doi:10.11959/j.issn.1000-436x.2016268

基于熵变的多租户云内 DDoS 检测方法研究

王淼[1,2]，王利明[1]，徐震[1]，马多贺[1]
（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 100093；
2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：分布式拒绝服务（DDoS）是攻击者通过入侵云内虚拟机组成攻击网络，以威胁多租户云系统安全的攻击。多租户云系统 DDoS 攻击检测难点在于如何确定攻击源虚拟机和攻击目标，尤其当攻击目标为云内主机时。提出一种基于熵度量的 DDoS 攻击检测方法，根据云环境特点在优先定位攻击源基础上再确定攻击目标，检测多租户云系统内发起的 DDoS 攻击。提出分布式检测架构，利用检测代理发现潜在攻击源端的可疑攻击流量，检测服务器识别 DDoS 攻击的真正攻击流。理论和实验分析验证了提出方法的可行性和有效性。
关键词：分布式拒绝服务攻击；攻击检测；多租户；云计算系统；熵
中图分类号：TP302 **文献标识码**：A

Research on DDoS detection in multi-tenant cloud based on entropy change

WANG Miao[1, 2], WANG Li-ming[1], XU Zhen[1], MA Duo-he[1]
(1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093,China;
2. College of Cyberspace Security, University of Chinese Academy of Sciences, Beijing 100049, China）

Abstract: An attacker compromised a number of VMs in the cloud to form his own network to launch a powerful distributed denial of service (DDoS) attack. DDoS attack is a serious threat to multi-tenant cloud. It is difficult to detect which VM in the cloud are compromised and what is the attack target, especially when the VM in the cloud is the victim. A DDoS detection method was presented suitable for multi-tenant cloud environment by identifying the malicious VM attack sources first and then the victims. A distributed detection framework was proposed. The distributed agent detects the suspicious VM which generate the potential DDoS attack traffic flows on the source side. A central server confirms the real attack flows. The feasibility and effectiveness of the proposed detection method are verified by experiments in the multi-tenant cloud environment.
Key words: DDoS attack, detection, multi-tenant, cloud computing system, entropy

1 引言

多租户云系统将“租户”概念引入云计算系统，允许租户间资源共用并确保不同租户的数据相互隔离[1,2]。随着云计算技术飞速发展，多租户云系统日渐普及。但由于技术本身不成熟，多租户云系统面临着一些安全威胁。攻击者通过网络或其他攻击方法成功入侵云内的若干虚拟机组成攻击平台[3,4]，在某个特定时间向一个或多个目标发动 DDoS 攻击，耗费受害主机和网络的大量资源，造成严重且恶劣的影响[5,6]。由于云系统网络结构和僵尸网络结构类似，云内虚拟机容易成为攻击者组建攻击网络

收稿日期：2016-08-20
通信作者：王利明，wangliming@iie.ac.cn
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016106）；中国科学院先导专项基金资助项目（No.XDA06010701, No.XDA06010306）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016106), Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDA06010701, No.XDA06010306)

的首选目标，而且云系统内部防御措施并不强健，攻击者掌握一台虚拟机更容易入侵云内其他虚拟机。DDoS 攻击严重威胁多租户云系统安全。为了保障云内网络安全，需要有效地检测方法发现云内 DDoS 攻击，多租户云系统的 DDoS 攻击检测有其特有的特点。

传统网络的 DDoS 攻击检测集中在攻击目标，当遭受攻击的受害者的某些特征指标发生改变，则认为攻击发生，其检测难点在于如何定位攻击源。由于攻击源在互联网中广泛分布，防御者无法获取攻击源所在的网络状态信息，源地址欺骗技术也给 IP 溯源带来巨大挑战。但是在云计算系统中，攻击源在云计算系统内部，管理者有机会探知虚拟机的网络行为。但是，虚拟租户网络作为云计算系统网络格局中的一种特殊存在形式，增加了 DDoS 攻击的检测难度：1) 网络虚拟化技术实现了网络资源的复用，部署在相同节点的不同租户的虚拟机可以共享同一个 IP 地址，使识别发送流量的源端变得困难；2) 租户的虚拟机运行在不同节点，资源部署分散，流量监控范围扩大。这些问题给定位云内攻击源和识别攻击目标带来挑战。

为了解决上述问题，本文提出一种基于熵度量的多租户云系统 DDoS 攻击检测方法。通过计算各节点虚拟机的流量熵，并根据熵变幅度识别可疑攻击源和可疑攻击流。使用相对熵作为可疑流相似性的评估指标，进一步确认真实 DDoS 攻击流。这种检测方法可以快速定位云内攻击源，能够区别 DDoS 攻击流和合法突发流量，提高检测准确性。基于上述检测方法提出一种分布式检测架构，包括一个运行在控制节点的中心检测服务器和一系列运行在计算节点的分布式检测代理，易于扩展的检测架构使其适用于任意规模的云计算系统。

2　背景及相关工作

2.1　DDoS 攻击检测方法

DDoS 攻击检测的目标主要有以下 2 点[7]：1) 发现已经发生的或正在进行的 DDoS 攻击；2) 发现更多的受害者、攻击者和攻击途径等相关信息，以防御下一次 DDoS 攻击。

为了实现上述目标，研究学者提出了一系列 DDoS 攻击检测方法。数据分组属性特征通常作为检测参数帮助有效识别 DDoS 攻击。Feinstein 等[8]选取源、目的 IP 地址、端口号和报文长度等属性识别异常行为。TTL 记录了数据分组从源端到目的端经过的跳数，可以检测和防御源地址欺骗攻击[9,10]。Gavaskar 等[11]提出了三计数器算法通过统计不同四元组（源、目的 IP 地址和端口号）的 SYN 数据分组检测 TCP SYN 洪泛攻击。Rai 等[12]通过收集 TCP SYN、PUSH 标识位等流量统计数据实现实时的 HTTP 异常检测。

基于信息论的度量方法可以克服 DDoS 攻击检测的局限性。计算属性的香农熵[13]是一种属性特征量化方法，熵变是许多异常流量检测的度量依据[8,14]。David 等[15]提出了一种基于流分析的快速熵方法，通过比较多项式时间内的熵值变化实现统计检测。信息熵距离可以用来区分攻击流量和合法流量[16,17]。Xiang 等[16]通过改变通用熵阶数找到 2 个新的信息度量参数，计算不同路由器的熵距和以检测 DDoS 攻击，假定可以控制所有路由器，在网络实现攻击回溯。Monowar 等[17]进行重复实验比较高速和低速 DDoS 攻击的不同检测方法，验证了每种熵度量检测方法的有效性。Yuan 等[18]使用 Sibson 距离区分局域网内的 DDoS 攻击流量和正常流量。Ain 等[19]提出 2 种等级相关方法识别恶意流量和合法流量的线性相关性，通过比较相关系数检测低速 DDoS 攻击。

2.2　熵度量参数

2.2.1　信息熵

信息熵用于度量随机变量的期望，定量表示变量的不确定性。随机变量 s 的取值集合为 $S=\{s_1,s_2,\cdots,s_n\}$，取值的概率分布为 $P=\{p_1,p_2,\cdots,p_n\}$，是独立分布，其中，$\sum_{i=1}^{n} p_i =1$, $0\leqslant p_i\leqslant 1$, $i\in(1,\cdots,n)$，变量 s 的信息熵为

$$H=-\sum_{i=1}^{n} p_i \mathrm{lb} p_i \tag{1}$$

对于一个流量样本，数据分组某些属性的概率分布可以反映流量特征，信息熵是一种常用的特征量化方法[7]。

2.2.2　相对熵

相对熵，也称为熵距，用来描述 2 个概率分布间的相似性。2 个离散概率分布 $P=\{p_1,p_2,\cdots,p_n\}$和 $Q=\{q_1,q_2,\cdots,q_n\}$，其中，$\sum_{i=1}^{n} p_i=\sum_{i=1}^{n} q_i=1$, $0\leqslant p_i\leqslant 1$, $0\leqslant q_i\leqslant 1$, $i\in(1,\cdots,n)$，P 和 Q 的相对熵公式为

$$D(P\|Q)=\sum_{i=1}^{n} p_i \mathrm{lb}\frac{p_i}{q_i} \tag{2}$$

相对熵也称作 Kullback-Leibler 距离。D 值越大表示 P 和 Q 的概率分布越不同。但对于大多数测试样本，$D(P||Q) \neq D(Q||P)$。为了便于比较，Kullback-Leibler 距离可以扩展为

$$D(P, Q)=D(P||Q)+D(Q||P)=\sum_{i=1}^{n}(p_i-q_i)\mathrm{lb}\frac{p_i}{q_i} \quad (3)$$

对于任意 2 个流，式(3)用来评估流分布的相似性。

3 DDoS 攻击检测算法

在云计算系统中，管理者能够掌握云内全部动态，可以探知虚拟机所有网络行为。所以，与传统网络 DDoS 攻击检测顺序相反，云内攻击检测应该始于攻击源止于攻击目标，以便在攻击规模形成之前发现攻击迅速定位攻击源，并采取应急措施。基于此提出 2 种 DDoS 攻击检测算法，虚拟机流量熵算法从攻击源端检测潜在 DDoS 攻击的可疑攻击流；流量相对熵算法识别可疑攻击流中的真正攻击流。本文做出如下合理假设：1) 一个僵尸网络发动 DDoS 攻击时产生攻击数据分组的方式相同；2) 同一时间可以有多个攻击者发起 DDoS 攻击，即云内可以存在多个僵尸网络。

3.1 云内 DDoS 攻击模型

如图 1 所示，攻击者通过系统漏洞、软件漏洞等入侵云内虚拟主机后，在云内实施拒绝服务攻击的过程如下。

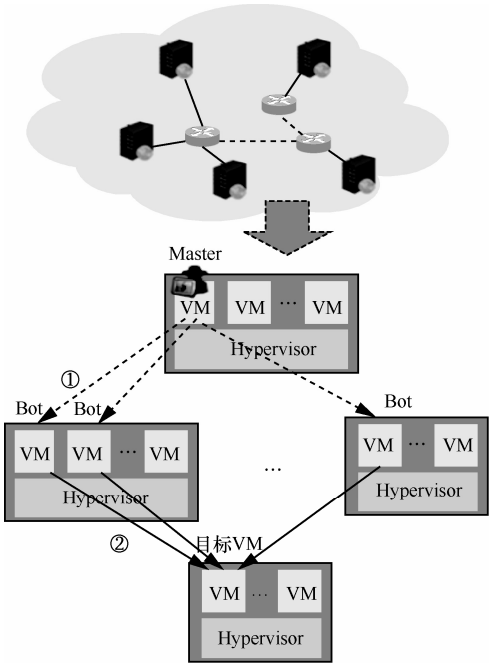

图 1 云内 DDoS 威胁模型

①在云内传播僵尸程序，成功感染云内虚拟机形成僵尸网络。

②下发指令控制僵尸虚拟机，发动 DDoS 攻击目标虚拟机。

3.2 虚拟机流量熵算法

云内多个虚拟机组成攻击网络，向一个或多个目标发动 DDoS 攻击，大量流量流向同一目标导致目的地址为攻击目标的数据分组突增。根据这个特征，基于目的地址统计一个时间间隔内虚拟机发送的数据分组数。虚拟机出流量的目的地址取值集合为 $A=\{a_1,a_2,\cdots,a_n\}$，相应的数据分组统计数据为 $N=\{n_1,n_2,\cdots,n_n\}$，虚拟机流量的地址概率分布为

$$p(a_i)=\frac{n_i}{\sum_{j=1}^{n}n_j} \quad (4)$$

虚拟机流量熵是地址概率分布的信息熵，计算式为

$$H(A)=-\sum_{i=1}^{n}p(a_i)\mathrm{lb}p(a_i) \quad (5)$$

当虚拟机与外界正常通信时，流量熵在一个很小的范围内变化；当虚拟机发动 DDoS 攻击时，流量熵会迅速减小。当变化量超过特定阈值，虚拟机有可能发动了 DDoS 攻击。基于此，提出一种基于虚拟机流量熵的检测算法，通过监控虚拟机流量熵随时间的变化率检测可疑攻击流。具体如下。

算法 1 虚拟机流量熵算法

输入 δ_1 为检测阈值

输出 可疑流信息

1) 初始化采样周期 $T=\{t_1,t_2,\cdots,t_m\}$，采样频率 f，滑动时间窗 $W=\{w_1,w_2,\cdots,w_n\}$，其中，n 为窗口大小；

2) 代理从虚拟交换机采样周期 T 内的虚拟机出流量，根据目的 IP 地址统计时间间隔 t_i 的数据分组；

3) 使用式(4)计算虚拟机流量的地址概率分布，使用式(5)计算时间周期 T 内的虚拟机流量熵；

4) 如果时间 T_i 到时间 T_{i+1} 的流量熵减少量超过阈值 δ_1，代理输出可疑攻击流信息，将可疑攻击流统计数据发送给检测服务器；

5) 返回步骤 2)。

3.3 流量相对熵算法

合法突发流量会引起虚拟机流量熵突变，流量相对熵算法可以将 DDoS 攻击流量从可疑流量中区分出来。已经假设攻击流的特征相同，攻击流在时

序上的概率分布是相似的，而攻击流和合法突发流是不同分布，通过计算流量时序分布概率的相对熵，可以识别 DDoS 攻击的攻击流量。当 2 个可疑流量的相对熵小于给定阈值，它们是攻击流量；一个流量和其他所有可疑流量的相对熵都大于给定阈值，则该流量是合法突发流量。

对一个流，每个时间间隔内的数据分组数为 $N=\{n_1,n_2,\cdots,n_n\}$，其时序概率分布为

$$p(t_i)=\frac{n_i}{\sum_{j=1}^{n} n_j} \tag{6}$$

2 个流的时序概率分布为 P 和 Q，它们的相对熵计算公式为

$$D(P,Q)=\sum_{i=1}^{n}(p(t_i)-q(t_i))\mathrm{lb}\frac{p(t_i)}{q(t_i)} \tag{7}$$

相对熵检测算法 2 如下所示。

算法 2　流量相对熵算法

输入　可疑流统计数据，检测阈值 δ_2

输出　DDoS 攻击告警信息

1) 初始化 2 个缓存空间 S_1 和 S_2，一个用于存储可疑流信息，一个用于存储攻击信息；

2) 服务器将接收的可疑攻击流存储到缓存空间 S_1；

3) 聚集目的地址相同的可疑流，聚集结果对应的可疑攻击流占总可疑攻击流的比例高于设定阈值，则该聚集结果对应的可疑攻击流判定为潜在攻击流；

4) 使用式(6)计算可疑流的时序概率分布，使用式(7)计算 2 个潜在攻击流的相对熵；

5) 如果相对熵小于给定阈值 δ_2，2 个流为攻击流，将攻击信息存储到缓存空间 S_2；如果一个流和其他可疑流的相对熵都大于给定阈值 δ_2，则为合法流量；

6) 将缓存空间 S_2 的攻击信息告警给系统；

7) 返回步骤 2)。

注意，经过反复实验测试确定阈值 δ_1 和 δ_2，以提高准确性，降低误报率。

4　DDoS 攻击检测系统架构

图 2 所示为分布式多租户云系统 DDoS 攻击检测架构，它是实验测试平台的基础，下面将描述基于开源云平台 OpenStack 的系统实现方法。基于此系统架构可以监控整个租户网络，形成监

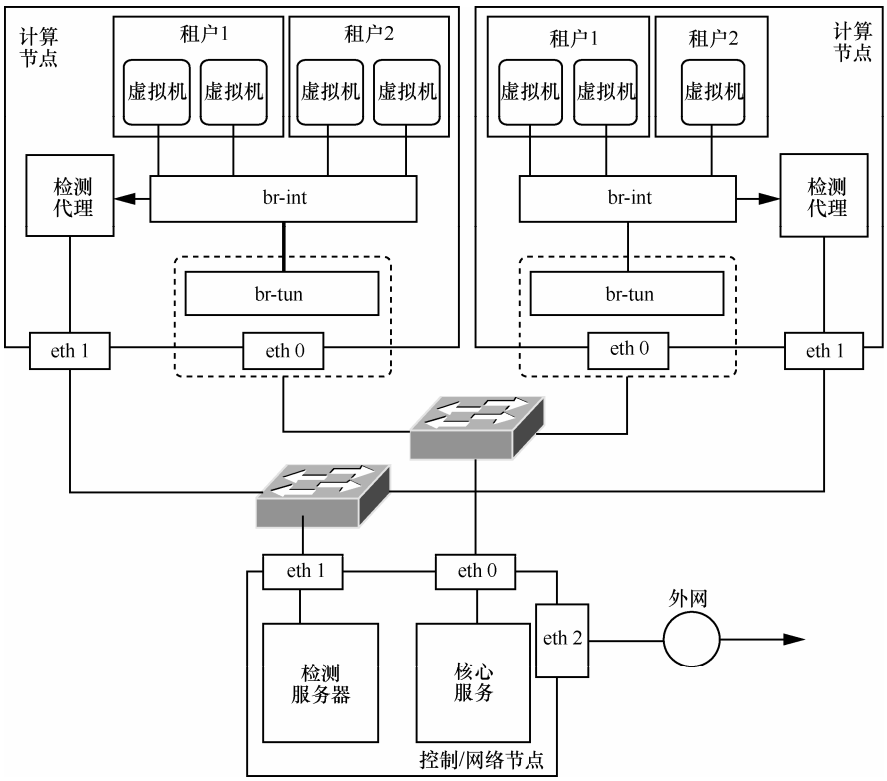

图 2　分布式多租户云系统 DDoS 攻击检测系统架构示意

控统计数据为攻击检测算法提供输入。图 2 中包含 3 个节点：1 个控制/网络节点和 2 个计算节点。控制/网络节点运行核心云服务，计算节点承载多个虚拟机实例并通过专用的虚拟交换机实现它们的网络连接。检测系统采用分布式的系统架构，检测代理嵌入计算节点，检测服务器运行在控制节点。

4.1 检测代理

检测代理运行在每个计算节点收集虚拟机流量统计数据并检测可疑攻击流。代理从虚拟交换机采样虚拟机发送的流量，为每个虚拟机组织流量特征统计数据，以目的 IP 地址为基准统计数据分组数。代理通过采样数据附加的网络设备信息区分不同虚拟机流量，解决 IP 地址重叠和源地址欺骗问题。如图 3 所示，使用一个按时间增序的缓存队列存储监控数据，连续时间间隔的统计数据存储在相应的队列节点上。一个固定大小的时间窗向时间增序方向滑动，时间窗内的数据将作为检测算法 1 的输入，时序小的数据优先被处理，每处理完一组数据，时间窗向前滑动一次。

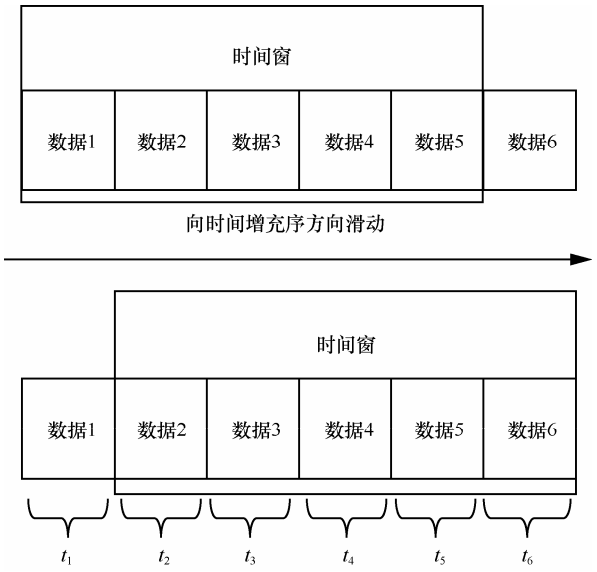

图 3 数据存储模型示意

当检测到可疑攻击流时，代理提取时间窗内的可疑流监控数据，附加虚拟机信息封装成 UDP 数据分组并通过独立的网络发送给检测服务器，这些数据将被服务器进一步处理。

4.2 检测服务器

中心检测服务器从分布式代理接收可疑流统计数据，使用检测算法 2 识别真正的攻击流量以提高检测准确性。服务器维护 2 个存储空间，一个用于存储可疑流统计数据，超出时间范围的可疑流数据将被定期删除；另一个用于存储检测输出的攻击相关信息，检测到新的攻击后服务器产生告警信息生成日志，将攻击信息上报给系统。

5 实验评估

5.1 实验环境

基于第 4 节提出的系统架构，在实验室云平台建立 DDoS 攻击检测系统。每个计算节点运行一个检测代理，检测代理实现了虚拟机流量熵算法检测潜在 DDoS 攻击的可疑攻击流量。检测服务器部署在控制节点，实现流量相对熵检测算法识别真正攻击流并定位攻击源虚拟机和攻击目标。云平台运行着不同租户的许多虚拟机，每个虚拟机运行自己的服务，正常流量是虚拟机服务交付和云平台管理控制产生的通信流量。使用网络安全工具 hping 模拟攻击流量，产生符合正态分布的突增流量，改变正态分布的期望和标准差模拟不同的突发流量。

5.2 虚拟机流量熵算法评估

检测代理每 5 s 采样一次虚拟机流量并计算流量熵，图 4 展示了正常网络状态下 6 台虚拟机的流量熵波动情况。分别选择虚拟机 1、2、3 的前 50 条流和虚拟机 4、5、6 的前 100 条流反映虚拟机流量的地址分布概率情况，用于计算虚拟机流量熵。图 5 为时间维度上的虚拟机熵变范围，明显发现熵变在 X 轴上下波动且幅度不超过 0.2。因此，检测阈值 δ_1 设置为 0.2，如果虚拟机流量熵的减小量大于 0.2，则认为虚拟机可能发动了 DDoS 攻击。

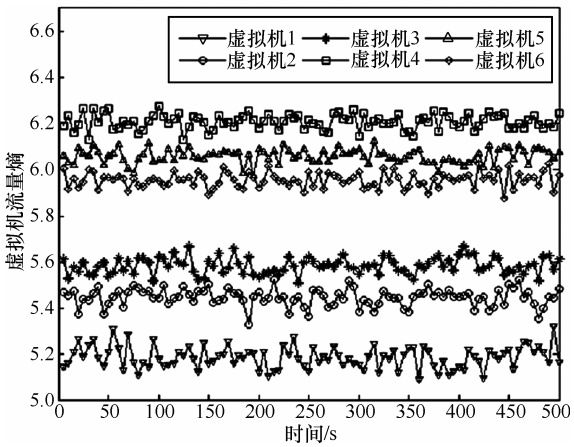

图 4 正常网络场景下的虚拟机流量熵波动

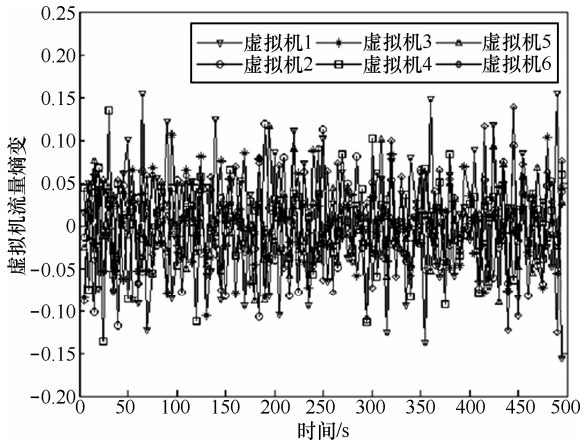

图 5　正常网络场景下的虚拟机流量熵变

上述 6 台虚拟机作为攻击源模拟 DDoS 攻击，使用同一个攻击工具 hping 产生相同攻击模式的攻击流。检测代理根据网络设备信息区分虚拟机流量可以识别源地址欺骗攻击。图 6 为攻击场景下虚拟机流量熵曲线，曲线下凸部分为攻击时刻，攻击持续了 30 s，当攻击开始时，虚拟机流量熵突然明显减小；当攻击结束后，虚拟机流量熵突然增大到原水平。图 7 描述了攻击场景下熵变情况，攻击开始时流量熵减少量超过 0.2，大于检测阈值 0.2；攻击过程中熵变平稳变化；攻击结束时流量熵超过 0.2。流量熵的突然减小和增大可以分别作为 DDoS 攻击开始和结束的标志。

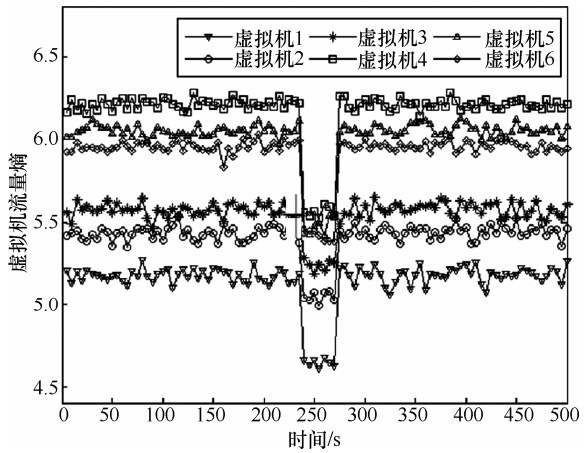

图 6　DDoS 攻击场景下的虚拟机流量熵波动

5.3　流量相对熵算法评估

正常突发流量也会引起流量熵剧烈变化，下面将证明相对熵检测算法可以区分 DDoS 攻击流量和正常突发流量。使用不同期望和标准差的正太分布，选择云内 10 台虚拟机产生突发流量，上述 6 台虚拟机产生 DDoS 攻击流量。检测代理检测到这些可疑流，将统计信息发送给检测服务器，服务器计算每 2 个可疑流的相对熵。图 8 为攻击流和其他可疑流的相对熵，X 轴坐标编号为 1 至 6 的流为攻击流，编号为 7 至 16 的流为合法突发流量。同一 DDoS 攻击的攻击流间的相对熵很小接近于 0，攻击流和突发流量的相对熵是较大的数值。相对熵反映出不同流量间的相似性，可以识别 DDoS 攻击的攻击流量，和正常突发流量有所区分。

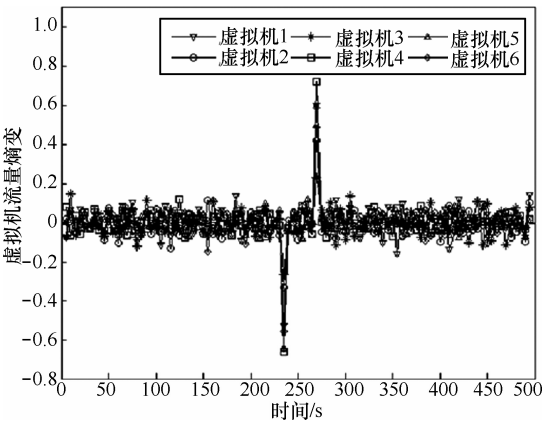

图 7　DDoS 攻击场景下的虚拟机流量熵变

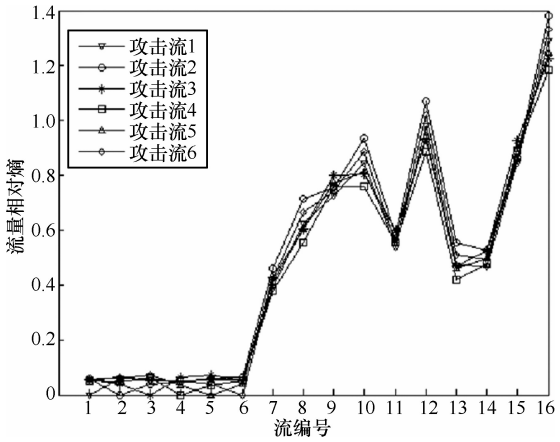

图 8　攻击流量和正常突发流量的相对熵

每个流上附加了虚拟机信息，检测服务器识别攻击流后可以迅速定位攻击源虚拟机，并发送警告信息通知检测代理密切监控相关虚拟机，通过攻击流目的地址可以发现攻击目标。该检测方法基于攻击模式，所以适用于多攻击目标的 DDoS 攻击。攻击告警信息将被发送给系统以协助攻击防御，这样，成功建立一套多租户云系统 DDoS 攻击检测机制，能够在攻击规模形成之前发现攻击采取应对措施。

6　结束语

本文提出了一种基于攻击源到攻击目标检测

顺序的多租户云系统 DDoS 攻击检测方法，使用 2 种熵度量参数，使用虚拟机流量熵发现源端的可疑攻击流量，使用流量相对熵识别 DDoS 攻击的真正攻击流。提出一种分布式的检测架构，可以监控整个云计算系统，检测代理和检测服务器分别实现检测算法 1 和检测算法 2，实现完整的攻击检测机制，在攻击规模形成之前迅速定位攻击源和攻击目标并采取应对措施。实验验证了 DDoS 攻击检测方法的可行性和有效性。该 DDoS 攻击检测方法适用于多攻击目标的 DDoS 攻击检测，通过区分攻击流量和合法突发流量提高了检测准确性，检测系统的分布式架构使其适用于任意规模的云计算系统。

参考文献：

[1] Amazon Inc. Amazon elastic compute cloud (Amazon EC2)[EB/OL]. http://aws.amazon.com/ec2/, 2011.

[2] CHOWDHURY N M M K, BOUTABA R. A survey of network virtualization[J]. Computer Networks, 2010, 54(5): 862-876.

[3] HASHIZUME K, ROSADO D G, FERNÁNDEZ-MEDINA E, et al. An analysis of security issues for cloud computing[J]. Journal of Internet Services and Applications, 2013, 4(1): 1.

[4] JASTI A, SHAH P, NAGARAJ R, et al. Security in multi-tenancy cloud[C]//2010 IEEE International Carnahan Conference on Security Technology (ICCST). 2010: 35-41.

[5] MIRKOVIC J, REIHER P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[6] PENG T, LECKIE C, RAMAMOHANARAO K. Survey of network-based defense mechanisms countering the DoS and DDoS problems[J]. ACM Computing Surveys (CSUR), 2007, 39(1): 3.

[7] BHUYAN M H, KASHYAP H J, BHATTACHARYYA D K, et al. Detecting distributed denial of service attacks: methods, tools and future directions[J]. Computer Journal, 2013, 57(4):537-556.

[8] FEINSTEIN L, SCHNACKENBERG D, BALUPARI R, et al. Statistical approaches to DDoS attack detection and response[C]//DARPA Information Survivability Conference and Exposition. 2003, 1: 303-314.

[9] YI F, YU S, ZHOU W, et al. Source-based filtering scheme against DDOS attacks[J]. International Journal of Database Theory and Application, 2008, 1(1): 9-20.

[10] CHOUHAN V, PEDDOJU S K. Packet monitoring approach to prevent DDoS attack in cloud computing[J]. International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN. 2013: 2315-4209.

[11] GAVASKAR S, SURENDIRAN R, RAMARAJ D E. Three counter defense mechanism for TCP SYN flooding attacks[J]. International Journal of Computer Applications, 2010, 6(6): 0975-8887.

[12] RAI M K, MISHRA V S. Detection of UDP and HTTP anomalies on real time traffic based on NIDS using OURMON tool[J]. 2015.

[13] SHANNON C E. A mathematical theory of communication[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2001, 5(1): 3-55.

[14] KUMAR K, JOSHI R C, SINGH K. A distributed approach using entropy to detect DDoS attacks in ISP domain[C]//2007 International Conference on Signal Processing, Communications and Networking. IEEE, 2007: 331-337.

[15] DAVID J, THOMAS C. DDoS attack detection using fast entropy approach on flow-based network traffic[J]. Procedia Computer Science, 2015, 50: 30-36.

[16] XIANG Y, LI K, ZHOU W. Low-rate DDoS attacks detection and traceback by using new information metrics[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(2): 426-437.

[17] BHUYAN M H, BHATTACHARYYA D K, KALITA J K. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection[J]. Pattern Recognition Letters, 2015, 51: 1-7.

[18] TAO Y, YU S. DDoS attack detection at local area networks using information theoretical metrics[C]//2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2013: 233-240.

[19] AIN A, BHUYAN M H, BHATTACHARYYA D K, et al. Rank correlation for low-rate DDoS attack detection: an empirical evaluation[J]. International Journal of Network Security, 2016, 18(3): 474-480.

作者简介：

王淼（1991-），女，河北廊坊人，中国科学院信息工程研究所硕士生，主要研究方向为云安全、网络与系统安全。

王利明（1978-），男，内蒙古赤峰人，博士，中国科学院信息工程研究所副研究员，主要研究方向为网络与系统安全、云安全、通信安全等。

徐震（1976-），男，山西大同人，博士，中国科学院信息工程研究所正高级工程师、博士生导师，主要研究方向为数据库安全、网络与系统安全、智能设备安全、云安全等。

马多贺（1982-），男，安徽六安人，博士，中国科学院信息工程研究所信息安全国家重点实验室助理研究员，主要研究方向为网络安全、云安全、拟态安全、移动目标防御等。