

## 基于模糊理论的分布式拒绝服务攻击检测

张彦波, 李 明

(华东师范大学 信息科学技术学院, 上海 200062)

(zybyanbo0903@sina.com)

**摘 要:**针对分布式拒绝服务攻击的检测问题,提出基于模糊逻辑的动态的阈值检测方法。通过对攻击的数据包进行模糊混合运算,按照择近原则得到判决结果,该结果即为待检测量的攻击程度(可信任程度)。网络管理员通过该结果做出及时的反应,在最大限度上降低攻击造成的损失。

**关键词:**分布式拒绝服务;模糊检测;数据包

**中图分类号:** TP309 **文献标识码:** A

## DDoS flood attacks detection based on fuzzy theory

ZHANG Yan-bo, LI Ming

(School of Information Science and Technology, East China Normal University, Shanghai 200062, China)

**Abstract:** To resolve the problem of detecting Distributed Denial of Service (DDoS) attacks, a dynamic threshold detection method based on fuzzy logic was proposed. Through fuzzy compound operation analysis and according to nearest neighbor principle, a decision was got, which is the attack level (trust degree) of detected packet. Web security masters can make responses betimes according to the result, and the responses can save furthest the loss under real time attacks.

**Key words:** Distributed Denial of Service (DDoS); fuzzy detection; packet

### 0 引言

本文提出的模糊检测方法能定量地分析分布式拒绝服务(Distributed Denial of Service, DDoS)攻击的程度(而不是可能性)。文中将模糊聚类同 DDoS 的检测进行了合理的结合,提出这一分类方法的目的在于:1)通过对数据的多途径分析来给 IDS 提供更多的有用的信息;2)通过对数据的模糊分析能够给出一种更能够令人接受的关于 DDoS 攻击的检测方法,这种分析方法能够将接受到的数据包的攻击程度用数字定量地刻画;3)能够实时地进行分析,其计算繁杂程度小,能够让受攻击对象在有限的时间内做出反应,减少攻击对服务器的危害程度。

### 1 关于 DDoS 攻击的特征提取

DDoS 攻击是攻击者通过直接或者间接地一些远程的计算机上安装程序,然后再发动这些计算机对某个对象进行攻击<sup>[9]</sup>。这些攻击大致可以分成逻辑攻击和流量攻击两部分。逻辑攻击主要是向受攻击对象发送使对方产生错误逻辑的一些数据包(如:Ping-to-Death);流量攻击主要是利用一些传输协议向受攻击对象发送大量的数据包,使受攻击对象不

能够及时地处理这些数据包,从而造成服务器不能正常地响应用户的使用请求(SYN flood, DNS Request floods 等)。那些代理攻击的计算机在实际攻击者的控制下一起发动攻击,在短时间内导致系统的资源耗尽,使合法的请求不能得到响应,这是 DDoS 攻击的一个显著的特征。本文提出的检测方法主要是针对流量攻击而设计。对于 DDoS 攻击的特征提取,由于 DDoS 攻击利用正常网络使用中的合法功能,而应用于非法的途径,因此对于网络实时监控数据包的异常行为是可行的。现有的检测系统主要侧重于对于数据流量的特征进行提取,包括数据包头标志位、相关性、有效时间长度(TTL)等<sup>[6,9,10]</sup>。例如 SYN flood 攻击的特征提取的是 TCP 的包头标志位,这是因为在 SYN flood 攻击中,SYN 和 FIN 的标志位是不匹配的<sup>[6]</sup>。我们这里假定所提取的特征是已经确定的特征向量。

### 2 原理分析

对于检测系统来说,要提高系统的性能应该从改善系统的检测率,误警率和漏报率三个方面来着手。在发动的 DDoS 攻击中,合法请求的数量远远小于恶意攻击的数量<sup>[9]</sup>,而且正常的访问请求的标准模型是更容易获得的。因此我们提

收稿日期:2005-06-13;修订日期:2005-09-01

作者简介:张彦波(1979-),男,河南安阳人,硕士研究生,主要研究方向:网络安全、随机数据分析;李明(1955-),男,江苏无锡人,教授,博士生导师,主要研究方向:网络安全、信号处理、随机数据分析和测试过程。

- Baltimore[C]. Maryland, USA, 1989: 369-407.
- [5] LANDWEHR CE, BULL AR, MCDERMOTT JP, et al. A Taxonomy of Computer Program Security Flaws, with Examples[R]. Naval Research Laboratory, Tech Rep: 9591, 1993.
- [6] HOWARD. A Taxonomy of Computer and Network Attacks[EB/OL]. <http://www.cert.org/research/JHThesis/Word6/chap06.doc>, 2003-09.
- [7] INDQVIST UL, JONSSON E. How to Systematically Classify Computer Security Intrusions[A]. IEEE Symposium on Security and Privacy[C]. Oakland, 1997. 154-163.
- [8] AMOROSO EG. Fundamentals of Computer Security Technology[M]. Upper Saddle River, NJ: Prentice-Hall PTR, 1994.
- [9] 戴英侠, 连一峰, 王航. 系统安全与入侵检测[M]. 北京: 清华大学出版社, 2002.
- [10] 王晓程, 刘恩德, 谢小权. 攻击分类研究与分布式入侵检测系统[J]. 计算机研究与发展, 2001, 38(6): 727-734.

出的检测包含两个方面的检测:正常信号检测和异常信号检测,前者用来提高系统的检测率,后者用来降低系统的漏报率,而最后的判决器输出的综合结果则可以有效降低系统的误警率。原理如图 1 所示。

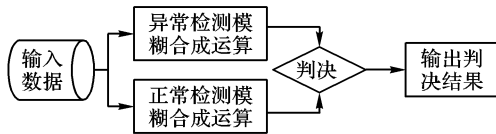


图1 模糊并行检测模型

这里处理的问题是隶属于元素对标准模糊集的识别这一范畴的问题,也就是将网络数据包看成是需要识别的元素,将其对标准的模糊集进行识别。设  $a, b \in F_{1 \times n}$ , 定义:

$$\sigma = (a \circ b) \wedge (a \cdot b)^c \quad (1)$$

式(1)为元素  $a$  与  $b$  之间的格贴近度(其中  $\circ, \cdot, \wedge, c$  分别表示模糊运算中的内积,外积,取最小值和求补)。显然,  $\sigma$  越大表明  $a$  与  $b$  越贴近( $\sigma_{\max} = 1$ )<sup>[8]</sup>。若  $A_{1 \times n}, B_{1 \times n} \in F_{1 \times n}$ , 则定义:

$$\sigma(A_{1 \times n}, B_{1 \times n}) = \sqrt{\sum_{i=1}^n [(a_i \circ b_i) \wedge (a_i \cdot b_i)^c]^2} \quad i \in \{1, 2, \dots, n\} \quad (2)$$

式(2)满足严格贴近度的定义<sup>[9]</sup>。然后用模糊数学中的择近原则进行最后的判决。所谓择近原则是指:若  $A_{1 \times n}^i \in F_{1 \times n}(u), i = 1, 2, \dots, m, A = \{A_{1 \times n}^1, \dots, A_{1 \times n}^m\}$  构成一个标准模型库。对于待检测的  $B_{1 \times n} \in F(u)$ , 若  $j \in \{1, 2, \dots, m\}$ , 使  $\sigma(B, A) = \max_{1 \leq j \leq m} \sigma(B_{1 \times n}, A_{1 \times n}^j)$ , 则说明在  $\sigma$  意义下  $B_{1 \times n}$  在  $A$  中最贴近  $A_{1 \times n}^j$ , 或者是  $B_{1 \times n}$  在  $A$  中相对取作  $A_{1 \times n}^j$ <sup>[8]</sup>。

综上所述,具体检测步骤为:设  $X_{1 \times n} = (x_1 \dots x_n)$  是待检测的  $n$  维向量构成的数据包,  $A_{1 \times n} = (a_1 \dots a_n)$  为异常信号模板  $n$  维向量;  $N_{1 \times n} = (n_1 \dots n_n)$  是正常信号模板的  $n$  维向量。将上述三个向量进行模糊合成运算就可以知道待检测的  $n$  维信号  $X_{1 \times n}$  与标准的异常信号的贴近度:

$$\sigma_a = \sigma(A_{1 \times n}, X_{1 \times n}) = \sqrt{\sum_{i=1}^n [(a_i \circ x_i) \wedge (a_i \cdot x_i)^c]^2} \quad (3)$$

与正常信号的贴近度:

$$\sigma_n = \sigma(N_{1 \times n}, X_{1 \times n}) = \sqrt{\sum_{i=1}^n [(n_i \circ x_i) \wedge (n_i \cdot x_i)^c]^2} \quad (4)$$

然后再按照择近原则对所得到的贴近度值  $\sigma_a, \sigma_n$  进行比较,就可以得出以下结论:

$$\sigma = \begin{cases} \sigma_a & \sigma_a \geq \sigma_n \\ \sigma_n & \sigma_a < \sigma_n \end{cases} \quad (5)$$

由于  $\sigma(A_{1 \times n}, B_{1 \times n})$  是欧式距离空间的距离表达式<sup>[7]</sup>, 所以从这一意义上来讲,本文提出的检测方法本质上便是利用待检测数据包的特征向量集与标准模板在  $\sigma$  意义下的距离作为依据进行判决的。通过对结果的比较来合理地判断一个信号是正常还是异常,相对于仅对信号进行异常检测的检测系统,本文的提出的系统更为合理。

### 3 有效性分析

为了保证入侵检测系统的效率和满足实时性的要求,入

侵检测必须在系统的性能和检测能力之间进行权衡,并且可能要牺牲一部分检测能力来保证系统可靠、稳定地运行并具有较快的响应速度,这就表现在阈值的选择上。阈值选取的是否合适在很大的程度上决定了系统的性能<sup>[1]</sup>。应该根据不同的背景使用不同的阈值,对于同一个检测系统也应该要求阈值是可变动的。但是什么样的阈值才是特定环境下的最佳阈值仍然是开放性课题。在本检测系统中,由于是对同一数据包进行的同步并行的贴近度计算、判决,因此是一个动态阈值检测系统。因为在判决空间中一个数据包要么为一个合法请求,要么为一个攻击的信号(所不同的就是攻击的程度有区别),所以数据包对哪一个模板的贴近度大就说明该数据包隶属于该模板的程度就大,根据这个就可以做出合理的判决。该检测系统的阈值就是由被检测数据包的具体情况(位置)来决定的,所以这一阈值和实时检测环境是一致的,检测率较高。同时检测系统的可移植性强,因为该系统不依赖于特定的网络结构,这也是模糊数学的一个优点。这就保证了检测系统在不同的环境中能够及时有效的检测出不同程度的攻击,并提高了系统的稳定性和可用性。

### 4 结语

本文提出的检测系统是基于模糊逻辑的并行检测系统,其可移植性强,因为该系统可以对不同的学习经历主机或服务器进行检测。作为一个复杂环境下的检测系统,该系统能够判断出该信号的可信任程度。因为对于 DDoS 攻击的检测来讲,最重要的是要能够让管理员能够及时的做出反应,而判断的依据就是利用可信任程度,也就是阈值的大小。本文提出的动态阈值检测系统能够很好地解决阈值设置的问题,采取这样的检测系统,对于改善整体系统的检测率、漏警率和误报率有很好的作用。

#### 参考文献:

- [1] LI M. An approach to reliably identifying signs of DDoS flood attacks based on LRD traffic pattern recognition[J]. Computer and Security, 2004, 23(7): 549-558.
- [2] LI M, LIU JG, LONG DY. Probability principle of a reliable approach to detect signs of DDoS flood attacks[A]. PDCAT 2004[C]. Springer LNCS 3320, 2004. 569-572.
- [3] LI M, JIA W, ZHAO W. Decision analysis of network-based intrusion detection systems for denial-of-service attacks[A]. IEEE ICII2001[C]. Beijing, 2001. 1-6.
- [4] JIN S, YEUNG DS. A covariance analysis Model for DDoS Attack Detection[A]. IEEE International Conference on Communications[C]. Paris, France, 2004.
- [5] 龚怀云, 寿纪麟, 王绵森. 应用泛涵分析[M]. 西安: 西安交通大学出版社, 1995.
- [6] 汪培庄, 韩立岩. 应用模糊数学[M]. 北京: 经济学院出版社, 1989.
- [7] PENG T, LECKIE C, RAMAMOHANARAO K. Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring[A]. Proceedings of the Third International IFIP-TC6 Networking Conference(NETWORKING 2004)[C]. 2004. 771-782.
- [8] HOWARD JD. An analysis of security incidents on the Internet 1989-1995[D]. PHD thesis, Carnegie Mellon University, 1997.