图神经网络在网络安全的应用

#homework

图神经网络有多种类型，不同的图神经网络有不同的应用，下面介绍几种不同的图神经网络

图卷积网络

图卷积网络将卷积运算从传统数据（例如图像）推广到图数据。其核心思想是学习一个函数映射f，通过该映射图中的节点vi可以聚合它自己的特征xi与它的邻居特征 xj（ j 属于N（vi））来生成节点vi的新表示。图卷积网络是许多复杂图神经网络模型的基础，包括基于自动编码器的模型、生成模型和时空网络等。下图直观地展示了图神经网络学习节点表示的步骤。

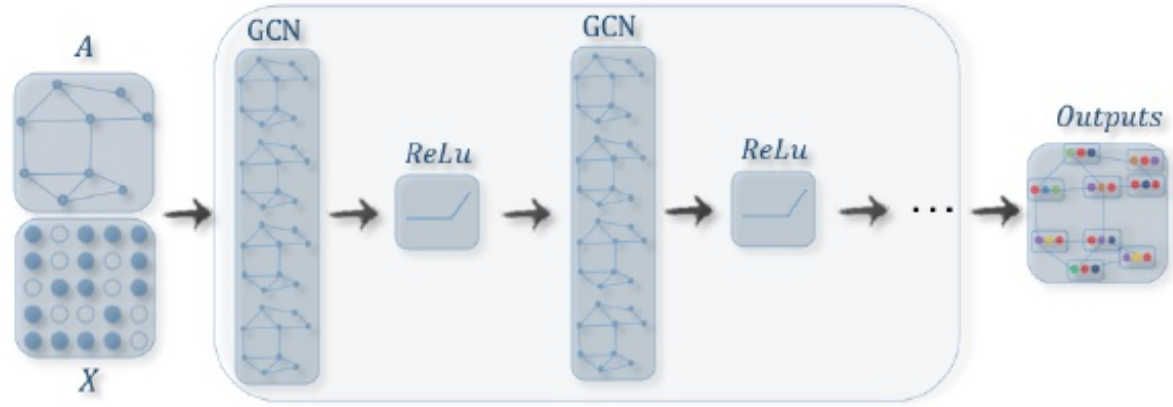

Fig. 4: A Variant of Graph Convolution Networks with Multiple GCN layers [14]. A GCN layer encapsulates each node's hidden representation by aggregating feature information from its neighbors. After feature aggregation, a non-linear transformation is applied to the resultant outputs. By stacking multiple layers, the final hidden representation of each node receives messages from a further neighborhood.

GCN方法又可以分为两大类，基于谱（spectral-based）和基于空间（spatial-based）。基于谱的方法从图信号处理的角度引入滤波器来定义图卷积，其中图卷积操作被解释为从图信号中去除噪声。基于空间的方法将图卷积表示为从邻域聚合特征信息，当图卷积网络的算法在节点层次运行时，图池化模块可以与图卷积层交错，将图粗化为高级子结构。如下图所示，这种架构设计可用于提取图的各级表示和执行图分类任务。

那么通过图卷积网络算法可以用于网络上的虚假多媒体智能检测，虚假多媒体是指伪造的图片、视频、音频等媒体，攻击者可以篡改相关媒体内的内容，从而发布不实的信息，而网络社会相当发达，如果不对这种行为加以遏制，若是造成谣言大规模扩散，会有难以估量的影响，我认为通过图卷积网络，利用其优势可以采用类似于GAN的算法，来输入大量的原图和篡改

图来对模型进行训练，利用图来建立起相关的联系，从而识别出虚假的多媒体（这里主要应该应用于虚假图片的检测）

图注意力网络

注意力机制如今已经被广泛地应用到了基于序列的任务中，它的优点是能够放大数据中最重要的部分的影响。这个特性已经被证明对许多任务有用，例如机器翻译和自然语言理解。如今融入注意力机制的模型数量正在持续增加，图神经网络也受益于此，它在聚合过程中使用注意力，整合多个模型的输出，并生成面向重要目标的随机行走。在本节中，我们将讨论注意力机制如何在图结构数据中使用。

众所周知，人们更加倾向于把自己的心理活动发布在社交平台当中，凭借图注意力网络在自然语言理解上的应用，我们可以根据此较为准确地去发现微博或相关社交平台上有抑郁倾向的人群，或是进行网络舆情的监测，即时掌握网络上舆情的动态，以便相关平台更好理解当前的舆论风向，采取相关的行动

除了以上所述的几个应用，图神经网络还已被探索可以应用于其他问题，如程序验证、程序推理、社会影响预测、对抗性攻击预防、电子健康记录建模、脑网络、事件检测和组合优化。

未来发展

由于网络安全是一个不断发展的学科，其中大部分的商业化应用的正常运行都需要网络安全辅助，所以未来还会有各种各样的新问题出现，而图神经网络作为近年来比较新兴的事物，我相信其还可以在网络的对抗与防御上有较多应用，例如通过图模型推导系统各个组件之间的关联性与依赖性，从而分析攻击者在入侵时可能的行迹，拥有广阔的前景。