

文章编号:1001-9081(2005)02-0409-03

## 基于 UDP 的分布式拒绝服务攻击的自相似性研究

任冬冬, 杨东勇

(浙江工业大学 信息工程学院, 浙江 杭州 310014)

(dongdon0038@163.com)

**摘 要:**在 NS-2 中模拟了基于 UDP 协议的分布式拒绝服务攻击, 实验结果表明, 针对不同的攻击模型和不同的网络负荷, 当网络中发生基于 UDP 协议的分布式拒绝服务攻击的时候, 网络流量仍具有较好的自相似性。这个对 DDoS 攻击流量的特性和 DDoS 防御的研究都具有十分重要的意义。

**关键词:**自相似性; 分布式拒绝服务攻击; 流量模型

**中图分类号:** TP393.08 **文献标识码:** A

## Research on self-similarity of DDoS traffic based on the UDP

REN Dong-dong, YANG Dong-yong

(College of Information Engineering, Zhejiang University of Technology, Hangzhou Zhejiang 310014, China)

**Abstract:** In this work, DDoS based on UDP was simulated in NS-2, Results show that traffic of network still has self-similarity when DDoS based on UDP is happening in the network regardless of different kind of attack model and different network load. This is significant to research of characteristic of DDoS traffic and defense against DDoS.

**Key words:** self-similarity; DDoS; traffic model

### 0 引言

长期的研究表明, 无论是在局域网、广域网还是在 Internet 上, 流量都呈现出长程相关性甚至是自相似性<sup>[1-3]</sup>, 而传统的 Poisson 流模型已经不再适合描述当代计算机网络的特性<sup>[2]</sup>。文献[4]指出, 网络的正常流量通常是长程相关的, 并可以用自相似模型来描述。关于网络自相似性的研究有很多, 如: 文献[5]中自相似性对网络性能的影响; 文献[5]和文献[6]中关于网络自相似性的建模, 以及文献[3]、文献[7]、[8]中对网络流量自相似性原因的探讨。但是对于单纯的 DDoS 攻击流量的自相似性研究却不多。文献[9]利用网络的自相似性的变化来检测 DDoS 的发生, 但却没有对攻击流是否具有自相似性给出结论; 文献[10]是对突发数据流对于在光纤上流量自相似性的影响做了研究, 但是, 突发数据流毕竟不同于 DDoS 的攻击流。

当 DDoS 发生的时候, 即当网络负荷比较大时, 大量的攻击流势必会影响网络本身的自相似特性。在本文中, 通过在 NS-2 中 DDoS 的仿真实验表明, 当网络中发生大量的 UDP 数据流时, 在所测试的攻击流量模型和网络负荷下, 网络依然保持着自相似性, 而基于 UDP 协议的 DDoS 攻击本身也具备自相似特性。

### 1 网络模型

在 NS-2 中, 我们建立了两个网络模型, 一个是最简单的两节点的网络模型, 如图 1(a)。链路带宽设置成 1M, 链路的

主队列大小设置成 10, 发送延时设置成 5ms, 数据包大小设置成 500 bytes。其中, 节点 1 作为发送节点, 向节点 2 发送 UDP 数据包。另一个是五节点的网络模型, 如图 1(b)。其中节点 3 到节点 4 的链路带宽设置成 1M, 链路的主队列大小设置成 10, 发送延时设置成 5ms, 数据包大小设置成 500 bytes。节点 0、节点 1、节点 2 作为发送节点产生网络流量, 而节点 4 作为接收节点。

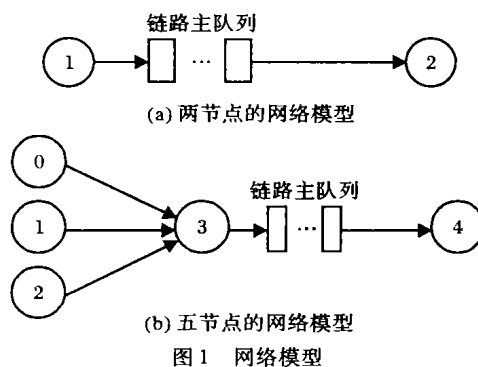


图 1 网络模型

### 2 两节点模拟测试

#### 1) 自相似性描述

有关自相似特性的描述有很多种, 如 R/S 统计分析、方差时间分析、周期圆分析和小波分析等。本文采用的是方差时间分析来描述自相似性。针对不同长度的时间段值( $m$ ), 求出其平均流量的方差, 然后分别以  $m$  和方差的 log 值作为横、纵坐标绘图(V-T图)。若图形的斜率 $\beta$ ( $-1 < \beta < 0$ ), 则

收稿日期: 2004-07-15; 修订日期: 2004-10-08

作者简介: 任冬冬(1977-), 男, 浙江余姚人, 硕士研究生, 主要研究方向: 网络安全、网络管理; 杨东勇(1961-), 男, 浙江天台人, 教授, 主要研究方向: 计算机智能系统、计算机网络。

表明该时间序列具有自相似特性。而描述自相似程度的 Hurst 参数和  $\beta$  有着如下的关系:  $H = 1 + \frac{\beta}{2}$ 。虽然方差时间分析并不是一个很精确的估计 Hurst 参数的方法,但是,当仅仅需要知道时间序列是否具有自相似特性时,这种方法是有效的<sup>[11]</sup>。

## 2) 不同的攻击模型

在第一种网络模型中,我们考虑是以下两种 DDoS 的攻击模型,如图 2。图 2(a)中是恒速的攻击模型,其攻击速度始终保持在一个恒定的数值,而图 2(b)则是周期性的攻击,攻击速度是一个周期性变化的过程。

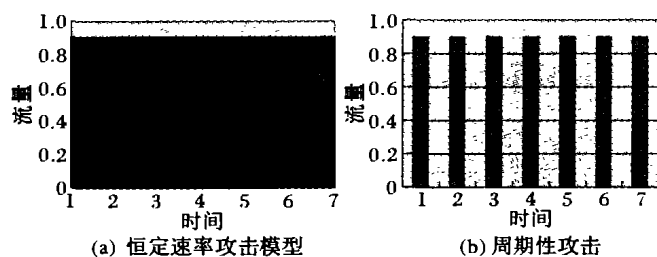


图 2 两种 DDoS 的攻击模型

为了更加接近于真实的进攻流,在实验中攻击流加入了随机的噪音,对  $m$  的取值从 10 毫秒到 10 秒不等,速度分别取了 0.3M、0.99M 和 1.1M,实验结果如图 3。图 3(a)是在恒定速率攻击下的流量的方差时间图,图 3(b)是在周期性攻击流量下的流量方差时间图。

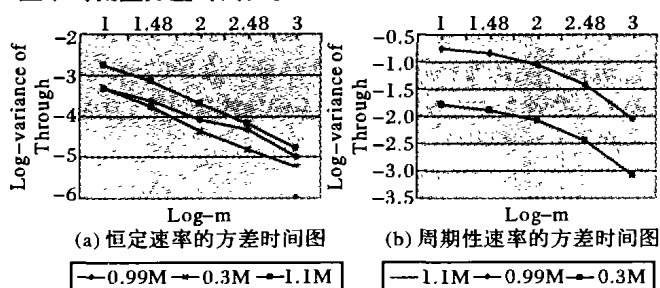


图 3 实验结果

当攻击速度在 0.3M 时,也就是网络处在轻负荷状态下,此时,链路的主队列中并无等待发送的数据包,从图 3 可以看出,其斜率是在  $-1 \sim 0$  之间,说明流量具有自相似特性。当发送速度在 0.99M 时,因为节点 1 和节点 2 之间的链路带宽设定在 1M,所以此时网络的负荷相对比较大,在链路的主队列中已经有了等待发送的数据包,而且由于随机噪音的加入,网络中已经不定时的出现丢包现象。从图 3(a)中看出,当发送速度恒定时,整条曲线的斜率依然还是在  $-1 \sim 0$  之间,所以,流量依然具有自相似的特性,但是,我们也看到,其曲线已经不如 0.3M 时那么的平滑,并且在  $\text{Log} - m = 2.48$ ,即  $m \approx 300$  时有了波动,这个是由于链路中出现随机丢包而造成的。另一方面,则由图 3(b)看出,当流量的产生机制为周期性变化时,除了数值上的变化外,其曲线形状几乎和 0.3M 时相同。这个和 NS-2 的流量发生器流量产生的特点有关,因为在模拟周期性流量时用的是服从指数分布的 On/Off 流量发生器,在“On”状态,数据包以一定的速率发送;在“Off”状态,数据包停止发送。两种状态的时间符合指数分

布。最后,用超过带宽的发送速度 1.1M 进行了网络大负荷实验,此时,在链路的主队列中已经充满了等待发送的数据包,并且链路上总是有丢包现象发生。从图 3(a)可以看出,1.1M 的曲线斜率依然在  $-1 \sim 0$  之间,流量还是具有自相似特性,而且整条曲线比较平滑。在图 3(b)中,1.1M 和 0.99M 的曲线几乎重合,说明流量具有了自相似特性。综上所述,无论处在哪种流量产生机制,哪种网络负荷下,流量都保持了自相似的特性。

## 3) 加入实际局域网流量数据的模拟测试

在上述的结果的基础上,实验中加入文献[12]中的实际局域网的流量数据,并挑选了两组有代表性的速率,分别是 0.99M 和 1.1M,因为这两种速度能描述发生基于 UDP 协议的分布式拒绝服务攻击时网络流量状况。结果如图 4 所示。从曲线的斜率在  $-1 \sim 0$  之间我们可以得出其流量都保持了自相似特性。其中,图 4(b)中,0.99M 和 1.1M 的曲线几乎重合。

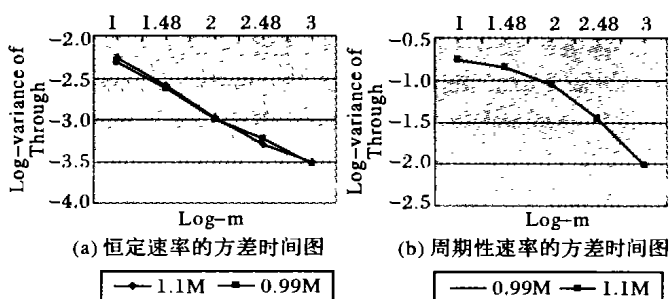


图 4 流量的曲线斜率

从上面的实验可以得出,无论对于恒定速率的攻击模型还是周期性变化的攻击模型,其攻击流量都具有自相似的特性。

## 3 加入实际流量数据的攻击模拟测试

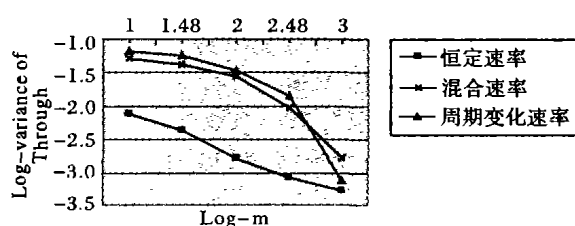


图 5 多节点的方差时间图

图 1(b)所示的网络模型是模拟了实际 DDoS 的多个攻击节点同时向目标主机发送大量数据包。图 5 是在第二个网络模型中实验结果的方差时间图,在网络的总流量中,除了设置的攻击流量外,还加入了实际局域网的流量数据。总共做了三次实验。第一次实验中,三个发送节点即节点 0、节点 1 和节点 2 均以恒定的速率发送数据包,其总流量是 0.99M;第二次实验中,三个发送节点都以周期变化速率发送数据包,其波峰的总流量也是 0.99M;第三次实验中,把节点 0 设置成恒速发送数据包,而其他两个节点设置成以周期变化速率发送数据包。从图中我们可以看出,无论是哪种攻击模型,曲线的斜率都在  $-1 \sim 0$  之间,所以流量都保持着自相似特性。

## 4 结语

由上述的实验可以得出,当网络中发生基于UDP协议的DDoS攻击时,其网络流量依然保持了自相似特性,而且攻击流量本身也具有自相似特性。无论是单节点的拒绝服务攻击还是多节点的协同的分布式拒绝服务攻击,无论是恒定攻击流量还是周期性变化的攻击流量都保持了自相似的特性。实验所用的协议之所以是UDP协议是因为从流量变化的角度看,相对于TCP和ICMP协议,UDP协议比较简单,只有攻击流而没有响应流,能更好的反映出流量本身的特性。当网络流量大时,TCP协议本身就有其拥塞控制机制来调节流量(虽然这种调节机制对于DDoS来讲是微不足道),而ICMP协议也有对等于攻击流的响应流在链路中。

实际的攻击流往往是这三种协议混合而成的,所以还有很多的问题有待研究,如当TCP拥塞机制作用时的流量变化、进出流量是否具有自相似特性,大规模网络的攻击流自相似特性等,都是下一步要做的工作。

#### 参考文献:

- [1] LELAND WE, TAQQU MS, WILLINGER W, *et al.* On the self-similarity nature of Ethernet traffic[ A ], in Proc ACM SIGCOMM [ C ], 1993. 183 - 193.
- [2] PAXSON V, FLOYD S. Wide-Area Traffic: The failure of Poisson modeling[ J ]. in IEEE/ACM Trans on Networking, 1995, 3(3): 226 - 44.
- [3] CROVELLA ME, BESTAVROS A. Self-similarity in World Wide Web traffic: Evidence and possible cause[ J ]. in IEEE/ACM Trans

on Networking, 1977, 6: 835 - 846.

- [4] POPESCU A. Traffic Self-Similarity[ A ]. ( invited ) tutorial, IEEE International Conference on Telecommunications, ICT2001 [ C ]. Jun, 2001.
- [5] PARK K, KIM G, CROVELLA M. On the effect of self - similarity on network performance[ A ]. in Proc of the SPIE International Conf on Performance and Control of Network System[ C ], 1997. 296 - 310.
- [6] OST A, BOUDEWIJN RH. Modeling and Evaluation of pseudo self-similar traffic with Infinite-State Stochastic Petri Nets[ A ]. in Proc of the workshop on formal method and telecom[ C ], 1999. 120 - 136.
- [7] PEHA JM. Protocols can make traffic appear self - similar [ A ]. in Proc of the 1997 IEEE/ACM/SCS Comm. Networks and Distributed System. Modeling and Simulation Conf[ C ], 1997. 47 - 52.
- [8] VERES A, BODA M. The chaotic nature of TCP congestion control [ A ]. in Proc IEEE INFOCOM 2000, Tel Aviv, Israel[ C ], 2000. 1715 - 1723.
- [9] 林原. 基于网络自相似性的DDoS攻击检测[ D ]. 成都: 电子科技大学, 2002.
- [10] HU G, DOLZER K, GAUGER CM. Does Burst Assembly Really Reduce the Self-Similarity[ J ]. Conference on Optical Fiber Communication( OFC2003 ). Technical Digest Series, 2003, 86: 124 - 126.
- [11] PAXON V. Fast Approximation of Self-Similar Network Traffic[ R ]. Technical Report LBL36750, U of California, Berkeley, Apr 1995.
- [12] The Internet Traffic Archive[ EB/OL ]. <http://ita.ee.lbl.gov/html/contrib/BC.html>, 1989 - 10 - 03.

(上接第408页)

订单 XML:

```
< order >
  < name > Yang </ name >
  < product > Computer </ product >
  < price > 5999 </ price >  < quantity > 1 </ quantity >
  < cardno > 5555 - 1234 - 4567 - 6789 </ cardno >
</ order >
```

加密 XSLT 代码片断:

```
< xsl: stylesheetversion = "1.0"
  xmlns: xsl = "http://www.w3.org/1999/XSL/Transform"
  xmlns: msxsl = "urn:schemas-microsoft-com:xslt"
  xmlns: encryption = "urn:the-xml-encryption:xslt-csharp" >
  < msxsl: script language = "C#" implement-prefix = "
    encryption" >
    <![CDATA[
      public string Encrypt( string s)
      { ..... }
    ]]>
  </msxsl: script >
  .....
  < xsl: template match = "cardno" >
    < xsl: copy >
      < xsl: value-of select = "encryption: Encrypt(text())" / >
    </xsl: copy >
  </xsl: template >
</xsl: stylesheet >
```

### 3 结语

尽管XSLT有处理XML文档的结构和内容的能力,但是如果其提供诸如加密/解密等其他附加功能则会增加样式表的复杂性并且限制的加密文档所能使用的方法。通过使用扩展函数可以很好地弥补XSLT的这一弱点。由此可见,使用基于扩展函数的XSLT来对XML文档进行元素级加密是有实际意义的。

#### 参考文献:

- [1] W3C. Extensible Markup Language ( XML ) 1.0 ( Third Edition ); W3C Recommendation 04 February 2004 [ S/OL ]. <http://www.w3.org/TR/2004/REC-xml-20040204>, 2004 - 02.
- [2] MARUYAMA H, IMAMURA T. Element - Wise XML Encryption [ EB/OL ]. <http://lists.w3.org/Archives/Public/xml-encryption/2000Apr/att-0005/01-xmlenc.html>, 2000 - 04.
- [3] W3C. XSL Transformations ( XSLT ) Version 1.0; W3C Recommendation 16 November 1999 [ S/OL ]. <http://www.w3.org/TR/1999/REC-xslt-19991116>, 1999 - 11.
- [4] W3C. XML Encryption Syntax and Processing; W3C Recommendation 10 December 2002 [ S/OL ]. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210>, 2002 - 12.
- [5] BARTLETT RG, COOK MW. XML Security Using XSLT[ R ]. Proceedings of the 36<sup>th</sup> Hawaii International Conference on System Sciences ( HICSS'03 ), 2003. 1.