DDoS攻击分类与效能评估方法研究*)

王永杰 鲜 明 陈志杰 王国玉
(国防科学技术大学电子科学与工程学院 长沙 410073)

摘 要 DDoS攻击是一类常见而又难以防范的网络攻击模式,对Internet网络系统的正常运行构成了巨大威胁。DDoS攻击的分类方法和攻击效能评估是计算机网络攻防对抗研究的一项重要而紧迫的任务。本文介绍了DDoS攻击的原理、方法、一般概念和主要目标,研究了基于攻击代理的传播模式、通讯方式、作用机制等特征的DDoS攻击分类方法体系,分析了DDoS攻击的攻击效能评价指标体系。在分析了DDoS攻击效能评估的特点的基础上提出了DDoS攻击效能评估的模糊评价评估模型。

关键词 DDoS攻击,分类方法,效能评估,评估模型

Study on Taxonomy and Effectiveness Evaluation of DDoS Attacks

WANG Yong-Jie XIAN Ming CHEN Zhi-Jie WANG Guo-Yu
(School of Electronic Science and Engineering, NUDT, Changsha 410073)

Abstract DDoS attack is a common but difficultly defensive computer network attack mode. It threatens the normal operation of the Internet greatly. Study on taxonomy and effectiveness evaluation of DDoS attack is an important and urgent task in the field of computer network attack and defense. In this paper, principle, method, common concept and main object of DDoS attacks are introduced, a taxonomy method of DDoS attacks based on spread mode, communication method and effect mechanism of attack agents is studied, and indexes of DDoS attack effectiveness evaluation are analyzed. The specialties of DDoS attack effectiveness evaluation are also analyzed. Then a fuzzy evaluation model of DDoS attack effectiveness is brought forward.

Keywords DDoS attack, Taxonomy, Effectiveness evaluation, Evaluation model

1 引言

DDoS(Distributed Denial of Service)攻击是目前Internet所面临的最为常见、最具威胁,同时也是最难防范的一种攻击模式,对Internet的正常运行构成了巨大威胁。正是由于DDoS攻击实施的简易性以及Internet网络协议和体系结构设计上的一些固有缺陷,才导致了DDoS攻击的泛滥和流行。目前Internet网络上充斥着大量的可以发起DDoS攻击的工具软件,使得稍微具有一定网络知识的人都可以发起DDoS攻击。Internet网络体系结构设计的初衷是使网络中间节点尽可能快地传递数据包,而将大量的检查、验证工作由终端节点来承担,这无疑增加了终端节点的负担,同时终端节点的带宽与中间节点的带宽相比通常要小许多,从而使得终端节点更易于受到DDoS攻击的危害。

由于DDoS攻击的普遍性和危害性,使得DDoS攻击机理和防范对策的研究成了当前网络信息安全领域里的一个研究热点,吸引了众多网络信息安全研究人员开展相关研究。据作者目前所掌握的资料,当前对DDoS攻击的研究主要集中于对特定类型DDoS攻击的分析、检测和防护,相应的研究成果也主要针对特定的DDoS攻击模式,存在通用性不足的问题。

本文主要目的在于研究DDoS攻击的攻击模式分类方法体系和DDoS攻击的攻击效能评价指标体系,为评价各种DDoS攻击和防护措施的效能提供统一的评价尺度和评估模型。文章第2节主要介绍相关的研究工作。第3节研究DDoS攻击的分类方法。第4节研究DDoS攻击效能评价的指标体系。第5节提出评估DDoS攻击效果的模糊综合评价方法。最后是全文的总结,概述全文的主要内容,分析进一步研究的方向。

2 相关研究工作

文[1]提出了一种按照拒绝服务攻击的目标类型(如防火墙、Web服务器或路由器等)、消耗资源类型(如网络带宽、TCP/IP协议栈等)和攻击机理(如系统漏洞、服务过载等)的分类方法。该分类方法侧重于从攻击实施阶段对DDoS进行分析。Howard在文[2]中提出了一种计算机与网络攻击的分类方法,该分类方法的研究对象是所有各方面的计算机与网络攻击类型,没有对DDoS攻击进行深入分析。文[3]对flood攻击进行了分析研究,提出了根据参与攻击的Agent主机的数量和是否采用反射攻击模式的分类方法。文[4]对DDoS攻击的机理和防护措施进行了有益探索和讨论。文[6]提出了一种检测DDoS攻击的框架模型。文[7]从攻击与防御两个方面对DDoS攻击进行了研究,提出了DDoS攻击和DDoS攻击防御措施的分类方法,并对各种DDoS攻击方法和防御措施的主要特征和优缺点进行了对比分析。文[9]将DDoS攻击的体系结构归纳为基于攻击代理型和基于IRC

*)国家自然科学基金项目(60372039)。王永杰 博士研究生,主要研究方向为信息网络安全;鲜 明 副教授,博士;陈志杰 副教授;王国玉 研究员,博导,博士。

(Internet Relay Chat)型,同时将 DDoS 攻击划分为资源占用型和带宽占用型,对典型 DDoS 攻击工具进行了分析。

3 DDoS 攻击分类方法

3.1 DDoS 攻击概述

在研究 DDoS 攻击前,我们首先了解一下 DoS(Denial of Service)攻击。DoS 攻击就是使合法用户不能访问某些计算机网络服务的攻击企图[5]。实现 DoS 的一种常见方式是向目标系统发送数据报文流,由这些数据报文流占据目标系统的重要资源(如带宽等),从而使目标系统无法向正常用户提供服务。实现 DoS 的另外一种常见方式是向目标系统发送特意构造的数据报文,使目标系统的服务程序或网络协议崩溃或死锁,从而使目标系统无法提供正常服务。此外,攻击关键性的 Internet 基础设施(如根 DNS 服务器),有可能导致整个 Internet 网络无法正常工作,从而实现大范围的 DoS。

WWW Security FAQ[8] 对 DDoS 攻击的定义是:"DDoS 攻击就是使用多个攻击代理对单个或多个目标进行协同 DoS 的攻击方式"。DDoS 攻击通过调度大量的攻击代理对攻击目标进行协同 DoS 攻击,可以产生比单源 DoS 攻击大得多的攻击效果,同时也使攻击变得更加隐蔽和更加难以防御。

3.2 DDoS 攻击分类方法

DDoS 攻击分类可以从攻击的实施准备、攻击的作用形式和攻击对目标的影响等方面展开研究,可以分别按照:(1)攻击自动化程度;(2)攻击作用方式;(3)攻击源地址有效性;(4)攻击数据包发送速率变化方式;(5)攻击行为特征;(6)攻击代理组合模式;(7)攻击目标类型;(8)对攻击目标可能产生的影响等进行分类。其中每种分类模式可以进一步分为多个小子类。具体分类方法如图 1 所示。当然,还可能存在其他众多的 DDoS 攻击模式没有被本分类方法所涵盖,只有在其大规模发作后才为人所知,因此本分类方法也需要随着 DDoS 攻击技术的发展而不断完善。

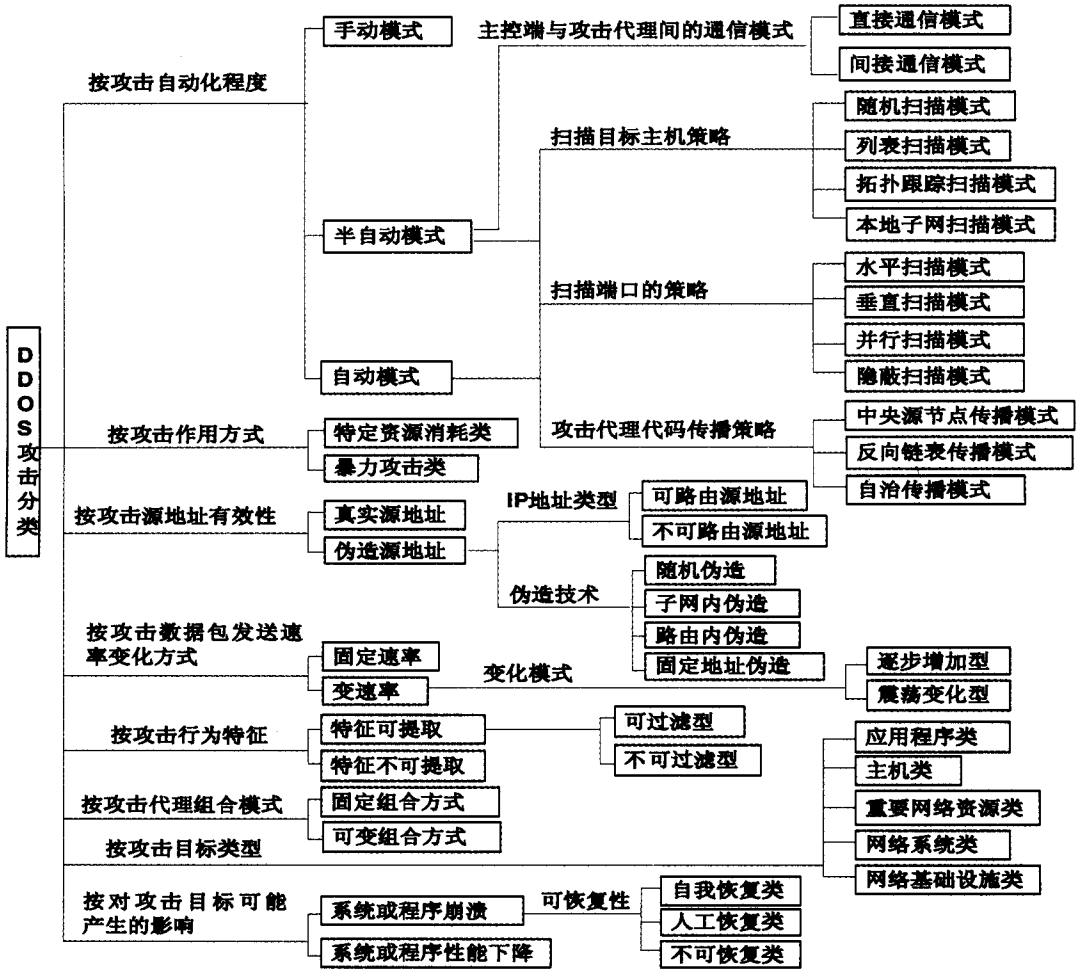

图 1 DDoS 攻击分类方法

3.2.1 按攻击自动化程度分类

按攻击自动化程度,DDoS 攻击可以分为:手动模式、半自动模式、自动模式。

根据主控端与攻击代理间的通信模式,半自动模式又可以分为:直接通信模式和间接通信模式。

在直接通信模式中,每个攻击代理要直接和主控端通信,就必须知道主控端的 IP 地址,这通常通过在攻击代理的代码中直接写入主控端 IP 地址来实现。直接通信模式的缺点在于安全性不高,任意一个攻击代理被识破,将导致整个攻击网络的暴露。

在间接通信模式中,攻击代理和主控端直接或不直接发生联系,所有的信息交流都通过某种形式的中间媒介进行。可行的中间媒介包括:IRC 聊天频道、免费的 Web 或 FTP 空间等。间接通信模式可以有效保护整个攻击网络的安全。

根据扫描目标主机的策略,半自动模式和自动模式又可以分为:随机扫描模式、列表扫描模式、拓扑跟踪扫描模式、本

地子网扫描模式。

随机扫描模式通过产生一个32字节的随机数作为扫描目标。列表扫描模式由主控端负责维护一个扫描目标IP地址列表，并分发部分IP列表给每个入侵成功的攻击代理继续进行扫描。拓扑跟踪扫描模式是指攻击代理入侵成功后，搜寻与该机有关联的主机、邮件列表等作为其继续扫描入侵的对象。本地子网扫描模式以攻击代理所在网段（通常为C类子网）作为继续扫描的对象。

根据扫描端口的策略，半自动模式和自动模式又可以分为：水平扫描模式、垂直扫描模式、并行扫描模式、隐蔽扫描模式。

水平扫描模式是指在所有扫描对象上检查同一种漏洞。垂直扫描模式是指在一个扫描对象上扫描所有可能存在的漏洞。并行扫描模式是水平扫描模式与垂直扫描模式的结合。隐蔽扫描模式是指通过放慢扫描速率、减少数据流量，使扫描过程更加隐蔽的扫描模式。

根据攻击代理代码传播策略，半自动模式和自动模式又可以分为：中央源节点传播模式、反向链表传播模式、自治传播模式。

中央源节点传播模式是指每次入侵成功后都从主控端获取攻击代理代码的传播模式。中央源节点传播模式增加了主控端的数据流量，有可能被检测出网络异常。反向链表传播模式是指每次入侵成功后从其上一级攻击代理处获取攻击代理代码的传播模式。自治传播模式是指将攻击代理代码随入侵代码一起直接发送的入侵对象的传播模式。

3.2.2 *按攻击作用方式分类*

按攻击作用方式，DDoS攻击可以分为：特定资源消耗类、暴力攻击类。

特定资源消耗类的DDoS攻击主要是利用TCP/IP协议栈、操作系统或应用程序设计上的缺陷，通过构造并发送特定类型的数据包，使目标系统的协议栈空间饱和、操作系统或应用程序资源耗尽或崩溃，从而到达DDoS的目的。

暴力攻击类的DDoS攻击则主要依靠发送大量的数据包占据目标系统有限的网络带宽或应用程序处理能力来达到DDoS的目的。通常暴力攻击需要比特定资源消耗攻击使用更大的数据流量才能达到DDoS的目的。

3.2.3 *按攻击源地址有效性分类*

按攻击源地址有效性，DDoS攻击可以分为：伪造源地址、真实源地址。

伪造源地址又可以分为：可路由源地址和不可路由源地址两类。伪造可路由源地址一方面可以逃避责任，另一方面可以用于发起反射式DDoS攻击。按照源地址伪造技术又可以分为：随机伪造、子网内伪造、路由内伪造、固定地址伪造。

随机伪造即是随机产生一个32字节的随机数作为发送数据包的源地址，随机伪造的IP很容易被识别并过滤掉。子网内伪造是指将攻击代理的IP地址伪装为其所在子网内的其他任意可用IP。路由内伪造是将源IP地址伪装为从攻击代理到攻击目标间任意路由跳点所在网段内的IP地址。固定地址伪造是将源IP地址伪装为某个固定的IP地址，可以起到反射攻击或嫁祸于人的目的。

3.2.4 *按攻击数据包发送速率变化方式分类*

按攻击数据包发送速率变化方式，DDoS攻击可以分为：固定速率、变速率。

根据数据包发送速率变化模式，变速率方式又可以分：逐步增加型和震荡变化型。

逐步增加型变速率发送方式可以使攻击目标的性能缓慢下降，并可以误导基于学习的检测系统产生错误的检测规则。震荡变化型变速率发送方式间歇性地发送数据包，使入侵检测系统难以发现持续的异常。

3.2.5 *按攻击行为特征分类*

按攻击行为特征，DDoS攻击可以分为：攻击行为特征可提取、攻击行为特征不可提取。

攻击行为特征可提取的DDoS攻击又可以分为可过滤型和不可过滤型。

可过滤型DDoS攻击主要指那些使用畸形数据包或攻击对象为目标系统的不重要服务的攻击，目标系统可以通过配置防火墙过滤规则将其滤除。不可过滤型DDoS攻击使用精心构造数据包，模仿合法用户的正常请求，一旦被过滤将影响合法用户的正常使用。

3.2.6 *按攻击代理组合模式分类*

按攻击代理组合模式，DDoS攻击可以分为：固定组合方式、可变组合方式。

3.2.7 *按攻击目标类型分类*

按攻击目标类型，DDoS攻击可以分为：应用程序类、主机类、重要网络资源类、网络系统类、网络基础设施类。

3.2.8 *按对攻击目标可能产生的影响分类*

按对攻击目标可能产生的影响，DDoS攻击可以分为：系统或程序崩溃类、系统或程序性能下降类。

根据可恢复的程度，系统或程序崩溃类又可以分为：自我恢复类、人工恢复类、不可恢复类等。

自我恢复类是指当攻击停止后系统功能可自动恢复正常。人工恢复类是指系统或服务程序需要人工重新启动才能恢复。不可恢复是指攻击给目标系统的硬件设备造成了不可修复性的损坏。

4 DDoS攻击效能评价指标体系

由于DDoS攻击的复杂性和作用效能的多重性，因此对其进行效能评价通常不能用单个明确定义的效能指标来表示，而需要用一组效能指标来刻画。这些效能指标分别表示DDoS攻击的各个重要属性或攻击行为的多重目的。

由于效能量度的复杂性，效能量度不像物理量的量度那样直接。在定义效能指标时，一般应考虑以下特点：

- 随机性
- 多尺度性
- 不确定性
- 局限性

从上面的分类方法可以看出，DDoS攻击的效能是多方面的，因此DDoS攻击的效能评价指标也必须从多方面进行研究。评价DDoS攻击的效能可以从DDoS攻击自身性能和对攻击目标的作用能力两个方面考虑。

从DDoS攻击自身性能方面来看，其评价指标主要有：攻击代理的自动化程度、攻击代理的传播速度、攻击代理的传播范围分布、攻击代理的传播途径数、攻击代理的入侵成功率、攻击代理间通信的隐蔽性、DDoS攻击的方法数、DDoS攻击方法的抗检测能力、DDoS攻击方法的抗过滤能力等。

从DDoS对攻击目标的作用能力来看，其评价指标主要有：目标的可恢复性、攻击对目标的影响、目标的类型、目标的重要程度、目标性能下降程度等。

上述的效能评价指标的取值有些是定性的量，有些是定量的量，在评估 DDoS 攻击的综合效能时必须首先进行适当的预处理。

5 DDoS 攻击效能评估方法

模糊评估是一种非常适用于处理评估项的观测结果难以定量表达的评估问题的综合评估方法。模糊综合评估方法的理论基础是模糊数学理论，模糊理论特别适用来处理定性的评估项目。从上述的分析可以看出，DDoS 攻击效果评估指标中既包含定性的指标项也包含定量的指标项，因此可以使用模糊评估方法来处理这些评估项的评估结果，并形成总的评估结果。

假设 $I=\{I_1,I_2,\cdots,I_n\}$ 是全体评估项的集合，$I_k(k=1,2,\cdots,n)$ 表示第 k 个评估项。

$L=\{L_1,L_2,\cdots,L_m\}$ 表示每个评估项 $I_k(k=1,2,\cdots,n)$ 的各种可能的定性评估结果。

则对每一个 $L_i(i=1,2,\cdots,m)$ 可建立一个模糊子集 l_i。

设 $d_{ki}=l_i|I_k$ 表示 I_k 对 l_i 的隶属度，即第 k 个评估项可以被指定评估结果 L_i 的程度。

有几种方法可以用来确定 d_{ki} 的值。当评估项目 I_k 是定性的情况下，可采用模糊统计实验的方法来确定。为了使评估员作出的评估结果断言 L_i 所占的比例趋近于隶属度 d_{ki}，模糊统计实验法需要足够的评估专家。当评估项 I_k 是定量的情况下，d_{ki} 可以使用隶属度函数 $\mu_{ki}(x)$ 计算得到，这里 x 是 I_k 的测量值。d_{ki} 也可以采用频率法获得。

当所有 $d_{ki}(i=1,2,\cdots,m$ 和 $k=1,2,\cdots,n)$ 经评估确定后，可以建立模糊关系矩阵：

$$R=(d_{ki})=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{bmatrix}$$

通常情况下，n 个评估项 $I_1,I_2,\cdots,I_n$ 并非同等重要，它们对综合评价结果的影响是不同的，所以在进行综合评价前，必须先确定模糊权向量。设 $W=(W_1,W_2,\cdots,W_n)$ 表示模糊权向量，$P=\{$对评价有意义的评估项$\}$，是一个模糊子集，则 $W_j(j=1,2,\cdots,n)$ 代表评估项 I_j 对 P 的隶属度。

模糊权向量的确定可以采用专家估计的办法。专家的估值需要经平均和归一化处理。也就是说，如果说 W'_j 是评估项 I_j 对 P 的平均隶属度，则归一化的模糊权向量计算如下：

$$W_j=W'_j/\sum_{i=1}^{n}W'_j$$

一旦确定了模糊权向量 W，便可得到模糊综合评估结果 E。

$$E=W\circ R=(W_1,W_2,\cdots W_n)\circ \begin{bmatrix} d_{11} & d_{12} & \cdots d_{1m} \\ d_{21} & d_{22} & \cdots d_{2m} \\ \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots d_{nm} \end{bmatrix}=(a_1,a_2,\cdots,a_m)$$

其中“$\circ$”是模糊综合运算符，可表示为 $F(*,\oplus)$，它包含两个操作“$*$”和“$\oplus$”。$a_i(i=1,2,\cdots,m)$ 是通过 W 和 R 的第 i 列元素运算得到的一个值，其含意是总的评估结果对模糊子集 l_i 的隶属度，也就是对总的评估结果可指定 L_i 的程度。

$$a_i=(w_1*d_{1i})\oplus(w_2*d_{2i})\oplus\cdots\oplus(w_n*d_{ni})\quad i=1,2,\cdots,m$$

模糊综合运算符 $F(*,\oplus)$ 中的两个操作可能有多种变化方式。例如，一种情况是 $F(\times,\vee)$ 运算符，其中“$\times$”代表两个数的积，“$\vee$”代表在几个数值中选择最大的。使用该运算符 $a_i(i=1,2,\cdots,m)$ 计算如下：

$$a_i=\vee(w_j\times d_{ji})=\max\{w_jd_{ji}\,|\,j=1,2,\cdots,n\}$$

至于模糊综合运算符 $F(*,\oplus)$ 中的运算如何定义，这里不做过细讨论。如果采用这种方法进行实际的系统安全评估，可在评估方法中专门研究和定义。

模糊评价的结果是一个向量(E)，为了能够比较多个系统的总的评估结果，或者为了其它某些目的，还应对 E 进行分析和单值化。可采用最大隶属度原则或加权平均的办法。例如，加权平均计算如下：

$$Q=\sum_{i=1}^{m}ia_i^k/\sum_{i=1}^{m}a_i^k$$

其中，Q 表示总的综合评价结果，常数 k 对较大的 a_i 有影响。当 $k\to\infty$，Q 的值将与最大隶属度原则得到的值相同。

结论 DDoS 攻击是一种易于实施、影响巨大的计算机网络攻击方式，已成为危害 Internet 网络安全和正常运行的主要因素，对其分类方法体系和攻击效能评估研究必须给以足够的重视。不同的 DDoS 攻击方式，其攻击代理传播模式、通讯方式、作用机制等各异，本文据此提出了一种 DDoS 攻击的分类方法体系。

DDoS 攻击的攻击效能是多元的，影响 DDoS 攻击行为攻击效能的因素也是多方面的。因此，评价 DDoS 攻击的攻击效能必须综合各方面的影响因素，才能够得到 DDoS 攻击效果的总体评估结果。模糊评估是一种非常适用于处理评估项的观测结果难以定量表达的评估问题的综评估方法，将在研究 DDoS 攻击效果评估中发挥重要作用。

参 考 文 献

1 Kargl F, Maier J, Weber M. Protecting web servers from distributed denial of service attacks. In: Proceedings of 10th International World Wide Web Conference, May 2001

2 Howard J D. An analysis of security incidents on the Internet: [PhD thesis]. Carnegie Mellon University, August 1998

3 Hussain A, Heidemann J, Papadopoulos C. A Framework for Classifying Denial of Service Attack. In: Proceedings of SIGCOMM 2003, 2003

4 Razmov V. Denial of Service Attacks and How to Defend Against Them. http://www.cs.washington.edu /homes/valentin/papers/DoSAttacks.pdf

5 CERT CC. Denial of Service Attacks. http://www.cert.org/tech tips/denial of service.html

6 Hussain A, Heidemann J, Papadopoulos C. A Framework for Classifying Denial of Service Attack. In: Proceedings of SIGCOMM 2003, 2003

7 Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 2004,44(5):643～666

8 Stein L D, Stewart J N. The World Wide WebSecurity FAQ, version 3.1.2, February 4, 2002. Available at: http://www.w3.org/Security/Faq

9 Specht S M, Lee R B. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In: Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, September 2004. 543～550