基于模糊博弈规则的网络节点入侵风险评估

刘建峰[1] 陈 健[2]

(南京大学网络信息中心 南京 210023)[1] (南京大学计算机科学与技术系 南京 210023)[2]

摘 要 为了实时评估网络安全状态,弥补传统网络节点入侵风险评估方法评估精度低、实用性差的不足,提出一种新的基于模糊博弈规则的网络节点入侵风险评估方法。该方法通过一组有限状态集合对网络进行描述,给出博弈双方的收益矩阵和模糊博弈元素,获取入侵者和网络节点的预期收益,在此基础上给出模糊博弈规则;通过模糊博弈规则,依据资产、威胁、弱点以及风险要素构建风险评估模型;完成策略成本与收益的量化处理后,建立网络节点模糊博弈树,求出纳什均衡;结合入侵者和网络节点的收益函数,获取模糊博弈规则下网络节点风险期望,确定网络节点入侵风险值,并依据阈值判断是否需报警,以防止网络节点被入侵。实验结果表明,所提方法的评估精度高、可靠性和实用性强。

关键词 模糊博弈规则,网络节点,入侵,风险,评估

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.10.026

Evaluation of Network Node Invasion Risk Based on Fuzzy Game Rules

LIU Jian-feng[1] CHEN Jian[2]

(Network Information Center, Nanjing University, Nanjing 210023, China)[1]

(Department of Computer Science and Technology, Nanjing University, Nanjing 210023, China)[2]

Abstract In order to evaluate network security state in real time and make up for the shortcomings of low accuracy and poor practicability of traditional network node intrusion risk assessment method, a new network node intrusion risk assessment method based on fuzzy game rules was proposed. A set of finite state sets is used to describe the network, and the benefit matrix and fuzzy game elements are given to obtain the expected income of intruders and network nodes. On this basis, the fuzzy game rules are given. The risk assessment model is constructed according to the assets, threats, weaknesses and risk factors through the fuzzy game rules. After the quantification of the strategy cost and income, the fuzzy game tree of the network node is established, and the nash equilibrium is obtained. Combined with the income function of intruders and network nodes, the expectation of network nodes' risk under fuzzy game rules is obtained, and the value of network node's intrusion risk is determined. The threshold value is used to judge whether alarm is needed to prevent the network node from being invaded. Experimental results show that the proposed method has high accuracy, reliability and practicability.

Keywords Fuzzy game rule, Network node, Intrusion, Risk, Evaluation

当前网络发展迅速,给人们的工作和生活带来了很大的改变,但其共享性、多样性和公开性的特性,导致网络节点容易遭遇入侵,使网络受到攻击[1]。若网络节点受到攻击,则会对网络中的用户产生很大的影响,使得损失大大增加[2]。对网络节点入侵风险进行评估,同时通过评估结果在节点遭遇入侵前采取相应的措施来降低入侵概率,则可大大增强网络的安全性,因此研究一种有效的网络节点入侵风险评估方法意义重大。本文提出了基于模糊博弈规则的网络节点入侵风险评估方法,为提高网络安全性提供了重要依据。

1 模糊博弈规则描述

在入侵者与网络节点进行博弈时,入侵者会利用不同的方式得到所需数据或者损坏网络节点,而网络节点会针对入侵者的入侵行为采取相应措施来尽可能地降低入侵导致的损失[3-4]。在进行模糊博弈时,网络节点想要达到的结果和采取的防御措施不仅与网络节点自身有关,还与入侵者的行为有关[5],因此研究网络节点入侵风险模糊问题时可选用模糊博弈规则。

入侵者与网络节点的博弈属于非合作博弈,同时不同行为都有独立性,因此需求解纳什均衡。博弈双方(即入侵者与网络节点)的收益必须采用相同的单位[6]。

通过一组有限状态集合对网络进行描述,$T=\{t_1,\cdots,t_i\}$;在网络处于 t_i 状态时,入侵者和网络节点的博弈过程被称作一个博弈元素,用 Λ_i 进行描述,则博弈双方的收益矩阵如图 1 所示。

到稿日期:2017-08-14 返修日期:2018-01-21 本文受国家下一代互联网信息安全专项试点计划课题(2012BAH01B01)资助。

刘建峰(1979-),男,硕士,工程师,主要研究方向为网络架构、IPV6、安全、大数据分析,E-mail:ljf@nju.edu.cn(通信作者);陈 健(1973-),男,硕士,高级工程师,主要研究方向为计算机网络、计算机网络安全。

入侵者 \ 网络节点	e_1	…	e_m
b_1	s_{11},o_{11}		s_{1m},o_{1m}
⋮	⋮	⋱	⋮
b_m	r_{m1},o_{m1}	…	r_{mm},o_{mm}

图 1　博弈双方的收益矩阵

Fig. 1　Game payoff matrix

图 1 中，s_{kl} 用于描述入侵者采取入侵行为 b_k 时网络节点采取相应防御措施 e_l 情况下的收益；o_{kl} 用于描述网络节点被 b_k 入侵后，采取措施 e_l 时的收益，其中 $1\leqslant k,l\leqslant m$。模糊博弈元素 Λ_i 如式(1)所示：

$$\Lambda_i=\begin{matrix}[e_1,\cdots,e_m]\\ \begin{bmatrix}\eta_{11} & \cdots & \eta_{1m}\\ \vdots & \ddots & \vdots\\ \eta_{m1} & \cdots & \eta_{mm}\end{bmatrix}\end{matrix}\begin{bmatrix}b_1\\ \vdots\\ b_m\end{bmatrix} \tag{1}$$

其中，$\eta_{kl}=s_{kl}+\sum_{\forall \Lambda_j}Q_{ij}(b_k,e_l)\Lambda_j$，$0<Q_{ij}(b_k,e_l)<1$ 用于描述入侵者采取入侵行为 b_k 时，网络节点采取防御措施 e_l 时网络由状态 t_i 转移至 t_j 的概率[7]；η_{kl} 用于描述入侵者得到的后续收益。

入侵者预期得到的收益为：

$$F(\Psi_i,\Omega_i)=\sum_{\forall b_k\in B_i}\sum_{\forall e_l\in E_i}\kappa_i(b_k)\vartheta_i(e_l)\eta_{kl} \tag{2}$$

网络节点预期收益为：

$$F(\Omega_i,\Psi_i)=\sum_{\forall e_l\in E_i}\sum_{\forall b_k\in B_i}\vartheta_i(e_l)\kappa_i(b_k)o_{kl} \tag{3}$$

在网络状态为 t_i 时，入侵者的入侵行为概率分布为 $\Psi_i(\kappa_i(b_1),\cdots,\kappa_i(b_m))$，其中 $\kappa_i(b_1)$ 用于描述入侵者选择入侵行为 b_1 的可能性[8]；在网络节点状态为 t_i 时，网络节点防御措施的概率分布为 $\Omega_i=(\vartheta_i(e_1),\cdots,\vartheta_i(e_m))$，其中 $\vartheta_i(e_1)$ 用于描述网络节点采取防御措施 e_1 的概率。

模糊博弈规则为：令入侵者自身收益达到最大，令网络节点尽可能降低入侵者的收益，即 $\min\limits_{\Omega_i}\max\limits_{\Psi_i}F(\Psi_i,\Omega_i)$。并且入侵者还需达到最小化网络节点收益的目的，网络节点则需令自身收益达到最大，即 $\max\limits_{\Psi_i}\min\limits_{\Omega_i}F(\Omega_i,\Psi_i)$。因此，在网络处于 t_i 状态下，双方采用的策略需达到纳什均衡，入侵者与网络策略依次是 Ψ_i^* 与 Ω_i^*，则 $F(\Psi_i^*,\Omega_i^*)=-F(\Omega_i^*,\Psi_i^*)$。

2　网络节点入侵风险评估方法

对网络节点的风险进行评估时，主要要素包括资产、威胁、弱点以及风险[9]，依据这些要素给出常用的风险评估模型，如图 2 所示。

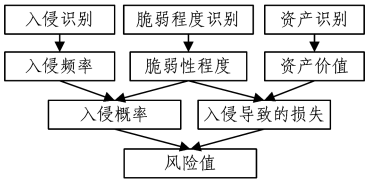

图 2　风险评估模型

Fig. 2　Risk assessment model

网络节点入侵风险如式(4)所示：

$$U=u(C,W,Z)=U(J,P(W,Z)) \tag{4}$$

其中，U 表示风险，C 表示资产，W 表示资产脆弱程度，Z 表示威胁，J 表示入侵对网络节点产生的影响，P 表示借助资产脆弱特性入侵导致安全事件出现的概率。

本节利用入侵出现概率 P 与入侵可能导致的后果 J 来进行网络节点入侵风险的评估。对网络节点入侵风险进行评估时，在博弈双方不了解对方信息的状态下，综合分析入侵行为与防御行为的收益较为复杂，因此可在模糊博弈规则下实现[10]。

网络中包含多个风险子域，不同风险子域采用相同的防御行为。入侵者都是相互独立的，因此能够根据风险子域中的网络节点构建模糊博弈场景[11]。

实现策略成本与收益的量化处理后，建立网络节点模糊博弈树，求出纳什均衡 $F(\Psi_i^*,\Omega_i^*)=-F(\Omega_i^*,\Psi_i^*)$。在模糊博弈规则中，网络节点对入侵者在正常情况下采取的入侵行为进行预测[12-13]，预测结果就是纳什均衡，$F(\Psi_i^*,\Omega_i^*)=\{F(\Psi_1^*,\Omega_1^*),F(\Psi_2^*,\Omega_2^*),\cdots,F(\Psi_n^*,\Omega_n^*)\}$，即 $F(\Psi_i^*,\Omega_i^*)$ 与入侵出现概率 P 相一致。而网络节点收益函数 $F(\Omega_i,\Psi_i)$ 实际上是入侵导致网络节点产生的损失，也就是入侵出现的可能结果 J。在实际应用中，网络节点采取的防御策略是固定的[14]。假设网络节点采用的防御策略用 e_l 进行描述，结合上述入侵者和网络节点的收益函数，即可获取该模糊博弈规则下网络节点的风险期望，如式(5)所示：

$$\begin{aligned}U&=U(J,P(W,Z))\\&=\sum_{i=1}^{k_i}P(\Psi_i^*,\Omega_i^*)\sum_{i=1}^{m}F(\Psi_i^*,\Omega_i^*)\frac{|e_l|}{\max|e_l|}\end{aligned} \tag{5}$$

分析不同风险子域的风险状态，即可获取不同风险子域的风险向量 $(U_1,U_2,\cdots,U_n)$。假设安全风险子域的资产价值向量为 $C=(C_1,C_2,\cdots,C_n)$，对其进行归一化处理，即可获取权向量 $X=(x_1,x_2,\cdots,x_n)$，则网络节点入侵风险为：

$$U_{all}=\sum_{j=1}^{n}U_j\cdot x_j \tag{6}$$

依据历史入侵数据确定网络节点入侵风险阈值，在评估的网络节点入侵风险值超过阈值的情况下，需报警，以防网络节点被入侵[15]。

3　实验结果与分析

3.1　实验网络

为了验证本文提出的基于模糊博弈规则的网络节点入侵风险评估方法的有效性，本节设计了一个如图 3 所示的简化的网络实例进行实验。

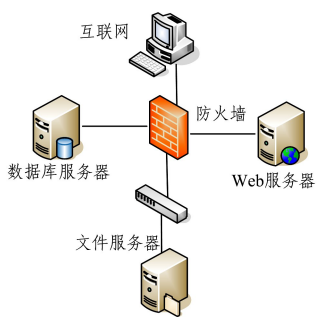

图 3　网络实例结构

Fig. 3　Network example structure

针对上述网络实例，存在下述准则：

1)入侵者在外网中存在 Root 权限，同时在外网中入侵网络节点；

2)防火墙对内网和外网进行划分，其规则如表 1 所列。

表 1 防火墙规则

Table 1 Firewall rules

源主机	目的主机	服务	访问策略
所有服务器	网络服务器	网络	允许
所有服务器	网络服务器	文件传输	允许
所有服务器	文件服务器	文件传输	允许
网络服务器	数据库服务器	数据库	允许
文件服务器	数据库服务器	文件传输	允许

3)通过弱点扫描软件对网络节点的弱点进行研究，获取的弱点信息入侵 AL 值与发现入侵后的惩罚代价相对应，如表 2 所列。

表 2 服务器弱点信息和 AL

Table 2 Server vulnerability information and AL

主机	操作系统	对应攻击的 AL	对应惩罚代价
网络服务器	Linux	12	115
文件服务器	Linux	6	75
数据库服务器	Linux	9	105

3.2 评估精度测试

假设在时间 T 内对实例网络进行监测，发现 4 种不同类型的入侵，依次用 G_1，G_2，G_3，G_4 进行描述。把监测时间 T 划分成 6 个相同的时段，每个时段用 t_i 进行描述。在不同时段，分别采用本文方法、贝叶斯方法和卡尔曼方法对实例网络节点的入侵风险进行评估，得到的报警结果和风险值如表 3 所列。

表 3 3 种方法的报警情况和风险值的比较结果

Table 3 Comparison of alarm and risk values of three methods

时段	本文方法		贝叶斯方法		卡尔曼方法	
	报警结果	风险值	报警结果	风险值	报警结果	风险值
t_1	G_1	0.16	G_2	0.15	G_2，G_3	0.26
t_2	G_1，G_2，G_4	0.42	G_1	0.13	G_1，G_2，G_4	0.45
t_3	G_2	0.13	G_2，G_3	0.27	G_1，G_2，G_5	0.47
t_4	G_1，G_3	0.21	G_1，G_3，G_2	0.46	G_1，G_4	0.29
t_5	无	0.00	G_4	0.16	G_1	0.12
t_6	G_4	0.15	G_2	0.16	G_2	0.15

依据表 3 中的数据，引入实际风险值数据绘制折线图，从而获取网络节点的风险评估曲线，得到的结果如图 4 所示。

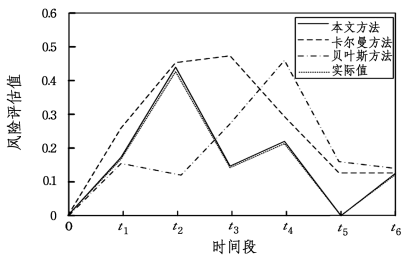

图 4 3 种方法的风险评估结果

Fig. 4 Risk assessment results of three methods

由表 3 和图 4 可知，使用本文方法对网络节点入侵风险进行评估时，在 t_2 时段网络节点遭遇的攻击类型最多，风险值高达 0.42，与实际风险值相符。且通过本文方法得到的整个风险评估曲线与实际结果最相符，明显优于贝叶斯方法和卡尔曼方法，这说明本文方法的评估精度最高，验证了其有效性。

3.3 评估结果实例测试

图 5 给出了网络节点覆盖区域的客观描述。不受控制的网络节点是无法进行全面覆盖的，而体积较大的蜂窝型节点为正常节点，能够为相邻节点提供屏蔽层，保护网络，也就是说此类节点是入侵者需要攻陷的头号敌人。令网络节点遭遇入侵，分别采用本文方法、贝叶斯方法和卡尔曼方法对网络节点入侵风险进行评估，通过节点变化情况评估方法的实用性。

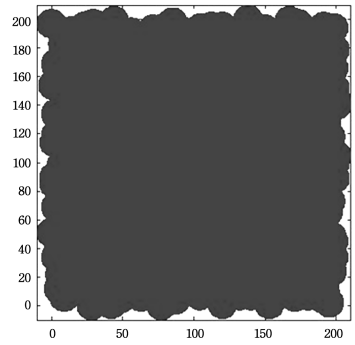

图 5 网络节点的客观描述

Fig. 5 Objective description of network node

图 6 给出了使用本文方法评估网络节点风险时得到的节点变化情况。由图 6 可知，将本文方法应用于实际网络后，部分网络节点死亡，这主要是因为在遭遇入侵后，网络节点的覆盖区域减小，以阻止入侵者达到网络节点中间的核心部位完成对节点的控制，从而实现网络节点防护。

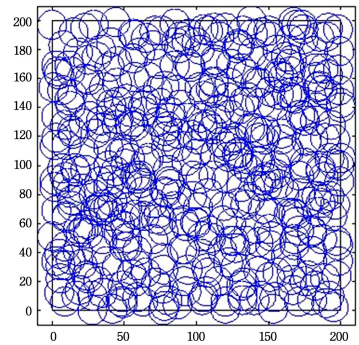

图 6 本文方法下网络节点的变化情况

Fig. 6 Change of network node under proposed method

图 7 和图 8 依次是将卡尔曼方法和贝叶斯方法应用于真实的被入侵网络时，网络节点的变化情况。

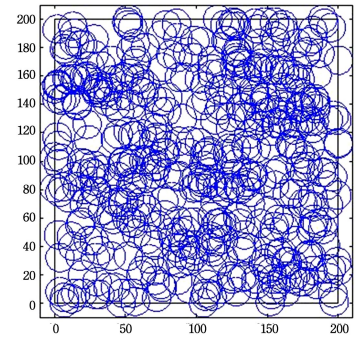

图 7 卡尔曼方法下网络节点的变化情况

Fig. 7 Change of network node under Calman method

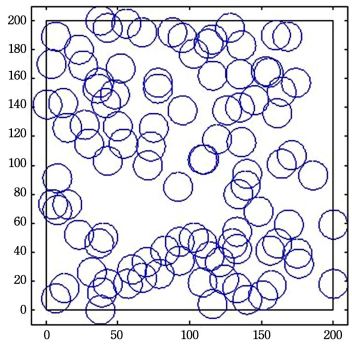

图 8　贝叶斯方法下网络节点的变化情况

Fig. 8　Change of network node under Bayesian method

分析图 7 和图 8 可以看出，在网络节点遭遇入侵时，通过卡尔曼方法和贝叶斯方法对网络节点入侵进行风险评估后，网络节点的覆盖区域发生了很大的改变，虽然部分节点的覆盖区域增大，但不符合客观情况，因此本文方法的评估结果的实用性更高。

结束语　本文提出了一种新的基于模糊博弈规则的网络节点入侵风险评估方法，并介绍了模糊博弈规则。该方法对策略成本与收益进行量化处理，建立网络节点模糊博弈树，并求出纳什均衡，从而确定网络节点的入侵风险值。实验结果表明，所提方法对网络节点入侵风险进行评估时的可靠性和实用性更强。

参 考 文 献

[1] LIU W F, ZHANG S W, GONG X. An Improved Network Risk Evaluation Method Based on Markov Game[J]. Telecommunications Science, 2014, 30(7): 13-18. (in Chinese)
刘文芬，张树伟，龚心. 一种优化的基于 Markov 博弈理论的网络风险评估方法[J]. 电信科学，2014，30(7)：13-18.

[2] ZHANG J, WANG J D, ZHANG H W, et al. Network Risk Analysis Method Based on Node-Game Vulnerability Attack Graph[J]. Computer Science, 2014, 41(9): 169-173. (in Chinese)
张健，王晋东，张恒巍，等. 基于节点博弈漏洞攻击图的网络风险分析方法[J]. 计算机科学，2014，41(9)：169-173.

[3] LEI J G. Simulation of Game Detection under Unbalanced Invasion Characteristics[J]. Computer Simulation, 2015, 32(9): 307-310. (in Chinese)
雷剑刚. 不平衡网络入侵特征下的博弈检测仿真[J]. 计算机仿真，2015，32(9)：307-310.

[4] LAI C, CHEN X, CHEN X, et al. A fuzzy comprehensive evaluation model for flood risk based on the combination weight of game theory[J]. Natural Hazards, 2015, 77(2): 1243-1259.

[5] GUI M Q, LIU Y B, ZHOU L Y. Intrusion detection based on game theory in wireless sensor network [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2016, 28(3): 414-420. (in Chinese)
桂明倩，刘宴兵，周嘹永. WSN 中基于博弈理论的入侵检测研究[J]. 重庆邮电大学学报(自然科学版)，2016，28(3)：414-420.

[6] REN L C, LI Z F. A New Model Based on the Games Theory and Fuzzy Mathematics in Bridge Engineering Risk Assessment [J]. Highway Engineering, 2017, 42(1): 163-169. (in Chinese)
任丽超，栗振锋. 基于博弈论和模糊数学的桥梁风险评价模型[J]. 公路工程，2017，42(1)：163-169.

[7] YU D K, WANG J D, ZHANG H W, et al. Risk assessment selection based on static Bayesian game[J]. Computer Engineering and Science, 2015, 37(6): 1079-1086. (in Chinese)
余定坤，王晋东，张恒巍，等. 基于静态贝叶斯博弈的风险评估方法研究[J]. 计算机工程与科学，2015，37(6)：1079-1086.

[8] XIE Q L. Design of wireless sensor network the sink node based on OK6410 [J]. Electronic Design Engineering, 2016, 24(6): 159-161. (in Chinese)
谢巧玲. 基于 OK6410 的无线传感器网络汇聚节点设计[J]. 电子设计工程，2016，24(6)：159-161.

[9] HAN L, SONG Y, DUAN L, et al. Risk assessment methodology for Shenyang Chemical Industrial Park based on fuzzy comprehensive evaluation[J]. Environmental Earth Sciences, 2015, 73(9): 5185-5192.

[10] SHI L B, JIAN Z. ulnerability Assessment of Cyber Physical Power System Based on Dynamic Attack-defense Game Model [J]. Automation of Electric Power Systems, 2016, 40(17): 99-105. (in Chinese)
石立宝，简洲. 基于动态攻防博弈的电力信息物理融合系统脆弱性评估[J]. 电力系统自动化，2016，40(17)：99-105.

[11] HUANG L L, YAO A L, XIAN T, et al. Research on risk assessment method of oil & gas pipeline with consideration of vulnerability[J]. China Safety Science Journal, 2014, 24(7): 93-99. (in Chinese)
黄亮亮，姚安林，鲜涛，等. 考虑脆弱性的油气管道风险评估方法研究[J]. 中国安全科学学报，2014，24(7)：93-99.

[12] ZHANG H W, ZHANG J, HAN J H, et al. Vulnerability risk analysis method based on game model and risk matrix[J]. Computer Engineering and Design, 2016, 37(6): 1421-1427. (in Chinese)
张恒巍，张健，韩继红，等. 基于博弈模型和风险矩阵的漏洞风险分析方法[J]. 计算机工程与设计，2016，37(6)：1421-1427.

[13] ZHANG Y. Research on the computer network security evaluation based on the DHFHCG operator with dual hesitant fuzzy information[J]. Journal of Intelligent & Fuzzy Systems, 2015, 28(1): 199-204.

[14] XI R R, YUN X C, ZHANG Y Z, et al. An Improved Quantitative Evaluation Method for Network Security[J]. Chinese Journal of Computers, 2015, 38(4): 749-758. (in Chinese)
席荣荣，云晓春，张永铮，等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报，2015，38(4)：749-758.

[15] SONG Y U, CHENE J. Research of Aircraft Maintenance Unit Risk Management Based on the Generalized Linear Regression Model[J]. Bulletin of Science and Technology, 2016, 32(1): 215-219. (in Chinese)
宋云雪，陈金. 基于广义线性回归模型的飞机维修单位风险管理研究[J]. 科技通报，2016，32(1)：215-219.

[16] DAI W. Application of Intrusion Detection Technology in Network Security[J]. Journal of Chongqing Institute of Technology, 2018, 32(4): 156-160, 185. (in Chinese)
代威. 入侵检测技术在网络安全中的应用[J]. 重庆理工大学学报(自然科学)，2018，32(4)：156-160，185.