doi:10.3969/j.issn.1671-637X.2014.01.007

节点崩溃条件下信息系统安全风险传播

熊金石[1,2], 李建华[1], 沈 迪[1], 郭威武[3]
(1.空军工程大学信息与导航学院,西安 710077; 2.中国人民解放军95793部队,贵阳 550025;
3.中国人民解放军93010部队89分队,沈阳 110016)

摘 要:风险传播研究是信息系统安全风险评估的重要研究方向。基于风险传播和风险传播模型,考虑邻居节点之间的相互影响,重新定义了信息系统网络节点的初始负荷和节点崩溃与失效的概念。引入负荷局域择优重新分配策略,提出运用信息系统网络节点崩溃和实效节点的数目反映信息系统抵御风险传播的能力。设计了两种袭击策略,即网络信息已知条件下的蓄意攻击和网络信息未知条件下的随机攻击,并结合实例仿真分析了不同节点崩溃条件下的信息系统安全风险的传播问题。结果表明,蓄意攻击策略引起的节点崩溃更易造成信息系统安全风险的迅速全域传播。

关键词:信息系统;安全风险;风险传播;节点崩溃;择优概率
中图分类号:V271.4;TN915 **文献标志码**:A **文章编号**:1671-637X(2014)01-0028-05

Security Risk Propagation of Information Systems Under Condition of Nodes Breakdown

XIONG Jin-shi[1,2], LI Jian-hua[1], SHEN Di[1], GUO Wei-wu[3]
(1. College of Information and Navigation, Air Force Engineering University, Xi'an 710077, China; 2. No. 95793 Unit of PLA, Guiyang 550025, China; 3. Element 89 of No. 93010 Unit of PLA, Shenyang 110016, China)

Abstract: Research on risk propagation is an important direction of information system security risk evaluation. We redefined the original load of information system network and the concept of node breakdown/failure based on risk propagation and risk propagation model as well as considering the mutual effect between the adjacent nodes. The local preferential redistribution rule of the load was proposed, and the information system network node breakdown and the number of effective nodes were used to reflect the resisting ability of information system to risk propagation. Two attacking strategies, deliberate attacking with known network information and random attacking without network information, were designed. Information system security risk propagation under conditions of different node breakdown was analyzed through simulation. The results show that node breakdown caused by a deliberate attack is more likely to cause the rapid global propagation of information system security risk.

Key words: information system; security risk; risk propagation; node breakdown; preferred probability

0 引言

在当今大规模开放互联网络环境下,即使采取相对完善的安全保护措施,信息系统的安全风险依然存在[1]。随着信息系统的逐渐普及,一旦风险事件发生,对信息系统的管理者、使用者都将造成损失,甚至对社会和国家也会产生重大影响。如何有效预防和控制风险事件的发生,从安全角度保障信息系统可以正常、有序和持续性地运行,合理地利用现有资源获取最大的社会和经济效益,是信息系统安全领域所面临的重大研究课题。

安全风险评估是评价信息系统安全状况的一种有效手段,正逐渐成为人们研究的热点。信息系统风险评估方法按照自动化程度可以分为人工评估和自动评估。目前,针对自动评估技术的相关研究工作较多:比较有代表性的是CORAS(Consultative Objective Risk

收稿日期:2013-03-12 修回日期:2013-04-01
基金项目:国家自然科学基金项目(61174162)
作者简介:熊金石(1985—),男,湖北随州人,博士生,研究方向为信息系统基本理论与规划建设。

Analysis System)风险评估方法、RSDS(Reactive System Design Support)方法和基于逻辑渗透图的网络安全风险评估方法(LEG-NSRA)[2-3]。

传统的安全风险评估方法是将自动弱点扫描工具获得的弱点实施量化后进行风险累加,此过程忽略了风险的传播性这一事实[4-5],即由于信息终端的高度互联,受干扰(攻击)终端引起的风险可能会传播给其他终端甚至整个信息系统,使得那些原本不直接具有风险的信息终端,因受干扰(攻击)终端的风险传播而遭到安全威胁。

鉴于此,在文献[6-9]的基础上,重新定义了信息系统网络节点的初始负荷和节点崩溃与失效的概念,引入超负荷重新分配择优概率机制,提出了两种袭击策略,即网络信息已知条件下的蓄意攻击和网络信息未知条件下的随机攻击,研究了这两种策略下信息系统网络安全风险的传播问题。

1　信息系统安全风险传播

信息系统的风险传播行为与网络上的相继故障有很多相似之处。本文的研究主要关注某个节点因为某种原因产生故障所导致的信息系统网络的全局动态属性,即风险传播现象。

首先给出风险传播的定义[5]。

定义 1　风险传播。设在访问关系网络中存在 3 个网络节点 A、B、C,两条边 $e(A,B)$ 和 $e(B,C)$,且节点 A 存在弱点。从攻击者的角度看,可以利用弱点侵入节点 A,进而利用 $e(A,B)$ 对节点 B 进行攻击。依此类推,侵入节点 B 后利用 $e(B,C)$ 攻击节点 C;而从安全风险的角度看,由于 $e(A,B)$ 和 $e(B,C)$ 的存在,使得具有弱点的节点 A 将自身的风险不同程度地扩散给原本没有风险的节点 B 和 C。因此,称风险具有可传播性,而风险扩散的这一过程称为风险传播。

事实上,风险传播是可能发生的攻击过程在风险上的体现。

定义 2　风险传播模型。定义风险传播模型为 $M=(D,F)$,其中:D 为风险网络;F 为传播算法集合,F 中的每个元素都是相互独立的算法,它们描述风险源将其风险沿着传播途径扩散到网络中的过程。在模型 M 中,网络 D 用于存储网络信息系统的风险状态,而每种传播算法体现了风险的运动规则,改变了网络 D 的风险状态。

如果所有节点没有受到外部攻击或攻击在其可承受范围内,那么所有的节点都将永远保持正常状态。文献[10]的研究认为网络中节点的初始负荷不仅与节点自身的度(即与该节点直接相连的节点的个数)有关,而且也受到邻居节点的度的影响,且网络中节点的负荷与节点本身的度和其邻居节点的度的总和的乘积是正相关的,如图 1 所示。

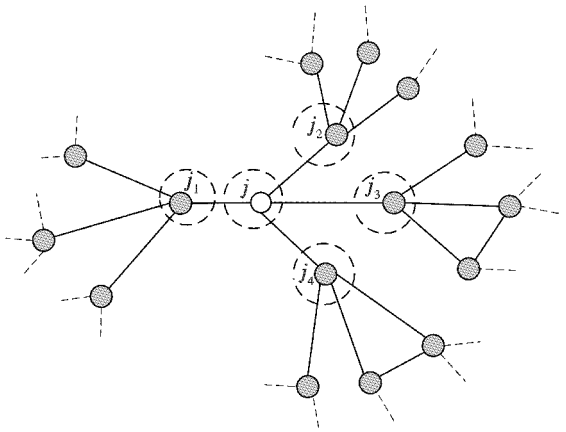

图 1　节点的负荷与它邻居节点度之间的关联

Fig. 1　Relationship between a node's load and its neighbor node's degree

图中,j 为节点。据此,给出节点初始负荷的定义。

定义 3　初始负荷。网络中节点的初始负荷定义为

$$L_i=\frac{\left(d_i\sum_{m\in\Gamma_i}d_m\right)^{\alpha}}{\sum_{i\in v}\left(d_i\sum_{n\in\Gamma_i}d_n\right)^{\alpha}}*L \tag{1}$$

式中:L 为网络中节点初始负荷的和,为一定值;d_i 为节点 i 的度;m 为节点 i 的一个邻居节点;d_m 为节点 m 的度;Γ_i 为节点 i 的邻居节点的集合;α 为可调参数,它控制着节点初始负荷的强度及负荷的分布,对于一个特定的信息系统网络而言,网络中每个节点的度是固定不变的。因此,为了描述节点度对节点上负荷的影响,模型中引入参数 α。α 越大,不同度节点上负荷之间的差异性就越大,即节点上负荷的分布就越不均匀。

信息系统网络中每个节点因受到各种原因的限制,承受打击或处理风险的能力各不相同。在此,假设每个节点的承受(或处理)能力与它的初始负荷成正比,即

$$C_i=(1+\beta)L_i,i=1,2,3,\cdots,N \tag{2}$$

式中,β 为能力参数,$\beta\geq 0$。

定义 4　节点崩溃。由于信息系统网络中的每个节点都有一定的承受能力来处理最大的负荷,所以,如果在某时刻,某节点受到攻击被摧毁或工作量超过负荷,那么称该节点在此刻崩溃。

假设节点崩溃后,在剩余时间内无法及时恢复其功能的情况下(这个假设对于一定时限内的工作而言是合理的),节点在以后的任意时刻都处于崩溃状态。

当一个节点崩溃后,会导致负荷的进一步重新分配,负荷会波及到其邻居节点,从而引起新一轮的节点崩溃。这个过程反复进行,节点崩溃就可能扩散,即风险传播,图 2 所示为风险传播的示意图。

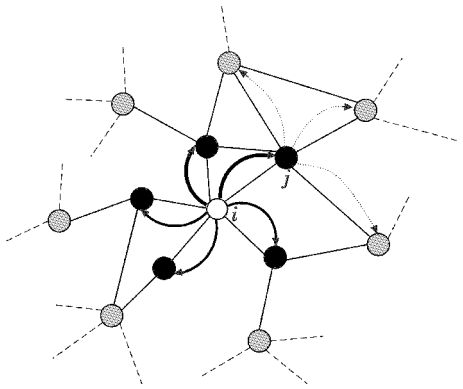

图2 风险传播示意图

Fig. 2 Sketch map of risk propagation

为了避免进一步的崩溃现象,重新分配的负荷更倾向于选择具有较高处理能力的邻居节点,以保持网络的整体流畅。鉴于此,采用基于崩溃节点负荷局域择优重新分配的原则[7]。

定义5 择优概率。崩溃节点 i 上的负荷重新分配到其邻居节点 j 上,择优概率定义为

$$\Pi_j = \frac{L_j}{\sum_{n\in\Gamma_i} L_n} = \frac{\dfrac{\left(d_j \sum_{m\in\Gamma_j} d_m\right)^{\alpha}}{\sum_{x\in v}\left(d_x \sum_{y\in\Gamma_x} d_y\right)^{\alpha}}}{\sum_{n\in\Gamma_i}\left(\dfrac{\left(d_n \sum_{m\in\Gamma_n} d_m\right)^{\alpha}}{\sum_{p\in v}\left(d_p \sum_{q\in\Gamma_p} d_q\right)^{\alpha}}\right)} \tag{3}$$

式中:L_j 为节点 j 的初始状态;n 为节点 i 的邻居节点;Γ_i 为节点 i 的所有邻居节点的集合;q 为节点 n 的邻居节点。

因此,节点 j 收到的额外负荷为

$$\Delta L_{ji} = L_i \Pi_j \tag{4}$$

在风险传播过程中,网络中可能会出现一类特殊节点,这类节点因与之相连接的节点崩溃而成为孤立节点,失去与网络中其他节点的联系。针对这类节点,有如下定义。

定义6 节点失效。如果在某时刻,节点 i 的所有邻居节点均崩溃,则节点 i 成为孤立节点,称此时的节点 i 失效。

为更好地探讨袭击信息系统网络上不同类型节点所引发的风险传播规模,提出一个新的计算量 S_i,即由节点 i 所导致的崩溃和失效节点的数量。很显然,$0 \leqslant S_i \leqslant N_{\text{node}} - 1$,其中,$N_{\text{node}}$ 为节点数量。为了量化袭击某一节点导致的整个信息系统网络的风险传播现象,采用袭击某一节点后的归一化指标 S_i',即

$$S_i' = S_i \Big/ N_{\text{node}} - 1。 \tag{5}$$

2 袭击策略与信息系统网络拓扑结构

2.1 袭击策略

在模型的研究中,考虑以下两种不同的袭击策略。

1) 网络信息已知条件下的蓄意攻击。此种策略亦即袭击信息系统网络中最重要的节点。在各种理论和实际的网络研究中,许多研究者采用袭击网络中度最大的节点,即 KN(Key Node)策略,并从不同角度得出无标度网络面对 KN 策略表现的强脆弱性[11-14]。如果某些节点具有同等重要性,则从中随机选取。文献[15-16]从复杂网络中心化的角度指出网络中最重要的节点不一定是网络的几何中心节点(度大节点),并运用复杂网络的中心化方法,得到了网络的最重要节点。

2) 网络信息未知条件下的随机攻击。此种策略亦即袭击信息系统网络的任一节点,即 RN(Random Node)策略。

2.2 信息系统网络拓扑结构

拓扑结构模型是在合理简化网络化信息系统后,利用适当表现形式对主要特征描绘得到的分析对象。

网络化信息系统可以用图 $G=(V,E)$ 表示,假设 G 有 n 个节点,m 条边,用 $V=\{v_1,v_2,\cdots,v_n\}$ 表示 G 的节点集合,$E=\{e_1,e_2,\cdots,e_m\}$ 表示边的集合。可以用图的全顶点关联矩阵来表征图的连接状态。图 G 的全顶点关联矩阵 $\boldsymbol{A}=[a_{ij}]$ 的每行对应一个节点,每列对应一条链路。

当 G 是无向图时,$\boldsymbol{A}$ 的元素 a_{ij} 的定义为 $a_{ij}=\begin{cases}1, & \text{第 } j \text{ 条边与第 } i \text{ 个节点相连}\\ 0, & \text{第 } j \text{ 条边与第 } i \text{ 个节点不相连}\end{cases}$。

3 实例仿真与分析

图3所示为某信息系统拓扑结构(局部)示意图。

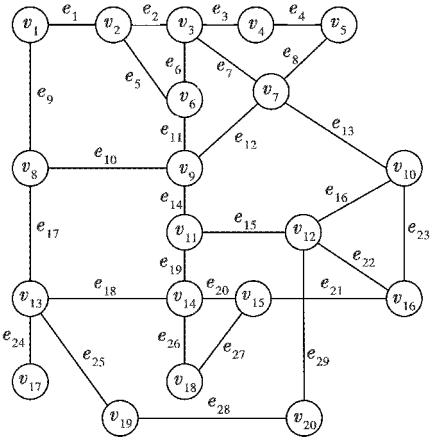

图3 某信息系统拓扑结构(局部)

Fig. 3 Topological structure of one information system (partial)

图中:○代表各信息实体;连线代表两信息实体之间有直接的信息联系。

连接矩阵为

$$A=\begin{vmatrix}
0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0
\end{vmatrix}\qquad(6)$$

仿真开始之前，首先需要确定该信息系统网络的最重要节点。文献[16]通过仿真分析，认为 v_9 和 v_{14} 节点是该信息系统网络中的最重要节点。

仿真过程中，分别考虑了 $\alpha=0.5$，$\alpha=1$ 和 $\alpha=2$ 这 3 种情况。KN 策略选取 v_{14} 节点，RN 策略分别选取 v_1 和 v_{17} 节点。仿真结果如图 4 所示。

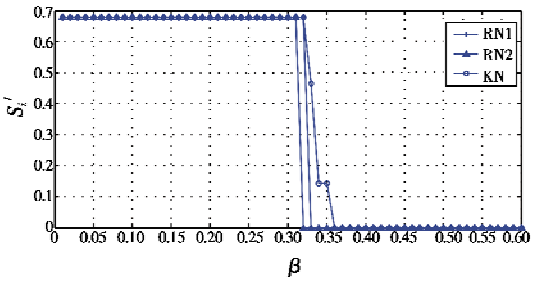

图 4　$\alpha=0.5$ 时不同袭击策略下风险传播情况

Fig. 4　Risk propagation based on different assault strategies when $\alpha=0.5$

从图 4 中可以看出，当 $\alpha=0.5$，即网络中各节点的初始负荷和承受(或处理)能力差异性不大时，两种攻击策略下信息系统安全风险的传播现象基本一致，并未表现出明显差异。但随着 α 的增大，如图 5、图 6 所示，两种攻击策略下风险传播的差异越来越明显，即节点之间的差异性越大，初始负荷分布越不均匀，风险传播的差异越明显。从总体趋势上来看，随着 β 值的不断增大，即节点承受打击或处理风险的能力的增强，系统抵御风险的能力不断增强。

同时，通过图 4、图 5、图 6 对比可以看出，KN 策略即蓄意攻击策略引起的节点崩溃更易造成信息系统安全风险的迅速全域传播。

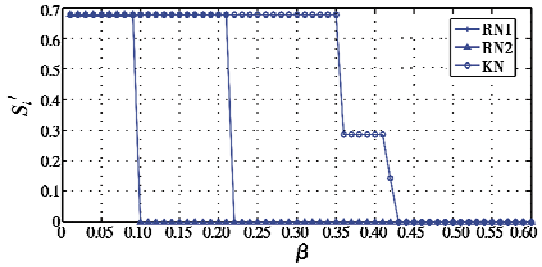

图 5　$\alpha=1$ 时不同袭击策略下风险传播情况

Fig. 5　Risk propagation based on different assault strategies when $\alpha=1$

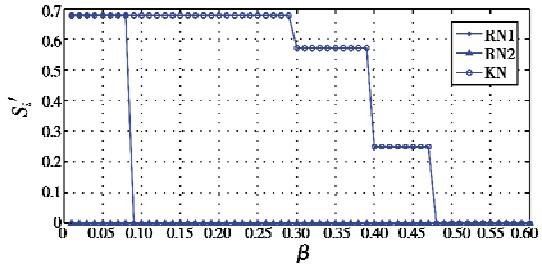

图 6　$\alpha=2$ 时不同袭击策略下风险传播情况

Fig. 6　Risk propagation based on different assault strategies when $\alpha=2$

4　结论与展望

本文基于风险传播思想，考虑节点的负荷与其邻居节点度之间的关联，重新定义了信息系统网络节点的初始负荷，并引入负荷局域择优重新分配策略，建立了信息系统安全风险传播模型。结合实例，仿真分析了不同攻击策略下的信息系统安全风险的传播问题。仿真结果表明，蓄意攻击策略引起的节点崩溃更易造成信息系统安全风险的迅速全域传播。

当然，本文的研究还有很多不完善之处，在实际应用过程中，应在节点负荷及其承受能力上做更进一步研究。

参 考 文 献

[1]　吴晓平，付钰. 信息系统安全风险评估理论与方法[M]. 北京：科学出版社，2011.
WU X P, FU Y. Security risk assessment theory and methods for information systems[M]. Beijing: Science Press, 2011.

[2]　冯登国，张阳，张玉清. 信息安全风险评估综述[J]. 通信学报，2004，25(7)：10-18.
FENG D G, ZHANG Y, ZHENG Y Q. Survey of information security risk assessment[J]. Journal of China Institute of Communications, 2004, 7(25): 10-18.

[3]　毛捍东. 基于逻辑渗透图模型的网络安全风险评估方法研究[D]. 长沙：国防科学技术大学，2008.
MAO H D. A novel assessment approach based on logial

exploitation graph model for network security[D]. Changsha: National University of Defense Technology, 2008.

[4] 张永铮,方滨兴,迟悦,等. 用于评估网络信息系统的风险传播模型[J]. 软件学报,2007,18(1):137-145.
ZHANG Y Z, FANG B X, CHI Y, et al. Risk propagation model for assessing network information systems[J]. Journal of Software, 2007, 18(1):137-145.

[5] 张永铮,田志宏,方滨兴,等. 求解网络风险传播问题的近似算法及其性能分析[J]. 中国科学 E 辑:信息科学,2008,38(8):1157-1168.
ZHANG Y Z, TIAN Z H, FANG B X, et al. Approximate arithmetic for solving problem of network risk propagation and its performance analysis[J]. Science in China(Series E: Information Sciences), 2008, 38(8):1157-1168.

[6] 王建伟,荣莉莉. 基于负荷局域择优重新分配原则的复杂网络上的相继故障[J]. 物理学报,2009,58(6):3714-3721.
WANG J W, RONG L L. Cascading failures on complex networks based on the local preferential redistribution rule of the load[J]. Acta Phys. Sin., 2009, 58(6):3714-3721.

[7] 王建伟,荣莉莉. 基于袭击的复杂网络上的全局相继故障[J]. 管理科学,2009,22(3):113-120.
WANG J W, RONG L L. Universal cascading failures on complex networks based on attacks[J]. Journal of Management Science, 2009, 22(3):113-120.

[8] 王建伟,荣莉莉,王铎. 基于节点局域特征的复杂网络上相继故障模型[J]. 管理科学学报,2010,13(8):42-50.
WANG J W, RONG L L, WANG D. Model for cascading failures on complex networks based on local characteristics of nodes[J]. Journal of Management Sciences in China, 2010, 13(8):42-50.

[9] 王建伟. 网络上的相继故障模型研究[D]. 大连:大连理工大学,2010.
WANG J W. Study on cascading failure models on networks [D]. Dalian: Dalian University of Technology, 2010.

[10] WU J J, GAO Z Y, SUN H J. Cascade and breakdown in scale-free networks with community structure[J]. Physical Review E, 2006, 74(6):066111(5).

[11] ALBERT R, JEONG H, BARABÁSI A L. Error and attack tolerance in complex networks[J]. Nature, 2000, 406(6794):378-382.

[12] VALENTE X C N, SARKAR A, STONE H A. Two-peak and three-peak optimal complex networks[J]. Physical Review Letters, 2004, 92(11):118702(1)-118702(4).

[13] BOLLOBÁS B, RIORDAN O. Robustness and vulnerability of scale-free random graphs[J]. Internet Mathematics, 2001, 1(1):1-35.

[14] BRODER A, KUMAR R, MAGHOUL F, et al. Graph structure in the web[J]. Compute Networks, 2000, 33(1-6):309-320.

[15] 王林,张婧婧. 复杂网络的中心化[J]. 复杂系统与复杂性科学,2006,3(1):13-20.
WANG L, ZHANG J J. Centralization of complex networks[J]. Complex Systems and Complexity Science, 2006, 3(1):13-20.

[16] 熊金石,李建华,杨迎辉,等. 基于复杂性理论的军事通信网络中心化方法比较[J]. 科技导报,2011,29(36):38-41.
XIONG J S, LI J H, YANG Y H, et al. Compare of centrality measures of military communication network based on complexity theory[J]. Science & Technology Review, 2011, 29(36):38-41.

下 期 要 目

基于递推质心算法的二元传感器网络分布式目标跟踪
像方扫描机制的红外成像制导光学系统设计
基于优化信息算子的 UWB 信道贝叶斯估计
机载空战训练信息一体化记录系统的设计
飞机战伤抢修研究中的建模仿真简述
一种机载红外跟瞄器动态跟踪精度测试方法
航电全光波分复用网络的波长路由算法研究
支持网络化应用的无人机 CGCS 功能体系研讨
UUV 国内外研究现状及若干关键问题综述
载波跟踪环路鉴别器的改进设计及 FPGA 实现
应用半导体激光器缩比仿真微波着陆系统辐射源研究
光耦在 EMCCD 电源中的应用
星敏感器误差模型及参数分析
贫数据多退化量产品可靠性评估