



融合 DDoS 威胁过滤与路由优化的 SDN 通信质量保障策略

张家华¹, 杨种学¹, 王江平¹, 史煜凯¹, 魏 亮²

(1. 南京晓庄学院数学与信息技术学院 南京 211171; 2. 江苏省未来网络创新研究院 南京 211100)

摘 要: 提出了将 DDoS 威胁识别与路由优化有机结合的软件定义网络(SDN)通信质量保障策略,即在 DDoS 攻击造成部分网络链路拥塞的情况下,对异常数据分组进行识别过滤,同时生成最优路径,以保障网络通信质量。首先,设计了一种 SDN 架构下的分布式入侵检测系统,实现了对欺骗报文、异常报文以及破坏报文 3 类 DDoS 威胁的检测识别和过滤处理。其次,实现了一种最优路径的生成算法。实验测试结果表明,部署了通信质量保障策略的 SDN 可有效识别并滤除 DDoS 攻击数据分组,且处理过程中网络平均传输时延无激增。

关键词: 软件定义网络;网络安全;路由优化;分布式拒绝服务攻击;威胁过滤

doi: 10.11959/j.issn.1000-0801.2015053

SDN Communication Quality Assurance Strategy with DDoS Defense and Routing Optimization

Zhang Jiahua¹, Yang Zhongxue¹, Wang Jiangping¹, Shi Yukai¹, Wei Liang²

(1. School of Mathematics and Information Technology, NanJing Xiaozhuang University, Nanjing 211171, China;

2. Jiangsu Future Networks Innovation Institute, Nanjing 211100, China)

Abstract: A SDN communication quality assurance strategy which organic combines DDoS threat identification with route optimization was put forward. It means, when the intent link was congestive attacked by DDoS, it will identify and filter the abnormal data packet, and will generate optimized routing to ensure the quality of network communications. First of all, a distributed intrusion detection system under SDN framework was designed. The system realizes the detection recognition, filtration and treatment about the DDoS threat, such as cheating message, excepting message and destroying message. Secondly, a kind of best algorithm about generating routing path was realized. The experimental result shows that the network deployment plan which mentioned in this paper, can identify and filter the aggressive data packet, and the average network data transmission delay doesn't increase sharply when the network is under attack.

Key words: software defined networking, network security, routing optimazation, distributed denial of service, threat filtering

收稿日期:2014-12-09;修回日期:2015-02-02

基金项目:未来网络前瞻性研究项目(No.BY2013095-3-11),江苏省大创重点项目(No.201411460009Z),南京晓庄学院科研基金(No.2013NXY04)

Foundation Items: Future Network Prospective Research Project (No.BY2013095-3-11), Innovation and Training Major Project of Jiangsu (No.201411460009Z), Nanjing Xiaozhuang University Fund (No.2013NXY04)

论文引用格式:张家华,杨种学,王江平等.融合 DDoS 威胁过滤与路由优化的 SDN 通信质量保障策略,电信科学,2015053

Zhang J H, Yang Z X, Wang J, *et al.* SDN communication quality assurance strategy with DDoS defense and routing optimization. Telecommunications Science, 2015053



1 引言

当前,高速广泛连接的网络已经成为现代社会的重要基础设施。然而,随着互联网规模的逐渐膨胀,传统规范体系的缺陷也日益呈现^[1,2]。国家计算机网络应急技术处理协调中心(CNCERT/CC)最新发布的报告表明,黑客活动日趋频繁,网站后门、网络钓鱼、Web 恶意挂马等攻击事件呈大幅增长趋势,国家、企业的网络安全性面临着严峻挑战。

其中,分布式拒绝服务攻击(distributed denial of service, DDoS)是影响互联网运行安全最主要的威胁之一。在过去的几年里,DDoS 攻击的数目、规模、类型都大幅上涨^[3-5]。

软件定义网络(software defined networking, SDN)具有可实时更新路由策略与规则、支持深层次的数据分组分析等特性^[6],因而可针对复杂网络环境中的 DDoS 威胁提供更迅速、更准确的网络监控及防御功能。

例如,针对 SYN flood 等淹没式攻击,参考文献[7]提出了一种 Avant-Guard 执行触发器策略,将部署了安全策略的 SDN 交换机作为第一道防御线,设定时间阈值并实时记录来自一个或多个攻击源的威胁数据分组,然后可通过不同处理模式的切换控制 Avant-Guard 交换机丢弃数据分组,或重定向到流量清洗设备。参考文献[8]提出了一种 FRESCO 应用架构,其攻击威胁检测基于自定义脚本实现,具有较好的业务伸缩性。上述两种策略实现了集控式的威胁数据识别与处理,但由于其连接迁移过程会造成较大的时延,无法保证网络通信的实时性。

针对 DDoS 攻击等造成部分网络链路拥塞的情况,参考文献[9]提出了一种 SDN 按需智能路由系统。参考文献[10]提出了一种 OpenFlow 网络的 FortNox 安全策略执行内核,可实现异常流量的重定向。但由于上述方案的检测和策略下发两个环节都为集控式处理架构,对控制平面的资源消耗过大,无法应用于规模庞大或结构复杂的网络环境。

本文针对 DDoS 威胁的特点,提出一种融合 DDoS 威胁过滤与路由优化的 SDN 通信质量保障策略(SDN communication quality assurance strategy, SDNQA)。本方案的突出特点是将 DDoS 威胁监测、威胁防护、路由优化等业务功能模块分别部署于数据平面、控制平面和应用平面。可使网络在遭受大规模 DDoS 威胁时,根据链路的实时状况实现路由优化的流量转发,同时迅速准确地进行 DDoS 威胁识别和处理响应,全面保障网络通信质量。

2 SDNQA 的思想

2.1 SDNQA 网络架构

SDNQA 在现有数据平面上进行了拓展。在数据平面引入了分布式入侵检测系统(distributed intrusion detection system, DIDS)监测实时流量中的攻击行为,在控制平面实现了基于流表控制的 DDoS 攻击流威胁处理和正常数据的路由优化策略。SDNQA 架构如图 1 所示。

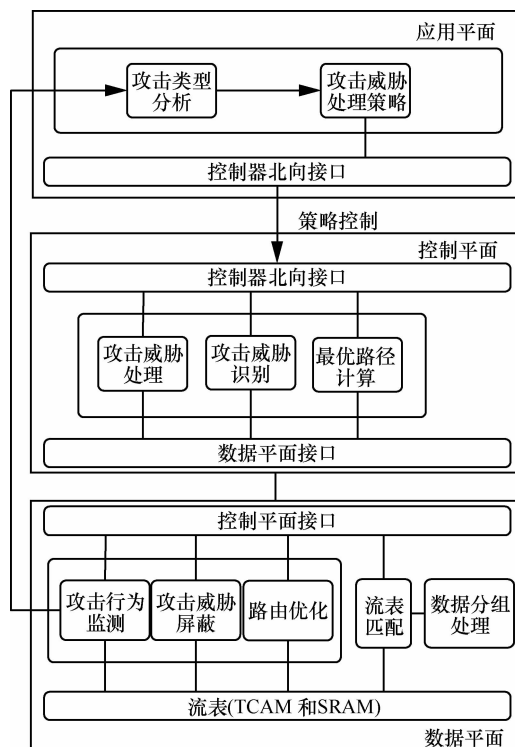


图 1 SDNQA 架构

在 SDNQA 架构下,控制平面向上为应用平面提供攻击威胁处理的功能业务接口,向下为数据平面提供最优路径计算和攻击威胁识别两大业务接口。其中,最优路径计算业务接口基于改进的 Dijkstra 算法实现,攻击威胁识别业务接口基于 DIDS 对攻击行为的监测规则进行定义。

当数据平面 DIDS 检测到攻击威胁时,将通知应用平面进入攻击类型分析流程。随后,在控制器端生成攻击威胁处理策略,并通过所部署的威胁处理业务接口进行策略下发,实现对攻击威胁的溯源屏蔽。

在数据平面上,网络的局部拥塞通常发生在遭受 DDoS 攻击或产生大流量正常数据的情况下。控制平面能根据网络的实时状况计算出实时最优路径,将用户的正常数据分组通过最优路径进行转发。

SDNQA 架构的特点在于,基于 SDN 标准架构扩展了 OpenFlow 协议,开发了“分布式入侵检测系统”,实现了对威胁数据分组的过滤以及对攻击程序或者攻击主机的屏蔽;并且可基于控制器对链路剩余带宽等网络参数进行实时感知,在网络拥塞时生成数据分组的最优传输路径。

2.2 SDNQA 架构特征

在 SDN 环境下,SDNQA 架构的实现及系统特征如图 2 所示。在 SDNQA 架构中,DDoS 攻击行为检测由各自网域内分布式部署的 IDS 设备进行实时监测。IDS 设备一经发现符合 DDoS 攻击特征的行为,即通过 SSL (secure sockets layer) 通信信道上报应用平面的决策服务器。决策服务器立即分析 IDS 设备上报的信息,并制定出处理对应攻击威胁的策略。然后通过控制器的北向接口 (north bound interface, NBI) 将这些攻击流屏蔽或者重定向到流量清洗中心,对这些异常用户发出的攻击数据分组进行过滤,以确保正常用户所使用的网络资源不被侵占。

SDNQA 架构不仅可以防护 DDoS 攻击,也可以通过控制层面定义和下发更多的安全检测规则,从而构建由分布式 IDS 设备、决策服务器及控制器组成的 SDN 智能防火墙系统。

3 SDNQA 策略设计与实现

SDNQA 是一个端到端的网络防护方案,具体如图 3 所示。为满足该防护方案的业务功能需求,需在 SDN 控制器端开发部署新的组件策略,以实现转发设备、IDS 决策服务器和分布式 IDS 设备的协同调度。例如,基于 SDN 控制器的可编程北向接口和拓扑感知功能,实现网络链路状态感知、流路径计算、SDN 域边界点识别、镜像流机制、基于命令规则的实时流量监测等策略。

3.1 网络初始化

要实现本文所述的 SDNQA 架构,控制器、决策服务器以及 IDS 设备需要感知网络状态并进行初始化。其主要步骤如下。

首先,决策服务器与每个 IDS 设备建立专用的 SSL 通信信道。该信道是应用层面的决策服务器与 IDS 设备的专用安全通信信道,数据层面其他设备无权通过这个信道与决策服务器进行交互。

其次,控制器构造网络设备信息绑定表,并将网络设备信息绑定表实时更新到 IDS 设备中。其中所述的网络设备信息绑定表,是指由在 OpenFlow 域中的所有主机(除去

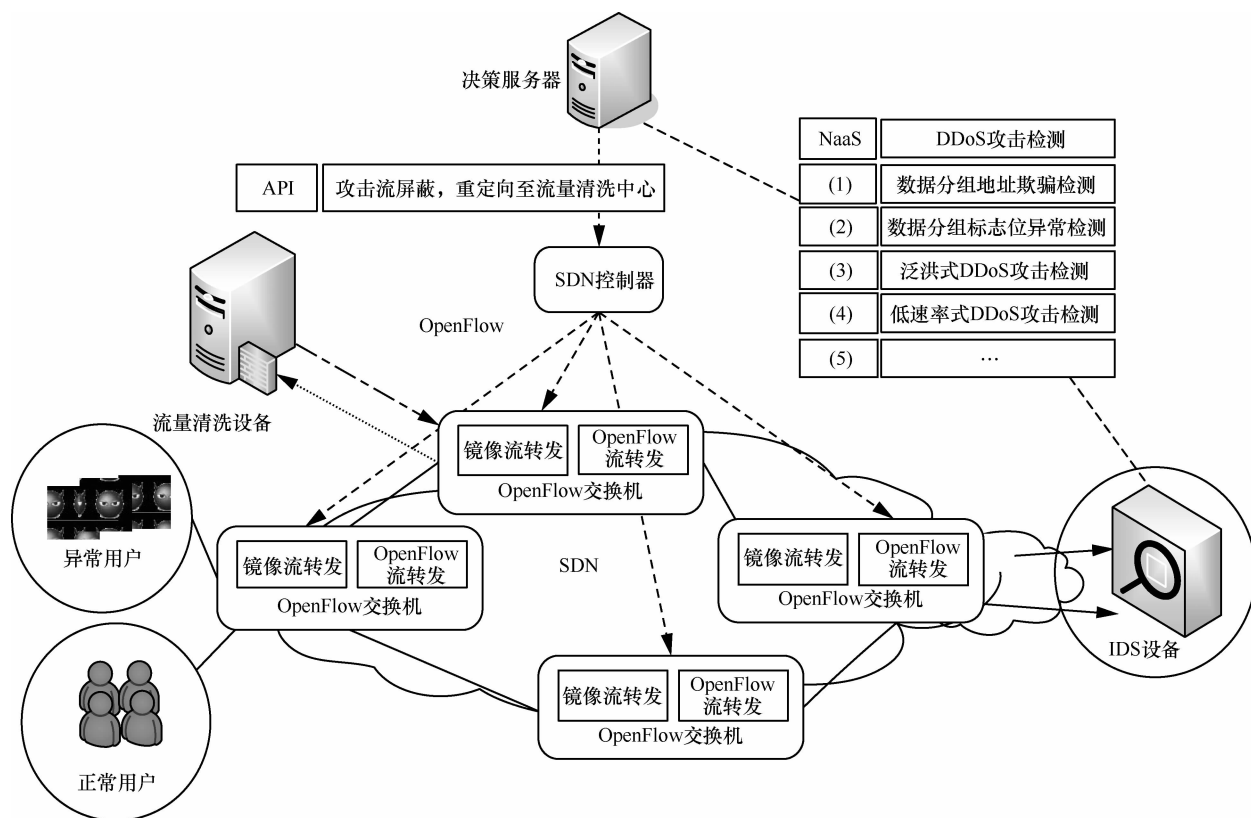


图 2 SDNQA 架构的实现及系统特征

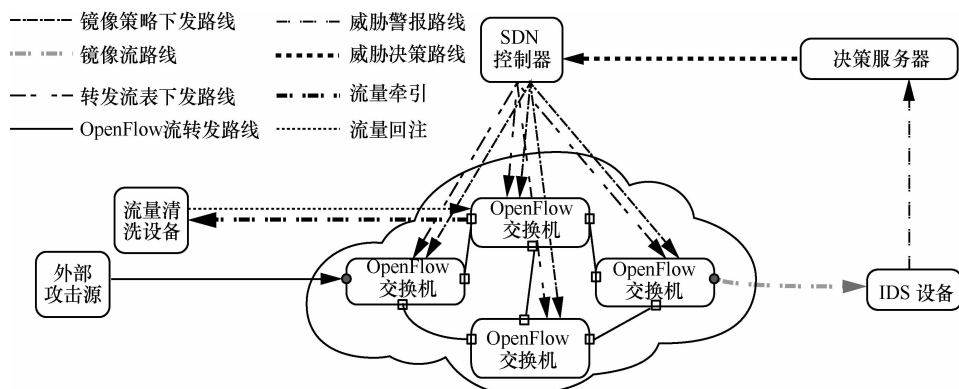


图3 SDNQA 架构处理流程

IDS设备)的IP地址、MAC地址、VLAN以及所接入的交换机的DPID和端口号作为绑定的记录表。

再次,控制器下发镜像策略的流表。将OpenFlow交换机所有拖载有主机的端口流量镜像转发给网域内对应的IDS设备。其中,镜像流表是指交换机查找流表匹配后,动作是mirror的流表。mirror动作意味着这条流表不但继续进行正常的数据转发,同时也将被复制一份发送到IDS设备,IDS设备将对这些网络流量进行实时的监测与分析。

最后,控制器下发DDoS威胁识别规则给每个网域中对应的IDS设备。分布式的IDS设备将协同监测DDoS的攻击行为。

3.2 分布式DDoS威胁监测

参考文献[8]中的DDoS攻击检测方案是在控制器端进行的攻击威胁检测,对于网络地址欺骗的欺骗报文攻击和数据分组标志位设置异常的破坏报文攻击,可以直接在控制器端直接识别,但对于使用傀儡机直接进行的攻击需要定时查询交换机中流表的计数器才能检测出来,这无疑给OpenFlow控制通道造成很大的负载压力,同时也给控制器造成了很大的处理压力。本文提出的方案将这些DDoS攻击威胁的监测任务均匀地派发给各个网域内的IDS设备,从而大大减少控制层面的负担,以保障网络更安全、高效地运行。

其中,IDS设备对攻击行为的监测基于对数据分组的实时分析。主要包括3个步骤,分别为欺骗报文检测、破坏报文检测和异常报文检测。3个检测步骤依次对每个数据分组进行检测,具体如图4所示。

若任一步骤检测不通过,IDS设备将向决策服务器上报告攻击源和攻击类型等信息。决策服务器接收到上报信息后,立即分析上报信息中所述的攻击威胁,并制定出处理对应攻击威胁的策略。

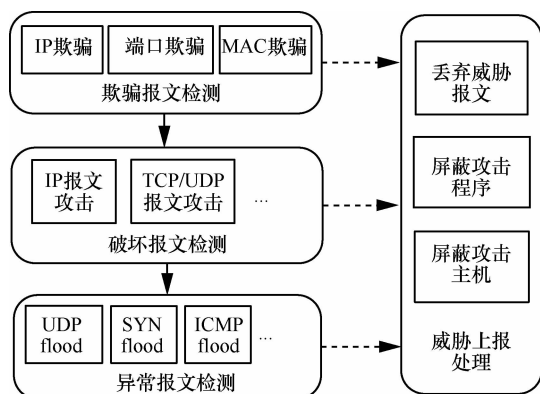


图4 分布式IDS设备威胁检测流程

3.2.1 欺骗报文检测

由于当前互联网没有完全部署对使用伪造源地址的报文进行过滤的机制,并且路由器对报文的转发只是基于报文的目的地址,这些报文一般情况下可以正常到达目的地。因此,通过伪造报文源地址可以发起更具隐蔽性的DDoS攻击行为,使得在攻击过程中和攻击后很难追溯到真正的攻击源。

SDNQA中的分布式IDS设备的第一道关卡主要针对上述伪造报文源地址的欺骗报文进行检测。欺骗报文检测单元首先对报文消息队列中当前所处理的报文进行解析,以获得相应的源IP地址、MAC地址以及此报文的发送交换机的DPID和端口号,并将上述各信息分别与网络设备信息绑定表中的相应信息进行比对。若报文中的上述信息与网络设备信息绑定表中的记录匹配,则将报文转入接下来的破坏报文检测步骤;若报文中的上述信息不能匹配网络设备信息绑定表,则向决策服务器上报告攻击源和攻击类型等信息,由决策服务器制定处理该攻击威胁的策略。

其中,网络设备信息绑定表中各条记录需要跟随网络配置参数的变化进行实时刷新(如交换机端口高/低电平

的跳变, port down / port up), 以保证网络设备信息绑定表中记录的可靠性。

3.2.2 破坏报文检测

以典型的 ping of death 攻击为例, 其攻击原理是攻击者故意发送大于 65 535 byte 的 IP 数据分组给目标系统。TCP/IP 的特征之一是碎片化, 允许 IP 分组分为若干个更小的数据分组。攻击者正是利用此特征, 使碎片分组可以将整个 IP 分组的大小增加到 IP 地址允许的 65 535 byte 以上。

当目标系统接收到全部分段并重组报文时, 总的长度超过了 65 535 byte, 就会导致内存溢出, 使主机出现内存分配错误而导致 TCP/IP 堆栈崩溃。此种攻击的特征是只需少量攻击分组即可将目标系统瘫痪。

破坏报文检测即对报文的各标志位进行检测, 以判断各标志位是否符合 TCP/IP 规范。若报文的各标志位符合, 则将报文转入异常报文检测步骤; 若报文的各标志位不符合, 则向决策服务器上报告攻击源和攻击类型等信息, 由决策服务器制定处理该攻击威胁的策略。

3.2.3 异常报文检测

针对如 SYN flood、UDP flood 等大流量的泛洪式 DDoS 攻击, 各分布式 IDS 设备将构建用于识别泛洪式攻击报文的散列表以及设定该散列表的阈值; 每当 IDS 设备检测到泛洪式攻击的报文时, IDS 设备则在散列表中更新计数。若计数值超过阈值, IDS 设备则向决策服务器上报告攻击源、攻击类型等信息, 由决策服务器生成处理该攻击威胁的策略。

3.3 威胁处理策略

DIDS 若发现有攻击行为, 则通过在网络初始化过程中建立的 SSL 通道将攻击类型、威胁目标等信息上报决策服务器。决策服务器根据不同的攻击类型做出决策。

针对欺骗报文攻击, 若攻击威胁在 OpenFlow 域中, 决策服务器则通过控制器所提供的北向接口直接屏蔽攻击主机; 若攻击威胁不在 OpenFlow 域中, 则将攻击威胁所对应的交换机接入端口流量重定向至流量清洗中心进行过滤。

针对破坏报文攻击, 由于 IDS 设备当前处理的报文通过了欺骗报文检测, 所以该报文地址是真实的。决策服务器只需通过控制器的北向接口下发动作为 drop 的流表, 将攻击程序或攻击主机的流量屏蔽。但这都只是粗粒度的决策, 只适用于攻击分组少量的破坏报文攻击。

针对泛洪式的异常报文攻击, 决策服务器将这些不可信的流量引入流量清洗中心进行流量清洗。流量清洗中心的安全设备也可以将防护的结果反馈给控制器, 调整网络策略, 实现 SDN 以及混合有传统网络的多维防护。

3.4 路由优化策略

当网络中发生 3 层或 4 层的 DDoS 攻击, 或大流量正常业务占用链路带宽时, 将造成网络局部拥塞, 严重影响用户体验。因此, 第 3.4 节基于 SDN 控制器对链路剩余带宽等网络参数进行实时感知, 实现了一种路径优化生成算法。

首先, 当数据流的首个分组到达交换机时, 因为没有匹配的流表, 将被交换机上交给指定的控制器。控制器获取全网的实时拓扑并生成拓扑图; 然后, 控制器根据链路负载系数计算出优化路径, 由控制器得出对应的转发流表并下发交换机, 路由优化策略算法流程如下。

设 $r_{n,(n+1)}$ 为两相邻节点的链路剩余带宽, 则其链路负载系数为 $cost_{n,(n+1)} = \frac{1}{r_{n,(n+1)}}$ /* 由控制器计算出链路负载系数 */

$U(a,b)$ 为任意两点间的负载系数和:

$$U(a,b) = U(a,b) = \sum_{n=a}^b cost_{n,(n+1)}$$

设初始网络拓图为 G^0 , 计算任意两点间的最优路径,

Initialize($G^0, G^c, path$) {

 Get $G^0, source, target$

$G^c = path = \phi$

 /* 初始化网络拓扑集合和起点以及一个空的集合 */

Initialize U foreach vertex of G^0

 /* 初始化每个节点与起点的负载系数和 */

while($G^c \neq G^0$) {

 Select min $U(source, x)$ except $x \in G^c$ /* 取最小的 $U(source, x)$ */

 /*

 Update U by x /* 根据 x 更新所有 U */

$path_{index} \leftarrow x$

 add x to G^c /* 记录 x , 并加入集合 G^c 防止被重复迭代 */

 }

 产生源节点和目的节点之间的最佳路径。

4 实验与分析

4.1 实验目标设计与实验场景部署

本文对所述的 SDNQA 系统进行了实际的部署和验



证,主要测试和验证内容如下。

- 基于 OpenFlow 1.3 协议,测试装有 DDoS 威胁过滤与通信质量保障组件的 FloodLight 控制器、OpenFlow 交换机、IDS 设备以及决策服务器之间的通信。
- 测试 IDS 设备是否能够实时监测网络中的异常攻击流量,并且通过 SSL 通信信道上报决策服务器。
- 测试决策服务器是否能够根据 IDS 设备上报的信息,制定出处理对应攻击威胁的策略,并通过控制器的北向接口下发。
- 测试控制器是否能够根据网络实时状况,生成并下发实时优化的转发路径,以提升用户体验。

实验场景的具体部署如图 5 所示,中间为基础网络区域,有两个虚拟网。其中,虚拟网 A 部署了 SDNQA 系统,虚拟网 B 未部署,各虚拟网中都可能存在若干台 DDoS 攻击傀儡机。图 5 右侧为实验效果对比区域,包括一台 Web 服务器和两台用户主机,其中 Web 服务器上运行 Tomcat 对外提供 Web 服务,用户主机 A、B 分别是接入虚拟网 A、虚拟网 B 的主机;图 5 左侧为攻击模拟区域,有一台 DDoS 攻击机,攻击机作为主控机控制虚拟网 A 和虚拟网 B 中的傀儡机对 Web 服务器发起混合式的 DDoS 攻击。

本文基于上述实验环境,从两方面对 SDNQA 架构的

性能进行验证;对比混合式的 DDoS 攻击下 Web 服务器端所承受的攻击频率;对比泛洪式攻击所造成的网络平均传输时延。

4.2 实验结果及分析

首先,对 Web 服务器端流量流入情况进行分析。攻击机控制各虚拟网中的傀儡机同时对 Web 服务器发起混合式的 DDoS 攻击,其最高频率为 55 Hz,攻击时长为 100 s。截取 Web 服务器所有的数据分组序列,并分离出各虚网的请求序列,分别得出虚拟网 A 和虚拟网 B 所流入服务器的请求序列,Web 服务器所承受的攻击频率对比如图 6 所示。

从图 6 可以看出,SDNQA 系统在 0~5 s 快速识别了典型的 DDoS 攻击,并在 0~40 s 采取了过滤防护措施。在 40 s 之后,网络流量已趋于正常,测试用户主机 A 一直可正常得到网页请求响应,响应时间不超过 1 s。而未部署 SDNQA 系统的虚拟网 B 中一直有大量的攻击流量流入,测试用户主机 B 无法得到网页请求响应。

其次,从之前截取的数据分组序列中提取出测试用户主机 A 和测试用户主机 B 的请求序列,从各请求序列中统计数据分组的平均传输时延,两个虚拟网的平均传输时延对比如图 7 所示。

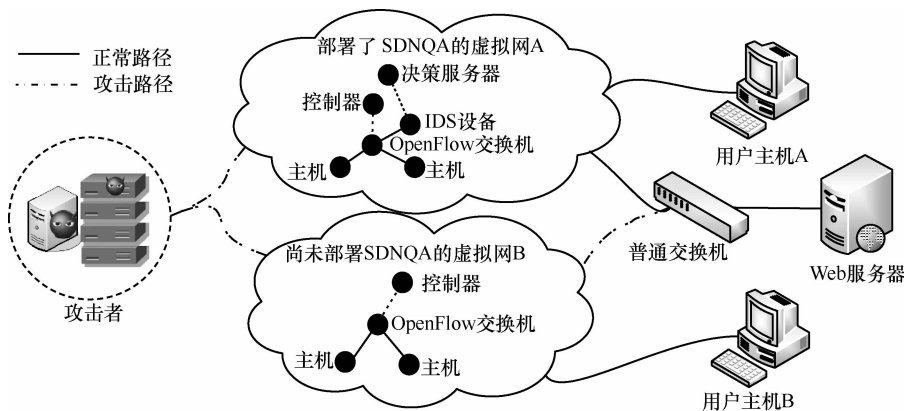


图 5 实验拓扑

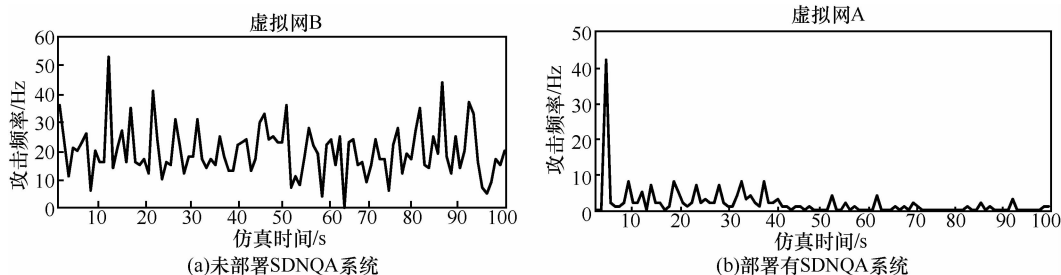


图 6 Web 服务器所承受的攻击频率对比

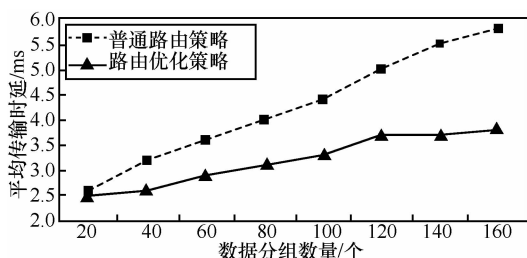


图7 平均传输时延对比

从图7中可以看出,经过路由优化,虚拟网A的平均传输时延没有随着数据量的增大而激增,且数据量增大至测试初始状态8倍时,网络平均传输时延由改进前的5.9 ms降低至3.5 ms。由此可见,SDNQA架构能够基于对网络实时状况的感知,实现对流转发路径的优化,从而在网络中存在DDoS攻击或正常大流量业务的情况下保证最佳用户体验。

5 结束语

为有效保证SDN的通信质量,本文提出了将DDoS威胁过滤技术与路由优化技术融合的SDNQA架构,并具体设计了基于DIDS的分布式威胁监测方案以及局部链路拥塞情况下的最优路径生成策略。

SDNQA架构使得传统网络体系架构下难以对伪造地址的DDoS攻击进行高效识别与溯源的难题从根本上得到了解决。在网络中存在DDoS攻击或正常大流量业务的情况下,控制器可基于对链路剩余带宽等网络参数的实时感知,实现对正常流量的路由优化,从而大幅提升用户体验。

基于已有基础,未来将实现业务可扩展机制,最终形成策略可定制的SDN智能防火墙系统,并进一步减小系统的响应时延,且系统可根据反馈灵活调整路由策略。后续将在上述方面继续进行深入研究。

参考文献

- Zhou Y X. Study on technology of network and information security. Proceedings of International Conference on Services Science, Management and Engineering, Wuhan, China, 2010
- 刘奇旭, 张翀斌, 张玉清等. 安全漏洞等级划分关键技术研究. 通信学报, 2012, 33(Z1)
- Liu Q X, Zhang C B, Zhang Y Q, *et al.* Research on the key technology of vulnerability threat classification. Journal on Communications, 2012, 33(Z1): 79~87
- Yaar A, Perrig A, Song D, *et al.* StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853~1863
- Zhou W, Wen S, Xiang Y, *et al.* Detection and defense of application-layer DDoS attacks in backbone web traffic. Future Generation Computer Systems, 2014(38): 36~46
- 金光, 张飞, 钱江波等. 融合路径追溯和标识过滤的DDoS攻击防御方案. 通信学报, 2011, 32(2): 61~67
- Jin G, Zhang F, Qian J B, *et al.* DDoS defense with IP traceback and path identification. Journal on Communications, 2011, 32(2): 61~67
- Jarraya Y, Madi T, Debbabi M. A survey and a layered taxonomy of software-defined networking. IEEE Communications Surveys & Tutorials, 2014, 16(4): 1955~1980
- Seungwon S, Vinod Y, Phillip G, *et al.* AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks. New York: ACM Press, 2013
- Seungwon S, Phillip P, Vinod Y. FRESKO: modular composable security services for software-defined networks. Proceedings of NDSS Symposium, San Diego, 2012
- 王歆平, 王茜, 刘恩慧等. 基于SDN的按需智能路由系统研究与验证. 电信科学, 2014, 30(4): 8~15
- Wang Y P, Wang X, Liu E H, *et al.* Research and verification on SDN-based on-demand smart routing system. Telecommunications Science, 2014, 30(4): 8~15
- Phillip P, Seungwon S, Vinod Y. A Security Enforcement Kernel for OpenFlow Networks. New York: ACM Press, 2012

[作者简介]



张家华,男,博士,南京晓庄学院讲师,主要研究方向为数据安全、软件定义网络、软件定义安全。

杨种学[通信作者],男,博士,南京晓庄学院教授、教务处处长,主要研究方向为数据安全、软件定义网络、软件定义安全。

王江平,女,博士,南京晓庄学院教授、教研室主任,主要研究方向为网络通信与光纤通信。

史煜凯,男,南京晓庄学院,主要研究方向为软件定义网络、软件定义安全。

魏亮,男,博士,江苏省未来网络创新研究院团队副总监,主要研究方向为软件定义网络、云计算、内容分发网络、网络试验床等。