Computer Science and Application 计算机科学与应用, 2019, 9(4), 721-730
Published Online April 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.94082

Hans汉斯

Research on DDoS Real-Time Monitoring and Mitigating in SDN Network

Dong Li, Qizhao Zhou

Network and Computation Center, Huazhong University of Science and Technology, Wuhan Hubei
Email: lidong@hust.edu.cn

Received: Mar. 30th, 2019; accepted: Apr. 12th, 2019; published: Apr. 19th, 2019

Abstract

SDN is a novel network architecture which provides centralized control of the whole network with global perspective. This paper establishes a mechanism to monitor and mitigate DDoS attack in SDN network. To detect DDoS attack in real time, characteristics of DDoS attack in traditional network and SDN network are devised as a vector. Based on the devised vector, the data collection module of SDN controller is modified and gradient decision classification algorithm (GBDT) is used to train model for anomaly data classification. To mitigate DDoS attack, according to the classified abnormal data of flow table, the network security policy can be performed by SDN controller. Simulated experiments demonstrate that the mechanism proposed by this paper can detect and mitigate the DDoS attack in SDN network effectively.

Keywords

DDoS, SDN, Flow Table, Gradient Decision Tree

SDN网络中DDoS攻击监测与防御方法研究

李　冬，周启钊

华中科技大学网络与计算中心，湖北　武汉
Email: lidong@hust.edu.cn

收稿日期：2019年3月30日；录用日期：2019年4月12日；发布日期：2019年4月19日

摘　要

软件定义网络(SDN)是一种新型的网络架构，具有全局视角，能够实现网络的集中管控。本文研究了SDN网络中DDoS攻击的特点和危害，设计实现了SDN网络中DDoS攻击实时监测和防御机制。在实时监测方

文章引用: 李冬, 周启钊. SDN 网络中 DDoS 攻击监测与防御方法研究[J]. 计算机科学与应用, 2019, 9(4): 721-730.
DOI: 10.12677/csa.2019.94082

面，本文综合分析了DDoS攻击的传统网络行为特征和SDN流表项数据特征后，提出了SDN网络中DDoS攻击检测特征，在进行特征去噪及降维优化后，利用梯度决策分类算法(GBDT)训练分类模型，对产生的SDN流表项数据进行异常分类。而攻击防御方面，针对SDN流表项数据的异常情况，利用SDN的全局视角配置相关参数，实时下发流表项，抑制DDoS攻击。模拟实验结果表明本文提出的DDoS攻击实时监测和防御机制能够有效地检测和缓解SDN网络中的DDoS攻击。

关键词

拒绝服务攻击，软件定义网络，流表，梯度决策分类

1. 引言

分布式拒绝服务(DDoS)是互联网面临的主要威胁之一，它通过伪造正常访问流量，对目标发动攻击，使得目标系统资源耗尽，无法提供正常的网络服务。现有的 DDoS 攻击检测方法主要针对传统网络架构，包括端系统的攻击流量检测与流量清洗，局部增加带宽、单点暂停服务等。这些方式在传统网络架构下曾起到过一些效果，但也具有单点视角的局限性和系统性能瓶颈等潜在问题。

在服务器虚拟化和 SDN 部署的大环境下，由于 SDN 掌握完整的网络拓扑、能够实时监测全局网络流量的特性，基于软件定义网络(SDN)的思路设计中间件实时监测网络中的 DDoS 攻击，并用数据驱动安全，进行相应安全应急处理策略的更新，及时对网络中的受攻击状态作出响应，成为行之有效的一条思路。当 SDN 网络受到 DDoS 攻击时，攻击方会发送大量数据包，这些数据包含有不同源地址、目的地址等信息。为获取转发规则，交换机需要不断向控制器发送请求，以获得新的转发规则，控制器也需要不断响应交换机的请求，制定、下发相应规则，以至于控制器的存储资源、计算资源大量消耗，控制器与交换机的连接资源大量占用[1]。基于上述的网络受攻击状态，设计基于 SDN 的 DDoS 实时攻击监测与应急处理系统，其关键点主要包括：

A、基于 SDN 控制器的数据收集与预处理。支持 Openflow 协议的控制器可以向交换机获取各类统计信息，其 RestAPI 提供可编程接口，针对 SDN 环境中 DDoS 攻击进行特征设计与优化，如何将数据收集粒度细化到 SDN 流表项级别，采用多线程向每个交换机发送请求，并行的将返回数据按照特征格式进行数据预处理，是数据收集模块需要解决的核心问题。

B、DDoS 攻击异常流表项数据分类模型训练。SDN 交换机流表项包含基础数据特征丰富，针对 DDoS 攻击带来的数据异常，为了达到较高的分类准确率，可基于较广的范围多元化的设计特征，再根据特征贡献权值和特征关联系数进行降维。在这样的情况下，采用哪种类型的分类算法及分类模型设计方式，能够适应 SDN 流表项数据多维度的数据特征，对于实时监测 SDN 网络中的 DDoS 攻击带来直观的效率提升，将十分关键。

C、基于 SDN 控制器的 DDoS 攻击应急处理的实现。由于 DDoS 攻击 IP 欺诈的特性，对于其来源的定位较为困难，本系统的应急处理策略将着眼于细粒度的定位受攻击的网络边缘交换机的端口、涉及传输层协议等信息，由此可实时制定精细的应急处理策略。如何根据异常流表项数据中的信息，进一步驱动 SDN 控制器进行安全策略下发，暂时闲置匹配相关端口、协议等的数据转发，达到初步缓解 DDoS 攻

击的效果，是应急处理模块需要重点设计解决的问题。

2. 相关工作

斯坦福大学等多家研究机构一直致力于 SDN 网络验证和调试与 SDN 控制层安全方面的研究[2]，将原型系统在多个 SDN 控制器平台实现并应用于实际的校园网。一些国内外知名企业发布了云数据中心 SDN 安全解决方案[3]，取得了一定安全防护效果，但缺少实际的应用场景。在 SDN 网络中，控制器集中管理网络设备，增大了网络安全风险[4]。文献[5]利用 NOX 控制器以及 OpenFlow 技术提出了一种轻量级的 DDoS 识别方法，通过提取 OpenFlow 流统计信息中与 DDoS 攻击相关的元组，采用人工神经网络方法进行降维处理，从而识别 DDoS 攻击。该方法与传统方法相比，利用 SDN 网络全局视图的特性，但其数据粒度较粗，缺少实际应用场景，也缺少有效的应急策略。针对网络大聚集流量的攻击识别，文献[6]利用 OpenFlow 交换机能够统计流数据的功能，设计了一种识别大规模聚集流量的功能。冲突检测是一种有效探测 DDoS 攻击的方法，文献[7]对冲突探测进行了说明。运用 SDN 的全局视角，文献[8]的模型很好的实现了精准实时流量的监控。而在实际应用场景方面，在数据中心的实用性无疑是 DDoS 攻击检测系统重要的测试场景，文献[9]设计了基于 MAC 地址进行溯源的数据中心标签系统用于实时的攻击定位。基于 Lin 等人的研究[10]，在 SDN 架构下配置第三方入侵检测系统以丰富数据监测方式，是未来在数据中心环境搭建各类数据驱动安全系统行之有效的思路。

3. 系统描述

3.1. 系统架构

图 1 是本文设计的 SDN 网络中 DDoS 攻击实时监测和防御系统框架，系统采用 Floodlight 作为 SDN 网络的控制器，利用 RestAPI 整合实现了 DDoS 实时监测与防御功能。在控制器内分别设计了数据检测和应急处理两个功能模块，同时基于机器学习建立了数据分析模块，各个模块通过文件系统进行的数据存储、读取和交互。

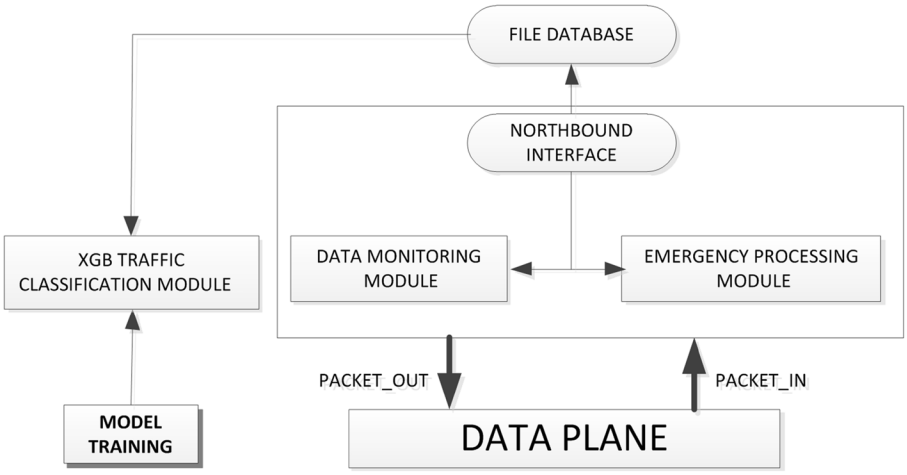

Figure 1. Architecture of global view
图 1. 全局结构图

3.2. SDN 数据收集

数据收集主要是利用在 OpenFlow 协议中控制器与交换机之间通过 OFPT_STATS_REQUEST 和

OFPT_STATS_REPLY 消息进行的数据交互(图 2)，控制器向交换机获取的各类统计信息，包括 Flow、Port、Queue 和 Table 的统计信息。本文模拟所用 FloodLight 控制器中的数据收集通过 Read-State 消息实现数据传输，可以针对交换机中的每张流表、每个数据流、每个设备端口、每个转发队列进行维护，同时获取相关信息以供其他模块调用。

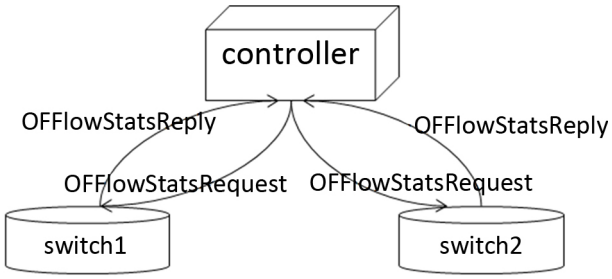

Figure 2. Principle of data queries
图 2. 数据交互原理图

在具体实现方面，本文采用多线程的方式，将每个交换机的消息由一个线程获取，线程之间并发执行。首先开启 Floodlight 中的数据收集线程 statisticsCollector，然后由 SDN 控制器向每个交换机发 oftp_stats_request，当交换机返回 oftp_stats_reply 之后，开启数据预处理线程，加入线程池管理，最后处理结果写入文件。

3.3. 数据分析

为了研究 SDN 网络中 DDoS 攻击的特征，本文数据分析主要基于以下三个方面进行特征设计：

A、世界经典入侵检测数据集 KDD99++(2013 年重制)中的传统网络数据特征设计方式；

B、SDN 网络中 DDoS 攻击引起的流表及流表项数据变化；

C、FloodLight 流表数据收集模块基础数据格式。

基于以上三种方式，DDoS 的攻击特征维度超过 30，然而，基于高维的数据特征，将为控制器带来巨大的数据收集和预处理的成本，此外在分类模型训练方面可也可能带来“维度灾难”以及过拟合的现象。

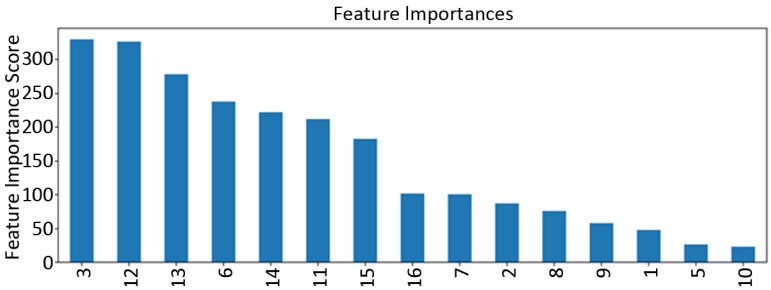

Figure 3. Ranking of feature weight
图 3. 特征权值排序

利用梯度决策算法以及特征关联分析，可对于特征对于分类结果的影响权值进行计算和排序(图 3)，最终，系统以两类粒度作为基本的特征维度标准，能够适用于不同的安全场景，在时延和精度方面各有优势，由此，本文设计了 7 元组快速检测模型和 16 元组精准检测模型。主要的特征设计结果如表 1、表 2。

Table 1. 16 indexes of DDoS
表 1. 16 元组特征

No.	FEATURE NAME	ILLUSTRATION
1	DURATION	Duration of flow entry
2	PROTOCOL_TYPE	Protocol type of traffic
3	BYTES	Bytes of traffic
4	LAND	Source of flow entry
5	DROP	Action of flow entry
6	SDIP_COUNT	pks with same DIP for current flow entry
7	SDPORT_COUNT	pks with same DPORT for current flow entry
8	SDIP_ DPORT_RATE	rate of pks (with same DPORT same DIP)
9	SDIP_DDPORT_RATE	rate of pks (with different DPORT same DIP)
10	DHOST_SRV_DHOST_RATE	rate of pks (with same DPORT; different DIP)
11	FT_SDIP_COUNT	In current flow table, pks that have the same DIP with current flow entry
12	FT_SDIP_SDPORT_COUNT	In current flow table, pks with same DPORT and same DIP
13	FT_SDIP_SDPORT_RATE	In current flow table, rate of pks (with same host same DPORT)
14	FT_SDIP_DDPORT_RATE	In current flow table, rate of pks (with different host different DPORT)
15	FT_DDIP_DSPORT_RATE	In current flow table, rate of pks(with different host different DPORT)
16	FT_SDIP_DDIFF_SIP_RATE	In current flow table, rate of pks (with same host and DIP different DPORT)

Table 2. 7 indexes of DdoS
表 2. 7 元组特征

No.	FEATURE NAME	ILLUSTRATION
1	MPF	Median of Packets per flowtable
2	MBF	Median of Bytes per flowtable
3	MDF	Median of Duration per flowtable
4	PPF	Percentage of Pair-flows
5	CSF	Count of Single-flows
6	CDSP	Count of Different sPorts
7	CDDP	Count of Different dPorts

梯度决策树分类算法(XGBoost)是本文数据分类的核心算法，也是近年来在天池、Kaggle 等各大数据挖掘算法比赛中出类拔萃的高效算法。XGBoost [11]是基于 GBDT (Gradient Boosting Decision Tree 梯度决策树)的优化分类模型，本质还是基于集成思想下的 Boosting 学习器，并采用梯度提升的方法进行每一轮的迭代最终组建出强学习器。这样的算法的运行往往要生成一定数量的树才能达到令我们满意的准确率，在 SDN 环境流表、流表项数据纷繁复杂的格式和数量的前提下，传统的分类算法如 SVM、KNN 可能带来极为复杂的运行成本或是不理想的准确率，且由于系统需要进行实时监测，重复的每运行一次都极有可能需要几千次的迭代运算，这将对我们的系统将造成巨大的计算瓶颈。梯度下降/上升作为XGBoost 决策算法的核心，是通过沿梯度求导得到损失函数极小值以获得模型参数的常用方式，其在损失项和正

则项上的多项优化，提升了算法所训练模型的准确率、效率及鲁棒性，能够适应与 SDN 控制器所收集到的多元组数据、多源数据的复杂性，并且达到较好的实时性和准确率。由图 4 的混淆矩阵可以发现，对于 DDoS 攻击检测最重要的两个指标误报、漏报，在 16 元组精准模型中的比例都很小，其综合的流表项数据预测准确率也达到了 98.98%。

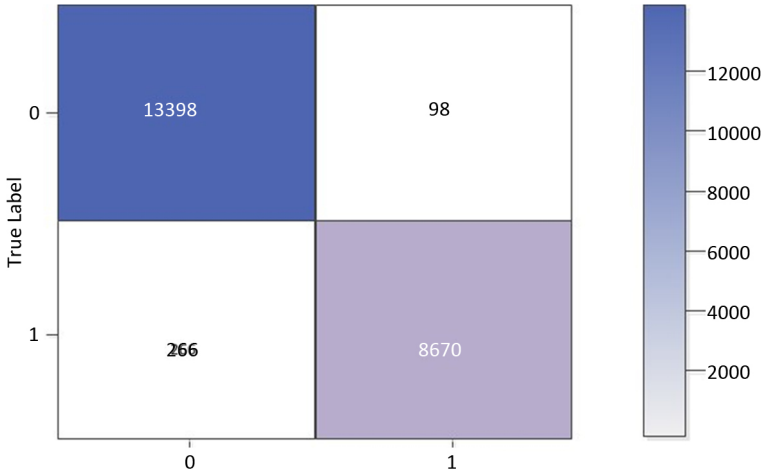

Figure 4. Matrix of 16-tuple features in XGBoost Model
图 4. 16 元组 XGBoost 模型混淆矩阵

3.4. 攻击防御

如图 5 所示，Floodlight 实现了 Firewall 模块，通过开放统一的北向 RestAPI 接口，帮助应用实现特定的流量过滤功能。其中主要接口方法包括：查询 Firewall 模块的开启状态，开启 Firewall 模块，根据要求添加新的过滤规则等。我们将 firewall 模块的指令配置方式进行封装，通过 Web 前端的方式实时监测的数据状态，以异常数据结果驱动安全策略的更新和下发：执行开启自动应急处理模块，上传 16 元组所反馈的细粒度异常节点信息，根据异常流表项数据中的相关附加字段，精确定位异常信息，自动下发相应规则，由控制器进行相应流表项下发，在靠近网络边缘的位置暂时闲置匹配该端口、协议等属性的数据转发，达到初步缓解 DDoS 攻击的效果，保证 SDN 交换机其他端口和其他网段的正常数据传输，防止攻击规模的升级。

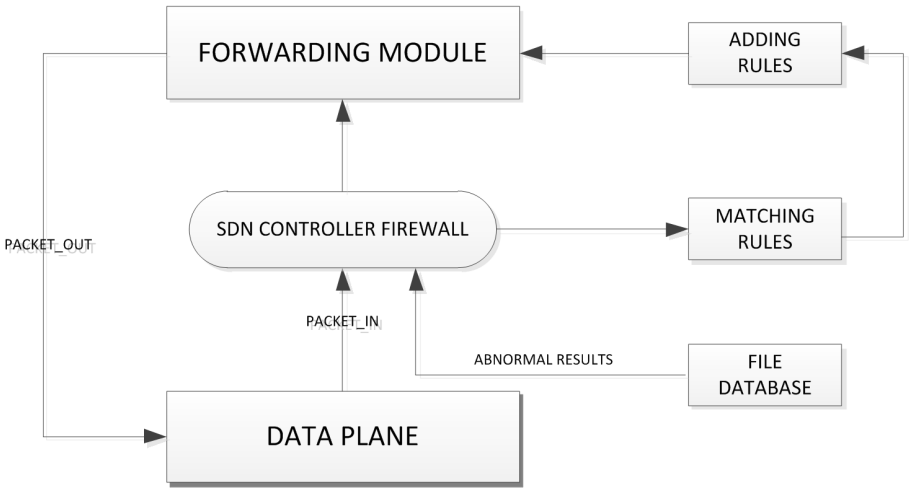

Figure 5. Principle of DDoS attack mitigation
图 5. 攻击防御原理图

4. 仿真实现与性能评价

4.1. 仿真环境搭建

系统仿真采用 Mininet 模拟 SDN 拓扑，Floodlight 作为控制器进行全局控制。h1~h11 共 11 台主机，s1~s4 共 4 台 OVS 交换机，s10 作为服务器提供服务。拓扑整体架构如图 6。

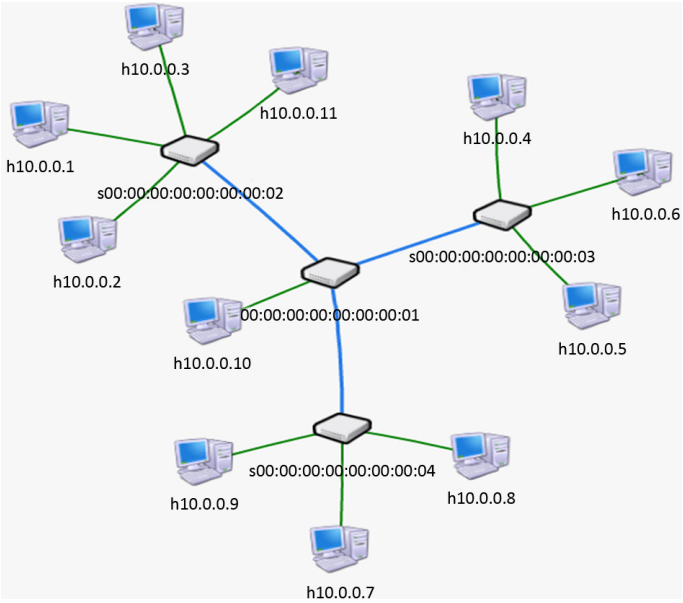

Figure 6. Topology of simulated SDN network
图 6. SDN 网络模拟仿真拓扑图

4.2. 网络流量模拟

通过各用户节点的文件下载、网页访问、视频访问等行为，在 SDN 网络拓扑中模拟各种传输协议类型混合的正常网络流量。当网络中仅有正常流量转发时，网络的各项性能指标保持良好，可正常执行访问 http 服务器、下载文件等操作，实时下载速度达 84.3 MB/s。图 7 是交换机 s10 正常状态时上下行包数，从中可以看出上下行流量比例维持在正常的水准，通过实时监测异常流表项数据状态发现网络中并没有异常报告。

DDoS 攻击方面，本文调研了历史上真实 DDoS 攻击事件，并根据攻击事件属性，按照相应洪泛协议的比例，在模拟环境中生成 DDoS 攻击流量。例如：针对游戏业务服务器进行的 DDoS 攻击，其洪泛协议类型组成比例约为：UDP FLOOD 占 83%，ICMP FLOOD 占 14%，SYN FLOOD 占 2%。其他有针对性的 DDoS 攻击还包括针对 Web 业务的攻击等。技术上的模拟方式主要是利用 hping3 伪造 IP 地址执行拒绝服务攻击(hping3 是一款 TCP/IP 协议的数据包生成和分析工具)。

4.3. 实时监测性能测试

开启 SDN 控制器的实时检测模块，图 8 展示了当在网络中模拟针对游戏业务的 DDoS 攻击后，实时监测模块的输出结果。可以发现目前 s10 的上下行流量比例已明显异常，且 7 元组快速模型的结果显示率先检测出异常，16 元组精准模型在结果报告中能够更精确、细粒度的输出异常结果。在 7 元组模型中，其中累计报告次数较多的是 2 号交换机的 2 号端口；16 元组模型中，能够更精确的定位受到攻击的 s2-2 端口和中心交换机的 s1-1 端口，这与我们模拟发起攻击的目标所在链路是一致的。在模拟攻击后，重新进行网络在攻击状态下的可用性测试，发现即时速度下降为 41.0 MB/s，在时延上也明显高于正常状态。

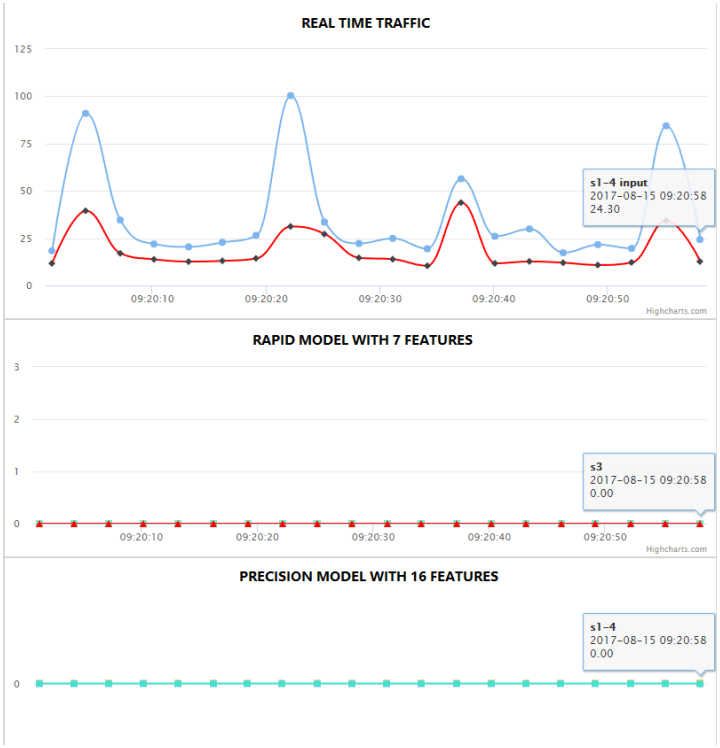

Figure 7. Traffic monitoring and attack detection in normal situation
图 7. 正常状态下流量监测和攻击检测

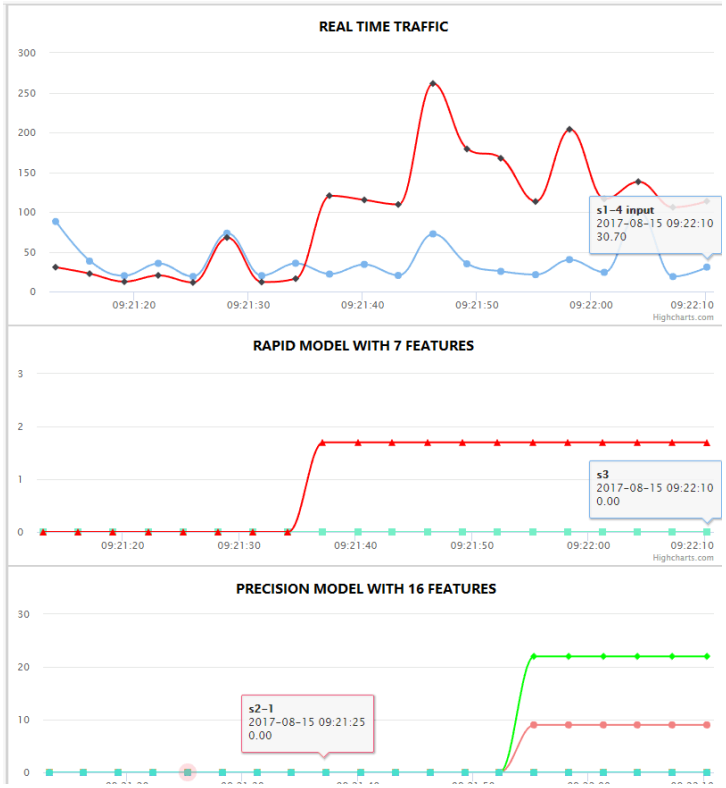

Figure 8. Traffic monitoring and attack detection in abnormal situation
图 8. 正常状态下流量监测和攻击检测

4.4. 攻击防御测试

开始攻击防御功能后，SDN 控制器选择对明显异常的流表项进行处理。经过一段时间的监测和响应，从图 9 中可以发现实时数据上下行流量比例恢复正常，7 元组/16 元组异常检测也不再出现报警。再次进行网络可用性测试，执行访问 http 服务器、下载文件等操作，发现下载速度恢复到只有正常流量时的水准，说明交换机其他端口的性能不再受到 DDoS 攻击的影响，网络状态恢复正常。

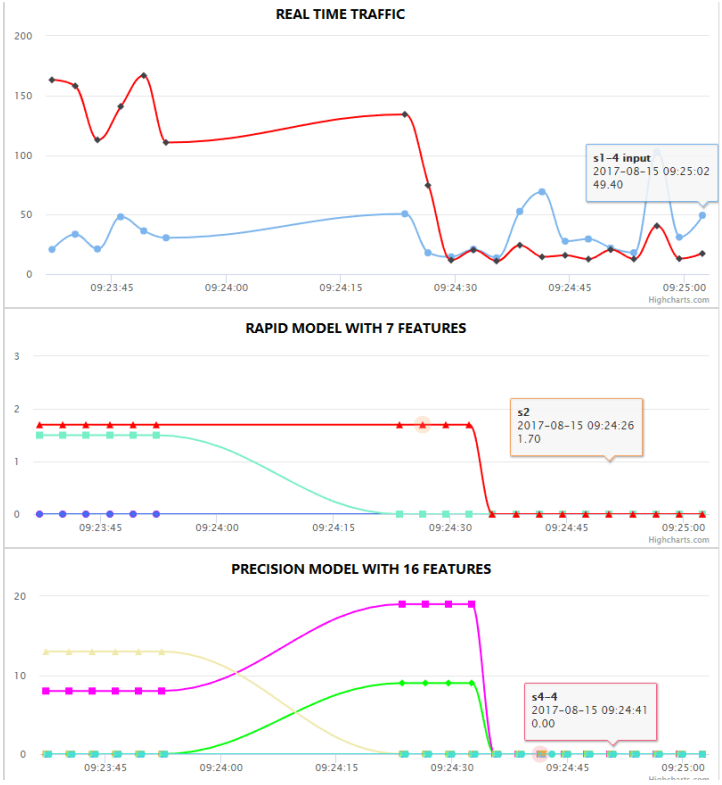

Figure 9. Traffic monitoring and attack detection after mitigating DDoS attack
图 9. 启用防御功能后流量监测和攻击检测

4.5. 算法评估

对 16 元组流表项数据进行分类分析，除了改进性能的梯度决策树分类(XGBoost)之外，本文还对 K 近邻(KNN)算法，支持向量机(SVM)，朴素贝叶斯(NaiveBayes)，随机森林(RandomForest)在 SDN 实验环境中的分类准确率和效率进行了测试，结果见表 3。

Table.3. Comparison of different algorithms
表 3. 算法性能比较

ALGORITHM	PRESICION	TIME COST(ms)
XGBoost	98.99%	358
KNN	96.93%	1068
SVM	95.27%	2512
NaiveBayes	89.64%	762
RandomForest	88.76%	1947

从表 3 可以看出，在异常流表项数据分类准确率和模型训练后测试数据分类处理效率两个方面，梯度决策树算法比传统的分类算法都有明显的优势；对于分析从支持 Openflow 协议的交换机所获取的流表项数据，梯度决策树分类算法也能很好的适应其数据量和特征维度，实时检测 SDN 网络中的 DDoS 攻击。

5. 结论

本文基于 SDN 全局视角，以数据驱动安全的思路，提出了 SDN 网络中 DDoS 攻击实时检测和防御方法。首先在传统网络和 SDN 网络中分析 DDoS 攻击特征，建立了 16 元组精确检测模型和 7 元组快速检测模型；然后基于该模型提取和处理 SDN 控制器获取的流表信息，再采用 XGBoost 算法进行分析，进而达到实时检测 DDoS 攻击的目的；最后和 Floodlight 控制器进行联动，下发安全流表抑制 DDoS 攻击。模拟实验表明本文提出的方法能够有效地检测和缓解 DDoS 攻击。

下一步我们将基于本文的原型系统融合入侵检测系统和防火墙等网络安全功能，提高 SDN 云数据中心的 DDoS 攻击监测和防御能力。

基金项目

本研究获得国家重点研发计划课题(2017YFB0801703)的资助。

参考文献

[1] Sood, K., Karmakar, K.K., Varadharajan, V., *et al*. (2019) Analysis of Policy-Based Security Management System in Software-Defined Networks. *IEEE Communications Letters*, 1. https://doi.org/10.1109/LCOMM.2019.2898864

[2] Montida, P., Ruan, H., Qipeng, S., *et al.* (2018) NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures. *IEEE Communications Surveys & Tutorials*, **20**, 3330-3368. https://doi.org/10.1109/COMST.2018.2859449

[3] Li, W., Meng, W. and Kwok, L.F. (2016) A Survey on Open Flow-Based Software Defined Networks: Security Challenges and Countermeasures. *Journal of Network & Computer Applications*, **68**, 126-139. https://doi.org/10.1016/j.jnca.2016.04.011

[4] Bates, A., Butler, K., Haeberlen, A., *et al*. (2014) Let SDN Be Your Eyes: Secure Forensics in Data Center Networks. The Workshop on Security of Emerging NETWORKING Technologies. https://doi.org/10.14722/sent.2014.23002

[5] Yang, L., Ng, B. and Seah, W.K.G. (2016) Heavy Hitter Detection and Identification in Software Defined Networking. 2016 25*th International Conference on Computer Communication and Networks* (*ICCCN*), Waikoloa, 1-4 August 2016, 1-10. https://doi.org/10.1109/ICCCN.2016.7568527

[6] Tu, R., Wang, X., Zhao, J., *et al*. (2015) Design of a Load-Balancing Middle Box Based on SDN for Data Centers. 2015 *IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), Hong Kong, 26 April-1 May 2015, 480-485. https://doi.org/10.1109/INFCOMW.2015.7179431

[7] Xie, J., Yu, F.R., Huang, T., *et al.* (2018) A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, **21**, 393-430. https://doi.org/10.1109/COMST.2018.2866942

[8] Edwards, T.G. and Belkin, W. (2014) Using SDN to Facilitate Precisely Timed Actions on real-Time Data Streams. *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, Chicago, 22 August 2014, 55-60. https://doi.org/10.1145/2620728.2620740

[9] Schwabe, A. and Karl, H. (2014) Using MAC Addresses as Efficient Routing Labels in Data Centers. *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, Chicago, Illinois, 22 August 2014, 115-120. https://doi.org/10.1145/2620728.2620730

[10] Lin, P.C., Liu, J.C. and Chiou, P.R. (2015) An Event-Based SDN Architecture for Network Security Analysis. 2015 *International Carnahan Conference on Security Technology* (*ICCST*), 21-24 September 2015, Taipei, 159-164. https://doi.org/10.1109/CCST.2015.7389675

[11] Chen, T. and Guestrin, C. (2016) XGBoost: A Scalable Tree Boosting System. *Proceedings of the* 22*nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining Pages*, San Francisco, 13-17 August 2016, 785-794. https://doi.org/10.1145/2939672.2939785

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org