



一种优化的基于 Markov 博弈理论的网络风险评估方法^{*}

刘文芬^{1,2}, 张树伟^{1,2}, 龚心^{1,2}

(1. 信息工程大学 郑州 450001; 2. 数学工程与先进计算国家重点实验室 郑州 450001)

摘要:对网络系统进行安全风险评估,是一种获取并掌握网络信息系统目前及未来安全状态的重要方法,对保障网络安全运行具有重要意义。提出了一种优化的基于 Markov 博弈理论的网络风险评估方法,不同于已有方法单纯地将网络资产的风险状态分为固定类别的方式,该方法依据攻击威胁与修复漏洞的博弈关系得到资产的具体风险情况,刻画更加细致,贴近网络实际;并且将攻击威胁以及漏洞信息进行了归类处理,减小了状态空间,使得模型输入规模大大降低,提高了对大规模网络进行评估的效率。此外,通过引入节点相关性,考虑节点之间风险状况的相互影响,解决了网络安全风险量化过程中普遍存在的忽视网络节点相关性的问题,提高了风险评估的准确性。仿真实验验证了该方法的可行性及有效性。

关键词:网络安全;风险评估;Markov 博弈;弱点漏洞

doi: 10.3969/j.issn.1000-0801.2014.07.003

An Improved Network Risk Evaluation Method Based on Markov Game

Liu Wenfen^{1,2}, Zhang Shuwei^{1,2}, Gong Xin^{1,2}

(1. Information Engineering University, Zhengzhou 450001, China;

2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract: Network security risk assessment is an important means of acquiring and mastering the current and future state of network, which is of great significance to maintain the safe operation of the network. An improved risk assessment method based on Markov game that has simply changed the past was presented, in which the risk status of the network assets were classified into fixed categories. Depending on the game relationship between vulnerabilities fixing and threat attacking, this method has more detailed characterization of the network risk. Network attacks and vulnerabilities were sorted, which reduced the state space, making the scale of model input greatly reduced, improving the assessment of large-scale network efficiency. In addition, the relative importance of the hosts was taken into account to distinguish the contribution of different hosts on the network risk. Simulation results demonstrate the feasibility and effectiveness of this method.

Key words: network security, risk assessment, Markov game, vulnerability

1 引言

随着互联网系统的日趋庞大复杂以及各种新型攻击

手段的不断涌现,网络安全问题受到越来越多的关注,如何快速准确地评估网络风险状况,是解决网络安全问题的基础和前提^[1]。因此,针对网络安全风险评估进行的建模及

^{*} 国家重点基础研究发展计划(“973”计划)基金资助项目(No.2012CB315905, No.2012CB315901)



其中的关键技术研究成为目前网络安全领域的研究热点,如何通过网络安全风险评估降低或者消除各种攻击给网络带来的损失,具有重要的现实意义^[2]。

目前,网络风险量化评估的方法较多,其中代表性的成果有:Gehani^[3]提出了基于主机的实时风险评估;Arnes 等^[4]通过组合主机风险得到网络风险,而主机的不同状态决定了其安全风险,进而利用隐马尔可夫模型描述主机状态变化,就可以实时刻画网络安全风险,但该模型的输入规模过大,计算效率较低而且没有考虑主机之间的相互影响;陈秀真等^[5]通过计算服务、主机以及整个网络系统的威胁指数,提出了一种服务、主机、网络系统的层次化安全威胁态势定量评估模型及量化方法,然而该方法在量化评估算法中,有很多地方都是采用加权分析方法,这使其具有一定的主观性;Leneutre 等^[6]认为入侵检测是一种非合作博弈行为,利用博弈论方法给出了入侵检测系统设计的一些原则和标准;林闯等^[7]提出了采用随机博弈模型的网络攻防实验整体框架,可以对目标网络的攻击成功率、脆弱节点以及潜在攻击路径等方面进行安全分析与评价,但其未对网络整体风险状况给出量化评价结果;方滨兴等^[8]对传统攻击图进行了改进和丰富,提出了用于网络系统安全评估的防御图模型,把网络攻防双方建模为二人非合作博弈模型,并详细地给出了攻防博弈模型的形式化描述,为进行网络风险的量化评估提供了参考。

针对上述评估方法中存在的计算效率低、忽视相邻资产风险关联性等不足,本文提出了一种优化的基于 Markov 博弈模型的量化评估方法,该方法改变了以往将网络资产孤立静态分析的模式,增加了对威胁传播和漏洞修复博弈关系的分析,可以对网络风险状况进行动态分析;对攻击威胁以及漏洞信息进行了归类近似处理,缩小了状态空间,使得模型输入规模大大降低,提高了对大规模网络的评估效率;针对网络安全问题出现的根源、资产弱点的存在,不仅给出了网络风险状况的现状评估,而且还给出了相应的补救措施;考虑节点之间风险状况的相互影响,解决了网络安全风险量化过程中普遍存在的忽视网络节点相关性的问题,提高了风险评估的准确性。

2 相关定义

本文在参考文献[9]的基础上,给出以下定义。

定义 1 (部件)将网络信息系统中的一台计算机设备称为一个网络节点,并将网络节点上的用户、操作系统、应

用程序或服务称为网络节点上的主体,而将网络节点 n 及其上的主体 s 构成的数对 (n,s) 称为节点 n 上的一个部件,记为 C_{ns} 。

定义 2 (网络节点关联性 (network node correlation, NNC)): 如果一个攻击者在成功入侵网络节点 A 之后,利用 A 上的某部件 C_{Ai} 对节点 B 上某部件 C_{Bj} 的访问关系,继续攻击节点 B,那么这种可被利用的访问关系被称为部件 C_{Ai} 到 C_{Bj} 的 NNC。

NNC 在连通性物理关系的基础上,更强调各节点部件间的一种带有权限特性的逻辑关系。根据 NNC 的影响程度可以将其分为 7 类,用集合 $W=\{W_1, \dots, W_7\}$ 表示,用 $\delta(W_j)$ ($1 \leq j \leq 7$) 表示每类 NNC 关系 W_j 的量化值。对于每一类 NNC 的具体量化值,根据不同网络环境、实践经验、主观期望等可以有不同取值。

在网络安全风险评估过程中,通过引入节点的关联性,可以丰富网络节点间的特权访问关系,提高风险评估以及检测网络弱点的准确性。节点间的关联性是基于物理连接关系的特殊逻辑关系,如节点之间存在的一方对另一方系统资源的控制关系、特权访问关系等。在量化网络风险时,考虑具有 NNC 关系的两个节点,若仅有控制方受到攻击,受控方没有遭受任何攻击,那么按照传统网络风险量化方法,整个网络风险变化量只是控制方风险增加的部分,被控方风险没有任何变化。显然,这不符合网络实际情况,因为控制方对被控方有一定的特权访问权限,控制方的风险一定会影响到被控方,使其风险增加。因此,考虑节点的关联性可以更加吻合网络实际状况,提高风险评估的准确性。

3 基于 Markov 博弈理论的风险评估方法

网络安全风险评估是一个系统工程,如图 1 所示,对

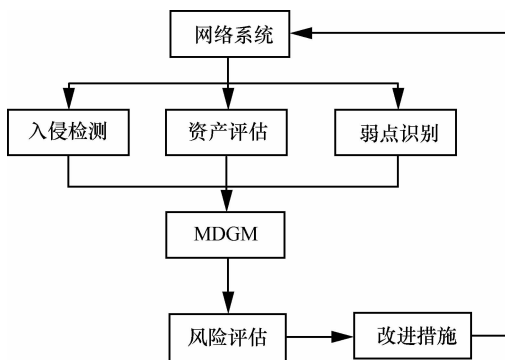


图 1 网络风险评估流程

网络系统进行风险评估,应确保风险分析的内容与范围覆盖整个网络体系。首先,收集网络状态信息,包括网络基本拓扑结构、资产评估、节点漏洞信息等;在掌握网络整体信息之后,依据 Markov 博弈理论建立评估模型;最后,估计网络风险状况,给出相应评价及修复加固措施,优化网络系统结构。

同时,在网络系统的运行过程中,绝对安全的措施是不存在的,实施的安全措施会随着时间而过时,因此网络的风险评估过程是一个动态循环的过程,应对网络安全进行周期性的评估,动态发现网络中存在的主要问题并提出改进方向。

3.1 风险评估框架

资产评估:资产的类型包括主机、服务器、路由器、网关、防火墙等,其价值评估包括资产的类型、资产提供的服务、资产所在主机的性能、资产所在的网络位置等。

弱点识别:脆弱性的类型包括管理配置脆弱性、漏洞等;脆弱性被利用的可能性表示脆弱性被利用的难易程度,在某个资产上,如果检测到某脆弱性,认为该脆弱性以一定的概率被相应威胁成功利用;脆弱性的影响表示该脆弱性引发的安全事件对资产价值的影响。

入侵检测:利用入侵检测系统,发现网络资产中存在的恶意攻击。

MDGM:基于 Markov 博弈理论的风险量化评估模型,第 3.2 节具体介绍。

改进措施:及时发现网络资产的风险变化情况,针对风险较高的重点资产,采取修复弱点等补救措施,降低网络风险。

3.2 基于 Markov 博弈的风险评估模型

本节给出基于 Markov 博弈理论的网络安全风险量化方法。博弈论是关于对智能的决策者之间冲突与合作的数学模型及理论,Markov 决策过程是研究随机环境下多阶段决策过程优化问题的理论工具,Markov 博弈由博弈论和 Markov 决策过程综合而来。本文建立如下风险评估模型。

模型假设如下。

- 同一个资产若存在多种漏洞和威胁,取造成风险值最高的一对漏洞及威胁为代表。
- 同一资产上只有相应的漏洞和威胁同时存在时,风险才会产生。
- 假设攻击者收益即管理员损失,即博弈类型为两人零和博弈。

模型描述如下。

(1) 博弈双方

博弈双方是网络系统中的攻击方和防守方。攻击方以威胁的形式存在,通过威胁传播对系统造成损害;防守方以管理员为代表,通过实施改进方案修复威胁利用的弱点漏洞,切断威胁传播途径,从而提高系统的安全性。

(2) 状态空间

首先,对网络系统中的资产进行编号,假设共有 L 个,即 $1, 2, \dots, L$ 。对于网络系统受到的攻击威胁 Y ,本文参考美国林肯实验室的入侵检测数据库中对攻击种类的划分以及我国反入侵病毒研究中心对攻击危害度的界定,按其威胁指数分为 4 类,见表 1。

表 1 攻击威胁分类

威胁程度	代表性方式	危害指数	符号表示
低	端口扫描	1	y_1
中	拒绝服务攻击	2	y_2
高	FTP 攻击	3	y_3
非常高	缓冲区溢出攻击	4	y_4

另用 y_0 表示资产未受到攻击威胁,危害指数为 0,记为 $Y=\{y_0, y_1, y_2, y_3, y_4\}$ 。对每种攻击威胁进行量化,其取值为相应的危害指数,即 $\rho(y_i)=i, 0 \leq i \leq 4$ 。由模型假设第一种,同一资产在同一时刻取造成风险最高的攻击方式为代表,因此,在时刻 t ,资产 k 受到攻击威胁 $a_k \in Y, 1 \leq k \leq L$ 时的状态记为 $S_k^a(t)$,其取值为 a_k 所对应的危害指数值,即资产 k 在时刻 t 受到攻击威胁的状态集为: $S_k^Y(t)=\{s_k^a(t): a \in Y\}$ 。

那么,整个网络系统在时刻 t 受到所有攻击威胁的状态集为 $S^Y(t): S^Y(t)=\{(s_k^a(t), s_k^a(t), \dots, s_L^a(t)): a_i \in Y, 1 \leq i \leq L\}$ 。

网络资产中存在漏洞 V ,根据漏洞的严重程度来衡量其危害度。美国国家漏洞数据库(National Vulnerability Database Version 2.2)是目前最权威的漏洞信息数据库之一,该数据库从漏洞的利用方式、对信息可用性的影响大小等多方面给出了漏洞严重性的度量,其值为 0~10,因此根据漏洞的危害程度将其分为 11 类,记为 $V=\{v_0, v_1, \dots, v_{10}\}$;相应的量化值为 $\rho(y_j)=j, 0 \leq j \leq 10$ 。资产 k 在时刻 t 存在漏洞 $b_k \in V$ 的状态记为 $S_k^b(t)$,其取值为 b_k 对应的量化值,即资产 k 在时刻 t 存在漏洞的状态集为 $S_k^V(t)=\{s_k^b(t): b \in V\}$ 。

那么,整个网络系统在时刻 t 的漏洞状态集 $S^V(t)$ 为:

$$S^V(t)=\{(s_k^b(t), s_k^b(t), \dots, s_L^b(t)): b_j \in V, 1 \leq j \leq L\} \quad (1)$$

网络风险产生的两个必备条件,一是网络攻击的存



在,二是网络资产自身存在漏洞;同时,由于网络风险的大小与网络攻击的危害程度、漏洞的严重性均成正比,因此定义网络风险大小为攻击危害程度与漏洞严重性量化值的乘积,即资产 k 在时刻 t 的风险状态集为:

$$S_k(t) = \{s_k^{ab}(t) = s_k^a(t) \cdot s_k^b(t) : a \in Y, b \in V\} \quad (2)$$

整个网络系统在时刻 t 的风险状态集 $S(t)$ 为:

$$\begin{aligned} S(t) = & \{(s_1^{a_1}(t) \cdot s_1^{b_1}(t), s_2^{a_2}(t) \cdot s_2^{b_2}(t), \dots, \\ & s_L^{a_L}(t) \cdot s_L^{b_L}(t)) : a_i \in Y, b_i \in V, 1 \leq i \leq L\} \\ \triangleq & \{(s_1^{a_1 b_1}(t), s_2^{a_2 b_2}(t), \dots, s_L^{a_L b_L}(t)) : \\ & a_i \in Y, b_i \in V, 1 \leq i \leq L\} \end{aligned} \quad (3)$$

(3) 行为空间(策略集)

行为空间是博弈双方所有可能的行为集合。在时刻 t , 攻击方的行为是威胁 a 利用某种方式从源资产传播到目的资产的一步传播,用 $Q^a(t)$ 表示,每次只可能传播到当前感染节点的邻居节点;防守方行为是管理员执行加固方案,每次只进行一步操作,修补某个漏洞 b (包括修补脆弱性、切断某条传播路径或关闭某个网络节点),用 $Q^b(t)$ 表示。

(4) 状态转移规则

博弈过程是各方参与者根据系统当前状态从行为空间中选取一个行为,然后系统转移到新的状态,参与者再根据新状态做出决策,以此反复进行。随着博弈各方的行为选择,系统的状态不断变化。网络中任一资产设备 k , 其风险状态的转换概率 p 为:

$$p_k^{ab,uv}(t) = p(s_k^{uv}(t+1) | s_k^{ab}(t), Q_k^a, Q_k^b) \quad (4)$$

其中, $S_k^{ab}(t)$ 表示资产 k 在时刻 t 所处的风险状态, $S_k^{uv}(t+1)$ 表示资产 k 在时刻 $t+1$ 所处的风险状态, Q_k^a 表示资产 k 出现威胁 a 时攻击方采取的策略, Q_k^b 表示管理员在资产 k 上采取针对漏洞 b 的加固策略。

(5) 报酬函数

由模型假设可知,攻击者的报酬大小即网络资产的损失。由于考虑了节点资产之间安全风险的相互影响,即节点的关联性,那么网络资产的损失 $D(S^b(t))$ 主要有两部分:一是直接损失 $D_1(S^b(t))$,由网络资产自身所处风险状态造成的损失大小;二是间接损失 $D_2(S^b(t))$,由存在风险的资产通过 NNC 对邻居节点造成的损失大小。

① 直接损失 $D_1(S^b(t))$ 的计算

由 Markov 博弈可知,采取每一博弈决策后的报酬包括:到下一个决策时刻的一次性收入,持续到下一阶段的累计收入以及转移到下个状态的随机收入等,而且报酬

大小还依赖下一个决策时刻的状态 $S(t+1)$ 。令 $R_k^{ab}(t) = \alpha \sum_{s_k^{uv}(t+1) \in S_k(t+1)} p(s_k^{uv}(t+1) | s_k^{ab}(t), Q^a, Q^b) s_k^{uv}(t+1)$, 表示转移到下个状态的随机损失, α 是衰减因子。记 $S^b(t) = (S_1^b(t), S_2^b(t), \dots, S_L^b(t))$, $R^b(t) = (R_1^b(t), R_2^b(t), \dots, R_L^b(t))$, 因此,在时刻 t 网络资产的直接损失 $D_1(S^b(t))$ 为:

$$D_1(S^b(t)) = A[S^b(t) + R^b(t)] \quad (5)$$

其中, A 是网络资产的价值向量。

② 间接损失 $D_2(S^b(t))$ 的计算

对于网络中的单个资产 k , 其资产价值记为 A_k , 在时刻 t 其风险状态为 $S_k^b(t)$, 其直接资产损失记为 $D_1(S_k^b(t))$ 。由于考虑了节点的关联性,下面计算与资产 k 具有 NNC 关系的邻居节点对其造成的损失大小 $D_2(S_k^b(t))$ 。

下面给出 $D_2(S_k^b(t))$ 的具体计算方法。

步骤 1 确定资产 k 与相邻节点的 NNC。

根据参考文献[9]中节点关联性的发现方法,确定资产 k 与相邻节点之间的 NNC, 数量记为 N' , $N' \geq 1$ ($N'=0$ 时,无需计算 $D_2(S_k^b(t))$), 对应的 N' 个节点简记为 $k_1, k_2, \dots, k_{N'}$ 。

步骤 2 确定每个 NNC 的量化值。

确定资产 k 与每个邻居节点 k_l ($1 \leq l \leq N'$) 的 NNC 关系所属类型 $W_{k_l k}$ 及相应的量化值 $\sigma(W_{k_l k})$ 。

其中,上述确定的每个 NNC 所属类型 $W_{k_l k} \in \{W_1, \dots, W_7\}$; 每个 NNC 的量化值 $\sigma(W_{k_l k})$ 是 7 种 NNC 类别所对应的量化值之一。

步骤 3 计算每个 NNC 对资产 k 损失的影响量。

上述与资产 k 有 NNC 的个节点 $k_1, k_2, \dots, k_{N'}$, 在时刻 t 的风险状态记为 $S_{k_l}^b(t)$, $1 \leq l \leq N'$, 那么,对于这 N' 个 NNC, 其中任意一个对资产 k 的损失影响大小可记作 $\Delta D_{k_l}^b(t)$; 规定 $\Delta D_{k_l}^b(t) = A_k \cdot \sigma(W_{k_l k}) \cdot S_{k_l}^b(t)$, $1 \leq l \leq N'$ 。

步骤 4 确定 $D_2(S^b(t))$ 的取值。

与资产 k 有 NNC 的每个节点都会对主机 k 的风险值产生影响,大小为 $\Delta D(S_{k_l}^b(t))$ 。对于资产损失,自然定义 $\Delta D(S_{k_l}^b(t))$ 中的最大值作为所有节点对资产 k 损失值的影响衡量指标,即:

$$\begin{aligned} D_2(S_k^b(t)) &= \max_{1 \leq l \leq N'} \{\Delta D(S_{k_l}^b(t))\} \\ &= \max_{1 \leq l \leq N'} \{A_k \sigma(W_{k_l k}) S_{k_l}^b(t)\} \end{aligned} \quad (6)$$

综上,整个网络中的资产受到的间接损失 $D_2(S^b(t))$ 的计算式为:

$$D_2(S^b(t)) = \sum_{k=1}^L D_2(S_k^b(t)) \quad (7)$$

③ 整个网络资产损失 $D(S^b(t))$ 的计算

网络资产损失 $D(S^b(t))$ 是直接损失 $D_1(S^b(t))$ 与间接损失 $D_2(S^b(t))$ 之和, 则可得网络资产损失 $D(S^b(t))$ 的计算式, 即报酬函数为:

$$D(S^b(t)) = D_1(S^b(t)) + D_2(S^b(t)) \\ = A[S^b(t) + R^b(t)] + \sum_{k=1}^L D_2(S_k^b(t)) \quad (8)$$

(6) 风险评估

本文定义网络风险即为网络资产损失, 由博弈策略, 管理员依据最小最大化原则, 攻击者依据最大最小化原则分别做出决策。

当管理员要修复弱点漏洞时, 攻击者的目的是要威胁最大, 而管理员要采取措施使风险最小, 则网络系统风险为:

$$D_{\text{net}}(S(t)) = \min_b \max_a D(S^b(t)) \quad (9)$$

当博弈达到均衡点时, 管理员针对漏洞采取的加固措施为:

$$\Psi = \arg \min_b \max_a D(S^b(t)) \quad (10)$$

4 仿真实验

为了阐明提出方法的有效性, 笔者利用办公室小型局域网进行了试验, 具体网络结构如图 2 所示, 其中 A、B、C、D、E 分别代表 5 台办公主机。

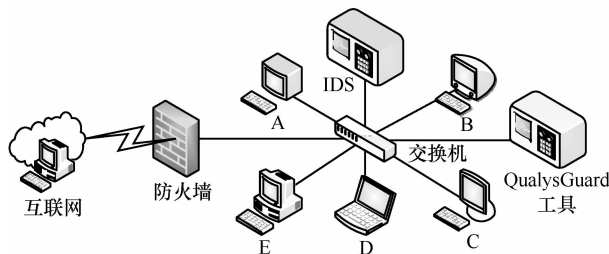


图 2 待评估的网络系统结构

首先, 利用 IDS 检测到网络系统中存在的攻击威胁, 发现主机 A 上存在 FTP 攻击, D 受到端口扫描, E 也受到端口扫描。主机 A 上存在的 FTP 具有高危害指数, 威胁指数为 3; 主机 D、E 上的端口扫描攻击威胁指数为 1。然后, 利用 QualysGuard 扫描到主机 A 以及 D 存在 FTP 漏洞, 主机 E 开有 23 及 80 端口。因此, 由所建模型方法可知, 上述整个网络系统在起始时刻 0 时的风险状态集 $S(0)$ 为: $S(0) = (6, 0, 0, 6, 1)$ 。另外, 对于上述网络实例中 5 台主机资产分别记为 1、2、3、4、5。由于同一漏洞在不同攻击者实际的利用上存在差异, 管理员修补措施的具体实现上同样存在区

别, 因此在此仿真实验中简单假定资产任一风险状态转换到下一状态的概率为 0.25, 模型中的衰减因子为 0.8; 根据参考文献[9]中 NNC 发现的规则, 得到局域网中具有 NNC 的节点及 NNC 量化权值, 计算间接风险值; 最终, 可得到局域网的风险大小为 72.659, 同时为说明本文方法的优势, 与参考文献[10]方法 TM(traditional method)对比, 得到如图 3 所示的结果。

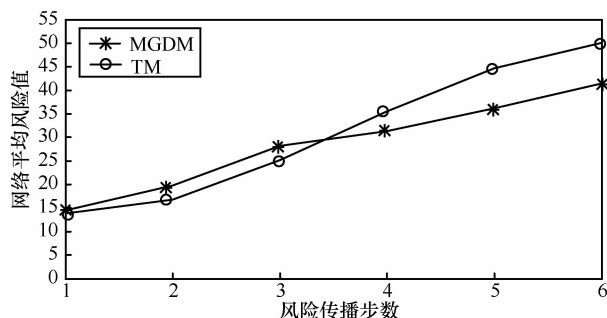


图 3 两种模型对比

由上述仿真实验看出, 图 3 中在第 2 步、第 3 步时本文模型计算的网路平均风险值要高于方法 TM, 原因在于考虑了节点的关联性, 计算了相邻节点间风险的影响部分, 可以更加充分地挖掘网络的潜在风险, 反映网络实际风险状况; 在第 4 步、第 5 步时, 本文模型方法得出的网络风险值较低, 原因在于本文方法可以及时提供修复加固措施, 管理员在每一个决策时刻改进防御策略, 可以适当降低一部分网络风险, 减小网络资产损失。

5 结束语

本文在基于 Markov 博弈模型风险评估方法的基础上, 将攻击威胁以及漏洞信息进行了归类近似处理, 减小了状态空间, 同时使得模型输入规模大大降低, 提高了对大规模网络进行评估的效率; 针对网络安全问题出现的根源、资产弱点的存在, 给出了网络风险状况的现状评估, 刻画更加真实且贴近风险根源, 而且还给出了相应的加固措施; 考虑节点之间风险状况的相互影响, 解决了网络安全风险量化过程中普遍存在的忽视网络节点相关性的问题, 提高了风险评估的准确性。

参考文献

- Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 2011, 9(2): 50-57
- 刘刚, 李千目, 张宏. 信度向量正交投影分解的网络安全风险评估方法. 电子与信息学报, 2012, 34(8): 1934-1938

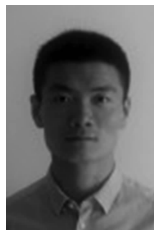


- 3 Gehani A, Kedem G. Rheostat: real time risk management. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection, French Riviera, France, 2004: 296~314
- 4 Arnes A, Valeur F, Vigna G, *et al.* Using hidden markov models to evaluate the risks of intrusions. Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection, Hamburg, Germany, 2006: 145~164
- 5 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. 软件学报, 2006, 17(4): 885~897
- 6 Chen L, Leneutre J. A game theoretical framework on intrusion detection in heterogeneous networks. IEEE Transactions on Information Forensics and Security, 2009, 4(2): 165~178
- 7 王元卓, 林闯, 程学旗等. 基于随机博弈模型的网络攻防量化分析方法. 计算机学报, 2010, 33(9)
- 8 姜伟, 方滨兴, 田志宏等. 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
- 9 张永铮, 方滨兴, 迟悦等. 网络风险评估中网络节点关联性的研究. 计算机学报, 2007, 30(2): 234~240
- 10 Cui X L, Tan X B, Zhang Y, *et al.* A markov game theory-based risk assessment model for network information system. Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Wuhan, China, 2008: 1057~1061

[作者简介]



刘文芬,女,博士,信息工程大学教授、博士生导师,主要研究方向为概率统计在通信和密码学中的应用。



张树伟,男,信息工程大学硕士生,主要研究方向为网络风险安全度量。



龚心,男,信息工程大学硕士生,主要研究方向为密码学中的逻辑函数。

(收稿日期:2014-06-22)

·简讯·

2014年5月通信业主要指标完成情况(一)

指标名称	单位	本年本月止累计到达	比上年同期累计(±%)	本月
电信营业收入	亿元	5 734.7	6.8	1 195.3
其中:电信主营业务收入	亿元	4 978.9	6.9	1 052.2
电信固定资产投资完成额	亿元	906.5	9.7	253.9
固定本地电话通话时长合计	万分钟	10 949 451.3	-14.0	2 284 768.9
区间电话通话时长	万分钟	1 089 408.5	-17.9	227 977.3
区内电话及拨号上网通话时长	万分钟	9 860 042.8	-13.5	2 056 791.6
固定长途电话通话时长合计	万分钟	2 204 744.4	-9.6	462 619.9
国内长途电话通话时长	万分钟	2 162 153.5	-9.1	453 952.7
国际电话通话时长	万分钟	24 875.3	-32.0	4 986.6
港澳台电话通话时长	万分钟	17 715.5	-23.2	3 680.6
移动电话通话时长合计(含本地)	万分钟	121 352 372.7	2.3	25 505 508.6
移动电话国内长途通话时长	万分钟	28 121 928.9	3.8	6 018 784.2
移动电话国际电话通话时长	万分钟	53 792.6	5.5	11 173.8
移动电话港澳台电话通话时长	万分钟	38 466.9	-4.4	7 717.2
移动短信业务量	万条	31 463 457.1	-18.4	6 377 028.2
移动互联网接入流量	万 GB	70 661.7	52.0	15 564.3

注:(1)收入增长率按可比口径计算。(2)固定长途电话通话时长和移动电话通话时长均包含相应的 IP 电话通话时长。(3)通话时长各项指标均为去话通话时长。

(来源:工业和信息化部运行监测协调局)