基于区块链与排队理论的 DDoS 防御机制研究

张星星,何利文,段红秀
(南京传媒学院,江苏 南京 211172)

摘　要:在软件定义网络(Software Defined Networking,SDN)中,控制层很容易受到分布式拒绝服务(Distributed Denial of Service,DDoS)攻击的威胁。攻击者通过恶意请求或数据流等方式,向 SDN 控制器发送大量请求,从而使控制器资源耗尽,导致控制器不能正常工作。因此,防范和处理控制层 DDoS 攻击是 SDN 安全的关键。该文提出一种基于区块链与排队理论的 DDoS 攻击检测防御机制,该防御机制结合区块链技术,设计了一种新的 SDN 架构模型,该模型对 SDN 控制层重新进行构造,在 SDN 控制层加入容量监控模块、安全模块及区块链模块。容量监控模块基于排队理论,计算进入控制器数据包队列的长度阈值,当队列内数据包数目连续 2 次超过阈值或控制器规则表容量达到 70% 容量触发报警,安全模块用于触发报警后在设置报警的数据包进行 DDoS 特征匹配,如果被确定为异常数据则将数据包摘要信息上传至区块链,利用智能合约共享异常数据包信息摘要,既能够防止过多的信息记录在区块链造成系统负载,又能够使 SDN 网络信息达成共识。对该攻击检测防御机制进行仿真实验,选出了效果最优参数,实验结果表明,与同类型系统相比,该机制对异常数据流的检测率及正常数据流的误报率均有所提升。

关键词:区块链;分布式拒绝服务;排队理论;容量监控;软件定义网络;智能合约
中图分类号:TP399　　**文献标识码**:A　　**文章编号**:1673-629X(2024)11-0117-08
doi:10.20165/j.cnki.ISSN1673-629X.2024.0213

Research on DDoS Defense Mechanism Based on Blockchain and Queuing Theory

ZHANG Xing-xing,HE Li-wen,DUAN Hong-xiu
(Communication University of China,Nanjing 211172,China)

Abstract:In Software Defined Networking (SDN),the control layer is easily threatened by Distributed Denial of Service (DDoS) attacks. Attackers send a large number of requests to the SDN controller through malicious requests or data streams,leading to the depletion of controller resources and the inability of the controller to function properly. Therefore,preventing and handling control layer DDoS attacks is crucial for SDN security. We propose a DDoS attack detection and defense mechanism based on blockchain and queuing theory. This defense mechanism combines blockchain technology and designs a new SDN architecture model. The model reconstructs the SDN control layer by adding capacity monitoring module,security module,and blockchain module. The capacity monitoring module is based on queuing theory and calculates the length threshold for entering the controller packet queue. When the number of packets in the queue exceeds the threshold twice in a row or the controller rule table capacity reaches 70%,an alarm is triggered. The security module is used to trigger the alarm and perform DDoS feature matching on the data packets that have set the alarm. If it is determined to be abnormal data,the packet summary information is uploaded to the blockchain. By using smart contracts to share the abnormal packet information summary,it can not only prevent excessive information from being recorded on the blockchain and causing system load,but also enable SDN network information to reach consensus. We conduct simulation experiments on the proposed attack detection and defense mechanism,selecting the most effective parameters. The experimental results show that compared with similar systems,the detection rate of abnormal data streams and the false alarm rate of normal data streams in the proposed mechanism have been improved.
Key words:blockchain;distributed denial of service;queuing theory;capacity monitoring;software-defined networking;smart contracts

0　引　言

软件定义网络(Software-Defined Networking,SDN)[1]将网络的控制层和数据层解耦,通过中心化的控制平面实现对网络的集中管控。目前,SDN 技术

收稿日期:2024-01-25　　**修回日期**:2024-05-28
基金项目:江苏省高校哲学社会科学研究一般项目(2023SJYB0635)
作者简介:张星星(1998-),女,硕士,助教,通信作者,研究方向为信息安全;何利文(1968-),男,博士,教授,研究方向为网络信息安全、云计算大数据分析与应用;段红秀(1981-),女,硕士,副教授,研究方向为计算机应用。

已经得到广泛应用,尤其是在数据中心、广域网和云计算等领域[2]。在 SDN 网络中,控制器负责管理整个网络的控制平面,包括流表下发、网络拓扑发现和控制消息的处理等任务[3]。分布式拒绝服务(Distributed Denial of Service,DDoS)是一种协同式攻击,攻击者利用恶意程序控制多个被攻击设备形成攻击平台,对一个或者多个对象进行攻击,消耗对象的网络性能或者带宽,最终造成服务器瘫痪[4]。然而,在 SDN 网络中,同样也无法避免 DDoS 攻击。当交换机收到一个新的数据包时,如果交换机转发表中不存在新数据包的路由规则,先将数据包存储在流缓冲区中,然后向控制平面发送 Packet_In 消息,请求新的路由规则[5]。DDoS 攻击会导致控制器暴露在大量恶意流量生成的 Packet_In 消息中,从而破坏正常流量的处理所需资源[6]。同时,大量的恶意流量会占用控制器和交换机之间的带宽,导致网络性能大幅下降。

近年来,区块链技术以其去中心化、安全性高、可追溯性等优点,被广泛应用于各个领域。将区块链技术应用于网络安全领域,也已成为一个新的研究方向。区块链技术可以提供分布式存储和共识机制,使得网络中的每个节点都可以共享和验证数据,从而有效防止网络攻击[7]。因此,将区块链技术应用于 SDN 中,能够进一步提高 SDN 的安全性和稳定性。

目前针对 DDoS 的检测手段主要是解决来自数据平面的大量传入流量导致控制器容量限制的问题,针对这一问题,文献[8]中提出了一种流表大小与控制器处理器相结合的结构,在资源受限的情况下提高系统吞吐量。文献[9]使用 OpenFlow 开关的委托控制器,从而动态调整多个控制器,以克服资源限制。一些学者结合区块链技术,对 DDoS 进行防范,赵婵等[10]提出了一种基于区块链的去中心化防御架构,利用网络中分散的空闲带宽和计算资源对流量数据进行转发和过滤。该架构可及时对 DDoS 进行防御,减少 DDoS 防御耗费的资源。Feng H 等[11]提出了一种基于 IP 信誉的可疑 IP 地址分类防御策略。该解决方案通过智能合约将 SDN 控制器之间的黑灰 IP 地址列表共享给其他应用服务器,使各个域可以安全地协作,分散地传递攻击信息。文献[12]使用智能合约,促进软件定义网络中各个域之间的相互协作,并以安全、高效和去中心化的方式共享攻击信息。虽然区块链技术已经相对成熟,并且已经有学者将其应用在 DDoS 攻击防御领域,但研究主要集中在共享可疑信息,针对 SDN 中的 DDoS 攻击检测防御的完整方案的相关研究还是相对较少。

该文提出一种基于区块链与排队理论的 DDoS 攻击检测防御机制,该防御机制结合区块链技术,设计了一种新的 SDN 架构模型,该模型对 SDN 控制层重新进行构造,在 SDN 控制层加入容量监控模块、安全模块及区块链模块。容量监控模块基于排队理论,计算进入控制器数据包队列的长度阈值,当队列内数据包数目连续 2 次超过阈值或控制器规则表容量达到 70% 时触发报警,在设置报警标志后送入安全模块进行 DDoS 特征匹配,如果被确定为异常数据就将数据信息摘要上传至区块链,并利用智能合约共享,既能够防止过多的信息记录在区块链造成系统负载,又能够使 SDN 网络信息达成共识。最后对提出的机制进行仿真实验得出结论。

1 基于区块链与排队理论的 DDoS 攻击检测防御机制

1.1 SDN 基础架构

SDN 主要由应用层、控制层、数据层构成。SDN 的应用层是 SDN 架构的最顶层,也是最直接与用户交互的层。应用层主要负责提供网络管理员和用户可视化的网络控制界面,用户可以通过应用层实现对网络的监控、管理和配置;SDN 控制层是 SDN 架构的核心,它为网络的数据层提供控制,并管理网络的配置。控制层利用一个中心化的控制器来实现网络的管理,该控制器可以通过南向接口与数据层的设备通信。控制器持有整个网络的拓扑信息,以及各个设备的配置信息;数据层是 SDN 的最底层,这一层提供了基础的网络连通性和可靠性,支持数据的传输。数据层的网络设备通常包括交换机、路由器、防火墙等,它们构成了数据传输的物理基础。SDN 基础架构如图 1 所示。

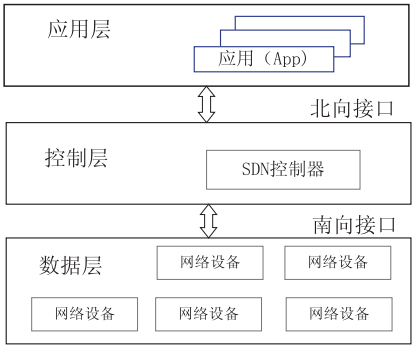

图 1 SDN 基础架构

1.2 系统模型

系统模型如图 2 所示。该模型沿用传统的 SDN 三层模型,不同的是,对 SDN 的控制层重新进行了构造,增加了区块链模块、容量监控模块、安全模块。区块链模块对网络信息进行记录,共享异常流量信息,保证数据的完整性和可靠性。控制器作为区块链节点对 SDN 网络内的数据进行管理、更新、共识。此外,容量监控模块负责监控进入控制器的数据包数量,安全模

块用于提取异常数据包的特征。

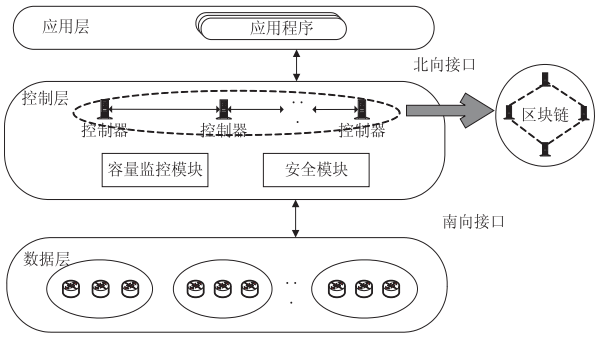

图 2　系统模型

1.3　工作流程

基于区块链与排队理论的 DDoS 攻击检测防御模型工作流程如图 3 所示。

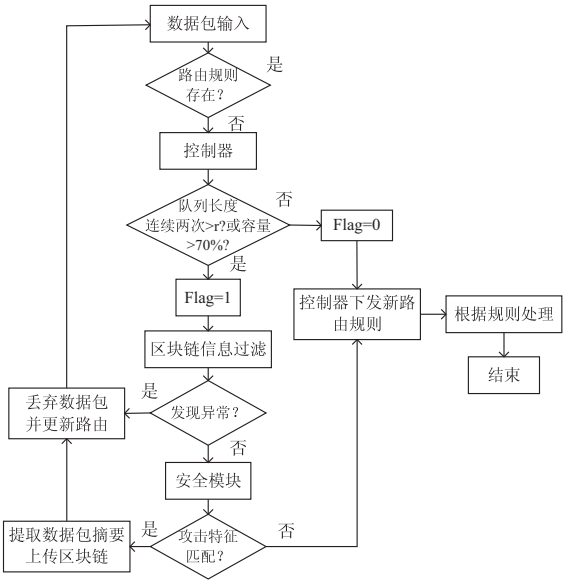

图 3　工作流程

步骤 1:当 SDN 交换机接收到数据包时,将其与流表中的条目进行比较。如果存在相应的路由规则,将按照该规则进行处理。反之,数据包将被传送至控制器,由控制器负责下发相应的路由规则。

步骤 2:数据包送至控制器后,将被加入到控制器的处理列表中进行排队。容量监控模块基于排队理论计算队列长度的阈值,如果队列长度超过该阈值,视为队列拥塞。值得强调的是,队列拥塞并非必然是由 DDoS 攻击引起的,大量数据包涌入控制器可能是正常现象。因此,在一段时间内发生两次以上拥塞时,才被视为紧急情况,设置示警标志 Flag 为 1。此外,以防止拥塞问题,考虑采用另一种测量方法对控制器的容量进行独立评估。当控制器容量超过 70% 时,示警标志 Flag 为 1。

步骤 3:在容量监控模块评估数据包后,如果 Flag 为 0,则执行步骤 6,否则执行步骤 4。

步骤 4:示警后的数据包先根据区块链共享的 DDoS 攻击信息对数据包进行筛选,如果发现异常数据包,则执行步骤 5。否则将在安全模块进行进一步检查,提取数据包特征与 DDoS 攻击特征进行对比,如果发现报文与 DDoS 攻击特征高度吻合,则提取数据包摘要信息上传至区块链进行信息共享。

步骤 5:丢弃数据包,并更新交换机中的路由规则。

步骤 6:控制器将指示交换机将数据包下发新的路由规则,从而更新路由表。

1.4　基于排队理论的 DDoS 检测策略

交换机流表中的每个表项都对应于一条路由规则,进入交换机的数据包将根据指定的路由规则重新被发送到网络的其他部分。如果没有找到路由规则,就会向控制器发送一个 Packet_In 消息,该消息是目的是授权其数据包的合法性,并将一个新的路由规则交给交换机并放置在流表中。

1.4.1　容量监控模块队列长度阈值计算

通过在控制器中创建一个表来存储交换机请求的每个规则,可以管理请求,控制数据量,并在被攻击时防止控制器拥塞。当没有新的数据包交付给控制器规则表时,队列的长度为零。对于 T 周期内数据包进入表的速率为 λ ,根据利特尔定律,表元素的平均数量为 $T\lambda$ 。因此,如果控制器规则表容量超过 70% ,则很可能出现 DDoS 攻击导致的拥塞。在产生数据包到达瞬时峰值的波动期间,当控制器规则表填满时,控制器无法接收数据包,从而中断网络功能。为了防止出现这种情况,当相应的服务器被占用时,考虑另一个队列在一段时间内容纳传入数据包。该方案允许控制器以较短的延迟接收和处理数据包,直到一些空间被释放,而不会丢失任何数据包。

为了防止在控制器队列中积累,建立一个特定的阈值,超过该阈值设置示警标志。假设 t 时刻队列长度为 N_q ,则队列长度阈值 L 计算如下[13]:

$$L = k\sigma_q + E[N_q]$$

其中, k 为常数, σ_q 为队列长度的方差, $E[N_q]$ 为队列长度的均值。进入交换机的数据包通常假设具有泊松分布,因为它在时间轴上产生恒定的平均值。

首先计算 t 时刻 j 长度队列概率稳态方程,计算方式如下:

$$\lambda p_0 = \mu p_0$$

$$(\lambda + \mu) p_1 = \lambda p_{j-1} \quad j = 0,1,2\cdots$$

其中, λ 为数据包进入表的速率, μ 为控制器处理速率, p_i 为系统中 i 个元素的概率,系统达到稳态的前提是 $\omega = \dfrac{\lambda}{\mu} < 1$,如果到达率大于服务率,那么队列长度将无限增加,其中 ω 为稳定性指标。由此,可得 t 时刻

j 长度系统概率稳态方程为：

$$P[N(t)=j]=(1-\omega)\omega^{j} \quad j=0,1,2\cdots$$

其中，$N(t)$ 为系统中元素个数，系统平均元素数可计算如下：

$$E[N(t)]=\sum_{j=0}^{\infty}jP[N(t)=j]=\frac{\omega}{1-\omega}$$

系统平均时延为：

$$E[T]=\frac{E[N(T)]}{\lambda}=\frac{\omega/\lambda}{1-\omega}=\frac{1/\mu}{1-\omega}=\frac{E[\tau]}{1-\omega}=\frac{1}{\mu-\lambda}$$

其中，τ 为控制器处理时间，$E[\tau]$ 为平均处理时间。

此外，通过从平均时延中减去控制器平均处理时间，可以得到队列中数据包的平均等待时间 $E[W]$。

$$E[W]=E[T]-E[\tau]=\frac{E[\tau]}{1-\omega}-E[\tau]=\frac{\omega}{1-\omega}E[\tau]$$

则队列长度平均值和方差计算如下：

$$E[N_q]=\lambda E[W]=\frac{\omega^2}{1-\omega}$$

$$\sigma_q^2=E\{N_q^2\}-E\{N_q\}^2=\frac{\omega^2(1+\omega)}{(1-\omega)^2}-\frac{\omega^4}{(1-\omega)^2}$$

$$\sigma_q=\frac{\omega\sqrt{1+\omega-\omega^2}}{1-\omega}$$

如果 r 是大于队列长度阈值 L 的最小整数，则：

$$P\{N_q\geqslant r\}=\sum_{j=r}^{\infty}(1-\omega)\omega^{j+1}=\omega(1-\omega)\sum_{j=r}^{\infty}\omega^{j}=\omega^{r+1}$$

1.4.2 安全模块基于特征提取的 DDoS 检测

安全模块识别攻击数据的思想在于，根据提取的唯一且高效的统计特征创建阈值数据库，准确地将攻击数据与正常数据区分开来。该文通过训练和测试两个阶段来实现这一思想。在训练阶段，使用正常数据库和攻击数据库，特征分别从每个数据库中提取。归一化后，比较正常数据和攻击数据的结果，得到每个特征的期望阈值并存储起来，以供下一阶段使用。

在测试阶段，再次使用正常数据和攻击数据对系统进行分析，与之前一样，分别抽取所选特征进行归一化，使用每个特征存储的阈值，对数据进行分类，如果与阈值偏差过大，则识别为 DDoS 攻击。安全模块 DDoS 攻击检测算法流程如图 4 所示。

在特征提取阶段，对各种 DDoS 特征进行了评估，选择了三个鲁棒特征：$H(\mathrm{SIP}\mid\mathrm{DIP})$、$H(\mathrm{SIP}\mid\mathrm{Dport})$ 和 $H(\mathrm{TTL})$。之所以依赖特征熵而不是特征，是因为它们的 DDoS 行为范围不同。例如，DDoS 攻击的 IP 来源分布较广，而某些特征则分布在本地。熵是用于度量随机变量信息和不确定性的指标。在正常网络中，数据流通常均匀分布，信息熵保持在某个范围内。若信息熵超出设定范围，表示数据分布不均匀，相关性增强，存在异常情况。对于变量，熵的定义[14]如下：

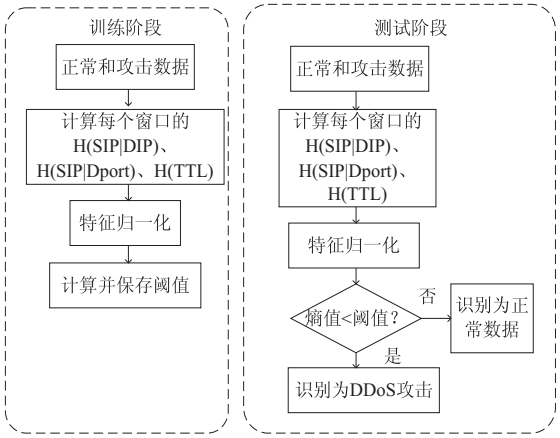

图 4 安全模块 DDoS 攻击检测算法流程

$$H(A)=-\sum_{a\in A}P(a)\log_2(P(a))$$

其中，A 是由网络信号衍生的选择性特征，其向量 $A(a_i\mid i=1,2,\cdots,n)$ 有 n 个值，$P(a_i)$ 表示向量 A 中每个值出现的概率，且满足：

$$\sum_{i=1}^{n}P(a_i)=1$$

然而，在复杂的网络环境中，单个变量的信息熵难以准确地表示流量特征的变化。因此，条件熵被用来度量在已知随机变量下另一随机变量的不确定性。通过计算条件熵，能够更准确地描述网络流量特征的变化情况。因此，条件熵更适用于检测 DDoS 攻击流量。条件熵的计算如下：

$$H(A\mid B)=-\sum_{a\in A,b\in B}P(a,b)\log\frac{P(a,b)}{P(b)}$$

用 SIP 表示源 IP，DIP 表示目的 IP，TTL 表示生存时间，Dport 表示目的端口。然后应用上述条件熵计算公式得到 $H(\mathrm{SIP}\mid\mathrm{DIP})$ 和 $H(\mathrm{SIP}\mid\mathrm{Dport})$，分别量化给定目的 IP 和源 IP 的无序程度。此外，$H(\mathrm{TTL})$ 表示数据包生存时间随机性的度量。对数据进行预处理后，将上述信息作为正常和攻击数据分类用于特征提取。并将得到的 $H(\mathrm{SIP}\mid\mathrm{DIP})$、$H(\mathrm{SIP}\mid\mathrm{Dport})$ 和 $H(\mathrm{TTL})$ 量化到 0 到 1 之间。

1.4.3 阈值计算

由于 DDoS 攻击的不确定性和多变性，采用固定阈值的方法无法准确区分报文是否属于 DDoS 攻击。指数加权移动平均算法是一种常用的序列处理方式，它的特点是对越接近当前时间的数据赋予越大的加权影响力，而对历史数据的影响逐渐减小，能够有效地反映数据的短期趋势变化。如果网络中存在 DDoS 攻击，当大量报文进入安全模块后，那么所在时间窗口的熵值一定会有明显变化，而正常情况下熵值波动趋于平滑，因此利用指数加权移动平均算法能够对某个时

刻的熵值进行预测,如果真实熵值与预测熵值偏差过大,那么就可以判定该时刻所接收的数据包存在 DDoS 攻击。

指数加权移动平均算法的计算方法为:

$$V_t = \beta V_{t-1} + (1-\beta)\theta_t \qquad t = 1,2,\cdots,n$$

其中,V_t 是 t 时刻的移动平均预测值,θ_t 为 t 时刻的真实值,β 是权重,系数 β 越小就说明对当前抽样值的权重越高。

1.5　基于区块链的 DDoS 异常信息共享方法

SDN 控制器之间使用基于区块链和智能合约来共享攻击信息。首先,利用智能合约创建和部署协作合约。然后添加授权参与者。区块链存储已发现的 DDoS 攻击的流量摘要信息,一旦发现接收的报文与已存储的异常流量摘要信息匹配,区块链的每个授权参与者都将有权直接丢弃数据包。

为了传输攻击信息,每个控制器都作为一个区块链节点,用于记录攻击信息。异常信息摘要共享智能合约如算法 1 所示。

算法 1　异常信息摘要共享智能合约

Algorithm:Exception information summary sharing smart contract

Input:AttackInfo[ ]//异常流量摘要信息

Ouput:Status of information sharing.//区块链同步状态

1:For AttackInfo[ ]　do

2:SHA-256(AttackInfo[i])　//对异常流量信息摘要进行签名

3:End For

4:if Verified　then

5:　　AttackInfos[ ] ← AttackInfo[i]　　//更新区块链上的异常流量新库

6:　　Status of information sharing ← 1　//同步成功

7:else　Status of information sharing ← 0　//同步失败

8:Return Status of information sharing

异常数据包摘要提取:

在进行摘要存储之前,提取数据包报头的一些部分进行计算。选择若干项组成最终摘要,如下所示:源地址、目的地址、数据包长度和协议。此外,针对 TCP 报文,配置 TCP 标志位。基于上述信息,摘要包括如下所示的五个项目:

数据包长度摘要:以不同的长度来对数据包进行分类,然后计算数据包长度的熵。DDoS 攻击发生时,数据包报文长度会集中在某一段,导致熵显著降低。定义如下:

$$H_{\text{item1}} = -\sum_{i=1}^{6} \frac{S_i}{N} \log_2 \frac{S_i}{N}$$

其中,S_i 为 i 段的个数,N 为该时间段内的总包数,并满足:

$$N = \sum_{i=1}^{6} S_i$$

TCP 标志摘要:通过 TCP 标志来计数数据包,例如 FIN, SYN, ACK, SYN + ACK 和 PSH + ACK。这是 DDoS 攻击的一个明显特征,因为 SYN 泛洪攻击和 ACK 泛洪攻击可以提高 SYN 和 ACK 的速率。

协议摘要:协议摘要还包括与协议相关的条目。根据不同类型的协议(如 TCP、UDP 和 ICMP)对数据包进行计数。通常情况下,TCP 报文占比较高。

源 IP 地址摘要:在没有恶意流量的情况下,访问服务器的源 IP 数量通常处于稳定状态,具有平滑熵。DDoS 攻击发起时通常源 IP 的数量会突然增加,特别是使用假 IP 地址和随机 IP 地址时。计算方法如下:

$$H_{\text{item4}} = -\sum_{i=1}^{J} \frac{X_i}{N} \log_2 \frac{X_i}{N}$$

其中,X_i 为第 i 类 IP 地址的频率,J 表示 IP 源地址类型的个数。

目的 IP 摘要:与上述内容类似,当攻击发生时,目的 IP 地址将开始集中。因此,它的熵会明显下降。最终结果定义如下:

$$H_{\text{item5}} = -\sum_{i=1}^{K} \frac{Y_i}{N} \log_2 \frac{Y_i}{N}$$

其中,Y_i 表示第 i 类 IP 目的地址的频率,K 表示 IP 目的地址类型的数量。

2　实验结果与分析

2.1　实验环境

仿真实验在处理器 AMD Ryzen 7 4800U with Radeon Graphics CPU@1.80 GHz 的 64 位 Windows10 操作系统的笔记本电脑上,实验利用 Mininet 仿真平台和 Ryu 控制器构建网络拓扑,共选取 4 台终端作为僵尸主机对其他终端发起攻击,使用 Scapy 作为流量生成工具,在 SDN 网络内发起 DDoS 攻击。DARPA 数据库提供二进制形式的 DDoS 攻击数据。在本项目中,使用 tShark 工具将二进制文件转换为. txt 文件,随后用于特征提取算法的其他部分。

2.2　容量监控模块仿真分析

容量监控模块的任务是产生 DDoS 攻击预警,防止系统中断。该模块由两部分组成,一部分用于监控控制器规则表容量,另一部分用于监控控制器的入包队列。对于队列监控模块,评估队列长度和错误概率,稳定性指标 ω 选择在 0.7 左右。评价考虑了不同的 k 值,结果如图 5 和图 6 所示。

假设临界稳态指数为 $\omega = 0.8$,因此根据图 5 中所示,在其他条件相同的情况下,k 值越大,所得到的错

误概率越小,队列长度大于阈值的情况越小,故 k 值与 ω 值均不能取最大。根据图 6 所示,k 值与 ω 值越大,队列长度阈值越大,如果阈值过大就不能够灵敏地检测到受到 DDoS 攻击时激增的数据包,阈值过小又容易将正常流量识别为异常情况,所以在实验中设置 ω = 0.7, r = 20 和 k = 7 的缓冲区大小来保持队列中的数据包。

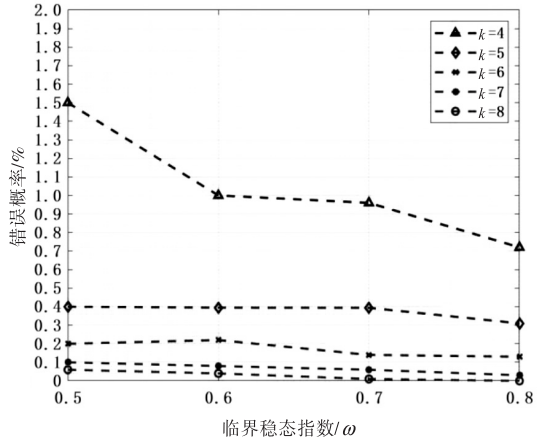

图 5 不同 ω 值及不同 k 值下的错误概率

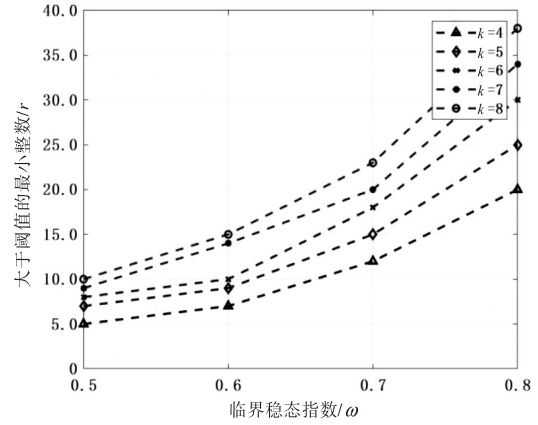

图 6 不同 ω 值及不同 k 值下的阈值长度

2.3 指数加权移动平均值方法 β 的选择

在保证流量大小不变的情况下,使攻击数据包占总数据包的比例分别为 20%、50% 以及 70% 进行实验。指数加权移动平均值方法 β 的值,分别为 0.2、0.5 和 0.8。以 H(SIP | DIP) 为例,统计连续 20 个窗口,比较不同攻击强度下归一化后的 H(SIP| DIP) 与阈值的变化情况。

图 7 ~9 展示了攻击数据包占比 20%、50%、70% 的情况下的值的变化情况,以及 β = 0.2、β = 0.5、β = 0.8 时阈值的变化。当网络受到 DDoS 攻击时,H(SIP | DIP) 值迅速下降,在此之前无论 β 值为多少,预测的阈值均小于 H(SIP | DIP) 值,但在 DDoS 攻击数据进入后,β = 0.2 及 β = 0.5 时,大部分窗口阈值均大于 H(SIP | DIP) 值,仍存在检测失败的情况;当 β = 0.8 时,计算出的阈值均大于 H(SIP | DIP) 值,因此 β = 0.8 的情况能有效检测出 DDoS 攻击。

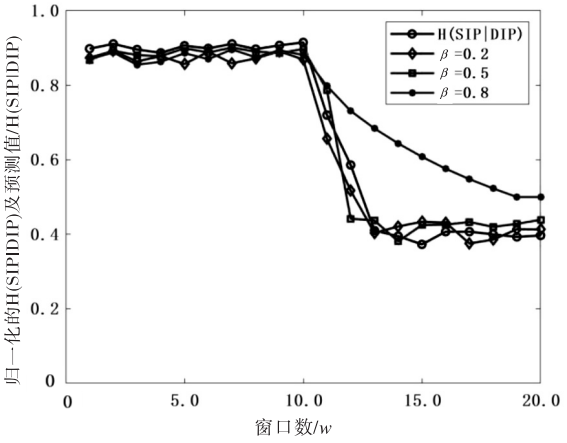

图 7 20% 攻击强度的 H(SIP | DIP) 与阈值变化

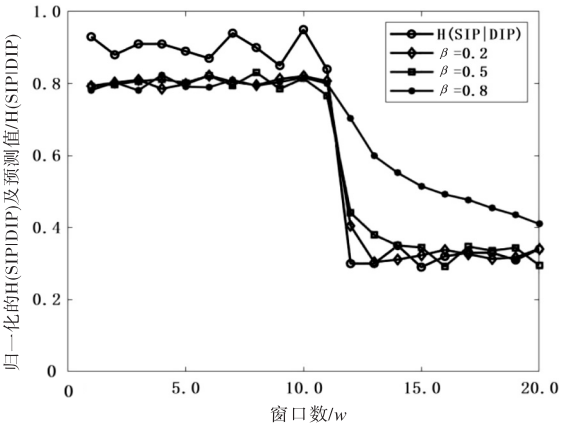

图 8 50% 攻击强度的 H(SIP | DIP) 与阈值变化

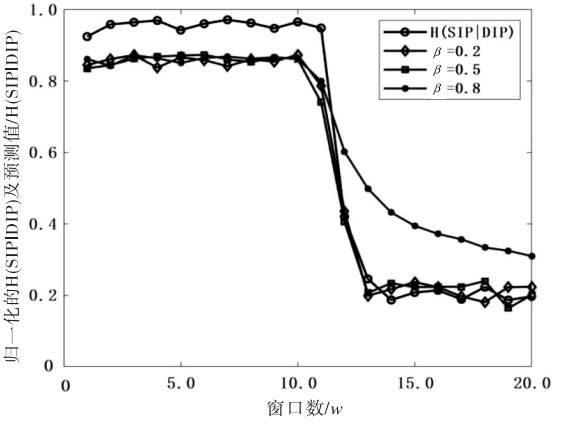

图 9 70% 攻击强度的 H(SIP | DIP) 与阈值变化

2.4 性能分析

为了更好地评价系统,本节对控制器的响应时间,丢包率与基础 SDN 系统[14]进行对比分析,并将所提出的 DDoS 防御系统与其他同类型的系统进行比较,来证明该方法的有效性。

从表 1 可以看出,对于流量在 4 000 包/秒以下,由于队列和包的处理,所提出的系统的控制器响应时间比基础 SDN 系统响应时间长。但当控制器上的攻击分布较广,且超过 9 000 包/秒速率时,采用所提出

的系统可以获得更好的效果。考虑到 SDN 控制器在超过 18 000 包/秒的输入流下中断并停止运行,流量仅增加到 15 000 包/秒,以便更好地和基础 SDN 系统比较。

除此之外,表 1 也对所提出的 DDoS 防御系统与基础 SDN 系统进行了系统丢包率的比较。随着系统控制器响应时间的增加,DDoS 攻击流量越大,基础 SDN 系统丢包量也越大。此外,由于控制器与交换机通信中存在潜在的丢包问题,导致前者的流量重发给控制器,进一步增加了响应时间,同时也增加了控制平面的负载,导致该层拥塞,降低控制器性能。同时,与基础 SDN 系统相比,所提系统中正常数据包丢失率要低得多,说明所提系统具有较高的效率。

表 1　控制器响应时间与丢包率对比

流量/(包/秒)	控制器响应时间(本系统)/ms	控制器响应时间(基础 SDN)/ms	丢包率(本系统)/%	丢包率(基础 SDN 系统)/%
3 000	600	500	0	1
4 000	621	579	0	2
5 000	650	667	1	4
6 000	662	702	1.3	4.2
7 000	690	867	1.7	5.7
8 000	728	935	2	6.4
9 000	740	2 064	2.1	9
10 000	769	5 000	2.15	13.2
11 000	794	6 638	2.21	14.8
12 000	840	7 395	2.4	16.7
13 000	853	7 904	2.51	18.5
14 000	978	8 693	2.63	19.8
15 000	1 023	9 000	2.8	21

在与同类型系统比较中,本章节采用检测率和误报率之比 PR 作为性能指标,计算方式如下:

$$DR = \frac{TP}{TP + FP}$$

$$FR = \frac{FN}{TP + FN}$$

$$PR = \frac{DR}{FR}$$

其中,TP 表示攻击流被成功检测的次数,FP 表示攻击流未被成功检测的次数,FN 表示正常流量被错误识别的次数。

表 2 展示了在 9 000 包/秒的流量下,攻击数据包占比 70% 的情况下本系统与 Kalkan[15] 和 Assis[16] 所提出的系统性能对比结果。

表 2　系统性能对比

系统	方法	检测率(DR)/%	误报率(FR)/%	性能指数(PR)	检测时间/s
Kalkan[15]	基于联合熵的检测	88.3	0.97	91.0	6.2
Assis[16]	博弈论与启发式	91	1.1	82.7	5.9
本系统	基于区块链与排队理论	93	0.94	98.9	8.2

由表 2 可得,与 Kalkan[15] 和 Assis[16] 两种系统相比,提出的 DDoS 防御系统对于异常数据流的检测率及正常数据流的误报率均较优,性能指数有所提升,鲁棒性更强,体现了系统的高效性。基于区块链及排队理论的 DDoS 防御系统不仅可以提高系统数据包验证的灵活性,快速发现攻击,还能够防止 DDoS 攻击导致的系统故障。

3　结束语

该文提出了一种基于区块链与排队理论的 DDoS 防御机制,该机制针对 SDN 控制层 DDoS 攻击,对控制层重新进行构造,加入容量监控模块、安全模块以及区块链模块。容量监控模块用于对传入控制器的数据包队列长度进行监控,安全模块用于特征提取,区块链用

于共享异常数据信息。最后对所提出的防御机制进行了仿真实验,选出了效果最优参数,且对所提出的系统与同类型系统进行对比,证明所提出系统的高效性及优异的鲁棒性。在后续工作中,计划对系统检测时间进行优化,从而快速对 DDoS 攻击进行处理。

参考文献:

[1] 卢向敏,王兴伟,易 波,等. 面向互联网的 SDN 流量多粒度处理机制[J]. 中国科学:信息科学,2020,50(12):1903-1918.

[2] 周琳娜,刘 丹. 网络信息安全问题及防护策略[J]. 软件导刊,2019,18(10):166-168.

[3] 孙浩博,王海涛. SDN 的安全隐患及应对策略研究[J]. 网络安全和信息化,2021(1):128-133.

[4] CHAGANTI R,BHUSHAN B,RAVI V. A survey on blockchain solutions in DDoS attacks mitigation:techniques,open challenges and future directions[J]. Computer Communications,2023,197:96-112.

[5] YANG S,CUI L,CHEN Z,et al. An efficient approach to robust SDN controller placement for security[J]. IEEE Transactions on Network and Service Management,2020,17(3):1669-1682.

[6] JIA B,LIANG Y. Anti-D chain:a lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain[J]. China Communications,2020,17(9):11-24.

[7] YANG F,ZHOU W,WU Q,et al. Delegated proof of stake with downgrade:a secure and efficient blockchain consensus algorithm with downgrade mechanism[J]. IEEE Access,2019,7:118541-118555.

[8] ZHAO G,HUANG L,YU Z,et al. On the effect of flow table size and controller capacity on SDN network throughput[C]// 2017 IEEE international conference on communications (ICC). Paris:IEEE,2017:1-6.

[9] ZHANG Q Y,WANG X W,HUANG M,et al. Software defined networking meets information centric networking:a survey[J]. IEEE Access,2018,6:39547-39563.

[10] 赵 婵,张瑞生. 基于区块链技术的 DDoS 协同防御方法研究[J]. 现代信息科技,2020,4(5):152-154.

[11] FENG Huifen,YAN Xincheng,ZHOU Na,et al. A cross-domain collaborative DDoS defense scheme based on blockchain-SDN in the IoT[C]//Proceedings of the 2021 ACM international conference on intelligent computing and its emerging applications (ACM ICEA '21). New York:ACM,2021:77-82.

[12] EL HOUDA Z A,HAFID A,KHOUKHI L. Co-IoT:a collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN[C]//2019 IEEE global communications conference (GLOBECOM). Waikoloa:IEEE,2019:1-6.

[13] MEMON R A,LI J,AHMED J,et al. Modeling of blockchain based systems using queuing theory simulation[C]//2018 15th international computer conference on wavelet active media technology and information processing (ICCWAMTIP). Chengdu:[s. n.],2018:107-111.

[14] 王文涛,王奇枫,郭 峰,等. 基于 Open vSwitch 的 SDN 网络平台构建方法[J]. 中南民族大学学报:自然科学版,2014,33(4):99-104.

[15] KALKAN K,ALTAY L,GÜR G,et al. JESS:joint entropy-based DDoS defense scheme in SDN[J]. IEEE Journal on Selected Areas in Communications,2018,36(10):2358-2372.

[16] DE ASSIS M V O,HAMAMOTO A H,ABRÃO T,et al. A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks[J]. IEEE Access,2017,5:9485-9496.