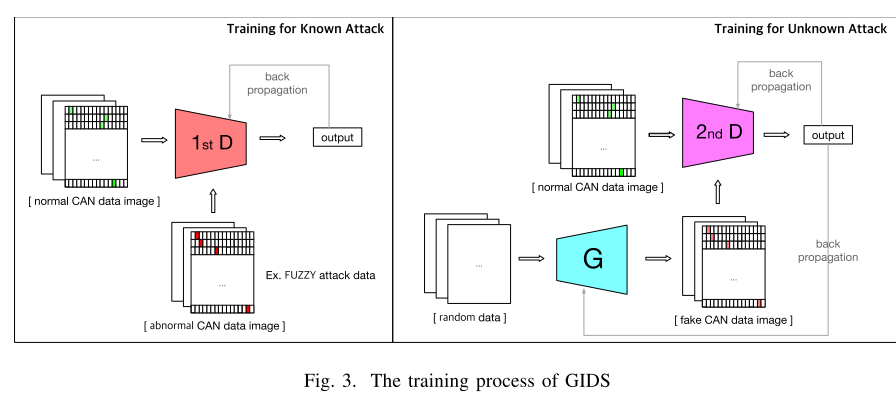
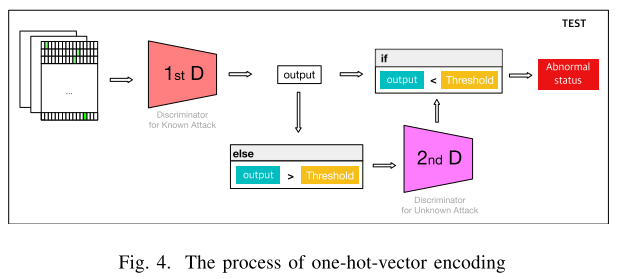
***论文复现***

***GIDS: GAN based Intrusion Detection System for In-Vehicle Network***

***论文使用2个Discriminator进行入侵检测。其中第一个Discriminator检测已知攻击，第二个Discriminator通过GAN训练正常数据和随机噪声，用来检测未知攻击。***





***数据预处理：将一个CAN标准帧ID，编码成3\*16个特征，再将48个CAN报文组成一张图片，得到一个48\*48的图片作为模型输入（论文中输入图片为64\*48）***

***First Discriminator for Known Attack (epoch=100)***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Training Set | DoS Accuracy | Fuzzy Accuracy | Gear Accuracy | RPM Accuracy |
| DoS | 1.00 | 0.67 | 0.42 | 0.42 |
| Fuzzy | 0.3 | 1.00 | 0.73 | 0.98 |
| RPM | 0.56 | 0.69 | 1.00 | 0.50 |
| GEAR | 0.47 | 0.78 | 0.45 | 1.00 |

***Second Discriminator for Unkown Attack（epoch=2）***

|  |  |
| --- | --- |
| Attack Type | Accuracy |
| DoS | 0.95 |
| Fuzzy | 0.97 |
| RPM | 0.99 |
| GEAR | 0.99 |

***Second Discriminator for Unkown Attack（epoch=10）***

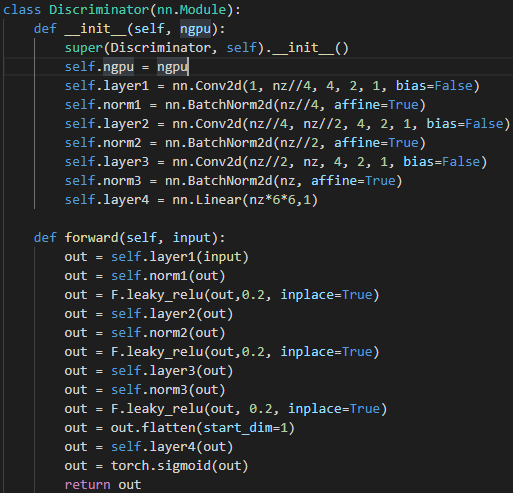
|  |  |
| --- | --- |
| Attack Type | Accuracy |
| DoS | 0.99 |
| Fuzzy | 0.99 |
| RPM | 0.97 |
| GEAR | 1.00 |

***深度卷积网络（与论文中的模型不同）：***

***Generator***



***Discriminator***



***参数：***

***优化器：SGD***

***损失函数：nn.BCELoss()***

***学习率：0.1***

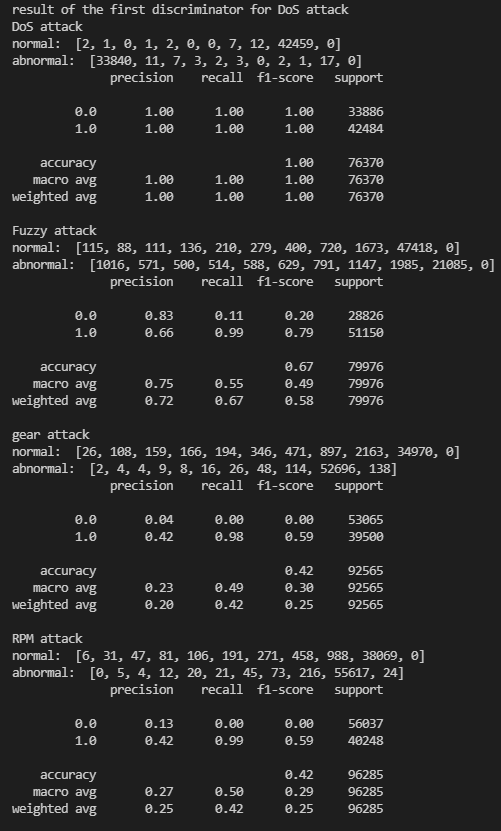
***nz=20***

***噪声：***

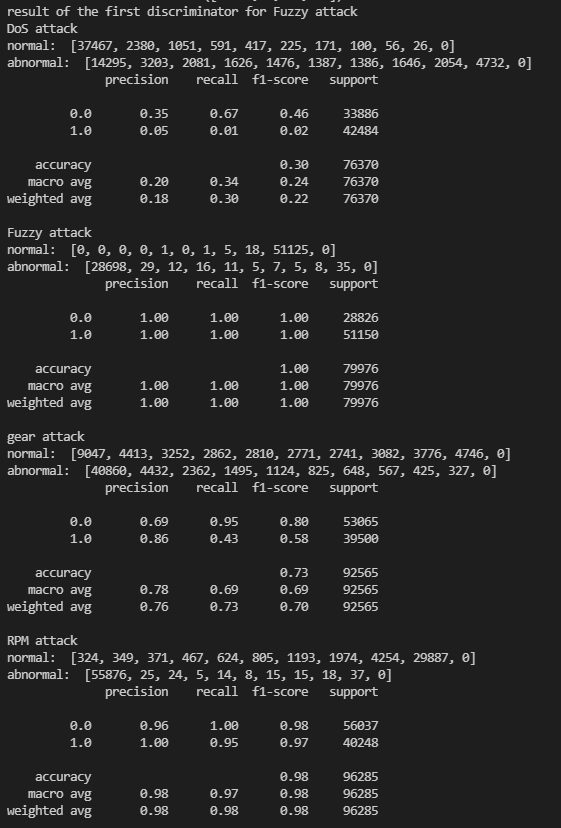


***分类阈值：0.5***

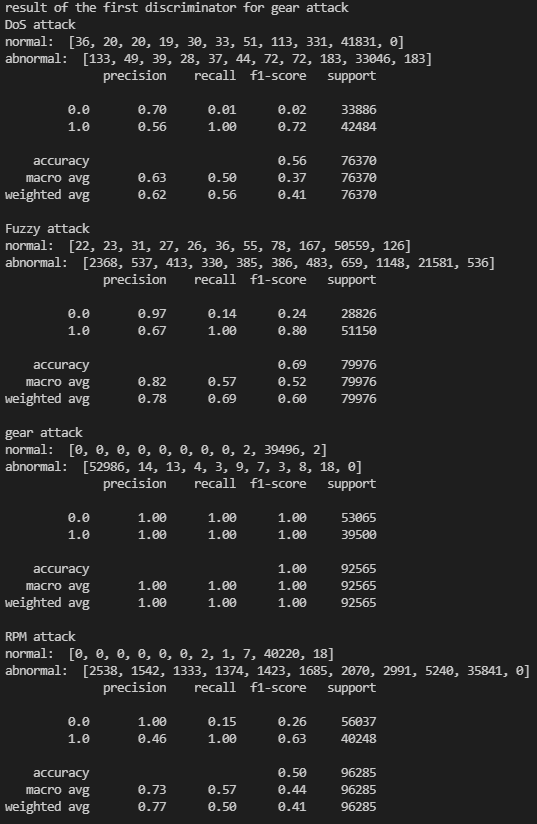
***First Discriminator train with DoS***



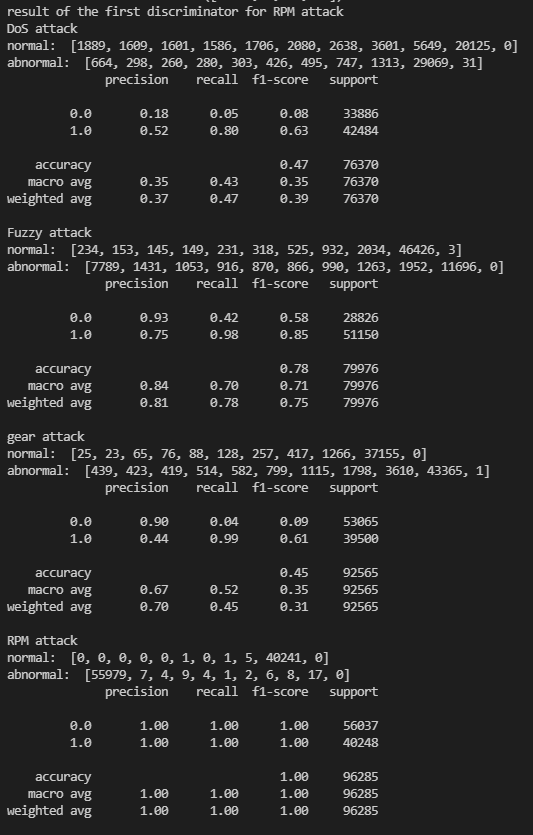
***First Discriminator train with Fuzzy***



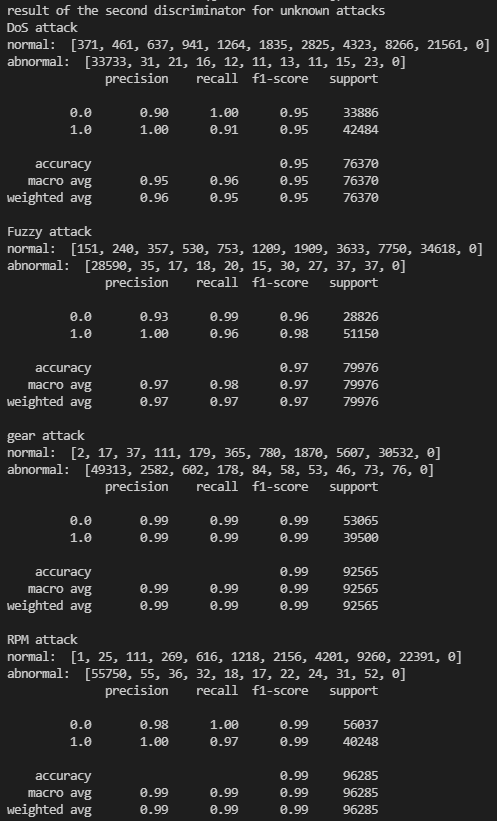
***First Discriminator train with gear***



***First Discriminator train with RPM***



***Second Discriminator train with GAN（epoch=2）***



***Second Discriminator train with GAN（epoch=10）***

