基于信息熵聚类的 DDoS 检测算法①

赵慧明　刘卫国　(中南大学 信息科学与工程学院 湖南 长沙 410083)

摘　要： 采用信息熵进行 DDoS 特征表示，再采用 K-means 算法分析熵值，通过分析正常网络的分布规律，确定 DDoS 攻击检测的阈值，并根据阈值来更新正常行为的特征训练集或做出攻击响应。实验结果显示，这种方法可以快速完成训练与测试工作，能够有效检测 DDoS 攻击。

关键词： 分布式拒绝服务；信息熵；K-means 算法

DDoS Detection Algorithm Based on Cluster of Entropy

ZHAO Hui-Ming, LIU Wei-Guo

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: The entropy is used to represent the feature of DDoS, and the entropy is clustered by K-means algorithm. The threshold of DDoS detection is gotten from analyzing statistical normal network packets, then the normal characteristics training set is updated, and the DDoS is recognized on the basis of threshold. The experiments show that the measure can implement trainings and testing processes rapidly, and it can detect existence of DDoS effectively.

Keywords: distributed denial of service; entropy; K-means algorithm

1　引言

近年来，互联网上不断遭受大规模的 DDoS 攻击，有效地检测和阻止 DDoS 攻击一直以来是构建网络安全的重要组成部分。

DDoS 具有分布式特性以及攻击者伪造源 IP 地址，而且随意改变攻击报文内容，使得 DDoS 攻击特征难以提取，攻击源的位置难以确定，因此检测困难。文献[1]提出了通过监控新的 IP 地址数量来实现 DDoS 检测的方法，但是如果攻击者事先让傀儡机采用欺骗的源地址向被攻击目标发送正常访问数据包，欺骗检测系统将这些 IP 地址存放进正常状态下出现过的 IP 地址数据库，将会出现漏警的问题。文献[2,3]提出了一种追踪 DDoS 攻击源 IP 地址的方法，但是攻击者伪造源地址，难以定位攻击源，而且还需要收集大量报文进行计算，还原出攻击路径，增加系统开销。文献[4,5]提出的算法只能用于检测单一的 SYN FLOOD 攻击，而对于其他的 DDoS 攻击则无法检测，因为新的 DDoS 攻击者采用多种服务攻击程序组合起来，同时使用多种攻击结合对某一 IP 进行攻击。目前 DDoS 攻击方法主要有 TCP SYN flood、UDP flood、ICMP flood，或者将这几种攻击混合起来形成 MIX flood 攻击。

本文首先通过对网络数据包信息提取，对提取的数据进行预处理，并进行熵值计算，然后对预处理的结果实施 K-means 聚类，从而有效地检测出不同类型的 DDoS 攻击。

2　DDoS特征分析

DDoS 攻击时，大量的傀儡机被控制同时发起攻击，而且攻击者会随机伪造攻击数据包源 IP 地址，或者使用的反射 DDoS 攻击方式，因而源 IP 地址更加分散，且数量会剧增；网络数据包集中流入受害机，向提供服务的某些端口发起攻击，所以网络数据包的目的 IP 地址、目的端口地址会相当集中。信息熵能有效反应通信中消息的信息量，还能反映系统不确定程度，可用于检测大规模网络流量 DDoS 攻击。信息熵[6]定

① 收稿时间:2010-03-24;收到修改稿时间:2010-05-06

义如下：

$$H(X)=-\sum_{i=1}^{N}P_i\mathrm{Log}_2P_i$$

其中 X 是信源的状态空间，它共有 N 个状态，即 $X=(X_1, X_2, \cdots, X_N)$。本文 N 为某一时间段出现的不同的 IP 地址或者端口总数，X_i 表示其中一个 IP 地址或者端口，X_i 出现的概率为 P_i，且 $\sum_{i=1}^{N}p_i=1$。

信息熵能有效表现同一属性上对应数据的集中和分散情况。如图 1 和图 2 所示，在 100 秒(s)时加入 DDoS 攻击流，基于目的 IP 和源 IP 的熵值发生了相对应的明显变化，基于目的 IP 熵值在 100 秒时急剧减小，而基于源 IP 熵值在 100 秒时急剧增大。因此信息熵能很好地反映出 DDoS 攻击时的特征变化，可用作 DDoS 的特征表示。

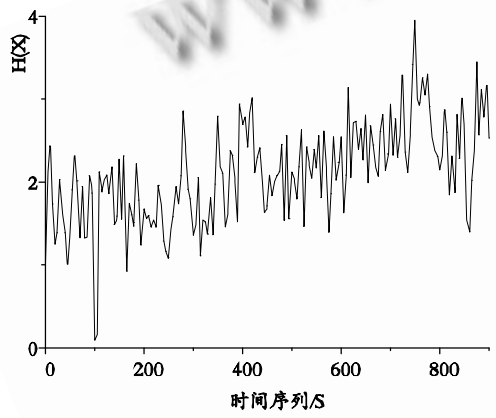

图 1　基于目的 IP 的熵值

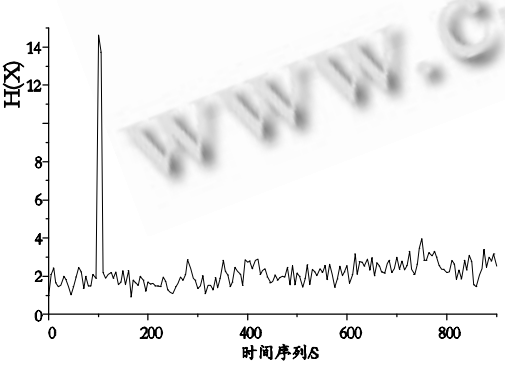

图 2　基于源 IP 的熵值

DDoS 攻击时，网络中存在许多虚假的源 IP 地址，这些数据将无法建立 TCP/IP 协议的 3 次握手，因此无法建立正常的连接。当发生攻击时，网络中不能建立正常连接的数据流会增加。单边连接密度[7](One-Way Connection Density, OWCD)可很好地反映 DDoS 攻击这种特性。OWCD 公式表示如下：

OWCD=∑OWC Packtes/∑IP Packtes×100%

其中 OWC Packtes 指建立正常连接的 IP 地址对数目，IP Packtes 指总的地址数目。

3　DDoS检测算法

本文算法流程如图 3 所示，分为预处理、训练和检测 3 个阶段。预处理阶段通过网络数据包 IP 信息提取，计算数据包的熵值与 OWCD 值，得到 DDoS 攻击特征表示。训练阶段采用无攻击状态下的数据，利用加权欧几里德距离公式对信息熵实施聚类，并确定阈值，建立正常行为特征训练集。检测阶段也要经过聚类过程，然后进行阈值分析，如果数据属于正常范围，则将正常数据归入训练集，并且进行归类，反之则进行攻击响应。

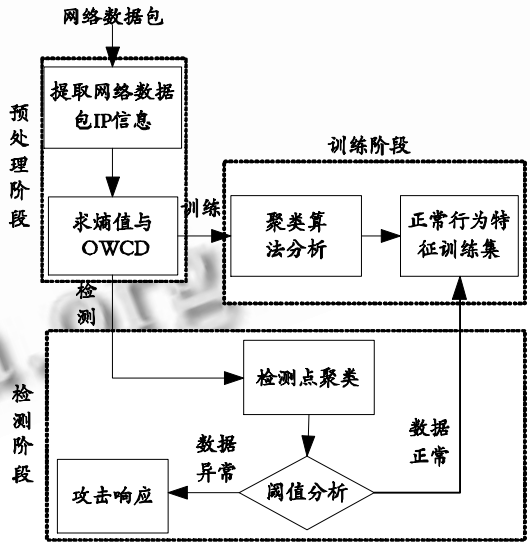

图 3　DDoS 检测算法流程

由于本文不仅要检测出 DDoS 攻击，还要检测出是否属于 TCP SYN flood、UDP flood、ICMP flood 攻击，所以共建立 DDoS、TCP SYN flood、UDP flood 和 ICMP flood 4 个训练集。在训练过程不需要建立 MIX flood 训练集，因为在 DDoS 攻击过程中，TCP、UDP 和 ICMP 数据包的比例是灵活多变的，如果建立 MIX flood 练集，则需要加入不同比例的数据包进行

训练，建立不同的训练集，而且得到的训练集不能检测出其他比例的攻击。本文中如果同时发生 TCP flood、UDP flood、ICMP flood 两种或者两者以上的攻击，则认为是 MIX flood 攻击。

3.1 预处理阶段

通过对网络中提取的数据包进行预处理，将原始的数据流信息计算转化为源 IP 熵 H(SrcIP)、源端口熵 H(SPort)、目的 IP 熵 H(DesIP)、目的端口熵 H(DPort)和 OWCD 等 5 个属性。

3.2 训练阶段

预处理阶段得到大量的数据样本，这些数据样本之间是无序的。聚类方法可将数据集中的数据进行分组，使得同一类的数据相似性尽量大，不同类间的数据相似性尽量小，通常使用加权欧几里德距离来描述 Y_i 和 Y_j 两个数据样本之间的相似程度，计算公式为：

$$dis(Y_i,Y_j)=\sqrt{\sum_{k=1}^{n} w_k(a_{ik}-a_{jk})^2}$$

其中，w_k 为权重系数，$Y_i=(a_{i1}, a_{i2}, \cdots, a_{in})$和 $Y_j=(a_{j1}, a_{j2}, \cdots, a_{jn})$是两个包含 n 个属性度量值的数据记录。本文取 n=5，a_{ik} 和 a_{jk} 分别表示两个在不同时刻得到的数据包的 H(SrcIP)、H(SPort)、H(DesIP)、H(DPort)和 OWCD 值。

K-means[8]算法是数据挖掘中一种普遍采用的方法。每个聚类可通过计算聚类中各维数据的平均值得到它的中心值 Y_{i0}，公式如下：

$$Y_{i0}=(\frac{1}{m}\sum_{i=1}^{m}a_{i1},\frac{1}{m}\sum_{i=1}^{m}a_{i2},\mathbf{L},\frac{1}{m}\sum_{i=1}^{m}a_{in})$$

其中 m 为某个聚类中样本数据的个数。

通过聚类把训练集中的数据样本分为 z 个聚类，具体算法描述如下：

(1) 任意选取 z 个数据作为初始的聚类中心。

(2) 分别计算未分配的数据与各聚类中心的距离，如果与第 t 个聚类的距离最小，则该数据划分到第 t 个聚类，直到不存在单独的样本为止。

(3) 重新计算每个聚类中所有数据的平均值，得到新的聚类中心。

(4) 如果新的聚类中心有变化，则转(2)，重新分配各数据样本。如果新的聚类中心没有变化，则算法收敛，计算完毕。

通过使用 k-means 方法，对网络正常时提取离散的网络数据进行聚类划分，得到数据流的正常行为特征训练集。

同理可分别建立 TCP、UDP、ICMP 流的正常行为特征训练集。训练过程中，不考虑出现某一段时间内没有任何数据包的情况，因为在此过程中不可能发生 DDoS 攻击。

3.3 检测阶段

训练集中的数据都是正常状态下的数据，具有较高的相似性，而在 DDoS 攻击过程中，流量特征突变，检测样本与训练集中的数据相似性降低，通过聚类分析可检测出是否发生了攻击。具体流程如下：

(1) 首先获取并计算数据包的源 IP 地址、目的 IP 地址、源端口和目的端口的熵和 OWCD，得到一个检测样本 Y_i。

(2) 分别计算其它数据样本与 z 个聚类中心的距离，求得最小距离 mindis(Y_i,Y_j)，则该样本属于该簇。

(3) 计算该聚类中各样本同 Yi 的距离，求得最大距离 maxdis，如果 maxdis 超出计算出来的阈值，据此可判定是否发生 DDoS 攻击。通过计算该聚类中任意两两数据样本的的距离，得到的最大距离为该聚类的阈值。如果 maxdis 没有超出设定的阈值范围，则说明没有攻击行为，则对正常行为特征训练集进行修改，将该样本加入训练集，否则进行攻击响应。

在检测过种中，如果某一时间段内没有数据包，就无需检测，这样可提高检测效率，节省资源。

使用 K-means 方法，使得检测过程中大大减少了模型产生和攻击检测所处理的数据量。只需要将需检测的数据与该聚类的数据比较，而不要与整个数据集比较，数据量的减少缩短了进行检测的时间，增加了单位时间内的网络数据处理量。

4 实验及算法分析

本文采用 MIT 林肯实验室于 2000 年提供的攻击场景测试 LLS-DDOS-1.0，正常数据集来自该实验室于 1999 年提供的正常数据集 inside[9]。在无攻击状态下，100 秒内每隔 0.1 秒采集一次数据，并分别计算数据包 TCP，UDP，ICMP 包的源、目的 IP，源、

目的端口的熵值，并且对数据实施 K-means 聚类，这样得到了正常网络状态下 4 个训练模型。然后在正常网络流中加入 DDoS 攻击流，再在无攻击状态下加大网络流量进行检测。

检测率和误报率是决定检测精度的两个重要指标，检测率是指正确检测的数目占实际数目的百分比，误报率是指错误检测的异常数目占检测数目的百分比。本文提出的算法与信息熵算法[6]相比，其检测性能明显提高，如表 1 所示。

表 1 本文算法和普通熵算法比较

	检测率/%	误报率/%
本文算法	94.1	8.6
普通熵算法	91.2	47.5

实验表明两者在检测率方面比较接近，而且都比较高，但在误报率上，后者的算法明显比基于信息熵算法的方法低，前者误报率仅为 8.6%，后者高达 47.5%。这是由于熵算法只是简单考虑某一特征值，进行简单的阈值划分，没有对多个特征值进行综合考虑，导致无法区别突然增大的正常流与攻击流。

为了检验不同类型的 DDoS 攻击检测类型，提取数据集的不同类型的攻击数据包，对某一主机分别实施 TCP flood，UDP flood，ICMP flood 和 MIX flood 攻击，检测过程中将检测数据分别放入不同的模型进行检测。实验结果如表 2 所示，表明本文的检测算法对不同的 DDoS 类型的检测率较高。

表 2 不同类型的 DDoS 攻击检测结果

	检测率/%	误报率/%
TCP SYN flood	92.8	7.1
UDP flood	90.5	8.5
ICMP flood	85.7	9.7
MIX flood	94.1	8.6

5 结束语

本文首先对抓取的数据包信息进行熵值计算，然后利用 K-means 算法对熵值进行聚类分析，再根据阈值做出攻击响应。实验研究表明，本文提出的基于信息熵聚类的 DDoS 检测算法，同普通的熵算法相比，降低了因正常网络数据流突然增大而引起的误报率。同时通过建立不同攻击类型的训练集，能检测不同类型的 DDoS 攻击。因此本文算法能够满足日常网络检测的需要。

参考文献

1 孙知信，李清东. 基于源目的 IP 地址对数据库的防范 DDoS 攻击策略. 软件学报，2007,18(10):2613－2623.

2 张健,陈松乔,戴昭. 一种通用的大规模 DDoS 攻击源追踪方案研究. 小型微型计算机系统，2007,28(3):431－437.

3 周曜,徐长江,徐佳. 基于随机包标记方案的 IP 追踪性能分析. 计算机科学, 2007,34(12):78－81.

4 严芬，王佳佳，殷新春. 一种基于 Hurst 参数的 SYN Flooding 攻击实时检测方法. 计算机科学，2008,35(12):109－113.

5 Yu Ming. A Probabilistic Drop Scheme for Miti- gating SYN Flooding Attacks. 2009 International Conference on Networks Security, Wireless Co- mmunications and Trusted Computing, 2009:732－734.

6 曲炜,朱诗兵.信息论基础及应用.北京:清华大学出版社, 2005:15－25.

7 Xu Tu, He Dake, Zheng Yu. Detecting DDoS Attack Based on One-way Connection Density. Proceedings of 10th IEEE International Conference on Communication Systems, 2006:1－5.

8 Jiavei Han, Micheline Kamber. 数据挖掘概念与技术. 范明,孟小峰译.北京:机械工业出版社, 2004:231－232.

9 http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_irrdes.htm.