Computer Science and Application 计算机科学与应用, 2018, 8(11), 1696-1705
Published Online November 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.811187

Hans汉斯

Anomaly Detection Technology of Network Traffic in SDN

Leijie Liu*, Wen Chen, Cong Chen

School of Information Science and Technology, Donghua University, Shanghai
Email: *2161243@mail.dhu.edu.cn, chenwen@dhu.edu.cn, congchen@mail.dhu.edu.cn

Received: Oct. 28th, 2018; accepted: Nov. 9th, 2018; published: Nov. 16th, 2018

Abstract

Software-Defined Networking (SDN) is a novel network architecture that has been successfully developed commercially. However, due to the increasing number and variety of network flows in the information society, abnormal detection of network traffic is becoming important. To realize anomaly detection of traffic in SDN network environment, this paper presents an algorithm based on Support Vector Regression (SVR) and Auto-Regressive Integrated Moving Average (ARIMA). The algorithm makes full use of the characteristics of SDN network, obtains the running state of the network periodically, and uses the ARIMA model to predict, then corrects the prediction results through the SVR model. The experimental results show that ARIMA-SVR model has higher accuracy and detection rate than ARIMA model; and compared with Support Vector Machine (SVM) model, ARIMA-SVR model can detect unknown types of abnormal traffic quickly.

Keywords

Support Vector Regression, Auto-Regressive Integrated Moving Average, Software-Defined Networking, Anomaly Detection

基于SDN的网络流量异常检测技术

刘雷杰*，陈　雯，陈　聪

东华大学信息科学与技术学院，上海
Email: *2161243@mail.dhu.edu.cn, chenwen@dhu.edu.cn, congchen@mail.dhu.edu.cn

收稿日期：2018年10月28日；录用日期：2018年11月9日；发布日期：2018年11月16日

*通讯作者。

文章引用: 刘雷杰, 陈雯, 陈聪. 基于 SDN 的网络流量异常检测技术[J]. 计算机科学与应用, 2018, 8(11): 1696-1705.
DOI: 10.12677/csa.2018.811187

摘 要

软件定义网络(Software-Defined Networking, SDN)作为一种新型的网络架构，已经成功地被商业化开发。但由于信息化社会的网络流量越来越大，种类越来越多，对于网络流量的异常检测日趋重要。为了实现在SDN网络环境下对流量进行异常检测，本文提出了一种基于支持向量回归(Support Vector Regression, SVR)和自回归积分滑动平均模型(Auto-Regressive Integrated Moving Average, ARIMA)的算法。该算法充分发挥SDN网络的特性，周期性的获取网络流量，并利用ARIMA模型对流量进行预测，之后通过SVR模型将预测结果进行校正。试验结果表明，相较于ARIMA模型，ARIMA-SVR模型拥有较高的准确率和检测率；相较于支持向量机模型，ARIMA-SVR模型能够快速地检测出未知类型的异常流量。

关键词

支持向量回归，自回归积分滑动平均模型，软件定义网络，异常检测

1. 引言

随着硬件技术的不断更新，软件技术的迅猛发展，使得现有网络的承载能力有了飞跃性的提高，但是仍旧存在着网络承载能力的上限。在信息化社会，每天都会产生海量的信息，这些网络信息有些是人们正常合理需求所产生的，有些则是垃圾信息。这些在网络负载中占着不小的比重，给网络带来巨大压力的同时，也会窃取人们的个人隐私信息的网络流量一般称为异常流量。造成网络流量异常的原因有很多，一般包括：恶意攻击，如病毒、DoS 攻击和 DDoS 攻击等；非法访问，如持续性端口扫描、远程未授权访问等。

传统的计算机网络由于观测点分布在各转发设备上，难以实现异常检测。然而，随着软件定义网络(Software-Defined Networking, SDN) [1]的出现，异常检测在 SDN 控制器中能很好地发挥作用。作为一种新型的网络架构，SDN 将传统的网络解耦成数据转发、网络控制、应用程序相互独立的三层结构，分别称为数据平面、控制平面和应用平面。数据平面主要负责数据转发功能，包括一切转发逻辑和转发表。控制平面掌控着网络全局信息，许多协议和算法都依赖于这个特征。由于 SDN 是未来网络发展的一个重要趋势，且其能提供比传统网络更完善的网络视图、更容易收集网络中的流信息、具有完善的管理平面，使得在 SDN 网络中研究网络流量异常检测技术成了一个重要的研究课题。

本文针对在 SDN 环境下的网络流量的异常检测提出了一种轻量级的算法。该算法利用 SDN 的特性，周期性地收集网络流量，使用自回归滑动平均模型(Auto-Regressive Integrated Moving Average, ARIMA) [2]来预测下一时刻的流量值，之后使用支持向量回归模型(Support Vector Regression, SVR) [3]对预测的流量值进行调整，以此来判断当前网络中的流量是否异常，提高了异常检测的实时性和准确性。

2. 相关工作

网络流量异常检测技术对于网络的监管有着重要的作用，被广泛应用于入侵检测、DDoS 攻击检测等技术中。网络流量本质上是一个随机时间序列，随着时间序列分析的发展，预测模型和算法已研究了

几十年。Box 等人[4]提出的时间序列模型通过自回归(Auto-Regressive, AR)，移动平均(Moving Average, MA)以及它们的组合为线性静止过程提供了解决方案。此外，常用的异常流量监测技术还有基于特征的检测。该方法通常需要建立一个详实的特征数据库，通过分析用户或主机日志[5]，或者统计网络中数据包的信息，例如流量、包头信息[6] (如源目 IP、源目端口、协议等)、内容特征[7]等，建立判定规则，与特征数据库中的数据进行匹配来检测。

从 2008 年以来，SDN 的出现以及其转控分离、集中控制等优良性能，使得人们对于在 SDN 网络环境下的异常流量检测技术做了深入的研究。王强[8]将传统网络中的生成树算法进行改进，利用 sFlow 控制器实现网络流量的监控。由于熵的特性，其经常被用来异常流量的检测。Wang 等人[9]、王文涛等人[10]分别将量子熵、Renyi 熵作为 SDN 网络流量的统计数据，通过设定阈值来检测异常。Carvalho 等人[11]提出了一个基于拓扑结构的网络流量监测系统。该系统通过 OpenFlow 协议收集网络流量，并对正常的流量行为构建数字签名，将当前流量与之进行对比，以此来识别异常的流量。Silva 等人[12]提出了一个可对异常流量进行分类的 ATLANTIC 框架，该框架使用信息理论来计算流表熵值的偏差，并结合一系列的机器学习算法对流量进行分类。Boero 等人[13]将入侵检测系统与 SDN 结合起来，选取机器学习中的支持向量机(support vector machine, SVM)作为核心算法，使用 SDN 控制器提取的流量特征作为 SVM 的输入，以此来训练模型并检测异常流量。作为监督学习算法的一种，SVM 算法具有很高的分类精度，但是其对于未知类型的攻击无法进行有效检测。近年来，由于大数据、人工智能等算法的兴起，基于 SDN 网络的异常流量检测技术有了很大的扩展。王晓瑞等人[14]为了快速识别 DDoS 异常流量，提出了一种基于 BP 神经网络的检测算法，该算法提取流表的特征，经过 BP 神经网络的训练后实现对数据包进行检测。王伟[15]将网络中的流特征以五元组的方式保存，并分别使用表征学习、LSTM 网络、CNN 网络来训练模型，以此来实现对异常流的检测。此外，在不同的 SDN 部署环境中，研究人员对于异常流量检测技术的研究一直都在进行，在云平台[16]、5G 网络[17]、物联网[18]、移动网络[19]等环境中，相继提出了一系列的检测技术。

本文受 ARIMA 的启发，能对具有周期性的时间序列有很好的预测效果，同时了解到网络流量具有很大的非线性和不规则性，需要有一个算法能对预测的结果进行矫正。而基于 SVM 在回归算法中的应用——SVR 算法，对于多种特征的回归问题具有良好的预测效果，且计算复杂度都较低，能够快速地进行矫正。因此，为了快速准确地对网络流量进行检测，本文从整体网络中网络流量变化情况的角度来考虑，提出了一个 ARIMA-SVR 组合模型。该模型利用每天网络流量变化的周期性特征来预测下一时刻的网络流量值，再将现实中重大节日、事件等活动对于网络流量的影响作为影响因子，调整网络流量的预测值，使之更精准。该模型充分利用了整体网络的变化情况，使得检测算法的速度得到提升，同时降低了控制器的资源消耗，提升了模型训练的速度。关于 ARIMA-SVR 模型的建立过程可见第三章。

3. 模型建立

3.1. 自回归滑动平均模型

对于网络流量来说，其具有周期性。例如白天网络流量大，晚上流量小；用餐时间段内，流量小等特点，且每日的流量变化情况较为相似，具有明显的周期性。对于这种有明显周期性的时间序列，ARIMA 模型具有较好的预测效果。

该模型可用 ARIMA(p, d, q)来表示，其中，p 表示自回归模型(AR)的阶数，d 表示差分次数，q 表示滑动平均模型(MA)的阶数，该模型的表达式形式为：

$$y_t = \sum_{k=1}^{p} \varphi_k y_{t-k} + e_t + \sum_{k=1}^{q} \theta_k e_{t-k} , \quad (1)$$

其中已知参数是，y_t 表示在时间 t 时的值；e_t 表示随机白噪声序列，为独立误差。未知参数为：φ_t 为 y_{t-k} 的系数，即自回归系数；θ_k 为 e_{t-k} 的系数，即滑动平均系数；AR 阶数 p；MA 阶数 q；以及差分次数 d。

ARIMA 模型通过对过去时刻的时间序列进行平稳性检查，通过 d 次差分，将非平稳序列转化为平稳序列，之后使用自相关函数和偏自相关函数确定模型的 p、q 值范围，再使用 BIC 最小化原则选择最优的 p、q 值，最后通过多项式拟合等曲线拟合方法来求得待求系数 φ_t 和 θ_k 的值。

3.2. 支持向量回归

网络流量中不定时地就会出现较大的波动，例如节假日，演唱会，明星直播等事件发生时，都伴随着较大的网络流量波动。因此，需要一种模型，能够根据这些情况，适时地调整网络流量的预测值。针对这种有多种特征的回归问题，SVR 有较好的预测效果。其是 SVM 在回归中的应用，泛化误差和计算复杂度都较低，且能够避免过学习的问题。

SVR 的核心思想与 SVM 相同，都是将样本空间通过核函数映射到特征空间中，在特征空间实现对样本的回归。对于数据集 $D=\{(x_1,y_1),\cdots,(x_m,y_m)\}$，其中 $x_i\in R^n, y_i\in R, i=1,\cdots,m$。引入松弛变量 ξ,ξ^*、不敏感系数 ε 以及惩罚参数 $C>0$。当满足条件 $-\varepsilon-\xi_i^*\le y_i-w\cdot x_i-b\le\varepsilon+\xi_i$ 时，可认为这些数据点都有同样的回归方程。其中 w 和 b 为待求系数，则该参数可由如下公式求出：

$$\min_{w,b,\xi_i,\xi_i^*}\frac{1}{2}\|w\|^2+C\sum_{i=1}^{m}(\xi_i+\xi_i^*),$$
$$\text{s.t.}\begin{cases}y_i-w\cdot x_i-b\le\varepsilon+\xi_i,\\ w\cdot x_i+b-y_i\le\varepsilon+\xi_i^*,\\ \xi_i,\xi_i^*\ge 0.\end{cases}\tag{2}$$

3.3. 异常检测模型

本文所使用的 ARIMA-SVR 模型充分利用了 SDN 网络对于网络监控的优点，快速采集网络流量，对其进行短期预测，以此来判断网络流量是否异常。我们的异常检测算法部署在 SDN 控制器内，如图 1 所示，控制器中主要包含了链路发现模块、流量采集模块、数据库模块、ARIMA 预测模块以及异常检测模块这 5 部分。

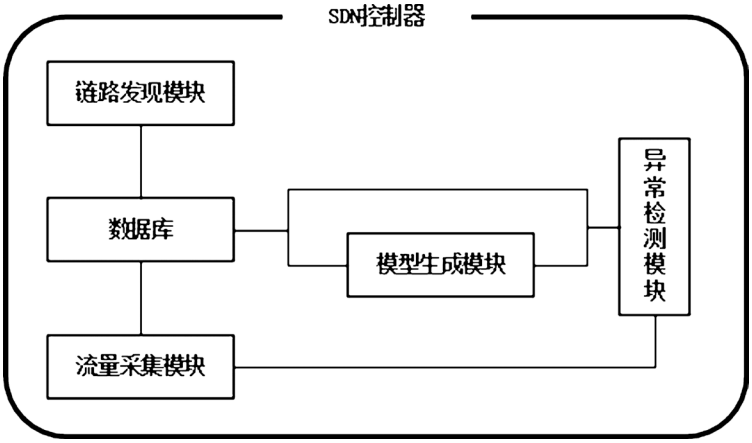

Figure 1. Diagram of module in SDN controller
图 1. 控制器中模块构成示意图

首先，由链路发现模块对网络中的交换机链路进行发现。在控制器和交换机通过 OpenFlow 协议建

立链接之后，控制器会定期向所链接的交换机发送 LLDP (Link Layer Discovery Protocol) [20]报文，根据返回的响应消息实现网络链路的发现。之后将收集到的网络拓扑，包括交换机及其使用的端口号，以集合的形式保存到数据库中。

之后，流量采集模块周期性地采集网络拓扑中各条网络的带宽使用情况。每经过一定的采样周期 sampling_time，控制器就会通过 OFPT_PORT_STATUS 消息向所链接的交换机发出端口查询消息，得到当前时刻通过该交换机各个端口的数据包字节数 current_byte，根据已记录的 pre_byte 计算出当前网络中各链路的已用带宽 BandWidth：

$$\text{BandWidth} = \frac{\text{current\_byte} - \text{pre\_byte}}{1024 * \text{sampling\_time}}, \tag{3}$$

单位为 KB/s，随后将 current_byte 赋值给 pre_byte，以便下一次的计算。同时，将计算出来的已用带宽 BandWidth 保存到存储模块的数据库中。

至此，存储模块就存储了链路发现模块每次探测到的网络拓扑集合，以及流量采集模块每次计算出的交换机各端口不同时刻的网络带宽。这些存储的数据将会被 ARIMA 预测模块和异常检测模块所调用，用于后续的计算。

接着，ARIMA 预测模块将会调用存储模块中存储的带宽使用数据，以一天内所测得的带宽数据作为基本单位，通过 ARIMA 算法训练模型，并预测下一次的带宽值 y_{ARIMA}。由于不同天次，不同时刻，通过网络的流量有所不同，为了模型能够更好地适应这些变化所带来的误差，需要定时地更新模型。该模块可以在任意时间，以最新的训练数据重新训练模型，以使得模型与现实网络带宽情况更好的匹配。

最后，异常检测模块将使用 SVR 算法，对当前的网络流量进行异常检测。我们先定义热点事件(Hot Point)为能在短时间内引起网络流量激增的事件，例如，双 11、比赛赛事、春节购票等情况。在热点事件发生前，网络中的流量变化较为平滑，但当热点事件发生后，大量的数据包被发送到目标主机，使得网络流量有一个向上的突增。由于 ARIMA 算法只是根据过去的流量数据进行预测的，但当网络中的流量因为热点事件而发生大幅度的改变后，这时预测出来的值就会与真实值有较大的差距。我们使用 SVR 算法对 ARIMA 预测的值进行调整，使其接近真实值。我们选择预测值 y_{ARIMA}，是否周末(W)，是否节日(F)，是否有热点事件(H)这四个变量作为输入变量，通过训练好的 SVR 模型进行预测，得到修正值 Q_{SVR}，最终可得到最后的预测值：

$$F_t = y_{\text{ARIMA}} + Q_{\text{SVR}}. \tag{4}$$

当真实值在预测值的 ±20% 范围内时，我们认为当前网络中并没有发生异常，反之，则说明网络流量异常，需要进行后续的干预。

具体步骤如下：

1) 控制器使用 LLDP 协议发现所有链接的交换机。

2) 控制器周期性发送 OFPT_PORT_STATUS 数据包，获得当前时刻通过交换机各个端口的数据包总字节数。之后利用公式(3)计算已用带宽，并将其保存到数据库中。

3) 选取一定数量的带宽值，使用 ARIMA 算法训练模型，得到预测值 y_{ARIMA}。

4) 使用预测值 y_{ARIMA}，是否周末(W)，是否节日(F)，是否有热点事件(H)这四个变量作为输入特征，通过 SVR 训练模型并进行预测，得到修正值 Q_{SVR}。

5) 根据公式(4)得到最终的预测值 F_t。如果下一时刻的真实值，没有超过 1.2 倍的 F_t，则说明当前是正常流量，反之，则说明当前流量有异常。

4. 实验结果与分析

我们使用树形网络拓扑来仿真。如图 2 所示，该拓扑是一个 3 层的二叉树，包括 7 台交换机(核心交换机-c1，汇聚交换机-a1 a2，边缘交换机-e1 e2 e3 e4)，6 台主机以及 2 台服务器。

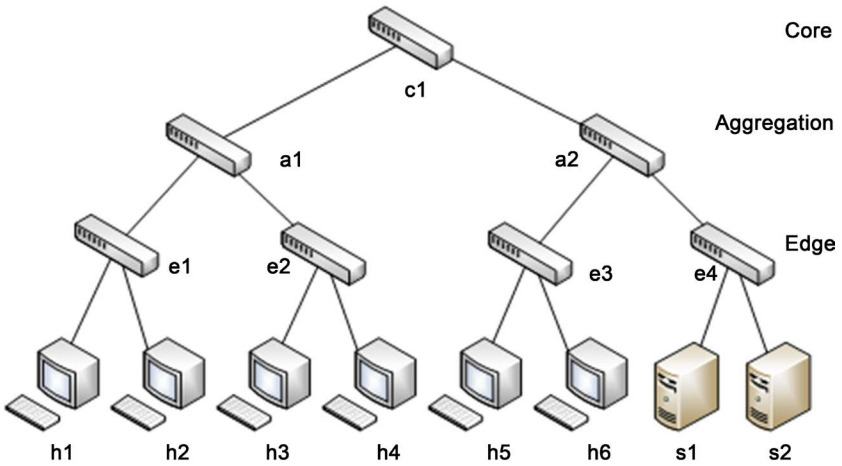

Figure 2. Simulation network topology
图 2. 仿真网络拓扑图

在实验中，我们将网络带宽设为 1 Mbit，从 2 台服务器中随机选取一台作为流量的接收方。6 台主机随机向服务器发送一定大小的流量。如图 3 所示，开始时通过的是正常的网络流量，网络带宽在 60 KB 左右。在 90 秒时，由于某热点事件的引发，使得网络流量在短期内有了突变，其增加到了 128 KB/s。

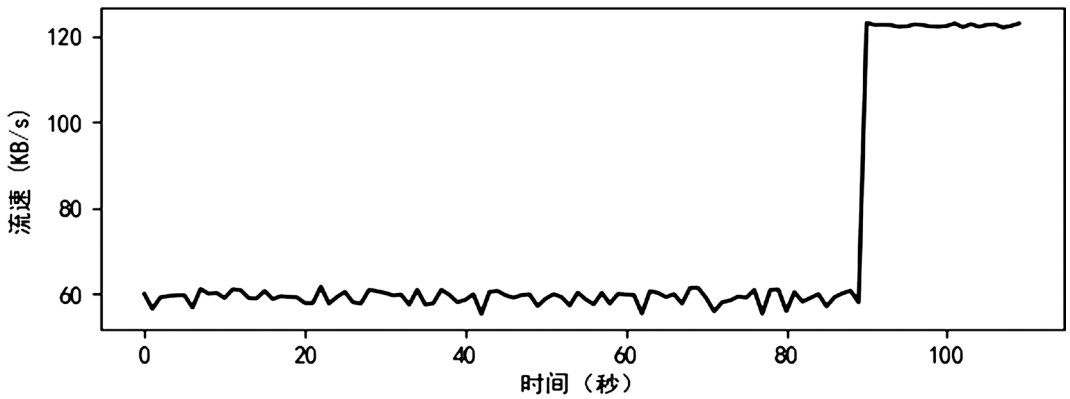

Figure 3. Raw network traffic data
图 3. 原始网络流量数据

我们对于原始数据进行平稳性和白噪声检验。对于非平稳序列，其存在单位根，因从可用单位根检验来判断序列是否平稳。其中 ADF 检验(Augmented Dickey-Fuller test，增项 DF 检验)就是一种检测序列中是否存在单位根的方法。该检验采用统计学中的假设检验方式，其假设序列存在单位根，即非平稳。因此，对于平稳序列，计算其在给定的置信水平上的显著性水平，若其统计值小于 1%的临界值，就说明其严格拒绝原假设，即序列平稳。如表 1 所示，原始数据的统计量 adf 值分别小于 critical_values 中的 1%，5%和 10%的三个临界统计值，且 p 值小于 0.01，说明此时数据符合平稳性的要求。同时，在白噪声检验中，p 值小于 0.05，说明此时的数据是随机分布的，符合白噪声检验的要求。

Table 1. Stationarity and white noise test
表 1. 平稳性和白噪声检验

	平稳性检验			白噪声检验	
	adf	p value	critical_values	lb value	p value
原始数据	−9.61	1.83e−16	{'1%': −3.49, '5%': −2.89, '10%': −2.58}	5.59	0.02

然后，训练最佳的 ARIMA 模型，获得 p 值和 q 值的取值，最优的取值应满足 BIC 最小的原则。根据这个原则，从表 2 中可知，最优的 p 值为 10。然而 q 的值可为 9 和 10，按照取最小值的原则，选取 q 为 9。至此，我们得到了时间序列预测的最优模型 ARIMA(10, 0, 9)。

Table 2. Related parameters of ARIMA model
表 2. ARIMA 模型相关参数

p	q	bic
…	…	…
10	7	367.26
10	8	368.02
10	9	352.23
10	10	352.23
…	…	…

模型的预测效果如图 4 所示。ARIMA 模型的预测值没有很好地贴近真实值，且当真实值有较大的流速变动时(例如在 90 秒时，流速超过 120 KB/s)，预测值变化的幅度不够。因此单纯的 ARIMA 模型无法有效地预测网络流量的变化情况。

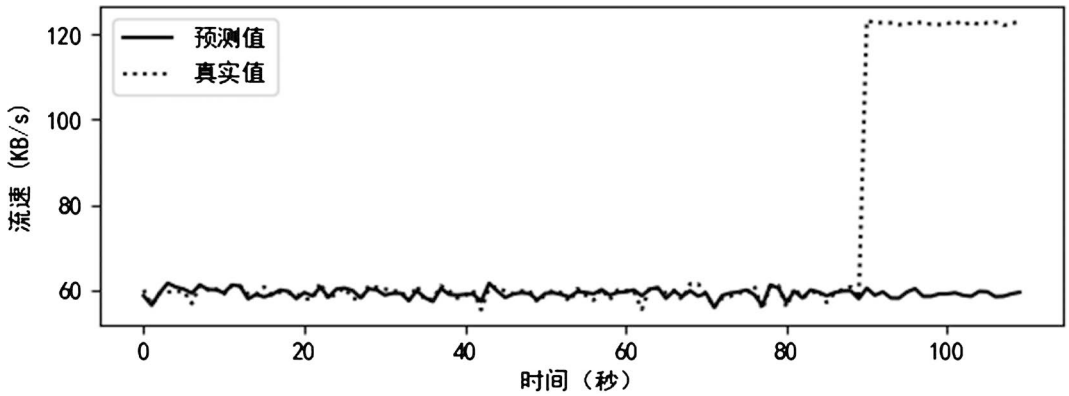

Figure 4. Prediction results of ARIMA model
图 4. ARIMA 模型预测结果

最后，将 ARIMA 模型的预测值与是否周末(W)，是否节日(F)，是否有热点事件(H)作为 SVR 模型的输入，训练模型，得到最后的预测结果。如图 5 所示，在预测的数据中，当真实值有较大上升时，预测值也会跟随上升。且绝大部分的真实值都小于 1.2 倍预测值。因此，所提的 ARIMA-SVR 模型能够很好的达到预期的效果。

由于本文所提模型来源于单一的 ARIMA 模型、SVM 模型，因此将这些模型与本文所提出的

ARIMA-SVR 模型进行比较。模型判断效果的性能可由如下公式的度量：

$$准确率 = \frac{正确匹配的流数}{总的流数}. \tag{5}$$

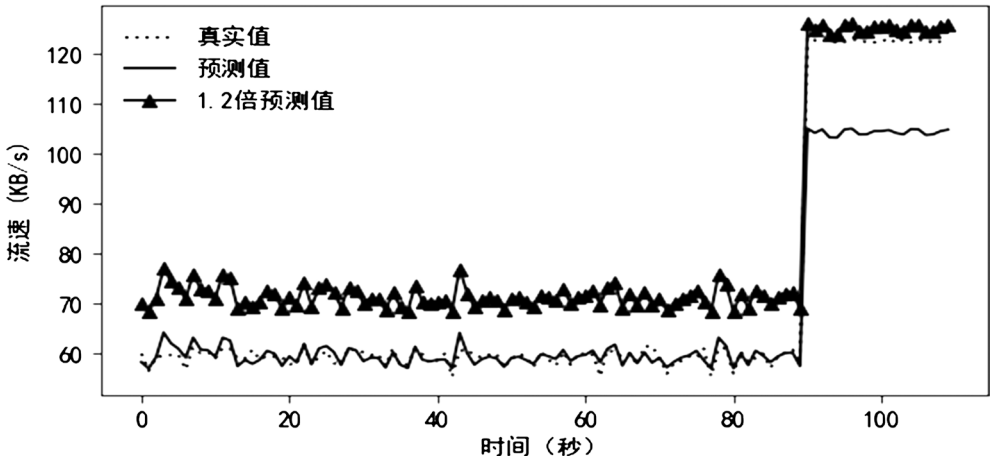

Figure 5. Prediction results of ARIMA-SVR model
图 5. ARIMA-SVR 模型的预测结果

分别使用正常流和异常流对模型进行测试，计算得到各模型的准确率。如图 6 所示，ARIMA-SVR 模型对于正常流和异常流都具有较高的准确率，能够很好的分辨出网络流量的异常情况。ARIMA 因为是基于正常流进行模型建立，故当由大量异常流导致的网络流量波动剧烈时，对于异常流检测的准确率较高。SVM 模型属于有监督的机器学习模型，其对于正常流有较高的检测准确率，但对于未知类型的异常流，其准确率较低。

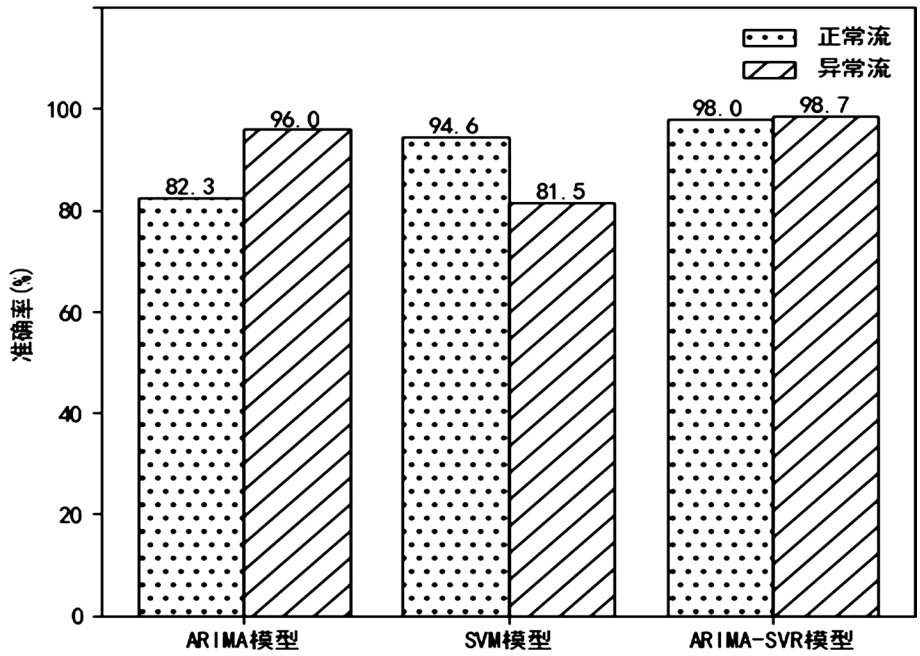

Figure 6. Accuracy of each anomaly detection model
图 6. 各模型异常检测效果的准确性

为了进一步比较各模型的性能，我们采用检测率(Detection Rate, DR)和误报率(False Acceptance Rate, FAR)对模型的稳定性和可用性进行分析。检测率和误报率可由下面的公式得出：

$$DR = \frac{\text{异常流中正确分类的流数}}{\text{已知的异常流数}}, \tag{6}$$

$$FAR = \frac{\text{正常流中错误分类的流数}}{\text{所有为果为异常流数}}. \tag{7}$$

检测率越低就意味着有大量的异常流没有被检测出来，这些流会给正常的访问造成困扰。误报率越高，就意味着大量的正常的数据包被错误检测，会使用户无法获得服务。如表 3 所示，本文的模型和其他两种模型相比，检测率高，同时误报率最低，检测效果更稳定。原因在于 SVM 模型对于部分偏差值较小的异常数据，无法有效的进行区分；ARIMA 模型对于短时间内流量波动特别剧烈的值，无法得到有效检测。本文所提的 ARIMA-SVR 模型利用整体网络中的流量变化情况来判断当前网络是否异常，特别是对于 DDoS 攻击、端口扫描等攻击有较强的检测能力。

Table 3. Stability of each anomaly detection model
表 3. 各模型异常检测效果的稳定性比较

模型	检测率(%)	误报率(%)
ARIMA 模型	96.0	7.4
SVM 模型	81.5	6.2
ARIMA-SVR 模型	98.7	2.0

5. 结论

基于 SDN 的网络使得控制器能够获取整个网络的信息。然而，现有的网络流量异常检测算法无法很好地适应 SDN 网络。因此，在本文中我们提出了一种基于时间序列预测和支持向量回归的方法，即 ARIMA-SVR 算法。该算法通过周期性的发送 LLDP 报文，可以有效的对网络的运行状态进行检测，并利用 ARIMA 模型来预测下一时刻的网络流量值，再将现实中重大节日、事件等活动对于网络流量的影响作为影响因子，使用 SVR 模型调整网络流量的预测值，使之更精准。该模型充分利用了整体网络的变化情况，使得检测算法的速度得到提升，同时降低了控制器的资源消耗，提升了模型训练的速度，提高了整体网络的效率。我们的实验结果有效地验证了算法的准确率以及稳定性和可靠性。

对于今后的工作，我们计划继续优化算法，使其能适应各种类型的网络流量，并能够在多控制器的网络中得到应用。

基金项目

本研究由国家自然科学基金资助项目(61501108)提供支持。

参考文献

[1] Kreutz, D., Ramos, F.M.V., Esteves, V.P., *et al*. (2014) Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, **103**, 10-13.

[2] Liu, C., Hoi, S.C.H., Zhao, P., *et al*. (2016) Online ARIMA Algorithms for Time Series Prediction. 30*th AAAI Conference on Artificial Intelligence*, AAAI Press, 1867-1873.

[3] Qian, Y.K. and Chen, M. (2011) MOADA-SVR: A Multivariate Online Anomaly Detection Algorithm Based on SVR. *Journal on Communications*, **32**, 106-113.

[4] Box, G.E.P., Jenkins, G.M., Reinsel, G.C., *et al*. (2015) Time Series Analysis: Forecasting and Control. 5th Edition, John Wiley and Sons Inc., Hoboken, pp. 712.

[5] 杨连群, 宋津旭, 李翔宇. 网络日志和流量关联分析的必要性[J]. 电子技术与软件工程, 2017(14): 11.

[6] 王珣. 基于 Netflow 的局域网流量异常检测系统的设计与实现[J]. 信息与电脑(理论版), 2016(21): 186-188.

[7] 曾建华. 一种基于核 PCA 的网络流量异常检测算法[J]. 计算机应用与软件, 2018, 35(3): 140-144.

[8] 王强. SDN 网络路由算法及流量监控方法的研究与应用[D]: [硕士学位论文]. 大连: 大连海事大学, 2016.

[9] Wang C., Mei W., Qin X., *et al*. (2017) Quantum Entropy Based Tabu Search Algorithm for Energy Saving in SDWN. *Science China* (*Information Sciences*), **60**, 040307. https://doi.org/10.1007/s11432-017-9044-x

[10] 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.

[11] Carvalho, L.F., Fernandes, G., Rodrigues, J.J.P.C., *et al*. (2017) A Novel Anomaly Detection System to Assist Network Management in SDN Environment. *IEEE International Conference on Communications*, Paris, 21-25 May 2017, 1-6. https://doi.org/10.1109/ICC.2017.7997214

[12] Silva, A.S.D., Wickboldt, J.A., Granville, L.Z., *et al*. (2016) ATLANTIC: A Framework for Anomaly Traffic Detection, Classification, and Mitigation in SDN. *IEEE/IFIP Network Operations and Management Symposium*, Istanbul, 25-29 April 2016, 27-35.

[13] Boero, L., Marchese, M. and Zappatore, S. (2017) Support Vector Machine Meets Software Defined Networking in IDS Domain. 29*th International Teletraffic Congress* (*ITC* 29), Genoa, 4-8 September 2017, 25-30. https://doi.org/10.23919/ITC.2017.8065806

[14] 王晓瑞, 庄雷, 胡颖, 等. SDN 环境下基于 BP 神经网络的 DDoS 攻击检测方法[J]. 计算机应用研究, 2018, 35(3).

[15] 王伟. 基于深度学习的网络流量分类及异常检测方法研究[D]: [博士学位论文]. 北京: 中国科学技术大学, 2018.

[16] 徐毅, 曾文兵. Openstack 虚拟化流量平台监控系统[J]. 计算机系统应用, 2018(2).

[17] Le, L., Sinh, D., Lin, B.P., *et al*. (2018) Applying Big Data, Machine Learning, and SDN/NFV to 5G Traffic Clustering, Forecasting, and Management. 4*th IEEE Conference on Network Softwarization and Workshops* (*NetSoft*), IEEE, 168-176.

[18] Kataoka, K., Gangwar, S. and Podili, P. (2018) Trust List: Internet-Wide and Distributed IoT Traffic Management Using Blockchain and SDN. *IEEE* 4*th World Forum on Internet of Things* (*WF-IoT*), Singapore, 5-8 February 2018, 296-301. https://doi.org/10.1109/WF-IoT.2018.8355139

[19] Monshizadeh, M., Khatri, V. and Kantola, R. (2017) An Adaptive Detection and Prevention Architecture for Unsafe Traffic in SDN Enabled Mobile Networks. *IFIP/IEEE Symposium on Integrated Network and Service Management* (*IM*), Lisbon, 8-12 May 2017.

[20] Nguyen, T.H. and Yoo, M. (2017) Analysis of Link Discovery Service Attacks in SDN Controller. *International Conference on Information Networking*, Da Nang, 11-13 January 2017.