doi:10.3969/j.issn.1001-893x.2015.09.014
引用格式:李方伟,黄卿,朱江,等.项目反应理论在实时网络风险评估中的应用[J].电讯技术,2015,55(9):1025-1030.[LI Fangwei, HUANG Qing, ZHU Jiang, et al. Application of Item Response Theory in Real-time Network Risk Assessment[J]. Telecommunication Engineering, 2015, 55(9):1025-1030.]

项目反应理论在实时网络风险评估中的应用*

李方伟,黄 卿**,朱 江,张海波

(重庆邮电大学 移动通信技术重庆市重点实验室,重庆 400065)

摘 要:为提高传统网络风险评估方法的准确性,针对大部分网络风险评估方法未考虑攻击能力值的问题,提出了一种基于项目反应理论的实时网络风险评估方法。该方法利用项目反应理论引入的攻击能力值参数以及服务安全等级参数,对传统攻击威胁值和攻击成功概率计算方法进行改进,并采用三标度层次分析法构建出更准确的服务重要性权重,最终获得符合网络环境的评估态势。仿真结果表明:该方法可以提高评估结果的准确度,并实时地绘制更符合真实网络环境的安全态势图。

关键词:网络安全;态势感知;项目反应理论;风险态势评估;层次化
中图分类号:TP393 **文献标志码**:A **文章编号**:1001-893X(2015)09-1025-06

Application of Item Response Theory in Real-time Network Risk Assessment

LI Fangwei, HUANG Qing, ZHU Jiang, ZHANG Haibo

(Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: In order to improve the accuracy of traditional risk assessment methods and solve the problem that most of risk assessment methods did not consider attack ability, this paper puts forward a risk assessment method for network security based on item response theory (IRT). Firstly, the attack ability introduced by IRT and the service security level is used to calculate the threat of attack and the success probability of attack. Secondly, the three-scale analytic hierarchy process is adopted to calculate the importance weight of service accurately. Finally, the risk situation graphs are generated by the improved method. The simulation results show that this method can improve the accuracy of evaluation and get a more realistic network risk situation graph in real-time.

Key words: network security; situational awareness; item response theory; risk assessment; hierarchical model

1 引 言

网络安全态势感知[1]是在分析历史数据、检测当前网络安全状况的基础上,对未来一段时间进行安全告警的新型安全技术,主要包括态势要素获取、态势评估、态势预测三个阶段。安全态势评估技术属于网络安全态势感知的重要环节,是衔接态势要

* **收稿日期**:2015-03-11;**修回日期**:2015-06-02 Received date: 2015-03-11; Revised date: 2015-06-02
基金项目:国家自然科学基金资助项目(61271260; 61301122)
Foundation Item: The National Natural Science Foundation of China (No. 61271260, 61301122)
** **通讯作者**:huangq46@163.com **Corresponding author**: huangq46@163.com

素获取和态势预测的重要桥梁。国外方面,文献[2]根据不同网络配置和无线网络的特性,提出了一种四层无线网络的风险评估机制;文献[3]根据国家漏洞数据库(National Vulnerability Database, NVD)提出了一种通过检测漏洞威胁来评估网络风险的方法;文献[4]基于模糊集理论,将数据信息映射为自然语言,并进行风险评估。国内方面,文献[5]在 DS 证据理论的多源数据融合基础上对网络风险进行评估;文献[6]针对入侵意图难于发现的问题,采用了一种基于动态攻击图,并结合资产、脆弱性的实时网络评估方法。以上研究在网络风险评估方面具有众多优势,但也普遍存在一些待完善的地方:一是攻击成功概率的计算只依赖漏洞信息,客观性不足;二是攻击威胁值的定义过于宽泛,多种相同威胁因子的攻击,威胁值存在差异;三是重要性权重的计算方法精确度不高,导致评估结果不够准确。

为了进一步完善网络风险评估,本文提出了一种项目反应理论与层次化网络风险评估模型相结合的方法,利用系统配置信息、系统运行信息以及通用漏洞评分系统(Common Vulnerability Scoring System, CVSS)[7],并结合安全防御强度,解决了计算攻击成功概率时客观性不足的问题;通过项目反应理论提出攻击能力值的概念,解决了攻击威胁值区分度不高的问题;依靠三标度层次分析法解决了重要性权重精确度不高的问题。最后对服务逻辑层、主机逻辑层和网络逻辑层分别进行风险定量分析,绘制各层的风险态势图,直观显示网络各部分的风险及变化规律,为安全策略的制定提供了依据。

2 基于项目反应理论的实时网络风险评估

2.1 实时网络风险态势评估框架

为应对现实生活中网络规模的不断扩大,依照通信系统架构,自底向上将网络系统(System)依次划分为漏洞逻辑层(Vulnerability)、服务逻辑层(Service)、主机逻辑层(Host)和网络逻辑层(Network),并利用态势图直观显示出网络的风险大小,再针对大风险服务或主机进行重点防范。

实时网络风险态势评估框架如图 1 所示。

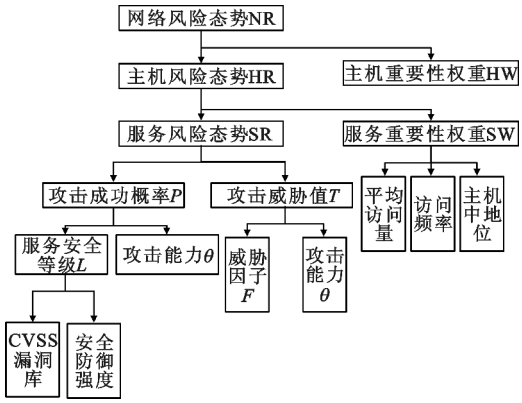

图 1 实时网络风险态势评估框架

Fig. 1 The real-time network security risk assessment framework

以入侵检测系统(Intrusion Detection System, IDS)的报警信息、目标网络拓扑、漏洞信息为基础,结合规则库,从服务逻辑层开始,逐步评估网络各逻辑层的风险态势。

2.2 基于项目反应理论的算法定义

项目反应理论[8-9]又称潜在特质理论,广泛应用于心理学与教育学,它是对测试者能力值的一种估计,并将测试者对每个测试项目的某种反应概率与此项目的一定特质联系起来的方法。

(1)攻击威胁值

针对网络攻击中的权限、流量威胁,采用了文献[5]和文献[10]中利用威胁因子对服务威胁值进行定义的方法,通过区分端口扫描攻击、拒绝服务攻击、提升权限攻击和远程用户攻击的方法对所有攻击行为分类,并以四种攻击类型的威胁因子作为评判威胁值大小的主要因素。

然而,考虑到相同攻击类型不同攻击行为的威胁值可能存在差异,为了提高传统攻击威胁值的区分度,利用项目反应理论引入攻击能力值的概念,并重新定义了一个新的攻击威胁值公式:

$$T_i = 10^{F_i \frac{\theta_i + 4}{7}}。 \tag{1}$$

式中,θ_i 表示第 i 种攻击行为的攻击能力值,由项目反应理论的单参数 Logistic 函数以及攻击反应矩阵进行参数估计确定;$F_i \in (1,2,3)$ 表示第 i 种攻击行为所属攻击类型的威胁因子。

(2)攻击成功概率

攻击成功执行与某些条件是密不可分的,如特殊端口的打开、某些位置具有安全缺陷、存在可被利用的安全漏洞等。针对文献[6]并未考虑安全防御强度和攻击能力值的影响,依据项目反应理论重新

定义了攻击成功概率的求取方法。

定义 1　服务安全等级(L):表示服务受到攻击后的阻抗程度,由服务存在的漏洞信息(C)和安全防御强度(I)组成,服务安全等级越高,安全性越强。漏洞信息由 CVSS 确定,并根据攻击复杂度(AC)、攻击途径(AV)以及身份认证(AU)的指标描述将高、中、低难度等级分别定量为 3、2、1,且规定 $C=\frac{AC+AV+AU}{3}$;根据服务所受到的保护措施,将安全防御强度 I 分为 3 个等级,且 $I\in(1,2,3)$。由以上分析,定义服务安全等级公式如下:

$$L_j=3(\lambda_1 C_j+\lambda_2 I_j-2)。\tag{2}$$

式中,λ_1、λ_2 分别表示漏洞与安防在服务安全性方面所占比重,依照以往经验,λ_1、λ_2 取值分别为 0.4、0.6。

通过定义 1 的服务安全等级,结合项目反应理论的单参数 Logistic 模型,进一步提出攻击成功概率 P 的计算公式如下:

$$P_{ij}=\{1+\exp[-D(\theta_i-L_j)]\}^{-1}。\tag{3}$$

式中,θ_i 表示第 i 种攻击行为的攻击能力值,$D=1.7$ 是一个常数。随着时间的推移,新的攻击行为被检测出来,使原有的攻击反应矩阵发生了改变,攻击能力值更新,从而达到了攻击威胁值和攻击成功概率实时更新的效果。

3　层次化风险态势

3.1　风险权重因子

根据影响服务性能因素可知,主机中服务重要性的客观反映主要由平均访问量、访问频率以及服务在主机中地位所决定,利用(0,1,2)三标度层次分析法[11]对服务重要性权重进行定量计算,获得相对准确的服务重要性权重。

3.2　风险态势值

定义 2　服务风险态势(R_S):在时间$(t,t+\Delta t)$内,服务 $S_i(0\leqslant i\leqslant m)$受到的攻击总数为 N_i,每项攻击的攻击成功概率为 P_i,其中第 $k(0\leqslant k\leqslant n)$项攻击的数目为 N_{ik},且 $N_i=\sum_{k=0}^{n}N_{ik}$,第 k 项攻击的威胁因子及能力值为 F_k 和 θ_k,则服务 S_i 的风险态势为

$$R_{S_i}=\sum_{k=1}^{n}\left(N_{ik}10^{F_{ik}}\frac{\theta_{ik}+4}{7}P_{ik}\right)。\tag{4}$$

定义 3　主机风险态势(R_H):在时间$(t,t+\Delta t)$内,主机 $H_g(1\leqslant g\leqslant v)$上运行 u 种服务,且服务 $S_i(0\leqslant i\leqslant u)$的重要程度为 $\bar{w}_{\mathrm{srv}}$,则主机 H_g 风险态势为

$$R_{H_g}=\sum_{i=1}^{u}(R_{S_i}\bar{w}_{\mathrm{srv}_i})。\tag{5}$$

定义 4　网络风险态势(R_N):在时间$(t,t+\Delta t)$内,网络中运行了 v 台主机,主机 $H_g(1\leqslant g\leqslant v)$在网络中的重要性权重为 $\bar{w}_{\mathrm{host}_g}$,则网络的风险态势为

$$R_N=\sum_{g=1}^{v}(R_{H_g}\bar{w}_{\mathrm{host}_g})。\tag{6}$$

4　实例仿真分析

为了验证提出方法的科学性和全面性,我们利用实验室搭建的模拟平台,建立了简易的网络拓扑结构图,如图 2 所示,利用 Nessus 检测主机的漏洞,采集了 2013 年 7 月 1 日到 8 月 31 日共两个月的校园网络防护数据进行仿真研究,并对存在服务漏洞的主机进行动态风险分析。

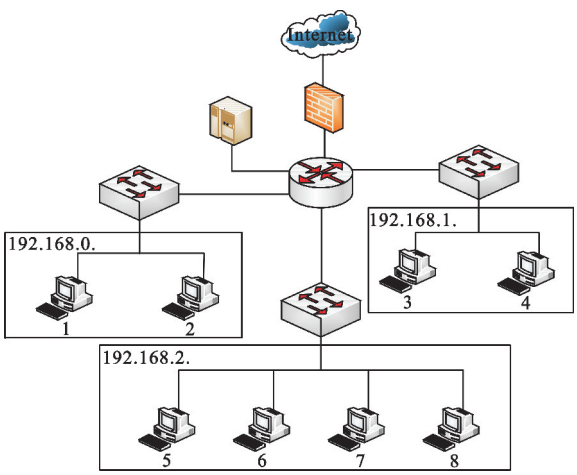

图 2　网络拓扑结构图

Fig. 2 The network topology

4.1　三标度法权重的计算

利用服务信息与漏洞信息,以服务重要性为目标层;以评判网络服务重要性的 3 个指标,即平均访问量、访问频率、主机中地位为准则层;以待确定重要性的服务为方案层,由专家经验定义平均访问量、访问频率、主机中地位的相互间比重为[0.2 0.2 0.6]。以存在漏洞且 IP 为 192.168.0.1 的主机为例,其含有 DNS、WWW、FTP、SMTP 四种服务,可得准则层的 3 个指标相对于四种服务的权重分别为 $B_{\mathrm{I}}=[0.1376\ 0.5132\ 0.2751\ 0.0741]$,$B_{\mathrm{II}}=[0.0989\ 0.5183\ 0.2839\ 0.0989]$,$B_{\mathrm{III}}=[0.0989\ 0.2839\ 0.5183\ 0.0989]$,根据(0,1,2)三标度法计算出服务重要性权重及主机重要性权重,如表 1 所示。

表 1 网络服务及权重分配

Table1 Network service and distribution of weight

主机 IP (192. 168.)	运行服务	服务重要性权重	主机重要性权重
0. 1	DNS	0. 106 64	0. 260 4
	WWW	0. 376 64	
	FTP	0. 422 78	
	SMTP	0. 093 94	
1. 4	WWW	0. 405 70	0. 233 9
	FTP	0. 182 88	
	ORACLE	0. 411 42	
2. 5	DNS	0. 325 72	0. 222 8
	POP3	0. 428 58	
	SMTP	0. 245 72	
2. 7	WWW	0. 3107 4	0. 282 9
	TELNET	0. 433 02	
	DNS	0. 107 34	
	FTP	0. 083 44	
	ORACLE	0. 065 46	

通过数据分析可知,三标度法在降低了九标度法复杂度的同时,也避免了构造判断矩阵时权重选择的模糊性,而较于等级赋值重要性权重的方法,求取的权重也更精确。

4.2 攻击成功概率和攻击威胁值

利用定义的攻击成功概率和攻击威胁值算法,以 7 月份系统服务信息、系统漏洞信息以及危险报警信息作为数据基础,经统计分析,总共有 12 种不同的攻击行为对网络中的 7 种服务进行了攻击,结合项目反应理论,利用参数估计得到每一种攻击行为的攻击能力值 θ,并通过系统漏洞信息和服务信息获得自定义参数服务安全等级 L 的值,从而根据公式(3)即可计算出相应攻击行为对主机服务的攻击成功概率,如表 2 所示。通过是否考虑攻击能力值来比较攻击威胁值的变化,与文献[10]方法结果比较如图 3 所示。

为实现网络风险态势的实时评估,对 8 月的每天进行攻击统计,若存在上月未出现的攻击情况,则将其添加到原来的攻击反应矩阵中,同时更新概率矩阵和攻击威胁值。

表 2 攻击成功概率

Table 2 Attack successful probability

攻击	攻击成功概率						
	WWW	FTP	SMTP	POP3	ORACLE	TELNET	DNS
Ipsweep(1)	0. 000 0	0. 175 0	0	0. 000 0	0. 000 0	0. 980 1	0. 696 8
Nmap(2)	0. 972 8	0. 625 6	0	0. 998 7	0. 724 6	0. 997 4	0. 000 0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Guess_passwd(11)	0. 494 5	0. 000 0	0	0. 000 0	0. 000 0	0. 913 8	0. 000 0
Warezmaster(12)	0. 494 5	0. 043 7	0	0. 000 0	0. 000 0	0. 000 0	0. 000 0

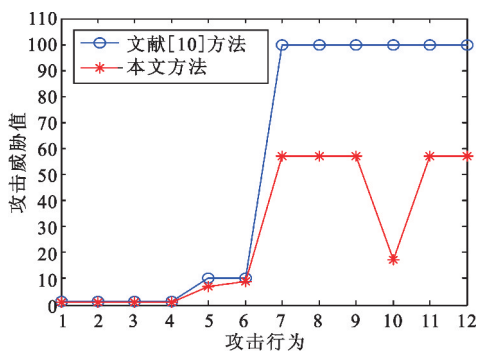

图 3 两种攻击威胁值方法的比较

Fig. 3 Comparison of threat of attack between two methods

4.3 实时风险态势评估

针对 2013 年 8 月的参数信息,利用改进的风险态势评估算法,每隔 $\Delta t = 1$ 天进行一次风险态势值的计算,并绘制出一个月的风险态势曲线,方便分析与决策。图 4 ~6 分别表示在 8 月内服务逻辑层、主机逻辑层、网络逻辑层的风险态势变化。图 4 表示 WWW、FTP、TELNET 三种服务的风险态势图,图 5 绘制了 4 台存在漏洞主机的风险态势图,图 6 则给出了整个网络的风险态势图。

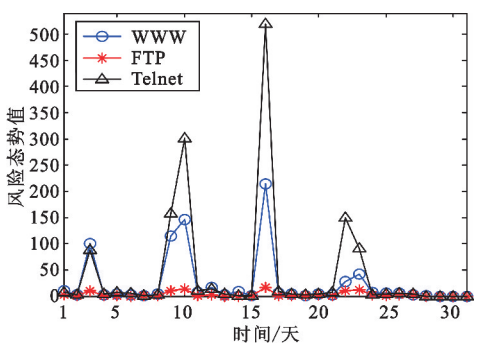

图 4 实时服务风险

Fig. 4 Risk of services in real-time

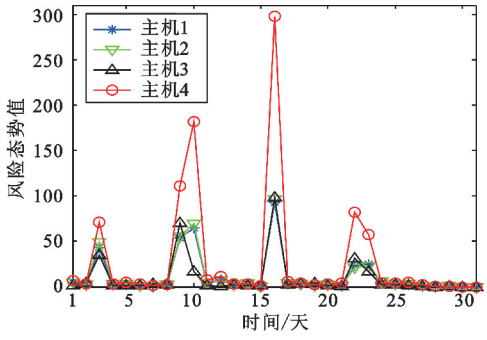

图 5　实时主机风险

Fig. 5 Risk of hosts in real-time

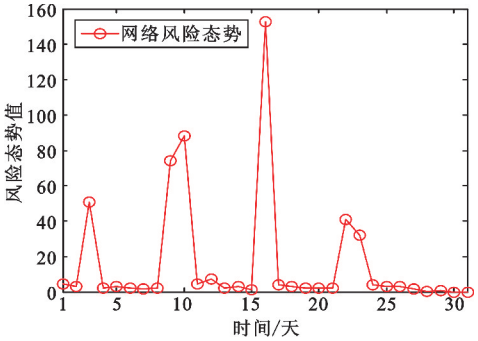

图 6　实时网络风险

Fig. 6 Risk of network in real-time

通过分析可得到以下结论:第一,TELNET 服务在当月遭受的攻击最为严重,WWW 服务其次,受到攻击风险最低的是 FTP 服务;第二,主机 4 受到的攻击风险最大,其余 3 台主机风险程度相近;第三,网络攻击的发生绝大部分集中在周末,因此猜测攻击者很有可能有正当职业,如在职工作者或学生。

4.4　网络风险态势的比较

网络安全事件的发生存在很大的偶然性与随机性,若仅考虑造成的损失并不能真实地还原安全状况,因此提出了通过攻击成功概率、服务安全等级、服务重要性权重以及攻击能力值等概念来对传统的风险态势评估方法进行改进,并融入到各逻辑层的风险评估中。

图 7 给出了本文方法与文献[5]方法的风险态势评估结果,可以看到,文献[5]方法得到的风险值明显高于本文方法,而实际上,由于文献[5]中并没有考虑攻击能力值参数和服务安全等级参数所带来的影响,从而导致了评估结果的不准确;同时,由于部分攻击行为存在,但并未攻击成功,以及攻击威胁值的计算存在偏差等问题,也很容易导致算法无法真实地反映网络安全状况,从而对网络安全管理员造成误导,甚至做出错误决策。本文方法为克服以上出现的问题,利用项目反应理论引入了攻击能力值的概念,使网络风险评估的准确性得到了针对性改善。

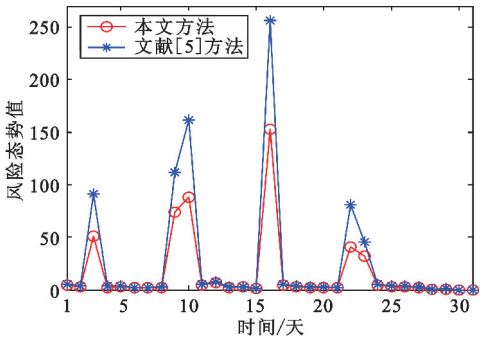

图 7　两种风险评估方法结果的比较

Fig. 7 Comparison of network risk assessment between two methods

5　结束语

本文以 IDS 报警信息、系统漏洞信息以及系统服务信息为输入,分别对服务逻辑层、主机逻辑层以及网络逻辑层的风险态势进行定量分析,提出了一种基于项目反应理论的层次化风险态势评估方法,与传统方法相比,存在以下优势:第一,将 CVSS 系统与安全防御强度相结合所定义的服务安全等级作为安全评价参数之一,使风险评估结果更全面、科学;第二,通过三标度层次分析法提高了重要性权重的精度;第三,结合项目反应理论,提出了一种区分度更高、更符合实际的攻击威胁值算法和攻击成功概率算法;第四,凭借攻击成功概率和攻击威胁值的动态更新,实现了风险态势的实时评估。受到所用数据集识别攻击的准确度影响,该方法也存在一定局限性,下一阶段准备在保证评估全面性的基础上,针对大规模网络环境,对提高数据集提取精度的方法展开研究。

参考文献:

[1]　龚正虎,卓莹. 网络态势感知研究[J]. 软件学报,2010,21(7):1605-1619.
GONG Zhenghu, ZHUO Ying. Research on cyberspace situational awareness[J]. Journal of Software, 2010, 21(7):1605-1619. (in Chinese)

[2]　Tsai H, Huang Y. An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks[J]. IEEE Transactions on Reliability, 2011, 60(4):801-816.

[3]　Abedin M, Nessa S, Al-Shaer E, et al. Vulnerability anal-

ysis for evaluating quality of protection of security policies [C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria, US: ACM, 2006: 49-52.

[4] Sanguansat K, Chen S M. A new method for analyzing fuzzy risk based on a new fuzzy ranking method between generalized fuzzy numbers[C]//Proceedings of 2009 International Conference on Machine Learning and Cybernetics. Baoding: IEEE, 2009: 2823-2827.

[5] 刘效武,王慧强,吕宏武,等. 基于融合的网络安全态势量化感知[J]. 吉林大学学报(工学版),2013,43(6):1650-1657.
LIU Xiaowu, WANG Huiqiang, LYU Hongwu, et al. Quantitative awareness of network security situation based on fusion[J]. Journal of Jilin University (Engineering and Technology Edition), 2013, 43(6): 1650-1657. (in Chinese)

[6] 罗智勇,尤波,许家忠,等. 基于三层攻击图的入侵意图自动识别模型[J]. 吉林大学学报(工学版),2014,44(5):1392-1397.
LUO Zhiyong, YOU Bo, XU Jiazhong, et al. Based on three layer attack graph automatic intrusion intention recognition model[J]. Journal of Jilin University (Engineering and Technology Edition), 2014, 44(5): 1392-1397. (in Chinese)

[7] Ali A, Zavarsky P, Lindskog D, et al. A Software Application to Analyze the Effects of Temporal and Environmental Metrics on Overall CVSS v2 Score[C]//Proceedings of 2011 World Congress on Internet Security. London: IEEE, 2011: 21-23.

[8] Baldiris S, Fabregat R, Graf S, et al. Learning Object Recommendations based on Quality and Item Response Theory[C]//Proceedings of 2014 IEEE 14th International Conference on Advanced Learning Technologies. Athens, Greece: IEEE, 2014: 34-36.

[9] Arnold F, Pieters W, Stoelinga M I A. Quantitative penetration testing with item response theory[C]//Proceedings of 2013 9th International Conference on Information Assurance and Security. Gammarth, Tunisia: IEEE, 2014: 49-54.

[10] 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[J]. 电子与信息学报,2012,34(8):1934-1938.
LIU Gang, LI Qianmu, ZHANG Hong. Reliability vector orthogonal projection decomposition method of network security risk assessment[J]. Journal of Electronics and Information Technology, 34(8): 1934-1938, 2012. (in Chinese)

[11] 蒋官澄,吴雄军,王晓军,等. 确定储层损害预测评价指标权值的层次分析法[J]. 石油学报,2011,32(6):1037-1041.
JIANG Guandeng, WU Xiongjun, WANG Xiaojun, et al. Application of the analytical hierarchy process to determining evaluation index weights for the prediction of reservoir damage[J]. Acta Petrolei Sinica, 2011, 32(6): 1037-1041. (in Chinese)

作者简介:

李方伟(1960—),男,重庆人,教授、博士生导师,主要研究方向为移动通信理论与技术、信息安全技术;

LI Fangwei was born in Chongqing, in 1960. He is now a professor and also the Ph. D. supervisor. His research concerns mobile communication theory and technology, information security technology.

Email: lifw@ cqupt. edu. cn

黄 卿(1990—),男,江西人,硕士研究生,主要研究方向为网络安全态势感知;

HUANG Qing was born in Jiangxi Province, in 1990. He is now a graduate student. His research concerns network security situational awareness.

Email: huangq46@ 163. com

朱 江(1977—),男,湖北人,2009 年于电子科技大学获博士学位,现为副教授,主要研究方向为认知无线电;

ZHU Jiang was born in Hubei Province, in 1977. He received the Ph. D. degree from University of Electronic Science and Technology of China in 2009. He is now an associate professor. His research concerns cognitive radio.

Email: zhujiang@ cqupt. edu. cn

张海波(1979—),男,重庆人,博士,讲师,主要研究方向为无线资源优化.

ZHANG Haibo was born in Chongqing, in 1979. He is now a lecturer with the Ph. D. degree. His research concerns radio resource optimization.

Email: zhuhb@ cqupt. edu. cn