计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
47(10): 1714-1723, 2010

基于攻防随机博弈模型的防御策略选取研究

姜 伟[1,2] 方滨兴[1] 田志宏[1] 张宏莉[1]
[1](哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001)
[2](北京工业大学计算机学院 北京 100124)
(jiangwei@pact518.hit.edu.cn)

Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model

Jiang Wei[1,2], Fang Binxing[1], Tian Zhihong[1], and Zhang Hongli[1]
[1](*School of Computer Science and Technology, Harbin Institute of Technology, Harbin* 150001)
[2](*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100124)

Abstract The defender needs to predict, detect and understand attacks, and makes good decisions about defense strategies. Because the target of attackers and defenders is oppositional and their strategies are interdependent, the selection of optimal defense strategy is a complex issue. In this paper, the issue of optimal defense strategy selection is defined and formalized. A new attack-defense stochastic game model is proposed to describe the offensive and defensive conflict of attackers and defenders in network security and address the issue of optimal defense strategy selection. The model is a dynamic multi-player and multi-state model which is expanded by normal attack-defense game and Markov decision process. By viewing privilege state in node of attacker as elements in attack-defense stochastic game, we can model the dynamic transition of attack and defense state and compute the probabilities of attacker and defender behavior. This paper analyzes the cost factors related to attack and defense and provides a cost-benefit analysis method that helps defender evaluate and select defense strategies. An algorithm for defense strategy selection based on those models is proposed. A representative network example is provided to illustrate our models and demonstrate the efficacy of our models in the prediction of attack behaviors and decision of optimal defense strategies.

Key words Internet security; active defense; policy selection; attack-defense stochastic game model; privilege elevation

摘 要 由于网络安全攻防双方的目标对立性和策略依存性,使得最优防御策略选取问题十分复杂.形式化定义了网络安全防御策略选取问题.提出了一种刻画网络安全攻防矛盾,解决防御策略选取问题的攻防随机博弈模型.该模型是矩阵型攻防博弈模型和 Markov 决策过程的扩展,是多人、多状态的动态攻防推演模型.将攻击者在网络实体上的特权状态作为攻防随机博弈模型的元素,建模网络攻防状态的动态变化,并预测攻击行为和决策最优防御策略.给出了基于上述模型的防御策略选取算法.用一个网络实例分析了该模型和算法在攻击策略预测和防御策略决策方面的有效性.

收稿日期:2009-01-06;**修回日期**:2010-04-02
基金项目:国家"九七三"重点基础研究发展计划基金项目(2007CB311100);国家自然科学基金项目(60903166);国家"八六三"高技术研究发展计划基金项目(2009AA01Z437)

关键词　网络安全;主动防御;策略选取;攻防随机博弈;特权提升

中图法分类号　TP309

0　引　　言

现在的计算机网络信息系统一般建立于多平台,运行着多种软件并支持多种连通模式,必然存在一些安全弱点和错误.同时网络攻击方式也呈现多样化、智能化、综合化的发展趋势.由于资源和能力的限制,管理员不可能消除每一个弱点,也不可能防御所有的攻击.如何在信息安全风险和投入之间寻求一种均衡,利用有限的资源作出最合理的决策一直困扰着信息安全的防守方.

当前网络安全挑战和突破口是研究新的合理的攻击和防护模型[1].为了更好地理解信息安全攻防对抗本质,本文用一个数学的框架模型描述信息安全攻防之间的矛盾冲突问题,解决攻击行为预测和最优防御策略选取问题.信息安全中攻防对抗的本质特征是攻防双方的目标对立性、关系非合作性、策略依存性,而这些特征正是博弈论[2]的基本特征.在网络攻防环境下,攻击者的总是希望通过破坏目标实体组件的功能或服务质量来获得最大化收益.防御者总是希望把系统的损害降为最少.将博弈论的思想应用到网络攻击和防御中,为解决网络信息安全攻防矛盾及其最优防御决策等难题研究提供了一种新的思路.

目前,有关攻防成本定量分析、主动防御、博弈论在网络安全领域的研究工作取得了一些研究成果,但还处于起步阶段,尚未形成系统化的理论方法,需要进一步深入研究.

文献[3]首次提出了成本敏感模型作为响应决策的基础,根据响应成本和攻击损失来决定是否响应.响应决策思想和各种成本的量化比较简单,但其代价量化、代价分类和攻击分类的思想和方法对本文的研究内容有一定的借鉴意义.文献[4]给出了比较完整的攻防分类及其成本敏感模型,有效地应用于主动防御中.文献[5]提出了一种基于攻击图的网络最小代价加固方法.文献[6]提出了脆弱性利用成本估算模型,对网络系统的脆弱性进行量化评估,为管理员在权衡修复成本和效果时提供参考.文献[7]提出利用随机博弈来对网络中的正常节点和恶意节点进行理性分析的思想.文献[8]利用不完全信息的重复博弈对信息战中参战双方的行为建模.文献[9]利用博弈论分析了攻击者和管理员关系和纳什均衡策略,但是在攻防收益函数量化方面比较简单.文献[10]提出了基于博弈理论的入侵意图、目标和策略推理模型.针对理性攻击者我们提出了一种静态矩阵型攻防博弈模型,将攻防双方建模为二人非合作博弈[4],从而构建一套基于防御图模型的风险评估和基于静态矩阵型攻防博弈模型的主动防御框架.在文献[11]中进一步提出了基于 Markov 特权链的攻防随机模型,但是比较简单.文献[12]在量化安全随机模型时利用博弈理论建模和计算攻击概率.文献[13]提出了一种基于博弈理论的动态入侵响应 DIRBGT 模型,有效提高了报警响应的准确性和效果.

1　防御策略选取问题形式化描述

在网络安全管理中,防御策略能够减少攻击风险和攻击损失,同时增加了防御成本,两者之间如何权衡,如何选取最优防御策略一直困扰着防御者.防御策略的选取不仅考虑防御成本,更要考虑网络资产关键度和可能发生的攻击.针对单个攻击,防御决策只需要选择综合防御代价最小的策略.而在多步攻击和多个攻击动作的情况下,有的防御策略可能对某个攻击动作有效,对其他攻击动作无效,这就需要考虑防御策略对特定攻击的有效性、防御操作成本、防御负面影响等因素.另外每个攻击策略的发生概率是未知的.如何保证防御策略最优,使得期望综合防御代价最低,这是一个十分复杂的问题.

根据以上分析,将防御策略选取问题定义为一个函数 $f_{\text{selection}}:(C,A,D,G)\rightarrow D'$,其中各个元素含义如下.

C:被保护的网络信息系统实体组件集合.实体组件 $c\in C$ 可以是主机、路由器、防火墙等资产,每一个实体组件由软件、硬件、数据和服务等一部分或多部分组成.如运行着 Http 服务的 Web 服务器等.

A:可能的攻击、正在发生和即将发生的攻击信息集合.对于网络实体组件 $c\in C$,c 存在弱点可能被攻击者利用,需要对这些可能的攻击、正在发生和即将发生的攻击 $a\in A$ 进行识别,从而对 C 进行防护.

D:防御系统可采用的防御策略集合(不采取防御措施 ϕ 也是一种策略,即 $\phi\in D$).如针对 Ftp

Buffer overflow 弱点的攻击,防御策略 $d=$(关闭 Ftp 服务),且 $d\in D$.

G:攻防博弈模型集合. 如矩阵型攻防博弈 ADG[4]、下面介绍的攻防随机博弈模型 ADSG 等,可以根据具体的网络攻防环境,选择合适的网络攻防博弈模型.

D':选取的最优防御策略集合,且 $D'\subseteq D$.

$f_{\text{selection}}$是一个从(C,A,D,G)到最优防御策略D'的映射,对于任意 i,j,有$(C_i,A_i,D_i,G_i)\rightarrow D'_i$,$(C_j,A_j,D_j,G_j)\rightarrow D'_j$,若$(C_i,A_i,D_i,G_i)=(C_j,A_j,D_j,G_j)$,则必有 $D'_i=D'_j$. 给定网络信息系统实体组件集合 C,通过脆弱性分析和入侵检测机制确定攻击信息集合 A,然后对 A 和 C 分析确定防御策略集合 D,根据网络攻防和需求情况选取合适的网络攻防博弈模型 G,通过 A,C 和 D 等相关信息构建攻防博弈模型 G. 本文将对给定的(C,A,D,G)信息,研究基于攻防随机博弈模型的最优防御策略选取函数的构造和求解.

2 攻防随机博弈模型

随机博弈[14]可以看作是一个在各个局中人的联合行动下,使得博弈系统从一个状态转移到另一个状态的状态机. 网络系统同样可以看作是一个状态机,攻防双方以目标冲突的联合行动使得系统状态转移. 攻击者的目标是对网络系统的安全属性进行破坏,防御者阻止攻击者进行安全属性损害. 系统状态变化不确定,以概率的方式从一个状态转移到另一个状态. 所以用随机博弈模型来刻画网络攻防冲突问题是合理的. 下面给出攻防双方在多个攻防状态下动态寻找最优攻防策略的攻防随机博弈模型.

2.1 攻防随机博弈模型

定义 1. 攻防随机博弈模型(attack-defense stochastic game, ADSG)是一个七元组 $ADSG=(N,S,A,D,P,U_a,U_d)$,其中:

① $N=\{\text{Attacker},\text{Defender}\}$是参加攻防博弈的局中人集合. 若攻击者的数量$\geqslant 2$,则表示分布式协同攻击;若防御者的数量$\geqslant 2$,则表示多个防御者协同防御,在本文中,仅考虑 $n=2$ 情况,一个攻击者和防御者,其他情况可以将多个攻击者和防御者进行合并看作是单个攻击者和防御者;

② $S=\{S_1,S_2,\cdots,S_K\}$是攻防随机博弈状态集合;

③ $A=\{a_1,a_2,\cdots,a_M\}$攻击者动作集合,攻击者在博弈状态 S_k 的攻击动作集合 $A_k\subset A$,且 $\bigcup_{k=1}^{K}A_k=A$;

④ $D=\{d_1,d_2,\cdots,d_N\}$防御动作集合,防御者在博弈状态 S_k 的防御动作集合 $D_k\subset D$,且 $\bigcup_{k=1}^{K}D_k=D$;

⑤ $P:S\times A\times D\times S\rightarrow[0,1]$是攻防随机博弈状态转移概率函数;

⑥ $U_k:S\times A\times D\times S\rightarrow\Re$,$k=a_i,d_j$ 局中人的收益函数集合(utility function),其中 $\Re$ 是收益值. 收益函数表达了攻防双方从博弈中能够得到的收益水平,它是所有局中人策略的函数. 攻防双方的收益关系可分为零和(Zero-sum)与非零和(Nonzero-sum). 如果攻防双方的收益 U_a 和 U_d 满足 $U_a+U_d=0$,称为零和攻防博弈. $U_a+U_d\neq 0$,称为非零和攻防博弈. 根据不同的网络环境和攻防情景选择零和或非零和博弈模型.

在网络攻防博弈的过程中,双方不会事先将策略决策信息告知对方或达成一致协议,攻击者和防御者之间的关系都是都是非合作的、对抗性的. 所以上述模型是一个非合作攻防随机博弈模型.

2.1.1 攻防随机博弈状态

本文将网络安全状态作为攻防随机博弈状态集. 网络安全状态表达了网络实体组件的软硬件资源属性、连接性和用户或攻击者对整个网络的访问能力. 安全状态的状态变化由攻防动作对(a_i,d_j)引起,可以表现为文件修改、系统配置改变、可执行程序运行、攻击者的特权提升等. 攻防随机博弈状态可以用一个有向图 $G=(S,E)$来表示,S 是图的节点集,每一个节点表示一种博弈状态,E 是边集,表示攻防随机博弈状态转换关系. 以图 1 为例说明博弈状态及其转换关系. 图 1 表示具有 3 个博弈状态 $S=\{S_1,S_2,S_3\}$的状态图. 图中状态相互可以转换,但是在一些具体的网络环境,不是所有状态可以相互转

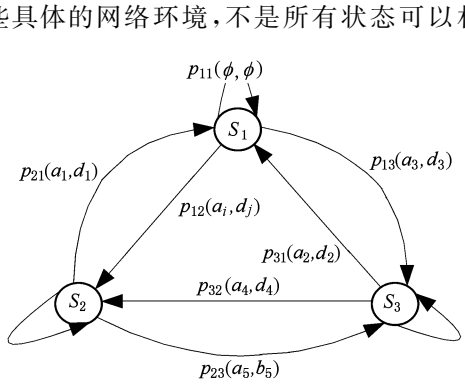


Fig. 1 Example of ADSG's state.

图 1 攻防随机博弈状态实例

换.图中状态之间标注 $p_{12}(a_i,d_j)$ 表示在攻防策略对 (a_i,d_j) 作用下博弈状态从状态 1 到状态 2 的转移概率.后面实例分析将给出攻防随机博弈状态图具体的描述.

2.1.2　状态转移概率函数

由于博弈状态转移是由攻防动作引起的,具有随机性,可以用概率来描述状态转移的可能性大小.如果信息系统有 n 个安全状态,可以用一个状态转移矩阵 $\boldsymbol{P}$ 来表示各个安全状态之间的状态转移概率:

$$\boldsymbol{P}=\begin{pmatrix} p_{11}(a_1,d_1) & p_{12}(a_1,d_2) & \cdots & p_{1n}(a_1,d_n) \\ p_{21}(a_2,d_1) & p_{22}(a_2,d_2) & \cdots & p_{2n}(a_2,d_n) \\ \vdots & \vdots & & \vdots \\ p_{n1}(a_n,d_1) & p_{n2}(a_n,d_2) & \cdots & p_{m}(a_n,d_n) \end{pmatrix}, \tag{1}$$

其中矩阵元素 $p_{ij}(a_i,d_j)$ 表示攻防博弈系统在攻防动作对 (a_i,d_j) 作用下从状态 i 转移到状态 j 的概率.由于攻击者是理性的,攻击的原则是以最快、最易、最省达到攻击目的,所以攻击动作具有规律性.状态转移概率可以根据历史数据、统计、模拟结果和专家知识并结合特定的信息系统环境来确定.

2.1.3　攻防策略及其收益量化

定义 2. 攻防策略.在博弈状态 S_k,攻击者或防御者采取动作的规则称为该状态下的攻防策略.用向量 $\boldsymbol{\pi}_k^{\mathrm{a}}=(\pi_k^{\mathrm{a}}(a_1),\pi_k^{\mathrm{a}}(a_2),\cdots,\pi_k^{\mathrm{a}}(a_i))$,$\boldsymbol{\pi}_k^{\mathrm{d}}=(\pi_k^{\mathrm{d}}(d_1),\pi_k^{\mathrm{d}}(d_2),\cdots,\pi_k^{\mathrm{d}}(d_j))$ 来表示攻击策略和防御策略,其中 $k=1,\cdots,K$,$a_i\in A_k$,$d_j\in D_k$.A_k,D_k 分别是攻防双方在博弈状态 S_k 所有可采用的攻防动作(包括不采取动作 ϕ)集合,且 $A_k\subset A$,$D_k\subset D$.攻防策略为 $\pi_k^{\mathrm{a}}(a_i)$ 表示在状态 S_k 攻击者选取攻击动作 a_i 的概率,$\pi_k^{\mathrm{d}}(d_j)$ 表示在状态 S_k 防御者选取防御动作 d_j 的概率.$\forall k,a_i\in A,d_j\in D,0\leqslant\pi_k^{\mathrm{a}}(a_i)\leqslant 1,0\leqslant\pi_k^{\mathrm{d}}(d_j)\leqslant 1,\sum\limits_{\forall a_i}\pi_k^{\mathrm{a}}(a_i)=1,\sum\limits_{\forall d_j}\pi_k^{\mathrm{d}}(d_j)=1$.攻击者和防御者以概率的形式选取可用的攻防动作,所以攻防策略有时也称为混合策略或随机策略.如果 $\pi_k^{\mathrm{a}}(a_i)=1,\forall i\neq j,\pi_k^{\mathrm{a}}(a_j)=0$,则称攻击策略 $\boldsymbol{\pi}_k^{\mathrm{a}}=(\pi_k^{\mathrm{a}}(a_1),\pi_k^{\mathrm{a}}(a_2),\cdots,\pi_k^{\mathrm{a}}(a_i))$ 是纯策略,$\boldsymbol{\pi}_k^{\mathrm{d}}=(\pi_k^{\mathrm{d}}(d_1),\pi_k^{\mathrm{d}}(d_2),\cdots,\pi_k^{\mathrm{d}}(d_j))$ 同理.可见,纯策略是混合策略的特殊情况.如果攻防策略向量 π_i 在所有状态下独立于时间和历史,则称为稳定攻防策略,本文仅考虑稳定攻防策略.

定义 3. 攻防纳什均衡(Nash equilibrium[2]).给定一个攻防随机博弈 $ADSG=(N,S,A,D,P,U_{\mathrm{a}},U_{\mathrm{d}})$,对于任意 $k=1,\cdots,K$,在博弈状态 S_k,攻防双方的混合策略分别是 $\boldsymbol{\pi}_k^{\mathrm{a}}=(\pi_k^{\mathrm{a}}(a_1),\pi_k^{\mathrm{a}}(a_2),\cdots,\pi_k^{\mathrm{a}}(a_i))$,$\boldsymbol{\pi}_k^{\mathrm{d}}=(\pi_k^{\mathrm{d}}(d_1),\pi_k^{\mathrm{d}}(d_2),\cdots,\pi_k^{\mathrm{d}}(d_j))$.稳定混合策略 $(\pi_i^{\mathrm{a}^*},\pi_i^{\mathrm{d}^*})$ 是一个纳什均衡,当且仅当该混合策略是攻防双方的最优响应策略,即满足:对于 $\forall\pi_i^{\mathrm{a}},v_{\mathrm{a}}(\pi_i^{\mathrm{a}^*},\pi_i^{\mathrm{d}^*})\geqslant v_{\mathrm{a}}(\pi_i^{\mathrm{a}},\pi_i^{\mathrm{d}^*})$;对于 $\forall\pi_i^{\mathrm{d}},v_{\mathrm{d}}(\pi_i^{\mathrm{a}^*},\pi_i^{\mathrm{d}^*})\geqslant v_{\mathrm{d}}(\pi_i^{\mathrm{a}},\pi_i^{\mathrm{d}})$.这里 $v_k(\pi_i^{\mathrm{a}},\pi_i^{\mathrm{d}}),k=a_i,d_j$ 表示攻击者和防御者分别采用稳定策略 $\pi_i^{\mathrm{a}},\pi_i^{\mathrm{d}}$ 时参与者 k 的收益期望值.

纳什均衡 $(\pi_i^{\mathrm{a}^*},\pi_i^{\mathrm{d}^*})$ 是攻防双方在攻防博弈状态 S_i 下的最优攻防策略,攻防双方只有采取纳什均衡策略才能最大化其收益.整个攻防随机博弈的纳什均衡,即最优攻击策略集可以表示为 $\pi^{\mathrm{a}^*}=\{\pi_1^{\mathrm{a}^*},\pi_2^{\mathrm{a}^*},\cdots,\pi_K^{\mathrm{a}^*}\}$,最优攻击策略集可以表示为 $\pi^{\mathrm{d}^*}=\{\pi_1^{\mathrm{d}^*},\pi_2^{\mathrm{d}^*},\cdots,\pi_K^{\mathrm{d}^*}\}$.

定理 1. 纳什均衡存在性.给定一个零和攻防随机博弈 $ADSG=(N,S,A,D,P,U_{\mathrm{a}},U_{\mathrm{d}})$,如果博弈状态集 S,攻防动作集 A,D 是有限集合,则存在一个稳定纳什均衡.

证明.因为攻防随机博弈模型是矩阵型攻防模型扩展到多个状态而得到的,在某一个状态 k 下,博弈状态 S_k 是一个矩阵型攻防博弈.又因为博弈状态集 S,攻防动作集 A,D,收益值 $U_{\mathrm{a}},U_{\mathrm{b}}$ 都是有限的,所以 $ADSG=(N,S,A,D,P,U_{\mathrm{a}},U_{\mathrm{d}})$ 是一个有限随机博弈.Fink[15] 给出了每一个有限随机博弈都存在一个稳定纳什均衡的结论.所以上述零和攻防随机博弈存在一个稳定纳什均衡.

因为攻防随机博弈模型是矩阵型攻防模型和 Markov 决策过程的整合和扩展,所以在某一个状态 k 下,攻击者动作集合为 $A_k=(a_1,a_2,\cdots,a_m)$,防御者动作集合 $D_k=(d_1,d_2,\cdots,d_n)$.博弈状态 S_k 可以看作是一个矩阵型攻防博弈,用一个 $m\times n$ 矩阵 $\boldsymbol{S}_k$ 来表示[14],矩阵元素为

$$s_{ij}^k=u_{ij}^k+\sum_{l=1}^{K}p_{ij}^{kl}(a_i,d_j)\boldsymbol{S}_l, \tag{2}$$

其中,$p_{ij}^{kl}(a_i,d_j)\geqslant 0$,$l=1,\cdots,K$,$i=1,\cdots,m$,$j=1,\cdots,n$;$\forall k,i,j,\sum\limits_{l=1}^{K}p_{ij}^{kl}(a_i,d_j)<1$.攻击者可能选取的攻击动作用矩阵中每一行来表示,防御者选取矩阵中每一列作为其防御动作.攻防双方的目标是最大化其收益,矩阵元素是攻防双方的收益和损

失.u_{ij}^k为攻击者采取攻击动作a_i的直接攻击收益AR,$\sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)\boldsymbol{S}_l$为间接收益.可见,攻击收益不仅与攻击动作有关,而且和当前状态有关.式(2)表示为在博弈状态S_k,如果攻击者选取行纯策略a_i、防御者选取列纯策略d_j进行博弈,则防御者支付给攻击者收益为$u_{ij}^k+\sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)\boldsymbol{S}_l$,博弈状态以概率$p_{ij}^{kl}(a_i,d_j)$从$S_k$到$S_l$,博弈系统终止的概率是$1-\sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)$或博弈系统终止于没有其他状态可以转移.

定理 2. 攻防博弈值存在性[14].给定一个攻防随机博弈$ADSG=(N,S,A,D,P,U_a,U_d)$,对于任意$k=1,\cdots,K$,博弈状态S_k的值v_k一定是式(3)的唯一解:

$$v_k = Val(\boldsymbol{S}_k), \tag{3}$$

其中$Val(\boldsymbol{S}_k)$是矩阵型博弈$\boldsymbol{S}_k$的值,矩阵$\boldsymbol{S}_k$的元素为

$$s_{ij}^k = u_{ij}^k + \sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)v_l. \tag{4}$$

文献[14]给出了随机博弈值的存在性证明,这里不再证明.

由于目标实体组件的重要程度是随着网络环境的不同而变化,而且各类攻击的固有危害也是不尽相同.所以攻击造成的损失不仅与攻击的类型有关,而且与攻击的目标有关.攻防收益和系统损失的量化可以结合攻击类型及其攻击目标进行计算.在文献[4]中,我们给出了比较完整的攻击分类和成本量化,将攻击动作分为6类,并结合攻击分类和主动防御的时空特点,将防御策略分为基于主机和基于网络的两大类,其中每一种防御分类包括若干个子类.这里不再赘述.结合前期工作的攻防成本、收益量化模型[4],给出攻防随机博弈模型的攻防成本量化方法.

定义 4. 防御有效率.对于攻击a,采用防御策略d的有效性,用$\varepsilon(a_i,d_j)$表示.当完全阻止攻击时,$\varepsilon(a_i,d_j)=1$,无效时,$\varepsilon(a_i,d_j)=0$,其他情况时$0<\varepsilon(a_i,d_j)<1$.

定义 5. 防御成本(DC).防御策略的操作代价、负面代价之和称为防御成本.即

$$DC(d) = Ocost(d) + Acost \times r(a_i,d_j), \tag{5}$$

其中,$Ocost(d)$和$Acost$分别表示操作代价、负面代价.

定义 6. 攻击收益(AR).攻击者发动一次成功攻击所得到的好处称为攻击收益.

$$AR = (1-\varepsilon)Dcost(a) + DC(d) - AC(a), \tag{6}$$

其中,$Dcost(a)$是系统损失代价,表示攻击a造成的系统损失,$DC(d)$是防御者采用防御动作d的防御成本,$AC(a)$是攻击成本,表示攻击者发动攻击a的所需要的成本.

定义 7. 防御收益(DR).表示防御者采取防御策略d后,网络系统免受的损失,也包括防御成本、攻击成本.

$$DR = AC(a) - (1-\varepsilon)Dcost(a) - DC(d), \tag{7}$$

这里,$AR+DR=0$,即零和攻防随机博弈.模型中的攻防双方由于他们的目标和利益对立,收益函数可能不同.但是考虑到攻防双方收益是互补的,即攻击者的收益即为防御者损失,所以本文选择零和攻防博弈是合理的.

3 基于攻防随机博弈模型的防御策略选取算法

3.1 算法描述

给定(C,A,D,G),其中$G=ADSG=(N,S,A,D,P,U_a,U_d)$,下面介绍最优防御策略$D'$的选取算法.由于攻防随机博弈有多个状态,求解式(2)比较复杂,可以使用 Shapley 迭代方法[14]来求解攻防随机博弈的值$\boldsymbol{v}=(v_1,v_2,\cdots,v_K)$及其最优攻防策略.首先任意初始$\boldsymbol{v}_0=(v_0(1),v_0(2),\cdots,v_0(K))$,用迭代公式$v_k^{r+1}=Val(u_{ij}^k+\sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)v_l^r)$迭代求解,直到满足$|v_k^{r+1}-v_k^r|<\delta$,$\delta$为精确度.最后得到值向量为$\boldsymbol{v}=(v_1,v_2,\cdots,v_K)$,对于任意$k=1,2,\cdots,K$,利用式(4)构建矩阵型博弈矩阵$\boldsymbol{S}_k$,求解$\boldsymbol{S}_k$得到攻防双方的最优策略$(\pi_k^a,\pi_k^d)$.本文参考文献[12]给出基于攻防随机博弈模型的攻防策略选取算法.

算法 1. 基于攻防随机博弈模型的防御策略选取算法.

输入:(C,A,D,G)和δ;

输出:最优攻防策略D'.

① 由C,A,D构建攻防随机博弈$G=ADSG$;

② 任意初始向量$\boldsymbol{v}^0=(v^0(1),v^0(2),\cdots,v^0(K))$;

③ Repeat

④　for 每一个博弈状态 $\boldsymbol{S}_k \in S$ do

⑤　for all s_{ij}^k do

⑥　　用 v_l 代替式(2)中的 $\boldsymbol{S}_l$;

⑦　end for

⑧　　计算 $v_k^{r+1}=Val(u_{ij}^k+\sum_{l=1}^{K} p_{ij}^{kl}(a_i,d_j)v_l^r)$;

⑨　end for

⑩　for 每一个博弈状态 $\boldsymbol{S}_k \in S$ do

⑪　　$v_k \leftarrow Val(\boldsymbol{S}_k)$;

⑫　end for

⑬ until $|v_k^{r+1}-v_k^r|<\delta, \forall \boldsymbol{S}_k \in S$

⑭ for 每一个博弈状态 $\boldsymbol{S}_k \in S$ do

⑮　　$(\pi_k^a,\pi_k^d)=Solve(\boldsymbol{S}_k)$;

⑯　end for

⑰ return $D'=\{\pi_k^d\}$.

3.2　算法复杂性分析

该算法的关键是攻防随机博弈模型的求解,整个算法的时间复杂度主要取决于迭代求值过程和 $Solve(\boldsymbol{S}_k)$. 由定理 1 和定理 2 可知,算法 1 的迭代求解攻防随机博弈值最终收敛,其时间复杂度与防御者输入精度参数 δ 相关. δ 的值可以根据迭代计算精度和计算时间来设置. $Solve(\boldsymbol{S}_k)$ 是计算矩阵型博弈纳什均衡,利用线性规划求解矩阵型攻防博弈混合攻防策略的时间复杂度是 $O(n^2)$[16].

4　实例分析

本文假定有如图 2 所示的典型的网络信息系统拓扑结构,攻击主机位于外部网络,被保护的网络信息系统实体组件集合 $C=\{$Attacker Host, Smtp Server, Ftp Server, Data Server$\}$. 防火墙将目标网络与外部网络分开,防火墙规则及连接信息如表 1 所示. 目标系统弱点信息如表 2 所示.

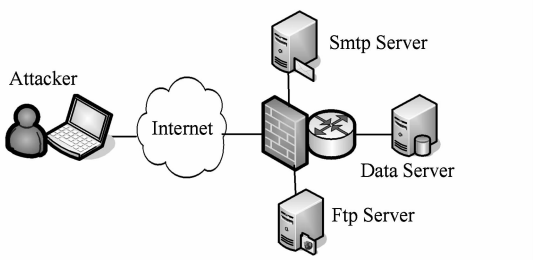


Fig. 2　Topology of example network.

图 2　网络拓扑结构

Table 1　Connectivity in Example Network

表 1　防火墙规则及连通信息

Source	Destination	Service	Action
All	Smtp Server	Ftp, Smtp	Allow
All	Ftp Server	Ftp, Ssh	Allow
Smtp Server	Database	Oracle	Allow
Ftp Server	Data Server	Oracle	Allow

Table 2　Vulnerability in Servers

表 2　服务器弱点信息

Host	Vulnerability	CVE ID	Effect
Smtp Server	Ftp . rhost	1999-0547	User privilege
Ftp Server	Ftp . rhost	1999-0547	User privilege
	Ssh Buffer overflow	2006-2421	User privilege
Data Server	Oracle TNS Listener	2002-0965	Root privilege

4.1　攻防随机博弈状态描述及其转移概率

攻击者对网络的攻击和控制体现在对网络中实体组件的掌控上,即表现为攻击者对实体组件特权的获得. 本实例将网络安全状态表达为攻击者在各个网络实体组件的访问能力(即特权)情况,并将网络安全状态作为攻防随机博弈状态集. 攻击动作引起网络安全状态的变化,即攻击者在各个组件上特权状态的变化. 一般地,可以根据具体的网络系统环境定义攻击者特权状态集合. 这里我们把攻击者的特权状态可以分为:无任何特权(no privilege)、远程访问特权(remote access privilege)、本地用户特权(user privilege)、根特权(root privilege)4 类,它们的特权由低到高顺序是无任何特权<远程访问特权<本地用户特权<根特权.

本文假定攻击者是理性的和贪婪的,即只要网络实体组件具有弱点,则攻击者就会知道如何利用它发动攻击且不会对已经具有特权的弱点发起攻击. 网络安全状态的变化总是向着攻击者特权逐渐提升的过程前进,即特权提升. 特权提升状态变化反映了攻击者的攻击演进过程,完整的网络安全状态图反映了攻击者为达到入侵目的而可能采用的各种攻击动作的组合. 例如,如果攻击者已经对某一网络实体组件具有本地用户特权,他不会再发动获取对该组件的低于本地用户特权的攻击. 攻击者在实体组件上特权提升包括在单个组件上的纵向提升和向着攻击目标的多个组件间横向提升.

假设攻击者在攻击主机上具有 Root 特权,并在此发起攻击,不能同时实施多个攻击动作,并以获取 Data Server 的 Root 特权作为目标. 根据防火墙

规则,攻击者在 Smtp Server 和 Ftp Server 上,仅仅具有最低的远程访问特权且无法访问数据库服务器.但是各个组件的弱点的存在及其依赖关系,攻击者可以通过利用这些具有关联关系的弱点,进行多步攻击和特权提升,获取 Data Server 的 Root 特权.具体过程如下:在状态 S_1,攻击者在攻击主机上具有 Root 特权,可以分别利用 Smtp Server 和 Ftp Server 的弱点发动 Ftp.rhosts 攻击获取它们的本地用户特权,到达状态 S_2,S_3.因为它们与 Data Server 有连接关系,从而攻击者可以以它们为跳板利用 Oracle TNS Listener 弱点,获取 Data Server 的 Root 特权到达状态 S_5.另外,攻击者还可以利用 Ftp Server 的弱点 Ssh Buffer overflow 发动攻击获取 Ftp Server 的特权到达状态 S_4,然后利用与 Data Server 连接关系,利用 Oracle TNS Listener 弱点获取 Data Server 的 Root 特权到达状态 S_5.具体的攻防随机博弈状态图 $G=(S,E)$,如图 3 所示.博弈状态 $S=\{S_1,S_2,S_3,S_4,S_5\}$,各个状态描述如表 3 所示:

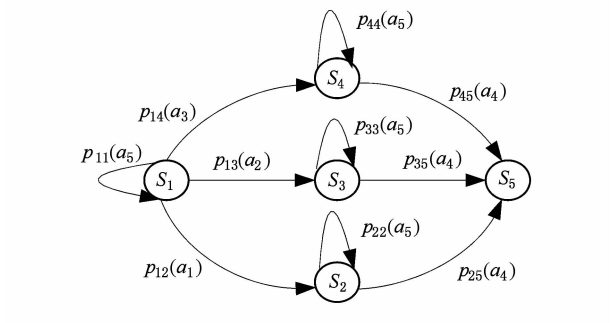


Fig. 3 Attack-defense stochastic game state graph.

图 3 攻防随机博弈状态图

Table 3 Description of Stochastic Game State

表 3 攻防博弈状态描述

State	Description of State
S_1	Root privilege on Attacker Host
S_2	User privilege on Ftp Server
S_3	User privilege on Smtp Server
S_4	User privilege on Ftp Server
S_5	Root privilege on Data Server

攻防随机博弈状态转移概率 $p_{ij}(a_m)$ 表示为攻击者发动攻击 a_m 的成功率,该值与攻击复杂度、网络环境等因素有关.根据专家知识、历史攻击数据并结合上述假定的信息系统环境确定,表 4 给出了状态转移概率的具体取值:

Table 4 Description of Attack Action

表 4 攻击动作描述

Symbol	Name	Category	Success Probability	AL
a_1	Ftp . rhost attack on Ftp Sever	User	0.8	7
a_2	Ftp . rhost attack on Smtp Sever	User	0.8	8
a_3	Ssh Buffer overflow	User	0.7	5
a_4	Oracle TNS Listener	Root	0.7	10
a_5	No action	Other	0	0

4.2 攻防动作集

分析攻击者的弱点利用过程,得到各个状态的攻击者动作集,$A_1=\{a_1,a_2,a_3,a_5\}$,$A_2=\{a_4,a_5\}$,$A_3=\{a_4,a_5\}$,$A_4=\{a_4,a_5\}$,$A_5=\phi$.全部攻击动作集且 $A=\bigcup_{i=1}^{5}A_i=\{a_1,a_2,a_3,a_4,a_5\}$.攻击者动作具体描述如表 4 所示,同时给出了攻击类别、攻击成功概率和致命度信息.对服务器弱点、可能的攻击动作及其关联关系进行分析,从防御策略库选出各个状态可用的防御动作集,$D_1=\{d_1,d_2,d_3,d_4,d_5,d_6,d_9\}$,$D_2=\{d_7,d_8,d_9\}$,$D_3=\{d_7,d_8,d_9\}$,$D_4=\{d_7,d_8,d_9\}$,$D_5=\phi$.全部防御动作集 $D=\bigcup_{i=1}^{5}D_i=\{d_1,d_2,d_3,d_4,d_5,d_6,d_7,d_8,d_9\}$.具体的防御动作及其操作代价和负面代价信息如表 5 所示:

Table 5 Description of Defense Action

表 5 防御动作描述

Symbol	Name	Ocost	Ncost
d_1	Patch Ftp . rhost on Ftp Sever	50	0
d_2	Close rsh on Ftp Sever	10	120
d_3	Close rsh on Smtp Sever	10	120
d_4	Patch Ftp . rhost on Smtp Sever	50	0
d_5	Close Ssh on Ftp Sever	10	120
d_6	Patch Ssh on Ftp Sever	50	0
d_7	Patch Oracle TNS Listener	50	0
d_8	Access control TNS Listener	30	0
d_9	No action	0	0

4.3 攻防收益计算

攻防动作集合确定之后,然后计算攻防动作收益和损失.因为采用零和非合作攻防博弈模型,从而仅需计算攻击收益即可.考虑到攻防收益的实际意义,攻击收益取正值.因为攻击都是针对某个服务器,可能对该服务器的机密性、完整性和可用性产生

危害,不妨设 $P_i=P_c=P_a=1/3$. Ftp Server 和 Smtp Server 的 Criticality 均为 3, Data Server 的 Criticality 为 5. 安全属性代价的高、中、低分别用 30,20,10 来表示,Ftp Server 和 Smtp Server 的安全属性代价($Icost$,$Ccost$,$Acost$)=(20,20,20),Data Server 的安全属性代价($Icost$,$Ccost$,$Acost$)=(30,30,30). 在这里,我们不考虑攻击者的攻击成本 AR,防御残余代价 $Rcost$. $Ocost$ 可以查询防御动作库得到,具体数值见表 5 所示. 若 $Ncost$ 很小时,可忽略不计,设为 0. 否则防御动作的负面影响可以看作是对服务器的一次 DOS 攻击,使得不能提供正常服务. 从而 Ncost 的转换为 DOS 攻击对服务器产生的系统损失代价. 为了简化分析,规定当防御动作 d 对攻击 a 有效时,$\varepsilon(a_i,d_j)=1$. 否则 $\varepsilon(a_i,d_j)=0$. 最后,通过用式(6)来计算每一个攻击动作的收益. 对于 $i=1,2,3,4,5$,构建攻防随机博弈状态 S_i 下攻防博弈矩阵 $\boldsymbol{S}_i$.

4.4　最优防御策略的选取

利用算法 1 求解各个攻防随机博弈状态值及其最优攻防策略,其中每个矩阵型博弈 $\boldsymbol{S}_i$ 的值利用 Gambit[17] 方法计算,最后得到最优攻防策略为 $\boldsymbol{\pi}^{a^*}=\{\pi_1^{a^*},\pi_2^{a^*},\pi_3^{a^*},\pi_4^{a^*}\}$,$\boldsymbol{\pi}^{a^*}=\{\pi_1^{d^*},\pi_2^{d^*},\pi_3^{d^*},\pi_4^{d^*}\}$,其中:$\pi_1^{a^*}=(0.3,0.27,0.43,0.0)$,$\pi_2^{a^*}=\pi_3^{a^*}=\pi_4^{a^*}=(1.0,0.0)$,$\pi_1^{d^*}=(0.39,0.0,0.0,0.47,0.0,0.14,0.0)$,$\pi_2^{d^*}=\pi_3^{d^*}=\pi_4^{d^*}=(0.0,1.0,0.0)$. 分析可知,在博弈状态 S_1,攻击者最优的攻击策略是以概率 0.3 选择攻击动作 a_1,以概率 0.27 选择攻击动作 a_2,以概率 0.43 选择攻击动作 a_3. 防御者最优的防御策略是以概率 0.39 选择防御动作 d_1,以概率 0.47 选择防御动作 d_4,以概率 0.14 选择防御策略 d_6. 在博弈状态 S_2,S_3,S_4 攻防双方都采取纯策略,这也符合攻防环境实际情况. 各个博弈状态的期望收益值向量如表 6 所示. 图 4 描述了用 Gambit 计算攻防双方在博弈状态 S_1 下攻防策略概率变化过程,逐渐收敛最后趋于稳定,即达到纳什均衡.

Table 6　Expected Payoff of Game State
表 6　博弈状态攻防期望收益值

Game State	Payoff of Attacker	Payoff of Defender
S_1	347.5	−347.5
S_2	54	−54
S_3	54	−54
S_4	54	−54
S_5	30	−30

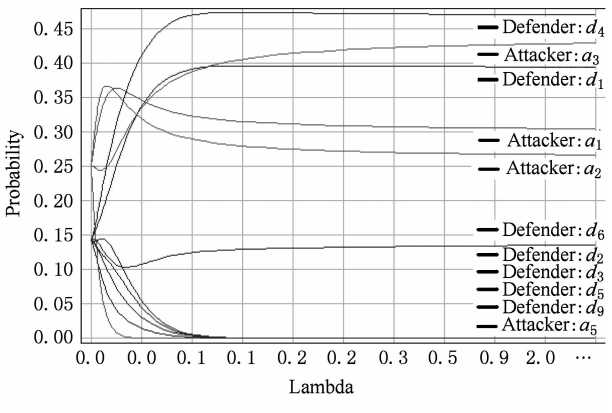


Fig. 4　Probability of all strategies in S_1.
图 4　博弈状态 S_1 下的攻防策略概率变化图

5　结　　论

针对网络安全最优防御策略选取的复杂性,形式化定义了网络安全防御策略选取问题. 提出了一种刻画网络安全攻防矛盾,解决最优防御策略选取问题的攻防随机博弈模型. 将网络攻防双方建模为二人非合作攻防随机博弈模型,并详细地描述了该模型的形式化定义及其构成元素. 该模型是矩阵型攻防博弈模型和 Markov 决策过程扩展为多人、多状态的动态攻防推演模型. 不仅考虑防御策略成本有效性,而且将攻击策略及其收益纳入攻防随机博弈模型中,全面考虑攻防双方矛盾,使得防御决策更加有效. 介绍了基于上述模型的主动防御选取算法,帮助防御者采取最优防御策略进行主动防御. 网络实例分析说明了该模型和算法在攻击策略预测和主动防御方面的有效性.

参　考　文　献

[1] Fang Binxing. Explain the innovation and breakthrough of information security [OL]. [2008-03-21]. http://www.cert.org.cn/articles/news/common/2007051823317.shtml (in Chinese)
(方滨兴. 解读信息安全创新突破点[OL]. [2008-03-21]. http://www.cert.org.cn/articles/news/common/2007051823317.shtml, 2008)

[2] Nash J. Equilibrium points in n-person games [J]. Proc of the National Academy of Sciences of the United States of America, 1950, 36(1): 48-49

[3] Lee W. Toward cost-sensitive modeling for intrusion detection and response [J]. Journal of Computer Security, 2002, 10(1/2): 5-22

[4] Jiang Wei, Fang Binxing, Tian Zhihong, et al. Evaluating network security and optimal active defense based on attack-defense game model [J]. Chinese Journal of Computers, 2009, 32(4): 817-827 (in Chinese)
(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[J]. 计算机学报, 2009, 32(4): 817-827)

[5] Wang L Y, Noel S, Jajodia S. Minimum-cost network hardening using attack graphs [J]. Computer Communications, 2006, 29(18): 3812-3824

[6] Feng Pinghui, Lian Yifeng, Dai Yingxia, et al. A vulnerability model of distributed systems based on reliability theory [J]. Chinese Journal of Computers, 2006, 29(8): 1375-1382 (in Chinese)
(冯萍慧, 连一峰, 戴英侠, 等. 面向网络系统的脆弱性利用成本估算模型[J]. 计算机学报, 2006, 29(8): 1375-1382)

[7] Syverson P F. A different look at secure distributed computation [C] //Proc of the 1997 IEEE Computer Security Foundations Workshop. Washington: IEEE Computer Society, 1997: 109-115

[8] Burke D. Towards a game theory model of information warfare [D]. Montgomery, AL: Air force Institute of Technology, Air University, 1999

[9] Lye Kong-wei, Wing J. Game strategies in network security. International Journal of Information Security, 2005, 4(1/2): 71-86

[10] Liu P, Zang W. Incentive-based modeling and inference of attacker intent, objectives, and strategies [C] //Proc of the 10th ACM Computer and Communications Security Conf (CCS'03). New York: ACM, 2003: 179-189

[11] Jiang Wei, Tian Zhihong, Zhang Hongli, et al. A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision [C] //Proc of 2008 IEEE Int Conf on Networking, Sensing and Control. Washington: IEEE Computer Society, 2008: 648-653

[12] Sallhammar K, Helvik B E, Knapskog S J. On stochastic modeling for integrated security and dependability evaluation [J]. Journal of Networks, 2006, 1(5): 31-42

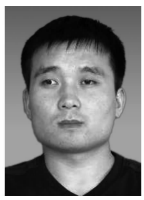
[13] Shi Jin, Lu Yin, Xie Li. Dynamic intrusion response based on game theory [J]. Journal of Computer Research and Development, 2008, 45(5): 747-757 (in Chinese)
(石进, 陆音, 谢立. 基于博弈理论的动态入侵响应[J]. 计算机研究与发展, 2008, 45(5): 747-757)

[14] Shapley L S. Stochastic games [J]. Proc of the National Academy of Sciences of the United States of America, 1953, 39(10): 1095-1100

[15] Fink A M. Equilibrium in a stochastic n-person game [J]. Journal of Science of the Hiroshima University, 1964, 28(1): 89-93

[16] Karmarkar N. A new polynomial-time algorithm for linear programming [J]. Combinatorica, 1984, 4(4): 373-395

[17] McKelvey R D, McLennan A M, Turocy T L. (2007) Gambit: Software Tools for Game Theory, Version 0.2007.01.30 [OL]. [2008-03-26]. http://www.gambit-project.org



Jiang Wei, born in 1979. PhD candidate. A student member of China Computer Federation. His mian research interests are network and information security, network attack and defense.
姜 伟,1979 年生,博士研究生,中国计算机学会学生会员,主要研究方向为网络与信息安全等.

Fang Binxing, born in 1960. Professor and PhD supervisor. His current research interests include computer architecture, information security and computer network.
方滨兴,1960 年生,教授,博士生导师,主要研究方向为计算机体系结构、信息安全和计算机网络等.

Tian Zhihong, born in 1978. PhD and lecturer. His main research interests include network and information security.
田志宏,1978 年生,博士,讲师,主要研究方向为网络与信息安全等.

Zhang Hongli, born in 1973. Professor and PhD supervisor. Her main research interests include network and information security, network measure, etc.
张宏莉,1973 年生,教授,博士生导师,主要研究方向为网络与信息安全、网络测量等.

Research Background

It is a complex issue for defenders to select optimal defense strategy in network security. Because of oppositional target and interdependent strategies of attackers and defenders, we think that the issue should be addressed in a more systematic manner, utilizing mathematic tools and models. In this paper, the issue of optimal defense strategy selection is defined and formalized. A

new attack-defense stochastic game model is proposed to describe the offensive and defensive conflict in network security and address the issue of optimal defense strategy selection. The model is a dynamic multi-player and multi-state model which is expanded by normal attack-defense game and Markov decision process. By viewing privilege state in node of attacker as elements in attack-defense stochastic game, we can model the dynamic transition of attack and defense state and compute the probabilities of attacker and defender behavior. An algorithm for defense strategy selection based on those models is proposed. A representative network example is provided to illustrate our models and demonstrate the efficacy of our models in the prediction of attack behaviors and decision of optimal defense strategies. This research is partly supported by the National Basic Research Program of China (973 Program) under grant No. 2007CB311100, the National Natural Science Foundation of China under grant No. 60903166, and the National High-Tech Research and Development Plan of China (863 Program) under grant No. 2009AA01Z437.

中国计算机学会
第 9 届全国搜索引擎和网上信息挖掘学术研讨会(SEWM2011)
征文通知
(2011 年 5 月 20—22 日, 河北大学,保定)

第 9 届全国搜索引擎和网上信息挖掘学术研讨会(SEWM2011)由中国计算机学会主办,河北大学承办. 该系列会议每年举行一次,现已成为国内海量网络信息处理与应用领域最主要的学术活动之一. 此次会议将为网络信息搜索与挖掘领域的学者交流最新研究成果、进行广泛的学术讨论提供便利,并且将邀请国内外该领域的著名学者做精彩报告,同时将保持 SEWM 会议的传统,组织搜索和挖掘相关技术的评测. 会议还将评出优秀学生论文,颁发证书并给予奖励.

征稿范围(包括但不限于如下主题)

信息检索模型、算法及基础理论	面向行业的信息检索
跨语言和多语言信息检索	面向信息检索的机器翻译技术
交互式检索	多媒体信息检索
用户模型及分析	基于任务的信息检索
智能问题回答系统	文本分类、文本聚类及相关的机器学习方法
信息过滤与信息抽取	文本倾向性分析、意见挖掘及舆情监控
社区发现	网络信息检索的建模、实现和应用
搜索引擎设计	信息检索中的机器学习

自然语言理解在信息检索中的应用.

投稿要求

论文必须未公开发表过;中、英文稿均可接受;严禁一稿多投.

论文应包括题目、作者姓名、作者单位、摘要、关键字、正文和参考文献;另附作者地址、邮编、电话或传真及 E-mail 地址.

参选优秀学生论文的稿件请注明(须由在校博士生、硕士生或本科生为第一作者).

联系信息

投稿信箱:sewm2011@hbu.cn

会议网站:http://sewm2011.hbu.cn

会议咨询:张明,袁方(sewm2011@hbu.cn,13933221661)

论文出版

会议录用中文论文推荐到《计算机研究与发展》(EI 检索、正刊)、《模式识别与人工智能》(EI 检索、正刊)、《华南理工大学学报(自然科学版)》(EI 检索、正刊)、《山东大学学报(理学版)》中文核心期刊正刊、《郑州大学学报》中文核心期刊正刊、《广西师范大学学报》中文核心期刊正刊、《广西大学学报(自然科学版)》中文核心期刊正刊、《智能系统学报》正刊等期刊上发表. 会议录用英文论文推荐到国际期刊《International Journal of Machine Learning and Cybernetics》正刊上发表.

重要日期

投稿截止日期:2010 年 11 月 7 日

录用通知发出日期:2010 年 12 月 7 日

正式论文提交截止日期:2010 年 12 月 22 日

会议召开日期:2011 年 5 月 20—22 日