·经典评述·

基于递归神经网络的网络安全事件预测*

郝怡然[1,2] 盛益强[1] 王劲林[1] 李超鹏[1,2]

([1]中国科学院 国家网络新媒体工程技术研究中心 北京 100190
[2]中国科学院大学 北京 100049)

摘要:针对现有安全事件预测算法所存在的过分依赖数据包头信息、所需历史数据较多、预测值误差较大、易陷入局部最优、训练时间较长等缺点,本文提出了一种基于递归神经网络进行分析数据包及其有效负载而在攻击发生前对安全事件进行预测的算法。该算法首先从数据包中提取源 IP 地址、协议类型和有效负载作为递归神经网络模型的输入,之后采用训练集对模型进行训练,同时引入批量梯度下降更新模型参数,最后采用测试集评估模型预测的准确率。通过递归神经网络分析有效负载可以更准确判断攻击性,大幅度提升网络安全事件的预测精度。

关键词:安全事件预测,递归神经网络,有效负载

Network Security Event Prediction Based on Recurrent Neural Network

HAO Yiran[1,2], SHENG Yiqiang[1], WANG Jinlin[1], LI Chaopeng[1,2]

([1]National Network New Media Engineering Research Center, Chinese Academy of Sciences, Beijing, 100190, China,
[2]University of Chinese Academy of Sciences, Beijing, 100049, China)

Abstract: Aiming at the shortcomings of the existing security event prediction algorithm, such as over - reliance on data packet header information, more historical data required, large error of prediction value, easy to fall into local optimum and training time is longer. This paper proposes a new method based on recurrent neural network to analyze packets and their payloads and to predict security events before an attack occurs. Firstly, the source IP address, protocol type and payload are extracted from the data packet as the input of recursive neural network model. Then the training set is used to train the model. At the same time, the model parameters are updated by the batch gradient descending. Finally, the test set is used to evaluate the prediction accuracy of the model. Through the recurrent neural network analysis of the payload can be more accurate to determine the attack, greatly enhance the network security event prediction accuracy.

Keywords: Network Security Event Prediction, Recurrent Neural Network, payload

1 引言

随着互联网规模日益庞大,各种新型网络攻击手段大量涌现,面对网络攻击危害度增强,网络安全问题日益严峻的现状,传统的网络防御技术已经很难满足网络安全的需求。由于传统的网络安全事件预测算法仅通过分析数据包的包头信息得到预测结果,受到分析的数据量的限制而导致预测精度较低。为了保障网络安全,把握网络状况,及时的进行网络安全状态估计,进而在攻击发生或造成严重后果之前[1],预先采取相应的防御措施,因此引入了网络安全态势预测。

本文于 2017 - 08 - 10 收到。
*中国科学院先导专项(XDA06040602);临港地区智能制造产业专项(ZN2016020103)。

目前不少学者在网络安全态势预测领域开展了很多研究工作，并取得了一定的研究成果。传统的预测方法主要是时间序列预测法和灰色理论预测法。时间序列预测法[2]在具有时变性的网络环境中预测的准确率较低；灰色理论预测法[3,4]当网络安全态势值的走势像“S”型变化的曲线时，预测的误差较大。并且传统的预测算法只能预测下一时刻网络是否受到攻击，无法体现网络安全系统的受威胁程度。

随着人工智能的发展，出现了基于支持向量机、神经网络等网络安全态势预测算法，提高了预测精度。支持向量机(Support Vector Machine, SVM)[5]对于大样本集训练速度慢。神经网络主要包括基于径向基函数(Radial Basis Function, RBF)[6]、卷积神经网络(Convolutional Neural Network, CNN)等预测算法。其中，基于 RBF 的神经网络态势预测方法，容易陷入局部最优[7-10]；基于 CNN 的神经网络态势预测方法，训练时间较长。

为了解决上述问题，本文提出了一种基于递归神经网络 (Recurrent neural Network, RNN)的网络安全事件预测方法。其基本思路是，通过分析网络数据包的包头信息和有效负载来改进现有的预测算法，但由于网络数据包中的有效负载长度会随着数据包而改变，因此采用基于递归神经网络的神经网络安全事件预测算法。该预测算法对非线性函数有良好的逼近性能，能存储当前时刻的输入和前一时刻输入之间的关系，且通过递归神经网络分析有效负载可以更准确的得到该数据包是否具有攻击性，大幅度提升网络安全事件的预测精度。

2　网络安全事件概率预测模型

2.1　递归神经网络结构

递归神经网络 (Recurrent neural Network, RNN)[11]由一个输入层 X，一个自连接隐含层 H，一个输出层 Y 组成。数据从输入层输入到模型中，神经元接收前一级输入和自反馈的输入，并输出到输出层。隐含单元选用 sigmoid 激活函数，输出为离散值。离散变量的每个可能值的未归一化对数概率表示离散变量的输出 o，输入给 Logistic 回归，输出概率向量 $\hat{y}^{(t)}$。其网络结构如图 1 所示。

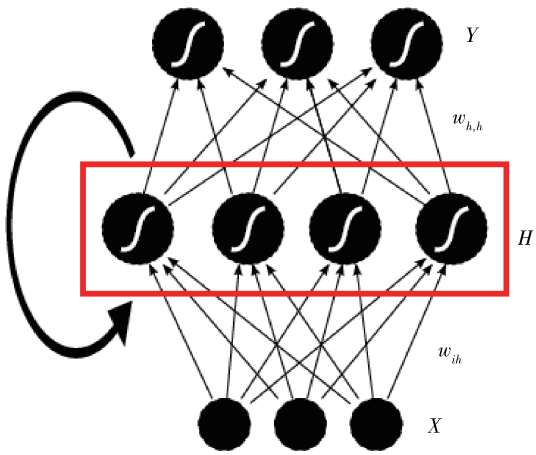

图 1　RNN 神经网络结构图

在前向传播中，各层之间的输入输出关系如式(1)所示。

$$\begin{aligned} a_h^t &= \sum_{i=1}^{I} w_{ih} x_i^t + \sum_{h'=1}^{H} w_{h'h} b_{h'}^{t-1} \\ b_h^t &= \theta_h(a_h^t) \\ a_k^t &= \sum_{h=1}^{H} w_{hk} b_h^t \\ \hat{y}^{(t)} &= \text{Logistic}(o^{(t)}) \end{aligned} \tag{1}$$

其中，$X=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$ 为输入数据向量，$H=[h_1,h_2,\cdots,h_l]^{\mathrm{T}}$ 为隐含层数据向量，$Y=[y_1,y_2,\cdots,y_m]^{\mathrm{T}}$ 为输出层数据向量。x_i^t 是指在时刻 t 的输入 i 的值，a_i^t 是指在时刻 t 将为单元 i 的网络输入，b_i^t 是指激活单元 i 在 t 时刻的输入。

在对前馈网络进行监督训练时，通过对代价函数最小化来调整层间权重。其中，代价函数如式[12,13](2)所示。

$$J(\theta) = 1/2m \sum_{i=1}^{m} (h_\theta(x^{(i)}) - y^{(i)})^2 \tag{2}$$

其中，$J(\theta_i)$是对于任意样本标签的代价，$h_\theta(x^{(i)})$是用于监督训练的样本标签，$y^{(i)}$是与样本标签对应的输出值，$J(\theta)$是对前馈网络进行监督训练的代价函数。

为了改善训练过程的稳定性和收敛速度，本文使用批量梯度下降方法进行训练，同时对误差反传方法

进行一个动量调整,这时的参数更新方法如式[14](3)所示。

$$\Delta w_{ij}(t) = -\eta \partial J/\partial w_{ij} + \alpha \Delta w_{ij}(t-1) \tag{3}$$

其中,$\Delta w_{ij}(t)$是第 t 次迭代进行的权值更新,η 是算法的学习速率,$0 \leqslant \alpha < 1$ 是动量项。

2.2 ISCX2012 IDS 数据集

随着网络行为和网络模式的变化及网络攻击方式的演变,迫切需要从网络攻击数据量较小,网络攻击方式较少的静态数据集向网络攻击数据量较大且包含多种网络攻击的动态生成数据集发展,这些包含网络攻击的 pcap 数据包不仅反映了当时的流量组合和网络攻击状态,而且该网络攻击过程也是可修改,可扩展,可再现。

本文采用的数据集是 ISCX2012 IDS,该数据集引入了一种基于配置文件的基本概念的方法来生成所需的数据集,以满足动态生成数据集的需求。其中,生成所需的数据集的方法包含对应用程序,协议或较低级别网络实体的入侵和抽象分发模型的详细描述。分析真实痕迹,为代理产生配置文件,生成 HTTP、SMTP、SSH、IMAP、POP3 和 FTP 的实际流量[15,16]。

该数据集记录了 2016 年 6 月 11 日至 17 日,每天连续 24 小时的网络状况。其中,6 月 11 日无网络攻击;12 日网络中有少量强攻击;13 日攻击渗透网络内部;14 日主要是 HTTP 拒绝服务;15 日是 IRC 僵尸网络的 DDOS 攻击;16 日有少量强力攻击;17 日为强力 SSH 攻击[17]。

2.3 数据预处理

ISCX 2012 IDS 数据集中,包含 pcap 数据包和 xml 文件。其中,pcap 数据包中包含了每个流的原 IP 地址,目标 IP 地址,相应的端口号以及有效负载等信息,xml 文件中主要包含了原 IP 地址,目标 IP 地址及相应的端口号,协议类型,标签等信息构成五元组。由于一个 pcap 包数据中存放了 24 小时的数据流,pcap 数据包过大,因此采用 pcap 文件分割器 splitcap 对 pcap 数据包进行切分。将每一组 IP 之间的交互切分到同一个 pcap 包中。且原 IP 地址,目标 IP 地址,相应的端口号以及时间戳可以构成一个五元组确定为一个数据流,将 pcap 数据包中的五元组和 xml 文件中的五元组进行匹配,匹配成功后将该五元组以及其对应的有效负载、是否有攻击等信息存入 pkl 文件中,为以后作为模型的输入提供便利。

2.4 训练过程

对以上提出的基于递归神经网络的网络安全事件预测模型进行训练,主要分为以下几个步骤:

(1)从 ISCX2012 IDS 数据集每天的入侵检测数据中随机选取连续的 6 个小时的数据作为测试数据,其余的作为训练数据。

(2)首先根据 2.1 节中介绍的递归神经网络构建预测模型,其中,反向传播时采用批梯度下降法防止过拟合(overfitting)。然后采用训练集对模型进行训练,选取标签、源地址、协议类型、有效负载作为模型的输入。其中,标签作为模型输入时的标签的取值 Normal 和 Attack 应分别转换为 0 和 1;源地址作为模型输入时建立源地址的索引,将索引值作为输入;有效负载作为模型的输入时需要先根据有效负载的字典,将有效负载的每一个单元映射到维度(de)上。设置窗口大小为 cs,则有效负载即为 de * cs[18]。

(3)采用测试集对模型进行测试,选取源地址、协议类型、有效负载作为模型的输入,按照步骤(2)中所述的方式对模型的输入进行处理。并存储模型的判断结果。将模型判断的结果与实际结果进行比较,并通过均方根误差指标、平均相对误差指标和正确趋势率等指标对模型进行评价[19]。

3 评价及讨论

本文采用了平均相对误差(Average relative error, ARE)和均方根误差(Root mean square error, RMSE)来衡量预测的效果,如公式(4)和公式(5)所示[20,21]。

平均相对误差指标为

$$\text{MAPE} = 1/N \sum_{i=1}^{N} | y_i - y_i' | / y_i \tag{4}$$

均方根误差指标为

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - y_i')^2} \tag{5}$$

其中，在式(4)和式(5)中，样本的数量为 N，第 i 个样本预测值为 y_i，第 i 个样本的实际值为 y_i'。

基于 ISCX2012 IDS 数据集和 DARPA1998 数据集的初步评价结果表明，与传统的过度依赖数据包头的预测相比，由于本文的安全事件预测模型中的输入包含数据包的有效负载，依据数据包的有效负载判断该数据包具有攻击性或者在为攻击做准备的概率，因此该预测模型可以更准确的得到该数据包是否具有攻击性，从而有望大幅提升了网络安全事件的预测精度。

安全事件预测的实验环境配置、所用预测方法比较以及数据说明如下表所示，表 1 为实验环境的配置，表 2 为本文所用的基于递归神经网络的网络安全态势预测方法与传统的时间序列法、支持向量机等预测方法进行对比，表 3 为 ISCX2012 IDS 数据的攻击情况，说明表 4 为 ISCX2012 IDS 预处理后的攻击数据。

表 1　实验环境配置

项	配置情况
操作系统	Windows 10 版本 1607
硬件配置	Intel(R) Core(TM) i7-4712MQ CPU@2.30GHz,4GB RAM
Python 版本	Anaconda 2.7

表 2　本文方法与传统方法对比表

预测方法	所需历史数据多	无法存储前后时刻的输入关系	对缺失数据敏感	对核函数选择敏感	对“S”型变化曲线预测误差大
时间序列	√	√			
灰色理论		√			√
支持向量机		√	√	√	
递归神经网络					

表 3　ISCX2012 IDS 数据说明

日期	攻击情况	数据大小
6 月 11 日	正常活动，无攻击	16.1GB
6 月 12 日	正常活动，有少量强攻击	4.22GB
6 月 13 日	正常活动，渗透网络内部	3.95GB
6 月 14 日	正常活动，HTTP 拒绝服务	23.4GB
6 月 15 日	正常活动，用 IRC 僵尸网络的 DDOS	23.4GB
6 月 16 日	正常活动，少量强力攻击	17.6GB
6 月 17 日	正常活动，强力 SSH	12.3GB

在以上研究工作的基础上，通过提取大量安全事件信息，进行理解和分析，找到安全事件之间的关联性，并将这些数据中相似度较高的事件进行融合，有望提高预测精度和预测效率[22,23]；进行实时网络安全态势预测[24]，并引入 Spark 分布式[25,26]，实现高效实时的网络安全态势预测；对于复杂网络进行安全态势预测[20]，针对现有的态势预测方法多数是态势值的预测，并未揭示网络态势要素动力学特征的问题，因此引入了一种通过复杂网络进行网络安全态势预测的方法，实现对网络安全状态的有效预测；由于网络系统的各个节点相互连接，当系统中某个节点被成功攻击后，威胁可以传播到与该节点相关联的其他节点，从而使这些节点遭受安全威胁。因此，在进行态势感知时不能仅静态考虑系统节点安全状况，还需对威胁传播及其影响进行动态分析[27]。

表 4　ISCX2012 IDS 预处理后的攻击数据

攻击类型	举例			
	源地址	目的地址	协议类型	长度
BruteForse SSH	192.168.5.122	67.23.167.37	SSHV2	210
Infiltrating	192.168.5.122	131.202.243.90	SMTP	68
Http Dos	131.202.241.200	192.168.1.101	TCP	1404
DDOS	192.168.5.122	131.202.243.90	TCP	66
SSH	192.168.5.122	58.211.72.43	SSHV2	850

4　结束语

本论文提出了一种基于递归神经网络的安全事件预测方法，对于把握网络状况，及时地进行网络安全状态估计，并试图在攻击发生或造成严重后果之前，预先采取相应的防御措施来加强网络的安全具有重要意义。本文中安全事件预测算法的输入包含数据包的有效负载，依据数据包的有效负载判断该数据包具有攻击性或者在为攻击做准备的概率。与传统的过分依赖数据包头的预测算法相比，该预测算法可以更准确

的得到当前时刻的数据包是否具有攻击性,从而有望大幅度提升了网络安全事件的预测精度。

未来的研究工作,可以尝试不同的方法进行预测,同时对预测得到的可能受到威胁的节点进行威胁传播分析等,以进一步提高训练速度和预测精度等指标。现有的安全事件预测模型存在很多有待解决的问题,例如实时根据网络安全事件预测、个性化预测、容错性等。

致谢 本篇文章的完成过程中,得到了实验室老师及同学的帮助,在此致以诚挚的谢意。

参 考 文 献

[1] Ho Q, Cipar J, Cui H, et al. More Effective Distributed ML via a Stale Synchronous Parallel Parameter Server[J]. Advances in Neural Information Processing Systems, 2013, 2013(2013):1223

[2] 席荣荣, 云晓春, 金舒原,等. 网络安全态势感知研究综述[J]. 计算机应用, 2012, 32(1):1-4

[3] 赵国生, 王慧强, 王健. 基于灰色 Verhulst 的网络安全态势感知模型[J]. 哈尔滨工业大学学报, 2008, 40(5):798-801

[4] 韦勇,连一峰,冯登国等.基于信息融合的网络安全态势评估模型[J].计算机研究与发展,2009,46(3):353-362

[5] 曾斌, 钟萍. 网络安全态势预测方法的仿真研究[J]. 计算机仿真, 2012, 29(5):170-173

[6] 甘文道, 周城, 宋波. 基于 RAN-RBF 神经网络的网络安全态势预测模型[J]. 计算机科学, 2016, 43(S2):388-392

[7] 薛丽敏, 李忠, 蓝湾湾. 基于在线学习 RBFNN 的网络安全态势预测技术研究[J]. 信息网络安全, 2016(4):23-30

[8] Su H, Chen H. Experiments on Parallel Training of Deep Neural Network using Model Averaging[J]. Computer Science, 2015.

[9] 任伟, 蒋兴浩, 孙锬锋. 基于 RBF 神经网络的网络安全态势预测方法[J]. 计算机工程与应用, 2006, 42(31):136-138

[10] 孟锦, 马驰, 何加浪,等. 基于 HHGA-RBF 神经网络的网络安全态势预测模型[J]. 计算机科学, 2011, 38(7):70-72

[11] Graves A. Supervised Sequence Labelling with Recurrent Neural Networks[M]. Springer Berlin Heidelberg, 2012.

[12] Zhang W, Gupta S, Lian X, et al. Staleness-aware async-SGD for distributed deep learning[C]//International Joint Conference on Artificial Intelligence. AAAI Press, 2016.2350-2356

[13] 陈秀真, 郑庆华, 管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4):885-897

[14] 盛益强, 赵震宇, 廖怡. 用于个性化数据挖掘的粗粒度分布式深度学习[J]. 网络新媒体技术, 2016, 5(6):1-6

[15] J Dean J, Corrado G S, Monga R, et al. Large scale distributed deep networks[C]// International Conference on Neural Information Processing Systems. Curran Associates Inc. 2012.1223-1231

[16] Gupta S, Zhang W, Milthorpe J. Model Accuracy and Runtime Tradeoff in Distributed Deep Learning[J]. Computer Science, 2015.

[17] Intrusion detection evaluation dataset[O/L]. http://www.unb.ca/cicresearch/datasets/ids.html.

[18] 谢丽霞, 王亚超, 于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版), 2013(12):1750-1760

[19]韦勇,连一峰.基于日志审计与性能修正算法的网络安全态势评估模型[J].计算机学报,2009,46(2):763-772

[20] 李方伟, 郑波, 朱江,等. 一种基于 AC-RBF 神经网络的网络安全态势预测方法[J]. 重庆邮电大学学报自然科学版, 2014, 26(5):576-581

[21] Chen K, Huo Q. Scalable training of deep learning machines by incremental block training with intra-block parallel optimization and blockwise model-update filtering[C]// IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2016.5880-5884

[22] 孟锦. 网络安全态势评估与预测关键技术研究[D]. 南京理工大学, 2012.

[23] 石并. 网络安全态势感知研究综述[J]. 网络安全技术与应用, 2014(8):156-157

[24] 黄同庆, 庄毅. 一种实时网络安全态势预测方法[J]. 小型微型计算机系统, 2014, 35(2):303-306

[25] 李文栋. 基于 Spark 的大数据挖掘技术的研究与实现[D]. 山东大学, 2015.

[26] 唐云. 基于 Spark 的大规模分布式矩阵运算算法研究与实现[D]. 南京大学, 2016.

[27] 张勇, 谭小彬. 一种基于隐 Markov 模型的网络安全态势感知方法研究[J]. 信息网络安全, 2011(10):47-51

作者简介

郝怡然,女,博士研究生,研究方向:网络安全态势感知、分布式机器学习。

盛益强,(通信联系人),男,工学博士,研究方向:智能集成系统、分布式机器学习、未来网络。