科 学 技 术 项 目 合 同

合同编号（甲方）：SGTYWAZQT2200040

合同编号（乙方）：2022GKF-0272

项目名称：基于深度学习的网上国网流量及微服务安全防护技术研究

委托方（甲方）：国家电网有限公司客户服务中心

受托方（乙方）：天津大学

签订日期：2022-5-10

签订地点：天津

1. 主要内容

1.1 主要技术内容

1.1.1 网络流量表征技术

网络流量特征提取对于异常网络流量刻画具有重要意义，准确且具有区分性的网络流量特征能有效指导异常流量检测模型高效准确的对异常流量进行检测。网络流量具有多维度特征，针对本项目中包含的大量 https 加密流量，其特征的贡献值不同，为了满足异常流量检测的实时性和性能要求，往往需要进行特征选择，通过对网络流量特征进行降维，选择区分度最大的部分特征。

1.1.2 恶意加密流量检测技术

研究基于深度学习模型编码的流量异常检测模型，通过深度神经网络对原始特征进行编码，对异常流量特征进行表征，研究适合异常流量特征表征的分类检测模型。

1.1.3 恶意流量检测系统

研究恶意网络流量实时检测系统设计，通过网络流量处理模块、网络流量特征提取和表征模块、恶意流量检测模块、结果输出模块，研究适合在线和离线多种工作模式的高带宽恶意网络流量实时检测系统。

1.2 主要技术难点

1.2.1 网络流量表征复杂

网络流量表征技术，通过分析网络流量自身特点，通过统计、机器学习和深度学习多种方法，将复杂难以区分的网络流量，通过抽象和语义化表征，从难以区分的网络流量空间映射到具有可区分性的网络流量表征空间，从而实现网络流量的分类和异常检测。其难点存在于如何设计网络流量的表征形式和表征方法。常见的网络流量表征方法有向量表征、图片表征等。

1.2.2 恶意流量检测建模难度大

网络异常流量检测中需要提取网络流量特征，常用的网络流量特征具有 200 多维度，如此高维度的样本会减低检测的效率，难以满足异常流量检测的实时性要求，因此需要根据不同的网络场景，选择适合该场景的网络流量特征。另外，由于加密流量的特殊设定，会导致有效特征的缺失，而特征的稀疏性对分类结果产生明显影响，需要通过行为建模的方式解决特征稀疏的挑战和难点。常见的异常流量检测模型有基于规则特征、基于机器学习和基于深度学习方法。每一种方法都有其适用性和特点，因此需要根据网络流量的场景和特征内容去选择合适的异常网络流量检测模型。

2. 预期目标

2.1 网络流量表征技术

实现网络流量表征，可应用于加密和非加密网络流量的数据表征，为后续的网络流量分类和检测提供支撑。针对该项目的网络流量可提供最高 500 维度的特征提取和多种表征。

2.2 恶意加密流量检测技术

实现加密网络流量中恶意流量的检测，可应用于国内外各网络出入口进行恶意加密流量的检测。针对目标加密恶意流量检测，相比较传统检测方法预期准确率提高 5-10%。

2.3 恶意网络流量检测系统

实现恶意网络流量检测系统，可以实时的针对网络流量中的可疑攻击和异常行为进行检测。支持在线和离线两种工作模式，支持高带宽高并发检测。

附件 2：

项目参加人员表

负责人	[redacted]						计算机科学与技术	项目管理，统筹	6 个月
	陈森	天津大学智能与计算学部	男	1990	副教授	副教授	计算机	算法设计与指导	6 个月
主要工作人员	[redacted]						计算机	算法设计与指导	6 个月
							计算机	相关工作调研，算法设计与研发	6 个月
							计算机科学与技术	可行性分析，算法设计与研发	6 个月
							计算机技术	系统研发与部署	6 个月
							计算机科学与技术	系统研发，系统测试与维护	6 个月