一种局部时空图卷积方法及其在网络漏洞预测的应用

张珣[1,2],张楚童[1],艾孜孜·吐尔逊[2],郝蒙蒙[3],张迎春[4*],江东[3]

1. 北京工商大学计算机学院,北京 100048
2. 和田师范专科学校数学与信息学院,和田 848099
3. 中国科学院地理科学与资源研究所,北京 100101
4. 北京工商大学人工智能学院,北京 100048

摘要　针对网络安全态势预测中时空特征提取的不足,提出了一种基于局部时空卷积的网络漏洞预测方法,即局部时空图卷积网络模型,并针对网络漏洞数据选取历史平均法、长短期记忆网络、支持向量回归、时空图卷积网络模型进行对比实验。实验结果表明,提出的局部时空图卷积网络模型能够有效提高预测漏洞的时间、位置以及网络漏洞类型的准确度。

关键词　网络安全;数据挖掘;图卷积神经网络;时空相关性

网络安全态势预测作为网络安全态势感知的重要组成部分,描述的是安全态势随时间动态变化的行为,具体是根据历史网络安全数据,建立特定的预测模型从而预测未来网络态势。历史网络安全数据包括时序上的特征和地理空间上的分布特征。因此,可以将网络安全数据看作一种时空数据进行特征学习并进行预测。例如,网络漏洞数据包含网络漏洞的地理空间位置、漏洞描述、漏洞等级以及时间戳。根据网络漏洞数据的时间特征和空间特征,对网络漏洞发生的时间、地点以及类型进行预测,能够对未来网络安全发展状况做出预测,有利于预防网络攻击及制定针对性的安全对策,提高网络安全维护效率。

早期的时空数据预测方法主要基于统计学习,大多采用线性回归的思想,只能对平稳时间序列或可以转换为平稳时间序列的数据进行预测,存在很大的局限性。主要包括历史平均法(historial average, HA)、自回归移动平均模型(autoregressive

收稿日期:2023-02-21;修回日期:2023-04-25
基金项目:中国科学院重点部署项目(ZDRW-XH-2021-3)
作者简介:张珣,教授,研究方向为网络安全、地理人工智能,电子信箱:zhangxun@btbu.edu.cn;张迎春(通信作者),实验师,研究方向为控制科学、地理信息,电子信箱:zhangyingchun@btbu.edu.cn
引用格式:张珣, 张楚童, 艾孜孜·吐尔逊, 等. 一种局部时空图卷积方法及其在网络漏洞预测的应用[J]. 科技导报, 2023, 41(13): 67-75; doi: 10.3981/j.issn.1000-7857.2023.13.007

moving average model,ARMA)、向量自回归模型(vector autoregressive model,VAR)等[1]。随着机器学习技术的发展,许多科研人员尝试使用机器学习方法解决时空数据预测问题。Hossain等[2]用决策树算法和K最近邻算法对旧金山市的犯罪活动进行了预测,通过将时空序列预测问题分解后再进行预测。Vapnik等[3]提出了支持向量机(support vector machine,SVM),Vlahogianni等[4]提出了一种基于高级遗传算法的多层结构优化策略,并将其与人工神经网络(artificial neural network,ANN)相结合,提高了预测的准确性。Zheng等[5]通过改进K最近邻算法进行短期交通数据预测。

尽管基于机器学习的方法提高了时空数据预测任务的准确性,但是它们依旧难以捕获到真实时空数据中高度复杂的时空相关性。深度学习技术具有能够捕获数据中高度复杂的非线性关系的特性,因此通过深度学习进行时空数据预测受到越来越多的关注。Song等[6]使用循环神经网络(recurrent neural network,RNN)模型对人类的运动及交通方式进行了预测。Ma等[7]通过时空矩阵将交通流量信息转换为图像,并使用卷积神经网络(convolutional neural networks,CNN)对其进行特征提取和预测。Ma等[8]使用长短期记忆网络(long short-term memory,LSTM)模型对时空数据进行了长期预测。

随着神经网络的不断发展,人们发现现有的网络模型不能很好地学习到非欧几里德数据中的特征,Kipf等[9]提出了图卷积神经网络(graph convolution neural networks, GCN)模型,该模型可以将节点邻域的信息聚集到节点自身,从而有效地提取网络中的空间结构信息,因此图卷积网络被广泛应用于时空数据预测中。Seo等[10]将RNN和GCN结合,提出了图卷积循环网络模型(graph convolutional recurrent network,GCRN)。Zhao等[11]引入了GCN和门控循环单元结构(gated recurrent unit,GRU)结合来提取时空数据的时间特征和空间特征,Yu等[12]提出了时空图卷积网络(spatial temporal graph convolutional networks,STGCN)模型,用纯卷积结构建立模型,在更少的参数下实现更快的训练速度。基于STGCN,Guo等[13]基于注意力机制,考虑到时间周期性对预测的影响,对交通流的3个时间特性进行建模,并引入时空注意力机制,提出基于注意力的时空图卷积网络(attention based spatial-temporal graph convolutional networks,ASTGCN)模型,有效地捕捉时空数据中的动态时空相关性。

虽然此类方法已经可以捕获到时空数据中的时空相关性,提高了时空数据预测任务的准确性。但所捕获到的时空特征是通过分别捕获到的时间特征和空间特征串联、拼凑而成的,是间接的、片面的,然而真实的网络空间中,时间特征和空间特征是相互交融的。针对该问题,通过在数据的时间维度添加边,构成一种局部时空图来直接捕获网络安全数据中的时空特征,并通过构建时空卷积网络模型对时空特征进行学习。本研究通过在网络漏洞检测数据上进行实验,证明该方法能够有效提升网络漏洞预测的精度。

1 局部时空图卷积网络模型

基于图卷积原理,提出了局部时空图卷积网络模型(local spatio-temporal graph convolutional network model,LSTGCN)由2层时空卷积模块和全连接层组成。模型首先通过在网络安全数据的时间维度添加边得到局部时空图。然后使用时空卷积模块对局部时空图进行特征提取,直接捕获网络安全数据中的时空相关性。时空卷积模块由2层时域卷积层中间插入1层空域卷积层构成。最后使用全连接层得到最终的预测结果。

1.1 模型结构

局部时空图卷积网络模型(图1)主要由时空卷积模块和全连接层组成。时空卷积模块由时域卷积层和空域卷积层构成。

时域卷积层将所构造的新的邻接矩阵和网络安全数据作为输入,使用叠堆的多个门控时间卷积单元来捕获网络安全数据的长期时空相关性;空域卷积层以时域卷积层的输出作为输入,通过图卷积网络强大的网络结构学习能力来直接捕获局部时空图中所包含的时空相关性,在空域卷积层后再接

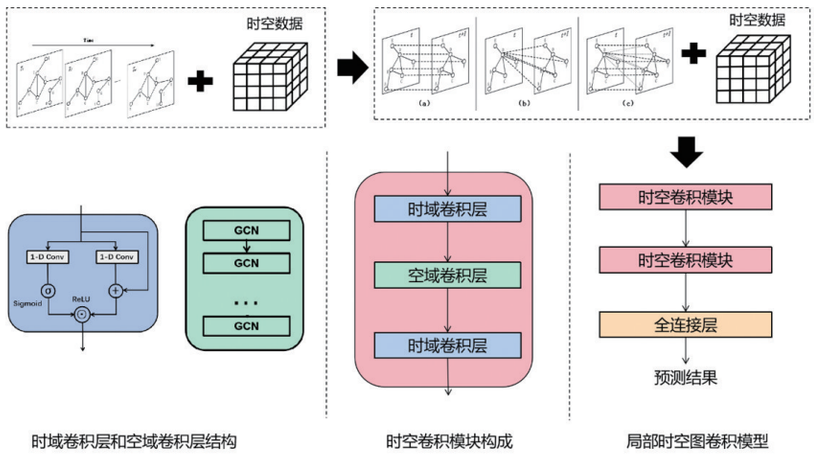

图1　LSTGCN模型结构图

1个时域卷积层,模型采用这种瓶颈结构,在2层时域卷积层中间插入1层空域卷积层,通过时域卷积实现图卷积的快速空间状态传播。最后使用全连接层来得到模型的最终预测结果。

1.2　局部时空图

网络安全数据具有时间和地理空间2方面的特征:时间特征指数据在时序上随时间变化的信息;空间特征指地理空间构成的网络拓扑结构信息。使用现有的时空预测方法捕捉网络安全数据特征时,大多结合时间序列分析法和动态网络表示学习法来对其进行分析处理。在真实的网络空间中,数据的时间特征和空间特征是相互交融、相互影响的,因此捕获其隐含的时空特征会对预测的准确性产生影响。因此,这种方式并不能准确反映网络安全数据中真实存在的时空相关性(图2)。

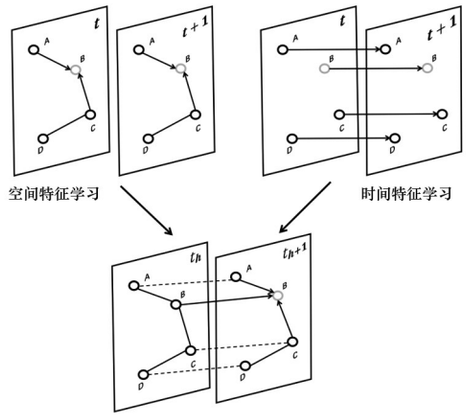

图2　现有时空特征挖掘方式

为直接捕获网络安全数据中显著存在的时空特征,提出一种新颖的局部时空图G_{ST}。G_{ST}通过在时间维度上的同一节点或邻居节点之间添加边,即用边将相邻2个时刻的节点相连接,从而将局部时间信息与空间信息相结合,构成同时含有局部时间特征、局部时空特征和空间特征的图结构。G_{ST}的构造方法如图3所示,本研究一共提出了3种构造G_{ST}的方法。第1种是把节点与其下一个时间点的节点自身相连接(图3(a));第2种是把节点与其下

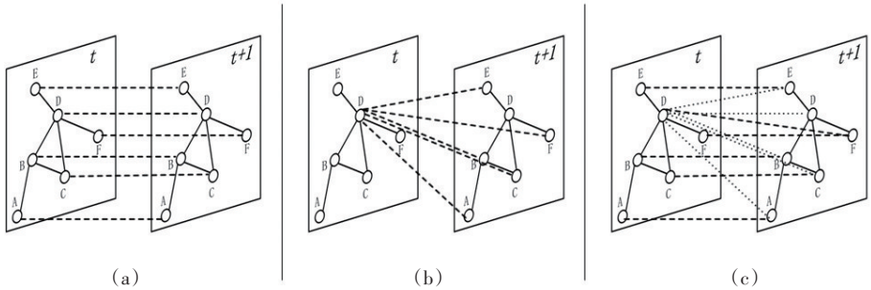

图3　3种局部时空图构造方法

一个时刻的相邻节点相连接(图3(b));第3种方式结合了前2种构图方式,不仅将2个时刻节点自身相连,同时将节点和相邻时刻的邻居相连(图3(c))。对G_{ST}进行观察可以发现,对于这3种连接方式的任何一个节点,均可以在两跳内对其时空邻居(相邻时刻的节点邻居)进行信息传播。

得到了直接含有时空特征的图结构,还需要将其表示为邻接矩阵的形式,以便开展后续工作。首先,含有N个节点的标准邻接矩阵$\boldsymbol{A}\in\boldsymbol{B}^{N\times N}$的构建方法为

$$\boldsymbol{A}=\begin{cases}W_{i,j}, & \left(V_i,V_j\right)=1\\ 0, & \left(V_i,V_j\right)=0\end{cases} \tag{1}$$

式中,$\left(V_i,V_j\right)=1$表示节点V_i和V_j之间连通,$\left(V_i,V_j\right)=0$表示节点V_i和V_j之间不连通,$W_{i,j}$表示连通节点V_i和V_j之间的权重。

构建局部时空图时将前后2个时刻进行连接,因此$\boldsymbol{A}_{ST}$中含有2个时间点的信息,故节点数为A的2倍,即$2N$。因此局部时空邻接矩阵可以表示为$\boldsymbol{A}_{ST}\in\boldsymbol{B}^{2N\times 2N}$。

将$2N$个节点分为当前时刻的节点集V_t和下一时刻的节点集$V_{t+1}2$部分,并将这2部分节点按照先V_t后V_{t+1}的顺序一一排列对应(即2个节点集中,节点的排列顺序一致),以图3(a)为例,构建方法如图4所示。

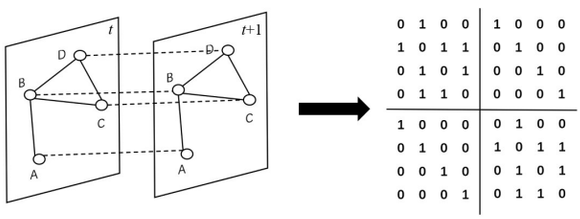

图4 局部时空图邻接矩阵示意

将$\boldsymbol{A}_{ST}$与$\boldsymbol{A}$进行对比可以发现,$\boldsymbol{A}_{ST}$可以表示为分块矩阵的形式。以图3(c)为例,$\boldsymbol{A}_{ST}=\begin{bmatrix}\boldsymbol{A}_{t-1} & \boldsymbol{A}_{(t-1)\sim t}\\ \boldsymbol{A}_{t\sim(t-1)} & \boldsymbol{A}_t\end{bmatrix}$,其中$\boldsymbol{A}_{t-1}$表示上一时刻网络数据地理空间的标准邻接矩阵,$\boldsymbol{A}_t$表示当前时刻网络数据地理空间的标准邻接矩阵,$\boldsymbol{A}_{(t-1)\sim t}$表示上一时刻节点与当前时刻节点的邻接矩阵,$\boldsymbol{A}_{t\sim(t-1)}$表示当前时刻节点与上一时刻节点的邻接矩阵。由于地理空间的网络数据在各时刻的空间结构信息都保持不变,因此$\boldsymbol{A}_{t-1}=\boldsymbol{A}_t=\boldsymbol{A}$,$\boldsymbol{A}_{(t-1)\sim t}=\boldsymbol{A}_{t\sim(t-1)}$。而邻接矩阵$\boldsymbol{A}_{(t-1)\sim t}$中包含了上一时刻节点与当前时刻节点自身之间的邻接关系以及上一时刻节点与当前时刻节点邻居之间的邻接关系,因此$\boldsymbol{A}_{(t-1)\sim t}=\boldsymbol{A}_t+\boldsymbol{I}=\boldsymbol{A}+\boldsymbol{I}$,$\boldsymbol{I}$为单位矩阵。最终,图3(c)的$\boldsymbol{A}_{ST}$可以表示为$\boldsymbol{A}_{ST}=\begin{bmatrix}\boldsymbol{A} & \boldsymbol{A}+\boldsymbol{I}\\ \boldsymbol{A}+\boldsymbol{I} & \boldsymbol{A}\end{bmatrix}$,构建$\boldsymbol{A}_{ST}$可以化简为先构建邻接矩阵$\boldsymbol{A}$,然后将$\boldsymbol{A}$与$\boldsymbol{A}+\boldsymbol{I}$进行拼接。类比上述推理过程,图3(a)的$\boldsymbol{A}_{ST}$可以表示为$\boldsymbol{A}_{ST}=\begin{bmatrix}\boldsymbol{A} & \boldsymbol{I}\\ \boldsymbol{I} & \boldsymbol{A}\end{bmatrix}$,图3(b)的$\boldsymbol{A}_{ST}$可以表示为$\boldsymbol{A}_{ST}=\begin{bmatrix}\boldsymbol{A} & \boldsymbol{A}\\ \boldsymbol{A} & \boldsymbol{A}\end{bmatrix}$。图5为该过程的简单示例。

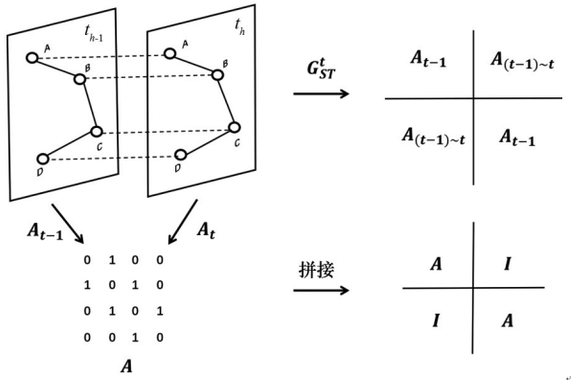

图5 $\boldsymbol{A}_{ST}$分块过程示意

1.3 时空卷积层

时空卷积模块包括2个时域卷积层和1个空域卷积层。为提取局部时空图中包含的时空特征,构造了时空卷积模块对局部时空图进行学习。模块本身可以根据特定情况的规模和复杂性进行堆叠或扩展。如图6所示,时空卷积模块采用瓶颈结构,在2层时域卷积层中间插入1层空域卷积层,通过瓶颈结构可以增加网络层数,使特征提取能力有相应的提升,通过时域卷积减少图卷积的计算量实现空域卷积层的快速空间状态传播。

时域卷积层由一维卷积神经网络层CNN和门控线性单元(gated linear unit,GLU)组合而成(图7)。其中,一维CNN用来捕获网络安全数据中的时间信息,门控线性单元GLU用来选择哪些时间

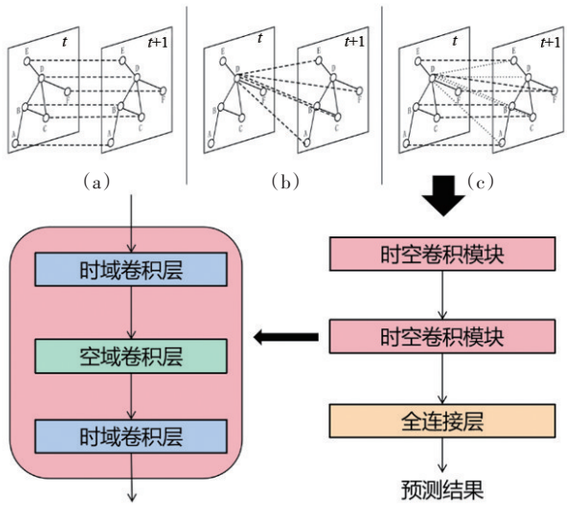

图6　时空卷积模块示意

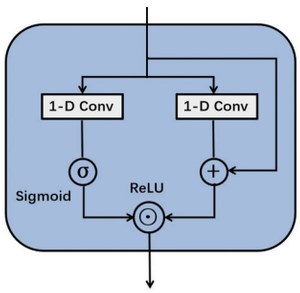

图7　时域卷积层示意

信息会被保留。第1个时域卷积层的输入 $X \in \boldsymbol{B}^{2N \times M \times C_i}$,$M$为输入的时间步。

门控时间卷积单元的公式为

$$C *_C \boldsymbol{G} = P \odot \delta(\boldsymbol{M}) \in \boldsymbol{B}^{2N \times (M-K+1) \times Q} \tag{2}$$

其中,C表示一维CNN的卷积核;$\boldsymbol{G}$表示输入的特征向量;$\boldsymbol{P}$和$\boldsymbol{M}$分别表示经过CNN后的输出矩阵,将$\boldsymbol{P}$和$\boldsymbol{M}$作为GLU的输入来得到最终的输出结果;$\delta(\boldsymbol{M})$表示GLU中的门控单元,用来对输入$\boldsymbol{P}$的时间信息进行筛选,从而保留其中与时间密切相关的信息,其中,$\delta(\cdot)$表示sigmoid函数,$\odot$表示哈达玛积。

第2个时域卷积层以空域卷积层的输出为输入,将其视为时间序列,沿着时间维度进行卷积操作,提取其中的长期时间信息。由于输入中已经含有空间特征和时空特征,因此时域卷积层可以将空间依赖性、时空依赖性与长期时间依赖性相结合,从而捕获网络安全数据中更为复杂的时空相关性。为防止梯度消失,在卷积层之间添加了残差连接。

此外,为得到最终的预测结果,在第2层时域卷积层后接入了全连接层来生成未来若干个时刻的预测值。

空域卷积层由多层GCN构成。不同于一般图片或文本数据,网络安全数据中的空间数据点的邻居数量是不同的,无法用一般的卷积方法计算。图卷积神经网络GCN是捕获网络结构信息的有效方法[14],本研究中的空域卷积层通过多个GCN堆叠来构建,通过快速聚合邻居节点的特征捕获局部时空图中的时空特征。

局部时空图卷积模块中单层GCN公式为

$$\boldsymbol{Z} = \sigma f(\boldsymbol{X}, \boldsymbol{A}) = \sigma\left(\hat{\boldsymbol{A}}\, \boldsymbol{X} \boldsymbol{W}\right) \tag{3}$$

其中,$\boldsymbol{X}$表示特征矩阵;$\hat{\boldsymbol{A}} = \widetilde{\boldsymbol{D}}^{-\frac{1}{2}} \widetilde{\boldsymbol{A}} \widetilde{\boldsymbol{D}}^{-\frac{1}{2}}$,其中,$\widetilde{\boldsymbol{A}} = \boldsymbol{A} + \boldsymbol{I}$,$\boldsymbol{A}$是邻接矩阵,$\boldsymbol{I}$是单位矩阵,$\widetilde{\boldsymbol{D}}$是$\widetilde{\boldsymbol{A}}$的度矩阵;$\boldsymbol{W}$是需要学习的权重矩阵;$\sigma(\cdot)$是非线性激活函数。

2　实验与结果分析

2.1　数据集

本研究数据来自国内某市网安支队提供的该市近6个月内的网络漏洞数据。该数据集包含40511条数据记录,每条记录E包括漏洞点ip、地理空间位置、漏洞描述、漏洞等级以及时间戳,如式(4)所示。

$$E = \left[ip, 经纬度, 描述, 等级, 时间戳\right] \tag{4}$$

数据包括网络特征、地理空间特征和时间序列,支持实现网络漏洞的时空预测。图8为某时间段城市网络漏洞点分布示意图,网络漏洞分布明显受所在城市空间分布和城市功能划分的影响。

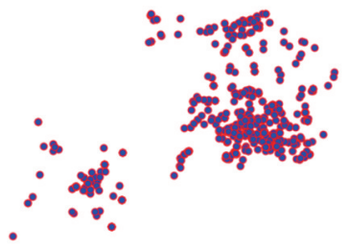

图8　网络漏洞点分布示意

在对网络漏洞数据进行时空结构化前,进行数据预处理,包括以下步骤。

1)去噪。首先对网络漏洞数据去噪,去除缺乏经纬度信息及位于城市外范围的网络漏洞数据。

2)空间划分。依照网络漏洞数据的地理位置信息,按照地理位置进行地理网格划分,将网络漏洞数据所处空间范围按照经纬度划分空间网格。

3)时间划分。对网络漏洞数据按时间段进行划分,以相近的网络漏洞检测时间段为范围,将各时间段的网络漏洞数据划分开,形成时间序列。

4)漏洞等级处理。网络漏洞等级分为低危、中危、高危和严重。在各个时间段内,将各空间网格内的网络漏洞点的漏洞等级以不同数值表示,并加和获得时间段内网格内的整体网络漏洞等级,形成时间序列网络漏洞特征矩阵。

5)构造地理关系邻接矩阵。将网格中网络漏洞时间序列不全为0的网格块作为图数据G的顶点V_i。根据地理位置相关性构成图网络,将距离在dist内的点V_i间的关系edge设为1,构造邻接矩阵$\boldsymbol{A}$。

处理后的数据集是一个大小为[88,44,1]的三维矩阵,将其划分为训练数据和测试数据2部分,划分后数据集维度如表1所示。其中第0维代表时间序列,即用于训练和测试的时间点数。第1维表示44个地理空间位置。第2维表示网络攻击的等级。

表1 原始实验数据集

数据集	节点数	边数	时间点数	特征数
网络漏洞时空数据	44	264	88	1
训练数据	44	264	66	1
测试数据	44	264	22	1

2.2 对比方法

将所提LSTGCN模型与多种经典的时空数据预测方法进行对比,包括如下典型的预测方法。

在基于统计学习的方法中,HA、LSTM、SVR(support vector regression,支持向量回归)和STGCN这4种方法均为时间序列预测领域内最经典的方法。其中,历史平均法HA考虑了时空数据的周期性特征,将与预测时间点相对应的前几个周期的历史数据的加权平均值作为预测结果,各方法详情如下。

历史平均法HA,考虑了时空数据的周期性特征,将与预测时间点相对应的前几个周期的历史数据的加权平均值作为预测结果。

支持向量回归模型SVR,将支持向量机应用于回归任务,进而对时空数据进行预测。

长短期记忆网络LSTM,是一种改进后的循环神经网络,可以解决循环神经网络无法处理的长期依赖问题,被广泛应用于时间序列预测任务中。

时空图卷积网络模型STGCN,考虑了时空数据中的空间结构信息,将GCN与一维CNN相结合,取得了良好的效果。

在基于传统机器学习的方法中,支持向量回归模型SVR为时空数据预测领域内最常用的方法,该方法将支持向量机应用于回归任务,进而对时空数据进行预测。

基于深度学习的方法包括全连接长短期记忆网络LSTM和时空图卷积网络模型STGCN。其中,LSTM是一种改进后的循环神经网络,可以解决循环神经网络无法处理的长期依赖问题,被广泛应用于时间序列预测任务中。STGCN方法考虑了时空数据中的空间结构信息,将GCN与一维CNN结合,取得了良好的效果。LSTM考虑到了时空数据中较长远的时间信息,但忽视了数据中的空间结构特征;而STGCN正好与之相反,考虑了空间结构特征却忽视了长期时间特征,以这2种模型为基准可以更好地反映空间特征与长期时间特征对时空数据预测任务准确性的影响。

2.3 评价方法

时空数据预测方法本质是一种定量预测模型,即用历史数据来预测未来数据,目标在于使预测数据尽可能接近真实数据。本研究采用时空数据预测常用的评价指标进行模型评价,包括:平均绝对误差(MAE)、均方根误差(RMSE)、平均绝对百分比误差(MAPE)等,计算公式如式(5)~(7)所示。

$$\mathrm{MAE}=\frac{1}{n}\sum_{i=1}^{n}\left|x_i-\hat{x}_i\right| \tag{5}$$

$$\mathrm{RMSE}=\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i-\hat{x}_i\right)^2} \tag{6}$$

$$\mathrm{MAPE}=\frac{100\%}{n}\sum_{i=1}^{n}\left|\frac{\hat{x}_i-x_i}{x_i}\right| \tag{7}$$

其中,n表示样本个数,x_i表示第i个样本的真实值,$\hat{x}_i$表示第i个样本的预测值。

2.4　实验设计

在实验中,按照时间顺序对所有数据集进行划分,将前75%作为训练集,用于模型训练,剩余25%作为测试集,用于模型测试。实验使用PyTorch深度学习框架搭建LSTGCN模型,模型按照图3的方法构造局部时空图G_{ST},并设空域卷积层中图卷积层GCN的个数为2,输出维度分别为16、32;设时域卷积层中一维CNN的个数为2,输出维度分别为32、64;全连接层的个数为1,输出维度为64。在训练过程中,使用平均绝对误差MAE作为损失函数,并采用随机梯度下降法进行迭代反向传播学习,迭代300次,每次选择batch size为50个训练样本。

3　结果与分析

将LSTGCN模型与上述4种对比模型进行性能对比,实验结果如表2所示。其中LSTGCN-a表示LSTGCN模型使用如图3(a)所示的构造方法,LSTGCN-b表示使用如图3(b)所示的构造方法,LSTGCN-c表示使用如图3(c)所示的构造方法。

表2　对比实验结果

对比模型	MAE	MAPE	RMSE
SVR	70.59	7.36	93.36
HA	69.02	6.51	156.20
LSTM	13.20	7.49	28.02
STGCN	13.42	2.88	23.47
LSTGCN-a	14.18	2.60	26.27
LSTGCN-b	11.06	1.63	23.68
LSTGCN-c	13.96	2.60	26.77

从表2可以看出,本研究提出的LSTGCN模型在3种评估指标下均优于原本的LSTGCN模型,相对传统的机器学习和深度学习预测网络安全数据的方法,性能提高更加明显。说明本文所构造局部时空卷积模型能够有效地捕获网络安全数据中的时空特征。

为比较不同的局部时空图构造方法对模型性能的影响,将3种网络结构构造方法在网络漏洞数据上进行了比较实验(图9)。

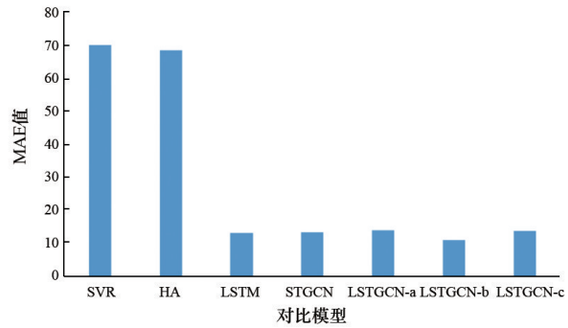

图9　预测结果示意

图10分别给出了3种构造方法在预测网络攻击的MAE、MAPE和RMSE指标结果,图中横轴代表不同的评价指标,纵轴代表相应的指标结果。其中LSTGCN-a表示LSTGCN模型使用如图3(a)所示的构造方法(即上文性能对比实验部分所定义的LSTGCN模型),LSTGCN-b表示使用如图3(b)所示的构造方法,LSTGCN-c表示使用如图3(c)所示的构造方法。

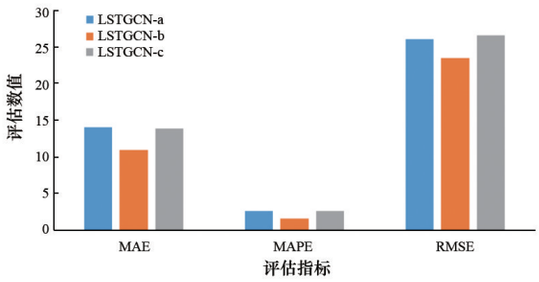

图10　不同构造方法性能对比

从图10可以看出,对于MAE指标,LSTGCN-b的结果要始终优于LSTGCN-a和LSTGCN-c的预测结果。这表明采用图3(b)构造方式构造的图结构更有利于捕获网络安全数据中的时空特征。这可能是由于LSTGCN-b只将自身与相对时刻的邻居节点相连,节点可以在一跳内对相邻时刻的邻居节点进行信息传播。能够更快速捕获到网络漏洞数据中历史时刻漏洞对相邻节点位置的影响。

LSTGCN-a只将相邻时刻同一节点之间相连,

由于网络漏洞时序数据具有很强的非线性,LSTGCN-a只引入时间维度的边,使信息能够在时序上进行快速传播,而在时空维度上则需要两跳才能学习到其特征,因此在对网络漏洞进行预测时表现弱于LSTGCN-b。

LSTGCN-c不仅将2个相邻时刻的节点自身相连接,还和2个相邻时刻的节点和其邻居相连接,引入了大量时空维度的边。这些边所学习到的特征是相同的,所以在预测时产生大量重复冗余信息,导致预测结果不理想。

4 结论

针对网络安全态势预测中时空特征提取的不足,通过在网络安全数据的时间维度添加边,构造一种新的图结构——局部时空图,来直接捕获网络安全数据中的时空特征,并提出了一种基于局部时空卷积的网络漏洞预测方法,即:局部时空图卷积网络模型LSTGCN,对构造的局部时空图进行学习。最后在网络漏洞数据上进行试验,选取HA、LSTM、SVR和STGCN模型进行对比实验。实验结果表明本研究提出的局部时空图卷积网络模型能够更好地预测漏洞的时间、位置以及网络漏洞类型。因此对其隐含的时空特征进行学习,能够提高网络安全态势预测的准确性。这种准确性的提高有利于提前预防网络攻击及制定针对性的安全对策,提高网络安全维护效率。

参考文献(References)

[1] Wang S, Cao J, Yu P. Deep learning for spatio-temporal data mining: A survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2020, 14(8): 1-21.

[2] Hossain S, Abtahee A, Kashem I. Crime prediction using spatio-temporal data[C]//International Conference on Computing Science, Communication and Security. Gujarat: Springer, 2020: 277-289.

[3] Vapnik V N, Lerner A Y. Recognition of patterns with help of generalized portraits[J]. Avtomat. i Telemekh, 1963, 24(6): 774-780.

[4] Vlahogianni E I, Karlaftis M G, Golias J C. Optimized and meta-optimized neural networks for short-term traffic flow prediction: A genetic approach[J]. Transportation Research Part C: Emerging Technologies, 2005, 13(3): 211-234.

[5] Zheng Z, Su D. Short-term traffic volume forecasting: A k-nearest neighbor approach enhanced by constrained linearly sewing principle component algorithm[J]. Transportation Research Part C: Emerging Technologies, 2014 (43): 143-157.

[6] Song X, Kanasugi H, Shibasaki R. Deeptransport: Prediction and simulation of human mobility and transportation mode at a citywide level[C]//the 25th International Joint Conference on Artificial Intelligence. New York: IJCAI, 2016: 2618-2624.

[7] Ma X, Dai Z, He Z, et al. Learning traffic as images: A deep convolutional neural network for large-scale transportation network speed prediction[J]. Sensors, 2017, 17 (4): 818-834.

[8] Ma X, Tao Z, Wang Y, et al. Long short-term memory neural network for traffic speed prediction using remote microwave sensor data[J]. Transportation Research Part C: Emerging Technologies, 2015, 54(1): 187-197.

[9] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks[C]//the 5th International Conference on Learning Representations. Toulon: ICLR, 2017: 1-14.

[10] Seo Y, Defferrard M, Vandergheynst P, et al. Structured sequence modeling with graph convolutional recurrent networks[C]//the 25th International Conference on Neural Information Processing. Siem Reap: Springer, 2018: 362-373.

[11] Zhao L, Song Y, Zhang C, et al. T-GCN: A temporal graph convolutional network for traffic prediction[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 17(99): 1-11.

[12] Yu B, Yin H, Zhu Z. Spatio-temporal graph convolutional networks: A deep learning framework for traffic forecasting[J]. In International Joint Conference on Artificial Intelligence, 2018(12): 3634-3640.

[13] Guo S, Lin Y, Feng N. Attention based spatial-temporal graph convolutional networks for traffic flow forecasting [C]//AAAI Conference on Artificial Intelligence. Washington, USA: AAAI Press, 2019, 33(1): 922-929.

[14] 徐冰冰, 岑科廷, 黄俊杰, 等. 图卷积神经网络综述[J]. 计算机学报, 2020, 43(5): 755-780.

A local spatio-temporal graph convolution-based approach and its application to network vulnerability prediction

ZHANG Xun[1,2], ZHANG Chutong[1], EZIZ Tursun[2], HAO Mengmeng[3], ZHANG Yingchun[4*], JIANG Dong[3]

1. School of Computer Science and Engineering, Beijing Technology and Business University, Beijing 100048, China
2. School of Mathematics and Information, Hotan Normal College, Hotan 848099, China
3. Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing 100101, China
4. School of Artificial Intelligence, Beijing Technology and Business University, Beijing 100048, China

Abstract To address the shortage of spatio-temporal feature extraction in network security situation prediction, a local spatio-temporal convolution-based network vulnerability prediction method, namely the local spatio-temporal graph convolutional network model, is proposed, and HA, LSTM, SVR and STGCN models are selected for comparison experiments on network vulnerability data. Experimental results show that the model proposed in this paper can effectively improve the accuracy in predicting the time and location of vulnerabilities as well as the type of network vulnerabilities.

Keywords internet security; data mining; graph convolutional networks; spatio-temporal correlation

（责任编辑　傅雪）