文章编号：2095-2163(2020)08-0097-04 中图分类号：TP393.0 文献标志码：A

基于 IPv6 的模拟集成 DDoS 攻击平台的设计与实现

周芃玮[1]，谭振江[1]，周 伟[1]，方大甲[2]
（1 吉林师范大学 计算机学院，吉林 四平 136000；2 吉林师范大学 附属小学，吉林 四平 136000）

摘 要：随着互联网的发展，IP 地址的需求越来越多，IPv4 地址资源即将耗尽。为了应对这种情况，IPv6 开始普及。由 IPv4 向 IPv6 过渡，不可忽视的就是网络安全，而 DDoS 作为一种易于操作且攻击性强的网络攻击，对 IPv6 网络的危害性不可忽视。网络攻击技术也到了很大的提升，为了应对未来可能发生的电子对抗战，更需要对网络攻击进行研究。本文对 IPv6 下的 DDoS 攻击进行研究，设计基于 IPv6 的模拟集成 DDoS 攻击平台。本文首先分析了 IPv6 的特点（包括 IPv6 的现状及先进性）及 DDoS 的特点（包括 DDoS 的分类、现象和原理），研究 IPv6 面临的 DDoS 威胁，基于树状结构的动态分布式网络模型和插件技术，设计与实现基于 IPv6 的模拟集成 DDoS 攻击平台。

关键词：IPv6；DDoS；网络安全

Design and implementation of simulated integrated DDoS attack platform based on IPv6

ZHOU Pengwei[1], TAN Zhenjiang[1], ZHOU Wei[1], FANG Dajia[2]
(1 Computer College, Jilin Normal University, Siping 136000, Jilin, China;
2 ComputerCollege, Jilin Normal University, Siping 136000, Jilin, China)

【Abstract】 With the development of Internet, the demand of IP is growing, and IPv4 is running out. To deal with this situation, IPv6 began to spread. Transition from IPv4 to IPv6 is a problem that can not be ignored is network security. As an easy to operate and highly aggressive network attack, DDoS is harmful to IPv6 network. At the same time, network attack technology has also been greatly improved.In order to deal with the possible cyber war in the future, we need to study the network attack. Therefore, this paper studies DDoS attacks under IPv6 and designs a simulated integrated DDoS attack platform based on IPv6.This paper first analyzes the characteristics of IPv6, including the status and advancement of IPv6, and the characteristics of DDoS, including the classification, phenomenon and principle of DDoS. Later the DDoS threat of IPv6 is studied. Based on the tree structure of dynamic distributed network model and plug-in technology, this paper designs and implements a simulation integrated DDoS attack platform based on IPv6.

【Key words】 IPv6; DDoS; network security

0 引 言

随着互联网的快速发展，网络已经成为人们日常生活中不可或缺的一部分。网上购物、休闲娱乐、办公作业都离不开互联网，网络安全的重要性越发凸显出来。可联网设备也从最初只有的电脑发展为手机、手表、耳机等等，越来越多的设备开始连入互联网，导致 IPv4 的地址资源已经不能满足这些需求。

因此出现了 IPv6。IPv6 基于 IPv4 对其进行了很大的改进，成为未来即将普遍使用的 IP 地址。

互联网的发展同时也使网络攻击技术得到了很大的提升。近年来，网络攻击事件频繁发生，网络安全已经成为一个不可忽视的问题。但是网络攻击是把“双刃剑”，自然也有有利的那一面，如：对于一些钓鱼网站、病毒网站、欺诈网站、外国宣传色情和暴力网站，甚至反动的一些网站采取网络攻击使网站瘫痪，可以净化网络环境。由此可见，研究网络攻击的重要性不言而喻。而 DDoS 作为一种易于操作且攻击性强的网络攻击方法，对网络的危害性不可忽视，但是如果可以利用 DDoS 作为工具，将成为净化

基金项目：教育部科技司赛尔网络下一代互联网技术创新项目（NGII20180408）；吉林省教育厅项目（JJKH20200441SK）；吉林省高等教育教学改革研究课题（JLJJ719920190723194557、吉林省高等学校计算机应用人才培养模式创新实验区的研究与实践）、吉林省职业教育教学改革研究课题（2017ZCZ045）；吉林师范大学教学成果培育项目（“三基一新”型计算机专业人才培养模式研究与实践）；吉林师范大学大学生科研基金项目；吉林师范大学研究生科研创新项目（研创新 201634）.

作者简介：周芃玮（1999-），女，本科生，主要研究方向：计算机网络；谭振江（1965-），男，博士，教授，博士生导师，主要研究方向：计算机网络、智能信息技术；周 伟（1979-），女，硕士，助理研究员，主要研究方向：信息资源管理、计算机应用。

通讯作者：周 伟 Email：867458539@qq.com

收稿日期：2020-06-15

网络的一把利刃。不论是防范 DDoS 攻击还是利用 DDoS 攻击,都有必要去研究它。因此,本文研究设计基于 IPv6 的模拟集成 DDoS 攻击平台,以应对未来可能面临的问题。

1 IPv6 技术基础

1.1 IPv6 发展现状

国家为了支持国内的 IPv6 网络建设,在 2004 年 12 月开通了 CERNET2,是目前世界上运行的最大的纯 IPv6 网络,连接着国内几十个城市的上百个节点[1]。截止 2019 年 6 月 IPv6 活跃用户数到达 1.3 亿,全国已有 12.07 亿用户获得 IPv6 地址[2]。但是 IPv6 的使用量很低,大部分依然使用原有的 IPv4 地址。

日本的主要运营商和 ISP 基本上已经提供 IPv6 商业化接入服务;韩国在 IPv6 的战略、政策、立法、项目资助、国际合作等方面已经采取相应措施;美国各主要厂商已经或者准备推出支持 IPv6 的试验性产品;欧洲目前已经建立了 IPv6 试验网络进行有关推广、部署 IPv6 的准备工作[3]。但是全球的 IPv6 使用率依然普遍较低。

1.2 IPv6 相较 IPv4 的先进性

IPv6 相较于 IPv4 的先进性见表 1。

表 1 IPv6 与 IPv4 的比较

Tab. 1 IPv6 versus IPv4

地址类型	地址长度	路由表	对自动配置的支持	对服务质量的支持	安全性
IPv4	32 位	较大	不支持	不支持	较低
IPv6	128 位	较小	支持	支持	较高

相比于 IPv4,IPv6 有更大的地址空间,IPv6 的地址长度为 128 位,而 IPv4 的地址长度为 32 位,大大增加了地址数量;IPv6 报头简洁,易于扩展,降低了数据处理过程的延迟;IPv6 增加了对自动配置的支持,提高了数据传送效率;IPv6 增加了对服务质量的支持;IPv6 的保密性、完整性比 IPv4 更高[4-5]。

2 DDoS 研究

2.1 DDoS 的分类

DDoS 即分布式拒绝服务攻击。是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击,或者一个攻击者通过控制位于不同位置的多台机器同时向目标发动攻击[6]。

DDoS 以从 5 个方面分类:自动化程度、攻击的弱点、攻击速率、攻击目标、攻击路线。

自动化程度分为手动 DDoS 攻击、半自动化 DDoS 攻击、自动化 DDoS 攻击。手动 DDoS 攻击即编程和发动全是手动完成;半自动化 DDoS 攻击大部分具有 handler 控制攻击用的 agent 程序,通过在 agent 程序植入自动化的入侵工具,利用 handler 控制所有 agents 程序对目标发动 DDoS 攻击[7];自动化 DDoS 攻击则是将攻击目标、攻击方式以及持续时间都写入程序,散布程序之后可以自动攻击。

从攻击的弱点分类分为洪水攻击、扩大攻击、利用协议的攻击、畸形数据包攻击。洪水攻击是攻击者向目标系统发送大量的数据流,影响目标系统的服务或致其瘫痪;扩大攻击是利用广播 IP 地址或者反射体影响目标系统的服务或致其瘫痪;利用协议的攻击是利用 IP 地址中某些协议的漏洞,大量消耗目标系统的资源;畸形数据包攻击是通过向目标系统发送错误的 IP 地址数据包,致使目标系统崩溃[8]。

从攻击速率分类分为持续速率攻击和可变速率攻击。持续速率攻击是攻击速率一直恒定,不发生改变;可变速率攻击是攻击时,攻击速率发生改变。

从攻击目标分类分为带宽攻击和连通性攻击。带宽攻击的攻击方向是带宽,通过向目标系统发送大量的数据包占用目标系统的带宽,从而使目标系统无法服务;连通性攻击则是利用发送大量的请求,导致目标系统回应时产生瘫痪。

从攻击路线分类分为直接攻击和反复式攻击。直接攻击是不通过反射体直接攻击;反复式攻击则是将很多主机作为反射体从而发动攻击。

2.2 DDoS 攻击时产生的的现象

(1)被攻击主机上存在大量等待的 TCP 连接;

(2)网络中存在大量无用的且源地址为假的数据包;

(3)存在高流量无用数据,引起网络拥塞,使受害主机无法正常和外界通讯;

(4)短时间内连续频繁的收到特定的服务请求,使受害主机无法及时处理所有正常请求;

(5)严重时系统死机。

2.3 DDoS 的原理

DDoS 攻击体系由攻击者、受控服务器、攻击代理和攻击目标共 4 部分组成,如图 1 所示。攻击者操控攻击,受控服务器的每一台服务器都是被入侵并设置了预定程序的主机,其不参与攻击,只向攻击

代理发布命令，攻击代理收到受控服务器的命令后发出 DDoS 的攻击包。攻击者可以控制主控端和代理端，使其在攻击时利用手段隐藏攻击者不被发现。攻击者发送攻击指令后就可以离开网络，从而逃避追踪[9]。

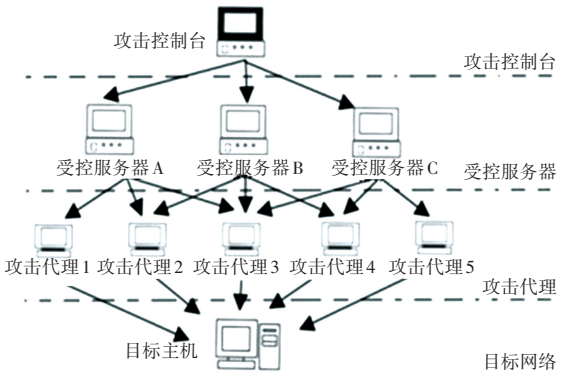

图 1　DDoS 入侵示意图

Fig. 1　Schematic diagram of DDoS invasion

3　IPv6 面临的 DDoS 威胁

（1）反弹型的 DDoS 威胁。反弹型 DDoS 攻击并不直接攻击服务器，而是攻击者利用伪造的 IP 地址，发送到目标网络的服务器，发送请求，这样该网络中的所有应答主机就会回送数据。通过类似于“反弹”的这一过程，大量消耗目标网络的流量，从而使目标系统发生拥堵或者瘫痪，无法提供正常的服务[10]。

（2）源路由器选择的 DDoS 威胁。在 IPv6 协议中，源路由器可以通过扩展报头中的路由报头，指定数据包经过的中间目标列表[11]。攻击者可以利用源路由器让数据包按照指定的路线多次来回经过目标路由器，从而产生大量的流量，使目标网络产生瘫痪。

（3）其他的 DDoS 威胁。第一种，IPv6 地址在配置时，需要先广播预设的地址，如果有主机回应已经存在该地址，就要另选地址再广播，直到没有主机回应才可使用，以此来避免地址重复。但是这一特性如果被攻击者利用，使想要加入网络的任何地址都收到重复回应，该网络将无法得到网络服务。

第二种，IPv6 中的数据流有很多，每个数据流都有预定义的服务，例如有固定的带宽，如果攻击者将伪装的数据流发送到目标流中，可以占用通信双方的带宽，从而使目标网络无法服务。攻击者还可以利用建立大量无用链接从而消耗目标网络的资源[7]。

4　基于 IPv6 的模拟集成 DDoS 攻击平台的设计与实现

4.1　基于树状结构的动态分布式网络模型

常见的分布式工具的控制体系一般是由控制台向一级傀儡主机发出指令，二级傀儡主机进行攻击。基于树状结构的动态分布式网络相较于常见的分布式网络体系的优先性显而易见，其攻击自上级到下级展开，下级无法追踪到上级，多层次的体系不易被追踪，见表 2。节点的状态由节点控制维护，不需要手动操作。

表 2　两种网络体系对比分析

Tab. 2　Comparative analysis of two network systems

	控制机制	被追踪性	效率
常见的分布式网络体系	手动操作	易被追踪	较低
基于树状结构的动态分布式网络体系	不需要手动操作	不易追踪	较高

4.2　插件技术

采用插件技术可以在不修改控制引擎的情况下对平台加强升级，使平台有良好的扩展性和可维护性[12]。控制引擎相当于电脑主机，它具有一些功能的特定接口，遵循该特定接口的“配件”可以在“主机”控制的环境下接受控制，并实现其特定功能，“主机”依赖这些“配件”以实现特定功能，“配件”依赖主机提供稳定的环境。每个插件都可以独立开发、测试和升级。插件的实现形式是多种多样的，只要适用于同一个调用接口，都可以由控制引擎启动运行。同一类插件和控制引擎定义调用接口以保证插件的功能实现、升级优化的一致性和易用性[13]。

4.3　基于 IPv6 的模拟集成 DDoS 攻击平台 GNS3 模型

基于 IPv6 的模拟集成 DDoS 攻击平台 GNS3 模型，如图 2 所示。此模型只能作为平台的显示样式，不能实现平台的相应功能。

此模型分为 3 个部分：攻击参数、仿真参数和仿真控制。攻击参数中分为泛洪式攻击开始时间、反射式攻击开始时间以及“更多参数设置”和“确定”2 个按键；仿真参数分为仿真时间和防御设置；仿真控制分为“连接”、“运行”、“结果分析”和“退出”4 个按键。

（下转第 104 页）