**人工智能概论课程设计**

随着互联网、人工智能、云计算等技术的快速发展，网络安全问题也日益严重。根据2019年Symantec发布的《互联网安全威胁报告》显示，2018年网络攻击活动在全球范围内的数量已经达到了4.6亿次，尤其是针对企业和政府机构的攻击成为主要趋势，导致了大量数据泄露和财产损失。全球网络安全形势非常严峻，网络恶意攻击数量正在不断增加，必须采取更加严密的网络安全防御措施来保障个人信息和国家安全。因此，了解网络攻击的机制和过程在现代网络安全防御中显得至关重要。有向因果图是在网络攻防领域中广泛使用的工具，它可以用于描述复杂的因果关系，不仅有助于分析网络攻击的过程，还可以用于发现网络系统中的漏洞，从而帮助我们更好地理解网络攻击的机制，制定更具有针对性的防御策略，提高网路安全防御的效果。由此派生出本次的课程设计题目：面向有向因果图的诊断算法研究。

**问题概述**

本研究的目标是如何利用面向有向因果图的诊断算法来实现网络防御策略的制定。因此，本研究主要是算法方向的研究。设计的场景为：通过建起一个具有实际意义的网络的有向因果图，将网络中的变量连接起来，以表示它们之间的关系。当发生网络攻击事件时，攻击行为会影响有向因果图上的节点。通过对有向因果图进行异常节点与关键节点的分析，可以最大限度地减少这些节点遭受攻击或者故障对整个网络或系统造成的影响，更好地预防和应对攻击。

**任务目标和要求**

有向因果图是一种基于因果关系的建模方法，它以箭头表示因果关系，并将节点与相应的变量或概念相关联。由于网络攻击的发生往往涉及多个因素和因果关系，因此有向因果图可以帮助我们更全面地理解问题。

1. 本研究的第一个任务是通过公开数据集进行**有向因果图的建模**。这个过程需要对数据进行预处理、选择适当的有向因果图模型以及评估模型的质量。
2. 本研究的第二个任务是基于有向因果图来进行**异常节点的识别**。异常节点指的是在图中出现异常的节点，这是攻击的主要目标。
3. 本研究的第三个任务是基于有向因果图来进行**关键节点的识别**。关键节点是指在整个网络中具有重要影响力的节点，攻击它们可能会影响整个系统的稳定性。

因此，我们需要利用算法来识别这些节点，将其作为制定防御策略的主要依据。

**问题分解**

本研究旨在建立有向因果图，结合图神经网络进行有向图分析，进一步实现网络攻防场景下的抗毁性与异常识别，其具体包括三个方面的子问题：

1）基于状态数据的有向因果图建模；

2）图神经网络驱动的有向图的异常节点识别算法研究；

3）图神经网络驱动的有向图的关键节点识别算法研究。

**子任务分配**

1. 任务1（基于状态数据的有向因果图建模）：调研并选取合适的数据集及建模方法，绘制有向因果图（清晰简洁），检验因果关系并解释因果关系，验证模型的准确性和可靠性并完成该部分的文字内容。
2. 任务2（有向图的异常节点识别算法研究）：阅读相关文献，了解有向图的异常节点识别算法并确定合适的图神经网络方法。进行代码的编写，实现此算法并完成该部分的文字内容。
3. 任务3（有向图的关键节点识别算法研究）：阅读相关文献，了解有向图的关键节点识别算法并确定合适的图神经网络方法。进行代码的编写，实现此算法并完成该部分的文字内容。

**参考文献/代码/教程**

在完成上述任务时，可以参考以下文献、代码和教程：

1. 算法（不限于以下参考文献）：

[1] 唐鹏，彭开香，董洁. 一种新颖的深度因果图建模及其故障诊断方法[J].自动化学报,2022,48(6):1616-1624.

[2] Munikoti, Sai, Deepesh Agarwal, Laya Das, Mahantesh Halappanavar and Balasubramaniam Natarajan. Challenges and Opportunities in Deep Reinforcement Learning with Graph Neural Networks: A Comprehensive review of Algorithms and Applications[R]. ArXiv abs/2206.07922, 2022.

[3] Rakaraddi, A., Pratama, M. Unsupervised Learning for Identifying High Eigenvector Centrality Nodes: A Graph Neural Network Approach[C]. IEEE International Conference on Big Data (Big Data), 2021:4945-4954.

1. 相关论文的查找：

* <https://www.semanticscholar.org/>
* <https://www.connectedpapers.com/>
* <https://www.cnki.net/>

1. 开源代码的查找：

* <https://github.com/>
* <https://paperswithcode.com/>

1. 有可能使用到的数据集：

* NSL-KDD数据集：

<https://blog.csdn.net/airenKKK/article/details/124619217>

* 基于网络入侵数据集的综述：

<https://arxiv.org/pdf/1903.02460.pdf>