基于区块链的防护物联网设备 DDoS 攻击方法研究*

周启惠[1,2]，邓祖强[4,5]，邹萍[3]，周静[4,5]，王秋生[4,5]，李艳东[3]，姜海森[3]，王雅哲[1,2]，陈亚[1,2]

[1]中国科学院信息工程研究所 信息安全国家重点实验室，北京 中国 100093

[2]中国科学院大学 网络空间安全学院，北京 中国 100049

[3]北京航天智造科技发展有限公司，北京 中国 100039

[4]南瑞集团公司（国家电网电力研究院），南京 中国 211106

[5]北京南瑞电研华源电力技术有限公司，北京 中国 102200

通讯作者：邓祖强, E-mail: baqiuxiao@163.com

摘 要:

随着物联网设备的普及使用，利用物联网设备发起的 DDoS 攻击愈演愈烈，针对此类问题，本文提出了一种基于边缘计算和区块链的检测防御架构，在边缘节点依据物联网设备特有的业务功能特点，实现初步的疑似 DDoS 异常检测，并利用区块链实现初步检测结果的共享分析得出 DDoS 预警，最终基于奖励机制在边缘节点处对物联网设备发出的 DDoS 连接过滤。本方案的检测和防御分布式部署在攻击源端，可以避免引流以及流量清洗造成的高额成本和网络阻塞，并且可以在检测到 DDoS 发生之初就在源头进行持续过滤阻止攻击流量的上涨。

关键词: 区块链，边缘计算，物联网设备，DDoS，共享分析

Research on DDoS Defense Method of Internet of Things Devices Based on Blockchain

ZHOU Qihui [1,2], Deng Zuqiang [4,5], ZOU Ping[3], ZHOU Jing[4,5], WANG Qiusheng[4,5], LI Yandong[3], JIANG Haisen[3], WANG Yazhe[1,2], CHEN Ya [1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

[3] Beijing Aerospace Smart Manufacturing Technology Development Co., Ltd, Beijing 100039, China

[4] NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China

[5] Beijing NARI Dianyan Huayuan Electric Power Technology Co. Ltd, Beijing 102200, China

Abstract:

With the popularity of the Internet of Things (IoT) devices, DDoS attacks initiated by IoT devices have become increasingly fierce. To solve such problems, this paper proposes a detection and defense architecture based on edge computing and blockchain. According to the unique business function characteristics of IoT devices, the initial suspected DDoS anomaly detection is implemented at the edge nodes. Then the DDoS warning is obtained by sharing and analyzing the preliminary results with the blockchain. Finally, the DDoS connection is filtered at the edge nodes based on the reward mechanism. The detection and defense is deployed at the source distributely, which can avoid the high cost and network congestion caused by traffic extraction and cleaning, and can prevent the increasement of total DDoS traffic by filtering the traffic continuously at the source when the DDoS is detected.

Key words: Blockchain, Edge Computing, IoT Devices, DDoS, Share & Analysis

* 国家重点研发计划（2018YFB1004000）

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

1 引言

现有物联网智能设备大都侧重于功能实现，传统设备厂商在系统设计上普遍忽略安全问题。因此，黑客可以轻易利用设备安全漏洞，使其成为传统网络攻击的新工具，如利用 Mirai、Aidra 等恶意代码感染智能设备并发动 DDoS 造成目标拒绝服务和相关服务下线[1]等严重后果。针对这类 DDoS 攻击，检测防御办法一般是在被攻击目标处部署，但高的数据包到达速率以及连接上下文的缺失，使得目标处的部署方案只能做有限的统计分析和数据包处理。另外，部署在目标处的防御方案在检测到 DDoS 后，由于无法立即区分正常流量与恶意流量，需要将所有的流量引流到其他网段进行流量清洗，在引流的过程中容易造成网络的堵塞。

为了克服目标处检测 DDoS 的弊端，考虑在源头处实施检测防御方案，即在源头处对流量进行检测并过滤恶意流量。首先，从 DDoS 发起的源头处进行检测，连接数较少，并且可以结合连接上下文进行精确的数据包处理分析；另外，从源头处进行检测防御，可以在源头处将恶意流量进行过滤，避免引流造成网络大面积的堵塞。虽然源端检测防御有诸多优势，但针对 DDoS 的源端检测方案很少，主要原因是以往的 DDoS 主要以 PC 作为肉鸡，而 PC 端的流量比较复杂，从源端区分正常流量与恶意 DDoS 流量是很困难的，而物联网设备由于其功能的专一性导致其流量特征的专一性，使得源端检测物联网设备的 DDoS 流量成为可能。被 DDoS 攻击利用的物联网设备包含智能摄像机、DVR、电视机顶盒等在内的众多设备，为了对这些设备的流量进行时效性高的检测，利用边缘计算的思想，由靠近物联网设备的边缘节点设备对其下辖的物联网设备进行流量的异常检测，检测结果可分为两类，一类为正常连接，另一类为疑似 DDoS 异常连接，由于 DDoS 攻击涉及成千上万个设备，单个边缘节点提交的疑似 DDoS 异常连接需要进行整合分析，即需要实现众多边缘节点提交的疑似异常结果的整合，基于整合后的大批量疑似异常连接进行分析实现 DDoS 预警，从而进一步确认 DDoS 异常连接并触发源端的过滤机制。

为实现上述方案，我们需要解决几个关键问题，包括如何在边缘节点对物联网设备进行异常连接检测，在源端部署检测方案，由于攻击流量很小容易被漏检，另外，从源端的视角看，异常 DDoS 流量与普通流量很相似容易误报，所以如何针对物联网设备在源端进行 DDoS 异常检测是有难度的。其次，如何实现疑似 DDoS 异常检测结果的整合分析，传统的云端汇总分析方案存在单点攻击的风险，因此，考虑采用去中心化的边缘节点数据自治共享分析方案，但现有的分布式方案以及一致性算法都无法同时保证数据共享过程中，节点存储数据的一致性，节点数据记录的不可篡改性以及提交数据节点的匿名性。最后，我们需要解决如何保证源端部署检测防御方案的合规性，被 DDoS 作为肉鸡的设备多属于私人家庭或部门，所以对其采取的干预措施，如提交设备的异常流量情况及直接在源头处的过滤，容易遭到用户的抵触，如何保障方案的合规性是个问题。针对以上问题，我们的方案分别提出了解决办法，首先，针对边缘节点对物联网设备的 DDoS 异常检测，我们充分调研分析了现有物联网设备自身的流量特点，然后综合分析了 DDoS 流量特点，利用协议特征匹配以及聚类分析算法对物联网设备的流量进行疑似 DDoS 检测；针对疑似 DDoS 异常检测结果的整合分析，我们用区块链实现节点间安全可信的数据共享分析，建立包含众多边缘节点的区块链架构，区块链作为一种新型的分布式架构可同时满足问题 2 中提到的共享要求；针对如何保证源端部署检测防御方案的合规性，我们引入了经济学因素，通过设立奖励机制，让用户能接受对物联网设备采取的措施。即建立一套从 DDoS 攻击受害者到异常结果提交者之间的奖励机制。

综上，本文的工作和贡献如下：

1. 提出了一种针对利用物联网设备发起 DDoS 攻击的检测防御架构，在攻击源头处部署检测防御方法，并利用区块链实现检测结果的共享分析

2. 依据物联网设备特有的业务功能特点，设计了一种源端处对物联网设备进行疑似 DDoS 流量检测的算法，可快速有效识别物联网设备发出的疑似 DDoS 连接

3. 设计基于区块链的奖励机制，以经济学激励手段保证方案的合规性和可行性

本文的组织结构如下：第 2 节描述相关背景技术；第 3 节详细介绍基于区块链防护物联网设备 DDoS 攻击方法的设计实现；第 4 节是方法的测评分析包括仿真实验验证及综合对比分析；第 5 节介绍相关工作；第

6 节总结全文。

2 背景技术

2.1 边缘计算及边缘节点

边缘计算是在网络边缘执行计算的一种新型计算模型[2]，其目的是利用边缘设备已具有的计算能力，将部分计算任务从云中心迁移到边缘设备端执行，从而降低云计算中心的计算负载。边缘节点的概念来自于边缘计算，边缘节点更接近于用户终端装置[3]，可加快数据的处理与传送速度减少延迟。

2.2 区块链及智能合约

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本[4]。智能合约是区块链的核心构成要素，为静态的底层区块链数据赋予了灵活可编程的机制和算法[5]，将智能合约以数字化形式写入区块链中，保障存储、读取、执行整个过程透明、可跟踪以及不可篡改[4]。

3 基于区块链防护物联网设备 DDoS 攻击方法

3.1 总体介绍

方案整体架构如图 1 所示，众多边缘节点组成区块链网络，边缘节点对其下辖的物联网设备进行异常初步检测，目标为物联网设备发起的疑似 DDoS 异常连接。然后边缘节点将初步检测结果提交到区块链上，实现疑似 DDoS 异常连接的共享。基于共享后的疑似异常连接集合，边缘节点通过执行智能合约中的分析代码，分析出针对某目标 IP 的 DDoS 预警。目标 IP 确认预警，发送奖励给对应的边缘节点，收到奖励后边缘节点基于本地新增的 DDoS 预警，触发过滤机制对物联网设备发起的 DDoS 连接进行过滤。在引言中，我们提到了要实现上述方案需要解决的三个关键问题以及对应的解决方法，下面进行详细阐述。

问题一：边缘节点处针对物联网设备进行 DDoS 异常检测，

我们的检测重点是物联网设备发生的 DDoS 异常，通过对常见 DDoS 的流量特征进行分析，我们将 DDoS 异常流量归为两大类：

一类可以直接利用协议特征来判定，如 SYN FLOOD，可以检测物联网设备有没有完成基于三次握手的 TCP 连接初始化，未完成三次握手的连接，有很大可能是 DDoS 异常流量，由于物联网设备的 TCP 连接数相对较少，为在源端进行三次握手的检测提供了便利条件。

另一大类是没有明显协议特征区分的，如 UDP FLOOD，检测的难度正是由这类攻击导致的，被控制的物联网设备向目标受害者发出的 UDP 连接与普通的 UDP 连接在协议特征上没有任何区别，无法直接判定。为了检测这类异常，我们的方案充分利用了物联网设备的特性，一般来说，物联网设备业务功能单一且固定，因此，其联网特征也是有规律可归纳的，我们实际测试了多个物联网设备正常使用的流量，印证了上述结论。通过对历史正常 UDP 数据包的内容进行聚类分析，得出具有特征的几类簇，实时捕获的 UDP 流量与这几类簇的聚类中心进行相似度匹配，据此判断异常。

问题二：如何实现初步检测得到的疑似 DDoS 异常连接的整合分析

传统的边缘计算方案中，数据的整合分析仍借助于云端，即边缘节点将初步检测结果汇总到云端。云端作为所有信息的汇总分析中心，若出现宕机则整个方案失效。在现有的架构下无法解决上述单点攻击问题，故考虑不借助云端，由边缘节点实现初步检测结果的共享分析。由于节点之间互不信任并且的确有存在恶意节点的可能，因此要实现节点间安全可信的共享分析，需要保证以下几点：

- 一致性。存在恶意节点时，各节点仍能正确记录其它节点提交的数据，达成各节点存储数据的一致。
- 不可篡改性。已经被各节点认可的记录，不可以被篡改。

➢ 匿名性。节点不希望攻击者依据提交的信息推测节点的行为活动，应保证提交数据节点的匿名性。

传统的分布式方案以及一致性算法都无法同时满足上述要求。本文基于区块链实现节点间安全可信的数据共享分析，区块链作为一种新型的分布式架构可同时满足上述要求。首先区块链的各节点通过一致性算法达到一致性的需求；其次，区块链以区块来存储节点的行为日志，区块间形成链式结构从而实现不可篡改性；最后，区块链可以综合利用密码学相关知识，如在每一次提交结果时都使用不同的证书实现匿名性。因此，将所有的边缘节点组成区块链网络，并编写运行在区块链上的智能合约，实现边缘节点自治的数据共享分析。

问题三：如何保证源端部署检测防御方案的合规性

我们引入了经济学的因素，通过设立奖励机制，让用户能接受对其物联网设备采取的措施。即建立一套从 DDoS 攻击受害者到异常结果提交者间的奖励机制，DDoS 攻击受害者因为收到了 DDoS 预警，可以避免损失所以提供奖励，而跟这次预警相对应的异常结果提交者会收到奖励。双方都要保证奖励过程的公开透明可验证，这可借助区块链的智能合约机制实现，把奖励规则编写在智能合约中，从而保证整个过程对所有节点都是公开透明的，奖励分发的过程可以依据奖励规则被验证。

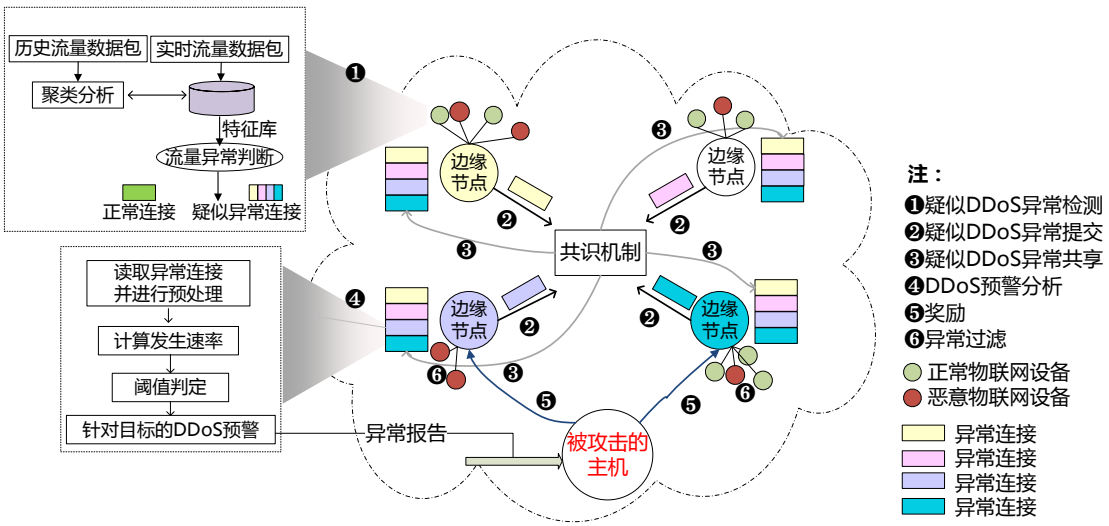

Fig.1 Architecture

图 1 方案整体架构图

3.2 设计与实现

3.2.1 疑似 DDoS 异常初步检测

边缘节点疑似 DDoS 异常初步检测是指在边缘节点对物联网设备发起的连接进行初步检测，得到疑似 DDoS 异常连接。物联网设备对外的流量即联网特征具有特定规律，这有助于设计针对物联网设备的 DDoS 异常检测方案。因此，本文首先基于实验结果分析物联网设备的联网特征，然后基于上述特征阐述疑似 DDoS 异常检测方案的设计。

1）物联网设备联网特征

物联网设备一般都具有专有的业务功能，因此其流量不同于 PC 端复杂多变，从物联网设备的流量中可归纳出特定规律。为印证上述结论，我们实际测试了 8 类共 30 个物联网设备的对外流量，设备列表如表 1 所示，按照正常使用习惯实际使用上述所有设备，并利用 WireShark 抓包工具捕获设备的流量。

表 1 物联网设备测试

名称	数量	品牌	功能
智能摄像头	5	罗技、小蚁	能够远程实时监控、安全检查等

DVR	4	海康威视	能够对图像语音等进行长时间录像、录音、远程监视及控制等
扫地机器人	4	石头、海尔	能够自动在房间内完成地板清理工作
智能音箱	3	小雅	实现语音上网，能够听歌、了解天气、控制智能家居设备等
智能机器人	4	科大讯飞、洛奇	通过语音交互，进行教育教学、人机聊天、视频通话和智能家电控制等
无人机	3	大疆	主要用于航拍
智能手环	5	华为、小米	心率监测、计步追踪、有氧锻炼、睡眠监测等
空气盒子	2	海尔	主要用于室内空气检测等

通过对捕获到的流量数据包进行分析，得出如下有关物联网设备的流量特征：

- 物联网设备由于业务单一，每个设备都有其独特的流量特征。如摄像机，除少量的 TCP 连接（信息认证）外，大部分是 UDP 连接（传送视频数据）；如智能机器人以及智能音箱，其流量绝大部分是 TCP 连接；
- 连接涉及到的外网 IP 较少，一般不超过 10 个；
- 不同的 TCP 连接总数较少，一般不超过 10 条；
- 所使用的的协议大部分是 TCP、UDP，掺杂少量的 ICMP 以及应用层协议；
- 基于数据包中传输的业务数据内容，可归纳出的数据特征集合的大小是确定的；

2）基于物联网设备联网特征的物联网设备疑似 DDoS 异常检测

边缘节点处针对物联网设备进行疑似 DDoS 异常检测主要包括以下三个步骤：

步骤 1：边缘节点利用 Wireshark 工具捕获物联网设备的对外流量；

步骤 2：对捕获流量中的每条连接进行分析，判断是否具有包括 TCP 三次握手未完成、伪造源 IP 在内的明显 DDoS 攻击特征；若具有明显攻击特征，则当前连接为疑似 DDoS 异常，否则进行下一步分析；

步骤 3：假定边缘节点已具有每个物联网设备正常运转三天的全部流量，对历史流量根据协议类型，利用聚类算法对数据包内容进行聚类分析，得出具有特征的类簇，形成如下的协议--特征簇：＜TCP，{簇 1，簇 2，簇 3...}＞、＜UDP，{簇 1，簇 2，簇 3...}＞、＜HTTP，{簇 1，簇 2，簇 3...}＞，基于上述基础，首先判断实时捕获流量中连接的协议类型，根据连接的协议类型匹配到上述得出的协议--特征簇，用连接的数据包内容与特征簇进行相似度匹配，若匹配程度低于设定的阈值，则当前连接为疑似 DDoS 异常连接，否则当前连接为正常连接。

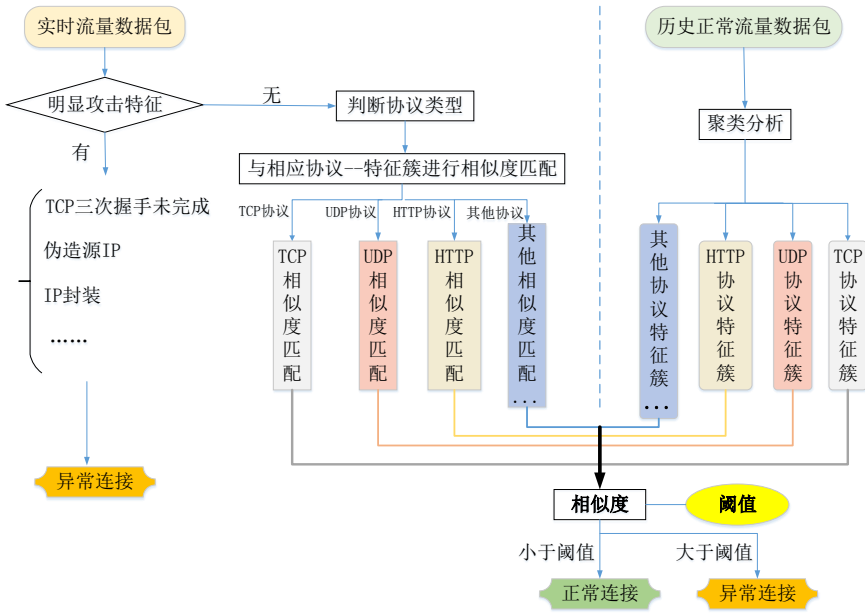

Fig.2　Suspected DDoS Anomaly Detection Flow chart

图 2　疑似 DDoS 异常检测流程图

3.2.2 **疑似 DDoS 异常共享**

上一步边缘节点初步检测得到的只是疑似 DDoS 异常连接，为进一步确认需要将边缘节点的初步检测结果进行整合分析，而整合分析的前提是边缘节点间疑似 DDoS 异常的共享，我们的方案利用区块链实现共享，建立由众多边缘节点组成的区块链，通过调用运行在区块链上的智能合约，并基于区块链共识机制实现边缘节点间初步检测结果的共享，使得各边缘节点存储相同的共享后疑似 DDoS 异常连接数据集合。

在智能合约中定义疑似 DDoS 异常连接数据集合 R_{Conn}，对 R_{Conn} 定义查询、添加等方法；边缘节点调用合约中 R_{Conn} 的添加方法发起添加请求，并对请求进行数字签名，发起的添加请求广播到全网；其他边缘节点收到广播后，对添加请求进行验证，如验证请求提交者的数字签名以及添加请求的数据格式等。若验证通过，则节点更新自己本地的 R_{Conn}，将验证通过的疑似 DDoS 异常连接信息添加到本地存储的 R_{Conn}，实现边缘节点间初步检测得到的疑似 DDoS 异常连接的共享；若验证不通过，则不更新自己本地的 R_{Conn}；各边缘节点按此进行集合的更新，使得每个边缘节点都存储一份相同的共享后疑似 DDoS 异常连接数据集合。

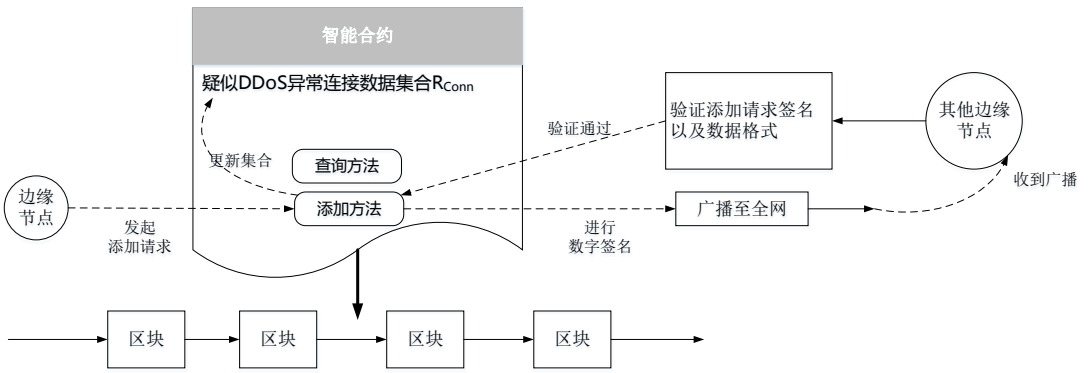

Fig.3　Suspected DDoS Anomaly Share

图 3　疑似 DDoS 异常共享

3.2.3 **DDoS 预警分析**

边缘节点对共享后的 R_{Conn} 调用智能合约进行分析得出 DDoS 预警信息，并将 DDoS 预警信息广播到其他边缘节点，其他边缘节点通过共识实现 DDoS 预警信息的本地存储，基于共享后的 R_{Conn} 进行 DDoS 预警分析由以下两个步骤实现：

步骤 1：在智能合约中对 R_{Conn} 定义分析方法，然后定义 DDoS 预警数据集合 R_{DDoS}，对该数据集合定义查询、添加等方法，边缘节点通过调用 R_{Conn} 的分析方法得出 DDoS 预警信息，如针对某目标 IP 的 DDoS 预警：<目标 IP，异常连接 1，异常连接 2，异常连接 3，…>，并对 DDoS 预警信息进行数字签名，广播到全网；

其中智能合约中 R_{Conn} 的分析方法具体实施如下：

- 读取边缘节点存储的 R_{Conn} 并对其进行相应的预处理操作；
- 计算经过预处理后的 R_{Conn} 中针对某目标 IP 每秒钟发生疑似 DDoS 异常连接的次数，即发生速率；
- 如果发生速率超过阈值，则判断为发生针对某目标 IP 的 DDoS 攻击，生成一条新的 DDoS 预警数据；

步骤 2：新生成的 DDoS 预警数据被广播到全网，其他边缘节点收到广播后，对步骤 1 中的 DDoS 预警进行验证，首先验证提交 DDoS 预警的边缘节点的数字签名；其次签名验证通过后，验证 DDoS 预警数据的真实性，即模拟执行智能合约中 R_{Conn} 的分析方法，判断与收到的 DDoS 预警数据是否一致；若数字签名和 DDoS 预警数据的真实性二者皆验证通过，则将该条 DDoS 预警数据添加至本地的 DDoS 预警数据集合 R_{DDoS}，

实现 R_{DDoS} 的本地更新；若验证不通过，则不添加至本地的 R_{DDoS}。

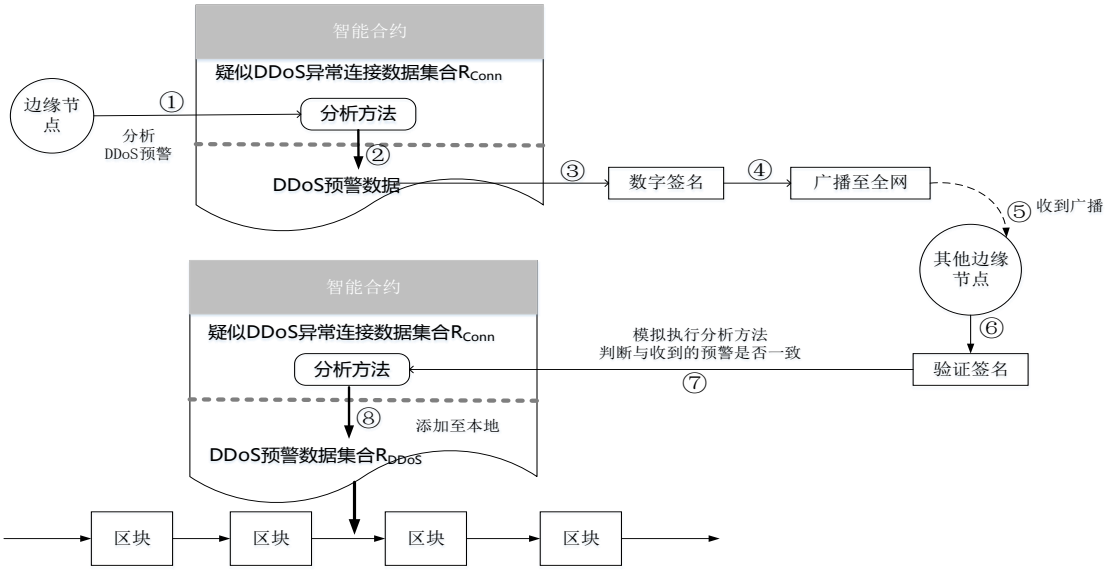

Fig.4　DDoS Warning Analysis

图 4　DDoS 预警分析

3.2.4　基于奖励机制的异常连接过滤

边缘节点异常连接过滤是指基于本地新增加的 DDoS 预警信息，边缘节点在收到 DDoS 攻击受害者发布的奖励后，触发过滤机制对物联网设备发起的 DDoS 连接进行过滤。

奖励机制采用积分形式实现，在智能合约中定义积分的转移规则，DDoS 攻击受害者在确认针对自身的 DDoS 预警后，会通过调用智能合约实现奖励的发放，即转移一定量的积分给提交有用异常连接信息的边缘节点。边缘节点在收到奖励后，首先查询 R_{DDoS}，得到 DDoS 预警<目标 IP，异常连接 1，异常连接 2，异常连接 3，…>中的异常连接标识，然后查询 R_{Conn}，得到异常连接的详细信息，从而定位发出异常连接的物联网设备，对涉及的恶意物联网设备的异常连接进行过滤。

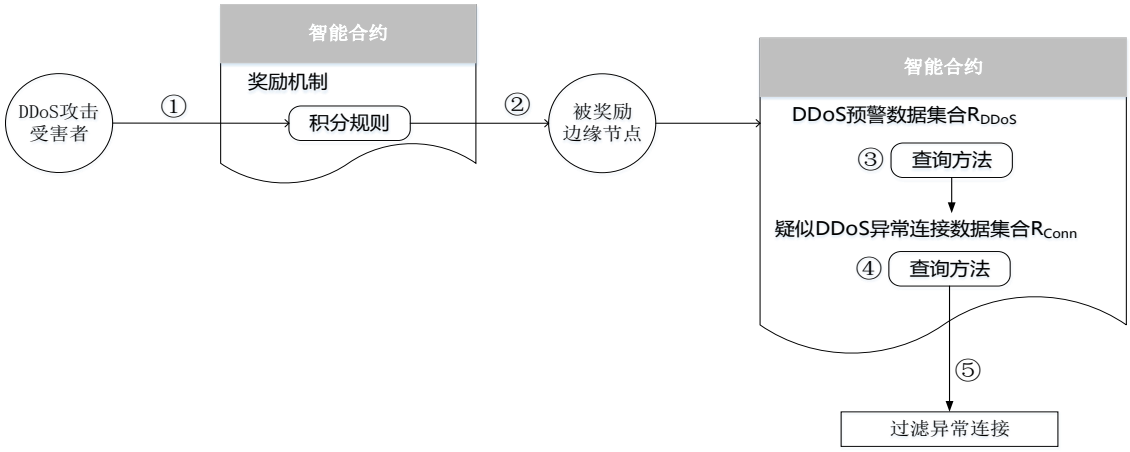

Fig.5　Abnormal Connection Filtering based on Reward Mechanism

图 5　基于奖励机制的异常连接过滤

4 测评分析

4.1 仿真实验验证

我们对本文提出的基于区块链的防护物联网设备DDoS攻击方法进行了仿真验证，搭建了15个边缘节点，每个边缘节点下辖 3~4 个物联网设备，物联网设备中有一半的设备被提前植入了 Mirai 恶意代码，边缘节点采用 ubuntu 16.04 系统，并将所有边缘节点组成区块链网络，将所需的智能合约部署到区块链网络中。另外，指定一台主机作为 DDoS 攻击的目标，将这台主机的 IP 作为参数指定给物联网设备中的 Miria 恶意代码，由于本实验中涉及的物联网设备数量较少，所以基于汇总后的疑似 DDoS 异常进行分析时的阈值，我们设置了相对较低的数值。最终的实验结果为，我们的方法可以成功检测到针对目标主机的这次 DDoS 攻击，且能定位到发起 DDoS 攻击的物联网设备，并且能过滤掉被感染物联网设备发往目标主机的连接，阻止 DDoS 的继续。

4.2 综合对比分析

我们将本方案与现有流行的抗 DDoS 方案分别从防御类型、防御能力、防御成本等方面进行了对比，结果如表 2 所示。从防御类型上来说，我们的方案与现有抗 DDoS 方案类似，都能防御现有各类 DDoS 攻击；但从防御能力上来说，与现有的抗 DDoS 方案采用的目标端防御不同，我们的方案由于采用的是源端的分布式的监测过滤，可以起到“防微杜渐”的效果，在检测到 DDoS 攻击发生时，就在攻击发起的源端进行持续过滤，阻断后续的恶意连接使恶意总流量不再上涨；从防御成本来说，现有的抗 DDoS 方案需要额外的流量引流通路以及流量清洗设备，因此成本较高，我们的方案不需要上述通路设备，成本相对较低。

但是，我们的方案也存在问题，需要后续进行改进和优化。首先，方案的大规模部署取决于现有的边缘节点设备如路由器，对区块链的支持情况，目前只有性能较好的路由器才可以支持区块链的运行，因此，想要实现方案的大规模部署，需要对区块链本身进行优化，降低其对资源的高要求，从而可以涵盖更多性能一般的边缘设备。其次，是方案的大规模部署时的性能问题，由于实验资源受限，我们进行的是小规模的仿真实验，虽然可以验证方案的可行性和有效性，但仿真实验中物联网设备的数量以及 DDoS 攻击的流量，与现实中的 DDoS 攻击存在较大差距，后续需要借助大规模测试工具进行测试，得出方案的性能从而证明方案的大规模可用性。

Table 2 Anti-DDoS system overall comparative evaluation

表 2 防范 DDoS 总体评价对比

	阿里云云盾	**知道创宇抗 D 保**	**腾讯云大禹**	**基于区块链的 DDoS 防御方案**
防御类型	有效抵御所有各类基于网络层、传输层及应用层的 DDoS 攻击	抗 D 保可以防御所有类型的 DDoS 威胁，包括基于网络层的攻击以及应用层攻击，同时可以有效的防御各种反射攻击僵尸网络攻击	有效抵御各种类型的 DDoS 攻击	防御现有各种类型的 DDoS 攻击，同时也能防范未知新的攻击
防御能力	防护峰值带宽 500Gbps（引自阿里云云盾官网）	600G 以上带宽抗 DDoS（引自抗 D 保官网）	300GBGP 防护带宽（引自腾讯云大禹官网）	动态自适应，攻击流量始终控制在较小范围
防御成本	约￥16800 / 月（20G 防护带宽）	约￥15000 / 月（20G 防护带宽）	约￥16600 / 月（20G 防护带宽）	不需要额外的流量引流通路，以及流量清洗设备，成本较低

5 相关工作

DDoS 防御始终是网络安全领域研究的热点之一[10]。RUKAVITSYN A 团队[11]利用 Netflow 协议收集有关网络流量的数据，并利用新数据重新自我学习检测模型的方式进行 DDoS 攻击检测。YU Y 团队[12]提出分

布式协调监控数据流系统 DCM，引入 SDN 在数据交换面实现自定义的动态检测。上述方案都属于目标端监测防御，传统的目标端检测防御 DDoS 方法[13-16]存在时效性低成本高，易造成网络阻塞等缺点。一些研究者考虑在源端部署检测 DDoS 方案，由 GILTM 等提出的 MULTOPS 方案[8]，在每个网络设备源端处都维护一个数据结构 MULTOPS，通过监控受害者或攻击者的数据包速率差异来检测攻击。由 MIRKOVIC J 等提出的 D-WARD 源端 DDoS 防御系统[9]，通过统计数据收集和分析可实现自主攻击检测以及准确响应过滤非法流量。源端检测能够在源端及早地阻止攻击行为，从而避免造成过多的资源浪费，但上述方案都是针对 PC 端流量特点设计的，并不适用于物联网设备。

随着网络分布式计算的发展，DDoS 攻击检测方面的研究思路逐渐从集中式单点检测向分布式检测方案转变[17]，后者更符合 DDoS 攻击的分布式特点，逐渐成为应对 DDoS 攻击的最有效方案之一。区块链技术作为一种新型的分布式技术开始考虑被应用到防范 DDoS 攻击中。

陈旭[18]提出了基于区块链技术的网络 DDoS 联合防御方法，通过在以太坊上开发智能合约，实现跨组织的攻击者名单更新和查询以及信息共享。但该方案只是用区块链实现攻击者名单的共享，并未将区块链技术用于 DDoS 攻击的检测。杨翊等[19]基于联合区块链以及由 H.jonathan chao 团队[20][21][22]提出的 LB ScoreGuard 模型，用去中心化的思路提出 DDoS 防御云网络模型，将传统防火墙的特征库和更新中心去除，改用区块链技术对 DDoS 数据包特征和标记结果进行分布式的存储和共享，但该方案缺少实验验证或模拟验证。我们的方案将区块链用于 DDoS 的整个检测防御流程，并且进行了仿真实验验证，证明了区块链技术对实现 DDoS 早期、高精确度防御的重要作用。

6 结束语

针对利用物联网设备发起的 DDoS 攻击，本文提出了一种基于边缘计算和区块链的检测防御架构，在边缘节点处针对物联网设备进行疑似 DDoS 异常检测，并利用区块链实现初步检测结果的共享分析得出 DDoS 预警，最终基于奖励机制实现源端物联网设备发出的 DDoS 连接过滤。本方案的检测和防御分布式部署在攻击源端，可以避免引流造成的高额成本和网络阻塞，并且可以做到“防微杜渐”，在检测到 DDoS 发生之初就在源头进行持续过滤阻止流量的上涨。后续需要在方案的大规模部署以及部署时的性能问题上进行详尽测试及优化，提高方案的大规模可用性。

References:

[1] Gubbi J, Buyya R, Marusic S, et al. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 2013, 29(7):1645-1660.

[2] Shi WS, Sun H, Cao J, et al. Edge Computing-An Emerging Computing Model for the Internet of Everything Era. Journal of Computer Research and Development, 2017, 54(5):907-924 (in Chinese with English abstract).

[3] Shi W, Cao J, Zhang Q, et al. Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, 2016, 3(5):637-646.

[4] Swan M. Blockchain: Blueprint for a New Economy// Blockchain : blueprint for a new economy. O'Reilly, 2015.

[5] Yuan Y, Wang YF. Blockchain: The State of the Art and Future Trends. Journal of Automatica Sinica, 2016, 42(4):481-494 (in Chinese with English abstract).

[6] Rodrigues B, Bocek T, Lareida A, et al. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. 2017:16-29.

[7] Rodrigues B, Bocek T, Stiller B. Multi-domain DDoS Mitigation Based on Blockchains. 2018:185-190.

[8] GIL T M, POLETTO M. MULTOPS: a data-structure for band width attach detection//The 10th Conference on USENIX Security Symposium. 2001.

[9] Mirkovic J, Reiher P. D-WARD: a source-end defense against flooding denial-of-service attacks. IEEE Transactions on Dependable & Secure Computing, 2005, 2(3):216-232.

[10] ZARGAR S T, JOSHI J, TIPPER D. A survey of defense mechanism against distributed denial of service flooding attacks. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069.

[11] Rukavitsyn A, Borisenko K, Shorov A. Self-learning method for DDoS detection model in cloud computing// Young Researchers in Electrical and Electronic Engineering. IEEE, 2017:544-547.

[12] YU Y, CHEN Q, LI X. Distributed collaborative monitoring in software defined networks. Computer Science, 2014.

[13] Kansal V, Dave M. Proactive DDoS attack detection and isolation[C]// International Conference on Computer, Communications and Electronics. IEEE, 2017:334-338.

[14] Yao G, Bi J, Vasilakos A V. Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(3):471-484.

[15] 12Sahi A, Lai D, Li Y, et al. An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. IEEE Access, 2017, PP(99):1-1.

[16] Yaar A, Perrig A, Song D. StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853-1863.

[17] Chen F, Bi XH, Wang JJ, et al. Survey of DDoS defense: challenges and directions. Chinese Journal of Network and Information Security, 2017, 3(10):16-24 (in Chinese with English abstract).

[18] Chen X. Research on Network DDoS Joint Defense Method Based on Blockchain. Network Security Technology & Application, 2017(11):29-30.

[19] Yang Y, Peng Y, Jiao Y. A DDoS Defense Cloud Based on Blockchain. Chinese Sciencepaper Online [2016-11-04] (in Chinese with English abstract). http://www.paper.edu.cn/releasepaper/content/201611-59.

[20] Kim Y, Lau W C, Chuah M C, et al. PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks. IEEE Transactions on Dependable & Secure Computing, 2006, 3(2):141-155.

[21] Kim Y, Lau W C, Chuah M C, et al. Packetscore: statistics-based overload control against distributed denial-of-service attacks[J]. Proc IEEE Infocom March, 2004, 3:2594-2604 vol.4.

[22] Beitollahi H, Deconinck G. A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks[C]// IEEE, International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2012:11-20.

附中文参考文献:

[2] 施巍松, 孙辉, 曹杰等. 边缘计算:万物互联时代新型计算模型. 计算机研究与发展, 2017, 54(5):907-924.

[5]袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4):481-494.

[17]陈飞, 毕小红, 王晶晶,等. DDoS 攻击防御技术发展综述. 网络与信息安全学报, 2017, 3(10):16-24.

[18]陈旭. 基于区块链技术的网络 DDoS 联合防御方法研究. 网络安全技术与应用, 2017(11):29-30.

[19]杨翊, 彭扬, 矫毅. 基于区块链的 DDoS 防御云网络. 中国科技论文在线[2016-11-04].
http://www.paper.edu.cn/releasepaper/content/201611-59.