云环境下 SDN 网络低速率 DDoS 攻击的研究

陈兴蜀[1,2]，滑强[1,2]，王毅桐[3]，葛龙[3]，朱毅[2]

（1. 四川大学网络空间安全学院，四川 成都 610065；2. 四川大学网络空间安全研究院，四川 成都 610065；
3. 四川大学计算机学院，四川 成都 610065）

摘 要：针对云环境 SDN 网络中存在的对低速率 DDoS 攻击检测精度较低，缺乏统一框架对数据平面、控制平面低速率 DDoS 攻击进行检测及防御等问题，提出了一种针对低速率 DDoS 的统一检测框架。首先，分析验证了数据平面低速率 DDoS 攻击的有效性，在此基础上结合低速率 DDoS 攻击在通信、频率等方面的特性，提取了均值、最大值、偏差度、平均离差、存活时间这 5 个方面的十维特征，实现了基于贝叶斯网络的低速率 DDoS 攻击检测。然后，通过控制器下发相关策略来阻断攻击流。实验表明在 OpenStack 云环境下对低速率 DDoS 攻击检测率达到 99.3%，CPU 占用率为 9.04%，证明了所提方案能够有效地完成低速率 DDoS 攻击的检测及防御。

关键词：云计算；软件定义网络；低速率 DDoS 攻击；贝叶斯网络

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019120

Research on low-rate DDoS attack of SDN network in cloud environment

CHEN Xingshu[1,2], HUA Qiang[1,2], WANG Yitong[3], GE Long[3], ZHU Yi[2]

1.College of Cybersecurity, Sichuan University, Chengdu 610065, China
2. Research Institute of Cybersecurity, Sichuan University, Chengdu 610065, China
3. College of Computer Science, Sichuan University, Chengdu 610065, China

Abstract: Aiming at the problems of low-rate DDoS attack detection accuracy in cloud SDN network and the lack of unified framework for data plane and control plane low-rate DDoS attack detection and defense, a unified framework for low-rate DDoS attack detection was proposed. First of all, the validity of the data plane DDoS attacks in low rate was analyzed, on the basis of combining with low-rate of DDoS attacks in the aspect of communications, frequency characteristics, extract the mean value, maximum value, deviation degree and average deviation, survival time of ten dimensions characteristics of five aspects, to achieve the low-rate of DDoS attack detection based on bayesian networks, issued by the controller after the relevant strategies to block the attack flow. Finally, in OpenStack cloud environment, the detection rate of low-rate DDoS attack reaches 99.3% and the CPU occupation rate is 9.04%. It can effectively detect and defend low-rate DDoS attacks.

Key words: cloud computing, software defined networking, low-rate DDoS attack, Bayesian network

1 引言

随着近些年基于虚拟化的云计算技术的发展，SDN（software defined networking）框架因其集中控制、可扩展性强等特点作为一种安全解决方案逐渐被云计算数据中心所采用，利用 SDN 框架可解

收稿日期：2018–12–06；**修回日期**：2019–04–21

基金项目：国家自然科学基金青年科学基金资助项目（No.61802270, No.61802271）；四川省重点研发基金资助项目（No.2018G20100）

Foundation Items: The National Natural Science Foundation of China Youth Science Foundation Project (No.61802270, No.61802271), The Key Research and Development Project of Sichuan Province (No.2018G20100)

决云环境中租户隔离、网络流量控制[1]、攻击检测等问题[2-3]。对于 SDN 框架本身来说，其数控分离的特性增大了攻击面[4]，在云环境中更易受到攻击。由于 DDoS（distributed denial of service）攻击易实施，针对 SDN 网络的低速率 DDoS 攻击检测防御是重要的研究方向之一，大部分研究者主要研究针对 SDN 控制平面的低速率 DDoS 攻击[5-11]，比如攻击者利用地址欺骗产生大量的流表规则不匹配的攻击流，每条攻击流都会向控制器发送 packet_in 消息，导致控制器产生拒绝服务的效果；一些研究者也研究对数据平面的低速率 DDoS 攻击[12-14]，旨在溢出虚拟交换机的流表空间来影响其资源的消耗，同时增加分组丢失率，达到拒绝服务的效果。对于数据平面的交换机来说，交换机流表存在 2 种流表机制，研究人员采用更贴合实际场景的空闲超时流表机制进行研究[15]。针对数据平面和控制平面的低速率 DDoS 攻击，有一个共有特性是攻击流都会经过交换机，但对于数据平面的低速率 DDoS 攻击隐蔽性更强[8]。

本文主要研究针对 SDN 网络进行低速率 DDoS 攻击的检测防御方法，首先针对 SDN 网络中数据平面低速率 DDoS 攻击的有效性进行了分析与验证；根据控制平面及数据平面的低速率 DDoS 攻击特性，提取了 10 项相关的特征，结合贝叶斯网络实现了云环境下低速率 DDoS 攻击检测方法，构建了检测防御框架。该框架能够有效地检测防御云环境中低速率 DDoS 攻击。

本文主要贡献有以下几点。

1) 详细分析了云环境 SDN 网络中针对数据平面的低速率 DDoS 攻击，研究了其在云环境中的有效性及可行性。

2) 提出了云环境下低速率 DDoS 攻击统一检测防御框架。根据低速率 DDoS 的攻击特性，提出了 10 项基于流量的相关特征，基于贝叶斯网络实现了低速率 DDoS 攻击的有效检测，之后利用 SDN 控制器集中控制的特性对攻击流量进行阻断、缓解，达到防御 DDoS 攻击的目的。

3) 在 OpenStack 云环境下，基于 POX 控制器实现了检测系统并进行了相关实验，检测结果显示，本文方法能够有效地检测防御云环境下低速率 DDoS 攻击，在攻击流量占比 50%时，检测防御框架的检测率可以达到 99.3%，内存占用率为 9.04%。

2　相关工作

目前，在云环境 SDN 网络中存在着多种协议类型的低速率 DDoS 攻击，例如基于 TCP 协议、基于 UDP 协议和基于 HTTP 协议的低速率 DDoS 攻击；同时还会存在周期性和非周期性的攻击模式，例如基于 HTTP 协议的低速率 DDoS 攻击，SlowHttpTest 工具可以产生周期性攻击，slowloris-ng[6]工具可以产生非周期性攻击。

对于低速率 DDoS 攻击的研究由 Kuzmanovic[16]首次提出了“Shrew”攻击的概念，在骨干网络上采集到低速率 DDoS 攻击的相关数据，并进行了相关的研究。目前，对于云环境下低速率 DDoS 攻击检测防御的研究主要有以下几类方法。一类是基于流量特征统计分析的检测方法。Sahoo 等[5]提出了一种基于广义熵的度量方法，利用 SDN 网络流的特点，使用信息距离来量化不同概率分布下流量的偏差作为度量来检测攻击行为。Lukaseder 等[6]基于 SDN 网络的低速率 DDoS 缓解机制，提出了 6 个相关特征并通过真实数据集来计算各个特征的精准度，得出最优的方案和阈值，以统计信息作为检测的标准，阈值依据实验样本得出。何亨等[7]提出了一种基于置信度过滤，同时结合链路带宽和数据流检测的 SDCC 方案，该方案计算数据分组 CBF（confidence-based filtering）分数，将低于阈值的分组判断为攻击分组，其还需要建立 SDCC 的攻击流特征库，维护 profile 表的更新，过程较为复杂；同时为了降低资源消耗，该方案在系统正常、预警、防御等状态下对数据流的抽检比例分别为 20%、40%、80%，然而，该方法仍存在一定漏检、误报的风险。刘孟[8]提出了云环境下 SDN 中低速率 DDoS 的检测方法，该方法通过设置多个检测周期内流表快照和可疑表，来逐步记录流表中各流规则的存活时间，设置报警阈值，以此判断是否受到低速率 DDoS 攻击。上述几种检测方法大多依赖于 packet_in 消息提供的信息，当攻击产生的 packet_in 消息较少时，难以达到检测效果。

另一类是基于流量特征的检测方法，大部分研究人员通过提取流量特征属性并结合机器学习的方法来检测低速率 DDoS 攻击。Wang 等[9]提出了针对低速率攻击的自适应 HMM-R（renyientropy and hidden Markov model），通过计算攻击流源 IP 与目的 IP 的瑞利熵，结合隐马尔可夫模型区分攻击流

量。Chen 等[10]提出基于 XGBoost 的低速率 DDoS 攻击检测方法，通过 TCP 连接的基本特性、基于时间流量统计特性和基于主机的流量统计特性这 3 个方面，提取了 9 个特征。XGBoost 有很强的可伸缩性，因此适用于大规模的网络环境。吴志军等[11]提出了一种基于联合特征的低速率 DDoS 检测方法，提出了可用带宽比、小分组比例及分组丢失率特征，并通过 BP（back propagation）神经网络训练出决策指标作为低速率 DDoS 攻击的判断依据，但是当攻击强度较弱时，攻击流的分组丢失率及可用带宽占比的变化并不会特别明显，可能会导致检测结果的偏离。

同时有研究者对于交换机流表的溢出问题进行了相关缓解方法的研究，如乔思祎等[13]提出了一种流表共享的方法来完善目前 table-miss 处理机制，其通过借用相邻交换机流表资源来缓解某一交换机的流表溢出风险。Kandoi 等[14]分析了针对控制平面及数据平面的低速率 DDoS 攻击，并提出了一种通过限制数据传输速率来缓解 DDoS 攻击的方法。

综上所述，目前的检测防御方法存在过分依赖于 packet_in 消息信息的问题，当 packet_in 消息信息不足或被干扰时，可能导致检测结果的偏离。针对攻击流特性所提取的特征不能准确反映攻击特点及可能存在变化的问题，本文采用基于贝叶斯网络的检测方法，根据攻击特性提取了十维特征，提高了检测精度。

3 低速率 DDoS 攻击分析

在云环境中低速率 DDoS 攻击可以分为两大类：一类是针对控制平面的低速率 DDoS 攻击；另一类是针对数据平面的低速率 DDoS 攻击。对于控制平面的低速率 DDoS 攻击来说，对其通信特性、周期性特性等攻击特性的研究较为成熟。对于针对数据平面低速率 DDoS 攻击来说，对其研究大多集中于利用洪泛攻击使流表溢出，而对于长期占用流表空间使流表溢出的攻击方式研究较少。本章主要研究针对数据平面的低速率 DDoS 攻击，对控制平面的低速率 DDoS 不再赘述。

云环境中，数据平面低速率 DDoS 攻击的目的是使云环境内攻击流经过的虚拟交换机上生成相关流规则，并长时间存活，当虚拟交换机的流表空间被占满后，后续数据分组无法进行正确转发，难以达到拒绝服务的效果。

针对数据平面低速率 DDoS 攻击的关键在于使虚拟交换机中的流规则长时间存活。攻击者必须不断地进行攻击以激活相应的规则，使流规则空闲超时时间重置，来达到长时间存活的目的。要使攻击性价比最大化及增强攻击的隐蔽性，低速率 DDoS 的攻击周期要近似于虚拟交换机的空闲超时时间，以此来减少攻击的次数，同时减少与控制器通信的 packet_in 消息。当攻击流的攻击周期小于流表空闲超时时间时，攻击流第一次出现，会产生一次 packet_in 消息上报至控制器，控制器下发相应的规则到虚拟交换机，之后当攻击数据分组再次出现时，不会产生 packet_in 消息。本文用 idle_time 表示空闲超时时间，用 hard_time 表示硬超时时间。

当攻击者的攻击周期小于 idle_time，攻击流的新数据分组到达时，虚拟交换机将不会产生 packet_in 消息上报控制器。控制器对于这条攻击流的记录只有第一次访问时的记录，如图 1 所示，为了实验的直观性，攻击流都包含正常流。本测试 idle_time 设置为 5 s，攻击流 T_1 周期为 4 s，包含 30 条不同的流并持续发送；攻击流 T_2 周期为 6 s，包含 20 条不同的流并持续发送；正常流 T_3 模拟正常流随机发送。

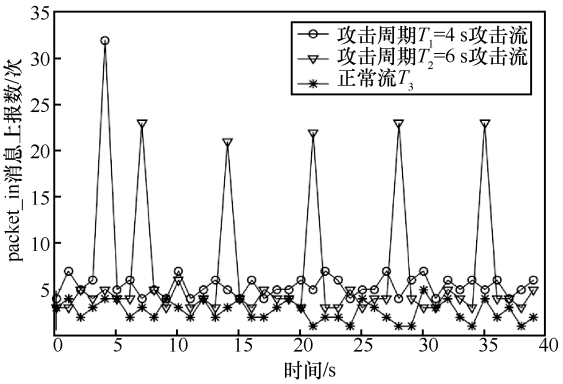

图 1 不同类型流量产生的 packet_in 消息数

图 1 表明，攻击周期小于 idle_time 的 T_1 流只产生了一次数量为 32 的 packet_in 消息上报，攻击周期大于 idle_time 的 T_2 流则产生了多次 packet_in 消息上报，相较于 T_1 流其攻击隐蔽性明显降低。由于在此机制下，packet_in 消息只被记录一次，多种涉及 packet_in 消息的 DDoS 检测方法[17]的检测效果将会降低，攻击的隐蔽性明显增强，同时加入了非周期性的机制，使一些通过周期性和时序特征来检测低速率攻击的检测方法的

效果同样会降低。

以近似空闲超时时间作为攻击周期，具有较强的隐蔽性及较高的性价比，攻击者在攻击前会试图获取该时间。以云环境作为本文的攻击场景，攻击者无法获取云环境内网络拓扑及虚拟交换机内流表的空闲超时时间，会通过多次探测的方法来获得这一近似空闲超时时间。初始攻击周期为 I，周期增加量为 Δt，流表空闲超时时间为 idle_time，攻击流攻击周期满足如式(1)所示的条件。

$$I + n\Delta t < \text{idle\_time} \tag{1}$$

本文定义发送访问请求到收到响应的时间为响应时间，虚拟交换机流表超时时间为 10 s。攻击流引发 packet_in 消息时，其响应时间必定大于非引发 packet_in 消息的攻击流，具体如图 2 所示。

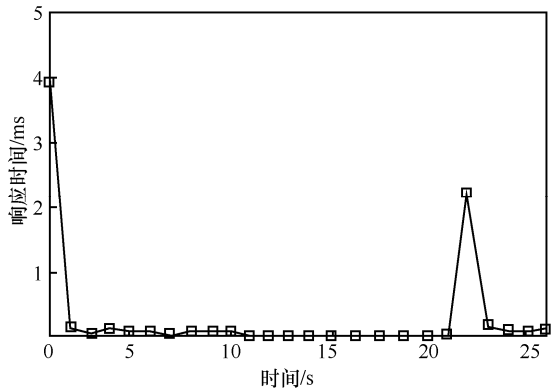

图 2　响应时间对比

验证性实验在 0 s 时发送了一条新的访问请求，流表中没有相应的流规则，故产生 packet_in 消息，其响应时间为 4.01 ms。1 s 至 10 s 持续发送访问请求，流表中存在相应规则，故没有产生 packet_in 消息，其响应时间大幅降低。11 s 之后，该流规则老化删除，再次发送访问请求，响应时间为 2.32 ms。通过响应时间的大小判断是否产生 packet_in 消息，从而逼近空闲超时时间来确定 SDN 网络中低速率 DDoS 的攻击周期，逼近机制如图 3 所示。

设初始攻击周期为 I，空闲超时时间为 idle_time，记录访问请求响应时间为 t_1，将周期增加Δt，变为 $I+\Delta t$，继续发送请求获得响应的时间为 t_2，当 t_2 约等于 t_1 时，说明攻击流所对应的流规则还存在于虚拟交换机的流表上，没有产生 packet_in 消息，攻击周期 $(I+\Delta t)$小于 idle_time。逐渐增加攻击周期，当攻击周期达到 T_1 时，访问请求响应时间 t_3，攻击周期达到 T_2 时，其响应时间 t_4 会明显地大于 t_3；当说明流表中没有攻击流所对应的流规则，会产生 packet_in 消息消耗时间，即攻击周期超过 idle_time。此时，攻击周期回退至上一周期时间 T_1，以较小的周期增量Δm 增加至周期 T_3，与 t_3 相比，此时响应时间没有明显差距，说明攻击周期还是在 idle_time 之内。以此类推，对于周期性攻击而言，攻击周期逐步逼近 idle_time，可以达到最佳的攻击性价比。

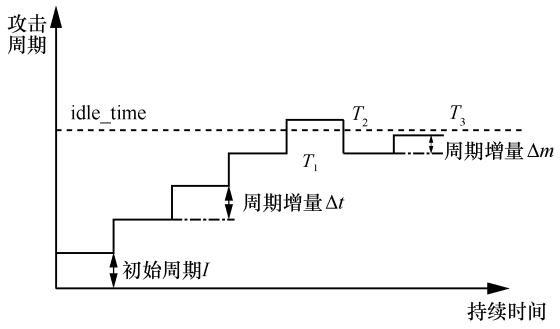

图 3　攻击周期逼近机制

云环境内多交换机场景获取近似空闲时间与单一交换机获取近似空闲时间的原理相同。首先攻击者会预估一个较大的空闲超时时间作为初始的攻击周期，记录访问请求响应时间，增加初始攻击周期，直到其响应时间趋于稳定，该响应时间可以认为是攻击路径上空闲超时时间的最大值。在此之后，攻击周期逐步减少，可以发现访问请求响应时间同样在减少，在这一过程中，在空闲超时时间较大的交换机上，相应的流规则已经存在且被不断被激活，当响应时间趋于稳定后，该响应时间可以认为是攻击路径上最小空闲超时时间的近似值，该值即为攻击者所需要的攻击周期。

在实验环境中来验证所提机制的有效性。为了简化实验，攻击者作为内网中交换机 s_1 下的主机，目标服务器是交换机 s_5 下的主机，攻击路径上的交换机 s_1、s_2、s_3、s_4、s_5 的空闲超时时间分别设置为 10 s、15 s、20 s、25 s、13 s，观察响应时间的变化，第一次的响应时间不计入观察范围，结果如图 4 所示。

根据模拟实验结果分析，通过不同的攻击周期进行探测，当攻击周期大于上述最小空闲超时时间（即 10 s）时，可以看到响应时间在不断升高，当攻击周期小于上述最小空闲超时时间时，响应时间一直为 0。通过观察响应时间的变化，可以逐步逼近最小的空闲超时时间，验证了该机制的有效性。

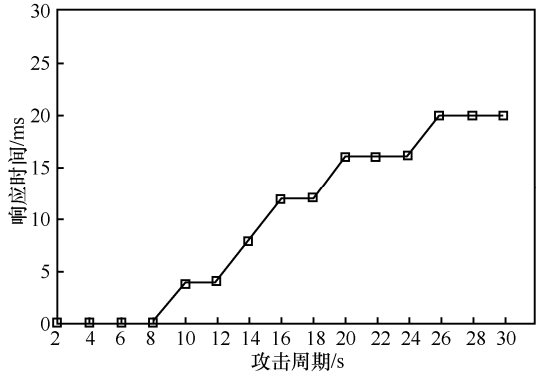

图 4　多控制器交换机环境响应时间变化

在 SDN 网络中，攻击流产生的恶意流规则会存在于攻击路径上所有的交换机中，当攻击流通过不同交换机到达目标服务器时，交换机上流规则的数量也不同，在此进行模拟实验，攻击者通过模拟 IP 发送攻击数据分组至虚拟服务器，攻击速率为每 9 秒 100 个，攻击场景如图 5 所示。

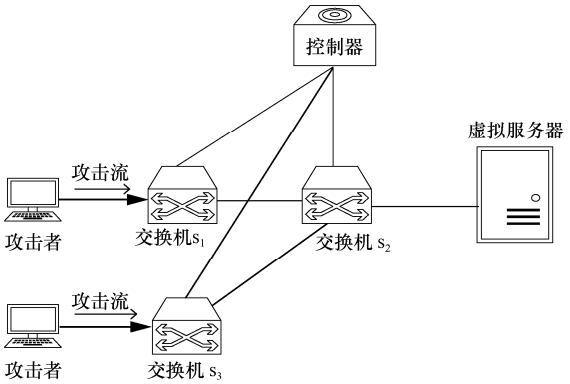

图 5　SDN 网络中低速率 DDoS 攻击模拟场景

交换机 s_1、s_3 中分别存在 110 条流规则，而交换机 s_2 中存在 210 条流规则。由实验结果可知，攻击通过不同的交换机到达目标服务器，所经过的交换机都会受到影响，路径汇聚处的交换机与目标服务器直连的交换机受影响程度较高。

在虚拟环境中对低速率攻击所产生的流规则的持续时间以及大量流规则对流表资源的占用情况进行实验，验证攻击的有效性。首先对攻击产生流规则的持续时间进行实验分析，模拟 100 个不同的 IP 对目标主机发送分组，间隔为 9 s，空闲超时时间为 10 s，其中攻击主机与客户主端机连接在 s_1 交换机上，目标主机连接在 s_2 交换机，实验结果如图 6 所示。实验中，从第 10 s 开始发送攻击数据分组，之后可以看到流规则数量保持 110 条不变（包含主机回复的流规则），同时随着攻击的进行，流规则持续时间超过空闲超时时间，达到长期占用的目的。

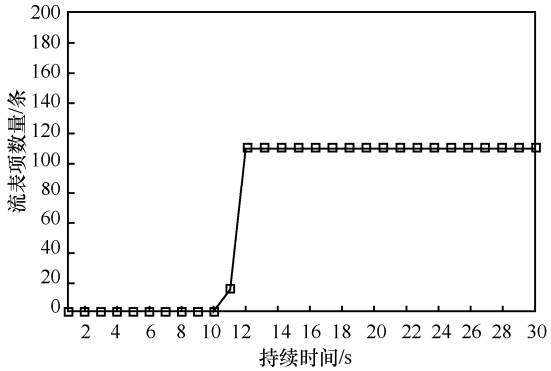

图 6　流规则数量变化

当大规模的攻击到来时，流规则数量逐渐增加，本文为简化实验通过攻击工具使用随机源 IP 低速率攻击每秒发送 1 000 个数据分组，实验环境与上文实验相同。在 11 s 时开始，通过 API 接口统计流表信息监测虚拟交换机的流规则数量变化，如图 7 所示。

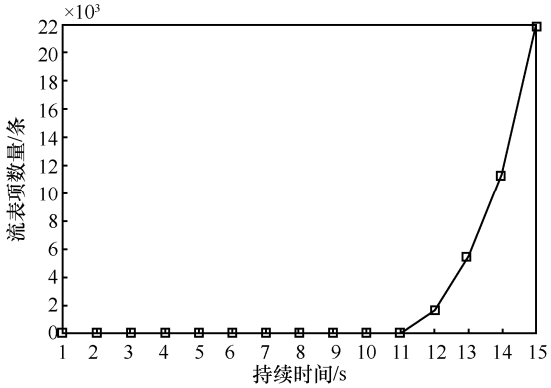

图 7　流规则数量变化

由实验结果分析可知，在攻击起始时，攻击流所影响到的流表资源不足以影响正常通信，随着攻击的进行，虚拟交换机中流表规则逐渐增加，可用流表空间资源与网络带宽资源逐渐减少，在 15s 后，统计程序无法获取流表信息，可能流表空间已经溢出。不同控制器在流表溢出后的 table_miss 处理方式不同，一种丢掉新来的数据分组，造成拒接服务的影响，另一种用新规则替换旧规则，这 2 种情况都会使分组丢失率显著增加[13]。攻击路径上的各交换机中大量流规则的存在，也增加了其对比查找正确规则的计算开销，还可能会导致目标服务器的拒绝服务（由于本文分析的攻击方法只会对一条链路

上的虚拟机产生影响，如果服务器相邻对接的虚拟交换机不是唯一的，经过其他交换机的请求是可以正常访问的）。

基于以上相关的攻击分析以及实验验证，可以验证数据平面低速率 DDoS 攻击在云环境下的有效性。

4　低速率 DDoS 攻击检测防御框架

4.1　框架介绍

检测框架主要由数据采集预处理模块、检测模块和防御模块组成，低速率 DDoS 攻击检测防御框架如图 8 所示。

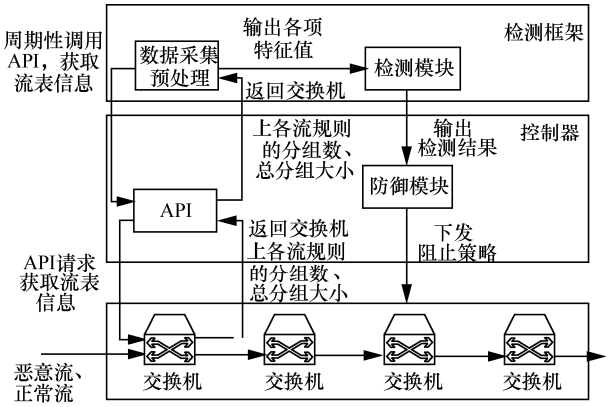

图 8　检测防御总体框架

首先是数据采集预处理模块。该模块主要通过调用支持 OpenFlow 协议的 OpenVSwitch 虚拟交换机的 API，获取虚拟交换机上流表的相关统计信息，再根据设置的采集窗口进行数据预处理并计算各项流量相关特征的值。然后将攻击流的各项特征值输入至检测模块，检测模块判定其是正常流量还是攻击流量。最后将攻击流量的六元组信息发送至防御模块，防御模块以应用的形式接入控制器，使控制器下发针对攻击流量的阻断及缓解策略。

4.2　数据采集预处理

数据采集预处理模块主要是通过控制器 API 读取流量的相关信息，对这些信息进行预处理，对每条流计算其各项特征值。数据采集点主要是在入口交换机上，可以支持多个入口交换机统一检测。

本文充分考虑针对控制平面与数据平面的低速率 DDoS 攻击特性，设置 2 个数据采集窗口。阿里云在其分析报告中指出[18]，近 80%的 DDoS 攻击持续时间不过 90 min，近 40%的 DDoS 攻击持续时间不超过 5 min。本文将第一个采集窗口设置为 5×10 s，在分钟级完成攻击的检测是合理的，主要针对控制平面的低速率 DDoS 攻击；第二个采集窗口设置为 5×idle_time，主要针对数据平面的低速率 DDoS 攻击。不同采集窗口得到的检测结果并不会影响对攻击的判断。

数据采集模块采集流表相关的信息为 match 匹配项中的 IP 地址、MAC 地址、端口号，以及数据分组的分组长度、数据分组数量、持续时间等。根据云环境中交换机流表不同的空闲超时时间，需要通过不同的采集周期进行数据采集，采集时间窗口设置为 T×idle_time，采集时间间隔为 idle_time。

作为检测方可以通过控制器配置文件获得空闲超时时间 idle_time，之后以 idle_time 为周期进行数据采集及预处理。

对于流表空闲超时时间 idle_time，本文进行合理假设。文献[19]指出在数据中心有 0.1%的流量的持续时间可以达到 200 s，大约 80%的流量持续时间约为 10 s。数据中心对于外网访问的流量会有一个统一的超时时间，基于以上 2 条假设本文将流的超时时间设置为 10 s，原始数据定义如下。

设采集时间窗口中进行第 i 次原始数据采集并预处理后数据为 f_i，那么源 IP 地址为 Sip_i，目的 IP 地址为 Dip_i，源 MAC 地址为 Smac_i，目的 MAC 地址为 Dmac_i，源端口为 Sport_i，目的端口为 Dport_i，持续时间为 $\mathrm{duration}_i$，流表空闲超时时间 idle_time，设相应流规则的数据分组数量为 fnum_i，相应流规则的数据总大小为 fsize_i。因流表中的数据为叠加值，所以在提取流初始数据时，需要时间窗口内的各采集点相减获取所需数据，则此数据流在采集时间窗口内第 i 次采集的数据分组数量表示为

$$\mathrm{Pnum}_i = \mathrm{fnum}_i - \mathrm{fnum}_{i-1} \tag{2}$$

数据分组长度表示为

$$\mathrm{Psize}_i = \frac{\mathrm{fsize}_i - \mathrm{fsize}_{i-1}}{\mathrm{Pnum}_i} \tag{3}$$

f_i 数据格式如式(4)所示。

$$\begin{aligned} f_i = \{&\mathrm{Sip}_i, \mathrm{Dip}_i, \mathrm{Smac}_i, \mathrm{Dmac}_i, \mathrm{Sport}_i, \\ &\mathrm{Dport}_i, \mathrm{Psize}_i, \mathrm{Pnum}_i, \mathrm{duration}_i\} \end{aligned} \tag{4}$$

4.3　基于贝叶斯网络的低速率 DDoS 检测方法

基于贝叶斯网络的低速率 DDoS 检测方法主要是区分攻击流量与正常流量。本文将前文所提到的针对控制平面的低速率 DDoS 攻击、针对数据平面的低速率 DDoS 攻击，统一划分为攻击流量，进行统一的检测与防御。考虑到攻击者可能使用非周期

性的攻击方式进行低速率 DDoS 攻击，本文将非周期性攻击的检测纳入检测范围。

4.3.1 特征提取

本文针对云环境 SDN 网络中低速率 DDoS 攻击在数据通信、攻击频率等方面的特性，以及频率可能进行的非周期性变化，提出了十维特征，并进行了相关验证，其中正常流量采集自校园网，攻击流量采用隐蔽性更强的数据平面低速率 DDoS 攻击。

1) 数据通信特性

在低速率 DDoS 攻击中，因攻击流通常是由脚本或工具产生，在攻击过程中人为干扰较少，一般认为攻击数据分组的数据分组负载基本不变，即数据分组长度基本不变，而对于正常流量来说数据分组长度的变化是无规律的。数据分组长度变化的程度可以区分攻击流量与正常流量，因此本文提出分组长度偏离度特征来描述变化程度的峰值，以及分组长度平均离差特征来描述总体变化程度的大小。

同时考虑到攻击成本及复杂程度，攻击数据分组负载较小，即数据分组的分组长度较小。而在正常流量中，需要传输业务信息，因此数据分组负载较大，一般情况下数据分组的分组长度要大于攻击流的数据分组的分组长度。攻击流数据分组的分组长度与正常流数据分组的分组长度存在明显差异，因此本文提出数据分组的分组长度均值特征及最大分组长度特征来描述这一特性。

基于上述分析，针对低速率 DDoS 攻击通信中的特性提出了数据分组的分组长度均值、最大分组长度、分组长度偏离度和分组长度平均离差这四维特征。相关特征的定义与验证性实验如下。

本文在多个采集点采集数据分组长均值为 $P\_size\_avg_k$，最大数据分组长 $P\_size\_max_k$，定义如式(5)与式(6)所示。

$$P\_size\_avg_k = \frac{\sum_{i=0}^{T} Psize_i}{T} \tag{5}$$

$$P\_size\_max_k = \max\{Psize_i\}, i = 1, \cdots, T \tag{6}$$

其中，$Psize_i$ 代表采集点采集到的数据分组长信息，T 代表了采集窗口内采集次数。特征的有效性验证如图 9 所示。正常流量的最大分组长度和分组长度均值、恶意流量的最大分组长度和分组长度均值有明显的差别，恶意流量的最大分组长度、分组长度均值大小基本不变。

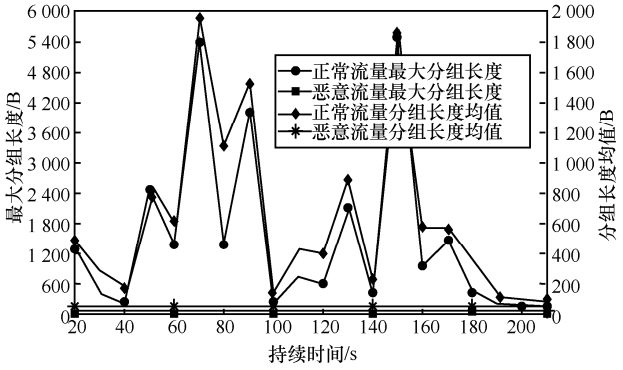

图 9 最大分组长度与分组长度均值变化

数据分组长偏差度 $P\_size\_dev_k$ 和数据分组长度平均绝对差 $P\_size\_avg\_MAD_k$ 定义如式(7)和式(8)所示。

$$P\_size\_dev_k = \frac{P\_size\_max_k - P\_size\_avg_k}{P\_size\_max_k} \tag{7}$$

$$P\_size\_avg\_MAD_k = \frac{\sum_{i=0}^{T} |Psize_i - P\_size\_avg_k|}{T} \tag{8}$$

其中，$P\_size\_max_k$、$P\_size\_avg_k$ 分别代表采集窗口内数据分组长最大值、数据分组长均值。实验验证如图 10 所示。正常流量的分组长度平均离差和分组长度偏差度、恶意流量的分组长度平均离差和分组长度偏差度有明显的差别。

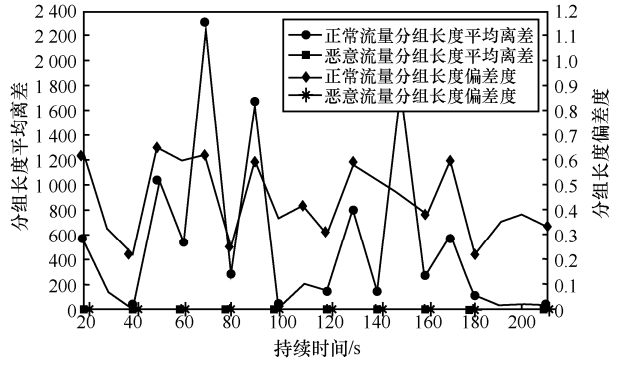

图 10 分组长度平均离差与分组长度偏差度变化

2) 数据频率特性

通常情况下，低速率 DDoS 攻击具有一定的周期性，利用脚本或工具产生的攻击流中攻击速率基本不变；正常流量中数据发送的速率没有规律性，在一段时间内数据分组发送速率变化程度较大。在一段时间内，攻击速率的变化程度可以区分攻击流量与正常流量，因此本文提出数据分组数量偏差度特征来描述变化程度的峰值，以及数据分组数量平均离差特征来描述该时段内数据分组发送速率的

总体变化程度的大小。

对于控制平面低速率 DDoS 攻击，在攻击时间内会持续发送大量的攻击数据分组，以洪泛的形式对目标造成攻击，为达到攻击效果，通常单位时间内攻击流数据分组数量会大于正常流数据分组数量。单位时间内数据分组数量可以用来区分攻击流量与正常流量，基于此本文提出了数据分组数量均值与最大分组数量特征来描述此特性。

考虑到攻击者可能发送具有一定程度非周期性的攻击流，在不改变攻击效果的前提下，这样的非周期性变化程度必须是较小的，其对于攻击特性上的影响较小，可以认为非周期性攻击特性与周期性攻击特性相似，同样与正常流量在通信、频率等特性上存在较大差异。

针对数据平面的低速率 DDoS 攻击通过恶意流规则长期占用流表空间，使流表空间溢出。在该攻击下，攻击流产生的流规则存活时间较长，一般情况下会远大于正常流规则的存活时间及交换机的空闲超时时间，而正常流量因业务的不同，存活时间大部分较短，在数据中心内约有 0.1%的正常流量其持续时间会达到 200 s，80%的流量持续时间会在 10 s 左右。流表中流规则的存活时间，可用于区分正常流量与攻击流量，本文提出存活时间特征及存活程度特征来描述这一特性。

基于上述分析，针对频率中的特性提出了数据分组数量均值、最大分组数量、数据分组数量偏差度、数据分组数量平均离差、存活时间及存活程这度六维特征。相关特征的定义与验证性实验如下。

本文在多个采集点采集数据分组数量均值、最大数据分组数量分别为 $P\_\text{num\_avg}_k$、$P\_\text{num\_max}_k$，如式(9)和式(10)所示。

$$P\_\text{num\_avg}_k = \frac{\sum_{i=0}^{T} \text{Pnum}_i}{T} \tag{9}$$

$$P\_\text{num\_max}_k = \max\{\text{Pnum}_i\}, i = 1,\cdots,T \tag{10}$$

其中，Pnum_i 代表采集点采集到的数据分组数量信息。实验验证如图 11 所示。正常流量的分组数量均值和最大分组数量的变化、恶意流量的分组数量均值和最大分组数量的变化有明显的差别。

数据分组数量偏差度 P_num_dev_k 及数据分组数量平均绝对差 P_num_avg_MAD_k 定义如式(11)和式(12)所示。

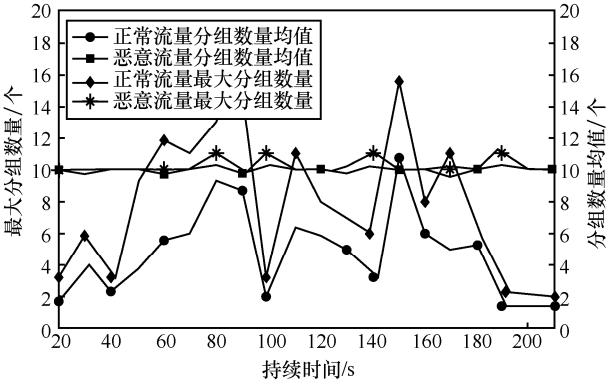

图 11　分组数量均值与最大分组数量变化

$$P\_\text{num\_dev}_k = \frac{P\_\text{num\_max}_k - P\_\text{num\_avg}_k}{P\_\text{num\_max}_k} \tag{11}$$

$$P\_\text{num\_avg\_MAD}_k = \frac{\sum_{i=0}^{T} \left|\text{Pnum}_i - P\_\text{num\_avg}_k\right|}{T} \tag{12}$$

其中，$P\_\text{num\_max}_k$、$P\_\text{num\_avg}_k$ 分别代表采集窗口内数据分组数量最大值、数据分组数量均值。实验验证如图 12 所示。正常流量的分组数量平均离差和分组数量偏差度变化、恶意流量的分组数量平均离差和分组数量偏差度变化有明显的差别。

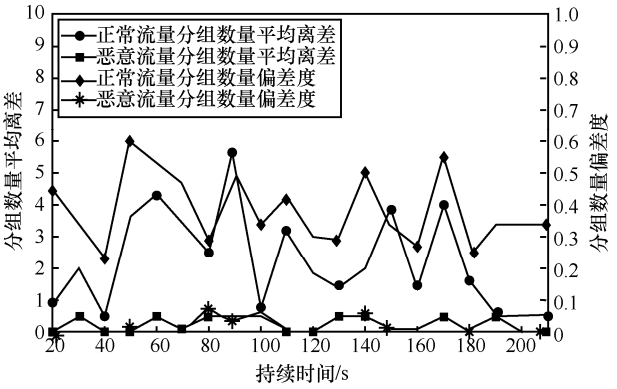

图 12　分组数量平均离差与分组数量偏差度变化

存活时间 duration_k 和存活程度 duration_degree_k 定义如式(13)和式(14)所示。

$$\text{duration}_k = \frac{\sum_{i=0}^{T} \text{duration}_i}{T} \tag{13}$$

$$\text{duration\_degree}_k = \frac{\text{duration}_k}{\text{idle\_time}} \tag{14}$$

其中，duration_i 代表采集点采集到的流规则持续时间，duration_k 代表采集窗口内流规则持续时间的均值，idle_time 代表该虚拟交换机空闲超时时间。

4.3.2 算法选择

本文十维特征的提取是通过人工方式来提取，检测算法主要测试监督学习中的分类算法，本文主要测试了 RandomForest 算法、BayesNet 算法、J48 决策树及 AdaBoostM1 算法，评价标准依据 F1-measure。各检测算法的评价结果如表 1 所示。

表 1 不同检测算法评价结果

检测算法	查准率	查全率	F1-measure
RandomForest	97.5%	97.4%	97.4%
BayesNet	99.7%	99.7%	99.7%
J48 决策树	86.2%	85.2%	85.1%
AdaBoostM1	83.5%	75.9%	74.4%

本文针对检测算法 F1-measure 值进行了初步筛选，并不对算法本身进行研究，因此选用 F1-measure 值最高的贝叶斯网络算法作检测算法。

4.4 防御方法

防御模块主要基于云环境下 SDN 网络集中控制的特性，以控制器应用的形式通过控制器下发相关策略来清洗恶意的流表规则及对恶意攻击流进行阻断，以此来缓解低速率 DDoS 攻击。检测模块在得到检测结果后提取攻击流的六元组基础信息（源 IP、源 MAC、源端口、目的 IP、目的 MAC、目的端口）发送给防御模块，防御模块使控制器对所监测的交换机下发相关策略拒绝攻击流的转发请求，同时依靠流修改事件(flow-modification)删除交换机上与攻击流相匹配的规则。

在检测防御框架中，除防御模块是作为应用连接控制器之外，数据采集预处理模块和检测模块安装部署在单独的物理节点上，必须保证其与控制器有完全的通信权限。

5 实验

本实验模拟云环境下 SDN 网络低速率 DDoS 攻击，分别进行了检测模型有效性实验、不同攻击模式下的检测模型评估及检测防御框架的性能测试。在本实验中将低速率 DDoS 攻击数据分为四大类进行采集：针对数据平面的周期性低速率攻击、针对控制平面的非周期性低速率攻击、针对数据平面的周期性低速率攻击以及针对控制平面的非周期性低速率攻击。

低速率 DDoS 攻击类型选择了 TCP 类型攻击、UDP 类型攻击、Http Head 攻击和 Http Body 攻击这 4 种低速率攻击类型，其中 TCP 和 UDP 这 2 种类型的攻击方式通过修改 hping3 工具发送攻击流量，Http Head 和 Http Body 攻击通过修改 SlowHttpTest 慢速 Http 攻击工具发送模拟攻击流量，正常流量采用某高校校内网用户访问的正常流量。

5.1 实验环境

本实验搭建了基于 OpenStack 的云计算平台作为实验云环境。实验一共使用 3 台物理服务器，其中，一台服务器作为控制节点且部署了 RYU 4.20 控制器，其余 2 台服务器作为计算节点，虚拟交换机采用 OpenvSwitch v2.5，OpenFlow 协议采用 OpenFlow1.3，虚拟机操作系统采用 ubuntu14.04 系统，虚拟核数为 2，内存为 4 GB。本文为了实验数据采集的便利性，将 5 台虚拟机作为攻击主机，一台搭建 Web 服务的虚拟机作为目标服务器，一台作为检测服务器，提供数据采集、检测及将检测结果发送至防御模块的功能，通过 2 台虚拟交换机进行连接，实验拓扑如图 13 所示。

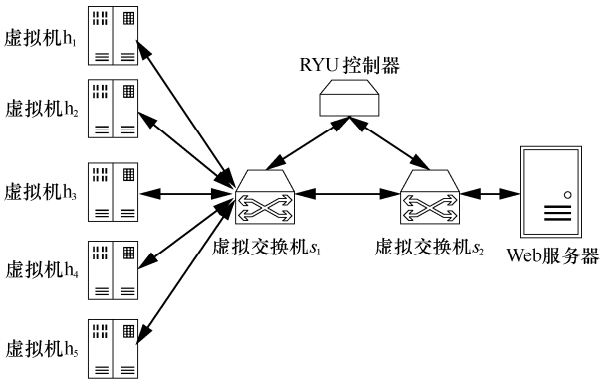

图 13 云环境下 SDN 网络低速 DDoS 攻击实验拓扑结构

5.2 实验数据

针对控制平面的低速率 DDoS 攻击数据中，TCP 类型攻击和 UDP 类型的低速率 DDoS 攻击攻击速率设置为每秒 100 个（数据分组数），Http Head 和 Http Body 攻击攻击速率设置为每秒 100 条（连接数），攻击周期为 1 s，数据采集窗口设置为 5×10 s，即 50 s。TCP 类型和 UDP 类型的非周期性低速率 DDoS 攻击的攻击速率设置为每秒发送 50~100 个数据分组，Http Head 和 Http Body 攻击的攻击速率设置为每秒发送 50~100 条连接。

在针对数据平面的低速率 DDoS 攻击数据中，假设虚拟交换机空闲超时时间为 10 s，攻击者通过逼近机制将估计的空闲超时时间作为攻击周期，攻击周期为 9 s。TCP 类型和 UDP 类型的低速率 DDoS 攻击速率设置为每 9 秒 100 个（数据分组数），Http

Head 和 Http Body 攻击的攻击速率设置为每 9 秒 10 条（连接数），攻击周期为 9 s。数据采集窗口设置为 5×idle_time，即 50 s。TCP 类型和 UDP 类型的非周期性低速率 DDoS 攻击的攻击速率设置为 9 s 以内的随机时间每次发送 100 个数据分组，Http Head 和 Http Body 攻击的攻击速率设置 9 s 以内的随机时间每次发送 10 条连接。

正常流量原始数据为 50 000 条，针对控制平面与数据平面的攻击由 TCP、UDP、Http Head 和 Http Body 类型的攻击组成，原始数据皆为 12 500 条，各类型攻击内包含周期性与非周期性的混合攻击。经预处理后，正常流量样本为 10 000 条，控制平面以及数据平面的低速率 DDoS 的 TCP、UDP、Http Head 和 Http Body 类型攻击流量样本各为 2 500 条，各类型攻击内包含周期性与非周期性的混合攻击。以上数据的混合比例皆为 1:1。

5.3　实验结果分析

实验分为两部分，其中实验 1 主要测试对 TCP、UDP 等不同类型的低速率 DDoS 攻击的检测效果；实验 2 主要测试在周期性低速率 DDoS 攻击下同类型检测方法的检测效果，以及对周期性与非周期性混合低速率 DDoS 攻击的检测效果。

5.3.1　评价标准

检测模型通过基于贝叶斯网络的检测算法对上述数据进行检测分析，评价标准主要为查准率（precision）、查全率（recall）、漏警率（MA, missing alarm）、虚警率（FA, false alarm）、F1-measure 值，相关指标的表示对应如式(15)~式(19)所示。同时本文声明将 F1-measure 作为本文的检测率，并对比分析查准率、查全率和 F1-measure。

$$\text{precesion}=\frac{\text{TP}}{\text{TP+FP}} \tag{15}$$

$$\text{recall}=\frac{\text{TP}}{\text{TP+FN}} \tag{16}$$

$$\text{MA}=\frac{\text{FN}}{\text{TP+FN}} \tag{17}$$

$$\text{FA}=\frac{\text{FP}}{\text{TP+FP}} \tag{18}$$

$$\text{F1-measure}=\frac{2}{\frac{1}{\text{precision}}+\frac{1}{\text{recall}}} \tag{19}$$

5.3.2　实验 1

首先分别对 TCP、UDP、Http Head 和 Http Body 这 4 种类型的低速率 DDoS 攻击进行检测。为了贴近真实攻击环境，将周期性攻击流量与非周期性攻击流量混合检测，同时设置攻击流量占比为 4%、8%、12%、16%、20%，分别对各类型低速率 DDoS 攻击进行分析，结果如图 14 所示。

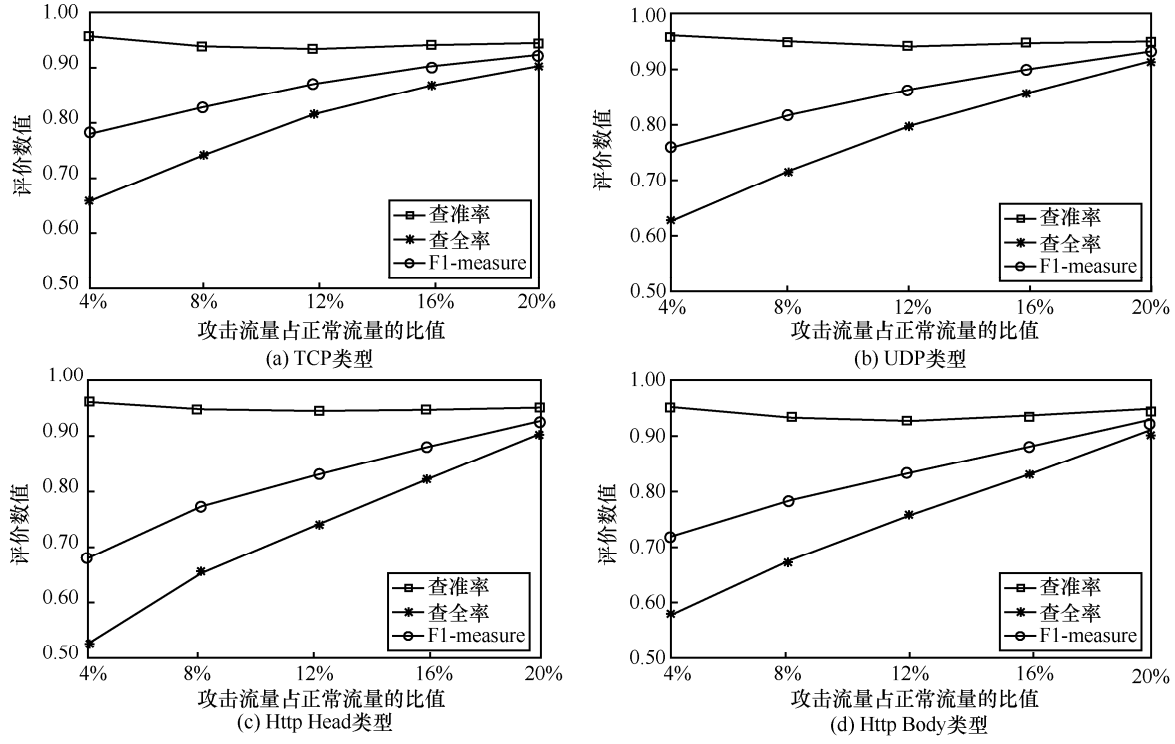

图 14　各类低速 DDoS 攻击不同流量比的评价变化

在对低速率 DDoS 攻击的检测中，TCP、UDP、Http Head 和 Http Body 这 4 种类型的低速率 DDoS 攻击的攻击流量占比在 20%时，其检测率均在 91%以上。当攻击流量占比为 4%时，TCP 和 UDP 类型攻击的检测率在 74%以上，Http Head 和 Http Body 类型的检测率分别为 68%和 71%。该检测模型可以对云环境下多类型的低速率 DDoS 攻击进行有效检测。

5.3.3 实验 2

周期性混合攻击流量包括了 TCP、UDP、Http Head 和 Http Body 这 4 种类型的周期性低速率 DDoS 攻击流量，各攻击数据量相同。同时设置攻击流量占比为 10%、15%、20%、25%、30%、35%、40%、45%、50%，分别对周期性混合攻击进行分析，结果如图 15 所示。

周期性混合低速率 DDoS 攻击流量占比为 50%时，检测率达到 99.6%，在极低的攻击流量占比为 10%时，检测模型检测率依旧能达到 90%以上，本文所提模型在攻击流量占比在 25%时，检测率可以达到 96%，可以有效地检测大部分情况下的攻击。

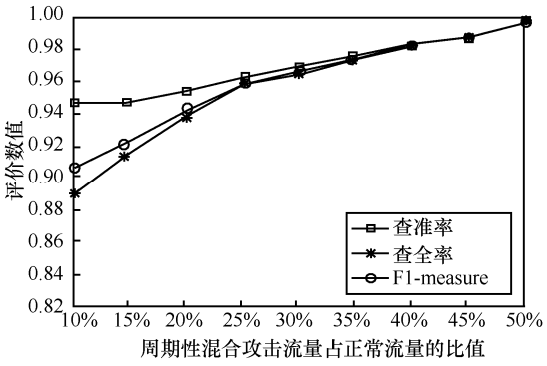

图 15 周期性混合攻击不同流量比的评价变化

将非周期性混合攻击流量及周期性混合攻击流量进行 1:1 的混合，各攻击数据量相同。同时设置攻击流量占比为 10%、15%、20%、25%、30%、35%、40%、45%、50%，分别对混合攻击进行分析，结果如图 16 所示。

混合低速率 DDoS 攻击流量占比为 50%时，检测率达到 95.5%，在极低的攻击流量占比为 10%时，对于混合攻击检测达到 87.99%。因为非周期性因素的影响，检测率会下降 4%。综上，本文的检测方法能够有效地检测出周期性低速率 DDoS 攻击及非周期性与周期性混合的低速率 DDoS 攻击，在攻击占比为 50%时检测效果分别达到了 99.6%和 95.5%。本文检测方法与基于联合特征的检测方法[11]和 SDCC[7]同类型周期性低速率 DDoS 攻击检测方法进行了对比分析，评价标准依据对比模型进行设计计算，主要有检测率、漏警率及虚警率，对比结果如表 2 所示。

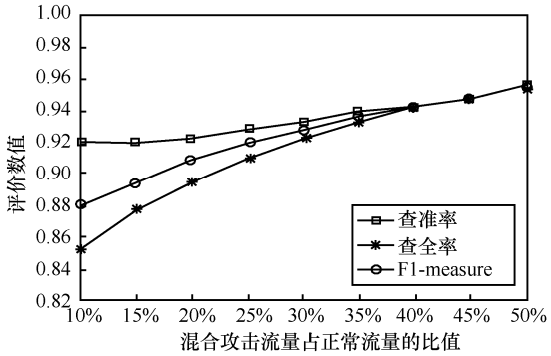

图 16 混合攻击不同流量比的评价变化

表 2 不同的检测方法结果对比

检测模型	检测率	漏警率	虚警率
基于联合特征的检测方法	96.68%	3.32%	3.89%
SDCC	—	—	2.5%
本文检测方法	99.6%	0.56%	0.10%

文献[11]的实验环境设置周期性低速率 DDoS 攻击流量占比为 50%，其检测率为 96.68%，漏警率与虚警率分别为 3.32%和 3.89%，而本文在同等条件下检测率为 99.6%，漏警率和虚警率分别为 0.56% 和 0.10%，检测效果有明显提升。这是由于文献[11]提出的联合特征之一的可用带宽百分比特征可能会对检测效果存在有一定的影响，当攻击处于初始阶段时，网络带宽的占用率会逐步升高，在该情况下，攻击时带宽占用率与正常带宽占用率的区分度不够明显，对攻击流进行特征提取的方法存在一定的不足之处。而本文针对单条攻击流的行为及通信特性进行建模检测，所建立的模型受整体流量特征（如可用带宽占比等）的影响较小，可以在攻击流量极低的环境下，依然能够有效地检测低速率攻击（在攻击流量占比为 25%时，检测率可以保持在 96%以上），与针对整个攻击流的检测方法相比，检测效果有明显提升。

文献[7]提出周期性低速率 DDoS 攻击流量占比在 50%时，触发为攻击状态，其发送分组密度为每秒 100 个时误判率为 2.5%左右，其定义的虚警率为正常数据分组判断成攻击分组的概率，而本文在攻击流量占比为 50%时，F1-measure 值达到了 99.6%，虚警率

为 0.22%，主要由于 SDCC 算法中属性值的权值需要人工根据实际情况设置，这可能会导致检测结果存在一定的误差。SDCC 方案为了提高数据处理速率，在不同的检测阶段会抽取不同比例的数据进行分析，当正常的业务流量存在突变情况时（如电商业务等），只抽取部分数据进行分析，可能会存在一定的误判情况。而本文的检测范围会覆盖全部的流量，对每条流的行为及通信特征进行分析检测以保证检测的准确性，同时通过控制器 API 采集流的统计信息等方式，与 SDN 框架结合紧密，保证整个检测框架的高效性。文献[7]在攻击流量占比在 25%以下时，判定为非攻击状态，而本文模型在 25%以下时，检测率能达到 95.8%；在攻击流量占比 10%时，检测率仍能达到 90.2%。

5.4　性能测试

对低速率 DDoS 攻击检测防御框架进行性能测试评估，主要监测框架在攻击前后的防御消解能力以及性能开销情况，检测模型的训练时间性能开销不在此范围内。

虚拟机流表 idle_time 设置为 10 s，5 个虚拟机使用每秒 100 个 UDP 类型数据分组以及每 9 秒 100 个 UDP 类型数据分组的混合攻击，测试时长为 90 min，10 s 时开始攻击持续，20 s 时开启检测防御功能，实验结果如图 17 所示。

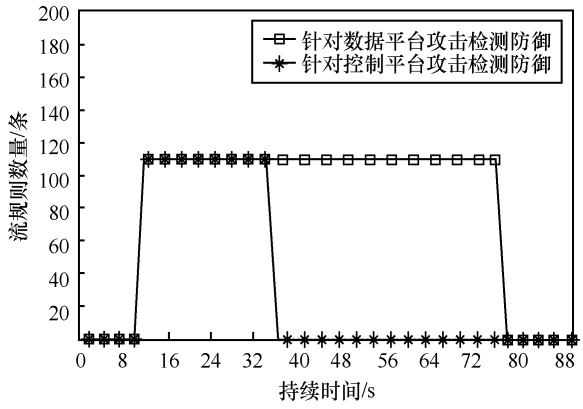

图 17　检测防御功能对流规则的消解

由实验结果所得，在 20 s 启动检测防御功能后，需要 8~9 s 的启动时间，在 35 s 时，针对控制器平面攻击的防御措施生效，下发阻断策略，可以将流表空间中 110 条流规则（包含部分回复流规则）降低至一条流规则；在 78s 时，针对数据平面攻击的防御措施生效，下发相应的阻断策略，同样能够将攻击流规则数量降低为一条流规则。在本实验中，检测防御框架能够在合理时间内对低速率 DDoS 攻击进行检测与防御。

在以上的实验基础上，对检测防御框架的内存资源消耗进行测试，测试时间为 70 s，1 s 时开启检测防御功能，如图 18 所示。

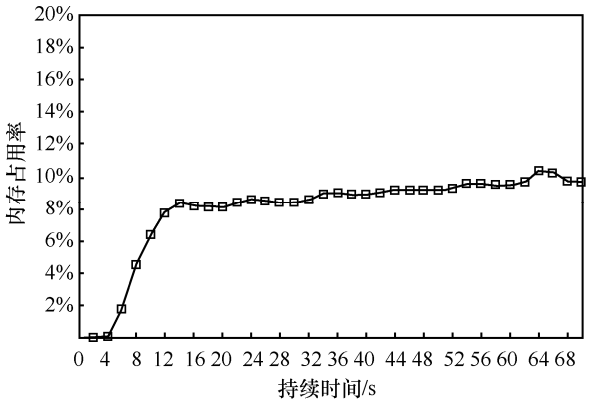

图 18　内存占用率变化

由实验结果可知，在开启检测防御功能时，内存占用率逐步升高，平均内存消耗为 9.04%，在 60s 时完成对攻击的检测并开始下发流表规则，内存消耗峰值为 10.7%，之后稳定在 9.7%，其在合理的资源消耗范围内，能够完成对攻击进行检测和消解，防止低速率 DDoS 攻击造成更大的破坏。

6　结束语

云环境下低速率 DDoS 攻击会占用数据中心大量的网络资源，降低被攻击者的服务质量，严重影响云计算平台和数据中心的正常运行。本文针对云环境 SDN 数据平面低速率 DDoS 攻击方式进行了详细的分析，验证了攻击的有效性，之后详细分析低速率 DDoS 攻击在通信、频率上的特性并提取了十维特征，基于贝叶斯网络实现了对低速率 DDoS 攻击的有效检测。在此基础上，提出了云环境下 SDN 网络中低速率 DDoS 攻击统一检测框架，同时采用相关攻击工具，基于真实正常流量在 OpenStack 云环境中进行了测试。测试结果表明，在攻击流量占比为 50%时，对周期性低速率 DDoS 的检测率达到 99.6%，与同类型检测方法相比提高了 2.92%，对非周期性低速率 DDoS 的检测率达到 95.5%，在百兆带宽环境下，检测防御框架以 9.7%的 CPU 性能消耗完成攻击的检测与消解。检测防御框架能够对云环境下低速率 DDoS 攻击进行有效的检测与防御。同时，本文的检测框架有着高度的可扩展性与可移植性，完全适用于云环境。

随着云计算技术的不断发展，云环境中业务流量不断增加，控制器的服务压力越来越大，单控制器的 SDN 网络架构无法满足正常的业务需求，多控制器的 SDN 网络架构将会逐渐发展。因此，本文未来将对多控制器下的攻击信息的采集以及控制器间攻击信息的共享方式进行进一步研究，同时对控制器策略下发过程优化进行研究。

参考文献：

[1] TRUNG V. Phan, Minho Park: efficient distributed denial-of-service attack defense in SDN-based cloud[J]. IEEE Access, 2019(7): 18701-18714.

[2] VICENTINI C, SANTIN A, VIEGAS E, et al. SDN-based and multitenant-aware resource provisioning mechanism for cloud-based big data streaming[J]. Journal of Network and Computer Applications, 2019(126): 133-149.

[3] HONG K, KIM Y, CHOI H, et al. SDN-assisted slow HTTP DDoS attack defense method[J]. IEEE Communications Letters, 2018, 22(4): 688-691.

[4] KREUTZ D, RAMOS F M V, VERISSIMO P. Towards secure and dependable software-defined networks[C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. ACM, 2013: 55-60.

[5] SAHOO K S, PUTHAL D, TIWARY M, et al. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics[J]. Future Generation Computer Systems, 2018(89): 685-697.

[6] LUKASEDER T, MAILE L, ERB B, et al. SDN-assisted network-based mitigation of slow DDoS attacks[J]. Secure Communication, 2018(2):102-121.

[7] 何亨, 胡艳, 郑良汉,等. 云环境中基于 SDN 的高效 DDoS 攻击检测与防御方案[J]. 通信学报, 2018, 39(4):139-151.
HE H, HU Y, ZHENG L H, et al. Efficient DDoS attack detection and prevention scheme based on SDN in cloud environment[J]. Journal on Communications, 2018, 39(4): 139-151.

[8] 刘孟. 云环境下 DDoS 攻防体系及其关键技术研究[D]. 南京:南京大学, 2016.
LIU M. Research on DDoS attack and defense system and key technologies in cloud environment[D].Nanjing: Nanjing University, 2016.

[9] WANG W, KE X, WANG L. A HMM-R approach to detect L-DDoS attack adaptively on SDN controller[J]. Future Internet, 2018, 10(9): 83.

[10] CHEN Z , JIANG F , CHENG Y , et al. XGBoostclassifier for DDoS attack detection and analysis in SDN-based cloud[C]//IEEE International Conference on Big Data and Smart Computing. IEEE Computer Society, 2018: 251-256.

[11] 吴志军, 张景安, 岳猛,等. 基于联合特征的LDoS攻击检测方法[J]. 通信学报, 2017, 38(5):19-30.
WU Z J, ZHANG J A, YUE M, et al. Approach of detecting low-rate DoS attack based on combined features[J]. Journal on Communications, 2017, 38(5): 19-30.

[12] KLOTI R, KOTRONIS V, SMITH P. OpenFlow: a security analysis[C]//The IEEE International Conference on Network Protocols. IEEE, 2013:1-6.

[13] 乔思祎, 胡成臣, 李昊. OpenFlow 交换机流表溢出问题的缓解机制[J]. 计算机学报,2018,41(9):2003-2015.
QIAO S Y, HU C C, LI H. Mitigation mechanism of flow table overflow problem in OpenFlow switch[J]. Chinese Journal of Computers, 2018, 41(9): 2003-2015.

[14] KANDOI R, ANTIKAINEN M. Denial-of-service attacks in OpenFlow SDN networks[C]//IFIP/IEEE International Symposium on Integrated Network Management. IEEE, 2015: 1322-1326.

[15] GUDE N, KOPONEN T, PETTIT J, et al. NOX: towards an operating system for networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(3):105-110.

[16] KUZMANOVIC A. Low-rate TCP-targeted denial of service attacks (the shrew vs. the mice and elephant)[J]. Proceedings ACM SIGCOMM, 2003(3):75-86.

[17] 王文涛, 王玲霞, 黄烨. SDN 环境下基于 Renyi 熵的低速率分布式拒绝攻击的检测[J]. 中南民族大学学报(自然科学版), 2017, 36(3):131-136.
WANG W T, WANG L X, HUANG Y. Detection of low rate distributed denial of attack based on Renyientropy in SDN environment[J].Journal of Central South University for Nationalities (Natural Science Edition), 2017, 36(3):131-136.

[18] 阿里云创新实验室.阿里云安全报告[R].阿里云创新实验室, (2018-09) [2018-12-26].
ALIYUN LABS. Aliyun security report[R]. Aliyun Labs, (2018-09) [2018-12-26].

[19] KANDULA S, SENGUPTA S, GREENBERG A, et al. The nature of data center traffic: measurements & analysis[C]//ACM SIGCOMM Conference on Internet Measurement. ACM, 2009:202-208.

[作者简介]

陈兴蜀（1968− ），女，贵州六枝人，博士，四川大学教授、博士生导师，主要研究方向为云计算与大数据安全、可信计算与信息保障。

滑强（1993− ），男，山西阳泉人，四川大学硕士生，主要研究方向为云计算与大数据安全。

王毅桐（1987− ），男，四川成都人，四川大学博士生，主要研究方向为云计算与大数据安全。

葛龙（1976− ），男，江苏丹阳人，四川大学博士生、讲师，主要研究方向为云计算与大数据安全。

朱毅（1991− ），男，四川内江人，四川大学网络空间安全研究院科研助理，主要研究方向为网络安全、大数据分析。