**基于多假设深度学习的流量异常检测研究-终期答辩稿**

**P1:尊敬的评委老师你们好，我们的项目是基于多假设深度学习的流量异常检测研究。**

**P2:接下来我将从以下三个方面进行介绍。**

**P3:首先是项目介绍。**

**P4:随着网络流量规模的增加，网络攻击的种类和规模也随之大量增长，这给异常流量检测带来了极大挑战，而我们的项目就是针对这一痛点提出的。**

**P5:我们设计了一个完整的VARU异常流量检测系统，包括特征提取模块，融合模型模块，分数评估模块，几大模块共同进行异常流量的检测。**

**P6:首先是特征提取模块，我们利用WireShark对数据集进行抓包，利用Kitsune进行特征处理。**

**P7:在融合模型模块，我们阅读了相关文献，发现多假设思想在表征复杂特性方面具有良好效果，于是我们创新性地将VAE中的解码器设计为多头解码器的形式，提出了多假设VAE模型。**

**P8:同时我们引入BILSTM模型，以此来更有效地描述网络流量及其异常行为的时序特性。**

**P9:接着我们提出临时标签的概念，将由无监督的VAE模型生成的RMSE作为训练BILSTM所需的标签，使其成为有监督的模型，实现模型融合，共同检测异常流量攻击。**

**P10:最后我们设计了分数评估模块，将融合模型中的参数进行计算得到异常分数，当分数大于阈值gp时，判断为异常流量。这是我们根据实验结果绘制的图表。**

**P11:以上就是异常流量检测系统VARU各个模块的介绍。**

**P12:接下来是实验设计部分。**

**P13:我们首先进行超参数的调整，发现当多假设个数为5，隐藏层神经元个数为50时，VARU算法表现最好。**

**P14:接着为了验证多假设深度学习的有效性，我们进行了9组对照试验，比较各个指标，从图中我们可以看到，多假设VAE与BILSTM的组合模型具有更好的性能和描述复杂流量的能力。**

**P15:接着我们通过比较MAWILAB数据集不同大小下VARU算法的各个指标，来探究数据集大小对于算法效果的影响，发现数据集越大，VARU表现越好，当数据集较小时，VARU效果较差；那么如何进一步优化VARU算法呢，我们提出两个解决方法：1.增大输入的特征值维度 2.优化p和gp参数**

**P16:我们首先将特征值数目分别设置为100和200，进行实验比较各个指标，发现增加输入特征值的维度，能进一步提升算法的性能。**

**P17:接着为了优化分数评估模块中的p和gp，我们分别进行实验，观察p和gp对于检测效果的影响，发现p和gp在数据集较小时作用较小，数据集较大时能够有效提升算法精度，且p=0.80时，gp=0.65时综合检测效果最好。**

**P18:接着我们将VARU算法与传统算法如SVM进行比较，同时也和近两年较为先进的HELAD模型进行比较，实验结果表明VARU算法准确率更高，误报率更低，检测效果更好。**

**P19:接下来介绍创新点及项目成果。**

**P20:关于创新点，我们首先结合多假设思想，将变分自编码器的解码器部分设计为多头解码器，形成多假设VAE；其次我们采用BILSTM模型，能够有效地利用输入的前向和后向的特征信息，进一步提高模型检测准确率；最后我们创新性提出TL标签概念，将多头变分自编码器的RMSE作为双向时间序列模型的标签，实现多模型的融合。**

**P21:关于可交付成果，我们已将一篇论文投至JNCA期刊，目前处于在审状态；一项专利正在申请；同时我们设计了良好的人机交互界面，最后我们已在GitHub实现代码开源，链接如图所示。**

**P22:以上就是全部答辩内容，请各位评委老师指正！**