$表示攻击者在节点 $e_i$ 时刻选择 $e_j$ 作为下一时刻攻击目标的概率。结合脆弱点相关概率集合，可以定义成功执行某一攻击路径的概率，攻击路径概率定义如下：

$P(ep_i)$表示攻击路径成功的概率，且有：

$$P(ep_i)=ps(e_{i1})\cdot P(e_{i1},e_{i2})\cdot Ps(e_{i2})\cdot\cdots\cdot P(e_{ik},e_{ik+1})\cdot Ps(e_{ik+1})$$

对于某一特定资产而言，最大 $P(ep_i)$的概率与资产重要度的乘积就是该资产的风险值，用 $Risk$ 表示，有：

$$Risk=P(ep_i)\cdot A_i$$

式中，$A_i=\sum a_j\beta_{ij}$，表示已定义的资产重要度。

当两条攻击路径具有相同的成功概率时，攻击者一般会选择攻击路径最短的一个。根据以上的分析可以得出以下结论，即攻击者实施的攻击路径是概率最大、攻击步骤最少的一条。

### 3.3.2　计算攻击路径概率步骤

Step1　获取基础概率数据。基础概率是指：单个原子攻击成功概率 $Ps(e_i)$和原子攻击之间的转移概率 $P(e_i, e_j)$，可以通过主观方法和客观方法获得。主观方法是指：依据网络系统的特点，由专家给出相应的概率值。客观方法是指：依据入侵检测、防火墙和审计系统的统计数据得到客观的概率值。

Step2　根据 Step1 获得的基础概率，形成原子攻击之间的转移概率矩阵 $T$ 和原子攻击执行概率 $B$。其中 $T$ 为 $n\times n$ 阶矩阵，且满足以下特点（$E$ 代表原子攻击数量）：

1）$n=|E|$，$t_{ij}=P(e_i,e_j)$，$i,j\in n$，$0\leqslant i,j\leqslant n$。

2）$t_{ii}=0$，$i\in n$，$0\leqslant i\leqslant n$（由于攻击者不会重复攻击同一个节点，因此脆弱点自身到自身的转移概率为 0）。

3）$t_{ij}=t_{ji}$是不一定成立的，表示攻击节点之间的转移是有序的对。

矩阵 $B$ 是一个 $3\times n$ 阶矩阵（$n=|E|$），且满足以下特点：

1）$b_{1i}=Ps(e_i)$，$b_{2i}=Pd(e_i)$，$b_{3i}=Pf(e_i)$，$0\leqslant i\leqslant n$；

2）$0\leqslant b_{ij}\leqslant 1$，$i=1,2,3$，$j\in n$，且$\sum_{i=1}^{3} bij=1$。

Step3　计算攻击路径的概率模型，求解出大于风险容忍度的攻击路径。

Step4　根据 Step3 中所得的结果综合生成攻击图模型。

在攻击图模型中引入攻击路径成功概率的计算过程，可以更加直观地反映出存在于网络组件中的脆弱性对整体网络系统的影响程度，进而可以使风险评估结果更加有效地指导网络系统安全措施的改进。

## 4　方法验证

验证环境由局域网中 3 台主机 ip1、ip2、ip3 组成，它们相互之间是可连通的，并且都会应用相同的协议和通信端口，其中主机 ip1 包含网络信息资产 A1、A2，主机 ip2 包含网络信息资产 A3，主机 ip3 包含网络信息资产 A4，其中资产的安全目标定义如下：

资产 A1、A2 的安全目标定义为 $SR(Oi)=(TA.privilege[ip_1]<Root)$。资产 A3 的安全目标为：$SR(Oi)=(TA.privilege[ip_2]<User)$。资产 A4 的安全目标为 $SR(Oi)=(TA.privilege[ip_3]<User)$。

在验证环境中，网络安全风险的后果属性由 3 部分组成，其重要程度分别如下：

1）P1 收入损失：重要程度为 0.3；

2）P2 生产力损失：重要程度为 0.1；

3）P3 公共信誉损失：重要程度为 0.6。

列出资产后果矩阵如下：

| 信息资源 | P1 | P2 | P3 |
|---|---|---|---|
| A1 | 0.3 | 0.2 | 0.5 |
| A2 | 0.4 | 0.3 | 0.3 |
| A3 | 0.5 | 0.4 | 0.1 |
| A4 | 0.2 | 0.1 | 0.7 |

根据矩阵中所列出的数据，可以计算出资产的重要度为：

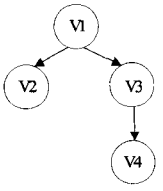
A1=0.3×0.3+0.2×0.1+0.5×0.6=0.41

A2=0.4×0.3+0.3×0.1+0.3×0.6=0.33

A3=0.5×0.3+0.4×0.1+0.1×0.6=0.25

A4=0.2×0.3+0.1×0.1+0.7×0.6=0.49

将网络主体参数输入验证环境中的脆弱点扫描工具，得出系统中存在以下脆弱点：主机 ip1 中的本地脆弱点为 V1，V2，V3，V4。其关联性由本地分析得出的攻击图表示为：




攻击者成功利用脆弱点 V4 后，可以获得主机 ip1 上的 Root 权限，相应的资产 A1、A2 将受到风险威胁。攻击者成功利用脆弱点 V2 后，只能获得主机 ip1 上的 User 权限。根据以上分析并结合脆弱点本体描述属性，可以得出本地攻击中脆弱点成功利用概率和路径选择概率如下：

由专家打分可以获得成功利用脆弱点 V1 的概率为 0.5，成功利用脆弱点 V2 的概率为 0.3，成功利用脆弱点 V3 的概率为 0.3，成功利用脆弱点 V4 的概率为 0.5。选择概率为：$P(V1,V2)=0.3$，$P(V1,V3)=0.7$，$P(V3,V4)=1$。计算得出攻击者成功利用脆弱点 V4 的概率为：0.5×0.7×0.3×1×0.5=0.0525，则主机 ip1 上的资产 A1，A2 的最终风险值为：(0.41+0.33)×0.0525=0.03885。

同理，在主机 ip2 上进行相同过程的风险分析得到攻击路径概率为 0.0334，不同的是在主机 ip2 上攻击者能获得的最高权限为 User 权限，不能获得 Root 权限；得出主机 ip2 上的资产最终风险值为：0.25×0.0334=0.00835。对主机 ip3 的分析过程与主机 ip2 相同，在主机 ip3 上攻击者可获得的最高权限是 Access，所以资产 A4 没有威胁风险。

根据以上分析，结合威胁主体属性和远程分析过程，将得出以下 3 种网络总体风险值：

1）威胁主体以主机 ip1 为发起攻击的起始点，则网络总

体风险值为 0.03885+0.00835=0.0472；

2)威胁主体以主机 ip2 为发起攻击的起始点，则网络总体风险值为 0.00835；

3)威胁主体以主机 ip3 为发起攻击的起始点，则网络总体风险值为 0。

所以依据最坏情况评估的原则，网络系统中存在的总体风险值为 0.0472。

**结束语** 计算机和网络技术的迅速发展深化了社会信息化的进程，也使得组织与网络系统的关系日趋密切。然而网络系统在提高信息资源共享性和业务运行效率的同时，也带来了网络系统的安全问题。因此，作为网络系统建设和安全管理的基础，网络系统安全风险评估具有极为重要的现实意义。本文在分析网络系统发展对安全风险评估提出的新需求的基础上，以网络系统为研究对象，基于风险评估理论，综合运用信息安全学提出了一种基于攻击图的分布式网络安全风险评估方法框架，建立了形式化的安全风险过程模型。在进一步的研究中还需要解决基础概率数据获取的问题，以及安全改进过程中关键节点的选定问题。

## 参 考 文 献


[1] 王永杰，鲜明，刘进，等. 基于攻击图模型的网络安全评估研究[J]. 通信学报，2007，28(3)：29-34

[2] Helmer G，Wong J，Slagell M，et al. A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System[J]. Requirements Engineering Journal，2010，7(4)：207-220

[3] Schneier B. Attack Trees[J]. Dr. Dobb's Journal，2010，24(12)：21-29

[4] Clark K，Dawkins J，Hale J. Security Risk Metrics：Fusing Enterprise Objectives and Vulnerabilities[C]//Proc 2009 Systems，Man and Cybermetics (SMC) Information Assurance Workshop. IEEE press，2009：388-393

[5] Edge K，Raines R，Bennington R，et al. The Use of Attack and protection Trees to Analyze Security for an Online Banking System[C]//Proc the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). Hawaii，USA，IEEE press，2007

[6] Bistarelli S，Fioravanti F，Peretti P. Defence Trees for Economic Evaluation of Security Investments[C]//Proc the First International Conference on Availability and Security (ARES'06). Vienna，IEEE press，2006：416-423

[7] Bistarelli S，Fioravanti F，Peretti P. Using CP-nets as a Guide for Countermeasure Selection[C]//Proc the 2007ACM Symposium on Applied Computing. Seoul，Korea，ACM press，2007：300-304

[8] Krishnan C R，Sekar R. Model-based Vulnerability Analysis of Computer Systems[C]//Proc the 2nd International Workshop on Verification，Model Checking and Abstrac Interpretation. NY，USA，1998

[9] Swiler L P，Phillips C，Ellis D，et al. Computer Attack Graph Generation Tool[C]//Proc 2001 DARPA Information Survivability Conference and Exposition. CA，USA，IEEE press，2001：307-321


(上接第 132 页)

从图 7 可看出，本文所提信誉模型在最初时成功率较低，这应该是主机节点对客户节点的拒绝造成的，但随着交易的进行，成功率一直处于明显的上升趋势，明显好于另外两者。

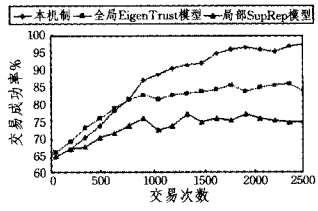



图 7 相同条件下 3 种模型的交易成功率

**结束语** P2P 文件共享系统作为资源共享领域的一次革命，引起了广泛的关注，但是对节点信誉评价的不准确、网络开销太大、节点的积极性缺乏及恶意节点和病毒的破坏等问题成为遏制其发展的重要因素。本文提出一种基于兴趣分组的信誉模型，并对其工作原理进行了详细阐述，最后对其进行了仿真和性能测试。实验数据表明，该算法降低了网络的消息负载，提高了搜索效率和交易成功率，并且能够有效地抑制自私节点，提高系统的可用性和服务质量。

## 参 考 文 献


[1] Ledlie J，Taylor J，Serban L，et al. Self-organization in peer-to-peer systems[C]//Tenth ACM SIGOPS European Workshop. 2002：45-48

[2] Schlosser M，Sintek M，Decker S，et al. A Scalable and Ontology-based p2p Infrastructure for Semantic Web Services[C]//Proceedings of the Second IEEE International Conference on Peer-to-Peer Computing. 2002：104-111

[3] Gnasa M，Alda S，Grilgull J，et al. Towards Virtual Knowledge Communities in Peer-to-Peer Networks[C]//Proceeding of ACM SIGIR Workshop on Distributed Information Retrieval Workshop at the 26th International ACM SIGIR Conference. 2003：3-8

[4] Khambatti M，Dasgupta P，Ryu K D. A role based trust model for peer to peer communities and dynamic coalitions[C]//Proceedings of the Second IEEE International Information Assurance Workshop. 2004：141-154

[5] Kamvar S D，Schlosser M T. EigenRep：Reputation Management in P2P Networks[C]//The 12th International World Wide Web Conference. 2003

[6] Kamvar S D，Schlosser M T，Molina H G. The EigenTrnst Algorithm for Reputation Management in P2P Networks[C]//Proceedings of the Twelfth International World Wide Web Conference. 2003：640-651

[7] 窦文，王怀民，贾焰，等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报，2004，15(4)：571-583

[8] Abdul-Rahman A，Hailes S. Supporting Trust in Virtual Communities[C]//Proceedings of International Conference on System Sciences. 2000，33

[9] Selcuk A A，Uzun E，Pariente M R. A Reputation-Based Trust Management System for P2P Networks [C]// International Workshop on Global and Peer-to-peer Computing. 2004

[10] Tran H，Hitchens M，Varadharajan V，et al. A Trust based Access Control Framework for P2P File-Sharing Systems[C]//Proceedings of the 38th Hawaii International Conference on System Sciences. 2005

[11] 李绍静. P2P 网络文件共享系统中的信誉激励机制研究[D]. 广州：华南农业大学，2007