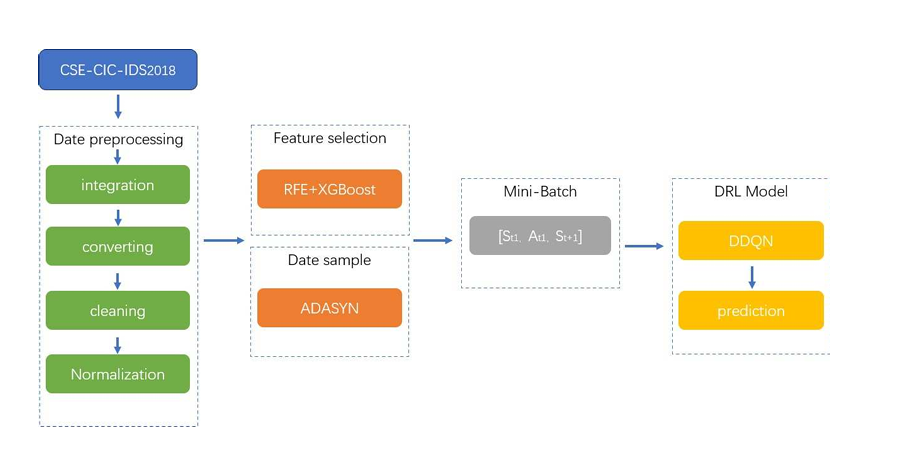
架构：

**一、数据处理部分**

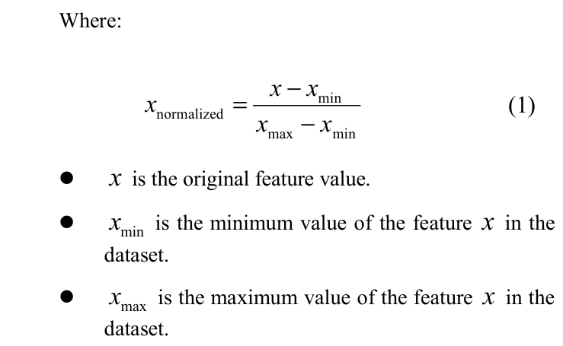
原始数据集为CSE-CIC-IDS2018数据集，由加拿大网络安全研究所提供，包含多种类型的网络攻击数据。该数据集通过收集五个网络部门中420个独立设备的系统日志构建，并采用CICFlowMeter-V3技术分析，最初包含80个特征。论文对数据集进行了清洗，去除了包含无穷值和缺失值的数据，最终将特征数量缩减为64个清洁特征。清洗后的数据集包含16,137,183个样本。

1.类别整合

CSE-CIC-IDS2018数据集包含10天的流量记录，涵盖了15种攻击类型（例如慢速DoS、SQL注入等）。为简化分析过程，将这15种攻击类型合并为7个类别：“良性”、“DDoS攻击”、“DoS攻击”、“暴力破解”、“僵尸网络”、“渗透”和“Web攻击”。这些攻击类别的分布情况如图所示。该整合步骤有效减少了数据类别的复杂性，使得后续模型能够更好地聚焦于主要的攻击特征。

2.数据标准化

在原始数据集中，不同特征的取值范围差异较大，这种不平衡会影响模型训练效果。为了解决该问题，采用了Min-Max归一化方法对特征进行了标准化处理，使每个特征的数值范围被压缩到[0,1]区间内。

其中，标准化的公式为：

3.特征选择

论文中采用了递归特征消除（RFE）与极端梯度提升（XGBoost）相结合的特征选择方法，来筛选出重要的特征子集，以提升模型的准确性并降低计算开销。具体步骤如下：

**步骤1**：使用XGBoost模型对包含所有特征的数据集进行训练。

**步骤2**：在验证集上评估模型的准确性、F1分数和精确度。

**步骤3**：基于XGBoost模型的内置特征重要性评估和排名。

**步骤4**：递归移除影响较小的特征，每次创建一个新的特征子集并重新训练XGBoost模型。

**步骤5**：选择所有迭代中表现最佳的特征子集。

最终，通过RFE和XGBoost方法筛选出的特征包括目标端口、流持续时间、向前和向后包长度等。这些特征子集被证明能够有效地表示网络攻击数据，有助于提高模型性能。

4.类别不平衡处理

在CSE-CIC-IDS2018数据集中，类别之间存在显著的不平衡现象，特别是Web攻击类别的样本数量极少。论文采用自适应合成采样（ADASYN）算法对少数类样本进行过采样，以增强模型对小样本类别的学习能力。ADASYN的核心思想是通过生成少数类的新样本，改善样本分布的平衡性。具体过程如下：

**步骤1**：使用最近邻方法计算少数类样本周围的样本密度。

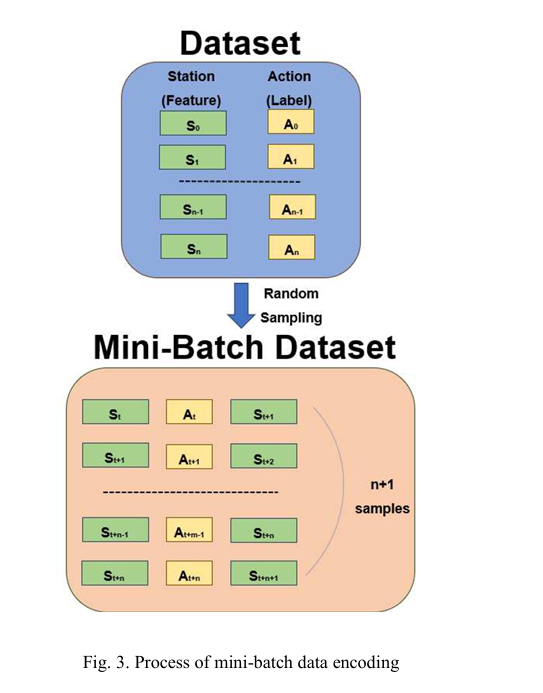
**步骤2**：根据密度计算少数类样本的采样比率，生成所需数量的合成样本。

**步骤3**：根据分布密度，对少数类样本生成新的样本。

**步骤4**：将合成样本添加到原始数据集中，形成新的数据集。

通过ADASYN方法，Web攻击类别的样本数量从93个增加到4994个，有效解决了数据不平衡问题，使得模型在训练时能更准确地分类少数类攻击样本。

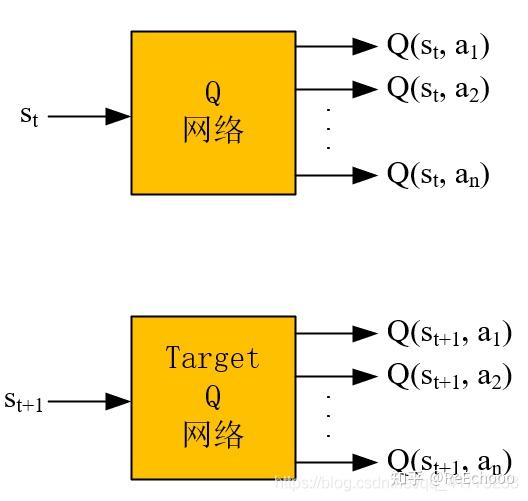
5. Mini-Batch数据编码



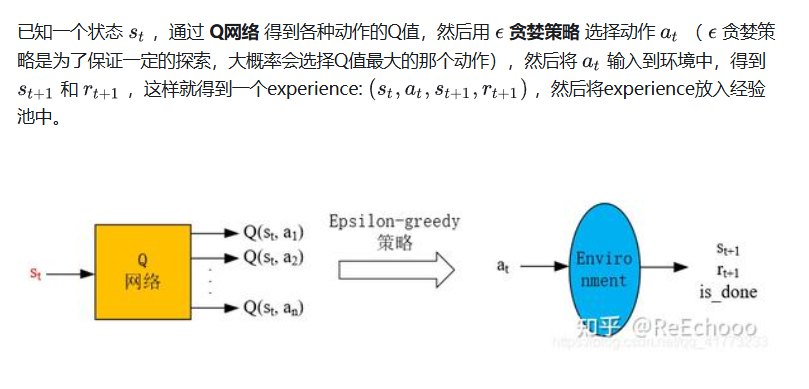
由于CSE-CIC-IDS2018数据集是监督学习数据集，并包含类别标签。为适应深度强化学习（DRL）的输入需求，论文中采用Mini-Batch数据编码方法。具体而言，将每条数据的特征（去除标签）作为当前状态St​，标签作为当前时间步的动作At，下一条数据的特征作为下一时间步的状态St+1。编码格式为St,At,St+1​，满足DRL模型的输入需求。

**二、对比试验部分(DQN与DDQN)**

1.DQN与DDQN的网络结果大体相同：



2.产生experience的过程也相同

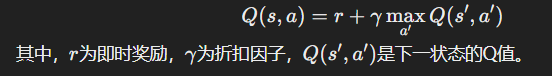


3.网络的更新流程

DQN:

DQN使用单个Q网络来同时执行动作选择和动作评估。在每个训练步骤中，DQN直接使用Q网络选择动作，并计算相应的Q值。

DQN在训练过程中更新Q值的公式为：

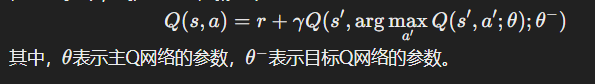


由于DQN依赖单个网络来估计Q值，容易在某些情况下对Q值进行过高的估计，导致模型不稳定，特别是在高维状态空间中，DQN的性能可能会受到影响。

DDQN：

 DDQN采用了两个Q网络，即**主Q网络**和**目标Q网络**。主Q网络用于选择当前的最优动作，而目标Q网络用于估算该动作的Q值。这种双网络结构减少了过高估计Q值的风险。

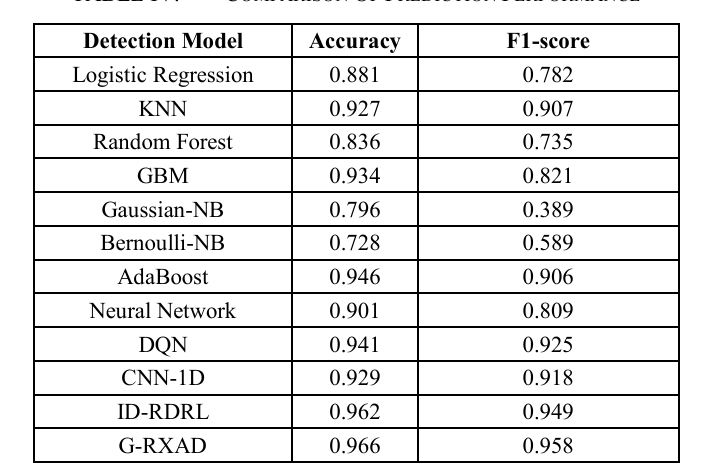
在DDQN中，Q值更新公式修改为：



目标Q网络的权重在训练时并不会频繁更新，而是定期与主Q网络同步。这样一来，DDQN能够更好地平滑Q值估计，提升模型的训练稳定性。

4. DQN和DDQN的性能对比

论文中通过实验评估了DQN和DDQN（G-RXAD）在CSE-CIC-IDS2018数据集上的表现，主要考察了准确率和F1score。



**准确率**：

DQN的准确率为0.941。

G-RXAD模型的准确率为0.9667，比DQN提高了约2.5%。这说明G-RXAD在检测网络攻击时更具准确性，尤其是在复杂和不平衡的网络攻击数据集中，能够更好地识别不同类别的攻击。

**F1score**：

DQN的F1分数为0.925。

G-RXAD模型的F1分数达到了0.9583，比DQN提高了3.3%。F1分数的提升表明G-RXAD在识别少数类攻击时表现更为出色，有更低的误报率和漏报率。





