测试子系统帮助文档

1 Gazebo与PX4链路

1.1 修改Gazebo端口

需要在文件“**px4-rc.simulator**”修改，该文件是px4-sitl启动脚本“rcS”所调用的端口文件“px4-rc.simulator”，其路径一般为”~/PX4_Firmware/build/px4_sitl/etc/init.d-posix“。在文件中，修改端口**4560**改成**4561**。

1.2 配置MAVProxy启动参数

配置mavproxy启动参数，`--master=tcpin:127.0.0.1:4561 --out=tcp:127.0.0.1:4560 --cmd="module load attack”`

1.3 启动仿真环境

先启动SITL仿真，如 `roslaunch px4 outdoor3.launch`。再运行mavproxy。

1.4 启动攻击

在mavproxy的console中，输入对应指令启动攻击，对应的攻击参数可以在“attack”模块中进行修改。目前已实施攻击：

- 执行器故障：`attack hardware_backdoor`，修改无人机的电机转速。
- GPS欺骗：`attack gps_spoofing`，修改GPS传感器读数。
- 传感器攻击：`attack sensor_injection`，注入一个新的传感器数据给飞控。

2 QGC与PX4链路

2.1 修改QGC端口

此端口修改可以直接在QGC软件中修改，具体操作“**Application Settings → Comm Links**”，添加一个新的连接，并设置**UDP连接**，端口为**14551**。

2.2 配置MAVProxy启动参数

配置mavproxy启动参数，`--master 127.0.0.1:14550 --out 127.0.0.1:14551 --cmd="module load attack”`

2.3 启动仿真环境

先启动SITL仿真，如 `roslaunch px4 outdoor3.launch`，再运行mavproxy，最后运行QGC。

2.4 启动攻击

在mavproxy的console中，输入对应指令启动攻击，对应的攻击参数可以在“attack”模块中进行修改。目前已实施攻击：

- GCS任务篡改：`attack mission_modification`，修改GCS发送任务的WAYPOINTS。
- GCS欺骗：`position_modification`，修改PX4发给QGC的位置信息，从而干扰QGC获得无人机准确的位置信息。
- 强制上锁命令：`disarm force`，强制无人机上锁。

3 MAVROS与PX4链路

3.1 修改MAVROS端口

修改MAVROS端口需要在launch文件如“**outdoor3.launch**”修改，其路径为”~/PX4_Firmware/launch”。将MAVROS端口从**24540**改成**24541**。

```
<group ns="iris_0">
        <!-- MAVROS and vehicle configs -->
            <arg name="ID" value="0"/>
            <arg name="ID_in_group" value="0"/>
            <arg name="fcu_url" default="udp://:24540@localho
```

3.2 配置MAVProxy启动参数

配置mavproxy启动参数，`--master 127.0.0.1:24540 --out 127.0.0.1:24541 --cmd="module load attack”`

3.3 启动仿真环境

此处一定要**先运行mavproxy**，先启动SITL仿真，如 `roslaunch px4 outdoor3.launch`。

3.4 启动攻击

在mavproxy的console中，输入对应指令启动攻击，对应的攻击参数可以在“attack”模块中进行修改。目前已实施攻击：

- 键盘控制反向：`attack reverse_velocity`，反向MAVROS的键盘速度控制。
- 强制上锁命令：`disarm force`，强制无人机上锁。