模块化动态博弈的网络可生存性态势跟踪方法

伍文，孟相如，马志强，陈铎龙
（空军工程大学信息与导航学院，710077，西安）

摘要：针对网络系统中可生存性能实时评估和生存决策能力的有效提高问题，提出了一种基于模块化动态博弈的网络可生存性态势跟踪方法.该方法根据提出的模块化动态博弈思想，将攻防双方的动态博弈过程分为抵抗、检测、容忍生存3个阶段，结合可生存性问题，给出了动态博弈的数学描述及3个生存阶段的动态博弈扩展式，将博弈收益量化结果转化为二维的可生存性态势评估结果.实验结果表明，该方法可依据网络现有的攻防数据，对网络系统遭遇的生存威胁，以及网络系统本身面对威胁的可生存能力进行实时跟踪评估，使网络系统的生存评估和决策能力得到了提高.

关键词：网络可生存性；动态博弈；收益量化
中图分类号：TP393.07 **文献标志码**：A **文章编号**：0253-987X(2012)12-0018-06

Tracking Network Survivability Situation Based on Modularized Dynamic Game

WU Wen, MENG Xiangru, MA Zhiqiang, CHEN Duolong
(School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China)

Abstract: A tracking method of network survivability situation following dynamic game theory was proposed to improve the ability of real time performance evaluation and decision-making of network survivability. A modularized dynamic game evaluation model was given, which divided dynamic game process of attacker and protector into three phases, ie. resistance, recognition and recover. Then the mathematical description of dynamic game and the game tree expression of each phase game process aiming at survivability were constructed. A new income calculating scheme suitable for survivability situation awareness was proposed in final planar form. The simulations show that the proposed method enables to obtain the real time evaluation of network survivability according to the existing attacking and protecting data acquired from network system, which contains both the threat the network system encountered and the survivability of network itself. The network system's capability of survivability evaluation and decision-making is thus improved.

Keywords: network survivability; dynamic game theory; income calculation

网络可生存性概念起源于军事领域，是继可靠性、可用性、安全性、可依赖性之后，对网络性能进行评价的又一重要概念，相比其他概念，可生存性涵盖的研究范围更广，并强调网络业务运行的持续性，因此近些年得到了人们较多的关注[1-4].

1999年，Bass等人[5-6]提出了网络态势感知的概念，至今已经发展成网络领域的一个热门研究方向.在网络可生存性态势感知方面，文献[7]给出了一种通过态势感知技术来提高可生存网络自适应能力的方法，将态势感知技术应用于可生存性问题中.

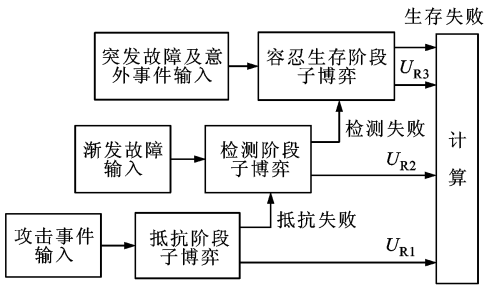
收稿日期：2012-03-21. 作者简介：伍文(1985—)，女，博士生；孟相如(通信作者)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(61003252)；全军军事学研究生课题(2011JY002—524)；空军工程大学信息与导航学院博士生创新基金资助项目(20110501).
网络出版时间：2012-10-31 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20121031.1106.001.html

文献[8]提出了一种从信息融合角度对网络可生存性进行评估的方法,但这些方法均未明确提出网络可生存性态势感知的概念,仅在思想上与可生存性态势感知相似. 文献[9-10]借鉴传统评估方法对网络可生存性态势进行了评估.

通过网络攻防行为建模对网络安全态势进行评估,已成为当前网络安全领域的研究热点[11]. 可生存性态势评估研究作为安全态势评估的发展和延续尚处于起步阶段,对网络可生存性态势评估的研究可借鉴安全态势的研究成果,结合可生存性的特点来构建适合于可生存性的评估模型. 本文基于此思想,提出了一种基于博弈理论的网络可生存性态势评估模型,先构建了可生存性态势感知的框架体系,其次提出了一种模块化的可生存性动态博弈模型,并给出了具体的量化评估方法,最后通过仿真说明了评估方法的有效性.

1　模块化动态博弈框架

为了降低模型的复杂度,本文提出了一种模块化的网络可生存性态势评估博弈模型,如图 1 所示. 可生存的 3 个重要属性——抵抗、检测和容忍生存是依次进行的,具有阶段性,且相互独立. 图 1 中当攻击事件发生后,首先与抵抗阶段的策略进行博弈,抵抗失败后,与检测阶段策略进行博弈,检测失败后再与容忍生存阶段策略进行博弈,容忍生存失败后系统针对该事件的生存机制则失效. 将故障分为渐发故障和突发故障,渐发故障是逐渐发生并影响网络的,因此认为渐发故障在产生初期可被故障检测系统检测到并进行处理,在模型中首先与检测阶段策略进行博弈,失败后再与容忍生存阶段策略进行博弈. 突发故障和意外事件在发生初始时,对网络性能可造成明显的影响,因此系统主要依赖容忍生存策略来削减其负面的影响.



$U_{R1}\sim U_{R3}$:分别表示由抵抗、检测、容忍生存阶段计算得到的收益值

图 1　模块化博弈示意图

2　可生存动态博弈模型

2.1　模型描述

在网络攻防过程中,参与人依次根据已有信息采取行动[12],因此采用动态博弈对图 1 中的博弈子模块进行分析. 动态博弈模型采用四元组(P,H,A,U)来表述.

(1)P 表示参与人集合,$P=\{\{P_A,P_F\},\{P_D\}\}$,$P_A$ 是指人为恶意攻击一方,它具备分析决策能力,可理性判断应该采取的行动. P_F 是指网络遭遇的故障和意外事件,具有随机性,服从一定的分布,但不具备理性分析能力,在博弈模型中也不分配策略集. P_D 是指网络防御者,通过实施各种防御策略达到对网络保护的目的.

(2)H 表示博弈的历史集,$H=\{h^k\mid k=1,2,\cdots,K\}$,其中,$h^k=(a^1,a^2,\cdots,a^{k-1})$表示 k 阶段的博弈历史(对于无限阶段数的博弈,$K=\infty$),$a^i\equiv(a_1^i,a_2^i,i=1,2,\cdots,k-1)$表示 i 阶段攻防双方的行动组合.

(3)A 表示行动策略集,$A=\{A_A,A_D\}$,其中 A_A 表示攻击方策略集,A_D 表示防御方策略集. 攻击方策略集又分为初始策略集 A_A^o 和行进间策略集 A_A^g,则 $A_A=\{A_A^o,A_A^g\}$. A_A^o 包含网络攻击者在攻击初始可选的策略,例如病毒、木马、蠕虫等. A_A^g 包含攻击者在确定攻击策略并实施后在动态各阶段的可选行动,例如继续攻击、停止攻击,停留观察等. 防御方策略分为策略防御集 A_D^{st} 和改进策略集 A_D^{im},$A_D=\{A_D^{st},A_D^{im}\}$. A_D^{st} 包含防御方的各类防御策略,例如防火墙、入侵检测等. A_D^{im} 是指防御策略的改进方式,例如针对防御策略防火墙,改进策略为增加对某 IP 地址的过滤等.

(4)U 表示参与人的收益函数. 在博弈的每一个阶段 k,参与人都有收益 $g(a^k)$. 用 H^k 表示所有阶段 k 的历史,则每个参与人在完整博弈的条件下,其收益表示一个函数 $u:H^K\rightarrow\mathbf{R}$,在大部分动态博弈中,参与人的收益函数都是阶段可加、可分离的,即 u 是 $g(a^k)$的某种加权平均.

2.2　博弈模块的扩展式表示

动态博弈扩展式是以树型结构将动态博弈过程形象直观地表示出来的一种博弈表达方式,并以示例的方式分别给出模块化博弈的 3 个模块的动态博弈扩展式.

2.2.1　抵抗阶段子博弈　由 $P=\{P_A,P_D\}$得到的

策略集如下:攻击初始策略集={木马,蠕虫,拒绝服务攻击},攻击行进间策略集={继续攻击,停止攻击};策略防御集={防火墙,认证};防御改进策略集为空集.在抵抗阶段子博弈中,攻击方采取主动策略,防御方则采取被动策略,为了简化模型,认定网络具备防火墙和认证系统两道防御措施,不做策略选择,扩展式如图2所示.

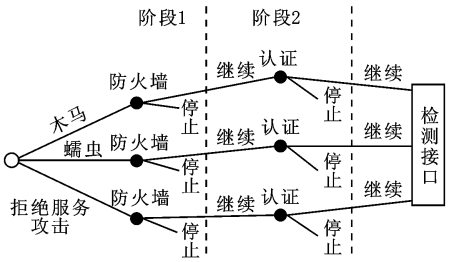


图2 抵抗阶段的博弈扩展式

2.2.2 检测阶段子博弈 由$P=\{P_A,P_F,P_D\}$得到的策略集分别为:攻击初始策略集={木马继续攻击,蠕虫继续攻击,拒绝服务继续攻击};攻击行进间策略集为空集;策略防御集={检测,不检测};防御改进策略集为空集.在检测阶段,攻击为被动攻击状态,不进行策略选择,防御系统具有主动权,可选择进行入侵检测和不检测策略.渐发故障以事件形式触发,由故障检测系统进行检测,在模型中简单认为检测到即可及时处理,扩展式如图3所示.

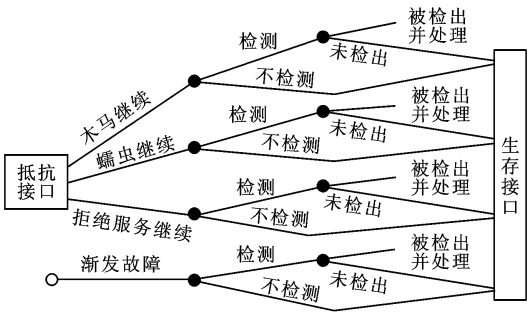


图3 检测阶段的博弈扩展式

2.2.3 生存容忍阶段子博弈 由$P=\{P_A,P_F,P_D\}$得到的策略集分别为:攻击初始策略集={恶意攻击继续};攻击行进间策略集={继续攻击,停止攻击};策略防御集={容忍,动态修复};防御改进策略集为空集.在生存容忍阶段,突发故障和意外灾害不是人为可控的,而是随机发生并以事件的形式触发的.防御方策略容忍包括多样化配置、冗余、备份等,动态修复策略包括服务漂移、IP地址重路由、光层重配置等.扩展式如图4所示.

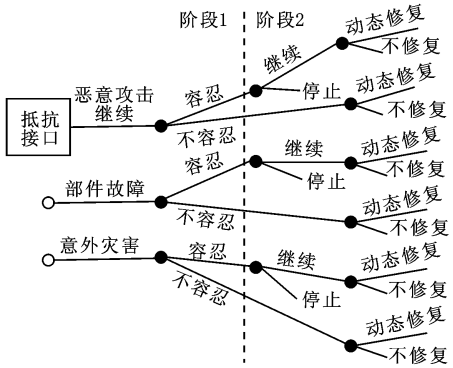


图4 生存阶段的博弈扩展式

3 收益计算及态势量化

将收益的相关定义[13]表述如下.

定义1 攻击回报A_R是指攻防博弈中,攻击者在一个阶段得到的益处.对大多攻击者而言,A_R的大小取决于系统受到的威胁及损害的大小.

定义2 攻击代价A_C是指攻击者实施一次攻击所需要消耗的资源、人力等代价.

定义3 防御回报D_R是指攻防博弈中,防御者在一个阶段得到的益处.D_R的大小取决于防御系统针对攻击事件所能发挥的防御作用的大小.

定义4 防御代价D_C是指防御者实施一次防御所需要消耗的资源、人力等代价.

可生存动态博弈的第i个博弈模块在k阶段时,攻防双方的收益向量为

$$\boldsymbol{g}^i(h^k)=\begin{pmatrix}g_A^i(h^k)\\ g_D^i(h^k)\end{pmatrix} \tag{1}$$

式中:$g_A^i(h^k)$为k阶段攻击方的收益;$g_D^i(h^k)$为k阶段防御方的收益.双方收益如下

$$g_A^i(h^k)=A_R^i(h^k)-A_C^i(h^k) \tag{2}$$

$$g_D^i(h^k)=D_R^i(h^k)-D_C^i(h^k) \tag{3}$$

式中:$A_R^i(h^k)$、$A_C^i(h^k)$、$D_R^i(h^k)$及$D_C^i(h^k)$的值参考文献[13]中的方法进行量化.将攻防策略划分类别及层次,再根据攻击造成的危害程度、持续时间,恢复策略的恢复时间、恢复程度,以及人力与资源消耗,软硬件成本等信息由管理员来拟定.

第i个博弈模块在历史为h^{K_i}时攻防双方的收益向量为

$$\boldsymbol{u}^i(h^{K_i})=\begin{pmatrix}u_A^i(h^{K_i})\\ u_D^i(h^{K_i})\end{pmatrix} \tag{4}$$

$\boldsymbol{u}^i(h^{K_i})$可根据博弈模块$i$中的$\boldsymbol{g}^i(h^k)$加权求和得到,即

$$\boldsymbol{u}^i(h^{K_i})=\sum_{k=1}^{K_i}\begin{bmatrix}Q & 0\\ 0 & 1/Q\end{bmatrix}^{k-1}\boldsymbol{g}^i(h^k)$$
$$Q\geqslant 1;\ i=1,2,3 \tag{5}$$

式中:Q 为奖励因子. 对于每一个模块,当攻击每前进一个阶段,攻击者将更具威胁性,而防御方则面临更大的威胁,因此定义 Q 对阶段间的收益进行调节,Q 的选取将直接影响态势评估的结果. Q 的取值范围一般在 1、2 之间,当 $Q<1$ 时,则无法体现出随着博弈阶段的渐进攻击方威胁增加的趋势,而 Q 取值太大则会忽视前期博弈阶段的作用. 因此,Q 值的确定应依据系统对生存性的需求,例如对于威胁敏感、生存性要求高的系统,Q 的取值应大一些,反之则取小一些.

在得到每一个模块的收益值 $\boldsymbol{u}^1(h^{K_1})$、$\boldsymbol{u}^2(h^{K_2})$、$\boldsymbol{u}^3(h^{K_3})$后,根据下式计算得到最终收益

$$\boldsymbol{U}^{\mathrm{T}}=(\boldsymbol{u}^1(h^{K_1}),\boldsymbol{u}^2(h^{K_2}),\boldsymbol{u}^3(h^{K_3}))\cdot\boldsymbol{\omega}=(U_{\mathrm{A}},U_{\mathrm{D}}) \tag{6}$$
$$\boldsymbol{\omega}=(\omega_1,\omega_2,\omega_3)^{\mathrm{T}}$$

式中:U_{A}、U_{D} 分别为攻防双方的收益;$\boldsymbol{\omega}$ 为 3 个模块的收益权重向量,由评估者根据实际需求来确定.

对攻防双方收益进行标准化后,得到一次攻击对网络可生存性态势的影响值

$$U_{\mathrm{A}}^0=U_{\mathrm{A}}/U_{\mathrm{Am}} \tag{7}$$
$$U_{\mathrm{D}}^0=U_{\mathrm{D}}/U_{\mathrm{Dm}} \tag{8}$$

式中:U_{Am}、U_{Dm}分别表示攻防双方收益的最大值. 由于威胁会产生一个阶段的持续影响,因此以滑动窗口的形式来计算态势值. 将 T 时刻的可生存态势值记为 $S(T)=(S_{\mathrm{th}}(T),S_{\mathrm{sa}}(T))$,其中 $S_{\mathrm{th}}(T)$表示 T 时刻攻击、故障及意外事件对网络可生存性造成的威胁程度,$S_{\mathrm{sa}}(T)$表示针对面临的威胁,系统的可生存能力,即

$$S_{\mathrm{th}}(T)=\sum_{\substack{t\in(T-\Delta t,T)\\ n_j\in N_{\mathrm{a}}}}\gamma_{n_j}U_{\mathrm{A}}^0(t,n_j) \tag{9}$$

$$S_{\mathrm{sa}}(T)=\sum_{\substack{t\in(T-\Delta t,T)\\ n_j\in N_{\mathrm{a}}}}\gamma_{n_j}U_{\mathrm{D}}^0(t,n_j)\Big/\sum_{n_j\in N_{\mathrm{a}}}\gamma_{n_j} \tag{10}$$

式中:n_j 为网络中第 j 个节点;N_{a} 为遭受攻击的节点集;γ_{n_j} 为节点的重要度,由节点类型、节点连接度、节点服务量等决定.

4　实例分析

为了对给出的可生存性态势评估方法的有效性进行验证,采用图 5 所示的网络拓扑结构对网络攻防场景进行模拟. 攻击者通过外网对内网的各个节点实施攻击,内网的路由器配置防火墙,作为保护内网的第一道屏障,通过交换机将 Web 服务器、文件服务器和个人电脑连接,其中在 2 个服务器和个人电脑上配置的 IDS 设备,是保护内网关键设施的第 2 道屏障. 由于未配置故障检测机制,因此将渐进故障和突发故障视为同类故障一起来处理,内网路由器的故障可通过备份路由器进行恢复,对于服务器和个人电脑也提供了备份和自动恢复机制.

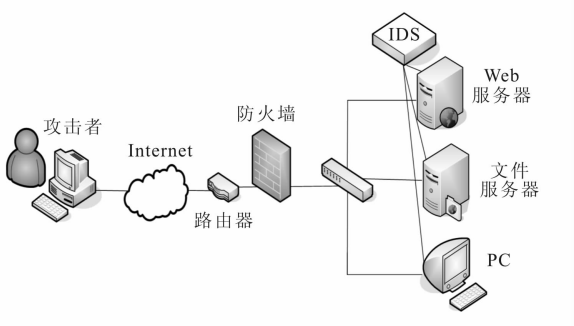


图 5　网络拓扑结构图

根据给出的网络攻防场景,建立的模块化动态博弈模型如图 6 所示. 为了简化评估过程,假设各节点类型在遭遇故障后的反应是相似的. 以模块 1 中的收益计算为例来说明收益的量化过程,以量化方法[13]为依据,由管理员给出模块 1 中各阶段的数据(见表 1、表 2).

表 1　攻击方数据

攻击状态	阶段 1		阶段 2	
	A_{R}/元	A_{C}/元	A_{R}/元	A_{C}/元
木马	5	4	5	4
蠕虫	6	4	6	4
拒绝服务	8	5	8	5

表 2　防御方数据

攻击状态	防火墙数据		认证数据	
	D_{R}/元	D_{C}/元	D_{R}/元	D_{C}/元
木马攻击继续	10	2	10	1
木马攻击停止	20	2	20	1
蠕虫攻击继续	15	2	15	1
蠕虫攻击停止	25	2	25	1
拒绝服务攻击继续	20	2	20	1
拒绝服务攻击停止	30	2	30	1

取 $Q=1.25$,$\boldsymbol{\omega}=(1,1,1)^{\mathrm{T}}$,根据表 1、表 2 中的数据,由式(4)计算得到博弈模块 1 中的末端数据,同理,可计算得到其他模块阶段的末端数据,攻防双方在各阶段的收益如图 6 所示.

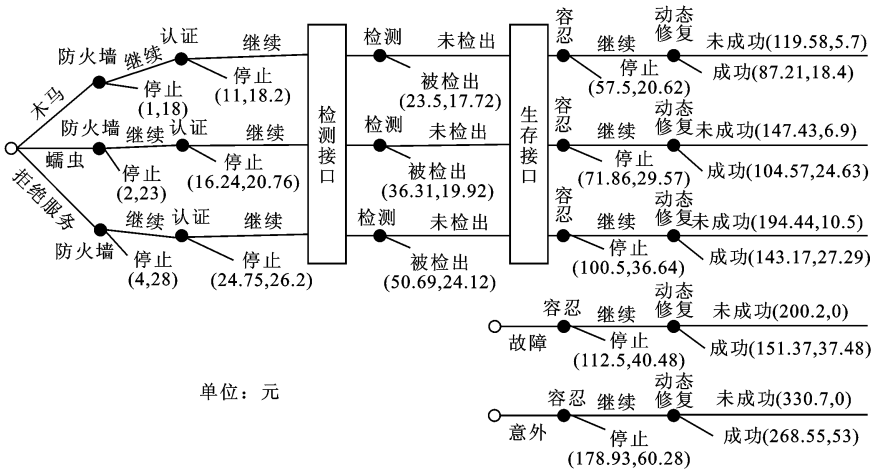


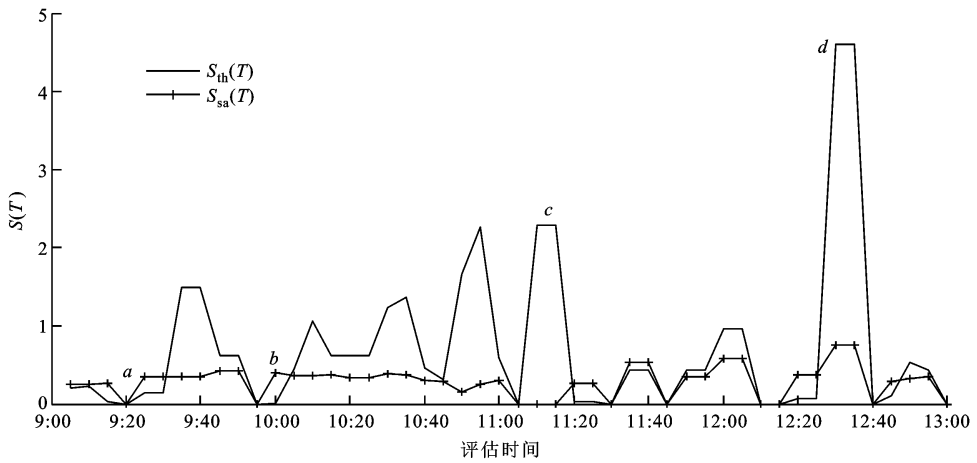
图 6 攻防双方在各阶段的收益图

态势评估是基于时间的持续过程，为了说明不同情况下的可生存态势评估问题，分别模拟 4 h 的网络攻防行为. 在 1 h 时，仅有恶意攻击事件发生，且发生频率较低. 在 2 h 时，仅有恶意攻击事件发生，但发生频率较高，且以危害较多的拒绝服务攻击居多. 在 3 h 时，威胁为恶意攻击伴随节点故障. 在 4 h 时，模拟意外故障导致服务器瘫痪的极端情况，如表 3 所示.

根据给出的收益值和威胁数据，$U_{Am}=350$ 元，$U_{Dm}=70$ 元，$\Delta t=10$ min，由式(7)计算得到的态势评估结果如图 7 所示. 从图 7 可以看出，网络在某时刻遭遇的威胁越大，则 $S_{th}(T)$ 的值也越大，体现出系统在可生存性上面临的风险程度. $S_{sa}(T)$ 依据当前风险表示出系统所具备的可生存能力，由于 $S_{sa}(T)$ 不随风险程度的变化而变化，因此其网络可生存性结果相对稳定.

表 3 网络可生存性威胁数据

序号	发生时刻	位置	威胁类型	资产类型	资产价值	结果
1	9：03	节点 4	木马	服务器	3	被检出
2	9：07	节点 5	木马	PC	1	认证过滤
3	9：25	节点 5	拒绝服务	PC	1	被检出
4	9：31	节点 1	蠕虫	路由器	5	生存成功
5	9：42	节点 3	蠕虫	服务器	3	容忍成功
⋮	⋮	⋮	⋮	⋮	⋮	⋮
27	12：43	节点 5	蠕虫	PC	1	被检出
28	12：47	节点 4	拒绝服务	服务器	3	被检出



a：畸点；b：正常生存能力；c：生存失败；d：较强生存能力

图 7 网络可生存性态势评估结果图

5 结 论

本文针对动态博弈理论在可生存性态势感知领域中的应用进行了探索性的工作，构建了基于博弈论的可生存性态势感知框架，以评估为目的提出了模块化的动态博弈模型，具体给出了可生存性态势评估的计算过程. 本文方法可对网络系统面临的生存性威胁及系统自身的可生存能力进行实时有效的评估，因此基本实现了对可生存性态势实时跟踪评估的目的.

参考文献：

[1] JAME S, HUTCHISON D, CTINKAYA K, et al. Resilience and survivability in communication networks: strategies, principles, and survey of disciplines [J]. Computer Networks, 2010, 54(8):1245-1265.

[2] AL-KUWAITI M, KYRIAKOPOULOS N, HUSSEIN S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability [J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 106-124.

[3] MA Zhanshan, KRINGS W. Dynamic hybrid fault modeling and extended evolutionary game theory for reliability, survivability and fault tolerance analyses [J]. IEEE Transactions on Reliability, 2011, 60(1): 180-196.

[4] 李黎，管晓宏，赵千川，等. 网络生存适应性的多目标评估 [J]. 西安交通大学学报，2010，44(10)：1-7.
LI Li, GUAN Xiaohong, ZHAO Qianchuan, et al. Multi-objective evaluation of network survival fitness [J]. Journal of Xi'an Jiaotong University, 2010, 44(10): 1-7.

[5] BASS T. Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness [J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] 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.

[7] OSTER D. Providing adaptability in survivable systems through situation awareness [D]. Skovde, Sweden: University of Skovde, 2006.

[8] LI Bai, BISWAS S. Survivability: an information fusion process metric from an operational perspective[C]//Proceedings of 10th International Conference on Information Fusion. Piscataway, NJ, USA: IEEE, 2007: 1-8.

[9] 赵国生，王慧强，王健. 基于灰色关联分析的网络可生存性态势评估研究 [J]. 小型微型计算机系统，2006，27(10)：1861-1864.
ZHAO Guosheng, WANG Huiqiang, WANG Jian. Study on situation evaluation for network survivability based on grey relation analysis [J]. Mini-Micro Systems, 2006, 27(10): 1861-1864.

[10] 王健，王慧强，赵国生. 基于序列蒙特卡罗的网络生存态势跟踪评估 [J]. 哈尔滨工业大学学报，2008，40(5)：802-806.
WANG Jian, WANG Huiqiang, ZHAO Guosheng. Situation tracking assessment for network survivability based on sequential Monte Carlo [J]. Journal of Harbin Institute of Technology, 2008, 40(5): 802-806.

[11] 朱建明，RAGHUNATHAN S. 基于博弈论的信息安全技术评价模型 [J]. 计算机学报，2009，32(4)：828-834.
ZHU Jianming, RAGHUNATHAN S. Evaluation model of information security technologies based on game theoretic [J]. Chinese Journal of Computers, 2009, 32(4): 828-834.

[12] 林旺群，王慧，刘家红，等. 基于非合作动态博弈的网络安全主动防御技术研究 [J]. 计算机研究与发展，2011，48(2)：306-316.
LIN Wangqun, WANG Hui, LIU Jiahong, et al. Research on active defense technology in network security based on non-cooperative dynamic game theory [J]. Journal of Computer Research and Development, 2011, 48(2): 306-316.

[13] 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.
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.

（编辑　管咏梅　武红江）