



文章编号:1001-9081(2018)10-2903-05

DOI:10.11772/j.issn.1001-9081.2018030710

## 基于混合卷积神经网络和循环神经网络的入侵检测模型

方圆<sup>1</sup>, 李明<sup>1</sup>, 王萍<sup>1</sup>, 江兴何<sup>2</sup>, 张信明<sup>2\*</sup>

(1. 国家电网 安徽省电力有限公司信息通信分公司, 合肥 230061;

2. 中国科学技术大学 计算机科学与技术学院, 合肥 230027)

(\* 通信作者电子邮箱 xinming@ustc.edu.cn)

**摘要:**针对电力信息网络中的高级持续性威胁问题,提出一种基于混合卷积神经网络(CNN)和循环神经网络(RNN)的入侵检测模型。该模型根据网络数据流量的统计特征对当前网络状态进行分类。首先,获取日志文件中网络流量的各统计值,进行特征编码、归一化等预处理工作;然后,通过深度卷积神经网络中可变卷积核提取不同主机入侵流量之间空间相关特征;最后,将已经处理好的包含空间相关特征的数据在时间上错开排列,利用深度循环神经网络挖掘入侵流量的时间相关特征。实验结果表明,该模型相对于传统的机器学习模型在曲线下方的面积(AUC)上提升了7.5%~14.0%,同时误报率降低了83.7%~52.7%。所提模型能准确地识别网络流量的类别,大幅降低误报率。

**关键词:**高级持续性威胁;网络流量;卷积神经网络;循环神经网络

**中图分类号:**TP391    **文献标志码:**A

### Intrusion detection model based on hybrid convolutional neural network and recurrent neural network

FANG Yuan<sup>1</sup>, LI Ming<sup>1</sup>, WANG Ping<sup>1</sup>, JIANG Xinghe<sup>2</sup>, ZHANG Xinming<sup>2\*</sup>

(1. Division of Information Communication, State Grid Anhui Electric Power Company Limited, Hefei Anhui 230061, China;

2. School of Computer Science and Technology, University of Science and Technology of China, Hefei Anhui 230027, China)

**Abstract:** Aiming at the problem of advanced persistent threats in power information networks, a hybrid Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) intrusion detection model was proposed, by which current network states were classified according to various statistical characteristics of network traffic. Firstly, pre-processing works such as feature encoding and normalization were performed on the network traffic obtained from log files. Secondly, spatial correlation features between different hosts' intrusion traffic were extracted by using deformable convolution kernels in CNN. Finally, the processed data containing spatial correlation features were staggered in time, and the temporal correlation features of the intrusion traffic were mined by RNN. The experimental results showed that the Area Under Curve (AUC) of the model was increased by 7.5% to 14.0% compared to traditional machine learning models, and the false positive rate was reduced by 83.7% to 52.7%. It indicates that the proposed model can accurately identify the type of network traffic and significantly reduce the false positive rate.

**Key words:** advanced persistent threat; network traffic; convolutional neural network; recurrent neural network

## 0 引言

高级持续性威胁(Advanced Persistent Threat, APT)攻击是一种高级的网络入侵技术,因其极强的隐蔽性、针对性、持续性和不计成本的长期入侵机制,使得各类核心网络的安全受到极大的威胁<sup>[1]</sup>。电力信息网络作为整个电力资源管理的核心,因其存储着海量的高价值数据,来自网络的安全威胁往往更为突出。例如,2015年乌克兰电网系统遭受了黑客入侵<sup>[2]</sup>,植入的恶意软件同时攻击了多个电网公司,这是史上首次导致大规模停电的恶意网络攻击。因此尽早地检测到网络的入侵行为,隔离处理各种潜在的威胁,为国民生活生产提供可靠的保障刻不容缓。

检测APT攻击行为是电力信息系统安全防护的前提,也是整个防御阶段最为核心的部分。常用的基于底层数据分析的检测方案有恶意代码异常检测、社交网络安全事件挖掘和网络流量异常检测<sup>[3]</sup>。恶意代码异常检测需要采用静态或动态的方式提取特征,由于APT攻击具有很强的伪装性、隐藏性和变异性,导致提取时难以识别变形、加密后的恶意代码且耗时较长;社交网络安全事件挖掘,往往需要处理海量低价值密度的数据且有隐私保护的限制,数据量过大且面临法律纠纷的风险<sup>[3]</sup>。由于上述两种检测方式存在一些不足,本文采用基于网络流量的异常检测方案,分析恶意入侵的行为模式、处理特定网络中的流量数据,避免伪装带来的干扰,降低数据规模。

收稿日期:2018-04-08;修回日期:2018-06-04;录用日期:2018-06-04。    基金项目:国家重点研发计划项目(017YFC0804402)。

**作者简介:**方圆(1983—),男,安徽黄山人,工程师,硕士,主要研究方向:信息安全; 李明(1971—),男,安徽合肥人,高级工程师,主要研究方向:信息安全; 王萍(1975—),女,安徽桐城人,高级工程师,主要研究方向:信息安全; 江兴何(1993—),男,安徽亳州人,硕士研究生,主要研究方向:深度学习; 张信明(1964—),男,安徽天长人,教授,博士,CCF高级会员,主要研究方向:无线网络、大数据、智能电网。



网络流量异常检测的方案需要先通过网络嗅探工具例如:Sniffer、NetFlow 和 flow-tools 等,周期性地采集来自网络数据流各分组不同维度数据的属性值或统计值作为原始的训练数据,预处理后再通过数据挖掘、统计学习、深度学习等方法去探测网络中存在的异常网络连接、数据转发、网络分组等。按照检测数据覆盖的范围可把异常检测方案分为两类:第一类是基于单一链路的入侵攻击异常检测;第二类是基于全网流量矩阵的入侵攻击异常检测。单一链路的入侵检测往往是考虑单链路流量数据的时间相关性,使用机器学习如朴素贝叶斯(Naive Bayes)<sup>[4]</sup>、支持向量机(Support Vector Machine, SVM)<sup>[5]</sup>等模型进行训练;全网流量矩阵则是利用各分组不同维度的数据属性,分析多条链路网络流量的空间相关性并针对全网流量高维度的特点使用主成分分析法(Principal Component Analysis, PCA)来降低数据维度<sup>[6]</sup>,提取出多个主要特征来进行分析。

全网流量矩阵数据中特征维度很高,一般的机器学习方法难以发现高维度特征之间的相关性,不能将 APT 入侵时不同主机的网络流量联系起来。卷积神经网络(Convolutional Neural Network, CNN)能很好地提取二维数据中不同特征之间的联系,通过不同的卷积核设置,CNN 能提取出流量矩阵中不同位置特征之间的深层特性,挖掘数据之间未知的恶意行为特征;此外,考虑到网络入侵行为往往会持续一段时间,通过分析流量矩阵在一段时间内的变化能更好地检测到入侵行为的发生,循环神经网络(Recurrent Neural Network, RNN)能将数据按照时间进行处理,层层训练获得流量数据在时间维度上变化的特性,找出流量数据内在的时间依赖。因此,为了提高 APT 入侵检测的效果,综合考虑了恶意入侵所带来网络流量的时间相关性和空间相关性,本文提出了一种基于混合卷积神经网络和循环神经网络(Hybrid Convolutional and RNN, H-CRNN)的入侵检测模型。相对于传统的机器学习模型,混合型深度学习网络结构能挖掘全网流量矩阵更复杂的结构特征,能对未知的恶意行为特征进行提取和封装。首先,通过 CNN 提取网络流量矩阵中的不同特征空间之间的相关性,再利用 RNN 进一步找出入侵流量数据在时间上依赖性,充分挖掘全网流量矩阵中的时空特征,提高入侵检测模型的准确性。

## 1 问题描述及模型介绍

### 1.1 问题描述

APT 攻击往往针对高价值的目标,使用多种先进的入侵手段,不间断地进行入侵攻击来窃取目标网络的数据或者进行破坏。如图 1 所示,网络入侵攻击大致可分为六个阶段<sup>[7]</sup>。入侵在不同阶段具有不同的实施步骤,检测模型要确保在攻击收益阶段之前探测到入侵行为,及时处理恶意攻击。电力信息网络作为电力运行控制的核心,难免会遭到各类先进的 APT 攻击,需要部署灵敏的 APT 检测系统,通过分析全网流量的特征及时地发现攻击活动。电力信息网络中记录了大量网络流量日志信息,预处理之后使用入侵模型进行判断,可以实时判断当前网络中是否存在入侵活动。由于 APT 攻击具有阶段性、多目标性等特点,构建网络流量检测模型时不仅要考虑到恶意行为在网络流量时间上的相关性,也要将空间上的相关性融入到模型中。此外网络流量中能提取的特征很

多,为了避免“维度灾难”,本文参考文献[5]中数据集 KDD 99 所包含的网络流量的基本属性,统计网络中不同链路中 TCP 连接的基本属性,如连接所持续的时长、协议的具体类型等;TCP 连接内容属性,如一段时间文件被操作的次数、shell 被使用的次数等;基于时间流量的统计属性,如一个周期内具有相同连接目标主机的数量等;基于主机的流量属性,如一定连接次数下具有相同目标或相同服务的比例等<sup>[8]</sup>。



图 1 APT 攻击的各阶段

Fig. 1 Stages of APT attack

### 1.2 卷积神经网络

卷积神经网络是由 Lecun 等<sup>[9]</sup>提出的一种能实现深度神经网络中局部感知、权值共享等功能的网络,其网络结构包含卷积层和池化层。卷积层作为 CNN 结构的核心部分,它的设计动机是减少参数数量、模拟生物行为、提取数据之间的深层特性等,通过局部连接降低高维度的输入数据带来的时间和空间代价。其中一个神经元只需与部分神经元连接,而没有必要对整体进行感知;池化层常常对应于统计函数如最大值、 $L_2$  范数、加权平均值等,用于降低参数规模和保持线性变换过后结果不变。卷积层提取的特征在用于分类模型的训练时,考虑到特征在不同位置具有空间局部性,需要使用池化层对不同位置的特征进行一定程度的聚合统计,降低数据维度,减少过拟合的问题。

图 2 是卷积神经网络的结构,其中包含 2 个卷积层和 2 个池化层,整个卷积网络的数据处理步骤如下:

C1 层:一个  $28 \times 28$  的矩阵  $A$  作为此次卷积网络的输入,经过  $M$  个  $5 \times 5$  的卷积核  $K_i^1$  ( $i = 1, 2, \dots, M$ ) 的卷积计算后生成  $M$  个  $24 \times 24$  的 feature map,第  $i$  个卷积核的卷积运算和激活函数处理如下:

$$\begin{cases} C_i^1 = \text{conv2}(A, K_i^1, 'valid') + b_i^1 \\ a_i^1 = f(C_i^1) \end{cases} \quad (1)$$

在经过卷积运算后通常会再连接一个激活层,把非线性特征引入一个刚经过线性卷积运算的系统,避免输入层仅仅对上一层的结果作一个简单的线性变换。

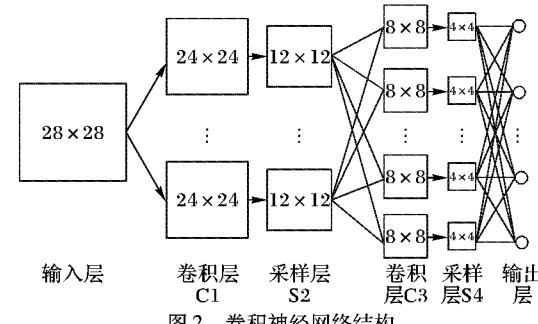


图 2 卷积神经网络结构

Fig. 2 Architecture of CNN

S2 层:第一次采样窗口大小为  $2 \times 2$ ,输入的  $24 \times 24$  的矩阵被池化成一个  $12 \times 12$  大小的 pool map,为了使得采样层具有学习性,加入标量  $M$  个卷积核使得生成  $M$  个 pool map:

$$\begin{cases} S_i^2 = \beta_i^2 \text{down}(a_i^1) + b_i^2 \\ a_i^2 = f(S_i^2) \end{cases} \quad (2)$$

C3 层:第二次卷积,C3 层中的每个  $8 \times 8$  的 feature map  $C_i^3$



都由 S2 中的 pool map 经过  $5 \times 5$  的卷积核  $\mathbf{K}_j^3 (j = 1, 2, \dots, M)$  生成 feature map, 第  $i$  个卷积核的卷积运算和激活函数处理如式(3) 所示:

$$\begin{cases} \mathbf{C}_i^3 = \sum_{j=1}^M \text{conv2}(\mathbf{a}_j^2, \mathbf{K}_j^3, \text{'valid'}) + \mathbf{b}_j^3 \\ \mathbf{a}_i^3 = f(\mathbf{C}_i^3) \end{cases} \quad (3)$$

S4 层: 第二次采样, 大小为  $2 \times 2$  的采样窗口将  $8 \times 8$  的 feature map 池化成一个  $4 \times 4$  的 pool map, 第  $i$  个采样结果为:

$$\begin{cases} \mathbf{S}_i^4 = \beta_i^4 \text{down}(\mathbf{a}_i^3) + \mathbf{b}_i^4 \\ \mathbf{a}_i^4 = f(\mathbf{S}_i^4) \end{cases} \quad (4)$$

最后将  $\mathbf{a}_i^4$  顺序展开为向量, 并有序连接成一个长向量作为全连接层网络的输入。在卷积神经网络中, 反向传播计算在不同处理层中采取的方式不同, 与卷积层  $l$  的神经元  $\delta$  相关的  $l+1$  层神经元通过上采样 up 的处理式(5) 所示:

$$\begin{cases} \delta_i^l = \beta_i^{l+1} (\mathbf{a}(\mu_i^l) \circ \text{up}(\delta_i^{l+1})) \\ \frac{\partial J}{\partial \mathbf{b}_i^l} = \sum_{s,t} (\delta_i^l)_{st} \\ \frac{\partial J}{\partial \mathbf{K}_{ij}^l} = \sum_{s,t} (\delta_i^l)_{st} (\mathbf{P}_j^{l-1})_{st} \end{cases} \quad (5)$$

其中:  $(\Phi)_{st}$  表示为遍历  $\Phi$  的元素;  $(\mathbf{P}_j^{l-1})_{st}$  由  $\delta_i^l$  在  $l-1$  层连接的与  $\mathbf{a}_j^{l-1}$  相关的元素而组成; “ $\circ$ ” 为逐元素相乘。类比到池化层, 对应的处理如式(6) 所示:

$$\begin{cases} \delta_i^l = \sum_{j=1}^{N_l} \mathbf{a}_i^l \circ \text{conv2}(\delta_j^{l+1}, \mathbf{K}_j^{l+1}, \text{'full'}) \\ \frac{\partial J}{\partial \mathbf{b}_i^l} = \sum_{s,t} (\delta_i^l)_{st} \\ \frac{\partial J}{\partial \mathbf{b}_i^l} = \sum_{s,t} (\delta_i^l \circ d_i^{l-1})_{st} \end{cases} \quad (6)$$

其中:  $N_l$  为  $l$  层中 pool map 的数量。

### 1.3 循环神经网络

循环神经网络能对时间序列数据进行建模, 将数据流按照循环的方式来层层处理, 其显著的特点是具有持续性和记忆性<sup>[10]</sup>。持续性是指在时间序列的数据中, 时间前后关系的数据并不是独立的, 而是具有某种内在的依赖性, 某个阶段的输入不仅仅和当前阶段的数据相关也受过去信息的影响; 记忆性是指 RNN 在处理序列数据时, 具备保留过去信息的能力。入侵检测需要挖掘数据流量中的时间相关特征, 同类型的统计数据之间隐藏着复杂的内在联系, 考察当前状态时不应该抛弃过往的结果。在时间和空间相关的场景中, 这些数据更是存在着不同的组合关系, 数据特征的糅合多种多样。为了挖掘深藏的依赖关系, 本文使用 RNN 去处理 CNN 所提取的特征数据。

在任意的时间  $t$ , 隐藏层和输出层处理如下:

$$\mathbf{s}_t = \text{sigmoid}(\mathbf{U}^T \times \mathbf{x}_t + \mathbf{W}^T \times \mathbf{s}_{t-1}) \quad (7)$$

$$\mathbf{o}_t = \text{softmax}(\mathbf{V}^T \times \mathbf{s}_t) \quad (8)$$

基保:  $\mathbf{U}$  是连接输入层和隐藏层的权重矩阵;  $\mathbf{W}$  是两个隐藏层之间连接的权重矩阵;  $\mathbf{V}$  是隐藏层到输出层的权重矩阵。反向传播时, 导入数据的损失函数可通过如式(9) 得出:

$$C(\mathbf{o}, y) = \sum_t C(\mathbf{o}_t, y_t) = \sum_t \ln(\mathbf{o}_t)_{y_t} \quad (9)$$

使用梯度下降来对其中的参数进行更新, 将任意时间的损失  $C(\mathbf{o}_t, y_t)$  对  $\mathbf{V}$  求导结果如下:

$$\frac{\partial C(\mathbf{o}_t, y_t)}{\partial \mathbf{V}} = \frac{\partial -\ln(\mathbf{o}_t)_{y_t}}{\partial \mathbf{V}} = \mathbf{s}_t \times (\mathbf{o}_t - \mathbf{e}(y_t))^T \quad (10)$$

其中:

$$\begin{cases} \mathbf{e}(y_t) = (1_{(y_t=1)}, 1_{(y_t=2)}, \dots, 1_{(y_t=d)})^T \\ \mathbf{o}_t = ((\mathbf{o}_t)_1 (\mathbf{o}_t)_2, \dots, (\mathbf{o}_t)_d)^T \\ \mathbf{s}_t = ((\mathbf{s}_t)_1 (\mathbf{s}_t)_2, \dots, (\mathbf{s}_t)_m)^T \end{cases} \quad (11)$$

$m$  为输入神经元个数;  $d$  为输出神经元个数。从结果可以看出对  $\mathbf{V}$  求导并不因为时间流逝而导致梯度的消失。损失函数  $C(\mathbf{o}_t, y_t)$  对  $\mathbf{W}$  求导的结果如式(12) 所示:

$$\frac{\partial -\ln(\mathbf{o}_t)_{y_t}}{\partial \mathbf{W}_{ij}} = \frac{-1}{(\mathbf{o}_t)_{y_t}} \times \frac{\partial (\mathbf{o}_t)_{y_t}}{\partial s_t} \times \sum_{i=0}^t \left( \frac{\partial s_t}{\partial s_i} \times \frac{\partial s_i}{\partial \mathbf{W}_{ij}} \right) \quad (12)$$

但是当时间序列跨度过长时会出现梯度消失的问题, 即梯度计算结果随着一层层的传递而指数级的降低, 此时一种基于 RNN 的改进的门控递归单元 (Gated Recurrent Unit, GRU)<sup>[11]</sup> 可以处理这样的问题。GRU 网络作为处理隐藏层的方式, 其原理如图 3 所示。

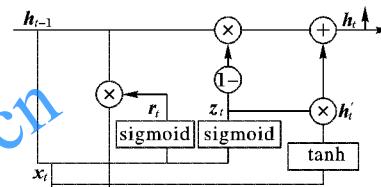


图 3 单个 GRU 网络节点结构

Fig. 3 Architecture of single GRU network node

GRU 含有重置门( $r_t$ ) 和更新门( $z_t$ ) 两类门。 $r_t$  用来保存所需多少个时间步之前的记忆, 其取值会影响过去记忆的信息与当前的组合;  $z_t$  确定了遗忘上一个时间的隐藏层  $\mathbf{h}_{t-1}$  多少信息, 和获取当前隐藏层  $\mathbf{h}'_t$  中的多少信息。

$$r_t = \text{sigmoid}(\mathbf{W}_r^T \times \mathbf{h}_{t-1} + \mathbf{U}_r^T \times \mathbf{x}_t + \mathbf{b}_r) \quad (13)$$

$$z_t = \text{sigmoid}(\mathbf{W}_z^T \times \mathbf{h}_{t-1} + \mathbf{U}_z^T \times \mathbf{x}_t + \mathbf{b}_z) \quad (14)$$

$$\mathbf{h}'_t = \tanh(\mathbf{W}_{h'}^T \times (r_t \circ \mathbf{h}_{t-1}) \mathbf{x}_t + \mathbf{U}_{h'}^T \times \mathbf{x}_t + \mathbf{b}_{h'}) \quad (15)$$

$$\mathbf{h}_t = z_t \circ \mathbf{h}_{t-1} + (1 - z_t) \circ \mathbf{h}'_t \quad (16)$$

其中: “ $\circ$ ” 表示矩阵逐元素点乘;  $\mathbf{W}_x^T$  为隐藏层到其他层的权重矩阵;  $\mathbf{U}_x^T$  为输入层到其他层的权重矩阵;  $\mathbf{b}_x$  为各层输出时添加的偏移量。当  $z_t$  设为 0 时, 当前时刻会选择丢弃过去隐藏层的结果, 用于过去的发生的情况对后来没有影响的场景; 若  $z_t$  设为 1, 则是把过去的隐藏层信息复制到当前时刻, 针对长距离的学习场景。

### 1.4 混合 CNN 和 RNN 的网络模型

如图 4 所示, 全网流量矩阵先经过 CNN 处理, 提取出网络流量的空间特征, 输出按时间排列的分组数据, 再通过 RNN 对已经时间序列化的数据进行训练最终得到结果。为了解决传统的矩形卷积核难以在二维矩阵中采集离散分布的特征的问题, 通过给训练的卷积窗口增加一个随机的偏移向量的方式获得可变的卷积核来处理 CNN 中的卷积和池化操作<sup>[12]</sup>, 其思想核心是对原有 CNN 中的采样方式进行一定的改进。

首先给出一个与输入矩阵窗口大小相同的偏移域( offset



field), 卷积窗口在偏移域中滑动得出卷积偏移的效果, 以此达到优化采样空间的效果。9 种偏移向量如下所示:

$$\Gamma = ((-1, -1), (-1, 0), \dots, (1, 1)) \quad (17)$$

任意一个点可以向周围八个方向偏移。原有的卷积的输出结果经过式(18)可得:

$$y(\mathbf{P}_g) = \sum_{\mathbf{P}_n \in \Gamma} w(\mathbf{P}_n) \cdot x(\mathbf{P}_g + \mathbf{P}_n) \quad (18)$$

每个卷积窗口每个元素  $\mathbf{P}_n$  有权重  $w$ , 其中  $\mathbf{P}_g$  则代表每个窗口输出的任意元素。通过加上  $\Delta\mathbf{P}_n$ , 可以使输入的数据矩阵  $x$  进行偏移:

$$y(\mathbf{P}_g) = \sum_{\mathbf{P}_n \in \Gamma} w(\mathbf{P}_n) \cdot x(\mathbf{P}_g + \mathbf{P}_n + \Delta\mathbf{P}_n) \quad (19)$$

其中:  $\Delta\mathbf{P}_n$  用来处理  $x$  输入层对应元素的采样, 对窗口元素权重  $w$  没有约束, 这里需要对  $w$  和  $\Delta\mathbf{P}_n$  两组参数进行训练。对于可变形的池化区域也可以通过类似的变形步骤, 将传统的池化区域转化成大小为 bin 的特征图:

$$y(i, j) = \sum_{\mathbf{P} \in \text{bin}(i, j)} x(\mathbf{P}_g + \mathbf{P}) / n_{ij} \quad (20)$$

其中:  $\mathbf{P}_g$  是池化区域上某个点;  $n_{ij}$  对应 bin 大小的特征图中元素的个数。再通过对池化区域进行偏移变形计算得出最终的池化区域:

$$y(i, j) = \sum_{\mathbf{P} \in \text{bin}(i, j)} x(\mathbf{P}_g + \mathbf{P} + \Delta\mathbf{P}_{ij}) / n_{ij} \quad (21)$$

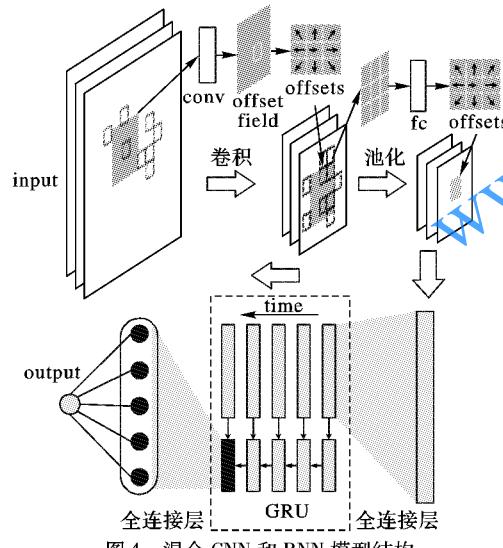


Fig. 4 Architecture of hybrid CNN and RNN model

## 2 模型性能评估

### 2.1 实验设置

本文实验是在 Linux 仿真平台上基于 TensorFlow<sup>[13]</sup>深度学习框架来进行训练的。实验包含两类数据:第一类数据来源于含有大量先进 APT 攻击技术的恶意软件数据库<sup>[14]</sup>; 第二类数据是 Predict 网络中“Defense Advanced Research Projects Agency (DARPA) Scalable Network Monitoring (SNM) Program Traffic”分类下的良性数据<sup>[15]</sup>。真实场景中的 APT 攻击往往隐藏在大量的正常网络数据流中, 本文将这两类数据融合在一起使得数据来源更贴近现实。APT 攻击常常使用多种先进的攻击手段而且攻击时间往往持续几天甚至几个星期。本文实验选取 40 个 IP 地址作为监听对象, 记录恶意入侵时各种网络流量特征的统计值, 收集其一个月的网络流量

数据。每个统计值数据 50 ms 更新一次, 间隔 5 s 得到一份全网流量矩阵原始样本。最后利用 4 GB 左右的 DAPRA 良性样本和 848 MB 的 APT 标记的恶意样本来进行模型训练。图 5 是数据处理的大致流程。

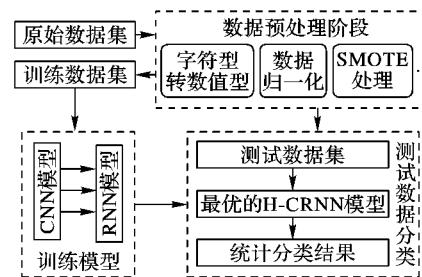


图 5 H-CRNN 模型训练过程

Fig. 5 H-CRNN model training process

通过观察损失值 (loss) 下降曲线图和准确率变化趋势, 在较大学习率时确定合适的参数范围, 循环缩小超参数的搜索空间。然后降低学习率, 利用网格搜索 (grid search) 的方式进行大量训练找出最优的模型参数。本文模型的 CNN、全连接层 (Fully Connected layer, FC) RNN 各超参数如表 1 所示。系统硬件配置如下:CPU 为 Intel Core i7 7700K, 内存为 DDR4 2333 MHz 64 GB, 显卡为 NVIDIA GTX 1080Ti。如图 6 所示, 在训练初期模型 loss 震荡下降, 训练后期损失值不再随着训练步数增加而减少。图 7 中模型预测准确率 (accuracy) 在训练初期随着训练步数增而加快上升, 训练后期预测准确率基本维持在 95.5% 左右。整个训练时间约 4.3 h。

表 1 各模块参数设置

Tab. 1 Parameters setting for each module

参数名称	CNN	FC	RNN
批处理尺寸	64	64	64
卷积核大小	[3, 3]	—	—
步长	[2, 2]	—	—
隐藏层神经元个数	第 1 层 40 第 2 层 60 第 3 层 80	第 1 层 1024 第 2 层 512 第 3 层 80	字向量维数: 256 LSTM: 128
输出层神经元个数	2000	256	1
激活函数	ReLU	Leaky ReLU	Sigmoid
dropout	—	0.3	0.5
下降方式	ADAM 优化	ADAM 优化	ADAM 优化
L2 正则化系数	$5 \times 10^{-4}$	$10^{-5}$	—
学习速率	$2 \times 10^{-4}$	$10^{-5}$	初始值: 0.1 衰减率: 0.9
max_epoch	—	—	20

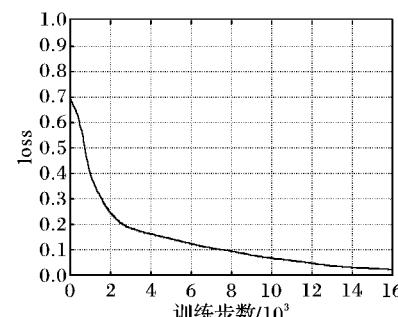


图 6 H-CRNN 模型损失值

Fig. 6 Loss of H-CRNN model

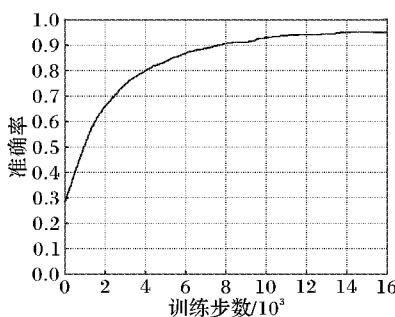


图 7 H-CRNN 模型准确率  
Fig. 7 Accuracy of H-CRNN model

## 2.2 实验结果与分析

为了验证本文模型的有效性, 表 2 给出了分类问题预测结果的交叉矩阵。测试样本总数  $S = TP + FN + FP + TN$ , 其中正确预测的样本数为  $TP + TN$ , 错误预测的样本数为  $FP + FN$ , 通用的样本分类问题评价指标如下。

误报率是预测为恶意样本中良性样本的比值, 表达式如下:

$$\text{误报率} = \frac{FN}{TP + FN} \quad (22)$$

查准率(*Precision*)是预测为良性的样本中, 真实值为良性样本的比值, 表达式如下:

$$\text{Precision} = \frac{TP}{TP + FP} \quad (23)$$

查全率(*Recall*)是真实的良性样本占预测为良性样本的比值, 表达式如下:

$$\text{Recall} = \frac{TP}{TP + FN} \quad (24)$$

*F1* 度量是精确度和召回率的平衡点, 可以看作是精确度和召回率的调和平均数, 表达式如下:

$$F1 = \frac{2}{\frac{1}{\text{Recall}} + \frac{1}{\text{Precision}}} = \frac{2 \times TP}{S + TP - TN} \quad (25)$$

表 2 分类结果的混淆矩阵  
Tab. 2 Confusion matrix of classification results

样本真实属性	样本预测结果	
	良性样本	恶意样本
良性样本	正确预测- <i>TP</i>	错误预测- <i>FN</i>
恶意样本	错误预测- <i>FP</i>	正确预测- <i>TN</i>

将本文模型 H-CRNN 与已有的基于单链路流量的 Naive Bayes<sup>[4]</sup>、SVM<sup>[5]</sup> 和基于全网流量矩阵的 PCA-based<sup>[6]</sup> 进行对比。随机截取数据集中 1/4 的数据作为测试集, 各模型预测结果统计如表 3 所示。混合模型能综合考虑发生 APT 攻击时网络流量的空间相关性和时间相关性, 使得模型在查准率、查全率、*F1* 度量上都有一定程度的提升。除此以外, 相对于其他模型, 本文模型 H-CRNN 大幅降低了误报率, 减少人力排查的时间。

图 8 给出四种模型的 ROC 曲线, 其中横坐标假正例率定义为  $FP/(TN + FP)$ , 纵坐标真正例率定义为  $TP/(TP + FN)$ 。H-CRNN 模型的 ROC 曲线一直位于其他模型的上方, 曲线下方的面积(Area Under Curve, AUC)相对于其他模型有 7.5% ~ 14.0% 的提升, 表明所提模型在综合性上能有了一定

的提高。

表 3 不同模型的分类结果统计

Tab. 3 Classification results of different models

算法	查准率/%	查全率/%	<i>F1</i> 度量/%	误报率/%
Naive Bayes	87.17	83.08	84.21	3.80
SVM	91.70	89.97	88.95	1.31
PCA-based	90.35	89.46	91.40	1.45
H-CRNN	95.17	93.32	94.24	0.62

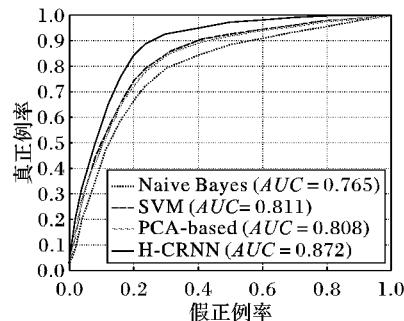


图 8 不同模型的 ROC 曲线  
Fig. 8 Different models' ROC curves

## 3 结语

本文针对电力信息网络中 APT 攻击问题设计一种高效的人侵检测模型。这种新型的人侵检测模型采用了混合卷积神经网络和循环神经网络的结构, 能综合分析 APT 攻击时网络流量的时空特性。除此以外, 本文在卷积核的设计上, 给卷积核添加随机偏移量来处理更广的空间特征, 使得模型具有更高的灵敏度和更低误报率。实验结果表明, 该模型在各项通用指标上都有一定的提升。值得注意的是, 针对不断迭代的各种网络人侵攻击, 实际部署的检测模型需要定期进行训练更新。

### 参考文献(References)

- [1] HU P, LI H, FU H, et al. Dynamic defense strategy against advanced persistent threat with insiders[ C]// INFOCOM 2015: Proceedings of the 2015 IEEE Conference on Computer Communications. Piscataway, NJ: IEEE, 2015: 747 – 755.
- [2] LIANG G, WELLERS R, ZHAO J, et al. The 2015 Ukraine black-out: implications for false data injection attacks[ J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317 – 3318.
- [3] 付钰, 李洪成, 吴晓平, 等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1 – 14. (FU Y, LI H C, WU X P, et al. Detecting APT attacks: a survey from the perspective of big data analysis[ J]. Journal on Communications, 2015, 36(11): 1 – 14.)
- [4] DASH S K, REDDY K S, PUJARI A K. Adaptive Naive Bayes method for masquerade detection[ J]. Security and Communication Networks, 2011, 4(4): 410 – 417.
- [5] PERVEZ M S, FARID D M. Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs[ C]// SKIMA 2014: Proceedings of the 2014 8th International Conference on Software, Knowledge, Information Management and Applications. Piscataway, NJ: IEEE, 2014: 1 – 6.

(下转第 2917 页)



对安全容量、安全中断概率等物理层安全关键性能的分析,得到了不同参数对网络安全的影响。针对多天线系统提出了一种安全波束成型方法。采用所提出了安全波束成型方法,全双工无线供能物联网比传统的半双工物联网在安全容量和安全中断概率上有较大的性能提升。

但是,本文仿真环境基于软件仿真和参数的假设,与实际真实网络可能存在区别,例如只考虑了单一窃听器对安全性能的影响,受限于篇幅未能进一步分析多干扰器联合干扰的情况,需要在未来结合实际网络环境进行验证。

#### 参考文献(References)

- [1] MUKHERJEE A, FAKOORIAN S A A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey [J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550 – 1573.
- [2] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1): 40 – 53. (WU C K. An overview on the security techniques and challenges of the Internet of things [J]. Journal of Cryptologic Research, 2015, 2(1): 40 – 53.)
- [3] BI S, ZENG Y, ZHANG R. Wireless powered communication networks: an overview [J]. IEEE Wireless Communications, 2016, 23(2): 10 – 18.
- [4] 黄博闻. 无线供电网络的多维资源优化分配研究 [D]. 杭州: 浙江理工大学, 2017: 11 – 17. (HUANG B W. Optimal allocation of multidimensional resource in wireless powered communication networks [D]. Hangzhou: Zhejiang Sci-Tech University, 2017: 11 – 17.)
- [5] ZHAI D, CHEN H, LIN Z, et al. Accumulate then transmit: multi-user scheduling in full-duplex wireless-powered IoT systems [EB/OL]. [2018-03-20]. <https://arxiv.org/abs/1803.02023>.
- [6] KANG X, LIANG Y C, YANG J. Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices [C]// ICC 2017: Proceedings of the 2017 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2017: 1 – 6.
- [7] WU Q, CHEN W, NG D W K, et al. Spectral and energy efficient wireless powered IoT networks: NOMA or TDMA? [J]. IEEE Transactions on Vehicular Technology, 2018, 67(7): 6663–6667.
- [8] GHADERIPOOR A, TELLAMBURA C, PAULRAI A. On the application of character expansions for MIMO capacity analysis [J]. IEEE Transactions on Information Theory, 2012, 58(5): 2950 – 2962.
- [9] JAMALI V, AHMADZADEH A, SCHOBER R. On the design of matched filters for molecule counting receivers [J]. IEEE Communications Letters, 2017, 21(8): 1711 – 1714.
- [10] GULCU T C, BARG A. Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component [J]. IEEE Transactions on Information Theory, 2017, 63(2): 1311 – 1324.
- [11] WU H, TAO X, LI N, et al. Secrecy outage probability in multi-RAT heterogeneous networks [J]. IEEE Communications Letters, 2016, 20(1): 53 – 56.
- [12] ZHANG H, LIU H, CHENG J, et al. Downlink energy efficiency of power allocation and wireless backhaul bandwidth allocation in heterogeneous small cell networks [J]. IEEE Transactions on Communications, 2017, 66(4): 1705 – 1716.

LIU Ming, born in 1987, Ph. D. candidate. His research interests include duplex wireless communication, wireless resource management.

MAO Yuming, born in 1956, M. S., professor. His research interests include broadband communication network, wireless communication network.

LENG Supeng, born in 1973, Ph. D., professor. His research interests include Internet of vehicles, next generation mobile network.

(上接第 2907 页)

- [6] CAMACHO J, PEREZ-VILLEGRAS A, GARCIA-TEODORO P, et al. PCA-based multivariate statistical network monitoring for anomaly detection [J]. Computers & Security, 2016, 59: 118 – 137.
- [7] CHEN P, DESMET L, HUYGENS C. A study on advanced persistent threats [C]// CMS 2014: Proceedings of the 2014 IFIP International Conference on Communications and Multimedia Security. Berlin: Springer, 2014: 63 – 72.
- [8] KDD cup 1999 data [EB/OL]. [2018-01-20]. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.
- [9] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition [J]. Proceedings of the IEEE, 1998, 86(11): 2278 – 2324.
- [10] GRAVES A, MOHAMED A, HINTON G. Speech recognition with deep recurrent neural networks [C]// ICASSP 2013: Proceedings of the 38th IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway, NJ: IEEE, 2013: 6645 – 6649.
- [11] CHUNG J, GULCEHRE C, CHO K H, et al. Empirical evaluation of gated recurrent neural networks on sequence modeling [EB/OL]. [2018-01-10]. <https://arxiv.org/abs/1412.3555>.
- [12] DAI J, QI H, XIONG Y, et al. Deformable convolutional networks [EB/OL]. [2018-01-10]. [http://openaccess.thecvf.com/content\\_ICCV\\_2017/papers/Dai\\_Deformable\\_Convolutional\\_Networks\\_ICCV\\_2017\\_paper.pdf](http://openaccess.thecvf.com/content_ICCV_2017/papers/Dai_Deformable_Convolutional_Networks_ICCV_2017_paper.pdf).
- [13] ABADI M, BARHAM P, CHEN J, et al. TensorFlow: a system

for large-scale machine learning [C]// OSDI 2016: Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2016: 265 – 283.

- [14] Mila parkour. (2013) Contagio malware database [EB/OL]. [2018-01-26]. [https://www.mediafire.com/folder/c2az029ch6cke/TRAFFIC\\_PATTERNS\\_COLLECTION#734479hwy1b97](https://www.mediafire.com/folder/c2az029ch6cke/TRAFFIC_PATTERNS_COLLECTION#734479hwy1b97).
- [15] Predict. (2009) DARPA Scalable Network Monitoring (SNM) Program Traffic [EB/OL]. [2018-01-26]. [https://ant.isi.edu/datasets/readmes/DARPA\\_Scalable\\_Network\\_Monitoring-20091103 README.txt](https://ant.isi.edu/datasets/readmes/DARPA_Scalable_Network_Monitoring-20091103 README.txt).

This work is partially supported by National Key Research and Development Program of China (017YFC0804402).

FANG Yuan, born in 1983, M. S., engineer. His research interests include information security.

LI Ming, born in 1971, senior engineer. His research interests include information security.

WANG Ping, born 1975, senior engineer. Her research interests include information security.

JIANG Xinghe, born in 1993, M. S. candidate. His research interests include deep learning.

ZHANG Xinning, born in 1964. Ph. D., professor. His research interests include wireless networks, big data, smart grid.