面向 IDS 的 DDoS 攻击检测真实性分析

李盼辉[1] 丁伟[2] 任文韬[3] 夏震[4]
（[1,2,3,4] 东南大学 计算机科学与工程学院，南京市 211189）

摘要：论文首先就现有的基于规则匹配的 DDoS 检测方法可能存在的误判进行了讨论。在此基础上，设计了一种从假冒源地址，攻击报文长度，反向散射报文强度以及攻击强度四个方面对每例 IDS 检测出的 DDoS 检测结果进行评价的真实性检验算法。检测结果可以为面向攻击流量的“洗流”操作提供合理的参数设置依据。随后将算法应用于实际工作环境中，并对其在 20 天的运行过程的检测结果进行了分析。分析结果表明了该算法的有效和实用性。

关键词：DDoS 检测，攻击误判,源地址分析，威胁响应
中图分类号　TP393

Analysis of authenticity of DDoS attack detection for IDS

LI Panhui[1] DING Wei[2] REN Wentao[3] XIA Zhen[4]
（[1,2,3,4] School of computer science and engineering, Southeast University，Nanjing 211189）

Abstract: This paper first discusses the possible misjudgment of existing DDoS detection methods based on rule matching. On this basis, this paper designs a authenticity checking algorithm to evaluate the detection of each IDS DDoS detection results from spoofed address, packet length,backscatter message strength and attack strength four aspects. The test results can provide reasonable parameter settings for the "flow filtering" operation for attack traffic. The algorithm is then applied to the actual working environment, and the detection results in the 20 day running process are analyzed. The analysis results show the effectiveness and practicability of the algorithm.

Key Word: DDoS detection, attack misjudgment, source address analysis, threat response

1 引言

分布式拒绝服务攻击(distributed denial of service attack， DDoS)是目前互联网上主流的恶意行为之一。Arbor Networks 在其第 12 届年度全球基础设施安全报告[1]中公布 2016 年 DDoS 攻击强度创下新纪录，单次 DDoS 攻击最高强度超过 800 Gbps,相比 2015 年提高了 60%。而绿盟科技 2016 年第三季度报告[2]表明：第三季度全球总 DDoS 攻击相比上个季度次数增加 40%，其中受攻击最严重的国家是中国。

从 1996 年 DDoS 攻击首次出现开始，相关的研究工作持续了 20 多年。各种面向 DDOS 攻击的检测、过滤和攻击来源追踪等各种防护方法相继提出[3]。“洗流”是目前比较常规的一种防范方法，即对攻击流量进行过滤[4]。这种方法可以在 SDN 流表技术的支持下工作，对攻击流量进行有效“清洗”，以达到对 DDoS 攻击的防护目的。采用“洗流”方法进行 DDoS

攻击防范的前提条件之一就是 DDoS 检测，即攻击能够被准确地检测出来。

目前大部分应用在实际工作环境中的 DDoS 检测算法，都是基于规则匹配设计的。对于规则的定义和选择，工业界与学术界有不同的角度，学术界更注重流量行为的异常，而工业界更注重是否有服务失效的情况出现。但是无论使用哪种标准，都可能出现误报。因为误报，而导致的对非攻击流量的进行“清洗”，会产生严重的后果，是不能被接受的网络流量管理行为。因此对 DDoS 检测结果进行真实性判定是一件有意义的工作。

本论文的研究工作围绕对 DDoS 攻击检测结果的真实性检验这个目标展开，尝试给出一组对检测结果的真实性进行评价的规则，并将其应用到实际网络环境中。

2 相关背景

2.1 相关工作

对 DDoS 检测算法的评价方法大部分是对检测算法的整体准确率进行评价[5]，很少有对于单个检测结果的真实性评价。

评价检测算法的整体准确率： 一般通过搭建网络试验床，构建一个真实的网络环境进行实验，然后比较相关数据来验证其检测结果的真实性。

在实际工作环境中，DDoS 检测算法需要面对大流量的处理压力，而无法对流量的细节信息进行分析。针对每一例检测结果进行的评价方法大都是通过这些细节信息进行的。

孙知信等人[6]针对使用信息熵变化来进行 DDoS 检测时，对正常大流量行为可能产生的误报，提出了一种基于拥塞控制机制的真实性检测方法。他们认为正常的大流量行为应该遵循拥塞控制机制，流速在经过最初的峰值后，会慢慢降低。但使用这种方式的前提是，数据传输使用的协议必须支持拥塞控制机制。

当前，不论是学术界，还是工业界都没有较为有效的针对单个检测结果的真实性评价方法。

2.2 检测实例

尽管当前 IDS 常用的基于规则匹配的检测方式已经能够很好的检测出多种类型的攻击。但是在实际的工作环境中，由于 TCP/IP 灵活的体系结构给应用系统在设计和实现过程带来方便的同时，也使得它们在应用过程中的流量行为不会受到限制，在某些情况下，会与 DDOS 的检测规则匹配，但它们实际上并不是真正的 DDOS 攻击。

以下是两个 SYN Flood 攻击的误报实例。对应 IDS 系统的检测规则是 SYN Flood 攻击检测，即短时间内，被攻击者收到大量的 SYN 报文，致使其资源耗尽，无法提供正常服务。

案例一

因为 IDS 高频率报告到主机 222.*.55.208 遭受到在阈值边缘的 SYN Flood 攻击。为了对其检测的真实性进行判定，使用了流量采集系统对该 IP 的流量进行保存。IDS 报告的图 2-1 所示的攻击同步采集的部分报文如图 2-2 所示。图中数据表明短时间内大量主机在向 222.*.55.208 发起连接请求触发了 IDS 的 SYN Flood 攻击检测规则。但这些主机都与

222.*.55.208 建立了连接并传送了报文。这并不是一起真正的 SYN Flood 攻击。进一步的调查确认，222.*.55.208 当时存在大量的视频资源。大量地址正常的客户机频繁访问 222.*.55.208 获取资源，应用程序设计每个会话只获取一小段数据，因此会出现大量的 TCP 连接。同样，应用程序还会在连接建立失败的情况下会频繁发送 SYN 请求争抢连接资源，导致出现大量 SYN 单包流，最终造成了误报的产生。

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type	avg_pps	max_pps	avg_kbps	max_kbps
222.[redacted]55.208	2016-09-12 18:40:00	2016-09-12 19:59:59	0x06	1124	1238	85	98

图 2-1 222.*.55.208 遭受 SYN Flood 攻击

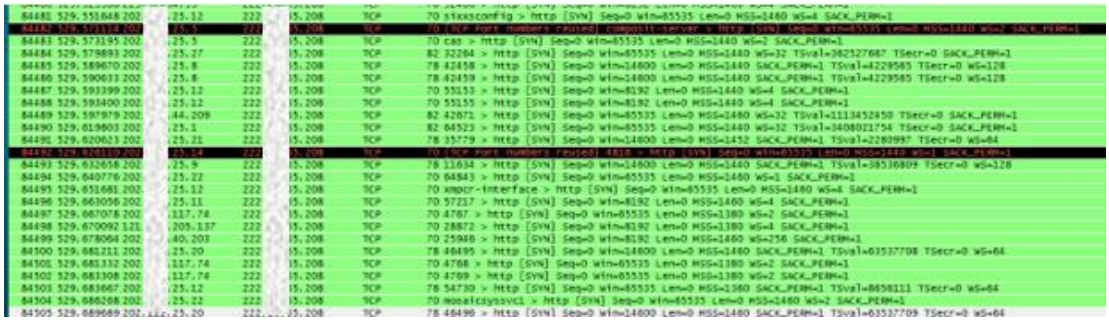

图 2-2 各对端与 222.*.55.208 通讯报文

案例二

图 2-3 和图 2-4 所示的是对 220.*.242.204 和 74.*.204.101 的 SYN Flood 攻击及攻击对端情况。这两次攻击也属于低强度攻击。但是通过对攻击对端的分析，发现攻击对端有明显的假冒源地址行为，因此这两次攻击应该是真实的 DDoS 攻击。

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type
220[redacted].242.204	2017-03-27 13:20:18	2017-03-27 13:20:50	0x06

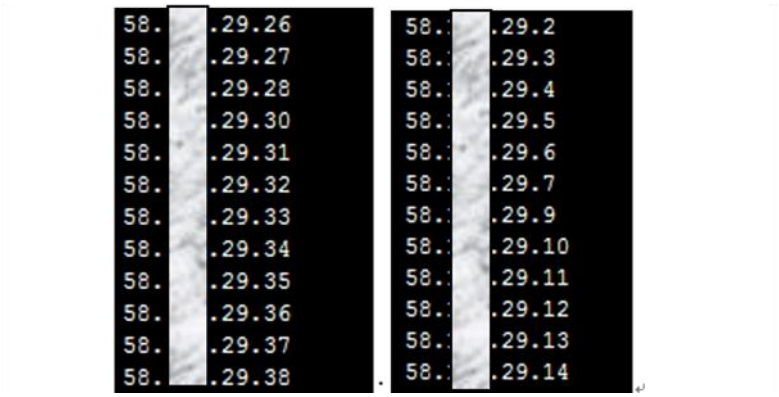

图 2-3 220.*.242.204 遭受 SYN Flood 攻击及攻击对端情况

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type
74. 204.101	2017-03-28 14:35:00	2017-03-28 17:14:59	0x06

42. .62.240	42. .62.224
42. .62.239	42. .62.223
42. .62.238	42. .62.222
42. .62.237	42. .62.220
42. .62.236	42. .62.219
42. .62.235	42. .62.218
42. .62.234	42. .62.217
42. .62.233	42. .62.216
42. .62.231	42. .62.215
42. .62.229	42. .62.213
42. .62.228	42. .62.212
42. .62.227	42. .62.211

图 2-4 74.*.204.101 遭受 SYN Flood 攻击及攻击对端情况

上述两个案例使用的相同的规则和阈值检出，攻击强度也基本相同。对检测结果的分析表明基于规则匹配的检测算法，确实会出现误判的情况，事实上，低强度是近年来最流行的 APT 攻击[7]的典型特征之一，因此简单的阈值调整并不能解决误判的问题。

3 原理和方法

上面的分析表明对 DDoS 检测结果的真实性进行分析是一件有意义的工作。本章尝试提出一种基于对端分析的 DDOS 检测结果真实性检验方法。这里的对端指的是攻击流量的源地址。

3.1 假设条件

真实性检验是基于 IDS 的 DDoS 攻击检测结果进行的，DDoS 检测算法的检测规则与检测结果对真实性检验算法的有效性有直接影响。因此需要首先对检测规则作出如下假设：

假设 IDS 的位置是在网络的边界，其 DDoS 检测算法在检测规则上基于流量特征的统计结果，阈值设置上参考工程中的实际攻击的强度，着重于检测能够造成服务失效的 DDoS 攻击。

此外假设检测系统针对每一例 DDoS 攻击都可以提供如下表 3-1 信息。

表 3-1 DDoS 攻击信息条件

编号	DDoS 攻击信息
1	对端地址
2	攻击起止时间
3	攻击报文的信息
4	被管网络的地址分配信息
5	被管网络的活跃地址信息

3.2 检测思路

通过利用上小节中提出的假设条件，本节将从对端地址分布，攻击报文长度，反向散射报文强度以及攻击强度四个方面对每一例 DDoS 检测结果进行评价。这些思路均是以准确为

最优先设计的，希望在最大程度上减少误判。

思路一：使用假冒源地址的攻击是真实攻击

正常的网络行为中，为了保证通讯的正常进行，双方必然会使用自身真实的地址进行通讯。但是在 DDoS 攻击中，攻击者经常通过假冒源地址达到隐藏身份或者反射放大的目的。因此，如果确定攻击者使用了假冒源地址，则可以确定攻击的真实性。

思路二：SYN 报文长度异常的 SYN Flood 攻击是真实攻击

在三次握手过程中，SYN 报文的长度=IP 头(20bytes)+TCP 头长度(20bytes)=40bytes，少部分情况下，会附带 TCP Option。此外协议规定以太网帧最小长度为 64 字节，所以 SYN 报文的长度一般为 64 字节。正常情况下，SYN 报文不携带数据，但是当前多数 SYN Flood 攻击中，攻击者会在 SYN 报文携带大量数据以同时达到堵塞带宽的效果，从而出现长度远大于 64 字节的 SYN 报文。因此，如果 SYN 报文长度远大于 64 个字节，则可以确定攻击的真实性。

思路三：反向散射报文强度异常的 SYN Flood 是真实攻击

这里的反向散射报文指的是 SYN+ACK 报文。正常通讯中，SYN 与 SYN+ACK 报文呈现一一对应的情况。即使受网络拥塞和重传机制的影响，两者的比值也会在合理范围内。但是当出现网外攻击者假冒网内地址时，就会出现大量 SYN+ACK 的被攻击服务器发出的 SYN+ACK 报文（反向散射报文），导致与被攻击服务器相关的 SYN+ACK 数远大于 SYN 报文数的情况，因此，如果反向散射报文强度异常，则可以确定是真实攻击。这实际上是假冒源地址攻击的一个特殊案例。

思路四：攻击强度较大，对网络带宽造成严重影响的攻击属于真实攻击

对于报文速率与字节速率过高的检测结果，无论是何种类型的攻击、是否出于恶意攻击的目的，从结果上看都严重消耗的带宽资源，影响了正常的服务，达到了使目标服务失效的效果，因此也确定是真实攻击。

3.3 分析测度

本小节基于上小节的思路，设计具体的分析测度，这些测度是形成检测规则。相关讨论按 4 个思路分别进行：

一、对端地址分布

对端地址分布主要用于判定攻击对端是否存在假冒源地址的情况，适用于所有攻击类型的检测结果评价。文献[7]将 DDoS 攻击地址分成三类：

1) 随机假冒地址：攻击者随机生成 32 位 IP 地址作为源地址进行攻击；

2) 子网假冒地址：攻击者假冒自身所在子网的地址，比如，在子网 143.89.124.0/24 中的主机假冒从 143.89.124.0 到 143.89.124.255 的地址进行攻击；

3) 固定地址：攻击者假冒固定的地址列表中的地址进行攻击，通常用于对有特定访问权限的主机发起攻击。

子网假冒地址特征相对明显。2.2 节的案例二中，从对端地址的分布情况可以很明显的看出攻击者使用了子网假冒地址。

随机假冒地址存在一些特殊情况：如图 3-1 所示的攻击，攻击者生成格式为”A.A.A.A”的地址对目标发起了 UDP Flood 攻击，其中还包括了部分私有地址，这种特殊格式的源地址多次出现的攻击是明显的假冒源地址类型的攻击。

图 3-1 “A.A.A.A”格式的随机假冒源地址攻击

除此之外，对于攻击者而言，被管网络内的地址分配情况是未知的。以网外主机遭受攻击为例：如果攻击者使用了网内未被分配的地址发起攻击，那么这些地址一定属于假冒地址。

根据上述分析，假冒源地址的判断主要统计以下内容：

测度 1 攻击对端地址分布

1) 攻击对端地址“A.A.A.A”格式的特殊地址的数量 Sum；
2) 将攻击对端地址按照/Slash 子网划分后的网段数 K；
3) 划分后各子网的统计情况，该子测度由一个三元组构成[网段掩码长度(Slash)，该网段包含攻击对端地址数(Count)，该网段包含攻击对端地址中不活跃地址数(Inactive[9])；

二、.攻击报文平均长度分析

由于 UDP 报文长度没有固定的大小，不适合使用报文平均长度对结果进行验证。该测度只统计 SYN Flood 攻击中 SYN 报文的长度，具体统计内容如测度 2 所示：

测度 2 SYN 报文平均长度

SYN Flood 攻击中 SYN 报文平均长度$Avg_Len = \frac{All_Octets}{All_Packets}$。其中 All_Octets 为 SYN 报文总字节数，All_Packets 为 SYN 报文总报文数。

三、反向散射报文强度分析

根据上一节的分析，反向散射报文强度适用于评价 SYN Flood 攻击结果，统计测度如 3 所示：

测度 3 反向散射报文强度

SYN Flood 攻击中反向散射报文与攻击报文比$Ratio = \frac{All_Reply}{All_Attack}$。其中 All_Reply 为被

攻击主机回复的 SYN+ACK 报文数，All_Attack 为被攻击主机接收的 SYN 报文数。

四、攻击强度分析

DDoS 攻击强度主要分为平均攻击报文速率以及平均攻击字节速率，同样适合所有攻击类型的检测结果评价，具体统计内容如下：

测度 4　攻击流量强度

攻击的平均攻击报文速率Pac = $\frac{All\_Packets}{Duration}$，平均攻击字节速率Byt = $\frac{All\_Bytes}{Duration}$。其中 Duration 表示攻击时长，All_packets 为总攻击报文数，All_Bytes 为总攻击字节数。

3.4 检测规则

基于上一节的原理分析，设计具体的检测如下所示：

表 3-2 DDoS 检测结果判定规则

判定规则	检测规则	对应测度	判断思路
1	$Sum \geq n1$	1	1
2	$\sum_1^k Inactive_i > \text{n2}$		
3	$P_i = \frac{Count_i}{2^{32-Slash}}$ ， $\text{P} = \frac{\sum_1^K Count_i}{K*2^{32-Slash}}$ $P \geq \text{n3} \,\|\|\, \sum_i^k bool(P_i \geq \text{n3}) \geq \text{n4}$		
4	$Avg\_Len > n5$	2	2
5	$Ratio > n6$	3	3
6	$Pac \geq \text{n7} \,\|\|\, Byt \geq \text{n8}$	4	4

表 3-2 中，n1-n8 为检测规则的阈值参数，需要根据实际工作环境进行设置。

4 检测算法

基于上述检测规则，我们设计实现了检测算法，并将其在基于 NBOS 平台部署在了 CERNET 南京主节点边界。NBOS（Network Behavior Observation System）是一个在 211 计划支持下自行开发的基于流记录的精细化的网管系统[10]，具有 DDOS 检测功能，本文上面所有的检测实例均由该系统提供。NBOS 也可以同时提供所有检测规则所需的数据。本节将详细介绍算法的实现细节和运行结果。

4.1 算法的实现和规则参数

在算法的实现过程中，根据 NBOS 平台的工作环境，设置了检测规则的阈值参数,具体参数取值和参数说明如表 4-1 所示:

表 4-1 检测规则的参数取值及说明

参数	参数取值	参数说明
n1	5	对端地址中形如“A.A.A.A”的特殊地址数过多的阈值
n2	5	对端地址中非活跃地址数过多的阈值

n3	80%	针对一个子网，有大多数子网地址参与攻击的阈值
n4	3	大多数子网地址参与攻击的子网数过多的阈值
n5	300	SYN 报文长度过长的阈值
n6	10	反向散射报文与攻击报文比值过大的阈值
n7	15000PPS	平均攻击报文速率过大的阈值
n8	100MBPS	平均攻击字节速率过大的阈值

对于检测结果，本文采用 bool 四元组存储 DDoS 攻击的评价结果，从高到低分别表示[Address(假冒源地址)，Length(SYN 报文长度异常)，Back (反向散射报文强度异常)，Strength(攻击强度异常)]，对应上述的四个测度。

如果对某次攻击的四元组检测结果中存在某项为 1，则认为该攻击是真实的 DDoS 攻击，即该 DDoS 攻击是由攻击者出于恶意目的发起的 DDoS 攻击行为；如果全部为 0，则表示所有的四个测度的检测结果均呈阴性，此时将对应的检测结果称为为可疑流量行为，可疑流量行为可能属于真实的 DDoS 攻击，也可能是由于网络阻塞等原因导致的流量异常。

根据上述的参数取值和检测结果的存储方式，可得检测结果及对应的判断逻辑，如表 4-2 所示。

表 4-2 检测结果及其判断逻辑

测度	判断逻辑
Address	$P \geq 80\% \,\|\|\, \sum_{i}^{k} bool(P_i \geq 80\%) \geq 3 \|\| Sum > 5 \|\| \sum_{1}^{k} Inactive_i > 5$
Length	bool$(AVG_Len > 300)$
Back	bool$(Ratio > 10)$
Strength	bool$(Pac \geq 15000\text{PPS} \,\|\|\, Byt \geq 100\text{MBPS})$

4.2 实验结果

选择的实验时间是 2017 年 3 月 9 日至 29 日，共 20 天。运行结果如表 4-3 所示。这一段时间 NBOS 共检测出 10925 次攻击，其中 SYN Flood 攻击 10881 次，UDP Flood 攻击 44 次。按照上述规则对检测结果进行检验，结果表明共有 7432 次攻击属于真实 DDoS 攻击，3493 次攻击属于可疑流量行为。

表 4-3 DDoS 攻击检测结果统计

	SYN Flood	UDP Flood	总计
真实 DDoS 攻击（次）	7399	33	7432
可疑流量行为（次）	3482	11	3493
总计	10881	44	10925

实际上，2.2 节中的两个案例是从本次实验的结果中选出的。对这两个案例中的三个攻击的真实性分析结果如图 4-1~图 4-3 所示。图 4-1 中，Reality=0：四元组[Address, Length, Back, Strength]=[0,0,0,0]，四个评价测度均没有出现异常，属于可疑的流量行为；图 4-2 和 4-3 中，Reality=8：四元组[Address, Length, Back, Strength]=[1,0,0,0]，攻击强度较低，但是存在假冒源地址的情况，因此属于真实的 DDoS 攻击。判断结果与 2.2 节中的分析结果一致。

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type	reality
222.[redacted]55.208	2016-09-12 18:40:00	2016-09-12 19:59:59	0x06	0

图 4-1 222.*.55.208 检测结果评价

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type	reality
220[redacted].242.204	2017-03-27 13:20:18	2017-03-27 13:20:50	0x06	8

图 4-2 220.*.242.204 检测结果的真实性检验结果

inet_ntoa(ip)	from_unixtime(start_time)	from_unixtime(end_time)	ddos_type	reality
74.[redacted]204.101	2017-03-28 14:35:00	2017-03-28 17:14:59	0x06	8

图 4-3 74.*.204.101 检测结果的真实性检验结果

5 总结与展望

论文讨论了对单个 DDOS 检测结果进行准确性评价的问题。算法给出了 4 个具体的检测思路，它们是在我们对 NBOS 大量的 DDOS 攻击检测结果的分析的基础上给出的。这个工作最重要的价值在于它们可以支持网络威胁响应系统对攻击流量进行更加精准的“清洗”，因此我们在设计这些规则时，主要考虑的是准确性，对整体的检测结果漏判的可能性还是很大的。今后的工作将围绕方法的科学原理进行深层次的研究，在保证研究工作保持可操作等实用属性的同时，使其在规范和严谨等科学属性方面有进一步的提高。

6 参考文献

[1] Arbor Networks’ 12th Annual Worldwide Infrastructure Security Report https://finance.yahoo.com/news/arbor-networks-12th-annual-worldwide-140000818.html

[2] 2016Q3 绿盟科技 DDoS 态势报告 http://www.nsfocus.com.cn/content/details_62_2257.html

[3] 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.

[4] Kalliola, Aapo, et al. Flooding DDoS mitigation and traffic management with software defined networking. Cloud Networking (CloudNet), 2015 IEEE 4th International Conference on. IEEE, 2015.

[5] 黄亮, 冯登国, 连一峰,等. 一种基于多属性决策的 DDoS 防护措施遴选方法[J]. 软件学报, 2015, 26(7):1742-1756.

[6] 孙知信, 姜举良, 焦琳. DDOS 攻击检测和防御模型[J]. 软件学报, 2007, 18(9): 2245-2258.

[7] 付钰, 李洪成, 吴晓平,等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11):1-14.

[8] Chen, Wei, and Dit-Yan Yeung. "Defending against TCP SYN flooding attacks under different types of IP spoofing." Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on. IEEE, 2006.

[9] 张凌峰. 基于流记录的热点主机非授权流量识别[D]. 东南大学, 2016.

[10] 张维维，龚俭，丁伟等. NBOS：一个基于流技术的精细化网管系统[C]. 中国教育和科研计算机网 cernet 学术年会，2012.