基于NS2的DDoS入侵流模拟

周 刚,孟海涛
(盐城工学院 信息工程学院,江苏 盐城 224051)

摘要:根据网络流量自相似性的形成机理和DDoS攻击流的特点,综合网络中两种常见协议:TCP和UDP协议,提出了一个新的基于NS2的DDoS入侵流模拟方法,实验结果表明,使用该法得到的模拟背景流保持了真实的网络业务流自相似性特征,可用于对入侵流流量特征方面的分析研究。

关键词:入侵检测;分布式拒绝服务;网络模拟器;自相似
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1671-5322(2010)03-0054-04

网络业务流在很长时间范围内都具有相关性,即业务流到达为长相关模型。渐近或严格的自相似模型就是最能够描述这种特性的模型之一[1]。Hurst(赫斯特)参数H是表征自相似程度的重要参数。H的取值范围为$0.5<H<1$,H越大,自相似性程度越高;相反则越低。DDoS(Distributed Denial of Service,分布式拒绝服务)攻击是目前Internet上最难防范的攻击方式之一,自1999年来,许多著名网站如Yahoo、eBay,cNN等都曾遭受过这种攻击,造成了难以挽回的经济损失。DDoS攻击流的存在会导致网络流量自相似性的变化,引起H值的改变,针对此特点进行早期的入侵检测已经成为一个重要的研究课题[2,3]。DDoS攻击对网络业务有较大的破坏性,所以现实的网络环境难以建立。NS2(Network Simulator version 2)是目前学术界广泛使用的一种网络模拟软件,本文就NS2提出一个DDoS入侵流模拟的新方法,该法保持了网络流量的基本特性—自相似性,同时综合了TCP和UDP协议。

1 自相似过程模型及DDoS攻击原理

一个随机过程$\{X(t),t\in R\}$,满足$X(t)=a^{-H}X(at)$,a为正实数,$H>0$是Hurst参数,等号表示统计意义上的相等,那么称这个过程是统计自相似的。

重尾分布:若一随机变量满足重尾分布,则$P[X>x]\sim x^{-\alpha}$,当$x\to\infty$,$0<\alpha<2$。

最简单的重尾分布是Pareto(佩瑞多)分布,其概率密度:

$$p(x)=\alpha k^{\alpha}x^{-\alpha-1},\alpha,k>0,x\geq k$$

分布函数为:

$$F(x)=P[X\leq x]=1-(k/x)_{\alpha}$$

当α减小,大量的概率质量集中在分布的尾部。

多个重尾的On/Off源叠加可产生自相似的业务流[4]。

DDoS攻击利用分布在不同地点的大量计算机,采用协作的方式,同时向被攻击目标发送大大超过其处理能力的数据包,其目的或是堵塞目标网络的出口,导致带宽消耗,或是消耗目标系统的如CPU,内存等关键资源,使被攻击目标不能提供正常服务,甚至瘫痪。

通常分布式拒绝服务攻击的步骤如下:

(1)探测扫描大量主机以寻找可入侵的傀儡机;

(2)入侵有安全漏洞的主机并获取控制权,作为DDoS攻击的傀儡机;

(3)选取一台傀儡机,在其中安装DDoS攻击控制程序,作为控制傀儡机;

(4)在其它傀儡机上,安装攻击程序;

(5)攻击者通过控制傀儡机,同时向攻击傀儡机发布攻击命令;

收稿日期:2010-06-03
作者简介:周刚(1967-),男,江苏盐城市人,讲师,硕士,软件设计师,主要研究方向为网络与信息安全。

(6)攻击傀儡机同时向目标系统发送洪水般的数据，造成目标系统拒绝服务。

DDoS攻击者通常使用伪造源IP地址向目标系统发送攻击包，使得从目标系统追踪攻击源变得很困难，目标系统也很难简单地过滤这类攻击包，因为它们与合法的数据包并没有什么显著区别。

2　NS2模拟方法

NS2由加利福尼亚大学伯克利分校和VINT项目组联合开发，是一种开放源码的多协议网络模拟软件。

NS2采用两级体系结构将数据操作与控制部分的实现相分离，事件调度器和大部分基本的网络组件对象后台使用C++实现和编译，NS2的前端是一个Otcl解释器，主要功能是配置、建立模拟环境。

NS2模拟过程如下：

添加NS2的新组件，TclCL机制的实现及新组件的C++实现→TCL脚本的编写，实现对模拟场景的产生和控制→运行TCL脚本，生成nam和trace文件→运行nam文件，查看模拟运行过程→对trace文件分析，得到相关数据结果→利用gnuplot等画图软件将数据结果直观地展示出来。

3　网络模拟拓扑

图1为模拟拓扑图。图中有一个路由节点R和一个接收节点D，发送节点共有$M+N+1$个，其中$1-M$个节点与节点D建立UDP连接，$1-N$个节点与节点D建立TCP连接，这$M+N$个节点模拟网络的正常背景流，发送TCP和UDP数据包，共发送1 000 s。节点A为攻击节点，在第300 s开始向节点D发送DDoS攻击数据包，到600 s结束，发起攻击共300 s。链路共有$M+N+2$条，链路带宽设定为1 Mb/s，延迟10 ms，使用DropTail被动队列管理机制；拓扑中其余参数默认。

4　正常业务背景流模拟

4.1　POO流量发生器

NS2提供的POO流量发生器Applicati－on/Traffic/Pareto类根据Pareto On/Off分布产生数据，在ON状态，以连续速率发送数据包；在OFF状态，不发送数据包。因此多个POO源叠加可产生自相似特性的业务流。

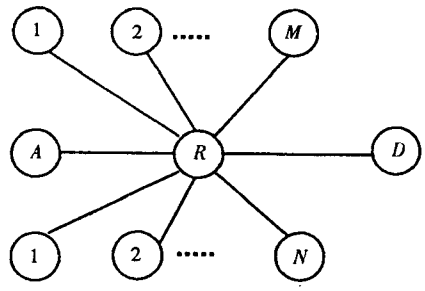

图1　模拟拓扑图

Fig. 1　Toplogical diagram of simulation

4.2　TCP业务流的模拟

TCP发送代理使用Agent/TCP，它采用了拥塞控制机制和环路时间估算：慢启动时，每收到一个新的ACK，冲突窗口就增加一个信息包；冲突避免时，每收到一个新的ACK，冲突窗口就增加1/cwcn_。设置窗口长50，TCP MSS值为200，接收代理使用Age——nt/TCPSink。

由于在NS2中，不管应用层是流量发生器还是应用模拟器，实际可用的包的传输仍然由TCP流和拥塞控制算法来控制。因此，根据“4.1”的结论，为生成基于自相似性的TCP背景流量，在应用层我们采用NS2提供的POO流量发生器：

```
for {set i 0} {$i < $N} {incr i} {
.....
#建立N个TCP代理并把它们和N个发送节点相连
set ntcpagent($i) [new Agent/TCP]
$ns attach－agent $nodetcp($i) $ntcpagent($i)
#建立N个POO流量发生器并配置其参数
set ntcptraffic($i) [new Application/Traffic/Pareto]
$ntcptraffic($i) set packetSize_ 210
$ntcptraffic($i) set burst_time_ 50 ms
$ntcptraffic($i) set idle_time_ 50 ms
$ntcptraffic($i) set rate_ 10k
$ntcptraffic($i) set shape_ 1.3
#连接应用与代理
$ntcptraffic($i) attach－agent $ntcpagent($i)
#建立TCP接收代理并与接收节点nodereceive相连
```

```
set ntcpsink( $i) [new Agent/TCPSink]
$ns attach - agent $nodereceive $ntcpsink ($i)
$ns connect $ntcpagent ($i) ntcpsink ($i);#建立 TCP 连接
……}
```

4.3 UDP 业务流的模拟

图 1 中,1—M 个节点发送 UDP 数据包。其应用层也采用 POO 流量发生器,POO 流量发生器参数设置同"4.2":

```
for {set j 0} {$j < $M} {incr j} {
……
set nudpagent( $j) [new Agent/UDP];#建立发送代理
#连接代理与发送节点
$ns attach - agent $nodeudp( $j) $nudpagent( $j)
#建立 M 个 POO 流量发生器并配置其参数
set nudptraffic( $j) [new Application/Traffic/Pareto]
……
#连接应用与代理
$ nudptraffic ( $j) attach - agent $nudpagent( $j)
#建立 UDP 接收代理并与接收节点 nodereceive 相连
set nudpsink( $j) [new Agent/LossMonitor]
$ns attach - agent $nodereceive $nudpsink ($j)
$ns connect $nudpagent ($j) nudpsink ($j);#建立 UDP 连接
……}
```

5 DDoS 攻击流模拟

图 1 中的节点 A 作为攻击节点,发送 DDoS 攻击流。根据 DDoS 攻击的特点,DDoS 攻击流的模拟只要在拓扑中放置大量的常数比特率数据源(Constant Bit rate,CBR),并且让这些 CBR 在较短的时间内同时发送即可。节点 A 与节点 D 建立的是 UDP 连接。CBR 流参数设置如下:

```
set cbrddostraffic [new Application/Traffic/CBR]
$cbrddostraffic set packetSize_ 200
$cbrddostraffic set rate_ 500kb; #代表 DDoS 流量为 500 kb/s。
$cbrddostraffic set random_ 1
```

6 实验结果及分析

对模拟得到的仿真流,间隔 0.01 s 采样。用小波法[5]估计其 Hurst 参数。模拟时先不发动 DDoS 攻击,这样图 1 的拓扑得到的就是没有 DDoS 攻击的正常的业务流,结果如表 1 所示。

表 1 正常业务流 Hurst 估计值

Table 1 The Hurst estimates of normal traffic

实验	M	N	应用层	平均流量 Mb/s	H 估计值
1	50	0	Pareto	0.390	0.896
2	0	10	Pareto	0.391	0.862
3	2	10	Pareto	0.407	0.833
4	0	10	FTP	0.861	-0.810
5	0	10	Telnet	0.195	0.498

由于在 NS2 中,对 TCP 协议连接的应用层习惯采用 FTP 和 Telnet 应用模拟器,所以我们同时在 TCP 协议中估计了 FTP 和 Telnet 应用模拟器产生的网络正常流的 H 值(表 1 中实验 4,5 所示)。

由实验 4,5 的 H 估计值可知,应用层使用 FTP 或 Telnet 应用模拟器,得到的正常网络模拟业务流都不具有自相似性。因此,在利用网络流量特征分析 DDoS 攻击的网络行为时,使用应用模拟器产生的正常业务流不适合作为 DDoS 攻击的背景流。实验 1,2 的 H 估计值表明:应用层使用 POO 流量发生器时,当网络中仅含有 UDP 协议或 TCP 协议时,模拟业务流都保持了自相似性。

根据 MCI 的统计,互联网上总字节数的 95% 及总数据包数的 90% 均使用 TCP 协议传输[6],在实验 3 中我们 M 仅取 2,N 取 10 以减小模拟中 UDP 流量的份额,增大 TCP 流量份额。由表 1 的结果可知在模拟网络中同时存在 TCP 协议和 UDP 协议时,网络依然保持着自相似性。

然后,我们在实验 3 中加入 DDoS 攻击,在第 300 s 开始发送 DDoS 数据包,600 s 结束,发送速率为 500 kb/s,表示中等强度的 DDoS 流对中等负荷的网络发生了攻击。对模拟得到的 DDoS 入侵流估计其 H 值,样本点的数量取 2 500,每隔 5 s 估计 1 次 H 值。图 2 列出了其 1 - 1 000 s 的采样时间为 1 s 的放大的时间 - 流量图,可以看到流

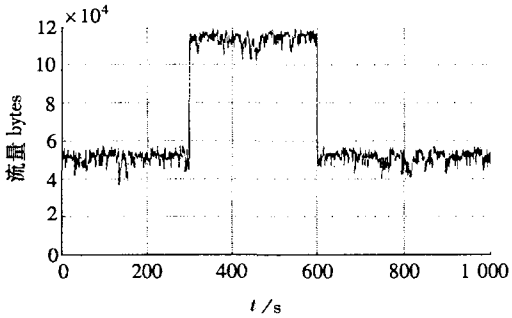

图2　1－1 000 s时间流量图

Fig. 2　Time－flow diagram within 1－1000 seconds

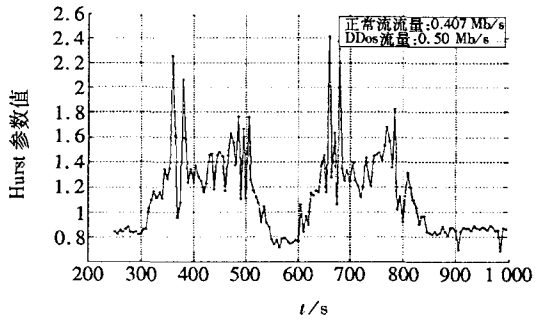

图3　1－1 000 s时间－Hurst参数图

Fig. 3　Time－Hurst diagram within 1－1000 seconds

量在300 s到600 s时间段内有一个平移,显示这段时间发生了DDoS攻击。

图3显示了DDoS攻击的时间－Hurst参数值间的关系,可以看到从第305 s开始,H估计值逐步增大,表示DDoS发生了攻击,而在第315 s开始,H估计值已达到1.028 5,根据文献[3],若取阈值为0.95,可在第315 s处检测到DDoS攻击。

7　结语

目前,对于TCP协议连接的应用层习惯采用FTP和Telnet应用模拟器,但这种方法模拟得到的网络流量不具有自相似性,不适合作为对DDoS入侵流的流量特征分析的背景流。由此,本文利用多个重尾的On/Off源叠加可产生自相似业务流这一机理,使用NS2提供的POO流量发生器,提出一个结合TCP,UDP协议的DDoS攻击的网络模拟方法,使用该法模拟产生的模拟背景流保持了真实的网络业务流自相似性特征,更接近真实网络环境;而模拟得到DDoS入侵流可应用于流量特征分析等方面的研究。

参考文献:

[1] Leland WE, Taqqu MS, Willinger W, et al. On the self－similar nature of ethernet traffic (extended version)[J]. IEEE/ACM Transactions on Networking. 1994,2(1):1－15.

[2] 任勋益,王汝传,王海艳. 基于自相似检测DDoS攻击的小波分析方法[J]. 通信学报,2006,27(5):6－11.

[3] 周刚,刘渊,陈晓光. 基于小波的DDoS入侵流分析[J]. 计算机工程,2008(15):156－158.

[4] Crovella M, Lipsky L. Long－Lasting Transient Conditions in Simulations with Heavy－Tailed Workloads[C]. In Proceedings of the 1997 Winter Simulation Conference, Atlanta, Georgia, 1997.

[5] Veitch D, Abry P. A wavelet based joint estimator for the parameters of LRD[J]. IEEE Transactions on Information Theory, 1999, 45(3):878－897.

[6] Thompson K, Miller G J, Wilder R. Wide－area Internet traffic patterns and characteristics[J]. IEEE Network, 1997, 11(6):10－23.

The Simulation of DDoS Traffic Based on NS2

ZHOU Gang, MENG Hai-tao

(School of Information Engineering, Yancheng Institute of Technology, Jiangsu Yancheng　224051, China)

Abstract: According to the formation mechanism of network self－similarity and characteristic of DDoS attack traffic, a new NS2－based DDoS traffic simulation method synthesizing TCP Protocol and UDP Protocol is presented. The experimental results show the the background traffic flow obtained by this method maintains the self－similarty characteristic of real traffic, so the simulated flow can be applied to the research on DDoS traffic characteristic.

Keywords: intrusion detection; distributed denial of service; Network Simulator version 2; self－similarity

(责任编辑:沈建新;校对:张英健)