文章编号:1673 - 0062(2009)01 - 0081 - 04

基于业务的复杂通信网络抗毁性仿真分析

丁　琳,谭敏生,肖　炜

(南华大学 计算机科学与技术学院,湖南 衡阳 421001)

摘　要:针对 Internet 这一典型的复杂网络,结合 TCP 拥塞控制协议能重新调整数据流流速的特点,提出了两个基于业务的抗毁性测度—通信效用和带宽利用率,从不同角度分析了 Internet 的抗毁性. 并与经典的随机图进行了比较分析,仿真结果表明,Internet 仍然具有鲁棒且脆弱性.

关键词:复杂网络;Internet;带宽分配;抗毁性

中图分类号:TP393.08　　**文献标识码**:B

Invulnerability Simulation Analysis of Complex Communication Networks Based on Traffic

DING Lin, TAN Min-sheng, XIAO Wei

(School of Computer Science and Technology, University of South China, Hengyang, Hunan 421001, China)

Abstract: Due to a typical example of complex networks for the Internet, according to the characteristics that the TCP congestion control protocols readjust the flow rates, two new measures of invulnerability based on traffic are proposed: the traffic utility and the utilization ratio of bandwidth, this paper analyzes Internet invulnerability from various angles, and compare the internet real data with the classic random graph, the simulation results also show that the Internet has "robust yet fragile" property.

Key words: complex networks; Internet; bandwidth allocation; invulnerability

近十年来,复杂网络研究得到了广泛的关注. 实证分析表明,从因特网到新陈代谢网,从社会关系网到城市公共交通网,许多领域的各种网络展现了某些共同的统计性质,如幂率度分布. 在理论研究方面,科学家们也提出了不同的演化网络模型,这些模型使我们进一步理解了复杂网络所具有的统计规律. 近年来研究者们又将目光转向了网络的动力学行为,包括网络容错性和攻击鲁棒性,相继故障以及网络上的传播、同步等各种动力学过程.

网络容错性和攻击鲁棒性是网络抗毁性的研究范畴. 抗毁性关系到网络的安全性,是许多现实世界中的网络普遍关注的问题. 当一个节点失效,原来通向这个节点的流量不得不重新选择路径. 流

收稿日期:2008 - 12 - 02

作者简介:丁　琳(1981 -),女,湖南桃江人,南华大学计算机科学与技术学院助教,硕士研究生. 主要研究方向:计算机网络与信息安全.

量的重分配影响了其它节点的负载,可能由于过载引起一系列的相继故障[1]. 此外,这方面研究最重要的成果就是无标度网络面对随机故障有着很强的鲁棒性,但面对有目的攻击却显得异常脆弱[2].

以往的复杂通信网络抗毁性研究主要关注的是基于连通性的网络抗毁性测度,用最大簇大小来衡量网络的抗毁性. 而且大多都以数据流流速为定值作为假设条件. 在真实的 Internet 中,当一个节点受到攻击,通过这个节点的数据流重新选择路由,TCP 会通过拥塞控制算法调整数据流的流速,使得数据流流速之和小于链路带宽,降低了相继故障发生的可能性,攻击后的网络很可能依然连通,但是流量的变化影响到网络的业务性能,同样可导致网络中的节点不能正常工作. 因此,在分析一个复杂通信网络的抗毁性时,不能仅仅简单地分析网络的连通性,而必须结合网络中的传输业务进行分析,才能较为准确地衡量这个网络的抗毁性. 本文定义了两个指标来测度 Internet 的业务性能,并在这些测度的基础之上,分析了 Internet 在遭受随机攻击和有目的攻击的抗毁性.

1 优化带宽分配算法

假定一个网络,有 L 条数据链路和 S 个数据流. 当数据流 i 通过链路 l,A_{li} 取值为1,否则为0,则矩阵 $\boldsymbol{A} = (A_{li}, 1 \leqslant l \leqslant L, 1 \leqslant i \leqslant S)$ 记录了所有路由信息. 假定数据流 i 流速为 x_i,$x = (x_i, 1 \leqslant i \leqslant S)$ 和 $C = (C_l, 1 \leqslant l \leqslant L)$ 分别表示流速和链路容量向量. 有以下不等式:

$$A_x \leqslant C \tag{1}$$

不等式表明了通信链路对数据流量的限制,即流速之和不能超过链路带宽.

从源节点到目的节点传输数据包的目的是为了满足用户的需求,例如下载文件,浏览新闻和在线预订等. 因此,需要为数据流 i 设置一个效用函数 U_i,并且 U_i 与流速 x_i 相关,本文将它表示为 $U_i(x_i)$. 为了得到最优带宽分配方法,拥塞控制协议要解决如下优化问题[3]:

$$\max_x \sum_i U_i(x_i) \text{ 且 } A_x \leqslant C, x \geqslant 0 \tag{2}$$

考虑两种攻击:随机攻击(随机移除网络中的节点)和有目的攻击(移除网络中度值最大的节点),当节点被攻击,则立即从网络中删除该节点以及与节点相邻的边,流经这个节点的数据流将重新选择路由,以找到最短路径. 节点和边的删除以及路由的重选改变了矩阵 A 的值. 基于被修改的路由信息,拥塞控制协议计算新的最优带宽分配值. 因为 Internet 的大规模性和全局拓扑信息的不可知性,使用分散式算法[4] 来解决优化问题.

下面是链路 l 的代价计算算法:

1) 得到经过链路 l 的所有数据流的流速;

2) 计算 l 的代价;

$$p_l(t+1) = [p_l(t) + \alpha(x^l(t) - C_l)]^+$$

3) 并向所有经过 l 的数据流发送新的代价 $p_l(t+1)$.

其中:$x^l(t) = \sum_{s \in S(s)} x_s(t)$ 为 t 时刻通过链路 l 的所有数据流的流速和,$S(l)$ 为经过链路 l 的所有数据流的集合,$[z]^+ = \max\{z, 0\}$.

下面是数据流 s 调整流速的算法:

1) 接收流 s 经过的所有链路的代价;

2) 基于 $p^s(t) = \sum_{l \in L(s)} p_l(t)$,选择一个新的传输速率 $x_s(t+1)$;

3) 并向所有链路 l 发送新的流速 $x_s(t+1)$.

其中:$L(s)$ 为流 s 经过的链路集合.

算法的思想如下:每一步,每条链路接收经过它的所有数据流的流速,然后基于流量调整它的代价,并且把新的代价发送给所有经过它的数据流. 同样地,每个数据流接收它经过的所有链路的代价,然后基于这些代价值计算新的流速,并且把新的流速发送给它要经过的链路. 通过这种方法,链路 l 和流 s 只需要知道有关它的局部信息,而不需要获得整个网络的全局信息.

2 仿真分析

2.1 仿真设计

仿真设计主要包括网络模型、链路容量以及抗毁性能指标的设计.

2.1.1 网络模型

从联机数据库里得到 Internet AS 层的互连信息[5],选择最大的连通部分作为 Internet 子网,它包含 1470 个节点和 3131 条链路,研究表明该子网的节点连接度服从幂率分布. 本文以该子网和 ER 模型生成的随机图作为研究对象. 为了进行对比分析,随机图的节点和边的数量也分别设置为 1470 和 3131. 每个网络随机产生 $S = 4\ 000$ 个数据流,随机选择每个数据流的源 - 目的节点,如果源 - 目的节点之间不只一条最短路径,则随机选择一条.

2.1.2 链路容量

在 Internet 中,链路容量是指链路带宽. 一般

来说,连接那些中心节点的链路需要更大的容量,因为更大的流量负荷要经过它们. 则有:

$$C_{ij} \propto B_i + B_j \tag{3}$$

其中,C_{ij} 为节点 i 到 j 之间链路容量,$\propto$ 表示成比例,B_i 为节点 i 的介数(负荷). 节点 i 的介数定义为任意节点对的最短路径之中,经过节点 i 的数量. 从介数的定义和数据流的路由规则(选择源 - 目节点间的最短路径) 看出,介数描述的是经过节点的平均流量负荷. 一般来说,与链路相连接节点的介数越大,则需要的链路容量也就越大.

2.1.3　性能指标

业务性能从两方面进行测度:效用和利用率. 优化带宽分配的任务就是调整数据流流速,以得到最大的效用. 本文使用总效用 $\sum_i U_i(x_i)$ 作为第一个性能指标,在下面的仿真中,使用:

$$U_i(x_i) = d_i \log(x_i + 1) \tag{4}$$

作为效用函数. 它实际上是 TCP Vegas[6] 中的通信效用函数的简化版本. 其中,d_i 为数据流 i 的最短路径长度.

第二个性能指标是带宽利用率. 当总效用达到最大值,仍然存在一些空闲带宽,也就是说带宽的一部分被浪费. 从经济的角度考虑,这种浪费应尽可能的少,或者说,带宽的利用率应该越高越好. 带宽利用率如下定义:

$$u = \frac{\sum_l \sum_i A_{li} x_i}{\sum_l C_l} \tag{5}$$

2.2　仿真结果

图 1 描述 Internet 子网总通信效用的仿真结果. 在图中,总效用是总容量的函数,当链路带宽增加,每个数据流就拥有更多的带宽资源,总效用将随之增加. 在图 1 里还比较了网络在随机攻击和有目的攻击两种情况下的网络性能,随机攻击曲线与初始网络曲线重叠,而有目的攻击曲线下降了大约 15%. 仿真结果表明:中心节点在 Internet 通信中确实扮演着重要的角色. 在 Internet 中,连接度大的节点往往承载着高负荷流量,假如该节点被攻击,大部分数据流将受到影响,导致 Internet 性能急剧下降;另一方面,幂率表明了只存在一小部分度值很大的节点,在随机攻击中,更有可能攻击到度值小的节点,这些节点对整个网络性能的影响不大. 这就是随机攻击曲线与初始图曲线重叠的原因.

图 2 画出 Internet 子网带宽利用率随总容量变化的曲线. 随着总容量 $\sum_l C_l$ 的增加,带宽利用率减少. 结合图 1 仿真可知,虽然总效用在增加,但是有更多的带宽资源被浪费. 图 2 也比较了三种情况,仿真结果与图 1 相类似,随机攻击曲线与初始网络曲线重叠,而有目攻击的曲线大大降低.

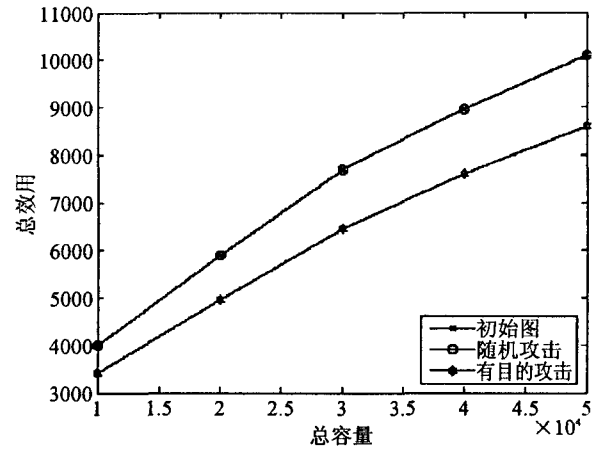

图 1　Internet 子网的总通信效用

Fig. 1　Total traffic utility in a subnetwork of the internet

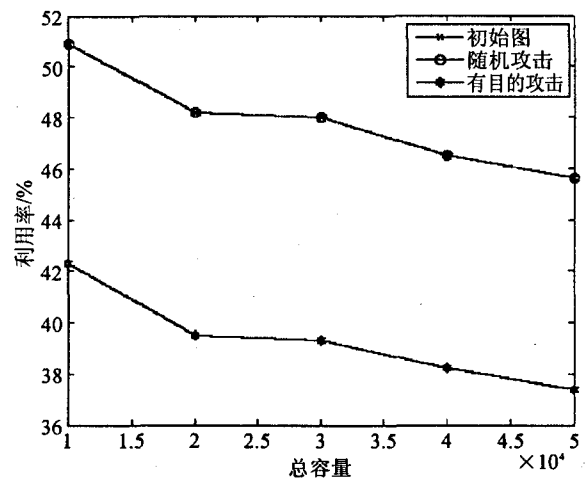

图 2　Internet 子网的带宽利用率

Fig. 2　Utilization ratio of the bandwidth in a subnetwork of the internet

相比之下,图 3 和图 4 表示随机网络的情况. 随机网络对随机攻击和有目的攻击都有很强的鲁棒性. 网络遭到攻击后,曲线稍有轻微下降. 这是因为随机图是同质网络[7],没有拥有巨大连接数量的节点,流量负载在所有节点中均匀分布,因此,攻击某个节点(不论随机还是有目的攻击)对

整个网络的业务性能影响不大. 仿真结果也验证了以往随机图相继故障的研究结果.

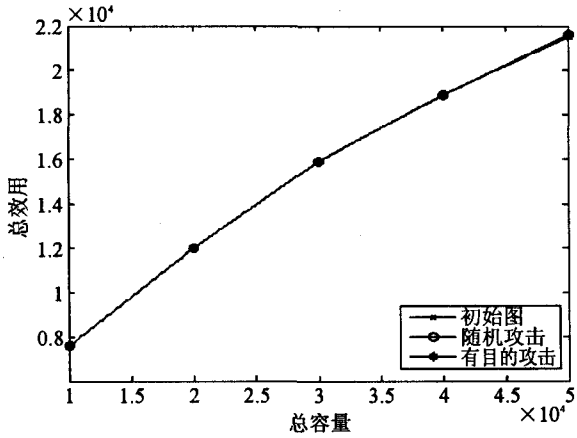

图 3 随机图的总通信效用

Fig. 3 Total traffic utility in a random graph

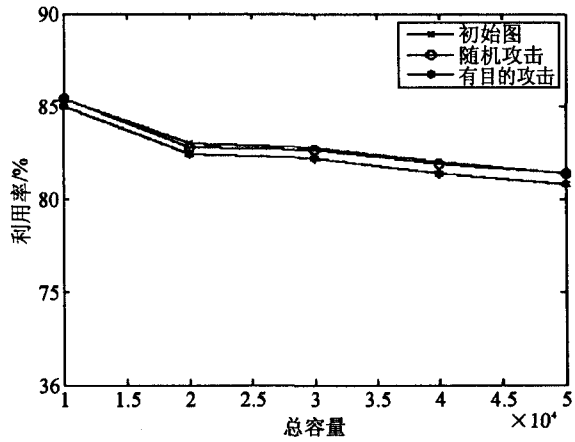

图 4 随机图的带宽利用率

Fig. 4 Utilization ratio of the bandwidth in a random graph

3 结论

抗毁性是网络可靠性的重要测度. 抗毁性分析是保证网络安全可靠必不可少的手段,对网络进行抗毁性分析就如同生活中的"体检",可使我们对网络安全做到"未雨绸缪",从而更好地部署安全措施.

本文研究了 Internet 在考虑实际 TCP 拥塞控制协议下的抗毁性. Internet 在遭受有目的攻击后,业务性能明显降低,而随机攻击对网络性能几乎没有影响. 对随机网络而言,随机攻击和有目的攻击都对网络性能影响不大. 虽然通信模型和测度指标与以往研究明显不同,但仿真结果得出相似的结论,无标度网络具有鲁棒且脆弱性,而随机图对随机攻击和有目的攻击都具鲁棒性. 因此,本文认为该评估方法能够有效地测度 Internet 的抗毁性.

参考文献:

[1] Asha J, Newthb D. Optimizing complex networks for resilience against cascading failure[J]. Physica A, 2007, 380:673 - 683.

[2] 谭跃进,吴 俊. 复杂网络抗毁性研究综述[J]. 系统工程, 2006, 24(10):1 - 5.

[3] Kelly F P, Maulloo A K, Tan D K H. Rate control for communication networks: shadow prices, proportional fairness and stability[J]. J. Oper. Res. Soc, 1998, 49(3):237 - 252.

[4] 黄利华. Internet 自治域层拓扑特性研究与建模[D]. 大连,大连理工大学, 2007.

[5] Low S H, Lapsley D E. Optimization flow control - I: Basic algorithm and convergence [J]. IEEE/ACM Trans. Netw, 1999, 7(6):861 - 874.

[6] Caida. Internet measurement, Internet analysis [DB/OL]. http:/moat. nlanr. net, 2006.

[7] Low S H, Paganini F, Doyle J C. Internet congestion control[J]. IEEE. Syst. Mag, 2002, 20:2 - 43.

[8] 张俊良. 复杂网络可靠性研究[D]. 大连:大连理工大学, 2006.