文章编号:1674 - 2869(2017)01 - 0091 - 05

DDoS攻击检测模型的设计

胡中功,程思婷,沈 斌,陈爱杰
武汉工程大学电气信息学院,湖北 武汉 430205

摘 要:为了有效检测服务器是否受到DDoS攻击,设计了一种基于朴素贝叶斯分类算法的DDoS攻击检测模型. 首先大量抓取服务器数据包,选择受到DDoS攻击时产生较明显变动的5种特征数据作为基本参数,所有数据可分为受攻击与未受攻击两类. 然后利用正态分布函数拟各合特征量的分布情况,并计算出各个特征量的条件概率. 最后,选取测试数据,得到测试数据在贝叶斯公式下被分为受攻击与未受攻击两类的后验概率,并通过比较此两个后验概率值的大小,判断出服务器是否受到DDoS攻击. 该模型经MATLAB仿真实验的验证,获得了较高的准确率,保证了对DDoS攻击的有效检测,并由C++代码进行实现.

关键词:DDoS攻击;朴素贝叶斯分类算法;特征数据;正态分布函数; 检测模型
中图分类号:TP309 **文献标识码**:A **doi**:10. 3969/j. issn. 1674-2869. 2017. 01. 016

Design of Attacks Detection Model of Distributed Denial of Service

HU Zhonggong, CHENG Siting, SHEN Bin, CHEN Aijie
School of Electrical and Information Engneering, Wuhan Institute of Technology, Wuhan 430205, China

Abstract: To effectively detect whether the server was attacked by distributed denial of service (DDoS), we designed a DDoS attacks detection model based on the naive Bias classification algorithm. Firstly, five kinds of data with obviously changed characteristic in DDoS attacks, which were obtained from the large number of server data packets, were chosen as the basic parameters and divided into two categories of being attacked or not. Then, the conditional probability of each characteristic was calculated by using normal distribution function to fit the characteristic parameters. Finally, whether the server was attacked or not by DDoS was judged by comparing the two posterior probabilities of the selected test data based on the Bayesian formula. The model established by C++ code ensures the effective detection of DDoS attacks with higher accuracy via the MATLAB simulation experiments.

Keywords: DDoS attacks; naive Bayes classification algorithm; feature data; normal distribution function; detection model

分布式拒绝服务(Distributed Denial of Service,DDoS)攻击,是通过大量合法的请求,占用大量的网络资源,使受害主机或网络不能及时接收并回应外界请求,以达到使网络瘫痪的目的. DDoS攻击容易实现且难以防范,它是一种在所有针对Internet攻击中,非常常见的攻击方式. DDoS攻击已经是当前网络安全所面临的最严峻的威胁之一[1-3].

2013年3月,Spamhaus、CloudFlare遭到攻击,攻击流量峰值达到每秒300 Gbit,“差点瘫痪欧洲网络”;2014年2月,受攻击对象为CloudFlare客户,据称当时包括维基解密在内的78.5万个网站

收稿日期:2016-06-27
作者简介:胡中功,硕士,教授. E-mail:hhyjs2004@163.com
引文格式:胡中功,程思婷,沈斌,等. DDoS攻击检测模型的设计[J]. 武汉工程大学学报,2017,39(1):91-95.
HU Z G,CHENG S T,SHEN B,et al. Design of attacks detection model of distributed denial of service [J]. Journal of Wuhan Institute of Technology,2017,39(1):91-95.

安全服务受到影响;2014年12月,阿里云在微博上发布一则声明,称部署在阿里云上的某知名游戏公司,遭遇了全球互联网史上最大的一次DDoS攻击,其攻击流量峰值达到每秒453.8 Gbit[4].

就现今的网络状况而言,世界的每一个角落都有可能受到DDoS攻击,但是只要尽可能进行分析和研究[5],检测到这种攻击并且作出反应,损失就能够减到最小程度. 对于DDoS攻击采取相应的检测和防范措施,也将有助于全球网络安全体系的建立.

目前许多防火墙安全系统采用的DDoS攻击检测方式仍是传统的选取经验值的方法,由于直接取值而未对服务器实际承载量作出准确判断,经常会出现判断失误的情况. 为了使检测更具有针对性,提高判断的准确率,提出一种智能化检测模型的设计. 通过分析DDoS攻击原理,结合服务器的特征数据,运用朴素贝叶斯分类算法,设计出DDoS攻击检测模型. 经MATLAB仿真测试成功后,利用C++语言编写出模型实现代码.

1 DDoS攻击原理

DDoS攻击网络[6-8]主要分为4个部分,分别为攻击者、攻击主控机、攻击执行机及受害者,如图1所示.

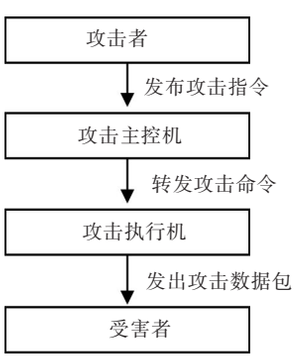

图1 DDoS攻击示意图

Fig. 1 Schematic diagram of DDoS attacks

攻击者首先入侵存在系统服务安全漏洞的服务器或计算机,并安装相关攻击软件,将少量机器作为攻击主控机,大量机器作为攻击执行机. 执行攻击任务时,攻击者首先通过控制攻击主控机,向其发布攻击命令;攻击主控机再控制攻击执行机,使其发出攻击数据包. 在攻击者向攻击主控机发布攻击命令后,攻击者可关闭或脱离网络,以避免追踪.

2 基于朴素贝叶斯算法的DDoS攻击检测模型设计

2.1 朴素贝叶斯分类算法

朴素贝叶斯分类算法[9-10],其分类原理是通过某对象的先验概率,利用贝叶斯公式计算出其后验概率,即该对象属于某一类的概率,然后选择具有最大后验概率的类作为该对象所属的类. 朴素贝叶斯分类算法是最小错误率意义上的优化.

2.1.1 *贝叶斯公式* 设A, B是两个随机事件且$P(A)>0$,称$P(B|A)=P(AB)/P(A)$为在条件A下,事件B发生的条件概率. 同理,$P(A|B)=P(AB)/P(B)$为在条件B下,事件A发生的条件概率. 则联合概率[11]为

$$P(AB)=P(A|B)P(B)=P(B|A)P(A) \tag{1}$$

设S为某一实验E的样本空间,B_1, B_2, …, B_n为E的一组事件,若$B_iB_j=\Phi$(即B_i,B_j是相互独立的),i=1, 2, …, n, j=1, 2, …, n;但i和j不同时取同一个值. $B_1\cup B_2\cup\cdots\cup B_n$则称$B_1$, B_2, …B_n为样本空间S的一个划分. 现存在A为E的事件,B_1, B_2, …B_n为E的样本空间S的一个划分,且$P(B_i)>0$(i=1, 2, …n),则有全概率公式:

$$P(A)=P(A|B_1)P(B_1)+P(A|B_2)P(B_2)+\cdots +P(A|B_n)P(B_n)=\sum P(A|B_i)P(B_i) \tag{2}$$

根据联合概率公式(1)及全概率公式(2)推导而知:

$$P(AB_i)=P(A|B_i)P(B_i)=P(B_i|A)P(A)= P(B_i|A)\ \sum P(A|B_i)P(B_i) \tag{3}$$

并且得到贝叶斯公式[12,13]:

$$P(B_i|A)=P(B_i)P(A|B_i)/P(A) \tag{4}$$

$P(B_i)$表示事件B_i发生的概率;$P(A)$表示事件A发生的概率;$P(A|B_i)$表示在事件发生的情况下,事件A发生的概率. $P(B_i)$、$P(A)$为已知的先验概率,$P(A|B_i)$为条件概率. $P(B_i|A)$表示在事件A发生的情况下,事件B_i发生的概率,$P(B_i|A)$为需要求取的后验概率.

2.1.2 *朴素贝叶斯分类器设计* 运用朴素贝叶斯分类器[14]的一个前提条件是,假设事件分类或条件之间的关系相互独立.

在设计朴素贝叶斯分类器时,考虑到事件A包含许多独立性特征A_1,A_2,…,A_m,由概率公式:

$$P(A|B_i)=P(A_1|B_i)P(A_2|B_i)\cdots P(A_m|B_i) \tag{5}$$

及贝叶斯公式(4)得:

$$P(B_i|A)=P(B_i)P(A|B_i)/P(A)= P(B_i)\ \prod_{j=1}^{m}P(A_j|B_i)/P(A) \tag{6}$$

利用此公式,可分别求得后验概率$P(B_1|A)$,$P(B_2|A)$,…,$P(B_n|A)$的值. 选择具有最高概率的值,判断在事件A发生的情况下,哪一个事件B_i最可能发生,并作出相应的归类决策.

在实际使用中,由于对比时,分母$P(A)$为相同值,则在计算中也可省略除法步骤,在不影响结果的前提下简化计算. 后验概率公式可简化后运用于计算中:

$$P(B_i|A)=P(B_i)\prod_{j=1}^{m}P(A_j|B_i) \tag{7}$$

某个服务器某时刻的特征及参数如表1所示.

由于网络占用率、TCP链接数、TCP链接数的增长率等皆为连续变量. 无法采用离散变量的方式来计算概率. 可假设5种特征数据都为正态分布,利用样本计算出均值及其方差,从而得到正态分布的密度函数. 根据密度函数,可算出某点的密度函数的值,即条件概率值.

表1　服务器参数

Tab. 1　Datas of Server

是否受到DDOS攻击 attacked by DDoS or not	网络占用率 occupancy rate of network/%	TCP链接数 TCP links/piece	TCP链接数的增长率 growth rate of TCP links/%	CPU占用率 occupancy rate of CPU/%	内存占用率 occupancy rate of memory/%
yes	95	637	235	97	93
yes	87	592	296	90	79
no	60	210	90	68	57
no	49	69	63	57	31

在服务器受到攻击的情况下,其网络占用率呈正态分布,期望值为μ=0.92,方差为σ^2=0.8. 当网络占用率为0.95时,其条件概率约为0.795 3.

$$P(\text{网络占用率}|\text{受到攻击})=\frac{1}{\sqrt{2\pi\sigma^2}}e^{\frac{-(0.95-\mu)^2}{2\sigma^2}}\approx 0.795\ 3$$

如此,在服务器是否受攻击情况下,通过事先计算出5种特征量的条件概率,结合是否受到攻击的先验概率,再利用贝叶斯公式得出后验概率,对服务器是否受到攻击作出判断.

P(受到攻击|网络占用率,TCP链接数,…,内存占用率)

$=P$(网络占用率|受到攻击)…P(内存占用率|受到攻击)P(受到攻击)

P(未受攻击|网络占用率,TCP链接数,…,内存占用率)

$=P$(网络占用率|未受攻击)…P(内存占用率|未受攻击)P(未受攻击)

最后,比较P(受到攻击|网络占用率,TCP链接数,…,内存占用率)与P(未受攻击|网络占用率,TCP链接数,…,内存占用率)的大小,选择概率较高的值作出分类决策.

朴素贝叶斯分类器的设计主要分为3个步骤:

1)收集并提取有效数据:有效数据的选取对于算法的训练非常重要. 利用抓包工具及数据抓取程序获取多组特征数据,选取的数据包含受攻击状态量和未受攻击状态量,并进行属性的分类标记. 然后对数据进行适当选择,选出5种有效的特征数据.

2)训练数据:随机提取部分所标记的多组5种特征数据,分别计算出在受到攻击与未受攻击分类下,此5种独立特征参数的各条件概率.

3)分类测试:选择未参与训练的数据进行测试,得出后验概率,以获得这些数据的分类结果. 统计并计算出错误率,验证算法的准确性.

2.2　DDoS攻击检测模型设计

DDoS攻击检测模型的设计流程如图2所示.

对不同情况下的数据包进行分类标记后,提取有效数据并对数据进行正态分布拟合[15-16],得到各特征数据的条件概率. 再结合得到的先验概率,利用朴素贝叶斯分类算法进行分类测试. 得到测试数据被分为受攻击与未受攻击的后验概率后,比较其大小并得出判断结果,即服务器是否受到攻击,再将分类结果与实际值做比较. 若测试结果未能达到要求,则重新提取并选择数据,确保所选择数据的有效性,再次进行训练;若测试结果达到预期要求,则此DDoS攻击检测模型设计基本成功. 基于目标服务器在受到DDoS攻击时的数据表现,选择数据变化较为明显的网络占用率、TCP连接数、TCP链接数的增长率、CPU占用率、内存占用率等5种特征数据作为有效数据. 一共选取600组样本数据包,其中既包含受攻击状态下的数据,也包括未受攻击状态下的数据;对应于选取的5种特

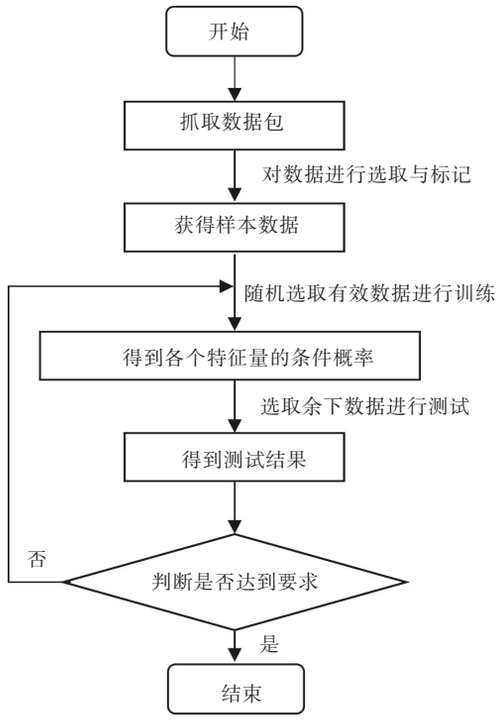

图2 DDoS攻击检测模型设计流程图

Fig. 2 Design flowchart of DDoS attacks detection model

征数据,受攻击情况下样本分类标记为1,未受攻击情况下样本分类标记为2. 若利用向量的形式表示出来,即形成一个600行(600组样本数据),6列(前5列为数据特征值,第6列为样本分类)的二维向量. 随机选择其中500组样本数据作为训练量,剩余100组样本数据为测试量,利用正态分布函数拟合样本数据的分布情况.

由于样本中5种特征数据的取值范围分布不均,在计算中可能会出现偏差较大或数据溢出的情形,所以得到各特征量的条件概率后,进行取对数值的平滑处理,以减小误差、方便计算.

3 MATLAB仿真及C++代码测试

3.1 MATLAB仿真实验

在实际编写DDoS攻击检测模型的C++代码前,首先利用MATLAB仿真平台进行仿真实验的验证. 经过随机取得数据的训练,得出条件概率后,利用余下数据进行测试,求出所设计模型的准确率.

采用MATLAB仿真得到DDoS攻击检测模型如图3所示.

图3中,横坐标表示受测试的数据有100组;纵坐标表明样本数据的分类属性,在纵坐标1.0处表示受到DDOS攻击,在纵坐标2.0处表示未受DDOS攻击. 图标"○"代表的是测试样本的真实分

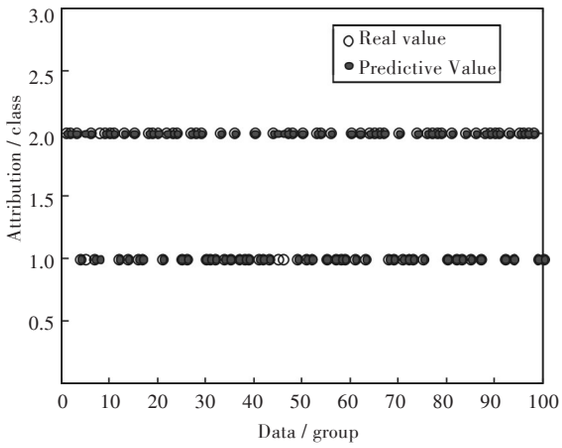

图3 DDoS攻击检测模型仿真图

Fig. 3 Simulation diagram of DDoS attacks detection model

类情况,图标"•"则代表经朴素贝叶斯分类后得出的样本的预测分类情况. 若"○"与"•"重合,则表明此组样本分类是准确的. 经多次仿真测试,对于是否受到攻击,最终测得的准确率都在90%以上,基本满足设计要求。

3.2 C++代码及测试结果

DDoS攻击检测模型主要C++函数代码介绍:

GetData(); //获取样本文件中的特征数据及分类

TrainData (); //对样本中的数据利用正态分布函数进行拟合,得到各个特征量的条件概率

Test(); //通过取对数的方式使数据平滑后,利用朴素贝叶斯分类方法对训练结果进行分类测试部分测试结果如示意图4和图5所示.

```
log_Prob2=-0.389 659
log_Prob1=-0.683 522
类别为2:-0.389 659
未受到攻击!
```

图4 判断受到攻击

Fig. 4 Judgment of being attacked

```
log_Prob2=-0.677 94
log_Prob1=-0.353 702
类别为1:-0.353 702
正受到攻击!
```

图5 判断未受攻击

Fig. 5 Judgment of not being attacked

4 结　语

笔者采用朴素贝叶斯算法设计了DDoS攻击检测模型,在设计过程中,省略了各个特征量之间相互独立这一条件.经过仿真测试,仍取得了较好的实验效果.此DDoS攻击检测模型可作为一个模块,嵌入到防火墙系统中.根据服务器的实际承载情况,对其是否受DDoS攻击进行有针对性的分类.并配合其他安全防护模块使用,以实现对服务器的有效保护.

参考文献:

[1] 张永铮,肖军,云晓春,等.DDoS攻击检测和控制方法[J].软件学报,2012,23(8):2058-2072.
ZHANG Y Z,XIAO J,YUN X C,et al. DDoS attacks detection and control mechanisms [J]. Journal of Software, 2012, 23(8):2058-2072.

[2] 刘敏霞,余杰,李强,等.基于P2P系统的DDoS攻击及其防御技术研究综述[J].计算机应用研究,2011,28(5):1609-1613.
LIU M X,YU J,LI Q,et al. Research on P2P-based DDOS attacks and their defense mechanism [J]. Application Research of Computers, 2011, 28(5):1609-1613.

[3] 徐琳.应用层DDoS攻击防御与检测方法[D].上海:上海交通大学,2012.

[4] 聚趣库.揭秘DDoS黑市:50块钱就能击瘫一家网站[EB/OL].(2014-12-29)[2016-06-20].http://www.vccoo.com/v/1ee99a.

[5] 严芬,王佳佳,赵金凤,等.DdoS攻击检测综述[J].计算机应用研究,2008,25(4):966-969.
YAN F,WANG J J,ZHAO J F,et al.Survey of detection on DDoS attack [J]. Application Research of Computers, 2008,25(4):966-969.

[6] 张锦平.DDoS攻击检测及响应技术的研究[D].秦皇岛:燕山大学,2012.

[7] 池水明,周苏杭.DDoS攻击防御技术研究[J].信息网络安全,2012,27(5):27-31.
CHI S M, ZHOU S H. Research on defend against DDoS attacks [J]. Netinfo Security, 2012,27(5):27-31.

[8] 梁海军.基于DDoS攻击的服务器拥塞控制研究[J].计算机与现代化,2009,25(3):100-102.
LIANG H J.Research on jammed server control based on DDoS attacking [J]. Computer and Modernization, 2009,25(3):100-102.

[9] 张亚萍,陈得宝,侯俊钦.基于EM的朴素贝叶斯分类算法[J].宿州学院学报,2010,25(11):12-13.
ZHANG Y P, CHEN D B, HOU J Q.Naive bayesian classification based on EM algorithm [J]. Journal of Suzhou College, 2010,25(11):12-13.

[10] 孙中华,蒋斌,贾克斌.基于朴素贝叶斯分类的路面积雪状态检测[J].吉林大学学报(工学版),2013,43(增刊1):380-383.
SUN Z H,JIANG B,JIA K B. Detection of the road snow coverage status based on naive bayesian classifier [J]. Journal of Jilin University (Engineering and Technology Edition), 2013,43(Suppl. 1):380-383.

[11] 盛骤,谢式千,潘承毅.概率论与数理统计[M].第4版.北京:高等教育出版社,2008:17-23.

[12] 王阳,李连发.空间贝叶斯分类器并行化[J].地理与地理信息科学,2013,29(4):47-51.
WANG Y,LI L F. A Parallel bayesian classifier [J]. Geography and Geo-information Science, 2013,29(4):47-51.

[13] 王双成,杜瑞杰,刘颖.连续属性完全贝叶斯分类器的学习与优化[J].计算机学报,2012,35(10):2129-2138.
WANG S C, DU R J, LIU Y. The learning and optimization of full bayes classifiers with continuous attributes [J]. Chinese Journal of Computers, 2012, 35(10):2129-2138.

[14] 王国才.朴素贝叶斯分类器的研究与应用[D].重庆:重庆交通大学,2010.

[15] 吴江霞.正态分布进入统计学的历史演化[D].石家庄:河北师范大学,2008.

[16] 汪新凡,肖满生.基于正态分布区间数的信息不完全的群决策方法[J].控制与决策,2010,25(10):1494-1498.
WANG X F, XIAO M S. Approach of group decision making based on normal distribution interval number with incomplete information [J]. Control and Decision, 2010,25(10):1494-1498.

本文编辑:陈小平