文章编号：2095-2163(2020)02-0263-05 中图分类号：TP393.08 文献标志码：A

一种针对 BGP 会话的低速率分布式拒绝服务攻击模拟研究

张源良，张 宇
（哈尔滨工业大学 计算机科学与技术学院，哈尔滨 150001）

摘 要：低速率分布式拒绝服务攻击是一种较难检测和实施的攻击方法，根据其周期性发送大量攻击流量的特性，本文研究其攻击 BGP 会话的可行性和各类攻击参数。由于很难在真实 BGP 路由进行攻击实验，本文采用模拟网络的方法对攻击进行模拟。首先说明虚拟网络中僵尸机调度方案和带宽限制方法，接着在攻击前评测各类攻击参数，最后确定参数后进行模拟攻击，给出模拟攻击的结果。模拟结果表明在限制网络带宽的情况下，在一定时间内设定好合适的攻击参数，以及低速率分布式拒绝服务攻击的周期，可以达到打断 BGP 会话的攻击效果。

关键词：边界网关协议；低速率分布式拒绝服务攻击；模拟攻击

A simulation study of low-rate distributed denial of service attack against BGP sessions

ZHANG Yuanliang, ZHANG Yu
(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

【Abstract】 The low-rate distributed denial of service attack is a difficult method to detect and implement. According to the characteristics of periodically sending a large amount of attack traffic, this paper studies the feasibility of attacking BGP sessions and various attack parameters. Because it is difficult to conduct attack experiments on real BGP routes, this paper simulates the attacks by simulating the network. Firstly, the zombie scheduling scheme and bandwidth limitation method in the virtual network are explained. Then, various attack parameters are tested before the attack, the parameters are determined. Finally, simulated attacks are made, and the results of the simulated attacks are given. The simulation results show that in the case of limiting the network bandwidth, setting the appropriate attack parameters and the period of the low-rate distributed denial of service attack within a certain period of time can achieve the attack effect of interrupting the BGP session.

【Key words】 BGP; low-rate DDos; simulated attack

0 引 言

BGP 是目前互联网实际使用的标准域间路由协议，可将为数众多、拓扑各异、大小不一的自治域连接在一起并相互交换路由信息。BGP 使用 TCP 作为路由交换的底层传输协议，通常工作在互联网提供商(ISP)搭建的大型 BGP 路由之间，在自治域之间建立 BGP 会话，使得自治域之间可达。

在互联网中针对不同的网络有各种不同的攻击手段，其中拒绝服务(DoS)攻击是一种常见的网络攻击手段，攻击者利用可达到受害者的机器对受害者发送大量流量使得受害者的正常工作受阻，达到攻击的目标。其中，受害者可以是网络服务器、网络链接或路由器、ISP 等等。几乎所有互联网服务都容易受到拒绝服务攻击。攻击者往往会感染足够多的终端主机，使很多终端主机变为可控制的僵尸机，利用足够多的散布整个网络的僵尸机对受害者进行拒绝服务攻击，这种攻击方法被称为分布式拒绝服务(DDos)攻击。

拒绝服务攻击的种类有很多，包括利用软件漏洞的 Ping of death 和 Teardrop、耗尽应用资源的 Fork bomb、耗尽操作系统资源的 TCP SYN flood、LAND 攻击、HTTP SlowPOST、BlackNurse 等[1]。本文要讨论的是低速率分布式拒绝服务(Low-rate DDos)攻击。与普通的 DDos 攻击最大的区别是，Low-rate DDos 攻击不会长时间地发送攻击流量，而是周期性地发送短暂的攻击流量，在 2 个攻击周期之间不发送任何攻击流量。这样的特性使得 Low-rate DDos 在统计流量特征中与普通用户的流量区别不明显，较难检测[2]。

Low-rate DDos 在实施上也比 DDos 复杂很多，需要针对攻击的受害者服务特性进行分析，选择合适的攻击周期，达到设定的攻击效果。本文研究的

基金项目：国家重点研发计划(2016YFB0801303)。

作者简介：张源良(1995-)，男，硕士研究生，主要研究方向：BGP、网络拓扑测量；张 宇(1979-)，男，博士，副教授，主要研究方向：网络测量、网络安全、未来网络。

收稿日期：2019-06-06

是针对 BGP 会话的 Low-rate DDos。

1 针对 BGP 会话的低速率分布式拒绝服务攻击原理

根据低速率分布式拒绝服务攻击周期性发送汇聚攻击流量的特性以及 BGP 会话周期性发送保活包的特性,自然地可以想到如何针对 BGP 会话进行低速率分布式拒绝服务攻击,其原理包括 3 个部分,对此可分述如下。

(1)2 个自治域在建立 BGP 会话后,会周期性(holdtime 时间通常为 120 s)地发送 Keepalive 包。

(2)如果 BGP 路由在会话过程中对于一个路由器的连续 3 个 Keepalive 包都没有收到,BGP 路由会认为会话已经失效,会发送 Notification 包,表示会话断开,并且向周围的 BGP 路由发送 Update 包,更新自治域的互连情况。

(3)使用 Low-rate DDos 攻击在攻击 BGP 会话时,在攻击峰值周期时有概率拥塞 BGP 路由器的接受队列,使得其他 BGP 路由发送的 Keepalive 包被丢弃。

综合以上原理,理论上,使用 Low-rate DDos 攻击对 BGP 会话的 Keepalive 包进行阻塞即可打断 BGP 会话,进而使 2 个自治域之间的通信受到影响。在应用中实施此攻击时还需要考虑组织 DDos 攻击流量的方法和攻击参数的确定。

2 模拟攻击研究

由于 BGP 路由往往是 ISP 间用于自治域互连的大型路由器,如果在其上进行 Low-rate DDos 攻击,会使得正常的自治域通信出现问题,因此本文在虚拟的网络环境中对攻击进行模拟,验证其攻击效果。

2.1 虚拟的网络环境

本文使用的虚拟网络环境,包括若干完全可控的僵尸主机 Bot 和若干建立 BGP 会话互连的 BGP 路由。整个网络由若干个自治域构成,每个自治域包括若干僵尸主机 Bot 和 BGP 路由 Router,自治域之间通过 BGO 路由互连,使得整个网络互通。

2.2 僵尸机调度的方法

僵尸机调度方法如图 1 所示,欲攻击的 BGP 连接为 Target Link,发送攻击流量 $f_1, f_2, \cdots, f_n$ 的僵尸机为 $Bot_1, Bot_2, \cdots, Bot_n$。给僵尸机下达攻击命令的控制机为 Controller C。

调度僵尸机攻击过程可阐释论述如下。

(1)选取控制机。控制机应该满足每个僵尸机都有到达控制机 C 的路径,而且每条路径都经过被攻击连接 Target Link,经过 Target Link 后通过同样的路径 Route 2,…,Route Z 到达控制机。这是最优的控制机选取,因为攻击机从被攻击链路到达控制机的路径相同,时钟同步时只需考虑攻击机到被攻击链路的网络延迟。

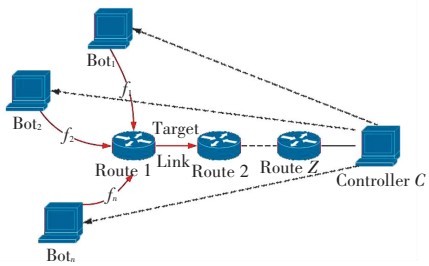

图 1 僵尸机调度方法

Fig. 1 Zombie scheduling method

(2)时钟同步。为了保证僵尸机的攻击流量同时到达被攻击链路,需要进行时钟同步。控制机对每台僵尸机发送时钟同步请求,僵尸机返回其当前时间 Ts_i,控制机收到 Ts 时根据本机当前时间 Tr_i 计算时间差,计算公式表示为:

$$D_i = Tr_i - Ts_i, \tag{1}$$

将 D_i 发送给僵尸机,每个僵尸机实际的开始时间 $bot\_start\_time_i = strat\_time - D_i$,其中 $start\_time$ 为控制机发送的开始攻击时间。

(3)环境参数的设定。对于 BGP 连接之间的 BGP 协议的 keepalive 发送间隔、holdtime 时间和 reconnect 时间等参数,以及被攻击链路带宽大小,在攻击前可通过读取配置文件中设定参数来求得。

(4)攻击参数的设定。攻击前从配置文件中读取开始时间、攻击流量、持续时间等参数,以此对僵尸机下达攻击指令。其中,产生攻击流量的方法为组装 UDP 包。以 14 字节以太网头,20 字节 IP 包头,8 字节 UDP 包头,32 字节数据组装 UDP 包。使用数据报套接字发包。指定接收方 IP 地址和端口,开启多个线程,用 SOCK_DGRM 类型套接字发送 UDP 包。

在此基础上,还需设定发包速率大小。设定预期发送流量大小为 $flow$,可以计算出发包速率为:

$$rate = (flow * 1\,024 * 1\,024)/(8 * (42 + length)). \tag{2}$$

每个线程中循环发包,设定全局变量记录发包数量,每发送一百个包判断当前速率是否达到设定值 $rate$,若达到,此次循环不发送包;未达到,则继续发包。

(5)攻击结果的分析。攻击的同时使用 tcpdump 抓包,待攻击结束后将抓包结果进行分析,将结果存为日志文件。

2.3　带宽限制

考虑到普通的 BGP 链路带宽为百兆或千兆带宽，僵尸机汇聚的攻击流量很难达到阻塞 BGP 链路的目的，所以在模拟实验中对 BGP 带宽链路进行限制。

本文的虚拟网络带宽限制采用 Linux 内核 Traffic Control 中的令牌桶算法。其原理如图 2 所示，主要有以下要点：

(1)每过 $1/r$ s，桶中增加一个令牌。

(2)桶中最多存放 b 个令牌，如果桶满了，新放入的令牌会被丢弃。

(3)当一个 n 字节的数据包到达时，消耗 n 个令牌，然后发送该数据包。

(4)如果桶中可用令牌小于 n，则该数据包将被缓存。

(5)缓存区满后，后续的包会被丢弃。

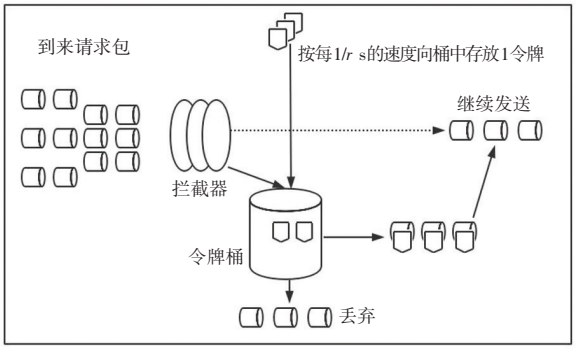

图 2　令牌桶算法

Fig. 2　Token bucket algorithm

本文在令牌桶算法的实际实施中采用集成 tc 的 tcconfig 模块，例如控制端口 eth1 带宽为 1Mb/s 的命令为 tcset --device eth1 --rate 1 024 K，等价于表 1 中的 Linux 流量控制命令。首先在端口 eth1 上建立 htb 令牌桶，接着设置令牌速率 *rate*，单位存储 cile 为 1 024 Kbit，缓冲区 burst 和子缓冲区 cburst 为 12.8 KB，最后设置进出口列表为 0.0.0.0/0，表示规则对所有 IP 地址有效。

表 1　流量控制方法

Tab. 1　Flow control method

Linux 流量控制方法
1. tc qdisc add dev eth1 root handle 16f1: htb default 1
2. tc class add dev eth1 parent 16f1: classid 16f1:2 htb rate 1 024.0 Kbit ceil 1 024.0 Kbit burst 12.8 KB cburst 12.8 KB
3. tc filter add dev eth1 protocol ip parent 16f1: prio 2 u32 match ip dst 0.0.0.0/0 match ip src 0.0.0.0/0 flowid 16f1:2

2.4　间隔发送流量

根据 Low-rate DDos 攻击的原理，模拟攻击对 BGP 会话采用如图 3 所示的间隔发送流量的方式。BGP 会话在建立连接后会周期性地发送 Keepalive 包，发送流量的方法即在 Keepalive 包发送的前后覆盖一段时间进行流量发送。因为模拟攻击时为理想情况，如此一来就可以在 BGP 路由的端口进行抓包，确定 Keepalive 包的发送具体时间，根据该时间和 holdtime 参数设定确定持续发送流量发起的时间和间隔需要的时间。

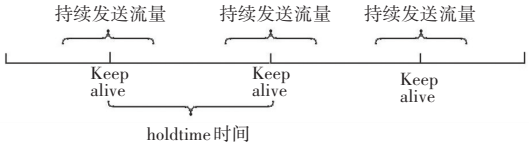

图 3　间隔发送流量

Fig. 3　Interval send traffic

3　发送流量参数确定及模拟攻击结果

在确定虚拟网络以及攻击方法后需要对每个僵尸机开启多少攻击线程，采用多少僵尸机，在哪个攻击范围内有打断 BGP 连接的可能等参数进行确定，然后使用确定后的攻击参数进行模拟攻击，分析模拟攻击结果。

3.1　僵尸机发送流量

分别设定发送 30 Mb/s、50 Mb/s、80 Mb/s、100 Mb/s 的流量，用 ifstat 在接收端口流量日志文件，流量发送控制是否精确。研究结果表明，4 种设定攻击流量时的接收端流量确切值与预期偏差不超过 1 Mb/s，达到了流量设定控制预期效果。特别地，跨路由发送流量的情况下与直接相连路由发送流量结果相同。

3.2　僵尸机发送流量参数确定

在调度僵尸机发送汇聚流量前，需要确定发送流量参数。首先确定单个僵尸机的攻击流量参数，然后确定同主机多个僵尸机攻击流量汇聚的参数，最后改变汇聚攻击流量和带宽限制确定有可能攻击成功的参数。

(1)单个僵尸机发送流量瓶颈。从 1~8 增加线程数量(高于 8 个线程内存占用过多)，每个线程永真循环发包，与使用 ifstat 写日志记录不同线程数下最大发包值，线程从 1~8 时的最大入口流量如图 4 所示。由图 4 中可以看到单个虚拟僵尸机发送最大流量所需的线程数为 4。

(2)多个僵尸机汇聚流量。通过多个连接相同 BGP 路由的僵尸主机，汇聚流量发送到与连接的 BGP 路由直连的 BGP 路由器，变化僵尸主机的数

量,记录汇聚攻击流量的大小。

多僵尸机汇聚流量的情况如图 5 所示,改变僵尸机数量,得到不同的僵尸机汇总流量大小,每个结果均为多次测试得到,仿真结果表明 4 台僵尸机时候达到瓶颈汇聚流量。

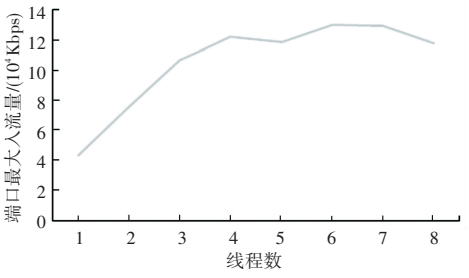

图 4 不同线程数发送流量

Fig. 4 Send traffic with different threads

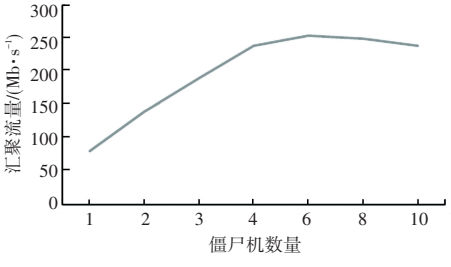

图 5 多僵尸机汇聚流量

Fig. 5 Multiple zombie aggregation traffic

3.3 间隔发送流量结果

以之前步骤测得的每个僵尸主机开启 4 个线程,使用 4 个僵尸主机的实验拓扑,链路带宽从 10 Mb/s到 100 Mb/s 进行变化,攻击流量从 40 Mb/s 变化到之前测试的瓶颈汇聚流量 260 Mb/s,进行攻击测试。每个参数进行 10 次实验,每次实验时设定最大攻击时间为 2 h,2 h 内若 BGP 连接断开则计数加 1,进行下一次实验,超过 2 h 则直接进行下一次实验。

带宽为 10 Mb/s、20 Mb/s、40 Mb/s 和 60 Mb/s 时的流量范围实验结果见表 2,带宽大于 60 Mb/s 时与 60 Mb/s 的实验结果相同。故只有 10 Mb/s、20 Mb/s和 40 Mb/s 有被打断的可能。

表 2 发送流量范围实验结果

Tab. 2 Send traffic range experiment results %

带宽	攻击流量							
	40	60	80	100	140	180	220	260
10	0	0	30	30	30	50	50	40
20	0	0	20	0	20	10	30	20
40	0	0	0	0	10	20	10	20
60	0	0	0	0	0	0	0	0

得到指导实验参数范围后,在能够打断 BGP 连接的参数范围内进行实验,每组参数进行 10 次攻击实验,每次实验攻击中记录 BGP 数据包,直到 BGP 连接断开为止,记录 BGP 连接断开所需的时间。实验结果记录如图 6 所示。该结果说明测试得能打断的 BGP 链路带宽为 10 Mb/s、20 Mb/s、40 Mb/s。其中,10 Mb/s 时可以用 100 Mb/s 攻击流量打断,其他带宽只能用大于 140 Mb/s 的攻击流量。大部分成功攻击参数下可以在 120 s 内打断 BGP 连接。

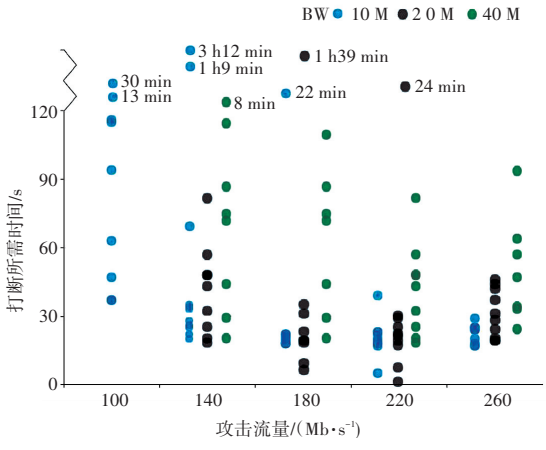

图 6 不同参数打断所需时间

Fig. 6 Time required to interrupt different parameters

4 结束语

本文研究了针对 BGP 会话的低速率分布式拒绝服务攻击,按照低速率分布式拒绝服务攻击周期性攻击的特性,对 BGP 会话的周期性 Keepalive 包进行周期性阻断,达到攻击 BGP 会话的目的,并对此攻击进行模拟。模拟结果说明在对网络进行相应带宽限制的情况下,按照一定攻击流量和频率,低速率分布式拒绝服务攻击可以打断 BGP 会话。

参考文献

[1] 何炎祥, 刘陶, 曹强, 等. 低速率拒绝服务攻击研究综述[J]. 计算机科学与探索, 2008, 2(1):1.

[2] 文坤, 杨家海, 张宾. 低速率拒绝服务攻击研究与进展综述[J]. 软件学报, 2014, 25(3):591.

[3] SCHUCHARD M, MOHAISEN A, KUNE D F, et al. Losing control of the Internet: Using the data plane to attack the control plane[C]// Proceedings of the Network and Distributed System Security Symposium, NDSS 2011. San Diego, California, USA: ACM, 2011:1.

[4] ZHANG Ying, MAO Zhuoqing, WANG Jia. Low-rate tcp-targeted dos attack disrupts Internet routing[C]// Proceedings of the Network and Distributed System Security Symposium, NDSS 2007. San Diego, California, USA:dblp,2007:1.

[5] KUZMANOVIC A , KNIGHTLY E W . Low-rate TCP-targeted denial of service attacks and counter strategies[J]. IEEE/ACM Transactions on Networking, 2006,14(4):683.

(下转第 271 页)