Result

实验和结果：

使用公共数据集Car\_Hacking\_Challenge\_Dataset\_rev20Mar2021测试我们提出的算法框架，并使用了一些其他的深度学习方法进行的对比。数据集分为动态和静态两部分，我们使用数据集中车辆的动态报文部分，使用80%的数据用于训练，使用20%的数据用于测试。我们的网络框架由图神经网络块和卷积网络块两部分组成，所以需要先把数据按照上述的方法先转换为图数据和01二进制数据。在两种网络块之前有强化学习网络负责动态采集输入检测系统的样本。

卷积网络部分预先训练26个初代，每个个体训练30epoch取最好的精度作为适应性指标。然后经过交叉、变异演化30代，每次取最好的26个个体为下一代的亲本，以此类推。得到30代的精度图像，每一代使用不同的颜色标注出来。从图中可以看出，随着演化过程的进行，精度低的个体越来越少，并且演化出了更高精度的个体。

图网络部分，先把数据转换为图数据，经过图坍缩，图卷积，预测层等得到预测结果。图网络的卷积层数，预测层层数，每个预测层的神经元都使用遗传算法进行优化。一开始随机生成100个初代，从初代选取7个帕累托前沿的个体作为下一代的亲代，进化30代。得到30代的复杂度，flops，为x轴，精度误差，acc\_error，为y轴的图像。图中用红色圆点标出了最后三代个体的点。Flops表示网络识别过程中矩阵运算的次数，除以超网的矩阵运算次数，把flops指标化成0到1的范围。Acc\_error指的是 1-acc，所以acc\_error越小，精度越高。从图中可以看到最后个体进化到图中的左下角的位置，代表更高的精度和更低的复杂度。

本实验对比实验结果为LSTM和DNN和单独CNN和单独GNN

LSTM是使用LSTM和全连接层提取CAN的数据部分的特征。每个CANID都需要单独训练一个完整的神经元网络，所以是比较繁琐的。LSTM提取的是CAN报文里的时序特征，LSTM使用每个位的和下一帧每个位的loss取平均作为整体的loss。在验证时使用取所有位的最大的损失值作为异常信号。我们同样使用了公共数据集Car\_Hacking\_Challenge\_Dataset\_rev20Mar2021进行了验证。使用正常的报文部分训练网络，使用掺有异常报文的数据测试网络。从结果可以看出经过较少的轮数就可以得到不错的结果。在论文中提到可以通过分析某个ID的数据段，一些变化频率很低的位不予考虑。

DNN同样使用了CAN报文的64位的数据段，直接将比特流输入到DNN网络。这个网络的好处是更加有效率，可以不做数据处理直接输入到网络。论文中没有指出网络的具体结构，我们采用了5层全连接，第一层64个神经元用来接收64位CAN报文比特流，第二层是128个神经元，第三层是512个神经元，第四层是256层神经元，第五层32个神经元，第六层输出二分类。通过公共数据集的验证，精度较低，但是神经网络简单而且不需要特别的构造数据。

CNN和我们的网络卷积块是相同的，我使用直接使用了我们的网络框架，使用基因444 4 0 444 直接可以构造和论文中一样的架构。它的精度没有我们算法的结果高。

我们的算法集合了卷积网络的空间特征提取和图网络逻辑特征的两个优势，并且在输出结果时比较两个网络输出的二维变量的差值，取差值较大的网络结果为最终结果。也就是取对样本分辨更加自信的网络的结果。使用这种方法可以让这两种形式的网络相互互补。如表所示，是这几种网络架构的对比结果，可以看到我们的网络可以达到更高的识别精度，这对于网络安全来讲至关重要。

GNN模块也是我们提出的神经网络架构中的一部分，从结果可以看出单独的GNN网络的精度比两个网络结合起来的精度要低。

结论和展望

我们使用多个网络合成构成在保证入侵检测精度的同时，最大限度减小网络的复杂度。据我们所知，在本工作中第一次使用图网络做CAN入侵检测工作，并且仅仅只有图网络检测结果也可以达到95%以上。同时我们汇聚了图网络和卷积网络的双重优点，通过对两个网络输出的结果，使得两个网络的检测结果形成互补。同时利用CAN数据的逻辑特征和空间特征。在本工作中还有一些不足，虽然可以达到非常好的识别精度，和之前的工作对比，我们的网络的复杂度要高一些。我们以后的工作可以更进一步应用演化算法更细致的对网络的结构进行精简。