IPv6 AS级Internet抗毁性研究

秦 李[1] 黄曙光[2] 陈 骁[1]
(电子工程学院研究生管理大队 合肥 230037)[1] (电子工程学院网络系 合肥 230037)[2]

摘 要 随着互联网和物联网的飞速发展,通信协议从IPv4过渡到IPv6已是必然趋势。采集了CAIDA Ark项目的最新数据(时间为2014年6月),通过对IPv6 AS级Internet建模,验证了该网络所具有的小世界和无标度特性。在分析Internet结构及常用抗毁性测度的基础上,提出了IPv6 AS级Internet的抗毁性测度指标和抗毁性实验方法。实验结果表明,在不同的攻击策略下,网络具有鲁棒且脆弱的特性,在遭到基于度的蓄意攻击时,网络抗毁性最差,同时也表明构建的抗毁性测度可以很好地表征Internet的抗毁性水平。

关键词 复杂网络,IPv6,AS级Internet,抗毁性
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.034

Research on Invulnerability of IPv6 AS-level Internet

QIN Li[1] HUANG Shu-guang[2] CHEN Xiao[1]
(Department of Graduate, Electronic Engineering Institute, Hefei 230037, China)[1]
(Department of Network, Electronic Engineering Institute, Hefei 230037, China)[2]

Abstract With the rapid development of Internet and the Internet of Things, it is an inevitable trend to transfer the communication protocol from IPv4 to IPv6. This paper collected the latest IPv6 AS-level Internet data from the project of CAIDA Ark(2014.6). By modeling this data based on complex network, we found that the IPv6 Internet also has small-world and scale-free properties. Furthermore, on the basis of analyzing the structure of the IPv4 Internet and the commonly measures of invulnerability, we proposed the measures of invulnerability for the IPv6 Internet and the method of how to do the invulnerability experiment. The results show that this measures can do well in describing the performance of invulnerability. Under different attack strategies, of which the attack based on the order of degree can make the largest effect of damage, we found that the IPv6 Internet has the characteristics of robustness and vulnerability.

Keywords Complex network, IPv6, AS-level Internet, Invulnerability

如今的Internet已经发展为一个复杂的大规模网络,与人类的生活息息相关,如网络订票、自动售货机支付、网购与在线支付、网上金融交易及其他银行业务,一旦出现大面积的网络故障,后果将会非常严重。比如,为近40万个网站提供域名解析服务的"DNSPOD"网络公司服务器在2009年突然遭受大流量攻击,这致使江苏、安徽、广西、海南、甘肃、浙江等6省和自治区出现了大范围的网络瘫痪,域名解析服务甚至完全中断。Internet每天都会发生各种各样的随机故障或遭到黑客的蓄意攻击,在这种情况下,对Internet的抗毁性进行测度与分析,毫无疑问地成为了当前研究的一个重要课题。

Internet的路由选择结构是一种层次式的选择结构,由若干路由器汇集成一个自治系统(Autonomous System, AS),不同AS之间再通过边界路由器(BGP)而彼此相连[1]。目前Internet拓扑的研究工作也主要集中在AS级和路由级两个层面。与路由级拓扑结构相比,AS级拓扑位于网络的更"上"一层,其特征的演化对Internet的影响更为巨大[2]。因此,对其进行相关研究,有利于未来网络的规划及发展,具有重大的意义。同时,自1995年IETF制定IPv6协议以来,许多学者和科研机构都致力于IPv6的研究、实现和测试,各项技术已日趋成熟。数据显示,截止2013年7月底,全球已有109个网络支持IPv6,全球94个国家IPv6的用户总数超过2000万,IPv4地址早已耗尽,而如今物联网的飞速发展,更加速了IPv4向IPv6的转变,IPv6的发展部署已成为各国的战略部署。但目前国内还没有针对IPv6 Internet而进行的实证研究,因此,为了把握IPv6的发展态势及为今后的Internet网络规划和管理提供理论依据有必要针对IPv6 AS级Internet进行抗毁性分析。

复杂网络的抗毁性研究最早始于Albert等人的工作,2000年出版的《Nature》的封面标题为"Internet的阿喀琉斯之踵",阐述了BA无标度网络的鲁棒又脆弱的双重特性。目前,关于抗毁性的公认定义由Ellison等[3]提出:网络系统在遭受攻击、故障和意外事故时仍能够及时完成其关键任务的能力。谭跃进等人认为网络抗毁性是指在网络中的节点(或边)发生随机失效或遭受故意攻击的条件下,网络维持其功能

到稿日期:2014-08-08 返修日期:2014-11-26 本文受安徽省自然科学基金(1208085QF107)资助。
秦 李(1990-),男,硕士生,主要研究方向为复杂网络,E-mail:qinli0836@qq.com;黄曙光(1960-),男,教授,博士生导师,主要研究方向为信息安全、复杂网络;陈 骁(1990-),女,硕士生,主要研究方向为复杂网络、社会网络分析。

的能力[4]。根据攻击方式选择的不同，一般有随机故障和蓄意攻击，网络的抗毁性主要测度的是“最坏情况”下的抗打击能力[5,6]。R. J. Mondragón 等[7]最早对 IPv4 AS 级 Internet 的抗毁性进行了分析，表明 Internet 服从幂指数约为 2.2 的幂率分布。相对国外而言，国内的研究起步较晚，只在最近几年，一些学者在不同网络中做了许多探索研究。如汪涛等人以国内 4 个城市公共交通系统为研究对象，考察了公交网络在不同攻击模式下的抗毁性[8]；谢丰等人针对 ER 随机模型、BA 无标度网络模型和 PFP 互联网拓扑等 3 种模型，通过不同的攻击策略研究了网络的动态性对抗毁性的影响[9]；曾小舟等人运用复杂网络理论建立了中国航空网络的抗毁性测度方法，并进行了抗毁性实证分析[10]；黄仁全等人在分析作战体系网络结构以及常用抗毁性测度的基础上，提出了自然连通度的复杂网络抗毁性测度[11]；种鹏云等人跟据危险品运输网络模型的配送特性，提出了“网络风险效率”和“最大连通度”抗毁性测度，很好地表征了危险品运输网络的抗毁性水平[12]。

本文主要以复杂网络理论为基础，结合 CAIDA Ark 项目的 IPv6 方面的最新实测数据，做了以下工作：首先，以 2014 年 6 月的 IPv6 AS 级拓扑图为基础，分析了 IPv6 的度分布等基本特征，验证了 IPv6 Internet 所具有的小世界和无标度特性；其次，提出以网络链路数、网络碎片数、最大连通子图相对大小以及网络聚类系数等 4 个指标对网络抗毁性进行测度，并设计了仿真实验；最后，通过对仿真实验的结果的综合分析，得出结论，并指出下一步的工作重点。

1 理论基础

AS 级 Internet 可以抽象成节点（自治系统）以及通过边（通信链路）相互作用的复杂网络。复杂网络的最基本特征是小世界特性和无标度特性。由于实际中的网络大多并非完全规则，也非完全随机，而是介于两者之间的具有小世界特性的复杂网络，并且节点的度分布具有明显的无标度性[13,14]，因此主要用以下 3 个参数对复杂网络的基本特征进行刻画。

1.1 度及度分布

复杂网络中，度是分析网络拓扑性质最基本的参数，常被用来描述节点在网络中的直接影响力。一个节点 i 的度中心性定义为节点 i 的实际连边数与节点 i 最大可能的连边数的比值，其表达式为 $DC_i=\frac{k_i}{N-1}$，其中，k_i 表示节点 i 的连边数，N 为网络的节点总数[15]。度中心性定义表明了一个节点与其他节点的直接通信能力，数值越大，在网络中越重要[16]。网络中所有节点的度的平均值称为网络的平均度（Average Degree）$\langle k\rangle$，一般记为 $\langle k\rangle=\frac{1}{N}\sum_{i=1}^{N}k_i$。

度分布（Degree Distribution）$P(k)$ 即可看作是网络中随机选择的一个节点的度值为 k 的概率，度的分布函数一般用 $P(k)$ 表示。节点的度分布常用来度量网络的无标度特性，如果一个网络的度分布 $P(k)$ 可以用如下形式的幂率分布来表示：$P(k)\propto k^{-\gamma}$（其中 $\gamma>0$ 为幂指数），则该网络具有无标度特性。在实际情况中，往往会有一些度值（特别是度分布的尾部）的分布会出现类似于噪声干扰的明显偏差，在这种情况下，常用补累积度分布（Complementary Cumulative Degree Distribution，CCDF）来对其进行光滑处理，表示度值不小于 k 的节点在整个网络中占的比例。

1.2 平均路径长度与网络直径

平均路径长度（Average Path Length）：定义为任意两个节点之间的距离的平均值，即 $L=\frac{2}{N(N-1)}\sum_{i\geqslant j}d_{ij}$[15]。

网络直径（Diameter）：网络中任意两个节点之间的距离的最大值，记为 D，即 $D=\max\limits_{i,j}d_{ij}$。

在 AS 级 Internet 中，这两个基本统计特征具有各自的实际意义，其中，平均路径长度描述了任意两个 AS 之间在路由选择时所经过的最少自治系统，而网络直径则表示距离最远的两个自治系统。

1.3 聚类系数

在复杂网络中，常用聚类系数（Clustering Coefficient）来定量刻画网络节点的聚类成团的特点。一个度为 k_i 的节点 i 的聚类系数 C_i 定义为：$C_i=\frac{E_i}{(k_i(k_i-1))/2}=\frac{2E_i}{k_i(k_i-1)}$[15]，其中，$E_i$ 是节点 i 的 k_i 个邻节点之间实际存在的边数，即节点 i 的 k_i 个邻节点之间实际存在的邻居对的数目。

2 AS 级 Internet 拓扑结构分析

2.1 AS 级拓扑数据的获取

CAIDA（Center Applied for Internet Data Analysis）是在全球范围内对 Internet 结构和数据进行收集、分析的国际合作研究机构。CAIDA 主要对 Internet 数据进行获取、研究、分析和共享，其主要研究的内容包括互联网的结构、发展、演化趋势和网络行为与动力特征等。CAIDA 在全球部署了 15 个测量点，这些测量点分布在全世界各大洲内，分别从不同的视角对 IPv6 的 Internet 拓扑结构进行长期大规模的测量与分析。CAIDA 监测点拥有完全自主的控制权与所属权，对 Internet 的测量无需任何授权，可不受影响地进行持久不间断的测量。所以，目前大部分学者都是通过 CAIDA 的测量数据来分析和研究 Internet。

本文分析和实验的数据是位于美国俄勒冈州尤金市观测点于 2014 年 6 月所采集的最新数据，图 1 是利用 Fruchterman-Reingold 算法[17]所绘制的 IPv6 AS 级 Internet 的可视化拓扑图。

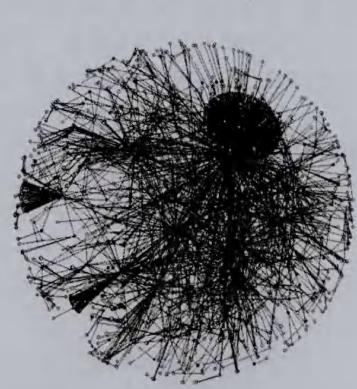

图 1 IPv6 AS 级 Internet 拓扑图

2.2 AS级Internet特征分析

表1列出了该网络和与其规模同等的E-R随机网络模型的基本统计特征。

表1 网络的基本统计特征

网络名称	N(M)	〈C〉	〈k〉	L	D
AS-20140602-eug	3686(4422)	0.0473	2.4	3.91	9
E-R随机网络	3686(4422)	0.00028	2.4	25.7	77

本文应用邻接链表的方法对Internet进行建模，相关计算与仿真基于Matlab 2013a-32bit实现。由表1可知，该网络共3686个节点，4422条链路。经过计算，AS拓扑图的平均度〈k〉为2.4，说明每个自治系统平均与2.4个系统相连。网络的聚类系数为0.0473，平均路径长度为3.91，与同等规模的E-R随机图相比，具有较大的聚类系数和较小的平均最短路径。因此，IPv6 Internet具有小世界特性，其度分布和累积度分布如图2和图3所示。

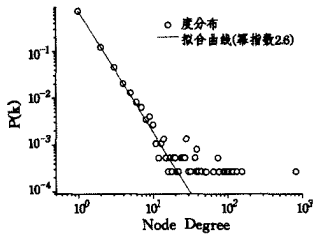

图2 IPv6 AS级Internet的度分布

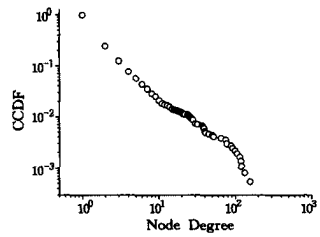

图3 IPv6 AS级Internet的累积度分布

从图3中容易看出，在双对数坐标中，度的累计分布近似呈一条直线，表明AS拓扑度分布近似服从幂率分布，但在尾部(即度值大的节点)出现了偏差，说明拓扑中Hub节点部分不完全符合幂率分布。但仅仅通过图表的直接观察还无法判断其在什么范围内符合怎样的幂率分布。所以，通过最小二乘直线拟合得到幂率的分布函数为：$P(k)=0.75\times k^{-2.60}$，即幂指数$\gamma\approx2.6$。由R. J. Mondragón等[7]对IPv4 AS级Internet的研究表明，Internet的幂指数$\gamma\approx2.2$，这表明目前IPv6 Internet的度分布与IPv4的度分布近似，所以会存在很多相似的特征，可以借鉴之前的研究成果来研究IPv6 Internet的相关特性。

3 网络的抗毁性分析

Internet遭受随机(如路由器故障)或蓄意攻击后，网络节点或边便会失效，为了完成路由任务，部分路径不得不做出调整。特别地，当失效的节点或边为路由的“必经之路”时，则该路由任务不得不终止。因此，一旦Internet遭受攻击，人们最关心两个问题：(1)网络的连通水平。部分节点和链路的失效将导致Internet拓扑网络结构改变，路由任务的可达性也随之降低。(2)网络的疏密程度。随着节点的失效，网络的聚类情况会发生怎样的改变？基于上述分析，本文在借鉴现有复杂网络抗毁性测度研究成果[5,18,19]的基础上，提出IPv6 AS级Internet抗毁性测度指标，并以此来分析网络的抗毁性。

3.1 抗毁性测度指标

复杂网络的抗毁性测度指标主要用来度量网络节点和边在遭受攻击后网络的连通水平或聚集程度的变化情况，因而，测度指标主要表现的是网络结构的全局或局部网络抗毁性能。目前常用的抗毁性指标如网络碎片数目、最大连通子图相对大小、网络直径、平均最短路径长度、网络效率、网络聚类系数、可达节点对数目等[5,6,18]。结合本例具体情况，选用网络链路数、网络碎片数、最大连通子图相对大小及网络聚类系数4个参数作为AS级Internet的抗毁性测度指标，其具体定义如下。

定义1(网络链路数) 即节点间的连边总数，记为M。随着节点删除比例的增大，M越来越小，严重影响着网络的连通性。

定义2(网络碎片数) 当网络出现随机故障或者遭受蓄意攻击时，连通的网络会被破坏，产生一定数量的连通子图，称为网络碎片。在相同的故障或者攻击下，网络碎片数量越大，则说明网络被破坏得越严重，从而网络的抗毁性越差。

定义3(最大连通子图) 当Internet遭受连续攻击后，网络会被分解成若干个连通片，因此网络的整体连通性也是衡量Internet的一个重要性指标，而最大连通子图可以很好地描述网络中各节点的连通程度。研究子图中最大连通子图的相对大小有助于分析网络被破坏后的连通性能，最大子图的规模越大，则网络的抗毁性越好。定义最大连通子图相对大小为$G=\frac{n_{MaxCom}}{N}$，其中，n_{MaxCom}为最大连通子图中网络节点的数量，即其规模大小；N为网络的初始规模。易知$G\in[0,1]$，即当网络完全崩溃时，$G=0$；当网络完全连通时，$G=1$。不难看出，网络的G越大，连通度越高，网络的抗毁性也越强。

定义4(网络聚类系数) 所有节点的聚类系数的平均值称为网络的聚类系数，定义为〈C〉，C值越大，表示整个网络中节点之间形成短距离联系的程度越大，则网络的效率越好。在完全连通图中，C有最大值1，C的大小可以反映网络的抗毁性大小。在AS级Internet拓扑结构中，节点的聚类系数反映了自治系统间联系的疏密程度，而其平均值则反映了整个Internet中所有自治系统分布的疏密程度。

3.2 实验设计

攻击策略是指采取什么方式移除网络中的节点或者边。节点攻击所带来的破坏效果比边攻击带来的破坏效果更严重，故本文以删除节点的方式来进行仿真实验。实验中，每移除一个节点，则相应地移除与之相连的链路。

1)随机故障实验：利用*rand*函数随机产生介于[0,3686]间的数作为待移除的节点(其中，3686为该网络的节点总数，利用*unique*函数对其进行唯一化处理，以避免产生重复的数)，由于随机过程的不确定性，每次实验均进行20次并求其平均值作为结果。

2)蓄意攻击：度中心性(DC)作为复杂网络最基本的参数，常用来衡量节点的直接影响力；介数中心性(BC)作为复

杂网络中一个重要的统计量，反映了节点或边在整个网络中的重要性和影响力，并能很好地反映网络的负载和流量信息；接近中心性(*CC*)最大的节点对于信息流动具有最佳的观察视野；2012 年 Robert D. duval 等[20]最先提出了拉普拉斯能量算子中心性(*LC*)，并通过不同网络验证了其对于节点重要性评价的准确性。本文采用以上 4 种常用的节点重要性评价方法作为蓄意攻击策略，研究 AS 级 Internet 的抗毁性，并对比其破坏效果。

实验中，按照不同攻击策略的参数值由大到小的顺序依次删除节点，由于该过程是确定性过程，因此每次实验只需进行一次。特别地，用 E_i 来表示某种蓄意攻击的破坏效果，例如，用 E_{DC} 来表示基于度的蓄意攻击所产生的破坏效果。

3.3 实验结果及分析

按照上述的实验步骤，分别采取随机故障和蓄意攻击两种方式对其进行仿真。下面对 4 个测度指标的仿真结果逐一进行分析。

3.3.1 网络链路数的变化图

图 4 和图 5 分别为随机故障的链路数相对大小变化曲线图和蓄意攻击的链路数相对大小变化曲线图。

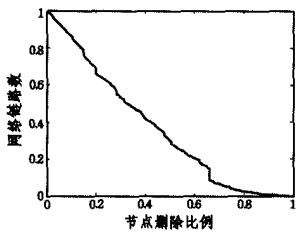

图 4 随机故障下的网络链路变化曲线

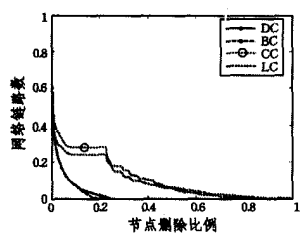

图 5 蓄意攻击下的网络链路变化曲线

由图 5 可知，在随机故障和蓄意攻击两种策略下，网络链路的数量总体上呈逐渐下降的趋势，且为单调递减。以 f 表示节点删除的比例，f_{random} 代表随机故障删除节点比例，由图 5 易知，当 $f_{DC}\in[0,0.15]$、$f_{BC}\in[0,0.17]$、$f_{CC}\in[0,0.04]$、$f_{LC}\in[0,0.05]$时，蓄意攻击的链路数目要比随机故障下降快得多，当 60%的节点被随机删除时，网络链路数才减少 80%；而以 *DC* 和 *BC* 为攻击策略时，仅仅删除 10%的节点，链路数已减少了 80%，删除 20%左右的节点时，链路数的相对大小接近于 0；而基于 *CC* 和 *LC* 的攻击在删除 30%左右的节点时，节点减少至 20%。不同攻击方式破坏效果排序为：$E_{BC}\approx E_{DC}>E_{LC}\approx E_{CC}\geqslant E_{random}$。

3.3.2 网络碎片数

图 6 和图 7 为不同攻击策略下，删除节点后生成的网络碎片数目的变化曲线。

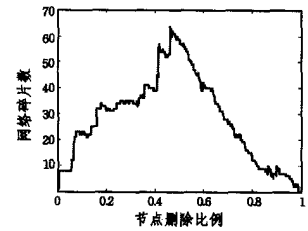

图 6 随机故障下的网络碎片变化曲线

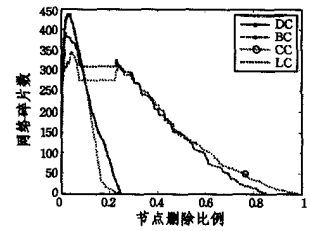

图 7 蓄意攻击下的网络碎片变化曲线

由图 6 可以看出，网络在出现随机故障时，网络碎片数存在一定的波动，总体呈先上升后下降的趋势，当删除 50%的节点左右时达到最大，最大值为 65；而在蓄意攻击作用下，仅删除2.5%的节点时网络碎片数就达到最大，最大值为 440，破坏效果：$E_{BC}\approx E_{DC}>E_{LC}\approx E_{CC}\geqslant E_{random}$。

3.3.3 最大连通子图相对大小

图 8 和图 9 为不同攻击策略下，最大连通子图的相对大小与节点删除比例之间的变化曲线。

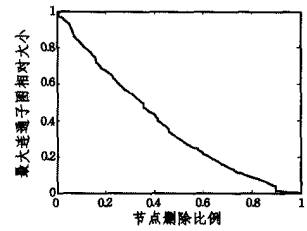

图 8 随机故障下最大连通子图相对大小变化曲线

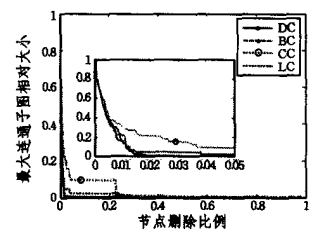

图 9 蓄意攻击下最大连通子图相对大小变化曲线

由图 8 可知，随着随机故障删除的节点比例增大，AS 级 Internet 的最大连通子图的相对大小逐渐减小，变化较为平缓，随机删除 10%的节点后，最大连通子图的相对大小为 80%，说明 AS 级 Internet 基本保持连通，不受影响。图 9 中，仅仅删除 5%的节点后，就可使最大连通子图的相对大小锐减至 10%以下。特别地，基于 *DC* 和 *BC* 的攻击作用下，仅需删除 1%的节点就可使整个网络接近崩溃，所以仅截取了前 5%的变化情况用于对比分析。对比图 8 和图 9 可知，蓄意攻击作用下的最大连通子图变化远远大于随机故障作用下的变化，攻击效果排序为：$E_{DC}\approx E_{BC}>E_{LC}>E_{CC}\geqslant E_{random}$。

3.3.4 网络聚类系数

图 10 和图 11 为不同攻击策略下网络的聚类系数相对变化曲线。

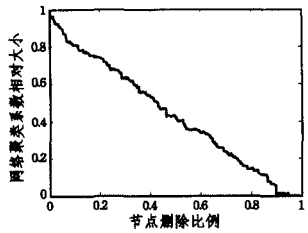

图 10　随机故障的网络聚类系数相对变化曲线

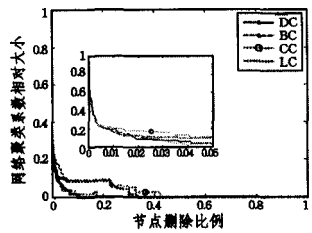

图 11　蓄意攻击下的网络聚类系数相对变化曲线

由图 10 和图 11 可知，随机故障下，聚类系数相对大小的变化与最大连通子图的变化近似，呈线性递减。而在蓄意攻击下，聚类系数的变化是相当迅速的，仅仅删除 1%的节点就可使聚类系数降低 85%，节点删除比例小于 0.5%时，基于 *CC* 的攻击策略的破坏效果最好，当节点删除比例大于 1%时，*DC* 和 *BC* 的破坏程度更大，删除 5%的节点基本可使网络聚类系数降低至 0。

结束语　无论是军用还是民用方面，对 Internet 的抗毁性研究都具有很强的理论意义和实用价值。本文对 CAIDA 最新的 IPv6 AS 级 Internet 数据的拓扑结构进行建模，并以复杂网络理论分析了其结构特性，研究了不同攻击策略下的抗毁性测度，得出了以下一些重要结论：

1）IPv6 Internet 与 IPv4 Internet 的拓扑结构存在相似之处，如度分布的幂指数近似相等（介于 2～3 之间）及都具有小世界和无标度特性。

2）IPv6 Internet 同样具有鲁棒且脆弱的特性，综合 4 组抗毁性测度分析结果可知，当攻击网络节点数小于 1%时，E_{DC} 和 E_{BC} 具有很强的相似性，当节点攻击数大地于 3%时，E_{DC} 破坏效果最好。从抗毁性的角度来说，度中心性能很好地度量 IPv6 AS 级 Internet 的节点重要性，并且其时间复杂度远低于其他的节点重要性指标，在以后分析更大规模的 Internet 时更具优势。

希望本文的研究结论可以为分析 IPv6 Internet 的拓扑结构特性、规划和管理 Internet 拓扑结构提供参考。下一步的工作重点是将不同观测点的数据进行整合，分析 IPv6 Internet 的演化规律以及构造更加完整的 IPv6 Internet 拓扑结构；同时还应该考虑网络的动态特性，研究基于级联失效的 IPv6 Internet 的抗毁性。

参 考 文 献

[1] 王大东，王洪军，王瑞，等. 一种基于 AS 的 Internet 拓扑模型[J]. 计算机工程，2005，31(4)：23-25
Wang Da-dong，Wang Hong-jun，Wang Rui，et al. A model of Internet topology based on AS[J]. Computer Engineering，2005，31(4)：23-25

[2] 付大愚，赵海，张君，等. AS 级 Internet 拓扑幂率和节点时效分析[J]. 计算机科学，2009，36(9)：21-24
Fu Da-yu，Zhao Hai，Zhang Jun，et al. AS-level Internet topology power-law and node aging analysis[J]. Computer Science，2009，36(9)：21-24

[3] Ellison B，Fisher A D，Linger R C，et al. Survivable network systems：an emerging discipline[R]. Pittsburgh：Carnegie Mellon University，1997

[4] 谭跃进，吕欣，吴俊，等. 复杂网络抗毁性研究若干问题的思考[J]. 系统工程理论与实践，2008，28(增刊)：116-120
Tan Yue-jin，Lv Xin，Wu Jun，et al. On the invulnerability research of complex networks[J]. Systems Engineering-Theory & Practice，2008，28(suppl)：116-120

[5] Albert R，Jeong H，Barabási A. Error and attack tolerance of complex networks[J]. Nature，2000，406(8064)：378-382

[6] Albert R，Barabasi A L，et al. Statistical mechanics of complex networks [J]. Revv Mod Phys，2002(74)：47-97

[7] Zhou Shi，Mondragón R J. Redundancy and Robustness of the AS-level Internet topology and its models[J]. Electronics Letters，2004，40(2)：151-152

[8] 汪涛，吴琳丽. 基于复杂网络的城市公交网络抗毁性分析[J]. 计算机应用研究，2010，27(11)：4084-4086
Wang Tao，Wu Lin-li. Research on invulnerability of erban transit network based on complex network[J]. Application Research of Computers，2010，27(11)：4084-4086

[9] 谢丰，程苏琦，陈冬青，等. 基于级联失效的复杂网络抗毁性[J]. 清华大学学报(自然科学版)，2011，51(10)：1342-1347
Xie Feng，Cheng Su-qi，Chen Dong-qing，et al. Cascade-based attack vulnerability in complex networks[J]. Journal of Tsinghua University(Science and Technology)，2011，51(10)：1342-1347

[10] 曾小舟，唐笑笑，江可申. 基于复杂网络理论的中国航空网络抗毁性测度分析[J]. 系统仿真技术，2012，8(2)：111-116
Zeng Xiao-zhou，Tang Xiao-xiao，Jiang Ke-shen，et al. Measure of China airline networks invulnerability based on complex networks[J]. System Simulation Technology，2012，8(2)：111-116

[11] 黄仁全，李为民，董雯，等. 不同攻击策略下作战体系网络抗毁性研究[J]. 复杂系统与复杂性科学，2012，9(3)：62-69
Huang Ren-quan，Li Wei-min，Dong Wen，et al. Research on the invulnerability of combat SoS under different attack strategies [J]. Complex Systems and Complexity Science，2012，9(3)：62-69

[12] 种鹏云，帅斌. 基于复杂网络的危险品运输网络抗毁性测度分析[J]. 系统工程理论与实践，2014，34(5)：1059-1065
Chong Peng-yun，Shuai Bin. Model of cascading failure in hazardous materials transportation network under series of terrorist attacks[J]. Systems Engineering-Theory&Practice，2014，34(4)：1059-1065

[13] Watts D J，Strogatz S H. Collective dynamics of "'small-world"' networks[J]. Nature，1998，393(6684)：440-442

[14] Barabási A-l，Albert R. Emergence of scaling in random networks [J]. Science，1999，286(5439)：509-512

[15] 汪小帆，李翔，陈关荣. 网络科学导论[M]. 北京：高等教育出版社，2012：158-159
Wang Xiao-fan，Li Xiang，Chen Guan-rong. NetWork Science：An Introduce[M]. Beijing：Higher Education Press，2012：158-159

（下转第 202 页）

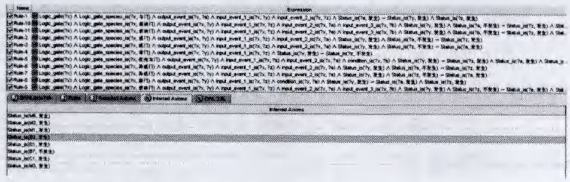

图 5　B6 事件不发生的实验结果

通过比较发现，利用本文提出的方法对故障树进行分析，实验结果与用故障树分析法得出的结果是一致的，说明本文提出的方法是可行的。

结束语　使用故障树分析法对故障树进行分析，能极大地提高硬件的可靠性和安全性，在系统安全工程中发挥着重要的作用。故障树分析法除了能对系统故障进行快速定位外，还能通过计算事件发生的概率，来找出系统的薄弱环节，从而提高系统的安全性。前者属于故障树分析法的定性分析，后者属于故障树分析法的定量分析。但故障树本身存在一些缺陷，例如重复构建问题。

本体是对概念以及概念之间关系的精确描述，在知识的重用和共享方面优势明显，能很好地解决故障树的重复构建问题。但是，目前还没有一个大规模、可共享、可重用的故障树本体。因此，建立一个良好的故障树本体具有重要的意义。本文根据“七步法”构建了一个故障树领域本体，在此基础上，对如何根据事件之间的逻辑关系来构建相应的 SWRL 规则进行了研究。实验证明，使用本文提出的方法能在解决故障树重复构建问题的同时，不对系统故障的快速定位产生影响。下一步的工作是研究探讨如何利用故障树领域本体和 SWRL 规则对故障树进行定量分析。

参 考 文 献

[1] Arnold F, Belinfante A, Van der Berg F, et al. DFTC$_{ALC}$: A Tool for Efficient Fault Tree Analysis[M]// Computer Safety, Reliability, and Security. Heidelberg: Springer Berlin Heidelberg, 2013: 293-301

[2] Weikum G, Theobald M. From information to knowledge: harvesting entities and relationships form web sources[C]// Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on principles of database system. Indiana: ACM Press, 2010: 65-76

[3] Navigli R, Ponzetto S P. BabelNet: The automatic construction, evaluation and application of a wide-coverage multilingual semantic network[J]. Artificial Intelligence, 2012, 193: 217-250

[4] Cimino J J. High-quality, standard, controlled healthcare terminologies come of age[J]. Methods of information in medicine, 2011, 50(2): 101-104

[5] 葛强，沈国华，黄志球，等. Web 服务中支持本体推理的隐私保护研究[J]. 计算机科学与探索，2013，7(6)：536-544
Ge Qiang, Shen Guo-hua, Huang zhi-qiu, et al. Web Research on Privacy Protection Based on Ontology in Web Service [J]. Journal of Frontiers of Computer Science and Technology, 2013, 7(6): 536-544

[6] 黄凤. 基于描述逻辑的访问控制策略冲突检测方法研究[D]. 南京：南京航空航天大学，2010
Huang Feng. A description logic-based approach for access control policy conflict detection [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2010

[7] 钟秀琴，符红光，佘莉，等. 基于本体的几何学知识获取及知识表示[J]. 计算机学报，2010，33(1)：167-174
Zhong Xiu-qin, Fu Hong-guang, She Li, et al. Geometry knowledge Acquisition and Representation on Ontology[J]. Chinese Journal of Computers, 2010, 33(1): 167-174

[8] 郑晓洁，张琳. 本体映射中相似度计算的改进[J]. 计算机科学，2013，40(12)：108-112
Zheng Xiao-jie, Zhang Lin. Modification of Similarity Computation in Ontology Mapping [J]. Computer Science, 2013, 40(12): 108-112

[9] 杜小勇，李曼，王珊. 本体学习研究综述[J]. 软件学报，2006，17(9)：1837-1847
Du Xiao-yong, Li Man, Wang Shan. A survey on ontology learning research[J]. Journal of Software, 2006, 17(9): 1837-1847

[10] Noy N F, McGuinness D L. Ontology Development 101: A Guide to Creating Your First Ontology[DB/OL]. (2001-08) [2014-08]. http://protege.stanford.edu/publications/ontology_development/ontology101.pdf

[11] Horrocks I, Patel-Schneider P F, Boley H, et al. SWRL: A semantic web rule language combining OWL and RuleML[OL]. http://xml.coverpages.org/ni2004-05-21-a.html

[12] Boley H B G, Tabet S. Rule Markup Tutorial[DB/OL]. (2005-05) [2014-08]. http://www.ruleml.org/papers/tutorialruleml-20050513.html

[13] W3C. OWL Web Ontology Language Semantics and Abstract Syntax[DB/OL]. (2004-02)[2014-08]. http://www.w3.org/TR/2004/REG-owl-semantics-20040210.html

(上接第 165 页)

[16] 于会，刘尊，李勇军. 基于多属性决策的复杂网络节点重要性综合评价方法[J]. 物理学报，2013，62(2)：20204-9
Yu Hui, Liu Zun, Li Yong-Jun, et al. Key nodes in complex networks identified by multi-attribute decision-making method[J]. Acta Physica Sinica, 2013, 62(2): 20204-9

[17] Fruchterman T M J, Reingold E M. Graph Drawing by Force-directed Placement[J]. Software-practice and Experience, 1991, 21(11): 1129-1164

[18] Holme P, Kim B J, Yoon C N, et al. Attack vulnerability of complex networks [J]. Physical Review E, 2002, 65(5): 56-109

[19] Jeong H, Mason S, Barabási A l, et al. Lethality and centrality in protein networks[J]. Nature, 2001(411): 41-42

[20] Qi Xing-qin, Duval R D, Christensen K, et al. Terrorist Networks, Network Energy and Node Removal A New Measure of Centrality Based on Laplacian Energy[J]. Scientific Research, 2013, 10(4236): 19-31