文章编号：2095-2163(2019)06-0073-04 中图分类号：TP393.08 文献标志码：A

一种基于深度学习的网络安全态势评估方法

叶 亮[1,2]，谭振江[1]
（1 吉林师范大学 计算机学院，吉林 四平 136000；2 四平市公路管理处，吉林 四平 136000）

摘 要：提出一种使用深度学习方法对网络环境进行态势评估的方法。根据网络扫描过程中获取的风险信息进行分类和特征提取，训练深度学习网络，并根据学习结果预测攻击对网络造成的影响，同时对当前网络态势进行整体评估。针对网络整体的安全问题进行定量描述，从而可以对不同协议层、不同来源、不同手段的攻击进行风险评价，并调度资源进行拦截及防护。

关键词：网络安全态势；深度学习；态势评估

A method of network security situation assessment based on deep learning

YE Liang[1,2], TAN Zhenjiang[1]
(1 College of Computer, Jilin Normal University, Siping Jilin 136000, China;
2 Siping Highway Administration Office, Siping Jilin 136000, China)

【Abstract】 A method of situation assessment of network environment based on deep learning is proposed. Risk network message which acquired in scanning is classified and its feature is extracted to train the CNN to predict the impact of attacks on the network. At the same time, the current network situation is evaluated as a whole. Quantitative description of the overall network security problem can be used to evaluate the risk of attacks from different protocol layers, different sources and different means, in order to schedule resources for interception and protection.

【Key words】 network security situation; deep learning; situation assessment

0 引 言

随着网络规模的不断扩展，网络安全问题的规模也随之扩大，攻击手段也不断在更新，这使得网络安全面临着数据规模庞大、识别方式复杂以及面对问题不断更新的挑战。在现实情况中，使网络中的所有接入设备都完全处于安全状态也相当艰难。

与传统的网络安全要求不同，网络安全态势感知不关注个体的状态，也不仅局限于检测一种特定类型的攻击。而是从宏观角度对当前网络的安全状态进行描述和评估，更关注于对整体网络的全部要素进行获取、整理、分析、理解，最终得到当前网络安全的总体评价及发展趋势[1]。其主要研究集中在可视化、分层和融合三条主线上。

(1)可视化侧重于人机交互的应用，管理人员易于从管理工具中直观检测到当前状况，主要根据对系统的日志分析来回答是否有攻击[2]，来自何处的攻击以及攻击的影响等[3]。但是该主线上较少关注网络管理设备的自主分析，而是依赖于系统管理员的经验或专家知识。

(2)在层次化的结构上[4-5]，将不同类型的硬件、服务、软件定义为不同层次上的节点，而在不同层次上，根据重要程度和对网络产生的影响定义其权值，自底向上，逐层评估，得到总体的概况，在这类认知的前提下，研究得到一系列评估的模型，大多数模型的框架建立在数据收集——规范化——权值生成——评价的过程上，而模型的区别在于数据来源[7]、清洗算法和权值学习算法[8-9]等方面。

(3)网络安全态势使用数据融合，来自不同层次的数据结果的总和能够对态势进行描述[10-12]。

数据分层和融合两条主线对安全态势的认知基础来源于不同软硬件或不同服务的数据，分层更注重来源数据的评价，融合则更侧重于数据的融合，而可视化将二者结果直观地表达出来。

综合各条主线，网络安全态势评估实际上表达的是对网络整体动态的综合评价，这种评价建立在

基金项目：吉林省教研项目(2017ZCZ045)；赛尔网络下一代互联网技术创新项目(NGII20180408)；吉林师范大学学术型研究生项目(研创新201951)。

作者简介：叶 亮(1982-)，男，硕士研究生，主要研究方向：网络安全、深度学习；谭振江(1965-)，男，博士后，教授，博士生导师，主要研究方向：网络与信息安全。

收稿日期：2019-10-11

较大规模的数据基础上。在攻击手段技术不断更新,人为预期相对滞后的情况下,提出一种使用深度学习的态势评估方法,在卷积神经网络上建立起针对各层网络数据的特征提取和判断,最终获取对网络的评估结果。

1 模型框架

在卷积神经网络上构建对态势评估的模型,通过深度学习提取在大规模网络数据中的特征,并加以分析和评估。经典的卷积神经网络通常包括输入层、卷积层、池化层、全连接层和输出层等部分,接下来介绍将态势评估建立在卷积神经网络模型上的过程。

1.1 输入层

输入层是数据进入卷积神经网络的第一层,在该层进行数据的均值化、归一化、降维和白化。将不同形式、不同规则的数据进行标准化,以便于准确抽取特征和构建评价。网络扫描获取的数据源自网络不同层次,需要获取的数据不同,但是数据格式相对整齐。因此在数据进行归一化前,使用 $\boldsymbol{m} \times \boldsymbol{n}$ 维矩阵接收实际获取数据,并将来自网络不同层的数据分布在矩阵的不同维。如:当前的数据包括 IP 地址、加密后的用户名和密码及服务请求等信息,则将数据记录为 $4 \times \boldsymbol{n}$ 的矩阵,每一行获取的是一类信息。

对于矩阵中的数据进行归一化处理, 二元的定性信息定义为[0,1]上的实数,n 元定性信息定义为[1,| n |]上的整数,并可以通过函数映射到[0,1]上。定量信息根据数据分布和范围,通过函数映射到[0,1]上。并且可以将 $\boldsymbol{m} \times \boldsymbol{n}$ 维矩阵,压缩为 m 维向量。

1.2 卷积层

卷积层是卷积神经网络中的核心部分,通过卷积层,将归一化的数据进行特征提取,自动学习数据的属性。根据网络层的结构,相关联的数据总是在当前的上层或下层,因此使用大小为(3,3)的滤波器,并设置步长为 1。

卷积层接受来自输入层标准化的数据,在数据中进行特征提取,对于标准化数据的矩阵形式,大小为(3,3)的滤波器提取的是相邻 3 条数据;对于每条数据,每次提取 3 列的值,该值来源于相邻层的信息。滤波器每次提取当前层的信息,同时考虑当前层上层和下层对评估的影响,也考虑前后相邻数据对当前数据的影响。滤波器主要提取当前数据的当前层特征,较少考虑其它因素影响,滤波器将采用如下形式:

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{b} \\ \boldsymbol{c} & \boldsymbol{b} & \boldsymbol{b} \\ \boldsymbol{c} & \boldsymbol{b} & \boldsymbol{b} \end{bmatrix}. \tag{1}$$

其中, $a,b,c \in [0,1]$, 但是 $a \gg b \approx c$。虽考虑其它因素影响,但以当前数据为主。

1.3 池化层

池化层获取来自卷积层的矩阵,用于缩减来自卷积层数据规模。来自卷积层的数据,因滤波器的特征提取结果,得到特征明显的数据。在 $\boldsymbol{m} \times \boldsymbol{m}$ 的矩阵中表现为在第 i 行第 j 列($i \leqslant m$, $j \leqslant m$)的元素 a_{ij},与矩阵中其它元素有较大的差异(如远大于或远小于)。那么将 $\boldsymbol{m} \times \boldsymbol{m}$ 的矩阵化简为 1×1 的值,选择 a_{ij} 为池化层的特征值来表达。根据(1)式,通常选择得到的是过滤结果矩阵 $\boldsymbol{a}_{11}$ 的值。

1.4 全连接层和输出层

该层获取卷积层或池化层的矩阵数据,并将其变为列向量进行加权,并向输出层输出。将 $\boldsymbol{m} \times \boldsymbol{n}$ 的矩阵数据转为有 $\boldsymbol{m} \times \boldsymbol{n}$ 个元素的列向量。即

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \Rightarrow \left.\begin{bmatrix} a_{11} \\ \\ \vdots \\ \\ a_{mn} \end{bmatrix}\right\} m \times n;$$

对于列向量进行加权输出,得到输出层的最终结果。但是通常情况下, $\boldsymbol{m} \times \boldsymbol{n}$ 的值是一个较大的数字,对其进行加权输出的计算量也较大。可采用取平均值的方法解决,即若输出层结果为 y_o, 则有:

$$y_o = \frac{\sum_{i=1,j=1}^{m \times n} a_{ij}}{m \times n}.$$

最终,由输出层得到的结果再次进行白化,得到当前输入态势评估的赋值。对一定时间段内的态势进行评估,将得到赋值的分类。

2 各层算法

使用网络扫描数据进行训练和评估,算法执行过程如图 1 所示。算法形式化表示如下:

输入:扫描数据集 X, 人工判断结果集合 Y, 卷积过滤器组 $F = f_1 \cdots f_n$

输出:分类输出向量 T, 评估值 a

初始化:划分扫描数据集 X 为训练集和测试

集，$X = \{X_1 \cdots X_{10}\}$，对应结果集合 $Y = \{Y_1 \cdots Y_{10}\}$，设定卷积层数 m。

1. $M = SetNum(X)$ //将数据集数据化

2. $M_0 = AVG(M)$ //均值化

3. $M_1 = NOR(M_0)$ //归一化

4. $M_2 = PCA(M_1)$ //使用主成分分析降维

5. $M_3 = WHI(M_2)$ //白化

6. $While(|OT(X) - Y| > \varepsilon)$ //当输出层结果与实际结果不同

7. { $While(|OT\_f_i(X) - f_i(Y)| > \varepsilon)$ //当每层结果与实际每层结果不同

8. { $SetFl(F)$ //设置卷积过滤器

9. $M_4 = Get(M_3, F)$ //卷积输出

10. $OT\_f_i(X) = MaxP(M_4)$ } // 最大池化

11. $NextL(OT\_f_i(X))$ } // 向下一层传递

12. $T = OT(X)$ //获取输出向量

13. $a = \dfrac{T}{|T|}$ //使用向量均值作为评估结果

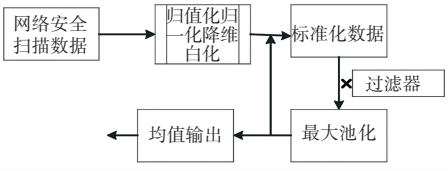

图 1　卷积神经网络处理过程

Fig. 1　Processing of CNN

在算法中，扫描数据集 X 可能获取到非数字化的结果，如 IP 地址、请求时间等，需将此类数据化为数字化结果。如来自内网地址记录为 0，外网地址为 1，不能获取地址为 -1；或更精确地，与当前网络地址的接近程度来标记 IP 地址的数字化结果等。

卷积过滤器使用 3×3，步长为 1 的矩阵与对应数据相乘，获取卷积后的结果。当预期值与实际值差值大于预期时，调整过滤器并进行进一步的计算。接下来使用该算法对网络扫描结果进行评估，获取实际评估值。

3　实验结果及分析

采用来自校园网络某月的扫描结果，对网络态势进行评估。扫描结果包括日期、时间、访问者 IP 地址、访问安全级别、访问类型等内容。对非定量信息进行分类标记，最终得出评价结果，如图 2 所示。

其中，纵轴表示评价值，横轴为依时间顺序选择的时间点，评价值在 0.5 附近为平均值。通常情况下，向上的高点为修复或拒绝某特定访问后的时段，而向下的低点为扫描发现攻击时段。

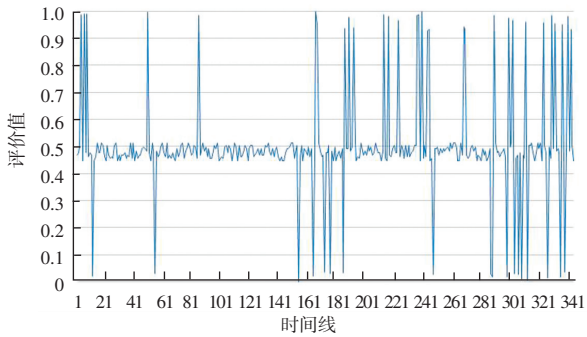

图 2　态势评价结果

Fig. 2　Result of situation assessment

使用深度学习方法可以处理网络多层或多步攻击情况，因此，在训练较好的深度学习方法中，能够对整体态势有更为精确的评估。在此基础上，将进一步研究不依赖于扫描结果，直接从访问数据中进行分析的方法，并且希望能够根据预测对网络资源进行调度。

4　结束语

训练深度学习网络，依赖校园网扫描到的风险数据，对网络风险和攻击进行特征提取和分类，对网络当前安全态势进行评估，从而进一步实现风险预测和网络资源调度。

参考文献

[1] WANG HQ, LAI JB, ZHU L, LIANG Y. Survey of network situation awareness system [J]. Journal of Computer Science, 2006,33(10):5-10.

[2] CHEN P, DESMET L, HUYGENS C. A study on advanced persistent threats[C].In:Proc. of the IFIP.2014,63-72.[doi:10.1007/978-3-662-44885-45].

[3] Mandiant APT1:Exposing One of China's Cyber Espion age Unit, 2013:http://www.cfr.org/china/mandiant-aptl-exposing-one-chinas-cyber-espionage-unints/p30020.

[4] CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2006,17(4):885-897.

[5] XI R R, YUN X C, ZHANG Y Z, HAO Z Y. An improved quantitative evaluation method for network security [J]. Chinese Journal of Computers, 2015,38(4):749-758.

[6] CUPPENS F, ORTALO R. Lambda: A language to model a database for detection of attacks [C]. In: Proc. of the 3rd Intelnational Workshop on Recent Advances in Intrusion Detection (RAID 2000), Vol.1907. 2000. 197-216.

[7] BHATT P, YANO E T, GUSTAVSSON P M. Towards a framework to detect multi-stage advanced persistent threats attacks [C]. In: Proc. of the IEEE International conference on Service Oriented System Engineering. 2014. 390-395.

（下转第 82 页）