# Quantitative Threat Evaluation Method for Large-scale Network Based on Attack Character

**Cai Jun[1], Xu XiShan[2], Cheng WenChong[3], Ye Yun[4]**

*School of Computer Science, National University of Defense Technology, ChangSha, China*

*1. cjgfkd@163.com, 2. xxs999@139.com，3. emailtocheng@yahoo.com.cn, 4. yeyun1234@tom.com*

**Abstract:** The rapid development of Internet in China brought an increasing number of network security issues. In order to enhance the defense capabilities of existing networks, it is necessary to establish a scientific Internet Security Status Indices (ISSI) to reflect the level of security status in time. In this paper, we first developed the basic framework of ISSI, and then focused on a quantitative network security threat evaluation model based on attack characters to evaluate threat status which is part of ISSI. The experimental results show that the model can accurately reflect security threat status of a large-scale network.

**Keywords:** internet security status indices; network security threat index; security event; attack character

# 基于攻击特征的大规模网络威胁量化方法

**蔡军[1]，徐锡山[2]，程文聪[3]，叶云[4]**

*国防科大计算机学院，长沙，中国，410073*

*1. cjgfkd@163.com, 2. xxs999@139.com，3. emailtocheng@yahoo.com.cn, 4. yeyun1234@tom.com*

**【摘要】**互联网在我国飞速发展的同时也带来了越来越多的网络安全问题，为提高现有网络的防御能力，有必要建立一套科学的互联网安全态势指数来及时反映我国互联网的安全态势水平。本文提出了互联网安全态势指数的基本框架，并重点研究了安全态势量化中的威胁量化方法，提出了基于攻击特征的网络安全威胁量化模型。实验表明，使用该模型能直观准确的反映大规模网络的安全威胁态势。

**【关键词】**互联网安全态势指数；网络安全威胁指数；安全事件；攻击特征

## 1 引言[1]

随着计算机和通信技术的飞速发展，网络应用日益普及，已经成为人们生活中不可缺少的一部分。根据中国互联网络信息中心(CNNIC)和国家计算机网络应急技术处理协调中心(CNCERT/CC)统计：截至 2008 年 6 月底，中国网民数量达到 2.53 亿，网民规模跃居世界第一位；中国网民规模继续呈现持续快速发展的趋势，比去年同期增长了 9100 万人，同比增长 56.2%[1]。

在网民数量激增和诸如网络音乐、网络新闻、即时通信、网络视频、搜索引擎、电子邮件、网络游戏、博客/个人空间、论坛/BBS 以及网络购物等网络应用飞速发展的同时，我国互联网面临的安全问题也越来越严重,各种网络安全事件如木马、僵尸网络、网络仿冒、网页恶意代码等层出不穷，增长迅速[2]。

为提高现有网络的防御能力，支撑政府宏观决策，减少人们对互联网安全问题的担忧，有必要建立一套科学的互联网安全态势指数来及时反映我国互连网的安全态势水平。这也是国家 863 课题（NO.2007AA010502）——“网络安全态势分析与预测系统”的研究内容之一。

本文首先提出了互联网安全态势指数的基本框架，接下来重点研究互联网安全态势量化中的威胁量化方法，提出了基于攻击特征的网络安全威胁量化模型，并采用 CNCERT/CC 提供的数据对该模型进行了实验分析。

## 2 相关研究

### 2.1 网络安全量化评估相关研究

网络安全评估按被评估对象分为面向局域网的安

基金项目：国家高技术研究发展计划(863 计划)资助（2007AA010502, 2007AA01Z474, 2006AA01Z451）**Foundation Item**: Supported by National High Technology Research and Development Program of China (2007AA010502, 2007AA01Z474, 2006AA01Z451)

全评估和面向大规模网络的评估。所谓大规模网络是指在网络的深度上呈现承载关系的复杂性，在网络的广度上呈现为广域特征的网络[3]。本文研究中涉及的大规模网络指国家骨干网级的网络。

在面向局域网的安全评估方面，陈秀真等人提出了层次化网络安全威胁态势定量评估模型及相应的计算方法[4]，该模型采用自下而上、先局部后整体的评估策略，结合服务、主机本身的重要性及网络系统的组织结构，从服务、主机、局域网三个层次来进行安全威胁评估。龙百元等人提出了基于近似权重计算的网络安全威胁评估方法，对传统 AHP 方法做了改进，建立了基于“威胁对资产的影响—安全属性—攻击”的威胁评估模型[5]。然而，由于大规模网络的处理复杂度和信息获取的难度，这些方法都不适用于大规模网络的评估。

在面向大规模网络的安全评估方面，Salim Hariri 等人提出了基于 Agent 的大规模网络弱点与攻击影响在线监测与评估框架[6]，该框架将网络构成分为客户端、路由器、服务器三种，其系统级的威胁由构成该系统的所有网络构成的威胁加权综合得到。该方法能实时评估网络安全威胁，但其在进行评估时仅考虑了单一影响因素，评估信息不够全面，且这种方法评估的规模依然有限。程学东提出了电信网网络安全评估指标体系[7]，其特点是将指标建立在由网络安全层面，网络安全侧面和网络安全维度三部分组成的网络安全框架体系之上，不过没有给出各指标的具体设定方法。赵阳等人提出了面向等级保护的大规模网络动态风险评估模型[3]，该模型试图自动识别和量化大规模网络的各风险要素，但没有提出具体的实施方法，而是一个理论上的框架设计。

### 2.2 多指标综合评价方法相关研究

由于网络安全涉及多个方面，要对网络安全态势做出总体评价，需要用某种手段或方法把影响网络安全的各个方面综合起来作为一个统一体来认识，多指标综合评价方法正是这种综合工具。多指标综合评价方法是利用多指标综合指数的理论及方法,将所选择的有代表性的若干个指标综合成一个指数,从而对事物的发展状况做出综合的评价[8]。多指标综合评价需要解决两个问题：一是指标的归一化，二是综合时的指标权数的确定。

由于不同的指标具有不同的量纲，只有统一消除量纲后才能对这些指标进行综合。归一化是将指标进行无量纲化处理得到一个 0～1 之间的相对数。常见的归一化方法有统计标准化，极值标准化等[8]。关于指标赋权目前也有多种方法,概括起来可分为三类，即主观赋权法、客观赋权法和组合赋权法[8-9]。主观赋权法是研究者根据其主观价值判断来指定各指标权数的一种方法，常见的有专家评判法、层次分析法等，该方法能较好地体现评价者的主观偏好，但由于每个人的主观价值判断标准有差异，因而构建的权数缺乏稳定性。客观赋权法是直接根据指标的原始信息，通过统计方法处理后获得权数的一种方法，常见的有主成分分析法、变异系数法、熵值法等。相对而言，这类方法受主观因素影响较小，它的缺陷在于权数的分配会受到样本数据随机性的影响，不同的样本即使用同一种方法会得出不同的权数。组合赋权法是将主观赋权法和客观赋权法得出的权数进行组合，以将两者的优点结合，一般有乘法合成和线性加权组合两种权数组合方法。

结合已有研究成果，针对大规模网络的宏观特性和复杂性，本文提出了互联网安全态势指数基本框架。以此框架为背景，重点研究了网络安全威胁量化方法，提出了基于攻击特征的网络安全威胁量化模型及相应的计算方法，并用 CNCERT/CC 提供的数据进行了实验分析。

## 3 互联网安全态势指数基本框架

互联网安全态势指数的选取应具有敏感性、单调性和可操作性等特点。即指数能够说明网络真实安全状态，并能够及时刻画安全状态所发生的变化；指数的变化应与网络安全的总体态势变化保持一致；同时，指数的计算依托于真实、可靠、稳定的数据和科学的计算方法。本文提出如图 1 所示的互联网安全态势指数基本框架。

**定义 1**.互联网安全态势指数. 是对某个时间周期内（一般不短于 24 小时）某个互联网区域内影响网络安全态势的各种因素采用一定的方法进行综合评估量化后得到的一个反映网络整体安全态势的数值。

本文提出的互联网安全态势指数的评估对象为国家骨干网，它由四大类下级指数经过加权综合得到，这四类指数又由具体的下级指标计算得到。网络运行安全指数主要反映网络链路、域名服务和路由等网络基础设施的当前运行状况；网络安全风险指数主要反映网络设备及系统当前所面临的风险，重点考察各种安全漏洞和骨干网络的流量异常情况；网络安全威胁指数主要反映互联网上已经发生的各类安全事件对网络安全的影响；网络安全感知指数主要反映用户对网络安全的感知，体现了网络安全对用户的影响。本文主要研究网络安全威胁指数的计算方法。


978-1-935068-01-3 © 2009 SciRes.

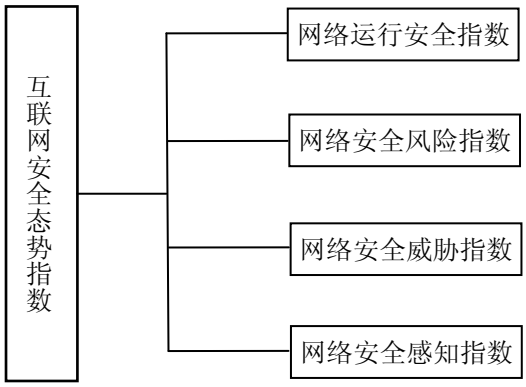


**图 1　互联网安全状况评价指标体系基本框架**

## 4 基于攻击特征的网络安全威胁量化模型及计算方法

### 4.1 基于攻击特征的网络安全威胁量化模型

由于网络安全事件多种多样，其攻击原理、攻击特征、攻击后果不尽相同，把这些安全事件不加区别的对

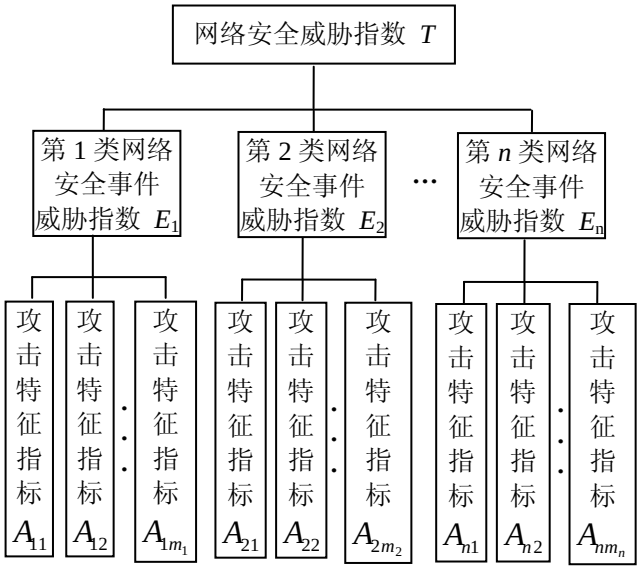


**图 2　基于攻击特征的网络安全威胁量化模型**

待，或者仅仅根据安全事件发生的数量来评估网络安全
事件的威胁显然是不合理的。因此，我们提出了基于安全事件攻击特征的网络安全威胁量化模型，如图 2 所示。

**定义 2**.网络安全威胁指数 *T*.是对一定时间周期内互联网上发生的各种网络安全事件造成的威胁进行综合评估量化后得到的数值，它反映了网络安全事件对网络的威胁程度。

网络安全威胁指数由各类安全事件的威胁指数 $E_i$ 进行加权综合得到，而各类安全事件的威胁指数又由其攻击特征指标经过多指标综合方法得到。

### 4.2 网络安全威胁指数的计算方法

网络安全威胁指数 *T* 的计算分两步：第一步是按照一定的分类标准将网络安全事件分为 *n* 类，然后根据每类安全事件的攻击特征确定其攻击特征指标 $A_1$、$A_2$、…、$A_m$，再由这些特征指标计算其威胁指数 *E*；第二步是将各类安全事件的威胁指数 $E_1$，$E_2$，…，$E_n$ 进行加权综合得到 *T*。

#### 4.2.1 各类网络安全事件威胁指数的计算

网络安全事件造成的威胁由其攻击特征指标确定，给定一定的时间周期 $\Delta t$（如一天、一周、一个月等），定义 *t* 时刻的某类网络安全事件的威胁指数为：

$$E(t)=100\times\sum_{i=1}^{m}g(A_i(t))\times w_i \qquad (1)$$

其中：

（1）$A_i(t)$ 为 *t* 时刻指标 $A_i$ 的数值，$g(A_i(t))$ 为 $A_i(t)$ 的归一化值。本文使用的归一化函数为：

$$g(x)=\begin{cases}1, & x>MaxValue\\ \dfrac{x-MinValue}{MaxValue-MinValue}, & MinValue\le x\le MaxValue\\ 0, & x<MinValue\end{cases}$$

其中 *MaxValue* 和 *MinValue* 分别为指标的历史最大值和历史最小值，通过分析保存在数据库中的历史数据得到。

（2）$w_i$ 为各指标 $A_i$ 对应的权重，满足归一化约束：

$$\sum_{i=1}^{m}w_i=1,\ w_i\ge 0,\ i=1,2,\cdots,m$$

指标权数的确定非常关键，权数的合理性、准确性直接影响评价结果的可靠性。本文采用客观赋权法中的熵值法[9-10]对指标进行赋权。在信息理论中，熵是系统无序程度的量度，可以度量数据所提供的有效信息。熵值法就是根据各指标传输给决策者的信息量的大小来确定指标权数的方法。某项评价指标的差异越大，熵值越小，该指标包含和传输的信息越多，相应权重越大。用熵值法进行赋权的步骤如下：

第一步：将数据库中的数据按照攻击特征指标进行聚集并按照一定顺序进行排列，取前 *top-k* 行，构造样本矩阵：

$$X=\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ A_{k1} & A_{k2} & \cdots & A_{km} \end{pmatrix}$$

其中 $A_{i1}, A_{i2}, \cdots, A_{im}$ 为该类安全事件的攻击特征指标。

第二步：将各项指标数值按如下方式进行归一化处理。

$$a_{ij}=A_{ij}\Big/\sum_{i=1}^{k}A_{ij},\quad i=1,2,\cdots,k,\quad j=1,2,\cdots,m$$

第三步：计算各指标的熵值。

$$H_j=-\frac{1}{\ln k}\sum_{i=1}^{k}a_{ij}\ln a_{ij},\quad j=1,2,\cdots,m$$

第四步：将熵值转换为反映差异大小的权数。

$$w_j=\frac{1-H_j}{k-\sum_{j=1}^{k}H_j},\quad j=1,2,\cdots,m$$

(3)乘数 100 是将威胁指数 $E(t)$ 的值域映射到 0～100。

#### 4.2.2 网络安全事件威胁指数的计算

*t* 时刻的网络安全威胁指数为:

$$T(t)=\frac{1}{n}\sum_{i=1}^{n}E_i(t) \qquad (2)$$

其中，$E_i(t)$ 为 $t$ 时刻安全事件 $E_i$ 的威胁指数，$n$ 为安全事件的种类数。

## 5 实验分析

将网络安全事件分为木马、僵尸网络、计算机病毒、蠕虫、拒绝服务攻击、网页篡改、网页挂马、域名劫持等八类，以木马威胁指数的计算为例进行实验分析，采用 CNCERT/CC 某网络安全监测平台 2007 年 6 月 18 日～2007 年 7 月 15 日四周的木马监测数据作为实验数据。

木马是一种由攻击者秘密安装在受害者计算机上的窃听及控制程序。计算机一旦被植入木马，其重要文件和信息不仅会被窃取，用户的一切操作行为也都会被密切监视，而且还会被攻击者远程操控实施对周围其他计算机的攻击。木马通常包含控制端和被控制端两部分。被控制端植入受害者计算机，而黑客利用控制端进入受害者的计算机，控制其计算机资源，盗取其个人信息和各种重要数据资料。

根据木马的特点，确定木马的攻击特征指标为：木马种类数，控制端数目，受控端数目和攻击次数。将数据库中的数据以天为周期按照这四个指标聚集生成一个聚集统计表。查询聚集统计表即可得到各指标的极值(出于保密原因，这里不展示具体数值)，将各指标归一化，可绘制 2007 年 6 月 25 日～2007 年 7 月 8 日两周内木马单一指标的变化趋势图如图 3 所示。

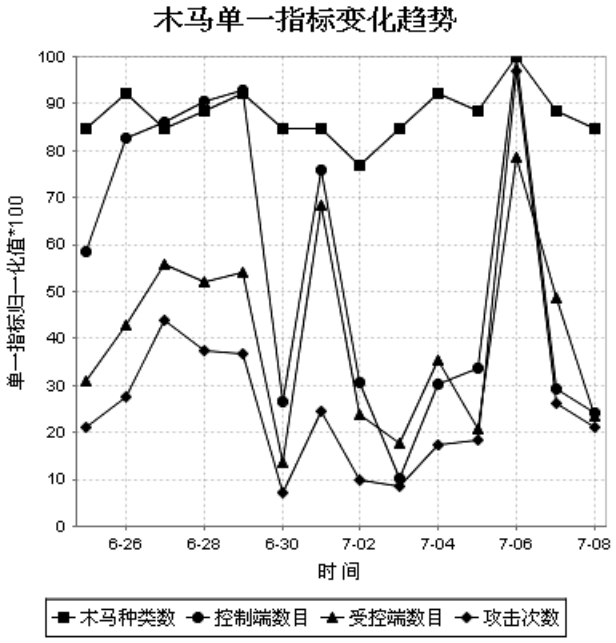


**图 3 木马单一指标变化趋势图**

将聚集统计表按“攻击次数”排序，取前 *top*-10 行构造样本矩阵，按照前面介绍的熵值法赋权的步骤计算得到各指标的权数如表 1 所示。

**表 1 各指标权数**

| | 木马种类数 | 控制端数目 | 受控端数目 | 攻击次数 |
|---|---|---|---|---|
| 权数 | 0.01 | 0.15 | 0.24 | 0.60 |

根据公式(1)计算出 2007 年 6 月 25 日～2007 年 7


978-1-935068-01-3 © 2009 SciRes.

月 8 日两周内每天的木马威胁指数，绘成曲线图，如图 4 所示。

对木马单一指标变化趋势图进行分析，可以看到各指标的变化曲线存在较大差异，而且一个指标只是反映木马对网络安全威胁的一个侧面，这说明仅仅考虑单一指标显然是不合理的。对木马威胁指数变化趋势图进行分析，从威胁指数的大小来看，在这两周内，威胁指数高于 60 的只有 7 月 6 号一天，威胁指数在 40～60 之间的有 5 天，剩下的 8 天都是在 40 以下，可以认为威胁指数在 0～40 之间为正常现象，在 40～60 之间为低风险，在 60～80 之间为中等风险，在 80～100 之间为高风险；从威胁指数的变化趋势来看，除了 7 月 6 号这个特殊点外，威胁指数整体维持在 30 上下波动。

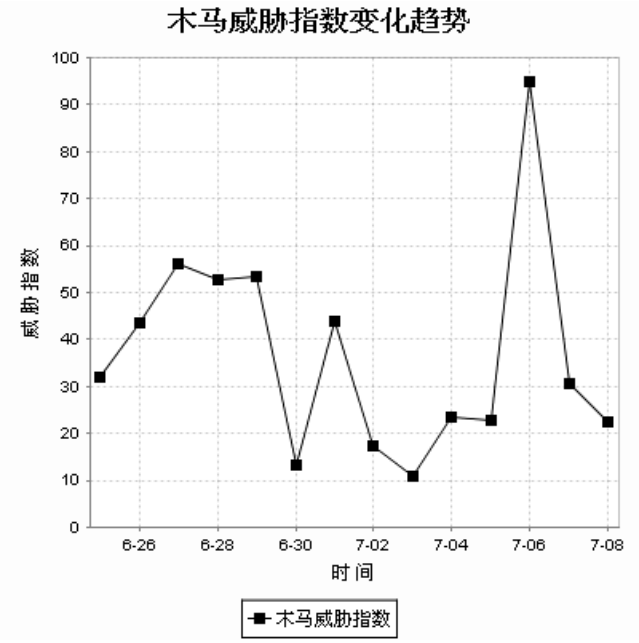


**图 4 木马威胁指数变化趋势图**

以上实验表明：

（1）提出的网络安全威胁量化模型具有合理性，对各种网络安全事件的威胁量化综合考虑了多个因素，且选择了适当的多指标综合方法，得到的威胁指数能直观准确的反映网络安全威胁。

（2）从长时期的威胁指数变化曲线可以发现网络安全威胁的变化规律。

## 6 结论及展望

本文针对大规模网络的宏观特性和复杂性提出了基于攻击特征的网络安全威胁量化模型，实验表明该模型具有合理性，得到的威胁指数能直观准确的反应网络安全威胁，而且从长时期的威胁指数变化曲线还可以发现其变化规律。

下一步的研究重点：（1）研究对网络安全事件进行合理分类，做到不遗漏也不重叠；（2）研究每一种网络安全事件的攻击特征，合理确定其攻击特征指标。

## 致谢

在此，我们向对本文的工作给予支持和建议的专家表示感谢。

## References（参考文献）

[1] CNNIC. 中国互联网络发展状况统计报告[EB/OL]. http://www.cnnic.net.cn/uploadfiles/pdf/2008/7/23/170516.pdfCNNIC. China Internet Development Statistical Report[EB/OL]. http://www.cnnic.net.cn/uploadfiles/pdf/2008/7/23/170516.pdf

[2] CNCERT/CC.2007 年网络安全工作报告[EB/OL].http://www.cert.org.cn/UserFiles/File/CNCERTCC2007AnnualReport_Chinese.pdf.CNCERT/CC. 2007 Network Security Annual Report[EB/OL].http://www.cert.org.cn/UserFiles/File/CNCERTCC2007AnnualReport_Chinese.pdf.

[3] 赵阳，陈运清，范红，等.面向等级保护的大规模网络动态风险评估方法研究[J].信息网络安全,2007,(8):19—21.Zhao Yang, Chen Yunqing, Fan Hong, et al. Research on Dynamic Risk Evaluation Method for Large-scale Network oriented Hierarchy Protection[J]. Netinfo Security, 2007,(8):19—21.

[4] 陈秀真，郑庆华，管晓宏，等.层次化网络安全威胁态势量化评估方法[J]. 软件学报 2006,17(4):885-897.Cheng Xiuzheng, Zheng qinghua, Guan Xiaohong, et al. Quantitative Hierarchical Threat Evaluation Model for Network Security[J]. Journal of Software, 2006,17(14):885-897.

[5] 龙百元，谢东清，万里平.基于近似权重计算的网络安全威胁评估方法[J].计算技术与自动化,2008,27(1):88-91.Long Baiyuan, Xie Dongqing, Wan Liping. Network Security Threat Evaluation Method Based on Approximate Weight Calculation[J]. Computing technology and Automation, 2008,27(1):88-91.

[6] Hariri S, Qu GZ, Dharmagadda T, et al. Impact analysis of faults and attacks in large-scale networks[J]. IEEE Security & Privacy, 2003,1(5):49−54.

[7] 程学东.电信网网络安全评估指标体系研究[J].现代电信科技,2005,(8):10-13.

[8] Cheng Xuedong. Research on Index System of Security Evaluation for Telecom Network[J]. Modern Science & Technology of Telecommunications, 2005, (8):10-13.

[9] 钟霞，钟怀军.多指标综合评价方法及应用[J].内蒙古大学学报,2004,36(4):107-111.Zhong Xia, Zhong Huaijun. Multi-criteria Estimation: Its Application as a Method[J]. Journal of Inner Mongolia University, 2004,36(4):107-111

[10] 杨宇.多指标综合评价中赋权方法评析[J].统计与决策 2006,(13):17-19.Yang Yu. Evaluation of Weight Calculation Method in Multi-criteria Estimation[J] .Statistics and Decision, 2006,(13):17-19.

[11] 赵冬梅，张玉清，马建峰.熵权系数法应用于网络安全的模糊风险评估[J].计算机工程,2004,30(18)：21-23. Zhao Dongmei, Zhang Yuqing, Ma Jianfeng. Fuzzy Risk Assessment of Entropy-weight Coefficient Method Applied in Network Security[J]. Computer Engineering, 2004,30(18)：21-23.